Calculating malware severity rating using threat tree analysis

By

Asheer Malhotra

A Thesis
Submitted to the Faculty of
Mississippi State University
in Partial Fulfillment of the Requirements
for the Degree of Master of Science
in Computer Science
in the Department of Computer Science and Engineering

Mississippi State, Mississippi

May 2015

ProQuest LLC.
789 East Eisenhower Parkway
P.O. Box 1346
Ann Arbor, MI 48106 - 1346

Calculating malware severity rating using threat tree analysis

By

Asheer Malhotra

Approved:

_____

David A. Dampier
(Major Professor)

_____

Robert Wesley McGrew
(Committee Member)

_____

Edward B. Allen
(Committee Member)

_____

T.J. Jankun-Kelly
(Graduate Coordinator)

_____

Jason M. Keith
Interim Dean
Bagley College of Engineering

Name: Asheer Malhotra

Date of Degree: May 8, 2015

Institution: Mississippi State University

Major Field: Computer Science

Major Professor: Dr. David A. Dampier

Title of Study: Calculating malware severity rating using threat tree analysis

Pages in Study: 327

Candidate for Degree of Master of Science

Malware analysts and researchers around the world are looking for innovative means of malware detection and classification. However, one concept of malware analysis that lacks focus is the rating of malware based on their feature set and capabilities. Malware severity rating is needed in order to prioritize the utilization of resources towards the analysis of a malware by an organization. This thesis proposes the utilization of threat trees for calculating malware severity using a goal oriented approach. This approach is applied to a set of sophisticated malware to study its contribution towards articulation of a useful severity rating.

DEDICATION

To Group Captain & Mrs. Malhotra.

ACKNOWLEDGEMENTS

I thank the Department of Computer Science and Engineering for support during this research. I thank Dr. David Dampier for his valuable guidance during the course of this research. I thank Dr. Robert McGrew for his guidance with reverse engineering towards this research. I thank Dr. Edward Allen for his guidance and valuable comments on this thesis.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER I

INTRODUCTION

Malware can generally be defined as pieces of code that intend to cause harm to a system. Computer malware today has evolved from being simple pieces of code to highly sophisticated software modules that perform espionage and millions of dollars' worth of damage to an organization's systems. Evasion techniques such as polymorphism and metamorphism allow for a piece of malware to retain the same functionality while avoiding detection by anti-virus (AV) software. The sheer volume of malware samples combined with advanced anti-analysis techniques means that a considerable amount of resources need to be spent on analysis of various malware. Limited resources make this a highly difficult task. Malware analysts today are in need of setups that can reliably provide a method of prioritizing malware so that the organization's efforts can be utilized effectively towards analyzing malware that may pose a greater threat than common variants of already existing malware.

This thesis aims to provide an introduction and description of a rating system that can be used to rate malware and estimate its severity. This rating of malware will provide the malware analysts with an idea of the severity & complexity and help assess the threat level of the malware. Malware can hence be prioritized and efforts can be diverted to a malware sample that poses a greater potential threat. This thesis will provide an introduction to the concept of threat/attack trees and leverage it to model a malware's

threat vectors. These vectors can subsequently be used to calculate a normalized rating of the malware.

Before this thesis delves into details of the proposed methodology, research conducted and subsequent results, it is imperative to understand the concepts of threat trees and malware analysis. Also important is to understand the current research and implementation landscape to realize the lack-of and utility of the proposed approach.

1.1 Background

The number of malware samples available today is huge and growing. Malware today consists of carefully crafted software modules that have the ability to perform a wide variety of functions and sometimes receive commands from control servers in real time (C&C)[7]. Malware analysts use a number of techniques such as static code analysis and dynamic analysis of malware samples to analyze their behavior today. Static code analysis is a cumbersome and difficult task due to the very nature of reverse engineering and analysis of machine code (assembly language). Dynamic analysis is a riskier approach to malware analysis that requires virtual machines and process monitors to trace the execution of malware on a sample system. As evident, these activities require a great amount of effort and a highly specialized skillset. With limited resources, an organization cannot afford to analyze each and every malware sample manually and then come up with mitigation strategies for them. Malware in the wild may include everything from new samples to already recognized re-packed samples (polymorph-ed again and again). Organizations constantly aim to put in efforts for malware that may cause the most harm to their systems. Hence prioritization of existing and new malware samples is required so that malware analysts can decide how much effort to utilize towards

countering a malware threat. Prioritization of malware would not only require analysis of malware to identify its capabilities but also a reliable method to be able to model these capabilities into threats and hence evaluate the malware's severity (ability to do damage).

1.1.1 Threat Trees

In order to prioritize a threat, we need to be able to successfully and comprehensively model the threat. This includes an exhaustive search for all feasible and infeasible scenarios that can cause harm to the system. Threat trees/Attack trees were popularized by Schneier[44] to provide a method for threat modeling. A threat tree consists of a tree based structure illustrating the threats to the system. Here, the goal of the adversary is set as the root node of the tree. All sub-goals that need to be achieved in order to achieve the root goal are placed in the tree as the children of the root node. Fig. 1.1 illustrates a threat tree modelling the threats where the ultimate goal is to open a safe[44]. The root node (Open Safe) can be achieved by achieving any of its immediate child goals.

Articulation of threat trees requires extensive security experience and may also require domain knowledge of specialized domains. Comprehensive threat trees may require more than one expert and may take more time to articulate.

Threat trees are used in multiple fields of security to model threats. The example above is just one of the domains of its use. Since this thesis is in computer science it is useful to illustrate that threat trees are used in multiple phases and activities of software development. One of the major uses of threat/attack trees is in the field of requirements engineering.

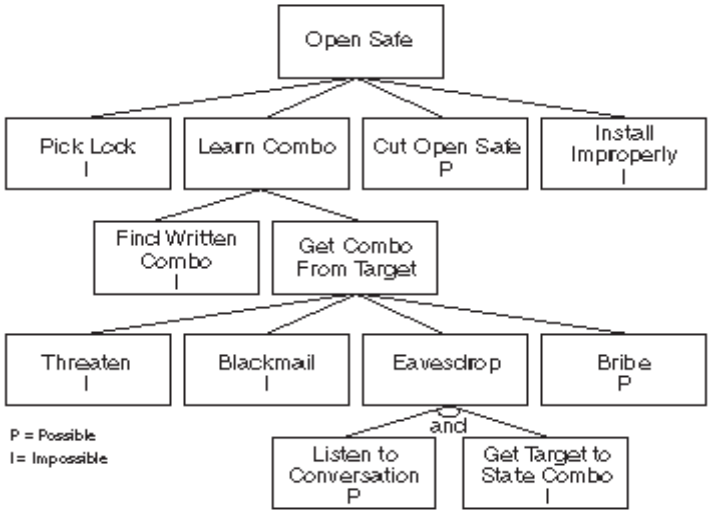

Figure 1.1 Sample threat tree to break into a safe[44]

Threat trees are used to model threats and are expressed in either a pictorial form or a textual representation. Threat trees have been successfully used with techniques such as misuse cases[47], abuse cases[31] etc. to provide a formalized requirements specifications set. Threat trees, once articulated, can also be used in verification of test scenarios[29]. Apart from all these applications, threat trees have been used in threat modelling to find out potential attack vectors on a system. Hence threat trees contribute to a wide variety of fields and have proven to be a highly useful threat modelling technique.

Apart from threat articulation, Threat trees can be used to calculate the feasibility and cost of each attack on the system. Every sub-goal of the tree can be provided a feasibility rating (such as P=Possible, IMP=Impossible) and, a cost (amount of cost or effort required). This helps the analyst evaluate the probability of a particular attack

sequence on the system. This functionality will be leveraged by this thesis to provide a cost/weight to every feature of the malware.

1.1.2 Malware Analysis

In order to model a threat from a piece of malware, we need to be able to identify the features and functionalities of malware samples. These features not only include modules implemented to cause harm but also modules that are used to evade anti-virus (AV) mechanisms. This includes detection of malware using host and network signature schemes, heuristic and behavioral techniques. Analysis of malware functionality is done via two broad categories of techniques:

- Static Analysis: Analysis of reverse engineered code of malware is called static analysis. This code is generally of the IA32 instruction set[23]. Once generated the assembly language code needs to be analyzed for functionality and patterns. Tools such as IDAPro[21] or Immunity debugger[22] provide the means of fast and reliable code reverse engineering for static analysis.
- Dynamic Analysis: Dynamic analysis is used in instances where static analysis is not enough to successfully evaluate the malware. These situations might arise when:
    - The malware is packed – Encoded to avoid detection/easy analysis.
    - Requires a specific context to make sense – E.g. System date and time may need to be provided to understand exact functioning of the malware.

- We may also need to know certain intermediate values at some point in the malware's execution.
- Exact parameter/ argument values for functions need to be recorded.

Dynamic analysis tools such as WinDbg[62], OllyDbg[36] etc. provide a comprehensive environment for running and analyzing malware samples.

Apart from dynamic and static analysis, other techniques such as the use of virtual machines, hypervisors, and emulators may also be used to analyze malware without any potential harm to the underlying native system. Malware authors today have been able to implement mechanisms that may be able to detect analysis environments and thwart the analysis of malware code. This has given rise to an arms race where malware authors are constantly trying to outdo malware analysts and vice versa.

1.2 Research Hypothesis

The hypothesis for this research is:

Attack trees provide a mechanism for calculating a useful severity rating for malware that can be utilized to assess their threat level.

In order to verify the hypothesis stated above, we need to be able to fulfill the research goals. Research goals of this study are:

1. Articulation of a method to calculate severity ratings of malware.
2. Show that threat trees can be successfully used to articulate malware threats.
3. Present analytical evidence that threat trees can be used to calculate malware severity ratings that aid in evaluating the threat level of malware.

The process of carrying out the research objectives includes analyzing samples for various features, construction of threat trees, assigning weights (that represent the maliciousness of a feature of the malware) and calculating severity ratings of malware. The severity rating can then be used to prioritize analysis of malware. The severity rating along with the attack tree patterns can also contribute to the building of detection mechanisms to identify and mitigate a variety of malware.

CHAPTER II

RELATED WORK

Reverse engineering and analysis is primarily done to understand the functional complexity and danger posed by a piece of malware. Many organizations and academicians have attempted to find ways to detect and classify malware. However, it is not the detection or classification that we focus on in this thesis. This thesis intends to focus on the problem of rating/ranking malware such that an analyst can prioritize his/her efforts towards more harmful malware. Successfully rating malware requires us to create a holistic view of the threats posed by the malware. In order to successfully model a threat to devise a mitigation strategy, we need a proven and reliable technique such as threat trees. Threat trees have been used across various industries and are considered a highly formal method of threat articulation.

A technique can be developed that utilizes the strengths of malware reverse engineering and threat trees to model each malware's threats into a visual representation along with corresponding individual threat ratings. This technique can prove to be a useful and reliable method of providing a severity rating for malware. The purpose of this literature review is to:

1. Review the usage of threat trees across various fields of computer/information security to prove the value of threat trees as a threat modelling technique.

2. Find evidence (if any) that threat trees have been used to model/detect/classify malware in the past. This will strengthen our argument that threat trees can be used to model the behavior of malicious software.
3. Review the different ways in which malware analysis has been used to detect, classify and rate malware.

This review will show that although there has been a lot of work around malware classification, there is little or no evidence of any efforts to rate malware to ease the pain of malware analysts. Hence this review aims to present the conviction that the need for a technique of malware rating is imperative. We aim to articulate a novel technique using threat trees.

2.1 Threat Trees

Per Schneier [44] "threat trees provide a formal, methodical way of describing the security of systems, based on varying attacks." This means that threat trees can be used to model threats in systems such as high assurance systems that require formal proofs/assurances of security. Varying attacks can be clubbed together according to high level goals. Different attacks can also be combined to produce a sequence/combination of attacks needed to carry out a higher goal. However, the real utility of threat trees is that they can be used to provide values to nodes to derive further information from them. These values include values such as the cost associated with a node, effort involved with a sub-goal, feasibility of a sub-goal, conditions for fulfillment of a goal etc. These features extend threats trees from being just a pictorial representation of threats into an

elaborate threat sequence diagram that is goal oriented and provides additional value to the threat modelling process.

2.1.1 Threat Trees and Threat Modelling

Threat modelling is the most popular use of threat trees. It involves discovering all the ways in which a particular type of harm can be carried out in the system. This can be done via multi-stage attacks[30] using multiple known or 0-day vulnerabilities. Threat trees aim to consolidate all the possible attack vectors under a common goal thus presenting a single structured view of the threat model. Even within the field of computer security, threat trees have been used to model a wide variety of threats:

- Traditional usage of threat trees: Wang et al. [59] have implemented attack trees towards the modelling of scenarios that occur during a distributed denial of services (DDoS) attack. Using an enhancement of attack trees known as Augmented Attack Trees (AAT) a DDoS attack can be modeled as well as detected based on the attack signature of the malicious steps involved. A similar example of the utility of threat trees is provided in [60] where they were used to model SQL injection attacks[49] and create signatures that can be used to identify SQL injection attacks based on the event types and data involved.
- System security modelling: Apart from individual attack modelling, threat trees have also been employed towards survivability analysis of multiple systems. Survivability analysis consists of identification of a system's assets and then computing their ability to survive the attack[16]. Survivability here means that the system should be able to offer continued

service in case of failure or attacks – also known as Availability[41] in the security domain. Xiao et al. [63] attempt to provide a survivability analysis of Service Oriented Architectures (SOA)[45] using a two-step approach – Attack scenario analysis via attack trees and survivability assessment using node attributes of the tree such as monetary effect, time and severity of attack.

- Threat trees and unconventional systems: Another category of systems that have benefited from the usage of threat trees is Supervisory Control and Data Acquisition (SCADA) systems[8]. SCADA systems monitor and control industrial control systems (ICS)[20]. Recent research into SCADA systems has shown that any successful attacks on SCADA systems could have massive consequences on human life and infrastructure. The discovery of highly specific malware such as Stuxnet[58] has led to large scale research in vulnerability analysis of SCADA systems. Apart from SCADA systems, threat trees have been shown to be useful towards threat modeling for internet based systems such as Internet Voting Systems and Internet Banking Systems. Research has proved that although online systems have such a variety of environments of operations, threat trees can be used for modeling highly generic attack scenarios[37]. Emergence of online systems has given rise to the usage of social networks systems (SNS) such as Facebook[19], Twitter[55] etc. Threat trees have also proven useful toward the identification of threats and attack scenarios for websites such as Facebook[61].

- Threat tree variations: Besides modelling threats, threat trees have been used to model protection and mitigation strategies for systems. An example of this practice is that Edge et al. [17] have created a set of Attack trees for DDoS attacks similar to [59]. However, this has further been extended to create protection trees[17] that illustrate how the system can be strengthened or fortified and attacks be prevented and/or mitigated. The protection strategies/sub-goals along with information such as cost and probability of success further strengthen the use of this model. Another variation of threat trees that has been used to model threats is the use of vulnerability trees towards vulnerability complexity analysis[56]. This variation of threat trees consists of a hierarchy of vulnerabilities of the system that assists the security experts in the decision process regarding security and threat assessment. Camtepe et al. [9] introduced the usage of enhanced threat trees towards construction of tree automata that changes the system's security state based on the transition from one sub-goal (node) of the threat tree to another. This helps create a real time view of the system's security landscape while being able to identify and trace the attack vector and its consequences to the system.

It is evident from the discussion above that threat trees have been highly useful towards multiple fields of threat modeling and system security assessment.

2.1.2 Threat Trees and Malware Research

The most popular usage of threat trees in malware research has been to use malware functionality as a leaf of a threat tree while expressing the threat model for a

larger system. Khand et al. [26] have demonstrated how malicious code can be used as a sub-goal towards achieving a high level goal (root node) of an attack tree used to model the security of a system. Analysis of malware requires the analyst to focus on the bigger picture instead of the smaller details of the reverse engineered code. This concept is utilized by threat trees in the sense that they provide a level of abstraction by providing a view of the sub-goals of the system i.e. focusing on the "what" instead of the "how". An example of this strategy is shown by Mishra et al. [33] where an analysis of Stuxnet has been performed and subsequent threat trees have been constructed to understand the security goals, functionality, vulnerabilities and commercial software applications used and targeted by the malware. Cong et al. [13] attempt to use threat trees towards the detection of Trojan horses. This technique provides a different approach where a generic attack tree can be constructed for a sequence of API calls to perform a malicious activity on the system. This tree can then be used to pattern match against the sequence of APIs called by a Trojan horse to accomplish its goals. The attack tree is constructed based on an intelligent mechanism that evaluates whether an API can be used by a Trojan horse based on mutual information and text classification [25]. This technique does not address issues such as Polymorphism and the ability of malware to run in kernel mode thus by-passing Operating System API calls and directly using Native OS APIs.

2.1.3 Standardized Threat Modelling Frameworks

As described in the previous sections, a substantial amount of research has been carried out towards the articulation of techniques towards the creation of threat trees. However in order to be able to create uniform threat trees and in turn enable analysts and experts to be trained towards the same, standardized procedures and dictionaries are

required. This requirement in the academic and commercial domains led to the creation of standardized threat modelling frameworks.

An example of an extensively used threat modelling framework is the Cyber Observable Expression (CyBox) [15] framework that was created by MITRE to aid the conversion of security incidents and alerts into standard representations based on provided vocabularies and rules. Evolution of the CyBox framework led to the creation of the Structured Threat Information (STIX) [48] which is intended to provide a representation of various types of attack vectors.

Although both these frameworks have proven threat modelling capabilities, a language for the illustration of malware based threats was required to be able to comprehensively model malware behavior and characteristics. This lead to the creation of the Malware Attribute Enumeration and Characterization (MAEC) [28] library. It introduces many new standards for the characterization of malware attributes and properties and leverages existing threat definition frameworks such as CvBox, STIX, CVE to enhance the definitions for malware capabilities.

A high level description of MAEC has been provided below. This description is essential since this study leverages the MAEC framework towards the articulation of well-formed threat trees derived from the analysis of various malware samples.

To provide uniformity, the MAEC framework consists of modelling a malware sample's features into three levels of high, mid and low level functionalities:

1. Actions: The lowest level of illustrations in MAEC is termed as an Action. Actions represent the lowest atomic level actions performed by the

malware. This may be as simple as the creation of a file or an HTTP GET request to fetch content from the CnC server.

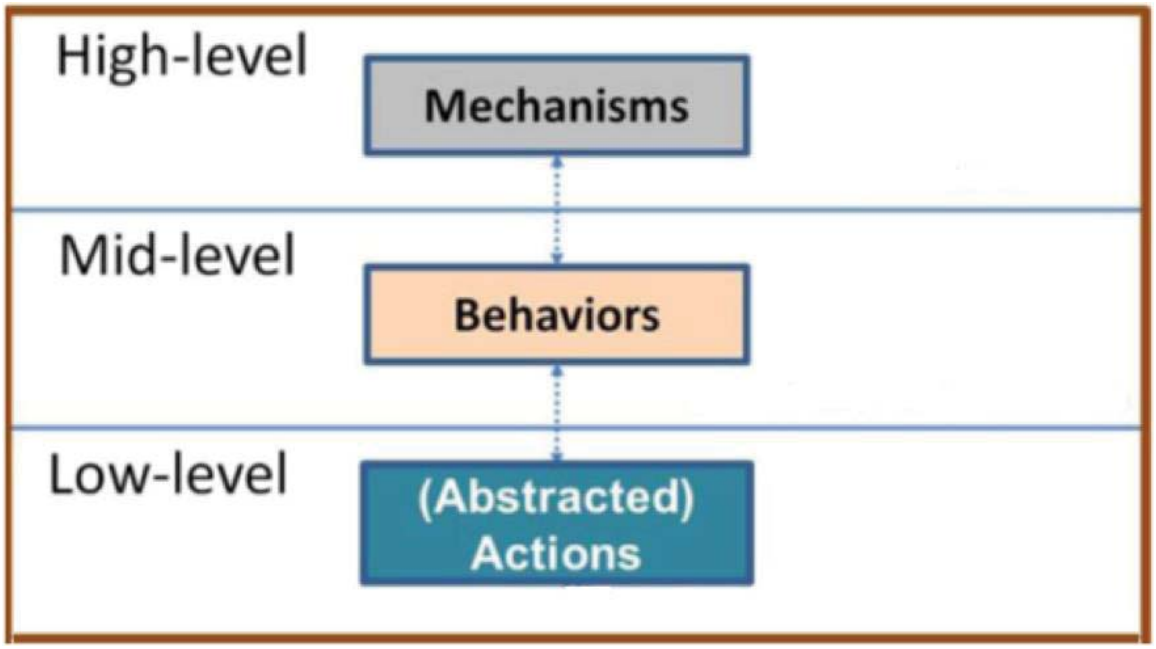

Figure 2.1 Malware Feature Hierarchy Illustration[5]

2. Behaviors: The actions are further grouped or organized into mid-level Behaviors. Behaviors group actions together to provide motive to the actions. For example the Action of the “HTTP GET request from CnC” can be grouped under the behavior “fetch commands to execute”. This immediately gives meaning and purpose to the action.
3. Capabilities: The highest level functionality is called a Capability. Capabilities represent the high level functionality of the malware. One such example of a capability is to “Run arbitrary commands”. This feature of the malware can consist of various mid-level behaviors. Hence the

capability of “Run arbitrary commands” consists of behaviors “fetch commands to execute” + “execute commands received” which in turn have corresponding actions.

This concept of Capabilities, Behaviors and Actions provides a natural hierarchy to the a malware’s functionalities and hence can be leveraged to create threat trees consisting of goals and sub-goals. This coupled with the fact that MAEC has standard XML schemas to formally represent malware characteristics results in the MAEC framework being a viable option for malware threat tree articulation for this study. Figure 2.1 provides an illustration of the hierarchy of high, mid and low level goals or features of a malware in the MAEC framework.

Other than its obvious utility towards building threat trees for malware, the MAEC framework also remedies other concerns that arise during the articulation of standardized threat trees. These remedies have been discussed in Section 3.4.1.

2.2 Malware Rating and Classification

This section provides an introduction and discussion on the research carried out around malware rating and classification.

2.2.1 Malware Rating

There is a huge set of malware plaguing information systems around the world. Symantec has discovered approximately 23 million pieces of malware to date [10]. This includes major malware families that have polymorphed variants. Due to this huge number of threats that are ever increasing, it becomes paramount for security organizations to be able to mitigate threats that pose the most danger to its internal and

customers' systems. Due to the lack of resources (both- human and technical, automated systems), it is essential to successfully identify malware that may pose a greater threat than others. These malwares can then be further analyzed in detail to provide solutions to their threats.

However, currently, most AV distributors do not have such a severity rating for use- thus making the threat mitigation process longer and cumbersome. Currently Symantec employs a threat severity calculation system that uses limited characteristics of the malware and its current infection spread in the wild[53]. These characteristics include the extent to which a malicious program has spread in the wild, the damage caused by the malware so far (this is not in terms of money – it refers to the effect the malware has on the availability of services and systems) and the rate at which the malware spreads in a system. Based on the criteria, the malware can be classified in any of the 5 categories of severity ranging from very severe (category 5) to very low (category 1). Microsoft uses a similar rating system based on the "alert level" assigned to a particular malware sample[1]. Here, 'severe' means a widespread or extremely malicious program, while 'low' means a potentially unwanted information collecting software. Sophos also defines a "threat prevalence" level for malware[52]. However, this technique attempts to define the severity based on the exploiting capabilities of vulnerabilities that may be patched, unpatched, 0-day, widely prevalent etc. Researchers in the past have made attempts to rate malware and have proposed a malware rating system[3]. This attempt aimed to rate malware based on a very broad range of characteristics and weighted scores. Also there was no provision for including known vulnerabilities that exploit software thus affecting the severity of malware.

2.2.2 Malware Classification

Although there has not been a lot of research in the industry and academia towards the creation of a reliable malware rating methodology, there has been substantial research with novel ways to classify malware samples into a known family of malware. This includes having to study the behavior of malware and identify and match the characteristics of the malware to existing databases/findings. This review of the research towards analysis of malware gives us a fair idea about the various techniques used in malware analysis and strengthens the argument that various techniques can be used towards quick analysis of malware to expedite the process of feature/functionality identification thereby expediting the process of construction of threat trees and subsequent calculation of severity ratings.

Linger et al. [27] use the concept of function extraction to compute the behavior of malware. This involves statically analyzing the malware sample and computing the semantics of the code to obtain a simplified version of the assembly language code for the malware. On obtaining the semantic structure of the malware, further analysis is possible to recognize the functionality of the malware. Islam et al. [24] use the concept of static analysis too that involves Function Length Frequency (FLF) and Printable String Information (PSI) to create a unique signature for malware samples. Function length frequency[51] is the frequency with which a function length occurs in a malware. Printable string information[50] is a technique that involves the generation of a digital fingerprint based on the combination of printable strings in the malware. Both FLF and PSI are then used to create a unique digital signature, which is then used to compare it with existing databases of malware signatures thus providing a method of easy

identification of malware. However the pre-requisite for this technique is that all pieces of malware must be unpacked. This may not be the case for most malware out in the wild. Yusoff et al. [67] present the concept of Class target operation (CTO) to classify malware samples into broad categories based on the type of targets that a malware works on. These targets include data, application, system etc. Although the authors suggest that mitigations for the malware can be produced based on the class of targets it works on, the fact is that many malware in the wild may target multiple types of entities and thus may need a composite mitigation strategy. Christodorescu et al. [11] also provide a way to perform static analysis of malware using Control Flow Graphs (CFG). This technique is further enhanced by Bonfante et al. [6] to create reduced CFGs and produce tree automata that match the shape of the CFG to an existing malware CFG database to detect malware.

Apart from static analysis that largely requires malware samples to be unpacked before analysis of code, dynamic analysis focuses on the behavior of malware in action. Dynamic analysis is a popular technique since it provides us with real life data about the malware without having to deal with the complexity of code and the hassle of obfuscators. Yin et al. [65] present an approach that involves the construction of taint graphs that trace marked sensitive information flow and usage throughout the system. The taint graphs are matched with policies that identify malicious behavior to detect malware. This technique involves the use of disposable virtual OS machines (that may not be used multiple times) to run malware samples thus making it a dynamic analysis routine. Nari et al. [35] utilize the network usage of a malware sample by creating network behavior graphs. These graphs are created using packet and dependency analysis

of the various protocol packets. The graphs are then analyzed to produce information on features of the graphs such as graph size, root-out degree etc. Once this information has been extracted, the pieces of malware are then classified based on similarity of features into various malware families. This technique is shown to have performed better than five popular anti-virus programs using only network packet analysis. Morales et al. [34] built infection trees based on data transitivity and parent-child process relationships to detect and analyze malware patterns. The infection trees were compared to predefined method call rules to determine if the sequence of system calls or APIs is malicious in nature. Zolkipli et al. [68] use dynamic malware analysis to create a profile of every malware sample based on resource usage patterns. The profile is then matched to an existing database that consists of profiles for popular malware families.

It is evident from the discussion above that there has been a lot of research into analyzing and identifying malware behavior, there has been little or no effort towards analyzing the behavior and functionality of malware towards implementing a rating system. This thesis attempts to show that the usage of threat trees towards analysis of malware and subsequent articulation of severity ratings is a novel and worthy technique.

CHAPTER III

METHODOLOGY

The main objective of this research is to introduce the usage of threat trees towards calculation of a severity rating of malware based on its feature set. The research objective is as follows:

> To formulate a methodology using threat trees for the analysis of malware to create a goal-oriented & capability dependent malware severity rating system.

This leads to the formulation of a formal hypothesis for this research endeavor:

> *"Attack trees provide a mechanism for calculating a useful severity rating for malware that can be utilized to assess their threat level."*

In order to verify the hypothesis stated above, we need to be able to fulfill the research objective (also stated above). This can be accomplished by dividing the high level research goal into sub-goals. Research sub-goals of this study are:

1. Articulation of a method to calculate severity ratings of malware.
2. Show that threat trees can be successfully used to articulate malware threats.
3. Present analytical evidence that threat trees can be used to calculate malware severity ratings.

The process of carrying out the research objectives includes analyzing samples for various features, construction of threat trees, assigning weights and calculating ratings of

malware. The severity rating can then be used to prioritize analysis of malware. The severity rating along with the attack tree patterns can also contribute to the building of detection mechanisms to identify and mitigate a variety of malware.

3.1 Severity Rating

Before this thesis explains the approach carried out to verify the hypothesis, it is very important to provide a definition of the "Severity Rating" of the malware. Severity rating of the malware in this study means the extent of damage the malware will cause to a target system provided it is run on the right platform and under ideal conditions for it to run solely based on its functionality. Hence this study does not take into consideration the environmental/infrastructural factors needed by the malware to be more (or less) malicious such as an organization's assets. For example, the study assumes that the malware is executed on the correct operating system version. However, this study does take into consideration the interdependencies between the various features of the malware needed to successfully achieve its highest level goals.

In Section 3.5 the weight of each sub-goal in the tree will be defined. This weight represents a combination of the degree of maliciousness of the goal/feature and ease with which the goal can be achieved by fulfilling its sub-goals. The focus of this study is to measure how feature-rich the malware is and then derive the overall degree of maliciousness of the malware.

3.2 Selection of Samples

Malware samples today consist of a wide variety of features and fulfill a range of objectives. These features can be functional in nature or purely implementation based.

The objective of this activity is to choose samples that provide maximum experimental/test coverage in terms of objectives, targeted applications and impact of the malware. The following criteria were chosen to select malware for analysis:

1. Features of the malware: Features of malware include concepts such as information stealing(spyware), holding the system for ransom, creating backdoors on the target for easy access, dropping other malicious software onto the system (Trojan horses) etc. Having seen capabilities such as these in the wild it becomes very important to be able to construct threat trees corresponding to these capabilities in order to prove the utility of the approach.
2. Packed malware: Almost all sophisticated malware today want to evade detection mechanisms. This consists of the activity of obfuscating malware[66] code in order to evade signature based detection systems. Not only for anti-evasion, using existing and custom software and techniques malware can encode their code to thwart manual/detailed analysis by malware analysts and heuristic based detection systems. Such malware also needed to be analyzed in order to determine the effectiveness of the proposed threat-based severity rating mechanism. This thesis will later illustrate that the obfuscation of malware does not affect the functionality of the malware that is intended to be evaluated. It is simply a means of anti-evasion and anti-analysis. However due to completeness of the test set, certain packed malware samples have been included in the test sample set.

3. Technical Abilities: Evaluation of what the malware does (features) is not enough to prove the effectiveness of any severity rating mechanism. Also of significance is the way the malware implements its capabilities (how). For example, Xorer.F[64] has the capability to spread by infecting other files in the system using a traditional file infection mechanism. This technique needed to be illustrated as part of the threat-tree. On the other hand Bangat[18] has the ability to spread by trojanizing(infecting) currently running processes in the system using in-line code injection[46]. Hence code injection needed to be illustrated as part of the threat tree for Bangat. The test set needed to cover a majority of the prevalent technical abilities of malware in the wild.
4. Platform: Samples chosen for analysis needed to be ones that had a high degree of infection. This needed evaluation of the platforms that are most severely affected by malware today. Based on this requirement all of the malware samples chosen for analysis were Windows[32] based malware. This is due to the popularity of Windows as the choice of platform among malware authors and target users. Also included in the sample set is a malicious PDF[54] sample. The justification behind this decision has been provided in a subsequent evaluation criteria (#6).
5. APT malware: Advanced Persistent Threats (APT) malware is malware that has been created by a malware author group with standardized software engineering practices. Also characteristic to such malware are their objectives which primarily include cyber espionage such as

sabotaging systems and stealing information from specified targets. This study would not be complete without the analysis of APT malware. Hence a majority of malware in the sample set have been chosen partly because they belong to active APT groups and partly because of the fact that they are highly feature-rich in nature.

6. Special malware: Based on the trends in the wild, there are certain pieces of malware that serve specific purposes such as dropping and executing further malware from infected sites. This usually involves the practice of exploiting an existing vulnerability on the target. In order to evaluate such malware this study needed a non-executable sample that appeared to be harmless to the untrained eye. Examples of such samples include Microsoft Office based samples and PDF samples. A sample was chosen that appeared to be a benign PDF but had exploits embedded in it that executed shellcode in the system once the exploit was successful. Although categorized as a special category of malware in this study, such malware are by no means a corner-case in malware samples. The wild is flooded with such malware due their ability to trick the target-user into thinking that they are non-malicious documents. Since such malware are usually accompanied by social-engineering and phishing artifacts such as emails to fulfill execution on the target system this study does not consider the activities involved to run such malware on the target as the malware's capabilities. The scope of this study is limited to evaluation of the capabilities of the malware included as part of it execution process. This

sample also allowed the study to evaluate the effectiveness of threat-tree articulation for CVE[12] based samples.

Based on the above listed criteria the following malware samples were selected for the study:

Table 3.1 Malware Sample Set

Malware Name	MD5Sum	Malware Type
WebC2-Greencat	ba0c4d3dbf07d407211b5828405a9b91	APT Malware + Trojan Horse
WebC2-Cson	f1e5d9bf7705b4dc5be0b8a90b73a863	APT Malware + Trojan Horse
Bangat	0f77af7fa673f5b3d36b926576002a1c	APT Malware
Beebus	ad6590e0df575228911852b1e401d46e	APT Malware
Glooxmail	3de1bd0f2107198931177b2b23877df4	APT Malware + Unpacked malware
Xorer.F	010bc5418ed1efc19ceb0fe9f71d83a1	Obfuscated Virus +File Infector
Sality.A	322a1203bbf5e12540df0e10adb21b58	Obfuscated Virus +File Infector
ShellCode_PDF_JS	b48ca8f2f3475f27d0693f98ff1080a4	Obfuscated Virus + Vulnerability Based
Cryptolocker	bc11c93f1b6dc74bf4804a35b34d9267	Ransomware
HacDef	39a9e5c05ffbda925da0d2ec9b4f512a	Rootkit
Zbot.gen!R	3025b97428a14c9bb808dacbc3bedbe7	Spyware

Table 3.1 above illustrates a total of 11 malware samples chosen for the study.

3.3 Malware Analysis Methodology

In order to build the threat tree for a malware sample, identification of its capabilities is paramount. To identify the capabilities, analysis of the sample needed to be carried out. To perform a comprehensive analysis, the malware samples were analyzed in

detail using a combination of static and dynamic manual & automated analysis techniques. The following list describes each of these techniques used:

1. Static Analysis: Static analysis involves analysis of malware samples without actually running the malware sample. In most cases static analysis gives the analyst a good idea about the capabilities of the malware. PE structure analysis tools such as PEView[40] were used to analyze the PE headers of the windows executable files. This activity provided valuable build information about the executable as well as the structure of the executable in terms of segments/sections and import tables. IDA Pro[21] was used to analyze the disassembled assembly code in the binary to gain as much information as possible. PDF analysis tools such as PDFiD[39] and pdf-parser[38] were used to analyze the malicious PDF sample to understand the structure of the PDF and identify malicious JavaScript code embedded in it.
2. Dynamic Analysis: Dynamic analysis of malware samples consists of running the malware in a Virtual Machine setup and analyzing its impact on the system in terms of filesystem changes, OS changes, network events and API calls. Dynamic analysis is particularly of use to identify encoded artifacts in the malware and their decryption mechanisms at runtime. Examples of encrypted artifacts includes encoded strings, API names, CnC server URLs etc. Tools such as Immunity Debugger, OllyDbg[36], WinDbg[62], Process Explorer[42], Process Monitor[43], VMMap[57], API monitor[2] were used to analyze the behavior of the malware.

Commercial malware analysis frameworks and anti-virus software heavily rely on the behavior of the malware at runtime to identify indicators of maliciousness for heuristic based detection.

3. Automated Analysis: Automated analysis consisted of a black-box type analysis approach where the malware was allowed to run in a virtual machine and its changes to the operating system were recorded and analyzed to understand the capabilities of the malware. Tools such as Cuckoo[14] were used to detonate the sample and analyze it in a closed, controlled environment.
4. Manual Analysis: Manual analysis of malware is a combination of static and dynamic analysis of malware done manually by the malware analyst to achieve an in-depth understanding of the implementation of malware. It may involve manually stepping through the code of the malware and is the most detailed analysis technique.

This study relied most heavily on manual static and dynamic analysis of malware to achieve maximum analytical coverage of the malware samples.

3.4 Threat Tree Articulation

Articulation of threat trees involved the identification of the high level goals and the underlying goals of the malware. These goals needed to be fulfilled in part or completely in order for the malware to be able to achieve its malicious intentions. Procedurally, after the malware analysis has been completed the capabilities and functionalities of the malware need to be articulated in a parent-child hierarchy to build the intended goal based threat tree.

Building of threat trees has some inherent issues that need to be solved in order to be able to create standardized threat trees for any kind of threat. The following is an illustration of the issues that needed to be handled to build useful threat trees for this study:

1. Variations in threat tree structures: As mentioned in Chapter 2, the articulation of threat trees is an activity that is heavily dependent on the domain experience of the security analyst that builds the trees. Hence different analysts can create different threat trees based on their experience, perceived threat structure and specified rules for creating the trees. Also different analysts can come up with trees that may be of different lengths based on their analysis. Many techniques have been introduced to remedy these issues. Some involve a collective effort to build the threat trees by a team of analysts. Other suggest extensive peer reviews of trees between the security and domain experts. Also of note are frameworks that allow for the definition of guidelines for the creation of hierarchy based structures such as STIX[48], CyBox[15], MAEC[28] etc.
2. Goal hierarchy definition: Definition of the hierarchy of goals is imperative to the correctness of the threat tree. However there are no specific guidelines that define which goal should be a parent goal along with the structure of its underlying sub-goals. This activity is currently an intuitive effort for threat tree creation in most domains. For creating the goal hierarchy of a malware sample however this is a relatively easy and straight forward activity. The functional threads of execution of the

malware can be followed to identify low level goals (atomic actions) and then re-trace the entire sequence of execution to identify the intermediate and high level goals of that thread of execution.

3. Interdependency of sub-goals: Multiple sub-goals in the threat tree may have interdependencies on each other to enable the fulfillment of their parent goal. This needs to be addressed since this concept will affect the severity of the goals in the threat trees of this study. For example if sub-goal 'A' is needed to be fulfilled along with sub-goal 'B' to achieve their parent goal 'P' then this relationship/dependency needs to be represented in the threat tree and accounted for during the calculation of the severity rating of the malware's goals.

3.4.1 MAEC Framework

In order to remedy the above mentioned issues, this study has chosen the usage of the Malware Attribute Enumeration and Characterization (MAEC) framework [28]. MAEC is a framework designed and developed specifically for the standardized representation of malware functionality using a hierarchy based model. The MAEC framework remedies the above mentioned issues with threat tree articulation in the following ways:

1. Variations in threat tree structures: The MAEC framework introduces the concept of a 3 level hierarchy based structure for enumerating malware attributes. It also defines the type of malware capabilities that can belong to each level. A definition of each level is provided as follows:

a. Mechanisms/Capabilities: Malware capabilities are at the highest level in the MAEC malware enumeration hierarchy. The capabilities represent the highest level goals of the malware. For example ‘Persistence’ is a capability of the malware and hence will be at the highest level of the hierarchy.
b. Behaviors: Behaviors in the MAEC framework represent the intermediate level goals that are needed to achieve the capabilities of the malware. Hence they can be treated as sub-goals of the Capabilities. For example achieving ‘Persistence across reboots’ is a behavior of the malware and is a sub-goal of the parent-goal (capability) ‘Persistence’. Multiple interdependent behaviors may be needed to be achieved in order to achieve the parent capability.
c. Actions: Actions are the implementation level actions that need to be performed in order to achieve the parent behavior defined. For example the Action ‘Modify Registry’ is a sub-goal of the parent goal (behavior) ‘Persistence across reboots’. Multiple interdependent actions can be needed to fulfill the parent behavior.
d. Objects: The MAEC framework also provides a way to represent artifacts that are used by the Actions. These are termed as Objects. Although objects are not used towards the calculation of the severity rating in this study, they have been included for completeness since they assist in the comprehensive enumeration of malware capabilities. An example of an object would be a

Windows registry key that is used in order to complete the action of ‘Modify Registry’.

2. Thus the MAEC framework provides a standardized method of creating the structure of a threat tree for the malware samples. It also defines a specific height for the tree to achieve vertical uniformity in the structure of the trees as well. Although the MAEC framework defines only 3 levels of hierarchy, this study has introduced another level at the top of the tree. This level is simply a place holder to define the generic malicious intentions of the malware and to unify all the Mechanisms/Capabilities of the MAEC based threat-tree into a common root node. This level/parent goal is not used towards the calculation of severity ratings since it does not provide any functional meaning to the malware’s functionalities.
3. Goal hierarchy definition: As described above the MAEC framework divides a malware’s functionalities into high-level capabilities, mid-level behaviors, and low-level abstract actions (each of which is a goal) to clearly define the hierarchy of the goals of the threat tree. Thus standardization can be achieved by evaluating the goal level at which a functionality of the malware belongs in turn simplifying the process of goal hierarchy definition.
4. Interdependency of sub-goals: Multiple actions, behaviors and capabilities may be interdependent on each other to fulfill their parent goals. This can be achieved in the MAEC framework by defining Candidate Indicators[4] in the MAEC document. Although intended for

providing information on indicators of infections to detection systems, this study has leveraged candidate indicators towards the definition of interdependencies between goals in the tree. For example in order to achieve the goal of ‘Persistence after reboots’ the sub-goals of ‘Drop exe on file system’ AND ‘Modify registry’ need to be fulfilled. This relationship can be easily and comprehensively modelled using the candidate indicators provided by the MAEC framework.

Figure 3.1 provides a hierarchy of the structure of the MAEC hierarchy.

The threat trees articulated using the MAEC framework are textually defined using the standard MAEC XML schema[4]. This schema consists of various malware specific artifacts as well as generic threat definition artifacts leveraged from other existing frameworks. The activity of articulating threat trees involves:

1. Identifying and categorizing malware functionality into MAEC capabilities, behaviors and actions.
2. Translating these capabilities, behaviors and actions into standard XML documents illustrating the actual hierarchy of goals.
3. Defining interdependencies between goals by defining candidate indicators in the MAEC XML threat tree document.

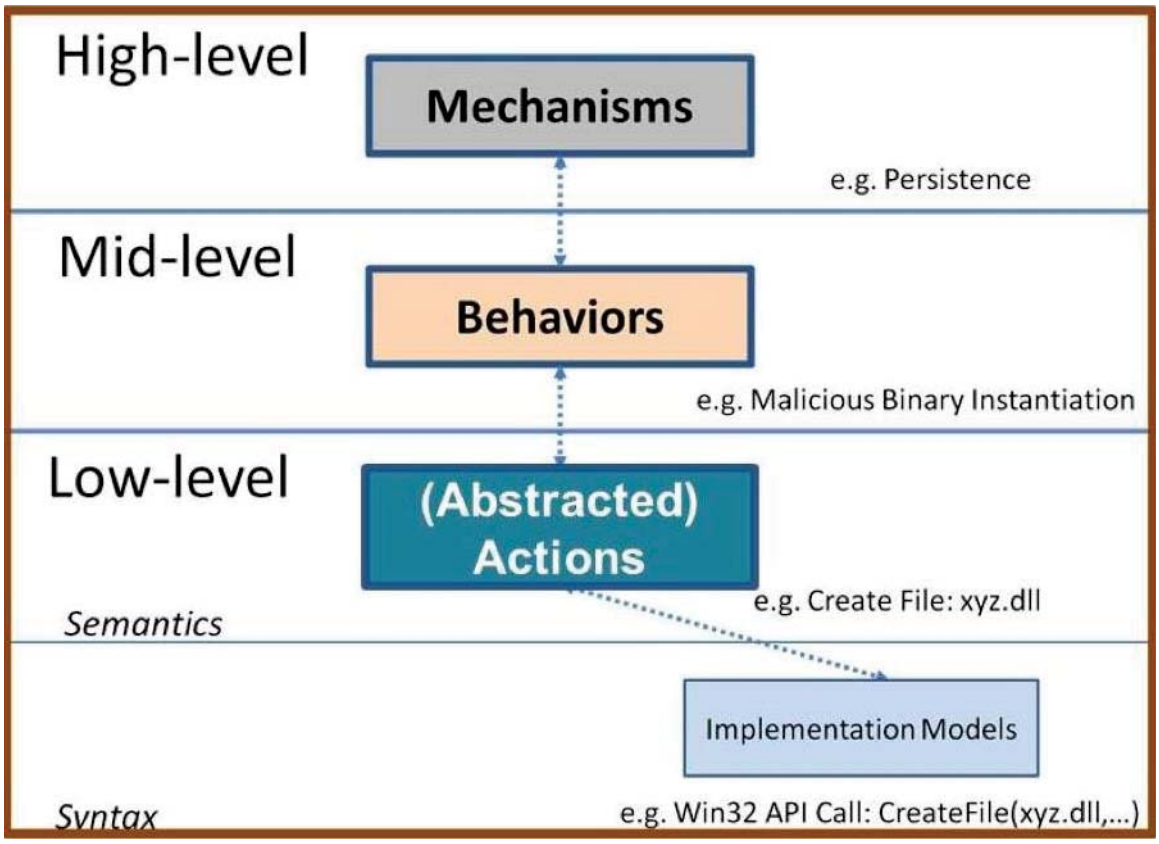

Figure 3.1 MAEC hierarchy of goals with Examples[5]

During the course of this study additional advantages of the MAEC framework were also discovered. These have been illustrated in the Results (Chapter IV) of this thesis.

3.5 Rating of Threat Tree Goals

Once the threat trees had been articulated, the rating of the threat trees was calculated based on:

1. The number of sub-goals of a goal.
2. The relationship between the sub-goals of a goal.
3. The levels in the hierarchy of the tree (= 3 in our study based on MAEC).

The algorithm for calculating the weight of a goal in the tree used a bottom up approach. The algorithm is listed below:

1. Assume that the tree is oriented left to right (leftmost is the root and the tree spreads towards the right). Thus the bottom of the tree are the lowest sub-goals also at the right most end and the top of the tree (root node) is the left most node.
2. Each level in the tree is assigned a sequential level-weight from right to left:
    a. i.e. All Actions(low-level goals) have a "level-weight" of 1,
    b. All Behaviors(mid-level goals) have a level-weight of 2,
    c. All Capabilities (high-level goals) have a level-weight of 3.
3. AND relationship: 2 or more goals in the system are said to have an AND relationship if all of them need to be accomplished in order to fulfill their parent goal.
4. OR relationship: 2 or more goals in the system are said to have an OR relationship if achievement of any one goal fulfills the parent goal.
5. Action (low-level goal) weights: All leaves in the tree (low-level goals or Actions) have a weight of 1 to start with.
6. Calculating the weight of a parent-goal in the tree:
    a. For the child-goals that have an OR relationship:
        i. Calculate the product of the weight of the child-goal and the level-weight of the child-goals.

ii. Add the products to get the effective weight of the parent-goal.

b. For the child-goals that have an AND relationship:

i. Calculate the product of the weight of the child-goal and the level-weight of the child-goals.

ii. Add the products of the child goals and then divide this number by the number of child-goals to get the effective weight of the parent-goal.

7. The effective-weight of the parent-goal is used to calculate the weight of the grand-parent goal based on its relationship with other parent-goals (at the same level as the parent goal).
8. This activity (Step 6 and 7) is repeated until the weight of all the goals has been calculated including the highest-level goal weight using capability(high-level goals, level 3) weights.

An explanation of some of the decisions made during the calculation of the weights (Refer to Step 6):

- Division of the added products by number of sub-goals for AND relationships is done to signify that the parent-goal has interdependencies and thus the ease of its accomplishment is less than those with sub-goals having OR relationships. Thus decreasing its effective degree of maliciousness towards the system.
- Multiplication of the weight of sub-goal with the level-weight of the sub-goal (both OR and AND scenarios) is done to signify the importance of

the context that is achieved by the combination of the parent-goal and its sub-goals.

CHAPTER IV

RESULTS

4.1 Complete Malware Severity Rating Calculation

In order to explain the approach used for calculating the severity rating of the malware it is beneficial to illustrate the calculation using an example. This example uses the APT malware WebC2-Greencat. A pictorial representation of the threat tree is provided in Figure 4.1.

Weight of a goal is represented as W(goal). Level-weight of sub-goal is represented a L(goal). All leaves in the tree (low-level goals or Actions) have a weight of 1 to start with (W=1 to start with).

Let us start with the top most leaf and its corresponding low-level goals (actions):

1. Since there is only action (low-level goal) “create_mutex” under the mid-level goal “Establish_runtime_persistence” the weight of the mid-level goal is

   = Weight of low-level goal * level-weight of low-level goal

   = W * L

   = 1* 1

   = 1

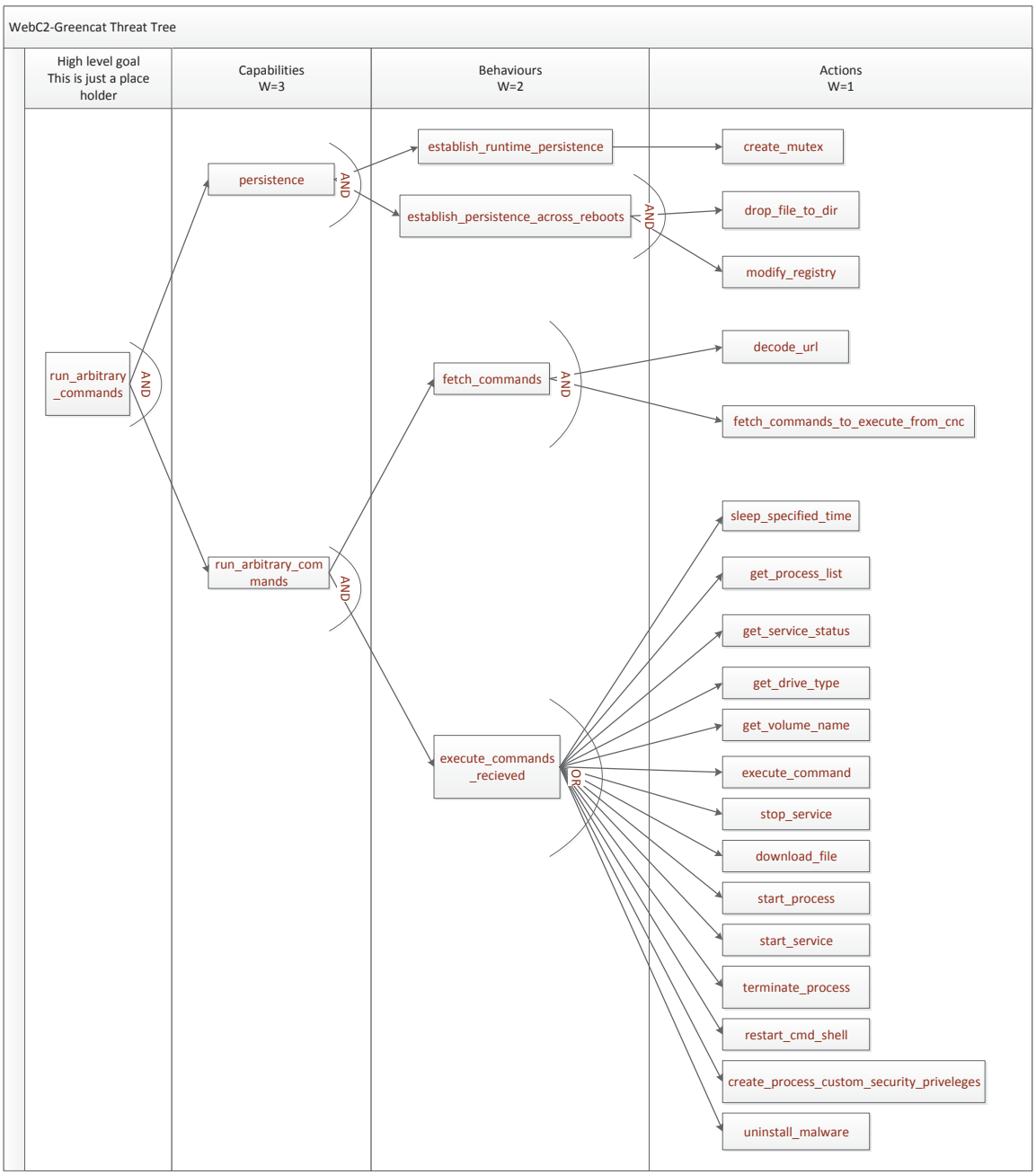

Figure 4.1 Threat Tree for WebC2-Greencat

2. Weight of mid-level goal “establish_persistence_across_reboots”

= (W(drop_file_to_dir)*L(drop_file_to_dir) +
W(modify_registry)*L(modify_registry)) / (Number of goals in AND relationship)

= (1*1 + 1*1) /2

= 1

3. Weight of mid-level goal “fetch_command”

   = (W(decode_url)*L(decode_url) +
   W(fetch_commands_from_cnc)*L(fetch_commands_from_cnc))/(# of goals in AND relationship)

   = (1*1 + 1*1)/2

   = 1

4. Weight of mid-level goal “execute_commands_recieved” is just and addition of all the low-level goals since fulfillment of any of the low-level goals fulfills the mid-level goal.

   = 14

5. Weight of the high-level goal “persistence” is a combination of the mid-level goal weights calculated in Steps 1 and 2. Level weight of mid-level goals is 2.

   = (W(establish_runtime_persistance)*L(establish_runtime_persistance) +
   W(establish_persistence_across_reboots)*L(establish_persistence_across_
   reboots))/(# of goals in AND relationship)

   = (1*2 + 1*2) /2

   = 2

6. Weight of the high-level goal “run_arbitrary_commands” is a combination of the mid-level goal weights calculated in Steps 3 and 4. Level weight of mid-level goals is 2.
7. = (W(fetch_commands)*L(fetch_commands) + W(execute_commands_recieved)*L(execute_commands_recieved))/(# of goals in AND relationship)
   = (1*2 + 14*2)/2
   = 15
8. Weight of the highest-level goal is the malware’s severity rating calculated as the combination of the weights of the high-level goals calculated in Steps 5 and 6. Level weight of high level goals (capabilities) is 3.
   = (W(persistence)*L(persistence) + W(run_arbitrary_commands)*L(run_arbitrary_commands))/(# of goals in AND relationship)
   = (2*3 + 15*3)/2
   = 25.5

Thus the overall severity rating of the malware sample analyzed (belonging to WebC2-Greencat) is 25.5. This also defines an absolute weight measuring the degree of maliciousness of the malware sample.

4.2 Ratings for Malware Sample Set

Based on the approach illustrated in Chapter III, the malware samples were analyzed in depth and threat trees were constructed based on the guidelines provided by the MAEC framework. The threat trees are represented in two ways in this study.

Although there is a difference in the representation of the threat trees, there are no differences in the structure/ hierarchies of the trees for each malware sample:

1. Formal XML documents: Formal XML documents have been created to textually illustrate a threat tree for each malware sample (Total of 11 in this study). The XML documents comply with the MAEC schemas for malware enumeration and attribution. Complaint XML documents can thus be used as inputs to existing utilities that can convert them into other formats (HTML etc.)
2. Pictorial tree structures: An example of pictorial tree structures has already been provided in Section 4.1 (Figure 4.1). Since the XML documents may appear to be complicated and disjoint (due to the schema specification), these trees have been constructed in order to simplify the trees and enhance our understanding of the threat tree structure for each sample.

Construction of both the representations of the tree have their own advantages. While the textual representation allowed for a tighter set of rules to create the trees (e.g. hierarchy, tree length etc.), the pictorial representation allowed for a simplified and unified view of the tree thus enabling easy calculations of ratings for the samples. Table 4.1 illustrates the ratings calculated for the malware sample set specified in Chapter III in descending order of their ratings.

The threat trees constructed for the samples have been illustrated in Appendices A and B.

Table 4.1 Malware sample set ratings

Malware Name	Severity Rating	Malware Type
Xorer.F	45.375	Obfuscated Virus +File Infector
HacDef	39	Rootkit
Sality.A	30	Obfuscated Virus +File Infector
Zbot.gen!R	29.5	Spyware
WebC2-Greencat	25.5	APT Malware + Trojan Horse
WebC2-Cson	24	APT Malware + Trojan Horse
Bangat	22.5	APT Malware
Glooxmail	22	APT Malware + Unpacked malware
Beebus	21	APT Malware
Shellcode_PDF_JS	18	Obfuscated Malware + Vulnerability Based
Cryptolocker	6	Ransomware

4.3 Observations

In order to understand the significance and correctness of the ratings, the following observations are discussed:

1. Xorer.F has the maximum rating in the sample set in spite of the presence of 5 APT samples deemed extremely dangerous by most commercial cyber-security enterprises. A quick look at the threat tree for Xorer.F tells us why:
    a. This is because of the fact that this malware sample is extremely feature rich. It consists of features like multiple ways of spreading across the system, running arbitrary commands, downgrading the target's security level etc.

b. Not only is the sample feature-rich but also most of its capabilities consist of sub-goals that are mutually exclusive from each other (OR relationships) thus increasing the chances of successful malicious behavior by the malware.

2. APT malware samples have almost the same severity ratings (ranging from 25.5 to 21) with minor variations based on their feature-sets and interdependencies of the goals of the trees. Samples such as WebC2-Greencat, WebC2-Cson, Bangat, Glooxmail and Beebus are suspected to have the same authors and relatively same functionalities. The fact that the severity ratings calculated for these samples fall into each other's vicinities gives credibility to the approach implemented.
3. Malware samples Hacdef and Zbot are considered sophisticated user mode rootkits. Now even though Zbot has more functionalities (stealing of data in addition to hooking APIs) it still has a lower severity rating than Hacdef due to the fact that the interdependency of goals for Zbot makes it a lesser threat than Hacdef.
4. Cryptolocker: The ransomware sample Cryptolocker has an extremely low rating of 6 in spite of the fact that it has caused a huge amount of monetary damage to organizations across the world. A low severity rating for the malware is justified due to the following reasoning:
    a. It has a very simple implementation and thus is not very feature rich. The visual threat tree for Cryptolocker (illustrated in Appendix B) indicates that the malware sample's features are

fairly limited and that the implementation of these features is fairly straight forward. For example, even though the data being transmitted is locally encoded, the network communication carried out between the malware and its CnC server does not use an encrypted channel.

b. All of the sub-goals and parent goals of the threat tree are dependent on each other via the 'AND' relationships, hence the malware needs all the goals in the threat tree's hierarchy to succeed in order to be able to carry out its malicious activities. For example, the malware checks to make sure that it has achieved persistence (at runtime AND across reboots) before trying to accomplish its other goals. Thus if the goal of persistence isn't accomplished, the malware stops its execution instead of trying to accomplish its other goals. Also if the goal of fetching the target specific encryption key from the CnC server fails, then the malware does start encoding the files on the target. This method of implementation diminishes the ease with which the malware can accomplish its malicious task. This implementation style consisting of close dependencies in the malware's feature set are not characteristic of APT malware groups who typically aim to achieve as much execution coverage as possible for their malware.

c. An interesting observation in Crytolocker's threat tree is that although it has sub-trees for both encryption and decryption of

files, the decryption sub-tree does not contribute towards the overall features of the malware. This is due to the fact that the decryption sub-tree does not contribute to its malicious actions (It actually contributes towards undoing the malicious activity of the malware). Also from a functional/design point of view it is highly unlikely that the malware authors would be motivated to ensure the decryption of data even after the bounty for a target has been received. Thus the decryption sub tree is dis-joint from the parent root node and does not contribute towards the severity rating of the malware sample. It has been included in the threat tree representations only to achieve completeness of feature/capabilities articulation.

d. At a very high level the malware performs the simple task of reading, modifying (encoding) and saving the file. This activity/feature-set does not represent a high degree of maliciousness unlike the case of Xorer.f which actively tries to kill antivirus services in the system or in the case of Zbot which places user-mode hooks for windows API imports (for intercepting information) or in the case of WebC2-Greencat which tries to open channels for unauthorized control of the target machine.

e. Cryptolocker (and ransomware in general) has been deemed dangerous by most antivirus vendors due to the damage implied by the concept of ransoms. Ransoms not only cause monetary losses

but can also lead to potential loss of resources and data. However in terms of implementation and feature richness Crytolocker (and most other ransomware) isn't as malicious as APT malware such as Bangat consisting of a variety of features and exploit based malware such as Shellcode_PDF_JS (discussed next).

5. Shellcode_PDF_JS is the PDF sample analyzed that implemented known CVEs. Analysis of this sample showed that the malware was a very simple piece of code implementing 3 buffer overflow CVEs based on the Adobe Acrobat Reader versions on the target system. Articulation of the threat tree for this sample enabled this methodology to be tested on CVE based samples and exploit-kit/dropper samples. The severity rating of this sample is relatively low (= 18) due to the fact that it is has a mediocre number of features/goals in it.

4.4 Results

The following are the results derived from this study:

1. Severity rating is dependent not only on the malware's feature set (goals) but also dependent on the relationships between the functionalities (goals and sub-goals). This is evident from the severity ratings of both Xorer.f (highest) and Cryptolocker (lowest).
2. This technique of calculating ratings for malware gives consistent results evident from the fact that similar APT samples have similar severity ratings.

3. Samples with a high severity rating have been deemed as highly dangerous by most anti-virus distributions.
4. Many malware samples consist of similar high, mid and low level goals. An example of such patterns is the “code_injection” feature set of samples like Bangat, Hacdef and Zbot. The pattern of representation for this functionality can be re-used for other samples that are discovered to have the same functionality in future.
5. The tree hierarchy of goals and sub-goals can be used not only for articulating other samples in future but also by detection systems. Heuristics based detection mechanisms can evaluate the features of a malware and build patterns out of them. These patterns can be matched with existing patterns from existing threat trees to detect malware and possibly identify their families depending on similarity of patterns.
6. The impact of ransomware is huge in terms of monetary and data loss simply because of the concept of ransoms. Factoring such factors into the calculation of severity ratings may enhance the ratings. However this is another research endeavor on its own and can be done as part of future work.

The reason that these factors were not accounted for in this study was due to fact that the study wanted to simulate the situation where the malware analyst gets a new a malware sample and has to take a call about its severity based on its features in order to dedicate resources towards the analysis and detection of the malware. At this point in

time the economic impact and loss/harm to systems in the wild is not available to the analyst to factor into the severity rating.

The process of analyzing the malware (at least a preliminary analysis) can be automated either by building an automated sandboxed analysis system or by using/customizing existing sandbox analysis solutions. This will not only take away a lot of manual effort by the analyst but will also help save time and resources used for analysis. However there may be a trade-off between the time and quality of feature detection. This evaluation can also be done as a different study in the future. This study deliberately performed manual analysis in order to create a comprehensive feature set/hierarchy for the malware samples in order to prove the research hypothesis.

CHAPTER V

CONCLUSION

The purpose of this study was to qualify the usage of threat trees towards the calculation of a useful severity rating. The severity rating for malware was defined as the extent of damage the malware will cause to a target system provided it is run on the right platform and under ideal conditions for it to run solely based on its functionality. To formally state the hypothesis again:

> *"Attack trees provide a mechanism for calculating a useful severity rating for malware that can be utilized to assess their threat level."*

In order to verify the hypothesis the following research sub-goals of this study were presented:

1. Articulation of a method to calculate severity ratings of malware.
2. Show that threat trees can be successfully used to articulate malware threats.
3. Present analytical evidence that threat trees can be used to calculate malware severity ratings.

The results of this study show that a method of calculation of the severity of malware can be articulated. In order for this method to be correct and consistent, interdependencies and relationships between the features/goals of the malware have to be taken into account.

The method of articulation of malware threats utilized in this study was the use of threat trees. The results show that threat trees can be utilized to represent the malware threats based on the results of an exhaustive manual analysis of the malware samples.

The results also show that leveraging threat trees along with the proposed severity rating calculation algorithm gives consistent and credible ratings. This technique can be used to effectively calculate a useful severity rating based on solely the features of the malware.

5.1 Contributions

This thesis proposes a methodology that can be used towards the calculating of severity ratings of malware samples thus enabling organizations to take decisions on resource utilization and prioritization towards malware samples deemed more severe. The patterns derived from threat trees can be used for deriving threat trees for future samples with similar functionalities. The patterns derived from threat trees can also be used as detection mechanisms by heuristic based system to detect malware.

5.2 Further Research

The techniques discussed in the thesis can be leveraged towards a more enriched severity rating that can be a combination of the malwares functionalities and it's environment and other factors as well. Although this activity is useful in some cases, it defeats the purpose of initial triage of the malware to dedicate resources to it before the damage has been done thus making it a reactive approach towards malware analysis, detection and mitigation.

A useful study that can further enhance the process of calculating severity ratings is to build an automated malware analysis system (or customize an existing system) to identify and automatically build threat trees (and patterns) out of the analysis with subsequent severity rating calculation. It would be highly beneficial to evaluate the trade off in accuracy and credibility of the automated vs manual analysis method towards the building of trees and rating calculation. This study can be the stepping stone towards building a useful and efficient malware analysis engine.

5.3 Publication Plan

This thesis provides a novel method of calculating severity ratings useful towards the prioritization of malware for analysis and mitigation/detection. The intention is to write a paper/article to share this research with the research community. This activity is intended to be completed during the summer of 2015.

5.3.1 Venues of publication

The following are some venues of publication that are being considered for sharing this study with the research community:

1. IEEE Security & Privacy: A popular journal in the cyber-security community.
2. IEEE Transaction on Information Forensics and Security: The IEEE journal focusing on forensics and security. Since this thesis uses forensic methods such as debugging, process memory analysis and in-depth dynamic malware analysis, this journal would be a relevant publication site for it.

3. ACM Transactions on Information and System Security (TISSEC): Another popular research journal in the cyber security community.
4. Computers & Security: A popular research journal focusing on all areas of computer security.

The following are some of the conferences where it would be highly relevant to present this research:

1. International Conference on Malicious and Unwanted Software (MALWARE)
2. International Conference on Risks and Security of Internet and Systems (CRiSIS)

REFERENCES

[1] Alert Levels in Microsoft Security Essentials, Microsoft, http://windows.microsoft.com/en-us/windows/understanding-alert-levels (current Jan. 2014)

[2] API Monitor, http://www.rohitab.com/apimonitor (current Nov. 2014)

[3] R. Bagnall, G. French, "The Malware Rating System," Veridian

[4] D. Beck, I. Kirillov, P. Chase, "Candidate Indicators," *The MAEC Language Version 4.1 Specification,* June 2014, pp. 29-31

[5] D. Beck, I. Kirillov, P. Chase, "Overview of the MAEC Data Models," *The MAEC Language Version 4.0.1 Specification,* Nov. 2013, pp. 6-14

[6] G. Bonfante, M. Kaczmarek, J. Marion, "Morphological detection of malware," *Proceedings of the 3rd International Conference on Malicious and Unwanted Software MALWARE 2008,* Fairfax, USA, Oct. 2008, pp. 1-8

[7] Bots and Botnets – A Growing Threat, http://us.norton.com/botnet/ (current Jan. 2014)

[8] S. Boyer, "SCADA: Supervisory control and Data Acquisition", USA:ISA – International Society of Automation, 4th ed.

[9] S. Camtepe, B. Yener, "Modeling and detection of complex attacks," *Proceedings of 3rd International Conference on Security and Privacy in Communications Networks and the Workshops SecureComm 2007,* Nice, France, Sept. 2007, IEEE, pp. 234-243

[10] Certified Definitions – Detections Added, Symantec, http://www.symantec.com/security_response/definitions/certified/ (current Jan. 2014)

[11] M. Christodorescu, S. Jha, S.A. Seshia, D. Song, R.E. Bryant, "Semantics-aware malware detection," *IEEE Symposium on Security and Privacy,* May 2005, pp. 32-46

[12] Common Vulnerabilities and Exposures, https://cve.mitre.org/ (current Nov. 2014)

[13] J. Cong, X. Wang, H. Tan, "Dynamic Attack Tree and Its Applications on Trojan Horse Detection," *Proceedings of the 2nd International Conference on Multimedia and Information Technology (MMIT)*, Kaifeng, China, Apr. 2010, pp. 56-59

[14] Cuckoo Sandbox, http://www.cuckoosandbox.org/ (current Nov. 2014)

[15] Cyber Observable eXpression, https://cybox.mitre.org/ (current Nov. 2014)

[16] F. David, R. Linger, H. Lipson, T. Longstaff, N. Mead, R. Ellison, "Survivable Network Systems: An Emerging Discipline," *Technical Report CMU/SEI-97-TR-013*, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, Pennsylvania, 1997

[17] K. Edge, G. Dalton, R. Raines, R. Mills, "Using Attack and Protection Trees to Analyze Threats and Defenses to Homeland Security," Proceedings of the *Military Communications Conference MILCOM 2006,* Washington D.C., USA, Oct. 2006, IEEE, pp.1-7

[18] Exposing one of China's cyber espionage units, http://www.mandiant.com/apt1 (current Nov. 2014)

[19] Facebook, www.facebook.com (current Jan. 2014)

[20] B. Galloway, G. Hancke, "Introduction to Industrial Control Networks," *Communications Surveys & Tutorials,* IEEE, vol. 15, no.2, 2013, pp. 860-880

[21] IDA, https://www.hex-rays.com/products/ida/ (current Jan, 2014)

[22] Immunity Debugger, https://www.immunityinc.com/products-immdbg.shtml (current Jan. 2014)

[23] Intel 64 and IA-32 Architectures Software Developer's Manual, http://www.intel.com/content/dam/www/public/us/en/documents/manuals/64-ia-32-architectures-software-developer-manual-325462.pdf (current Jan. 2014)

[24] M. R. Islam, T. Ronghua, L. Batten, S. Versteeg, "Classification of Malware Based on String and Function Feature Selection," *Proceedings of the 2nd Workshop on Cybercrime and Trustworthy Computing Workshop (CTC),* Ballarat, Australia, July 2010, pp. 9-17

[25] W. Jianjun, K. Yaohong, "Text Classification Based on Improved Mutual Information," Computer Application, vol. 26, 2006, pp. 172-173

[26] P. Khand, P.A., "System level security modeling using attack trees," *Proceedings of the 2nd International Conference on Computer, Control and Communication IC4 2009,* Karachi, Pakistan, Feb. 2009, pp. 1-6

[27] R. Linger, K. Sayre, T. Daly, M. Pleszkoch, "Function Extraction Technology: Computing the Behavior of Malware," *Proceedings of the 44th Hawaii International Conference on System Sciences (HICSS),* Kauai, Hawaii, Jan. 2011, pp. 1-9

[28] Malware Attribute Enumeration and Characterization, http://maec.mitre.org/ (current Nov. 2014)

[29] A. Marback, D. Hyunsook,H. Ke. S. Kondamarri, X. Dianxiang, "Security test generation using threat trees," Workshop on Automation of Software Test, 2009, AST '09. ICSE, pp.62-69, May 2009

[30] S. Mathew, R. Giomundo, S. Upadhyaya, M. Sudit, A. Stotz,"Understanding multistage attacks by attack-track based visualization of heterogeneous event streams," *Proceedings of the 3rd international workshop on Visualization for computer security* (VizSEC '06). ACM, New York, NY, USA, 2006, pp. 1-6

[31] J, McDermott,C. Fox, "Using abuse case models for securityrequirements analysis," *Proceedings of the 15th Annual Computer Security Applications Conference*, *ACSAC '99*, pp. 55-64, 1999

[32] Microsoft Windows, http://windows.microsoft.com/en-us/windows/home (current Nov. 2014)

[33] S. Mishra, K. Kant, R.S. Yadav, "Multi Tree View of Complex Attack – Stuxnet," Advances in Computing and Information Technology, Springer-Verlag, vol. 176, 2012, pp. 171-188

[34] J.A. Morales, M. Main, L. Weiliang, X. Shouhuai, R. Sandhu, "Building malware infection trees," *Proceedings of the 6th International Conference on Malicious and Unwanted Software (MALWARE),* Fajardo, Puerto Rico, Oct. 2011, IEEE,pp.50-57

[35] S. Nari, A.A. Ghorbani, "Automated malware classification based on network behavior," *Proceedings of the 2013 International Conference on Computing, Networking and Communications (ICNC),* San Diego, USA, Jan. 2013, IEEE, pp.642-647

[36] OllyDbg, http://www.ollydbg.de/ (current Jan. 2014)

[37] H. Pardue, A. Yasinsac, J. Landry, "Towards Internet voting security: A threat tree for risk assessment," *Proceedings of the 5th International Conference on Risks and Security of Internet and Systems (CRiSIS)*, Montreal, Oct. 2010, IEEE, pp.1-7

[38] Pdf-parser, http://blog.didierstevens.com/programs/pdf-tools/ (current Nov. 2014)

[39] PDFiD, http://blog.didierstevens.com/2009/03/31/pdfid/ (current Nov. 2014)

[40] PeView, http://wjradburn.com/software/ (current Nov. 2014)

[41] C. Pfleeger, S. Pfleeger, "Security in Networks," *Security in Computing,* 4th ed., Prentice Hall, Massachusetts, USA, 2006, pp. 484-487

[42] Process Explorer v16.04, http://technet.microsoft.com/en-us/sysinternals/bb896653.aspx (current Nov. 2014)

[43] Process Monitor v3.1, http://technet.microsoft.com/en-us/sysinternals/bb896645.aspx (current Nov. 2014)

[44] B. Schneier, "Attack Trees,"*Dr. Dobb's Journal 24*, Dec. 1999, pp. 21-29

[45] Service Oriented Architecture (SOA), http://msdn.microsoft.com/en-us/library/bb833022.aspx (current Jan. 2014)

[46] M. Sikorski, A.Honig, "Direct Injection," *Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software,* 1st ed., No Starch Press, San Francisco, California, USA, 2012, pp. 254-257

[47] G. Sindre, A.L. Opdahl, "Eliciting security requirements by misusecases," *Proceedings of the 37th International Conference on Technology of Object-Oriented Languages and Systems*, pp. 120-131, 2000

[48] Structured Threat Information eXpression, https://stix.mitre.org/ (current Nov. 2014)

[49] SQL Injection, https://www.owasp.org/index.php/SQL_Injection (current Jan. 2014)

[50] R. Tian, L. Batten, R. Islam, S. Versteeg, "An automated classification system based on the strings of Trojan and virus families," *Proceedings of the 4th International Conference on Malicious and Unwanted Software MALWARE 2009,* Montreal, Canada, pp. 23-30

[51] R. Tian, L. Batten, S. Versteeg, "Function length as a tool for malware classification," *Proceedings of the 3rd International Conference on Malicious and Unwanted Software MALWARE 2008,* Fairfax, USA, pp. 69-76

[52] Threat Prevalence Definition, Sophos, http://www.sophos.com/en-us/threat-center/threat-monitoring/threat-prevalence-definition.aspx (current Jan. 2014)

[53] Threat Severity Rating, Symantec, http://www.symantec.com/security_response/severityassessment.jsp (current Jan. 2014)

[54] Trojan.Pidief.C, http://www.symantec.com/security_response/writeup.jsp?docid=2008-020915-1008-99 (current Nov. 2014)

[55] Twitter, www.twitter.com (current Jan. 2014)

[56] S. Vidalis, A. Jones, "Using vulnerability trees or decisions making in threat Assessment," School of Computing Technical Report CS-03-2, University of Glamorgan, UK, 2003

[57] VMMap v3.12, http://technet.microsoft.com/en-us/sysinternals/dd535533.aspx (current Nov. 2014)

[58] W32.Stuxnet Dossier, http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf, Symantec, (current Jan. 2014)

[59] J. Wang; R. Phan, J. Whitley, D. Parish, "Augmented Attack Tree Modeling of Distributed Denial of Services and Tree Based Attack Detection Method," *Proceedings of the 10th International Conference on Computer and Information Technology (CIT)*, Bradford, UK, Jun.2010, IEEE, pp. 1009-1014

[60] J. Wang; R. Phan, J. Whitley, D. Parish, "Augmented Attack Tree Modeling of SQL Injection Attacks," *Proceedings of the 2nd International Conference on Information Management and Engineering (ICIME)*, Chengdu, China, April 2010, IEEE, pp. 182-186

[61] M. Warren, S. Leitch, I. Rosewall, "Attack vectors against social networking systems: the Facebook example," *Proceedings of the 9th Australian Information Security Management Conference,* Perth, Australia, Dec. 2011

[62] WinDbg, http://msdn.microsoft.com/en-us/windows/hardware/hh852365 (current Jan. 2014)

[63] Y. Xiao; Y. Wang, Z. Huang, "Survivability analysis of SOA based on attack tree models," *Proceedings of the 14th International Conference on Communication Technology (ICCT),* Chengdu, China, Nov. 2012, IEEE, pp. 819-823

[64] Xorer.F, http://www.microsoft.com/security/portal/threat/encyclopedia/entry.aspx?Name=Virus%3aWin32%2fXorer.F (current Nov. 2014)

[65] H. Yin, D. Song, M. Egele, C. Kruegel, E. Kirda, "Panorama: capturing system-wide information flow for malware detection and analysis," *Proceedings of the 14th ACM Conference on Computer and Communications Security* (CCS '07),New York, USA, Oct. 2007, ACM, pp. 116-127

[66] I. You, K. Yim, "Malware Obfuscation Techniques: A brief survey," *Proceedings of the 3rd International Conference on Broadband, Wireless Computing, Communication and Applications (BWCCA),* Fukuoka, Japan, Nov. 2010, IEEE, pp. 297-300

[67] M.N. Yusoff, A. Jantan, "Optimizing decision tree in malware classification system by using genetic algorithm," *International Journal of New Computer Architectures and their Applications (IJNCAA),* vol. 3, no. 1, 2011, pp. 694-713

[68] M.F. Zolkipli, A. Jantan, "An approach for malware behavior identification and classification," *Proceedings of the 3rd International Conference on Computer Research and Development (ICCRD),* Shanghai, China, March 2011, ACM, vol.1, no., pp. 191-194

APPENDIX A

XML THREAT TREES FOR SAMPLES BASED ON THE MAEC FRAMEWORK

A.1 Bangat

<?xml version="1.0" encoding="UTF-8"?>

<maecBundle:MAEC_Bundle xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"

xsi:schemaLocation="http://cybox.mitre.org/objects#ArtifactObject-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/Artifact_Object.xsd

http://cybox.mitre.org/objects#WinRegistryKeyObject-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/Win_Registry_Key_Object.xsd

http://cybox.mitre.org/objects#WinExecutableFileObject-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/Win_Executable_File_Object.xsd

http://cybox.mitre.org/common-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/cybox_common.xsd

http://cybox.mitre.org/objects#APIObject-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/API_Object.xsd

http://maec.mitre.org/XMLSchema/maec-bundle-4

maec/maec_4.1_offline/maec_bundle_schema.xsd

http://cybox.mitre.org/objects#WinExecutableFileObject-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/Win_Executable_File_Object.xsd

http://cybox.mitre.org/objects#PDFFileObject-1

maec/maec_4.1_offline/cybox_2.1_offline/objects/PDF_File_Object.xsd

http://cybox.mitre.org/objects#APIObject-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/API_Object.xsd

http://cybox.mitre.org/objects#WinExecutableFileObject-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/Win_Executable_File_Object.xsd

http://cybox.mitre.org/default_vocabularies-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/cybox_default_vocabularies.xsd

http://cybox.mitre.org/objects#PDFFileObject-1

maec/maec_4.1_offline/cybox_2.1_offline/objects/PDF_File_Object.xsd

http://cybox.mitre.org/objects#WinRegistryKeyObject-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/Win_Registry_key_Object.xsd

http://cybox.mitre.org/objects#WinMutexObject-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/Win_Mutex_Object.xsd

http://cybox.mitre.org/objects#ArtifactObject-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/Artifact_Object.xsd

http://cybox.mitre.org/objects#EmailMessageObject-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/Email_Message_Object.xsd

http://cybox.mitre.org/objects#MutexObject-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/Mutex_Object.xsd

http://cybox.mitre.org/objects#PipeObject-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/Pipe_Object.xsd

http://cybox.mitre.org/objects#HTTPSessionObject-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/DNS_Query_Object.xsd

http://cybox.mitre.org/objects#UserAccountObject-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/User_Account_Object.xsd

"

xmlns:HTTPSessionObj="http://cybox.mitre.org/objects#HTTPSessionObject-2"

xmlns:DNSQueryObj="http://cybox.mitre.org/objects#DNSQueryObject-2"

xmlns:maecBundle="http://maec.mitre.org/XMLSchema/maec-bundle-4"

xmlns:ProcessObj="http://cybox.mitre.org/objects#ProcessObject-2"

xmlns:SocketAddressObj="http://cybox.mitre.org/objects#SocketAddressObject-1"

xmlns:AddressObj="http://cybox.mitre.org/objects#AddressObject-2"

xmlns:NetworkConnectionObj="http://cybox.mitre.org/objects#NetworkConnectionObje
ct-2"

xmlns:PDFFileObj="http://cybox.mitre.org/objects#PDFFileObject-1"

xmlns:cyboxVocabs="http://cybox.mitre.org/default_vocabularies-2"

xmlns:HostnameObj="http://cybox.mitre.org/objects#HostnameObject-1"

xmlns:CodeObj="http://cybox.mitre.org/objects#CodeObject-2"

xmlns:FileObj="http://cybox.mitre.org/objects#FileObject-2"

xmlns:DNSRecordObj="http://cybox.mitre.org/objects#DNSRecordObject-2"

xmlns:WinRegistryKeyObj="http://cybox.mitre.org/objects#WinRegistryKeyObject-2"

xmlns:maecVocabs="http://maec.mitre.org/default_vocabularies-1"

xmlns:APIObj="http://cybox.mitre.org/objects#APIObject-2"

xmlns:WinExecutableFileObj="http://cybox.mitre.org/objects#WinExecutableFileObject
-2"

xmlns:cyboxCommon="http://cybox.mitre.org/common-2"

xmlns:URIObj="http://cybox.mitre.org/objects#URIObject-2"

xmlns:cybox="http://cybox.mitre.org/cybox-2"

xmlns:WinMutexObj="http://cybox.mitre.org/objects#WinMutexObject-2"
xmlns:ArtifactObj="http://cybox.mitre.org/objects#ArtifactObject-2"
xmlns:EmailMessageObj="http://cybox.mitre.org/objects#EmailMessageObject-2"
xmlns:MutexObj="http://cybox.mitre.org/objects#MutexObject-2"
xmlns:PipeObj="http://cybox.mitre.org/objects#PipeObject-2"
xmlns:UserAccountObj="http://cybox.mitre.org/objects#UserAccountObject-2"
id="Bangat_exe_TT" schema_version="4.1"
defined_subject="true">

<maecBundle:Malware_Instance_Object_Attributes>
<cybox:Description>The Malware is an exe sample that performs a variety of information stealing acitvities</cybox:Description>
<cybox:Properties xsi:type="WinExecutableFileObj:WindowsExecutableFileObjectType">
<FileObj:File_Extension>EXE</FileObj:File_Extension>
<FileObj:Size_In_Bytes>598528</FileObj:Size_In_Bytes>
<FileObj:Hashes>
<cyboxCommon:Hash>
<cyboxCommon:Type>MD5</cyboxCommon:Type>

<cyboxCommon:Simple_Hash_Value>0f77af7fa673f5b3d36b926576002a1c</cyboxCommon:Simple_Hash_Value>
</cyboxCommon:Hash>

```
</FileObj:Hashes>
 </cybox:Properties>
  </maecBundle:Malware_Instance_Object_Attributes>

 <!-- Placeholder for capabilities -->
 <maecBundle:Capabilities>
  <maecBundle:Capability id="persistence" name="persistence">
   <maecBundle:Behavior_Reference behavior_idref="persistence_across_reboots"/>
  </maecBundle:Capability>
  <maecBundle:Capability id="run_arbitrary_commands">
   <maecBundle:Behavior_Reference behavior_idref="fetch_commands"/>
   <maecBundle:Behavior_Reference
behavior_idref="execute_misc_commands_received"/>
  </maecBundle:Capability>
  <maecBundle:Capability id="trojanize_binaries">
   <maecBundle:Behavior_Reference behavior_idref="code_injection"/>
  </maecBundle:Capability>

  <maecBundle:Capability id="control_system_remotely">
   <maecBundle:Behavior_Reference behavior_idref="control_desktop"/>
  </maecBundle:Capability>

 </maecBundle:Capabilities>
```

```
<!-- Placeholder for behaviours -->
<maecBundle:Behaviors>
 <maecBundle:Behavior id="persistence_across_reboots">
  <maecBundle:Action_Composition>
   <maecBundle:Action_Reference action_id="copy_self_to_new_dll"/>
   <maecBundle:Action_Reference action_id="register_dll_as_service"/>
  </maecBundle:Action_Composition>
 </maecBundle:Behavior>
 <maecBundle:Behavior id="fetch_commands">
  <maecBundle:Action_Composition>
   <maecBundle:Action_Reference
action_id="fetch_commands_to_execute_from_cnc"/>
  </maecBundle:Action_Composition>
 </maecBundle:Behavior>
 <maecBundle:Behavior id="execute_commands_received">
  <maecBundle:Action_Composition>
   <maecBundle:Action_Reference action_id="start_service"/>
   <maecBundle:Action_Reference action_id="stop_service"/>
   <maecBundle:Action_Reference action_id="open_remote_shell"/>
   <maecBundle:Action_Reference action_id="download_file"/>
   <!-- record system information -->
   <maecBundle:Action_Reference action_id="get_os_version"/>
```

```
  <maecBundle:Action_Reference action_id="get_computer_name"/>
  <maecBundle:Action_Reference action_id="get_user_name"/>
  <maecBundle:Action_Reference action_id="get_system_dir"/>
  <maecBundle:Action_Reference action_id="get_dll_versions"/>
  <maecBundle:Action_Reference action_id="get_ram_info"/>
  <maecBundle:Action_Reference action_id="get_drive_type"/>
  <maecBundle:Action_Reference action_id="get_disk_space"/>
  <maecBundle:Action_Reference action_id="get_volume_info"/>

  <maecBundle:Action_Reference action_id="copy_file_locally"/>
  <maecBundle:Action_Reference action_id="start_process"/>

  <!-- record process info -->
  <maecBundle:Action_Reference action_id="get_pid"/>
  <maecBundle:Action_Reference action_id="get_ppid"/>
  <maecBundle:Action_Reference action_id="get_priorityclass"/>
  <maecBundle:Action_Reference action_id="get_thread_count"/>
  <maecBundle:Action_Reference action_id="get_heap_count"/>
  <maecBundle:Action_Reference action_id="get_process_image_size"/>
  <maecBundle:Action_Reference action_id="get_base_address"/>
  <maecBundle:Action_Reference action_id="get_image_address"/>

</maecBundle:Action_Composition>
```

```
 </maecBundle:Behavior>
 <maecBundle:Behavior id="code_injection">
  <maecBundle:Action_Composition>
   <maecBundle:Action_Reference action_id="list_processes"/>
   <maecBundle:Action_Reference action_id="open_process"/>
   <maecBundle:Action_Reference action_id="copy_self_to_process"/>
  </maecBundle:Action_Composition>
 </maecBundle:Behavior>
 <maecBundle:Behavior id="control_desktop">
  <maecBundle:Action_Composition>
   <maecBundle:Action_Reference action_id="capture_screenshots"/>
   <maecBundle:Action_Reference action_id="simulate_mouse_events"/>
   <maecBundle:Action_Reference action_id="simluate_keyboard_events"/>
  </maecBundle:Action_Composition>
 </maecBundle:Behavior>



</maecBundle:Behaviors>


 <!-- Placeholder for actions -->
<maecBundle:Actions>
 <maecBundle:Action id="copy_self_to_new_dll">
  <cybox:Associated_Objects>
```

<cybox:Associated_Object>
<cybox:Properties xsi:type="FileObj:FileObjectType">
<FileObj:File_Name>%systemroot%\system32\rasauto32.dll</FileObj:File_Name>
</cybox:Properties>
</cybox:Associated_Object>
</cybox:Associated_Objects>
</maecBundle:Action>
<maecBundle:Action id="register_dll_as_service">
<cybox:Associated_Objects>
<cybox:Associated_Object id="registry_service_entry_1">
<cybox:Association_Type xsi:type="maecVocabs:RegistryActionNameVocab-1.0">create registry key</cybox:Association_Type>
<cybox:Properties xsi:type="WinRegistryKeyObj:WindowsRegistryKeyObjectType">
<WinRegistryKeyObj:Key>System\CurrnetControlSet\Services\Iprip</WinRegistryKeyObj:Key>
<WinRegistryKeyObj:Hive>HKLM</WinRegistryKeyObj:Hive>
</cybox:Properties>
</cybox:Associated_Object>
<cybox:Associated_Object id="registry_service_entry_2">
<cybox:Association_Type xsi:type="maecVocabs:RegistryActionNameVocab-1.0">create registry key</cybox:Association_Type>
<cybox:Properties xsi:type="WinRegistryKeyObj:WindowsRegistryKeyObjectType">

<WinRegistryKeyObj:Key>System\CurrnetControlSet\Services\Iprip\Parameters\Service
Dll</WinRegistryKeyObj:Key>
<WinRegistryKeyObj:Hive>HKLM</WinRegistryKeyObj:Hive>
<WinRegistryKeyObj:Values>

<WinRegistryKeyObj:Value>%systemroot%\system32\rasauto32.dll</WinRegistryKeyO
bj:Value>
</WinRegistryKeyObj:Values>
</cybox:Properties>
</cybox:Associated_Object>
<cybox:Associated_Object id="registry_service_entry_3">
<cybox:Association_Type xsi:type="maecVocabs:RegistryActionNameVocab-
1.0">create registry key</cybox:Association_Type>
<cybox:Properties xsi:type="WinRegistryKeyObj:WindowsRegistryKeyObjectType">

<WinRegistryKeyObj:Key>System\CurrnetControlSet\Services\Iprip\DisplayName</Wi
nRegistryKeyObj:Key>
<WinRegistryKeyObj:Hive>HKLM</WinRegistryKeyObj:Hive>
<WinRegistryKeyObj:Values>
<WinRegistryKeyObj:Value>Iprip</WinRegistryKeyObj:Value>
</WinRegistryKeyObj:Values>
</cybox:Properties>

```
  </cybox:Associated_Object>
 </cybox:Associated_Objects>
</maecBundle:Action>

<maecBundle:Action id="fetch_commands_to_execute_from_cnc">
 <cybox:Associated_Objects>
  <cybox:Associated_Object>
   <cybox:Properties xsi:type="URIObj:URIObjectType">
    <URIObj:Value>216.15.210.68</URIObj:Value>
   </cybox:Properties>
  </cybox:Associated_Object>
 </cybox:Associated_Objects>
</maecBundle:Action>

<maecBundle:Action id="start_service">
 <cybox:Associated_Objects>
  <cybox:Associated_Object id="StartService">
   <cybox:Properties xsi:type="APIObj:APIObjectType">
    <APIObj:Function_Name>StartServiceA</APIObj:Function_Name>
   </cybox:Properties>
  </cybox:Associated_Object>
 </cybox:Associated_Objects>
</maecBundle:Action>
```

<maecBundle:Action id="stop_service">
<cybox:Associated_Objects>
<cybox:Associated_Object id="ControlService">
<cybox:Properties xsi:type="APIObj:APIObjectType">
<APIObj:Function_Name>ControlService</APIObj:Function_Name>
</cybox:Properties>
</cybox:Associated_Object>
</cybox:Associated_Objects>
</maecBundle:Action>
<maecBundle:Action id="open_remote_shell">
<cybox:Associated_Objects>
<cybox:Associated_Object id="cmd_file">
<cybox:Properties xsi:type="FileObj:FileObjectType">
<FileObj:File_Name>cmd.exe</FileObj:File_Name>
</cybox:Properties>
<cybox:Association_Type xsi:type="maecVocabs:FileActionNameVocab-1.1">copy file</cybox:Association_Type>

</cybox:Associated_Object>
<cybox:Associated_Object id="ati_file">
<cybox:Properties xsi:type="FileObj:FileObjectType">
<FileObj:File_Name>ati.exe</FileObj:File_Name>
</cybox:Properties>

```
  </cybox:Associated_Object>
  <cybox:Associated_Object id="input_pipe">
   <cybox:Description>Pipe that acts as source of commancds to cmd. The other end of the pipe is an HTTP session with the CnC server.</cybox:Description>
   <cybox:Properties xsi:type="PipeObj:PipeObjectType">
    <PipeObj:Name/>
   </cybox:Properties>
  </cybox:Associated_Object>
  <cybox:Associated_Object id="output_pipe">
   <cybox:Description>Pipe that acts as source of output of commands from cmd. The other end of the pipe is an HTTP session with the CnC server.</cybox:Description>
   <cybox:Properties xsi:type="PipeObj:PipeObjectType">
    <PipeObj:Name/>
   </cybox:Properties>
  </cybox:Associated_Object>
 </cybox:Associated_Objects>
</maecBundle:Action>
<maecBundle:Action id="download_file">
 <cybox:Associated_Objects>
  <cybox:Associated_Object id="InternetReadFile">
   <cybox:Properties xsi:type="APIObj:APIObjectType">
    <APIObj:Function_Name>InternetReadFile</APIObj:Function_Name>
   </cybox:Properties>
```

```
 </cybox:Associated_Object>
 <cybox:Associated_Object id="WriteFile">
  <cybox:Properties xsi:type="APIObj:APIObjectType">
   <APIObj:Function_Name>WriteFile</APIObj:Function_Name>
  </cybox:Properties>
 </cybox:Associated_Object>
</cybox:Associated_Objects>
</maecBundle:Action>

<maecBundle:Action id="get_os_version">
 <cybox:Associated_Objects>
  <cybox:Associated_Object id="get_os_version_API">
   <cybox:Properties xsi:type="APIObj:APIObjectType">
    <APIObj:Function_Name>GetVersionExA</APIObj:Function_Name>
   </cybox:Properties>
  </cybox:Associated_Object>
 </cybox:Associated_Objects>
</maecBundle:Action>
<maecBundle:Action id="get_computer_name">
 <cybox:Associated_Objects>
  <cybox:Associated_Object>
   <cybox:Properties xsi:type="APIObj:APIObjectType">
    <APIObj:Function_Name>GetComputerNameA</APIObj:Function_Name>
```

```
   </cybox:Properties>
  </cybox:Associated_Object>
 </cybox:Associated_Objects>
</maecBundle:Action>
<maecBundle:Action id="get_user_name">
 <cybox:Associated_Objects>
  <cybox:Associated_Object>
   <cybox:Properties xsi:type="APIObj:APIObjectType">
    <APIObj:Function_Name>GetUserNameA</APIObj:Function_Name>
   </cybox:Properties>
  </cybox:Associated_Object>
 </cybox:Associated_Objects>
</maecBundle:Action>
<maecBundle:Action id="get_system_dir">
 <cybox:Associated_Objects>
  <cybox:Associated_Object>
   <cybox:Properties xsi:type="APIObj:APIObjectType">
    <APIObj:Function_Name>SHGetKnownFolderPath</APIObj:Function_Name>
   </cybox:Properties>
  </cybox:Associated_Object>
 </cybox:Associated_Objects>
</maecBundle:Action>
<maecBundle:Action id="get_dll_versions"/>
```

<maecBundle:Action id="get_ram_info"/>

<maecBundle:Action id="get_drive_type">

<cybox:Associated_Objects>

<cybox:Associated_Object>

<cybox:Properties xsi:type="APIObj:APIObjectType">

<APIObj:Function_Name>GetDriveTypeA</APIObj:Function_Name>

</cybox:Properties>

</cybox:Associated_Object>

</cybox:Associated_Objects>

</maecBundle:Action>

<maecBundle:Action id="get_disk_space"/>

<maecBundle:Action id="get_volume_info">

<cybox:Associated_Objects>

<cybox:Associated_Object>

<cybox:Properties xsi:type="APIObj:APIObjectType">

<APIObj:Function_Name>GetVolumeInformationA</APIObj:Function_Name>

</cybox:Properties>

</cybox:Associated_Object>

</cybox:Associated_Objects>

</maecBundle:Action>

<maecBundle:Action id="copy_file_locally">

<cybox:Associated_Objects>

<cybox:Associated_Object>

<cybox:Properties xsi:type="FileObj:FileObjectType">

</cybox:Properties>

<cybox:Association_Type xsi:type="maecVocabs:FileActionNameVocab-1.1">copy file</cybox:Association_Type>

</cybox:Associated_Object>

</cybox:Associated_Objects>

</maecBundle:Action>

<maecBundle:Action id="start_process">

<cybox:Associated_Objects>

<cybox:Associated_Object id="CreateProcess_API">

<cybox:Properties xsi:type="APIObj:APIObjectType">

<APIObj:Function_Name>CreateProcess</APIObj:Function_Name>

</cybox:Properties>

</cybox:Associated_Object>

</cybox:Associated_Objects>

</maecBundle:Action>

<maecBundle:Action id="get_pid"/>

<maecBundle:Action id="get_ppid"/>

<maecBundle:Action id="get_priorityclass"/>

<maecBundle:Action id="get_thread_count"/>

<maecBundle:Action id="get_heap_count"/>

```
<maecBundle:Action id="get_process_image_size"/>
<maecBundle:Action id="get_base_address"/>
<maecBundle:Action id="get_image_address"/>

<maecBundle:Action id="list_processes"/>
<maecBundle:Action id="open_process"/>
<maecBundle:Action id="copy_self_to_process"/>

<maecBundle:Action id="capture_screenshots"/>
<maecBundle:Action id="simulate_mouse_events"/>
<maecBundle:Action id="simluate_keyboard_events"/>

</maecBundle:Actions>

<maecBundle:Candidate_Indicators>
 <!-- Capability CIs -->
<maecBundle:Candidate_Indicator id="capabilities_id">
 <maecBundle:Composition operator="AND">
  <maecBundle:Capability_Reference capability_idref="persistence"/>
  <maecBundle:Capability_Reference capability_idref="run_arbitrary_commands"/>
  <maecBundle:Capability_Reference capability_idref="trojanize_binaries"/>
  <maecBundle:Capability_Reference capability_idref="control_system_remotely"/>
 </maecBundle:Composition>
```

```
</maecBundle:Candidate_Indicator>
 <!-- Behaviour CIs -->
 <maecBundle:Candidate_Indicator id="run_arbitrary_commands_id">
  <maecBundle:Composition operator="AND">
   <maecBundle:Behavior_Reference behavior_idref="get_cnc_host_to_use"/>
   <maecBundle:Behavior_Reference behavior_idref="fetch_commands"/>
   <maecBundle:Behavior_Reference behavior_idref="execute_commands_received"/>
  </maecBundle:Composition>
 </maecBundle:Candidate_Indicator>
 <!-- Action CIs -->
 <maecBundle:Candidate_Indicator id="execute_commands_received_id">
  <maecBundle:Composition operator="OR">
    <maecBundle:Action_Reference action_id="start_service"/>
    <maecBundle:Action_Reference action_id="stop_service"/>
    <maecBundle:Action_Reference action_id="open_remote_shell"/>
    <maecBundle:Action_Reference action_id="download_file"/>
    <maecBundle:Action_Reference action_id="copy_file_locally"/>
    <maecBundle:Action_Reference action_id="start_process"/>

    <maecBundle:Action_Reference action_id="get_os_version"/>
    <maecBundle:Action_Reference action_id="get_computer_name"/>
    <maecBundle:Action_Reference action_id="get_user_name"/>
    <maecBundle:Action_Reference action_id="get_system_dir"/>
```

```
  <maecBundle:Action_Reference action_id="get_dll_versions"/>
  <maecBundle:Action_Reference action_id="get_ram_info"/>
  <maecBundle:Action_Reference action_id="get_drive_type"/>
  <maecBundle:Action_Reference action_id="get_disk_space"/>
  <maecBundle:Action_Reference action_id="get_volume_info"/>

  <maecBundle:Action_Reference action_id="get_pid"/>
  <maecBundle:Action_Reference action_id="get_ppid"/>
  <maecBundle:Action_Reference action_id="get_priorityclass"/>
  <maecBundle:Action_Reference action_id="get_thread_count"/>
  <maecBundle:Action_Reference action_id="get_heap_count"/>
  <maecBundle:Action_Reference action_id="get_process_image_size"/>
  <maecBundle:Action_Reference action_id="get_base_address"/>
  <maecBundle:Action_Reference action_id="get_image_address"/>


 </maecBundle:Composition>
</maecBundle:Candidate_Indicator>
<maecBundle:Candidate_Indicator id="code_injection_id">
 <maecBundle:Composition operator="AND">
  <maecBundle:Action_Reference action_id="list_processes"/>
  <maecBundle:Action_Reference action_id="open_process"/>
  <maecBundle:Action_Reference action_id="copy_self_to_process"/>
```

```
 </maecBundle:Composition>
</maecBundle:Candidate_Indicator>
<maecBundle:Candidate_Indicator id="control_desktop_id">
 <maecBundle:Composition operator="AND">
  <maecBundle:Action_Reference action_id="capture_screenshots"/>
  <maecBundle:Action_Reference action_id="simulate_mouse_events"/>
  <maecBundle:Action_Reference action_id="simluate_keyboard_events"/>
 </maecBundle:Composition>
</maecBundle:Candidate_Indicator>
<!-- Object CIs -->
<maecBundle:Candidate_Indicator id="register_dll_as_service_id">
 <maecBundle:Composition operator="AND">
  <maecBundle:Object_Reference object_idref="registry_service_entry_1"/>
  <maecBundle:Object_Reference object_idref="registry_service_entry_2"/>
  <maecBundle:Object_Reference object_idref="registry_service_entry_3"/>
 </maecBundle:Composition>
</maecBundle:Candidate_Indicator>
<maecBundle:Candidate_Indicator id="open_remote_shell_id">
 <maecBundle:Composition operator="AND">
  <maecBundle:Object_Reference object_idref="cmd_file"/>
  <maecBundle:Object_Reference object_idref="ati_file"/>
  <maecBundle:Object_Reference object_idref="input_pipe"/>
  <maecBundle:Object_Reference object_idref="output_pipe"/>
```

```
  </maecBundle:Composition>
 </maecBundle:Candidate_Indicator>
 <maecBundle:Candidate_Indicator id="download_file_id">
  <maecBundle:Composition operator="AND">
   <maecBundle:Object_Reference object_idref="InternetReadFile"/>
   <maecBundle:Object_Reference object_idref="WriteFile"/>
  </maecBundle:Composition>
 </maecBundle:Candidate_Indicator>

</maecBundle:Candidate_Indicators>



</maecBundle:MAEC_Bundle>
```

A.2 Beebus

```
        <?xml version="1.0" encoding="UTF-8"?>
<maecBundle:MAEC_Bundle xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance"
 xsi:schemaLocation="http://cybox.mitre.org/objects#ArtifactObject-2
../cybox_2.1_offline/objects/Artifact_Object.xsd
http://cybox.mitre.org/objects#WinRegistryKeyObject-2
maec/maec_4.1_offline/cybox_2.1_offline/objects/Win_Registry_Key_Object.xsd
http://cybox.mitre.org/objects#WinExecutableFileObject-2
```

../cybox_2.1_offline/objects/Win_Executable_File_Object.xsd

http://cybox.mitre.org/common-2

../maec/maec_4.1_offline/cybox_2.1_offline/cybox_common.xsd

http://cybox.mitre.org/objects#APIObject-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/API_Object.xsd

http://maec.mitre.org/XMLSchema/maec-bundle-4

file:/Users/asheer.malhotra/Documents/TT/maec/maec_4.1_offline/maec_bundle_schema

.xsd http://cybox.mitre.org/objects#WinExecutableFileObject-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/Win_Executable_File_Object.xsd

http://cybox.mitre.org/objects#PDFFileObject-1

maec/maec_4.1_offline/cybox_2.1_offline/objects/PDF_File_Object.xsd

http://cybox.mitre.org/objects#APIObject-2

../maec/maec_4.1_offline/cybox_2.1_offline/objects/API_Object.xsd

http://cybox.mitre.org/objects#WinExecutableFileObject-2

../maec/maec_4.1_offline/cybox_2.1_offline/objects/Win_Executable_File_Object.xsd

http://cybox.mitre.org/default_vocabularies-2

../cybox_2.1_offline/cybox_default_vocabularies.xsd

http://cybox.mitre.org/objects#PDFFileObject-1

../cybox_2.1_offline/PDF_File_Object.xsd

http://cybox.mitre.org/objects#WinRegistryKeyObject-2

../cybox_2.1_offline/Win_Registry_key_Object.xsd"

xmlns:HTTPSessionObj="http://cybox.mitre.org/objects#HTTPSessionObject-2"

xmlns:DNSQueryObj="http://cybox.mitre.org/objects#DNSQueryObject-2"

xmlns:maecBundle="http://maec.mitre.org/XMLSchema/maec-bundle-4"

xmlns:ProcessObj="http://cybox.mitre.org/objects#ProcessObject-2"

xmlns:SocketAddressObj="http://cybox.mitre.org/objects#SocketAddressObject-1"

xmlns:AddressObj="http://cybox.mitre.org/objects#AddressObject-2"

xmlns:NetworkConnectionObj="http://cybox.mitre.org/objects#NetworkConnectionObje
ct-2"

xmlns:PDFFileObj="http://cybox.mitre.org/objects#PDFFileObject-1"

xmlns:cyboxVocabs="http://cybox.mitre.org/default_vocabularies-2"

xmlns:HostnameObj="http://cybox.mitre.org/objects#HostnameObject-1"

xmlns:CodeObj="http://cybox.mitre.org/objects#CodeObject-2"

xmlns:FileObj="http://cybox.mitre.org/objects#FileObject-2"

xmlns:DNSRecordObj="http://cybox.mitre.org/objects#DNSRecordObject-2"

xmlns:WinRegistryKeyObj="http://cybox.mitre.org/objects#WinRegistryKeyObject-2"

xmlns:maecVocabs="http://maec.mitre.org/default_vocabularies-1"

xmlns:APIObj="http://cybox.mitre.org/objects#APIObject-2"

xmlns:WinExecutableFileObj="http://cybox.mitre.org/objects#WinExecutableFileObject
-2"

xmlns:cyboxCommon="http://cybox.mitre.org/common-2"

xmlns:URIObj="http://cybox.mitre.org/objects#URIObject-2"

xmlns:cybox="http://cybox.mitre.org/cybox-2"

id="Beebus_exe_TT" schema_version="4.1"

defined_subject="true">

<maecBundle:Malware_Instance_Object_Attributes>

<cybox:Description>The Malware is an EXE sample that runs prediefined commands on the target system</cybox:Description>

<cybox:Properties xsi:type="WinExecutableFileObj:WindowsExecutableFileObjectType">

<FileObj:File_Extension>EXE</FileObj:File_Extension>

<FileObj:Size_In_Bytes>80896</FileObj:Size_In_Bytes>

<FileObj:Hashes>

<cyboxCommon:Hash>

<cyboxCommon:Type>MD5</cyboxCommon:Type>

<cyboxCommon:Simple_Hash_Value>7ed557921ac60dfcb295ebabfd972301</cyboxCommon:Simple_Hash_Value>

</cyboxCommon:Hash>

</FileObj:Hashes>

</cybox:Properties>

</maecBundle:Malware_Instance_Object_Attributes>

<!-- Placeholder for capabilities -->

<maecBundle:Capabilities>

```
 <maecBundle:Capability id="run_information_stealing_commands" name="spying">
  <maecBundle:Behavior_Reference behavior_idref="send_beacon_cnc"/>
  <maecBundle:Behavior_Reference behavior_idref="execute_commands_recieved"/>
 </maecBundle:Capability>
</maecBundle:Capabilities>


<!-- Placeholder for behaviours -->
<maecBundle:Behaviors>
 <maecBundle:Behavior id="send_beacon_cnc">
  <maecBundle:Action_Composition>
   <maecBundle:Action_Reference action_id="get_host_name"/>
   <maecBundle:Action_Reference action_id="get_os_version"/>
   <maecBundle:Action_Reference action_id="encrypt_beacon_data"/>
   <maecBundle:Action_Reference action_id="send_beacon_data"/>
  </maecBundle:Action_Composition>

 </maecBundle:Behavior>
 <maecBundle:Behavior id="execute_commands_recieved">

  <maecBundle:Action_Composition>
   <maecBundle:Action_Reference action_id="get_drive_information"/>
```

```
    <maecBundle:Action_Reference action_id="get_os_information"/>
    <maecBundle:Action_Reference action_id="get_product_information"/>
    <maecBundle:Action_Reference action_id="get_processor_information"/>
    <maecBundle:Action_Reference action_id="get_process_information"/>
    <maecBundle:Action_Reference action_id="download_and_run_binary"/>
   </maecBundle:Action_Composition>
   <maecBundle:Relationships>
    <maecBundle:Relationship xsi:type="maecBundle:BehaviorRelationshipType"
type="Preceded_By">
     <maecBundle:Behavior_Reference behavior_idref="send_beacon_cnc"/>
    </maecBundle:Relationship>
   </maecBundle:Relationships>
 </maecBundle:Behavior>
</maecBundle:Behaviors>

 <!-- Placeholder for actions -->
 <maecBundle:Actions>
  <maecBundle:Action id="get_host_name">
   <cybox:Associated_Objects>
    <cybox:Associated_Object id="get_host-name_API">
     <cybox:Properties xsi:type="APIObj:APIObjectType">
      <APIObj:Function_Name>gethostname</APIObj:Function_Name>
     </cybox:Properties>
```

```
  </cybox:Associated_Object>
 </cybox:Associated_Objects>
</maecBundle:Action>
<maecBundle:Action id="get_os_version">
 <cybox:Associated_Objects>
  <cybox:Associated_Object id="get_os_version_API">
   <cybox:Properties xsi:type="APIObj:APIObjectType">
    <APIObj:Function_Name>GetVersionExA</APIObj:Function_Name>
   </cybox:Properties>
  </cybox:Associated_Object>
 </cybox:Associated_Objects>

</maecBundle:Action>
<maecBundle:Action id="encrypt_beacon_data">
<cybox:Description>Base64 encode data</cybox:Description>
</maecBundle:Action>
<maecBundle:Action id="send_beacon_data">
 <cybox:Associated_Objects>
  <cybox:Associated_Object id="cnc_URL">
   <cybox:Properties xsi:type="URIObj:URIObjectType">
    <URIObj:Value>http://bee.businessconsultants.net</URIObj:Value>
   </cybox:Properties>
  </cybox:Associated_Object>
```

```
 </cybox:Associated_Objects>
</maecBundle:Action>
<maecBundle:Action id="get_drive_information">
 <cybox:Associated_Objects>
  <cybox:Associated_Object id="GetDriveType">
   <cybox:Properties xsi:type="APIObj:APIObjectType">
    <APIObj:Function_Name>GetDriveType</APIObj:Function_Name>
   </cybox:Properties>
  </cybox:Associated_Object>
  <cybox:Associated_Object id="GetFreeDiskSpaceExW">
  <cybox:Properties xsi:type="APIObj:APIObjectType">
    <APIObj:Function_Name>GetDriveTypeExA</APIObj:Function_Name>
   </cybox:Properties>
  </cybox:Associated_Object>
  <cybox:Associated_Object id="GetVolumeInformationA">
   <cybox:Properties xsi:type="APIObj:APIObjectType">
    <APIObj:Function_Name>GetVolumeInformationA</APIObj:Function_Name>
   </cybox:Properties>
  </cybox:Associated_Object>
 </cybox:Associated_Objects>
</maecBundle:Action>
<maecBundle:Action id="get_os_information">
 <cybox:Associated_Objects>
```

<cybox:Associated_Object id="GetVersion">

<cybox:Properties xsi:type="APIObj:APIObjectType">

<APIObj:Function_Name>GetVersion</APIObj:Function_Name>

</cybox:Properties>

</cybox:Associated_Object>

</cybox:Associated_Objects>

</maecBundle:Action>

<maecBundle:Action id="get_product_information">

<cybox:Name xsi:type="maecVocabs:RegistryActionNameVocab-1.0">read registry key value</cybox:Name>

<cybox:Associated_Objects>

<cybox:Associated_Object id="product_info">

<cybox:Properties xsi:type="WinRegistryKeyObj:WindowsRegistryKeyObjectType">

<WinRegistryKeyObj:Key>SYSTEM\CurrentControlSet\Control\ProductionOptions</WinRegistryKeyObj:Key>

<WinRegistryKeyObj:Hive>HKLM</WinRegistryKeyObj:Hive>

<WinRegistryKeyObj:Values>

<WinRegistryKeyObj:Value>

<WinRegistryKeyObj:Name>ProductType</WinRegistryKeyObj:Name>

</WinRegistryKeyObj:Value>

</WinRegistryKeyObj:Values>

```
    </cybox:Properties>
   </cybox:Associated_Object>
  </cybox:Associated_Objects>
 </maecBundle:Action>
 <maecBundle:Action id="get_processor_information"/>
 <maecBundle:Action id="get_process_information">
  <cybox:Name xsi:type="cyboxVocabs:ActionNameVocab-1.1">Enumerate
Processes</cybox:Name>
  <cybox:Associated_Objects>
   <cybox:Associated_Object id="PID">
    <cybox:Properties xsi:type="ProcessObj:ProcessObjectType">
     <ProcessObj:PID/>
     </cybox:Properties>
   </cybox:Associated_Object>
  <cybox:Associated_Object id="StartTime">
   <cybox:Properties xsi:type="ProcessObj:ProcessObjectType">
    <ProcessObj:Creation_Time/>
   </cybox:Properties>
  </cybox:Associated_Object>
   <cybox:Associated_Object id="CurrentUser">
    <cybox:Properties xsi:type="ProcessObj:ProcessObjectType">
     <ProcessObj:Username/>
    </cybox:Properties>
```

```
   </cybox:Associated_Object>
  </cybox:Associated_Objects>
 </maecBundle:Action>
 <maecBundle:Action id="download_and_run_binary">
  <cybox:Description>Fetch and execute binary</cybox:Description>
  <cybox:Associated_Objects>

   <cybox:Associated_Object id="download_url">
    <cybox:Association_Type xsi:type="maecVocabs:NetworkActionNameVocab-
1.1">download file</cybox:Association_Type>
    <cybox:Properties xsi:type="URIObj:URIObjectType">
     <URIObj:Value/>
    </cybox:Properties>

   </cybox:Associated_Object>

   <cybox:Associated_Object id="malware_binary">
    <cybox:Association_Type xsi:type="maecVocabs:FileActionNameVocab-
1.1">execute file</cybox:Association_Type>
    <cybox:Properties
xsi:type="WinExecutableFileObj:WindowsExecutableFileObjectType">
     <FileObj:File_Name>iSun32.exe</FileObj:File_Name>
    </cybox:Properties>
```

```
  </cybox:Associated_Object>
 </cybox:Associated_Objects>
</maecBundle:Action>
</maecBundle:Actions>

<maecBundle:Candidate_Indicators>

 <!-- Behaviour CIs -->
 <maecBundle:Candidate_Indicator id="run_commands_on_target">
  <maecBundle:Composition operator="AND">
   <maecBundle:Behavior_Reference behavior_idref="send_beacon_cnc"/>
   <maecBundle:Behavior_Reference behavior_idref="execute_commands_recieved"/>
  </maecBundle:Composition>
 </maecBundle:Candidate_Indicator>

 <!-- Action CIs -->
 <maecBundle:Candidate_Indicator id="send_beacon_cnc_id">
  <maecBundle:Composition operator="AND">
   <maecBundle:Action_Reference action_id="get_host_name"/>
   <maecBundle:Action_Reference action_id="get_os_version"/>
   <maecBundle:Action_Reference action_id="encrypt_beacon_data"/>
   <maecBundle:Action_Reference action_id="send_beacon_data"/>
  </maecBundle:Composition>
```

```
</maecBundle:Candidate_Indicator>

<maecBundle:Candidate_Indicator id="execute_commands_received_id">
 <maecBundle:Composition operator="OR">
  <maecBundle:Action_Reference action_id="get_drive_information"/>
  <maecBundle:Action_Reference action_id="get_os_information"/>
  <maecBundle:Action_Reference action_id="get_product_information"/>
  <maecBundle:Action_Reference action_id="get_processor_information"/>
  <maecBundle:Action_Reference action_id="get_process_information"/>
  <maecBundle:Action_Reference action_id="download_and_run_binary"/>
 </maecBundle:Composition>
</maecBundle:Candidate_Indicator>

<!-- Object CIs -->
<maecBundle:Candidate_Indicator id="get_drive_information_id">
 <maecBundle:Composition operator="AND">
  <maecBundle:Object_Reference object_idref="GetDriveType"/>
  <maecBundle:Object_Reference object_idref="GetFreeDiskSpaceExW"/>
  <maecBundle:Object_Reference object_idref="GetVolumeInformationA"/>
 </maecBundle:Composition>
</maecBundle:Candidate_Indicator>
<maecBundle:Candidate_Indicator id="get_process_information_id">
 <maecBundle:Composition operator="AND">
```

<maecBundle:Object_Reference object_idref="PID"/>

<maecBundle:Object_Reference object_idref="StartTime"/>

<maecBundle:Object_Reference object_idref="CurrentUser"/>

</maecBundle:Composition>

</maecBundle:Candidate_Indicator>

<maecBundle:Candidate_Indicator id="download_and_run_binary_id">

<maecBundle:Composition operator="AND">

<maecBundle:Object_Reference object_idref="download_url"/>

<maecBundle:Object_Reference object_idref="malware_binary"/>

</maecBundle:Composition>

</maecBundle:Candidate_Indicator>

</maecBundle:Candidate_Indicators>

</maecBundle:MAEC_Bundle>

A.3 Cryptolocker

<?xml version="1.0" encoding="UTF-8"?>

<maecBundle:MAEC_Bundle xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"

xsi:schemaLocation="http://cybox.mitre.org/objects#ArtifactObject-2 maec/maec_4.1_offline/cybox_2.1_offline/objects/Artifact_Object.xsd

http://cybox.mitre.org/objects#WinRegistryKeyObject-2 maec/maec_4.1_offline/cybox_2.1_offline/objects/Win_Registry_Key_Object.xsd

http://cybox.mitre.org/objects#WinExecutableFileObject-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/Win_Executable_File_Object.xsd

http://cybox.mitre.org/common-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/cybox_common.xsd

http://cybox.mitre.org/objects#APIObject-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/API_Object.xsd

http://maec.mitre.org/XMLSchema/maec-bundle-4

maec/maec_4.1_offline/maec_bundle_schema.xsd

http://cybox.mitre.org/objects#WinExecutableFileObject-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/Win_Executable_File_Object.xsd

http://cybox.mitre.org/objects#PDFFileObject-1

maec/maec_4.1_offline/cybox_2.1_offline/objects/PDF_File_Object.xsd

http://cybox.mitre.org/objects#APIObject-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/API_Object.xsd

http://cybox.mitre.org/objects#WinExecutableFileObject-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/Win_Executable_File_Object.xsd

http://cybox.mitre.org/default_vocabularies-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/cybox_default_vocabularies.xsd

http://cybox.mitre.org/objects#PDFFileObject-1

maec/maec_4.1_offline/cybox_2.1_offline/objects/PDF_File_Object.xsd

http://cybox.mitre.org/objects#WinRegistryKeyObject-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/Win_Registry_key_Object.xsd

http://cybox.mitre.org/objects#WinMutexObject-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/Win_Mutex_Object.xsd

http://cybox.mitre.org/objects#ArtifactObject-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/Artifact_Object.xsd

http://cybox.mitre.org/objects#EmailMessageObject-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/Email_Message_Object.xsd

http://cybox.mitre.org/objects#MutexObject-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/Mutex_Object.xsd

http://cybox.mitre.org/objects#PipeObject-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/Pipe_Object.xsd

"

xmlns:HTTPSessionObj="http://cybox.mitre.org/objects#HTTPSessionObject-2"

xmlns:DNSQueryObj="http://cybox.mitre.org/objects#DNSQueryObject-2"

xmlns:maecBundle="http://maec.mitre.org/XMLSchema/maec-bundle-4"

xmlns:ProcessObj="http://cybox.mitre.org/objects#ProcessObject-2"

xmlns:SocketAddressObj="http://cybox.mitre.org/objects#SocketAddressObject-1"

xmlns:AddressObj="http://cybox.mitre.org/objects#AddressObject-2"

xmlns:NetworkConnectionObj="http://cybox.mitre.org/objects#NetworkConnectionObje

ct-2"

xmlns:PDFFileObj="http://cybox.mitre.org/objects#PDFFileObject-1"

xmlns:cyboxVocabs="http://cybox.mitre.org/default_vocabularies-2"

xmlns:HostnameObj="http://cybox.mitre.org/objects#HostnameObject-1"

xmlns:CodeObj="http://cybox.mitre.org/objects#CodeObject-2"

```
 xmlns:FileObj="http://cybox.mitre.org/objects#FileObject-2"
 xmlns:DNSRecordObj="http://cybox.mitre.org/objects#DNSRecordObject-2"
 xmlns:WinRegistryKeyObj="http://cybox.mitre.org/objects#WinRegistryKeyObject-2"
 xmlns:maecVocabs="http://maec.mitre.org/default_vocabularies-1"
 xmlns:APIObj="http://cybox.mitre.org/objects#APIObject-2"

xmlns:WinExecutableFileObj="http://cybox.mitre.org/objects#WinExecutableFileObject
-2"
 xmlns:cyboxCommon="http://cybox.mitre.org/common-2"
 xmlns:URIObj="http://cybox.mitre.org/objects#URIObject-2"
 xmlns:cybox="http://cybox.mitre.org/cybox-2"
 xmlns:WinMutexObj="http://cybox.mitre.org/objects#WinMutexObject-2"
 xmlns:ArtifactObj="http://cybox.mitre.org/objects#ArtifactObject-2"
 xmlns:EmailMessageObj="http://cybox.mitre.org/objects#EmailMessageObject-2"
 xmlns:MutexObj="http://cybox.mitre.org/objects#MutexObject-2"
 xmlns:PipeObj="http://cybox.mitre.org/objects#PipeObject-2"
 id="Cryptolocker_exe_TT" schema_version="4.1"
 defined_subject="true">

 <maecBundle:Malware_Instance_Object_Attributes>
  <cybox:Description>The Malware holds the targets data to ransom:
ransomware</cybox:Description>
 <cybox:Properties
```

xsi:type="WinExecutableFileObj:WindowsExecutableFileObjectType">
<FileObj:File_Extension>EXE</FileObj:File_Extension>
<FileObj:Size_In_Bytes>708608</FileObj:Size_In_Bytes>
<FileObj:Hashes>
<cyboxCommon:Hash>
<cyboxCommon:Type>MD5</cyboxCommon:Type>

<cyboxCommon:Simple_Hash_Value>bc11c93f1b6dc74bf4804a35b34d9267</cyboxCommon:Simple_Hash_Value>
</cyboxCommon:Hash>
</FileObj:Hashes>
</cybox:Properties>
</maecBundle:Malware_Instance_Object_Attributes>

<!-- Placeholder for capabilities -->
<maecBundle:Capabilities>
<maecBundle:Capability id="persistence" name="persistence">
<maecBundle:Behavior_Reference behavior_idref="persistence_at_runtime"/>
<maecBundle:Behavior_Reference behavior_idref="persistence_across_reboots"/>
</maecBundle:Capability>
<maecBundle:Capability id="encrypt_files_on_target" name="destruction">
<maecBundle:Behavior_Reference
behavior_idref="fetch_public_key_for_encryption"/>

<maecBundle:Behavior_Reference behavior_idref="encrypt_files"/>
</maecBundle:Capability>
<maecBundle:Capability id="decrypt_files_on_target">
<maecBundle:Behavior_Reference behavior_idref="display_ransom_note"/>
<maecBundle:Behavior_Reference behavior_idref="send_payment_id_to_cnc"/>
<maecBundle:Behavior_Reference behavior_idref="fetch_private_key_for_target"/>
<maecBundle:Behavior_Reference behavior_idref="decrypt_key_from_files"/>
<maecBundle:Behavior_Reference behavior_idref="decrypt_to_original_file"/>
</maecBundle:Capability>

</maecBundle:Capabilities>

<!-- Placeholder for behaviours -->
<maecBundle:Behaviors>
<maecBundle:Behavior id="persistence_at_runtime">
<maecBundle:Action_Composition>
<maecBundle:Action_Reference action_id="create_mutex_BACD"/>
<maecBundle:Action_Reference action_id="create_mutex_3F3F"/>
</maecBundle:Action_Composition>
</maecBundle:Behavior>
<maecBundle:Behavior id="persistence_across_reboots">
<maecBundle:Action_Composition>
<maecBundle:Action_Reference action_id="copy_self_to_new_exe"/>

<maecBundle:Action_Reference action_id="modify_registry"/>
</maecBundle:Action_Composition>
</maecBundle:Behavior>
<maecBundle:Behavior id="fetch_public_key_for_encryption">
<maecBundle:Action_Composition>
<maecBundle:Action_Reference action_id="create_publice_key_seed"/>
<maecBundle:Action_Reference action_id="send_seed_to_cnc_over_HTTP_SHA1"/>
</maecBundle:Action_Composition>
</maecBundle:Behavior>
<maecBundle:Behavior id="encrypt_files">
<maecBundle:Action_Composition>
<maecBundle:Action_Reference action_id="enumerate_files"/>
<maecBundle:Action_Reference action_id="compare_to_whitelist_folders"/>
<maecBundle:Action_Reference action_id="compare_to_blacklist_extensions"/>
<maecBundle:Action_Reference
action_id="generate_AES_key_for_each_file_type"/>
<maecBundle:Action_Reference
action_id="replace_original_file_contents_with_encrypted"/>
<maecBundle:Action_Reference action_id="encrypt_AES_encryption_key"/>
<maecBundle:Action_Reference
action_id="embed_encryption_key_into_encrypted_file"/>
<maecBundle:Action_Reference action_id="add_file_to_list_registry"/>
</maecBundle:Action_Composition>

```
 </maecBundle:Behavior>
 <maecBundle:Behavior id="display_ransom_note">
  <maecBundle:Action_Composition>
   <maecBundle:Action_Reference action_id="show_gui_informing_target_user"/>
  </maecBundle:Action_Composition>
 </maecBundle:Behavior>
 <maecBundle:Behavior id="send_payment_id_to_cnc">
  <maecBundle:Action_Composition>
   <maecBundle:Action_Reference action_id="send_transcation_id_to_cnc"/>
  </maecBundle:Action_Composition>
 </maecBundle:Behavior>
 <maecBundle:Behavior id="fetch_private_key_for_target">
  <maecBundle:Action_Composition>
   <maecBundle:Action_Reference action_id="get_key_from_cnc"/>
  </maecBundle:Action_Composition>
 </maecBundle:Behavior>
 <maecBundle:Behavior id="decrypt_key_from_files">
  <maecBundle:Action_Composition>
   <maecBundle:Action_Reference
action_id="enumerate_encrypted_files_from_registry"/>
   <maecBundle:Action_Reference
action_id="decrypt_AES_key_using_private_RSA_key"/>
  </maecBundle:Action_Composition>
```

```
  </maecBundle:Behavior>
  <maecBundle:Behavior id="decrypt_to_original_file">
   <maecBundle:Action_Composition>
    <maecBundle:Action_Reference action_id="decrypt_files_using_AES_key"/>
   </maecBundle:Action_Composition>
  </maecBundle:Behavior>

</maecBundle:Behaviors>

 <!-- Placeholder for actions -->
 <maecBundle:Actions>
  <maecBundle:Action id="create_mutex_BACD">
   <cybox:Name xsi:type="maecVocabs:SynchronizationActionNameVocab-1.0">create
mutex</cybox:Name>
   <cybox:Associated_Objects>
    <cybox:Associated_Object>
     <cybox:Properties xsi:type="MutexObj:MutexObjectType" named="true">
      <MutexObj:Name>{34184A33-0407-212E-3300-
09040709BACD}</MutexObj:Name>
     </cybox:Properties>
    </cybox:Associated_Object>
   </cybox:Associated_Objects>
   </maecBundle:Action>
```

<maecBundle:Action id="create_mutex_3F3F">
<cybox:Name xsi:type="maecVocabs:SynchronizationActionNameVocab-1.0">create mutex</cybox:Name>
<cybox:Associated_Objects>
<cybox:Associated_Object>
<cybox:Properties xsi:type="MutexObj:MutexObjectType" named="true">
<MutexObj:Name>{34184A33-0407-212E-3300-090407093F3F}</MutexObj:Name>
</cybox:Properties>
</cybox:Associated_Object>
</cybox:Associated_Objects>
</maecBundle:Action>
<maecBundle:Action id="copy_self_to_new_exe">
<cybox:Name xsi:type="maecVocabs:FileActionNameVocab-1.1">create file</cybox:Name>
<cybox:Associated_Objects>
<cybox:Associated_Object>
<cybox:Properties xsi:type="WinExecutableFileObj:WindowsExecutableFileObjectType">
<FileObj:File_Name>{34184A33-0407-212E-3300-09040709E2C2}.exe</FileObj:File_Name>
<FileObj:File_Path>%roaming%</FileObj:File_Path>
<FileObj:File_Extension>exe</FileObj:File_Extension>

```
    </cybox:Properties>
   </cybox:Associated_Object>
  </cybox:Associated_Objects>
 </maecBundle:Action>
 <maecBundle:Action id="modify_registry">
  <cybox:Name xsi:type="maecVocabs:RegistryActionNameVocab-1.0">create registry
key</cybox:Name>
  <cybox:Associated_Objects>
   <cybox:Associated_Object>
    <cybox:Properties
xsi:type="WinRegistryKeyObj:WindowsRegistryKeyObjectType">

<WinRegistryKeyObj:Key>\Software\Microsoft\Windows\CurrentVersion\Run</WinRe
gistryKeyObj:Key>
     <WinRegistryKeyObj:Hive>HKCU</WinRegistryKeyObj:Hive>
     <WinRegistryKeyObj:Values>
      <WinRegistryKeyObj:Value>
       <WinRegistryKeyObj:Name>Cryptolocker</WinRegistryKeyObj:Name>
       <WinRegistryKeyObj:Data>%romaing%\{34184A33-0407-212E-3300-
09040709E2C2}.exe</WinRegistryKeyObj:Data>
      </WinRegistryKeyObj:Value>
     </WinRegistryKeyObj:Values>
    </cybox:Properties>
```

```
 </cybox:Associated_Object>
</cybox:Associated_Objects>
</maecBundle:Action>
<maecBundle:Action id="create_public_key_seed">
 <cybox:Associated_Objects>
  <cybox:Associated_Object id="GetVersion">
   <cybox:Properties xsi:type="APIObj:APIObjectType">
    <APIObj:Function_Name>GetVersion</APIObj:Function_Name>
   </cybox:Properties>
  </cybox:Associated_Object>
  <cybox:Associated_Object id="GetComputerName">
   <cybox:Properties xsi:type="APIObj:APIObjectType">
    <APIObj:Function_Name>GetComputerName</APIObj:Function_Name>
   </cybox:Properties>
  </cybox:Associated_Object>
  <cybox:Associated_Object id="GetUserDefaultLCID">
   <cybox:Description>Language ID</cybox:Description>
   <cybox:Properties xsi:type="APIObj:APIObjectType">
    <APIObj:Function_Name>GetUserDefaultLCID</APIObj:Function_Name>
   </cybox:Properties>
  </cybox:Associated_Object>
  <cybox:Associated_Object id="user_group_name"/>
 </cybox:Associated_Objects>
```

```
</maecBundle:Action>
<maecBundle:Action id="send_seed_to_cnc_over_HTTP_SHA1">
 <cybox:Associated_Objects>
  <cybox:Associated_Object>
   <cybox:Properties xsi:type="HTTPSessionObj:HTTPSessionObjectType">
    <HTTPSessionObj:HTTP_Request_Response>
     <HTTPSessionObj:HTTP_Client_Request>
      <HTTPSessionObj:HTTP_Request_Line>
       <HTTPSessionObj:HTTP_Method>GET</HTTPSessionObj:HTTP_Method>
       <HTTPSessionObj:Value>oqcqedagwnnkcl.org</HTTPSessionObj:Value>
      </HTTPSessionObj:HTTP_Request_Line>
     </HTTPSessionObj:HTTP_Client_Request>
    </HTTPSessionObj:HTTP_Request_Response>
   </cybox:Properties>
  </cybox:Associated_Object>
 </cybox:Associated_Objects>
</maecBundle:Action>
<maecBundle:Action id="enumerate_files">
<cybox:Associated_Objects>
 <cybox:Associated_Object>
  <cybox:Properties xsi:type="APIObj:APIObjectType">
   <APIObj:Function_Name>FindFirstFile</APIObj:Function_Name>
  </cybox:Properties>
```

```
 </cybox:Associated_Object>
</cybox:Associated_Objects>
</maecBundle:Action>
<maecBundle:Action id="compare_to_whitelist_folders">
 <cybox:Associated_Objects>
  <cybox:Associated_Object>
   <cybox:Properties xsi:type="FileObj:FileObjectType">
    <FileObj:Digital_Signatures>

<cyboxCommon:Digital_Signature>C:\Users\username\AppData\Local\Temp</cyboxCo
mmon:Digital_Signature>
<cyboxCommon:Digital_Signature>C:\Users\username\AppData\Locallow</cyboxCom
mon:Digital_Signature>
<cyboxCommon:Digital_Signature>C:\Users\username\AppData\Local\Microsoft\Windo
ws\Temporary Internet Files</cyboxCommon:Digital_Signature>
<cyboxCommon:Digital_Signature>C:\Users\username\AppData\Roaming\Microsoft\Wi
ndows\Templates</cyboxCommon:Digital_Signature>

<cyboxCommon:Digital_Signature>C:\ProgramData\Microsoft\Windows\Templates</cy
boxCommon:Digital_Signature>
     <cyboxCommon:Digital_Signature>C:\Program
Files</cyboxCommon:Digital_Signature>
```

<cyboxCommon:Digital_Signature>C:\Windows</cyboxCommon:Digital_Signature>

<cyboxCommon:Digital_Signature>%ProgramW6432%</cyboxCommon:Digital_Signature>

</FileObj:Digital_Signatures>

</cybox:Properties>

</cybox:Associated_Object>

</cybox:Associated_Objects>

</maecBundle:Action>

<maecBundle:Action id="compare_to_blacklist_extensions">

<cybox:Associated_Objects>

<cybox:Associated_Object>

<cybox:Properties xsi:type="FileObj:FileObjectType">

<FileObj:Digital_Signatures>

<cyboxCommon:Digital_Signature>.odt</cyboxCommon:Digital_Signature>

<cyboxCommon:Digital_Signature>.ods</cyboxCommon:Digital_Signature>

<cyboxCommon:Digital_Signature>.odp</cyboxCommon:Digital_Signature>

<cyboxCommon:Digital_Signature>.odm</cyboxCommon:Digital_Signature>

<cyboxCommon:Digital_Signature>.odc</cyboxCommon:Digital_Signature>

<cyboxCommon:Digital_Signature>.odb</cyboxCommon:Digital_Signature>

<cyboxCommon:Digital_Signature>.doc</cyboxCommon:Digital_Signature>

<cyboxCommon:Digital_Signature>.docx</cyboxCommon:Digital_Signature>

<cyboxCommon:Digital_Signature>.docm</cyboxCommon:Digital_Signature>

<cyboxCommon:Digital_Signature>.wps</cyboxCommon:Digital_Signature>

<cyboxCommon:Digital_Signature>.xls</cyboxCommon:Digital_Signature>

<cyboxCommon:Digital_Signature>.xlsx</cyboxCommon:Digital_Signature>

<cyboxCommon:Digital_Signature>.xlsm</cyboxCommon:Digital_Signature>

<cyboxCommon:Digital_Signature>.xlk</cyboxCommon:Digital_Signature>

<cyboxCommon:Digital_Signature>.</cyboxCommon:Digital_Signature>

<cyboxCommon:Digital_Signature>.ppt</cyboxCommon:Digital_Signature>

<cyboxCommon:Digital_Signature>.pptx</cyboxCommon:Digital_Signature>

<cyboxCommon:Digital_Signature>.pptm</cyboxCommon:Digital_Signature>

<cyboxCommon:Digital_Signature>.mdb</cyboxCommon:Digital_Signature>

<cyboxCommon:Digital_Signature>.accdb</cyboxCommon:Digital_Signature>

<cyboxCommon:Digital_Signature>.pst</cyboxCommon:Digital_Signature>

<cyboxCommon:Digital_Signature>.dwg</cyboxCommon:Digital_Signature>

<cyboxCommon:Digital_Signature>.dxf</cyboxCommon:Digital_Signature>

<cyboxCommon:Digital_Signature>.dxg</cyboxCommon:Digital_Signature>

<cyboxCommon:Digital_Signature>.wpd</cyboxCommon:Digital_Signature>

<cyboxCommon:Digital_Signature>.rtf</cyboxCommon:Digital_Signature>

<cyboxCommon:Digital_Signature>.wb2</cyboxCommon:Digital_Signature>

<cyboxCommon:Digital_Signature>.pdf</cyboxCommon:Digital_Signature>

<cyboxCommon:Digital_Signature>.mdf</cyboxCommon:Digital_Signature>

<cyboxCommon:Digital_Signature>.dbf</cyboxCommon:Digital_Signature>

<cyboxCommon:Digital_Signature>.psd</cyboxCommon:Digital_Signature>

<cyboxCommon:Digital_Signature>.pdd</cyboxCommon:Digital_Signature>

<cyboxCommon:Digital_Signature>.eps</cyboxCommon:Digital_Signature>

<cyboxCommon:Digital_Signature>.ai</cyboxCommon:Digital_Signature>

<cyboxCommon:Digital_Signature>.indd</cyboxCommon:Digital_Signature>

<cyboxCommon:Digital_Signature>.cdr</cyboxCommon:Digital_Signature>

<cyboxCommon:Digital_Signature>.dng</cyboxCommon:Digital_Signature>

<cyboxCommon:Digital_Signature>.3fr</cyboxCommon:Digital_Signature>

<cyboxCommon:Digital_Signature>.arw</cyboxCommon:Digital_Signature>

<cyboxCommon:Digital_Signature>.srf</cyboxCommon:Digital_Signature>

<cyboxCommon:Digital_Signature>.sr2</cyboxCommon:Digital_Signature>

<cyboxCommon:Digital_Signature>.bay</cyboxCommon:Digital_Signature>

<cyboxCommon:Digital_Signature>.crw</cyboxCommon:Digital_Signature>

<cyboxCommon:Digital_Signature>.cr2</cyboxCommon:Digital_Signature>

<cyboxCommon:Digital_Signature>.dcr</cyboxCommon:Digital_Signature>

<cyboxCommon:Digital_Signature>.kdc</cyboxCommon:Digital_Signature>

<cyboxCommon:Digital_Signature>.erf</cyboxCommon:Digital_Signature>

<cyboxCommon:Digital_Signature>.mef</cyboxCommon:Digital_Signature>

<cyboxCommon:Digital_Signature>.mrw</cyboxCommon:Digital_Signature>

<cyboxCommon:Digital_Signature>.nef</cyboxCommon:Digital_Signature>

<cyboxCommon:Digital_Signature>.nrw</cyboxCommon:Digital_Signature>

<cyboxCommon:Digital_Signature>.orf</cyboxCommon:Digital_Signature>

<cyboxCommon:Digital_Signature>.raf</cyboxCommon:Digital_Signature>

<cyboxCommon:Digital_Signature>.raw</cyboxCommon:Digital_Signature>

<cyboxCommon:Digital_Signature>.rwl</cyboxCommon:Digital_Signature>

<cyboxCommon:Digital_Signature>.rw2</cyboxCommon:Digital_Signature>

<cyboxCommon:Digital_Signature>.r3d</cyboxCommon:Digital_Signature>

<cyboxCommon:Digital_Signature>.ptx</cyboxCommon:Digital_Signature>

<cyboxCommon:Digital_Signature>.pef</cyboxCommon:Digital_Signature>

<cyboxCommon:Digital_Signature>.srw</cyboxCommon:Digital_Signature>

<cyboxCommon:Digital_Signature>.x3f</cyboxCommon:Digital_Signature>

<cyboxCommon:Digital_Signature>????????.jpg</cyboxCommon:Digital_Signature>

<cyboxCommon:Digital_Signature>????????.jpe</cyboxCommon:Digital_Signature>

<cyboxCommon:Digital_Signature>img_*.jpg</cyboxCommon:Digital_Signature>

<cyboxCommon:Digital_Signature>????????.m4v</cyboxCommon:Digital_Signature>

<cyboxCommon:Digital_Signature>????????.mp4</cyboxCommon:Digital_Signature>

<cyboxCommon:Digital_Signature>????????.mov</cyboxCommon:Digital_Signature>

<cyboxCommon:Digital_Signature>????????.3gp</cyboxCommon:Digital_Signature>

<cyboxCommon:Digital_Signature>*.der</cyboxCommon:Digital_Signature>

<cyboxCommon:Digital_Signature>.cer</cyboxCommon:Digital_Signature>

<cyboxCommon:Digital_Signature>.crt</cyboxCommon:Digital_Signature>

<cyboxCommon:Digital_Signature>.pem</cyboxCommon:Digital_Signature>

<cyboxCommon:Digital_Signature>.pfx</cyboxCommon:Digital_Signature>

<cyboxCommon:Digital_Signature>.p12</cyboxCommon:Digital_Signature>

<cyboxCommon:Digital_Signature>.p7b</cyboxCommon:Digital_Signature>

<cyboxCommon:Digital_Signature>.p7c</cyboxCommon:Digital_Signature>

</FileObj:Digital_Signatures>

</cybox:Properties>

</cybox:Associated_Object>

</cybox:Associated_Objects>

</maecBundle:Action>

<maecBundle:Action id="generate_AES_key_for_each_file_type">

<cybox:Associated_Objects>

<cybox:Associated_Object>

<cybox:Description> AES key generated for each filetype</cybox:Description>

</cybox:Associated_Object>

</cybox:Associated_Objects>

</maecBundle:Action>

<maecBundle:Action id="replace_original_file_contents_with_encrypted"/>

<maecBundle:Action id="encrypt_AES_encryption_key"/>

<maecBundle:Action id="embed_encryption_key_into_encrypted_file"/>

<maecBundle:Action id="add_file_to_list_registry">

<cybox:Associated_Objects>

<cybox:Associated_Object>

<cybox:Properties

xsi:type="WinRegistryKeyObj:WindowsRegistryKeyObjectType">

<WinRegistryKeyObj:Key>Software\Cryptolocker\Files</WinRegistryKeyObj:Key>

<WinRegistryKeyObj:Hive>HKCU</WinRegistryKeyObj:Hive>

<WinRegistryKeyObj:Values>

<WinRegistryKeyObj:Value>full_file_path</WinRegistryKeyObj:Value>

</WinRegistryKeyObj:Values>

</cybox:Properties>

</cybox:Associated_Object>

</cybox:Associated_Objects>

</maecBundle:Action>

<maecBundle:Action id="show_gui_informing_target_user"/>

<maecBundle:Action id="get_key_from_cnc">

<cybox:Associated_Objects>

<cybox:Associated_Object>

<cybox:Properties xsi:type="HTTPSessionObj:HTTPSessionObjectType">

<HTTPSessionObj:HTTP_Request_Response>

<HTTPSessionObj:HTTP_Client_Request>

<HTTPSessionObj:HTTP_Request_Line>

<HTTPSessionObj:HTTP_Method>GET</HTTPSessionObj:HTTP_Method>

<HTTPSessionObj:Value>oqcqedagwnnkcl.org/target_id</HTTPSessionObj:Value>

```
      </HTTPSessionObj:HTTP_Request_Line>
     </HTTPSessionObj:HTTP_Client_Request>
    </HTTPSessionObj:HTTP_Request_Response>
   </cybox:Properties>
  </cybox:Associated_Object>
 </cybox:Associated_Objects>
</maecBundle:Action>
<maecBundle:Action id="enumerate_encrypted_files_from_registry"/>
<maecBundle:Action id="decrypt_AES_key_using_private_RSA_key"/>
<maecBundle:Action id="decrypt_files_using_AES_key"/>

</maecBundle:Actions>

<maecBundle:Candidate_Indicators>
 <!-- Capability CIs -->
 <maecBundle:Candidate_Indicator id="capabilities_id">
  <maecBundle:Composition operator="AND">
   <maecBundle:Capability_Reference capability_idref="persistence"/>
   <maecBundle:Capability_Reference capability_idref="encrypt_files_on_target"/>
  </maecBundle:Composition>
 </maecBundle:Candidate_Indicator>
 <!-- Behaviour CIs -->
 <maecBundle:Candidate_Indicator id="persistence_id">
```

```
  <maecBundle:Composition operator="AND">
   <maecBundle:Behavior_Reference behavior_idref="persistence_at_runtime_id"/>
   <maecBundle:Behavior_Reference behavior_idref="persistence_across_reboots_id"/>
  </maecBundle:Composition>
 </maecBundle:Candidate_Indicator>
 <maecBundle:Candidate_Indicator id="encrypt_files_on_target_id">
  <maecBundle:Composition operator="AND">
   <maecBundle:Behavior_Reference
behavior_idref="fetch_public_key_for_encryption"/>
   <maecBundle:Behavior_Reference behavior_idref="encrypt_files"/>
  </maecBundle:Composition>
 </maecBundle:Candidate_Indicator>
 <!-- Action CIs -->
 <maecBundle:Candidate_Indicator id="persistence_at_runtime_id">
  <maecBundle:Composition operator="AND">
   <maecBundle:Action_Reference action_id="create_mutex_BACD"/>
   <maecBundle:Action_Reference action_id="create_mutex_3F3F"/>
  </maecBundle:Composition>
 </maecBundle:Candidate_Indicator>
 <maecBundle:Candidate_Indicator id="persistence_across_reboots_id">
  <maecBundle:Composition operator="AND">
   <maecBundle:Action_Reference action_id="copy_self_to_new_exe"/>
   <maecBundle:Action_Reference action_id="modify_registry"/>
```

```
 </maecBundle:Composition>
</maecBundle:Candidate_Indicator>
<maecBundle:Candidate_Indicator id="fetch_public_key_for_encryption_id">
 <maecBundle:Composition operator="AND">
  <maecBundle:Action_Reference action_id="create_publice_key_seed"/>
  <maecBundle:Action_Reference action_id="send_seed_to_cnc_over_HTTP_SHA1"/>
 </maecBundle:Composition>
</maecBundle:Candidate_Indicator>
<maecBundle:Candidate_Indicator id="encrypt_files_id">
 <maecBundle:Composition operator="AND">
  <maecBundle:Action_Reference action_id="enumerate_files"/>
  <maecBundle:Action_Reference action_id="compare_to_whitelist_folders"/>
  <maecBundle:Action_Reference action_id="compare_to_blacklist_extensions"/>
  <maecBundle:Action_Reference
action_id="generate_AES_key_for_each_file_type"/>
  <maecBundle:Action_Reference
action_id="replace_original_file_contents_with_encrypted"/>
  <maecBundle:Action_Reference action_id="encrypt_AES_encryption_key"/>
  <maecBundle:Action_Reference action_id="embed_encryption_key_into_file"/>
  <maecBundle:Action_Reference action_id="add_file_to_list_registry"/>
 </maecBundle:Composition>
</maecBundle:Candidate_Indicator>
<!-- Object CIs -->
```

<maecBundle:Candidate_Indicator id="create_public_key_seed_id">

<maecBundle:Composition operator="AND">

<maecBundle:Object_Reference object_idref="GetComputerName"/>

<maecBundle:Object_Reference object_idref="GetUserDefaultLCID"/>

<maecBundle:Object_Reference object_idref="GetVersion"/>

<maecBundle:Object_Reference object_idref="user_group_name"/>

</maecBundle:Composition>

</maecBundle:Candidate_Indicator>

</maecBundle:Candidate_Indicators>

</maecBundle:MAEC_Bundle>

A.4 WebC2-Cson

<?xml version="1.0" encoding="UTF-8"?>

<maecBundle:MAEC_Bundle xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"

xsi:schemaLocation="http://cybox.mitre.org/objects#ArtifactObject-2 maec/maec_4.1_offline/cybox_2.1_offline/objects/Artifact_Object.xsd http://cybox.mitre.org/objects#WinRegistryKeyObject-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/Win_Registry_Key_Object.xsd

http://cybox.mitre.org/objects#WinExecutableFileObject-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/Win_Executable_File_Object.xsd

http://cybox.mitre.org/common-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/cybox_common.xsd

http://cybox.mitre.org/objects#APIObject-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/API_Object.xsd

http://maec.mitre.org/XMLSchema/maec-bundle-4

maec/maec_4.1_offline/maec_bundle_schema.xsd

http://cybox.mitre.org/objects#WinExecutableFileObject-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/Win_Executable_File_Object.xsd

http://cybox.mitre.org/objects#PDFFileObject-1

maec/maec_4.1_offline/cybox_2.1_offline/objects/PDF_File_Object.xsd

http://cybox.mitre.org/objects#APIObject-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/API_Object.xsd

http://cybox.mitre.org/objects#WinExecutableFileObject-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/Win_Executable_File_Object.xsd

http://cybox.mitre.org/default_vocabularies-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/cybox_default_vocabularies.xsd

http://cybox.mitre.org/objects#PDFFileObject-1

maec/maec_4.1_offline/cybox_2.1_offline/objects/PDF_File_Object.xsd

http://cybox.mitre.org/objects#WinRegistryKeyObject-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/Win_Registry_key_Object.xsd

http://cybox.mitre.org/objects#WinMutexObject-2

.maec/maec_4.1_offline/cybox_2.1_offline/objects/Win_Mutex_Object.xsd

http://cybox.mitre.org/objects#ArtifactObject-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/Artifact_Object.xsd

"

xmlns:HTTPSessionObj="http://cybox.mitre.org/objects#HTTPSessionObject-2"

xmlns:DNSQueryObj="http://cybox.mitre.org/objects#DNSQueryObject-2"

xmlns:maecBundle="http://maec.mitre.org/XMLSchema/maec-bundle-4"

xmlns:ProcessObj="http://cybox.mitre.org/objects#ProcessObject-2"

xmlns:SocketAddressObj="http://cybox.mitre.org/objects#SocketAddressObject-1"

xmlns:AddressObj="http://cybox.mitre.org/objects#AddressObject-2"

xmlns:NetworkConnectionObj="http://cybox.mitre.org/objects#NetworkConnectionObje

ct-2"

xmlns:PDFFileObj="http://cybox.mitre.org/objects#PDFFileObject-1"

xmlns:cyboxVocabs="http://cybox.mitre.org/default_vocabularies-2"

xmlns:HostnameObj="http://cybox.mitre.org/objects#HostnameObject-1"

xmlns:CodeObj="http://cybox.mitre.org/objects#CodeObject-2"

xmlns:FileObj="http://cybox.mitre.org/objects#FileObject-2"

xmlns:DNSRecordObj="http://cybox.mitre.org/objects#DNSRecordObject-2"

xmlns:WinRegistryKeyObj="http://cybox.mitre.org/objects#WinRegistryKeyObject-2"

xmlns:maecVocabs="http://maec.mitre.org/default_vocabularies-1"

xmlns:APIObj="http://cybox.mitre.org/objects#APIObject-2"

xmlns:WinExecutableFileObj="http://cybox.mitre.org/objects#WinExecutableFileObject
-2"
 xmlns:cyboxCommon="http://cybox.mitre.org/common-2"
 xmlns:URIObj="http://cybox.mitre.org/objects#URIObject-2"
 xmlns:cybox="http://cybox.mitre.org/cybox-2"
 xmlns:WinMutexObj="http://cybox.mitre.org/objects#WinMutexObject-2"
 xmlns:ArtifactObj="http://cybox.mitre.org/objects#ArtifactObject-2"

 id="CSON_exe_TT" schema_version="4.1"
 defined_subject="true">

 <maecBundle:Malware_Instance_Object_Attributes>
  <cybox:Description>The Malware is an EXE sample that runs prediefined commands
on the target system</cybox:Description>
 <cybox:Properties
xsi:type="WinExecutableFileObj:WindowsExecutableFileObjectType">
  <FileObj:File_Extension>EXE</FileObj:File_Extension>
<FileObj:Size_In_Bytes>9728</FileObj:Size_In_Bytes>
<FileObj:Hashes>
 <cyboxCommon:Hash>
  <cyboxCommon:Type>MD5</cyboxCommon:Type>

<cyboxCommon:Simple_Hash_Value>f1e5d9bf7705b4dc5be0b8a90b73a863</cyboxCo
mmon:Simple_Hash_Value>
</cyboxCommon:Hash>
</FileObj:Hashes>
</cybox:Properties>
</maecBundle:Malware_Instance_Object_Attributes>

<!-- Placeholder for capabilities -->
<maecBundle:Capabilities>

<maecBundle:Capability id="run_arbitrary_commands" name="command and
control">
<maecBundle:Behavior_Reference behavior_idref="fetch_commands"/>
<maecBundle:Behavior_Reference behavior_idref="execute_commands_recieved"/>
</maecBundle:Capability>
</maecBundle:Capabilities>

<!-- Placeholder for behaviours -->
<maecBundle:Behaviors>
<maecBundle:Behavior id="fetch_commands">
<maecBundle:Action_Composition>
<maecBundle:Action_Reference

```
action_id="fetch_commands_to_execute_from_cnc"/>
    <maecBundle:Action_Reference action_id="decode_commands"/>
   </maecBundle:Action_Composition>
  </maecBundle:Behavior>
  <maecBundle:Behavior id="execute_commands_recieved">

   <maecBundle:Action_Composition>
    <maecBundle:Action_Reference action_id="sleep_specified_time"/>
    <maecBundle:Action_Reference action_id="base64_encode_POST_requests"/>
    <maecBundle:Action_Reference action_id="send_hello_beacon"/>
    <maecBundle:Action_Reference action_id="exit_from_execution"/>
    <maecBundle:Action_Reference action_id="list_processes"/>
    <maecBundle:Action_Reference action_id="download_file"/>
    <maecBundle:Action_Reference action_id="execute_command"/>
    <maecBundle:Action_Reference action_id="execute_xcmd"/>
   </maecBundle:Action_Composition>
 </maecBundle:Behavior>

</maecBundle:Behaviors>

 <!-- Placeholder for actions -->
 <maecBundle:Actions>
  <maecBundle:Action id="fetch_commands_to_execute_from_cnc">
```

<cybox:Name xsi:type="maecVocabs:HTTPActionNameVocab-1.0">send http get request</cybox:Name>
<cybox:Associated_Objects>
<cybox:Associated_Object id="cnc_url">
<cybox:Properties xsi:type="HTTPSessionObj:HTTPSessionObjectType">
<HTTPSessionObj:HTTP_Request_Response>
<HTTPSessionObj:HTTP_Client_Request>
<HTTPSessionObj:HTTP_Request_Line>
<HTTPSessionObj:HTTP_Method>GET</HTTPSessionObj:HTTP_Method>

<HTTPSessionObj:Value>70.62.232.98/Default.aspx?INDEX=10_aplhanumeric_chars</HTTPSessionObj:Value>
</HTTPSessionObj:HTTP_Request_Line>
<HTTPSessionObj:HTTP_Message_Body>
<HTTPSessionObj:Message_Body condition="Contains">Base64_encoded_command</HTTPSessionObj:Message_Body>
</HTTPSessionObj:HTTP_Message_Body>
</HTTPSessionObj:HTTP_Client_Request>
</HTTPSessionObj:HTTP_Request_Response>
</cybox:Properties>
</cybox:Associated_Object>
</cybox:Associated_Objects>
</maecBundle:Action>

```
 <maecBundle:Action id="decode_commands">
  <cybox:Associated_Objects>
   <cybox:Associated_Object id="base_64_encdode_command">
    <cybox:Properties xsi:type="ArtifactObj:ArtifactObjectType">
     <ArtifactObj:Packaging>
      <ArtifactObj:Encoding algorithm="Base64"/>
     </ArtifactObj:Packaging>

<ArtifactObj:Raw_Artifact>ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmno
pqrstuvwxyz0123456789+/</ArtifactObj:Raw_Artifact>
    </cybox:Properties>
   </cybox:Associated_Object>
  </cybox:Associated_Objects>
 </maecBundle:Action>

 <maecBundle:Action id="sleep_specified_time">
  <cybox:Associated_Objects>
   <cybox:Associated_Object id="sleep_API">
    <cybox:Properties xsi:type="APIObj:APIObjectType">
     <APIObj:Function_Name>Sleep</APIObj:Function_Name>
    </cybox:Properties>
   </cybox:Associated_Object>
```

```
  </cybox:Associated_Objects>
 </maecBundle:Action>
 <maecBundle:Action id="send_hello_beacon">
  <cybox:Description>Get information on processes, service status,
drives</cybox:Description>
  <cybox:Associated_Objects>
   <cybox:Associated_Object id="cnc_url_POST">
    <cybox:Properties xsi:type="HTTPSessionObj:HTTPSessionObjectType">
     <HTTPSessionObj:HTTP_Request_Response>
      <HTTPSessionObj:HTTP_Client_Request>
       <HTTPSessionObj:HTTP_Request_Line>
        <HTTPSessionObj:HTTP_Method>POST</HTTPSessionObj:HTTP_Method>
        <HTTPSessionObj:Value>70.62.232.98</HTTPSessionObj:Value>
       </HTTPSessionObj:HTTP_Request_Line>
       <HTTPSessionObj:HTTP_Message_Body>
        <HTTPSessionObj:Message_Body
condition="Contains">Base64_encoded_hello</HTTPSessionObj:Message_Body>
       </HTTPSessionObj:HTTP_Message_Body>
      </HTTPSessionObj:HTTP_Client_Request>
     </HTTPSessionObj:HTTP_Request_Response>
    </cybox:Properties>
   </cybox:Associated_Object>
  </cybox:Associated_Objects>
```

```
  </maecBundle:Action>
  <maecBundle:Action id="base64_encode_POST_requests">
   <cybox:Associated_Objects>
    <cybox:Associated_Object id="base_64_encdoded_hello">
     <cybox:Properties xsi:type="ArtifactObj:ArtifactObjectType">
      <ArtifactObj:Packaging>
       <ArtifactObj:Encoding algorithm="Base64"/>
      </ArtifactObj:Packaging>

<ArtifactObj:Raw_Artifact>ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmno
pqrstuvwxyz0123456789+/</ArtifactObj:Raw_Artifact>
      <![CDATA[hello]]>
     </cybox:Properties>
    </cybox:Associated_Object>
   </cybox:Associated_Objects>
  </maecBundle:Action>
  <maecBundle:Action id="execute_command">
   <cybox:Associated_Objects>
    <cybox:Associated_Object id="CreateProcess">
     <cybox:Description> CreateProcess is called with 'cmd.exe + command' as
argument</cybox:Description>
     <cybox:Properties xsi:type="APIObj:APIObjectType">
      <APIObj:Function_Name>CreateProcess</APIObj:Function_Name>
```

<APIObj:Platform></APIObj:Platform>

</cybox:Properties>

</cybox:Associated_Object>

</cybox:Associated_Objects>

</maecBundle:Action>

<maecBundle:Action id="download_file">

<cybox:Associated_Objects>

<cybox:Associated_Object id="InternetReadFile">

<cybox:Properties xsi:type="APIObj:APIObjectType">

<APIObj:Function_Name>GetVersion</APIObj:Function_Name>

</cybox:Properties>

</cybox:Associated_Object>

<cybox:Associated_Object id="fwrite">

<cybox:Properties xsi:type="APIObj:APIObjectType">

<APIObj:Function_Name>fwrite</APIObj:Function_Name>

</cybox:Properties>

</cybox:Associated_Object>

</cybox:Associated_Objects>

</maecBundle:Action>

<maecBundle:Action id="exit_from_execution">

<cybox:Description>Jump to end of WinMain</cybox:Description>

</maecBundle:Action>

<maecBundle:Action id="list_processes">

```
  <cybox:Associated_Objects>
   <cybox:Associated_Object id="process_list">
    <cybox:Properties xsi:type="APIObj:APIObjectType">
     <APIObj:Function_Name>CreateToolhelp32Snapshot</APIObj:Function_Name>
    </cybox:Properties>
   </cybox:Associated_Object>
  </cybox:Associated_Objects>
 </maecBundle:Action>
 <maecBundle:Action id="execute_xcmd">
  <cybox:Associated_Objects>
   <cybox:Associated_Object id="CreateProcess_API">
    <cybox:Description> CreateProcess is called with 'xcmd.exe + command' as
argument</cybox:Description>
    <cybox:Properties xsi:type="APIObj:APIObjectType">
     <APIObj:Function_Name>CreateProcess</APIObj:Function_Name>
     <APIObj:Platform></APIObj:Platform>
    </cybox:Properties>
   </cybox:Associated_Object>
  </cybox:Associated_Objects>
 </maecBundle:Action>

</maecBundle:Actions>
```

```
<maecBundle:Candidate_Indicators>
 <!-- Capability CIs -->

 <!-- Behaviour CIs -->
 <maecBundle:Candidate_Indicator id="run_arbitrary_commands_id">
  <maecBundle:Composition operator="AND">

   <maecBundle:Behavior_Reference behavior_idref="fetch_commands"/>
   <maecBundle:Behavior_Reference behavior_idref="execute_commands_recieved"/>


   </maecBundle:Composition>
 </maecBundle:Candidate_Indicator>
 <!-- Action CIs -->
 <maecBundle:Candidate_Indicator id="fetch_commands_id">
  <maecBundle:Composition operator="AND">
   <maecBundle:Action_Reference
action_id="fetch_commands_to_execute_from_cnc"/>
   <maecBundle:Action_Reference action_id="decode_commands"/>
  </maecBundle:Composition>
 </maecBundle:Candidate_Indicator>
 <maecBundle:Candidate_Indicator id="execute_commands_received_id">
  <maecBundle:Composition operator="OR">
```

```
 <maecBundle:Sub_Composition operator="OR">
 <maecBundle:Action_Reference action_id="sleep_specified_time"/>
 <maecBundle:Action_Reference action_id="execute_command"/>
 <maecBundle:Action_Reference action_id="exit_from_execution"/>
 <maecBundle:Action_Reference action_id="list_processes"/>
 <maecBundle:Action_Reference action_id="download_file"/>
 <maecBundle:Action_Reference action_id="execute_command"/>
 <maecBundle:Action_Reference action_id="execute_xcmd"/>
 </maecBundle:Sub_Composition>
 <maecBundle:Sub_Composition operator="AND">
  <maecBundle:Action_Reference action_id="base64_encode_POST_requests"/>
  <maecBundle:Action_Reference action_id="send_hello_beacon"/>
 </maecBundle:Sub_Composition>
</maecBundle:Composition>
</maecBundle:Candidate_Indicator>
<!-- Object CIs -->
<maecBundle:Candidate_Indicator id="download_file_id">
 <maecBundle:Composition operator="AND">
  <maecBundle:Object_Reference object_idref="InternetReadFile"/>
  <maecBundle:Object_Reference object_idref="fwrite"/>
 </maecBundle:Composition>
</maecBundle:Candidate_Indicator>
```

</maecBundle:Candidate_Indicators>

</maecBundle:MAEC_Bundle>

A.5 Glooxmail

<?xml version="1.0" encoding="UTF-8"?>

<maecBundle:MAEC_Bundle xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"

xsi:schemaLocation="http://cybox.mitre.org/objects#ArtifactObject-2
maec/maec_4.1_offline/cybox_2.1_offline/objects/Artifact_Object.xsd
http://cybox.mitre.org/objects#WinRegistryKeyObject-2
maec/maec_4.1_offline/cybox_2.1_offline/objects/Win_Registry_Key_Object.xsd
http://cybox.mitre.org/objects#WinExecutableFileObject-2
maec/maec_4.1_offline/cybox_2.1_offline/objects/Win_Executable_File_Object.xsd
http://cybox.mitre.org/common-2
maec/maec_4.1_offline/cybox_2.1_offline/objects/cybox_common.xsd
http://cybox.mitre.org/objects#APIObject-2
maec/maec_4.1_offline/cybox_2.1_offline/objects/API_Object.xsd
http://maec.mitre.org/XMLSchema/maec-bundle-4
maec/maec_4.1_offline/maec_bundle_schema.xsd
http://cybox.mitre.org/objects#WinExecutableFileObject-2
maec/maec_4.1_offline/cybox_2.1_offline/objects/Win_Executable_File_Object.xsd

http://cybox.mitre.org/objects#PDFFileObject-1

maec/maec_4.1_offline/cybox_2.1_offline/objects/PDF_File_Object.xsd

http://cybox.mitre.org/objects#APIObject-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/API_Object.xsd

http://cybox.mitre.org/objects#WinExecutableFileObject-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/Win_Executable_File_Object.xsd

http://cybox.mitre.org/default_vocabularies-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/cybox_default_vocabularies.xsd

http://cybox.mitre.org/objects#PDFFileObject-1

maec/maec_4.1_offline/cybox_2.1_offline/objects/PDF_File_Object.xsd

http://cybox.mitre.org/objects#WinRegistryKeyObject-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/Win_Registry_key_Object.xsd

http://cybox.mitre.org/objects#WinMutexObject-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/Win_Mutex_Object.xsd

http://cybox.mitre.org/objects#ArtifactObject-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/Artifact_Object.xsd

http://cybox.mitre.org/objects#EmailMessageObject-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/Email_Message_Object.xsd

http://cybox.mitre.org/objects#MutexObject-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/Mutex_Object.xsd

http://cybox.mitre.org/objects#PipeObject-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/Pipe_Object.xsd

http://cybox.mitre.org/objects#HTTPSessionObject-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/DNS_Query_Object.xsd

http://cybox.mitre.org/objects#UserAccountObject-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/User_Account_Object.xsd

"

xmlns:HTTPSessionObj="http://cybox.mitre.org/objects#HTTPSessionObject-2"

xmlns:DNSQueryObj="http://cybox.mitre.org/objects#DNSQueryObject-2"

xmlns:maecBundle="http://maec.mitre.org/XMLSchema/maec-bundle-4"

xmlns:ProcessObj="http://cybox.mitre.org/objects#ProcessObject-2"

xmlns:SocketAddressObj="http://cybox.mitre.org/objects#SocketAddressObject-1"

xmlns:AddressObj="http://cybox.mitre.org/objects#AddressObject-2"

xmlns:NetworkConnectionObj="http://cybox.mitre.org/objects#NetworkConnectionObje

ct-2"

xmlns:PDFFileObj="http://cybox.mitre.org/objects#PDFFileObject-1"

xmlns:cyboxVocabs="http://cybox.mitre.org/default_vocabularies-2"

xmlns:HostnameObj="http://cybox.mitre.org/objects#HostnameObject-1"

xmlns:CodeObj="http://cybox.mitre.org/objects#CodeObject-2"

xmlns:FileObj="http://cybox.mitre.org/objects#FileObject-2"

xmlns:DNSRecordObj="http://cybox.mitre.org/objects#DNSRecordObject-2"

xmlns:WinRegistryKeyObj="http://cybox.mitre.org/objects#WinRegistryKeyObject-2"

xmlns:maecVocabs="http://maec.mitre.org/default_vocabularies-1"

xmlns:APIObj="http://cybox.mitre.org/objects#APIObject-2"

xmlns:WinExecutableFileObj="http://cybox.mitre.org/objects#WinExecutableFileObject
-2"
xmlns:cyboxCommon="http://cybox.mitre.org/common-2"
xmlns:URIObj="http://cybox.mitre.org/objects#URIObject-2"
xmlns:cybox="http://cybox.mitre.org/cybox-2"
xmlns:WinMutexObj="http://cybox.mitre.org/objects#WinMutexObject-2"
xmlns:ArtifactObj="http://cybox.mitre.org/objects#ArtifactObject-2"
xmlns:EmailMessageObj="http://cybox.mitre.org/objects#EmailMessageObject-2"
xmlns:MutexObj="http://cybox.mitre.org/objects#MutexObject-2"
xmlns:PipeObj="http://cybox.mitre.org/objects#PipeObject-2"
xmlns:UserAccountObj="http://cybox.mitre.org/objects#UserAccountObject-2"
id="Glooxmail_exe_TT" schema_version="4.1"
defined_subject="true">

<maecBundle:Malware_Instance_Object_Attributes>
<cybox:Description>The Malware is a functionality rich exe sample that perofrms a
variety of information stealing acitvities</cybox:Description>
<cybox:Properties
xsi:type="WinExecutableFileObj:WindowsExecutableFileObjectType">
<FileObj:File_Extension>EXE</FileObj:File_Extension>
<FileObj:Size_In_Bytes>353792</FileObj:Size_In_Bytes>
<FileObj:Hashes>
<cyboxCommon:Hash>

<cyboxCommon:Type>MD5</cyboxCommon:Type>

<cyboxCommon:Simple_Hash_Value>3de1bd0f2107198931177b2b23877df4</cyboxCommon:Simple_Hash_Value>

</cyboxCommon:Hash>

</FileObj:Hashes>

</cybox:Properties>

</maecBundle:Malware_Instance_Object_Attributes>

<!-- Placeholder for capabilities -->

<maecBundle:Capabilities>

<maecBundle:Capability id="run_arbitrary_commands">

<maecBundle:Behavior_Reference behavior_idref="get_cnc_host_to_use"/>

<maecBundle:Behavior_Reference behavior_idref="fetch_commands"/>

<maecBundle:Behavior_Reference behavior_idref="execute_commands_received"/>

</maecBundle:Capability>

</maecBundle:Capabilities>

<!-- Placeholder for behaviours -->

<maecBundle:Behaviors>

<maecBundle:Behavior id="get_cnc_host_to_use">
<maecBundle:Action_Composition>
<maecBundle:Action_Reference
action_id="use_gloox_to_query_gmail_dns_servers"/>
</maecBundle:Action_Composition>
</maecBundle:Behavior>
<maecBundle:Behavior id="fetch_commands">
<maecBundle:Action_Composition>
<maecBundle:Action_Reference
action_id="fetch_commands_to_execute_from_cnc"/>
</maecBundle:Action_Composition>
</maecBundle:Behavior>
<maecBundle:Behavior id="execute_misc_commands_received">
<maecBundle:Action_Composition>
<maecBundle:Action_Reference action_id="start_process"/>
<maecBundle:Action_Reference action_id="list_processes"/>
<maecBundle:Action_Reference action_id="terminate_process"/>
<maecBundle:Action_Reference action_id="download_file"/>
<maecBundle:Action_Reference action_id="upload_file"/>
<maecBundle:Action_Reference action_id="get_drive_info"/>
<maecBundle:Action_Reference action_id="get_directory_list"/>
<maecBundle:Action_Reference action_id="open_remote_shell"/>
<maecBundle:Action_Reference action_id="sleep_specified_time"/>

```
  </maecBundle:Action_Composition>
 </maecBundle:Behavior>

</maecBundle:Behaviors>

 <!-- Placeholder for actions -->
<maecBundle:Actions>
 <maecBundle:Action id="use_gloox_to_query_gmail_dns_servers">
  <cybox:Associated_Objects>
   <cybox:Associated_Object id="dns_server">
    <cybox:Properties xsi:type="DNSQueryObj:DNSQueryObjectType">
     <DNSQueryObj:Question>
      <DNSQueryObj:QName>alt1/2/3/4.xmpp.google.com</DNSQueryObj:QName>
     </DNSQueryObj:Question>
    </cybox:Properties>
   </cybox:Associated_Object>
   <cybox:Associated_Object id="gmail_credentials">
    <cybox:Properties xsi:type="UserAccountObj:UserAccountObjectType">

<UserAccountObj:Username>gale.rosside@gmail.com/16897168</UserAccountObj:Use
rname>
    </cybox:Properties>
   </cybox:Associated_Object>
```

```
 </cybox:Associated_Objects>
</maecBundle:Action>
<maecBundle:Action id="fetch_commands_to_execute_from_cnc">
 <cybox:Description>CnC unknown at the time of analysis. The communication is
HTTPS by default</cybox:Description>
</maecBundle:Action>
<maecBundle:Action id="start_process">
 <cybox:Associated_Objects>
  <cybox:Associated_Object id="CreateProcess_API">
   <cybox:Properties xsi:type="APIObj:APIObjectType">
    <APIObj:Function_Name>CreateProcess</APIObj:Function_Name>
   </cybox:Properties>
  </cybox:Associated_Object>
 </cybox:Associated_Objects>
</maecBundle:Action>
<maecBundle:Action id="list_processes">
 <cybox:Associated_Objects>
  <cybox:Associated_Object id="process_list">
   <cybox:Properties xsi:type="APIObj:APIObjectType">
    <APIObj:Function_Name>CreateToolhelp32Snapshot</APIObj:Function_Name>
   </cybox:Properties>
  </cybox:Associated_Object>
 </cybox:Associated_Objects>
```

```
</maecBundle:Action>
<maecBundle:Action id="terminate_process">
 <cybox:Associated_Objects>
  <cybox:Associated_Object id="TerminateProcess">
   <cybox:Properties xsi:type="APIObj:APIObjectType">
    <APIObj:Function_Name>TerminateProcess</APIObj:Function_Name>
   </cybox:Properties>
  </cybox:Associated_Object>
 </cybox:Associated_Objects>
</maecBundle:Action>
<maecBundle:Action id="download_file">
 <cybox:Associated_Objects>
  <cybox:Associated_Object id="InternetReadFile">
   <cybox:Properties xsi:type="APIObj:APIObjectType">
    <APIObj:Function_Name>InternetReadFile</APIObj:Function_Name>
   </cybox:Properties>
  </cybox:Associated_Object>
  <cybox:Associated_Object id="WriteFile">
   <cybox:Properties xsi:type="APIObj:APIObjectType">
    <APIObj:Function_Name>WriteFile</APIObj:Function_Name>
   </cybox:Properties>
  </cybox:Associated_Object>
 </cybox:Associated_Objects>
```

```
</maecBundle:Action>
<maecBundle:Action id="upload_file">
 <cybox:Associated_Objects>
  <cybox:Associated_Object id="ReadFile">
   <cybox:Properties xsi:type="APIObj:APIObjectType">
    <APIObj:Function_Name>ReadFile</APIObj:Function_Name>
   </cybox:Properties>
  </cybox:Associated_Object>
  <cybox:Associated_Object id="InternetWriteFile"></cybox:Associated_Object>
 </cybox:Associated_Objects>
</maecBundle:Action>
<maecBundle:Action id="get_drive_info">
 <cybox:Associated_Objects>
  <cybox:Associated_Object>
   <cybox:Properties xsi:type="APIObj:APIObjectType">
    <APIObj:Function_Name>GetDriveTypeA</APIObj:Function_Name>
   </cybox:Properties>
  </cybox:Associated_Object>
 </cybox:Associated_Objects>
</maecBundle:Action>
<maecBundle:Action id="get_directory_list">
 <cybox:Associated_Objects>
  <cybox:Associated_Object>
```

<cybox:Properties xsi:type="APIObj:APIObjectType">

<APIObj:Function_Name>FindFirstFileA</APIObj:Function_Name>

</cybox:Properties>

</cybox:Associated_Object>

</cybox:Associated_Objects>

</maecBundle:Action>

<maecBundle:Action id="open_remote_shell">

<cybox:Associated_Objects>

<cybox:Associated_Object id="cmd_file">

<cybox:Properties xsi:type="FileObj:FileObjectType">

<FileObj:File_Name>cmd.exe</FileObj:File_Name>

</cybox:Properties>

</cybox:Associated_Object>

<cybox:Associated_Object id="input_pipe">

<cybox:Description>Pipe that acts as source of commancds to cmd. The other end of the pipe is an HTTP session with the CnC server.</cybox:Description>

<cybox:Properties xsi:type="PipeObj:PipeObjectType">

<PipeObj:Name/>

</cybox:Properties>

</cybox:Associated_Object>

<cybox:Associated_Object id="output_pipe">

<cybox:Description>Pipe that acts as source of output of commands from cmd. The other end of the pipe is an HTTP session with the CnC server.</cybox:Description>

```
   <cybox:Properties xsi:type="PipeObj:PipeObjectType">
    <PipeObj:Name/>
   </cybox:Properties>
  </cybox:Associated_Object>
 </cybox:Associated_Objects>
</maecBundle:Action>
<maecBundle:Action id="sleep_specified_time">
 <cybox:Associated_Objects>
  <cybox:Associated_Object id="sleep_API">
   <cybox:Properties xsi:type="APIObj:APIObjectType">
    <APIObj:Function_Name>Sleep</APIObj:Function_Name>
   </cybox:Properties>
  </cybox:Associated_Object>
 </cybox:Associated_Objects>
</maecBundle:Action>

</maecBundle:Actions>

<maecBundle:Candidate_Indicators>
 <!-- Capability CIs -->

 <!-- Behaviour CIs -->
 <maecBundle:Candidate_Indicator id="run_arbitrary_commands_id">
```

```
 <maecBundle:Composition operator="AND">
  <maecBundle:Behavior_Reference behavior_idref="get_cnc_host_to_use"/>
  <maecBundle:Behavior_Reference behavior_idref="fetch_commands"/>
  <maecBundle:Behavior_Reference behavior_idref="execute_commands_received"/>
 </maecBundle:Composition>
</maecBundle:Candidate_Indicator>
<!-- Action CIs -->
<maecBundle:Candidate_Indicator id="execute_commands_received_id">
 <maecBundle:Composition operator="OR">
  <maecBundle:Sub_Composition operator="OR">
   <maecBundle:Action_Reference action_id="start_process"/>
   <maecBundle:Action_Reference action_id="list_processes"/>
   <maecBundle:Action_Reference action_id="terminate_process"/>
   <maecBundle:Action_Reference action_id="download_file"/>
   <maecBundle:Action_Reference action_id="upload_file"/>
   <maecBundle:Action_Reference action_id="open_remote_shell"/>
   <maecBundle:Action_Reference action_id="sleep_specified_time"/>
  </maecBundle:Sub_Composition>
  <maecBundle:Sub_Composition operator="AND">
   <maecBundle:Action_Reference action_id="get_drive_info"/>
   <maecBundle:Action_Reference action_id="get_directory_list"/>
  </maecBundle:Sub_Composition>
 </maecBundle:Composition>
```

```
</maecBundle:Candidate_Indicator>
<!-- Object CIs -->
<maecBundle:Candidate_Indicator id="use_gloox_to_query_gmail_dns_servers_id">
 <maecBundle:Composition operator="AND">
  <maecBundle:Object_Reference object_idref="dns_server"/>
  <maecBundle:Object_Reference object_idref="gmail_credentials"/>
 </maecBundle:Composition>
</maecBundle:Candidate_Indicator>
<maecBundle:Candidate_Indicator id="download_file_id">
 <maecBundle:Composition operator="AND">
  <maecBundle:Object_Reference object_idref="InternetReadFile"/>
  <maecBundle:Object_Reference object_idref="WriteFile"/>
 </maecBundle:Composition>
</maecBundle:Candidate_Indicator>
<maecBundle:Candidate_Indicator id="upload_file_id">
 <maecBundle:Composition operator="AND">
  <maecBundle:Object_Reference object_idref="ReadFile"/>
  <maecBundle:Object_Reference object_idref="InternetWriteFile"/>
 </maecBundle:Composition>
</maecBundle:Candidate_Indicator>
<maecBundle:Candidate_Indicator id="open_remote_shell_id">
 <maecBundle:Composition operator="AND">
  <maecBundle:Object_Reference object_idref="cmd_file"/>
```

<maecBundle:Object_Reference object_idref="input_pipe"/>

<maecBundle:Object_Reference object_idref="output_pipe"/>

</maecBundle:Composition>

</maecBundle:Candidate_Indicator>

</maecBundle:Candidate_Indicators>

</maecBundle:MAEC_Bundle>

A.6 WebC2-Greencat

<?xml version="1.0" encoding="UTF-8"?>

<maecBundle:MAEC_Bundle xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"

xsi:schemaLocation="http://cybox.mitre.org/objects#ArtifactObject-2

../cybox_2.1_offline/objects/Artifact_Object.xsd

http://cybox.mitre.org/objects#WinRegistryKeyObject-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/Win_Registry_Key_Object.xsd

http://cybox.mitre.org/objects#WinExecutableFileObject-2

../cybox_2.1_offline/objects/Win_Executable_File_Object.xsd

http://cybox.mitre.org/common-2

../maec/maec_4.1_offline/cybox_2.1_offline/cybox_common.xsd

http://cybox.mitre.org/objects#APIObject-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/API_Object.xsd

http://maec.mitre.org/XMLSchema/maec-bundle-4

file:/Users/asheer.malhotra/Documents/TT/maec/maec_4.1_offline/maec_bundle_schema

.xsd http://cybox.mitre.org/objects#WinExecutableFileObject-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/Win_Executable_File_Object.xsd

http://cybox.mitre.org/objects#PDFFileObject-1

maec/maec_4.1_offline/cybox_2.1_offline/objects/PDF_File_Object.xsd

http://cybox.mitre.org/objects#APIObject-2

../maec/maec_4.1_offline/cybox_2.1_offline/objects/API_Object.xsd

http://cybox.mitre.org/objects#WinExecutableFileObject-2

../maec/maec_4.1_offline/cybox_2.1_offline/objects/Win_Executable_File_Object.xsd

http://cybox.mitre.org/default_vocabularies-2

../cybox_2.1_offline/cybox_default_vocabularies.xsd

http://cybox.mitre.org/objects#PDFFileObject-1

../cybox_2.1_offline/PDF_File_Object.xsd

http://cybox.mitre.org/objects#WinRegistryKeyObject-2

../cybox_2.1_offline/Win_Registry_key_Object.xsd

http://cybox.mitre.org/objects#WinMutexObject-2

./cybox_2.1_offline/Win_Mutex_Object.xsd

"

xmlns:HTTPSessionObj="http://cybox.mitre.org/objects#HTTPSessionObject-2"

xmlns:DNSQueryObj="http://cybox.mitre.org/objects#DNSQueryObject-2"

xmlns:maecBundle="http://maec.mitre.org/XMLSchema/maec-bundle-4"

xmlns:ProcessObj="http://cybox.mitre.org/objects#ProcessObject-2"

xmlns:SocketAddressObj="http://cybox.mitre.org/objects#SocketAddressObject-1"

xmlns:AddressObj="http://cybox.mitre.org/objects#AddressObject-2"

xmlns:NetworkConnectionObj="http://cybox.mitre.org/objects#NetworkConnectionObje
ct-2"

xmlns:PDFFileObj="http://cybox.mitre.org/objects#PDFFileObject-1"

xmlns:cyboxVocabs="http://cybox.mitre.org/default_vocabularies-2"

xmlns:HostnameObj="http://cybox.mitre.org/objects#HostnameObject-1"

xmlns:CodeObj="http://cybox.mitre.org/objects#CodeObject-2"

xmlns:FileObj="http://cybox.mitre.org/objects#FileObject-2"

xmlns:DNSRecordObj="http://cybox.mitre.org/objects#DNSRecordObject-2"

xmlns:WinRegistryKeyObj="http://cybox.mitre.org/objects#WinRegistryKeyObject-2"

xmlns:maecVocabs="http://maec.mitre.org/default_vocabularies-1"

xmlns:APIObj="http://cybox.mitre.org/objects#APIObject-2"

xmlns:WinExecutableFileObj="http://cybox.mitre.org/objects#WinExecutableFileObject
-2"

xmlns:cyboxCommon="http://cybox.mitre.org/common-2"

xmlns:URIObj="http://cybox.mitre.org/objects#URIObject-2"

xmlns:cybox="http://cybox.mitre.org/cybox-2"

xmlns:WinMutexObj="http://cybox.mitre.org/objects#WinMutexObject-2"

id="Greencat_exe_TT" schema_version="4.1"

defined_subject="true">

<maecBundle:Malware_Instance_Object_Attributes>

<cybox:Description>The Malware is an EXE sample that runs prediefined commands on the target system</cybox:Description>

<cybox:Properties xsi:type="WinExecutableFileObj:WindowsExecutableFileObjectType">

<FileObj:File_Extension>EXE</FileObj:File_Extension>

<FileObj:Size_In_Bytes>17408</FileObj:Size_In_Bytes>

<FileObj:Hashes>

<cyboxCommon:Hash>

<cyboxCommon:Type>MD5</cyboxCommon:Type>

<cyboxCommon:Simple_Hash_Value>ba0c4d3dbf07d407211b5828405a9b91</cyboxCommon:Simple_Hash_Value>

</cyboxCommon:Hash>

</FileObj:Hashes>

</cybox:Properties>

</maecBundle:Malware_Instance_Object_Attributes>

<!-- Placeholder for capabilities -->

<maecBundle:Capabilities>

<maecBundle:Capability id="persistence" name="persistence">

<maecBundle:Behavior_Reference behavior_idref="establish_runtime_persistence"/>

<maecBundle:Behavior_Reference behavior_idref="establish_persistence_across_reboots"/>

</maecBundle:Capability>

<maecBundle:Capability id="run_arbitrary_commands" name="command and control">

<maecBundle:Behavior_Reference behavior_idref="fetch_commands"/>

<maecBundle:Behavior_Reference behavior_idref="execute_commands_recieved"/>

</maecBundle:Capability>

</maecBundle:Capabilities>

<!-- Placeholder for behaviours -->

<maecBundle:Behaviors>

<maecBundle:Behavior id="establish_runtime_persistence">

<maecBundle:Action_Composition>

<maecBundle:Action_Reference action_id="create_mutex"/>

</maecBundle:Action_Composition>

</maecBundle:Behavior>

<maecBundle:Behavior id="establish_persistence_across_reboots">

<maecBundle:Action_Reference action_id="drop_file_to_dir"/>

<maecBundle:Action_Reference action_id="modify_registry"/>

</maecBundle:Behavior>

<maecBundle:Behavior id="fetch_commands">

<maecBundle:Action_Composition>

<maecBundle:Action_Reference action_id="decode_url"/>

<maecBundle:Action_Reference

action_id="fetch_commands_to_execute_from_cnc"/>

</maecBundle:Action_Composition>

</maecBundle:Behavior>

<maecBundle:Behavior id="execute_commands_recieved">

<maecBundle:Action_Composition>

<maecBundle:Action_Reference action_id="sleep_specified_time"/>

<maecBundle:Action_Reference action_id="get_process_list"/>

<maecBundle:Action_Reference action_id="get_service_status"/>

<maecBundle:Action_Reference action_id="get_drive_type"/>

<maecBundle:Action_Reference action_id="get_volume_name"/>

<maecBundle:Action_Reference action_id="execute_command"/>

<maecBundle:Action_Reference action_id="stop_service"/>

<maecBundle:Action_Reference action_id="download_file"/>

<maecBundle:Action_Reference action_id="start_process"/>

<maecBundle:Action_Reference action_id="start_service"/>

<maecBundle:Action_Reference action_id="terminate_process"/>

<maecBundle:Action_Reference action_id="restart_cmd_shell"/>

<maecBundle:Action_Reference
action_id="create_process_custom_security_priveleges"/>

<maecBundle:Action_Reference action_id="uninstall_malware"/>

</maecBundle:Action_Composition>

</maecBundle:Behavior>

</maecBundle:Behaviors>

<!-- Placeholder for actions -->

<maecBundle:Actions>

<maecBundle:Action id="create_mutex">

<cybox:Name xsi:type="maecVocabs:SynchronizationActionNameVocab-1.0">create
mutex</cybox:Name>

<cybox:Associated_Objects>

<cybox:Associated_Object>

<cybox:Properties xsi:type="WinMutexObj:WindowsMutexObjectType"
named="true">

<MutexObj:Name>ADR32</MutexObj:Name>

</cybox:Properties>

```
    </cybox:Associated_Object>
   </cybox:Associated_Objects>
  </maecBundle:Action>
  <maecBundle:Action id="drop_file_to_dir">
   <cybox:Name xsi:type="maecVocabs:FileActionNameVocab-1.1">create
file</cybox:Name>
   <cybox:Associated_Objects>
    <cybox:Associated_Object>
     <cybox:Description> the malware creates a copy of itself in the
directory</cybox:Description>
     <cybox:Properties
xsi:type="WinExecutableFileObj:WindowsExecutableFileObjectType">
      <FileObj:File_Name>reader_sl.exe</FileObj:File_Name>
      <FileObj:File_Path>user_profile_directory\Application
Data\Adobe\</FileObj:File_Path>
      <FileObj:File_Extension>exe</FileObj:File_Extension>
      <FileObj:Size_In_Bytes>17408</FileObj:Size_In_Bytes>
     </cybox:Properties>
    </cybox:Associated_Object>
   </cybox:Associated_Objects>
  </maecBundle:Action>
  <maecBundle:Action id="modify_registry">
   <cybox:Name xsi:type="maecVocabs:RegistryActionNameVocab-1.0">create registry
```

key</cybox:Name>
<cybox:Associated_Objects>
<cybox:Associated_Object>
<cybox:Properties xsi:type="WinRegistryKeyObj:WindowsRegistryKeyObjectType">

<WinRegistryKeyObj:Key>\Software\Microsoft\Windows\CurrentVersion\Run</WinRegistryKeyObj:Key>
<WinRegistryKeyObj:Hive>HKCU</WinRegistryKeyObj:Hive>
<WinRegistryKeyObj:Values>
<WinRegistryKeyObj:Value>
<WinRegistryKeyObj:Name>Adobe Reader Speed Launcher</WinRegistryKeyObj:Name>
<WinRegistryKeyObj:Data>user_profile_directory\Application Data\Adobe\sl_reader.exe</WinRegistryKeyObj:Data>
</WinRegistryKeyObj:Value>
</WinRegistryKeyObj:Values>

</cybox:Properties>
</cybox:Associated_Object>
</cybox:Associated_Objects>
</maecBundle:Action>
<maecBundle:Action id="decode_url">
<cybox:Associated_Objects>

<cybox:Associated_Object id="encoded_url">
<cybox:Properties xsi:type="URIObj:URIObjectType">
<URIObj:Value>-FFat^^eee\µ+-+-|-S-\||+^|-+-^</URIObj:Value>
</cybox:Properties>
<cybox:Association_Type
xsi:type="cyboxVocabs:ActionObjectAssociationTypeVocab-
1.0">utlized</cybox:Association_Type>
</cybox:Associated_Object>
<cybox:Associated_Object id="decoded_url">
<cybox:Properties xsi:type="URIObj:URIObjectType">
<URIObj:Value>http://smilecare.com/file/</URIObj:Value>
</cybox:Properties>
<cybox:Association_Type
xsi:type="cyboxVocabs:ActionObjectAssociationTypeVocab-
1.0">returned</cybox:Association_Type>
</cybox:Associated_Object>
</cybox:Associated_Objects>
</maecBundle:Action>
<maecBundle:Action id="fetch_commands_to_execute_from_cnc">
<cybox:Name xsi:type="maecVocabs:HTTPActionNameVocab-1.0">send http get
request</cybox:Name>
<cybox:Associated_Objects>
<cybox:Associated_Object id="cnc_url">

<cybox:Properties xsi:type="HTTPSessionObj:HTTPSessionObjectType">

<HTTPSessionObj:HTTP_Request_Response>

<HTTPSessionObj:HTTP_Client_Request>

<HTTPSessionObj:HTTP_Request_Line>

<HTTPSessionObj:HTTP_Method>GET</HTTPSessionObj:HTTP_Method>

<HTTPSessionObj:Value>http://smilecare.com/file/</HTTPSessionObj:Value>

</HTTPSessionObj:HTTP_Request_Line>

<HTTPSessionObj:HTTP_Message_Body>

<HTTPSessionObj:Message_Body condition="Contains"> <![CDATA[<!--<img

..... />]]></HTTPSessionObj:Message_Body>

</HTTPSessionObj:HTTP_Message_Body>

</HTTPSessionObj:HTTP_Client_Request>

</HTTPSessionObj:HTTP_Request_Response>

</cybox:Properties>

</cybox:Associated_Object>

</cybox:Associated_Objects>

</maecBundle:Action>

<maecBundle:Action id="sleep_specified_time">

<cybox:Associated_Objects>

<cybox:Associated_Object id="sleep_API">

<cybox:Properties xsi:type="APIObj:APIObjectType">

<APIObj:Function_Name>Sleep</APIObj:Function_Name>

```
    </cybox:Properties>
   </cybox:Associated_Object>
  </cybox:Associated_Objects>

 </maecBundle:Action>
 <maecBundle:Action id="get_process_list">
<cybox:Description>Get information on processes, service status,
drives</cybox:Description>
  <cybox:Associated_Objects>
   <cybox:Associated_Object id="process_list">
    <cybox:Properties xsi:type="APIObj:APIObjectType">
     <APIObj:Function_Name>CreateToolhelp32Snapshot</APIObj:Function_Name>
    </cybox:Properties>
   </cybox:Associated_Object>
  </cybox:Associated_Objects>
 </maecBundle:Action>
 <maecBundle:Action id="get_service_status">
  <cybox:Associated_Objects>
   <cybox:Associated_Object id="service_status">
    <cybox:Properties xsi:type="APIObj:APIObjectType">
     <APIObj:Function_Name>EnumServicesStatusExA</APIObj:Function_Name>
    </cybox:Properties>
   </cybox:Associated_Object>
```

```
 </cybox:Associated_Objects>
</maecBundle:Action>
<maecBundle:Action id="get_drive_type">
 <cybox:Associated_Objects>
 <cybox:Associated_Object id="drive_type">
   <cybox:Properties xsi:type="APIObj:APIObjectType">
    <APIObj:Function_Name>GetDriveTypeA</APIObj:Function_Name>
   </cybox:Properties>
  </cybox:Associated_Object>
 </cybox:Associated_Objects>
</maecBundle:Action>
<maecBundle:Action id="get_volume_name">
 <cybox:Associated_Objects>
 <cybox:Associated_Object id="volume_name">
   <cybox:Properties xsi:type="APIObj:APIObjectType">
    <APIObj:Function_Name>GetVolumeInformationA</APIObj:Function_Name>
   </cybox:Properties>
  </cybox:Associated_Object>
 </cybox:Associated_Objects>
</maecBundle:Action>

<maecBundle:Action id="execute_command">
 <cybox:Associated_Objects>
```

<cybox:Associated_Object id="CreateProcess">

<cybox:Description> CreateProcess is called with 'cmd.exe + command' as argument</cybox:Description>

<cybox:Properties xsi:type="APIObj:APIObjectType">

<APIObj:Function_Name>CreateProcess</APIObj:Function_Name>

<APIObj:Platform></APIObj:Platform>

</cybox:Properties>

</cybox:Associated_Object>

</cybox:Associated_Objects>

</maecBundle:Action>

<maecBundle:Action id="stop_service">

<cybox:Associated_Objects>

<cybox:Associated_Object id="TerminateProcess">

<cybox:Properties xsi:type="APIObj:APIObjectType">

<APIObj:Function_Name>TerminateProcess</APIObj:Function_Name>

</cybox:Properties>

</cybox:Associated_Object>

<cybox:Associated_Object id="ControlService">

<cybox:Properties xsi:type="APIObj:APIObjectType">

<APIObj:Function_Name>ControlService</APIObj:Function_Name>

</cybox:Properties>

</cybox:Associated_Object>

```
 </cybox:Associated_Objects>
</maecBundle:Action>
<maecBundle:Action id="download_file">
 <cybox:Associated_Objects>
  <cybox:Associated_Object id="InternetReadFile">
   <cybox:Properties xsi:type="APIObj:APIObjectType">
    <APIObj:Function_Name>InternetReadFile</APIObj:Function_Name>
   </cybox:Properties>
  </cybox:Associated_Object>
  <cybox:Associated_Object id="WriteFile">
   <cybox:Properties xsi:type="APIObj:APIObjectType">
    <APIObj:Function_Name>WriteFile</APIObj:Function_Name>
   </cybox:Properties>
  </cybox:Associated_Object>
 </cybox:Associated_Objects>
</maecBundle:Action>
<maecBundle:Action id="start_process">
 <cybox:Associated_Objects>
  <cybox:Associated_Object id="CreateProcess_API">
   <cybox:Properties xsi:type="APIObj:APIObjectType">
    <APIObj:Function_Name>CreateProcess</APIObj:Function_Name>
   </cybox:Properties>
  </cybox:Associated_Object>
```

```
 </cybox:Associated_Objects>
</maecBundle:Action>
<maecBundle:Action id="start_service">
 <cybox:Associated_Objects>
  <cybox:Associated_Object id="StartService">
   <cybox:Properties xsi:type="APIObj:APIObjectType">
    <APIObj:Function_Name>StartServiceA</APIObj:Function_Name>
   </cybox:Properties>
  </cybox:Associated_Object>
 </cybox:Associated_Objects>
</maecBundle:Action>
<maecBundle:Action id="terminate_process">
 <cybox:Associated_Objects>
  <cybox:Associated_Object id="TerminateProcess">
   <cybox:Properties xsi:type="APIObj:APIObjectType">
    <APIObj:Function_Name>TerminateProcess</APIObj:Function_Name>
   </cybox:Properties>
  </cybox:Associated_Object>
 </cybox:Associated_Objects>
</maecBundle:Action>
<maecBundle:Action id="restart_cmd_shell">
 <cybox:Associated_Objects>
  <cybox:Associated_Object id="GetExitCodeProcess">
```

<cybox:Properties xsi:type="APIObj:APIObjectType">
<APIObj:Function_Name>GetExitCodeProcess</APIObj:Function_Name>
</cybox:Properties>
</cybox:Associated_Object>
<cybox:Associated_Object id="CreateProcess_API_1">
<cybox:Properties xsi:type="APIObj:APIObjectType">
<APIObj:Function_Name>CreateProcess</APIObj:Function_Name>
</cybox:Properties>
</cybox:Associated_Object>
</cybox:Associated_Objects>
</maecBundle:Action>
<maecBundle:Action id="create_process_custom_security_priveleges">
<cybox:Associated_Objects>
<cybox:Associated_Object id="CreateProcessAsUser">
<cybox:Properties xsi:type="APIObj:APIObjectType">
<APIObj:Function_Name>CreateProcessAsUser</APIObj:Function_Name>
</cybox:Properties>
</cybox:Associated_Object>
</cybox:Associated_Objects>
</maecBundle:Action>
<maecBundle:Action id="uninstall_malware">
<cybox:Name xsi:type="maecVocabs:RegistryActionNameVocab-1.0">delete registry key</cybox:Name>

```
  <cybox:Associated_Objects>
   <cybox:Associated_Object>
    <cybox:Properties
xsi:type="WinRegistryKeyObj:WindowsRegistryKeyObjectType">

<WinRegistryKeyObj:Key>\Software\Microsoft\Windows\CurrentVersion\Run</WinRe
gistryKeyObj:Key>
     <WinRegistryKeyObj:Hive>HKCU</WinRegistryKeyObj:Hive>
     <WinRegistryKeyObj:Values>
      <WinRegistryKeyObj:Value>
       <WinRegistryKeyObj:Name>Adobe Reader Speed
Launcher</WinRegistryKeyObj:Name>
       <WinRegistryKeyObj:Data>user_profile_directory\Application
Data\Adobe\sl_reader.exe</WinRegistryKeyObj:Data>
      </WinRegistryKeyObj:Value>
     </WinRegistryKeyObj:Values>

    </cybox:Properties>
   </cybox:Associated_Object>
  </cybox:Associated_Objects>
 </maecBundle:Action>

</maecBundle:Actions>
```

```
<maecBundle:Candidate_Indicators>
 <!-- Capability CIs -->
 <maecBundle:Candidate_Indicator id="capability_id">
  <maecBundle:Composition operator="AND">
   <maecBundle:Capability_Reference capability_idref="persistence"/>
   <maecBundle:Capability_Reference capability_idref="run_arbitrary_commands"/>
  </maecBundle:Composition>
 </maecBundle:Candidate_Indicator>
 <!-- Behaviour CIs -->
 <maecBundle:Candidate_Indicator id="persistence_id">
  <maecBundle:Composition operator="AND">
   <maecBundle:Behavior_Reference behavior_idref="establish_runtime_persistence"/>
   <maecBundle:Behavior_Reference
behavior_idref="establish_persistence_across_reboots"/>
  </maecBundle:Composition>
 </maecBundle:Candidate_Indicator>
 <maecBundle:Candidate_Indicator id="run_arbitrary_commands_id">
  <maecBundle:Composition operator="AND">
   <maecBundle:Behavior_Reference behavior_idref="fetch_commands"/>
   <maecBundle:Behavior_Reference behavior_idref="execute_commands_recieved"/>
  </maecBundle:Composition>
 </maecBundle:Candidate_Indicator>
```

```
<!-- Action CIs -->
<maecBundle:Candidate_Indicator id="establish_persistence_across_reboots">
 <maecBundle:Composition operator="AND">
  <maecBundle:Action_Reference action_id="drop_file_to_dir"/>
  <maecBundle:Action_Reference action_id="modify_registry"/>
  </maecBundle:Composition>
</maecBundle:Candidate_Indicator>
<maecBundle:Candidate_Indicator id="fetch_commands_id">
 <maecBundle:Composition operator="AND">
  <maecBundle:Action_Reference action_id="decode_url"/>
  <maecBundle:Action_Reference
action_id="fetch_commands_to_execute_from_cnc"/>
 </maecBundle:Composition>
</maecBundle:Candidate_Indicator>

<maecBundle:Candidate_Indicator id="execute_commands_received_id">
 <maecBundle:Composition operator="OR">
  <maecBundle:Sub_Composition operator="OR">
  <maecBundle:Action_Reference action_id="sleep_specified_time"/>
  <maecBundle:Action_Reference action_id="get_system_info"/>
  <maecBundle:Action_Reference action_id="execute_command"/>
  <maecBundle:Action_Reference action_id="stop_services"/>
  <maecBundle:Action_Reference action_id="download_file"/>
```

<maecBundle:Action_Reference action_id="start_process"/>

<maecBundle:Action_Reference action_id="start_service"/>

<maecBundle:Action_Reference action_id="terminate_process"/>

<maecBundle:Action_Reference action_id="close_cmd_shell"/>

<maecBundle:Action_Reference

action_id="create_process_custom_security_priveleges"/>

<maecBundle:Action_Reference action_id="uninstall_malware"/>

</maecBundle:Sub_Composition>

<maecBundle:Sub_Composition operator="AND">

<maecBundle:Action_Reference action_id="get_process_list"/>

<maecBundle:Action_Reference action_id="get_service_status"/>

<maecBundle:Action_Reference action_id="get_drive_type"/>

<maecBundle:Action_Reference action_id="get_volume_name"/>

</maecBundle:Sub_Composition>

</maecBundle:Composition>

</maecBundle:Candidate_Indicator>

<!-- Object CIs -->

<maecBundle:Candidate_Indicator id="decode_url_id">

<maecBundle:Composition operator="AND">

<maecBundle:Object_Reference object_idref="encoded_url"/>

<maecBundle:Object_Reference object_idref="decoded_url"/>

</maecBundle:Composition>

</maecBundle:Candidate_Indicator>

```
 <maecBundle:Candidate_Indicator id="stop_services_id">
  <maecBundle:Composition operator="AND">
   <maecBundle:Object_Reference object_idref="TerminateProcess"/>
   <maecBundle:Object_Reference object_idref="ControlService"/>
  </maecBundle:Composition>
 </maecBundle:Candidate_Indicator>
 <maecBundle:Candidate_Indicator id="download_file_id">
  <maecBundle:Composition operator="AND">
   <maecBundle:Object_Reference object_idref="InternetReadFile"/>
   <maecBundle:Object_Reference object_idref="WriteFile"/>
  </maecBundle:Composition>
 </maecBundle:Candidate_Indicator>
 <maecBundle:Candidate_Indicator id="restart_cmd_shell_id">
  <maecBundle:Composition operator="AND">
   <maecBundle:Object_Reference object_idref="GetExitCodeProcess"/>
   <maecBundle:Object_Reference object_idref="CreateProcess_API_1"/>
  </maecBundle:Composition>
 </maecBundle:Candidate_Indicator>
</maecBundle:Candidate_Indicators>


</maecBundle:MAEC_Bundle>
```

A.7 HacDef.A

<?xml version="1.0" encoding="UTF-8"?>

<maecBundle:MAEC_Bundle xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"

xsi:schemaLocation="http://cybox.mitre.org/objects#ArtifactObject-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/Artifact_Object.xsd

http://cybox.mitre.org/objects#WinRegistryKeyObject-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/Win_Registry_Key_Object.xsd

http://cybox.mitre.org/objects#WinExecutableFileObject-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/Win_Executable_File_Object.xsd

http://cybox.mitre.org/common-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/cybox_common.xsd

http://cybox.mitre.org/objects#APIObject-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/API_Object.xsd

http://maec.mitre.org/XMLSchema/maec-bundle-4

maec/maec_4.1_offline/maec_bundle_schema.xsd

http://cybox.mitre.org/objects#WinExecutableFileObject-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/Win_Executable_File_Object.xsd

http://cybox.mitre.org/objects#PDFFileObject-1

maec/maec_4.1_offline/cybox_2.1_offline/objects/PDF_File_Object.xsd

http://cybox.mitre.org/objects#APIObject-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/API_Object.xsd

http://cybox.mitre.org/objects#WinExecutableFileObject-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/Win_Executable_File_Object.xsd

http://cybox.mitre.org/default_vocabularies-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/cybox_default_vocabularies.xsd

http://cybox.mitre.org/objects#PDFFileObject-1

maec/maec_4.1_offline/cybox_2.1_offline/objects/PDF_File_Object.xsd

http://cybox.mitre.org/objects#WinRegistryKeyObject-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/Win_Registry_key_Object.xsd

http://cybox.mitre.org/objects#WinMutexObject-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/Win_Mutex_Object.xsd

http://cybox.mitre.org/objects#ArtifactObject-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/Artifact_Object.xsd

http://cybox.mitre.org/objects#EmailMessageObject-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/Email_Message_Object.xsd

http://cybox.mitre.org/objects#MutexObject-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/Mutex_Object.xsd

http://cybox.mitre.org/objects#PipeObject-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/Pipe_Object.xsd

http://cybox.mitre.org/objects#HTTPSessionObject-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/DNS_Query_Object.xsd

http://cybox.mitre.org/objects#UserAccountObject-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/User_Account_Object.xsd

"

xmlns:HTTPSessionObj="http://cybox.mitre.org/objects#HTTPSessionObject-2"

xmlns:DNSQueryObj="http://cybox.mitre.org/objects#DNSQueryObject-2"

xmlns:maecBundle="http://maec.mitre.org/XMLSchema/maec-bundle-4"

xmlns:ProcessObj="http://cybox.mitre.org/objects#ProcessObject-2"

xmlns:SocketAddressObj="http://cybox.mitre.org/objects#SocketAddressObject-1"

xmlns:AddressObj="http://cybox.mitre.org/objects#AddressObject-2"

xmlns:NetworkConnectionObj="http://cybox.mitre.org/objects#NetworkConnectionObje
ct-2"

xmlns:PDFFileObj="http://cybox.mitre.org/objects#PDFFileObject-1"

xmlns:cyboxVocabs="http://cybox.mitre.org/default_vocabularies-2"

xmlns:HostnameObj="http://cybox.mitre.org/objects#HostnameObject-1"

xmlns:CodeObj="http://cybox.mitre.org/objects#CodeObject-2"

xmlns:FileObj="http://cybox.mitre.org/objects#FileObject-2"

xmlns:DNSRecordObj="http://cybox.mitre.org/objects#DNSRecordObject-2"

xmlns:WinRegistryKeyObj="http://cybox.mitre.org/objects#WinRegistryKeyObject-2"

xmlns:maecVocabs="http://maec.mitre.org/default_vocabularies-1"

xmlns:APIObj="http://cybox.mitre.org/objects#APIObject-2"

xmlns:WinExecutableFileObj="http://cybox.mitre.org/objects#WinExecutableFileObject
-2"

xmlns:cyboxCommon="http://cybox.mitre.org/common-2"

xmlns:URIObj="http://cybox.mitre.org/objects#URIObject-2"

xmlns:cybox="http://cybox.mitre.org/cybox-2"

xmlns:WinMutexObj="http://cybox.mitre.org/objects#WinMutexObject-2"
xmlns:ArtifactObj="http://cybox.mitre.org/objects#ArtifactObject-2"
xmlns:EmailMessageObj="http://cybox.mitre.org/objects#EmailMessageObject-2"
xmlns:MutexObj="http://cybox.mitre.org/objects#MutexObject-2"
xmlns:PipeObj="http://cybox.mitre.org/objects#PipeObject-2"
xmlns:UserAccountObj="http://cybox.mitre.org/objects#UserAccountObject-2"
id="HacDef_exe_TT" schema_version="4.1"
defined_subject="true">

<maecBundle:Malware_Instance_Object_Attributes>
<cybox:Description>The Malware is an exe sample with rootkit functionalities.
It hides processes, registry keys, services specified in it's configuration
file</cybox:Description>
<cybox:Properties
xsi:type="WinExecutableFileObj:WindowsExecutableFileObjectType">
<FileObj:File_Extension>EXE</FileObj:File_Extension>
<FileObj:Size_In_Bytes>50688</FileObj:Size_In_Bytes>
<FileObj:Hashes>
<cyboxCommon:Hash>
<cyboxCommon:Type>MD5</cyboxCommon:Type>

<cyboxCommon:Simple_Hash_Value>39a9e5c05ffbda925da0d2ec9b4f512a</cyboxCo
mmon:Simple_Hash_Value>

```
 </cyboxCommon:Hash>
</FileObj:Hashes>
 </cybox:Properties>
  </maecBundle:Malware_Instance_Object_Attributes>

 <!-- Placeholder for capabilities -->
 <maecBundle:Capabilities>
  <maecBundle:Capability id="persistence" name="persistence">
   <maecBundle:Behavior_Reference
behavior_idref="establish_persistence_across_reboots"/>
  </maecBundle:Capability>
  <maecBundle:Capability id="run_arbitrary_commands">
   <maecBundle:Behavior_Reference
behavior_idref="execute_commands_in_config_file"/>
  </maecBundle:Capability>

  <maecBundle:Capability id="hide_os_info" name="anti-detection">
   <maecBundle:Behavior_Reference behavior_idref="code_injection"/>

   <maecBundle:Behavior_Reference behavior_idref="Hook_ZwQuerySystemInfo"/>
   <maecBundle:Behavior_Reference behavior_idref="Hook_ZwVdmControl"/>
   <maecBundle:Behavior_Reference behavior_idref="Hook_ZwEnumerateKey"/>
   <maecBundle:Behavior_Reference behavior_idref="Hook_ZwEnumerateValueKey"/>
```

<maecBundle:Behavior_Reference behavior_idref="Hook_LdrLoadDll"/>

<maecBundle:Behavior_Reference behavior_idref="Hook_ReadFile"/>

<maecBundle:Behavior_Reference behavior_idref="Hook_WriteFile"/>

<maecBundle:Behavior_Reference behavior_idref="Hook_GetModuleFileName"/>

<maecBundle:Behavior_Reference behavior_idref="Hook_GetEnvironmentVariable"/>

<maecBundle:Behavior_Reference behavior_idref="Hook_EnumerateServiceGroup"/>

<maecBundle:Behavior_Reference
behavior_idref="Hook_EnumerateServiceStatusEx"/>

<maecBundle:Behavior_Reference behavior_idref="Hook_EnumerateServiceStatus"/>

<maecBundle:Behavior_Reference behavior_idref="Hook_send"/>

<maecBundle:Behavior_Reference behavior_idref="Hook_recv"/>

<maecBundle:Behavior_Reference behavior_idref="Hook_WSARecv"/>

<maecBundle:Behavior_Reference behavior_idref="Hook_WSAEventSelect"/>

<maecBundle:Behavior_Reference behavior_idref="Hook_ZwQueryDirectoryFile"/>

<maecBundle:Behavior_Reference behavior_idref="Hook_ZwQueryObject"/>

<maecBundle:Behavior_Reference behavior_idref="Hook_ZwOpenKey"/>

</maecBundle:Capability>

<maecBundle:Capability id="receive_commands_communication_channel">

<maecBundle:Behavior_Reference behavior_idref="create_named_mailslot"/>

<maecBundle:Behavior_Reference behavior_idref="refresh"/>

<maecBundle:Behavior_Reference behavior_idref="uninstall"/>

</maecBundle:Capability>

```
</maecBundle:Capabilities>

<!-- Placeholder for behaviours -->
<maecBundle:Behaviors>
 <maecBundle:Behavior id="establish_persistence_across_reboots">
  <maecBundle:Action_Composition>
   <maecBundle:Action_Reference action_id="drop_ini_config_file"/>
   <maecBundle:Action_Reference action_id="copy_self_to_new_sys"/>
   <maecBundle:Action_Reference action_id="register_sys_as_service"/>
   <maecBundle:Action_Reference action_id="register_sys_as_service_safemode"/>
   <maecBundle:Action_Reference
action_id="register_sys_as_service_safemode_networking"/>
  </maecBundle:Action_Composition>
 </maecBundle:Behavior>
 <maecBundle:Behavior id="execute_commands_in_config_file">
  <maecBundle:Action_Composition>
   <maecBundle:Action_Reference action_id="start_process"/>
 </maecBundle:Action_Composition>
 </maecBundle:Behavior>
 <maecBundle:Behavior id="code_injection">
  <maecBundle:Action_Composition>
   <maecBundle:Action_Reference action_id="list_processes"/>
   <maecBundle:Action_Reference action_id="open_process"/>
```

<maecBundle:Action_Reference action_id="copy_self_to_process"/>
</maecBundle:Action_Composition>
</maecBundle:Behavior>
<maecBundle:Behavior id="Hook_ZwQuerySystemInfo">
<maecBundle:Action_Composition>
<maecBundle:Action_Reference action_id="remove_process_from_list"/>
<maecBundle:Action_Reference action_id="set_artificial_disk_info"/>
</maecBundle:Action_Composition>
</maecBundle:Behavior>
<maecBundle:Behavior id="Hook_ZwVdmControl">
<maecBundle:Action_Composition>
<maecBundle:Action_Reference action_id="remove_process_from_list"/>
</maecBundle:Action_Composition>
</maecBundle:Behavior>
<maecBundle:Behavior id="Hook_ZwEnumerateKey">
<maecBundle:Action_Composition>
<maecBundle:Action_Reference action_id="hide_registry_key"/>
</maecBundle:Action_Composition>
</maecBundle:Behavior>
<maecBundle:Behavior id="Hook_ZwEnumerateValueKey">
<maecBundle:Action_Composition>
<maecBundle:Action_Reference action_id="hide_registry_key"/>
</maecBundle:Action_Composition>

```
</maecBundle:Behavior>
<maecBundle:Behavior id="Hook_LdrLoadDll">
 <maecBundle:Action_Composition>
  <maecBundle:Action_Reference action_id="hide_dlls_from_list"/>
 </maecBundle:Action_Composition>
</maecBundle:Behavior>
<maecBundle:Behavior id="Hook_ReadFile">
 <maecBundle:Action_Composition>
  <maecBundle:Action_Reference action_id="prevent_file_read"/>
 </maecBundle:Action_Composition>
</maecBundle:Behavior>
<maecBundle:Behavior id="Hook_WriteFile">
 <maecBundle:Action_Composition>
  <maecBundle:Action_Reference action_id="prevent_file_write"/>
 </maecBundle:Action_Composition>
</maecBundle:Behavior>
<maecBundle:Behavior id="Hook_GetModuleFileName">
 <maecBundle:Action_Composition>
  <maecBundle:Action_Reference action_id="hide_file_name"/>
 </maecBundle:Action_Composition>
</maecBundle:Behavior>
<maecBundle:Behavior id="Hook_GetEnvironmentVariable">
 <maecBundle:Action_Composition>
```

<maecBundle:Action_Reference action_id="hide_file_name"/>
</maecBundle:Action_Composition>
</maecBundle:Behavior>
<maecBundle:Behavior id="Hook_EnumerateServiceGroup">
<maecBundle:Action_Composition>
<maecBundle:Action_Reference action_id="hide_service_name"/>
</maecBundle:Action_Composition>
</maecBundle:Behavior>
<maecBundle:Behavior id="Hook_EnumerateServiceStatusEx">
<maecBundle:Action_Composition>
<maecBundle:Action_Reference action_id="hide_service_name"/>
</maecBundle:Action_Composition>
</maecBundle:Behavior>
<maecBundle:Behavior id="Hook_EnumerateServiceStatus">
<maecBundle:Action_Composition>
<maecBundle:Action_Reference action_id="hide_service_name"/>
</maecBundle:Action_Composition>
</maecBundle:Behavior>
<maecBundle:Behavior id="Hook_send">
<maecBundle:Action_Composition>
<maecBundle:Action_Reference action_id="hide_traffic"/>
</maecBundle:Action_Composition>
</maecBundle:Behavior>

<maecBundle:Behavior id="Hook_recv">
 <maecBundle:Action_Composition>
  <maecBundle:Action_Reference action_id="hide_traffic"/>
 </maecBundle:Action_Composition>
</maecBundle:Behavior>
<maecBundle:Behavior id="Hook_WSARecv">
 <maecBundle:Action_Composition>
  <maecBundle:Action_Reference action_id="hide_traffic"/>
 </maecBundle:Action_Composition>
</maecBundle:Behavior>
<maecBundle:Behavior id="Hook_WSAEventSelect">
 <maecBundle:Action_Composition>
  <maecBundle:Action_Reference action_id="hide_traffic"/>
 </maecBundle:Action_Composition>
</maecBundle:Behavior>
<maecBundle:Behavior id="Hook_ZwQueryDirectoryFile">
 <maecBundle:Action_Composition>
  <maecBundle:Action_Reference action_id="hide_file_name"/>
 </maecBundle:Action_Composition>
</maecBundle:Behavior>
<maecBundle:Behavior id="Hook_ZwQueryObject">
 <maecBundle:Action_Composition>
  <maecBundle:Action_Reference action_id="hide_file_name"/>

</maecBundle:Action_Composition>

</maecBundle:Behavior>

<maecBundle:Behavior id="Hook_ZwOpenKey">

<maecBundle:Action_Composition>

<maecBundle:Action_Reference action_id="hide_registry_key"/>

</maecBundle:Action_Composition>

</maecBundle:Behavior>

<maecBundle:Behavior id="create_named_mailslot">

<maecBundle:Action_Composition>

<maecBundle:Action_Reference action_id="create_mailslot_static_name"/>

</maecBundle:Action_Composition>

</maecBundle:Behavior>

<maecBundle:Behavior id="refresh">

<maecBundle:Action_Composition>

<maecBundle:Action_Reference action_id="fetch_new_config_file"/>

<maecBundle:Action_Reference action_id="update_config_file"/>

</maecBundle:Action_Composition>

</maecBundle:Behavior>

<maecBundle:Behavior id="uninstall">

<maecBundle:Action_Composition>

<maecBundle:Action_Reference action_id="unregister_service"/>

<maecBundle:Action_Reference action_id="unregister_sys_as_service_safemode"/>

<maecBundle:Action_Reference

action_id="unregister_sys_as_service_safemode_networking"/>
  </maecBundle:Action_Composition>
 </maecBundle:Behavior>

</maecBundle:Behaviors>

 <!-- Placeholder for actions -->
<maecBundle:Actions>
 <maecBundle:Action id="drop_ini_config_file">
  <cybox:Associated_Objects>
   <cybox:Associated_Object>
    <cybox:Properties xsi:type="FileObj:FileObjectType">
     <FileObj:File_Name>malware_file_name.ini</FileObj:File_Name>
    </cybox:Properties>
   </cybox:Associated_Object>
  </cybox:Associated_Objects>
 </maecBundle:Action>
 <maecBundle:Action id="copy_self_to_new_sys">
  <cybox:Associated_Objects>
   <cybox:Associated_Object>
    <cybox:Properties xsi:type="FileObj:FileObjectType">
     <FileObj:File_Name>%currentdir%*servicename*.sys</FileObj:File_Name>

```
    </cybox:Properties>
   </cybox:Associated_Object>
  </cybox:Associated_Objects>
 </maecBundle:Action>
 <maecBundle:Action id="register_sys_as_service">
  <cybox:Associated_Objects>
   <cybox:Associated_Object id="registry_service_entry_1">
    <cybox:Association_Type xsi:type="maecVocabs:RegistryActionNameVocab-
1.0">create registry key</cybox:Association_Type>
    <cybox:Properties xsi:type="WinRegistryKeyObj:WindowsRegistryKeyObjectType">

<WinRegistryKeyObj:Key>System\CurrnetControlSet\Services\*Service_Name*</Win
RegistryKeyObj:Key>
     <WinRegistryKeyObj:Hive>HKLM</WinRegistryKeyObj:Hive>
    </cybox:Properties>
   </cybox:Associated_Object>
  </cybox:Associated_Objects>
 </maecBundle:Action>
 <maecBundle:Action id="register_sys_as_service_safemode">
  <cybox:Associated_Objects>
   <cybox:Associated_Object>
    <cybox:Association_Type xsi:type="maecVocabs:RegistryActionNameVocab-
1.0">create registry key</cybox:Association_Type>
```

<cybox:Properties xsi:type="WinRegistryKeyObj:WindowsRegistryKeyObjectType">

<WinRegistryKeyObj:Key>System\CurrnetControlSet\Control\SafeBoot\Minimal*Servi
ce_Name*</WinRegistryKeyObj:Key>

<WinRegistryKeyObj:Hive>HKLM</WinRegistryKeyObj:Hive>

</cybox:Properties>

</cybox:Associated_Object>

</cybox:Associated_Objects>

</maecBundle:Action>

<maecBundle:Action id="register_sys_as_service_safemode_networking">

<cybox:Associated_Objects>

<cybox:Associated_Object>

<cybox:Association_Type xsi:type="maecVocabs:RegistryActionNameVocab-
1.0">create registry key</cybox:Association_Type>

<cybox:Properties xsi:type="WinRegistryKeyObj:WindowsRegistryKeyObjectType">

<WinRegistryKeyObj:Key>System\CurrnetControlSet\Control\SafeBoot\Network*Servi
ce_Name*</WinRegistryKeyObj:Key>

<WinRegistryKeyObj:Hive>HKLM</WinRegistryKeyObj:Hive>

</cybox:Properties>

</cybox:Associated_Object>

</cybox:Associated_Objects>

</maecBundle:Action>

```
<maecBundle:Action id="start_process">
 <cybox:Associated_Objects>
  <cybox:Associated_Object id="CreateProcess_API">
   <cybox:Properties xsi:type="APIObj:APIObjectType">
    <APIObj:Function_Name>CreateProcess</APIObj:Function_Name>
   </cybox:Properties>
  </cybox:Associated_Object>
 </cybox:Associated_Objects>
</maecBundle:Action>

<maecBundle:Action id="list_processes"/>
<maecBundle:Action id="open_process"/>
<maecBundle:Action id="copy_self_to_process"/>
<maecBundle:Action id="remove_process_from_list"/>
<maecBundle:Action id="set_artificial_disk_info"/>
<maecBundle:Action id="hide_registry_key"/>
<maecBundle:Action id="hide_dlls_from_list"/>
<maecBundle:Action id="prevent_file_read"/>
<maecBundle:Action id="prevent_file_write"/>
<maecBundle:Action id="hide_file_name"/>
<maecBundle:Action id="hide_service_name"/>
<maecBundle:Action id="hide_traffic"/>
```

```
<maecBundle:Action id="create_mailslot"/>
<maecBundle:Action id="fetch_new_config_file"/>
<maecBundle:Action id="update_config_file"/>
<maecBundle:Action id="unregister_service"/>
<maecBundle:Action id="unregister_sys_as_service_safemode"/>
<maecBundle:Action id="unregister_sys_as_service_safemode_networking"/>

</maecBundle:Actions>

<maecBundle:Candidate_Indicators>
 <!-- Capability CIs -->
<maecBundle:Candidate_Indicator id="capabilities_id">
 <maecBundle:Composition operator="AND">
  <maecBundle:Capability_Reference capability_idref="persistence"/>

  <maecBundle:Sub_Composition operator="OR">
   <maecBundle:Capability_Reference capability_idref="hide_os_info"/>
   <maecBundle:Capability_Reference capability_idref="run_arbitrary_commands"/>
   <maecBundle:Capability_Reference capability_idref="trojanize_binaries"/>
   <maecBundle:Capability_Reference
capability_idref="receive_commands_communication_channel"/>
  </maecBundle:Sub_Composition>
```

```
 </maecBundle:Composition>
</maecBundle:Candidate_Indicator>
 <!-- Behaviour CIs -->
 <maecBundle:Candidate_Indicator id="persistence_id">
  <maecBundle:Composition operator="OR">
   <maecBundle:Behavior_Reference
behavior_idref="establish_persistence_across_reboots"/>
  </maecBundle:Composition>
 </maecBundle:Candidate_Indicator>
 <maecBundle:Candidate_Indicator id="run_arbitrary_commands_id">
  <maecBundle:Composition operator="OR">
   <maecBundle:Behavior_Reference
behavior_idref="execute_commands_in_config_file"/>
  </maecBundle:Composition>
 </maecBundle:Candidate_Indicator>
 <maecBundle:Candidate_Indicator id="trojanize_binaries_id">
  <maecBundle:Composition operator="OR">

  </maecBundle:Composition>
 </maecBundle:Candidate_Indicator>
 <maecBundle:Candidate_Indicator id="hide_os_info_id">
  <maecBundle:Composition operator="AND">
  <maecBundle:Behavior_Reference behavior_idref="code_injection"/>
```

<maecBundle:Sub_Composition operator="OR">
<maecBundle:Behavior_Reference behavior_idref="Hook_ZwQuerySystemInfo"/>
<maecBundle:Behavior_Reference behavior_idref="Hook_ZwVdmControl"/>
<maecBundle:Behavior_Reference behavior_idref="Hook_ZwEnumerateKey"/>
<maecBundle:Behavior_Reference behavior_idref="Hook_ZwEnumerateValueKey"/>
<maecBundle:Behavior_Reference behavior_idref="Hook_LdrLoadDll"/>
<maecBundle:Behavior_Reference behavior_idref="Hook_ReadFile"/>
<maecBundle:Behavior_Reference behavior_idref="Hook_WriteFile"/>
<maecBundle:Behavior_Reference behavior_idref="Hook_GetModuleFileName"/>
<maecBundle:Behavior_Reference
behavior_idref="Hook_GetEnvironmentVariable"/>
<maecBundle:Behavior_Reference
behavior_idref="Hook_EnumerateServiceGroup"/>
<maecBundle:Behavior_Reference
behavior_idref="Hook_EnumerateServiceStatusEx"/>
<maecBundle:Behavior_Reference behavior_idref="Hook_EnumerateServiceStatus"/>
<maecBundle:Behavior_Reference behavior_idref="Hook_send"/>
<maecBundle:Behavior_Reference behavior_idref="Hook_recv"/>
<maecBundle:Behavior_Reference behavior_idref="Hook_WSARecv"/>
<maecBundle:Behavior_Reference behavior_idref="Hook_WSAEventSelect"/>
<maecBundle:Behavior_Reference behavior_idref="Hook_ZwQueryDirectoryFile"/>
<maecBundle:Behavior_Reference behavior_idref="Hook_ZwQueryObject"/>
<maecBundle:Behavior_Reference behavior_idref="Hook_ZwOpenKey"/>

```
  </maecBundle:Sub_Composition>
  </maecBundle:Sub_Composition>
 </maecBundle:Candidate_Indicator>
 <maecBundle:Candidate_Indicator
id="receive_commands_communication_channel_id">
  <maecBundle:Composition operator="AND">
   <maecBundle:Behavior_Reference behavior_idref="create_named_mailslot"/>
   <maecBundle:Sub_Composition operator="OR">
    <maecBundle:Behavior_Reference behavior_idref="refresh"/>
    <maecBundle:Behavior_Reference behavior_idref="uninstall"/>
   </maecBundle:Sub_Composition>

  </maecBundle:Composition>
 </maecBundle:Candidate_Indicator>
 <!-- Action CIs -->
 <maecBundle:Candidate_Indicator id="persistence_across_reboots_id">
  <maecBundle:Composition operator="AND">
   <maecBundle:Action_Reference action_id="drop_ini_config_file"/>
   <maecBundle:Action_Reference action_id="copy_self_to_new_sys"/>
   <maecBundle:Action_Reference action_id="register_sys_as_service"/>
   <maecBundle:Action_Reference action_id="register_sys_as_service_safemode"/>
   <maecBundle:Action_Reference
action_id="register_sys_as_service_safemode_networking"/>
```

```
 </maecBundle:Composition>
</maecBundle:Candidate_Indicator>
<maecBundle:Candidate_Indicator id="execute_commands_in_config_file_id">
 <maecBundle:Composition operator="OR">
   <maecBundle:Action_Reference action_id="start_process"/>
 </maecBundle:Composition>
</maecBundle:Candidate_Indicator>
<maecBundle:Candidate_Indicator id="code_injection_id">
 <maecBundle:Composition operator="AND">
  <maecBundle:Action_Reference action_id="list_processes"/>
  <maecBundle:Action_Reference action_id="open_process"/>
  <maecBundle:Action_Reference action_id="copy_self_to_process"/>
 </maecBundle:Composition>
</maecBundle:Candidate_Indicator>
<maecBundle:Candidate_Indicator id="Hook_ZwQuerySystemInfo_id">
 <maecBundle:Composition operator="AND">
  <maecBundle:Action_Reference action_id="remove_process_from_list"/>
  <maecBundle:Action_Reference action_id="set_artificial_disk_info"/>
 </maecBundle:Composition>
</maecBundle:Candidate_Indicator>
<maecBundle:Candidate_Indicator id="Hook_ZwVdmControl_id">
 <maecBundle:Composition operator="OR">
  <maecBundle:Action_Reference action_id="remove_process_from_list"/>
```

```
 </maecBundle:Composition>
</maecBundle:Candidate_Indicator>
<maecBundle:Candidate_Indicator id="Hook_ZwEnumerateKey_id">
 <maecBundle:Composition operator="OR">
  <maecBundle:Action_Reference action_id="hide_registry_key"/>
 </maecBundle:Composition>
</maecBundle:Candidate_Indicator>
<maecBundle:Candidate_Indicator id="Hook_ZwEnumerateValueKey_id">
 <maecBundle:Composition operator="OR">
  <maecBundle:Action_Reference action_id="hide_registry_key"/>
 </maecBundle:Composition>
</maecBundle:Candidate_Indicator>
<maecBundle:Candidate_Indicator id="Hook_LdrLoadDll_id">
 <maecBundle:Composition operator="OR">
  <maecBundle:Action_Reference action_id="hide_dlls_from_list"/>
 </maecBundle:Composition>
</maecBundle:Candidate_Indicator>
<maecBundle:Candidate_Indicator id="Hook_ReadFile_id">
 <maecBundle:Composition operator="OR">
  <maecBundle:Action_Reference action_id="prevent_file_read"/>
 </maecBundle:Composition>
</maecBundle:Candidate_Indicator>
<maecBundle:Candidate_Indicator id="Hook_WriteFile_id">
```

<maecBundle:Composition operator="OR">
<maecBundle:Action_Reference action_id="prevent_file_write"/>
</maecBundle:Composition>
</maecBundle:Candidate_Indicator>
<maecBundle:Candidate_Indicator id="Hook_GetModuleFileName_id">
<maecBundle:Composition operator="OR">
<maecBundle:Action_Reference action_id="hide_file_name"/>
</maecBundle:Composition>
</maecBundle:Candidate_Indicator>
<maecBundle:Candidate_Indicator id="Hook_GetEnvironmentVariable_id">
<maecBundle:Composition operator="OR">
<maecBundle:Action_Reference action_id="hide_file_name"/>
</maecBundle:Composition>
</maecBundle:Candidate_Indicator>
<maecBundle:Candidate_Indicator id="Hook_EnumerateServiceGroup_id">
<maecBundle:Composition operator="OR">
<maecBundle:Action_Reference action_id="hide_service_name"/>
</maecBundle:Composition>
</maecBundle:Candidate_Indicator>
<maecBundle:Candidate_Indicator id="Hook_EnumerateServiceStatusEx_id">
<maecBundle:Composition operator="OR">
<maecBundle:Action_Reference action_id="hide_service_name"/>
</maecBundle:Composition>

```
</maecBundle:Candidate_Indicator>
<maecBundle:Candidate_Indicator id="Hook_EnumerateServiceStatus_id">
 <maecBundle:Composition operator="OR">
  <maecBundle:Action_Reference action_id="hide_service_name"/>
 </maecBundle:Composition>
</maecBundle:Candidate_Indicator>
<maecBundle:Candidate_Indicator id="Hook_send_id">
 <maecBundle:Composition operator="OR">
  <maecBundle:Action_Reference action_id="hide_traffic"/>
 </maecBundle:Composition>
</maecBundle:Candidate_Indicator>
<maecBundle:Candidate_Indicator id="Hook_WSARecv_id">
 <maecBundle:Composition operator="OR">
  <maecBundle:Action_Reference action_id="hide_traffic"/>
 </maecBundle:Composition>
</maecBundle:Candidate_Indicator>
<maecBundle:Candidate_Indicator id="Hook_WSAEventSelect_id">
 <maecBundle:Composition operator="OR">
  <maecBundle:Action_Reference action_id="hide_traffic"/>
 </maecBundle:Composition>
</maecBundle:Candidate_Indicator>
<maecBundle:Candidate_Indicator id="Hook_ZwQueryDirectoryFile_id">
 <maecBundle:Composition operator="OR">
```

<maecBundle:Action_Reference action_id="hide_file_name"/>
</maecBundle:Composition>
</maecBundle:Candidate_Indicator>
<maecBundle:Candidate_Indicator id="Hook_ZwQueryObject_id">
<maecBundle:Composition operator="OR">
<maecBundle:Action_Reference action_id="hide_file_name"/>
</maecBundle:Composition>
</maecBundle:Candidate_Indicator>
<maecBundle:Candidate_Indicator id="Hook_ZwOpenKey_id">
<maecBundle:Composition operator="OR">
<maecBundle:Action_Reference action_id="hide_registry_key"/>
</maecBundle:Composition>
</maecBundle:Candidate_Indicator>
<maecBundle:Candidate_Indicator id="create_named_mailslot_id">
<maecBundle:Composition operator="OR">
<maecBundle:Action_Reference action_id="create_mailslot_static_name"/>
</maecBundle:Composition>
</maecBundle:Candidate_Indicator>
<maecBundle:Candidate_Indicator id="refresh_id">
<maecBundle:Composition operator="AND">
<maecBundle:Action_Reference action_id="fetch_new_config_file"/>
<maecBundle:Action_Reference action_id="update_config_file"/>
</maecBundle:Composition>

```
  </maecBundle:Candidate_Indicator>
  <maecBundle:Candidate_Indicator id="uninstall_id">
   <maecBundle:Composition operator="AND">
    <maecBundle:Action_Reference action_id="unregister_service"/>
    <maecBundle:Action_Reference action_id="unregister_sys_as_service_safemode"/>
    <maecBundle:Action_Reference
action_id="unregister_sys_as_service_safemode_networking"/>
   </maecBundle:Composition>
  </maecBundle:Candidate_Indicator>

  <!-- Object CIs -->

 </maecBundle:Candidate_Indicators>


</maecBundle:MAEC_Bundle>
```

A.8 Sality.A

```
<?xml version="1.0" encoding="UTF-8"?>
<maecBundle:MAEC_Bundle xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance"
 xsi:schemaLocation="http://cybox.mitre.org/objects#ArtifactObject-2
maec/maec_4.1_offline/cybox_2.1_offline/objects/Artifact_Object.xsd
```

http://cybox.mitre.org/objects#WinRegistryKeyObject-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/Win_Registry_Key_Object.xsd

http://cybox.mitre.org/objects#WinExecutableFileObject-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/Win_Executable_File_Object.xsd

http://cybox.mitre.org/common-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/cybox_common.xsd

http://cybox.mitre.org/objects#APIObject-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/API_Object.xsd

http://maec.mitre.org/XMLSchema/maec-bundle-4

maec/maec_4.1_offline/maec_bundle_schema.xsd

http://cybox.mitre.org/objects#WinExecutableFileObject-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/Win_Executable_File_Object.xsd

http://cybox.mitre.org/objects#PDFFileObject-1

maec/maec_4.1_offline/cybox_2.1_offline/objects/PDF_File_Object.xsd

http://cybox.mitre.org/objects#APIObject-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/API_Object.xsd

http://cybox.mitre.org/objects#WinExecutableFileObject-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/Win_Executable_File_Object.xsd

http://cybox.mitre.org/default_vocabularies-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/cybox_default_vocabularies.xsd

http://cybox.mitre.org/objects#PDFFileObject-1

maec/maec_4.1_offline/cybox_2.1_offline/objects/PDF_File_Object.xsd

http://cybox.mitre.org/objects#WinRegistryKeyObject-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/Win_Registry_key_Object.xsd

http://cybox.mitre.org/objects#WinMutexObject-2

.maec/maec_4.1_offline/cybox_2.1_offline/objects/Win_Mutex_Object.xsd

http://cybox.mitre.org/objects#ArtifactObject-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/Artifact_Object.xsd

http://cybox.mitre.org/objects#EmailMessageObject-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/Email_Message_Object.xsd

"

xmlns:HTTPSessionObj="http://cybox.mitre.org/objects#HTTPSessionObject-2"

xmlns:DNSQueryObj="http://cybox.mitre.org/objects#DNSQueryObject-2"

xmlns:maecBundle="http://maec.mitre.org/XMLSchema/maec-bundle-4"

xmlns:ProcessObj="http://cybox.mitre.org/objects#ProcessObject-2"

xmlns:SocketAddressObj="http://cybox.mitre.org/objects#SocketAddressObject-1"

xmlns:AddressObj="http://cybox.mitre.org/objects#AddressObject-2"

xmlns:NetworkConnectionObj="http://cybox.mitre.org/objects#NetworkConnectionObje

ct-2"

xmlns:PDFFileObj="http://cybox.mitre.org/objects#PDFFileObject-1"

xmlns:cyboxVocabs="http://cybox.mitre.org/default_vocabularies-2"

xmlns:HostnameObj="http://cybox.mitre.org/objects#HostnameObject-1"

xmlns:CodeObj="http://cybox.mitre.org/objects#CodeObject-2"

xmlns:FileObj="http://cybox.mitre.org/objects#FileObject-2"

xmlns:DNSRecordObj="http://cybox.mitre.org/objects#DNSRecordObject-2"

```
 xmlns:WinRegistryKeyObj="http://cybox.mitre.org/objects#WinRegistryKeyObject-2"
 xmlns:maecVocabs="http://maec.mitre.org/default_vocabularies-1"
 xmlns:APIObj="http://cybox.mitre.org/objects#APIObject-2"

xmlns:WinExecutableFileObj="http://cybox.mitre.org/objects#WinExecutableFileObject
-2"
 xmlns:cyboxCommon="http://cybox.mitre.org/common-2"
 xmlns:URIObj="http://cybox.mitre.org/objects#URIObject-2"
 xmlns:cybox="http://cybox.mitre.org/cybox-2"
 xmlns:WinMutexObj="http://cybox.mitre.org/objects#WinMutexObject-2"
 xmlns:ArtifactObj="http://cybox.mitre.org/objects#ArtifactObject-2"
 xmlns:EmailMessageObj="http://cybox.mitre.org/objects#EmailMessageObject-2"

 id="Sality_exe_TT" schema_version="4.1"
 defined_subject="true">

 <maecBundle:Malware_Instance_Object_Attributes>
  <cybox:Description>The Malware is an EXE sample that infects files and performs
other data stealing activities</cybox:Description>
 <cybox:Properties
xsi:type="WinExecutableFileObj:WindowsExecutableFileObjectType">
  <FileObj:File_Extension>EXE</FileObj:File_Extension>
<FileObj:Size_In_Bytes>175373</FileObj:Size_In_Bytes>
```

<FileObj:Hashes>

<cyboxCommon:Hash>

<cyboxCommon:Type>MD5</cyboxCommon:Type>

<cyboxCommon:Simple_Hash_Value>322a1203bbf5e12540df0e10adb21b58</cyboxCo

mmon:Simple_Hash_Value>

</cyboxCommon:Hash>

</FileObj:Hashes>

</cybox:Properties>

</maecBundle:Malware_Instance_Object_Attributes>

<!-- Placeholder for capabilities -->

<maecBundle:Capabilities>

<maecBundle:Capability id="persistence" name="persistence">

<maecBundle:Behavior_Reference behavior_idref="persistence_at_runtime"/>

<maecBundle:Behavior_Reference behavior_idref="persistence_on_disk"/>

<maecBundle:Behavior_Reference

behavior_idref="persistence_against_process_shutdown"/>

</maecBundle:Capability>

<maecBundle:Capability id="spread_across_system" name="infection/propagation">

<maecBundle:Behavior_Reference behavior_idref="copy_self_to_files"/>

</maecBundle:Capability>

```
 <maecBundle:Capability id="gather_system_info_and_send_to_attacker">
  <maecBundle:Behavior_Reference behavior_idref="gather_system_info"/>
  <maecBundle:Behavior_Reference behavior_idref="send_to_attacker"/>
 </maecBundle:Capability>

</maecBundle:Capabilities>

<!-- Placeholder for behaviours -->
<maecBundle:Behaviors>

 <maecBundle:Behavior id="persistence_at_runtime">
  <maecBundle:Action_Composition>
   <maecBundle:Action_Reference action_id="create_mutex"/>
  </maecBundle:Action_Composition>
 </maecBundle:Behavior>
 <maecBundle:Behavior id="persistence_on_disk">
  <maecBundle:Action_Composition>
   <maecBundle:Action_Reference action_id="drop_file_on_filesystem"/>
  </maecBundle:Action_Composition>
 </maecBundle:Behavior>
 <maecBundle:Behavior id="persistence_against_process_shutdown">
  <maecBundle:Action_Composition>
   <maecBundle:Action_Reference action_id="run_copy_of_malware"/>
```

```
 </maecBundle:Action_Composition>
</maecBundle:Behavior>

<maecBundle:Behavior id="copy_self_to_files">
 <maecBundle:Action_Composition>
  <maecBundle:Action_Reference action_id="enumerate_files"/>
  <maecBundle:Action_Reference action_id="infect_files"/>
 </maecBundle:Action_Composition>
</maecBundle:Behavior>
<maecBundle:Behavior id="gather_system_info">
 <maecBundle:Action_Composition>
  <maecBundle:Action_Reference action_id="get_os_version"/>
  <maecBundle:Action_Reference action_id="get_computer_name"/>
  <maecBundle:Action_Reference action_id="get_user_name"/>
  <maecBundle:Action_Reference action_id="get_drive_type"/>
  <maecBundle:Action_Reference action_id="get_volume_info"/>

  <maecBundle:Action_Reference action_id="get_product_name"/>
  <maecBundle:Action_Reference action_id="get_product_version"/>
  <maecBundle:Action_Reference action_id="get_product_version_number"/>
  <maecBundle:Action_Reference action_id="get_registered_owner"/>
  <maecBundle:Action_Reference action_id="get_registered_organization"/>
  <maecBundle:Action_Reference action_id="get_program_files_dir"/>
```

<maecBundle:Action_Reference action_id="get_urls_visited"/>

<maecBundle:Action_Reference action_id="get_passwords_cached"/>

</maecBundle:Action_Composition>

</maecBundle:Behavior>

<maecBundle:Behavior id="send_to_attacker">

<maecBundle:Action_Composition>

<maecBundle:Action_Reference action_id="send_email_to_attacker"/>

</maecBundle:Action_Composition>

</maecBundle:Behavior>

</maecBundle:Behaviors>

<!-- Placeholder for actions -->

<maecBundle:Actions>

<maecBundle:Action id="create_mutex">

<cybox:Name xsi:type="maecVocabs:SynchronizationActionNameVocab-1.0">create mutex</cybox:Name>

<cybox:Associated_Objects>

<cybox:Associated_Object>

<cybox:Properties xsi:type="WinMutexObj:WindowsMutexObjectType" named="true">

<MutexObj:Name>ADR32</MutexObj:Name>

```
    </cybox:Properties>
   </cybox:Associated_Object>
  </cybox:Associated_Objects>
 </maecBundle:Action>
 <maecBundle:Action id="drop_file_on_filesystem">
  <cybox:Name xsi:type="maecVocabs:FileActionNameVocab-1.1">create
file</cybox:Name>
  <cybox:Associated_Objects>
   <cybox:Associated_Object>
    <cybox:Description> the malware creates a copy of itself in the
directory</cybox:Description>
    <cybox:Properties
xsi:type="WinExecutableFileObj:WindowsExecutableFileObjectType">
     <FileObj:File_Name>syslib32.dll</FileObj:File_Name>
     <FileObj:File_Path>%sysdir%</FileObj:File_Path>
     <FileObj:File_Extension>dll</FileObj:File_Extension>

    </cybox:Properties>
   </cybox:Associated_Object>
  </cybox:Associated_Objects>
 </maecBundle:Action>
 <maecBundle:Action id="run_copy_of_malware">
  <cybox:Associated_Objects>
```

<cybox:Associated_Object id="CreateProcess_API">
<cybox:Properties xsi:type="APIObj:APIObjectType">
<APIObj:Function_Name>CreateProcess</APIObj:Function_Name>
</cybox:Properties>
</cybox:Associated_Object>
</cybox:Associated_Objects>
</maecBundle:Action>
<maecBundle:Action id="enumerate_files">
<cybox:Name xsi:type="maecVocabs:FileActionNameVocab-1.1">find file</cybox:Name>
<cybox:Associated_Objects>
<cybox:Associated_Object id="find_file">
<cybox:Properties xsi:type="APIObj:APIObjectType">
<APIObj:Function_Name>FindFirstFileA</APIObj:Function_Name>
</cybox:Properties>
</cybox:Associated_Object>
<cybox:Associated_Object id="file_type">
<cybox:Properties xsi:type="FileObj:FileObjectType">
<FileObj:File_Extension>.exe</FileObj:File_Extension>
</cybox:Properties>
<cybox:Association_Type>returned</cybox:Association_Type>
</cybox:Associated_Object>
</cybox:Associated_Objects>

```
</maecBundle:Action>
<maecBundle:Action id="infect_files">
 <cybox:Associated_Objects>
  <cybox:Associated_Object id="WriteFile">
   <cybox:Properties xsi:type="APIObj:APIObjectType">
    <APIObj:Function_Name>WriteFile</APIObj:Function_Name>
   </cybox:Properties>
  </cybox:Associated_Object>
 </cybox:Associated_Objects>
</maecBundle:Action>

<maecBundle:Action id="get_os_version">
 <cybox:Associated_Objects>
  <cybox:Associated_Object id="get_os_version_API">
   <cybox:Properties xsi:type="APIObj:APIObjectType">
    <APIObj:Function_Name>GetVersionExA</APIObj:Function_Name>
   </cybox:Properties>
  </cybox:Associated_Object>
 </cybox:Associated_Objects>
</maecBundle:Action>
<maecBundle:Action id="get_computer_name">
 <cybox:Associated_Objects>
  <cybox:Associated_Object>
```

<cybox:Properties xsi:type="APIObj:APIObjectType">
<APIObj:Function_Name>GetComputerNameA</APIObj:Function_Name>
</cybox:Properties>
</cybox:Associated_Object>
</cybox:Associated_Objects>
</maecBundle:Action>
<maecBundle:Action id="get_user_name">
<cybox:Associated_Objects>
<cybox:Associated_Object>
<cybox:Properties xsi:type="APIObj:APIObjectType">
<APIObj:Function_Name>GetUserNameA</APIObj:Function_Name>
</cybox:Properties>
</cybox:Associated_Object>
</cybox:Associated_Objects>
</maecBundle:Action>
<maecBundle:Action id="get_drive_type">
<cybox:Associated_Objects>
<cybox:Associated_Object>
<cybox:Properties xsi:type="APIObj:APIObjectType">
<APIObj:Function_Name>GetDriveTypeA</APIObj:Function_Name>
</cybox:Properties>
</cybox:Associated_Object>
</cybox:Associated_Objects>

```
 </maecBundle:Action>
 <maecBundle:Action id="get_volume_info">
  <cybox:Associated_Objects>
   <cybox:Associated_Object>
    <cybox:Properties xsi:type="APIObj:APIObjectType">
     <APIObj:Function_Name>GetVolumeInformationA</APIObj:Function_Name>
    </cybox:Properties>
   </cybox:Associated_Object>
  </cybox:Associated_Objects>
 </maecBundle:Action>

 <maecBundle:Action id="get_product_name">
  <cybox:Name xsi:type="maecVocabs:RegistryActionNameVocab-1.0">read registry
key value</cybox:Name>
  <cybox:Associated_Objects>
   <cybox:Associated_Object id="product_info">
    <cybox:Properties
xsi:type="WinRegistryKeyObj:WindowsRegistryKeyObjectType">

<WinRegistryKeyObj:Key>Software\Microsoft\Windows\CurrentVersion</WinRegistry
KeyObj:Key>
     <WinRegistryKeyObj:Hive>HKLM</WinRegistryKeyObj:Hive>
     <WinRegistryKeyObj:Values>
```

<WinRegistryKeyObj:Value>

<WinRegistryKeyObj:Name>ProductName</WinRegistryKeyObj:Name>

</WinRegistryKeyObj:Value>

</WinRegistryKeyObj:Values>

</cybox:Properties>

</cybox:Associated_Object>

</cybox:Associated_Objects>

</maecBundle:Action>

<maecBundle:Action id="get_product_version">

<cybox:Name xsi:type="maecVocabs:RegistryActionNameVocab-1.0">read registry key value</cybox:Name>

<cybox:Associated_Objects>

<cybox:Associated_Object>

<cybox:Properties xsi:type="WinRegistryKeyObj:WindowsRegistryKeyObjectType">

<WinRegistryKeyObj:Key>Software\Microsoft\Windows\CurrentVersion</WinRegistryKeyObj:Key>

<WinRegistryKeyObj:Hive>HKLM</WinRegistryKeyObj:Hive>

<WinRegistryKeyObj:Values>

<WinRegistryKeyObj:Value>

<WinRegistryKeyObj:Name>Version</WinRegistryKeyObj:Name>

</WinRegistryKeyObj:Value>

```
      </WinRegistryKeyObj:Values>
     </cybox:Properties>
    </cybox:Associated_Object>
   </cybox:Associated_Objects>
  </maecBundle:Action>
  <maecBundle:Action id="get_product_version_number">
   <cybox:Name xsi:type="maecVocabs:RegistryActionNameVocab-1.0">read registry
key value</cybox:Name>
   <cybox:Associated_Objects>
    <cybox:Associated_Object>
     <cybox:Properties
xsi:type="WinRegistryKeyObj:WindowsRegistryKeyObjectType">

<WinRegistryKeyObj:Key>Software\Microsoft\Windows\CurrentVersion</WinRegistry
KeyObj:Key>
      <WinRegistryKeyObj:Hive>HKLM</WinRegistryKeyObj:Hive>
      <WinRegistryKeyObj:Values>
       <WinRegistryKeyObj:Value>
        <WinRegistryKeyObj:Name>VersionNumber</WinRegistryKeyObj:Name>
       </WinRegistryKeyObj:Value>
      </WinRegistryKeyObj:Values>
     </cybox:Properties>
    </cybox:Associated_Object>
```

```
  </cybox:Associated_Objects>
 </maecBundle:Action>
 <maecBundle:Action id="get_product_registered_owner">
  <cybox:Name xsi:type="maecVocabs:RegistryActionNameVocab-1.0">read registry
key value</cybox:Name>
  <cybox:Associated_Objects>
   <cybox:Associated_Object>
    <cybox:Properties
xsi:type="WinRegistryKeyObj:WindowsRegistryKeyObjectType">

<WinRegistryKeyObj:Key>Software\Microsoft\Windows\CurrentVersion</WinRegistry
KeyObj:Key>
     <WinRegistryKeyObj:Hive>HKLM</WinRegistryKeyObj:Hive>
     <WinRegistryKeyObj:Values>
      <WinRegistryKeyObj:Value>
       <WinRegistryKeyObj:Name>Registered Owner</WinRegistryKeyObj:Name>
      </WinRegistryKeyObj:Value>
     </WinRegistryKeyObj:Values>
    </cybox:Properties>
   </cybox:Associated_Object>
  </cybox:Associated_Objects>
 </maecBundle:Action>
 <maecBundle:Action id="get_product_registered_organization">
```

<cybox:Name xsi:type="maecVocabs:RegistryActionNameVocab-1.0">read registry key value</cybox:Name>
<cybox:Associated_Objects>
<cybox:Associated_Object>
<cybox:Properties xsi:type="WinRegistryKeyObj:WindowsRegistryKeyObjectType">

<WinRegistryKeyObj:Key>Software\Microsoft\Windows\CurrentVersion</WinRegistryKeyObj:Key>
<WinRegistryKeyObj:Hive>HKLM</WinRegistryKeyObj:Hive>
<WinRegistryKeyObj:Values>
<WinRegistryKeyObj:Value>
<WinRegistryKeyObj:Name>Registered Organization</WinRegistryKeyObj:Name>
</WinRegistryKeyObj:Value>
</WinRegistryKeyObj:Values>
</cybox:Properties>
</cybox:Associated_Object>
</cybox:Associated_Objects>
</maecBundle:Action>
<maecBundle:Action id="get_program_files_dir">
<cybox:Name xsi:type="maecVocabs:RegistryActionNameVocab-1.0">read registry key value</cybox:Name>

```
  <cybox:Associated_Objects>
   <cybox:Associated_Object>
    <cybox:Properties
xsi:type="WinRegistryKeyObj:WindowsRegistryKeyObjectType">

<WinRegistryKeyObj:Key>Software\Microsoft\Windows\CurrentVersion</WinRegistry
KeyObj:Key>
     <WinRegistryKeyObj:Hive>HKLM</WinRegistryKeyObj:Hive>
     <WinRegistryKeyObj:Values>
      <WinRegistryKeyObj:Value>
       <WinRegistryKeyObj:Name>Program File Directory</WinRegistryKeyObj:Name>
      </WinRegistryKeyObj:Value>
     </WinRegistryKeyObj:Values>
    </cybox:Properties>
   </cybox:Associated_Object>
  </cybox:Associated_Objects>
 </maecBundle:Action>

 <maecBundle:Action id="get_urls_visited">
  <cybox:Name xsi:type="maecVocabs:RegistryActionNameVocab-1.0">read registry
key value</cybox:Name>
  <cybox:Associated_Objects>
   <cybox:Associated_Object>
```

<cybox:Properties
xsi:type="WinRegistryKeyObj:WindowsRegistryKeyObjectType">
<WinRegistryKeyObj:Key>Software\Microsoft\Internet
Explorer</WinRegistryKeyObj:Key>
<WinRegistryKeyObj:Hive>HKCU</WinRegistryKeyObj:Hive>
<WinRegistryKeyObj:Values>
<WinRegistryKeyObj:Value>
<WinRegistryKeyObj:Name>Typed URLs</WinRegistryKeyObj:Name>
</WinRegistryKeyObj:Value>
</WinRegistryKeyObj:Values>
</cybox:Properties>
</cybox:Associated_Object>
</cybox:Associated_Objects>
</maecBundle:Action>
<maecBundle:Action id="get_passwords_cached">
<cybox:Name xsi:type="maecVocabs:RegistryActionNameVocab-1.0">read registry
key value</cybox:Name>
<cybox:Associated_Objects>
<cybox:Associated_Object>
<cybox:Properties
xsi:type="WinRegistryKeyObj:WindowsRegistryKeyObjectType">
<WinRegistryKeyObj:Key>Software\Microsoft\Internet
Explorer</WinRegistryKeyObj:Key>

```
    <WinRegistryKeyObj:Hive>HKCU</WinRegistryKeyObj:Hive>
    <WinRegistryKeyObj:Values>
     <WinRegistryKeyObj:Value>
      <WinRegistryKeyObj:Name>Cached Passwords</WinRegistryKeyObj:Name>
     </WinRegistryKeyObj:Value>
    </WinRegistryKeyObj:Values>
   </cybox:Properties>
  </cybox:Associated_Object>
 </cybox:Associated_Objects>
</maecBundle:Action>

<maecBundle:Action id="send_email_to_attacker">
 <cybox:Associated_Objects>
  <cybox:Associated_Object>
   <cybox:Properties xsi:type="EmailMessageObj:EmailMessageObjectType">
    <EmailMessageObj:Header>
     <EmailMessageObj:From>alien-z@mail.ru</EmailMessageObj:From>
     <EmailMessageObj:To>
      <EmailMessageObj:Recipient>imager@mail.ru</EmailMessageObj:Recipient>
     </EmailMessageObj:To>
    </EmailMessageObj:Header>
    <EmailMessageObj:Email_Server>smtp.mai.ru</EmailMessageObj:Email_Server>
    </cybox:Properties>
```

```
    </cybox:Associated_Object>
   </cybox:Associated_Objects>
  </maecBundle:Action>
 </maecBundle:Actions>

 <maecBundle:Candidate_Indicators>
  <!-- Capability CIs -->
  <maecBundle:Candidate_Indicator id="capabilties_id">
   <maecBundle:Composition operator="OR">

    <maecBundle:Sub_Composition operator="AND">
    <maecBundle:Capability_Reference capability_idref="persistence"/>
    <maecBundle:Capability_Reference
capability_idref="gather_system_info_and_send_to_attacker"/>
    </maecBundle:Sub_Composition>

    <maecBundle:Capability_Reference capability_idref="spread_across_system"/>

   </maecBundle:Composition>
  </maecBundle:Candidate_Indicator>

  <!-- Behaviour CIs -->
  <maecBundle:Candidate_Indicator id="persistence_id">
```

```
  <maecBundle:Composition operator="AND">
   <maecBundle:Behavior_Reference behavior_idref="persistence_at_runtime"/>
   <maecBundle:Behavior_Reference behavior_idref="persistence_on_disk"/>
   <maecBundle:Behavior_Reference
behavior_idref="persistence_against_process_shutdown"/>
  </maecBundle:Composition>
 </maecBundle:Candidate_Indicator>
 <maecBundle:Candidate_Indicator id="gather_system_info_and_send_to_attacker">
  <maecBundle:Composition operator="AND">
   <maecBundle:Behavior_Reference behavior_idref="gather_system_info"/>
   <maecBundle:Behavior_Reference behavior_idref="send_to_attacker"/>
  </maecBundle:Composition>
 </maecBundle:Candidate_Indicator>


 <!-- Action CIs -->
 <maecBundle:Candidate_Indicator id="copy_self_to_files">
  <maecBundle:Composition operator="AND">
   <maecBundle:Action_Reference action_id="enumerate_files"/>
   <maecBundle:Action_Reference action_id="infect_files"/>
  </maecBundle:Composition>
 </maecBundle:Candidate_Indicator>
 <maecBundle:Candidate_Indicator id="gather_system_info_id">
```

```
 <maecBundle:Composition operator="OR">
  <maecBundle:Action_Reference action_id="get_os_version"/>
  <maecBundle:Action_Reference action_id="get_computer_name"/>
  <maecBundle:Action_Reference action_id="get_user_name"/>
  <maecBundle:Action_Reference action_id="get_drive_type"/>
  <maecBundle:Action_Reference action_id="get_volume_info"/>

  <maecBundle:Action_Reference action_id="get_product_name"/>
  <maecBundle:Action_Reference action_id="get_product_version"/>
  <maecBundle:Action_Reference action_id="get_product_version_number"/>
  <maecBundle:Action_Reference action_id="get_registered_owner"/>
  <maecBundle:Action_Reference action_id="get_registered_organization"/>
  <maecBundle:Action_Reference action_id="get_program_files_dir"/>
  <maecBundle:Action_Reference action_id="get_urls_visited"/>
  <maecBundle:Action_Reference action_id="get_passwords_cached"/>
</maecBundle:Composition>
</maecBundle:Candidate_Indicator>

<!-- Object CIs -->
<maecBundle:Candidate_Indicator id="enumerate_files">
 <maecBundle:Composition operator="AND">
  <maecBundle:Object_Reference object_idref="find_file"/>
  <maecBundle:Object_Reference object_idref="file_type"/>
```

</maecBundle:Composition>

</maecBundle:Candidate_Indicator>

</maecBundle:Candidate_Indicators>

</maecBundle:MAEC_Bundle>

A.9 Shellcode_PDF_JS

<?xml version="1.0" encoding="UTF-8"?>

<maecBundle:MAEC_Bundle xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://cybox.mitre.org/objects#ArtifactObject-2 ../cybox_2.1_offline/objects/Artifact_Object.xsd http://cybox.mitre.org/objects#WinExecutableFileObject-2 ../cybox_2.1_offline/objects/Win_Executable_File_Object.xsd http://cybox.mitre.org/common-2 ../maec/maec_4.1_offline/cybox_2.1_offline/cybox_common.xsd http://maec.mitre.org/XMLSchema/maec-bundle-4 file:/Users/asheer.malhotra/Documents/TT/maec/maec_4.1_offline/maec_bundle_schema.xsd http://cybox.mitre.org/objects#WinExecutableFileObject-2 maec/maec_4.1_offline/cybox_2.1_offline/objects/Win_Executable_File_Object.xsd http://cybox.mitre.org/objects#PDFFileObject-1

maec/maec_4.1_offline/cybox_2.1_offline/objects/PDF_File_Object.xsd

http://cybox.mitre.org/objects#WinExecutableFileObject-2

../maec/maec_4.1_offline/cybox_2.1_offline/objects/Win_Executable_File_Object.xsd

http://cybox.mitre.org/default_vocabularies-2

../cybox_2.1_offline/cybox_default_vocabularies.xsd

http://cybox.mitre.org/objects#PDFFileObject-1

../cybox_2.1_offline/PDF_File_Object.xsd"

xmlns:HTTPSessionObj="http://cybox.mitre.org/objects#HTTPSessionObject-2"

xmlns:DNSQueryObj="http://cybox.mitre.org/objects#DNSQueryObject-2"

xmlns:maecBundle="http://maec.mitre.org/XMLSchema/maec-bundle-4"

xmlns:ProcessObj="http://cybox.mitre.org/objects#ProcessObject-2"

xmlns:SocketAddressObj="http://cybox.mitre.org/objects#SocketAddressObject-1"

xmlns:AddressObj="http://cybox.mitre.org/objects#AddressObject-2"

xmlns:NetworkConnectionObj="http://cybox.mitre.org/objects#NetworkConnectionObje

ct-2" xmlns:PDFFileObj="http://cybox.mitre.org/objects#PDFFileObject-1"

xmlns:cyboxVocabs="http://cybox.mitre.org/default_vocabularies-2"

xmlns:HostnameObj="http://cybox.mitre.org/objects#HostnameObject-1"

xmlns:CodeObj="http://cybox.mitre.org/objects#CodeObject-2"

xmlns:FileObj="http://cybox.mitre.org/objects#FileObject-2"

xmlns:DNSRecordObj="http://cybox.mitre.org/objects#DNSRecordObject-2"

xmlns:maecVocabs="http://maec.mitre.org/default_vocabularies-1"

xmlns:WinExecutableFileObj="http://cybox.mitre.org/objects#WinExecutableFileObject

-2" xmlns:cyboxCommon="http://cybox.mitre.org/common-2"

xmlns:URIObj="http://cybox.mitre.org/objects#URIObject-2"
xmlns:cybox="http://cybox.mitre.org/cybox-2"
xmlns:PortObj="http://cybox.mitre.org/objects#PortObject-2"
id="ShellcodePDFJS_Manual_Analysis" schema_version="4.1"
defined_subject="true">

<maecBundle:Malware_Instance_Object_Attributes>
<cybox:Description>The Malware is a PDF based sample that downloads binaries by exploting vulnerabilties of Adobe PDF Reader</cybox:Description>
<cybox:Properties xsi:type="PDFFileObj:PDFFileObjectType">
<FileObj:File_Extension>PDF</FileObj:File_Extension>
<FileObj:Size_In_Bytes>53214</FileObj:Size_In_Bytes>
<FileObj:Hashes>
<cyboxCommon:Hash>
<cyboxCommon:Type>MD5</cyboxCommon:Type>

<cyboxCommon:Simple_Hash_Value>b48ca8f2f3475f27d0693f98ff1080a4</cyboxCommon:Simple_Hash_Value>
</cyboxCommon:Hash>
</FileObj:Hashes>
</cybox:Properties>
</maecBundle:Malware_Instance_Object_Attributes>

```
<!-- Placeholder for capabilities -->
<maecBundle:Capabilities>
 <maecBundle:Capability id="drop_and_run_binaries" name="infection/propagation">

   <maecBundle:Behavior_Reference behavior_idref="CVE-2007-5659"/>
   <maecBundle:Behavior_Reference behavior_idref="CVE-2008-2992"/>
   <maecBundle:Behavior_Reference behavior_idref="CVE-2009-0927"/>



 </maecBundle:Capability>

</maecBundle:Capabilities>



<!-- Placeholder for behaviours -->
<maecBundle:Behaviors>

 <maecBundle:Behavior id="CVE-2007-5659">
  <maecBundle:Purpose>
   <maecBundle:Vulnerability_Exploit>
    <maecBundle:CVE cve_id="CVE-2007-5659"/>
    <maecBundle:Targeted_Platforms>
     <maecBundle:Platform xsi:type="cyboxCommon:PlatformSpecificationType">
```

<cyboxCommon:Identifier>Adobe Reader version gt or eq
8</cyboxCommon:Identifier>
</maecBundle:Platform>
<maecBundle:Platform xsi:type="cyboxCommon:PlatformSpecificationType">
<cyboxCommon:Identifier>Adobe Reader version lt
8.102</cyboxCommon:Identifier>
</maecBundle:Platform>
<maecBundle:Platform xsi:type="cyboxCommon:PlatformSpecificationType">
<cyboxCommon:Identifier>Adobe Reader version lt 7.1</cyboxCommon:Identifier>
</maecBundle:Platform>
</maecBundle:Targeted_Platforms>
</maecBundle:Vulnerability_Exploit>
</maecBundle:Purpose>
<maecBundle:Action_Composition>
<maecBundle:Action_Reference action_id="collab.CollectEmailInfo_Overflow"/>
<maecBundle:Action_Reference action_id="Run_shellcode"/>
</maecBundle:Action_Composition>

</maecBundle:Behavior>

<maecBundle:Behavior id="CVE-2008-2992">
<maecBundle:Purpose>
<maecBundle:Vulnerability_Exploit>

<maecBundle:CVE cve_id="CVE-2008-2992"/>

<maecBundle:Targeted_Platforms>

<maecBundle:Platform xsi:type="cyboxCommon:PlatformSpecificationType">

<cyboxCommon:Identifier>Adobe Reader version gt or eq 8.102</cyboxCommon:Identifier>

<cyboxCommon:Identifier> Adobe Reader version lt 8.104</cyboxCommon:Identifier>

</maecBundle:Platform>

<maecBundle:Platform xsi:type="cyboxCommon:PlatformSpecificationType">

<cyboxCommon:Identifier>Adobe Reader version gt or eq 9</cyboxCommon:Identifier>

<cyboxCommon:Identifier>Adobe Reader version lt 9.1</cyboxCommon:Identifier>

</maecBundle:Platform>

<maecBundle:Platform xsi:type="cyboxCommon:PlatformSpecificationType">

<cyboxCommon:Identifier>Adobe Reader version lt or eq 7.101</cyboxCommon:Identifier>

</maecBundle:Platform>

</maecBundle:Targeted_Platforms>

</maecBundle:Vulnerability_Exploit>

</maecBundle:Purpose>

<maecBundle:Action_Composition>

<maecBundle:Action_Reference action_id="util.printf_Overflow"/>

<maecBundle:Action_Reference action_id="Run_shellcode"/>

```
 </maecBundle:Action_Composition>
</maecBundle:Behavior>

<maecBundle:Behavior id="CVE-2009-0927">
 <maecBundle:Purpose>
 <maecBundle:Vulnerability_Exploit>
  <maecBundle:CVE cve_id="CVE-2009-0927"/>
  <maecBundle:Targeted_Platforms>
   <maecBundle:Platform xsi:type="cyboxCommon:PlatformSpecificationType">
    <cyboxCommon:Identifier>Adobe Reader version eq
8.102</cyboxCommon:Identifier>
   </maecBundle:Platform>
   <maecBundle:Platform xsi:type="cyboxCommon:PlatformSpecificationType">
    <cyboxCommon:Identifier>Adobe Reader version eq
7.1</cyboxCommon:Identifier>
   </maecBundle:Platform>
  </maecBundle:Targeted_Platforms>
 </maecBundle:Vulnerability_Exploit>
</maecBundle:Purpose>
<maecBundle:Action_Composition>
 <maecBundle:Action_Reference action_id="collab.GetIcon_Overflow"/>
 <maecBundle:Action_Reference action_id="Run_shellcode"/>
</maecBundle:Action_Composition>
```

```
 </maecBundle:Behavior>

</maecBundle:Behaviors>

<!-- Placeholder for actions -->
<maecBundle:Actions>
 <maecBundle:Action id="collab.CollectEmailInfo_Overflow"/>
 <maecBundle:Action id="util.printf_Overflow"/>
 <maecBundle:Action id="collab.GetIcon_Overflow"/>

 <maecBundle:Action id="Run_shellcode">

  <cybox:Description>Fetch and execute binary</cybox:Description>
  <cybox:Associated_Objects>
   <cybox:Associated_Object id="download_url">
    <cybox:Association_Type xsi:type="maecVocabs:NetworkActionNameVocab-
1.1">download file</cybox:Association_Type>
    <cybox:Properties xsi:type="URIObj:URIObjectType">
     <URIObj:Value>http://grobin1.cn/pol/update.php?id=[3,5]</URIObj:Value>
    </cybox:Properties>

   </cybox:Associated_Object>
```

```
    <cybox:Associated_Object id="malware_binary">
     <cybox:Association_Type xsi:type="maecVocabs:FileActionNameVocab-
1.1">execute file</cybox:Association_Type>
     <cybox:Properties
xsi:type="WinExecutableFileObj:WindowsExecutableFileObjectType">
      <FileObj:File_Name>itLatinTheory.exe OR
beenLoremCities.exe</FileObj:File_Name>
      </cybox:Properties>
     </cybox:Associated_Object>

   </cybox:Associated_Objects>
  </maecBundle:Action>
 </maecBundle:Actions>


 <maecBundle:Candidate_Indicators>
  <maecBundle:Candidate_Indicator id="drop_and_run_binaries_id">
   <maecBundle:Composition operator="OR">
    <maecBundle:Behavior_Reference behavior_idref="CVE-2007-5659"/>
    <maecBundle:Behavior_Reference behavior_idref="CVE-2008-2992"/>
    <maecBundle:Behavior_Reference behavior_idref="CVE-20090927"/>
   </maecBundle:Composition>
  </maecBundle:Candidate_Indicator>
```

```
<maecBundle:Candidate_Indicator id="CVE-2007-5659_id">
 <maecBundle:Composition operator="AND">
  <maecBundle:Action_Reference action_id="collab.CollectEmailInfo_Overflow"/>
  <maecBundle:Action_Reference action_id="Run_shellcode"/>
 </maecBundle:Composition>
</maecBundle:Candidate_Indicator>

<maecBundle:Candidate_Indicator id="CVE-2008-2992_id">
  <maecBundle:Composition operator="AND">
   <maecBundle:Action_Reference action_id="util.printf_Overflow"/>
   <maecBundle:Action_Reference action_id="Run_shellcode"/>
  </maecBundle:Composition>
 </maecBundle:Candidate_Indicator>

<maecBundle:Candidate_Indicator id="CVE-20090927_id">
   <maecBundle:Composition operator="AND">
    <maecBundle:Action_Reference action_id="collab.GetIcon_Overflow"/>
    <maecBundle:Action_Reference action_id="Run_shellcode"/>
   </maecBundle:Composition>
  </maecBundle:Candidate_Indicator>

 <maecBundle:Candidate_Indicator id="run_shellcode_id">
```

<maecBundle:Composition operator="AND">

<maecBundle:Object_Reference object_idref="download_url"/>

<maecBundle:Object_Reference object_idref="malware_binary"/>

</maecBundle:Composition>

</maecBundle:Candidate_Indicator>

</maecBundle:Candidate_Indicators>

</maecBundle:MAEC_Bundle>

A.10 Xorer.F

<?xml version="1.0" encoding="UTF-8"?>

<maecBundle:MAEC_Bundle xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"

xsi:schemaLocation="http://cybox.mitre.org/objects#ArtifactObject-2 maec/maec_4.1_offline/cybox_2.1_offline/objects/Artifact_Object.xsd

http://cybox.mitre.org/objects#WinRegistryKeyObject-2 maec/maec_4.1_offline/cybox_2.1_offline/objects/Win_Registry_Key_Object.xsd

http://cybox.mitre.org/objects#WinExecutableFileObject-2 maec/maec_4.1_offline/cybox_2.1_offline/objects/Win_Executable_File_Object.xsd

http://cybox.mitre.org/common-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/cybox_common.xsd

http://cybox.mitre.org/objects#APIObject-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/API_Object.xsd

http://maec.mitre.org/XMLSchema/maec-bundle-4

maec/maec_4.1_offline/maec_bundle_schema.xsd

http://cybox.mitre.org/objects#WinExecutableFileObject-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/Win_Executable_File_Object.xsd

http://cybox.mitre.org/objects#PDFFileObject-1

maec/maec_4.1_offline/cybox_2.1_offline/objects/PDF_File_Object.xsd

http://cybox.mitre.org/objects#APIObject-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/API_Object.xsd

http://cybox.mitre.org/objects#WinExecutableFileObject-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/Win_Executable_File_Object.xsd

http://cybox.mitre.org/default_vocabularies-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/cybox_default_vocabularies.xsd

http://cybox.mitre.org/objects#PDFFileObject-1

maec/maec_4.1_offline/cybox_2.1_offline/objects/PDF_File_Object.xsd

http://cybox.mitre.org/objects#WinRegistryKeyObject-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/Win_Registry_key_Object.xsd

http://cybox.mitre.org/objects#WinMutexObject-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/Win_Mutex_Object.xsd

http://cybox.mitre.org/objects#ArtifactObject-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/Artifact_Object.xsd

http://cybox.mitre.org/objects#EmailMessageObject-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/Email_Message_Object.xsd

http://cybox.mitre.org/objects#MutexObject-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/Mutex_Object.xsd

"

xmlns:HTTPSessionObj="http://cybox.mitre.org/objects#HTTPSessionObject-2"

xmlns:DNSQueryObj="http://cybox.mitre.org/objects#DNSQueryObject-2"

xmlns:maecBundle="http://maec.mitre.org/XMLSchema/maec-bundle-4"

xmlns:ProcessObj="http://cybox.mitre.org/objects#ProcessObject-2"

xmlns:SocketAddressObj="http://cybox.mitre.org/objects#SocketAddressObject-1"

xmlns:AddressObj="http://cybox.mitre.org/objects#AddressObject-2"

xmlns:NetworkConnectionObj="http://cybox.mitre.org/objects#NetworkConnectionObje

ct-2"

xmlns:PDFFileObj="http://cybox.mitre.org/objects#PDFFileObject-1"

xmlns:cyboxVocabs="http://cybox.mitre.org/default_vocabularies-2"

xmlns:HostnameObj="http://cybox.mitre.org/objects#HostnameObject-1"

xmlns:CodeObj="http://cybox.mitre.org/objects#CodeObject-2"

xmlns:FileObj="http://cybox.mitre.org/objects#FileObject-2"

xmlns:DNSRecordObj="http://cybox.mitre.org/objects#DNSRecordObject-2"

xmlns:WinRegistryKeyObj="http://cybox.mitre.org/objects#WinRegistryKeyObject-2"

xmlns:maecVocabs="http://maec.mitre.org/default_vocabularies-1"

xmlns:APIObj="http://cybox.mitre.org/objects#APIObject-2"

xmlns:WinExecutableFileObj="http://cybox.mitre.org/objects#WinExecutableFileObject-2"

xmlns:cyboxCommon="http://cybox.mitre.org/common-2"

xmlns:URIObj="http://cybox.mitre.org/objects#URIObject-2"

xmlns:cybox="http://cybox.mitre.org/cybox-2"

xmlns:WinMutexObj="http://cybox.mitre.org/objects#WinMutexObject-2"

xmlns:ArtifactObj="http://cybox.mitre.org/objects#ArtifactObject-2"

xmlns:EmailMessageObj="http://cybox.mitre.org/objects#EmailMessageObject-2"

xmlns:MutexObj="http://cybox.mitre.org/objects#MutexObject-2"

id="Xorer_exe_TT" schema_version="4.1"

defined_subject="true">

<maecBundle:Malware_Instance_Object_Attributes>

<cybox:Description>The Malware is an EXE sample that infects files and performs other data stealing activities</cybox:Description>

<cybox:Properties

xsi:type="WinExecutableFileObj:WindowsExecutableFileObjectType">

<FileObj:File_Extension>EXE</FileObj:File_Extension>

<FileObj:Size_In_Bytes>258263</FileObj:Size_In_Bytes>

<FileObj:Hashes>

<cyboxCommon:Hash>

<cyboxCommon:Type>MD5</cyboxCommon:Type>

<cyboxCommon:Simple_Hash_Value>010bc5418ed1efc19ceb0fe9f71d83a1</cyboxCo
mmon:Simple_Hash_Value>
</cyboxCommon:Hash>
</FileObj:Hashes>
</cybox:Properties>
</maecBundle:Malware_Instance_Object_Attributes>

<!-- Placeholder for capabilities -->
<maecBundle:Capabilities>

<maecBundle:Capability id="persistence" name="persistence">
<maecBundle:Behavior_Reference behavior_idref="persistence_at_runtime"/>
<maecBundle:Behavior_Reference behavior_idref="persistence_on_disk"/>
<maecBundle:Behavior_Reference behavior_idref="persistence_across_reboots"/>
</maecBundle:Capability>
<maecBundle:Capability id="spread_across_system" name="infection/propagation">
<maecBundle:Behavior_Reference behavior_idref="copy_self_to_exe_files"/>
<maecBundle:Behavior_Reference behavior_idref="copy_self_to_zipped_exe_files"/>
<maecBundle:Behavior_Reference behavior_idref="copy_self_to_removable_drives"/>
<maecBundle:Behavior_Reference behavior_idref="copy_code_to_html_files"/>
</maecBundle:Capability>

<maecBundle:Capability id="run_arbitrary_commands" name="command and control">
<maecBundle:Behavior_Reference behavior_idref="fetch_commands"/>
<maecBundle:Behavior_Reference behavior_idref="execute_commands_recieved"/>
</maecBundle:Capability>
<maecBundle:Capability id="downgrade_system_security_level" name="security degradation">
<maecBundle:Behavior_Reference behavior_idref="kill_av_processes"/>
<maecBundle:Behavior_Reference behavior_idref="modify_acli_settings"/>
<maecBundle:Behavior_Reference behavior_idref="prevent_process_run_on_startup"/>
<maecBundle:Behavior_Reference behavior_idref="modify_registry_settings"/>
</maecBundle:Capability>

</maecBundle:Capabilities>

<!-- Placeholder for behaviours -->
<maecBundle:Behaviors>
<maecBundle:Behavior id="persistence_at_runtime">
<maecBundle:Action_Composition>
<maecBundle:Action_Reference action_id="create_mutex_random_name"/>
<maecBundle:Action_Reference action_id="create_mutex_xcgucvnzn"/>
<maecBundle:Action_Reference action_id="create_mutex_BLAIPBOFFCNJ"/>

```
 </maecBundle:Action_Composition>
</maecBundle:Behavior>
<maecBundle:Behavior id="persistence_on_disk">
 <maecBundle:Action_Composition>
  <maecBundle:Action_Reference action_id="enumerate_files"/>
  <maecBundle:Action_Reference action_id="copy_self_to_new_log_files"/>
  <maecBundle:Action_Reference action_id="copy_self_to_new_exe_files"/>
 </maecBundle:Action_Composition>
</maecBundle:Behavior>
<maecBundle:Behavior id="persistence_across_reboots">
 <maecBundle:Action_Composition>
  <maecBundle:Action_Reference action_id="copy_self_to_new_dll"/>
  <maecBundle:Action_Reference action_id="copy_self_to_new_sys"/>
  <maecBundle:Action_Reference action_id="register_sys_as_service"/>
 </maecBundle:Action_Composition>
</maecBundle:Behavior>

<maecBundle:Behavior id="copy_self_to_exe_files">
 <maecBundle:Action_Composition>
  <maecBundle:Action_Reference action_id="enumerate_files"/>
  <maecBundle:Action_Reference action_id="infect_exe_files"/>
  </maecBundle:Action_Composition>
</maecBundle:Behavior>
```

<maecBundle:Behavior id="copy_self_to_zipped_exe_files">
<maecBundle:Action_Composition>
<maecBundle:Action_Reference action_id="enumerate_files"/>
<maecBundle:Action_Reference action_id="extract_files_using_winrar"/>
<maecBundle:Action_Reference action_id="infect_exe_files"/>
</maecBundle:Action_Composition>
</maecBundle:Behavior>
<maecBundle:Behavior id="copy_self_to_removable_drives">
<maecBundle:Action_Composition>
<maecBundle:Action_Reference action_id="copy_self_to_pagefile"/>
<maecBundle:Action_Reference action_id="configure_autorun"/>
<maecBundle:Action_Reference
action_id="enable_autorun_for_all_drives_registry"/>
</maecBundle:Action_Composition>
</maecBundle:Behavior>
<maecBundle:Behavior id="copy_code_to_html_files">
<maecBundle:Action_Composition>
<maecBundle:Action_Reference action_id="enumerate_htm_files"/>
<maecBundle:Action_Reference action_id="embed_file_with_htm_tags"/>
</maecBundle:Action_Composition>
</maecBundle:Behavior>

<maecBundle:Behavior id="fetch_commands">

<maecBundle:Action_Composition>

<maecBundle:Action_Reference action_id="fetch_commands_from_cnc"/>

</maecBundle:Action_Composition>

</maecBundle:Behavior>

<maecBundle:Behavior id="execute_commands_recieved">

<maecBundle:Action_Composition>

<maecBundle:Action_Reference action_id="start_process"/>

<maecBundle:Action_Reference action_id="terminate_process"/>

</maecBundle:Action_Composition>

</maecBundle:Behavior>

<maecBundle:Behavior id="kill_av_processes">

<maecBundle:Action_Composition>

<maecBundle:Action_Reference action_id="list_processes"/>

<maecBundle:Action_Reference action_id="kill_rav"/>

<maecBundle:Action_Reference action_id="kill_avp"/>

<maecBundle:Action_Reference action_id="kill_twister"/>

<maecBundle:Action_Reference action_id="kill_kv"/>

<maecBundle:Action_Reference action_id="kill_watch"/>

<maecBundle:Action_Reference action_id="kill_kissvc"/>

<maecBundle:Action_Reference action_id="kill_scan"/>

<maecBundle:Action_Reference action_id="kill_guard"/>

<maecBundle:Action_Reference action_id="kill_kmailmon"/>

```
 </maecBundle:Action_Composition>
</maecBundle:Behavior>
<maecBundle:Behavior id="modify_acli_settings">
 <maecBundle:Action_Composition>
  <maecBundle:Action_Reference action_id="cacls_grant_full_access"/>
 </maecBundle:Action_Composition>
</maecBundle:Behavior>
<maecBundle:Behavior id="prevent_process_run_on_startup">
 <maecBundle:Action_Composition>
  <maecBundle:Action_Reference action_id="remove_from_registry_ksysmon"/>
  <maecBundle:Action_Reference action_id="remove_from_registry_eqservice"/>
  <maecBundle:Action_Reference action_id="remove_from_registry_rsravmon"/>
  <maecBundle:Action_Reference action_id="remove_from_registry_mcshield"/>
  <maecBundle:Action_Reference action_id="remove_from_registry_tmmbd"/>
  <maecBundle:Action_Reference action_id="remove_from_registry_pavsrv"/>
  <maecBundle:Action_Reference action_id="remove_from_registry_symevent"/>
  <maecBundle:Action_Reference action_id="remove_from_registry_ekrn"/>
  <maecBundle:Action_Reference action_id="remove_from_registry_kwatchsvc"/>
  <maecBundle:Action_Reference action_id="remove_from_registry_avp"/>
  <maecBundle:Action_Reference action_id="remove_from_registry_antivirservice"/>
  <maecBundle:Action_Reference action_id="remove_from_registry_mpsvcservice"/>
 </maecBundle:Action_Composition>
</maecBundle:Behavior>
```

<maecBundle:Behavior id="modify_registry_settings">
<maecBundle:Action_Composition>
<maecBundle:Action_Reference
action_id="disable_safe_mode_boot_with_network"/>
<maecBundle:Action_Reference
action_id="disable_safe_mode_boot_without_network"/>
<maecBundle:Action_Reference action_id="delete_image_file_execution_options"/>
<maecBundle:Action_Reference action_id="delete_group_policy_objects"/>
<maecBundle:Action_Reference
action_id="disable_show_super_hidden_objects_option"/>
</maecBundle:Action_Composition>
</maecBundle:Behavior>

</maecBundle:Behaviors>

<!-- Placeholder for actions -->
<maecBundle:Actions>
<maecBundle:Action id="create_mutex_random_name">
<cybox:Name xsi:type="maecVocabs:SynchronizationActionNameVocab-1.0">create
mutex</cybox:Name>
<cybox:Associated_Objects>
<cybox:Associated_Object>
<cybox:Properties xsi:type="MutexObj:MutexObjectType" named="true">

<MutexObj:Name>[a-z]*[A-Z]*[0-9]*</MutexObj:Name>

</cybox:Properties>

</cybox:Associated_Object>

</cybox:Associated_Objects>

</maecBundle:Action>

<maecBundle:Action id="create_mutex_xcgucvnzn">

<cybox:Name xsi:type="maecVocabs:SynchronizationActionNameVocab-1.0">create mutex</cybox:Name>

<cybox:Associated_Objects>

<cybox:Associated_Object>

<cybox:Properties xsi:type="MutexObj:MutexObjectType" named="true">

<MutexObj:Name>xcgucvnzn</MutexObj:Name>

</cybox:Properties>

</cybox:Associated_Object>

</cybox:Associated_Objects>

</maecBundle:Action>

<maecBundle:Action id="create_mutex_BLAIPBOFFCNJ">

<cybox:Name xsi:type="maecVocabs:SynchronizationActionNameVocab-1.0">create mutex</cybox:Name>

<cybox:Associated_Objects>

<cybox:Associated_Object>

<cybox:Properties xsi:type="MutexObj:MutexObjectType" named="true">

<MutexObj:Name>BLAIPBOFFCNJ</MutexObj:Name>

```
    </cybox:Properties>
   </cybox:Associated_Object>
  </cybox:Associated_Objects>
 </maecBundle:Action>

 <maecBundle:Action id="enumerate_files">
  <cybox:Name xsi:type="maecVocabs:FileActionNameVocab-1.1">find
file</cybox:Name>
  <cybox:Associated_Objects>
   <cybox:Associated_Object id="find_file">
    <cybox:Properties xsi:type="APIObj:APIObjectType">
     <APIObj:Function_Name>FindFirstFileA</APIObj:Function_Name>
    </cybox:Properties>
   </cybox:Associated_Object>
  </cybox:Associated_Objects>
 </maecBundle:Action>

 <maecBundle:Action id="copy_self_to_new_log_files">
  <cybox:Name xsi:type="maecVocabs:FileActionNameVocab-1.1">create
file</cybox:Name>
  <cybox:Associated_Objects>
   <cybox:Associated_Object>
    <cybox:Description> the malware creates a copy of itself in the
```

directory</cybox:Description>
<cybox:Properties
xsi:type="WinExecutableFileObj:WindowsExecutableFileObjectType">
<FileObj:File_Name>[0-9][0-9][0-9][0-9][0-9][0-9].log</FileObj:File_Name>
<FileObj:File_Path>c:\bak</FileObj:File_Path>
<FileObj:File_Extension>log</FileObj:File_Extension>
</cybox:Properties>
</cybox:Associated_Object>
</cybox:Associated_Objects>
</maecBundle:Action>
<maecBundle:Action id="copy_self_to_new_exe_files">
<cybox:Name xsi:type="maecVocabs:FileActionNameVocab-1.1">create
file</cybox:Name>
<cybox:Associated_Objects>
<cybox:Associated_Object>
<cybox:Description> the malware creates a copy of itself in the
directory</cybox:Description>
<cybox:Properties
xsi:type="WinExecutableFileObj:WindowsExecutableFileObjectType">
<FileObj:File_Extension>exe</FileObj:File_Extension>
</cybox:Properties>
</cybox:Associated_Object>
</cybox:Associated_Objects>

```
  </maecBundle:Action>


  <maecBundle:Action id="copy_self_to_new_dll">
   <cybox:Name xsi:type="maecVocabs:FileActionNameVocab-1.1">create
file</cybox:Name>
   <cybox:Associated_Objects>
    <cybox:Associated_Object>
     <cybox:Properties
xsi:type="WinExecutableFileObj:WindowsExecutableFileObjectType">
      <FileObj:File_Name>netapi000.dll</FileObj:File_Name>
      <FileObj:File_Path>%sysdir%</FileObj:File_Path>
      <FileObj:File_Extension>dll</FileObj:File_Extension>
     </cybox:Properties>
    </cybox:Associated_Object>
   </cybox:Associated_Objects>
  </maecBundle:Action>
  <maecBundle:Action id="copy_self_to_new_sys">
   <cybox:Name xsi:type="maecVocabs:FileActionNameVocab-1.1">create
file</cybox:Name>
   <cybox:Associated_Objects>
    <cybox:Associated_Object>
     <cybox:Properties
xsi:type="WinExecutableFileObj:WindowsExecutableFileObjectType">
```

<FileObj:File_Name>netapi000.sys</FileObj:File_Name>

<FileObj:File_Path>%sysdir%</FileObj:File_Path>

<FileObj:File_Extension>sys</FileObj:File_Extension>

</cybox:Properties>

</cybox:Associated_Object>

</cybox:Associated_Objects>

</maecBundle:Action>

<maecBundle:Action id="register_sys_as_service">

<cybox:Name xsi:type="maecVocabs:RegistryActionNameVocab-1.0">create registry key value</cybox:Name>

<cybox:Associated_Objects>

<cybox:Associated_Object>

<cybox:Properties xsi:type="WinRegistryKeyObj:WindowsRegistryKeyObjectType">

<WinRegistryKeyObj:Key>System\CurrentControlSet\Services\NetAPI000</WinRegistryKeyObj:Key>

<WinRegistryKeyObj:Hive>HKLM</WinRegistryKeyObj:Hive>

<WinRegistryKeyObj:Values>

<WinRegistryKeyObj:Value>%sysdir%\netAPI000.sys</WinRegistryKeyObj:Value>

</WinRegistryKeyObj:Values>

</cybox:Properties>

```
  </cybox:Associated_Object>
 </cybox:Associated_Objects>
</maecBundle:Action>
<maecBundle:Action id="infect_exe_files">
 <cybox:Associated_Objects>
  <cybox:Associated_Object id="WriteFile">
   <cybox:Properties xsi:type="APIObj:APIObjectType">
    <APIObj:Function_Name>fwrite</APIObj:Function_Name>
   </cybox:Properties>
  </cybox:Associated_Object>
 </cybox:Associated_Objects>
</maecBundle:Action>

<maecBundle:Action id="extract_files_using_winrar">
 <cybox:Associated_Objects>
  <cybox:Associated_Object>
   <cybox:Description> runs winrar using ShellExecute</cybox:Description>
   <cybox:Properties xsi:type="APIObj:APIObjectType">
    <APIObj:Function_Name>ShellExecute</APIObj:Function_Name>
   </cybox:Properties>
  </cybox:Associated_Object>
 </cybox:Associated_Objects>
</maecBundle:Action>
```

<maecBundle:Action id="copy_self_to_pagefile">
<cybox:Associated_Objects>
<cybox:Associated_Object>
<cybox:Association_Type xsi:type="maecVocabs:FileActionNameVocab-1.1">create file</cybox:Association_Type>
<cybox:Properties xsi:type="FileObj:FileObjectType">
<FileObj:File_Name>pagefile.pif</FileObj:File_Name>
</cybox:Properties>
</cybox:Associated_Object>
</cybox:Associated_Objects>
</maecBundle:Action>
<maecBundle:Action id="configure_autorun">
<cybox:Associated_Objects>
<cybox:Associated_Object>
<cybox:Association_Type xsi:type="maecVocabs:FileActionNameVocab-1.1">modify file</cybox:Association_Type>
<cybox:Properties xsi:type="FileObj:FileObjectType">
<FileObj:File_Name>autorun.inf</FileObj:File_Name>
</cybox:Properties>
</cybox:Associated_Object>
</cybox:Associated_Objects>
</maecBundle:Action>

```
  <maecBundle:Action id="enable_autorun_for_all_drives_registry">
   <cybox:Associated_Objects>
    <cybox:Associated_Object>
     <cybox:Properties
xsi:type="WinRegistryKeyObj:WindowsRegistryKeyObjectType">

<WinRegistryKeyObj:Key>SOFTWARE\Microsoft\Windows\CurrentVersion\policies\E
xplorer\NoDriveTypeAutorun</WinRegistryKeyObj:Key>
      <WinRegistryKeyObj:Hive>HKCU</WinRegistryKeyObj:Hive>
      <WinRegistryKeyObj:Values>
       <WinRegistryKeyObj:Value>0x00</WinRegistryKeyObj:Value>
      </WinRegistryKeyObj:Values>
     </cybox:Properties>
    </cybox:Associated_Object>
   </cybox:Associated_Objects>
  </maecBundle:Action>

  <maecBundle:Action id="enumerate_htm_files">
   <cybox:Name xsi:type="maecVocabs:FileActionNameVocab-1.1">find
file</cybox:Name>
   <cybox:Description>find htm files</cybox:Description>
   <cybox:Associated_Objects>
    <cybox:Properties xsi:type="APIObj:APIObjectType">
```

<APIObj:Function_Name>FindFirstFileA</APIObj:Function_Name>

</cybox:Properties>

</cybox:Associated_Object>

</cybox:Associated_Objects>

</maecBundle:Action>

<maecBundle:Action id="embed_file_with_htm_tags">

<cybox:Name xsi:type="maecVocabs:FileActionNameVocab-1.0">modify file</cybox:Name>

<cybox:Associated_Objects>

<cybox:Associated_Object id="htm_file">

<cybox:Properties xsi:type="FileObj:FileObjectType">

<FileObj:File_Name>*.htm</FileObj:File_Name>

</cybox:Properties>

</cybox:Associated_Object>

<cybox:Associated_Object id="script_code">

<cybox:Properties xsi:type="CodeObj:CodeObjectType">

<CodeObj:Code_Language>html/js</CodeObj:Code_Language>

<CodeObj:Digital_Signatures>

<cyboxCommon:Digital_Signature>*ScRiPt src=*</cyboxCommon:Digital_Signature>

<cyboxCommon:Digital_Signature>*/sCrIpT*</cyboxCommon:Digital_Signature>

<cyboxCommon:Digital_Signature>*script src=*</cyboxCommon:Digital_Signature>

<cyboxCommon:Digital_Signature>http://%6A%73%2E%6B%30%31%30%32%2E%6
3%6F%6D/%30%31%2E%61%73%70</cyboxCommon:Digital_Signature>
</CodeObj:Digital_Signatures>
</cybox:Properties>
</cybox:Associated_Object>
</cybox:Associated_Objects>
</maecBundle:Action>

<maecBundle:Action id="fetch_commands_from_cnc">
<cybox:Associated_Objects>
<cybox:Associated_Object id="cnc_url_1">
<cybox:Properties xsi:type="HTTPSessionObj:HTTPSessionObjectType">
<HTTPSessionObj:HTTP_Request_Response>
<HTTPSessionObj:HTTP_Client_Request>
<HTTPSessionObj:HTTP_Request_Line>
<HTTPSessionObj:HTTP_Method>GET</HTTPSessionObj:HTTP_Method>

<HTTPSessionObj:Value>http://jj.gxgxy.net/html/qb2.html</HTTPSessionObj:Value>
</HTTPSessionObj:HTTP_Request_Line>
</HTTPSessionObj:HTTP_Client_Request>
</HTTPSessionObj:HTTP_Request_Response>
</cybox:Properties>

```
  </cybox:Associated_Object>
  <cybox:Associated_Object id="cnc_url_2">
   <cybox:Properties xsi:type="HTTPSessionObj:HTTPSessionObjectType">
    <HTTPSessionObj:HTTP_Request_Response>
     <HTTPSessionObj:HTTP_Client_Request>
      <HTTPSessionObj:HTTP_Request_Line>
       <HTTPSessionObj:HTTP_Method>GET</HTTPSessionObj:HTTP_Method>

<HTTPSessionObj:Value>http://jj.gxgxy.net/html/dg2.html</HTTPSessionObj:Value>
      </HTTPSessionObj:HTTP_Request_Line>
     </HTTPSessionObj:HTTP_Client_Request>
    </HTTPSessionObj:HTTP_Request_Response>
   </cybox:Properties>
  </cybox:Associated_Object>
 </cybox:Associated_Objects>
</maecBundle:Action>

<maecBundle:Action id="start_process">
 <cybox:Associated_Objects>
  <cybox:Associated_Object id="CreateProcess_API">
   <cybox:Properties xsi:type="APIObj:APIObjectType">
    <APIObj:Function_Name>CreateProcess</APIObj:Function_Name>
   </cybox:Properties>
```

```
  </cybox:Associated_Object>
 </cybox:Associated_Objects>
</maecBundle:Action>
<maecBundle:Action id="terminate_process">
 <cybox:Associated_Objects>
  <cybox:Associated_Object id="TerminateProcess">
   <cybox:Properties xsi:type="APIObj:APIObjectType">
    <APIObj:Function_Name>TerminateProcess</APIObj:Function_Name>
   </cybox:Properties>
  </cybox:Associated_Object>
 </cybox:Associated_Objects>
</maecBundle:Action>

<maecBundle:Action id="list_processes">
 <cybox:Associated_Objects>
  <cybox:Associated_Object id="process_list">
   <cybox:Properties xsi:type="APIObj:APIObjectType">
    <APIObj:Function_Name>CreateToolhelp32Snapshot</APIObj:Function_Name>
   </cybox:Properties>
  </cybox:Associated_Object>
 </cybox:Associated_Objects>
</maecBundle:Action>
```

<maecBundle:Action id="kill_rav">

<cybox:Description> kil process named rav </cybox:Description>

<cyox:Associated_Objects>

<cybox:Associated_Object id="TerminateProcess">

<cybox:Properties xsi:type="APIObj:APIObjectType">

<APIObj:Function_Name>TerminateProcess</APIObj:Function_Name>

</cybox:Properties>

<cybox:Associated_Object>

</cybox:Associated_Object>

</cyox:Associated_Objects>

</maecBundle:Action>

<maecBundle:Action id="kill_avp">

<cybox:Description> kil process named a </cybox:Description>

<cyox:Associated_Objects>

<cybox:Associated_Object id="TerminateProcess">

<cybox:Properties xsi:type="APIObj:APIObjectType">

<APIObj:Function_Name>TerminateProcess</APIObj:Function_Name>

</cybox:Properties>

<cybox:Associated_Object>

</cybox:Associated_Object>

</cyox:Associated_Objects>

</maecBundle:Action>

<maecBundle:Action id="kill_kv">

<cybox:Description> kil process named kv </cybox:Description>

<cyox:Associated_Objects>

<cybox:Associated_Object id="TerminateProcess">

<cybox:Properties xsi:type="APIObj:APIObjectType">

<APIObj:Function_Name>TerminateProcess</APIObj:Function_Name>

</cybox:Properties>

<cybox:Associated_Object>

</cybox:Associated_Object>

</cyox:Associated_Objects>

</maecBundle:Action>

<maecBundle:Action id="kill_watch">

<cybox:Description> kil process named watch </cybox:Description>

<cyox:Associated_Objects>

<cybox:Associated_Object id="TerminateProcess">

<cybox:Properties xsi:type="APIObj:APIObjectType">

<APIObj:Function_Name>TerminateProcess</APIObj:Function_Name>

</cybox:Properties>

<cybox:Associated_Object>

</cybox:Associated_Object>

</cyox:Associated_Objects>

</maecBundle:Action>

<maecBundle:Action id="kill_kissvc">

<cybox:Description> kil process named rav </cybox:Description>

<cyox:Associated_Objects>

<cybox:Associated_Object id="TerminateProcess">

<cybox:Properties xsi:type="APIObj:APIObjectType">

<APIObj:Function_Name>TerminateProcess</APIObj:Function_Name>

</cybox:Properties>

<cybox:Associated_Object>

</cybox:Associated_Object>

</cyox:Associated_Objects>

</maecBundle:Action>

<maecBundle:Action id="kill_scan">

<cybox:Description> kil process named rav </cybox:Description>

<cyox:Associated_Objects>

<cybox:Associated_Object id="TerminateProcess">

<cybox:Properties xsi:type="APIObj:APIObjectType">

<APIObj:Function_Name>TerminateProcess</APIObj:Function_Name>

</cybox:Properties>

<cybox:Associated_Object>

</cybox:Associated_Object>

</cyox:Associated_Objects>

</maecBundle:Action>

<maecBundle:Action id="kill_guard">

<cybox:Description> kil process named rav </cybox:Description>

<cyox:Associated_Objects>

<cybox:Associated_Object id="TerminateProcess">

<cybox:Properties xsi:type="APIObj:APIObjectType">

<APIObj:Function_Name>TerminateProcess</APIObj:Function_Name>

</cybox:Properties>

<cybox:Associated_Object>

</cybox:Associated_Object>

</cyox:Associated_Objects>

</maecBundle:Action>

<maecBundle:Action id="kill_kmailmon">

<cybox:Description> kil process named rav </cybox:Description>

<cyox:Associated_Objects>

<cybox:Associated_Object id="TerminateProcess">

<cybox:Properties xsi:type="APIObj:APIObjectType">

<APIObj:Function_Name>TerminateProcess</APIObj:Function_Name>

</cybox:Properties>

<cybox:Associated_Object>

</cybox:Associated_Object>

</cyox:Associated_Objects>

</maecBundle:Action>

<maecBundle:Action id="cacls_grant_full_access">

<cybox:Associated_Objects>

<cybox:Associated_Object>

<cybox:Properties xsi:type="FileObj:FileObjectType">

<FileObj:Full_Path>cacls.exe /e /t /g Everyone:F</FileObj:Full_Path>

</cybox:Properties>

</cybox:Associated_Object>

</cybox:Associated_Objects>

</maecBundle:Action>

<maecBundle:Action id="remove_from_registry_ksysmon">

<cybox:Name xsi:type="maecVocabs:RegistryActionNameVocab-1.0">delete registry key value</cybox:Name>

<cybox:Associated_Objects>

<cybox:Associated_Object>

<cybox:Properties xsi:type="WinRegistryKeyObj:WindowsRegistryKeyObjectType">

<WinRegistryKeyObj:Key>SYSTEM\CurrentControlSet\Services\KSysMon</WinRegistryKeyObj:Key>

<WinRegistryKeyObj:Hive>HKLM</WinRegistryKeyObj:Hive>

</cybox:Properties>

</cybox:Associated_Object>

</cybox:Associated_Objects>

</maecBundle:Action>

<maecBundle:Action id="remove_from_registry_eqservice">

<cybox:Name xsi:type="maecVocabs:RegistryActionNameVocab-1.0">delete registry key value</cybox:Name>
<cybox:Associated_Objects>
<cybox:Associated_Object>
<cybox:Properties xsi:type="WinRegistryKeyObj:WindowsRegistryKeyObjectType">

<WinRegistryKeyObj:Key>SYSTEM\CurrentControlSet\Services\KSysMon</WinRegistryKeyObj:Key>
<WinRegistryKeyObj:Hive>HKLM</WinRegistryKeyObj:Hive>
</cybox:Properties>
</cybox:Associated_Object>
</cybox:Associated_Objects>
</maecBundle:Action>
<maecBundle:Action id="remove_from_registry_rsravmon">
<cybox:Name xsi:type="maecVocabs:RegistryActionNameVocab-1.0">delete registry key value</cybox:Name>
<cybox:Associated_Objects>
<cybox:Associated_Object>
<cybox:Properties xsi:type="WinRegistryKeyObj:WindowsRegistryKeyObjectType">

<WinRegistryKeyObj:Key>SYSTEM\CurrentControlSet\Services\RsRavMon</WinRegi

stryKeyObj:Key>
<WinRegistryKeyObj:Hive>HKLM</WinRegistryKeyObj:Hive>
</cybox:Properties>
</cybox:Associated_Object>
</cybox:Associated_Objects>
</maecBundle:Action>
<maecBundle:Action id="remove_from_registry_mcshield">
<cybox:Name xsi:type="maecVocabs:RegistryActionNameVocab-1.0">delete registry key value</cybox:Name>
<cybox:Associated_Objects>
<cybox:Associated_Object>
<cybox:Properties xsi:type="WinRegistryKeyObj:WindowsRegistryKeyObjectType">

<WinRegistryKeyObj:Key>SYSTEM\CurrentControlSet\Services\McShield</WinRegistryKeyObj:Key>
<WinRegistryKeyObj:Hive>HKLM</WinRegistryKeyObj:Hive>
</cybox:Properties>
</cybox:Associated_Object>
</cybox:Associated_Objects>
</maecBundle:Action>
<maecBundle:Action id="remove_from_registry_tmmbd">
<cybox:Name xsi:type="maecVocabs:RegistryActionNameVocab-1.0">delete registry

key value</cybox:Name>
<cybox:Associated_Objects>
<cybox:Associated_Object>
<cybox:Properties
xsi:type="WinRegistryKeyObj:WindowsRegistryKeyObjectType">

<WinRegistryKeyObj:Key>SYSTEM\CurrentControlSet\Services\tmmbd</WinRegistry
KeyObj:Key>
<WinRegistryKeyObj:Hive>HKLM</WinRegistryKeyObj:Hive>
</cybox:Properties>
</cybox:Associated_Object>
</cybox:Associated_Objects>
</maecBundle:Action>
<maecBundle:Action id="remove_from_registry_pavsrv">
<cybox:Name xsi:type="maecVocabs:RegistryActionNameVocab-1.0">delete registry
key value</cybox:Name>
<cybox:Associated_Objects>
<cybox:Associated_Object>
<cybox:Properties
xsi:type="WinRegistryKeyObj:WindowsRegistryKeyObjectType">

<WinRegistryKeyObj:Key>SYSTEM\CurrentControlSet\Services\PAVSRV</WinRegist
ryKeyObj:Key>

<WinRegistryKeyObj:Hive>HKLM</WinRegistryKeyObj:Hive>

</cybox:Properties>

</cybox:Associated_Object>

</cybox:Associated_Objects>

</maecBundle:Action>

<maecBundle:Action id="remove_from_registry_symevent">

<cybox:Name xsi:type="maecVocabs:RegistryActionNameVocab-1.0">delete registry key value</cybox:Name>

<cybox:Associated_Objects>

<cybox:Associated_Object>

<cybox:Properties xsi:type="WinRegistryKeyObj:WindowsRegistryKeyObjectType">

<WinRegistryKeyObj:Key>SYSTEM\CurrentControlSet\Services\SymEvent</WinRegistryKeyObj:Key>

<WinRegistryKeyObj:Hive>HKLM</WinRegistryKeyObj:Hive>

</cybox:Properties>

</cybox:Associated_Object>

</cybox:Associated_Objects>

</maecBundle:Action>

<maecBundle:Action id="remove_from_registry_ekrn">

<cybox:Name xsi:type="maecVocabs:RegistryActionNameVocab-1.0">delete registry key value</cybox:Name>

<cybox:Associated_Objects>

<cybox:Associated_Object>

<cybox:Properties

xsi:type="WinRegistryKeyObj:WindowsRegistryKeyObjectType">

<WinRegistryKeyObj:Key>SYSTEM\CurrentControlSet\Services\ekrn</WinRegistryKeyObj:Key>

<WinRegistryKeyObj:Hive>HKLM</WinRegistryKeyObj:Hive>

</cybox:Properties>

</cybox:Associated_Object>

</cybox:Associated_Objects>

</maecBundle:Action>

<maecBundle:Action id="remove_from_registry_kwatchsvc">

<cybox:Name xsi:type="maecVocabs:RegistryActionNameVocab-1.0">delete registry key value</cybox:Name>

<cybox:Associated_Objects>

<cybox:Associated_Object>

<cybox:Properties

xsi:type="WinRegistryKeyObj:WindowsRegistryKeyObjectType">

<WinRegistryKeyObj:Key>SYSTEM\CurrentControlSet\Services\KWatchSvc</WinRegistryKeyObj:Key>

<WinRegistryKeyObj:Hive>HKLM</WinRegistryKeyObj:Hive>

```
    </cybox:Properties>
   </cybox:Associated_Object>
  </cybox:Associated_Objects>
 </maecBundle:Action>
 <maecBundle:Action id="remove_from_registry_avp">
  <cybox:Name xsi:type="maecVocabs:RegistryActionNameVocab-1.0">delete registry
key value</cybox:Name>
  <cybox:Associated_Objects>
   <cybox:Associated_Object>
    <cybox:Properties
xsi:type="WinRegistryKeyObj:WindowsRegistryKeyObjectType">

<WinRegistryKeyObj:Key>SYSTEM\CurrentControlSet\Services\AVP</WinRegistryK
eyObj:Key>
     <WinRegistryKeyObj:Hive>HKLM</WinRegistryKeyObj:Hive>
    </cybox:Properties>
   </cybox:Associated_Object>
  </cybox:Associated_Objects>
 </maecBundle:Action>
 <maecBundle:Action id="remove_from_registry_antivirservice">
  <cybox:Name xsi:type="maecVocabs:RegistryActionNameVocab-1.0">delete registry
key value</cybox:Name>
  <cybox:Associated_Objects>
```

<cybox:Associated_Object>

<cybox:Properties

xsi:type="WinRegistryKeyObj:WindowsRegistryKeyObjectType">

<WinRegistryKeyObj:Key>SYSTEM\CurrentControlSet\Services\AntiVirService</Win

RegistryKeyObj:Key>

<WinRegistryKeyObj:Hive>HKLM</WinRegistryKeyObj:Hive>

</cybox:Properties>

</cybox:Associated_Object>

</cybox:Associated_Objects>

</maecBundle:Action>

<maecBundle:Action id="remove_from_registry_mpsvcservice">

<cybox:Name xsi:type="maecVocabs:RegistryActionNameVocab-1.0">delete registry

key value</cybox:Name>

<cybox:Associated_Objects>

<cybox:Associated_Object>

<cybox:Properties

xsi:type="WinRegistryKeyObj:WindowsRegistryKeyObjectType">

<WinRegistryKeyObj:Key>SYSTEM\CurrentControlSet\Services\MPSVCService</Win

RegistryKeyObj:Key>

<WinRegistryKeyObj:Hive>HKLM</WinRegistryKeyObj:Hive>

</cybox:Properties>

```
    </cybox:Associated_Object>
   </cybox:Associated_Objects>
  </maecBundle:Action>

  <maecBundle:Action id="disable_safe_mode_boot_with_network">
   <cybox:Name xsi:type="maecVocabs:RegistryActionNameVocab-1.0">delete registry
key value</cybox:Name>
   <cybox:Associated_Objects>
    <cybox:Associated_Object id="safe_mode_network_key1">
     <cybox:Properties
xsi:type="WinRegistryKeyObj:WindowsRegistryKeyObjectType">

<WinRegistryKeyObj:Key>SYSTEM\ControlSet001\Control\SafeBoot\Network\{4D36
E967-E325-11CE-BFC1-08002BE10318}</WinRegistryKeyObj:Key>
      <WinRegistryKeyObj:Hive>HKLM</WinRegistryKeyObj:Hive>
     </cybox:Properties>
    </cybox:Associated_Object>
    <cybox:Associated_Object id="safe_mode_network_key2">
     <cybox:Properties
xsi:type="WinRegistryKeyObj:WindowsRegistryKeyObjectType">

<WinRegistryKeyObj:Key>SYSTEM\CurrentControlSet\Control\SafeBoot\Network\{4
D36E967-E325-11CE-BFC1-08002BE10318}</WinRegistryKeyObj:Key>
```

<WinRegistryKeyObj:Hive>HKLM</WinRegistryKeyObj:Hive>

</cybox:Properties>

</cybox:Associated_Object>

</cybox:Associated_Objects>

</maecBundle:Action>

<maecBundle:Action id="disable_safe_mode_boot_without_network">

<cybox:Name xsi:type="maecVocabs:RegistryActionNameVocab-1.0">delete registry key</cybox:Name>

<cybox:Associated_Objects>

<cybox:Associated_Object id="safe_mode_minimal_key1">

<cybox:Properties xsi:type="WinRegistryKeyObj:WindowsRegistryKeyObjectType">

<WinRegistryKeyObj:Key>SYSTEM\ControlSet001\Control\SafeBoot\Minimal\{4D36E967-E325-11CE-BFC1-08002BE10318}</WinRegistryKeyObj:Key>

<WinRegistryKeyObj:Hive>HKLM</WinRegistryKeyObj:Hive>

</cybox:Properties>

</cybox:Associated_Object>

<cybox:Associated_Object id="safe_mode_minimal_key2">

<cybox:Properties xsi:type="WinRegistryKeyObj:WindowsRegistryKeyObjectType">

<WinRegistryKeyObj:Key>SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\{4D

36E967-E325-11CE-BFC1-08002BE10318}</WinRegistryKeyObj:Key>
<WinRegistryKeyObj:Hive>HKLM</WinRegistryKeyObj:Hive>
</cybox:Properties>
</cybox:Associated_Object>
</cybox:Associated_Objects>
</maecBundle:Action>
<maecBundle:Action id="delete_image_file_execution_options">
<cybox:Name xsi:type="maecVocabs:RegistryActionNameVocab-1.0">delete registry key</cybox:Name>
<cybox:Associated_Objects>
<cybox:Associated_Object>
<cybox:Properties xsi:type="WinRegistryKeyObj:WindowsRegistryKeyObjectType">
<WinRegistryKeyObj:Key>SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options</WinRegistryKeyObj:Key>
<WinRegistryKeyObj:Hive>HKLM</WinRegistryKeyObj:Hive>
</cybox:Properties>
</cybox:Associated_Object>
</cybox:Associated_Objects>
</maecBundle:Action>
<maecBundle:Action id="delete_group_policy_objects">
<cybox:Name xsi:type="maecVocabs:RegistryActionNameVocab-1.0">delete registry key</cybox:Name>

<cybox:Associated_Objects>

<cybox:Associated_Object>

<cybox:Properties

xsi:type="WinRegistryKeyObj:WindowsRegistryKeyObjectType">

<WinRegistryKeyObj:Key>Software\Microsoft\Windows\CurrentVersion\Group

Policy Objects</WinRegistryKeyObj:Key>

<WinRegistryKeyObj:Hive>HKCU</WinRegistryKeyObj:Hive>

</cybox:Properties>

</cybox:Associated_Object>

</cybox:Associated_Objects>

</maecBundle:Action>

<maecBundle:Action id="disable_show_super_hidden_objects_option">

<cybox:Name xsi:type="maecVocabs:RegistryActionNameVocab-1.0">modify

registry key</cybox:Name>

<cybox:Associated_Objects>

<cybox:Associated_Object>

<cybox:Properties

xsi:type="WinRegistryKeyObj:WindowsRegistryKeyObjectType">

<WinRegistryKeyObj:Key>Software\Microsoft\Windows\CurrentVersion\Explorer\Adv

anced\Show Super Hidden</WinRegistryKeyObj:Key>

<WinRegistryKeyObj:Hive>HKCU</WinRegistryKeyObj:Hive>

<WinRegistryKeyObj:Values>

<WinRegistryKeyObj:Value>0x01</WinRegistryKeyObj:Value>

</WinRegistryKeyObj:Values>

</cybox:Properties>

</cybox:Associated_Object>

</cybox:Associated_Objects>

</maecBundle:Action>

</maecBundle:Actions>

<maecBundle:Candidate_Indicators>

<!-- Capability CIs -->

<maecBundle:Candidate_Indicator id="capabilities_id">

<maecBundle:Composition operator="AND">

<maecBundle:Capability_Reference capability_idref="persistence"/>

<maecBundle:Capability_Reference capability_idref="spread_across_system"/>

<maecBundle:Capability_Reference capability_idref="run_arbitrary_commands"/>

<maecBundle:Capability_Reference
capability_idref="downgrade_system_security_level"/>

</maecBundle:Composition>

</maecBundle:Candidate_Indicator>

<!-- Behaviour CIs -->

<maecBundle:Candidate_Indicator id="persistence_id">

<maecBundle:Composition operator="AND">

<maecBundle:Behavior_Reference behavior_idref="persistence_at_runtime"/>

<maecBundle:Behavior_Reference behavior_idref="persistence_on_disk"/>

<maecBundle:Behavior_Reference behavior_idref="persistence_across_reboots"/>

</maecBundle:Composition>

</maecBundle:Candidate_Indicator>

<maecBundle:Candidate_Indicator id="spread_across_system_id">

<maecBundle:Composition operator="OR">

<maecBundle:Behavior_Reference behavior_idref="copy_self_to_exe_files"/>

<maecBundle:Behavior_Reference behavior_idref="copy_self_to_zipped_exe_files"/>

<maecBundle:Behavior_Reference behavior_idref="copy_self_to_removable_drives"/>

<maecBundle:Behavior_Reference behavior_idref="copy_code_to_html_files"/>

</maecBundle:Composition>

</maecBundle:Candidate_Indicator>

<maecBundle:Candidate_Indicator id="run_arbitrary_commands_id">

<maecBundle:Composition operator="AND">

<maecBundle:Behavior_Reference behavior_idref="fetch_commands"/>

<maecBundle:Behavior_Reference behavior_idref="execute_commands_recieved"/>

</maecBundle:Composition>

</maecBundle:Candidate_Indicator>

<maecBundle:Candidate_Indicator id="downgrade_system_security_level_id">

<maecBundle:Composition operator="OR">

<maecBundle:Behavior_Reference behavior_idref="kill_av_processes"/>

<maecBundle:Behavior_Reference behavior_idref="modify_acli_settings"/>

<maecBundle:Behavior_Reference

behavior_idref="prevent_process_run_on_startup"/>
<maecBundle:Behavior_Reference behavior_idref="modify_registry_settings"/>
</maecBundle:Composition>
</maecBundle:Candidate_Indicator>
<!-- Action CIs -->
<maecBundle:Candidate_Indicator id="persistence_at_runtime_id">
<maecBundle:Composition operator="AND">
<maecBundle:Action_Reference action_id="create_mutex_random_name"/>
<maecBundle:Action_Reference action_id="create_mutex_xcgucvnzn"/>
<maecBundle:Action_Reference action_id="create_mutex_BLAIPBOFFCNJ"/>
</maecBundle:Composition>
</maecBundle:Candidate_Indicator>
<maecBundle:Candidate_Indicator id="persistence_on_disk_id">
<maecBundle:Composition operator="AND">
<maecBundle:Action_Reference action_id="enumerate_files"/>
<maecBundle:Sub_Composition operator="OR">
<maecBundle:Action_Reference action_id="copy_self_to_new_log_files"/>
<maecBundle:Action_Reference action_id="copy_self_to_new_exe_files"/>
</maecBundle:Sub_Composition>
</maecBundle:Composition>
</maecBundle:Candidate_Indicator>
<maecBundle:Candidate_Indicator id="persistence_across_reboots_id">
<maecBundle:Composition operator="AND">

<maecBundle:Action_Reference action_id="copy_self_to_new_dll"/>

<maecBundle:Action_Reference action_id="copy_self_to_new_sys"/>

<maecBundle:Action_Reference action_id="register_sys_as_service"/>

</maecBundle:Composition>

</maecBundle:Candidate_Indicator>

<maecBundle:Candidate_Indicator id="copy_self_to_exe_files_id">

<maecBundle:Composition operator="AND">

<maecBundle:Action_Reference action_id="enumerate_files"/>

<maecBundle:Action_Reference action_id="infect_exe_files"/>

</maecBundle:Composition>

</maecBundle:Candidate_Indicator>

<maecBundle:Candidate_Indicator id="copy_self_to_zipped_exe_files_id">

<maecBundle:Composition operator="AND">

<maecBundle:Action_Reference action_id="enumerate_files"/>

<maecBundle:Action_Reference action_id="extract_files_using_winrar"/>

<maecBundle:Action_Reference action_id="infect_exe_files"/>

</maecBundle:Composition>

</maecBundle:Candidate_Indicator>

<maecBundle:Candidate_Indicator id="copy_self_to_removable_drives_id">

<maecBundle:Composition operator="AND">

<maecBundle:Action_Reference action_id="copy_self_to_pagefile"/>

<maecBundle:Action_Reference action_id="configure_autorun"/>

<maecBundle:Action_Reference
action_id="enable_autorun_for_all_drives_registry"/>
</maecBundle:Composition>
</maecBundle:Candidate_Indicator>
<maecBundle:Candidate_Indicator id="copy_code_to_html_files_id">
<maecBundle:Composition operator="AND">
<maecBundle:Action_Reference action_id="enumerate_htm_files"/>
<maecBundle:Action_Reference action_id="embed_file_with_htm_tags"/>
</maecBundle:Composition>
</maecBundle:Candidate_Indicator>

<maecBundle:Candidate_Indicator id="execute_commands_recieved_id">
<maecBundle:Composition operator="OR">
<maecBundle:Action_Reference action_id="start_process"/>
<maecBundle:Action_Reference action_id="terminate_process"/>
</maecBundle:Composition>
</maecBundle:Candidate_Indicator>

<maecBundle:Candidate_Indicator id="kill_av_processes_id">
<maecBundle:Composition operator="AND">
<maecBundle:Action_Reference action_id="list_processes"/>

<maecBundle:Sub_Composition operator="OR">

<maecBundle:Action_Reference action_id="kill_rav"/>

<maecBundle:Action_Reference action_id="kill_avp"/>

<maecBundle:Action_Reference action_id="kill_twister"/>

<maecBundle:Action_Reference action_id="kill_kv"/>

<maecBundle:Action_Reference action_id="kill_watch"/>

<maecBundle:Action_Reference action_id="kill_kissvc"/>

<maecBundle:Action_Reference action_id="kill_scan"/>

<maecBundle:Action_Reference action_id="kill_guard"/>

<maecBundle:Action_Reference action_id="kill_kmailmon"/>

</maecBundle:Sub_Composition>

</maecBundle:Composition>

</maecBundle:Candidate_Indicator>

<maecBundle:Candidate_Indicator id="prevent_process_run_on_startup_id">

<maecBundle:Composition operator="OR">

<maecBundle:Action_Reference action_id="remove_from_registry_ksysmon"/>

<maecBundle:Action_Reference action_id="remove_from_registry_eqservice"/>

<maecBundle:Action_Reference action_id="remove_from_registry_rsravmon"/>

<maecBundle:Action_Reference action_id="remove_from_registry_mcshield"/>

<maecBundle:Action_Reference action_id="remove_from_registry_tmmbd"/>

<maecBundle:Action_Reference action_id="remove_from_registry_pavsrv"/>

<maecBundle:Action_Reference action_id="remove_from_registry_symevent"/>

<maecBundle:Action_Reference action_id="remove_from_registry_ekrn"/>

<maecBundle:Action_Reference action_id="remove_from_registry_kwatchsvc"/>

<maecBundle:Action_Reference action_id="remove_from_registry_avp"/>

<maecBundle:Action_Reference action_id="remove_from_registry_antivirservice"/>

<maecBundle:Action_Reference action_id="remove_from_registry_mpsvcservice"/>

</maecBundle:Composition>

</maecBundle:Candidate_Indicator>

<maecBundle:Candidate_Indicator id="modify_registry_settings_id">

<maecBundle:Composition operator="OR">

<maecBundle:Action_Reference
action_id="disable_safe_mode_boot_with_network"/>

<maecBundle:Action_Reference
action_id="disable_safe_mode_boot_without_network"/>

<maecBundle:Action_Reference action_id="delete_image_file_execution_options"/>

<maecBundle:Action_Reference action_id="delete_group_policy_objects"/>

<maecBundle:Action_Reference
action_id="disable_show_super_hidden_objects_option"/>

</maecBundle:Composition>

</maecBundle:Candidate_Indicator>

<!-- Object CIs -->

<maecBundle:Candidate_Indicator id="embed_file_with_htm_tags_id">

<maecBundle:Composition operator="AND">

<maecBundle:Object_Reference object_idref="htm_file"/>

<maecBundle:Object_Reference object_idref="script_code"/>
</maecBundle:Composition>
</maecBundle:Candidate_Indicator>
<maecBundle:Candidate_Indicator id="fetch_commands_from_cnc">
<maecBundle:Composition operator="OR">
<maecBundle:Object_Reference object_idref="cnc_url_1"/>
<maecBundle:Object_Reference object_idref="cnc_url_2"/>
</maecBundle:Composition>
</maecBundle:Candidate_Indicator>
<maecBundle:Candidate_Indicator id="disable_safe_mode_boot_with_network_id">
<maecBundle:Composition operator="OR">
<maecBundle:Object_Reference object_idref="safe_mode_network_key1"/>
<maecBundle:Object_Reference object_idref="safe_mode_network_key2"/>
</maecBundle:Composition>
</maecBundle:Candidate_Indicator>
<maecBundle:Candidate_Indicator
id="disable_safe_mode_boot_without_network_id">
<maecBundle:Composition operator="OR">
<maecBundle:Object_Reference object_idref="safe_mode_minimal_key1"/>
<maecBundle:Object_Reference object_idref="safe_mode_minimal_key2"/>
</maecBundle:Composition>
</maecBundle:Candidate_Indicator>

</maecBundle:Candidate_Indicators>

</maecBundle:MAEC_Bundle>

A.11 Zbot.gen!R

<?xml version="1.0" encoding="UTF-8"?>

<maecBundle:MAEC_Bundle xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"

xsi:schemaLocation="http://cybox.mitre.org/objects#ArtifactObject-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/Artifact_Object.xsd

http://cybox.mitre.org/objects#WinRegistryKeyObject-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/Win_Registry_Key_Object.xsd

http://cybox.mitre.org/objects#WinExecutableFileObject-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/Win_Executable_File_Object.xsd

http://cybox.mitre.org/common-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/cybox_common.xsd

http://cybox.mitre.org/objects#APIObject-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/API_Object.xsd

http://maec.mitre.org/XMLSchema/maec-bundle-4

maec/maec_4.1_offline/maec_bundle_schema.xsd

http://cybox.mitre.org/objects#WinExecutableFileObject-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/Win_Executable_File_Object.xsd

http://cybox.mitre.org/objects#PDFFileObject-1

maec/maec_4.1_offline/cybox_2.1_offline/objects/PDF_File_Object.xsd

http://cybox.mitre.org/objects#APIObject-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/API_Object.xsd

http://cybox.mitre.org/objects#WinExecutableFileObject-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/Win_Executable_File_Object.xsd

http://cybox.mitre.org/default_vocabularies-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/cybox_default_vocabularies.xsd

http://cybox.mitre.org/objects#PDFFileObject-1

maec/maec_4.1_offline/cybox_2.1_offline/objects/PDF_File_Object.xsd

http://cybox.mitre.org/objects#WinRegistryKeyObject-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/Win_Registry_key_Object.xsd

http://cybox.mitre.org/objects#WinMutexObject-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/Win_Mutex_Object.xsd

http://cybox.mitre.org/objects#ArtifactObject-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/Artifact_Object.xsd

http://cybox.mitre.org/objects#EmailMessageObject-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/Email_Message_Object.xsd

http://cybox.mitre.org/objects#MutexObject-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/Mutex_Object.xsd

http://cybox.mitre.org/objects#PipeObject-2

maec/maec_4.1_offline/cybox_2.1_offline/objects/Pipe_Object.xsd

"

xmlns:HTTPSessionObj="http://cybox.mitre.org/objects#HTTPSessionObject-2"

xmlns:DNSQueryObj="http://cybox.mitre.org/objects#DNSQueryObject-2"

xmlns:maecBundle="http://maec.mitre.org/XMLSchema/maec-bundle-4"

xmlns:ProcessObj="http://cybox.mitre.org/objects#ProcessObject-2"

xmlns:SocketAddressObj="http://cybox.mitre.org/objects#SocketAddressObject-1"

xmlns:AddressObj="http://cybox.mitre.org/objects#AddressObject-2"

xmlns:NetworkConnectionObj="http://cybox.mitre.org/objects#NetworkConnectionObje
ct-2"

xmlns:PDFFileObj="http://cybox.mitre.org/objects#PDFFileObject-1"

xmlns:cyboxVocabs="http://cybox.mitre.org/default_vocabularies-2"

xmlns:HostnameObj="http://cybox.mitre.org/objects#HostnameObject-1"

xmlns:CodeObj="http://cybox.mitre.org/objects#CodeObject-2"

xmlns:FileObj="http://cybox.mitre.org/objects#FileObject-2"

xmlns:DNSRecordObj="http://cybox.mitre.org/objects#DNSRecordObject-2"

xmlns:WinRegistryKeyObj="http://cybox.mitre.org/objects#WinRegistryKeyObject-2"

xmlns:maecVocabs="http://maec.mitre.org/default_vocabularies-1"

xmlns:APIObj="http://cybox.mitre.org/objects#APIObject-2"

xmlns:WinExecutableFileObj="http://cybox.mitre.org/objects#WinExecutableFileObject
-2"

xmlns:cyboxCommon="http://cybox.mitre.org/common-2"

xmlns:URIObj="http://cybox.mitre.org/objects#URIObject-2"
xmlns:cybox="http://cybox.mitre.org/cybox-2"
xmlns:WinMutexObj="http://cybox.mitre.org/objects#WinMutexObject-2"
xmlns:ArtifactObj="http://cybox.mitre.org/objects#ArtifactObject-2"
xmlns:EmailMessageObj="http://cybox.mitre.org/objects#EmailMessageObject-2"
xmlns:MutexObj="http://cybox.mitre.org/objects#MutexObject-2"
xmlns:PipeObj="http://cybox.mitre.org/objects#PipeObject-2"
id="ZBot_exe_TT" schema_version="4.1"
defined_subject="true">

<maecBundle:Malware_Instance_Object_Attributes>
<cybox:Description>The Malware is a functionality rich exe sample that perofrms a variety of information stealing acitvities</cybox:Description>
<cybox:Properties xsi:type="WinExecutableFileObj:WindowsExecutableFileObjectType">
<FileObj:File_Extension>EXE</FileObj:File_Extension>
<FileObj:Size_In_Bytes>130048</FileObj:Size_In_Bytes>
<FileObj:Hashes>
<cyboxCommon:Hash>
<cyboxCommon:Type>MD5</cyboxCommon:Type>

<cyboxCommon:Simple_Hash_Value>3025b97428a14c9bb808dacbc3bedbe7</cyboxCommon:Simple_Hash_Value>

```
 </cyboxCommon:Hash>
</FileObj:Hashes>
 </cybox:Properties>
  </maecBundle:Malware_Instance_Object_Attributes>

 <!-- Placeholder for capabilities -->
 <maecBundle:Capabilities>
  <maecBundle:Capability id="persistence" name="persistence">
   <maecBundle:Behavior_Reference behavior_idref="persistence_at_runtime"/>
   <maecBundle:Behavior_Reference behavior_idref="persistence_across_reboots"/>
  </maecBundle:Capability>
  <maecBundle:Capability id="trojanize_binaries_establish_ipc_mechanism"
name="integrity violation">
   <maecBundle:Behavior_Reference behavior_idref="code_injection_winlogon"/>
   <maecBundle:Behavior_Reference behavior_idref="code_injection_svchost"/>
  </maecBundle:Capability>
  <maecBundle:Capability id="run_arbitrary_commands">
   <maecBundle:Behavior_Reference behavior_idref="fetch_commands"/>
   <maecBundle:Behavior_Reference behavior_idref="execute_commands_received"/>
  </maecBundle:Capability>
  <maecBundle:Capability id="steal_data_from_processes" name="data theft">
   <maecBundle:Behavior_Reference behavior_idref="code_injection_processes"/>
   <maecBundle:Behavior_Reference behavior_idref="Hook_HttpSendRequests"/>
```

<maecBundle:Behavior_Reference behavior_idref="Hook_InternetReadFile"/>

<maecBundle:Behavior_Reference

behavior_idref="Hook_InternetQueryDataAvaliable"/>

<maecBundle:Behavior_Reference behavior_idref="Hook_CloseHandle"/>

<maecBundle:Behavior_Reference behavior_idref="Hook_HttpQueryInfo"/>

<maecBundle:Behavior_Reference behavior_idref="Hook_Send_WSASend"/>

<maecBundle:Behavior_Reference behavior_idref="Hook_closesocket"/>

<maecBundle:Behavior_Reference behavior_idref="Hook_BeginPaint"/>

<maecBundle:Behavior_Reference behavior_idref="Hook_EndPaint"/>

<maecBundle:Behavior_Reference behavior_idref="Hook_DefWindowProc"/>

<maecBundle:Behavior_Reference behavior_idref="Hook_TranslateMessage"/>

<maecBundle:Behavior_Reference behavior_idref="Hook_GetClipboradData"/>

<maecBundle:Behavior_Reference behavior_idref="Hook_PFXImportCertStore"/>

</maecBundle:Capability>

</maecBundle:Capabilities>

<!-- Placeholder for behaviours -->

<maecBundle:Behaviors>

<maecBundle:Behavior id="persistence_at_runtime">

<maecBundle:Action_Composition>

<maecBundle:Action_Reference action_id="create_mutex_AVIRA_21099"/>

<maecBundle:Action_Reference action_id="create_mutex_AVIRA_2109"/>

<maecBundle:Action_Reference action_id="create_mutex_AVIRA_2108"/>

```
 </maecBundle:Action_Composition>
</maecBundle:Behavior>
<maecBundle:Behavior id="persistence_across_reboots">
 <maecBundle:Action_Composition>
  <maecBundle:Action_Reference action_id="copy_self_to_new_exe"/>
  <maecBundle:Action_Reference action_id="modify_registry"/>
 </maecBundle:Action_Composition>
</maecBundle:Behavior>
<maecBundle:Behavior id="code_injection_winlogon">
 <maecBundle:Action_Composition>
  <maecBundle:Action_Reference action_id="create_config_file"/>
  <maecBundle:Action_Reference action_id="create_stolen_data_file"/>
  <maecBundle:Action_Reference action_id="create_pipe_for_communication_2109"/>
  <maecBundle:Action_Reference
action_id="create_pipe_server_for_config_user_file_access"/>
 </maecBundle:Action_Composition>
</maecBundle:Behavior>
<maecBundle:Behavior id="code_injection_svchost">
 <maecBundle:Action_Composition>
  <maecBundle:Action_Reference action_id="configure_registry_with_uniqueID"/>
  <maecBundle:Action_Reference action_id="query_system_info"/>
  <maecBundle:Action_Reference action_id="create_pipe_for_communication_2108"/>
  <maecBundle:Action_Reference action_id="send_commands_to_other_processes"/>
```

<maecBundle:Action_Reference action_id="fetch_config_file_from_cnc"/>

</maecBundle:Action_Composition>

</maecBundle:Behavior>

<maecBundle:Behavior id="fetch_commands">

<maecBundle:Action_Composition>

<maecBundle:Action_Reference

action_id="fetch_commands_to_execute_from_cnc"/>

</maecBundle:Action_Composition>

</maecBundle:Behavior>

<maecBundle:Behavior id="execute_commands_received">

<maecBundle:Action_Composition>

<maecBundle:Action_Reference action_id="reboot_target"/>

<maecBundle:Action_Reference action_id="shutdown_system"/>

<maecBundle:Action_Reference action_id="update_config_file"/>

<maecBundle:Action_Reference action_id="kill_malware"/>

<maecBundle:Action_Reference action_id="rename_target"/>

<maecBundle:Action_Reference action_id="upload_stolen_certificates"/>

<maecBundle:Action_Reference action_id="upload_flash_player_cookies"/>

<maecBundle:Action_Reference action_id="delete_flash_player_cookies"/>

<maecBundle:Action_Reference action_id="set_home_page_of_IE"/>

<maecBundle:Action_Reference action_id="block_url"/>

<maecBundle:Action_Reference action_id="unblock_url"/>

<maecBundle:Action_Reference action_id="download_binary_and_execute_binary"/>

<maecBundle:Action_Reference action_id="execute_local_file"/>

</maecBundle:Action_Composition>

</maecBundle:Behavior>

<maecBundle:Behavior id="code_injection_processes">

<maecBundle:Action_Composition>

<maecBundle:Action_Reference action_id="list_processes"/>

<maecBundle:Action_Reference action_id="open_process"/>

<maecBundle:Action_Reference action_id="copy_self_to_process"/>

<maecBundle:Action_Reference action_id="setup_inline_api_hooking"/>

</maecBundle:Action_Composition>

</maecBundle:Behavior>

<maecBundle:Behavior id="Hook_HttpSendRequests">

<maecBundle:Action_Composition>

<maecBundle:Action_Reference action_id="get_url_info"/>

<maecBundle:Action_Reference action_id="get_http_cookies"/>

<maecBundle:Action_Reference action_id="get_flash_player_cookies"/>

<maecBundle:Action_Reference action_id="get_temporary_request_buffer"/>

<maecBundle:Action_Reference action_id="get_input_data_from_html"/>

</maecBundle:Action_Composition>

</maecBundle:Behavior>

<maecBundle:Behavior id="Hook_InternetReadFile">

<maecBundle:Action_Composition>

<maecBundle:Action_Reference action_id="embed_file_with_htm_tags"/>

<maecBundle:Action_Reference action_id="new_binary_setup_inline_api_hooking"/>

</maecBundle:Action_Composition>

</maecBundle:Behavior>

<maecBundle:Behavior id="Hook_InternetQueryDataAvaliable">

<maecBundle:Action_Composition>

<maecBundle:Action_Reference action_id="get_query_options_for_request"/>

</maecBundle:Action_Composition>

</maecBundle:Behavior>

<maecBundle:Behavior id="Hook_CloseHandle">

<maecBundle:Action_Composition>

<maecBundle:Action_Reference action_id="free_memory_for_request"/>

</maecBundle:Action_Composition>

</maecBundle:Behavior>

<maecBundle:Behavior id="Hook_HttpQueryInfo">

<maecBundle:Action_Composition>

<maecBundle:Action_Reference action_id="check_info_received_in_memory"/>

</maecBundle:Action_Composition>

</maecBundle:Behavior>

<maecBundle:Behavior id="Hook_Send_WSASend">

<maecBundle:Action_Composition>

<maecBundle:Action_Reference action_id="record_user_password_from_buffer"/>

<maecBundle:Action_Reference action_id="record_ftp_information"/>

<maecBundle:Action_Reference action_id="record_pop3_email_passwords"/>
</maecBundle:Action_Composition>
</maecBundle:Behavior>
<maecBundle:Behavior id="Hook_closesocket">
<maecBundle:Action_Composition>
<maecBundle:Action_Reference action_id="clear_memory"/>
</maecBundle:Action_Composition>
</maecBundle:Behavior>
<maecBundle:Behavior id="Hook_BeginPaint">
<maecBundle:Action_Composition>
<maecBundle:Action_Reference action_id="create_new_buffer"/>
</maecBundle:Action_Composition>
</maecBundle:Behavior>
<maecBundle:Behavior id="Hook_EndPaint">
<maecBundle:Action_Composition>
<maecBundle:Action_Reference action_id="clear_memory"/>
</maecBundle:Action_Composition>
</maecBundle:Behavior>
<maecBundle:Behavior id="Hook_DefWindowProc">
<maecBundle:Action_Composition>
<maecBundle:Action_Reference action_id="get_device_context"/>
<maecBundle:Action_Reference action_id="get_window_resolution"/>
<maecBundle:Action_Reference action_id="create_buffer_for_translate_api_hook"/>

```
 </maecBundle:Action_Composition>
</maecBundle:Behavior>
<maecBundle:Behavior id="Hook_TranslateMessage">
 <maecBundle:Action_Composition>
  <maecBundle:Action_Reference action_id="check_mouse_click"/>
  <maecBundle:Action_Reference action_id="generate_screenshot"/>
 </maecBundle:Action_Composition>
</maecBundle:Behavior>
<maecBundle:Behavior id="Hook_GetClipboradData">
 <maecBundle:Action_Composition>
  <maecBundle:Action_Reference action_id="copy_clipboard_data_to_memory"/>
 </maecBundle:Action_Composition>
</maecBundle:Behavior>
<maecBundle:Behavior id="Hook_PFXImportCertStore">
 <maecBundle:Action_Composition>
  <maecBundle:Action_Reference action_id="copy_certificates_to_stolen_data_file"/>
 </maecBundle:Action_Composition>
</maecBundle:Behavior>

</maecBundle:Behaviors>

 <!-- Placeholder for actions -->
 <maecBundle:Actions>
```

<maecBundle:Action id="create_mutex_AVIRA_21099">
<cybox:Name xsi:type="maecVocabs:SynchronizationActionNameVocab-1.0">create mutex</cybox:Name>
<cybox:Associated_Objects>
<cybox:Associated_Object>
<cybox:Properties xsi:type="MutexObj:MutexObjectType" named="true">
<MutexObj:Name>AVIRA_21099</MutexObj:Name>
</cybox:Properties>
</cybox:Associated_Object>
</cybox:Associated_Objects>
</maecBundle:Action>
<maecBundle:Action id="create_mutex_AVIRA_2109">
<cybox:Name xsi:type="maecVocabs:SynchronizationActionNameVocab-1.0">create mutex</cybox:Name>
<cybox:Associated_Objects>
<cybox:Associated_Object>
<cybox:Properties xsi:type="MutexObj:MutexObjectType" named="true">
<MutexObj:Name>AVIRA_2109</MutexObj:Name>
</cybox:Properties>
</cybox:Associated_Object>
</cybox:Associated_Objects>
</maecBundle:Action>
<maecBundle:Action id="create_mutex_AVIRA_2108">

<cybox:Name xsi:type="maecVocabs:SynchronizationActionNameVocab-1.0">create mutex</cybox:Name>
<cybox:Associated_Objects>
<cybox:Associated_Object>
<cybox:Properties xsi:type="MutexObj:MutexObjectType" named="true">
<MutexObj:Name>AVIRA_2108</MutexObj:Name>
</cybox:Properties>
</cybox:Associated_Object>
</cybox:Associated_Objects>
</maecBundle:Action>

<maecBundle:Action id="copy_self_to_new_exe">
<cybox:Name xsi:type="maecVocabs:FileActionNameVocab-1.1">create file</cybox:Name>
<cybox:Associated_Objects>
<cybox:Associated_Object>
<cybox:Properties xsi:type="WinExecutableFileObj:WindowsExecutableFileObjectType">
<FileObj:File_Name>sdra64.exe</FileObj:File_Name>
<FileObj:File_Path>%sysdir%</FileObj:File_Path>
<FileObj:File_Extension>exe</FileObj:File_Extension>
</cybox:Properties>
</cybox:Associated_Object>

```
  </cybox:Associated_Objects>
 </maecBundle:Action>
 <maecBundle:Action id="modify_registry">
  <cybox:Name xsi:type="maecVocabs:RegistryActionNameVocab-1.0">create registry
key</cybox:Name>
  <cybox:Associated_Objects>
   <cybox:Associated_Object>
    <cybox:Properties
xsi:type="WinRegistryKeyObj:WindowsRegistryKeyObjectType">

<WinRegistryKeyObj:Key>\Software\Microsoft\Windows\CurrentVersion\Run</WinRe
gistryKeyObj:Key>
     <WinRegistryKeyObj:Hive>HKCU</WinRegistryKeyObj:Hive>
     <WinRegistryKeyObj:Values>
      <WinRegistryKeyObj:Value>
       <WinRegistryKeyObj:Name>userinit</WinRegistryKeyObj:Name>
       <WinRegistryKeyObj:Data>%sysdir%\sdra64.exe</WinRegistryKeyObj:Data>
      </WinRegistryKeyObj:Value>
     </WinRegistryKeyObj:Values>
    </cybox:Properties>
   </cybox:Associated_Object>
  </cybox:Associated_Objects>
 </maecBundle:Action>
```

<maecBundle:Action id="create_config_file">
<cybox:Name xsi:type="maecVocabs:FileActionNameVocab-1.1">create file</cybox:Name>
<cybox:Associated_Objects>
<cybox:Associated_Object>
<cybox:Properties xsi:type="FileObj:FileObjectType">
<FileObj:File_Name>local.ds</FileObj:File_Name>
<FileObj:File_Path>c:\Windows\System32\lowsec\</FileObj:File_Path>
<FileObj:File_Extension>ds</FileObj:File_Extension>
</cybox:Properties>
</cybox:Associated_Object>
</cybox:Associated_Objects>
</maecBundle:Action>
<maecBundle:Action id="create_stolen_data_file">
<cybox:Name xsi:type="maecVocabs:FileActionNameVocab-1.1">create file</cybox:Name>
<cybox:Associated_Objects>
<cybox:Associated_Object>
<cybox:Properties xsi:type="FileObj:FileObjectType">
<FileObj:File_Name>user.ds</FileObj:File_Name>
<FileObj:File_Path>c:\Windows\System32\lowsec\</FileObj:File_Path>
<FileObj:File_Extension>ds</FileObj:File_Extension>
</cybox:Properties>

```
  </cybox:Associated_Object>
 </cybox:Associated_Objects>
</maecBundle:Action>
<maecBundle:Action id="create_pipe_for_communication_2109">

 <cybox:Associated_Objects>
  <cybox:Associated_Object>
   <cybox:Properties xsi:type="PipeObj:PipeObjectType">
    <PipeObj:Name>AVIRA_2109</PipeObj:Name>
   </cybox:Properties>
  </cybox:Associated_Object>
 </cybox:Associated_Objects>
</maecBundle:Action>
<maecBundle:Action id="create_pipe_server_for_config_user_file_access">
 <cybox:Associated_Objects>
  <cybox:Associated_Object>
   <cybox:Properties xsi:type="APIObj:APIObjectType">
    <APIObj:Function_Name>ConnectNamedPipe</APIObj:Function_Name>
   </cybox:Properties>
  </cybox:Associated_Object>
 </cybox:Associated_Objects>
</maecBundle:Action>
<maecBundle:Action id="configure_registry_with_uniqueID">
```

<cybox:Name xsi:type="maecVocabs:RegistryActionNameVocab-1.0">create registry key</cybox:Name>
<cybox:Associated_Objects>
<cybox:Associated_Object>
<cybox:Properties xsi:type="WinRegistryKeyObj:WindowsRegistryKeyObjectType">

<WinRegistryKeyObj:Key>\Software\Microsoft\Windows\CurrentVersion\network</WinRegistryKeyObj:Key>
<WinRegistryKeyObj:Hive>HKLM</WinRegistryKeyObj:Hive>
<WinRegistryKeyObj:Values>
<WinRegistryKeyObj:Value>
<WinRegistryKeyObj:Name>UID</WinRegistryKeyObj:Name>
<WinRegistryKeyObj:Data>netbios_pc_nme</WinRegistryKeyObj:Data>
</WinRegistryKeyObj:Value>
</WinRegistryKeyObj:Values>
</cybox:Properties>
</cybox:Associated_Object>
</cybox:Associated_Objects>
</maecBundle:Action>
<maecBundle:Action id="query_system_info">
<cybox:Associated_Objects>
<cybox:Associated_Object>

<cybox:Name xsi:type="maecVocabs:RegistryActionNameVocab-1.0">read registry key value</cybox:Name>
<cybox:Associated_Objects>
<cybox:Associated_Object id="installdate">
<cybox:Properties xsi:type="WinRegistryKeyObj:WindowsRegistryKeyObjectType">
<WinRegistryKeyObj:Key>\Software\Microsoft\Win NT\CurrentVersion\Installdate</WinRegistryKeyObj:Key>
<WinRegistryKeyObj:Hive>HKLM</WinRegistryKeyObj:Hive>
</cybox:Properties>
</cybox:Associated_Object>
<cybox:Associated_Object id="digitalproductid">
<cybox:Properties xsi:type="WinRegistryKeyObj:WindowsRegistryKeyObjectType">
<WinRegistryKeyObj:Key>\Software\Microsoft\Win NT\CurrentVersion\digitalproductid</WinRegistryKeyObj:Key>
<WinRegistryKeyObj:Hive>HKLM</WinRegistryKeyObj:Hive>
</cybox:Properties>
</cybox:Associated_Object>
</cybox:Associated_Objects>
</cybox:Associated_Object>
</cybox:Associated_Objects>
</maecBundle:Action>

<maecBundle:Action id="create_pipe_for_communication_2108">
 <cybox:Associated_Objects>
  <cybox:Associated_Object>
   <cybox:Properties xsi:type="PipeObj:PipeObjectType">
    <PipeObj:Name>AVIRA_2108</PipeObj:Name>
   </cybox:Properties>
  </cybox:Associated_Object>
 </cybox:Associated_Objects>
</maecBundle:Action>
<maecBundle:Action id="send_commands_to_other_processes"/>
<maecBundle:Action id="fetch_config_file_from_cnc">
 <cybox:Associated_Objects>
  <cybox:Associated_Object id="cnc_url">
   <cybox:Properties xsi:type="URIObj:URIObjectType">
    <URIObj:Value>nekovo.ru/cbd/nekovo.bri</URIObj:Value>
   </cybox:Properties>
  </cybox:Associated_Object>
  <cybox:Associated_Object id="config_file">
    <cybox:Properties xsi:type="FileObj:FileObjectType">
     <FileObj:File_Name>local.ds</FileObj:File_Name>
     <FileObj:File_Path>c:\Windows\System32\lowsec\</FileObj:File_Path>
     <FileObj:File_Extension>ds</FileObj:File_Extension>
    </cybox:Properties>

```
   </cybox:Associated_Object>
  </cybox:Associated_Objects>
 </maecBundle:Action>
 <maecBundle:Action id="fetch_commands_to_execute_from_cnc">
  <cybox:Name xsi:type="maecVocabs:HTTPActionNameVocab-1.0">send http get
request</cybox:Name>
  <cybox:Associated_Objects>
   <cybox:Associated_Object id="cnc_url_1">
    <cybox:Properties xsi:type="HTTPSessionObj:HTTPSessionObjectType">
     <HTTPSessionObj:HTTP_Request_Response>
      <HTTPSessionObj:HTTP_Client_Request>
       <HTTPSessionObj:HTTP_Request_Line>
        <HTTPSessionObj:HTTP_Method>GET</HTTPSessionObj:HTTP_Method>
        <HTTPSessionObj:Value>nekovo.ru/</HTTPSessionObj:Value>
       </HTTPSessionObj:HTTP_Request_Line>
      </HTTPSessionObj:HTTP_Client_Request>
     </HTTPSessionObj:HTTP_Request_Response>
    </cybox:Properties>
   </cybox:Associated_Object>
  </cybox:Associated_Objects>
 </maecBundle:Action>
 <maecBundle:Action id="reboot_target">
  <cybox:Associated_Objects>
```

<cybox:Associated_Object>

<cybox:Description>Reboot parameter:0x02</cybox:Description>

<cybox:Properties xsi:type="APIObj:APIObjectType">

<APIObj:Function_Name>ExitWindowsEx</APIObj:Function_Name>

</cybox:Properties>

</cybox:Associated_Object>

</cybox:Associated_Objects>

</maecBundle:Action>

<maecBundle:Action id="shutdown_system">

<cybox:Associated_Objects>

<cybox:Associated_Object>

<cybox:Properties xsi:type="APIObj:APIObjectType">

<APIObj:Function_Name>shutdown</APIObj:Function_Name>

</cybox:Properties>

</cybox:Associated_Object>

</cybox:Associated_Objects>

</maecBundle:Action>

<maecBundle:Action id="update_config_file"/>

<maecBundle:Action id="kill_malware">

<cybox:Associated_Objects>

<cybox:Associated_Object>

<cybox:Properties xsi:type="APIObj:APIObjectType">

<APIObj:Function_Name>ExitProcess</APIObj:Function_Name>

</cybox:Properties>

</cybox:Associated_Object>

</cybox:Associated_Objects>

</maecBundle:Action>

<maecBundle:Action id="rename_target"/>

<maecBundle:Action id="upload_stolen_certificates"/>

<maecBundle:Action id="upload_flash_player_cookies"/>

<maecBundle:Action id="delete_flash_player_cookies"/>

<maecBundle:Action id="set_home_page_of_IE"/>

<maecBundle:Action id="block_url"/>

<maecBundle:Action id="unblock_url"/>

<maecBundle:Action id="download_binary_and_execute_binary"/>

<maecBundle:Action id="execute_local_file"/>

<maecBundle:Action id="list_processes"/>

<maecBundle:Action id="open_process"/>

<maecBundle:Action id="copy_self_to_process"/>

<maecBundle:Action id="setup_inline_api_hooking">

<cybox:Associated_Objects>

<cybox:Associated_Object>

<cybox:Properties xsi:type="CodeObj:CodeObjectType">

<CodeObj:Digital_Signatures>

<cyboxCommon:Digital_Signature>jmp

0xAddress_of_hook</cyboxCommon:Digital_Signature>
</CodeObj:Digital_Signatures>
</cybox:Properties>
</cybox:Associated_Object>
</cybox:Associated_Objects>
</maecBundle:Action>
<maecBundle:Action id="get_url_info">
<cybox:Associated_Objects>
<cybox:Associated_Object>
<cybox:Properties xsi:type="HTTPSessionObj:HTTPSessionObjectType">
<HTTPSessionObj:HTTP_Request_Response>
<HTTPSessionObj:HTTP_Client_Request>
<HTTPSessionObj:HTTP_Request_Line>

<HTTPSessionObj:HTTP_Method>GET/POST</HTTPSessionObj:HTTP_Method>
<HTTPSessionObj:Value/>
</HTTPSessionObj:HTTP_Request_Line>
</HTTPSessionObj:HTTP_Client_Request>
</HTTPSessionObj:HTTP_Request_Response>
</cybox:Properties>
</cybox:Associated_Object>
</cybox:Associated_Objects>
</maecBundle:Action>

<maecBundle:Action id="get_http_cookies"/>

<maecBundle:Action id="get_flash_player_cookies"/>

<maecBundle:Action id="get_temporary_request_buffer">

<cybox:Associated_Objects>

<cybox:Associated_Object>

<cybox:Properties xsi:type="APIObj:APIObjectType">

<APIObj:Function_Name>PStoreCreateInstance</APIObj:Function_Name>

</cybox:Properties>

</cybox:Associated_Object>

</cybox:Associated_Objects>

</maecBundle:Action>

<maecBundle:Action id="get_input_data_from_html">

<cybox:Associated_Objects>

<cybox:Associated_Object id="htm_file">

<cybox:Properties xsi:type="FileObj:FileObjectType">

<FileObj:File_Name>*.htm</FileObj:File_Name>

</cybox:Properties>

</cybox:Associated_Object>

<cybox:Associated_Object id="script_code">

<cybox:Properties xsi:type="CodeObj:CodeObjectType">

<CodeObj:Code_Language>html/js</CodeObj:Code_Language>

<CodeObj:Digital_Signatures>

<cyboxCommon:Digital_Signature>*select*</cyboxCommon:Digital_Signature>

<cyboxCommon:Digital_Signature>*option*</cyboxCommon:Digital_Signature>

<cyboxCommon:Digital_Signature>*input data=*</cyboxCommon:Digital_Signature>

</CodeObj:Digital_Signatures>

</cybox:Properties>

</cybox:Associated_Object>

</cybox:Associated_Objects>

</maecBundle:Action>

<maecBundle:Action id="embed_file_with_htm_tags">

<cybox:Name xsi:type="maecVocabs:FileActionNameVocab-1.0">modify file</cybox:Name>

<cybox:Associated_Objects>

<cybox:Associated_Object id="script_code">

<cybox:Properties xsi:type="CodeObj:CodeObjectType">

<CodeObj:Code_Language>html/js</CodeObj:Code_Language>

<CodeObj:Digital_Signatures>

<cyboxCommon:Digital_Signature>*script src=*</cyboxCommon:Digital_Signature>

</CodeObj:Digital_Signatures>

</cybox:Properties>

</cybox:Associated_Object>

```
 </cybox:Associated_Objects>
</maecBundle:Action>
<maecBundle:Action id="new_binary_setup_inline_api_hooking">
 <cybox:Associated_Objects>
  <cybox:Associated_Object id="binary_file">
   <cybox:Properties xsi:type="FileObj:FileObjectType">
    <FileObj:File_Extension>exe</FileObj:File_Extension>
   </cybox:Properties>
  </cybox:Associated_Object>
  <cybox:Associated_Object id="execute_binary">
   <cybox:Properties xsi:type="APIObj:APIObjectType">
    <APIObj:Function_Name>CreateProcess</APIObj:Function_Name>
   </cybox:Properties>
  </cybox:Associated_Object>
 </cybox:Associated_Objects>
</maecBundle:Action>
<maecBundle:Action id="get_query_options_for_request"/>
<maecBundle:Action id="free_memory_for_request"/>
<maecBundle:Action id="check_info_received_in_memory">
 <cybox:Description>Check if the header information retrieved by the API is already
present in the the heap memory for the HTTP request</cybox:Description>
</maecBundle:Action>
<maecBundle:Action id="record_user_password_from_buffer">
```

<cybox:Associated_Objects>
<cybox:Associated_Object id="user_string">
<cybox:Properties xsi:type="CodeObj:CodeObjectType">
<CodeObj:Digital_Signatures>
<cyboxCommon:Digital_Signature>USER </cyboxCommon:Digital_Signature>
</CodeObj:Digital_Signatures>
</cybox:Properties>
</cybox:Associated_Object>
<cybox:Associated_Object id="pass_string">
<cybox:Properties xsi:type="CodeObj:CodeObjectType">
<CodeObj:Digital_Signatures>
<cyboxCommon:Digital_Signature>PASS </cyboxCommon:Digital_Signature>
</CodeObj:Digital_Signatures>
</cybox:Properties>
</cybox:Associated_Object>
</cybox:Associated_Objects>
</maecBundle:Action>
<maecBundle:Action id="record_ftp_information">
<cybox:Associated_Objects>
<cybox:Associated_Object id="type_string">
<cybox:Properties xsi:type="CodeObj:CodeObjectType">
<CodeObj:Digital_Signatures>
<cyboxCommon:Digital_Signature>TYPE</cyboxCommon:Digital_Signature>

```
 </CodeObj:Digital_Signatures>
</cybox:Properties>
</cybox:Associated_Object>
<cybox:Associated_Object id="feat_string">
 <cybox:Properties xsi:type="CodeObj:CodeObjectType">
  <CodeObj:Digital_Signatures>
   <cyboxCommon:Digital_Signature>FEAT</cyboxCommon:Digital_Signature>
  </CodeObj:Digital_Signatures>
 </cybox:Properties>
</cybox:Associated_Object>
<cybox:Associated_Object id="pasv_string">
 <cybox:Properties xsi:type="CodeObj:CodeObjectType">
  <CodeObj:Digital_Signatures>
   <cyboxCommon:Digital_Signature>PASV</cyboxCommon:Digital_Signature>
  </CodeObj:Digital_Signatures>
 </cybox:Properties>
</cybox:Associated_Object>
<cybox:Associated_Object id="stat_string">
 <cybox:Properties xsi:type="CodeObj:CodeObjectType">
  <CodeObj:Digital_Signatures>
   <cyboxCommon:Digital_Signature>STAT</cyboxCommon:Digital_Signature>
  </CodeObj:Digital_Signatures>
 </cybox:Properties>
```

```
   </cybox:Associated_Object>
  </cybox:Associated_Objects>
 </maecBundle:Action>
 <maecBundle:Action id="record_pop3_email_passwords">
  <cybox:Associated_Objects>
   <cybox:Associated_Object>
    <cybox:Properties xsi:type="CodeObj:CodeObjectType">
     <CodeObj:Digital_Signatures>
      <cyboxCommon:Digital_Signature>pop3</cyboxCommon:Digital_Signature>

<cyboxCommon:Digital_Signature>%s://%s:%s@%s/</cyboxCommon:Digital_Signatur
e>
     </CodeObj:Digital_Signatures>
    </cybox:Properties>
   </cybox:Associated_Object>
  </cybox:Associated_Objects>
 </maecBundle:Action>
 <maecBundle:Action id="clear_memory">
  <cybox:Associated_Objects>
   <cybox:Associated_Object>
    <cybox:Properties xsi:type="APIObj:APIObjectType">
     <APIObj:Function_Name>FreeHeap</APIObj:Function_Name>
    </cybox:Properties>
```

```
  </cybox:Associated_Object>
 </cybox:Associated_Objects>
</maecBundle:Action>
<maecBundle:Action id="create_new_buffer"/>
<maecBundle:Action id="get_device_context">
 <cybox:Associated_Objects>
  <cybox:Associated_Object>
   <cybox:Properties xsi:type="APIObj:APIObjectType">
    <APIObj:Function_Name>GetDC</APIObj:Function_Name>
   </cybox:Properties>
  </cybox:Associated_Object>
 </cybox:Associated_Objects>
</maecBundle:Action>
<maecBundle:Action id="get_window_resolution">
 <cybox:Associated_Objects>
  <cybox:Associated_Object>
   <cybox:Properties xsi:type="APIObj:APIObjectType">
    <APIObj:Function_Name>GetWindowInfo</APIObj:Function_Name>
   </cybox:Properties>
  </cybox:Associated_Object>
 </cybox:Associated_Objects>
</maecBundle:Action>
<maecBundle:Action id="create_buffer_for_translate_api_hook"/>
```

<maecBundle:Action id="check_mouse_click"/>

<maecBundle:Action id="generate_screenshot">

<cybox:Associated_Objects>

<cybox:Associated_Object>

<cybox:Properties xsi:type="FileObj:FileObjectType">

<FileObj:File_Name>screenshots\%s\%04x_%08x.jpg</FileObj:File_Name>

</cybox:Properties>

</cybox:Associated_Object>

</cybox:Associated_Objects>

</maecBundle:Action>

<maecBundle:Action id="copy_clipboard_data_to_memory"/>

<maecBundle:Action id="copy_certificates_to_stolen_data_file">

<cybox:Associated_Objects>

<cybox:Associated_Object>

<cybox:Properties xsi:type="FileObj:FileObjectType">

<FileObj:File_Name>certs\\%s_%02u_%02u_%04u.pfx</FileObj:File_Name>

</cybox:Properties>

</cybox:Associated_Object>

</cybox:Associated_Objects>

</maecBundle:Action>

</maecBundle:Actions>

```
 <maecBundle:Candidate_Indicators>
  <!-- Capability CIs -->
  <maecBundle:Candidate_Indicator id="capabilities_id">
   <maecBundle:Composition operator="AND">
    <maecBundle:Capability_Reference capability_idref="persistence"/>
    <maecBundle:Capability_Reference
capability_idref="trojanize_binaries_establish_ipc_mechanism"/>
    <maecBundle:Capability_Reference capability_idref="run_arbitrary_commands"/>
    <maecBundle:Capability_Reference capability_idref="steal_data_from_processes"/>
   </maecBundle:Composition>
  </maecBundle:Candidate_Indicator>
  <!-- Behaviour CIs -->
  <maecBundle:Candidate_Indicator id="persistence_id">
   <maecBundle:Composition operator="AND">
    <maecBundle:Behavior_Reference behavior_idref="persistence_at_runtime_id"/>
    <maecBundle:Behavior_Reference behavior_idref="persistence_across_reboots_id"/>
   </maecBundle:Composition>
  </maecBundle:Candidate_Indicator>
  <maecBundle:Candidate_Indicator
id="trojanize_binaries_establish_ipc_mechanism_id">
   <maecBundle:Composition operator="AND">
    <maecBundle:Behavior_Reference behavior_idref="code_injection_winlogon"/>
    <maecBundle:Behavior_Reference behavior_idref="code_injection_svchost"/>
```

```
 </maecBundle:Composition>
</maecBundle:Candidate_Indicator>
<maecBundle:Candidate_Indicator id="run_arbitrary_commands_id">
 <maecBundle:Composition operator="AND">
  <maecBundle:Behavior_Reference behavior_idref="fetch_commands"/>
  <maecBundle:Behavior_Reference behavior_idref="execute_commands_received"/>
 </maecBundle:Composition>
</maecBundle:Candidate_Indicator>
<maecBundle:Candidate_Indicator id="steal_data_from_processes_id">
 <maecBundle:Composition operator="AND">
  <maecBundle:Behavior_Reference behavior_idref="code_injection_processes"/>

  <maecBundle:Sub_Composition operator="OR">
   <maecBundle:Behavior_Reference behavior_idref="Hook_HttpSendRequests"/>
   <maecBundle:Behavior_Reference behavior_idref="Hook_InternetReadFile"/>
   <maecBundle:Behavior_Reference
behavior_idref="Hook_InternetQueryDataAvaliable"/>
   <maecBundle:Behavior_Reference behavior_idref="Hook_CloseHandle"/>
   <maecBundle:Behavior_Reference behavior_idref="Hook_HttpQueryInfo"/>
   <maecBundle:Behavior_Reference behavior_idref="Hook_Send_WSASend"/>
   <maecBundle:Behavior_Reference behavior_idref="Hook_closesocket"/>
   <maecBundle:Behavior_Reference behavior_idref="Hook_BeginPaint"/>
   <maecBundle:Behavior_Reference behavior_idref="Hook_EndPaint"/>
```

<maecBundle:Behavior_Reference behavior_idref="Hook_DefWindowProc"/>

<maecBundle:Behavior_Reference behavior_idref="Hook_TranslateMessage"/>

<maecBundle:Behavior_Reference behavior_idref="Hook_GetClipboradData"/>

<maecBundle:Behavior_Reference behavior_idref="Hook_PFXImportCertStore"/>

</maecBundle:Sub_Composition>

</maecBundle:Composition>

</maecBundle:Candidate_Indicator>

<!-- Action CIs -->

<maecBundle:Candidate_Indicator id="persistence_at_runtime_id">

<maecBundle:Composition operator="AND">

<maecBundle:Action_Reference action_id="create_mutex_AVIRA_21099"/>

<maecBundle:Action_Reference action_id="create_mutex_AVIRA_2109"/>

<maecBundle:Action_Reference action_id="create_mutex_AVIRA_2108"/>

</maecBundle:Composition>

</maecBundle:Candidate_Indicator>

<maecBundle:Candidate_Indicator id="persistence_across_reboots_id">

<maecBundle:Composition operator="AND">

<maecBundle:Action_Reference action_id="copy_self_to_new_exe"/>

<maecBundle:Action_Reference action_id="modify_registry"/>

```
 </maecBundle:Composition>
</maecBundle:Candidate_Indicator>
<maecBundle:Candidate_Indicator id="code_injection_winlogon_id">
 <maecBundle:Composition operator="AND">
  <maecBundle:Action_Reference action_id="create_config_file"/>
  <maecBundle:Action_Reference action_id="create_stolen_data_file"/>
  <maecBundle:Action_Reference action_id="create_pipe_for_communication_2109"/>
  <maecBundle:Action_Reference
action_id="create_pipe_server_for_config_user_file_access"/>
 </maecBundle:Composition>
</maecBundle:Candidate_Indicator>
<maecBundle:Candidate_Indicator id="code_injection_svchost_id">
 <maecBundle:Composition operator="AND">
  <maecBundle:Action_Reference action_id="configure_registry_with_uniqueID"/>
  <maecBundle:Action_Reference action_id="send_system_info_to_server"/>
  <maecBundle:Action_Reference action_id="create_pipe_for_communication_2108"/>
  <maecBundle:Action_Reference action_id="send_commands_to_other_processes"/>
  <maecBundle:Action_Reference action_id="fetch_config_file_from_cnc"/>
 </maecBundle:Composition>
</maecBundle:Candidate_Indicator>
<maecBundle:Candidate_Indicator id="fetch_commands_id">
 <maecBundle:Composition operator="OR">
  <maecBundle:Action_Reference
```

action_id="fetch_commands_to_execute_from_cnc"/>
  </maecBundle:Composition>
 </maecBundle:Candidate_Indicator>
 <maecBundle:Candidate_Indicator id="execute_commands_received_id">
  <maecBundle:Composition operator="OR">
   <maecBundle:Action_Reference action_id="reboot_target"/>
   <maecBundle:Action_Reference action_id="shutdown_system"/>
   <maecBundle:Action_Reference action_id="update_config_file"/>
   <maecBundle:Action_Reference action_id="kill_malware"/>
   <maecBundle:Action_Reference action_id="rename_target"/>
   <maecBundle:Action_Reference action_id="upload_stolen_certificates"/>
   <maecBundle:Action_Reference action_id="upload_flash_player_cookies"/>
   <maecBundle:Action_Reference action_id="delete_flash_player_cookies"/>
   <maecBundle:Action_Reference action_id="set_home_page_of_IE"/>
   <maecBundle:Action_Reference action_id="block_url"/>
   <maecBundle:Action_Reference action_id="unblock_url"/>
   <maecBundle:Action_Reference action_id="download_binary_and_execute_binary"/>
   <maecBundle:Action_Reference action_id="execute_local_file"/>
  </maecBundle:Composition>
 </maecBundle:Candidate_Indicator>
 <maecBundle:Candidate_Indicator id="code_injection_processes_id">
  <maecBundle:Composition operator="AND">
   <maecBundle:Action_Reference action_id="list_processes"/>

<maecBundle:Action_Reference action_id="open_process"/>

<maecBundle:Action_Reference action_id="copy_self_to_process"/>

<maecBundle:Action_Reference action_id="setup_inline_api_hooking"/>

</maecBundle:Composition>

</maecBundle:Candidate_Indicator>

<maecBundle:Candidate_Indicator id="Hook_HttpSendRequests_id">

<maecBundle:Composition operator="OR">

<maecBundle:Action_Reference action_id="get_url_info"/>

<maecBundle:Action_Reference action_id="get_http_cookies"/>

<maecBundle:Action_Reference action_id="get_flash_player_cookies"/>

<maecBundle:Action_Reference action_id="get_temporary_request_buffer"/>

<maecBundle:Action_Reference action_id="get_input_data_from_html"/>

</maecBundle:Composition>

</maecBundle:Candidate_Indicator>

<maecBundle:Candidate_Indicator id="Hook_InternetReadFile_id">

<maecBundle:Composition operator="OR">

<maecBundle:Action_Reference action_id="embed_file_with_htm_tags"/>

<maecBundle:Action_Reference action_id="new_binary_setup_inline_api_hooking"/>

</maecBundle:Composition>

</maecBundle:Candidate_Indicator>

<maecBundle:Candidate_Indicator id="Hook_InternetQueryDataAvaliable_id">

<maecBundle:Composition operator="OR">

<maecBundle:Action_Reference action_id="get_query_options_for_request"/>

```
 </maecBundle:Composition>
</maecBundle:Candidate_Indicator>
<maecBundle:Candidate_Indicator id="Hook_CloseHandle_id">
 <maecBundle:Composition operator="OR">
  <maecBundle:Action_Reference action_id="free_memory_for_request"/>
 </maecBundle:Composition>
</maecBundle:Candidate_Indicator>
<maecBundle:Candidate_Indicator id="Hook_HttpQueryInfo_id">
 <maecBundle:Composition operator="OR">
  <maecBundle:Action_Reference action_id="check_info_received_in_memory"/>
 </maecBundle:Composition>
</maecBundle:Candidate_Indicator>
<maecBundle:Candidate_Indicator id="Hook_Send_WSASend_id">
 <maecBundle:Composition operator="OR">
  <maecBundle:Action_Reference action_id="record_user_password_from_buffer"/>
  <maecBundle:Action_Reference action_id="record_ftp_information"/>
  <maecBundle:Action_Reference action_id="record_pop3_email_passwords"/>
 </maecBundle:Composition>
</maecBundle:Candidate_Indicator>
<maecBundle:Candidate_Indicator id="Hook_closesocket_id">
 <maecBundle:Composition operator="OR">
  <maecBundle:Action_Reference action_id="clear_memory"/>
 </maecBundle:Composition>
```

```
</maecBundle:Candidate_Indicator>
<maecBundle:Candidate_Indicator id="Hook_BeginPaint_id">
 <maecBundle:Composition operator="OR">
  <maecBundle:Action_Reference action_id="create_new_buffer"/>
 </maecBundle:Composition>
</maecBundle:Candidate_Indicator>
<maecBundle:Candidate_Indicator id="Hook_EndPaint_id">
 <maecBundle:Composition operator="OR">
  <maecBundle:Action_Reference action_id="clear_memory"/>
 </maecBundle:Composition>
</maecBundle:Candidate_Indicator>
<maecBundle:Candidate_Indicator id="Hook_DefWindowProc_id">
 <maecBundle:Composition operator="AND">
  <maecBundle:Action_Reference action_id="get_device_context"/>
  <maecBundle:Action_Reference action_id="get_window_resolution"/>
  <maecBundle:Action_Reference action_id="create_buffer_for_translate_api_hook"/>
 </maecBundle:Composition>
</maecBundle:Candidate_Indicator>
<maecBundle:Candidate_Indicator id="Hook_TranslateMessage_id">
 <maecBundle:Composition operator="AND">
  <maecBundle:Action_Reference action_id="check_mouse_click"/>
  <maecBundle:Action_Reference action_id="generate_screenshot"/>
 </maecBundle:Composition>
```

```
</maecBundle:Candidate_Indicator>
<maecBundle:Candidate_Indicator id="Hook_GetClipboradData_id">
 <maecBundle:Composition operator="AND">
  <maecBundle:Action_Reference action_id="copy_clipboard_data_to_memory"/>
 </maecBundle:Composition>
</maecBundle:Candidate_Indicator>
<maecBundle:Candidate_Indicator id="Hook_PFXImportCertStore_id">
 <maecBundle:Composition operator="AND">
  <maecBundle:Action_Reference action_id="copy_certificates_to_stolen_data_file"/>
 </maecBundle:Composition>
</maecBundle:Candidate_Indicator>

<!-- Object CIs -->
<maecBundle:Candidate_Indicator id="query_system_info_id">
 <maecBundle:Composition operator="AND">
  <maecBundle:Object_Reference object_idref="installdate"/>
  <maecBundle:Object_Reference object_idref="digitalproductid"/>
 </maecBundle:Composition>
</maecBundle:Candidate_Indicator>
<maecBundle:Candidate_Indicator id="fetch_config_file_from_cnc_id">
 <maecBundle:Composition>
  <maecBundle:Object_Reference object_idref="cnc_url"/>
  <maecBundle:Object_Reference object_idref="config_file"/>
```

```
 </maecBundle:Composition>
</maecBundle:Candidate_Indicator>
<maecBundle:Candidate_Indicator id="get_input_data_from_html_id">
 <maecBundle:Composition>
  <maecBundle:Object_Reference object_idref="htm_file"/>
  <maecBundle:Object_Reference object_idref="script_code"/>
 </maecBundle:Composition>
</maecBundle:Candidate_Indicator>
<maecBundle:Candidate_Indicator id="new_binary_setup_inline_api_hooking_id">
 <maecBundle:Composition operator="AND">
  <maecBundle:Object_Reference object_idref="binary_file"/>
  <maecBundle:Object_Reference object_idref="execute_binary"/>
 </maecBundle:Composition>
</maecBundle:Candidate_Indicator>
<maecBundle:Candidate_Indicator id="record_user_password_from_buffer_id">
 <maecBundle:Composition operator="AND">
  <maecBundle:Object_Reference object_idref="user_string"/>
  <maecBundle:Object_Reference object_idref="pass_string"/>
 </maecBundle:Composition>
</maecBundle:Candidate_Indicator>
<maecBundle:Candidate_Indicator id="record_ftp_information_id">
 <maecBundle:Composition operator="AND">
  <maecBundle:Object_Reference object_idref="type_string"/>
```

<maecBundle:Object_Reference object_idref="feat_string"/>

<maecBundle:Object_Reference object_idref="pasv_string"/>

<maecBundle:Object_Reference object_idref="stat_string"/>

</maecBundle:Composition>

</maecBundle:Candidate_Indicator>

</maecBundle:Candidate_Indicators>

</maecBundle:MAEC_Bundle>

APPENDIX B

PICTORAL REPRESENTATION OF THREAT TREES

B.1 Bangat

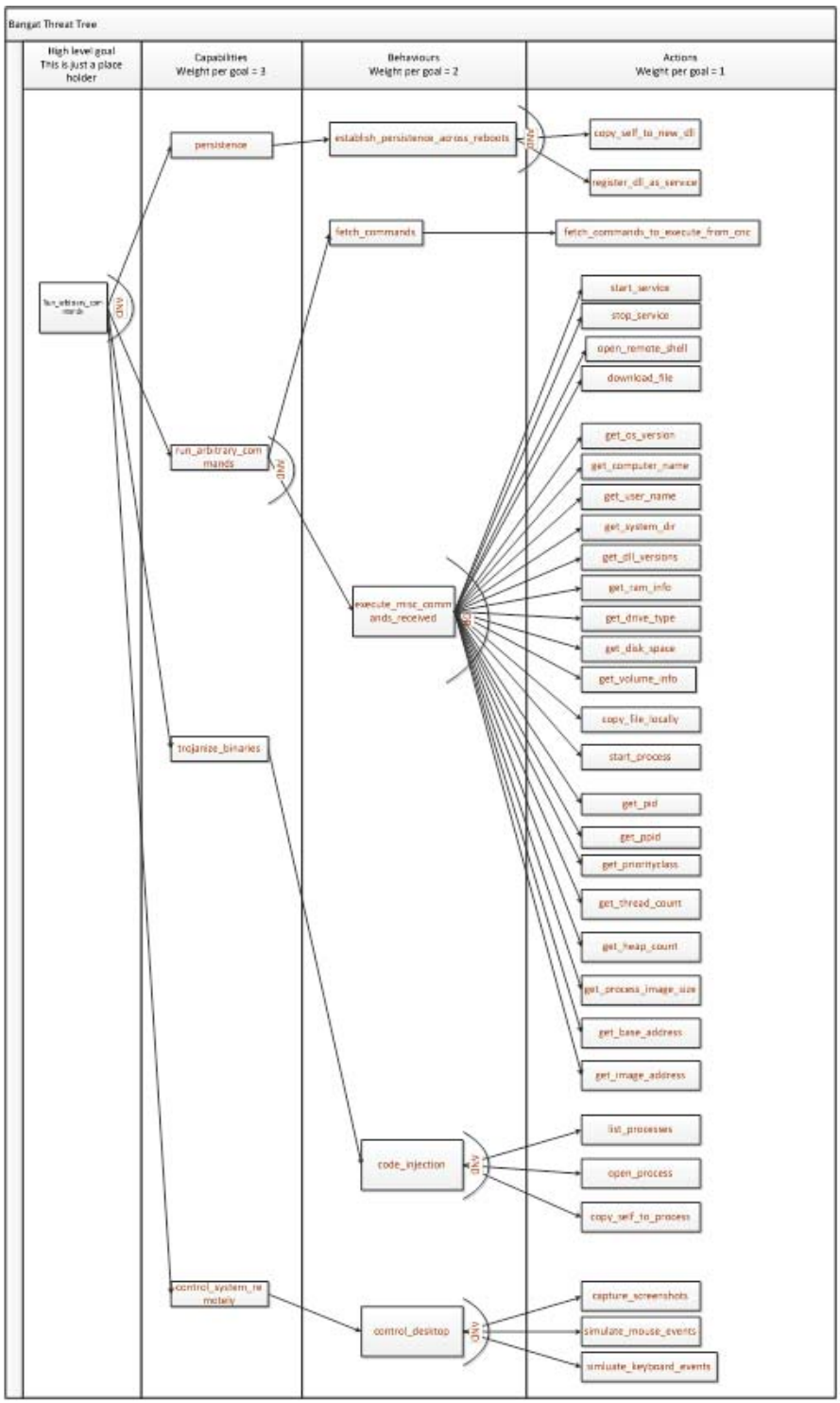

Figure B.1 Bangat Threat Tree

B.2 Beebus

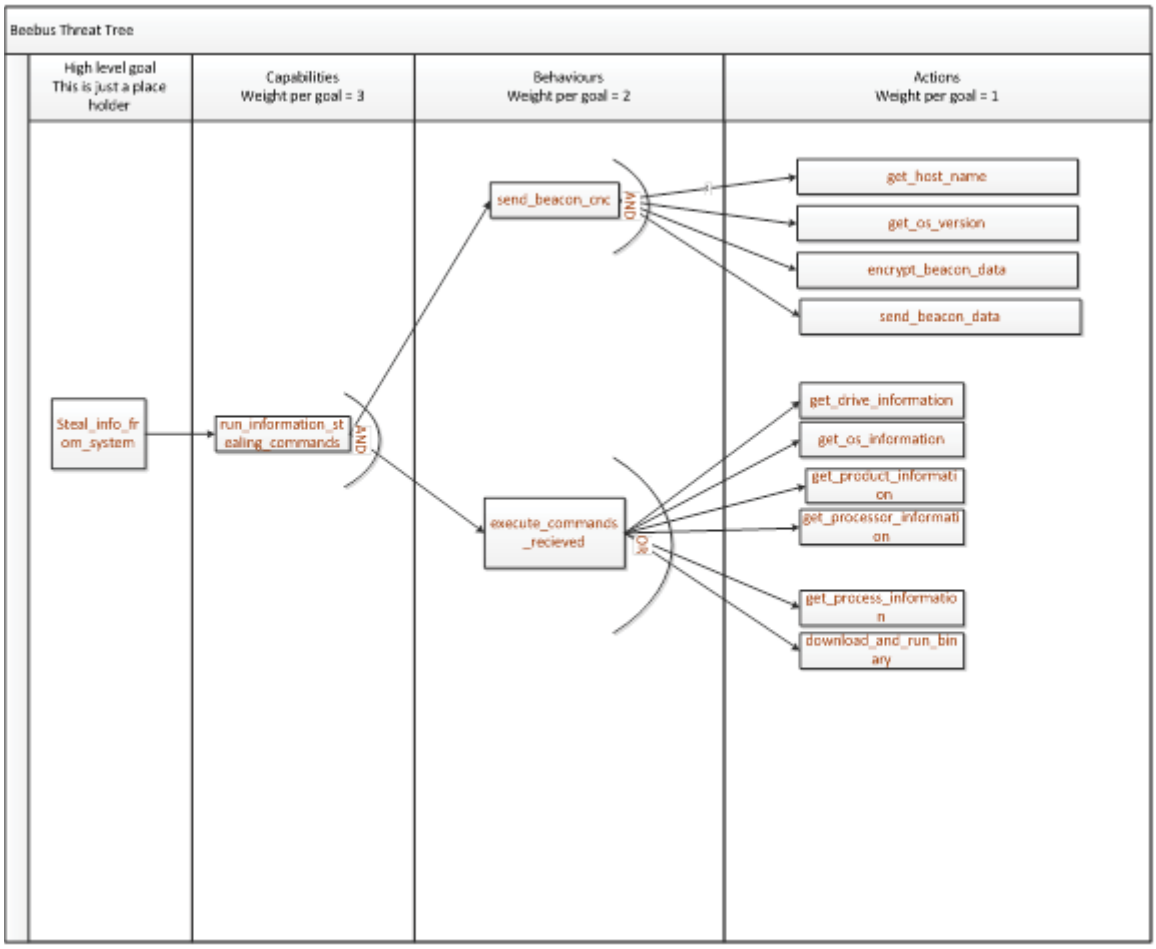

Figure B.2 Beebus Threat Tree

B.3 Cryptolocker

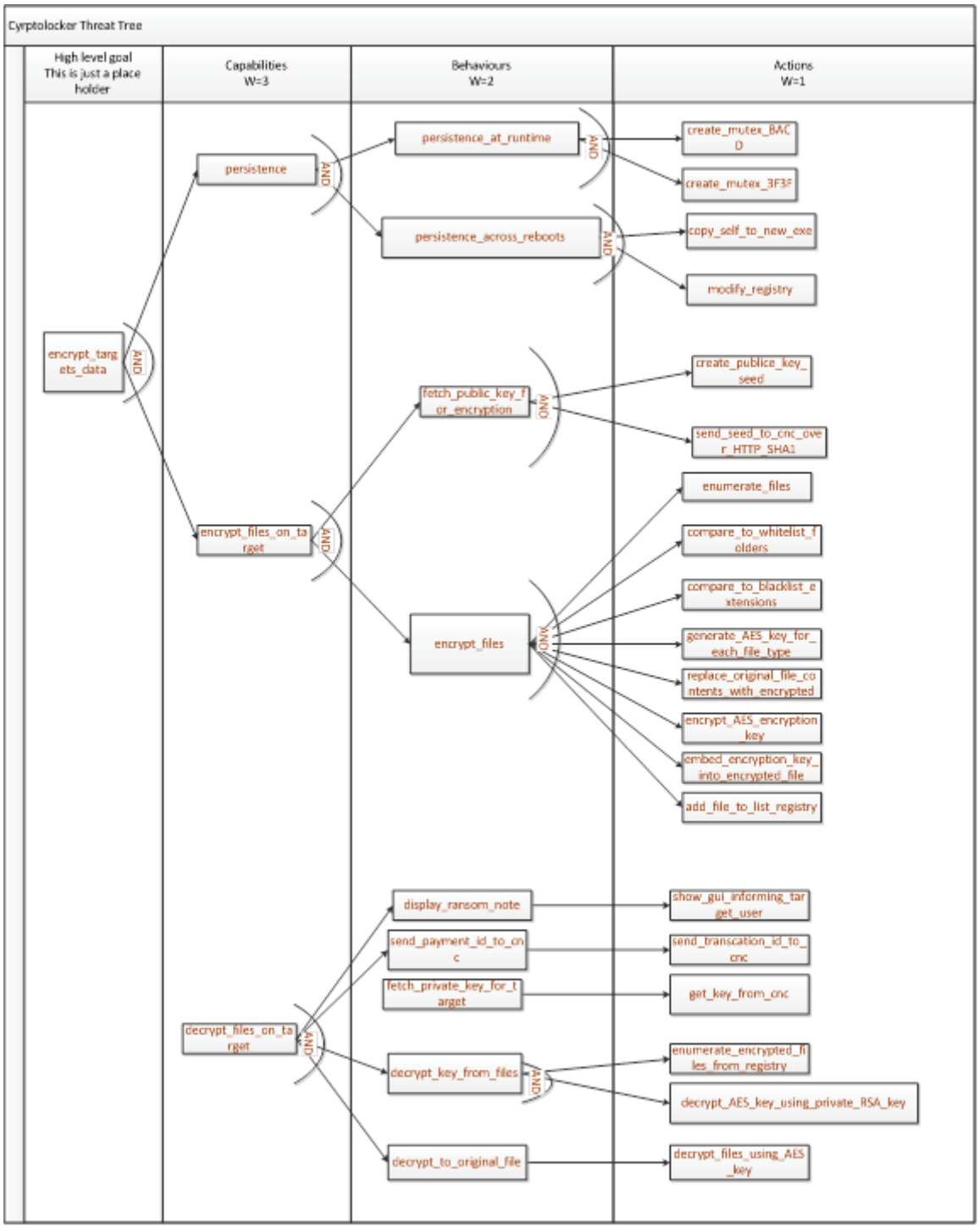

Figure B.3 Cryptolocker Threat Tree

B.4 WebC2-Cson

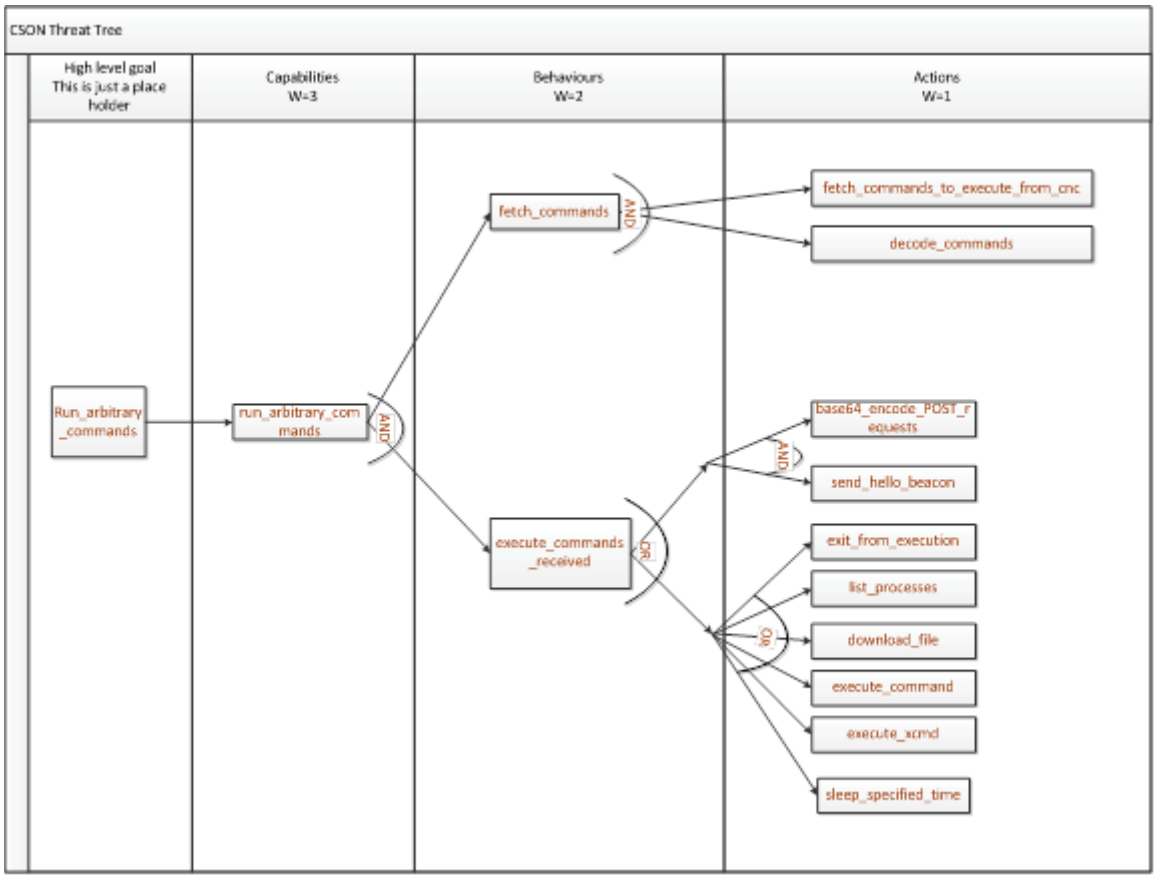

Figure B.4 WebC2-CSON Threat Tree

B.5 Glooxmail

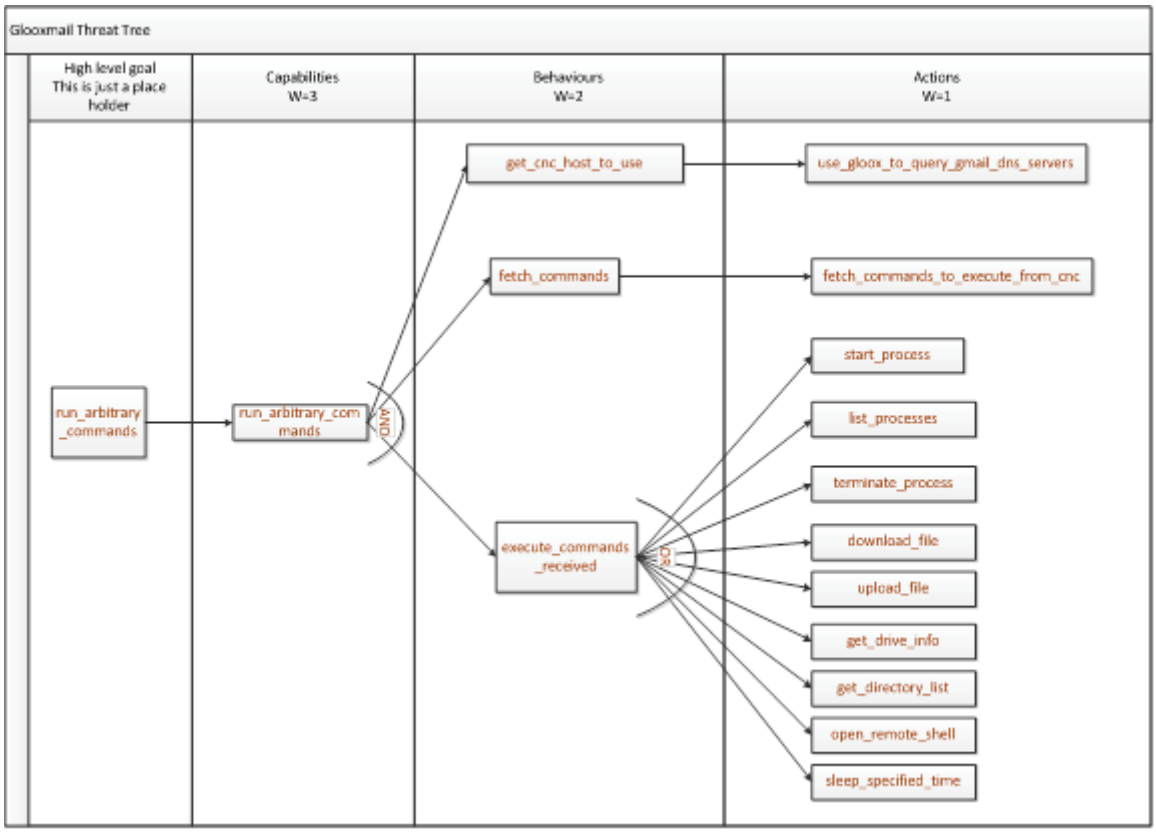

Figure B.5 Glooxmail Threat Tree

B.6 WebC2-Greencat

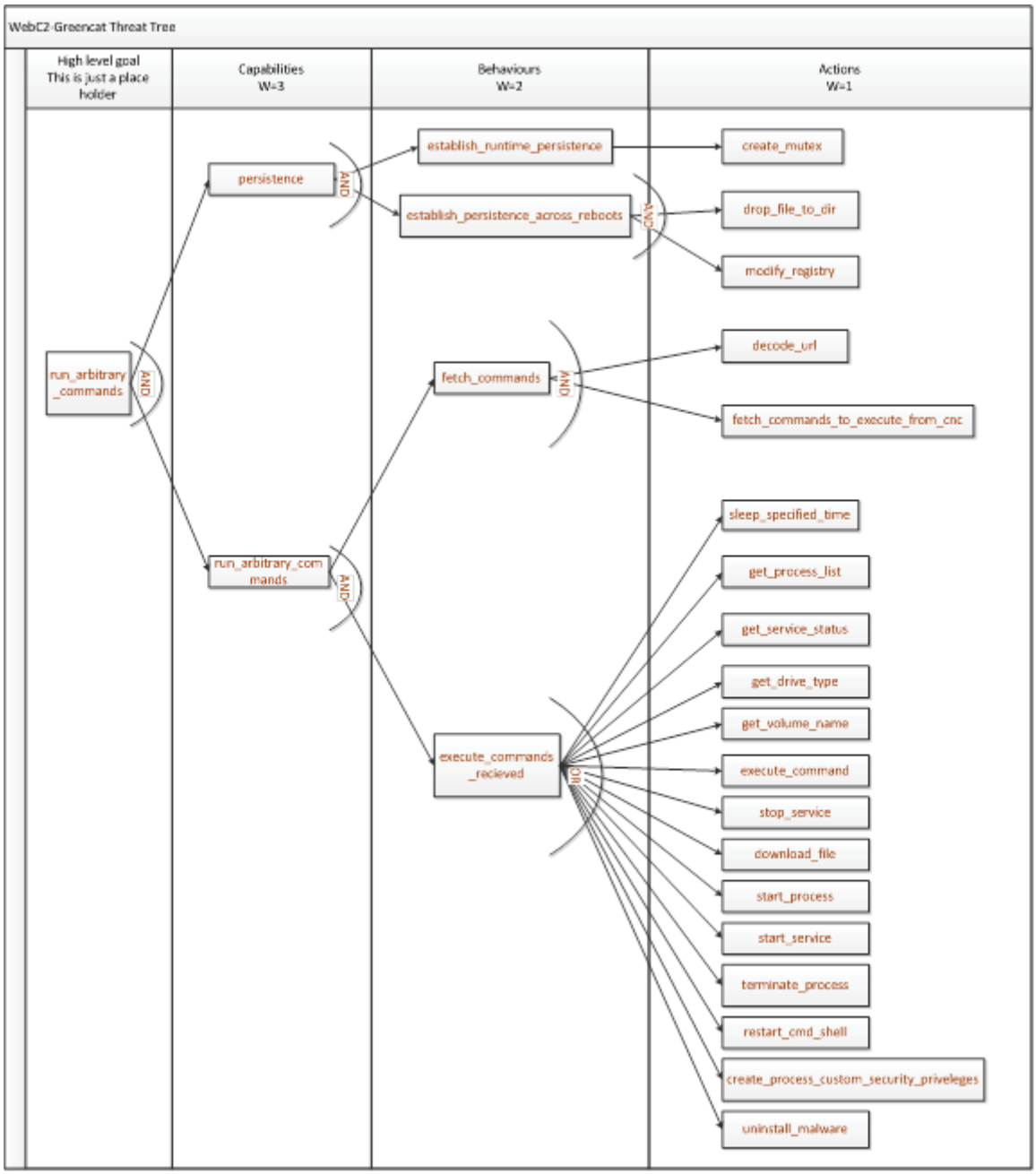

Figure B.6 WebC2-Greencat Threat Tree

B.7 HacDef.A

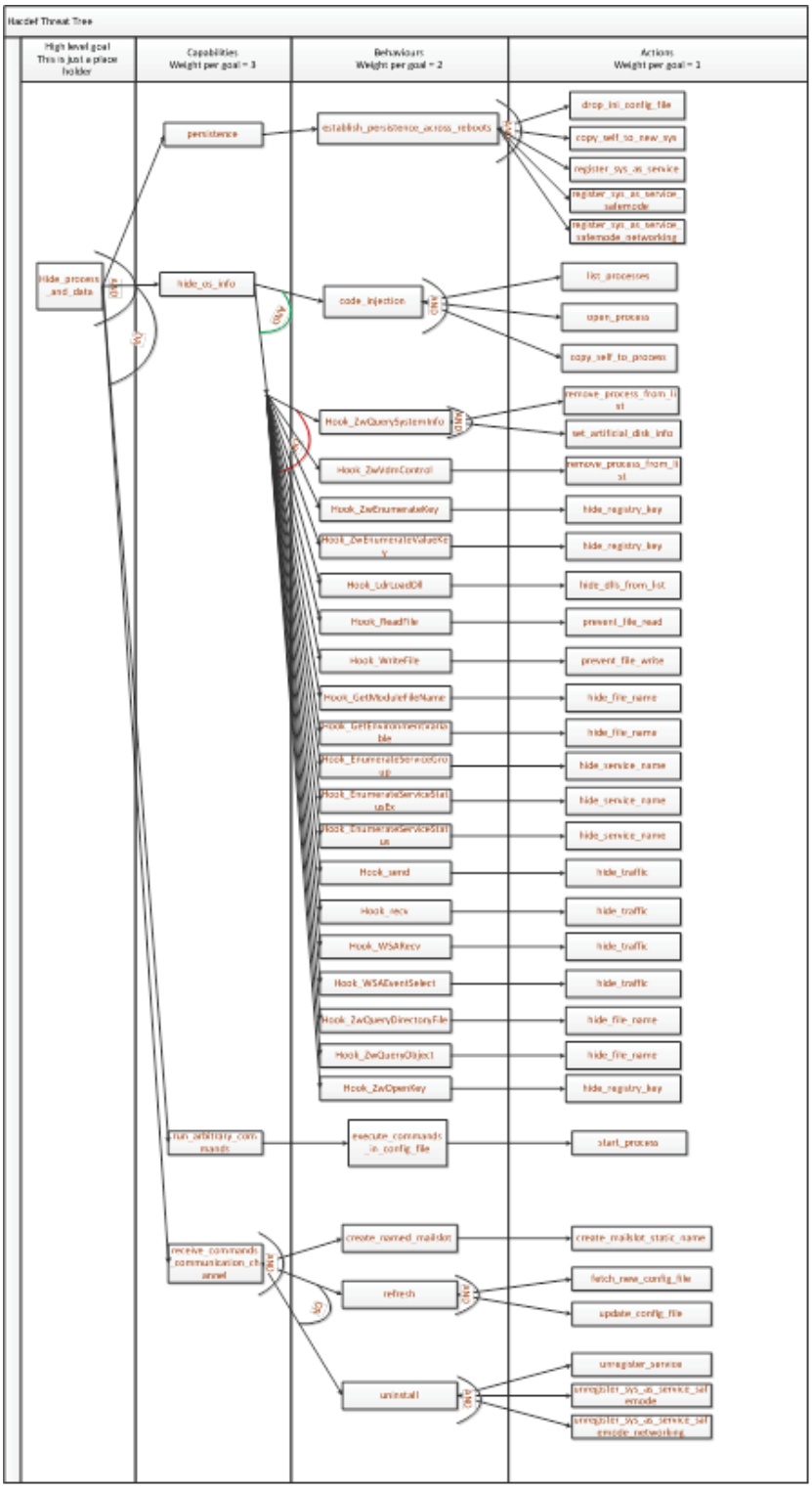

Figure B.7 Hacdef.A Threat Tree

B.8 Sality.A

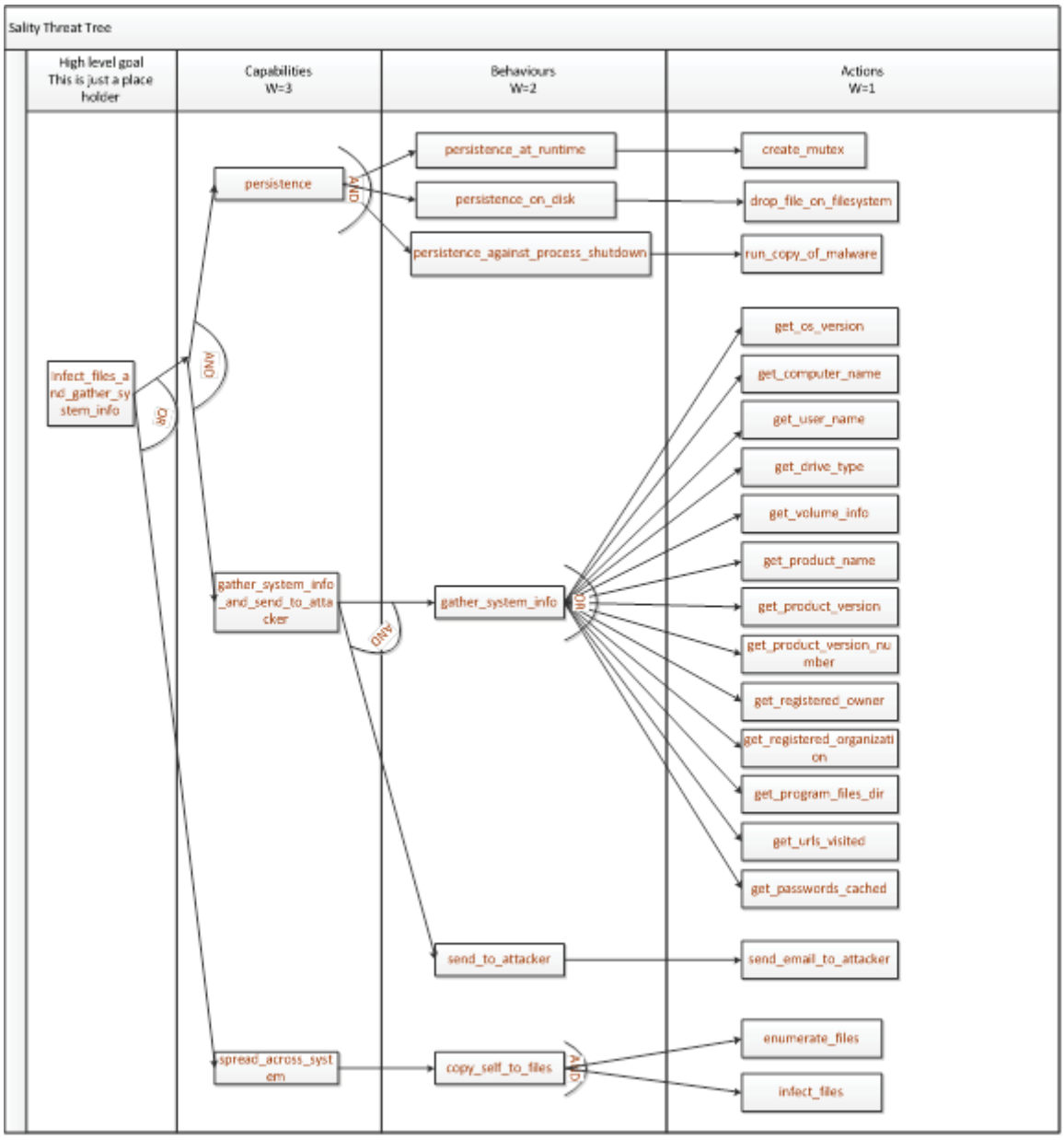

Figure B.8 Sality.A Threat Tree

B.9 Shellcode_PDF_JS

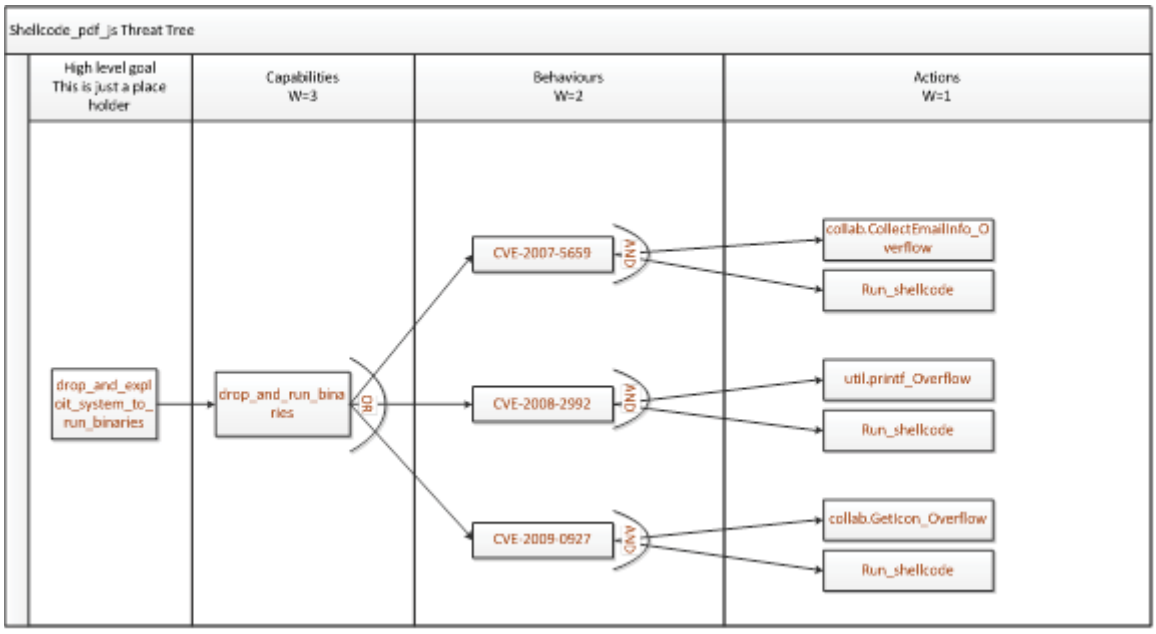

Figure B.9 Shellcode_PDF_JS Threat Tree

B.10 Xorer.F

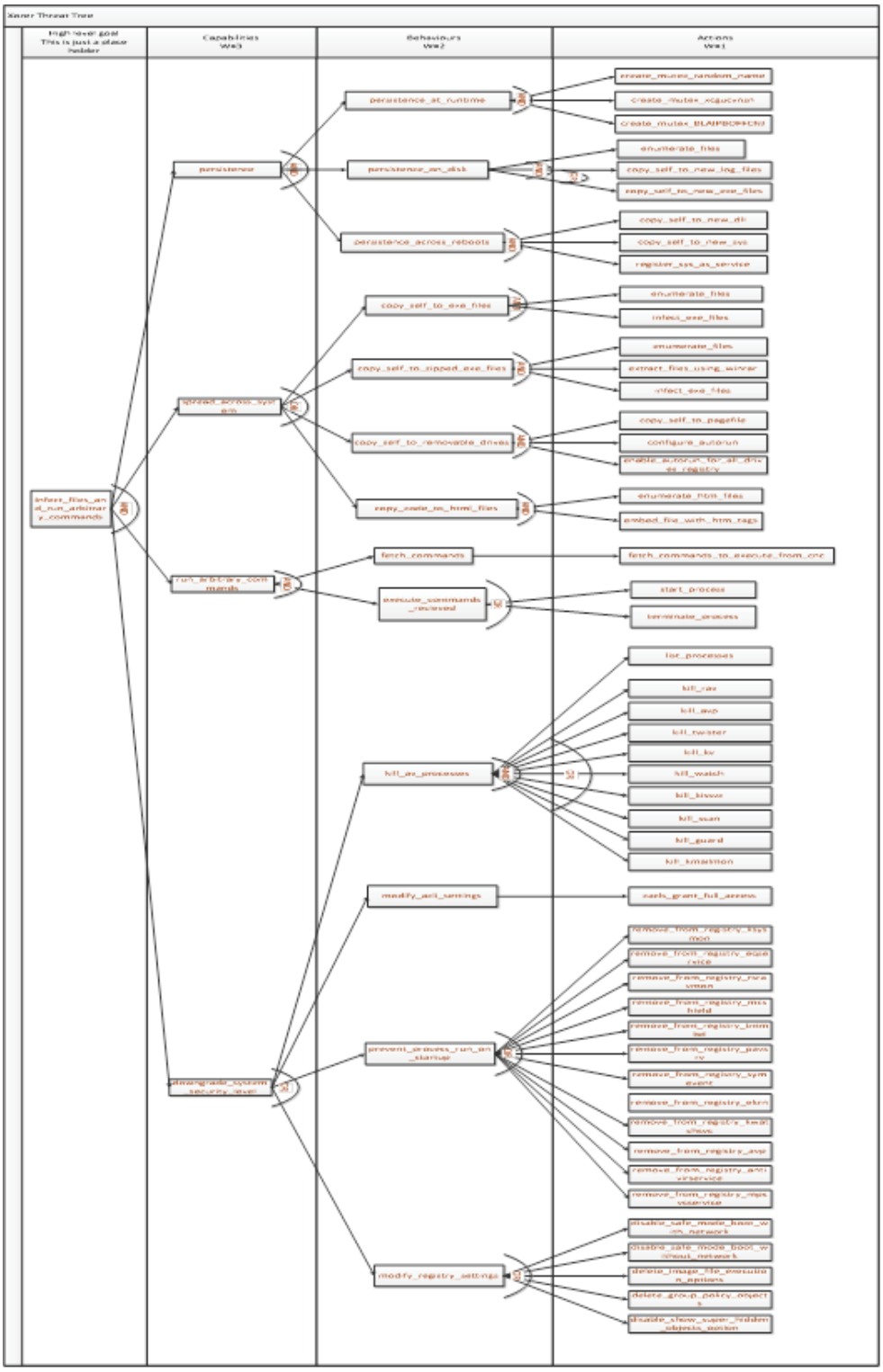

Figure B.10 Xorer.F Threat Tree

B.11 Zbot.gen!R

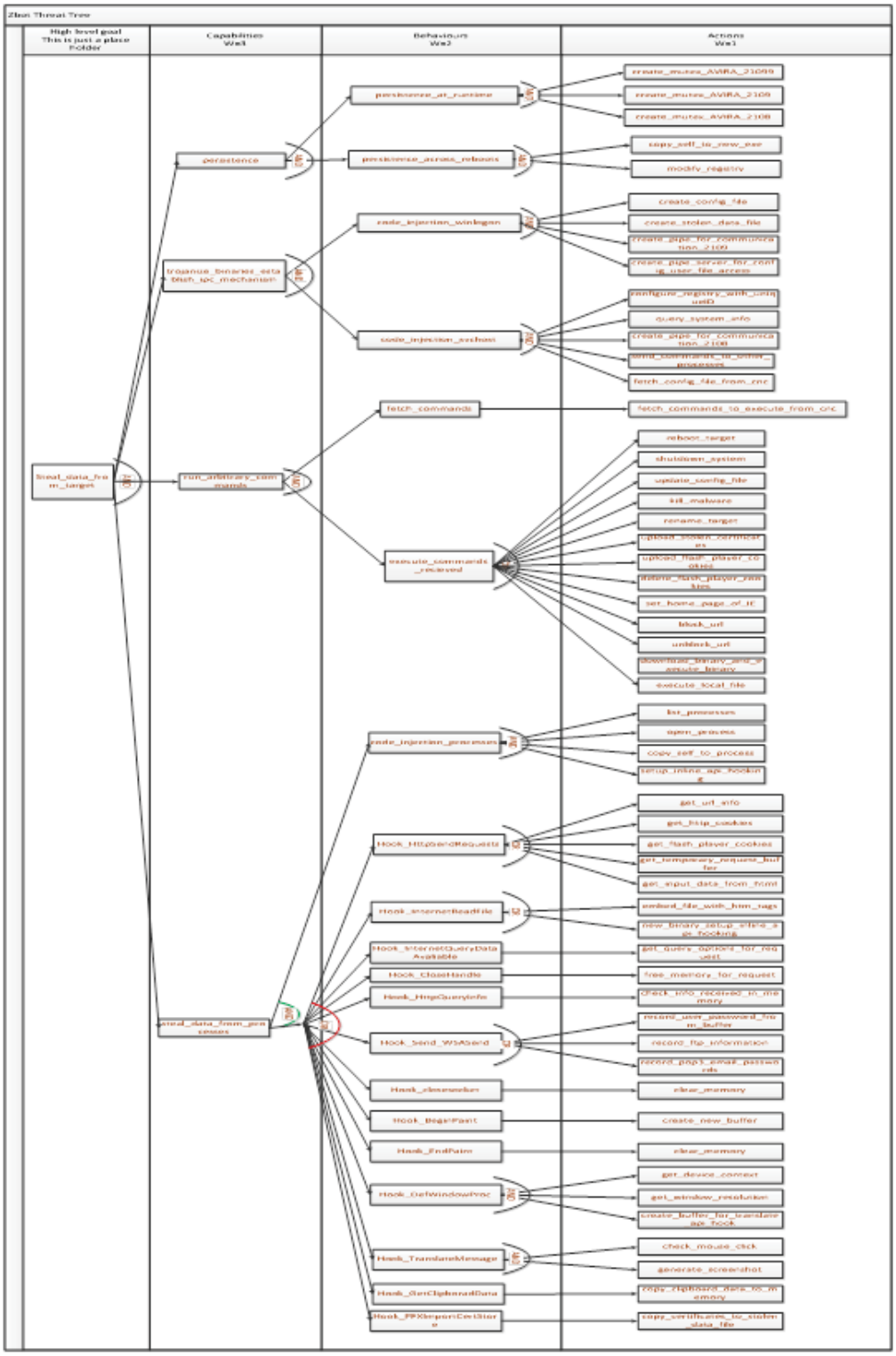

Figure B.11 Zbot.gen!R Threat Tree