YAŞAR UNIVERSITY
GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES

PHD THESIS

FORTIFYING APT DEFENSE SYSTEM BY CREATING LOG RULESETS

ADEM ŞİMŞEK

THESIS ADVISOR: ASSOC. PROF. DR. AHMET KOLTUKSUZ

COMPUTER ENGINEERING

PRESENTATION DATE: 18.09.2018

BORNOVA / İZMİR
SEPTEMBER 2018

We certify that, as the jury, we have read this thesis and that in our opinion it is fully adequate, in scope and in quality, as a thesis for the degree of the Doctor of Philosophy.

Jury Members: **Signature:**

Assoc. Prof. Dr. Ahmet KOLTUKSUZ
Yaşar University ....

Dr. Mutlu BEYAZIT
Yaşar University ....

Dr. Selma TEKİR
Izmir Institute of Technology ....

Dr. Tuğkan TUĞLULAR
Izmir Institute of Technology ....

Assoc. Prof. Dr. Ayşegül ALAYBEYOĞLU
Izmir Katip Çelebi University ....

Prof. Dr. Cüneyt GÜZELİŞ
Director of the Graduate School of
Natural and Applied Sciences

ABSTRACT

FORTIFYING APT DEFENSE SYSTEM

BY CREATING LOG RULESETS

Şimşek, Adem
PHD, Computer Engineering
Advisor: Assoc. Prof. Dr. Ahmet Koltuksuz
September 2018

This thesis strives to investigate advanced persistent threats (APT). Indicators of compromise give advantanges for researchers to fortify security defence system. By analyzing indicators thesis aims to have new log rulesets. This thesis mainly aims to strengthen the defensive system through the traces that the APTs leave behind during the attack. In order to achieve this goal intends to create Security Information Event Management log rulesets.

Key Words: information security, advanced persistent threat, indicator of compromise, log management, security information event management

ÖZ

LOG KURALSETLERI YARATARAK

APT SAVUNMA SISTEMININ GÜÇLENDIRILMESI

Şimşek, Adem
Doktora Tezi, Bilgisayar Mühendisliği
Danışman: Doç. Dr. Ahmet Koltuksuz
Eylül 2018

Bu tez ileri seviye dirençli tehditleri araştırmak için çabalamaktadır. Tehdit göstergeleri araştırmacılara savunma sistemini güçlendirmek için avantajlar sağlar. Göstergeleri analiz ederek yeni log kurallarına sahip olmak istenmektedir. Bu tez temel olarak saldırı sırasında tehditlerin geride bıraktığı izler yoluyla güvenlik savunma sisteminin güçlendirilmesi hedeflenmektedir. Bu hedefe ulaşmak için güvenlik bilgi olay yönetimi sistem günlüğü kuralları oluşturmayı amaçlamaktadır.

Anahtar Kelimeler: bilgi güvenliği, ileri seviye dirençli tehdit, tehlikeli gösterge, sistem günlüğü yönetimi, güvenlik bilgi olay yönetimi

ACKNOWLEDGEMENTS

First of all, I would like to thank my supervisor Assoc. Prof. Dr. Ahmet Koltuksuz for his guidance and patience during this study.

I would like to express my enduring love to my parents, who are always supportive, loving and caring to me in every possible way in my life.

Adem Şimşek
İzmir, 2018

TEXT OF OATH

I declare and honestly confirm that my study, titled "FORTIFYING APT DEFENSE SYSTEM BY CREATING LOG RULESETS" and presented as a PhD Thesis, has been written without applying to any assistance inconsistent with scientific ethics and traditions. I declare, to the best of my knowledge and belief, that all content and ideas drawn directly or indirectly from external sources are indicated in the text and listed in the list of references.

Adem Şimşek

Signature

....

September 21, 2018

TABLE OF CONTENTS

ABSTRACT v

ÖZ vii

ACKNOWLEDGEMENTS ix

TEXT OF OATH xi

TABLE OF CONTENTS xiii

LIST OF FIGURES xvii

SYMBOLS AND ABBREVIATIONS xix

CHAPTER 1 INTRODUCTION 1

1.1. Subject of the Thesis 1

1.2. Aims and Problem Definition 1

1.3. Context of the Thesis 3

1.4. Structure of the Thesis 4

CHAPTER 2 ACTIVE APT ATTACKS 5

2.1. Duke Family 5

2.2. Dark Hotel 7

2.3. Uroburous 8

2.4. Dragonfly 10

2.5. Adwind 11

2.6. Blue Termite 12

2.7. APT28 13

2.8. Equation 14

2.9. NetTraveler 15

2.10. Regin 16

2.11. Duqu 17

2.12. Wild Neutron 18

2.13. Winnti 20

2.14. Poseidon 21

2.15. FinSpy 22

2.16. Black Energy 24

2.17. Hacking Team RCS 25

2.18. Naikon 27

2.19. Cloud Atlas 28

2.20. Hellsing 30
2.21. Kimsuky 31
2.22. Carbanak 32

CHAPTER 3 IN PURSUIT OF INDICATORS 35
3.1. Related works 35
3.2. Determining Attack Indicators 37
3.2.1. Duke Family 37
3.2.2. Dark Hotel 37
3.2.3. Uroburous 38
3.2.4. Dragonfly 38
3.2.5. Adwind 38
3.2.6. Blue Termite 39
3.2.7. APT28 39
3.2.8. Equation 39
3.2.9. NetTraveler 39
3.2.10. Regin 40
3.2.11. Duqu 41
3.2.12. Wild Neutron 41
3.2.13. Winnti 42
3.2.14. Poseidon 42
3.2.15. FinSpy 42
3.2.16. Black Energy 43
3.2.17. Hacking Team RCS 43
3.2.18. Naikon 44
3.2.19. Cloud Atlas 44
3.2.20. Hellsing 45
3.2.21. Kimsuky 45
3.2.22. Carbanak 45

CHAPTER 4 IMPLEMENTATION 47

4.1. Infrastructure 47
4.2. Creating Rulesets 51
4.3. Outputs of Rulesets 60

CHAPTER 5 LISTING OF RESULTS 61

CHAPTER 6 DISCUSSION 63
6.1. Future Works 65

CHAPTER 7 CONCLUSIONS 66

REFERENCES 69

APPENDIX 1 – Json Formatted Rulesets 77

APPENDIX 2 – Outputs Of Rulesets On Elk Platform 83

LIST OF FIGURES

Figure 2.1 Snake Virtual File System architecture 9

Figure 4.1 Open Source APT Log Analysing Framework.. 48

Figure 4.2 Registry Changes - Event when a registry key is created or modified. 49

Figure 4.3 File Changes - Event when a file is copied or changed....................................... 50

Figure 4.4 Privilege Escalation - Event when a member added to Adminstrators group. 51

Figure 5.1 Ruleset table of attacks, 1/4.. 61

Figure 5.2 Ruleset table of attacks, 2/4.. 62

Figure 5.3 Ruleset table of attacks, 3/4.. 62

Figure 5.4 Ruleset table of attacks, 4/4.. 62

Figure 6.1 Phases that non-generated log rules... 64

Figure 6.2 Relationship between phases.. 65

SYMBOLS AND ABBREVIATIONS

ABBREVIATIONS:

APT	Advanced Persisten Threat
SIEM	Security Information Event Management
BSD	Berkeley Software Design
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
ELK	Elasticsearch Logstash Kibana
SOC	Secırity Operation Center
CSIRT	Computer Security Information Response Teams
FTP	File Transfer Protocol
TCP	Transmission Control Protocol
HTTP	Hypertext Transfer Protocol
SCADA	Supervisory Control and Data Acquisition

CHAPTER 1
INTRODUCTION

1.1. Subject of the Thesis

The subject of thesis consists of cyber attacks, advanced persistent threat types and defense systems. During this study, known 22 advanced persistent threats were researched and reviewed. Stages of these attacks, the most used technics and indicators of compromised of incidents were searched and prepared for examination in the applied lab.

Developed defense systems towards cyber attacks such as firewall, e-mail security, IDS and IPS systems were examined. Active and passive defense systems, log management, security information and event management (SIEM) frameworks were investigated. SIEM architecture and core rule databases are reviewed.

In order to fortify passive defensive system against advanced persistent threats, a dozen of log rule sets were researched and created, demonstration of logs and monitoring alerts were explored.

1.2. Aims and Problem Definition

Information Technologies are becoming very important and dominant in daily life for individuals and communities. Everything is meanly being of digitalized. In this frame a term of cyber wars are more real than conventional wars. As a sample of Stuxnet is explaining how cyber-attacks and defenses could be organized. Why cyber wars are occured, the reasons like as national benefits and priorities, industrial sabotages, to conquer secret documents, infiltrate commercial data can give the best answer to this question. So it can be agreed that this war is strategically as meanly described as APT (Advanced Persistent Threat).

The most known APTs start with “The Cuckoo’s Egg” in 1989 and has carried on until now. One of the properties of an APT attack is to behave silently, that means no one knows when APT attack starts. For instance, one of the known APT attack was

“Eurograbber” that appeared in December 2012, and “attack was used to steal an estimated €36 million from over 30,000 customers of over 30 banks in Italy, Spain, Germany and Holland”. (IT BusinessEdge, 2018) Most of the APTs have been used to steal information or to damage critical infrastructures. This war is between countries, so it can affect many people over time.

APTs could not be easily detected by users and there is low chance to detect in any normal data processing in daily life. So, it does not sense to have a look for APTs at enclosed seas. As such, Stuxnet case has created a butterfly effect on states by changes on national security strategies, and noticing security risks on critical infrastructures. Meanwhile, this case will be a reference point for the next APT cases, and will be a good experiment for states.

APT attacks can be prevented by cooperationist and multi-dimensional defense systems. According to unsteady feature of attacks we cannot insist steady defense solutions. Defense solution types need to be various according to this disposition of complex information structures. So it needs to have progressed as innovative, extensive, and self-developing as new generation and sustainable defense systems.

Firewall, e-mail security, IDS/IPS, network monitoring, anti-virus are the tools to detect the APT attacks but also log management system. Every tool has self-effect but effect to whole system is more important. Log is a system which registers the entries in a pool to activate them to detect the attacks where is need. Correlation and security information and event management (SIEM) are armament of log system which alerts the users for attacks. SIEM is open-ended and optimizing operation system that gives the operators flexible using tool, “it gives enterprise security professionals both insight into and a track record of the activities within their IT environment”.

Multi-dimensional and continuously active attacks threat the defense solutions. So there will be need advanced rules and algorithms which they may be missing in log system as default and not advanced. The log system needs to be designed as smart tool to activate itself repeatedly.

This thesis strives to investigate advanced persistent threats, lifecycles of APTs and indicators while act on compromised machine, indicator/incident of compromise give advantanges for researchers to fortify defence system. By analyzing indicators thesis aims to have new log rule sets. Thus, it is hoped that the work will add new security rules in the APT heading to SIEM policies in log management systems. It is also aimed at strengthening the institutional security infrastructure such as Security operation centers (SOC) or computer security information response teams (CSIRT).

This thesis mainly aims to strengthen the defensive system through the traces that the APTs leave behind during the attack. In order to achieve this goal aims to create SIEM log rule sets.

1.3. Context of the Thesis

This thesis content is based on advanced persisten threats, foundamental phases of active APTs, indicators of comprime and defensive log rule sets. At the first part of this work; definition known active 22 APT, basic features, target areas, specific persistences and exfiltration techniques were researched and investigated.

Investigation of APT attacks can create an input for various defense techniques. Sometimes they can be a firewall, an e-mail security system or an IPS / IDS system. With the developing log systems, it is now possible to add a corporate log management system to this defense system. With the created SIEM rules, any events in the network traffic or a bad scenario that may be experienced in a server can be monitored and the compliance with these rules can be checked at desired periods.

In this context, this thesis examines the possibility of establishing SIEM rule sets in stopping and detecting target-focused attacks. Whether or not the traces of the attacks show an integrity is to reveal whether the multiple arcs have the same behavioral algorithm. Thus, a strong defense structure can be established with alarms and feedback from log management system for defensive security.

There are a number of situations that limit work. As such, the study was conducted over 22 APT events active between 2014 and 2016. The new forms of attack occurring during and after the study were not evaluated within the scope of this thesis.

1.4. Structure of the Thesis

Chapter 2 analyses phases of advanced persistent threats. For each of attack type definition, features, target, persistence and exfiltration details were described as well. Totally 22 APT attack type were investigated and researched.

Chapter 3 begins with a literature search that examines some of the previous studies on attack indicators. At this point, the most prominent types of rule have been examined, and what has to be observed in attack indicators is experienced. Later on, it was attempted to explain which rule algorithm could be created for each type of attack, which indicator could help it.

Chapter 4 is the implementation point of the rules that are scripted through the indicators. In this section, the rules of the attacks are enabled to generate alarms. General information about ELK's installation infrastructure, which is an open source log system, respectively, describes the determination of rule sets to be created for each type of attack, and the testing of attack scenarios and rule sets afterwards.

Chapter 5 contains a visual representation of the resulting alarms after being tested in the improved log system with the scenario enacted by the SIEM rules. it can be seen which alarm was generated in this section.

CHAPTER 2
ACTIVE APT ATTACKS

Active attack types have been evaluated under a number of headings while being examined. Firstly, a general attack definition has been tried to provide information. Later, the known characteristics of the attack were listed. Then, the target countries, systems and sectors are described. The most basic persistence points are explained. Finally, the methods used when doing data leakage of attacks are defined.

2.1. Duke Family

Definition: Duke Family consists MiniDuke, CozyDuke and CosmicDuke malwares. In early 2013, the MiniDuke malware was discovered in use in a series of attacks against NATO and European government agencies. (F-Secure, 2013). Researchers identify that “after the 2013 exposure, the actor behind Miniduke appears to have switched to using another custom backdoor, capable of stealing various types of information”. Researchers while investigating MiniDuke loaders in April 2014, “they were surprised to notice that the malicious executable being decompressed and loaded into memory was very similar to the Cosmu family of information-stealers, which they saw as long ago as 2001. Cosmu is the first malware family they have seen to share code with MiniDuke”.

Features: The attackers are using at least two different methods for infecting the systems; exploits and social engineering:

Document-Based Exploit: CosmicDuke malware samples that use exploits to gain entry onto a target system (referred to as exploit files in the rest of this document) start with a malicious Flash object embedded into a PDF file. When the file is launched, the object exploits the known CVE-2011-0611 vulnerability in specific versions of Adobe Flash, Reader and Acrobat products. Unlike the CosmicDuke files geared towards social engineering, the exploit files do not actually display any documents to the user as a form of distraction; the malware simply straightaway exploits the vulnerability.

Social Engineering: Less technically challenging CosmicDuke samples use simple social engineering to trick the user into willingly launching the attack file. Once launched, the file drops the malware onto the system (such files are therefore referred to as droppers in the rest of this documents). To do so, the malware's executable file is first disguised as an image or document to make it seem innocuous. When launched, a document or image is displayed in order to draw the user's attention away from any background activity. In the meantime, the malware's malicious files are silently installed and executed on the system. (F-Secure, 2013)

Target: Paganini identifies that "top target countries are Belgium, Brazil, Bulgaria, Czech Republic, Georgia, Germany, Hungary, Ireland, Israel, Japan, Latvia, Lebanon, Lithuania, Montenegro, Portugal, Romania, Russian Federation, Slovenia, Spain, Turkey, Ukraine, United Kingdom and United States" (Paganini, 2013). According to Kaspersky Lab "target sectors are diplomatic embassies, energy companies, telecoms, military, and individuals". (KasperskyLab, 2016)

Persistence: According to Kaspersky Lab researchers Duke family "is capable of starting via Windows Task Scheduler, via a customized service binary that spawns a new process set in the special registry key, or is launched when the user is away and the screensaver is activated." (KasperskyLab, 2016)

Exfiltration: The malware implements several methods to exfiltrate information, including uploading data via FTP and three variants of HTTP-based communication mechanisms. These three methods are "direct TCP connection and HTTP session via Winsock library, HTTP session via Urlmon.dll, and HTTP session via invisible instance of Internet Explorer as OLE object." (KasperskyLab, 2016) Malware also can exfiltrate variety of information, including most used extensions such as .exe, .rar, pptx, docx, etc., and file names such as login, admin, etc.

Researchers investigated that "the backdoor has many other capabilities including keylogger, Skype password stealer, general network information harvester, screen grabber (grabs images every 5 minutes), clipboard grabber (grabs clipboard contents every 30 seconds), Microsoft Outlook, Windows Address Book stealer, Google Chrome password stealer, Google Talk password stealer, Opera password stealer, TheBat! password stealer, Firefox, Thunderbird password stealer, Drives/location/locale/installed software harvester, WiFi network/adapter information harvester, LSA secrets harvester, Protected Storage secrets harvester, Certificate/private keys exporter, URL History harvester, InteliForms secrets harvester, IE Autocomplete, Outlook Express secrets harvester, and more.” (KasperskyLab, 2016)

2.2. Dark Hotel

Definition: The Darkhotel APT, discovered in 2014 and first known sample seemed in 2007, researchers defines “is a threat actor possessing a seemingly inconsistent and contradictory set of characteristics, some advanced and some fairly rudimentary. Inhospitably operating for almost a decade, the threat actor is currently active. The actor’s offensive activity can be tied to specific hotel and business center Wi-Fi and physical connections, some of it is also tied to p2p/file sharing networks, and they have been known to spear-phish targets as well”. (Kaspersky, 2014) It tools are detected as “Tapaoux”, “Pioneer”, “Karba”, and “Nemim”, among other names.

Features: The top features of this attack are:

- The first aim is to target C-suite victims: CEOs, Vice Presidents, Directors and top R&D staff,
- Attackers use both targeted attacks and botnet style operations,
- The gang uses zero day attacks such as IE and Adobe,
- They use advanced keylogger to steal confidential data,
- Stolen digital certificates used for malicious code signing,
- Darkhotel has been operating for almost a decade. (Kaspersky, 2015)

Target: Target countries are Japan, Taiwan, China, Russia, Korea, Hong Kong, India, Indonesia, Germany, United States, and Ireland.

Persistence: In the dark hotel, toolset consists multiple components. One of them is msieckc.exe executable file. It is a small downloader, and according to Kasperky Lab “this module is designed to update malicious components through recurring checks at the C&C server. It is also capable of removing some older components, the names of which are hardcoded in the body of the malware. The module adds autorun registry settings to enable an automatic start during system boot. One of the most interesting functions of this executable is its unusual delay and persistence. If a special file exists on the system, the module will not start calling back to C&C server until the special file is 180 days old. So, if some other critical malicious component was removed during this period, current module backs up and restores access to the system within 6 months." (Kaspersky, 2014)

Exfiltration: Scott and Spaniel defines exfiltration process as "evidence suggests that the adversary possesses knowledge of the personal information of targets, at which hotel individual targets will stay, and the duration of their stay. Upon connection to the hotel Wi-Fi, target users encounter a malicious iframe that redirects their browsers to fake update installers. Victims see a pop-up for a software update (Adobe Flash, Google Toolbar, Windows Messenger, etc.) that is actually a malicious executable piggybacking off a legitimate update installer. The installer delivers one of the group's backdoors to the victim system. And then exfiltration process begins easily. When the target concludes their stay, the adversary removes all or most traces of the attack from the hotel network. Neither backdoors nor tools are left behind." (Scott & Spaniel, 2016) In addition to the hotel attacks, the group may infect targets through spear-phishing attacks and P2P networks.

2.3. Uroburous

Definition: Uroburous can be named as Turla, Epic Turla and Snake. G Data researchers describes Uroburos as "is a rootkit, composed of two files, a driver and an encrypted virtual file system. The rootkit is able to take control of an infected machine, execute arbitrary commands and hide system activities. It can steal information and it is also able to capture network traffic." (GData, 2014) Most known feature is about its structure which lets "extending it with new features easily".

Features: According to researchers "The Uroburos group uses spear phishing campaigns, drive-by-infections, watering hole attacks, and social engineering to push their malware onto target networks. In spear phishing campaigns, the target receives a tailored email containing an executable RAR selfextracting archive. (Scott & Spaniel, 2016) It uses several driver names which some of them are Ultra3.sys, msw32.sys, vstor32.sys. The driver is important because;

- Need to decrypt virtual file systems,
- Creates many hooks to hide needed activities,

- Injects libraries in the users machines,

- Establishs communication channels.

Target: The top target countries are “France, Russia, Belarus, Romania, USA, Netherlands, Kazakhstan, Saudi Arabia, Iran, and Poland”. (Kaspersky, 2018)

Persistence: The persistence of this malware is creation a registry service that starts itself during system startup and located in

- HKLM\System\CurrentControlSet\Services\Ultra3

Dereszowski and Tecamac identify that “the rootkit uses two virtual file systems. One is persistent over reboot and NTFS formatted. The other one volatile and FAT formated; its content is never flushed to a real file system, as a result its content is only accessible on a live infected machine. Both are encrypted with a CAST like algorithm. The filesystem clusters are decrypted on access via cache management. As a result the file systems do no appear in clear text even in the physical memory.” Figure 2.1 shows virtual file system architecture of Uroborus malware. (Dereszowski & Tecamac, 2014)

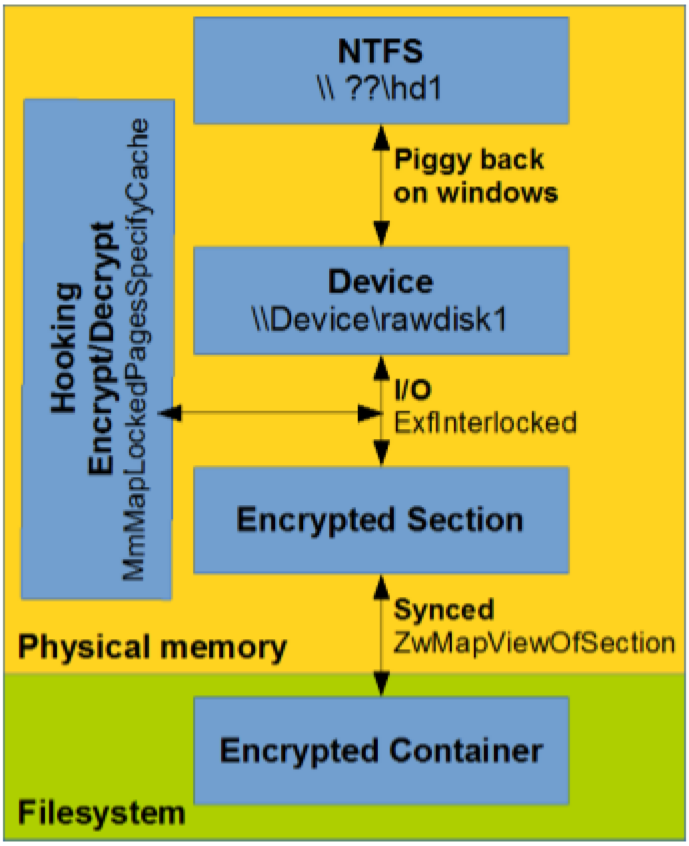


Figure 2.1 Snake Virtual File System architecture

Exfiltration: “It can spy on each and every infected machine and manages to send the exfiltrated information back to the attackers, by relaying this exfiltrated data through infected machines to one machine with Internet connection.” (GData, 2014)

2.4. Dragonfly

Definition: Dragonfly can named also Energetic Bear, Crouching Yeti and Havex. Symantec defines that “Dragonfly group, which is also known by other vendors as Energetic Bear or Crouching Yeti” (Karspersky, 2016), and Symantec gives detail that “a capable group who are evolving over time and targeting primarily the energy sector and related industries” (Symantec Response, 2014) This group has been associated with a particular piece of malware that has been named Havex. Historically, Energetic Bear has used Havex and other malware to attack targets in the energy sector. (IBM MSS, 2014)

Features: The attackers have used spear phishing and compromised websites (Watering Hole attacks) to infect victims. According to IBM researchers “Dragonfly has used spam email campaigns and watering hole attacks to infect targeted organizations. The group has used two main malware tools: Trojan.Karagany and Backdoor.Oldrea. The latter appears to be a custom piece of malware, either written by or for the attackers.” (IBM MSS, 2014) Kaspersky identifies malware that “they interest in OPC/SCADA systems, trojanized software used to administer remote OPC servers as well as modules to scan networks for OPC servers” (Kaspersky, Targeted Cyberattack Logbook, 2015).

Target: The target industries of attackers are energy and industrial control systems particularly those based in Europe. (Symantec Response, 2014) Top target countries are European countries such as Germany, Spain, and USA.

Persistence: Symantec team defines persistence process as file and registry modifications (Symantec Response, 2014). File system modifications carry out at Temp and System folders for qln.dbx and TMPprovider038.dll files. Registry modifications are

- “HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run \TmProvider”

- “HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion \Run\TmProvider”

- “HKEY_LOCAL_MACHINE\ SOFTWARE\Microsoft\Internet Explorer \InternetRegistry\fertger”

- “HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer \InternetRegistry”

Exfiltration: Symantec researchers defines that group uses another malware tool that is Karagany. Karagany’s primary aim is to download and installation files and exfiltrate confidential data. Karagany’s basic features are (Symantec Response, 2014)

- “Can upload, download, and execute files on the system”

- “Has plugin capability (may load several plugins for added functionality, such as Web injects)”

- “Payload is approximately 72Kb in size and is programmed in C/C++”

- “Contains a small embedded DLL file, which monitors WSASend and send APIs for capturing ‘Basic Authentication’ credentials”

2.5. Adwind

Definition: Adwind can be defined as AlienSpy, Frutos and Unrecom. Kaspersky Lab defines Adwind as “is a backdoor available for purchase and written purely in Java which makes it cross-platform”. (Kamluk & Gostev, 2016) According to Dinkar Adwind is “typically propagated through spam campaigns that employ malware-laden email attachments, compromised web pages, and drive-by downloads. Because spam campaigns are now short lived, with frequently changing subjects and carefully crafted attachments, it has become more difficult for users and security technologies to spot attacks.” (Dinkar, 2016)

Features: Adwind RAT has many capabilities (Kamluk & Gostev, 2016) these are “listing amd managing of any operational security software, processes, network connections, local services, file transfer, startup entries and locally installed softwares, password stealing, recording microphone, keylogger, stealing keys for cryptocurrency wallets, remote desktop control and etc."

Target: Most targeted sectors are "Manufacturing, Finance, Engineering, Design, Retail, Government, Shipping, Telecom, Software, Education, Food production, Healthcare, Media, Energy". Most targeted countries are USA, Italy, Germany, Turkey, UAE, India, Russia, Hong Kong, Taiwan. (Kamluk & Gostev, 2016)

Persistence: The malware uses random folder and file names. "Depending on the variant of Adwind, the Java archive copied in the %AppData% folder may use a different file extension than .jar: %AppData%\[random folder name]\[random filename].[random file extension]. And then The Trojan changes the folder and file attributes to system, hidden, and read only." (Dinkar, 2016)

Exfiltration: According to Dinkar "after Adwind successfully infects a system, it log keystrokes, modify and delete files, download and execute further malware, take screenshots, access the system's camera, take control of the mouse and keyboard, update itself, and more." (Dinkar, 2016)

2.6. Blue Termite

Definition: Blue Termite can be defined as Emdivi and CloudyOmega. Kaspersky Lab team defines that Blue Termite is a cyberespionage campaign that has been targeting hundreds of organizations in Japan for at least two years. (Kaspersky, 2015) Sy from Trend Micro group gives detail about Blue Termite "has been leveraging customized malware of the Emdivi family to steal valuable data from victims. Trend Micro has also analyzed attacks involving Emdivi malware and the Hacking Team Flash Player exploit aimed at organizations in Japan" (Sy, 2015). Symantec has also been monitoring this threat group's activities. In November 2014, the security firm published a report detailing a campaign dubbed "CloudyOmega" (Symantec, 2014).

Features: Blue Termite attackers uses spear-phishing emails. According to Kaspersky Lab researchers "operators changed their tactics and started to spread the malware via a zero-day Flash exploit (CVE-2015-5119). Using a drive-by-download technique, the attackers compromised several Japanese websites so that visitors of these sites would automatically download an exploit once they were on the website and become infected" (Kaspersky, 2015).

Target: The target country is Japan. Kovacs gives detail about target sectors as "hundreds of organizations have been targeted in this operation over the past two years, including government agencies, universities, public interest groups, financial services firms, banks, news companies, and various organizations from sectors such as automotive, chemical, healthcare, electrical, real estate, food, construction, insurance, transportation, robotics, semiconductors, and information services." (Kovacs, 2015)

Persistence: "One of the most interesting things about the malware is that each victim is supplied with a unique malware sample that is made in a way that it could only be launched on a specific PC, targeted by the Blue Termite actor. According to Kaspersky Lab researchers, this has been done in order to make it difficult for security researchers to analyze the malware and detect it." (Kaspersky, 2015)

Exfiltration: Scott and Spaniel defines more features about Blue Termite attack. "The group uses Backdoor.Emdivi, Backdoor.Korplug, and Backdoor.ZXshell to compromise a system and establish a persistence presence. The backdoor enables a remote adversary to execute commands from a C&C server via HTTP. The malware contains components to search files, delete files, upload files to C2 servers, execute code, acquire a list of running processes, steal auto-complete information and saved credential information from Internet Explorer, and steal the proxy settings of browsers such as Mozilla Firefox." (Scott & Spaniel, 2016)

2.7. APT28

Definition: APT28, also known as Sofacy, Sednit, Fancy Bear, Strontium and Pawn Storm, "is an advanced threat group that has been active since around 2008, targeting mostly military and government entities worldwide, with a focus on NATO countries." (Securelist, 2018)

Features: Hacquebord from Trend Micro team defines that "the group used three very distinct attack scenarios. One was to send spear-phishing emails with malicious Microsoft Office documents containing the information-stealing SEDNIT/Sofacy malware. Another was to inject selective exploits into legitimate Polish government websites, leading to the same malware. A final strategy was to send out phishing emails redirecting users to fake Microsoft Outlook Web Access (OWA) login pages." (Hacquebord, 2015)

Target: Target countries are USA and NATO members.

Persistence/Exfiltration: Attackers use a backdoor that’s names is CHOPSTICK. Its variants may move messages and information using at least three methods (FireEye, 2014):

1. “Communications with a C2 server using HTTP”.

2. “Email sent through a specified mail server. One CHOPSTICK v1 variant contained modules and functions for collecting keystroke logs, Microsoft Office documents, and PGP files. The monitoring for new files of interest is performed by a “Directory Observer” module”.

3. “Local copying to defeat closed networks. One variant of CHOPSTICK focuses on apparent air gap / closed network capabilities by routing messages between local directories, the registry and USB drives”.

2.8. Equation

Definition: The Equation is a highly sophisticated threat actor that “uses multiple malware platforms, some of which surpass the well-known Regin threat in complexity and sophistication. The Equation group is probably one of the most sophisticated cyber attack groups in the world; and they are the most advanced threat actor, and it should be called mother of all APTs”. (Kaspersky, 2015)

Features: Researchers discovered that “Equation Group relies on multiple attack techniques to compromise victims’ computers, including self-replicating code, USB sticks exploits, and web-based exploits”. (Infosec, 2018)

“The hackers behind the Equation Group used several attack tools and malware, some of which are exclusive to the group.” (Kaspersky Lab, 2015) List of attack tools are equationdrug, doublefantasy, equestre, triplefantasy, triplefantasy, grayfish, fanny, and equationlaser.

Target: Researchers from Kaspersky have documented nearly 500 infections. (Infosec, 2018) Target countries are India, Russia, Iran, Afghanistan, Pakistan and Syria.

Persistence: According to Kaspersky Lab researchers “the most powerful tool in the Equation group’s arsenal is a mysterious module known only by a cryptic name:

nls_933w.dll. It allows them to reprogram the hard drive firmware of over a dozen different hard drive brands, including Seagate, Western Digital, Toshiba, Maxtor and IBM. This is an astonishing technical accomplishment and is testament to the group's abilities. (Kaspersky Lab, 2015)

Checkpoint defines their surprises that "a unique feature of some tools from the Equation APT group astounded researchers and engineers around the world with an unprecedented technological feat: both EquationDrug and CrayFish had a plugin in place that enables the functionality of reprogramming hard drive firmware. This never-before-seen technique abuses the firmware upgrade feature of hard drives and solid state disks by various vendors and models, to write specific code into these secret compartments, invisible to operating systems and typically left unnoticed even in rigorous forensics examinations." (Check Point , 2015)

Exfiltration: Fanny is a critical malware of Equation Group in order to exfiltrate sensitive data and "was able to penetrate isolated systems which are not connected to the internet such as nuclear power plants and electricity companies, by storing itself on a USB stick, infecting the isolated system, and then sending all information when it is plugged into a computer connected to the internet. "Grok" is another malware used by the group, which is a key-logger that steals user names and password to various websites which are accessed through the infected computer." (Check Point , 2015)

2.9. NetTraveler

Definition: NetTraveler also known as Travnet or Netfile is the main tool used by the threat actors during attacks. Researchers from Kaspersky Lab identifies that "the name NetTraveler comes from an internal string which is present in early versions of the malware: "NetTraveler Is Running!" This malware is used by APT actors for basic surveillance of their victims". (Kaspersky Lab, 2013)

Features: Trojan Travnet, which exfiltrates data, takes advantage of unpatched software. It exploits old vulnerabilities, such as - CVE-2012-0158 and CVE-2010-3333, in Microsoft Office, Excel and RTF documents. (Taneja, 2013) Kaspersky researchers defines that "the attacks use spear-phishing e-mails with malicious Microsoft Office documents as attachments. Gathered data includes file system listings, keylogs, various types of documents (.doc, .xls, .ppt, .pdf, etc...) and other private information”. (Kaspersky Lab, 2013)

Target: According to Securelist “target of NetTraveler includes Tibetan/Uyghur activists, oil industry companies, scientific research centers and institutes, universities, private companies, governments and governmental institutions, embassies and military contractors”. (Securelist, 2018)

Persistence: Kaspersky Lab researchers identifies that “NetTraveler is an automatic data exfiltration tool, designed to extract large amounts of private information from the victim’s system over long periods of time. The malware uses compression techniques and a fail-safe protocol to ensure that uploaded data is safely transferred to the attacker’s C2s”. (Kaspersky Lab, 2013)

Exfiltration: Taneja from Mcafee team defines that “once Travnet infects a machine, it searches for all document files, such as PDF, PPT, and DOC, and uploads this data to remote servers. To evade detection from network-monitoring appliances such as intrusion detection and prevention systems, the malware sends the stolen data in encrypted format. To reduce the data size, it first uses a compression algorithm and then a Base64 algorithm”. (Taneja, 2013)

2.10. Regin

Definition: Symantec describes Regin “is a multi-purpose data collection tool and has a wide range of standard capabilities, particularly around monitoring targets and stealing data. It also has the ability to load custom features tailored to individual targets. Some of Regin’s custom payloads point to a high level of specialist knowledge in particular sectors, such as telecoms infrastructure software, on the part of the developers”. (Symantec, 2015)

Features: Researchers identifies that “Regin is capable of installing a large number of additional payloads, some highly customized for the targeted computer. Regin is also configured to steal passwords, monitor network traffic, and gather information on processes and memory utilization. It can also scan for deleted files on an infected computer and retrieve them. More advanced payload modules designed with specific goals in mind were also found in our investigations”. (Symantec, 2015)

Target: Target countries are Pakistan, Iran, Ireland, Saudi Arabia, India, Russia, Belgium, Mexico, Ireland, India, Afghanistan, and Austria.

Persistence: Researchers from Kaspersky Lab defines that “the structures of the file system are unencrypted, the file entries are encrypted. The encryption algorithm used is RC5, and many records are also compressed using the nrv2e algorithm from the UCL library. The reason why the attackers chose UCL is simple: it’s small, compact and requires little to no additional memory for decompression”. (Kaspersky Lab, 2014)

2.11. Duqu

Definition: CrySys Lab has discovered Duqu in 2011 while investigation of an incident in a company. “They gave it the name Duqu because it has an infostealer component that creates files in the infected system with filenames starting with the string ~DQ”. (Bencs, Pek, Buttyan´, & Felegyhazi, 2012) “Duqu malware, sometimes referred to as the stepbrother of Stuxnet. Kaspersky Lab named this new malware and its associated platform “Duqu 2.0” ”. (Kaspersky Lab, 2015)

Features: Duqu uses three zero-day vulnerabilities, one of them is CVE-2014-6324 which patched by MS14-068. This exploit allows an unprivileged domain user to elevate credentials to a domain administrator account. Rest of them is kernel mode exploit (CVE-2015-2360, CVE-2014-4148) that allow attackers to run code with the highest privileges in the system. As used before in Duqu malware, same vulnerability is used in Duqu 2.0 which is CVE-2014-4148, Microsoft has released security update MS14-058 that addresses this vulnerability.

Target: According to Kaspersky Lab “victims of Duqu 2.0 have been found in several places, including western countries, the Middle East and Asia. The actor appears to compromise both final and utilitarian targets, which allow them to improve their cyber capabilities”. (Kaspersky Lab, 2015)

Persistence: Kaspersky Lab researchers defines that “Duqu 2.0 malware platform was designed in a way that survives almost exclusively in memory of the infected systems, without need for persistence. To achieve this, the attackers infect servers with high uptime and then re-infect any machines in the domain that get disinfected by reboots. Surviving exclusively in memory while running kernel level code through exploits is a testimony to the technical prowess of the group. In essence, the attackers were confident enough they can survive within an entire network of compromised computers without relying on any persistence mechanism at all". (Kaspersky Lab, 2015)

Exfiltration:

Researchers of Kaspersky Lab describes that "attackers deploy more sophisticated packages to domain controllers and to the victims of interest inside the LAN. These MSI packages can contain tens of different modules designed for various cyberespionage functions. One of modules is 09A0 – 64-bit, exfiltrates file contents, particularly searching for files matching rules". (Kaspersky Lab, 2015)

2.12. Wild Neutron

Definition: Wild Neutron can be defined as Butterfly or Morpho. "The hacker group known as Wild Neutron is still actively attacking companies around the world, a number of years after the group was first discovered in 2011". Both Kaspersky Lab (Kaspersky, 2015) and Symantec (Symantec, 2015) have reported renewed activity, Symantec now refers to the group as "Butterfly". Hacker group also known as jirimbot and morpho.

Symantec researchers defines that "Wild Neutron/Butterfly is technically proficient and well resourced. The group has developed a suite of custom malware tools capable of attacking both Windows and Apple computers, and appears to have used at least one zero-day vulnerability in its attacks. It keeps a low profile and maintains good operational security. After successfully compromising a target organization, it cleans up after itself before moving on to its next target". (Symantec, 2015)

Features: Wild Neutron threat actor has several component groups (Kaspersky, 2015), including:

- "A main backdoor module that initiates the first communication with C&C server",
- "Several informaton gathering modules",
- "Exploitation tools",
- "SSH-based exfiltration tools",

- “Intermediate loaders and droppers that decrypt and run the payloads”.

Hacker group operates consistently across its breaches, deploying the same set of tools and targeting the same types of computers. Butterfly adapts quickly to targeted environments and takes advantage of systems already in place, such as remote access tools or management systems, in order to spread across the network. .While Butterfly has used one confirmed zero-day exploit (CVE-2013-0422), the group appears to have used at least one more zero-day exploit against a vulnerability in Internet Explorer 10.

Target: Top target countires are France, Russia, Switzerland, Germany, Austria, Slovenia, Kazakhstan, United Arab Emirates, Algeria and USA. Target indusries are pharmaceutical, technology, law, commodities, goverment, logistic and education sectors.

Persistence: The following registry subkeys may be used by Butterfly to maintain persistence: (Symantec, 2015)

- “HKEY_CURRENT_USER\Software\Adobe\Preferences”
- “HKEY_CURRENT_USER\Software\Adobe\Options”
- “HKEY_CURRENT_USER\Software\Adobe\UID”
- “HKEY_CURRENT_USER\Software\Acer\UPDATE_ID”
- “HKEY_CURRENT_USER\Software\Acer\Preferences”
- “HKEY_CURRENT_USER\Software\Acer\Options”
- “HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\Acer LiveUpdater (likely named Liveupdater.exe)”
- “HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\Adobe Flash Plugin Updater (FlashUtil.exe)”

Exfiltration: Kaspersky Lab observed “the attackers deploying custom, OpenSSH-based Win32 tunnel backdoors that are used to exfiltrate large amounts of data in a reliable manner. These tunnel backdoors are written as “updt.dat” and executed with two parameters, -z and -p.” (Kaspersky, 2015)

2.13. Winnti

Definition: Kaspersky defines that "main objective of the group is to steal source code of online game projects as well as digital certificates of legitimate software vendors. Besides that, they are deeply interested in the set-up of network infrastructure) and new developments such as conceptual ideas, design and more". (Kaspersky Lab, 2013)

Features: The hacking group has some features: (Kaspersky Lab, 2013)

- "Massive abuse of digital signatures; the attackers used digital signatures of one victim company to attack other companies and steal more digital certificates",
- "Usage of kernel level 64-bit signed rootkit",
- "Abusing great variety of public internet resources to store control commands for the malware in an encrypted form",
- "Sharing/selling stolen certificates to other groups that had different objectives (attacks against Uyghur and Tibetan activists)",
- "Stealing source codes and other intellectual property of software developers in online gaming industry".

Target: Researchers describes that group targets South East Asia. "However, online gaming companies located in Germany, the USA, Japan, China, Russia, Brazil, Peru, and Belarus were also identified as victims of the Winnti group". (Kaspersky, Kaspersky Lab Analyzes Active Cyberespionage Campaign Targeting Online Gaming Companies Worldwide, 2018) Specifically, group focused on Tibetan and Uyghur activists.

Persistence: The group uses DLL library. The PlusDLL library has an embedded driver. The driver is stored in %WINDIR%System32 file, registered as a service and started by NtLoadDriver system API function. Immediately after that, the driver's file is removed, as well as all the registry entries created during service registration. The executable preserved the original driver names which are "PortLess" and "PointFilter"; however, the driver files used during infection are saved with as "sp1itter.sys" and "acplec.sys".

The purpose of the driver is to hide network connections established by the malware. For example, if the user decides to check a list of established connections (e.g., using the ‘netstat -a’ command or the tcpview program) while the bot is communicating to the control center, the driver will protect and hide the malware connections. This approach is used by many rootkits on Windows platform.

The driver uses an unusual method to determine which addresses should be concealed and which shouldn’t. This information is available in the PlusDLL control library, which normally operates in the context of the explorer.exe process when the infection is active on the computer. This information is sent from the user mode, in which PlusDLL works, to the kernel level, at which the driver works, via the NtSetQuotaInformationFile function, which is available in both modes.

Exfiltration: Kaspersky Lab has “singled out three main monetization schemes that could be used by the Winnti team”: (Kaspersky Lab, 2013)

- “The unfair accumulation of in-game currency/”gold” in online games and the conversion of virtual funds into real Money”,
- “Theft of source code from the online games server to search for vulnerabilities in games”,
- “Theft of source code from the server part of popular online games to further deploy pirate servers”.

2.14. Poseidon

Definition: Security researchers defines as “the Poseidon Group is a long-running team operating on all domains: land, air, and sea. They are dedicated to running targeted attacks campaigns to aggressively collect information from company networks through the use of spear-phishing packaged with embedded, executable elements inside office documents and extensive lateral movement tools”. (Kaspersky Lab, 2016)

Features: In detail, Kaspersky Lab defines main features as “the main infection vector for Poseidon is the use of spear-phishing emails including RTF/DOC files, usually with a human resources lure. Once the infection happens, it reports to the command and control servers before beginning a complex lateral movement phase. This way the attackers actually know what applications and commands they can use without raising an alert to the network administrator during lateral movement and exfiltration”. (Kaspersky Lab, 2016)

Target: Target countries are Brazil, the United States, France, Kazakhstan, United Arab Emirates, India and Russia. And target sectors are energy, telecommunications, financial and governmental institutions.

Persistence: After gathering data by attackers Kaspersky Lab researchers gives detailed information. “The information exfiltrated is then leveraged by a company front to blackmail victim companies into contracting the Poseidon Group as a security firm. Even when contracted, the Poseidon Group may continue its infection or initiate another infection at a later time, persisting on the network to continue data collection beyond its contractual obligation”. (Kaspersky Lab, 2016)

Exfiltration: The Poseidon Group actively targets corporate environment for the theft of intellectual property and commercial information, occasionally focusing on personal information on executives. (Kaspersky Lab, 2016)

2.15. FinSpy

Definition: The FinSpy or FinFisher is described by its distributors, Gamma International UK Ltd, as “Governmental IT Intrusion and Remote Monitoring Solutions.” “The toolset first gained notoriety after it was revealed that the Egyptian Government’s state security apparatus had been involved in negotiations with Gamma International UK Ltd. over the purchase of the software. Promotional materials have been leaked that describe the tools as providing a wide range of intrusion and monitoring capabilities. Despite this, however, the toolset itself has not been publicly analyzed”. After many advanced analysis and investigations Morgan Marquis-Boire and Bill Marczak (Marquis-Boire & Marczak, 2013) declared that this toolset is a malware.

Features: Functionality of malware can be listed as:

- “Bypassing of 40 regularly tested Antivirus Systems”,
- “Covert Communication with Headquarters”,
- “Full Skype Monitoring (Calls, Chats, File Transfers, Video, Contact List)”,
- “Recording of common communication like Email, Chats and Voice-over-IP”,

- “Live Surveillance through Webcam and Microphone”,

- “Country Tracing of Target”,

- “Silent Extracting of Files from Hard-Disk”,

- “Process-based Key-logger for faster analysis”,

- “Live Remote Forensics on Target System”,

- “Advanced Filters to record only important information”,

- S”upports most common Operating Systems (Windows, Mac OSX and Linux)”.

Target: The most targeted countries are Germany, Vietnam, Russia, Mongolia, China, USA, Cambodia, Japan, Indonesia and Lao People's Democratic Republic, activists and criminal suspects are also targeted.

Persistence: Known strong abilities are:

1. A registry key is added which ensures the persistence of the backdoor after reboot:

“HKU\s-1-5-21-1177238915-1336601894-725345543-500\software\microsoft
\windows\currentversion\run\*U1o4r7MC:\WINDOWS\system32\rundll32.exe
C:\DOCUME~1\ADMINI~1\LOCALS~1\UbY5xEcD\V46lMhsH.shv,F7ed728
REG_EXPAND_SZ 0”

2. According to researchers, following path “appears to reference the functionality that the malware uses to modify the boot sequence to enable persistence”:

“y:\lsvn_branches\finspyv4.01\finspyv2\src\target\bootkit_x32driver\objfre_w2k_x86\ i386\bootkit_x32driver.pdb”

3. Some files are written to disk, the file “ZsROY7X.-MP” appears to provide the main backdoor functionality. It is executed via rundll32 and the following registry entry created to ensure persistence:

“HKU\s-1-5-21-1177238915-1336601894-725345543-500\software\microsoft\
windows\currentversion\run\*J7PugHy C:\WINDOWS\system32\rundll32.exe
C:\DOCUME~1\ ADMINI~1\LOCALS~1\jlc3V7we\IZsROY7X.-MP,F1dd208”

Exfiltration: Maslennikov defines main exfiltration features of Finspy as: (Maslennikov, 2013)

- “Logging incoming and outgoing calls”,

- “Concealed calls to eavesdrop on the target’s surroundings”,

- “Stealing information from smartphones (call logs, text and media messages, contacts, etc.)”,

- “Coordinate tracking”,

- “Internet and text message communication with the command center”.

2.16. Black Energy

Definition: According to F-Secure Lab security researchers “BlackEnergy is a popular crimeware that is sold in the Russian cyber underground and dates back to as early as 2007. Originally, it was designed as a toolkit for creating botnets for use in conducting Distributed Denial of Service (DDoS) attacks. Over time, the malware has evolved to support different plugins, which are used to extend its capabilities to provide necessary functions, depending on the purpose of an attack”. (F-Secure, 2013)

Features: We can group blackenergy variants as:

Blackenergy 1: This toolkit first emerged in 2007, Nazario describes toolkit as “it is an HTTP-based botnet used primarily for DDoS attacks. Unlike most common bots, this bot does not communicate with the botnet master using IRC. BlackEnergy 1 gives the attackers an easy to control web-based bot that can launch various attacks and control the bots using a minimal syntax and structure”. (Nazario, 2007)

Blackenergy 2: Unlike the BlackEnergy 1, Stewart defines differences as“BlackEnergy 2 uses modern rootkit/process-injection techniques, strong encryption and a modular architecture. The original BlackEnergy kit did have a rudimentary trojan component used to hide the trojan executable and process, but BlackEnergy 2 is much more sophisticated. The basis for the new rootkit seems to be found in an older rootkit project released by the author called BlackReleaver”. (Stewart, 2010)

Blackenergy 3: Security researchers of F-Secure identify that “In contrast to previous variants, BlackEnergy 3 uses a simpler installer component. It does not have a driver component and the installer drops the main DLL component directly to the local application data (nonroaming) folder. The installer then creates a LNK file in the startup folder, using a filename generated based on the volume serial number as a launch point. The LNK file is a shortcut to execute the main DLL using rundll32.exe”. (F-Secure, 2013)

Target: Attackers aims to reach wide range of targets. Most targeted countries are Ukraine, Lithuania, Poland, Azerbaijan, Belarus, Russia, Kyrgyzstan, Iran, Kazakhstan and Israel.

Persistence: Nazario gives detail about the main features that “the BlackEnergy 1 bot author likes to promote in forums is that the bot can target more than one IP address per hostname. The authors promote that this feature is designed for targets that use DNS load balancing and ensures that their bots target all hosts for the attack. Also, the bot author has used a runtime encrypter to thwart antivirus detection”. (Nazario, 2007)

BlackEnergy 2 uses start menu locations for persistence: (Baumgartner & Golovkin, The Naikon APT, 2015)

“Users\user\AppData\Roaming\Microsoft\Windows\StartMenu\Programs\Startup\flashplayerapp.exe”

Exfiltration: According to F-secure Labs, “one particular plugin that was used in the campaign was called ‘si’, perhaps to mean ‘steal information’. The latest sample attempts to gather the following information and send them to the C&C server”: (F-Secure, 2013) System configuration information, Operating system version, Privileges, Current time, Up time, Idle Time, Proxy, Installed apps, Process list, IP configurations, Network connections, Routing tables, Traceroute and Ping information to Google, Registered mail, browser, and instant messaging clients, Account and password information, Stored username and passwords in applications”.

2.17. Hacking Team RCS

Definition: Hacking Team is an Italian company that focuses on offensive security, it proposes to government authorities an offensive solution for cyber investigations. Their commercial product’s name is Remote Control System (RCS) software.

Features/Exfiltration: Currier and Marquis-Boire define that “RCS has ability to ctivate cameras, exfiltrate emails, record Skype calls, log typing, and collect passwords on targeted devices. It also catalogs a range of pre-bottled techniques for infecting those devices using wifi networks, USB sticks, streaming video, and email attachments to deliver viral installers. With a few clicks of a mouse, even a lightly trained technician can build a software agent that can infect and monitor a device, then upload captured data at unobtrusive times using a stealthy network of proxy servers, all without leaving a trace”. (Currier & Marquis-Boire, 2014)

According to Kaspersky Lab (Golovanov, 2013), software has more capabilities such as:

- “Self-replication via USB flash drive”,
- “Using a standard Autorun.inf mechanism”,
- “Using a fake “Open folder to view files” entry (a method commonly used for self-replicating worms, especially with the Kido/Confiker worms)”,
- “Exploiting the CVE-2010-2568 vulnerability (used by Stuxnet for self-replication via LNK files)””.
- “Infection of virtual VMware machines by copying itself into the autorun folder on the virtual drive”,
- “Infection of mobile BlackBerry and Windows CE devices”,
- “Ability to self-update”,
- “Use of an AES encryption algorithm to work with files and control servers”,
- “Installation of drivers”.

Target: RCS is used by goverment authorities over 35 countries. Activists, journalists, politicians and criminal suspects are targeted.

Persistence: There are two registry key (Boire, 2012) are added during installation:

“HKU\s-1-5-21-1177238915-1336601894-725345543-
500\software\microsoft\windows\currentversion\run\*U1o4r7M
C:\WINDOWS\system32\rundll32.exe
C:\DOCUME~1\ADMINI~1\LOCALS~1\UbY5xEcD\V46lMhsH.shv",F7ed728
REG_EXPAND_SZ 0”

“HKU\s-1-5-21-1177238915-1336601894-725345543-
500\software\microsoft\windows\currentversion\run\*J7PugHy

C:\WINDOWS\system32\rundll32.exe
C:\DOCUME~1\ADMINI~1\LOCALS~1\jlc3V7we\IZsROY7X.-MP",F1dd208”

2.18. Naikon

Definition: Naikon APT is one of the most active APTs in Asia, especially around the South China Sea. Kaspersky Labs, which has authored the most comprehensive introduction to the Naikon APT, describes a group conducting high-volume, high-profile, geopolitically motivated attacks over at least five years. (Baumgartner & Golovkin, The MsnMM Campaings: The Earliest Naikon APT Campaigns, 2015)

Features: Kaspersky researchers (Baumgartner & Golovkin, The Naikon APT, 2015) give a detailed feature of Naikon APT:

> - “Each target country has a designated human operator, whose job it is to take advantage of cultural aspects of the country, such as a tendency to use personal email accounts for work”,
>
> - “The placing of infrastructure (a proxy server) within the country’s borders to provide daily support for real-time connections and data exfiltration”,
>
> -“At least five years of high volume, high profile, geo-political attack activity”,
>
> - “Platform-independent code, and the ability to intercept the entire network traffic”,
>
> - “48 commands in the repertoire of the remote administration utility, including commands for taking a complete inventory, downloading and uploading data, installing add-on modules, or working with the command line”.

Key technical characteristics of Naikon APT is:

- use CVE-2012-0158 vulnerability,
- start with spear phishing document with oil & gas themed decoy document,
- Right-to-Left character override,
- Self-extracting executables. (Threat Connect and Defense Group, 2015)

Target: Kaspersky assesses Naikon has a high success rate infiltrating national organizations in countries affiliated with the Association of Southeast Asian Nations (ASEAN) with early victims located mostly throughout Myanmar, Vietnam, Singapore, Laos, Malaysia, and the Philippines. (Baumgartner & Golovkin, The MsnMM Campaings: The Earliest Naikon APT Campaigns, 2015) Target profiles included high-profile government and military agencies around the South China Sea as well as state media and energy organizations both public and private. (Threat Connect and Defense Group, 2015) Target organizations are goverment entities and offices, military forces, intelligence services, law enforcement, economic administration, state media and publice and private energy companies.

Persistence: Researchers describes that "some APTs like Naikon distribute tools such as these across multiple systems in order to regain control if it is lost accidentally and to maintain persistence". (Baumgartner & Golovkin, The Naikon APT, 2015)

Exfiltration: The structure of Naikon operations suggests campaigns focused on individual countries, with specific toolsets deployed against a range of organizations within the designated country. To get into target networks, the Naikon APT relies on email as an attack vector and precise social engineering to identify appropriate targets. Data collection prior to an attack has included full names, email addresses, date of birth, interests in current events, nationality, gender, and previous email and social network communications to and from a target. (Threat Connect and Defense Group, 2015)

2.19. Cloud Atlas

Definition: Cloud Atlas can be defined as also Red October. Kaspersky Lab announced a complex cyber-espionage operation targeting diplomatic embassies worldwide, and this attack was named as Red October because researchers started this investigation in October 2012. (Kaspersky Lab, 2014) And after one year simultaneously BlueCoat and Kaspersky Lab researchers published their reports for Cloud Atlas APT attack which is highly automated, and extremely sophisticated framework for performing targeted attacks. "The framework is notable for a number of reasons, including its use of a cloud-based infrastructure for command-and-control and its use of the WebDAV protocol to send instructions and receive exfiltrated information from compromised systems". (Blue Coat, 2015)

Features: Attack starts with a spear-phishing method bu using documents. According to Blue Coat "the use of exploits in document formats like PDF, DOC and

RTF is in some ways especially noteworthy. Documents are commonly exchanged via mail, which make them perfect for email-borne targeted attacks".

Vulnerability list that attackers use to trigger execution of the malicious payload;

- "CVE-2014-1761",
- "CVE-2010-3333",
- "CVE-2012-0158",
- "CVE-2014-1761",
- "CVE-2012-0158".

Kaspersky Lab researchers describes that "the Cloud Atlas implants utilize a rather unusual C&C mechanism. All the malware samples communicate via HTTPS and WebDav with the same server "cloudme.com", a cloud services provider. According to their website, CloudMe is owned and operated by CloudMe AB, a company based in Linköping, Sweden". (Kaspersky Lab, 2014)

Target: Top target countries are Russia, Kazakhstan, Belarus, India and Czech Republic. Targeted units are diplomatic organizations/embassies and government entities.

Persistence: Attackers use many modules to perform advanced threat successfully. One of them is scheduler module: (Kaspersky Lab, 2013)

"Known locations: %APPDATA%MicrosoftRtkN32Gdi.exe"

Registry values to ensure its automatic start:

"HKLMSOFTWAREMicrosoftWindowsCurrentVersionPoliciesExplorerRunservise= %path to the module's executable file%"

"HKCUSoftwareMicrosoftWindows NTCurrentVersionWindowsload=%path to the module's executable file%"

Exfiltration: In this part attackers use three modules:

WNFTPSCAN module: According to researchers the main purpose of this module is "to make directory listings, copy files of interest (JPG, DOC, PPT, XLS, EMF, PDF) which are smaller than 1 MB and not older than specified date. The module is also capable of checking if remote FTP directories are available for write-access, but this functionality is currently not used”. (Kaspersky Lab, 2013)

GetFileReg module: Researchers defines other module as “the file is a PE DLL file, 0 exports, compiled with Microsoft Visual Studio 2008. All functionality is implemented in the DllMain function. When loaded, the module deletes the file named “dump”, then proceeds to its main function. After executing the main function, the module tries to delete the same file again”.

FileInfo module: The module is very similar to the “GetFileReg” module. It is stored on disk as an encrypted file that is loaded by the “Scheduler” module. It creates encrypted log files: “%TMP%smrdprevsmrdprev_%p_%p.tmp”, where “%p” parameters are formatted from the return values of subsequent GetTickCount API calls. It creates encrypted storage files: “%TEMP%%08 hex digits%hst”, where 8 hex digits represent the CRC32 checksum of the current user’s name, and creates mutex: “Win32Wbem32Prefetchfamt”. (Kaspersky Lab, 2013)

2.20. Hellsing

Definition: According to Kaspersky Lab experts, “Hellsing is a small and technically unremarkable cyberespionage group targeting mostly government and diplomatic organisations in Asia, was subjected to a spear-phishing attack by another threat actor and decided to strike back”. (Kaspersky Lab, 2015)

Features: Makrushin defines that “at the stage of “infection” attackers use various techniques for delivering malicious code to the victim’s operating system, sending emails containing the exploit, delivery of malicious code through social engineering, etc. The ultimate goal of these attacks is to deliver the backdoor to the victim’s operating system and run it. “Payload” is an executable (.exe) file or library (.dll), containing malicious code. In Hellsing’s case, the attacker uses social engineering to dupe the user into launching an exe-file from RAR-archive. The exe-file extension was replaced with an innocuous one and the victim did not notice the suspicious file”. (Makrushin, 2015)

Target: The top countries are “CIS, Canada, Indonesia, Lao People&#039;s Democratic Republic, Malaysia, Myanmar, Nepal, Philippines, Singapore, Thailand, Vietnam”. (Securulist, 2018)

Persistence: Golovkin defines as “the targeting of the Naikon group by the Hellsing APT is perhaps the most interesting part. In the past, some APT groups accidentally hit each other while stealing address books from victims and then mass-mailing everyone on each of these lists. But, considering the timing and origin of the attack, the current case seems more likely to be an APT-on-APT attack”. (Golovkin, 2015)

Exfiltration: Deeper analysis of the Hellsing threat actor by Kaspersky Lab (Kaspersky Lab, 2015) “reveals a trail of spear-phishing emails with malicious attachments designed to propagate espionage malware among different organisations. If a victim opens the malicious attachment, their system becomes infected with a custom backdoor capable of downloading and uploading files, updating and uninstalling itself”.

2.21. Kimsuky

Definition: Paganini defines malware that “this cyber espionage campaign dubbed "Kimsuky" has targeted several South Korean think tanks. Researchers believe the Kimsuky malware is most likely delivered via spear-phishing e-mails and used multiple Dropbox email accounts. It has been following a sustained attack on South Korea by hackers seemingly based in North Korea”. (Paganini, 2013)

Features: Attack starts with an e-mail spear phishing method via the public e-mail server in Bulgarian. According to Paganini “victims download a Trojan dropper which is used to download additional malware. At system startup, the basic library disables the system firewall and any firewall produced by the South Korean security product vendor AhnLab. The malware does not include a custom back door, instead the attackers modified a TeamViewer client as a remote control module. Bot agents communicate with C&C through the Bulgarian web-based free email server.” (Paganini, Kaspersky revealed "Kimsuky" Cyber Espionage campaign targeting South Korea, 2013)

Target: Tarakanov identifies attack target as “this attack seemed to only target 11 South Korean and 2 Chinese groups, some of these groups include: the Sejong Institute, KIDA (Korea Institute for Defense Analysis), South Korea’s Ministry of Unification, Hyundai Merchant Marine, and supporters of the Korean Unification”. (Tarakanov, 2013)

Persistence: Persistence process is described by Tarakanov: “Once the malware disables the AhnLab firewall, it checks whether the file taskmgr.exe is located in the hardcoded c:\windows folder. If the file is present, it runs this executable. Next, the malware loops every 30 minutes to report itself and wait for response from its operator”. (Tarakanov, 2013)

Exfiltration: According to Taranakov “there are a lot of malicious programs involved in this campaign but, strangely, they implement a single spying function. Besides the basic library (kbdlv2.dll / auto.dll) that is responsible for common communication with its campaign master, some modules performing the following functions” (Tarakanov, 2013): “Keystroke logging, directory listing collection, document theft, remote control download and execution, remote control access”.

2.22. Carbanak

Definition: Kaspersky researchers defines as “Carbanak is a remote backdoor (initially based on Carberp), designed for espionage, data exfiltration and to provide remote access to infected machines. The main difference with other APT attacks is that attackers do not see data but money as their primary target”. Researchers say “APT-like, however the attack is not strictly speaking advanced. Strictly speaking, the main feature defining the attackers is Persistence”. (Kaspersky Lab, 2015)

Features: Sanger and Perlroth identift the features as “the scope of this attack on more than 100 banks and other financial institutions in 30 nations could make it one of the largest bank thefts ever”. (Sanger & Perlroth, 2015) According to Kaspersky researchers “all observed cases used spear phishing emails with Microsoft Word 97 – 2003 (.doc) files attached or CPL files. The doc files exploit both Microsoft Office (CVE-2012-0158 and CVE-2013-3906) and Microsoft Word (CVE- 2014-1761)”. (Kaspersky Lab, 2015)

The main steps of the attack progression are the following ones (Fox IT, 2014):

1. “Primary infection of an ordinary employee computer”,

2. “Getting a password of a user with administrative”,

3. “Rights on some computers. For example, a password of a technical support engineer”,

4. “Gaining legitimate access to one server”,

5. “Compromising the domain administrator password from the server”,

6. “Gaining access to the domain controller and compromising of all active domain accounts”,

7. “Gaining access to e-mail and workflow servers”,

8. “Gaining access to server and banking system administrator workstations”,

9. “Installing the software to monitor activity of interesting system operators. Usually photo and video recording was used”,

10. “Configuring remote access to servers of interest including firewall configuration changes”.

Target: The target is financial institutions and targeted countries are “Russia, USA, Germany, China, Ukraine, Canada, Taiwan, Hong-Kong, United Kingdom, Spain, Norway, India, France, Poland, Pakistan, Nepal, Morocco, The Czech Republic, Switzerland, Bulgaria, Australia, Iceland and Brazil”. (Kaspersky Lab, 2015)

Persistence: Kaspersky Lab researchers define persistence process as “the Carbanak malware checked victim systems for the presence of specialized and specific banking software. Only after the presence of banking systems was confirmed, were victims further exploited. To date, attacks against approximately 300 IP addresses around the world have been observed on analyzed C2s. Carbanak contains an espionage component that allows the attackers to take control of video capabilities on the victim systems”. (Kaspersky Lab, 2015) Fox IT reports that “the group uses Metasploit as one of their main hacking tools, either stand alone or as part of a framework. The activity includes port scanning and system reconnaissance, escalating privileges on systems by using for example the recent CVE-2014-4113 vulnerability, gathering credentials and hopping on to other systems and networks. Metasploit is being used to its full potential with scanning, exploiting, privilege escalation and post exploitation persistence being achieved with its standard toolset”. (Fox IT, 2014)

Exfiltration: Fox IT reports that “the Anunak malware has multiple ways of connecting to backends, which includes a PHP based backend reachable over HTTP and HTTPS, and a Windows server based component using a proprietary protocol. Additionally various ways of creating incidental and regular screen captures of the desktop of persons of interest within compromised organizations were methods employed by these attackers” (Fox IT, 2014) Kaspersky Lab announces that “more than 100 banking entities impacted up to now, at least half have suffered financial losses. The magnitude of the losses is significant, at least $1 billion (USD)”. (Kaspersky Lab, 2015)

CHAPTER 3
IN PURSUIT OF INDICATORS

3.1. Related works

Security Information and Event Management (SIEM) tools collect, analyze, normalize and correlates all files and analyze data coming from the various device and give a centralized view of logs. Sekharan and Kandasamy articulates "an abstraction of SIEM tools and event correlation engines, furnishing a description of their technical comparative study, focusing on most popular SIEM tools and open source rule-based correlation engines and profiles them". (Sekharan & Kandasamy, 2017)

Raja and Vasudevan express that "SIEM solution can be used at TCP SYN flood attacks. SIEM helps in the collection of events from heterogeneous devices and ordering into Common Event Format. The events collected are correlated and observed for changes in the system behaviour. Homogeneous Events such as DoS/Probe attacks can be detected by monitoring single event source". (Raja & Vasudevan, 2017) As an example rule that can be used in these attacks is:

"If {attribute IP <137.2> & kbthres < 70-130 > & tcp_bpsthres < 1000-10000 > & tcp_kbpsthres < 2.0-10 > & evt_raw_kbpsthres < 1.00-4.00 > then Threat = TCP-SYN-Flood}"

Among the security solutions SIEM closes a significant gap. It can easily find itself in IT infrastructures in many different sectors. Coppolino at al. (Coppolino, D'Antonio, Romano, Sgaglione, & Staffa, 2017) propose "the use of a SIEM-based framework specifically tailored for an ehealthcare portal developed within the context of the Italian National Project eHealthNet, which allows real time monitoring of portal accesses with the aim of detecting potential threats and anomalies that could cause major security issues".

Having SIEM solutions can be expensive in some cases. Similar results with open source solutions are possible. Detken at al. (Detke, 2017) state that it would be possible to monitor network traffic and generate alarms to strengthen access control by using open source SIEM tools.

In topologies where there is high log flow, security professionals spend more time and effort. The collection and monitoring of logs alone does not give enough results. The solution that facilitates this is the expectation of an alarm output through the incoming logs. Russ Anthony (Anthony, 2013) has done this through a sample log collection implementeation. In this work Anthony states that some log rules can be used to catch APT attacks. In his research he defined that a log rule can be created via log event id from multiple workstations. Some of his rules are:

- “Alert on < windows_process_name > unless the path is correct”,
- “Alert on svchost.exe unless its path is C:\Windows\System32\svchost.exe”,
- “Alert on explorer.exe unless its path is C:\Windows\explorer.exe”.

Bryant and Saiedian (Bryant & Saiedian, 2017) found a proper solution to the kill-chain model. In their study, they have extracted how many different log sources from each APT phase data can be obtained. So, areas strengthening the SIEM structure have been identified.

SIEM is an effective solution for monitoring logs and generating alarms. Feng at al. (Feng, 2017) “refer to the importance of the SOC process being included in the log investigation. Because of this, SOC may choose to investigate only the alerts with high severity or suppress the same type of alerts. This could potentially miss some severe attacks. The machine learning system sits in the middle of SOC work flow, incorporates different event logs, SIEM alerts and SOC analysis results and generates comprehensive user risk score for security operation center”.

SOC is of course important for instant follow-up of attacks. In this study, an APT rule set was created to support the SIEM structure by creating an open source infrastructure. A similar example of the infrastructure was also created by Falk et al. (Feng, 2017). They have demonstrated the availability of SIEM solutions in the virtual security operation center.

This security-centric approach to log management has taken its place in Chuvakin's output-driven approach. Chuvakin (Chuvakin, 2012) expresses that “deploying your security information and event management tool in such a way that nothing comes into your SIEM unless and until you know how it would be utilized and/or presented. In this context, an alarm-centric approach to SIEM is important”.

3.2. Determining Attack Indicators

This section aims to capture the indicators that can create log rules from the traces of attackers. With the correct configuration of these indicators, alarms can be generated.

3.2.1. Duke Family

Attackers in this attack use CVE-2011-0611 vulnerability. Microsoft defines as “this vulnerability could cause a crash and potentially allow an attacker to take control of the affected system. There are reports that this vulnerability is being exploited in the wild in targeted attacks via a Flash (.swf) file embedded in a Microsoft Word (.doc) file delivered as an email attachment, targeting the Windows platform”. (Microsoft, 2018) The starting point for this vulnerability is the creation of a word document in the Temp folder. If an alarm can be generated when a file is created in the Temp folder, advancement of the device will be prevented in advance. (Space, 2018)

Researchers describes that “The malware creates in * HKCU\Software\Microsoft\ApplicationManager a value ’AppID’ with the data it calculates from GetTickcount(), used as an identifier/mutex”. (CIRCL, 2014) If there is a registry value change in the specified registry path and there is an "AppID" phrase in it, this could be an attack indicator.

So the rules might be:

- Generate an alarm when a new word or text document is created in the Temp folder.

- Generate an alarm when a registry value “AppID” is created.

3.2.2. Dark Hotel

In the case of the Dark Hotel, the attackers erased their tracks during the attack. If an alarm is generated during file movement, the attack may be noticeable. The list of deleted files includes the following: (Kaspersky, 2014)

- dtlcntr.exe

- googletoolbar.exe

- active.dll
- detect.dll

So the rule might be:

- Generate an alarm when a known file is deleted in the Appdata folder.

3.2.3. Uroburous

In this attack, attackers create system files. According to researhers “The malware makes itself persistent on the system and creates a service with the following parameters, which loads the file usbdev.sys as a kernel driver:” (CIRCL, 2018)

In: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services:

Key: usblink

Type: 1 (SERVICE_KERNEL_DRIVER)

Start: 1 (SERVICE_SYSTEM_START)

ErrorControl: 0 (SERVICE_ERROR_IGNORE)

Group: Streams Drivers

DisplayName: usblink

ImagePath: \SystemRoot\$NtUninstallQ722833$\usbdev.sys

If an alarm can be generated when the above registry entry is made, it may have been caught from a point. So the rule might be:

- Generate an alarm when a registry key is created in “HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services”.

3.2.4. Dragonfly

For this APT any log rule has not been created.

3.2.5. Adwind

For this APT any log rule has not been created.

3.2.6. Blue Termite

Attackers use an executable file in this attack. They save the extracted executable file as “rdws.exe” in the current temp directory, then execute it with WinExec(). (Kaspersky, 2018)

If an alarm can be generated when rdws.exe file created it may have been caught from a point. So the rule might be:

- Generate an alarm when rdws.exe file is created in the temp folder.

3.2.7. APT28

In this type of attack, attackers collect information about the target machine. FireEye reports that “after collecting host information, malware creates a hidden file that may be named edg6EF885E2.tmp”. (FireEye, 2014)

If an alarm can be generated when edg6EF885E2.tmp file created then attack will be detected in phase 1, intelligence gathering. So the rule might be:

- Generate an alarm when edg6EF885E2.tmp file is created.

3.2.8. Equation

Attackers use MS09-025 vulnerability to get privilege escalation, adding an unauthorized user to the Administrator group. (Kaspersky Lab, 2015) In this case an alarm can be generated. So the rule might be:

- Generate an alarm when a user has added to a security-enabled local group.

3.2.9. NetTraveler

In this attack type, attackers exploit old vulnerabilities such as CVE-2012-0158 and CVE-2010-3333 in microsoft office, excel and rtf documents. They create some files and change registry configurations. So, the rules might be:

- Generate alarm when a certain file is created. These files are listed here: (Kaspersky Lab, 2013)

  “%Appdata%\Adobe\netmgr.dll”

  “%Appdata%\Adobe\netmgr.exe”

  “%Appdata%\Adobe\perf2012.ini”

“%Appdata%\Adobe\sysinfo2012.dll”

“%Appdata%\Adobe\enumfs.ini”

“%temp%\winlogin.exe”

“%temp%\smcs.exe”

“%windir%\system\config_t.dat”

“%windir%\system32\6to4ex.dll”

“%windir%\system32\svchost.log”

- Generate an alarm when windowsupdataney.dll file is created in System32 folder. (Raiu & Baumgartner, 2014)

- Generate an alarm when a registry key is created in “HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Windows updata” (Raiu & Baumgartner, 2014)

3.2.10. Regin

In this attack, malware samples contain a hardcoded registry path and value name to be used as a fallback location for content retrieval. In this case content is simply the value of the provided key/value-name combination. (F-Secure, 2014) An example registry location is:

\REGISTRY\Machine\System\CurrentControlSet\ Control\RestoreList

So, the rule migh be:

- Generate an alarm when a registry key is created in \System\CurrentControlSet\ Control\RestoreList

In Regin attack some files are loaded which “consist of a user-mode orchestrator and multiple kernel payload modules”. (Symantec, 2015)

So, the rule migh be:

- Generate an alarm when systemaudit.evt file is created in System\Config folder.

3.2.11. Duqu

In this attack, According to Symantec security researchers “when the word document is opened, the exploit is triggered. The exploit contains kernel mode shellcode, which will first check if the computer is already compromised by looking for the registry value HKEY_LOCAL_MACHINE\ SOFTWARE \Microsoft \Windows \CurrentVersion\Internet Settings\Zones\4\“CF1D”. If the computer has already been compromised, the shellcode gracefully exits”. (Symantec, 2011) This is CVE-2011-3402 vulnerability. So, the rule might be:

- Generate an alarm when a registry value is modified in “SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4 path”.

3.2.12. Wild Neutron

The attackers use the following file names. Alarms can be generated when these names are generated. List of filenames is:

“%APPDATA%\Roamng\FlashUtl.exe”

“%APPDATA%\Roamng\Acer\LveUpdater.exe”

“%APPDATA%\Roamng\Realtek\RtlUpd.exe”

“%ProgramData%\Realtek\RtlUpd.exe”

“%APPDATA%\Roamng\sqlte3.dll (UPX packed)”

“%WINDIR%\wnsesson.dll”
“%APPDATA%\appdata\local\temp\teamvewer\verson9\update.exe”
“%SYSTEMROOT%\temp_dbg.tmp”

“%SYSTEMROOT%\temp\ok.tmp”

“C:\wndows\temp\debug.txt”

“C:\wndows\syswow64\mshtaex.exe”

“%SYSROOT%\System32\mshtaex.exe %SYSROOT%\System32\wdgestEx.dll”

“%SYSROOT%\System32\dpcore16t.dll”

“%SYSROOT%\System32\astor32.exe”

“%SYSROOT%\System32\mspool.dll”

“%SYSROOT%\System32\msvcse.exe”

“%SYSROOT%\System32\mspool.exe”

“C:\Program Fles (x86)\LNVSute\LnrAuth.dll”
“C:\Program Fles (x86)\LNVSute\LnrAuthSvc.dll”
“C:\Program Fles (x86)\LNVSute\LnrUpdt.exe”

“C:\Program Fles (x86)\LNVSute\LnrUpdtP.exe”

3.2.13. Winnti

Mallware starts if some benign application depends on Windows winmm.dll (located in %WINDIR%\System32\winmm.dll) but the evil twin library with the same name (winmm.dll) is located in the folder of benign application, the malicious library will be loaded instead of the system one. Taking advantage of their control of an infected computer, the attackers place a malicious library in the %WINDIR% folder. The same folder also contains explorer.exe. “This enables the attackers to ensure that the malicious DLL is loaded at system startup”: explorer.exe loads the malicious winmm.dll from the %WINDIR% folder as soon as it launches during system startup. (Kaspersky Lab, 2013) According to this scenario, if winmm.dll is created in any folder alarm can be generated. On the other hand, attackers create a system file which name is splitter.sys. So, the rules might be:

- Generate an alarm when winmm.dll is created in any folder.

- Generate an alarm when splitter.sys is created in System32 folder.

3.2.14. Poseidon

For this APT any log rule has not been created.

3.2.15. FinSpy

Attackers use a malware which “displays a picture. This differs from sample to sample. When clicked it creates a directory, then it drops following files”: (Marquis-Boire & Marczak, 2013)

“C:\DOCUME~1\%USER%\LOCALS~1\Temp\delete.bat”
“C:\DOCUME~1\%USER%\LOCALS~1\Temp\driverw.sys”

Alarm can be generated when one of the above is created. On the other hand, “the malware uses encryption in an attempt to disguise harvested data in the .dat files intended for exfiltration. The AES key structure is highly predictable, as the quantum for updating the system clock (HKLM\SYSTEM\CurrentControlset\services\W32Time\Config\lastClockrate) is set to 0x2625A hundred-nanoseconds by default”. So, the rules might be:

- Generate an alarm when delete.bat is created in Temp folder.

- Generate an alarm when lastClockrate registry value is modified.

3.2.16. Black Energy

In this attack, if the attackers do not have administrator rights, they want to run windows with this right by restarting the operating system to bypass User Access Control (UAC). In this case, an alarm can be generated against the request of the non-administrators group. (F-Secure Labs, 2014) So, the rule might be:

- Generate an alarm when a member added to Administrators group.

3.2.17. Hacking Team RCS

In this attack, Boire defines that “windows backdoor contains a variety of clear-text strings which are found in the SSH-client, “Putty”. Execution of the windows backdoor writes the following files to disk”: (Boire, 2012)

“C:\DOCUME~1\ADMINI~1\LOCALS~1\jlc3V7we\IZsROY7X.-MP”
“C:\DOCUME~1\ADMINI~1\LOCALS~1\jlc3V7we\eiYNz1gd.Cfp”
“C:\DOCUME~1\ADMINI~1\LOCALS~1\jlc3V7we\t2HBeaM5.OUk”
“C:\DOCUME~1\ADMINI~1\LOCALS~1\jlc3V7we\WeP1xpBU.wA-”
“C:\DOCUME~1\ADMINI~1\LOCALS~1\jlc3V7we\6EaqyFfo.zIK”
“C:\DOCUME~1\ADMINI~1\LOCALS~1\jlc3V7we\lUnsA3Ci.Bz7”

In this case, if the directory where the files are located is monitored, an alarm can be generated when any file is added or changed. Directory name is jlc3V7we.

According to Citizen Lab researchers “the file ‘ZsROY7X.-MP’ appears to provide the main backdoor functionality. It is executed via rundll32 and the following registry entry created to ensure persistence” (Boire, 2012):

“HKU\s-1-5-21-1177238915-1336601894-725345543500\software\microsoft\windows\currentversion\run\*J7PugHy”
“C:\WINDOWS\system32\rundll32.exe”
“C:\DOCUME~1\ADMINI~1\LOCALS~1\jlc3V7we\IZsROY7X.-MP",F1dd208”

In this case, when a registry key is created which name is *J7PugHy an alarm can be generatd. So the rules might be:

- Generate an alarm when a certain folder is created which is jlc3V7we
- Generate an alarm when a registry key is created which is *J7PugHy.

3.2.18. Naikon

Attackers use e-mail spear-phish method by sending decoy documents to target groups. In this case, they create some files in Temp folder, these are:

“C:\Documents and Settings\user\Local Settings\ Temp\mshtml.dat”

“C:\DOCUME~1\user\LOCALS~1\Temp\upd.exe”

“C:\DOCUME~1\user\LOCALS~1\Temp\update.exe”

“C:\DOCUME~1\user\LOCALS~1\Temp\adobe.pdf”

So, the rule migh be:

- Generate an alarm when update.exe is created in Temp folder.

3.2.19. Cloud Atlas

Attackers use a log file to store credentials and send to command-and-control servers. In this case, log file name can be traced and can be generate an alarm when it is created. This file may placed following locations:

%ALLUSERSPROFILE%adt.dat

%LOCALAPPDATA%adt.dat

On the other hand, attackers use a module which its task is to write to a temporary file ‘%TMP%%number%.exe‘. “The file is removed when the process terminates”. This file can be traced for creating alarm. So, the rules might be:

- Generate an alarm when adt.dat is created in any folder.
- Generate an alarm when number.exe is created in Temp folder.

3.2.20. Hellsing

Golovkin describes that "once the Hellsing attackers compromise a computer, they deploy other tools which can be used for gathering further information about the victim or doing lateral movement. Attack tool deployed in a victim's environment is a file system driver, named "diskfilter.sys", although internally it claims to be named xrat.sys". (Golovkin, 2015) If an alarm can be generated while creating diskfilter.sys, this may be an indication for us to identify the attack. On the other hand, some of the debug paths are listed as follow:

"e:\Hellsing\release\irene\irene.pdb"

"d:\hellsing\sys\irene\objchk_win7_x86\i386\irene.pdb"

"d:\hellsing\sys\xkat\objchk_win7_x86\i386\xKat.pdb"

"d:\Hellsing\release\msger\msger_install.pdb"

"d:\Hellsing\release\msger\msger_server.pdb"

"d:\hellsing\sys\xrat\objchk_win7_x86\i386\xrat.pdb"

"d:\Hellsing\release\exe\exe\test.pdb"

One of above file can be traced such as msger_install.pdb. So, the rules might be:

- Generate an alarm when diskfilter.sys is created in drivers folder.

- Generate an alarm when msger_install.pdb is created in any folder.

3.2.21. Kimsuky

Tarakanov express that "there are two basic library (KBDLV2.DLL / AUTO.DLL) that is responsible for common communication with its campaign master, some modules performing the following functions" (Tarakanov, 2013). So, the rule might be:

- Generate an alarm when auto.dll is created in any folder.

3.2.22. Carbanak

Kaspersky Lab researchers defines that "Carbanak copies itself into "%system32%\com" with the name "svchost.exe" with the file attributes: system, hidden and read-only. The original file created by the exploit payload is then deleted". (Kaspersky Lab, 2015) So, the rule might be:

- Generate an alarm when svchost.exe is created in system32 folder.

CHAPTER 4
IMPLEMENTATION

4.1. Infrastructure

Different security techniques and solutions are implemented in preventing cyber attacks. IPS / IDS, firewall, e-mail security, etc. have an important role in the instant detection and prevention of attack. In addition, increased security needs also make it important to examine system and user logs. Therefore, it is possible to make meaningful conclusions from the event logs with the structure of SIEM.

In this study, it is aimed to facilitate the detection of APT attacks by the data obtained from the event logs. It would be enough to set up a log management infrastructure in the lab environment. The open source log management system allows us to experiment with rule sets and analyze their results.

An ELK open source log management system can be installed for this process. It will be sufficient to have installed windows server 2012 R2 at the basic level to the 3 virtual or physical servers. Also, it can be retrieved by using WinlogBeat from APT log sources. The main log collector must be loaded on the server as well as java, elasticsearch, kibana and x-pack applications. Eleasticsearch is a search engine, kibana is the visualization tool, and x-pack is a package for security analysis. The framework of this setup is visualized in Figure 4.1.

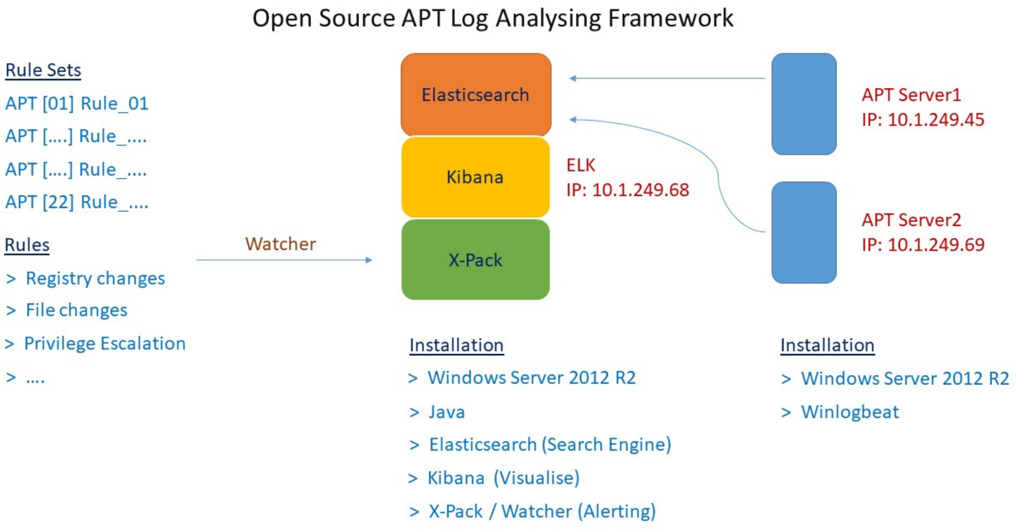


Figure 4.1 Open Source APT Log Analysing Framework

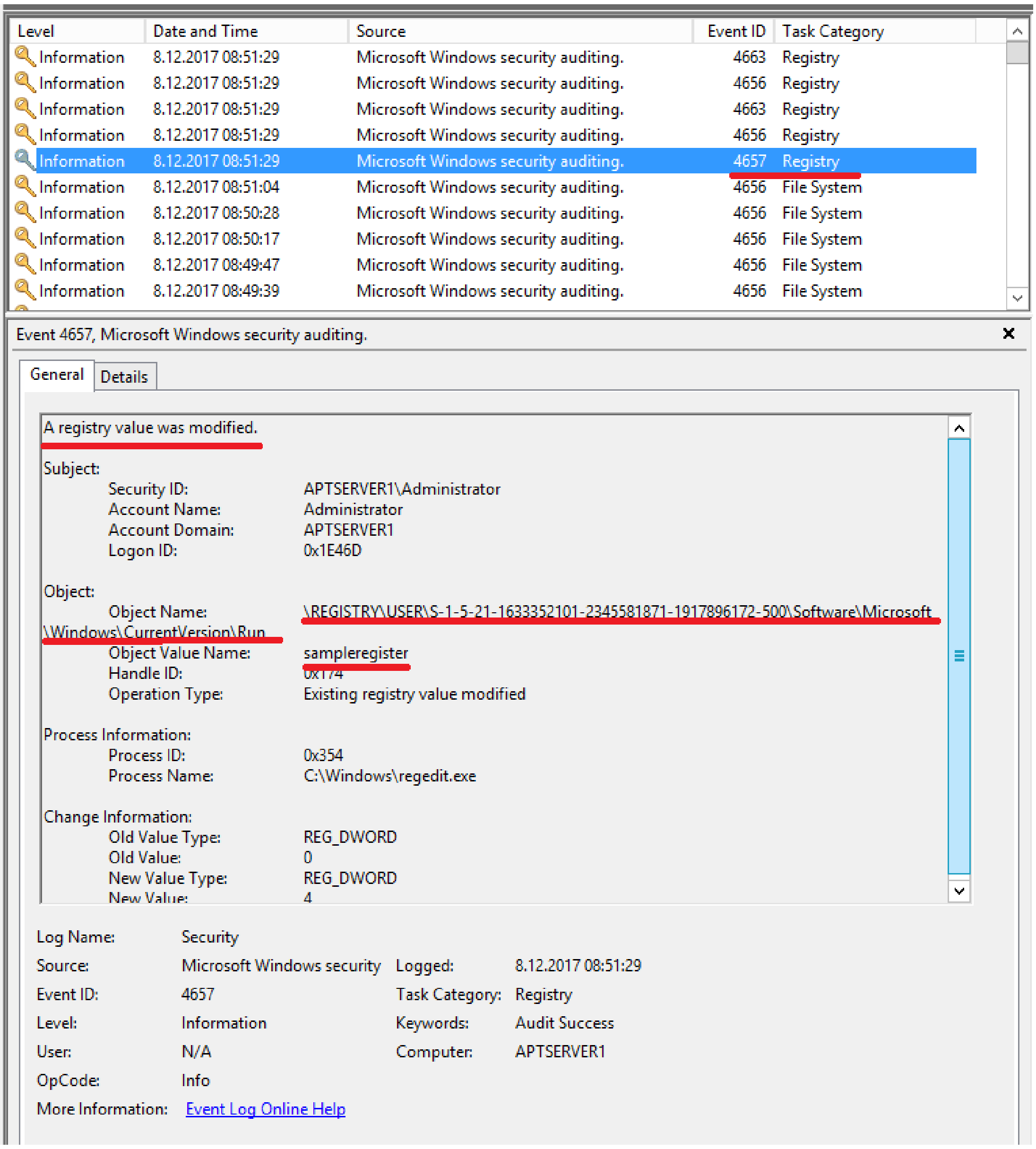
During this study, 22 APT attacks were examined. In this review log records are mainly concentrated at 3 points. These are;

- File changes

- Registry changes

- Privilege escalation attempts

In the majority of APT episodes there are changes in the registry. This process provides more convenient access to some initial processes in the infected machine. Figure 4.2 contains an example of the event log for a registry operation. An event created when making changes to the object named sampleregister.



Level	Date and Time	Source	Event ID	Task Category
Information	8.12.2017 08:51:29	Microsoft Windows security auditing.	4663	Registry
Information	8.12.2017 08:51:29	Microsoft Windows security auditing.	4656	Registry
Information	8.12.2017 08:51:29	Microsoft Windows security auditing.	4663	Registry
Information	8.12.2017 08:51:29	Microsoft Windows security auditing.	4656	Registry
Information	8.12.2017 08:51:29	Microsoft Windows security auditing.	4657	Registry
Information	8.12.2017 08:51:04	Microsoft Windows security auditing.	4656	File System
Information	8.12.2017 08:50:28	Microsoft Windows security auditing.	4656	File System
Information	8.12.2017 08:50:17	Microsoft Windows security auditing.	4656	File System
Information	8.12.2017 08:49:47	Microsoft Windows security auditing.	4656	File System
Information	8.12.2017 08:49:39	Microsoft Windows security auditing.	4656	File System

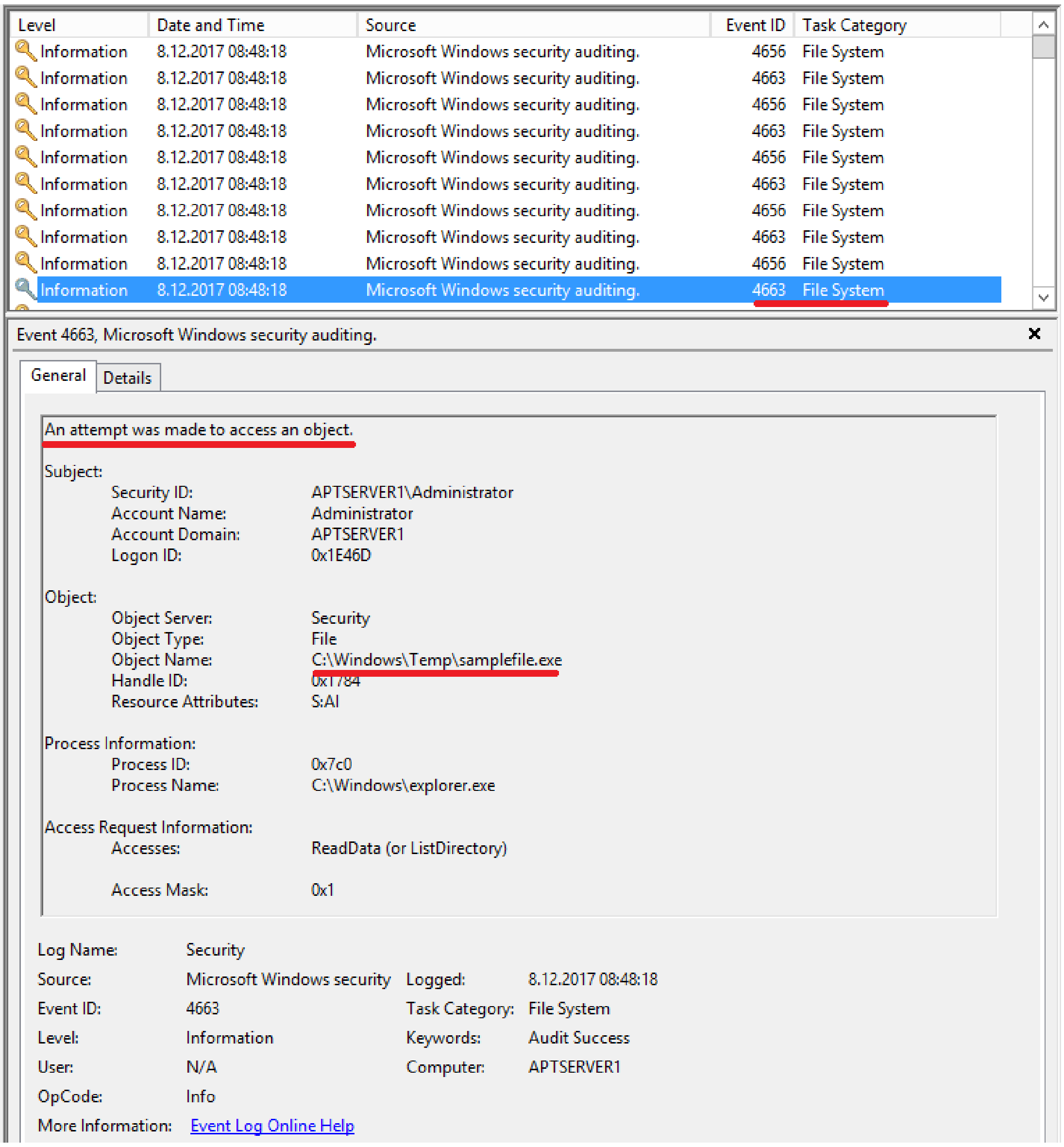
Event 4657, Microsoft Windows security auditing.

```
A registry value was modified.

Subject:
        Security ID:            APTSERVER1\Administrator
        Account Name:           Administrator
        Account Domain:         APTSERVER1
        Logon ID:               0x1E46D

Object:
        Object Name:            \REGISTRY\USER\S-1-5-21-1633352101-2345581871-1917896172-500\Software\Microsoft
\Windows\CurrentVersion\Run
        Object Value Name:      sampleregister
        Handle ID:              0x174
        Operation Type:         Existing registry value modified

Process Information:
        Process ID:             0x354
        Process Name:           C:\Windows\regedit.exe

Change Information:
        Old Value Type:         REG_DWORD
        Old Value:              0
        New Value Type:         REG_DWORD
        New Value:              4
```

```
Log Name:          Security
Source:            Microsoft Windows security   Logged:          8.12.2017 08:51:29
Event ID:          4657                         Task Category:   Registry
Level:             Information                  Keywords:        Audit Success
User:              N/A                          Computer:        APTSERVER1
OpCode:            Info
More Information:  Event Log Online Help
```

Figure 4.2 Registry Changes - Event when a registry key is created or modified.

During the APT attack, various main module files need to be loaded and run. These files are kept in file paths that will not pay attention during installation. One of the basic rules is the generation of a warning in the case of creating or executing a file. A file change event record shown in Figure 4. and a file called samplefile is provided. This process is processed in event logs. Therefore, the data in the event logs can be viewed via the file names.



Level	Date and Time	Source	Event ID	Task Category
Information	8.12.2017 08:48:18	Microsoft Windows security auditing.	4656	File System
Information	8.12.2017 08:48:18	Microsoft Windows security auditing.	4663	File System
Information	8.12.2017 08:48:18	Microsoft Windows security auditing.	4656	File System
Information	8.12.2017 08:48:18	Microsoft Windows security auditing.	4663	File System
Information	8.12.2017 08:48:18	Microsoft Windows security auditing.	4656	File System
Information	8.12.2017 08:48:18	Microsoft Windows security auditing.	4663	File System
Information	8.12.2017 08:48:18	Microsoft Windows security auditing.	4656	File System
Information	8.12.2017 08:48:18	Microsoft Windows security auditing.	4663	File System
Information	8.12.2017 08:48:18	Microsoft Windows security auditing.	4656	File System
Information	8.12.2017 08:48:18	Microsoft Windows security auditing.	4663	File System

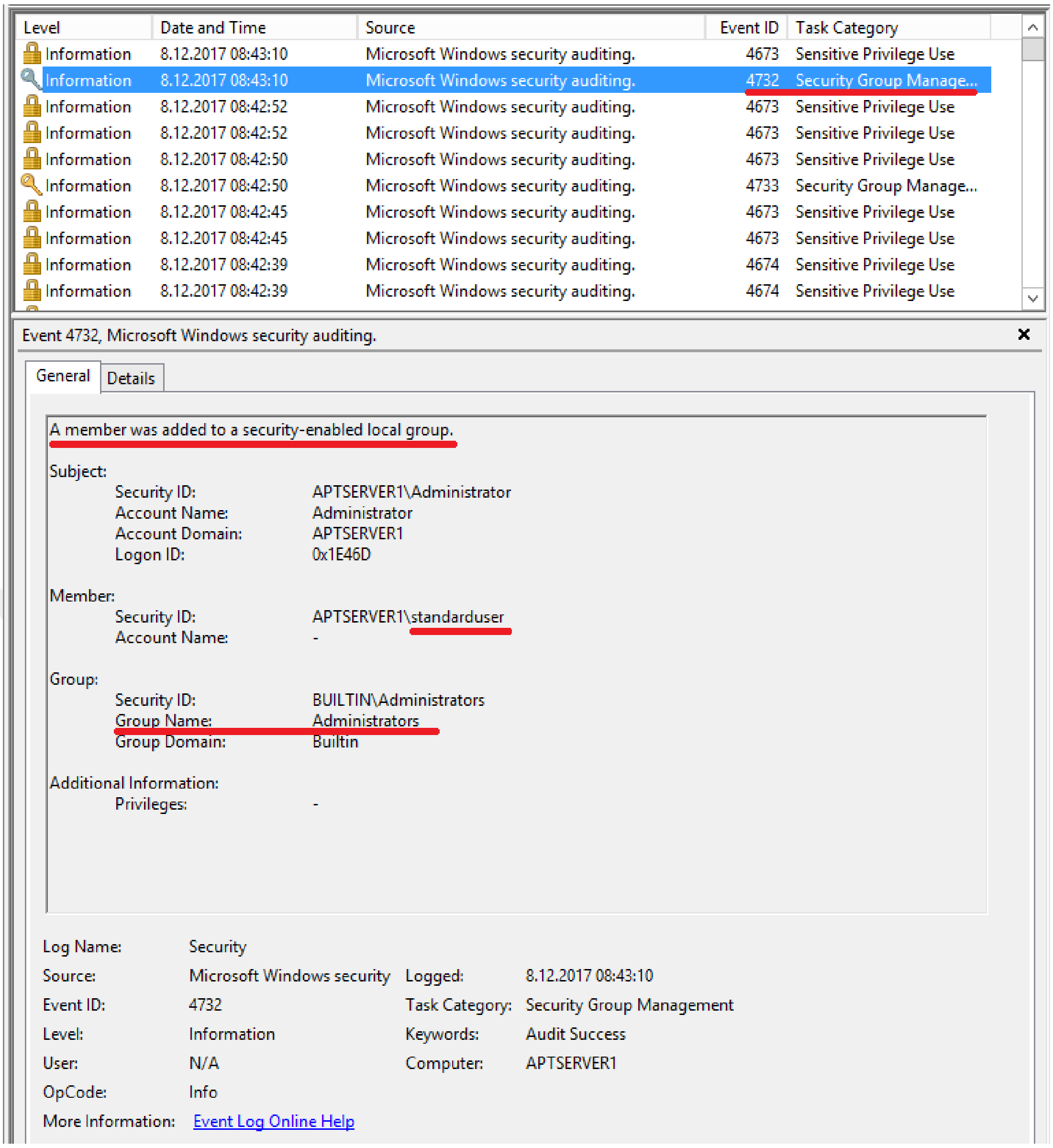
Event 4663, Microsoft Windows security auditing.

```
An attempt was made to access an object.

Subject:
        Security ID:            APTSERVER1\Administrator
        Account Name:           Administrator
        Account Domain:         APTSERVER1
        Logon ID:               0x1E46D

Object:
        Object Server:          Security
        Object Type:            File
        Object Name:            C:\Windows\Temp\samplefile.exe
        Handle ID:              0x1784
        Resource Attributes:    S:AI

Process Information:
        Process ID:             0x7c0
        Process Name:           C:\Windows\explorer.exe

Access Request Information:
        Accesses:               ReadData (or ListDirectory)

        Access Mask:            0x1
```

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	8.12.2017 08:48:18
Event ID:	4663	Task Category:	File System
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	APTSERVER1
OpCode:	Info		
More Information:	Event Log Online Help		

Figure 4.3 File Changes - Event when a file is copied or changed

It does not usually matter which user profile they have access to for attackers. Often they can upgrade the standard user profile they have acquired to the administrator profile. This process has been visualized in Figure 4.4. In this case, privilege escalations can be monitored.



Level	Date and Time	Source	Event ID	Task Category
Information	8.12.2017 08:43:10	Microsoft Windows security auditing.	4673	Sensitive Privilege Use
Information	8.12.2017 08:43:10	Microsoft Windows security auditing.	4732	Security Group Manage...
Information	8.12.2017 08:42:52	Microsoft Windows security auditing.	4673	Sensitive Privilege Use
Information	8.12.2017 08:42:52	Microsoft Windows security auditing.	4673	Sensitive Privilege Use
Information	8.12.2017 08:42:50	Microsoft Windows security auditing.	4673	Sensitive Privilege Use
Information	8.12.2017 08:42:50	Microsoft Windows security auditing.	4733	Security Group Manage...
Information	8.12.2017 08:42:45	Microsoft Windows security auditing.	4673	Sensitive Privilege Use
Information	8.12.2017 08:42:45	Microsoft Windows security auditing.	4673	Sensitive Privilege Use
Information	8.12.2017 08:42:39	Microsoft Windows security auditing.	4674	Sensitive Privilege Use
Information	8.12.2017 08:42:39	Microsoft Windows security auditing.	4674	Sensitive Privilege Use

Event 4732, Microsoft Windows security auditing.

```
A member was added to a security-enabled local group.

Subject:
          Security ID:              APTSERVER1\Administrator
          Account Name:             Administrator
          Account Domain:           APTSERVER1
          Logon ID:                 0x1E46D

Member:
          Security ID:              APTSERVER1\standarduser
          Account Name:             -

Group:
          Security ID:              BUILTIN\Administrators
          Group Name:               Administrators
          Group Domain:             Builtin

Additional Information:
          Privileges:               -
```

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	8.12.2017 08:43:10
Event ID:	4732	Task Category:	Security Group Management
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	APTSERVER1
OpCode:	Info		
More Information:	Event Log Online Help		

Figure 4.4 Privilege Escalation - Event when a member added to Adminstrators group.

4.2. Creating Rulesets

During creation of rules all rules are written in json format and it can be converted into any common format like XML etc. So, rules can be placed in any SIEM solution. Full codes in json format for file change, registry change and privilege escalation behaviors rule can be shown at Appendix 1 – Json Formatted Rulesets.

Duke Family

Rule 01: Search and find “text document” phrase inside the message body of windows log in Temp folder,

```
"match": {
          "message": "\\Temp\\New Text Document"
         }
```

Rule 02: Wait for a registry change in a folder

```
"must": [
         {
          "match": {
           "message": "a registry value was modified"
          }
         },
         {
          "match": {
           "message": "AppID”
          }
         }
```

Dark Hotel

Rule 01: Find a file movement request to an object.

```
"must": [
         {
          "match": {
           "message": "A handle to an object was requested"
          }
         },
         {
          "match": {
```

```
          "message": "\\Microsoft\\Crypto\\detect.dll"
         }
        }
```

Uroburous

Rule 01: Wait for a registry change, registry name is usblink.

```
"match": {
          "message":
"\\HKEY_LOCAL_MACHINE\\SYSTEM\\CurrentControlSet\\Services\\usblink"
         }
```

Blue Termite

Rule 01: Alarm when rdws.exe is created in the current temp directory,

```
"match": {
          "message": "\\Windows\\Temp\\rdws.exe"
         }
```

APT28

Rule 01: Alarm when a certain file is created which name is edg6EF885E2.tmp,

```
"match": {
          "message": "\\edg6EF885E2.tmp"
         }
```

Equation

Rule 01: Wait for a user has added to administrator group,

```
"must": [
{
  "match": {
    "message": "A member was added to a security-enabled local group"
  }
},
{
  "match": {
    "message": "Administrators"
  }
```

NetTraveler

Rule 01: Alarm when a certain file is created which name is netmgr.dll,

```
"match": {
          "message": "\\AppData\\Adobe\\netmgr.dll"
        }
```

Rule 02: Alarm when a certain file is created which name is \system32\Windowsupdataney.dll,

```
"match": {
          "message": "\\system32\\Windowsupdataney.dll"
        }
```

Rule 03: Create an alarm when a certain registry key is created,

```
"match": {
          "message":
"\\HKEY_LOCAL_MACHINE\\SYSTEM\\CurrentControlSet\\Services\\Windowsupdata"
        }
```

Regin

Rule 01: Create an alarm when a registry key is created,

```
"match": {
           "message": "\\SYSTEM\\CurrentControlSet\\Control\\RestoreList"
          }
```

Rule 02: Create an alarm when a certain file is created,

```
"match": {
           "message": "\\Config\\SystemAudit.Evt"
          }
```

Duqu

Rule 01: Create an alarm when a registry value is changed,

```
"must": [
         {
          "match": {
           "message": "a registry value was modified."
          }
         },
         {
          "match": {
           "message":
"\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Internet Settings\\Zones\\4"
          }
         },
         {
          "match": {
            "message": "CF1D"
          }
        }
      ],
```

Wild Neutron

Rule 01: Alarm when a certain windows file is created,

```
"match": {
            "message": "\\Appdata\\Roaming\\Flashutl.exe"
          }
```

Rule 02: Alarm when a certain windows temporary file is created,

```
"match": {
            "message": "\\Temp\\ok.tmp"
          }
```

Rule 03: Alarm when a certain executable file is created,

```
"match": {
            "message": "\\System32\\mspool.exe"
          }
```

Winnti

Rule 01: Create an alarm when a certain DLL file is created,

```
"match": {
            "message": "\\winmm.dll"
          }
```

Rule 02: Create an alarm when a certain system file is created,

```
"match": {
          "message": "\\System32\\splitter.sys"
         }
```

Finspy

Rule 01: Create an alarm when a certain file is created,

```
"match": {
          "message": "\\Temp\\delete.bat"
         }
```

Rule 02: Alarm when a registry value is changed,

```
"match": {
          "message":
"\\HKEY_LOCAL_MACHINE\\SYSTEM\\CurrentControlSet\\Services\\W32Time\
\lastClockrate"
         }
```

Black Energy

Rule 01: Create an alarm when a member added to Administrators group.

```
"match": {
          "message": "A member was added to a security-enabled local group"
         }
        },
        {
         "match": {
          "message": "Administrators"
         }
```

Hacking Team RCS

Rule 01: Create an alarm when a certain folder is created.

```
"match": {
            "message": "\\jlc3V7we"
           }
```

Rule 02: Create an alarm when a registry key is created.

```
"match": {
            "message":
"\\Software\\Microsoft\\Windows\\CurrentVersion\\Run\\*J7PugHy"
           }
```

Naikon

Rule 01: Create an alarm when a certain file is created in Temp folder.

```
"match": {
            "message": "\\Temp\\update.exe"
           }
```

Cloud Atlas

Rule 01: Create an alarm when a certain file is created.

```
"match": {
            "message": "\\adt.dat"
           }
```

Rule02: Create an alarm when a certain file is created.

```
"match": {
```

```
              "message": "\\number.exe"
            }
```

Hellsing

Rule 01: Create an alarm when a system file is created in a certain folder.

```
"match": {
              "message": "\\drivers\\diskfilter.sys"
            }
```

Rule 02: Create an alarm when a data file is created.

```
"match": {
              "message": "\\msger_install.pdb"
            }
```

Kimsuky

Rule01: Create an alarm whan a certain dll file is created.

```
"match": {
              "message": "\\System32\\auto.dll"
            }
```

Carbanak

Rule 01: Create an alarm when a certain file is created in a certain folder.

```
"match": {
              "message": "\\System32\\Com\\svchost.exe"
            }
```

4.3. Outputs of Rulesets

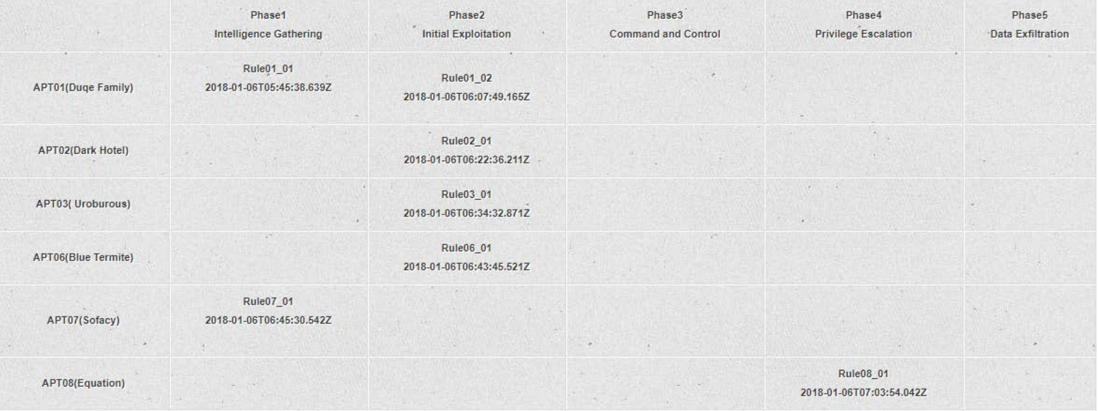
Outputs or alerts can be shown in different types such as an e-mail alert, a jira ticket or xml format for any application. In this study, Outputs of rulesets were shown as a screen message and listed at Appendix 1 – Outputs of Rulesets on ELK Platform.

CHAPTER 5
LISTING OF RESULTS

One of the various security solutions for detecting cyber attacks is the log management system. With this solution all system movements can be followed. There may be some traces left behind every advanced attacks. In this study, the traces left by 22 APTs previously experienced were analyzed. Through these analyzes, 30 different rules have been set up to determine the attacks.

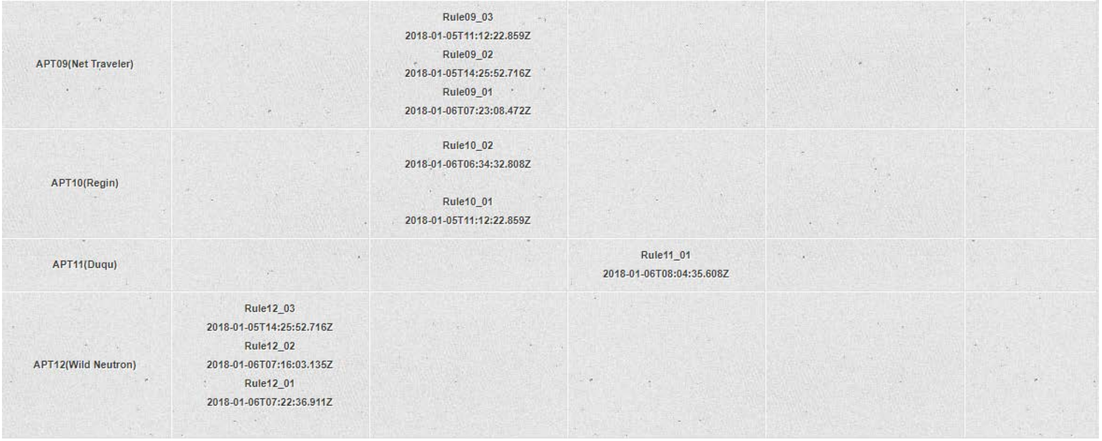
Reports can be generated shortly after the attacks are monitored and the data obtained. This section provides details of the reporting example. The aim here is to visualize the data related to APT attacks.

As you can see in the figures below, the names of the attacks are given in the column on the left. The data for the 5 phases of the APT are shown in the top row. The rules established for each of the attack are in the matching phase.



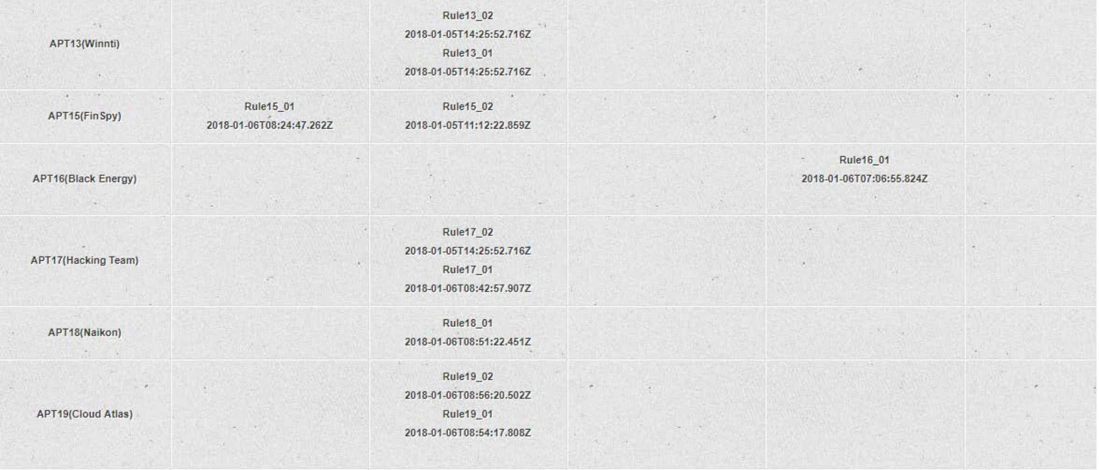
	Phase1 Intelligence Gathering	Phase2 Initial Exploitation	Phase3 Command and Control	Phase4 Privilege Escalation	Phase5 Data Exfiltration
APT01(Duqe Family)	Rule01_01 2018-01-06T05:45:38.639Z	Rule01_02 2018-01-06T06:07:49.165Z			
APT02(Dark Hotel)		Rule02_01 2018-01-06T06:22:36.211Z			
APT03(Uroburous)		Rule03_01 2018-01-06T06:34:32.871Z			
APT06(Blue Termite)		Rule06_01 2018-01-06T06:43:45.521Z			
APT07(Sofacy)	Rule07_01 2018-01-06T06:45:30.542Z				
APT08(Equation)				Rule08_01 2018-01-06T07:03:54.042Z	

Figure 5.1 Ruleset table of attacks, 1/4



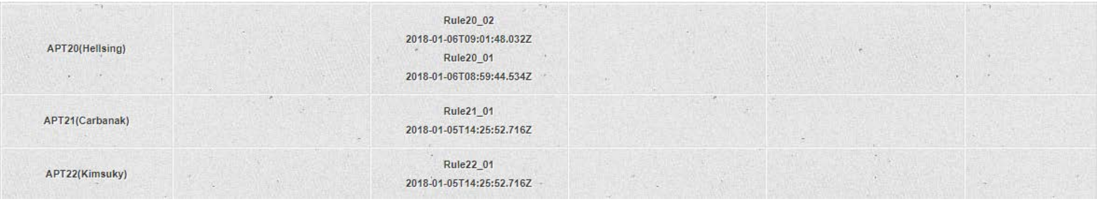
APT09(Net Traveler)		Rule09_03 2018-01-05T11:12:22.859Z Rule09_02 2018-01-05T14:25:52.716Z Rule09_01 2018-01-06T07:23:08.472Z			
APT10(Regin)		Rule10_02 2018-01-06T06:34:32.808Z Rule10_01 2018-01-05T11:12:22.859Z			
APT11(Duqu)			Rule11_01 2018-01-06T08:04:35.608Z		
APT12(Wild Neutron)	Rule12_03 2018-01-05T14:25:52.716Z Rule12_02 2018-01-06T07:16:03.135Z Rule12_01 2018-01-06T07:22:36.911Z				

Figure 5.2 Ruleset table of attacks, 2/4



APT13(Winnti)		Rule13_02 2018-01-05T14:25:52.716Z Rule13_01 2018-01-05T14:25:52.716Z			
APT15(FinSpy)	Rule15_01 2018-01-06T08:24:47.262Z	Rule15_02 2018-01-05T11:12:22.859Z			
APT16(Black Energy)				Rule16_01 2018-01-06T07:06:55.824Z	
APT17(Hacking Team)		Rule17_02 2018-01-05T14:25:52.716Z Rule17_01 2018-01-06T08:42:57.907Z			
APT18(Naikon)		Rule18_01 2018-01-06T08:51:22.451Z			
APT19(Cloud Atlas)		Rule19_02 2018-01-06T08:56:20.502Z Rule19_01 2018-01-06T08:54:17.808Z			

Figure 5.3 Ruleset table of attacks, 3/4



APT20(Hellsing)		Rule20_02 2018-01-06T09:01:48.032Z Rule20_01 2018-01-06T08:59:44.534Z			
APT21(Carbanak)		Rule21_01 2018-01-05T14:25:52.716Z			
APT22(Kimsuky)		Rule22_01 2018-01-05T14:25:52.716Z			

Figure 5.4 Ruleset table of attacks, 4/4

If we take a look at the above, for example Duqe Family, we can see that each rule catches the attack marks in two different phases. At the same time, if we look at the Hacking Team, we can see that two different rules have been established and that they are in phase 2 - initial exploitation.

Some of the attackers were not included in the table above, though they were examined in chapter 2. The log of these attacks was not formulated. For this reason, it has not been added to the table.

CHAPTER 6
DISCUSSION

Advanced persistent threats are beginning to pose risks within organizations of all levels as well as critical institutions. Business continuity is important for organizations. For this reason, the interruption of critical business activities poses a great risk for each company. Attacks targeting critical infrastructures continue to evolve over time, including critical business activities at every level. In this context, attack types and resources are increasing day by day.

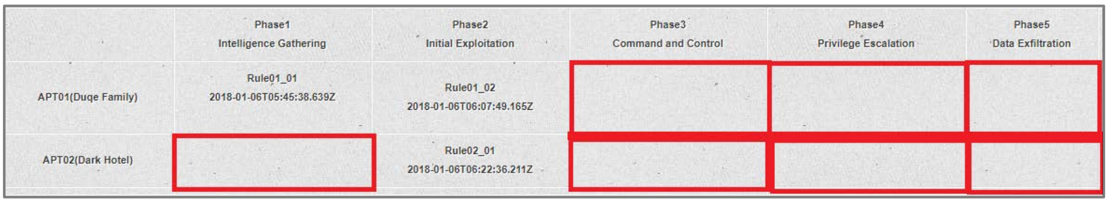
In such a case, this study had to examine the types of attacks at specific time intervals. It was examined in 2014 and 2016 between 22 APT attacks. The main focus here is on the different forms of attack and the common forms of behavior that they exhibit. According to these behaviors, it is expected that the security rules will be hardened by the log rules. New types of attacks are known to have similarities to existing forms of attacks. For this reason, even if the limit of work is specified, it is easy to apply it to all attacks showing similar behaviors.

Throughout this study, several reports that published by security laboratories were examined. In these reports, the rule sets that can be activated in any SIEM product have been defined through the attack indicators that stand out. Verification of these log rules was done by simulating the indicators of the attack in a lean SIEM test environment. Of course, there is no real APT test environment in the verification process. The reason for this is that APT attacks are a target-oriented and long-term attack. Targets can sometimes be a uranium cementing nuclear power plant or an internal operation application software coded specifically for a very large bank. The cost of such an extensive testing environment is very high. It is also unrealistic for the simulation to reflect the real environment. Therefore, in this study, it is analyzed which rule can be produced when similar images are generated in event indicators.

According to Net MarketShare's report, (NetMarketShare, 2018) the worldwide operating system usage rate is as follows: Windows 88.18%, Mac OS 9.17%, Linux 2.16, Chrome OS 0.31, Unknwon 0.17, BSD 0.01. If we look at these figures, it is normal for the operating system to be targeted by the attackers. This research was carried out only events that can be taken from windows machines. Therefore, the point where the SIEM rules are most needed against the APT threat is windows operating systems. Of course, future work can create rules within other operating systems.

The results of this study are listed in Figure 6-9. From there, a warning system can be created for logs corresponding to the rule created in security operation centers or applications with simple SIEM infrastructure. It is also intended that these warning systems be strengthened, including APT attacks.

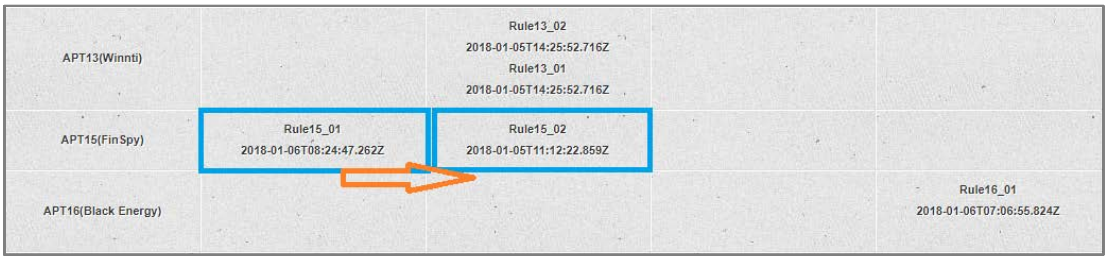
As seen in Figure 6.1, it was observed that no log corresponding to each of the APT phases was observed. The reason for this is quite obvious, these log rules have been established by taking into consideration the attack reports followed during the study. Technical analysis reports may have examined only a specific example of an attack over a certain period of time. Therefore, it is not expected that the research laboratories that set up the technical reports will create a study that can reveal the entire phase. However, as the work done in the labs over time increases, more log indicators can be obtained. It is therefore possible that at least one log rule corresponding to all the apt phases is generated.



	Phase1 Intelligence Gathering	Phase2 Initial Exploitation	Phase3 Command and Control	Phase4 Privilege Escalation	Phase5 Data Exfiltration
APT01(Duqe Family)	Rule01_01 2018-01-06T05:45:38.639Z	Rule01_02 2018-01-06T06:07:49.165Z			
APT02(Dark Hotel)		Rule02_01 2018-01-06T06:22:36.211Z			

Figure 6.1 Phases that non-generated log rules

The relationship between generated log rules is also important. There are several attacks in this study that can create more than one rule. However, this does not require a direct relationship between log rules. Because, these log rules were created by examining the attack indicators. There may be sufficient reason to make this relation meaningful during phase transitions. However, it is not correct to look for this relation in the log rules. Because the behavior of the attackers is different in all phases. They may not even choose to complete the entire phase in some attack types. For this reason, relational modeling between phases is difficult, even if there are significant indications. In this context, it can be said that there is a memoryless approach. As shown in Figure 6.2, there are 2 rules for phase 1 and phase 2 in FinSpy. However, these rules are not related to each other.



APT13(Winnti)		Rule13_02 2018-01-05T14:25:52.716Z Rule13_01 2018-01-05T14:25:52.716Z		
APT15(FinSpy)	Rule15_01 2018-01-06T08:24:47.262Z	Rule15_02 2018-01-05T11:12:22.859Z		
APT16(Black Energy)				Rule16_01 2018-01-06T07:06:55.824Z

Figure 6.2 Relationship between phases

6.1. Future Works

This research aims to strengthen the log management, which is an important part of security defense system. With the log rules obtained, an apt attack will be detectable without reaching result. However, the continuation of such a study is open. The writing of the SIEM rules can be continued considering the new APT types. On the other hand, at least one log rule can be generated on all of the APT phases. This action can be sustained through new notifications and indicators about attacks. Following the analysis of the attacks in the technical reports and security operations centers, these attack indicators may continue to be revealed.

This study is focused on APT attacks. The need to update log rules can come up in time. This may be the result of increasing technical reports of attacks.

In this research, an open source log management system, Elacticsearch Logstash and Kibana was used. Therefore, it may take time to implement these rules on different platforms. For example, this work can also be done to create YARA rule which is a rule-based approach to create descriptions of malware families based on textual or binary patterns. Also, it can be tested in different commercial log management systems.

CHAPTER 7
CONCLUSIONS

Sans Institute reports that “cyber security incidents will cause significant financial and reputation impacts on enterprise. In order to detect malicious activities, the SIEM (Security Information and Event Management) system is built in companies or government. The system correlates event logs from endpoint, firewalls, IDS/IPS (Intrusion Detection/Prevention System), DLP (Data Loss Protection), DNS (Domain Name System), DHCP (Dynamic Host Configuration Protocol), Windows/Unix security events, VPN logs etc.” (SANS Institute, 2013) From this point, log source inputs are expected to be transformed into active outputs. Significant results have been obtained when these outputs generate alarms.

In this study 22 APT attacks were examined and their indicators were collected. These indicators formed the base of the log rule sets as the source input. It was designed as a set with 30 different log rules and produces meaningful output. These outputs were examined in a test environment and it was found that they produced an alarm successfully. Thus, the detection of APT attacks can be more beneficial than the log management system. If the behavior of previous and present APT attacks is examined, these sets of rules will be replicated by removing robust indicators.

The following headings are impressive in this research. These are:

- Detection of APT attacks is a difficult process. However, it is not impossible. Indicators from the attack reports can be used to generate useful output. Beyond that, after an advanced laboratory test, many indicator points can be captured for each APT phase.

- There are many log management systems, both commercial and non-commercial. It may be necessary to work separately for the integration of the generated log rules with all systems. Creation and announcement of rule sets over a common language can be done.

- Highly critical APT attacks can be prevented with 3 different rule types, these are file changes, registry entries and privilege escalation requests. Only by activating them, high-level detection and monitoring can be done.

- A log management system with SIEM integration is an important advantage. However, it may not be enough. The SIEM structure integrated into the SOC system can give stronger results. Thus, all active and passive defense systems can produce strong results from a single point.

- Open source systems have more flexible structure than commercial products. It allows full development. For this reason, it may be advantageous to develop SIEM log rules through these systems.

At the onset of this investigation, it was predicted that a log rule set could be established upon examination of the technical reports on APT attacks. This prediction was made after the study. The APT rule group can be established within the SIEM structure. With this study, 30 rules were tested and alarms could be generated when windows event logs were followed.

REFERENCES

Anthony, R. (2013). Detecting Security Incidents Using Windows Workstation Event Logs. SANS Institute: Maryland.

Baumgartner, K., & Garnaeva, M. (2014, November 3). BE2 Custom Plugins, Router Abuse, and Target Profiles. apt.securelist.com: Retrieved from https://securelist.com/blog/research/67353/be2-custom-plugins-router-abuse-and-target-profiles/

Baumgartner, K., & Golovkin, M. (2015). The MsnMM Campaings: The Earliest Naikon APT Campaigns. Moscow: Kaspersky Lab.

Baumgartner, K., & Golovkin, M. (2015, May 14). The Naikon APT. Securelist.com: Retrieved from https://securelist.com/analysis/publications/69953/the-naikon-apt/

Bencs, B., Pek, G., Buttyan´, L., & Felegyhazi, M. (2012). The Cousins of Stuxnet: Duqu, Flame, and Gauss. Future Internet, 971-1003.

Blue Coat. (2015). The Inception Framework: Cloud-Hosted APT. CA: Blue Coat.

Boire, M. M. (2012). Backdoors are Forever:Hacking Team and the Targeting of Dissent. Toronto: The Citizen Lab.

Check Point . (2015, March 26). Intelligence Report: Equation Group. blog.checkpoint.com: Retrieved from http://blog.checkpoint.com/2015/03/26/intelligence-report-equation-group/

Chuvakin, A. (2012, 09 24). On “Output-driven” SIEM. https://blogs.gartner.com: Retrieved from https://blogs.gartner.com/anton-chuvakin/2012/09/24/on-output-driven-siem/

CIRCL. (2014). Analysis Report (TLP:WHITE) Analysis of a stage 3 Miniduke sample. Luxembourg: CIRCL.

CIRCL. (2018, March 11). TR-25 Analysis - Turla / Pfinet / Snake/ Uroburos. Retrieved from www.circl.lu: https://www.circl.lu/pub/tr-25/

Coppolino, L., D’Antonio, S., Romano, L., Sgaglione, L., & Staffa, M. (2017). Addressing Security Issues in the eHeatlh Domain Relying on SIEM Solutions. 2017 IEEE 41st Annual Computer Software and Applications Conference (s. 510-515). Naples: IEEE.

Currier, C., & Marquis-Boire, M. (2014, October 30). Secret Manuals Show the Spyware Sold to Despots and Cops Worldwide. theintercept.com: Retrieved from https://theintercept.com/2014/10/30/hacking-team/

Dereszowski, A., & Tecamac. (2014). Uroburos: The Snake Rootkit.

Detke, K.-O. J. (2017). Combining Network Access Control (NAC) and SIEM Functionality based on Open Source. The 9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (s. 300-305). Bucharest: IEEE.

Dinkar, D. e. (2016). McAfee Labs Threats Report. McAfee Labs.

Feng, C. W. (2017). A user-centric machine learning framework for cyber security operations center. 2017 IEEE International Conference on Intelligence and Security Informatics (s. 173-175). Beijing: IEEE.

FireEye. (2014). APT28: A Window Into Russia's Cyber Espionage Operations? CA: FireEye.

Fox IT. (2014). Anunak: APT Against Financial Institutions. Delft: Group IB and Fox IT.

F-Secure. (2013). Cosmicduke Cosmu with a twist of MiniDuke. Helsinki: F-Secure Labs.

F-Secure. (2014). Malware Analysis Report W32/Regin Stage #1. Helsinki: F-Secure.

F-Secure Labs. (2014). Blackenergy & Quedagh: The Convergence of Crimeware. Helsinki: F-Secure.

GData. (2014). Uroburos Highly Complex Espionage Software with Russian Roots. G Data Security Labs.

Golovanov, S. (2013, April 23). Spyware. HackingTeam. securelist.com: Retrieved from https://securelist.com/analysis/publications/37064/spyware-hackingteam/

Golovkin, M. (2015, April 15). The Chronicles of the Hellsing APT: the Empire Strikes Back. securelist.com: Retrieved from https://securelist.com/analysis/publications/69567/the-chronicles-of-the-hellsing-apt-the-empire-strikes-back/

Hacquebord, F. (2015, April 16). Operation Pawn Storm Ramps Up its Activities; Targets NATO, White House. blog.trendmicro.com: Retrieved from http://blog.trendmicro.com/trendlabs-security-intelligence/operation-pawn-storm-ramps-up-its-activities-targets-nato-white-house/

IBM MSS. (2014). When Aa Energetic Bear Creates Havex. IBM.

Infosec. (2018, 06 14). Equation Group APT and TAO NSA: Two Hacking Arsenals Too Similar. resources.infosecinstitute.com: Retrieved from https://resources.infosecinstitute.com/equation-group-apt-tao-nsa-two-hacking-arsenals-similar/#gref

IT BusinessEdge. (2018, 08 19). The Most Famous Advanced Persistent Threats in History. www.itbusinessedge.com: Retrieved from https://www.itbusinessedge.com/slideshows/the-most-famous-advanced-persistent-threats-in-history-24.html

Kamluk, V., & Gostev, A. (2016). Adwind — A Cross-Platform RAT. Kaspersky Lab.

Karspersky. (2016, August 02). Energetic Bear: more like a Crouching Yeti. https://securelist.com: Retrieved from https://securelist.com/blog/research/65240/energetic-bear-more-like-a-crouching-yeti/

Karspersky Lab. (2016, August 15). Adwind: Malware-as-a-Service Platform that Hit more than 400,000 Users and Organizations Globally. http://www.kaspersky.com: Retrieved from http://www.kaspersky.com/about/news/virus/2016/Adwind

Kaspersky. (2014). The Darkhotel APT a Story of Unusual Hospitality. Moscow: Karspersky Lab.

Kaspersky. (2015, August 19). Blue Termite: Sophisticated Cyber Espionage Campaign After High-Profile Japanese Targets. http://usa.kaspersky.com/: Retrieved from http://usa.kaspersky.com/about-us/press-center/press-releases/2015/blue-termite-sophisticated-cyber-espionage-campaign-after-high-

Kaspersky. (2015, February 16). Equation: The Death Star of Malware Galaxy. securelist.com: Retrieved from https://securelist.com/blog/research/68750/equation-the-death-star-of-malware-galaxy/

Kaspersky. (2015). Targeted Cyberattack Logbook. apt.securelist.com: Retrieved from https://apt.securelist.com

Kaspersky. (2015, July 8). Wild Neutron – Economic Espionage Threat Actor Returns With New Tricks. securelist.com: Retrieved from https://securelist.com/blog/research/71275/wild-neutron-economic-espionage-threat-actor-returns-with-new-tricks/

Kaspersky. (2018, June 12). Epic Turla. apt.securelist.com: Retrieved from https://apt.securelist.com/#!/threat/1032

Kaspersky. (2018, 06 21). Kaspersky Lab Analyzes Active Cyberespionage Campaign Targeting Online Gaming Companies Worldwide. www.kaspersky.com: Retrieved from https://www.kaspersky.com/about/press-releases/2013_kaspersky-lab-analyzes-active-cyberespionage-campaign-targeting-online-gaming-companies-worldwide

Kaspersky. (2018, March 15). New activity of the Blue Termite APT. www.securelist.com: Retrieved from https://securelist.com/new-activity-of-the-blue-termite-apt/71876/

Kaspersky Lab. (2013). The NetTraveler . Moscow: Kaspersky.

Kaspersky Lab. (2013, January 17). “Red October”. Detailed Malware Description 4. Second Stage of Attack. securelist.com: Retrieved from https://securelist.com/analysis/publications/36884/red-october-detailed-malware-description-4-second-stage-of-attack/#11

Kaspersky Lab. (2013, January 17). “Red October”. Detailed Malware Description 5. Second Stage of Attack. securelist.com: Retrieved from https://securelist.com/analysis/publications/36879/red-october-detailed-malware-description-5-second-stage-of-attack/#14

Kaspersky Lab. (2013). “Winnti” More Than Just A Game. Moscow: Kaspersky.

Kaspersky Lab. (2014, December 10). Cloud Atlas: RedOctober APT is back in style. securelist.com: Retrieved from https://securelist.com/blog/research/68083/cloud-atlas-redoctober-apt-is-back-in-style/

Kaspersky Lab. (2014). The Regin Platform Nation-State Ownage of GSM Networks. Moscow: Kaspersky.

Kaspersky Lab. (2015). Carbanak APT: The Great Bank Robbery. Moscow: Kaspersky.

Kaspersky Lab. (2015). Equation Group: Questions and Answers. Moscow: Kaspersky.

Kaspersky Lab. (2015, April 15). The Chronicles of Hellsing: a Spy vs Spy Story. http://newsroom.kaspersky.eu/: Retrieved from http://newsroom.kaspersky.eu/fileadmin/user_upload/en/Campaign/KESB_2013/Pdfs/Amended_Kaspersky_Lab_press_release_Hellsing_final_eng.pdf

Kaspersky Lab. (2015, June 15). The Duqu 2.0 persistence module. securelist.com: Retrieved from https://securelist.com/blog/research/70641/the-duqu-2-0-persistence-module/

Kaspersky Lab. (2015, February 16). The Great Bank Robbery: the Carbanak APT. securelist.com: Retrieved from https://securelist.com/blog/research/68732/the-great-bank-robbery-the-carbanak-apt/

Kaspersky Lab. (2015, June 10). The Mystery of Duqu 2.0: A Sophisticated Cyberespionage Actor Returns. securelist.com: Retrieved from https://securelist.com/blog/research/70504/the-mystery-of-duqu-2-0-a-sophisticated-cyberespionage-actor-returns/

Kaspersky Lab. (2016, February 9). Poseidon Group: A Targeted Attack Boutique Specializing In Global Cyber-espionage. securelist.com: Retrieved from https://securelist.com/blog/research/73673/poseidon-group-a-targeted-attack-boutique-specializing-in-global-cyber-espionage/

KasperskyLab. (2016, 06 06). Miniduke is back: Nemesis Gemina and the Botgen Studio. https://apt.securelist.com: Retrieved from https://apt.securelist.com

Kovacs, E. (2015, August 20). Blue Termite APT Targets Japanese Organizations. http://www.securityweek.com/: Retrieved from http://www.securityweek.com/blue-termite-apt-targets-japanese-organizations

Makrushin, D. (2015, April 15). Deny the Hellsing APT by default. business.kaspersky.com: Retrieved from https://business.kaspersky.com/deny-the-hellsing-apt-by-default/3851/

Marquis-Boire, M., & Marczak, B. (2013). The Commercialization of Digital Spying. Toronto: Citizen Lab.

Maslennikov, D. (2013, February 28). Mobile Malware Evolution: Part 6. securelist.com: Retrieved from https://securelist.com/analysis/publications/36996/mobile-malware-evolution-part-6/

Microsoft. (2018, March 06). Exploit:SWF/CVE-2011-0611.A. www.microsoft.com: Retrieved from https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Exploit:SWF/CVE-2011-0611.A

Nazario, J. (2007). BlackEnergy DDoS Bot. Massachusetts: Arbor Networks.

Paganini, P. (2013, September 11). Kaspersky revealed "Kimsuky" Cyber Espionage campaign targeting South Korea. http://thehackernews.com/: Retrieved from http://thehackernews.com/2013/09/Kimsuky-malware-Cyber-Espionage-campaign-South-Korea.html

Paganini, P. (2013, February 28). MiniDuke hackers target European governments and researchers. securityaffairs.co: Retrieved from https://securityaffairs.co/wordpress/12634/malware/miniduke-hackers-target-european-governments-and-researchers.html

Raiu, C., & Baumgartner, K. (2014, August 27). NetTraveler APT Gets a Makeover for 10th Birthday. securelist.com: Retrieved from https://securelist.com/nettraveler-apt-gets-a-makeover-for-10th-birthday/66272/

Raja, N. M., & Vasudevan, R. A. (2017). Rule Generation for TCP SYN Flood attack in SIEM Environment. 7th International Conference on Advances in Computing

& Communications (s. 580-587). Cochin: Elsevier.

Sanger, D. E., & Perlroth, N. (2015, February 14). Bank Hackers Steal Millions via Malware. nytimes.com: Retrieved from http://www.nytimes.com/2015/02/15/world/bank-hackers-steal-millions-via-malware.html?_r=0

SANS Institute. (2013). The 6 Categories of Critical Log Information. https://www.sans.edu: Retrieved from https://www.sans.edu/cyber-research/security-laboratory/article/6toplogs

Scott, J., & Spaniel, D. (2016). Know Your Enemies. Institute for Critical Infrastructure Technology. Retrieved from www.icitech.org

Securelist. (2018, 8 2). “NetTraveler is Running!” – Red Star APT Attacks Compromise High-Profile Victims. securelist.com: Retrieved from https://securelist.com/nettraveler-is-running-red-star-apt-attacks-compromise-high-profile-victims/35936/

Securelist. (2018, 07 21). Sofacy APT hits high profile targets with updated toolset. securelist.com: Retrieved from https://securelist.com/sofacy-apt-hits-high-profile-targets-with-updated-toolset/72924/

Securulist. (2018, 06 11). Naikon. apt.securelist.com: Retrieved from https://apt.securelist.com/#!/threat/1006

Sekharan, S. S., & Kandasamy, K. (2017). Profiling SIEM Tools and Correlation Engines for Security Analytics. WiSPNET 2017 Conferenc (s. 717-721). Chennai: IEEE.

Space, M. T. (2018, March 06). How to Track File Access, Modify and Delete Actions in Windows Folder. http://www.morgantechspace.com: Retrieved from http://www.morgantechspace.com/2014/11/How-to-monitor-or-track-File-Access-in-Windows.html

Stewart, J. (2010, March 3). BlackEnergy Version 2 Analysis. archive.is: Retrieved from http://archive.is/QS5oj#selection-1163.0-1163.30

Sy, B. (2015, September 1). Attackers Target Organizations in Japan; Transform Local Sites into C&C Servers for EMDIVI Backdoor. http://blog.trendmicro.com/: Retrieved from http://blog.trendmicro.com/trendlabs-security-intelligence/attackers-target-organizations-in-japan-transform-local-sites-into-cc-servers-for-emdivi-backdoor/

Symantec. (2011). W32.Duqu. CA: Symantec.

Symantec. (2014, November 12). Operation CloudyOmega: Ichitaro zero-day and ongoing cyberespionage campaign targeting Japan. http://www.symantec.com/:

Retrieved from http://www.symantec.com/connect/blogs/operation-cloudyomega-ichitaro-zero-day-and-ongoing-cyberespionage-campaign-targeting-japan

Symantec. (2015). Butterfly: Corporate Spies Out For Financial Gain. CA: Symantec Security Response.

Symantec. (2015, July 8). Butterfly: Profiting From High-level Corporate Attacks. symantec.com: Retrieved from https://www.symantec.com/connect/blogs/morpho-profiting-high-level-corporate-attacks

Symantec. (2015). Regin: Top-tier Espionage Tool. CA: Symantec.

Symantec Response. (2014). Dragonfly: Cyberespionage Attacks Against Energy Suppliers. Symantec.

Taneja, V. (2013, March 14). Travnet Trojan Could Be Part of APT Campaign. blogs.mcafee.com: Retrieved from https://blogs.mcafee.com/mcafee-labs/travnet-trojan-could-be-part-of-apt-campaign/

Tarakanov, D. (2013, September 11). The “Kimsuky” Operation: A North Korean APT ? securelist.com: Retrieved from https://securelist.com/analysis/publications/57915/the-kimsuky-operation-a-north-korean-apt/

Threat Connect and Defense Group. (2015). CAMERASHY Closing The Aperture On China's Unit 78020. Arlington, Vienna.

APPENDIX 1 – Json Formatted Rulesets

A file change rule:

```
{
  "trigger": {
    "schedule": {
      "interval": "1m"
    }
  },
  "input": {
    "search": {
      "request": {
        "search_type": "query_then_fetch",
        "indices": [
          "winlogbeat-*"
        ],
        "types": [],
        "body": {
          "query": {
            "bool": {
              "must": [
                {
                  "match": {
                    "message": "\\Temp\\rdws.exe"
                  }
                },
                {
                  "match": {
                    "message": "A handle to an object was requested"
                  }
                }
              ],
              "filter": {
                "range": {
                  "@timestamp": {
                    "from": "now-1d",
                    "to": "now"
                  }
                }
              }
            }
          }
        }
      }
    }
  },
  "condition": {
    "compare": {
      "ctx.payload.hits.total": {
        "gt": 0
      }
    }
  },
  "actions": {
    "log": {
      "logging": {
        "level": "info",
        "text": "A windows file has been created, Blue Termite APT Phase 2 may have begun."
      }
    }
  }
}
```

A registry change rule:

```
{
  "trigger": {
    "schedule": {
      "interval": "1m"
    }
```

```
},
"input": {
  "search": {
    "request": {
      "search_type": "query_then_fetch",
      "indices": [
        "winlogbeat-*"
      ],
      "types": [],
      "body": {
        "query": {
          "bool": {
            "must": [
              {
                "match": {
                  "message": "An attempt was made to access an object"
                }
              },
              {
                "match": {
                  "message":
"\\HKEY_LOCAL_MACHINE\\SYSTEM\\CurrentControlSet\\Services\\Windowsupdata"
                }
              }
            ],
            "filter": {
              "range": {
                "@timestamp": {
                  "from": "now-1d",
                  "to": "now"
                }
              }
            }
          }
        }
        }
      }
    }
  },
  "condition": {
    "compare": {
      "ctx.payload.hits.total": {
        "gt": 0
      }
    }
  },
  "actions": {
    "log": {
      "logging": {
        "level": "info",
        "text": "A registry key has been created, Net Traveler APT Phase 2 may have begun."
      }
    }
  }
}
```

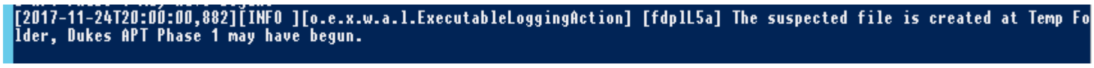
A privilege escalation rule:

```
{
  "trigger": {
    "schedule": {
      "interval": "2m"
    }
  },
  "input": {
    "search": {
      "request": {
        "search_type": "query_then_fetch",
        "indices": [
          "winlogbeat-*"
      ],
      "types": [],
      "body": {
        "query": {
          "bool": {
            "must": [
              {
                "match": {
                  "message": "A member was added to a security-enabled local group"
                }
              },
              {
                "match": {
                  "message": "Administrators"
                }
              }
            ],
            "filter": {
              "range": {
                "@timestamp": {
                  "from": "now-1d",
                  "to": "now"
                }
              }
            }
          }
        }
      }
    }
  }
},
"condition": {
  "compare": {
    "ctx.payload.hits.total": {
      "gt": 0
      }
    }
  },
  "actions": {
    "log": {
      "logging": {
        "level": "info",
        "text": "A user has been added to Administrators Group, Black Energy APT may have begun."
      }
    }
  }
}
```

APPENDIX 2 – Outputs Of Rulesets On Elk Platform

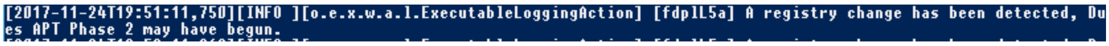
Dukes APT;

Rule1:



```
[2017-11-24T20:00:00,882][INFO ][o.e.x.w.a.l.ExecutableLoggingAction] [fdplL5a] The suspected file is created at Temp Fo
lder, Dukes APT Phase 1 may have begun.
```

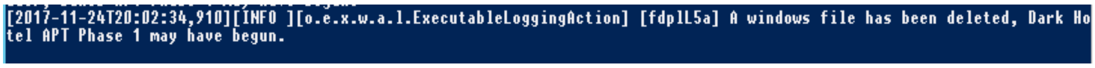
Rule2:



```
[2017-11-24T19:51:11,750][INFO ][o.e.x.w.a.l.ExecutableLoggingAction] [fdplL5a] A registry change has been detected, Du
es APT Phase 2 may have begun.
```

Dark Hotel;

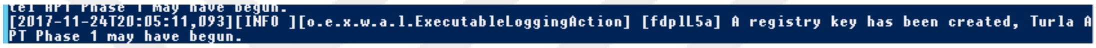
Rule1:



```
[2017-11-24T20:02:34,910][INFO ][o.e.x.w.a.l.ExecutableLoggingAction] [fdplL5a] A windows file has been deleted, Dark Ho
tel APT Phase 1 may have begun.
```

Uroburous/Turla/Epic Turla/Snake;

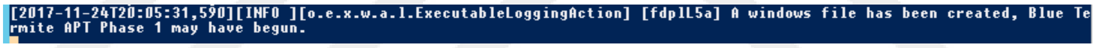
Rule1:



```
tel APT Phase 1 may have begun.
[2017-11-24T20:05:11,093][INFO ][o.e.x.w.a.l.ExecutableLoggingAction] [fdplL5a] A registry key has been created, Turla A
PT Phase 1 may have begun.
```

Blue Termite / Emdivi / CloudyOmega;

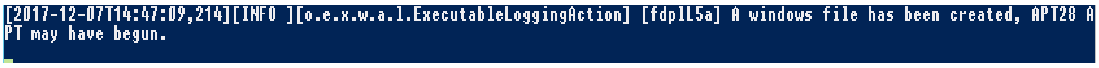
Rule1:



```
[2017-11-24T20:05:31,590][INFO ][o.e.x.w.a.l.ExecutableLoggingAction] [fdplL5a] A windows file has been created, Blue Te
rmite APT Phase 1 may have begun.
```

Sofacy / APT28 / Sednit / Fancy Bear / STRONTIUM / Pawn Storm;

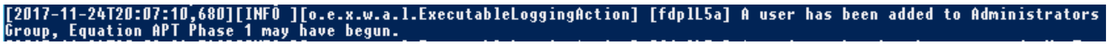
Rule1:



```
[2017-12-07T14:47:09,214][INFO ][o.e.x.w.a.l.ExecutableLoggingAction] [fdplL5a] A windows file has been created, APT28 A
PT may have begun.
```

Equation;

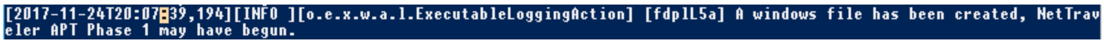
Rule1:



```
[2017-11-24T20:07:10,680][INFO ][o.e.x.w.a.l.ExecutableLoggingAction] [fdplL5a] A user has been added to Administrators
Group, Equation APT Phase 1 may have begun.
```

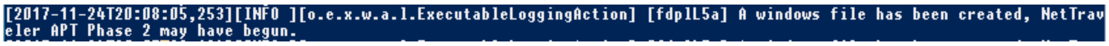
NetTraveler / Travnet / Netfile;

Rule1:



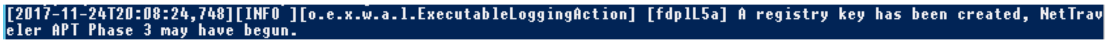
```
[2017-11-24T20:07:39,194][INFO ][o.e.x.w.a.l.ExecutableLoggingAction] [fdplL5a] A windows file has been created, NetTrav
eler APT Phase 1 may have begun.
```

Rule2:



```
[2017-11-24T20:08:05,253][INFO ][o.e.x.w.a.l.ExecutableLoggingAction] [fdplL5a] A windows file has been created, NetTrav
eler APT Phase 2 may have begun.
```

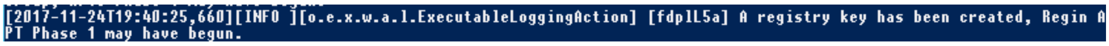
Rule3:



```
[2017-11-24T20:08:24,748][INFO ][o.e.x.w.a.l.ExecutableLoggingAction] [fdplL5a] A registry key has been created, NetTrav
eler APT Phase 3 may have begun.
```

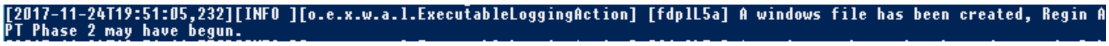
Regin;

Rule1:



```
[2017-11-24T19:40:25,660][INFO ][o.e.x.w.a.l.ExecutableLoggingAction] [fdplL5a] A registry key has been created, Regin A
PT Phase 1 may have begun.
```

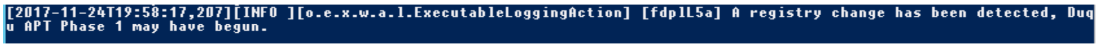
Rule2:



```
[2017-11-24T19:51:05,232][INFO ][o.e.x.w.a.l.ExecutableLoggingAction] [fdplL5a] A windows file has been created, Regin A
PT Phase 2 may have begun.
```

Duqu;

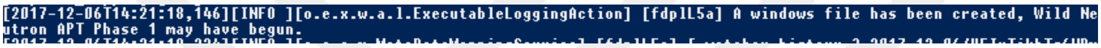
Rule1:



```
[2017-11-24T19:58:17,207][INFO ][o.e.x.w.a.l.ExecutableLoggingAction] [fdplL5a] A registry change has been detected, Duq
u APT Phase 1 may have begun.
```

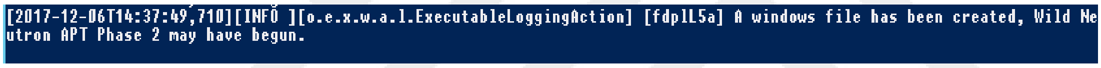
Wild Neutron / Butterfly / Morpho;

Rule1:



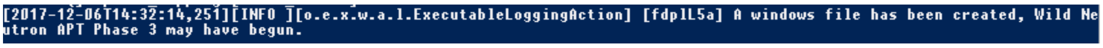
```
[2017-12-06T14:21:18,146][INFO ][o.e.x.w.a.l.ExecutableLoggingAction] [fdplL5a] A windows file has been created, Wild Ne
utron APT Phase 1 may have begun.
```

Rule2:



```
[2017-12-06T14:37:49,710][INFO ][o.e.x.w.a.l.ExecutableLoggingAction] [fdplL5a] A windows file has been created, Wild Ne
utron APT Phase 2 may have begun.
```

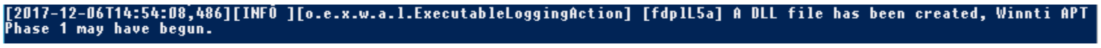
Rule3:



```
[2017-12-06T14:32:14,251][INFO ][o.e.x.w.a.l.ExecutableLoggingAction] [fdplL5a] A windows file has been created, Wild Ne
utron APT Phase 3 may have begun.
```

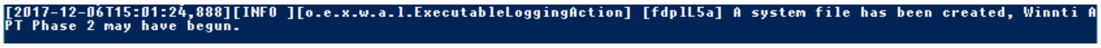
Winnti;

Rule1:



```
[2017-12-06T14:54:08,486][INFO ][o.e.x.w.a.l.ExecutableLoggingAction] [fdplL5a] A DLL file has been created, Winnti APT
Phase 1 may have begun.
```

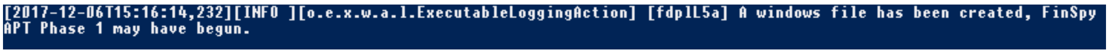
Rule2:



```
[2017-12-06T15:01:24,888][INFO ][o.e.x.w.a.l.ExecutableLoggingAction] [fdplL5a] A system file has been created, Winnti A
PT Phase 2 may have begun.
```

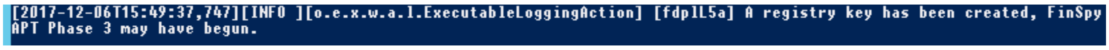
Finspy;

Rule1:



```
[2017-12-06T15:16:14,232][INFO ][o.e.x.w.a.l.ExecutableLoggingAction] [fdplL5a] A windows file has been created, FinSpy
APT Phase 1 may have begun.
```

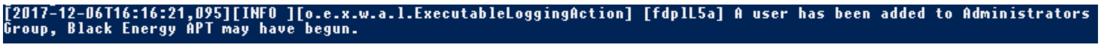
Rule2:



```
[2017-12-06T15:49:37,747][INFO ][o.e.x.w.a.l.ExecutableLoggingAction] [fdplL5a] A registry key has been created, FinSpy
APT Phase 3 may have begun.
```

Black Energy;

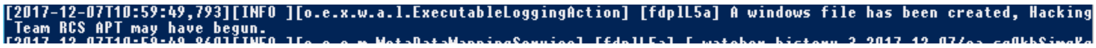
Rule1:



```
[2017-12-06T16:16:21,095][INFO ][o.e.x.w.a.l.ExecutableLoggingAction] [fdplL5a] A user has been added to Administrators
Group, Black Energy APT may have begun.
```

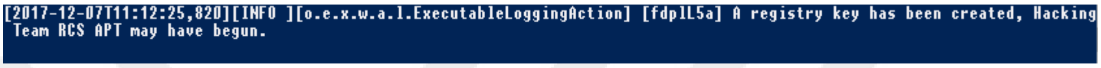
Hacking Team RCS;

Rule1:



```
[2017-12-07T10:59:49,793][INFO ][o.e.x.w.a.l.ExecutableLoggingAction] [fdplL5a] A windows file has been created, Hacking
 Team RCS APT may have begun.
[2017-12-07T10:59:49,860][INFO ][o.e.c.m.MetaDataMappingService] [fdplL5a] [.watcher-history-3-2017.12.07/oa-ca0kbSimgKe
```

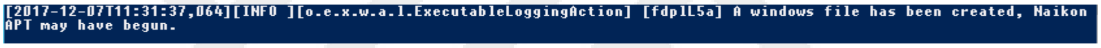
Rule2:



```
[2017-12-07T11:12:25,820][INFO ][o.e.x.w.a.l.ExecutableLoggingAction] [fdplL5a] A registry key has been created, Hacking
 Team RCS APT may have begun.
```

Naikon;

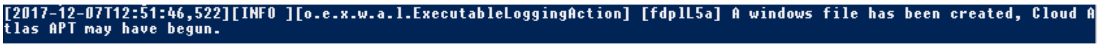
Rule1:



```
[2017-12-07T11:31:37,064][INFO ][o.e.x.w.a.l.ExecutableLoggingAction] [fdplL5a] A windows file has been created, Naikon
APT may have begun.
```

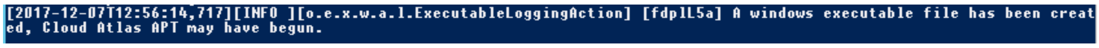
Cloud Atlas / Red October;

Rule1:



```
[2017-12-07T12:51:46,522][INFO ][o.e.x.w.a.l.ExecutableLoggingAction] [fdplL5a] A windows file has been created, Cloud A
tlas APT may have begun.
```

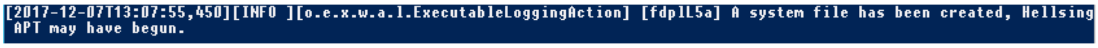
Rule2:



```
[2017-12-07T12:56:14,717][INFO ][o.e.x.w.a.l.ExecutableLoggingAction] [fdplL5a] A windows executable file has been creat
ed, Cloud Atlas APT may have begun.
```

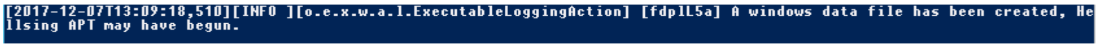
Hellsing;

Rule1:



```
[2017-12-07T13:07:55,450][INFO ][o.e.x.w.a.l.ExecutableLoggingAction] [fdplL5a] A system file has been created, Hellsing
 APT may have begun.
```

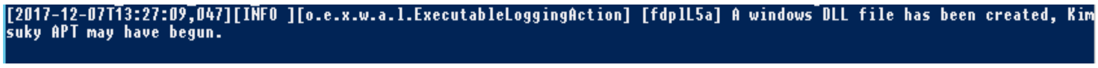
Rule2:



```
[2017-12-07T13:09:18,510][INFO ][o.e.x.w.a.l.ExecutableLoggingAction] [fdplL5a] A windows data file has been created, He
llsing APT may have begun.
```

Kimsuky;

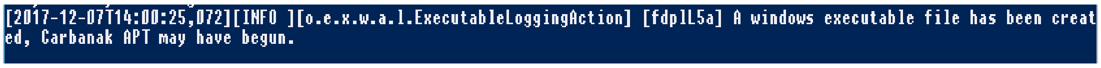
Rule1:



```
[2017-12-07T13:27:09,047][INFO ][o.e.x.w.a.l.ExecutableLoggingAction] [fdplL5a] A windows DLL file has been created, Kim
suky APT may have begun.
```

Carbanak;

Rule1:



```
[2017-12-07T14:00:25,072][INFO ][o.e.x.w.a.l.ExecutableLoggingAction] [fdplL5a] A windows executable file has been creat
ed, Carbanak APT may have begun.
```