Advanced Persistent Threats – Detection and Defense

J. Vukalović, D. Delija
INsig2 Ltd., Buzinska cesta 58, 10010 Zagreb, Croatia
jakob.vukalovic@insig2.eu, damir.delija@insig2.eu

Abstract – **The term "Advanced Persistent Threat" refers to a well-organized, malicious group of people who launch stealthy attacks against computer systems of specific targets, such as governments, companies or military. The attacks themselves are long-lasting, difficult to expose and often use very advanced hacking techniques. Since they are advanced in nature, prolonged and persistent, the organizations behind them have to possess a high level of knowledge, advanced tools and competent personnel to execute them. The attacks are usually preformed in several phases – reconnaissance, preparation, execution, gaining access, information gathering and connection maintenance. In each of the phases attacks can be detected with different probabilities. There are several ways to increase the level of security of an organization in order to counter these incidents. First and foremost, it is necessary to educate users and system administrators on different attack vectors and provide them with knowledge and protection so that the attacks are unsuccessful. Second, implement strict security policies. That includes access control and restrictions (to information or network), protecting information by encrypting it and installing latest security upgrades. Finally, it is possible to use software IDS tools to detect such anomalies (e.g. Snort, OSSEC, Sguil).**

I. INTRODUCTION

One of the main challenges in information security today is a new type of threat that has become a significant concern for various organizations. Organizations now face advanced groups of attackers who are determined to gain access to their resources. They are not just opportunistic criminals. Instead, they are well organized and possess enough resources to launch prolonged and sophisticated attacks. That is how they got the name – *Advanced Persistent Threat* (APT).

Over the last few years, there has been a significant increase in the amount of APT attacks. FireEye, a US based network security company detected 4,192 attacks associated with APT groups during 2013 [1]. That amounts to 11.48 unique daily attacks. FireEye also reports that APT groups caused 17,995 unique malware infections. Command and control servers that APT groups use to coordinate attacks have been found in 206 countries, most of them in the USA, Germany, South Korea and China. During 2013, they have produced over 22 million control messages. Most often, APT groups target organizations in the USA, South Korea and Canada. Most of these organizations belong to education, finance, government or high technology sector [2].

Exploitation of zero-day vulnerabilities in APT attacks is particularly worrying. During 2013, FireEye reported 11 attacks of that type. Most exploited were Java's zero-day vulnerabilities, followed by Internet browsers and Adobe Reader.

APT attacks cause damage to business operations of organizations affected by them. A study [3] conducted by Ponemon Institute shows that victims of APT attack are most likely to experience downtime of information technologies, loss of sensitive information, and disruption of business processes. Even though all these events cause significant losses, the worst and most expensive consequence is damage to brand and reputation. Ponemon Institute's research shows that, on average, damages to organization's reputation caused by APT attacks amount to $9.4 million.

APT attacks often remain undetected for a long period of time. Some of them, however, gained media recognition. For example, operation Aurora that resulted in loss of Google's intellectual property in 2009, or Stuxnet, a worm discovered in 2010 that infected uranium enrichment plants in Iran.

APTs bring changes in attack methodology. New attack methodologies mandate that organizations change their approach to information security. While there is no such thing as a completely secure system, it is possible to establish countermeasures that will greatly reduce the risk of falling victim to APT attacks.

This paper explains the nature of APTs and provides an overview of appropriate methods of countering attacks. The second chapter gives an overview of APTs, a definition and description of the term, their lifecycle, mode of operation and tools they use to exploit weaknesses in information systems. The third chapter lists some characteristic detection points for APT attacks, particularly outgoing traffic. It also contains a summary of tools that can be used for purposes of detection. The fourth chapter lists basic countermeasures in order to establish proactive defense in an organization.

II. ADVANCED PERSISTENT THREAT

A. What are APTs?

The term *Advanced Persistent Threat* refers to a well-coordinated group of people (typically controlled by an organized entity such as a government, terrorist group, corporate entity or other) with malicious intent that targets

a specific organization, government or company. APTs perform persistent prolonged attacks until they gain access to organization's computer systems, sensitive data or other resources. Individual hackers and opportunistic criminals are not APTs. They either do not possess the resources or abilities to execute complex and prolonged attacks, are rarely well organized, or they are not targeted. Traditional hackers attack for financial gain, because of social and economic issues, or just for fun and to gain recognition. APTs, however, have a very specific target. They are after the target's intellectual property, and they do not just try several methods to get access and then stop trying if they are unsuccessful, but attack continuously. If they are unsuccessful on the first few attempts, they will keep trying until they find a way to compromise the organization.

A description of an advanced persistent threat can be inferred from its name. Traditional attacks lack one or more of these characteristics.

Advanced – the attacks are coordinated by a group of people that possess advanced resources and knowledge, and are often well funded. The attacks themselves do not necessarily have to be highly sophisticated for the breach to be successful. Attackers often use phishing and widely available tools for malware creation [4] [5]. However, if needed, they can also develop their own tools to target specific vulnerabilities (such as zero-day exploits), and use multiple types of attacks in order to breach the target. Therefore, the term *advanced* refers to attackers' capabilities and knowledge which makes it different from traditional attacks.

Persistent – the attackers persist, they repeatedly try to compromise the victim's systems until they gain access to their resources. Then, the attacker maintains access. They create backdoors and, when one connection is severed, another one can be opened and used to continue extracting sensitive information. If the attacker loses access to the victim's system, he will repeat the whole process until he reestablishes access.

Threat – a threat is a possible source of harm or danger. Since APTs possess both the intention and the means to harm their targets, and are not just automated pieces of software, they present a threat.

APTs have a very specific target, and their main objective is to maintain **prolonged access to the target's intellectual property**, sensitive information, or otherwise interesting data that is useful to the attacker. To achieve that, the attack needs to remain concealed.

Even though APT most often attacks target computer systems, attackers can also use other, more traditional and simpler attack methods, such as social engineering or intercepting phone calls. APTs also perform attacks in order to acquire data that may help them execute more attacks in the future.

B. *Life Cycle of APT Attacks*

APT attacks are complex and consist of several stages. Each step of an attack is carefully adapted to attack the specific victim's vulnerabilities. Although these steps are not a rule, but a general scheme of an APT attack, their existence is vital in maintaining stealthiness and prolonged access to sensitive information, and it is expected in most attacks (**Error! Reference source not found.**).

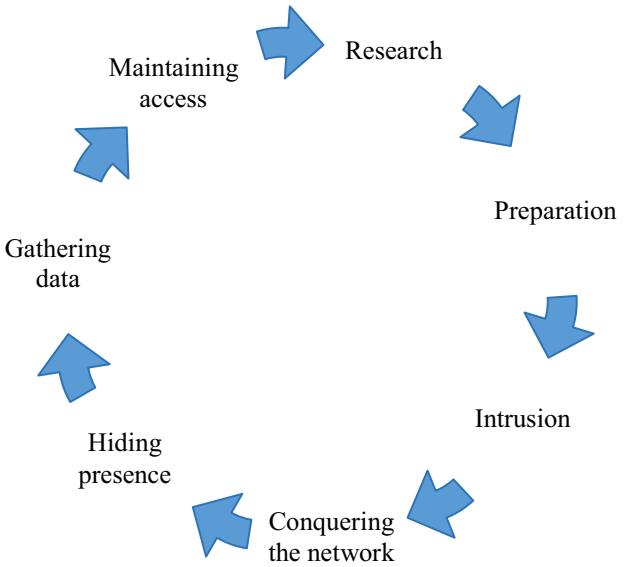

Figure 1 Life cycle of an APT attack

1. **Research.** The attackers gather information about the victim, trying to find weak points to exploit. The information that attackers search for is often publicly available. The attackers research employees' social network profiles and personal information, organization's website, technologies, communications, hierarchy, and premises. APTs differ from traditional attackers at this point. Since traditional attackers (individual hackers, *script kiddies*, inadequately organized hacking groups) do not target a specific organization, or at least do not do so persistently, over a prolonged period of time, they do not care if some of their attacks are unsuccessful, because they know there will be other, successful cases. APTs target a specific organization, therefore they must conduct extensive research if they want to find a vulnerability that can be exploited. Chances of a successful attack increase with the amount of information researched. The attackers will also search for individuals to be targeted (e.g. with phishing messages). At this phase, the attack is almost impossible to detect because it does not involve interaction with the organization's systems. Once the target has been identified, attacker moves on to the next phase.
2. **Preparation.** Using information they acquired in the first step, attackers prepare the attack. In this step they perform active extraction of specific information about the victim. They also prepare and test methods and tools that will be used to exploit found vulnerabilities. Activities in this step include scanning the network, ports, and running services, finding or creating customized malware that will exploit the victim's vulnerabilities, and planning malware

deployment (e.g. phishing messages, removable media). During this stage, APTs also have to prepare the infrastructure that will be used to manage and control attack flow. This includes taking control of servers to use as command and control centers, modifying DNS entries, creating fake domains and email accounts etc. At this phase, the probability of detecting the attack is very low. Once the attack methods and command-and-control infrastructure have been set up, the attacker proceeds to the next step.

3. **Intrusion.** Attackers launch first attacks. Most often, it is done using phishing email messages. These emails contain a message that will convince a gullible employee to open a document or a URL that contains malicious code. The attackers can impersonate a coworker, business partner, or any other person that the employee trusts. Assuming that the attacker gathered enough information in previous steps, and since people are typically the weakest link in the security chain, this approach is probably the easiest way to compromise an organization, and very likely to succeed. Other possible methods are exploiting vulnerabilities in organization's systems, including zero-day vulnerabilities, and spreading malware infections using removable media. Smartphones and tablet computers also present a security risk in this context. Since employees use their personal devices to connect to their workplace network, these devices can be used to spread malware in the organization's network. Absence of security policies and protocols increases the probability of success for this stage of attack. After the attack has been launched, the attacker monitors command and control infrastructure waiting for a sign of successful breach.

4. **Conquering the network.** If the attack has been successful, that means the attackers have gained access to one or more computers in the organization's network. If possible, they will try to obtain administrative (*root*) privileges on victims' systems. After initial breach, they install additional malware and create backdoors (e.g. remote administration tools – RAT) to act as a convenient way to remotely access and control the system. They also try to spread through the network identifying other machines susceptible to compromise, and trying to find valuable data that will be extracted. In this phase the attacker actively controls computers in the network, therefore the intrusion is easiest to detect. Some APTs also execute fake and easily detectable attacks against the organization in order to keep system administrators busy while the real attack takes place quietly.

5. **Hiding presence.** One of the main goals of the attack is to maintain prolonged access to organization's network and, consequently, their data. In order to avoid detection, APTs need to conceal their presence in the system. For traditional attackers this component is not crucial for the same reason it is not crucial for them to research their potential victims – even if they lose access to some of the machines they have infected, they can always find other vulnerable machines. For them, it is a numbers game. On the other hand, APTs have a specific target, which makes it harder to reestablish connection every time they are detected. Because of that, APTs install rootkits, modify event and audit log entries, periodically enter a sleeping state for some time, and delete traces of their own files on the system.

6. **Gathering data.** While exploring the organization's network, attacker searches for data of interest. When found, the data is gathered and, most often, encrypted to conceal its true identity on the way out of the network. Then, the data is masked to resemble legal traffic and slowly extracted from the organization's network. Using the command and control infrastructure that has been set up, it is then routed back to the attacker.

7. **Maintaining access.** In order to extract the maximum possible amount of data from the victim without getting caught, the attacker needs to maintain prolonged access to the victim's network. The attacker needs to make sure the backdoors are working as expected, the infected systems are accessible, and that command and control infrastructure is working, so he periodically checks their status. He could also update existing or install new malware in order to exploit other weaknesses or improve stealthiness, reconfigure the malware, and expand or reconfigure the command and control infrastructure. If, despite everything, the communication is severed, the attacker has to persist and go back to step 1.

C. Attack Toolbox

Attackers employ a variety of tools and methods when trying to access the organization's systems. One of most used techniques is **phishing**. It involves sending a specifically crafted message with an embedded malicious document or link to employees of an organization via email or social networks. In case of **spear phishing**, the attackers send such messages to specific people within an organization, after obtaining their personal information to increase the probability of success. Attackers also spread malware using **infected removable media**, or embedding it into **installation files** of popular programs. **Zero-day** vulnerabilities in commonly used programs or operating systems are targeted as well.

In the second phase, and while spreading through the network, attackers use **network scanning and enumeration tools** to discover computers and other devices connected to the network, their operating systems, open ports, running services and possible vulnerabilities.

When the system has been infiltrated, the attackers create **backdoors**. Backdoors enable the attacker to evade normal security controls and get remote access to the

system. They are created as modifications to the operating system, or they can be installed as a service. Attackers use **rootkits** to hide the presence of unwanted programs in the system. They also use **malware generators** to quickly and easily create customized malware.

In order to facilitate remote access to the machines, the attackers use **remote administration tools** (RATs). While such tools are often used in legal activities, they can also give the attacker complete control of infected systems.

APTs utilize **command and control infrastructure** to communicate with the infected machines, pass control messages, and extract data. Command and control servers are most typically infected servers under attacker's control. The communication is **encrypted** to make it harder to detect and block.

D. Notable Cases

1) Operation Aurora [6]

Operation Aurora was a sequence of multiple hacking attacks in 2009 that targeted Google, Adobe Systems, Rackspace, Juniper Networks and probably many others. The attacks originated from China, and exploited several zero-day vulnerabilities in Internet Explorer. Google's intellectual property was stolen. As a result, Google left the Chinese market.

2) Stuxnet [7]

Stuxnet is a worm, discovered in 2010, that infected industrial control systems, mostly in Iran. The worm propagated through infected USB thumb drives, exploited several zero-day vulnerabilities in Windows OS, and then corrupted PLC control software. The worm destroyed nuclear centrifuges in Iran's uranium enrichment facilities. It is speculated that creation of Stuxnet was a joint effort between Israel and the USA.

3) Operation Shady RAT [2]

A sequence of attacks that started in 2006 and continue to this day. McAfee, a cyber-security company, claims that the attacks targeted more than 70 organizations, most of them in the USA. The attacks utilize RATs and encrypted HTML comments that are used to pass commands to RATs. The attack most likely originates from China.

4) GhostNET [8]

A cyber espionage operation, discovered in 2009, that targets computer systems in more than 100 countries. The attackers use phishing and remote administration tools. The attacks originate from China, and target governments, ministries, and embassies. China's government denies involvement.

5) Darkhotel [9]

An active APT that targets guests using wireless networks in high-end hotels. The APT misuses hotel's check-in data and targets very specific individuals. It offers them software updates for frequently used packages, bundled with trojans and key loggers. It also possess some unusual features. The programs were signed with stolen certificates. Most of the attacks occurred in Japan.

6) RSA [10]

In 2011 it was reported that RSA Security was a victim of an APT attack. The attackers used phishing messages which contained an Excel document which exploited a vulnerability in Adobe Flash Player. The attackers used a RAT tool to control the infected computers and access data on company's servers. This incident caused $66.3 million damage. It is probable that the attackers stole information about RSA SecurID token seeds.

III. DETECTION

Even in the best of circumstances, systems get compromised and computers become infected. Attack vectors are numerous, and covering each option is almost always impossible. If the breach happens, there are several options that can help detect and remove the threat. With APTs, well-timed detection is very important.

Traditional methods of detection rely on examining the signature of unknown files to determine if they correspond to known malware, examining protocols or blocking specific network ports, and intrusion prevention systems (IPS) that can detect a very small subset of threats. APTs, however, rely on masking and encrypting network traffic, port hopping, newly created malware that does not exist in malware databases, malware with mutating code etc. For that reason traditional methods of detection are ineffective. Since malware has developed from infecting individual machines into organized networks of *zombies*, organizations need to implement not just endpoint security mechanisms, but also network security mechanisms.

Since one of the main activities of APTs is to extract data from an organization, analyzing data that leaves the network can help in discovering the command and control messages of an attack. The following characteristics of outgoing traffic can be used to discover malicious activities and should be analyzed:

- **Amount of data and packet quantity.** When normal users establish connections, they typically send out small amounts of data and receive large amounts of data. Since APTs extract data *from* the organization, this is one of key areas to monitor. Infected machines may generate large amounts of outgoing data that looks unusual (encrypted or masked). However, when analyzing outbound data, it is necessary to consider organization's common data flow in normal circumstances. It facilitates adjusting the monitoring engine precisely and decreasing the number of false positives it might produce.
- **Connection duration.** Normal connections are rarely established for longer periods of time. APTs establish connections that last longer when extracting larger amounts of data from an organization. Again, when monitoring connection duration it is necessary to consider types and duration of connections that normal business activities use.
- **Transmission period.** If the machines generate a certain type of outgoing traffic consistently in regular periods of time (a pattern which does not

correspond to normal usage), it could indicate presence of malware that regularly extracts data from the network.

- **Malicious sites.** Network monitoring system should keep a list of sites that have hosted malicious content. Existence of machines that communicate with such sites could indicate the existence of an attack. It will not prevent communication with newly established malware servers, however such communication will stand out from usual and can be detected by other means.
- **Internet Relay Chat (IRC) communication.** Botnets often use IRC to pass control messages between command and control servers and infected machines.
- **Destination IP addresses.** It is possible to determine the country in which the destination IP address resides. If there are outgoing IP packets with destination addresses in countries which have no association with the organization, it is possible that these connections were established by malware.
- **New domains.** In order to create command and control infrastructure, APTs often register new domain names and use dynamic DNS to route traffic between multiple infected machines which makes such traffic hard to track. Frequent communication with a previously unknown new domain could indicate presence of malware.
- **DNS cache.** Normal users typically do not use IP addresses when establishing network connections, they use URLs (uniform resource locators). When the user types a URL or clicks on a hyperlink, their DNS resolver must find the matching IP address for the URL. The domain name and its IP address are then stored in the DNS cache for some time. If outgoing connections do not have a corresponding entry in the DNS cache (which means someone established a pure IP connection), that could indicate malware infection.

Detection of network security breaches can be done using various IDS and SIEM (Security Information and Event Management) tools. It is important to note that these tools do not exempt users from using traditional endpoint security tools, such as personal firewalls and antivirus programs.

Various tools exist which can automate network monitoring tasks, correlate events and help detect breaches in network security:

- **OSSEC [11].** OSSEC is an open source host based intrusion detection system which detects intrusions by examining logs generated by various applications. OSSEC has two work modes, *local* (monitoring only one system) and *agent/server* (collecting and monitoring logs from multiple sources across the network). OSSEC can read and analyze log files of over 40 different programs and devices. It has separate components for collecting, reading, analyzing logs, and sending email alerts. It is also possible to install OSSEC agents on network devices. These agents collect logs on devices and send them to the central server for analysis using UDP. When logs are received, their field values are extracted, crucial information contained within logs is identified, and checked against pre-set or manually created rules. If needed, it sends email alerts. OSSEC works on most operating systems.
- **Snort [12].** Snort is an open source network intrusion detection and prevention tool. It is capable of performing packet analysis and logging on the network. Snort works in one of three modes: sniffer mode, packet logger mode, or network intrusion detection mode. The first two modes are simpler modes used for displaying or storing network packets. The last mode is used for traffic analysis according to a predefined set of rules, and generating alerts. Snort consists of several components which capture packets, decode and preprocess information in packets, analyze extracted information, find patterns within this information, and perform logging, alerting and outputting data. It is also possible to filter generated events in order to reduce false positives (e.g. by rate, number of events, or completely hiding events).
- **Sguil.** Sguil is a set of network monitoring tools that combines an IDS (Snort), network connection security profiling (SANCP), TCP connection analyzer (Tcpflow), stores results from multiple tools in a database (MySQL), and provides a GUI. When deployed, a system consists of a Sguil server and several Sguil sensors which monitor the network and send collected data back to the server. Sguil clients receive and display data from the server. Sguil improves common IDS systems by integrating different data sources and analysis solutions, thereby improving detection rate and reducing workload.
- **Splunk.** Splunk is a tool for processing machine-generated big data [13]. It provides searching, analyzing, indexing, correlating, visualizing and reporting capabilities. Splunk is used in various information technology domains, e.g. web analytics, internet of things, operational analysis, and security [14]. When used for security monitoring, Splunk can collect, index and analyze data from logs, firewalls, IDSs, perform statistical analysis of events within the network and thereby detect threats that would otherwise escape rule-based systems.

IV. DEFENSE

It is possible to undertake actions that can reduce the probability of system security breach. Of course, these efforts should be focused on critical areas – those which

present a high risk of security breach or high cost of repairing the damage. For that reason it is important for organizations to recognize their critical data and potential weaknesses which may present an attack vector.

In order to stop attackers from breaching the system, and discover those who have succeeded, both prevention and detection of attacks is important.

Some basic prevention measures are:

- **User education.** People are often the weakest link in organization's security. Due to the lack of knowledge and understanding of the threat employees become a critical point that attackers exploit. Educating users can greatly improve organization's level of security. It is necessary to educate employees about good password practices, social engineering (particularly phishing messages), malware, and other dangers.
- **Implementing access and usage policies.** Organizations should implement strict access policies and permissions for wired and wireless networks, files and other data. Access should be granted to users at the lowest necessary permission level. When authenticating users, TFA (Two-factor Authentication) should be used and strong passwords should be enforced. Detailed authentication logs should be kept.
- **Controlling external media.** All external storage media (USB drives, optical disks etc.) should be controlled in order to prevent spreading malware infections or losing valuable data.
- **Protecting valuable data.** Valuable data should be encrypted, with limited access. The most critical data should be kept on machines without network connection.
- **Managing endpoint security.** It is important that all operating systems and other programs used by organization's employees have all the latest security updates installed and enabled. It is also important that they have personal firewalls and antivirus programs installed and updated. When detecting or preventing security incidents, endpoint security must not be disregarded, but not exclusively relied upon.
- **Implementing NAC (Network Access Control).** Network Access Control is a method of enforcing network access policies for client devices. Non-compliant devices can be automatically repaired or upgraded when they are first connected. Network access is granted only to devices which satisfy certain security requirements such as security patches or antivirus protection. Other devices are given limited access until they are updated. NAC can also be used to control access based on assigned roles.
- **Blocking high risk applications.** Organizations should block usage of known high risk applications which could be used to spread malware or facilitate data leakage, such as P2P (peer-to-peer) programs, encrypted tunneling applications, and proxies.
- **Blocking known malware servers.** Organizations should keep a list of known malware sites, block access to them, and alert system administrators of any requests to these sites.
- **Analyzing security breaches.** Finally, if an attack does penetrate organization's security, it is necessary to thoroughly analyze how it happened, which parts of the system were compromised, and what data was lost. That way organizations can get a complete picture of the incident and protect themselves from future attacks.

V. CONCLUSION

APTs have become a significant concern for organizations from various domains. This trend is not showing signs of slowdown. Due to their stealthiness and focus on data, APTs present a growing danger that is very hard to prevent, detect and defend against. In the recent years, we have witnessed numerous cases where APTs have caused significant damage to various organizations, not only in form of data theft, but immediate physical damage.

APTs have an advanced approach to attacking organizations, they have the resources and knowledge, they do not stop give up when they are unsuccessful, they conceal their presence, and they target organization's valuable resources. Because of that, new security approaches are needed. Organizations cannot rely on traditional firewalls and malware detection. They need to employ various advanced intrusion detection tools and, based on their activities, develop new methods of detecting anomalies in a specific network, and correlate them in order to discover security breaches.

Even though there is no guarantee that any network is completely secured, organizations can implement tools and security policies that can greatly reduce the risk of an attack. However, doing that requires knowledge, resources and time.

REFERENCES

[1] FireEye Inc., "FireEye Advanced Threat Report: 2013", 2013

[2] D. Alperovich, "Revealed: Operation Shady RAT", 2011

[3] Ponemon Institute, "The State of Advanced Persistent Threats", 2013

[4] FireEye Inc., "Spear Phishing Attacks – Why They are Successful and How to Stop Them", 2014

[5] FireEye Inc., "Poison Ivy: Assessing Damage and Extracting Intelligence", 2014

[6] R. Varma, "McAfee Labs: Combating Aurora", https://kc.mcafee.com/resources/sites/MCAFEE/content/live/CORP_KNOWLEDGEBASE/67000/KB67957/en_US/Combating%20Threats%20-%20Operation%20Aurora.pdf

[7] A. Matrosov, E. Rodionov, D. Harley, J. Malcho, "Stuxnet Under the Microscope", http://www.eset.com/us/resources/white-papers/Stuxnet_Under_the_Microscope.pdf

[8] The SecDev Group Information Warfare Monitor, “Tracking GhostNet: Investigating a Cyber Espionage Network”, 2009

[9] Kaspersky Lab Global Research and Analysis Team, “The Darkhotel APT: A Story of Unusual Hospitality”, 2014

[10] RSA FraudAction Research Labs, “Anatomy of an Attack”, https://blogs.rsa.com/anatomy-of-an-attack/, 2011

[11] D. B. Cid, “Log Analysis Using OSSEC”, 2007

[12] M. Roesch, C. Green, Sourcefire Inc., Cisco Systems Inc., “SNORT User’s Manual: The Snort Project”, http://manual.snort.org/, 2014

[13] Splunk Inc., “Splunk for Security: Supporting a Big Data Approach for Security Intelligence”, http://www.splunk.com/web_assets/pdfs/secure/Splunk_for_Security.pdf, 2014

[14] Splunk Inc., “Advanced Threat Detection and Response: Using Splunk Software to Defend Against Advanced Threats”, http://www.splunk.com/web_assets/pdfs/secure/Splunk_for_APT_Tech_Brief.pdf, 2014