Clandestine Cell Based Honeypot Networks

Cagatay Yucel, Ahmet Koltuksuz, Huseyin Yagci
Department of Computer Engineering, Yaşar University, Izmir, Turkey
cagatay.yucel@yasar.edu.tr
ahmet.koltuksuz@yasar.edu.tr
huseyin.yagci@stu.yasar.edu.tr

Abstract: A Clandestine Cell is a type of an intelligence organization where a cell only knows the immediate superior and the associated members of itself. This kind of organizational structure is used by intelligence agencies throughout the world to provide security against a breach, thus ensuring the safety of the members. This well-known intelligence organization is applied to solve an advanced cyber security issue. A relatively new kind of a cyber threat known as an Advanced Persistent Threat (APTs) has been around for some time now, Stuxnet being the very first identified.

There are several points to consider when identifying the characteristics of an APT, such as the aim, its interactions with Internet, way of collecting information, operations they do disrupt and concealment mechanisms utilized. An important aspect is whether it is statistically analyzable or dynamically identifiable, that its communication patterns need to be inspected to identify the characteristics. The traces of an APT might be identified this way.

In this research, a honeypot network with a communication policy based on a clandestine cell is introduced. Each honeypot only knows a hub. And a hub only knows the main malware analysis server. By utilizing this approach, the communications are hidden from possible attackers without compromising the main server. In each honeypot server, dead-ends are created and implemented in the honeypot servers. Advantages and ramifications are discussed regarding the types of malware. It is aimed to create yet another taxonomy of malware regarding the network activities as they are being trapped by our introduced honeypot network. A clandestine cell format is one of its kind within organizations. This is the very first time that such kind of format is being applied to honeypot design for APT hunting. This is the paper in which an intelligence organizational structure meets with a network architecture in order to solve a very hard to crack cyber security problem. The idea itself is a new and untried one.

Keywords: Clandestine Cell, Honeypots, Advanced Persistent Threats, Clandestine Network Organizations

1. Introduction

Malicious activities of computer systems started almost at the same time with the invention of *Von Neumann* computer architecture. In this computational model, John Von Neumann foresaw a program that is able to self-reproduce on the memory, which is considered the first computer virus (Neumann, 1969). On 1988, a harmful computer program that was able to self-reproduce on networks named *Morris Worm* effecting a large number of computers have been unleashed (Eisenberg et al., 1989). From then on, advances have been made on both sides of this war: the security professionals and the attackers.

A relatively new kind of cyber threat, Advanced Persistent Threats (APTs) has been around for almost 8 years now (Langner, 2011). Mainly targeting the industrial control systems, political institutions and critical infrastructures, this type of threats are way ahead of conventional defense mechanisms. They are advanced as in they use vulnerabilities which have not been identified and combining social engineering techniques with computer intrusion technologies. They stay under the radar until they reach their targets (Saud & Islam, 2015).

These advanced threats require advance proactive defense techniques to cope with them. One of the recent solutions of such is Honeypots. Honeypots are information systems used for exploiting the attacker by luring them with decoys. A honeypot is expected to be probed, attacked and exploited (Spitzner, 2003). A honeypot network or a honeynet is a collection of honeypots for large networks, collecting information about most recently developed attacks as well as the attackers. One of the biggest challenges whilst collecting information is that the network should not be compromised.

In this research, a well-known intelligence organization, Clandestine Cell Network is implemented on honeypot networks in order to provide the maximum secrecy of the honeypot network when a cell or a single honeypot is compromised. This paper is organized as follows: Section 2 presents the characteristics of APTs, Section 3 describes and defines honeypots. In Section 4, proposed model is explained with the organizational charts and Section 5 addresses the advantages and ramifications of such system and concludes the paper.

2. Advanced Persistent Threats (APTs)

An advanced persistent threat is an adversary that utilizes advanced levels of expertise, significant resources and objective specific tools to execute its objectives by series of attacks. These attacks may include cyber, physical and deceptive techniques. These objectives typically include gaining access to the targeted infrastructure for the aims of gathering, disrupting or modifying the critical aspects of a mission, program, or organization or infiltrating the infrastructure to accomplish its objectives in the future.

An advanced persistent threat must have the following characteristics:

- It should try to achieve its objectives repeatedly over an extended period of time,
- It should overcome the defending mechanisms,
- It should accomplish the necessary infiltration and maintain a connection with the Command and Control.

2.1 Characteristics of Known APTs

Stuxnet

Stuxnet is the first known megahit APT attack on the Industrial Control Systems (ICSs). The APT designed and developed for disrupting Iran's nuclear enrichment program. The APT directly affected programmable logic controllers (PLCs) and caused overloading on the centrifuge that is used in the enrichment operation. There were many suspicious dead-end IP addresses to hide the source code of Stuxnet. Waves of attacks started from 2009 and continued to 2010 (Falliere, Murchu, & Chien, 2011).

Operation Aurora

Operation Aurora is an attack which shows APT properties. Victims are infected with social engineering techniques and a malware known as **Trojan.Hydraq** is downloaded via a zero-day exploit on the web browser Microsoft Internet Explorer. Finally, the malware created a backdoor on the infected computer and gave access to the sensitive data. Operation Aurora was publicly discovered in 2010 (Varma, 2010).

GhostNet

GhostNet is an APT attack that involves a malicious network and a malware. The malware forces infected nodes to send an email with an attached Trojan named **"gh0st RAT"** and exploitation code to the victims on the network as a crafted email. Moreover, "gh0st RAT" gains root privileges on the host computer. Starting from 2007, the incident had effected more than 1,300 computers in 103 countries. There were also military, diplomatic and political networks known to be infected (Information Warfare Monitor, 2009).

Taidoor

Taidoor is a Trojan that has been used since 2008. Taidoor's victims are government agencies, corporate entities, and think tanks, especially those with interests in Taiwan and US (Doherty & Krysiuk, 2011). Taidoor has been spreading itself as an email attachment and once the email is opened the backdoor is injected into the memory as an operating system service and connection is established with the Command and Control server of the Trojan.

IXESHE

IXESHE is an APT that is notable for targeting East Asian governments, electronics manufacturers, and a telecommunications company in 2011. Adobe Acrobat Reader, and Flash Player, Microsoft Excel exploits; CVE-2009-43243, CVE-2009-09274, CVE-2011-06095, CVE-2011-06116, CVE-2009- 43247, CVE-2011-06098, CVE-2009-3129 are used after infection (Sancho, Torre, Bakuei, Villeneuve, & McArdle, 2012).

Poison Ivy (PIVY), "Nitro"

Nitro is a cyber-incident that is targeted to the chemical industry and government agencies in 2011. Poison Ivy is a totally free windows based remote access tool. The tool and Internet Explorer based zero day exploit are used in this incident. Adversaries generate code for maintenance and networking with using PIVY tool and the code is

injected into the running instance of an Internet Explorer process. Based on adversaries' configuration, a remote shell is activated over TCP ports (Fireeye, 2014).

Duqu

Duqu is announced as the latest discovered version of Stuxnet. The reason that this relation between Duqu and Stuxnet has been made is due to Duqu's aim to collect valuable data about industrial infrastructure. This incident doesn't have any kind of remote access Trojan (RAT) to control or effect the industrial system. It focuses on stealing valuable data. The malware uses Microsoft Word files which contains a zero day (CVE-2011-3402) on targets (Symantec, 2011).

Flame

Flame is an APT mainly designed for espionage activities. It has targeted Microsoft Windows OS computers and been stealing critical information by utilizing key logging, capturing screen shots and switching microphone and camera on to record some valuable information. It also, searches for available neighbor computer and turns the first infected computer into a proxy server for Windows Update [6]. Adversaries used the same zero day vulnerabilities as Stuxnet which are Print Spooler (MS10-061) and Windows Shell (MS10-046) (Bencsáth, Pék, Buttyán, & Félegyházi, 2012).

Red October

Red October is a wide scaled cyber espionage operation that has been effective in more than 39 countries. It is discovered in 2012 by Kaspersky Labs. Focused targets are critical infrastructures such as governmental, military, energy information systems. The aim of this incident is gathering assets. Spear phishing techniques are used alongside with the malware embedded in email attachments. Encrypted servers are used in C&C stage (Chavez, Kranich, & Casella, 2015).

MiniDuke

MiniDuke is an information stealer type of malware that has effected more than 23 countries. MiniDuke uses malicious crafted emails for spreading and it has a unique communication mechanism with the Command and Control servers via encrypted URL on twitter. If twitter accounts are blocked and unreachable, it uses Google Search to reach its C&C servers (Virvilis, Gritzalis, & Apostolopoulos, 2013).

In Table 1 below, aforementioned APTs are summarized. Zero day exploits are given in the numbering form of *Common Vulnerabilities and Exposures* dictionary ("Common Vulnerabilities and Exposures," 1999).

Table 1. APT Characteristics Table for Designing the Honeypot Network

Name	Time	Port/s	Protocol	Zero-Day Exploits	Target System(Attack Vectors)	Functionality
GhostNet	2007	80, 8000, 4501,	HTTP	CVE-2006-2492, CVE-2006-2492	Government, Energy industry, Military, Universities	Taking full control
Taidoor	2008	80	HTTP	CVE-2009-1129, CVE-2011-0611, CVE-2011-2100	Multinational big companies, Think Tank,	Information gathering
IXESHE	2009	80, 443, 8080	HTTP, HTTPS	CVE-2009-4324, CVE-2009-0927, CVE-2011-0609, CVE-2011-0611	Multinational	information stealing, Remote code execution
Poison Ivy "Nitro"	2011	3460, 80, 443, 8080, 1863, 8000	HTTP, HTTPS,	CVE-2012-0158, CVE-2009-4324, CVE-2013-0422, CVE-2013-1347, CVE-2011-3544	Chemical industry, Government agencies	information stealing, Remote code execution
Duqu	2011	80, 443	HTTP, TCP	CVE-2011-3402	Multinational	information stealing
Flame	2012	80, 443, 22	HTTP, HTTPS, SSH	MS10-061, MS10-046	Middle East	information stealing, Remote code execution
Red October	2012	40080	TCP	CVE-2009-3129, CVE-2010-3333, CVE-2012-0158, CVE-2011-3544	Government, Energy industry, Military, Universities	High level cyber espionage, information stealing
MiniDuke	2013	443, 80, 8080	HTTP, HTTPS	APSB13-08, CVE-2013-0643, CVE-2013-0648,	Multinational	information stealing
Stuxnet	2010	80	HTTP	MS10-061, MS08-067, MS10-062, MS10-046, CVE-2010-2568	Industrial control systems and (PLC)	Disruption
Operation Aurora	2010	80	HTTP	CVE-2010-0249	Multinational big companies	information stealing

3. Honeypots

The term "*honeypot*" or "*honeytrap*" comes from human intelligence (HUMINT) terminology and refers to a strategy where an attractive male or female agent is used to seduce individuals and exploit this sexual relationship to force individuals to cooperate with them. History shows that even a well-trained, most clever and patriotic person can fall into this trap if set properly. The honeypot driven espionage operations have been heavily referenced in intelligence literature (Digby Diehl & Clarridge, 1997; Earley, 1997; Wright & Greengrass, 1988).

A honeypot in computer terminology is a decoy based information system designed to lure the attackers into its traps and try to log information about malwares and attackers. The concept of the honeypots and deception in information systems is first introduced by Fred Cohen's Deception Toolkit (Cohen, 1998). The attackers often search for the vulnerabilities in an information system and attack the weakest points, therefore a vulnerable system to attract the attackers shall be used as a honeypot. After an attack is conducted, the aim is to detect an attack, identify the vulnerability and find out the attacker and Command and Control (C&C) center of the attack.

Intrusion Detection Systems (IDS) is a conventional tool that monitors the network traffic and searches for a potential malicious activity. A major shortcoming of IDS is these systems are equipped with a pattern database of known attacks and a pattern matching is done by deep package inspection techniques. However, this operation is quite resource consuming and is open to Denial of Service (DoS) attacks. Another ramification of an IDS is they are highly detectable and therefore when an attacker knows that the traffic is monitored and inspected, IDS can be forced to blind its sensors by false negatives or network flooding techniques. However, a honeypot system acts like any other server on the network with an unused address. Therefore if there is a malicious attempt or a breach made on the honeypot server, there is a very high probability of that attempt is an actual malicious activity (Fanfara, Dufala, & Radušovský, 2013).

Honeypots can be installed in multiple numbers to a network which forms a Honeynet. A Honeynet can be used for wider networks where one honeypot would not suffice (Jasek, Kolarik, & Vymola, 2014). In this case, the communication of honeypots become critical: it must be accomplished in a stealthy way in order to hide the existence of these fake systems and it is as important as is the information of attacks must be disseminated as quickly as possible to alert the overall system which is being protected. This research proposes a communication protocol inspired by intelligence agencies described in the next section.

A honeypot should interact with the attacker in order to trick the attacker to believe that it is a legitimate system. Regarding the level of interaction honeypots can be divided in two:

- *Low-interaction honeypots*

This type of honeypots only emulate a few steps and replies of the vulnerable network protocol and network stack that is being imitated. It is easy to deploy and use. However it is easy for an attacker to detect one.

- *High-interaction honeypots*

High-interaction honeypots have a vulnerable operating system and network services fully implemented in it, generally have reduced operating system kernels. It is the most complex type having the ability of collecting all malicious activity with the possibility of takeover by an attacker as a disadvantage. They are generally monitored by an external IDS for such possibility.

A significant advantage of utilizing these systems is the possibility to detect new types of attacks and vulnerabilities that are used by attackers. Honeypots are attracting computer security researchers as they lure the attackers as well, many interesting research have been done on honeypots. A hybrid honeypot system is proposed in (Fanfara et al., 2013) where a low interaction honeypot is combined with a high interaction one in cooperation with an IDS. Hardware abstraction methodology is proposed in (Zhang, He, & Kim, 2015) and the benefits of a low cost yet highly functional system are added to a Honeynet framework. Another APT detection methodology similar to this research is presented in (Jasek et al., 2014), however this research differentiates from others by importing HUMINT Clandestine Network strategy in it. The advantages and ramifications of

such systems are discussed in Section 5. Significant work have been done on analyzing the collected data by honeypots in (Ghourabi, Abbes, & Bouhoula, 2014; Prathapani, Santhanam, & Agrawal, 2013; Zhan, Xu, & Xu, 2013). A design for installing honeypots on industrial control systems via proxy servers is discussed in the paper of (Winn, Rice, Dunlap, Lopez, & Mullins, 2015) and on small scale organizations using open source tools is discussed in the paper of (Singh, Sharma, & Singh, 2013).

4. Proposed Honeypot Network

A Clandestine Cell is a type of an intelligence organization where a cell only knows the immediate superior and the associated members of itself. This kind of organizational structure is used by intelligence agencies throughout the world to provide a security against a breach, thus ensuring the safety of the members. Compartmentalization in clandestine cell networks provides minimization of damage due to exposure of one of the cells or honeypots. The visible part to the attackers of the proposed network is only the cells that are in direct contact with the attackers. Therefore, in case of exposure, removal of one single element of the network is A Clandestine cell communicates in indirect passive methods. They are; Dead-drops (Letter-drops or Mail-drops), Live-drops and Steganography.

- A Live-Drop is a technique where couriers are used in order to deliver messages or items and at the drop site, the receiver waits to secure the package.
- In Dead-Drops, one of the members places a message or item in the drop site and leaves a certain message to another location as an indicator to the receiver of the message. After some time later which is unknown to the dropper, the receiver recovers the package. Known as “the safest form of communication” (Codevilla, 1992) in between the case officer and the agent who is run by him in the intelligence circles during the cold war years, the dead-drops would be used in substitution for knowledgeable human beings wherever feasible (Cooper & Redlinger, 1990).
- Steganography is the art of hiding information in an ordinary file, picture, text or other kinds of media.

In this research, Dead-drops and Steganography is implemented for providing the clandestine communication of honeypots. A communication in a cell is illustrated in Figure 1.

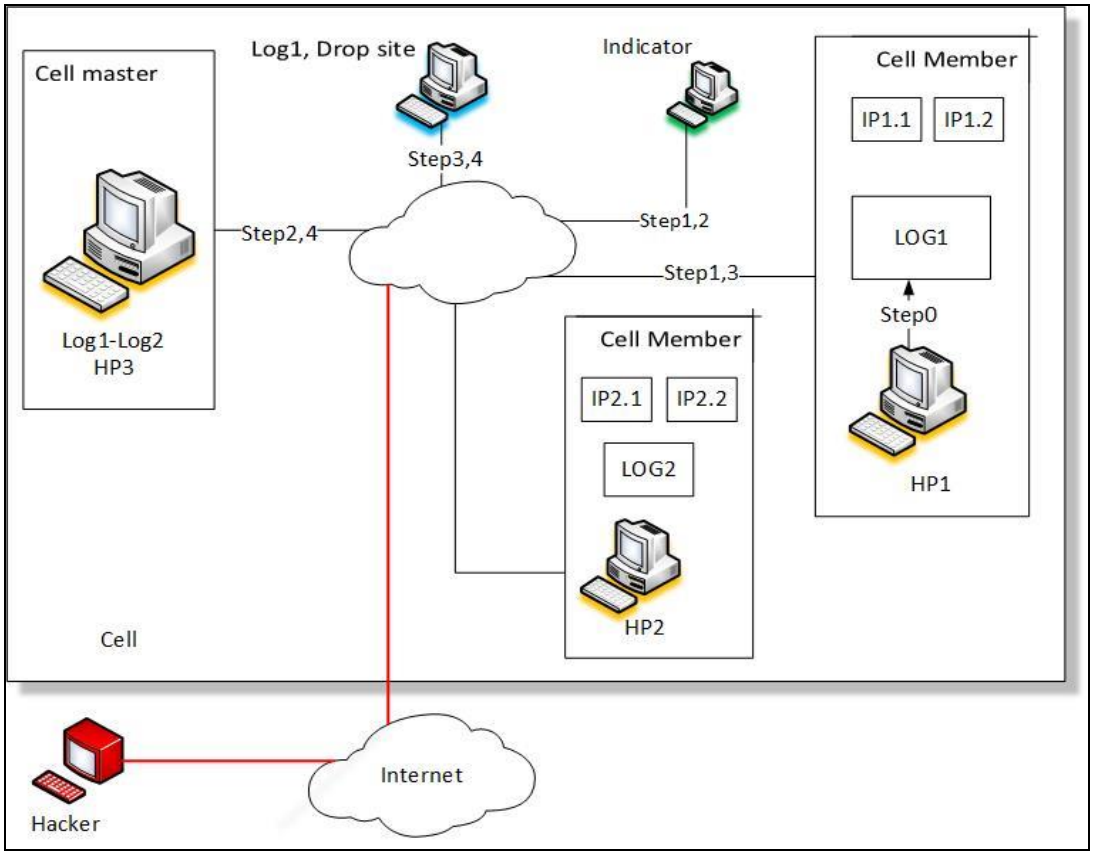

Figure 1. A cell of the proposed network.

A cell member is a host to a virtual machine having a high interaction honeypot. High interaction honeypots are implemented as Linux servers (Ubuntu 14.04 Server Edition). Vulnerable services are implemented in accordance with the APTs characteristics as shown in Table 1.

A honeypot cell member has two IP addresses shown as IP1.1 and IP1.2 in the Figure 1. These IPs are used when an attack is being conducted. The first IP address is the indicator location where a cell member sets a predefined flag to notify the cell master that it has the log files of an attack. Second IP is the location where the log files are uploaded in a crafted image prepared with steganography. For steganography implementations, Steghide is used in this research (Hetzl, 2003).

The cell master is responsible of polling the indicator hosts periodically in a predefined interval of time. When it sees a flag is set, it connects to the corresponding second IP location which is the drop site of the cell member and it extracts the crafted image from the virtual honeypot and send it to the master of its cell. After successfully extracting the information, the master of the cell, randomly selects another two different IP addresses from predefined pool and leaves them to the drop site. The sequence diagram for these two flows are illustrated in Figure 2.

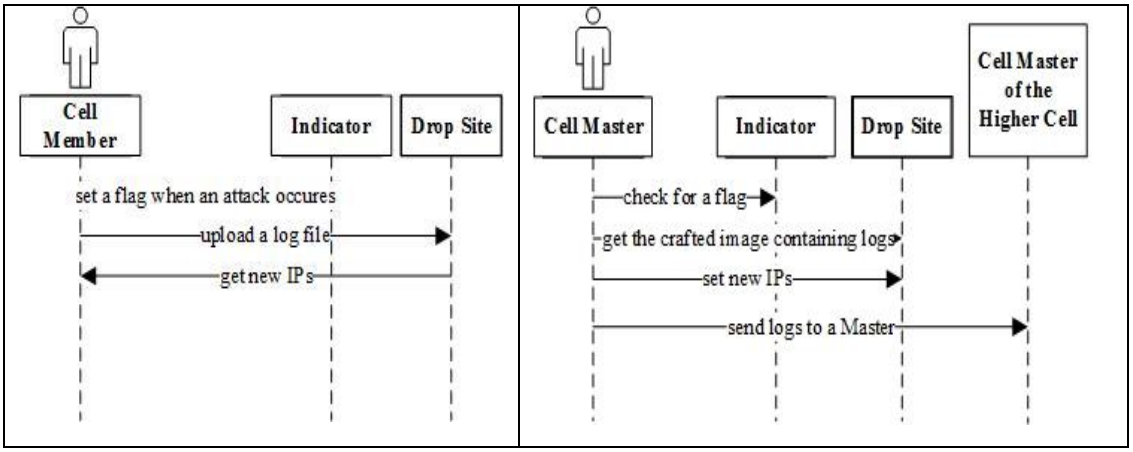

Figure 2. Sequence Diagrams for the communication of a cell member with the cell network (a) and cell masters communication with the cell network (b).

Depending on the size of the network, this clandestine cell approach can be increased in levels. Figure 3 illustrates such wide networks compartmentalized by the cells. On top of the system, a Command and Control (C&C) database is installed where all the information about attacks and attackers are saved.

The log files includes source IP addresses of the attacks, ports that are under attack, type of the attack, all the network connections with the honeypot that are established after taken control and to identify the type of the APT, how the communication is achieved. All these logs are compressed and inserted in a JPEG file.

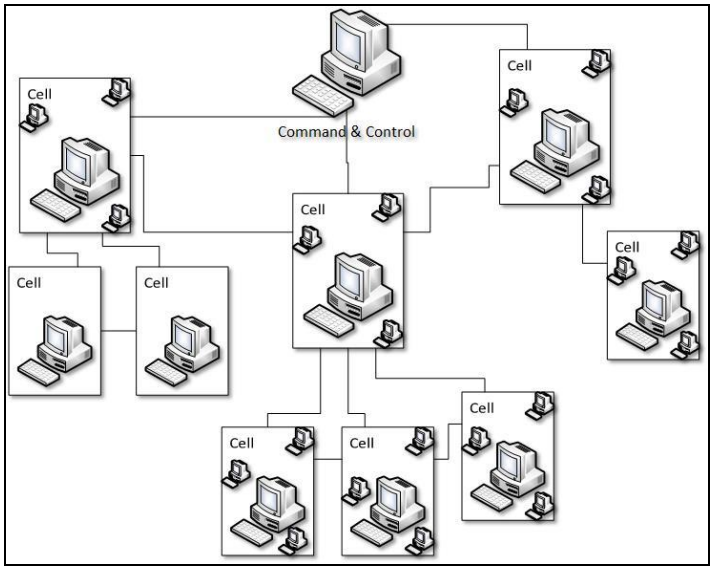

Figure 3. Overall schema for the Clandestine Network

5. Discussions & Conclusion

As a consequence of zero-day vulnerabilities and the concept of APTs, it is assumed that the system eventually will be possessed. By compartmentalizing the overall honeypot network design with this approach, these advantages are achieved:

- The log files are extracted from the cell member and not from the honeypot itself. Thus, when the honeypot is possessed, the chances of fooling the attacker is higher as there are no traces of an IDS process or service.
- By utilizing the indicator and drop site hosts, the communication of the cell member and cell master can never be exposed.
- Even a cell member or a complete cell is possessed, the system will continue to work and the analysis of the attacks can be disseminated by the C&C in real time.
- When compared with a decentralized honeypot network, this approach provides the advantage of automated collection of logs and identifying the diffusion of the attacks.

The main disadvantages of this system are the high cost of installing, maintaining it and overall complexity of analyzing the log files from all cells.

Being the tools of a spy craft, the dead-drops and honeypots were extensively utilized in human intelligence operations during the cold war years, and are still being used contemporarily as well, albeit in a different space defined by computers and other means of communication devices collectively known as the cyberspace. Some of the present day applications of dead drops and honeypots are thus being delineated in this paper.

References

Bencsáth, B., Pék, G., Buttyán, L., & Félegyházi, M. (2012). The Cousins of Stuxnet: Duqu, Flame, and Gauss. *Future Internet*, *4*(4), 971–1003. http://doi.org/10.3390/fi4040971

Chavez, R., Kranich, W., & Casella, A. (2015). *Red October and Its Reincarnation*. Retrieved from https://www.cs.bu.edu/~goldbe/teaching/HW55815/presos/redoct.pdf

Codevilla, A. (1992). *Informing Statecraft: Intelligence for a New Century*. New York: Free Press.

Cohen, F. (1998). A Note on the Role of Deception in Information Protection. Retrieved from http://all.net/journal/deception/deception.html

Common Vulnerabilities and Exposures. (1999). Retrieved February 19, 2016, from https://cve.mitre.org/about/index.html

Cooper, H. H. A., & Redlinger, L. J. (1990). *Catching Spies*. USA: Bantam.

Digby Diehl, & Clarridge, D. R. (1997). *A Spy For All Seasons: My Life in the CIA*. Scribner.

Doherty, S., & Krysiuk, P. (2011). *Trojan.Taidoor*. Retrieved from http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/trojan_taidoor-targeting_think_tanks.pdf

Earley, P. (1997). *Confessions of a Spy: The Real Story of Aldrich Ames*. Blackstone Audiobooks; Unabridged edition.

Eisenberg, T., Gries, D., Hartmanis, J., Holcomb, D., Lynn, M. S., & Santoro, T. (1989). The Cornell commission: on Morris and the worm. *Communications of the ACM*, *32*(6), 706–709. http://doi.org/10.1145/63526.63530

Falliere, N., Murchu, L. O., & Chien, E. (2011). *W32.Stuxnet Dossier*. *Symantec-Security Response* (Vol. Version 1.). Retrieved from https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

Fanfara, P., Dufala, M., & Radušovský, J. (2013). Autonomous hybrid honeypot as the future of distributed computer systems security. *Acta Polytechnica Hungarica*, *10*(6), 25–42.

Fireeye. (2014). *Assesing Damage and Extracting Intelligence*. Retrieved from https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-poison-ivy.pdf

Ghourabi, A., Abbes, T., & Bouhoula, A. (2014). Characterization of attacks collected from the deployment of Web service honeypot. *Security and Communication Networks*, *7*(2), 338–351. http://doi.org/10.1002/sec.737

Hetzl, S. (2003). Steghide. Retrieved February 19, 2016, from http://steghide.sourceforge.net/

Information Warfare Monitor. (2009). *Tracking GhostNet*. Retrieved from https://www.nsi.org/pdf/reports/Cyber Espionage Network.pdf

Jasek, R., Kolarik, M., & Vymola, T. (2014). Extended system of honeypots to detect threats, *8*.

Langner, R. (2011). Stuxnet: Dissecting a cyberwarfare weapon. *IEEE Security and Privacy*, *9*(3), 49–51. http://doi.org/10.1109/MSP.2011.67

Neumann, J. Von. (1969). Theory of self-reproducing automata. *Information Storage and Retrieval*. http://doi.org/10.1016/0020-0271(69)90026-6

Prathapani, A., Santhanam, L., & Agrawal, D. P. (2013). Detection of blackhole attack in a Wireless Mesh Network using intelligent honeypot agents. *Journal of Supercomputing*, *64*(3), 777–804. http://doi.org/10.1007/s11227-010-0547-3

Sancho, D., Torre, J. dela, Bakuei, M., Villeneuve, N., & McArdle, R. (2012). *IXESHE: An APT Campaign*. Retrieved from http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_ixeshe.pdf

Saud, Z., & Islam, M. H. (2015). Towards Proactive Detection of Advanced Persistent Threat (APT) Attacks Using Honeypots. *Proceedings of the 8th International Conference on Security of Information and Networks*, 154–157. http://doi.org/10.1145/2799979.2800042

Singh, G., Sharma, S., & Singh, P. (2013). Design and Develop a Honeypot for Small Scale Organization, *2*(3), 170–174.

Spitzner, L. (2003). Honeypots: Catching the insider threat. *Proceedings - Annual Computer Security Applications Conference, ACSAC*, 170–179. http://doi.org/10.1109/CSAC.2003.1254322

Symantec. (2011). *W32.Duqu The precursor to the next Stuxnet*. *Symantec Security Response* (Vol. version 1.). Retrieved from https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_duqu_the_precursor_to_the_next_stuxnet.pdf

Varma, R. (2010). *McAfee Labs: Combating Aurora*. Retrieved from https://kc.mcafee.com/resources/sites/MCAFEE/content/live/CORP_KNOWLEDGEBASE/67000/KB67957/en_US/Combating Threats - Operation Aurora.pdf

Virvilis, N., Gritzalis, D., & Apostolopoulos, T. (2013). Trusted computing vs. Advanced persistent threats: Can a defender win this game? *Proceedings - IEEE 10th International Conference on Ubiquitous Intelligence and Computing, UIC 2013 and IEEE 10th International Conference on Autonomic and Trusted Computing, ATC 2013*, 396–403. http://doi.org/10.1109/UIC-ATC.2013.80

Winn, M., Rice, M., Dunlap, S., Lopez, J., & Mullins, B. (2015). Constructing cost-effective and targetable industrial control system honeypots for production networks. *International Journal of Critical Infrastructure Protection*, *10*, 47–58. http://doi.org/10.1016/j.ijcip.2015.04.002

Wright, P., & Greengrass, P. (1988). *Spycatcher CST*. New York, U.S.A.: Dell Pub Co.

Zhan, Z., Xu, M., & Xu, S. (2013). Characterizing honeypot-captured cyber attacks: Statistical framework and case study. *IEEE Transactions on Information Forensics and Security*, *8*(11), 1775–1789. http://doi.org/10.1109/TIFS.2013.2279800

Zhang, W., He, H., & Kim, T. hoon. (2015). Xen-based virtual honeypot system for smart device. *Multimedia Tools and Applications*, *74*(19), 8541–8558. http://doi.org/10.1007/s11042-013-1499-4