2014 6th International Conference on Cyber Conflict
P.Brangetto, M.Maybaum, J.Stinissen (Eds.)
2014 © NATO CCD COE Publications, Tallinn

Changing the game: The art of deceiving sophisticated attackers

Nikos Virvilis
Cyber Defence and Assured Information Sharing
NATO Communications and Information Agency
The Hague, Netherlands

Oscar Serrano Serrano
Cyber Defence and Assured Information Sharing
NATO Communications and Information Agency
The Hague, Netherlands

Bart Vanautgaerden
Consultant for NATO Office of Security, InfoSec
NATO HQ
Brussels, Belgium

Abstract: The number and complexity of cyber-attacks has been increasing steadily in the last years. Adversaries are targeting the communications and information systems (CIS) of government, military and industrial organizations, as well as critical infrastructures, and are willing to spend large amounts of money, time and expertise on reaching their goals. In addition, recent sophisticated insider attacks resulted in the exfiltration of highly classified information to the public. Traditional security solutions have failed repeatedly to mitigate such threats. In order to defend against such sophisticated adversaries we need to redesign our defences, developing technologies focused more on detection than prevention. In this paper, we address the attack potential of advanced persistent threats (APT) and malicious insiders, highlighting the common characteristics of these two groups. In addition, we propose the use of multiple deception techniques, which can be used to protect both the external and internal resources of an organization and significantly increase the possibility of early detection of sophisticated attackers.

Keywords: *Advanced persistent threat, deception, insiders, honeypot, honey net, honey tokens*

1. INTRODUCTION

In the last decade, there have been a large number of advanced, well-orchestrated cyber-attacks against industry, military and state infrastructures. The main goal of most of these attacks is the exfiltration of large amounts of data. For example in 2006, China was accused of downloading

10 to 20 terabytes of data from the US NIPRNet[1] Military Network [1], and in 2008 a USB drive was deliberately left in the parking lot of a US Department of Defense facility in the Middle East for the purpose of subsequently infecting a laptop computer connected to the United States Central Command, resulting in the exfiltration of sensitive information [2]. In 2010 "Operation Aurora" targeted more than 20 organizations including Google, Adobe, Symantec and US defence contractors [3]. Furthermore, cyber-attacks intended to cause physical destruction have been known to occur [4].

While it is believed that these attacks were originated by different threat actors, they share certain common features and some of them have been categorized as advanced persistent threats. The term "advanced persistent threat" (APT), coined by the US Air Force in 2006[2], is not strictly defined and loosely covers threats with a number of characteristics in common. The definition of APT given by the National Institute of Standards and Technology (NIST) [5] is:

> *"An adversary with sophisticated levels of expertise and significant resources, allowing it through the use of multiple different attack vectors (e.g. cyber, physical, and deception) to generate opportunities to achieve its objectives, which are typically to establish and extend its presence within the information technology infrastructure of organizations for purposes of continually exfiltrating information and/or to undermine or impede critical aspects of a mission, program, or organization, or place itself in a position to do so in the future; moreover, the advanced persistent threat pursues its objectives repeatedly over an extended period of time, adapting to a defender's efforts to resist it, and with determination to maintain the level of interaction needed to execute its objectives."*

In addition, organizations face the always present threat of malicious insiders, a clear example of which is Edward Snowden, who recently downloaded 50,000 to 200,000 classified documents belonging to the US National Security Agency [6]. This incident arose shortly before Bradley Manning was convicted and sentenced to 35 years in prison in connection with the largest data leak in US history [7].

The ability of current security solutions to address such attackers has been questioned openly [8] [9] [10] [11], with authors stating that prevention techniques (e.g. network-intrusion prevention and antivirus products), and especially those focused on signatures, will never be able to successfully address sophisticated attacks.

The shortcomings of signature-based detection are well accepted, and the research community has focused on the use of anomaly-based detection systems. However, the effectiveness of such systems has also been challenged. Sommer and Paxson [12] describe anomaly detection as flawed in its basic assumptions. Research relies on the belief that anomaly detection is suitable for finding new types of attacks, however it is known that machine learning techniques are best suited to finding events similar to ones seen previously. Therefore, these approaches show promising detection possibilities for specific (training) data sets, but are subject to serious operational limitations.

1 Non-classified Internet Protocol Router Network

2 It was initially used as a generic term to describe intrusions without disclosing the classified threat name [32].

APTs use unique attack vectors and custom-built tools tuned for the particular target, making detection very challenging whether either signature or anomaly detection techniques are used. In this context, deception techniques are valuable for monitoring enterprise networks and identifying attack preparation and subsequent exploitation.

We present in this paper: (a) a comparison of APTs and malicious insiders, highlighting the common characteristics of these two attacker groups and suggesting that malicious insiders should be considered a subcategory of APTs, and (b) a proposal for the use of multiple deception techniques, such as social network avatars, fake (honey token) Domain Name System (DNS) records, and HTML comments – none of which, to the best of our knowledge, has been proposed before – that can significantly increase the likelihood of early detection in every phase of an attack's life-cycle.

The remainder of the paper is structured as follows: Section 2 presents related work. Section 3 focuses on the similarities between APTs and malicious insiders, as we believe that both can be treated in the same way for the purpose of detecting sophisticated attacks. In Section 4, we propose a number of deception techniques for protecting both the Internet-facing and the internal assets of an organization. Conclusions and further work are reported in Section 5.

2. RELATED WORK

Decoys, a popular strategy long used in warfare, played an important role during the Second World War [13] and the Cold War [14]. Decoys are also an integral part of electronic warfare strategies [15], however they are rarely used in the cyber domain. The first general reference to cyber decoys is attributed to Clifford Stoll, who describes them in his 1989 novel 'The Cuckoo's Egg' [16]. More than 10 years later, Spitzer described mechanisms for the detection of insider attacks using honeypots [17] and honey tokens, which share similar characteristics with honey files, as described in [18] and [19].

Elsewhere, honeypots [20] [21] have been proposed for attack detection [22] [23], including detection and analysis of botnets/worms, while honey nets [24] have been proposed as an effective means for the classification of network traffic and the detection of malicious users on Wi-Fi networks [25].

Honey files that include beacon signaling are discussed by Bowen et al. [26], who propose an architecture for monitoring multiple system events, including user interactions with a set of previously marked honey files. Similar work was pursued by Whitham [27], who introduced canary files, which have similar characteristics to honey files. Most of the published work concentrates on the creation and distribution of "perfectly believable" honey files [28], which contain certain properties that make them indistinguishable from real files to malicious users and at the same time are enticing enough to attract attention. Finally, researchers have also proposed embedding, in legitimate documents, code that will be automatically executed when the files are opened and will initiate a connection to a monitoring server [29] to provide a means of detecting unauthorized access.

To the best of our knowledge, there has been no research on the use of deception techniques for the detection of advanced persistent threats (APT).

3. ADVANCED PERSISTENT THREATS AND INSIDERS

The definition of a malicious insider based on Silowash et al. [30] is:

> *"... a current or former employee, contractor, or business partner who meets the following criteria:*
>
> - *has or had authorized access to organization's network, system, or data*
> - *has intentionally exceeded or intentionally used that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems."*

The motives of insiders vary, and can be based on revenge or can be financial, ethical or political [31].

APTs and malicious insiders share specific characteristics that markedly differentiate them from traditional (e.g. opportunistic) attackers:

- Their attacks require detailed planning [32], and are spread over a long period of time in an effort to evade detection. Insiders have a potential advantage over APTs in planning their attack, as they may be aware of existing security controls. This is very likely if an insider holds a privileged position (e.g. an administrator is expected to have knowledge of the deployed security mechanisms and potentially has the access rights to control them, while a less privileged user would not [32]). Nevertheless, experience has shown that APTs have also managed to reach their goals while evading detection without prior knowledge of the infrastructure [3].
- Both groups are willing to spend a substantial amount of time exploring all possible attack paths for reaching their goals, including social engineering and deception [32]. APT groups tend to have teams of highly skilled individuals with access to important resources (financial, technical, intelligence). Malicious insiders, although they work mostly alone, as in the case of Manning and Snowden, might also have well developed technical skills.
- Both are interested in maintaining access to the penetrated infrastructure and continuing the exfiltration of data for as long as possible.

The main difference between the two types of attackers is that malicious insiders have by definition authorized access to the infrastructure and potentially even to the servers storing sensitive information (e.g. file servers, database servers), while APTs need to gain unauthorized access.

APTs and insider threats are currently considered to be two different threat groups. However, given the known instances of APT groups blackmailing or bribing an insider to perform a malicious action on their behalf [33], we strongly believe that malicious insiders should be regarded as a subset of advanced persistent threats.

Robust models have been proposed for the detection of insider threats [34], however they assume that the malicious insider(s) will perform the entire attack life-cycle on their own (information gathering, exploitation, exfiltration). Yet, in the Stuxnet case [33], a malicious insider was used only to deliver the payload, while the rest of the exploitation was performed in an automated way. Such an attack strategy, which combines APT with the insider element, poses a serious challenge for insider threat detection models.

Taking into consideration the substantial resources available to APT groups [35], we can expect similar attacks to occur in the future, and thus we strongly believe that further research is necessary to augment the detection capabilities of such models against combined insider-APT attacks.

4. DECEPTION TECHNIQUES

Detection of network-based security threats can significantly increase the likelihood of detecting APT and insider attacks by monitoring the operational networks/infrastructure as well as the unused IP address space ("darknets") [36]. The APT attack life-cycle [37] consists of several stages: attack preparation and initial compromise, establishing a foothold, escalation of privileges, internal reconnaissance, exploitation of systems and exfiltration of data. For the sake of simplicity in this paper, we group these stages into two general phases: attack preparation (information gathering), and exploitation and data exfiltration.

A. Phase 1: Attack preparation (information gathering)

The initial step of an APT attack is the preparation phase, in which perpetrators gather as much information as possible about their target. Identification of the operating system, third-party software and publicly accessible services (e.g. web servers, mail servers) of the organization is crucial for planning a successful attack. Information related to the security solutions in use (intrusion-detection and intrusion-prevention systems, endpoint protection, data leakage prevention) is also important for the attackers to have, as it allows them to test their tools and techniques in advance.

An additional element of the preparation phase is collection of information about employees, their positions in the organization, their skills and their connections with other employees. Using such information, APTs can create highly targeted spear-phishing campaigns. For example, if an attacker has identified an employee working in the human resources (HR) department as well as his supervisor, he can send a spoofed email from the email address of the supervisor to the employee, asking him to review an attached file (e.g. a curriculum vitae). The attachment can be a malicious Word or PDF file that when opened will execute the attacker's payload. The fact that the email originates from a person known to the victim significantly increases the likelihood of its being accepted as legitimate.

In order to address this first phase of the attack life-cycle, we propose the following deception techniques.

1) DNS honey tokens
DNS honey tokens are proposed as a complementary technique to honeypots.

Because attackers will try to identify Internet-facing systems/services belonging to the organization, defenders can deploy honeypots spread over the unused public IP range of the organization. Based on the fact that these systems will not be publicly listed (e.g. not returned as part of a search query with a link to the organization's web site), a connection attempt could be due to: (a) user error (mistyping an IP address), (b) an automated attack such as a worm randomly scanning the IP address space to find vulnerable hosts to compromise, or (c) an attacker trying to identify all publicly accessible systems and services of the organization.

However, the use of honeypots generates a substantial amount of noise owing to the vast number of automated attacks on the Internet [38]. In addition, it can be difficult to differentiate between an automated non-targeted attack and a targeted one.

We propose a technique that is simpler to implement than honeypots and will significantly limit the number of false positives occurring. It consists of inserting fake DNS records (a type of honey token) in the DNS servers.

Attackers are very likely to use "brute force" for common subdomains or attempt a zone transfer [39] on an organization's DNS servers to try to identify interesting resources (e.g. sub-domains, servers) as part of their information-gathering process. By creating a small number of fake DNS records on the authoritative DNS servers of the organization and configuring them to initiate an alert when these specific records are requested, defenders can receive an early warning of DNS-related information-gathering attempts against their infrastructure.

2) Web server honey tokens
The public web servers of an organization are another fruitful source of information for attackers. We propose three ways of using honey tokens to help detect malicious web-site visitors:

- Addition of fake entries in robots.txt files
- Use of invisible links
- Inclusion of honey-token HTML comments.

A robots.txt file [40] is a simple text file located in the root folder of the web server, which legitimate bots (e.g. Google bot) parse to identify which folders on the web server they should not access and index. The file is one of the first places that attackers (and automated web-vulnerability scanning tools) look for potentially sensitive directories. By including non-existing directories such as "/admin" or "/login" in the robots.txt file and monitoring for access requests to these locations, administrators can be alerted to visitors with malicious intentions.
The inclusion of invisible links (e.g. white links on white font) at random parts of the web site(s), pointing to non-existing (but interesting from the attacker's perspective) resources, can

serve a similar purpose. Although these links will be invisible to legitimate visitors, they will be detected by the crawling tools that attackers are likely to use. A request for such a fake URL should raise an alert.

A final deception mechanism, particularly useful for web sites that support authentication, is the inclusion of fake accounts in HTML comments. Legitimate users have no need to review the source code of a web page, however attackers frequently do in trying to identify vulnerabilities. The inclusion of a comment such as the following in the HTML source code of a login page is very likely to tempt the attacker to use it:

<!--test account: admin, pass: passworD123. Please remove at the end of development!-->.

Once more, an attempt to login with these credentials is a clear indication of malicious activity.

3) Social network avatars

Social networks are an invaluable source of information for attackers. In order to identify malicious activity, we propose the creation of avatars (fake personas) on the major social networks. It is important that the avatars appear to be realistic, having connections with people from both inside and outside the organization and with positions that are likely to be of interest to the attackers (e.g. HR department, financial department, developer, etc.). In addition, such avatars should have real, but very closely monitored, accounts in the organization (e.g. active directory accounts), as well as valid email addresses. Interaction with the avatars should be regularly monitored (friend requests, private messages, attachments, etc.).

External applicants interested in applying for a position in the organization may contact the human resources avatar (producing a false positive). However, because internal employees should know the correct contact details, communication between an internal employee and the avatar can be considered suspicious. Such interaction could be an indication that the employee's account has been compromised, as will be any login attempts using the avatar account(s).

B. Phase 2: Exploitation and data exfiltration

The second step of the APT life-cycle is exploitation of the target. The attackers, after gaining access to the internal network (e.g. taking advantage of 0-day vulnerabilities, social engineering, spear-phishing attack), will start the exfiltration process and try to identify (a) systems that they can compromise to be used as alternative access points to the network (in case the initial ones are detected and quarantined), and (b) systems that may contain the information they are seeking or that can help them access that information.

In order to address this phase of the attack we propose the following deception techniques.

Deception techniques for network layer defences

In a medium to large organization in which hundreds or even thousands of systems are active, identifying the location of targeted information is not a trivial task. Attackers will need to explore the network, hop between networks and exploit multiple systems. Use of darknets and

or honey nets can be invaluable in detecting such actions, as attackers may eventually access them, raising an immediate alert.

1) Darknets

A darknet, also known as a black hole, Internet sink or darkspace, is a portion of routed, unallocated IP space in which no workstations/servers or other network devices are located. Access to such regions of the network can occur by a legitimate mistake (e.g. a user mistyping an IP address), however multiple connection attempts should be considered suspicious. Monitoring such segments for connection attempts can be an easy-to-deploy and effective mechanism, however it is not guaranteed that attackers will actually access these parts of the network.

2) Honey nets

Honey nets [41] are used for monitoring larger and/or more diverse networks in which one honeypot may not be sufficient. Defenders can use honey nets to create multiple fake systems in the same IP ranges as legitimate systems/servers. An attacker who gains access to a specific network segment is very likely to access these fake systems along with the real ones. Interaction with such systems should be very closely monitored as it is a strong indication of an active attack.

Deception techniques for application layer defences

The same techniques used for detecting malicious activity on external web servers can be used for protecting internal ones. Furthermore, as the majority of organizations make use of database and files servers on their internal networks, we propose the following deception techniques for the detection of malicious activity against those servers.

1) Database server honey tokens

Use of honey tokens in the databases can be used to highlight malicious activity. For example, a number of fake patient records (with fake patient names) can be introduced in a hospital's patient database. Attempts to access such records should be considered highly suspicious. However, database auditing must be enabled for logging the queries, and this will negatively affect the performance of the database.

2) Honey files

As described in related work, a number of strategies for creating decoys (honey files) have been proposed, focusing either on the generation of perfectly believable decoys or the modification of legitimate files to include some alerting functionality. Although the practical use of perfectly believable decoys has been questioned, use of legitimate files can interfere with the operation of the organization.

We propose a combination of file system auditing and the generation of honey files with potentially interesting content for attackers (e.g. passwords.docx, new_investments.pdf, etc.). These files should be spread across the file servers of the organization and/or even workstations, however the latter will increase the number of false positive alerts [29]. In environments in which document markings are used (i.e. TOP SECRET, SECRET, etc.), those can easily be

taken advantage of for generating decoy files. For example, it is easy to mark a fake document with a classification higher than the maximum level authorized to be stored in the system. Since such a situation indicates a security infraction, all users interacting with that document should report the infraction to security, and non-reported interactions are therefore highly suspicious.

A number of detection techniques can be implemented, including:

- File system auditing [42], which will log access attempts to these files.
- Inclusion of code that when executed will report back to a monitoring server. This can be achieved by using JavaScript for PDF files, or remote images that are downloaded when the document is opened [43].
- Inclusion of bait information, such as fake credentials, that attackers may try to use.

3) Honey accounts
Creating bait accounts (such as accounts for avatars) is an additional way of detecting attackers, as any interaction (e.g. login attempts) with these accounts is a clear indication of an active attack. This could be combined with the aforementioned example of placing bait files on file servers, where a file with fake credentials (user names and passwords) could be created. An attacker who has gained access to the file is very likely to try to use these accounts to gain further access to the network and as a result will immediately raise an alert.

C. Evaluation

Preventive techniques will eventually fail against sophisticated attackers [9], thus it is critical to switch our focus to detection measures. Use of deception techniques such as those proposed will significantly increase the possibility of detecting attacks early in the attack life-cycle, allowing defenders to mitigate a threat before the attackers achieve their goals.

Although the effectiveness of such measures against insiders is open to discussion, based on the fact that insiders are likely to be aware of their use and will try to evade them, we believe that combining a number of deception techniques will make evasion very difficult, provided that it is not the insider who has implemented the deception measures.

There is a risk that the introduction of deception techniques to monitor internal assets may interfere with the normal functioning of the organization. Therefore we have focused on techniques that are non-intrusive and that will seldom result in false positives. We recommend integrating them into an anomaly-detection system [44] incorporating some additional data sources, such as HR databases (e.g. user data, leave data), access rights matrices, net-flow data, etc., as this would further increase the reliability of the detection system and limit the number of false positives occurring.

5. CONCLUSIONS AND FUTURE WORK

Insider threats and APTs have a number of characteristics in common and should be considered as a single threat type. Furthermore, current security solutions do not effectively address

sophisticated attackers. We propose the use of deception techniques as a potential solution to this multidimensional problem. Several deception techniques can be used to increase the possibility of early detection at any stage of the attack life-cycle. Furthermore, such techniques can be combined with traditional collection and correlation systems to further increase the capability to detect sophisticated attackers.

Finally, future work will focus on the improvement of existing insider threat detection models through the introduction of deception techniques.

REFERENCES

[1] R. Marquand and B. Arnoldy, "China Emerges as Leader in Cyberwarfare," *The Christian Science Monitor*, Aug. 2007.

[2] J. P. Farwell and R. Rohozinski, "The New Reality of Cyber War," *Survival: Global Politics and Strategy*, vol. 54, no. 4, pp. 107–120, 2012.

[3] K. Zetter, "Google hack attack was ultra sophisticated, new details show," *Wired Magazine*, vol. 14, 2010.

[4] R. Langner, "Stuxnet: Dissecting a Cyberwarfare Weapon," *Security Privacy, IEEE*, vol. 9, no. 3, pp. 49–51, 2011.

[5] "Guide for Conducting Risk Assessments (Rev 1)," National Institute of Standards and Technology, Gaithersburg, USA, NIST Special Publication 800-30, Sep. 2012.

[6] M. Hosenball, "NSA chief says Snowden leaked up to 200,000 secret documents," Reuters, 14-Nov-2013. [Online]. Available: http://www.reuters.com/article/11/14/us-usa-security-nsa-idUSBRE9AD19B2013114.

[7] D. Nicks, *Private Bradley Manning, WikiLeaks, and the Biggest Exposure of Official Secrets in American History*. Chicago Review Press, 2012.

[8] E. Cole, *Advanced Persistent Threat: Understanding the Danger and How to Protect Your Organization*. Newnes, 2012.

[9] R. Bejtlich, *The Practice of Network Security Monitoring: Understanding Incident Detection and Response*. No Starch Press, 2013.

[10] N. Virvilis and D. Gritzalis, "The Big Four -- What we did wrong in Advanced Persistent Threat detection?," in *Availability, Reliability and Security (ARES), 2013 Eighth International Conference on*, 2013, pp. 248–254.

[11] N. Virvilis, D. Gritzalis, and T. Apostolopoulos, "Trusted Computing vs. Advanced Persistent Threats: Can a defender win this game?," in *Ubiquitous Intelligence and Computing, 2013 IEEE 10th International Conference on and 10th International Conference on Autonomic and Trusted Computing (UIC/ATC)*, 2013, pp. 396–403.

[12] R. Sommer and V. Paxson, "Outside the Closed World: On Using Machine Learning for Network Intrusion Detection," in *Security and Privacy (SP), 2010 IEEE Symposium on*, 2010, pp. 305–316.

[13] T. Holt, *The Deceivers: Allied Military Deception in the Second World War*. Simon and Schuster, 2010.

[14] G. R. Mitchell, *Strategic Deception: Rhetoric, Science, and Politics in Missile Defense Advocacy*. Michigan State Univ Press, 2000.

[15] K. B. Alexander, *Electronic Warfare in Operations: U.S. Army Field Manual FM 3-36*. DIANE Publishing Company, 2009.

[16] C. Stoll, *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage*. New York, NY, USA: Doubleday, 1989.

[17] L. Spitzner, "Honeypots: Catching the Insider Threat," presented at the 19th Annual Computer Security Applications Conference, 2003, pp. 170–179.

[18] J. Yuill, M. Zappe, D. Denning, and F. Feer, "Honeyfiles: Deceptive Files for Intrusion Detection," presented at the Fifth Annual IEEE SMC Conference Workshop on Information Assurance, 2004, pp. 116–122.

[19] M. Bercovitch, M. Renford, L. Hasson, A. Shabtai, L. Rokach, and Y. Elovici, "HoneyGen: An automated honeytokens generator," *in Intelligence and Security Informatics (ISI), 2011 IEEE International Conference on*, 2011, pp. 131–136.

[20] N. Provos and T. Holz, *Virtual Honeypots: from Botnet Tracking to Intrusion Detection*. Pearson Education, 2007.

[21] R. Joshi and A. Sardana, *Honeypots: A New Paradigm to Information Security*. Science Publishers, 2011.

[22] P. Wang, L. Wu, R. Cunningham, and C. C. Zou, “Honeypot detection in advanced botnet attacks,” *International Journal of Information and Computer Security*, vol. 4, no. 1, pp. 30–51, 2010.
[23] C. C. Zou and R. Cunningham, “Honeypot-aware advanced botnet construction and maintenance,” in *Dependable Systems and Networks, 2006. DSN 2006. International Conference on*, 2006, pp. 199–208.
[24] O. Thonnard and M. Dacier, “A framework for attack patterns’ discovery in honeynet data,” *digital investigation*, vol. 5, pp. S128–S139, 2008.
[25] B. M. Bowen, V. P. Kemerlis, P. Prabhu, A. D. Keromytis, and S. J. Stolfo, “A system for generating and injecting indistinguishable network decoys,” *Journal of Computer Security*, vol. 20, no. 2, pp. 199–221, 2012.
[26] B. Bowen, M. Ben Salem, A. Keromytis, and S. Stolfo, “Monitoring Technologies for Mitigating Insider Threats,” in *Insider Threats in Cyber Security*, vol. 49, C. W. Probst, J. Hunker, D. Gollmann, and M. Bishop, Eds. Springer US, 2010, pp. 197–217.
[27] B. Whitham, “Canary Files: Generating Fake Files to Detect Critical Data Loss from Complex Computer Networks,” presented at the Second International Conference on Cyber Security, Cyber Peacefare and Digital Forensic (CyberSec2013), Malaysia, 2013.
[28] J. A. Voris, J. Jermyn, A. D. Keromytis, and S. J. Stolfo, “Bait and Snitch: Defending Computer Systems with Decoys,” 2013.
[29] M. Ben Salem and S. Stolfo, “Decoy Document Deployment for Effective Masquerade Attack Detection,” in *Detection of Intrusions and Malware, and Vulnerability Assessment*, 2011, vol. 6739, pp. 35–54.
[30] G. J. Silowash, D. M. Cappelli, A. P. Moore, R. F. Trzeciak, T. Shimeall, and L. Flynn, “Common Sense Guide to Mitigating Insider Threats (4th Edition),” *Software Engineering Institute*, no. 677, 2012.
[31] B. Gellman and J. Markon, “Edward Snowden says motive behind leaks was to expose ‘surveillance state’,” *Washington Post*, 09-Jun-2013.
[32] J. Hudson, “Deciphering How Edward Snowden Breached the NSA,” *Venafi*, 12-Nov-2013. [Online]. Available: http://www.venafi.com/deciphering-how-edward-snowden-breached-the-nsa/?goback=%2Egde_135559_member_5806426207796871171#%21. [Accessed: 21-Nov-2013].
[33] M. Kelley, “The Stuxnet Virus at Iran’s Nuclear Facility was Planted by an Iranian Double Agent,” *Military & Defense*. 13-Apr-2012.
[34] M. Kandias, A. Mylonas, N. Virvilis, M. Theoharidou, and D. Gritzalis, “An insider threat prediction model,” in *Trust, Privacy and Security in Digital Business*, Springer, 2010, pp. 26–37.
[35] D. Fisher, “What have we learned: FLAME malware,” *Threat Post*. 15-Jun-2012.
[36] R. Pang, V. Yegneswaran, P. Barford, V. Paxson, and L. Peterson, “Characteristics of Internet Background Radiation,” in *Proceedings of the 4th ACM SIGCOMM Conference on Internet Measurement*, New York, NY, USA, 2004, pp. 27–40.
[37] “Exposing One of China’s Cyber Espionage Units,” Mandiant, Feb. 2013.
[38] M. Gebauer, “Warfare with Malware: NATO Faced with Rising Flood of Cyberattacks,” *Spiegel*, Mons, Belgium, 26-Apr-2012.
[39] C. Edge, W. Barker, B. Hunter, and G. Sullivan, “Network Scanning, Intrusion Detection, and Intrusion Prevention Tools,” in *Enterprise Mac Security*, Springer, 2010, pp. 485–504.
[40] J. Hendler and T. Berners-Lee, “From the Semantic Web to social machines: A research challenge for AI on the World Wide Web,” *Artificial Intelligence*, vol. 174, no. 2, pp. 156–161, 2010.
[41] L. Spitzner, “The Honeynet Project: Trapping the Hackers,” *Security Privacy*, IEEE, vol. 1, no. 2, pp. 15–23, Mar. 2003.
[42] D. Melber, “Securing and Auditing High Risk Files on Windows Servers,” *Windows Security*. 17-Apr-2013.
[43] B. Bowen, M. Ben Salem, S. Hershkop, A. Keromytis, and S. Stolfo, “Designing Host and Network Sensors to Mitigate the Insider Threat,” *Journal of Security & Privacy IEEE*, vol. 7, pp. 22–29, Nov. 2013.
[44] C.-F. Tsai, Y.-F. Hsu, C.-Y. Lin, and W.-Y. Lin, “Intrusion detection by machine learning: A review,” *Expert Systems with Applications*, vol. 36, no. 10, pp. 11994 – 12000, 2009.