최신 APT 해킹공격에 대한 방어

조나단 마평, 이훈재
동서대학교 유비쿼터스 IT 학과

Defending Against Today's Advanced Persistent Threats

Jonathan A.P. Marpaung*, HoonJae Lee*
*Dept. of Ubiquitous IT, Graduate School, Dongseo University
e-mail : jonathan@spentera.com

ABSTRACT

Recent high profile attacks have brought the attention of governments, corporations, and the general public towards the dangers posed by Advanced Persistent Threats. This paper provides an analysis of the attack vectors employed by these actors by studying several recent attacks. We present recommendations on how to best defend against these threats by better classification of critical information infrastructure and assets, people protection, penetration tests, access control, security monitoring, and patch management.

1. Introduction

Significant strides have been made in defending against cyber threats since the early days of the internet. In protecting their assets, many organizations have deployed state of the art defense technologies, obtained standards certification for enforcing policies and controls, hired expert computer security teams, and performed regular penetration tests. The combination of these mechanisms has proven to be resilient against the conventional hacker who is more likely to seek softer targets to maximize profit or damage. The financially motivated attacker is interested in using fewer resources and infecting as many targets as possible; not on spending a lot of time on compromising one particular target. However, recent attacks upon several organizations and high level targets have shown characteristics only possessed by an intrepid adversary.

These kinds of attacks are carried out by parties classified as Advanced Persistent Threats (APTs). As the name implies, APTs are highly motivated, can operate over an extended period of time, and typically have access to abundant resources be it money or expertise. Today's APT attacks have also been mostly successful in compromising their targets and achieving their goals. In an already challenging and dynamic cyber space environment, owners of critical information infrastructure and intellectual property must now also consider the existence of these threats and whether they are adequately prepared or not. This paper discusses the nature of APTs, provides an analysis on several recent attacks, and presents suggestions on how to mount a defense

2. Advanced Persistent Threats

APTs are a class of hackers that are well resourced, persistent, and highly motivated [1]. Their targets have typically been political as the main actors with these resources are nation states and their foreign intelligence services. However there has been a shift towards targeting enterprises with the goal of obtaining intellectual property or industrial espionage, which has led to the idea the involvement of other threat actors such as rival corporations or organized crime.

2.1 Specific Targets

Unlike common malware that have the goal of infecting as many hosts as possible, attacks made by APTs are intended for one particular domain or organization. Attackers limit the propagation features of their malware to keep it contained. As a result these attacks will mostly escape detection of Computer Emergency Response Teams (CERTs) or other security operation centers due to the low profile generated and absence of widespread suspicious network traffic.

2.2 Utilize New and Customized Malware

In order to increase the probability of success, APTs design customized malware payloads and attack vectors according to their targets. Unpublished Zero-Day exploits remain at the core of APT attacks. A vivid example of this is how an unprecedented 4 Zero-Day exploits were used in Stuxnet [2]. The importance of exploit development was underscored at the 2012 AusCERT conference where Mikko Hypponen mentioned that the fourth largest defense contractor in the U.S., had 137 top secret openings exclusively for exploit developers [3]. This suggests a cyber-arms stockpiling of Zero-Day exploits is underway. Meanwhile an already thriving black market exploit industry is making this commodity accessible to criminal organizations and other parties with prices ranging from $500 - $250,000 [4].

2.3 Employ Evasion Techniques

As the APTs have the objective of infiltrating their targets undetected for as long as it takes to achieve their goals, evasion techniques are used to hide malware payloads. The methods used vary from obfuscation, network based fragmentation and session splicing, application or protocol violations, disabling intrusion detection systems (IDSs), to more advanced techniques such as code reuse attacks [5].

2.4 Operate Over Extended Period of Time

APT actors are willing to invest months, if not years of preparation and actual execution of the attack. After gaining a foothold into the target, the malware can be controlled to remain dormant or propagate laterally through the network until the makers are sure right host or intellectual property is found. In the example of Stuxnet, over a period of a year, the malware was continuously propagated and updated until it reached the PLC's (Programmable Logic Controllers) of Iran's enrichment centrifuges.

2.5 Exploit Vulnerabilities in People

A key characteristic of APT attacks is that the actors take the time to research actual people in order to exploit them. People are often the weakest link in an organization's security posture and this fact has been exploited for decades since the first phishing attacks. Potential human targets can be found by searching through social networking sites such as Facebook and LinkedIn. They could be either employees or contractors of the organization being targeted. The next step would conduct spear-phishing attacks with the intention of infecting a host or USB storage device. This would become the initial entry point of the attack vector and is a characteristic found in common among most APT attacks.

3. Recent High Profile APT Attacks

APT attacks have been steadily increasing over the past decade as more and more governments and corporations rely on networked resources. Table 1 shows that the number of APT attacks have increased significantly in recent years, especially in 2011. In this paper we look at three recent cases, Stuxnet, RSA, and the attacks on Comodo and DigiNotar Certificate Authorities (CAs).

3.1 Stuxnet

Stuxnet was discovered in July 2010, but is confirmed to have existed at least one year before and likely even earlier. Stuxnet caught many security researchers and professionals by surprise, being the first advanced malware of its kind. According to Symantec's report, Stuxnet is a complex threat that was primarily written to target an industrial control system (ICS) or set of similar systems. A vast array of components was implemented in the malware including four Zero-Day exploits, a windows rootkit, antivirus evasion techniques, complex process injection and hooking code, network infection routines, peer-to-peer updates, a command and control interface, as well as the first ever PLC rootkit. Stuxnet's main payload has the main purpose of modifying code on Siemens industrial PLCs in order to sabotage the system.

It is widely believed that Iran's Natanz nuclear Fuel Enrichment Plant (FEP) was the intended target. Hosts in five domains of organizations based in Iran were heavily infected over 3 attack waves. The deliberate containment of the malware to targets in Iran is also apparent from the number of hosts infected worldwide, which reached only around 100,000 with approximately 60% being in Iran. This attack has been claimed to setback Iran's nuclear program by several years as 1,000 out of 9,000 centrifuges were disabled and had to be replaced [6]. The initial attack point is likely to be via a USB infection.

3.2 RSA

In March 2011, security company RSA was hacked by an APT [7]. The attackers employed spear-phishing emails targeted at two small groups of employees. The email attachment used was a spreadsheet titled "2011 Recruitment Plan.xls". The file contained a Zero-Day exploit for an Adobe Flash vulnerability, installing a backdoor. The tool used to take control of the machine was a variant of the Poison Ivy remote administration tool. Using a reverse TCP connection compromised machines contacted command & control servers to receive commands to execute. Privilege escalation and pivoting to high value targets was done until the attackers reached the servers containing valuable intellectual property. In this case they obtained information regarding RSA's SecurID two-factor authentication products which they transferred out in .rar files over an FTP connection.

RSA admitted that this breach could potentially reduce the effectiveness of SecurID implementations, suggesting that client seeds (secret keys) had been compromised. Three months later RSA announced that it was replacing security tokens for several of its customers including defense contractors Lockheed Martin and L-3 after they were reportedly breached using duplicate SecurID keys [8].

3.3 Comodo & DigitNotar Certificate Authorities

A Comodo Root Authority (RA) was breached in March 2011. The attacker created a user account and used it to issue nine fraudulent SSL certificates across seven different domains including Google, Yahoo, and Skype [9]. Comodo responded quickly though and revoked the certificates within hours of the incident. Another CA, DigitNotar was attacked in June 2011 with hackers issuing fraudulent SSL certificates for Google, Skype, and other domains [10]. These attacks both originated from Iran and are suspected to be a state sponsored attack. As the certificates were used on Iranian sites and required modification of DNS entries to effectively launch a man-in-the-middle (MITM) attacks, it is likely that the Iranian government was monitoring the Gmail communications of more than 300,000 users based in the country.

An audit by Fox-IT found that DigiNotar's servers ran out of date software, had poor network segmentation, and had no server side antivirus software. Not long after the major browsers blacklisted DigiNotar, it declared bankruptcy.

4. Defending Against the APT

The attacks against Iran's nuclear program, RSA, Comodo, and DigiNotar provides insight on lessons learned both from classic security practices as well as areas where governments and corporations need to be more aggressive. In this section we discuss important measures that need to be taken in order to be resilient against APTs.

3.4 Update Identification of Critical Information Infrastructure and Assets

It is common practice for organizations with mature security management practices to identify their most valuable assets and focus their efforts on hardening the security around these assets. It is now necessary to expand this principle to a more global level to start identifying companies and organizations that possess intellectual property or services that are critical to the security of users on the Internet. CAs are the most vital link in SSL infrastructure and their compromise jeopardizes the safety of millions of users. Likewise for companies that provide security products requiring storage of crucial data, such as cryptographic secret keys or seeds. Both of these examples should fall under the category of global critical information infrastructure or assets providing products and services to the public.

We propose that an international institution approach be taken to ensure governance of these infrastructure and assets with sanctions for corporations/institutions that fail to meet a high level of assurance. It should be understood that a successful attack against any of these assets constitute an attack on the safety of the general public.

3.5 People protection

The majority of APT attacks exploit human vulnerabilities as their initial entry point, however not enough attention has been brought to seriously address this. It is just as important to consider the security level of employees, as it is to deploy the state of the art firewalls, antivirus, and IDS devices. Apart from ensuring awareness programs and compliance of security policies, social engineering tests should be regularly carried out in order to assess the security robustness of the human factor. Limitation of employee participation in social networks should also be considered as the information gained could be used in launching an attack against the organization.

3.6 Penetration Tests

Regular penetration tests are vital in understanding the possible attack vectors used by adversaries as well as for determining the correct countermeasures for protection. Already a common practice in the banking and finance industry, rigorous testing must be conducted against other critical information infrastructure and assets.

3.7 Access Control

The attacks on RSA were claimed to be quickly detected by their security team, however detection did not prevent access to the machines storing the critical SecurID seeds nor did it circumvent the FTP connection used to transfer the .RAR files to a remote command & control server. Considering that the initial entry point for this attack were PC's used by employees not directly attached to the SecurID program, it is a failure of access control design that the breach was not contained to one network segment. Firewall policies should also have prevented outgoing FTP connections.

Further mechanisms that could be implemented are email attachment filtering for sources that are not trusted (i.e. not verified by digital signature), multifactor authentication, I/O device limitation, and host based firewalls or sandboxing of applications running on end devices. The latter can be used to prevent applications making unauthorized outgoing connections, such as in the case of the Adobe Reader exploit. Containment and harm minimization is only possible with well designed and enforced access control.

3.8 Security Monitoring Systems and Response

Early detection and response requires the deployment of up-to-date IDS and SIEM (Security Information and Event Management) Systems monitored by trained analysts and CERT teams. Routine log analysis and event correlation can be used to detect anomalous activities when even antivirus software has been thwarted due to evasion techniques or Zero-Day exploits. Policies and procedures should also be defined and ready to execute in the event of an incident as there is only a limited window of opportunity between detection of intrusion and completion of a successful attack. Automated incident response will also become an important component of these systems and security personnel should define which conditions must be responded to by machines or people.

3.9 Updates and Patch Management

The DigiNotar breach is a prime example of poor update and patch management. New vulnerabilities are being found everyday and software vendors are struggling to release tested patches. In today's world of vulnerability management, owners of vital assets and infrastructure must ensure that all networked devices and applications are maintained in pace with the releases.

5. Conclusion

Defending against the APT can only be effective if it is holistic; ensuring all components involved are well protected. In light of the nature of APTs we presented several recommendations, some of them being classic such as penetration tests, access control, security monitoring and response, and patch management. We also suggested that the definition of critical information infrastructure be expanded to include certificate authorities and companies that provide security products or services to the public. Furthermore we propose that an international body should be established to ensure governance of these infrastructures and assets. People security is an aspect often left out of the equation in favor for sophisticated technologies and we emphasized on assessing the robustness of the human factor.

A resilient defense against the APT is a daunting task but can be made possible by proper management of these various components.

6. Acknowledgement

This research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education, Science and Technology(grant number: 2012-0008447).

References

[1] Command Five Pty Ltd: Advanced Persistent Threats: A Decade in Review. (2011)

[2] Fallier, N., Murchu, L.O., Chien, E.: W32.Stuxnet Dossier. Symantec Security Response. (2011)

[3] ZDNet: Up in cyber arms: AusCERT 2012. http://www.zdnet.com.au/up-in-cyber-arms-auscert-2012-339338008. [Accessed May 18, 2012]

[4] Miller, C.: The Legitimate Vulnerability Market. Independent Security Evaluators. (2007)

[5] Marpaung, J.A.P., Sain, M., Lee, H.J.: Survey on Malware Evasion Techniques: State of the Art and Challenges. In: 14th International Conference on Advanced Communication Technologies, pp 744-749. (2012)

[6] Albright, D., Brannan P., Walrond, C.: Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? Institute for Science and International Security. (2010)

[7] Rivner, U.: Anatomy of an Attack. RSA Blog. http://blogs.rsa.com/rivner/anatomy-of-an-attack. [Accessed May 18, 2012]

[8] Zetter, K.: RSA Agrees to Replace Security Tokens After Admitting Compromise. Wired.com. http://www.sired.com/threatlevel/2011/06/rsa-replaces-securid-tokens/. [Ac-cessed May 18, 2012]

[9] Bradley, T.: Hackers target Google, Skype with rogue SSL certificates. InfoWorld.com http://www.infoworld.com/d/security/hackers-target-google-skype-rogue-ssl-certificates-603. [Accessed May 18, 2012]

[10] Leyden, J.: Inside ‘Operation Black Tulip’: DigiNotar hack analyzed. The Register. http://www.theregister.co.uk/2011/09/06/diginotar_audit_damning_fail. [Accessed May 18, 2012]