산업융합연구 제16권 제2호 pp. 25-31, 2018
ISSN 1738-2289
https://doi.org/10.22678/JIC.2018.16.2.025

A Study on the Countermeasures against APT Attacks in Industrial Management Environment

Sunghyuck Hong*
Div. of Information and Communication, Baekseok University

산업경영환경에서 지속적 APT 공격에 대한 대응방안 연구

홍성혁*
백석대학교 정보통신학부

요 약 An APT attack is a new hacking technique that continuously attacks specific targets and is called an APT attack in which a hacker exploits various security threats to continually attack a company or organization's network. Protect employees in a specific organization and access their internal servers or databases until they acquire significant assets of the company or organization, such as personal information leaks or critical data breaches. Also, APT attacks are not attacked at once, and it is difficult to detect hacking over the years. This white paper examines ongoing APT attacks and identifies, educates, and proposes measures to build a security management system, from the executives of each organization to the general staff. It also provides security updates and up-to-date antivirus software to prevent malicious code from infiltrating your company or organization, which can exploit vulnerabilities in your organization that could infect malicious code. , And provides an environment to respond to APT attacks.

Key Words : Industry Convergence security, Hacking, Network security, Policy convergence, Security policy

Abstract APT공격은 특정 목표를 두고, 지속적으로 공격하는 신종 해킹기법으로 해커가 다양한 보안위협을 악용해 특정 기업이나 조직의 네트워크에 지속해서 공격하는 것을 APT 공격이라고 한다. 특정 조직 내부 직원의 PC를 장악한 후, 내부 서버나 데이터베이스에 접근하여 개인정보 유출 사고나 중요자료 유출과 같이 기업이나 기관 내 중요 자산 탈취에 성공할 때까지 공격하는 것이 특징이다. 또한, APT 공격은 한순간에 공격이 이루어지지 않고 있으며, 수년에 거쳐 이루어지므로 해킹 감지가 어렵다. 본 논문에서는 지속적인 APT 공격에 대해 고찰하고, 대응방안을 제시하여 각 조직에 근무하는 경영진부터 일반 직원까지 보안 필요성을 인식하고 교육하고 보안 관리체계를 구축을 목표로 한다. 또한, 보안 업데이트, 최신 백신을 설치하여 악성코드 침투를 예방하는 방법을 제시하여 기업이나 조직은 항상 해킹당할 수 있다는 인식을 심어주어 조직 내에 근무하는 사람들은 악성 코드가 침투할 수 있는 취약점을 설명하고, APT공격에 대응할 수 있는 환경을 제시한다.

키워드 : 산업융합보안, 해킹, 네트워크 보안, 정책융합, 보안정책

1. Introduction

In Korea, serious security accidents such as data deletion through the hacking of the NACF system, network paralysis, and leakage of Hyundai Capital

*Corresponding Author : Sunghyuck Hong(shong@bu.ac.kr)
Received May 7, 2018 Revised May 29, 2018
Accepted June 15, 2018 Published June 30, 2018

customer information have continued to occur and become important social 1738-2289 problems[1].

These security incidents, when compared with existing security incidents, are characterized by continuous and long-time attempts by organizations with a specific purpose, such as government or private enterprise, aimed at acquiring important information to be. This special purpose group is called ATP (Advanced Persistent Threat) attack by continuously collecting information by using various techniques for a single target, finding weaknesses, and damaging the target based on such information.

The ATP attack is a much more detailed and intelligent attack than the previous attacks in that it collects and attacks the information of the object in a long term by accurately referring to the specific object unlike the existing unspecified attack.

2. Related Research

2.1 APT

APT stands for Advanced Persistent Threat. It is an attack in which an attacker collects information of a specific object in the long term and finds the weakness of the target based on the information and damages it. The term APT is not a recently defined term, but its origins began at the US Air Force Command. The US Air Force Command used the term APT to mean a specific form of threat identified for smooth communications between the US Department of Defense and government agencies. In APT, Advanced refers to the technical scope, not only to use a specific technique, but also to use various attack methods for the purpose. Persistent means that this organization should continue to do new attacks and methods for some purpose. Threat is a threat in the field of information protection, and it contains social engineering techniques such as vulnerability, hacking, malicious code, etc., rather than attacking only within a defined frame, but analyzing a specific object and performing various attacks based on it.

2.2 APT Attack Method

APT attacks are basically classified into seven attack methods such as zero-day attacks, social engineering techniques, privilege escalation, persistence, adaptation, preliminary investigation and concealment.

- Preliminary investigation: It is a step carried out to analyze target attack target and find attack method to achieve final goal.
- Zero-Day Attack: By using weakness of security, it means attacking attack target by using virus that is not detected in existing security system.
- Social engineering technique: means sending emails or SNS attachments with zero-day weaknesses.
- Elevation of Privilege: This means collecting information through concealment after successful primary attack, collecting personal information such as password for system access, and also including brute force attack to collect account information.
- Concealment: Collecting information by disguising as a normal account, collecting information as much as the account can access through a legitimate account.
- Persistence: Gathering information over a long period of time involves setting up a backdoor to continue access to the target even after the removal of critical information.
- Adaptation: Contains countermeasures such as preventing attacks from being encrypted by encrypting them to the server inside the attacking target, and what to do when an attack is detected or an attack is detected[2].

2.3 APT Attack Examples

<Table 1> Examples of International APT Attack

Institution	damage scale	Detail
Sony Hack	Customer information leak	100 million personal information leak of Sony
EMC / RSA Hacking	Security Authenticati on Technology (OTP)	After collecting attack target information with sns, social engineering technique, virus infection
Morgan Stanley Hack	Industrial secret leak	Google and Morgan Stanley hack, hacking key information inside
Global energy	Corporate hacking Manufacturi ng / sales related confidential data leakage	After acquiring internal account information through spear phishing, after accessing the target information server
Iran Nuclear Power Station Paralysis	Nuclear power plant System paralysis	1,000 centrifuges used to exploit weaknesses in Zero-Day techniques Normal PC infecting internal information scan confidential
Embassy hacking in over 100 countries National secret leak	National secret leak	Government confidential leak after government infiltration
Pentagon Hacking Aerospace	National secret leak	Lasted about one year

There are many examples of APT overseas cases as shown in Table 1. Global energy company hacking has been attacked from China server for about two years since 2009 and through the server built in that process, it has been able to use computer systems of various countries such as Kazakhstan and Taiwan to collect important documents such as production system oil exploration I pulled it out.

And the Iranian nuclear power plant hack was attacked using a malicious code called Stuxnet, through which Iran lost 20% of the centrifuges in the nuclear power plant. This attack was carried out through four Zero Day Vulnerability weaknesses within the nuclear power plant and is a good example of a highly sophisticated APT attack.

<Table 2> Examples of Domestic APT attack

Institution	damage scale	Detail
3.20 Computeri zation	Major broadcastin g financial network paralysis	Infected internal PC to exploit authentication weaknesses
Nexon Maple Story Hack	Customer information leak	Infecting internal PC to leak personal information
SK Communic ations Hack	Customer information leak	Leaked personal information of 35 million subscribers stored in Nate
Nonghyup Hacking	Service paralysis	Infected laptop for server management and collect information after occupying the inside
Hyundai	Customer	Hijack customer

Capital	information leak	information by hijacking retired employee accounts
Auction hack	Customer information leak	Leaked customer information after infiltration of internal PC via e-mail

In Korea, there are many cases as shown in Table 2. Of these, 35 million personal information of SK Communications leaked in July 2011. The number of personal information leaked is the biggest accident. An internal PC was used as the attacker's attack path, and the attacker entered the inside using the update server vulnerability of the unauthorized SW used by internal personnel. The attacker took control of the DB administrator PC and the developer PC through ongoing internal investigation. Through this, we accessed the personal information database and collected information and then leaked it to the outside.

The NACF hacking incident that occurred in April 2011 is a good example of not only technical security but also administrative security. The NACF did not manage PCs (notebooks) for servers and changed server passwords. Administrative loopholes were exploited by attackers to provide financial services for 18 days. While distributing the malicious code disguised as a Web hard site program, the attacker realized that the NACF administrator PC was infected and monitored the notebook for about 7 months and tried to attack it. As a result of this attack, 550 internal servers were damaged and the server for disaster recovery was destroyed and could not be used. It is known that this aggravated hacking accident caused at least 8 billion won damage.

HYUNDAI CAPITAL Hacking was a leak of customer information in April 2011. At this time, the attacker used the information of the retired employee to access the internal server and extract about 1.75 million customer information.

3.20 The computer offense attack was prepared in preparation for intrusion over a long period of time, and on March 20, 2013, three domestic major broadcasters and three banks were paralyzed[3].

2.4 Intelligent attack technology of APT

The APT attack is a more sophisticated and intelligent attack method than the previous hacking techniques, such as thorough preparation and attack target setting, rather than a simple attack. We need to know what intelligent attacks are in order to defend them first, so we will explain some of the attacking techniques that are being used recently[4].

2.4.1 Spear phishing

Phishing means attacking an unspecified number using a fake Internet site, but spear phishing means attacking certain objects. It is a typical method to send e-mails that spoof trusted agencies, companies, people, etc. by means of spear phishing method. Recently, it has been used through a method of clicking on malicious links using sns.

2.4.2 PDF Attack

A PDF attack is an attack method that is used continuously by an attacker trying to trick users into a new way by using the weak points of the PDF and sending or distributing the malicious code in the PDF file. This method of attack is the most vulnerable to the endpoint, so it has a high success rate, and even if you do not have the information or important information you want to get at the specific endpoint, you may still have access to other endpoints, It is a frequently used attack method in APT attack. Especially in terms of attack effectiveness and versatility, this attack method is widely used because it is effective.

2.4.3 Zero-day malware

Most of the malicious codes used in APT attacks are zero-day malware that is not detected by programs that catch viruses. There is a lot of difficulty in finding out because it is developed and used in a way that is specialized for attacking attack target. Zero-day malware uses a variety of methods to avoid detection of security programs, such as randomly assigning a folder or file name where malicious files are stored, and changing an executable file every time a new infection occurs [7]. The hacker's script is executed in the user's web browser[6].

2.4.4 Response of APT attack

In the past, APT attacks are intelligent, sophisticated and very dangerous, and they continue to evolve and explain how they are used. In order to cope with APT attack more effectively, it is necessary to strategically analyze APT attack and systematically approach it, and to repair and reconstruct internal security management system. So, I explained some important ways of how to respond more effectively to APT attacks.

2.5 Security Management and Operation

The APT attack analyzes the security system of the target that is the attack target, analyzes several weaknesses based on the analysis, and runs through the gathered information. Therefore, in order to respond to the APT attack, the security system of the organization is first analyzed, The overall vulnerability and security risk of the organization should be analyzed and reorganized. In order to improve the security system, the overall security policy and operational method should be thoroughly checked in the upper security policy to analyze the organization's risks and respond accordingly And plans should be established and implemented. In order to continue to operate this security system after restructuring the security system, it is more important than ever to continue to manage the overall security management around the security management organization. In order to confirm this effect in performing security management and operation, security consulting including various methods such as security control and static simulation hacking may be an important method.

2.5.1 Strengthening Security Education

One of the most effective ways to deal with APT attacks is to actively involve members of the organization because the attack methods are so diverse, persistent and detailed. In this way, effective education is required for the entire USA organization, and in particular, employees who are judged to be vulnerable to APT attacks in the security system analysis phase are distinguished from each other, If employees are taught how to respond, they may be the primary line of defense against APT attacks. In many organizations, security education can often be seen as a formality that mimics only the method. For example, I can often see firefighting education in the army, and sexuality education in school. However, in order to effectively cope with APT attacks, educating members of the organization is effective education rather than formal education. If educated employees receive suspicious e-mails or computer problems, they will be able to know and defend themselves . In this analysis, it is necessary to educate the attacker about the attack of APT attack and to be able to cope effectively with a lot of information.

3. Conclusion

Through this paper, we describe the APT attacks that are approaching serious threats both at home and abroad. The APT attack is much larger than the attacks with the personal goals, which are the targets of the existing attacks, and the APT attacks

are fairly large in order to cope with the APT attacks in that they are prepared for a long period of time and have specific purposes such as political or monetary policy. Difficulties exist. Nonetheless, recent cases of APT attacks continue to be analyzed, and new APT attack methods have been continuously released, and countermeasures have been actively developed through the efforts of various people. It is important for the APT attack to ensure that the members of the organization receive effective education and systematically cope with the situation in order to cope with the persistent digging of a specific object for a long period of time. To this end, the security solution program that is operated by the organization should not have individual functions but should be structured as a concept of a more systematic and tightly connected security solution.

ACKNOWLEDGMENTS

This research is supported by 2018 Baekseok University Research Fund.

REFERENCES

[1] Best Practices for Big Data Analytics. (2015). Big Data Analytics, 93-109

[2] Hong, S. (2013). The Counter Attack for Physical Attacks on Wireless Sensor Networks by Secure and Optimized Group Diffie-Hellman. *International Journal of Advancements in Computing Technology, 5(11), 227-232*

[3] M.G.Lee, C.S.Bae. (2013). A Study on the Major Cases of APT Attack. *Korea Electronic Engineering Association conference, 939-942.*

[4] Hong, S. (2015). Two-channel user authentication by using USB on Cloud. *Journal of Computer Virology and Hacking Techniques, 12(3), 137-143*

[5] Mun, H., Hong, S., & Shin, J. (2017). A novel secure and efficient hash function with extra padding against rainbow table attacks. *Cluster Computing,* 21(1), 1161-1173

[6] S.H.Ji, H.G.Kim. (2012). A Study on the Effective Detection of Malicious Codes through Automatic Decoding of obfuscated JavaScript *Journal of the Society for Information Protection, 22(4), 869-882.*

[7] M.C.Lee, D.S.Moon, I.G.Kim. (2015). Fast data-based real-time abnormal behavior detection system. *Journal of the Society for Information Protection, 25(5), 1027-1041.*

[8] J.Kim. (2017). IP Spoofing Detection detection to enhance endpoint security. *Journal of the Information Technology Association of Korea, 15(8), 75-83.*

[9]J.W.Chei, Y.J.Lee, J.M.Park. (2012). E-DRM-based privacy technologies to overcome DLP-enabled problems. *Journal of the Society for Information Protection, 22(5), 1103-1113.*

[10] Y.J.Song, J.M.Do. (2010). Proxy-based access to medical data. *A Study on the Internet e-commerce, 10(3), 235-248.*

[11]Hong, S. (2013). The Counter Attack for Physical Attacks on Wireless Sensor Networks by Secure and Optimized Group Diffie-Hellman. International. *Journal of Advancements in Computing Technology, 5(11), 227-232*

[12] Kilroy, R. J. (2011). "Obamas Wars," Bob Woodward, (New York, NY: Simon and Schuster, 2010). *Journal of Strategic Security, 4(2), 121-123.*

[13]Hong, S., Lim, S., & Song, J. (2011). Unified Modeling Language based Analysis of Security Attacks in Wireless Sensor Networks: A Survey. *KSII Transactions on Internet and Information Systems, 805-821*

[14]Fang, X., Zhai, L., Jia, Z., & Bai, W. (2014). A Game Model for Predicting the Attack Path of

APT. *2014 IEEE 12th International Conference on Dependable, Autonomic and Secure Computing*

[15] Galatas, I. (2008). Medical Countermeasures Following Terrorism CBRNE Attack in Urban Environment. *In Resilience of Cities to Terrorist and other Threats (pp. 401-415). Springer, Dordrecht.*

홍성혁 (Sunghyuck Hong) [정회원]

- 2007년 8월 : Texas Tech University, Computer Science (공학박사)
- 2007년 9월 ~ 2012년 2월 : Texas Tech University, Office of International Affairs, Senior Programmer
- 2012년 3월 ~ 현재 : 백석대학교 정보통신학부 부교수
- 관심분야 : 영지식증명, 블록체인, Network Security, Hacking, Secure Sensor Networks
- E-mail : shong@bu.ac.kr