March - April 2020
ISSN: 0193-4120 Page No. 4045 - 4051

A Study on the Response Model to Malware Distribution through Update Servers

Yangha Chun
Assistant Professor, Department of Computer Science and Engineering,Yongin University, Republic of Korea.
yangha00@yongin.ac.kr

Article Info
Volume 83
Page Number: 4045 - 4051
Publication Issue:
March - April 2020

Abstract
Hackers are endeavoring to infect specific or undesignated systems by distributing malware as a preliminary step to cyberterrorism and hacking, such as through an APT attack or DDoS. Here, they abuse the updating servers of commonly used software programs to easily distribute their malware.

The problem of malware distribution through updating servers can be summarized as having two causes: absence of authentication procedures during updating, and absence of response measures in case of authentication certificate leak for code signing in a normal updating program. If an updating server has been hacked, the hacker can easily replace the normal updating program with malware, which is difficult to detect. Also, it is not easy to detect an infection because the client program in PC automatically downloads, installs and executes the updating file through the automatic update function.

As existing updating systems simply consist of 2 approaches, they may be efficient for quick updating but are exposed to threats, as malware can be transmitted in addition to normal files. These systems cannot confirm whether the PC user has updated using normal files or malware. As the safety and security of updating servers cannot be guaranteed, these systems are vulnerable to cyber-attacks that replace normal files with malware.

The security update server model is proposed to solve this problem. The security updating service model presented above blocks malware distribution, even if the updating server has been hacked, and notifies the corporation of any leaks of the code signing certificate in real time, in addition to reliably reporting the results of real-time authentication on the normality of the updating program by a third party for effective certificate security.

This study suggests several measures and models that can be applied to fundamentally block malware distribution via program updating servers.

Article History
Article Received*: 24 July 2019*
Revised*: 12 September 2019*
Accepted*: 15 February 2020*
Publication*: 26 March 2020*

Keywords: *Malware, Update system, Cyber attack, Intelligent Continuous attack, Cyber crime, Cyber security*

1. Introduction

Cyber terror has arisen and developed as networks and the Internet developed[1]. APT(Advanced Persistent Threat, APT) is defined as an intelligent, persistent attack that uses unknown new or variant malware and new vulnerabilities[2,3]. Advanced persistent threats(APT) are one of the hot spots of security issues[2]. Attacks of advanced persistent threats appear as infiltrations, searches, collections, and outflows, and are based on military and monetary objectives[4,5]

Cyberterrorism has been an ongoing issue since 2009. It has long been known that North Korea has been behind a number of cyberterrorist attacks, including the DDoS attack of July 7, 2009; the DDoS attack and Nonghyup computer network

attack of March 4, 2011; the attack on the newspaper production system of Jungang Ilbo in 2012; the cyber-attack on media and financial networks on March 20, 2013; and cyber-attacks on governmental and media networks on June 25, 2013. In addition to these incidents, massive cybercrimes continue to occur: the personal information leakage Auction Co. in 2008; leakages from SK Communications Co., Ltd. and Nexon Co., Ltd. in 2008; and leakages from the Educational Broadcasting System (EBS) and KT Corporation in 2002[6,7].

While these repeated cyber-attacks and crimes tend to be orchestrated by the same attackers, there are certain technical characteristics of the attacks that are common across different attackers. The attacks commonly employ malware that is distributed right before the attack, and the method of distribution has been consistent for years[8]. Hackers target the automatic updating servers of certain service providers connected to widely used programs in order to distribute their malware to targeted PCs[9]. In the past, attackers would hack the updating servers of file sharing websites (referred to in Korea as 'web hard') to replace the normal program with their malware, enabling them to infect massive numbers of PCs. More recently, they have been hacking the updating servers of utility programs, such as renowned security and anti-virus programs or video players, to distribute malware in the same way[10,11].

It is not practically possible to ensure the updating servers of countless corporations maintain perfect security[12]. But one way for corporations to be free from this risk would be to share a third-party authentication server that guarantees safe program updates and authenticates the program distributed by the corporation. In order to do this, they will need a server directly operated by a reliable organization, and their procedures and types of updates will need to be standardized to some degree.

2. Methods

Major cases of updating server hacking: Analyses on major cyber-attacks and crimes in recent years have found that the updating servers of various software programs were consistently targeted by hackers to distribute their malware.

2.1 Current updating system

DDoS attack of July 7, 2009: This incident paralyzed 35 websites, including those of major Korean and American organizations, for 3 days from July 7 to 9. Following a planning period that is believed to have lasted for 4 months, the attackers launched the largest DDoS attack in history by infecting approximately 27,000computers via 442 servers in 61 countries

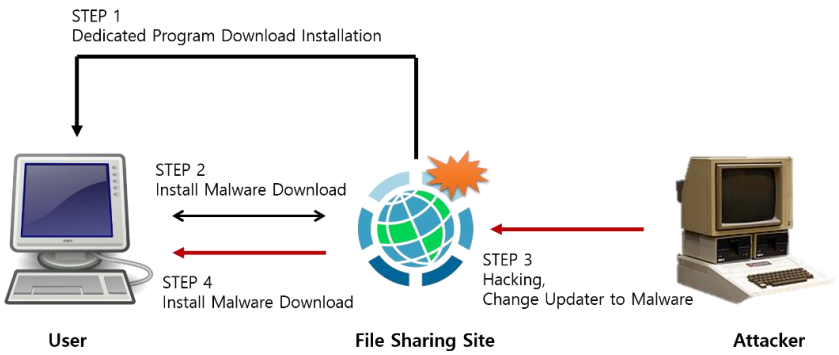

Figure 1. Malware distribution through an updating server.

around the world[13,14]. An analysis of North Korea's method of malware distribution showed that the attackers hacked two file sharing website servers to replace the updating program (.exe) with malware. Afterwards, the file sharing program in PCs that visited the file sharing website auto-upgraded to download the malware file, instead of the normal updating file, resulting in the infection of countless PCs that were then used for crime. Figure 1 shows the process of malware distribution through an updating server. The first incident was the second cyber-attack from North Korea on 40 major websites in South Korea, including the website of the Blue House, for 3 days from March 3 to 5. It is believed the attackers planned this attack for 7 months, and infected approximately 100,000 PCs via 746 servers in about 70 countries around the world. The attack used the same method as the previous attack, hacking the server of a file sharing website to replace their updating program (.exe) with malware. This incident was followed by heated criticism of security companies, as it repeated the damages of the same cyber-attack a second time[15].

The second incident distributed malware to infiltrate the intranet of major online game companies in South Korea, and leaked internal information, such as server programs. The hackers hacked the updating server of Gom Player of Gretech Co. Ltd. so that it would distribute the normal updating program to general users and malware to the IP addresses of certain game companies. The hackers distributed malware selectively according to the IP addresses of the targets through the .htaccess file (limited access setting file on a web server) provided from the web service program of the Linux server.

The third incident involved the leakage of the personal information of about 35 million users (the largest number from a single website) to China from July 26 to 27. Hackers infected the intranet PCs of the employees of SK Communications Co. Ltd., who managed the user accounts of Nateon and Cyworld, with malware, and then used these zombie PCs to infiltrate the database server where personal information was stored via the server network. Here, the hackers abused the updating server of 'Alzip,' a widely used software program by East Soft Co., Ltd., to infect the intranets with zombie PCs. They hacked the updating server of 'Alzip' by East Soft Co., Ltd. (a security company) to distribute the normal updating program to general users and send malware to the intranet IP addresses of SK Communication Co., Ltd. The hackers distributed malware selectively according to the IP addresses of the access target by using the ISAPI function provided by the web service program of the Windows server.

At the last incident hackers distributed malware to infiltrate the intranet of popular game companies in South Korea in order to hack the PCs of the employees, through similar methods that were used in the first attack in 2011. The hackers hacked the program updating server of Hangul by Hancom Inc. to modify the jsp file where the updating functions and setting contents were saved to distribute the normal updating program to general users and send malware, saved on a server in the United States, to the IP addresses of the intranets of certain game companies.

2.2. Current updating system of problems

The problem of malware distribution through updating servers can be summarized as having two causes: absence of authentication procedures during updating, and absence of response measures in case of authentication certificate leak for code signing in a normal updating program.

• Absence of authentication system for update

If an updating server has been hacked, the hacker can easily replace the normal updating program with malware, which is difficult to detect. Also, it

is not easy to detect an infection because the client program in PC automatically downloads, installs and executes the updating file through the automatic update function, and there is no authentication system that can detect any malware posing as a pre-saved normal updating program in the server. The lack of any updating authentication system caused this type of malware distribution to continue uninterrupted for years.

• Code authentication certificate leak

This section briefly summarizes the concept, principles and issues of the code signing certificate, which is widely used around the world to include producer information before a developed program is distributed to the Internet.

The code signing certificate is a means of authentication that electronically signs a program to indicate its completeness, reliability and safety to users before distribution and after corporate development. This concept applies to program distribution by developers in a manner similar to an authorized certificate that identifies and indicates an individual online.

For example, when a user downloads an execution program such as ActiveX from an online website, it is impossible for them to know whether the program is safe or malicious until they download, install and run it. On the other hand, if the distributor of the software program is indicated clearly, users will trust it more. Electronically signed programs can be downloaded with full trust in and responsibility of the distributor, even in the event of any risk of the program. Code signing certificates include the basic information (version, signature, algorithm ID, whole field signature), developer information (name of the issuer, effective period, open key information), user information (user name, effective period, open key information), etc. as an authorized certificate. The issuers of code signing certificates include the Korea Financial Telecommunications and Clearings Institute, among other organizations.

Problems with the code signing certificate: The fatal problem with the code signing certificate is its potential leakage by hackers. Imagine that a hacker has hacked a corporation and taken a code signing certificate. The hacker will electronically sign their own malware with the code signing certificate leaked from the corporation. If they distribute this electronically signed malware online, users will mistake this malware for the normal program distributed by the corporation and install it on their computers, resulting in the unrestricted distribution of malware. The corporation will detect the leakage of their code signing certificate and hurriedly dispose of that certificate. Here arises a serious problem: Unlike an authorized certificate that cannot be used once it is discarded, the code signing certificate can be used within the effective period even if it has been discarded, because there is no authentication procedure with regard to its discarded status. Therefore, there is no appropriate way for a corporation to respond to such leakage and prevent such abuse of the code signing certificate.

3. Results and Discussion

As the cases above show, hackers target the updating servers of widely used software programs as the most effective way of distributing malware, either to the masses or to specific groups. Once the updating server of the service provider has been hacked, it is incredibly easy to distribute malware. But while the risks and damages of malware distribution brought by the hacking threat of such updating servers are massive beyond assessment, it is impractical to expect the updating servers of the providers of widely used program services to maintain 100% perfect security. Therefore, for the security of the update server operated by each corporation, it is necessary to present a security update service model that reflects a mechanism that can take

March - April 2020
ISSN: 0193-4120 Page No. 4045 - 4051

responsibility for itself and standardize the update procedure and verify whether the normal update has been carried out.

3.1. Security updating service model

As existing updating systems simply consist of 2 approaches, as shown in Figure 2, they may be efficient for quick updating but are exposed to threats, as malware can be transmitted in addition to normal files. These systems cannot confirm whether the PC user has updated using normal files or malware. As the safety and security of updating servers cannot be guaranteed, these systems are vulnerable to cyber-attacks that replace normal files with malware.

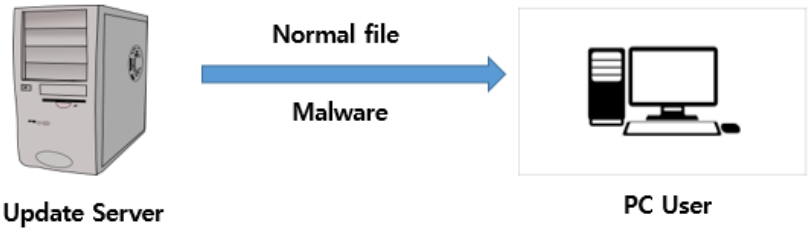

Figure 2. Procedure of the security updating service model

3.2. Procedure of the security updating service model

The security updating service model consists of 3 approaches, as shown in Figure 3. An updating authentication server is added to the conventional 2-way linear structure in a flat structure with PC in mutual communication with the updating server. The updating authentication server is independent from the updating server of the corporation, as it is operated by a reliable third-party organization or group. The authentication server shall have a web server supporting SSL and DB, communicate with the updating server of each program and engage in encrypted communication with user PCs in which updates are performed. The major information that shall be saved in the DB are emergency contact information (mobile phone number, email address) of the owner of the updating server, hash value information as the original information of the updating program files (date of distribution, updating server IP, size and hash value of the updating program file, etc.) and information of the electronically signed code signing certificate on the program (issuer, issuance subject, date of issuance and effective

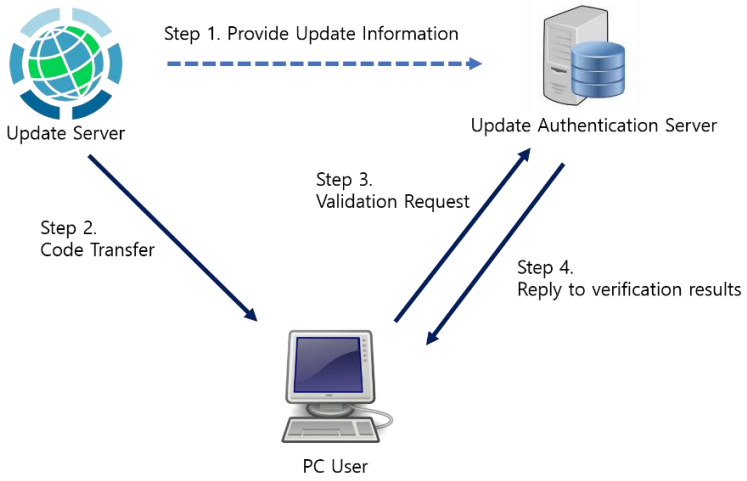

Figure 1. Security updating service model

period, etc.).

The procedure of the security update service model is as follows.

Step 1: An updating server transmits core updating information to the updating authentication server operated by a third party prior to distributing the updating files online. The transmitted information includes the hash value (MD5 or SHA1) of the updating program files to send the information about the currently effective code signing certificate. The updating authentication server that receives this information will save the information along with the information about the corporation to the DB server.

Step 2: The client PC accesses the updating server and downloads the updating program, and temporarily postpones installation and execution.

Step 3: The client PC accesses the updating authentication server of the third party, transmits the information about the program downloaded from the above updating server and requests authentication of its safety. Hash values and electronically signed certificate information on the program will be sent.

Step 4: The update authentication server compares the hash value and certificate information sent from the client PC with those saved in the DB server. With the hash value saved in the DB, it checks whether the normal updating files have been modified into other files – i.e., malware – and with the certificate information saved in the DB, checks whether the certificate is the one guaranteed by the corporation. If the hash values are different, the files are not the normal files distributed by the corporation, regardless of the consistency of the certificate information. And if the certificate information (particularly effective period) is different, the certificate has been leaked and electronically signed without authorization. If inconsistencies are found during the authentication process, an SMS or email will immediately be sent to the corporation operating the updating server.

Step 5: The client PC will determine to install and execute the updating files according to the authentication result of the updating authentication server. If the hash values and certificate information are consistent, updating will be completed; if any of the above is inconsistent, updating files will not be installed or executed.

4. Conclusion

The security updating service model presented above blocks malware distribution, even if the updating server has been hacked, and notifies the corporation of any leaks of the code signing certificate in real time, in addition to reliably reporting the results of real-time authentication on the normality of the updating program by a third party for effective certificate security. The corporation providing updates does not need to provide sensitive personal information to any third-party organization operating the updating authentication server other than minimal information for authentication, such as the hash values of the updating files and code signing certificate information, to guarantee safe and reliable updates in a simple structure.

If this model is actualized and used by multiple known online programs, further incidents of abusing those programs for massive malware distribution can be avoided, even if a corporation has been hacked. This can also provide an alternative approach to preventing massive malware distribution, which has been part of cyberterrorism and cyber-crimes since 2009. In sum, it is expected to build a safe social and national online environment for users.

March - April 2020
ISSN: 0193-4120 Page No. 4045 - 4051

References

[1] 1. 1.S.w. Lee, R. Gandhi, D. Muthurajan, D. Yavagal, G.-J. Ahn, “Building Problem Domain Ontology from Security Requirements in Regulatory Documents,” %1 Proceedings of the 2006 international workshop on Software engineering for secure systems. ACM, 2006.

[2] 2. J. D. Moffett, C. B. Haley, B. Nuseibeh, “Core Security Requirements Artefacts,” Department of Computing, The Open University, Milton Keynes, UK, Technical Report 23, 2004.

[3] K. D. Mitnick, W. L. Simon, The Art of Deception: Controlling the Human Element of Security, John Wiley & Sons, 2011.

[4] 4. “Security Technical Implementation Guides,” DoD CYBER EXCHANGE, 04 04 2019. [Internet] Available from: https://public.cyber.mil/stigs/srg-stig-tools/, 2019.

[5] 5. M. Ussath, D. Jaeger, F. Cheng, C. Meinel, “Advanced Persistent Threats: Behind the Scences,” %1 2016 Annual Con ference on Information Science and Systems (CISS) , 2016.

[6] B. I. Messaoud, K. Guennoun, M. Wahbi, M. Sadik, “Advanced Persistent Threat: new analysis driven by life cycle phases and their challenges,” %1 Advanced Communication Systems and Information Security (ACOSIS), International Conference on, IEEE , 2016.

[7] 7. I. Watson, “Case-based reasoning is a methodology not a technology,” Research and Development in Expert Systems, XV, 1999, pp. 213-223.

[8] S.-J. Kim, S.-W. Lee, “Social Engineering Based Security Requirements Elicitation Model for Advanced Persistent Threats,” , Singapore, Asia Percific Requirements Engineering Conference, 2017.

[9] 9. “Security Technical Implementation Guides,” DoD CYBER EXCHANGE, 04 04 2019. [Internet] Available from: https://public.cyber.mil/stigs/srg-stig-tools/

[10] 10. Chen, Ping, D. Lieven, H.Christophe, “A study on advanced persistent threats,” %1 IFIP International Conference on Communications and Multimedia Security , 2014.

[11] 11.W.A.J, G.P.B, “CHEAT, an approach to incorporating human factors in cyber security assessments,” %1 System Safety and Cyber - Security Conference 2015, 10th , 2015.

[12] SkyEye Helios Team, “OPERATION ONIONDOG -Diclosing Targeted Attacks on Government and Industry Sectors in Korea [White paper],” SkyEye, 2016.

[13] M. Bere, F. Bhunu-Shava, A. Gamundani, I. Nhamu, “How Advanced Persistent Threats Exploit Humans,” International Jounal of Computer Science Issues (IJCSI), 2015, 12th, 6, p. 170.

[14] Protecting Your Critical Assets Lessons Learned from “Operation Aurora” McAfee, 2010.

[15] Ahnlab “[Special Report] APT Attack Present and Countermeasures”, [Internet] http://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?menu_dist=2&seq=22113, 2014.01.