Involvers' Behavior-based Modeling in Cyber Targeted Attack

Youngsoo Kim and Ikkyun Kim
Cyber Security Research Laboratory
Electronics & Telecommunications Research Institute
Daejeon, Korea
e-mail: {blitzkrieg, ikkim21}@etri.re.kr

Abstract— **Cyber targeted attack has sophisticated techniques using malwares to exploit vulnerabilities in systems and an external command and control is continuously monitoring and extracting data off a specific target. Since this attacking process is working continuously and uses diverse malicious codes and attacking routes, it is considered to be difficult to detect in advance. In this paper, we categorized cyber targeted attacks into four steps and defined potential behaviors of involvers like attackers or victims, in order to make a model. Each behavior of our model can include a couple of methods. Furthermore, we applied our behavior-based model to the real targeted attacks, "3.20 South Korean Malware Attack" and "The Targeted Attack for SK Communications".**

Keywords-APT; Targeted Attacks; Behavior-based Modeling; Malicious Codes; 3.20 DarkSeoul.

I. INTRODUCTION

Cyber targeted attack, which is also known as Advanced Persistent Threat (APT), is a kind of intelligent attacking method having a goal of acquiring classified information or control of critical infrastructure, by penetrating networks of targets in a stealthy way and staying there in the long term. It usually targets organizations or nations for business or political motives. It has complicated techniques using malicious codes to take advantage of vulnerabilities in systems and an outer command and control is constantly observing and deriving data from a specific target [1]. This attacking method is working continuously and utilizes various malwares and attacking routes, so it is deemed to be hard to discover beforehand. In Section 2, we classified advanced persistent threat and described possible behaviors of involvers like attackers or victims for modeling. Each behavior of our model can include several methods. In Section 3, we introduced a couple of real targeted attacks and indicated that our behavior-based model is fit to depict them and described some useful cases of proposed modeling map, and conclude with some remarks and further works in Section 4.

II. EACH STEP OF BEHAVIORS/METHODS FOR CYBER TARGETED ATTACKS

Cyber targeted attacks can be divided into 4 phases: The preparation phase, the penetration phase, the control phase, and the achievement phase. Figure 1 depicts the detailed behaviors of attackers and victims.

In the preparation phase, attackers collect and analyze diverse data of targeting web sites, and they hack servers with vulnerabilities and make them Command and Control (C&C) servers. Also, they use various ways for triggering download of malicious codes. In the penetration phase, attackers try to acquire user authority using diverse methods and user's Personal Computers (PCs) can be infected with malicious codes by running malicious attached files, updating falsified software, or using unauthorized USBs. In the control phase, attackers try to acquire additional user authorities and collect additional information using various ways. They can also control victimized systems with backdoors or web-shells and spread malicious codes to all connected devices. In the achievement phase, attackers can acquire critical information using remote commands or web-mails and they can also emasculate systems using automatic termination or remote starting.

A. The Preparation Phase

If attackers decide attacking targets, they visit targeting web pages for looking into vulnerabilities [2]. They could acquire user information by falsifying URLs of targets. First, they register the targeting website and try to read web-board messages requiring the higher-level accessing authority. Even though they are rejected to access, they can watch an URL of web-board message which they want to read using right-hand mouse-clicking. And then, they try to falsify that URL to acquire user information without reading authority.

They can collect and analyze information related to targeting victims using web-crawlers or bots, which look around enormous web pages, including web sites providing Social Network Service (SNS), such as Facebook, Twitter, etc., to get information. They can also use meta-search engines connecting diverse searching engines for same reason.

Attackers hack servers (e.g., web-board, web-mail server, and web-disk) with vulnerabilities and make them C&C servers. After they acquire authorities of accessing the targeting servers using malicious codes, they falsify them to play a role of the C&C servers.

After that, attackers prepare for inducing the victims to download malicious codes in diverse ways. They could send e-mails including attached malicious codes to targeting users or attach them to web-board messages for triggering downloads. Also, they could falsify software of updating servers in case of installing. If they can do it, users download them and install falsified updating software unconsciously. They could use Cross Site Script (XSS) vulnerabilities in two

 ISBN: 978-1-61208-376-6

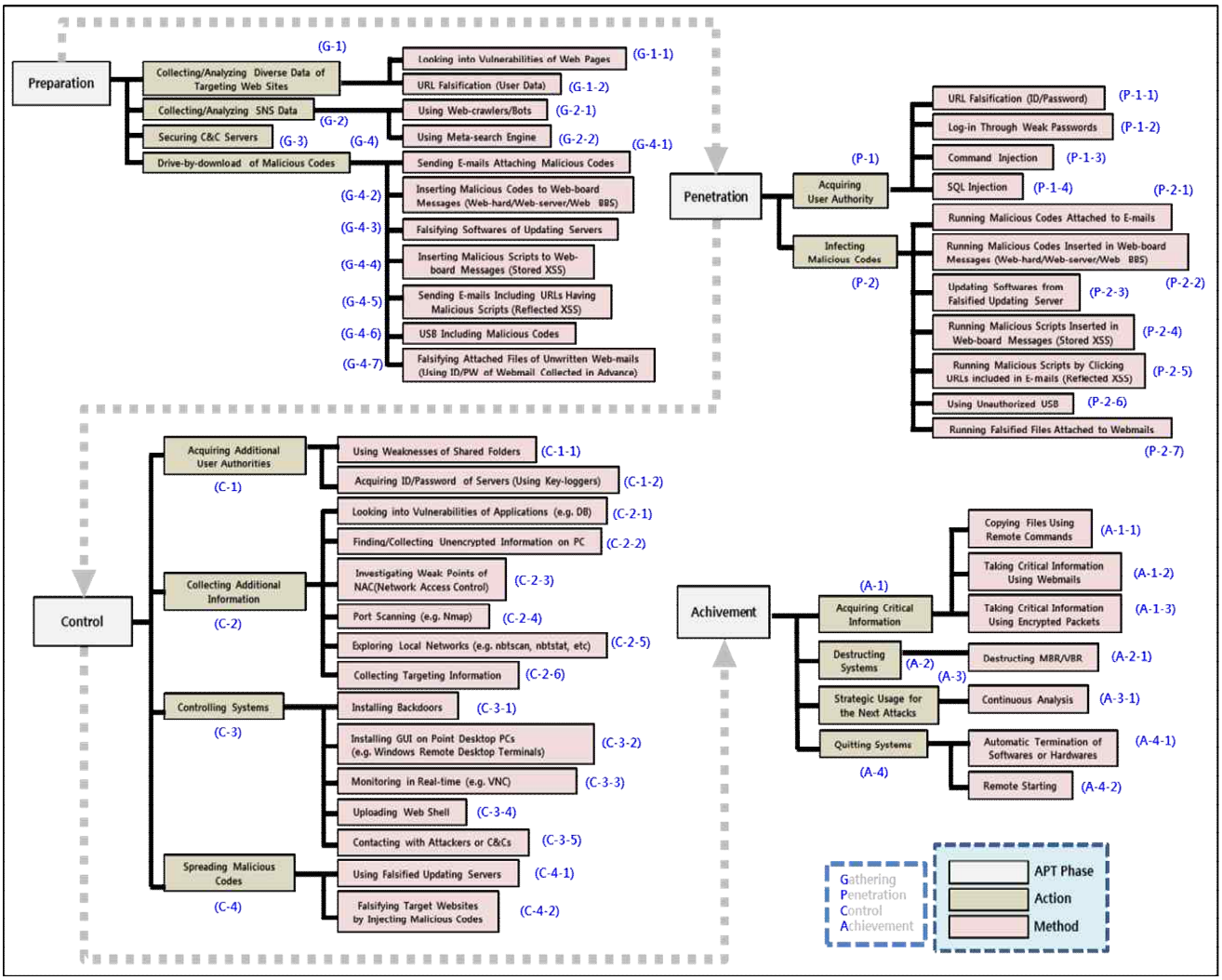

Figure 1. Each Step Behaviors/Methods for Cyber Targeted Attacks

ways, i.e., Stored XSS and Reflected XSS. Attackers can insert malicious scripts to web-board messages using XSS-vulnerability of the targets for triggering infection of malicious scripts. After they find that XSS vulnerability, they write web-board messages with malicious scripts and post those messages on the web-board [3]. They could also send e-mails including URL links of targeting web sites having malicious scripts to users for infection. After they find the XSS vulnerability of targeting web sites, they write e-mail messages including URL links having malicious scripts and send them to the targeting users in order to be infected by clicking those URL links. Sometimes, they prepare USB sticks including malicious codes and putting them on somewhere in the targeted area [4]. Also, attackers could replace attached files of unwritten web-mails with malicious files using ID/password of web-mail collected in advance. After they collect many pairs of ID/password, they check unwritten web-mails using collected ID/passwords and replace attached files with malicious files.

B. *The Penetration Phase*

After preparing, attackers try to acquire user authority using diverse methods, such as URL falsification, weak passwords, command injection, or SQL injection. They acquire user authority by falsifying the URL of targeting web site. First, they check a pattern of URL attributes of the targets and repeatedly access to those web sites by typing randomly changed URL links. They could login and acquire user authorities if randomized user-codes are matched. Sometimes, attackers acquire weak passwords using password cracking tools. Additionally, they run local system commands remotely because of the vulnerability of insufficient authorizing input variables [5]. First, they check the address of targeting web site. After injecting a system command to this address, they could access with this changes address. And then, they could see and get some system information. Finally, attackers could watch, falsify, or delete database data by fabricating input data of database application [6]. It occurs since database applications do not check the validity of input data from users. They could

 ISBN: 978-1-61208-376-6

bypass certificating process for users or administrators using SQL injection. After checking if they could input special characters to log-in windows, they input SQL commands to log-in windows and then, they become able to log-in without a certificating process.

User PCs can be infected with malicious codes in various methods. A user runs attached files of received e-mails including malicious codes and he becomes infected. When a user receives an e-mail attaching malicious files, he reads the message of that e-mail. And then, if he activates malicious attached files, he will become infected. If a user runs malicious files attached in web-board messages and he becomes infected. When a user clicks a message of web-hard, web-server, or web-board having attached malicious files, he runs attached malicious files. As a result, he becomes infected. Furthermore, a user could be infected through automatic activating of updating software falsified in advance. First, updating software having been falsified in advance are executed automatically. If a user activates the updating process or automatic updates are activated, the user's PC is infected. A user could be infected by reading a web-board message including malicious scripts. After accessing the web, a user read a web-board message having malicious scripts. And then, contents of the web-board message including malicious scripts are sent to the user. Finally, the user's PC is infected and the user's cookies are sent to the attacker. Sometimes, if a user receives an e-mail with a malicious URL link and accesses to that URL link, he could be infected by malicious scripts. First, he receives an e-mail including a malicious URL link and clicks that link. As a result, he can access a link having a malicious script, and the user PC is infected since the malicious script is activated. Finally, the user's cookies are sent to the attacker. Local systems could be infected by bringing and executing infected unauthorized USB sticks. If a user brings infected unauthorized USB sticks and he put them on local systems like PCs or servers, local systems are infected. A user could also be infected by running a falsified attached file of a web-mail. If a user logs in his web-mail account and checks an attached file of web-mail falsified by an attacker in advance, his PC is infected by executing the attached file.

C. The Control Phase

To achieve final goals, attackers try to acquire additional user authorities using weakness of shared folders or key-loggers and collect additional information using various ways such as port scanning, weak points of Network Access Control (NAC), vulnerabilities of applications, etc. Furthermore, they can control victimized systems by installing backdoors or uploading web-shells and spread malicious codes to all connected devices by falsifying updating servers or web servers of targets.

Attackers could access the shared PC if a pair of ID/password of the infected PC is same as that of the shared PC. After that, they could access the agent server at a time, if they install a scheduler like at.exe at the shared PC. If they log in with a pair of ID/password of infected PC, they try to access to the shared PC using the same pair. In case that the pair is the same, they could access. If they install a scheduler at the shared PC, they could access the agent server at a time. Additionally, all keyboard-typing logs on infected PCs could be recorded in real-time using key-loggers. First, attackers install a key-logging program on infected PCs. If users make use of the infected PCs, the key-logging program records all keyboard-typing logs in real-time. After receiving recorded logging data, attackers check and get some pairs of ID/password.

Attackers can get additional information by analyzing vulnerabilities of various web applications such as SQL injection, file upload, XSS, path traversal, cookies, parameter manipulation, configuration setting errors, admin page, backup/temporal files, etc. Attackers can also collect additional information by finding unencrypted folders or files in infected PCs. After logging in the infected PCs, they search all folders or files. If they find unencrypted ones, they can get additional information. Sometimes, attackers can find vulnerabilities of NAC by checking security policies or security solutions, and then, can access to the local network without authority checks. They find vulnerabilities of NAC by checking security policies or security solutions in order to access to the targeting local network. And then, they can access servers and check data to get information. Attackers can access the infected PCs and scan all ports to check whether they are open or not. They access the infected PCs and check opened ports using nmap command or port-scanning tools to get information. They can also check the status of local network, for example some PCs are grouping or some devices are powered off, by scanning such as nbtscan, nbtstat, etc. Additionally, attackers harvest target information related to the final goals. They access to the admin computer dealing with local information and find and harvest the target information.

Attackers can hide backdoor files in advance, and they get root authority by activating them to control the target system [7]. First, they access the infected PCs and make backdoor files. Backdoor files are compiled at temp directory. And then, they run backdoor files in a general account, they get root authority and become to be able to control the target system. Attackers can also control the targeting system by installing terminal programs for remote control and database accessing tools, after finding PCs operating 24 hours a day. First, they find PCs operating 24 hours a day, and they install database related tools and terminal programs for remote control. And then, they check database and logs on the mainframe computer. As a result, they become to control the targeting system and gets information. Sometimes, attackers acquire critical information and control the targeting system by monitoring the infected PCs with Virtual Network Computing (VNC). After accessing the infected PCs, they install a VNC program. If administrators or developers use the infected PCs, attackers can watch what they do with VNC. As a result, they can control the targeting system and acquire critical information. Attackers can acquire control of the target system by uploading a web-shell, a web script file (e.g., asp, jsp, php, and sci) usually made maliciously in order to run instructions on the targeting web server remotely [8]. First, they make a web script file and upload it on local web-board. After searching a URL enabling them to move

 ISBN: 978-1-61208-376-6

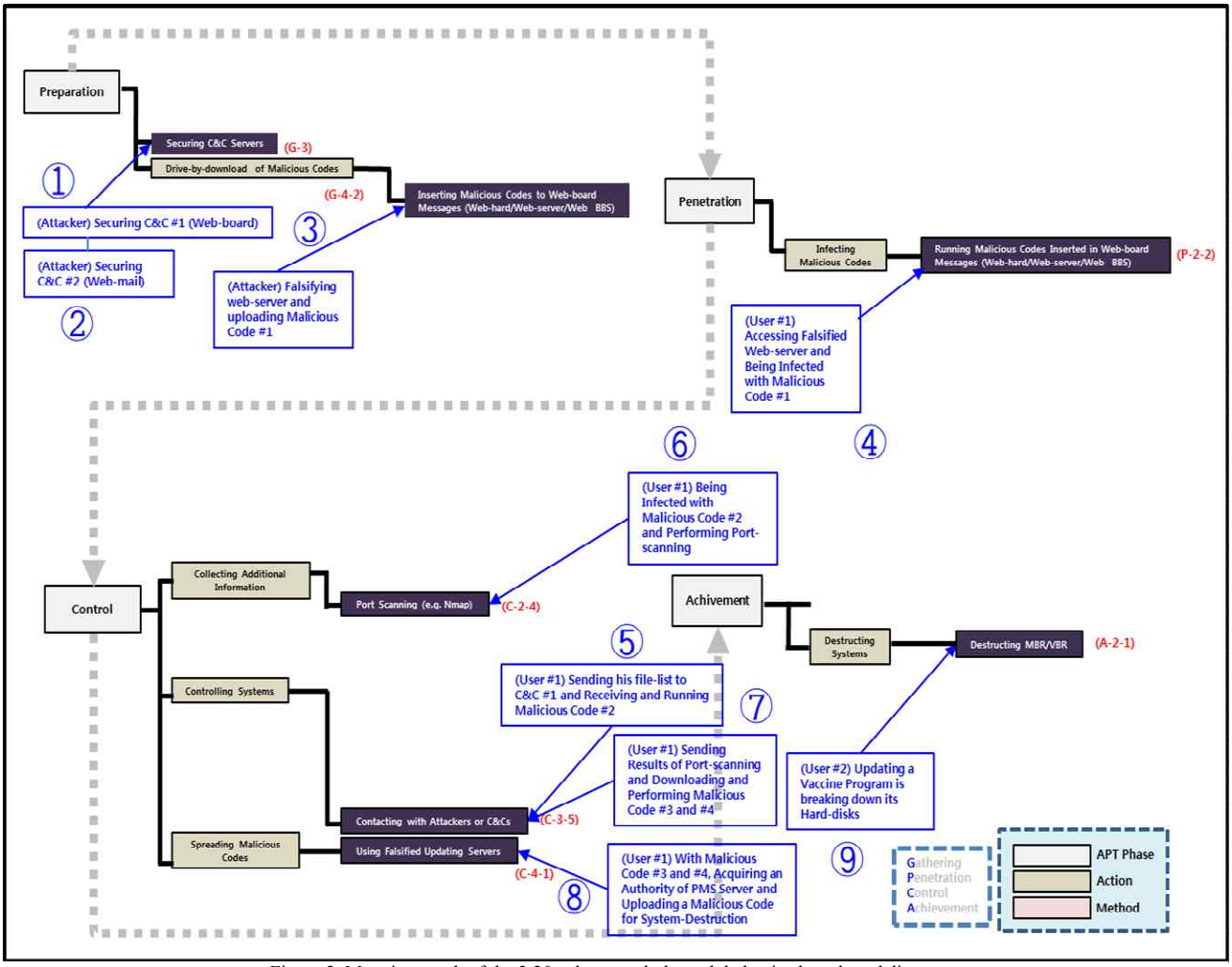

Figure 2. Mapping result of the 3.20 cyber-attack through behavior-based modeling map

into the uploading location using file attributes, they access the shell by entering this URL. And then, they get some system information by using some commands. Additionally, attackers connect the infected PCs with themselves or C&Cs for sending instructions or additional malicious codes to the infected PCs or receiving the targeting system information from them. After getting control of system, they send instructions or additional malicious codes to the infected PCs or receive the targeting system information by way of C&Cs.

Attackers can spread malicious codes using the updating server including falsified updating software. All PCs activating automatic updates can be infected. They can also trigger infection of malicious codes through adding falsified web pages or banners enabling users to access and click on them. They add web pages or banners including malicious codes to the target web server. And then, if users visit the targeting web site, their PCs are infected.

D. The Achievement Phase

In this phase, attackers can acquire critical information by copying files with remote commands or using web-mails or encrypted packets. Also, they can emasculate systems by destructing Master Boot Record (MBR)/Volume Boot Record (VBR), for example, or quit systems using automatic termination or remote starting.

Attacker can control infected PCs and take away critical files from them using a remote command like scp or web-mails. They can also encrypt packets of critical data using packet-extracting commands/tools and take them. Attackers run destruction commands for MBR/VBR of infected PCs and preclude system booting. Additionally, they can catch the following decisive opportunities by monitoring and analyzing infected PCs. Sometimes, attackers terminate the targeting system using commands for automatic termination of specific software or hardware or quit the targeting system using commands for remote starting.

III. MODELLING FOR REAL CASES

We applied our behavior-based model to two real targeted attacks. One was occurred in July of 2011 and the other was occurred in March 20, 2013.

 ISBN: 978-1-61208-376-6

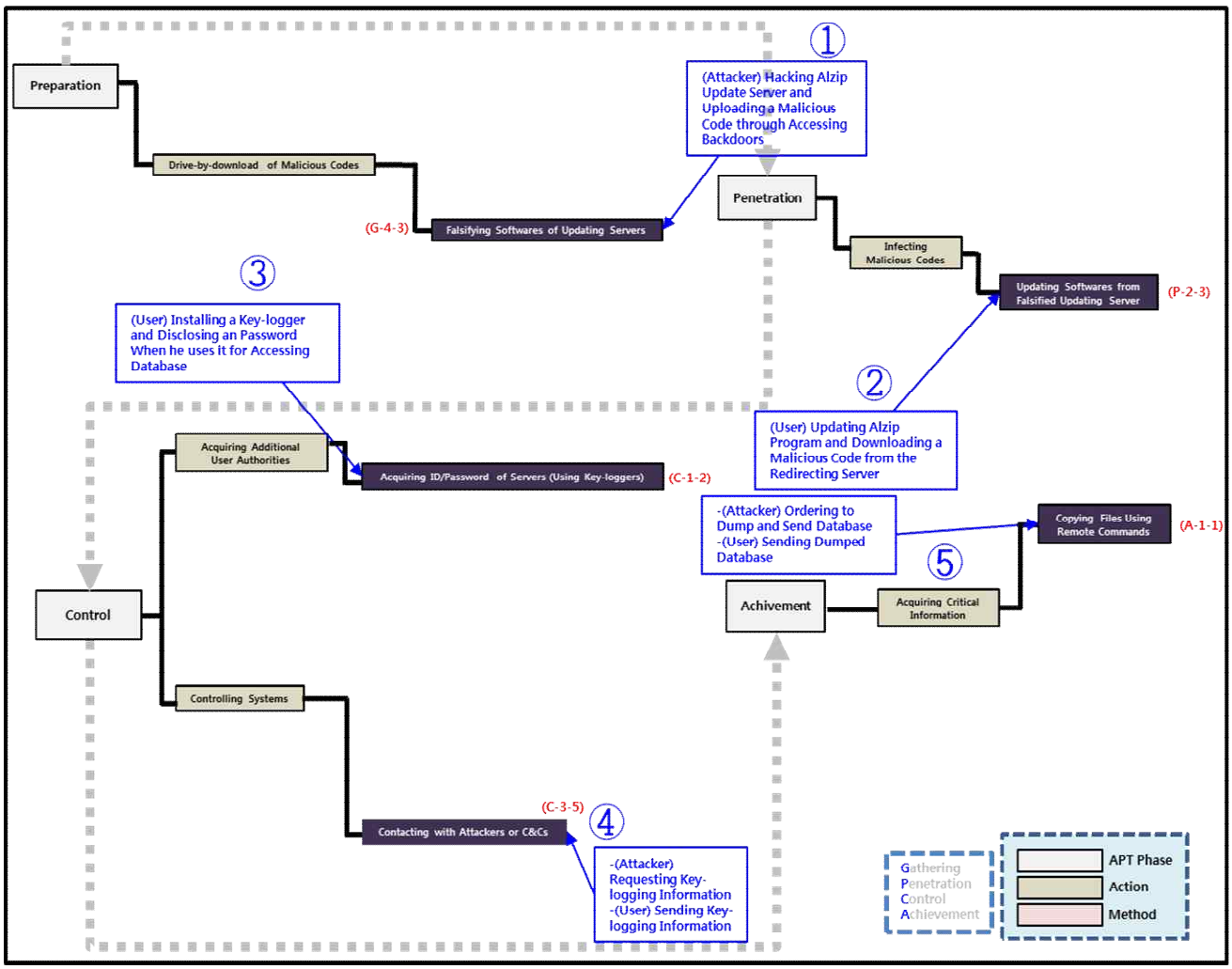

Figure 3. Mapping result of the Targeted Attack for SK Communications through behavior-based modeling map

A. *Modelling for 3.20 South Korean Malware Attack*

The attack, dubbed DarkSeoul, against South Korean media and banking organizations severely disrupted a handful of organizations with a coordinated distribution of "wiper" malware designed to destroy data on hard drives and render them unbootable [9]. It is known that the malware will overwrite MBR and VBR. The records and files overwritten by the malware so far have been wiped with patterns of 'HASTATI' or 'PR!NCPES'. We referenced some analysis reports and described detailed processes of this attack as follows [10]. We mapped 8 steps of this attack to potential behaviors we categorized. Figure 2 depicts the mapping result of the 3.20 cyber-attack.

1. An attacker secures C&Cs using vulnerabilities of web-boards or web-mails.
2. The attacker falsifies the (C&C #1 and C&C #2) web-server and uploads malicious code #1.
3. A user (User #1) accesses falsified web-server and is infected with malicious code #1.
4. User #1 sends his file-list to C&C #1 and receives and runs malicious code #2.
5. User #1 is infected with malicious code #2 and performs port-scanning.
6. User #1 sends results of port-scanning and downloads/performs malicious code #3 and #4.
7. With malicious code #3 and #4, user #1 acquires an authority of Patch Management System (PMS) server and uploads a malicious code for system-destruction.
8. Other users update vaccine programs and their hard-disks are broke down.

B. *Modeling for Targeted Attack for SK Communications*

Between 18 and 25 July 2011, attackers infected over 60 SK Communications computers and used them to gain access to the user databases. They infected these computers by first compromising a server belonging to a South Korean

 ISBN: 978-1-61208-376-6

software company, used to deliver software updates to customers (including SK Communications). Attackers modified the server so that the SK Communications computers would receive a trojaned update file when they conducted their routine checks for software updates [11]. We mapped 5 steps of this attack to potential behaviors we categorized. Figure 3 depicts the mapping result of the 3.20 cyber-attack.

1. An attacker hacks Alzip update server and uploads a malicious code through accessing backdoors [12].
2. A user updates Alzip program and downloads a malicious code from the redirecting server unconsciously.
3. The key-logger is installed in that user's computer and user's password can be logged when he uses it for accessing database.
4. The attacker requests and receives key-logging information.
5. The attacker orders to dump and send database and gets it from the key-loggers of user's PC.

This proposed involver's behavior-based model of cyber targeted attack could be useful for the following cases.

First, attacking methods are very diverse, so our model can be a basic scale for deciding whether the attack is cyber targeted attack or not. Second, generally cyber targeted attack can occur over a long period of time. If some behaviors related to cyber targeted attack can be found in its middle stages, the following potential behaviors can be prevented in advance, referencing to our model. Third, if some attacking behaviors are found in its middle stages or final stages, we can guess what happened in the beginning stages using our model. Fourth, since our model includes analysis points at each phase, it can be a guidance map for analyzing causes of hacking accidents. If cause analysis can be achieved rapidly, services delayed due to this hacking accident could be restored faster. Finally, according to 44 methods of our model, detailed analyses of devices relating to involvers can be done.

IV. CONCLUSION AND FUTURE WORK

We categorized cyber targeted attacks into 4 steps and defined potential behaviors of involvers like attackers or victims, in order to make a model. Each behavior of our model can include a couple of methods. Furthermore, we applied our behavior-based model to the real targeted attacks, "3.20 South Korean Malware Attack" and "The Targeted Attack for SK Communications" and described use cases. For testing, we are building the cyber hacking test-bed including routers, switches, servers, PCs, and notebooks. We have plans to make some APT-scenarios similar to real targeted attack like DarkSeoul, and implement them on the cyber hacking test-bed to verify our model.

REFERENCES

[1] N. Virvilis and D. Gritzalis, "The big four-what we did wrong in protecting critical ICT infrastructures from Advanced Persistent Threat detection?," The Eighth International Conference on Availability, Reliability & Security (ARES 2013), IEEE Press, Sep. 2013, pp. 248-254, doi:10.1109/ARES.2013.32.

[2] W. Gary and S. Zhendong, "Sound and precise analysis of web applications for injection vulnerabilities," Conference on Programming Language Design and Implementation (PLDI 2007), ACM, Jun. 2007, pp. 32-41, ISBN: 978-1-59593-633-2.

[3] M. Michael and L. Monica, "Automatic generation of XSS and SQL injection attacks with goal-directed model checking," Proc. of the Conference on Security Symposium (SS 2008), USENIX Association Berkeley, Jul. 2008, pp. 31-43.

[4] C. Harlan and A. Cory, "Tracking USB storage: Analysis of windows artifacts generated by USB storage devices," Digital Investigation, vol. 2, Jun. 2005, pp. 94-100, doi:10.1016/j.diin.2005.04.006.

[5] S. Zhendong and W. Gary, "The essence of command injection attacks in web applications," Conference record of the 33rd ACM SIGPLAN-SIGACT Symposium on Principles of Programming Language (POPL 2006), ACM, Jan. 2006, pp. 372-382, ISBN: 1-59593-027-2.

[6] W. Halfond, J. Viegas, and A. Orso, "A classification of SQL-injection attacks and countermeasures," Proc. of the IEEE International Symposium on Secure Software Engineering, IEEE, Mar. 2006, pp. 13-15.

[7] S. Gaspers and S. Stefan, "Backdoors to Satisfaction," The Multivariate Algorithmic Revolution and Beyond, Springer Berlin Heidelberg, pp. 287-317, Nov. 2012, ISBN: 978-3-642-30890-1.

[8] A. Straniery and Z. John, "WebShell: The development of web based expert systems," Research and Development in Intelligent Systems XVIII. Springer London, Dec. 2001, pp. 245-258, ISBN: 978-1-85233-535-9.

[9] US-CERT, "South Korean Malware Attack", 2013. https://www.us-cert.gov/sites/default/files/publications [Retrived: Oct, 2014].

[10] IssueMakersLab, "Operation 1Mission aka 3.20 DarkSeoul," http://www.issuemakerslab.com [Retrived: Oct, 2014].

[11] L. Moon-young, "Personal Information Hack Traced to Chinese IP address," The Hankyoreh Media Company, 2011. http://english.hani.co.kr/arti/english_edition/e_national/491514.html [Retrived: Oct, 2014]

[12] Altools, http://www.altools.com [Retrived: Oct, 2014]

 ISBN: 978-1-61208-376-6