Dark Seoul Cyber Attack: Could it be worse?

Jonathan A.P. Marpaung[1], HoonJae Lee[1]

[1]*Cryptography & Network Security Lab, Dongseo University*
San 69-1, Jurye 2-dong, Sasang-gu, Busan 617-716, Korea

[1]jonathan@spentera.com
[1]hjlee@dongseo.ac.kr

Abstract. On March 20, 2013 a cyber attack now known as Dark Seoul, paralyzed several major banking services and broadcasters in South Korea. Labeled by the media as cyber terror, the attack significantly disrupted these services for at least one day. Despite these facts, various indicators suggest that the attack had a low level of sophistication. Major cyber attacks in the past such as Ten Days of Rain and the SK Communications breach employed far more advanced techniques compared to Dark Seoul. We examine the technical details of Dark Seoul by outlining the primary attack vector used, describing the malware components, and discussing the malware's evasion techniques. Furthermore we compare this incident to previous attacks in order to determine its technical sophistication using these attacks as a relative benchmark. Lastly we explore various malware design techniques that were not used in the malware such as multiple propagation vectors, 0-day exploits, and evasion techniques, thus presenting a proof of concept of the malware's low technical sophistication.

Keywords: *advanced persistent threat; cyber attack; Dark Seoul; defense; malware analysis;*

A. INTRODUCTION

On March 20, 2013, at approximately 14.15PM South Korea suffered a cyber attack that resulted in the denial of service of several major banks and broadcasters. Reported as a major cyber attack, our analysis of the malware and attack vectors employed suggests that the malware had a relatively low level of technical sophistication. Firstly we explore the technical components of Dark Seoul to analyze the sophistication of the malware and attack vectors used. This analysis is based on information obtained from the media as well as technical reports of various malware research labs such as AhnLab, Imperva, Symantec, Avast, Kaspersky, Alienvault, and Sophos. Secondly we conduct a comparative study of Dark Seoul by looking at prior cyber attacks, namely Stuxnet, 10 Days of Rain, and the SK Communications breach. By doing so we draw a picture of South Korea's current security posture since those attacks. Lastly we discuss several design characteristics of advanced malware used by determined adversaries to carry out more technically advanced and stealthier attacks, therefore highlighting the components where Dark Seoul lacked sophistication.

B. POSTMORTEM

Television broadcasters YTN, MBC, and banks KBS, Shinhan, Nonghyup, and Jeju were targeted in this recent attack. The Korea Internet Security Agency (KISA) reported that about 48,000 computers were affected making services inaccessible and the victim organizations needed weeks to fully restore all functions [1]. In terms of impact, the attackers managed to successfully penetrate the target networks, pivot their way into critical assets, wipe out systems, cause denial of services, and trigger enough public response to spur the media into using terminology such as cyber terror and advanced persistent threats.

In this paper we take an in-depth look of the malware by examining the attack vectors used, and later discuss whether the claims in the media are warranted. According to the investigating team consisting of government, military, and civilian members, as many as 76 samples of malware were collected from infected machines [2]. We present the most likely primary attack vector used by the attackers by discussing information summarized from reports by Avast [3], Trend Micro [4], and Symantec [5][6] issued in the first few days following the attack.

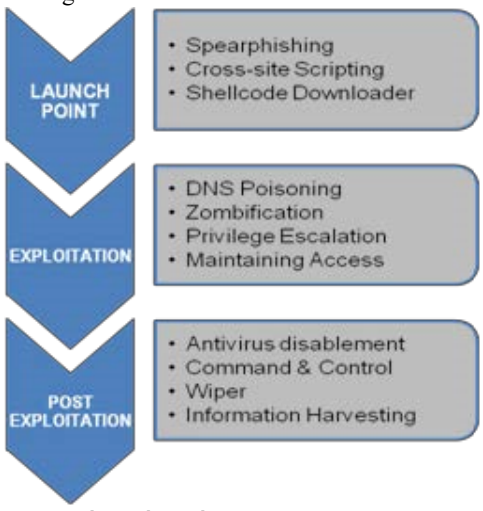

Fig. 1. Dark Seoul Attack Vector

1. Spearphishing

Trend Micro researchers discovered a phishing email sent to South Korean organizations on March 19. The email contained a malicious Trojan downloader which the researchers report to have been detected by their Deep Discovery software. This is likely to be the initial attack point.

2. Launch Platform – Cross-Site Scripting

Avast detected the attacks originating from the Korea Software Property Right-Council (SPC) website (http://www.spc.or.kr) possibly infected via the phishing email sent on the 19th. Usage of a legitimate website/server in the target nation/region for launching attacks is a common tactic used to minimize detection. The SPC website contained JavaScript causing the client browser to load an iframe loading the contents of http://rootadmin2012.com, which was the main attack site for hosting the malicious payloads.

3. Exploitation

Examination of rootadmin2012.com revealed heapspray and shellcodes with references to Internet Explorer (IE). Avast managed to identify the vulnerability exploited as CVE-2012-1889 [7] which allows remote attackers to execute arbitrary code or cause a denial of service via a crafted website. The vulnerability targets Microsoft XML Core Services 3.0 – 6.0 with a published metasploit exploit targeting MS XML Core Services 3.0 via IE6 and IE7 over Windows XP [8]. After gaining access the second stage downloader file (sun.exe) performs the following actions:

a. *Check for internet connection*: Downloads an image from naver.com.

b. *Local DNS cache poisoning*: Redirects requests to certain Korean banking websites listed in Figure 2 to another server in Japan.

```
126.114.224.53 www.kbstar.com
126.114.224.53 www.ibk.co.kr
126.114.224.53 www.shinhan.com
126.114.224.53 www.wooribank.com
126.114.224.53 www.hanabank.com
126.114.224.53 www.nonghyup.com
```

Fig. 2. New entries appended to Windows hosts file

c. *Update download counter*: Runs a counter script by opening http://myadmin2012.com/tong.htm.

d. *Makes itself persistent*: Modifies the Windows registry by adding value with name "skunser" and data "C:\ntldrs\svchest.exe", where it was previously copied to.

e. *Download backdoor*: Downloads dropper file pao.exe from http://www.hisunpharm.com/files/File/product/ and stores it to C:\Program Files\tongji2.exe

f. *Drops and execute batch file*: schedules downloader every 30 minutes and ensures svchest.exe is started with Local System privileges.

4. Post-exploitation

The tongji2.exe module injects itself into iexplore.exe in an attempt to mask itself. Avast classified this as a backdoor Trojan and infostealer. This malware allowed attackers to control the computer as a compromised zombie part of a wider botnet network – a theory suggested by Alienvault [9] – which then wiped hard disks, and harvested personal information. Examination of the file names and the Safeengine executable protector suggest that the malware was made in China. Although capable of executing many functions, only the following were widely utilized in the attack:

a. *Antivirus disablement*: Malware attempts to disable Ahnlab and Hauri antivirus.

b. *Command & control (C&C)*: Using a simple XOR loop for encryption, the malware attempts to connect to laoding521.eicp.net over port 889 to communicate with the attackers.

c. *Harddisk wiper*: Symantec identified Trojan.Jokra as the malware component that wiped harddisks in the attack. It is likely that it was downloaded onto the victim's computer after receiving an instruction by the C&C servers. The malware overwrites the master boot record (MBR) and the rest of the harddisk with the strings "PRINCIPES" or "HASTATI.". Other attached drives or removable devices may also be targeted. The malware then forces the computer to restart thus making it unusable. An interesting feature of this malware is that it has components to wipe out harddisks on both Windows and Linux platforms. Detailed analysis of Jokra can be found here [10].

d. *Information harvesting*: After gaining root privileges the attackers can intercept any information that goes in or out of the infected computer. However the most apparent information taken was user credentials. As a result of DNS poisoning, users believe they are accessing the authentic internet banking website, but are decepted into interacting with a fake website. An error message pops up stating that the user's computer was infected by a virus and that for security reasons they need to apply for a fraud prevention service. If the user clicks the OK button, the user is directed to a page requesting their name and national identification number. If the format entered is correct, the user is then asked to fill in more details including address, phone number, etc..

C. Case Studies: Previous Major Cyber Attacks

1. Stuxnet

Stuxnet was discovered in July 2010, but the earliest known variant is confirmed to have existed since 2007 [11]. Stuxnet caught many security researchers and professionals by surprise, being the first advanced malware of its kind. According to Symantec's report [12], 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 0-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 [13]. The initial attack point is likely to be via a USB infection.

2. 10 days of Rain

On March 4, 2011, exactly 20 months after a similar incident during the U.S. Independence Day celebrations of 2009, a botnet based in South Korea launched DDoS attacks against 40 websites affiliated with South Korean government, military, and civilian critical infrastructure as well as U.S. forces based in Korea [14]. The botnet was dynamically updated via new malware binaries, launched a DDoS non-stop for more than a week, and then wiped the harddisks with zeroes, overwriting the MBR making the machines unusable. This attack used malware with a much higher level of sophistication than is necessary to launch a trivial distributed denial of service (DDoS) attack. Encryption of code and configurations using cipher algorithms such as the Advanced Encryption Standard (AES), RSA, and Rivest Cipher 4 (RC4) enabled them to evade detection and prolong analysis. A multitier botnet architecture included 40 C&C servers distributed across the globe including servers in the USA, Taiwan, Saudi Arabia, Russia, and India. Highlighting the overkill in this attack, McAfee went so far as to call it "analogous to bringing a Lamborghini to a go-cart race" [15]. Considering the limited timeframe scope and target list, McAfee suggested the motivation of the attack was a cyber war exercise to test the preparedness of South Korea's cyber defense capabilities and to better understand the technical requirements for a successful campaign.

3. SK Communications – CyWorld

In July 2011 SK Communications became the victim of an attack that resulted in the loss of the personal details of 35 million users [16]. The users of CyWorld and Nate, services owned by SK Communications, were affected by this attack. Judging from the sophistication of the attack and the time needed for planning it, researchers concluded that the attack was likely to be carried out by an Advanced Persistent Threat. Between July, 18 and 25, more than 60 computers were infected then used to gain access to the user databases. The launch point was a South Korean software company's update server, normally used to deliver software updates to customers [17]. The attackers compromised the server and created a Trojan that would be downloaded to user computers during a routine update. Poor change management policy resulted in the full trust of software updates, allowing attackers to fully exploit this weakpoint. During this time attackers used C&C servers to monitor the activities on the infected machines and uploaded tools on a previously compromised legitimate Taiwanese website. An elaborate infrastructure of waypoints and C&C servers was created to make tracing the sources of their activities difficult. In-depth investigation of the attack reveal that preparation went back as early as September 2010 before finally culminating in the compromise of the user databases between July 26-28, 2011.

Comparing Dark Seoul with previous attacks shows that it was technically low in sophistication while causing high impact to the organizations affected. An intuitive indicator of this sophistication is that it was completely preventable if the organizations had used existing software updates and antivirus solutions, whereas prior attacks could not have been detected. However judging from the high number of infections, services disrupted, and the fact that information was being harvested from the infected machines at least 8 months [18] before the d-day wipeout, we consider the impact to be high.

Table 1. Comparison with Previous Attacks.

Metric	Stuxnet (2007-2010)	SK Comm (2011)	10 days of rain (2011)	Dark Seoul (2013)
Sophistication	VERY HIGH	HIGH	VERY HIGH	LOW
Impact	VERY HIGH	HIGH	HIGH	HIGH
#of Infections	>100,000	60	>100,000	>48,000
Losses	Nuclear Program	35 million users	8 billion KRW	DDoS
Time Before Detection	>3 years	>10 months	>1 year	>8 months

D. ADVANCED MALWARE DESIGN

1. Multiple Propagation Vectors

To increase the probability of successfully infecting the target systems, various propagation vectors should be embedded into the malware. The most likely attack vector is social engineering via phishing emails, USB sticks, and other techniques. Although people can be used as the initial point of entry, propagation needs to continue laterally through the network till the specific target host is reached. During this process the malware may need higher privileges (e.g. root) and further exploits will be utilized. Therefore the persistent adversary will need to consider multiple vectors to infiltrate target systems.

2. 0-day Exploits

The problem with publicly published vulnerabilities is people can defend against them. 0-day exploits are written to exploit vulnerabilities that have not been disclosed to the public nor the concerned software vendor. These exploits are at the core payload of any advanced malware, and are virtually unstoppable until vendors release a patch or anti-virus providers come up with a signature definition. The only other method of minimizing the 0-day threat is by actively designing security into software. Dark Seoul did not use any 0-days.

3. Evasion Techniques

The deployment of anti-virus software, intrusion detection systems, firewalls and other malware detection or prevention technology has done much to defend against many attacks. Advanced malware bypasses these defenses by employing techniques such as dynamic botnet obfuscation, network based fragmentation and session splicing, application or protocol violations, disabling intrusion detection systems (IDSs), to more advanced techniques such as encryption and code reuse attacks [19]. Carefully crafted exploits can avoid even advanced heuristic detection algorithms used in today's anti-virus software. Evasion techniques are crucial for successful attacks against high level targets, such as in the case of the Iranian nuclear program.

E. CONCLUSION

Dark Seoul was a low tech threat which managed to escalate into a high impact attack. Successful in carrying out its goals, the malware was lacking in many areas that would be typically found in attacks by advanced persistent threats. We highlighted the components of the malware used and the possible design principles that could have been employed to make the attack more sophisticated.

South Korea is more at risk now than before the attack, as now adversaries less capable than advanced persistent threats realize they could also successfully perform damaging attacks. Undertaking the needed remediation strategies to prevent similar attacks as well as understanding the anatomy of more advanced malware is vital for mounting an adequate defense against the advanced cyber threats.

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] "South Korea blames North for bank and TV cyber-attacks," BBC News, [online] 10 April 2013, Available: http://www.bbc.co.uk/news/technology-22092051 (Accessed: 18 April 2013)

[2] He-suk Choi. "Seoul blames Pyongyang for cyber attacks," The Korea Herald, [online] 10 April 2013, Available: http://www.koreaherald.com/view.php?ud=20130410000766 (Accessed: 18 April 2013)

[3] J. Horejsi. "Analysis of Chinese attack against Korean banks," Avast! Blog, [online] 19 March 2013, Available: https://blog.avast.com/2013/03/19/analysis-of-chinese-attack-against-korean-banks/ (Accessed: 18 April 2013)

[4] J. Schwartz, "South Korea Changes Story On Bank Hacks," Information Week [online] 22 March 2013, Available: http://www.informationweek.com/security/attacks/south-korea-changes-story-on-bank-hacks/240151542 (Accessed: 18 April 2013)

[5] "Remote Linux Wiper Found in South Korean Cyber Attack," Symantec Connect [online] 20 March 2013, Available: http://www.symantec.com/connect/blogs/remote-linux-wiper-found-south-korean-cyber-attack (Accessed: 18 April 2013)

[6] "Trojan.Jokra," Symantec Security Response, [online] 27 March 2013, Available: http://www.symantec.com/security_response/writeup.jsp?docid=2013-032014-2531-99 (Accessed: 18 April 2013)

[7] "CVE-2012-1889," Common Vulnerabilities and Exposures, [online] 22 March 2012, Available: http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1889 (Accessed: 18 April 2013)

[8] Metasploit, "Microsoft XML Core Services MSXML Uninitialized Memory Corruption," The Exploit Database, [online] http://www.exploit-db.com/exploits/19186/ (Accessed: 18 April 2013)

[9] J. Blasco, "A theory on the South Korean attacks," Alien Vault Labs [online] 20 March 2013, Available: http://labs.alienvault.com/labs/index.php/2013/a-theory-on-the-south-korean-attacks/ (Accessed: 18 April 2013)

[10] "Trojan.Jokra," Symantec Security Response, [online] 27 March 2013, Available: http://www.symantec.com/security_response/writeup.jsp?docid=2013-032014-2531-99&tabid=2 (Accessed: 18 April 2013)

[11] G. McDonald, L.O. Murchu, S. Doherty, and E. Chien, "Stuxnet 0.5: The Missing Link," Symantec Security Response [online] 26 February 2013, Available: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/stuxnet_0_5_the_missing_link.pdf

[12] N. Falliere, L. O. Murchu, and E. Chien, "W32.stuxnet dossier," Symantec, Symantec Security Response [online] February 2011. [online]. Available: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

[13] Albright, D., Brannan P., Walrond, C. "Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?" Institute for Science and International Security [online] 22 December 2010, Available: http://isis-online.org/isis-reports/detail/did-stuxnet-take-out-1000-centrifuges-at-the-natanz-enrichment-plant/ (Accessed: 18 April 2013)

[14] "10 Days of Rain in Korea," McAfee Blog Central [online] 5 July 2011, Available: http://blogs.mcafee.com/mcafee-labs/10-days-of-rain-in-korea (Accessed: 18 April 2013)

[15] "Ten Days of Rain Whitepaper," McAfee, 5 July 2011

[16] "SK Hack by an Advanced Persistent Threat," Command Five [online] September 2011, Available: http://www.commandfive.com/papers/C5_APT_SKHack.pdf (Accessed: 18 April 2013)

[17] Moon-young Lee, "Personal information hack traced to Chinese IP address" The Hankyoreh [online] 12 August 2011, Available: http://www.hani.co.kr/arti/english_edition/e_national/491514.html (Accessed: 18 April 2013)

[18] "South Korea Probe Blames North for Cyber Attack" VOA News [online] 10 April 2013, Available: http://www.voanews.com/articleprintview/1638361.html (Accessed: 18 April 2013)

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