National Cybersecurity and Communications Integration Center

March 27, 2013

South Korean Malware Attack

Executive Summary

(U) This report covers initial analysis of the malware, dubbed DarkSeoul by Sophos labs, used in the 20 March 2013 attack on South Korean infrastructure. Though details vary from one report or variant to the next, there are a number of attributes that are commonly agreed upon:

- There are multiple JavaScript programs that result in the delivery of a malicious file.
- The malicious file wipes the master boot record (MBR) and other files.
- The malware was hard coded with a specific execution date and time and searches machines for credentials with root access to servers.
- It is written to specifically target South Korean victims.
- The attack is effective on multiple operating systems.
- The design is low sophistication – high damage.

(U) The attacks details become more convoluted when attempting to identify the initial infection vector. Working theories range from unauthorized access of a patch management system with stolen credentials to social engineering techniques like spearphishing. These theories are likely based on the uptick in cyber related incidents impacting South Korea recently.

(U) Well orchestrated cyber attacks have occurred in the Korean peninsula for several years. This may indicate that the most recent attack is part of an ongoing campaign in that region.

(U) When assessing the potential impact to U.S. Critical Infrastructure and Key Resources (CIKR), it's important to understand that DarkSeoul itself was successful in this case because it was designed specifically for its targets, evading antivirus processes commonly deployed on South Korean systems. The most commonly used AV solutions deployed on U.S. systems have detected the DarkSeoul Trojan for some time. For this reason, U.S. CIKR owners and operators should continue the best standard security practices to avoid infection and propagation of a wiper or other type of malware that may impact their systems.

Technical attributes of DarkSeoul

(U) There are general details that seem to be agreed upon among those analyzing variants of DarkSeoul.

- One thing all of the variants had in common was what they used to overwrite the data in the MBR record: the words "PRINCIPES" (a Latin word for Roman heavy infantry) and "HASTATI" (a word for Roman light infantry)[1].
- The malware contained a file that triggered the data wiping on March 20, 2013 at 2pm local time (hex string in the file: 4DAD4678). This is the piece of the malware that allowed for the simultaneous impact to all targets[2].
- The malware searches for saved SSH credentials from two known SSH clients: mRemote and Secure CRT.
- The malware then checked the credentials stored in those locations for accounts with root access to servers. If it finds any, the malware will attempt to log onto these serves. If it finds the following operating systems (AIX, HP-UX, Linux, SunOS) it uploads a file to the server and runs it[3].

Ahn Labs' Depiction of the Malware Behavior in Two Cases[4]

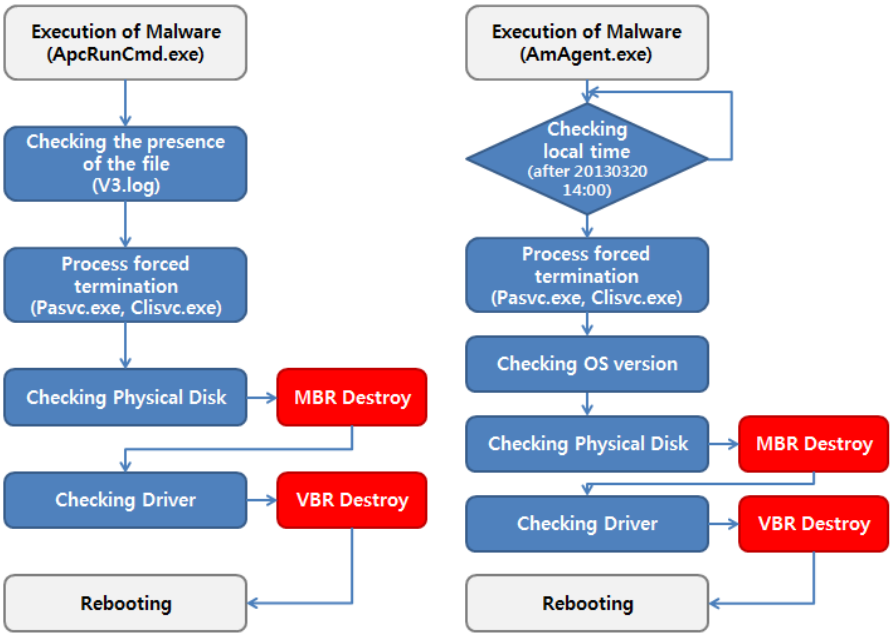

Figure 1: Malware Behavior

Possible Infection Vectors

(U) The NCCIC has been unable to determine the actual infection vector used in the 20 March 2013 South Korean malware attacks. However, there are several theories being proposed by security researchers which bear consideration. These theories are summarized below:

(1) AVAST! Theory: Watering Hole used to Infect Banks and Harvest Customer Data[5]

(U) Avast! posted a malware report which outlined a two stage attack. The actors compromised a popular website (aka the Watering Hole) and embedded malicious JavaScript that redirected users and downloaded additional malware. The Korea Software Property Rights Council (SPC) website (spc.or.kr, image on right) was compromised and redirecting users to the second stage domain, rootadmina2012.com, which was identified as the main attack site.

Figure 2: Korea Software Property Right Council

(U) If an infected user visits one of the bank URLs hard coded into the malware (see Figure 3) – the main module, tongji2.exe, executes, injecting itself into iexplore.exe then tries to initiate a connection via custom communication. Avast! classifies this as a backdoor Trojan and infostealer, which allows attackers to control the compromised computer. It also tries to connect to laoding521.eicp.net on port 889. Of note, the eicp.net site is a free Chinese webhosting site which belongs to oray.com.

```
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
```

Figure 3: URLs Hard Coded into Malware

(U) The Avast! analysis of this attack concludes that the malicious actors likely exploited a known Internet Explorer (IE) (CVE-2012-1889)[6]. Avast! notes this attack was only successful on computers with disabled data execution prevention (DEP). CVE-2012-1889 is a vulnerability that allows a remote attacker to execute arbitrary code via a crafted web site. Microsoft released a tool to fix the vulnerability in August 2012. This vulnerability has been associated with a number of watering hole style attacks. In July 2012, the vulnerability was used in an watering hole attack that leveraged a Chinese high school webpage[7]. For detailed technical details on the vulnerability, visit http://contagiodump.blogspot.com/2012/07/brian-mariani-high-tech-bridge-htbridge.html**.**

(2) AhnLabs Theory: Unauthorized Access to Patch Management Systems[8]

(U) AhnLabs believes the malicious actors obtained user IDs and passwords, using them to gain access to individual patch management systems located on the affected networks. Initial findings by the company stated that a security hole in an AhnLab server or product was used to propagate the malware. This finding has been debunked and the company now believes the patch management system, which is used to distribute new software and software updates to a network of computers, was likely the original source of the malware. Just as the system pushes legitimate patch updates throughout the network, the company believes it pushed the malware throughout some target networks.

(U) The infection vector in the AhnLabs theory then is the theft of user names and passwords belonging to persons with access to the patch management system. It is unclear what stance the company has on the original theft of credentials (be it watering hole attacks as mentioned previously, or perhaps spear phishing attempts).

(3) F-Secure Theory: Spearphishing Causes Users to Download Malicious File[9]

(U) F-Secure's spearphishing theory may not be completely separate from that of AhnLabs' patch management systems propagation. F-Secure's stance regarding how the malware was delivered to the victims could possibly be the step prior to AhnLabs propagation through the network theory. Finnish cybersecurity firm F-Secure analyzed a report released by South Korean NSHC Red Alert Team. F-Secure noticed an archive in the report, whose file name roughly translated to "the customer's account history". Note in Figure 4, the first part of the file name is Shinhan, which is the name of one of the banks targeted in the 20 March attacks.

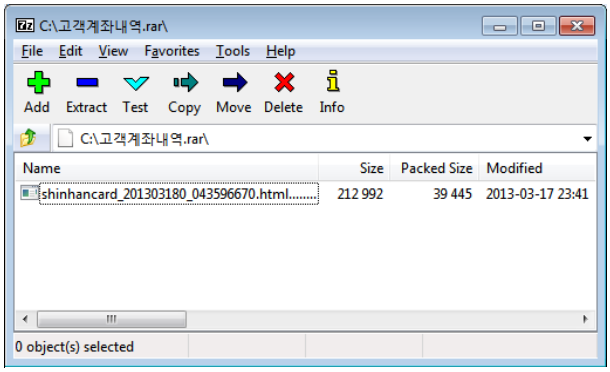

Figure 4: Archive from NSHC Red Alert Report

(U) F-Secure states that the malware inside the archive is using double extensions combined with a very long filename to hide the real extension, which is a common social engineering tactic. This leads the company to believe the file was sent via an attachment in a spearphishing email.

(U) The malware, according to F-Secure, was dated March 17, 2013, just a few days before the outages occurred. It used a fake Internet Explorer icon to tempt users into opening it, and launched an IE lookalike page in System32 once clicked. Note: System32 is a required directory on any Microsoft Windows system. At least one of the payloads was the time triggered dynamic link library (DLL) sample, set to execute on March 20 at 15:00. After initiation, the malware downloaded and executed a number of files from a handful of compromised sites and made other HTTP requests as well, either to throw off any

system administrators who might be monitoring traffic logs or to download further malicious components.[10]

(4) RSA Theory: Xgate Buffer Overflow[11]

(U) RSA asserted that the DarkSeoul attack targets the popular Korean Encryption Xgate module, wiping the master boot record and rebooting the system. The key exchange RSA analyzed in the packet capture (PCAP) from a sample found at one of the banks seems to go from structured to garbled. This is the initial indicator leading them to their overflow concept. Additionally, the researchers state that while researching the source IP address from the PCAP, they noted it belonged to Korea Telecom and had a user-agent string earlier in the month indicating it came from an Android phone. The IP address which is typically used for a mobile network in South Korea leads RSA to their theory that a mobile network was used at some point to carry out the attack. The theory is that the South Korea attackers either used an authorized app that connected victims to an online payment site, or a buffer overflow attack on the key generation process that injected code and ultimately spread.

(5) NCCIC Theory: Multi-vector Attack, Executed Over Time

(U) At the time of this report, there has been nothing to completely confirm or exclude these theories. When more details emerge, we may likely discover that the DarkSeoul malware was deployed in a multi-vector attack against South Korean critical infrastructure. The infection vectors likely included some sort of social engineering to convince a user to either give up credentials, open an attachment or click on a malicious link. All signs point in that direction, but removable media (like thumb drives) and watering hole attacks (web) have all be effective methods of malware delivery in the past and should not be discounted.

Recent Cyber Attacks in the Korean Peninsula

(U) There's been a history of significant cyber attacks in both North and South Korea in the past few years, with a notable uptick in the past couple of weeks. The following is not all inclusive, but provides a background on high visibility attacks that have taken place in the region.

- **7 July 2009 –** Multiple South Korean government sites with distributed denial of service (DDoS) attacks. Sites included those of the presidential Blue House, the Defense Ministry, the National Assembly, Shinhan Bank, the mass-circulation newspaper Chosun Ilbo and the top Internet portal Naver.com [12]

- **4 March 2011 –** 'Ten Days of Rain' - DDoS attacks impacted multiple South Korean government websites as well as the network of U.S. Forces Korea (USFK)[13].

- **12 April 2011 -** South Korean officials said that 30 million customers of the Nonghyup agricultural bank were unable to use ATMs or online services for several days and that key data were destroyed.[14]

- **13 March 2013** - North Korea sustained a cyber attack that disrupted internet connectivity to the country. Renesys observed disruptions beginning at 00:59:30 UTC, which briefly removed North Korea's four networks from the global routing table. Note that all four networks are routed by a single Internet service provider Star JV (AS 131279), which has two international Internet service providers: China Unicom (AS 4837) and Intelsat (AS 22351). Renesys reported a significant drop-off in successful responses (via trace routes), suggesting a loss of connectivity not visible in routing data alone[15]. Though North Korea has an extremely small internet for a country of 24 million people and exhibits routing instabilities, this data does serve as validation to the outage claims.

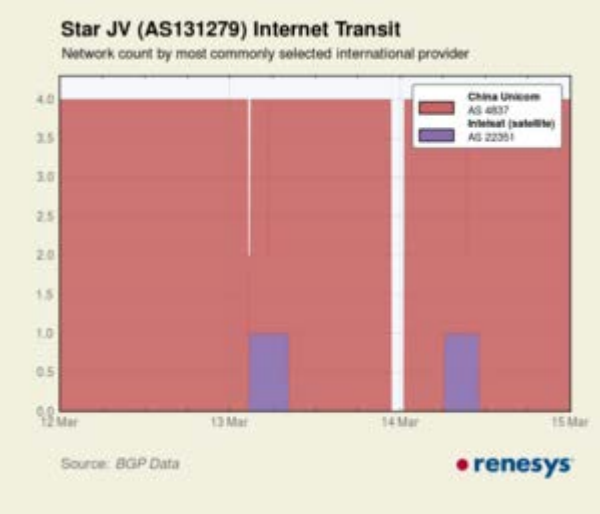

Figure 5: N. Korea Networks Removed From Routing Table

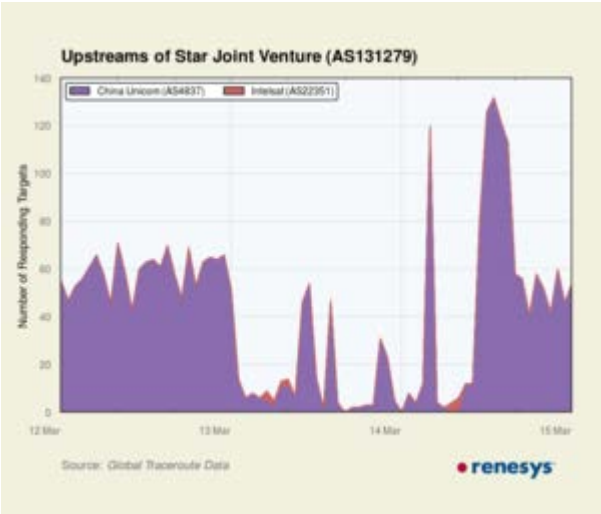

Figure 6: Traceroutes Suggest Additional Loss of Connectivity

- **20 March 2013**– wiper malware deployed on the systems of South Korean broadcasters and financial institutions caused massive disruptions to operations. Impacts continue to be assessed. Targets: Nonghyup Bank, Shinhan Bank, Jeju Bank, Nonghyup Life, KBS, MBC, YTN. LG UPlus Corp seems to have been targeted with a site defacement from the WhoIs Team. US-based Committee for Human Rights in North Korea was also hit by a cyber attack that disabled its website for several hours the same day.

- **26 March 2013**- Anti-North Korea Web sites run by defectors now living in South Korea said their servers crashed simultaneously around 11:00 local time and were down for about an hour. Reported victims included: The Free North Korea Radio, Daily NK, and North Korea Intellectuals Solidarity[16]. Information regarding cause, attribution and validation were unavailable at the time of this report.

Impact Analysis of the Malware

(U) While it is possible for this type of malware to impact U.S. based CIKR assets, it would require a significant modification of the code.

(U) U.S. CIKRs are not vulnerable to the DarkSeoul malware as it is designed specifically to kill the processes of two popular South Korean security companies, AhnLab's (policy agent process - pasvc.exe) and HAURI Inc's (ViRobot ISMS process - clisvc.exe)[17]. Many antivirus tools already detect the 'DarkSeoul' trojan. The figure below lists how some of these tools reference the malware.

AV Tool	Common Name
Malwarebytes	Trojan.MBR.Killer
Symantec	Trojan.Jokra
TrendMicro	TROJ_INJECTO.BDE
Sophos	Mal/EncPk-ACE
ViRobot	Trojan.Win32.U.KillMBR.24576.A
AhnLab-V3	Win-Trojan/Agent.24576.JPG
PCTools	Trojan.Jokra

Figure 7: AV Tool Recognition of DarkSeoul

(U) Symantec provides a full scope of information regarding DarkSeoul malware (aka Trojan.Jokra) to include a summary, technical details and removal steps[18]. End users that want to know more about the malware, how it's detected and what the defenses and remediation may be can visit the sites of the antivirus solution currently running on their machines.

(U) It is possible to rewrite the malware code with the intent of evading or deactivating the most commonly used antivirus software tools in the U.S.

(U) According to a December 2012 OPSWAT market share report[19], the top vendors serving the U.S. are Microsoft, Symantec, avast!!, AVG, ESET, McAfee, Avira, Kaspersky, Trend Micro and Lavasoft (see chart).

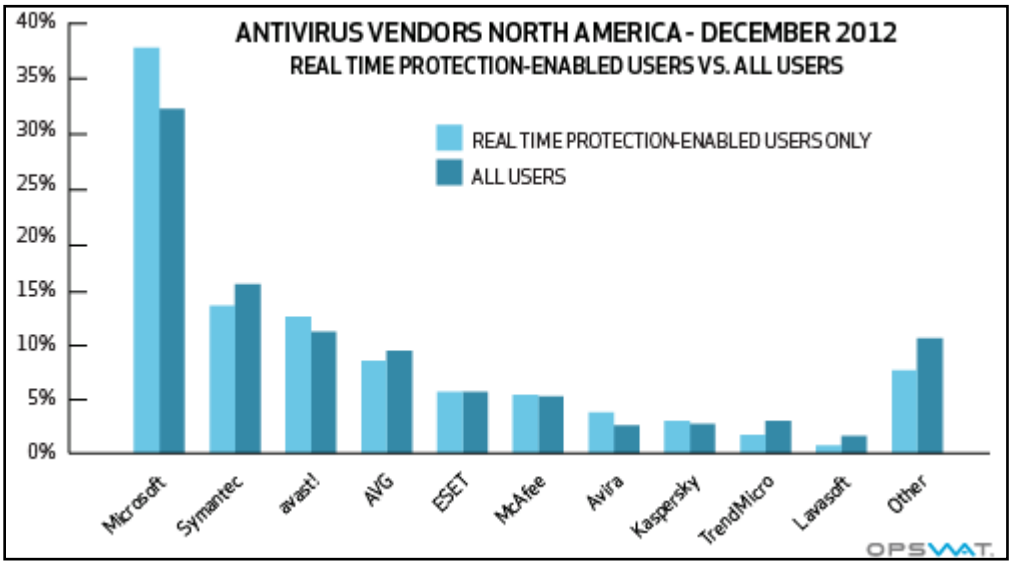

Figure 8: Top AV Vendors by Market Share

Defensive Measures

(U) The cyber attacks occurring in both North and South Korea seem to be due to defacements, distributed denial of service (DDoS) attacks and destructive malware intended to erase data. Initial infection vectors and propagation tools may be taking advantage of social engineering tactics and vulnerable security practices.

(U) US-CERT would like to remind users and administrators of the following best practices to strengthen the security posture of their organization's systems:

- Maintain up-to-date antivirus signatures and engines.
- Restrict users' ability (permissions) to install and run unwanted software applications.
- Enforce a strong password policy and implement regular password changes.
- Exercise caution when opening e-mail attachments even if the attachment is expected and the sender appears to be known.
- Keep operating system patches up-to-date.
- Enable a personal firewall on agency workstations.
- Disable unnecessary services on agency workstations and servers.
- Scan for and remove suspicious e-mail attachments; ensure the scanned attachment is its 'true file type' (i.e. the extension matches the file header).

- Monitor users' web browsing habits; restrict access to sites with unfavorable content.
- Exercise caution when using removable media (e.g. USB thumbdrives, external drives, CDs, scan all software downloaded from the Internet prior to executing.
- Maintain situational awareness of the latest threats; implement appropriate ACLs.

---

[1] http://arstechnica.com/security/2013/03/your-hard-drive-will-self-destruct-at-2pm-inside-the-south-korean-cyber-attack/
[2] http://www.wired.com/threatlevel/2013/03/logic-bomb-south-korea-attack/
[3] http://blog.trendmicro.com/trendlabs-security-intelligence/summary-of-march-20-korea-mbr-wiper/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+Anti-MalwareBlog+%28Trendlabs+Security+Intelligence+Blog%29
[4] http://training.nshc.net/KOR/Document/virus/20130321_320CyberTerrorIncidentResponseReportbyRedAlert%28EN%29.pdf
[5] http://blog.avast!.com/2013/03/19/analysis-of-chinese-attack-against-korean-banks/
[6] http://www.computerworlduk.com/news/security/3436305/south-korea-cyberattacks-hold-lessons-for-us/
[7] http://blog.trendmicro.com/trendlabs-security-intelligence/high-school-webpage-targeted-by-cve-2012-1889-exploit/
[8] http://www.theregister.co.uk/2013/03/25/sk_data_wiping_malware_latest/
[9] http://www.f-secure.com/weblog/archives/00002531.html
[10] http://threatpost.com/en_us/blogs/spear-phishing-cause-south-korean-cyber-attack-032513
[11] https://community.emc.com/community/connect/rsaxchange/netwitness/blog
[12] http://www.nytimes.com/2009/07/09/technology/09cyber.html?hp&_r=0
[13] http://blogs.mcafee.com/wp-content/uploads/2011/07/McAfee-Labs-10-Days-of-Rain-July-2011.pdf
[14] http://www.koreatimes.co.kr/www/common/printpreview.asp?categoryCode=117&newsIdx=86369
[15] http://www.renesys.com/blog/2013/03/north-korea-suffers-outage.shtml
[16] http://www.zdnet.com/north-korean-defector-sites-report-planned-cyberattack-7000013163/
[17] http://www.tripwire.com/state-of-security/it-security-data-protection/cyber-security/south-korean-attack-malware-analysis/
[18] http://www.symantec.com/security_response/writeup.jsp?docid=2013-032014-2531-99&tabid=3
[19] http://www.opswat.com/about/media/reports/antivirus-december-2012