GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

Tracing the Lineage of DarkSeoul

GIAC (GSEC) Gold Certification

Author: David M. Martin, david.martin.c16@gmail.com
Advisor: Christopher Walker
Accepted: 11/20/15

Abstract

This paper presents a case study of the April 2013 "DarkSeoul" cyber-attack, which crippled tens of thousands of computers in South Korea's banking and media sectors through the use of destructive malware. While the attack was initially believed to be the work of hacktivists, malware researchers discovered it was actually the outgrowth of a multi-year cyber-espionage campaign waged by the North Korean government. By analyzing the code commonalities and tracing the malware used in a number of seemingly unrelated incidents, researchers were able to trace the evolution of the intruders' techniques and reach the conclusion that the attacks represented a targeted attack by North Korea. At the same time, the South Korean government reached the same conclusion through its investigation and publically attributed the attacks to North Korea. In particular, this study will focus on the malware lineage analysis techniques used by researchers and identify critical security controls that were subverted in order to successfully launch the attack. This study will also address critical security controls that could have helped prevent this attack, or significantly mitigated its damage.

© 2016 The SANS Institute Author retains full rights.

1. Introduction

The highly publicized 2014 cyber-attack on Sony brought the threat of cyber-warfare, broadly defined as destructive cyber-attacks launched by one nation state against another, to the attention of the American public. The Republic of Korea (South Korea) has been contending with similar attacks for a number of years, the best known and most destructive of which was a 2013 attack known as DarkSeoul. On April 20, 2013, South Korea suffered a coordinated strike by simple, but effective destructive malware that rendered tens of thousands of computers in the media and financial services sectors inoperable. The attack was first mistaken for, and indeed intentionally disguised as the work of hacktivists.

South Korean authorities launched an investigation that quickly laid the blame for the attacks at the feet of the Democratic People's Republic of Korea (North Korea). While hardly surprising behavior from a nation with a habit of loudly and publically threatening the annihilation anyone within earshot, the announcement was greeted with some skepticism, as this was not the type of nation-state sponsored computer intrusion most people were familiar with. For the security researchers investigating DarkSeoul without access to the national intelligence and law enforcement resources available to the South Korean government, the key to understanding the true nature of the attack came from the tools themselves. A careful examination of the malware began to reveal commonalities with previously seen malware used in previous attacks against South Korea. When placed in context, the different malware code samples revealed the evolution of an ongoing campaign of cyber-espionage and attack by North Korea.

2. Anatomy of the Attack

At approximately 14:00 Korean Standard Time (KST) (UTC +9), South Korean media began reporting widespread outages in computer networks at the "big three" Korean television broadcasters, KBS, MBC and YTN (Dong-A, 2013). The network outages did not directly affect on-air broadcasts. Korean banks Jeju, Nonghyup, Shinhan,

© 2016 The SANS Institute Author retains full rights.

and Woori, as well as several subsidiaries also reported widespread outages affecting ATMs, payment terminals, and mobile banking services. (SecureWorks, 2013).



(Dong-A, 2013)

Users attempting to reboot their systems found that their operating systems were gone and on closer inspection, their hard drives appeared to be completely blank. The attacks affected both Windows and Unix-like operating systems (Branigan, 2013).

Korean law enforcement and national security agencies immediately launched an investigation into the attacks, which they claimed had rendered approximately 30,000 computers inoperable. Later reports would place this figure closer to 45-50,000 systems (Minji, 2013). The Korean government released a statement indicating that the outages were the result of a deliberate attack using malicious software and not a DDoS attack. They reported that they were investigating the incident, but did not yet place blame on North Korea. Non-governmental sources quickly reached the same conclusion. The Associated Press quoted Lim Jong-in, dean of Korea University's Graduate School of Information Security, as saying that "It's got to be a hacking attack. Such simultaneous shutdowns cannot be caused by technical glitches" (Branigan, 2013). Suspicion was immediately cast upon North Korea, which only weeks before, had accused the South and their US allies of attacking their networks and causing a multiple day internet outage that had affected that country's estimated several thousand internet users, mostly believed to be government officials. Both the US and South Korea denied any involvement in the outages (Branigan, 2013).

Author Name, email@address

© 2016 The SANS Institute Author retains full rights.

2.1. Delivery

The investigation eventually determined that while similar malware had been used throughout the attacks, the hackers had employed a number of different vectors to deliver the malware. The most widely reported vector was the use of the AhnLab patch management software used by several of the affected organizations. It appears that the attackers did not compromise the PMS, but instead used stolen legitimate credentials to gain access, according to a statement released by the AhnLab Security Emergency Response Center (ASEC) (Schwartz, 2013). Once they had access, the attackers used the PMS' ability to install software with system level access, thus bypassing the need for user interaction or visibility. This ability allowed them to deliver their malware to the entire victim organization simultaneously, hidden among the new software and updates delivered by the PMS.

Other reports indicated that some victims had received spear phishing emails on March 19 containing a malicious HTML archive with a long file name and double extension to conceal its true nature (Trend Micro, 2013). Research by McAfee revealed the presence of a remote access Trojan (RAT) referred to as 3Rat, on several victim systems (Sherstobitoff, Itai, & Walter, 2013, p. 5). It is speculated that this RAT, found to have a compile time of 2013-01-26, gave the attackers access to the victim networks for over a month before the attacks occurred (p. 5). This would have given the attackers ample time perform network reconnaissance, identify the patch management system and obtain credentials for it well in advance of the attack. The RAT may have also been used to directly distribute malware over victim networks that did not have a patch management system the actors could subvert. This allowed the attackers to deliver an effective payload to each victim network and have their pieces in place prior to the coordinated execution.

2.2. Detonation

2.2.1. Dropper Malware

Regardless of its delivery method, each target received a similar executable "dropper" containing one of several similar, malicious payloads that were extracted from the PE Resource section of the dropper into the Windows %Temp% directory.

© 2016 The SANS Institute Author retains full rights.

Researchers observed that there were at several variants of the dropper malware observed with slightly varying payloads. Several analyses of the attack reported different numbers and characteristics of malware, however, when these reports are correlated, it appears that there were at least three separate dropper variants, at least three Windows wiper variants and a wiper shell script targeting Unix systems. While some samples were designed to begin wiping immediately upon execution, most were set to execute at a specific time and date. The majority of the samples analyzed were set to execute on 2013-03-20 at 14:00 KST, although there were some samples designed to execute on March 20 of any given year at 15:00 KST (ASEC, 2013, p. 9).

Dropper A contained a Windows portable executable (PE) files designed to wipe the victim's hard drive (Wiper A), a Bash script designed to remotely wipe the hard disk of a Unix-like systems and the Windows PuTTY SSH and SCP clients to deliver and execute the script on the remote victim (Dell Secureworks, 2013, p. 2). The dropper attempted to locate mRemote or SecureCRT remote management tools, and if present, use them to obtain valid root credentials to connect to and wipe *nix systems. After attempting to destroy all *nix system to which it could connect, the malware attempted to locate the file % SystemDirectory% \ TEMP \ ~ v3.log (ASEC, 2013, p. 3). If this file was detected, the malware would use the taskkill command to shut down processes associated with the AhnLab and Hauri antivirus programs commonly used in Korea, before launching the Windows wiper malware to destroy the host it had implanted (p. 4).

Dropper B contained only a Windows wiper variant (Wiper B) and a configuration file. This variant would attempt to shut down a different set of antivirus programs before launching the wiper (ASEC, 2013, p. 5).
Dropper C was similar to Dropper B, except that it extracted a slightly different wiper (Wiper C) and config file to the %SystemRoot%/System32 directory and executed the wiper by injecting its code into the heap of lsass.exe. This variant did not attempt to disable antivirus software (ASEC, 2013, p. 8).

© 2016 The SANS Institute Author retains full rights.

2.2.2. Unix Wiper

The Unix wiper Bash script, reported by AhnLab to be effective against AIX Unix, HP Unix, Solaris, Linux systems, used the 'dd' command to overwrite the first 10 – 81mb of each partition on the victim system and the 'rm' command to delete the /etc, /home, /kernel and /usr directories, rendering the system un-bootable and likely crashing the operating system (ASEC, 2013, p. 2).

2.2.3. Windows Wipers

Wiper A was designed to begin wiping the master boot record (MBR) and volume boot record (VBR) of the first 10 physical hard disks with the string "PRINCPES" immediately upon execution (ASEC, 2013, p. 5). The malware would also overwrite all attached fixed or removable logical drives B – Z with the same string (p. 5). Five minutes after execution, the malware would use WinExec to issue the "Shutdown -r -t 0" to reboot the system immediately (Dell Secureworks, 2013, p. 4).

Wiper B behaved similarly to Wiper A, but used the string "HASTATI" to overwrite the drives and was set to sleep until the time was later than 2013-03-20 14:00 KST (ASEC, 2013, p. 7).

Wiper C behaved similarly to Wiper B, but used the string "PR!NCPES" to overwrite the drives, which it was designed to do immediately upon execution (ASEC, 2013, p. 8).

2.3. Denial and Deception

Shortly after the attacks were discovered, the "NewRomanic Cyber Army Team" and the "Whois Crew", two different, heretofore unknown hacker groups took responsibility. The Whois Crew left behind graphics files on several victim computer and defaced several websites, including LG +U and Nocut News, with the same images of skulls with bright green lettering announcing their arrival and listing several, apparently fictitious email addresses (GReAT, 2013). The supposed hacker group had no social media presence and was never heard from again (Dell Secureworks, 2013, p. 5).

© 2016 The SANS Institute Author retains full rights.



(GReAT, 2013)

A day after the attack, the "NewRomanic Cyber Army Team" defaced the public websites of several victim companies to display a popup containing the following message:

> Hi, Dear Friends, We are very happy to inform you the following news. We, NewRomanic Cyber Army Team, verified our #OPFuckKorea2003. We have now a great deal of personal information in our hands. Those includes; 2.49M of [redacted by MacAfee] member table data, cms_info more than 50M from [redacted]. Much information from [redacted] Bank. We destroyed more than 0.18M of PCs. Many auth Hope you are lucky. 11th, 12th, 13th, 21st, 23rd and

© 2016 The SANS Institute Author retains full rights.

> 27th HASTATI Detachment. Part of PRINCIPES Elements. p.s For more information, please visit www.dropbox.com login with joseph.r.ulatoski@gmail.com::lqaz@WSX3edc$RFV. Please also visit pastebin.com. (Sherstobitoff, Itai, & Walter, 2013, p. 4).

The Dropbox and Pastebin accounts mentioned were verified to exist, but quickly taken down, presumably at the request of the victims or Korean law enforcement. It is unclear whether the accounts contained the information the hackers claimed and whether it was actually stolen during or related to the attack. The NRCAT message was interesting in its use of the terms Principes and Hastati, the names of two kinds of infantry units used by the ancient Roman army (Krebs, 2014). These terms are similar to the strings used by the Windows wiper malware to overwrite the victim hard drives, although the "PRINCPES" and "PR!NCPES" strings in the malware appear to have been shortened to 8 characters by the omission of the second "I". Like the Whois Crew, there were no indicators that the NRCAT had existed prior to the attack, nor did they claim responsibility for any further attacks.

While the two purported hacktivist groups exhibited many of the hallmarks of Anonymous-style hacktivists: hashtags with the "Op(Name of Victim)" nomenclature, information leaks to Pastebin and Dropbox and website defacements; upon closer examination they appear much more likely to have been attempts to provide plausible deniability to the real attackers and cause investigators to waste time chasing phantom hacktivists. Such groups tend to be loosely organized, amorphous collectives that assemble for a short-term goal, then disperse. Even among the more organized groups like Anonymous and LulzSec, it is hardly unusual to see sub-groups at cross purposes and even attacking the same targets for which another sub-group is advocating. One of the key elements missing in the hacktivists' message was a grievance the attacks were supposed to be in retaliation for. Most hacktivist attacks are purportedly designed to punish a company or government for some perceived injustice, such as the attacks against the PlayStation network in response to Sony's controversial anti-piracy efforts or attacks on financial institutions in support of the Occupy Wall Street movement. There were no such claims attached to the DarkSeoul attacks, and while some hackers will launch

© 2016 The SANS Institute Author retains full rights.

attacks out of a sense of pure nihilism, the degree of preparation and coordination involved militates against that possibility.

3. Investigation and Attribution

In the days following the attack, a picture was beginning to form of an attack that initially appeared unsophisticated work of hacktivists due to the crude, destructive nature of the payload, but had in fact been a coordinated strike delivered with the precision and planning commonly associated with state-sponsored intrusion campaigns. With the two hacktivist groups claiming responsibility both apparent dead ends, investigators turned to the network trail and, most importantly the malware itself to uncover the true nature of the attack.

3.1. Following the Network Trail

When investigators began piecing together the network traffic logs from the attack, they discovered that different elements of the attack had been launched from a variety of addresses, both within South Korea and abroad. Unsurprisingly, a number of the addresses resolved to anonymous proxy servers or TOR exit nodes (Symantec, 2013). Others were compromised infrastructure and a few led directly to North Korea (Minji, 2013). Different infrastructure was used for each aspect of the attack, with some exploiting the patch management systems, others serving as command and control nodes for the 3RAT implant or hosting one of the malicious software variants for download (Minji, 2013). This approach provided several benefits, none the least of which was redundancy in case one or more nodes were lost. It also made the collection and correlation of evidence more difficult since no one node could see the entire picture. The fact that the infrastructure was spread across different providers with different data retention policies, capabilities and laws further complicated the investigation.

While this approach offered many benefits to the attackers, it was not without its drawbacks. The more systems used in an attack, the more places an attacker must cover their tracks and the greater likelihood that incriminating evidence will be left behind. Obtaining control of and maintaining a large network of intrusion infrastructure is often

© 2016 The SANS Institute Author retains full rights.

difficult and time-consuming, which increases the temptation to keep the same infrastructure throughout multiple campaigns. In April 2013, Korea Internet & Security Agency spokesman Chun Kil-soo announced that 22 of the addresses used in the attacks were ones that had been used by North Korean hackers since 2009 (Minji, 2013).

3.2. Malware Analysis

Kil-soo also pointed to 18 pieces of malicious code used in the attacks that were tied to previous North Korean attacks. This would prove to be the "smoking gun" linking North Korea to the attacks (Minji, 2013). McAfee Labs researcher Ryan Sherstobitoff was the first to publicly identify the presence of the 3RAT Trojan, which he used as the starting point of his analysis. This program was compiled and presumably deployed several days before the wipers or droppers.

The 3RAT Trojan contained a reference to the path where it was originally compiled, Z:\Work\Make_Troy\3RAT_Project\3RATClient_Load\Release\3RATClient, revealing the name of the malware and the campaign to which it belonged. This artifact provided a starting point for Sherstobitoff to compare the DarkSeoul malware against other samples McAfee had obtained from previous attacks targeting South Korea (Sherstobitoff, Itai, & Walter, 2013, p. 7). A 2011 piece of malware dubbed httpTroy was the first known sample to mention "Troy" in its compile path, Z:\source\1\HttpTroy\BsDll-up\Release\BsDll.pdb (p. 12). Http Troy was something of an anomaly, having only been detected one time and, while disguised as the AhnLab Smart Update Utility, the dropper actually launched a simple GUI that was visible to the user and installed a non-malicious screensaver containing images related to the March 2010 sinking of the South Korean Navy ship ROKS Cheonan by a suspected North Korean submarine (p. 12). It also dropped an implant, bs.dll, that established an RSA encrypted IRC command and control channel to one of several hardcoded hostnames using functions imported from the Microsoft Cryptography API (p. 11). The dll included a file-mapping function with the unique string "FFFFFFF-198468CD-6937629023-EF90000000" (p. 10). The implant dll would prove to be the key to linking the

© 2016 The SANS Institute Author retains full rights.

generations of Troy malware, as Sherstobitoff was able to locate several structurally identical samples in McAfee's sizable malware repository (p. 9).

The first appearance of bs.dll was in a 2009 - 2010 military espionage campaign, and was dubbed NSTAR from its compile path of E:\Work\BackUp\2011\nstar_1103\BackDoor\BsDll-up\Release\BsDll.pdb (Sherstobitoff, Itai, & Walter, 2013, p. 8). It contained the same file mapping function and IRC/HTTP C2 scheme. NSTAR was followed by two other 2010 variants, EagleXP (D:\VMware\eaglexp(Backup)\eaglexp\vmshare\Work\BsDll-up\Release\BsDll.pdb) and Chang (D:\\Chang\\vmshare\\Work\\BsDll-up\\Release\\BsDll.pdb) (Sherstobitoff, Itai, & Walter, 2013, p. 10). Each variant included a different hardcoded list of compromised web servers, indicating that the command and control infrastructure had been already been compromised in preparation for campaign prior to the compilation of each variant (Sherstobitoff, Itai, & Walter, 2013, p. 12). Aside from the change in C2 hostnames and compile times, the bs.dll implants from NSTAR, EagleXP, Chang, and Http Troy were essentially identical.

A closer examination of bs.dll indicated that it was designed to search for certain strings, both in English and Hangul (the Korean character set) corresponding to such military terms as "Army", "Division", "Corps" and "weapon" in addition to more generic search terms like "password", "hacking" and "exploit" (Sherstobitoff, Itai, & Walter, 2013, p. 22). The presence of these search terms is a clear indicator that the malware was designed to target sensitive military information. Each of the observed variants of the Troy implants encrypted stolen data prior to exfiltration using the same unique, hard coded password "dkwero38oerA^t@#" (p. 23).

Beginning in 2012, a second generation of the Troy malware made its appearance in a dropper known as Http Dr0pper (Z:\1Mission\Team_Project\ [2012.6~]\HTTP Troy\HttpDr0pper\Win32\Release) that was disguised as AhnlabUpdate.exe and installed an implant with filename HTTPSecurityProvider.dll (Sherstobitoff, Itai, & Walter, 2013, p. 13). While not identical to bs.dll, this implant used the same unique file-mapping

© 2016 The SANS Institute Author retains full rights.

function and also employed the Microsoft Cryptography API to secure its IRC communications. This was followed shortly by a similar variant known as Tong (E:\Tong\Work\Op\1Mission\Team_Project\[2012.6~]\HTTP Trojan 2.0\HttpDr0pper\Win32\Release) (p. 13).

TDrop, the third generation of Troy malware, was detected in early 2013 and contained a number of advancements allowing it to operate effectively in modern Windows environments as well as anti-reverse engineering features (Sherstobitoff, Itai, & Walter, 2013, p. 14). TDrop continued to use familiar compile paths, D:\Work\Op\Mission\TeamProject\[2012.11~12]\TDrop\Dropper32\Release\Dropper.pdb, but was significantly more modular, containing an executable installer, RunCmd.exe, a configuration file, RunCmd.ini and two separate DLL's, payload32.dll and payload64.dll. When executed, RunCmd.exe extracted and ran AhnlabUpdate.exe, a variant of the Http Dr0pper of which it injected one of the two implant DLL's into svchost.exe based on the operating system architecture (p. 15). The implants both contained code to cause them to terminate if they detected the presence of a debugger or automated analysis software that attempted to monitor API calls by the implant.

Around the same time in early 2013, the most current versions of the Troy malware, Concealment Troy, and 3RAT made their appearance (Sherstobitoff, Itai, & Walter, 2013, p. 15). Both used the similar compile paths: Z:\\Work\\Make Troy\\Concealment Troy\\Exe_Concealment_Troy(Winlogon_Shell)\\SetKey_WinlogOn_Shell_Modify\\BD_Installer\\Release\\BD_Installer.pdb and Z:\Work\Make_Troy\3RAT_Project\3RATClient_Load\Release\3RATClient, respectively. Concealment Troy was similar to TDrop but abandoned the IRC command and control channel in favor of strictly HTTP communication (p. 16).

When the links between the malware are examined, a gradual progression from NSTAR to 3RAT can be seen. The pattern of feature accretion around a central code base should be familiar to any developer. New functionality is implemented and old features

© 2016 The SANS Institute Author retains full rights.

are deprecated as needed, but many core functions are retained from version to version. No coder is eager to rewrite tested and working functions that still prove useful. In this respect, malware authors are no different than any other coder and it is unsurprising to find the same file handles and cryptography functions included in multiple generations of malware. The minor alterations such as beacon domains and different filenames would allow new variants to evade many signature-based detection systems using signatures developed from previous samples without the time-consuming process of rewriting the entire code base for each campaign.

In addition to the DarkSeoul attacks and the ongoing military espionage operation, the Operation Troy campaign was suspected to have been involved in several previous attacks against South Korea, including the July 2009 DDoS Attacks and the "10 Days of Rain" DDoS attacks in 2011 (Sherstobitoff, Itai, & Walter, 2013, p. 8). The same group was also linked to a June 2013 cyber-attack against the South Korean government, during which they masqueraded as a purported Anonymous splinter group calling themselves "High Anonymous" (Symantec, 2013).



Author Name, email@address

© 2016 The SANS Institute Author retains full rights.

The same group would also be implicated in the aforementioned 2014 Sony attack, during which they deployed similar wiper malware and left similar, taunting messages, now using the name "Guardians of Peace (GOP)" (Krebs, 2014).



4. Conclusion

4.1. Lessons Learned

In the aftermath of the DarkSeoul attacks, numerous security blogs commented on the lack of technical sophistication exhibited by the actors, compared to the typical state sponsored cyber-espionage campaigns (Marpaung & Lee, 2013). Mainstream, non-technical media outlets were quick to use the terms "cyber-terrorism" or "cyber-warfare", while the more technical security researchers scoffed at such designations and in some cases, expressed doubt that the attacks were, indeed state sponsored (Schwartz, 2013). An important distinction in comparing such disparate cases is the difference between espionage and warfare, whether conventional or computerized.

Author Name, email@address

© 2016 The SANS Institute Author retains full rights.

In espionage, the goal is to collect information on an opponent, while avoiding detection, as the detection of the asset would result in a loss of its capability and the information it was providing. Espionage is frequently a slow, painstaking operation, taking years to develop an asset that has the ability to report on the information being sought. Ideally, an effective espionage operation is never detected, and if it is, cannot be traced back to its origin. These requirements result in the development and maintenance of tradecraft such as false identities, cover stories, front companies and covert communication channels. All of these methods can be time-consuming and require significant resources to effectively backstop.

By contrast, the goal of warfare is to inflict damage on an opponent. While operational security and avoiding detection are critical before an attack is launched to ensure the element of surprise and deny the opponent the chance to prepare for and stop the attack, the target must inevitably realize they are under attack. During and after an attack, it is frequently advantageous to conceal what aspects of the attack are possible, in order to create confusion in the opponents' decision-making process and prevent effective retaliation. In warfare, an attack should generally employ the minimum level complexity that will achieve the goal. Indeed, the level of an attack's sophistication is frequently inversely proportional to its destructive magnitude. For example, highly targeted Special Forces operations are effective in attacking a small handful of well defended, high-value targets behind enemy lines, where a much less sophisticated artillery barrage is far more effective in targeting a large mass of ground forces.

When placed in this context with its conventional parallels, the DarkSeoul attacks clearly fall into the category of cyber-warfare, albeit asymmetric warfare, with the obvious goal of causing damage to a rival nation. In this context, the sophistication of the attack is logical, given its operational objectives and large number of targets.

4.2. Critical Security Controls Failures

A coordinated attack by a state sponsored adversary is, perhaps, the most difficult of all cyber threats for any organization to defend against. When confronted by a well-

© 2016 The SANS Institute Author retains full rights.

secured network, a traditional hacker or hacktivist may get bored, frustrated or find an easier target. Similarly, a for-profit hacker will move on when confronted with a challenge that renders a target unprofitable. A state-sponsored hacker, however, is a government employee, contractor or member of the military whose full-time job is to comprise the assigned target and will continue to work toward that end until they succeed or receive different orders.

The DarkSeoul attack exhibited the coordination and persistence commonly associated with state-sponsored cyber-espionage and indeed was later found to have been launched using the same tools and infrastructure as an ongoing North Korean cyber-espionage campaign. The widespread nature of the attacks makes it difficult to pinpoint the initial point of compromise though it is clear that several different critical security controls were subverted during the course of the attacks. Malware defenses failed to detect any of the dropper, remote access Trojan or wiper malware, but the root critical security control that failed, in this case, was account monitoring and control.

The key to the attackers' ability to distribute their destructive payload to tens of thousands of victim systems was their access to the AhnLab's patch management software. This access, using stolen legitimate credentials, gave the attackers the ability to install software using a trusted mechanism that was, itself exempt from suspicion. Most IT personnel and even most incident responders immediately filter out the constant stream of patch management activity in the logs of any computer or network that uses such a system. Without this access, it is doubtful that the DarkSeoul attackers would have been able to affect as many systems as they did. It is unlikely that the attack could have been completely prevented, however, denying them access to the patch management system might have delayed the attack or forced North Korea to settle for a much smaller scale attack if they were operating on an operational or political deadline.

4.3. Recommendations

The DarkSeoul attacks clearly demonstrate the importance of monitoring account access patterns for anomalies. It is a common mistake in network monitoring to focus on

© 2016 The SANS Institute Author retains full rights.

unsuccessful login attempts and ignore successful logins. While failed logins can certainly indicate malicious activity, the successful logins from compromised accounts, particularly administrative accounts, can be far more damaging as can be seen in this case.

A number of different approaches can help to mitigate this attack vector, but none is as important as being aware of the usual patterns of activity and looking for logins that do not fit the pattern. Red flags like a user logging in from an unfamiliar IP, outside of business hours, or while the user is on vacation can indicate their account has been compromised. While detection of these anomalies can be automated to some extent by intelligent pattern matching and well-designed alerting criteria, there is no substitute for skilled human inspection. Some suspicious logins may have a perfectly reasonable explanation, but scrutiny and follow-up are required to make this determination. Additionally, steps such as limiting the number of administrative accounts, only allowing administrative logins from internal systems and enforcing two-factor authentication can provide additional protection from compromised user accounts.

Author Name, email@address

© 2016 The SANS Institute Author retains full rights.

References

Sherstobitoff, Ryan, and Liba, Itai, and Walter, James. (2013, July 8). *Dissecting Operation Troy: Domestic Intelligence Gathering.* McAfee Labs. Retrieved from http://www.mcafee.com/us/resources/white-papers/wp-dissecting-operation-troy.pdf.

ASEC Threat Research & Response Blog. (2013, March 21). *Major broadcasters and Bank computer network failure caused malware analysis* [Web log post]. Retrieved from http://asec.ahnlab.com/926 through Google Translate (Original in Korean).

Dong-A, (2013, March 21). *Broadcasters Highly Hacking Attack Situation*. Retrieved from http://news.donga.com/Main/3/all/20130320/53842793/1 through Google Translate (Original in Korean).

Schwartz, Matthew A. (2013, March 25). *How South Korean Banking Malware Spread.* Dark Reading [Web log post]. Retrieved from http://www.darkreading.com/attacks-and-breaches/how-south-korean-bank-malware-spread/d/d-id/1109239.

Marpaung, Jonathon AP, and Lee, HoonJae. (2013, July). *Dark Seoul Cyber Attack: Could it be Worse?* Conference of Indonesian Student Association in Korea. Retrieved from http://cisak.perpika.kr/wp-content/uploads/2013/07/2013-08.pdf.

General Dynamics Fidelis Cybersecurity Systems. (2013, March 21). DarkSeoul/Jokra Analysis and Recovery. Fidelis Threat Advisory #1008. Retrieved from http://www.fidelissecurity.com/sites/default/files/FTA%201008%20-%20Darkseoul-Jokra%20Analysis%20and%20Recovery.pdf.

Dell SecureWorks Counter Threat Unit(TM) Threat Intelligence. (2013, March 21). Wiper Malware Analysis Attacking Financial Sector. Dell SecureWorks Cyber Threat Intelligence [Web log post]. Retrieved from http://www.secureworks.com/cyber-threat-intelligence/threats/wiper-malware-analysis-attacking-korean-financial-sector.

Minji, Lee. (2013, April 10). Gov't confirms Pyongyang link in March cyber attacks. Yonhap News, Retrieved from

Author Name, email@address

© 2016 The SANS Institute Author retains full rights.

http://english.yonhapnews.co.kr/northkorea/2013/04/10/49/0401000000AEN20130410007352320F.HTML.

Branigan, Tania. (2013, March 21). South Korea on alert for cyber-attacks after major network goes down. The Guardian. Retrieved from http://www.theguardian.com/world/2013/mar/20/south-korea-under-cyber-attack

Global Research and Analysis Team (GReAT). (2013, March 20). South Korean Whois Team Attacks. Kaspersky Securelist [Web log post]. Retrieved from https://securelist.com/blog/incidents/65106/south-korean-whois-team-attacks/.

Trend Micro. (2013, March 21). How Deep Discovery Protected Against The Korean Cyber Attack. TrendLabs Security Intelligence Blog [Web log post]. Retrieved from http://blog.trendmicro.com/trendlabs-security-intelligence/how-deep-discovery-protected-against-the-korean-mbr-wiper/.

Krebs, Brian. (2104, December 23). The Case for North Korea's Role in Sony Hack. Krebs on Security [Web log post]. Retrieved from http://krebsonsecurity.com/2014/12/the-case-for-n-koreas-role-in-sony-hack/#more-29249.

Symantec Security Response. (2013, June 26). Four Years of DarkSeoul Cyberattacks South Korea Continue on the Anniversary of Korean War. Symantec Security Response Blog [Web log post]. Retrieved from http://www.symantec.com/connect/blogs/four-years-darkseoul-cyberattacks-against-south-korea-continue-anniversary-korean-war.

[untitled photograph of crashed computer terminal]. (2013). Retrieved from http://news.donga.com/Main/3/all/20130320/53842793/1.

Author Name, email@address

© 2016 The SANS Institute Author retains full rights.