Companion report

HP Security Briefing
Episode 16, August 2014

Profiling an enigma: The mystery of North Korea’s cyber threat landscape

HP Security Research

Table of Contents

Introduction ................................................................................................................................. 3
Research roadblocks .................................................................................................................. 4
Ideological and political context .............................................................................................. 5
   Juche and Songun .................................................................................................................. 5
   Tension and change on the Korean Peninsula ...................................................................... 8
North Korean cyber capabilities and limitations ................................................................. 10
   North Korean infrastructure ............................................................................................... 10
   An analysis of developments in North Korean cyberspace since 2010 ............................. 14
   North Korean cyber war and intelligence structure ........................................................... 21
North Korean cyber and intelligence organizational chart .................................................... 26
North Korea’s cyber doctrine, strategies and goals ............................................................... 26
Cyber warfare operations ........................................................................................................ 27
Gaming for profit and pwnage ................................................................................................ 29
Intelligence and counterintelligence ....................................................................................... 29
Psychological operations ......................................................................................................... 32
Electronic warfare .................................................................................................................... 38
Training cyber warriors .......................................................................................................... 39
Important political and military ties ..................................................................................... 42
China ..................................................................................................................................... 42

© Copyright 2014 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.
Episode 16

Thank you for subscribing to Episode 16 of the HP Security Briefing. In this edition we discuss the cyber landscape within the Democratic People’s Republic of Korea.

**Introduction**

The Democratic People’s Republic of Korea (DPRK), known in the West as North Korea, is a unique country with a military-focused society and an unconventional technology infrastructure. While North Korea was formerly on the U.S. list of state sponsors of terrorism, it was removed in 2008.\(^1\) However, due to North Korea’s hostility toward other nations, its pursuit of nuclear weapons, and human rights violations against its own citizens, the United Nations and many Western entities have placed sanctions and embargoes against North Korea.\(^2\) \(^3\) For example, U.S. export laws forbid the sale of dual-use technologies, or those that can be used or repurposed for both civilian and military use, to North Korea.\(^4\) \(^5\) Additionally, the U.S. has a military alliance with the Republic of Korea (ROK), known in the West as South Korea, North Korea’s primary target of conflict.\(^6\)

Due to North Korea’s global interactions, its cyber warfare capabilities are of particular interest to the U.S. According to a 2009 report by Major Steve Sin, an intelligence analyst at U.S. Forces Korea, North Korean hackers have successfully penetrated U.S. defense networks more frequently than any other country that has targeted U.S. defense assets.\(^7\) While Major Sin may have been overly optimistic about North Korea’s abilities, it is clear that they should not be underestimated. Frank Cilluffo, co-director of the Cyber Center for National and Economic Security at George Washington University, testified before Congress that North Korea’s cyber capability "poses an important 'wild card' threat, not only to the United States but also to the region and broader international stability..."\(^8\) In an April 2014 testimony given to the House Armed Services Committee, General Curtis M. Scaparrotti noted that “North Korea remains a significant threat to United States’ interests, the security of South Korea, and the international community due to its willingness to use force, its continued development and proliferation of nuclear weapon and long-range ballistic missile programs, and its abuse of its citizens’ human rights, as well as the legitimate interests of its neighbors and the international community.” Scaparrotti stressed that “While North Korea’s massive conventional forces have been declining due to aging and lack of resources...North Korea is emphasizing the development of its asymmetric capabilities. North

---

1. [http://thecable.foreignpolicy.com/posts/2010/05/25/why_the_state_department_wont_put_north_korea_back_on_the_terror_list](http://thecable.foreignpolicy.com/posts/2010/05/25/why_the_state_department_wont_put_north_korea_back_on_the_terror_list)
2. [http://www.sanctionswiki.org/North_Korea](http://www.sanctionswiki.org/North_Korea)
3. [https://www.fas.org/irp/offdocs/eo/eo-13551.pdf](https://www.fas.org/irp/offdocs/eo/eo-13551.pdf)
5. [http://www.state.gov/strategictrade/overview/](http://www.state.gov/strategictrade/overview/)
Korea’s asymmetric arsenal includes...an active cyber warfare capability.” While one would expect the regime’s digital infrastructure to also suffer from aging or lack of resources, these factors do not take away from their technical abilities to wage cyber warfare.

While the U.S. views North Korea’s cyber warfare program as the regime’s foray into modern asymmetrical warfare, South Korea views the regime’s cyber capabilities as a terrorist threat, -a build-up for an impending multifaceted attack. It is important to note that, to date, no such attack has occurred. According to a report written by Captain Duk-Ki Kim, Republic of Korea Navy officer and Ph.D. “...the North Korean regime will first conduct a simultaneous and multifarious cyber offensive on the Republic of Korea’s society and basic infrastructure, government agencies, and major military command centers while at the same time suppressing the ROK government and its domestic allies and supporters with nuclear weapons.” South Korea’s view of North Korea as a terrorist threat may be an attempt to downgrade North Korea politically, since South Korea does not recognize the regime as a legitimate state. South Korean reports also claim that North Korea’s premier hacking unit, Unit 121, trails Russia and the U.S. as the world’s third largest cyber unit. While this claim may be exaggerated, in 2012, South Korean reports estimated North Korea’s hacker forces at around 3000 personnel. In a July 2014 report from South Korea’s Yonhap News Agency, that figure was upgraded to 5900 hacker elite. We must stress that although these claims have not been corroborated, South Korea has taken the regime’s cyber threats very seriously and is reportedly training 5000 personnel to defend against North Korean cyber attacks.

Obtaining details on North Korea’s cyber warfare capabilities is not an easy task. This paper will examine the known cyber capabilities of North Korea’s regime and how the country maintains secrecy in these matters. Through information obtained via open source intelligence (OSINT), we will present what is known about North Korea’s cyber warfare and supporting intelligence and psychological operations capabilities.

**Research roadblocks**

The following conditions proved to be research roadblocks when gathering intelligence regarding North Korea’s cyber warfare capabilities:

- Much of the intelligence available on North Korea is dated and may not accurately reflect the regime’s current capabilities.
- Much of the intelligence available on North Korea comes from U.S. or South Korean military or agency reports. These reports omit details that are likely classified, such as specific IP addresses and individual actor information.
- While South Korea is an ally of the United States, its reports on North Korean cyber activity potentially contain incomplete or biased information. Cultural factors that stem
from a history of tension and conflict between the two nations may skew perception and make objectivity difficult.  

- North Korea’s Internet infrastructure and the regime’s strict control over its use ensures that there are no rogue actors and that all officially sanctioned actors exercise careful OPSEC and PERSEC practices in order to prevent inadvertent information leaks. In other words, there was no significant identifying information in the form of an OSINT trail left behind by the actors. This hinders collection of original, actionable threat intelligence and individual actor attribution.

- North Korea is well-isolated from the outside world, and its strong intelligence and psychological operations presence effectively creates confusion via counterintelligence and disinformation about the regime’s capabilities. For this reason, any “official” reports emanating from North Korea must be taken with a grain of salt. This also hinders attempts to obtain original, actionable threat intelligence.

**Ideological and political context**

In order for Westerners to understand the North Korean mindset, it is necessary to examine the key components of North Korean political and ideological thought. It is also necessary to provide a brief explanation of how North Korea and South Korea view one another, in order to understand the basis for conflict between the two.

**Juche and Songun**

North Korea has two primary ideologies that provide context for the regime’s motivations and activities: juche (ju-cheh) and songun (sun-goon). Juche is the official political ideology of North Korea. It was instituted in 1972 and is based on the ideologies of Kim Il-Sung, the founder of the DPRK. Juche emphasizes self-reliance, mastering revolution and reconstruction in one’s own country, being independent of others, displaying one’s strengths, defending oneself, and taking responsibility for solving one’s own problems. North Korea’s air-gapped intranet, described below, exemplifies this philosophy in the country’s cyber infrastructure. The juche philosophy explains North Korea’s disdain for outside cultural and political influence. Juche challenges North Koreans to contribute to the regime’s chaju (ja-ju), a concept of national sovereignty and independence. The regime’s greatest fear is internal dissent and resulting destabilization. In a June 2014 Reddit AMA session, Dr. Andrei Lankov, an expert on North Korean culture and society, noted “there are also serious signs of public alienation and discontent. And I cannot rule out a public outbreak of such discontent in the near future. Of course, if it happens, it will have a serious impact on the government.” Despite North Korea’s strong conviction in juche, the regime collaborates with and receives support from other nations. However, due to this deep-seated
ideology, it is doubtful that North Korea fully trusts these apparent allies. Later in this document, we will show that North Korea relies heavily on China for Internet access. North Korea also collaborates with China and Russia to train its cyber warriors and has longstanding political and military relationships with several nations.

Songun is North Korea’s “military first” doctrine. Songun emphasizes the priority of the military in resource allocation and political and economic affairs. This doctrine stems from the belief that the military is vital for preservation of chaju. Understanding songun mindset gives context for this potential threat actor’s motivations. According to a 2013 Congressional report, the strategy established under former leader Kim Jong-II focused on “internal security, coercive diplomacy to compel acceptance of its diplomatic, economic and security interests, development of strategic military capabilities to deter external attack, and challenging South Korea and the U.S.-South Korean alliance.”

North Korea’s songun permeates the lives of all North Korean citizens. Article 58 of the North Korean Constitution states that the nation should base itself on a nationwide defense system that includes all people. North Korea, with a population of 25 million, has an active duty force of 1.19 million personnel, the fourth largest in the world. The country’s reserve and paramilitary units comprise 7.7 million additional personnel. In other words, over a third of the country’s population serves in a military or paramilitary capacity.

Some North Korean youth aged 7-13 are inducted into the Korean Children’s Union. The Korean Children’s Union is responsible for indoctrinating youths who pledge to build up their strength to later defend the regime.

---

Figure 1 A group of North Korean children being inducted into the Korean Children's Union.  

Figure 2 Members of the Korean Children’s Union with the regime’s leader Kim Jong Un.  

---

Children aged 14-16 can begin military training as members of the Young Red Guards, a paramilitary unit. Beginning at age 17, North Koreans are eligible to join the Reserve Military Training Unit. The Reserve Military Training Unit forms the core of North Korea’s reserves and is typically assigned to the front or regional defense in wartime. The youngest age at which a citizen can be conscripted for active duty is unclear; reported ages range from 18-20. Youths can volunteer for active duty service at age 16 or 17. The Worker-Peasant Militia, or Red Guards, includes males ages 17-60 and unmarried females ages 17-30 who are not part of active duty units or the Reserve Military Training Unit.

The regime has an impressive number of conventional weapons, considering the nation’s small land area and population size. According to statistics released by CNN in 2014, North Korea’s ground arsenal includes 4100 tanks, 2100 armored vehicles, and 8500 pieces of field artillery. The regime’s sea weaponry includes 70 submarines, 420 patrol combatants, and 260 amphibious landing craft. Their airpower includes 730 combat aircraft, 300 helicopters, and 290 transport aircraft. While the limits of the regime’s ballistic missile program are unknown, North Korea is thought to have fewer than 100 short-range missiles and fewer than 100 medium to long-range missiles. However, in recent years, North Korea has suffered oil, fuel, electricity, and food shortages. Without aid from another entity, the regime does not have sufficient resources to maintain and sustain the majority of its weapons and associated personnel for rapid deployment or prolonged combat.

Tension and change on the Korean Peninsula

Tension between North and South Korea has continued well past the armistice meant to end the Korean War. Neither nation recognizes the other as a legitimate state. South Korea’s constitution legally defines South Korean territory as the entire Korean peninsula and its adjacent islands, with “North Korea” being a part of South Korea. North Korea also claims to be the sole government of the Korean Peninsula. Each country’s claim of sovereignty and refusal to acknowledge the other as a legitimate state creates the condition for perpetual conflict. North Korea’s negative sentiment towards the U.S. stems from two major factors: the U.S. – South Korea military alliance and North Korea’s perception that the U.S. is imperialistic and prone to exploitative capitalism.
In recent years, two primary factors have heavily influenced the current state of North Korea’s relations with South Korea and her allies: the rise of the regime’s leader Kim Jong Un and the inauguration of South Korean president Park Guen Hye. Kim Jong Un officially rose to power in April 2012, following the death of his father Kim Jong Il in December 2011. While his age remained a mystery for quite some time, it was later revealed that he was born in January 1983, making him age 31 at present. This makes Kim Jong Un the world’s youngest leader of an established nation. The young leader’s rise to power brought about several changes in North Korea. First, Kim Jong Un’s personal life is more public and more extravagant than that of his father. Unlike his father, the young Kim is often accompanied by his wife when making public appearances. Second, the young Kim, who is more high-tech than his predecessor, is reported to have an affinity for luxury items and is an avid gamer and basketball fan. Third, Kim Jong Un is more totalitarian than his father. Following his rise to power, the regime reportedly expanded its labor camps, and more military resources were allocated to target those attempting to defect. Kim also executed his own uncle, a high-ranking official who did not share his ideals. These moves indicate the regime’s priority to deter internal destabilization and dissent, which is perceived to be a greater threat than outside adversity. According to Phil Robertson, deputy Asia director at Human Rights Watch, “The government now recognizes that the accounts of escaping North Koreans reveal Pyongyang’s crimes – so it is doing what it can to stop people from fleeing.” Under Kim Jong Un’s rule, the regime has stepped up its nuclear materials production, and the propaganda distributed by state media has become more menacing.

The regime’s response to perceived threats has also become more volatile. Christian Whiton, a former deputy envoy to North Korea, noted that following Kim Jong Un’s rise to power, “the regime still acts in a very belligerent manner, but it seems less predictable, and more random.” Ellen Kim, assistant director of the Korea Chair at the Center for Strategic and International Studies, assessed the situation thusly: “Since [Kim Jong Un] took power he has purged almost all of his elder guardians ... and filled his surroundings with new faces. We are in a situation where we are learning about him a little bit every day through his unpredictable behavior and actions, which is why the current situation with North Korea is a lot more dangerous than before.” The regime’s recent reaction to an upcoming film supports these statements. The plot for the comedy film “The Interview” follows two talk show hosts who are asked to assassinate Kim Jong Un. The regime even sent a complaint about the movie to the UN. In response to the film, a North Korean official stated, “The enemies have gone beyond the tolerance limit in their despicable moves to dare hurt the dignity of the supreme leadership.” The official referred to the movie as “the most undisguised terrorism and a war action to deprive the service personnel and people of the DPRK of their mental mainstay and bring down its social system.” The official also issued a threat: “If the U.S. administration connives at and patronizes the screening of the film, it will invite a strong and merciless countermeasure.” This reaction demonstrates North Korea’s priority of preserving the
regime’s self-perceived dignity in the global arena and its intolerance of any disrespect directed at the Kim family.

While tensions between North and South Korea have persisted since the Korean War, these tensions escalated following the 2013 inauguration of South Korea’s current president, Park Geun Hye. Her platform, in her words, is as follows: “North Korea must keep its agreements made with South Korea and the international community to establish a minimum level of trust, and second there must be assured consequences for actions that breach the peace. To ensure stability, trustpolitik should be applied consistently from issue to issue based on verifiable actions, and steps should not be taken for mere political expediency.” Shortly after Park’s inauguration, North Korea denounced UN Security Council Resolution 2094, which is “a resolution strengthening and expanding the scope of United Nations sanctions against the Democratic People’s Republic of Korea by targeting the illicit activities of diplomatic personnel, transfers of bulk cash, and the country’s banking relationships, in response to that country’s third nuclear test on 12 February [2013].” North Korea also responded strongly to joint U.S.-South Korea military exercises in March 2013, as is noted later in this paper.

### North Korean cyber capabilities and limitations

#### North Korean infrastructure

North Korea’s cyber infrastructure is divided into two major parts: an outward-facing Internet connection and a regime-controlled intranet. North Korea’s outward-facing Internet connection is only available to select individuals and is closely monitored for any activity that is deemed anti-regime. Individuals using the outward-facing Internet connection must be authorized. In 2013, Jean H. Lee, the Associated Press bureau chief in Pyongyang, stated that foreigners visiting North Korea are allowed Internet access with no firewalls. Common citizens are limited to using the Kwangmyong (gwang me-young), a nationwide intranet with no access to the world outside North Korea. According to Lee, Kwangmyong allows citizens “access to the state media, information sources that are vetted by the government, and picked and pulled from the Internet and posted to their intranet site.” As of May 2013, North Korea had only one “Internet café.” A 2003 report from the Office of the National Counterintelligence Executive stated that North Korea’s “Internet café” was “the only place in North Korea for the public to access the Internet” and that foreigners were allowed to access the Internet from this café. Whether citizens are allowed to access the Internet from this location is unknown.

Star Joint Venture Co. is responsible for providing North Korea’s Internet access. Star Joint Venture Co. was established by the Post and Telecommunications Corporation in cooperation with Loxley

---

54http://www.un.org/News/Press/docs/2013/sc10934.doc.htm
57http://www.computerworld.com/s/article/9177968/North_Korea_moves_quietly_onto_the_Internet?taxonomyId=18&pageSize=2
Pacific in Thailand. In December 2009, Star Joint Venture became responsible for North Korea’s Internet address allocation. Previously, Internet access was provided by a German satellite link via Korea Computer Center Europe or via direct connections with China Netcom, which was later merged into China Unicom. By October 2010, North Korea had made its first known direct connection to the Internet, hosting an outward-facing Korean Central News Agency website accessible from the global Internet. However, many of North Korea’s globally accessible websites are hosted in other countries. In 2001, South Korean reports indicated that North Korea had joined the International Telecommunications Satellite Organization (INTELSAT). As of April 2012, North Korea reportedly used the Intelsat connection, which appeared in border gateway protocol (BGP) announcements. Some reports referred to the Intelsat connection as North Korea’s backup Internet connection, in case the China Unicom connection fails. A March 2013 post on the blog rdns.im showed that North Korea no longer used the Intelsat connection. In the blog post, the author noted his method for proving that The Pirate Bay was not hosted in North Korea. While his analysis of The Pirate Bay’s hosting is irrelevant to our research, he did detail that 175.45.177.0/24 always routes through AS4837, and AS131279. AS131279 is Star-KP, North Korea’s Star Joint Venture Company, and AS4837 is China Unicom. The author concluded that “all [traffic] is ONLY routed through China Unicom and NOT through Intelsat.” In February 2014, North Korean and South Korean officials agreed to extend Internet access to Kaesong Industrial Zone, a jointly operated industrial complex just north of the border. However, this would likely require a major electrical and network infrastructure expansion.

North Korea’s electrical grid cannot support a large technological infrastructure. Electrical power is reported to be unreliable and sporadic, with many citizens only receiving a few hours of electricity per day.

61 http://www.northkoreatech.org/2011/05/19/more-details-on-star-joint-venture/
62 http://www.computerworld.com/s/article/9177968/North_Korea_moves_quietly_onto_the_Internet?taxonomyId=18&pageNumber=2
65 http://www.northkoreatech.org/2012/04/08/dprk-gets-second-link-to-internet/
66 http://www.computerworld.com/s/article/9237652/North_Korea_39_s_Internet_returns_after_36_hour_outage
68 http://www.northkoreatech.org/2014/02/10/internet-coming-to-kaesong-industrial-zone/
Figure 3 North and South Korean power grid

The photo above (Figure 3), from the International Space Station, shows North Korea’s sparse power grid, in comparison with surrounding nations.\(^71\) We have highlighted North Korea in red.

Koryolink, the country’s only cellular phone network,\(^72\) is tightly controlled by the regime.\(^73\) Cell phone data plans are not available to most users. Most cellular phones cannot access the Internet and can only make domestic calls.\(^74\) According to a 2013 report, North Korea has a 3G data network for cellular phones. Visiting reporter Jean H. Lee purportedly used this 3G network to post to both Twitter and Instagram. However, citizens are not generally allowed to use the 3G network.\(^75\)

Email is also regulated by the regime. The first email provider in North Korea was Silibank. Silibank has servers in Pyongyong and Shenyang and is a joint venture with China. The North Korean Silibank homepage is silibank.net, and the Chinese homepage is silibank.com. In order to use the email service, users had to initially register, provide personal information, and pay a registration fee and monthly service fees.\(^76\) This registration information was current as of 2001. However, it is unknown whether the same process still applies.

WHOIS records for silibank.net show that the site was registered anonymously via a Japanese registrar. This information can be found in Appendix A at the end of this paper.

---

Korea Computer Center (KCC) is North Korea’s leading government research center for information technology. KCC has eleven regional information centers and eight development and production centers. Other countries with KCC branch offices include China, Syria, Germany, and United Arab Emirates. KCC has a vested interest in Linux research and is responsible for the development of North Korea’s national operating system, Red Star OS, which is discussed in more detail below. KCC’s other projects have included a proprietary search engine, a document writer, a game called Jang-Gi, the Kwangmyong intranet, a food study program, a Korean input method editor, a pen-based English-Korean and Korean-English translator, Korean voice recognition software, a video conferencing system, a distance education system, SilverStar Paduk software, HMS Player\(^\text{77}\), and the Samjiyon tablet.\(^\text{78}\) In addition to research and development, KCC also monitors websites of foreign government and business entities and conducts technical reconnaissance to blueprint the technical specifications and vulnerabilities in foreign systems and technologies. KCC has also been involved in clandestine information and cyber operations, serving as a command center.\(^\text{79}\)

North Korea’s proprietary operating system is Red Star OS. The development of this Linux-based operating system started in 2002. Red Star OS is only offered in the Korean language and features proprietary software including Naenara (a Firefox-based browser), as well as a text editor, email client, audio and video players, and games.\(^\text{80}\) Red Star OS’s keyboard layouts include Korean, English, Russian, Chinese, and Japanese. Regime ideals extend to Red Star OS. The readme file, which goes with the installation disc, reportedly includes a quote from Kim Jong-II regarding the importance of North Korea having its own Linux-based operating system that is compatible with Korean traditions. While prior versions of Red Star were KDE-based, version 3.0 mimics Apple’s OS X.\(^\text{81}\)\(^\text{82}\) This could indicate the regime leader Kim Jong Un’s preference for the OS X environment, as Kim reportedly uses an iMac.\(^\text{83}\) Citizens do not need permission to obtain Red Star OS. However, the purchase of computers is heavily regulated.\(^\text{84}\) The OS’s design suggests it was developed with means for the regime to monitor user activity.\(^\text{85}\)

North Korea is known to use two IP ranges. 175.45.176.0/22 is North Korea’s own IP block.\(^\text{86}\) Additionally, North Korea’s Telecommunications Ministry is the registered user of China Unicom IP range 210.52.109.0/24.\(^\text{87}\) The country’s only autonomous system (AS) number is AS131279, and its only peer is AS4837, the AS for China Unicom.\(^\text{88}\)

North Korea’s country code top-level domain (ccTLD) is .kp. In 2007, the .kp TLD was initially delegated to and administered by the German-based KCC Europe.\(^\text{89}\) After KCC Europe failed to

\(^{79}\) http://www.lsts.dartmouth.edu/docs/cyberwarfare.pdf
\(^{80}\) http://ashen-rus.livejournal.com/4300.html
\(^{81}\) http://news.bbc.co.uk/2/hi/technology/8604912.stm
\(^{85}\) http://news.bbc.co.uk/2/hi/technology/8604912.stm
\(^{86}\) http://librarycore.org/2012/05/29/investigating-north-koreas-netblock-part-2-dns/
\(^{87}\) https://www.northkoreatech.org/2011/06/26/north-koreas-chinese-ip-addresses/
\(^{88}\) http://news.bbc.co.uk/2/hi/technology/8604912.stm
\(^{89}\) http://news.bbc.co.uk/2012/05/29/investigating-north-koreas-netblock-part-2-dns/
maintain the TLD, it was re-delegated to Star Joint Venture Company. The .kp TLD uses the following nameservers and IP addresses:

<table>
<thead>
<tr>
<th>Nameserver</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>ns1.kptc.kp</td>
<td>175.45.176.15</td>
</tr>
<tr>
<td>ns2.kptc.kp</td>
<td>175.45.176.16</td>
</tr>
<tr>
<td>ns3.kptc.kp</td>
<td>175.45.178.173</td>
</tr>
</tbody>
</table>

Various U.S., U.N, and other sanctions prohibit export of dual-use technologies to North Korea. In light of this, North Korea has managed to develop both hardware and software and hosts an annual National Exhibition of Invention and New Technologies to promote its products. However, the regime has historically failed in its attempts at large-scale production of electronic components. The country’s sparse electrical grid is one of the major obstacles hindering large-scale manufacturing. Additionally, the famine in the early 1990’s negatively impacted existing manufacturing facilities, and the regime simply does not have the capital to modernize those factories. A member of the World International Property Organization (WIPO), North Korea joined the WIPO Patent Cooperation Treaty that protects patents and trademarks worldwide, and leverages intellectual property laws to ensure Westerners do not take credit for North Korean inventions. The regime, in its efforts to isolate its citizens from Western influence, leverages intellectual property laws to ensure Westerners do not take credit for North Korean inventions. This is ironic since foreign-made electronic components are sometimes smuggled into North Korea for military use and for personal use by the regime’s upper echelon.

**An analysis of developments in North Korean cyberspace since 2010**

A comparison of a scan of North Korea's IP ranges in November 2010, just one month after North Korea made its first direct connection to the Internet, and a series of several scans we conducted in May 2014, shows that North Korea has made significant headway in establishing its Internet presence.

In the November 2010 scan, 175.45.176.0 - 175.45.176.16 showed a variety of devices including D-link, Cisco, Linksys, HP, and Nokia devices, and a Juniper networks firewall. Operating systems detected included FreeBSD 6.x, Linux 2.6.x, and Red Hat Enterprise Linux. 175.45.176.14 returned “Naenara” as an html-title. Most hosts in the 175.45.176.xx and 175.45.177.xx ranges were down. As of 2014, IP addresses 175.45.176.0 - 175.45.177.255 appear to be used for websites, nameservers, databases, email, and voice over IP (VoIP). In November 2010, the 175.45.178.xx range showed all hosts down, and the 175.45.179.xx range showed most hosts were down.
In 2014, several webservers and nameservers were found in the 175.45.178.xx range, and several nameservers and mail servers were found in the 175.45.179.xx range. This comparison demonstrates that there has been some growth in DPRK Internet infrastructure over the past four years. However, it seemingly lags behind even most third world nations. The 2014 scans detected dated technology that is potentially susceptible to multiple vulnerabilities and consistently showed the same open ports and active devices on scanned hosts. It is not clear whether the regime failed to notice and react to the scanning or whether the regime allows these open ports and devices to be detected or spoofed to serve as a distraction or possible honeypot.

Domains, nameservers, and mail servers present during the May 2014 scan are listed in Appendix B at the end of this report.

According to Alexa rankings, the three most visited websites in North Korea are kcna.kp, the official website of the Korean Central News Agency (KCNA)\(^\text{100}\); rodong.rep.kp, another North Korean news site\(^\text{101}\); and naenara.com.kp, North Korea’s official web portal.\(^\text{102}\) Naenara translates to “my country”.

The kcna.kp site was registered using a Loxley.co.th email address and is administrated by Star Joint Venture Company. The WHOIS Record can be found in Appendix A.

\(^{100}\) http://dig.do/kcna.kp
\(^{101}\) http://dig.do/rodong.rep.kp
\(^{102}\) http://dig.do/naenara.com.kp
Rodong.rep.kp was registered using the same loxley.co.th email address and is also administered by Star Joint Venture Company. The WHOIS Record for this site can be found in Appendix A.
The WHOIS information for Naenara.com.kp was not available.

Figure 5 A screenshot from the rodong.rep.kp homepage.¹⁰⁴
In March 2013, there were reports that the Chrome browser was blocking Naenara.com.kp due to malware.

Figure 6 A screenshot of the Naenara.com.kp website.

Figure 7 Screenshot of what visitors to Naenara.com.kp saw when using the Chrome browser.

---

106 http://www.rkeconwatch.com/2013/03/25/chrome-blocking-naenara/
107 http://www.rkeconwatch.com/2013/03/25/chrome-blocking-naenara/
It is difficult to say whether this incident is a case of North Korea serving malware or whether a third party took advantage of an improperly secured website.

Several major North Korean websites are hosted outside of North Korea. The popular Uriminzokkiri.com website, whose name translates to “our nation,” is hosted in China. The administrative contact for the website is Kim Sejun, and the email address given as contact information is hyk1979@hotmail.com. The WHOIS Record for this site can be found in Appendix A.

108 http://www.nkconwatch.com/2013/03/25/chrome-blocking-naenara/
Figure 9 A screenshot of the Uriminzokkiri website

The website for Kim Il Sung Open University, otherwise known as “Our Nation School” is also hosted in China. The WHOIS record for this site can be found in Appendix A.

109 http://www.uriminzokkiri.com/
North Korean cyber war and intelligence structure

At the top of North Korea’s military structure is the National Defense Commission (NDC). The NDC is also the highest branch of government and the regime’s supreme policymaking body. Along with the Central Committee of the Workers’ Party of Korea and the Cabinet, NDC is at the top of
North Korea’s political hierarchy. Article 106 of North Korea’s Constitution gives the NDC the following powers:

- The power to establish policies of the state in accordance with the military-first revolutionary line.
- The power to guide the armed forces and oversee defense building.
- The power to supervise and ensure the NDC and its chairman’s orders are executed and to establish necessary measures.
- The power to override any state decisions or directives that are in opposition to the NDC or its chairman’s decisions and directives.
- The power to create or remove central organs of the national defense sector.
- The power to create and bestow military titles above general-grade officer rank.

The NDC oversees several defense and intelligence bodies including the Ministry of State Security, the Ministry of People’s Security, the Ministry of People’s Armed Forces, and the Korean People’s Army. The Ministry of State Security (MSS), also known as the State Security Department, is North Korea’s primary counterintelligence service. It is considered an autonomous agent of the regime and reports directly to leader Kim Jong Un. The MSS’s duties include oversight of North Korean prison camps, investigation of domestic espionage, repatriation of defectors, and overseas counterespionage operations. The Ministry of People’s Security is also known as the Ministry of Public Security (MPS). Focused on domestic order, it oversees North Korea’s national police force, conducts criminal investigations and preliminary examinations, and oversees correctional facilities, excluding prison camps. While the roles of the MSS and MPS focus more on intelligence than on cyber operations, the MSS also reportedly has a communications monitoring and computer hacking group.

The Ministry of People’s Armed Forces (MPAF) administrates the Korean People’s Army (KPA) and oversees the General Staff Department (GSD), which is responsible for operational command and control of North Korea’s armed forces. The General Staff Department also oversees the Reconnaissance General Bureau (RGB), North Korea’s agency for clandestine operations. The RGB has a role in both traditional and cyber operations. In the past, the RGB has sent agents on overseas military assistance missions to train insurgent groups. The RGB reportedly has a special operations forces (SOF) element and oversees six bureaus that specialize in operations, reconnaissance, technology and cyber matters, overseas intelligence collection, inter-Korean talks, and service support. Two of these bureaus have been identified as the No. 91 Office and Unit 121. The No. 91 Office, an office responsible for hacking, operates out of the Mangkyungdae-district of

Unit 121 comprises both an intelligence component and an attack component. One of Unit 121’s command posts is Chilbosan Hotel in Shenyang, China. Unit 121 maintains technical reconnaissance teams responsible for infiltration of computer networks, hacking to obtain intelligence, and planting viruses on enemy networks.

---

112 http://whataboutnorthkorea.nl/2013/02/the-korean-workers-party/
115 http://www.factba.se/handbook-page.php?id=1129700
Pyongyang.\(^{120}\) Unit 121 comprises both an intelligence component and an attack component. Unit 121’s headquarters is in the Moonshin-dong area of Pyongyang, near the Taedong River.\(^{121}\) It also has components that conduct operations from within China. One of Unit 121’s command posts is Chilbosan Hotel\(^{122}\) in Shenyang, the capital of Liaoning Province, which borders North Korea.\(^{123}\) Shenyang is a Chinese military district.\(^{124}\) According to Dr. Alexandre Mansourov, an expert on North Korea and a visiting scholar at the U.S.-Korea Institute at Johns Hopkins University, “They [Unit 121] are believed to have conducted hacking operations from inside China that falsify classified data and disrupt U.S. and South Korean systems.”\(^{125}\) Both Unit 121 and an entity known as Lab 110 are reported to maintain technical reconnaissance teams responsible for infiltrating computer networks, hacking to obtain intelligence, and planting viruses on enemy networks.\(^{126,127}\)

![Figure 11 A map pinpointing the location of the Chilbosan Hotel.\(^{128}\)](maps.google.com)


\(^{126}\) [https://www.usnwc.edu/getattachment/8e487165-a3ef-4ebc-83ce-0ddd7899f16a/The-Republic-of-Korea-s-Counter-asymmetric-Strategy](https://www.usnwc.edu/getattachment/8e487165-a3ef-4ebc-83ce-0ddd7899f16a/The-Republic-of-Korea-s-Counter-asymmetric-Strategy)


\(^{128}\) maps.google.com
Several entities are nested under the Workers’ Party. The Central Party Committee oversees the Central Party Investigative Group, also known as Unit 35. Unit 35 is reportedly responsible for technical education and training of cyber warriors. The Unification Bureau’s Operations Department is responsible for cyber-psychological warfare, organizational espionage, and oversight of Unit 204. Unit 204’s responsibilities include planning and execution of cyber-psychological warfare operations and technological research. The Psychological Operations Department of the North Korea Defense Commission also engages in cyber-psychological warfare. The 225th Bureau, or Office 225, is responsible for training agents, infiltration operations in South Korea, and creation of underground political parties in order to incite disorder and revolution. It plays a more traditional intelligence and psychological operations role, rather than focusing on cyber operations. The United Front Department (UFD) conducts overt operations to create pro-North Korean groups in South Korea. Examples of this activity include the Korean Asia-Pacific Committee and the Ethnic Reconciliation Council. The UFD also manages inter-Korean dialogue and North Korea’s policy toward South Korea. Its operations are also more traditional rather than cyber-focused.
The Liaison Department of the Worker’s Party oversees a faction of ethnic North Koreans residing in Japan who are critical to North Korea’s cyber and intelligence programs. This group, which was established in 1955, is referred to by various names including the Chosen Soren, Chongryon, and the General Association of Korean Residents in Japan. The Chongryon ascribe to *juche* and seek to preserve North Korean culture while living in Japan. They operate North Korean style schools and refuse to assimilate with Japanese culture. According to Mitsuhiro Suganuma, former section head of the second intelligence department of the Japanese Public Security Intelligence Agency (PSIA), “Chongryon is virtually under the direct control of the Liaison Department of the Workers’ Party of Korea, which has been in charge of North Korea’s covert operations and underground activities against South Korea. Chongryon in Japan has been a strong support organization aimed at bringing a revolution in South Korea, or a red unification by force.” He also stated “North Korea will continue to make Chongryon serve as Pyongyang’s pawn in covert operations against South Korea.” The Chongryon are vital to North Korea’s military budget, raising funds via weapons trafficking, drug trafficking, and other black market activities. The group also forms “front companies” abroad that benefit the regime by generating hard currency. One example is Unikotech, which was formed to sell KCC products abroad. The Chongryon’s underground group known as the Gakushu-gumi, or “the study group”, gathers intelligence for North Korea and helps the regime procure advanced technologies. The Chongryon’s role in North Korean intelligence and resource acquisition is discussed below in more detail.

The regime also has several government bodies under the Cabinet that oversee its infrastructure, intelligence, and technological development. These include the Central Scientific and Technological Information Agency (CSTIA), the Ministry of Electronics Industry, and the Ministry of Posts and Telecommunications. The CSTIA collects, analyzes, and processes data regarding advanced science and technology then sends relevant information to appropriate areas of the national economy. The amount of information contained in CSTIA’s technical database makes it North Korea’s largest scientific facility. According to a CIA article, review of CSTIA’s publications showed that China, Russia, and Japan are important sources of technical data. CSTIA’s publications include newsletters and an 18-volume science and technology reference series. The Ministry of Posts and Telecommunications is the body of oversight for Star Joint Venture Co.
North Korea's cyber doctrine, strategies and goals

North Korea’s cyber warfare doctrine has not been clearly stated. However, based on cultural and technical observations, we may deduce that North Korea’s cyber doctrine follows the tenets of juche nationalism and the songun doctrine.

Although North Korea’s limited online presence makes a thorough analysis of their cyber warfare capabilities a difficult task, it must be noted that what is known of those capabilities closely mirrors their kinetic warfare tactics. Cyber warfare is simply the modern chapter in North Korea’s long history of asymmetrical warfare. North Korea has used various unconventional tactics in the
past, such as guerilla warfare, strategic use of terrain, and psychological operations.\textsuperscript{146} The regime also aspires to create viable nuclear weapons.\textsuperscript{147} Asymmetrical warfare is defined as “a conflict in which the resources of two belligerents differ in essence and in the struggle, interact and attempt to exploit each other’s characteristic weaknesses. Such struggles often involve strategies and tactics of unconventional warfare, the ‘weaker’ combatants attempting to use strategy to offset deficiencies in quantity or quality”.\textsuperscript{148}

According to the aforementioned report to the House Armed Service Committee, “Cyber warfare is an important asymmetric dimension of conflict that North Korea will probably continue to emphasize — in part because of its deniability and low relative costs.”\textsuperscript{149} North Korea’s poor economic state\textsuperscript{150}, further explains the regime’s reliance on these tactics. In 2014, the regime reportedly spent 16% of its budget on defense.\textsuperscript{151} The North Korean military places a strong emphasis on information warfare capabilities including political and psychological warfare\textsuperscript{152} and cyber or hacker warfare.\textsuperscript{153}

The report by Capt. Duk-Ki Kim, Ph.D. highlighted North Korea’s counter-asymmetric strategy and ranked each based on intensity and frequency:

![Threat matrix of North Korean asymmetric war capabilities.\textsuperscript{154}](https://www.usnwc.edu/getattachment/8e4b7165-a3ef-4ebc-83ce-0dd78f98e16a/The-Republic-of-Korea-s-Counter-asymmetric-Strategic.pdf)

### Cyber warfare operations

Just ten years ago, experts noted that North Korea was one of the “least network-ready and most isolated societies on the planet.”\textsuperscript{155} Today North Korea’s air-gapped networks and prioritization of resources for military use provide both a secure and structured base of operations for cyber operations and a secure means of communications.\textsuperscript{156} North Korea’s hermit infrastructure creates

---

\textsuperscript{146} http://www.history.army.mil/brochures/kw-balance/balance.htm
\textsuperscript{147} http://www.bbc.com/news/world/asia/pacific-11813699
\textsuperscript{148} http://www.princeton.edu/~achaney/tmve/wiki100k/docs/Asymmetric_warfare.html
\textsuperscript{149} http://docs.house.gov/meetings/AS/AS00/20140402/101985/HHRG-113-AS00-Wstate-ScaparrottiUSAC-20140402.pdf
\textsuperscript{150} http://www.foreignpolicy.com/articles/2013/04/29/7_things_north_korea_is_really_good_at
\textsuperscript{151} http://blogs.wsj.com/korearealtime/2014/04/10/north-korea-details-budget-plans/
\textsuperscript{152} https://www.usnwc.edu/getattachment/8e4b7165-a3ef-4ebc-83ce-0dd78f98e16a/The-Republic-of-Korea-s-Counter-asymmetric-Strategic.pdf
\textsuperscript{153} http://www.giac.org/paper/gsec/1870/information-warfare/103284
\textsuperscript{154} https://www.usnwc.edu/getattachment/8e4b7165-a3ef-4ebc-83ce-0dd78f98e16a/The-Republic-of-Korea-s-Counter-asymmetric-Strategic.pdf
\textsuperscript{155} http://www.apcss.org/Publications/Edited%20Volumes/BytesAndBullets/CH4.pdf
\textsuperscript{156} http://docs.house.gov/meetings/AS/AS00/20140402/101985/HHRG-113-AS00-Wstate-ScaparrottiUSAC-20140402.pdf
a cyber-terrain that deters reconnaissance. Because North Korea has few Internet connections to the outside world, anyone seeking intelligence on North Korea’s networks has to expend more resources for cyber reconnaissance.\textsuperscript{157} A 2003 article by the U.S. Office of the National Counterintelligence Executive assessed that “Development of the nation, rather than empowerment of the individual, appears to be driving DPRK efforts to develop domestic IT infrastructure and industry.”\textsuperscript{158} In November 2013, Kim Jong Un referred to cyber warfare capabilities as a “magic weapon” in conjunction with nuclear weapons and missiles.\textsuperscript{159}

According to Kim Heung-kwang, a North Korean defector and former computer science professor, the regime has the following motivations for expanding its cyber warfare capabilities:\textsuperscript{160}

- Cyber capabilities are a cost-effective way to offset North Korea’s lack of kinetic military prowess.
- North Korea’s school systems place a strong emphasis on math, giving the nation confidence in its programmers, cryptographers, and security researchers.
- In the modern warfare landscape, cyber capabilities are potentially more utilitarian than heavy artillery or aircraft.
- Cyber warfare capabilities provide a platform for espionage, psychological operations, and other forms of non-kinetic warfare.
- Considering the separatist nature of North Korea’s infrastructure, cyber warfare provides a strategic advantage since outbound attacks are possible, but inbound attacks would have limited reach.
- Cyber warfare allows North Korea to leverage the Internet’s inherent flaws for offensive purposes while maintaining its defenses, primarily via air-gapping its most critical networks from the outside world.

North Korea’s attack and defense capabilities reportedly include the following cyber warfare and electronic warfare components: offensive cyber operations (OCO); computer network operations (CNO), which includes both computer network attack (CNA) and computer network exploitation (CNE); distributed denial of service (DDoS);\textsuperscript{161} satellite monitoring; drones; GPS jamming capabilities\textsuperscript{162}; and deployment of electromagnetic pulse (EMP).\textsuperscript{163} North Korea’s OCO and CNO capabilities became apparent as early as 2004, when North Korea reportedly gained access to 33 of 80 South Korean military wireless communication networks. In June 2006, an attack on the U.S. State Department originating in the East Asia-Pacific region coincided with U.S.-North Korea negotiations over the regime’s nuclear missile testing.\textsuperscript{164} A month later, a South Korean military report implicated North Korea’s Unit 121 in hacking the South Korean and U.S. Defense Departments. North Korea also tested a logic bomb in October 2007. A logic bomb is malicious.

\textsuperscript{157}http://www.huffingtonpost.com/2011/07/25/digital-revolution-north-korea_n_908368.html
\textsuperscript{158}http://www.ncix.gov/publications/archives/docs/NORTH_KOREA_AND_FOREIGN_IT.pdf
\textsuperscript{159}http://english.chosun.com/site/data/html_dir/2013/11/05/20131110501790.html
\textsuperscript{160}http://www.aljazeera.com/indepth/features/2011/06/20116201543573839.html
\textsuperscript{161}http://www.defense.gov/pubs/ReporttoCongressMilitaryandSecurityDevelopmentsInvolvingtheDPRK.pdf
\textsuperscript{162}https://www.usnwc.edu/getattachment/8e487165-a3ef-4ebc-b83ce-0dd0789b1e6a/The-Republic-of-Korea-s-Counter-asymmetric-Strateg
\textsuperscript{163}http://www.theregister.co.uk/2014/04/22/norks_drones_made_in_china/
\textsuperscript{164}http://www.informationweek.com/state-department-releases-details-of-computer-system-attacks/d/d-id/1045112?
code programmed to execute based on a pre-defined triggering event. Following the logic bomb test, the UN passed a resolution banning sales of certain computer hardware to North Korea.¹⁶⁵

North Korea considers its cyber warfare capabilities an important asymmetric asset in the face of its perceived enemies, the U.S. and South Korea. While North Korea does not have an immersive digital culture, both the U.S. and South Korea are heavily dependent upon technological infrastructure for social, economic, and political stability.¹⁶⁶ For this reason, a cyber attack that cripples or compromises the reliability of the U.S. or South Korea’s technological infrastructure could have a far-reaching impact.

Gaming for profit and pwnage

North Korea has reportedly used computer games for both illegal capital gain and orchestrating cyber attacks. In 2011, South Korean police arrested five individuals, including one Chinese national, for allegedly collaborating with North Korean hackers affiliated with the Korea Computer Center to steal money via online games.¹⁶⁷ According to South Korean reports, the culprits used an auto-player to quickly progress in the massively multiplayer online role-playing game (MMORPG) “Lineage” and were able to use the game’s market to obtain real currency.¹⁶⁸ In 2013, South Korean officials released information stating they had found evidence that North Korea was using games as a medium for infecting machines and launching cyber attacks. North Korea had used game downloads to infect 100,000 South Korean machines for a botnet used to launch a distributed denial of service (DDoS) attack against Incheon Airport.¹⁶⁹ This clever tactic sought to leverage a seemingly innocent game as a force multiplier in order to amplify the effects of a DDoS attack on a critical infrastructure target. However, in this case, there was little impact on the target.

Intelligence and counterintelligence

North Korea’s intelligence program is one of its strongest military assets, providing foundational support for all other military operations. The regime’s cyber warfare capabilities, in particular, rely heavily on open-source intelligence (OSINT) collection and cyber-espionage.¹⁷⁰ As noted in a CIA publication, “It is a significant irony of our information age that open-source intelligence is contributing to the survival and development of one of the world’s most secretive regimes.”¹⁷¹ Historically, the primary goals of the regime’s intelligence program included collection and dissemination of intelligence concerning any possible political, military, or economic threat to the regime’s security and stability. Secondary goals have included “acquisition of foreign military and civilian technologies and equipment, support of the DPRK’s foreign policy goals, training and

¹⁶⁶ http://www.apcss.org/Publications/Edited%20Volumes/BytesAndBullets/CH2.pdf
¹⁶⁸ http://english.chosun.com/site/data/html_dir/2011/05/06/2011050600827.html
¹⁷⁰ http://docs.house.gov/meetings/AS/AS00/20140402/101985/HHRG-113-AS00-Wstate-ScaparrottiUSAC-20140402.pdf
support for foreign revolutionary and terrorist organizations, and the acquisition of foreign capital for state and intelligence operations.\textsuperscript{172}

North Korea has a broad reach for intelligence collection, which extends to cyber intelligence.\textsuperscript{173} In April 2013, Solutionary, a company providing managed security services, reported a marked increase in both overt attacks and information gathering attempts originating from North Korean IPs. Solutionary refers to any overt external attacks on company networks or attempts to steal data as "touches." They reportedly recorded 12,473 of these touches in February 2013, 11,000 of which were directed at a single financial institution. As a baseline, Solutionary noted that typically only 200 incidents per month are traced to North Korean origin.\textsuperscript{174} This is an interesting claim, considering that attacks attributed to North Korea are usually routed through other countries.

As mentioned above, a faction of ethnic North Koreans residing in Japan, known as the Chongryon, are critical to North Korea’s cyber and intelligence programs and help generate hard currency for the regime. The Chongryon headquarters has been recognized as the de facto North Korean embassy in Japan. In 2012, the organization’s headquarters was seized to pay for the group’s past due debts.\textsuperscript{175}

Figure 15 Headquarters of the Chongryon.\textsuperscript{176}

\textsuperscript{172} http://www.apcss.org/Publications/Edited%20Volumes/BytesAndBullets/CH13.pdf
\textsuperscript{173} http://docs.house.gov/meetings/AS/AS00/20140402/101985/HRRG-113-AS00-Wstate-ScaparrottiUSAC-20140402.pdf
\textsuperscript{174} http://www.usatoday.com/story/tech/2013/04/26/cyberspying-from-north-korean-ip-addresses-spike/2115349/
\textsuperscript{175} http://sundaytimes.lk/?option=com_content&view=article&id=21034:japan-court-approves-seizure-of-nkorea-embassy-media&catid=81:news&Itemid=625
\textsuperscript{176} http://www.rknnews.org/2014/02/chongryon-still-pyongyangs-pawn-in-covert-operations-former-intelligence-officer/
It was then purchased by a monk named Ekan Ikeguchi, who let the Chongryon continue to use the building in what he referred to as a “goodwill gesture”. Ikeguchi is one of the Chongryon’s many ties to organized crime. Ikeguchi was arrested in the past for an attempted coup against the Japanese government. He also has ties to the political group Nihon Seinensya, which is involved in illegal activities in conjunction with the yakuza syndicate Sumiyoshi-kai, which imports and sells amphetamines made in North Korea. North Korea also has black market ties to Sumiyoshi-kai’s rival syndicate, Yamaguchi-gumi. Many members of the Kodo-kai, Yamaguchi-gumi’s ruling faction, are Korean-Japanese, with ties to North Korea. Masahiro Namikawa, leader of the drug trafficking Seido-kai yakuza organization, also has ties to the Chongryon.

The Chongryon operate at least two websites, chongryon.com, which is in Japanese, and korea-np.co.jp.

WHOIS records for chongryon.com indicate that it was registered by “guanin o” using the email address park2@mac.com. The WHOIS information for korea-np.co.jp shows that it was registered by Choson Shinbo Company Inc. The WHOIS records for these sites can be found in Appendix A.

Additionally, the Chongryon operate a ferry called the Mangyongbong-92, the only direct transit from Japan to North Korea. In 2003, they were suspected of using the ferry to smuggle missile parts. In 2006, the ferry was temporarily banned from Japanese waters when Japanese officials discovered the Chongryon were using it to smuggle dual-use electronics to North Korea to be used for military purposes.

North Korea has a global network of state-run businesses located in 30 to 40 countries that is used for espionage activities. The Reconnaissance General Bureau is responsible for oversight of this network. The businesses include cafes and other non-suspect establishments. The highest concentration of these is in China. Members of this espionage network reportedly “send more than $100 million in cash per year to the regime and provide cover for spies.” These establishments are also used for money laundering and drug trafficking.

The regime is also known to kidnap foreign citizens and use them as instruments for intelligence. Prisoners are first tortured and psychologically conditioned to bend to the regime’s will. They are then used based on their skillset. This may include teaching their language to North Koreans, spreading propaganda in their native language, providing translation services,

177 http://japandailypress.com/religious-group-that-bought-north-korean-embassy-building-has-mob-ties-0826568/
178 http://culuremag.de/crimemag/jake-adelstein-the-yakuza-2/20212
180 http://news.bbc.co.uk/2/hi/asia-pacific/2958968.stm
181 http://worldnews.nhk.or.jp/entertainment/200610162958968/index.html
conducting military training, or other skills the regime deems useful. In July 2014, Japanese officials agreed to lift some sanctions on North Korea when the regime agreed to investigate the whereabouts of Japanese citizens who were allegedly abducted by North Korean agents decades ago. Sanctions to be lifted include the ban on port calls to Japan by North Korean ships.

North Korea has also infiltrated important positions in South Korea for both intelligence and psychological operations purposes. In 2011, South Korea’s National Intelligence Service reportedly discovered the presence of Communist spies. These spies within their trusted circles had been reporting back to North Korea for almost 10 years. The embedded spies included a Democratic Party representative. According to the agency, the spies were on a mission to infiltrate and influence the Democratic Party and to gather military intelligence. The regime also attempts to infiltrate organizations made up of North Koreans who seek shelter in South Korea, in order to gain intelligence. In the past several years, South Korea has arrested at least 14 defectors who were found to be spies.

These intelligence collection and counterintelligence capabilities are an attempt to provide the regime with a strategic asymmetrical advantage. The regime leverages its human and cyber resources around the globe to provide an influx of intelligence, while very little credible intelligence about the regime’s activities and capabilities ever becomes available to the outside world.

Psychological operations

North Korea continues to be a master of propaganda and deception and leverages the cyber realm for psychological operations. Modern North Korean psychological operations tactics include distribution of propaganda via traditional media outlets, websites, and social media. Many of these psychological operations campaigns are politically focused. According to Dr. Andrei Lankov, the North Korean government has “very rational and highly successful manipulators who usually get what they want by outsmarting everybody else in the process.”

The regime’s Unit 204 is responsible for cyber-psychological operations. These operations are PSYOP tailored for the cyber arena. In order to be successful, cyber-psychological campaigns require speed, precision, and creativity. These campaigns leverage the phenomenon of viral, unverified news stories that tend to rapidly propagate via social media, mobile text messaging, and other electronic communications. This phenomenon creates an arena for strategic propagation of both fact and fiction for the purposes of sentiment manipulation. Such messages may be used for recruitment, cyber mobilization, and to instill fear in a target population.

Such messages can be used for recruitment, cyber mobilization, and to instill fear in a target population.
recruitment, cyber mobilization, and to instill fear in a target population. Cyber-psychological operations may also include mental suggestion using technology as a delivery mechanism for subliminal cues. It is unknown whether North Korea possesses this capability.\textsuperscript{192}

North Korean citizens have access to state-approved social networks on the Kwangmyong.\textsuperscript{193}

Figure 16 A photo posted by Jean Lee on Instagram shows one of the social networking sites on the Kwangmyong.\textsuperscript{194}

The regime has a limited overt social media presence on the Internet. Some of the known social media platforms employed by the regime include Twitter, Facebook, and YouTube. The YouTube channel North Korea Today, operated by user rodrigorojo1, features news clips from North Korea. It is unclear whether this channel is officially sanctioned.\textsuperscript{195} The North Korea Today YouTube channel also has corresponding profiles on Twitter\textsuperscript{196} and Facebook.\textsuperscript{197}

\textsuperscript{192} \url{http://fmso.leavenworth.army.mil/documents/new-psysop.pdf}
\textsuperscript{193} \url{http://www.austinchronicle.com/daily/sxsw/2013-03-11/social-media-in-north-korea/}
\textsuperscript{194} \url{http://instagram.com/p/WpcJs1OCkb/}
\textsuperscript{195} \url{https://www.youtube.com/user/rodrigorojo1}
\textsuperscript{196} \url{https://twitter.com/NorthKoreaT0day}
\textsuperscript{197} \url{https://www.facebook.com/pages/Korean-Central-Television/380193555435568?ref=ts}
The Uriminzokkiri website, known for pushing juche ideology and anti-American and anti-South Korean messages, has accompanying social media profiles on YouTube, Google+, and Facebook. It also has Twitter profiles in both Korean and English.

---

198 https://www.youtube.com/user/rodrigorojo1
199 https://www.youtube.com/user/uriminzokkiri
200 https://plus.google.com/u/0/112306344682887627095
201 https://www.facebook.com/pages/Uriminzokkiri/124452740935216
202 https://twitter.com/uriminzok
203 https://twitter.com/uriminzok_engl
Figure 18 A screenshot of the Uriminzokkiri YouTube channel.\textsuperscript{204}

Figure 19 A screenshot from the Uriminzokkiri Facebook page shows anti-U.S. and pro-\textit{juche} rhetoric.\textsuperscript{205}

\textsuperscript{204} https://www.youtube.com/user/uriminzokkiri/featured

\textsuperscript{205} https://www.facebook.com/pages/Uriminzokkiri/124452740935216
North Korean propaganda is used for several purposes: to enforce the ideals of allies and sympathizers, to frame North Korea in a favorable light to outsiders, to sensationalize the regime’s perceived self-reliance and military prowess, and to shield its own citizens from the outside world. Juche ideology and indoctrination of the regime’s youth ensure support of the local population. North Koreans accept military duty as an honor and strive to excel in their service to the regime. In the spirit of juche, the regime uses disinformation to “hide lapses or tout accomplishments that may have never been achieved.”

---

206 https://www.facebook.com/pages/Uriminzokkiri/124452740935216
207 https://twitter.com/uriminzok_english
achieved.” Limiting citizen access to the outside world by instituting the Kwangmyong intranet, North Korea ensures its citizens are not exposed to outside information that is counterproductive to citizen indoctrination or in conflict with juche ideals. North Korea portrays the West, particularly the United States, as an enemy. The regime uses this strategy of shifting the population’s negative sentiments toward an external entity to keep its citizens ignorant of North Korea’s own economic hardship, regime brutality, and systemic incompetence. For example, prior to Kim Jong Il’s death in 2011, North Korean media altered photos of their “Dear Leader” to make him appear younger and healthier than he really was. This became obvious when the altered photos were compared to those taken by Western media around the same time.

According to Dr. Andrei Lankov, “North Koreans now have a much better understanding of what is going on in the outside than they did before. This is largely thanks to the spread of DVDs and video content in the country, but also because some of them have been to China and talk about what they have seen...many [of] them sincerely believe that the United States remains ready to attack at any moment and that Japan is an incurably aggressive place...nearly all of them swallow the official propaganda myths about the Korean War being started by the ‘American Imperialists’ who invaded them. Hence, they see the outside world as an inherently dangerous place.” Some human rights groups seek to reach out to North Korean citizens and break them from this isolation. In August 2014, the New York-based charity Human Rights Foundation sponsored a hackathon in San Francisco called "Hack North Korea" to find new ways to get information in, out, and around North Korea. The event brought together many programmers, human rights campaigners, and defectors.

North Korea even uses “trolling” as a PSYOP tactic. On the Internet, “trolls” are users who post messages that are often crass, controversial, inflammatory, or offensive, in order to evoke a strong reaction or influence a reader’s opinion. Often, the motivation for trolling is simply for the troll’s enjoyment. The rude and offensive trolling tactics are in stark contrast to traditional forms of persuasive rhetoric. However, North Korea reportedly utilizes over 200 military intelligence operatives to troll South Korean message boards and social media pages with pro-North Korean sentiments. Matt Rhoades, director of the cyberspace and security program at the Truman National Security Project, said, "North Korea's cyber-development is almost just a new harassment mechanism for them, a low-cost, asymmetric method to harass its neighbor in the south..."

Leveraging the cyber and intelligence resources noted above, North Korea’s psychological operations serve an important strategic role. The ability to influence outsiders, while effectively isolating its own population from most outside influence, allows North Korea to remain an enigma. Additionally, in line with its PSYOP tactics, North Korea may strategically take credit for cyber attacks that were, in reality, launched by another entity. Whether the targeted entity blames

---

210 http://www.ists.dartmouth.edu/docs/cyberwarfare.pdf
211 http://docs.house.gov/meetings/AS/AS00/20140402/101985/HHRG-113-AS00-Wstate-ScaparrottiUSAC-20140402.pdf
212 https://www.strategypage.com/htmw/htmufr/articles/20131106.aspx
213 http://www.reddit.com/r/NorthKoreaNews/comments/296ryd/I_am_dr_andrei_lankov_i_studied_in_north_korea/
214 http://www.northkoreatech.org/2014/08/05/hack-north-korea-focuses-silicon-valley-on-information-flow/
North Korea for the attacks, or the regime simply takes credit for an attack that has not yet been attributed, several PSYOP goals can come into play. First, to claim credit for an attack amplifies the impact of a show of force, particularly if South Korea is the target. This tactic can be used to stir sentiments in order to provoke a reaction. Second, North Korea may lay claim to responsibility for an attack that exceeds its capabilities in order to seem more technologically advanced and more capable. Third, any success, or the appearance thereof, enforces the juche ideal of regime self-sufficiency. Finally, North Korea may act as a scapegoat and claim credit for a cyber attack of an ally such as China so the attack is not attributed to the real actors.\(^\text{217}\)

**Electronic warfare**

North Korea reportedly has the electronic warfare capabilities to jam GPS and to inject false GPS coordinates.\(^\text{218}\) North Korea demonstrated these capabilities in March 2011 by jamming South Korea's GPS signals during a joint U.S.-South Korea military exercise.\(^\text{219}\) North Korea has the capability to create an EMP.\(^\text{220}\) An EMP is a sudden, extreme outburst of atmospheric electricity creating an intense magnetic field that can burn out electrical equipment.\(^\text{221}\) A report from the U.S. Department of Homeland Security (DHS) noted North Korea’s ability to deliver a nuclear warhead as a satellite over the South Pole, effectively creating the burst needed to deliver an EMP targeting the United States. An EMP could effectively disrupt electronic communications including critical infrastructure components such as telecommunications, financial institutions, the energy sector, transportation, food and water delivery, emergency services, and space systems.\(^\text{222}\) North Korea reportedly acquired its EMP technology from Russia.\(^\text{223}\)

North Korea also has a drone program. The regime reportedly acquired its first drones in the late 1980’s or early 1990’s. The regime’s drones are complimentary to its intelligence program and are primarily used for surveillance.\(^\text{224}\) In early 2014 a North Korean drone crashed south of the 38th parallel, the line dividing North Korea from the south.\(^\text{225}\) While early reports noted that the drones appeared similar to those manufactured by Chinese company Tauyuan Navigation Friend Aviation Technology, the company denied involvement.\(^\text{226}\)

\(^{217}\) [http://fas.org/irp/doddir/army/fm3-05-301.pdf](http://fas.org/irp/doddir/army/fm3-05-301.pdf)

\(^{218}\) [https://www.usnwc.edu/getattachment/8e487165-a3ef-4ebc-83ce-0ddd7898e16a/The-Republic-of-Korea-s-Counter-asymmetric-Strategy.pdf.aspx](https://www.usnwc.edu/getattachment/8e487165-a3ef-4ebc-83ce-0ddd7898e16a/The-Republic-of-Korea-s-Counter-asymmetric-Strategy.pdf.aspx)

\(^{219}\) [http://www.reuters.com/article/2011/05/03/us-korea-northcyber-idUSTRE7421Q520110503](http://www.reuters.com/article/2011/05/03/us-korea-northcyber-idUSTRE7421Q520110503)


Stressing the importance of the regime’s electronic warfare capabilities, in 1999 former regime leader Kim Jong Il said “The basic key to victory in modern warfare is to do well in electronic warfare.” Since the regime’s advanced technology lags behind that of South Korea and the U.S., its capability to disrupt the communications of these perceived adversaries is a vital asymmetric capability.

**Training cyber warriors**

North Korea utilizes primary and secondary education and the university system to train its cyber warfare operators. According to reports by defectors, the regime seeks out children who show mathematical talent and sends them through rigorous advanced training. A vintage North Korean animation stresses the importance of mathematics in North Korean education. The short film follows a young boy as he does his geometry homework. The frustrated boy begins to daydream then has visions of going to war with the U.S. and needing geometry to effectively calculate missile trajectory during the battle.

---


Science and technology students are expected to learn foreign languages, which may include Chinese, Japanese, and English. Student emails, chats, and web browsing activities are heavily monitored. Around age twelve or thirteen, chosen students are enrolled in accelerated computer courses at First and Second Geumseong Senior-Middle Schools.
The successful students are then sent to Kim Il-sung University, Kim Chaek University of Technology, or the Command Automation University, traditionally known as Mirim University.

Kim Il-sung University’s computer center was started in 1985. Its computer courses have a heavy programming element. The university reportedly developed the Intelligent Locker hard disk protection program, Worluf Antivirus, SIMNA (simulation and system analysis program), a war games program, a hepatitis diagnosis and prescription system, and a C++ program development tool called FC 2.0. Kim Il-sung University also has programs focusing on nuclear research.

Kim Chaek University of Technology was established in 1948. In the late 1990s, it began to restructure its computer-focused courses to reflect more modern technologies. As of 2002, the university had three colleges focusing on computer science, information science and technology, and machine science. Software developed by the university includes Computer Fax and SGVision, an image-reprocessing program used for steganography. Students and instructors must submit a formal request for permission in order to use the Internet for research.

---

237 http://www.ists.dartmouth.edu/docs/cyberwarfare.pdf
238 http://www.nit.org/facilities/789/
239 http://www.ists.dartmouth.edu/docs/cyberwarfare.pdf
240 http://www.theguardian.com/world/2013/jan/08/north-korean-google-chief-search
The Command Automation University periodically chooses around 100 students for an intensive five-year course prior to their assignment to serve in cyber intelligence and cyber warfare capacities. Programs at the Command Automation University include command automation, computers, programming, automated reconnaissance, and electronic warfare. Other students attend a two-year accelerated university program, then study abroad in Russia or China before they are assigned to a cyber-operator role.

The elite cyber operators are given special incentives. For example, parents of students graduating from the cyber program with top scores are given the opportunity to live in Pyongyang; and married cyber operators are given housing, a food allowance, and a stipend if operating overseas. Due to the nature of their profession, these cyber elite are some of the only North Koreans allowed to access the outside Internet.

**Important political and military ties**

While this report focuses on North Korea’s cyber warfare capabilities, these capabilities cannot be fully separated from the implications of partnerships with countries known to deal in illegal weapons trade with the regime. Now that cyberspace has become a legitimate arena for warfare, these nations are also potential allies in the cyber realm. For this reason, the regime’s key political and military relationships are explored below.

**China**

North Korea has a longstanding historical relationship with China. During the Korean War (1950-1953), China allied with North Korea’s Communist forces. China has also provided ongoing political and economic support to the regime’s leadership and is a primary trade partner. North Korea is economically dependent on China. North Korea gets an estimated 90 percent of its energy imports, 80 percent of its consumer goods, and 45 percent of its food supply from China. This relationship is prudent—it in the event of a military conflict, China can strategically use North Korea as a buffer zone between itself and South Korea, where many U.S. military personnel are stationed. Chinese aid to North Korea also deters the likelihood that the regime will collapse, resulting in internal destabilization that could catalyze a U.S.-China conflict.

North Korea relies heavily on China for technological resources. As noted above, North Korea relies on China’s Unicom for Internet access. Additionally, the regime sends some of its cyber warriors to train in China and stations a portion of its Unit 121 personnel in Shenyang. Some of North Korea’s official websites are hosted in China, and KCC has a branch office there.
North Korea also relies on China to provide much of its network hardware, including servers and routers.  

**Russia**

North Korea has a long history of ties to Russia. The former Soviet Union was the major sponsor of the North Korean state and a major trading partner. Following the dissolution of the Soviet Union, aid to North Korea was halted and trade diminished significantly. This chain of events contributed to North Korea’s eventual economic collapse, as it could not survive without aid.  

North Korea currently has a collaborative relationship with Russia in the cyber realm. The regime’s CSTIA relies on Russia as one of several sources for technical data. North Korea also sends some of its cyber warriors to train in Russia, and the regime reportedly acquired its EMP technology from there.  

Political ties between Russia and North Korea have become stronger in recent months. In 2014, potentially as a result of the U.S. response to the Russian-Ukrainian conflict, Russia began to strengthen ties with North Korea. Negotiations reportedly included promises of trade and development projects. Narushige Michishita, a North Korea and Asia security expert at Japan’s National Graduate Institute for Policy Studies, stated “By strengthening its relationship with North Korea, Russia is trying to enhance its bargaining position vis-à-vis the United States and Japan.”  

Russia also recently forgave most of the regime’s debts.  

**Iran**

North Korea and Iran have longstanding political and military ties. North Korea supplied Iran with conventional arms during the Iran-Iraq War. Iran and North Korea reportedly collaborate closely in ballistic missile development efforts. In the past, Iran provided the North Korean regime with necessary funds and oil in exchange for missile parts and technology. In 2009, a North Korean plane transporting 35 tons of weapons and allegedly bound for Iran was seized after making an unscheduled stop in Bangkok, Thailand. That same year, United Arab Emirates seized a ship bound for Iran that was transporting several containers of North Korean weapons, including rocket-propelled grenades and ammunition. Reportedly, the customer was a company affiliated with Iran’s Islamic Revolutionary Guard Corps.  

North Korea also has cyberwar ties with Iran. In 2012, North Korea and Iran signed a technology treaty to help combat “common enemies” in cyberspace. The treaty included provisions for cooperation in research, student exchanges, and joint laboratories. Joint projects reportedly

---

255 http://www.extremetech.com/extreme/170563-north-korea-emp
257 http://www.voanews.com/content/russia-forgives-north-korean-debt/1939188.html
258 http://thediplomat.com/2013/10/the-iran-secret-explaining-north-koreas-rocket-success/2/
259 http://humanities.tau.ac.il/iranian/en/previous-reviews/10-iran-pulse-en/117-10
260 http://www.armscontrol.org/factsheets/dprkchron
261 http://www.irantraiker.org/foreign-relations/north-korea-iran-foreign-relations
include IT information sharing, engineering, biotechnology, renewable energy, and sustainability. F-Secure’s Mikko Hypponen stated, “It’s highly likely that one of the reasons for this co-operation is for them to work together regarding their cyber defence and cyber offense strategies”. Hypponen cited Flame malware as a possible triggering event for the creation of this treaty. Others also suspect that Iran and North Korea’s mutual interest in development of nuclear weapons and the need to protect refineries against malware such as Stuxnet were driving factors in the establishment of the treaty.262 U.S. House Foreign Affairs Committee leaders assert that the treaty indicates North Korea and Iran are collaborating on a joint nuclear weapons program.263

Additionally, North Korea, in conjunction with Iran and Syria, reportedly supports both Hamas and Hezbollah in procuring kinetic weaponry and communications equipment and in establishing operational infrastructure.264 265 266

**Syria**

North Korea has both a cyber relationship and kinetic weapons ties with Syria. KCC reportedly has a branch in Syria.267

In 2007, Israel launched an airstrike, destroying a Syrian target that was allegedly a nuclear facility under construction with North Korea’s assistance. U.S. officials noted the facility was modeled on the North Korean nuclear reactor at Yongbyon.268

The North Korea-Syria relationship becomes more important in the context of both countries’ ties with Iran. As noted above, Iran, North Korea, and Syria jointly provide support to extremist groups Hamas and Hezbollah.269 270 271 Additionally, as we explored in HPSR Security Briefing Episode 11, Iran and Syria’s military alliances extend to joint SIGINT and cyber operations.272

**Cuba**

North Korea also has an interesting relationship with Cuba — one that includes supplying weapons and apparent attempts to illegally smuggle weapons. In 2013, a North Korean cargo ship on its return voyage was stopped near the Panama Canal. The ship was carrying surface-to-air missile parts, disguised as containers of sugar. In an attempt to save face, Cuba’s Ministry of Foreign Affairs stated that the cargo included “240 metric tons of obsolete defensive weapons -- two anti-aircraft missile complexes Volga and Pechora, nine missiles in parts and spares, two Mig-21 Bis and 15 motors for this type of airplane, all of it manufactured in the mid-20th century -- to be

---

263 http://www.vanews.com/content/ties-among-north-korea-syria-iran-a-major-security-threat/1639769.html
264 http://38north.org/2014/08/aberger080514/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+38North+%2838+North%3A+Informed+Analysis+of+North+Korea%29
265 http://www.jewishjournal.com/opinion/article/hamas_global_support_network_must_be_targeted
266 http://www.armscontrol.org/factsheets/dprkchron
268 http://www.armscontrol.org/factsheets/dprkchron
269 http://38north.org/2014/08/aberger080514/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+38North+%2838+North%3A+Informed+Analysis+of+North+Korea%29
270 http://www.jewishjournal.com/opinion/article/hamas_global_support_network_must_be_targeted
While no apparent cyber relationship exists between North Korea and Cuba at this time, their track record for weapons trade means the potential for future collaboration in the cyber realm cannot be discounted.

**Timeline of significant North Korean cyber activity**

**2004**
- North Korea gains access to 33 South Korean military wireless communication networks.

**2006**
- The U.S. State Department is attacked by entities in the East Asia-Pacific region. The attacks coincided with State Department negotiations with North Korea regarding the regime’s nuclear missile tests. (June)
- A South Korean military official states North Korea’s Unit 121 has breached South Korean and U.S. military entities. (July)

**2007**
- North Korea tests a logic bomb (October)

**2009**
- North Korea states that it is “fully ready for any form of high-tech war.” (June)
- DarkSeoul DDOS and disk wiping malware targeting South Korean and U.S. government, media outlet, and financial websites. These attacks also coincided with U.S. Independence Day. (July)
- Malware for “Operation Troy” was likely planted.

**2010**
- DarkSeoul Backdoor.Prioxer detected
- Korean Central News Agency website becomes North Korea’s first known direct connection to the Internet

---

2011
- “10 Days of Rain” Attack - DarkSeoul DDoS and disk wiping malware against South Korean media, financial, and critical infrastructure targets (March)\(^ {285} \) \(^ {286} \)
- North Korea disrupts South Korean GPS signals (March)\(^ {287} \)
- North Korea reportedly attempts DDoS attack against Incheon Airport \(^ {288} \)
- Nonghyup bank suffers DDoS attack (April)\(^ {289} \)

2012
- South Korean newspaper JoongAng Ilbo attacked (June)\(^ {290} \)
- DarkSeoul Downloader.Castov detected (October)\(^ {291} \)
- North Korea signs treaty with Iran, agreeing to combat “common enemies” in cyberspace\(^ {292} \)

2013
- “March 20” disk wiping attacks against South Korean media and financial institutions (March)\(^ {293} \)
- Whois Team claims responsibility for attacking LG +U website with wiper malware and defacement, impacting South Korean media and financial institutions (March)\(^ {294} \) \(^ {295} \)
- The New Romantic Cyber Army Team claims responsibility for the same attacks\(^ {296} \)
- North Korea experiences 36-hour Internet outage. The cause was never definitively determined\(^ {297} \)
- Anonymous launches #OpNorthKorea and targets North Korean websites (March)\(^ {298} \)
- Anonymous allegedly hacks Uriminzokkiri and takes over its Twitter and Flickr pages (April)\(^ {299} \)
- DarkSeoul attack on South Korean financial institutions (May)\(^ {300} \)
- DarkSeoul DDoS attacks against South Korean government’s DNS server (June)\(^ {301} \)
- Details on Kimsuky malware, which targeted South Korean think tanks, first released (September)\(^ {302} \)

2014
- North Korean drones found near South Korean border (March and April)\(^ {303} \)

---
\(^ {285} \) http://www.symantec.com/connect/blogs/four-years-darkseoul-cyberattacks-against-south-korea-continue-anniversary-korean-war
\(^ {286} \) https://docs.google.com/file/d/0B6CK-ZBGuMe4dGVHdFZnenJMRUk/preview?pli=1
\(^ {287} \) http://www.reuters.com/article/2011/05/03/us-korea-north-cyber-ds3RE74210520110503
\(^ {288} \) http://threatpost.com/report
\(^ {289} \) http://www.northkoreatech.org/2013/03/30/tango
\(^ {290} \) http://www.computerworld.com/s/article/9237652/North_Korea’s_39s_Internet_returns_after_36_hour_outage
\(^ {291} \) http://www.theregister.co.uk/Print/2013/03/22/sk_megahack/
\(^ {292} \) http://www.csmonitor.com/World/Security-Watch/2013/1019/In-cyberarms-race-North-Korea-emerging-as-a-power-not-a-pushover/page/2
\(^ {294} \) http://www.symantec.com/connect/blogs/four-years-darkseoul-cyberattacks-against-south-korea-continue-anniversary-korean-war
\(^ {295} \) http://www.v3.co.uk/v3
\(^ {296} \) http://www.theregister.co.uk/Print/2013/03/22/sk_megahack/
\(^ {297} \) http://www.zdnet.com/massive-attack-on-lg-uplus-sparks-n-korea-reprisal-fears-7000012881/
\(^ {299} \) http://threatpost.com/report
\(^ {300} \) http://www.symantec.com/connect/blogs/four-years-darkseoul-cyberattacks-against-south-korea-continue-anniversary-korean-war
\(^ {301} \) http://www.northkoreatech.org/2013/03/30/tango
\(^ {302} \) http://www.reuters.com/article/2011/05/03/us
\(^ {303} \) http://blogs.wsj.com/korearealtime/2014/04/02/seoul-points-to-north-korea-in-crashed-drones-investigation/
Patterns in the noise: cyber incidents attributed to North Korean actors

It is interesting to note that much of North Korea’s cyber activity follows a distinct pattern. Analysis of North Korean cyber activity gives insight into these patterns and also helps tie together North Korea’s strategic, tactical, and operational capabilities. Strategic capabilities refer to the assets used in support of a long-term, overarching goal. Tactical capabilities refer to the methods and maneuvers actually implemented in pursuit of the strategic goal. Operational capabilities refer to the potential use of these capabilities.304

In 2004, in response to the annual U.S. – South Korea joint military exercises, North Korea reportedly gained access to 33 South Korean military wireless communication networks.306 The next significant cyber attack attributed to North Korea was in June 2006. The U.S. State Department was attacked by entities in the East Asia-Pacific region. The attacks coincided with State Department negotiations with North Korea regarding the regime’s nuclear missile tests.307 In July 2006, North Korea’s Unit 121 reportedly breached South Korean and U.S. military entities.308 This attack was concurrent with the regime’s test-fire of at least one long-range missile and several medium-range missiles.309

2007 was politically tumultuous for North Korea. Following multi-national talks, the UN’s International Atomic Energy Agency (IAEA) ordered the shutdown of the regime’s nuclear facilities in Yongbyon in July.310 Its nuclear efforts temporarily thwarted, North Korea tested a logic bomb in October 2007.311

In April 2009, North Korea ejected IAEA and U.S. nuclear compliance officials. The regime indicated refusal to comply with any UN agreements regarding nuclear weaponry and announced it would reinstate its nuclear materials production. The next month, North Korea conducted an underground nuclear test and voiced its confidence that the regime was well on its way to producing viable nuclear technology. The UN called an emergency meeting condemning the nuclear weapons test, and South Korea joined the Proliferation Security Initiative (PSI). North Korea issued a statement via KCNA calling South Korea’s involvement in PSI an act of war.312 In June 2009, North Korea stated that it was “fully ready for any form of high-tech war.”313 The following month, DDoS and disk wiping malware, later known as DarkSeoul, targeted South Korean and U.S. government entities, media outlets, and financial websites. The attacks coincided with...
with U.S. Independence Day.\textsuperscript{314} Other malware used for Operation Troy was also planted. Operation Troy would continue for several years, largely undetected.\textsuperscript{316}

In early 2011, political and military tensions were high. In February, James Clapper, United States Director of National Intelligence, testified that North Korea likely had undeclared uranium enrichment facilities as part of its nuclear weapons program.\textsuperscript{317} In March 2011, South Korean media, financial, and critical infrastructure targets suffered a DDoS and disk-wiping malware attack later known as the “10 Days of Rain”. U.S. and South Korean military entities were also targeted by DDoS during this attack. The attack used the DarkSeoul malware.\textsuperscript{318} North Korea also disrupted South Korean GPS signals. Additionally, North Korean actors reportedly attempted a DDoS attack against South Korea’s Incheon Airport that same month.\textsuperscript{319} These incidents coincided with the annual U.S. – South Korea joint military exercises.\textsuperscript{320} The following month, North Korean actors reportedly launched a DDoS attack against South Korea’s Nonghyup bank.\textsuperscript{321}

In 2012, an attack on South Korean Newspaper JoongAng Ilbo was attributed to North Korean actors. This attack also coincided with the timing of the annual joint U.S. – South Korea military exercises.\textsuperscript{322} In September 2012, North Korea signed a cyber treaty with Iran, agreeing the two nations would collaborate to combat “common enemies” in cyberspace.\textsuperscript{323}

The week of March 11, 2013, the U.S. and South Korea began their annual joint military exercise near the Korean Peninsula. Like clockwork, attacks attributed to North Korea and now known as the March 20 attacks targeted three South Korean media outlets and Shinhan, Nonghyup, and Jeju banks. North Korea also exhibited other hostile activity at that time. North Korea cut communication with Seoul and announced it had scrapped the 1953 armistice between the two Koreas. North Korea’s foreign ministry also issued a statement that it perceived this exercise as a precursor to invasion and that the regime would respond with a “strong military counteraction” if the situation escalated.\textsuperscript{324} That same week, the North Korean military conducted a drone attack simulation.\textsuperscript{325}

On March 18, the Uriminzokkiri YouTube channel posted an anti-U.S. video entitled “Firestorms Will Rain on the Headquarters of War” that showed a depiction of the White House in crosshairs, followed by an explosion.\textsuperscript{326}

\textsuperscript{314} http://www.symantec.com/connect/blogs/four-years-darkseoul-cyberattacks-against-south-korea-continue-anniversary-korean-war
\textsuperscript{315} http://powerofcommunity.net/poc2009/sl.pdf
\textsuperscript{316} http://www.symantec.com/connect/blogs/four-years-darkseoul-cyberattacks-against-south-korea-continue-anniversary-korean-war
\textsuperscript{317} http://www.armscontrol.org/factsheets/dprkchron
\textsuperscript{318} http://www.threatpost.com/report/north-korea-accused-ddos-attack-south-korean-airport-060712/76664
\textsuperscript{319} http://www.reuters.com/article/2011/05/03/us-korea-north-cyber-idUSTRE74210520111003
\textsuperscript{320} http://koreajoongandaily.joins.com/news/article/article.aspx?id=2965629
\textsuperscript{321} http://www.theguardian.com/news/world/2013/mar/19/north-korea-hacks-south-korea-attacks
\textsuperscript{322} http://www.v3.co.uk/v3-news/2202493/iran-and-north-korea-sign-technology-treaty-to-combat-hostile-malware
\textsuperscript{323} http://www.reuters.com/article/2011/03/20/north-korea-threatens-us-over-bombers/
\textsuperscript{324} http://www.huffingtonpost.com/2013/03/20/north-koreas-drone_n_2914794.html
\textsuperscript{325} https://www.youtube.com/watch?v=Dyap eCI08A
In May 2013, DarkSeoul malware was used to attack several South Korean financial institutions; and in June, DarkSeoul DDoS attacks were launched against the South Korean government’s DNS server. The latter took place on June 25, the anniversary of the start of the Korean War.

As evidenced above, much of North Korea’s cyber activity coincides with the annual U.S. – South Korea joint military exercises. Attacks not following that pattern were typically in response to political events impacting the regime or correlated with significant dates, such as the anniversary of the start of the Korean War. The regime’s strategic assets and tactical capabilities in the cyber arena seem to have evolved only slightly since 2009. Most of the attacks attributed to North Korea employ limited tactics, and their operational capability demonstrates an increase in the frequency and volume of attacks but is otherwise unimpressive to date.

In June 2014, the regime demanded cancellation of the annual U.S. – South Korea joint military exercise, attempting to use participation in the upcoming Asian Games as a bargaining chip. The regime’s demands may have had other political motivations, as they preceded the July 2014 meeting between South Korean president Park and Chinese President Xi Jinping. The meeting

---

327 https://www.youtube.com/watch?v=DyapeCi09A
328 http://www.symantec.com/connect/blogs/four-years-darkseoul-cyberattacks-against-south-korea-continue-anniversary-korean-war
centered on trade and regional security issues, including the ever-present rhetoric around
denuclearization of North Korea.³³⁰ Both leaders were critical of Japan’s recent announcement to
soften sanctions on North Korea.³³¹ As this report headed to press, the annual U.S. – South Korea
joint military exercises were underway.³³²

**DarkSeoul**

The most prominent North Korean threat actor group is the group responsible for the DarkSeoul
malware. According to statements from the South Korean government, North Korea’s Lab 110
were the actors behind the DarkSeoul malware. South Korean intelligence reports
stated that Lab 110, which is affiliated with the regime’s defense ministry, was
ordered by the North Korean regime to destroy South Korean communications
networks.³³³ Although the March 20 attacks used DarkSeoul malware, it is interesting
to note that two groups, Whols Team and New Romantic Cyber Army Team, claimed
responsibility for the “March 20” 2013 attacks on South Korean media and financial
institutions.³³⁴

Some of the DarkSeoul attacks corresponded with significant dates, such as U.S. Independence
Day or the anniversary of the start of the Korean War. DarkSeoul attacks go beyond denial of
service and sabotage. As early as 2009, the group responsible for the Dark Seoul attacks
launched “Operation Troy”, an espionage campaign targeting the South Korean military. The
operation was codenamed “Troy” due to the frequent use of the word “Troy” in the malware’s
compile path strings.³³⁵ The malware used in these attacks sought out and exfiltrated data, based
on keyword searches. While the malware was clearly intended to search for and exfiltrate certain
types of data, its true impact on the targets was never revealed.³³⁶ The March 2011 “10 Days of
Rain” DDoS attacks on U.S. and South Korean sites have also been attributed to the actors
associated with DarkSeoul.³³⁷ According to Symantec, the politically motivated attacks have
required a level of intelligence, coordination, monetary support, and technical sophistication that
suggests state sponsorship.³³⁸ This designation means the group can be considered an advanced
persistent threat (APT).

A March 20, 2013 attack attributed to the DarkSeoul actors targeted three South Korean media
outlets and Shinhan, Nonghyup, and Jeju banks. The impact of the March 20 attacks included
disruption of service at financial institutions and data deletion. However, the targeted entities
resumed normal operations shortly thereafter.³³⁹ According to South Korean reports, the media
outlets targeted corresponded with those listed by the North Korean regime in 2012 as right-wing
press that manipulated South Korea’s public opinion. In April 2012, the regime reportedly listed

³³⁹ http://motherboard.vice.com/blog/the-dark-seoul-hackers-were-after-south-korean-military-secrets
³⁴¹ http://www.symantec.com/connect/blogs/four-years-darkseoul-cyberattacks-against-south-korea-continue-anniversary-korean-war
³⁴² http://www.nytimes.com/2013/03/21/world/asia/south-korea-computer-network-crashes.html?pagewanted=all&%r=1
those entities as attack targets. The malware used in the March 20, 2013 attacks were wiper malware. The malware attempted to disable AhnLab and Hauri AV antivirus products then proceeded to overwrite the master boot record (MBR). The attack was capable of wiping both Linux and Windows machines. McAfee found that these attacks were the culmination of the malware campaign they dubbed “Operation Troy”.

A report from IssueMakersLab tied the actors responsible for the March 20, 2013 attacks to cyber attack activity occurring as early as 2007. IssueMakersLab found that these actors consistently used the same 16-digit password for file compression, the same stage 1 C2 protocol, the same collection keywords and encryption keys, and the same development path. According to South Korea’s Korea Internet and Security Agency, the North Korean IP address 175.45.178.xx was found scanning South Korean routes the month before the attacks, and the same IP was reportedly logged as accessing one of the targets 13 times. Details of the March 20 attack also suggested possible ties to China. AlienVault suspected the Chinese exploit kit GonDad was used to spread the malware, and the Korean domains serving the malware were registered using a Chinese email address. Additionally, researchers at AhnLab in South Korea noted a Chinese IP address linked to the attacks.

While no concrete evidence has been released that indicates Lab 110 was responsible for the DarkSeoul attacks, the responsible group’s targets, TTP, and attack timing demonstrate a strong pro-North Korean sentiment.

Known tactics, techniques and procedures

- Customized wiper malware
- DDoS
- Multi-staged, coordinated attacks
- Destructive payloads with politically significant trigger dates
- Use of politically themed strings when overwriting disk sectors
- Utilizing legitimate patching mechanisms to spread malware across corporate networks
- Encryption and obfuscation methods that have become their signature
- Repeated use of a specific webmail server
- Consistent C2 structures
- Antivirus disablement and evasion
- Watering hole attacks
- Zero-days
- Spearphishing
Targets

- South Korean military
- U.S. sites
- Shinhan Bank
- Nonghyup Bank
- Jeju Bank
- Munhwa Broadcasting Corp.
- YTN
- Korea Broadcasting System
- South Korean government DNS server
- South Korea financial institutions

WhoIs Team

WhoIs Team is one of two groups that claimed responsibility for the “March 20” attacks targeting South Korea. A defacement on the LG +U webpage stated that it was “Hacked by WhoIs Team” and that the attackers would return. The page featured three skulls. However, no other attacks by WhoIs Team have been observed.

---

Note: The numbers 351, 352, 353, and 354 are not part of the natural text and should be removed.
Figure 26 A defacement by “WhoIs Team”  

Known tactics, techniques, and procedures

- Wiper malware
- Defacements

Targets

- Took credit for an attack on the LG +U website.

---

355 http://nakedsecurity.sophos.com/2013/03/20/south-korea-cyber-attack/
Associated actors

- dbM4st3r
- d3sign3r
- APTM4st3r
- s3ll3r
- vacc1nm45t3r
- r3cycl3r

Based on North Korea’s affinity for disinformation and counterintelligence, we must note the distinct possibility that operatives claiming to be Whols Team are part of another group and that the defacement was a false flag operation meant to pin blame on RAON_ASRT. RAON_ASRT is a South Korean white hat capture the flag (CTF) team, whose members also operate under the name “Whols.”

Figure 27 A screenshot showing that South Korea’s RAON_ASRT white hat CTF team also uses the moniker Whols.

RAON_ASRT (the RaonSecure Advanced Security Research Team) and its sub-teams Whols Team and Cpark Team have participated in and performed well in CTF contests such as the one hosted by DefCon. In 2013, a member of RAON_ASRT was invited to Blue House, the residence of the South Korean president, to meet with president Park and discuss the security industry. RAON_ASRT runs the Secuinside CTF competition. Their parent organization RaonSecure operates a whitehat training program. The group also runs the Korea WhiteHat Contest, which is hosted by South Korea’s Ministry of National Defense and National Intelligence Service and

\[357\] https://ctftime.org/team/3206
\[358\] https://ctftime.org/team/3206
\[359\] http://ls-al.org/asrt-has-become-the-winner-of-codegate-2013/
\[360\] http://blog.raonsecure.com/62
\[361\] http://ls-al.org/asrt-researcher-meets-the-president-park-in-korea/
\[362\] http://ls-al.org/asrt-runs-secuinside-ctf/
\[363\] http://www.whitehat.co.kr/
supervised by South Korean Cyber Command. For these reasons, it seems unlikely that the RAON_ASRT Whols Team would maliciously target South Korean entities.

IsOne

IsOne is the group that claimed responsibility for the June 2012 attack on the website of South Korean newspaper JoongAng Ilbo. The attack included an attempt to wipe JoongAng Ilbo’s servers as well as a defacement depicting a laughing cat. Despite efforts to wipe the target’s servers, the target only suffered defacement and temporary downtime.

IsOne is the group that claimed responsibility for the June 2012 attack on the website of South Korean newspaper JoongAng Ilbo. The attack included an attempt to wipe JoongAng Ilbo’s servers as well as a defacement depicting a laughing cat. Despite efforts to wipe the target’s servers, the target only suffered defacement and temporary downtime.

Although the groups have a similar name and both use a cat theme, it is unclear whether a CTF team known as “The Cat is Number 1” and IsOne are the same actors. “The Cat is Number 1” members claim to hail from North Korea, but there is no hard evidence linking team members to

---

364 http://ls-al.org/%EB%8C%80%ED%95%9C%EB%A1%8C%EA%B5%AD-%ED%99%94%ED%9D%84%ED%8A%B8%ED%98%9C%EB%BD%98%ED%85%8C%EC%BD%A4%ED%8A%B8korea-whitehat-contest-%EA%B0%9C%EC%B5%9C/


366 http://bad-bytes.blogspot.co.uk/2012/06/joongang-ilbo-cyber-attack.html
the region.\textsuperscript{367} Again, it seems that the actors responsible for the attack borrowed the moniker of another group.

![Figure 29 A screenshot of “The Cat is Number One” profile on CTF Time \textsuperscript{368}](https://ctftime.org/team/2538)

According to South Korea’s National Police Agency, the attack on JoongAng Ilbo shares characteristics with previous attacks attributed to North Korean actors. An investigation conducted by the agency’s Cyber Terror Response Center found that the actors targeting JoongAng Ilbo used two North Korean servers and 17 servers in 10 other countries. One server maintained a constant connection to an IP address belonging to Joson Telecommunication Company, which is affiliated with North Korea’s Ministry of Posts and Telecommunications. Investigators found that one of the servers used in the attack on JoongAng Ilbo was also used in the March 2011 DDoS attacks on South Korean critical infrastructure sites and the April 2011 attack on Nyongyup Bank.\textsuperscript{369}

Known tactics, techniques and procedures

- Wiper malware
- Defacements

Targets

- Took credit for defacing JoongAng Ilbo.

\textsuperscript{367} https://ctftime.org/team/2538
\textsuperscript{368} https://ctftime.org/team/2538
Kimsukyang

The Kimsuky malware, which targeted South Korean think tanks, is loosely attributed to an actor referred to as Kimsukyang. Little is known about the actor or group responsible for the malware. However, the following email addresses are associated with the Kimsuky operation:

- beautifl@mail.bg
- ennemyman@mail.bg
- fashionman@mail.bg
- happylove@mail.bg
- lovest000@mail.bg
- monneyman@mail.bg
- sportsman@mail.bg
- veryhappy@mail.bg
- iop110112@hotmail.com
- rsh1213@hotmail.com

The email address iop110112@hotmail.com was registered using the alias “kimsukyang”, and rsh1213@hotmail.com was registered using the alias “Kim asdfa”.

Kaspersky found that the Kimsuky operation used 10 IP addresses in two Chinese provinces that border North Korea: Jilin and Liaoning.

Known tactics, techniques and procedures

- Malware with keylogger and data exfiltration capabilities
- Malware disables AhnLab security software

Targets

- Sejong Institute
- Korea Institute for Defense Analyses (KIDA)
- Ministry of Unification
- Hyundai Merchant Marine
- The Supporters of Korean Unification

New Romantic Cyber Army Team / Hastati

The New Romantic Cyber Army Team also took credit for the March 20, 2013 attacks. McAfee suspected New Romantic Cyber Army Team were responsible for Operation Troy and the resulting March 20, 2013 attacks due to the group’s “frequent use of Roman and classical terms in their campaigns.”
code."\textsuperscript{374} It is unknown whether Hastati is an alternate name for the group or whether Hastati is an individual actor within the group.

It is interesting to note that the malware associated with these actors uses the strings "HASTATI" and "PRINCIPES" to overwrite the MBR. The name Hastati likely refers to a class of infantrymen of the early Roman Republic. The Hastati were less experienced soldiers who fought on the frontlines with spears and swords. Principes likely refers to more experienced Roman soldiers who fought on the second line of battle. \textsuperscript{375}

![Figure 30 Defacement by Hastati.\textsuperscript{376}](image)

Known tactics, techniques and procedures

- Wiper malware

Targets

- KBS TV\textsuperscript{377}
- Entities targeted in Operation Troy\textsuperscript{378}

**Malware summary**

HP researchers had previously analyzed samples of the DarkSeoul dropper, and findings were published in our annual \textit{HP Cyber Risk Report 2013}. Analysis of this malware is included in \textbf{Appendix C}. Analysis of additional malware used in these campaigns produced no new findings and only corroborated what was found by external security researchers. These publicly available analyses have been cited throughout the report. Some of the malware samples were no longer publicly available. However, CrowdStrike obtained these missing samples before they disappeared from the wild and conducted thorough analysis, which was released in their subscription-only reports. While we cannot divulge detailed information from those reports, an overview of the findings is provided below.

\textsuperscript{374} http://www.darkreading.com/attacks-and-breaches/south-korean-bank-hackers-target-us-military-secrets/d/d-id/1110674?

\textsuperscript{375} http://www.roman-empire.net/army/army.html#early/legion

\textsuperscript{376} http://eromang.zataz.com/2013/04/02/dark-south-korea-total-war-review/

\textsuperscript{377} http://eromang.zataz.com/2013/04/02/dark-south-korea-total-war-review/

The majority of the malware used in cyber incidents attributed to North Korea were variations of three types of malware: dropper, wiper, and IRC remote access trojan (RAT). CrowdStrike’s attribution of this malware to North Korean actors stemmed from two primary factors: Korean language characters found in the binaries and the propensity to specifically target South Korean entities.\textsuperscript{379}

Dropper samples consistently targeted AhnLab Policy Center as a propagation method. This information is corroborated in a Black Hat Asia 2014 presentation by Fortinet researcher Kyle Yang.\textsuperscript{380} CrowdStrike’s report also briefly noted the use of an update server vector.\textsuperscript{381} Yang analyzed the malware’s update config metadata and matched its format to the AhnLab Policy Center. To test its payload, Yang set up a server/client and executed the update through the server. As Yang had predicted, it wiped the client.\textsuperscript{382} While the method for initial compromise of the update server is not noted in detail, CrowdStrike’s report cites “collateral information” that suggests targeted email attacks were used to gain initial entry, and policy servers were then compromised. The upload server vector included a time-based logic bomb that allowed the wiper to target a large number of systems, on a set time and date, with full permissions on all of the targeted systems.\textsuperscript{383}

According to CrowdStrike, the wiper malware was dropped on the systems as AgentBase.exe. The wiper used the Windows utility 'taskkill' to kill the processes pasvc.exe and clisvc.exe, which are the main processes for the Ahnlab and Hauri antivirus applications.\textsuperscript{384} The wiper then performed system reconnaissance, gathering drive information and operating system version. Depending on the OS used, the wiper recursively deleted files on the file system, deleting the Windows folder last. It then overwrote the MBR with the strings "HASTATI", "PRINCPE", "PRINCIPES", or "PR!NCPES".\textsuperscript{385}

While there are several variants of the wiper, all seem to have been used on the same date. It is unclear why multiple wiper variants with slightly differing behavior were used for the same campaign. One possible explanation is that multiple variants were used to minimize the operational damage to the mission in the case of an early detection of one of the variants. For example, if one wiper variant was compromised or detected by antivirus or IDS signatures, the other variants may have differed enough to remain undetected, still resulting in mission success.

According to CrowdStrike, a third malware component downloaded an IRC RAT from various compromised websites. This RAT is detected by Symantec as Backdoor.Prioxer. Prioxer has been linked to other 2011 attacks on South Korea. It is unclear whether these downloaders were

\textsuperscript{379} CrowdStrike Intelligence Report CSIR-13013  
\textsuperscript{380} Yang, Kyle. Z'Make Troy', Not War: Case Study of the Wiper APT in Korea, and Beyond. Black Hat Asia, March 2014.  
\textsuperscript{381} CrowdStrike Intelligence Report CSIR-13013  
\textsuperscript{382} Yang, Kyle. Z'Make Troy', Not War: Case Study of the Wiper APT in Korea, and Beyond. Black Hat Asia, March 2014.  
\textsuperscript{383} CrowdStrike Intelligence Report CSIR-13013  
\textsuperscript{384} CrowdStrike Intelligence Report CSIR-13030  
\textsuperscript{385} Yang, Kyle. Z'Make Troy', Not War: Case Study of the Wiper APT in Korea, and Beyond. Black Hat Asia, March 2014.  
\textsuperscript{386} CrowdStrike Intelligence Report CSIR-13030
pushed out in the same update server vector as the wipers. However, the two malware types both use the same packer 'Jokra' and both contain the strings "HASTATI" and "PRINCPES". 387

Analysis

Based on the information above, we have identified strategic challenges that impact the development of North Korea’s cyber warfare capabilities. We have also noted relevant implications:

- The North Korean regime strictly controls all Internet infrastructure, 388 meaning cyber activity by dissidents or autonomous hacker groups are very unlikely. In other words, any cyber attacks originating in North Korea can be assumed to be state sponsored. For this reason, according to defectors, the regime’s cyber operators do not typically launch attacks directly from within North Korea. Instead, many regime-sponsored attacks are launched from cells based in China, U.S., South Asia, Europe, and even South Korea. 389
- North Korea has a limited number of outgoing connections. 390 For this reason, there is a low probability of DDoS originating from within. However, this does not preclude the use of botnets with a local C2 server or the use of networks in third-party nations to launch attacks. As seen in the July 2009 attacks on South Korean and U.S. targets, North Korea has leveraged networks in countries such as Austria, Georgia, Germany, and even South Korea and the U.S., in order to launch cyber attacks. 391 North Korea will likely be forced to rely on third parties for quite some time, due to its lack of sufficient infrastructure for launching large-scale CNO.
- Several outward facing websites are hosted in China and other countries. This implies two possibilities: that North Korea’s infrastructure cannot handle a heavy incoming traffic load 392 or that the regime wants to separate the propaganda crafted for an outside target audience from internally-focused propaganda. This arrangement seems unlikely to change in the foreseeable future.
- North Korea is known to have unstable power supplies 393, which limits scalability of the regime’s current CNO capabilities. This is another reason why expansion of CNO capabilities using the nation’s own infrastructure seems unlikely in the foreseeable future.
- North Korea is known to have monetary deficiencies, 394 which further limit expansion of infrastructure and CNO capabilities, at least without third-party aid. North Korea continues to rely heavily on China for sustainment. 395
- Although we see few instances of overt cyber operations, that North Korea reportedly spends so much of its limited resources on training and equipping cyber operators speaks volumes. The human element of the regime’s cyber war program, at least, has potential.

387 CrowdStrike Intelligence Report CSIR-13013
392 http://binarycore.org/2012/05/30/investigating-north-koreas-netblock-part-3-topology/
Sanctions against North Korea and export laws prohibit the sale of certain technologies to the regime. In other words, in order to obtain the technology needed for a cyber warfare program, the regime must improvise. North Korea must develop its own technology, manufacture technology using plans obtained via industrial espionage, or rely on third parties to procure it for them. However, the regime has historically failed in its attempts of large-scale production of electronic components. At present, North Korea relies on China to provide much of its network hardware, including servers and routers. It is unlikely that North Korea will compromise on its nuclear program, meaning sanctions will likely be longstanding, and the regime will have to continue to rely on third parties to procure technology.

Cyber incidents attributed to North Korean actors seem to follow distinct patterns:

- According to reports by other researchers, the conventions and C2 structure used by North Korean cyber actors show continuity and consistency over time.
- The majority of the incidents attributed to North Korean actors consistently used wiper malware.
- Several of the incidents included defacements, with a different group taking credit each time. Additionally, little information or attack history was found about any of the groups, aside from information acknowledged in this report. These factors seem to indicate that a single group may have been responsible for several attacks over time, using different group names as a false flag.
- On more than one occasion, the malware included provisions to disable security software made by South Korean security company AhnLab. This detail strengthens the case that the malware was written or modified to specifically target South Korean machines.
- The attacks followed an explicit pattern: most were around the time of U.S. – South Korean joint military exercises, while the others fell on a significant date or were in response to political events.
- The primary targets were South Korean and U.S. entities. While these nations are traditionally targeted by the regime, it is also possible that South Korean entities are quick to attribute any attack on their infrastructure to North Korean actors. In fact, in some cases, South Korean reports were the only source of attribution.

Summary

Does North Korea have sufficient cyber infrastructure and cyber warfare capabilities to harm the U.S. and its allies? While North Korea’s cyber warfare capabilities pale in comparison to those of wealthier nations, the regime has made significant progress in developing its infrastructure and in establishing cyber operations. The rate of this progress warrants a closer look at North Korea’s motivations, TTPs, and capabilities. As noted above, North Korea views the U.S. and South Korea as its primary adversaries. The U.S. and South Korea are high-tech nations with economies that
depend heavily on technology.\textsuperscript{398} In contrast, North Korea does not have a high tech culture. For these reasons, we should not overestimate the regime’s advanced cyber capability, yet we should never underestimate the potential impact of North Korea utilizing less advanced, quick-and-dirty tactics like DDoS to cripple their high-tech targets. Both government and corporate entities are susceptible to being targeted by North Korean cyber attacks. North Korean juche ideology places the survival of the regime as its primary goal, and any perceived threat to the regime may be targeted. Several attacks on U.S. and South Korean government, financial, and critical infrastructure entities have been attributed to North Korean origins. These attacks were often preceded by or occurred in conjunction with North Korea voicing negative sentiments about the targeted entities. As we saw with Iranian cyber actors in HP Security Research Briefing Episode 11,\textsuperscript{399} state sponsored cyber actors often launch an attack in response to a political trigger. The same pattern seems to apply to pro-North Korean cyber actors, who have launched attacks to coincide with U.S. Independence Day and the anniversary of the start of the Korean War, as well as propaganda and cyber attacks in response to joint military exercises between the U.S. and South Korea.\textsuperscript{400, 401}

As shown by North Korea’s past behavior (which is consistent with their doctrine), they are easily “pushed into a corner”. At the slightest perceived threat, the regime responds with saber-rattling and peacocking. The regime is extremely defensive and will, in turn, flex its muscles to show the world how capable it is, even if this is an inaccurate display of their overall capabilities.

The regime fears losing its control and the nation’s culture to the ever-growing threat of outside influence, as is evidenced in the regime’s reaction to the comedy film “The Interview”. The regime has represented itself to its citizens as a powerful and capable entity and has used this status to control the populace. For this reason, the regime’s leaders are forced to continually demonstrate this strength and power, or an illusion thereof, both domestically and globally, in order to maintain the status needed to ensure continued suppression of the population. This show of power may require that the regime takes chances and stretches beyond its abilities at times, but in the spirit of juche and songun, the regime will continue this façade, fearful of losing the image its leaders have worked so hard to maintain.

**HP Security Research recommendations**

North Korean cyber operations are not generally observed originating from home field IP address space, so geo-IP based blocking of traffic originating from those net-blocks is ineffective.

\textsuperscript{398} http://www.apcss.org/Publications/Edited%20Volumes/BytesAndBullets/CH2.pdf
\textsuperscript{400} http://www.zdnet.com/south-korea-braces-for-norths-cyberattacks-7000012587/
\textsuperscript{401} http://www.symantec.com/connect/blogs/four-years-darkseoul-cyberattacks-against-south-korea-continue-anniversary-korean-war
Given that North Korea has capable and technically trained forces and will demonstrate their power when they feel provoked, western entities should consciously avoid promoting ideas or doctrine that is blatantly slanderous to the regime. Encouraging such ideas could cause those entities to become a focal point for North Korean cyber attacks.

Due to the fact that North Korean infrastructure is aging and its resources are not able to keep up with the rest of the world, entities with interesting R&D or IP (intellectual property) - especially military in nature – could become targets of interest for North Korea. Interest in defense-related IP and R&D could also stem from North Korea’s relationship with China. In the Chinese business culture, taking another entity’s IP or R&D is not stealing – it is accepted as business as usual. It is possible that North Korea, if under Chinese influence, would adopt the same attitude, given the regime’s limited capacity for homegrown innovation.

Known DPRK targets have been limited primarily to South Korean and U.S. organizations and government entities. For these targets, prudent measures should include:

- Following traditional defense in depth approaches and security best practices
- Monitoring for malware that disables Korean language antivirus software, such as that from AhnLab
- To protect against the attack vectors used in North Korean malware campaigns, an advisable prevention tactic is to focus on hardening update/patch management systems. These systems are appealing targets due to the potential for a large impact
Appendix A – WHOIS records

WHOIS record for silibank.net:
Domain Name: silibank.net
Registry Domain ID:
Registrar WHOIS Server: whois.discount-domain.com
Registrar URL: http://www.onamae.com
Updated Date: 2014-03-11 17:27:55.0
Creation Date: 2006-03-13 13:14:53.0
Registrar Registration Expiration Date: 2015-03-13 03:14:53.0
Registrar: GMO INTERNET, INC.
Registrar IANA ID: 49
Registrar Abuse Contact Email: abuse@gmo.jp
Registrar Abuse Contact Phone:
Domain Status: ACTIVE
Registry Registrant ID:
Registrant Name: Whois Privacy Protection Service by MuuMuuDomain
Registrant Organization: Whois Privacy Protection Service by MuuMuuDomain
Registrant Street1: 2-7-21 Tenjin Chuo-ku
Registrant Street2: Tenjin Prime 8F
Registrant City: Fukuoka-shi
Registrant State/Province: Fukuoka
Registrant Postal Code: 810-0001
Registrant Country: JP
Registrant Phone: 81-927137999
Registrant Phone Ext:
Registrant Fax: 81-927137944
Registrant Fax Ext:
Registrant Email: privacy@whoisprivacyprotection.info
Registry Admin ID:
Admin Name: Whois Privacy Protection Service by MuuMuuDomain
Admin Organization: Whois Privacy Protection Service by MuuMuuDomain
Admin Street1: 2-7-21 Tenjin Chuo-ku
Admin Street2: Tenjin Prime 8F
Admin City: Fukuoka-shi
Admin State/Province: Fukuoka
Admin Postal Code: 810-0001
Admin Country: JP
Admin Phone: 81-927137999
Admin Phone Ext:
Admin Fax: 81-927137944
Admin Fax Ext:
Admin Email: privacy@whoisprivacyprotection.info
Registry Tech ID:
WHOIS Record for kcna.kp:
inetnum: 175.45.176.0 - 175.45.179.255
netname: STAR-KP
descr: Ryugyong-dong
descr: Potong-gang District
country: KP
admin-c: SJVC1-AP
tech-c: SJVC1-AP
status: ALLOCATED PORTABLE
mnt-by: APNIC-HM
mnt-lower: MAINT-STAR-KP
mnt-routes: MAINT-STAR-KP
remarks: ++++++-----------------------------+++++-----------------------------+++++
remarks: This object can only be updated by APNIC hostmasters.
remarks: To update this object, please contact APNIC
remarks: hostmasters and include your organisation's account
remarks: name in the subject line.
remarks: ++++++-----------------------------+++++-----------------------------+++++
mnt-irt: IRT-STAR-KP
changed: hm-changed@apnic.net 20091221
source: APNIC
irt: IRT-STAR-KP
address: Ryugyong-dong Potong-gang District
e-mail: sahayod@loxley.co.th
abuse-mailbox: sahayod@loxley.co.th
admin-c: SJVC1-AP
tech-c: SJVC1-AP
auth: # Filtered
WHOIS Record for rodong.rep.kp:
inetnum: 175.45.176.0 - 175.45.179.255
netname: STAR-KP
descr: Ryugyong-dong
descr: Potong-gang District
country: KP
admin-c: SJVC1-AP
tech-c: SJVC1-AP
nic-hdl: SJVC1-AP
mnt-by: MAINT-STAR-KP
changed: hm-changed@apnic.net 20091221
source: APNIC

mnt-by: MAINT-STAR-KP
changed: sahayod@loxley.co.th 20120202
source: APNIC
role: STAR JOINT VENTURE CO LTD - network administrat
address: Ryugyong-dong Potong-gang District
country: KP
phone: +66 81 208 7602
fax-no: +66 2 240 3180
e-mail: sahayod@loxley.co.th
admin-c: SJVC1-AP
tech-c: SJVC1-AP
nic-hdl: SJVC1-AP
mnt-by: MAINT-STAR-KP
changed: hm-changed@apnic.net 20091221
source: APNIC

This object can only be updated by APNIC hostmasters.
To update this object, please contact APNIC hostmasters and include your organisation's account name in the subject line.

mnt-irt: IRT-STAR-KP
WHOIS Record for uriminzokkiri.com:
Domain Name : uriminzokkiri.com
PunnyCode : uriminzokkiri.com
Creation Date : 2003-02-09 00:00:00
Updated Date : 2012-06-28 13:22:18
Expiration Date : 2015-02-09 00:00:00
Registrant:
Organization : chaoxianLiuYiYuBianJishe ShenYang Ban SHICHU
Name : Korea 615 Shenyang company
Address : shenyang hepingqu xifudalu 168 hao 2 danyuan 2-12-1
City : shenyangshi
Province/State : liaoningsheng
Country : china
Postal Code : 123456
Administrative Contact:
Name : kim sejun
Organization : Shenyang xin neng yuang
Address : shenyang hepingqu xifudalu 168 hao 2 danyuan 2-12-1
City : shenyangshi
Province/State : liaoningsheng
Country : china
Postal Code : 123456
Phone Number :
Fax : 86-024-22523102
Email : hyk1979@hotmail.com
Technical Contact: Name : kim sejun
Organization : Shenyang xin neng yuang
Address : shenyang hepingqu xifudalu 168 hao 2 danyuan 2-12-1
City: shenyangshi
Province/State: liaoningsheng
Country: china
Postal Code: 123456
Phone Number:
Fax: 86-024-22523102
Email: hyk1979@hotmail.com
Billing Contact:
Name: kim sejun
Organization: Shenyang xin neng yuang
Address: shenyang hepingqu xifudalu 168 hao 2 danyuan 2-12-1
City: shenyangshi
Province/State: liaoningsheng
Country: china
Postal Code: 123456
Phone Number:
Fax: 86-024-22523102
Email: hyk1979@hotmail.com

WHOIS Record for ournation-school.com:
Domain Name: ournation-school.com
Registry Domain ID:
Registrar WHOIS Server: whois.paycenter.com.cn
Registrar URL: http://www.xinnet.com
Updated Date: 2012-06-28 13:22:20
Creation Date: 2004-10-29 00:00:00
Registrar Registration Expiration Date: 2014-10-29 00:00:00
Registrar: XINNET TECHNOLOGY CORPORATION
Registrar IANA ID: 120
Registrar Abuse Contact Email: supervision@xinnet.com
Registrar Abuse Contact Phone: +86.1087128064
Domain Status:
Registry Registrant ID:
Registrant Name: Korea 615 Shenyang company
Registrant Organization: chaoxian liuyiyubianjishe shenyangbanshichu
Registrant Street: shenyang hepingqu xifudalu 168 hao 2 danyuan 2-12-1
Registrant City: shenyangshi
Registrant State/Province: liaoningsheng
Registrant Postal Code: 123456
Registrant Country: China
Registrant Phone: +86.024 22523102
Registrant Phone Ext:
Registrant Fax: +86.024 22523102
Registrant Fax Ext:
Registrant Email: urimanager@silibank.com
Registry Admin ID:
Admin Name: Korea 615 Shenyang company
Admin Organization: Korea 615 Shenyang company
Admin Street: shenyang hepingqu xifudalu 615 hao 2 danyuan 6-1-5
Admin City: shenyangshi
Admin State/Province: liaoningsheng
Admin PostalCode: 123456
Admin Country: China
Admin Phone: +86.024 22523102
Admin Phone Ext:
Admin Fax: +86.024 22523102
Admin Fax Ext:
Admin Email: urimanager@silibank.com
Registry Tech ID:
Tech Name: Korea 615 Shenyang company
Tech Organization: Korea 615 Shenyang company
Tech Street: shenyang hepingqu xifudalu 615 hao 2 danyuan 6-1-5
Tech City: shenyangshi
Tech State/Province: liaoningsheng
Tech PostalCode: 123456
Tech Country: China
Tech Phone: +86.024 22523102
Tech Phone Ext:
Tech Fax: +86.024 22523102
Tech Fax Ext:
Tech Email: urimanager@silibank.com
Name Server: ns13.xincache.com
Name Server: ns14.xincache.com
DNSSEC: unsigned

WHOIS Record for chongryon.com:
Domain Name: chongryon.com
Registry Domain ID: 69711868_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.melbourneit.com
Registrar URL: http://www.melbourneit.com.au
Updated Date: 2014-03-26T00:31:24Z
Creation Date: 2001-04-20T06:45:46Z
Registrar Registration Expiration Date: 2015-04-20T06:45:46Z
Registrar: Melbourne IT Ltd
Registrar IANA ID: 13
Registrar Abuse Contact Email: abuse@melbourneit.com.au
Registrar Abuse Contact Phone: +61.386242300
Domain Status: ok
Registry Registrant ID:
Registrar Name: o guanin
Registrar Organization: o guanin
Registrar Street: "hujimi2-14-15,"
Registrar City: chiyodaku
Registrar State/Province: tokyo
Registrar Postal Code: 1028138
Registrar Country: JP
Registrar Phone: +81.332627111
Registrar Fax:
Registrar Fax Ext:
Registrar Email: park2@mac.com
Registry Admin ID:
Admin Name: guanin o
Admin Organization:
Admin Street: "hujimi2-14-15,"
Admin City: chiyodaku
Admin State/Province: tokyo
Admin Postal Code: 1028138
Admin Country: JP
Admin Phone: +81.332627111
Admin Fax:
Admin Fax Ext:
Admin Email: park2@mac.com
Registry Tech ID:
Tech Name: Link Club
Tech Organization: Link Club
Tech Street: 5-39-6 Jingumae Shibuya-ku
Tech City: TOKYO
Tech State/Province: 150-0001
Tech Postal Code: JP
Tech Country: JP
Tech Phone: +81.462643403
Tech Fax:
Tech Fax Ext:
Tech Email: mel-tech@hosting-link.ne.jp
Name Server: USR-NS1.LINKCLUB.JP
Name Server: USR-NS2.LINKCLUB.JP
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdrprs.internic.net
WHOIS Record for korea-np.co.jp:

Domain Information: KOREA-NP.CO.JP
a. [B%I%a%$%s>pJs]  
b. [B%I%a%$%sL>]
KOREA-NP.CO.JP  
c. [B$=$7$-$a$]$  
B$+$V$7$-$,$$$7$c  
d. [BAH?%L>]  
B3t<02q<R BD+A/?7Js<R  
e. [Organization]  
The Choson Shinbo Company Inc.  
f. [BAH?%<oJL]  
B3t<02q<R  
g. [Organization Type]  
CO  
h. [BEPO?C4Ev<T]  
YK18923JP  
i. [B5;=QO"MmC4Ev<T]  
YK18923JP  
j. [B%M!<%`%5!<%P]  
uns01.usen.ad.jp  
k. [B%M!<%`%5!<%P]  
uns02.usen.ad.jp

[B=pL>80]  
[B>uBV]  
Connected (2015/02/28)  
[BEPO?G/7nFl]  
1997/02/14  
[B@\B3G/7nFl]  
1997/06/03  
[B:G=\99???]  
2014/03/01 01:16:34 (JST)
**Appendix B – Sites found on North Korean IP space**

<table>
<thead>
<tr>
<th>Host Name</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>smtp.star-co.net.kp</td>
<td>175.45.176.10</td>
</tr>
<tr>
<td>smtp.start-di.net.kp</td>
<td>175.45.176.10</td>
</tr>
<tr>
<td>spinef1.star.net.kp</td>
<td>175.45.176.10</td>
</tr>
<tr>
<td>spinef2.star.net.kp</td>
<td>175.45.176.11</td>
</tr>
<tr>
<td>ns1.co.kp</td>
<td>175.45.176.15</td>
</tr>
<tr>
<td>ns1.com.kp</td>
<td>175.45.176.15</td>
</tr>
<tr>
<td>ns1.edu.kp</td>
<td>175.45.176.15</td>
</tr>
<tr>
<td>ns1.gov.kp</td>
<td>175.45.176.15</td>
</tr>
<tr>
<td>ns1.kptc.kp</td>
<td>175.45.176.15</td>
</tr>
<tr>
<td>ns1.kptc.kp</td>
<td>175.45.176.15</td>
</tr>
<tr>
<td>ns1.net.kp</td>
<td>175.45.176.15</td>
</tr>
<tr>
<td>ns1.org.kp</td>
<td>175.45.176.15</td>
</tr>
<tr>
<td>ns1.org.kp</td>
<td>175.45.176.15</td>
</tr>
<tr>
<td>ns1.rep.kp</td>
<td>175.45.176.15</td>
</tr>
<tr>
<td>ns2.co.kp</td>
<td>175.45.176.16</td>
</tr>
<tr>
<td>ns2.com.kp</td>
<td>175.45.176.16</td>
</tr>
<tr>
<td>ns2.edu.kp</td>
<td>175.45.176.16</td>
</tr>
<tr>
<td>ns2.gov.kp</td>
<td>175.45.176.16</td>
</tr>
<tr>
<td>ns2.kptc.kp</td>
<td>175.45.176.16</td>
</tr>
<tr>
<td>ns2.kptc.kp</td>
<td>175.45.176.16</td>
</tr>
<tr>
<td>ns2.net.kp</td>
<td>175.45.176.16</td>
</tr>
<tr>
<td>ns2.org.kp</td>
<td>175.45.176.16</td>
</tr>
<tr>
<td>ns2.rep.kp</td>
<td>175.45.176.16</td>
</tr>
<tr>
<td>friend.com.kp</td>
<td>175.45.176.39</td>
</tr>
<tr>
<td>friend.com.kp</td>
<td>175.45.176.67</td>
</tr>
<tr>
<td>gnu.rep.kp</td>
<td>175.45.176.67</td>
</tr>
<tr>
<td>koredfund.org.kp</td>
<td>175.45.176.67</td>
</tr>
<tr>
<td>koredfund.org.kp</td>
<td>175.45.176.67</td>
</tr>
<tr>
<td>ksf.com.kp</td>
<td>175.45.176.67</td>
</tr>
<tr>
<td>naenara.com.kp</td>
<td>175.45.176.67</td>
</tr>
<tr>
<td>vok.rep.kp</td>
<td>175.45.176.67</td>
</tr>
<tr>
<td>rodong.rep.kp</td>
<td>175.45.176.68</td>
</tr>
<tr>
<td>airkoryo.com.kp</td>
<td>175.45.176.69</td>
</tr>
<tr>
<td>spwebh2.star.net.kp</td>
<td>175.45.176.7</td>
</tr>
<tr>
<td>mail.silibank.net.kp</td>
<td>175.45.176.7</td>
</tr>
<tr>
<td>kcna.kp</td>
<td>175.45.176.71</td>
</tr>
<tr>
<td>gnu.rep.kp</td>
<td>175.45.176.73</td>
</tr>
<tr>
<td>vok.rep.kp</td>
<td>175.45.176.75</td>
</tr>
<tr>
<td>friend.com.kp</td>
<td>175.45.176.8</td>
</tr>
<tr>
<td>korelcfund.org.kp</td>
<td>175.45.176.8</td>
</tr>
<tr>
<td>ns1.cooks.org.kp</td>
<td>175.45.176.8</td>
</tr>
<tr>
<td>ns1.friend.com.kp</td>
<td>175.45.176.8</td>
</tr>
<tr>
<td>ns1.gnu.rep.kp</td>
<td>175.45.176.8</td>
</tr>
<tr>
<td>ns1.kcna.kp</td>
<td>175.45.176.8</td>
</tr>
<tr>
<td>ns1.koredfund.org.kp</td>
<td>175.45.176.8</td>
</tr>
<tr>
<td>ns1.korelcfund.org.kp</td>
<td>175.45.176.8</td>
</tr>
<tr>
<td>ns1.korfilm.com.kp</td>
<td>175.45.176.8</td>
</tr>
<tr>
<td>ns1.ksf.com.kp</td>
<td>175.45.176.8</td>
</tr>
<tr>
<td>ns1.naenara.com.kp</td>
<td>175.45.176.8</td>
</tr>
<tr>
<td>ns1.rodong.rep.kp</td>
<td>175.45.176.8</td>
</tr>
<tr>
<td>ns1.silibank.net.kp</td>
<td>175.45.176.8</td>
</tr>
<tr>
<td>ns1.star-co.net.kp</td>
<td>175.45.176.8</td>
</tr>
<tr>
<td>ns1.star-di.net.kp</td>
<td>175.45.176.8</td>
</tr>
<tr>
<td>ns1.star.net.kp</td>
<td>175.45.176.8</td>
</tr>
<tr>
<td>ns1.vok.rep.kp</td>
<td>175.45.176.8</td>
</tr>
<tr>
<td>ns2.airkoryo.com.kp</td>
<td>175.45.176.8</td>
</tr>
<tr>
<td>friend.com.kp</td>
<td>175.45.176.9</td>
</tr>
<tr>
<td>gnu.rep.kp</td>
<td>175.45.176.9</td>
</tr>
<tr>
<td>koredfund.org.kp</td>
<td>175.45.176.9</td>
</tr>
<tr>
<td>koredfund.org.kp</td>
<td>175.45.176.9</td>
</tr>
<tr>
<td>ns2.cooks.org.kp</td>
<td>175.45.176.9</td>
</tr>
<tr>
<td>ns2.friend.com.kp</td>
<td>175.45.176.9</td>
</tr>
<tr>
<td>ns2.gnu.rep.kp</td>
<td>175.45.176.9</td>
</tr>
<tr>
<td>Domain</td>
<td>IP Address</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>ns2.kcna.kp</td>
<td>175.45.176.9</td>
</tr>
<tr>
<td>ns2.koredfund.org.kp</td>
<td>175.45.176.9</td>
</tr>
<tr>
<td>ns2.korelcfund.org.kp</td>
<td>175.45.176.9</td>
</tr>
<tr>
<td>ns2.korfilm.com.kp</td>
<td>175.45.176.9</td>
</tr>
<tr>
<td>ns2.ksf.com.kp</td>
<td>175.45.176.9</td>
</tr>
<tr>
<td>ns2.naenara.com.kp</td>
<td>175.45.176.9</td>
</tr>
<tr>
<td>ns2.rodong.rep.kp</td>
<td>175.45.176.9</td>
</tr>
<tr>
<td>ns2.silibank.rep.kp</td>
<td>175.45.176.9</td>
</tr>
<tr>
<td>ns2.star-co.net.kp</td>
<td>175.45.176.9</td>
</tr>
<tr>
<td>ns2.star-di.net.kp</td>
<td>175.45.176.9</td>
</tr>
<tr>
<td>ns2.star.net.kp</td>
<td>175.45.176.9</td>
</tr>
<tr>
<td>ns2.vok.rep.kp</td>
<td>175.45.176.9</td>
</tr>
<tr>
<td>vok.rep.kp</td>
<td>175.45.176.9</td>
</tr>
<tr>
<td>gnu.rep.kp</td>
<td>175.45.177.73</td>
</tr>
<tr>
<td>vok.rep.kp</td>
<td>175.45.177.75</td>
</tr>
<tr>
<td>friend.com.kp</td>
<td>175.45.177.77</td>
</tr>
<tr>
<td>koredfund.org.kp</td>
<td>175.45.177.77</td>
</tr>
<tr>
<td>korelcfund.org.kp</td>
<td>175.45.177.77</td>
</tr>
<tr>
<td>naenara.com.kp</td>
<td>175.45.177.77</td>
</tr>
<tr>
<td>vok.rep.kp</td>
<td>175.45.177.77</td>
</tr>
<tr>
<td>mail.chosunexpo.com</td>
<td>175.45.178.101</td>
</tr>
<tr>
<td>ns3.kptc.kp</td>
<td>175.45.178.173</td>
</tr>
<tr>
<td>ns3.kptc.kp</td>
<td>175.45.178.173</td>
</tr>
<tr>
<td>ns1.knic.com.kp</td>
<td>175.45.178.8</td>
</tr>
<tr>
<td>ns1.knic.com.kp</td>
<td>175.45.178.8</td>
</tr>
<tr>
<td>ns1.star.edu.kp</td>
<td>175.45.179.66</td>
</tr>
<tr>
<td>ns1.star.edu.kp</td>
<td>175.45.179.66</td>
</tr>
<tr>
<td>email.kp.col.cn</td>
<td>175.45.179.67</td>
</tr>
<tr>
<td>mail.star.edu.kp</td>
<td>175.45.179.69</td>
</tr>
</tbody>
</table>
Appendix C – Analysis of DarkSeoul Dropper

Dropper

MD5: 9263e40d9823aecf9388b64de34eae54
Also known as/detected as:
  • Dropper-FDH (McAfee)
  • Trojan:Win32/Dembr.A (Microsoft)
  • Trojan:Jokra (Symantec)

The dropper component that we examined was distributed as a UPX-packed binary.

Installation

When executed it creates the following files in the affected user’s %Temp% directory:

• alg.exe: A legitimate binary used to open SSH connections with remote servers
  MD5: e45cd9052dd3dd502685dfd9a2575ca
  Size: 166,912 bytes
• conime.exe: A legitimate binary used to open SSH connections with remote servers
  MD5: 6a702342e8d9911bde134129542a045b
  Size: 153,600 bytes
• ~pr1.tmp: Payload - A destructive bash script
  MD5: dc789dee20087c5e1552804492b042cd
  Size: 1,186 bytes
  Also known as/detected as:
    KillMBR-FBIA (McAfee)
    Trojan:SH/Kofornix.A (Microsoft)
    Trojan:Jokra (Symantec)
• AgentBase.exe: Payload - Win32 wiper component (see details below)
  MD5: db4bbdc36a78a8807ad9b15a562515c4
  Size: 24,576

Payload—attempts to connect to remote servers and upload a destructive bash script

After determining the location of user profile directories on the affected computer, the malware searches these directories for configuration files and directories that may be associated with the connection manager clients mRemote and SecureCRT.

• mRemote—an open source tool for centrally managing remote server connections using a GUI (Kevin Kline, 2008).69 This tool is no longer being actively developed or supported.
• SecureCRT—a commercial SSH and Telnet client by VanDyke Software.

If an mRemote installation is located, the dropper reads the configuration file and checks if there’s a NODE that is defined with “Username=root”, “Protocol=SSH”, and a password that is not blank. If
those conditions are satisfied it extracts the information. The password is decrypted after being extracted.

If a SecureCRT installation is located, the dropper extracts information from sessions that have Username=root, Protocol=SSH and a saved password. If these conditions are satisfied, the username, hostname, port, and password are extracted. The password is then decrypted.

After extracting these connection and server details, the dropper uses the previously dropped alg.exe and conime.exe to attempt to connect remote servers, upload and run the bash script ~pr1.tmp.

The bash script initially checks which UNIX it is running on (of HP-UX, SunOS, Linux, or AIX) and then attempts to wipe the /kernel, /usr /etc and /home directories, thus rendering the machine inoperative.

**Win32 Wiper component**

When the AgentBase.exe component is executed, it first attempts to stop the following processes, presumably in order to evade detection:

- pasvc.exe – policy agent from AhnLab
- clisvc.exe – ViRobot ISMS from Hauri

It then enumerates all physical drives and overwrites the first 512 bytes with the string: “principes”, effectively destroying the MBR (master boot record) of the affected drive.

It continues to look for removable and fixed drives, locates the root directory on these drives, and then attempts to delete all files and folders in this directory.

Finally, the affected computer is shut down and rebooted, although if the wiping mechanisms were successful then the machine will not be able to boot.

**Learn more at**

[hp.com/go/hpsr](http://hp.com/go/hpsr)