Recorded Future

REPORT

North Korea Cyber Activity

Recorded Future Insikt Group

Table of Contents

Part 1: North Korea is Not Crazy

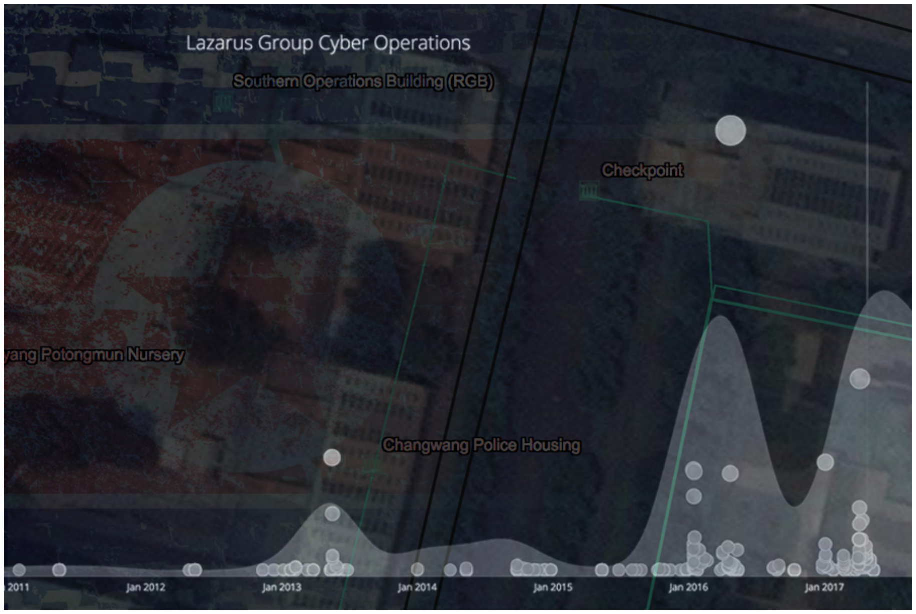
Part 2: North Korea’s Ruling Elite Are Not Isolated

PART 1

North Korea Is Not Crazy

Intent is critical to comprehending North Korean cyber activity.

Recorded Future



Understanding North Korean national objectives, state organizations, and military strategy are key to, and often missing from, discussions about attributing North Korean cyber activity. Frequently, senior political leaders, cyber security professionals, and diplomats describe North Korean leaders or their respective actions as “crazy,” “erratic,” or “not rational.” This is not the case. When examined through the lens of North Korean military strategy, national goals, and security perceptions, cyber activities correspond to their larger approach.

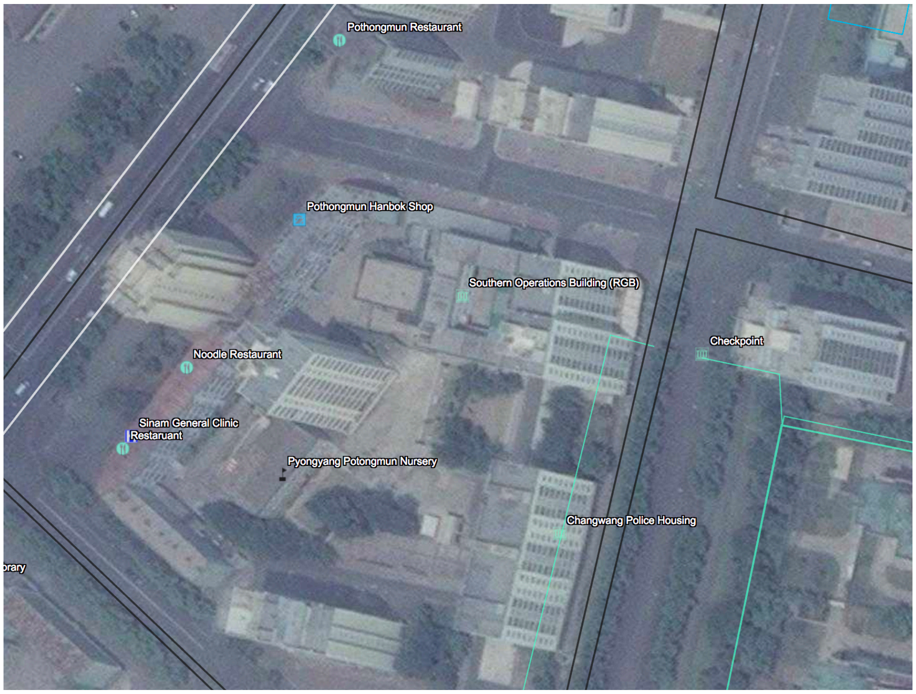
Recorded Future research reveals that North Korean cyber actors are not crazy or irrational: they just have a wider operational scope than most other intelligence services.

This scope comprises a broad range of criminal and terrorist activity, including illegal drug manufacturing and selling, counterfeit currency production, bombings, assassination attempts, and more. The National Security Agency (NSA) has attributed the April WannaCry ransomware attacks to North Korea’s intelligence service, the Reconnaissance General Bureau (RGB). We assess that use of ransomware to raise funds for the state would fall under both North Korea’s asymmetric military strategy and ”self-financing” policy, and be within the broad operational remit of their intelligence services.

Background

The Democratic People's Republic of Korea (DPRK or North Korea) is a hereditary, Asian monarchy with state, party, and military organizations dedicated to preserving the leadership of the Kim family. North Korea is organized around its communist party, the Korean Worker's Party (KWP), and the military, the Korean People's Army (KPA).

The Reconnaissance General Bureau (RGB), also known as "Unit 586," was formed in 2009 after a large restructure of several state, military, and party intelligence elements. Subordinate to the KPA, it has since emerged as not just the dominant North Korean foreign intelligence service, but also the center for clandestine operations. The RGB and its predecessor organizations are believed responsible for a series of bombings, assassination attempts, hijackings, and kidnappings commencing in the late 1950s, as well as a litany of criminal activities, including drug smuggling and manufacturing, counterfeiting, destructive cyber attacks, and more.

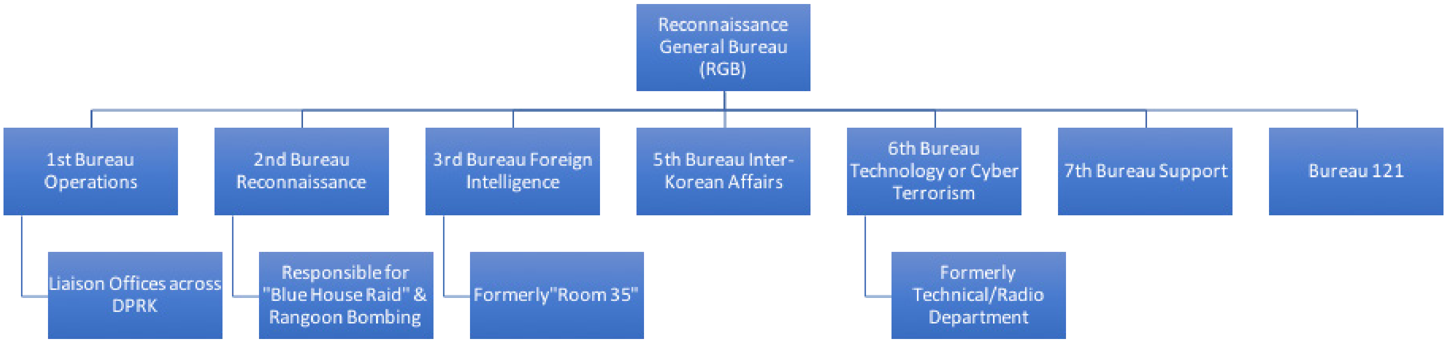


Satellite Image of the RGB Southern Operations Building in Pyongyang. (Source)

As North Korea's lead for clandestine operations, the RGB is also likely the primary cyber operations organization as well. As described by the Center for Strategic and International Studies in 2015 report:

The RGB is a hub of North Korean intelligence, commando, and sabotage operations. The RGB history of its leadership and component parts paints a picture of a one-stop shop for illegal and clandestine activity conducted outside the DPRK. The RGB and, prior to 2009 its component parts, have been involved in everything from maritime-inserted commando raids to abductions and spying. For the RGB to be in control of cyber assets indicates that the DPRK intends to use these assets for provocative purposes.

The RGB probably consists of seven bureaus; six original bureaus and a new seventh (Bureau 121) that was likely added sometime after 2013.


Reconnaissance General Bureau (RGB)
1st Bureau Operations
2nd Bureau Reconnaissance
3rd Bureau Foreign Intelligence
5th Bureau Inter-Korean Affairs
6th Bureau Technology or Cyber Terrorism
7th Bureau Support
Bureau 121
Liaison Offices across DPRK
Responsible for "Blue House Raid" & Rangoon Bombing
Formerly "Room 35"
Formerly Technical/Radio Department

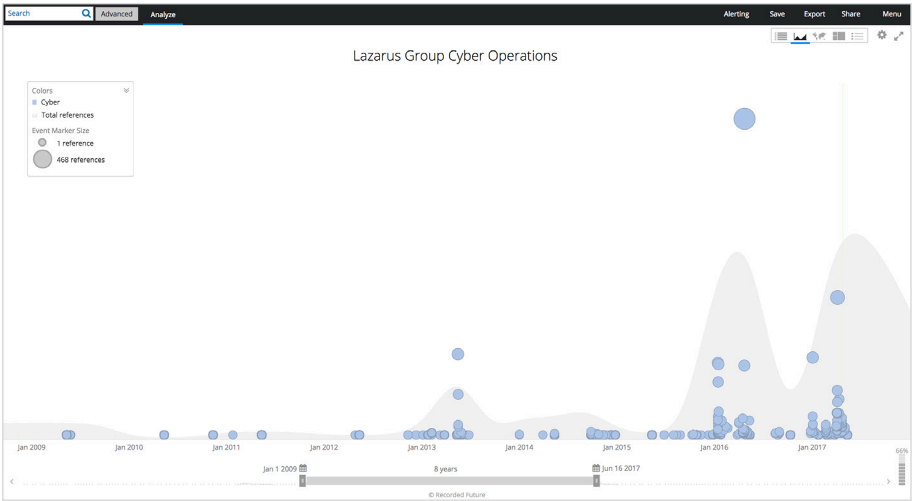
RGB organizational chart, compiled with information from The Korea Herald, 38 North, and CSIS.

Bureau 121 is probably North Korea's primary cyber operations unit, but there are other units within the KPA and KWP that may also conduct cyber operations.

Attribution of specific cyber activity to the North Korean state or intelligence organizations is difficult, and up until recently, circumstantial. On June 12, US-CERT released a joint technical alert that summarized analysis conducted by the U.S. Department of Homeland Security (DHS) and FBI on the "tools and infrastructure used by cyber actors of the North Korean government to target the media, aerospace, financial, and critical infrastructure sectors in the United States and globally."

This alert marked the first time the U.S. government linked threat actor groups and malware long-suspected to be utilized by North Korean state-sponsored actors with the with North Korean government itself. DHS and FBI explicitly identified two threat actor groups, Lazarus Group and Guardians of Peace, and three tools, Destover, Wild Positron/Duuzer, and Hangman, as used by the North Korean government. While the FBI and DHS identified many indicators of compromise, Yara rules, and network signatures, the report did not provide any evidence supporting the attribution to the North Korean government or details on which organization or unit might be responsible.

Lazarus Group, now known to be North Korean state-sponsored actors, have been conducting operations since at least 2009, with a DDoS attack on U.S. and South Korean websites using the MYDOOM worm. Until late 2015, Lazarus Group cyber activities primarily focused on South Korean and U.S. government and financial organizations, including destructive attacks on South Korean banking and media sectors in 2013 and highly publicized attack on Sony Pictures Entertainment in 2014.



Timeline of Lazarus Group cyber operations since 2009.

In early 2016, a new pattern of activity began to emerge in an unusual operation against the Bangladesh Central Bank. Actors obtained the legitimate Bangladesh Central Bank credentials for the SWIFT interbank messaging system and used them to attempt to transfer $951 million of the bank's funds to accounts around the world. A few simple errors by the actors (and some pure luck) allowed central bankers to prevent the transfer of or recover most of the funds, but the attackers ended up getting away with nearly $81 million.

The National Security Agency (NSA) has attributed this attack on the Bangladesh Central Bank to the North Korean state, however, the investigation within the U.S. government is still ongoing. Threat analysts from numerous companies have attributed this attack and subsequent attacks on banks around the world through early 2017 to the Lazarus Group (which DHS, FBI, and NSA have all linked to the North Korean government over the past three days).

According to a Washington Post report published on June 14, the NSA has compiled an intelligence assessment on the WannaCry campaign and has attributed the creation of the WannaCry worm to “cyber actors sponsored by” the RGB. This assessment, which was apparently issued internally last week, cited “moderate confidence” in the attribution and ascribed the April campaign as an “attempt to raise revenue for the regime.”

The attacks on the Bangladesh Central Bank, additional banks around the world, and the WannaCry ransomware campaign represent a new phase in North Korean cyber operations, one that mirrors the phases of violence and criminality North Korea has passed through over the past 50 years. We will examine these phases later in this post.

The broad operational range of known and suspected North Korean cyber operations has for years raised questions about the rationality of North Korean leadership, possible motivations and benefits for the country from this type of cyber activity, and why North Korea would deny responsibility for these attacks. Recorded Future research addresses these questions by examining the whole picture and pairing geopolitical and strategic intelligence with threat intelligence.

Analysis

Digging into some of these past North Korean activities is important to add context to the cyber operations we have tracked since 2009. North Korea’s engagement in a wide range of criminal and terrorist activities is part of its broad national strategy, which employs asymmetric operations and surprise attacks to overcome North Korea’s conventional national power deficit.

According to an interview with a former U.S. State Department official, and North Korea expert, in Vanity Fair, “crime, in other words, has become an integral part of North Korea’s economy. ‘It not only pays, it plays to their strategy of undermining Western interests.[1]”

It is critical to place North Korea’s criminal and cyber activity in the context of its larger military and national security strategies which support two primary objectives:

1. Perpetuation of the Kim regime,
2. Unification of the Korean peninsula under North Korean leadership.

A 2016 University of Washington study succinctly summarizes North Korea's asymmetric military strategy:

Since the end of the Korean War, North Korea has developed an asymmetric military strategy, weapons, and strength because its conventional military power is far weaker than that of the U.S. and South Korea. Thus, North Korea has developed three military strategic pillars: surprise attack; quick decisive war; mixed tactics. First, its surprise attack strategy refers to attacking the enemy at an unexpected time and place. Second, its quick decisive war strategy is to defeat the South Korean military before the U.S. military or international community could intervene. Lastly, its mixed tactics strategy is to use multiple tactics at the same time to achieve its strategic goal.

Despite their near-constant tirade of bellicose rhetoric and professions of strength, North Korea fundamentally views the world from a position of weakness, and has developed a national strategy that utilizes its comparative strengths — complete control over a population of 25 million people and unflinching, amoral devotion to the Kim hereditary dynasty.

In this context, criminality, terrorism, and destructive cyber attacks all fit within the North Korean asymmetric military strategy which emphasizes surprise attacks and mixed tactics. The criminality and cyber attacks also have the added bonus of enabling North Korea to undermine the very international economic and political systems that constrain and punish it.

Evidence is mounting that sanctions, international pressure, and possibly increased enforcement by China are beginning to take their toll on the North Korean economy and in particular, North Korea intelligence agent's ability to procure goods for regime leadership. A May 2017 report from the Korea Development Institute concluded that North Korea's black market had helped the nation endure the impacts of the international sanctions last year.

Detailed below are numerous non-cyber operations that have been conducted by the predecessor organizations of the RGB. The violence, destruction, and criminal breadth of these operations reveal the broad operational scope of these intelligence services and the context in which they are conducted.

This data further reveals a history of denials by North Korea of responsibility for operations dating back to the 1960s, putting into context the current leadership's denials of cyber operations.

Note

The activities detailed below are intended to be illustrative, not an exhaustive list, of the broad operational remit for North Korean operations.

"Blue House Raid"

One of the first major attacks on South Korea since the armistice was declared after the Korean War in 1953 occurred in 1968. The so-called "Blue House Raid" was an assassination attempt on then-President Park Chung Hee by 31 North Korean special operations soldiers on the night of January 20, 1968. The 31 North Korean soldiers crossed the DeMilitarized Zone (DMZ) on foot and managed to get within a half mile of the President's residence (the so-called "Blue House") before being exposed. Upon discovery the North Korean soldiers engaged in a series of firefights with South Korean forces; 68 South Koreans and three U.S. soldiers were killed. Most of the North Korean soldiers were killed in the eight days after the raid; two made it back across the DMZ and one was captured.

The captured North Korean soldier claimed during a press conference that they had come to "cut Park Chung Hee's throat." That account was disputed during a secret meeting in 1972 between a South Korean intelligence official and the then-Premier Kim Il-sung. Kim claimed his government had nothing to do with the raid and "did not even know about it at the time."

A captured North Korean soldier after the Blue House Raid. (Source)

1983 Rangoon Bombing

On October 9, 1983, three North Korean soldiers attempted to assassinate then-South Korean President Chun Doo Hwan while on a trip to Myanmar. A bomb at a mausoleum the President was scheduled to visit detonated early, killing 21 people, including the Korean Foreign Minister and Deputy Prime Minister.

During the trial for the bombers, testimony revealed that the North Korean agents used a North Korean trading vessel to travel to Myanmar and the home of a North Korean diplomat to prepare the bombs. In a classified report (report was declassified in 2000) ten days after the bombing, CIA analysts laid out a strong case that North Korea was responsible for the attack despite official denials of involvement from the official North Korean news agency. North Korean state media even accused President Chun of using the attack to increase tensions on the peninsula.

South Korean officials wait at the mausoleum in Rangoon minutes before the bomb detonated. (Source)

Korean Air Flight 858 Bombing

On November 29, 1987, two North Korean intelligence agents boarded and placed a bomb on a Korean Air flight from Baghdad, Iraq to Seoul. During a layover in Abu Dhabi, the two agents de-planed but left the bomb (disguised as a radio) onboard. The bomb detonated and the plane crashed in the jungle on the Thai-Burma border and killed all 115 people on board.

One of the North Korean intelligence agents, who was captured alive, later revealed that the bombing was meant to "discourage foreign participation in the 1988 Olympic Games in Seoul and create unrest" in South Korea. The agent also confessed that the order to bomb the plane had come directly from then North Korean leader Kim Il-Sung or his son, later leader Kim Jong-il.

Transition to Criminality

By the mid-1990s, North Korea had generally shifted from acts of terrorism to criminality. While North Korea had held a policy of "self-financing,[2]" in which embassies and diplomatic outposts were forced to earn money for their own operations typically via engaging in illicit activity such as smuggling, since the late 1970s, it was during the 1990s that this criminality became a business of the entire state and not just the diplomatic establishment. A number of factors affected this shift, including the end of the Cold War and the withdrawal of crucial aid from benefactors (like the Soviet Union and China), a crippling famine, a leadership transition, and years of international condemnation and punitive actions.

A 2015 report from the Committee for Human Rights in North Korea characterizes North Korea's involvement in "illicit economic activities" into three separate phases. First, from the origins of North Korea state involvement in the 1970s through mid-1990s, from the mid-90s through the mid-2000s, and approximately 2005 to today. The RGB, its predecessor organizations, and other military and intelligence services support these illicit activities.

Illegal Drug Manufacturing and Smuggling

North Korea has had a state-sponsored drug smuggling (and later manufacturing as well) program since the mid-1970s. This vast enterprise has been supported by the military, intelligence services, and diplomats and has often included working with criminal organizations such as the Taiwanese gang United Bamboo, Philippine criminal syndicates, and Japanese organized crime.[3]

Academic research indicates that North Korea has developed extensive covert smuggling networks and capabilities primarily to provide a means of hard currency for the Kim regime.

The North Korean state actively cultivates opium poppy and produces as much as 50 metric tons of raw opium per year. To put that in context, the United Nations estimates that Afghanistan produced 6,400 tons of raw opium in 2014, which makes North Korea a minor producer in comparison. According to a Congressional Research Service report, government processing labs have the capacity to process twice that amount into opium or heroin each year. Experts estimate that North Korea brings in as much as $550 million to $1 billion annually from illicit economic activities.

Counterfeiting

One of the more widely reported North Korean criminal enterprises has been the production of counterfeit American $100 (and $50) bills, or so-called "supernotes." In a 2006 Congressional testimony, the U.S. Secret Service made a definitive link between the production of the "supernote" and the North Korean state.

According to interviews in a 2006 New York Times Magazine article, North Korean state support for counterfeiting U.S. currency dates back to a directive issued by Kim Jong-il in the mid-1970s. Original counterfeiting involved bleaching $1 bills and reprinting them as $100 notes and evolved over time as North Korea's international isolation grew and its economy collapsed.

Distribution and production of the supernotes followed a similar pattern to North Korean-produced narcotics, utilizing global criminal syndicates, state and intelligence officials, and legitimate businesses. North Korea has repeatedly denied involvement in counterfeiting or any illegal operations

"Supernote" and a real $100 bill. (Source)

A History of Denial

As outlined above, North Korea has a history of denying responsibility for their violent, illicit, and destructive operations. This includes denying involvement in the Blue House Raid, the Rangoon Bombing, all criminal and illicit activity including counterfeiting U.S. dollars, the Sony Pictures Entertainment attack, and the Bangladesh Central Bank robbery. Some scholars argue that acts such as counterfeiting a nation's currency constitutes a casus belli, an action or event that justifies war, and others argue that "international legal norms and constructs do not adequately address what constitutes casus belli in the cyber domain."

Both of these arguments, as well as an understanding of North Korea's asymmetric military strategy, underscore why North Korea would not want to claim responsibility for many of these destructive and violent acts. Acknowledging state responsibility could provide the United States or South Korea with a valid casus belli, resulting in a war that North Korea would most certainly lose. Even if the evidence is strong, official government denials create uncertainty and give North Korea space to continue operations.

Impact

What has been missing from the discussion about whether North Korea is responsible for the WannaCry campaign and the bank heists has been the why — the geopolitical and strategic intelligence that give CSOs, security professionals, and threat analysts context for the activity they are seeing.

As of last week the NSA and several companies, including Symantec and Kaspersky, have linked the recent WannaCry ransomware campaign to North Korea; Recorded Future assesses that this type of cyber activity would fall within both North Korea's "self-financing" policy and asymmetric military strategy.

In this context, as a nation that is under immense international financial and political pressure and one that employs these types of policies and strategies, Recorded Future believes that North Korean cyber operations (with the goal of acquiring hard currency) will continue for at least the short to medium term (one to three years). Additionally, destructive cyber operations against the South Korean government and commercial entities will persist over this same term and likely expand to Japanese or Western organizations if U.S. and North Korea tensions remain high.

The cyber threat environment and military strategy framed above indicate that companies in several major economic sectors should increase monitoring of North Korean cyber activity. Financial services firms must remain constantly vigilant to exploitation of their SWIFT connections and credentials, possible destructive malware attacks and DDoS, and threats to customer accounts and data. Companies in the government contracting and defense sectors, especially companies that support the Terminal High Altitude Area Defense (THAAD) system deployment as well as U.S. or South Korean operations on peninsula, should be aware of the heightened threat environment to their networks and operations on the Korean peninsula.

Energy and media companies, particularly those located in or that support these sectors in South Korea, should be alert to a wide range of cyber activity from North Korea, including DDoS, destructive malware, and ransomware attacks. Broadly, organizations in all sectors should continue to be aware of the adaptability of ransomware and modify their cyber security strategies as the threat evolves.

This is part one of a two-part series on North Korea. In part two, we will examine patterns of behavior and internet activity from North Korea, including the widespread use of virtual private servers (VPS) and virtual private networks (VPN) to obfuscate browsing, internet transactions, and other, possibly malicious, activity.

[1] While there is no perfect analog to the state-sponsored criminality that North Korea engages in, Iran is probably the closest in terms of intelligence services' operational scope. For more on Iranian security services and cyber activity see: http://iranprimer.usip.org/sites/default/files/Military_Nader_Revolutionary%20Guards.pdf, https://www.foreignaffairs.com/articles/iran/2016-01-11/fallout-ploy, http://www.tandfonline.com/doi/abs/10.1080/09700161.2012.689528.

[2] Not all operations to generate funds under this "self-financing" policy are illegal in their host countries.

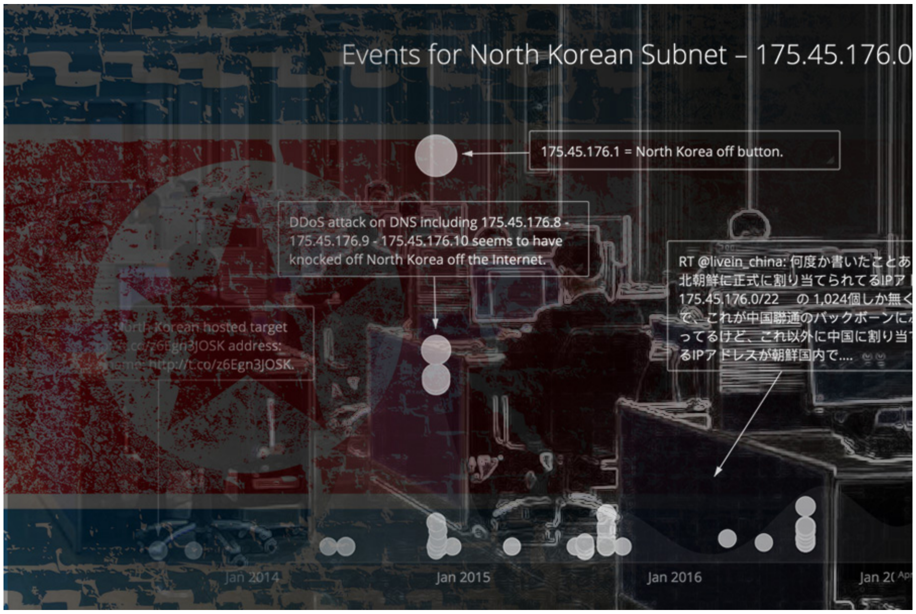
[3] Ibison, David. "Pyongyang's spy ship reveals a dark secret: Evidence from vessel suggests North Korea is working with criminal gangs to distribute drugs in Japan." Financial Times 28 May 2003: 12.

PART 2

North Korea's Ruling Elite Are Not Isolated

In-depth analysis of North Korean internet activity reveals an informed, modern, and technologically savvy ruling elite.

Recorded Future



Executive Summary

This is part two of our series on North Korea. In part one entitled "North Korea Is Not Crazy," we revealed that North Korean cyber actors are not crazy or irrational: they just have a wider operational scope than most other intelligence services.

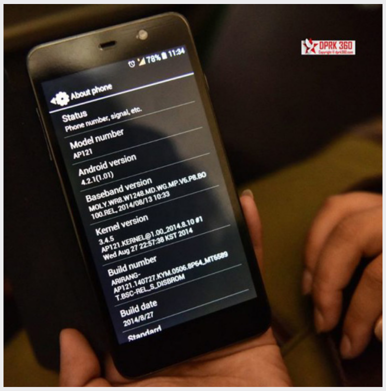
Here we enrich our analysis via our intelligence partner, Team Cymru, and conduct a comprehensive study revealing unique insights into how North Korean leadership and ruling elite use the internet and what that can tell us about their plans and intentions.

Our analysis demonstrates that the limited number of North Korean leaders and ruling elite with access to the internet are actively engaged in Western and popular social media, regularly read international news, use many of the same services such as video streaming and online gaming, and above all, are not disconnected from the world at large or the impact North Korea's actions have on the community of nations. Further, we have concluded that:

- Attempts to isolate North Korean elite and leadership from the international community are failing. In fact, their internet activity is in many ways not that different from most Westerners.
- The data set reviewed suggests that general internet activity in North Korea may not provide early warning of a strategic military action, contrary to conventional hypotheses. If there is a correlation between North Korean activity and missile tests, it is not telegraphed by leadership and ruling elite internet behavior.
- North Korea is not using territorial resources to conduct cyber operations and most North Korean state-sponsored activity is likely perpetrated from abroad, which presents an opportunity to apply asymmetric pressure on the Kim regime.

This analysis, together with part one of our blog series, demonstrates that there are likely other regime pressure points, and as a result, other tools, techniques, and partners that could be explored toward a path for North Korean denuclearization.

Background



11:34
78%
About phone
Status
Phone number, signal, etc.
Model number
AP121
Android version
4.2.1(1.01)
Baseband version
MOLY.WR8.W1248.MD.WG.MP.V6.P8.BO
100.REL, 2014/08/13 10:33
Kernel version
3.4.5
AP121.KERNEL@1.00_2014.8.10 #1
Wed Aug 27 22:57:38 KST 2014
Build number
ARIRANG-
AP121.140727.KYM.0506.8P64_MT6589
T.BSC-REL_S_DISBROM
Build date
2014/8/27
Standard

South Korean media assesses that there may be as many as 4 million mobile devices in North Korea. So while mobile devices are widespread in North Korea, the vast majority of North Koreans do not have access to the internet. Mobile devices (see image of a North Korea-made device to the left) sold to ordinary North Koreans are enabled with minimal 3G services, including voice, text messaging, and picture/video messaging, and are restricted to operating only on North Korea's domestic provider network, Koryolink.

A small minority of users, such as university students, scientists, and select government officials, are allowed access to North Korea's domestic, state-run intranet via common-use computers at universities and internet cafes. Slate described the domestic intranet this way:

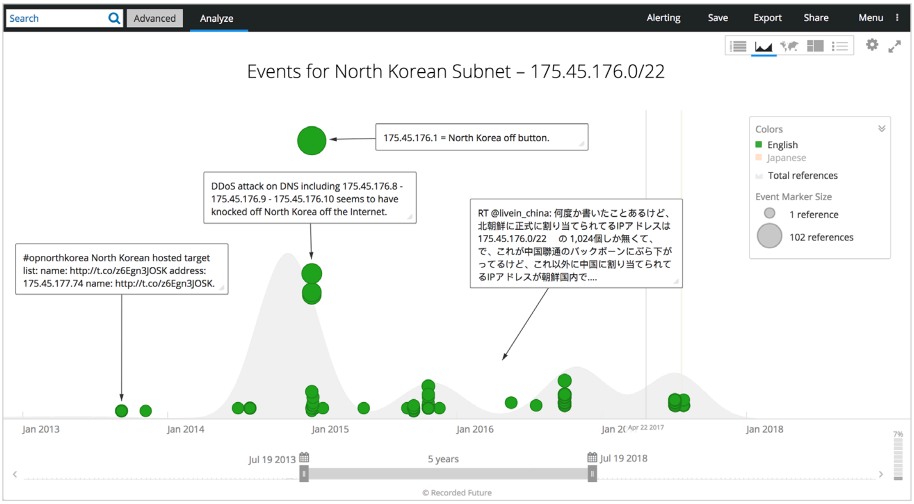
The network, called Kwangmyong, currently connects libraries, universities, and government departments and is slowly making its way into homes of better-off citizens. It houses a number of domestic websites, an online learning system, and email. The sites themselves aren't much to get excited about: They belong to the national news service, universities, government IT service centers, and a handful of other official organizations. There's also apparently a cooking site with recipes for Korean dishes.

Computer lab at Kim Il Sung University. Source: Sophie Schmidt.

Among the select few with permission to use the country's intranet are an even slimmer group of the most senior leaders and ruling elite who are granted access to the worldwide internet directly. While there are no reliable numbers of North Korean internet users, reporters estimate anywhere from "only a very small number" to "the inner circle of North Korean leadership" to "just a few dozen families." Regardless of the exact number, the profile of a North Korean internet user is clear; trusted member or family member of the ruling class.

There are three primary ways North Korean elites access the internet.

First is via their allocated .kp range, 175.45.176.0/22, which also hosts the nation's only internet-accessible websites. These include nine top-level domains (such as co.kp, gov.kp, and edu.kp) and approximately 25 subdomains for various North Korean state-run media, travel, and education-related sites.



Events for North Korean Subnet – 175.45.176.0/22

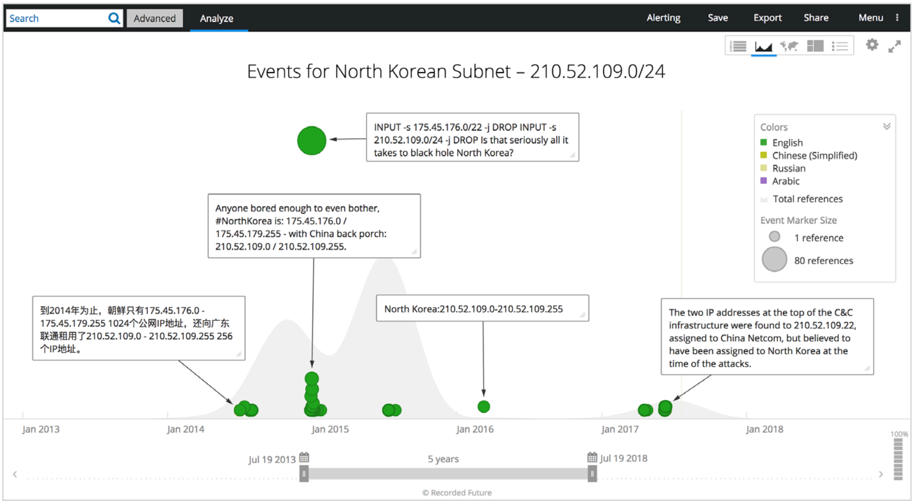
175.45.176.1 = North Korea off button.

DDoS attack on DNS including 175.45.176.8 - 175.45.176.9 - 175.45.176.10 seems to have knocked off North Korea off the Internet.

#opnorthkorea North Korean hosted target list: name: http://t.co/z6Egn3JOSK address: 175.45.177.74 name: http://t.co/z6Egn3JOSK.

RT @livein_china: 何度か書いたことあるけど、北朝鮮に正式に割り当てられてるIPアドレスは175.45.176.0/22　の 1,024個しか無くて、で、これが中国聯通のバックボーンにぶら下がってるけど、これ以外に中国に割り当てられてるIPアドレスが朝鮮国内で....

The second method is via a range assigned by China Netcom, 210.52.109.0/24. The netname "KPTC" is the abbreviation for Korea Posts and Telecommunications, Co, the state-run telecommunications company.



Events for North Korean Subnet – 210.52.109.0/24

INPUT -s 175.45.176.0/22 -j DROP INPUT -s 210.52.109.0/24 -j DROP Is that seriously all it takes to black hole North Korea?

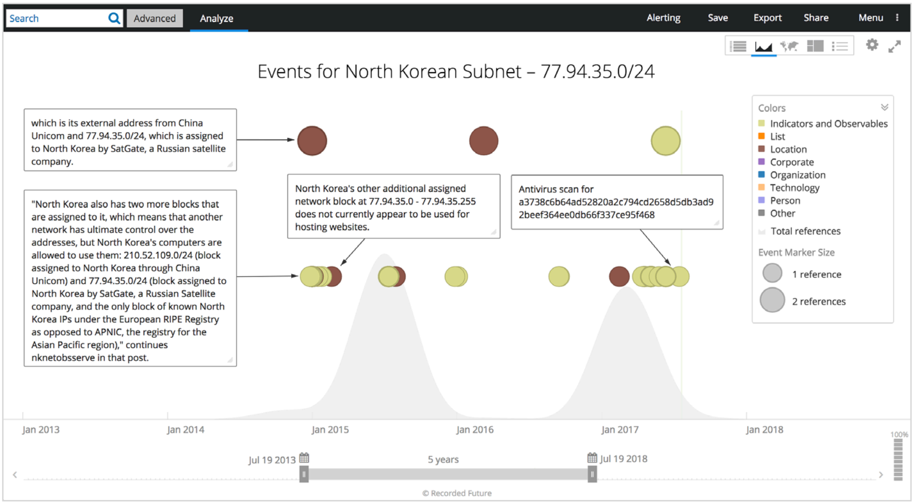
Anyone bored enough to even bother, #NorthKorea is: 175.45.176.0 / 175.45.179.255 - with China back porch: 210.52.109.0 / 210.52.109.255.

到2014年为止，朝鲜只有175.45.176.0 - 175.45.179.255 1024个公网IP地址，还向广东联通租用了210.52.109.0 - 210.52.109.255 256个IP地址。

North Korea:210.52.109.0-210.52.109.255

The two IP addresses at the top of the C&C infrastructure were found to 210.52.109.22, assigned to China Netcom, but believed to have been assigned to North Korea at the time of the attacks.

The third method is through an assigned range, 77.94.35.0/24, provided by a Russian satellite company, which currently resolves to SatGate in Lebanon.



Events for North Korean Subnet – 77.94.35.0/24

which is its external address from China Unicom and 77.94.35.0/24, which is assigned to North Korea by SatGate, a Russian satellite company.

"North Korea also has two more blocks that are assigned to it, which means that another network has ultimate control over the addresses, but North Korea's computers are allowed to use them: 210.52.109.0/24 (block assigned to North Korea through China Unicom) and 77.94.35.0/24 (block assigned to North Korea by SatGate, a Russian Satellite company, and the only block of known North Korea IPs under the European RIPE Registry as opposed to APNIC, the registry for the Asian Pacific region)," continues nknetobsserve in that post.

North Korea's other additional assigned network block at 77.94.35.0 - 77.94.35.255 does not currently appear to be used for hosting websites.

Antivirus scan for a3738c6b64ad52820a2c794cd2658d5db3ad92beef364ee0db66f337ce95f468

Editor's Note

Two important notes: One, from this point on when we refer to "North Korean internet activity" or "behavior," we are referring to use of the internet (not the North Korean domestic intranet Kwangmyong) by the select few leaders and ruling elite that are permitted access. This data does not give us any insight into intranet activity or behavior by the larger group of privileged North Koreans permitted access to Kwangmyong or diplomatic and foreign establishments that are located in North Korea.

Two, we chose this date range, April 1 through July 6, 2017, because it represented one of the periods of highest missile launching and testing activity, and also because it was the time period during which the data had the greatest depth and fidelity. While we have data stretching back to January 1, 2017, that dataset (January 1 to March 31) is much less robust.

Analysis

In the early hours of April 1, 2017, as many in the West were just waking up, checking email and social media, a small group of North Korean elites began the day in much the same manner. Some checked the news on Xinhua or the People's Daily, others logged into their 163.com email accounts, while still others streamed Chinese-language videos on Youku and searched Baidu and Amazon.

Recorded Future's analysis of this limited-duration data set has given us new insight into this isolated country and ruling regime. Our analysis demonstrates that the limited number of North Korean leaders and ruling elite with access to the internet are much more active and engaged in the world, popular culture, international news, and with contemporary services and technologies than many outside North Korea had previously thought. North Korean leaders are not disconnected from the world and the consequences of their actions.

While this data source is not absolute, it gives us a detailed picture of North Korean internet use and activity during the April to July 2017 timeframe, and as a result, we are able to reach a number of unique new insights.

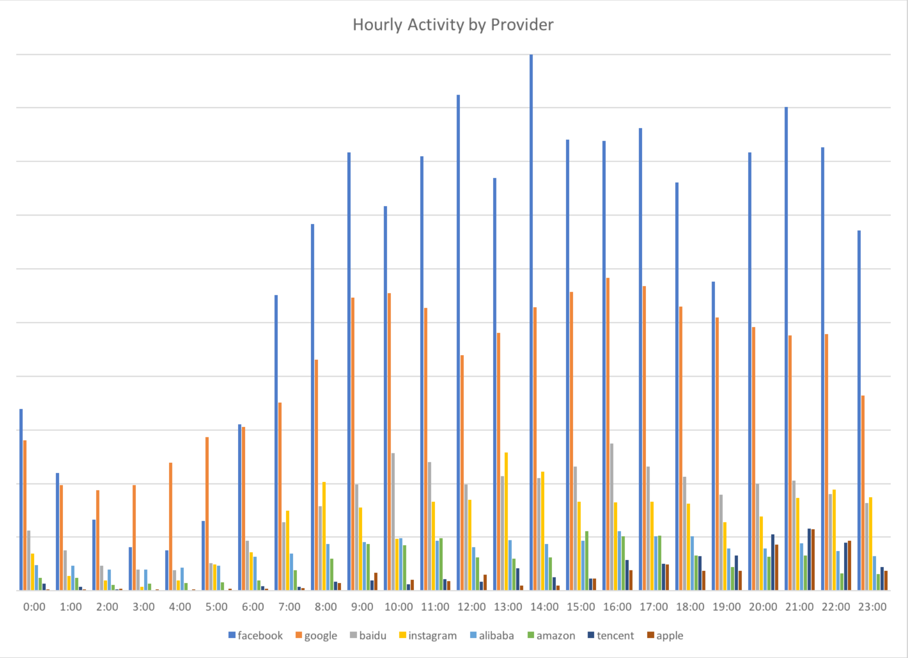
The data reveals that North Korea's leadership and ruling elite are plugged into modern internet society and are likely aware of the impact that their decisions regarding missile tests, suppression of their population, criminal activities, and more have on the international community. These decisions are not made in isolation nor are they ill-informed as many would believe.

Patterns of Use Mirror Western Users

North Korean elite and leadership internet activity is in many ways not that different from most Westerners, despite the extremely limited number of people who can access the internet; the relatively few numbers of both computers and IP space from which to reach it; the linguistic, cultural, social, and legal barriers; and sheer hostility to the rest of the world.

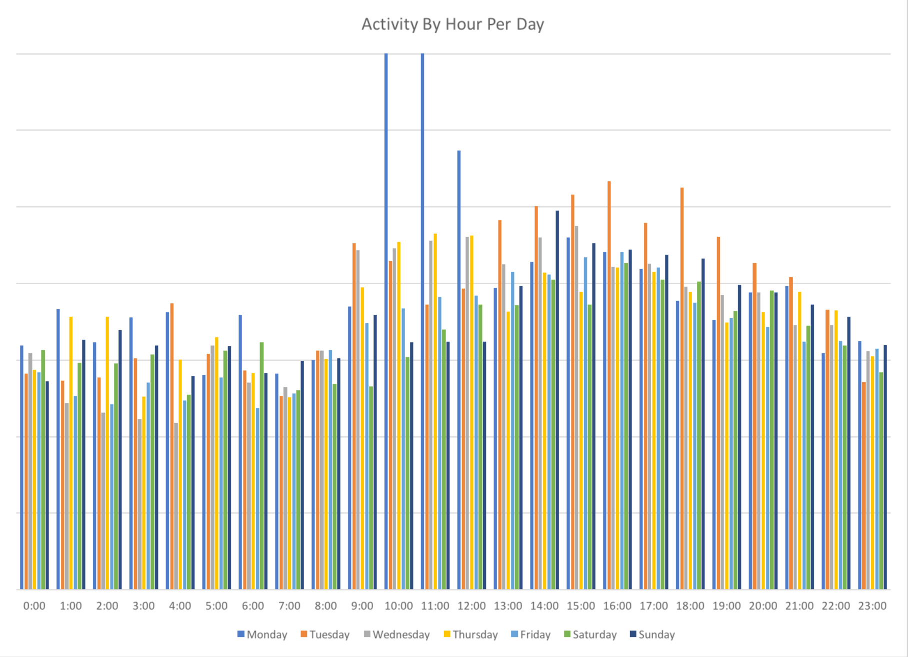
For example, similar to users in the developed world, North Koreans spend much of their time online checking social media accounts, searching the web, and browsing Amazon and Alibaba.

Facebook is the most widely used social networking site for North Koreans, despite reports that it, Twitter, YouTube, and a number of others were blocked by North Korean censors in April 2016.



Hourly activity on eight social networking, shopping, and search sites for April 1 through July 6, 2017 (actual). Providers are listed by popularity, from Facebook (highest) to Apple (lowest).

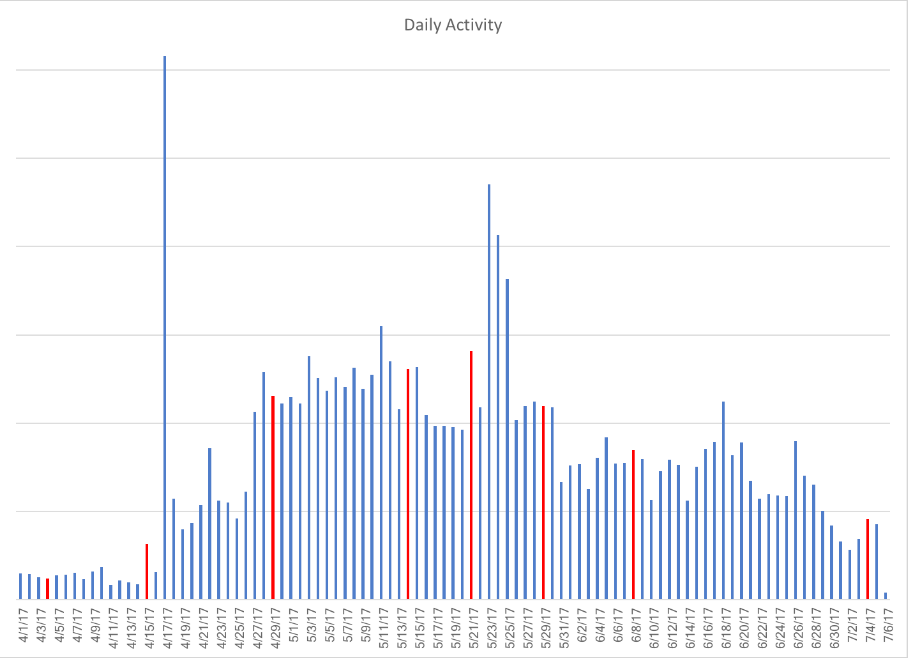
Additionally, North Koreans have distinct patterns of daily usage over this period as well. On weekdays, times of highest activity are from approximately 9:00 AM through 8:00 or 9:00 PM, with Mondays and Tuesdays being the days of consistently highest activity.



Daily internet usage by hour (not an average).

Not an Early Warning for Missile Activity

Many researchers and scholars have hypothesized that there may be a connection between North Korean cyber activity and missile launches or tests. In particular, that we may be able to forecast or anticipate a missile test based on North Korean cyber or internet activity. While we were not able to examine levels of North Korean malicious cyber activity, for this limited time period using this data set, there does not appear to be a correlation between North Korean internet activity at large and missile tests or launches.



Daily actual internet activity for April 1 through July 6, 2017. Red bars are dates of North Korean missile tests or launches.

This current data set is too short a duration of time to apply any long-term conclusions about the utility of internet activity as a warning device for missile tests. However, our analysis does suggest that if there is a correlation between North Korean activity and missile tests, it is not telegraphed by leadership and ruling elite internet behavior.

Presence in Foreign Countries

The near absence of malicious cyber activity from the North Korean mainland from April to July 2017 likely indicates that, for the most part, they are not using territorial resources to conduct cyber operations and that most state-sponsored activity is perpetrated from abroad. This is a significant operational weakness which could be exploited to apply asymmetric pressure on the Kim regime, limit current North Korean cyber operational freedom and flexibility, and reduce the degree at which they are able to operate with impunity.

This data and analysis demonstrate that there are significant physical and virtual North Korean presences in several nations around the world — nations where North Koreans are likely engaging in malicious cyber and criminal activities (as demonstrated in part one). These nations include India, Malaysia, New Zealand, Nepal, Kenya, Mozambique, and Indonesia.

Based on our analysis, we were able to determine the following:

- It is clear that North Korea has a broad physical and virtual presence in India. Characterized by the Indian Ministry of External Affairs as a relationship of "friendship, cooperation, and understanding," the data we analyzed supports the reports of increasingly close diplomatic and trade relationship between India and North Korea.
- Patterns of activity suggest that North Korea may have students at least seven universities around the country and may be working with several research institutes and government departments.
- Nearly one-fifth of all activity observed during this time period involved India.

North Korean embassy in India. (Source)

North Korea also has large and active presences in New Zealand, Malaysia, Nepal, Kenya, Mozambique, and Indonesia. Our source revealed not only above-average levels of activity to and from these nations, but to many local resources, news outlets, and governments, which was uncharacteristic of North Korean activity in other nations.

It has been widely reported that North Korea has a physical presence to conduct cyber operations in China, including co-owning a hotel in Shenyang with the Chinese from which North Korea conduct malicious cyber activity. Nearly 10 percent of all activity observed during this timeframe involved China, not including the internet access points provided by Chinese telecommunications companies.

Our analysis finds that the profile of activity for China was different than the seven nations identified above, mainly because North Korean leadership users utilized so many Chinese services, such as Taobao, Aliyun, and Youku, which skewed the data. After accounting for use of Chinese internet services, which of course do not signify either physical or virtual presence in China, the pattern of activity to local Chinese resources, news outlets, and government departments mirrored the seven previously identified nations.

This Chinese example, where the distinct pattern of activity we discovered combined with the already known facilities for cyber operations, provides us with a model we can apply to the other seven nations.

Together with the fact that North Korea has a significant physical and virtual presence in several nations around the world, and our previous research in part one, it is highly likely that North Korea is conducting cyber operations from third-party countries. Therefore, an alternative avenue to explore would be whether malicious cyber activity from these nations correlates with missile launches or tests, as opposed to activity from territorial North Korea.

Poor Security Leads to New Intelligence

Less than one percent of North Korean internet activity during this period was obfuscated or protected in any way. Among the activity that met this criteria, tradecraft varied broadly from incorrect implementation of TLS/SSL, to utilizing nearly untraceable chains of multiple virtual private networks (VPN) and virtual private servers (VPS) to transfer large amounts of data.

As an example of incorrect implementation, one North Korean user went to the trouble of using Tor (The Onion Router) to obfuscate their activity but then proceeded to use torrent file sharing and exited the Tor network from the same node every day for over three months.

Of the users that employed obfuscation technologies, a wide range of VPN and VPS services and providers were utilized. Almost all VPN and VPS consumed by North Koreans are monthly subscriptions, likely managed by an individual or government department.

It is not clear how these services are purchased and many of the providers are large and well-known Western companies. These include Sharktech, iWeb, Digital Ocean, Linode, Leaseweb USA, Telemax, Touch VPN, and others.

Many VPN and VPS were used to obfuscate or facilitate browsing, either from passive internet monitoring or domestic censors.

One U.S. VPN was used by an iPad to check a Gmail account, access Google Cloud, check Facebook and MSN accounts, and view adult content. Other VPN and VPS were used to run Metasploit, make purchases using bitcoin, check Twitter, play video games, stream videos, post documents to Dropbox, and browse Amazon.

As a result of this generally poor obfuscation, this data afforded us insight into North Korean leadership and elite interests that we have never had before. For example, many users utilized VoIP services to talk and message others overseas; others still had AOL accounts and checked them regularly; some users frequented beauty and health sites; others purchased expensive sneakers online; many users investigated industrial hardware and technology optimization services; others used iPhones, iPads, and Blackberries to communicate.

Other users spent time every day researching cybersecurity companies and their research, including Kaspersky, McAfee, Qihoo360, and Symantec; and DDoS prevention companies and technologies such as DoSarrest and Sharktech. One user received training on the use of THURAYA and satellite communications equipment and others researched the physics and engineering departments at several Malaysian, U.S., and Canadian universities.

Gaming and content streaming accounted for sixty-five percent of all internet activity in North Korea. Broadly, users consume content mostly from the Chinese video hosting service Youku, iTunes, and various BitTorrent and peer-to-peer streaming services. For games, North Korean users seem to prefer games hosted by Valve and a massively multiplayer online game called World of Tanks.

Suspect Activity

While the majority of activity from North Korea during this timeframe was not malicious, there was a smaller, but significant, amount of activity that was highly suspect. One instance was the start of Bitcoin mining by users in North Korea on May 17.

According to the Bitcoin wiki, bitcoin mining is "the process of adding transaction records to Bitcoin's public ledger of past transactions (or block chain)." Bitcoin mining is difficult because it is a computationally complex task and can require up to 90 percent of a machine's power.

The benefit to using all of this energy and adding the transaction record to the blockchain is that each miner is awarded not only the fees paid by the users sending the transaction, but 25 bitcoins once they discover a new block.

Before that day, there had been virtually no activity to Bitcoin-related sites or nodes, or utilizing Bitcoin-specific ports or protocols. Beginning on May 17, that activity increased exponentially, from nothing to hundreds per day. The timing of this mining is important because it began very soon after the May WannaCry ransomware attacks, which the NSA has attributed to North Korea's intelligence service, the Reconnaissance General Bureau (RGB), as an attempt to raise funds for the Kim regime.

By this point (May 17) actors within the government would have realized that moving the bitcoin from the three WannaCry ransom accounts would be easy to track and ill-advised if they wished to retain deniability or the attack.

It is not clear who is running the North Korean bitcoin mining operations; however, given the relatively small number of computers in North Korea coupled with the limited IP space, it is not likely this computationally intensive activity is occurring outside of state control.

Additionally, during this time frame it appeared that some North Korean users were conducting research, or possibly even network reconnaissance, on a number of foreign laboratories and research centers.

In particular, activity targeting the Indian Space Research Organization's National Remote Sensing Centre, the Indian National Metallurgical Laboratory, and the Philippines Department of Science and Technology Advanced Science and Technology Research Institutes raised flags of suspicion, but we could not confirm malicious behavior.

Impact

The international policy and engagement strategy toward North Korea has struggled to be impactful for decades because it has relied on the same set of tools (sanctions, increasing international isolation) and engaged the same nations (China, Russia, UN Security Council Permanent Five) as partners. This two-part series demonstrates that there are likely other pressure points on the regime and as a result, other tools, techniques, and partners that should be explored.

Team Cymru's intelligence and Recorded Future's analysis have revealed two separate realities.

First, in spite of the sanctions and massive international pressure, North Korea's leaders are not isolated from the outside world. They are active and engaged participants in the contemporary internet society and economy; meaning that attempts to shut North Korean leadership off from the global economy have largely failed.

Second, new tools that do not focus on Pyongyang and territorial North Korea are needed to achieve a lasting negative impact on the current Kim regime. We have identified other nations with which the West could partner and alternate tools and techniques that could be utilized to apply asymmetric pressure on North Korea. Partnering with nations such as India, Malaysia, Indonesia, or others identified above, would enable the U.S. and other Western nations to circumvent uncooperative partners in China and Russia and exert pressure on the broad North Korean operational diaspora, which, because of the regime's dependency, would likely impose larger real costs on leadership.

For cybersecurity professionals and network defenders, this two-part series reveals just how complex defending from North Korean malicious cyber activity can be. We continue to recommend that financial services firms and those supporting U.S. and South Korean military THAAD deployment as well as on-penninsula operations maintain the highest vigilance and awareness of the heightened threat environment to their networks and operations on the Korean peninsula.

Similarly, energy and media companies, particularly those located in or that support these sectors in South Korea, should be alert to a wide range of cyber activity from North Korea, including DDoS, destructive malware, and ransomware attacks. Broadly, organizations in all sectors should continue to be aware of the adaptability of ransomware and modify their cybersecurity strategies as the threat evolves.

Recorded Future

www.recordedfuture.com

@RecordedFuture

About Recorded Future

Recorded Future arms security teams with threat intelligence powered by patented machine learning to lower risk. Our technology automatically collects and analyzes information from an unrivaled breadth of sources and provides invaluable context that's delivered in real time and packaged for human analysis or instant integration with existing security technology.