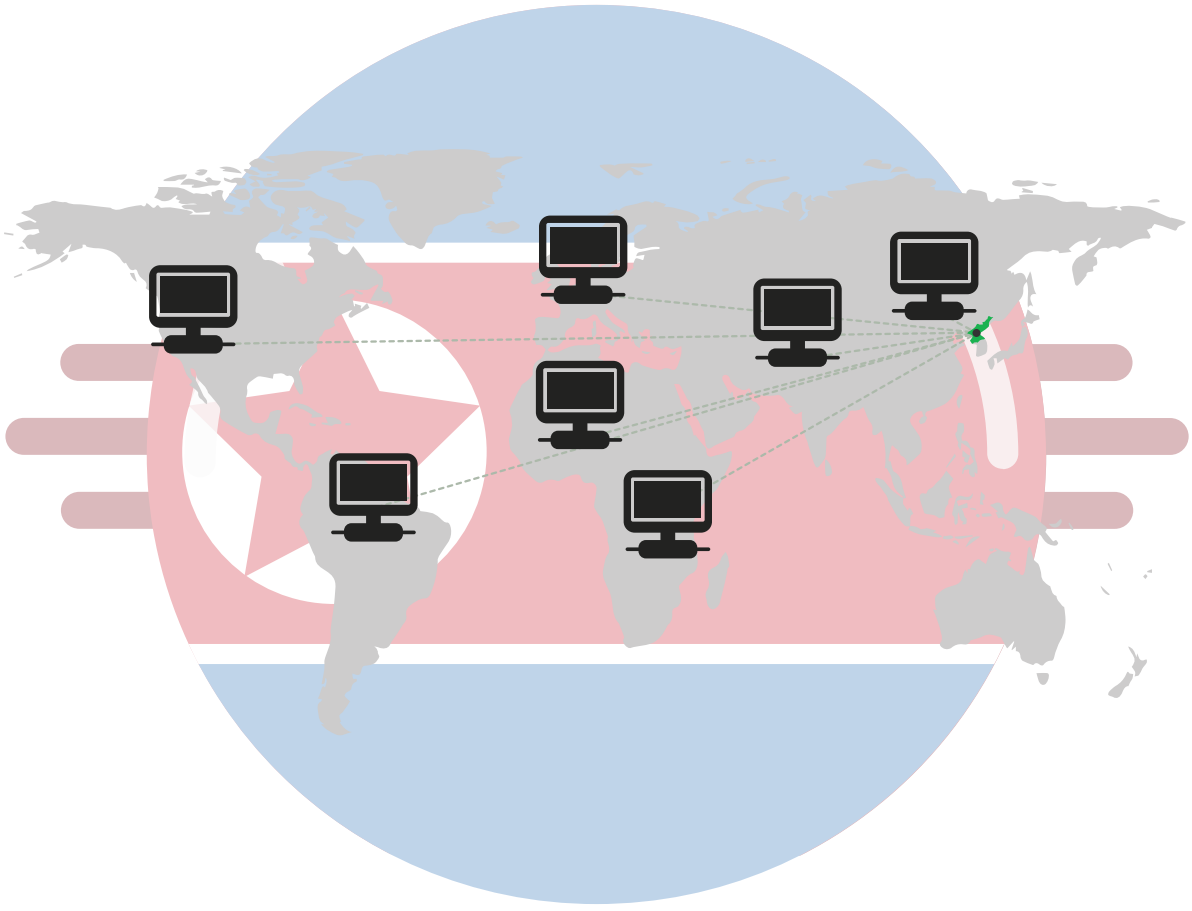
Recorded Future®

CYBER THREAT ANALYSIS

How North Korea Revolutionized the Internet as a Tool for Rogue Regimes

By Insikt Group®



CTA-2020-0209

For this research, Insikt Group examined North Korean senior leadership's internet activity by analyzing third-party data, IP geolocation, Border Gateway Protocol (BGP) routing tables, network traffic analysis, and open source intelligence (OSINT) using a number of tools. The data analyzed for this report spans from January 1, 2019 to November 1, 2019.

This report will be of most interest to government departments and organizations within the technology, finance, defense, cryptocurrency, and logistics sectors, as well as those investigating North Korean sanctions circumvention, illicit financing, and state-sponsored cyberespionage.

Executive Summary

Over the past three years, Recorded Future has published a series of research pieces revealing unique insight into the behavior of North Korea's most senior leadership. Our observations and findings during 2019 expand on these observations and point to broader conclusions about the way that North Korean leaders use the internet. For the North Korean political and military elite, the 2019 data show that the internet is not simply a fascination or leisure activity, but is a critical tool for revenue generation, gaining access to prohibited technologies and knowledge, and operational coordination.

Further, we assess that North Korea has developed an internet-based model for circumventing international financial controls and sanctions regimes imposed on it by multinational organizations and the West. This includes not only using the internet as a mechanism for revenue generation, but as an instrument for acquiring prohibited knowledge and skills, such as those enabling the development of North Korea's nuclear and ballistic missile programs, and cyber operations. This model uses three primary tactics for generating revenue — internet-enabled bank theft; use and exploitation of cryptocurrencies and blockchain technology; and low-level information technology (IT) work and financial crime.

At its most basic, North Korea has developed a model that leverages the internet as a mechanism for sanctions circumvention that is distinctive, but not exceptional. This model is unique but repeatable, and most concerningly can serve as an example for other financially isolated nations, such as Venezuela, Iran, or Syria, for how to use the internet to circumvent sanctions.

Key Judgments

- We have observed a 300% increase in the volume of activity to and from North Korean networks since 2017. We assess this is due to a number of factors, including the increased use of the Russian-routed TransTelekom infrastructure, the use of some of North Korea's previously unresolved IP space, and the stand-up of new mail servers, FTP servers, and DNS name servers to support an increased traffic load.
- Continued pattern-of-life and content shifts indicate that the internet has likely become a professional tool for North Korea's most senior leadership. The highest levels of internet use are now on weekdays during North Korean work hours, a shift from 2017, when activity was highest on the weekends and during late afternoons and evenings.
- We assess that when combined with the 300% increase in volume of activity, the increased bandwidth and capacity provided by routing an additional /24 subnet through TransTelekom infrastructure, and the recent utilization of some previously unresolved IP space, that the internet is no longer simply a fascination or leisure activity, but has become a critical tool for North Korean leaders.
- We have discovered that North Korea has created its own unique virtual private network (VPN) by exploiting domain name service (DNS). This VPN uses a technique called DNS tunneling, which refers to when the DNS process is used not for a domain resolution, but to transfer data or tunnel inside of a closed network. We assess that this technique could be used by North Korean users to exfiltrate data from the networks of unsuspecting targets, or as a means of circumventing government-imposed content controls.
- We believe that the apparent focus by the Kim regime on increasing the accessibility of its remaining four state-run insurers over the course of 2019 could be an attempt to both revitalize insurance fraud as a means of revenue generation after the sanctioning of KNIC in 2017, and to reassure potential investors in North Korea.

- We have observed an at least tenfold increase in Monero mining activity from North Korean IP ranges since May 2019. We believe that Monero's anonymity and lower processing power requirements likely make Monero more attractive than Bitcoin to North Korean users.

Recorded Future®

How North Korea Uses the Internet to Circumvent International Sanctions

Recorded Future spent most of 2019 tracking internet usage in North Korea, which provided startling insight into the many creative ways this Kim regime gets around sanctions to earn money and feed its military programs.

How North Korea Uses the Internet to Circumvent International Sanctions

Continued pattern-of-life and content shifts indicate that the internet has likely become a professional tool for North Korea's most senior leadership.

- The highest levels of internet use are now on weekdays during North Korean workhours — a shift from 2017, when activity was highest on weekends, late afternoons, and evenings.

North Korea plugs into the internet through Russian and Chinese telecom companies.

Since 2017, Recorded Future researchers have seen a **300% increase** in online activity in North Korea.

The Internet as a Tool

North Korea has devised some creative ways of evading international sanctions. These methods have helped the Kim regime with:

- Generating revenue
- Gaining prohibited information (especially related to science and technology)
- Coordinating cyber operations

Using the Internet to Generate Revenue

The North Korean government has established multiple means of making money through its use of the internet:

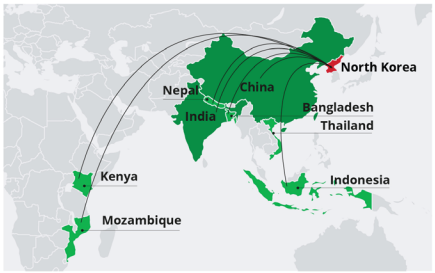
- Bank theft aided by illegal access to the SWIFT financial messaging network
- Generation and theft of cryptocurrencies
- Expansive low-level cyber crime, such as those found in video games

This combination of criminal and licit activities helps the regime to evade international sanctions and financial controls

Acquiring Prohibited Knowledge and Skills

In addition to online activities undertaken within sovereign territory, North Korea sends citizens around the world as students — in person or online — to acquire knowledge and deliver it back to the country.

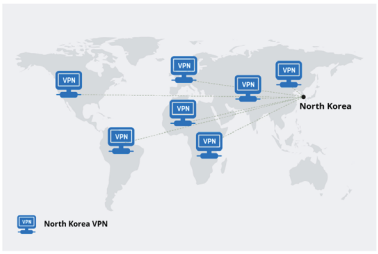
- **India and China** likely host North Korean service or information economy workers or students.



Employing New Security Technologies

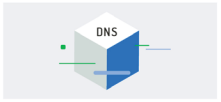
As North Korean online activity has grown, so too have its attempts to mask its activities through modern security mechanisms.

The government has increasingly employed technologies to obscure the data that moves into and out of North Korea, such as **virtual private networks (VPNs), HTTPS, and DNS tunneling.**



VPNs can make it appear that North Korean web traffic is coming from somewhere else.

HTTPS encrypts communications between a user and destination.



DNS tunneling helps them bypass firewall and service restrictions.

Insurance Fraud and the Expanding Online Presence of National Carriers

Recently, the North Korean government increased the internet accessibility of its four remaining state-operated insurers.

- This could be an attempt to both revitalize insurance fraud as a means of revenue generation after the sanctioning of its primary insurer in 2017, and to reassure potential investors in North Korea.

Background

As our research since April 2017 has shown, there are a select few among North Korea's most senior leadership who are allowed direct access to the global internet. 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: they are a family member or otherwise trusted member of the ruling class.

There are three primary ways North Korean elites access the global internet. The first method is via their allocated .kp range, 175.45.176.0/22, which also hosts the nation's only global 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.

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. 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.

We note here that when we refer to "North Korean internet activity" or "behavior," we are referring to the use of the global internet, for which only select few leaders and ruling elite are permitted access, not the North Korean domestic intranet (Kwangmyong). This data does not give us any insight into intranet activity or behavior by the larger group of North Koreans who are permitted access to Kwangmyong, or diplomatic and foreign establishments that are located in North Korea.

Analysis

Normalization of Internet Use

As we observed in our October 2018 report, the volume of internet activity has increased since we began studying North Korean leaders' behavior in early 2017. Over the course of the past nearly three years, the volume of activity to and from North Korean networks has increased by nearly 300%. We believe there are several possible reasons for this increase in internet usage.

First, North Korea has increased its bandwidth and capacity for accessing the global internet. Back in October 2017, North Korea acquired a new partner, Russia's TransTelekom (AS20485), to route the internet traffic for one of the subsets of its largest IP range, 175.45.176.0/22. Prior to then, all traffic from the entire 175.45.176.0/22 range had been routed by China Unicom (AS4837), and as of early September 2019, only the 175.45.178.0/24 subnet had ever used the TransTelekom infrastructure.

However, in mid-September 2019, we observed a change in BGP routing tables, indicating that the 175.45.177.0/24 subnet had been transitioned completely from China Unicom to TransTelekom. Both traceroutes and BGP route queries run by Hurricane Electric and other services confirm that the 175.45.177.0/24 subnet now traverses TransTelekom infrastructure.

Further, subnet analysis indicates that 45% of all DPRK internet traffic now transits TransTelekom infrastructure, up from only 36% in early 2018. We assess that the increased capacity accounts for at least some of the increase in volume of internet traffic over the past year. Routing separate subnets through both the TransTelekom and China Unicom infrastructure likely decreases latency in internet communications and increases speed and accessibility for North Korean leadership users.

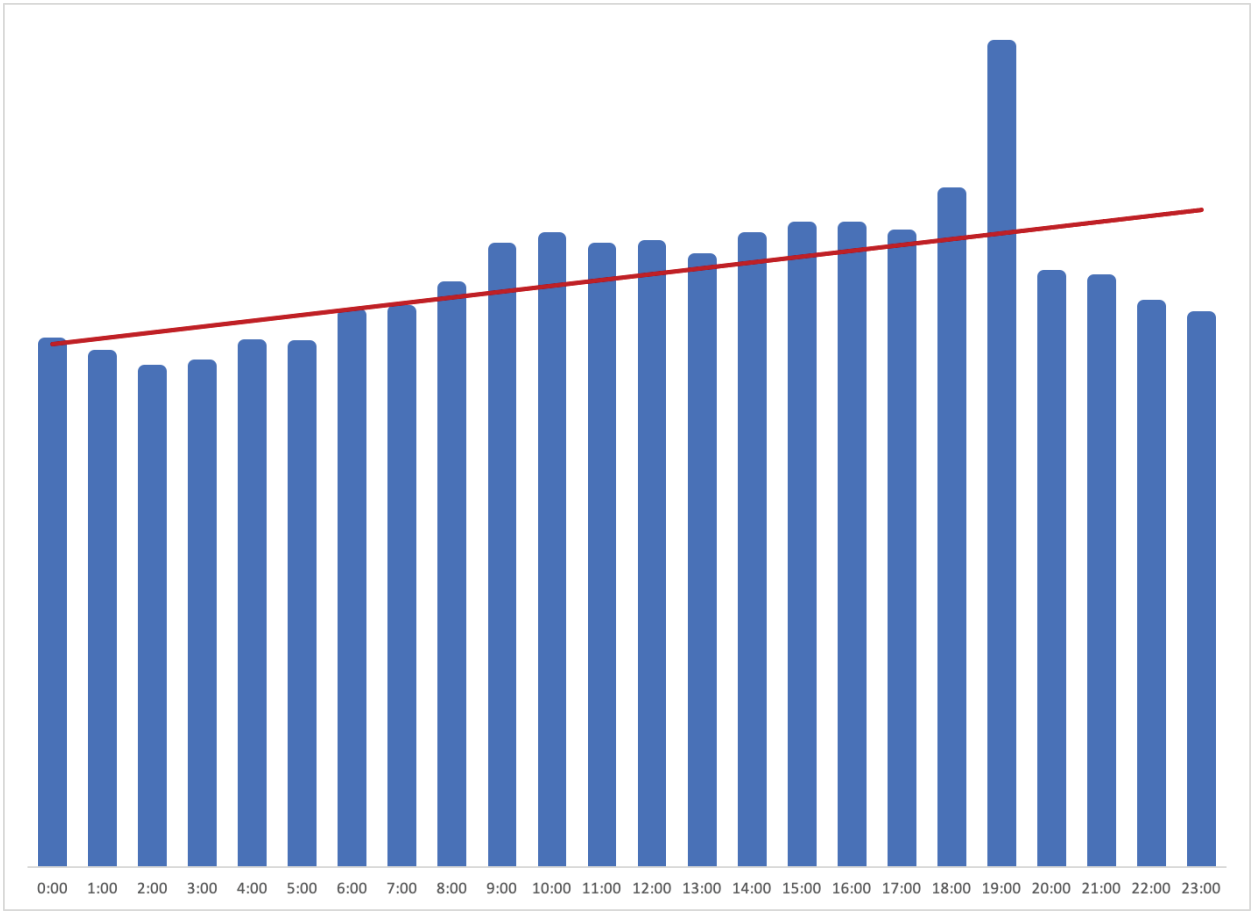
Second, North Korea has begun to use some of its previously unresolved IP space over the last six months. In early June, North Korean network administrators moved the IP resolution of two DNS nameservers for the kptc[.]kp domain. Previously, the nameservers for kptc[.]kp resolved to 175.45.176.15 and 175.45.176.16. As of early June 2019, those nameservers moved to 175.45.177.15 and 175.45.177.16, respectively. Prior to early June, those two IP addresses did not resolve at all. Since then, these two IPs have taken on additional roles as SMTP (or mail) and FTP servers.

While these changes may at first appear trivial, what they signify is the expansion of services being offered to North Korean users. We believe that the kptc[.]kp nameservers were migrated away from 175.45.176.15 and 175.45.176.16 because those IP addresses have traditionally handled a significant portion of both inbound and outbound North Korean internet traffic. On average, over the past nearly three years, 175.45.176.15 and 175.45.176.16 have handled 30% of all North Korean inbound and outbound traffic — a substantial load for two machines, which we assessed in June 2018 likely caused page loading delays and latency problems for both foreign and domestic users.

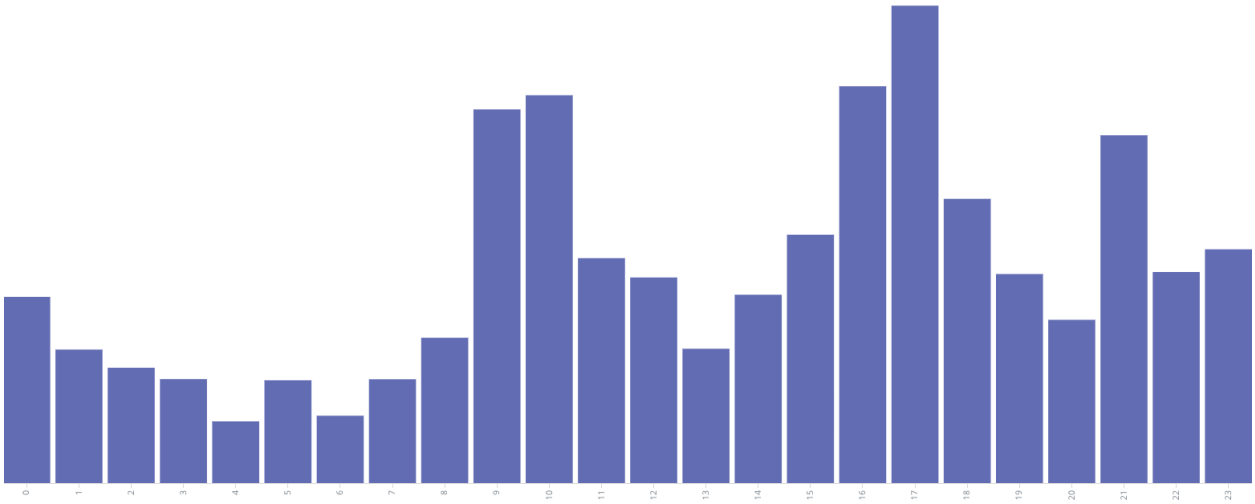
We assess that the changes in network administration we have observed over the past six months are probably in response to increased demand from North Korean users both at home and abroad. For example, setting up an internet-accessible mail server indicates that people want to be able to email users at those domains, and that users want to be able to access their mail remotely. We have observed this increase in demand via the 300% increase in internet activity over the past three years and assess that this also reflects the normalization and professionalization of internet use among the North Korean elite.

Pattern of Life Analysis

Over the course of the past three years, we have also been monitoring the evolution in North Korean leaders' patterns of daily internet usage. Below are two charts demonstrating the pattern of daily internet use by North Korean leadership by each hour in the day. What is remarkable about the most recent chart (built from data from January through October 2019) is the degree to which most of the daily activity peaks and valleys have moderated.

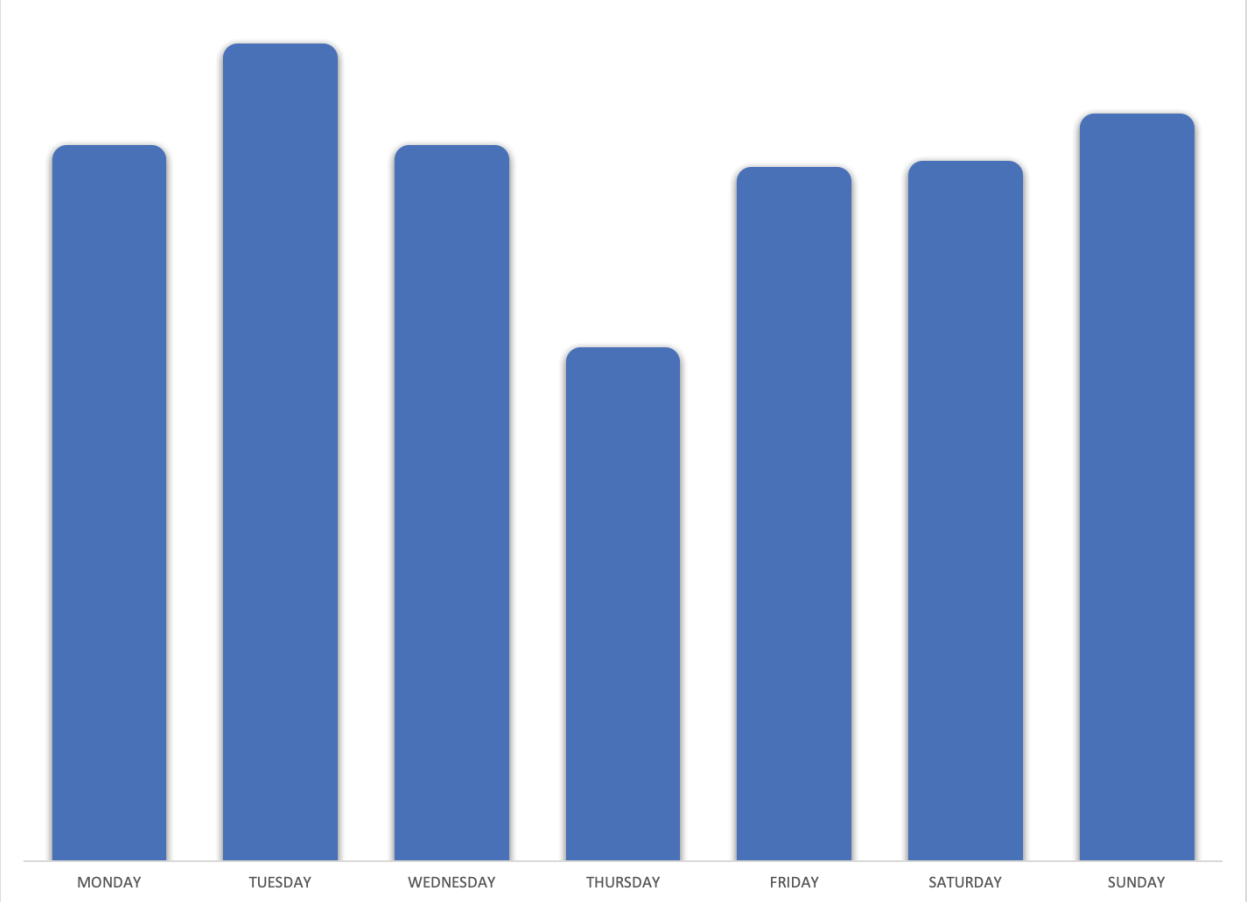


Daily internet usage by hour (not an average) from January through October 2019.

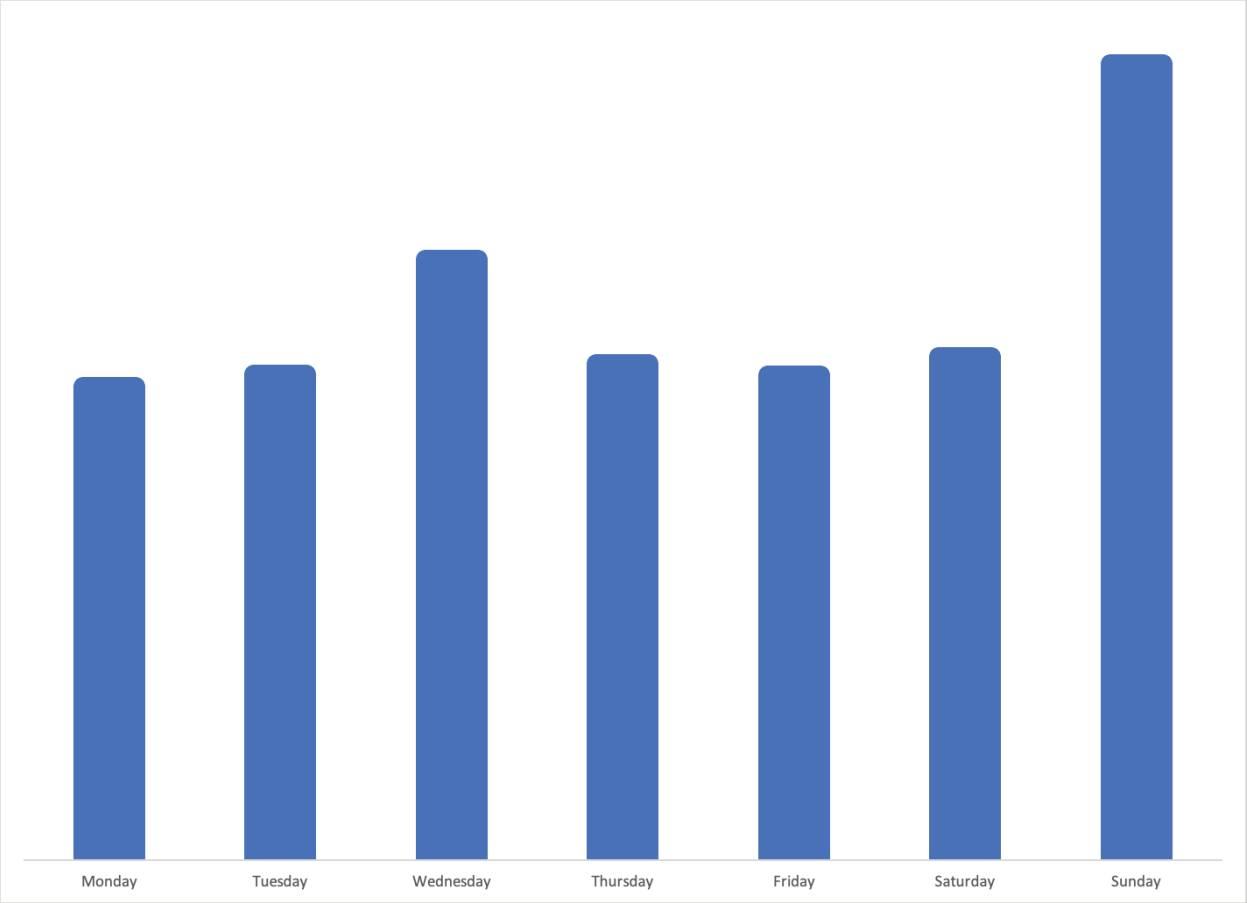


Daily internet usage by hour (not an average) from March through August 2018.

In 2019, North Korean leaders on average use the internet more during working hours and on working days than they did in 2017 (see activity-by-day charts below).



Daily internet usage by day of the week (not an average) from January through October 2019.



Daily internet usage by day (not an average) from March through August 2018.

We first observed this shift in 2018, and the data above demonstrates that these changing patterns were not an anomaly. The highest levels of internet use are now on weekdays during work hours, a huge shift from 2017, when activity was highest on the weekends and during late afternoons and evenings.

We assess that when combined with the 300% increase in volume of activity, the increased bandwidth and capacity provided by routing an additional /24 subnet through TransTelekom infrastructure, and the recent utilization of some previously unresolved IP space, that the internet is no longer simply a fascination or leisure activity, but has become a critical tool for North Korean leaders.

The Internet as a Tool

All of the findings above and our previous research point to a much broader conclusion about the way North Korean leaders use the internet. For the North Korean political and military elite, the internet has become a critical tool. This includes not only using the internet as a mechanism for revenue generation, but as an instrument for acquiring prohibited knowledge and skills, such as those enabling the development of North Korea's nuclear and ballistic missile programs, and cyber operations.

Further, we assess that North Korea has developed an internet-based model for circumventing international financial controls and sanctions regimes imposed on it by multinational organizations and the West.

Revenue Generation

We have established that the North Korean model uses three main operational pillars as their likely primary sources for internet-based revenue generation. These include:

1. Banking operations
2. Cryptocurrencies
3. Low-level information technology (IT) work and financial crime

Banking Operations

According to the United Nations Security Council Panel of Experts on the DPRK, over the past four years, financial institutions and cryptocurrency exchanges in at least 35 countries have been victimized by North Korean cyber operations, which have generated as much as $2 billion for the Kim regime. The attacks on financial institutions have been conducted via the Society for Worldwide Interbank Financial Telecommunication (SWIFT) network, where after gaining initial access to the SWIFT terminal, North Korean operators then executed a series of fraudulent transactions. These transactions transferred money from the victim bank to dummy accounts which were cashed out by North Korean operatives shortly thereafter. Information contained in the Department of Justice's September 2018 indictment of 34-year-old North Korean operator Park Jin Hyok indicates that operators would often use North Korean IP space to visit the websites of intended victims, send phishing emails to employees, and conduct network reconnaissance.

In studying both public and nonpublic information on known, DPRK-attributed banking operations, we have identified a set of generic tactics, techniques, and procedures (TTPs) for operations over the past four years.

- We assess that these banking operations are well researched and resourced by the North Koreans. Attackers likely spent anywhere from nine to 18 months inside of a target network conducting further reconnaissance, moving laterally, escalating privileges, studying each organizations' specific SWIFT instance, and disabling security procedures.
- We believe there is an emerging set of data indicating that North Korean actors have targeted websites of central banks or banking regulators via strategic web compromises (SWC). These web compromises may have then enabled follow-on intrusion attempts into the banks themselves, and the subsequent fraudulent interbank transfer attempts.
- Among publicly attributed banking operations, the initial attack vector has been a spearphish, or a SWC. However, in at least one attack against Turkish banks in 2018, North Korean operators leveraged a previously unknown Adobe Flash exploit (or zero-day) delivered via a spearphish.

- We are aware of at least two cases where destructive malware may have been used to mask or divert intrusion response efforts away from fraudulent transactions.
- Known North Korean fraudulent SWIFT transactions have been executed over holidays or long weekends in the target nation.

Cryptocurrencies

In July 2017, we published one of the first reports demonstrating North Korean leadership's interest in and use of cryptocurrencies. Since that time, North Korea has been implicated in large-scale thefts from South Korean cryptocurrency exchanges, cryptocurrency scams, cryptojacking, and cryptocurrency mining. Our research has demonstrated that North Korea has mined, stolen, or generated coins in at least three cryptocurrencies — Bitcoin, Litecoin, and Monero — and engaged in at least one blockchain-based scam that the U.N. assessed was funded by North Korea's "extortion" of cryptocurrencies.

As of November 2019, we continue to observe small-scale mining of Bitcoin. The traffic volume and rate of communication with peers has remained relatively static over the course of the last two years, however, we remain unable to determine hash rate or builds. We believe this particular mining effort is likely still small scale and limited to just a few machines.

However, since May 2019, we have observed a tenfold increase in Monero mining activity since 2018. In October 2018, North Korean Monero mining activity was similar in both traffic volume and rate of communication with peers to the Bitcoin mining mentioned above. By our assessment, as of November 2019, we have observed at least a tenfold increase in Monero mining activity. We are unable to determine the hash rate because all of the activity is proxied through one IP address, which we believe hosts at least several unknown machines behind it.

Monero has been used by North Korean operators since at least August 2017, when the Bitcoin profits from the WannaCry attack were laundered through a Bitcoin mixer and ultimately converted to Monero. Monero is distinguished from Bitcoin in that Monero is truly anonymous. All transactions are encrypted within the blockchain so that only the sender or receiver of a transaction can discover the other. Monero is also different in that it was designed to be mined by non-specialized machines, and its mining ports tend to scale by capacity. For example, many miners use port 3333 for low-end machines, and port 7777 for higher-end, higher-capacity machines.

Similar to 2018, we observed this increase in mining over port 7777, which suggests that higher-capacity machines were conducting the mining, and also at a higher hash rate. The port numbers and activity we observed were insufficient to determine hash rate — all we could assess was that mining was occuring. However, we believe that these two factors — anonymity and the ability to be mined by non-specialized machines — likely make Monero more attractive than Bitcoin to North Korean users.

According to the August 2019 U.N. Panel of Experts midterm report, a member state identified to the panel that "a professional branch of the Democratic People's Republic of Korea military" was also engaged in cryptocurrency mining. It is possible that either the Bitcoin or Monero mining activity we have observed from the North Korean IP space is being conducted by this branch of the military; however, we have no insight beyond the data we have and are unable to confirm which North Korean entity is responsible for the observed mining.

North Korean operators have also employed a number of covert techniques designed to deceive victims into installing malicious crypto-related software. One, known as cryptojacking, involved hijacking an unknowing user's computer to mine cryptocurrency and has heavily targeted South Korean and global users. Cryptojacking allows attackers to leverage the computing capacity and energy of victim machines, which significantly drives down the opportunity costs for mining cryptocurrency.

A second technique, which emerged in late 2018, utilized a malicious version of a common cryptocurrency tool called a "trading application." In this case, North Korean operators developed a legitimate and functional application that provided a single point for trading a number of cryptocurrencies. Upon installation, the application checked for updates, and instead installed a well-known North Korean remote access trojan (RAT) called FALLCHILL. This malicious trading application then facilitated access to the network of a targeted cryptocurrency exchange, although it is not clear in this instance if the attack was successful.

Blockchain analysis company Chainalysis documented the use of a similar technique to steal nearly $7 million in several cryptocurrencies from a Singapore-based exchange called DragonEx in March 2019. In this case, North Korean operators created a functional automated cryptocurrency trading bot called Worldbit-bot, which also contained a RAT that facilitated access to DragonEx networks and ultimately the theft of $7 million worth of coins.

We assess that cryptocurrencies are a valuable tool for North Korea as an independent, loosely regulated source of revenue generation, but also as a means for moving and using illicitly obtained funds. The U.N. concluded that "cryptocurrency attacks allow the DPRK to more readily use the proceeds of their attacks abroad," and that North Koreans go to great lengths, including initiating thousands of transactions, routing through multiple countries, and conversions to different coins, to evade attempts to track the funds.

Low-Level IT work and Financial Crime

A seies of defector interviews conducted by reporters, scholars, and researchers since approximately 2012 has given the outside world a glimpse into the goals and staffing of North Korean cyber operations. Defectors have built a picture of a North Korean operational apparatus composed largely of operators and programmers living in facilities overseas, tasked with the overarching goal of generating revenue for the Kim regime.

Defectors have detailed the degree to which counterfeiting video games and scamming their users has become critical to revenue generation for the Kim regime. One defector, who had worked in a house in China with dozens of other North Korean hackers, reported that these men were required to earn nearly $100,000 a year, with 80% being sent back to the Kim regime. To meet this requirement, the men created counterfeit video games, bots that stole digital items such as weapons, points, and gear, resold them for profit, and discovered and sold new vulnerabilities in gaming software. Further reports have confirmed that North Korean operators have also targeted online casinos, gamers, and Automated Teller Machine (ATM) users in South Korea to generate funds.

In September 2018, the Wall Street Journal reported that North Korean operatives had been using "gig economy" IT freelancing websites, such as UpWork and Freelancer, to solicit jobs from unknowing global users. In particular, some of the jobs included website and application development, such as "a bot to facilitate bulk purchases on Canadian e-commerce platform Shopify; a website for a U.S. job-search company; and a graphic-design project." In this case, these North Koreans were operating out of a city called Shenyang, in northeast China.

This paints the picture of an operational model which is heavily, although not entirely, dependent upon sending North Koreans overseas to conduct cyber operations.

Gaining Access to Prohibited Technologies and Knowledge

North Korean defectors have also talked extensively about the role that foreign countries play — many unknowingly — in the Kim regime's cyber operations. From the cyber perspective, third-party countries are used by the Kim regime to both train and host state-sponsored operators.

North Korea is not only exploiting third-party nations to train cyber operators, but also possibly even to acquire nuclear-related knowledge banned by U.N. sanctions. In a September 2017 investigation, the Wall Street Journal discovered that North Koreans were engaged in study abroad, particularly in China, of subjects that "could contribute to the DPRK's proliferation of sensitive nuclear activities or the development of nuclear weapon delivery systems, including teaching or training in advanced physics, advanced computer simulation and related computer sciences, geospatial navigation, nuclear engineering, aerospace engineering, aeronautical engineering, and related disciplines."

Further, defectors have reported that cyber operators are often sent abroad after university to obtain advanced training as well. Countries explicitly named by defectors have included China, Russia, and India.

This operational model of sending North Koreans abroad to train and conduct cyber operations becomes especially relevant when comparing the means by which these hackers earned money for the regime to the North Korean elite web traffic that we analyzed. In our prior research, we developed a heuristic to identify significant physical and virtual North Korean presence in nations around the world. That heuristic included above-average levels of North Korean internet activity to and from these nations, but also included the browsing and use of many local resources, such as news outlets, district or municipal governments, local educational institutions, and more.

This technique enabled us to identify nations where North Koreans were likely physically located or living. We have continued to refine our techniques and this analytic over the course of 2019, and have primarily observed a continuation of activity we observed in eight countries — India, China, Nepal, Kenya, Mozambique, Indonesia, Thailand, and Bangladesh — during 2019. However, while this analytic has been useful in the past, it has gradually yielded less substantive insight into North Korean behavior in these nations for two reasons.

First, even though the North Korean ruling elite do not universally exercise strong internet security procedures, the broad trend for both North Koreans and across all internet users is toward greater security. This means that it has gotten harder over time to track North Korean internet activity and reveal new insights.

Second, large technology companies are providing an increasing breadth of services to customers, including DNS, content delivery, cloud services, and more. From a network perspective, it is incredibly difficult to discern the end content behind generic DigitalOcean, Cloudflare, or GoDaddy infrastructure. Even ports and protocols only provide so much data, and oftentimes, a session that terminates in a DigitalOcean box reveals nothing.

Based on our data, we continue to assess that both China and India, knowingly or unknowingly, host and enable North Korean operations. India, in particular, likely continues to be both a host for and victim to North Korean cyber operations.

Operational Security

In early 2018, we noticed that North Koreans dramatically increased their use of operational security techniques, such as virtual private networks (VPN), virtual private servers (VPS), transport layer security (TLS), The Onion Router (Tor), and others. By late 2018, that operationally secure behavior had moderated, from 13% of traffic overall, to just above 5%. We believe that monitoring the use of secure browsing technologies by North Korean leaders is an indicator of two things: technological savvy and responsiveness, and the degree of state-level control over elite behavior.

In 2019, the use of secure browsing technologies rebounded slightly to 9.5% of all internet traffic. Among them, HTTPS was the most widely used by North Korean leaders. This is likely a function of the fact that nearly half of the world's top one million websites default to HTTPS.

Another change we observed in North Korean operational security behavior in 2019 was the incorporation of DNS tunneling. DNS (Domain Name System) was created to enable computers to resolve a domain name (pyongyangtimes[.]com[.]kp, for example) to an IP address (175.45.176.67). The original intent for DNS was to ease the lookups and associations of domains and IP addresses, not to secure that process. As a result, and because DNS is so critical to a network's operation, DNS ports (port 53 typically) are left open, and traffic is relatively unscrutinized. DNS tunneling is when the DNS process is used not for a domain resolution, but for data transfer or tunnel between networks or devices.

In the case of North Korea, we observed users introduce DNS tunneling in mid-2019. Again, because DNS is typically lightly scrutinized, it is an ideal protocol for bypassing firewall and service restrictions, and DNS tunneling toolkits are widely available. DNS tunneling is not a new technique, but we believe it has only recently been employed by North Korean users. In the case of the North Korean DNS tunneling activity, the majority of destination IPs were also identified by Shodan as VPN endpoints and MicroTik devices, indicating that this solution was likely intended as an alternate VPN.

Use of this specific technique provides another window into how technologically savvy some North Korean elite internet users are, as DNS tunneling is not a technique most average internet users would be familiar with. We assess that there are two likely reasons for leadership to employ DNS tunneling:

1. **To obfuscate intrusion activity**. DNS tunneling can be used to to exfiltrate data from victim networks or to create a communications channel between an infected endpoint and a command-and-control (C2) server. Malicious communications over DNS are less likely to be blocked or identified because most organizations employ permissive DNS security policies in order to facilitate network connectivity.

2. **To bypass government-imposed security controls or content restrictions**. Although North Korean internet users are members of the most senior leadership class, it is possible that some may wish to access content outside of what is permitted by the Kim regime. For example, we know that in 2016, the Kim regime began to block domestic users from accessing Facebook, YouTube, and Twitter. However, by using network traffic analysis, we have observed North Korean users browsing to those platforms ever since. DNS tunneling could be a way for more savvy internet users to bypass content restrictions like these or other security controls by using a rarely restricted protocol.

DDoS Attacks Targeting DPRK Infrastructure

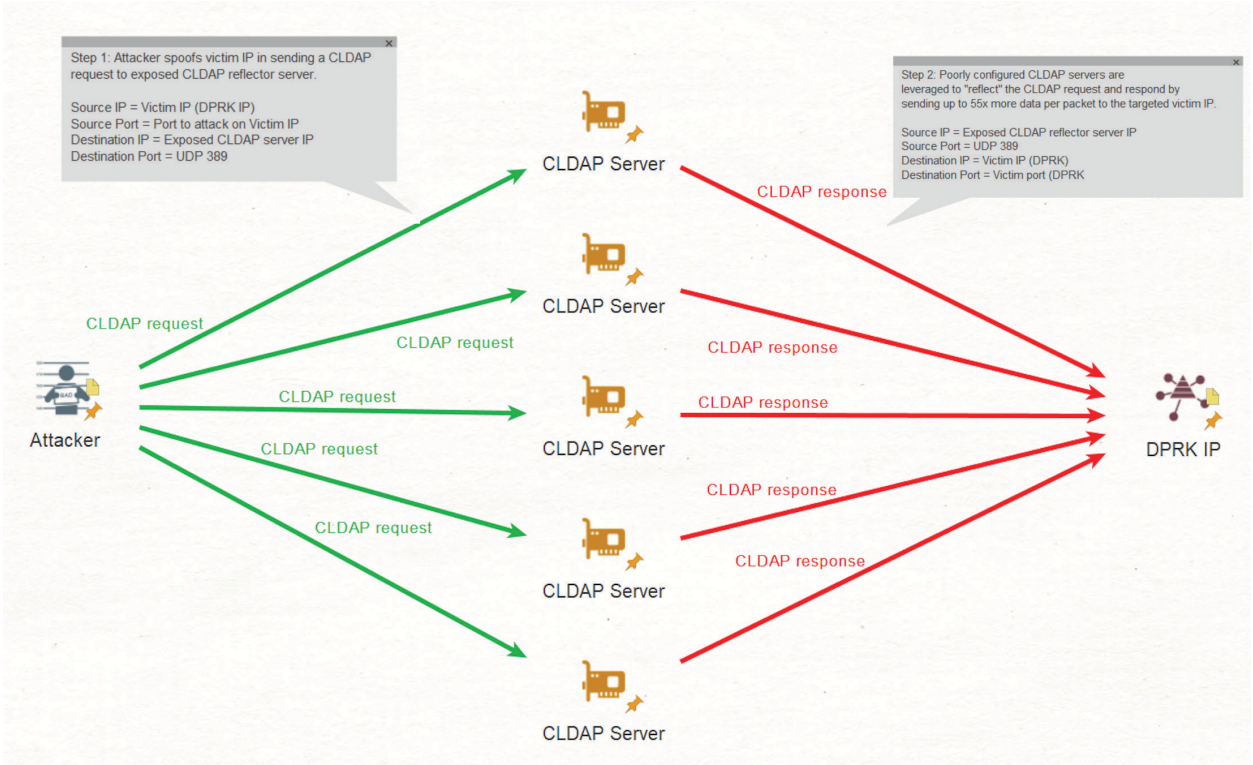
It is not unusual for North Korean websites to be targeted by denial-of-services (DoS) or distributed denial-of-service (DDoS) attacks. For example, on May 28, 175.45.176.67, which hosted websites for the Pyongyang Times, Naenara, and several North Korean insurance companies, was targeted by a DDoS attack lasting one hour with DNS traffic levels peaking at an observed rate of at least 550 megabits per second. DNS flooding is the most common type of DDoS we have observed utilized against North Korean infrastructure.

Beginning in late April 2019, we observed a unique type of DDoS attack, identified by a surge in coordinated connectionless LDAP (CLDAP) activity emanating from devices in at least 161 countries around the world and targeting a single North Korean IP address. The activity began at around midday North Korea local time and only lasted 25 minutes, with CLDAP traffic levels peaking at an observed rate of at least 1.5 gigabits per second — several orders of magnitude higher than observed daily norms for the mainland North Korea-hosted IP address space.

CLDAP is typically used on corporate networks for directory services, such as accessing usernames and passwords from the active directory. However, in 2016 and 2017, security companies began to see CLDAP and LDAP being abused in DDoS attacks. The technique of executing a DDoS over CLDAP simply requires the attacker to replace their source IP address with their intended victim's IP in a CLDAP request to an open reflector server that has the connectionless LDAP service running. The spoofed address then tricks the CLDAP reflector server into sending the CLDAP response not back to the requestor, but to the intended victim.

We also observed that the average CLDAP request packet size was around 80 bytes with an average corresponding response packet size of around 1472 bytes. This implied an approximate amplification factor of 18x was achieved by the attackers during the 40 minutes of the DDoS attack. In a 2017 interview, an Akamai security responder conveyed that the largest CLDAP attack they had observed had achieved rates of three gigabits per second and assessed that an attack of that size would be "enough to bring smaller sites offline and potentially cause latency issues on others."

The rate of the attack we observed was 1.5 gigabits per second, which we assess was possibly enough to cause disruptions, at the least, to North Korean public-facing internet infrastructure.



Top-level diagram of reflective DDoS amplification attack methodology used against DPRK global-internet-facing infrastructure in late April 2019.

We also identified two further suspected reflective CLDAP DDoS amplification attacks: one on the morning of May 7, 2019 lasting just over 40 minutes, and another the next evening on May 8, which lasted approximately an hour. Both of these attacks were an order of magnitude smaller in terms of the number of unique CLDAP reflector servers used, although the relative CLDAP amplification factor in data size remained consistent at 18x. Interestingly, almost all of the reflector servers used in the May 8 attacks were also used in the attacks against North Korean IPs a day earlier. Further, despite the order of magnitude difference in total number of resolvers used, 62% of the resolvers used in the May 7 attack were found to have also been used in the earlier April 23 attack.

Attack	Date (Zulu)	Peak Activity Duration	DDoS Amplification Factor	Total Number of Observed CLDAP Reflectors Used
Attack 1	23/04/2019	40 minutes	18.88	10529
Attack 2	06/05/2019	41 minutes	18.35	1338
Attack 3	07/05/2019	61 minutes	18.34	598

We have no information regarding who executed either the April or May attacks. Again, DDoS attacks are not uncommon for North Korea, and we chose to explore this one simply because of the uniqueness of the protocol and rate of attack.

North Korean Insurance Industry

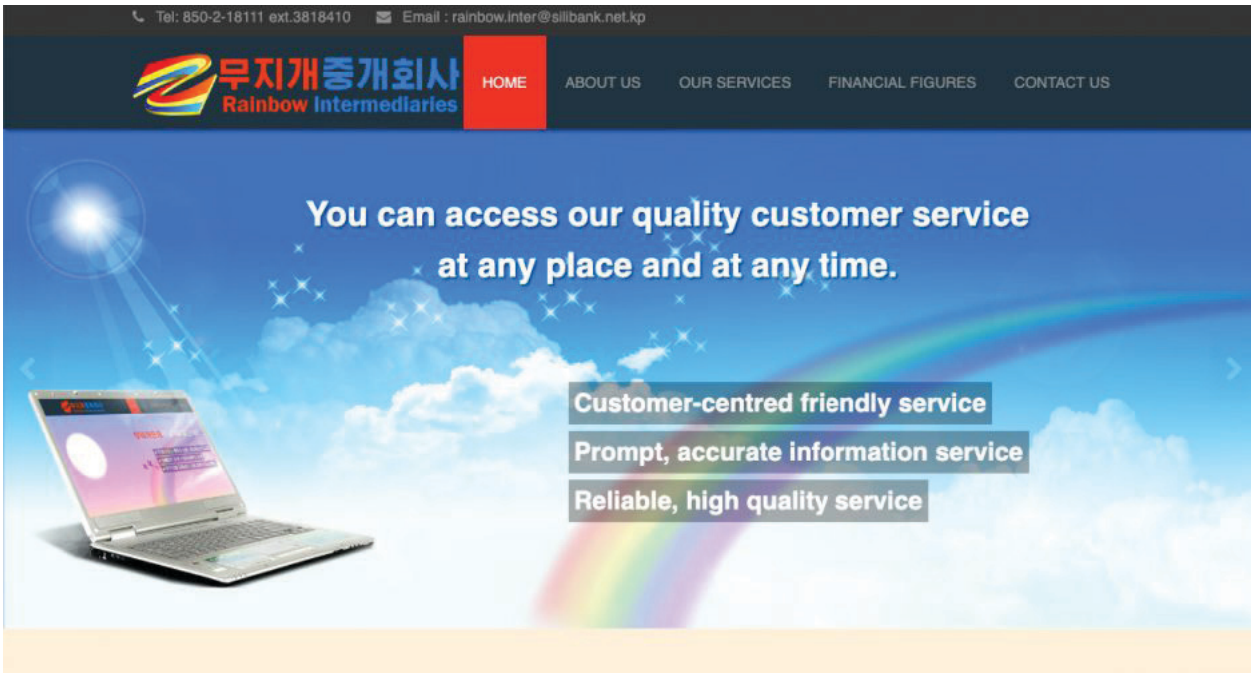
We assess that North Korea began digitizing and internationalizing its insurance industry in 2019, possibly as a way to spur increased foreign investment and/or fraudulently generate revenue for the Kim regime.

According to NK News, North Korea has five insurance companies:

1. Korea National Insurance Company (KNIC), established in 1947, general insurance
2. Rainbow Intermediaries, established in May 2015, fire, motor, contractors, machinery breakdown, life, travel, personal accident, tourist, reinsurance
3. Samhae Insurance Company, established in October 2016, marine hull, cargo, liability, and aviation
4. Polestar Insurance Company, established in August 2016, insurance and reinsurance services in fields of fire, engineering, credit, and agriculture
5. Future Re Company, established in October 2017, facultative and treaty reinsurance

In August 2017, the United Nations designated KNIC a sanctioned entity because of its links to Office 39 of the Reconnaissance General Bureau (RGB) and their involvement in insurance claim scams linked to the funding of the North Korean missile program. Despite their establishment several years prior, our data reveals that the last four insurance companies did not have a presence on the global internet until late 2018 and early 2019.

Within the last year, Samhae, Polestar, and Future Re all acquired global internet websites and mail servers. The websites for all three companies, as of November 2019, are hosted at 175.45.176.67. Future Re established a mail server in late December 2018 at 175.45.176.20, which also hosts the mail server for Silibank, an internet company based in Shenyang, China that became one of North Korea's first internet service providers (ISP) back in 2001. Silibank still offers email services for North Korean clients, including Rainbow Intermediaries, which lists a Silibank domain as an email contact on its webpage.



Screenshot of the Rainbow Intermediaries website taken by NK News in July 2019.

The global internet infrastructure for all four insurance companies was only created within the last year. Further, our data demonstrates increasing levels of traffic to the Future Re mail server and Samhae, Polestar, and Future Re websites from users in India, Russia, and Iran since February 2019. Far from being independent corporate entities, the digital footprints of all four insurance companies suggest that they are run and managed from the same internet infrastructure and likely represent a single state-led effort.

In December 2018, the President of Polestar, Kim Kyung-hoon, stated that the company had established 11 branches and 70 local offices across North Korea and planned "to expand our services further to the international market," by "building networks with

internationally renowned insurance companies." Similarly, the president of Samhae Insurance told South Korean media that the company had branches and agents at all "major port cities, fisheries bases, and transportation bases," in North Korea and that the company had started the reinsurance of fishing boats in November 2018.

However, what makes North Korean insurance companies an interesting topic is the role that they have played historically in generating funds for the Kim regime and how they are necessary to encouraging foreign investment. In 2017, a North Korean diplomatic defector described how the Kim regime would use KNIC to earn tens of millions of dollars a year from insurance fraud:

> *"In North Korea, there is only one state-owned insurance company, so that even if it fabricates an accident, there is no way to verify its claims. After purchasing international insurance or reinsurance for state infrastructure, documents are forged (on alleged accidents), which earns the state tens of millions of dollars a year."*

For thirty years, the primary state-owned insurance company, KNIC, has exploited reinsurance contracts purchased with international reinsurers to file potentially false claims and generate tens of millions of dollars for the Kim regime. According to The Times, in 2014, KNIC's global assets reached £787 million, or nearly $1.3 billion.

Although verifiable instances of North Korean insurance fraud are difficult to find, there are a couple cases over the last decade that demonstrate the likely scope of this fraud. In 2011, a joint Malaysian-North Korean construction company was awarded a contract for $18 million to build 213 condo units in a suburb of the Ugandan capital. Over the course of the next year, the construction company purchased a series of over-valued insurance policies and was paid 20% up front before work even started. After years of negotiations, court cases, and likely fraud, in 2018, both the North Korean-owned construction company and Uganda housing authority walked away from the project without completing the condos and having claimed several million dollars in insurance payouts.

In one of the most infamous cases, KNIC filed a claim for damage from a helicopter crash in Pyongyang in 2005 which destroyed a warehouse containing emergency relief goods. KNIC had insured the goods with a consortium of international insurers for nearly $60 million. The insurers refused to pay for several years, citing overstated property damage and suspect documentation, but eventually settled with KNIC for nearly $57 million. At the time, North Korea was believed to be pursuing a number of claims worth nearly $150 million with Western insurance companies.

According to some Chinese investors, these additional insurance companies may also have the effect of boosting confidence in North Korean investments. Specifically, "the new insurance intermediary shows a sign of growing complexity and competition in the commercial services within the North Korean economy."

We believe that the apparent focus by the Kim regime on increasing the accessibility of its remaining four state-run insurers over the course of 2019 could be an attempt to both revitalize insurance fraud as a means of revenue generation after the sanctioning of KNIC in 2017, and reassure potential investors in North Korea.

Outlook

Over the course of the last two and a half years, our research on North Korea has provided an unparalleled window into the digital lives of North Korea's most senior leadership. We have tracked and analyzed leadership activity at a unique time in U.S.-DPRK relations, encompassing the duration of the "maximum pressure" campaign, the period of the highest missile launching and testing activity, and the first ever series of summits between an American and North Korean leader.

At its core, this research series has demonstrated how adaptable and innovative North Korea's most senior leadership are. They are quick to embrace new services or technologies when useful and cast them aside when not. The Kim regime has developed a model for using and exploiting the internet that is unique — it is a nation run like a criminal syndicate.

The DPRK has also developed a new, creative, and innovative internet-based model for circumventing sanctions imposed on it by multinational organizations and the West. This model includes generating revenue via both blatant crimes such as bank robbery and fraud, and non-criminal activity such as cryptocurrency mining and freelance IT work.

This model also provides an instrument for acquiring prohibited knowledge and skills, such as those enabling the development of North Korea's nuclear and ballistic missile programs, and enabling cyber operations. At its most basic, North Korea has developed a model that leverages the internet as a mechanism for sanctions circumvention that is distinctive but not exceptional. This model is unique but repeatable, and most concerningly can serve as an example for other financially isolated nations in how to use the internet for sanctions circumvention.

We believe that we will begin to see other isolated nations use some of the same criminal and non-criminal techniques leveraged by North Korea to generate revenue and evade their own sanctions.

For example, over the course of 2019, we assess that Iran has begun to pursue cryptocurrencies as a method for facilitating international payments and circumventing U.S. financial controls. A New York Times article from January indicated that European and Asian business associates were "increasingly cooperative" and supportive of using cryptocurrencies to make payments to Iranian companies; in July, the Iranian government announced a domestic cryptocurrency that would be supported by gold; and in August, Iran legalized cryptocurrency mining as an industry.

Network Defense Recommendations

Recorded Future recommends that organizations conduct the following measures when identifying potential North Korean activity on their networks:

- Configure your intrusion detection systems (IDS) and intrusion prevention systems (IPS) to alert on, and upon review, consider blocking connection attempts from the following prominent North Korean IP ranges:
    - 175.45.176.0/22
    - 210.52.109.0/24
    - 77.94.35.0/24
- More specifically, to detect and prevent North Korean cryptocurrency mining efforts, consider configuring your intrusion detection systems (IDS) and intrusion prevention systems (IPS) to alert on, and upon review, block illicit connection attempts from the following prominent North Korean IP ranges connecting to your network over TCP ports:
    - 8332 and 8333 for Bitcoin
    - 18080 and 18081 for Monero
    - 9332 and 9333 for Litecoin

Note: The aforementioned ports are the default ports configured for the given cryptocurrencies. It is plausible for cryptocurrency mining software to have been modified to override the default ports. Furthermore, other services may also be configured to operate on the listed ports based on your enterprise configuration, and therefore, IDS and/or IPS alerting of network traffic on the listed ports may yield false positives.

- DNS tunneling can be detected by examining network traffic logs or packet captures. High throughput DNS tunneling, which is what we have identified in this case with North Korean users, can be detected because it typically causes significant changes to DNS traffic "with regards to: (1) volume, (2) message length, and (3) shorter mean time between messages."

- For general DNS security:
    - Use a DNS firewall or filter, such as DNS Response Policy Zones (RPZ), with a DNS intelligence feed.
    - Log all DNS requests and connections and retain logs to enable future investigations.
    - Use DNSSEC if possible.

- To defend against a potential CLDAP DDoS attack:
    - Do not expose CLDAP services to the global internet. This will ensure that these machines are not unwitting participants in a CLDAP DDoS attack.
    - Employ DDoS mitigation services.

- Know your organization's VPN services and protocols and block or carefully scrutinize non-standard VPN traffic.
- Consider implementing a software whitelisting program across the enterprise to counteract the possibility of cryptocurrency mining software being downloaded and operated from within the network.
- Many cryptocurrency miners use Internet Relay Chat (IRC) for coordination. Unless IRC is an application required for your enterprise, consider blocking the default IRC TCP port 6667 via your IDS and IPS to mitigate cryptocurrency mining activity using IRC.
- North Korean operators have commonly leveraged both Flash and Silverlight exploits, particularly in operations targeting financial institutions and South Korea. Recorded Future recommends patching these programs frequently, or mitigating their use generally.

Additionally, we advise organizations to follow the following general information security best practice guidelines:

- Keep all software and applications up to date; in particular, operating systems, antivirus software, and core system utilities.
- Filter email correspondence and scrutinize attachments for malware.
- Make regular backups of your system and store the backups offline, preferably offsite so that data cannot be accessed via the network.
- Have a well-thought-out incident response and communications plan.
- Adhere to strict compartmentalization of company-sensitive data. In particular, look at which data anyone with access to an employee account or device would have access to (for example, through device or account takeover via phishing).
- Strongly consider instituting role-based access, limiting company-wide data access, and restricting access to sensitive data.
- Employ host-based controls; one of the best defenses and warning signals to thwart attacks is to conduct client-based host logging and intrusion detection capabilities.
- Implement basic incident response and detection deployments and controls like network IDS, netflow collection, host logging, and web proxy, alongside human monitoring of detection sources.
- Be aware of partner or supply chain security standards. Being able to monitor and enforce security standards for ecosystem partners is an important part of any organization's security posture.

About Recorded Future

Recorded Future arms security teams with the only complete security intelligence solution 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 in real time and packaged for human analysis or integration with security technologies.