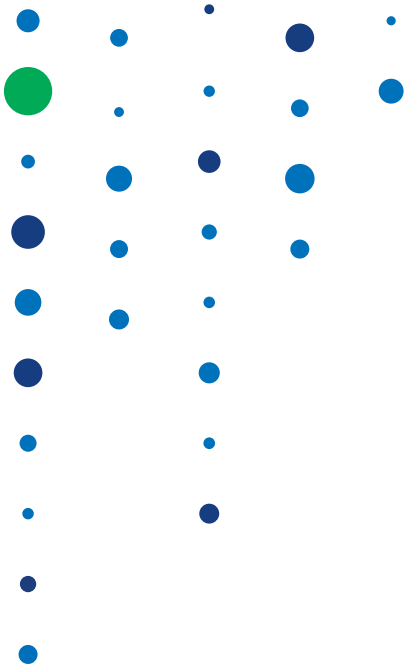
Recorded Future

CYBER THREAT ANALYSIS

North Korea's Ruling Elite Adapt Internet Behavior to Foreign Scrutiny

In-depth analysis of North Korean internet activity reveals the abandonment of Western social media and a dramatic increase in operational security practices.

By Priscilla Moriuchi
Recorded Future



Scope Note: Insikt Group examined North Korea's most senior leadership's internet activity by analyzing third-party data, IP geolocation, Border Gateway Protocol (BGP) routing tables, and open source intelligence (OSINT) using a number of tools. This is a follow-up to our July 2017 analysis, and the data analyzed for this report spans from December 1, 2017 through March 15, 2018.

Executive Summary

In July 2017, Recorded Future published research on the internet browsing behavior of North Korea's most trusted leaders, or the North's ".1 percent." While conducting that research, we discovered that North Korea's ruling elite were plugged into contemporary internet society, were technologically savvy, and had patterns of internet use that were very similar to users in the West.

In December, we decided to revisit the analysis and discovered substantive changes in how North Korea's ruling elite utilize the internet. In particular, North Korean leadership nearly totally abandoned Western social media and significantly increased their operational security procedures in the six months since our original analysis.

It is likely that this dramatic change in behavior is the result of any one, or a combination of, the following: 1) increasing foreign research into and attention to North Koreans' media consumption, 2) new enforcement of the official ban on these Western social media services which has been in place since April 2016, or 3) increased operational security by the North Korean elite.

Key Judgments

- North Korean elites migrated almost completely from Western social media and services to their Chinese equivalents — Alibaba, Tencent, and Baidu.
- Over the course of six months, North Korean elite increased their use of internet obfuscation services by 1,200 percent. This includes a dramatic increase in services such as Virtual Private Networks (VPN), Virtual Private Servers (VPS), Transport Layer Security (TLS), and The Onion Router (Tor).
- We discovered two additional nations, Thailand and Bangladesh, where heuristic[1] analysis identified North Koreans were likely living and conducting illicit revenue-generation activities. This is in addition to eight nations we discovered in 2017, including India, Malaysia, New Zealand, Nepal, Kenya, Mozambique, Indonesia and China.
- North Korea continued to mine Bitcoin, and in late January began to mine Monero as well.

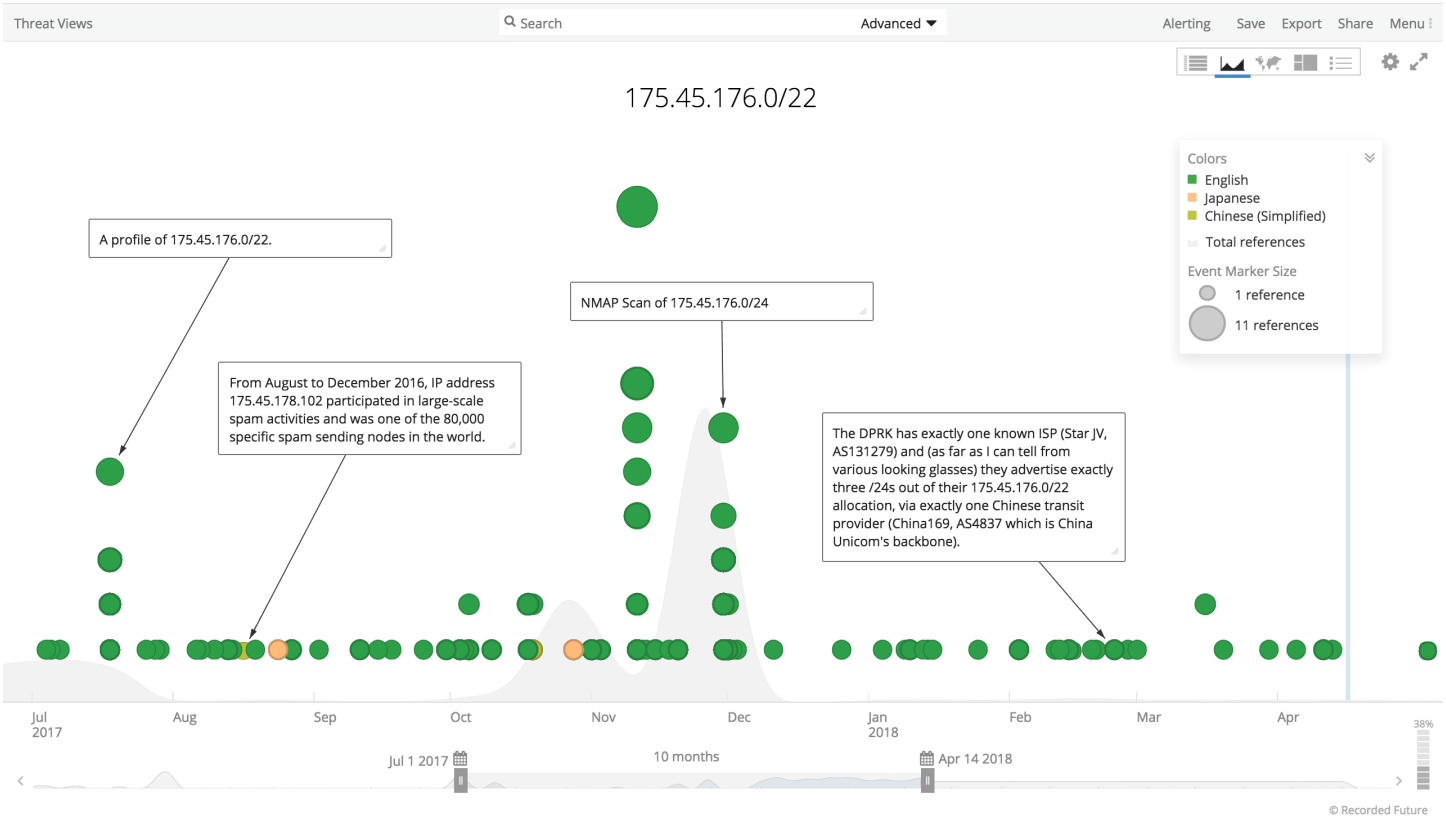
[1] *Heuristic analysis refers to a problem-solving approach that leverages methodical approximation to derive an analytical outcome based on the application of several criteria on the underlying data. In this case, it is the result of in-depth analysis of a large dataset combined with an intimate knowledge of the likely operating environment of North Korean nationals based in foreign countries.*

Background

As we detailed back in July, 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: a trusted member or family member of the ruling class.

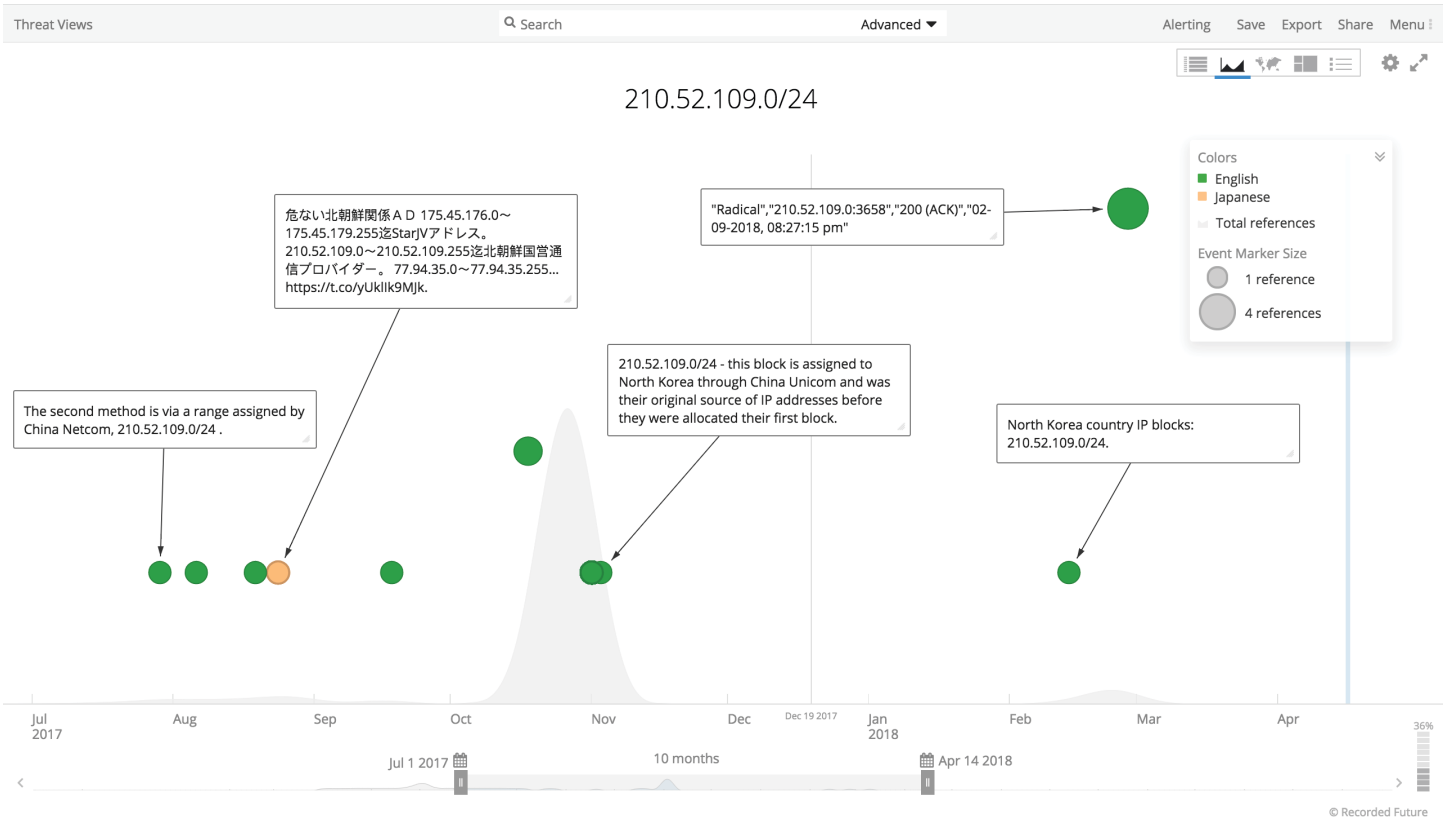
There are three primary ways North Korean elites access the global internet. Like with any internet-connected networks, there are occasionally reports of malicious activity from these ranges. However, the majority of North Korean malicious cyber operations are likely conducted from overseas (more on this in the "Presence in Foreign Countries" section below).

The first method 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.



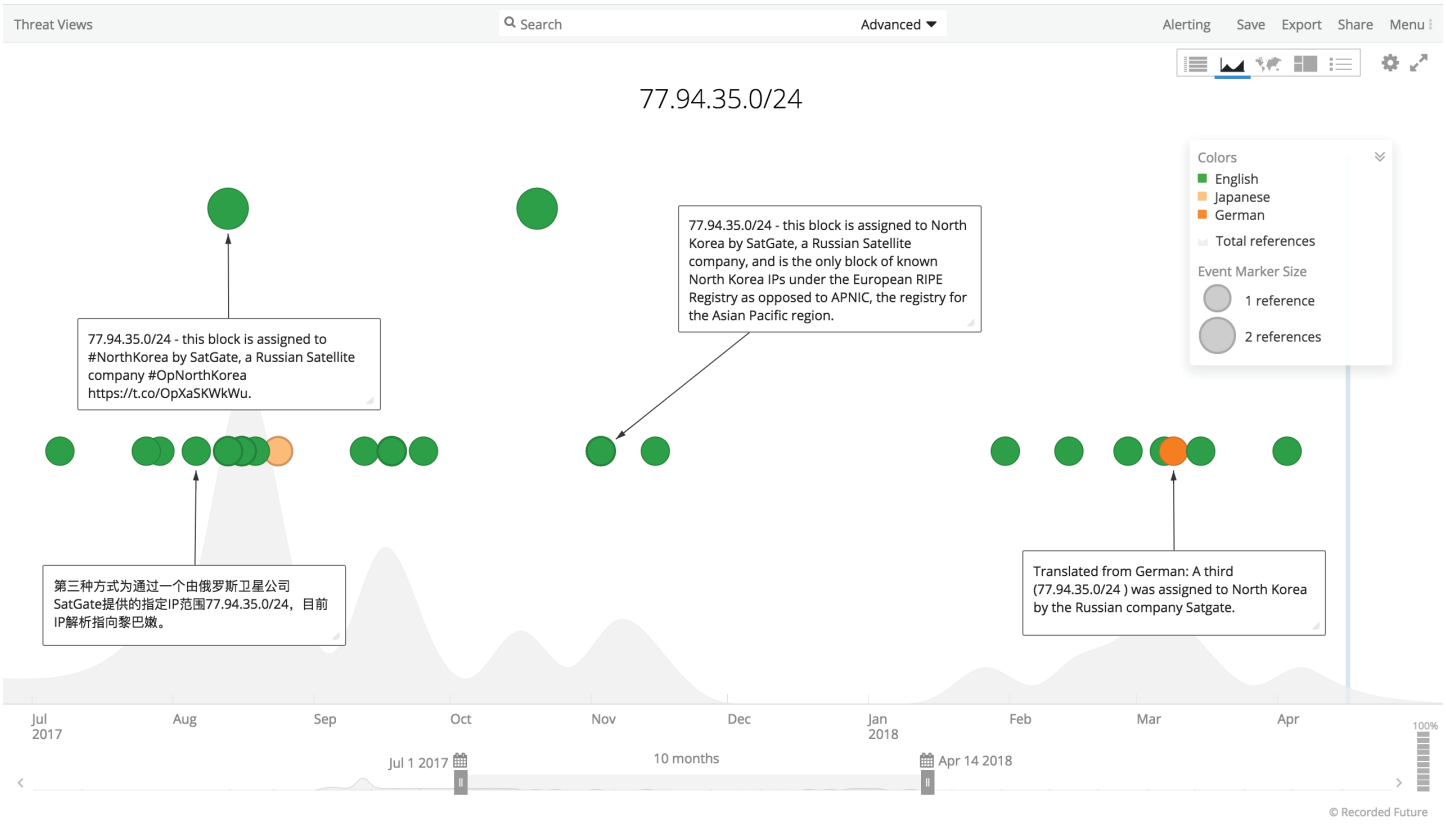
Timeline of events involving 175.45.176.0/22 range from July 2017 through April 2018.

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.



Timeline of events involving 210.52.109.0/24 range from July 2017 through April 2018.

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.



Timeline of events involving 77.94.35.0/24 range from July 2017 through April 2018.

Editor's Note

From this point on, when we refer to "North Korean internet activity" or "behavior," we are referring to the use of the global internet, not the North Korean domestic intranet, Kwangmyong, for which only select few leaders and ruling elite 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.

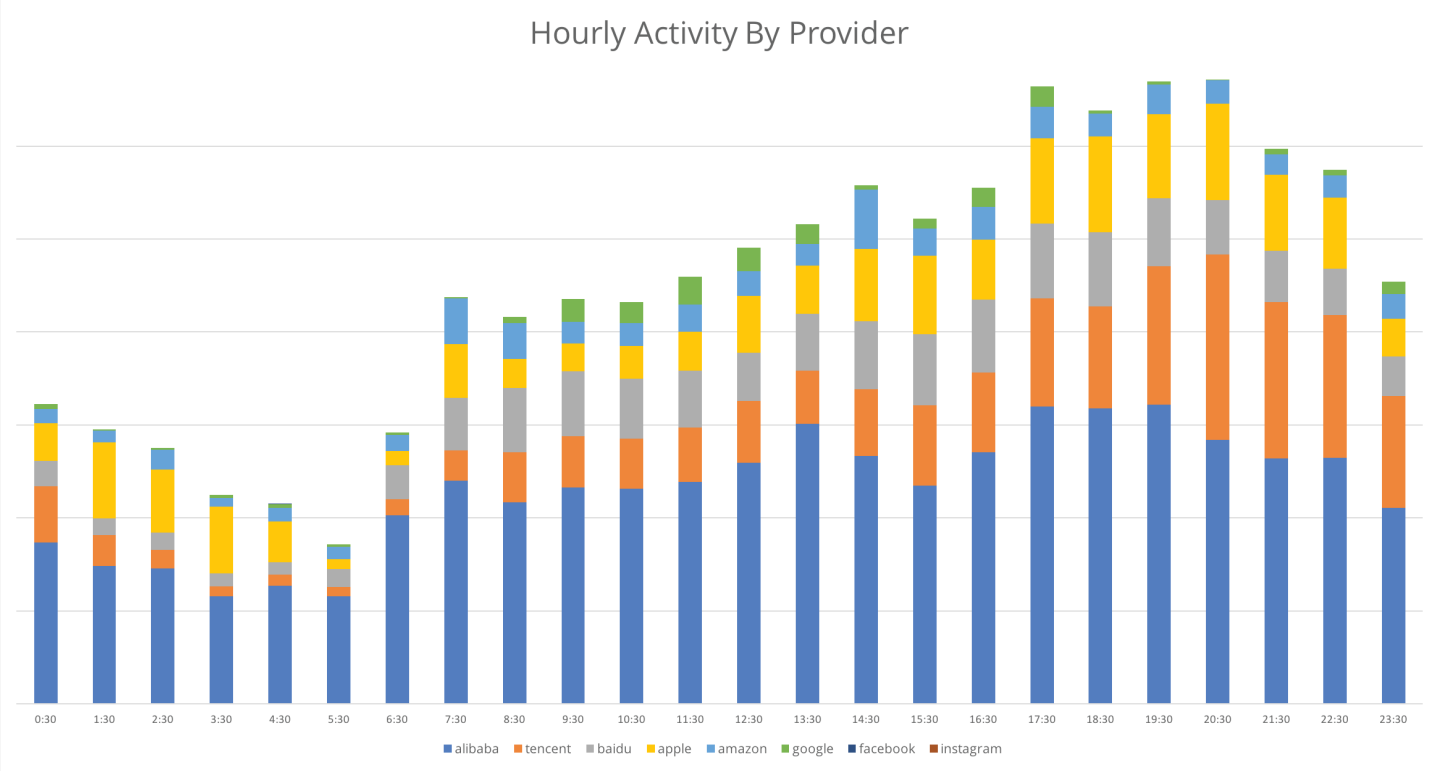
Additionally, we chose this date range, December 1, 2017 through March 15, 2018, because it represented a period of transition and intensified intra-Korean dialogue in advance of the February 2018 Winter Olympics in South Korea.

Analysis

Similar to international users of the global internet, North Korean elite internet activity is largely comprised of internet video, online gaming, and web browsing. A Cisco analysis revealed that 77 percent of global internet traffic in 2017 consisted of internet video and online gaming. For North Korean users, 70 percent of activity consisted of internet video or online gaming; 17 percent consisted of web browsing, checking email, and data downloads; and 13 percent was in a Virtual Private Network (VPN), or otherwise obfuscated.

Change in Social Media Consumption

North Korean leadership spent roughly the same amount of time on social media, shopping, and search sites for December through March as they did last summer. However, the services they utilized changed dramatically.



Hourly activity on eight social networking, shopping, and search sites for December 1, 2017 through March 15, 2018 (actual). Providers are listed by popularity, from Alibaba (highest) to Instagram (lowest).

In July, our data demonstrated that North Korean leadership heavily consumed Western social media, especially Facebook, Google, and Instagram. In fact, Facebook was by far the most popular service, with more than double the daily actual usage than any of its Chinese-language counterparts.

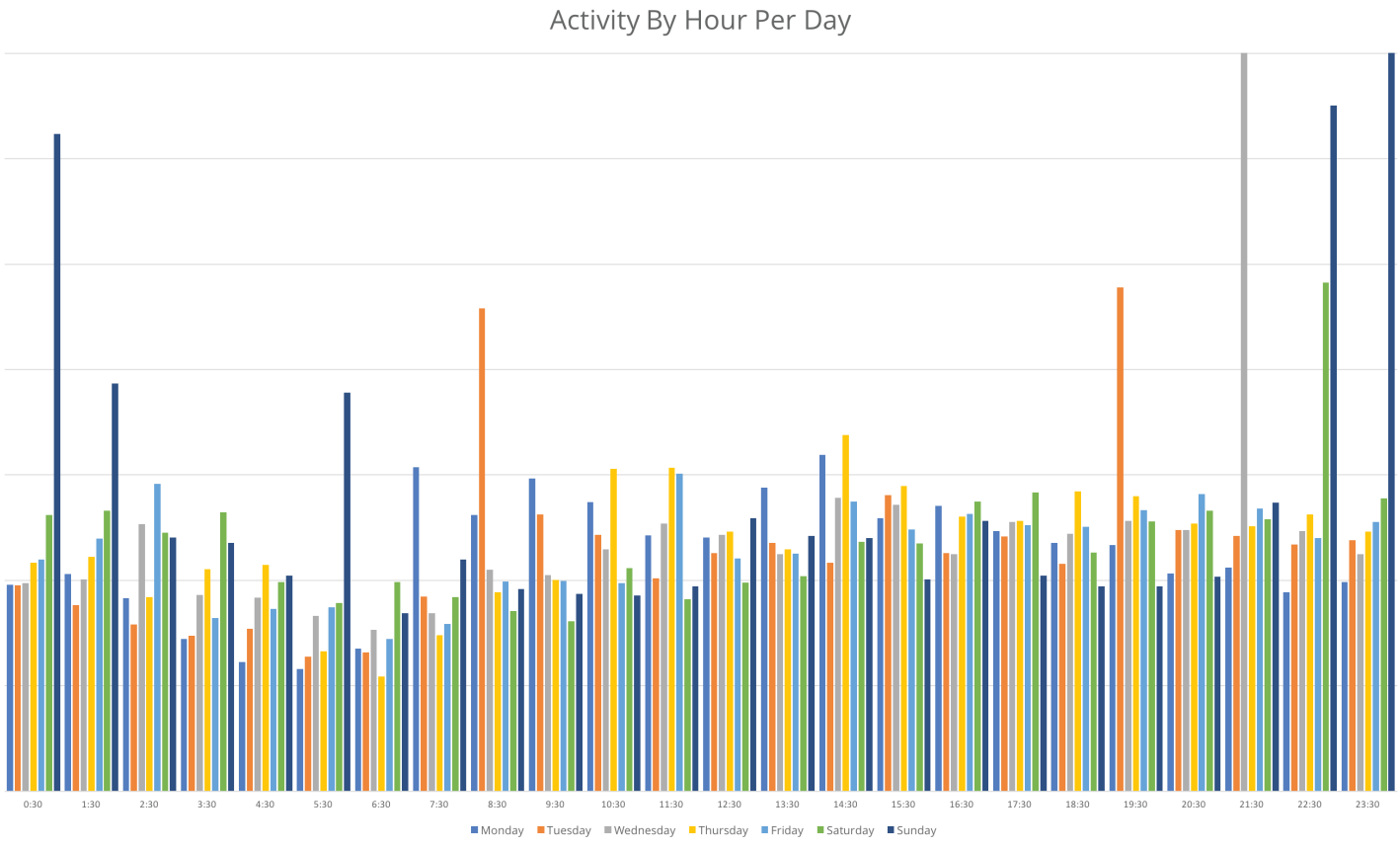
What is most striking about the social media activity from the December 2017 through March 2018 dataset is the near absence of Facebook and Instagram activity, and the significant increase in use of Chinese services. Facebook and Instagram activity are so low that they are not visible on the chart above.

In six short months, North Korean elites migrated almost completely from Western social media and services to Alibaba, Tencent, and Baidu. The remaining Western services in the top eight were utilized primarily for content streaming and not social networking.

This change in behavior could be the result of increasing foreign research into and attention to North Koreans' media consumption, new enforcement of the official ban on these Western social media services which has been in place since April 2016, or increased operational security by North Korean elite.

Pattern of Life

North Korean leaders have distinct patterns of daily usage over this period that are similar to the summer of 2017. Generally, the times of highest activity are still from approximately 9:00 AM through 8:00 PM or 9:00 PM, with Saturdays and Sundays being the days of consistently highest activity. The peaks of activity on late Saturday nights and early Sunday mornings consisted mainly of content streaming or online gaming, suggesting that North Korean elite are allowed leisure time on the weekends.



Daily internet usage by hour (not an average).

Gaming as a For-Profit Enterprise

A series 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 primarily of operators and programmers living in facilities overseas, tasked with the overarching goal of generating revenue for the Kim regime.

This operational model of sending North Koreans overseas to 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. Defectors have detailed the degree to which counterfeiting and scamming video and online games and 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 percent 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.

The list below represents a wider usage of online games by North Korean elite since July 2017 and could give researchers leads on which games overseas North Korean hackers are exploiting to generate revenue for the regime. It is not clear how much of this type of revenue generation is conducted from territorial North Korea. However, it is clear that overseas operators would often develop bots or gaming hacks for platforms and services they were already familiar with.

- 0AD: Empires Ascendant
- Ace of Spades
- Quake
- The Marathon trilogy games
- Armed Assault 1-3
- World of Warcraft
- Cube 2: Sauerbraten
- Diablo 2
- League of Legends
- Second Life
- Accounts and games on Steam

North Korean elite also utilize a number of gaming consoles or systems, including Nintendo and PlayStation, as well as game storage and account providers like Steam and Blizzard.

Presence in Foreign Countries

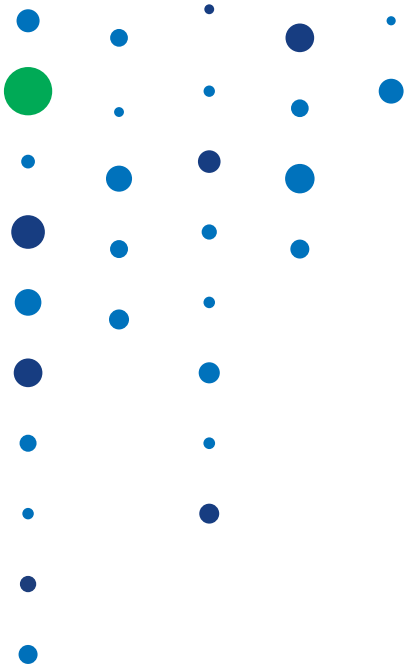
In our July research, we developed a heuristic to identify significant physical and virtual North Korean presences in nations around the world. That heuristic included above-average levels of North Korean internet activity to and from these nations, but also browsing and use of many local resources, such as news outlets, district or municipal governments, local educational institutions, and more.

This technique enabled us to identify eight nations where North Koreans were physically living or located, including India, Malaysia, New Zealand, Nepal, Kenya, Mozambique, Indonesia, and China. For this December through March dataset, we reexamined the data for those eight countries and included examples of countries that did not fit the pattern in order to provide greater fidelity on the analytic conclusions.

Top export destinations for North Korea in 2015 (data courtesy of MIT Observatory of Economic Complexity). China, India, Indonesia, Thailand, Bangladesh, Nepal (as part of "Other Asia"), and Mozambique fall within this list of top export destinations.

Among the eight identified last summer, only Malaysia and New Zealand no longer fit the behavioral heuristic, but in slightly different ways.

For New Zealand, while the volume of traffic remained relatively steady, the activity no longer exhibited the second half of the heuristic (local resources and more) and instead appeared to be primarily a hub for North Korean bittorrent, video streaming, and gaming services. Over a three-day period in early January, a New Zealand Defence Forces IP attempted to repeatedly connect with North Korean networks. The activity was repetitive and noisy, but was not at the level where it would have caused a disruption of North Korean internet services.



It is possible that New Zealand countered some North Korean operational activity through actions it undertook in August 2017 to deny visas to North Korean academics and its support for United Nations and United States sanctions regimes.

For Malaysia, the volume of traffic dropped significantly, but there are clearly some North Koreans in Malaysia. For example, we see repeated checking of North Korean official email accounts from Kuala Lumpur, however, the breadth of the localized North Korean activity is much narrower than last summer.

Malaysia-North Korea relations have degraded significantly since last summer, and in the wake of the Kim Jong-nam assassination. Malaysia recalled its ambassador in Pyongyang, imposed restrictions on North Korean guest workers, businesses, and flights, imposed a travel ban, and may require North Korea to reduce the size of its mission in Kuala Lumpur.

In addition to the remaining six nations — India, Nepal, Kenya, Mozambique, Indonesia, and China — internet activity involving two other nations emerged as fitting the behavioral signature: Thailand and Bangladesh.[2] We assess that these eight nations wittingly or unwittingly host North Koreans. These North Koreans are likely conducting illicit revenue-generation activities with the intent of circumventing international sanctions or obtaining advanced education, with the goal of progressing the North's nuclear weapons and cyber operations programs.

In part one of our research on North Korea's strategic motivations for conducting cyber operations, we detailed some of the extensive overseas criminal operations that the Kim regime runs to obtain funding for the country's missile and nuclear development programs.

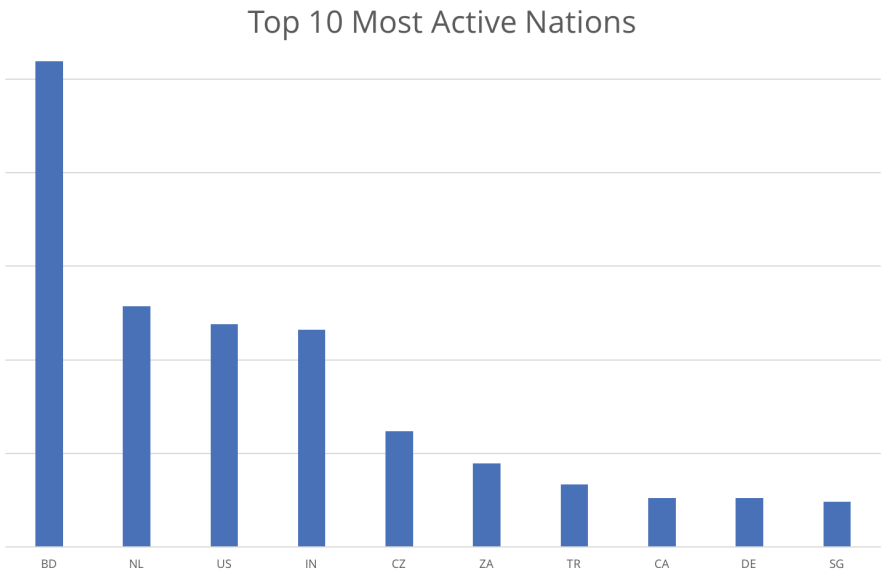
North Korea's illicit revenue-generating networks have been extensively studied by researchers, reporters, and academics. These studies, and numerous more, detail how North Korea uses its overseas diplomatic establishments, state-run restaurant chain, and citizens living abroad to facilitate illicit revenue generation and nuclear and cyber operations training.

Thailand and Bangladesh host North Korean state-run restaurants, diplomatic establishments tied to criminal activity, and allow North Korean investment. The digital signature that we developed and applied is simply one more data point in raising our confidence in including these two nations on this list.

[2] *Eight is not a magic number — it just seems to be the number of countries where the behavior fits the signature.*

High Volume But No Signature Match

There are several countries that exhibited high volumes of activity with North Korean ranges but did not meet the second, or local, half of the heuristic. Particularly among the top 10 nations, the majority of these nations were simply utilized by North Korean users for video streaming, content delivery, or VPN/VPS services.



Top 10 nations with the most internet activity to or from North Korea (actual numbers).

Interestingly, Alibaba's video streaming and content delivery networks seem to be routing North Korean-originated traffic through U.S. servers, which was the major driver of U.S.-based activity. In the case of the Netherlands and Germany, infrastructure in both nations was utilized heavily to obfuscate activity, primarily through VPN or VPS services and Tor exit nodes.

This is in stark contrast to last summer, when less than one percent of all North Korean internet activity was obscured or concealed in any way. The drivers for this move to European providers is not clear, however, we assess it could be driven by the implementation of the GDPR and the European focus on individual internet privacy.

Cryptocurrency Activity

Since our initial reports that North Korea had been mining Bitcoin since at least May 2017, the North's interest in and exploitation of cryptocurrencies has exploded. In 2017, North Korea committed numerous thefts from South Korean cryptocurrency exchanges, was linked to the May WannaCry attack, and has begun to mine Monero.

In this new dataset, we see an expanded interest in cryptocurrencies by North Korean elites and a continuation of the Bitcoin mining. While our data does not give us insight into the full scope of North Korea's Bitcoin activity, we saw a continuation of the mining activity we observed in May from January 24 through the end of this dataset on March 15. The traffic volume and rate of communication with peers was the same as last summer, but we were still unable to determine hash rate or build. This mining effort appears small-scale and limited to just a few machines, similar to the activity from last summer.

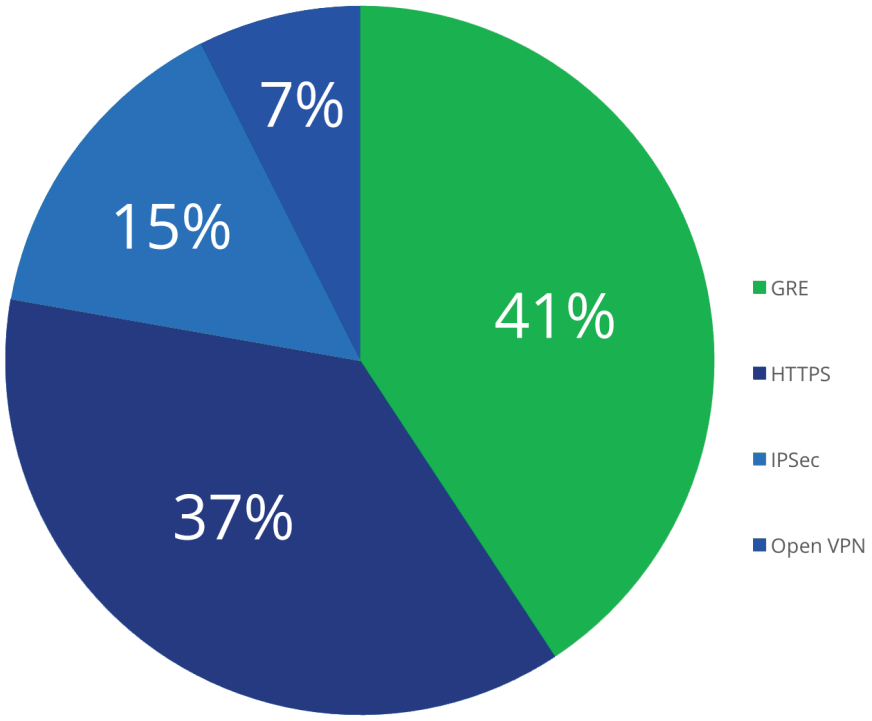
We also saw a likely separate user utilizing the Bitcoind interface, which allows for local or remote control and integration with other software, or in larger payment systems. This is a strong indicator that North Korean users are conducting Bitcoin transactions, but we cannot confirm what was purchased, the associated wallets, or how many coins the user possesed.

On top of the Bitcoin activity detailed above, beginning on January 29, we observed Monero mining from North Korean networks. This activity continued through the end of our dataset on March 15. Monero mining is similar to Bitcoin mining in that it utilizes the same "proof-of-work" method where one must discover the hash which matches a certain target value.

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 lower capacity 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. In this case, we observed the mining over port 7777, which suggests a higher-capacity machine was conducting the mining, and also 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.

Obfuscated Activity

A much higher percentage — nearly 13 percent — of leadership internet activity was obfuscated in some way for this time period, as opposed to the less than one percent of activity last summer. From April through July 2017, less than one percent of all North Korean internet activity was obfuscated. Over the course of approximately six months, North Korean leadership significantly changed the manner in which they browse, search, and retrieve web content.



North Korean leadership use of obfuscation services by percentage of total.

Point-to-Point Tunneling Protocol (PPTP) was the most widely utilized obfuscation service, followed by probably HTTPS (via port 443), or secured browsing, and the IPSec VPN.

From April through July 2017, North Korean leadership obfuscated less than one percent of all of their internet activity — this included TLS-enabled browsing, the use of VPN or VPS, and other tunneling protocols, or even the use of Tor. By December, North Korean users had fundamentally altered their browsing behavior, increasing their use of obfuscation services twelvefold.

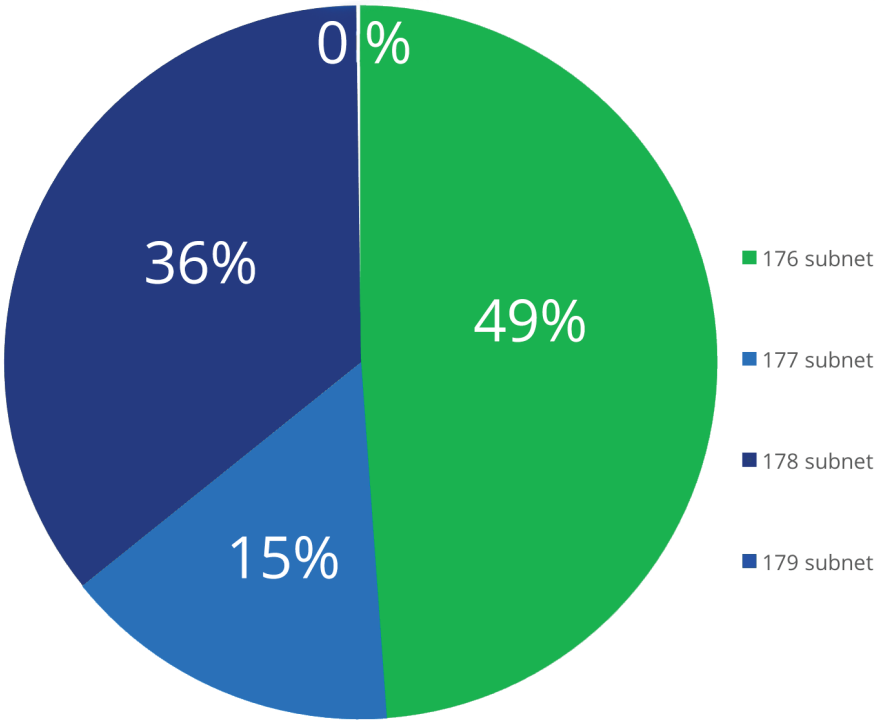
Given that 70 percent of North Korean internet activity consists of internet video or online gaming, 13 percent is a substantial portion of the remaining web traffic, which narrows our optic into leadership activities even further.

Network Analysis

On October 1, 2017, researchers observed that a Russian telecommunications company, Trans TeleCom (AS 20485), began appearing in the internet routing databases for North Korea's primary IP range, 175.45.176.0/22. Prior to October 2017, North Korea's principle connection to the global internet had been provided by Chinese telecommunications company, China Unicom (AS4837).

At varying times on October 1, three of the four subnets of 175.45.176.0/22 (175.45.176.0/24, 175.45.177.0/24, 175.45.178.0/24, and 175.45.179.0/24) were routed by Trans Telecom until the connection stabilized and then only the 175.45.178.0/24 subnet remained transiting over the Trans Telecom infrastructure, with the other three utilizing China Unicom.

From December 2017 through March 15, 2018, only the 175.45.178.0/24 subnet was ever routed through Trans Telecom, while the other three remained transiting China Unicom infrastructure. Although the Trans Telecom route has given North Korea an alternate internet access point, it seems to only be utilized for about one third of North Korea's overall internet activity.



Usage of each subnet within the primary range of 175.45.176.0/24 by percentage of total traffic.

The 176 subnet generates the most activity because it hosts the vast majority of North Korea's publicly accessible websites. Additionally, this subnet is also composed of a number of shared servers that both host websites and route outgoing traffic, as well as proxies and load balancers. For example, our analysis indicates that North Korea utilizes an F5 BIG-IP load balancer to distribute outgoing traffic through at least eight IP addresses in this subnet. Load balancers manage ingoing and outgoing internet traffic and distribute it to a specific range of servers to increase capacity and network reliability for concurrent users.

For many who have attempted to access any of the North Korean-hosted websites, this may sound surprising because the sites are notoriously slow to load and often require several attempts before content is presented. Our analysis indicates that this load balancing is utilized primarily for the shared servers, and its performance is likely degraded by both a lack of a redundant system and the stress on the limited bandwidth due to the amount of video streaming and online gaming.

This means that there are likely more physical computers behind each of these IP addresses, although exactly how many there are is not known. The volume of internet activity we observed to and from North Korean IP ranges is quite small, especially for a national network. Because such a small percentage of the population has access to the global internet, the number of computers behind these subnets is likely to be closer to the equivalent of a medium-sized corporation than a nation with an equivalent population (approximately 25 million).

For the 210.52.109.0/24 range, routing tables confirm that the access point is managed by China Netcom, under AS9929. Routing data also notes that at least half of the time, data from this range is also routed via an Autonomous System Number (AS or ASN) assigned to Sprint, AS1239. It is not clear if this path actually traverses physical infrastructure in the United States or if it is the result of a joint AS membership.

In October 2017, security researchers at an antivirus company conducted a survey of this 175.45.176.0/22 range and speculated that certain IP addresses are assigned to foreign visitors and used specifically for their internet access. This was based on seeing "web traffic" coming from thirteen IP addresses in the 175.45.178.0/24 subnet.

Our analysis indicates that "web traffic" from North Korean IP addresses is insufficient to determine use by foreigners — otherwise, this entire /22 range could be assessed as assigned to foreign visitors. We did see internet browsing, video streaming, online gaming, VPN use, and other types of traffic from the thirteen IP addresses identified. This traffic comprised less than .5 percent of our total observed traffic and we eliminated it from our overall analysis because it was statistically insignificant.

Outlook

Back in July, we argued that our research revealed how connected to modern internet society North Korea's ruling elite actually were, and that international sanctions had been ineffective at isolating North Korea from the outside world. Further, we stated that new tools and relationships were needed to affect a lasting negative impact on the Kim regime.

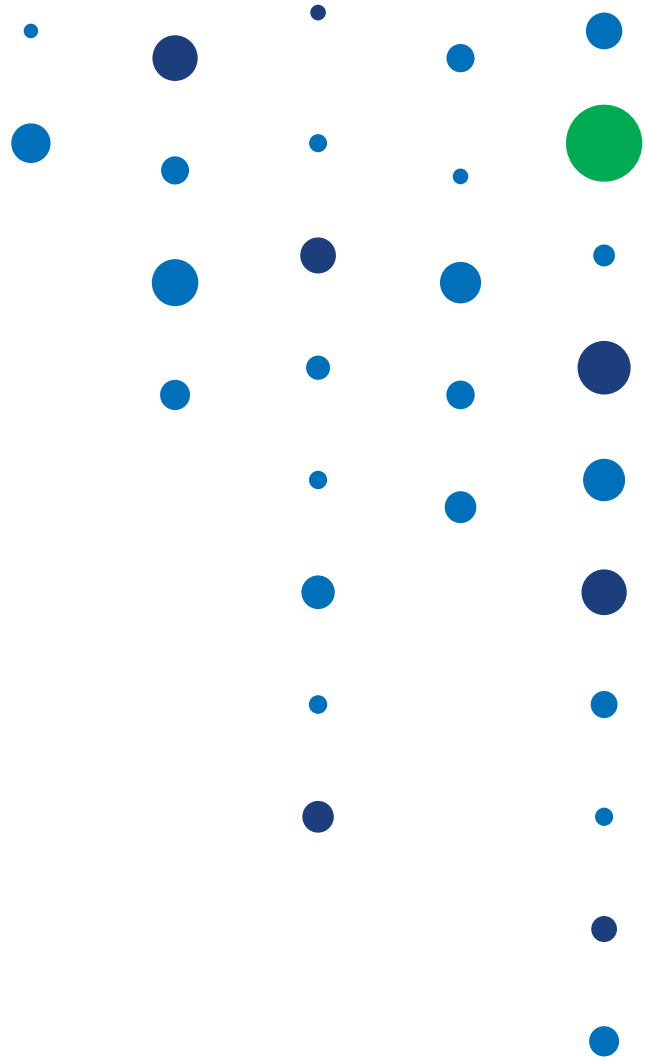
In the months since that initial report, we have noticed substantive changes in both how North Korean elite utilize the internet, but also in the diversity of international participation in sanctions and pressure on the Kim regime. In less than half a year, North Korean leadership has fundamentally changed the internet services they use and their behavior online to increase anonymity. They have pursued cryptocurrencies as a means of circumventing sanctions and attempted to steal funds from financial institutions worldwide.

North Korean elite internet users are adapting to their changing digital environment as physical sanctions continue to tighten, and coalitions of nations cut off activity with the Kim regime. However, our July assessment that new tools that do not focus on territorial North Korea are needed to achieve a lasting negative impact on the current Kim regime still holds. The United Nations Panel of Experts on North Korea continues to focus narrowly on cyber-enabled theft of military secrets, and U.S. sanctions have yet to address cyber operations.

The breadth of North Korea's embrace of the internet, from leadership browsing, to revenue generation, to tactical cyber operations, indicates how indispensable this medium is to the Kim regime. International efforts to restrict the activities and operational scope of this rogue nation must include sanctions or punitive measures on North Korean cyber operations.

For cybersecurity professionals and network defenders, this change in leadership internet behavior continues to underscore just how complex defending against malicious North Korean cyber activity can be. We continue to recommend that financial services firms, banks, cryptocurrency exchanges, users, those supporting U.S. and South Korean military THAAD deployment, and on-peninsula operations maintain the highest vigilance and awareness of the heightened threat environment to their networks.

Similarly, energy and media companies, particularly those located in or that support these sectors in South Korea, should be on 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 the only complete threat 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.