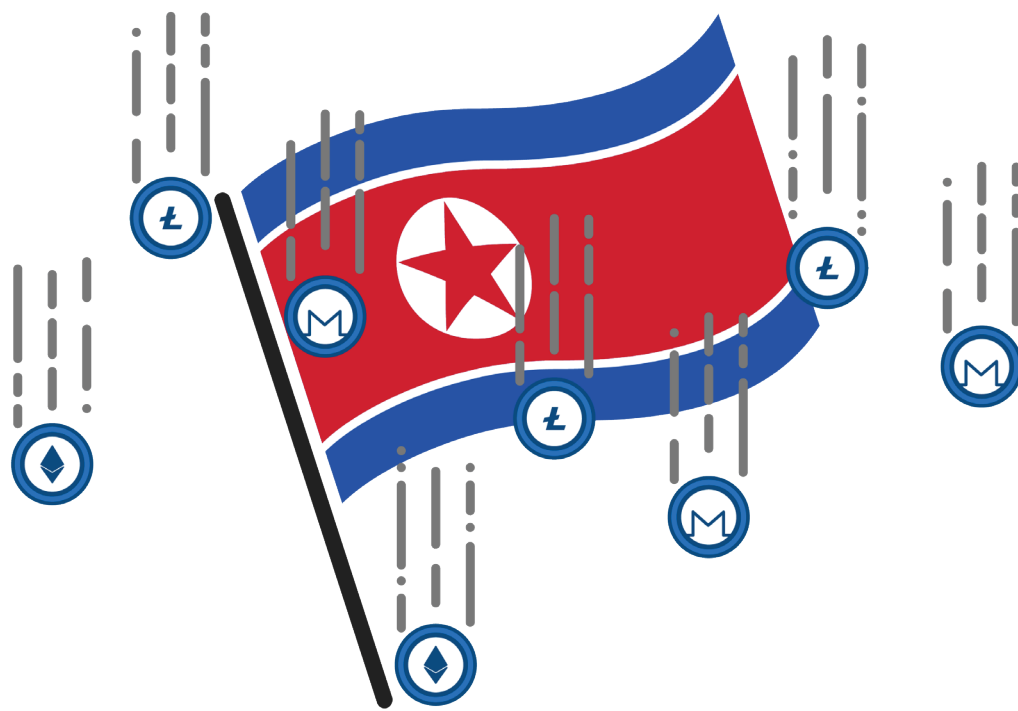


Shifting Patterns in Internet Use Reveal Adaptable and Innovative North Korean Ruling Elite

By Insikt Group
Recorded Future



Scope Note: Insikt Group examined North Korean 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. The data analyzed for this report spans from March 16, 2018 through August 30, 2018.

This report will be of greatest 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 course of the past year and a half, Recorded Future has published a series of research pieces revealing unique insight into the behavior of North Korea's most senior leadership. We discovered that [North Korea's ruling elite are technologically savvy, use a full range of older and cutting-edge computers, phones, and devices, use the internet as a tool for sanctions circumvention, and recently shifted to embrace Chinese social networking services over Western ones.](#)

In this final piece in our series, we explore the persistence of trends in internet security, social media use, and cryptocurrency, and reveal greater insight into the way North Korea uses the internet to generate revenue for the Kim regime. In particular, shifting patterns in the ruling elite's internet usage reveal just how adaptable and innovative North Korea's most senior leadership are. The Kim regime has developed a model for using and exploiting the internet that is unique, and leadership are quick to embrace new services or technologies when useful and cast them aside when not.

Key Judgments

- Pattern-of-life and content shifts indicate that the internet is probably becoming a more regular professional tool for North Korea's most senior leadership. As senior leadership become more internet savvy and professionalize their use of the internet, it will exacerbate existing challenges in sanctions enforcement and computer network defense.

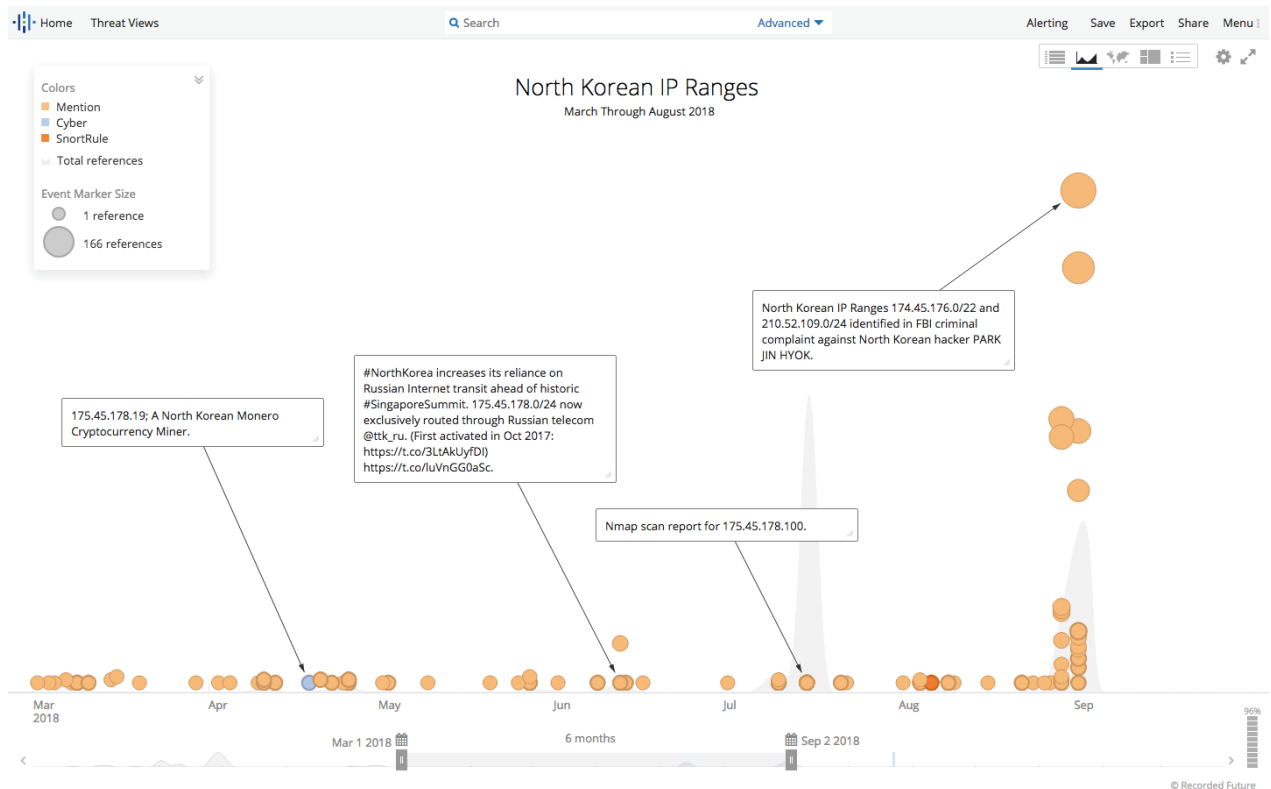
- North Korean senior leaders exhibit significantly greater operational security today than in early 2017. This awareness combined with the increasing global use of large domain hosting and internet infrastructure providers has over time negatively impacted our visibility into the daily internet activities of North Korea's ruling elite.
- Using behavioral heuristic, we identified several nations that are likely to be hosting North Korean workers who are employed in the service or information economy as opposed to purely manual laborers. These countries include China, India, Nepal, Bangladesh, Mozambique, Kenya, Thailand, and Indonesia.
- We have discovered an asset-backed cryptocurrency scam called Marine Chain operated by a network of North Korea enablers in Singapore, and at least one other scam coin, called Interstellar, Stellar, or HOLD (recently rebranded as HUZU after a swap), also possibly tied to North Korea.
- The migration away from Western social media and services we observed in early 2018 has persisted, with the exception of LinkedIn. We observed low-volume but regular and consistent use of LinkedIn by North Korean leaders beginning in April 2018. We were not able to identify any individual LinkedIn users.

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 trusted member or family 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 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.



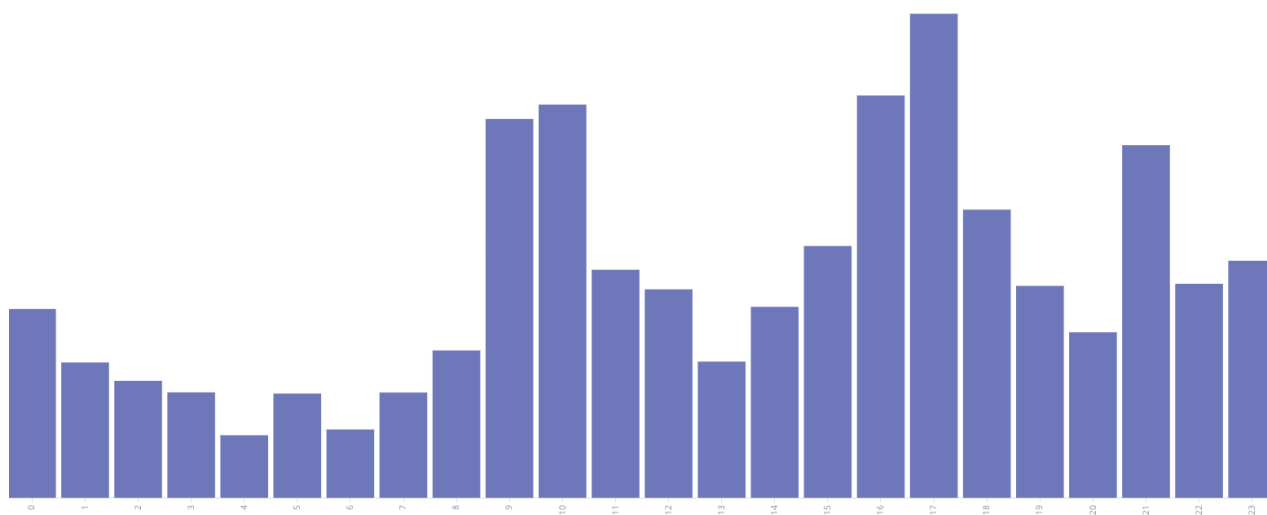
Timeline of events involving North Korea's IP ranges from March through August 2018.

Additionally, as we identified [back in April](#), the 175.45.176.0/22 range is routed by both China Unicom ([AS4837](#)) and Russia's TransTelekom ([AS20485](#)). Of the four subnets of this range (175.45.176.0/24, 175.45.177.0/24, 175.45.178.0/24, and 175.45.179.0/24), we continued to observe only the 175.45.178.0/24 being routed through TransTelekom; the other three were exclusively routed by China Unicom.

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, 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 privileged North Koreans who are permitted access to Kwangmyong, or diplomatic and foreign establishments that are located in North Korea.

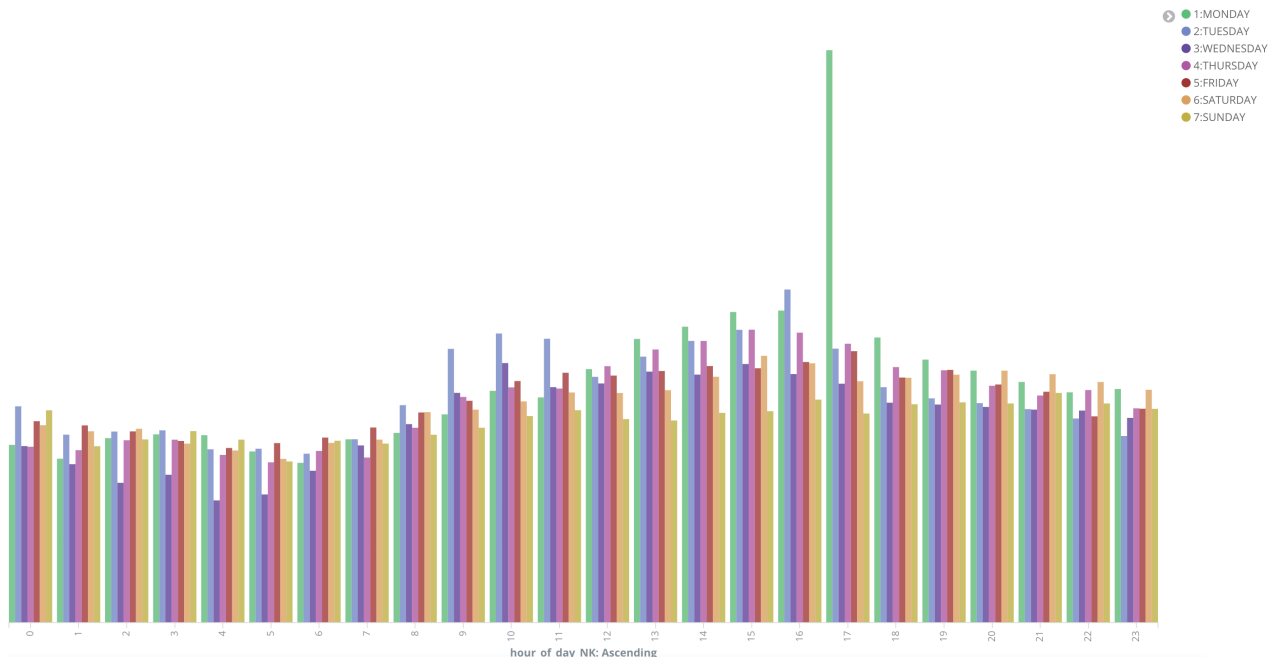
Internet Usage Consistent — Pattern Shifts Since April 2017

North Korean leaders’ distinct patterns of daily internet usage have remained consistent since April 2017. Generally, the times of highest activity are from approximately 8:00 AM through 8:00 PM or 9:00 PM.



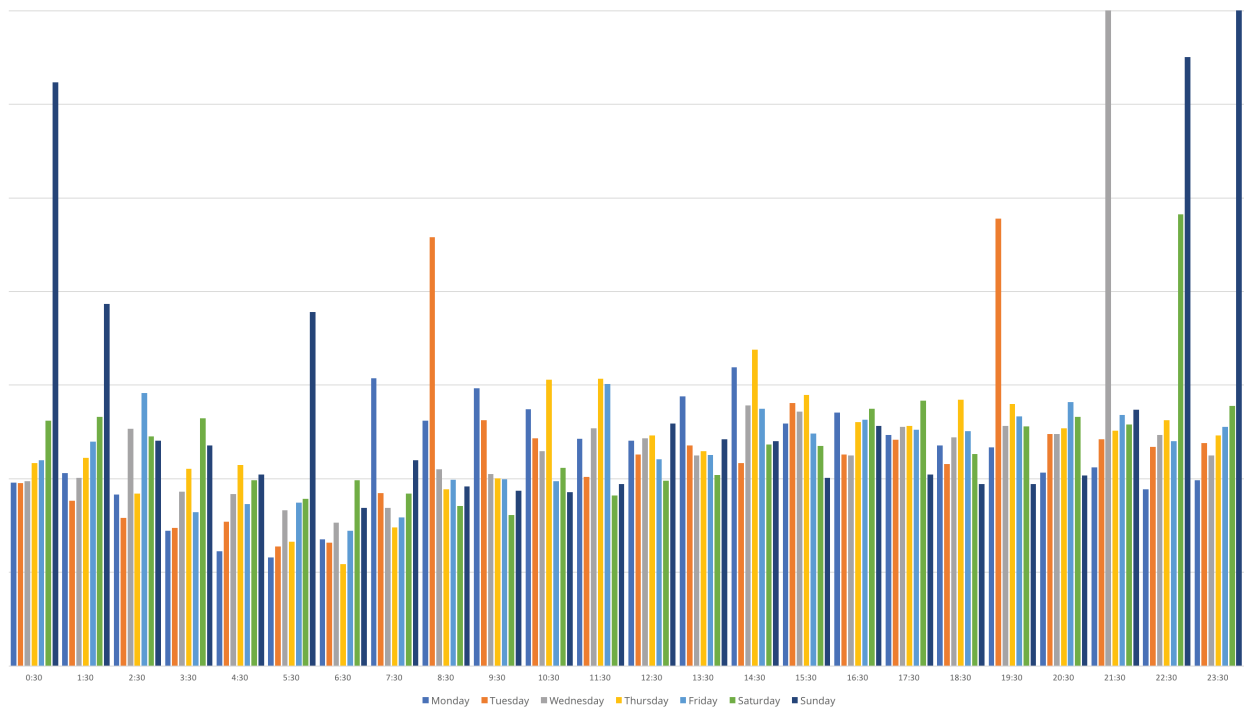
Daily internet usage by hour (not an average) from March through August 2018.

However, the days of peak activity have shifted over time. In 2017, Saturdays and Sundays were consistently the days with the highest activity. In particular, Saturday nights and early Sunday mornings had peaks that consisted primarily of online gaming or content streaming. Over the course of 2018, the pattern has shifted, and internet use on traditional workdays (Monday through Friday) has increased while weekend usage has decreased. On Saturdays and Sundays, content streaming and gaming still remains dominant; however, it represents a smaller portion of the overall weekly internet use than we observed last year.



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

Activity By Hour Per Day



Daily internet usage by hour (not an average) from pre-March 2018.

While the drivers of this shift are unknown, this adjustment over time indicates that internet use has become a greater part of North Korean leaders' workday. In August 2018, North Korea completed external construction of its new [Internet Communication Bureau headquarters](#), located in Pyongyang. According to [North Korea Tech](#), the purpose of the new headquarters is not clear, but it may be focused on access to the global internet.

It appears the new building plays a part in facilitating Pyongyang's connection to the greater global internet, but its exact role hasn't been reported. It could perhaps be meant to hold servers that provide the handful of sites that Pyongyang has on the web, or as a gateway center to monitor and help control all traffic flowing between North Korea and the rest of the world.

It is possible that this shift in usage patterns combined with the completion of the Internet Communication Bureau headquarters could signify a professionalization of internet use across North Korea's most senior leadership. This would mean that these leaders utilize the internet to a greater extent as part of their jobs, as opposed to for their own entertainment.

Operational Security Behavior Moderates

In our April analysis, we noticed two dramatic behavioral trends among North Korean internet users. First was the marked increase in the use of operational security techniques, such as Virtual Private Networks (VPN), Virtual Private Servers (VPS), Transport Layer Security (TLS), and The Onion Router (Tor). In April, we identified a 1,200 percent increase in the use of these services by North Korean leaders, which marked a significant departure from their previous behavior in conducting primarily unprotected internet activity.

Since then, that spike in operational security measures has moderated. In early 2018, obfuscated browsing accounted for 13 percent of all North Korean leadership internet activity. By September 2018, that percentage declined to just over five percent. Previously, the use of VPN technologies accounted for 63 percent of obfuscated internet activity. Over the subsequent six months, VPN use among North Korean leadership declined to just 50 percent of obfuscated activity. The use of HTTPS (via port 443), or secured browsing, increased to 49 percent of operationally secure browsing. In the aggregate, however, the reduction in VPN use accounted for most of the decline in obfuscated browsing.

The reasons for this decline in VPN use by North Korean leaders are not immediately clear in our data. On one hand, some VPN protocols can be [computationally intensive](#) or unreliable, most require a [subscription and regular payments](#), and [many have device limits or still do not accept cryptocurrencies](#). On the other hand, most VPN service providers have an application and easy-to-configure instructions; further, the price of VPNs has fallen so far that users can utilize [reputable and reliable VPNs](#) for as little as \$3 a month.

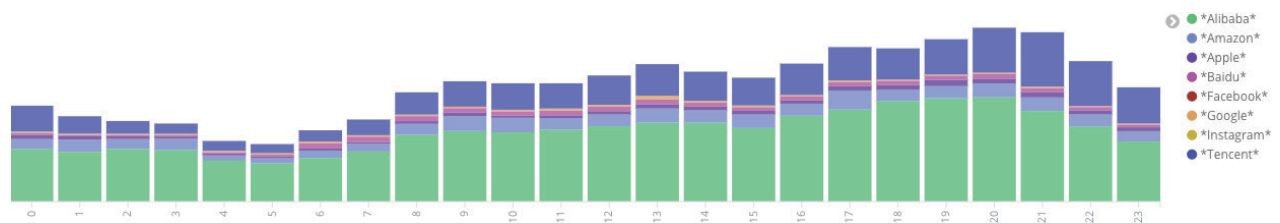
What is most likely is that North Korean internet users initially adopted stronger internet privacy methodologies because of an external stimulus or requirement. In April of this year, we assessed that this behavioral change was likely a result of increasing international attention on North Korea's internet and media activities, new enforcement of an official ban, or a new operational security requirement.

The imposition of a requirement or policy on North Korean users was the most likely source for the dramatic increase in internet security followed by this subsequent moderation. The requirement likely drove a spike in security measures by North Korean leadership users, which then slowly waned over time as the costs in time, money, and accessibility began to outweigh the benefits.

Continued Use of Chinese Social Media Since Early 2018

In early 2018, we observed North Koreans migrate almost completely away from Western social media and services to their Chinese equivalents. This change occurred over the course of six months, from late 2017 through early 2018. North Korean leadership users abruptly switched from services such as Facebook, Instagram, and Google to services run by their Chinese equivalents, such as Baidu, Alibaba, and Tencent.

Since March 1, 2018, that migration away from Western social media and services has persisted. North Korean leaders use Alibaba more than twice as much as any other service, Western or Chinese. Activity on Alibaba includes video and game streaming, search, and shopping.



Hourly activity on eight social networking, shopping, and search sites from March 1, 2018 through August 28, 2018 (actual). Providers are listed by popularity, from Alibaba (highest) to Instagram (lowest).

While the majority of U.S. services continued to experience decreased North Korean leadership use, since April 2018, we observed an increase in the use of LinkedIn. The volume of activity on LinkedIn was lower than the levels we observed on Facebook or Instagram [in July 2017](#). However, the use of LinkedIn was regular and persisted through the end of this dataset in August 2018. The traffic levels indicate far fewer current LinkedIn users than Facebook users in 2017, but represent an interesting counter to the persistent movement away from western social networking services.

Increase in Cryptocurrency Exploitation

In our prior research, we discovered that North Korean leaders were mining both Bitcoin and Monero, albeit at a limited or relatively small scale. For this time period — March 2018 through August 2018 — the traffic volume and rate of communication with peers was the same for both coins as last year, and we were still unable to determine hash rates or builds. We believe these particular mining efforts are likely still small scale and limited to just a few machines.

What has changed dramatically over this March 2018 through August 2018 time frame, however, is the exploitation of cryptocurrencies, asset-backed “altcoins,” and the cryptocurrency ecosystem by North Korea.

In June 2018, we began to notice a number of connections and a large amount of data transfer with several nodes that were associated with the altcoin called [Interstellar, Stellar, or HOLD coin](#). HOLD coin is known as an “[altcoin](#),” which refers to any cryptocurrency other than Bitcoin including some of the more established and widely utilized coins like Monero, Ethereum, and Litecoin. There are over 1,000 altcoins, and most are variations on the Bitcoin framework.

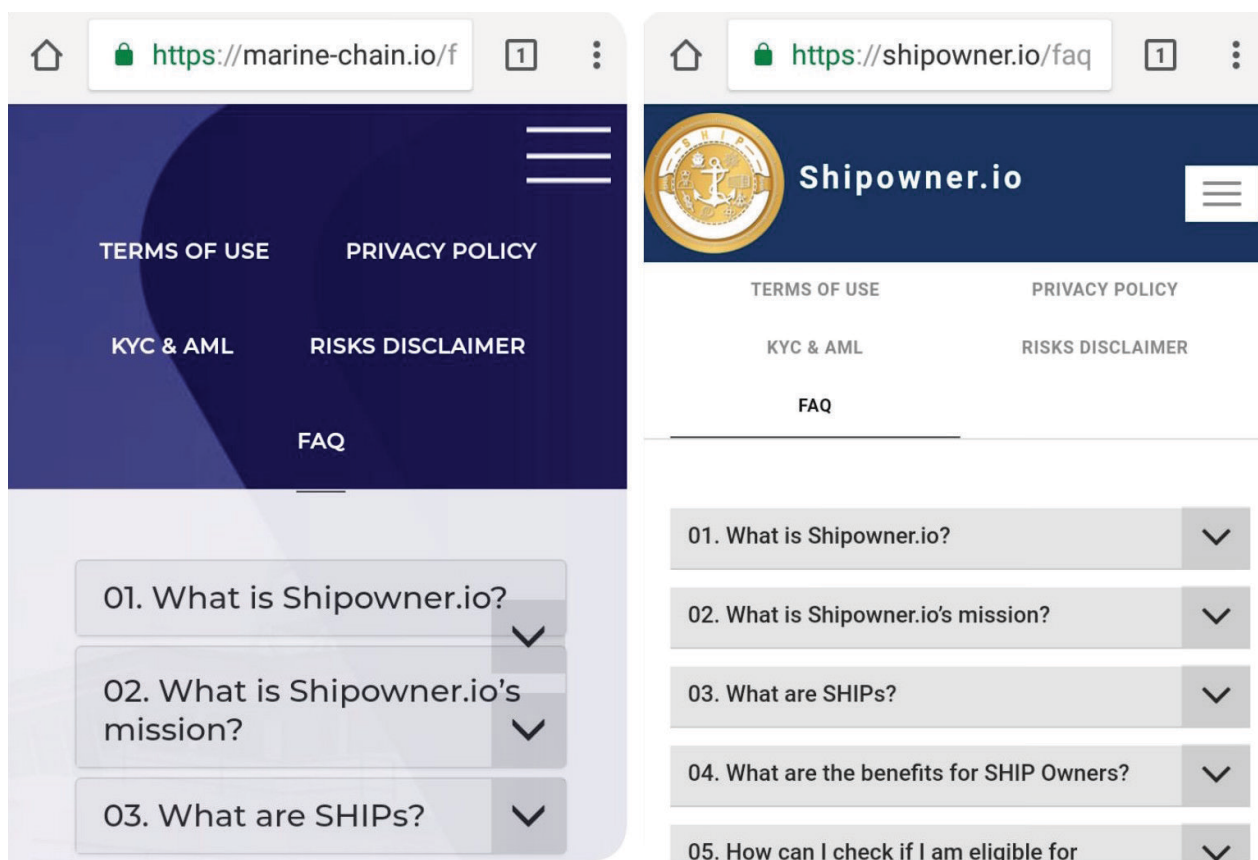
In early 2018, HOLD coin went through a process to generate interest and initial revenue called staking. Staking is when users mine an initial number of coins but are not allowed to trade them for a set period of time. The coin is then able to build up value and a user base, allowing the coin developers to control the value of the coin by regulating which wallets can trade at any one point in time. Participating in the staking of a new or unknown altcoin can be risky because the developers control the staking time frame and can limit trades to the extent that many users lose their investments when the value of the coin depreciates, and they are then unable to trade their staked coins.

Over the course of 2018, HOLD coin was listed and delisted on a series of [exchanges](#), underwent a swap and rebranding in August 2018 (the new name is [HUZU](#)), and, as of this publication, has left its HOLD investors high and dry. We assess with low confidence that North Korean users were involved in the Interstellar, Stellar, or HOLD altcoin.

Editor’s Note: We have edited the above paragraph to clarify that the swap and rebrand from HOLD to HUZU appeared at the end of the report period.

We have discovered at least one other blockchain scam that we assess with high confidence was conducted on behalf of North Korea. This was a blockchain application called Marine Chain Platform.

We came across discussions of Marine Chain as a cryptocurrency in a couple of [Bitcoin forums](#) in August 2018. Marine Chain was supposedly an asset-backed cryptocurrency that enabled the tokenization of maritime vessels for multiple users and owners. Users on [other forums](#) pointed out that [www\[.\]marine-chain\[.\]io](http://www.marine-chain.io) was a near mirror image of another site, [www\[.\]shipowner\[.\]io](http://www.shipowner.io).



[April 2018 screenshots](#) of [marine-chain\[.\]io](http://marine-chain.io) and [shipowner\[.\]io](http://shipowner.io) provided by forum participants.



▼ Resource record type A

▼ Most recent

Bailiwick **marine-chain.io**
 First Seen Jul 31, 2018, 04:19
 Last Seen Sep 10, 2018, 04:38
 IP Address **162.241.218.151**
 Resource record name **www.marine-chain.io**

▼ 2018 (3)

Bailiwick **marine-chain.io**
 First Seen Apr 9, 2018, 02:58
 Last Seen May 28, 2018, 18:09
 IP Address **104.25.81.109**
 Resource record name **www.marine-chain.io**

Bailiwick **marine-chain.io**
 First Seen Mar 26, 2018, 17:53
 Last Seen Apr 7, 2018, 12:16
 IP Address **104.20.85.112**
 Resource record name **www.marine-chain.io**

Bailiwick **marine-chain.io**
 First Seen Dec 8, 2017, 14:00
 Last Seen Mar 10, 2018, 01:42
 IP Address **180.235.134.254**
 Resource record name **www.marine-chain.io**

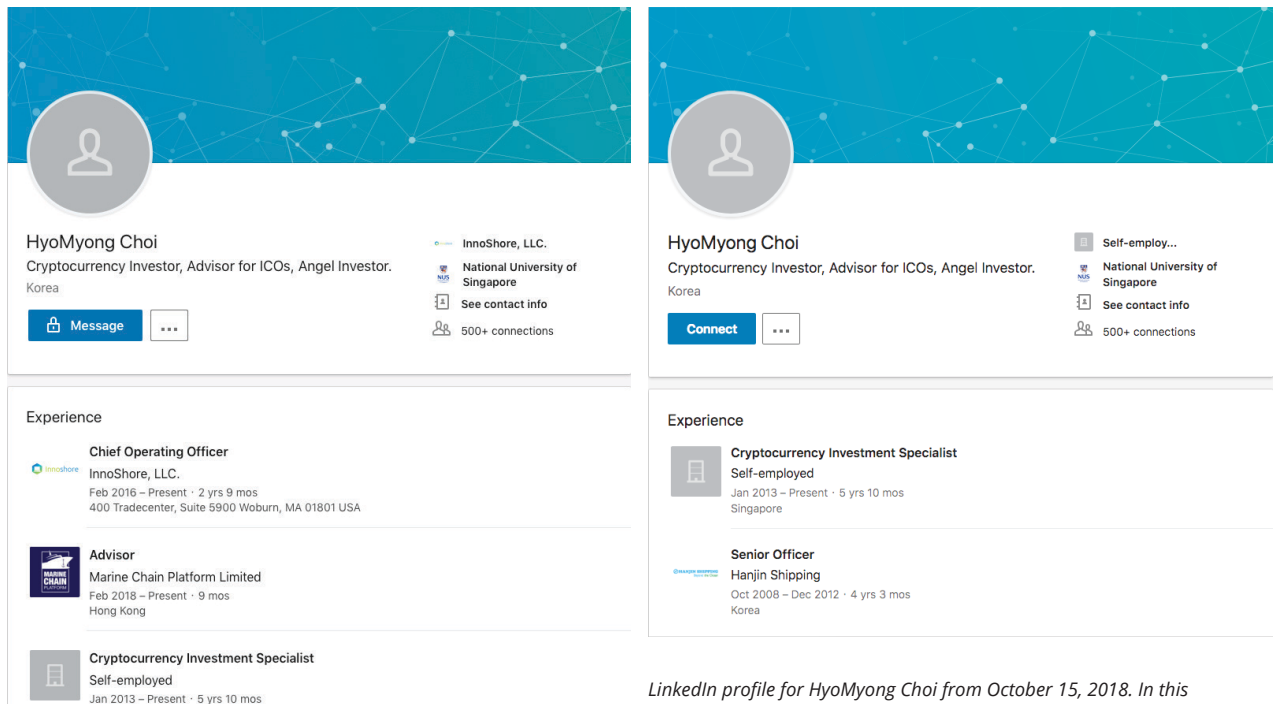
▼ Resource record type AAAA

Domain registration history for marine-chain[.]io.

Marine-chain[.]io has been hosted at four different IP addresses since its registration. From April 9, 2018 through May 28, 2018, marine-chain[.]io was registered at 104[.]25[.]81[.]109. During this time, this IP address also hosted a defunct crypto news site called allcryptotalk[.]net, which has not posted new content since June 2015, and the website for a fraudulent binary options trading company called Binary Tilt. This company was declared [fraudulent by the government of Ontario, Canada](#), and [dozens of users](#) have posted testimonials of losses of tens to hundreds of thousands of dollars and [scams](#) on this site.

The Marine Chain website no longer resolves but was operated by a company called Marine Chain Platform. Aside from a [LinkedIn page](#), the company had minimal online presence, no customer testimonials, and few staff. The Marine Chain LinkedIn page was synonymous with someone named Tony Walker, who claimed to be a “maritime industry blockchain specialist” and advisor to the CEO of Marine Chain Platform since May 2017.

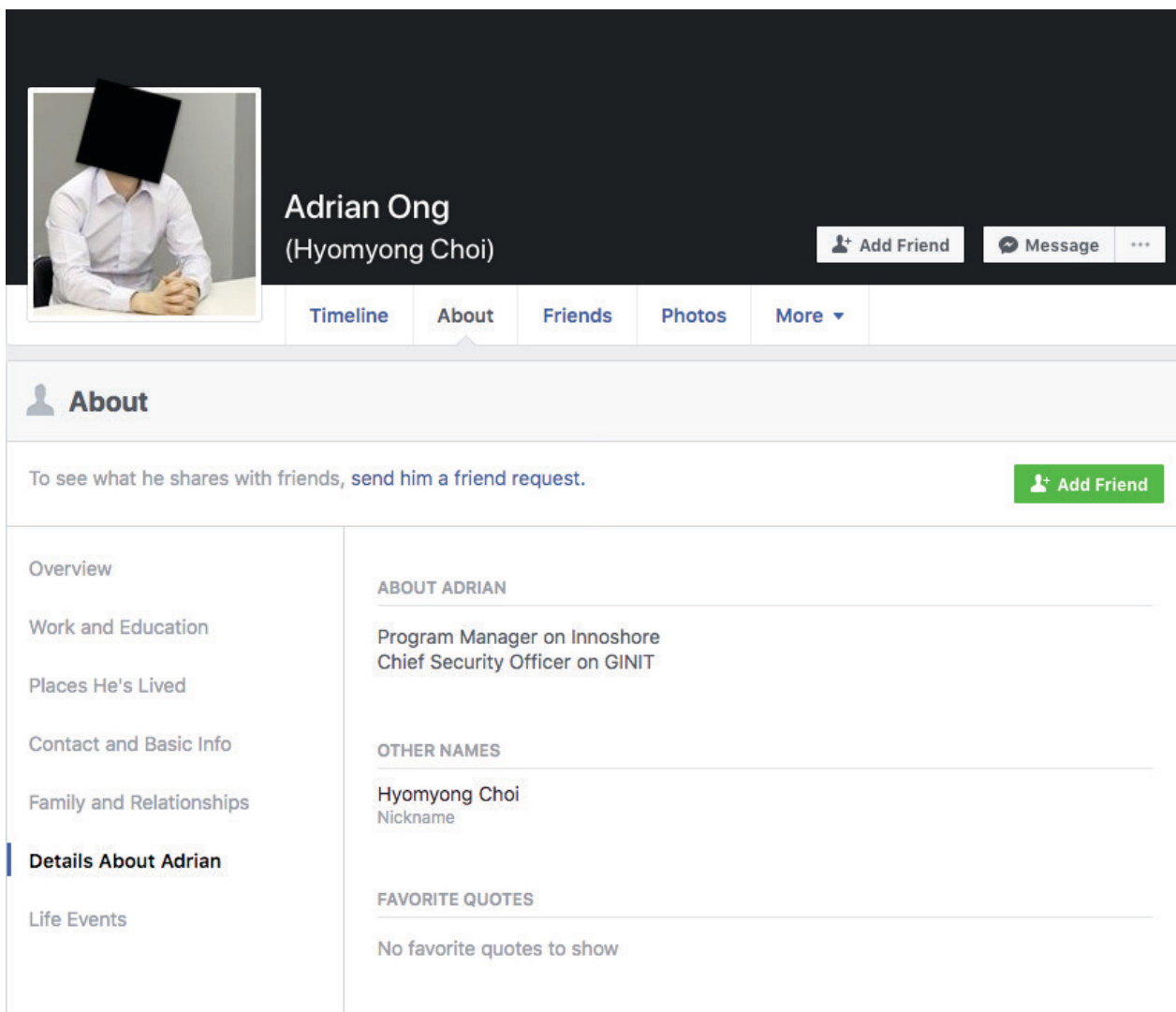
On October 1, 2018, a search for Marine Chain Platform on LinkedIn also yielded another advisor named [HyoMyong Choi](#). Mr. Choi listed himself as a cryptocurrency investor in Korea, an advisor for ICOs, and an angel investor. He also listed himself as being concurrently employed as the chief operating officer (COO) for another company called InnoShore, LLC.



LinkedIn profile for HyoMyong Choi from October 1, 2018.

LinkedIn profile for HyoMyong Choi from October 15, 2018. In this screenshot, Mr. Choi has removed both his Marine Chain Platform and InnoShore, LLC experiences.

Both Mr. Walker and Mr. Choi claim to have attended the National University of Singapore and possess many of the same endorsers. Mr. Choi is also known as Adrian Ong, as evidenced by his (likely fake) Facebook page. The account was created in March 2018 and the profile picture was stolen from an employee of a South Korean company that helps Korean students attend U.S. and U.K. universities.



Adrian Ong
(Hyomyong Choi)

[Add Friend](#) [Message](#) [...](#)

[Timeline](#) [About](#) [Friends](#) [Photos](#) [More ▾](#)

About

To see what he shares with friends, send him a friend request. [Add Friend](#)

Overview

Work and Education

Places He's Lived

Contact and Basic Info

Family and Relationships

Details About Adrian

Life Events

ABOUT ADRIAN

Program Manager on Innoshore
Chief Security Officer on GINIT

OTHER NAMES

Hyomyong Choi
Nickname

FAVORITE QUOTES

No favorite quotes to show

Facebook page for Hyomyong Choi, or Adrian Ong (face blacked out to preserve privacy of victim).

Choi (Mr. Ong) had only two friends, both located in Southeast Asia with large social networks. Aside from these two accounts, Choi (or Mr. Ong) has no other online presence.

The other prominent Marine Chain Platform employee we could track down was the CEO, a man named Captain Jonathan Foong Kah Keong. According to his [LinkedIn profile](#), Capt. Foong has been active in the maritime industry in Singapore for decades. While he does not currently list his position with Marine Chain on his LinkedIn profile, he has spoken at [numerous events](#) over the past year and repeatedly [cited his position](#) at Marine Chain or as the founder of marine-chain[.]io.

🔄 <https://wallstreetcn.com/articles/3278564>

🗨️ 参与评论

★ 收藏

👤 微信

🐦 微博

上一篇:

全球首艘! 风能+LNG动力客船长啥样? | 航运界

下一篇:

地缘政治风险加剧 全球原油供应缩减或远超预期

周诗豪, 运去哪创始人

唐红斌, 鸭嘴兽供应链创始人

郭辉, 运可安创始人

方保利, 长江汇创始人

【拟邀请嘉宾】

Peter Ludvigsen, Blockshipping创始人兼CEO

MITUL DAVE, Shipowner.io 创始人

Capt Jonathan Foong, marine-chain.io CEO

Dovey Wan, 丹华资本董事总经理

陈黎明, IBM大中华区董事长

罗荣阁, 万向区块链CTO

Screenshot of a [forum](#) Foong attended on the shipping industry and blockchain from April 2018 that lists his title as CEO of [marine-chain.io](#).

What makes Capt. Foong stand out from the average cryptocurrency or blockchain scammer is that he has been connected to Singaporean companies that have assisted North Korean sanctions circumvention efforts since at least 2013. In research published by North Korea-specific policy research website [38North.org](#) in 2015, Capt. Foong is [identified twice](#) as working for or advising companies in Singapore that “have facilitated illicit activity on North Korea’s behalf and that have dealings with UN-sanctioned entities.”

The companies Capt. Foong has worked for [have been linked to manipulating](#) the national flag registries for three countries, which were frequently used as [flags of convenience](#) for North Korean vessels.

Capt. Foong is part of a network of enablers throughout the world that assist North Korea in circumventing international sanctions. These connections to Marine Chain Platform mark the first time this vast and illicit network has utilized cryptocurrencies or blockchain technology to raise funds for the Kim regime.

Broadly, these types of cryptocurrency scams fit the template of low-level financial crime [described by defectors](#) that has [plagued South Korea for years](#), and that the [international community](#) is just beginning to track. It is a natural step for both a group of actors that has been so embedded in the cryptocurrency world for years and for a network that is being forced to innovate new funding streams to counter the effects of international sanctions.

North Korean Presence in Foreign Countries: More Details Emerge

In our [prior 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 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 eight nations where North Koreans were physically located or living, including India, China, Nepal, Kenya, Mozambique, Indonesia, Thailand, and Bangladesh. For this latest time period (March 2018 through August 2018), we re-examined North Korean internet activity involving these eight nations and obtained greater fidelity on data from China and India.

China

Distilling the internet activity from likely North Koreans in China has been complicated by the extensive use of Chinese internet services by North Korean leaders, such as those provided by Alibaba, Baidu, and Tencent. Until now, Recorded Future has had little insight into the geographies that may host North Koreans or the local resources utilized.

At the local level, and as a subset of our heuristic data, we discovered high volumes of activity involving the Beijing, Shanghai, and Shenyang regions, but also Nanchang, Wuhan, and Guangzhou. Some of these cities and regions are outside of what was considered the [traditional northeast footprint](#) for North Koreans operating in China.

We also discovered additional leads on North Koreans in the Chinese academic sector that had been previously obscured. The following is a list of Chinese universities that we assess with moderate confidence currently host, or previously hosted, North Korean students, teachers, or partners.

- Shanghai Jiaotong University
- Jiangxi Normal University
- Tsinghua University
- Wuhan Commercial Service College
- Guangxi Normal University
- Fudan University
- Tianjin Medical University

India

While the pattern of behavior did not change for North Korean activity involving India during this time period, we were able to pin down a few additional details. Much of the Indian activity involved several [Special Economic Zones](#) (SEZ), particularly the Noida and Cochin SEZ.

At the local level, and as a subset of our heuristic data, we discovered high volumes of activity involving Delhi, Bangalore, Kolkata, and Hyderabad. We again observed suspicious traffic involving the Indian Meteorological Department and National Remote Sensing Centre, but were not able to determine maliciousness.

For most of these nations, this heuristic tracked closely with known North Korean illicit financing or logistics networks. The research conducted by the non-profit [C4ADS](#) on North Korea's illicit financing networks is an excellent example. In August, C4ADS released a [report](#) that profiled North Korean overseas forced labor by country and sector, including restaurants and products. This repeated overlap between North Korean illicit financing networks and internet activity prompted us to re-examine why Russia did not fit our behavioral heuristic.

Russia

From a volume perspective, activity involving Russia was a mere fraction of the North Korean internet activity that involved China or India (about .05 percent of the volume from China, for example). In terms of services, North Koreans used Russian services on a very limited basis, with regular visits to mail.ru and only occasional use of Yandex. At the city level, the small volume of activity involved primarily Sochi, the Moscow region, and Vladivostok.

It is possible that the types of North Koreans in Russia during this time frame (March 2018 through August 2018) were different than many of the other countries we have identified. A [large number](#) of North Korean workers in Russia are manual laborers, often housed and working in “[slave-like](#)” or “[inhumane](#)” conditions. This is in contrast to some North Korean workers in other countries, such as China, who are [laborers in the information economy](#) and build mobile games, apps, bots, and other IT products for a global customer base. While there are certainly a [large number](#) of [manual laborers](#) in China as well, it is possible that Russia hosts fewer skilled North Korean workers. This type of information economy work creates a different internet fingerprint than exploitative manual labor and likely clarifies the discrepancy between physical presence and internet activity.

Therefore, we assess that the nations we identify through our behavioral heuristic are more likely to be hosting North Korean workers in the service or information economy. Although these workers still send [large percentages of their earnings back](#) home, they need internet access for their daily work, or because they are customer facing, likely live in less oppressive conditions.

Outlook

Over the course of the last year and a half, 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; the duration of the "[maximum pressure](#)" campaign, the period of the highest missile launching and testing activity, and the [first ever summit](#) 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.

In particular, the Kim regime has cultivated the internet as a potent tool for revenue generation and sanctions circumvention by utilizing (and exploiting) cryptocurrencies, various interbank transfer systems, the pluralized nature of the "gig economy," online gaming, and more. They have paired this with a decades-old smuggling network and system of corrupted diplomats, embassies, and consulates.

It is this marrying of the physical and virtual that enables North Korea's success and confounds international regulators and enforcers. It may never be possible to assign an exact dollar figure to the value North Korea derives from the internet, but its significance cannot be underestimated.

Internationally, nations have just begun to address the globalized nature of and threat from North Korean internet operations. The United States in particular filed a [criminal complaint](#) against one North Korean operator, Park Jin Hyok, and implicated many others.

This is an excellent first step, and one that needs to be followed up with further action publicizing internet operations, outreach to nontraditional diplomatic partners, and more flexible and dynamic mechanisms to degrade North Korean internet-enabled sanctions evasion.

This will also be our final regular report on North Korean leadership internet activity because our insight has been limited as a result of two trends: the use of internet security and anonymization services by North Korean leaders, and the proliferation of domain privacy and large-scale hosting services.

First, even though North Korean ruling elite have scaled back on their internet security procedures, the broad trend for both North Koreans and across all internet users is up. This means that it will only get harder over time to track North Korean internet browsing and reveal new insights.

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

We will still monitor North Korea's IP ranges and report on critical discoveries or events on an ad hoc basis.

Network Defense Recommendations

Recorded Future recommends 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 illicit 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:
 - 10130 and 10131 for HOLD coin
 - 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.

- Analyze network DNS traffic to detect and block suspicious traffic relating to HOLD coin cryptocurrency mining (e.g., domains including the term “stellarhold”).
- 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.
- Know your organization’s VPN services and protocols and block or carefully scrutinize non-standard VPN traffic.

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 (e.g., 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 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.