CYBER THREAT ANALYSIS

NORTH KOREA

Recorded Future®

By Insikt Group®

July 18, 2024

Despite Sanctions, North Koreans Continue to Use Foreign Technology

Despite sanctions, North Koreans continue to use foreign devices released as recently as 2024, signifying that they are acquiring the latest device models almost as fast as consumers in other markets.

Insikt Group observed Network Intelligence between North Korean IP space and proxy services designed to circumvent censorship, indicating some North Koreans are likely trying to avoid local censors.

Insikt Group observed Network Intelligence suggesting that North Koreans abroad very likely visit official regime news websites to stay up to date on events and policy positions in the country.

Executive Summary

North Koreans continue to use foreign technology to access the internet for personal and professional use, though more users seem to be adopting obfuscation services designed for circumventing censorship. These findings are based on Insikt Group's recent analysis of Recorded Future Network Intelligence data associated with North Korea, building on previous analyses between 2017 and 2020 to establish trends. These findings consistently show that the country is not isolated from the rest of the world; instead, some users are active in browsing social media, streaming content, and playing video games. The most recent analysis is unique in that it shows that the activity is highly likely related to North Korean individuals and not foreign visitors with internet access in the country, as North Korea closed its borders to foreigners during the COVID-19 pandemic.

Our findings show that North Koreans continue to use foreign technology, including Apple, Samsung, Windows, and Huawei devices. Individuals with access to the internet continue to use social media and play video games, with a mixture of United States (US), Chinese, and Korean social media and chat applications observed in the data. While we observed North Koreans continuing to use virtual private network (VPN) and proxy services, this is the first time we have seen North Koreans likely using obfuscation services to avoid domestic surveillance or censorship, demonstrating an increased awareness of operational security for online activities of which the regime disapproves. In addition to VPN and proxy services, we also observed likely foreign antivirus products in use. Insikt Group also analyzed Network Intelligence data associated with external-facing North Korean websites that are accessible online and found evidence that North Koreans abroad regularly visit official news websites, indicating that these publications are not just for foreign audiences but for expatriates as well.

Our findings show that despite heavy sanctions, North Korea continues to acquire foreign technology and software. A select subset of North Koreans with access to the internet are living similar lives to those in other parts of the world, using the latest mobile phones and gaming consoles while browsing social media and chatting with friends. Continued access to foreign technology and services across the internet likely contributes to North Korea's ability to avoid sanctions and earn additional revenue for the regime. The potential points of interaction with North Korea are both physical and virtual, as organizations may find their products in the hands of North Koreans or their online services being used by North Koreans with access to the internet or even developed by North Korean IT workers.

Organizations that suspect their products may end up in the hands of North Koreans should conduct proper due diligence on their buyers and users, specifically those in regions where third parties may resell their products to sanctioned entities affiliated with the regime, particularly Russia and China. In the event that products or services are transferred to sanctioned entities affiliated with North Korea, companies may face financial penalties from government agencies. Moreover, once in the hands of North Koreans, a device could be analyzed for vulnerabilities to be used in cyberattacks or copied to produce a domestic version. This is especially pertinent as North Korea will very likely continue to import foreign technology because of its renewed trade relationship with China following the reopening of its border post-pandemic and its burgeoning trade relationship with Russia, as it helps supply arms

for Russia's ongoing invasion of Ukraine. The long-term implications of North Korea's continued imports of foreign technology will likely reduce the effectiveness of sanctions placed upon the regime.

Key Findings

- Insikt Group observed evidence of North Koreans using American social media services and video game consoles, Chinese and Japanese messenger applications, and American, Russian, and Chinese search engines.
- As in Insikt Group's previous research, North Korean internet users are most active Monday through Friday between 9:00 AM and 1:00 AM Korea Standard Time (KST).
- Despite sanctions, North Korean internet users continue to use foreign devices, including Apple, Samsung, Huawei, and Xiaomi products.
- Windows was the most popular desktop operating system (OS) observed; approximately 43% of OS observations were Windows 8 or older, with some North Koreans still using Windows XP.
- Insikt Group observed Network Intelligence events between North Korean IP space and 35 unique VPN or proxy services, including services designed to circumvent censorship, indicating that some North Koreans are likely trying to avoid local censors.
- North Koreans abroad very likely visit official news websites to stay up to date on current events in the country and the regime's policy positions.
- North Koreans will likely continue to acquire foreign technology despite sanctions imposed on North Korea due to its ongoing trade relations with China and Russia, limiting the future effectiveness of outside actions.

Background and Methodology

North Korea's internet system is unlike any other in the world. Established in 1990, the country's internet, or rather intranet, is completely separate from the wider internet that the rest of the world uses every day. The intranet is called Kwangmyong (광명망) and uses entirely private IPv4 networks; North Korean users cannot access the broader internet, and the broader internet cannot access the Kwangmyong network.

The intranet is becoming increasingly popular in the country. In 2015, the first online shopping mall was opened on the intranet, and by 2021, there were 22 shopping mall websites. In 2020, the Central Bank of North Korea (중앙은행) launched an electronic payment system; however, as of 2021, it is unclear as to whether users can make purchases online. In 2018, it was estimated that 18-20% of North Koreans had mobile phones with access to Kwangmyong, and in 2020, it was estimated that 70% of North Koreans in major cities between the ages of 20 and 50 were mobile phone subscribers. While there is an ever-growing number of Kwangmyong users, the number of individuals with access to the wider internet remains extraordinarily low.

According to reporting from 2022, North Korea has the lowest internet penetration rate in the world, at approximately 0.1%, or 20,000 users. For comparison, worldwide average internet penetration is approximately 65.6%, and just across the border in South Korea, internet penetration is 97%. Even for the select few North Koreans with internet access, getting approval for one hour of internet use is a days-long process. Once online, only English and Chinese websites are available. Only a few dozen families close to Kim Jong Un are believed to have unrestricted internet access, along with foreigners in the country who are separated from domestic users.

Insikt Group has previously investigated North Korean internet traffic in 2017, 2018, and 2020. These reports provided evidence of North Korean internet users doing the same things other people in other parts of the world do on the internet — browsing social media, playing video games, streaming videos, and engaging in activities associated with the cryptocurrency industry. Over the years, we saw an increase in the use of obfuscation services, such as VPNs, likely in response to increasing user operation security awareness. We also observed multiple countries that likely host North Korean individuals based on internet traffic patterns.

Insikt Group conducted an updated analysis of North Korean internet user behavior using our Network Intelligence dataset. Recorded Future Network Intelligence analytics are derived from monitoring and analyzing data traveling through a network. This data is used to observe traffic between attackers and their victims as attackers build, stage, and launch cyberattacks. In North Korea's case, we could use a subset of this data to observe events emanating from the country's primary IP range, *175.45.176[.]0/24*. While this Network Intelligence is only a small sample of all activity across the IP range, we believe there was sufficient data to draw several conclusions, explored in detail below.

The reason for this analysis is twofold. First, it has been four years since we conducted our last analysis, and we wanted an updated understanding of North Korean internet behavior, including how it may have changed over the previous four years, evidence of North Korean users outside of the country, and signs of malicious activity emanating from North Korea. Second, the COVID-19 pandemic presented a unique opportunity to observe what may be purely North Korean internet traffic. In 2020, following the COVID-19 pandemic, foreigners left the country and were not allowed back into North Korea until late 2023, with the first foreign tour group arriving in February 2024. While previous analyses of North Korean internet behavior very likely included foreigners, our analysis of Network Intelligence between January 2023 and March 2024 focuses on a timeframe with little to no foreign presence in the country.

Technical Analysis

Trends in Activity

Similar to our previous analyses, North Korean internet behavior mirrors that of users outside the country. We observed North Koreans using the social media services Facebook, X (formerly Twitter), and Instagram, the messenger applications WeChat, LINE, and QQ, and the search engines Yahoo, Baidu, Yandex, and Sogou. We know North Koreans sometimes use these social network services for reconnaissance during cyber operations. Our findings also show that North Koreans very likely play video games using consoles such as Xbox, browse e-commerce sites, and watch pornography. We also saw evidence of McAfee antivirus products, indicating that some North Koreans are concerned about cybersecurity.

Pattern of Life

Insikt Group looked more closely at a subset of Network Intelligence during June 2023. We chose this month because of its relatively consistent data coverage and because it was still before foreign visitors were allowed back into the country. It is most likely representative of North Korean internet usage. In our previous analysis of North Korean internet activity, we observed peak activity on the weekends in 2017, but that activity shifted to weekdays in 2018, likely as a result of increasing professional use of the internet by those with access in North Korea. Data compiled using Recorded Future's Network Intelligence in June 2023 is consistent with what we reported in 2018. Peak activity in June 2023 was from Monday to Friday, with activity dropping noticeably on Saturday and Sunday. In 2018, activity peaked between 8:00 and 21:00 KST. While a similar pattern continues, peak activity in June 2023 lasted longer, until 12:00 to 1:00, dropping at 2:00 before picking back up at 9:00. The data was not conclusive enough to determine the reason for this increased activity during night hours, but North Koreans may be working later into the night to accommodate another time zone, especially as there has been an increase in the number of North Korean IT workers generating revenue for the regime.

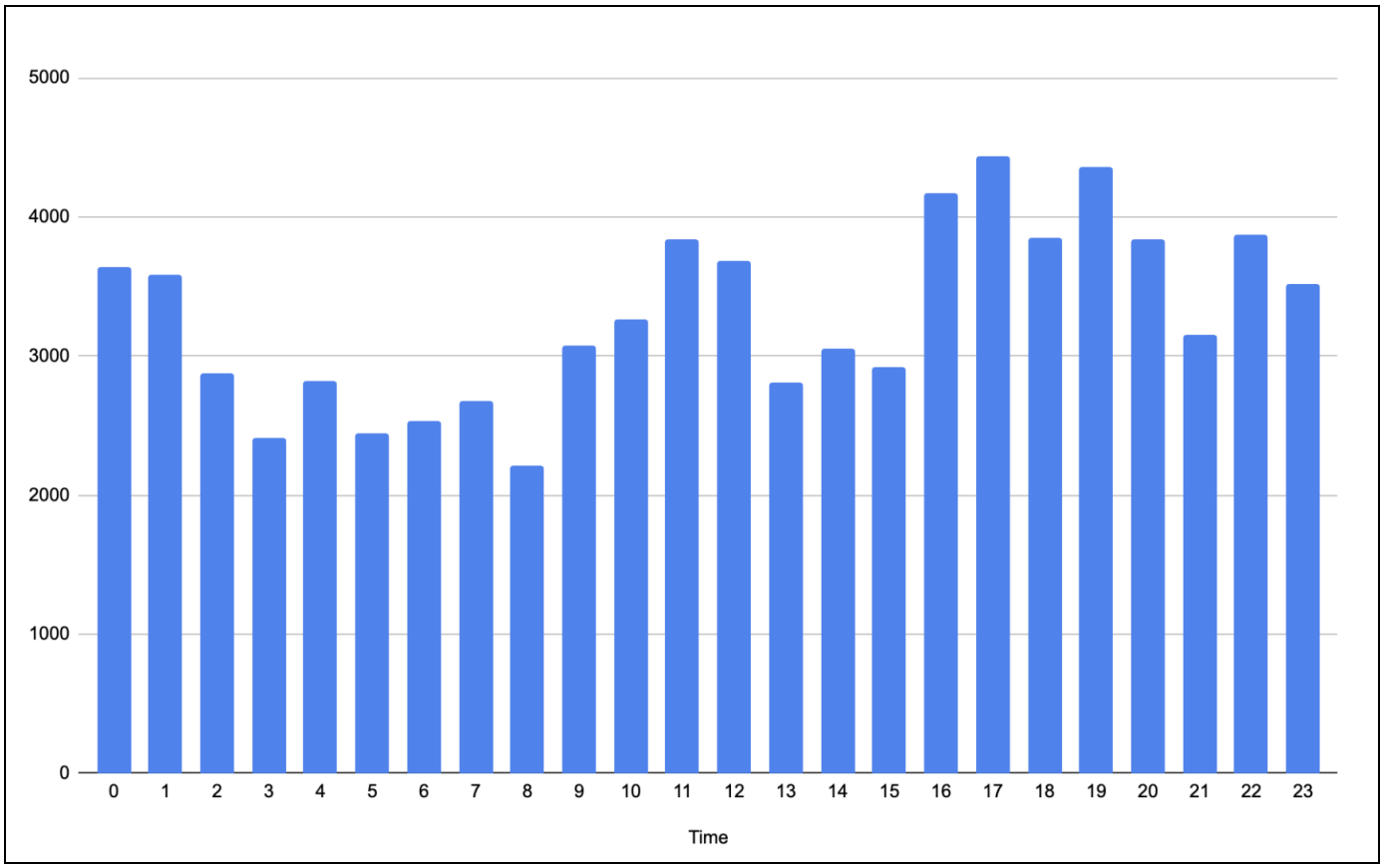

Figure 1: *Observed North Korean internet activity by the hour during June 2023 (KST); the Y-axis represents observations of Recorded Future Network Intelligence (Source: Recorded Future)*

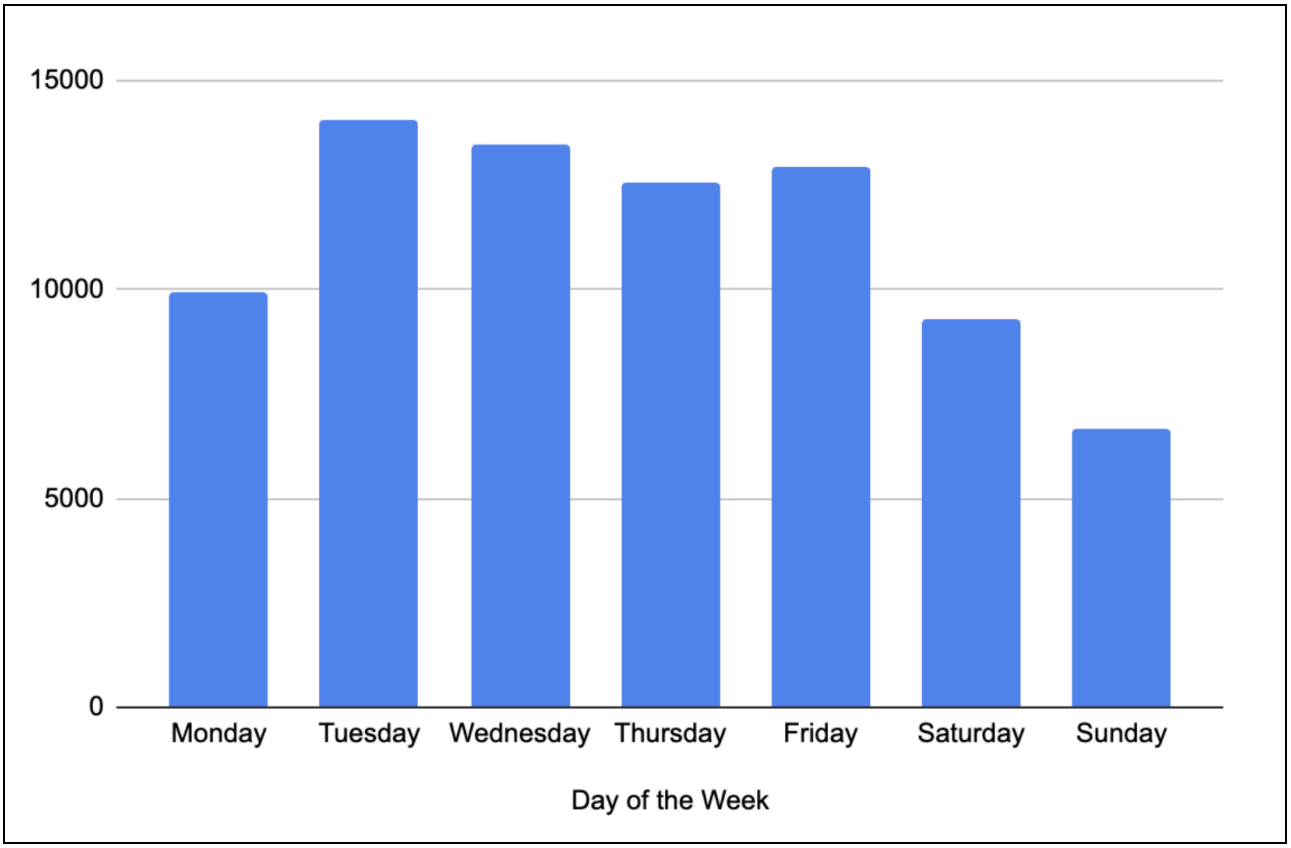

Figure 2: *Observed North Korean internet activity by day of the week during June 2023; the Y-axis represents observations of Recorded Future Network Intelligence (Source: Recorded Future)*

Devices

The North Korean regime develops its own devices and software, including its own heavily modified Linux OS distribution, Red Star OS, and a widespread domestic mobile network (1, 2). However, we also know that the regime imports foreign technology, including Dell computers and Chinese mobile phones. Recorded Future Network Intelligence confirms the presence of devices imported into the country, including desktop computers and mobile phones. Insikt Group saw slightly more mobile devices being used in North Korea than desktop or laptop computers.

North Koreans, like consumers in the US, prefer Apple products; Apple devices remain the single most popular brand in North Korea, with Samsung, Xiaomi, and Huawei comprising the next three most popular brands. However, when all Android device brands are considered, there are more Android users in the country. Phone models as recent as the Samsung Galaxy S24 Ultra, released on January 31, 2024, were observed. Considering our analysis cutoff was March 2024, this indicates that some North Koreans are acquiring the latest device models almost as fast as consumers in other markets. Other open-source reports have also corroborated that the regime continues to import foreign phones from China.

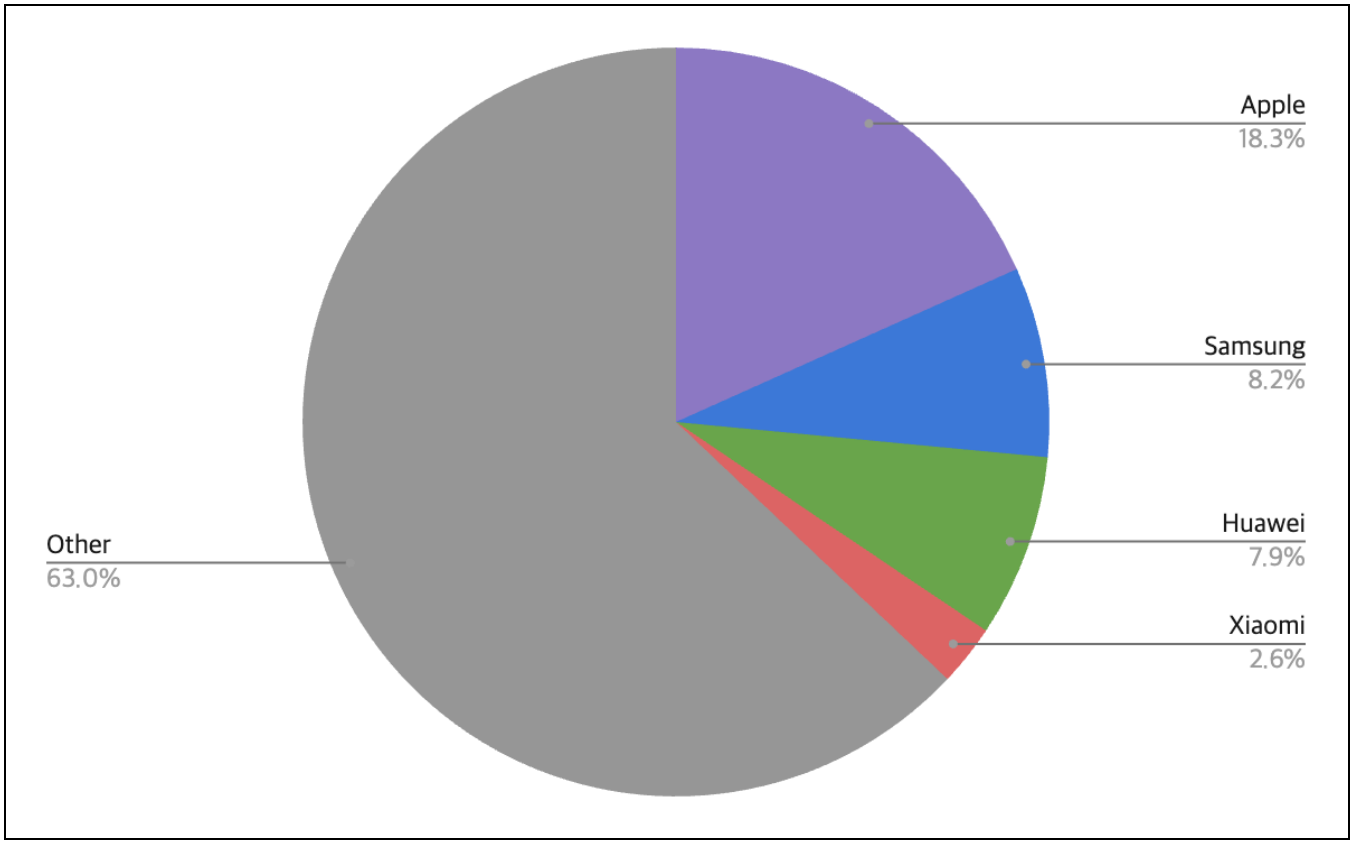

Figure 3: *Breakdown of observed device manufacturers in North Korea (Source: Recorded Future)*

Windows is the most popular desktop OS, and many North Koreans regularly update their Windows software. Approximately 57% of Windows devices were running Windows 10 or 11. Browser developers have stopped updating their user agents with Windows versions, so Windows 11 devices will show up as Windows 10. The remaining 43% of Windows device observations were Windows 8 or older, with some North Koreans still using Windows XP, for which Microsoft ended updates and support in April 2014. For web browsers, while most Firefox versions were up to date, we did observe some instances of older Firefox versions, such as 52, which was released in March 2017. Similarly, most Chrome versions were up to date, but we observed a smaller number of outdated Chrome versions, such as 49.0.2623.112, which was released in April 2016.

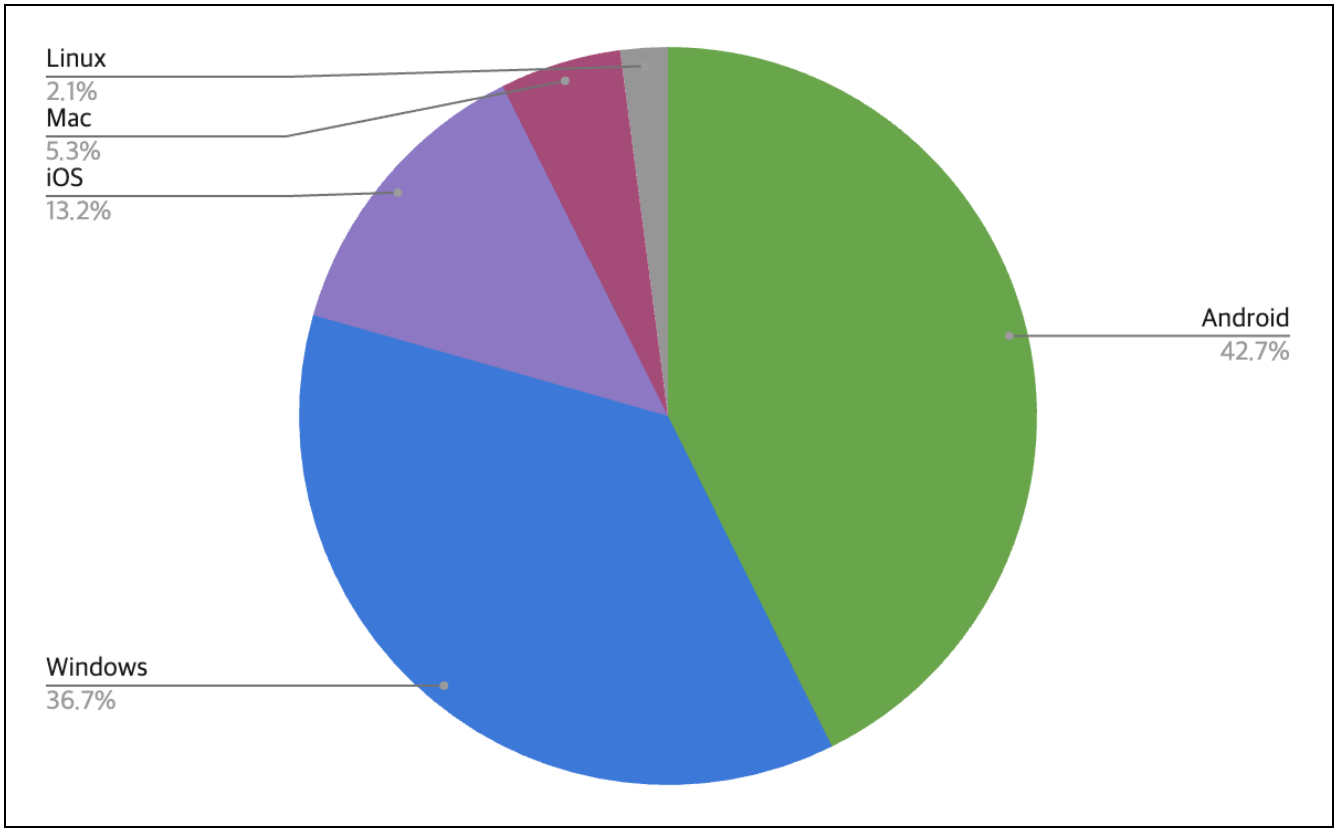

Figure 4: *Breakdown of observed operating systems in North Korea (Source: North Korea)*

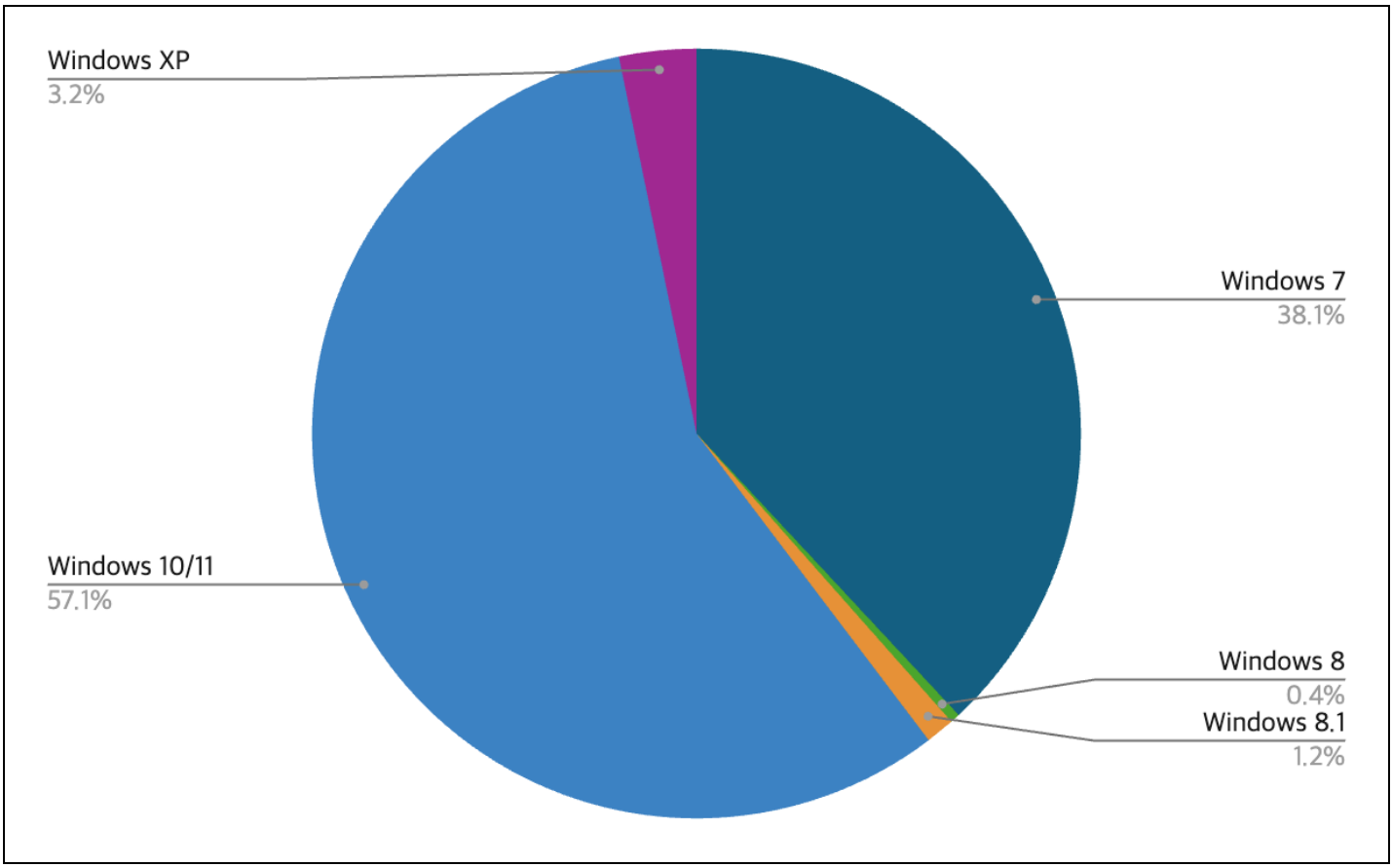

Figure 5: *Breakdown of observed Windows versions in North Korea (Source: North Korea)*

VPN and Proxy Services

Insikt Group observed consistent communication between North Korean IP addresses and VPN endpoints over the period of analysis. We saw 31 unique North Korean IP addresses communicating with 35 different VPN or proxy services. North Koreans overwhelmingly use Hotspot Shield, followed by Express VPN, Private Internet Access (PIA), and Psiphon 3. While Hotspot, Express, and PIA are common VPN services used around the world, Psiphon 3 is a VPN service designed to circumvent internet censorship.[1] We know from previous interviews with defectors that North Koreans are aware of online monitoring and censorship and actively try to avoid it. North Koreans with internet access in the country may be using this service to avoid censors put in place by the regime.

[1] *https://s3[.]amazonaws[.]com/0ubz-2q11-gi9y/en[.]html*

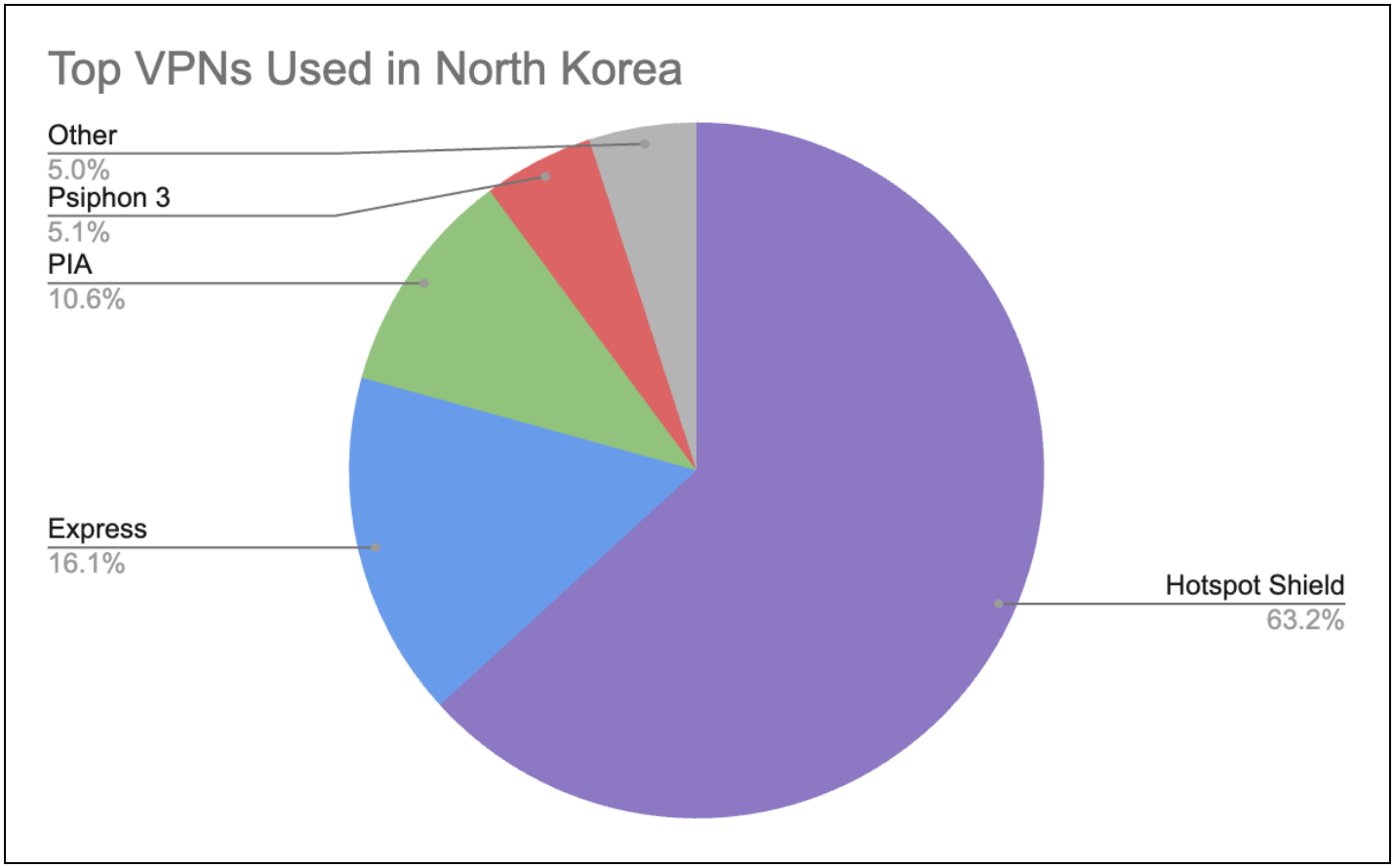

Figure 6: *Breakdown of VPN use in North Korea (Source: Recorded Future)*

Visitors to North Korean Websites

Insikt Group also analyzed global Recorded Future Network Intelligence associated with North Korean websites publicly accessible online. As seen below in **Figure 6**, over half of the traffic during the timeframe was to Rodong Sinmun and the Korean Central News Agency (KCNA). Rodong Sinum is the official newspaper of the Central Committee of the Workers' Party of Korea, which provides viewpoints of the party for domestic and foreign audiences. The KCNA is North Korea's main state news agency, offering heavily censored news from within the country and from official government positions. Unsurprisingly, these two websites comprise the largest share of observed Network Intelligence, as both foreign researchers and those interested in North Korea would be viewing the content, and North Koreans abroad would be checking in on news and policy positions at home. The remaining traffic was to other North Korean websites accessible from the wider internet.

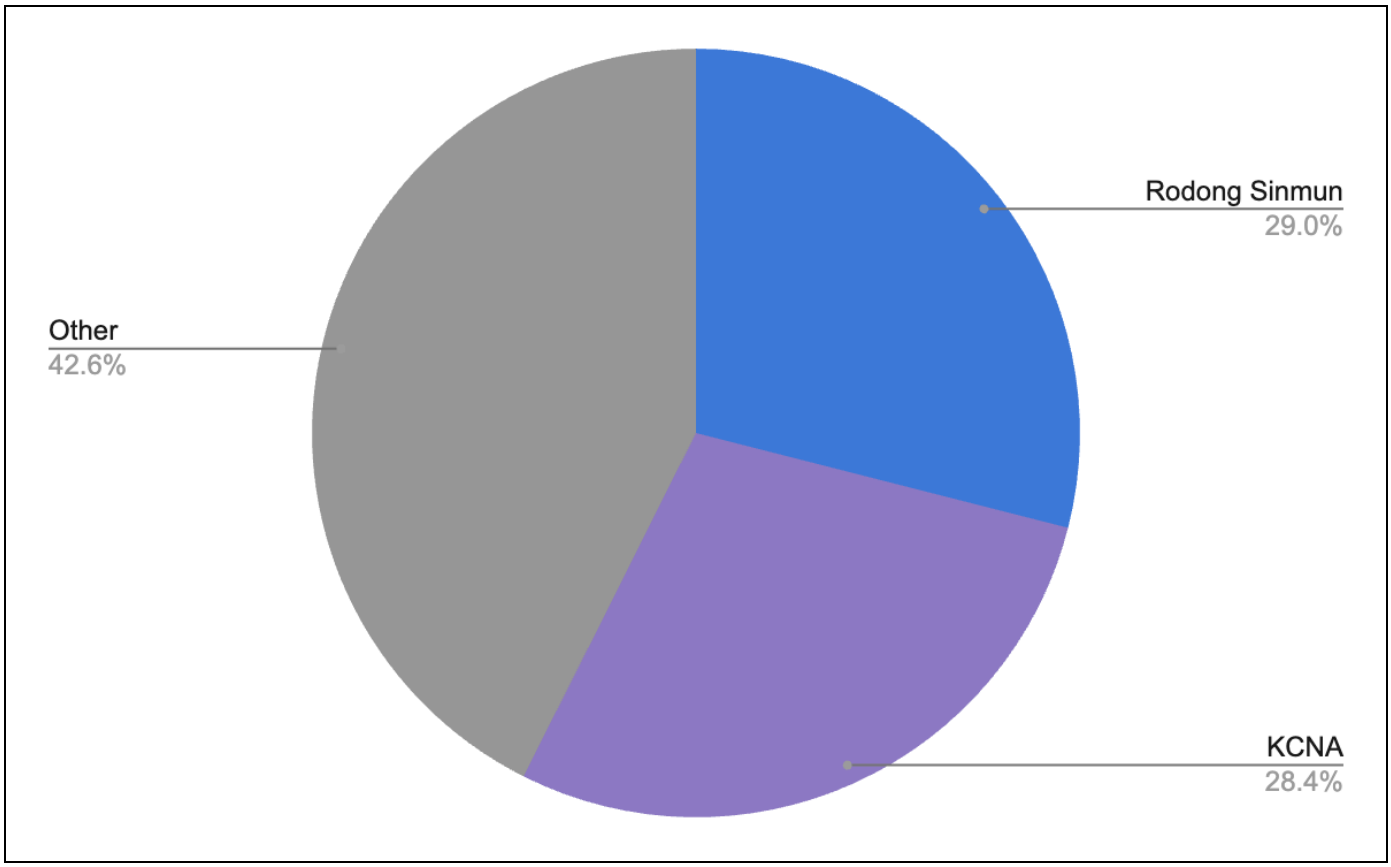

Figure 7: *Breakdown of Network Intelligence to North Korean websites (Source: Recorded Future)*

North Koreans Abroad

As mentioned above, we assess that some of the observed Network Intelligence is associated with North Koreans abroad keeping up with the latest official news and statements from the regime. A subset of Network Intelligence further strengthened this assessment. During the analysis period, we observed consistent traffic to North Korean websites from the continent of Africa. Insikt Group has previously written about the North Korean regime's activity and long-standing relationships in the region; however, in late 2023, the North Korean government began closing embassies in Africa, with some speculating that the closures resulted from financial difficulties and worsening ties with African countries. Recorded Future Network Intelligence associated with traffic to North Korean websites from Africa correlated with the embassy closures, with traffic dropping noticeably around the time of the embassy closures. It is likely that North Korean staff at these embassies regularly viewed North Korean news from official sources back home.

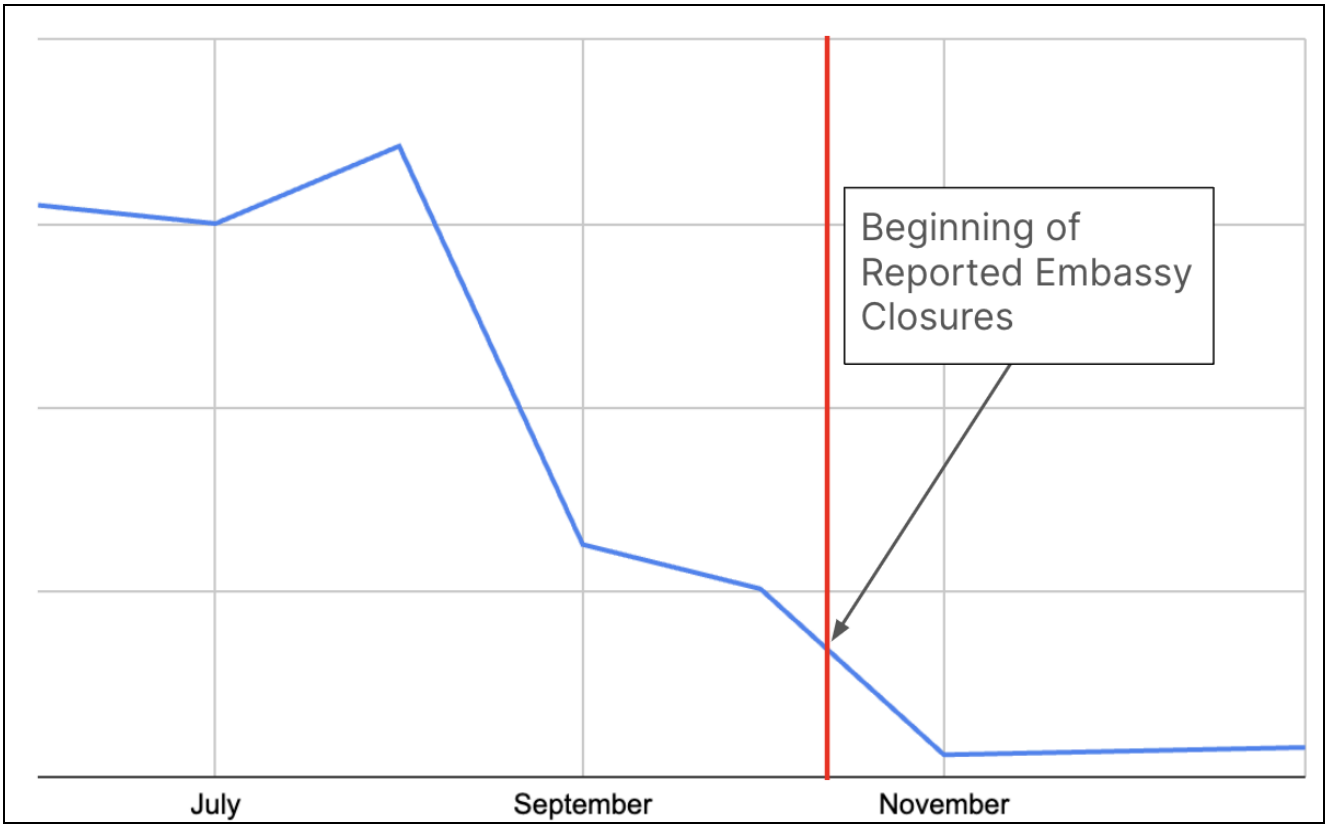

Figure 8: *Observed Network Intelligence from the African region to North Korean websites over time by month during 2023 (Source: Recorded Future)*

Outlook

North Koreans will likely continue to acquire and use foreign technology despite sanctions due to continuing trade with China and a recently burgeoning trade relationship with Russia, with North Korea supplying arms used in Russia's ongoing invasion of Ukraine. This is especially pertinent due to Russia vetoing the United Nations mandate for a panel of experts to monitor sanctions on North Korea in May 2024. As a result, it is unlikely that new international sanctions will be imposed on North Korea; however, individual countries continue to sanction North Korean entities suspected of supporting the regime. Such sanctions will likely increase the financial costs of conducting due diligence in regions where there is a higher likelihood of accidentally selling to a third party that conducts business with sanctioned entities. Companies that suspect their devices or technology may be imported into North Korea should conduct proper due diligence on their buyers and consult the US Office of Foreign Assets Control (OFAC) for the most up-to-date information on sanctions.

We expect to see the browsing behavior of North Koreans with broader access to the global internet to continue mirroring those in other countries, with peak activity taking place during weekday work hours. Additionally, North Koreans will likely continue using VPN and proxy services to mask their online activities from those watching abroad and those who may be watching at home. Finally, North Korean official news sources are important for expatriates abroad, confirming that the content produced by these sources is not just for foreign audiences but for the country's citizens as well.

Recorded Future reporting contains expressions of likelihood or probability consistent with US Intelligence Community Directive (ICD) 203: Analytic Standards (published January 2, 2015). Recorded Future reporting also uses confidence level standards employed by the US Intelligence Community to assess the quality and quantity of the source information supporting our analytic judgments.

About Insikt Group®

Recorded Future's Insikt Group, the company's threat research division, comprises analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence that reduces risk for clients, enables tangible outcomes, and prevents business disruption.

About Recorded Future®

Recorded Future is the world's largest threat intelligence company. Recorded Future's Intelligence Cloud provides end-to-end intelligence across adversaries, infrastructure, and targets. Indexing the internet across the open web, dark web, and technical sources, Recorded Future provides real-time visibility into an expanding attack surface and threat landscape, empowering clients to act with speed and confidence to reduce risk and securely drive business forward. Headquartered in Boston with offices and employees around the world, Recorded Future works with over 1,800 businesses and government organizations across more than 75 countries to provide real-time, unbiased, and actionable intelligence.

Learn more at recordedfuture.com