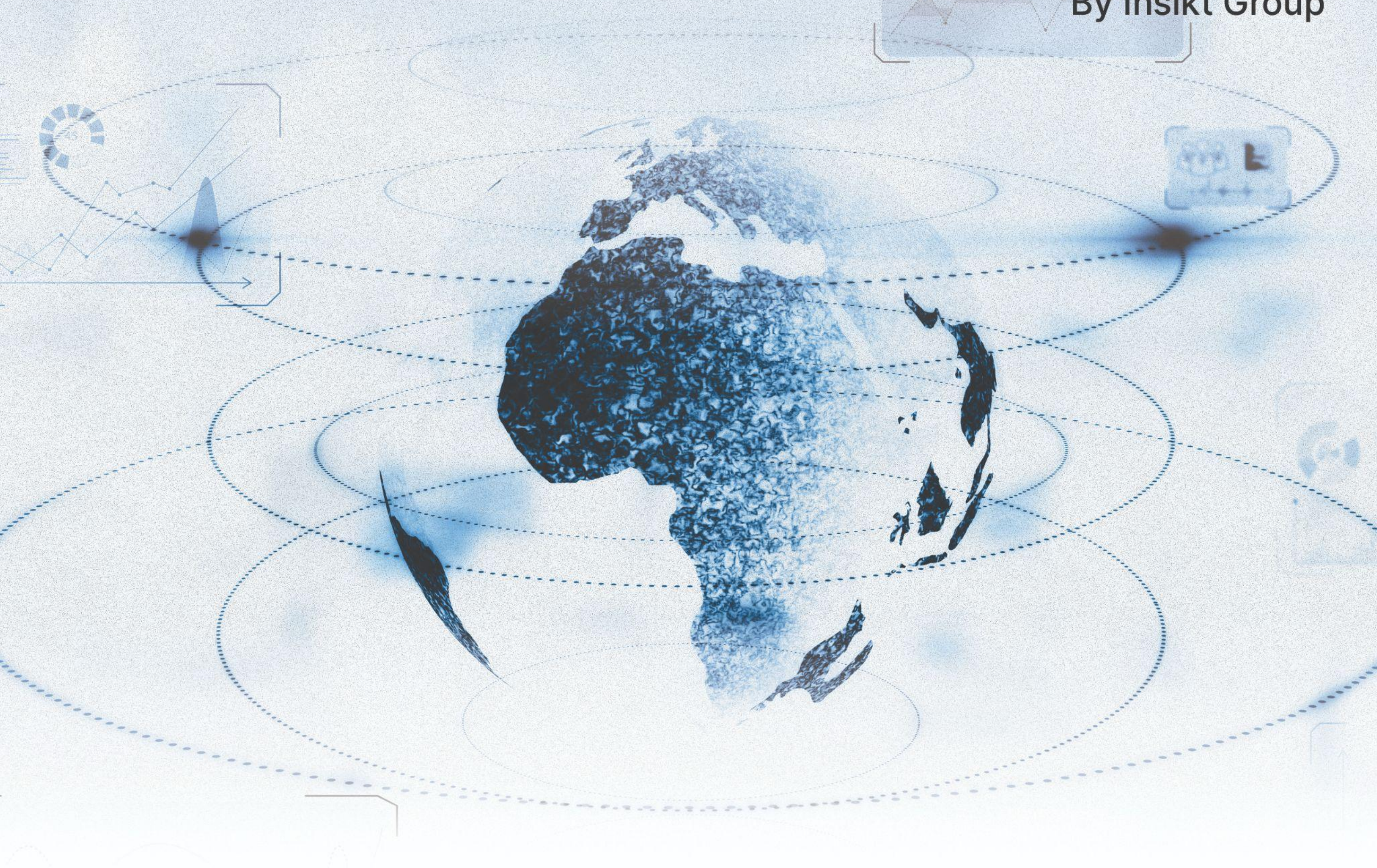
Recorded Future®

By Insikt Group®



North Korea's Cyber Strategy

CTA-NK-2023-0622

Executive Summary

Despite the ever-increasing number of cyberattacks publicly attributed to North Korea, the regime does not publish an official cyber-strategy doctrine. Based on the analysis conducted in this report, North Korea's cyber strategy is aggressive, high-tempo information collection and financial theft operations to support its broader goals of perpetuation of the Kim family dynasty and unification of the Korean peninsula under North Korean leadership. North Korea conducts information collection operations to gain insight into how its adversaries think — including academics, media, defectors, and others with a nexus to North Korea — to better anticipate the operational environment during heightened tensions or conflict. Additionally, it attempts to gain access to information on technologies, such as missile technology, which will help it gain an asymmetric advantage during the aforementioned times of crisis. It also uses financial theft to supplement its continued funding of the regime, including its nuclear and missile programs, while under international sanctions. It does all this by creatively targeting a geographically diverse, wide range of industries, despite its centralized leadership system.

Insikt Group conducted a quantitative analysis of 273 cyberattacks attributed to North Korean state-sponsored threat actors to assess the regime's cyber strategy based on past actions. Overwhelmingly, North Korea's actions in cyberspace consist of cyber espionage and financial theft in support of the regime. Despite the asymmetric advantage of being able to conduct disruptive or destructive cyberattacks with limited resources and a low risk of retaliation, threat actors linked to the Democratic People's Republic of Korea (DPRK; North Korea) rarely conduct such disruptive or destructive computer network operations.

Entities in the Republic of Korea (ROK; South Korea) and the United States (US), North Korea's 2 longtime geopolitical adversaries, are the victims of the majority of cyberattacks attributed to threat actors sponsored by the DPRK. However, North Korean threat actors maintain a global reach as well, targeting entities in at least 29 different countries since 2009. The targets and purpose of cyberattacks vary between threat actors — for instance, Kimsuky-attributed attacks have targeted entities in South Korea for espionage purposes, while Lazarus Group appears to have a much more diverse scope and global purview, targeting entities in a multitude of countries for various reasons. North Korea has been linked to an ever-increasing number of cryptocurrency heists, but the regime's primary goal in its use of cyberattacks continues to be espionage.

Key Findings

- The primary objective of North Korea's cyber strategy is espionage; 71.5% of cyberattacks with a known purpose were likely for information collection.
- North Korea has rarely conducted disruptive or destructive cyberattacks in the last 14 years in relation to the overall amount of cyber activity attributed to actors sponsored by the regime.
- North Korea primarily conducts computer network operations in Asia; 77.4% of the cyberattacks for which we have geographic region information took place in Asia.

- The top 5 industry verticals targeted by North Korean state-sponsored threat actors in descending order are government, cryptocurrency, media, traditional finance, and defense.
- Individual North Korean threat actor groups display differences in the purpose of their operations, their targets, and the geographic regions where they are most active.
- Kimsuky and APT37 primarily target entities in Asia, whereas Lazarus and its subgroups have a more dispersed targeting profile.
- In the near-term, North Korea will most likely continue to consistently conduct cyber-espionage and financially motivated cyberattacks to support its strategic goals.

Background

Cyberattacks attributed to threat actors sponsored by North Korea are an ever-increasing issue that continues to make headlines. Cybersecurity vendors regularly publish new technical analysis blog posts on North Korean activity, expert researchers post their latest findings on social media, and media continue to publish stories on large cryptocurrency heists pulled off by North Korean cyber operators. Considering all the ongoing North Korean cyber activity, it might seem surprising that North Korea does not publish a strategic doctrine on its cyber strategy. Moreover, little open-source literature exists on this topic; previous reports (1, 2, 3) have focused on the regime's cyber command structure, actions it might take in the event of a kinetic conflict, a limited selection of past cyber aggressions, and policy proposals for the US, South Korea, and the international community.

Recorded Future has previously covered North Korea's asymmetric strategy, outlining how the regime uses a combination of criminal activity, terrorist attacks, and nuclear weapons development to achieve 2 goals: perpetuation of the Kim regime and unification of the Korean peninsula under North Korean leadership.

The regime's cyber activities can also be grouped into its asymmetric strategy to achieve the above goals. North Korea has long recognized the values of science, technology, engineering, and math (STEM) education and nurturing promising domestic talent. An education program for gifted youth was set up in 1960, followed by the establishment of a similar program at Pyongyang's Pyongyang Senior Middle School No.1 (제1중학교) in 1984. The regime then reportedly sends the programs' top 100 students in computer science to Kim Il Sung National Defense University (김일군사대학) for further education. University students who excel are then sent to China and Russia where they are exposed to additional computer science education and access to the outside world. The students also gain exposure to technology not easily available in North Korea due to sanctions, such as servers, routers, and other networking equipment they will be expected to exploit in their future careers.

Limited information on the regime in open sources means that accurately counting the number of North Korean cyber operators is a difficult task. Estimates on the number of North Koreans working for the regime in roles that support cyber operations vary widely, from as little as 1,800 in 2017 to as high as 7,000 in 2019. It's important to note that North Korea also trains and deploys thousands of IT workers to earn revenue for the regime through online services and freelance platforms. While the relationship between these workers and those conducting cyber operations on behalf of the regime is unclear, it is likely that there is overlap between the 2 groups, further complicating official estimates.

As mentioned above, despite North Korea's long history of developing STEM programs to train its promising youth in computer science into a large force of cyber operators, little literature exists on how the regime employs these individuals. Rather than trying to discern North Korean cyber strategy from a one-thousand-foot view, such as by gathering the little public information available from official regime statements, defector interviews, and previous foreign visitors to the country, Insikt Group instead investigated the history of cyberattacks attributed to North Korean state-sponsored groups. By compiling a comprehensive data set of cyberattacks attributed to the regime, we hope to shed light on the regime's cyber strategy from a slightly different perspective than previous research — conducting a quantitative analysis focusing on the everyday activities of threat actors sponsored by North Korea, as captured through the large body of publicly available research in the cybersecurity community.

Methodology and Scope

This report looks at cyberattacks that have been publicly attributed to North Korean state-sponsored threat actors. Insikt Group tracks multiple North Korean state-sponsored threat actors using our Threat Actor and Malware Taxonomy. For the purposes of this report, however, we chose to use the most common public name for each threat actor so readers have the clearest understanding of which group we are referencing. Although the names of some groups vary among different cybersecurity vendors, we attempted to simplify them as much as possible, as the focus of this report is the regime's cyber strategy and not the differences between individual intrusion sets. We separated 2 Lazarus sub-groups because the industry tracks them as separate entities. The threat actors we tracked in this report are:

- Lazarus (also known as HIDDEN COBRA, Diamond Sleet, Labyrinth Chollima, TEMP.Hermit, and Black Artemis): an umbrella term covering several state-sponsored threat groups that have conducted espionage and financially motivated cyber activities on behalf of North Korea since at least 2009.
    - APT38 (also known as Bluenoroff, Stardust Chollima, BeagleBoyz, Sapphire Sleet, Cryptocore, Leery Turtle, Dangerous Password, TA444, and CryptoMimic): primarily conducts financially motivated cyber operations and has been active since at least 2014. The group has overlap with campaigns attributed to the Lazarus Group and some researchers classify it as a subgroup of Lazarus.
    - Andariel (also known as Silent Chollima, Stonefly, Onyx Sleet, Wassonite, and DarkSeoul): conducts both destructive and financially motivated cyberattacks against primarily South Korea-based entities and has been active since at least 2009. The group has overlap with campaigns attributed to the Lazarus Group and some researchers classify it as a subgroup of Lazarus.
- Kimsuky (also known as TEMP.Firework, Black Banshee, Velvet Chollima, Group G0094, Emerald Sleet, TA406, and Stolen Pencil): primary focus is cyber-espionage operations (with occasionally seen, financially motivated cyberattacks) since at least 2012.

- APT37 (also known as Group 123, Red Eyes, ScarCruft, NOKKI, Guemsong 121, Ricochet Chollima, KONNI, and InkySquid): gathers information to support North Korea's national interests, and has been active since at least 2012. The group's tactics, techniques, and procedures (TTPs), tools, and targets overlap with Kimsuky, likely due to similar missions between North Korean cyber operators.

As the focus of this report is discerning the overarching cyber strategy of the North Korean regime, we did not attempt to attribute threat actors — or break out specific strategies— to individual government organizations. And as researchers from the Center for Strategic & International Studies (CSIS) pointed out in their report on North Korea's cyber operations, due to the limited nature of open sources on the regime, the strict control of information inside North Korea, the potential for disinformation operations, and the echo chamber effect where unverified statements are taken as facts over time, Insikt Group judges assessments of threat actor attribution to specific government organizations in North Korea as having low confidence.

There is some debate in the cybersecurity community as to what is considered a cyberattack — some see network scanning as sufficient, while others require a complete intrusion where actions-on-objectives were achieved. For this study, Insikt Group used the National Institute for Standards and Technology's (NIST) cyberattack definition: "Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself".

The majority of the attacks analyzed come from cybersecurity vendor analyses (Recorded Future and others) and government notifications on North Korea-affiliated activity. In a small number of cases within the data set, only media reporting citing other sources was found. While we did attempt to verify the attribution of each attack reported by other sources, in many cases limitations in the amount of publicly shared data prevented us from completely and independently doing so. This issue of multiple reports on the same activity was also addressed. Cybersecurity vendors often publish reports on overlapping sets of activity due to differences in visibility on the threat actors. In cases where 2 or more reports on the same set of activity were discovered, if the additional report(s) expanded the scope of the activity, we included them in the data set. However, if the additional report(s) only analyzed already-reported activity (such as a deeper dive into a threat actor tool), while beneficial for threat research, we removed them from the data set as it was unclear if new activity was discovered.

We attempted to collect any publicly reported cyberattack attributed to North Korean cyber operators from 2009 onward, as this is the year of the first-known Lazarus Group activity, and the year the Reconnaissance General Bureau (정찰총국; RGB), North Korea's main intelligence agency, was supposedly formed. Cybersecurity vendors, incident responders, and government agencies often do not publicly provide their research on attacks. Therefore, the actual number of cyberattacks is likely multiple times higher than the data set we present here.

While this data set may not be comprehensive, we collected from a wide variety of sources in English, Korean, Mandarin Chinese, and Russian in order to have a data set large enough to produce insights, and where adding additional incidents would be unlikely to change the conclusions.

Threat Analysis

We compiled a total of 273 cyberattacks attributed to North Korean state-sponsored threat actors, classifying information regarding each event into the following categories:

- **Threat actor group:** The North Korean state-sponsored threat actor responsible for the cyberattack.
- **Target:** The targeted victim(s) in the cyberattack. This does not always mean that the objectives of the attack were successful; rather, that there was confirmed evidence an entity was targeted. Targets were not always as specific as an individual or organization name and sometimes were left more generic, such as “a Gmail user”, “a cryptocurrency user”, or “a job seeker”, among other generalizations.
- **Vertical:** The industry category of the target(s). Sometimes reports only mentioned the industry vertical of the targets and not the targeted entities themselves.
- **Country:** The country/countries of the targeted entity/entities or vertical(s).
- **Geographic region:** The geographic region of the targeted entity/entities or vertical(s).
- **Purpose:** The purpose of the cyberattack. Most of the cyberattacks in the data set have one purpose, but in some cases the activity has more than one purpose. For example, a campaign that exfiltrates system data and installs cryptomining software would be categorized as both espionage and financially motivated activity. Purpose was grouped into the following categories:
    - *Espionage:* Activity with the intent to gather information from victim(s) and use it for a specific purpose in line with the state’s strategic goals.
    - *Financially motivated:* Activity with the intent to steal currency or information that can help threat actors steal currency.
    - *Destructive:* Activity with the intent to destroy systems or render them inoperable.
    - *Disruptive:* Activity with the intent to cause a disruption or degradation of access to the targeted network or system.

We attempted to categorize each cyberattack into the above categories, but reports on threat actor activity do not always state these categories in an easy-to-digest format. In many cases, not every category could be filled out, as cybersecurity vendors do not always have or publicly provide all information regarding a cyberattack. Reports on activity attributed to North Korean cyber operators where none of the above categories could be filled out were not included in the analysis as they did not help answer our research question.

The data set of 273 cyberattacks begins in July 2009 and ends in May 2023. Readers will notice a significant increase in the yearly number of cyberattacks from 2016 onward. We believe the explanation for this is twofold: 1) collection has increased with the growth of the cyber threat intelligence industry, as more cybersecurity researchers, companies, and governments track North Korean state-sponsored actors; and 2) as mentioned in the background section, North Korea continues to train new cyber operators and, with its continued success in the cyber realm, it is likely there are more regime-sponsored threat actors conducting computer network operations today than 10 years ago.

There is also a dramatic increase in the number of cyberattacks in 2022 likely due to a greater volume of public reporting on Kimsuky activity, which is explored later in the report. We also note that 2023 appears to be on a similar trajectory of a much higher number of publicly reported cyberattacks than years prior to 2022.

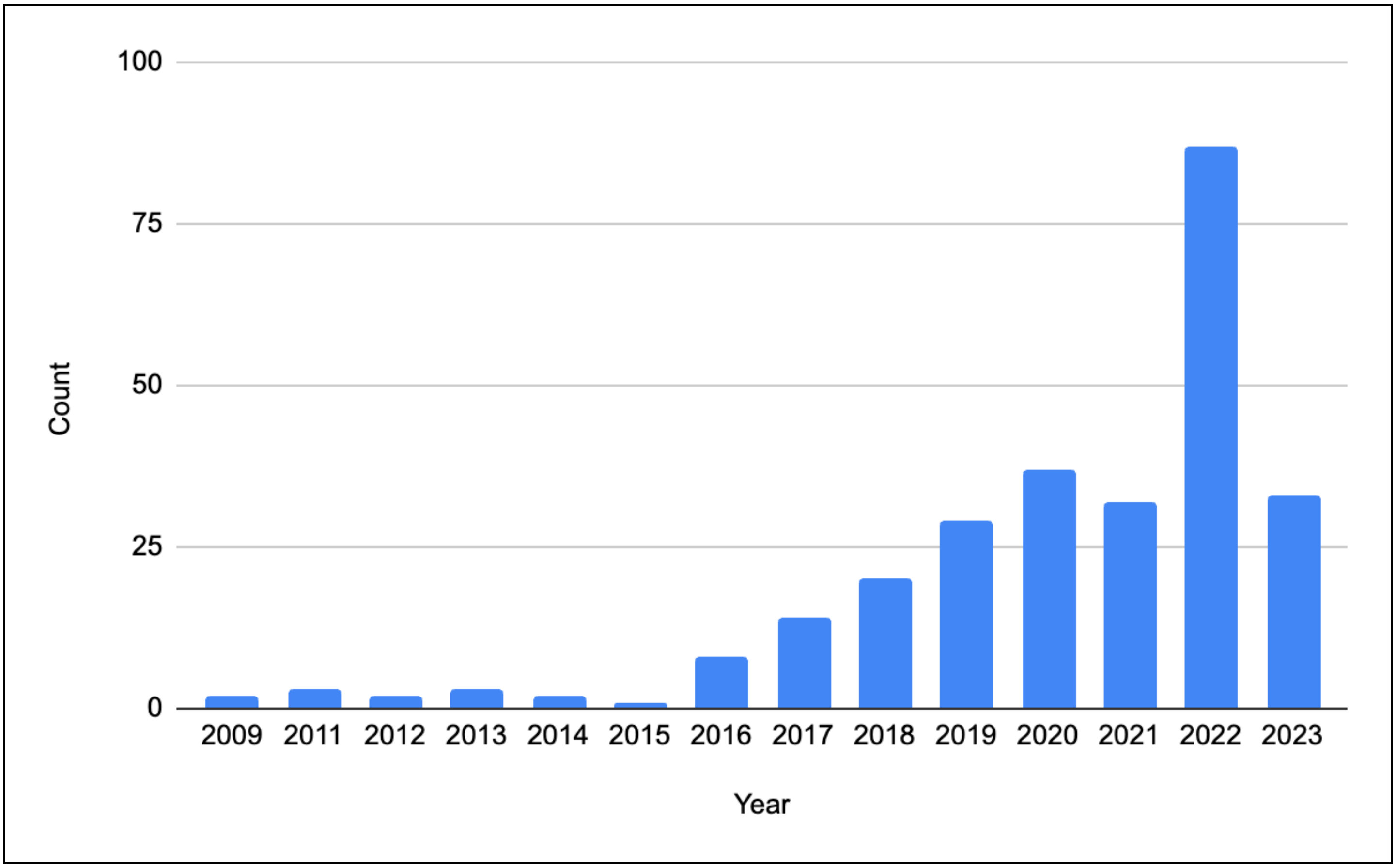


Figure 1: *Breakdown of cyberattacks attributed to North Korean state-sponsored actors by year (Source: Recorded Future)*

Threat Groups

Kimsuky was the most common threat group in the data set, comprising over 100, or 37.7%, of the attacks. We will explore the reason for Kimsuky's prevalence in the following sections of the report. Lazarus Group was the second-most prevalent group in the data set, followed by APT37; Lazarus's subgroups APT38 and Andariel appeared the lowest number of times in the data set. 25 events in the data set were not attributed to a specific threat group.

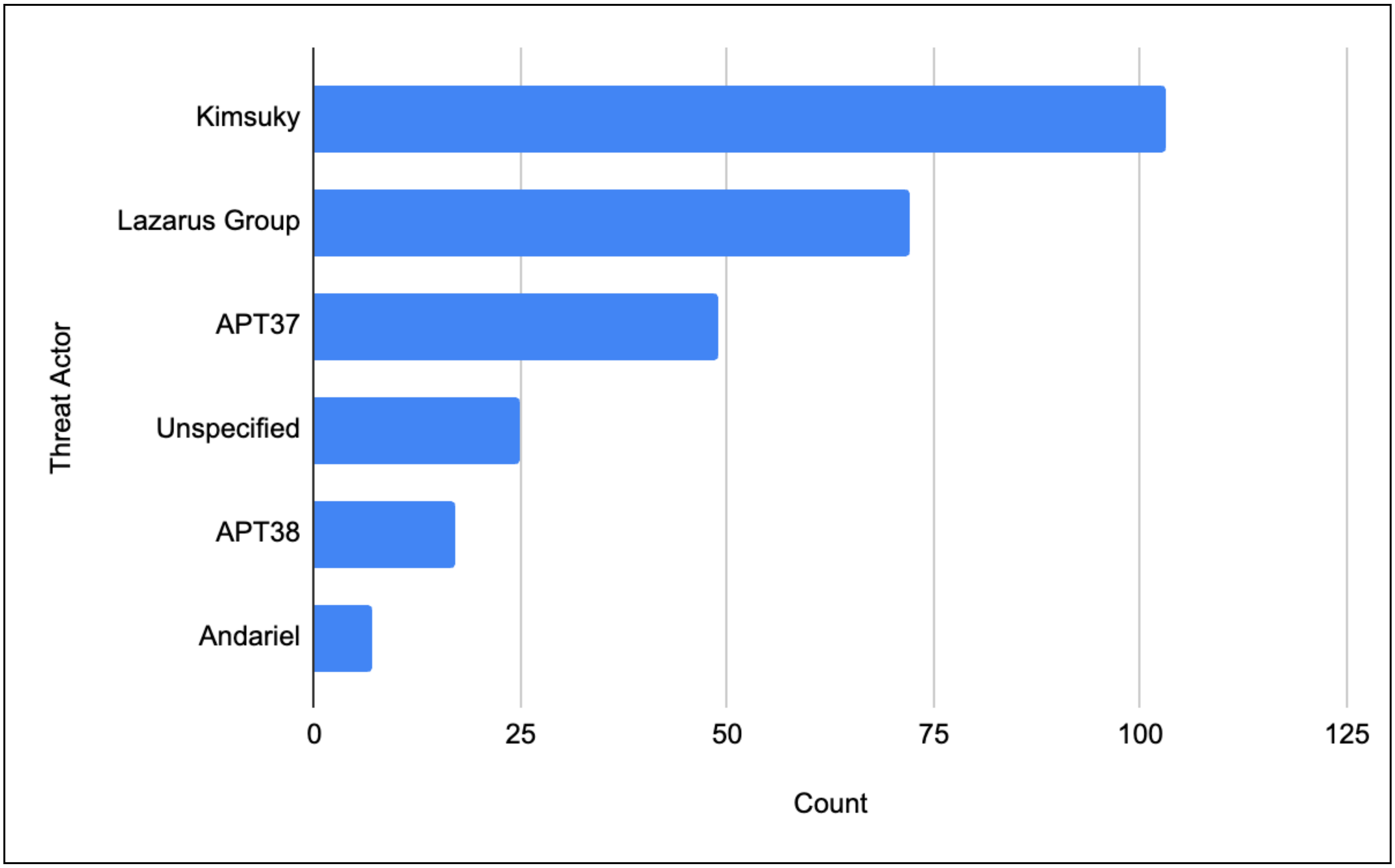


Figure 2: *Number of appearances of each North Korean state-sponsored threat actor in the data set (Source: Recorded Future)*

Analyzing the different threat groups' activity over time revealed that Kimsuky is also the most-active group year-to-year, followed by Lazarus Group and APT37. As mentioned earlier, as we have not compiled every cyberattack attributed to North Korea, these historical trends may look different with more data, but we are confident that we acquired a large-enough data set from which to make general inferences.

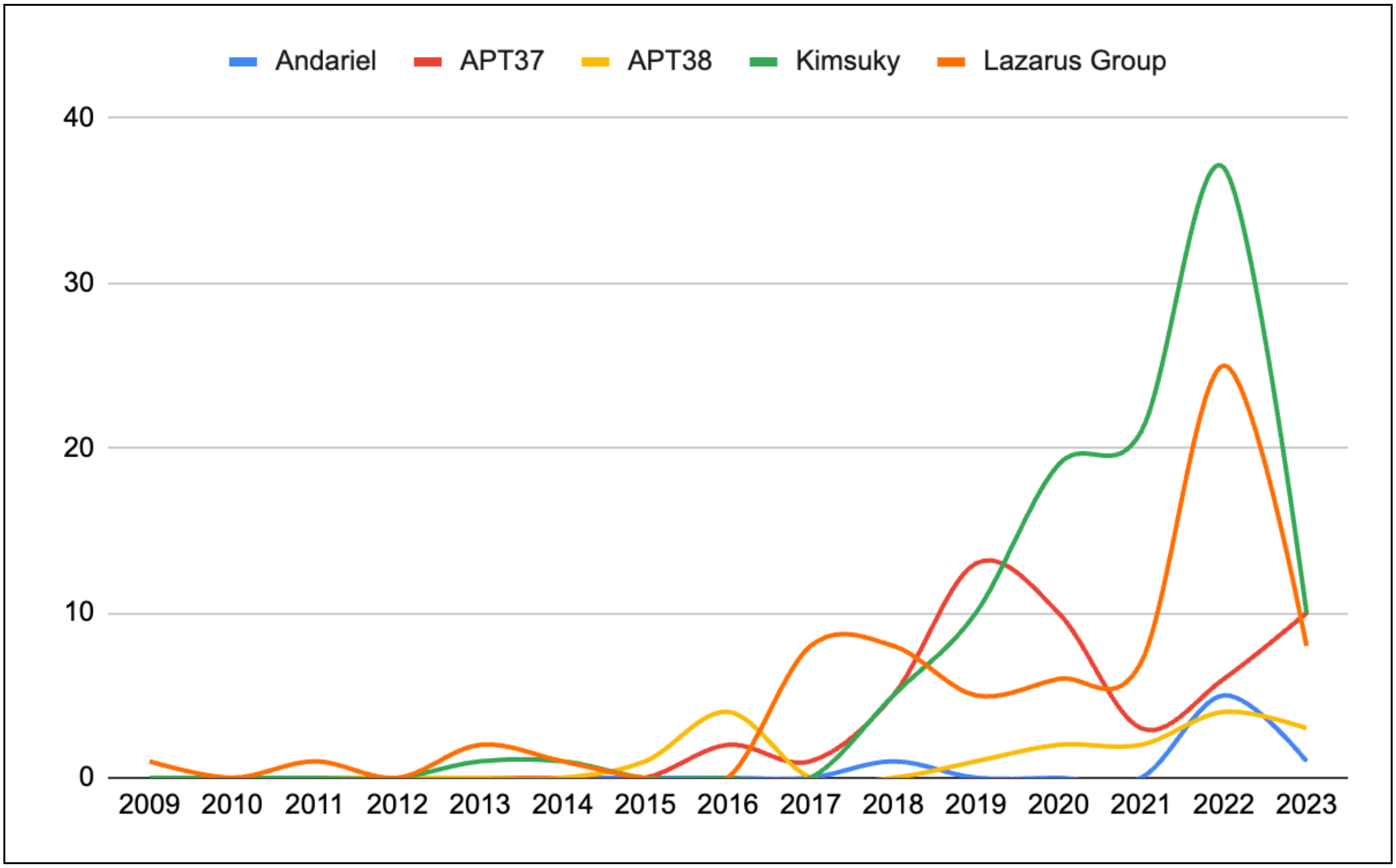


Figure 3: *Timeline of cyberattacks broken down by threat actor group. Note: Attacks for 2023 only go to May and, based on current projects, will likely be much higher than years prior to 2022. (Souce: Recorded Future)*

Victims and Industry Verticals

Of the 273 cyberattacks, 172 events had identified victims or targets in the report on the activity; the victims or targets were not mentioned in the other 101 events. As the victim list was almost as diverse as the number of events with victims in the data set, little additional insight could be gleaned from this data point.

As for industry verticals, we were able to classify some of the targeted victims into general industries, but 112 events did not specify the industry vertical of their victims. Note that this is higher than the number of attacks with unspecified victims — the reason is that in some cases, report publishers only mentioned a general victim group such as “users with a nexus to North Korea”. While this information is helpful for other forms of analysis, we were unable to classify instances such as the above into an industry vertical.

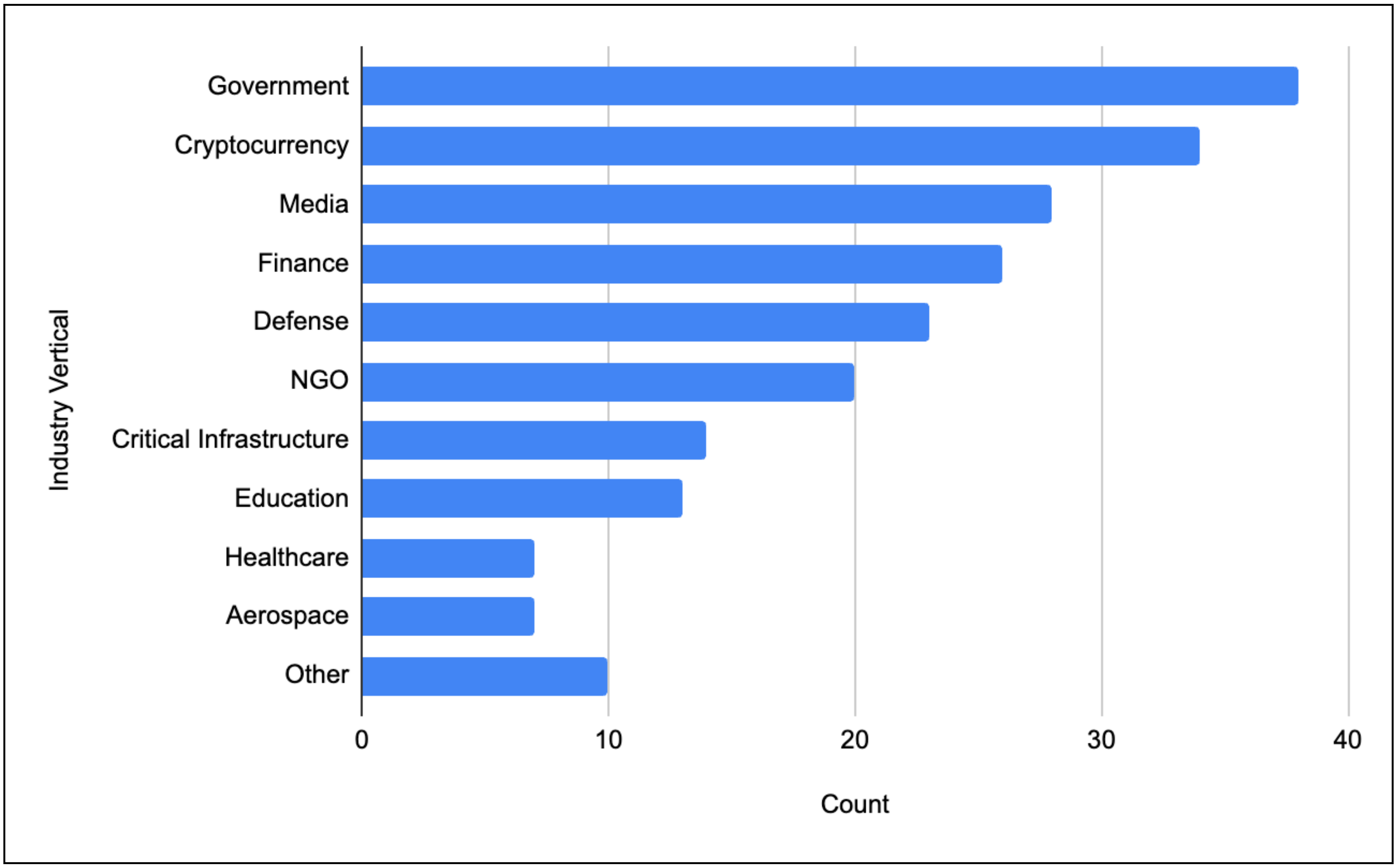


Figure 4: *Breakdown of industry verticals of victims targeted by North Korean state-sponsored threat actors (Source: Recorded Future)*

The most-targeted industry vertical was government, followed by cryptocurrency, media, finance, defense, and non-governmental organizations (NGOs). This ordering is not entirely unexpected, as the targeting of these industry verticals fits with the strategic objectives of conducting espionage (in the case of government, media, defense, and NGOs), and with gathering currency to compensate for the regime remaining under strict international sanctions (cryptocurrency and finance). Cryptocurrency targeting (1, 2) being the second-most-targeted demonstrates how successful North Korea has been in stealing cryptocurrency, as well as how much it likely relies on this source of cybercrime as a means to finance its activities. Less-frequently targeted industries include critical infrastructure, education, healthcare, and aerospace.

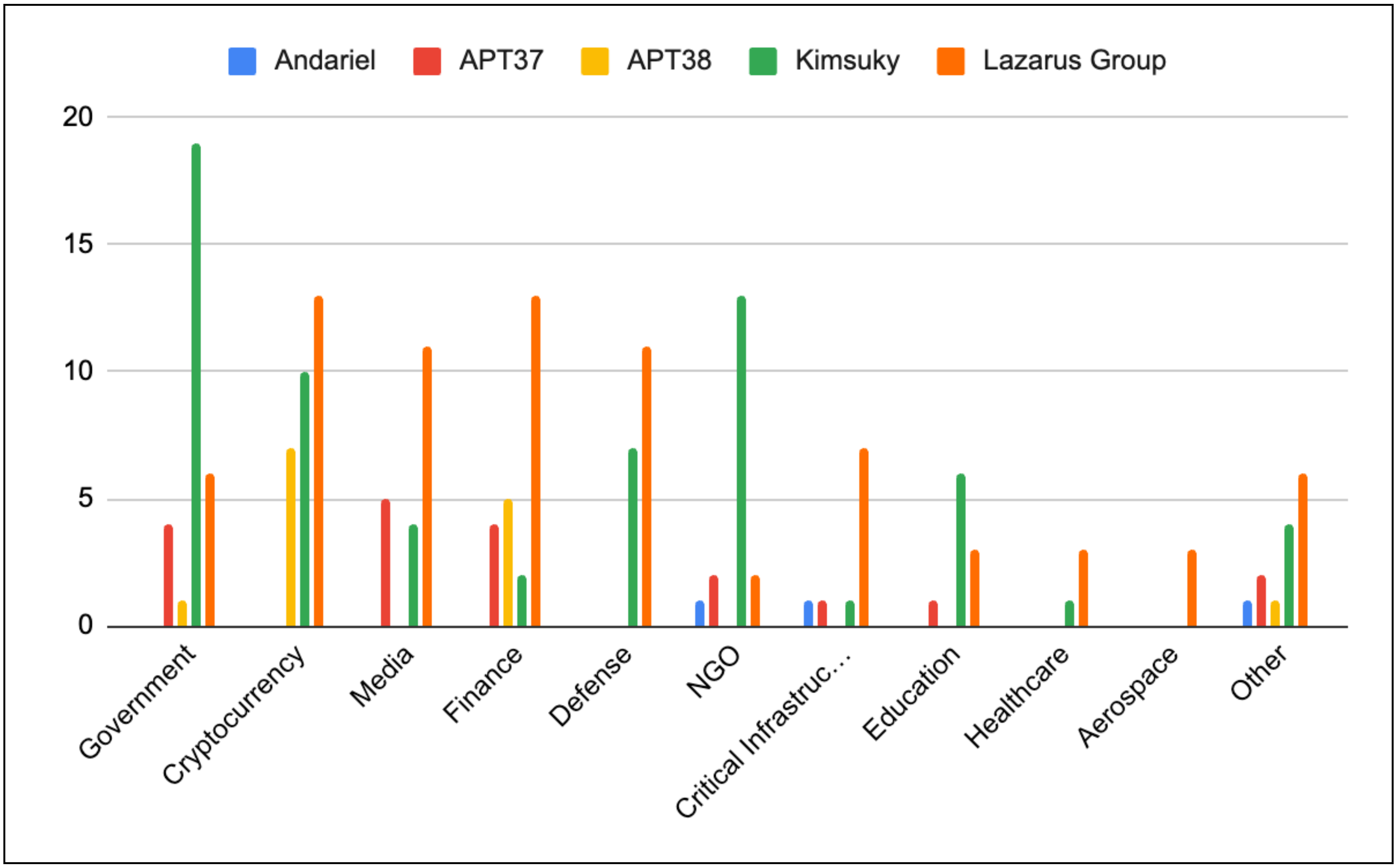


Figure 5: *Breakdown of industry verticals of victims grouped by North Korean state-sponsored threat actors (Source: Recorded Future)*

Note that the numbers are slightly different when breaking down industry vertical targeting by threat actor groups. This is due to the fact that some reported activity attributed to North Korea did not specify a group or we were unable to attribute a threat actor group. The data shows that threat actor groups have different targeting profiles:

- Kimsuky heavily focuses on government and NGO targets
- Lazarus Group has a diverse target set, but focuses slightly more on cryptocurrency and traditional finance
- APT38 conducts almost solely financially motivated cyberattacks
- Similar to Kimsuky, APT37 targets more government and media entities
- Andariel had the least amount of cyberattacks with known industries of the victims; its attacks were for information collection operations

Country and Geographic Region

80.5% of the events in the data set had information on the geographic region in which the activity took place. Of those, 77.4% took place in Asia, followed by North America and Europe at roughly 10% each, South America with 2%, and only 1 event in Africa. While several high-profile cyberattacks in North America and Europe have made headlines in the past, such as the Sony Pictures wiper incident in the US and WannaCry ransomware affecting the United Kingdom's (UK) National Health Service (NHS), the data shows that the overwhelming majority of North Korean state-sponsored activity remains targeted against entities in Asia.

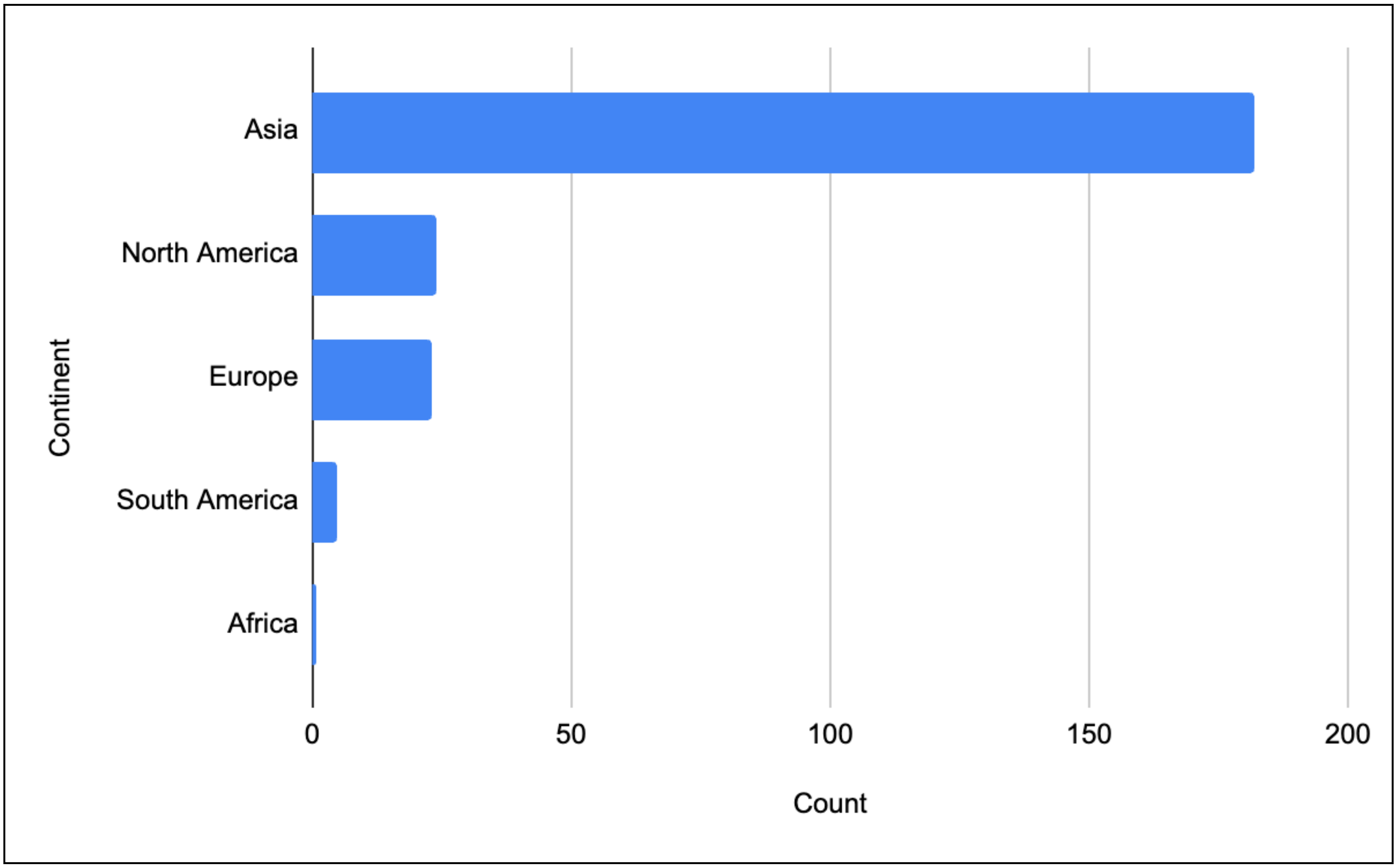


Figure 6: *Geographic region of targeted victims in the data set (Source: Recorded Future)*

Breaking down cyberattacks by country reveals even more-focused targeting. 29 individual countries were in the data set; however, of the events with country information, 65.7% of the target victims were located in South Korea, followed by 8.5% in the US. No other country accounted for more than 3% of the data set. While North Korea has a global reach in its cyber operations, its focus is still clearly on its 2 traditional enemies, South Korea and the US.

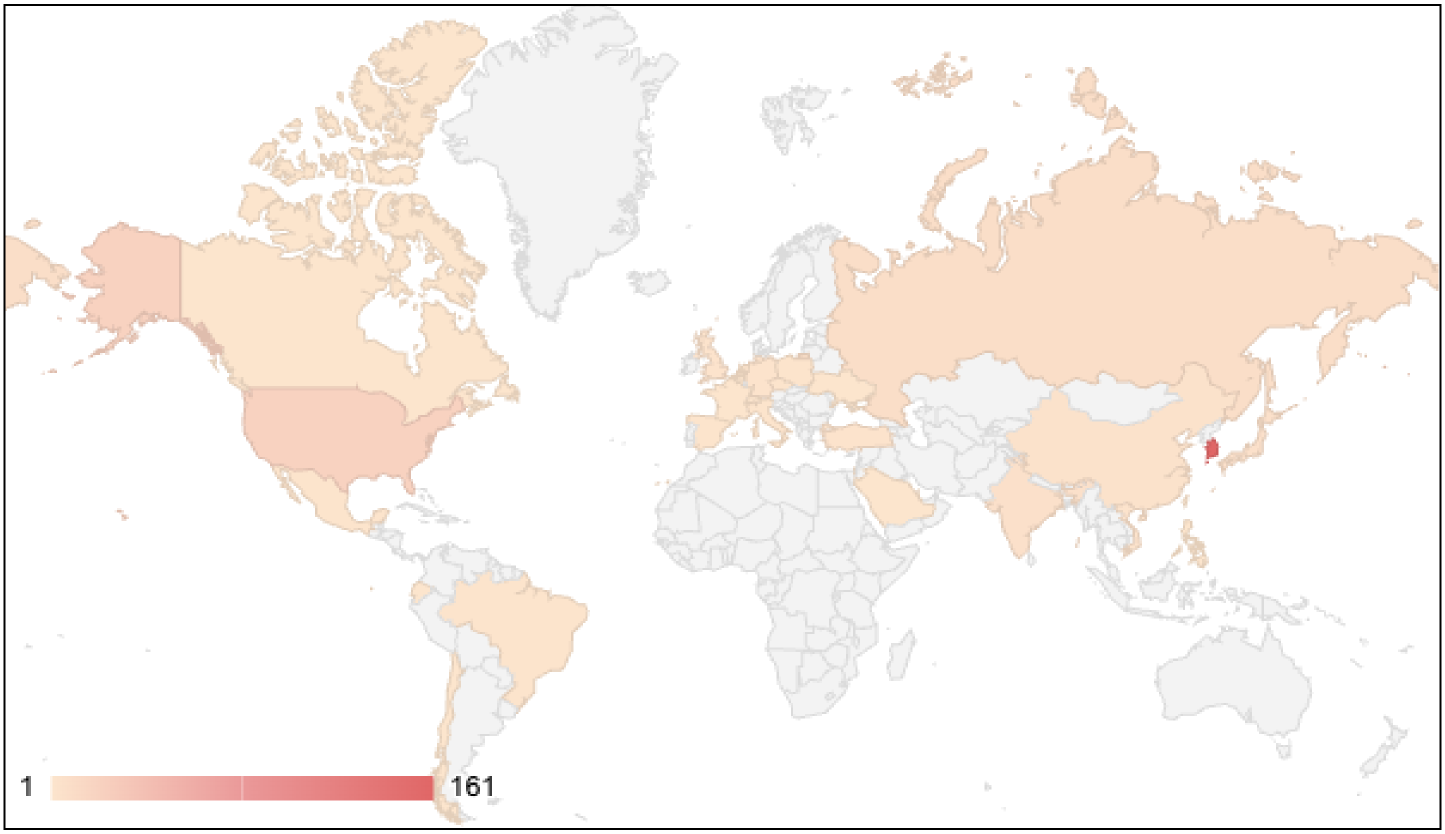


Figure 7: *Country of targeted victims in the data set — the country with the highest number of victims (161) was South Korea (Source: Recorded Future)*

When looking at the geographic breakdown of target victims by threat actor, every group was most active in Asia, with the majority of Kimsuky's and APT37's targets or victims based in Asia. Lazarus Group's geographic breakdown was more even across regions, with higher targeting in North America and Europe than South America and Africa. Lazarus Group and its subgroups appear to have a more worldwide purview, whereas Kimsuky and APT37 focus almost exclusively on targets in Asia, the overwhelming majority of which are in South Korea. The reason for the differences in activity is discussed further below.

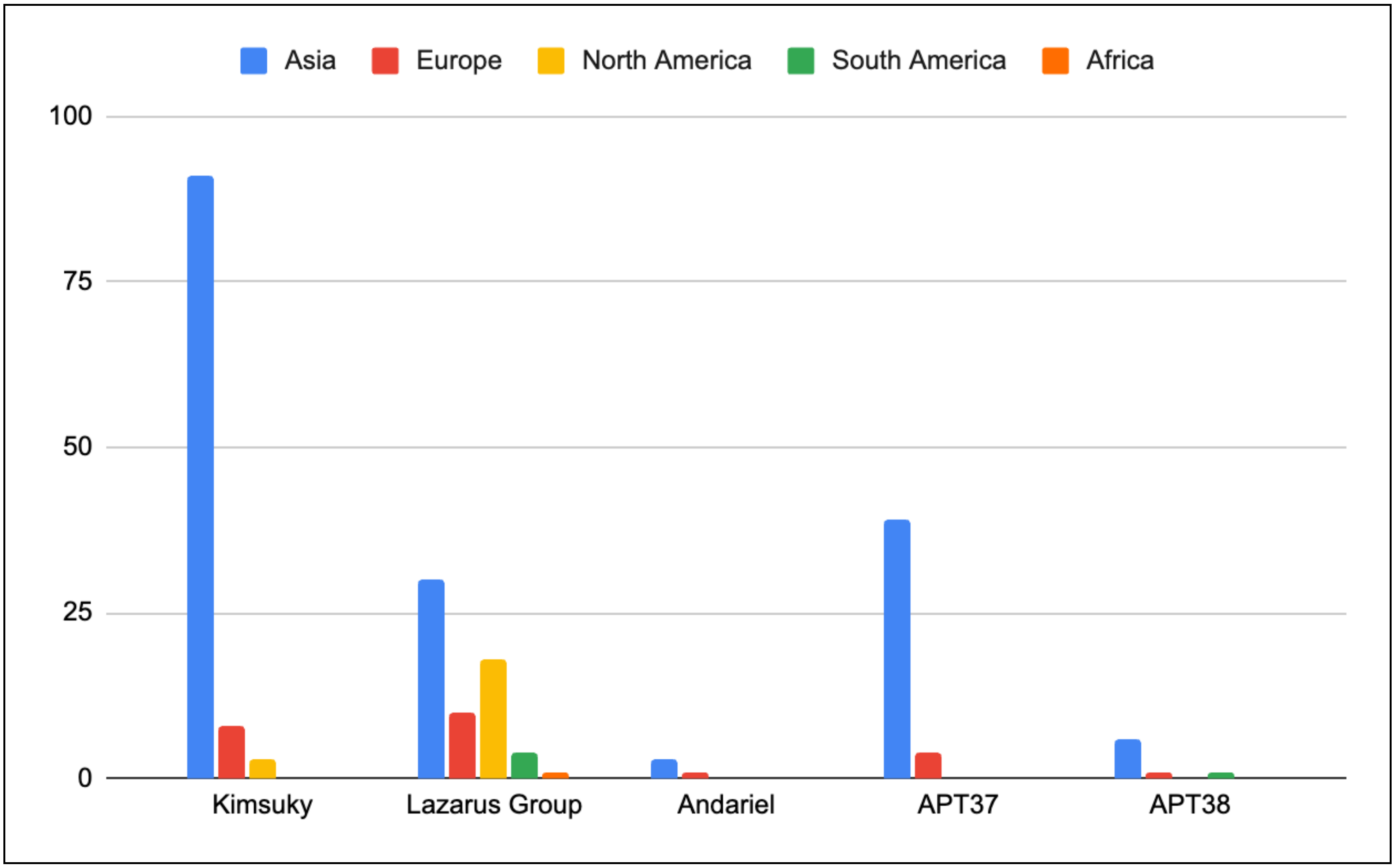


Figure 8: *Breakdown of geographic region by threat actor group (Source: Recorded Future)*

Purpose

Similar to the breakdown of geographic regions, the purpose of cyberattacks in the data set overwhelmingly falls under 1 category: espionage, followed by financially motivated activity and a minor number of disruptive and destructive cyberattacks. Again, cyberattacks attributed to Kimsuky and APT37 are overwhelmingly in the top category of espionage, with a smaller amount of financially motivated activity, and, in the case of APT37, 1 instance of a destructive cyberattack. Events attributed to Lazarus Group are more diverse in purpose, with a higher share of financially motivated cyberattacks, especially among its subgroups Andariel and APT38.

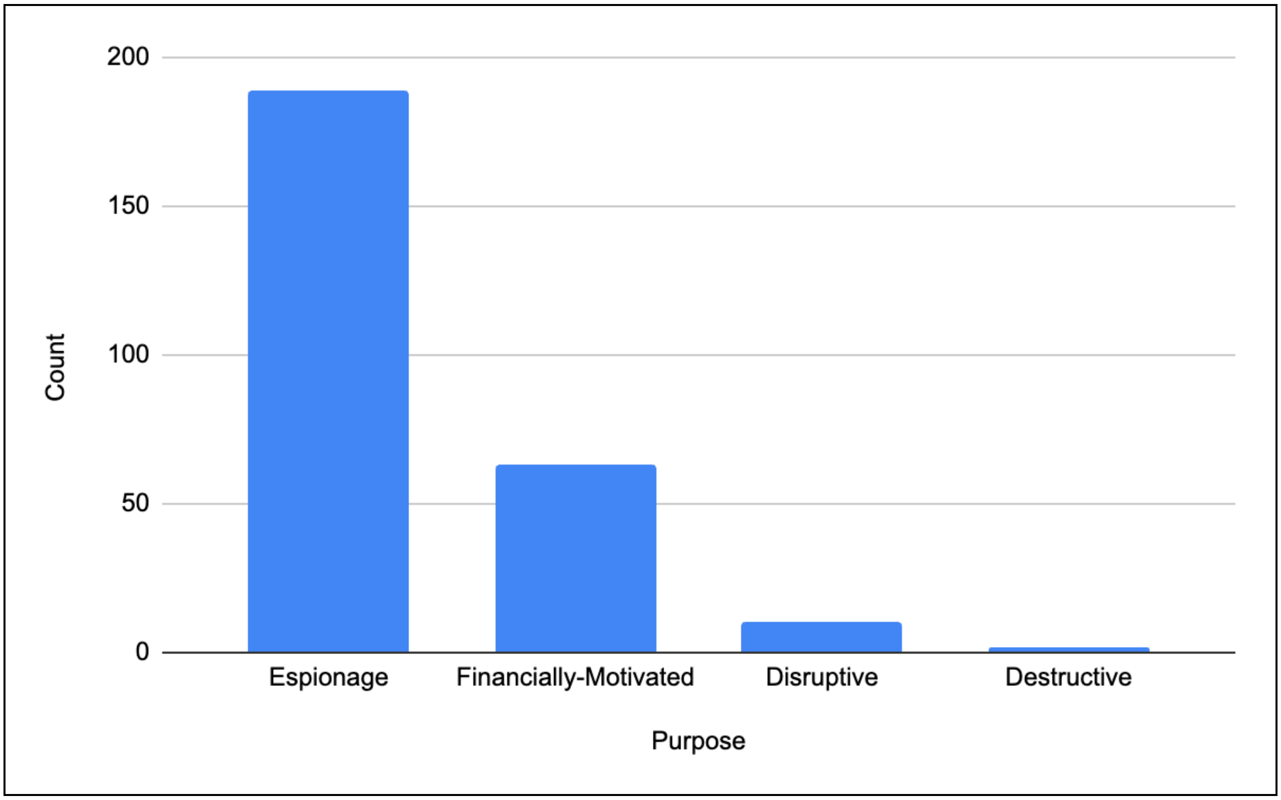


Figure 9: *Breakdown of the purpose of cyberattacks (Source: Recorded Future)*

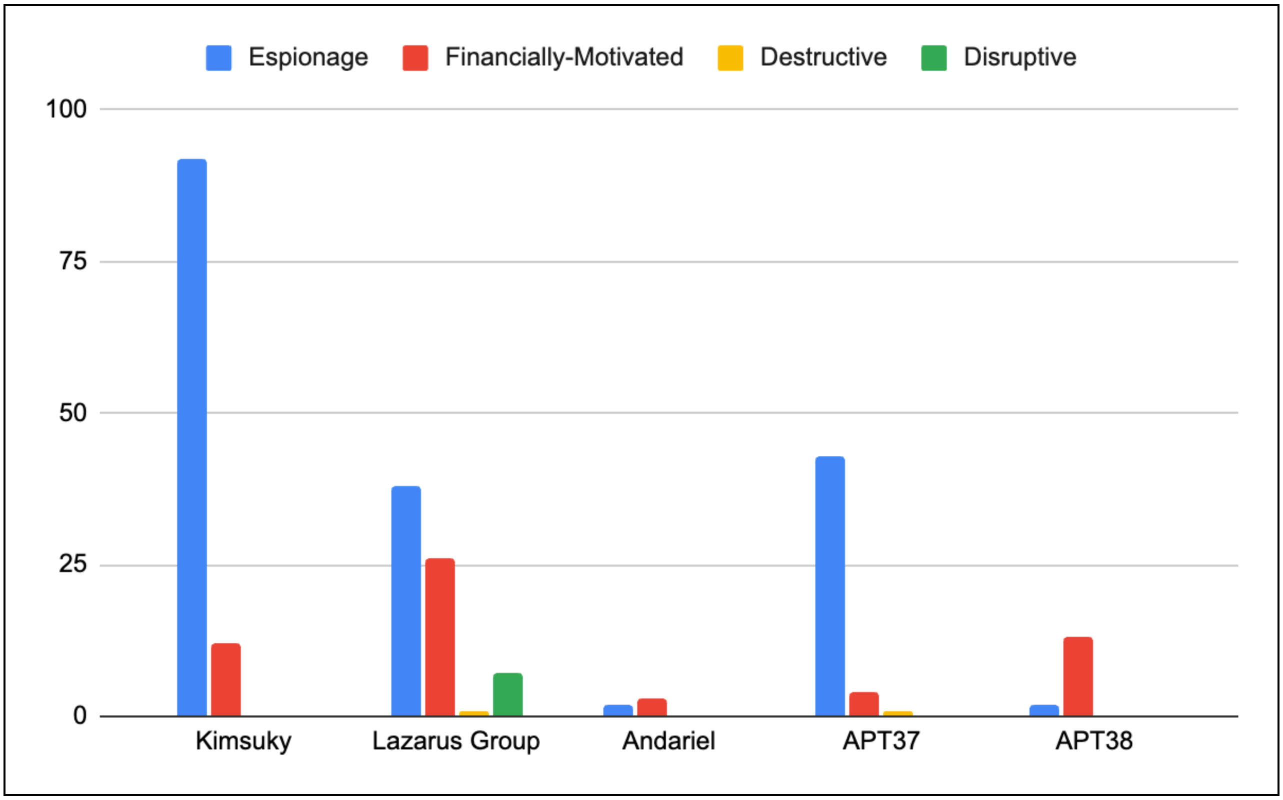


Figure 10: *Breakdown of the purpose of cyberattacks by threat actor group (Source: Recorded Future)*

Taking all of the above into account, we can see that despite the widespread media coverage linked to North Korea's theft of cryptocurrency or other financial assets and involvement in destructive attacks, the regime is primarily engaged in cyber espionage, with financially motivated activity an increasingly important but secondary goal. Disruptive and destructive cyberattacks are rarely seen in the data, and while others have analyzed how the regime could use these types of cyberattacks to asymmetrically conduct operations below the threshold where a retaliatory use of force would be required, the regime appears to rarely use them under current circumstances. Rather, North Korea's leadership appears to be much more interested in learning about what others think of them, gathering information that can help them develop nuclear and ballistic missile technology, and stealing money to fund their regime.

North Korea is also primarily active within its local region, choosing to focus on its neighbor, South Korea, with occasional cyberattacks against its other longtime enemy, the US. The operators behind Kimsuky and APT37 appear to be mostly conducting espionage against entities in Asia, while Lazarus and its subgroups are called in for operations that are more diverse in scope and global in nature. This is likely due to a separation in units within the North Korean government. Researchers at Mandiant linked Kimsuky activity to the 5th Bureau of the RGB, which is in charge of Inter-Korean Affairs, and Lazarus Group and its subgroups to the 3rd Bureau of the RGB, which is responsible for foreign intelligence collection. Our analysis is consistent with that assessment.

Further Research

While the research presented here is helpful in understanding North Korea's cyber strategy, there are areas for further research. Our data set was limited to the data we collected, both from our own internal research and what was available in open sources. Others with a more comprehensive data set not available in open sources, both in terms of the amount of cyberattacks and the level of available detail, may be able to draw additional conclusions regarding North Korea's cyber strategy. A more granular analysis of TTPs, tooling and malware variants, and infrastructure usage across time, region, and threat group may reveal additional trends helpful from an operational context for decision makers. The purpose of each cyberattack could also be explored further if additional data were available, such as answers to the following questions: What kind of information does the regime value stealing? Has it changed over time? Does it vary by threat group? The regime has taken a larger interest in stealing cryptocurrency in recent years to fund itself, but how has this changed over time? Has the focus shifted entirely from stealing cash to stealing cryptocurrency, or are there groups that still attempt to steal from financial institutions and individuals?

Outlook and Mitigations

North Korea's cyber strategy is predictable based on observations of past activity, as detailed in this report. The DPRK values information collection and financial resource gain over more attention-gathering activities, such as disruptive and destructive cyber operations. North Korea's operations are overwhelmingly conducted against targets in South Korea, with a smaller amount targeting US-based entities. However, victims from other regions of the world may occasionally find themselves targeted by a North Korean state-sponsored threat actor. The two primary objectives, espionage and financial theft, support the regime's broader goals of securing the leadership position of the Kim family and collecting information against its longtime adversary, South Korea, in order to better anticipate the operational environment during heightened tensions or conflict.

Government agencies, reporters, and NGOs with a nexus to North Korea should be more vigilant, as well as defense contractors and aerospace companies supporting US, South Korean, or other allied nations. Cryptocurrency organizations should place extra emphasis on defending against North Korean cyberattacks because of the high proportion of targeting against this industry in our data set and in open sources. In both the short and long run, Insikt Group expects the regime to continue to consistently conduct cyber-espionage and financially motivated cyberattacks to support its strategic goals, especially as the regime remains under international sanctions. However, North Korea may conduct the occasional destructive or disruptive cyberattack, especially during a time of heightened geopolitical tensions, particularly in the East Asian region.

For organizations and entities that may be of higher interest to North Korean threat actors, such as aerospace, defense contractors, NGOs, media, academia, defectors, and other entities with a nexus to North Korea, we recommend the following mitigations:

- Train employees on the types of phishing emails they may be sent by North Korean threat actors and teach them how to report suspected phishing emails, including conducting regular, randomized phishing exercises.
- Keep all software and applications up to date, especially 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 (such as through a 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.

For cryptocurrency organizations, we recommend the following mitigations:

- Users should always check the legitimacy of the domain on which they enter credentials, even if the website contains credible features like a 2-factor authentication (2FA) relay page and a customer chat.
- Note that legitimate emails received from cryptocurrency platforms and exchanges will always come from the platform's main domain.
- Cryptocurrency users should use cold storage and hardware wallets that are disconnected from the internet to store their cryptocurrencies, and enable multi-factor authentication (MFA) for any accounts on cryptocurrency platforms.
- Current or prospective employees at cryptocurrency companies should remain aware of social engineering campaigns, as being compromised by such campaigns could lead to the wider compromise of their employers, potentially leading to the draining of funds for thousands of customers.
- Cryptocurrency users should be wary of social media communications from unknown phone numbers or accounts that attempt to build an emotional rapport. Scammers conducting romance scams typically attempt to create an emotional bond with victims for several weeks before displaying any visible signs of malicious activity, such as requesting financial assistance or promoting an investment opportunity.
- Cryptocurrency users should remain vigilant for any social media accounts (even verified celebrities or corporate accounts) promising to double or multiply tokens sent to their wallet.
- Cryptocurrency users should always conduct due diligence before investing in a specific token or project. Users should measure the project's transparency, including:
  - Whether the projects' developers have their identities public (also called "fully doxxed")
  - The project's transparency and frequency in communications
  - Whether the project publishes its financial records
  - Whether the project has a clear plan or roadmap
  - Whether the project has a clear use case
- Cryptocurrency projects typically publish a manifesto outlining the project's functioning and plans, known as a "white paper". Investors should always read and consider these documents and look for any signs of inauthentic activity, including spelling and grammar mistakes as well as technical inconsistencies.
- Cryptocurrency and NFT users who leverage in-browser cryptocurrency wallets like MetaMask should be wary of any unverified projects or pages asking to connect to their wallets without prior inspection.
- NFT users should always check the legitimacy of NFTs before purchasing, and stay vigilant for platform communications around technical issues.
- Users should only purchase NFTs on platforms they trust.

About Insikt Group®

Insikt Group is Recorded Future's threat research division, comprising analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence on a range of cyber and geopolitical threats that reduces risk for clients, enables tangible outcomes, and prevents business disruption. Coverage areas include research on state-sponsored threat groups; financially-motivated threat actors on the darknet and criminal underground; newly emerging malware and attacker infrastructure; strategic geopolitics; and influence operations.

About Recorded Future®

Recorded Future is the world's largest intelligence company. Recorded Future's cloud-based Intelligence Platform provides the most complete coverage across adversaries, infrastructure, and targets. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future provides real-time visibility into the vast digital landscape and empowers clients to take proactive action to disrupt adversaries and keep their people, systems, and infrastructure safe. Headquartered in Boston with offices and employees around the world, Recorded Future works with more than 1,600 businesses and government organizations across more than 70 countries.

Learn more at recordedfuture.com and follow us on Twitter at @RecordedFuture