



| Flash |

Cybersecurity Risk Ahead of South Korea Elections

F-2024-04-09a

Classification: TLP:CLEAR

Criticality: High

Intelligence Requirements: Geopolitical, Physical Security, Terrorism

April 9, 2024

Scope Note: ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were **identified prior to 12:00 PM (EDT) on April 8, 2024**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | Cybersecurity Risk Ahead of South Korea Elections

> Key Findings

- ZeroFox has not identified any evidence of a coordinated cyber campaign targeting South Korea's National Assembly elections.
- ZeroFox anticipates that threats to South Korean firms will continue irrespective of the elections, likely due to the country's growing ties with the United States and Japan.
- South Korea has developed closer economic ties with the United States to restrict sales of advanced technology to China, while it has deepened ties with Japan over their shared concern about the military threat posed by China and North Korea.
- The North Korean security threat is largely a secondary concern for South Korean voters, who are more focused on domestic issues such as the cost of living, low fertility rates, and party corruption.
- The likelihood of a positive electoral outcome for South Korea's adversaries is possibly behind the lack of coordinated nation-state cyber campaigns targeting the April 10 elections.

| Overview

South Korea will hold elections to determine the composition of its 300-member legislative National Assembly on April 10, 2024.¹ The National Assembly is currently dominated by the opposition Democratic Party of Korea (DPK), which has left President Yoon Seok-Yeol of the conservative People Power Party (PPP) unable to advance his economic agenda.² Most voters are very likely treating this election as a referendum on President Yoon.

- Voters are very likely to be focused on domestic cost-of-living issues, South Korea's low fertility rate, and corruption linked to the two leading parties.³
- Foreign policy issues regarding an increasingly aggressive North Korea and South Korea's growing ties with the United States and Japan are secondary voting concerns.
- PPP is a minority in the National Assembly; if PPP fails to regain control of the National Assembly, President Yoon will likely be a lame duck until his term ends in 2027.

Polling currently suggests that the PPP will remain in the minority and the opposition may have enough seats to impeach Yoon. The most likely outcome is a divided parliament that continues to restrict PPP policies. Polls indicate that PPP and DPK will likely remain the largest parties; however, with both parties struggling over corruption allegations, this election could also see the National Assembly become more divided, with third parties expected to pick up as many as 20 percent of the seats.⁴

- PPP has had greater success in the foreign policy arena, where relations have been re-established with Japan after decades of strain and strengthened with the United States.
- A divided parliament that weakens President Yoon likely appeals to South Korea's geopolitical adversaries. Yoon is considered "hawkish" on North Korea; during his term, he has expanded economic and military ties with Japan and the United

¹ [hXXps://www.stimson\[.\]org/2024/south-koreas-2024-legislative-election-primer/](https://www.stimson.org/2024/south-koreas-2024-legislative-election-primer/)

² [hXXps://www.electionguide\[.\]org/elections/id/4195/](https://www.electionguide[.]org/elections/id/4195/)

³

[hXXps://apnews\[.\]com/article/south-korea-election-hot-issues-green-onions-860cbb313a4afb3776fd87052a051c9d](https://apnews[.]com/article/south-korea-election-hot-issues-green-onions-860cbb313a4afb3776fd87052a051c9d)

⁴ [hXXps://www.rfi\[.\]fr/en/international-news/20240408-south-korea-set-to-vote-in-crucial-parliamentary-election](https://www.rfi[.]fr/en/international-news/20240408-south-korea-set-to-vote-in-crucial-parliamentary-election)

States aimed at containing both the military threat posed by North Korea and the economic threat posed by China. A divided assembly appeals to North Korean and Chinese threat actors because it would require more time spent debating domestic issues instead of foreign policy, which is increasingly anti-China and North Korea under President Yoon.⁵

Cyber Campaigns

ZeroFox has identified no evidence of significant cyber threats from cybercriminals, hacktivists, or other politically motivated actors intended to specifically affect the elections. However, South Korea's geopolitical rivals have targeted South Korean-based entities in the past year. It is more likely than not that these threat actors will continue attacks before, during, and after the election period, but they are very unlikely to be able to interfere with the result.

- Cyber campaigns aimed at disruption are commonly observed surrounding high-profile elections, particularly in the months preceding them. While China has a history of attempting to influence elections in the region—most recently in Taiwan's January elections with disinformation and voter-manipulation campaigns—ZeroFox did not identify any such campaigns relating to South Korea's upcoming elections.
- ZeroFox assesses that the threat posed by Chinese-backed actors is low but cannot rule out the possibility that actors may use synthetically generated content to boost their preferred candidates and parties or to otherwise harm candidates that adopt anti-China policies.⁶ Microsoft recently issued a warning that a Chinese-backed group called Storm 1376 may seek to hone generative artificial intelligence (AI)-enabled election interference techniques used in the Taiwan election during the upcoming elections in South Korea, India, and the United States.⁷

The lack of a large-scale, Chinese-backed cyber campaign is likely due to the mid-term National Assembly elections being focused on domestic issues unique to South Korea and because current polling indicates the election will likely lead to a favorable political

⁵ [hXXps://www.cfr.org/blog/yoon-revitalizing-seventy-year-old-alliance-taking-political-chances](https://www.cfr.org/blog/yoon-revitalizing-seventy-year-old-alliance-taking-political-chances)

⁶ [hXXps://www.theguardian.com/technology/2024/apr/05/china-using-ai-disrupt-elections](https://www.theguardian.com/technology/2024/apr/05/china-using-ai-disrupt-elections)

⁷ [hXXps://blogs.microsoft.com/on-the-issues/2024/04/04/china-ai-influence-elections-mtac-cybersecurity/](https://blogs.microsoft.com/on-the-issues/2024/04/04/china-ai-influence-elections-mtac-cybersecurity/)

outcome for South Korea's primary geopolitical adversaries. High-profile interference from a foreign actor like North Korea or China could provide the major parties with a distraction from domestic issues surrounding the cost of living or large protests.

- ZeroFox assesses that the seeming disinterest in conducting a large-scale disinformation campaign is likely due to the anticipated low political returns on an expensive effort, especially when current polling suggests threat actors will obtain their preferred election outcome.

Election Integrity

Direct cyber interference is highly unlikely during the voting process, primarily because paper ballots are used in South Korean elections. However, the voter registration process and ballot-counting systems, which rely on electronic devices, remain vulnerable to cyberattacks.

- In 2023, the National Intelligence Service (NIS) of South Korea and the internet-safety watchdog Korea Internet and Security Agency disclosed that vulnerabilities in the National Election Commission (NEC) network could allow North Korean hackers to penetrate the network "at any time."⁸ However, no evidence of infiltration was observed.
- Classified NEC documents were compromised in 2021 after North Korea-backed hacker group Kimsuky (also known as Velvet Chollima, Black Banshee, THALLIUM, or Emerald Sleet) breached the NEC network after infecting a system with malware.⁹
- Any valuable data obtained during the 2021 hack was likely utilized by North Korean threat actors during the 2022 presidential election, which Yoon won.

Election Adjacent Targeting

ZeroFox notes that South Korea's geopolitical rivals—particularly North Korea and China—have targeted South Korea-based entities in the past year. It is more likely than not that these countries will continue attacks before, during, and after the election period, but they are very unlikely to be able to interfere with the result. The selection of the

⁸ [hXXps://en.yna\[.\]co\[.\]kr/view/AEN20231010004001315](https://en.yna[.]co[.]kr/view/AEN20231010004001315)

⁹ [hXXps://koreatimes\[.\]co\[.\]kr/www/nation/2023/10/356_360811.html](https://koreatimes[.]co[.]kr/www/nation/2023/10/356_360811.html)

entities recently targeted by North Korean and Chinese-based threat actors is likely at least partially inspired by geopolitics.

While a series of well-documented escalatory activity by North Korea-linked actors has been observed in 2024, South Korean voters have traditionally been less concerned with the threat posed by North Korea, and the 2024 military maneuvers rank low in voter issues.

- On February 14, 2024, North Korean threat actors were able to access South Korean President Yoon's emails and text messages after breaching a system belonging to the president's aide.¹⁰ ZeroFox has not been able to identify the specific nature of the data stolen. The timing of the hack coincided with increasingly aggressive North Korean rhetoric and military drills. The targeting of Yoon may have been designed to steal information on South Korean policy towards North Korea or its ally, China.
- In January 2024, North Korean leader Kim Jong Un declared that North Korea would no longer seek peaceful reunification with South Korea and that it would be a mistake to engage in diplomacy. This significant declaration reversed decades of stated policy that one day the two Koreas would peacefully reunify.¹¹
- North Korean missile launches have also increased in number and sophistication in 2024.¹²

South Korea, like many of its neighbors, is a leading exporter of electronic goods like smartphones and laptops, as well as the advanced semiconductor chip technologies that power these products. ZeroFox has observed multiple instances of actors linked to adversarial nation-states targeting semiconductor firms in the last year. Chinese and North Korean threat actors are likely seeking to obtain information about advanced technologies being withheld from them via cyber espionage campaigns.

- North Korean hacking groups attacked two South Korean semiconductor chip-making equipment manufacturers in late 2023 and early 2024. The hackers reportedly stole product design drawings and facility photographs.

¹⁰ [hXXps://www.bbc.com/news/business-68476035](https://www.bbc.com/news/business-68476035)

¹¹ [hXXps://www.bbc.com/news/world-asia-67990948](https://www.bbc.com/news/world-asia-67990948)

¹² [hXXps://www.cnn.com/2024/04/01/asia/north-korea-missile-test-intl-hnk-ml/index.html](https://www.cnn.com/2024/04/01/asia/north-korea-missile-test-intl-hnk-ml/index.html)

- In October 2023, Chinese cyber espionage campaigns targeted semiconductor companies in Taiwan, Hong Kong, and Singapore with backdoors.¹³ While this hack targeted only countries where Mandarin is widely spoken, it likely contributed to South Korea's concern that Chinese technology used in South Korean systems could facilitate cyber espionage campaigns.
- In September 2023, South Korean officials discovered malware in China-sourced weather equipment procured by South Korea's weather agency (NIS). NIS subsequently launched an investigation to determine whether China-sourced electronics used by other government agencies involved similar cyber hazards.¹⁴
- China-supplied electronics parts pose a threat to the South Korean technology industry, including the semiconductor industry.

It is highly likely that the targeting of South Korean semiconductor producers by threat actors is tied to South Korea abiding by U.S. trade restrictions. South Korea is almost certainly key to the success of the U.S. Chips and Science Act (CHIPS Act) because it is one of the leading producers of semiconductor chips, along with Japan and Taiwan.¹⁵ Under the Yoon administration, South Korea has closely aligned with U.S. trade restrictions on limiting sales of advanced semiconductor chips to China.

- The United States has pursued the policy under its CHIPS Act, which seeks to bar China from using the most advanced forms of chips for military purposes.
- The technology is also being withheld from North Korea, with South Korea in particular concerned that the chips could be used to advance North Korea's weapons programs.

ZeroFox anticipates that threats to South Korean technology firms will continue irrespective of the elections; any targeting of these firms during the election cycle is likely tied to broader cyber espionage campaigns rather than to the election itself.

¹³

[hXXps://blog.electiciq\[.\]com/chinese-state-sponsored-cyber-espionage-activity-targeting-semiconductor-industry-in-east-asia](https://blog.electiciq[.]com/chinese-state-sponsored-cyber-espionage-activity-targeting-semiconductor-industry-in-east-asia)

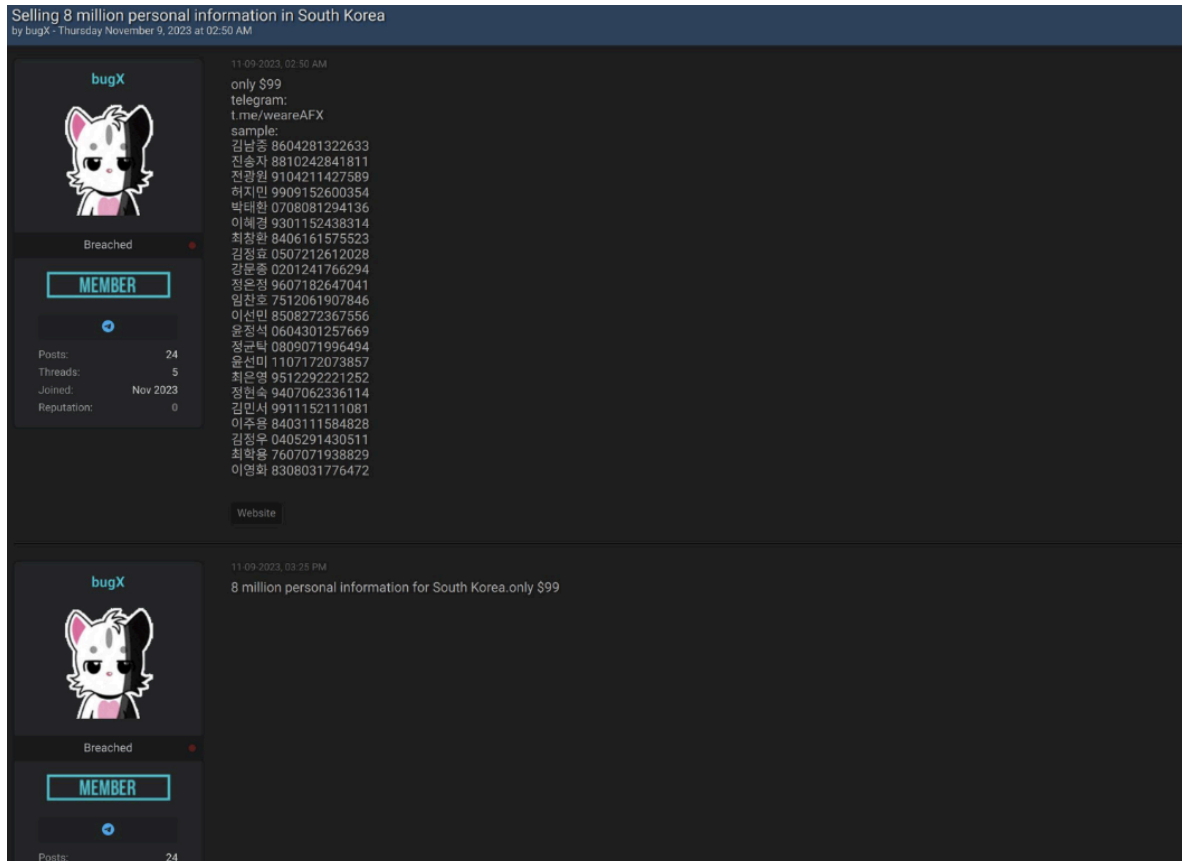
¹⁴ [hXXps://news.kbs\[.\]co\[.\]kr/news/pc/view/view.do?ncd=7754114](https://news.kbs[.]co[.]kr/news/pc/view/view.do?ncd=7754114)

¹⁵ [hXXps://www.reuters\[.\]com/technology/south-korea-asks-us-review-china-rule-chip-subsidies-2023-05-24/](https://www.reuters[.]com/technology/south-korea-asks-us-review-china-rule-chip-subsidies-2023-05-24/)

Hacktivism

North Korea has historically targeted South Korean events (such as holidays and elections) with disruptive activity, and there is a threat of hacktivism during this election cycle. However, ZeroFox has observed no evidence of coordinated hacktivism campaigns targeting South Korea across the deep and dark web (DDW) in the run-up to these elections.

- Such attacks usually take the form of low-complexity and unsophisticated acts of cyber vandalism, such as website defacements and distributed denial-of-service (DDoS) attacks. These attacks primarily cause reputational harm and embarrassment for the targeted country or entities and rarely have significant long-term effects.
- Public-facing websites are the typical targets of such attacks, which usually cause only minor inconveniences. However, ZeroFox has observed that airline and airport websites across the world are being increasingly targeted by DDoS attacks, which can lead to passengers being unable to book tickets and track flights. There is a roughly equal chance of prominent technology companies and airports in South Korea facing such attacks.
- In November 2023, a database allegedly containing eight million records from the South Korean Ministry of Public Safety and Security was listed for sale on an underground forum.
- While isolated instances such as the one mentioned above continue to be observed, sustained campaigns directly targeting the elections in South Korea have not been detected.



Threat actor offering South Korean Ministry of Public Safety and Security records for sale

Source: ZeroFox Intelligence

Conclusion

South Korea's foreign policy under President Yoon makes entities within the country vulnerable to cyber threat activity. South Korean technology firms and those involved in defense are likely experiencing constant threats to their systems. However, the April 2024 elections are largely focused on domestic issues, and there is a notable absence of observed cyber threats.

| Appendix A: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	Sources may use TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	Recipients may NOT share TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	Recipients may ONLY share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note that TLP:AMBER+STRICT restricts sharing to the organization only.
	Green	Clear
WHEN SHOULD IT BE USED?	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	Sources may use TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.	Recipients may share TLP:CLEAR information without restriction, subject to copyright controls.

| Appendix B: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.

Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%