



| Brief |

North Korean and Chinese APT Groups Targeting the Aerospace Sector

B-2023-10-13a

Classification: TLP:CLEAR

Criticality: Medium

Intelligence Requirements: Military, Government, Threat Actor Targeting, Geopolitical

October 13, 2023

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 October 12, 2023**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

Brief | North Korean and Chinese APT Groups Targeting the Aerospace Sector

Executive Summary

A series of attacks occurred against the aerospace industry in 2022 and 2023. The attacks were perpetrated by Chinese and North Korean state-advanced persistent threat (APT) groups in what appears to be a broader cyber espionage effort. While the aerospace industry covers a broad spectrum of activities, the focus of these attacks appears to be on the military applications within the sector—emphasizing rocketry and associated products of high intelligence value to both nations. The APT groups to whom the attacks are attributed have an established history of conducting intelligence operations to satisfy their respective nations' strategic requirements. The focus on the aerospace industry is occurring in a broader geopolitical context.

Analyst Commentary

As of early October 2023, ZeroFox researchers have been tracking an increase in the number of APT group attacks against the aerospace industry in multiple countries. While these incidents took place over an extended period of time between 2021 and early 2023, the most recent attacks came to light in the last month. The worldwide geopolitical situation is becoming increasingly tense, adding to the topic's urgency. ZeroFox assesses

that the attacks are likely to be aimed at collecting intelligence and stealing sensitive intellectual property. Additionally, the attacks appeared likely to be separate long-term efforts by North Korean and Chinese state APT groups, with a noticeable increase in late 2021. Below are the key incidents:

- **June 2021:** An unspecified North Korean APT group breached South Korean aerospace company Korea Aerospace Industries (KAI).¹ The breach resulted in the theft of confidential information on rocket propulsion technologies developed for KSLV-II, South Korea's indigenously manufactured space launch vehicle. Additionally, reports stated the attack may have compromised sensitive information about major defense items, such as the KF-21 indigenous fighter jet, FA-50 light combat aircraft, and unmanned aircraft and radars.
- **May 2022:** A Chinese cyber espionage group known as "Space Pirates" was discovered targeting the Russian aerospace industry with a spear-phishing campaign. The group has been active since at least 2017 and is linked to other China-affiliated APT groups such as APT41 (Winnti), Mustang Panda, and APT27. The Space Pirates APT group has been observed targeting government institutions and firms in Russia, Georgia, and Mongolia, with focus on the aerospace and other related industries.² The Space Pirates' malware toolkit includes a variety of loaders and previously undetectable backdoors such as MyKLoadClient, BH_A006 and Deed RAT. The toolkit also contains well-known malware such as the PlugX RAT, ShadowPad backdoor, Poison Ivy RAT, a modified version of PcShare, and the public ReVBSHELL shell. To tunnel traffic, the APT group also makes use of the dog-tunnel utility. The exchange and use of these exploit tools between APT groups is a common behavior in the Asian region.³
- **May 2022:** APT41 (Winnti) conducted a global cyber espionage campaign targeting manufacturers across North America, Europe, and Asia in the

¹ <https://spacenews.com/north-korea-linked-hackers-accessed-souths-rocket-developer-spy-agency/>

² <https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/space-pirates-a-look-into-the-group-s-unconventional-techniques-new-attack-vectors-and-tools/>

³ <https://securityaffairs.com/131440/apt/space-pirates-targets-space-industry.html>

aerospace, defense, and energy sectors.⁴ The campaign went undiscovered for years as the group siphoned intellectual property and critical data. DEPLOYLOG, a previously unidentified malware strain, was used by the group in the campaign. Updated versions of APT41 malware, such as Spyder Loader, PRIVATELOG, and WINNKIT were also utilized. In order to hide their payloads and avoid being discovered by conventional security tools, the group made use of the Windows CLFS mechanism and NTFS transaction manipulations. With years of performing covert reconnaissance and selecting important material, the group is reported to have exfiltrated hundreds of gigabytes of data. APT41 targeted the victims' intellectual property, including confidential papers, plans, schematics, formulas, and manufacturing-related data. Furthermore, the attackers gathered data that could be exploited in future cyberattacks, such as information about the target company's business units, network architecture, user accounts and credentials, employee emails, and customer data.

- **May 2022:** North Korean state APT groups ScarCruft and Lazarus reportedly breached computer networks at a major Russian missile developer for at least five months in 2022.⁵ The APT groups covertly inserted stealthy backdoors into systems at NPO Mashinostroyeniya, a Russian rocket design firm, with the intent to conduct cyber espionage. According to missile experts cited, the targeted company has been a pioneer developer of hypersonic missiles, satellite technologies, and newer generation ballistic armaments—three areas of keen interest to North Korea. Technical data indicated the intrusion began in late 2021 and lasted until May 2022, when engineers discovered the hackers' activity.⁶
- **February 2023:** China state APT group Volt Typhoon, which typically focuses on cyber espionage and information gathering, was reportedly discovered to be

4

<https://www.cybereason.com/blog/operation-cuckoo-bees-cybereason-uncovers-massive-chinese-intellectual-property-theft-operation>

5

<https://www.sentinelone.com/labs/comrades-in-arms-north-korea-compromises-sanctioned-russian-missile-engineering-company/>

6

<https://www.reuters.com/technology/north-korean-hackers-breached-top-russian-missile-maker-2023-08-07/>

targeting the aeronautical vertical.⁷ Volt Typhoon has been active since mid-2021 targeting critical organizations in Guam and the United States. The observed behavior indicates that the threat actor aims to conduct espionage and remain undetected for as long as feasible. Around the time the FBI was investigating the equipment recovered from the Chinese spy balloon shot down off the coast of South Carolina in February 2023, Microsoft discovered Volt Typhoon's malware in telecommunications networks in Guam, the Pacific island with a vast American air base, and elsewhere in the United States.⁸ The APT group places a focus on stealth, relying largely on off-the-grid means and hands-on keyboard activity. They employ the command line to (1) harvest data, including credentials, from local and network systems; (2) prepare the data for exfiltration; and (3) exploit the stolen valid credentials to maintain persistence. Volt Typhoon also attempts to blend into normal network activity by routing traffic through infected small office and home office (SOHO) network equipment such as routers, firewalls, and VPN devices. To further avoid detection, the group employs customized versions of open-source software to establish a command and control (C2) channel over proxy.

- **March 2023:** An unspecified North Korean APT group reportedly targeted Russian diplomats and successfully penetrated a Russian aerospace research institute.⁹ Further such cyber espionage activities by China and North Korea are anticipated in the months ahead in light of a continued tense geopolitical situation.
- **March 2023:** Security researchers attributed a cyber espionage attack against an undisclosed aerospace company in Spain to the Lazarus APT group.¹⁰ The attack was part of a campaign dubbed Operation Dream Job in which employees were

⁷

<https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/>

⁸ <https://www.nytimes.com/2023/05/24/us/politics/china-guam-malware-cyber-microsoft.html>

⁹

<https://blogs.microsoft.com/on-the-issues/2023/09/07/digital-threats-cyberattacks-east-asia-china-north-korea/>

¹⁰

<https://www.welivesecurity.com/en/eset-research/lazarus-luring-employees-trojanized-coding-challenges-case-spanish-aerospace-company/>

approached by a threat actor impersonating as a Meta recruiter.¹¹ Operation Dream Job is a long-term spear-phishing campaign orchestrated by Lazarus Group. The goal of the campaign is to entice employees working at prospective targets of strategic interest with job opportunities in order to activate the infection chain. The goal of the breach, which is tailored for Windows systems, is the placement of a LightlessCan implant. LightlessCan is a complicated and evolving instrument with a high level of complexity that marks a substantial advancement in capabilities over its predecessor, BLINDINGCAN. According to the researchers, BLINDINGCAN¹² (also known as AIRDRY or ZetaNile) is a feature-rich malware capable of stealing sensitive data from infected hosts.

The attacks against aerospace sector targets were carried out using techniques common to APT groups, often with proprietary tools. However, the scope of the threat also includes access vectors available to cybercriminal groups on the deep and dark web (DDW). ZeroFox Intelligence identified a number of advertised network accesses for aerospace firms. While there was no indication that the APT groups leveraged the underground for access to aerospace firms, this vector represents an opportunity that APT groups could exploit to gain access to sensitive information.

The focus by China and North Korea's intelligence services on aerospace-related military applications is occurring in a broader geopolitical context; it is noteworthy that both nations separately targeted different aspects of Russia's aerospace sector. Russia's missile capabilities are advanced, and both China and North Korea likely have intelligence needs that can be answered by targeting Russia's aerospace sector.

In July 2023, North Korean leader Kim Jong Un publicly pushed for the nation to focus on developing its rocket capabilities. This statement occurred around the time North Korea tested a liquid-fueled intercontinental ballistic missile (ICBM).¹³ A body of reporting indicates China is close to development of a hypersonic missile production capability. While China is believed to possess a small number of these missiles,¹⁴ it likely places a priority on improving its hypersonic program. Russia is believed to be much further along

¹¹ <https://thehackernews.com/2023/03/north-korean-unc2970-hackers-expands.html>

¹² <https://thehackernews.com/2023/09/lazarus-group-impersonates-recruiter.html>

¹³ <https://www.cnn.com/2023/07/12/asia/north-korea-icbm-explainer-intl-hnk/index.html>

¹⁴ <https://wmdcenter.ndu.edu/Publications/Publication-View/Article/2484178/chinas-hypersonic-weapons/>

in possessing functional hypersonic weapons¹⁵ and the ability to produce them. Chinese APT groups would likely carry out targeting and collection in accordance with this requirement.

Recommendations

Chinese and North Korean APT groups have demonstrated the capacity and long-term focus to conduct successful cyber espionage campaigns against high-priority intelligence targets. The aerospace sector is one of these targets and will continue to be at high risk of attack by APT groups and cybercriminals alike. As demonstrated in this analysis, private aerospace sector organizations with overlap into the defense sector are frequently targeted for collection. This will continue to be the case, as they are relatively soft targets. ZeroFox recommends a proactive identification of organizations that fit this criterion. Monitoring these organizations outside the United States for compromise by APT groups will provide indications of the attackers' intelligence priorities. U.S.-based organizations that fit this criteria should be made aware of the heightened risk of sophisticated attack and implement appropriate countermeasures.

¹⁵ <https://wmdcenter.ndu.edu/Publications/Publication-View/Article/2039639/russias-hypersonic-weapons/>

| 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%