ZEROFOX Intelligence

Brief

Lazarus Group Exploitation of MagicLine4NX Vulnerability

B-2023-12-01c

Classification: TLP:CLEAR

Criticality: High

Intelligence Requirements: Vulnerability Exploitation, Malware, Deep Dark Web & Criminal Underground

December 1, 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 (EST) on November 30, 2023; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Brief | Lazarus Group Exploitation of MagicLine4NX Vulnerability

› Key Findings

- On November 23, 2023, intelligence agencies from the United Kingdom (UK) and South Korea released a joint cybersecurity advisory highlighting recent supply chain attacks utilizing a zero-day vulnerability in security authentication tool MagicLine4NX.
- Agencies and organizations have attributed the use of this vulnerability to the North Korean-linked Advanced Persistent Threat (APT) group Lazarus, which has grown adept at leveraging zero-day vulnerabilities to conduct supply chain attacks for financial gain.
- The exploit is currently tracked as CVE-2023-45797 and is a buffer overflow vulnerability that allows an attacker to remotely execute code affecting versions 1.0.0.1 to 1.0.0.26 of the MagicLine4NX software.
- While most notable activity has been tracked within the past year, Lazarus Group may have been exploiting a separate vulnerability within MagicLine4NX in 2021.

| Details

The UK's National Cyber Security Centre (NCSC) and South Korea's National Intelligence Service (NIS) recently released a joint advisory highlighting what they claim is Lazarus Group's use of a zero-day vulnerability in security authentication tool MagicLine4NX to

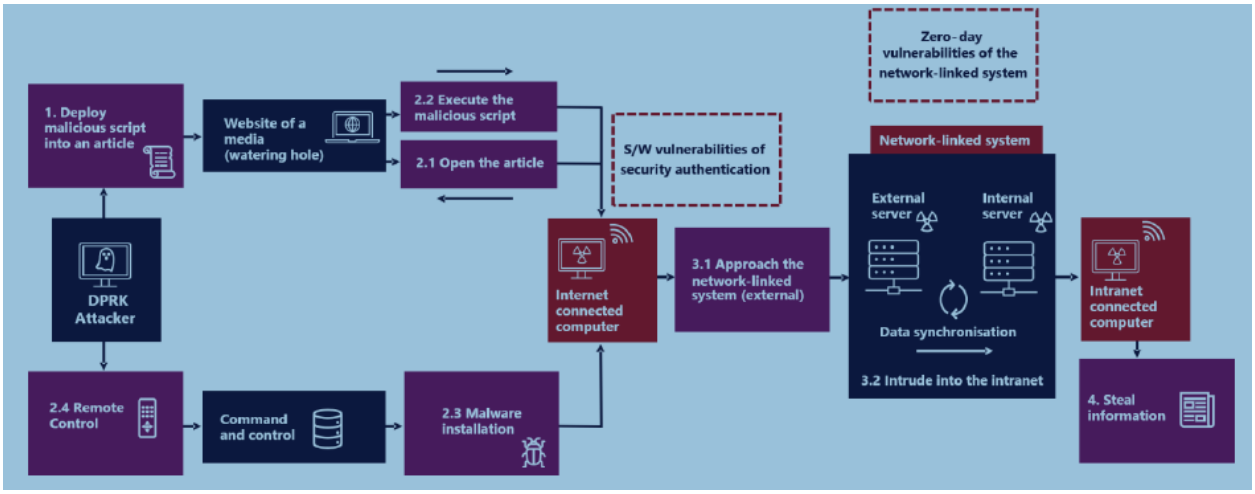
carry out several supply chain attacks.[1] While the group has leveraged this vulnerability against organizations around the globe, it has predominantly concentrated on targeting South Korean entities. Developed by South Korean-based company Dream Security, MagicLine 4NX allows users to conduct logins with joint certificates and digitally sign transactions. Users of MagicLine4NX also have the ability to integrate the software with other applications, such as web browsers, file explorers, and email clients.[2]

According to the advisory, the Lazarus Group reportedly exploited the MagicLine4NX vulnerability in March 2023 to gain access to the intranet of an unnamed targeted organization (likely South Korean), which has led to additional attacks of other unnamed targets.[3] However, ASEC's AhnLab reported in October 2023 that it detected 105 cases of the exploitation in 40 organizations from January to July 2023.[4]

Attack Breakdown

Codenamed "Operation Dream Magic" by ASEC, the attack begins with a watering hole technique in which the group compromises the website of certain unnamed media outlets, deploying malicious scripts into articles. However, the scripts only target users within specific IP ranges. Once users who utilize the vulnerable version of the MagicLineNX software visit an infected article's webpage, the code executes. After the group obtains access to the target system, it exploits a second zero-day vulnerability in the organization's network-linked system to move laterally and collect and exfiltrate data. Specifically, the group exploits the data synchronization feature between servers to move from the external network server to the internal network server.[5][6]

[1] hXXps://eng.nis.go[.]kr/ECM/1_3_1_1.do?seq=83&currentPage=1
[2] hXXps://securityaffairs[.]com/154765/apt/lazarus-magicline4nx-supply-chain-attack.html
[3] hXXps://eng.nis.go[.]kr/ECM/1_3_1_1.do?seq=83&currentPage=1
[4] hXXps://asec.ahnlab[.]com/en/57736/
[5] hXXps://securityaffairs[.]com/154765/apt/lazarus-magicline4nx-supply-chain-attack.html
[6] hXXps://cybermaterial[.]com/lazarus-group-targets-magicline4nx-flaw/



Operation Dream Magic Attack Chain

Source:
hXXps://securityaffairs[.]com/154765/apt/lazarus-magicline4nx-supply-chain-attack.html

Threat Actor Background

Lazarus Group is an umbrella term used to cover a large portion of North Korea's APT activity.[7] The group is responsible for many of North Korea's most sophisticated cyberattacks and has been active since roughly 2009. While Lazarus Group targets many sectors with seemingly no geographic boundaries, it has focused largely on financial crime in recent years. In particular, the group has become very active and adept at cryptocurrency theft, with numerous estimates placing its theft totals in the billions.[8]

Lazarus Group, like many other state-affiliated APT groups, often utilizes supply chain attacks that provide a persistent, low-visibility attack vector into the networks of a broad range of targets. The group has grown adept at leveraging zero-day vulnerabilities to conduct supply chain attacks for financial gain. For example, Lazarus conducted a successful supply chain attack against JumpCloud in the summer of 2023 with the goal of stealing cryptocurrency.[9] While the group may focus largely on financial crime,

[7] hXXps://www.nccgroup[.]com/us/the-lazarus-group-north-korean-scourge-for-plus10-years/

[8] hXXps://www.wsj[.]com/articles/how-north-koreas-hacker-army-stole-3-billion-in-crypto-funding-nuclear-program-d6fe8782

[9] hXXps://www.scmagazine[.]com/news/north-korean-linked-lazarus-group-tied-to-supply-chain-attack-on-jumpcloud

elements within Lazarus Group also respond to North Korean strategic requirements. Lazarus is generally believed to be a component of North Korea's Reconnaissance General Bureau,[10] the nation's primary foreign intelligence service.[11] As with other nation-state APTs, one of Lazarus Group's roles is the collection of high-value information. In late November 2023, a subgroup of Lazarus conducted a supply chain attack targeted at cyber espionage.[12]

Vulnerabilities Exploited

The vulnerability most recently exploited by Lazarus was a zero-day that is now being tracked as CVE-2023-45797.[13] It is a buffer overflow vulnerability in versions 1.0.0.1 to 1.0.0.26 of MagicLine4NX that allows an attacker to execute code remotely. It was first published on the National Vulnerability Database on October 30, 2023.

In October 2022, an ASEC blog post revealed that Lazarus was exploiting a different vulnerability in the MagicLine4NX software[14] to gain access to the internal systems of targets. That vulnerability is tracked as CVE-2021-26606[15] and affects MagicLine4NX versions 1.0.0.17 or earlier. It is a buffer overflow vulnerability that could allow the attacker to remotely execute arbitrary code on a target system.

Recommendations

As NCSC and NIS assess that the level of supply chain attacks is likely to increase,[16] implementing robust cybersecurity measures is crucial. To mitigate the exploitation of this vulnerability and others exploited in supply chain attacks, organizations should:

- Prioritize patch management for this vulnerability on all public, internet-facing assets.
- Conduct regular vulnerability scans.

[10] hXXps://www.bugcrowd[.]com/glossary/lazarus-group/
[11] hXXps://irp.fas[.]org/world/dprk/index.html
[12] hXXps://www.securityweek[.]com/north-korean-software-supply-chain-attack-hits-north-america-asia/
[13] hXXps://nvd.nist[.]gov/vuln/detail/CVE-2023-45797
[14] hXXps://asec.ahnlab[.]com/en/40830/
[15] hXXps://nvd.nist[.]gov/vuln/detail/CVE-2021-26606
[16] hXXps://eng.nis.go[.]kr/ECM/1_3_1_1.do?seq=83&currentPage=1

- Assess software supply chain risks, especially with the use of third-party and open-source software.
- Conduct heightened social engineering awareness and training for relevant stakeholders.
- Diligently monitor integrated networks and software for suspicious activity.

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%