Hive Pro®

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

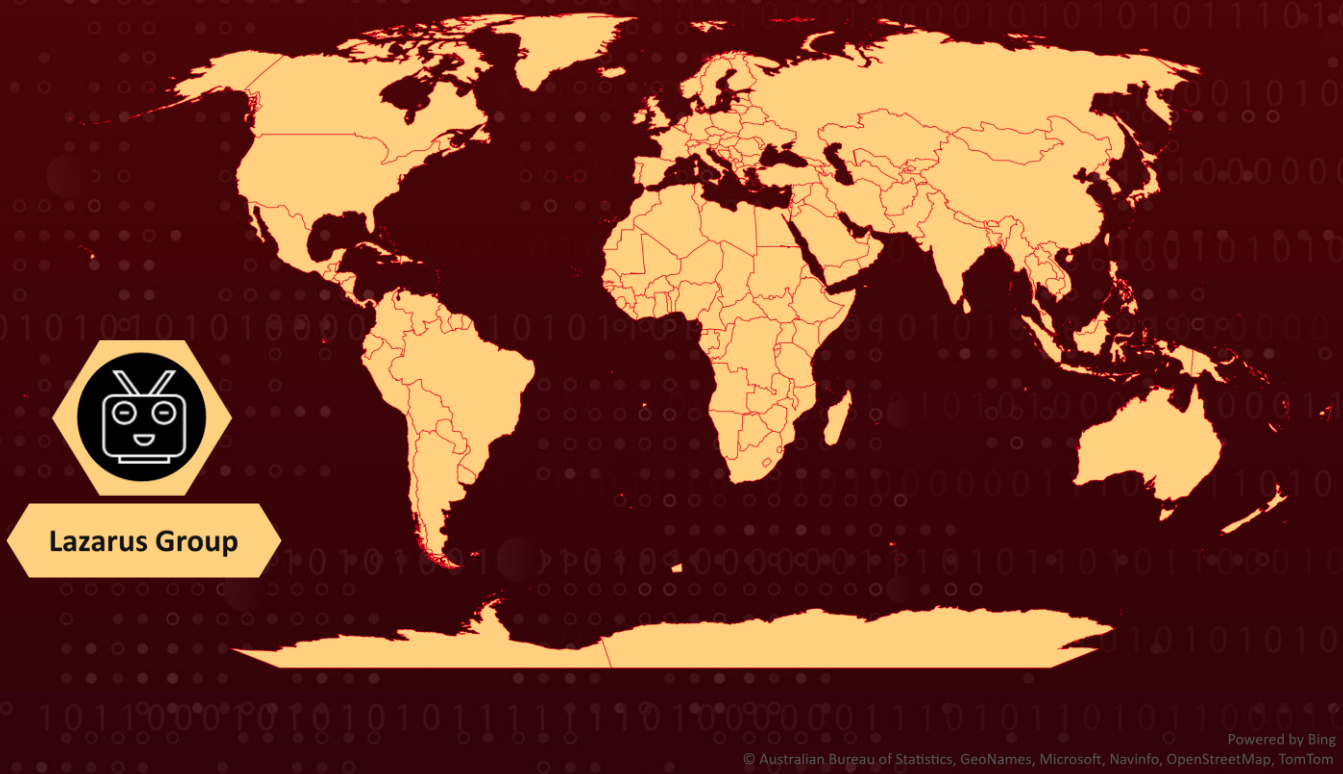
North Korean APT's Covert Supply-Chain Ambush

Date of Publication	Admiralty Code	TA Number
November 27, 2023	A1	TA2023478

Summary

Attack Began: March 2023
Threat Actor: Lazarus Group (aka Labyrinth Chollima, Guardians Of Peace, Zinc, Nickel Academy, Group 77, Hastati Group, Whois Hacking Team, Newromanic Cyber Army Team, Hidden Cobra, Appleworm, APT-C-26, Atk 3, Sectora01, ITG03, TA404, DEV-0139, Gods Apostles, Gods Disciples, UNC577, UNC2970, UNC4034, UNC4736, UNC4899, Diamond Sleet, Jade Sleet, TraderTraitor)
Attack Region: Worldwide
Targeted Industries: Government Organizations, Financial Institutions and Defense
Attack: There has been a significant increase in software supply chain attacks orchestrated by North Korean hackers. Notably, the MagicLine4NX and 3CX compromises gained attention, with the Lazarus hacking group employing a sophisticated approach. They leverage a zero-day vulnerability in the MagicLine4NX software to execute supply-chain attacks.

Attack Regions



Attack Details

#1 In recent years, there has been a significant surge in software supply chain attacks orchestrated by North Korean hackers. Notably, the compromises involving MagicLine4NX and **3CX** gained traction in March 2023. The **Lazarus** hacking group from North Korea employs a sophisticated approach, leveraging a zero-day vulnerability within the MagicLine4NX software to execute supply-chain attacks.

#2 Lazarus's modus operandi involves exploiting vulnerabilities in security authentication and network-linked systems sequentially to illicitly access a target organization's intranet. The initial breach entails exploiting a software vulnerability in the MagicLine4NX security authentication program to infiltrate a target's internet-connected computer.

#3 Subsequently, a zero-day vulnerability in the network-linked system is exploited to traverse laterally, thereby gaining unauthorized access to sensitive information. The offensive maneuver initiates with the compromise of a media outlet's website, where malicious scripts are embedded into an article, creating an avenue for a 'watering hole' attack. This attack, codenamed 'Dream Magic,' specifically impacts versions preceding 1.0.0.26.

#4 A cyber assault on **CyberLink** orchestrated by the Lazarus hacking group involved the exploitation of a supply chain vulnerability. This tactic facilitated the dissemination of trojanized CyberLink installers, which bore digital signatures, ultimately resulting in the compromise of at least one hundred computers with the 'LambLoad' malware.

#5 Consistently, state-backed North Korean hacking operations employ supply chain attacks and capitalize on zero-day vulnerabilities as integral components of their cyber warfare strategies. These tactics are strategically employed to target specific companies, whether for cyber espionage, financial fraud, or cryptocurrency theft.

Recommendations

Vet Third-Party Software: Given the exploitation of legitimate software in their attacks, organizations must diligently vet and monitor third-party software components, especially those used in critical systems. This process involves assessing the reputation and security practices of software providers, as well as evaluating the authenticity of their digital signatures.

Anomaly Detection: Implement anomaly detection algorithms to identify deviations from normal network behavior. This includes monitoring network traffic, system logs, and user activities for any unusual patterns.

Zero-Trust Architecture: Consider adopting a zero-trust architecture, where no device or user is inherently trusted, and verification is required from everyone trying to access resources. This approach can limit the lateral movement within a compromised network.

Enhance Endpoint Security: Deploy advanced endpoint security solutions, such as endpoint detection and response (EDR) tools, to identify and respond to malicious activities promptly. Keep security software, including antivirus and endpoint protection, up to date to defend against known threats.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation
TA0005 Defense Evasion	TA0007 Discovery	TA0008 Lateral Movement	TA0011 Command and Control
TA0010 Exfiltration	T1190 Exploit Public-Facing Application	T1129 Shared Modules	T1027 Obfuscated Files or Information
T1036 Masquerading	T1563 Remote Service Session Hijacking	T1112 Modify Registry	T1056 Input Capture
T1012 Query Registry	T1018 Remote System Discovery	T1082 System Information Discovery	T1518.001 Security Software Discovery
T1071 Application Layer Protocol	T1095 Non-Application Layer Protocol	T1105 Ingress Tool Transfer	T1588.006 Vulnerabilities
T1573 Encrypted Channel	T1041 Exfiltration Over C2 Channel		

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	316c088874a5dfb8b8c1c4b259329257, 33ca34605e8077047e30e764f5182df0, d5101c3b86d973a848ab7ed79cd11e5a, 660ea9b8205fbd2da59fefd26ae5115c, 5faf36ca90f6406a78124f538a03387a
URLs	hxxps[:]//msstorageazure[.]com/analysis, hxxps[:]//officestoragebox[.]com/api/biosync, hxxps[:]//visualstudiofactory[.]com/groupcore, hxxps[:]//azuredeploystore[.]com/cloud/images, hxxps[:]//msstorageboxes[.]com/xbox, hxxps[:]//officeaddons[.]com/quality, hxxps[:]//sourceslabs[.]com/status, hxxps[:]//zacharryblogs[.]com/xmlquery, hxxps[:]//pbxcloudeservices[.]com/network, hxxps[:]//pbxphonenetwork[.]com/phone, hxxps[:]//akamaitechcloudservices[.]com/v2/fileapi, hxxps[:]//azureonlinestorage[.]com/google/storage, hxxps[:]//msedgepackageinfo[.]com/ms-webview, hxxps[:]//glcloudservice[.]com/v1/status, hxxps[:]//pbxsources[.]com/queue, hxxps[:]//sbmsa[.]wiki/blog/_insert,
Domains	msstorageazure[.]com, officestoragebox[.]com, visualstudiofactory[.]com, azuredeploystore[.]com, msstorageboxes[.]com, officeaddons[.]com, sourceslabs[.]com, zacharryblogs[.]com, pbxcloudeservices[.]com, pbxphonenetwork[.]com, akamaitechcloudservices[.]com, azureonlinestorage[.]com, msedgepackageinfo[.]com, glcloudservice[.]com, pbxsources[.]com, sbmsa[.]wiki
SHA1	3dc840d32ce86cebf657b17cef62814646ba8e98, 769383fc65d1386dd141c960c9970114547da0c2, 9e9a5f8d86356796162cee881c843cde9eaedfb3

TYPE	VALUE
SHA256	e6bbc33815b9f20b0cf832d7401dd893fbc467c800728b5891336706da0dbcec, a64fa9f1c76457ecc58402142a8728ce34ccba378c17318b3340083eeb7acc67, 6c121f2b2efa6592c2c22b29218157ec9e63f385e7a1d7425857d603ddef8c59s

References

https://www.ncsc.gov.uk/news/uk-republic-of-korea-issue-warning-dprk-state-linked-cyber-actors-attacking-software-supply-chains

https://s3.documentcloud.org/documents/24174869/rok-uk-joint-cyber-security-advisoryeng.pdf

https://www.hivepro.com/threat-advisory/smoothoperator-campaign-trojanizes-3cxdesktopapp/

https://www.hivepro.com/threat-advisory/malicious-dprk-actors-target-the-healthcare-industry-in-the-us-south-korea/

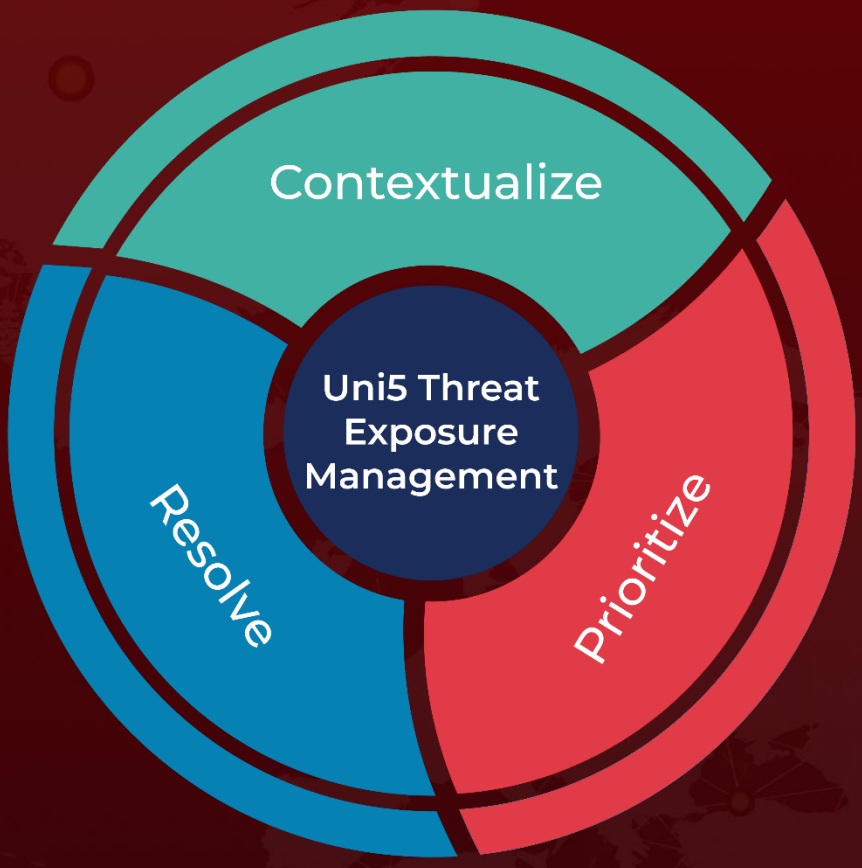
https://www.hivepro.com/threat-advisory/lazarus-group-orchestrates-supply-chain-attack-on-cyberlink-corp/

https://asec.ahnlab.com/en/57736/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

November 27, 2023 . 09:30 PM

More at www.hivepro.com