Hive Pro®

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

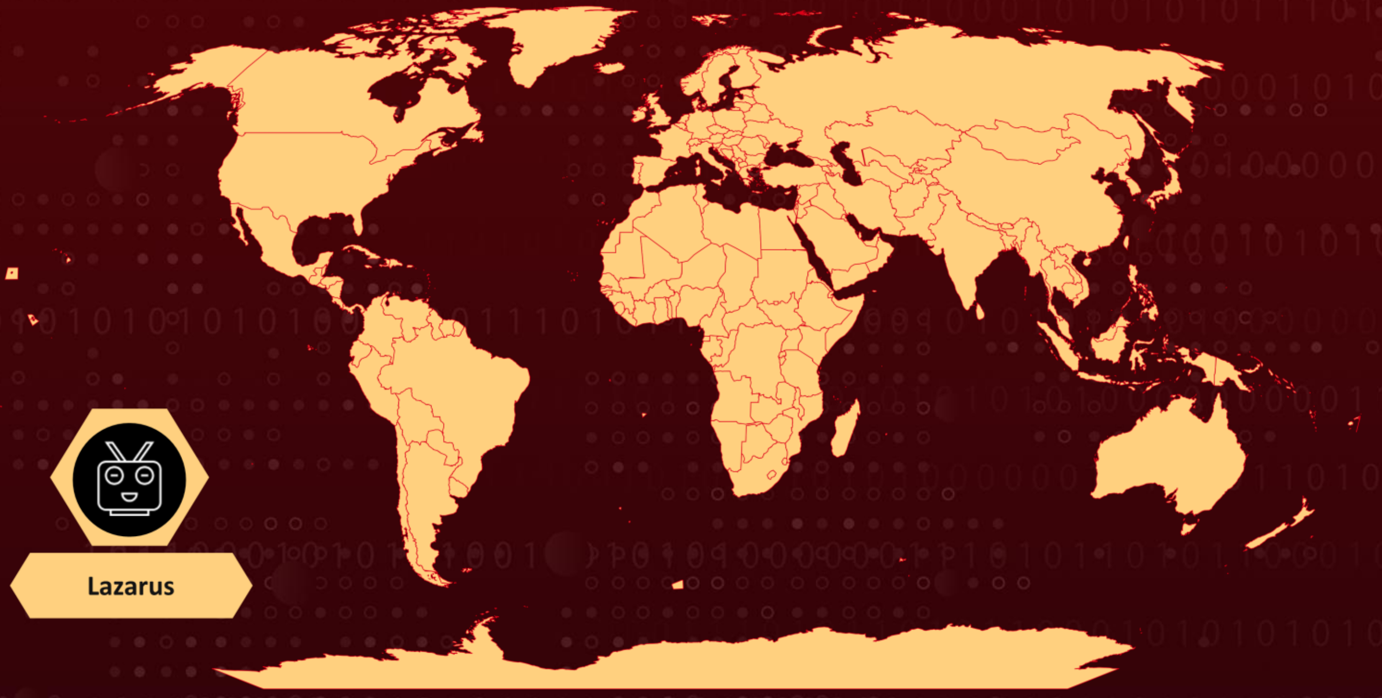
North-Korean Cyber-Espionage Operations Grapples Defense Sector

Date of Publication	Admiralty Code	TA Number
February 20, 2024	A1	TA2024066

Summary

Attack Began: Late 2022
Attack Region: Worldwide
Targeted Industries: Defense sector, Research centers
Actor: Lazarus (aka Labyrinth Chollima, Group 77, Hastati Group, Who is Hacking Team, NewRomanic Cyber Army Team, Zinc, Hidden Cobra, Appleworm, APT-C-26, ATK 3, SectorA01, ITG03, TA404, DEV-0139, Guardians of Peace, Gods Apostles, Gods Disciples, UNC577, UNC2970, UNC4034, UNC4736, UNC4899, Diamond Sleet, Jade Sleet, TraderTraitor)
Attack: There is an ongoing cyber-espionage campaign purportedly led by the North Korean threat actors, specifically targeting the global defense industry. The primary objective of these attacks is to acquire data pertaining to advanced military technology, with the intention of assisting North Korea in modernizing its conventional weapons and developing new military capabilities. Notably, the Lazarus group is one of the two examples associated with North Korean actors in this context.

Attack Regions



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, TomTom, Zenrin

Attack Details

#1

Cyber operations that are probably being directed by North Korean cyber actors seem to be specifically going for the defence industry. It is purported that North Korea is employing the pilfered data to create new strategic military systems, including ballistic missiles, submarines, and reconnaissance satellites, as well as to update and improve the capabilities of conventional weapons.

#2

The cyber campaigns targeting the defense sector are believed to involve the notorious threat groups LAZARUS and another purported North Korean cyber threat group. Two attack vectors exemplify systematic attacks on the defense sector: one involving supply chain attacks and the other employing social engineering tactics by LAZARUS.

#3

In late 2022, a North Korean cybercriminal infiltrated a research center focusing on maritime and shipping technologies. Once inside, they exploited vulnerabilities in the web server maintenance operations, enabling a supply-chain attack. Leveraging legitimate tools, the attacker moved laterally across the network and exfiltrated SSH credentials. They distributed a malicious patch file through the Patch management system, downloaded malicious files, and masqueraded as a security manager. Subsequently in another round of attacks, attacker persisted with new waves of Initial Access techniques involving spear-phishing emails and the exploitation of vulnerabilities in the center's website.

#4

The second case demonstrates how the Lazarus group's "Operation Dream Job," a strategy was applied against the defence industry. The actor created profile is posing as a headhunter with a wide network of contacts in the defence industry and constructing a false profile on an internet employment platform. By adding contacts from the target's social circle and offering a job in English, the attacker wins the target's trust. The attacker then uses techniques like providing a PDF file with a job offer, brief information, links to more in-depth files, zip files with ISO images, or a rogue VPN client to convince the employee to change channels of contact.

#5

Despite the well-documented nature of these strategies, threat actors can still succeed if companies fail to update their staff on the latest cyberattack techniques. Implementing a robust security posture, including the principle of least privilege and restricting employee access, is crucial in mitigating such threats.

Recommendations

Remain Vigilant: It is essential to remain cautious. Be wary of clicking on suspicious links or visiting untrusted websites, as they may contain malicious content. Exercise caution when opening emails or messages from unknown sources, as they could be part of phishing attempts.

Security Trainings: Conduct regular cybersecurity awareness training sessions to educate employees about the risks associated with spear-phishing and social engineering tactics. Emphasize the importance of carefully scrutinizing email attachments, especially those received from unfamiliar or suspicious sources.

Limit Access: When obtaining remote maintenance and repair services, restrict access to only the systems that are absolutely required. Prior to granting user permissions and privileges, authentication and authorization checks are must be completed.

Robust Endpoint Security: Deploy advanced endpoint security solutions that include real-time malware detection and behavioral analysis. Regularly update antivirus and anti-malware software to ensure the latest threat definitions are in place. A multi-layered approach to endpoint security can prevent malwares from infiltrating the network through vulnerable endpoints and can detect and block malicious activities effectively.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0005 Defense Evasion
TA0006 Credential Access	TA0007 Discovery	TA0008 Lateral Movement	TA0009 Collection
TA0010 Exfiltration	TA0011 Command and Control	T1133 External Remote Services	T1059 Command and Scripting Interpreter
T1078 Valid Accounts	T1070 Indicator Removal	T1140 Deobfuscate/Decode Files or Information	T1040 Network Sniffing

T1046 Network Service Discovery	**T1021** Remote Services	**T1213** Data from Information Repositories	**T1001** Data Obfuscation
T1071 Application Layer Protocol	**T1572** Protocol Tunneling	**T1041** Exfiltration Over C2 Channel	**T1566** Phishing
T1566.001 Spearphishing Attachment			

Indicators of Compromise (IOCs)

TYPE	VALUE
URL	connection.lockscreen.kro[.]kr/index.php, updating.dothome.co[.]kr/microsoft/app/google
MD5	3c2aa3687ac9f466ce909e2cb12b07a5, 4631ef8db9c36b0f2534ac7193f2587e, 607a2a8d2863c3144b8e901a16a76c33
Domains	chrysalisc[.]com, sifucanva[.]com, thefrostery.co[.]uk, rginfotechnology[.]com, job4writers[.]com, contact.rgssm[.]in
SHA1	7da62cdb447a7ae3ae7b5f67a511e7cf2b26c7df, 2e0d374f1e706ae1fa24558b54c5a1630302eab1, 294706ae0585abaf4e6c5e66a7f5141ac4281d57, 127ced578e041f53b5988a7fefaa6e09e64f4bf9, 3bc8acdd07c6d91652101d9c8b3326bee372a007, 7906270679014234b70aa63dd89e8282a945919c, 7b4d0d8e3bfcd634bc7d7a17fb546b7e8316a681, d5c8edb84e4ff33aea8865676ffe801ff0a71701, ac9021eb798de8323702a5aeb7c590f1ebaa3786, d5c8edb84e4ff33aea8865676ffe801ff0a71701
SHA256	F3482A38BEFDCD7D0B87D86F24CDB209028BD8471BAA6610548FB721086F5B85, 47999FA014B6CC5A2A71BE590C93830371E259242DFDBA7FFA2698F1900919EC

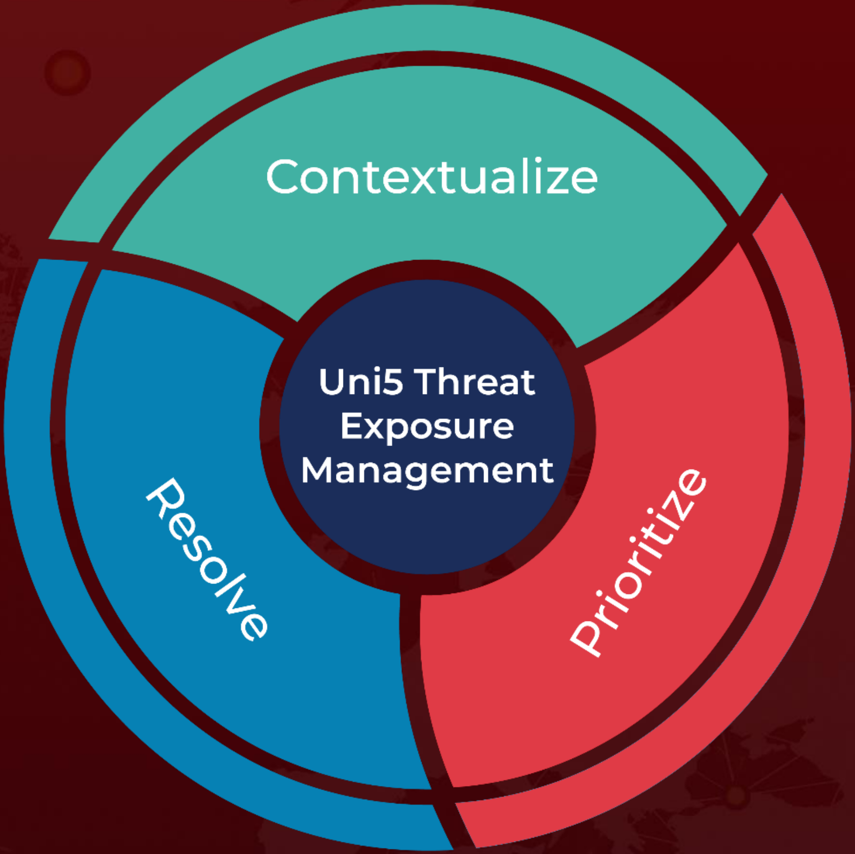
References

https://www.verfassungsschutz.de/SharedDocs/publikationen/DE/cyberabwehr/2024-02-19-joint-cyber-security-advisory-englisch.pdf?__blob=publicationFile&v=2

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

February 20, 2024 • 5:20 AM

More at www.hivepro.com