Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

Operation SyncHole: Lazarus Escalates Cyberattacks Against South Korean Industries

Date of Publication	Admiralty Code	TA Number
April 25, 2025	A1	TA2025127

Summary

Attack Discovered: November 2024
Targeted Country: South Korea
Affected Industries: Software, IT, Financial, Semiconductor Manufacturing, and Telecommunications Industries
Campaign: Operation SyncHole
Malware: ThreatNeedle, wAgent, SIGNBT, COPPERHEDGE, Agamemnon, LPEClient
Actor: Lazarus group (aka Labyrinth Chollima, Group 77, Hastati Group, Whois 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, Citrine Sleet, Jade Sleet, TraderTraitor, Gleaming Pisces, Slow Pisces)
Attack: The Lazarus group has launched a stealthy campaign, "Operation SyncHole," targeting South Korean industries with a mix of software exploits, watering hole attacks and lateral movement techniques. By compromising trusted local software like Cross EX and Innorix Agent, the attackers slipped malware such as ThreatNeedle, SIGNBT, and COPPERHEDGE into corporate networks aiming to dig deep into internal systems. Using clever tricks like DLL sideloading, fake websites, and even a downloader named Agamemnon, they blended into trusted environments. This operation shows how Lazarus continues to sharpen its tactics quietly evolving tools while targeting supply chains to maximize damage.

Attack Regions

Attack Details

#1 The North Korea-linked Lazarus group has launched a sweeping and stealthy cyber-espionage campaign dubbed Operation SyncHole, targeting at least six South Korean organizations across sectors like finance, IT, semiconductors, telecom, and software. This operation hinged on exploiting supply chain vulnerabilities in widely used South Korean software, including a one-day flaw in Innorix Agent for lateral movement.

#2 The campaign began around November 2024, when a ThreatNeedle variant one of Lazarus' hallmark backdoors was found running as a subprocess of Cross EX, a legitimate Korean software. This tool was used as a launchpad to compromise other organizations. Lazarus also ran watering hole attacks, injecting malicious code into compromised South Korean media sites, redirecting unsuspecting visitors to attacker-controlled infrastructure mimicking legitimate services.

#3 Lazarus split the operation into two attack phases. The first deployed ThreatNeedle and wAgent, while the second introduced updated malware strains like SIGNBT and COPPERHEDGE. One standout component was Agamemnon, a downloader used to retrieve and execute additional payloads from the C2 server. It played a critical role in expanding capabilities post-initial compromise, serving as a pivot for additional tools once the host was infected. The use of Agamemnon reveals Lazarus' growing reliance on modular tooling to improve stealth and persistence.

#4 The updated version of ThreatNeedle used advanced encryption, generating Curve25519-based key pairs to establish a shared key for ChaCha20-encrypted communications with the C2. It came in Core and Loader variants, enabling stealthy data exfiltration and persistence via system services like IKEEXT or through SSP registration. Meanwhile, wAgent another implant used RSA encryption via the open-source GMP library, and cleverly embedded tracking headers in HTTP cookies to stay under the radar.

#5 Innorix Agent was also abused through a targeted sideloading attack, leading to the execution of ThreatNeedle and a profiling tool called LPEClient. Although this vulnerability was never exploited in the wild, Innorix quickly released a patch in March 2025. The campaign also made heavy use of compromised South Korean websites as C2 infrastructure, some posing as defunct domains of former ISPs or insurance companies. Operation SyncHole reinforces the Lazarus group's long-term strategy of exploiting South Korean supply chains, continuously upgrading their malware and infrastructure to avoid detection while expanding their foothold.

Recommendations

Keep your Software Up to Date: Make sure to regularly install updates for tools like Cross EX and Innorix Agent, as these are often targeted by attackers. Patching known flaws quickly helps block the paths hackers use to get in.

Boost your Supply Chain Defenses: Carefully evaluate third-party software vendors especially local ones often targeted by advanced threat groups. Make sure your suppliers use code signing and follow secure delivery practices.

Watch for Lateral Movement Clues: Keep an eye out for unusual activity like process injections, DLL sideloading, or suspicious services being created. Be alert to the unauthorized use of files like AppVShNotify.exe and USERENV.dll these are telltale signs of Lazarus' sideloading tactics.

Enhance Web and Email Defenses: Set up web filtering to block access to malicious or fake websites often used in Lazarus attacks. Strengthen your email security to catch and stop phishing messages before they can drop malware into your network.

Enhance Endpoint Protection: Deploy next-generation antivirus (NGAV) and endpoint detection & response (EDR) solutions to identify and block malware. Leverage behavioral analysis and machine learning-based detection to spot suspicious activity.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	**TA0043** Reconnaissance	**TA0001** Initial Access	**TA0002** Execution
TA0003 Persistence	**TA0004** Privilege Escalation	**TA0005** Defense Evasion	**TA0006** Credential Access
TA0007 Discovery	**TA0008** Lateral Movement	**TA0011** Command and Control	**T1584** Compromise Infrastructure

T1584.001 Domains	T1588 Obtain Capabilities	T1588.006 Vulnerabilities	T1189 Drive-by Compromise
T1068 Exploitation for Privilege Escalation	T1583 Acquire Infrastructure	T1583.001 Domains	T1036 Masquerading
T1608 Stage Capabilities	T1608.004 Drive-by Target	T1190 Exploit Public-Facing Application	T1059 Command and Scripting Interpreter
T1543 Create or Modify System Process	T1543.003 Windows Service	T1574 Hijack Execution Flow	T1574.001 DLL
T1547 Boot or Logon Autostart Execution	T1547.005 Security Support Provider	T1573 Encrypted Channel	T1573.002 Asymmetric Cryptography
T1573.001 Symmetric Cryptography	T1105 Ingress Tool Transfer	T1218 System Binary Proxy Execution	T1218.011 Rundll32
T1140 Deobfuscate/Decode Files or Information	T1027 Obfuscated Files or Information	T1027.013 Encrypted/Encoded File	T1027.009 Embedded Payloads
T1071 Application Layer Protocol	T1071.001 Web Protocols	T1105 Ingress Tool Transfer	T1570 Lateral Tool Transfer
T1564 Hide Artifacts	T1564.004 NTFS File Attributes	T1082 System Information Discovery	T1083 File and Directory Discovery
T1057 Process Discovery	T1049 System Network Connections Discovery	T1016 System Network Configuration Discovery	T1087 Account Discovery
T1087.001 Local Account	T1087.002 Domain Account	T1569 System Services	T1569.002 Service Execution
T1583 Acquire Infrastructure	T1583.003 Virtual Private Server	T1135 Network Share Discovery	T1007 System Service Discovery

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	f1bcb4c5aa35220757d09fc5feea193b, dc0e17879d66ea9409cdf679bfea388c, 2d47ef0089010d9b699cd1bbbc66f10a
SHA256	94868D8DB5A22DF0B841D282D5D408D00179224EC7031386FBD80F0473F486B3, 922A2FFDBFBBC3998FF38111D20C6ED88BBA0E09DE7F0F66A28B06C0EE51F69C, 23AC99FB8DE813172BB641BAEFFF59FD8B84F1B39B362D7FD11736B5667BEE56
Domains	www[.]smartmanagerex[.]com
URLs	hxxps://thek-portal[.]com/eng/career/index[.]asp, hxxps://builsf[.]com/inc/left[.]php, hxxps://www[.]rsdf[.]kr/wp-content/uploads/2024/01/index[.]php, hxxp://www[.]shcpump[.]com/admin/form/skin/formBasic/style[.]php, hxxps://htns[.]com/eng/skin/member/basic/skin[.]php, hxxps://kadsm[.]org/skin/board/basic/write_comment_skin[.]php, hxxp://bluekostec[.]com/eng/community/write[.]asp, hxxp://dream[.]bluit[.]gethompy[.]com/mobile/skin/board/gallery/index[.]skin[.]php

References

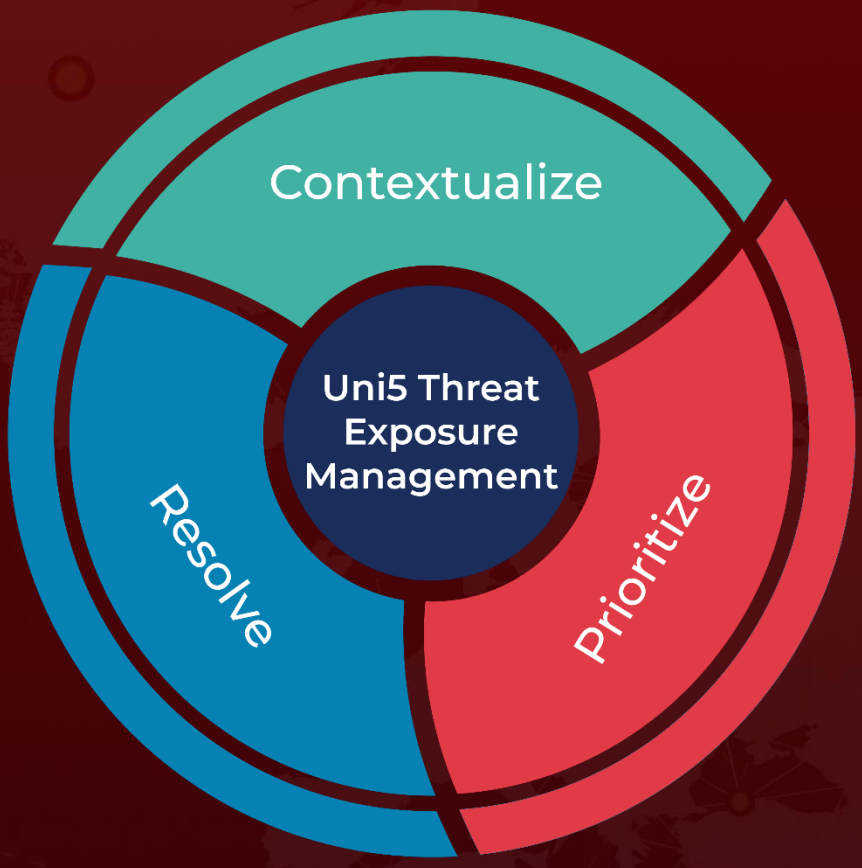
https://securelist.com/operation-synchole-watering-hole-attacks-by-lazarus/116326/

https://www.krcert.or.kr/kr/bbs/view.do?searchCnd=&bbsId=B0000133&searchWrd=&menuNo=205020&pageIndex=1&categoryCode=&nttId=71693

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

April 25, 2025 • 5:45 AM

More at www.hivepro.com