IMPORTANT CYBERSECURITY NEWS: LAZARUS HITS 6 SOUTH KOREAN FIRMS VIA CROSS EX, INNORIX FLAWS AND THREATNEEDLE MALWARE

Vairav Cyber Security News Report

Date: April 25, 2025

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148

Baluwatar, Kathmandu

Phone: +977 4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

EXECUTIVE SUMMARY

A recent cybersecurity campaign, dubbed "Operation Synchole," orchestrated by the North Korean-linked Lazarus Group, has targeted multiple South Korean organizations across the software, IT, finance, and telecommunications sectors. Utilizing watering hole attacks, the threat actors exploited vulnerabilities in widely used South Korean software, including Innorix Agent and CrossEX, to deliver malicious payloads such as the PowerModul malware. This campaign underscores the persistent threat posed by Lazarus and highlights the importance of securing software supply chains and web infrastructures.

DETAILS OF THE INCIDENT

Description of the Cyber Threat: Operation Synchole represents a sophisticated watering hole attack campaign where the Lazarus Group compromised legitimate websites frequented by target organizations. By injecting malicious scripts into these sites, they exploited vulnerabilities in South Korean software products, notably Innorix Agent and CrossEX, to facilitate the download and execution of malware on visitors' systems. The primary malware deployed, PowerModul, is a modular backdoor that allows for extensive control over infected machines, including data exfiltration and command execution.

Identification: The campaign was uncovered by Kaspersky's Global Research and Analysis Team (GReAT), who identified the malicious activities through threat intelligence and analysis of the compromised websites and malware samples. Their investigation revealed the tactics, techniques, and procedures (TTPs) employed by Lazarus in this operation.

Threat Actor: The Lazarus Group, a well-known Advanced Persistent Threat (APT) group linked to North Korea, is attributed to this campaign. They have a history of conducting cyber espionage and financially motivated attacks worldwide.

Affected Entities/Industries: The campaign primarily targeted organizations in South Korea, specifically within the software development, information technology, financial services, and telecommunications sectors.

Potential Impact: The successful exploitation of these vulnerabilities could lead to unauthorized access to sensitive information, disruption of services, financial losses, and potential further compromise of connected networks. The deployment of PowerModul allows attackers to maintain persistent access, execute arbitrary commands, and exfiltrate data, posing significant risks to affected organizations.

Exploitation Methods:

- Compromise of legitimate websites (watering hole attacks)
- Exploitation of vulnerabilities in South Korean software (e.g., Innorix Agent, CrossEX)
- Deployment of malicious scripts to deliver PowerModul malware
- Use of obfuscated JavaScript and PowerShell commands for malware execution

RELATED THREAT INTELLIGENCE & IOCs

Suspicious URLs

- *www[.]smartmanagerex[.]com*
- *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*

Malware Hashes (MD5)

- *f1bcb4c5aa35220757d09fc5feea193b*
- *dc0e17879d66ea9409cdf679bfea388c*
- *2d47ef0089010d9b699cd1bbbc66f10a*

RECOMMENDED ACTIONS

Immediate Mitigation Steps

- Identify and patch vulnerabilities in Innorix Agent, CrossEX, and other affected software.
- Scan networks for indicators of compromise (IOCs) related to PowerModul and associated infrastructure.
- Isolate and remediate infected systems to prevent further spread.

Security Best Practices

- Implement network segmentation to limit lateral movement.
- Regularly update and patch all software and systems.
- Educate employees on recognizing phishing attempts and suspicious websites.
- Deploy web filtering solutions to block access to known malicious domains.

For Advanced Security Teams

- Conduct threat hunting exercises focusing on TTPs associated with Lazarus Group.
- Monitor for unusual outbound traffic patterns indicative of data exfiltration.
- Utilize behavioral analytics to detect anomalies in user and system activities

ADDITIONAL RESOURCES AND OFFICIAL STATEMENTS

- https://thehackernews.com/2025/04/lazarus-hits-6-south-korean-firms-via.html
- https://securelist.com/operation-synchole-watering-hole-attacks-by-lazarus/116326/

CONTACT US

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

Website: https://vairavtech.com