مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Operation Phantom Circuit: Cyber Espionage Campaign

Tracking #:432316822

Date:04-02-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cybersecurity Council has observed that security researchers reported the Lazarus Group launched a global cyberattack, codenamed Operation Phantom Circuit, targeting developers in the technology and cryptocurrency sectors starting in late 2024.

TECHNICAL DETAILS:

In December 2024, the Lazarus Group, advanced persistent threat (APT) group launched a sophisticated global cyber campaign dubbed Operation Phantom Circuit. The operation targeted cryptocurrency and technology developers by embedding malware into trusted development tools, compromising over 1,500 systems worldwide. The campaign leveraged advanced obfuscation techniques, including VPNs and proxy servers in Hasan, Russia, to evade detection and exfiltrate sensitive data such as development credentials, authentication tokens, and system configurations.

The Lazarus Group's infrastructure demonstrated unprecedented sophistication, featuring a custom-built administrative platform powered by React and Node.js to manage stolen data. This campaign highlights a critical shift in their tactics, emphasizing stealth, scalability, and long-term access to compromised systems.

Infrastructure:

- C2 servers hosted on Stark Industries infrastructure.
- Traffic routed through Astrill VPNs and Oculus Proxy nodes in Hasan, Russia, to obscure origins.
- Data exfiltrated to Dropbox for storage and organization.

Tactics, Techniques, and Procedures (TTPs):

- Malware embedded in trusted software updates.
- Use of spoofed domains and persistent remote desktop protocol (RDP) sessions.
- Advanced administrative platform for managing stolen data.

Indicators of Compromise (IOCs)

- 94.131.9.32
- 185.153.182.241
- 86.104.74.51
- 5.253.43.122
- 45.128.52.14
- sageskills-uk[.]com

RECOMMENDATIONS:

- Conduct thorough audits of third-party software and libraries used in development environments.
- Deploy endpoint detection and response (EDR) solutions to identify suspicious activity.
- Monitor network traffic for connections to known malicious IPs and domains.
- Enforce strict access controls and multi-factor authentication (MFA) for all systems.

- Ensure all software, including development tools, is up to date with the latest security patches.
- Educate developers and IT staff on the risks of using untrusted software and the importance of verifying sources.
- Subscribe to threat intelligence feeds to stay informed about emerging threats and indicators of compromise (IOCs).
- Share information with industry peers and cybersecurity organizations to improve collective defense.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://securityscorecard.com/blog/operation-phantom-circuit-north-koreas-global-data-exfiltration-campaign/