January 30, 2023

Lazarus Group's React-Based Admin Panel for Global Cyber Attacks

Overview

Lazarus Group, a North Korean state-sponsored threat actor, has been found using a React-based web-admin panel to manage its command-and-control (C2) infrastructure, centralizing attack operations across multiple campaigns. This Node.js-backed platform facilitated the delivery of malicious payloads, victim management, and data exfiltration, primarily in **Operation Phantom Circuit**, which targeted the cryptocurrency sector and developers worldwide between September 2024 and January 2025. The attack, which affected 233 victims, relied on trojanized software, LinkedIn-based social engineering, and VPN obfuscation techniques to evade detection, with traffic routed through Astrill VPN and Oculus Proxy exit nodes.

CTI Analysis

The campaign employed a sophisticated blend of social engineering, supply chain compromise, and hidden C2 infrastructure to infect victims and maintain persistence. Lazarus Group tricked targets into downloading backdoored applications, enabling remote control and data theft via React-based admin panels hosted on Stark Industries servers. Obfuscated traffic through VPN services and proxy networks made attribution challenging, but links to North Korea were established through six distinct IP addresses and previous use of Astrill VPN, which has ties to fraudulent IT schemes. The attack's structure suggests a high level of coordination, automation, and adaptability, allowing Lazarus to fine-tune tactics while maintaining a centralized control system.

Impact Analysis

The campaign had significant implications for the cryptocurrency and technology sectors, exposing financial institutions, blockchain developers, and software companies to data breaches, asset theft, and operational disruptions. Victims were identified across multiple

regions, with Brazil, France, and India being primary targets, and over 110 unique victims in India alone in January 2025. By compromising legitimate software supply chains, Lazarus expanded its reach while making detection more difficult, leading to potential long-term consequences for organizations and individuals that unknowingly installed the infected applications.

Mitigation Strategies

- Organizations and individuals must adopt proactive security measures to defend against similar threats, including cryptographic code signing for software, strict network monitoring, and multi-factor authentication (MFA) to prevent unauthorized access.
- Security awareness training is crucial to counter LinkedIn-based social engineering tactics.
- Intrusion Detection/Prevention Systems (IDS/IPS) should be configured to detect unusual C2 traffic patterns.
- Regular threat intelligence monitoring and incident response planning will further strengthen defenses, ensuring a swift and effective response to emerging attack methods.

Conclusion

The React-based C2 infrastructure used in Operation Phantom Circuit highlights Lazarus Group's ability to innovate and refine its cyber-attack strategies, posing a persistent threat to high-value targets in the financial and technology sectors. By exploiting supply chain vulnerabilities, leveraging advanced obfuscation techniques, and deploying centralized victim management systems, the group has demonstrated an evolving threat model that requires continuous vigilance and enhanced cybersecurity measures. Organizations must remain alert to evolving attack techniques, implement strong security controls, and foster a culture of cybersecurity awareness to mitigate the risks posed by state-sponsored cyber threats.

Source:

- https://thehackernews.com/2025/01/lazarus-group-uses-react-based-admin.html