February 06, 2025

Cross-Platform JavaScript Stealer Targets Crypto Wallets in New Lazarus Group Campaign

Overview: The Lazarus Group is conducting a cyber campaign using fake LinkedIn job offers in the crypto and travel sectors to infect Windows, macOS, and Linux systems. Victims are tricked into providing personal data and downloading malicious GitHub/Bitbucket repositories that contain an obfuscated JavaScript stealer. This malware harvests crypto wallet credentials, deploys a Python-based backdoor, and installs .NET malware to maintain persistence, exfiltrate data, and run a crypto miner.

CTI Analysis: This campaign follows the Contagious Interview pattern, leveraging social engineering and multi-stage malware. The attack chain includes phishing via LinkedIn, delivering malicious repositories, and executing JavaScript, Python, and .NET payloads to steal credentials, hijack clipboards, evade defenses, and establish C2 communication via Tor. Victims are instructed to clone or debug Web3 repositories, ensuring execution of the malicious code.

Impact Analysis: The attack leads to financial loss through crypto wallet theft, data exfiltration from LinkedIn, GitHub, and browsers, and operational disruption due to persistent backdoors and resource-intensive malware. Reputational damage is also a risk, as victims may unknowingly spread malware within their networks.

Mitigation

- **Awareness & Training**: Educate employees on LinkedIn phishing scams and fake recruiters.
- **Endpoint & Network Security**: Use EDR solutions and firewall rules to block C2 domains.

- **Secure Development**: Avoid running unverified GitHub code outside sandbox environments.
- **Multi-Factor Authentication**: Enable MFA for LinkedIn, GitHub, and crypto wallets.
- **Browser & Wallet Security**: Update/remove browser extensions and use hardware wallets.
- **Threat Intelligence**: Monitor threat reports and implement incident response playbooks.

Conclusion: The Lazarus Group's LinkedIn job scam is a highly sophisticated attack targeting cryptocurrency professionals through multi-platform malware. Victims are lured into running malicious repositories, leading to credential theft, persistent access, and financial loss. Organizations must enhance employee awareness, endpoint protection, secure development, and authentication measures to mitigate these ongoing cyber threats.

Source:

- https://thehackernews.com/2025/02/cross-platform-javascript-stealer.html