IMPORTANT CYBERSECURITY NEWS: REDOX STEALER CAMPAIGN ABUSES GITHUB TO TARGET GAMERS AND SOFTWARE PIRATES

Vairav Cyber Security News Report

Date: March 04, 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 new malware distribution campaign leveraging GitHub repositories has been identified, spreading Redox Stealer, an information-stealing malware targeting gamers, modding enthusiasts, and software pirates. Cybercriminals are creating thousands of fake repositories offering modifications, game cheats, and cracked software to lure victims. Once downloaded and executed, the malware silently exfiltrates sensitive data—including banking credentials, crypto wallet keys, and gaming accounts—to Discord-controlled servers. Attackers use SEO poisoning and AI-generated content to evade detection and maximize visibility.

INCIDENT ANALYSIS

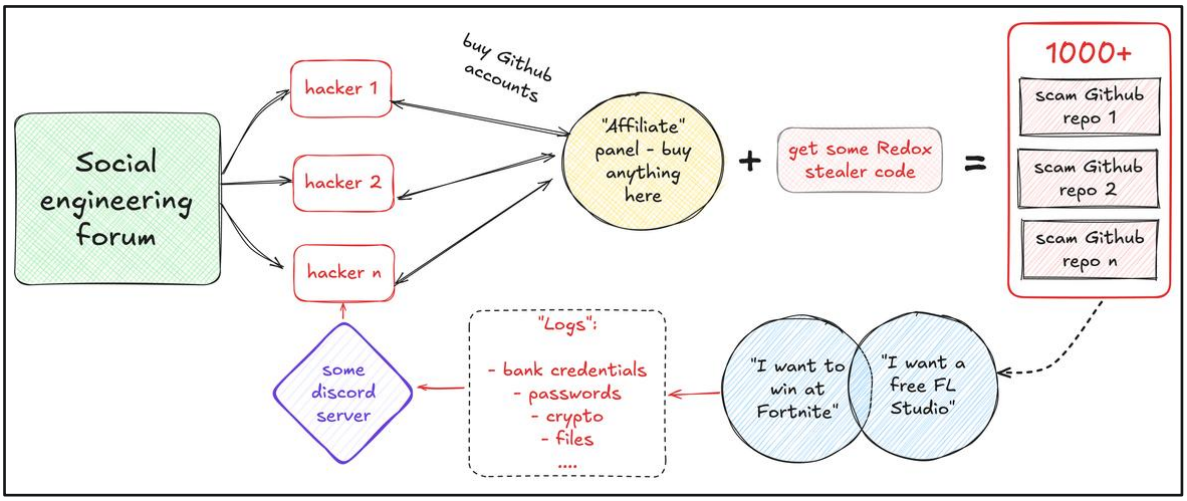

Figure 1: GitHub Scams process

Cybercriminals exploit GitHub repositories to distribute Redox Stealer, disguising malware as game mods, software cracks, and cheats for Roblox, Fortnite, FL Studio, and Photoshop. The attack chain involves:

- SEO poisoning to rank malicious repositories higher in search results.
- AI-generated README files and fabricated screenshots to enhance credibility.
- Obfuscated malware payloads hidden in ZIP/RAR archives to bypass security checks.
- Data theft targeting stored passwords, crypto wallets, banking details, and gaming accounts.

The stolen data is sent to Discord webhooks, allowing attackers to sift through logs for high-value credentials manually. Over 1,115 malicious repositories have been identified, with GitHub struggling to keep pace as attackers continuously re-upload under new accounts.

The Redox Stealer campaign demonstrates how cybercriminals weaponize legitimate platforms to distribute malware at scale. Attackers effectively bypass traditional security defenses by leveraging GitHub for hosting and Discord for exfiltration. Users must remain vigilant, scrutinize repository sources, and adopt robust cybersecurity measures to prevent credential theft.

RECOMMENDED ACTIONS

To mitigate the risk posed by the Redox Stealer campaign, users should:

- Verify sources before downloading mods, cheats, or cracked software.
- Avoid downloading software from GitHub repositories with minimal history or suspicious metadata.
- Use security tools that detect obfuscated scripts in compressed archives.
- Monitor clipboard activity for unauthorized data exfiltration.
- Enable two-factor authentication (2FA) on gaming, banking, and cryptocurrency accounts.
- Report suspicious repositories to GitHub and Discord for takedown.

RESOURCES

https://securityonline.info/massive-github-malware-campaign-targets-gamers-and-software-pirates-with-redox-stealer/

https://timsh.org/github-scam-investigation-thousands-of-mods-and-cracks-stealing-your-data/

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