IMPORTANT CYBERSECURITY NEWS: ENCRYPTHUB DEPLOYS RANSOMWARE AND STEALER VIA TROJANIZED APPS, PPI SERVICES, AND PHISHING

Vairav Cyber Security News Report

Date: March 7, 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 incident involving a financially motivated threat actor known as EncryptHub has been actively orchestrating sophisticated phishing campaigns to deploy information stealers and ransomware. The group has also been working on a new malware product, EncryptRAT. Security researchers at Outpost24 KrakenLabs and PRODAFT have observed EncryptHub leveraging trojanized applications, Pay-Per-Install (PPI) distribution services, and advanced social engineering techniques. EncryptHub is linked to RansomHub and Blacksuit ransomware groups and continues to evolve its attack strategies, posing a significant cybersecurity risk.

DETAILS OF THE INCIDENT

Description of the Cyber Threat: EncryptHub has been actively distributing trojanized versions of popular applications to deploy stealer malware and ransomware. Once access is gained, EncryptHub runs PowerShell scripts to deploy malware such as Fickle, StealC, and Rhadamanthys, which often lead to ransomware infections.

Identification: Security researchers at Outpost24 KrakenLabs and PRODAFT identified EncryptHub's malicious activities. Analysis of underground forums, such as XSS, revealed EncryptHub's use of LabInstalls for malware distribution.

Threat Actor: EncryptHub, also tracked as LARVA-208 by PRODAFT, is affiliated with RansomHub and Blacksuit ransomware groups. The group has been active since June 2024 and continues to evolve its techniques.

Affected Entities/Industries: The campaign has been observed targeting users of popular applications by distributing their trojanized versions. These include counterfeit versions of QQ Talk, QQ Installer, WeChat, DingTalk, VooV Meeting, Google Meet, Microsoft Visual Studio 2022, and Palo Alto Global Protect.

Potential Impact: The activities of EncryptHub pose significant risks, including financial losses due to ransomware attacks, operational downtime, data breaches, and reputational damage for affected organizations.

Exploitation Methods: The group employs phishing sites impersonating IT teams and helpdesks to steal credentials. Additionally, they use trojanized applications for initial access, Pay-Per-Install services to distribute malware at scale, and PowerShell scripts to execute payloads and gain further control over infected systems.

RECOMMENDED ACTIONS

Immediate Mitigation Steps

- Monitor and restrict execution of PowerShell scripts.
- Implement multi-factor authentication (MFA) for VPN access.

Security Best Practices

- Conduct security awareness training on phishing and social engineering tactics.
- Implement endpoint detection and response (EDR) solutions.
- Regularly update and patch software to mitigate exploit risks.

For Advanced Security Teams

- Monitor threat intelligence feeds for new IOCs.
- Conduct proactive threat hunting for EncryptHub-related indicators.
- Isolate and analyze suspected trojanized applications in a sandbox environment.

ADDITIONAL RESOURCES AND OFFICIAL STATEMENTS

- https://thehackernews.com/2025/03/encrypthub-deploys-ransomware-and.html
- https://catalyst.prodaft.com/public/report/larva-208/overview
- https://outpost24.com/blog/unveiling-encrypthub-multi-stage-malware/

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