BREAKING CYBERSECURITY NEWS: EncryptHub BREACHES 618 ORGS TO DEPLOY INFOSTEALERS, RANSOMWARE

Vairav Cyber Security News Report

Date: 2025-02-27

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

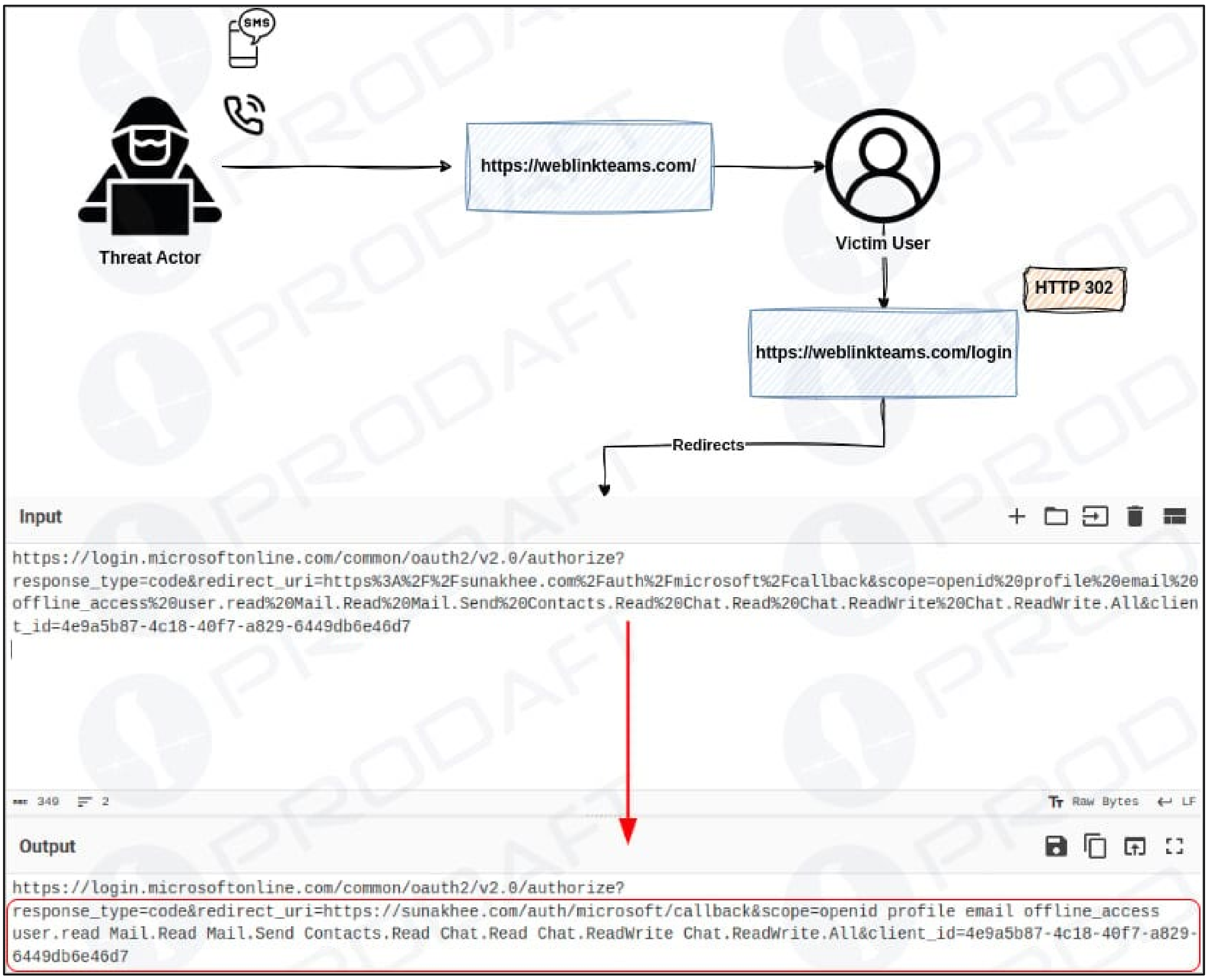
Thirbam Sadak 148
Baluwatar, Kathmandu

Phone: +977 4541540
Mobile: +977-9820105900
Email: sales@vairavtech.com

EXECUTIVE SUMMARY

A recent cybersecurity incident involving the threat actor known as 'EncryptHub' or 'Larva-208' has resulted in the compromise of at least 618 organizations worldwide. Attackers employed spear-phishing and social engineering techniques to infiltrate corporate networks, subsequently deploying information stealers and ransomware. This incident underscores the evolving tactics of cybercriminals and highlights the critical need for robust security measures to protect organizational data and infrastructure.

DETAILS OF THE INCIDENT



```
https://login.microsoftonline.com/common/oauth2/v2.0/authorize?
response_type=code&redirect_uri=https%3A%2F%2Fsunakhee.com%2Fauth%2Fmicrosoft%2Fcallback&scope=openid%20profile%20email%20
offline_access%20user.read%20Mail.Read%20Mail.Send%20Contacts.Read%20Chat.Read%20Chat.ReadWrite%20Chat.ReadWrite.All&clien
t_id=4e9a5b87-4c18-40f7-a829-6449db6e46d7
```

```
https://login.microsoftonline.com/common/oauth2/v2.0/authorize?
response_type=code&redirect_uri=https://sunakhee.com/auth/microsoft/callback&scope=openid profile email offline_access
user.read Mail.Read Mail.Send Contacts.Read Chat.Read Chat.ReadWrite Chat.ReadWrite.All&client_id=4e9a5b87-4c18-40f7-a829-
6449db6e46d7
```

Figure 1: Infection Chain of EncryptHub campaign

Description of the Cyber Threat: EncryptHub conducted targeted spear-phishing and social engineering campaigns to gain unauthorized access to corporate networks. Post-infiltration, they deployed Remote Monitoring and Management (RMM) tools and malicious software, including information stealers like Stealc and Rhadamanthys, and in many cases, ransomware. Active since June 2024, EncryptHub has compromised over 618 organizations. Their attack vectors include SMS phishing, voice phishing, and counterfeit login pages mimicking corporate VPN solutions such as Cisco AnyConnect, Palo Alto GlobalProtect, Fortinet, and Microsoft 365. These tactics are designed to harvest user credentials and multi-factor authentication tokens in real-time. The group is also linked to other ransomware operations like RansomHub and BlackSuit, suggesting a role as an initial access broker or direct affiliate.

Identification: The cybersecurity firm Prodaft identified and reported on EncryptHub's activities, releasing an internal report last week that was made public on February 25, 2025. The report details the group's methods and the scope of their operations.

Threat Actor: EncryptHub, also known as Larva-208, is the primary threat actor. They are associated with ransomware groups RansomHub and BlackSuit, indicating possible collaboration or shared resources among these entities.

Affected Entities/Industries: The attack has affected a diverse range of industries on a global scale. Specific organizations have not been publicly disclosed, but the widespread nature of the compromise suggests that multiple sectors are at risk.

Potential Impact: Organizations compromised by EncryptHub face significant risks, including financial losses in the form of costs associated with ransom payments, system restoration, and potential regulatory fines, operational downtime in the form of disruption of business activities due to encrypted or inaccessible data, data exposure in the form of unauthorized access to sensitive information and Reputational Damage due to erosion of trust from clients, partners, and the public.

Exploitation Methods: EncryptHub's methods include phishing campaigns utilizing SMS and voice phishing to deceive employees into revealing credentials, fake login pages by creating counterfeit portals resembling legitimate VPN and corporate login interfaces to capture authentication details, deployment of RMM tools by installing software like AnyDesk, TeamViewer, ScreenConnect, Atera, and Splashtop to maintain persistent remote access and malware deployment by introducing information-stealing malware and custom PowerShell-based ransomware to extract data and encrypt systems.

RECOMMENDED ACTIONS

Immediate Mitigation Steps

- **Enhance Email and Communication Security**: Implement advanced email filtering to detect and block phishing attempts.
- **User Education**: Conduct training sessions to help employees recognize and report phishing and social engineering attempts.
- **Multi-Factor Authentication (MFA)**: Enforce MFA across all user accounts to add an extra layer of security.
- **Network Monitoring**: Continuously monitor network traffic for signs of unauthorized access or data exfiltration.

Security Best Practices

- **Regular Software Updates:** Keep all systems and applications up to date with the latest security patches.
- **Access Controls:** Apply the principle of least privilege, ensuring users have only the access necessary for their roles.
- **Incident Response Plan:** Develop and regularly update an incident response plan to address potential security breaches promptly.
- **Data Backups:** Maintain regular, secure backups of critical data to facilitate recovery in case of an attack.

For Advanced Security Teams

- **Threat Hunting:** Proactively search for signs of compromise related to EncryptHub's known tactics and tools.
- **IOC Monitoring:** Stay informed about emerging IOCs related to EncryptHub and update detection systems accordingly.

- **Network Segmentation:** Isolate critical systems to prevent lateral movement within the network.
- **Collaboration:** Engage with cybersecurity communities and information-sharing organizations to stay updated on the latest threats and mitigation strategies.

ADDITIONAL RESOURCES AND OFFICIAL STATEMENTS

- https://www.bleepingcomputer.com/news/security/encrypthub-breaches-618-orgs-to-deploy-infostealers-ransomware/
- https://catalyst.prodaft.com/public/report/larva-208/overview

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