BREAKING CYBERSECURITY NEWS: NEW MALWARE CAMPAIGN USES CRACKED SOFTWARE TO SPREAD LUMMA AND ACR STEALER

Vairav Cyber Security News Report

Date: 2025-02-25

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

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

Thirbam Sadak 148
Baluwatar, Kathmandu

EXECUTIVE SUMMARY

A recent cybersecurity incident has emerged where attackers are distributing information-stealing malware, specifically Lumma and ACR Stealer, through cracked software versions. Users downloading pirated applications are at risk of compromising sensitive data, including personal information and financial records. Attackers employ sophisticated techniques, such as dead drop resolvers, to conceal their command-and-control (C2) servers, making detection and mitigation challenging. Security experts advise individuals and organizations to avoid using unauthorized software and to implement robust security measures to protect against such threats.

DETAILS OF THE INCIDENT

Description of the Cyber Threat: Cybercriminals are leveraging cracked versions of popular software to disseminate malware like Lumma and ACR Stealer. Once installed, these malicious programs harvest a wide range of information from compromised systems, including files, web browser data, and cryptocurrency wallet extensions. The threat actors utilize a technique known as a dead drop resolver to extract the actual C2 server addresses. This involves embedding encoded C2 information within legitimate services such as Steam, Telegram's Telegraph, Google Forms, and Google Slides. The malware accesses these services, decodes the C2 address, and establishes communication for further malicious activities.

Identification: The AhnLab Security Intelligence Center (ASEC) observed a significant increase in ACR Stealer distributions starting in January 2025. Their analysis uncovered the use of dead drop resolvers and the exploitation of legitimate platforms to obfuscate malicious operations.

Affected Entities/Industries: Individuals and organizations engaging in the download and installation of unauthorized or pirated software are primarily at risk. This includes sectors where software licensing costs are high, potentially leading users to seek unlicensed alternatives.

Potential Impact: The deployment of Lumma and ACR Stealer can lead to significant financial losses, operational disruptions, exposure of sensitive data, and reputational damage. Stolen credentials and data can be sold on underground forums, facilitating further attacks such as identity theft, fraud, and unauthorized access to corporate networks.

Exploitation Methods: Attackers distribute malware through cracked software available on various platforms, including file-sharing websites and forums. The malware employs dead drop resolvers, utilizing legitimate services to retrieve encoded C2 addresses, thereby evading traditional detection mechanisms.

RECOMMENDED ACTIONS

Immediate Mitigation Steps

- Uninstall any unauthorized or pirated software from all systems.
- Conduct comprehensive scans using updated antivirus and anti-malware solutions to detect and remove potential infections.
- Change passwords and enable multi-factor authentication for all sensitive accounts.

Security Best Practices

- Educate users about the risks associated with downloading and using pirated software.
- Implement application whitelisting to allow only approved software to run on systems.
- Regularly update and patch all software and operating systems to protect against known vulnerabilities.

For Advanced Security Teams

- Monitor network traffic for anomalies, particularly communications with external services that may serve as dead drop resolvers.
- Utilize threat intelligence feeds to stay informed about emerging threats and associated IOCs.

- Develop and test incident response plans specifically addressing malware infections originating from unauthorized software.

ADDITIONAL RESOURCES AND OFFICIAL STATEMENTS

- https://thehackernews.com/2025/02/new-malware-campaign-uses-cracked.html

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