IMPORTANT CYBERSECURITY NEWS: RESEARCHERS EXPOSE NEW POLYMORPHIC ATTACK THAT CLONES BROWSER EXTENSIONS TO STEAL CREDENTIALS

Vairav Cyber Security News Report

Date: March 11th, 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 revelation has uncovered a novel polymorphic attack targeting Chromium-based web browsers, including Google Chrome, Microsoft Edge, Brave, and Opera. This sophisticated technique enables malicious browser extensions to impersonate legitimate ones, leading to unauthorized access to users' credentials and sensitive information. Attackers exploit this method to deceive users into interacting with fake extensions, thereby compromising personal and financial data.

DETAILS OF THE INCIDENT

Description of the Cyber Threat: The attack involves malicious browser extensions that can morph to replicate any installed legitimate add-on. These polymorphic extensions duplicate the target's icon, HTML popup, and workflows, temporarily disabling the genuine extension to avoid detection. This deception convinces victims that they are interacting with their legitimate extensions while, in reality, their credentials are being harvested.

Identification: Cybersecurity researchers from SquareX identified and demonstrated this attack technique, highlighting its potential to compromise user security across various Chromium-based browsers.

Affected Entities/Industries: Users of Chromium-based web browsers, including Google Chrome, Microsoft Edge, Brave, and Opera, are at risk. Industries relying heavily on these browsers for daily operations, such as corporate environments, educational institutions, and individual users, could be affected.

Potential Impact: The risks include unauthorized access to personal and financial information, potential account takeovers, financial losses, and reputational damage for organizations if corporate credentials are compromised.

Exploitation Methods: Attackers publish malicious extensions disguised as utilities on extension marketplaces. Once installed, these extensions scan for specific target

extensions and morph to replicate them, deceiving users into providing sensitive information.

RECOMMENDED ACTIONS

Immediate Mitigation Steps

- Uninstall any suspicious or unnecessary browser extensions.
- Reset browser settings to default to remove potential malicious configurations.

Security Best Practices

- Install extensions only from trusted sources and verify their authenticity.
- Regularly review and manage installed browser extensions.
- Keep browsers and security software up to date to protect against known vulnerabilities.

For Advanced Security Teams

- Implement policies restricting the installation of unauthorized browser extensions.
- Monitor network traffic for unusual patterns indicative of malicious extension activity.
- Educate users about the risks associated with installing unverified browser extensions.

ADDITIONAL RESOURCES AND OFFICIAL STATEMENTS

- https://thehackernews.com/2025/03/researchers-expose-new-polymorphic.html
- https://labs.sqrx.com/polymorphic-extensions-dd2310006e04

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