U UNISPHERE SOLUTIONS

info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 0303

MALICIOUS BROWSER EXTENSION PHISHING CAMPAIGNS

DATE ISSUED: 10th April 2023

IMPACT	LOW	MEDIUM	[✓ HIGH]
EASE OF EXPLOIT	HARD	MEDIUM	[✓ EASY]

OVERVIEW

A new strain of malware dubbed Rilide uses a legitimate browser extension to target Chromium-based browsers such as Google Chrome, Microsoft Edge, Brave, and Opera. The malware disguises itself as a legitimate Google Drive extension, enabling threat actors to carry out malicious activities.

BREAKDOWN

Trustwave SpiderLabs discovered a browser extension that could allow attackers to conduct various malicious activities, including monitoring browsing history, taking screenshots, and injecting malicious scripts to withdraw funds from multiple cryptocurrency exchanges. There are two known separate campaigns distributing Rilide. The first uses Ekipa Remote Access Trojan (RAT), and the other uses Google Ads and Aurora Stealer to load the extension using a Rust loader. Once the malicious extension executes, it runs a script to connect to a command and control (C2) server that injects additional scripts into the webpage to steal cryptocurrencies, email account credentials, etc. The extension also disables 'Content Security Policy,' a security feature designed to protect against cross-site scripting (XSS) attacks, to load external resources that the browser would typically block. The extension has the ability to exfiltrate browsing history on a regular basis and capture screenshots to send to the C2. It can also utilise forged dialog pop-ups to deceive users into entering and thus revealing their two-factor authentication (2FA) and use this to proceed with withdrawing cryptocurrencies in the background.

REMEDIATION STEPS

- Insist employees only install extensions only from the official extension store and check the developer's credibility as part of due diligence checks. Enforce restrictions to browser extension installation through policy.
- Educate employees on techniques that help them to avoid social engineering schemes, such as phishing attacks, and how to report suspicious system behaviours and to whom.
- Conduct regular security audits to identify and remove unnecessary installed add-ons and third-party apps and services.
- Use a layered approach that utilises a combination of detection tools and protection capabilities, i.e., combine Next-Generation Firewalls (NGFW) and anti-virus/malware software (NGAV), implement an Intrusion Detection and/or Prevention System (IDS/IPS) to detect and protect against malware.
- Continuously monitor network traffic, and use real-time threat intelligence feeds to add context to security alerts.

REFERENCES & RESOURCES

The Bleeping Computer	https://www.bleepingcomputer.com/news/security/hackers-use-rilide-browser-extension-to-bypass-2fa-steal-crypto/