UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 0400

RILIDE MALWARE TARGETS CHROMIUM BROWSERS

DATE ISSUED: 9th August 2023

IMPACT	LOW	MEDIUM	**HIGH**
EASE OF EXPLOIT	HARD	MEDIUM	**EASY**

OVERVIEW

A fresh variant of malicious software known as Rilide has been identified by cybersecurity experts. This malware specifically targets web browsers based on Chromium, aiming to pilfer sensitive information and hijack cryptocurrency.

BREAKDOWN

In April 2023, cybersecurity experts initially reported Rilide. They identified two distinct attack methods involving Ekipa RAT and Aurora Stealer, which were employed to distribute malicious browser extensions for data and cryptocurrency theft. It demonstrates increased sophistication due to its modular structure, coded complexity, and compatibility with Chrome Extension Manifest V3, with added functionalities like harvesting history and cookies and collecting login credentials. The latest malware extension now also targets banking accounts. It can exfiltrate the stolen data via a Telegram channel or by capturing screenshots at pre-determined intervals and sending them to the Command and Control (C2) server. A particular campaign is directed at various financial institutions, email services, cryptocurrency exchanges, VPNs, and cloud services. It employs injection scripts and predominantly targets users located in Australia and the United Kingdom.

REMEDIATION STEPS

- Educate Employees: Train the employees to recognise the risks associated with browser extensions and the potential signs of malicious activity. Encourage them to only use well-known and reputable extensions.
- Access Control: Limit the installation of browser extensions to authorized personnel only. Establish a policy that requires approval from IT or security teams before adding any new extensions.
- Regular Updates: Ensure that web browsers and extensions are kept up to date with the latest security patches and updates.
- Multi-Factor Authentication (MFA): Implement MFA for accessing sensitive systems and data.

REFERENCES & RESOURCES

Bleeping Computer https://www.bleepingcomputer.com/news/security/chrome-malware-rilide-targets-enterprise-users-via-powerpoint-guides/

The Hacker News https://thehackernews.com/2023/08/new-version-of-rilide-data-theft.html