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

CYBER GUIDANCE ISSUE 0312

VIPERSOFTX TARGETS PASSWORD MANAGERS

DATE ISSUED: 1st May 2023

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

OVERVIEW

A new version of ViperSoftX, an information-stealing malware, is targeting a wide range of browsers, cryptocurrency wallets, and most recently, password managers. The new version has more robust encryption, a broader range of targets, and better evasion techniques to avoid detection by security software.

BREAKDOWN

Trend Micro researchers have reported a new ViperSoftX information-stealing malware that can target more browsers and password managers. ViperSoftX is an information-stealing malware that infects computers, stealing personal and confidential data. The latest malware version targets password managers such as 1Password and KeePass, attempting to steal data stored in their browser extensions. The malware typically appears as software crackers, activators, or key generators using DLL sideloading to execute on the system to avoid detection. It is able to target a range of browsers, including Chrome, Brave, Edge, Opera, and Firefox. The malware targets the consumer and enterprise sectors worldwide, with over 50% of the detected activity originating from Australia, Japan, the United States, India, Taiwan, Malaysia, France, and Italy. The malware update includes a more sophisticated encryption method of byte remapping and a monthly change in the command-and-control (C&C) server. The malware's increased functionality highlights the importance of better security measures and stronger passwords for consumers and businesses to avoid falling victim to information-stealing malware.

REMEDIATION STEPS

- Set long and complex passwords, particularly master passwords for password managers, and enable multi-factor authentication wherever possible. Please refer to the Importance of Strong Passwords and Practices to create solid organization-wide password policies.
- Adopt a 'defence-in-depth' approach to your security strategy that provides layers of defence with several mitigations at each layer.
- Install and regularly update your Next Generation Antivirus software (NGAV)
- Network monitoring and analysis should be conducted regularly to detect and investigate anomalous network behaviour.

REFERENCES & RESOURCES

Bleeping Computer https://www.bleepingcomputer.com/news/security/vipersoftx-info-stealing-malware-now-targets-password-managers/

Trend Micro https://www.trendmicro.com/en_id/research/23/d/vipersoftx-updates-encryption-steals-data.html