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

# CYBER GUIDANCE ISSUE 0282

## NEW STEALC MALWARE-AS-A-SERVICE

**DATE ISSUED:** 27th February 2023

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

## OVERVIEW

Cybersecurity researches at Sekoia discovered a new information-stealing malware that is rapidly growing in popularity on dark web marketplaces. The malware tends to live in an infected computer and steals sensitive and confidential data to send it to the attacker.

## BREAKDOWN

A new information-stealing malware dubbed as 'Stealc' by researchers at Sekoia has emerged that shares stealing capabilities and similarities with comparable malware such as Vidar, Raccoon, Mars and Redline. It has been advertised on hacking forums by a user called "Plymouth" as a fully featured and ready-to-use stealer with an easy-to-use administration panel. The seller also set up a Telegram channel to promote the malware and publishes a new version every week. As well as promoting the malware to other malicious actors on various forums, the malware is currently being deployed through fake YouTube tutorials on how to crack software. The videos direct an unsuspecting user to a download website that will deploy Stealc. It collects sensitive data from web browsers, extension, cryptocurrency wallets, and applications like email clients and messenger software.

Threat actors may customize the data collection, which sets it apart from some of the other information stealers that are sold on the dark web. An additional component is a customizable file grabber, that looks for files specified during configuration, making this a very powerful and unpredictable tool. Once the data is stolen, it self-erases and downloaded DLL files are removed from the device to avoid detection.

## REMEDIATION STEPS

- Set up a robust anti-malware solution on all endpoint devices with schedule scanning enabled.
- Develop good security habits when browsing the Internet and refrain from opening unknown attachments.
- Always download software, updates, and plugins from trusted official websites, never third-party sites.
- Check that all software is up to date, including operating system, firmware, drivers, and software applications.

## REFERENCES & RESOURCES

The Bleeping Computer https://www.bleepingcomputer.com/news/security/new-stealc-malware-emerges-with-a-wide-set-of-stealing-capabilities/
Silicon Angle https://siliconangle.com/2023/02/21/new-stealc-information-stealing-malware-grows-popularity-dark-web/
Malware Bytes https://www.malwarebytes.com/blog/threats/info-stealers