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

# CYBER GUIDANCE ISSUE 00180

## RACOON STEALER-AS-ASERVICE PLATFORM UPDATES

**DATE ISSUED:** 9th August 2021

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

## OVERVIEW

Stealer-as-a-service platforms like Racoon Stealer are available for amateur hackers to dip their toes without having to develop their own toolset. The platform has had a recent update and now includes more tools than ever.

## BREAKDOWN

Racoon stealer specialised in using turnkey services to steal browser-stored passwords and authentication cookies and with the new update is now has tools available to mine cryptocurrencies, install malware droppers and exfiltrate files or other information. Leveraging Google Searches and SEO, the attackers plant their bait on websites that facilitate the download of pirated software, software crackers and key generators – a technique seen earlier this year featured in Cyber Guidance Issue 00116. When a victim accesses a link for the software, they are redirected to an AWS hosting JavaScripts that deliver variants of malware droppers. This behaviour comes as a shift away from the previous preferred delivery method of targeted inbox-based attack methods. The setup executable file is contained withing a 7zip or Winzip SFX (or similar) that must be opened by the user. Other capabilities include Clippers – tools that steal currency from crypto wallets, miners, malicious browser extensions, click-fraud bots for YouTube and Djvu/Stop – a ransomware typically used to target home users.

## REMEDIATION STEPS

- Never open zipped files from new or unusual websites
- Use blacklisting to prevent users from being able to visit known malicious websites.
- Educate users on the dangers of any practices relating to this article – particularly cracking software.

## REFERENCES & RESOURCES

Threatpost https://threatpost.com/raccoon-stealer-google-seo/168301/
Sophos https://news.sophos.com/en-us/2021/08/03/trash-panda-as-a-service-raccoon-stealer-steals-cookies-cryptocoins-and-more/