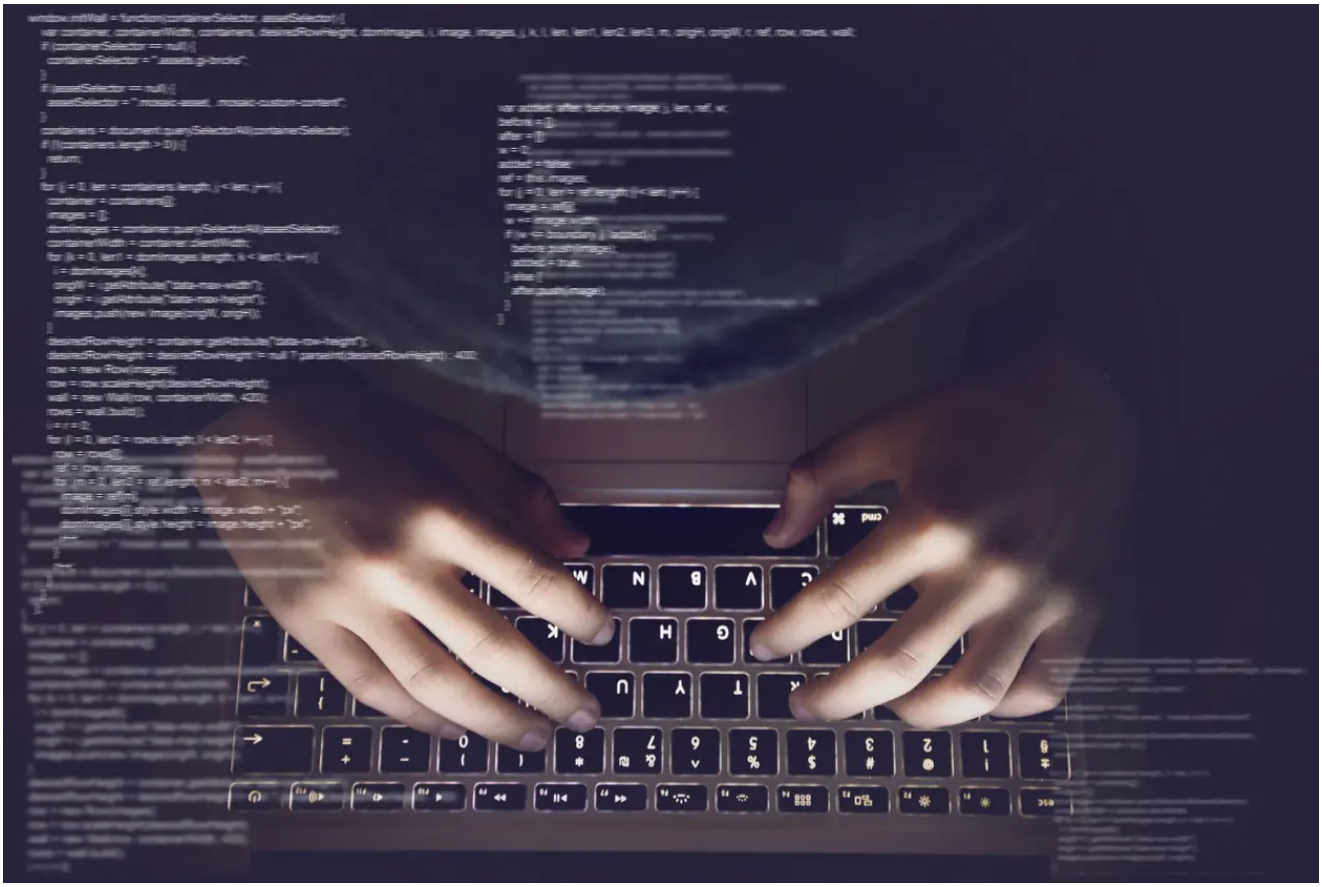
Raccoon Stealer Pivots Towards Self-Protection

zerofox.com/blog/raccoon-stealer-pivots-towards-self-protection/

September 23, 2021



BLOG

September 23, 2021 | by Stephan Simon

5 minute read

Malware has become an ever-growing threat in the cyber landscape with the rise in ransomware and as-a-service offerings. ZeroFox Threat Research has identified a change in focus among the developers of an information stealer known as Raccoon Stealer. In this post, we'll take a closer look at the pivot towards protecting this information stealer through the use of "crypters" and offer recommendations for how security teams can address this ongoing threat.

Defining Raccoon Stealer

An information stealer (also known as an infostealer) typically acts as a Trojan designed to gather information from a system. The most common stealers collect data such as usernames and passwords, which it then sends to another system via email, over a network or other means of export. Keyloggers are another popular information stealer that focuses on logging a user's keystrokes to uncover sensitive information and additional access.

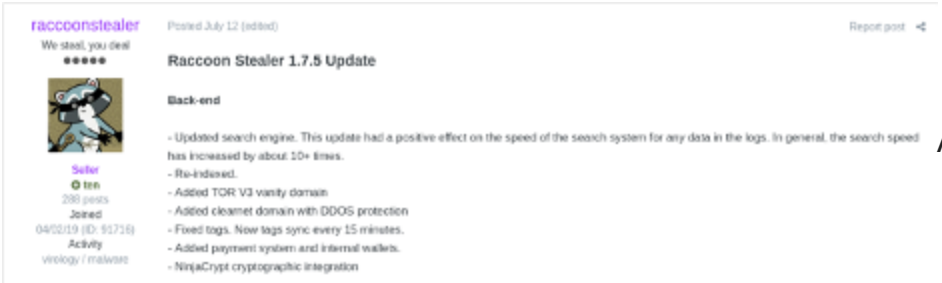
Raccoon Stealer is an information stealer type of malware first advertised on various underground forums in April 2019 by an actor going by the handle "raccoonstealer." Like most stealers, it can steal stored auto-fill data, cookies, credentials, credit card data and history from Chromium-based browsers such as Google Chrome and Microsoft Edge. Targeted theft of several cryptocurrency wallets is also supported. Updates often add support for new cryptocurrencies, though it can also be configured to locate any wallet.dat file as well.

Original advertisement for Raccoon Stealer (in Russian) in 2019
Source: ZeroFox Threat Research

Its focus is on being small, efficient and simple enough for anyone to use. To accomplish this, Raccoon Stealer was created as a service offering, complete with a cloud control panel allowing would-be subscribers to configure everything in “just a few clicks.” At just $75 per week or $200 per month, Raccoon Stealer is relatively cheap for threat actors as well.

Raccoon Stealer Updates Focus on Protecting Payloads

Multiple updates have happened since the start of the quarter, most notable among them being the addition of new “crypters.” A crypter’s purpose is to obfuscate a given binary by using tactics such as inserting junk code, breaking up the flow of code without changing the original functionality or encrypting sections of code so static signatures cannot detect them. Other updates include support for stealing several new cryptocurrency wallets and adding Discord to the list of targeted applications.



A Raccoon Stealer update adds support for a new crypter, “NinjaCrypt”
Source: ZeroFox Threat Research

On August 4, 2021, the actor raccoonstealer announced that they were looking to cooperate with other crypter developers and had completed an “automatic system for issuing an encrypted build.” This was seemingly in response to subscriber feedback.

Actor raccoonstealer announces they are seeking out new crypter projects
Source: ZeroFox Threat Research

The actor racoonstealer has also been observed reminding others that “usage without crypt is prohibited.”

Actor raccoonstealer reminds a subscriber that crypters must be used against deployed binaries
Source: ZeroFox Threat Research

The recently introduced “Raccoon Clipper” was also updated at the end of July 2021, adding support for the Monero and ZCash cryptocurrencies. Racoon Clipper is an add-on developed separately from the main stealer and works as the name may suggest: monitoring the Windows clipboard. Once it detects a supported cryptocurrency address, it will replace it with one configured by the subscriber in hopes that unsuspecting victims will continue the transaction, unaware that the target address has been changed.

Update notes for Raccoon Clipper, a paid add-on to Raccoon Stealer
Source: ZeroFox Threat Research

The group behind Raccoon Stealer has established itself as a capable group in the two years since they debuted, providing new features regularly and earning a primarily positive reputation within the community. They've also shown a willingness to add features based on the demands of their subscribers, as demonstrated by the recently created API for automatically generating encrypted builds. With the development of a new API for automatically providing obfuscated or "crypted" builds, new targeted applications and support for more cryptocurrency wallets, this quarter has been an active one for Raccoon Stealer.

Information Stealer Resources and Recommendations

As malware attacks continue to increase and the tactics evolve, security teams must act quickly. Here are a few recommendations from the ZeroFox Threat Research team:

- When breaches occur, always change known compromised passwords, as well as passwords on critical accounts.
- If the initial attack vector is known, ensure that the vulnerabilities leveraged are corrected immediately.
- Perform a penetration test to determine weaknesses in the network configuration and correct the findings as soon as possible.
- Enable 2-factor authentication for all your organizational accounts to help mitigate phishing and credential stuffing attacks.
- Review network logs for potential signs of compromise and data egress.
- Enforce administrative or application control restrictions to prevent the unauthorized installation of software or media.

The ZeroFox team continues to produce informative resources and engaging events to help security teams and organizations as a whole navigate unknown territory. To learn more about the top threat trends as well as predictions on the tactics and techniques expected to increase, download the latest ZeroFox Quarterly Threat Landscape Report.


ZEROFOX
Quarterly Threat Landscape Review: Q2 2021
PRINCETON
MUNICIPAL COURT
Full dump of data, direct link
Figure 4: Marketo Marketplace listing for data from Municipal Court of Princeton
Source: ZeroFox Threat Research
11
ZEROFOX
Quarterly Threat Landscape Review: Q2 2021
As part of ZeroFox Threat Research's ongoing tracking of ransomware groups on underground networks, we have observed fluctuating ransomware infection rates on a weekly basis. The highest volume of attacks this quarter was during the week of May 30, 2021, when there was an increase in Pysa ransomware attacks, followed by Avaddon and Conti. The lowest volume of attacks occurred during the week of June 27, 2021, with 23 attacks. Figure 5 is a bar chart displaying the number of victims of ransomware and digital extortion by week in Q2 2021.
Victim Count By Week: April - June
Figure 5: Ransomware and Digital Extortion by Week
Source: ZeroFox Threat Research
Legislation to Improve National Cybersecurity Response
Geopolitical & Physical
From the SolarWinds Orion breach to Microsoft Exchange Server vulnerabilities to continuous ransomware attacks, cybersecurity becomes more important as the number of attacks increases daily. Thus far in 2021, organizations around the world have been impacted by almost cyber threats, and this trend demonstrates that threat actors will not cease activity any time soon. This quarter, increased ransomware attacks on organizations prompted the US federal government to create a response plan to bolster national cybersecurity. Attacks like those against Colonial Pipeline, JBS, and Kaseya underscored the evolving threat of ransomware. Threat actors utilizing supply chain attacks and zero-day exploits demonstrate the
12