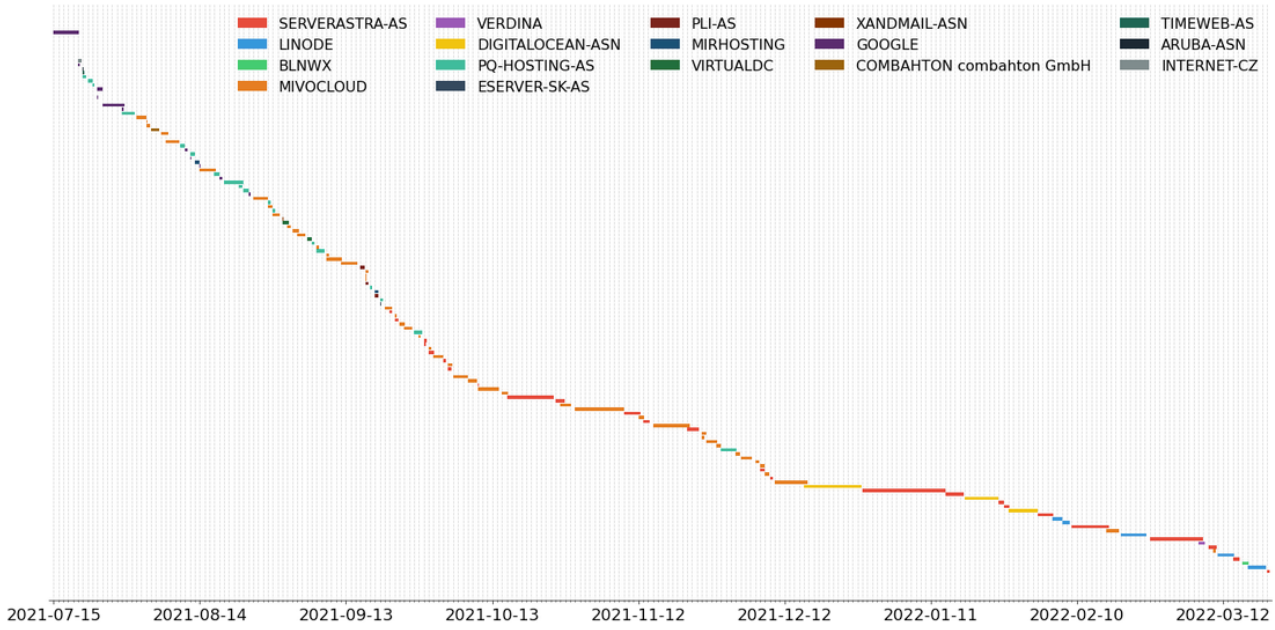
Raccoon Stealer – An Insight into Victim “Gates”

team-cymru.com/blog/2022/03/23/raccoon-stealer-an-insight-into-victim-gates/

S2 Research Team View all posts by S2 Research Team March 23, 2022



Co-authored by Brian Eckman, Josh Hopkins, Andy Kraus, and Paul Welte

Raccoon Stealer is one of 40-plus malware families tracked through Team Cymru’s Botnet Analysis and Reporting Service (BARS), a service which underpins our Threat Intelligence Feeds.

Introduction to Raccoon Stealer

Raccoon Stealer is an information stealer sold to ‘affiliates’ as a Malware-as-a-Service (MaaS) on multiple underground forums. Affiliates are provided access to a control panel hosted on the Tor network as an onion site, where they can generate new malware builds and review data collected from infected hosts.

Raccoon Stealer has been marketed as a service in the underground economy since at least April 2019.

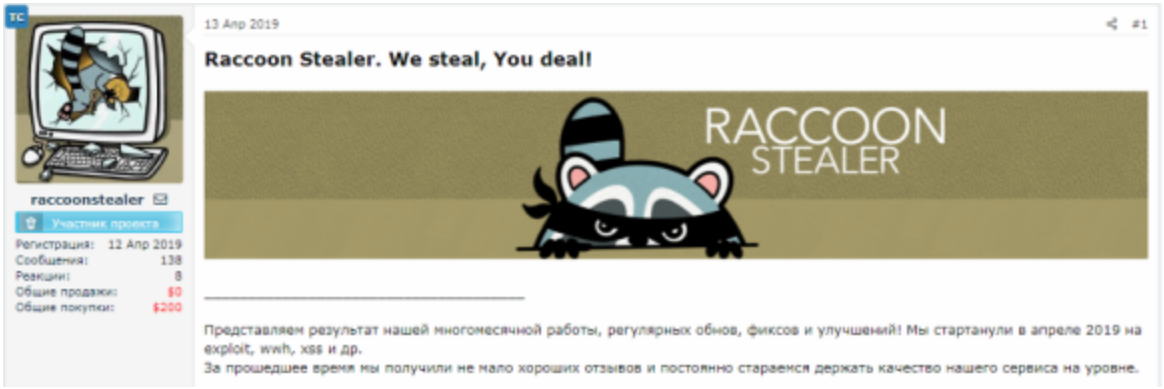


Figure 1 – Raccoon Stealer Advertisement

Raccoon Stealer has the capability to steal the following data from infected systems:

- Saved passwords
- Credit card information
- Cryptocurrency wallets
- Browser data (cookies, saved forms, etc.)

In this blog we will examine Raccoon Stealer's initial command and control (C2) infrastructure and assess the scale of the threat based on recent victim data.

Raccoon Stealer C2 Infrastructure

Raccoon Stealer advertisements refer to its back-end infrastructure as 'the heart' of the project. The following points are emphasised as strengths over its competitors:

- Automated deployment of new 'gates' to minimise downtime.
- Existing builds still function after new 'gates' are deployed.
- Control panel hosted on the Tor network as an onion site.

In this context, a *gate* is a reverse proxy that forwards traffic from victims to upstream C2 infrastructure.

At the time of execution, Raccoon Stealer samples retrieve the URL of the active *gate* from a Telegram channel that is unique to the affiliate. The URL is stored in an encrypted string located in the public description of the Telegram channel.

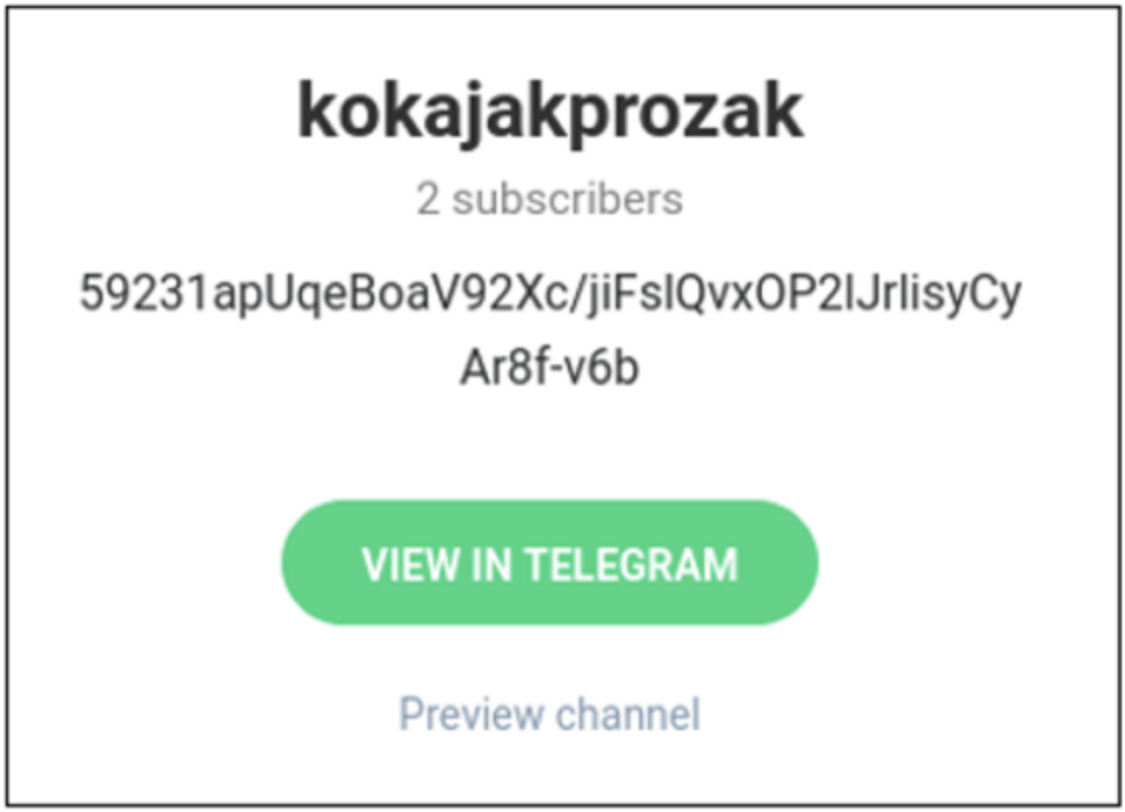


Figure 2 – An Example of an Affiliate Telegram Channel

A Telegram channel is created for each Raccoon Stealer affiliate, with the currently active *gate* information supplied as an encrypted string in the public channel description. When a new *gate* is deployed, the public channel description for all affiliates' Telegram channels are automatically updated to point to the new *gate*.

Further insight into the Raccoon Stealer infection chain is detailed in Avast's recent blog on the same topic.

Tracking *Gates*

Since July 2021 (a period of approximately 250 days), we have observed a total of 135 distinct *gates*, indicating an average 'up time' of less than two days. However, this average is impacted by a small number of longstanding *gates* – particularly around the Christmas / New Year period in 2021/22. Over 25% of the *gates* were active for less than 12 hours.

One key observation we were able to make is that regardless of the number of affiliates or Telegram channels in operation, Raccoon Stealer only ever uses a single *gate* IP address at any one time, which is consistent across all affiliate operations.

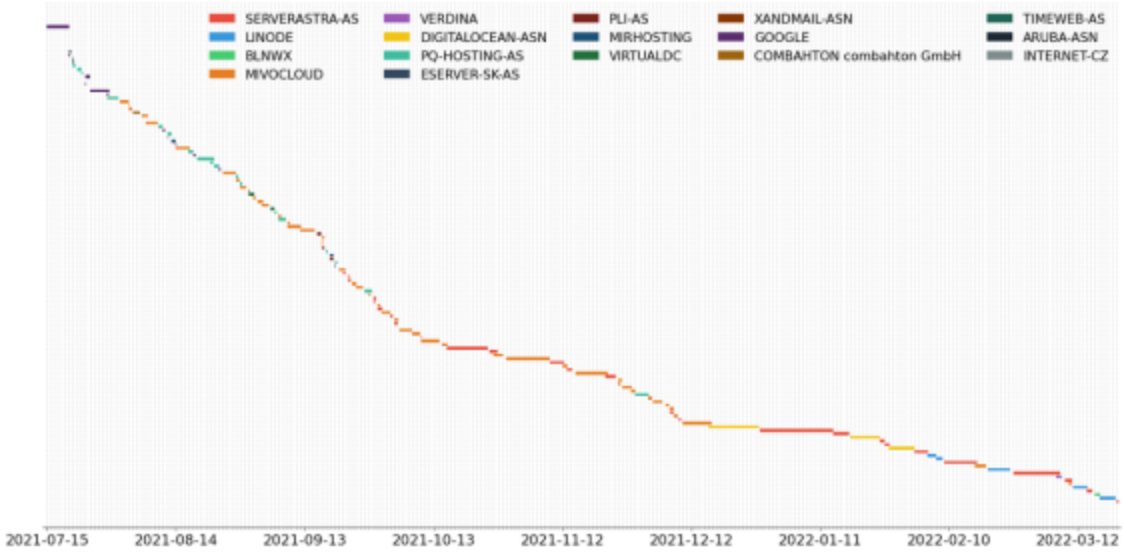


Figure 3 – A Summary of Raccoon Stealer 'Gates'

As can be seen, based on the legend in Figure 3, several hosting providers are utilised by the Raccoon Stealer operators. Since July 2021, a total of 17 distinct providers were observed, nearly half on just one occasion, with MIVOCLOUD (47), SERVERASTRA-AS (26), PQ-HOSTING-AS (21) and GOOGLE (18) being the most frequently occurring providers.

Overall, it is clear the operators of Raccoon Stealer have deployed a dynamic approach to limit the impact of cyber defence techniques (e.g., the active blocking of IPs) on their service. Although we would note that beyond the initial *gates* the infrastructure remains broadly static.

Victimology

Previous research published by Cybereason in October 2019 assessed that Raccoon Stealer had, at the time, already infected over 100,000 endpoints. In this victimology we seek to provide an updated indication as to the global impact of Raccoon Stealer today.

As previously referenced, during December 2021 and January 2022, several *gate* IP addresses remained static for multiple days. This afforded us the opportunity to examine a larger victim data sample than is usually available for any one particular *gate* IP address.

We will focus on two such *gates* which were active for 21-days combined.

When examining network telemetry for these *gates*, a total of ~95,000 distinct IP addresses were observed connecting over TCP/80 (the port used for initial victim connections to the *gate*).

Attempts were made to filter out 'unlikely' victims, for example by omitting connections from large hosting providers, or from IP addresses identified as proxies or anonymisation services. Caveats must also be made for occurrences involving dynamically assigned IPs or scanning activity.

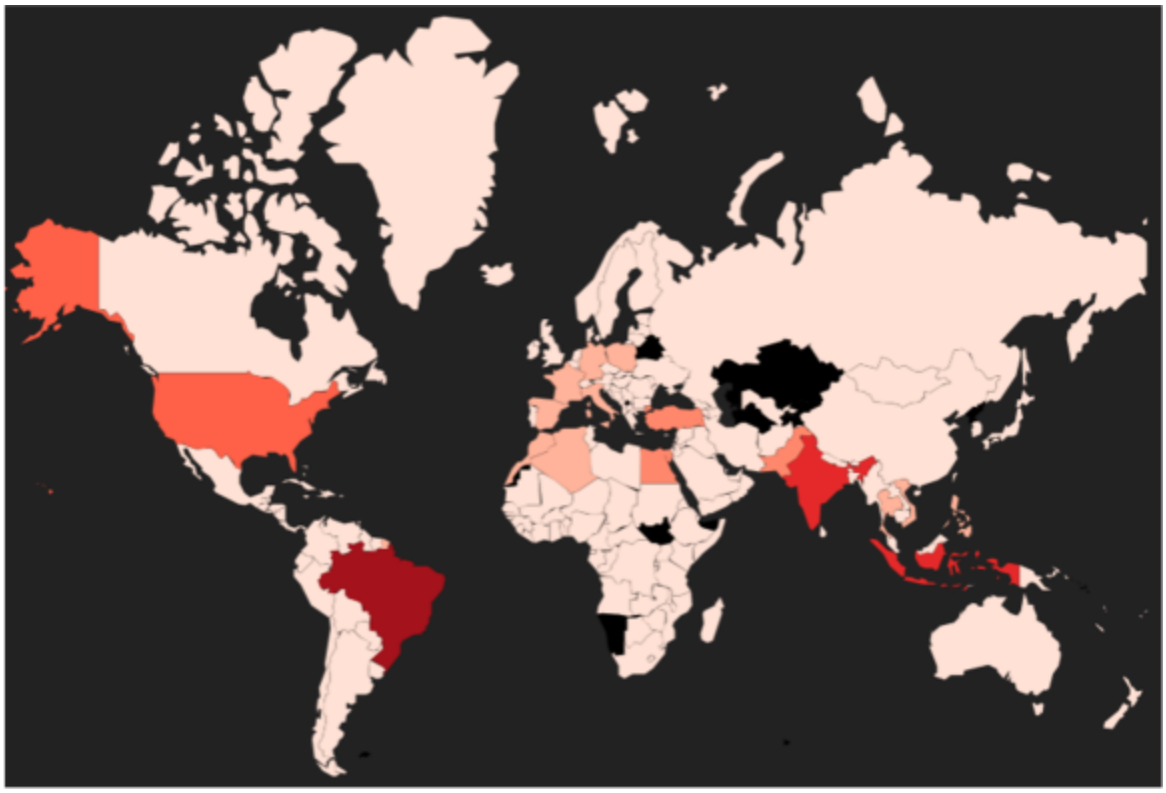


Figure 4 – Potential Raccoon Stealer Victims

Figure 4 provides an illustration of WHOIS information for the ~95,000 IP addresses beaconing to the Raccoon Stealer *gates*. This data indicated significant concentrations in Brazil, India, Indonesia, and the United States, as well as clusters in Southeast Asia, Northern Africa and Europe.

As has been covered by other commentators on this threat activity, we also note an absence of potential victims in Commonwealth of Independent States (CIS) countries – which remains consistent with the Raccoon Stealer advertising ('NO CIS EVER!').

Our assessment of the Raccoon Stealer operators is 'likely Russian-speaking, but not necessarily Russian-based'. A future blog will explore our understanding of the management of Raccoon Stealer.

In conclusion, based on Team Cymru's snapshot of global internet activity, Raccoon Stealer continues to 'create' thousands of new victims per week from countries around the world.
