Inside the V1 Raccoon Stealer's Den

By Team Cymru

Published: 2025-04-08 · Archived: 2026-04-05 21:02:29 UTC

Exposing links to Kharkiv (Ukraine) and the CC2BTC Marketplace

Introduction

Team Cymru's S2 Research Team has blogged previously on the initial Raccoon stealer command and control methodology (Raccoon Stealer - An Insight into Victim "Gates"), which utilized "gate" IP addresses to proxy victim traffic / data to static threat actor-controlled infrastructure.

Since the publication of our previous blog, the following timeline of events has occurred:

1. Raccoon Stealer version one (V1) ceased operations in late March 2022, citing the loss of a developer during the Russian invasion of Ukraine.

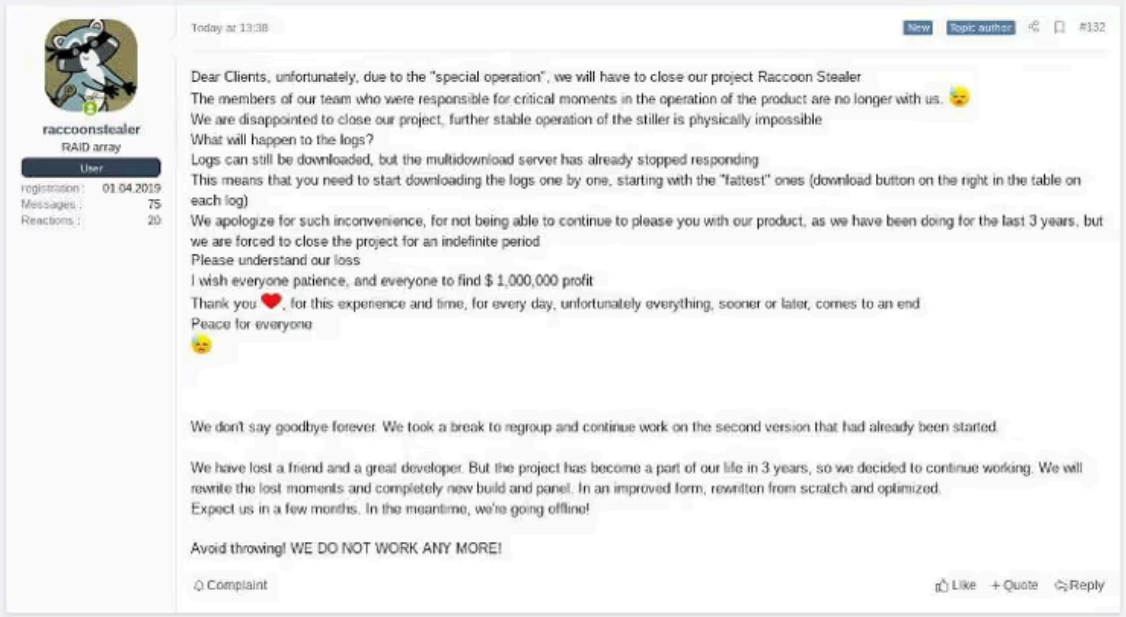

Figure 1 - Suspension of Raccoon Stealer V1

2. Raccoon Stealer re-emerged with version two (V2) in early June 2022.

3. The US Department of Justice unseals the indictment of Mark Sokolovsky, for crimes related to the operation of Raccoon Stealer (V1), on 25 October 2022.

Following the unsealed indictment, we wanted to share additional insights from our long-term tracking of Raccoon Stealer V1 operations, which were previously shared with law enforcement and industry partners.

While our previous blog post focused on victim-facing infrastructure, this post will highlight aspects of upstream infrastructure and management of Raccoon Server V1 and its associated services.

Note, from this point onwards we will refer to Raccoon Stealer V1 simply as Raccoon.

Key Findings

- Key elements of the Raccoon infrastructure identified, including the likely location of victim data storage, a Tor .onion control panel, and a Telegram update server. Providing a snapshot into threat actor TTPs with regards to 'internal' architecture.
- Pivoting from these key elements identified threat actor infrastructure located in Kharkiv, Ukraine, likely used to operate the service (MaaS).
- Attribution of the CC2BTC marketplace to the Raccoon operators, a business model which allowed the threat actors to profit twice from the theft of victim data.

Starting at the "Gate"

To paraphrase our previous blog:

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

The full decryption process has been covered verbosely by other vendors, and therefore it is unnecessary to repeat it here.

Though each "customer" had their own Telegram channel, our research found that the "gate" URL, once decrypted, was common across all samples at any particular time, indicating this detail was updated centrally.

The initial infection traffic, where Raccoon checked-in for the first time with the C2 server, therefore appeared as follows:

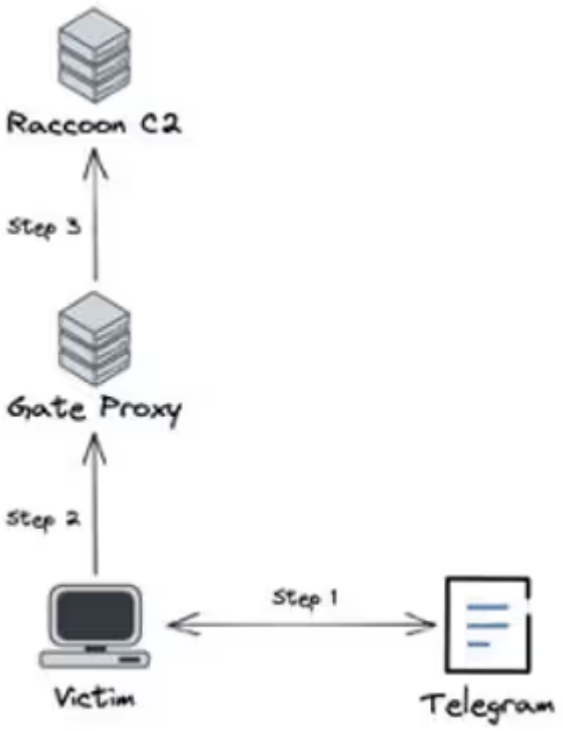

Figure 2: Initial Infection Traffic

By examining common upstream peers of the Raccoon “gate” IPs over time, we were able to identify two key hosts involved in these C2 communications (Step 3 in Figure 2).

Both IP addresses were assigned to an Italian VPS provider and, with a small number of exceptions, remained static up to the point the Raccoon infrastructure was dismantled.

Note, all threat actor-controlled IP addresses have been redacted from this blog post and are instead replaced with descriptive names. Researchers requiring sight of these IPs should contact outreach@cymru.com for further information.

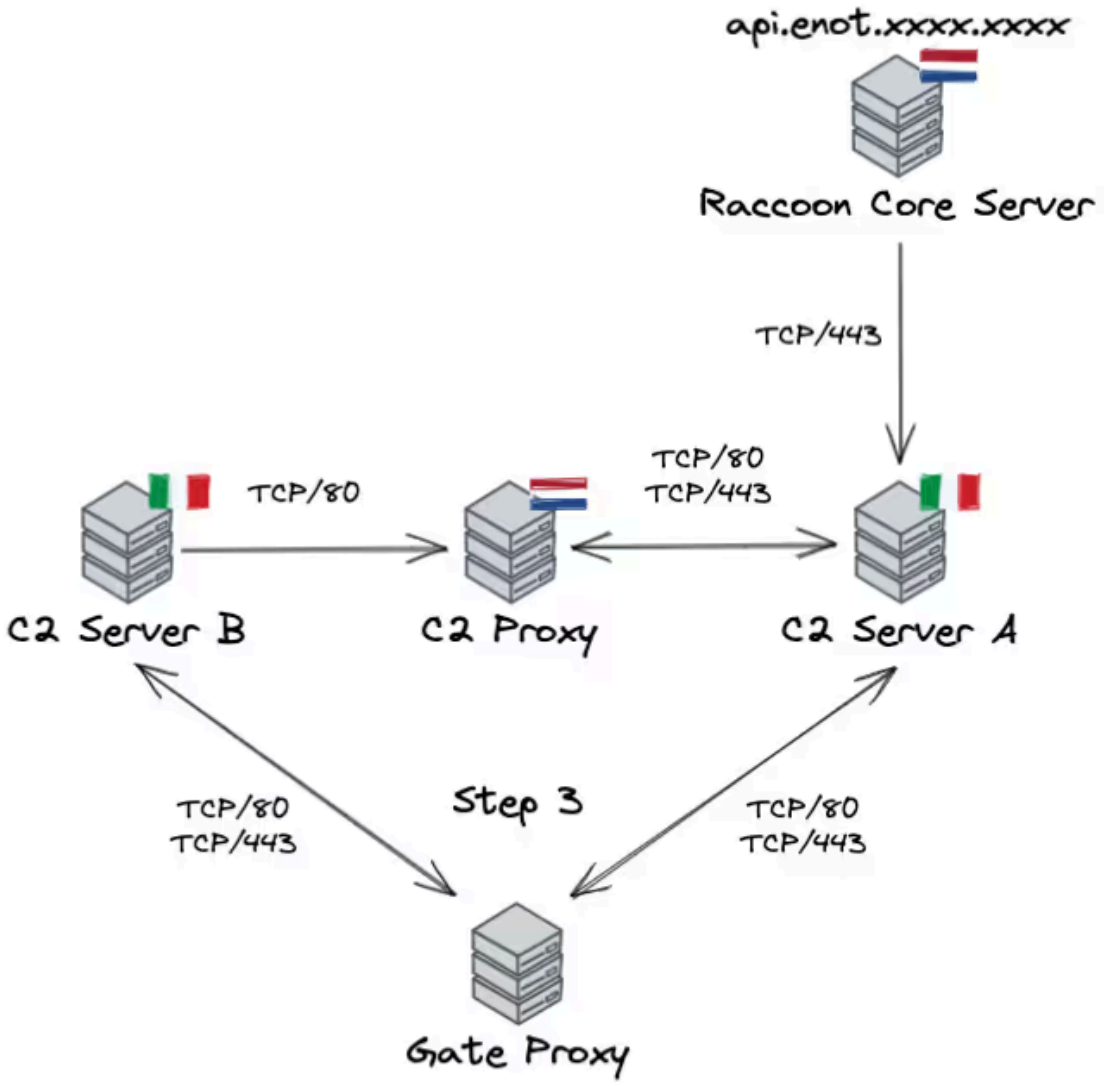

Figure 3: Raccoon C2 Infrastructure

The Italian IPs both communicated with an IP address assigned to a Dutch provider (**C2 Proxy**), which appeared to manage the proxying of data between the two, specifically from **C2 Server B** to **C2 Server A**.

It was noted throughout the threat actors' infrastructure that communications would alternate between hosts assigned to either the Dutch or Italian VPS provider (the same two providers were used in all cases). We assess this was likely a mechanism intended to cover / disguise activities, whereby one VPS provider would not have the complete picture without the other.

We also observed communications originating from a second IP address assigned to the Dutch provider (**Raccoon Core Server**), connecting to **C2 Server A** on TCP/443. It is our assessment that this IP hosted the core Raccoon server, where much of the victim data was likely stored.

Passive DNS data for **Raccoon Core Server** showed it hosting a domain containing the string "enot". "Enot" is the romanized version of the Russian / Ukrainian word for Raccoon ("енот / єнот").

Tor Control Panel

One of the “selling points” of Raccoon was the provision of a control panel for its customers, accessible over the Tor network as a .onion site. The control panel was most recently hosted at:

dq7shlx5o67t64ljuzisyp34s3n7vepnhc5ijt5hjh433qzaatyj5bid[.]onion

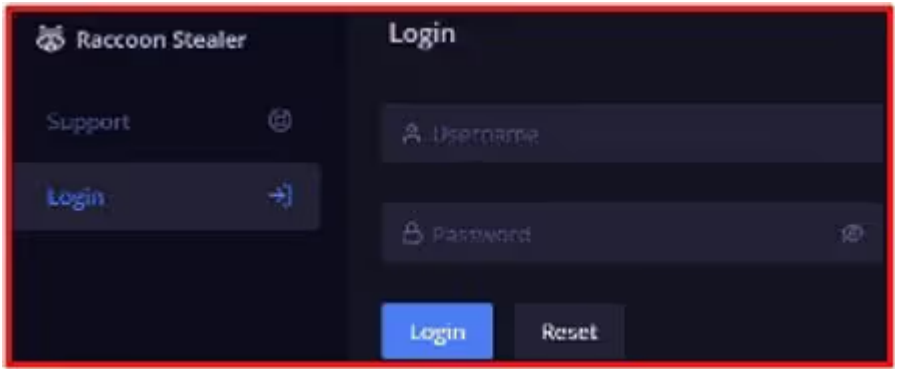

Figure 4: Login Page for the Raccoon Control Panel

When assessing inbound connections to the **Raccoon Core Server**, we observed a high volume of communications originating from **Possible Tor Host** (assigned to the Italian VPS provider), an IP which in turn exchanged a large number of communications with known Tor relays; based on available Consensus data at the time of analysis.

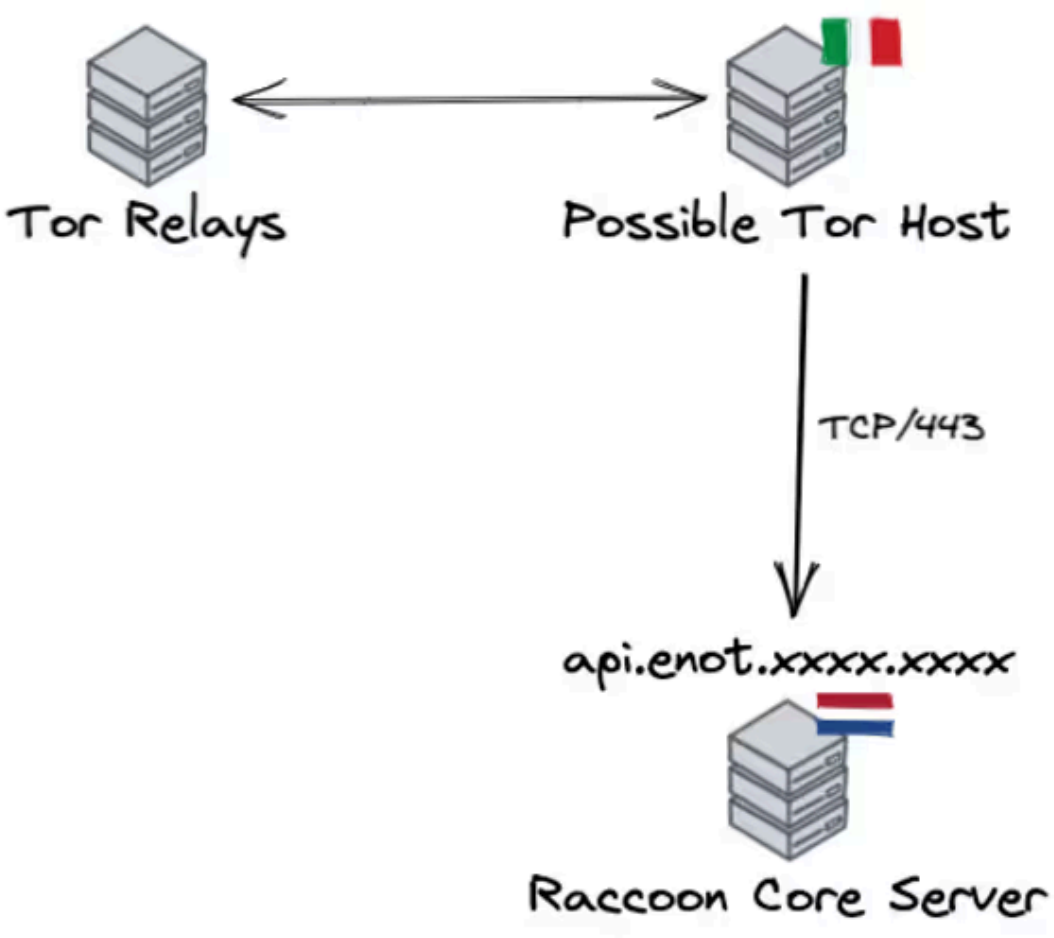

Figure 5: Communications with Raccoon Core Server

Our hypothesis is that **Possible Tor Host** hosted the back-end infrastructure for the Tor .onion site, which Raccoon "customers" used to access / manage stolen data stored on the **Raccoon Core Server**, and to provide further updates to victim machines back through the infrastructure described in Figure 3.

Telegram Updates

Another element of Raccoon's core functionality, as already described above, was the use of Telegram channels - which we believe were updated centrally.

Whilst building out infrastructure communicating with key elements of the threat actors' operation, and also hosted on IPs assigned to the Dutch and Italian VPS providers, we identified a candidate for the Telegram update server.

Telegram Update Server was observed in regular communications with IPs overtly assigned to Telegram, generally coinciding with when "gate" IPs were updated in the Raccoon campaigns we were tracking. In addition, **Telegram Update Server** received regular inbound connections from a number of Cloudflare IPs, potentially indicating a clearweb service hosted on this IP behind Cloudflare's infrastructure.

Passive DNS data for **Telegram Update Server** showed it hosting a domain containing the string “raccoon-core” as of late 2019.

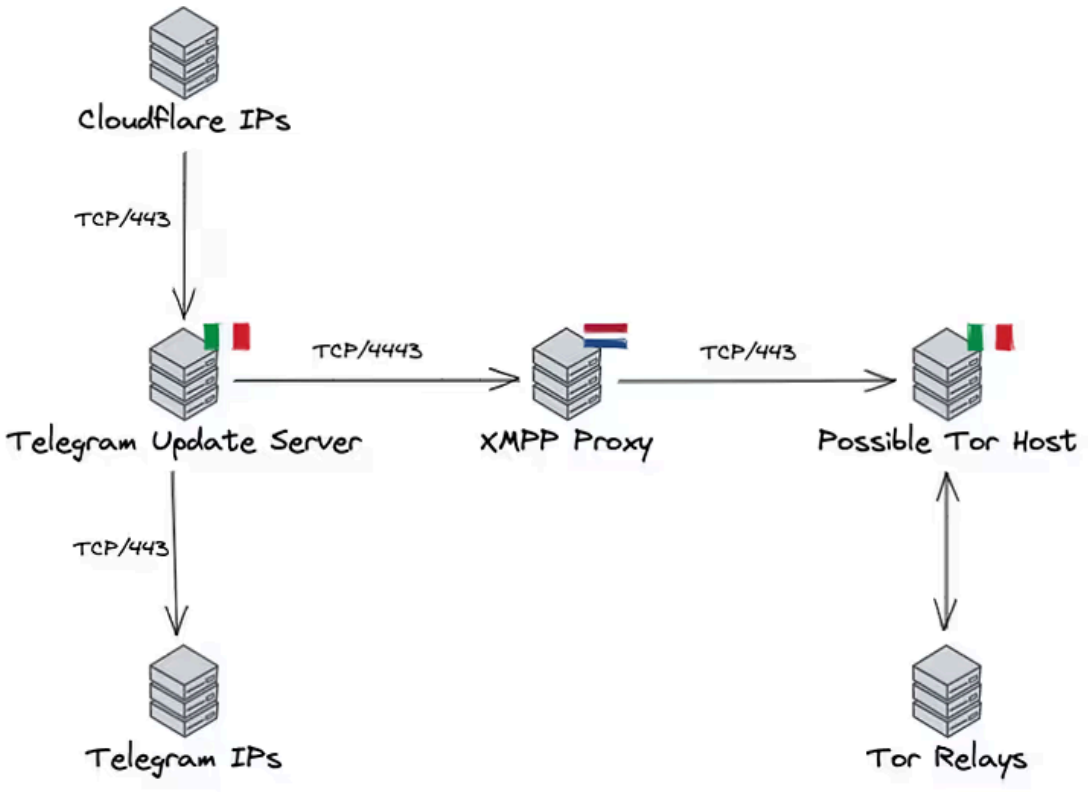

Figure 6: Infrastructure Overview

Telegram Update Server also communicated with **Possible Tor Host**, believed to host the Tor .onion site referenced above, via an intermediary (**XMPP Proxy**). Open ports information, particularly relating to the use of TCP/4443 in these communications, indicated the use of a XMPP file transfer protocol. It is possible these communications were indicative of a “closing of the loop” between the Telegram channel updates and the information presented to the Raccoon “customers” in the .onion control panel.

Management Leads to Kharkiv, Ukraine

With several key elements of infrastructure identified, we began to look for IPs outside of the network which might be used for management purposes, i.e., connecting into the Dutch and Italian hosts.

Fortunately, like many aspects of the Raccoon infrastructure, the external management IPs remained consistently static. From 2021 onwards, we observed the same two IP addresses connecting to several key hosts, including the Tor .onion site and Telegram update servers, on TCP/22 (SSH).

WHOIS information for both IPs pointed to a Ukrainian ISP called TRIOLAN (AS13188), and in particular to the company’s Kharkiv infrastructure.

```
% Information related to '          .0/24AS13188'

route:                  .0/24
descr:          Triolan, Kharkiv
origin:         AS13188
mnt-by:         TRIOLANMNT
mnt-by:         SALTOVKAMNT
created:        2016-10-19T13:01:13Z
last-modified:  2019-07-22T15:15:26Z
source:         RIPE
```

```
% Information related to '          .0/24AS13188'

route:                  .0/24
descr:          Triolan, Kharkiv
origin:         AS13188
mnt-by:         TRIOLANMNT
mnt-by:         SALTOVKAMNT
created:        2016-10-19T13:00:55Z
last-modified:  2019-07-22T15:15:06Z
source:         RIPE
```

Figure 7: Management IP WHOIS Information

Based on the available information, TRIOLAN appears to be a provider of home / small office broadband services - indicating to us that these may in fact be the ultimate source of the threat actors' Internet access.

Where Else Does the Management Lead Us?

Having identified the threat actors' management IPs, we decided to look in more detail at the other IP addresses they were accessing via SSH (TCP/22).

One such IP quickly became very intriguing to us.

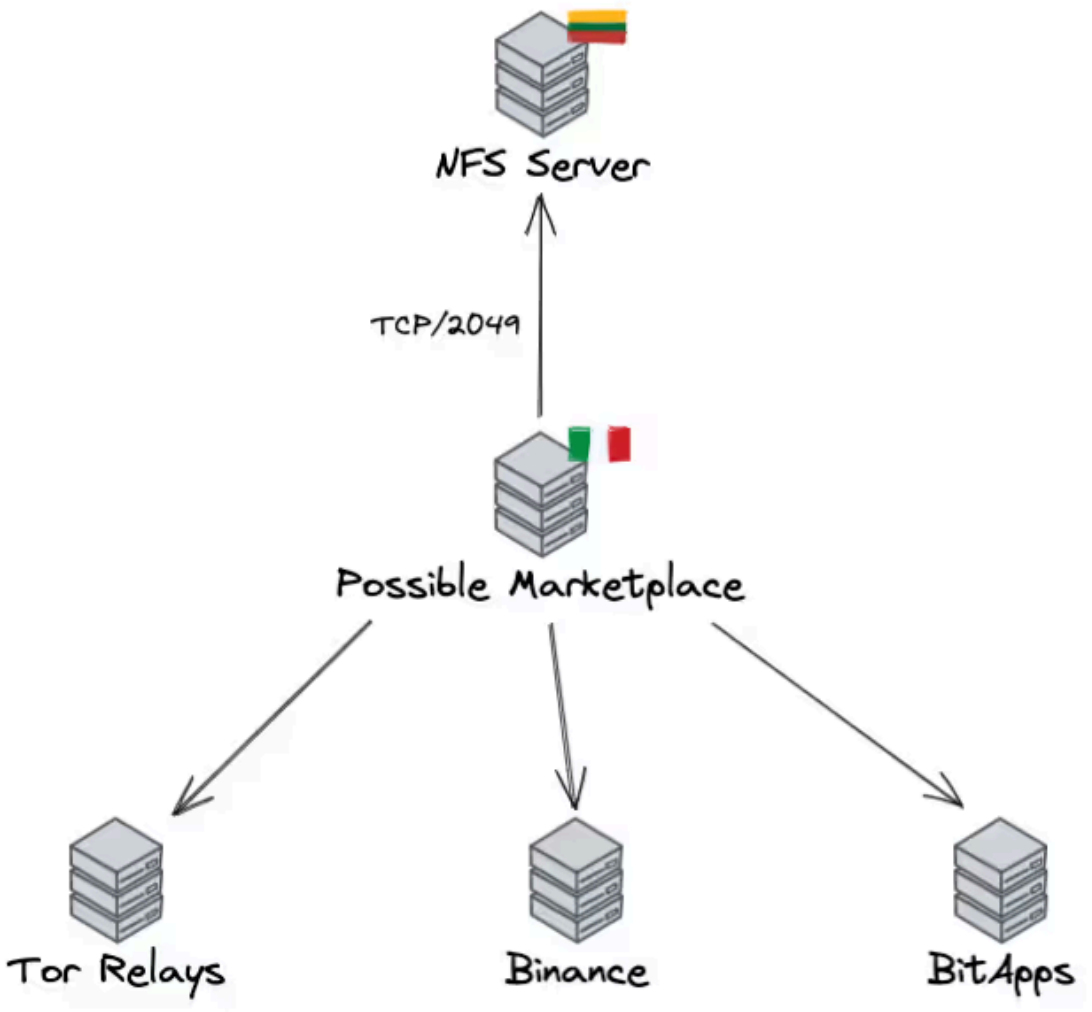

Figure 8: Is this a Marketplace?

Possible Marketplace, assigned to the same Italian VPS as referenced previously, received inbound management connections from both Ukrainian IPs. Additionally, it made outbound connections to two cryptocurrency platforms and a number of Tor relays.

Our initial thoughts were that this IP address was connected to the operation of a marketplace or payment service.

In October 2021 we hit gold.

We began to observe outbound connections from **Possible Marketplace** to an IP assigned to a Lithuanian VPS provider (**NFS Server**) on TCP/2049. Port 2049 is commonly associated with Network File System (NFS), a file system protocol from the prehistoric age of the Internet.

NFS is generally deployed within networks and is used to mount exported shares on remote servers - enabling users to access data as if it were stored locally, but without the hard disk constraints.

Using NFS across the Internet is NOT advisable in 2022 (or in this case also 2021).

But in this case, this is exactly what the threat actors were doing. Internet scan data for **NFS Server** listed its exported shares, and from which IP addresses in particular they were accessible from.

Note, we did not seek to access any of the data stored on NFS Server and therefore cannot comment on its contents.

```
Export list for  NFS Server
/var/nfs/rst   Raccoon Core Server
/var/nfs/cbtc  Possible Marketplace
```

Figure 9: Shares Mounted on NFS Server

A few things in Figure 9 stood out to us:

1. The first share, entitled “rst” mapped to **Raccoon Core Server** - the IP identified above (Figure 3) as the likely Raccoon core server.
2. The likelihood that “rst” = Raccoon stealer.
3. The second share, entitled “cbtc” mapped to **Possible Marketplace** (Figure 8).

Based on our initial assessments of **Possible Marketplace**, we began to look at candidate underground economy marketplaces for potential matches with the string “cbtc”.

CC2BTC Marketplace

Our search led us to CC2BTC, a marketplace intended specifically for trade of stolen credit card information; handily one of the key targets of Raccoon.

Figure 10: Advertisement for CC2BTC

Reviewing the advertisements for CC2BTC, it appeared that the business model was to charge “customers” to access the marketplace, limiting the number of credit card details they could purchase per day based on their membership tier; Aluminum, Bronze, Silver, Gold, or Platinum.

A post from May 2020 identified the cost of each tier - although it is not clear if this was a one-off payment or a subscription.

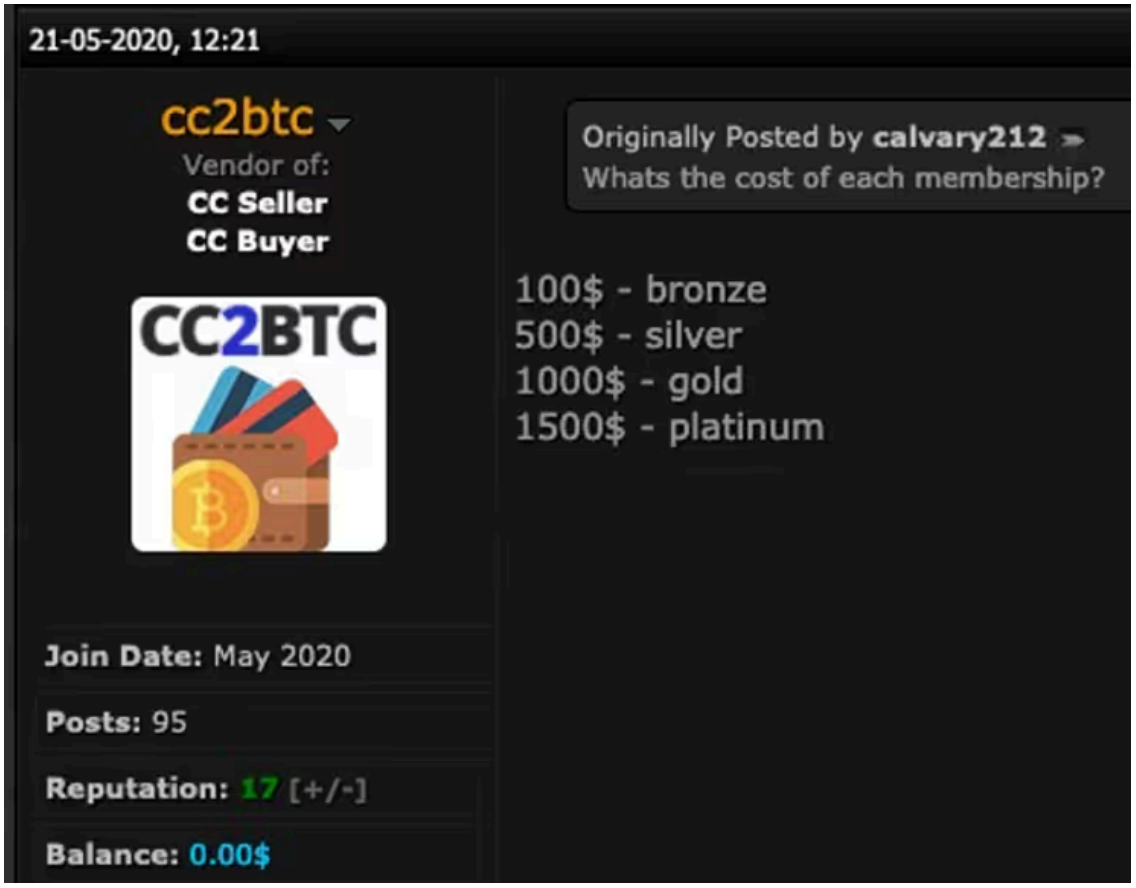

Figure 11: CC2BTC Membership Tiers

We were also able to identify a Telegram channel utilized by the operators of CC2BTC to update “customers” on a daily basis, and often several times per day, on the latest “merchandise” available for purchase.

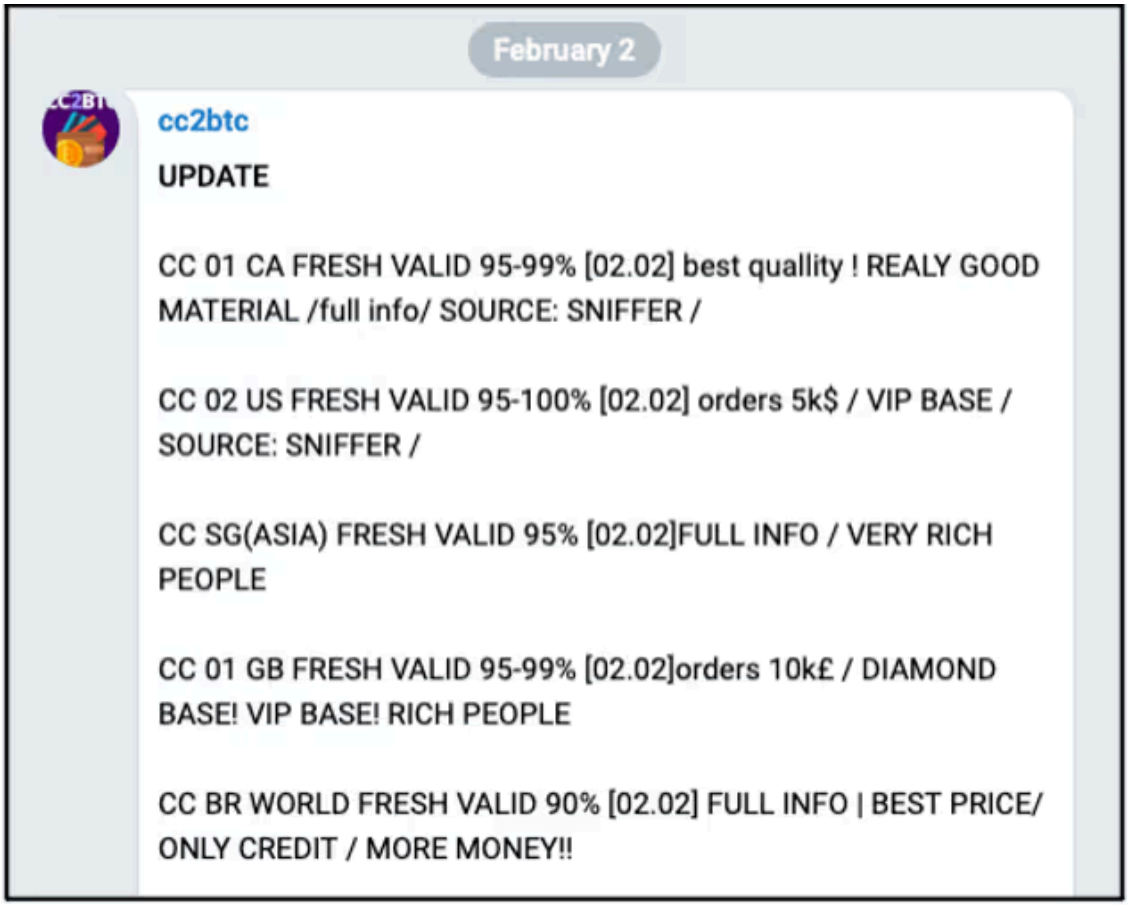

Figure 12: Example of the CC2BTC Telegram Updates

In Figure 12, credit cards from Canada, the United States, Singapore, the United Kingdom, and Brazil (in order of appearance) were offered for sale on 2 February 2022.

At this stage, the idea that “cbtc” = CC2BTC seemed plausible, however the following series of events in March 2022 helped us to solidify this assessment.

Firstly, on 20 March 2022, the “last” update was made to the CC2BTC Telegram channel.

Figure 13: Final Update in the CC2BTC Telegram Channel

Secondly, around 25 March 2022, users of CC2BTC begin to realize something had “gone wrong”, discussing this fact in other underground forums.

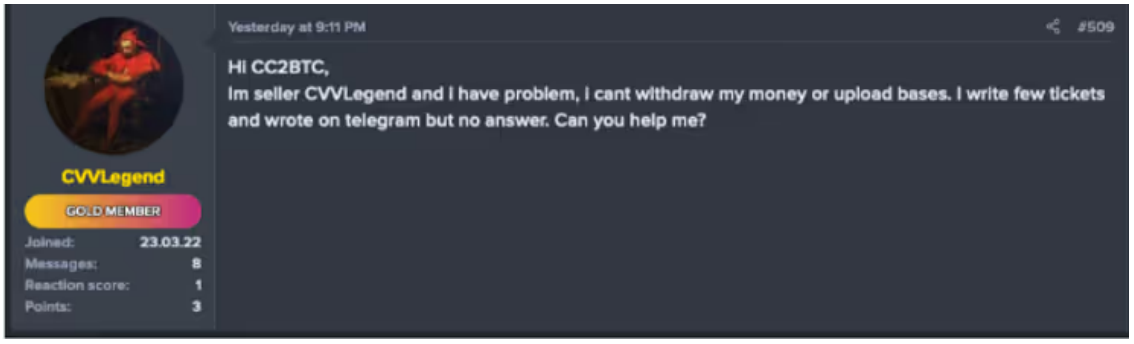

Figure 14: Concern is Raised About the Fate of CC2BTC

It was around this time that CC2BTC disappeared completely, with no response to any of their concerned customers.

By the end of March 2022, the user “cc2btc” was banned from one carding forum, and the CC2BTC logo removed as a ‘sponsor’ from another.

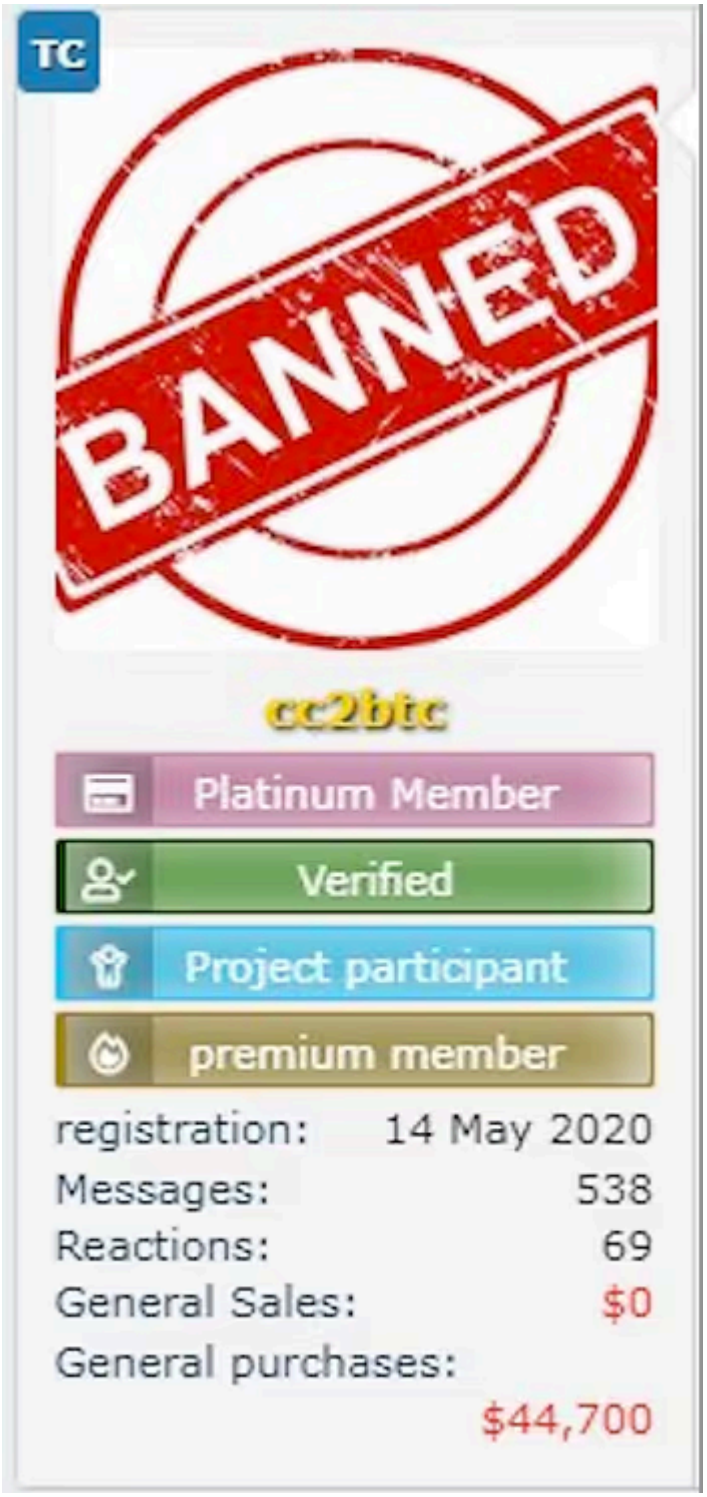

Figure 15: User 'cc2btc' Banned from Carding Forum

Without wanting to state the obvious, the disappearance of CC2BTC coincided completely with the cessation of Raccoon operations.

Conclusion

Based on our assessment that the operators of Raccoon and CC2BTC are one and the same, it appears that they had established a savvy business model prior to the disappearance of both services. By firstly charging "customers" of Raccoon for access to their malware, which was subsequently used by those customers to steal victim data, and secondly charging "customers" of CC2BTC access to their marketplace to, in theory, purchase credit card information stolen via Raccoon deployments, they were in effect able to profit twice from the same data theft.

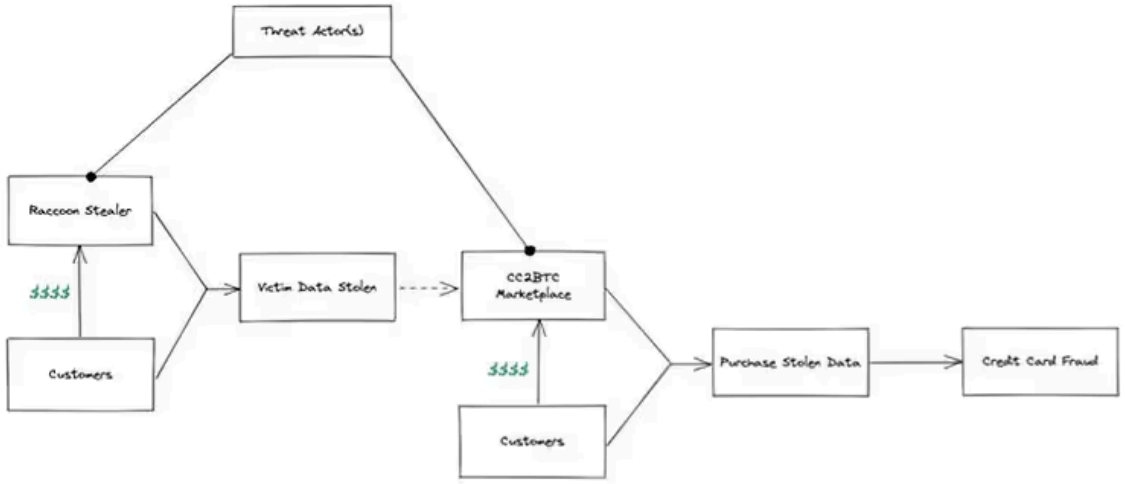

Figure 16: Hypothetical Business Model

We hope that in sharing these findings that we have provided another snapshot into the 'business world' of cyber-crime, providing additional considerations to investigators when assessing the extent and impacts of data theft over the Internet.

The news of an arrest in the case of Raccoon demonstrates that offenders can and will face justice.
