Tracing the Path From SmartApeSG to NetSupport RAT

By Team Cymru

Published: 2025-04-08 · Archived: 2026-04-05 19:11:03 UTC

This investigation began with the analysis of SmartApeSG, a FakeUpdate threat that delivers NetSupport RAT to victims. Initial efforts to track its Command and Control (C2) infrastructure led to unexpected discoveries through analysis of Internet telemetry data.

By pivoting from one connection to the next, we uncovered related C2 management hosts, active NetSupport RAT servers, and cross-connections to suspicious infrastructure, including RATs, cryptocurrency services, and platforms linked to illicit activity.

This write-up details these findings and demonstrates how exploring Internet telemetry data can uncover interconnected threats.

Key Findings

- **Management Hosts:** Identified three Moldovan IPs (assigned to MivoCloud) likely used for C2 management—two tied to SmartApeSG and one to the NetSupport RAT cluster

- **Active NetSupport RAT Cluster:** Found an active NetSupport RAT cluster, including several old C2s reported nearly a year ago, which were still receiving victim communication.

- **Link Between Infrastructures:** Observations suggest a connection between the SmartApeSG and NetSupport RAT clusters, including shared characteristics in management activity and overlapping components such as X.509 certificates.

- **Recent Infrastructure Updates:** The old NetSupport RAT infrastructure was recently replaced with new IPs and domains, with some of the same domains now pointing to these new IPs.

- **Quasar RAT Connection:** Observed communication between a NetSupport RAT C2 and a Quasar RAT C2, along with several unusual hosts. It is unclear if this activity is directly related to the threat actor's infrastructure or represents unrelated compromise.

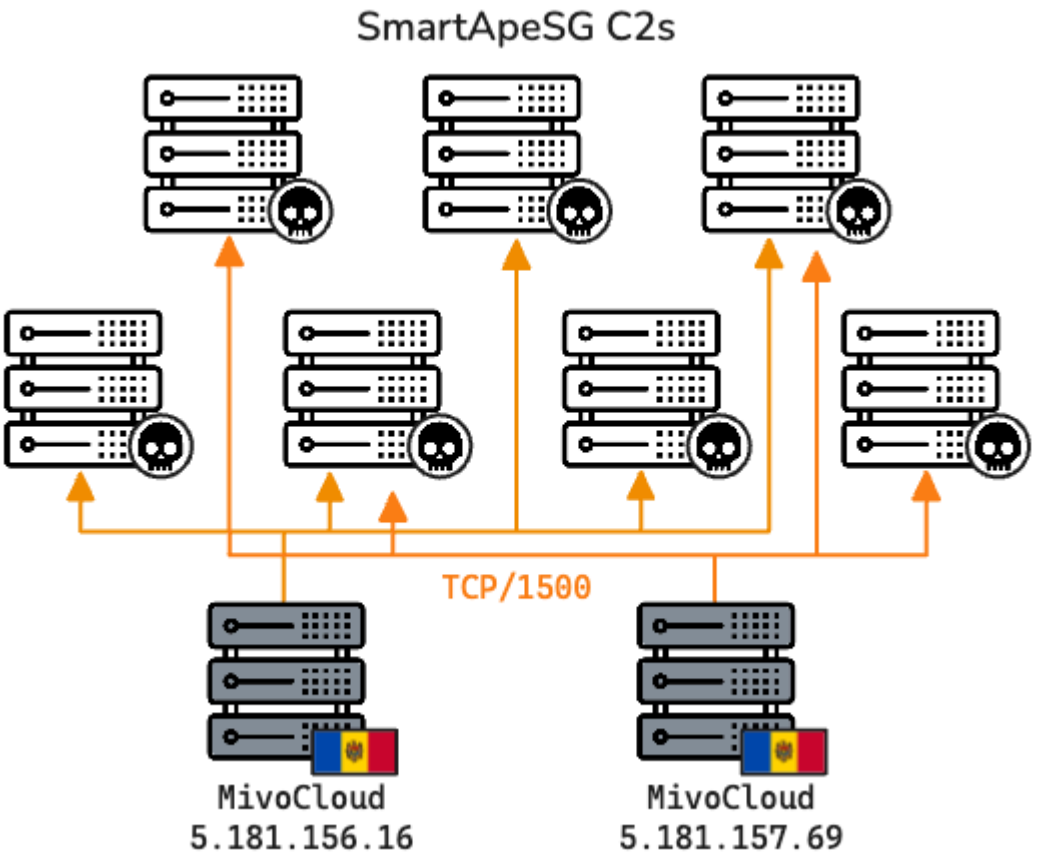
Tracking SmartApeSG Infrastructure

A brief background: SmartApeSG is a type of FakeUpdate threat first observed in the wild in June 2023. Like other FakeUpdate threats like SocGholish, LandUpdate808, and ClearFake, SmartApeSG deceives users into installing a fake browser update after visiting a compromised website. In most cases, this results in the deployment of NetSupport RAT on the victim's machine.

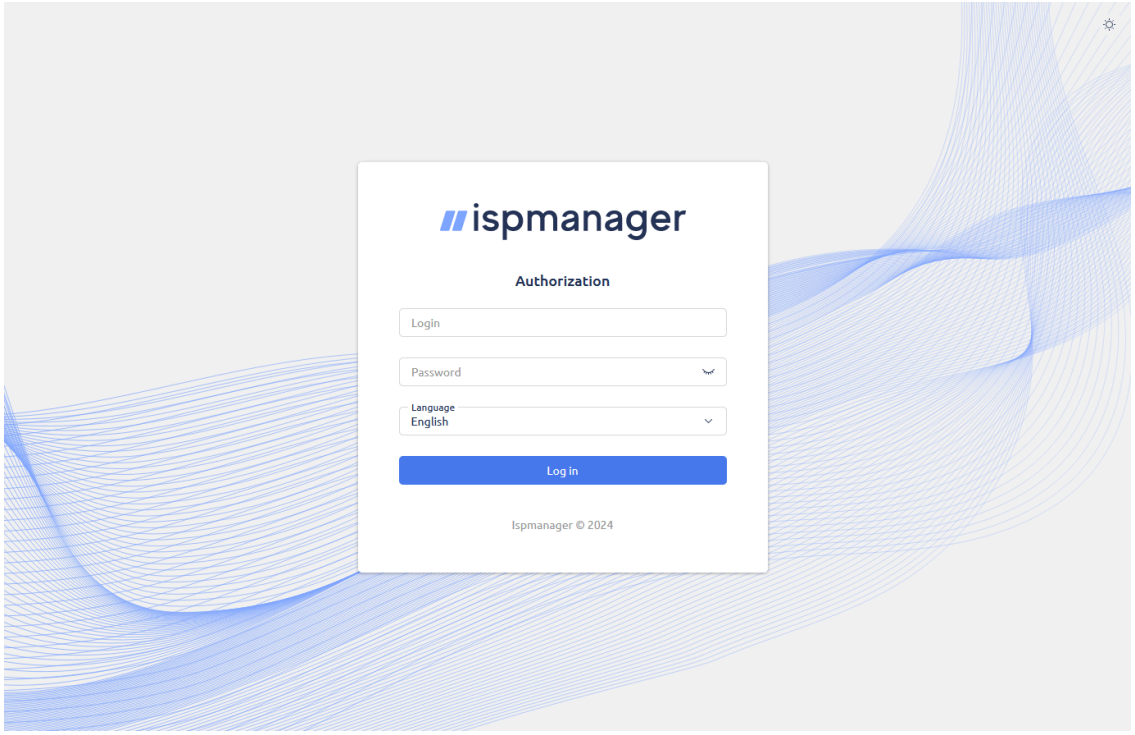
NetSupport RAT refers to the malicious use of NetSupport Manager, a legitimate remote administration tool. When abused, it can be used to control systems, steal data, or install malware. It is often delivered through phishing or fake update campaigns such as SmartApeSG or SocGholish.

Our analysis began by examining the Internet telemetry data of SmartApeSG C2 servers and searching for outlier IPs that communicated with multiple C2s. Such activity can indicate related backend infrastructure or threat actor operations. At the time, the C2 infrastructure was hosted on Stark Industries, however this is no longer the case following takedown action by the hosting provider.

While there was no significant outbound activity originating from the SmartApeSG C2s, two hosts were consistently observed connecting to them over TCP/**1500**. This behavior persisted for periods ranging from a few days to a week.



Visiting one of the C2s on port 1500 in a browser revealed an ISPManager login page.



ISPManager is a widely used control panel software, particularly popular among Russian-speaking users. According to their website, it is "a Linux-based control panel for managing dedicated, game, and VPS web servers, as well as selling shared hosting." Conveniently for the threat actors, the platform offers a two-week free trial per server—longer than the typical lifespan of these C2s.

The service includes an API that enables site management without requiring manual login to the panel. The default port for API authentication calls is the same as the one used by these C2s: port 1500. We suspect these two hosts were used to manage the C2s, connecting through the API to perform automated tasks, monitor activity, pull statistics, etc..

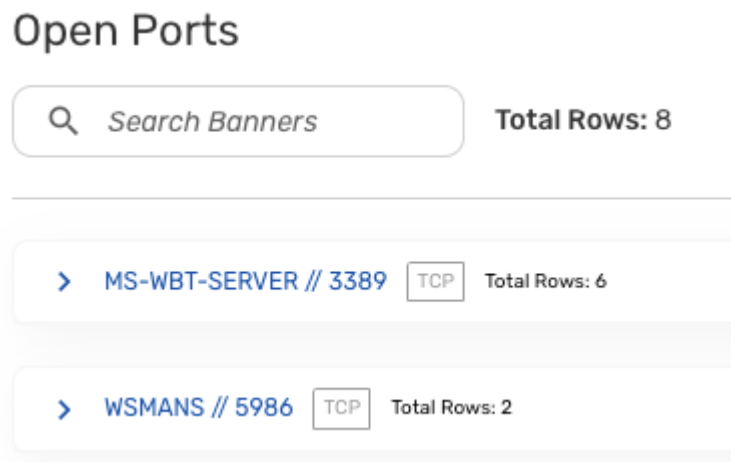
First Pivot: Exploring Moldovan C2 Management Hosts

The next step was to pivot to the two IPs identified as potentially being used for C2 management. Both IPs were geolocated in Moldova and hosted by MivoCloud, but their profiles differed in terms of observed open ports and hosted X.509 certificates.

5.181.156.16

The server hosted on **5.181.156.16** had a service listening on TCP/**3389** (the common port for RDP traffic) at the time of the observed outbound connections to the SmartApeSG C2 servers (via TCP/**1500**). Immediately

following this time period, we also identified a service listening on TCP/**5986**, however it is unclear whether the IP was still associated with the threat actors at this point.

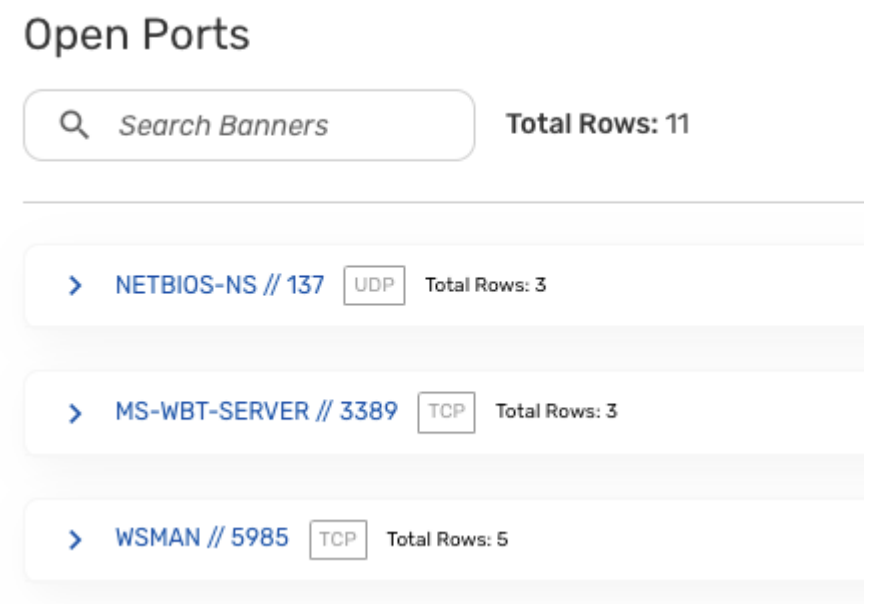


The X.509 certificate hosted on TCP/**3389** had both its subject and issuer set to **CN=55554rac**.

```
Issuer: CN=55554rac
Validity
    Not Before: Sep  3 22:20:00 2024 GMT
    Not After : Mar  5 22:20:00 2025 GMT
Subject: CN=55554rac
```

5.181.157.69

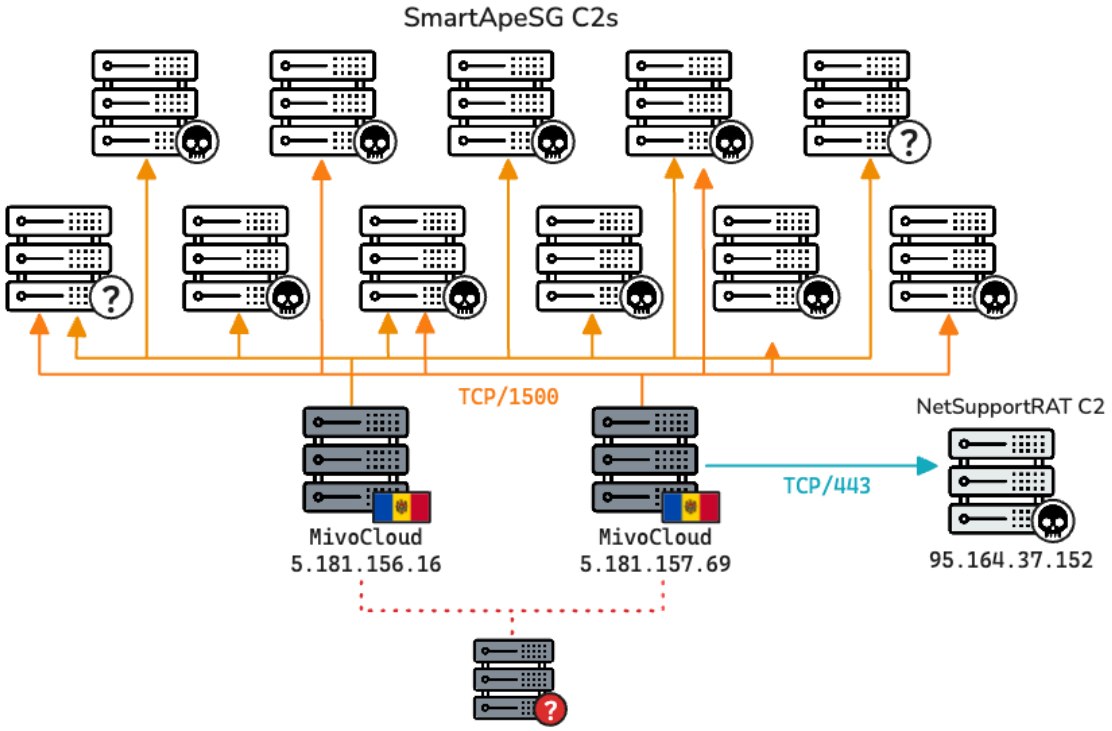
The server hosted on **5.181.157.69** had services listening on TCP/**137**, TCP/**3389**, and TCP/**5985** at the time of the observed outbound connections to the SmartApeSG C2 servers



The X.509 certificate hosted on TCP/3389 listed both its subject and issuer as **CN=MATRACHEDICIDGA**.

```
Issuer: CN=MATRACHEDICIDGA
Validity
    Not Before: Jul 12 10:19:03 2024 GMT
    Not After : Jan 11 10:19:03 2025 GMT
Subject: CN=MATRACHEDICIDGA
```

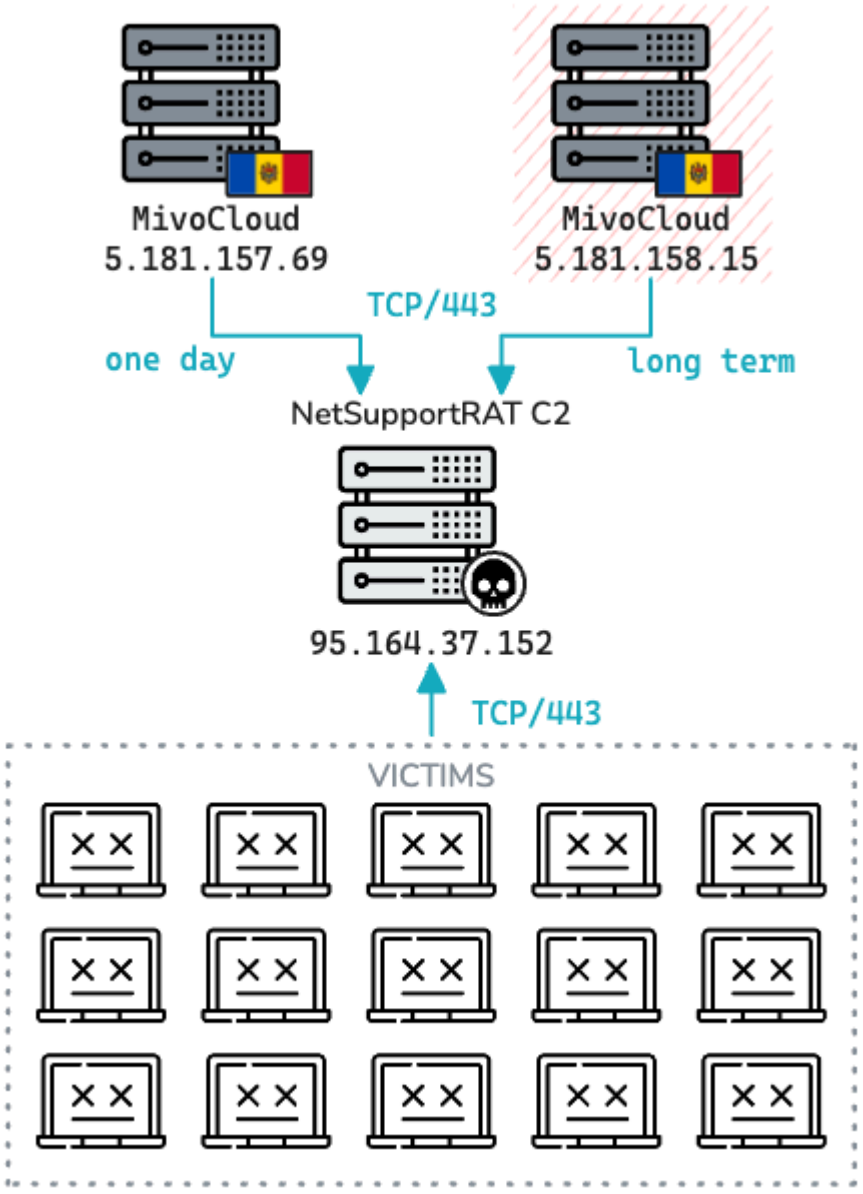
Internet telemetry analysis of these two hosts revealed additional C2s they were communicating with. Most of the observed Internet telemetry data was related to TCP/**1500** activity associated with C2 management, with **5.181.156.16** interacting with SmartApeSG C2s more frequently than **5.181.157.69**. It is possible that the threat actor operates from a single upstream host and uses these two Moldovan IPs as proxies to route their activity to the C2s. However, this potential upstream host was not identified in the data available for analysis.



Interestingly, for one day, **5.181.157.69** established a connection to **95.164.37.152**:443, which was reported as a NetSupport RAT C2 in 2023. Time to pivot again!

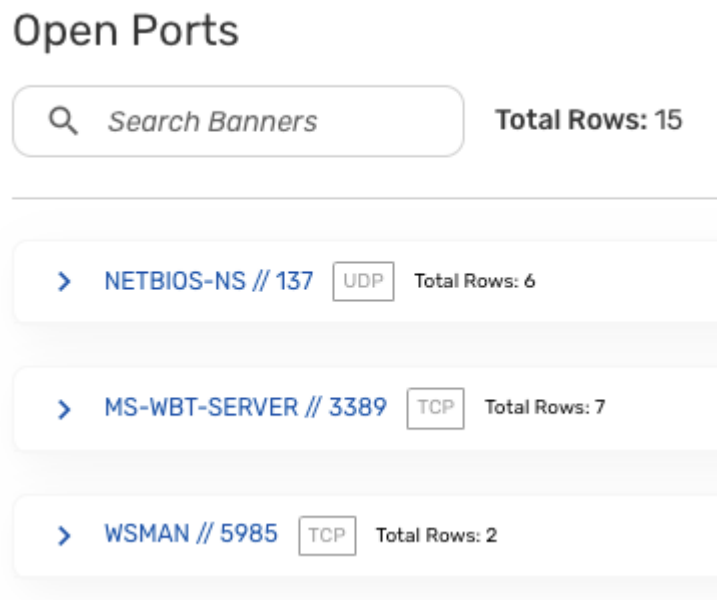
Second Pivot: Uncovering NetSupport RAT Connections

Analysis of Internet telemetry data for this NetSupport RAT C2 server revealed that the infrastructure was still active and receiving victim communications. The most notable finding was a third IP **5.181.158.15**, also hosted on MivoCloud, which had been connecting to the same C2 on remote TCP/**443** for several months.



5.181.158.15

The server hosted on **5.181.158.15** had services listening on TCP/**137**, TCP/**3389**, and TCP/**5985**, in an identical pattern to **5.181.157.69**.

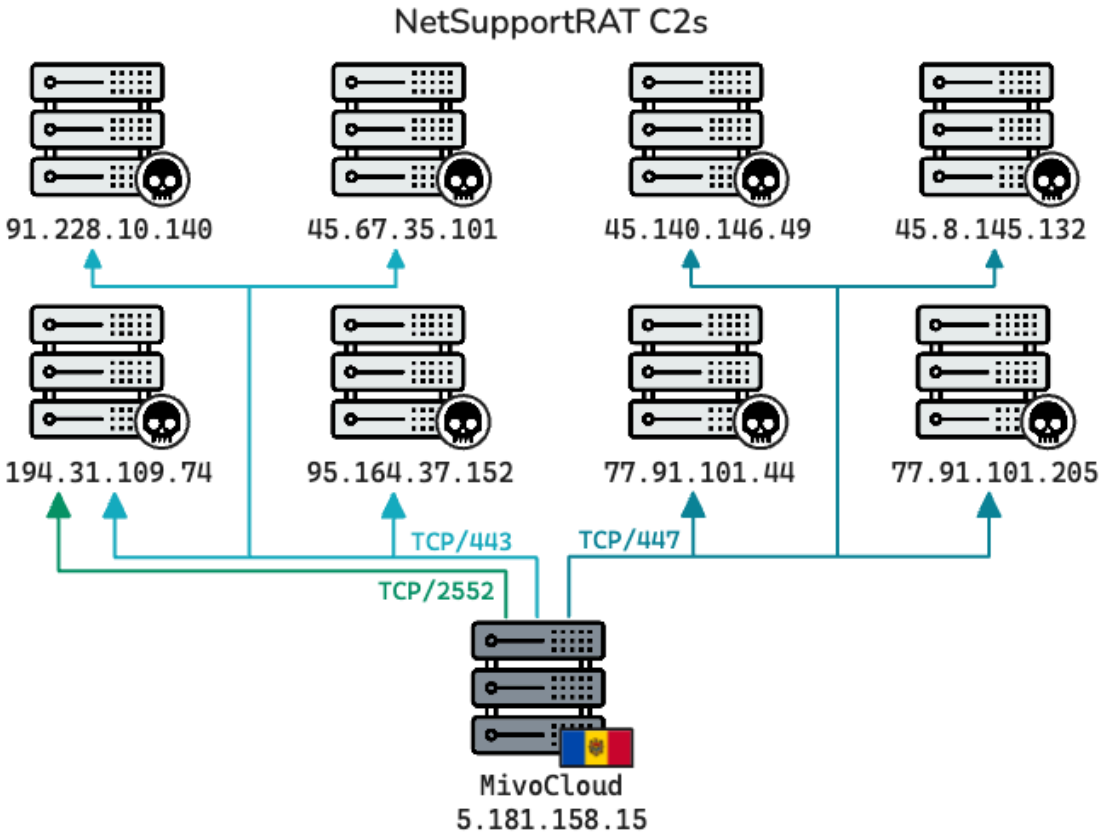


The X.509 certificate for this host had both its subject and issuer set to **CN=WIN-7FUHAU7D2HV**. Initially, the certificate was hosted on TCP/**6778**, but this was later updated to TCP/**3389**.

```
Issuer: CN=WIN-7FUHAU7D2HV
Validity
    Not Before: Aug 12 11:25:52 2024 GMT
    Not After : Feb 11 11:25:52 2025 GMT
Subject: CN=WIN-7FUHAU7D2HV
```

Analysis of Internet telemetry data for **5.181.158.15** uncovered seven additional NetSupport RAT C2s that it was communicating with on remote TCP/**443** or TCP/**447**. For one of these C2s, there was also a period of connections on remote TCP/**2552** lasting about a month. This activity was consistent and had been ongoing for several months, suggesting another form of backend management activity.

The only other long-term activity from this IP occurred from at least April 2024 until recently and consisted of outbound connections to **derelay.rabby[.]io**, a public relay for Rabby Wallet.



Third Pivot: Cross-Connections with Quasar RAT and More

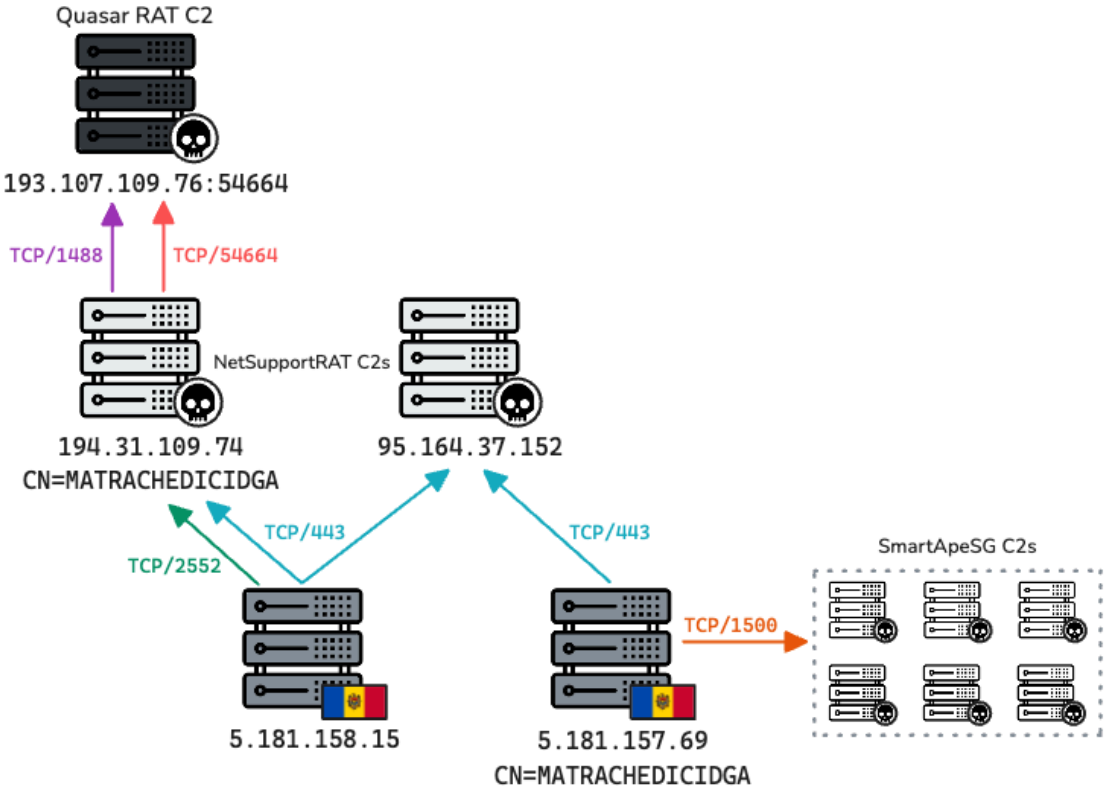
Interestingly, all but one of the eight NetSupport RAT C2 IPs had been publicly reported around a year earlier. Most of these IPs had domains pointing to them that were known NetSupport RAT C2s that were also up to a year old.

Analyzing Internet telemetry data for these C2s confirmed that they were still actively receiving victim communication—an unexpected finding given the age of the infrastructure. On a few occasions, four of these C2s established connections to **fex[.]net**, a Russian-language cloud storage and file-sharing service.

One notable C2, **194.31.109.74**, was receiving connections on local TCP/**2552** and had multiple NetSupport RAT domains pointing to it, yet it had never been publicly reported as malicious. Additionally, the X.509 certificate this IP initially hosted used the common name **CN=MATRACHEDICIDGA**, matching the Moldovan SmartApeSG management host **5.181.157.69** that had also connected to a NetSupport RAT C2 in this cluster. In October 2024, a new X.509 certificate was observed, with the common name **CN=WIN-J9D866ESIJ2**.

This C2 also frequently communicated with **193.107.109.76**, which was reported to ThreatFox as a Lycantrox C2 in 2023 and later as a Quasar RAT C2 in August 2024, a few weeks after we observed its communication with the NetSupport RAT C2. This activity occurred primarily to remote **TCP/1488** but occasionally remote TCP/**54664**.

The latter port was associated with Quasar RAT C2 communication, but there was no public information about activity on **193.107.109.76**:1488.



Quick SidePivot

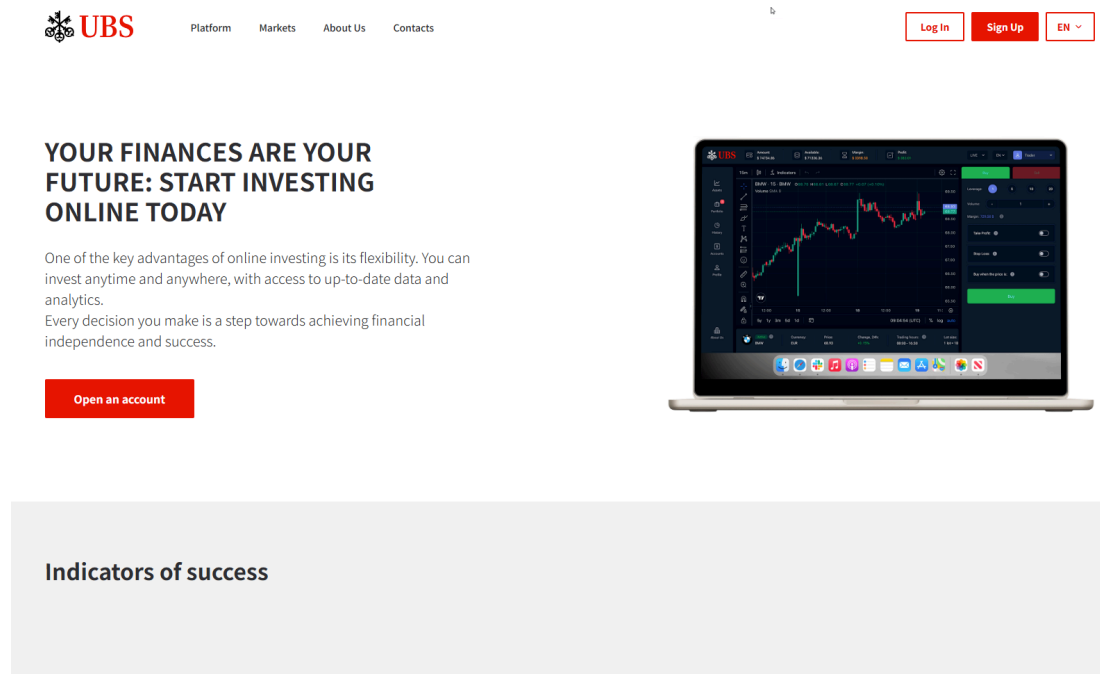
Pivoting to the Quasar RAT C2 hosted on **193.107.109.76**, Internet telemetry analysis revealed approximately 15 hosts communicating with it on TCP/**1488**, TCP/**54664**, or both. Activity on TCP/**54664** could potentially indicate victim communication with the Quasar RAT C2, but the purpose of the service listening on TCP/**1488** remains unclear.

Many of these hosts shared the X.509 certificate **CN=DESKTOP-TCRDU4C**, often linked to malicious infrastructure, and displayed Internet telemetry activity atypical of normal victim machines. Some were used for Tox, Telegram, or Jabber server communication, with Jabber activity connecting to **exploit[.]im**. Others appeared to be part of an unidentified proxy network. One host was identified as another known QuasarRAT C2, while others interacted with services related to cryptocurrency, including Rabby Wallet. A few led to Russian-language marketplaces such as DarkSeller and DarkMarket, as well as Russian-language forums for bitcoin and cryptocurrency.

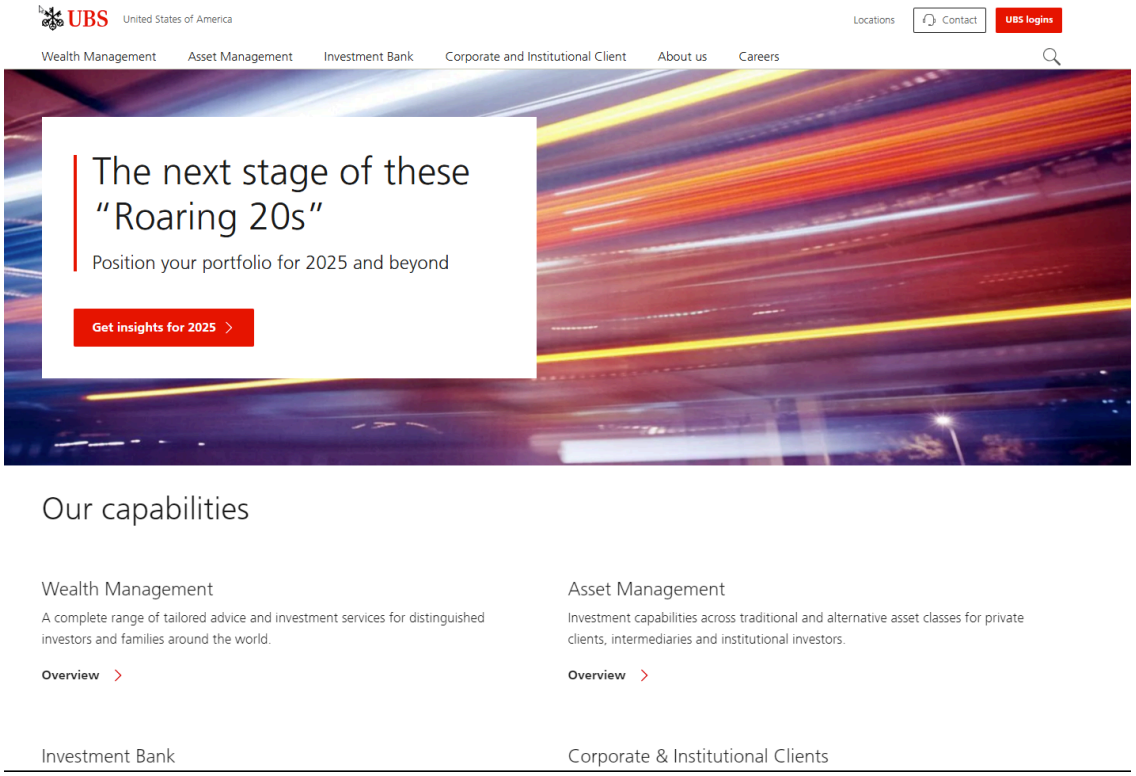
One of these hosts, which communicated with the Quasar RAT C2 on TCP/**54663**, appeared to SSH (connections to remote TCP/**22**) into sites used for cryptocurrency scams and visited numerous others on TCP/**443**. Among the

sites it connected to over SSH was **ubsglobalmarkets[.]com**, which appeared to impersonate **ubs[.]com**, the legitimate website of a major investment bank and financial services company.

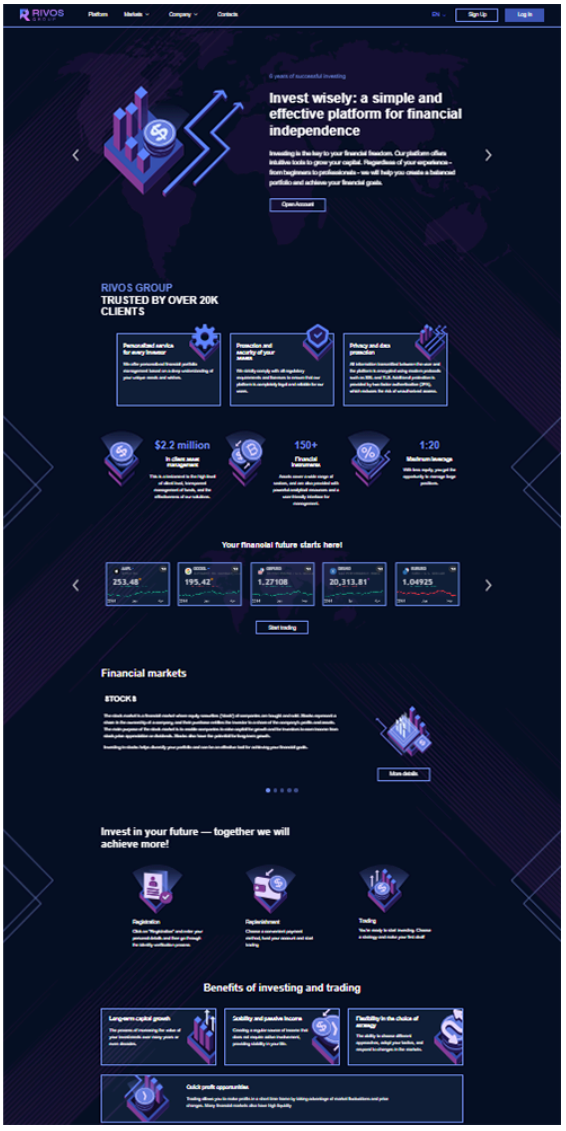
Fake UBSWebsite:



Real UBSWebsite:



Other recent SSH connections were made to **k-trades[.]com** and **rivosgroup[.]com**, both of which use the same website template. Neither site appears to represent a legitimate company; although they claim to have been established for years, no information about them exists online.



Overall, the activity observed from these 15 hosts was more consistent with threat actor behavior than that of typical victim machines. The reason why only this NetSupport RAT C2 is communicating with a Quasar RAT C2 remains unclear. It's possible that this C2 is compromised, and its activity is unrelated to the other infrastructure. However, the unusual behavior of the other "infected" hosts suggests they maybe connected to threat actor operations.

At this stage, there isn't enough information to draw definitive conclusions. Regardless, this pivoting detour uncovered intriguing infrastructure worth investigating further in the future.

Reporting and Recent Developments

We reported the SmartApeSG C2s to Stark Industries, and they were promptly taken down. SmartApeSG continued using Stark for a couple more weeks, procuring new VPS hosts which were also promptly taken down, before transitioning to Hivelocity (HVC-AS) for about a month, and then to HostZealot (HZ-US-AS). Since that

time, no additional ISPManager activity has been observed from the two Moldovan management hosts. While there have been minor changes in Internet telemetry patterns and open ports, the X.509 certificates associated with these hosts have remained consistent.

The NetSupport RAT C2s were also reported and taken offline, although some were discovered after the initial reporting. Since then, most of the previous NetSupport RAT domains have been randomly reassigned to new IPs, with the most recent setup occurring at the end of November. Additionally, some new domains have been created.

The same management host, **5.181.158.15**, is now communicating with some of these new IPs as it did with the previous set. While it's likely that other hosts are also involved in this communication, available Internet telemetry visibility has not illuminated them at this stage. We have reported these new IPs to the relevant hosting providers, and Stark has responded by taking them down. It is probable that **5.181.158.15** is engaging with additional NetSupport RAT C2 servers beyond those identified in our Internet telemetry data, though they have not yet been discovered.

Conclusion

This investigation demonstrates how pivoting through Internet telemetry data can uncover unexpected connections and shed light on complex threat actor infrastructure. Starting with SmartApeSG C2s, the analysis expanded to reveal active NetSupport RAT clusters, potential links between infrastructures, and additional malicious activity involvingQuasar RAT and cryptocurrency scams. While many components were taken down through proactive reporting, the continued evolution of these infrastructures highlights the persistence of the associated threat actors.

Recommendations

- Pure Signal^{TM} users can hunt for this activity by querying for the indicators of compromise shared below or based on characteristics such as X.509 certificate common names as shared in this blog post.
- More broadly, this research highlights the re-use of infrastructure in cyber-attack campaigns, potentially targeting a flaw in cyber defense rulesets and blocklists where indicators "age out" after a pre-determined time period. This is a good reminder to periodically review "old" indicators to check for current utilization.

Indicators of Compromise

IPs

5.181.159.111

5.181.159.113

5.181.159.119

45.8.145.132

45.67.35.101

185.153.183.59

Domains

23mtkro[.]cn

allenew1[.]com

asdgelvasd[.]icu

asdsrjhegrhj[.]xyz

compareggjs[.]com

dgdsrzzw45tg[.]cn

dsfygfnb3[.]icu

duvje6egvuas[.]com

dvtrstrhdbcvbxr[.]xyz

e3ubj753ifg[.]xyz

fdoshbjdo[.]icu

fufvnasie[.]icu

gfu6nfmgnm86gm[.]xyz

gjuauyfhjha[.]cn

gkdkr[.]icu

gsdgtruhu45[.]cn

huntaget[.]cn

isaydiuaysoidalkspw[.]com

jintsung[.]cn

jkhmzxvidfyidu[.]xyz

mgsubneu4hgba[.]xyz

mixuvvvjsurub[.]cn

moreeu[.]cn

msguguudfh4[.]xyz

nfdsnvuusds7d64jg[.]cn

recsfgsfxvdgr[.]xyz

ruhvsvya[.]icu

safvyhgdrsdfhd[.]xyz

sasfyvuaseyzzs[.]cn

sasygzsu4zusaty[.]cn

scheduleyaraupd2[.]cn

sdfojbeufibibsuu8u[.]cn

sdgn446yhd[.]cn

sdjbizirebz[.]cn

sertte56gzxes[.]cn

sevndgkhkidgr[.]xyz

sidfbuz8egozs[.]cn

ssdghgrehndx[.]cn

tojh5roh4[.]top

torpoa[.]cn

tripdsbeacgsa43wes[.]xyz

u4snvsrtvlrui[.]xyz

u55fbwiubyuere[.]xyz

usjnvovoo4[.]net

zjdhduv[.]com

zytjbgev[.]icu
