PROXY.AM Powered by Socks5Systemz Botnet | Bitsight

Archived: 2026-04-05 15:58:15 UTC

A year ago, Bitsight TRACE published a blog post on Socks55Systemz,a proxy malware with minimal mentions in the threat intelligence community at the time. In that post, we correlated a Telegram user to the botnet operation and estimated its size at around 10,000 compromised systems. After a year-long investigation, we are shedding new light on these conclusions.

- Socks5Systemz, identified last year during large-scale distribution campaigns involving Privateloader, Smokeloader, and Amadey, has actually been active since 2013.
- This malware was sold as a standalone product or integrated into other malware as a SOCKS5 proxy module. Such malware included, at least, Andromeda, Smokeloader and Trickbot.
- In recent months, Bitsight TRACE investigated a Socks5Systemz botnet with 250,000 compromised systems at its peak, geographically dispersed across almost every country in the world.
- The proxy service PROXY.AM, active since 2016, exploits the botnet to provide its users with proxy exit nodes and enable them to pursue broader criminal objectives.

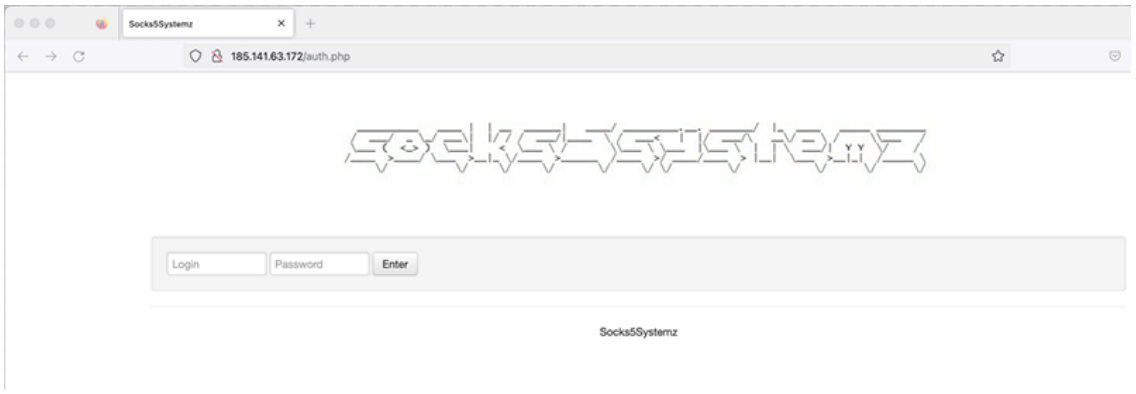

Image 1: The login page of the Socks5systemz C2 panel.

Socks5Systemz is a proxy malware designed to turn compromised systems into proxy exit nodes. Its name comes from the text that the threat actor uses in the backend panel.

Bitsight has described the inner workings of the malware in the previous post, Although it changed a bit in the last 12 months, this time we will not delve into the details of Socks5systemz, such as its malware analysis and

command and control protocols. Instead, we will outline the updates made to the malware later in this post.

Although Bitsight observed multiple distribution campaigns of the malware over the last year, it remained under the radar until September 2023—not just for us, but for the entire threat intelligence community, since there were almost zero references to it. After digging up, we discovered posts in multiple underground Russian forums linking to the malware dating back to 2013.

The image below shows a post, that was cross posted in multiple forums, where the actor *BaTHNK* is selling a "SOCKS5 backconnect system":

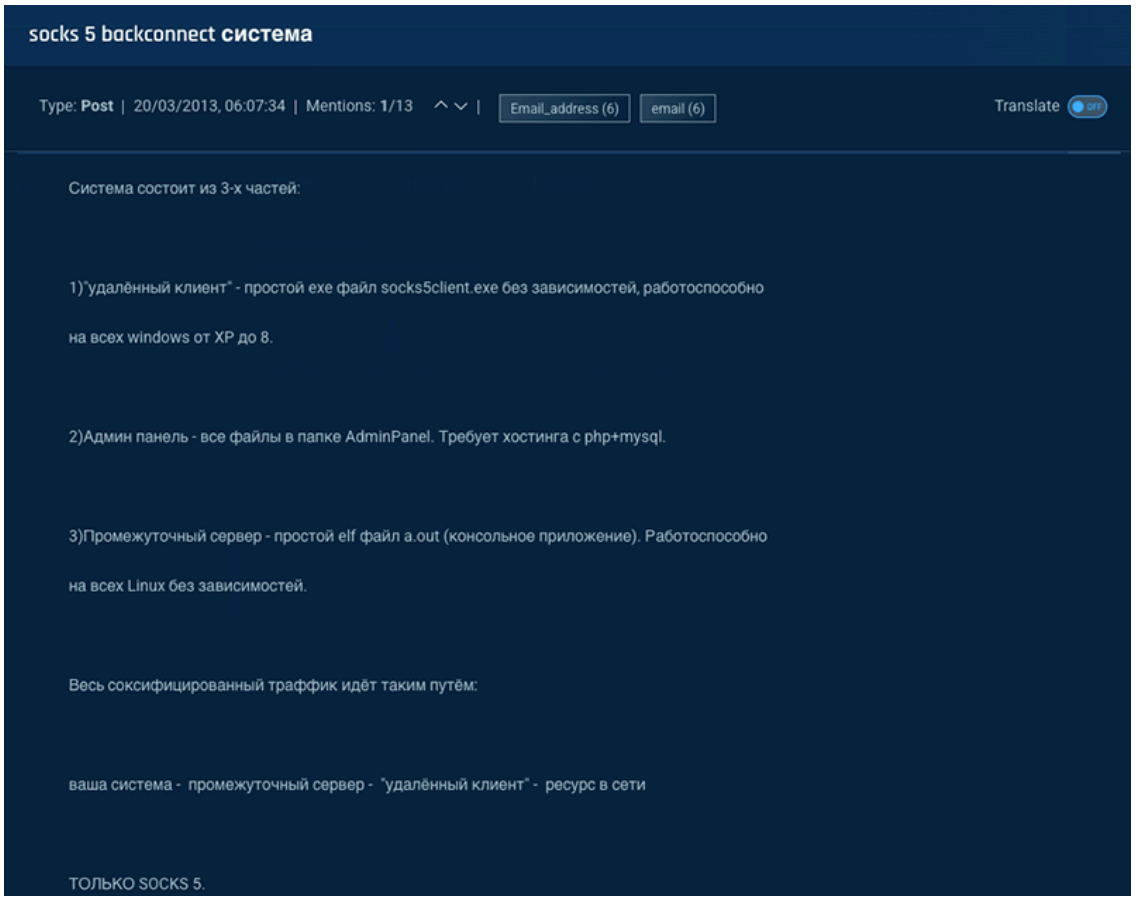

Image 2: Archived post from 2013 on forum XSS, where actor BaTHNK sells a SOCKS5 backconnect system

In the same thread, the actor posted some screenshots of the C2 panel with the same branding and template that we saw in current Socks5Systemz panels:

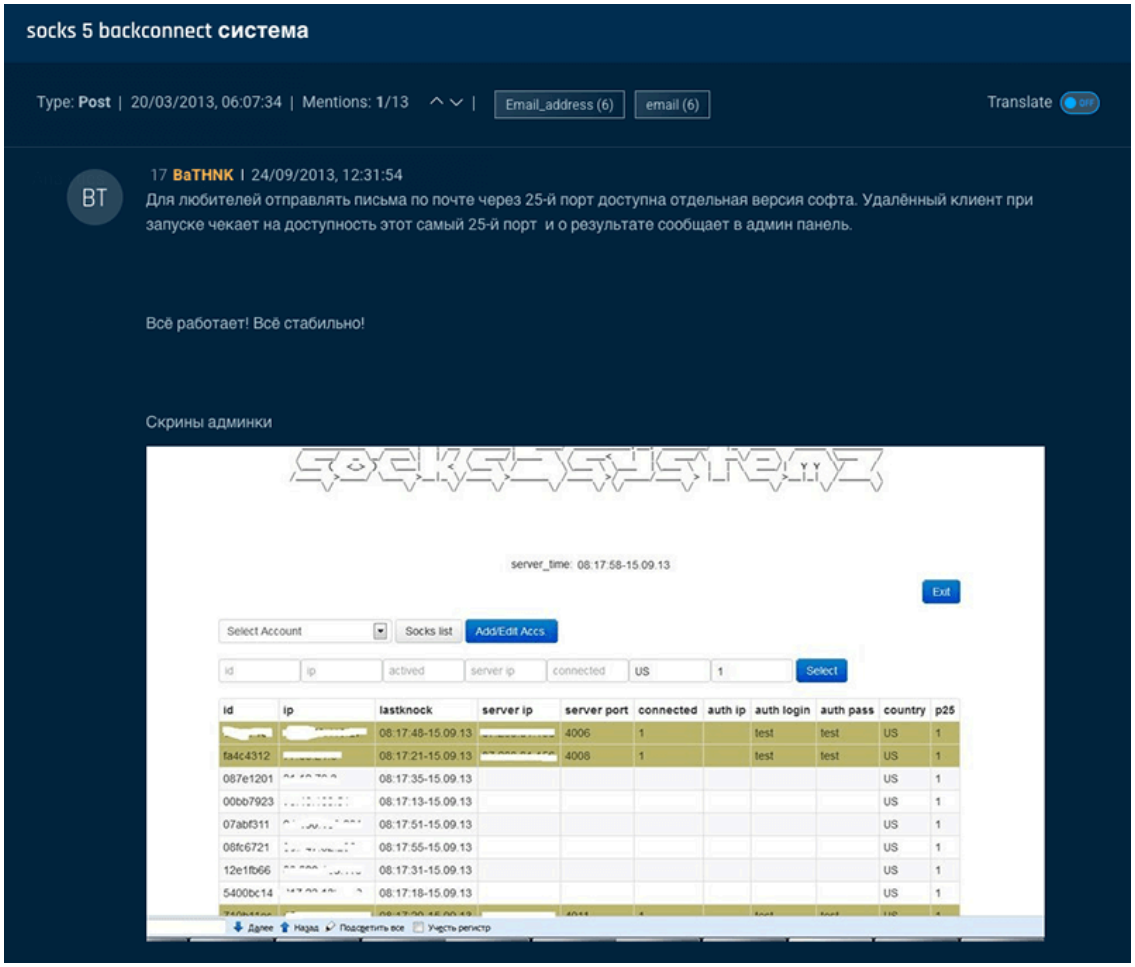

Image 3: A comment to a forum post in 2013, where actor BaTHNK posts screenshots of Socks5Systemz backend panel

The question is:

Why has a malware family that has been around for over a decade only recently been widely distributed?

The answer may be in one comment on that same thread, where actor *Ar3s* provided positive feedback on the malware and BaTHNK ability to customize the malware to suit customer needs:

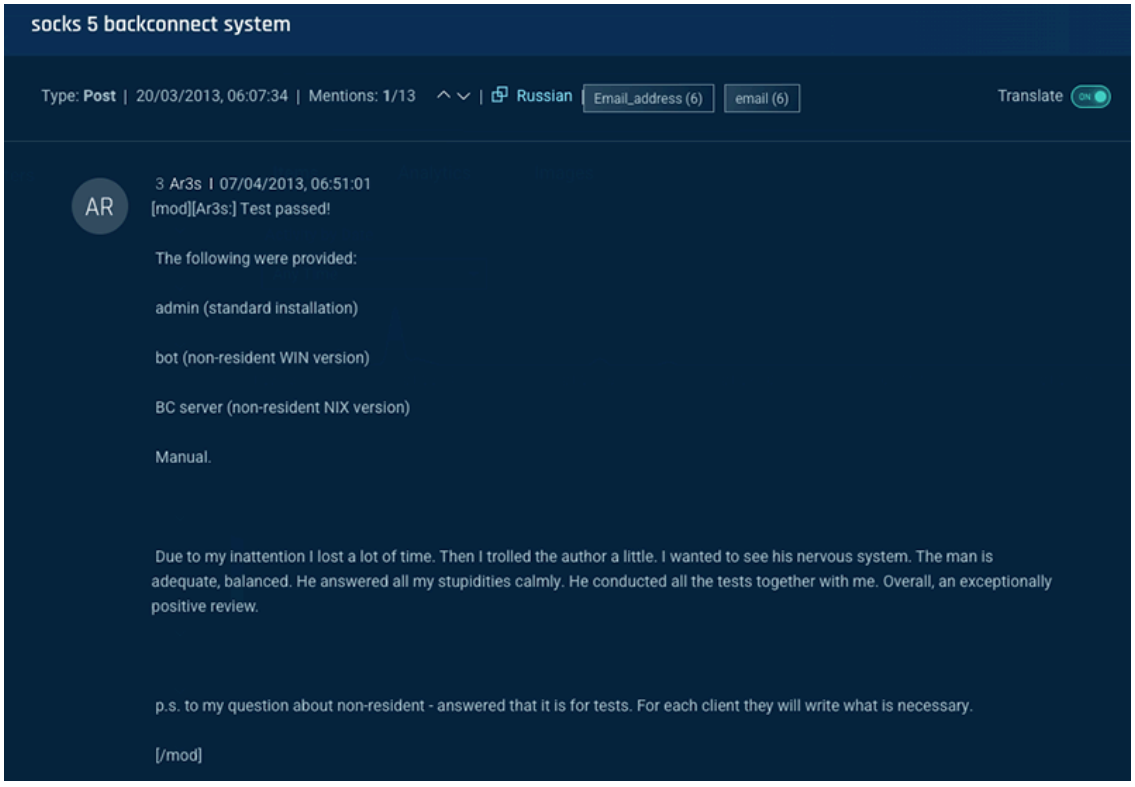

Image 4: A comment in the same thread, auto translated to english, where actor Ar3s provides positive feedback about the malware.

Ar3s, was one of the most prolific actors in the Russian crimeware scene until 2017, when he was arrested in Belarus in the outcome of Operation Avalanche. He was charged as the primary operator of the biggest Andromeda botnet, used to distribute more than 80 different malware families between 2011 and 2017.

After that positive review, *BaTHNK* adapted the malware to be used as a SOCKS5 proxy module of Andromeda, and a few weeks later, also added support for Smokeloader.

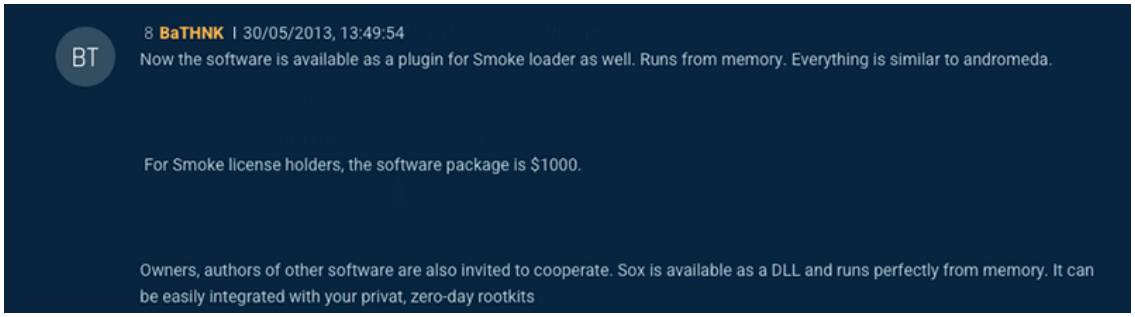

Image 5: Actor BaTHNK announces socks5systemz as a proxy module for Andromeda and Smokeloader malware (auto-translated from Russian)

During our research, we also found a proxy module for Trickbot (2017) with lots of code similarity and the same functionality as Socks5Systemz. At the time, *Vitali Kremez* (rest in peace), conducted an analysis of it.

The use of Socks5Systemz as a proxy module within other malware may explain the lack of references to it prior to November 2023; it likely operated under the radar, being detected as part of other malware, and didn't catch the

attention of the threat intelligence community.

In September 2023, we started to see widely distributed campaigns of Socks5Systemz using Privateloader, Amadey, and Smokeloader. This was the standalone version of Socks5Systemz as the final payload. We don't know why the *modus operandi* changed, but it may be linked to shifts in the crimeware ecosystem that prompted threat actors to adopt this approach.

With the support of the Registrar of Last Resort (RoLR), Bitsight was able to collect infection telemetry from the botnet due to how bots communicate with the command and control (C2) servers.

Image 6: Infected systems telemetry collected from late november 2023 to january 2024 for Socks5Systemz.

The botnet, which we've called Socks5Systemz V1, is widely spread around the world with bots in almost all countries on the planet. In late January 2024, the daily average of bots was around 250,000.

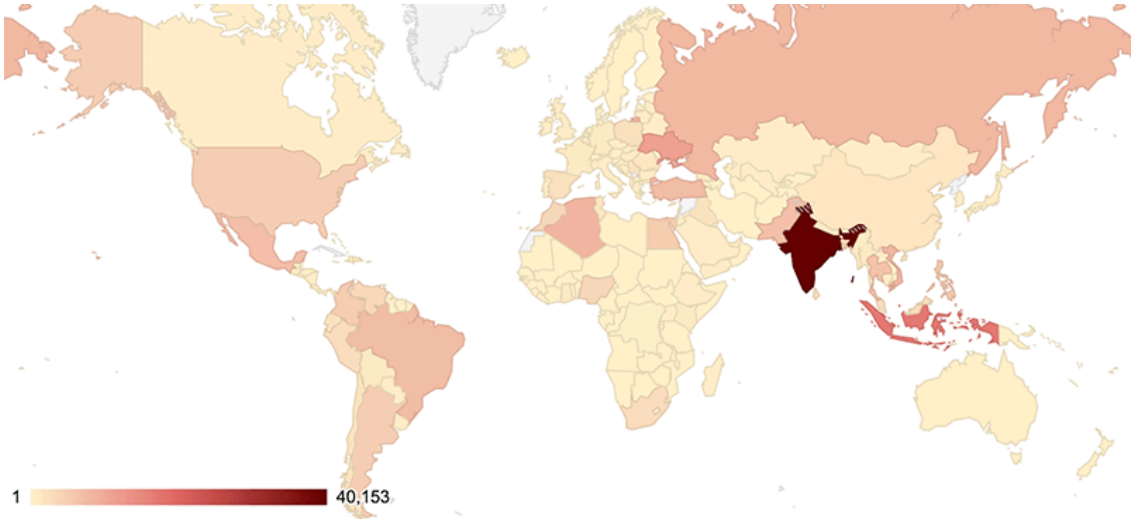

Image 7: Socks5Systemz V1 botnet geographic dispersion.

The table below lists the top countries affected by Socks5Systemz infections:

Country	**Infections**
India	40153
Indonesia	17027

Ukraine	11178
Algeria	8255
Viet Nam	8047
Russian Federation	7826
Turkey	7288
Brazil	7224
Mexico	6987
Pakistan	6802
Thailand	6452
Philippines	5664
Colombia	5165
Egypt	5164
United States	4784
Argentina	4756
Bangladesh	4432
Morocco	3758
Nigeria	3625
Others	73573

With 250k bots as a daily average, this is a huge botnet in today's landscape. For comparison, in its glory days, Andromeda had a 2M daily average—albeit with a vastly different business model. Similar proxy malware has daily averages between 15k and 50k bots.

Since January 2024, our telemetry counters have decreased over time. We're currently seeing around ~120k bots for the Socks5Systemz v1 botnet.

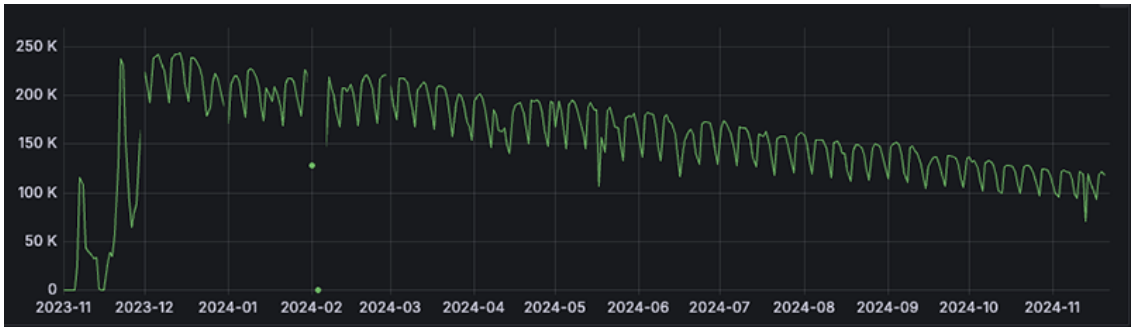

Image 8: Socks5Systemz botnet telemetry between Nov 2023 and Nov 2024.

The decrease in telemetry can be attributed to two factors:

- In December 2023, the threat actor lost control of Socks5Systemz V1 and had to rebuild the botnet from scratch with a completely different C2 infrastructure—which we call the Socks5Systemz V2 botnet.
- Because Socks5Systemz is dropped by loaders (such as Privateloader, Smokeloader or Amadey) that persist on the system, new distribution campaigns were used to replace old infections with new payloads.

Bitsight TRACE estimates that the current botnet maintains a daily average size of 85,000 to 100,000 bots.

In our previous post about Socks5Systemz, we linked the malware to a proxy service called BoostyProxy, which is being sold on Telegram by the actor 'boost'. While this association remains valid, further investigation reveals that boost is likely just a reseller in a larger operation.

Looking at infrastructure indicators of Socks5Systemz V1 and using the fallback domain `bddns[.]cc` (active until November 2023) as a pivot point, we see that its WHOIS information from 2018-03-06 reveals the original registrant, as well as the technical, administrative, and billing contacts as:

```
Name: Alexey Pavlov
Address: ul. Karla Marksa 77 - 41 - Novosibirsk, 314932 - Russia
Phone: +79264921021
Email: unvizik@gmail.com
```

The same name, phone number and address were used in 2016-01-09 to register the domain `proxy[.]am`, with the following WHOIS details:

```
Domain name: proxy.am
Registrar: globalar (GlobalAR LLC)
Status: active

Registrant:
 Alexey Pavlov
 ul. Karla Marksa 77 - 41
 Novosibirsk, 314932
 RU
```

```
Administrative contact:
  Alexey Pavlov
  ul. Karla Marksa 77 - 41
  Novosibirsk, 314932
  RU
  hostmaster@globalar.net
  +79264921021

Technical contact:
  Alexey Pavlov
  ul. Karla Marksa 77 - 41
  Novosibirsk, 314932
  RU
  hostmaster@globalar.net
  +79264921021

DNS servers:
  ns1.reg.ru
  ns2.reg.ru

Registered: 2016-01-09
Last modified: 2016-01-09
Expires: 2017-01-09
```

Upon examining the C2 infrastructure and investigating one of the backconnect servers associated with Socks5Systemz, operating with the IP address `109.236.51[.]104`, between February 2022 and November 2023, passive DNS records reveal the following:

Query	Type	Source	Count	Response	First Seen	Last Seen	Duration
109-236-81-104.hosted-by-worldstream.net	A	D	534	109.236.81.104	2023-12-11, 01:01	2024-05-03, 01:58	143d 23h 48m
hpf.proxy.am	A	B	11	109.236.81.104	2019-07-16, 06:38	2021-02-13, 20:23	1y 213d 14h
design.proxy.am	A	D	10	109.236.81.104	2018-03-20, 07:19	2019-01-17, 22:16	303d 14h 56m
hpf.proxy.am	A	D	97	109.236.81.104	2018-02-15, 18:23	2021-08-09, 22:21	3y 176d 2h
api.proxy.am	A	D	1387861	109.236.81.104	2018-02-12, 17:36	2021-08-30, 06:14	3y 199d 11h
api.proxy.am	A	B	44	109.236.81.104	2018-02-12, 17:36	2021-04-29, 23:08	3y 77d 4h

Figure 9: PDNS records for 109.236.51[.]104

This is an indicator that the IP of a C2 server for Socks5Systemz was reused from a server that hosted `design.proxy[.]am, hpf.proxy[.]am and api.proxy[.]am` on or about 2018-02-12 and 2021-08-30.

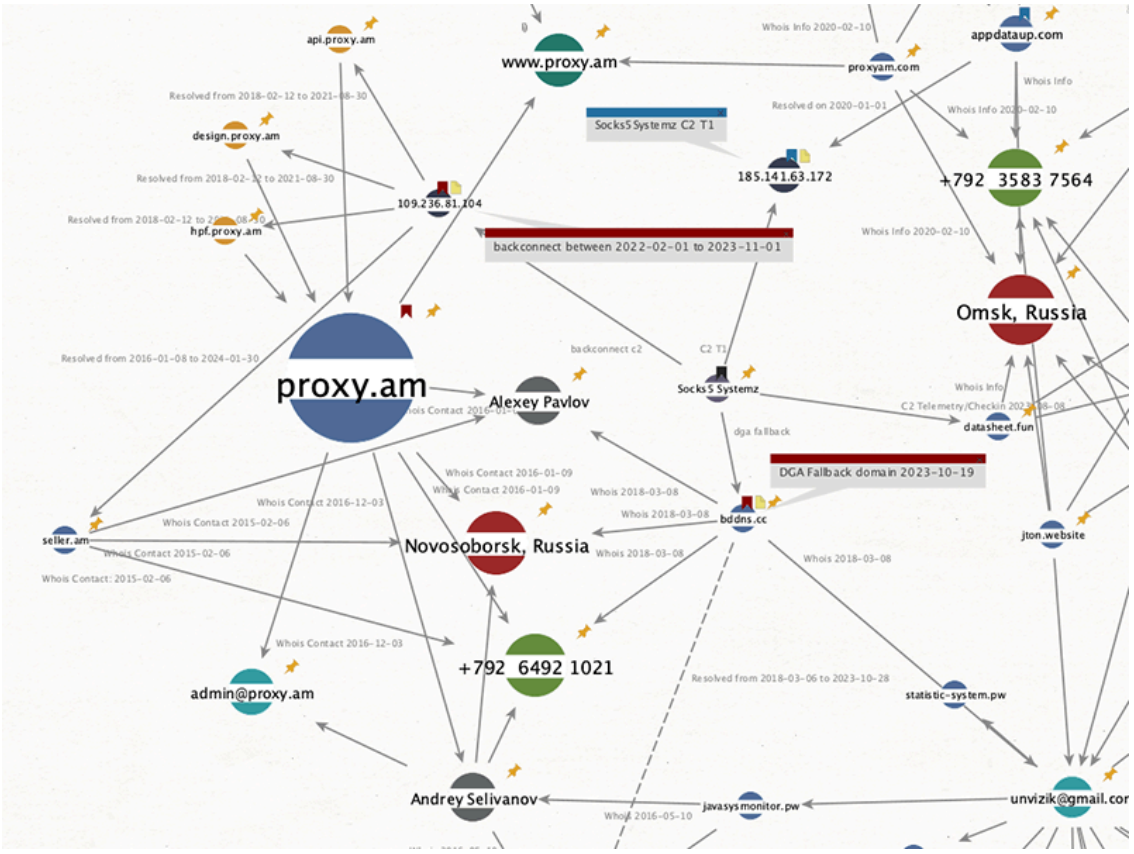

Figure 10: Relationship graph between bddns[.]cc, proxy[.]am and 109.235.81[.]104

`PROXY.AM` markets itself as a service that "*provides elite, private and anonymous proxies*", with plans ranging from $90 to $700 USD.

The main URL for access to the proxy service was `https://proxy[.]am`, until November 2023. Since then, the threat actors have registered `proxyam[.]one`. The former redirects to this new domain.

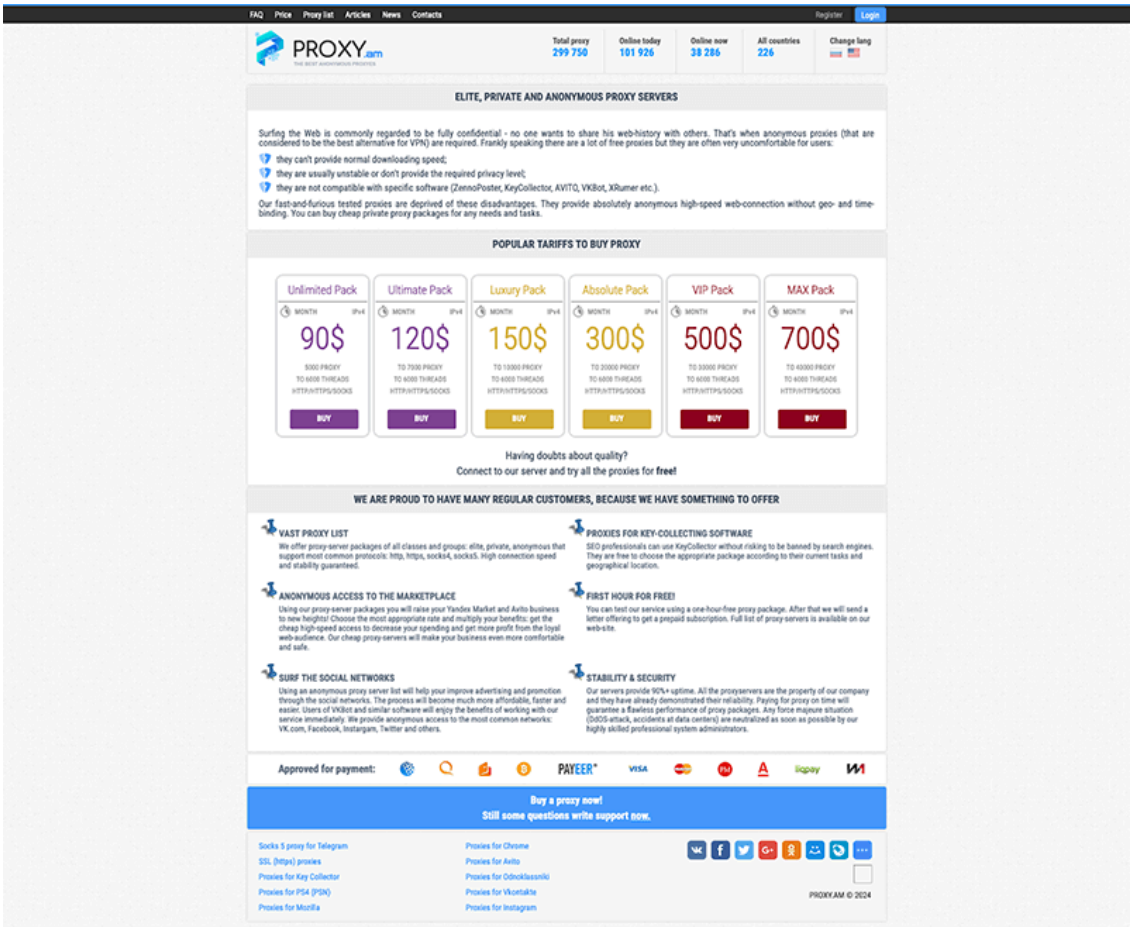

Figure 11: Screenshot of Proxy.AM homepage in November 2023

The website advertised a total of around 300,000 proxies in November 2023. Since then, PROXY.AM redesigned their website and their proxy packages:

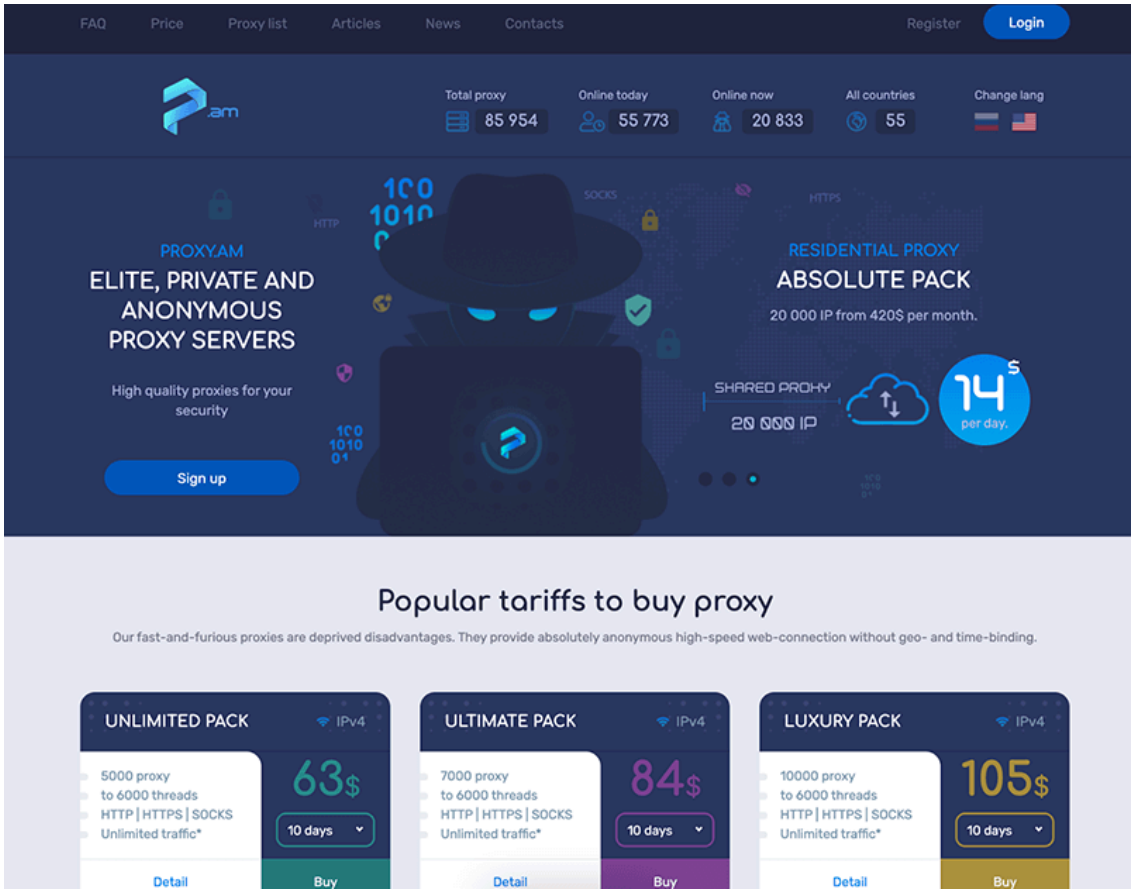

Figure 12: New PROXY.AM website in November 2024

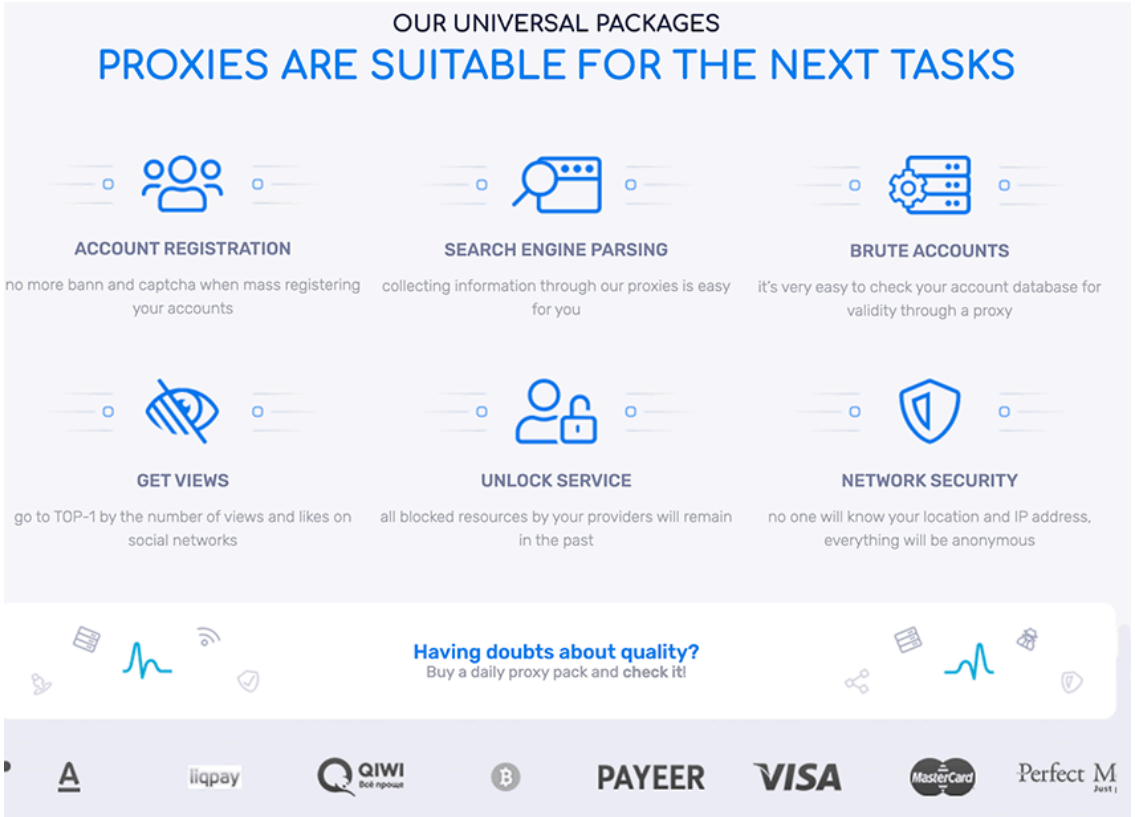

Figure 13: PROXY.AM advertised use cases. Mind the "Brute Accounts".

The service provides contact via telegram and email.

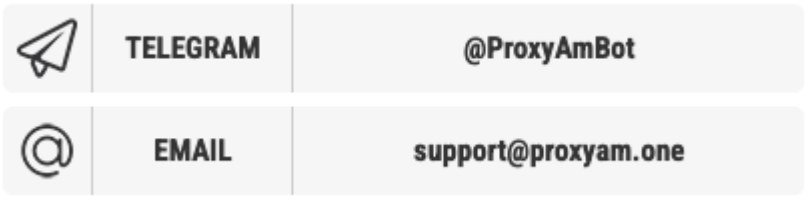

Figure 14: Support addresses for Proxy.AM

Between December 2023 and October 2024, some changes in the malware and C2 infrastructure were implemented. Bitsight TRACE observed:

- New infrastructure:
  - 26 servers in total (14 backconnect servers, 6 C2 servers, 5 nameservers, 1 fallback)
  - More geographic dispersion across Europe
  - New host providers
  - New fallback domain(s)
- Malware updates:
  - Updated C2 protocol
  - New RC4 keys, new URL paths, new beacon data format
  - Backconnect protocol is now done over port 2023/TCP
  - Obfuscation! It's not easy to extract the malware configuration statically

Besides these changes, the core functionality remains unchanged, as detailed in our previous analysis.

Proxy malware and proxy services aren't new, but they're becoming more relevant because of the increased offer announced in underground forums and the silent impact they have in our networks. We've covered this kind of malware in the past and Lumen's Black Lotus Labs has recently published a similar review of Ngioweb and NSOCKS. Proxy malware and services enable other types of criminal activity adding uncontrolled layers of anonymity to the threat actors, so they can perform all kinds of malicious activity using chains of victim systems.

In this post, we uncovered a possible explanation to how Socks5Systemz has remained under the radar for the last 10 years by being deployed as a SOCKS5 proxy module for other malware and being detected as other malware and not for what it is in reality. We also uncovered the proxy service that exploits the largest Socks5Systemz botnet we know of at the moment.

Bitsight TRACE thanks The Registrar of Last Resort (RoLR) and Lumen's Black Lotus Labs for ongoing support in this investigation.

Below are indicators of compromise to help you detect Socks5Systemz in your network or leverage them for further research. Happy Hunting.

This section contains IOCs for Socks5Systemz V2

Threat Actor Controlled DNS Servers

```
141.98.234.31
81.31.197.38
45.155.250.90
152.89.198.214
91.211.247.248
```

Command and Control

```
185.208.158.248
185.237.207.107
185.208.158.202
79.132.128.13
176.10.111.126
194.62.105.143
```

Backconnect Servers

```
195.154.176.209
89.105.201.183
46.8.225.74
88.80.150.13
195.154.174.225
62.210.201.223
185.141.63.209
195.154.173.35
195.154.174.12
62.210.204.81
62.210.204.131
185.141.63.216
195.154.185.134
88.80.148.252
```

Samples

```
5260154782dd66c6a7b0e14c077c4b44ed1f483c6708495d0344edf8a14e2b27
36cffd7d54385e0473cb7f7bf2d33910027428837725c4d3649ff1af2d88cb2b
aa93289a23603efc27f70a7eb38f8e81fa7c30f4a5dff71f70c6f2ee583df619
e185e43f039f7a97672db4a44597abd6d2bf49c08d7bc689318a098ec826bb00
f6bbff3463d01da463091dc3347f5f42b32378353d2f7ddfab6285ecf0450c14
a2a41ff58541f577ea1580932cc89642e987239a2fa1ccdb33a3029a520ecd0b
fa3fe68c4a784c01e170098296b3212696b611e0239b69a40f4438532ca33e88
54feb0e02729304c1c054e34c3bcb4e76be31b31ec2276187ccc4479378ce130
```

```
0fc2f189aa3ebc1ff836079e49dac9758ab5e807d7ab4b42ff37c2376bcc2705
bf34984756336bc78428f3f856be287ef364afa3330cac5facf019c39be73657
b1e5b0e42e039b9711c435d691f1372ec663b2cb5a5d6a733d859d75a9f2d662
f4456c54b840b5650d131ee27ffc9f23b7b3d8344cd88bd2dd2dbad05741e401
c742642edeae783ffdc9efd52f514a5eef830ec115f8e723ee7cfd82ca7c0ba6
dd075ec25d314f2d97d89065239ccb1d6c680d3f08ea94bf59f522545a1546c9
75e722495c157a05b557580863f90b856d6ec229c7cb4974a008c823377369f5
```

Source: https://www.bitsight.com/blog/proxyam-powered-socks5systemz-botnet