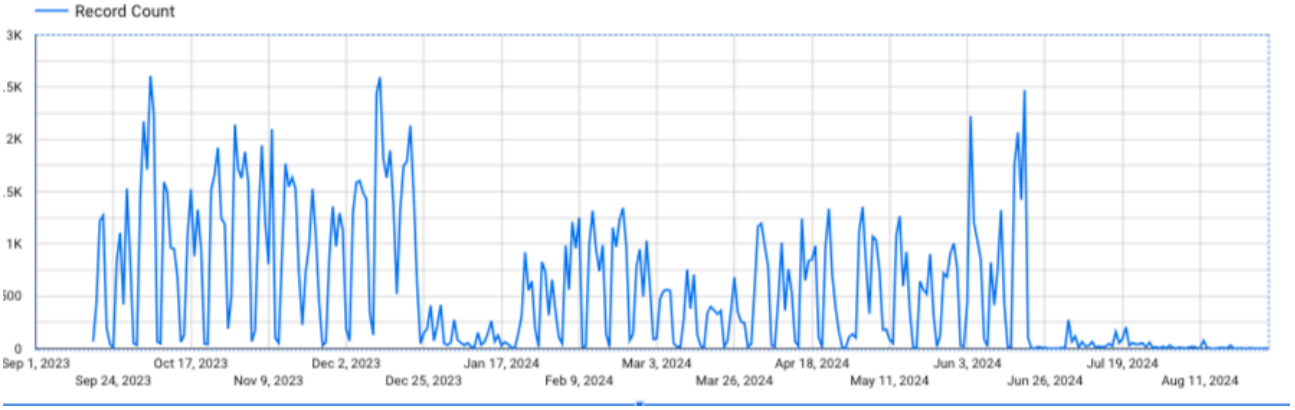
/var/log/notes

Archived: 2026-04-05 21:38:54 UTC

By Jeff White (karttoon)

Threat researchers...Hear me and rejoice!

A dump of the Black Basta ransomware group's chat messages has surfaced! Totalling almost 200K entries and spanning a little over a year from late 2023 to late 2024. These moments are always a great insight into the inner workings of these well established organizations that we so rarely are able to see. They're worth the read even if you're just a slight bit curious, it's a treasure trove of information!



The logs were posted early on February 20th and were mostly in Russian which meant a lot of us scrambled to find ways to quickly translate it so that we could better analyze the conversations. After that was squared away and, while the translators were roaring, I started conducting typical searches for reliable patterns (IP, domain, url, hash, coins, etc) which is a typical method to zero in on a starting point to begin reading the translated content. I'd flag messages and add 1 hour to each side of the message so that I can get a little more context. While doing this, one pattern that I kept noticing when looking at the Russian text were strings like "ftp4", "ftp3", and "ftp1".

4) MAIN FTP4 138.201.81.174 root 7hQfaOF5*6q1SOljCbh#eKa@hI pass 2: Xn7Y4zq1uU$!gG#Fjwgl$26exubE&QM

Pivoting on those types of labels ("FTP4") would lead to messages like the below, providing a potentially related onion address and new IP address.

ftp4 6y2qjrzzt4inluxzygdfxccym5qjy2ltyae7vnxtoyeotfg3ljwqtaid.onion 179.60.150.111 это ☝ у нас фтп от блога куда мы выкладываем дату.

This repeated pattern started to pique my interest since it was a clear naming structure of servers which might imply more importance. Plus, when you stop to think about it objectively, what would a ransomware group need a large amount of FTP servers and storage for? The loot of course! This made it feel like a good starting point for some analysis and to see what could be derived simply through the chats between threat actors.

This blog is going to cover that specific avenue of research I went down while reading through this cache of data. I'll piece together some of their infrastructure based on messages and then take a look at the infrastructure itself. It's easy to get lost in the volume of messages within these leaks so this will help to highlight how you can hone in on disparate data to generate some actionable intelligence.

But before diving in further, I wanted to drop a couple of points and/or lessons learned from going through this exercise, incase its helpful for others in the future.

- Find and test a way to bulk translate a large amount of messages reliably and quickly -- you never know when you might need to!
- As new translations from different engines came out, the differences were very noticeable. Try not to rely on one translation as keywords might significantly change the context, eg one might say "Gasket" while the other says "Proxy".
- Patterns are your friend. Give in to grep and regex as your lord and savior. The better you are with them, the easier it is to slice and dice large amounts of random data.
- Once the leak occurs, any live services should be considered compromised and tainted. Recent activity you see could be another researcher. I know of at least one such instance in this leak where a site was access by numerous folks on Twitter who stumbled on the same messages within a day of the leak.
- Strike while the iron is hot because things go down quickly. Have a solid plan to collect related files or data before they vanish for good. Make sure your collection techniques work reliably over TOR as well.
- Don't get tunnel vision looking for "malware" or other just indicators. Messages with things like linked screenshots or paste's can prove extremely valuable.
- Contextualize each interesting match with hours of chats before and after. Seeing how it came up in conversation is extremely valuable, what the response was, and what the subsequent messages can quickly lead you to many new places.

[gets off soapbox]

Pivot Research:

As I was reading a lot of these conversations, the topic of FTP servers usually came up in two contexts. First was in a tech support/maintenance perspective discussing migrating IP's, storage, cost, etc. The second was support around the usage of them - how to upload files and get data published. This revealed lots of interesting insights into how they effectively operate.

Take this translated post below - it's a guide on how to post a new victim to the Black Basta DLS (Data Leak Site) - this is effectively the beginning of the extortion phase of ransomware attacks.

A guide to publishing a blog. 1. Go to https://passwordsgenerator.net/ and uncheck the first checkbox for special characters. 2. Set the size to 40 and generate a new password. 3. Connect to FTP and create a folder with a new name. 3.1 Fill the date into this folder 4. In the blog in the Data folder name input enter the generated password. 5. In the Public blog name input enter the company name. In the future there will be a public link like: https://stniiomyjliimcgkvdszvgen3eaaoz55hreqqx6o77yvmpwt7gklffqd.onion/?id=company. 6. In the Public ftp link input enter the domain of the ftp server. ftp1: fmzipzpirdpfelbbvnfhoehqxbqg7s7efmgce6hpr5xdcmeazdmic2id.onion ftp2: r6qkkk55wxvy2ziy47oyhptesucwdqqqaip23uxuxregdgquqq5oxxlpeecad.onion ftp3:

weqv4fxkacebqrjd3lmnss6lrmoxoyihtcc6kdc6mblbv62p5q6skgid.onion ftp4: 6y2qjrzzt4inluxzygdfxccym5qjy2ltyae7vnxtoyeotfg3ljwqtaid.onion 7. Fill in the Total data & Data published items. 8. Click the Unhide company button. Now the blog is published and anyone can download the date.

This message alone provides four labels and four onion addresses which allegedly feed the stnii* onion address (Black Basta's primary DLS site). Other chats show them discussing listed victims or fixing posts - typical website issues. You can't effectively extort victims and get paid if the website doesn't work!

[23:56:17] AA: We won't get paid. [AA: if we don't publish. [23:56:22] AA: dat. [23:56:26] AA: Do you realize that, brother? [23:56:33] Bio_2: so the gasket died. [Bio_2: when you were on vacation. [23:56:45] Bio_2: and you couldn't pour anything in. [23:56:48] Bio_2: whatever I could get. [23:56:58] AA: We'll make a new gasket. [23:56:59] AA: and fill it up. [23:57:03] Bio_2: ++ [23:57:05] Bio_2: http://stniiomyjliimcgkvdszvgen3eaaoz55hreqqx6o77yvmpwt7gklffqd.onion/?id=BION_2 [23:57:07] Bio_2: it works.

As you start reading more of the messages you can start piecing together the information for each server. FTP4 has had IP addresses "138.201.81.174" and "179.60.150.111", along with an onion address of "6y2qjrzzt4inluxzygdfxccym5qjy2ltyae7vnxtoyeotfg3ljwqtaid.onion". It hosted victim data for the "stniiomyjliimcgkvdszvgen3eaaoz55hreqqx6o77yvmpwt7gklffqd.onion" DLS.

[ftp4] type = sftp host = 138.201.81.174 user = ftp_white pass = HntCeYIUyxC2mPwOrmNiSnEKhBreZaXXyTqtJoVtNE898nwi_qPJuGKbLwZ_zEanSi6f0q5L8dc

Below is a message, which appears a few times, and seems to list the cost for servers/services. More importantly though, it exposes a list of collected IP addresses which they control.

95.217.43.112 40tb drives $280. 138.201.196.90 240$ 144.76.223.74 240$ 148.251.236.201 240$ 144.76.235.89 240$ 138.201.81.174 40tb disks 280 95.217.225.177 40tb disks 280$ 138.201.31.166 220$ 136.243.93.236 220$ 46.4.78.94 under panel 210$ 5.9.158.84 20tb disks 250$ ...

In the same message you can see discussion about migrating from one server/IP to another.

gasket (178.236.246.148 It's been removed) REPLACED TO --> 95.216.97.206 148$

Along with subsequent replies giving further context on multiple servers.

144.76.235.89 240$ \\\\\\\\\\\\\\ according to my docs - it's sox bot 2023!!! I think you can delete it!!!! 138.201.81.174 40tb disks 280$ \\\\\\\\\\\\\\ old FTP can be deleted, I don't use it for a long time already!!!! it doesn't work already! 95.217.225.177 40tb disks 280$ \\\\\\\\\\\\\\ it's ftp5 it doesn't even work it doesn't connect there! you can delete it! 5.9.158.84 20tb disks 250$ \\\\\\\\\\\\\\ it's ftp3 it doesn't even work it doesn't connect! You can delete it!

This process is repeated for every label, every domain, every onion address, and every IP until I have pieced together a decent collection of their infrastructure that I can pivot on. For this research, I focused on looking at the FTP server ecosystem as it's likely to be highly trafficked, especially given the success of Black Basta over the

time period in question with numerous victims being uploaded. Below are a few observations that stood out regarding them:

- They rotate FTP servers a fair bit and migrate them to different IPv4 addresses, while keeping the advertised onion address.
- The FTP servers are setup in Primary/Secondary configurations for redundancy and backups.
- A lot of the FTP servers have non-onion domains attached to them. This may make direct backend access easier for affiliates.
- They have good password hygiene both in using password generators for sufficiently complex passwords and changing them regularly.
- The FTP servers, along with some other servers like proxies and CobaltStrike instances, shared a label of BraveX (where X was a number) possibly implying a cluster.

The servers with the Brave labels are referenced frequently with their non-onion FQDN, providing amusing context clues such as "public blog download" and "data blog download".

Brave3 = downloaddotaviablogadd.io Brave4 = publicblogdownloaddotaviablog.su Brave5 = datablogdownloaddotaviablog.su Brave6 = privatdatecomdote.su

Below are my notes on the servers I felt most relevant to this discourse and aggregated into a single list. These were pieced together from commentary, maintenance messages, troubleshooting conversations, guides, purchase orders, and anything else that provided additional context for grouping. Keep in mind these chat logs are a picture in time and represent only a subset of their overall communication as we know they used other mediums for conversations and even in-person meetings or phone calls.

Labels: FTP1 Main IPs: 179.60.150.124 Onions: fmzipzpirdpfelbbvnfhoehqxbqg7s7efmgce6hpr5xdcmeazdmic2id.onion Labels: FTP1 Proxy IPs: 23.81.246.105 Labels: FTP2 Main, FTP1 Middle, Brave3, Brave7 IPs: 178.236.246.138 -> 185.224.113.13 Domains: megatron.top, megatron2.top, megatron3.top, publicblogdownloaddotaviablog.com, downloaddotaviablogadd.io Onions: r6qkk55wxvy2ziy47oyhptesucwdqqaip23uxregdgquq5oxxlpeecad.onion Labels: FTP2 Middle IPs: 178.236.246.13 Labels: FTP3 Main IPs: 185.190.24.13 Onions: 6y2qjrzzt4inluxzygdfxccym5qjy2ltyae7vnxtoyeotfg3ljwqtaid.onion Labels: FTP3 Middle, Brave5, Proxy IPs: 178.236.246.147 -> 185.224.133.15 Domains: downloaddotaviablog.su, downloaddotaviablog.com, datablogdownloaddotaviablog.su, stuffsteven.top, stuffstevenpeters.top, stuffstevenpeters2.top Labels: FTP3 Proxy IPs: 192.52.166.115 Labels: FTP3 IPs: 5.9.158.84 Onions: weqv4fxkacebqrjd3lmnss6lrmoxoyihtcc6kdc6mblbv62p5q6skgid.onion Labels: FTP4 Main IPs: 138.201.81.174 -> 179.60.150.111 Onions: 6y2qjrzzt4inluxzygdfxccym5qjy2ltyae7vnxtoyeotfg3ljwqtaid.onion Labels: FTP4 Middle IPs: 45.182.189.120 Labels: FTP5 Proxy IPs: 142.234.157.12 Labels: FTP5 IPs: 95.217.225.177 Labels: FTP6 Pad IPs: 23.81.246.165 -> 192.52.166.141 Labels: FTP7 Pad IPs: 185.243.112.107 Labels: FTP9 Proxy IPs: 104.243.37.25 Labels: FTP Routing, Proxy, Advert Pad IPs: 45.15.157.234 Labels: Brave2, fastflux IPs: 5.182.86.108 -> 5.42.76.214 Domains: downloaddotaviablog.com, privatdatecomdote.su, databasebb.top, onlylegalstuff.top Labels: Brave4, Proxy IPs: 95.217.40.220 -> 65.108.98.161 Domains: downloaddotaviablogadd.io, publicblogdownloaddotaviablog.su, greenmotor.top, greenmotors.top, greenmotors2.top Labels: Brave6 IPs: 178.236.246.148 Domains: downloaddotaviablog.io, privatdatecomdote.su,

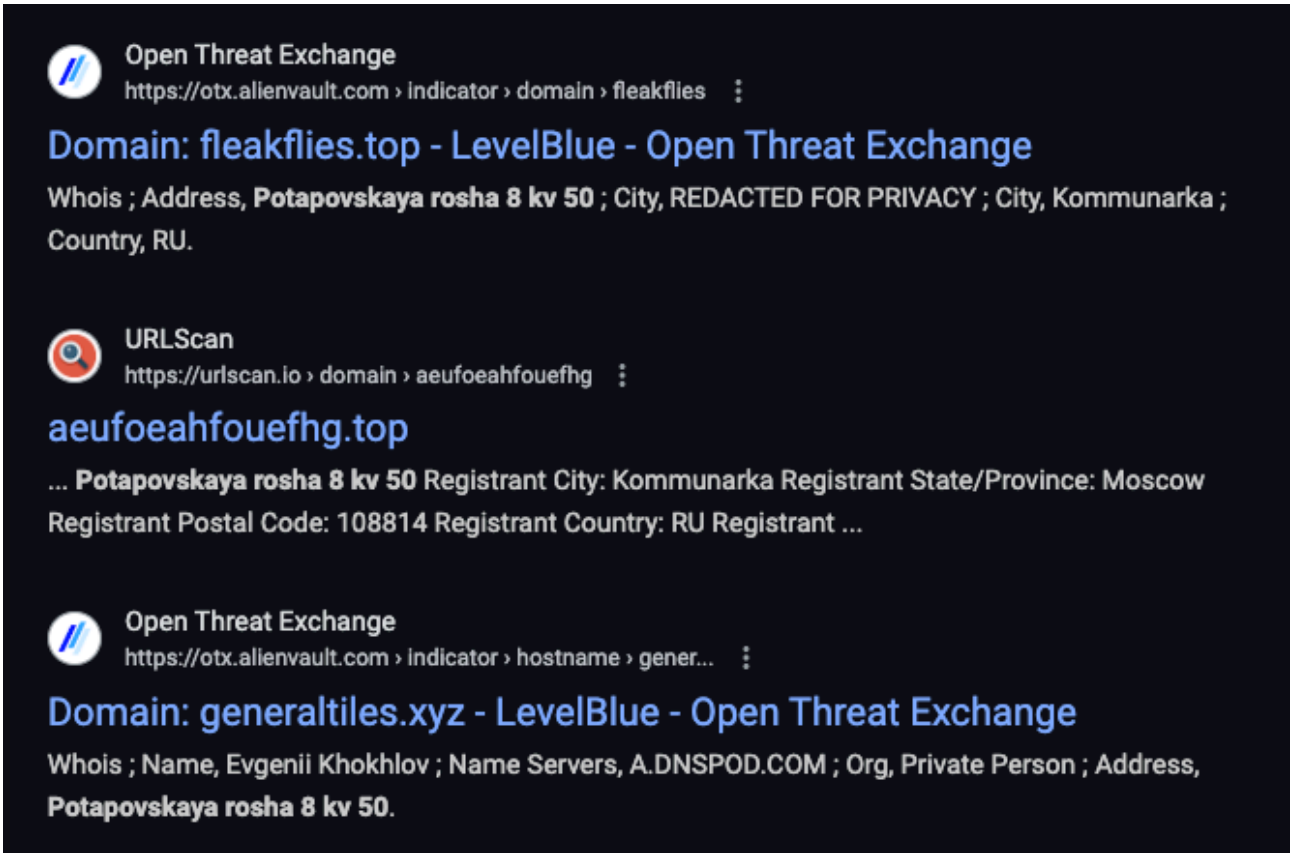
thesiliconroad.top Labels: Basta Blog IPs: 138.201.199.104 Labels: Basta Blog 2 IPs: 95.216.39.254 Labels: CobaltStriker Server IPs: 104.200.72.124 Labels: CobaltStrike Server IPs: 172.93.101.47 Labels: None IPs: 23.88.64.226 Onions: qlcquql6hx6qle4oib2euefnjoqi4uk7i2iofahu4d44n3d7hfs3oeid.onion

This provides a solid base to start pivoting on to seek out new information *outside* of the leaks. Also of note, you can observe how some of the onion addresses and domains are hosted on multiple servers over time just by looking for the overlaps in hosting. For example, "6y2qjrzzt4inluxzygdfxccym5qjy2ltyae7vnxtoyeotfg3ljwqtaid.onion" was seen referenced on FTP3 and FTP4, while servers Brave2 and Brave6 both at some point resolved to "privatdatecomdote.su" and "downloaddotaviablog.com". Most of these servers are no longer up so trying to do any kind of door knocking or more introspective searches is, unfortunately, not really on the table. Likewise, as this activity is a bit older, things like netflow become extremely difficult to source for trying to figure out how may be uploading data to them. But, since not all of their infrastructure is hosted in RU, there is a possibility additional logs could be gathered from hosting companies which may shed further light on access. Either way, there are a good amount of domains so one of the first orders of business is to review the domain registrations and passive DNS.

While going down the list of domains in my aggregate list and pulling up historical registrant information, I kept noticing certain values re-appearing across the records. As a lot of the domains had some form of domain privacy, the historical records sometimes only exposed one or two facets of the registrant but, given the context, we can relate them together easy enough:

Evgenii Khokhlov Potatpovskaya Rosha 8 KV 50 +7 916 511 46 15 geraregaettemu@mail.ru

It's entirely possible it's fraudulent registration information, which is a common occurrence, but the repeated usage of these values allows us to cluster them all the same. Googling any of these leads you to numerous posts concerning site reputation and scams that contained at least one of these pieces of information.



Even a tweet back in 2022, prior to the leak, linking the e-mail to a Ukraine aid scam.

Focusing on the historical registrations associated to the name "Evgenii Khokhlov" reveals the following domains:

aefieiaehfiaehr.top aeufoeahfouefhg.top databasebb.top greenmotors2.top greenmotors5.top greentrees.top marathones.top megatron3.top onlylegalstuff.top sauria.top stuffstevenpeters2.top teams-microsoft.top

thesiliconroad1.top thesiliconroad2.top wdqwhfusad.top yeahweliftbro.cz

This was a relatively small list of domains but it had a high overlap with what I had already collected from the messages. This also means we can assume further relations based on the naming structure, even if context wasn't derived from the leaked chat logs. For example, "thesiliconroad1.top" is mentioned in the below message, along with some other obviously related domains.

thesiliconroad1.top greenmotors5.top onlylegalstuff5.top stuffstevenpeters4.top databasebb3.top

So it's safe to assume "thesiliconroad2.top" is either a new iteration or an additional server in this cluster. Similarly, we can draw some conclusions about these other domains - "onlylegalstuff.top" only contains legal stuff and "yeahweliftbro.cz" is an homage to their ideology of healthy living.

Switching over to e-mail we're provided with a much larger list of domains, albeit with a bit less overlap in the logs; however, based on the names they all appear malicious in nature. This could be due to a number of reasons. First, we know from the logs that Black Basta, like most ransomware/cybercrime groups operate as a business and do business with other entities for services they don't specialize in or want to do in-house. Second, for a lot of these threat actors, they don't just have a singular job or hustle going, they diversify and dip their toes into many ventures. Basically, someone running phishing campaigns for Black Basta may also run them for other groups so we have to recognize that while it's badness, it might not be directly related badness.

What does that mean for this list? Well, it could be that the individual used the e-mail for most of their registrations, Black Basta related or not, but maybe used the Evgenii name when it was. It's also clear there are some clusters of activity where the name gives the activity away - some of these activities might overlap with known TTP's for Black Basta and using stolen credentials to gain access to victims and is yet another link worth exploring if you have case-related data to correlate against.

I'm going to break up some of the domains into related clusters to highlight some interesting patterns but if you want to see the full list, it can be found here:

Consider this cluster for Scotiabank. Multiple auth related landing pages and secure login sites. Typical for credential phishing against users of their service.

auth-scotiabank.com auth-scotiabankcanada-online.com auth-scotiabankcanada-secure.com auth-scotiabankcanada.com auth-scotiacanada.com auth-scotiaonline-scotiabank-secure.com authmobileapplscotiaonline.com scotiabankcanada-auth.com scotiabankcanada-secure.com scotiaonlurl.com secure-scotiabankcanada.com securelogin-scotiabank.com securescotiabankmobile.com

This can be observed for other Canadian based banks as well, such as Royal Bank of Canada:

1omniroyalbanksignin.com auth-rbcroyalbank-online.com auth-rbcsecure.com auth-royalbank-secure.com auth-royalbankrbc-online.com auth-securerbc.com https-rbc.com inforbcroyalbank-secure.com infosecure-rbcroyalbank.com login-rbcroyalbank.com login-royalbank.com login-royalbankrbc-secure.com login-secure-royalbankrbc.com rbc-accountreset.com rbcnotif.com rbcroyalbank-canada.com rbcroyalbank-infosecure.com rbcroyalbank-secureinfo.com rbcroyalbanksecure.com reactivatemycardstatus.com royalbank-secure-online.com royalbankofcanada-rbc.com royalbankrbc-auth.com royalbankrbc-login.com royalblogin.com royalmenupage.com royalusermanager.com secure-inforbcroyalbank.com secure-rbc-auth.com secure-rbcroyalbankinfo.com secureinfo-rbcroyalbank.com

This pattern continues to repeat itself for a number of other banks and institutions, likely aligned to spam campaigns targeting their respective user bases.

bankofcyrpus.com banquenationale-nationalbank.com bmobankofmontreal-secure.com bmoverifyclientcard.com bnc-connexionsecure.com bnc-reset.com bncclientconnexion.com bncmessage.com bncsecure-banquenationale.com canadarevenueagency-deposit.com canadarevenueagency-securedeposit.com lloydsbank-livechat.com metrobank-livechat.com metroonlinesupport.com royalmail-redirect.com royalmail-slot.com

Even containing some of the usual remote access service masquerading to trick users into inputting their credentials.

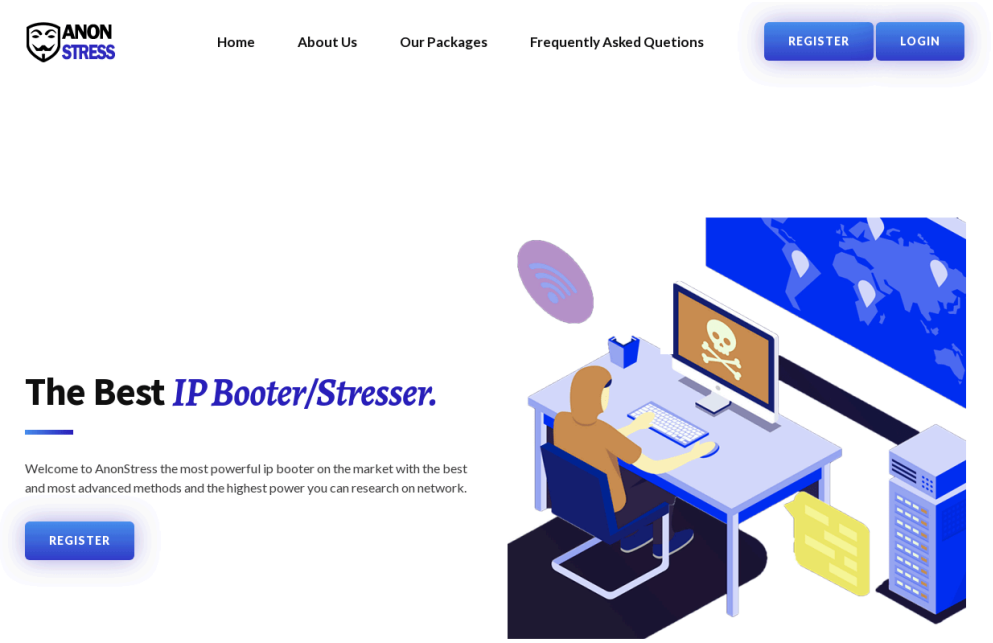
While the previously mentioned bank ones are likely targeting the banks customers, remote access services are usually for targeting employees of companies. These are the types of credentials which lead to compromise and subsequent ransomware deployment.

annydeskk.com annydessk.com any-deesk.com any-dessk.com teams-microsoft.top teams-microsotf.net teams-microstf.com

In addition to the potential credential theft, there are domains which indicate DDoS services that this threat actor might provide or were paid to register.

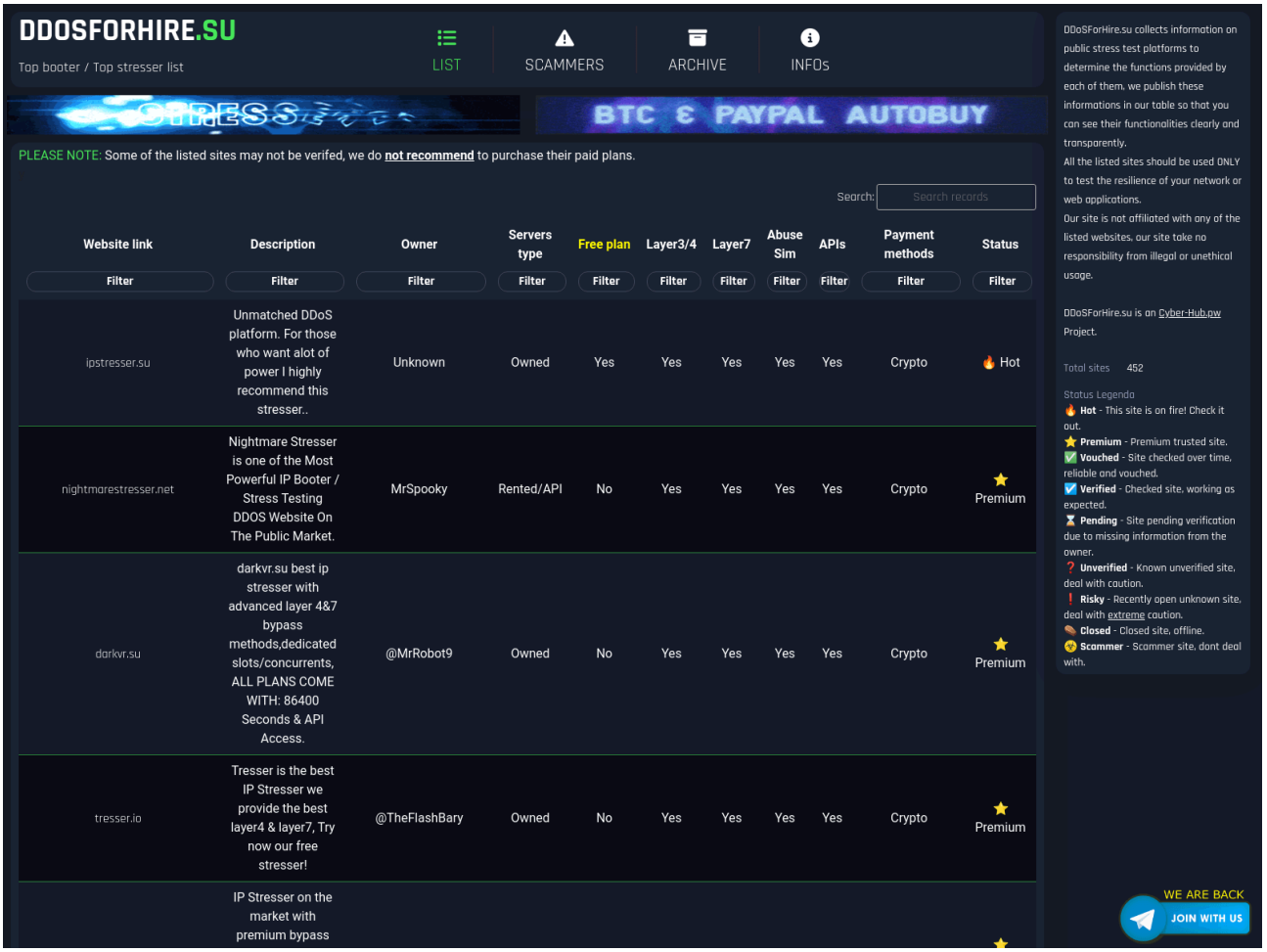
anonstress.su

->



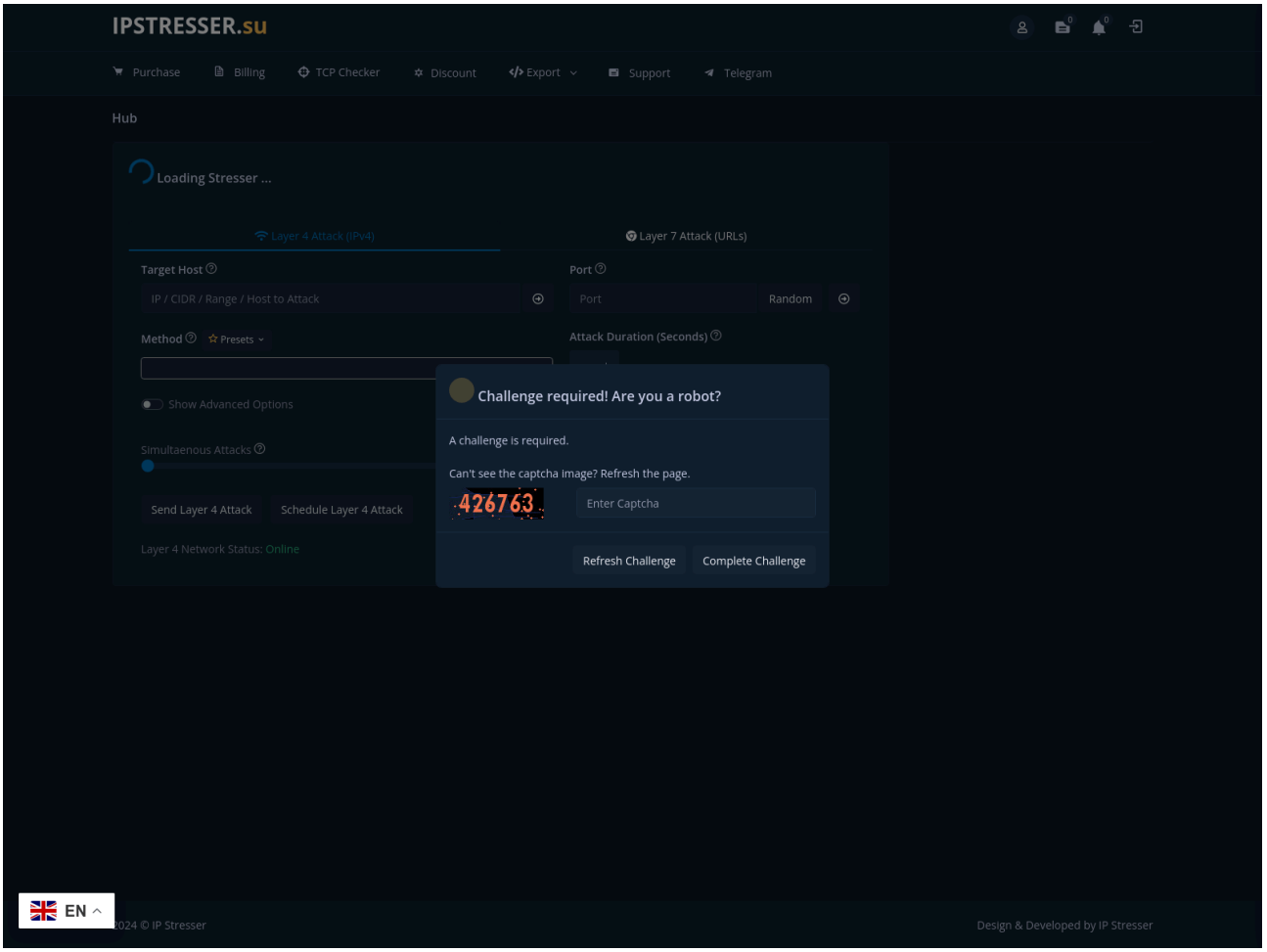
ddosforhire.su

->



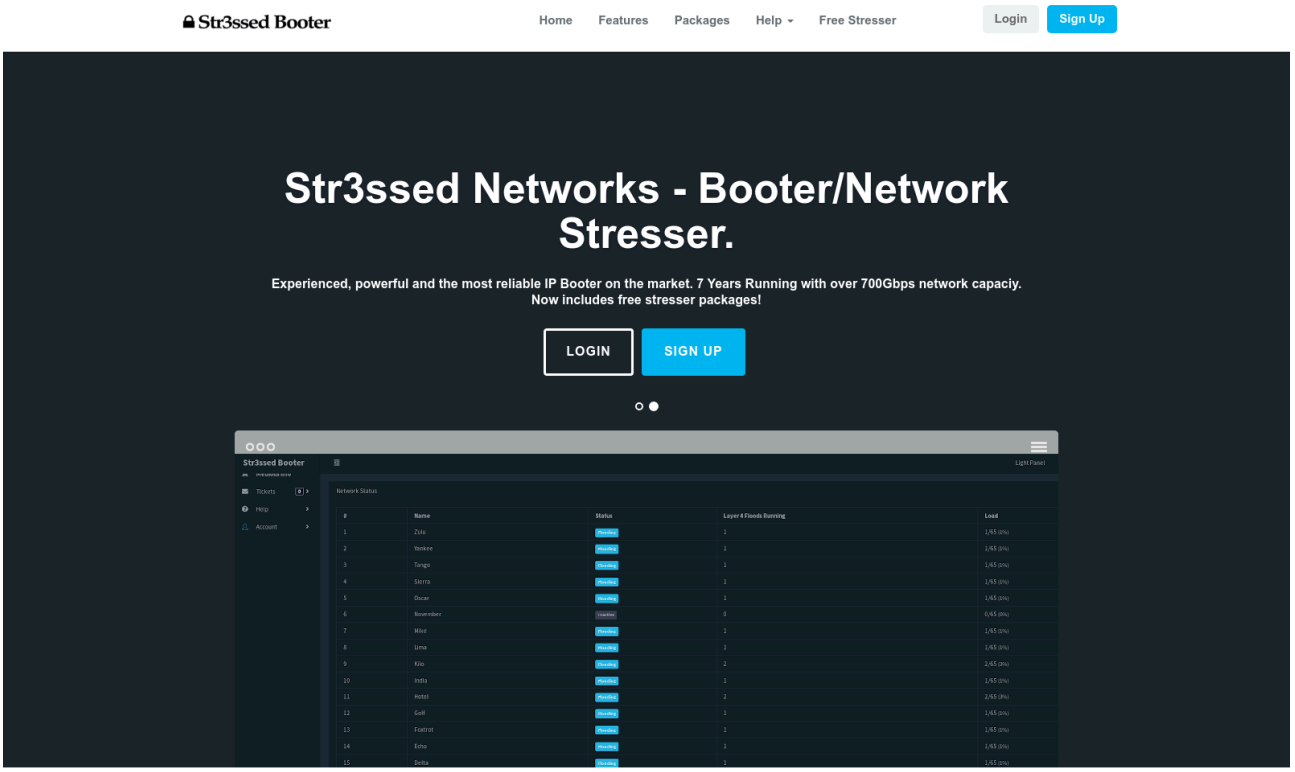
ipstresser.su

->

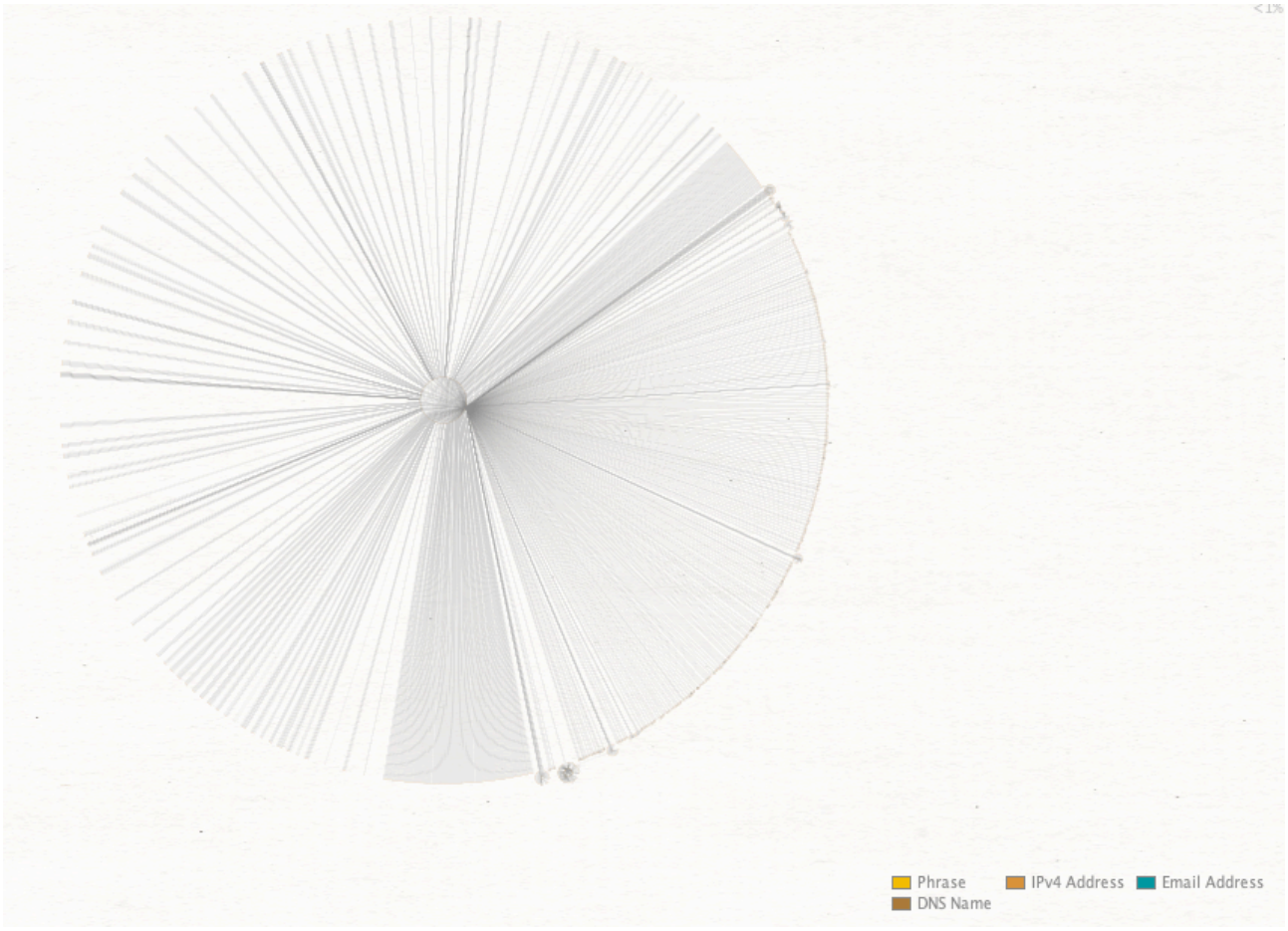

IPSTRESSER.su
Purchase
Billing
TCP Checker
Discount
Export
Support
Telegram
Hub
Loading Stresser ...
Layer 4 Attack (IPv4)
Layer 7 Attack (URLs)
Target Host
IP / CIDR / Range / Host to Attack
Port
Port
Random
Method
Presets
Attack Duration (Seconds)
Show Advanced Options
Simultaenous Attacks
Send Layer 4 Attack
Schedule Layer 4 Attack
Layer 4 Network Status: Online
Challenge required! Are you a robot?
A challenge is required.
Can't see the captcha image? Refresh the page.
426763
Enter Captcha
Refresh Challenge
Complete Challenge
EN
2024 © IP Stresser
Design & Developed by IP Stresser

str3ssed.su

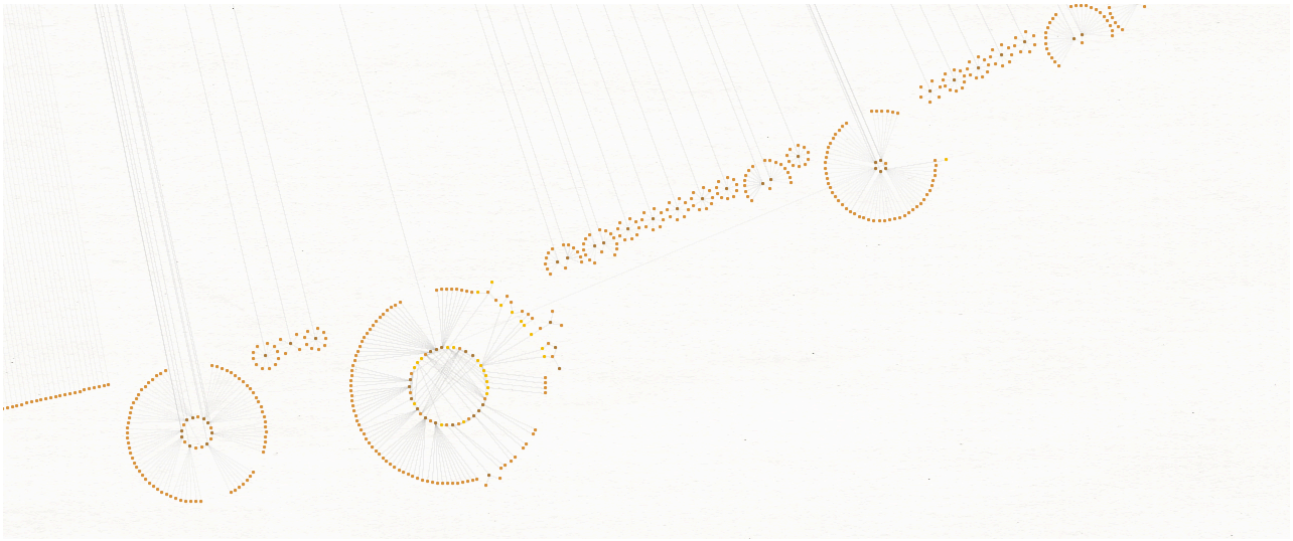
->



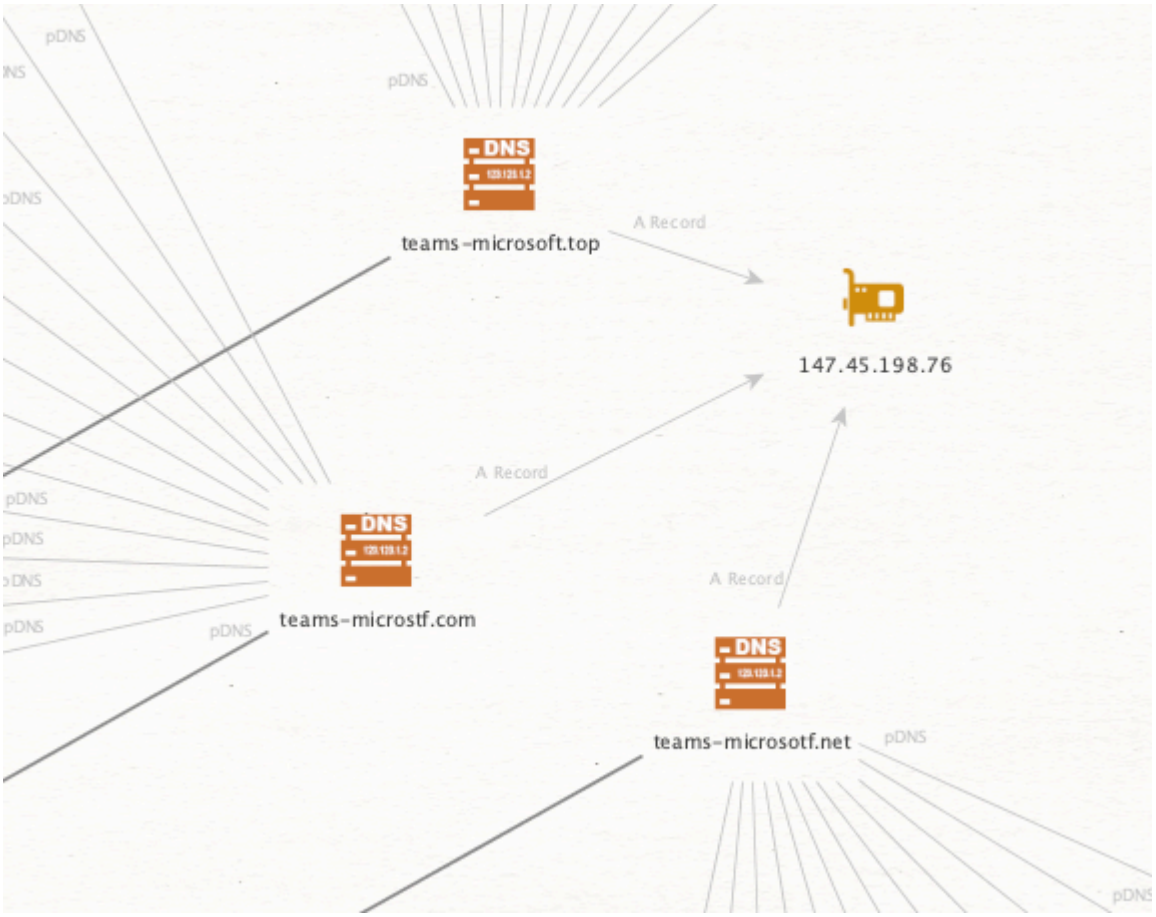
With all the domains collected, we can check them against historical resolutions and see if there are any further infrastructure overlaps that might standout. Using the initial seed list of domains from the leak and subsequent domains identified via registrant information, the next step is to pull passive DNS data for every domain. It's a sizable list of domains and the graph becomes a little intimidating when it first generates.



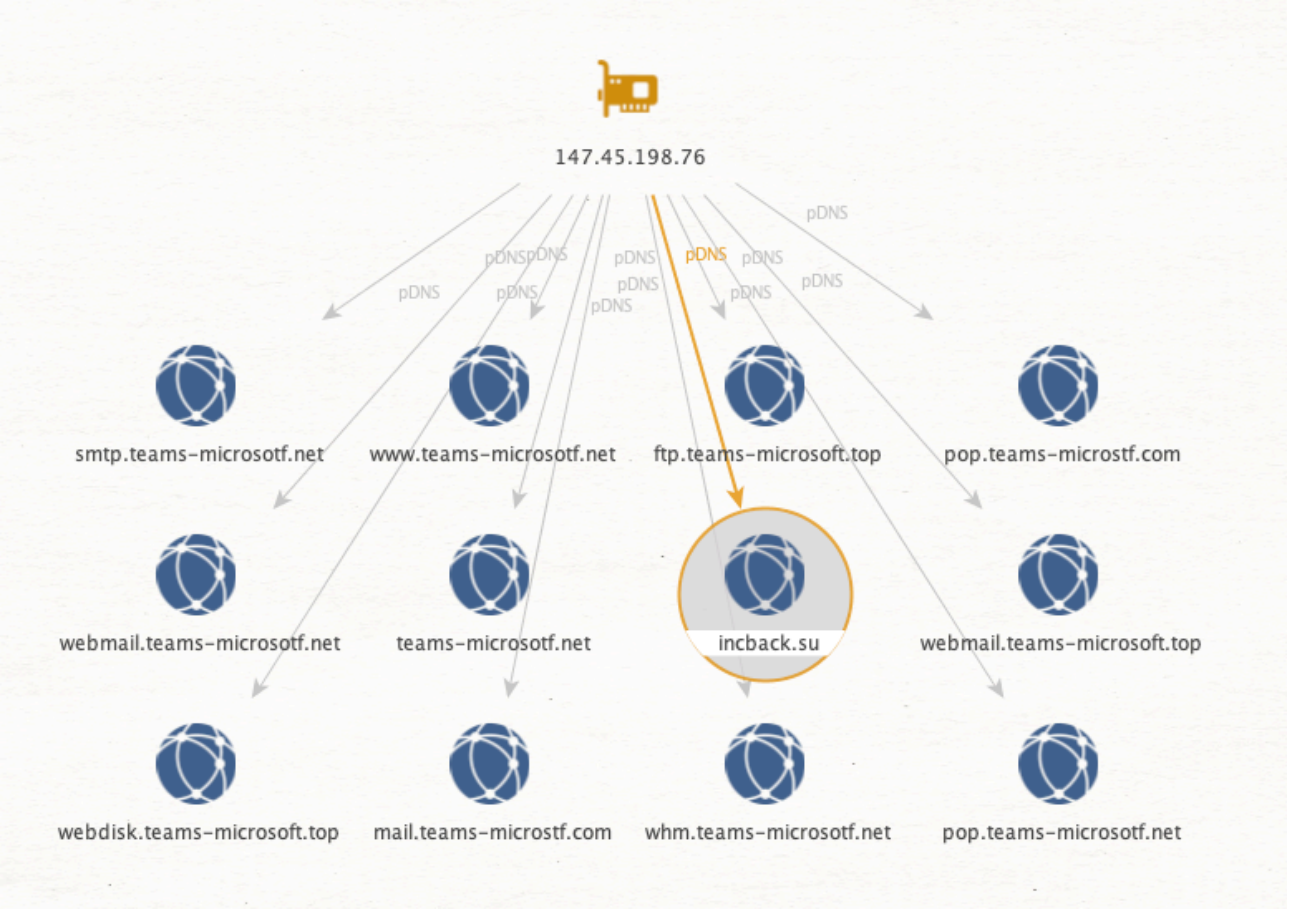
When you start to zoom in on the outer edges, clusters start to emerge.



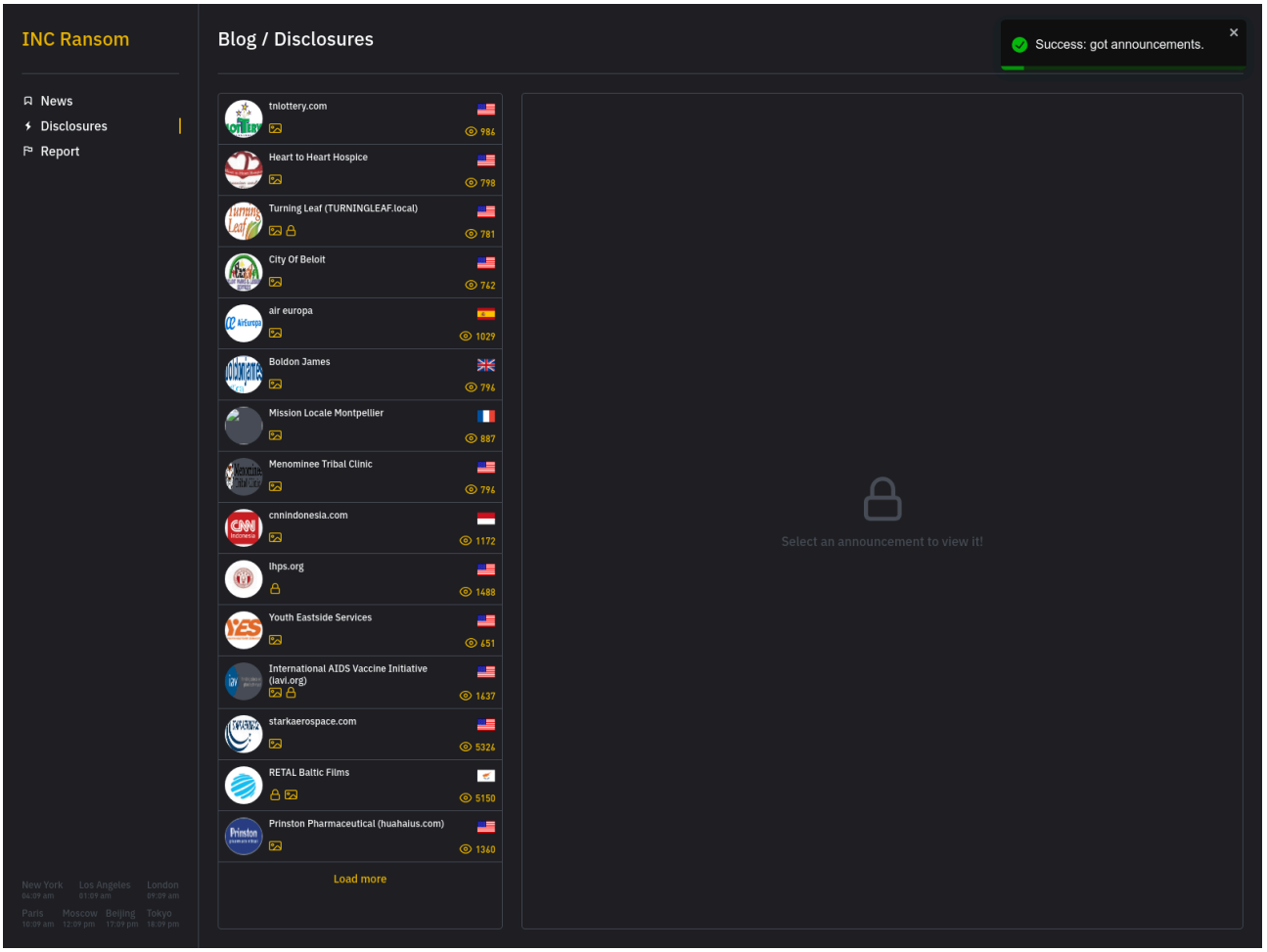
The question is how do we make sense of this or derive further value? If we presume that these registrations are possibly from an offered service *and* that those same services might be sold to other (non-Black Basta related) individuals, then seeing IP overlaps will help to identify the clusters which may be of import. Take for example this cluster of fake Microsoft Teams related pages.



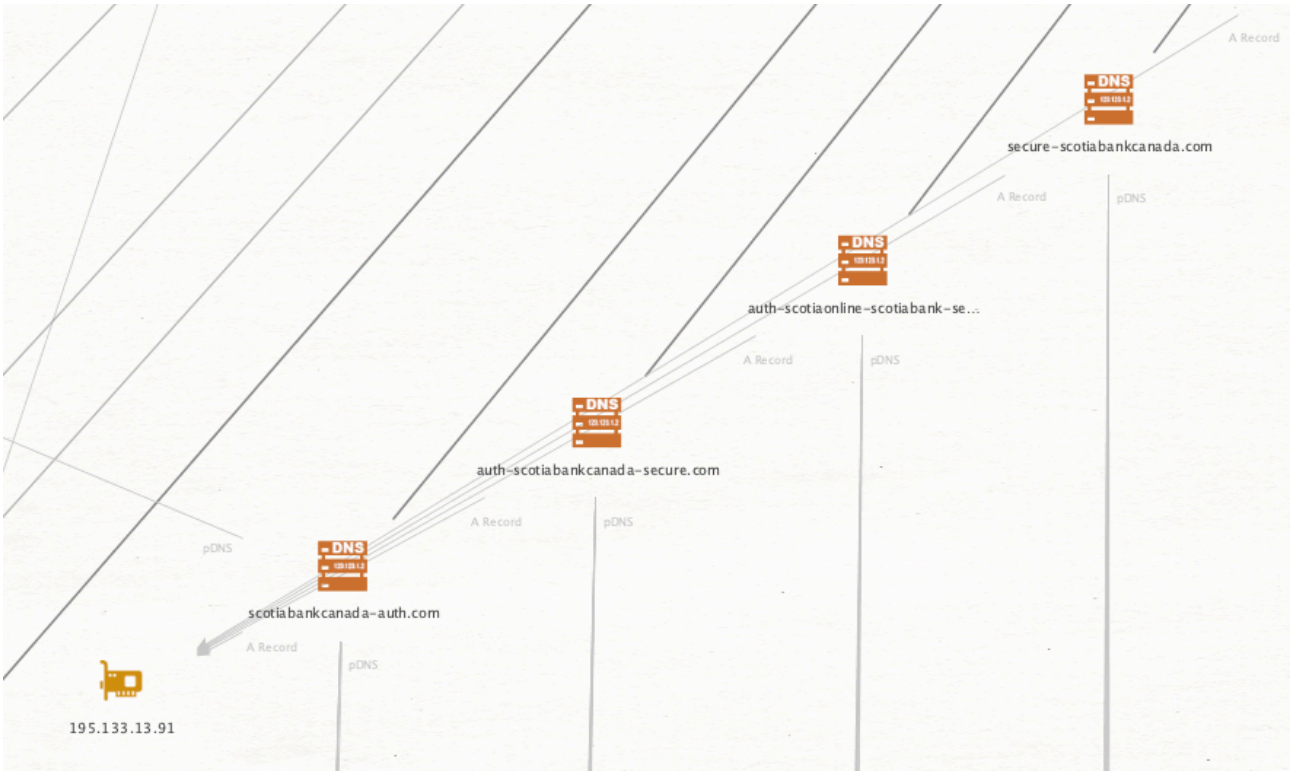
They all resolved at one point to the same singular IP. Now looking at the domains this one IP resolved to, we can spot an outlier.



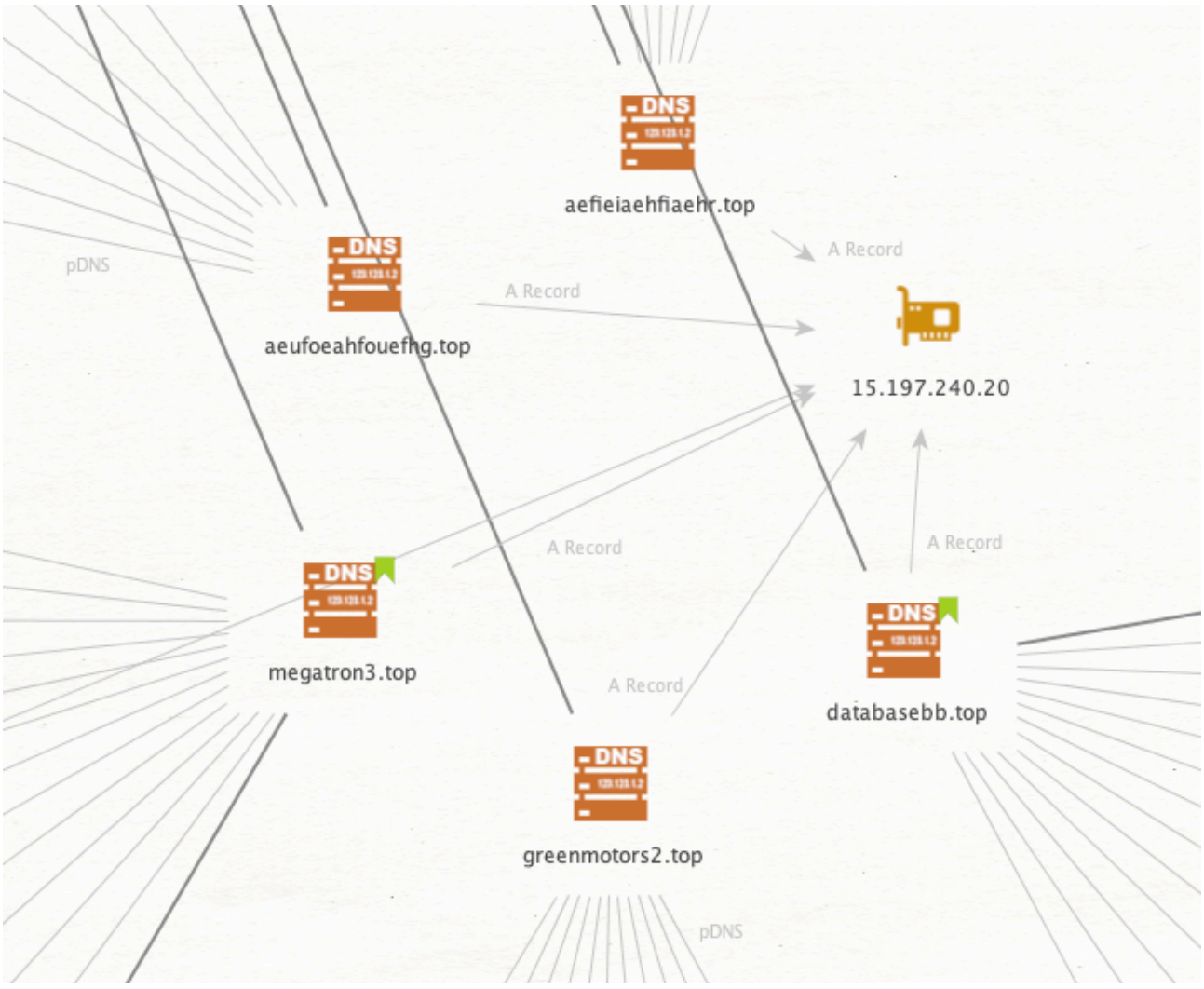
This domain appears to be for the INC Ransomware groups DLS site.



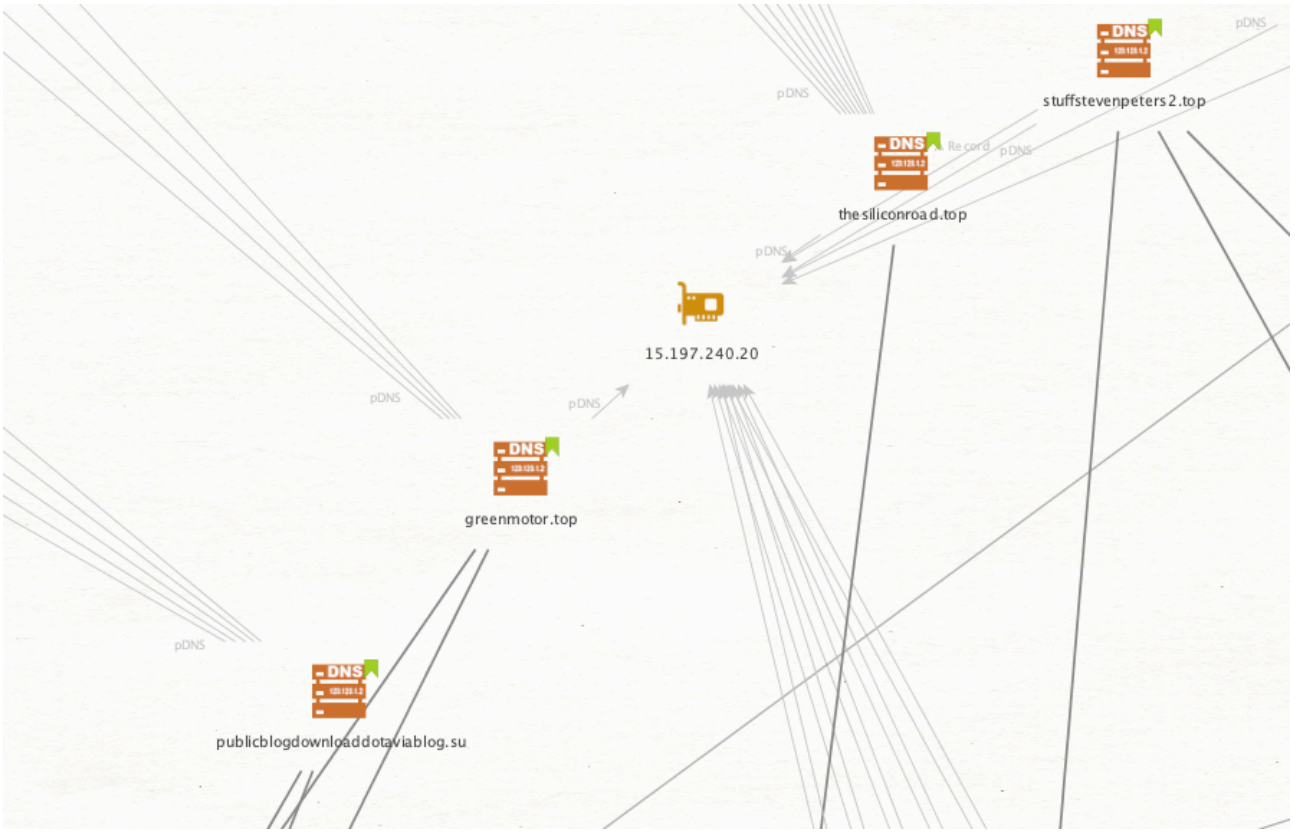
We can also identify unknown infrastructure that may be related to campaigns. In the below case, a new IP address to investigate related to the probable Canadian banking phish scams.



Focusing back to our leaked domains, we can see that 3 of the known ones resolved to "15.197.240.20" and reasonably assume "aefieiaehfiaehr.top" and "aeufoeahfouefhg.top" are related, even if not discussed in any messages.



Following this process for the core set of domains reveals that most of the infrastructure was flagged already except for that IP.



A quick check on VirusTotal relationships shows over 200 URLs and 50K communicating files. Randomly picking a few samples they all exhibited the same behavior and matched Simda Stealer YARA rules. Looking at the strings output for a few does indeed imply a stealer.

{BotVer: {Process: {Username: PROCESSOR_IDENTIFIER {Processor: {Language: %dx%d@%d {Screen: dd:MMM:yyyy {Date: HH:mm:ss {Local time: %c%d:%02d ... /login.php ... keygrab %02u.bmp ********** [/pst] GetClipboardData ... keylog.txt passwords.txt %s%u.zip ---------- Content-Disposition: form-data name="pcname" name="file" filename="report"

Whether it's related to Black Basta, or even the domain registrant, is unknown but it's yet another rabbit hole you can go down.

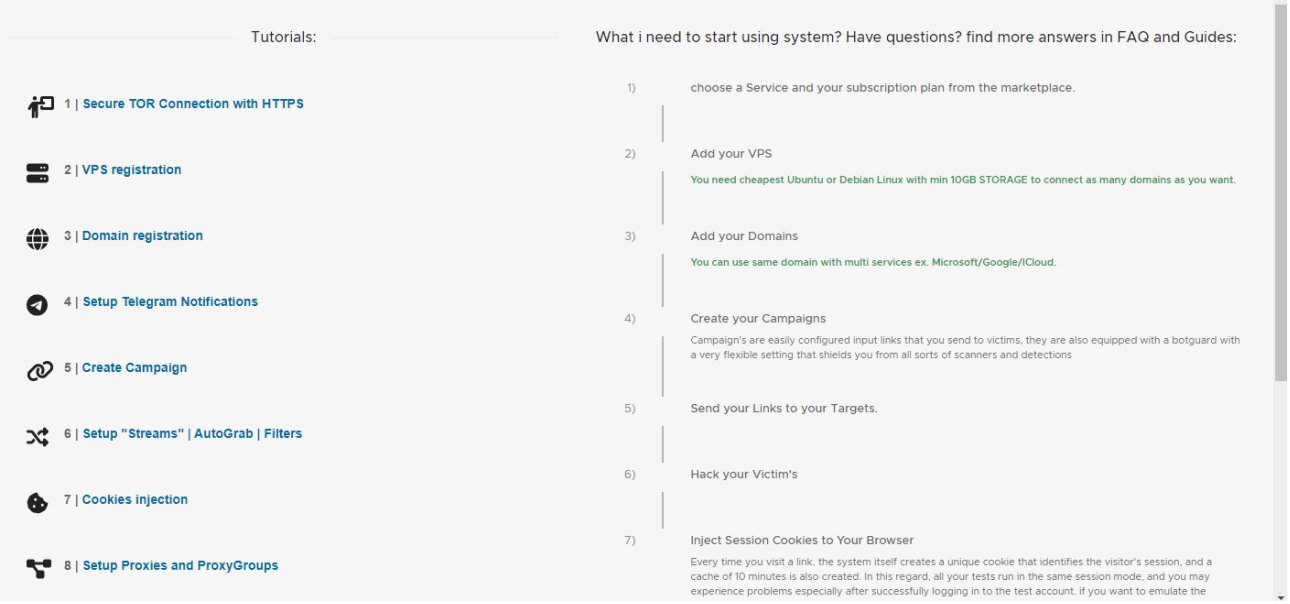
Using these leaks and pulling on even a single thread in the sea of logs is a great way to unravel malicious infrastructure and gain additional knowledge about how threat actors operate. With that, I'll concludes the pivoting from the infrastructure side of things but I would highly recommend continuing this path if the topic is of interest to you.

Bonus Content:

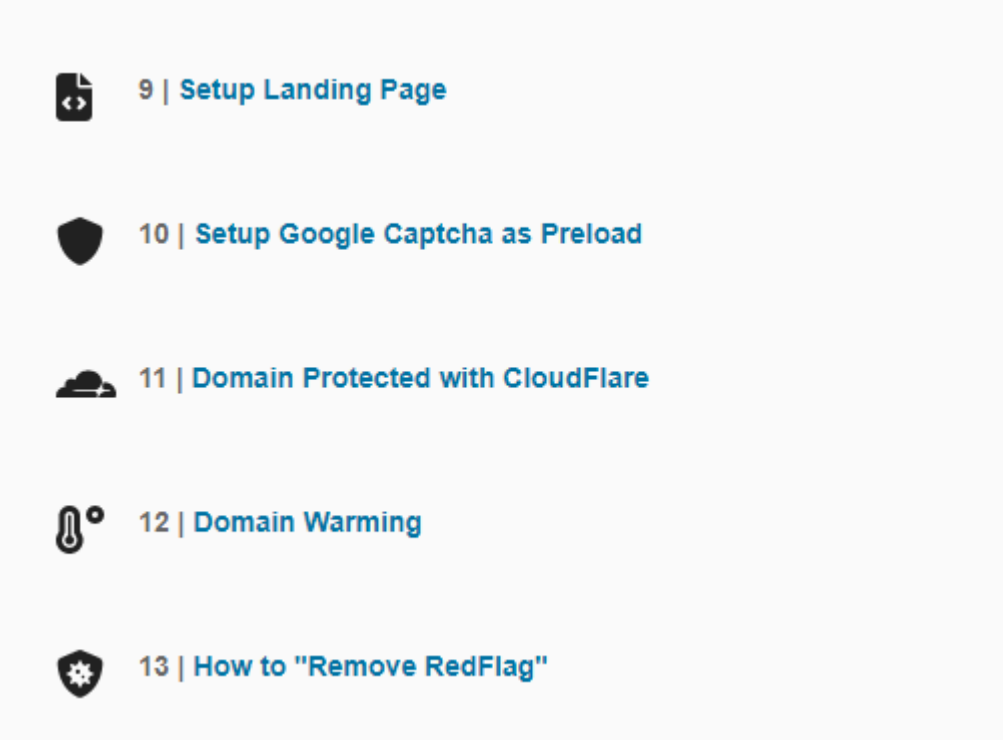
While I don't plan to write anymore on this subject, I figured I would share a handful of screenshots from some of the live infrastructure still out there. Not necessarily related to any of the above infrastructure but for other services they leveraged in their operations.

The first I stumbled on while trying to identify tutorials they kept referring to in chat messages - this lead to an EvilProxy panel site which, along with hosting many guides for affiliates, acted as a central site to manage their

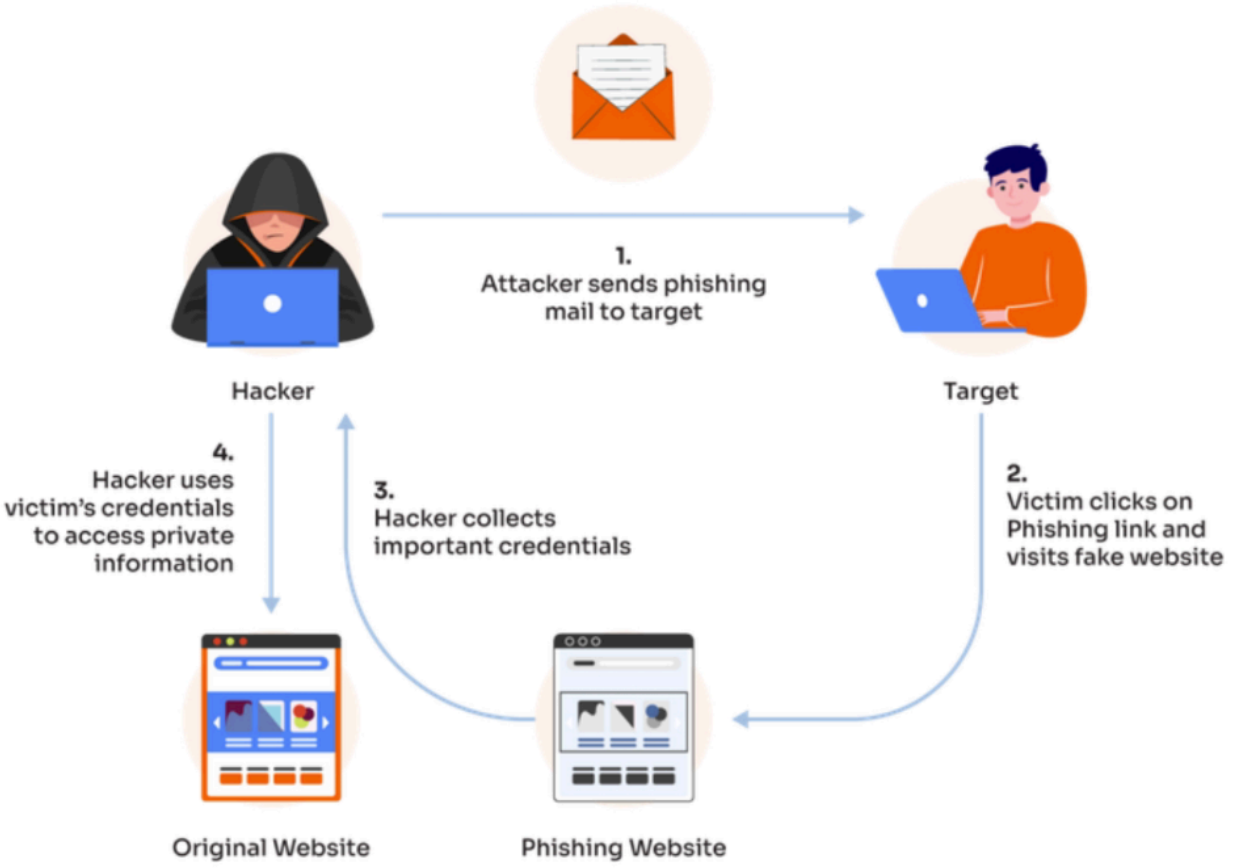
phishing infrastructure.



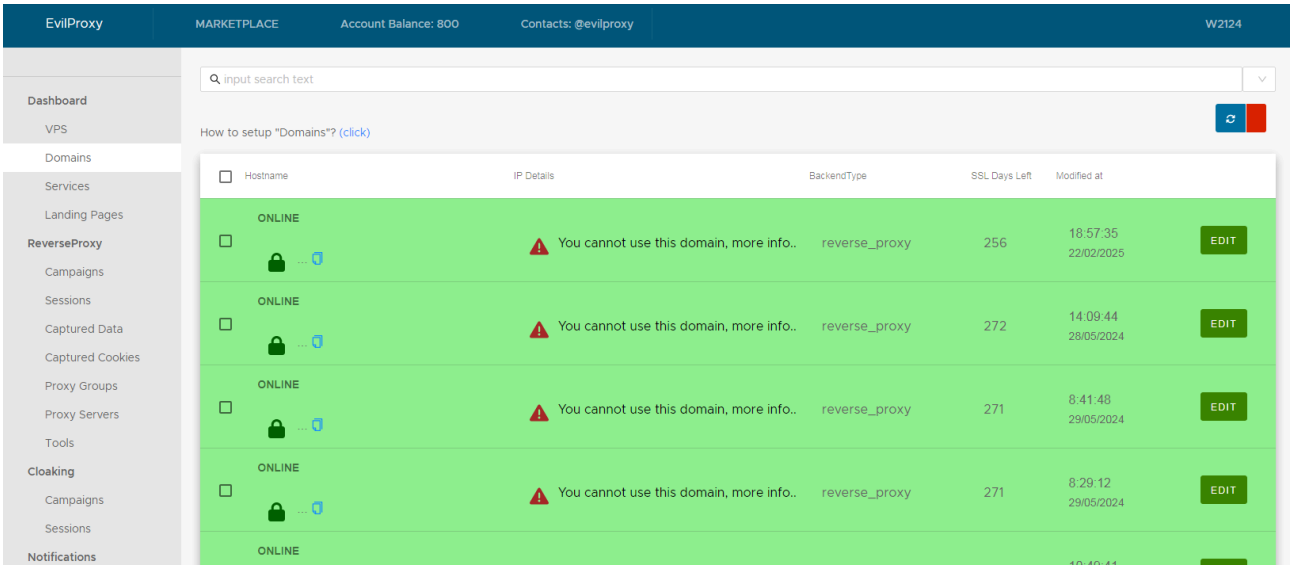
Continued...



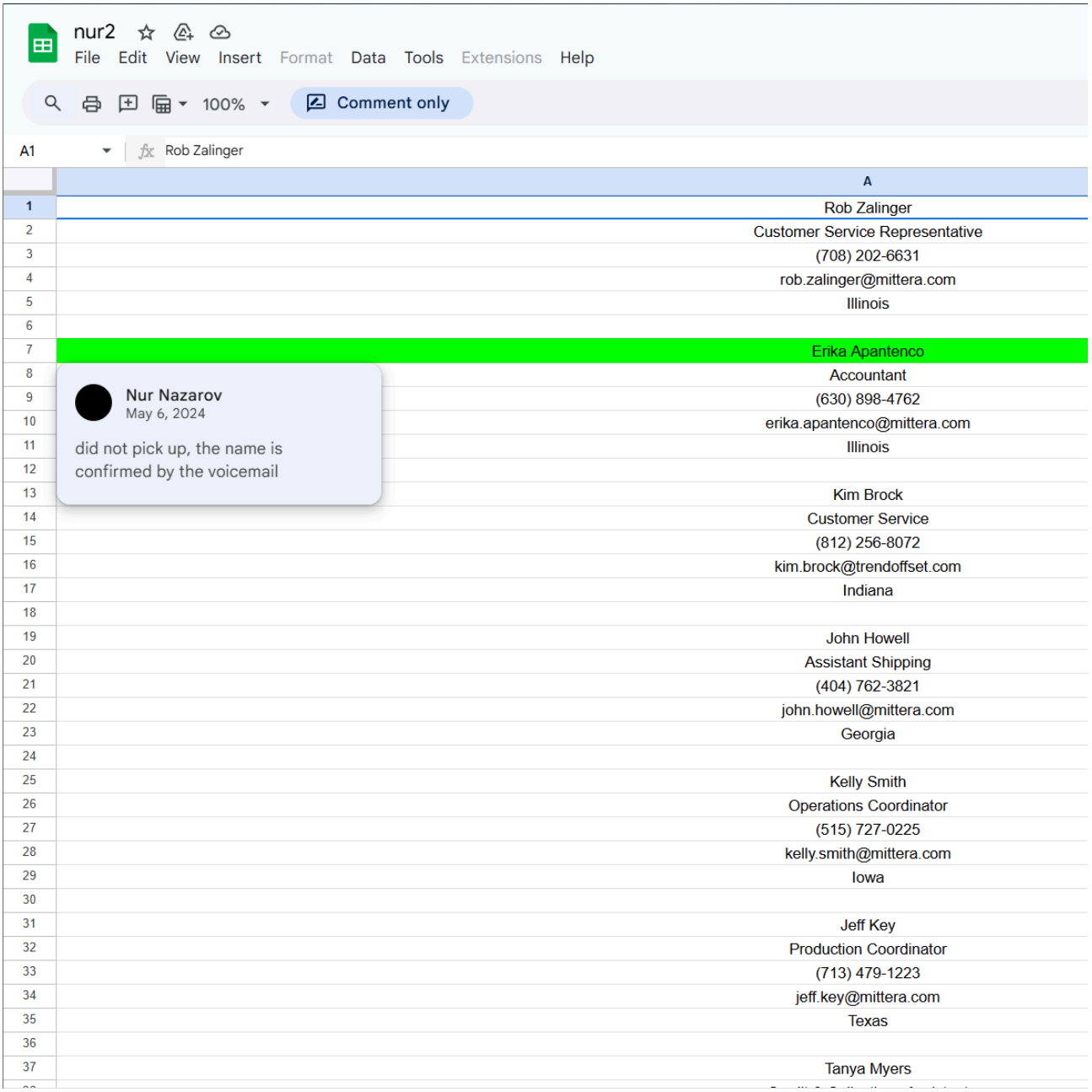
The tutorials are relatively straight forward and sometimes contain hilariously corporate looking slides.



With active proxy hosts.

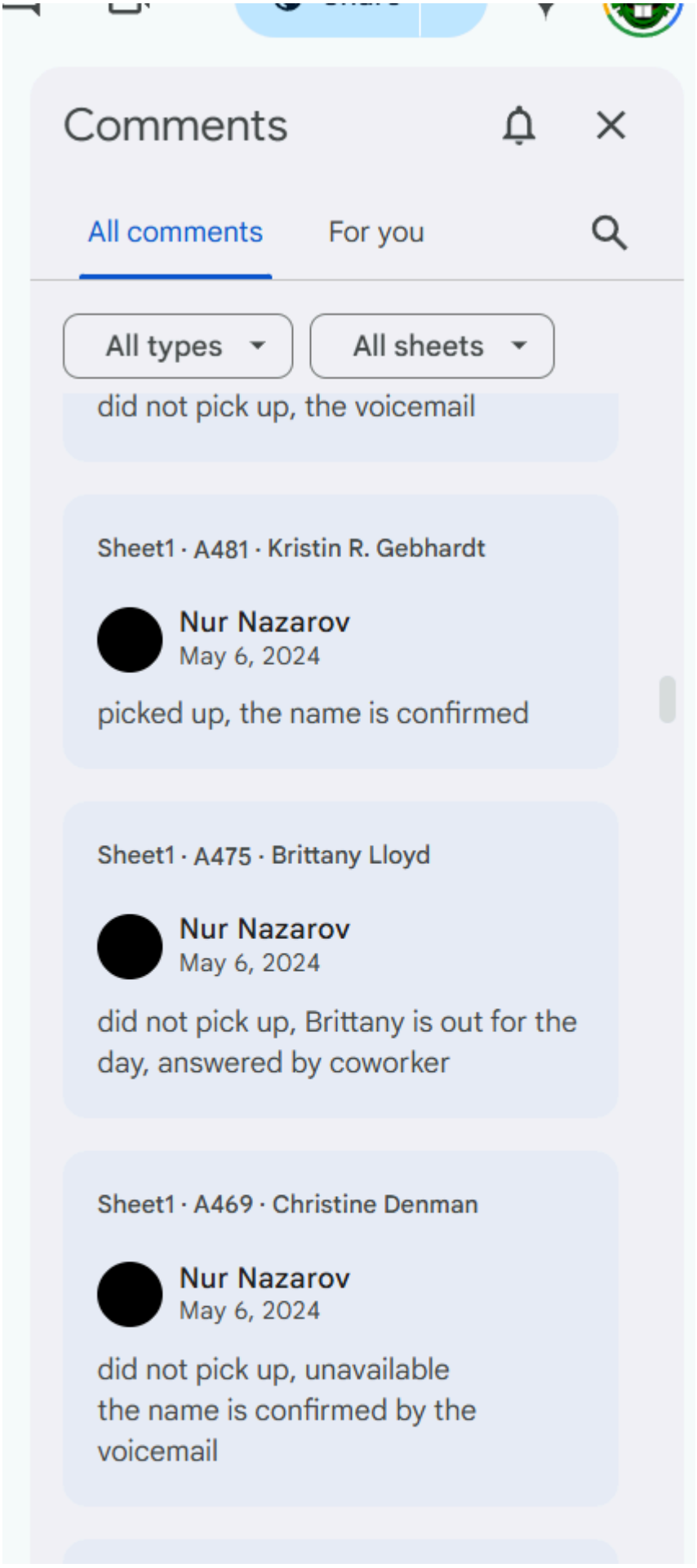


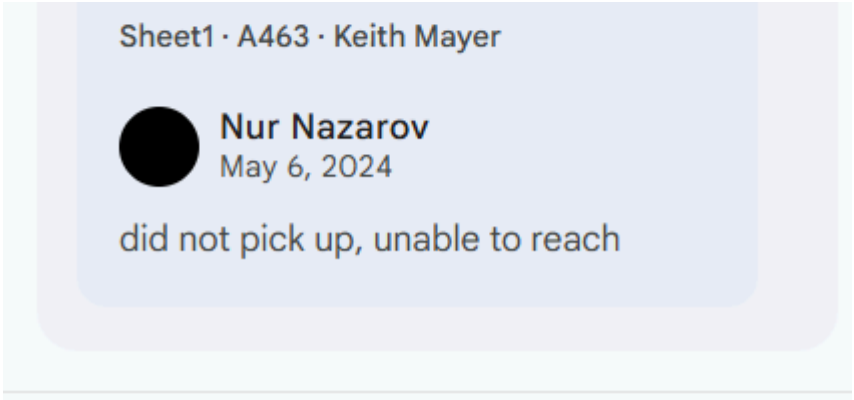
This next one was for Google docs shared in the chats which were still up, associated to an account, and used for tracking cold calls for verification of individuals.



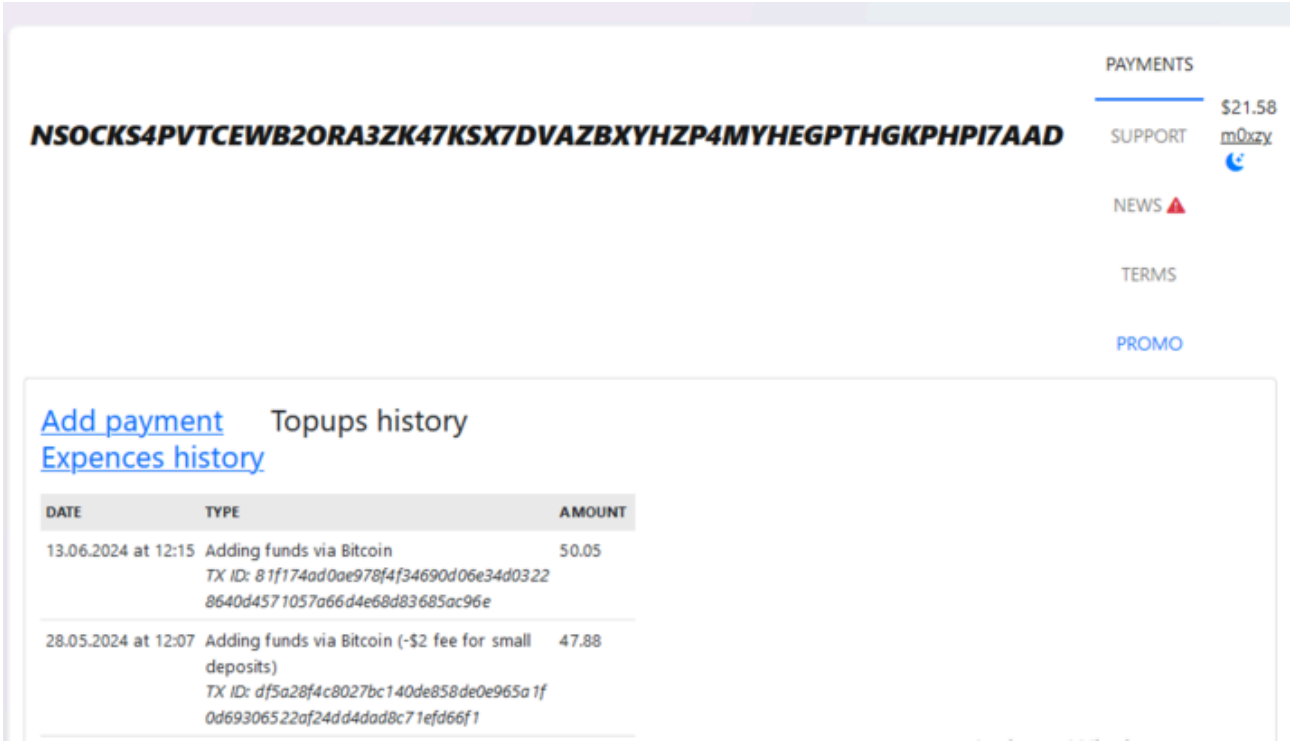
	A
1	Rob Zalinger
2	Customer Service Representative
3	(708) 202-6631
4	rob.zalinger@mittera.com
5	Illinois
6	
7	Erika Apantenco
8	Accountant
9	(630) 898-4762
10	erika.apantenco@mittera.com
11	Illinois
12	
13	Kim Brock
14	Customer Service
15	(812) 256-8072
16	kim.brock@trendoffset.com
17	Indiana
18	
19	John Howell
20	Assistant Shipping
21	(404) 762-3821
22	john.howell@mittera.com
23	Georgia
24	
25	Kelly Smith
26	Operations Coordinator
27	(515) 727-0225
28	kelly.smith@mittera.com
29	Iowa
30	
31	Jeff Key
32	Production Coordinator
33	(713) 479-1223
34	jeff.key@mittera.com
35	Texas
36	
37	Tanya Myers

Thanks Nur.

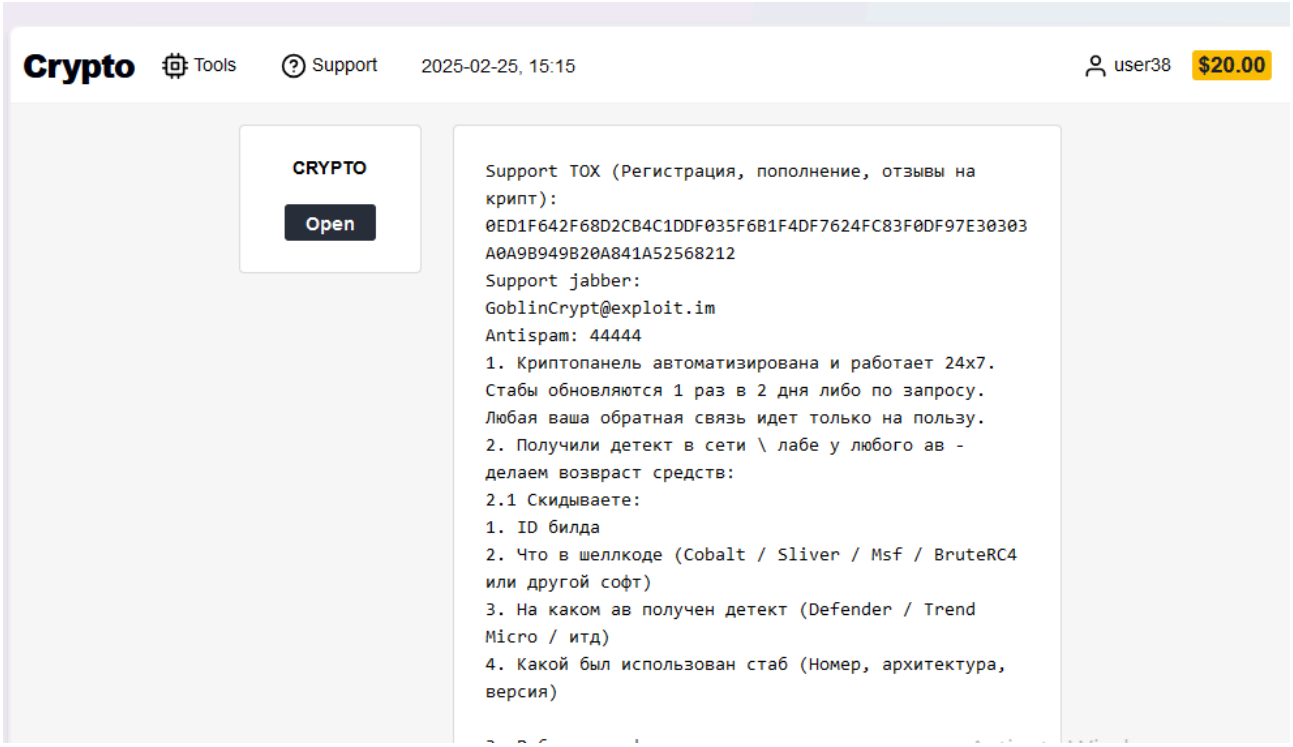

Comments
All comments
For you
All types
All sheets
did not pick up, the voicemail
Sheet1 · A481 · Kristin R. Gebhardt
Nur Nazarov
May 6, 2024
picked up, the name is confirmed
Sheet1 · A475 · Brittany Lloyd
Nur Nazarov
May 6, 2024
did not pick up, Brittany is out for the day, answered by coworker
Sheet1 · A469 · Christine Denman
Nur Nazarov
May 6, 2024
did not pick up, unavailable
the name is confirmed by the voicemail



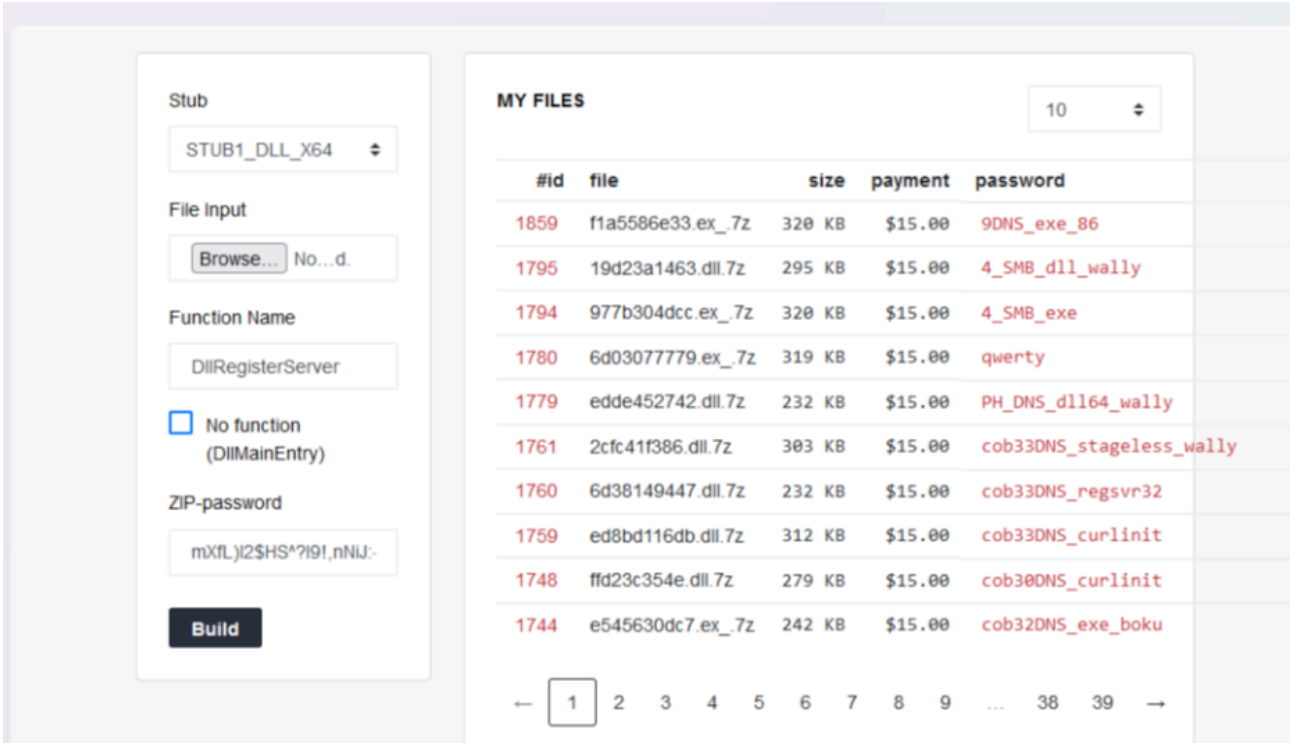
A service for purchasing and managing proxies (using the onion address for "nsocks.net").



Finally, I'll close out with some screenshots from GoblinCrypt, a service they use to generate CobaltStrike/Sliver/MSF/BR4 payloads in an attempt to avoid AV.



Payloads:



Happy hunting folks!

Older posts...
