An inside view of domain anonymization as-a-service — the BraZZZerSFF infrastructure

Benoit ANCEL · Follow
Published in CSIS TechBlog
15 min read · Aug 8, 2022

One, if not the main, challenge with producing good intelligence is to have access to the right information at the right moment. The right telemetry from the right angle helps you to detect and dig out the right signal. Sometimes, in order to obtain good telemetry, you need a bit of luck .

The story we are writing here will try to explain how, from a simple mistake made by an operator, we managed to collect and exploit a lot of precious information from a “Fast Flux” network called **BraZZZerS Fast Flux** between end of 2018 and 2022.

After sharing this data as TLP:amber with partners for years, the service now going into decline and the misconfiguration finally being fixed, we think it is now the right time to release this data and explain what can be found inside. It is a good occasion to try to fill any holes in your documentation and keep track of the technical facts about the cybercrime history.

BraZZZerS Fast Flux: Domain anonymization for all

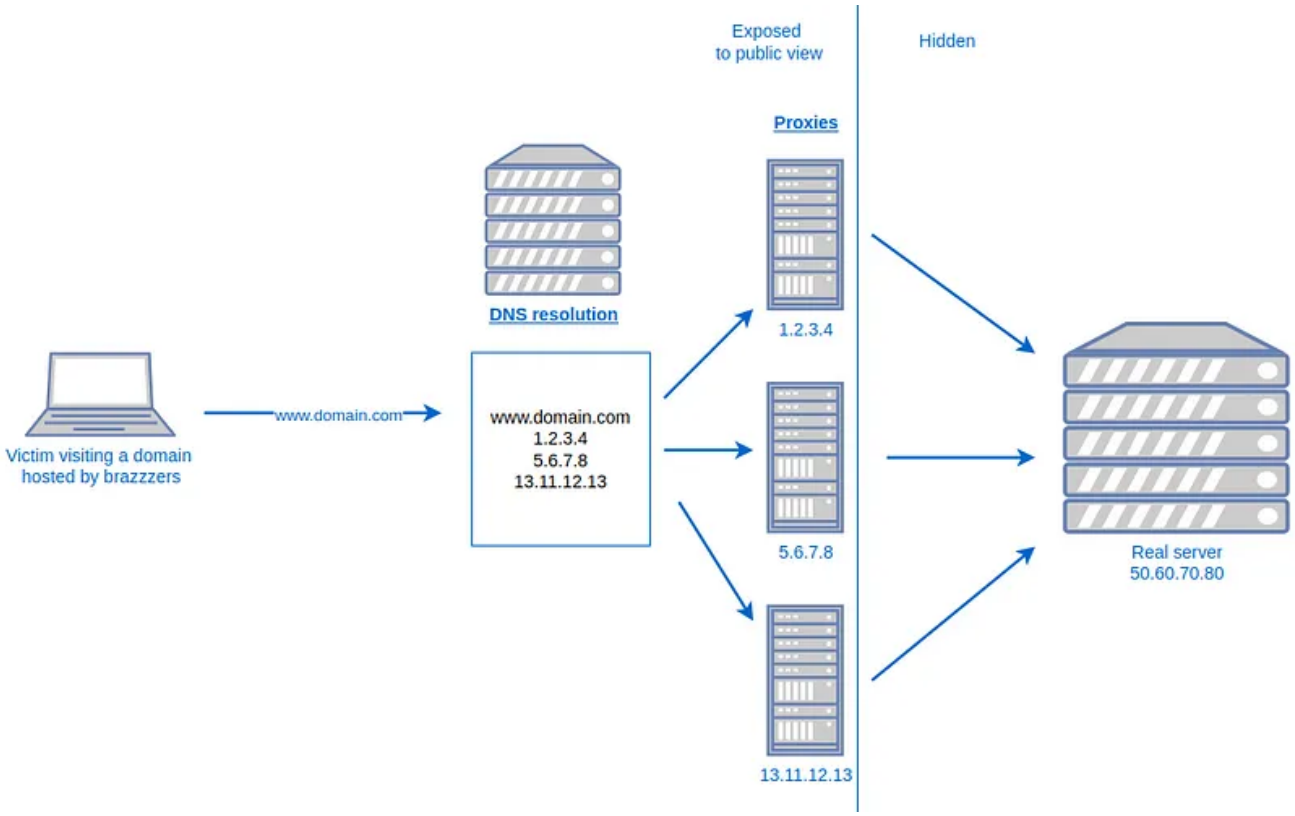
During mid-2018, we observed an actor using the nickname *BrazzzersFF* to promote a service based on a system of domain anonymization described as a fast flux:

> *Hey. We are called BraZZZers, and we know three things:*
> *1. On the Internet, millions of projects, but "locating" the server of any of them is easy — thanks to the IP-address.*
> *2. Projects are different. There are some who, for certain reasons, better hide the IP address.*
> *3. It is possible to make sure that no one knows about the real location of the server. No one — from the word "in general".*
> *For this, we have FastFlux technology, which will change your IP addresses faster than anyone can track them. We are ready to install this system on your servers and in the future to ensure that it will work as a clock. And we will do it around the clock, since we, unlike most of the services of this type, have real and professional support 24 hours a day, without holidays and weekends.*
> *We are BraZZZers. We are a group of experienced professionals, who at one time separated from another similar company in order to make the quality of our services even better. And we will make you completely invisible, elusive and impregnable.*
> *Now it is more concrete. Except actually FastFlux, we offer you a lot of additional privileges.*
> *1. Qualitative, professional round-the-clock technical support in any time zone.*
> *2. Launch services within 15 minutes after payment.*
> *3. Own control panel FastFlux:*
> *- with automation of actions and processes*
> *- with domain registrations — coming soon*
> *- with automatic billing and notifications — coming soon*
> *- with instructions for any types of records for domains (MX, etc.) — coming soon*
> *- and with a lot of other pleasant and useful bonuses, over which we are working hard.*
> *4. The tariff includes server rental, at your service:*
> *- a set of standard configurations, as well as the ability to select a server with individual parameters according to your request*
> *- constant protection from DDoS attacks*

- 24-hour monitoring and support
- Guaranteed communication channel.
5. Absolute bulletproof / fault tolerance. All systems are under round-the-clock automatic and manual monitoring of our specialists.
6. A large database of own DNS-addresses , which is constantly expanding.
7. The ability to create or configure your own DNS addresses with the required geography.
8. We are always ready to meet you and completely create FastFlux for you with your individual settings and conditions.
9. We have the highest uptime on the market. We guarantee this.
10. Support for .bit domains and SSL certificates (getting or creating your own certificate in one click).
11. You choose the traffic receiving port yourself.
12. Our technical support is quite extensive. We will be happy to set up your server, install the necessary software and help with other technical issues.
We are working to ensure that the list of our advantages is expanded and expanded. More detailed conditions we will discuss with you personally and strictly confidential.
Also, we have a keshbek system. If for some reason, for some reason, we can not provide you with the agreed services in full, you are guaranteed to get your money back. It should be remembered that the cacheback does not work in the following cases:
- If your project failed due to reasons beyond our control
- If your software is not installed for some reason (in the conditions that we have installed a predefined OS, php version, etc.)
- If you are blocked by the server after launching traffic directly, bypassing FastFlux.
Are you tired of the constant failures of the old supplier? Or do you want to receive services at a more attractive price? For us this is a matter of principle. We guarantee that we will pay you less than our competitors. In addition, we have an extremely flexible pricing policy, and we are ready to consider the individual tariff for each of your requests.
Also, we are working on improving our panel every day. Therefore, new features and capabilities will always appear.
In general, if you are looking for a reliable and optimal provider of Internet privacy services, then you are at the right address. The only nuance is we are absolutely against violence against children and animals, therefore on our servers will never be neither childish nor zoo. And in the rest — write to us and enjoy online invisibility!
P.S. If you are a reseller who is tired of the administration and imperfection of your product, we will happily take on your shoulders your cares for customers. Right now we are developing API for resellers — and you can safely work on our software under your

> *own brand. You will need a minimum deposit, and we are ready to discuss the remaining conditions individually.*

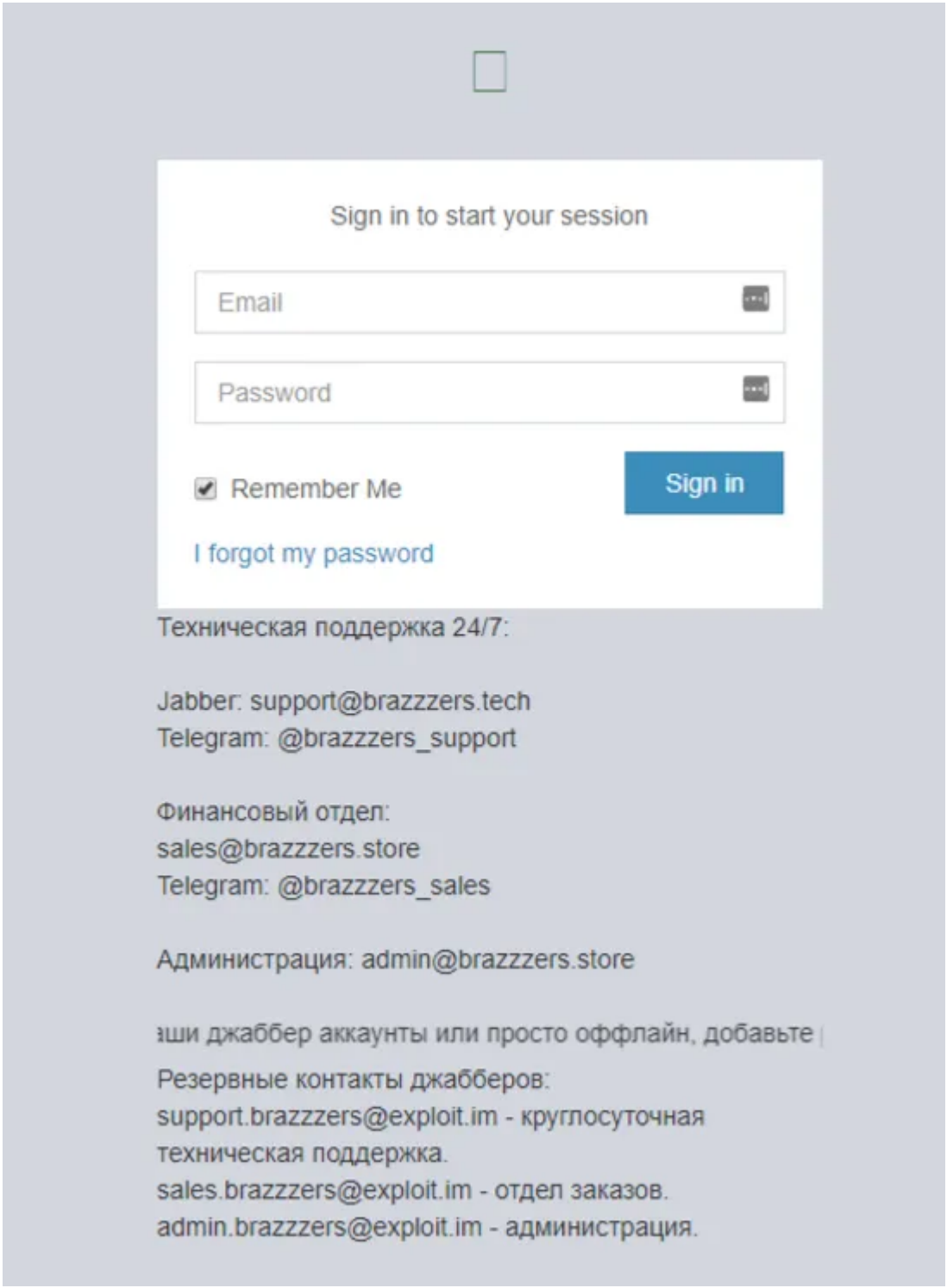
The service is described as a Fast flux but in reality it's more a simple proxy system. BraZZZers rents a pool of VPSs all around the internet and uses them as proxy IPs in order to hide the real IP of a server.



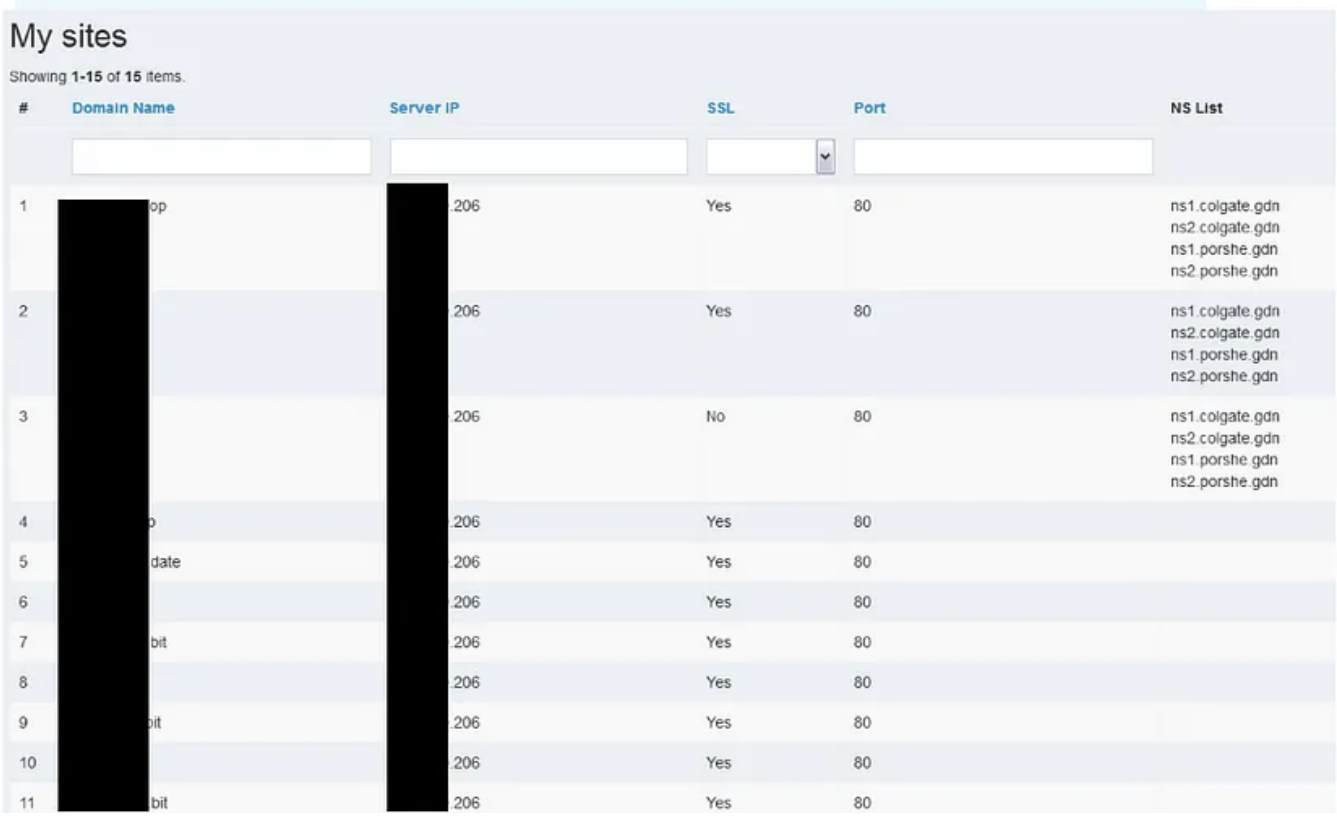
Brazzzers mechanism

The domains involved are resolving to a list of IPs, (we observed from 1 up to more than 20 IPs per domain) that are just redirecting the traffic to the real server. The abuse complaints are usually sent to the host of the IP resolving to the malicious domain but with BraZZZers each domain has backup volatile IPs and the real malicious server is protected.

In order to configure their domains, each client of BraZZZers has access to a panel where they can configure their domain records. In the early beginning, BraZZZers suggested the use of their own name servers but they ended up proposing DNSpod by default like most criminals are now doing.



BraZZZers login panel



My sites

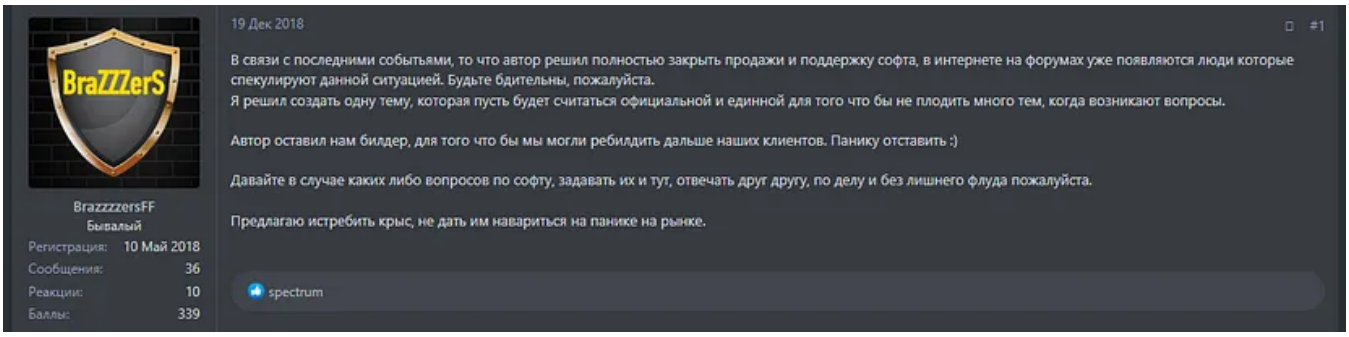
Showing **1-15** of **15** items.

#	Domain Name	Server IP	SSL	Port	NS List
1	[redacted]op	[redacted].206	Yes	80	ns1.colgate.gdn ns2.colgate.gdn ns1.porshe.gdn ns2.porshe.gdn
2	[redacted]	.206	Yes	80	ns1.colgate.gdn ns2.colgate.gdn ns1.porshe.gdn ns2.porshe.gdn
3	[redacted]	.206	No	80	ns1.colgate.gdn ns2.colgate.gdn ns1.porshe.gdn ns2.porshe.gdn
4	[redacted]o	.206	Yes	80	
5	[redacted]date	.206	Yes	80	
6	[redacted]	.206	Yes	80	
7	[redacted]bit	.206	Yes	80	
8	[redacted]	.206	Yes	80	
9	[redacted]bit	.206	Yes	80	
10	[redacted]	.206	Yes	80	
11	[redacted]bit	.206	Yes	80	

BraZZZers client panel

BraZZZers is just another domain protection service like Yalishanda or even Sandiflux/Fluxxy.

In order to find and track BraZZZers clients in the wild, we had to make sure that the fast flux we were observing was really BraZZZers and not one of the other similar services. In December 2018, an announcement made on the forum BHF helped us to understand where to look in order to find BraZZZers nodes.



> *19 Dec 2018*
> *In connection with recent events, the fact that the author decided to completely close the sale and support of software, people are already appearing on the Internet forums who speculate on this situation. Please be vigilant.*
> *I decided to create one topic, which will be considered official and unified in order not to*

> *Let's, in case of any questions about the software, ask them here, answer each other, to the point and without unnecessary flooding, please.*
>
> *I propose to exterminate the rats, to prevent them from getting rich on the panic in the market.*

At the end of 2018, the manager of the Azorult stealer gave up on the project and left a builder to the BraZZZers admins.

Similar signs came from the managers of the password stealer KPOT who where directly reselling BraZZZers with the KPOT package:

> *The price now is $ 75, but you can still buy at the old price ($ 65) in the case of buying a pre-installed KPOT on the BraZZZerS hosting. The price for everything will be $ 215 and $ 150 for each subsequent month of hosting. When buying a pre-installed version, you immediately get a ready-to-work admin and build, initially configured for a bit domain, change it if necessary. The number of pre-installed versions is limited!*

Thanks to those posts and several other intel signals (like the association to MoreneHost) we managed to attribute the correct IPs and map the BraZZZers network.

Mapping BraZZZers nodes

Mapping the BraZZZers infrastructure is actually quite simple.

The first and easiest way is to use passive DNS.

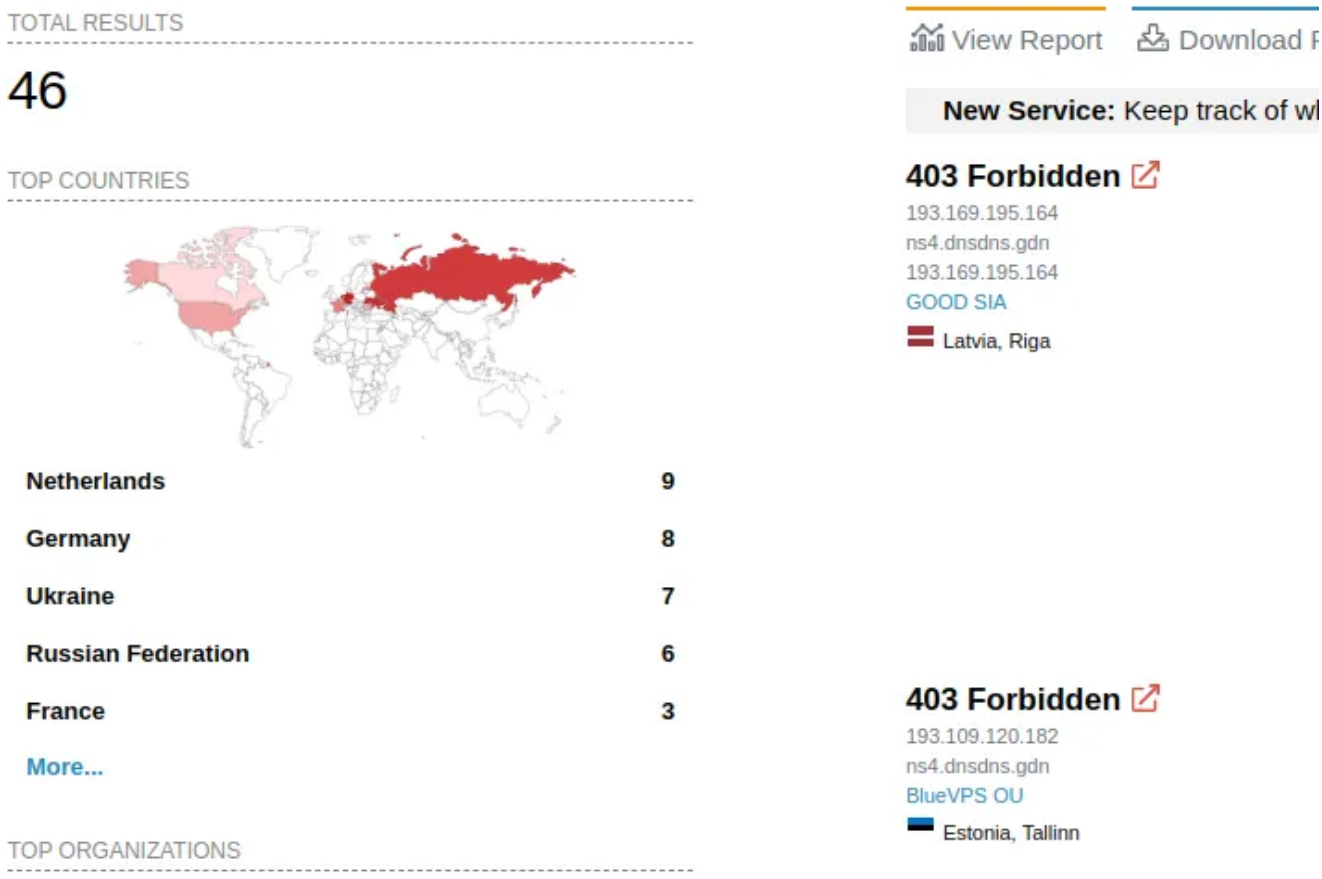
- You identify a BraZZZers customer
- You resolve their domains
- You use pDNS on the IPs (BraZZZers nodes are shared between customers)
- You pivot until covering the maximum of IPs.

However, the pDNS method has its limits for mapping infrastructure since you can only discover known DNS resolutions and must to be very careful with the time frame while pivoting in pDNS.

In the same way, we quickly observed that since 2018, BraZZZers used the same TLS certificate for its nodes:

03:21:56:e1:5c:92:6a:e6:3d:a4:c1:b6:51:54:c3:ff:cc:35

You can then use your favorite mass scan provider and look for new IPs.



We also realized that every BraZZZers node uses the hostname “ns4.dnsdns.gdns”, which makes the nodes searchable for mass scan providers and then pDNS pivot is possible.

Yet, we found an even better way to map the network. By analyzing each node of the infrastructure we discovered an interesting Nginx configuration problem.

The Nginx misconfiguration

While configuring the deployment of a new node for protecting domains, the Nginx vhost configuration was setup to disable error_log logging.

The admins edited the Nginx configuration file by setting “error_log off” where “off” should actually be **a path.** The way the virtual hosts were configured ended up writing the error_log in a file called “off” in the html directory!

http://wiki.nginx.org/CoreModule#error_log

From wiki

> Note that error_log off does not disable logging - the log will be written to a file named "off". To disable logging, you may use:
>
> `error_log /dev/null crit;`

Share Follow

answered Nov 1, 2011 at 15:59

Marcelo Bittencourt

587 ● 3 ● 10

The logs contain two types of logs. The first kind are the upstream errors:

Date	**02/09/2019 21:37**
Error	**[error] 8814#0: *31959 connect() failed (111: Connection refused) while connecting to upstream**
Client	**176.221.XX.XX**
Server	**90–43430–34–34.com**
Request	**GET / HTTP/1.1**
Upstream	**http://45.10.219.9:80/**
Host	**0–43430–34–34.com**
Referrer	**https://check-host.net/check-report/b0f5f12kdac**

The upstream error tells us:

- A client: *176.221.XX.XX*- tried to resolve *90–43430–34–34.com*
- The connection between the proxy node and the real server has failed, generating an upstream error.
- The upstream shows us that on the 2019/09/02*, the real IP of 90–43430–34–34.com was 45.10.219.9*.
- The request was generated from a referrer: https://check-host.net/check-report/b0f5f12kdac

By looking at that log we can understand that it's a request sent from a check-host account, a web service used to monitor the up-time of a domain.

The second kind is less interesting but still leak a lot of information, it's basic error_log information. Every 404 detected on the nodes (you can see a lot of mass

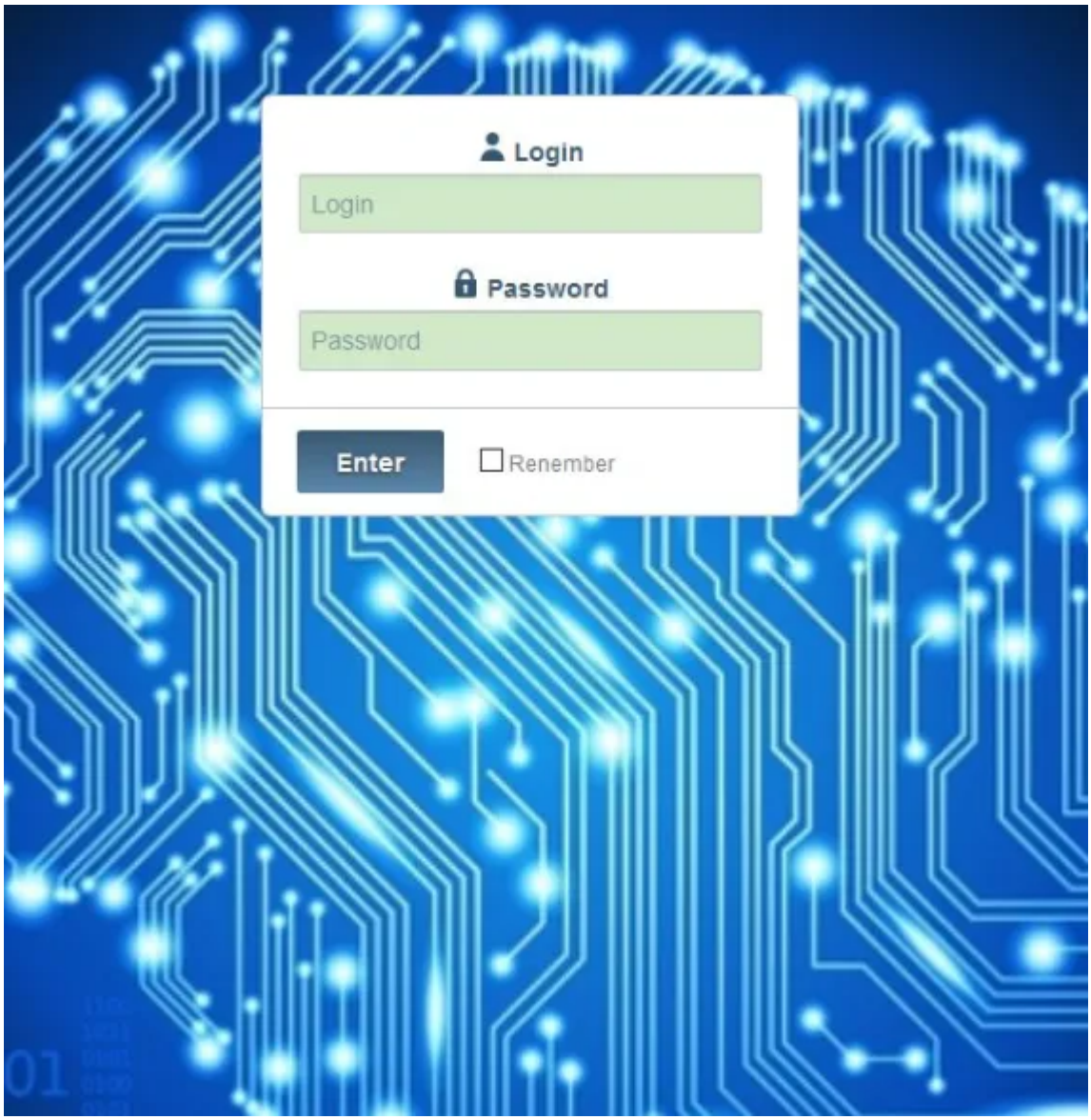
web crawlers mass scanning IPs for example). These errors are often generated when a domain is resolving to a BraZZZers node and that node doesn't have a virtual host configured for the domain. Example of log:

Date	03/09/2019 00:39
Error	[error] 13528#0: *63889 open() "/usr/share/nginx/l3k42hj56h634gkj2lk14356jk4gh23k5jl6h4/gate.php" failed (2: No such file or directory)
Client	96.57.xx.xxx
Server	dnsdns.gdn
Request	GET /l3k42hj56h634gkj2lk14356jk4gh23k5jl6h4/gate.php?ped=RTY3M0E4NjhDQ0I5JE1DLTEwNw%3D%3D
Host	tuneappservice.org

In the log we can see that:

- A client 96.57.xx.xxx
- Sent a web request "GET tuneappservice.org/l3k42hj56h634gkj2lk14356jk4gh23k5jl6h4/gate.php?ped=RTY3M0E4NjhDQ0I5JE1DLTEwNw"

We can see here what looks like a malware callback, it's in fact Riltok (Android malware). The log leaks victims information (IP and "ped") but also a web path 3k42hj56h634gkj2lk14356jk4gh23k5jl6h4/gate.php. Enough data to generate more intel.



Riltok panel

After understanding the value of that data, we quickly built different tools to store and parse those logs and just like that started a very interesting 4 years journey.

As a reminder, these logs represent a very small fraction of the BraZZZers traffic. We only catch the requests that have failed. If we compare the number of requests collected on BraZZZers with a botnet like Dreambot and the effective traffic captured on the control server, the error_logs represent less than 5% of the total traffic; but those 5% are still gold.

We will now try to describe a few use cases observable in these logs in order to demonstrate what kind of data are available.

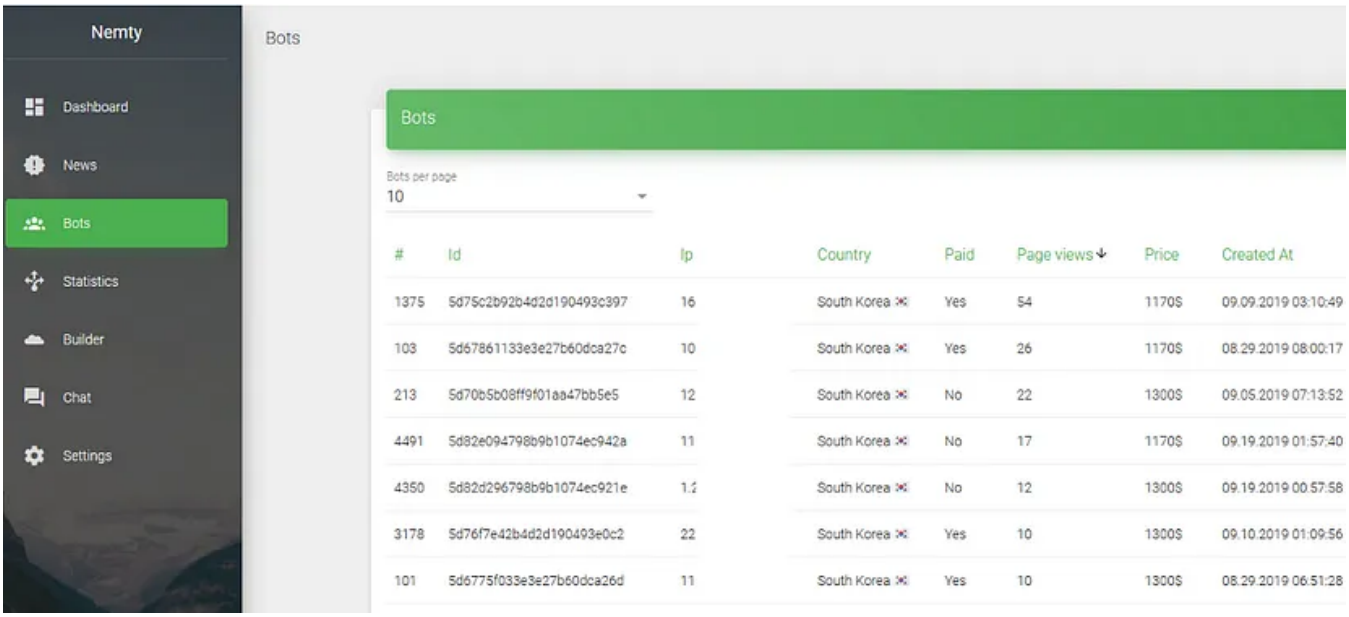
Use cases

Nemty ransomware and JWT leak

Nemty was using BraZZZers to protect its domains nemty.top and nemty.hk.

2019/09/24 15:44:18	nemty.hk	http://5.182.39.200:3000/socket.io/?token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJfaWQiOiI1ZDVjMjUxYjgyMDgwODBhMjhmMjQ0ZjIiLCJpYXQiOjE1NjkyOTY3NjZ9.hW_JHmDR3nC2iq1AdIDPWn3jCeE5frH28IRvY6sMiIY&EIO=3&transport=polling&t=MrZIni4&sid=3mZSAViiyMBu_T2nAAEP	https://nemty.hk/panel/bots/5d86676e67a11406100e2d5d
2019/09/24 15:44:17	nemty.hk	http://5.182.39.200:3000/socket.io/?token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJfaWQiOiI1ZDgxMzM4Njc5OGI5YjEwNzRlYzhlMWIiLCJpYXQiOjE1NjkzMjY0Mzd9.HD5PCr-0-iuJg-wQSTeeV9WzMEOhwGwKZw7l4cgYxCc&EIO=3&transport=polling&t=MrZDcEy	https://nemty.hk/panel/news
2019/09/24 15:44:06	nemty.hk	http://5.182.39.200:3000/socket.io/?fileid=undefined&EIO=3&transport=polling&t=MrZIl7O	
2019/09/24 15:44:05	nemty.hk	http://5.182.39.200:3000/socket.io/?token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJfaWQiOiI1ZDgxMzM4Njc5OGI5YjEwNzRlYzhlMWIiLCJpYXQiOjE1NjkzMjY0Mzd9.HD5PCr-0-iuJg-wQSTeeV9WzMEOhwGwKZw7l4cgYxCc&EIO=3&transport=polling&t=MrZDW8K	https://nemty.hk/panel/news
2019/09/24 15:44:01	nemty.hk	http://5.182.39.200:3000/socket.io/?fileid=undefined&EIO=3&transport=polling&t=MrZItu9	https://nemty.hk/
2019/09/24 15:44:00	nemty.hk	http://5.182.39.200:3000/socket.io/?token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJfaWQiOiI1ZDVlY2U3NGZiN2E0YjBlZTBiNTc2MDciLCJpYXQiOjE1NjkzMTg3NjN9.-9Gj_IQkwH5d8wv2XRI73CpxoxkxIG4MRYwyOleeo98&EIO=3&transport=polling&t=MrZI-2S&sid=s12-9GKyzSICOTkeAAEX	https://nemty.hk/panel/news

The logs showed us that the Nemty's web panel was based (until the last year of Nemty's life) on socket.io. The polling service was leaking very important information on a GET request: the JWT token. By reusing that token in a cookie, you could access the Nemty's panel authenticated as the user related to the token:



By observing Nemty's requests, we can easily analyze which IPs are contacting the admin panel section and then start an intel operation against the threat actors.

Date	Client	Request
2019/10/15 18:04:15	109.7	nemty.hk/socket.io/?fileid=undefined&EIO=3&transport=websocket&sid=JZC2jA3bTwhcseJWAB-F
2019/10/15 18:04:14	162.2	nemty.hk/socket.io/?fileid=undefined&EIO=3&transport=polling&t=MtFyCPu&sid=JZC2jA3bTwhcseJWAB-F
2019/10/15 18:04:13	195.1	nemty.hk/socket.io/?token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJfaWQiOiI1ZDVlY2U3NGZiN2E0YjBlZTBiNTc2MDciLCJpYXQiOjE1NzEwOTM2ODB9.fSoxQ-534R2jzYrlBzk5FXhVQbguGKkweKdZiTo2EWg&EIO=3&transport=polling&t=MtFyCSK&sid=8P96pRMKdU1ROKaKAB9-
2019/10/15 18:04:10	104.2	nemty.hk/api/bots/dashboard
2019/10/15 18:04:00	104.2	nemty.hk/api/bots/dashboard
2019/10/15 18:03:46	46.1	nemty.hk/socket.io/?fileid=undefined&EIO=3&transport=polling&t=MtFy5nZ&sid=Jlu3X_n8S3FewQxhAB-A
2019/10/15 18:03:43	195.1	nemty.hk/socket.io/?token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJfaWQiOiI1ZDVlY2U3NGZiN2E0YjBlZTBiNTc2MDciLCJpYXQiOjE1NzEwOTM2ODB9.fSoxQ-534R2jzYrlBzk5FXhVQbguGKkweKdZiTo2EWg&EIO=3&transport=polling&t=MtFy57I&sid=8P96pRMKdU1ROKaKAB9-

A simple config mistake from BraZZZers ended up compromising the whole operation. Like most of the other clients of BraZZZers, Nemty trusted the service to hide their backend and didn't take any extra precaution to hide the real IP from the BraZZZers network.

The hidden panel of Azorult

The leaked BraZZZers logs has been particularly handy with the Azorult stealer. In order to protect the webpanel of Azorult, the developers of the stealer forced the installation of the webpanel into a web directory with a random name (I.E. domain.com/fsebkjfxbefxdrhvbrghjkvb/admin.php)

This random name makes it theoretically impossible for anybody to guess the webpanel URL.

When the Azorult project was abandoned, the malware was still very active in the wild and omnipresent around BraZZZers infrastructure.

2020/12/26 10:32:21	morgenhyergen.xyz	http://5.182.39.4:80/vccxxs22/vdasaaa222.php?page=reports	
2020/07/03 22:22:33	mmakaronagre.xyz	http://5.182.39.4:80/asdaxgh423/asdnbgn32.php?page=reports	http://mmakaronagre.xyz/asdaxgh423/asdnbgn32.php?page=home
2020/07/03 22:20:30	mmakaronagre.xyz	http://5.182.39.4:80/asdaxgh423/asdnbgn32.php?page=reports	http://mmakaronagre.xyz/asdaxgh423/asdnbgn32.php?page=home
2020/07/03 22:09:02	mmakaronagre.xyz	http://5.182.39.4:80/asdaxgh423/asdnbgn32.php?page=reports	http://mmakaronagre.xyz/asdaxgh423/asdnbgn32.php?status=0&datefrom=2020-07-03&dateup=&search=&cookiesearch=paypal.%3A3&countries=us&nocountries=&inc_il=1&page=reports
2020/07/03 22:07:51	wildberriesqa.xyz	http://5.182.39.4:80/bfsdcx451/fhdfv234.php?datefrom=&dateup=&search=&cookiesearch=&countries=&nocountries=&page=reports	http://wildberriesqa.xyz/bfsdcx451/fhdfv234.php?page=reports
2020/07/03 22:07:44	wildberriesqa.xyz	http://5.182.39.4:80/bfsdcx451/fhdfv234.php?page=reports	http://wildberriesqa.xyz/bfsdcx451/fhdfv234.php?page=home
2020/07/03 22:01:12	wildberriesqa.xyz	http://5.182.39.4:80/bfsdcx451/fhdfv234.php?page=reports	http://wildberriesqa.xyz/bfsdcx451/fhdfv234.php?page=home
2020/07/03 22:00:59	mmakaronagre.xyz	http://5.182.39.4:80/asdaxgh423/asdnbgn32.php?page=reports	http://mmakaronagre.xyz/asdaxgh423/asdnbgn32.php?page=home

Thanks to the logs, you can now follow every hidden panel and filter every request sent to the admin panel php pages in order to collect threat actor information.

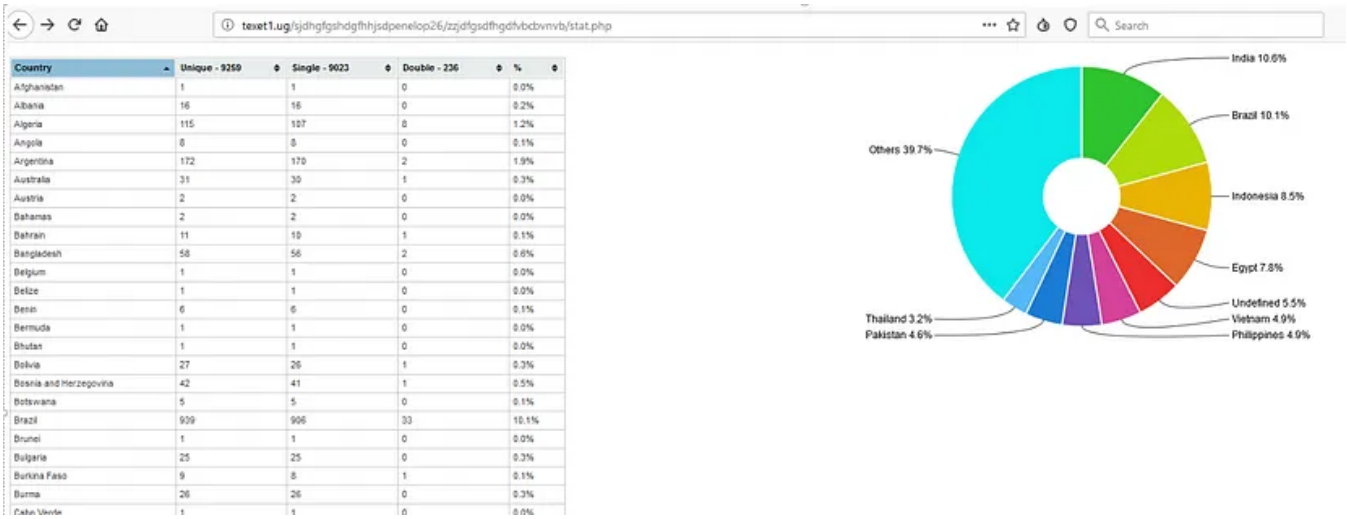
The hidden panel / random directory name trick is very popular among malware developer and BraZZZers helped us a lot to collect precious intel.

DJVU/STOP ransomware

Another example of client of BraZZZers leaking its panel was DJVU/STOP ransomware:

Date	Domain	Upstream
2019/07/11 21:55:33	bronze2.hk	http://91.243.83.127:80/tesptc/penelop/updatewin1.exe
2019/07/11 21:54:53	bronze2.hk	http://91.243.83.127:80/tesptc/penelop/3.exe
2019/07/11 21:54:53	bronze2.hk	http://91.243.83.127:80/tesptc/penelop/4.exe
2019/07/11 21:54:53	bronze2.hk	http://91.243.83.127:80/tesptc/penelop/updatewin.exe
2019/07/11 21:53:11	bronze2.hk	http://91.243.83.127:80/tesptc/penelop/5.exe
2019/07/08 21:09:33	texet2.ug	http://91.243.83.127:80/tesptc/penelop/5.exe
2019/07/08 21:09:33	texet2.ug	http://91.243.83.127:80/tesptc/penelop/updatewin.exe
2019/07/08 21:09:33	texet2.ug	http://91.243.83.127:80/tesptc/penelop/updatewin2.exe
2019/07/08 21:09:33	texet2.ug	http://91.243.83.127:80/tesptc/penelop/updatewin1.exe
2019/07/08 21:07:57	texet1.ug	http://91.243.83.151:80/sjdhgfgshdgfhhjsdpenelop26/zzjdfgsdfhgdfvbcbvnvb/get.php?pid=4B5ED3C9D83F37B03384E418DBEBD767
2019/07/08 21:07:52	texet1.ug	http://91.243.83.151:80/sjdhgfgshdgfhhjsdpenelop26/zzjdfgsdfhgdfvbcbvnvb/get.php?pid=4B5ED3C9D83F37B03384E418DBEBD767
2019/07/08 21:07:47	texet1.ug	http://91.243.83.151:80/sjdhgfgshdgfhhjsdpenelop26/zzjdfgsdfhgdfvbcbvnvb/get.php?pid=4B5ED3C9D83F37B03384E418DBEBD767
2019/07/08 21:07:42	texet1.ug	http://91.243.83.151:80/sjdhgfgshdgfhhjsdpenelop26/zzjdfgsdfhgdfvbcbvnvb/get.php?pid=4B5ED3C9D83F37B03384E418DBEBD767
2019/07/08 21:07:21	texet2.ug	http://91.243.83.127:80/tesptc/penelop/updatewin2.exe
2019/07/08 21:07:16	texet2.ug	http://91.243.83.127:80/tesptc/penelop/5.exe

The logs leaked the hidden web panel “sjdhgfgshdgfhhjsdpenelop26” giving us access to an affiliates panel:



Country	Unique - 9259	Single - 9023	Double - 236	%
Afghanistan	1	1	0	0.0%
Albania	16	16	0	0.2%
Algeria	115	107	8	1.2%
Angola	8	8	0	0.1%
Argentina	172	170	2	1.9%
Australia	31	30	1	0.3%
Austria	2	2	0	0.0%
Bahamas	2	2	0	0.0%
Bahrain	11	10	1	0.1%
Bangladesh	58	56	2	0.6%
Belgium	1	1	0	0.0%
Belize	1	1	0	0.0%
Benin	6	6	0	0.1%
Bermuda	1	1	0	0.0%
Bhutan	1	1	0	0.0%
Bolivia	27	26	1	0.3%
Bosnia and Herzegovina	42	41	1	0.5%
Botswana	5	5	0	0.1%
Brazil	939	906	33	10.1%
Brunei	1	1	0	0.0%
Bulgaria	25	25	0	0.3%
Burkina Faso	9	8	1	0.1%
Burma	26	26	0	0.3%
Cabo Verde	1	1	0	0.0%

Some developers also used a password in a GET request to display the login form of the panel. The interesting Coalabot was doing this years ago, and again BraZZZers compromised them.

2019/01/13 13:16:33	esek412782.com	http://91.243.82.44:80/new/login?k=vDDyKKNo0jaNNK6p
2019/01/13 13:07:28	esek412782.com	http://91.243.82.44:80/new/login?k=vDDyKKNo0jaNNK6p
2019/01/13 12:54:38	esek412782.com	http://91.243.82.44:80/new/login?k=vDDyKKNo0jaNNK6p
2019/01/04 15:59:07	goldchainsblue.com	http://91.243.82.44:80/new/login?k=9OGSf1gFSn7yBPxz
2018/12/11 05:32:06	esek412782.com	http://91.243.82.44:80/new/login?k=OjuNvD2uyun4OBYt

ISFB

One of the most interesting clients of BraZZZers is for sure ISFB. We observed several branches of ISFB using BraZZZers to hide its domains, the most active branch was Dreambot. The BraZZZers proxies were responsible for huge damage to the Dreambot setup.

First, the upstream logs of course leaked the control panel IPs:

2018/12/06 08:29:23	anti-doping.at	http://46.17.96.3:80/images/wH3coQXFrfl_2BA_/2BSen_2BWYTJiAw/wGQJJHBleoVsi3USjk/YEvcVei93/uafOSFcSowwVRxDdJo69/Xq1_2FqA44emD7AMCII/WpObUDEdTeNrkbN4piBhcH/2aKyA1RUC1D3t/rYrzadZI/UmvGc4OSoB2T6Vt7n2AQPXU/bH3potyzqr/Mnf1ttkFqUqZiWH8e/xAdI4yAQo8j1/A7erkLfu_2FKV/C4FVkdad/U.bmp
2018/12/06 07:55:12	anti-doping.at	http://46.17.96.3:80/images/LgTwkNsxWaTfBL89CLDpkz/6Tuw7hStQDt2Z/5rNAxv2B/HAQRkrMUaS_2BnJqoTC56ZG/1De7l2W_2B/9McWxvKAyLaYYNhoT/k3HyLh3blrU_/2BKLVdFdxq4/LnBinhfr_2FiBA/jtuQK7AfwefTj_2FcvIni/3FIuVa0f3asm0u_2/FvJ0OZNfvslclxa/1hQOeMVQeugaw12BDj/n9ooccMNe/rZ7R9P6X/5uIkLNaF/7.bmp
2018/12/06 07:50:35	anti-doping.at	http://46.17.96.3:80/images/bYKIhchV89Yqu/7giJBg8v/73dVC_2FuM5nzRuGp3AX77Y/IkrfzX912h/C_2BoucvhaiMxXHhw/t8_2FVH0ZsLh/djxR_2BHD3o/qwAPfb_2BMy9sO/V9C0fvHGdtnbZwSnkvefT/ZLHPLknf3B6CY9ms/3w90zVXLdBWB_2B/_2BgOG7L35wW79ukVw/B8zgg_2Fx/Ylp9W7xa4N/QPrtT3ycd/Si.gif
2018/12/06 01:23:09	twithoutforsyntaxformat.online	http://85.25.246.28:80/images/r4sdK8CH03IWfcz/NMQaVOz7G1QQsOSEEv/nNVcdVPET/QTNFGjLPTPsCvUf4MQvK/LZiZWTRqT7YQTjOq9vL/s1NYxuRjmZoUAWB0_2FCX3/hz7RYRgd8R5oW/mqmQOtJM/whpXWrHVM0GoXcsaGMkgD2D/AMHvWaU4Nv/cybUnl3B0zIsVqAoh/j_2FUpNE9SOu/UrUGUEWZlad/L5OhCUe2XRzO/Lw55VAkR/V.bmp

Requests like this were very typical for ISFB bots. With Dreambot, the port 80 of the control server was reserved for the bots and the port 3000 for the panel.

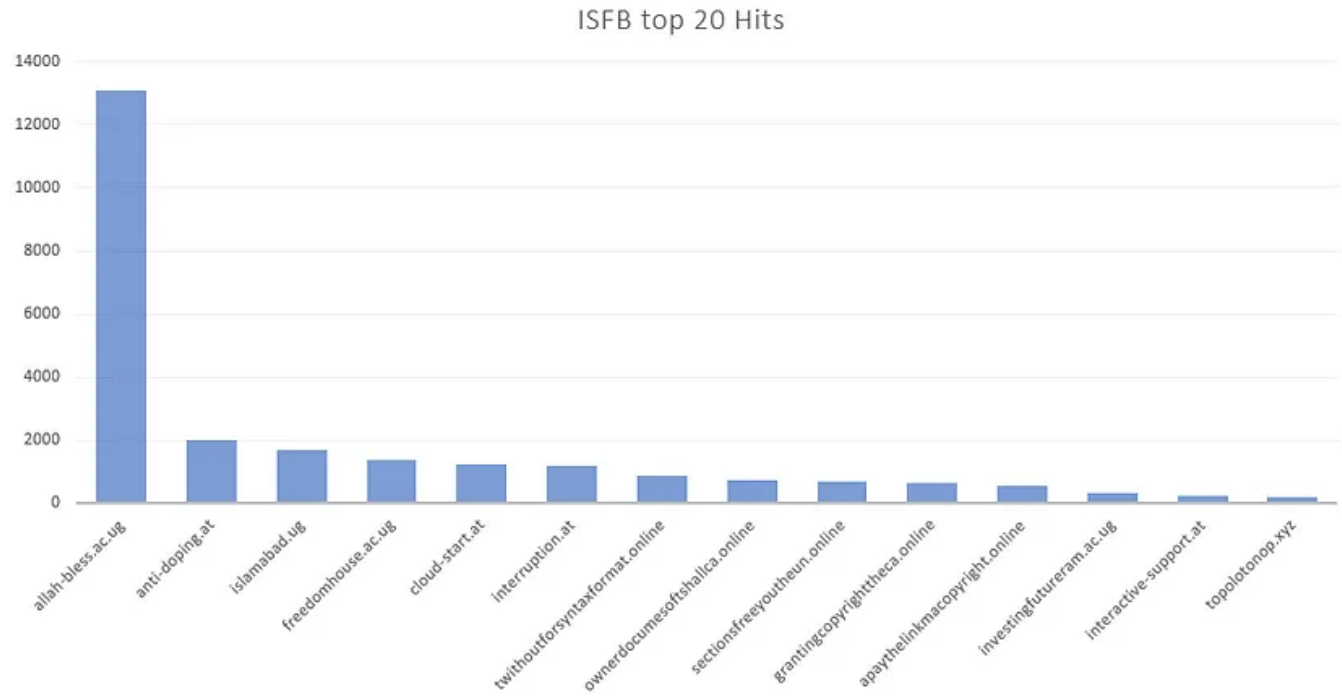
Even if we imagine that the Dreambot operators were using basic security like, for example, not using admin:admin as credentials, the BraZZZers requests acted like a sinkhole and allowed us to capture and analyse lots of Dreambot campaigns and alert victims.

When BraZZZers leaked a log like:

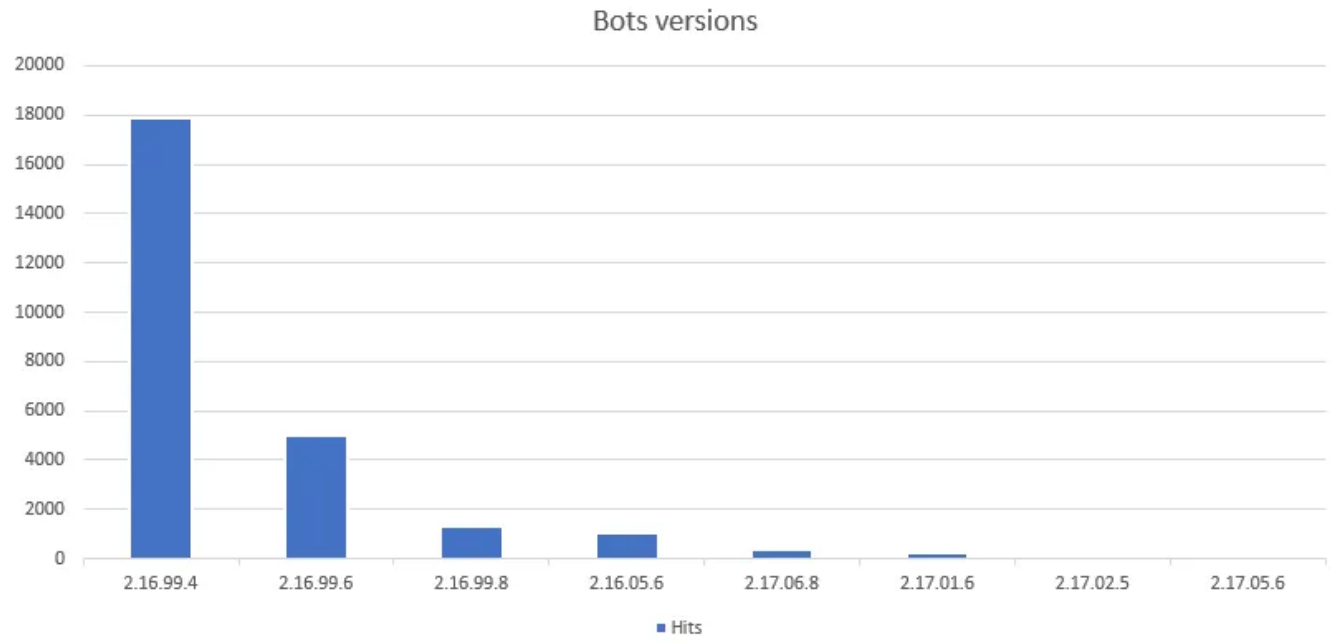
> *http://anti-doping.at/images/W7DM8fQnAkZl5/w_2BSbbA/6KBhhx7wg5evMuvuMv1oao4/U6yRGzURZD/XiL01nc5vbfiBN4bX/1hU3GL4_2F8A/_2Br5AtZAwV/A9odyEI1ZXMvvh/PyF7OtEFdbtoa6ixqh_2F/kovs8YDK7vDDr2cc/iLrdTIARsyp9z_2/FT_2BFFd_2BUGwOjfW/ZEZOwXx.gif*

We could easily (thanks here to Fumiko) parse those requests and extract campaigns data without even having to look for a binary:

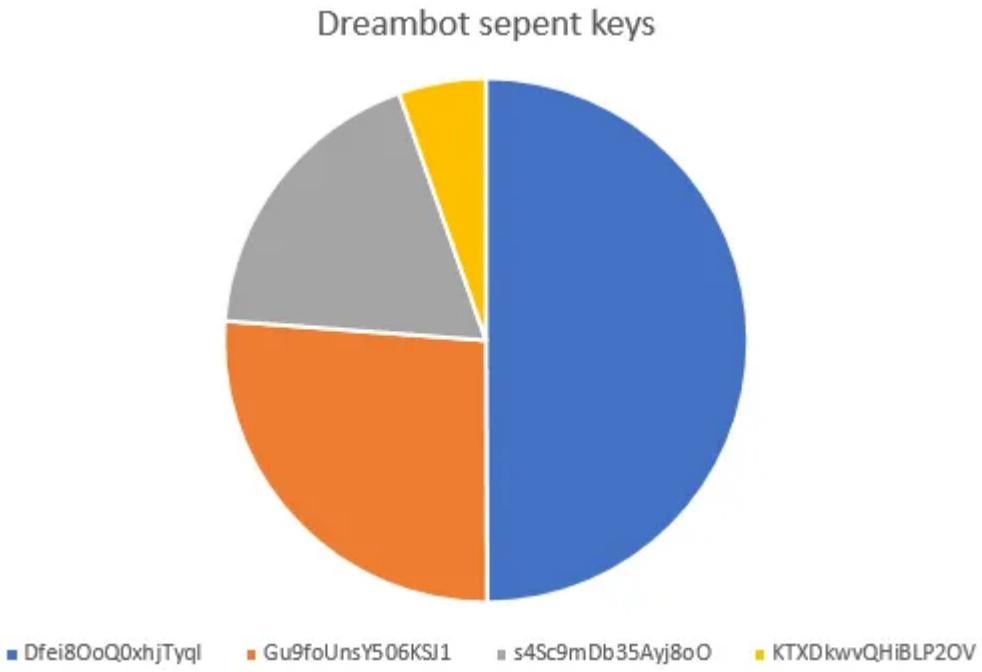
```
[i] Extension .gif: Ask for a task
[i] Key: Gu9foUnsY506KSJ1
[i] Domain: anti-doping.at
[i] Parsed path: W7DM8fQnAkZl5w+SbbA6KBhhx7wg5evMuvuMv1oao4U
yF7OtEFdbtoa6ixqh/kovs8YDK7vDDr2cciLrdTIARsyp9z/T+FFd+UGwOjf
[i] Decrypted path: nolia=bynuvxmrp&soft=1&version=216994&us
013d&os=6.1_1_7601_x64
[+] This beaconning looks like Dreambot
[+] Soft: 1
[+] Bot version: 2.16.99.4
[+] CnC server ID: 12
[+] Unknown requested payload ID: 4ad013d
[+] Bot group ID: 106
[+] Bot ID: 8749d2c1f6adc6ece3e60d081a1647b1
[+] Bot OS: 6.1_1_7601_x64
```



Top 20 hits by an ISFB domains to BraZZZers



ISFB versions distribution from the logs



Dreambot serpent keys observed in the logs

Victims clusters, showing the 3 botnets US, JP, DE/BG/EU

While parsing the logs we found some interesting ISFB requests, like the early deployments of IAP2; or even surprisingly GoziAT with domains configured on localhost.

2018/12/17 20:31:57	api.gkspsafoe.net	http://127.0.0.1:80/images/Jr_2BA1y/Bh5qwSKSg4tU/mTgUM2ILEjv1HnsV0zBB4SEbVAH486YsU_2Fmv7lFwHw14hXYJTzeyDE_2FTvuOWmCyiJLaj_2BTrrseJA1RUMUN_2FXps6uaensBKVzB5chWAjAPk_2Bt7MhnMHCjq07k8h23KBCiHVlglwubPHdNaCakSLrcVTy_2F5TXvLkMxAVLj_2FpK688VHVm.jpeg
2018/12/15 18:33:07	api.gkspsafoe.net	http://185.254.121.11:80/images/lW1ZDj9c/OMF_2FRlE8ZB/hw5E4NJ7btVtjK5CQmTSoObg6sFqesgLYvafK6lTiipvJsezxU9_2FRrraexdzPNJkk9HI5SKWKFrf344P_2F7SDsWQ3R2rf_2FGDKMJxmgQUS_2BwS7XMrQjQ5z8QQG647OBOubkorMuNMkBB9hQCkwv4qLULZsnTBMQsmXIXZ5oi_2BgQVLikoac1Puc4BnFX_2B4SYLZfLXBQ.jpeg
2018/12/15 16:33:00	api.gkspsafoe.net	http://185.254.121.11:80/images/OVWpAdL2/UP1t4wyZcmrL/026M0ojEPhPycVDj6J2E_2B08hcvDyOnuRsqiZTfRrsuIsQvMWkihRBvWfJYF8QOv0mXO9JRr3QpDAdeN9ttlumBqI4fbjz7rJCPyOQu8Zntm_2FoQowwnXaJdGb7k0RnhL0kF_2FAfOfFFiZQA1sLpMD9OErNY4ubElr4MHmZg1LjvnyN.jpeg
2018/12/15 14:33:00	api.gkspsafoe.net	http://185.254.121.11:80/images/gRzijyJE/g1ujJtI35D_2/B_2Fpfk3C9g5smC7a8sqxNzHssvfyoHPJqzc9LFF_2BIyHPlHmHpE38VVxZcsniaGnJNWNr2VsqkW_2BeOQsI84ylUfc9bQMbKodc1IfDI_2FWuXPo2784V_2BeySOzhVUGVpzO0YhIre2RBzK0P3YzbufDOJLOq9QGwmHVNY5imn17uqEE38madfNcj8L0YXmlMNMq0_2F_2BYZew.jpeg

Cryptbot Stealer

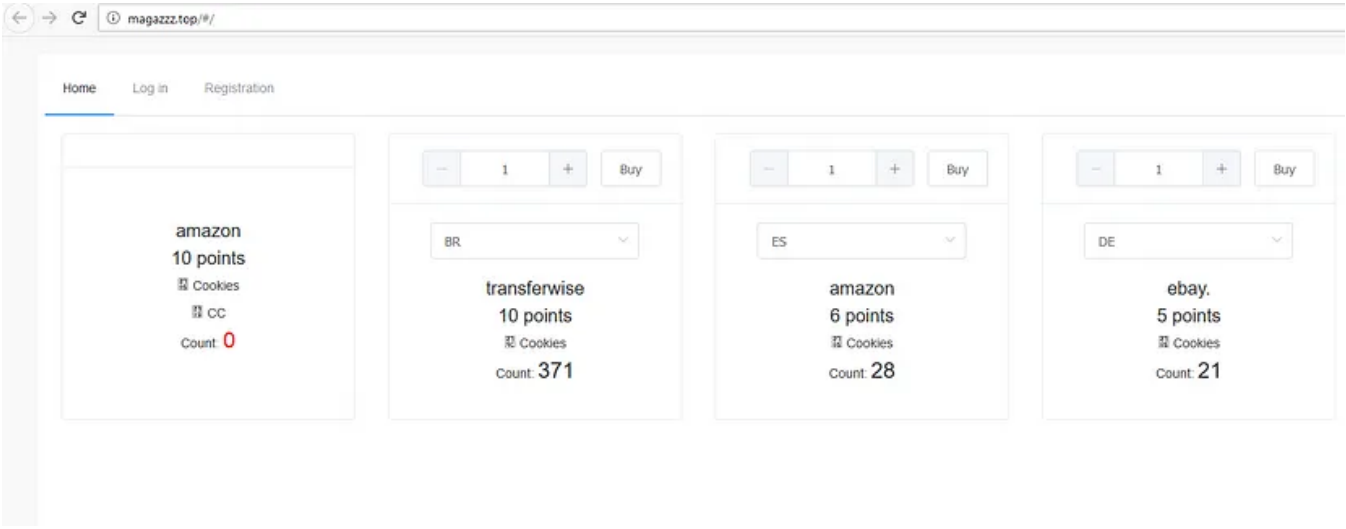
Another cool piece of malware to follow in these logs is Cryptbot. The operator of Cryptbot managed to build a huge botnet hidden behind a quite resilient infrastructure. It has been very hard to obtain intel - until we looked at BraZZZers.

We can observe the early days of Cryptbot dating back to 2019. Thanks to the upstream we were able to monitor them using the same IP as central CnC for months: 5.182.39[.]172.

If you do a reverse lookup and look for all the domains configured to that IP, you will see that Cryptbot in its early days was hosting its own marketplace in order to resell their stolen logs.

2020/08/13 00:29:38	otteppp15.top	http://5.182.39.172:80/index.php	
2020/08/13 00:29:32	otteppp13.top	http://5.182.39.172:80/index.php	
2020/08/13 00:29:08	otteppp15.top	http://5.182.39.172:80/index.php	
2020/08/13 00:29:03	otteppp15.top	http://5.182.39.172:80/index.php	
2020/08/13 00:28:36	otteppp11.top	http://5.182.39.172:80/index.php	
2020/08/13 00:28:23	otteppp11.top	http://5.182.39.172:80/index.php	
2020/08/13 00:28:13	otteppp15.top	http://5.182.39.172:80/index.php	
2020/04/29 02:18:15	larek.info	http://5.182.39.172:80/	
2020/04/29 02:18:12	larek.info	http://5.182.39.172:80/	
2020/04/29 02:18:09	larek.info	http://5.182.39.172:80/	
2020/04/28 16:50:00	larek.info	http://5.182.39.172:80/js/chunk-4ad984f0.a84d28ce.js	http://larek.info/
2020/04/28 16:25:08	larek.info	http://5.182.39.172:80/js/chunk-62bf7974.78f18c64.js	http://larek.info/
2020/04/28 16:23:24	larek.info	http://5.182.39.172:80/css/chunk-d35d7648.53270ba5.css	http://larek.info/

On top of the usual .top domains used as CnC gateway, we saw the infrastructure hosting shops like larek.info or magazzz.top



Month after month you can observe the botnet evolving into multiple botnets split on different infrastructures.

This is just another example of how useful these logs can be. Looking up every domain attached to the same hidden IP is a great way to help your attribution. Lots of actors were sloppy with real server IPs, thinking they were protected by BraZZZers.

Marketplaces

BraZZZers was not only reserved to malware, we observed a fair amount of Market places / carding shops. Some well-known ones like slilpp.top or cop.su could be found here.

2021/03/29 20:35:01	slilpp.top	https://45.139.236.33:443/shops/admin/support.php?user=308648	https://slilpp.top/shops/admin/support.php?user=308648
2021/03/29 20:35:01	slilpp.top	https://45.139.236.33:443/shops/admin/content.php	https://slilpp.top/shops/admin/stats.php?user=259173
2021/03/29 20:35:01	slilpp.top	https://45.139.236.33:443/shops/admin/stats.php?user=308648	https://slilpp.top/shops/admin/stats.php?user=308648
2021/03/29 18:15:01	slilpp.top	https://45.139.236.33:443/admin/users.php?token=2ea7356f2515546c1c8284af5a76025e&uid=224594	https://slilpp.top/shops/admin/stats.php?user=224594
2021/03/29 18:15:01	slilpp.top	https://45.139.236.33:443/shops/admin/tickets.php	https://slilpp.top/shops/admin/support.php?user=308546
2021/03/29 14:30:01	slilpp.top	https://45.139.236.33:443/shops/admin/support.php?user=204784	
2021/03/29 14:15:01	slilpp.top	https://45.139.236.33:443/shops/admin/img/rettiwt.png	https://slilpp.top/shops/admin/stats.php?user=308082
2021/03/29 10:05:01	slilpp.top	https://45.139.236.33:443/admin/tickets.php	https://slilpp.top/admin/support.php?user=104780
2021/03/28 23:20:01	slilpp.top	https://45.139.236.33:443/shops/admin/support.php?user=77898	https://slilpp.top/shops/admin/tickets.php
2021/03/28 23:20:01	slilpp.top	https://45.139.236.33:443/shops/admin/support.php?user=119022	https://slilpp.top/shops/admin/tickets.php

We extracted a list of the most known ones from the logs:

- darknet.so

- cop.su
- vor.nz
- srost.biz
- slilpp
- v-market
- cvv2.name
- cvvshop.lv
- hybra2web.ru
- vault.ug

Magecart

As a final example, we will show how to exploit the referrers with Magecart (a.k.a. eCommerce skimmers) . Several domains on BraZZZers were used for Magecart attacks:

2020/06/01 03:32:29	toplevelstatic.com	http://45.141.86.31:80/_dom.check.php	
2020/06/01 03:27:29	toplevelstatic.com	http://45.141.86.31:80/_dom.check.php	
2020/06/01 03:27:23	toplevelstatic.com	http://45.141.86.31:80/setting/min.min.js	https://www.thepinkdoormemphis.com/
2020/06/01 02:04:19	toplevelstatic.com	http://45.141.86.31:80/setting/min.min.js	https://www.drilldoctor.com/?utm_medium=ppc&utm_campaign=Custom+Intent&utm_term=&utm_source=adwords&hsa_cam=2066108374&hsa_mt=b&hsa_ver=3&hsa_grp=77827644458&hsa_net=adwords&hsa_ad=367120984248&hsa_tgt=&hsa_kw=&hsa_acc=4924738831&hsa_src=
2020/05/27 14:40:38	toplevelstatic.com	http://45.141.86.31:80/setting/min.min.js	https://www.blockandcompany.com/sales/order/history/
2020/05/27 14:40:34	toplevelstatic.com	http://45.141.86.31:80/setting/min.min.js	https://www.blockandcompany.com/customer/account/
2020/05/27 14:40:30	toplevelstatic.com	http://45.141.86.31:80/setting/min.min.js	https://www.blockandcompany.com/customer/account/login/
2020/05/27 14:40:29	toplevelstatic.com	http://45.141.86.31:80/setting/min.min.js	https://genuineappliancеparts.com.au/
2020/05/27 14:40:27	toplevelstatic.com	http://45.141.86.31:80/setting/min.min.js	https://www.blockandcompany.com/

By looking at the referrer in the logs, we could see that the domain *toplevelstatic.com* is called from several shops *blockandcompany.com*, *thepinkdoormemphis.com*… From the logs you can easily create a list of web shops infected by a web skimmer.

As can be seen from those few examples, different approaches are possible in order to extract valuable data. Those logs are quite diverse, you can see requests from

multiple botnet families, for example ISFB, PsixBot, DJVU, Nemty, Ako, Riltok, Coalabot, Cryptbot, Megumin, Azorult, KPOT, Betabot, ZLoader, DiamandFox, Vidar, Lokibot, TinyNuke, OSX malware…

Global stats

Again, please bear in mind that these logs only show the failed requests of the BraZZZers infrastructure. The below statistics can help to see tendencies but cannot necessarily be used to determine who was receiving the most traffic.

Families	Domains	Hits
Marketplace	slilpp.top	728449
Redline	matjiva.top	313211
Nemty	nemty.top	138293
BuerLoader	koralak.hk	116108
DJVU/STOP	loot.ug	82794
PsiXBot	the-best.hk	44681
Nemty	nemty.hk	35128
TriumphLoader	gxd3fp7fe7cac6jzn2sac.online	27851
CoalaBot	esek412782.com	26352
Ako Ransomware	recovery.hk	22299
SmokeLoader	taj.co.ug	22099
Azorult	localhelporganizerngo.co.ug	21757
Phushing	blcolchian.lcglin.com	20637
Marketplace	v-market.pro	20088
Phishing	apeswapcar.com	19536
Anubis	lastver4563.top	19440
DJVU/STOP	texet1.ug	18527
Marketplace	validcc.su	18274
SmokeLoader	svhost-system-update.net	17036
Phishing	login-blockcheln.com	15906
Phishing	apeswapmove.com	14621
DJVU/STOP	rosalos.ug	14442
Cryptbot	bbload01.top	13498
Dreambot	allah-bless.ac.ug	13147
Gcleaner	prettycleaner.hk	13081
Cryptbot	bbload02.top	12714

Top hits by domains in the BraZZZers logs

Nodes ASN	Countries
ASRELINK	RU
ASGHOSTNET	DE
MGNHOST-AS	RU
NANO-AS	LV
HOSTWINDS	US
ASBAXETN	RU
ASBAXET	RU
NTSERVICE-AS	UA
OVH	FR
ITLDC-NL	UA
VODAFONE-CZ-AS	CZ
ITL-BG	UA
TEAM-HOSTAS	RU
TENNET	RO
IST-AS	LT
SERVERserver.ua	UA
SPRINTLINK	US
GREENFLOID-AS	US
INTERNET-IT	VG
STARK-INDUSTRIES (MORENE HOST)	MD
HZ-US-AS	BG
IOMART-AS	GB
LITESERVER	NL
PRIVATEHOSTING-NET	IT
STARK-INDUSTRIES (MORENE HOST)	GB
HETZNER-AS	DE

Top hosters used to host the BraZZZers proxy nodes

This story teach us that nobody is immune from a incompetent supply chain. It's a good example of the limits of the open cybercrime industry. The business is mainly based on trust and reviews and we have seen several cases where BraZZZers admins were pushing fake reviews to boost the reputation of the service. From here it's the snow ball effect and it just needs one big name like Azorult or a ransomware group patient enough to tolerate the poor quality service to attract more clients.

While following the business side of BraZZZers, we observed several users reporting the poor quality of the service, the grey links to the hosting company MoreneHost or the low frequency of nodes renewal but that hasn't been enough to scare away the majority of customers.

We expect to see more and more cases like this one. The cybercrime industry is growing much faster than the skills of the cyber criminals. Almost every step of fraudulent activity is now supported by a third party within the market. Malware, VNC, infrastructure, drop data, drops, marketplaces. The industry end up with a

multitude of poorly developed services sold in open marketplaces to customers completely unable to understand if a service should be trusted or not as long as it works.

Opening the data

As explained in the introduction, the data is composed of upstream and 404 logs from end of 2018 to March 2022. To make the interesting data available, while trying not to expose victims IPs, we are opening all the upstream logs without client IPs as TLP;WHITE.

The file is a csv: date,domain,upstream,referrer.

[Download] — Zip password: infected

ef2a69c94e5420f44ee0932abbfaf8e3b4f5f5bb6308a4928dc4dd4bc06f6d4c

We hope these logs will maybe make somebody out there able to look at them from yet another angle.

Happy hunting!

Malware Brazzzersff Fast Flux DNS Security Research

Follow

Written by Benoit ANCEL

81 Followers · Writer for CSIS TechBlog

@benkow_

More from Benoit ANCEL and CSIS TechBlog