GCleaner — Garbage Provider Since 2019

By Benoit ANCEL

Published: 2021-01-18 · Archived: 2026-04-05 19:49:56 UTC

Reselling access to infected machines (aka “loads reselling”) has become a huge part of the cybercrime industry. In this article we investigate an active threat actor, who has been in the loads industry for over two years, reselling access to hundreds of thousands of machines every month.

When botnet operators want to start their business, they have to face different challenges. They have to buy (or build) a piece of malware and a backend, rent different servers, pay for cryptors, certificates etc — but in the end, one very important point is how to distribute the malicious software.

They can distribute the malware themselves (which is a lot of work) or pay a third-party, so called “load resellers”. Spammers, exploit kit distributors, Pay-Per-Install (PPI) vendors — all of them are just load resellers. You don’t buy a number of spam campaigns from a spammer, you buy a number of infections — no matter how they are obtained.

As profitable as the loads business might be, it’s also a complex industry facing lots of changes that requires a strong adaptive capacity in order to survive. Selling loads is not only about how many people you can infect; it’s also what quality of infections you can provide to your clients.

Loads sellers also have to protect their customers. When they distribute a payload they have to avoid ending up analyzed by sandboxes, or talked about in social media. Otherwise the malware IOCs would be burned and their clients would have to buy new domains or certificates in order to stay outside blacklists, such as Spamhaus.

When a cybercrime operation tries to steal money from a bank, the operators need victims who are accessing their online banking accounts. That means you can forget about distributing a fake Roblox crack, but instead need to find a way to infect accounting services and such.

Spam is of course one of the main ways to sell loads, you can craft a specific mailing lists targeting only companies or specific sectors in order to obtain good quality bots, but banking trojan admins are sometimes very picky and will only pay the spammer if an infected bot reaches the webinjects CNC. It’s not an easy job.

When you’re good at spamming you can make good money: We observed good spamming actors earning up to 60 000 USD a week when they work well, but as strange as it seems, spamming starts being more and more complicated and lots of spammers lose their clients to other kinds of loads resellers.

We observed spammers complaining about different factors, the first one being that from their estimations, up to 40% of the emails sent to the victims are opened on mobile devices. They cannot infect easily a tablet or a smartphone and that means that half of the work they do goes directly in the trash. 2020 didn’t helped them either,

the medical crisis sending everybody home and various companies closing down caused a huge loss in term of spam ratio.

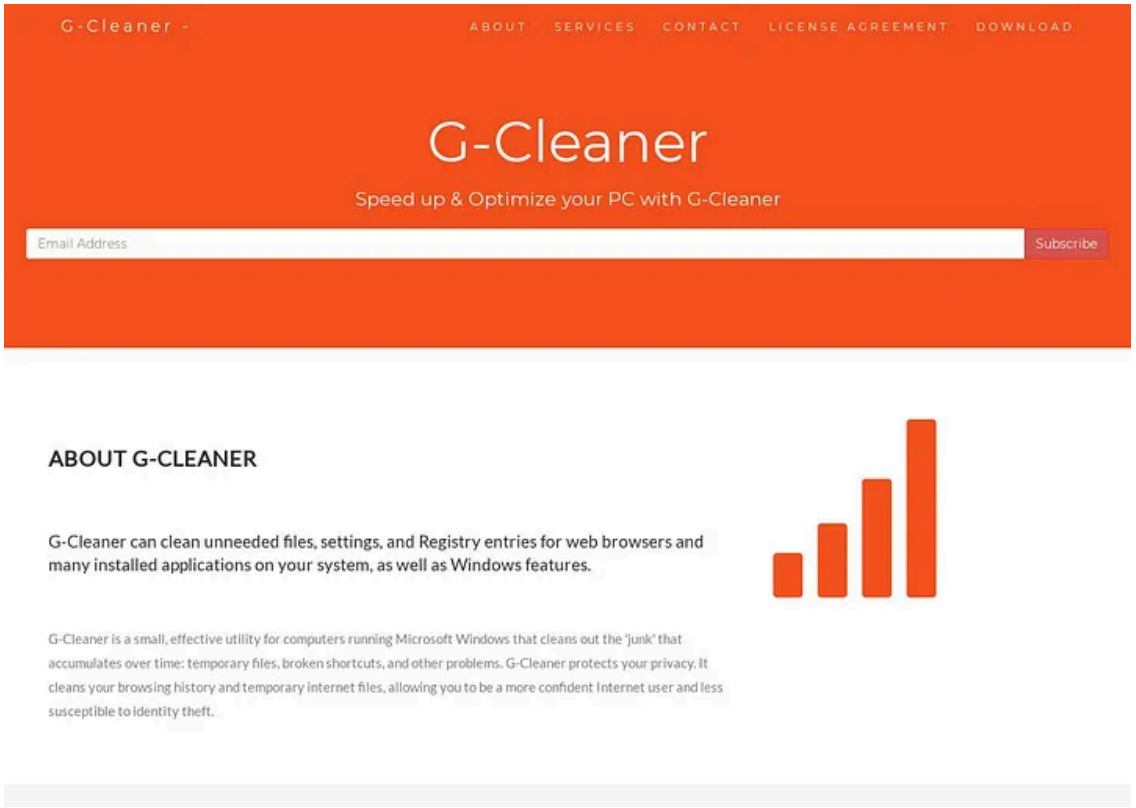
Having done this long introduction about the state of loads selling business, we are going to introduce you to an actor that is becoming very powerful.

It is a load seller working mainly for ransomware and password stealers actors for at least two years and who is starting to reach huge monthly infections numbers.

Garbage cleaner — Selling garbage since 2019

In the beginning of 2019 we observed a new actor becoming a client of the Fast Flux network called Brazzzers. This client was using the fast flux to host a website called G-Cleaner for Garbage Cleaner, mimicking cleaning tools like CCleaner.

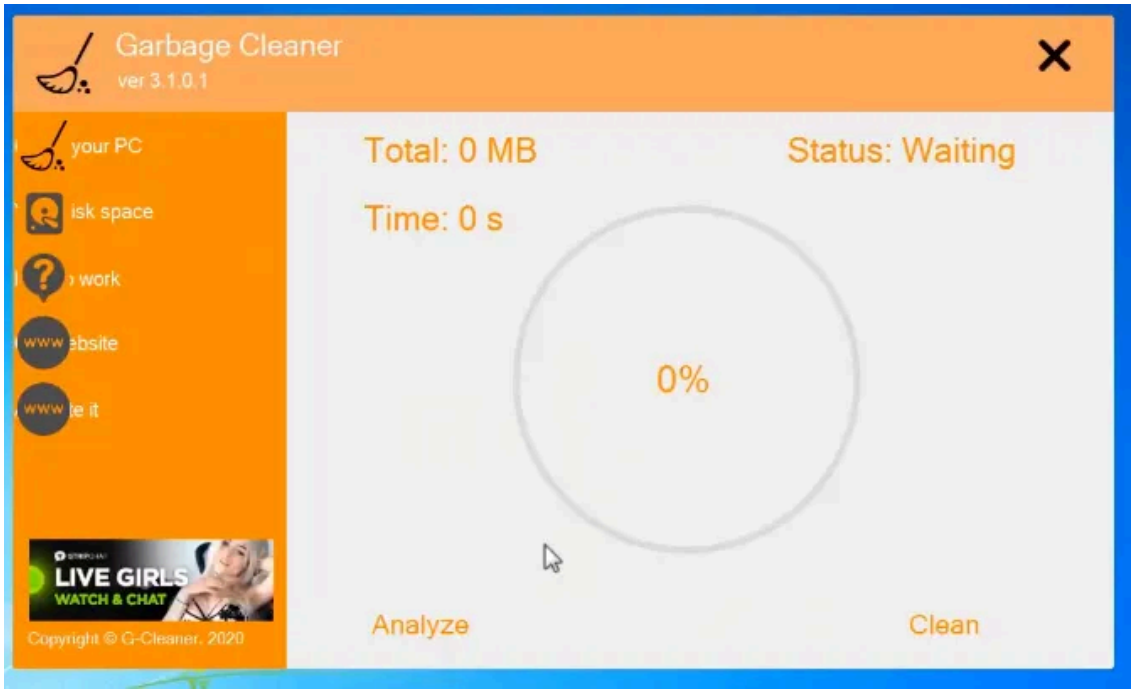
Press enter or click to view image in full size



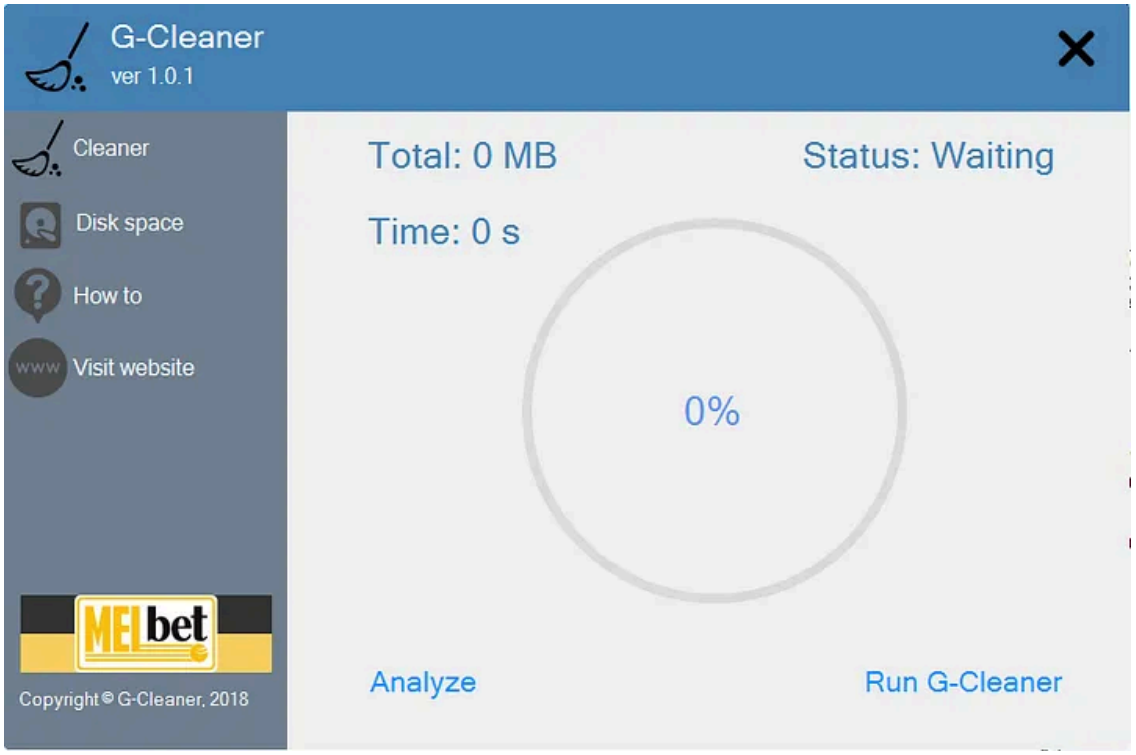
g-cleaner[.]info

Back then the admin was promoting the fake software via emails in order to have his cleaning tool downloaded, which was in fact dropping the Azorult password stealer.

Press enter or click to view image in full size



Press enter or click to view image in full size



Quickly we observed the website implementing a Traffic Direction System (TDS) using IPLogger in order to distribute different malware samples depending on the location the victim was downloading the fake cleaner from, and the list of these distributed malware samples started to grow.

Azorult, PredatorTheThieff, and Miners started to be distributed but the infection ratio seemed to not be very good for a load reseller. The problem was that you could download the fake software from the fake website, so any AV company could just automatically retrieve all the payloads and blacklist the IOCs automatically.

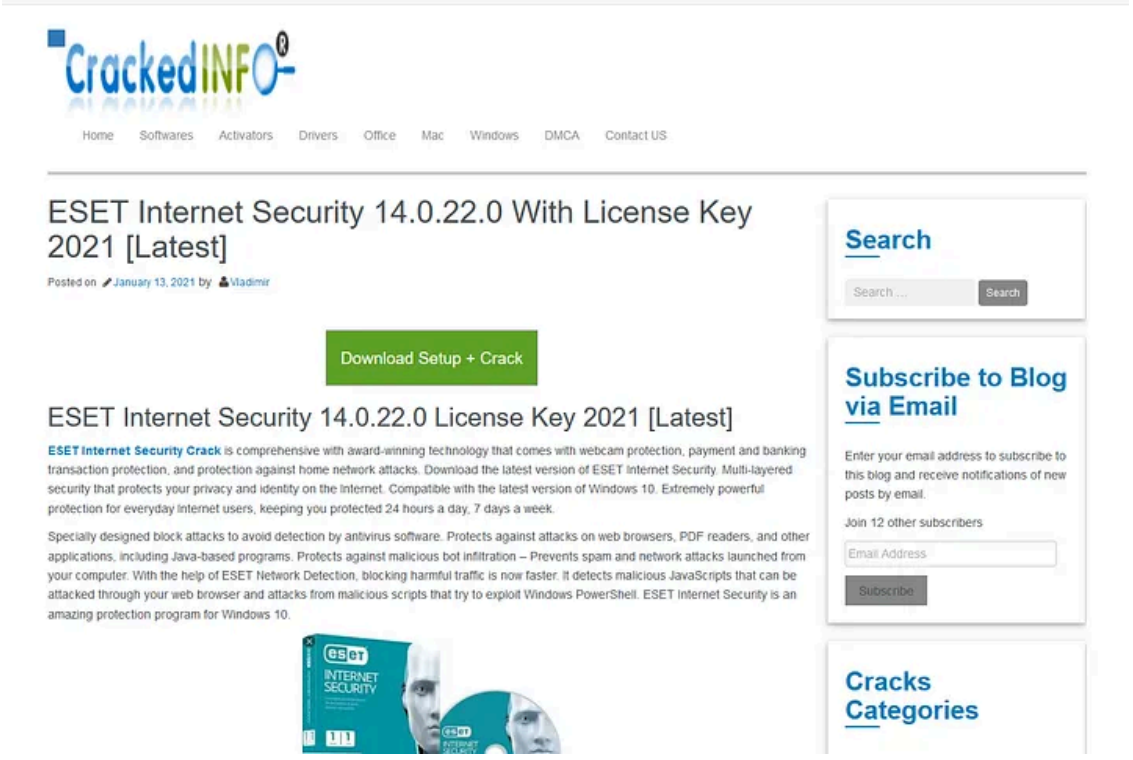
Get Benoit ANCEL's stories in your inbox

Join Medium for free to get updates from this writer.

Remember me for faster sign in

That's when the load sellers started to change their way of spreading the fake software. No more G-cleaner direct download around, the distribution is now done by various different crack websites.

Press enter or click to view image in full size



Example of crack websites

After running one of those cracks, many different pieces of malware are deployed on the victim's computer.

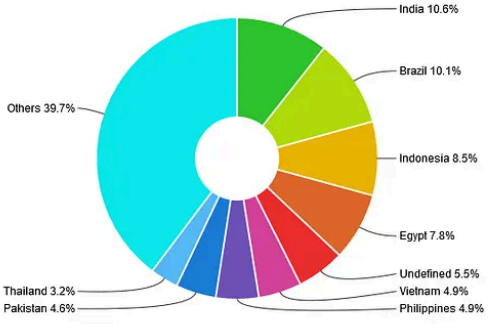
Press enter or click to view image in full size

Depending on your country, you receive different malware. In January 2021 we observed:

- STOP/DJVU ransomware

  Press enter or click to view image in full size

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%
Cambodia	38	35	3	0.4%
Cameroon	15	15	0	0.2%
Canada	2	2	0	0.0%
Chile	86	86	0	0.9%
China	33	33	0	0.4%
Colombia	95	92	3	1.0%
Comoros	1	1	0	0.0%
Congo	1	1	0	0.0%
Costa Rica	11	10	1	0.1%
Cote d'Ivoire	20	19	1	0.2%
Croatia	7	7	0	0.1%
Cuba	8	8	0	0.1%
Cyprus	3	3	0	0.0%
Democratic Republic of the Congo	7	7	0	0.1%
Djibouti	1	1	0	0.0%
Dominica	1	1	0	0.0%



  DJVU stats backend

The infrastructure

As mentioned earlier, this loads seller seems to try to hide his servers behind the Brazzzers fast flux. We managed to extract the real location of the backend over time:

```
cleaner-g.online - 91.243.83.187
cleaner-g.site - 91.243.83.187
gcleaner.info - 91.243.83.187
g-cleaner.info - 91.243.83.187
gcleaner.ru - 91.243.83.187
ggcleaner.top - 91.243.83.187
ggcleaner.xyz - 91.243.83.187
sfccleaner.top - 91.243.83.187
ge-cleaner.tech - 5.182.39.210
ge-cleaner.xyz - 5.182.39.210
ggcleaner.space - 5.182.39.203
ggcleaner.tech - 5.182.39.203
gcc-partners.in - 5.182.39.44
```

As we can see, despite the frequent renewal of the domains, the backend stayed at the same place for 2 years, showing the efficiency of the Brazzzer Fast flux to protect their servers.

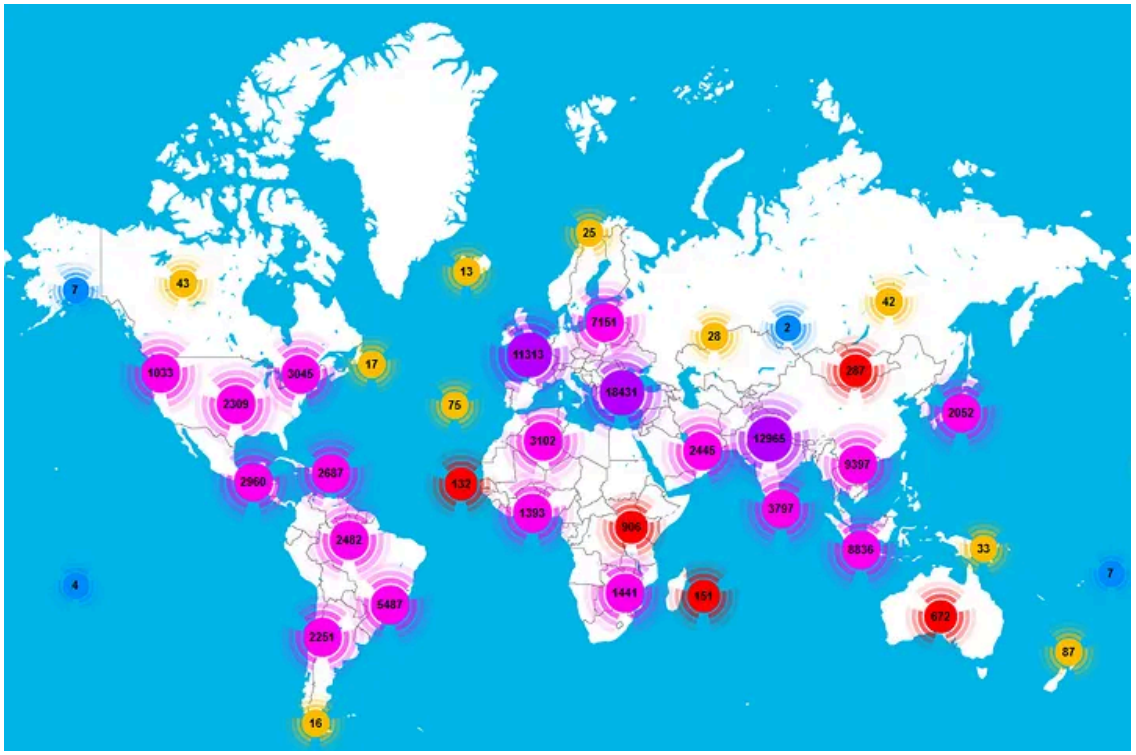
Statistics

We managed to obtain infection statistics for a month of activity, between December 2020 and January 2021.

The G-Cleaner network generated over 150,000 infections worldwide during this timeframe. It’s a huge number considering that December and January are not the best months for the cybercrime industry.

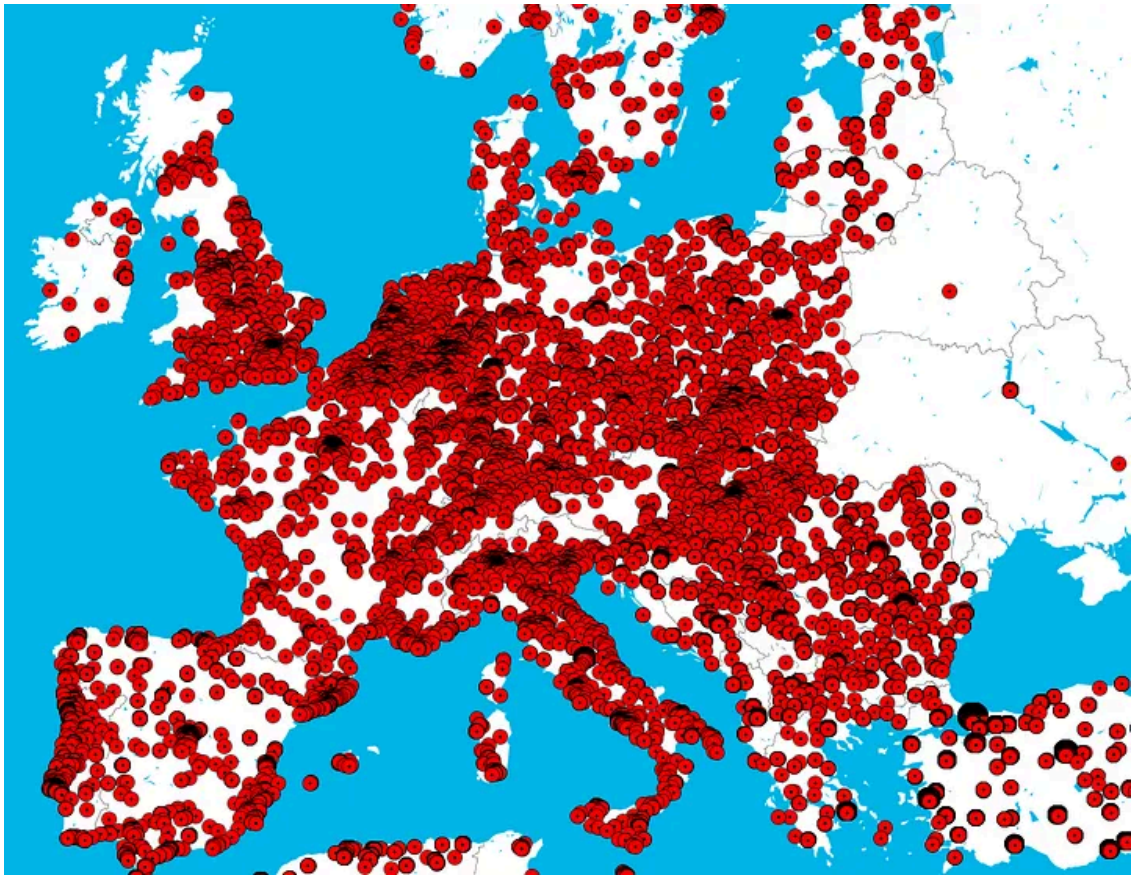
Those infections seem to be split between 4 partners, with each partner targeting a specific region: US, CA, EU and MIX (common word for a bit of every country).

Press enter or click to view image in full size



World map of infections

Press enter or click to view image in full size



European map showing the clear CIS border

Top 25 infected countries for January 2021:

Country	Numbers
IN	16623
TR	8759
BR	7809
ID	5546
PK	4891
EG	3966
TH	3256
US	3197
VN	3072
PH	3027
IT	2710
PL	2582
DE	2460
ES	2439
MX	2371
FR	1912
NL	1818
BD	1766
RO	1613
GB	1604
KR	1505
DZ	1483
AR	1380
MY	1358

We can see here that the loads seller seems to bet on quantity and not quality of infections. They infect the maximum number of victims they can, regardless of whether it's an interesting victim or not. That's why the majority of malware seen related to this threat is password stealers. They distribute lots of password stealers to collect a huge amount of various credentials for services like Netflix, Apple, Google, Spotify in order to fuel the black market and make extra money.

We unfortunately didn't find the price list for that particular loads seller, but if we refer to the actual market, Asian and South American bots can be sold for around 0.2 USD per infection, European goes up to 0.60 USD and US bots can be sold for more than 1 USD. So, even working on quantity and not quality we can see that loads selling is a very profitable business.

Recent IOCs

```
crackedinfo.net
softkeygenpro.com
topkeygen.com
cleaner-g.online
cleaner-g.site
gcleaner.info
g-cleaner.info
```

```
gcleaner.ru
ggcleaner.top
ggcleaner.xyz
sfccleaner.top
ge-cleaner.tech
ge-cleaner.xyz
ggcleaner.space
ggcleaner.tech
gcc-partners.in
covid2023.info
f241beb45db9a8b7.xyz
naritouzina.net
prodocomelo.info
dream.pics
landoflegendstore.net
chrome-booster.com
331befdc5416a898.xyz
noabuseshere.top
havalpartsch.top
mmmmonsterpack.info
radrile.xyz
telete.in
topprogress.top
davincieditor.com
wheredoyougo.cn
vjsi.top
```

Related work

https://www.bleepingcomputer.com/news/security/fake-windows-pc-cleaner-drops-azorult-info-stealing-trojan/

Happy hunting!
