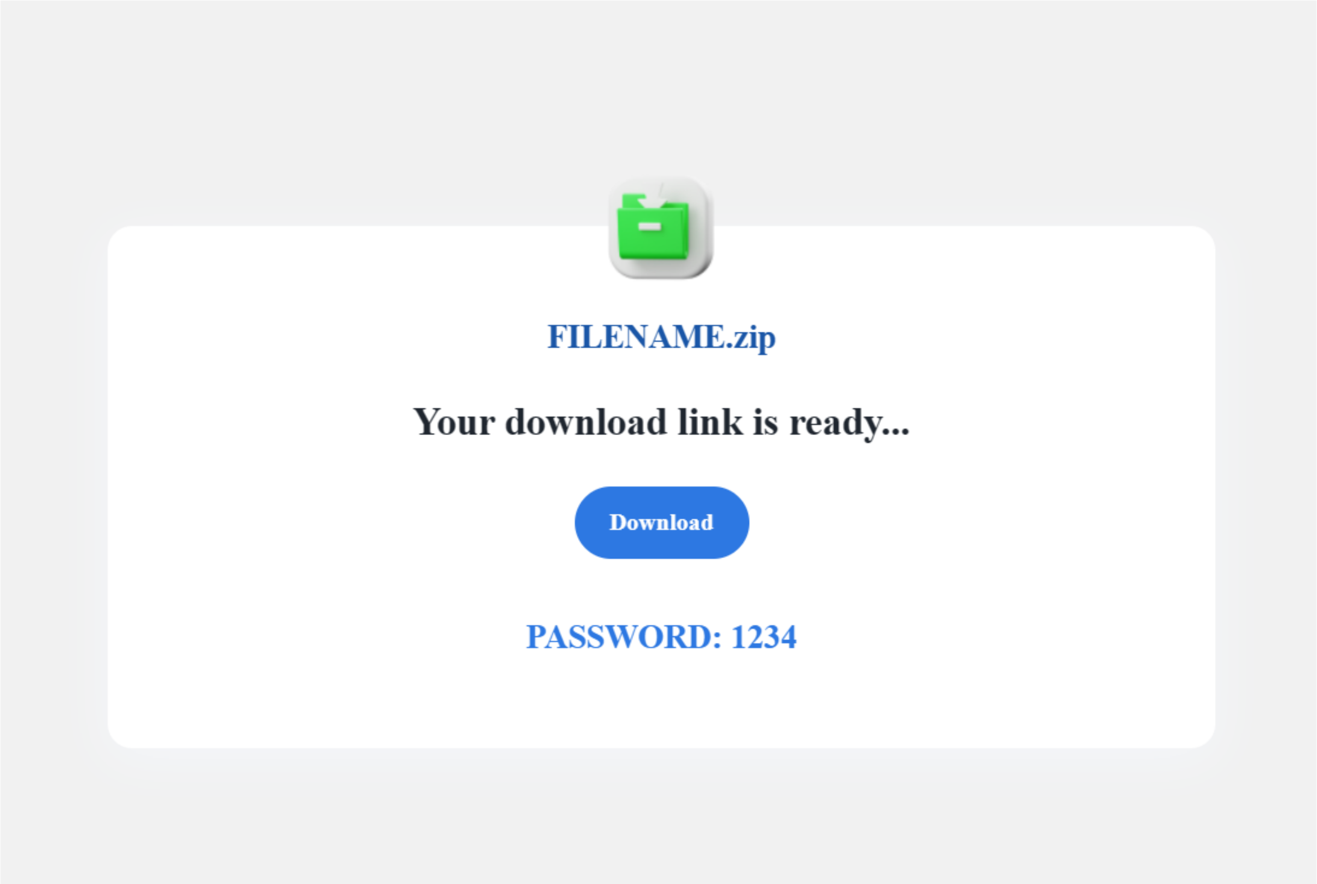
PrivateLoader: InstallsKey Rewind 2023

g0njxa.medium.com/privateloader-installskey-rewind-2023-c1ce027cbe65

g0njxa

February 1, 2024



FILENAME.zip

Your download link is ready...

PASSWORD: 1234

g0njxa

--

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:

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-privetstvuju-k-vashemu-vnimaniju-servis-installskey-po-prodazhe-ustanovok-na-fajl-klienta.31649/)
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.1958/)
Odiscus (https://m.odiscus.com/topic_3081)
Instagram Forum (https://instagramforum.ru/threads/installskey-installs-mix-world-europe-usa-uniques.147130/)
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

Translated from Russian / Original Post

And managing draws and contests

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.

Privateloader has been documented very heavily in 2022, please find some technical analysis from old builds here:
PrivateLoader: The first step in many malware schemes | Intel471
Peeking into PrivateLoader | Zscaler
Tracking PrivateLoader: Malware Distribution Service (bitsight.com)
PrivateLoader: the loader of the prevalent ruzki PPI service — (sekoia.io)

This report is not going to be technical but a recap of a year of my observation on the Privateloader campaign. (May 2023 to December 2023).

But first some insights:

Introduction

Sekoia analysts reported Privateloader as the “prevalent loader of the *ruzki* Pay-per-Install service”, on September 15, 2022. This service was known as and was managed by aka les0k aka zhigalsz.

Source:

A week later, on September 21, 2022, this PPI service was terminated due to “lack of good quality traffic sources”:

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, Italy, Luxembourg, Netherlands, New Zealand, Norway, Spain, Sweden,
Switzerland, United Kingdom, United States.
Tier 2 countries: Andorra, Argentina, Bahamas, Belarus, Bolivia, Bosnia and
Herzegovina, Brazil, Bulgaria, Brunei, Greece, Guyana, Hungary, Greece, Guyana, Hong
Kong, Indonesia, Iceland, Israel, Kazakhstan, Qatar, China, Colombia, Costa Rica,
Latvia, Lithuania, Macau, Malaysia, Malta, Mexico, Morocco, Nepal, United Arab
Emirates (UAE), Oman, Panama, Paraguay, Peru, Poland, Portugal, Puerto Rico, Republic
of Korea (South), Russian Federation, Philippines, Chile, Croatia, Czech Republic,
Ecuador, Estonia, Fiji, Montenegro, Romania, Saudi Arabia, Serbia, Singapore,
Slovakia, Slovenia, South Africa, South Africa, Thailand, Turkey, Uruguay.
Tier 3 countries: Albania, Algeria, Angola, Armenia, Azerbaijan, Bahrain, Bangladesh,
Barbados, Belize, Benin, Botswana, Burkina Faso, Burundi, Cambodia, Cameroon, Cape
Verde, Comoros, Congo, Egypt, Gabon, Georgia, Guatemala, Guinea, Haiti, Honduras,
India, Iraq, Jordan, Kenya, Kenya, Kuwait, Kyrgyzstan, Laos, Lesotho, Lebanon,
Mauritius, Madagascar, Macedonia, Mali, Mauritius, Mauritius, Madagascar, Macedonia,
Mali, Mozambique, Moldova, Mongolia, Namibia, Niger, Nigeria, Nicaragua, Pakistan,
Chad, El Salvador, Ethiopia, Senegal, Suriname, Tajikistan, Tanzania, Togo, Trinidad
and Tobago, Tunisia, Turkmenistan, Uganda, Ukraine, Uzbekistan, Jamaica.
```

```
Tier 1 & 2 must be considered the aiming of these services, while Tier 3
areconsidered 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:

User “Fasilcrypt” alledgelly paid “DozKey” 700 USDT for a Mix of installs on his .exe file Transaction 5a922fe966a188d9e057b0e0fb843ccd7d673178fd988d38845a40e70d4c977f | TRONSCANAnd 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>>
```

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.

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)

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.

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:

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.

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:

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”.

Source: InstallsKey channels (Translated from Russian)

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

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:

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=V9sXR6aIOgK4znoIV3QEJiCPc0YxrQNplx



PLmp.bmp
https://vk.com/doc418490229_669753443?
hash=xBPbo5OmmjzwJojlZOFbmu9Qg1TtR9d8MRZqMGAVdH0&dl=HHirDf6vFga94nqdq5sutIGzHeDDVd3WN4



BotClients.bmp
https://vk.com/doc418490229_669637079?
hash=VdguLglaUQxQEWy7OPzp09fMiy3JG1498Od7lJ6mEhw&dl=Z0vdo01g0fZfW08T5s4JBiEH2UzpBHOBxg



WWW11_32.bmp (Url tagged as WW_11)
https://vk.com/doc418490229_669753909?
hash=WT7APgrulCXZFZTSEvdEhpp2wKrYTIZVouZnBZXB72g&dl=7ei7VkBuvhBOPmO5RJDS1eEOZh0NZgZcXN



file191223.bmp (Url tagged as test22)
https://vk.com/doc418490229_669783554?
hash=BH6rDsCdPWk2J9y1TmstXOZKSIMojhaG8Fw9a8GF3Ps&dl=gYknZQrp3U8V5VDWqeRDZZgAOIRQPc5uWY



onxin.bmp (Url tagged as 1)
https://vk.com/doc418490229_669783497?
hash=lpgJt6qZJygrnJD46sqduKmXlfiOOex3pEVxJqSqyH4&dl=mlJSM2PcfjV0k8snB6UZHzCmbEp5F7WBEz



crypted.bmp (Url tagged as 1)
https://vk.com/doc418490229_669744741?
hash=OaF1x9qtGSlulTdzzPxQkefg8M8fGibH0KNgx7Org7k&dl=ynpLFb3qBIWJi5nuaxht4tO3jWmOzcwNRL

LG.bmp (Url tagged as logger_statistics)https://vk.com/doc418490229_669653354?
hash=l8DHCu4lEp9Sb8CTCk5eithtVIhhbBkli1pjUtPjJNP&dl=7vSjZ36UYD1hlgYVc9MzZLLGmShUHLSQat
```

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.

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):

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

```
Full list of Fake Shortner links (CAMPAIGN ID09)
Every path with a length >= 2 will lead to a PrivateLoader download

5.149.248.110cinurl.compicfs.combll tly.comurllio.comurloho.combltlly.comtinourl.comtin
```

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.bloggamezfull.comzdescargas.orgcrackzipp.comindir.torrentabi.compastemytxt.c
 (wordcounter.icu & pwrpa.cc)fc-lc.xyz
(digitalmarktrend.com)uploadrar.comadurly.ccshrinkme.orgturbobit.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.

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.

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.

Source:

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**

```
https://adstructor.com/share/file?
AMCMtmXoTQUAi2UCAEVTFwAoAAAAAADA.filehttps://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.

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

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/adbuhohttps://pivigames.blog/pged.phphttps://adbuho.com/pivigam
2.phphttps://www.linkonclick.com/jump/next.php?
r=2558259https://page.strtgic.com/click?
pid=10&offer_id=20738&sub1=17058359281000TESTV431140760274V30&sub2=2558259&sub3=86077
```

Everything seems to be managed by .js files:

/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

Downloading Privateloader from gamezfull.com

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

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

This domain is involved with victim logs

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

This domain has fake download buttons coded on his pages

```
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[
```

This domain is involved with victim logs

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

This domain has fake download links coded on his pages

```
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-downloadhttps://href.li/?https://track.redis06.sbs/go/19a45436-cb73-4be8-
8e51-8ee0e9a6e90d?
affiliate=648adb2ebbf11&channel=&keyword=adobecreativecloudcrackdownload&clickid=https
q=adobecreativecloudcrackdownload&s1=648adb2ebbf11&s2=&s3=DvHbEoqQPRN5ASTKqJ75Eq[Priva
```

This domain is involved with victim logs

> 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 chainhttps://highfile1.click/go.php?
a_aid=55d0ea51596f4https://href.li/?https://track.redis06.sbs/go/19a45436-cb73-4be8-
8e51-8ee0e9a6e90d?
affiliate=55d0ea51596f4&channel=&keyword=Setup&clickid=https://unleakyammiolitesmithia
q=Setup&s1=55d0ea51596f4&s2=&s3=MifHrsziFQJpNszsRQNQgm[Privateloader]
```

This domain is involved with victim logs

> pastemytxt.com (Target: WorldWide)

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 chainhttp://get.claruspolaris.com/?
a=197977&o=149408&c=0&co=251140&mt=5https://aditmedia.g2afse.com/click?
pid=3052&offer_id=20972&sub1=71b3e999867c4446b9a28eae4bcd25af247a0&sub2=197977_https:/
offer_id=851&pub_id=5&pub_sub_id=3052_197977_&pub_click_id=65b2de0e46cb830001eaf487htt
s1=5&s2=3052_197977_&s3=BOTKssIAAAGNQrN1tgAAA1MAAAAFAAAAAAAAAABq[Privateloader]
```

This domain is involved with victim logs

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

This domain has fake download buttons coded on his pages

```
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%20Converter%20(2024)%20(x64)%20[Full]%20Espa%C3%B1ol%20[Mega]
```

This domain is involved with victim logs

> freegamesdl.net (Target: English-speaking 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 chainhttps://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

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

Extended redirection chainhttps://bluedownload10.sbs/go.php?
a_aid=63ba729511d6d&chan=devtek&fn=street-fighter-4-champion-edition-mod-
apkhttps://href.li/?https://track.redis06.sbs/go/19a45436-cb73-4be8-8e51-
8ee0e9a6e90d?
affiliate=63ba729511d6d&channel=devtek&keyword=streetfighterchampioneditionmodapk&clic
q=streetfighterchampioneditionmodapk&s1=63ba729511d6d&s2=devtek&s3=A1XkF5mpfCQR6KzTkzW
```

This domain is involved with victim logs

> buyurindir.org (Target: Turkish users)

This domain has fake download buttons coded on his pages

```
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/ahttps://href.
https://track.redis06.sbs/go/19a45436-cb73-4be8-8e51-8ee0e9a6e90d?
affiliate=623cb2bc22496&channel=buyurindir&keyword=a&clickid=https://unleakyammiolites
q=a&s1=623cb2bc22496&s2=buyurindir&s3=UiVQynvsuVeg7CmhhJSEf3[Privateloader]
```

This domain is involved with victim logs

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

This domain has fake download buttons coded on his pages

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.

```
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=422023&sub3=86077
[Privateloader]

From clicking the fake
buttonhttps://awdescargas.com/go/aHR0cHM6Ly9hd2xpbmtzLnh5ei8/cD0xNjU5Ng==clickhttps://
url=https://www.greatdexchange.com/jump/next.php?
r=3873611https://page.strtgic.com/click?
pid=10&offer_id=20658&sub1=1706263910000TPTTV415800791604V1f&sub2=422023&sub3=86077[Pr
```

This domain is involved with victim logs

> 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.phphttps://braisingalackadayentr.monster/3or02363a39e65c756
```

This domain is involved with victim logs

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

This domain has fake download buttons coded on his pages

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

https://onclickalgo.com/jump/next.php?r=6058394https://page.strtgic.com/click?
pid=10&offer_id=20738&sub1=17054101901000OTPTTV425055776704V0e&sub2=374483083-
132550085-0&sub3=86077[Privateloader]
```

This domain is involved with victim logs

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

#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.

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 chainhttps://uii.io/full?
api=c292a05bb7dc2de70d01890ac99b711b8992e0be&url=aHR0cHM6Ly9kcml2ZS5nb29nbGUuY29tL2Zpb
 on fake
buttons]https://magpiesblemisherombudsman.com/Uur86779dad79f3b39b84fd4f16176e0fcb6046a
```

And this domain is involved with infostealer infections:

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

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

#2 fc-lc.xyz

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

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

That has more fake buttons redirecting us to the same domain

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

#3 uploadrar.com

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

Example in video:

s0ft4pc.com >> portable4pc.com

```
https://canoestallowrootsabre.com/jKr1Qed15878d1333c59e199f1f0956713d3614ab6b3b?
q=EssentialPIM.Pro.BE.11.8.1.Portable.rar
```

Other domains identified using this service are:

fcportables.com

#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.

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

Example from video:

kmspico.co

#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.

```
https://kuy8h8e.com/jwroWc58c8a6ae95b504791a8c81e29a34c4c9ea2a649?q=Windows 11 23H2
Build 22631.3007 AIO 13in1 Preactivated Multilingual Jan 2024.part1.rar - MegaUp
```

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%20Download%20file%20Vivaldi-v6.5.3206.57-
win64.rar%20(112%2C09%20Mb)%20In%20free%20mode%20%7C%20Turbobit.net?
q=%0A%20%20%20%20Download%20file%20Vivaldi-v6.5.3206.57-
win64.rar%20(112%2C09%20Mb)%20In%20free%20mode%20%7C%20Turbobit.net
```

Example from video:

fullprogramlarindir.net

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/

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

In fact, some .js scripts are stored there

```
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

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.comdaubreeitebumboatmenmisdeal.combluedownload10.sbsunleakyammiolitesmithi
```

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.iofc-lc.xyzuploadrar.comadurly.ccshrinkme.orgturbobit.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/R9SH4IRAUa 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)consciencepropre.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 by Privateloader were taken into account ** /*

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

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

185.161.248.37163.123.143.445.12.253.74109.206.243.208176.113.115.23991.215.85.147209.
```

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:

Transaction #2 — $5000

Transaction 123967b28ca50be06288b37afee86b2d5f2a008a9b3ddf1f3b0bd6995ddd9d6d | TRONSCAN

Source:

```
BTC

bc1qp2rlyxetphma0tv5v87f520h74633ce55hrlfn
```

Transaction #1–0.00260123 BTC

Blockstream Block Explorer

Blockstream Explorer is an open source block explorer providing detailed blockchain data across Bitcoin, Testnet, and…

blockstream.info

Source:

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

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)
```

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:

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

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
 -
https://cdn.discordapp.com/attachments/1189944781556695173/1190293054809178213/release
 -
https://cdn.discordapp.com/attachments/1189944781556695173/1190684453756993536/release
 -
https://cdn.discordapp.com/attachments/1189944781556695173/1190684573965754398/release
```

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.**

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

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)

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.

TRONSCAN | TRON BlockChain Explorer

TRONSCAN is the first blockchain browser in the tron community. It supports multiple login methods and provides a…

tronscan.org

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)

Of course, I can’t determine how true this statement is because it is based only on the review, but *LogsDiller Cloud* is a long-time customer of the InstallsKey service and relies on his traffic installation sources to fill his cloud.

In fact, *asap_rocky* was a customer of the old ruzki PPI service, where he also left a review:

Translated from Russian —

Transaction: 7bbf3afadfae00aa1690662d44246ea38a1fca1fc5aa3bc33b2c1d6c9aff80dc | Blockchain.com

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

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 |
Ddoska176.123.4.46:33783    | @oleh_ps | @ytlogsbot185.216.70.238:37515  |
@oleh_ps194.169.175.235:42691 | YT&TEAM CLOUD | @ytlogsbot |
@oleh_ps176.123.7.190:32927   | @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.

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-easy1543974212-26990097-packlab5904899475-93lhAj6K-
alice678468341-26990097-packlab678468341-26990097-alice678468341-26990097-
easy6663705738-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: installs213.21.220.222:8080 | 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:

```
@Chicagotraficomusor1mixBigBossmitro2@Chicacgominamisagogamusamundermaximetro29.05.202
 cloud yt wq12lux3Stukaet normMr
Leungjokerrt2prolivkawertamazajasongrom1006@nudikq1haresBOGO2muchart243rt5narkobuil1Lc
6-111MILtaigaFILE1getmoney16.11.23_ObhordaLiveTraffic1124newTEST1132kPREMIUM1193-
1201new1PREMIUMwork001word13371211-55000work13371214-550001215-550001216-
550006661217-55000newestwork28.71219-55000uniq2newsss24k
```

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)
```

```
GhYTuYBVgYtiV566Iu--inerinoVcFuIq88BbUqV566Iu--sdelkaOpUUUyYTghyIGyVvdOiOqpIq--
gr5555555ZomIjNVgYiqp--GRRrM068VgYiqp--gergRyInGu--LylaBundle09.10HVvByi--
source1Zaaaac--pw7HqweNgRyInGu--BarretBundleRyInGu--Hook17.10HvBvV9--DirtyhJgToq--
dozkeyRyInGu--Lyla3Zaaaac--oi2Zaaaac--oi5Zaaaac--oi7SaRBgiHVvByi--bundleHHhUQl--
newHvBvV9LGNDRY996NvtC1TNmL97HgTiYmMYnuPeDDloPeRFCk--doZkeyAmNsA2--backdoWgJyoO--
bSvBmLBAmNsA2--ausMV90NvWgJyoO--testedT1mOs2NmLpQW--spam2AmNsA2--uniqAmNsA2--
legAmNsA2--unicalWWH111LPnhqo--@usernemer9FATE99--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):

```
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”

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.

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.

@g0njxa | Also available at t.me/privateloader (EN & RU)