INTRINSEC

Innovative by design

CryptBot: Hunting for intial access vectors

Cyber Threat Intelligence

December 2024

@Intrinsec @Intrinsec Blog Website

Table of contents

1. Key findings

- **CryptBot** continues to be deployed mainly from websites offering **fake cracked software** and "**Pay-Per-Install**" solutions like **PrivateLoader** (also known as "**InstallsKey**" on Telegram) or the now defunct **360Installer**.

- By searching for the **Matomo tracking script** used by the threat actor to get web statistics measurement on its campaigns, we were able to retrieve **every domain** that hosted CryptBot throughout time and the ones currently hosting it. We also found that in some cases, those domains were redirecting to **Lumma** payloads loaded by **HijackLoader** depending on the URL the user was originating from.

- Through the analysis of the websites offering infected versions of cracked software, we were able to **pivot** on certain OPSEC errors made during their setup to find **additional malicious websites** with the same purpose of distributing CryptBot.

- Both CryptBot and PrivateLoader continue to use **bulletproof hosting solutions** such as the infamous *"Aeza International Ltd"* and "*Karina Rashkovska*" to host their phishing pages, command-and-control panels, and malware payloads overall. We notably highlight how "*Psb Hosting Ltd*", a company based in the United Kingdom and run by a Russian individual, now possesses an IPv4 range previously owned by *Karina Rashkovska,* and how this company promotes its bulletproof hosting capacities on underground forums.

- The **Amadey** cluster hosted by the Seychellois autonomous system "*1337TEAM LIMITED*" that was first analysed by *Team Cymru*'s threat research team in September 2022, continues its activities with the latest version of the malware (version **4.41**), to push additional payloads including **CryptBot**, **Lumma**, **Redline** and **Stealc**.

2. Introduction

First discovered in 2019, **CryptBot** is a 32-bit infostealer designed to exfiltrate various sensitive information from an infected system and eventually later sell them to other threat actors as initial access vectors for more complex data breach campaigns. Its main spreading technique is based on the distribution of infected cracked versions of commonly used software. In a lesser volume, CryptBot also relies on other threat actors to expend its botnet of infected machines like for example the "**Pay-Per-Install**" service named "**InstallKeys**" still active on Telegram, that offers access to the machines it infects through its personal malware named **PrivateLoader**. In addition to this service, Mandiant discovered in August 2024 that "**PeakLight**", a memory-only dropper spreading through fake video files, was used to deploy CryptBot along other malwares such as LummaC2 and ShadowLadder[1].

[1] *https://cloud.google.com/blog/topics/threat-intelligence/peaklight-decoding-stealthy-memory-only-malware?hl=en*

Regarding other deployments of the malware, Mandiant assessed with moderate confidence in 2021 that the **state-sponsored Russian intrusion set APT29** used logs stolen by CryptBot operators to gain a foothold in the system of a targeted entity.[2] As CryptBot is designed to steal the user content of some internet browsers including **Google Chrome**, *Google* decided to file a complaint against fifteen Pakistani individuals believed to be running the malware's "*criminal enterprise*". Additionally, other software owned by Google such as Google Earth Pro were part of the long list of programs infected with CryptBot and advertised on these fake websites. In the complaint file provided by the Southern District court of New York, Google also mentions that infected cracked software distribution alone had led to approximately **672,220 CryptBot infections** between 2022 and 2023.[3] This information was corroborated by *Prodaft* in a tweet from August 2023, in which they mentioned that more than **17 million unique devices worldwide** had been infected by the malware in the last 5 years.[4] Following this complaint, the court decided to grant Google the right to take down current and future domains tied to the distribution of CryptBot. Google stated that decision would "*slow new infections from occurring and decelerate the growth of CryptBot*".

The numbers indeed crashed to **40,581 infections in 2023** according to *Prodaft*[5]. However, despite those actions, Intrinsec CTI team observed new domains registered in **September 2024** used as CryptBot C2s, or to host and deploy its payloads along additional malwares such as **Lumma**. With this report, we aim to notably present the current infrastructure leveraged by threat actors to maintain the malware, as well as the methods of distribution it presently uses to maximise the growth of its botnet.

3. Sources of infections observed in September

3.1. Search Engine Optimization

As mentioned in the introduction of this report, CryptBot is mainly distributed through cracked versions of commonly used software. The websites offering those software tend to be quite good in Search Engine Optimization as they often appear in the first results of most browsers when looking for cracked programs. For example, in the figure below (*Figure 1*), we tried to see what websites would be put forward by Google when searching for a cracked version of "*Wondershare Filmora*", a video editing software frequently used by professionals. Out of the first four websites displayed by Google, the first one (**haxpc**[.]**net**) was already offering a version of the software infected with **CryptBot**.

[2] *https://cloud.google.com/blog/topics/threat-intelligence/russian-targeting-gov-business/?hl=en*
[3] *https://regmedia.co.uk/2023/04/28/handout_google_cryptbot_complaint.pdf*
[4] *https://x.com/PRODAFT/status/1687107709626363905*
[5] *https://x.com/PRODAFT/status/1687107709626363905*

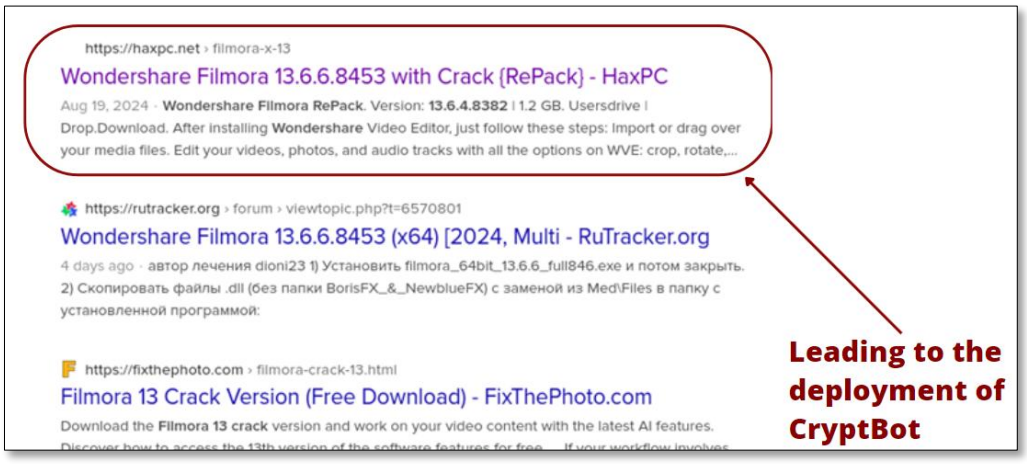


Figure 1. Google results when searching for cracked versions of Wondershare Filmora.

Sometimes the websites were typosquatted domains of legitimate software distributers like "filecr[.]com" from which a malicious domain "**filecrr**[.]**org**" was mimicking the landing page and name. In the figure below (*figure 2*), this fake website was distributing a version of Windows Professional also infected with CryptBot.

Figure 2 Website distributing an infected version of Windows 10 Professional.

The email address "**filecrr.org**@**gmail**[.]**com**" linked to the website, was registered on LinkedIn and other various websites like Quora and Pinterest, with what we believe to be for SEO purposes as the infected cracked software were being advertised on these websites with this account.

The location provided by the account on LinkedIn pointed to **Pakistan**, which matches with the nationality of the defendants accused by Google of running CryptBot's distribution. Additionally, the mail server "**mx1.hosting**[.]**pk**", used to register "**filecrr**[.]**org**", happened to be a **Pakistani server** provided by Hostinger, as the TLD indicates.

Figure 3. LinkedIn account registered with the email address linked to filecrr[.]org.

Overall, all those malicious websites came in different languages and offered a wide range of commonly used software.

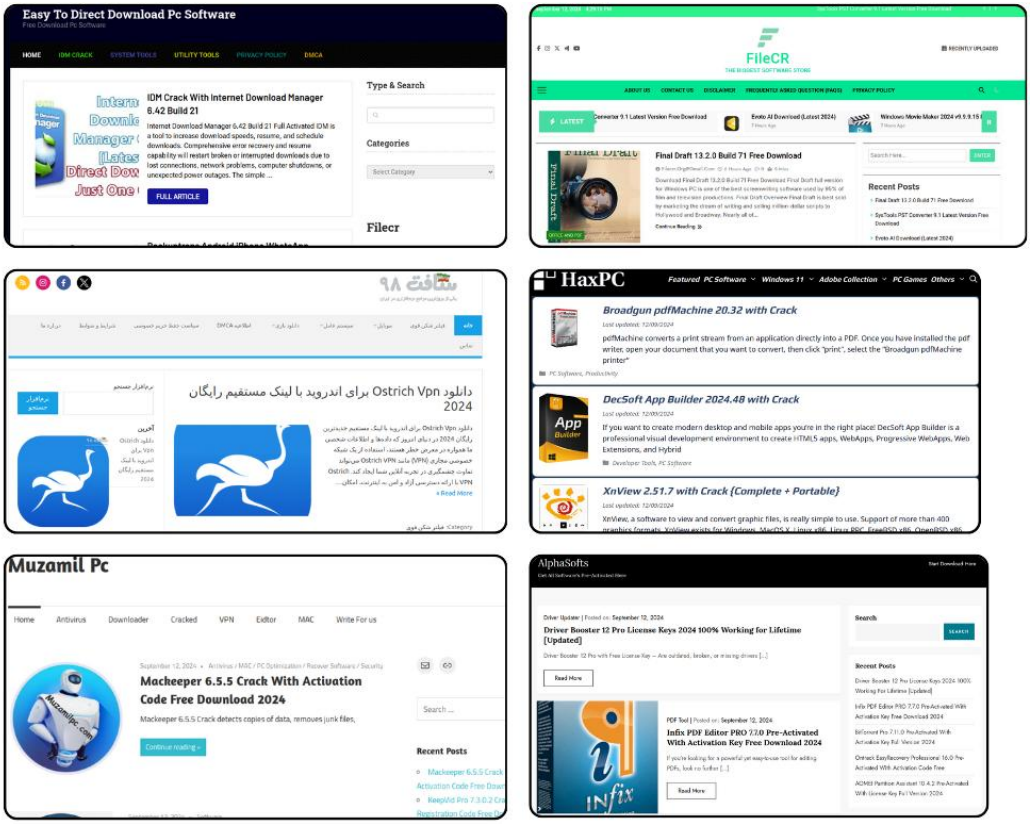


Figure 4. Snippet of different websites distributing infected cracked software.

3.1.1. Domains hosting the download links

Once a user tries to download a software from those websites, they get redirected to another page displaying a **Mega** or **Dropbox** link to a password protected archive.

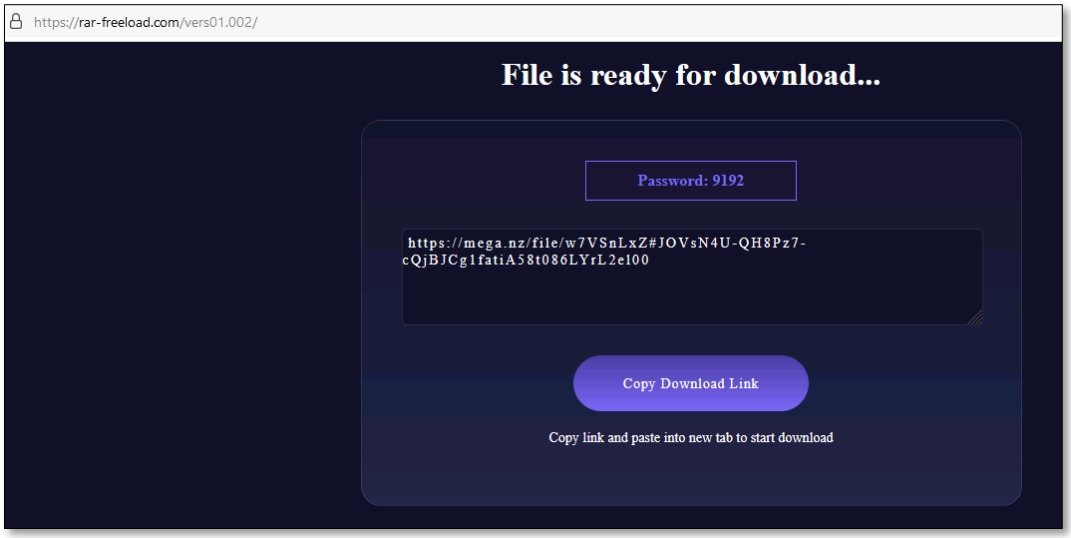


Figure 5. Domain displaying a link to a Mega folder with the password of the archive hosted on it.

The page is available in other languages, including **Russian**, **French**, **Spanish**, and **German**. If the visiting system is not from those countries, it just displays it in English by default.

```
<script type="text/javascript">
        const translations = {
            "en": {
                "title": "Download File",
                "header": "File is ready for download...",
                "password": "Password:",
                "button": "Copy Download Link",
                "instruction": "Copy link and paste into new tab to start download",
                "copied": "Link Copied!! Open in New Tab"
            },
            "es": {
                "title": "Descargar archivo",
                "header": "El archivo está listo para descargar...",
                "password": "Contraseña:",
                "button": "Copiar enlace de descarga",
                "instruction": "Copie el enlace y péguelo en una nueva pestaña para comenzar la descarga",
                "copied": "¡Enlace copiado! Ábralo en una nueva pestaña"
            },
            "fr": {
                "title": "Télécharger le fichier",
                "header": "Le fichier est prêt à être téléchargé...",
                "password": "Mot de passe:",
                "button": "Copier le lien de téléchargement",
                "instruction": "Copiez le lien et collez-le dans un nouvel onglet pour commencer le téléchargement",
                "copied": "Lien copié ! Ouvrez-le dans un nouvel onglet"
            },
            "de": {
                "title": "Datei herunterladen",
                "header": "Datei ist zum Download bereit...",
                "password": "Passwort:",
                "button": "Download-Link kopieren",
                "instruction": "Kopieren Sie den Link und fügen Sie ihn in ein neues Tab ein, um den Download zu starten",
                "copied": "Link kopiert! Öffnen Sie ihn in einem neuen Tab"
            },
            "ru": {
                "title": "Скачать файл",
                "header": "Файл готов к загрузке...",
                "password": "Пароль:",
                "button": "Скопировать ссылку для загрузки",
                "instruction": "Скопируйте ссылку и вставьте в новую вкладку, чтобы начать загрузку",
                "copied": "Ссылка скопирована! Откройте в новой вкладке"
            }
        };
```

Figure 6. Snippet of the JS code contained in the source code of the page.

Firebase hosting

On a Russian website distributing torrents for games and generic software, the provided link containing the URL to the Mega/Dropbox folder happened to be hosted on a Firebase instance instead of the previous self-crafted website.

*Figure 7. Snippet of the page distributing and alleged Russian version of Windows 10 on **only-soft**[.]**org**.*

Only two days later, this instance would be taken down by Google. The website offering the cracked software thus switched back to a generic domain "**rar-freeload**[.]**com/vers01.0011**", crafted by the threat actor. Despite Google's complaint, CryptBot continues to be distributed through Google solutions like Firebase. We can nonetheless acknowledge Google's reactivity regarding the takedown time laps.

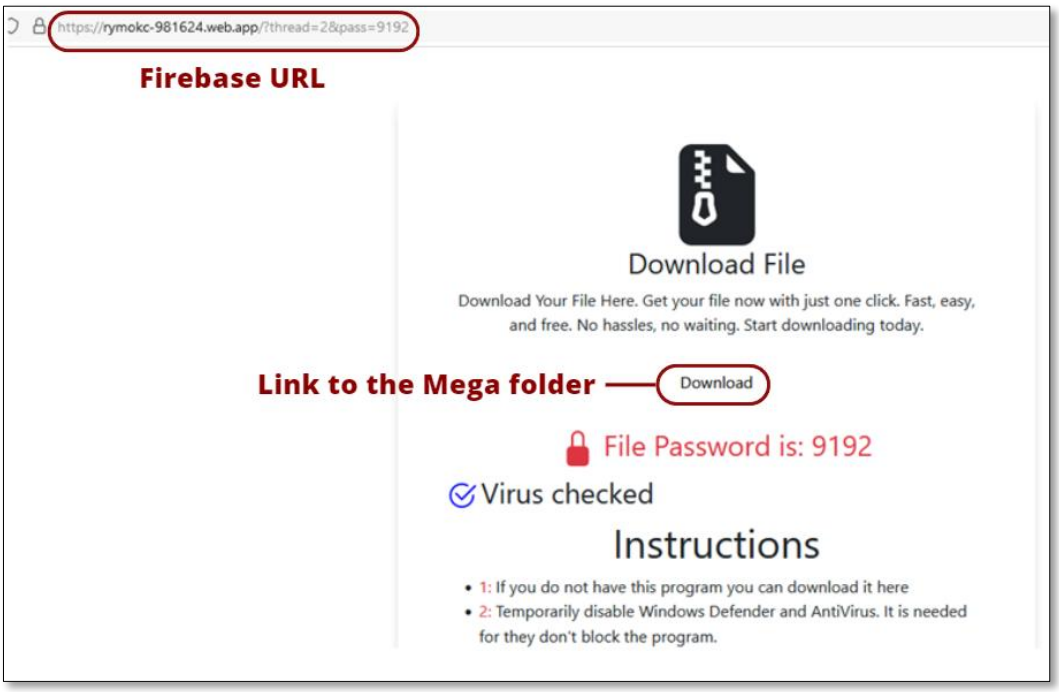


Figure 8. Firebase page redirecting to the Mega folder containing the CryptBot archive.

3.1.2. The CryptBot payload

Once we download the archive and decrypt it with the previously provided password, we obtain part of the legitimate software along with an executable named "**Set-up.exe**"; being the actual **CryptBot** malware.

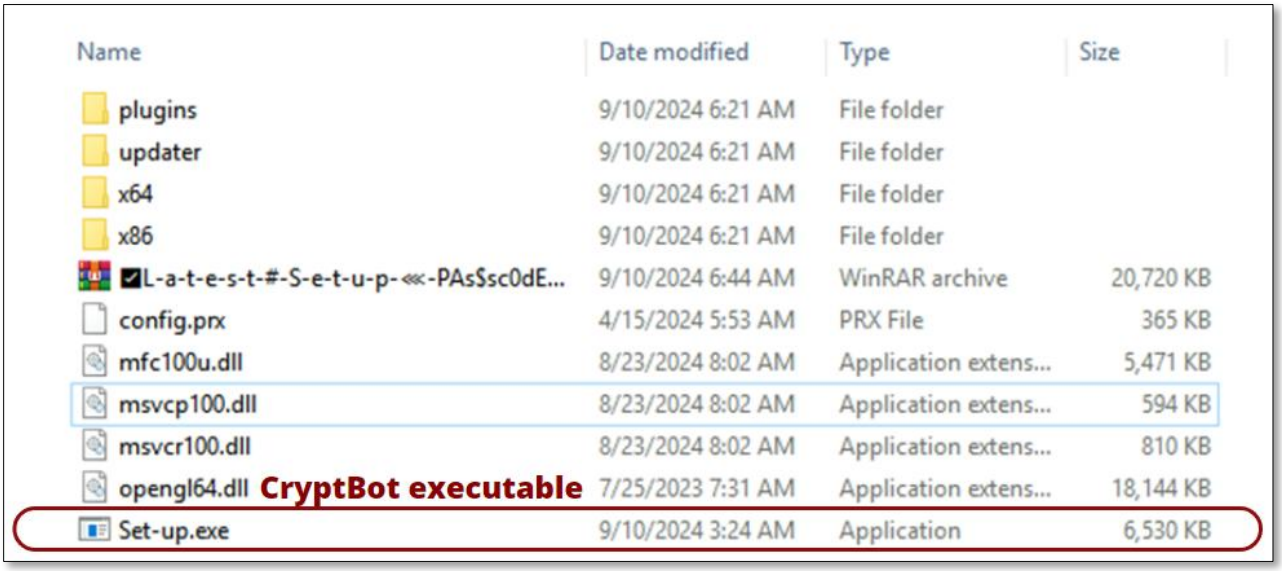


Figure 9. Content of the downloaded archive.

To remain persistent on the system, CryptBot copied itself in *AppData\Local\Temp* under the name "**service123.exe**" and created a schedule task with *schtasks.exe* named "**ServiceData4**", in order for the copy of the malware to launch at every start of the system.

```
"C:\Windows\System32\schtasks.exe" /create /tn "ServiceData4" /tr "C:\Users\
<USER>\AppData\Local\Temp\/service123.exe" /st 00:01 /du 9800:59 /sc once /ri 1 /f
```

Figure 10. Schtasks command launched by the CryptBot executable at launch to stay persistent.

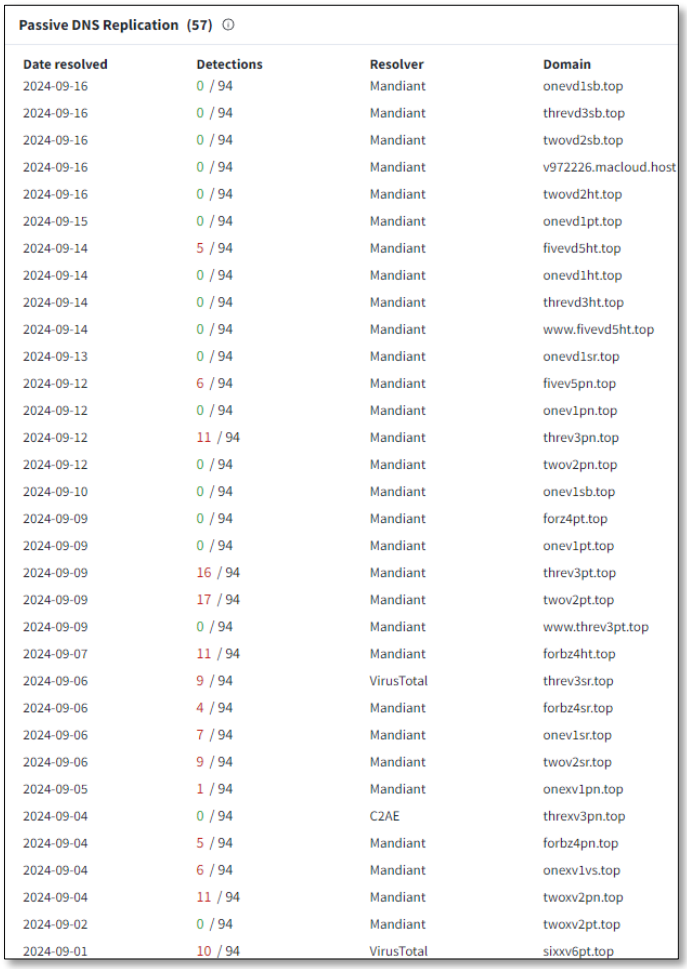
To avoid reinfecting the same host, CryptBot created a mutex in:

- *\Sessions\1\BaseNamedObjects\QLEvFWjDaxiNdJEADjHk*

After collecting the login information of the browsers installed on the system, CryptBot exfiltrated the data by saving it in a seemingly encrypted file with a random name "**Kecavase.bin**" and sent it to its C2 with URL: "**twov2pn**[.]**top/v1/upload.php**".

Figure 11. Content of the POST request that CryptBot sent to its C2.

The IP **185.244.181**[.]**38** the C2 domain resolved happens to resolve many other domains generated with CryptBot's DGA algorithm.



Passive DNS Replication (57)

Date resolved	Detections	Resolver	Domain
2024-09-16	0 / 94	Mandiant	onevd1sb.top
2024-09-16	0 / 94	Mandiant	threvd3sb.top
2024-09-16	0 / 94	Mandiant	twovd2sb.top
2024-09-16	0 / 94	Mandiant	v972226.macloud.host
2024-09-16	0 / 94	Mandiant	twovd2ht.top
2024-09-15	0 / 94	Mandiant	onevd1pt.top
2024-09-14	5 / 94	Mandiant	fivevd5ht.top
2024-09-14	0 / 94	Mandiant	onevd1ht.top
2024-09-14	0 / 94	Mandiant	threvd3ht.top
2024-09-14	0 / 94	Mandiant	www.fivevd5ht.top
2024-09-13	0 / 94	Mandiant	onevd1sr.top
2024-09-12	6 / 94	Mandiant	fivev5pn.top
2024-09-12	0 / 94	Mandiant	onev1pn.top
2024-09-12	11 / 94	Mandiant	threv3pn.top
2024-09-12	0 / 94	Mandiant	twov2pn.top
2024-09-10	0 / 94	Mandiant	onev1sb.top
2024-09-09	0 / 94	Mandiant	forz4pt.top
2024-09-09	0 / 94	Mandiant	onev1pt.top
2024-09-09	16 / 94	Mandiant	threv3pt.top
2024-09-09	17 / 94	Mandiant	twov2pt.top
2024-09-09	0 / 94	Mandiant	www.threv3pt.top
2024-09-07	11 / 94	Mandiant	forbz4ht.top
2024-09-06	9 / 94	VirusTotal	threv3sr.top
2024-09-06	4 / 94	Mandiant	forbz4sr.top
2024-09-06	7 / 94	Mandiant	onev1sr.top
2024-09-06	9 / 94	Mandiant	twov2sr.top
2024-09-05	1 / 94	Mandiant	onexv1pn.top
2024-09-04	0 / 94	C2AE	threxv3pn.top
2024-09-04	5 / 94	Mandiant	forbz4pn.top
2024-09-04	6 / 94	Mandiant	onexv1vs.top
2024-09-04	11 / 94	Mandiant	twoxv2pn.top
2024-09-02	0 / 94	Mandiant	twoxv2pt.top
2024-09-01	10 / 94	VirusTotal	sixxv6pt.top

Figure 12. Snippet of the list of domains hosted on the above-mentioned IP.

The following layout aims to summarize the overall kill chain related to a CryptBot infection.

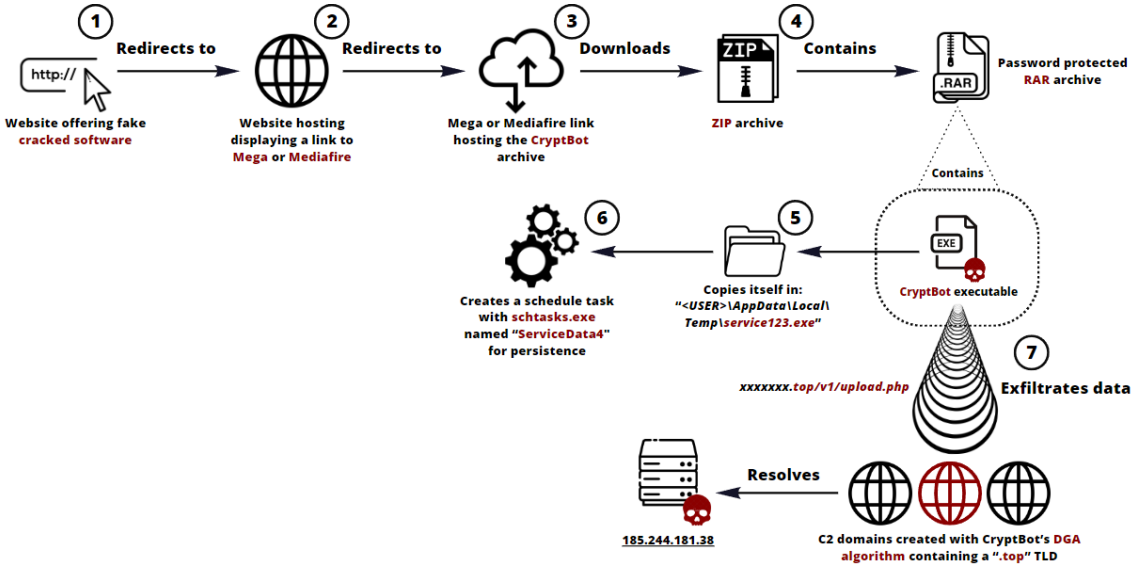


Figure 13. Layout of CryptBot's kill chain.

3.2. Deployed by PrivateLoader

CryptBot also relies on "**Pay-Per-Install**" services such as **InstallKeys** on Telegram, which offers access to machines by downloading its clients' malwares on the systems that it previously infected with **PrivateLoader**. Like CryptBot, this service infects its victims through SEO and cracked software.

In the month of **September**, user "iamaachum" on MalwareBazaar observed that CryptBot was indeed being deployed by PrivateLoader payloads when the system language was set to **Italian**.[6] Once infected by PrivateLoader, CryptBot would be downloaded from the following URLs:

- *147.45.44[.]104/prog/66dd5fafdeab3_lyla.exe*
- *147.45.44[.]104/revada/66deebee3b2d7_lyla2.exe*
- *147.45.44 [.]104/lopsa/66e2d83e11e31_lyla3.exe*
- *147.45.44[.]104/yuop/66e1de4b31f49_lyla23.exe*
- *103.130.147[.]211/Files/1.exe*
- *103.130.147[.]211/Files/Channel3.exe*
- *103.130.147[.]211/Files/Channel4.exe*

PrivateLoader currently communicates with the following command-and-control servers:

- *45.91.200[.]135/api/crazyfish.php*
- *147.45.47[.]169/api/crazyfish.php*
- *212.113.116[.]202/api/crazyfish.php*
- *62.133.61[.]172/api/crazyfish.php*
- *92.246.139[.]82/api/crazyfish.php*

[6] *https://bazaar.abuse.ch/user/14172/*

3.2.1. Leveraging bulletproof hosting solutions

As you can observe, PrivateLoader uses IPs from ranges **147.45.47**[.]**0/24** and **147.45.47**[.]**0/24** which are part of the **Ukrainian autonomous system** named "*Karina Rashkovska*" (**AS215789**). *In a previous investigation*[7], Intrinsec CTI Team linked this network to a bulletproof hosting solution named "Marshall Servers", currently advertised on underground forums. We also believe *with a high level of confidence* that this service is run by a **Byelorussian individual** named "**Aliaksei Bolbas**" leading the company "*Waicore Hosting LTD.*" registered in the United Kingdom. The mail server of the company "mail.waicore[.]com" happened to be hosted on **185.106.92**[.]**254**, an IP now owned by "*PSB Hosting Ltd*" (AS214927), the new owner of the IPv4 range **82.115.223**[.]**0/24** that *Karina Rashkovksa* used to possess.

Composed of four IPv4 ranges, this autonomous system based in the UK can also be linked to a bulletproof hosting service named "*PSB Offshore*" which promotes its services on underground forums with the mention: "*Bulletproof servers with a wide range of acceptable content*". We indeed previously reported how threat actors linked to Russia like **UAC-0006** and **Latrodectus** decided to host some of their infrastructure on this network, at a time where it was only composed of one IPv4 range[8]. The director of the company *PSB HOSTING LTD* is a Russian individual named "**Skipin Vladislav Andreevich**". In addition to AS "*Karina Rashkovksa",* PrivateLoader also used IPs from Russian bulletproof hosting solution "*Aeza International Ltd*" (**AS210644**), including **92.246.139**[.]**82** and **212.113.116**[.]**202**, as C2 servers.

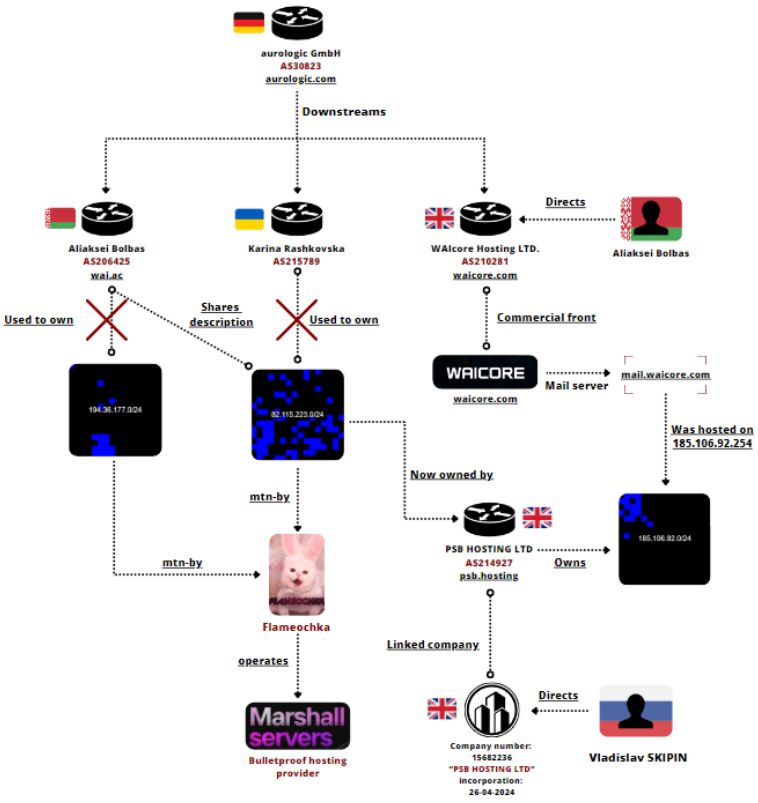


Figure 14. Layout of the links made between the above-mentioned entities.

[7] Intrinsec private report. "*Identifying Upstream Providers Peering with Bulletproof Networks*". July 2024.
[8] Intrinsec private report. "*Unveiling UAC-0006's Infrastructure and Operations on Ukraine's assets and its Allies throughout 2024*". July 2024.

3.3. Deployed by SmokeLoader

In addition to PrivateLoader, we observed that **SmokeLoader**, another Russian loader sold on underground forums that also spreads through cracked software, was being used to deploy CryptBot throughout September. The malware was downloaded from the same URL as the one PrivateLoader used: "*103.130.147*[.]*211/Files/Channel3.exe*". We believe that SmokeLoader was only used as a dropper since it did not communicate with the C2s contained in its configuration and only downloaded CryptBot along other malwares.

The following SmokeLoader command-and-control domains could nonetheless be found in the malware's code (2022 version):

- *epohe*[.]*ru/tmp/*
- *olihonols.in*[.]*net/tmp/*
- *nicetolosv*[.]*xyz/tmp/*
- *jftolsa*[.]*ws/tmp/*

CryptBot communicate with only one command-and-control domain contained in its configuration:

- *thirtv13pn*[.]*top/v1/upload.php* (resolved IP 195.133.13[.]230)
- *analforeverlovyu*[.]*top/v1/upload.php*

The IP of this single C2 was hosting a trove of other similar DGA generated domains used as CryptBot C2s:

Passive DNS Replication (100)

Date resolved	Detections	Resolver	Domain
2024-09-14	12 / 94	VirusTotal	fiftvd15pt.top
2024-09-14	0 / 94	Mandiant	forvd14pt.top
2024-09-14	13 / 94	Mandiant	forvd14sr.top
2024-09-14	5 / 94	Mandiant	thirtvd13pt.top
2024-09-14	4 / 94	VirusTotal	elevenvd11pt.top
2024-09-14	2 / 94	Mandiant	twelvevd12pt.top
2024-09-14	3 / 94	Mandiant	fiftvd15ht.top
2024-09-14	14 / 94	Mandiant	sevtvd17ht.top
2024-09-14	14 / 94	Mandiant	sixvd16ht.top
2024-09-13	12 / 94	Mandiant	elevenvd11sr.top
2024-09-13	8 / 94	Mandiant	fiftvd15sr.top
2024-09-13	10 / 94	Mandiant	sevtv17pn.top
2024-09-13	11 / 94	Mandiant	sevtvd17sr.top
2024-09-13	11 / 94	Mandiant	sixv16pn.top
2024-09-13	10 / 94	Mandiant	sixvd16sr.top
2024-09-13	8 / 94	Mandiant	tenvd10sr.top
2024-09-13	10 / 94	Mandiant	thirtv13pn.top
2024-09-13	13 / 94	Mandiant	thirtvd13sr.top
2024-09-13	11 / 94	Mandiant	twelvevd12sr.top
2024-09-13	0 / 94	Mandiant	www.twelvevd12sr.top
2024-09-12	6 / 94	Mandiant	fiftv15pn.top
2024-09-12	4 / 94	Mandiant	forv14pn.top
2024-09-10	15 / 94	Mandiant	elevenv11sb.top
2024-09-10	16 / 94	Mandiant	fiftv15sb.top
2024-09-10	13 / 94	Mandiant	forv14sb.top
2024-09-10	13 / 94	Mandiant	sixv16sb.top
2024-09-10	15 / 94	Mandiant	thirtv13sb.top
2024-09-10	13 / 94	Mandiant	twelvev12sb.top
2024-09-10	0 / 94	Mandiant	www.fiftv15sb.top
2024-09-10	0 / 94	Mandiant	www.forv14sb.top

Figure 15. Snippet of the domains hosted on IP 195.133.13[.]230.

3.4. Deployed by the Seychellois Amadey cluster

Two years ago, in September 2022, Team Cymru's research team reported on an Amadey cluster hosted on an anonymous autonomous system based in **Seychelles** (initially declared as **Russian** before November 2020[9]) named "*1337TEAM LIMITED*" (**AS51381**) that shares 100% of its peering agreements with a **Russian** autonomous system named "*Storm Networks LLC*" (**AS43298**).[10] As a reminder, Amadey is Remote Access Trojan (RAT) sold underground forums by a Russian-speaking user named "**InCrease**". The Amadey C2s were hosted on the only IPv4 range of this autonomous system "**185.215.113**[.]**0/24**" The other autonomous systems registered by the company (**AS60424**, **AS56873** and **AS39770**) did not announce any IPv4 ranges.

We noticed that this cluster was **still online** and was now using the **latest version** of Amadey released in August (version **4.41**, botnet IDs: **fed3aa** & **1176f2**) to deploy **CryptBot** during the month of **September 2024**, along other malwares such as **Redline**, **Stealc** and **Lumma**.

CryptBot happened to be downloaded from the **same IP** as the one we found in the PrivateLoader and SmokeLoader campaigns:

- *103.130.147*[.]*211/Files/2.exe*
- *103.130.147*[.]*211/Files/Channel4.exe*

The first Amadey payload named "**ednfoki.exe**" associated to botnet "**1176f2**", communicated with the following C2:

- *185.215.113*[.]*19/CoreOPT/index.php*

The second Amadey payload named "**apxlong.exe**" associated to botnet "**fed3aa**", communicated with the following C2:

- *185.215.113*[.]*16/Jo89Ku7d/index.php*

Overall, This C2 was used to host more than around **70,000 bots** since its creation.

Figure 16. Number of infected systems that connected to the C2.

[9] *https://bgpranking.circl.lu/asn*
[10] *https://www.team-cymru.com/post/seychelles-seychelles-on-the-c-2-shore*

Regarding the other malwares that were deployed by these Amadey campaigns, the Redline payload communicated with IP "**65.21.18**[.]**51**" on port **45580** and was associated to the botnet ID "**@OLEH_PSP**". This is a reference signature to the Telegram channel of the same name that sells logs stolen by infostealers, inducing that the owner of this channel "**KomandoR**" (now banned from XSS forum) has indeed control over this Redline botnet.

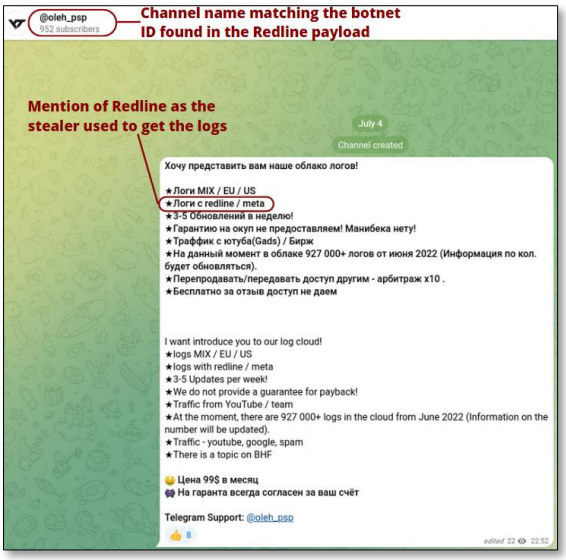


Figure 17. Telegram channel allegedly in control of the previously found Redline payload.

We believe that this Amadey cluster could be owned by bigger "*traffers*" selling traffic to those kinds of Telegram channel, as multiple other stealers with C2s hosted by different AS other than *1337TEAM LIMITED* were deployed. We unfortunately could not associate the rest of those payloads to any known botnet or Telegram channel.

The Stealc payload for example, communicated with a different Russian bulletproof autonomous system named "*PROSPERO OOO*" (**AS200593**), with a C2 hosted on IP **91.202.233**[.]**158**. This autonomous system indeed mainly hosts criminal activities on its network,[11] and in particular a major part of Gootloader's infrastructure.[12] We have notably released a public report on Intrinsec's blog regarding this network.

PROSPERO OOO
The Russian autonomous system *PROSPERO OOO* (**AS200593**) could be linked with a high level of confidence to *Proton66 OOO* (**AS198953**), another Russian AS, that we believe to be connected to the bulletproof services named "**SecureHost**" and "**BEARHOST**". The connection between PROSPERO and Proton66 could be made through similarities in the way both networks are operated, notably in their respective peering agreements shared with other Russian networks.[13]
SecureHost is a bulletproof hosting provider advertised since 2022 on underground Russian-speaking forums. It notably declares ignoring DMCA and Spamhaus requests. The servers are located in Russia, with a direct access to an Internet Exchange Point (IX).

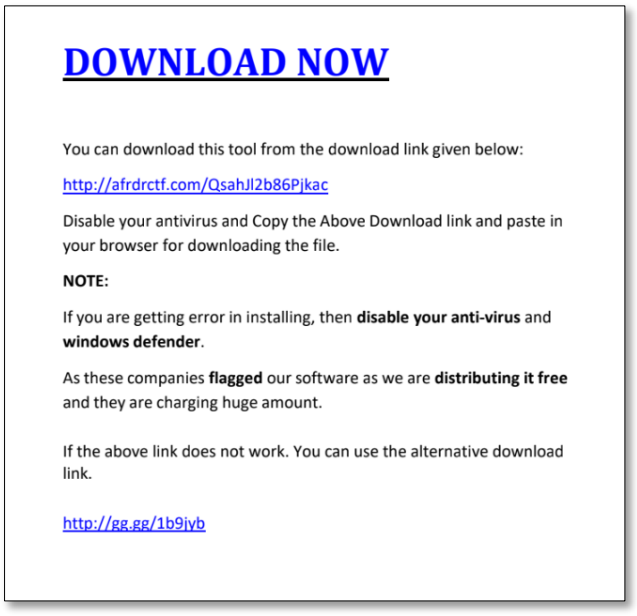
[11] *https://web.archive.org/web/20231018093233/https:/oliverhough.io/prospernot-prospero-as-the-little-as-that-could-part-1/*

[12] *https://x.com/Gootloader/status/1778786008219128088*

[13] https://www.intrinsec.com/wp-content/uploads/2024/11/TLP-CLEAR-PROSPERO-Proton66-Uncovering-the-links-between-bulletproof-networks.pdf

3.5. Deployed through PDF documents

CryptBot is also currently being deployed through PDF documents displaying fake instructions for downloading cracked commercial software. The instructions contained in the document simply ask the user to disable their anti-virus and click on a provided link that happens to redirect to the domains we previously found (see "3.1.1. Domains hosting the download links" part of this report).



DOWNLOAD NOW

You can download this tool from the download link given below:

http://afrdrctf.com/QsahJl2b86Pjkac

Disable your antivirus and Copy the Above Download link and paste in your browser for downloading the file.

NOTE:

If you are getting error in installing, then **disable your anti-virus** and **windows defender**.

As these companies **flagged** our software as we are **distributing it free** and they are charging huge amount.

If the above link does not work. You can use the alternative download link.

http://gg.gg/1b9jyb

Figure 18. Content of one of those malicious PDF documents.

This specific PDF file was contained in many archives downloaded from websites distributing cracked software. As one can observe in the figure below (*figure 18*), the archives' names could give us a hint of which software were targeted and spoofed.

Compressed Parents (32)

Scanned	Detections	Type	Name
2024-07-06	2 / 63	RAR	Atoll 3.4.0.15114 Key Generator Full Version & Keys 2023 100 % Working.rar
2024-07-09	2 / 64	ZIP	Embraer Erj Family.zip
2024-07-11	6 / 63	RAR	Zoom Math 500 Portable Free Download.rar
2024-07-12	6 / 65	ZIP	Naughty America Login And Password.zip
2024-07-14	6 / 65	ZIP	Parashara Light 9.0 Activation Code Generator Download.zip
2024-07-19	6 / 67	ZIP	Free Video To Gif Converter Portable Download & Activation Code.zip
2024-07-19	6 / 63	RAR	Free Video To Gif Converter Portable Download With Activator.rar
2024-07-19	6 / 65	ZIP	Mod Apk Minecraft Mod.bin
2024-07-26	6 / 54	RAR	Rustangelo Pro Preactivated.rar
2024-07-26	6 / 64	RAR	Scrivener Download Cracked.rar
2024-07-27	6 / 66	ZIP	Gsa Search Engine Ranker Cracked Free Download.zip
2024-07-28	6 / 64	RAR	The Villain Simulator Download.rar
2024-08-01	6 / 66	ZIP	Super Email Validator V4.3.zip
2024-08-01	6 / 66	ZIP	Faro Cam2 Software Download.zip
2024-08-01	6 / 64	RAR	Faro Cam2 2020 Download.rar
2024-08-04	6 / 62	RAR	Zbrush 4.0 Activation Code.rar
2024-08-06	8 / 66	ZIP	Steam Vdf File.zip
2024-08-11	8 / 66	ZIP	Net Share Pro Apk.zip
2024-08-31	22 / 67	ZIP	Surgeon Simulator Vr Oculus Quest 2.zip
2024-09-03	22 / 68	ZIP	Recurbate Downloader 1.9.9.7 Full Version.zip
2024-08-15	8 / 64	RAR	Baixar Cheat Omatic.rar
2024-08-25	8 / 64	RAR	Esoteric Spine 2D Version 4.2 Rar.rar
2024-08-27	9 / 64	RAR	Black Myth Wukong Steam.rar
2024-09-08	21 / 65	ZIP	Launchbox License Xml Download.zip
2024-09-02	8 / 64	RAR	Youwave 3.22 Activation Key Activation Code Download.rar
2024-09-08	19 / 66	ZIP	Naboota Full Version With Activator.zip
2024-09-06	8 / 62	RAR	Telerik Ui For Winforms Full Cracked.rar
2024-09-07	7 / 62	RAR	Fmrte License Key Generator.rar
2024-09-09	8 / 63	RAR	Proxyfire Master Suite.rar
2024-09-09	8 / 63	RAR	Mediachips Preactivated Download + License Key Download.rar
2024-09-09	8 / 63	RAR	mediaChips Key Generator + License Key Download.rar
2024-09-09	8 / 63	RAR	mediaChips Cracked + License Key Download.rar

Figure 19. Snippet of the list of archives that deployed the above-mentioned PDF document.

4. Following Matomo to find the redirecting domains

All the domains that provided the URL to the Mega folder containing CryptBot's archive used a **Matomo tracking script**. As a reminder, Matomo, like Google Analytics, is a web analytics software platform providing detailed reports on a website and its visitors. This includes the search engines and keywords they used, the language they speak, which pages they like, **the files they download** and other various things.

This tracking script named "**track.js**", sent all those details to "**mtmoweb**[.]**website**", a Matomo instance operated by the threat actor. We believe that the threat actor uses this method to get an overview of which websites distributing cracked software generate the most traffic and with which software specifically to improve their campaigns. This could even be a way for the threat actor to remunerate the individuals operating those websites according to the amount of traffic they generate.

```
var MATOMO_URL = "mtmoweb.website";
var SITE_ID = '19';

var _paq = window._paq = window._paq || [];
/* tracker methods like "setCustomDimension" should be called before "trackPageView" */
_paq.push(['trackPageView']);
_paq.push(['enableLinkTracking']);
(function() {
var u="https://" + MATOMO_URL + "/";
_paq.push(['setTrackerUrl', u+'matomo.php']);
_paq.push(['setSiteId', SITE_ID]);
var d=document, g=d.createElement('script'), s=d.getElementsByTagName('script')[0];
g.async=true; g.src=u+'matomo.js'; s.parentNode.insertBefore(g,s);
})();
```

Figure 20. Content of the "track.js" script.

By scanning websites containing this specific script, we were able to track every domain hosting the URL link to the Mega folder distributing CryptBot infected archives (see "Indicators of compromise" section of this report for the full list). The figure below (*figure 20*) aims to summarize the followed method:

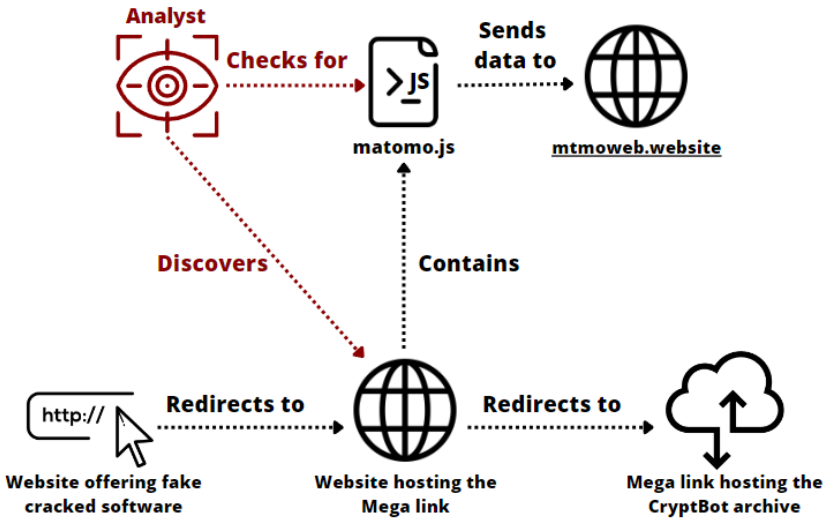


Figure 21. Layout summarizing the method employed to track the domains redirecting to the Mega folders.

4.1. Domains hosted by Aeza servers in France

Retrieving those domains enabled us to get an overview of how they were operated throughout time. We noticed that they were fronted by either *DDOS-Guard* – AS57724 (a Russian Cloudflare-like solution) or directly by *Cloudflare* – AS13335; thus, hiding the real IP of the servers hosting them. However, some of them would sometime not be fronted by those services and directly revealing their IP.

When not fronted, all those domains were hosted on one of the two autonomous systems managed by the **Russian bulletproof hosting provider Aeza**, being either **AS210644** (*Aeza International Ltd*) or **AS216246** (*Aeza Group Ltd.*). One IP, **147.45.68**[.]**130**, managed by AS210644 and apparently located in **France**, was hosting redirecting domains with instructions displayed in French. The other IP that we mostly observed to be hosting the same domains was located in Russia and managed by AS216246 (**185.112.83**[.]**145**).

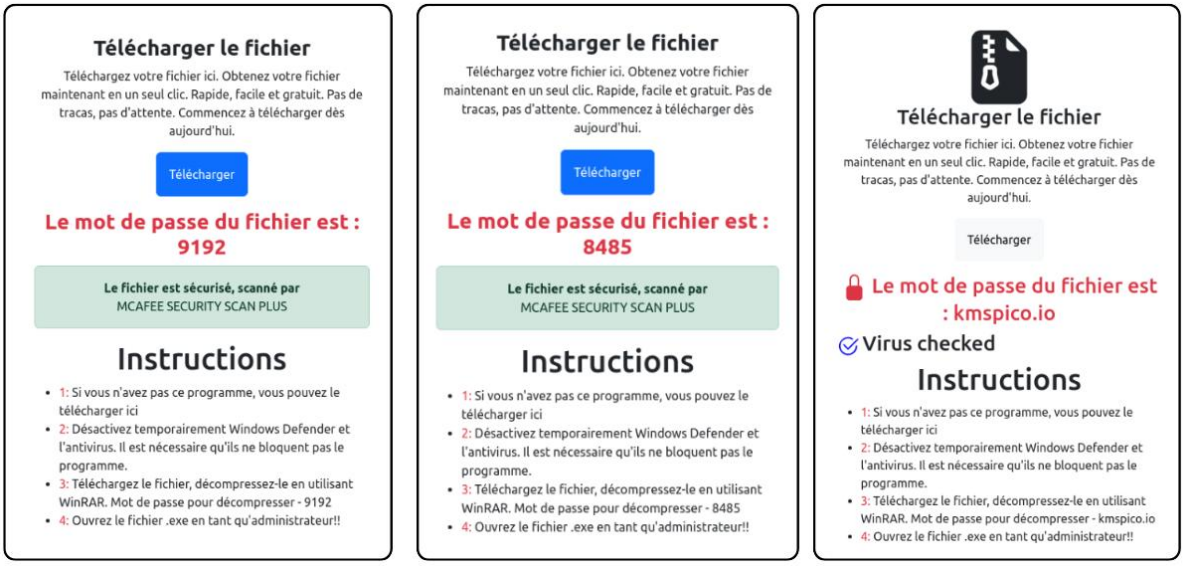


Figure 22. Instructions displayed in French and hosted on French Aeza server 147.45.68[.]130. Domains: sarahmakesitbetter[.]com, rivistablog[.]com, anotherconversation[.]com, and puntext[.]com.

Aeza International Ltd.
In recent months, Intrinsec's CTI team has been noticing the recrudescence of a variety of malware command-and-control servers being hosted on the same Autonomous System named *Aeza International Ltd.* (**AS210644**). This service has been growing since 2021 under a different name *Aeza Group Ltd.* (**AS216246**). Before creating the company, the founder of Aeza was involved in another Russian bulletproof hosting provider named "MskHost", which was hacked by hacktivists and eventually shutdown by their creators.
Major actors like **TA577** have been using this service for their campaigns and we believe that it will remain the case for both sophisticated and basic threat actors.

4.2. Lumma deployment

After retrieving those domains by scanning for the present of the Matomo script in their code, we found that the same domain could in fact redirect to multiple other Mega or Dropbox folders. Depending on the URL, the website could point to either a CryptBot or a Lumma infected archive.

Like the domain "**rars-freeload**[.]**com**", where the URL "*rars-freeload*[.]*com/thre*" would point to a Mega folder hosting a **Lumma** infected archive, and "*rars-freeload*[.]*com/vs012/*" would point to a **CryptBot** infected archive.

The downloaded Lumma payload happened to communicate with the same C2 domains as the payload downloaded by the Amadey cluster hosted on *1337TEAM LIMITED*.

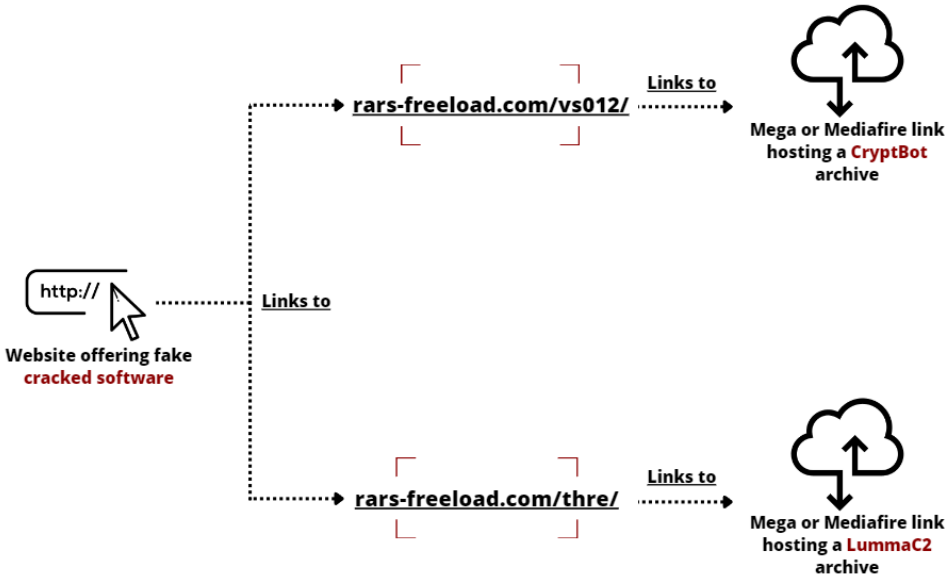


Figure 23. Layout summarizing the concept above-mentioned.

5. Pivoting to find other distribution websites

More than a hundred of websites offering cracked versions of software were hosted on IP **195.66.210**[.]**137**, managed by **Ukrainian autonomous system "*Virtual Systems LLC*"** (**AS6698**). Among those, "**drapk**[.]**net**" for example, distributes fake APK and redirects to "**techjbc**[.]**cfd**", a different domain that the ones we previously observed but **still** linked to an URL leading to the same Mega folder containing the identical archive infected with **CryptBot**. Consult the "Indicator of compromise" section of this report for the complete list of websites that could be found.

1	domain	17	crackfullpc.org
2	bcrack.org	18	crackmacs.org
3	crack4tech.org	19	crackmarkets.com
4	crackedaxe.com	20	pesktop.org
5	crackingcity.org	21	crackpcsoft.org
6	crackspc.net	22	crackdownloads.org
7	fileserialkey.net	23	iup4pc.net
8	fullycracksoft.com	24	crackingpc.net
9	ifree4pc.net	25	downloadvst.com
10	productkeysfree.org	26	licensedfull.com
11	tech4pc.org	27	vstcrackpc.com
12	winows4pc.com	28	vstpropc.com
13	4mirrorpc.net	29	vstdownload.org
14	drapk.net	30	activationskey.com
15	drfiles.net	31	allmacworld.net
16	haxacademy.net	32	cracked-minecraft.com
		33	crackedvpn.com
		34	crackfix.net
		35	crackfullkeys.com

Figure 24. Snippet of the domains found to be hosted on 195.66.210[.]137.

Some of the domains used as redirectors would display the same *Common Name* (CN) field. Through this pivot, a few additional ones could be discovered.

Domain name
techjbc[.]cfd
sultanisback[.]pro
filemirrormegaz[.]shop
allgetinopcc[.]cfd
free4pc[.]shop

Additionally, by inspecting the content of autonomous systems like *IP Volume Inc.* - **AS202425**, a network based in the Seychelles that we attribute with a high level of confidence to the creators of the new defunct **Ecatel**, we discovered much more domains used for the same purposes. The table below only highlights a snippet of them

Domain name
securecracked[.]info
muzamilpc[.]com
mycrackfree[.]com
windows4pc[.]com
windowsprodcutkey[.]com
activationkeysfree[.]org

IP Volume Inc. | Ecatel

Considered "*one of [The Netherlands']most criticized hosting businesses*" according to The New York Times[14], Ecatel was founded in 2005 by two Dutch nationals. The company was registered in Kent (United Kingdom) with its headquarters in The Hague. In 2011, the company got into an argument with the data centre in Alphen aan de Rijn where they rented servers. Thereupon, they decided to start their own data centre called **DataOne** in Wormer.[15]

In December 2015, IP addresses from Ecatel moved to a new company registered in Seychelles named *Quasi Network*, which later changed to "*IP Volume Inc*". In 2020, the Ministry of Justice and Security of the Netherlands published a ranking of Dutch hosting companies with the most child pornography on their servers. With 4,500 out of 175,000 verified reports, IP Volume Inc ranked **second**.[16]

In addition to IP Volume Inc, Ecatel's directors created another company in the Netherlands named "*FiberXpress BV*"[17], associated to the autonomous system **AS57717**. *IP Volume Inc* obtains upstream from this network by sharing **74.5**% of its peering agreements. Overall, the autonomous system manages **1,792 IPv4**. The address of the company is the same as their datacentre in Wormer, where all of their other Dutch companies are also located.[18]

By analysing the various contents hosted on *FiberXpress BV*, we discovered a trove of domains that were part of a large network of fake websites distributing copies of cracked software or video games. In some cases, those websites switched from being hosted on *IP Volume Inc* to *FiberXpress BV*, such as "**crackedkeys.softwaresdaily**[.]**com**" for example.

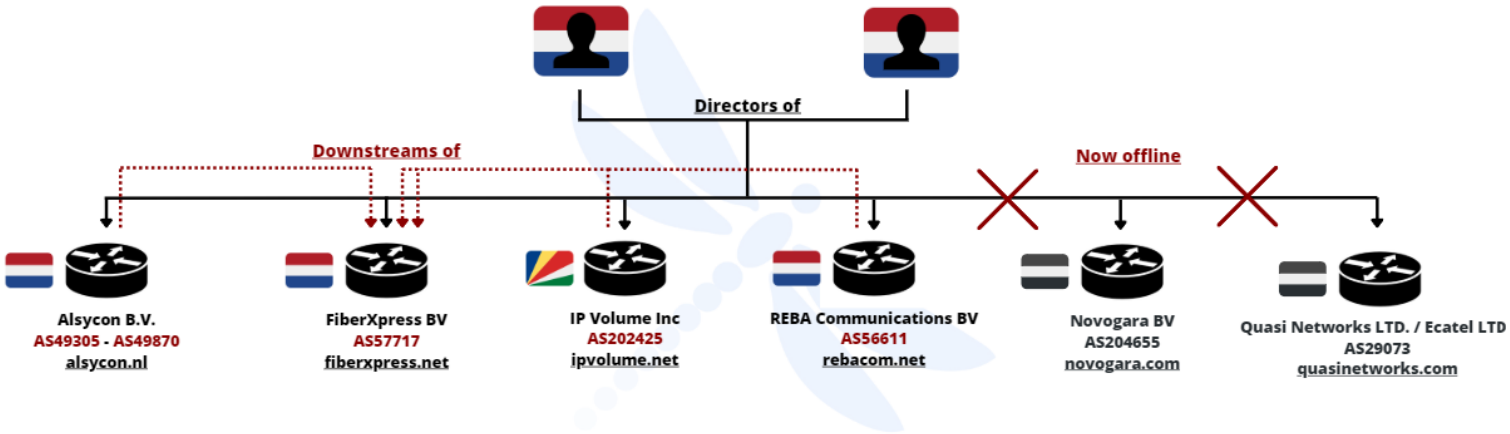


Figure 25. Layout of the companies and autonomous systems linked to the creators of Ecatel.

[14] *https://www.nytimes.com/interactive/2019/12/22/us/child-sex-abuse-websites-shut-down.html*

[15] *https://nl.wikipedia.org/wiki/IP_Volume*

[16] *https://www.nrc.nl/nieuws/2020/10/08/vier-bedrijven-hosten-overgrote-deel-kinderporno-a4015235*

[17] *https://www.dnb.com/business-directory/company-profiles.fiberxpress_bv.98ecba6e933249d62edbcef242871a0f.html*

[18] Intrinsec private report. "*Mapping Ecatel ramifications & bulletproof networks fronted by offshore companies*". October 2024.

6. Conclusion

This report aimed to give an insight on the current spreading methods leveraged by **CryptBot** and the various collaborations that it maintains with other threat actors within the cybercrime ecosystem. We also highlighted how some of these actors like the ***Pay-Per-Install* service** running the PrivateLoader malware continue to rely on **bulletproof hosting providers**. This requires keeping on monitoring these networks due to the frequency of their infrastructure changes, as we could observe in the IPv4 ranges that were moved from a bulletproof autonomous system to another. Most of those networks' malicious nature had already been unveiled in previous investigations of Intrinsec's CTI team. By blocking those autonomous systems, the campaigns analysed in this report could have eventually been diffused.

All those different sources of infections leading to the deployment of CryptBot underline the threat actor's will to **rapidly expand its botnet**, probably in response to Google's efforts in taking down the malware's infrastructure which drastically lowered the infection rate. This also shows that despite having companies with major strike power like Google engaging in legal procedures, those threats can **still prosper and expand**. The main solution continues to be proactive in tracking their last TTPS, related IoCs, code evolution, capacities, and C2 communications overall.

7. Actionable content

7.1. Indicators of compromise

Value	Type	Description
da7fadc671804e093c7dcad3455a266e77d2c84b641ae037c70004daaa05b897	SHA-256	CryptBot – "Channel4.exe"
8874ee4d9c878a6dc7f2681ec36df05cb09c44ccb3be0ec89569f5bdece80519	SHA-256	CryptBot – "66dd5fafdeab3_lyla.exe"
2a5dd73271b9eabe63e7aefc5dc2ec01921ffba8bfa7ee278a2180e597c97bf7	SHA-256	CryptBot – "Set-up.exe"
319d1dc217b7e83a85dd62cb2c066156ba5579087f11c991a99089606979ca28	SHA-256	PrivateLoader payload
7631726b15a0cba30f88268df626df7a053c044efc78f772ade21e879cc7ae58	SHA-256	SmokeLoader payload
7b41cabcafca0e5725c874d316f4f5f83561fa571240c0ccdd8b19034282bf41	SHA-256	Amadey payload
tventyv20sb[.]top	Domain	CryptBot C2
twoxv2sr[.]top	Domain	CryptBot C2
analforeverlovyu[.]top	Domain	CryptBot C2
thirtv13pn[.]top	Domain	CryptBot C2
bdtwo2sb[.]top	Domain	CryptBot C2
neiz19ht[.]top	Domain	CryptBot C2
levz11ht[.]top	Domain	CryptBot C2
fifxv15pn[.]top	Domain	CryptBot C2
fivevd5ht[.]top	Domain	CryptBot C2
sevtvd17ht[.]top	Domain	CryptBot C2
rxeight8ht[.]top	Domain	CryptBot C2
salvatiiywo[.]shop	Domain	Lumma C2
ignoracndwko[.]shop	Domain	Lumma C2
preachstrwnwjw[.]shop	Domain	Lumma C2
complainnykso[.]shop	Domain	Lumma C2
basedsymsotp[.]shop	Domain	Lumma C2
charistmatwio[.]shop	Domain	Lumma C2
grassemenwji[.]shop	Domain	Lumma C2
stitchmiscpaew[.]shop	Domain	Lumma C2
commisionipwn[.]shop	Domain	Lumma C2
epohe[.]ru	Domain	SmokeLoader C2
olihonols.in[.]net	Domain	SmokeLoader C2
nicetolosv[.]xyz	Domain	SmokeLoader C2
jftolsa[.]ws	Domain	SmokeLoader C2
download-rarfree[.]com	Domain	Redirecting to CryptBot payloads
rar-uploader[.]com	Domain	Redirecting to CryptBot payloads
economartbd[.]com	Domain	Redirecting to CryptBot payloads
rarz-uploader[.]com	Domain	Redirecting to CryptBot payloads

adsbell[.]com	Domain	Redirecting to CryptBot payloads
voiceofchangeinternational[.]com	Domain	Redirecting to CryptBot payloads
rar-freeload[.]com	Domain	Redirecting to CryptBot payloads
rars-freeload[.]com	Domain	Redirecting to CryptBot payloads
download-rarsfree[.]com	Domain	Redirecting to CryptBot payloads
rarzload-official[.]com	Domain	Redirecting to CryptBot payloads
Chuanpupu[.]com	Domain	Redirecting to CryptBot payloads
techjbc[.]xyz	Domain	Redirecting to CryptBot payloads
papiblendz[.]com	Domain	Redirecting to CryptBot payloads
sarahmakesitbetter[.]com	Domain	Redirecting to CryptBot payloads
rivistablog[.]com	Domain	Redirecting to CryptBot payloads
anotherconversation[.]com	Domain	Redirecting to CryptBot payloads
super6-star[.]buzz	Domain	Redirecting to CryptBot payloads
bluelineagenciamentodecargas[.]com	Domain	Redirecting to CryptBot payloads
peace-motion[.]buzz	Domain	Redirecting to CryptBot payloads
131ldvip[.]com	Domain	Redirecting to CryptBot payloads
onlineofficetutorials[.]com	Domain	Redirecting to CryptBot payloads
puntext[.]com	Domain	Redirecting to CryptBot payloads
free4pc[.]shop	Domain	Redirecting to CryptBot payloads
allgetintopcc[.]cfd	Domain	Redirecting to CryptBot payloads
techjbc[.]cfd	Domain	Redirecting to CryptBot payloads
sultanisback[.]pro	Domain	Redirecting to CryptBot payloads
filemirrormegaz[.]shop	Domain	Redirecting to CryptBot payloads
uznhmij5kr2307244[.]click	Domain	Redirecting to CryptBot payloads
afrdrctf[.]com	Domain	Redirecting to CryptBot payloads
up4pc[.]com	Domain	Offering fake cracked software
driver-booster-key[.]com	Domain	Offering fake cracked software
securecracked[.]info	Domain	Offering fake cracked software
filecrr[.]org	Domain	Offering fake cracked software
soft98[.]org	Domain	Offering fake cracked software
haxpc[.]net	Domain	Offering fake cracked software
muzamilpc[.]com	Domain	Offering fake cracked software
alphasofts[.]net	Domain	Offering fake cracked software
preactivated[.]net	Domain	Offering fake cracked software
mycrackfree[.]com	Domain	Offering fake cracked software
drapk[.]net	Domain	Offering fake cracked software
rgames31[.]com	Domain	Offering fake cracked software
windows-7-activator[.]com	Domain	Offering fake cracked software
modcrack[.]net	Domain	Offering fake cracked software
office-activator[.]com	Domain	Offering fake cracked software
official-kmspico[.]com	Domain	Offering fake cracked software
kmspico[.]ws	Domain	Offering fake cracked software
kmspicoofficial[.]com	Domain	Offering fake cracked software
windows4pc[.]com	Domain	Offering fake cracked software

windowsprodcutkey[.]com	Domain	Offering fake cracked software
activationkeysfree[.]org	Domain	Offering fake cracked software
serialhax[.]org	Domain	Offering fake cracked software
bcrack[.]org	Domain	Offering fake cracked software
crack4tech[.]org	Domain	Offering fake cracked software
crackedaxe[.]com	Domain	Offering fake cracked software
crackingcity[.]org	Domain	Offering fake cracked software
crackspc[.]net	Domain	Offering fake cracked software
fileserialkey[.]net	Domain	Offering fake cracked software
fullycracksoft[.]com	Domain	Offering fake cracked software
ifree4pc[.]net	Domain	Offering fake cracked software
productkeysfree[.]org	Domain	Offering fake cracked software
tech4pc[.]org	Domain	Offering fake cracked software
winows4pc[.]com	Domain	Offering fake cracked software
4mirrorpc[.]net	Domain	Offering fake cracked software
drapk[.]net	Domain	Offering fake cracked software
drfiles[.]net	Domain	Offering fake cracked software
haxacademy[.]net	Domain	Offering fake cracked software
crackfullpc[.]org	Domain	Offering fake cracked software
crackmacs[.]org	Domain	Offering fake cracked software
crackmarkets[.]com	Domain	Offering fake cracked software
pesktop[.]org	Domain	Offering fake cracked software
crackpcsoft[.]org	Domain	Offering fake cracked software
crackdownloads[.]org	Domain	Offering fake cracked software
iup4pc[.]net	Domain	Offering fake cracked software
crackingpc[.]net	Domain	Offering fake cracked software
downloadvst[.]com	Domain	Offering fake cracked software
licensedfull[.]com	Domain	Offering fake cracked software
vstcrackpc[.]com	Domain	Offering fake cracked software
vstpropc[.]com	Domain	Offering fake cracked software
vstdownload[.]org	Domain	Offering fake cracked software
activationskey[.]com	Domain	Offering fake cracked software
allmacworld[.]net	Domain	Offering fake cracked software
cracked-minecraft[.]com	Domain	Offering fake cracked software
crackedvpn[.]com	Domain	Offering fake cracked software
crackfix[.]net	Domain	Offering fake cracked software
crackfullkeys[.]com	Domain	Offering fake cracked software
crackfullpc[.]net	Domain	Offering fake cracked software
cracksecure[.]com	Domain	Offering fake cracked software
cracksoftpro[.]com	Domain	Offering fake cracked software
crackswatch[.]com	Domain	Offering fake cracked software
crackvstpc[.]com	Domain	Offering fake cracked software
downloadworld[.]org	Domain	Offering fake cracked software
fullidmcrack[.]com	Domain	Offering fake cracked software

fullproductkeys[.]com	Domain	Offering fake cracked software
idmfreedownload[.]net	Domain	Offering fake cracked software
idmfullcrack[.]info	Domain	Offering fake cracked software
idmpatchdownload[.]com	Domain	Offering fake cracked software
idmpatched[.]com	Domain	Offering fake cracked software
idmpc[.]co	Domain	Offering fake cracked software
igetintopc[.]com[.]pk	Domain	Offering fake cracked software
kanjupc[.]com	Domain	Offering fake cracked software
keyproductkey[.]com	Domain	Offering fake cracked software
licensekey[.]cc	Domain	Offering fake cracked software
macsoftkey[.]com	Domain	Offering fake cracked software
naveedcrack[.]com	Domain	Offering fake cracked software
office4pc[.]com	Domain	Offering fake cracked software
pc4download[.]com	Domain	Offering fake cracked software
pcbank[.]org	Domain	Offering fake cracked software
pccrack[.]org	Domain	Offering fake cracked software
pcdrives[.]org	Domain	Offering fake cracked software
pcexe[.]net	Domain	Offering fake cracked software
pcsoftcrack[.]net	Domain	Offering fake cracked software
pdffree[.]net	Domain	Offering fake cracked software
pluginstorrent[.]net	Domain	Offering fake cracked software
premiumpc[.]net	Domain	Offering fake cracked software
premiumpc[.]org	Domain	Offering fake cracked software
procracked[.]org	Domain	Offering fake cracked software
procrackwin[.]com	Domain	Offering fake cracked software
productkeycrack[.]com	Domain	Offering fake cracked software
productkeyspc[.]com	Domain	Offering fake cracked software
productskey[.]org	Domain	Offering fake cracked software
prolicensefree[.]com	Domain	Offering fake cracked software
proserialcrack[.]com	Domain	Offering fake cracked software
proserialfree[.]com	Domain	Offering fake cracked software
provstpc[.]com	Domain	Offering fake cracked software
pubgcrack[.]net	Domain	Offering fake cracked software
rootcracks[.]com	Domain	Offering fake cracked software
sadeempc[.]info	Domain	Offering fake cracked software
securecracked[.]info	Domain	Offering fake cracked software
seriakkeyforfree[.]com	Domain	Offering fake cracked software
softsmac[.]net	Domain	Offering fake cracked software
softwarein1[.]com	Domain	Offering fake cracked software
softwarekeep[.]info	Domain	Offering fake cracked software
starcracked[.]net	Domain	Offering fake cracked software
startcrack[.]info	Domain	Offering fake cracked software
topfullcrack[.]com	Domain	Offering fake cracked software
topfullkeys[.]com	Domain	Offering fake cracked software

torrent4pc[.]com	Domain	Offering fake cracked software
torrentpc[.]org	Domain	Offering fake cracked software
vst4cracked[.]com	Domain	Offering fake cracked software
vst4pc[.]com	Domain	Offering fake cracked software
vstfree[.]org	Domain	Offering fake cracked software
vstfreedownload[.]com	Domain	Offering fake cracked software
vstfullpc[.]com	Domain	Offering fake cracked software
vstpc[.]com	Domain	Offering fake cracked software
vstpluginsdownload[.]org	Domain	Offering fake cracked software
vstzip[.]com	Domain	Offering fake cracked software
wincrackbox[.]com	Domain	Offering fake cracked software
soft-got[.]org	Domain	Offering fake cracked software
185.244.181[.]38	IPv4	CryptBot C2
81.94.159[.]120	IPv4	CryptBot C2
103.130.147[.]211	IPv4	Hosting malwares
147.45.44[.]104	IPv4	Hosting malwares - Operated by PrivateLoader
31.41.244[.]9	IPv4	Hosting malwares - Operated by PrivateLoader
176.111.174[.]109	IPv4	Hosting malwares - Operated by PrivateLoader
147.45.47[.]169	IPv4	PrivateLoader C2
212.113.116[.]202	IPv4	PrivateLoader C2
62.133.61[.]172	IPv4	PrivateLoader C2
45.91.200[.]135	IPv4	PrivateLoader C2
92.246.139[.]82	IPv4	PrivateLoader C2
185.215.113[.]16	IPv4	Amadey C2
185.215.113[.]19	IPv4	Amadey C2
185.215.113[.]17	IPv4	Stealc C2
91.202.233[.]158	IPv4	Stealc C2
185.215.113[.]67	IPv4	Redline C2
65.21.18[.]51	IPv4	Redline C2
215789	ASN	“Karina Rashkoska”
214927	ASN	“PSB HOSTING LTD”
210644	ASN	“Aeza International Ltd”
216246	ASN	“Aeza Group Ltd.”
51381	ASN	“1337TEAM LIMITED”
60424	ASN	“1337TEAM LIMITED”
56873	ASN	“1337TEAM LIMITED”
39770	ASN	“1337TEAM LIMITED”
200593	ASN	“PROSPERO OOO”

7.2. Recommendations

- Monitor all traffic from/to any IP addresses and domains above mentioned.
- Check for the presence of the above-mentioned files on your systems.
- Monitor all traffic from/to any IP address belonging to above mentioned autonomous systems and organisations.
- Consider a proactive employee credential assessment (logs, session cookies, login/pass etc.) on prioritized Dark web forums by CTI teams to mitigate the risk of account takeover.
- Raise awareness on the risk of downloading external software from untrusted sources in your company.

8. Sources

- *https://regmedia.co.uk/2023/04/28/handout_google_cryptbot_complaint.pdf*
- *https://blog.google/technology/safety-security/continuing-our-work-to-hold-cybercriminal-ecosystems-accountable/*
- *https://malpedia.caad.fkie.fraunhofer.de/details/win.cryptbot*
- *https://research.openanalysis.net/cryptbot/botnet/yara/config/2023/03/16/cryptbot.html*
- *https://www.gdatasoftware.com/blog/2020/02/35802-bitbucket-abused-as-malware-slinger*
- *https://cloud.google.com/blog/topics/threat-intelligence/peaklight-decoding-stealthy-memory-only-malware/?linkId=10719875&hl=en*
- *https://intezer.com/blog/research/cryptbot-yet-another-silly-stealer-yass/*
- *https://cloud.google.com/blog/topics/threat-intelligence/russian-targeting-gov-business/?hl=en*
- *https://any.run/cybersecurity-blog/cryptbot-infostealer-malware-analysis/*
- *https://asec.ahnlab.com/en/24423/*
- *https://x.com/vql3n/status/1831624490603753503*
- *https://darktrace.com/fr/blog/cryptbot-how-darktrace-foiled-a-fast-moving-information-stealer-in-just-2-seconds*
- *https://www.bleepingcomputer.com/news/security/google-starts-taking-down-cryptbot-malware-infrastructure/*
- *https://x.com/RussianPanda9xx/status/1766163567873593476*
- *https://www.team-cymru.com/post/seychelles-seychelles-on-the-c-2-shore*
- *https://web.archive.org/web/20231018093233/https://oliverhough.io/prospernot-prospero-as-the-little-as-that-could-part-1/*

INTRINSEC

Innovative by design

Cyber Threat Intelligence

@Intrinsec @Intrinsec Blog Website

If you have any inquiries regarding this report, please contact veille-cti@intrinsec.com