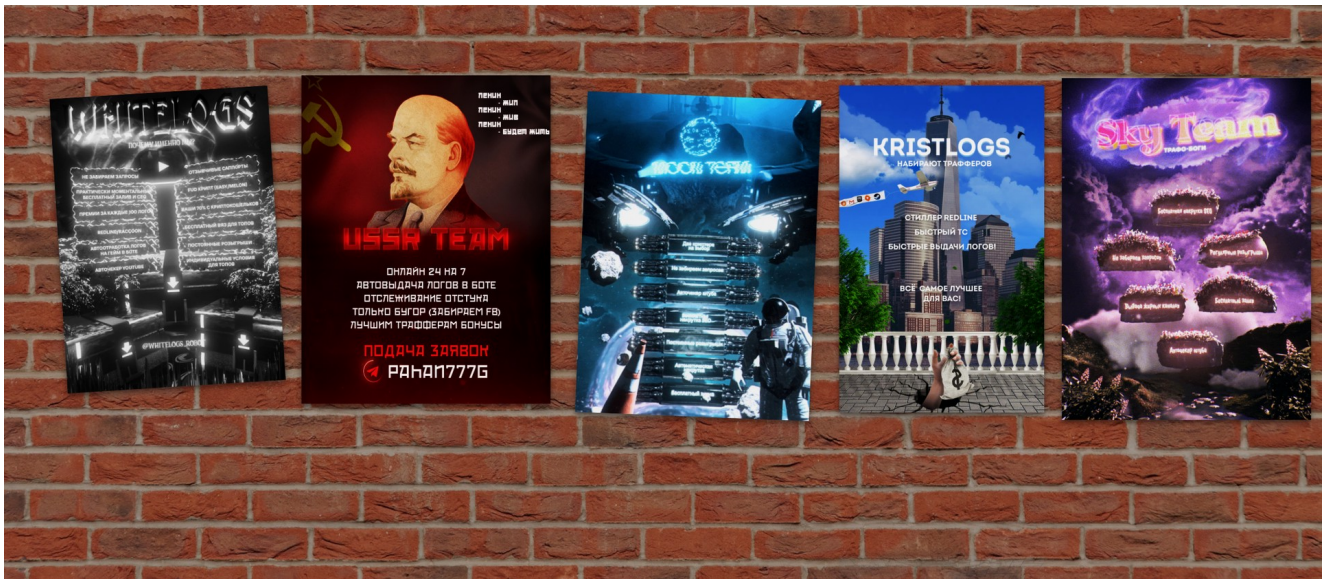
Traffers: a deep dive into the information stealer ecosystem

blog.sekoia.io/traffers-a-deep-dive-into-the-information-stealer-ecosystem

29 August 2022



Log in

Whoops! You have to login to access the Reading Center functionalities!

Forgot password?

Search the site...

- All categories
- Blogpost
- Blogpost

Reset

Threat & Detection Research Team August 29 2022
272 0

Read it later Remove

22 minutes reading

Accueil » Blogpost » Traffers: a deep dive into the information stealer ecosystem

Background

The cybercrime ecosystem is filled with a multitude of threat actors that share the same financial motivation through malicious activities. Although not well described by the global cybersecurity industry, the actors in charge of **generating non-legitimate traffic** play a **key role in the distribution of threats**, as well as the underground economy.

Commonly referred to as **traffers** (from the Russian word “Трафферер”, also referred to as “worker” in the underground community), these actors are responsible for redirecting user’s traffic to malicious content (malware, fraud, phishing, scam, etc.) operated by others. They **monetise the traffic** to these botnet operators who intend to compromise users either widely, or specifically to a region, or an operating system. The main challenge facing traffer is therefore to generate high-quality traffic without bots, undetected or analysed by security vendors, and eventually filtered by traffic type. In other words, **traffers’ activity is a form of lead generation**.

To generate traffic, traffers lure users from legitimate or compromised websites to redirect them to a server, a website, or malicious content operated by the botnet owner. Some sophisticated traffers make use of the Traffic Distribution System (TDS) to operate and redirect traffic. This tool allows traffers to filter traffic based on its characteristics, such as location, operating system, and HTTP headers, enabling them to sell high-quality traffic to threat actors with specific targets. Other traffers focus on generating traffic to a very large audience over a short period of time while avoiding detection.

As part of a growing trend, numerous **traffers join a team to distribute information-stealing malware** on behalf of the team administrator(s). In these teams, traffers can both be highly skilled threat actors and newcomers in the threat landscape, as they usually get training sessions when hired by a team. These groups are therefore a gateway into the cybercrime ecosystem for newcomers. Administrator(s) of the traffers team gather the user’s logs (stolen information including cookies, passwords, crypto wallets, documents, etc.) to exploit or sell them.

Introduction

In the first half of 2022, SEKOIA identified an increase in the use of information-stealing malware as the preferred commodity malware for cybercriminals. We observed this trend through our Darkweb monitoring routine, our information stealers related indicators of compromise trackers, and our insights of the threat landscape. These observations led us to analyse the main methods of distribution of this threat, as well as the organisation of traffers delivering stealers.

Traffers teams dealing with stealers are mostly found on Russian-speaking cybercrime forums, especially for recruitment purposes. SEKOIA observed hundreds of advertisements aiming at recruiting traffers to distribute information stealers. Further investigation led us to **identify a**

structure and a common *modus operandi* to most **traffers teams distributing stealers**. We also share information on the **main infection chain** used by traffers dealing with information stealers and their **arsenal**.

This report is based on data collected from the Lolz Guru and BHF cybercrime forums between January and mid-August 2022. We focused **our analysis on traffers' activity related to information stealer distribution**.

Traffers distributing stealers: an immersion in the world of highly proliferating cybercriminals

Traffers teams as part of the cybercrime ecosystem

Similarly to other threat actors in the continuously professionalising cybercrime landscape, traffers are either operating on their own, or join a team, called "traffers team".

Traffers teams operating on cybercrime forums display different focuses, some scamming NFT (Non-Fungible Token) or crypto currency owners, others targeting online casino users. Several of them deliver malware, such as RAT (Remote Access Trojan), miner or information-stealing malware. SEKOIA observed that more than 90% of traffers teams operate information stealers, either commercial or developed within the team ones. Some even operate two or three stealers.

Most of the traffers teams SEKOIA monitored operate on Russian-speaking cybercrime forums, *e.g.* Lolz Guru and BHF forums, commonly referred to as "social engineering forums" in the underground community. These forums are used to advertise products and services, to announce the emergence of new teams, and to collect reviews to gain visibility. In parallel, the Telegram instant messaging service is leveraged to organise teams' activities. The majority of investigated traffers are native Russian speakers.

From our observations, a team can grow to hundreds, even thousands of members (*e.g.* TigerTeams had over 200 members and 340 bot subscriptions in April 2022 and BandanaTeam declared more than 5000 team members in July 2022).

To better understand the evolution of the traffers-related threat, we monitored the emerging traffers teams on the Lolz Guru underground forum since early 2022.

We registered 125 traffers teams created since January 2022 on the Lolz Guru forum's "Traffers" section. At least half of them were still active during the last month.

Figure 1. Number of newly launched traffers teams by month in 2022 (Source: Lolz Guru forum, Traffers section)

The longevity of a traffers team is complex to assess. As the resources involved remain fairly accessible, teams demonstrated flexibility in reorganising themselves, by merging with other teams or simply restarting from scratch. According to a declaration of the *Dead Team*'s administrator in June 2022, it cost him $3,000 to build a team of 600 traffers before selling it. Another example, the entire infrastructure of *TigersTeam* (between 200 and 340 traffers) was put on sale for $300 in April 2022, and the *Moon Team* (1000 traffers) was priced at $2, 300 in May 2022. Based on several publications collected on the Lolz Guru forum, this represents an "investment" that can break even in less than a month.

A spotlight on a typical traffers team organisation

A traffers team is an organised, centrally managed structure headed by one or several team administrators. Here is an overview of a typical traffers team and its interactions within the cybercrime ecosystem:

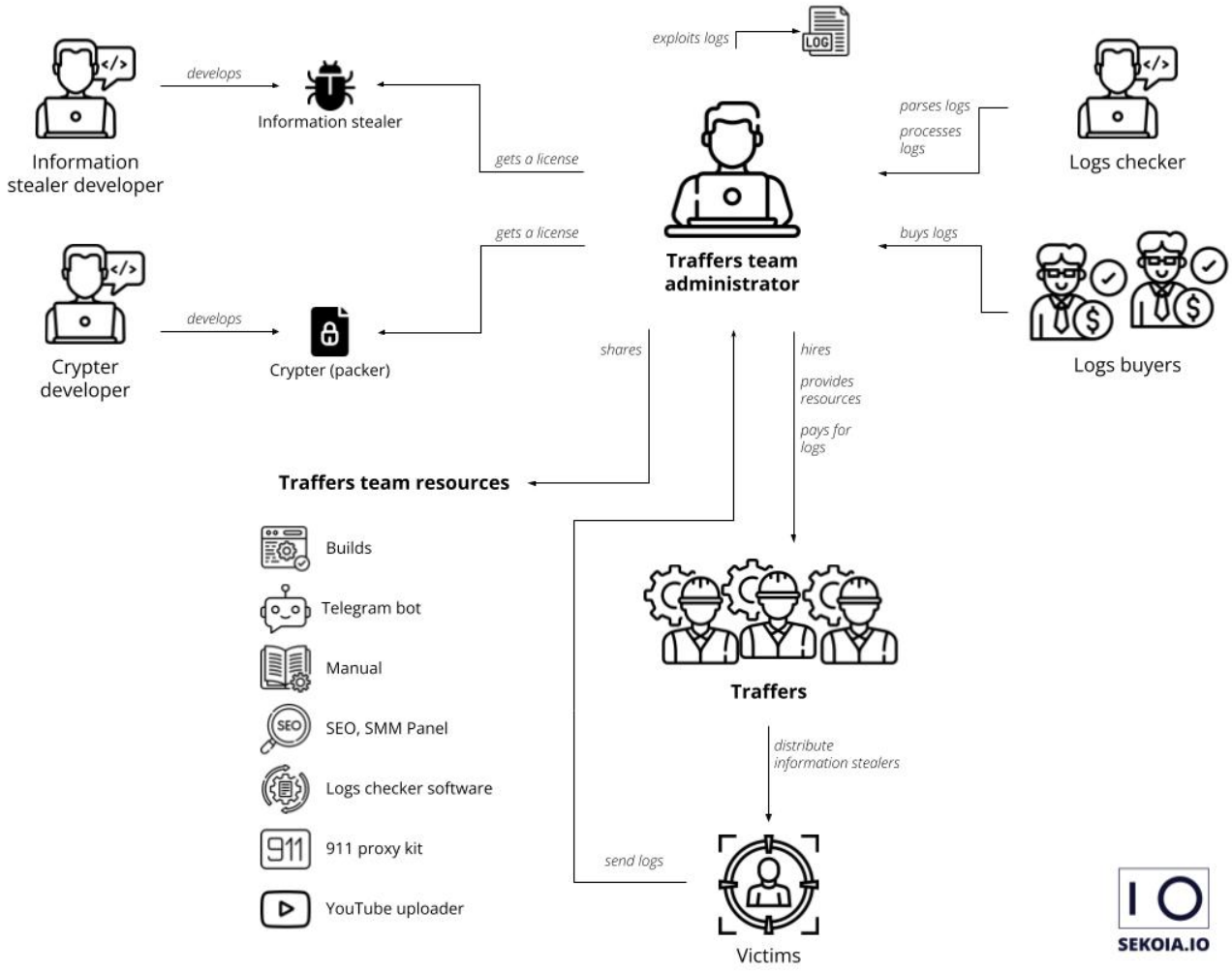


Figure 2. Overview of a typical traffers team structure and its interactions

Team administrators' role

Team administrators hire traffers in charge of generating traffic to distribute stealer builds.

A team administrator is responsible for the management of all tasks complementary to traffic generation. This notably includes getting a stealer licence and sharing builds ready for distribution to the team members, checking the received logs for validity, and exploiting them quickly.

Therefore, team administrators provide their team members a kit containing the following resources:

- Builds automatically generated and pushed to traffers by a Telegram bot;
- A crypter service to encrypt or obfuscate malware builds to evade detection solutions;
- A "traffer's manual" which includes guidelines for team members and full technical support. Team administrators can draft a handbook by themselves or they can use the services of an independent third party writing a traffer's manual as-a-service;

- SEO (Search Engine Optimization) services to improve the visibility of videos uploaded on YouTube using the 911 scheme (the 911 scheme is detailed later in the report and the Annex 2 illustrates the infection chain);
- A YouTube uploader software or a YouTube uploading service (by hiring a dedicated team member responsible for uploading on YouTube on behalf of traffers);
- A Telegram channel for communication and support within the team;
- A Telegram bot for automating tasks, such as sharing new malware builds, statistics, money earned by the traffer;
- A dedicated service for parsing, processing, exploiting and selling logs. The team administrators coordinate the process of log qualification and analysis, extraction of logs of interest, and exploitation.

Team administrators prompt recruited members to distribute the builds widely, to generate a large volume of logs via stealer infections, and reward them based on a formula in which both quantity and quality of the collected information are taken into account.

Team administrators regularly organise competitions in which traffers are challenged to collect a maximum of logs, *i.e.* distribute a maximum number of builds. Winners are awarded with cash prizes, and upgraded to a Pro version of the membership. The Pro version unlocks access to a second stealer, traffers are invited to a private Telegram channel, they get better services (like SEO and else) and bonuses.

Traffers team's primary interest lies in crypto wallets logs.The generated revenue through exploitation is shared with the traffer who submitted the logs (who gets from 60% to 90% of the revenue). A team might also extract and resell video games, e-commerce and social network accounts. The remaining logs are transferred back to the traffers to be reused.

Logs selling price within the underground community varies widely depending on their validity and the information they contain. Generally, the more recent a log is, the highest the probability of containing active cookies, the more it is wanted.

Traffers' role within a team

Once a traffer joined a team, it is able to make requests to a Telegram bot for builds to receive a malware sample. A traffer can make multiple requests to this bot, the number of builds it can generate being limited to a daily quota, as defined by team administrator(s).

When joining teams, traffers often have to abide by a number of requirements at the risk of being expelled. Requirements include:

- They can not use their own malware or glue a malware to the one delivered by the team, distributing ransomware is also forbidden;
- They can not share the received build with third parties;
- They can not check the build on online services such as VirusTotal;
- They can not be inactive for more than two weeks in a row.

SEKOIA assess that this serves to frame the traffers' activity to avoid abusive behaviour that could lead to burning the C2 server. This is also a way to avoid an improper mass distribution of builds on channels easily detectable by security vendors.

Once a traffer gets a build, it is responsible for spreading the malware using the team's delivery methods, or its own infection chain.

Traffers can also distribute their own information stealer, and monetize the collected logs by themselves by selling them on underground marketplaces. They can as well steal cryptocurrency from crypto wallets without integrating an organised team. Nevertheless, from our observations, joining a team is largely preferred by traffers, as it comes along with a number of advantages, to name a few:

- Experience is not mandatory – newcomers are welcomed and trained;
- Necessary tools are accessible and ready to use – traffers have no extra costs related to the stealer, crypter and other software;
- Traffers capitalise on the different services provided by their team administrator(s);
- Technical support is guaranteed;
- Traffers team operators monetize collected logs immediately, as fresh and bulk logs are more valuable.

At the same time, the interest of traffers teams representatives in hiring a large number of traffers lies in having access to large volumes of fresh data when cumulating all the submissions.

Modus Operandi observed in traffers teams dealing with stealers

Traffers working with information-stealing malware are free to generate traffic and distribute the provided builds using their own methods, as long as they comply with the team requirements. Each traffer therefore sets up and operates its own delivery chain.

However, the majority of traffers teams SEKOIA observed provide tools and services to assist their members in generating traffic from YouTube videos. Most of them therefore use the tools made available to set up their delivery chain. This infection chain, that consists in luring users from the legitimate YouTube website to redirect them to the malicious content, is called 911 in the cybercrime ecosystem.

In the next part, we share more details on the common spreading methods used by traffers, as well as the malware arsenal observed in most teams.

911 infection chain

Known on the Russian-speaking cybercrime forums as "911", this infection chain consists in delivering the final payload using stolen YouTube accounts to distribute a download link. For this purpose, the traffer or a dedicated member of the traffers team uploads a video on

YouTube enticing the user to download an archive, disable Windows Defender and execute its content. In most observed cases, the uploaded video is a tutorial for installing a cracked software, a product licence key generator or even a cheat software for video games. The traffer abuses legitimate file transfer services, such as Mega, Mediafire, OneDrive, Discord or GitHub, to store the payload. The downloaded file is often a password-protected archive making it undetectable, containing an executable file which turns out to be the information-stealing malware.

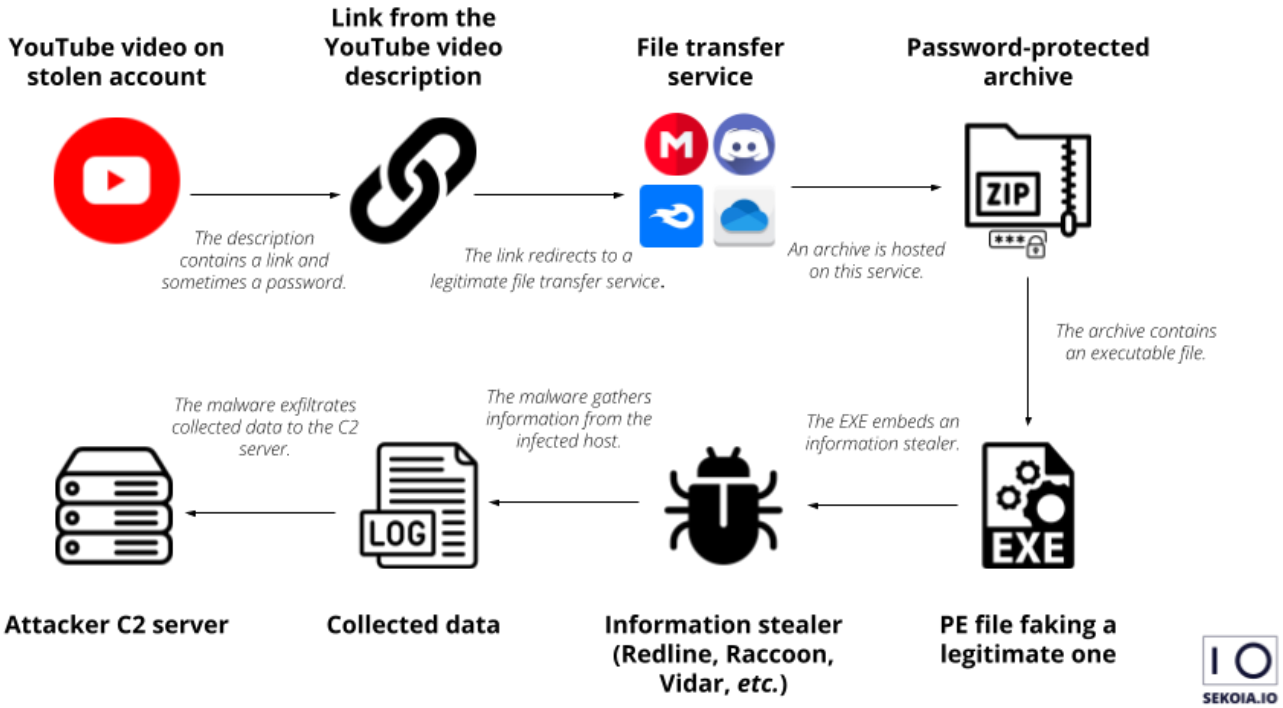


Figure 3. Typical 911 Infection chain

Uploading this content on YouTube requires bypassing YouTube's anti-fraud system. For that purpose, the "911" method makes use of proxies to fake the IP address of the YouTube channel owner. Given the amount of stolen data passing through the logs, SEKOIA assess that traffers teams likely use valid YouTube credentials and the associated IP address in follow-up activities.

While we observed this delivery method is widely leveraged by traffers, it is used to target individuals rather than companies. Some traffers teams (*e.g. Bebra Team)* don't use the "911" method.

Several hypotheses can be made about the choice not to use the 911 infection chain:

- Selling logs from stealers distributed via YouTube traffic may not be as profitable as the distribution via other legitimate service or websites, or company emails. Lured users on YouTube are more likely to be young people owning small accounts. Related credentials and wallets (crypto, Paypal, or others) linked to these accounts are likely of lesser value, they are less likely to raise traffers teams' primary interest.

- On the other hand, YouTube offers a wide audience and a high volume of traffic. It is almost certain that the 911 infection chain is a choice oriented on the quantity of traffic, rather than on the quality.
- Spreading payloads over an open channel, like YouTube, is likely to reduce the lifespan of the malware build, or the C2 server. Every step of the 911 is publicly available. It is therefore obvious to quickly burn the malware builds and the information-stealer C2 servers.

  Distributing stealers using the 911 infection chain possibly results in a low infection rate. Convincing users to download and install cracked software from an unofficial site after disabling their antivirus would only be effective on less sensibilized targets.

Other common infection chains

Other common delivery methods include websites masquerading as blogs or software installation pages to deliver password-protected archives. Some traffers teams display good knowledge of Google Ads, Facebook Ads, Reddit Ads, or other advertising platforms to promote their websites and reach a larger audience through indexing on search engines. Such campaigns are often put in the spotlight as they affect many victims.

Lastly, phishing emails remain one of the most common intrusion vectors used by the traffers. As done earlier by Initial Access Brokers to improve malware delivery performance, traffers adapted their infection chain, moving from Office VBA macros, which are now deactivated by default, to the use of LNK files.

Malware arsenal of traffers teams

Based on data collected from the traffer section (*Трафферы*) on Lolz Guru, SEKOIA established the list of the most used information-stealing malware by traffers teams. For that purpose, we collected the publications of new traffers teams entering into the information stealer business between January and mid-August 2022. The results are as follows:

Redline	54
Meta	8
Raccoon	6
Vidar	5
Private Stealer	4

Here is a timeline of the newly created traffers teams since early 2022:

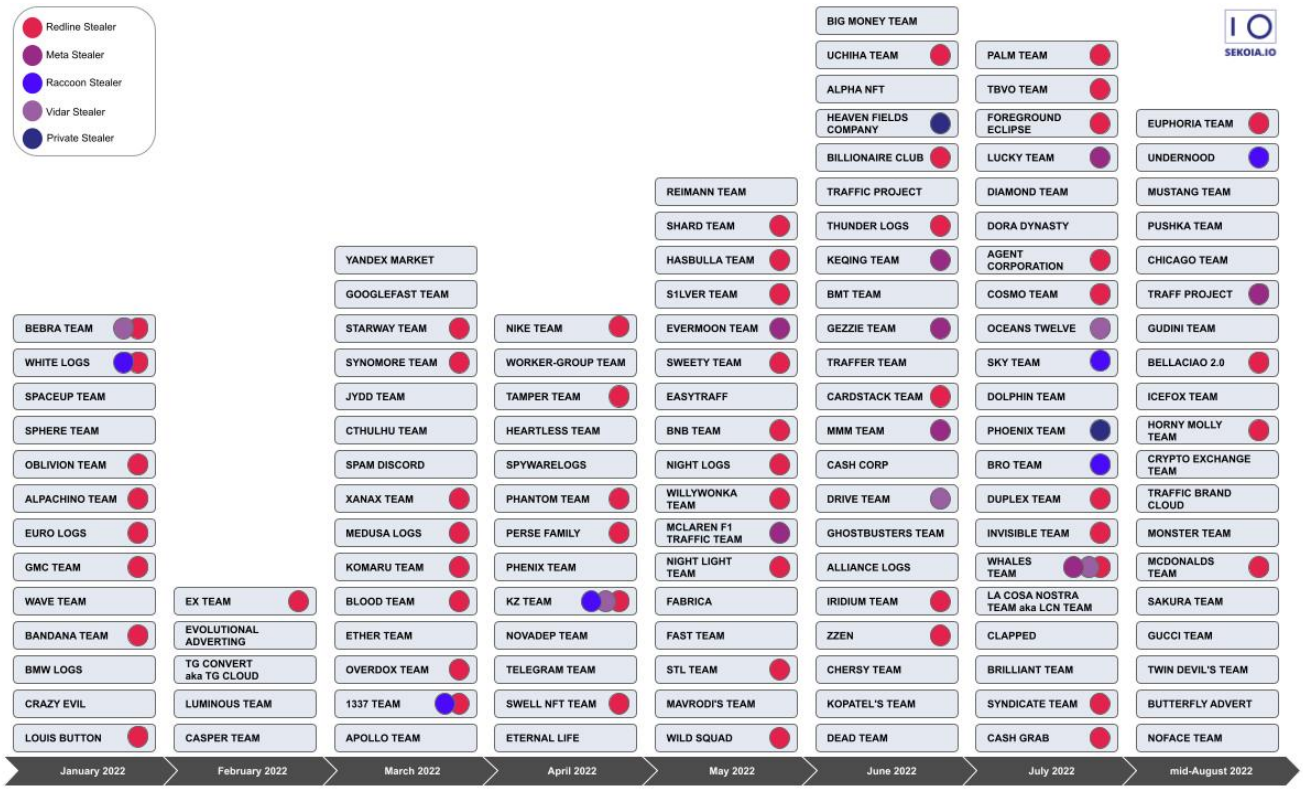


Figure 4. Newly created traffers teams and their associated information stealer, by month in 2022 (Source: Lolz Guru forum, "Traffers" section)

Redline

The majority of traffers teams SEKOIA observed on forums distribute the Redline information stealer, including *Bandana Team, Tigers Team, Cosmo Team, Sky Team, White Logs, Hydra Family, Heartless Team*. Considered by experienced threat actors as the best stealer on the market, Redline offers wide download and execution capabilities, as well as stealing capabilities targeting web browsers, cryptocurrency wallets, data from local system, and several applications (VPN, video games, messenger and others).

Its logs (stolen data) are sold on multiple marketplaces, and custom tools to extract information of interest are also developed and sold on underground forums. Redline's reputation is even used as an asset by the team to recruit new traffers.

From an operational perspective, the Redline builder, which is the software used to compile a new sample of the malware, easily allows traffers team operators to associate a Redline build with a traffer, making it easier to track stolen data by each of the members. This association is possible because a unique botnet name is included in the sample distributed by a traffer. This feature enables SEKOIA to track traffers whose Telegram profile is used for the botnet name, and associate malware builds with Telegram profiles.

Meta

Compared to other stealers mentioned above, Meta Stealer is a newcomer in the Stealer-as-a-Service world. Launched in March 2022, Meta is advertised as an updated version of Redline, with the same main capabilities. It is now the preferred stealer of a few traffers teams, including *EverMoon Team*, *Gezzie Team*, *Lucky Team*, *TraffProject Team*.

Raccoon

Raccoon Stealer 2.0 returns after a few months' break. As shared in our analysis of this threat, Raccoon targets web browsers, desktop applications and extensions for cryptocurrency wallets and data from local systems. It also allows the attacker to download and execute another payload.

Vidar

Although not widely used in traffers teams monitored by SEKOIA, Vidar Stealer is used by *Bebra Team,* the team with the most active community observed on the Lolz Guru forum. Similarly to the previous three, Vidar collects sensitive information from web browsers, cryptocurrency applications and extensions, as well as files from local systems whose extension matches those listed in the configuration. The malware also behaves as a loader by downloading and executing payloads.

Although the 911 infection chain is not highly advanced, traffers using it target a **substantial audience** using the YouTube platform, ranked in the **top 5 most visited websites worldwide**. Traffic generated via this method therefore leads to numerous compromises by the **Redline**, **Meta**, **Raccoon** and **Vidar** stealers. Victims may be **impacted by theft of money, sensitive data, corporate and private accounts, identity theft, or other cascading consequences**.

Later in the report, SEKOIA shares general guidelines to prevent being infected by an information stealer, or to mitigate the threat.

Conclusion

Traffers are threat actors playing a **key role in the augmentation of the threat surface**, and more generally in non-legitimate traffic generation. While the concept of traffers is not new, it is likely their **leveraging of information-stealing malware** will continue in the short term. Additionally, as this model offers low entry barriers and quick investment return, more traffers teams will highly likely emerge in the near future.

Traffers teams dealing with stealers are **organised and centrally managed structures** in which resources and services are made available to members by the team administrators. This allows traffers to focus on distributing team's malware builds, using in most cases the **911 infection chain**, and thus earn money directly from the logs generated from successful compromises.

SEKOIA analysts will continue to monitor the traffers' threat and share the latest trends with our customers. Additionally, we monitor emerging or well established stealers to produce actionable intelligence to our customers, including indicators of compromise for multiple families of information-stealing malware.

How to mitigate the threat?

Understanding how information stealers are distributed and how they work is the first step towards protecting a company's or an individual's information system from this threat.

Here are some general guidelines to prevent being infected by an information stealer:

- Limit software execution to trusted repositories: traffers abuse fake cracked software to spread information stealers. Apply a strict software execution policy to prevent users from downloading malware disguised as fake software installers.
- Use endpoint protection software to automatically quarantine malicious executable files.
- Train users to be aware of phishing threats and avoid clicking on attached files or links in case of any doubt.
- Block outbound traffic on non-standard ports.
- Hunt or block stealer-related indicators of compromise (IoCs).

If prevention was not enough, a successful compromise often leads to the collection and exfiltration of sensitive information from the infected host. In this case, our recommendations of mitigation are:

- Isolate the infected machine and remove the threat.
- Perform anti-malware scan on the infected host to ensure that neither a persistence mechanism was established on the infected machine, nor that another payload was dropped.

- Reset passwords and session cookies, block credit cards. If passwords are stored in web browsers, it is absolutely necessary to renew them, same goes for session cookies. If credit card data is saved into the web browsers, contact the bank to block the affected credit cards.
- Take appropriate measures to limit the consequences of a leak of sensitive documents located on the infected host.

Annex

Annex 1 – Basic concepts used by traffers dealing with stealers

List of some basic concepts routinely used by traffers in their daily activities:

- Build (“билд” in Russian) – a stealer’s sample linked to the traffer’s Telegram account, to gather all collected logs on its Telegram bot;
- Crypter (“крипт” in Russian) – a software used for encryption of a malicious file for anti-virus evasion;
- Installs (“инсталлы” in Russian) – a method to get logs by inciting the user to download a malicious file. Installs are usually developed within a traffers team and shared amongst the team members;
- Logs parsing (from the Russian “чек логов”) – the process of verifying logs to identify and sort logs of interest based on a given query. This can be done manually or automatically, with open source, paid or custom-made software;
- Logs processing (from the Russian “отработка логов”) – the process of analysing logs, also used to refer to log exploitation;
- Knock time (from the Russian “отстук”) – a term used by traffers and team administrators to qualify the rapidity with which a log is received by a traffer after a build is distributed. This term is used to stress a malware’s successful execution rate;
- 911 – a term used to designate an infection chain consisting of taking over a YouTube channel.

Annex 2 – Presentation of the Reimann Team’s organisation and evolution

This case illustrates the evolution of the highly active traffers team Reimann Team and its internal organisation.

Reimann Team has been advertised on the Lolz Guru forum since May 2022. Its representative on the forum stated that the group was active since at least early 2021 and it is almost certain it still is.

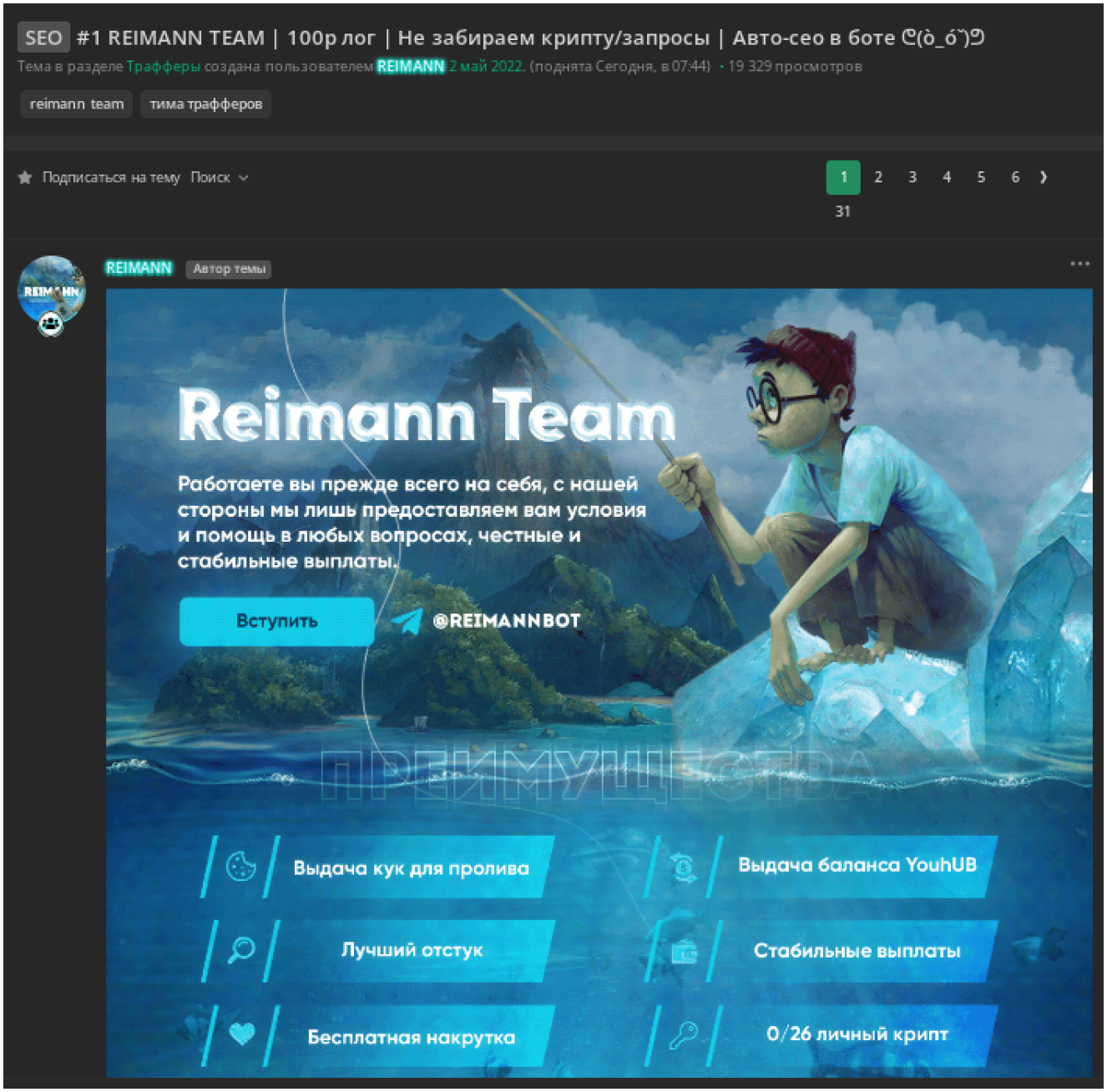


Figure 5. Advertisement aiming at recruiting traffers in Reimann Team (Source: Lolz Guru forum)

Reimann Team is currently recruiting new traffers and offers their team members the following kit of resources:

- Telegram bot for log collection
- Telegram bot for log parsing
- A dozen of Telegram chats and groups for technical support
- YouTube Uploader
- SEO services
- Automated crypts and builds
- A traffer’s manual

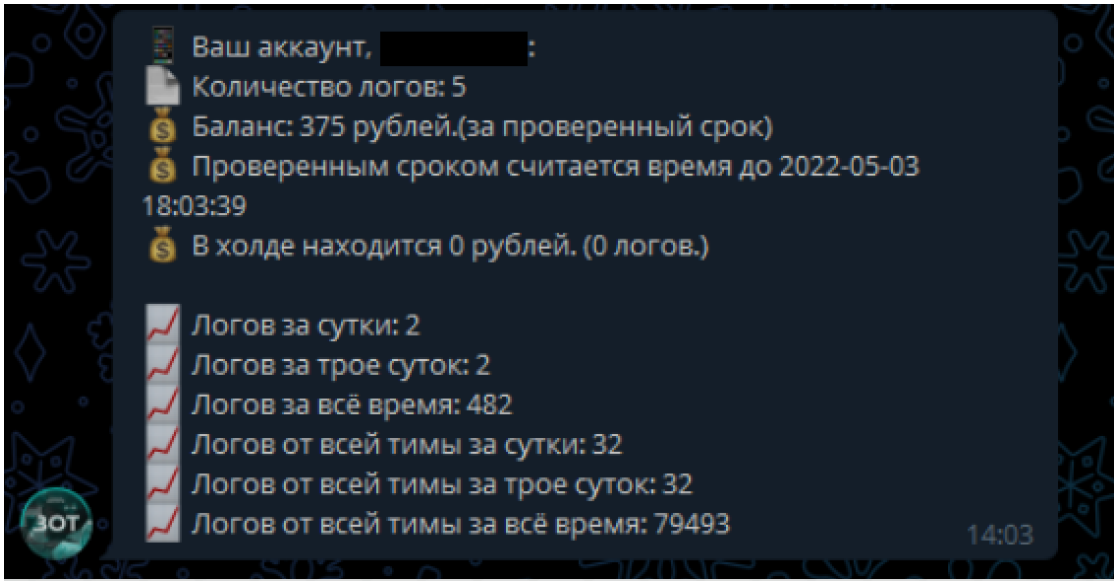


Figure 6. Example of a user interaction with the Reimann Team's Telegram bot. The number of logs collected by each of the traffers and by the entire traffers team is displayed, as well as the revenue generated by every team member at a given time. (Source: Lolz Guru forum)

Reimann Team has two different approaches to pay its members:

- Traffers can submit all the collected logs to its team administrator and then be paid by number of logs;
- Traffers can choose to keep a part of the collected logs to exploit them by themselves;
- Traffers can get 70% of the revenue after the team has exploited its logs.

To encourage a high level of activity, its administrator organises quests and challenges and allocates bonuses.

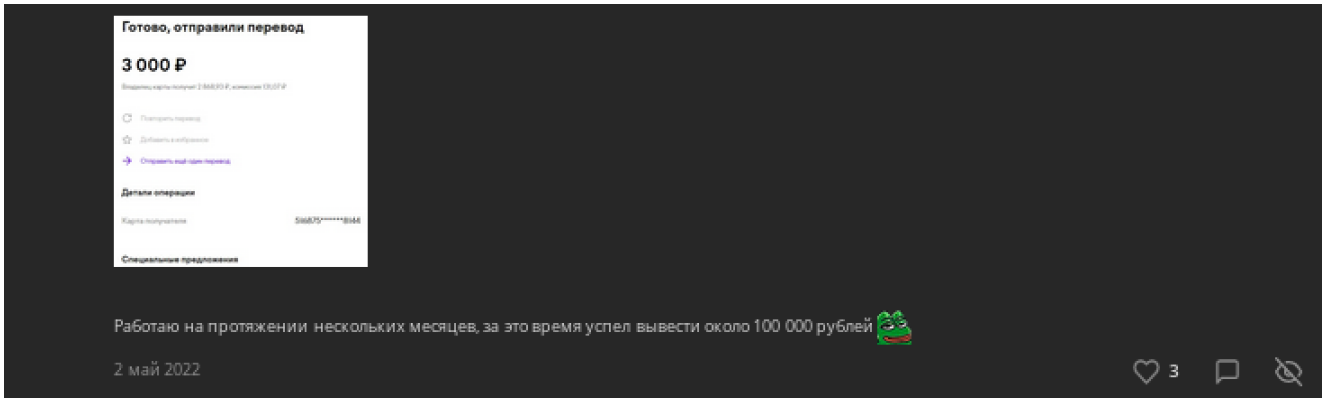


Figure 7. A Reidmann Team traffer's review on the Lolz Guru forum: "I am working now for a few months, and during this time I already received about 100,000 roubles" (the equivalent of 1,350 euros at the date of publication) (Source: Lolz Guru forum)

To monetize received logs, the team representatives are selling them via a marketplace called "Reimann Logs". So they gather the logs obtained by traffers and sell them within 7 days. Logs from Steam, Minecraft and Roblox are particularly mentioned.

Annex 3 – 911 infection chain example

To illustrate the 911 infection chain described in the report, here is a campaign distributing the Redline information stealer using this method, as performed on 18 August 2022.

Step 1

User searches for a tutorial to download Photoshop for free on YouTube. To reproduce this, we entered "*photoshop free download*" in the search bar.

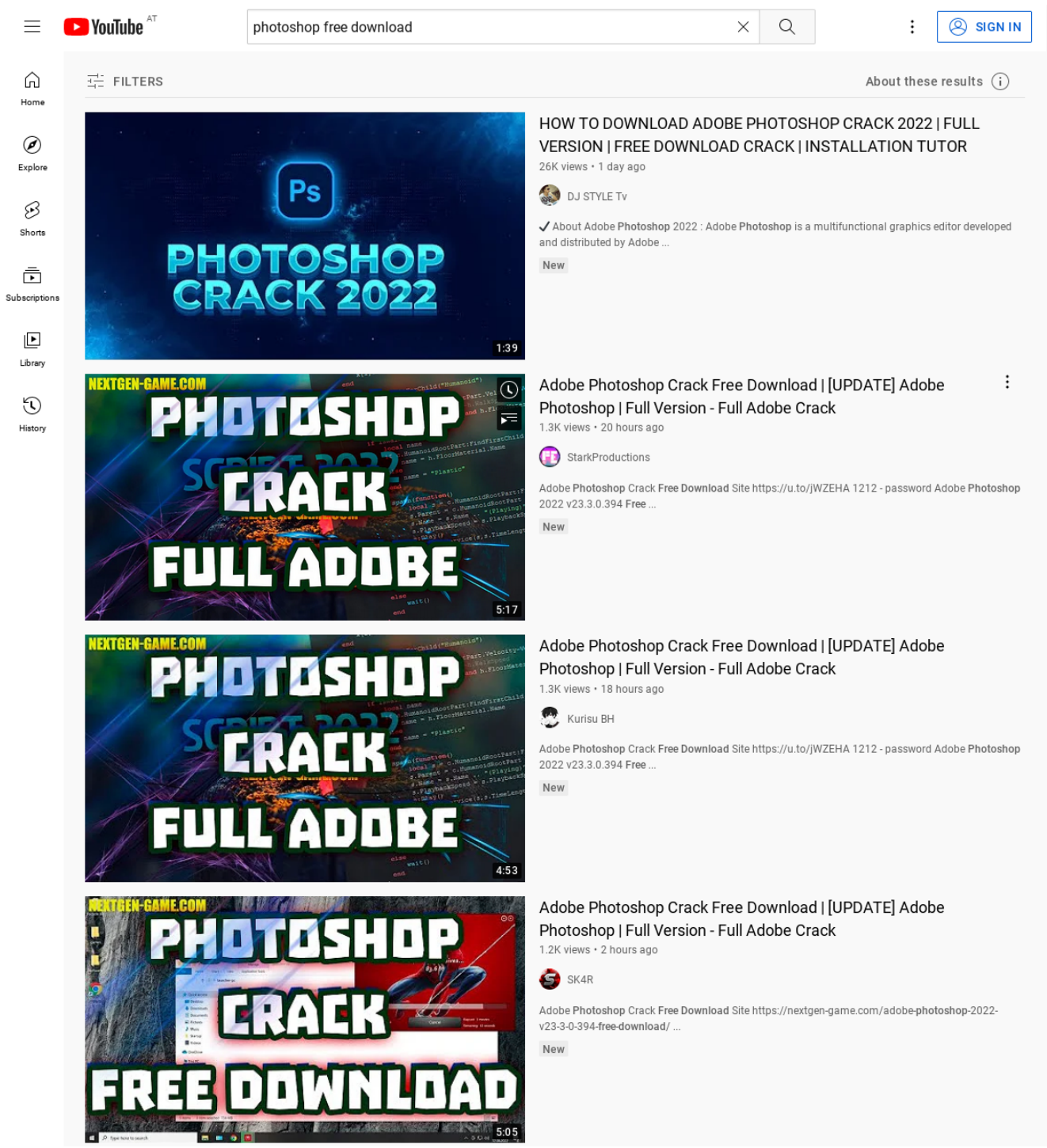


Figure 8. Results for the search “photoshop free download” on YouTube as of August 18, 2022
`hxxps://www.youtube[.]com/results?search_query=photoshop+free+download`

First results are very recent as the videos were published a few hours or days earlier. They were all uploaded on stolen YouTube accounts and they all contain a download link and a password in the description.

Step 2

The content of the first video describes how to install the allegedly free Photoshop version through the following steps:

- Downloading the archive;
- Disabling the “Real-time protection” of the Windows for Microsoft Defender Antivirus;
- Extracting files from the password-protected archive using the password “5105”;
- Running as administrator the executable file.

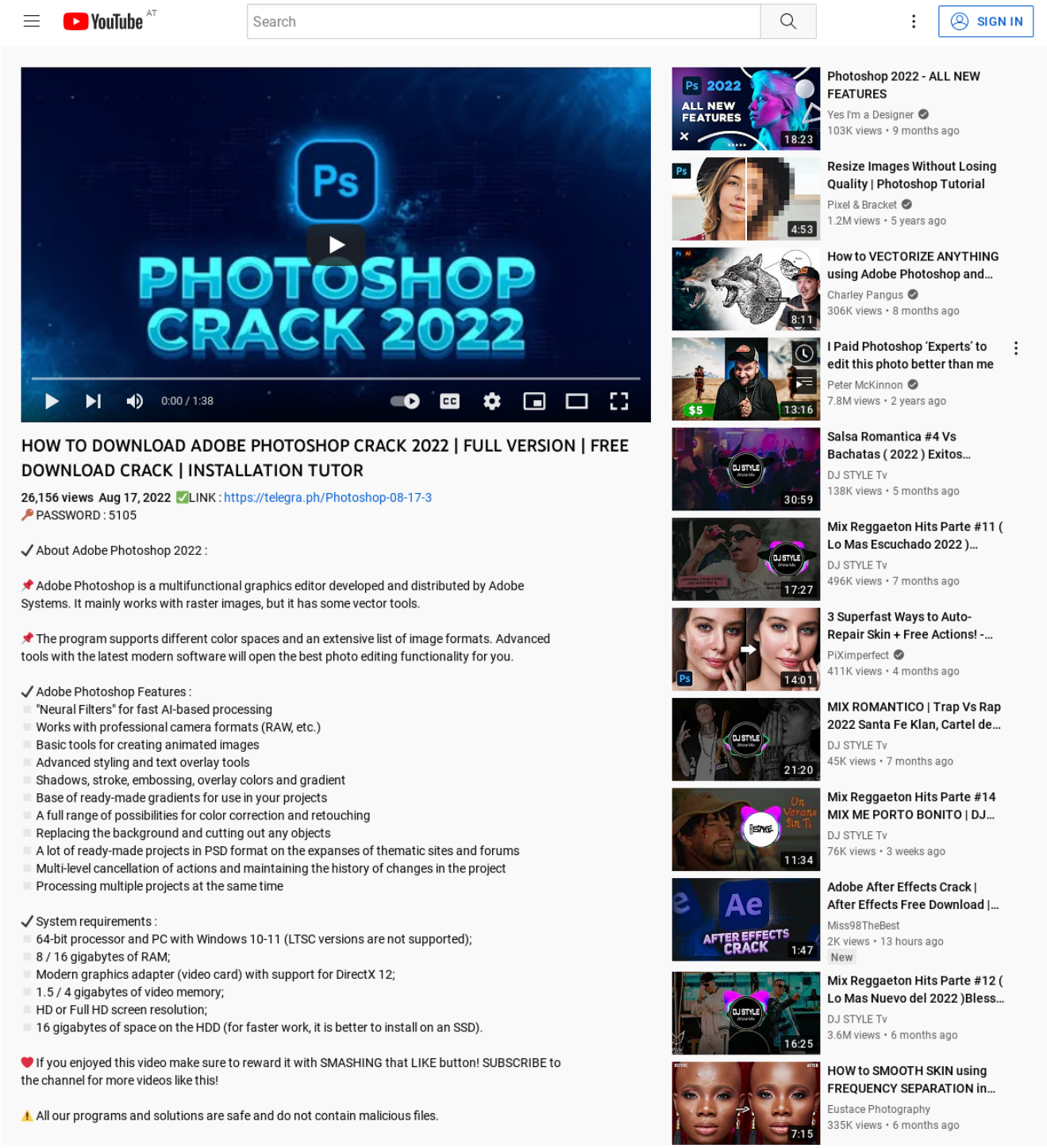


Figure 9. Tutorial to install the allegedly free Photoshop version

`hxxps://www.youtube[.]com/watch?v=7A-yeYc63NY`

The description of the YouTube video contains a link to a telegra[.]ph webpage and a password.

Step 3

The video was uploaded on the stolen YouTube account “*DJ STYLE Tv*” with more than 400,000 subscribers. The legitimate owner of the account was still using this account two weeks earlier to share music mixes.

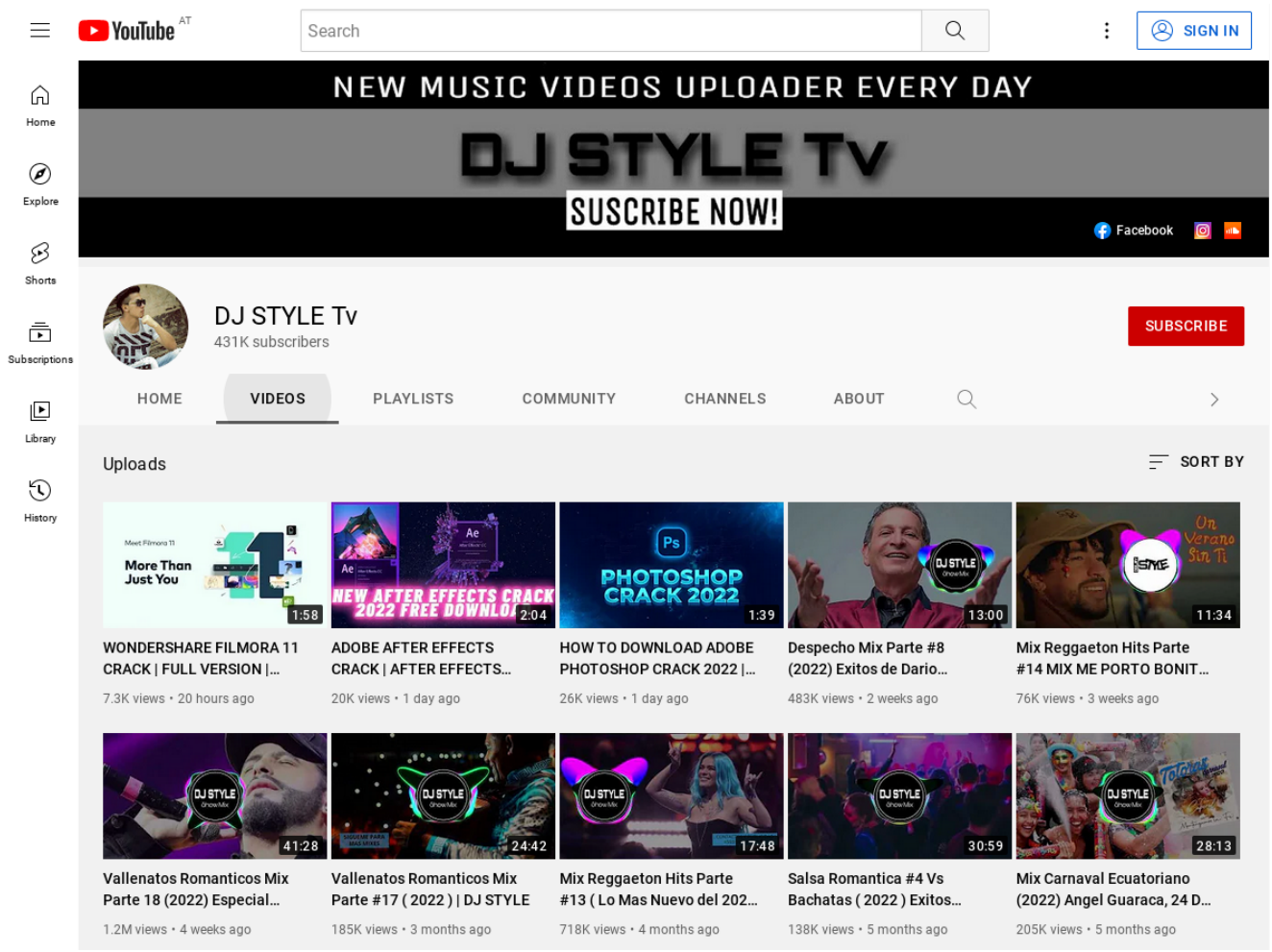


Figure 10. 400k YouTube account on which the tutorial was uploaded

`hxxps://www.youtube[.]com/channel/UCSdTq3mF_zRDyJCR1jxAANw`

Step 4

The user is redirected on a telegra[.]ph web page after clicking the link in the description. The webpage contains a MediaFire link and again the password “5105”.

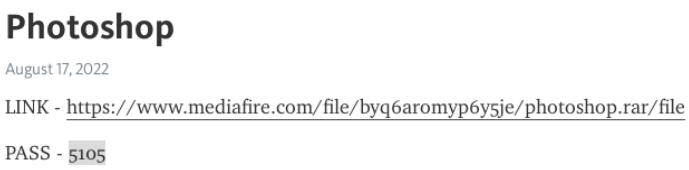


Figure 11. Telegra[.]ph webpage mentioned in the YouTube video description

`hxxps://telegra[.]ph/Photoshop-08-17-3`

Step 5

The user is now redirected to the MediaFire website, on a download page of a RAR archive named "*photoshop.rar*".

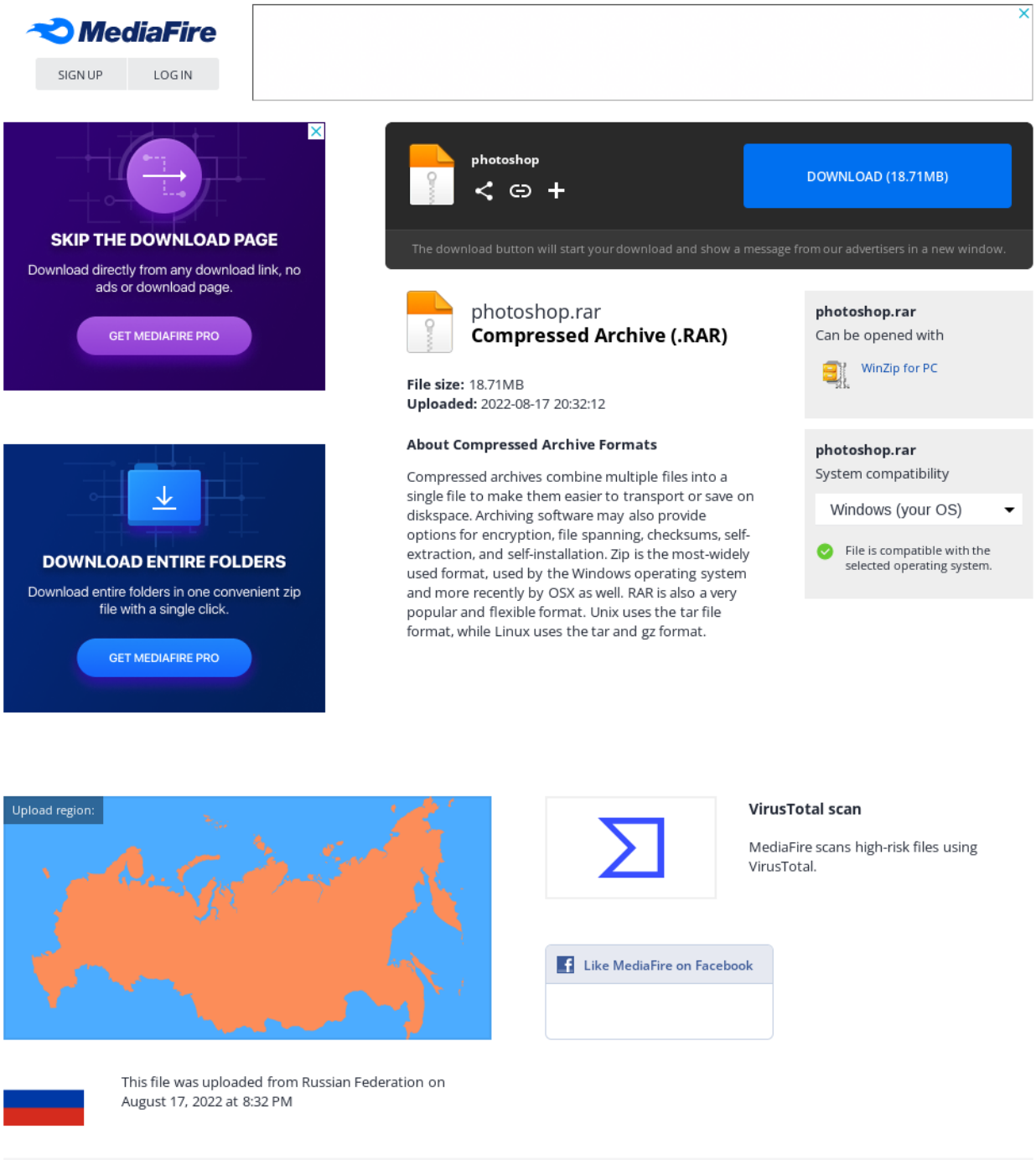


Figure 12. Archive "photoshop.rar" hosted on MediaFire

`hxxps://www.mediafire[.]com/file/byq6aromyp6y5je/photoshop.rar/file`
`hxxps://download2294.mediafire[.]com/vd7oeq9fu5pg/byq6aromyp6y5je/photoshop.rar`

The RAR archive was uploaded on MediaFire from the Russian Federation the previous day.

Step 6

At that stage, the user downloads the password-protected archive and follows instructions from the YouTube video to disable Windows Defender protection, decompress the archive "*photoshop.rar*" and execute the executable file "*photoshop.exe*".

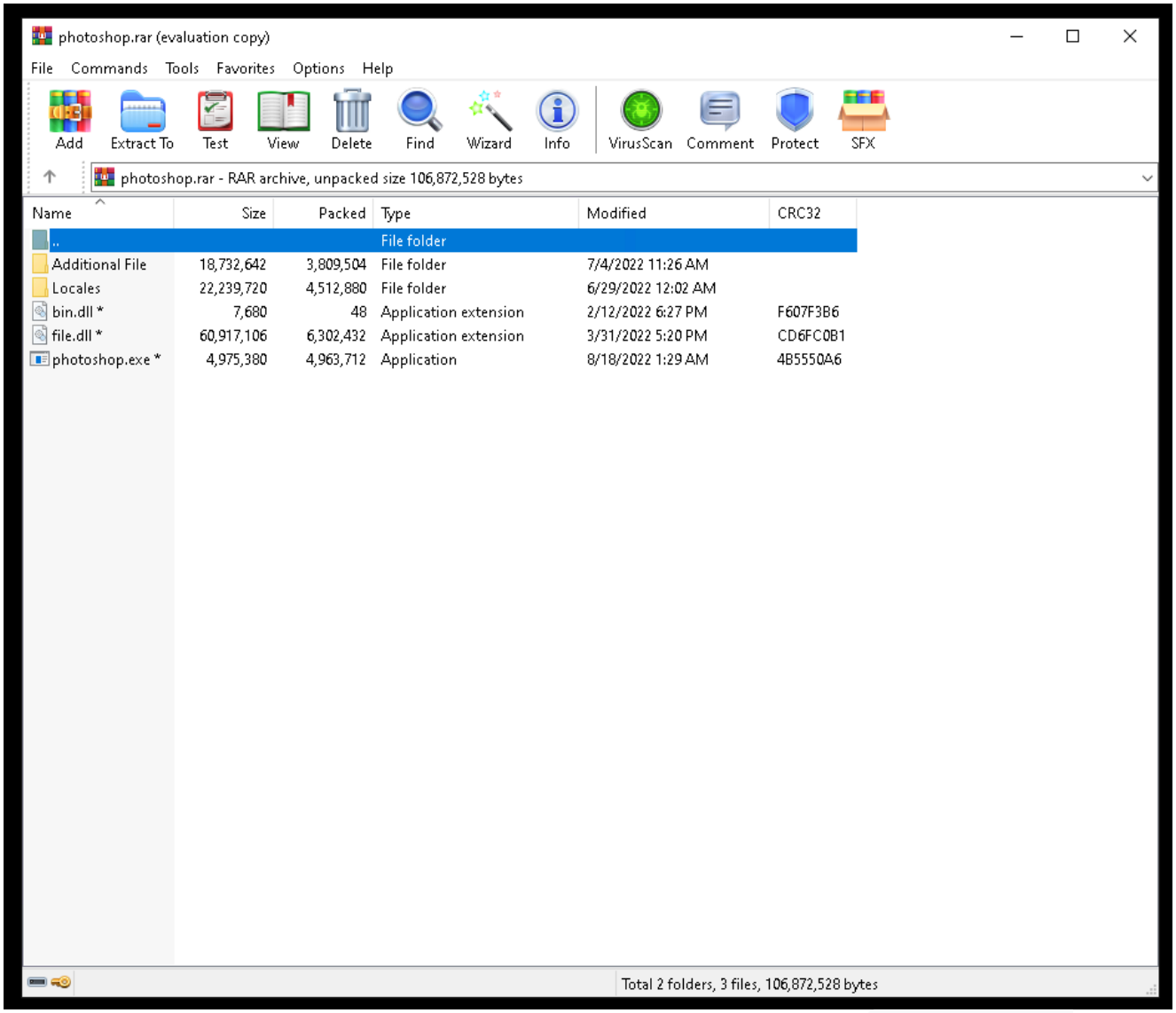


Figure 13. Content of the password-protected archive "photoshop.rar" `photoshop.rar SHA256 462524577af8eb243217386c635682108a17f617d22299492310c1a05605c629 photoshop.exe SHA256 7be64a3fd654b4217c6cf82e6de8fa45e30555b58e7422d77ab49da2f6a10a57`

When run on an environment monitored by SEKOIA.IO XDR, the file is dected as Redline and YTStealer according to SEKOIA.IO CTI. The Redline C2 server is `185.200.191[.]18:80`. Indicators are available on our public portal:

- Network-related IoC on SEKOIA.IO
- File-related IoC on SEKOIA.IO

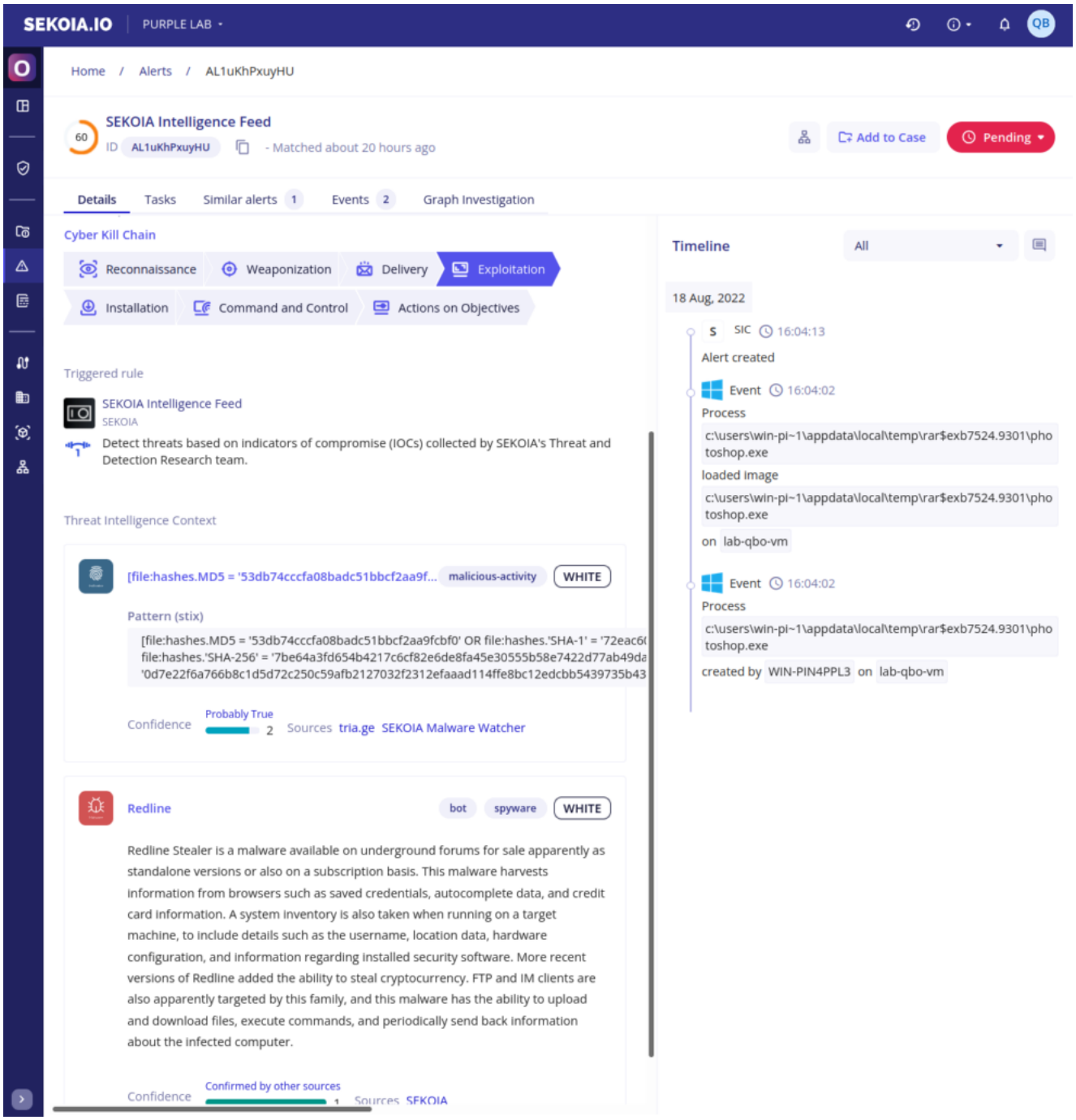


Figure 14. Detection of "photoshop.exe" as Redline in SEKOIA.IO XDR

Chat with our team!

Would you like to know more about our solutions? Do you want to discover our XDR and CTI products? Do you have a cybersecurity project in your organization? Make an appointment and meet us!

Contact us

Comments are closed.