kaspersky

Understanding Malware-as-a-Service

What is Malware-as-a-Service?

The line between renting/selling malware and the Malware-as-a-Service (MaaS) business model is rather fine. Information security experts cite various criteria by which malware can be classified as MaaS. Some believe that MaaS operators must provide bulletproof hosting, drawing an analogy with Software-as-a-Service; for others, a subscription fee is enough to regard malware for hire as MaaS. Malware operators who apply the MaaS label to themselves also attribute a variety of services to this model.

To answer the above question, we analyzed numerous offers and references to MaaS on the surface web, deep web, and dark web, and identified the common components inherent in this model. Further in this report, we consider malware that combines five or more of these components to be MaaS.

Affiliate

A client who purchases malware as a service.

Operator

The owner of a MaaS program (may also call their offer “malware for hire” or an “affiliate program”).

Malware-as-a-Service components

Team of several people

Founders, developers, administrators, support, managers can be singled out. Depending on team size, roles may overlap.

Command-and-control (C2) panel

Core actions are performed on the command-and-control (C2) server. Often the C2 panel is located in the TOR network, but it can also be implemented as an executable file.

Malware and interface upgrades

Operators periodically update the malware and control panel interface, which is included in the cost of the service or carried out for an additional fee.

Support

Available through the C2 panel or Telegram, sometimes 24/7.

Subscription fee paid in cryptocurrency

MaaS is purchased by subscription, but in some cases there is also a lifetime license or a fee on profits.

Builds

Affiliates get a builder in the C2 panel or as separate software; or the operators release builds themselves. These may be included in the cost of the service or provided for an additional fee.

Instructions

Malware operators can provide affiliates with instructions, manuals, and playbooks.

Bulletproof hosting

Provided by the malware operator.

Malware families and categories

During our analysis of various sources, including the dark web, we identified 97 families comprised of malware with similar behavior, modules, and code that were distributed under the MaaS model between 2015 and 2022 inclusive. These families can be split into five categories as per the primary objective: ransomware, infostealers, loaders, backdoors, botnets. In this study, we combined loaders, backdoors, and botnets into one group, since they often have a common goal: to upload and run other malware on the victim's device. Note that we did not include IoT botnets used mainly for DDoS attacks, such as Mirai, Mēris, or Reaper, as these are not distributed under the MaaS model. Operators of such botnets can rent out bots under the DDoS-as-a-Service model, but this is not classified as MaaS.

As can be seen from the graph, most of the malware families distributed under the MaaS model are ransomware. This may be due to their ability to generate higher profits for attackers in a shorter period of time than other types of malware.

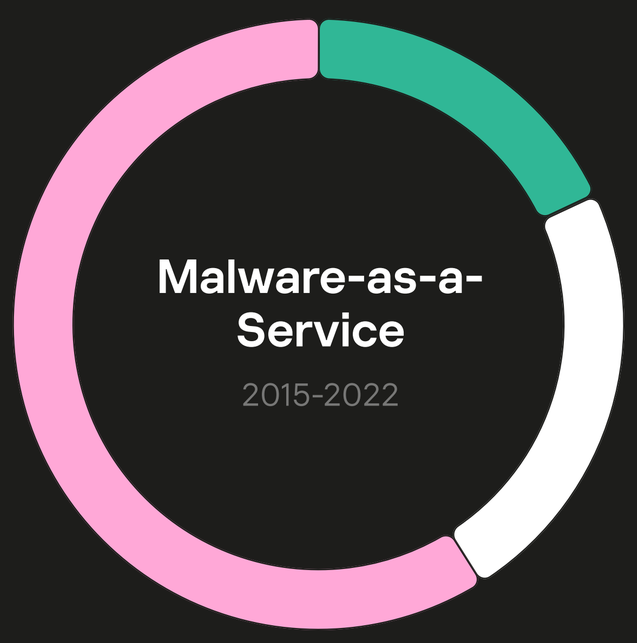
To assess how cybercriminal interest in various MaaS-distributed families has changed, we carried out a retrospective and operational analysis of the activity of dark web communities and identified the ups and downs of individual families by popularity from 2018 to 2022. When studying popularity, we took into account sales, mentions, discussions, posts, and search ads.

Malware families distributed under the MaaS model between 2015 and 2022 inclusive, by type:

Ransomware — 58%

The primary goal of such malware is to encrypt data or block access to it, and then demand a ransom.

Conti | REvil | LockBit | Cl0p | DarkSide



Botnets, loaders, and backdoors — 18%

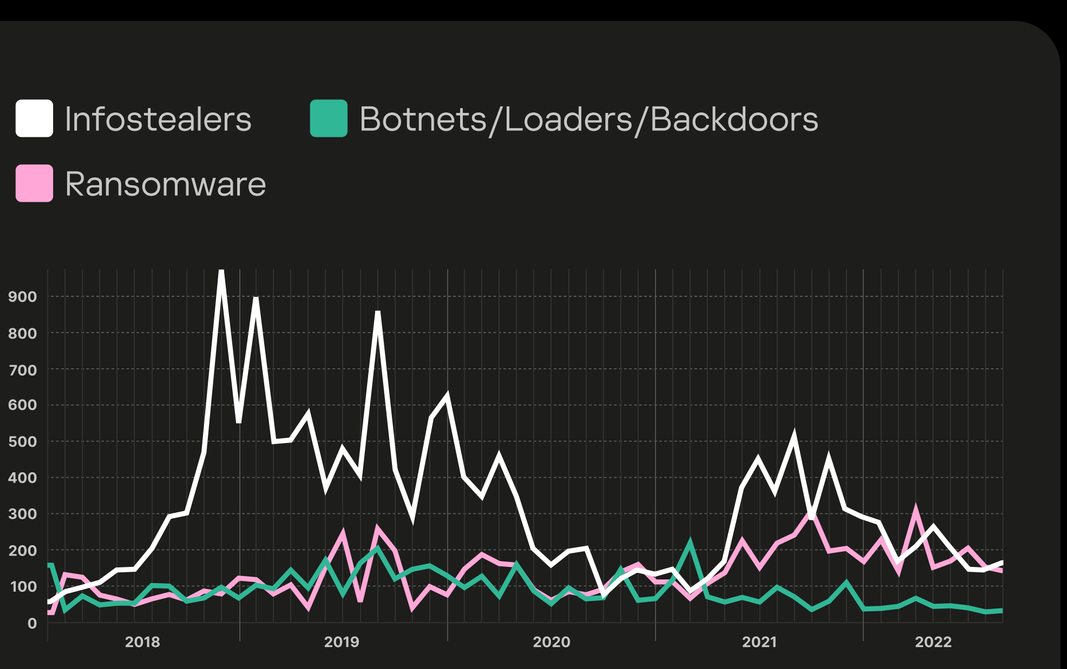
Are combined into one group, as they often have a common goal: to upload and run malicious programs and commands on the victim's device.

Emotet | SmokeLoader | Warzone RAT | TrickBot

Infostealers — 24%

Are malicious programs designed to steal the victim's data.

RedLine | Vidar | AZORult | Taurus | Raccoon

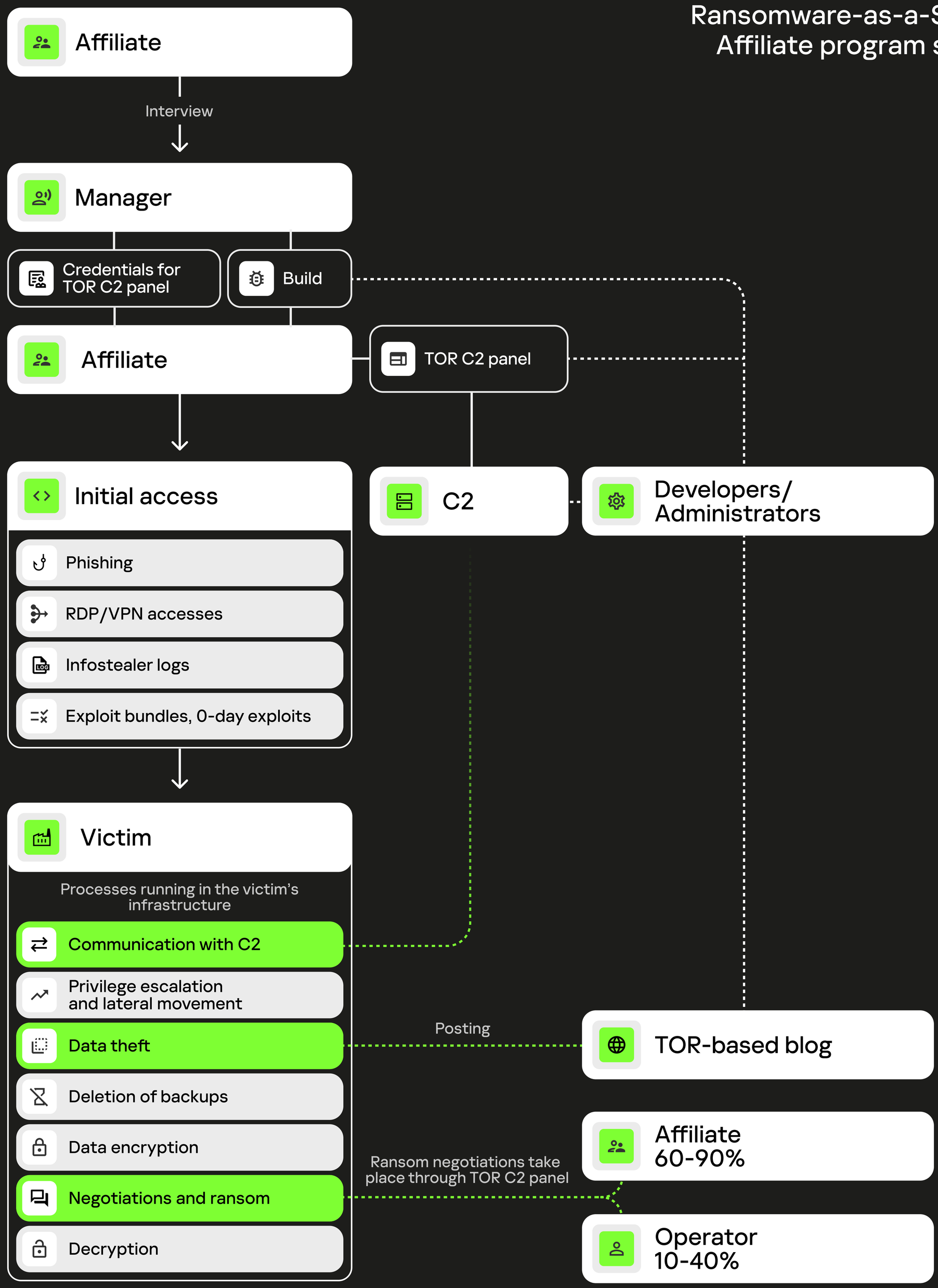


Trends in the number of mentions of MaaS families on the dark web and deep web, January 2018 – August 2022

Despite the fact that most of the malware families detected were ransomware, the most frequently mentioned families in dark web communities were infostealers. Ransomware ranks second in terms of activity on the dark web, showing an increase since 2021. At the same time, the total number of mentions of botnets, backdoors, and loaders is gradually decreasing. For each malware group, we analyzed the main events that generate this activity on dark web resources.

Ransomware (RaaS)

Ransomware-as-a-Service.
Affiliate program scheme



kaspersky

Digital Footprint Intelligence

In the case of ransomware, the average number of affiliates is limited to 5-20 clients. To join an affiliate program, the candidate must pass an interview with the manager. After examining posts about joining affiliate programs, we identified the general requirements for potential affiliates:

- recommended by a current affiliate;
- has a solid reputation on dark web forums;
- can prove their experience with RaaS or demonstrate payments from other affiliate programs;
- deposit of 1 BTC.

If the interview is successful, the partner receives access to the C2 panel in the TOR network, the builder, or the ransomware build.

The affiliate can also contact support. Although support usually answers only questions related directly to the product, malware operators provide various instructions, manuals, and playbooks, covering how to get initial access to the victim's system, methods of lateral movement, privilege escalation, etc.

By analyzing RaaS-related messages in dark web communities, we were able to compile a set of common rules for affiliates, some of which are relevant for other types of malware too:

- do not post the build/builder/C2 panel on VirusTotal, and do not send it to antivirus companies. The source of a leak can be established by digital signature or hash value: affiliates are provided with unique files that can unambiguously be identified;
- do not target companies in specific countries. Malware modules check the system language or keyboard layout at startup;
- do not attack medical, charity, non-profit, or government organizations. The operator will learn about violations from the news. In addition, many operators control or themselves conduct the negotiations with victims;
- do not participate in multiple RaaS programs simultaneously;
- avoid breaks in activity. Inactivity for 1–2 weeks results in exclusion from the affiliate program;
- do not pass builds/accounts to third parties;
- do not disseminate the address of the TOR C2 panel.

Builder in the context of MaaS

A program for quickly creating unique malware samples.

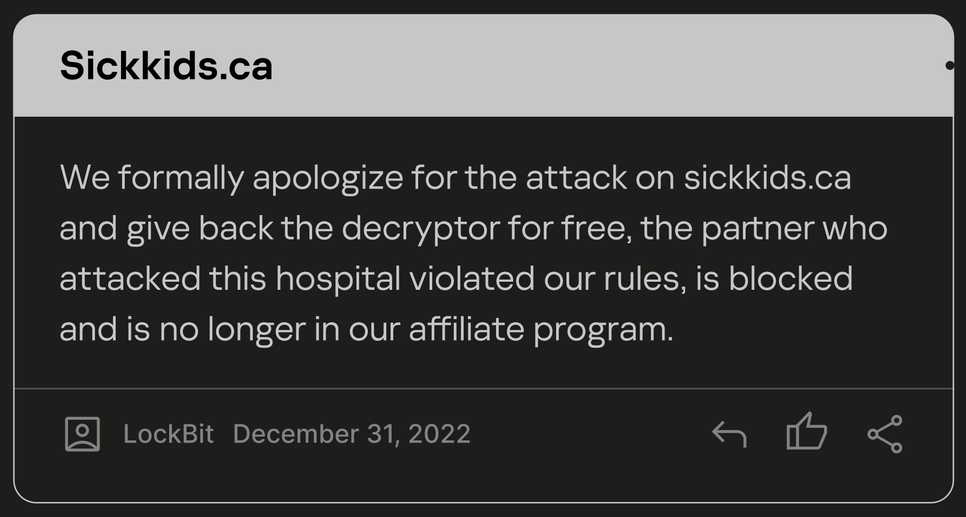
Build in the context of MaaS

Is compiled malware.

Cryptor

A program for encrypting a build to evade detection by antivirus software.

Post about SickKids on LockBit's blog



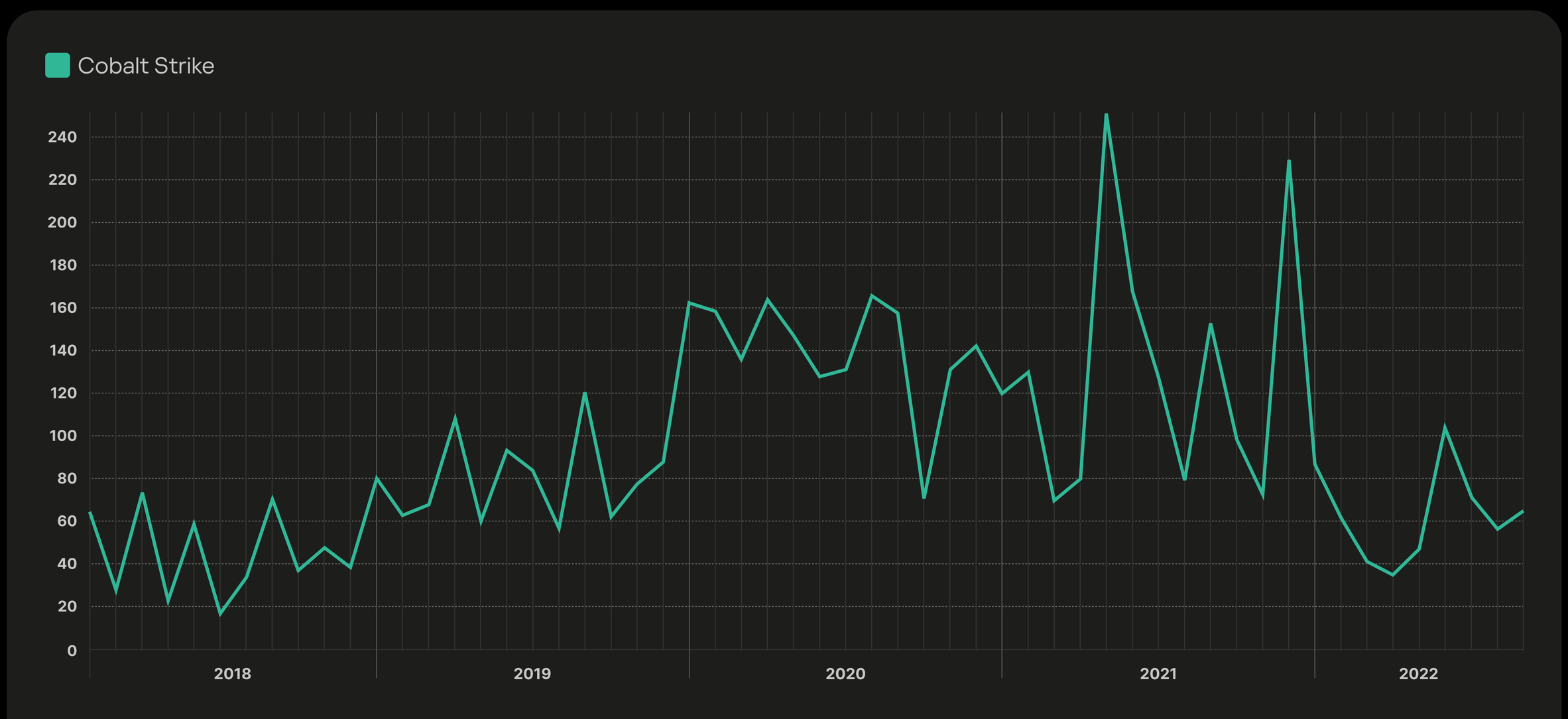
View the screenshot of the post ›

For non-compliance, malware operators threaten to block the affiliate and, in the case of RaaS, to send the decryption keys to victims or security companies. In December 2022, for example, LockBit operators gave the decryption keys to a children's hospital mistakenly attacked by an affiliate, who was subsequently excluded from the program.

On receiving access to the C2 panel and the build, the affiliate independently looks for ways to penetrate the victim's network. Initial access to the infrastructure is obtained by means of:

- phishing;
- RDP/VPN access acquired on the dark web;
- accounts compromised using infostealers;
- exploit bundles, 0-day exploits.

Once the victim is compromised, a periodic connection is established with C2, which is linked directly to the affiliate's C2 panel. The attackers then attempt to escalate their privileges in the system and infect as many devices on the victim's network as they can. Cybercriminals often use Cobalt Strike to communicate with C2 and move laterally. Although popular with attackers, Cobalt Strike is, first and foremost, a legitimate tool used for penetration testing.



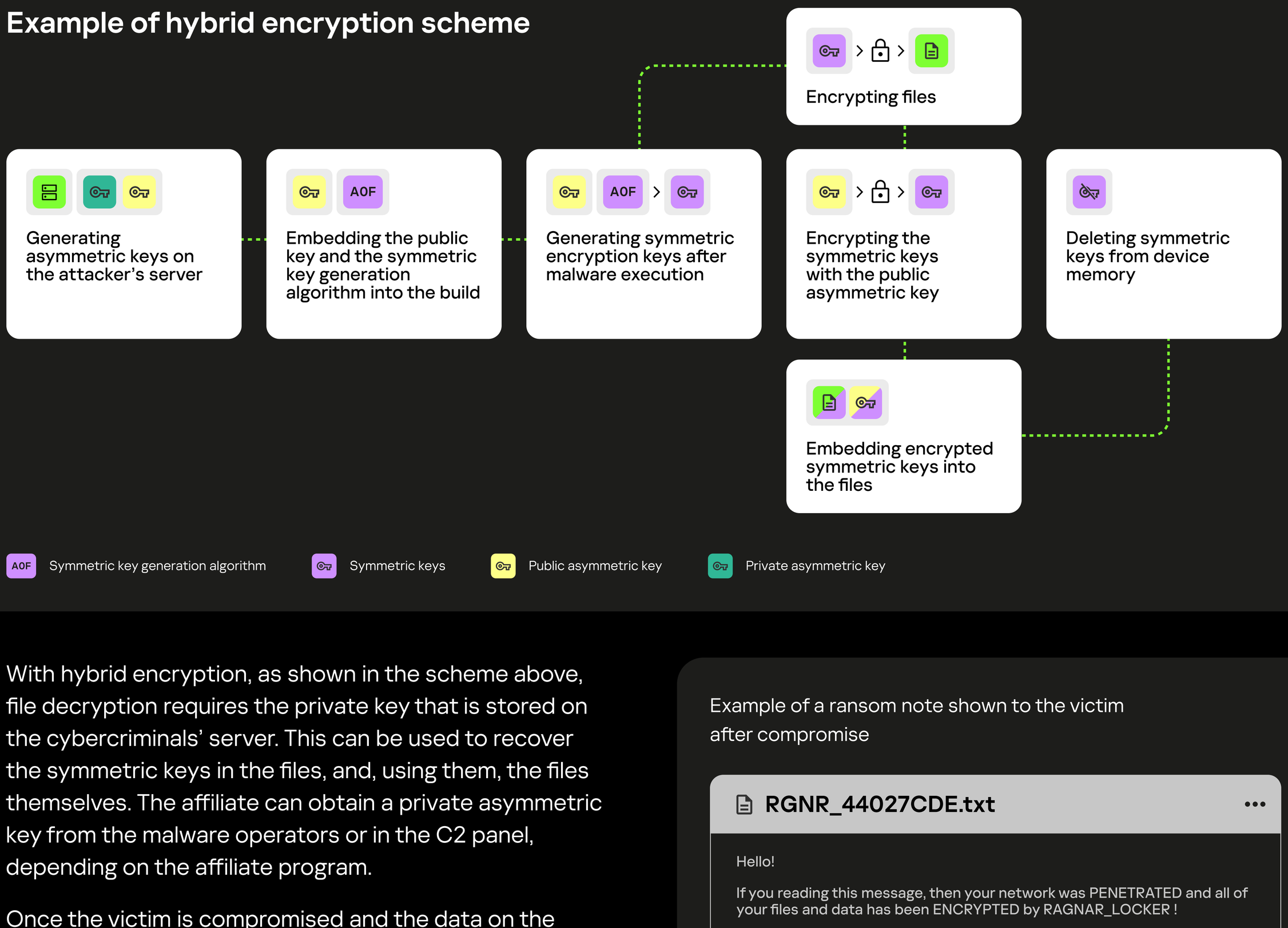
Number of mentions of Cobalt Strike on the dark web and deep web, January 2018 – August 2022

Since early 2018, the number of mentions of Cobalt Strike has increased in dark web communities, many of which are involved in hacking different versions of this software and reselling license keys. Its popularity continued to grow until 2021, peaking in April: after the release of the new version of Cobalt Strike 4.3 in March, numerous ads appeared on the dark web selling licenses and cracks for it.

After successfully infiltrating the target company's infrastructure through privilege escalation and lateral movement, the affiliate's main task is to extract as much sensitive corporate information as possible, deleting backups and recovery points along the way. Some malware operators provide a specialized stealer for data theft; the malware can also feature modules that delete, for example, shadow copies. Once the data is copied and the backups are deleted, the affiliate sets about encrypting the files on the compromised devices.

Attackers use hybrid encryption: symmetric for encrypting files because it is faster, and asymmetric for encrypting the symmetric key because this is often stored in the compromised system. A pair of asymmetric keys can be generated on the attacker's server, after which the public key is embedded in the build, while the private one remains on the server. The symmetric key can be generated directly on the victim's device; at the same time, the malicious sample can create a unique symmetric key for each file. Multiple key generation became widespread after security experts managed to recover a symmetric key by analyzing a large amount of encrypted data. After generating a symmetric key, the malware encrypts the files, then uses the public key to encrypt the key itself and embeds it in the encrypted file. Commonly used symmetric algorithms include AES, ChaCha, and Salsa; asymmetric ones are RSA and ECC.

Example of hybrid encryption scheme



With hybrid encryption, as shown in the scheme above, file decryption requires the private key that is stored on the cybercriminals' server. This can be used to recover the symmetric keys in the files, and, using them, the files themselves. The affiliate can obtain a private asymmetric key from the malware operators or in the C2 panel, depending on the affiliate program.

Once the victim is compromised and the data on the devices is encrypted, ransom notes with initial instructions are created. In one common scenario, the victim is prompted to install the Tor Browser, go to the site specified in the note, and follow the on-screen instructions. In addition, the victim can be assigned a unique ID, which is often associated with the ransomware build or with the address of the cybercriminals' TOR site.

Malware operators or affiliates, depending on the program, post an announcement in a TOR-based blog about the compromise, with the date when they plan to publish the victim's data.

Besides demanding a ransom, some attackers hold an auction on their blog, allowing bidders to get hold of the stolen data before this date or to have the files permanently (so say the attackers) deleted from their servers. This only increases the pressure on the victim, nudging them to pay up. Along with blog posts, pressure can also be applied through L3-L7 DDoS attacks, spam calls and emails, as well as sending the demands to the victim's printer. What's more, the ransom amount can be increased after a certain period of time.

Example of a ransom note shown to the victim after compromise

RGNR_44027CDE.txt

Hello!

If you reading this message, then your network was PENETRATED and all of your files and data has been ENCRYPTED by RAGNAR_LOCKER !

! ! ! ! ! WARNING ! ! ! ! !

- DO NOT Modify, rename, copy or move any files or you can DAMAGE them and decryption will be impossible
- DO NOT use any third party or public decryption software, it also may damage files
- DO NOT Shutdown or reset your system

There is ONLY ONE possible way to get back your files - contact us and pay for our special decryption key! For your GUARANTEE we will decrypt 2 of your files FOR FREE, as a proof of our capabilities. Don't waste your TIME, the link for contacting us will be deleted if there is no contact made in closest future and you will never restore your DATA. HOWEVER if you will contact us within 2 day since get penetrated - you can get a very SPECIAL PRICE.

ATTENTION !

We had downloaded more than 10TB of data from your file servers and if you don't contact us for payment, we will publish it or sell to interested parties. We gathered the most sensitive and confidential information about your transactions, billing, contracts, clients and partners. And be assure that if you wouldn't pay, all files and documents would be publicated for everyones view and also we would notify all your clients and partners about this leakage with direct links. So if you want to avoid such a harm for your reputation, better pay the amount that we asking for.

! HERE IS THE SIMPLE MANUAL HOW TO GET CONTACT WITH US VIA LIVE CHAT !

We provide you with links to download a TOR browser and to Live Chat, as well as a link to a blog with your details. Install TOR browser and open Live Chat. Follow the further instructions on the site, you will see a "chat" tab at the top. Send your message there and wait for a reply (we are not online 24/7, so you will have to wait your turn).

If TOR is restricted in your area, use VPN.

View the screenshot of the ransom note ›

Example of LockBit's RaaS blog

Depending on the program, either the affiliates themselves can lead the negotiations with the victim and set the ransom amount through the C2 panel, or the malware operators. In the second case, affiliates may be allowed to read the exchange of messages.

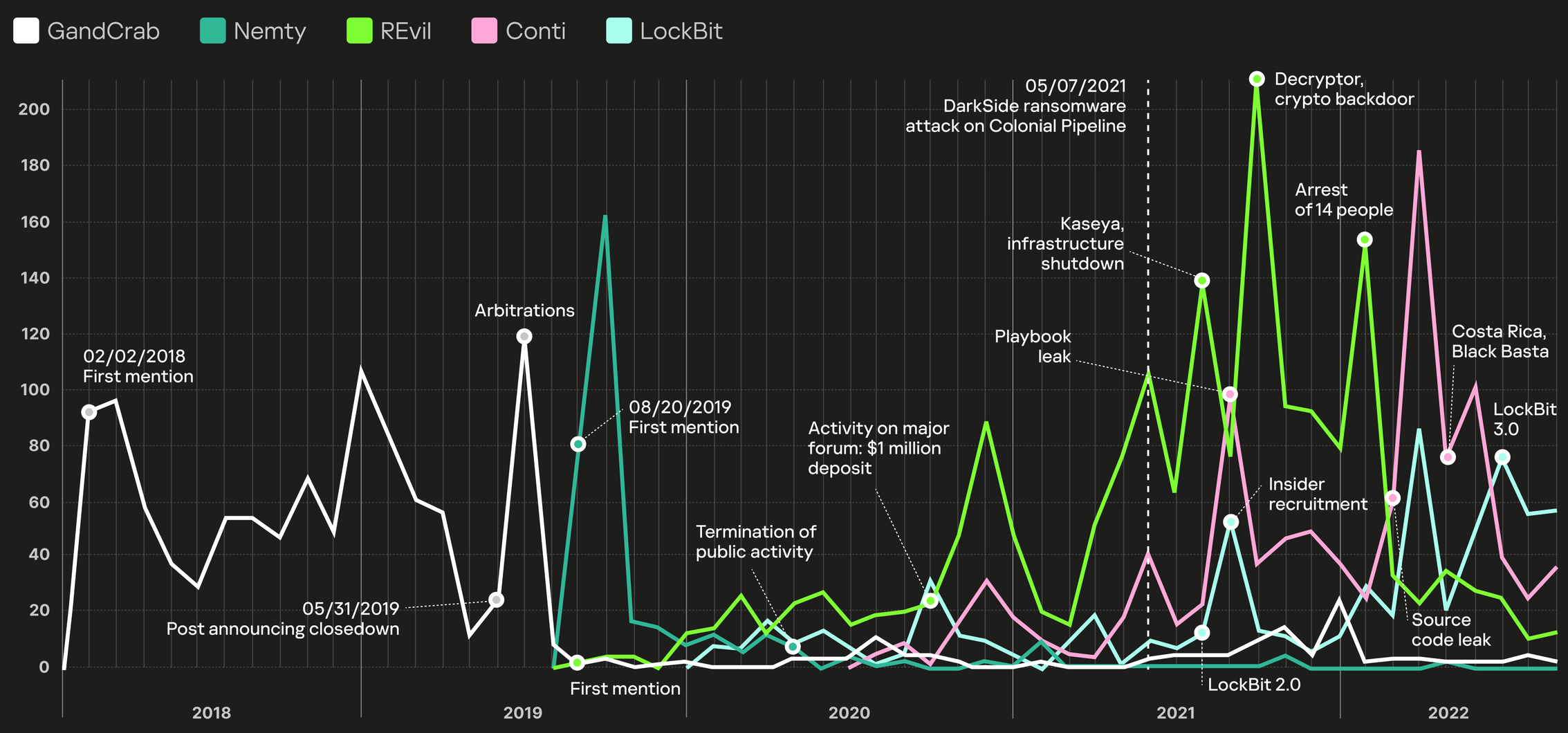
The ransom can be paid either to an escrow cryptocurrency wallet – from where the malware operators' system automatically distributes the money to their and the affiliate's wallet – or straight to the latter's wallet, who then pays an agreed percentage to the operators. On average, the operator's share is 10-40% of the ransom payment.

RaaS evolution

We analyzed the evolution of the five most popular RaaS families based on mentions in dark web communities.

On February 2, 2018, a major forum saw the first post about the new RaaS operation GandCrab, which quickly gained popularity in underground circles and earned operators and affiliates $2 billion, according to a group spokesperson.

The RaaS operation developed rapidly at first, but then the release of updates was delayed, which was followed on May 31, 2019, by an announcement of its closure; GandCrab's operators blocked access to C2 panels and deleted the decryption keys, causing affiliates to issue claims against the group soon afterwards.



Number of mentions of five ransomware families distributed under the MaaS model on the dark web and deep web, 2018–2022

In August 2019, the first mentions of the REvil ransomware appeared in dark web communities, and it was assumed to be GandCrab's successor. The emergence of this malware dates back to April 2019, when mentions of GandCrab were minimal. In September 2020, on a well-known forum, REvil made a deposit of 99 BTC ($1 million at the time), showing they had no problems with money and thus attracting new affiliates. Also in August 2019, in addition to the first mentions of REvil, a new RaaS operation called Nemty reared its ugly head. Again, researchers speculate links with GandCrab.

A turning point for ransomware was the DarkSide attack on Colonial Pipeline on May 7, 2021. After this incident, major forums announced the removal of all posts related to the distribution of any ransomware. They were indeed removed, but the total number of mentions of this type of malware only increased: operators' and affiliates' accounts remained active, and they continued to discuss their activity.

Deposit

Is used to guarantee quality of service. If a dispute arises, the affected party can open an arbitration. On proving their case, they receive compensation from the forum out of the deposit. If there are multiple claimants, the deposit is distributed proportionally.

On July 2, 2021, the REvil group attacked Kaseya's supply chain using a zero-day vulnerability. Shortly afterwards, on July 13, the operators' infrastructure was shut down. In September 2021, REvil decryptors appeared in the public domain, as did posts about an internal crypto backdoor that allowed the malware operators to defraud their affiliates at the ransom payout stage. In January 2022, 14 individuals associated with REvil were arrested. According to US authorities, at least one of those detained had taken part in the DarkSide attack on Colonial Pipeline.

Example of a post about banning ransomware on a well-known forum

No more ransom! Banning lockers on the forum ...

No more ransom! Friends, our forum has **banned lockers** (ransomware) and everything related to them. Specifically:

- Ransomware affiliate programs
- Ransomware for hire
- Sale of lockers (ransomware)

All topics that fall under this rule will be deleted. Fortunately, not many were found.

A more detailed explanation. Reasons behind the ban.

It's no secret that I personally don't like lockers. Why? Few lockers are of technical interest. Most (not all) are mediocre technical tools.

The main reason for the forum's existence is knowledge. We're a technical forum: we learn, research, share knowledge, write interesting articles. The sole purpose of ransomware is to make money. The goals don't match. Sure, everyone needs money, but not to the detriment of one's core aspirations. After all, we're not a marketplace.

The degradation is evident. Newbies hear crazy stories in the media about millions of virtual dollars to be had, which they'll never get their hands on. They don't want to learn how to code or anything, they just think it's all a matter of "encrypt, get $." They run to github, look for lockers, then race off to encrypt everything they see. Since our forum is geared toward newbies, this factor matters to us.

There's too much PR. Lockers (ransomware) have accumulated a critical mass of nonsense, gibberish, hype, and noise. When you meet a "professional ransomware negotiator," you realize you're staring through the Looking-Glass, or just gone mad. What's more, 90% of this madness was created artificially, feeding the hype. By those who make a tidy sum from it (exchanges, insurers, intermediaries, media, etc.)

Admin May 14, 2021

View the screenshot of the post >

In August 2021, the manuals for the Conti ransomware provided to affiliates were made public. They describe in some detail what to download and how to use Cobalt Strike, attack the Kerberos protocol, disable Windows Defender, collect account information, and much more. In late February 2022, as a result of a conflict inside the group, some internal chats and source code were leaked. In April, Conti terrorized Costa Rica with a series of cyberattacks accompanied with a stream of posts on the group's blog. Immediately after these attacks, the group's infrastructure was shut down. There is speculation that the onslaught on Costa Rica was part of an advertising drive by the group and its discreet division into smaller affiliate programs. In particular, the new RaaS operation Black Basta that appeared in April is believed to consist of Conti members.

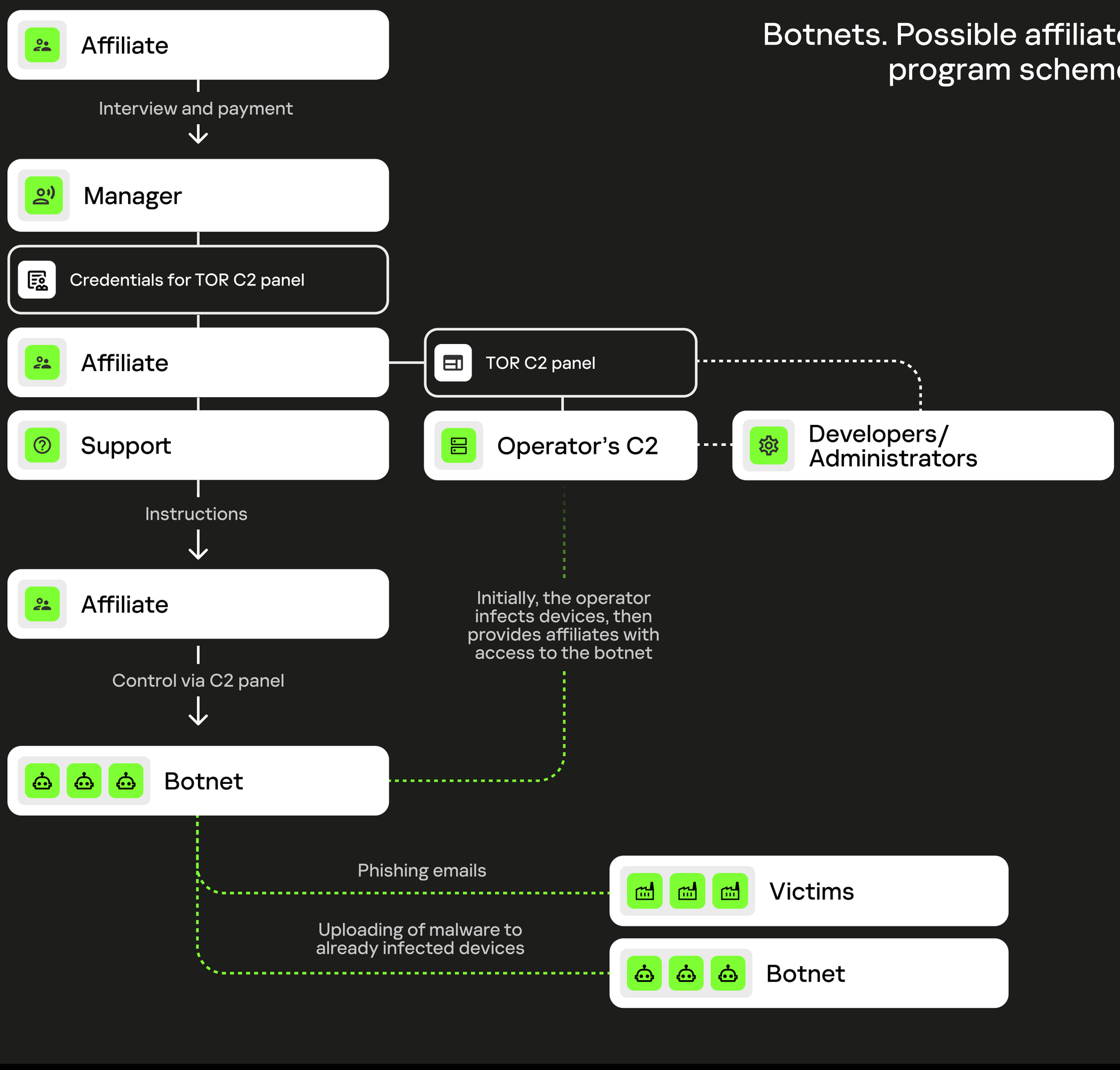
Botnets, loaders, backdoors

We grouped botnets, loaders, and backdoors together based on their common goal of uploading and running malware on infected devices. They are somewhat similar to each other, but with characteristic differences.

1. Botnets are built to control infected devices en masse. For the purposes of this report, we selected those families provided to affiliates in the form of a C2 panel for managing infected devices with the ability to upload their malware to those devices.
2. Loaders are aimed at single targets; the affiliate receives a sample of the malware.
3. Backdoors, in addition to loader modules, have many others for managing infected devices; the affiliate receives a sample of the malware.

The basic difference between a loader and a backdoor lies in the chief purpose of the malware. The main requirement for a loader is to stealthily install and execute files on the victim's device. Backdoors, on the other hand, generate a fair bit of noise on the part of protection tools, but deliver full control over the compromised system, sometimes in more than one way, while uploading and executing files is a secondary goal for them.

Let's see how MaaS operators and affiliates interact in the case of a botnet.



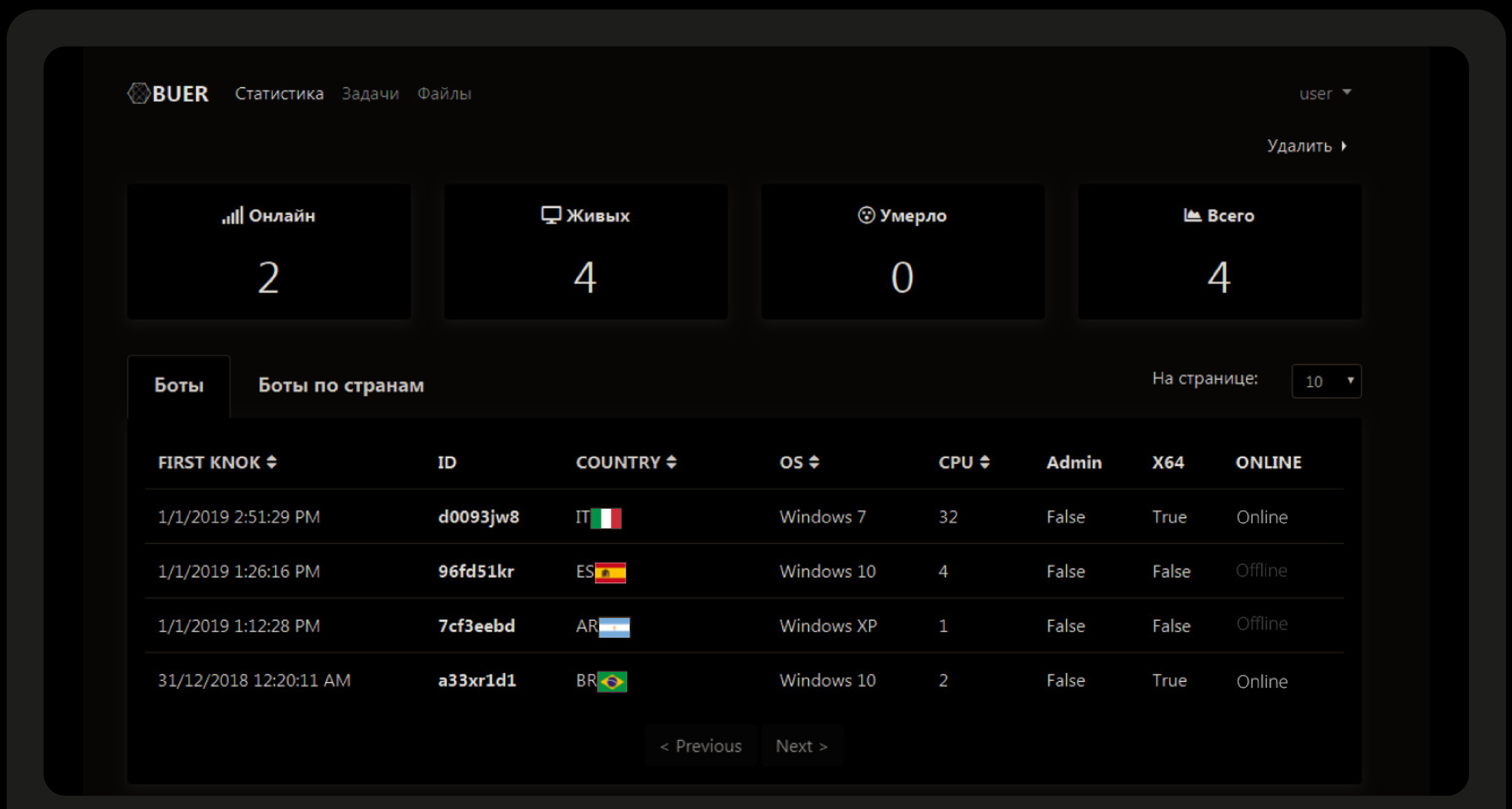
Botnets. Possible affiliate program scheme

Most often, malware operators infect devices by means of phishing. Victims' devices are grouped into one network, ready to execute the attackers' commands. Frequently, malware operators use botnets to send out more malicious emails and infect new devices in order to expand the botnet.

After negotiations with the operator's manager, the affiliate gains access to the botnet's C2 panel. In this case, instead of a sample of the malware, the affiliate gets access to the infected infrastructure, which is broadly analogous to the Platform-as-a-Service model. Because malware of this type has loader modules, affiliates can deliver other malware to already infected devices. Another way for affiliates to use a botnet is to send mass phishing emails with their own malware, which further helps to spread it. Such botnets are not geared toward DDoS attacks. After successfully infecting the victim, the compromised device establishes a connection with the C2 server of the affiliate, not of the operators.

Loaders are similar in functionality to the type of botnets mentioned above: they use similar modules for uploading other malware onto the infected device. The main difference is that the affiliate must find their own ways to spread the malware, since here the operators provide only the malware, and not ready-made infected infrastructure.

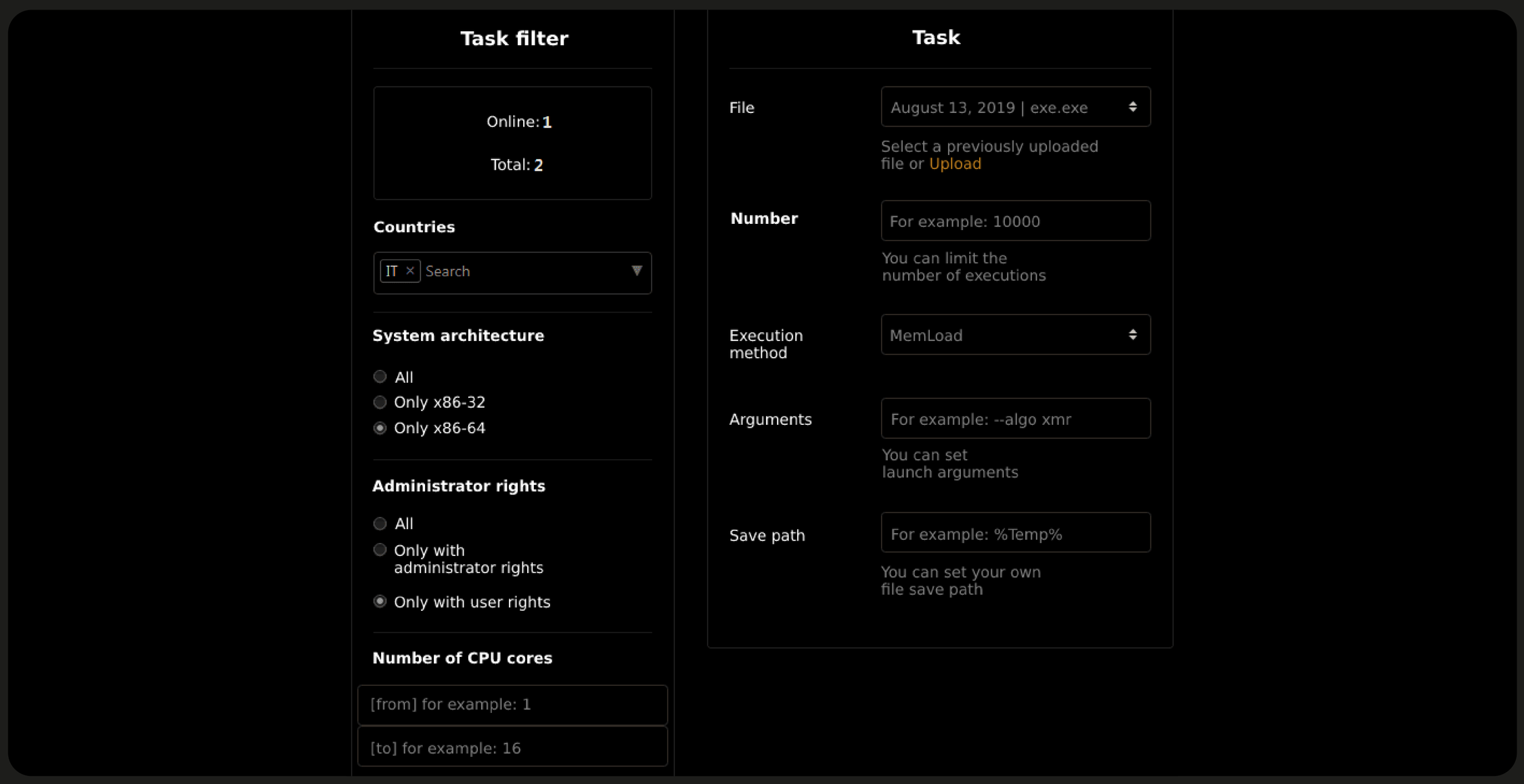
Below is the C2 panel of a loader. The statistics tab shows how many devices are infected in total as well as how many of them are online. There is also information about the victim's first communication with the C2 server, the country where the device is located, the operating system, the rights of the compromised user, and status.



C2 panel of Buer Loader. Statistics

In the C2 panel, the attacker can schedule tasks and configure filters and parameters for them. The loader makes it possible to upload any file up to 28 MB in size to the victim's device at the specified path, and run it with the selected execution method and arguments.

C2 panel of Buer Loader. Tasks



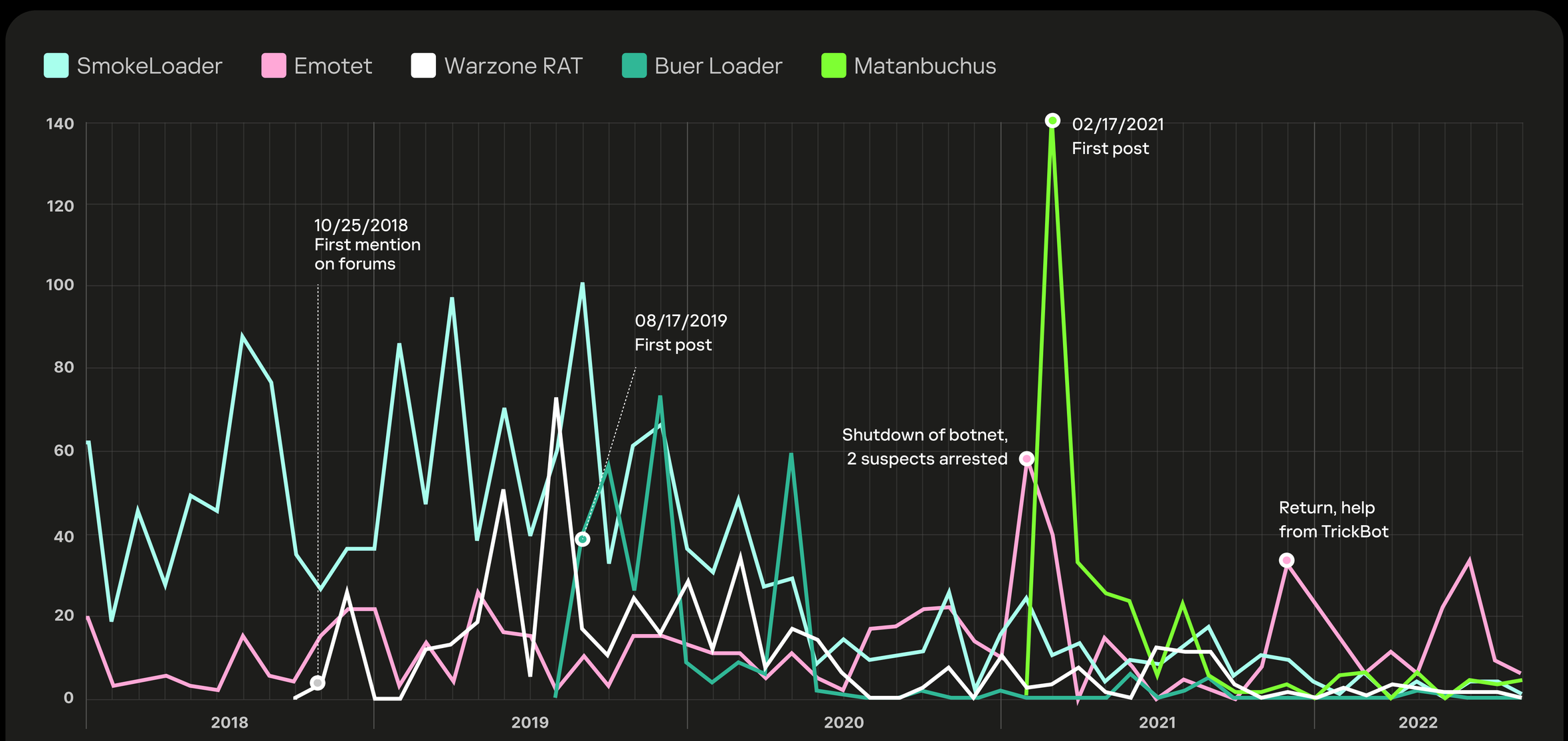
View the original screenshot ›

In the case of a backdoor distributed under the MaaS model, the affiliate likewise independently spreads the malware and infects devices. Below is a C2 panel with a built-in builder and a list of possible actions in the compromised system.

Malware can be used as a tool for uploading and running other malicious programs, and for executing malicious commands on the victim's device.

C2 panel of Warzone RAT

Evolution of botnets, loaders, and backdoors



Number of mentions of five families of botnets/backdoors/loaders distributed under the MaaS model in dark web and deep web communities, January 2018 – August 2022

We analyzed the evolution of the five most popular families of botnets, backdoors, and loaders distributed under the MaaS model, based on mentions in dark web communities.

Bursts of activity related to this category of malware are few and far between on dark web forums. That said, Emotet is worth a look.

Emotet is a private botnet, its creators do not post ads on forums, and only major malware operators can purchase it under the MaaS model. This malware is known for uploading TrickBot and QBot onto infected devices.

In January 2021, Europol, the FBI, and law enforcement agencies in many countries managed to seize control of the botnet. At the same time, Ukraine's cyberpolice announced the arrest of two individuals suspected of supporting the Emotet infrastructure. In the spring of 2021, the botnet was effectively liquidated by sending an update to the infected devices that caused Emotet to self-delete.

Emotet and TrickBot

Were originally implemented as bankers, but later evolved into botnets capable of sending out mass phishing emails and uploading various malware onto infected devices.

It took the cybercriminals almost 10 months to rebuild the infrastructure, and in November 2021 Emotet returned. At first, it was delivered to victims through TrickBot, a private botnet also supplied under the MaaS model, and Emotet operators, in turn, provided access to the compromised infrastructure as initial access broker to Quantum, Conti and BlackCat ransomware. Now, Emotet is distributed on its own through phishing emails.

Below is an example of interaction between Emotet, TrickBot, and Ryuk/Conti.

Clearly, the operators of different affiliate programs interact with each other – note in this regard that Conti is considered the successor to Ryuk. Researchers also believe it was Conti's operators who persuaded the Emotet group to revive its botnet.

Emotet and TrickBot trade places

Infostealers

How they work

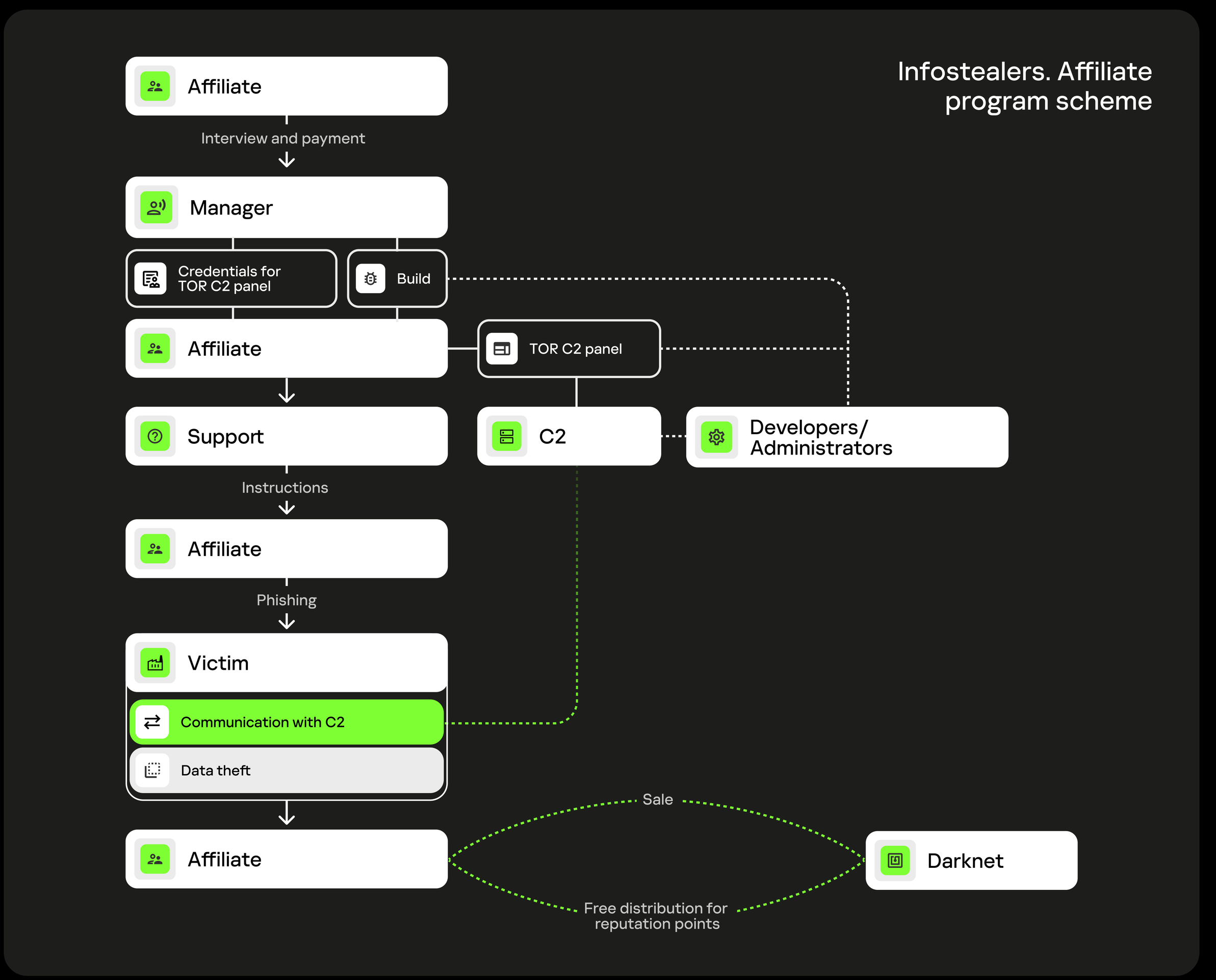
Infostealers got most mentions in dark web communities in 2018-2022. They are more mass-distributed than members of the other categories of malware under review. Whereas the main target of ransomware is companies, infostealers are used to infect all kinds of victims. Botnets, backdoors, and loaders also target everyone, but are less widespread than infostealers.

At the beginning of this report, we mentioned the blurring of the boundaries of the whole MaaS concept. This is particularly true for infostealers. The services provided by operators are very similar and differ mainly in whether C2 hosting is included or the affiliate has to provide it. Hence the blurred boundaries between malware for hire and MaaS.

This study considers stealers that come both with and without hosting, so long as the program satisfies other MaaS criteria. For example, Raccoon Stealer's operators provide hosting for affiliates, while RedLine's do not. Their remaining services differ less obviously, however both families are considered MaaS.

Operators that provide their own hosting have access to all data stolen by affiliates. While we know of no cases of stealer operators openly selling affiliate-collected data, it is possible some may use it surreptitiously.

Below are the steps taken by affiliates when purchasing an infostealer under the MaaS model.



Infostealers. Affiliate program scheme

After passing the interview, the affiliate gets access to the C2 panel and the build or builder, which can be part of the C2 panel. The build is encrypted, and the malware becomes ready for distribution. Build encryption can also be done directly from the C2 panel: operators often connect encryption services via API to automate the process.

Delivering the malware to the victim's device is the affiliate's responsibility. Phishing remains one of the most common methods of infection: attackers send emails with a malicious link or document in attachment. When the victim runs the malicious file, it establishes a connection to C2, and data is siphoned off. Stealers can implement multiple modules for data theft from various sources on the victim's device. Most stealers are capable of stealing the following information:

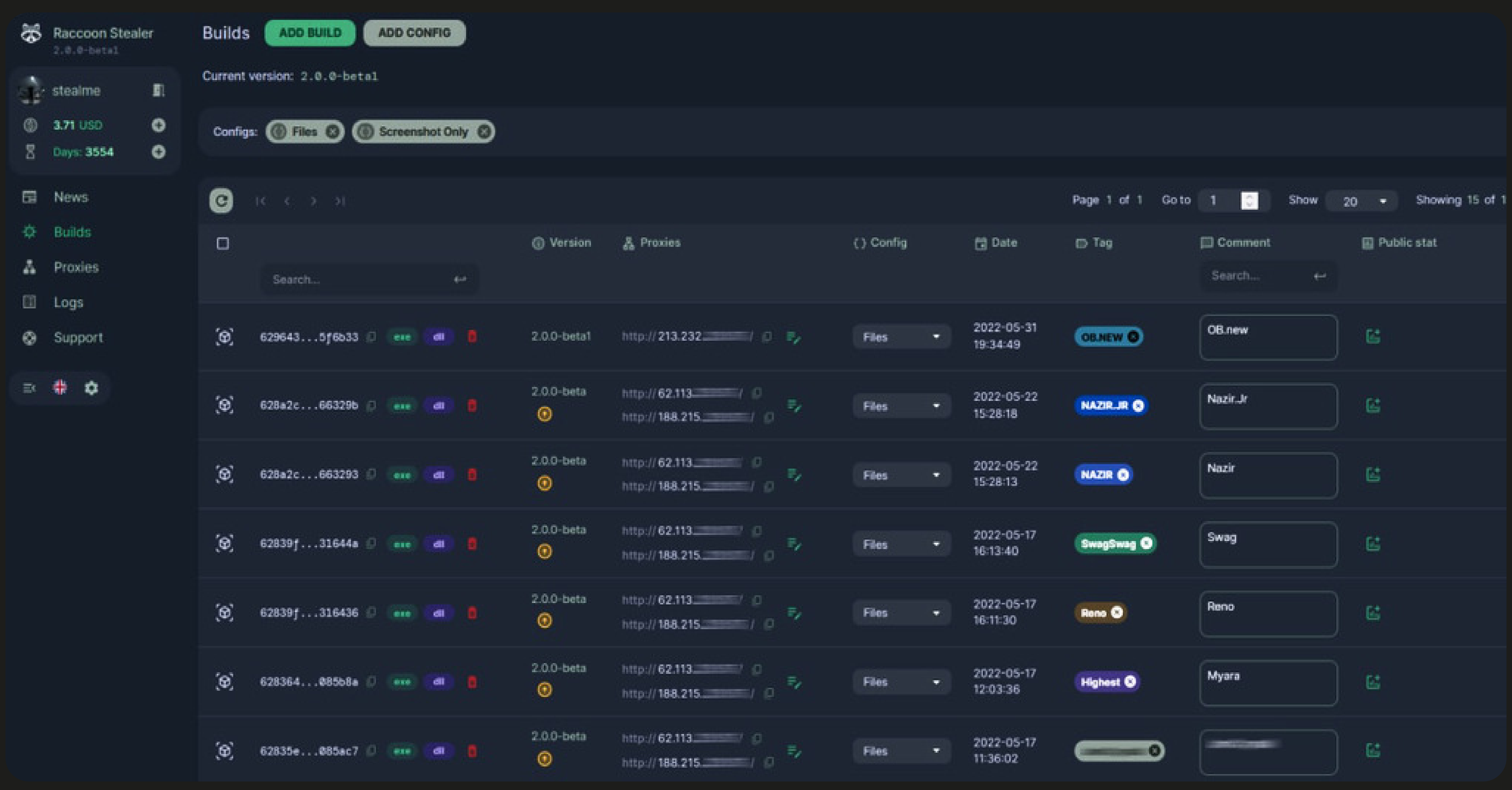
- cryptowallet data;
- credentials for FTP/VPN/email clients, messengers and various services, plus information stored in them;
- cookies, bank cards, saved passwords, browser histories;
- detailed data about the victim's device;
- screenshots, files with a specific path, name, or extension.

Stealers can also have a built-in clipper or loader modules. However, this type of malware lacks modules for lateral movement, so data is stolen only from the device that executed the stealer.

Clipper

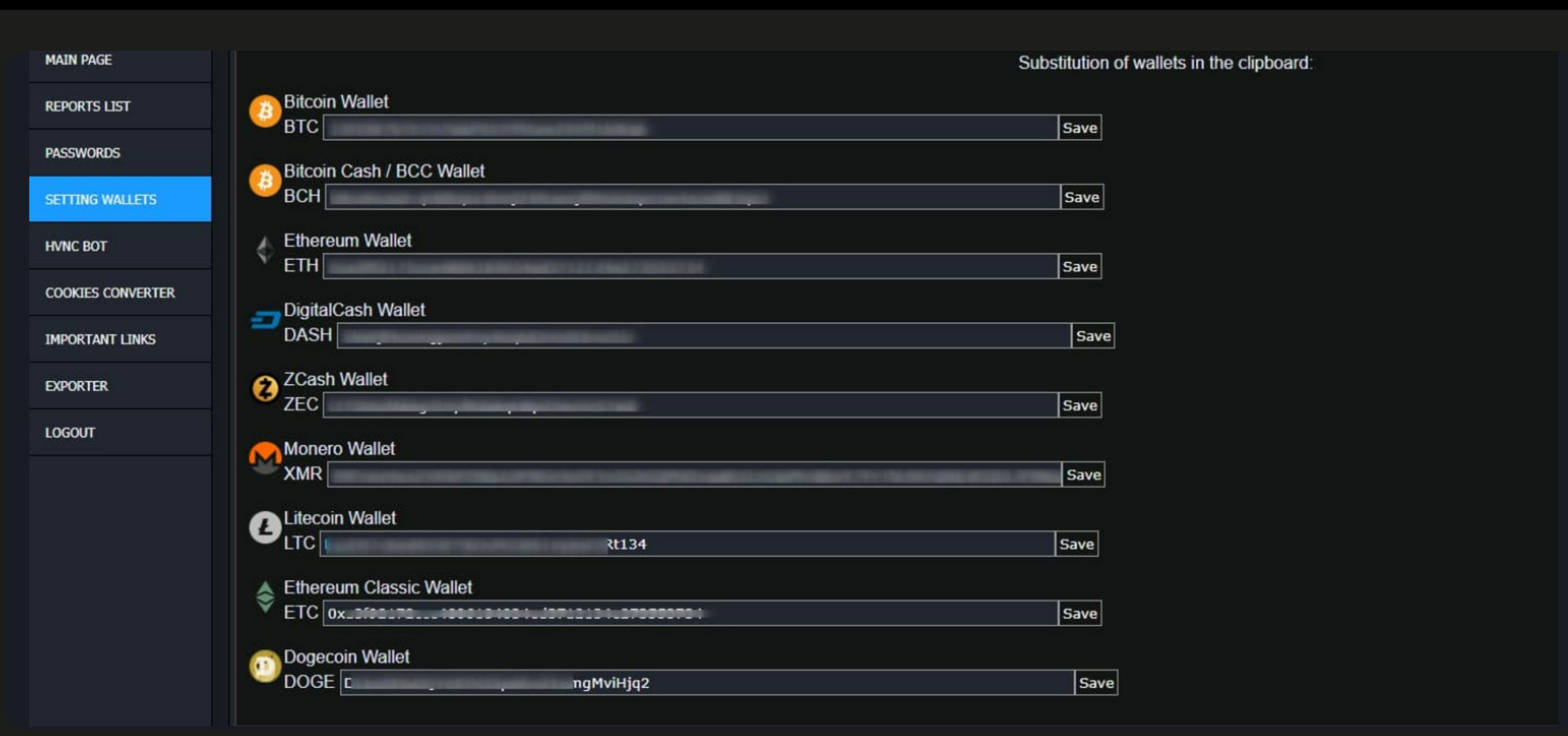
A piece of malware that checks the victim's clipboard for cryptowallet addresses and replaces them with the attacker's addresses.

Below are examples of the infostealer C2 panels and components. For example, the C2 panel in the first screenshot displays the subscription expiry date, plus there is the option to add a build and configuration to allow the attackers to identify their version of the malware, set parameters, and add tags. The C2 panel can also be used to dump stolen data and contact support.



C2 panel of Raccoon Stealer

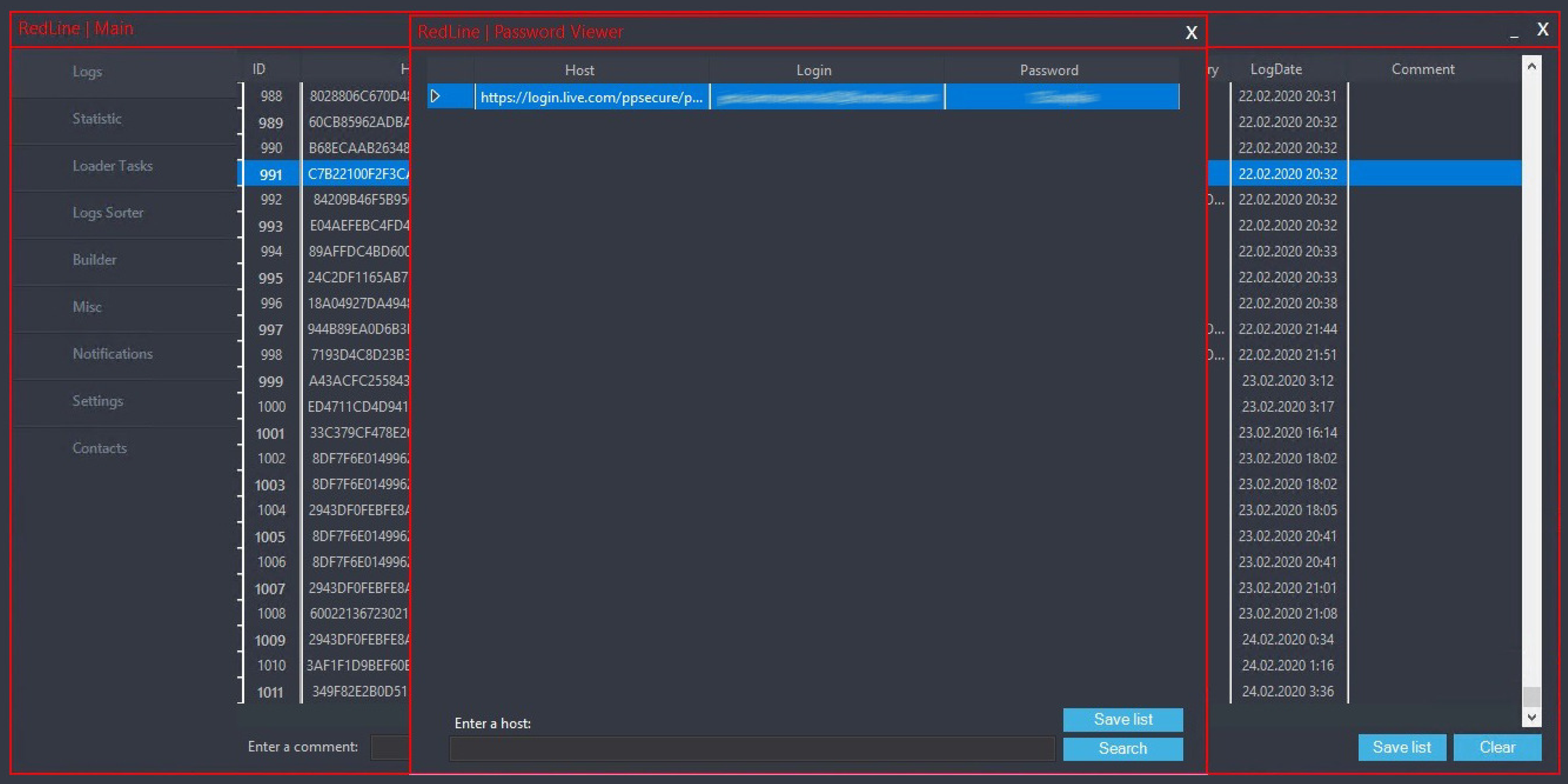
The second screenshot shows a clipper on the C2 panel of AZORult.



C2 panel of AZORult

The third example is the logs tab of the RedLine stealer. In it, you can see the victim's username and password, the URL of the site where the credentials were entered, and meta-information about the device: HWID, IP, OS, country, as well as date of data theft.

Through the C2 panel, logs can be cleaned and sorted; there are tabs with statistics, settings, and support contact details. In addition, the malware has a loader function that can also be controlled through the C2 panel.



C2 panel of RedLine

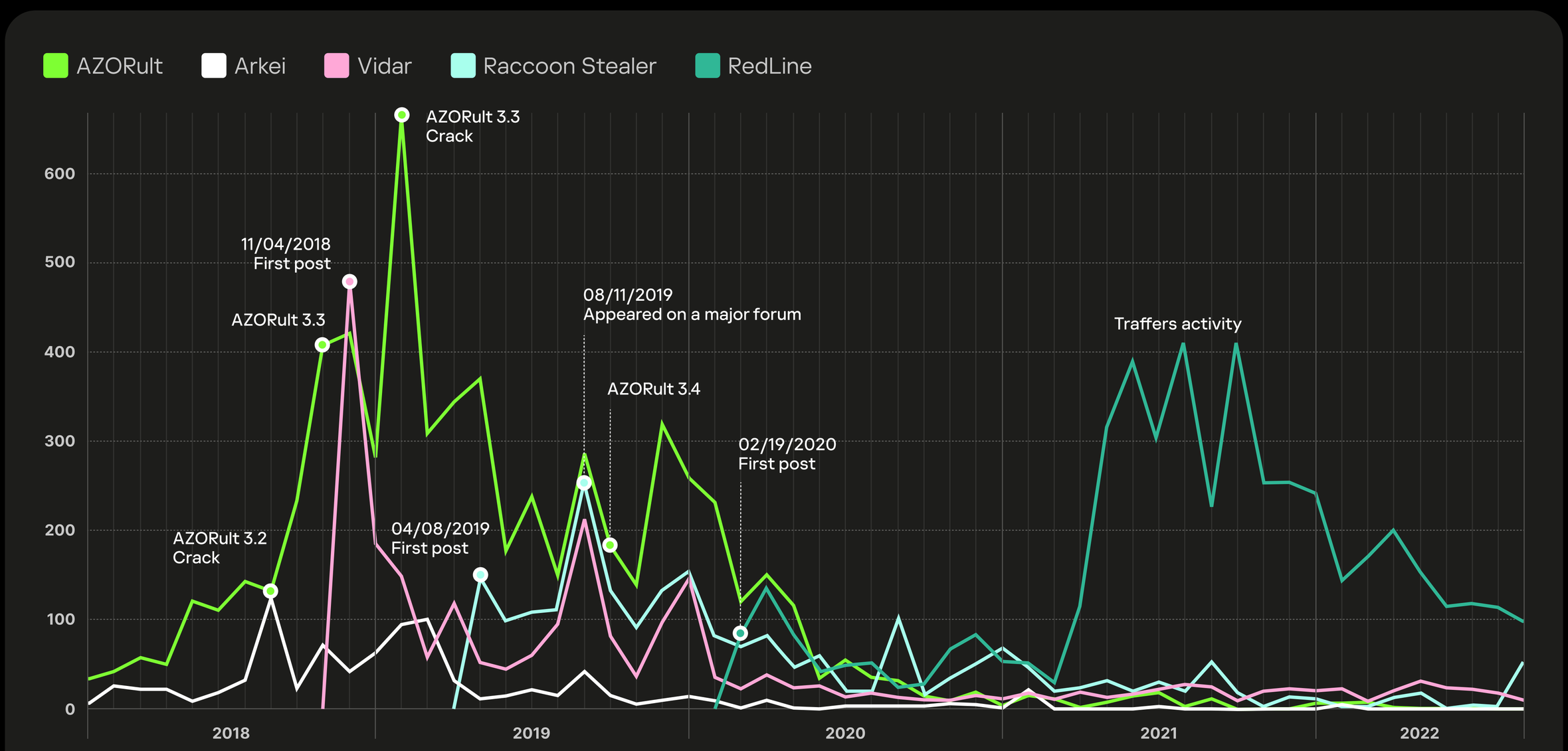
Affiliates can use the stolen data themselves or distribute it in dark web communities: sell it or publish it for free to bolster their reputation.

Ransomware often uses stealers, including those with a built-in loader, to steal accounts for performing lateral movement. For example, in January 2019, researchers at Malwarebytes identified a malicious campaign distributing the GandCrab ransomware together with the Vidar stealer.

Malware logs

Are compromised credentials collected in files. Combining mass data into one file can be done by various parameters, such as date of collection or region of victims.

Evolution of infostealers



Number of mentions of five families of infostealers distributed under the MaaS model in dark web and deep web communities, January 2018 – August 2022

We analyzed the evolution of the five most common infostealer families distributed under the MaaS model, based on mentions in dark web communities.

The most frequently mentioned infostealer on dark web forums is AZORult. After the source code of its C2 panel and builder were leaked, the AZORult 3.2 crack appeared in August 2018. CrydBrox, the malware's creator, released the updated 3.3 version to compensate for the leak of the previous version, but stopped selling this malware in late 2018, posting the message:

> ...
>
> All software has a shelf life. It's run out for AZORult. It's with sadness and joy that I announce that sales are closed forever.
>
> CrydBrox

As a result, the task of modifying and distributing AZORult fell to other attackers. Version 3.3 was also hacked eventually, and so, in September 2019, AZORult 3.4 was born. This is not the only case of code reuse among cybercriminals. During our analysis of various infostealer families, we found a lot of instances of borrowing.

In particular, Vidar used the same structure of data sent to C2 as Arkei. There are other similarities between the two families, too.

ARKEI

```
POST /index.php HTTP/1.1
Accept: text/html, application/xml;q=0.9, application/xhtml+xml,
image/png, image/jpeg, image/gif, image/x-xbitmap, */*;q=0.1
Accept-Language: ru-RU,ru;q=0.9,en;q=0.8
Accept-Charset: iso-8859-1, utf-8, utf-16, *;q=0.1
Accept-Encoding: deflate, gzip, x-gzip, identity, *;q=0
Content-Type: multipart/form-data; boundary=1BEF0A57BE110FD467A
Content-Length: 80295
Host: ****IP address****
Connection: Keep-Alive
Cache-Control: no-cache

--1BEF0A57BE110FD467A
Content-Disposition: form-data; name="hwid"

--1BEF0A57BE110FD467A
Content-Disposition: form-data; name="os"

Windows 7 Ultimate
--1BEF0A57BE110FD467A
Content-Disposition: form-data; name="platform"

x86
--1BEF0A57BE110FD467A
Content-Disposition: form-data; name="profile"

1
--1BEF0A57BE110FD467A
Content-Disposition: form-data; name="user"

--1BEF0A57BE110FD467A
Content-Disposition: form-data; name="pcount"
```

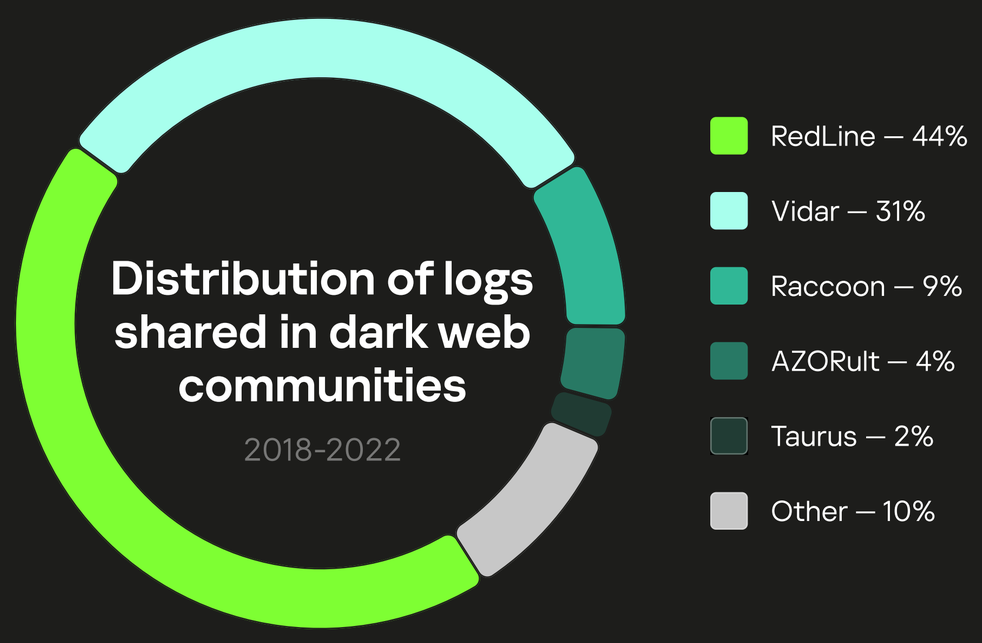
VIDAR

```
POST / HTTP/1.1
Accept: text/html, application/xml;q=0.9, application/xhtml+xml,
image/png, image/jpeg, image/gif, image/x-xbitmap, */*;q=0.1
Accept-Language: ru-RU,ru;q=0.9,en;q=0.8
Accept-Charset: iso-8859-1, utf-8, utf-16, *;q=0.1
Accept-Encoding: deflate, gzip, x-gzip, identity, *;q=0
Content-Type: multipart/form-data; boundary=1BEF0A57BE110FD467A
Content-Length: 36849
Host: ****Domain****
Connection: Keep-Alive
Cache-Control: no-cache

--1BEF0A57BE110FD467A
Content-Disposition: form-data; name="hwid"

--1BEF0A57BE110FD467A
Content-Disposition: form-data; name="os"

Windows 7 Home Premium
--1BEF0A57BE110FD467A
Content-Disposition: form-data; name="platform"

x86
--1BEF0A57BE110FD467A
Content-Disposition: form-data; name="profile"

251
--1BEF0A57BE110FD467A
Content-Disposition: form-data; name="user"

--1BEF0A57BE110FD467A
Content-Disposition: form-data; name="cccount"
```

Structure of data sent to C2: Arkei and Vidar

Many mentions of infostealers are about the distribution of logs in dark web communities. The number of logs runs into the hundreds of millions. Cybercriminals often use accounts from logs for initial access to the target company's infrastructure. On the right is a rough percentage breakdown of logs into major stealer families. "Other" covers all remaining families, including those not distributed under the MaaS model.

Most of the logs from stealers (>90%) in dark web communities belong to families distributed under the MaaS model. Of these, RedLine (44%) and Vidar (31%) logs are the most common.



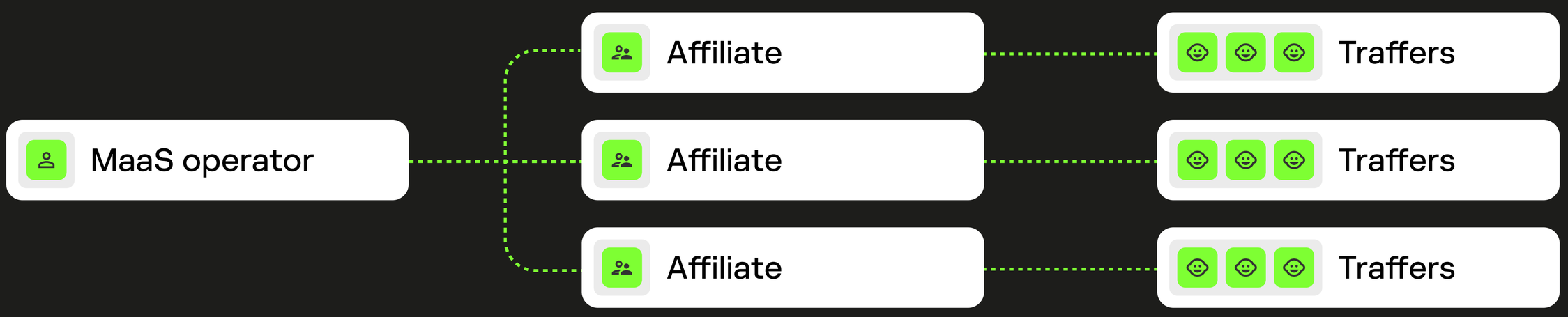
Traffers

As already mentioned, most cybercriminals want to get as much money as possible. This applies to both malware operators and affiliates alike. To increase their profits, they can bring in additional resources to distribute malware more effectively – traffers. Note that traffer services are mainly used by affiliates of infostealers.

Traffers (workers)

Are teams of cybercriminals who distribute malware to make a profit (interest, bonuses, other payments from affiliates). Traffers do not have access to C2 panels, logs, or builders. They scale up the spread of the malware, and all logs they collect go to the affiliate's C2 panel.

Hierarchy of malefactors



Traffer teams in dark web communities are usually made up of people unable to purchase malware themselves or provide their own bulletproof hosting, which malware operators do not always supply. Recruitment posts by affiliates detail the structure and requirements for traffers, which are similar to those of operators for affiliates. For example, the requirement not to upload builds to VirusTotal is found in almost all ads.

On the right is a screenshot of an add to join a traffer team.

Example of an ad to join a team

...

1. WE DON'T TAKE REQUESTS
2. NEAR INSTANT FREE UPLOAD AND SEO
3. BONUS FOR EVERY 100 LOGS
4. REDLINE/RACCOON
5. AUTO-PROCESSING OF GAME LOGS IN BOT
6. YOUTUBE AUTOCHECKER
7. RESPONSIVE SUPPORT
8. FUD CRYPT (EASY/MELON)
9. YOUR 70% FROM CRYPTOWALLETS
10. FREE RELINK FOR TOP TRAFFERS
11. REGULAR GIVEAWAYS
12. SPECIAL CONDITIONS FOR TOP TRAFFERS

View the screenshot of the post ›

Explanation of conditions of an ad to join a team

We don’t take requests

Requests are accounts for certain services that affiliates often take from traffers.

Near instant free upload and SEO

This is about uploading a YouTube video with a link to a stealer and promoting it.

Free relink for tops

The cybercriminals relink YouTube accounts. Most often, account login uses freshly stolen YouTube cookies. This service is free for top traffers who steal the most data.

Regular giveaways

Periodic cash giveaways for top traffers from clipper profits.

Auto-processing of game logs in bot

Stolen data from the stealer’s C2 panel is automatically passed to a Telegram bot, which sends it to team members or third-party services that change the passwords for hijacked gaming accounts.

FUD crypt (Easy/Melon)

Fully undetectable (FUD) means the build is encrypted to evade detection by security solutions using static analysis. The encryption is done using EasyCrypt or MelonCrypt.

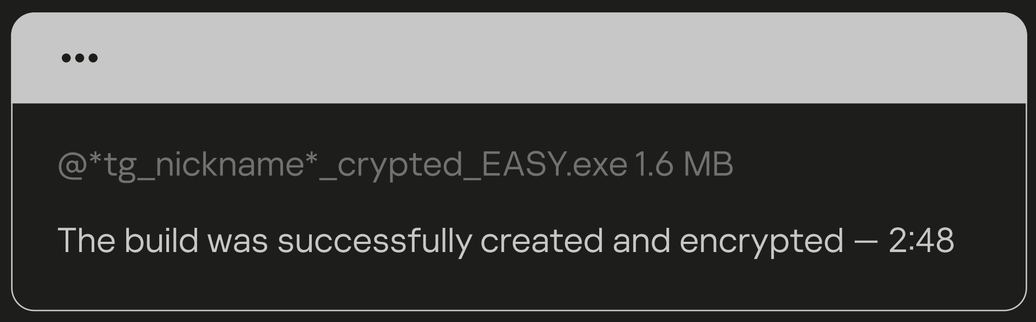
YouTube autochecker

Using a script, the attackers collect information about the channel linked to the stolen YouTube account: number of subscribers/views, date of creation, etc.; the harvested data helps to determine which channels will be better for spreading the stealer.

Traffers and affiliates typically communicate via Telegram. The affiliate sets up channels and bots for these purposes. Then, having access to the builder, they create samples of the malware, encrypt them, and send them to traffers through one of these bots or channels.

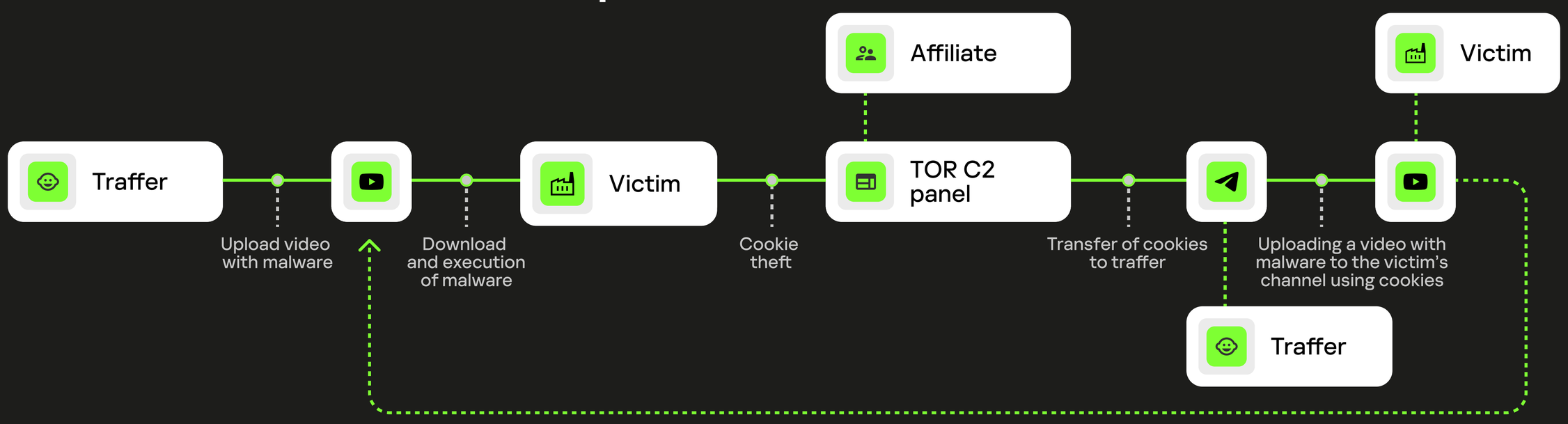
Most often, traffers distribute malware under the guise of cracks and instructions for hacking legitimate programs on YouTube. To post videos, attackers like to steal fresh cookies from YouTube channels using a stealer and use them to upload videos to these channels supposedly about how to hack a particular program, with a malware download link in the description.

Example of a bot issuing a malware sample encrypted using EasyCrypt



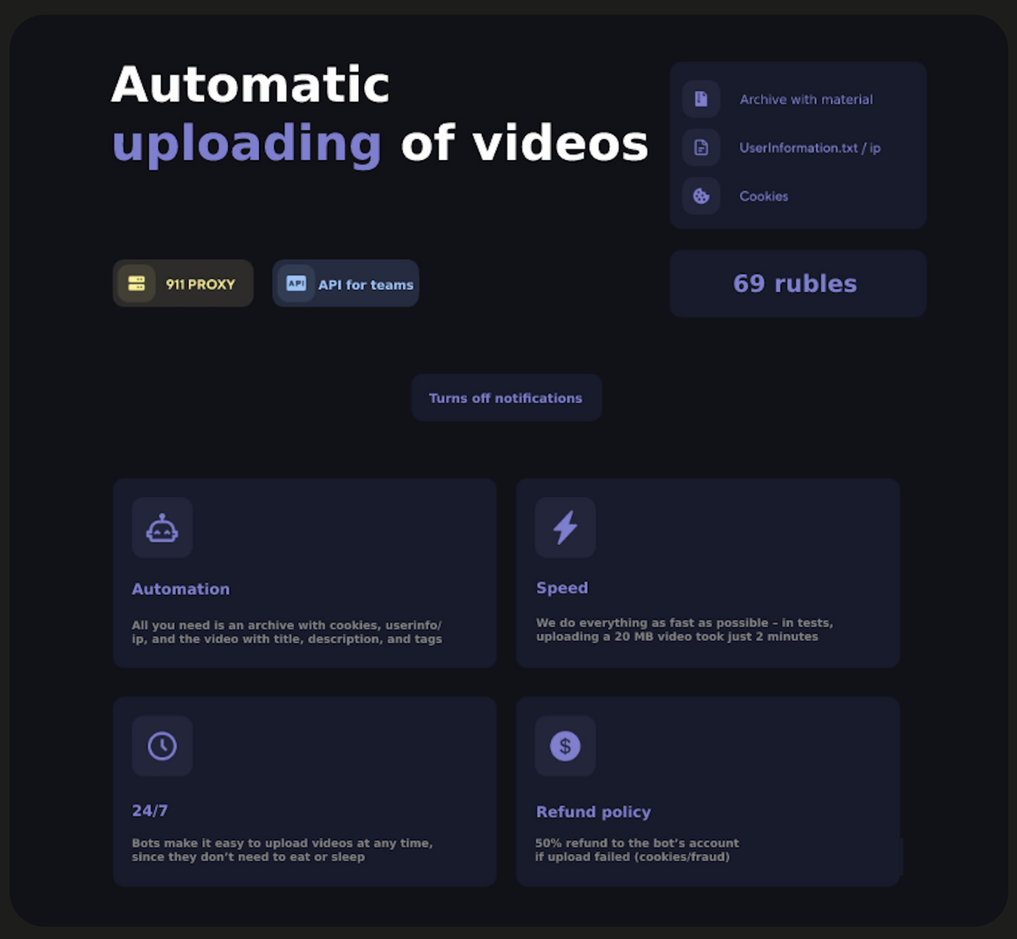
View the screenshot of the message ›

A scheme of how traffers operate



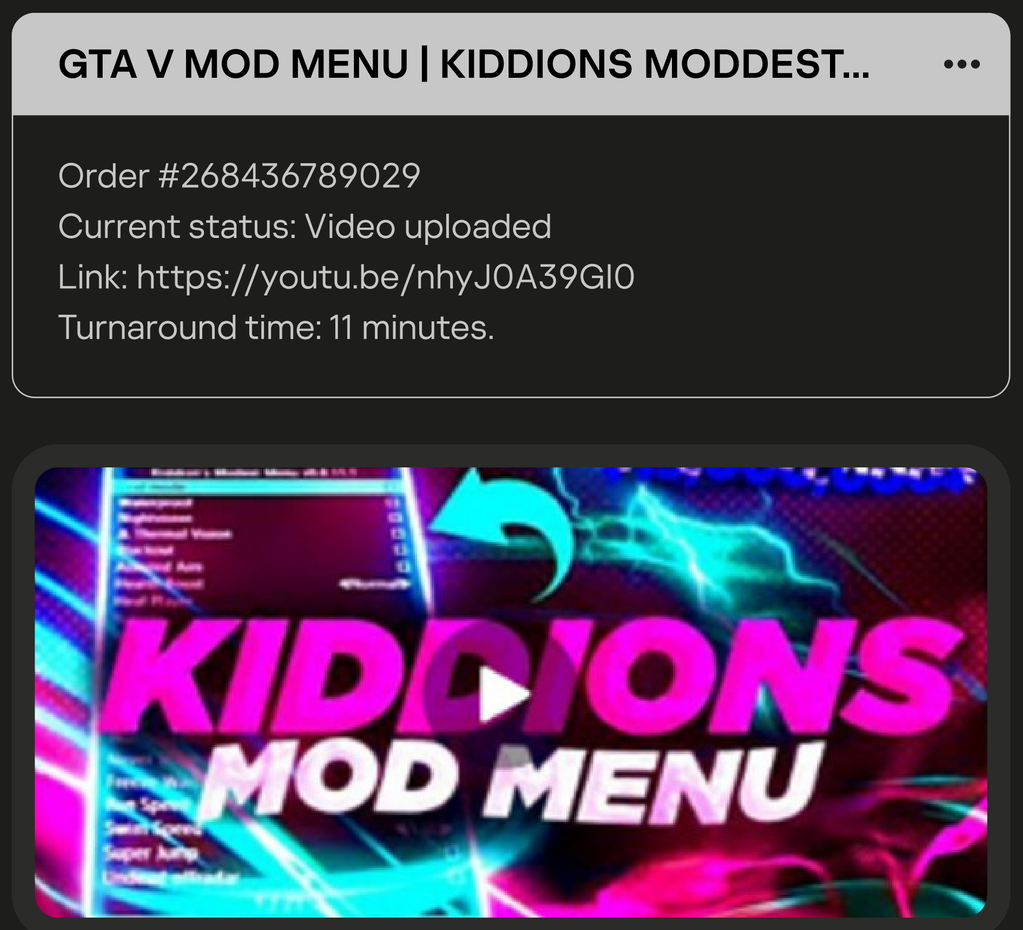
To automate the uploading of videos through YouTube cookies, there are services that traffer teams use.

Example of a service for auto-uploading videos on YouTube



View the original screenshot of the post ›

Example of a bot notification in Telegram that attackers receive when using an auto-upload service



View the screenshot of the message ›

kaspersky

Digital Footprint Intelligence

The service uploads the video and sends a notification with a link to it to a messenger, such as Discord or Telegram. The video upload procedure is usually like that described in our post about a self-spreading stealer. The structure of traffer-uploaded videos is identical, so it is not possible to determine which stealer is being distributed by looking at the video's description, cover image, or title. It is likely that the traffers are using some kind of unified instruction for posting videos with a link to the stealer.

Attackers post lots of videos with malware download links every day, but Google (which owns YouTube) is aware of the issue and acts quickly to detect and remove such videos.

More often than not, the description of such videos contains a link to download the stealer in the form of a password-protected archive. The password prevents the browser's antivirus engine from scanning the content.

In this case, the stealer sample is written in .NET, which allows us to analyze it using the dnSpy debugger.

Example of a video used to spread an infostealer

FORTNITE HACK FREE DOWNLOAD...

DOWNLOAD LINK: https://www.mediafire.com/file/w33pn9...
Password:123
INSTRUCTIONS:

1. Download the hack;
2. Unzip the file to any folder/desktop;
3. Open Umbrella Hack.exe file;
4. Run Fortnite;
5. Press the inject button;
6. The hack should appear when you press the shortcut.

View the screenshot of the publication ›

Downloading an archive from the video

As mentioned earlier, communication between traffers and affiliates takes place in Telegram. Some affiliates implement the traffer's Telegram nickname into the build configuration module, and use it as an identifier for sending logs via the messenger.

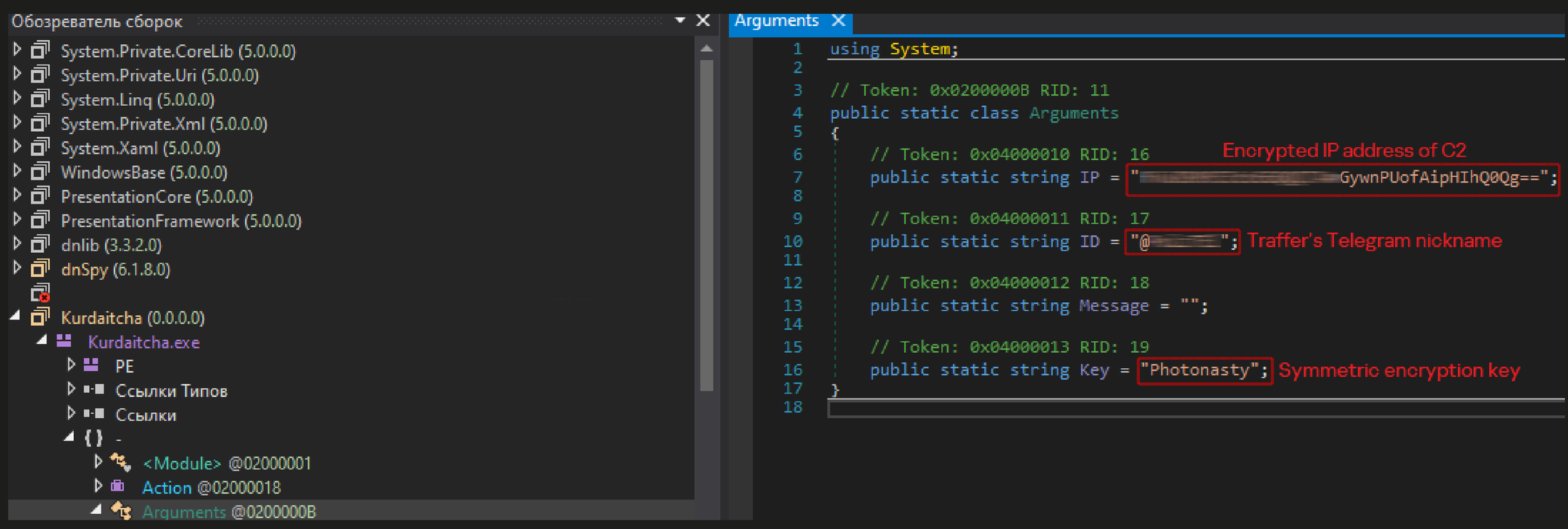
Example of archive contents

Fortnite Umbrella Hack (Aim+Wh).rar - RAR archive, unpacked size 12 464 686 bytes

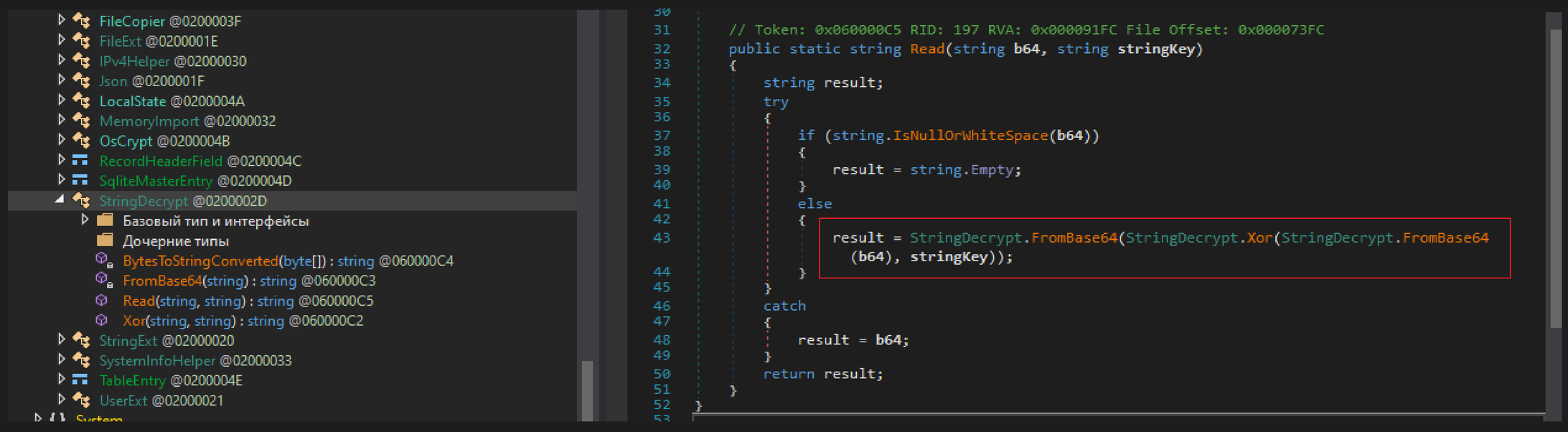
Name	Size	Packed	Type	Modified	CRC32
..			Папка с файлами		
config	94 432	43 472	Папка с файлами	15.02.2022 16:33	
data	208 378	21 360	Папка с файлами	03.02.2022 14:53	
config.ini *	970 912	396 736	Параметры конф...	08.09.2020 18:49	AE33CA0B
injector.dll *	6 831 616	2 506 944	Расширение при...	04.08.2021 20:14	86B9F7AB
main.dll *	1 610 096	466 288	Расширение при...	08.09.2020 18:52	F40FCDD9
Umbrella Hack.exe *	2 749 252	651 184	Приложение	06.10.2022 0:03	3F9E880A

The screenshots below are an example of parsing the file Umbrella Hack.exe. The Arguments module contains the configuration data of the build: C2 IP address; traffer's Telegram nickname as the build ID; encryption key used to encrypt the IP string.

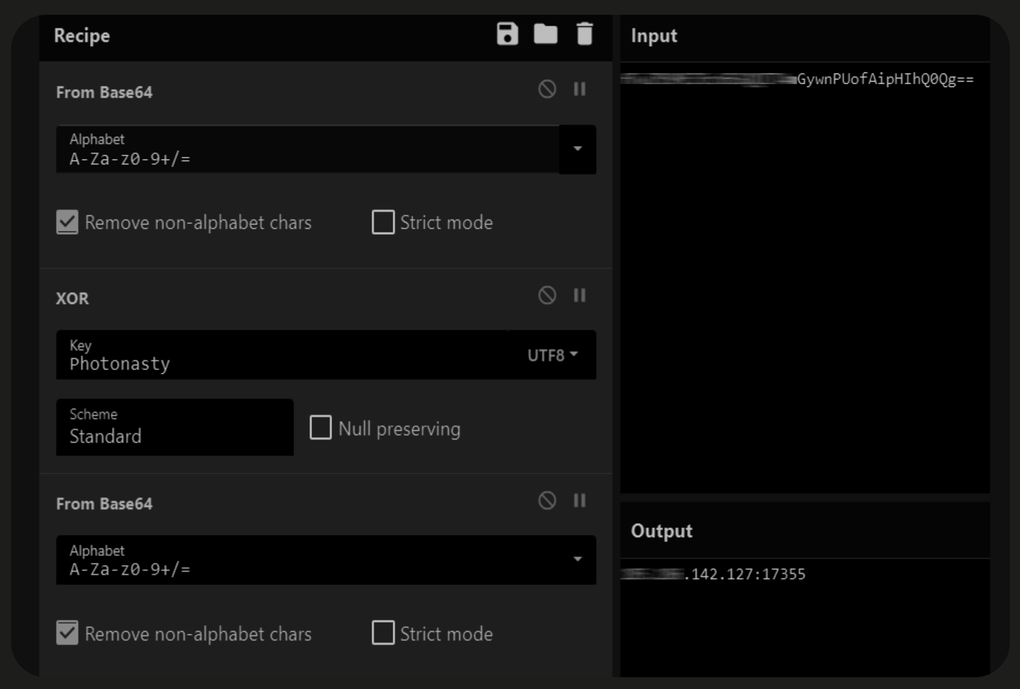
In the StringDecrypt module, you can see the string decryption algorithm. It uses the following encoding sequence: base64, then XOR with the symmetric key displayed on the picture above, and then base64 again. The IP string specified in the Arguments module can be decrypted with CyberChef.



Arguments module of the infostealer



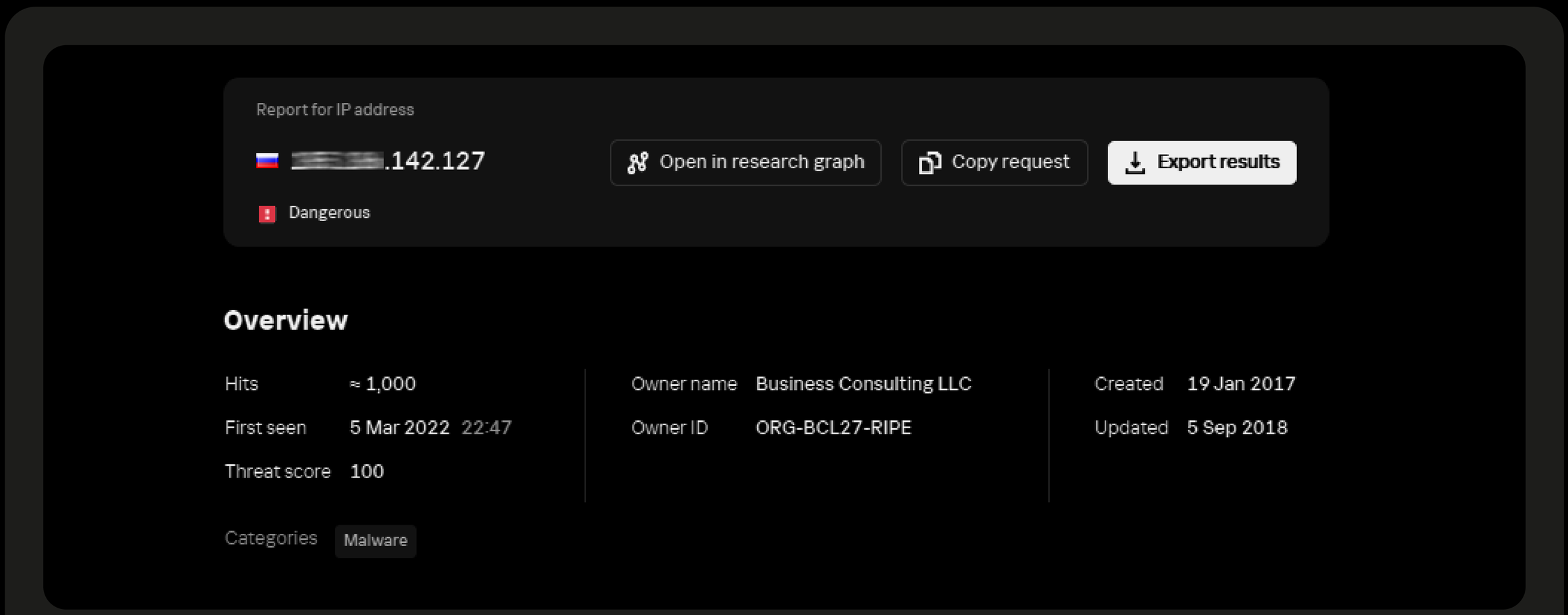
StringDecrypt module of the infostealer



Decryption of C2 IP address from the build using CyberChef

As the output we get the IP address and the port used as C2. The Threat Intelligence Portal shows the number of communications (~1000) with the given IP address throughout the entire monitoring period.

Note that this IP has the maximum Threat Score, which indicates the probability that the address is malicious.



Information about C2 on Kaspersky Threat Intelligence Portal

Below is information from VirusTotal about files that communicate with this IP address.

It is obvious from the filenames that the malicious samples are disguised as legitimate programs or as cracks for them.

Most of the communicating files are detected as infostealers, and in many of them various vendors have clearly marked their verdict: RedLine Stealer.

Information about C2 from VirusTotal

https://www.virustotal.com/gui/ip-address/relations

Scanned	Detections	Type	Name
09/12/2022	30 / 71	Win32 EXE	JailBreak Ios 15.exe
05/09/2022	28 / 69	Win32 EXE	Spotify 1.1.80.699.exe
05/24/2022	21 / 68	Win32 EXE	Windscribe (1).exe
05/13/2022	29 / 69	Win32 EXE	Synapse x.exe
05/06/2022	13 / 67	Win32 EXE	ExpressVPN_setup.exe

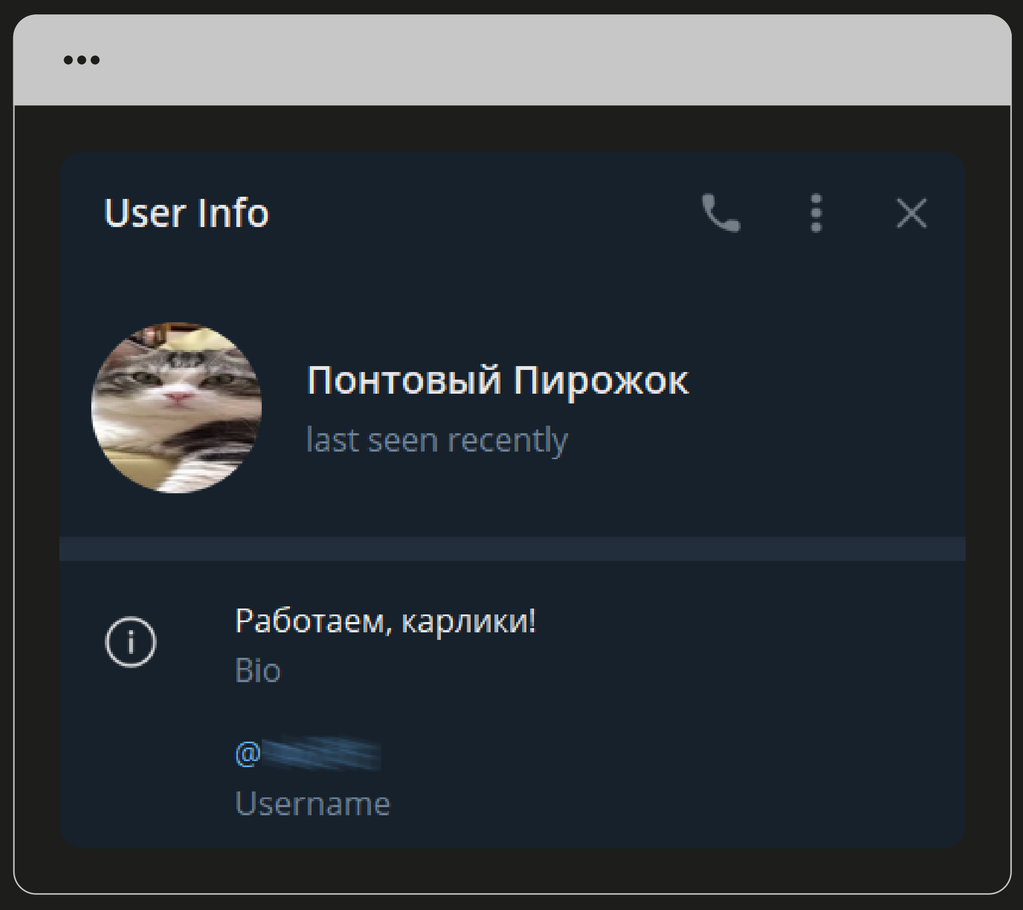
View the screenshot ›

With the traffer's Telegram nickname, which is specified in the Arguments module as an open ID, it is also possible to find their profile on a dark web forum. An affiliate who uses this ID thus, in effect, deanonymizes the traffer.

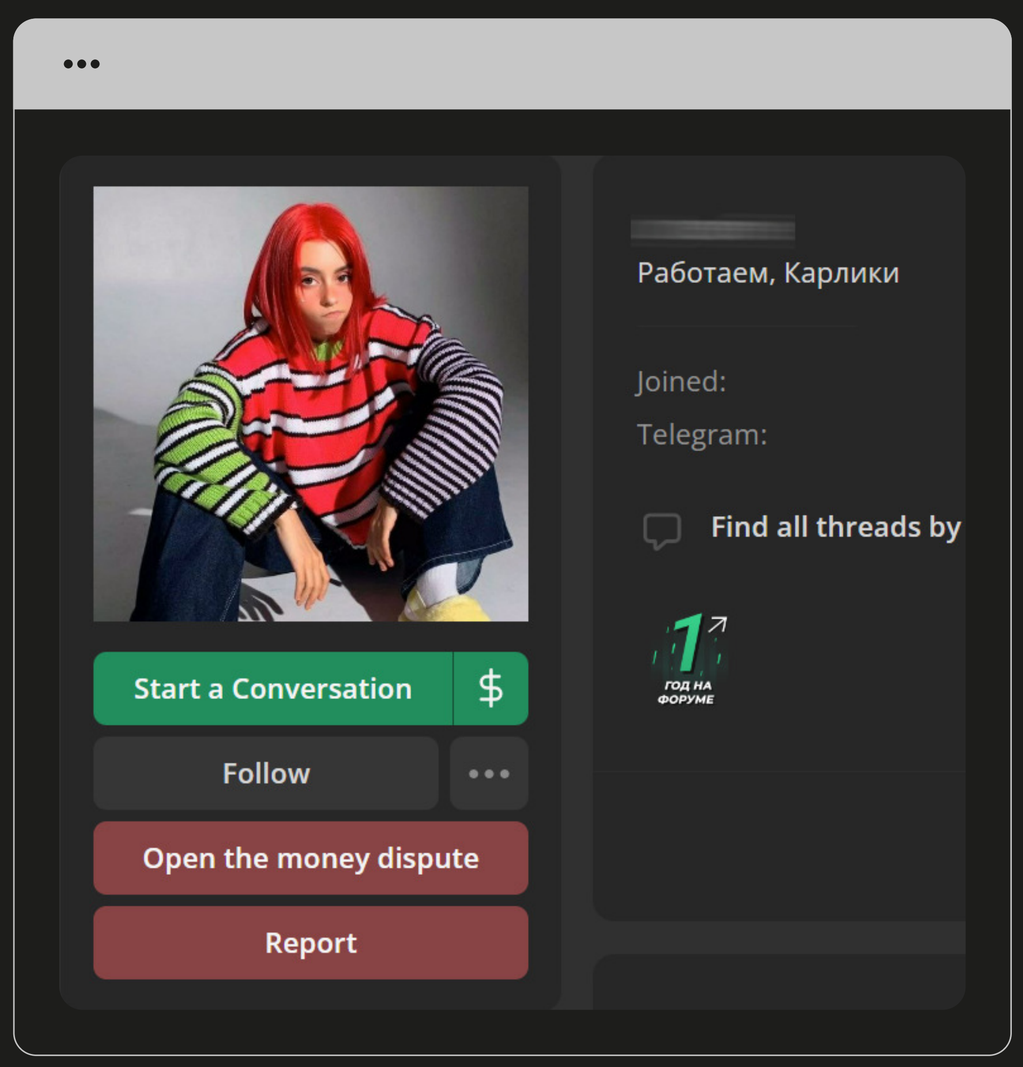
The number of traffers working under an affiliate can reach into the hundreds. Affiliates have access to all the logs they collect. Although traffers can join the team for free, the affiliate can take "requests" (accounts for certain services), as well as a percentage of the stolen cryptocurrency.

Traffers' profits depend on how honest the affiliate is. Since only the latter has access to the C2 panel, they could easily defraud the distributor of the stealer, who will be unable to prove they were cheated. In turn, the affiliate might get conned by the malware operator, who provides hosting for them. The operator has access to all the stolen data and can use it for personal gain.

Pontoviy Pirozhok's Telegram account from the build



Profile of a build distributor on a forum



Conclusion

Malware-as-a-Service is an ever-evolving business model that brings cybercriminals a steady profit. They use this profit to maintain a team and constantly update their malware. This is leading to improvements in MaaS services, but there is also a trend towards standardization. This allows us to conclude that affiliate programs will eventually become more generic and more predictable, which, in turn, should cause a drop in the number of new malware families being distributed under this model.

Given that ransomware accounts for 58% of all families found since 2015, we can further conclude that RaaS is the most in-demand and actively developing area of MaaS. But the popularity of ransomware should not allow other categories of malware to go unnoticed. Attackers collaborate with each other, borrowing or reusing malicious code, and use every conceivable tool, including stealers, botnets, loaders, and backdoors, to achieve their goals.

The level of information protection in your company must be commensurate with the scale of its internal processes; if it is, when faced with an attack, you won't have to try your luck and find out whose business model is more resilient – yours or Malware-as-a-Service's.

To prevent compromise and infection, companies with any level of information security maturity should:

1. Regularly update software used both on the external perimeter and in the internal infrastructure. Take inventory of services and applications on the external perimeter, paying special attention to the protection of remote-access interfaces.
2. Raise employee awareness of information security. Hold training sessions on phishing and social engineering threats.
3. Protect corporate devices with EDR (Endpoint Detection and Response) systems.
4. Leverage Threat Intelligence data to get strategic actionable insights to respond to advanced threats. An understanding of the tools as well as typical tactics and techniques of cybercriminals will ensure maximum protection when combining automated security tools with the expertise of infosec professionals.

To inquire about threat monitoring services for your organization, please contact us at

dfi@kaspersky.com

Thanks to our colleagues at BI.ZONE for reading and commenting on the material.