Evolving Info-Stealers: RedLine, Raccoon & New Threats

Published: 2022-07-13 · Archived: 2026-04-05 16:28:24 UTC

The Next Generation of Info Stealers

KELA

By KELA Cyber Team

Edited by Ben Kapon

Published July 13, 2022

In recent years, information-stealing Trojans have become a very popular attack vector. This type of malware is used for harvesting saved information on machines including usernames and passwords (“logs”) which are further sold on automated botnet marketplaces such as RussianMarket, TwoEasy, and Genesis, or privately. If purchased by threat actors, these credentials pose a significant risk to an organization, as they allow actors to access various resources which may result in data exfiltration, lateral movement, and malware deployment, such as ransomware.

Some of the most popular info-stealers advertised on cybercrime forums and identified on these marketplaces are RedLine, Raccoon, and Vidar. While some of these commodity stealers remain relevant, KELA observed that the threat landscape started to change under various conditions. The Russia-Ukraine war, the info-stealer operators’

need to improve malware capabilities, and their financial motivation, resulted in new stealers and services becoming available.

This report focuses on the currently active information stealers, highlighting the evolution of the old stealers, as well as the debut of new ones.

Diversification of Stealers

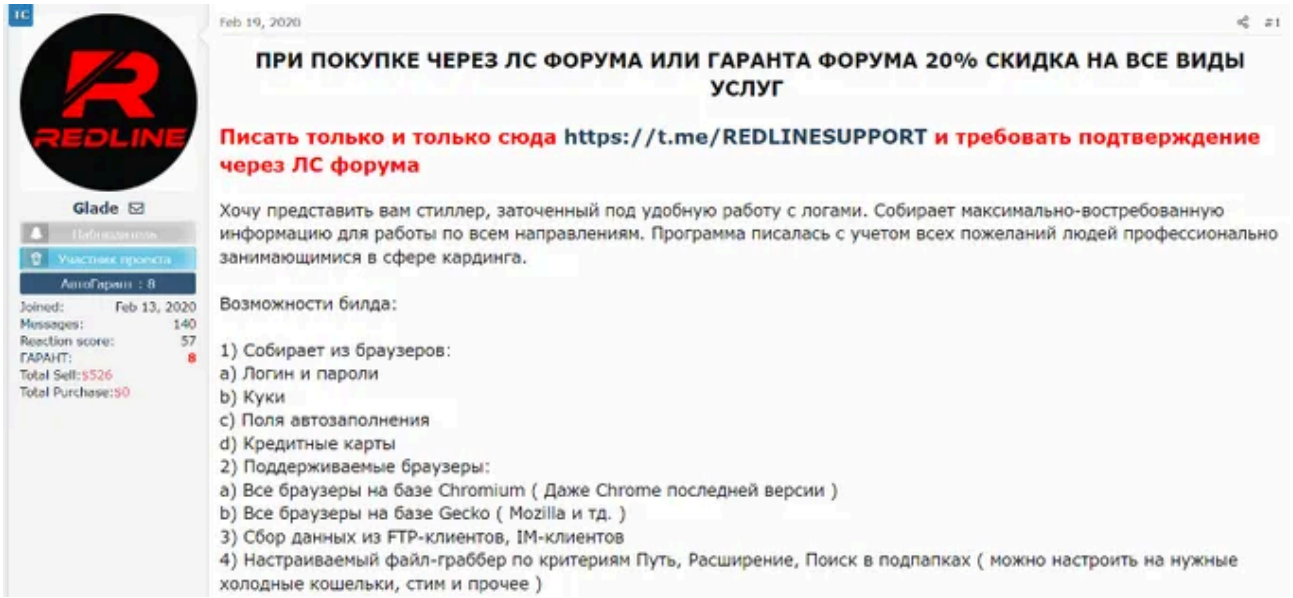
Changes in the threat landscape, as listed above, have determined a more evident diversification of stealers. While some of the well-known commodity information stealers continue to stay relevant for threat actors and be observed in malicious campaigns, other options, such as private stealers, have also become available. Commodity information stealers refers to malware and tools that are widely available for purchase on cybercrime forums and markets, thus used by a wide range of threat actors. Private information stealers, on the other hand, refers to customized malware that is not made available to all threat actors, mostly to avoid being widely spread and losing the capability to remain undetected by security tools.

In this chapter, KELA highlights both the journey of commodity stealers and how they evolved and changed over time, and the newly advertised private stealers.

The Journey of Commodity Stealers RedLine Stealer

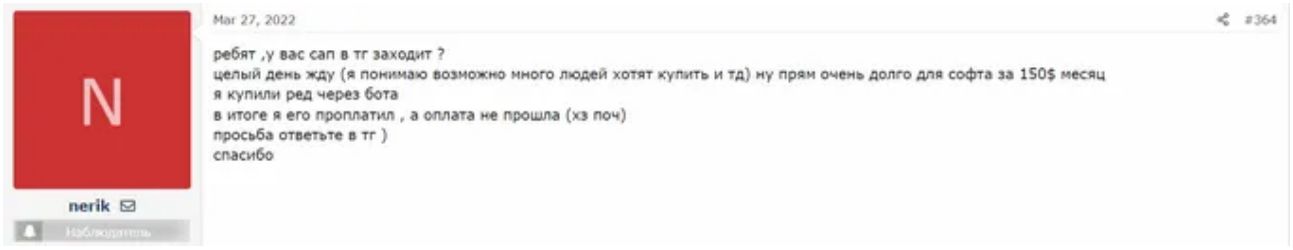
RedLine has been advertised and sold on various cybercrime forums since early 2020. For instance, threat actor Glade aka REDGlade, potentially one of the RedLine developers, first announced the stealer in February 2020 on the WWH Club and BHF forums and the Telegram channel. The RedLine stealer is still being sold for USD150 per month or for USD800 for the “pro” unlimited version.

The information-stealing malware seems to maintain its popularity among threat actors, a fact confirmed by the number of infected machines listed on marketplaces. For instance, the TwoEasy marketplace currently has around 575,000 bots available for sale, out of which over 55% are machines infected with RedLine. When compared with KELA’s analysis on December 21, 2021, this seems to be a continuing trend for the info-stealer.



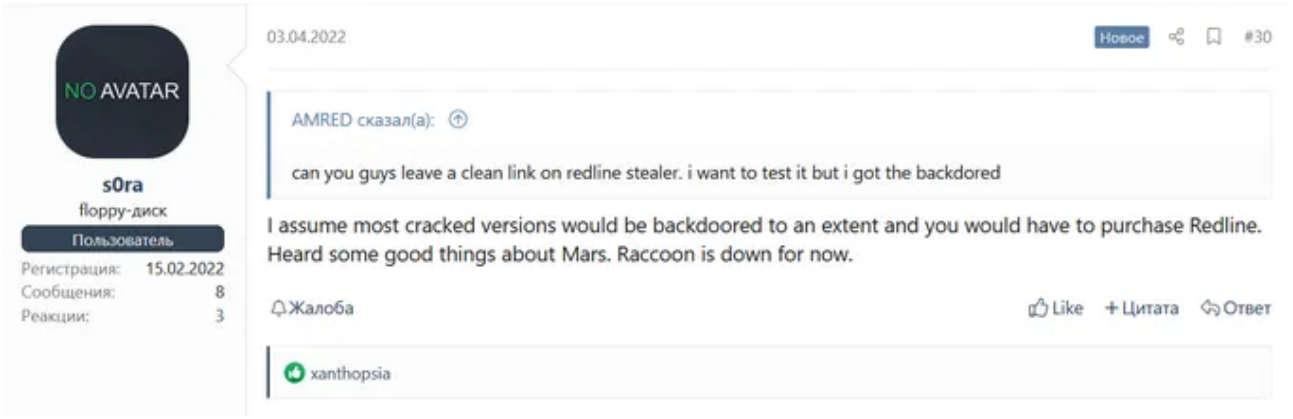
User Glade introduces RedLine Stealer. Source: WWH Club

As more and more users are anxiously looking to acquire the RedLine software, complaints have been recorded regarding the delays in the support chat.

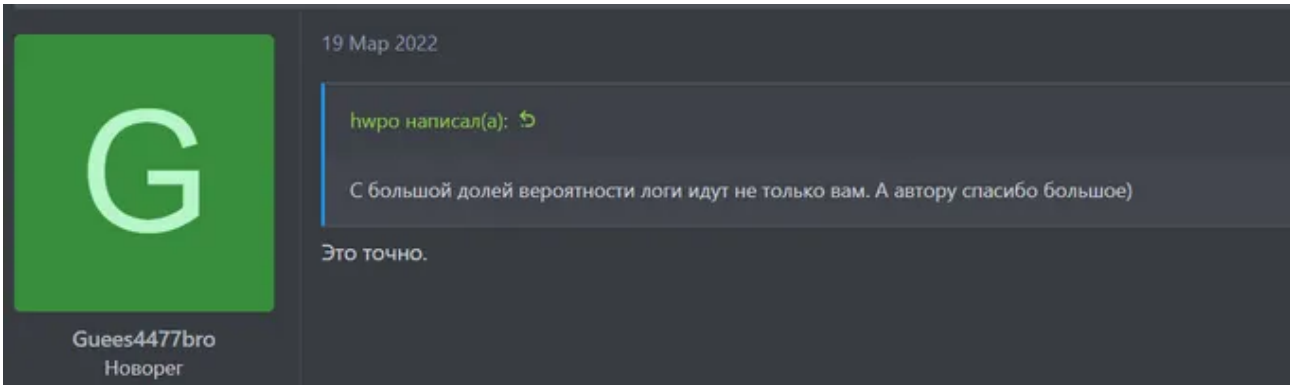


User complaining about delays. Source: WWH Club

A common tactic observed among users is to try the “cracked” free versions for testing purposes, to avoid purchasing the software, however, with less successful outcomes.

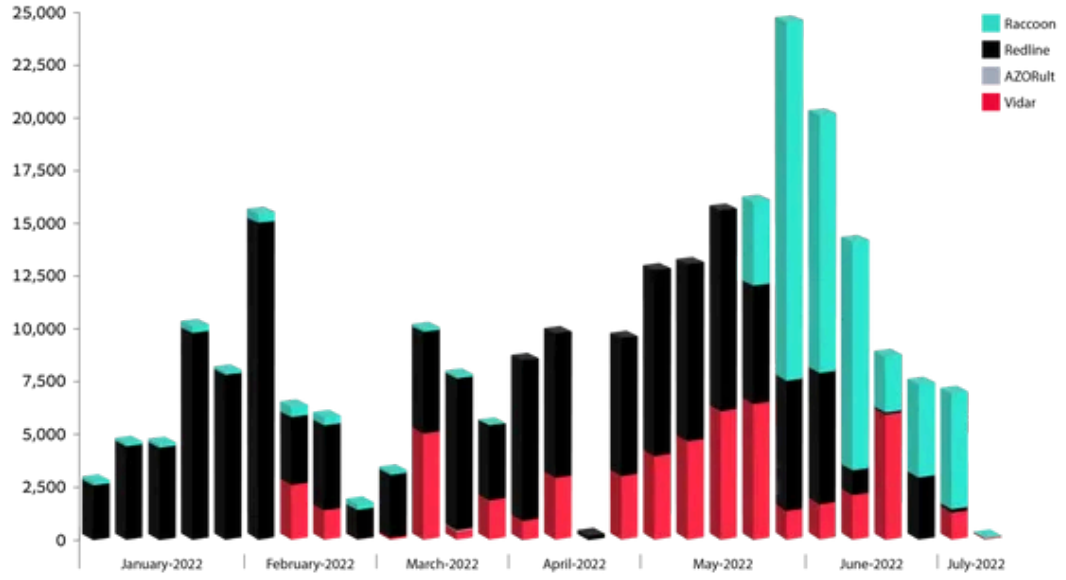


Source: XSS



User claiming that the logs obtained with the “cracked” version are also sent to others. Source: BHF

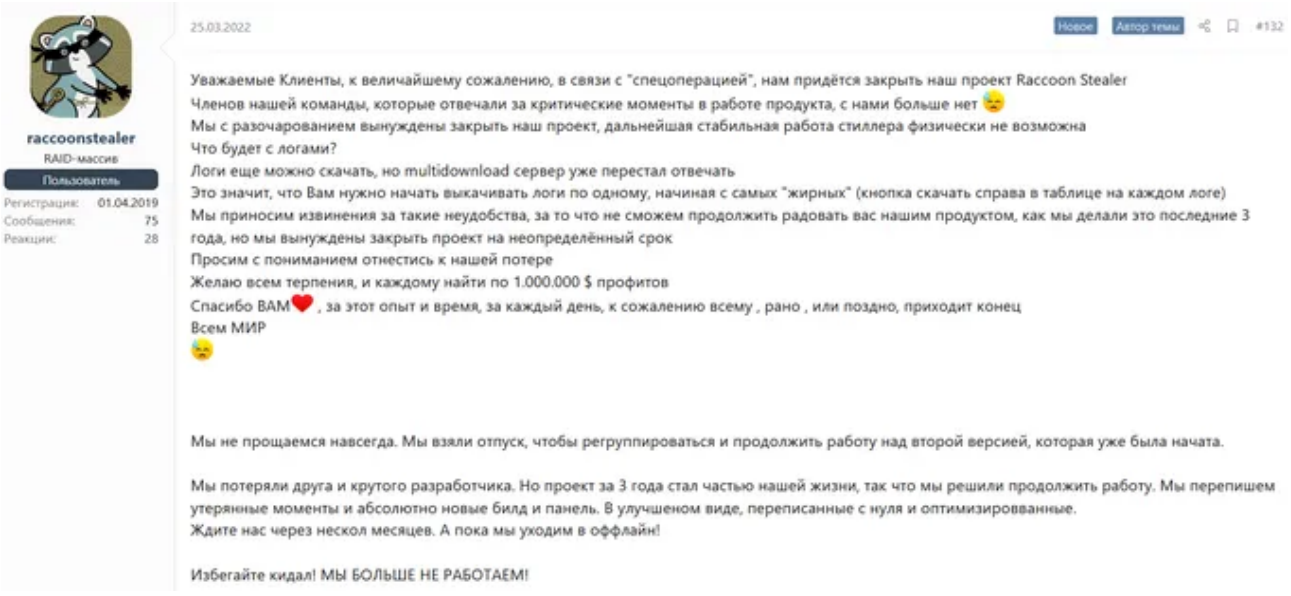
While RedLine still remains relevant, it is evident that the information stealer is not fulfilling the expectations of all users, therefore some of them choose to look for alternatives.

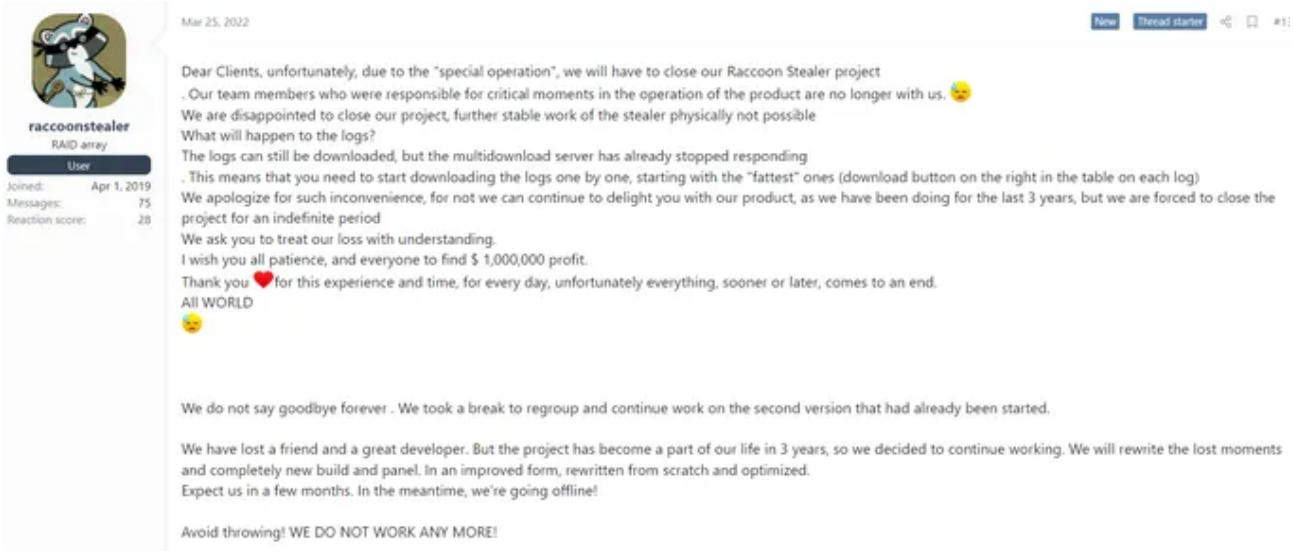


Distribution of bots offered for sale in Russian Market in January 2022 – July 2022, by stealer, as collected by KELA's systems

Raccoon Stealer

Raccoon stealer was among the recommendations for users willing to leave RedLine. The information stealer was offered for rent for USD200 per month for basic use plus USD50 for additional services. However, on March 25, 2022, the operators announced that, after three years of activity, they are suspending the project due to the loss of their developer during Russia's invasion of Ukraine ("the special operation"). They stated that the project will return in an optimized form in a few months.





Source: XSS

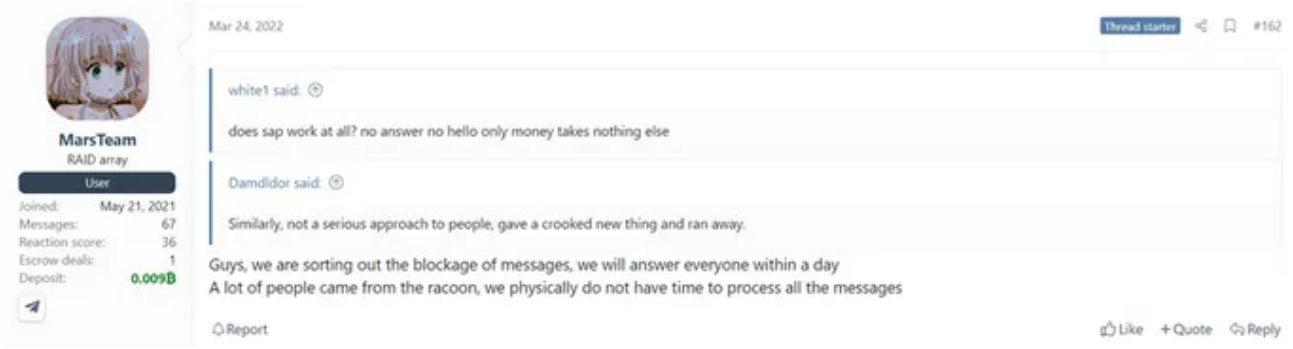
Several users expressed their disappointment following Raccoon's decision to suspend the operations stating that they are looking forward to their return, while others started searching for other options.

Source: WWH Club

On June 2, 2022, the actors behind Raccoon Stealer claimed they developed version 2.0 of their malware. On June 30, 2022, threat actors behind the Raccoon Stealer officially released its 2.0 version.

Mars Stealer

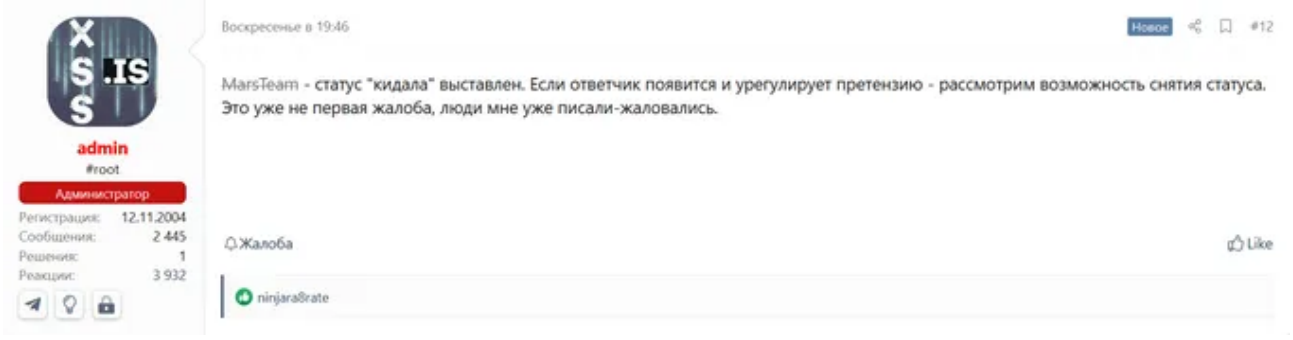
Although threat actors may be loyal to their providers, the business must go on. KELA observed the MarsTeam – developers of the Mars stealer – claiming on the XSS forum that many Raccoon users switched to the Mars stealer, even prior to Raccoon suspending their operations. The Mars stealer, first advertised on June 21, 2021, is being offered for USD140 per month or USD800 as a lifetime subscription.



Auto-translated from Russian. Source: XSS

Based on the above screenshot, the Mars stealer seemed to be a promising stealer to replace Raccoon, however, at the beginning of April 2022, KELA observed several complaints from users on XSS who stated that the Mars operators were not responsive. On April 16, threat actor JohnCrystall opened a dispute, claiming that, upon making a purchase, MarsTeam failed to provide the requested tools. Upon these allegations, on April 17, the forum's administrator banned the MarsTeam account and marked them as "scammers".

As of now, there is no recent activity from MarsTeam, and some users suggested that the operations may have been affected by the invasion in Ukraine, however, the reason remains unclear.

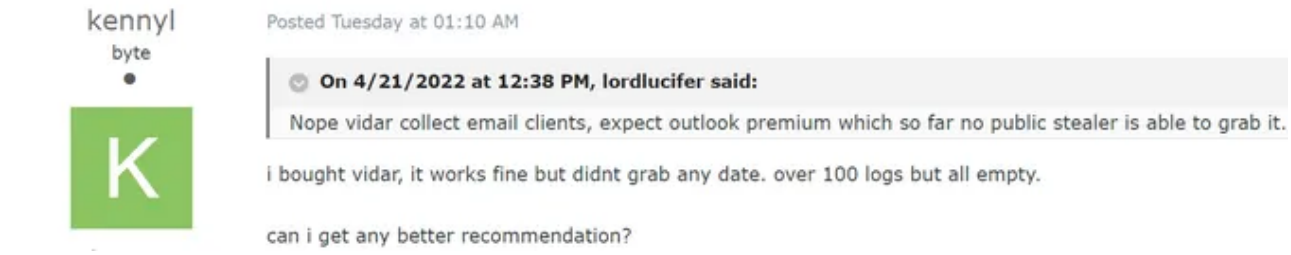


Translation from Russian: The "scam" status is set. If the defendant appears and settles the claim, we will consider the possibility of removing the status. This is not the first complaint, people have already written to me, complained. Source: XSS

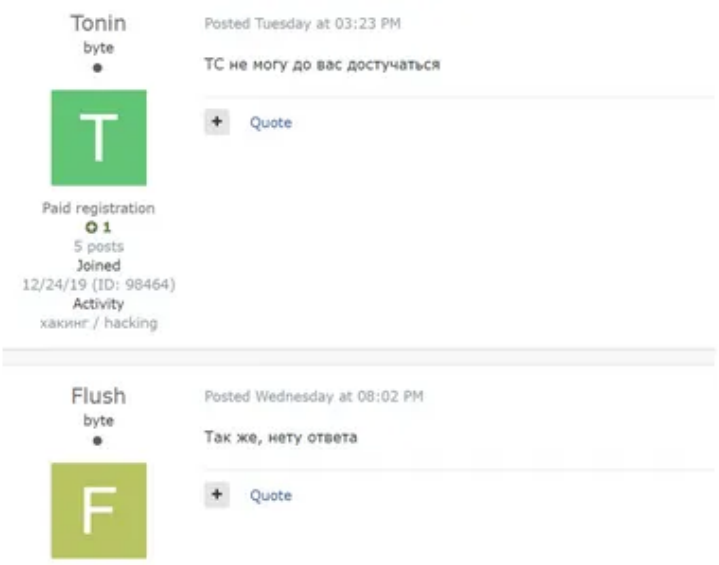
Vidar Stealer

Vidar was first introduced in November 2018 and remains one of the most popular and used information stealers. The operators maintain a support Telegram channel @Vidar_supwwh where they sell the software for USD1500 and offer additional installation services. KELA also identified Vidar in recent bots on RussianMarket and TwoEasy.

On April 25, 2022, KELA observed several actors on the Exploit forum complaining about the stealer's capabilities.



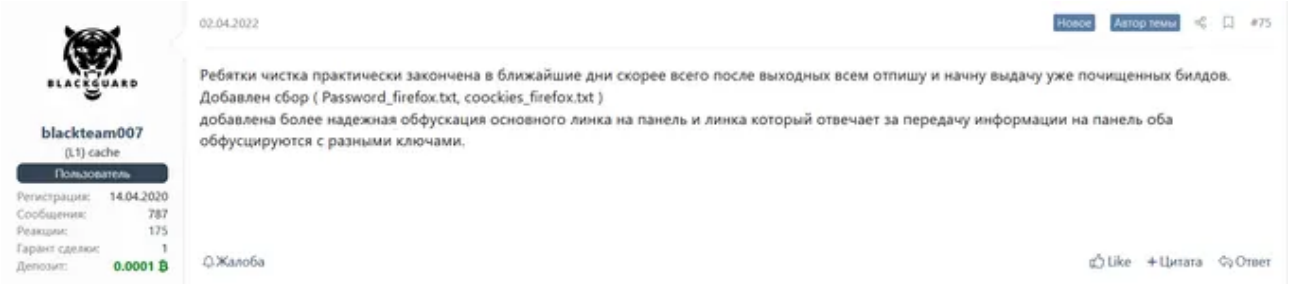
Moreover, on April 26 and 27, 2022, users stated that the Vidar Telegram support team is not responsive. This seems to be a pattern in some of the commodity stealers services and it is yet to be determined if Vidar stealer will continue to be a primary choice for threat actors.



Source: Exploit

BlackGuard Stealer

As cybercriminals are constantly testing the capabilities of such malicious tools, they do not shy away from demanding more quality and improvements. One example in this regard is the BlackGuard stealer, launched in early 2021. KELA came across several recent discussions in which users were complaining about BlackGuard not being able to properly avoid detection. As in any business, the operators promised to provide an updated version in no time.



Translation from Russian: Guys, the cleaning is almost finished in the coming days, most likely after the weekend I will write to everyone and start issuing the already cleaned builds. (…) Added more reliable obfuscation of the main link to the panel and the link that is responsible for transferring information to the panel, both are obfuscated with different keys. Source: XSS

Private Stealers

The previous chapter showed that some of the well-known commodity stealer operators, although present in the cybercrime ecosystem for a long time, may encounter difficulties in the way they conduct business, which leaves their customers unsatisfied. As the threat landscape is constantly changing, other threat actors may find new financial opportunities in developing "private stealers", either by using the source code of commodity stealers or by creating brand-new ones. KELA has observed several such stealers being advertised on cybercrime forums and researchers also confirmed them being actively exploited in the wild.

On March 7, 2022, KELA observed a threat actor named _META_ announcing the launch of META – a new information-stealing malware, available for sale for USD125 per month or USD1000 for unlimited use. The actor claimed it has the same functionality, code, and panel as the Redline stealer, but with several improvements:

1) Removed unnecessary functionality from the panel

2) Added setting for collecting extensions from the browser

3) Added the Reset default settings button, which allows you to return the default settings of the panel if you suddenly need it

4) Cleaned stub

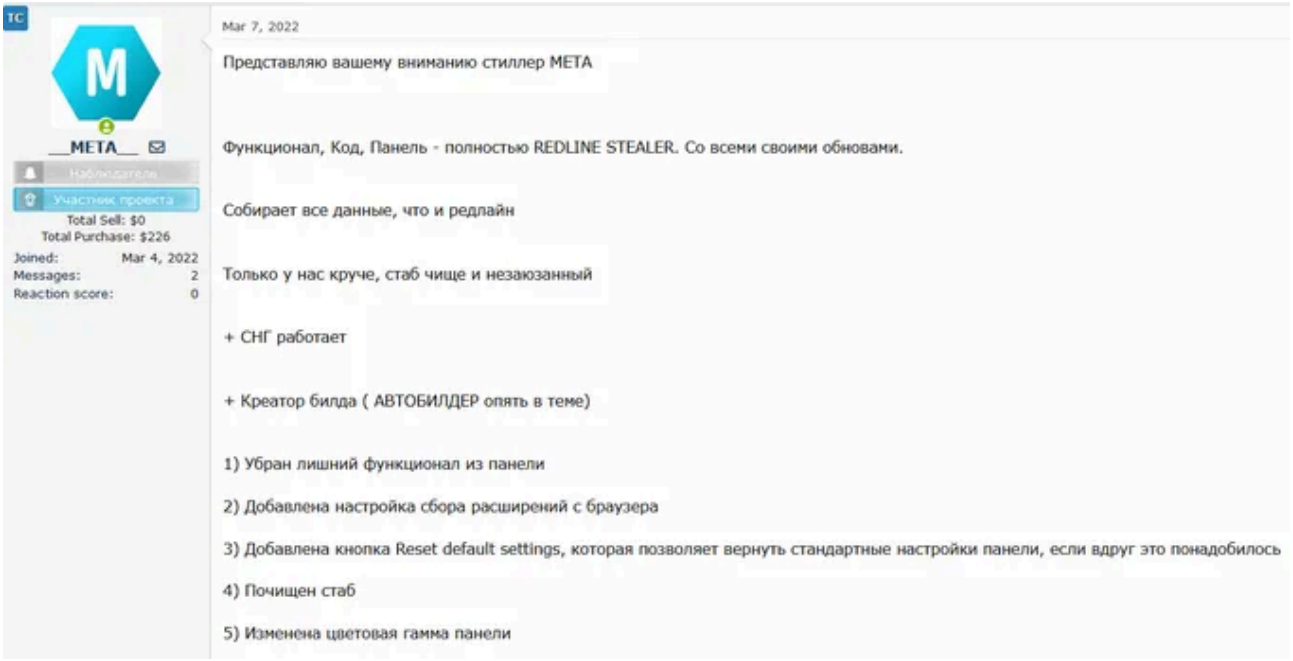
5) Changed the color scheme of the panel

6) Removed AntiCNG

7) Added the ability to view the private key for the generator (needed for auto-build in your bots for the team), to view it, you must re-enter the password from the panel (2FA, not to steal the key)

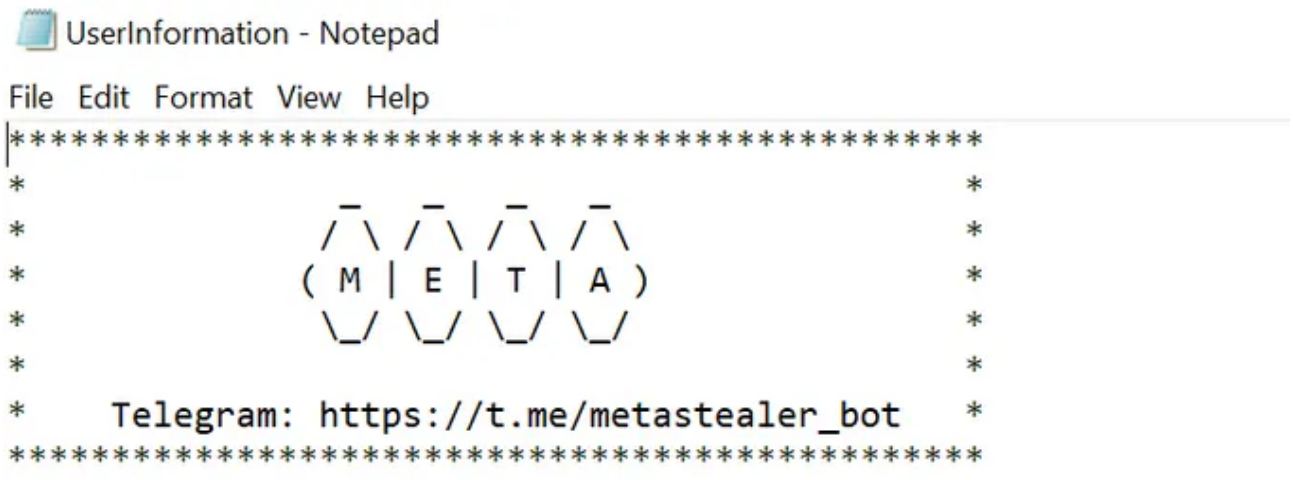
8) The weight of the build is reduced to 88KB, thanks to the new stub

9) Cleaned build runtime



User _META_ announcing the META stealer

KELA also identified the stealer in several bots sold on the TwoEasy botnet marketplace and can confirm its similarities with Redline based on the folder's structure. As of now, there are around 1200 bots containing the META strain available for sale on the TwoEasy market.



Bot sample infected with Meta stealer malware. Source: KELA

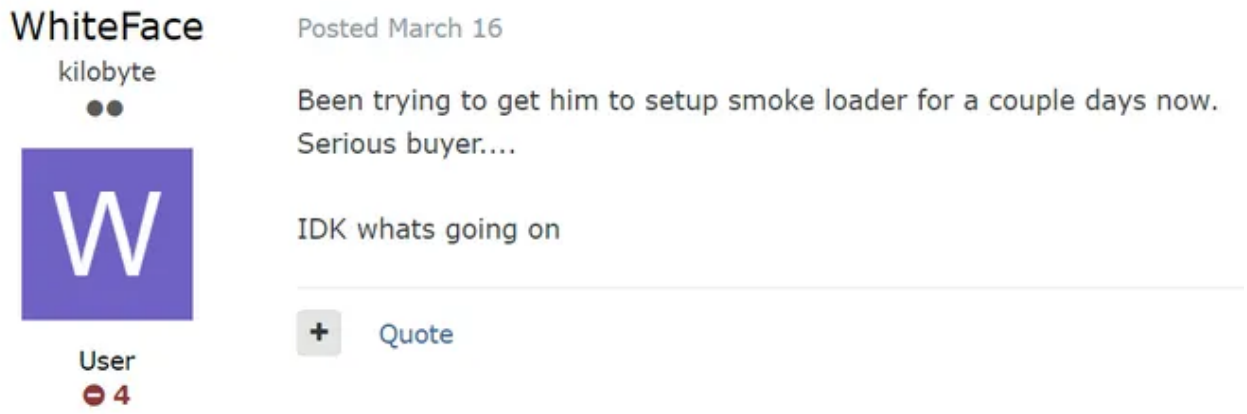
Researchers confirmed that several samples of a specific Excel file containing the Meta stealer have been submitted to VirusTotal. Based on the findings, the malicious files are distributed via phishing emails.

Arkei Stealer

In February 2022, researchers observed new variants of the Arkei malware – an information stealer focused on collecting, among others, 2FA or MFA data from its victims. Arkei has also been previously seen in the wild and advertised on cybercrime forums, and it now has improved its malware capabilities. The malware only targets

Windows-operating machines and their initial attack vector may vary, however it has been recently seen deployed from phishing websites offering malicious software masquerading as legitimate applications and programs.

Arkei was observed being deployed by SmokeLoader aka Dofoil – a malware downloader initially observed in 2011 and used to deliver other malware via email attachments in phishing campaigns. Later, the malware was seen delivering information stealers including Raccoon and RedLine. Since the beginning of 2022, KELA has observed several actors on cybercrime forums interested in purchasing SmokeLoader.



Threat actor willing to purchase SmokeLoader.

Ginzo Stealer

The Ginzo Stealer (also referred to as ZingoStealer) was announced on March 4, 2022, by the Russian-speaking threat actor “HaskersGang” on their Telegram channel. The malware can exfiltrate credentials, steal cryptocurrency wallet information, and perform crypto mining. According to researchers, the ZingoStealer is currently being distributed under the guise of game cheats, cracks, and code generators. In several cases, ZingoStealer also delivers additional malware such as the RedLine Stealer. On April 13, 2022, HaskersGang announced on their Telegram channel that an updated version of the bot has been released and that they are transferring the ownership to user CryptoGinzo, as the previous “owner” – part of the HaskersGang – is no longer involved in the operation.

Translation from Russian: *We are pleased to present to you our free product that can freely compete with other projects – @ginzostealer_bot (…). Source: Telegram*

Translation from Russian: Attention! We have updated our bot! You need to enter /start again to update the bot. A little about recent events: the stealer is now owned by @CryptoGinzo, the previous owner is no longer involved in the stealer. At the moment, the project is in good hands, I declare this with confidence – Keepye. Source: Telegram.

Eternity Stealer

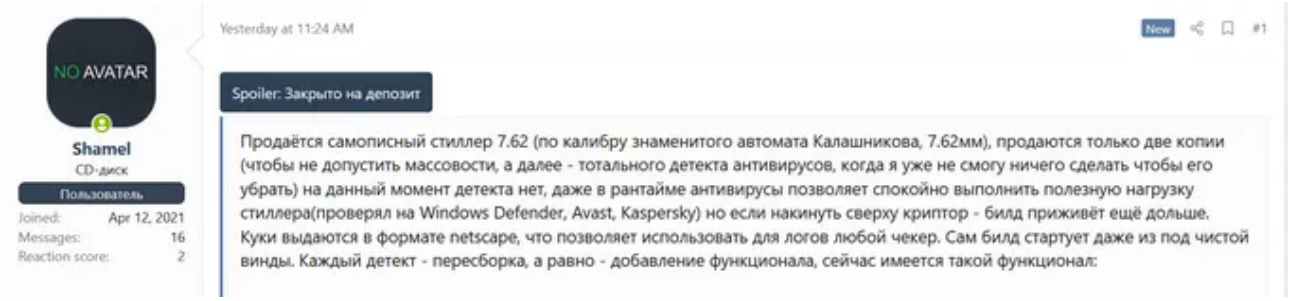
Eternity Stealer was announced by EternityTeam on the XSS forum on March 26, 2022. The stealer is able to gather passwords, cookies, tokens, history, bookmarks, credit card and crypto-wallet information from the infected machines. It works on a variety of browsers, password managers, VPN and FTP clients, email clients and messengers, and gaming software.

Users can create and customize the stealer through a web builder with options such as preventing second start from one computer (AntiRepeat), enabling AntiVM, self-destruction upon execution, preventing execution in CIS countries, as well as selection the preferred output file execution. The builder price is USD300 for a lifetime subscription and USD320 with crypt included.

7.62mm Private Stealer

On April 25, 2022, KELA observed threat actor Shamel advertising a new private stealer – 7.62mm – on the XSS forum. The actor stated that they will sell only two copies to prevent mass usage and wide antivirus detection. Based on the post, the 7.62mm stealer is, as of date, undetectable, and can target crypto wallets such as Ethereum, Exodus, Bitcoin Core, Armory, wallet browser extensions including Binance, Coinbase, Phantom, browsers such as Chrome, Mozilla, Opera, Edge, Waterfox, as well as sessions of client applications including Telegram, Steam, Minecraft, FileZilla.

The stealer is sold in two formats – DLL or EXE and the actor also provides a search engine for the “logs” obtained. The price for unlimited use is USD500.



Threat actor Shamel advertising the 7.62mm private stealer. Source: XSS

Inno Stealer

On April 18, 2022, researchers revealed that cybercriminals are using a malicious website offering fake Windows 11 upgrades. Users are lured into downloading an ISO file that contains the executable for the new Inno information-stealing malware. The stealer's capabilities include collecting web browser cookies and stored credentials, data in cryptocurrency wallets, and data from the filesystem. Researchers stated that although this is the typical activity for stealers, Inno does not have any code similarities to other known information-stealers. This is an advantage of such private stealers that allows for a limited number of users to deploy the malware and reduces the chances of detection.

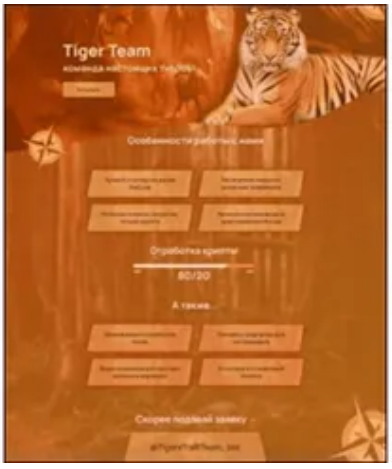
Info-stealers' "affiliate programs"

To ensure good business development and to facilitate the use of their products, information-stealer operators started to offer additional tools and services. KELA also observed threat actors looking for users to help test their products prior to their release, to speed up the developing process.

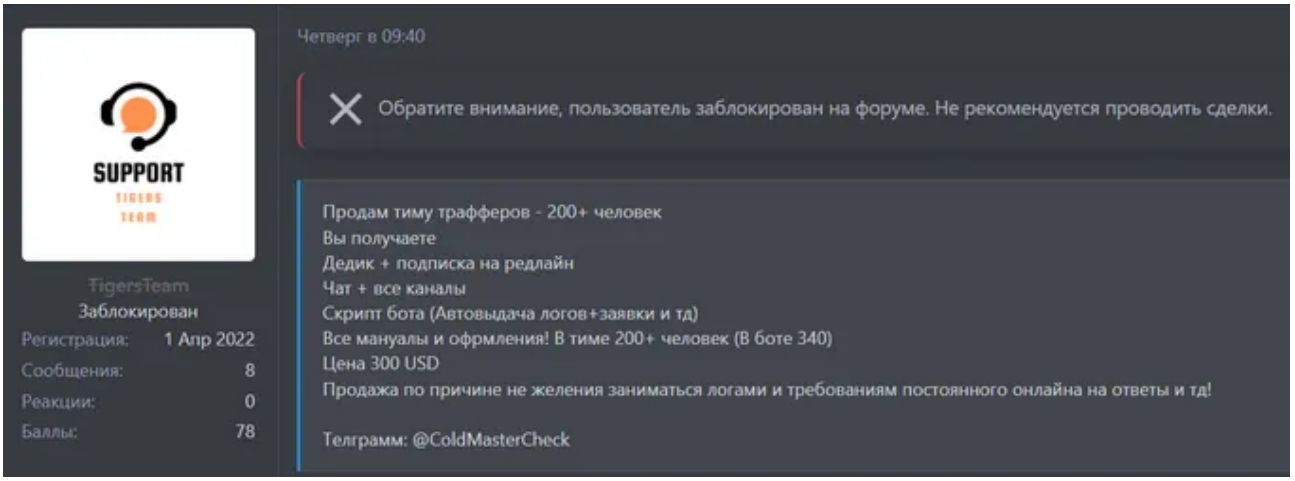
Particularly interesting are info-stealers' "affiliate programs": KELA observed various groups advertising new so-called "traffer kits/sets" – an operational structure where interested users ("traffers" – related to the word traffic, potentially referring to actors who have the means to infect multiple targets) are provided with the necessary tools including the information stealer build, channels to exfiltrate the data, software to exploit the obtained logs, and technical support, in exchange for various deals. For instance, some would require affiliates to pay a fee in exchange for access to the kit and full ownership of the obtained logs, while others would request a percentage of the logs.

TigersTeam

On April 1, 2022, TigersTeam introduced its information-stealer services: "The best stealer on the market – RedLine; free promotion for active "traffers"; automatic issuance of crypto build; echo channel (logs coming in); excellent and helpful colleagues; all logs are yours! We work out only the crypt – 80% to you!"



On April 14, upon being banned from the BHF forum, the TigersTeam offered to sell their team of "traffers" for USD300. The deal would include all related channels, RedLine stealer + "dedik" (dedicated server), the bot script, and over 200 people in the team.



Source: BHF

Aurora Project

On April 18, 2022, KELA observed actor cheshire666 on the WWH Club forum who introduced themselves as a coder for the “Aurora project” looking for 3-5 people to beta test their product before the final release. The actor promised that those who will take an active part in finding bugs or improving the project will be awarded a free subscription for a month.

The product would consist of:

1) Builder (with the possibility of polymorphic compilation and compression)

2) Stealer

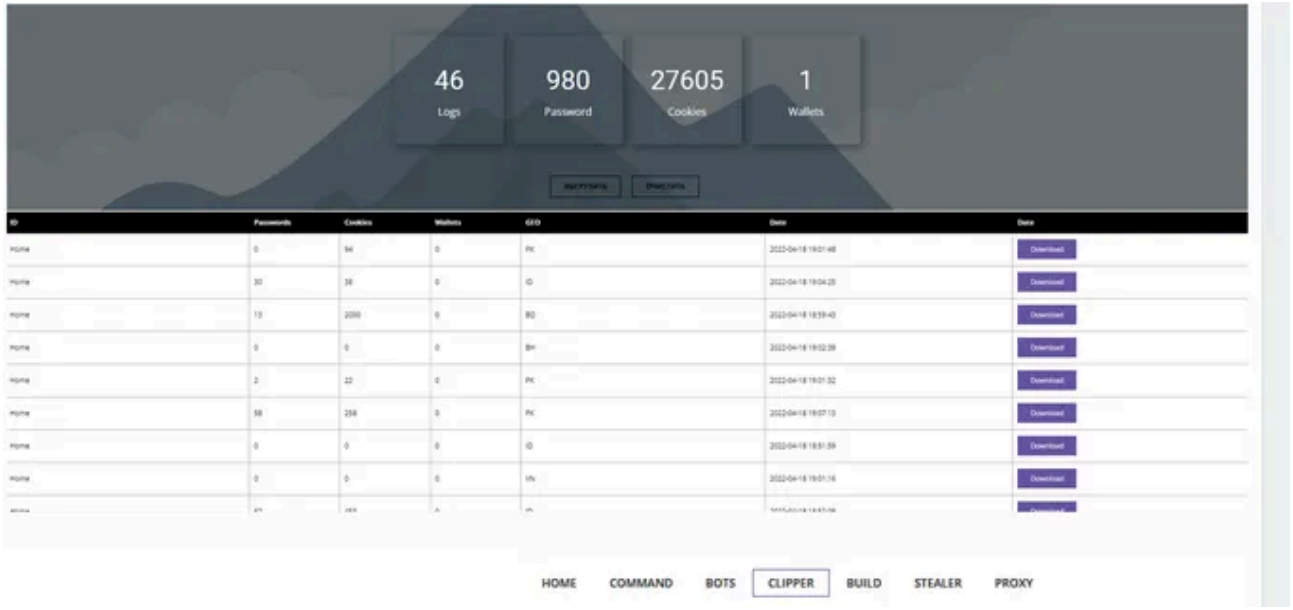
3) Clipper BTC, ETH, LTC

4) The botnet is located on a shared dedicated server and has spare servers for migration

5) If the server is unavailable, the bots will automatically start searching for a new server

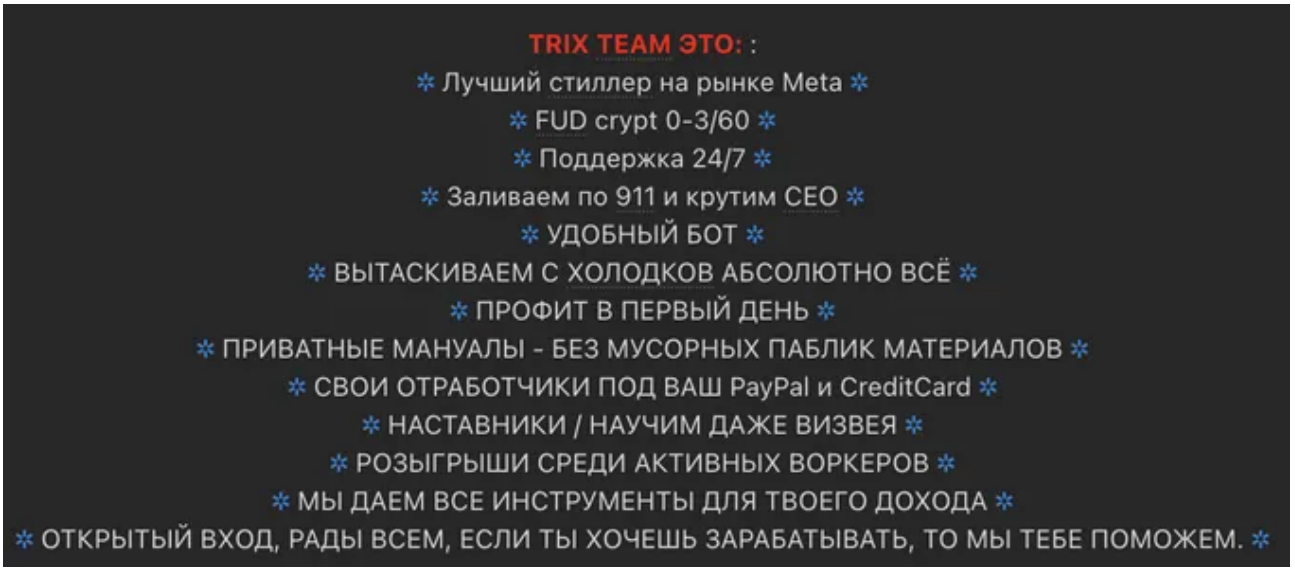
6) 2FA via Telegram

Actor cheshire666 looking for testers for the "Aurora project". Source WWH Club

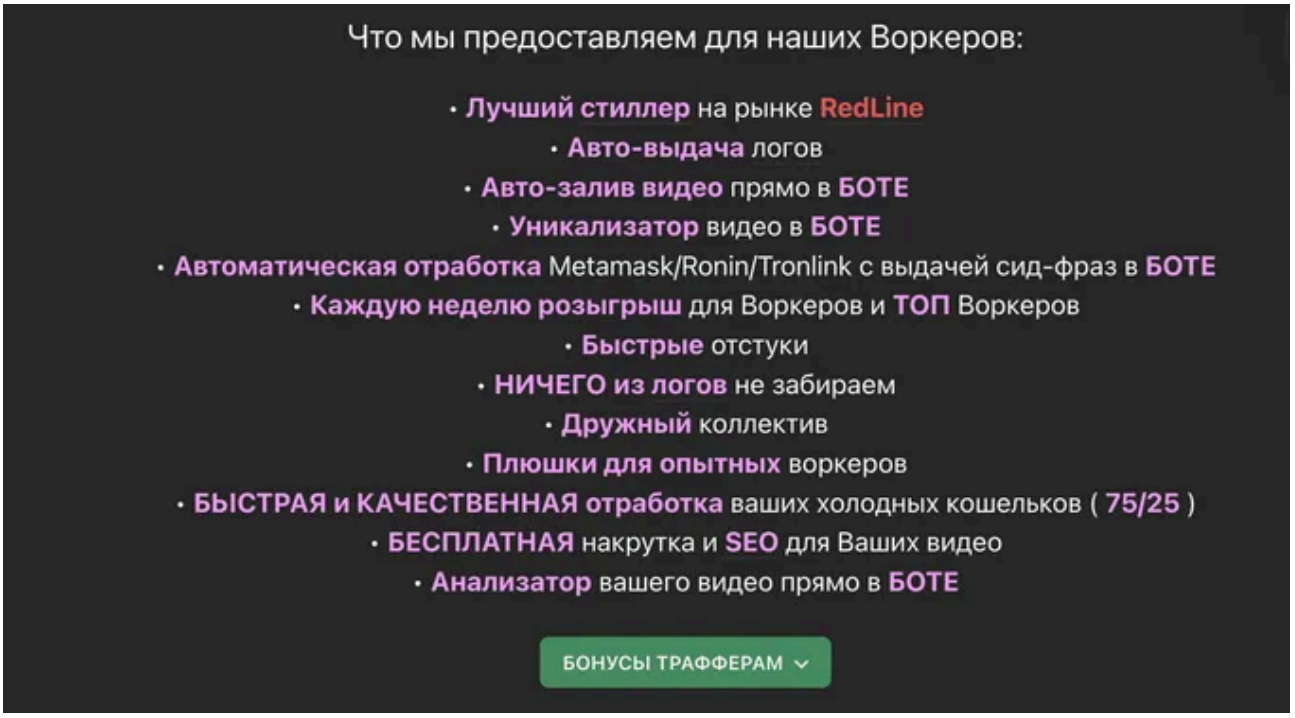


Screenshot of the product provided by cheshire666. Source: WHH Club

Other similar new "affiliate programs" identified by KELA are the Trix Team and Amethyst Family. They provide access to stealers (Meta and RedLine, respectively) and related tools, auto-issuance of logs, manuals, mentorship, and bonuses.



Trix Team announcement. Source: Lolz.guru market



Amethyst Family announcement. Source: Lolz.guru market

Source: https://ke-la.com/information-stealers-a-new-landscape/