DELVING INTO THE EMERGING INFOSTEALERS OF 2023

KELA

Delving into the emerging infostealers of 2023

Yael Kishon, Cyber Threat Intelligence Analyst

Table of Contents

Executive Summary

The risk of cyber attack by information stealers continually poses a threat on organizations in the last few years, and continues to be a significant concern for companies in 2023. The emergence of new infostealers highlights the ongoing efforts of cybercriminals to create new tools for stealing sensitive data.

Information stealer (infostealer) malware is malicious software that steals sensitive information from the victim's computer ("bot"). This information ("logs") usually contains browser login information including passwords, cookies, credit card details, crypto wallet data, and more.

Cybercriminals are constantly developing new variants of infostealer malware to evade detection and maximize profits. Threat actors put the logs for sale on automated markets, Telegram channels, and other platforms. Thus, threat actors aim to infect as many machines as possible, steal data, sell it for profit, or use it in their next malicious campaigns.

Among the most widely recognized commodity infostealers are RedLine, Raccoon, and Vidar. Stolen credentials compromised through this malware are available for sale on automated marketplaces such as RussianMarket, Genesis, and TwoEasy, as well as on other platforms.

Cybercriminals work hard to develop new commodity stealers and release them into the automated botnet markets at affordable prices to appeal to a wider audience.

In this report, KELA focuses on new infostealers like Titan, LummaC2, WhiteSnake, and others who have recently emerged from the cybercrime underground and have already gained popularity among threat actors. The current report is the next in a series following our previous report published in 2022.[1]

[1] The Next Generation of Info Stealers

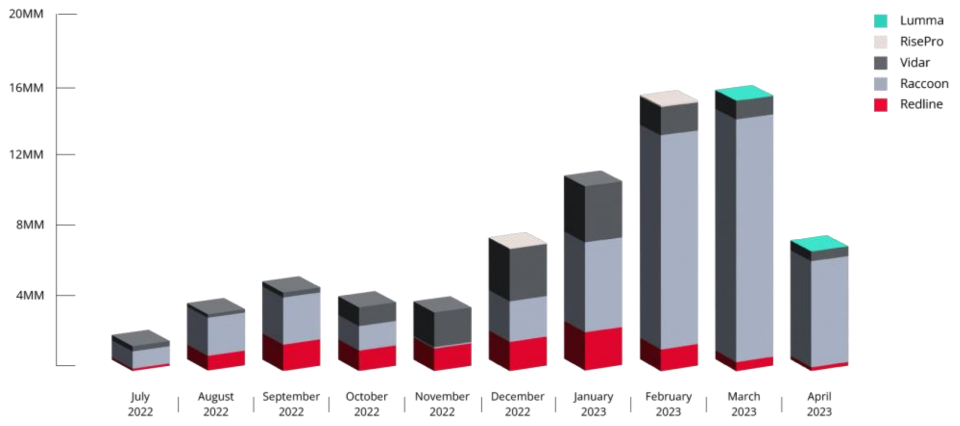
Botnet Marketplaces

Over the past few years, KELA has been closely tracking automated stores that sell stolen login credentials obtained from computers infected with an infostealer. These include RussianMarket, TwoEasy, and Genesis. In the first half of 2022, we identified the most popular stealers on the Russian Market, based on its metadata, as Redline, Raccoon, Vidar, and META.

Since July 2022, Raccoon and Vidar stealers have outplayed Redline as the most popular information-stealing malware. They were accountable for over 85% of all credentials that were advertised on RussianMarket within the focus period of this study (10 months).

In March 2022, the developer behind the Raccoon stealer was arrested and faced charges.[2] However, it seems that the charges did not have an impact on the malware's success. Although around the time of his arrest, Raccoon representatives announced they were suspending their operations, in fact, Raccoon 2.0 version was nevertheless released in June 2022.

Distribution of bots on Russian Market since July 2022



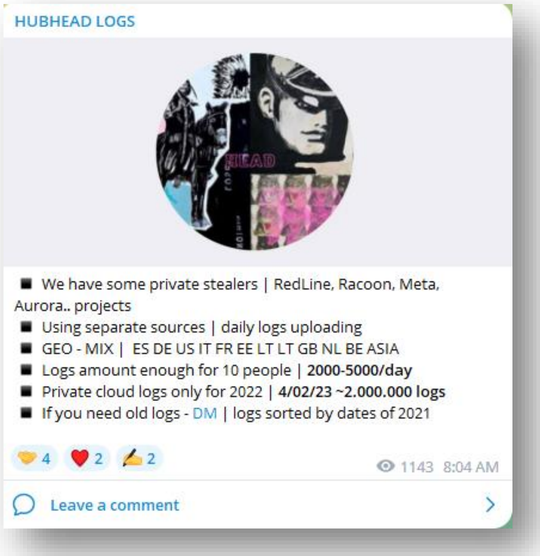
From 2022 through 2023, Russian Market listed bots stolen through diverse infostealer strains, including RisePro alongside other prominent ones previously mentioned.

[2] Ukrainian charged for operating Raccoon Stealer malware service

RisePro is a relatively new stealer that was spotted in the cybercrime ecosystem at the end of 2022. It was quickly adopted by some cybercriminals. On January 23, 2023, the actor 'doZKey' claimed on a Russian hacking forum called "BHF", as well as on a Telegram channel called "InstallsKey", that they are able to infect machines using RisePro, becoming one of the first public reviews for the stealer. In the same month, credentials stolen through RisePro were almost immediately put on sale on RussianMarket. Researchers have found that RisePro is actually a clone of the info-stealer Vidar.[3]

Clouds of logs

In recent years, a new type of product emerged named "clouds of logs", in addition to automated marketplaces Cloud of logs offers users to purchase access to threat actors' collections of files via private cloud-based platforms, with Telegram becoming one of such platforms.[4] Usually, the purchase is based on a subscription fee.



HUBHEAD LOGS

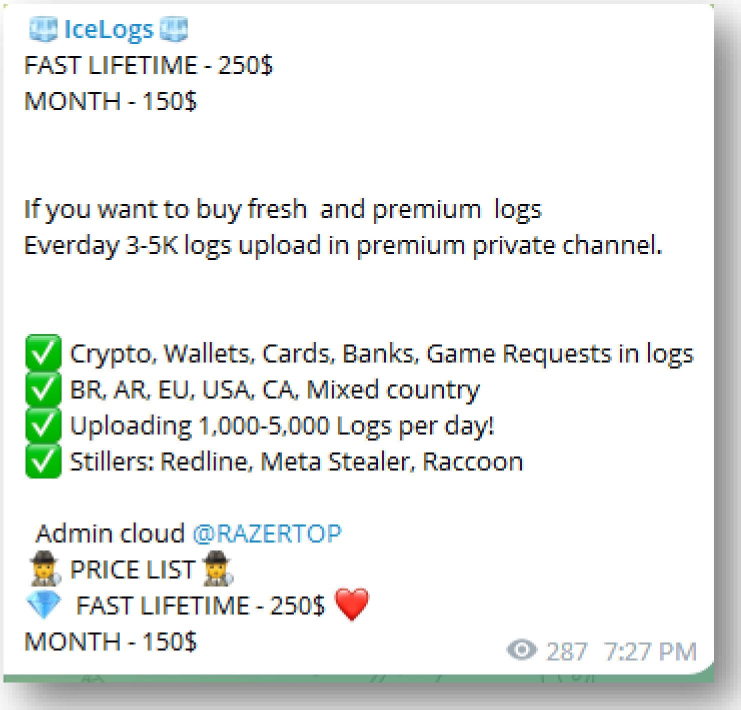
■ We have some private stealers | RedLine, Racoon, Meta, Aurora.. projects
■ Using separate sources | daily logs uploading
■ GEO - MIX | ES DE US IT FR EE LT LT GB NL BE ASIA
■ Logs amount enough for 10 people | **2000-5000/day**
■ Private cloud logs only for 2022 | **4/02/23 ~2.000.000 logs**
■ If you need old logs - DM | logs sorted by dates of 2021

HUBHEAD LOGS selling logs obtained through different stealers

[3] New info-stealer malware infects software pirates via fake cracks sites

[4] Telegram. How a messenger turned into a cybercrime ecosystem by 2023

KELA has identified dozens of Telegram channels promoting logs for free, as well as those offering private logs collected by custom or commodity stealers. Popular channels usually include information on how the credentials have been obtained, which gives an opportunity to gain insights into the trendiest tools. Analysis of several popular Telegram channels shows that it is mostly Redline bots that are being leaked and distributed through Telegram channels. Other top stealers are Vidar, Raccoon, META, and Mars, all of which are well-known commodity stealers that emerged during 2021-2022. However, other infections can also be found on Telegram channels, even the most recent ones that came up as late as 2022 (Offx stealer being an example).



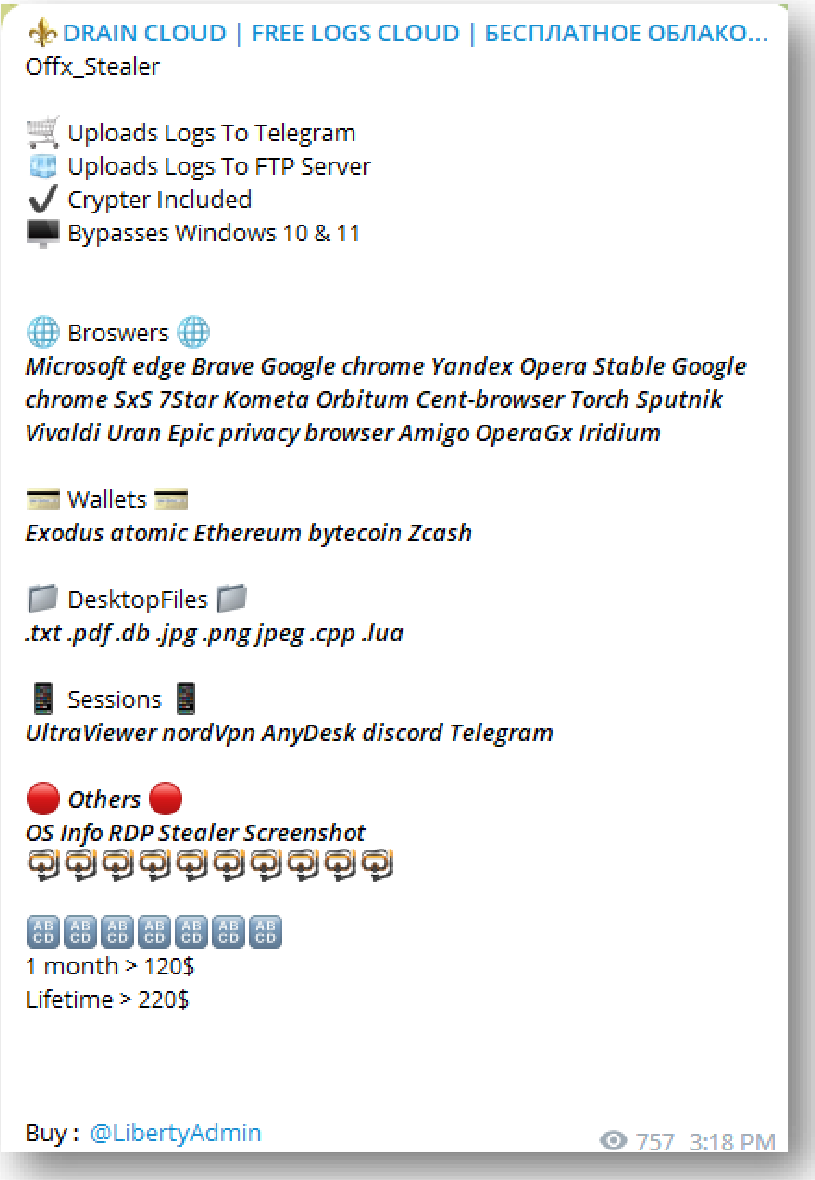
🧊 IceLogs 🧊
FAST LIFETIME - 250$
MONTH - 150$

If you want to buy fresh and premium logs
Everday 3-5K logs upload in premium private channel.

✅ Crypto, Wallets, Cards, Banks, Game Requests in logs
✅ BR, AR, EU, USA, CA, Mixed country
✅ Uploading 1,000-5,000 Logs per day!
✅ Stillers: Redline, Meta Stealer, Raccoon

Admin cloud @RAZERTOP
🕵 PRICE LIST 🕵
💎 FAST LIFETIME - 250$ ❤️
MONTH - 150$

IceLogs is selling logs obtained through Redline, META, and Raccoon stealers



⚜ DRAIN CLOUD | FREE LOGS CLOUD | БЕСПЛАТНОЕ ОБЛАКО...

Offx_Stealer

🛒 Uploads Logs To Telegram
🧊 Uploads Logs To FTP Server
✔ Crypter Included
🖥 Bypasses Windows 10 & 11

🌐 Broswers 🌐
Microsoft edge Brave Google chrome Yandex Opera Stable Google chrome SxS 7Star Kometa Orbitum Cent-browser Torch Sputnik Vivaldi Uran Epic privacy browser Amigo OperaGx Iridium

💳 Wallets 💳
Exodus atomic Ethereum bytecoin Zcash

📁 DesktopFiles 📁
.txt .pdf .db .jpg .png jpeg .cpp .lua

📱 Sessions 📱
UltraViewer nordVpn AnyDesk discord Telegram

🔴 *Others* 🔴
OS Info RDP Stealer Screenshot
🤿🤿🤿🤿🤿🤿🤿🤿🤿🤿

🔠🔠🔠🔠🔠🔠🔠
1 month > 120$
Lifetime > 220$

Buy : @LibertyAdmin

757 3:18 PM

Drain Cloud shares logs from Offx stealer, which emerged at the end of 2022

Emerging infostealers of 2023

Threat actors never rest. They constantly work on developing new infostealers to effectively steal browser information and infect as many machines as possible, as well as develop Malware-as-a-Service (MaaS) operations to distribute the stealers and gain customers. As a result, new infostealers can quickly be adopted by cybercriminals and used to compromise more victims.

One such stealer - Aurora, identified by KELA in April 2022, has transformed over a year into a MaaS operation with over 6,000 subscribers on its Telegram channel. We found at least five affiliate programs that claimed they worked with Aurora malware to steal logs. The price for the Aurora monthly subscription is USD 125, whereas an unlimited lifetime version is available for USD 1,000.

In this section, KELA delves into the world of these infostealers, exploring their unique characteristics, techniques, and the potential ramifications they pose for individuals and businesses. The cybercrime chatter suggests that in recent months, actors have continued launching their operations and renting their infostealers to other threat actors. KELA identified several rising stealers that emerged at the end of 2022.

Titan

The Titan stealer was published on Russian-speaking hacking forums BHF and Dark2Web on November 26, 2022, by an actor named ‘TitanSeller’. The same post was published on XSS forum in December 2022 also promoting the corresponding Telegram channel and chat. The Telegram channel titled “Titan Stealer” was created on November 5, 2022.

The actor behind the malware claimed that the stealer was able to steal information from twenty browsers, which is similar to the capabilities of other stealers. Titan enables cybercriminals to obtain information like passwords, cookies, history, credit cards, and crypto wallets. The malware is written in Golang language, as is Aurora, which is considered to be Titan’s main competitor, as claimed by Titan’s developer.

TITAN STEALER

Быстрая тех поддержка
Быстрый сбор данных
Серверный декрипт
Большой функционал
MAAS
Цена: 100$/месяц.

Titan Stealer's ad on BHF forum

On March 1, 2023, an updated 1.5 version of Titan was released. As of April 2023, the Telegram channel of Titan has more than 600 subscribers. Based on the comments on the channel, it seems that some users are interested in buying the stealer or are already using it and are satisfied with the level of communication with the channel administrator.

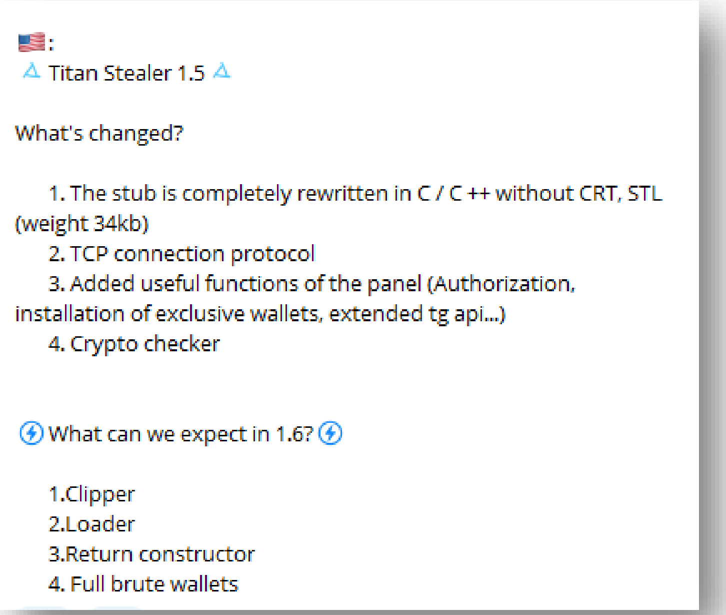
There is also a "Titan Stealer Chat," where the administrator posts announcements about new versions, and users can ask questions about the stealer. Interestingly enough, KELA has identified a team called "Factory Traffer"[5] as a group subscriber, which could mean that the group already distributes Titan malware or is interested in cooperation.

Actors can buy access to Titan malware for a monthly subscription of USD 120 for beginners or unskilled actors, as well as USD 140 for more experienced actors, or USD 999 for a team.

On April 14, the threat actor posted that the team would release another version soon.

[5] Traffers are actors who are responsible for redirecting users' traffic to malicious content

On April 16, the pro-Russian hacktivist group Killnet announced that the Titan Stealer team joined their community. Since then, Killnet and Titan have already collaborated on one attack, allegedly targeting NATO, according to the group's Telegram channel.



🇺🇸:
△ Titan Stealer 1.5 △

What's changed?

1. The stub is completely rewritten in C / C ++ without CRT, STL (weight 34kb)
2. TCP connection protocol
3. Added useful functions of the panel (Authorization, installation of exclusive wallets, extended tg api...)
4. Crypto checker

⚡ What can we expect in 1.6? ⚡

1.Clipper
2.Loader
3.Return constructor
4. Full brute wallets

Titan stealer 1.5 version release announcement

LummaC2

The first version of LummaC2 stealer was released by the actor ‘Shamel’ on XSS forum on August 15, 2022. The malware is written in C and can steal information from eleven browsers. On December 21, 2022, the actor released an updated version of the stealer, able to gather information from 70 browsers cryptocurrency wallets, and 2FA extensions of the infected machines. The malware can steal 2FA codes from the following applications: Authenticator, Authy, EOS Authenticator, GAuth Authenticator, and Trezor Password Manager.[6] The LummaC2 malware can affect operating systems from Windows 7 to Windows 11.

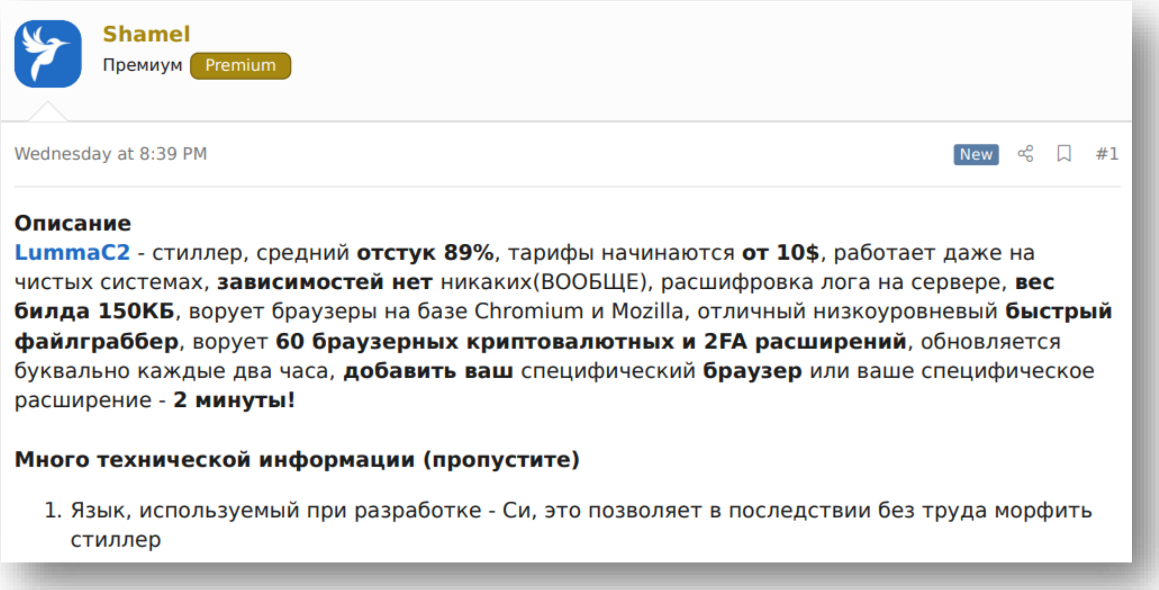
The stealer was offered for USD 250 per month, while an upgraded version for professionals costs USD 500, allowing users to delete logs and share statistics with others.

Interestingly, the LummaC2 Telegram channel was created before the actual release date on XSS in December 2021. However, it seems that the actor later deleted a few posts and the first post that shows on the channel is now from January 2023.

Since February 2023, LummaC2 bots have been put on sale on RussianMarket.

As of April 2023, its Telegram channel has over 1,000 subscribers.

[6] New Infostealer LummaC2 Being Distributed Disguised As Illegal Cracks



Shamel

Премиум Premium

Wednesday at 8:39 PM New #1

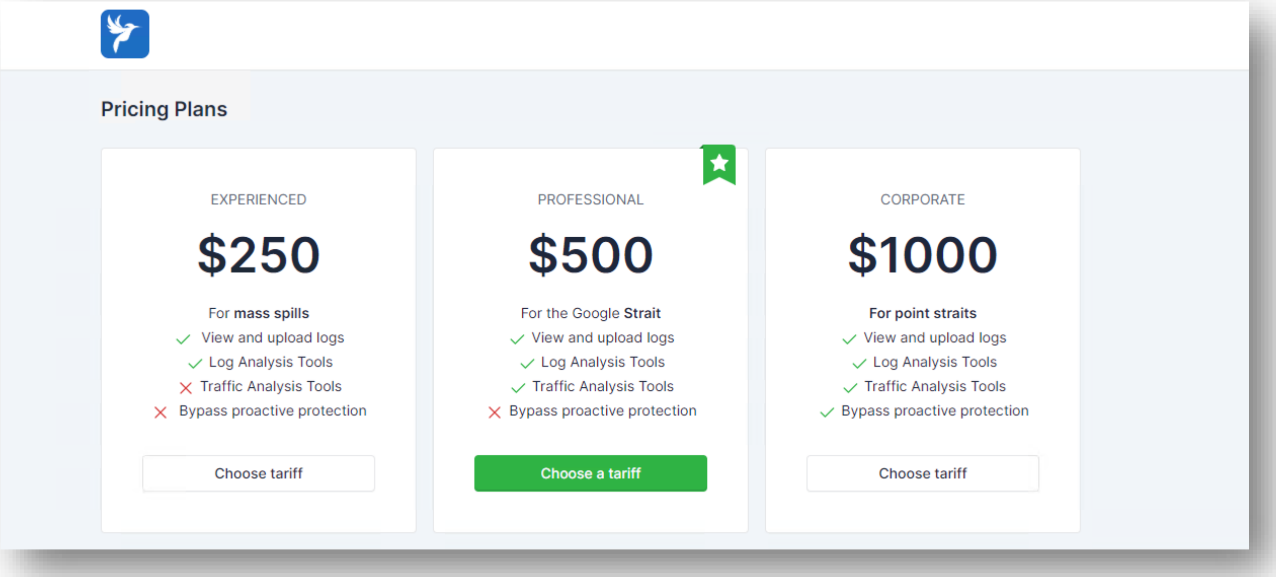
Описание

LummaC2 - стиллер, средний **отстук 89%**, тарифы начинаются **от 10$**, работает даже на чистых системах, **зависимостей нет** никаких(ВООБЩЕ), расшифровка лога на сервере, **вес билда 150КБ**, ворует браузеры на базе Chromium и Mozilla, отличный низкоуровневый **быстрый файлграббер**, ворует **60 браузерных криптовалютных и 2FA расширений**, обновляется буквально каждые два часа, **добавить ваш** специфический **браузер** или ваше специфическое расширение - **2 минуты!**

Много технической информации (пропустите)

1. Язык, используемый при разработке - Си, это позволяет в последствии без труда морфить стиллер

Lummac2 stealer advertised on XSS forum

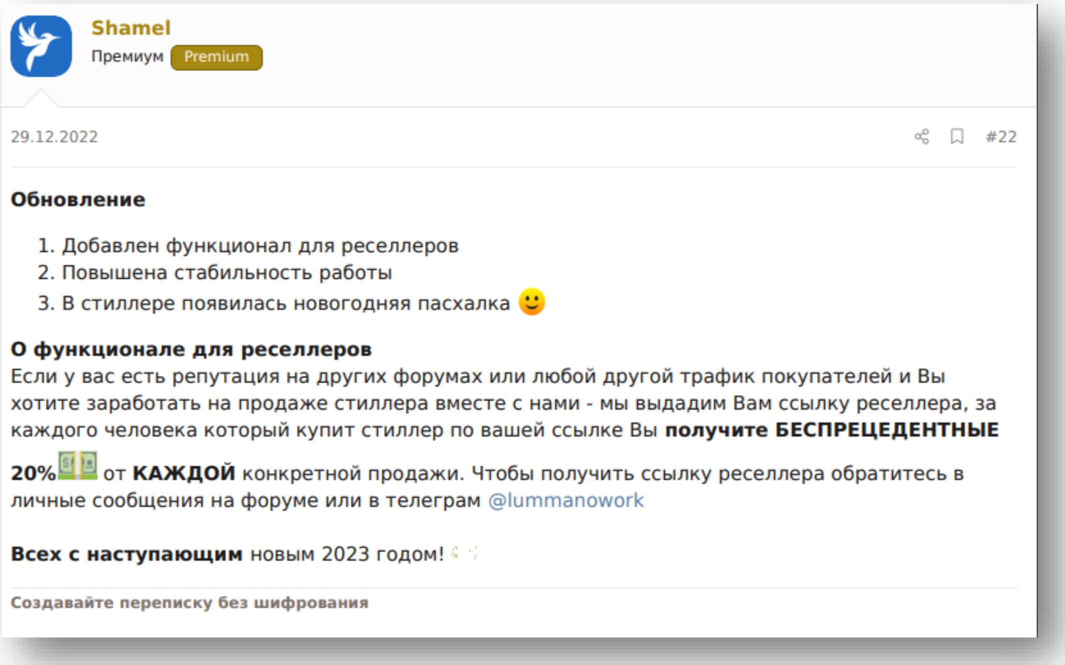


Pricing Plans

EXPERIENCED	PROFESSIONAL	CORPORATE
$250	$500	$1000
For **mass spills**	For the Google **Strait**	**For point straits**
✓ View and upload logs	✓ View and upload logs	✓ View and upload logs
✓ Log Analysis Tools	✓ Log Analysis Tools	✓ Log Analysis Tools
✗ Traffic Analysis Tools	✓ Traffic Analysis Tools	✓ Traffic Analysis Tools
✗ Bypass proactive protection	✗ Bypass proactive protection	✓ Bypass proactive protection
Choose tariff	Choose a tariff	Choose tariff

LummaC2's pricing

The feedback regarding LummaC2 stealer appears to be positive: KELA has identified several threat actors satisfied with the product. They have also recommended it to other cybercriminals who were looking to purchase a stealer for USD 300 per month maximum.



Shamel

Премиум Premium

29.12.2022 #22

Обновление

1. Добавлен функционал для реселлеров
2. Повышена стабильность работы
3. В стиллере появилась новогодняя пасхалка 🙂

О функционале для реселлеров
Если у вас есть репутация на других форумах или любой другой трафик покупателей и Вы хотите заработать на продаже стиллера вместе с нами - мы выдадим Вам ссылку реселлера, за каждого человека который купит стиллер по вашей ссылке Вы **получите БЕСПРЕЦЕДЕНТНЫЕ 20%**💵💵 от **КАЖДОЙ** конкретной продажи. Чтобы получить ссылку реселлера обратитесь в личные сообщения на форуме или в телеграм @lummanowork

Всех с наступающим новым 2023 годом! ✨

Создавайте переписку без шифрования

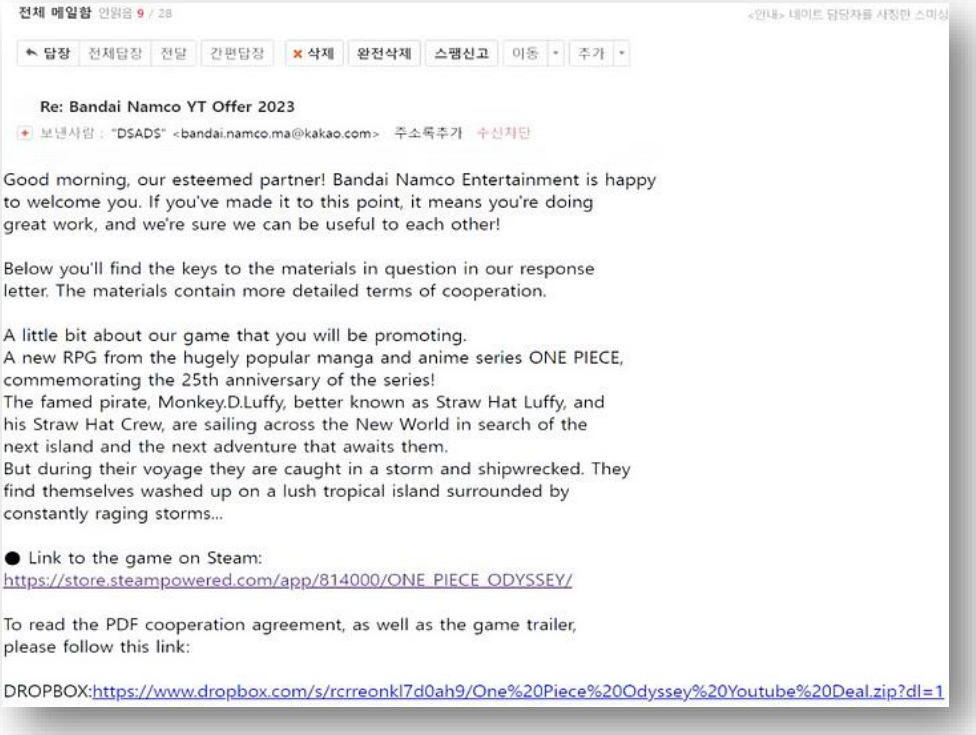
The actor Shamel sharing updates for LummaC2 and offering resellers to join the effort for 20% from each stealer sale

LummaC2 seems to be actively used in ongoing campaigns. In February 2023, researchers found that phishing sites related to OpenAI and ChatGPT were being utilized to deliver different malware families including LummaC2 and Aurora. Threat actors used fake ChatGPT websites and replaced the "TRY CHATGPT" button link with malicious links hosting LummaC2.[7]

Another phishing campaign was detected targeting a South Korea-based voice actor YouTuber. The hacker sent a spear-phishing email impersonating a Bandai Namco game company. A video file and a malicious PDF document were then downloaded from a Dropbox link included in the email. As a next step, the downloaded PDF file installed additional malware - a loader called Pure Crypter, which in turn executed the LummaC2 payload.[8]

[7] Hackers use fake ChatGPT apps to push Windows, Android malware

[8] Lumma Stealer targets YouTubers via Spear-phishing Email



Re: Bandai Namco YT Offer 2023

보낸사람 : "DSADS" <bandai.namco.ma@kakao.com>

Good morning, our esteemed partner! Bandai Namco Entertainment is happy to welcome you. If you've made it to this point, it means you're doing great work, and we're sure we can be useful to each other!

Below you'll find the keys to the materials in question in our response letter. The materials contain more detailed terms of cooperation.

A little bit about our game that you will be promoting.
A new RPG from the hugely popular manga and anime series ONE PIECE, commemorating the 25th anniversary of the series!
The famed pirate, Monkey.D.Luffy, better known as Straw Hat Luffy, and his Straw Hat Crew, are sailing across the New World in search of the next island and the next adventure that awaits them.
But during their voyage they are caught in a storm and shipwrecked. They find themselves washed up on a lush tropical island surrounded by constantly raging storms...

● Link to the game on Steam:
https://store.steampowered.com/app/814000/ONE_PIECE_ODYSSEY/

To read the PDF cooperation agreement, as well as the game trailer, please follow this link:

DROPBOX:https://www.dropbox.com/s/rcrreonkl7d0ah9/One%20Piece%20Odyssey%20Youtube%20Deal.zip?dl=1

A phishing email that delivers LummaC2 malware[9]

LummaC2 developer Shamel has been active on the XSS forum since January 2022. The actor started operating under the new handle Lumma on December 23, 2022 but kept switching back and forth to his original moniker Shamel, adding the logo of the stealer LummaC2 as it appears on the Telegram channel. The actor also posted about LummaC2 on other hacking forums under the name LummaStealer with the same Telegram contact details.

The actor has created a few additional stealers and promoted them on forums. KELA observed that on April 25, 2022, Shamel posted about a private stealer dubbed 7.62mm on the XSS forum. Shamel then said that only two copies would be sold, in order to prevent mass usage and wide antivirus detection. The price for unlimited use was then USD 500. Based on the cybercrime chatter discussions, it seems that none of the actors has bought the stealer and it is still available for purchase.

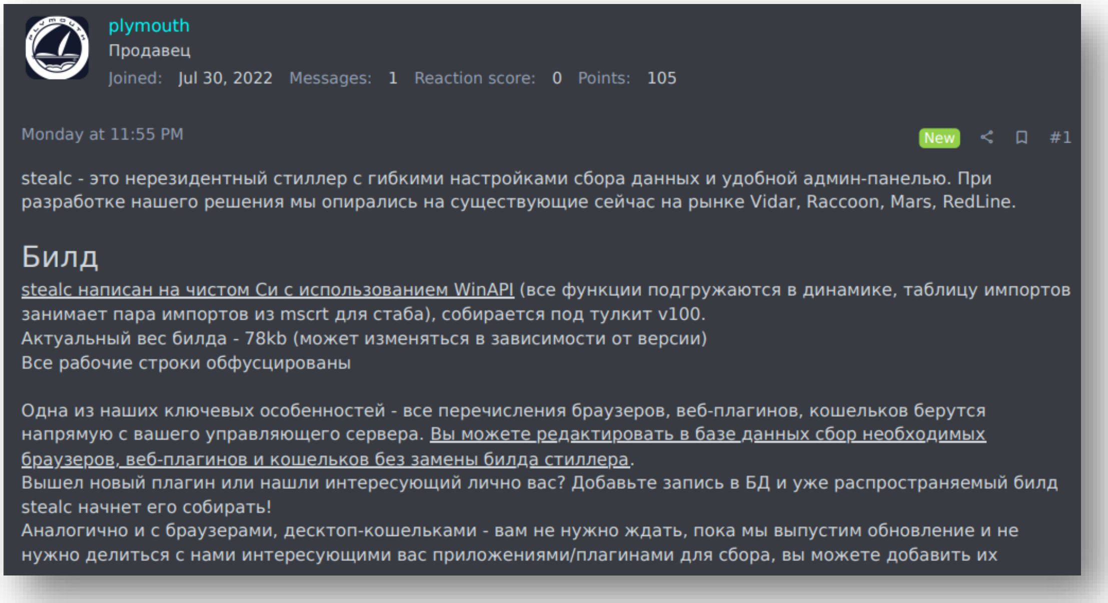
[9] https://www.youtube.com/watch?v=LI9fwFEU8z0

Stealc

On January 9, 2023, the actor ‘plymouth’ published a post on XSS forum, saying they had developed a stealer called Stealc which was based “on Vidar, Raccoon, Mars, and RedLine stealers,”. The actor was probably implying that they attempted to re-create the same features as in these popular stealers.

The Stealc malware is written in C and enables cybercriminals to steal browser information. The actor promoted the stealer on the Exploit and BHF forums, as well as shared there the associated Telegram channel, which had around 200 subscribers as of April 2023.

The price for a monthly subscription for the stealer is USD 200 while a 6-month subscription costs USD 800. On February 26, 2023, the actor released Stealc 1.3.1 version, which enables the upload of a larger number of logs.



plymouth
Продавец
Joined: Jul 30, 2022 Messages: 1 Reaction score: 0 Points: 105

Monday at 11:55 PM

stealc - это нерезидентный стиллер с гибкими настройками сбора данных и удобной админ-панелью. При разработке нашего решения мы опирались на существующие сейчас на рынке Vidar, Raccoon, Mars, RedLine.

Билд

stealc написан на чистом Си с использованием WinAPI (все функции подгружаются в динамике, таблицу импортов занимает пара импортов из mscrt для стаба), собирается под тулкит v100.
Актуальный вес билда - 78kb (может изменяться в зависимости от версии)
Все рабочие строки обфусцированы

Одна из наших ключевых особенностей - все перечисления браузеров, веб-плагинов, кошельков берутся напрямую с вашего управляющего сервера. Вы можете редактировать в базе данных сбор необходимых браузеров, веб-плагинов и кошельков без замены билда стиллера.
Вышел новый плагин или нашли интересующий лично вас? Добавьте запись в БД и уже распространяемый билд stealc начнет его собирать!
Аналогично и с браузерами, десктоп-кошельками - вам не нужно ждать, пока мы выпустим обновление и не нужно делиться с нами интересующими вас приложениями/плагинами для сбора, вы можете добавить их

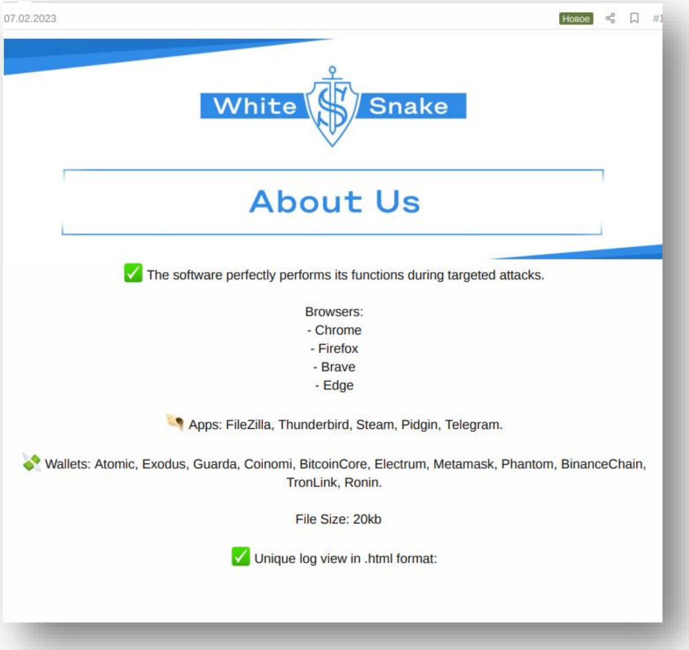
The actor ‘plymouth’ is promoting Stealc stealer on BHF

Additionally, researchers found a campaign that distributes the stealer via YouTube videos. The videos show how to install cracked software and link to a website for download. This is a typical way of infostealers delivery. Researchers discovered more than 40 Stealc samples distributed in the ecosystem, as well as thirty-five active C2 servers. Thus, the popularity of this malware seems to be on the rise.[10] Discussions on cybercrime forums reinforce this assumption: KELA has identified several actors who show a high level of satisfaction with Stealc malware and its value for money.

WhiteSnake

The infostealer was first promoted by WhiteSnake actor on February 7, 2023, on BHF. The stealer is capable of targeting both Windows and Linux (which has a smaller market share compared to Windows and, in this regard, is usually less attractive for cybercriminals), collecting sensitive information on its victims. For instance, it has the ability to steal files from various cryptocurrency wallets (Atomic, Bitcoin, Coinomi, Electrum, Exodus, and Guarda) and to gather sensitive session data from multiple applications including FileZilla, Thunderbird, Steam, Pidgin, and Telegram. The infostealer was advertised under the following pricing: 1 month (USD 140), 3 months (USD 315), 6 months (USD 580), 1 year (USD 1,100), or lifetime access (USD 1,950).

[10] Stealc: a copycat of Vidar and Raccoon infostealers gaining in popularity



About Us

✅ The software perfectly performs its functions during targeted attacks.

Browsers:
- Chrome
- Firefox
- Brave
- Edge

Apps: FileZilla, Thunderbird, Steam, Pidgin, Telegram.

Wallets: Atomic, Exodus, Guarda, Coinomi, BitcoinCore, Electrum, Metamask, Phantom, BinanceChain, TronLink, Ronin.

File Size: 20kb

✅ Unique log view in .html format:

WhiteSnake infostealer promoted on BHF

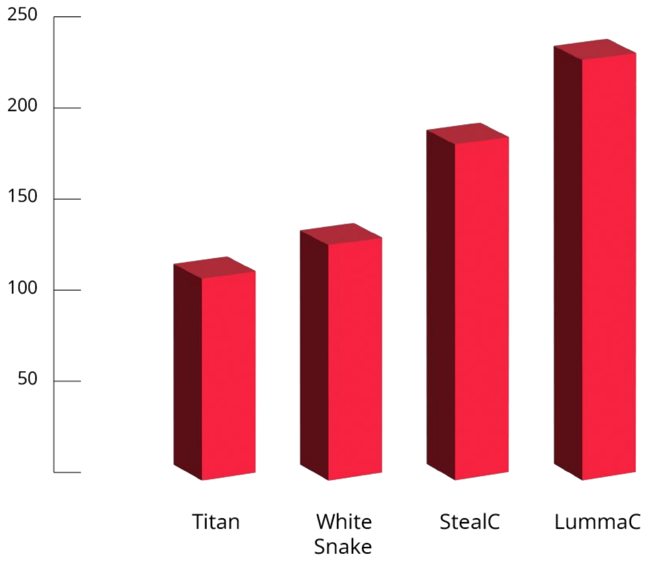
The WhiteSnake Telegram channel was created on February 3, 2023, and has more than 750 subscribers as of April 2023. The threat actor WhiteSnake is also active on another Telegram channel called Stealers Developers, where he provides updates about the stealer. Developer’s messages on this channel imply that he is willing to compete with the market’s leading player, Redline.

Costs of infostealers

The new stealers are offered at similar prices as older popular ones. The cheapest stealer is Titan which can be purchased for USD 120 per month as a monthly subscription, while the most expensive is LummaC2, which is available for USD 250 per month. WhiteSnake and StealC can be purchased for USD 140 and USD 200 respectively.

The prices are consistent with the pricing range of well-known stealers like Redline, Mars, Vidar, Meta, and Raccoon whose cost would range between USD 140 and USD 300. To attract customers, threat actors sell new infostealers for affordable prices. This tactic also contributes to the integration of the low-skilled actors into the malware market further lowering the entry barrier for them.

Monthly subscription per stealer (in USD)



Conclusion

Stealers such as Redline, Raccoon, and Vidar are renowned in the MaaS market for their stealing capabilities and are expected to preserve their popularity in 2023.

More and more threat actors offer MaaS infostealers operations in various markets and Telegram channels, with Titan, LummaC2, Stealc, and WhiteSnake gaining popularity.

In addition to Titan, LummaC2, Stealc, and WhiteSnake, we identified several other stealers that haven't received much attention from threat actors yet, but show potential to grow into strong competition. For instance, the Offx stealer was introduced on cybercrime forums in December 2022, and though its Telegram channel has fewer than 50 subscribers, logs stolen through Offx already show up on several dedicated Telegram channels featuring "clouds of logs".

Another example is Typhon, an infostealer that popped up in June 2022. And though it didn't get much attention back then, the developer released an updated version called Typhon Reborn, available for sale for USD 59 per month or USD 540 for unlimited use. Researchers observed that the new version features enhanced anti-analysis capabilities to evade detection.[11] The actor has already announced that version 3.0 will be released in June 2023.

KELA expects some new infostealers to gain more popularity over the course of the year and to be distributed through automated botnet marketplaces and Telegram channels.

[11] Typhon Reborn V2: Updated stealer features enhanced anti-analysis and evasion capabilities