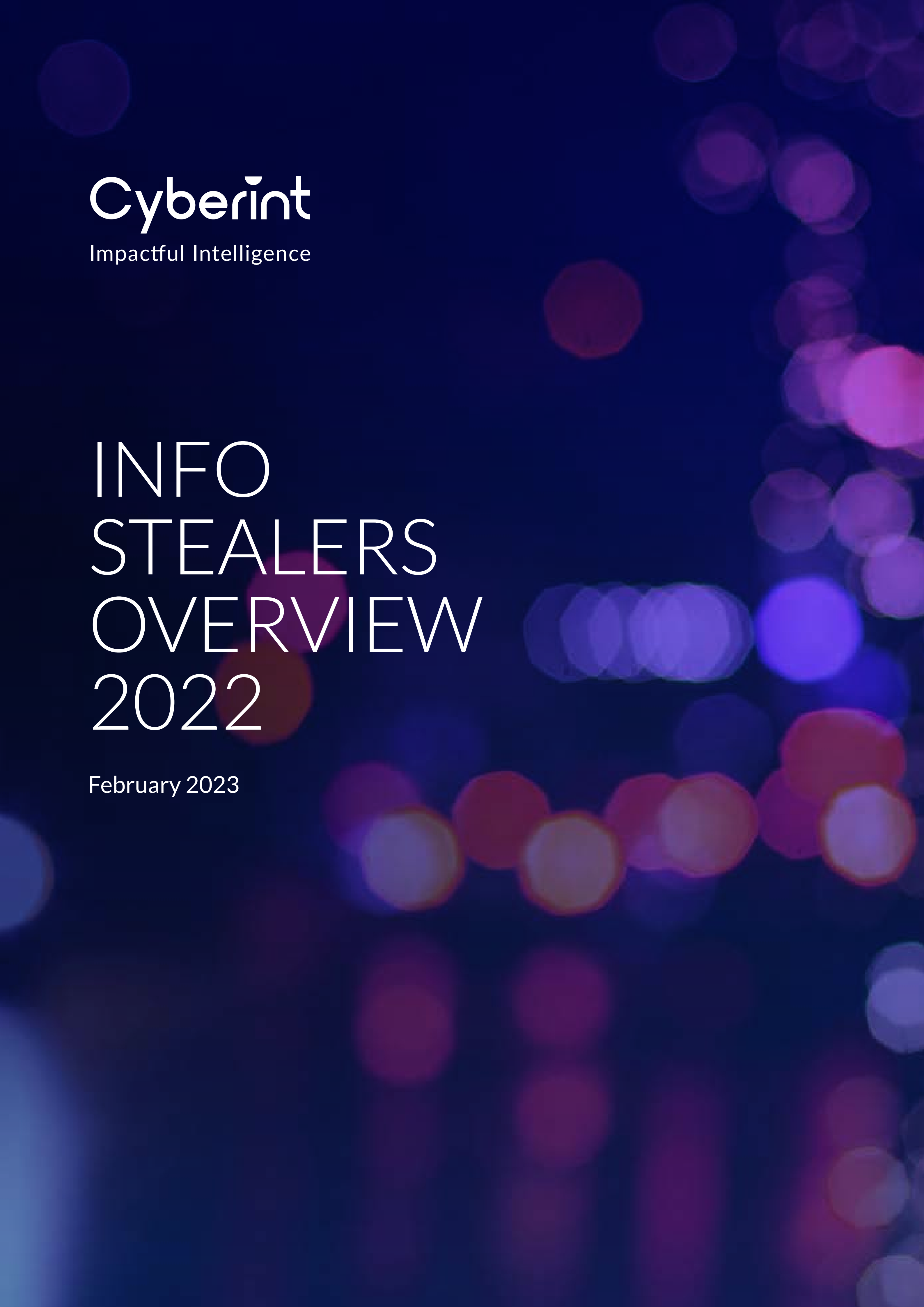


Cyberint

Impactful Intelligence

INFO STEALERS OVERVIEW 2022

February 2023

TABLE OF CONTENTS

SUMMARY

INTRO

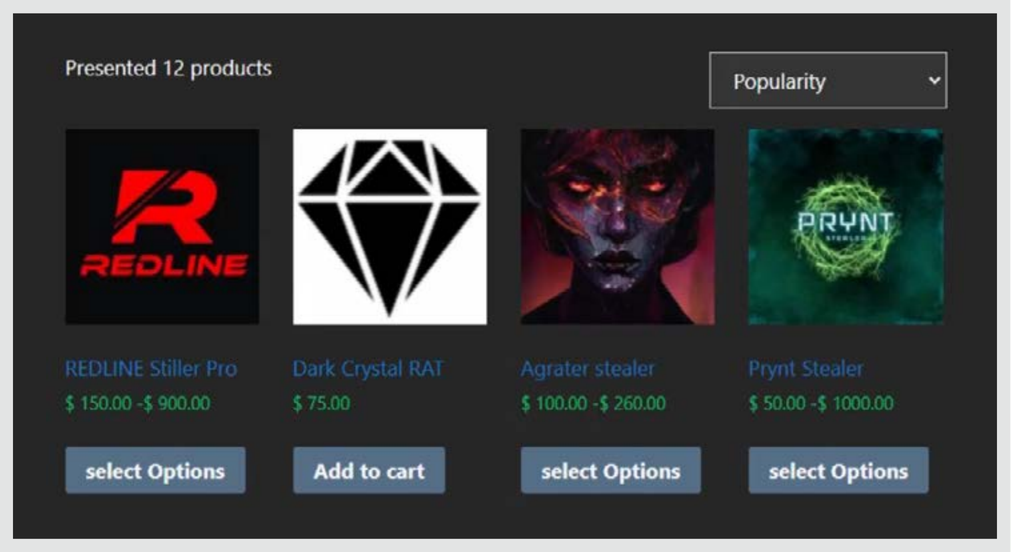
The information stealers ecosystem continues to expand as we witness the ongoing maintenance and new capabilities in the latest stealers versions. 2022 was a good year for info stealers as they keep evolving along with exploiting the popular vulnerabilities from the last years to infiltrate the targeted devices.

Looking into the dark web domain, info stealer malware has become increasingly widespread in 2022. Redline had the lion's share of the market, while Raccoon/RecordBreaker Stealer, Vidar, Meta, Cryptbot, and AZORult are some of the typical information stealers used in 2022.

During 2022 we witnessed some of the 2021 newcomers vanish from the landscape and others took their place. New business models were introduced and new detection evasion capabilities were implemented.

Figure 1 //

STEALERS OFFERED FOR SALE



Presented 12 products

Popularity

REDLINE Stiller Pro
$ 150.00 -$ 900.00

Dark Crystal RAT
$ 75.00

Agrater stealer
$ 100.00 -$ 260.00

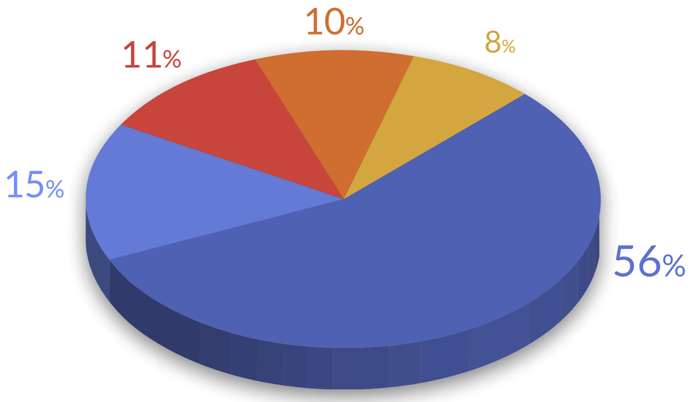
Prynt Stealer
$ 50.00 -$ 1000.00

STATISTICS

The leading information stealer is Redline with 56% of the share, second is the Raccoon Stealer with 15%, both the newcomer Meta and Vidar take the 3rd and 4th place with 11% and 10% respectively. Compared to 2021, the margin between Redline and its competitors Raccoon and Vidar widened significantly, in addition to the almost complete disappearance of notorious stealers from past years.

Figure 2 //

TOP STEALERS DISTRIBUTION IN 2022



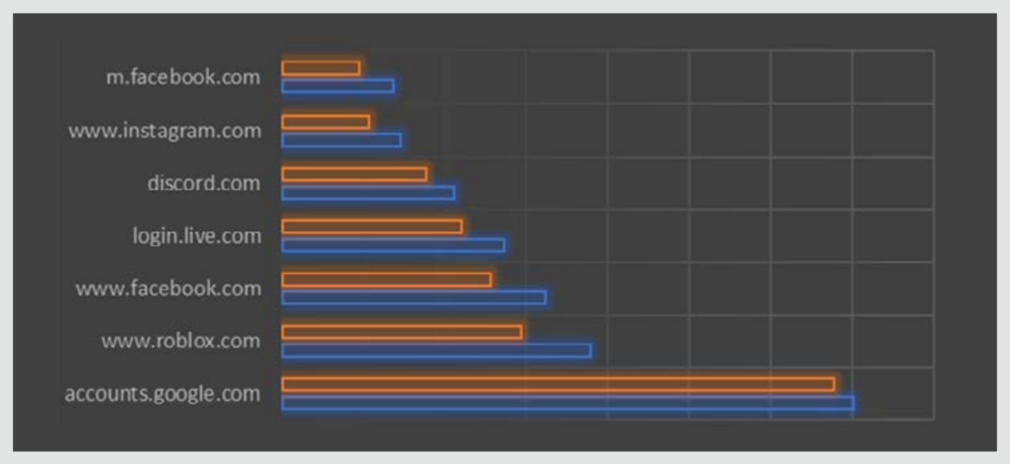
- 🟦 REDLINE
- 🟦 RACCOON
- 🟥 META
- 🟧 VIDAR
- 🟨 OTHERS

MOST AFFECTED SERVICES

The most affected stolen services are Gmail, Roblox, Facebook, Microsoft Live, and Discord. The top 5 have remained the same since 2021. The most affected sectors are gaming, file sharing, and social media interfaces

Figure 3 //

TOP COMPROMISED INTERFACES



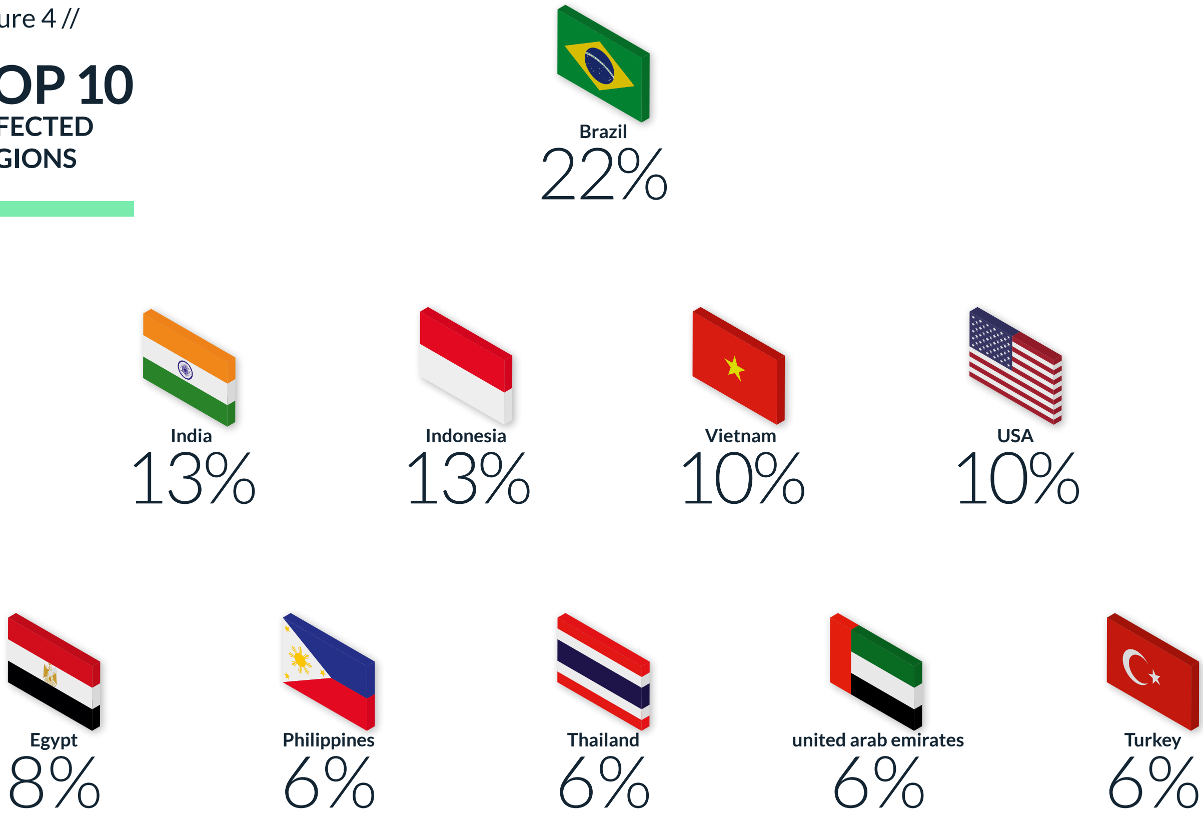
- □ 2021
- □ 2022

MOST TARGETED REGIONS

The most targeted regions are Brazil, India and Indonesia. In comparison to 2021, Brazil overtook India for first place on the chart after being 3rd in 2021. Surprisingly, the USA dropped from 2nd to 5th place and India lost 1st place and dropped into second.

Figure 4 //

TOP 10 AFFECTED REGIONS



EXECUTABLE LOCATION

Cyberint Research Team examined the locations which the stealer installs itself, most of the paths are under the .NET Framework directory while the executable file name differs.

Figure 5 //

MOST COMMON STEALER LOCATION

EXE 60%
C:\Windows\Microsoft.Net\Framework\v4.0.30319\Applaunch.exe

EXE 10%
C:\Windows\Microsoft.Net\Framework\v4.0.30319\InstallUtil.exe

EXE 9%
C:\Windows\Microsoft.Net\Framework\v4.0.30319\vbc.exe

EXE 7%
C:\Windows\Microsoft.Net\Framework\v4.0.30319\RegAsm.exe

EXE 5%
C:\Windows\Microsoft.Net\Framework\v4.0.30319\MSBuild.exe

EXE 4%
C:\Windows\Microsoft.Net\Framework\v4.0.30319\RegSvcs.exe

EXE 3%
C:\Users\97158\AppData\Roaming\Green\neofim.exe

TOP BRANDS OF INFO STEALERS

REDLINE STEALER

THE RETURN OF THE EXPLOIT KITS?

Since they targeted flaws in web browsers caused by plug-in software like the now-defunct Flash Player and Microsoft Silverlight, exploit kits (EKs) have substantially decreased in popularity. However, EKs have yet to run out of targets, as consumers still use outdated browsers, particularly Internet Explorer.

One exploit kit witnessed in 2022 is the RIG EK-dependent campaign that makes use of CVE-2021-26411, an Internet Explorer flaw that results in memory corruption when visiting a specially created webpage. This info stealer maintains its popularity among threat actors, confirmed by the number of infected machines listed on marketplaces.

DELIVERY THROUGH ONENOTE FILES

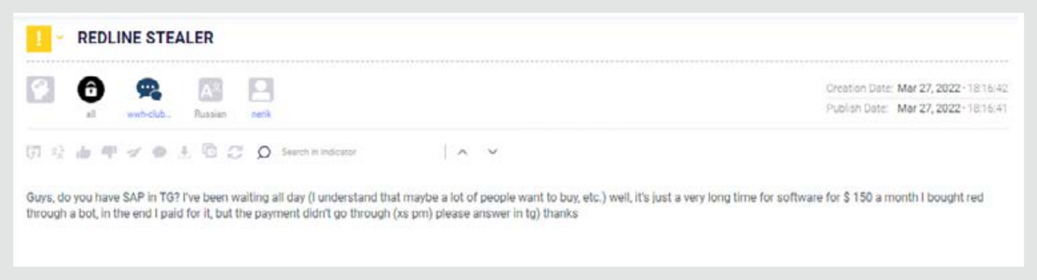
Recently, researchers shared that Redline is being delivered through phishing emails containing OneNote files containing batch scripts. Upon execution, an instance of a renamed PowerShell process is to decrypt and execute a base64 encoded binary.

CYBER GROUPS UTILIZING AND DEPLOYING THE INFO STEALER

The notorious LAPSUS$ group used the Redline stealer in at least one of their campaigns to compromise user identities. The group was seen to be deploying the malicious Redline password stealer to obtain passwords and session tokens.

Late in November, it was reported that Redline deployed a potential Cobalt Strike instance which led to a Royal Ransomware infection.

Not all shine bright in the malware services, as with the ongoing demand for the MaaS, the service was less on top of the operator's mind while complaints were received about delays in the support chat.



Creation Date: Mar 27, 2022 - 18:16:42
Publish Date: Mar 27, 2022 - 18:16:41

Guys, do you have SAP in TG? I've been waiting all day (I understand that maybe a lot of people want to buy, etc.) well, it's just a very long time for software for $ 150 a month I bought red through a bot, in the end I paid for it, but the payment didn't go through (xs pm) please answer in tg) thanks

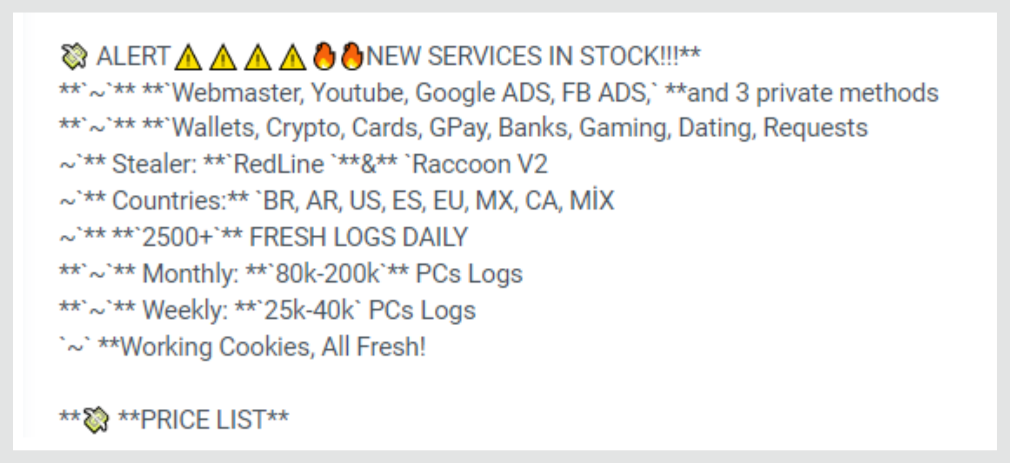
Figure 6 //

REDLINE STEALER CUSTOMER COMPLAINT IN A DARKNET FORUM

RACCOON V2/RECORDBREAKER STEALER

One of the most talked-about types of malware from 2019 through to 2022 was the Raccoon info stealer. Raccoon was an alternative to the Redline stealer. Cybercriminals offered this basic but functional info stealer as a MaaS for $200 per month, with possible additional fees for dedicated services. Numerous systems were successfully attacked by the malware. However, Raccoon's operators suspended the project due to a loss of developers during Russia's invasion of Ukraine. The operator's announced on March 25, 2022 that they would regroup in the near future and ceased to operate.

In July 2022, a statement was released, and a new version of Raccoon was made available. Raccoon Stealer V2, as a result, became well-known under the name RecordBreaker. Since the release of RecordBreaker, over 1000 samples of the malware have been witnessed in multiple AV repositories.



ALERT⚠⚠⚠⚠🔥🔥NEW SERVICES IN STOCK!!!**
`~` **`Webmaster, Youtube, Google ADS, FB ADS,` **and 3 private methods
`~` **`Wallets, Crypto, Cards, GPay, Banks, Gaming, Dating, Requests
~`** Stealer: **`RedLine `**&** `Raccoon V2
~`** Countries:** `BR, AR, US, ES, EU, MX, CA, MİX
~`** **`2500+`** FRESH LOGS DAILY
`~` Monthly: **`80k-200k`** PCs Logs
`~` Weekly: **`25k-40k` PCs Logs
`~` **Working Cookies, All Fresh!

** **PRICE LIST**

Figure 7 //

REDLINE & RACCOON STEALER OFFERED IN A DARKNET FORUM

A new malvertising operation that utilizes Google Ads to sell malware such as Raccoon Stealer and Vidar trojanized variations targets users looking for popular applications. The practice uses websites with typosquatted domain names that appear on top of Google search results as harmful adverts by tricking users into searching for particular keywords.

On November, US Department of Justice has indicted one of Raccoon's operators. If convicted, he will be sentenced to a maximum of 20 years. The FBI identified at least 50 million unique credentials stolen by the Raccoon Stealer and created a dedicated website for potential victims to check if their data has been stolen – raccoon.ic3.gov.

VIDAR STEALER

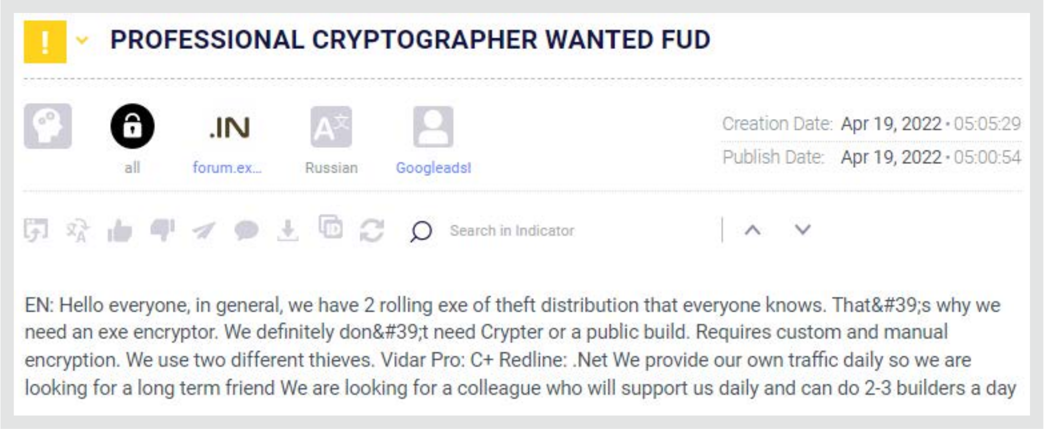
Vidar, which was initially discovered in 2018 and was likely forked from the Arkei Stealer, is capable of gathering data from affected machines. It typically relies on delivery methods like phishing emails and cracked software for dissemination.

In February 2022, researchers came across an email virus campaign as an example of the complexity attackers add to the delivery mechanism to evade detection. The new campaign sends Vidar, a dated but frequently updated info stealer. An ISO file disguised as a Doc file to lure the user into accessing is just one example of the delivery method used by the info stealers operators.

An additional significant campaign in 2022 was an attempt to spoof the official AnyDesk website over 1,300 domains, all of which point to a Dropbox folder spreading the Vidar stealer. In addition, Vidar operators have been witnessed using Mastodon, Telegram, Steam, and other well-known social media platforms as middle command-and-control (C2) servers.

Figure 8 //

THE VIDAR STEALER OPERATED BY THREAT ACTOR IN A DARKNET FORUM



PROFESSIONAL CRYPTOGRAPHER WANTED FUD

Creation Date: Apr 19, 2022 • 05:05:29
Publish Date: Apr 19, 2022 • 05:00:54

EN: Hello everyone, in general, we have 2 rolling exe of theft distribution that everyone knows. That&#39;s why we need an exe encryptor. We definitely don&#39;t need Crypter or a public build. Requires custom and manual encryption. We use two different thieves. Vidar Pro: C+ Redline: .Net We provide our own traffic daily so we are looking for a long term friend We are looking for a colleague who will support us daily and can do 2-3 builders a day

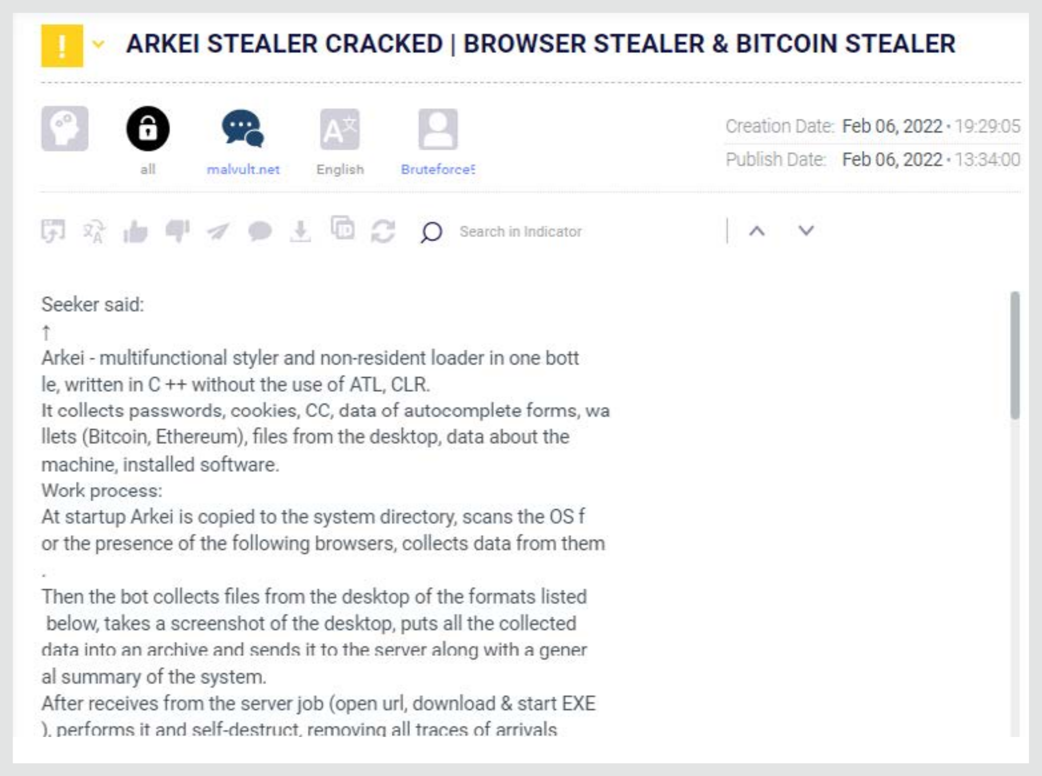
As mentioned in the Raccoon section above, Vidar also participated in a malvertising operation that utilizes Google Ads and targets users looking for popular applications.

ARKEI'S RENAISSANCE?

New versions of the information-stealing malware known as Arkei were discovered in February 2022. This stealer is primarily focused on obtaining 2FA or MFA data from its victims. SmokeLoader, also called Dofoil, a malware downloader first noticed in 2011 and used to transmit other malware via email attachments in phishing campaigns, was seen deploying Arkei.

Figure 9 //

THE ARKEI STEALER OFFERED IN A DARKNET FORUM



ARKEI STEALER CRACKED | BROWSER STEALER & BITCOIN STEALER

all
malvult.net
English
Bruteforce£
Creation Date: Feb 06, 2022 · 19:29:05
Publish Date: Feb 06, 2022 · 13:34:00
Search in Indicator

Seeker said:
↑
Arkei - multifunctional styler and non-resident loader in one bott
le, written in C ++ without the use of ATL, CLR.
It collects passwords, cookies, CC, data of autocomplete forms, wa
llets (Bitcoin, Ethereum), files from the desktop, data about the
machine, installed software.
Work process:
At startup Arkei is copied to the system directory, scans the OS f
or the presence of the following browsers, collects data from them
.
Then the bot collects files from the desktop of the formats listed
below, takes a screenshot of the desktop, puts all the collected
data into an archive and sends it to the server along with a gener
al summary of the system.
After receives from the server job (open url, download & start EXE
), performs it and self-destruct, removing all traces of arrivals

Arkei downloads a range of trustworthy components, often hosted by compromised websites, and uses them for malevolent ends. Arkei's flexibility depends on its configuration file, which is frequently hosted alongside these legal components. The malware will carry out various tasks, such as collecting saved password information, plundering auto-complete forms, and stealing saved credit card information and browser cookies, depending on what is enabled in the file.

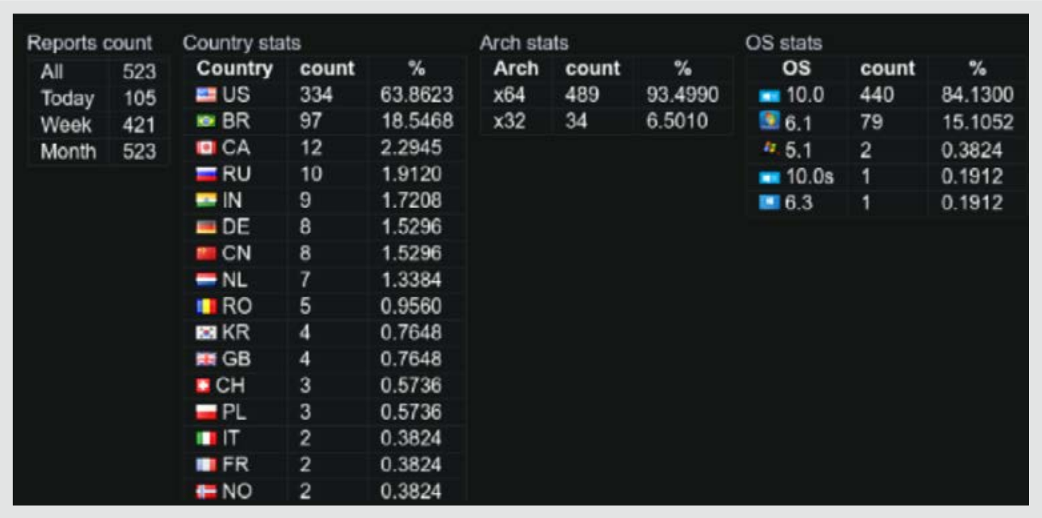
AZORULT STEALER

AZORult stealer was first discovered in 2016 and is regarded as a high-risk Trojan-type virus created to collect private data. Over time, the AZORult stealer evolved into a free, open-source program. We discovered advertising with instructions for installing the stealer in “TheJavaSea” and “Nulled” within the prominent Darknet forums.

AZORult maintains various delivery methods, including phishing emails containing deceptive text meant to lure users into opening attached files (e.g., fake job application forms delivered in MS Office format), password-protected office documents containing malicious Macros, Key-Gen based software, adware, and other malware (Ramnit, Chthonic) that delivers or drops the malware.

Figure 10 //

AZORULT’S ADMIN PANEL



Reports count

All	523
Today	105
Week	421
Month	523

Country stats

Country	count	%
US	334	63.8623
BR	97	18.5468
CA	12	2.2945
RU	10	1.9120
IN	9	1.7208
DE	8	1.5296
CN	8	1.5296
NL	7	1.3384
RO	5	0.9560
KR	4	0.7648
GB	4	0.7648
CH	3	0.5736
PL	3	0.5736
IT	2	0.3824
FR	2	0.3824
NO	2	0.3824

Arch stats

Arch	count	%
x64	489	93.4990
x32	34	6.5010

OS stats

OS	count	%
10.0	440	84.1300
6.1	79	15.1052
5.1	2	0.3824
10.0s	1	0.1912
6.3	1	0.1912

As mentioned above, AZORult makes use of the CVE-2017-11882 exploit, an RCE in Microsoft Office that starts to infect a chain and downloads the executable. Over 75 instances of AZORult have been detected in the past year.

CVES IN USE

Cyberint's latest Cyber Forecast reports multiple CVEs rising in 2022. However, information stealer developers are utilizing other vulnerabilities to infiltrate devices and it might imply their exploit change frequency:

- CVE-2021-26411 is in use by Redline, the RIG EK-dependent campaign that was recently studied makes use of CVE-2021-26411.
- CVE-2022-1096 is used by Redline. Type confusion in V8 in Google Chrome prior to 99.0.4844.84 allows a remote attacker to potentially exploit heap corruption via a crafted HTML page.
- CVE-2017-0199 is used by Redline. Remote code execution vulnerability allows attackers to exploit a flaw that exists in the Windows Object Linking and Embedding (OLE) interface of Microsoft Office to deliver malware.
- CVE-2016-0101 is in use by Raccoon/Arkei/Vidar/Mars. It allows remote attackers to execute arbitrary code via crafted media content, aka "Windows Media Parsing Remote Code Execution Vulnerability."
- CVE-2022-20813 is in use by Arkei/Vidar/Mars. Multiple vulnerabilities in the API and the web-based management interface of Cisco Expressway Series and Cisco TelePresence Video Communication Server (VCS) could allow a remote attacker to overwrite arbitrary files or conduct null byte poisoning attacks on an affected device.
- CVE-2016-2569 is in use by DarkCrystal/Raccoon. Squid 3.x before 3.5.15 and 4.x before 4.0.7 does not properly append data to String objects, which allows remote servers to cause a denial of service (assertion failure and daemon exit) via a long string, as demonstrated by a crafted HTTP Vary header.
- CVE-2016-4535 is in use by Raccoon. Integer signedness error in the AV engine before DAT 8145, as used in McAfee LiveSafe 14.0, allows remote attackers to cause a denial of service (memory corruption and crash) via a crafted packed executable.
- CVE-2017-0147 is in use by Azorult. Allows remote attackers to obtain sensitive information from process memory via crafted packets, aka "Windows SMB Information Disclosure Vulnerability."
- CVE-2017-11882 is in use by AZORult – An RCE in Microsoft Office is used to start to infection chain and download the executable.

NEWCOMERS

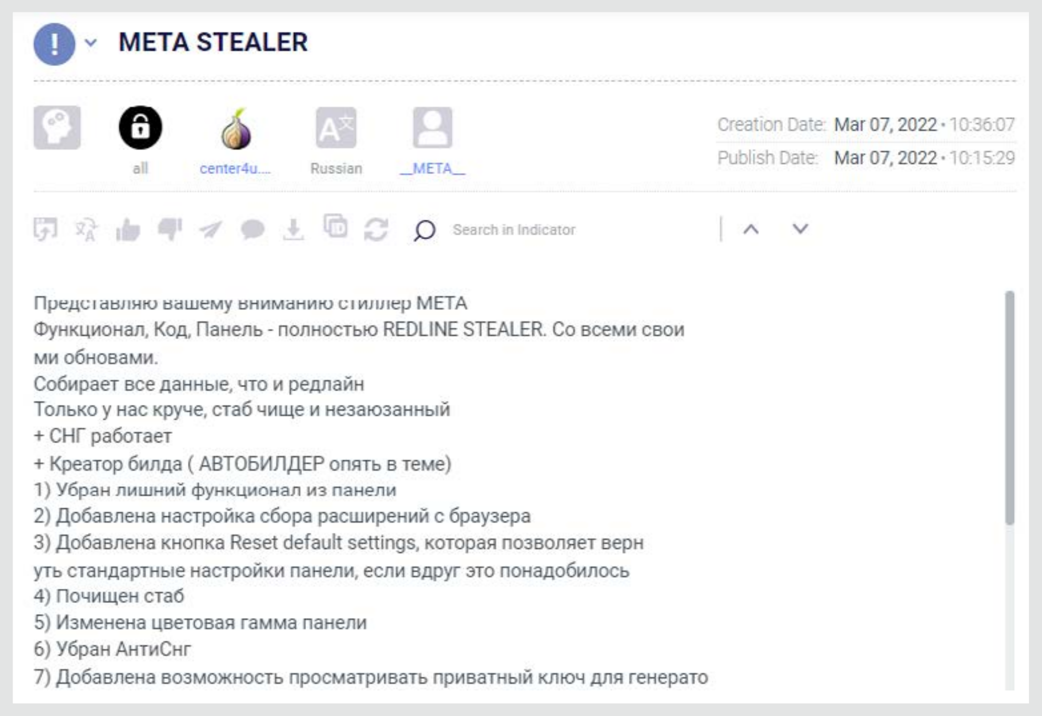
The Cyberint Research Team detected over 20 novel stealers (Appendix A) emerged in the cybercriminal community in 2022, some of which were delivered through phishing campaigns, others through dependencies and also via Google ad campaigns. The delivery methods are getting trickier and require cyber security companies to seek out help in dealing with them. Business-wise, the newcomer operators are getting better at providing business models to support various numbers of client types. 2022 saw a significant rise in the number of developed stealers. However, the newcomers still have to gain reputation before they can challenge the big-league stealers. It seems that both parties can benefit from each other as we witnessed in the Ransomware domain, where the big players make use of the new but innovative and agile groups.

META STEALER

In mid-April, after the abovementioned Raccoon stealer halted is operations, the Meta info stealer took a chance and entered the market. Meta's techniques and procedures are standard. The victim's PC is invaded, where an email with an attachment serves as the first step. For seasoned users, this has already become something to avoid, but there are still people who fall prey to this method. The bait is standard: You have been paid, but you must fill in a form before getting your money.

Figure 11 //

META STEALER SERVICES OFFERED IN A DARKNET FORUM



Creation Date: Mar 07, 2022 · 10:36:07
Publish Date: Mar 07, 2022 · 10:15:29

Представляю вашему вниманию стиллер META
Функционал, Код, Панель - полностью REDLINE STEALER. Со всеми свои
ми обновами.
Собирает все данные, что и редлайн
Только у нас круче, стаб чище и незаюзанный
+ СНГ работает
+ Креатор билда (АВТОБИЛДЕР опять в теме)
1) Убран лишний функционал из панели
2) Добавлена настройка сбора расширений с браузера
3) Добавлена кнопка Reset default settings, которая позволяет верн
уть стандартные настройки панели, если вдруг это понадобилось
4) Почищен стаб
5) Изменена цветовая гамма панели
6) Убран АнтиСнг
7) Добавлена возможность просматривать приватный ключ для генерато

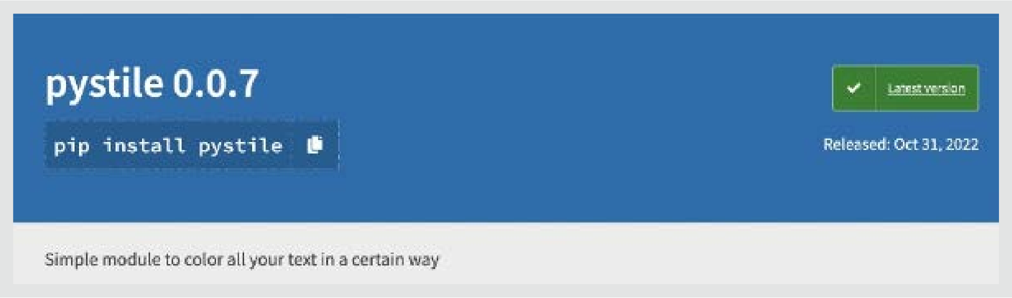
The product is marketed as an enhanced version of RedLine and is available for purchase for $125 for monthly subscribers or $1,000 for unrestricted lifetime access.

W4SP STEALER

Attackers are still trying to infect developers' systems with the W4SP Stealer Trojan, designed to steal cryptocurrency information, exfiltrate sensitive data, and gather credentials from developers' systems. They do this by creating fake Python packages and employing simple obfuscation techniques. The ongoing supply chain attack, with 29 Malicious PyPI packages, has been leveraging the packages to distribute malware called W4SP Stealer, with over hundreds of victims. What makes it notable is the use of steganography to extract a polymorphic malware payload hidden within an image file hosted on Imgur.

Figure 12 //

A COMPROMISED DEPENDENCY ON PYPI



pystile 0.0.7

```
pip install pystile
```

Released: Oct 31, 2022

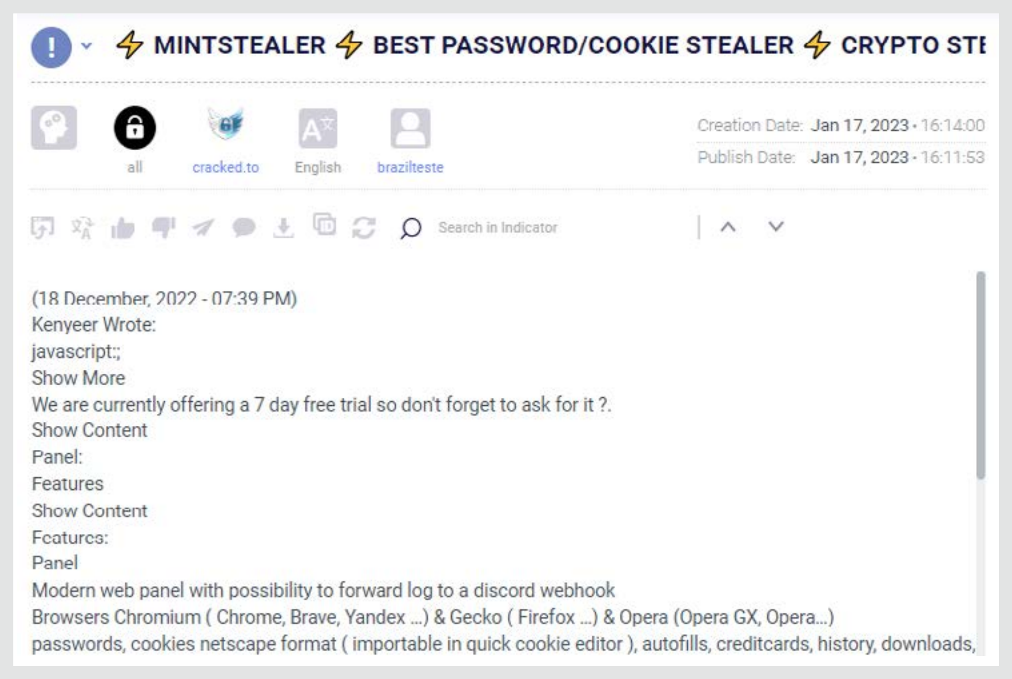
Simple module to color all your text in a certain way

MINT STEALER

Another stealer that gained traction, with capabilities to hook logs back to Discord, is the Mint Stealer. Mint Stealer preys on users of web browsers, instant messengers, mail clients, VPN clients, game sessions, and other applications. It is employed to extract private information. Malware-as-a-service vendors are marketing Mint Stealer (as MaaS) and are available to other online threat actors for $8 per week, $30 per month, and $75 for three months.

Figure 13 //

MINT STEALER PROMOTED IN A DARKNET FORUM



⚡ MINTSTEALER ⚡ BEST PASSWORD/COOKIE STEALER ⚡ CRYPTO STE

Creation Date: Jan 17, 2023 · 16:14:00
Publish Date: Jan 17, 2023 · 16:11:53

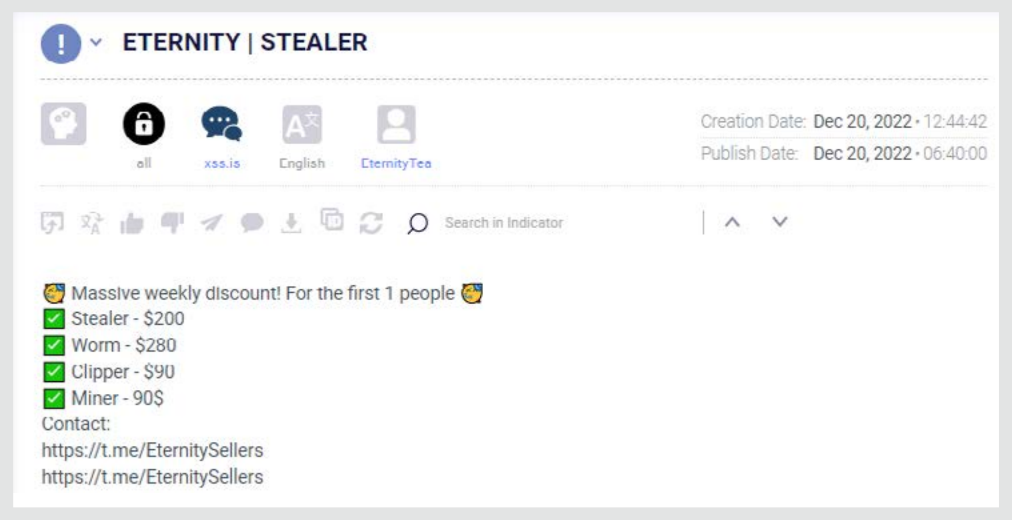
(18 December, 2022 - 07:39 PM)
Kenyeer Wrote:
javascript:;
Show More
We are currently offering a 7 day free trial so don't forget to ask for it ?.
Show Content
Panel:
Features
Show Content
Features:
Panel
Modern web panel with possibility to forward log to a discord webhook
Browsers Chromium (Chrome, Brave, Yandex ...) & Gecko (Firefox ...) & Opera (Opera GX, Opera...)
passwords, cookies netscape format (importable in quick cookie editor), autofills, creditcards, history, downloads,

ETERNITY STEALER

On March 26, 2022, EternityTeam posted an announcement about the Eternity Stealer on the XSS forum. From the compromised machines, the stealer can acquire passwords, cookies, tokens, history, bookmarks, credit card information, and information on crypto wallets. The EternityTeam frequently updates the malware and offers discounts on the services from time to time.

Figure 14 //

ETERNITY STEALER OFFERED FOR SALE IN A DARKNET FORUM



ETERNITY | STEALER

Creation Date: Dec 20, 2022 • 12:44:42
Publish Date: Dec 20, 2022 • 06:40:00

Massive weekly discount! For the first 1 people
✅ Stealer - $200
✅ Worm - $280
✅ Clipper - $90
✅ Miner - 90$
Contact:
https://t.me/EternitySellers
https://t.me/EternitySellers

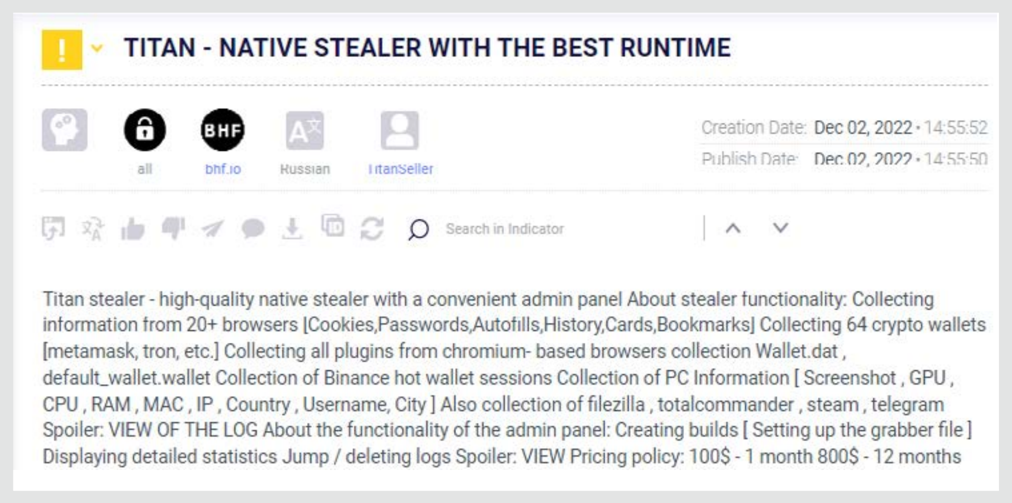
TITAN STEALER

Titan is marketed as a malware builder that enables users to alter the malware binary's functionality and the type of data that will be extracted from a victim's computer. The pricing policy ranges from $100 for one month to $800 for a year.

The stealer can take a wide range of data from infected Windows workstations, including screenshots, system information, system credentials from browsers and cryptocurrency wallets, and seized files.

Figure 15 //

TITAN STEALER ADVERTISED IN A DARKNET FORUM



TITAN - NATIVE STEALER WITH THE BEST RUNTIME

Creation Date: Dec 02, 2022 • 14:55:52
Publish Date: Dec 02, 2022 • 14:55:50

Titan stealer - high-quality native stealer with a convenient admin panel About stealer functionality: Collecting information from 20+ browsers [Cookies,Passwords,Autofills,History,Cards,Bookmarks] Collecting 64 crypto wallets [metamask, tron, etc.] Collecting all plugins from chromium- based browsers collection Wallet.dat , default_wallet.wallet Collection of Binance hot wallet sessions Collection of PC Information [Screenshot , GPU , CPU , RAM , MAC , IP , Country , Username, City] Also collection of filezilla , totalcommander , steam , telegram Spoiler: VIEW OF THE LOG About the functionality of the admin panel: Creating builds [Setting up the grabber file] Displaying detailed statistics Jump / deleting logs Spoiler: VIEW Pricing policy: 100$ - 1 month 800$ - 12 months

CONCLUSIONS

Summarizing 2022, the major info stealers such as Redline, Raccoon and Vidar are still leading the pack. It seems that the newcomers are trying to take advantage in two different vectors:

1. If one of the major info stealers halts its operations, newcomers will try to lure the abandoned seekers.
2. Newcomers will modify leaked versions of the major stealers to create an alternative to the legacy info stealers.

The Russian-Ukrainian war also affected the information stealers' domain as some halted their operations due to a lack of developers based in those countries.

In addition, info stealers are a prolific ground for dropping and deploying more sophisticated threats such as ransomware and spyware used by more prominent actors. APTs were witnessed making use of info stealers for initial access.

Due to the significant surge in 2022 newcomers alongside the current steady development of prominent stealers and AI tools, Cyberint Research Team expect to witness in 2023 various new info stealers that will try to bite the market share of the major info stealers with upgraded capabilities, evasion techniques and business models. Moreover, we predict to see even more extensive utilization, coordination and collaboration between APTs, Ransomware groups and threat actors.

APPENDIX A
NEWCOMERS CHEAT SHEET

NAME	DESCRIPTION	DETECTION	PRICE
StealC	StealC is built in C, and it is only 78Kb in size. The operators announced that they relied on popular info stealers such as Vidar, Redline and Raccoon.	Jan-23	N/A
Spectre5.0	Spectre5.0 is written in C++ and is defined as Windows modular RAT. The operators declared that the RAT is not based on other malware. The current setup consists of 3 modules/exes: Bot/loader, Stealer and Hidden Apps.	Apr-22	$300 Per Month
Rhadamanthys Stealer	Rhadamanthys is operated as Malware as a Service (MaaS) model. The stealer is written in C language to compile without dependency, the malware is compatible with xp-win11, and adaptively supports x86 & x64 architecture. The developers declare that all network communications are encrypted. Each structure has a unique encryption key.	Aug-22	$250 Per Month
Aurora Stealer	Aurora Stealer collects data from all browsers (Cookie, Password, Wallets), collecting 50+ crypto wallets (PC/WEB), File Grabber, provided with built-in Loader. Additional capability is that the Aurora Stealer Decipher the log on the server The developers declare that it is “soft native”, compiling without dependencies.	Nov-22	$125 Per month/$1000 for Lifetime
Jester Stealer	The Jester Stealer, detected in January 2022, is focused on operating in the areas of credit cards and cryptocurrency wallet theft, in addition to the common browser information, password managers, VPN clients, FTP clients, system credentials and more.	Jan-22	$150-300

NAME	DESCRIPTION	DETECTION	PRICE
BlueFox V2	After the first Bluefox version, which appeared in December 2021, the second version of the stealer is now sold as MaaS. The stealer is provided with self-destruct of the executable capability after sending a log file. The stealer does not work in CIS countries (Confederation of Independent States) and is accessed using TOR.	Sep-22	$350
Arctic Stealer	Arctic Info Stealer is a browser stealing tool that can collect passwords, cookies, history, bookmarks, and other system information from 13 browsers. It also has anti-debugging capabilities and can be used to inject malicious code into Discord processes. The origin of name probably came from the Arctic Foxes that are known for stealing food from polar bears or seabird eggs.	Aug-22	N/A
BlackNET v2	BlackNET v2 is a free, advanced, modern Windows botnet with a secure PHP panel developed using VB.NET. BlackNET is mainly available in Darknet Forums as multiple posts appeared in Nulled.to, Sinister.ly and has lately also been seen in the cracked.to forum.	Jan-22	Free
Mitsu Stealer	In July 2022, a new stealer, dubbed the Mitsu stealer, was detected. The payload is distributed via an AnyDesk Campaign. Mitsu was written in Python, which was subsequently compiled into an executable file. After successfully executing, Mitsu grabs sensitive information, dumps the Python supporting files (.pyd &.dll files), and deletes them.	July-22	N/A
Ginzo Stealer	Ginzo Stealer (also dubbed ZingoStealer) was announced on March 4, 2022. Ginzo is a new info stealer malware created by the Haskers Gang. It can steal sensitive user data such as login credentials, cryptocurrencies and deliver malicious payloads to target machines. It has been spreading widely on Telegram, and is being given away for free to other cybercriminal groups. ZingoStealer is being distributed via game cheats, cracks, and code generators. The stealer is gaining little affection from the crowd, as the credibility of the info stealer is still being determined.	Mar-22	Free

CONTACT US

www.cyberint.com | sales@cyberint.com | blog.cyberint.com

ISRAEL

Tel: +972-3-7286-777
17 Ha-Mefalsim St 4951447 Petah Tikva

UNITED KINGDOM

Tel: +44-203-514-1515
6 The Broadway, Mill Hill NW7 3LL, London

USA – TX

Tel: +1-646-568-7813
7700 Windrose Plano, TX 75024

SINGAPORE

Tel: +65-3163-5760
135 Cecil St. #10-01 MYP PLAZA 069536

USA - MA

Tel: +1-646-568-7813
22 Boston Wharf Road Boston, MA 2210

JAPAN

Tel: +81 080-6611-7759
27F, Tokyo Sankei Building, 1-7-2 Otemachi,
Chiyoda-ku, Tokyo 100-0004

ABOUT CYBERINT

Cyberint's impactful intelligence solution fuses real-time threat intelligence with bespoke attack surface management, providing organizations with extensive integrated visibility into their external risk exposure.

Leveraging autonomous discovery of all external-facing assets, coupled with open, deep & dark web intelligence, the solution allows cybersecurity teams to uncover their most relevant known and unknown digital risks - earlier.

Global customers, including Fortune 500 leaders across all major market verticals, rely on Cyberint to prevent, detect, investigate, and remediate phishing, fraud, ransomware, brand abuse, data leaks, external vulnerabilities, and more, ensuring continuous external protection from cyber threats.