



Infostealers : investiguer la menace cybercriminelle dans son écosystème

Quentin BOURGUE
Pierre LE BOURHIS
Livia TIBIRNA

Qui
sommes-
nous ?

**Threat & Detection Research (TDR),
Sekoia.io**



Quentin BOURGUE

Analyste CTI

quentin.bourgue@sekoia.io



Pierre LE BOURHIS

Analyste CTI

pierre.le-bourhis@sekoia.io



Livia TIBIRNA

Analyste CTI

livia.tibirna@sekoia.io

Plan de la présentation

- 1 Introduction : définitions, contexte et impact
- 2 Écosystème russophone autour des *infostealers*
- 3 Investigations et résultats d'analyse
- 4 Conclusion : tendances et éléments-clés

Introduction : définitions, contexte et impact

Infostealers



Les *infostealers* sont des logiciels malveillants conçus pour collecter des données sensibles sur les appareils infectés et les exfiltrer vers l'infrastructure contrôlée par l'attaquant.

Informations collectées :

- des navigateurs web (*cookies*, authentifications, bancaires, extensions)
- des applications installées
- portefeuilles de cryptoactifs
- fichiers et documents d'intérêt
- emails
- etc.

```
*****
*
*
* [REDACTED] *
* [REDACTED] *
* [REDACTED] *
* [REDACTED] *
* [REDACTED] *
*
* Telegram: https://t.me/redline_market_bot *
*****

URL: https://play.hbomax.com/page/urn:hbo:page:home
Username: cfuentes428@gmail.com
Password: [REDACTED]
Application: Google_[Chrome]_Default
=====
URL: https://login.live.com/login.srf
Username: nca8285@gmail.com
Password: [REDACTED]
Application: Google_[Chrome]_Default
=====
URL: https://www.roblox.com/login
Username: Shinzo_666
Password: [REDACTED]
Application: Google_[Chrome]_Default
=====
```

MacBook Pro

Acteurs, objectifs et impacts

- **Cybercriminalité : motivation financière**
- **APT : menace persistante avancée**

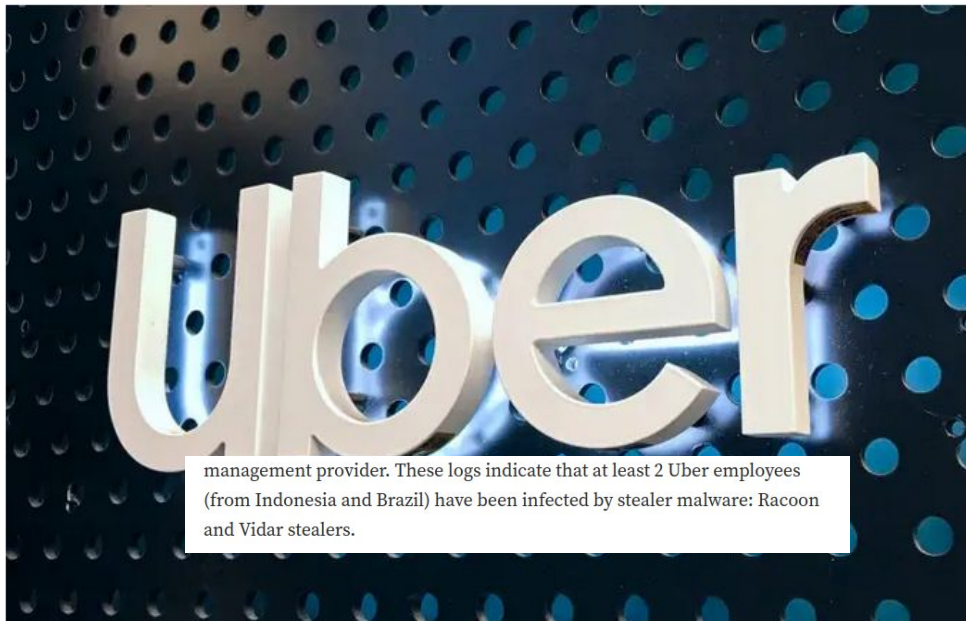


Group-IB

Sep 19, 2022 · 3 min read · Listen



What Group-IB found about the Uber Hack



management provider. These logs indicate that at least 2 Uber employees (from Indonesia and Brazil) have been infected by stealer malware: Racoon and Vidar stealers.



NFT God
@NFT_GOD

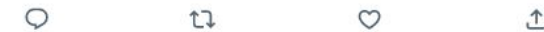
Last night my entire digital livelihood was violated.

Every account connected to me both personally and professionally was hacked and used to hurt others.

Less importantly, I lost a life changing amount of my net worth

2:59 AM · Jan 15, 2023 · 2.9M Views

1,534 Retweets 836 Quote Tweets 7,542 Likes



NFT God · Jan 15

Replying to @NFT_GOD

Every channel I have with my community, friends, and family was compromised over the last 24 hours

My Twitter, Substack, Gmail, Discord, and wallets were all invaded and taken over by bad actors

Significantly less important than all of that I lost all of my digital assets

20 44 819 231.4K



NFT God · Jan 15

Yesterday afternoon I went to download OBS onto my personal desktop computer.

OBS is industry standard video streaming software. I was excited to live stream some video games for the first time in my life.

What I didn't realize was I clicked the sponsored link on google

81 273 1,054 744.3K

Écosystème cybercriminel russophone autour des infostealers



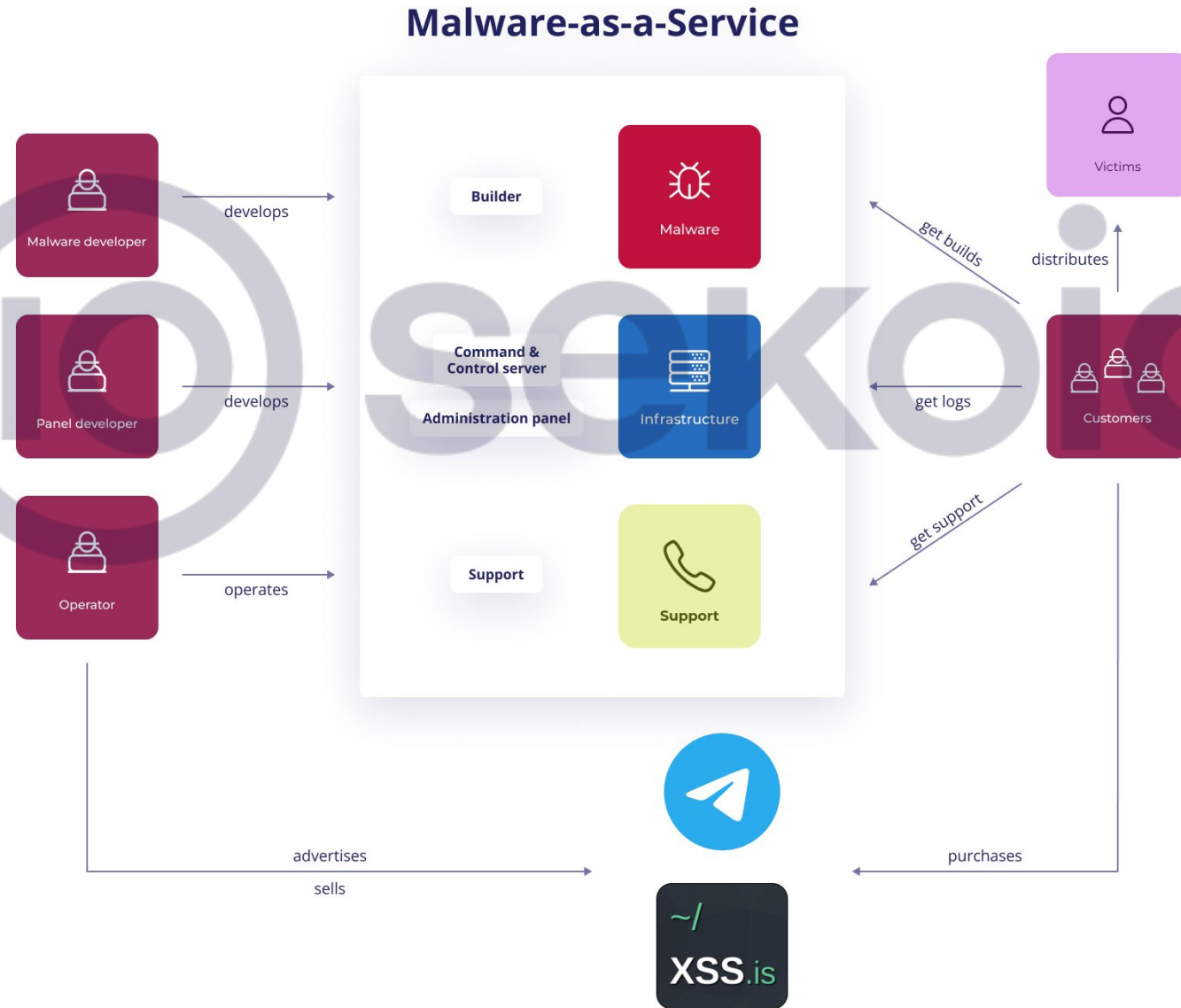
Un écosystème caractérisé par :

- la **structuration** des différentes activités
- des **services** pour chaque activité
- la **mise en commun** des ressources et des connaissances
- une barrière d'entrée très **accessible**
- des **places de marchés spécialisées**

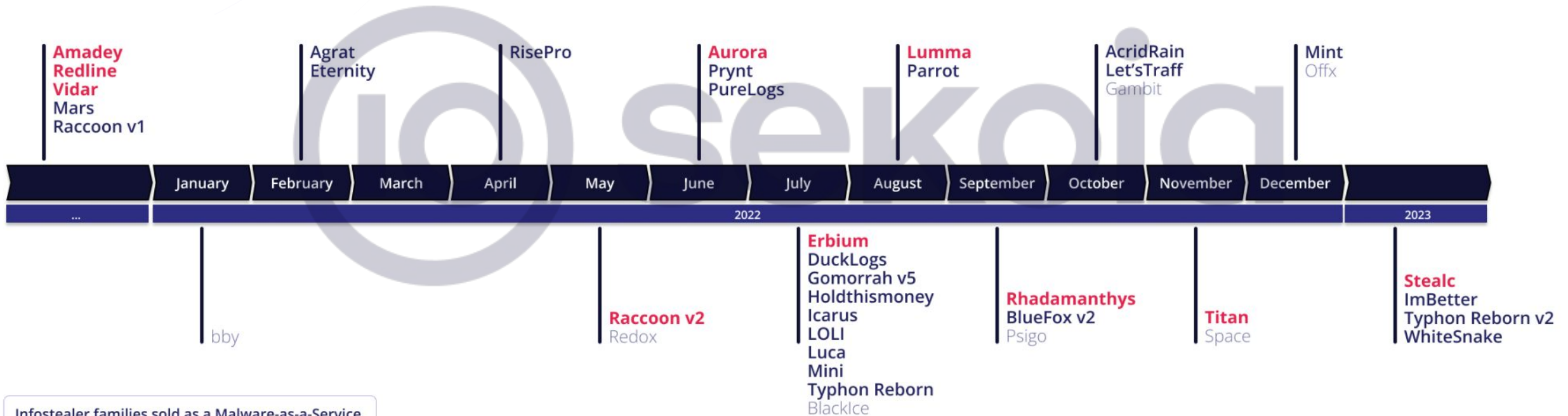
Écosystème russophone autour des infostealers



Malware-as-a-Service : un modèle clé en main




Malware-as-a-Service : liste des infostealers en vente sur le marché



Infostealer families sold as a Malware-as-a-Service, which SEKOIA.IO observed to be:

- The most distributed in early 2023
- Distributed in the wild
- Not distributed in the wild

Malware-as-a-Service : exemple de mise en vente



MarsTeam
RAID-массив
Пользователь

Регистрация: 21.05.2021
Сообщения: 67
Реакции: 36
Гарант сделки: 1
Депозит: 0.009 ₪

22.06.2021

🔊 📄 #1

Mars Stealer — нативный, нерезидентный стиллер с функционалом лоадера и грабера

Наш софт разрабатывался с учетом пожеланий людей, работающих по крипте, поэтому в Mars вы можете найти всё необходимое для работы с криптовалютой и не только.

ВНИМАНИЕ! МЫ НЕ РАБОТАЕМ ПО СНГ И ВАМ НЕ СОВЕТУЕМ!

Mars написан на **ASM/C WinAPI**, весит всего 95kb (упакованный в UPX 40kb), использует техники для скрытия запросов к WinAPI, шифрует используемые строки, собирает весь лог в памяти, а так же поддерживает защищенное SSL-соединение с командным сервером.
Не используются crt, std.

Список поддерживаемых браузеров:
Internet Explorer, Microsoft Edge
Google Chrome, Chromium, Microsoft Edge (Chromium version), Kometa, Arnigo, Torch, Orbitum, Comodo Dragon, Nichrome, Maxthon5, Maxthon6, Sputnik Browser, Epic Privacy Browser, Vivaldi, CocCoc, Uran Browser, QIP Surf, Cent Browser, Elements Browser, TorBro Browser, CryptoTab Browser, Brave Browser, Opera Stable, Opera GX, Opera Neon.
Firefox, SlimBrowser, PaleMoon, Waterfox, Cyberfox, BlackHawk, IceCat, KMeleon, Thunderbird.

Собирает [пароли](#), [куки](#), [сс](#), [автозаполнение](#), [историю посещений сайтов](#), [историю скачивания файлов](#).
Поддерживаются все последние обновления браузеров, включая Chrome v80.

Важным функционалом, выделяющим нас на фоне конкурентов является сбор плагинов браузеров с упором на [плагины-криптокошельки](#) и [2FA-плагины](#).

Список поддерживаемых крипто-плагинов:
TronLink, MetaMask, Binance Chain Wallet, Yoroi, Nifty Wallet, Math Wallet, Coinbase Wallet, Guarda, EQUAL Wallet, Jaxx Liberty, BitAppWallet, iWallet, Wombat, MEW CX, Guild Wallet, Saturn Wallet, Ronin Wallet, NeoLine, Clover Wallet, Liquality Wallet, Terra Station, Keplr, Sollet, Auro Wallet, Polymesh Wallet, ICONex, Nabox Wallet, KHC, Temple, TezBox, Cyano Wallet, Byone, OneKey, Leaf Wallet, DAppPlay, BitClip, Steem Keychain, Nash Extension, Hycon Lite Client, ZilPay, Coin98 Wallet.

Список 2FA-плагинов:
Authenticator, Authy, EOS Authenticator, GAuth Authenticator, Trezor Password Manager.

Список поддерживаемых крипто-кошельков:
Bitcoin Core и все производные (Dogecoin, Zcash, DashCore, Litecoin), и так далее), Ethereum, Electrum, Electrum LTC, Exodus, Electron Cash, MultiDoge, JAXX, Atomic, Binance, Coinomi.

Софт собирает [цифровой отпечаток компьютера](#):

Source : XXS forum

AURORA STEALER | BOTNET

❤️ Pre-order is open ❤️

Why do you need to pre-order?

- 1) You will get LifeTime Aurora Botnet and LifeTime Aurora Stealer
- 2) You will get all kinds of modules for free and forever
- 3) You will get one of the first access to beta testing of the product

The official release of the first version is scheduled for February 1, and you will be able to get the product in the coming days!

Price: \$1000

Modules:

- 1) Loader | X64,X32 - Run, Run Memory
- 2) Proxy | Reverse - works without ports
- 3) VNC/RDP/RDP/VNC - works without ports
- 4) DDOS | L4,L7,Bypass
- 5) SiteScanner | NMAP,Scanner - for finding vulnerabilities and hacking
- 6) Port | Working with ports - it is easy to make tunnels and reverse ports, the possibility of a mass scanner
- 7) Brute | Metamask, RDP, SSH, FTP
- 8) The ability to raise web servers on bots
- 9) PowerShell,CMD | Work without ports
- 10) SFTP file manager | Work without ports

📧 @aurora_botnet_support
👁️ 10.5K 22:09

Source : chechire666_aurora Telegram channel

3 года+ | Быстрый холд
Опыта в данной сфере | 24 часа

Лучшая трафф тима Brazzers Logs

Мы как Джонни Синс, только в мире логов

Написать ►► @BrazzersLogs_bot

BRAZZERS LOGS

Наши преимущества

Опыт

3 года+

В сфере

Цена

70 рублей

За лог

Быстрый

24 часа

Холд

Racson stealer

5.0
рейтинг



Raccoon, также известный как «Mohazo» или «Rasealer», по своей сути является простым средством для кражи информации. Стиллер Raccoon написан на языке программирования C++ и работает как в 32-битных, так и в 64-битных операционных системах.

Aurora stealer

5.0
рейтинг

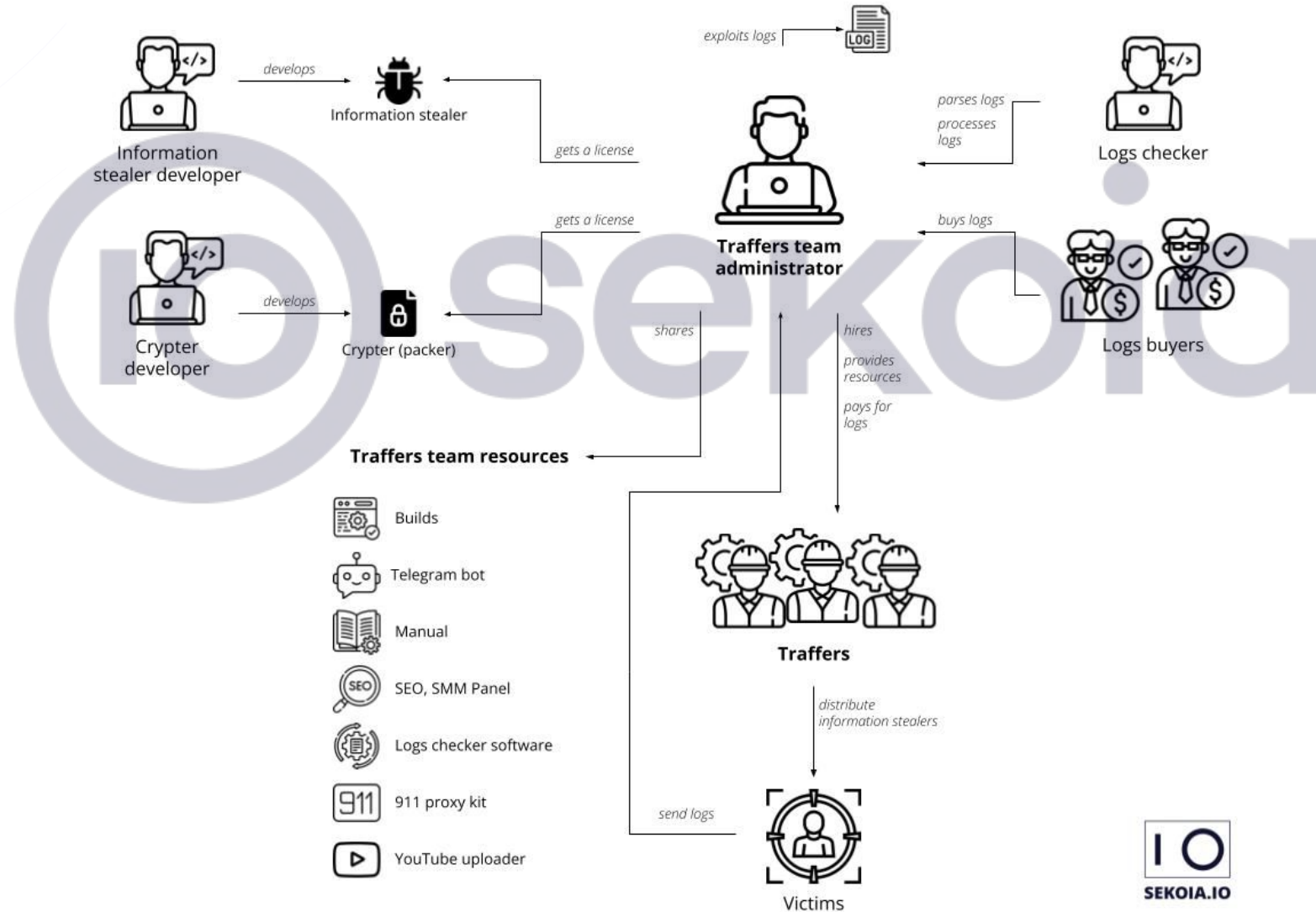


Данный стиллер позволит вам собирать данные со всех браузеров (Cookie, Password, Wallets), имеет Мощный File Grabber, Панель на вашем сервере, Встроенный Loader (Download, PowerShell). Нет зависимостей, софт нативный, а также мощная база, протокол связи TCP.



Les **traffers** (du russe *траффер*) sont des acteurs de la menace en charge de **rediriger du trafic** vers des contenus malveillants.

Structure et interactions propres à une équipe de traffers



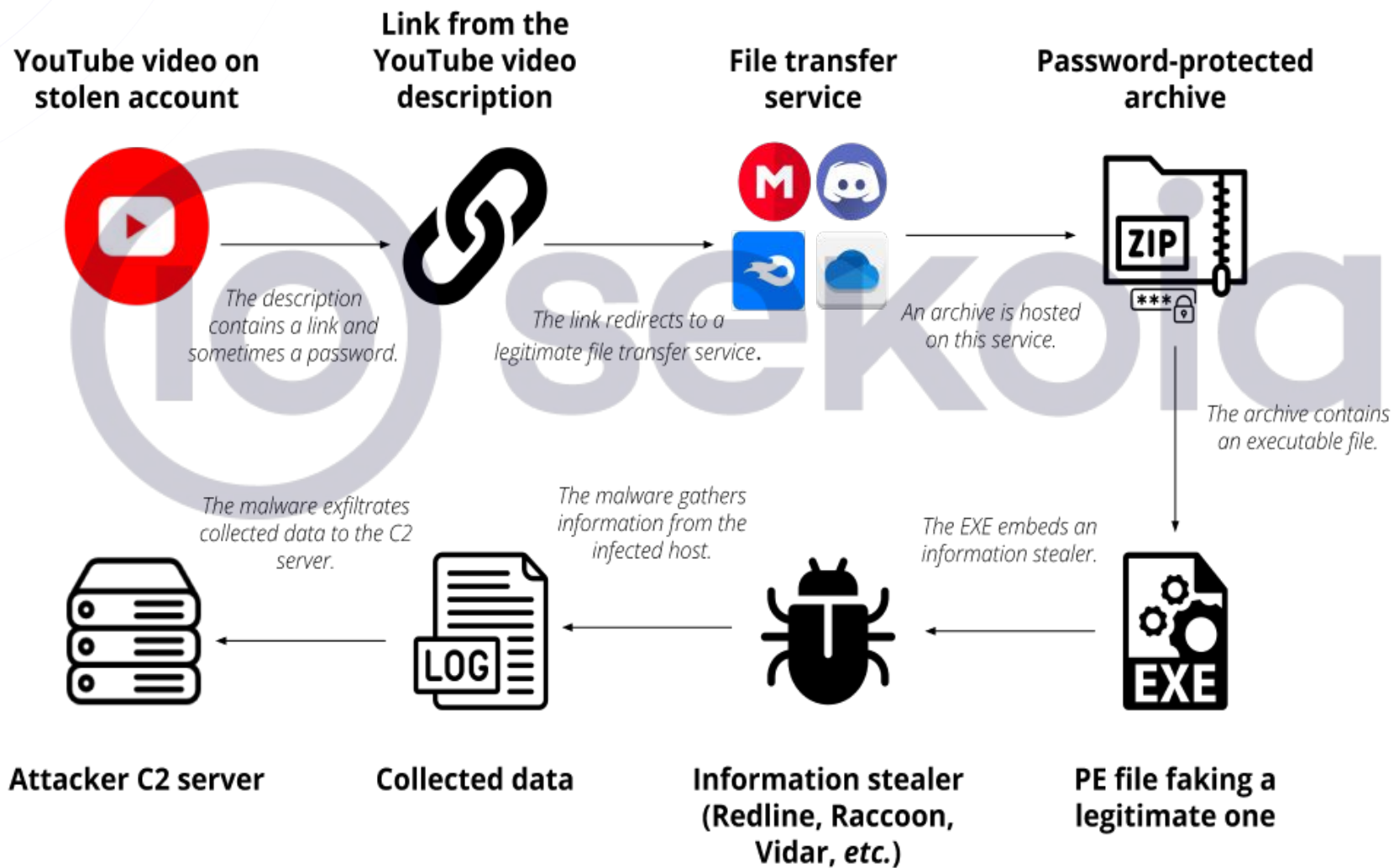
Méthodes de distributions



Canaux de distribution et techniques de social engineering ciblant le grand public :

- *malspam*
- *malvertising (Ads + landing pages)*
- *phishing* sur les réseaux sociaux
- logiciels crackés
- fausses mises à jour
- documents liés aux affaires

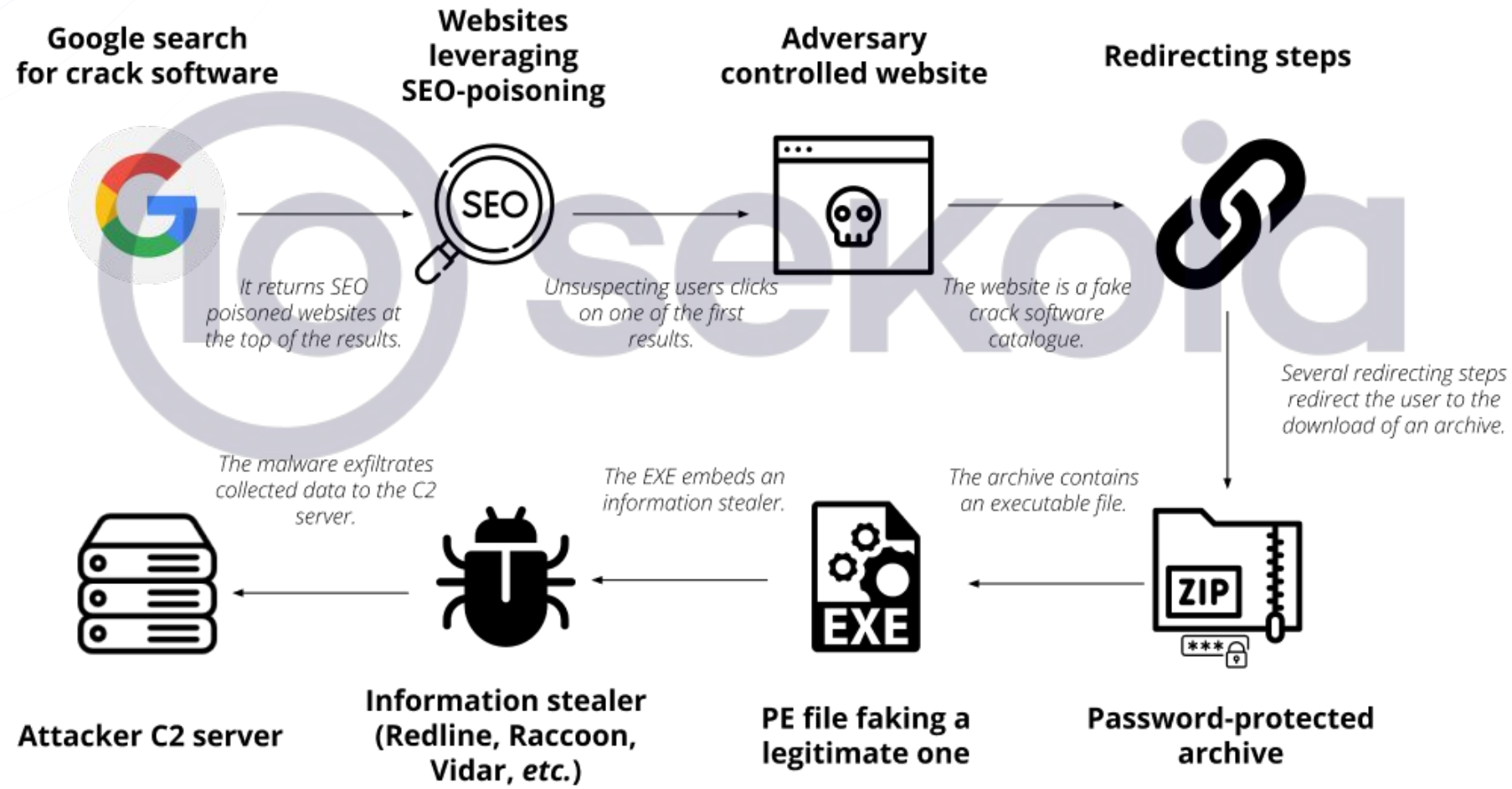
Chaîne d'infection "911"



Exemple : sur YouTube, cherchez "free download crack photoshop" et observez les descriptions des vidéos récentes

Chaîne d'infection

“empoisonnement par SEO + faux logiciel cracké”



Exemple : sur Google, cherchez “download crack software” et observez les premiers résultats.

Chaîne d'infection "malvertising"

Google search results for "zoom download".

Search query: zoom download

Results:

- Ad** · https://fr.seekblend.com/look_no_more/quality_info

Download Zoom - Best Virtual Meeting Platforms

Search for best virtual meeting platformss. Relevant Results. All the Info You Need. Visit & Lookup Immediate Results Now.
- Ad** · <https://www.zoomdowndesktop.store/>

Choose the best conference app - Zoom as a high level indicator

This app will help you create a conference
- Ad** · <https://www.info.com/>

Download Free Zoom Meeting - Download Free Zoom Meeting

Find **Download** Free **Zoom** Meeting. Examine Now. Info.Com Results. Variety of Reliable Info. Trusted Sources. Types: Variety of Reliable Info, Trusted Sources, Info.Com Results.
- <https://zoom.us> > support > download

Download Center - Zoom

Download Zoom. Download from Google Play · Download from Zoom.

<https://support.zoom.us> > en-us > articles > 441529417...

Downloading the Zoom desktop client and mobile app

Nov 3, 2022 — You can **download** the **Zoom** desktop client for macOS, Windows, Linux, and Chrome PWA, as well as the **Zoom** mobile app for iOS and Android, ...

zoom

Download Center

Download for IT Admin

Zoom Client for Meetings

The web browser client will download automatically when you start or join your first Zoom meeting, and is also available for manual download here.

[Download](#) Version 5.10.1 (4420)

[Download 64-bit Client](#) [Download ARM Client](#)

Zoom Plugin for Microsoft Outlook

The Zoom Plugin for Outlook installs a button on the Microsoft Outlook tool bar to enable you to start or schedule a meeting with one-click.

[Download](#) Version 5.10.0.301

[Add Zoom as an Add-in for Outlook on the web](#)

Zoom Plugin for IBM Notes

The Zoom Plugin for IBM Notes installs a button on the IBM Notes meeting schedule window to enable you to schedule a meeting with one click.

[Download](#) Version 5.10.0.306

Services tiers associés à la distribution d'infostealers

Лэнды для пролива
191 subscribers

December 9, 2022
Channel created

Лэнды для пролива

Заказать ленд для пролива
Готовый (по шаблону) - 10-15\$
Создание с нуля - 20-40\$
Лендинг под ключ - 35-50\$ (+ хостинг и домен)

Дополнительные услуги:
Украсть готовый лендинг - от 25\$
Установка на хостинг - 10\$

Оплатить можно с помощью:
LOLZ | BTC | ETH | USDT TRC-20

Ваш заказ будет выполнен в течение 2-8 часов

Заказать - @nightiks

1.2K edited 22:53

Лэнды для пролива pinned «
Заказать ленд для пролива Гот...»

Лэнды для пролива

CELEWA

With this App, PREMIUM PROGRAMS ARE FREE FOR YOU

Popular Applications

Ae
Ai
Lr

Цена - 10\$

В цену входит:
- Смена названия & логотипа
- Редактирование содержимого

Покупка - @nightiks

1.3K edited 22:55

Лэнды для пролива
191 subscribers

Pinned message

Заказать ленд для пролива Готовый (по шаблону) - 10-15\$ Создание

Лэнды для пролива

zoom

Products, Solutions, Resources, Plans & Pricing

One platform to innovate

Bring teams together: reimagine workflows, engage new audiences, and delight your customers – all on the Zoom platform you know and love.

Flexible solutions for modern team collaboration

Zoom One, Zoom Spaces, Zoom Events, Zoom Contact Center, Zoom Developer

Trusted by businesses, loved by people

Ready to get started?

Новый выполненный заказ

Стоимость - 30\$
Срок выполнения - 2 часа

Для заказа - @nightiks

153 19:45

Mise en vente de logs collectés

A screenshot of a forum listing various log collections for sale. The items listed are:

- 421 stealer logs (logs_admin started an hour ago) - Free data, Stealer logs
- 796 stealer logs (logs_admin started 5 hours ago) - Free data, Stealer logs
- 93k Hong Kong Combolist (Administrator started a day ago) - Free data, Combolists
- 1354 stealer logs (logs_admin started a day ago) - Free data, Stealer logs

A screenshot of a forum thread titled "Stealer Logs". The thread is part of a series of 21 pages. The thread is titled "Free Stealer logs | 2000 JANUARY 2023 - part45" by user NP402, posted yesterday at 04:21 PM. Other threads in the list include:

- #1 Paid RAT Logs - 9,449,841 Lines - +400 Listings for Target Sites (Pages: 1 2 3 4) by Demonologist, January 28, 2023, 05:46 AM
- 5x Reline Stealer Logs Private by dece12121212, 2 hours ago
- Cookies [242 Netflix, 161 Steam, 293 Yahoo] by HMU420, 7 hours ago

Moon Chat | Ru&Eng
771 members

Pinned message #2611
Curry Cloud FREE LOGS.rar

A screenshot of a Telegram chat channel named "Moon Cloud | Free Logs". The channel contains several pinned messages, each offering a zip file of logs for free. The messages are:

- Logs by @prdscloud 1461449785.zip (147.9 MB) - Password: [redacted]
- Logs by @prdscloud 2583780216.zip (51.2 MB) - Password: [redacted]
- Logs by @prdscloud 2871378693.zip (165.6 MB) - Password: [redacted]
- Logs by @prdscloud 2983018111.zip (97.7 MB) - Password: [redacted]
- Logs by @prdscloud 5943114326.zip (40.3 MB) - Password: [redacted]

Sources : SQLi Cloud, BreachedForum, Telegram



Mise en vente de *logs* collectés : plateformes centralisées

<p>C22A5B10D4C2A30906204DCE00AF12FF</p> <p>📅 2023-03-15 17:11:09 📅 2023-03-15 19:41:07</p>	<p></p> <p>account.battle.net eu.battle.net</p> <p>eu.account.battle.net us.battle.net</p>	<p>✉️ 0 📄 12 💎 0 = 12</p> <p>FR 2a01:e0a:a8fec50...</p> <p>17.00</p> <p>🗑️ 🗑️</p>
<p>65DC0B671AA4685B977D4896FC314D99</p> <p>📅 2023-03-15 16:26:52 📅 2023-03-15 19:41:07</p>	<p></p> <p>account.prusa3d.com accounts.thingiverse.com</p> <p>accounts.autodesk.com accounts.thingive...</p>	<p>✉️ 0 📄 35 💎 0 = 35</p> <p>FR 2a02:8428:e2c:6a01...</p> <p>8.00</p> <p>🗑️ 🗑️</p>
<p>C6F6C54A53A63D83CD51F709EE85F8F0</p> <p>📅 2023-03-15 14:27:32 📅 2023-03-15 19:41:06</p>	<p></p> <p>com.contextlogic.wish 9710981p.index-education.net</p> <p>tv.twitch.android.app</p>	<p>✉️ 0 📄 50 💎 0 = 50</p> <p>FR 78.121...</p> <p>5.00</p> <p>🗑️ 🗑️</p>
<p>74724859075A0A6281F22E55090D4A90</p> <p>📅 2023-03-15 14:26:10 📅 2023-03-15 19:41:06</p>	<p></p> <p>cellmapper.net.cellmapper</p> <p>cgeo.geocaching</p>	<p>✉️ 0 📄 215 💎 0 = 215</p> <p>FR 86.73...</p> <p>48.00</p> <p>🗑️ 🗑️</p>


Source : Genesis Market

Mise en vente de *logs* collectés : qualification des *logs*

Log Parser | Dumper | Сортёр | Парсер Логов | Profit Maker v1.5 | Max Stealer support

KijomBa · Jan 26, 2023 · crystalsorter logparser logs logsorter parser sorter

1 2 Next ▶

 **KijomBa**
RAM
Пользователь


Joined: Jan 17, 2022
Messages: 136
Reaction score: 83
Escrow deals: 2

Jan 26, 2023

Profit Maker v1.5 - новая выжимка моих скитаний по миру логов и их обработки.

- Поддерживает 18+ стиллеров
- Каждый скан - расширение функционала
- Если попадают неизвестные логи: отправляете мне -> 10 минут -> парсер поддерживает новый тип.
- Работает на ядре log_processor, в будущем ядро(библиотека) будет расширяться
- Новые типы стиллеров, выше скорость работы, выжимка всей даты, не только строк
- Формат URL:USER:PASS
- Скорость **1000+** логов/секунду (на не самом топовом ПК)
- Класный ГУЙ 😊

Стоимость **30\$**, с поддержкой на месяц **50\$** (оперативный фикс багов, расширение поддержки)
Доработки под ваши нужды, за небольшую плату.
Гарант только за.



PARANOID CHECKER

- Не убивает логи**
Сделка сканирует агентов, чтобы "пропустить" агентов из данных логов.
- Doesn't kill logs**
Doesn't kill user agents, option to "skip" user agent from log data.
- Никаких пропусков!**
Мы всегда следим за качеством процесса и ищем за него.
- No skips!**
We always monitor the quality of the checking process and we watch for it.
- Дружелюбный саппорт**
Поможем с любой проблемой, если вы всегда идёте в нашу сторону.
- Friendly support team**
We will help with any problem, give advice, we always go towards the client.
- Скорость работы**
Один из самых быстрых сканеров, пока логов за пару минут.
- Work speed**
One of the fastest scanners, a bunch of logs in a couple of minutes.
- Частые обновления**
Каждую неделю мы добавляем новые сканеры.
- Frequent updates**
Every week we add new scanners.
- Приемлемая цена**
За оптимальную цену вы получите весь функционал софта.
- Acceptable price**
For the optimal price you get all the functionality of the software.

@Checker_support



Investigations et résultats d'analyses

Méthodologie d'investigation et d'analyse



Objectifs :

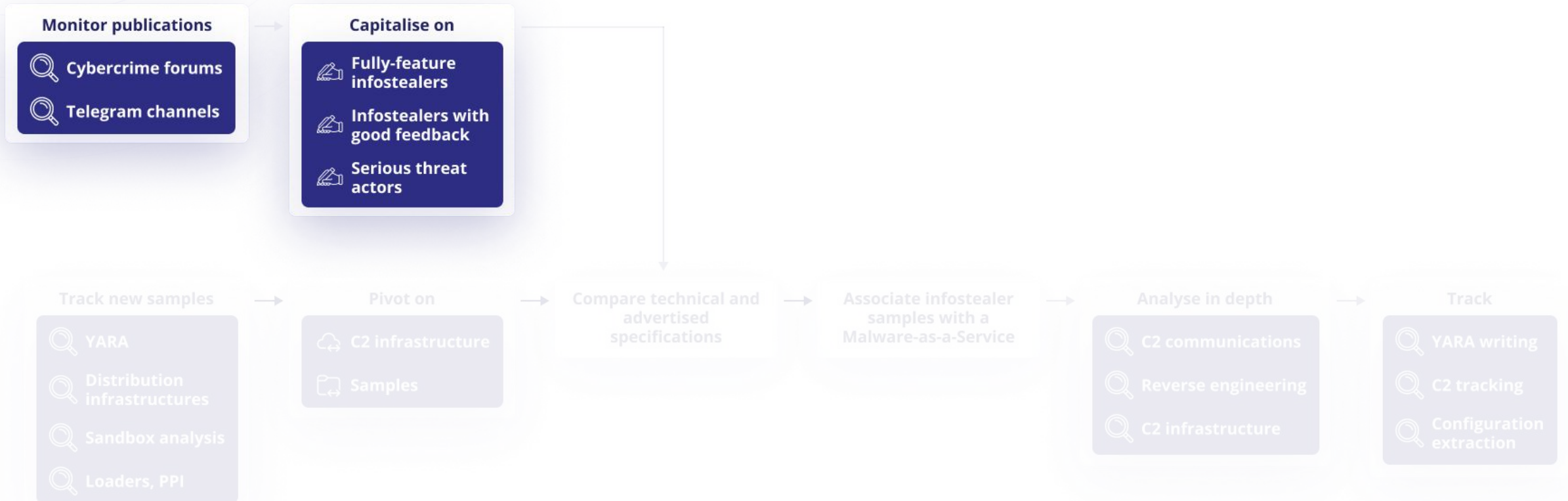
- dénicher des nouveaux infostealers émergents
- associer des samples trouvés dans la nature et des Malware-as-a-Service (contexte)
- tracker et détecter

Méthodologie d'investigation et d'analyse



Méthodologie d'investigation et d'analyse

Monitoring et capitalisation



Méthodologie d'investigation et d'analyse

Monitoring et capitalisation

Objectif : découvrir de nouvelles familles d'infostealer

- détecter des signaux faibles dans l'évolution de l'écosystème
- anticiper l'appropriation d'un infostealer par la communauté cybercriminelle
- suivre les engagements financiers des acteurs



plymouth

флорру-диск

Messages: 0 · Reaction score: 0

Dec 14, 2022 (0.02 ₿)



Phoenix1

флорру-диск

Messages: 5 · Reaction score: 0

Feb 23, 2023 (0.01 ₿)



arv6

Премиум

Messages: 77 · Escrow deals: 1

Mar 4, 2023 (0.02 ₿)



WhiteSnake

Seller

Messages: 17 · Reaction score: 4

Mar 18, 2023 (0.026 ₿)

Méthodologie d'investigation et d'analyse

Recherche proactive de nouveaux samples



Méthodologie d'investigation et d'analyse

Recherche proactive de nouveaux samples

Objectif : trouver des samples de nouveaux infostealers distribués dans la nature

- suivre les **infrastructures de distribution** d'infostealers
- écrire des **signatures YARA** de recherche
- suivre les **résultats d'analyse en *sandbox***
- suivre les ***payloads* distribués par les *loaders***

Méthodologie d'investigation et d'analyse

Recherche proactive de nouveaux samples



Suivre les infrastructures de distribution d'infostealers

SEKOIA.IO | SEKOIA

I

Intelligence >

SelfGame websites distributing commodity malware as free software

WHITE

Type Infrastructure Confidence ⓘ Created at Feb 22, 2023 Modified at Feb 22, 2023

Aliases RED0018 AllSoft websites distributing commodity malware as free software

Details Threat Context Graph exploration

Type	Name	Valid from	Valid until	Conf.	External Source
← indicates	🌐 crack-all.space	01/01/2023	16/09/2023	📍 1	SEKOIA, SEKOIA C2 Tracker
← indicates	🌐 http://crack-all.space/	01/12/2022	30/05/2023	📍 1	SEKOIA, SEKOIA C2 Tracker
← indicates	🌐 https://cracked-programs.xyz/	01/12/2022	30/05/2023	📍 1	SEKOIA, SEKOIA C2 Tracker
← indicates	🌐 cracked-programs.xyz	01/01/2023	16/09/2023	📍 1	SEKOIA, SEKOIA C2 Tracker
← indicates	🌐 http://cracked-programs.xyz/	20/03/2023	19/04/2023	📍 1	SEKOIA C2 Tracker
← indicates	🌐 jstclub.space				SEKOIA C2 Tracker
← indicates	🌐 45.87.2.44				SEKOIA, SEKOIA C2 Tracker
← indicates	🌐 allsoftclub.com				SEKOIA, SEKOIA C2 Tracker
← indicates	🌐 while-games.com				SEKOIA C2 Tracker
← indicates	🌐 www.while-games.com				SEKOIA C2 Tracker
← indicates	🌐 http://allsoftclub.com/				SEKOIA, SEKOIA C2 Tracker
← indicates	🌐 https://allsoftclub.com/				SEKOIA, SEKOIA C2 Tracker
← indicates	🌐 https://while-games.com/				SEKOIA C2 Tracker
← indicates	🌐 46.151.30.9				SEKOIA, SEKOIA C2 Tracker
← indicates	🌐 rcc-software.com				SEKOIA
← indicates	🌐 www.disasoft.org				SEKOIA

RCC-SOFTWARE
Programs & Apps
FAQ

Programs & Apps

↓

All programs
Soft
Video & Illustration & Audio
Adobe & IOBIT

Recuva Pro

Recover your deleted files quickly and easily

FREE DOWNLOAD ↓

uTorrent pro

Advanced security, no ads, HD media player, support and more

FREE DOWNLOAD ↓

FUTUREMARK PCMARK 10 BASIC EDITION

The Complete Benchmark

FREE DOWNLOAD ↓

Auslogics Driver Updater

Update drivers on your PC in one click to prevent device conflicts and ensure smooth hardware operation!

FREE DOWNLOAD ↓

Méthodologie d'investigation et d'analyse

Recherche proactive de nouveaux samples



Écrire des signatures YARA basées sur les données ciblées des :

- navigateurs web
- portefeuilles de crypto monnaies (logiciel)
- portefeuilles de crypto monnaies (extensions de navigateur)

```
strings:
  $str01 = "wallet.dat" wide ascii
  $str07 = "logins.json" wide ascii
  $str08 = "Google\\Chrome\\User Data" wide ascii
  $str09 = "BraveSoftware\\Brave-Browser\\User Data" wide ascii
  $str10 = "Chromium\\User Data" wide ascii
  $str11 = "Opera Software\\Opera " wide ascii
  $str12 = "Mozilla\\Firefox\\Profiles" wide ascii
  $str13 = "password" wide ascii nocase
  $str14 = "\\Steam" wide ascii
condition:
  uint16(0)==0x5A4D and filesize > 10KB and filesize < 500KB and
  4 of ($str*) and vt.metadata.new_file
```

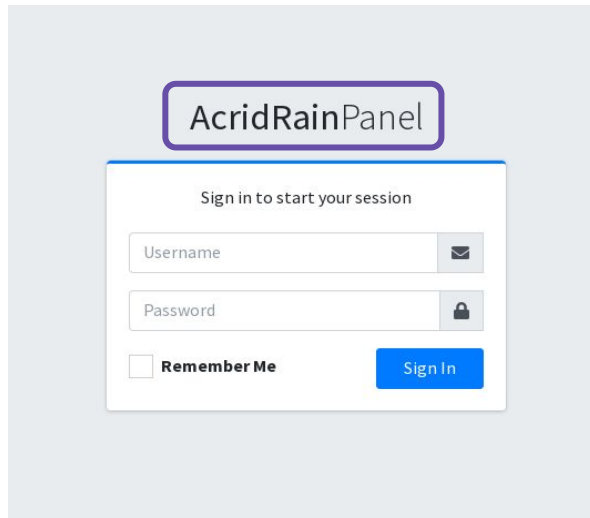
```
strings:
  $sql0 = "SELECT " wide ascii
  $sql1 = "username_value" wide ascii
  $sql2 = "password_value" wide ascii
  $sql3 = " FROM " wide ascii
  $sql4 = "logins" wide ascii
  $sql5 = "moz_cookies" wide ascii
  $sql6 = "moz_places" wide ascii
condition:
  uint16(0)==0x5A4D and filesize > 50KB and filesize < 5MB and
  4 of ($sql*) and vt.metadata.new_file
```

Méthodologie d'investigation et d'analyse

Recherche proactive de nouveaux samples



Suivre les résultats d'analyse en sandbox avec des comportements d'infostealers



Recorded Future Triage

Submit Researcher Reports

Search My Samples All Public Samples

Search Export

tagstealer AND score:7

Created	Filename	Tags	Status/Score	SHA256
20-03-2023 16:44	tmp	spyware stealer upx	7 Reported	b512788...
20-03-2023 16:41	tmp	spyware stealer upx	7 Reported	c511c5...
20-03-2023 16:38	tmp	spyware stealer	7 Reported	c15da02...
20-03-2023 16:24	Loader_Planner_SD.exe	spyware stealer	7 Reported	38afa70...
20-03-2023 16:12	Loader_Planner_SD.zip	spyware stealer	7 Reported	fcd868a...
20-03-2023 16:12	Payment_advice.rar	spyware stealer	7 Reported	be2b86b...
20-03-2023 15:54	tmp	spyware stealer	7 Reported	bce69d0...
20-03-2023 15:52	Loader_Planner_SD.zip	spyware stealer	7 Reported	fcd868a...
20-03-2023 15:52	tmp	spyware stealer	7 Reported	64b1737...
20-03-2023 15:37	Loader_Planner_SD.exe	spyware stealer	7 Reported	daca1d...
20-03-2023 15:35	Shipment_notification.exe	spyware stealer	7 Reported	90e8605...
20-03-2023 15:31	FortniteChair.exe	pyinstaller spyware stealer	7 Reported	7bb49db...
20-03-2023 15:28	ChatGPT_setup.rar	persistence spyware stealer	7 Reported	56a3ccf...
20-03-2023 15:22	230320-rj9vyadh37_pw_infect...	spyware stealer	7 Reported	5598760...

General

Target tmp.exe

Size 5MB

MD5 ba3f02e6940a29aae6458f87c3da08e

Score 7/10

spyware stealer

Signatures

Collection Credential Access

Reads user/profile data of web browsers - 2 TTPs
Infostealers often target stored browser data, which can include saved credentials etc.

spyware stealer

Suspicious behavior: EnumeratesProcesses - 2 IoCs

Processes

C:\Users\Admin\AppData\Local\Temp\tmp.exe PID:4340

"C:\Users\Admin\AppData\Local\Temp\tmp.exe"

Network

Requests TCP UDP

POST https://acridpanel.top/stealer/in tmp.exe

Méthodologie d'investigation et d'analyse

Recherche proactive de nouveaux samples



Suivre les payloads distribués par les loaders associés à des services de Pay-Per-Install

Exemple : bot de suivi des payloads distribués par le loader GCleaner



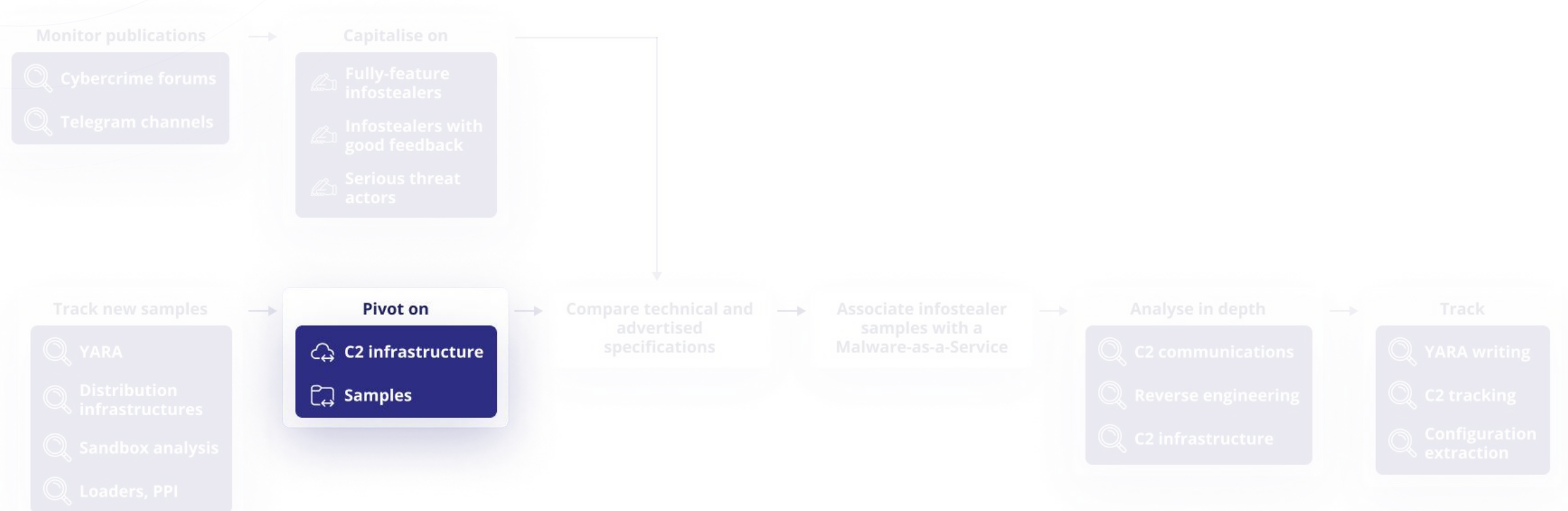
TDR - Cybercrime bot BOT 09:24

GCleaner PPI payloads tracking - 2023-03-17 09:19:42 - [hxxp://45.12.253.75/addons/_links.json](https://45.12.253.75/addons/_links.json)

GEO	Payload URLs	Triage analysis	Malware Family	Score	Tags
D1	hxxp://rymcsa03.top/download.php?file=file.exe	https://private.tria.ge/230317-j78c1sdpne	cryptbot	10	family:cryptbot discovery evasion spyware stealer themida trojan
D2	hxxp://v1678610.hosted-by-vdsina.ru/babaiko.php?filename=FileInstall.exe	https://private.tria.ge/230317-j78c1sgrf6	laplas redline	10	family:laplas family:redline botnet:fm clipper easycrypt infostealer infostealer_generic stealer
D3	hxxp://rymcsa03.top/download.php?file=file.exe	https://private.tria.ge/230317-j78nsafnrx	cryptbot	10	family:cryptbot discovery evasion spyware stealer themida trojan
D4	hxxp://v1678610.hosted-by-vdsina.ru/babaiko.php?filename=FileInstall.exe	https://private.tria.ge/230317-j78nsamvvl	redline laplas	10	family:laplas family:redline botnet:fm clipper easycrypt infostealer infostealer_generic stealer
EU	hxxp://qdm57.shop/f/fz0311356e.exe	https://private.tria.ge/230317-j78zjsfnry		1	
US	hxxp://qdm57.shop/f/fz0312351u.exe	https://private.tria.ge/230317-j78zjsfnrz		1	
MIXTWO	hxxp://getgoodsb.link/notepadp.exe	https://private.tria.ge/230317-j79abadpnf	stealc	10	family:stealc discovery spyware stealer
MIXONE	hxxp://getgoodsb.link/notepadp.exe	https://private.tria.ge/230317-j79k3sjtys	stealc	10	family:stealc discovery spyware stealer

Méthodologie d'investigation et d'analyse

Pivot sur les nouveaux samples



Méthodologie d'investigation et d'analyse

Pivot sur les nouveaux samples

Objectif : estimer la propagation d'une nouvelle famille d'infostealer

- pivoter sur l'infrastructure de Command & Control (C2)
- pivoter sur les samples

Méthodologie d'investigation et d'analyse

Pivot sur les nouveaux samples

Pivoter sur l'infrastructure de Command & Control (C2) :

- à partir des patterns d'URLs de C2 :
 - requêtes POST

/http://[^\\]*\[a-f0-9]{16}.php/

- requêtes GET

/http://[^\\]*\[a-f0-9]{16}\sqlite3.dll/

/http://[^\\]*\[a-f0-9]{16}\freebl3.dll/

/http://[^\\]*\[a-f0-9]{16}\mozglue.dll/

/http://[^\\]*\[a-f0-9]{16}\msvcpl40.dll/

/http://[^\\]*\[a-f0-9]{16}\nss3.dll/

/http://[^\\]*\[a-f0-9]{16}\softokn3.dll/

/http://[^\\]*\[a-f0-9]{16}\vcruntime140.dll/

```
POST /984dd96064cb23d7.php HTTP/1.1
HTTP/1.1 200 OK (text/html)
POST /984dd96064cb23d7.php HTTP/1.1
HTTP/1.1 200 OK
GET /a02fc2187db8cd88/sqlite3.dll HTTP/1.1
HTTP/1.1 200 OK (application/x-msdos-program)
GET /a02fc2187db8cd88/freebl3.dll HTTP/1.1
HTTP/1.1 200 OK (application/x-msdos-program)
GET /a02fc2187db8cd88/mozglue.dll HTTP/1.1
HTTP/1.1 200 OK (application/x-msdos-program)
GET /a02fc2187db8cd88/msvcpl40.dll HTTP/1.1
HTTP/1.1 200 OK (application/x-msdos-program)
GET /a02fc2187db8cd88/nss3.dll HTTP/1.1
HTTP/1.1 200 OK (application/x-msdos-program)
GET /a02fc2187db8cd88/softokn3.dll HTTP/1.1
HTTP/1.1 200 OK (application/x-msdos-program)
GET /a02fc2187db8cd88/vcruntime140.dll HTTP/1.1
HTTP/1.1 200 OK (application/x-msdos-program)
POST /984dd96064cb23d7.php HTTP/1.1
```

Méthodologie d'investigation et d'analyse

Pivot sur les nouveaux samples



Pivoter sur l'infrastructure de Command & Control (C2) :

- à partir des en-têtes HTTP et HTML :

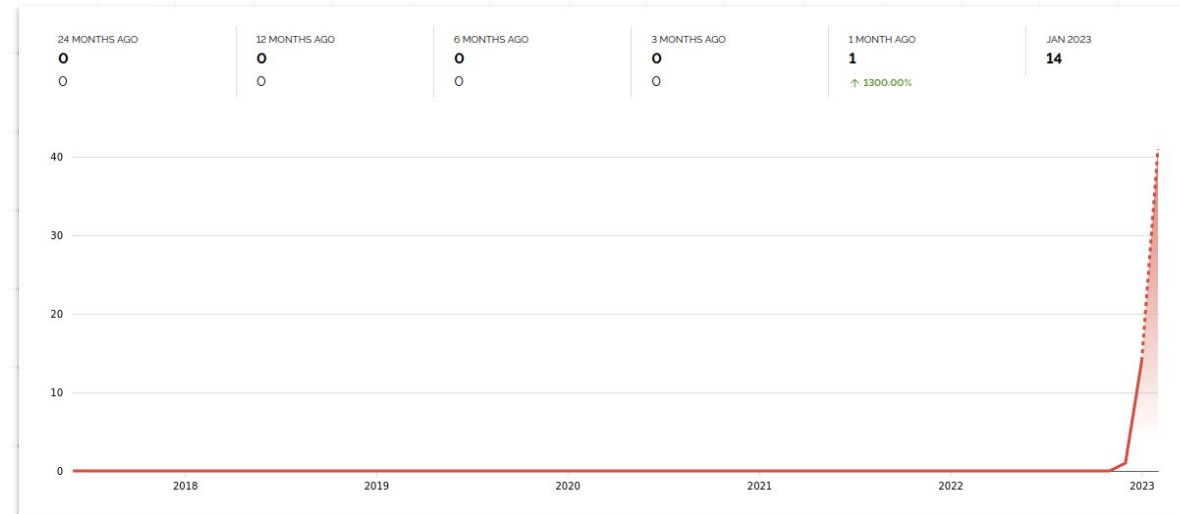
```
HTTP/1.1 200 OK
Date: <REDACTED>
Server: Apache/2.4.41 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 145
Content-Type: text/html; charset=UTF-8
```

Janvier 2023

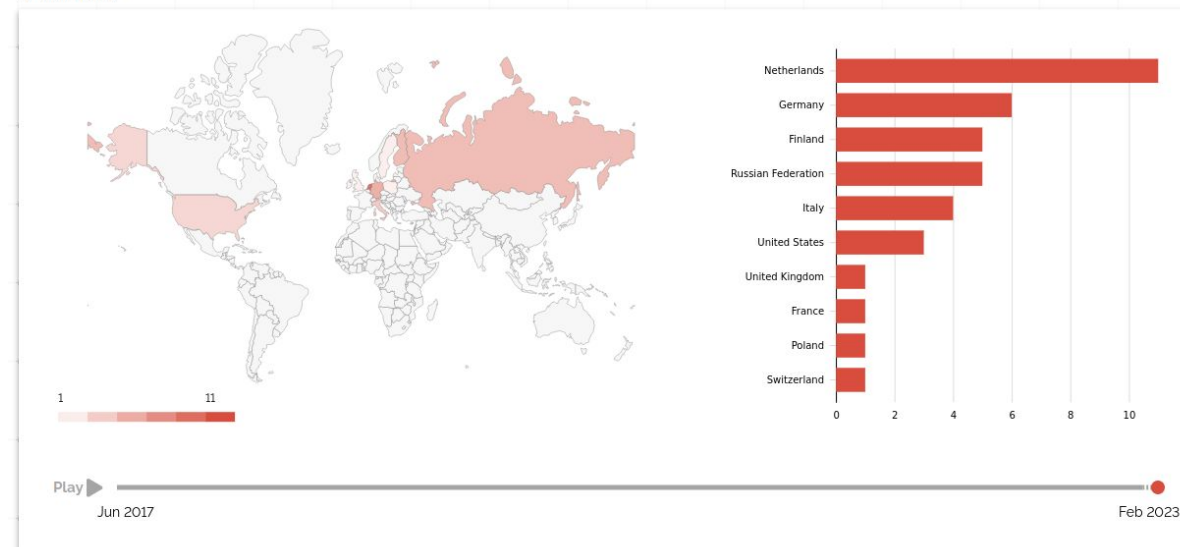
```
<html> <head><title>404 Forbidden</title></head> <body> <center><h1>404
Forbidden</h1></center> <hr><center>apache</center> </body> </html>
```



// TOTAL RESULTS



// WORLDMAP



Méthodologie d'investigation et d'analyse

Pivot sur les nouveaux samples



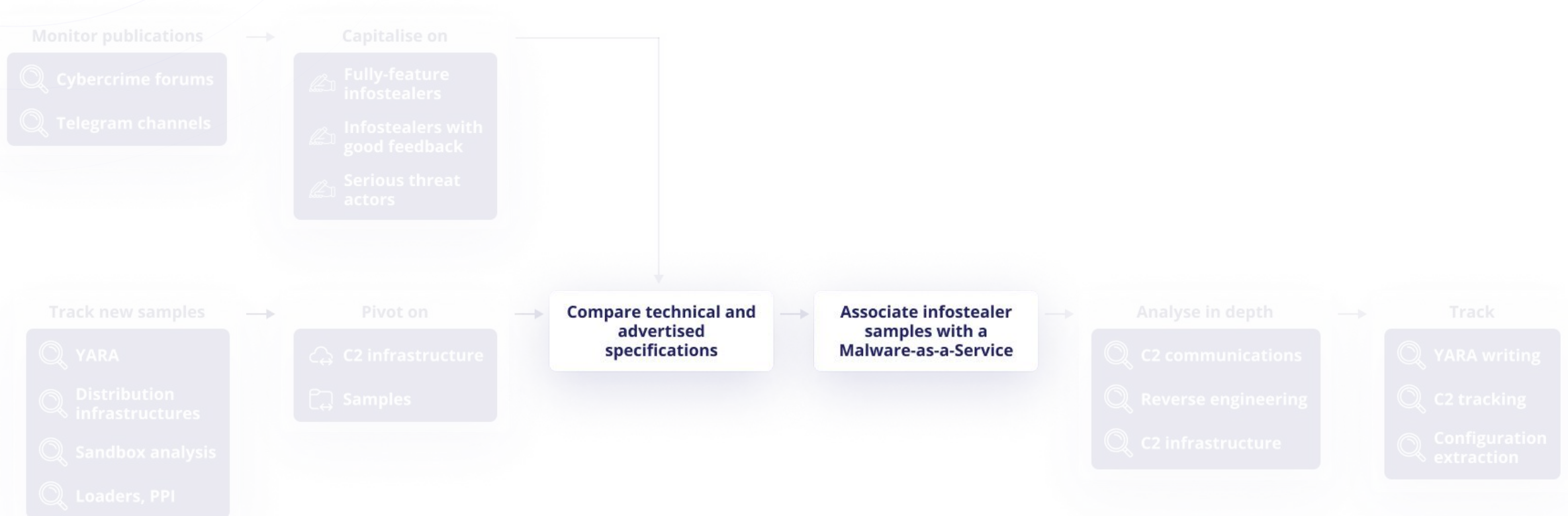
behaviour:"C:\ProgramData*.dll" behaviour:"timeout /t 5" behaviour:"sqlite3.dll"

FILES - 20 / 40 90 days

		Detections	Size	Filter by	Export	Tools	Help
				First seen	Last seen	Submitters	
<input type="checkbox"/>	525AEDD02E010F2BD7932CC63D4B61A29EF0854D578A1EBB14DC6E7B1F92AE68 cbPermissions peexe checks-network-adapters runtime-modules direct-cpu-clock-access overlay checks-cpu-name ...	15 / 55	4.77 MB	2023-02-13 22:35:36	2023-02-13 22:35:36	1	
<input type="checkbox"/>	FCD93986AF7AFF6C06CC8D6580C25049FFDB7B7C20AB05F83C652EC155B05895 cbPermissions peexe checks-network-adapters runtime-modules direct-cpu-clock-access overlay checks-user-input checks-cpu-name ...	16 / 58	4.77 MB	2023-02-13 19:44:16	2023-02-13 19:44:16	1	
<input type="checkbox"/>	0EAE25A4E19D5CD68FCFFDCA06B4DA06CC467FD6F19059F7C9AD51D720F72A6E cbPermissions peexe checks-network-adapters runtime-modules direct-cpu-clock-access overlay detect-debug-environment long-sleeps ...	29 / 71	4.77 MB	2023-02-13 19:24:04	2023-02-13 19:24:04	1	
<input type="checkbox"/>	B1A8F2D734F50BB13C2ADB0FBDA81BDE4A8E95B5D3D4F5FCB83D69EBDC92DF5 jv16PT.exe peexe overlay direct-cpu-clock-access detect-debug-environment long-sleeps runtime-modules checks-cpu-name	9 / 68	123.24 MB	2023-02-13 19:08:35	2023-02-13 19:08:35	1	
<input type="checkbox"/>	BB22503D8958ACDB29EA1F66CCF2C855149072178FD1F8725E41615BC7EA86B2 cbPermissions peexe overlay direct-cpu-clock-access checks-network-adapters runtime-modules checks-user-input checks-cpu-name ...	29 / 71	4.77 MB	2023-02-13 19:00:01	2023-02-13 19:00:01	1	
<input type="checkbox"/>	A2AC136CAE32F65AB0048DD491AA1EAF2BDCB54A7EB95880751BEE7C7567F4E8 cbPermissions peexe overlay checks-cpu-name runtime-modules detect-debug-environment checks-network-adapters long-sleeps ...	38 / 70	4.77 MB	2023-02-13 08:40:30	2023-02-13 08:40:30	1	

Méthodologie d'investigation et d'analyse

Association d'un MaaS avec des nouveaux samples



Méthodologie d'investigation et d'analyse

Association d'un MaaS avec des nouveaux samples

Objectif : associer un infostealer vendu en MaaS et une nouvelle famille distribuée dans la nature

- comparer les caractéristiques techniques et annoncées
- confirmer l'association d'un MaaS et d'une famille d'infostealer

Méthodologie d'investigation et d'analyse

Association d'un MaaS avec des nouveaux samples

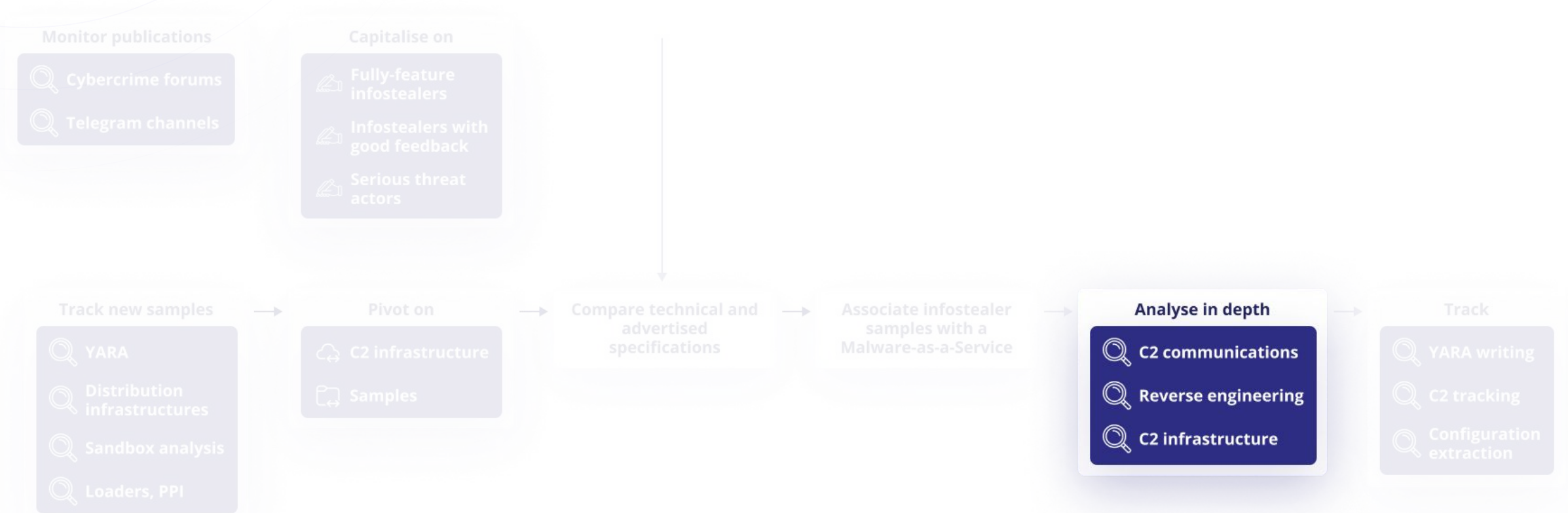


- Caractéristiques techniques
- Données ciblées
- Exfiltration des données

Stealc features, as described by Plymouth on XSS	SEKOIA.IO observations based on samples of the new malware family
<i>When developing our solution, we relied on Vidar, Raccoon, Mars and RedLine</i>	download legitimate third-party DLLs
<i>Current build weight - 78kb</i>	~ 80KB
<i>stealc was written in pure C using WinAPI</i>	WinAPI functions
<i>all functions are dynamically loaded</i>	load the WinAPI functions using GetProcAddress and LoadLibraryA
<i>import table is taken by couple of imports from msct</i>	import 6 functions from MsvcrtDLL
<i>All lines of work are obfuscated.</i>	obfuscated using RC4 and base64
<i>each file to be collected is sent to the server in a separate request</i>	exfiltrate the collected data file by file
<i>more than 23 supported browsers</i>	target 22 browsers
<i>more than 70 web plugins</i>	target 75 plugins
<i>more than 15 desktop wallets</i>	target 25 wallets.
<i>email clients</i>	\\Outlook\\accounts.txt
<i>added random name generation for script-gate (api.php), in stealc update v1.1.2</i>	random paths ([a-f0-9]{16}) used for recent samples
<i>recorded user-agents in the system_info.txt file, in stealc update v1.1.2</i>	exfiltrate victim host's user agents.
<i>recorded ip and country in file system_info.txt, in stealc update v1.1.2</i>	exfiltrate IP address and country of the infected host (ISO)

Méthodologie d'investigation et d'analyse

Analyse en profondeur



Méthodologie d'investigation et d'analyse

Analyse en profondeur

Objectif : comprendre le fonctionnement de l'infostealers d'un point de vue système et réseau

- comparer les caractéristiques techniques observées et celles annoncées
- documenter le malware
- identifier des similarités entre infostealers

Méthodologie d'investigation et d'analyse

Analyse en profondeur : rétro ingénierie



Présence d'anti-analyse (technique Jump in the middle)



Obfuscation des chaînes de caractères et des fonctions : RC4



Import des fonctions : résolution dynamique des API

```

00: 74 03      jn loc_1+1
02: 75 01      jnz loc_1+1
      loc_1
04: B8 E8 9D 00 00  mov eax, 9DE9h
  
```

↓

```

00: 74 03      jn loc_2
02: 75 01      jnz loc_2
04: 90         nop
      loc_2
06: E8 9D 00 00  call functionA
  
```

```

int decrypt_string()
{
    int result; // eax

    RC4_key = (int)"74934157919546113795";
    str_04 = mw_decrypt_string("Uyk=");
    str_02 = mw_decrypt_string("Uy8=");
    str_20 = mw_decrypt_string("US0=");
    str_23 = mw_decrypt_string("US4=");
    str_GetProcAddress = mw_decrypt_string("JHgZG2hCC4cSYENc09A=");
    str_LoadLibrary = mw_decrypt_string("L3ImL1ZECrQXdkh4");
    str_lstrcatA = (LPCSTR)mw_decrypt_string("D24zOX1MHic=");
    str_OpenEventA = (LPCSTR)mw_decrypt_string("LG0iJV9bDagCRQ==");
    str_CreateEventA = (LPCSTR)mw_decrypt_string("IG8iKm5ILbATakV4");
}
  
```

```

lstrlenA = (int (__stdcall *)(LPCSTR))GetProcAddress(ptr_PE_header, str_lstrlenA);
ExitProcess = (void (__stdcall __noreturn *) (UINT))GetProcAddress(ptr_PE_header, str_ExitProce
GlobalMemoryStatusEx = (BOOL (__stdcall *) (LPMEMORYSTATUS_EX))GetProcAddress(ptr_PE_header, str
GetSystemTime = (void (__stdcall *) (LPSYSTEMTIME))GetProcAddress(ptr_PE_header, str_GetSystem
SystemTimeToFileTime = (BOOL (__stdcall *) (const SYSTEMTIME *, LPFILETIME))GetProcAddress(ptr_P
ptr_PE_header,
str_SystemTimeTo
}
hAdvapi32 = (HMODULE)LoadLibrary(str_advapi32_dll);
hgdi32 = (HMODULE)LoadLibrary(str_gdi32_dll);
hUser32 = (HMODULE)LoadLibrary(str_user32_dll);
hCrypt32 = (HMODULE)LoadLibrary(str_crypt32_dll);
hNtdll = (HMODULE)LoadLibrary(str_ntdll_dll);
if ( hAdvapi32 )
    GetUserNames = (BOOL (__stdcall *) (LPSTR, LPDWORD))GetProcAddress(hAdvapi32, str_GetUserNames);
if ( hgdi32 )
{
    CreateDCA = (HDC (__stdcall *) (LPCSTR, LPCSTR, LPCSTR, const DEVMODEA *))GetProcAddress(hgdi32, str_CreateDCA);
    GetDeviceCaps = (int (__stdcall *) (HDC, int))GetProcAddress(hgdi32, str_GetDeviceCaps);
}
}
  
```

Rétro ingénierie : communications réseaux



1. Navigateurs web
 - a. Cookies, mots de passe, cartes de crédits
 - b. Extensions de navigateurs
2. Applications
 - a. Messageries
 - b. Jeux vidéo
 - c. Portefeuilles de cryptomonnaie
3. File grabber

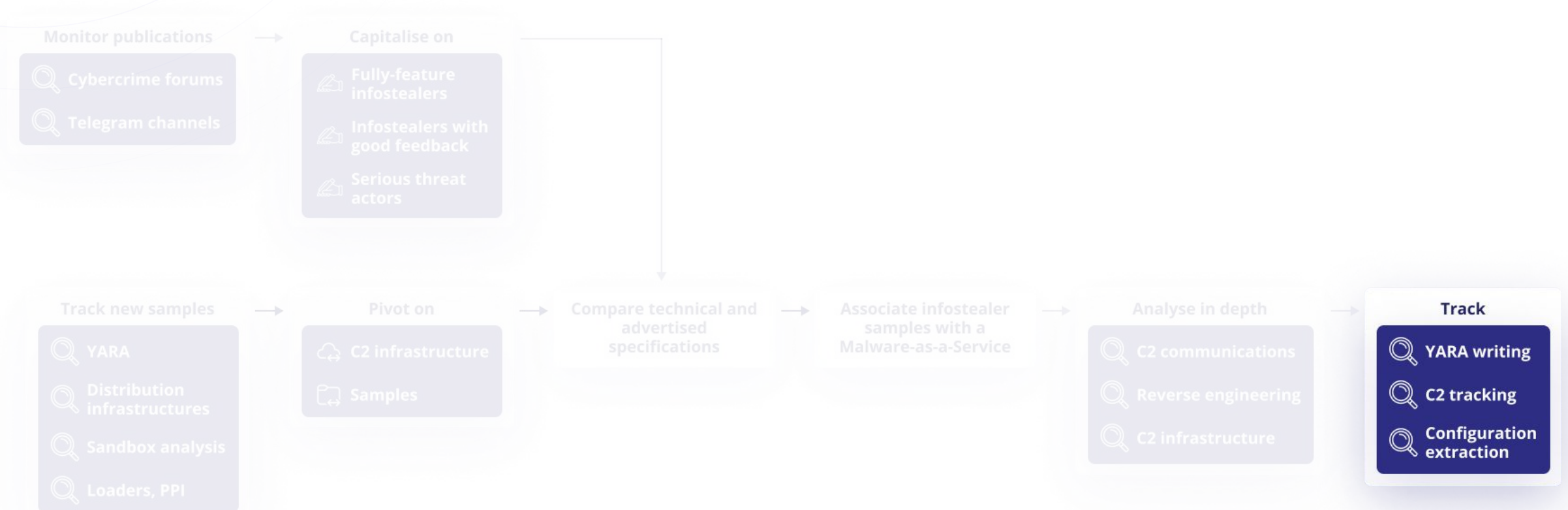
No.	Protocol	Source	Destination	Info	Comment
1	HTTP	192.168.122.1...	162.0.238.10	POST /752e382b4dcf5e3f.php HTTP/1.1	Send hwid and build name
2	HTTP	162.0.238.10	192.168.122.1...	HTTP/1.1 200 OK (text/html)	Recieved configuration ID
3	HTTP	192.168.122.1...	162.0.238.10	POST /752e382b4dcf5e3f.php HTTP/1.1	Ask for browsers configuration
4	HTTP	162.0.238.10	192.168.122.1...	HTTP/1.1 200 OK (text/html)	
5	HTTP	192.168.122.1...	162.0.238.10	POST /752e382b4dcf5e3f.php HTTP/1.1	Ask for plugins configuration
7	HTTP	162.0.238.10	192.168.122.1...	HTTP/1.1 200 OK (text/html)	
20	HTTP	192.168.122.1...	162.0.238.10	POST /752e382b4dcf5e3f.php HTTP/1.1	Send fingerprint information
21	HTTP	162.0.238.10	192.168.122.1...	HTTP/1.1 200 OK	
22	HTTP	192.168.122.1...	162.0.238.10	GET /dbe4ef521ee4cc21/sqlite3.dll HTTP/1.1	download sqlite3.dll
395	HTTP	162.0.238.10	192.168.122.1...	HTTP/1.1 200 OK (application/x-msdos-progr...	
397	HTTP	192.168.122.1...	162.0.238.10	POST /752e382b4dcf5e3f.php HTTP/1.1	Post google chrome cookies
398	HTTP	162.0.238.10	192.168.122.1...	HTTP/1.1 200 OK	
400	HTTP	192.168.122.1...	162.0.238.10	POST /752e382b4dcf5e3f.php HTTP/1.1	List google chrome extensions
401	HTTP	162.0.238.10	192.168.122.1...	HTTP/1.1 200 OK	
507	HTTP	192.168.122.1...	162.0.238.10	POST /752e382b4dcf5e3f.php HTTP/1.1	
508	HTTP	162.0.238.10	192.168.122.1...	HTTP/1.1 200 OK	
509	HTTP	192.168.122.1...	162.0.238.10	POST /752e382b4dcf5e3f.php HTTP/1.1	Get google chrome extension (h

Rétro ingénierie : fonctions personnalisées

- Détection de l'environnement
- Empreinte du poste infecté
- Blocage de l'exécution en fonction d'une date d'expiration
- Exécution d'une charge malveillante additionnelle

Méthodologie d'investigation et d'analyse

Suivi de la menace dans le temps



Méthodologie d'investigation et d'analyse

Suivi de la menace dans le temps

Objectif : mise en production des signatures et des heuristiques de suivi d'infrastructure



Conclusion : tendances et éléments-clés

Conclusion : tendances et éléments-clés



Évolution vers le modèle MaaS comme signe de **maturité** de l'écosystème

Multiplication et **professionnalisation** de la menace

Optimisation des opérations

Écosystème **réactif** aux évolutions du marché

Infostealers comme élément de la **“petite cybercriminalité”**

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION

FILED

September 26, 2022

CLERK, U.S. DISTRICT COURT
WESTERN DISTRICT OF TEXAS

BY: JF
DEPUTY

UNITED STATES OF AMERICA)
)
v.) Criminal No. 1:21-CR-224-LY
)
MARK SOKOLOVSKY,) **EX PARTE & UNDER SEAL**
)
Defendant)

**GOVERNMENT'S MOTION FOR
ALTERNATIVE VICTIM NOTIFICATION PROCEDURES**

The defendant is a native and citizen of Ukraine. On March 4, 2022, the defendant (together with other individuals) left Ukraine in what appeared to be a Porsche Cayenne, transited Poland and Germany, and eventually arrived in the Netherlands. Dutch law enforcement arrested Sokolovsky on March 20, 2022, pursuant to a Provisional Arrest Warrant requested by the United States.

Merci !



Quentin Bourgue

Analyste CTI

quentin.bourgue@sekoia.io



Pierre Le Bourhis

Analyste CTI

pierre.le-bourhis@sekoia.io



Livia TIBIRNA

Analyste CTI

livia.tibirna@sekoia.io

blog.sekoia.io