



# Infostealers

investigating the cybercrime threat  
within its ecosystem

Pierre LE BOURHIS  
Livia TIBIRNA

# Who we are?

## Threat & Detection Research (TDR) team, Sekoia.io



**Pierre LE BOURHIS**

CTI analyst

@plebourhis



**Livia TIBIRNA**

CTI analyst

@liviaticbirna

# Summary

- 1 Infostealers: definition, context and impact
- 2 Overview of the Russian-speaking infostealers ecosystem
- 3 Identifying emerging infostealers : investigation and analysis
- 4 Conclusion : current trends and key facts

# Infostealers: definition, context and impact

# Infostealers



**Infostealers are a type of malware that collect sensitive data stored on infected machines and exfiltrate it to attackers' infrastructure.**

Data is collected from:

- web browsers (cookies, authentication data, banking data, extensions)
- installed applications
- cryptocurrency wallets
- stored files and documents
- 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

# Infostealer-as-a-Service: goals and impacts

- **Cybercrime: lucrative goals**
- **APT: advanced persistent threat**
- **Hacktivists**

**Corporate Credentials Found: 9**

URL	Login	Password
https://akademi.thy.com/oturumac.aspx	[REDACTED]@thy.com	Ara [REDACTED]
https://dccflr.thy.com/oamssso-bin/login.pl	koc12	Ara [REDACTED]
https://w3.airbus.com/H380/external/pw/airbus pwservices.fcc	koc12	Ara [REDACTED]
https://innovation.thy.com/my.policy	koc12	Ara [REDACTED]
https://dccflr.thy.com/oamssso-bin/login.pl	koc12	Ara [REDACTED]
https://info.thy.com/my.policy	koc12	Ara [REDACTED]
https://turuncuhat.thy.com/CAisd/pdmweb.exe	koc12	Ara [REDACTED]
https://dcc.thy.com/oamfed/idp/samlv20	koc12	Ara [REDACTED]

Credentials of the infected employee, discovered in Hudson Rock's database.

**Machine ID:** TR969000B9C336C19E07DF0849B97D1D0A\_2023\_08\_21T01\_14\_37\_528177 [REDACTED]

**Stealer Family:** RedLine

**IP Address:** 176.42. [REDACTED]

**Malware Path:** C:\\Windows\\Microsoft.NET\\Framework\\v4.0.30319\\AppLaunch.exe

**Date Compromised:** 2023-08-21 01:14:37

**Last Time Added:** 2023-08-21 11:56:23

## An Avoidable Breach: FBI Hacker Leaks Sensitive Airbus Data

A HUDSON ROCK INVESTIGATION



# Overview of the Russian-speaking infostealers ecosystem

# Russian-speaking infostealers ecosystem

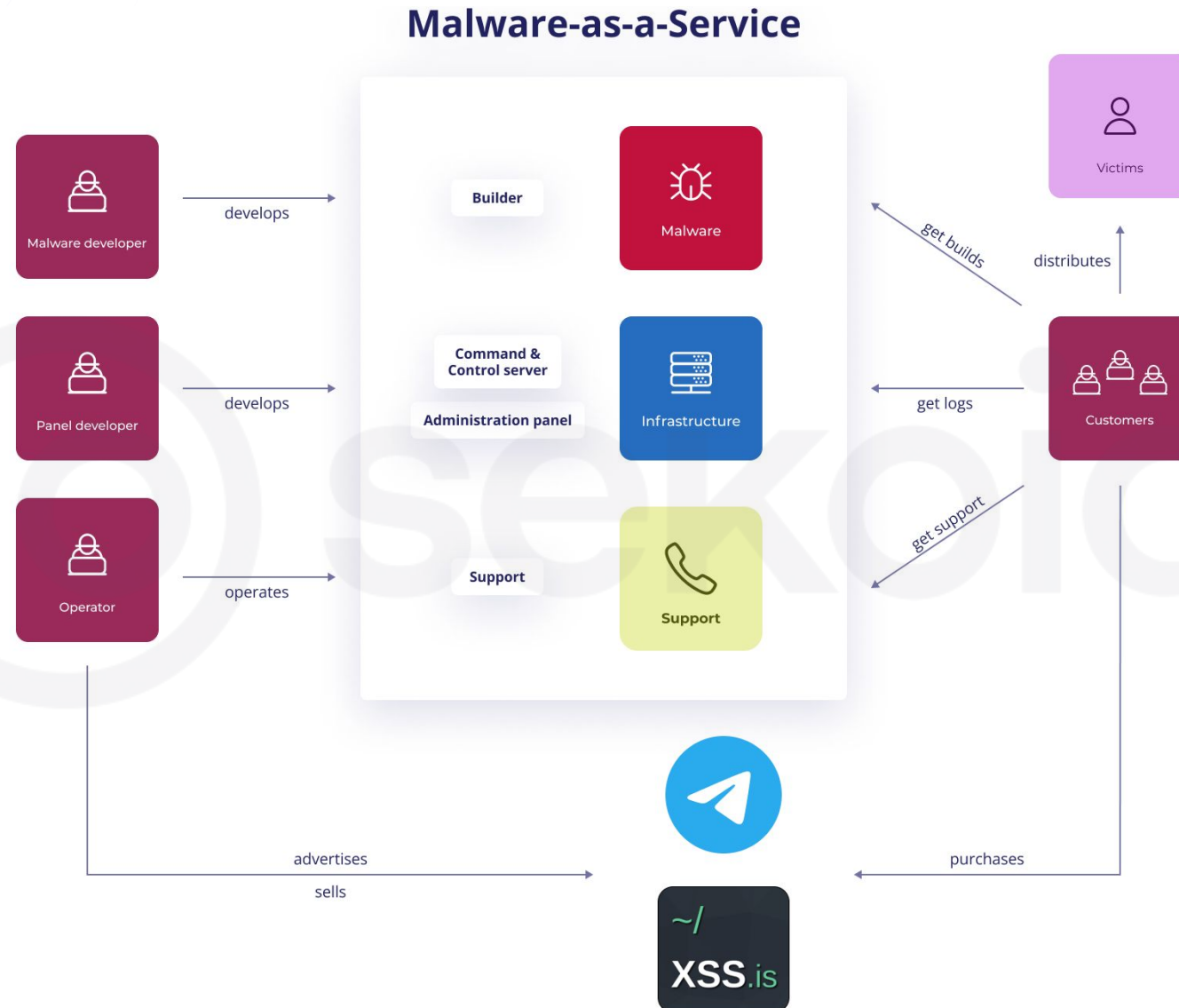


The ecosystem is shaped by:

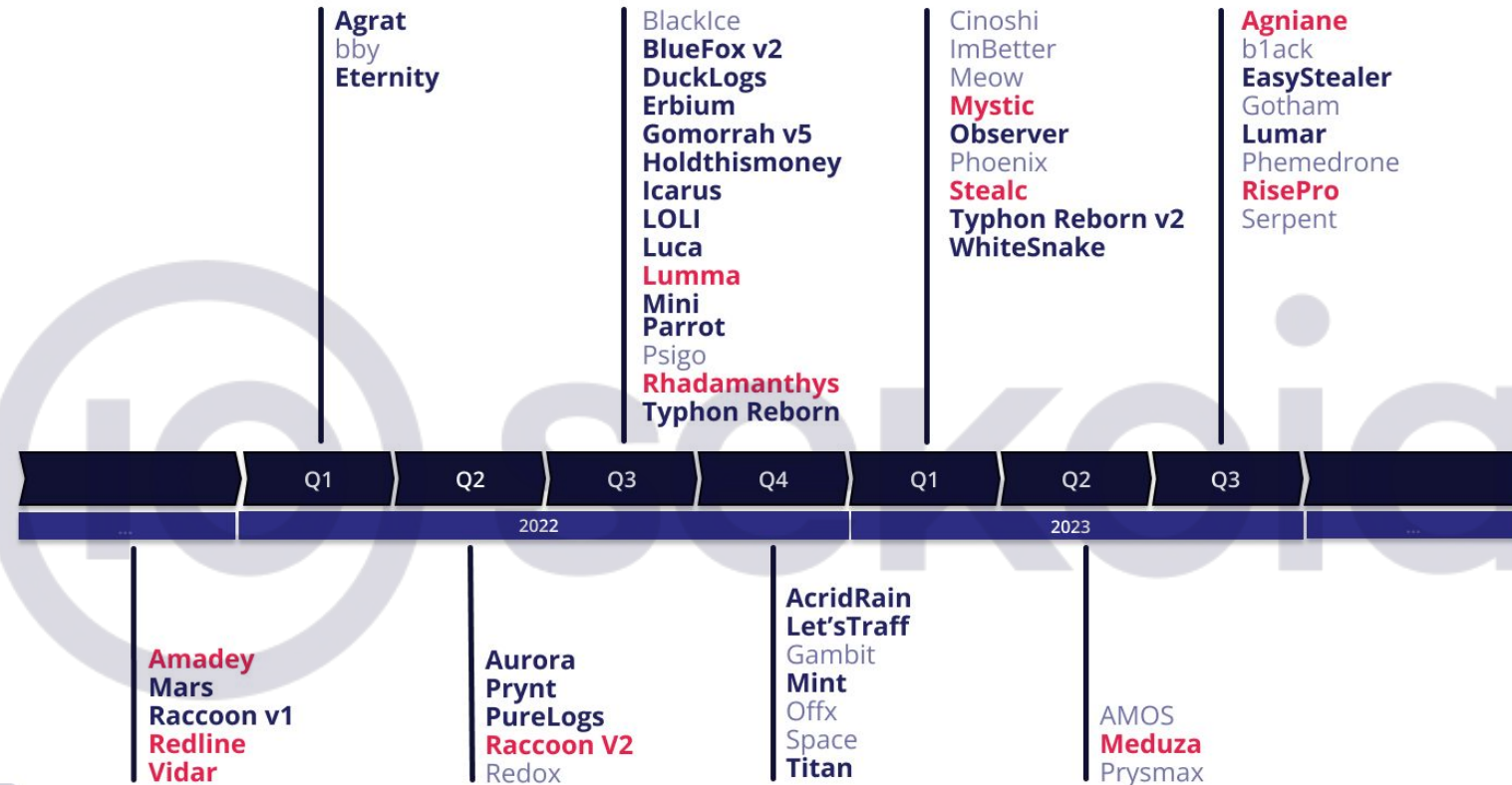
- **structured** activities
- associated **services** for each type of activity
- **sharing** of resources and knowledge
- a **low barrier** to entry
- **specialised** marketplaces



# Malware-as-a-Service: a ready to use model



# Malware-as-a-Service: ecosystem's dynamics



Infostealer families sold as a Malware-as-a-Service, that Sekoia.io observed to be:

- The most distributed in 2023
- Known to be distributed in the wild
- Less distributed in the wild

# Malware-as-a-Service : an illustration of an infostealer advertisement

stealc - стилер с гибкими настройками и удобной админ-панелью

plymouth · Jan 9, 2023 · stealc | продажа | стилер

ESCROW AVAILABLE IN THIS THREAD!

New deal

Jump to new

Watch



plymouth

форум-диск

Пользователь

Joined: Jul 30, 2022  
Messages: 9  
Reaction score: 2  
Deposit: 0.02

Jan 9, 2023

stealc - это нерезидентный стилер 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 msctd для стаба), собирается под тулkit 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 стилера.

Вышел новый плагин или нашли интересный 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 самостоятельно, не создавая конкуренции себе же в трафике.

С другой стороны, вы можете сократить сбор только до тех плагинов и кошельков, что вам действительно нужны и не забивать место на диске.

stealc не генерирует архив на стороне клиента, каждый собираемый файл передается на сервер в отдельном запросе - даже если антивирус среагирует в рантайме, хотя бы часть данных уже будет лежать на сервере.

Это очень важная функция - мы сами использовали все достойные внимания решения на рынке и чаще всего антивирусы реагируют в рантайме на сбор файлов граббером. Если к этому моменту на сервере не будет лога, то в принципе его уже не будет.

Поэтому в своем софте мы реализовали передачу каждого генерируемого/собираемого файла на сервер отдельным запросом сразу после генерации/сбора файла.

Простыми словами - софт собрал данные о системе и сразу передал на сервер, собрал пароли из браузеров и передал на сервер и так далее по списку. Если на каком то этапе в рантайме софт будет пойман антивирусом, то какая-то часть данных уже будет лежать на сервере, а не утеряна.

stealc по умолчанию собирает большое количество данных:

- более 23 поддерживаемых браузеров (Chromium, Google Chrome, Chrome Canary, Amigo, Torch, Vivaldi, Comodo, EpicPrivacyBrowser, CocCoc, Brave, Cent, 7Star, Chedot, Microsoft Edge, 360, QQBrowser, CryptoTab, Opera, Opera GX, Opera Crypto, Mozilla Firefox, Pale Moon)
- более 70 веб-плагинов (MetaMask, TronLink, Opera Wallet, Binance, Yoroi, Coinbase, Guarda, Jaxx, iWallet, MEW CX, GuildWallet, Ronin Wallet, NeoLine, CLV, Liquidity, Terra Station, Keplr, Sollet, Auro Wallet, Polymesh, ICONex, Coin98, EVER, KardianChain, Rabby, Phantom, Brave, Oxygen, Pali, BOLT X, XDEFI, Nami, Maiar DeFi Wallet, Keeper, Solflare, Cyano, KHC, TezBox, Temple, Goby, Ronin, Byone, OneKey, DAppPlay, SteemKeychain, Braavos, Enkrypt, OKX, Sender, Hashpack, Eternl, Pontem Aptos, Petra Aptos, Martian Aptos, Finnie, Leap Terra, Trezor Password Manager, Authenticator, Authy, EOS Authenticator, GAuth Authenticator, Bitwarden, KeePassXC, Dashlane, NordPass, Keeper, RoboForm, LastPass, BrowserPass, MYKI, Splikity, CommonKey, Zoho Vault)
- более 15 десктоп-кошельков (Bitcoin Core, Dogecoin, Dogecoin, Raven, Daedalus, Blockstream Green, Wasabi, Ethereum, Electrum, Electrum-LTC, Exodus, Electron Cash, MultiDoge, Jaxx Desktop, Atomic, Binance, Coinomi)
- мессенджеры: Telegram, Discord, Tox, Pidgin
- сессии Steam
- почтовые клиенты: Microsoft Outlook, Thunderbird

Встроенный нерезидентный ладер подгрузит во временную папку и запустит указанный файл, возможен запуск от имени админа (используется метод с запросом прав доступа на cmd.exe для обхода желтого окна UAC)

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 : XXS forum

Source : chechire666\_aurora Telegram channel 11

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



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

### Aurora stealer

5.0  
рейтинг

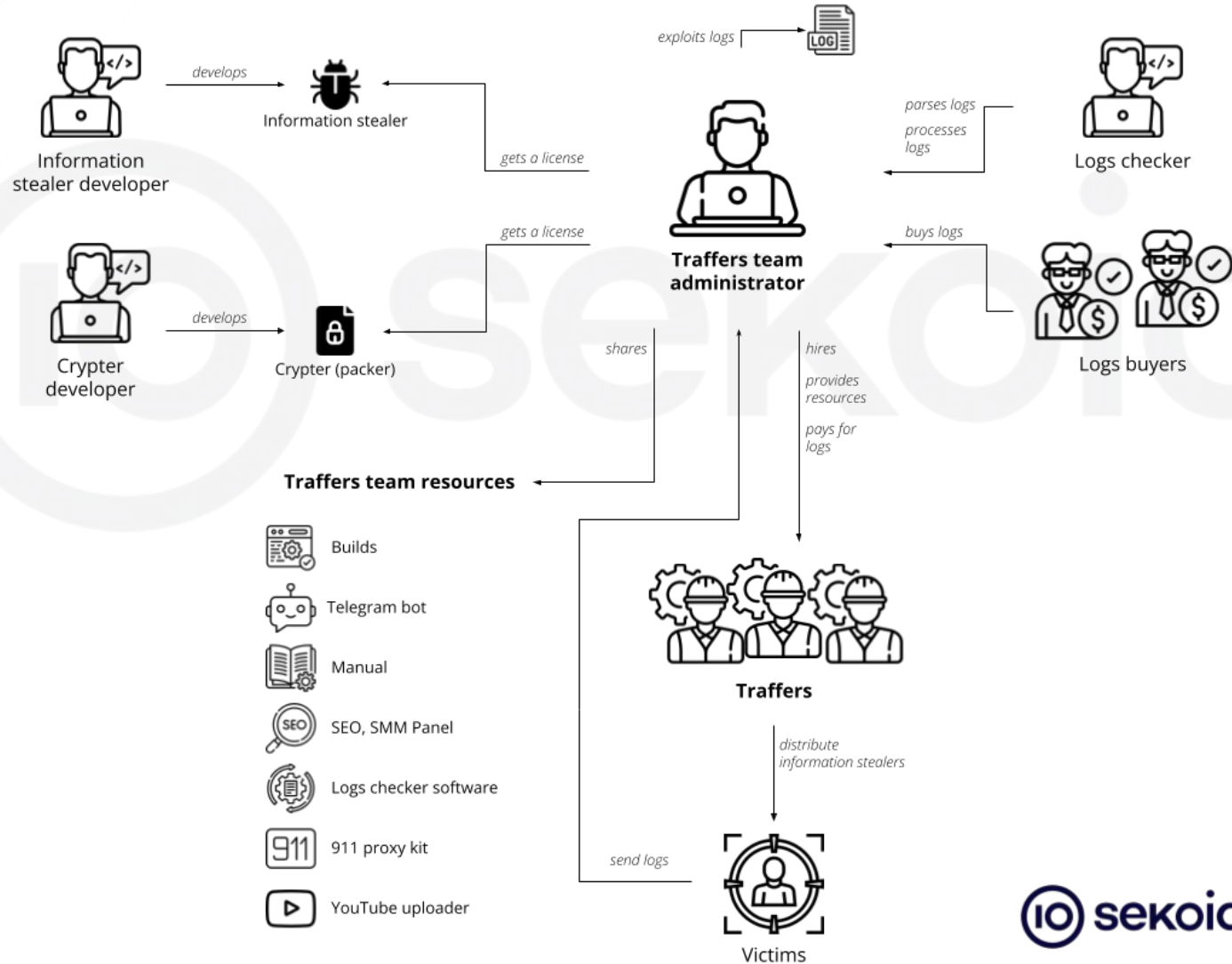


Данный стиллер позволит вам собирать данные со всех браузеров (Cookie, Password, Wallets), имеет Мощный File Grabber, Панель на вашем сервере, Встроенный Loader (Download, PowerShell). Нет зависимостей, софт нативный, а также мощная база, протокол связи TCP.



**Traffers** (from the Russian *траффер*) are threat actors specialised in redirecting traffic to massively distribute infostealers.

# A typical traffers team structure and its interactions



# Infostealers

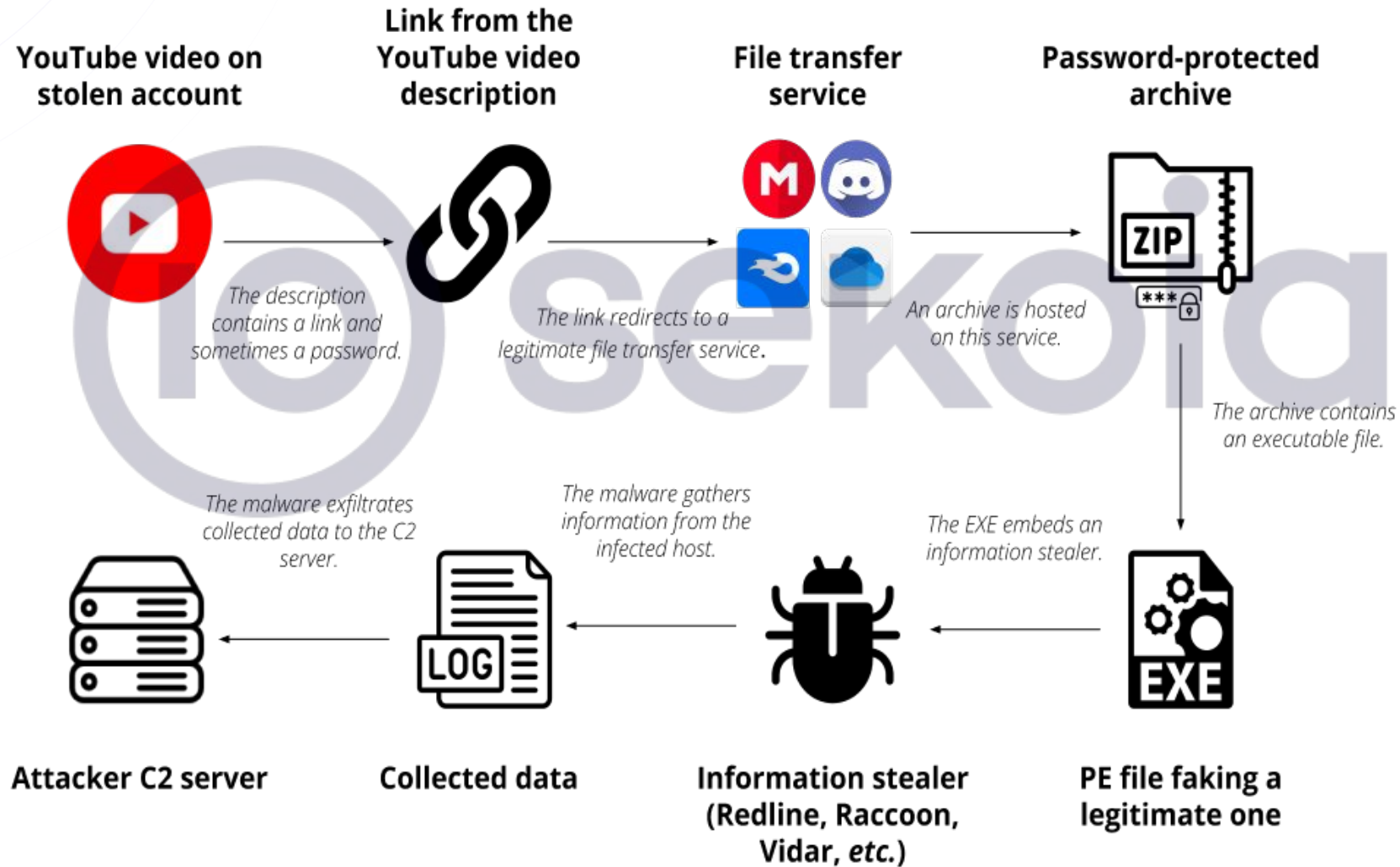
## distribution channels



Actors distributing infostealers leverage the following distribution channels and social engineering techniques:

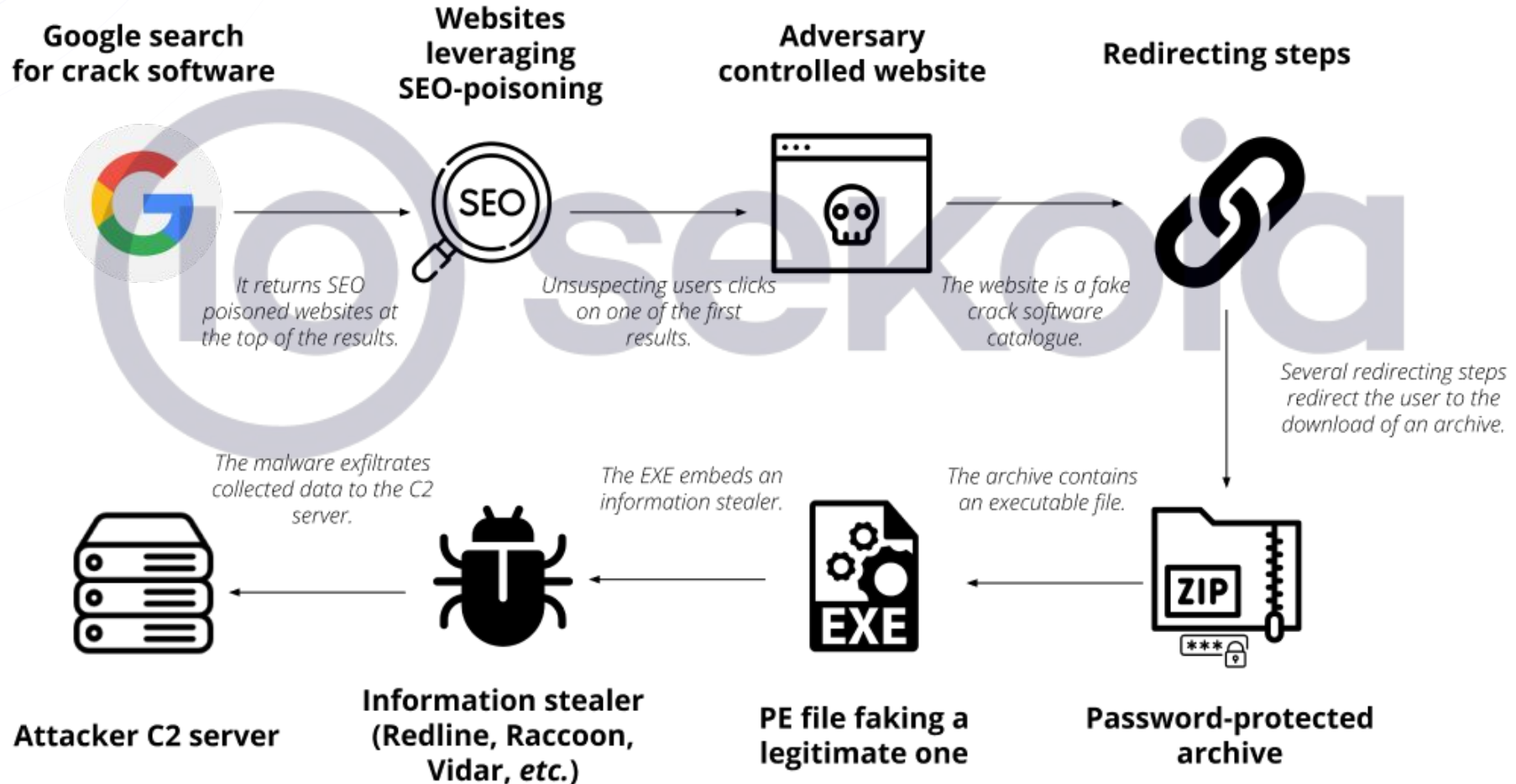
- malspam
- malvertising (Ads + landing pages)
- phishing on social networks
- cracked software
- fake updates
- web pages imitating legitimate software sites
- documents related to corporate activities

# "911" infection chain



Example: on YouTube, search for "free download crack photoshop"

# “SEO poisoning + cracked software” infection chain



Example: on Google, search for “download crack software”



# Example: "Malvertising"

Google search results for "zoom download". The search bar shows "zoom download" and the results page displays several sponsored ads:

- Ad** · [https://fr.seekblend.com/look\\_no\\_more/quality\\_info](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.

Navigation: <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

# Dedicated services associated with infostealer distribution

**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	Accounting	Accounting	Accounting
Ai	Accounting	Accounting	Accounting
Lr	Accounting	Accounting	Accounting

Цена - 10\$

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

Покупка - @nightiks  
1.3K edited 22:55

**Лэнды для пролива**  
@TrafLand

191 5 5 1  
Subscribers Photos Videos Link

Разработка одностраничных сайтов для пролива до 50\$

Администратор - @nightiks

DOWNLOAD TELEGRAM

About Blog Apps Platform

**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

# Sale of stolen data

A screenshot of a forum listing stolen data items. The items are:

- 421 stealer logs (logs\_admin started an hour ago) with buttons for 'Free data' and 'Stealer logs'.
- 796 stealer logs (logs\_admin started 5 hours ago) with buttons for 'Free data' and 'Stealer logs'.
- 93k Hong Kong Combolist (Administrator started a day ago) with buttons for 'Free data' and 'Combolists'.
- 1354 stealer logs (logs\_admin started a day ago) with buttons for 'Free data' and 'Stealer logs'.

A screenshot of a forum thread titled 'Stealer Logs'. The thread is part of a series of 21 pages. The content includes:

- Forum Announcements: Leak Section Rules by [pompompurin](#).
- Normal Threads:
  - Free Stealer logs | 2000 JANUARY 2023 - part45 by [NFU02](#), Yesterday, 04:21 PM
  - #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 titled 'Moon Cloud | Free Logs'. The channel has 438 members and a pinned message #2611. The pinned message is 'Curry Cloud FREE LOGS.rar'. Below the pinned message, there are several messages from the channel:

- Message 1: 3 likes, 438 views, 09:21. Content: 'Logs by @prdscloud 1461449785.zip' (147.9 MB), Password: [redacted]
- Message 2: 2 likes, 418 views, 09:43. Content: 'Logs by @prdscloud 2583780216.zip' (51.2 MB), Password: [redacted]
- Message 3: 1 like, 454 views, 09:43. Content: 'Logs by @prdscloud 2871378693.zip' (165.6 MB), Password: [redacted]
- Message 4: 1 like, 468 views, 09:44. Content: 'Logs by @prdscloud 2983018111.zip' (97.7 MB), Password: [redacted]
- Message 5: 1 like, 468 views, 09:44. Content: 'Logs by @prdscloud 5943114326.zip' (40.3 MB), Password: [redacted]

Sources: SQLi Cloud, BreachedForum, Telegram

# Sale of stolen data: centralised platforms

<p><a href="#">C22A5B10D4C2A30906204DCE00AF12FF</a></p> <p>📅 2023-03-15 17:11:09 📅 2023-03-15 19:41:07</p>	<p>👤 </p> <p>📧 Amazon 📧 Live</p> <p>account.battle.net eu.battle.net</p>	<p>📧 Google 📧 AppleStore</p> <p>eu.account.battle.net us.battle.net</p>	<p>📧 Facebook 📧 PayPal</p> <p>...known 6 ...other 6</p>	<p>✉️ 0 📄 12 💎 0 = 12</p> <p>🇫🇷 FR 2a01:e0a:a8fec50...</p> <p>Windows 10 Enterprise</p>	<p>17.00</p> <p>🗑️ 🗑️</p>
<p><a href="#">65DC0B671AA4685B977D4896FC314D99</a></p> <p>📅 2023-03-15 16:26:52 📅 2023-03-15 19:41:07</p>	<p>👤 </p> <p>📧 SFR 📧 GitHub</p> <p>account.prusa3d.com accounts.thingiverse.com</p>	<p>📧 Google 📧 Orange</p> <p>accounts.autodesk.com accounts.thingive...</p>	<p>📧 Aliexpress 📧 Booking</p> <p>...known 10 ...other 25</p>	<p>✉️ 0 📄 35 💎 0 = 35</p> <p>🇫🇷 FR 2a02:8428:e2c:6a01...</p> <p>Windows 10 Home</p>	<p>8.00</p> <p>🗑️ 🗑️</p>
<p><a href="#">C6F6C54A53A63D83CD51F709EE85F8F0</a></p> <p>📅 2023-03-15 14:27:32 📅 2023-03-15 19:41:06</p>	<p>👤 </p> <p>📧 SonyEntertainm... 📧 SFR 📧 Uber</p> <p>com.contextlogic.wish 9710981p.index-education.net</p>	<p>Leboncoin 📧 Live</p> <p>tv.twitch.android.app</p>	<p>📧 Spotify 📧 LidlStore</p> <p>...known 10 ...other 40</p>	<p>✉️ 0 📄 50 💎 0 = 50</p> <p>🇫🇷 FR 78.121...</p> <p>Windows 10 Home</p>	<p>5.00</p> <p>🗑️ 🗑️</p>
<p><a href="#">74724859075A0A6281F22E55090D4A90</a></p> <p>📅 2023-03-15 14:26:10 📅 2023-03-15 19:41:06</p>	<p>👤 </p> <p>📧 CDiscountStore 📧 Twitter 📧 Rakuten 📧 SFR 📧 CarrefourStore</p> <p>cellmapper.net.cellmapper</p>	<p>Impotsgouv 📧 iCloud 📧 Aliexpress 📧 GitHub 📧 Steam</p> <p>cgeo.geocaching</p>	<p>📧 EasyJet 📧 Google 📧 Amazon 📧 PayPal 📧 Orange</p> <p>...known 66 ...other 149</p>	<p>✉️ 0 📄 215 💎 0 = 215</p> <p>🇫🇷 FR 86.73...</p> <p>Windows 7 Home Premium</p>	<p>48.00</p> <p>🗑️ 🗑️</p>


Source: Genesis Market

# Sale of stolen data: logs qualification

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 сделана оперативно, чтобы "похоронить" аналитику из данных логов.
- Doesn't kill logs**  
I don't delete user agents, option to "kill" user agent from log data.
- Никаких пропусков!**  
Мы всегда следим за качеством процесса и работаем 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 парсеров, логика логов за пару минут.
- Work speed**  
One of the fastest attackers, a bunch of logs in a couple of minutes.
- Частые обновления**  
Каждую неделю мы добавляем новые сервисы.
- Frequent updates**  
Every week we add new services.
- Приемлемая цена**  
За оптимальную цену вы получаете весь функционал софта.
- Acceptable price**  
For the optimal price you get all the functionality of the software.

@Checker\_support



# Identifying emerging infostealers : investigation and analysis



# Investigation and analysis methodology



## Goals:

- identifying emerging infostealers
- assigning samples distributed in the wild to advertisements of Malware-as-a-Service on cybercrime platforms
- tracking and detecting known threats

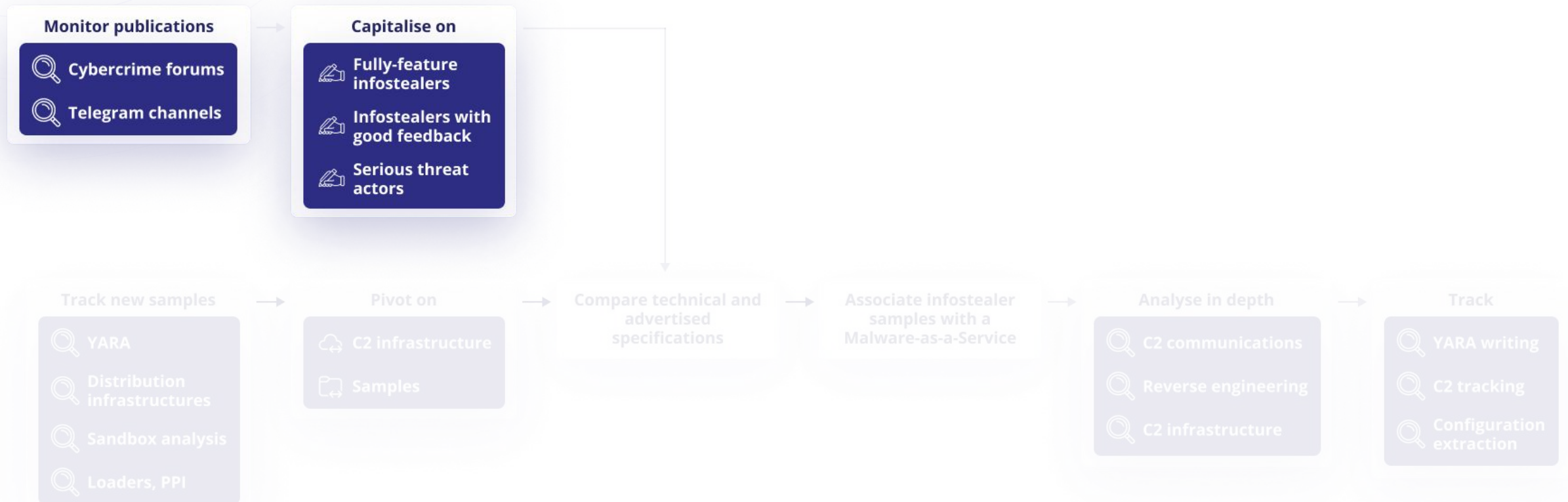
# Investigation and analysis methodology





# Investigation and analysis methodology

## Monitoring and capitalisation



# Investigation and analysis methodology

## Monitoring and capitalisation

### Goal: unveiling new infostealer families

- detecting weak signals related to the ecosystem's evolution
- anticipate the adoption of an infostealer by the cybercrime community
- monitoring the financial submissions of threat actors



**plymouth**

форру-диск

Messages: 0 · Reaction score: 0

Dec 14, 2022 (0.02 ₿)



**Phoenix1**

форру-диск

Messages: 5 · Reaction score: 0

Feb 23, 2023 (0.01 ₿)



**arv6**

Премиум

Messages: 77 · Escrow deals: 1

Mar 4, 2023 (0.02 ₿)



**WhiteSnake**

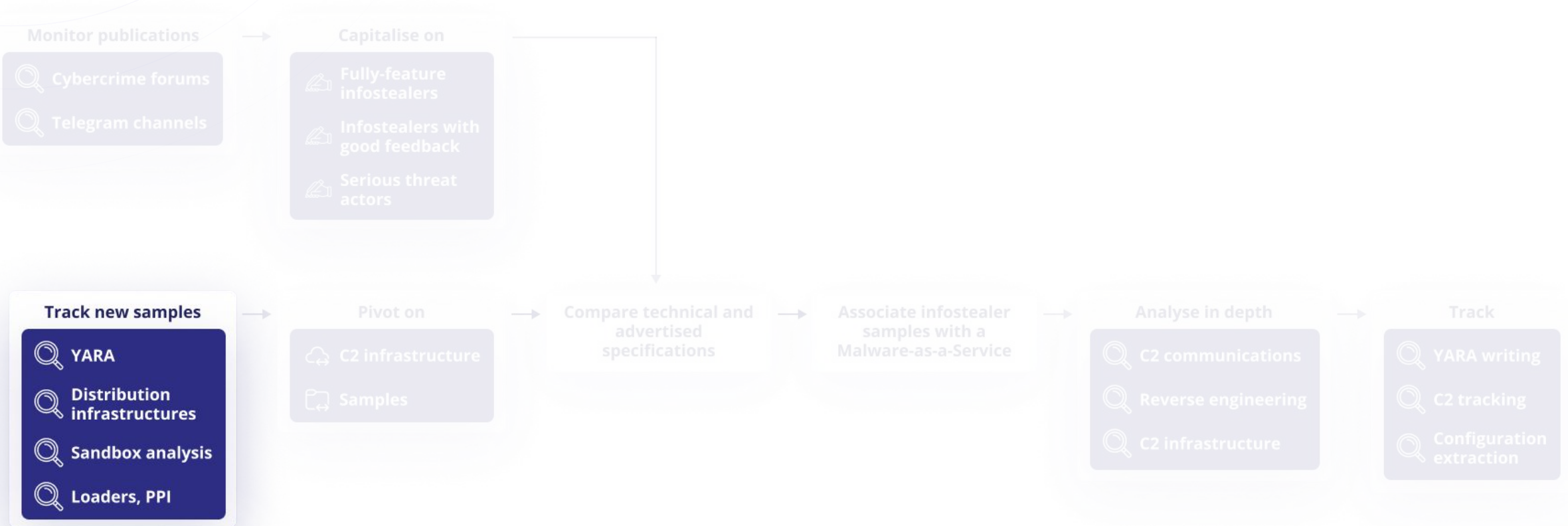
Seller

Messages: 17 · Reaction score: 4

Mar 18, 2023 (0.026 ₿)

# Investigation and analysis methodology

## Proactively tracking of new samples



## Investigation and analysis methodology

### Proactively tracking of new samples

#### Goal: tracking samples of emerging infostealers distributed in the wild

- tracking the **distribution infrastructure** leveraged to deliver infostealers
- Writing **YARA rules** for hunting purposes
- tracking **sandbox** analysis results
- tracking **payloads** distributed by popular loaders

# Investigation and analysis methodology

## Proactively tracking of new samples



tracking the distribution infrastructure

**SEKOIA.IO** SEKOIA

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](#)

# Investigation and analysis methodology

## Proactively tracking of new samples



Writing **generic** YARA rules based on targeted data from:

- web browsers
- cryptocurrency wallets (software)
- cryptocurrency wallets (web extensions)

```
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
```

# Investigation and analysis methodology

## Proactively tracking of new samples

### Tracking payloads distributed by loaders associated with Pay-Per-Install services

Example : a bot monitoring payloads distributed by GCleaner loader



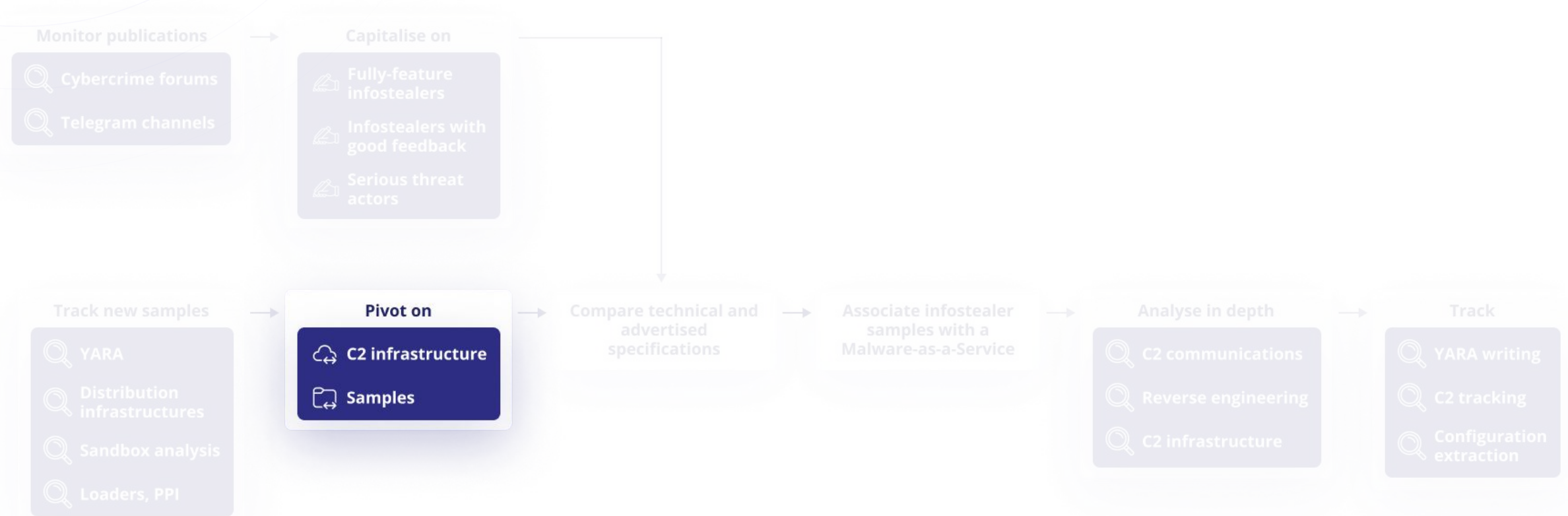
TDR - Cybercrime bot BOT 09:24

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

# Investigation and analysis methodology

## Pivoting on new samples





# Investigation and analysis methodology

## Pivoting on new samples



### **Goal: estimation an infostealer family's propagation**

- pivoting on Command & Control (C2) infrastructure
- pivoting on samples

# Investigation and analysis methodology

## Pivoting on new samples

### Pivoting on Command & Control (C2) infrastructure:

- via C2' URL patterns:
  - POST requests

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

- GET requests

/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
```

# Investigation and analysis methodology

## Pivoting on new samples



### Pivoting on Command & Control (C2) infrastructure:

- via HTTP and HTML headers:

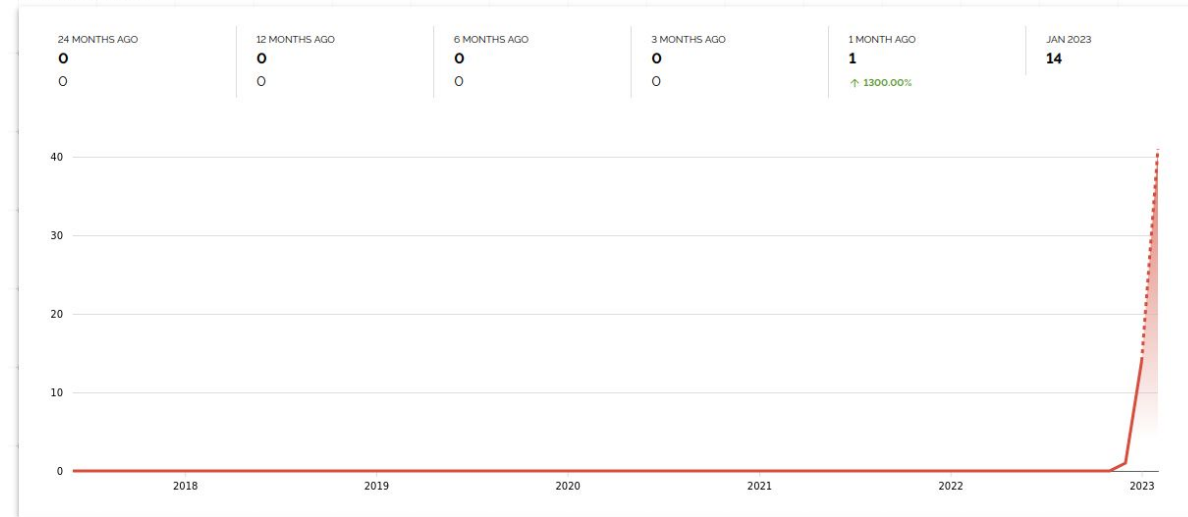
```
HTTP/1.1 200 OK
Date: <REDACTED>
Server: Apache/2.4.41 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 145
Content-Type: text/html; charset=UTF-8
```

Janvier 2023

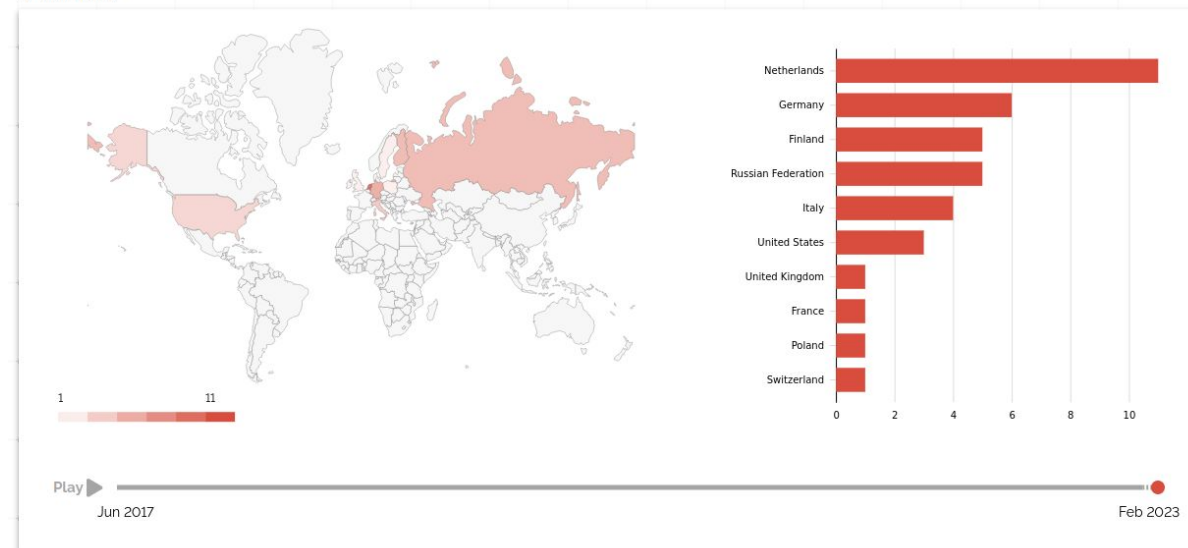
```
<html> <head><title>404 Forbidden</title></head> <body> <center><h1>404
Forbidden</h1></center> <hr><center>apache</center> </body> </html>
```



// TOTAL RESULTS

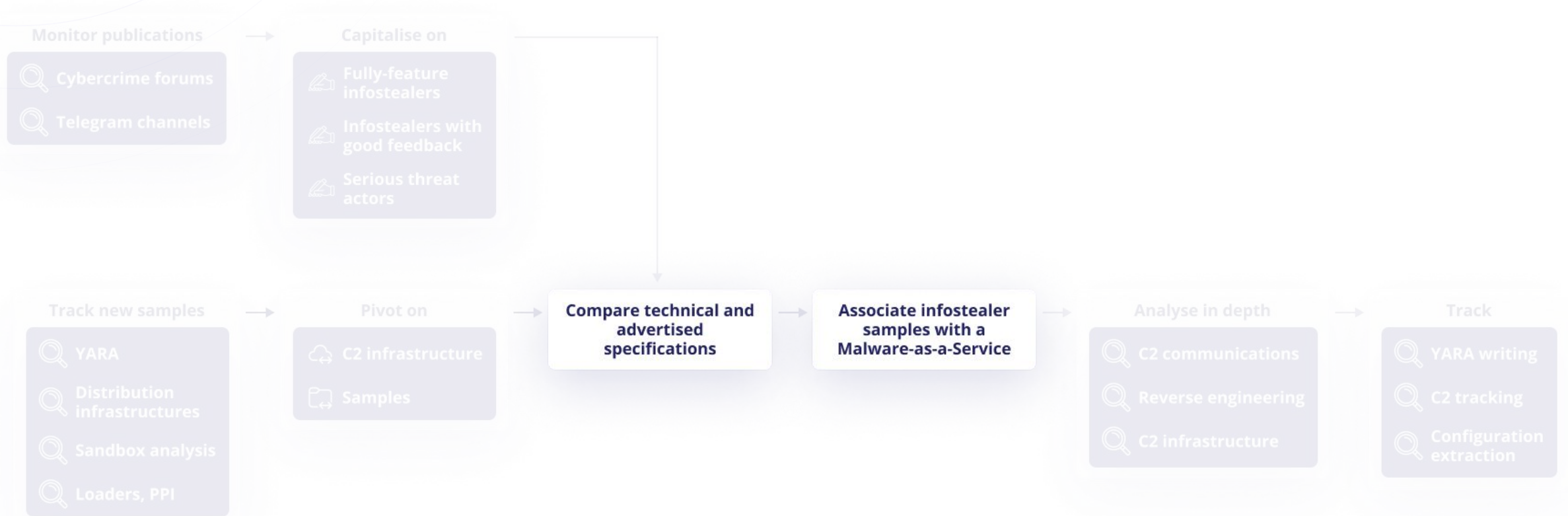


// WORLDMAP



# Investigation and analysis methodology

## Linking new samples to advertised MaaS



## Investigation and analysis methodology

### Linking new samples to advertised MaaS

**Goal: assigning samples distributed in the wild to Malware-as-a-Service advertised on cybercrime platforms**

- comparing advertised technical characteristics with those observed in the wild
- assessing links between a MaaS and an infostealer family

# Investigation and analysis methodology

## Linking new samples to advertised MaaS

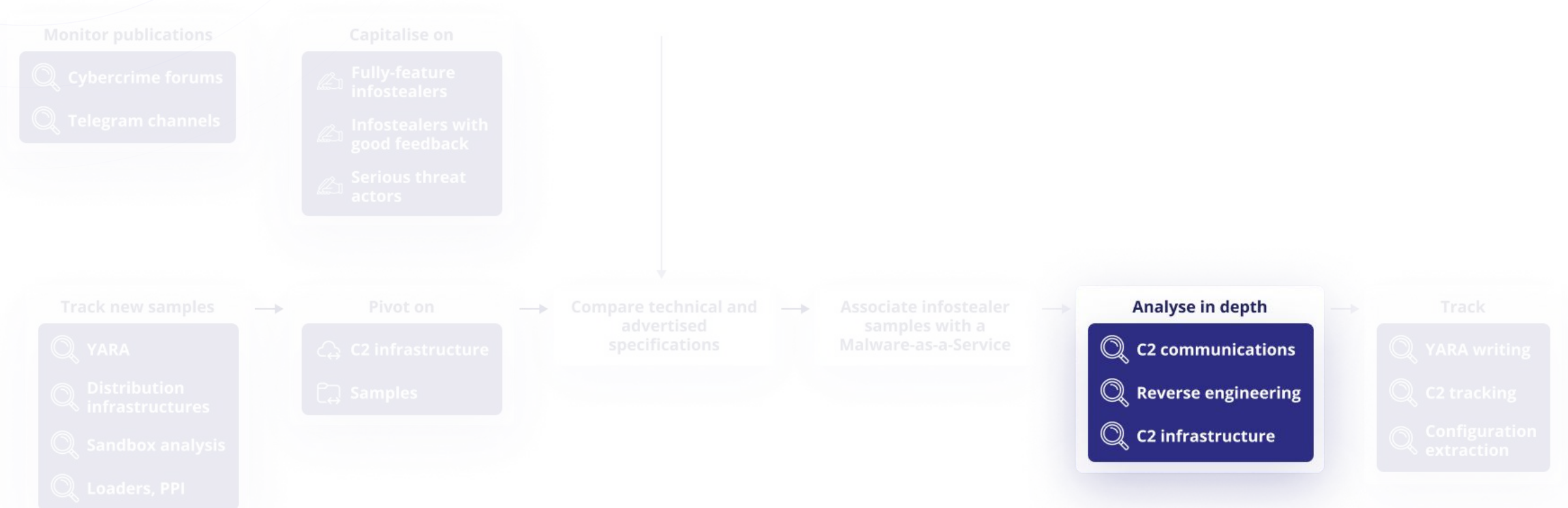


- technical characteristics
- targeted data
- data exfiltration

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)

# Investigation and analysis methodology

## In-depth analysis



**Goal: analysing the infostealers *modus operandi***

- to compare the technical characteristics announced by the developer and those observed during the reverse engineering process
- to provide documentation of the malware in order to improve the knowledge and coverage of the threat
- to write advanced YARA rules
- to identify similarities between this threat and other stealers in the ecosystem



# Investigation and analysis methodology

## In-depth analysis: reverse engineering

- Anti-analyse (Jump in the middle technique)**
- String and function obfuscation: RC4**
- Importing functions: API dynamic resolution**

```

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("JHgZ2hCC4cSYENc09A=");
    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 *) (LPMEMORYSTATUSEX))GetProcAddress(ptr_PE_header, st
GetSystemTime = (void (__stdcall *) (LPSYSTEMTIME))GetProcAddress(ptr_PE_header, str_GetSystem
SystemTimeToFileTime = (BOOL (__stdcall *) (const SYSTEMTIME *, LPFILETIME))GetProcAddress(ptr_PE_header,
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 )
    GetUserNameA = (BOOL (__stdcall *) (LPSTR, LPDWORD))GetProcAddress(hAdvapi32, str_GetUserNamel
if ( hgdi32 )
{
    CreateDCA = (HDC (__stdcall *) (LPCSTR, LPCSTR, LPCSTR, const DEVMODEA *))GetProcAddress(hgdi32, str_CreateDCA);
    GetDeviceCaps = (int (__stdcall *) (HDC, int))GetProcAddress(hgdi32, str_GetDeviceCaps);
}
}
    
```

# Reverse engineering: network communications

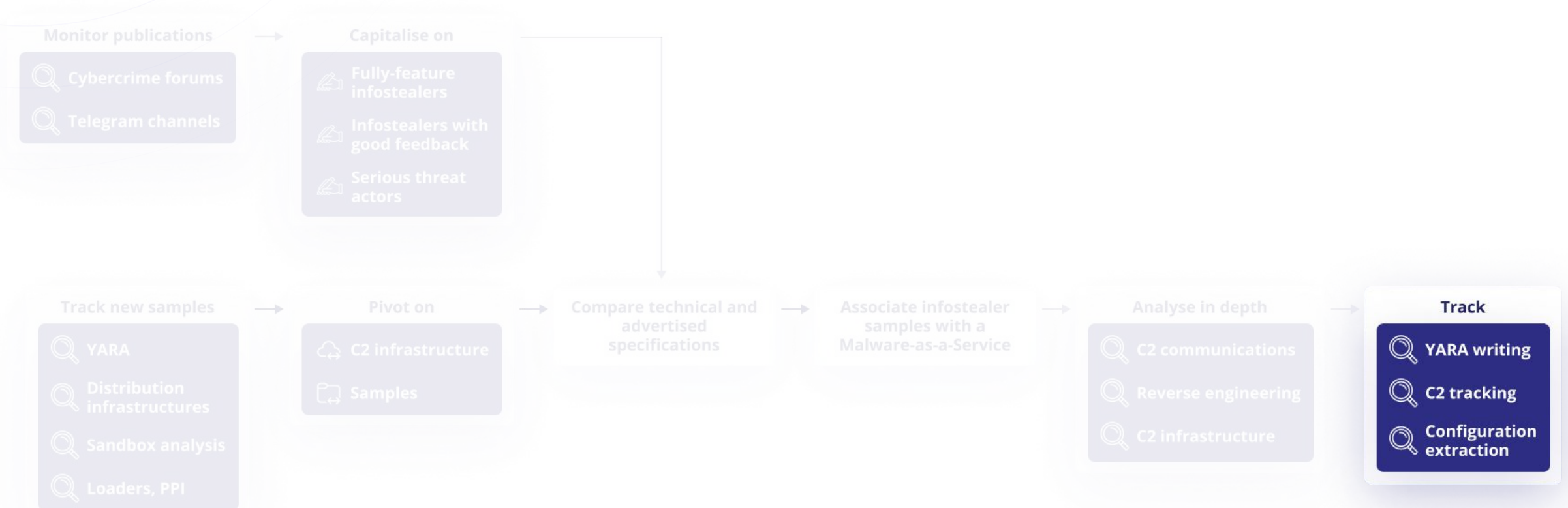


1. Web browsers
  - a. Cookies, passwords, credit cards number
  - b. Extensions
2. Applications
  - a. Messageries
  - b. Video games
  - c. Crypto wallets
3. File grabber

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

# Investigation and analysis methodology

## Tracking over time



# Investigation and analysis methodology

## Tracking over time

**Goal: production of signatures and infrastructure monitoring heuristics**



Conclusion :  
current trends and  
key facts



## Conclusion: current trends and key facts



Evolution towards the MaaS model as a sign of ecosystem **maturity**

**Multiplication** and **professionalisation** of the threat

**Optimisation** of operations

An ecosystem **reactive** to market developments

Infostealer-related actors as part of the "**small scale**" cybercrime

### AFFIDAVIT IN SUPPORT OF SEIZURE WARRANT

I, [REDACTED] being duly sworn, hereby declare as follows:

#### INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a seizure warrant for the following domains, which are also listed in Attachments A-1 through A-3: Genesis.market ("Subject Domain 1"), g3n3sis.pro ("Subject Domain 2"), g3n3sis.org ("Subject Domain 3"), gsconnects.com ("Subject Domain 4"), approveconnects.com ("Subject Domain 5"), tracecontrol.net ("Subject Domain 6"), gen2dev.net ("Subject Domain 7"), g3n3sis.net ("Subject Domain 8"), genesis-update.net ("Subject Domain 9"), genesis-security.net ("Subject Domain 10"), and [REDACTED] ("Subject Domain 11") (collectively, the "Target Properties"). Subject

# Thank you!



**Pierre Le Bourhis**

@plebourhis



**Livia TIBIRNA**

@liviaticbirna

**blog.sekoia.io**