Infostealers : investiguer la menace cybercriminelle dans son écosystème

Quentin BOURGUE
Pierre LE BOURHIS
Livia TIBIRNA

DATE MOIS ANNÉE

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

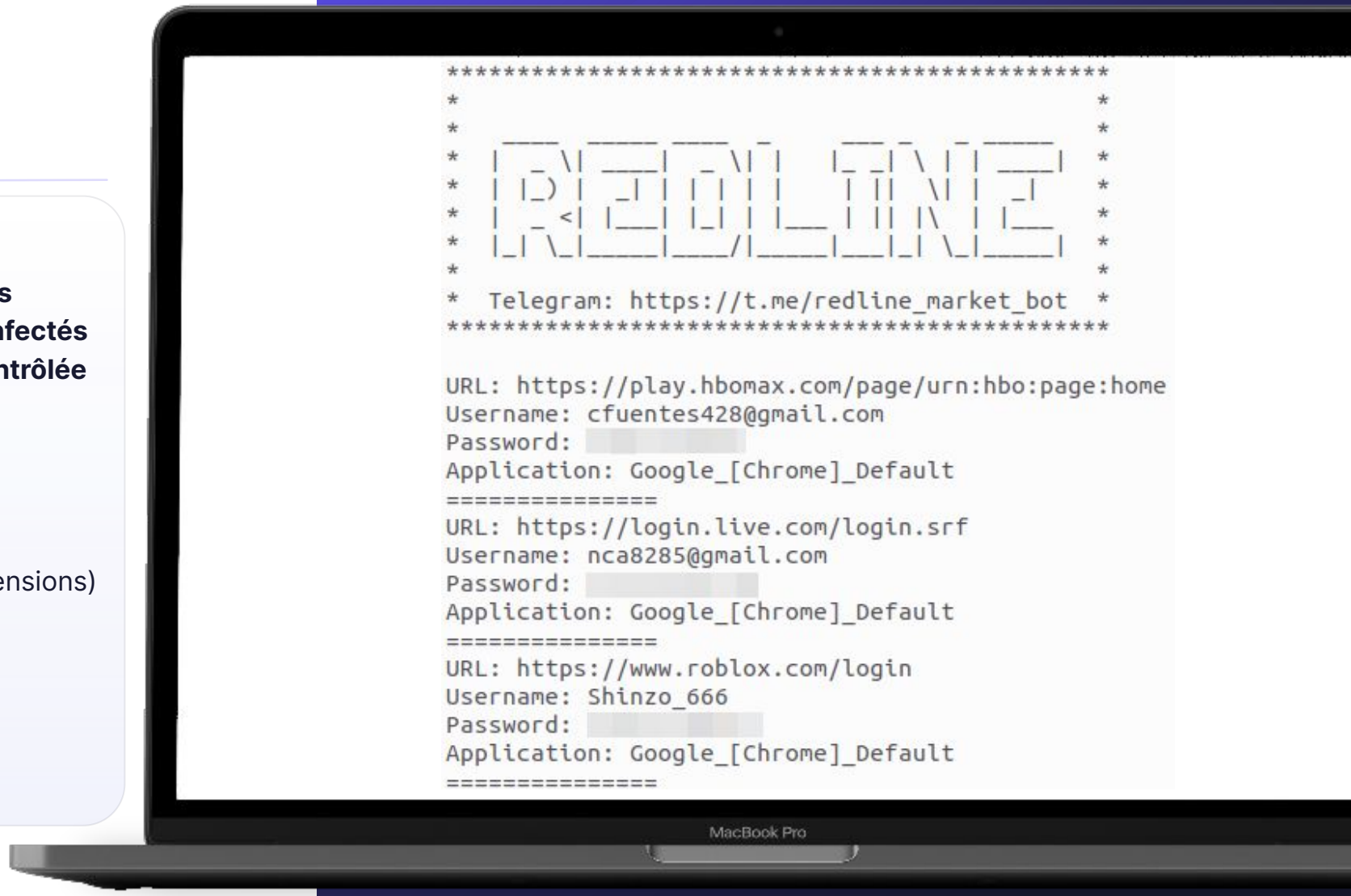
Introduction : définitions, contexte et impact

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.*

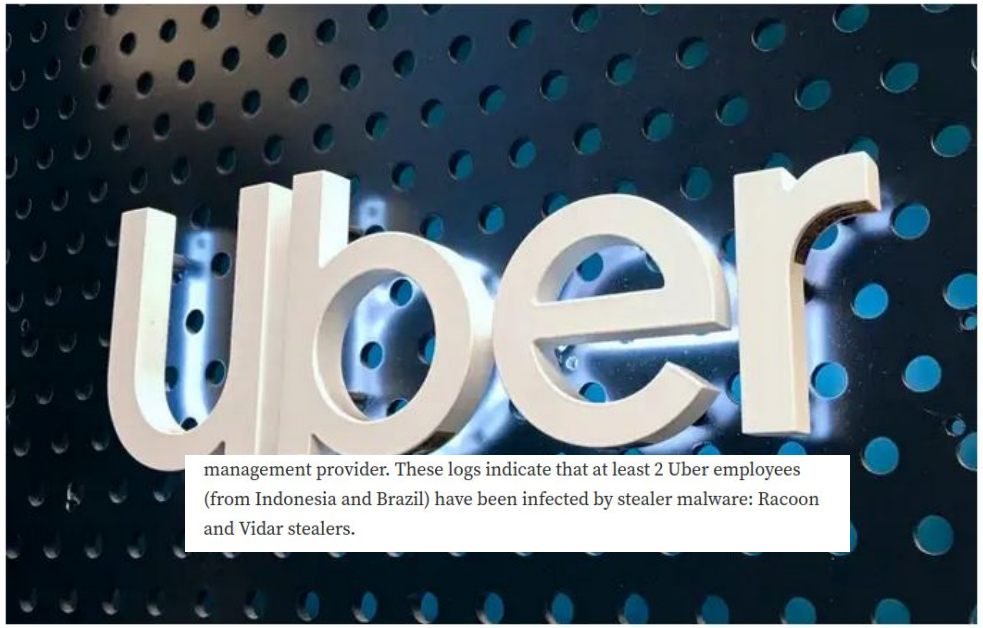


Acteurs, objectifs et impacts

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

Group-IB
Sep 19, 2022 · 3 min read · Listen

What Group-IB found about the Uber Hack



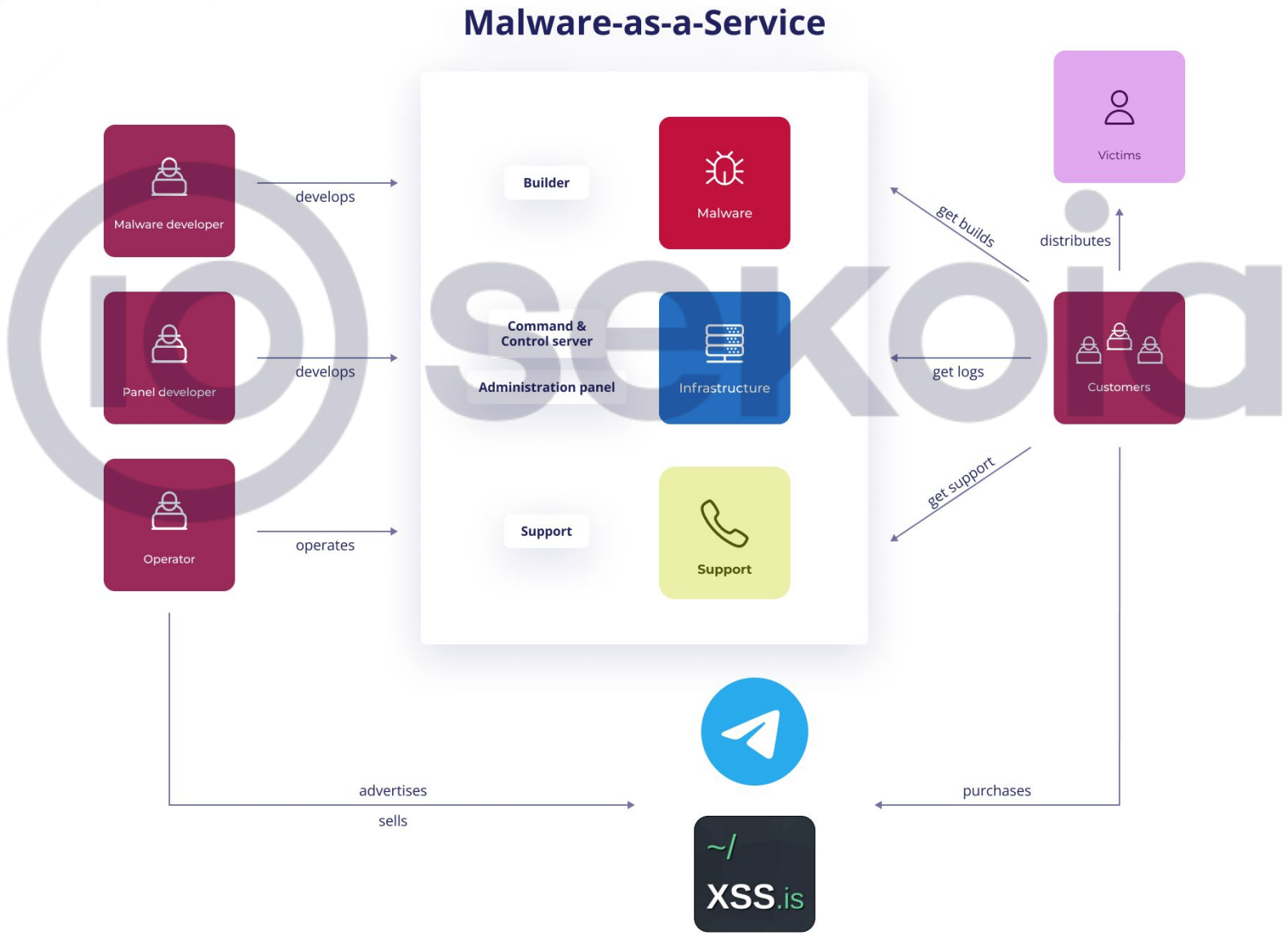
Écosystème cybercriminel russophone autour des infostealers

Un écosystème caractérisé par :

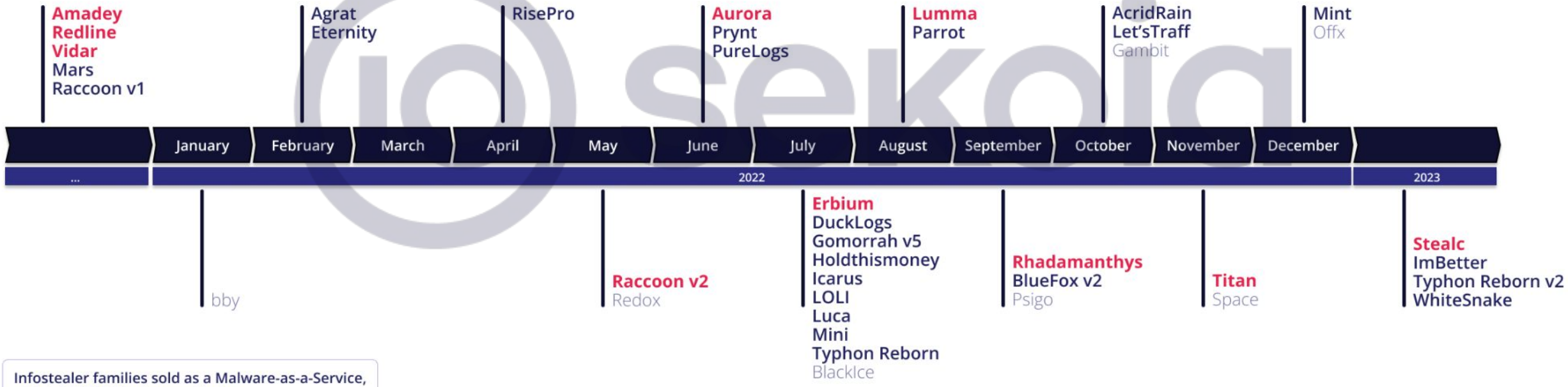
- la **structuration** des différentes activités
- des **services** pour chaque activité
- la **mise en commun** des ressources et des connaissances
- une barrière d'entrée très **accessible**
- des **places de marchés spécialisées**

Écosystème russophone autour des infostealers

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



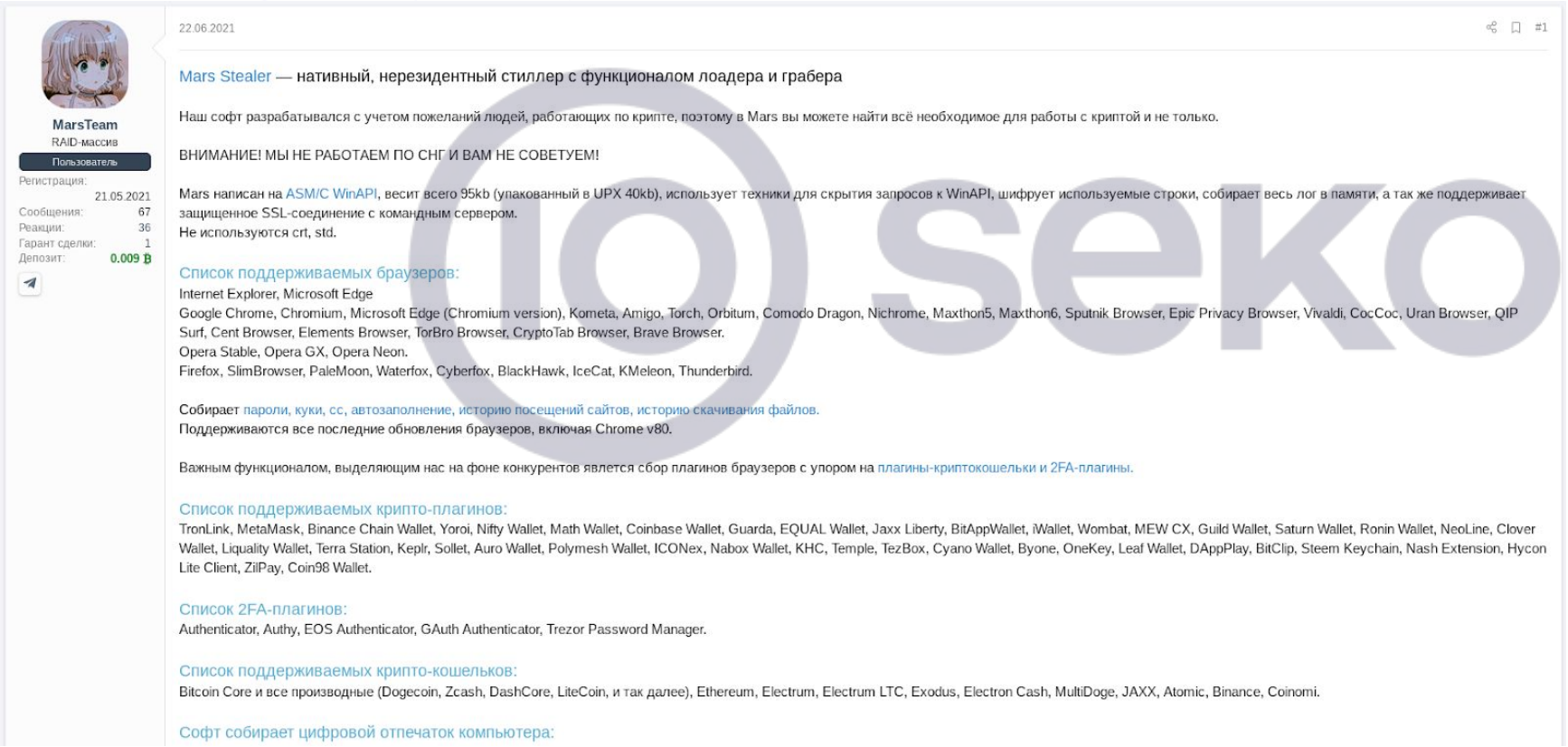
Malware-as-a-Service :
liste des infostealers en vente sur le marché



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 Ƀ

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 криптой 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, Amigo, 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, cc, 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:

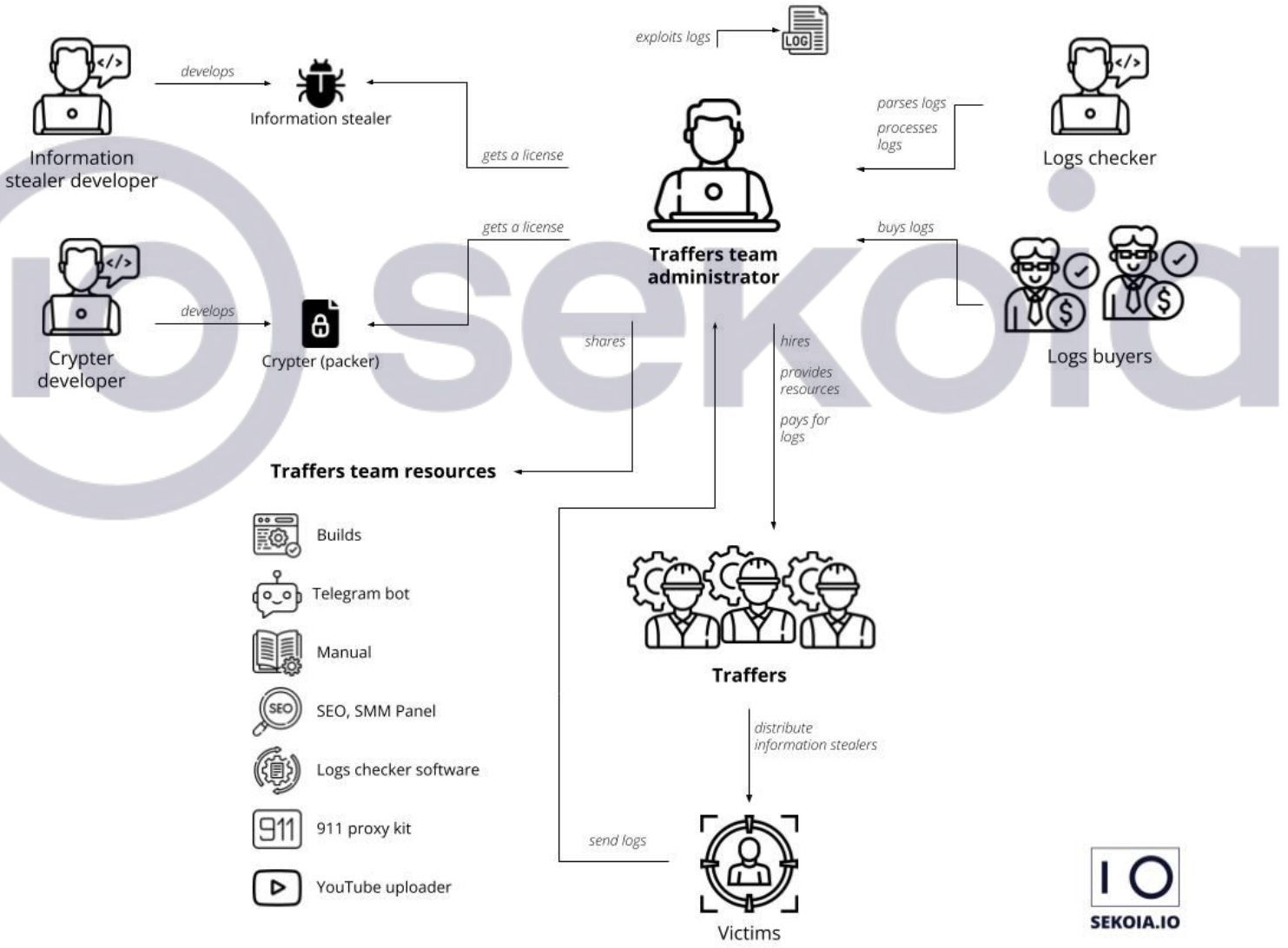
1) Loader | X64,X32 - Run, Run Memory
2) Proxy | Reverse - works without ports
3) VNC/RDP/RDP/VNC - works without ports
4) DDOS | L4.L7,Bypass
5) SiteScanner | NMAP,Scanner - for finding vulnerabilities and hacking
6) Port | Working with ports - it is easy to make tunnels and reverse ports, the possibility 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

Les ***traffers*** (du russe *трафферы*) 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

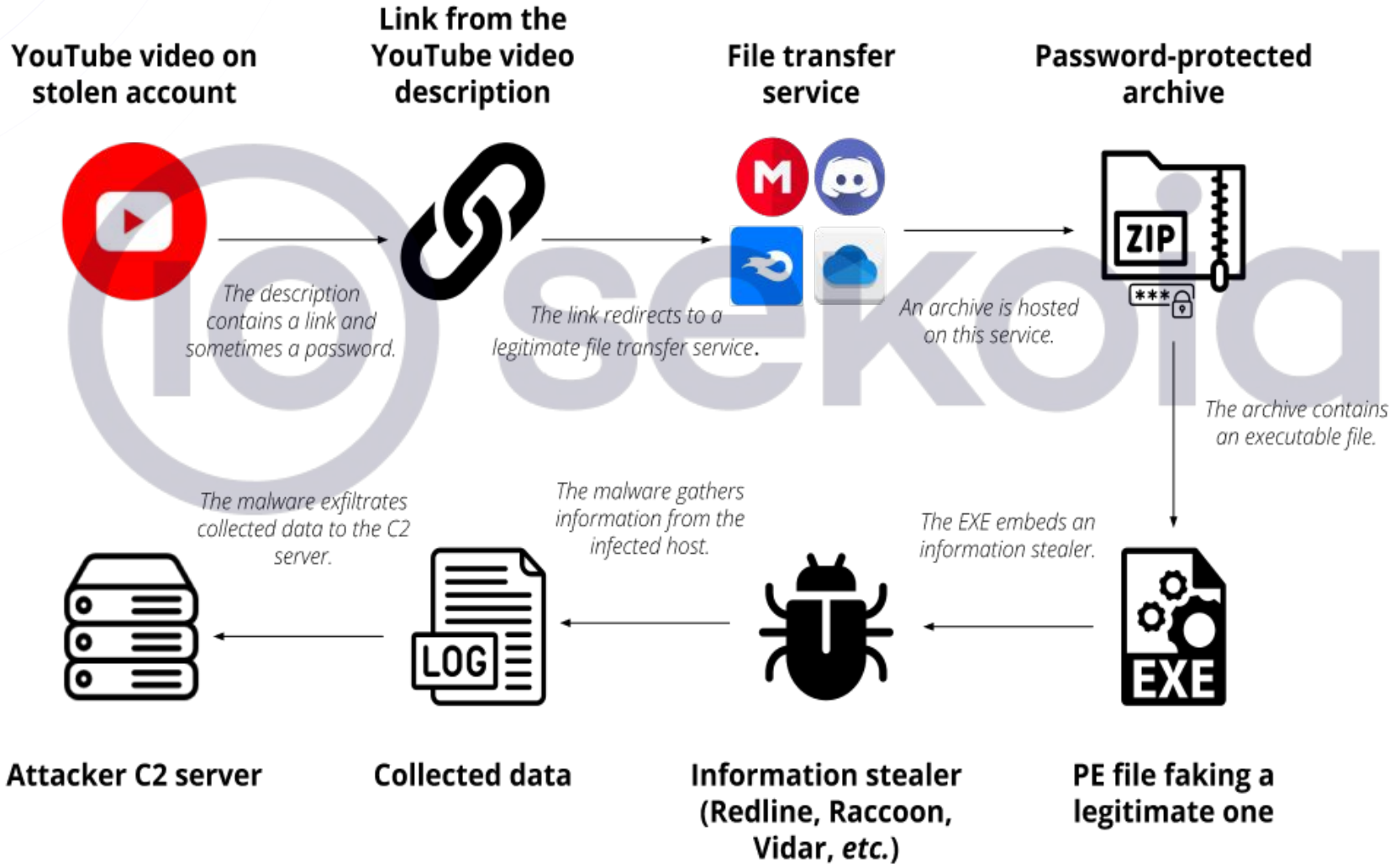


Méthodes de distributions

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

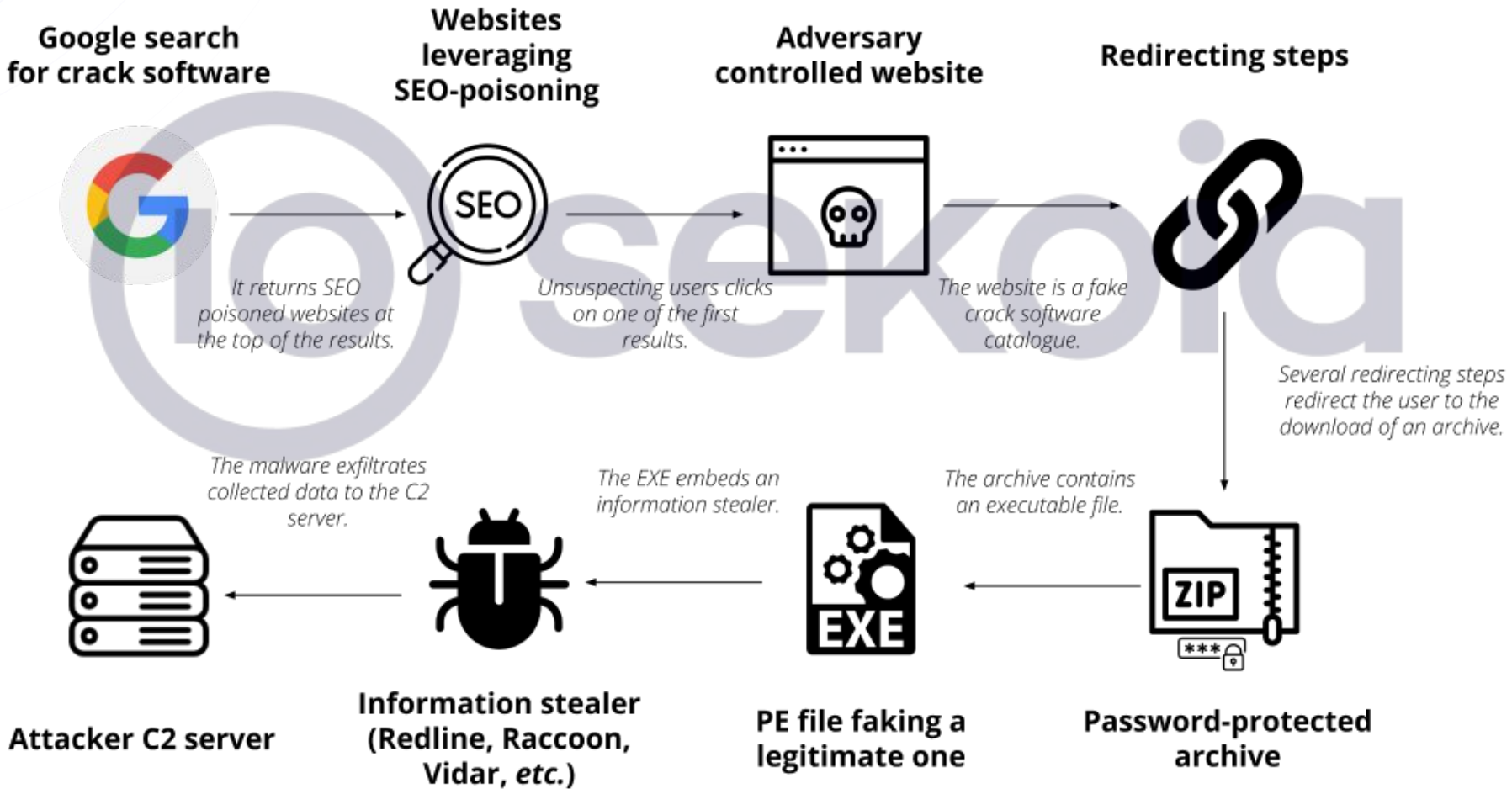
- *malspam*
- *malvertising* (Ads + *landing pages*)
- *phishing* sur les réseaux sociaux
- logiciels crackés
- fausses mises à jour
- documents liés aux affaires

Chaîne d'infection
"911"



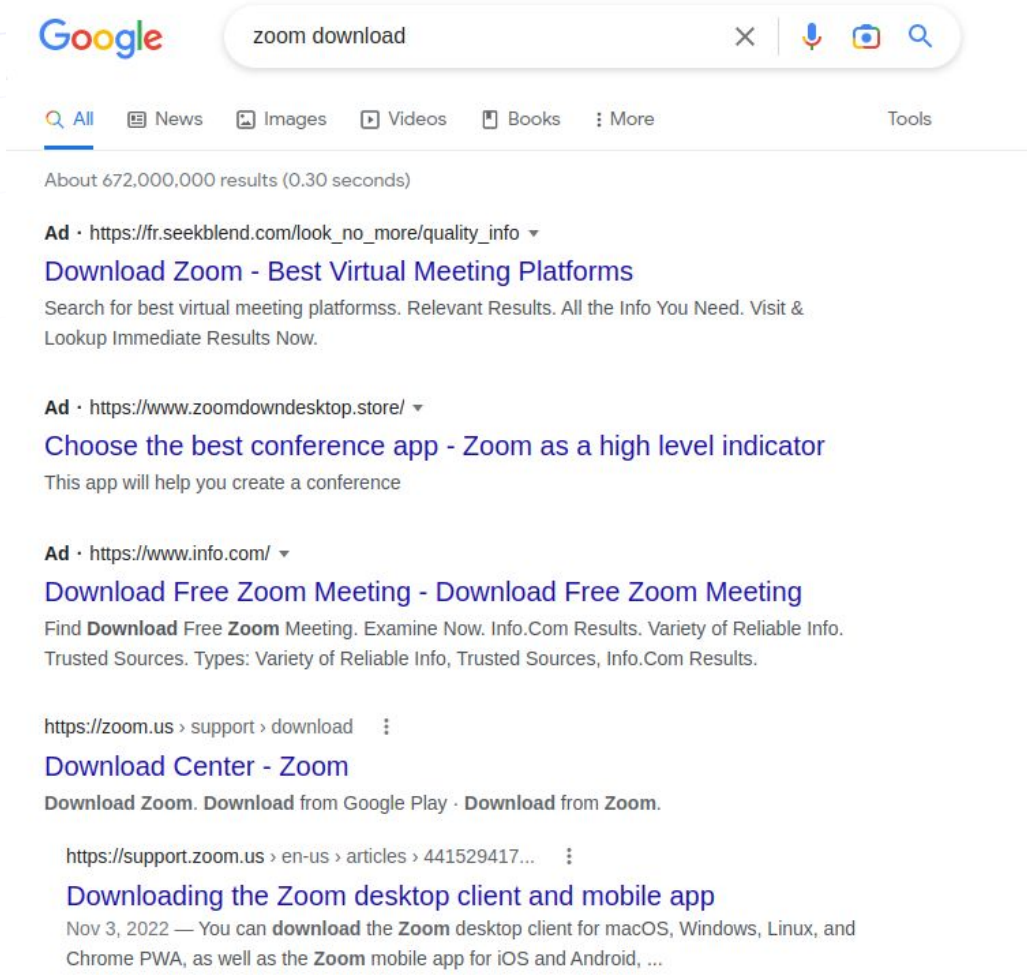
Exemple : sur YouTube, cherchez **"free download crack photoshop"** et observez les descriptions des vidéos récentes

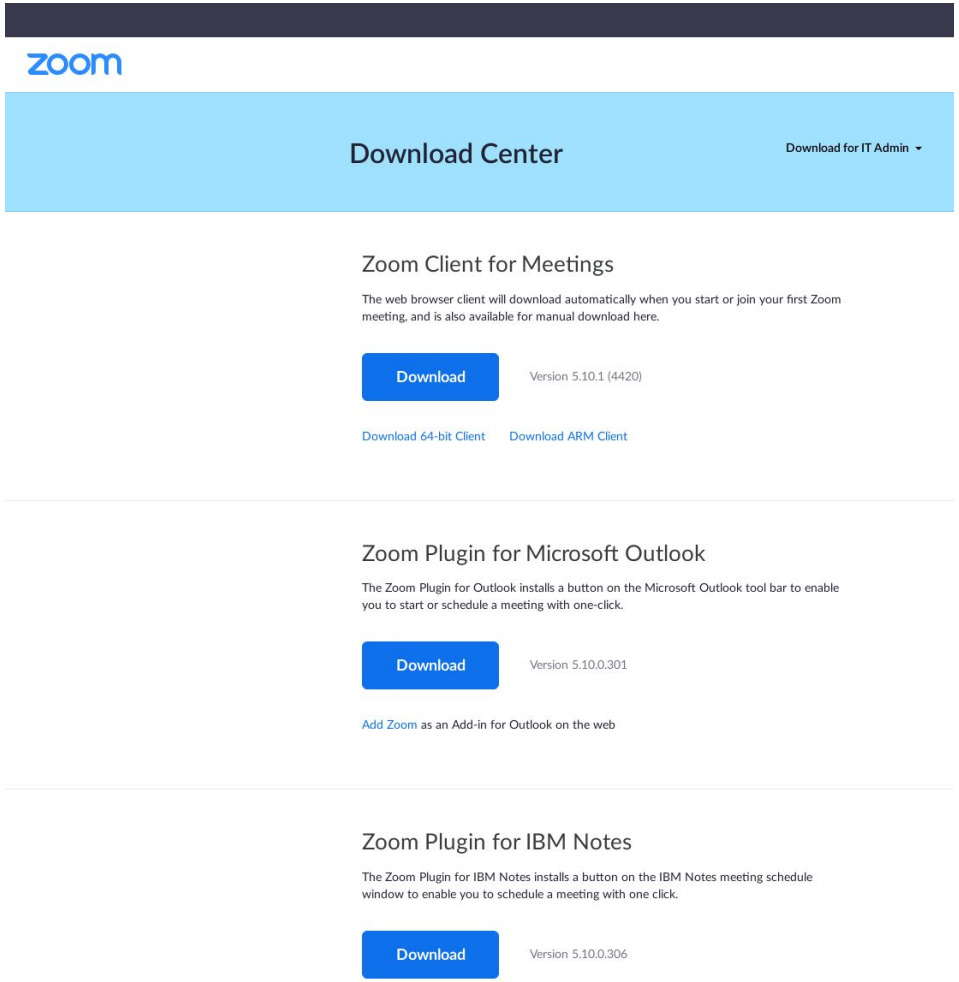
Chaîne d'infection
"empoisonnement par SEO + faux logiciel cracké"



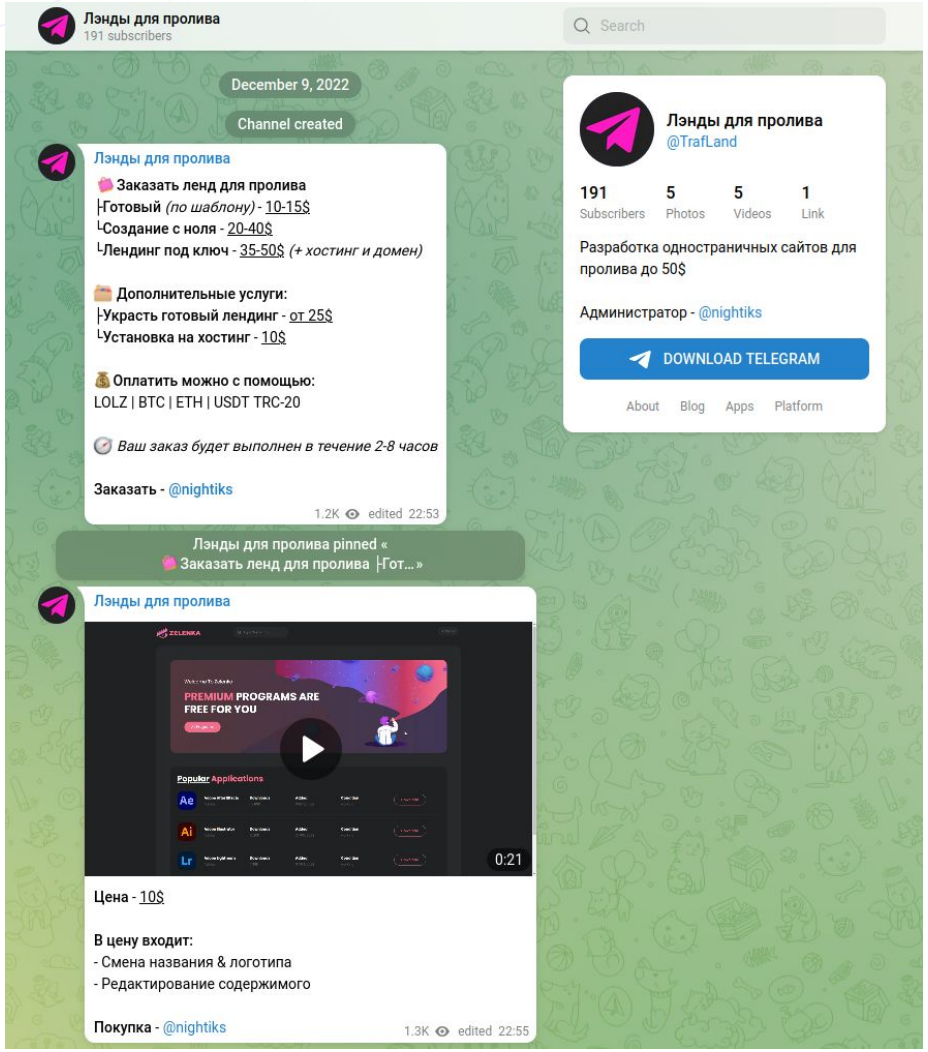
Exemple : sur Google, cherchez **"download crack software"** et observez les premiers résultats.

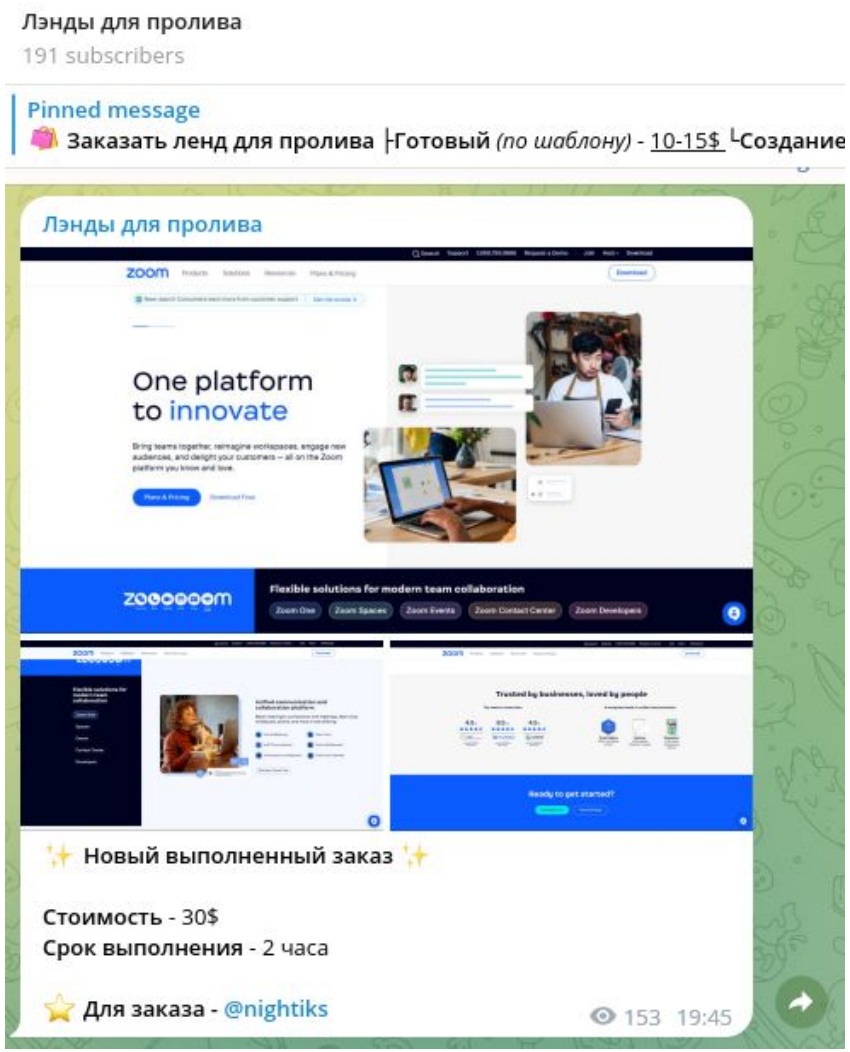
Chaîne d'infection
"malvertising"



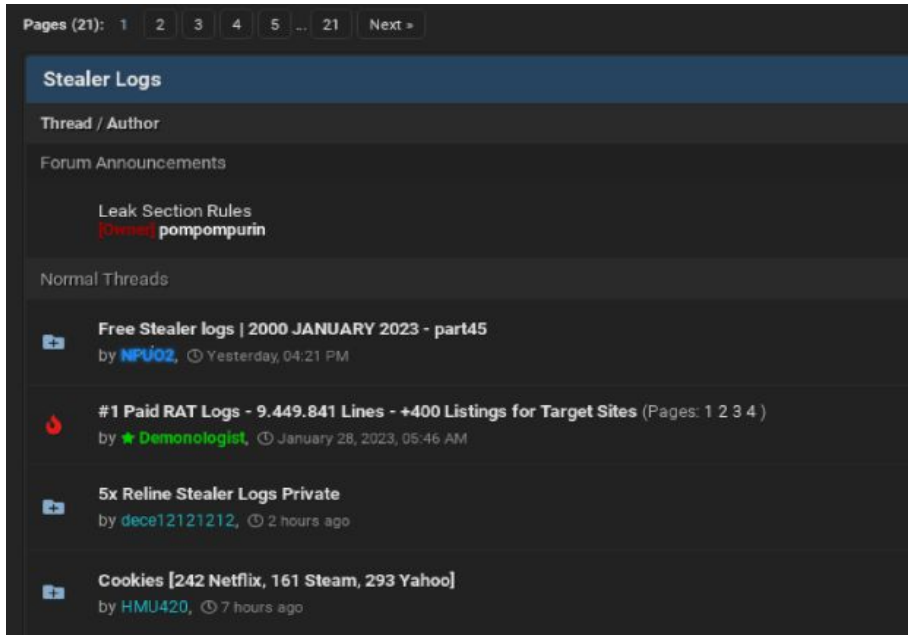


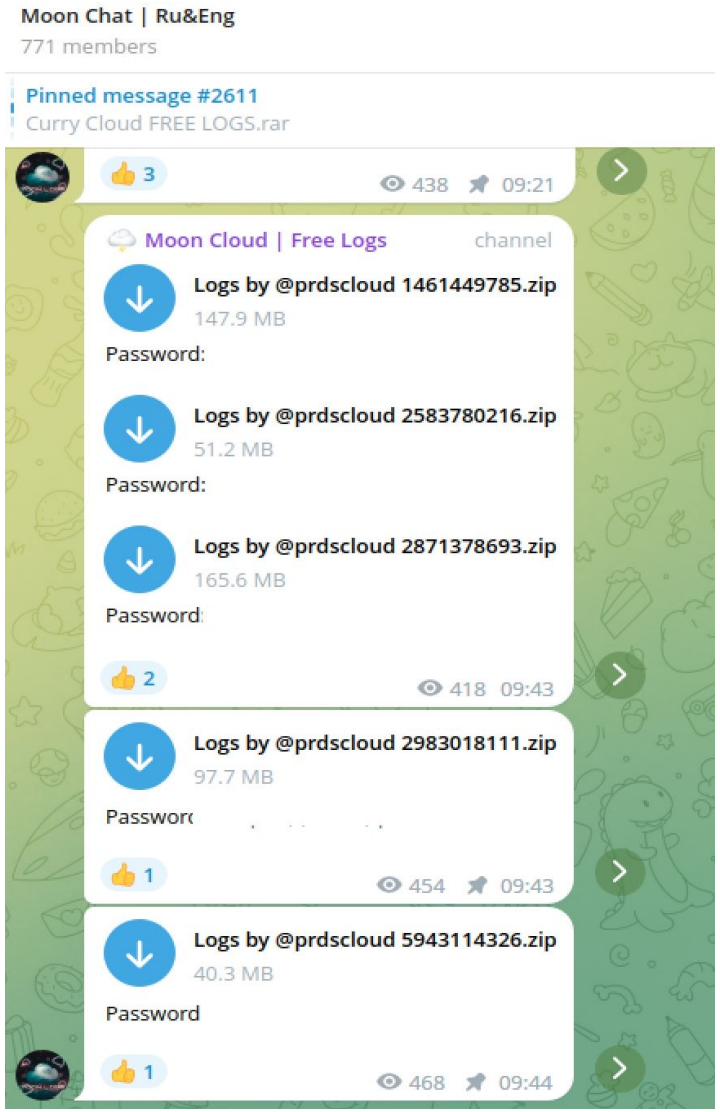
Services tiers
associés à la distribution d'infostealers





Mise en vente de logs collectés





Sources : SQLi Cloud, BreachedForum, Telegram

Mise en vente de *logs* collectés : plateformes centralisées

C22A5B10D4C2A30906204DCE00AF12FF 2023-03-15 17:11:09 2023-03-15 19:41:07	Amazon Live account.battle.net eu.battle.net	Google AppleStore	eu.account.battle.net us.battle.net	Facebook PayPal	0 12 0 = **12** ...known 6 ...other 6	FR 2a01:e0a:a8f:ec50... Windows 10 Enterprise	**17.00**	
65DC0B671AA4685B977D4896FC314D99 2023-03-15 16:26:52 2023-03-15 19:41:07	SFR GitHub account.prusa3d.com accounts.thingiverse.com	Google Orange	accounts.autodesk.com accounts.thingive...	Aliexpress Booking	0 35 0 = **35** ...known 10 ...other 25	FR 2a02:8428:e2c:6a01... Windows 10 Home	**8.00**	
C6F6C54A53A63D83CD51F709EE85F8F0 2023-03-15 14:27:32 2023-03-15 19:41:06	SonyEntertainm... SFR Uber com.contextlogic.wish 9710981p.index-education.net	Leboncoin Live	tv.twitch.android.app	Spotify LidlStore	0 50 0 = **50** ...known 10 ...other 40	FR 78.121... Windows 10 Home	**5.00**	
74724859075A0A6281F22E55090D4A90 2023-03-15 14:26:10 2023-03-15 19:41:06	CDiscountStore Twitter Rakuten SFR CarrefourStore cellmapper.net.cellmapper	Impotsgouv iCloud Aliexpress GitHub Steam	cgeo.geocaching	EasyJet Google Amazon PayPal Orange	0 215 0 = **215** ...known 66 ...other 149	FR 86.73... Windows 7 Home Premium	**48.00**	

Source : Genesis Market

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

Log Parser | Dumper | Сортер | 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 обрабтки.
- Поддерживает 18+ стиллеров
- Каждый скан - расширение функционала
- Если попадаются неизвесные 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.

Sources : XSS forum, LolzGuru

3

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

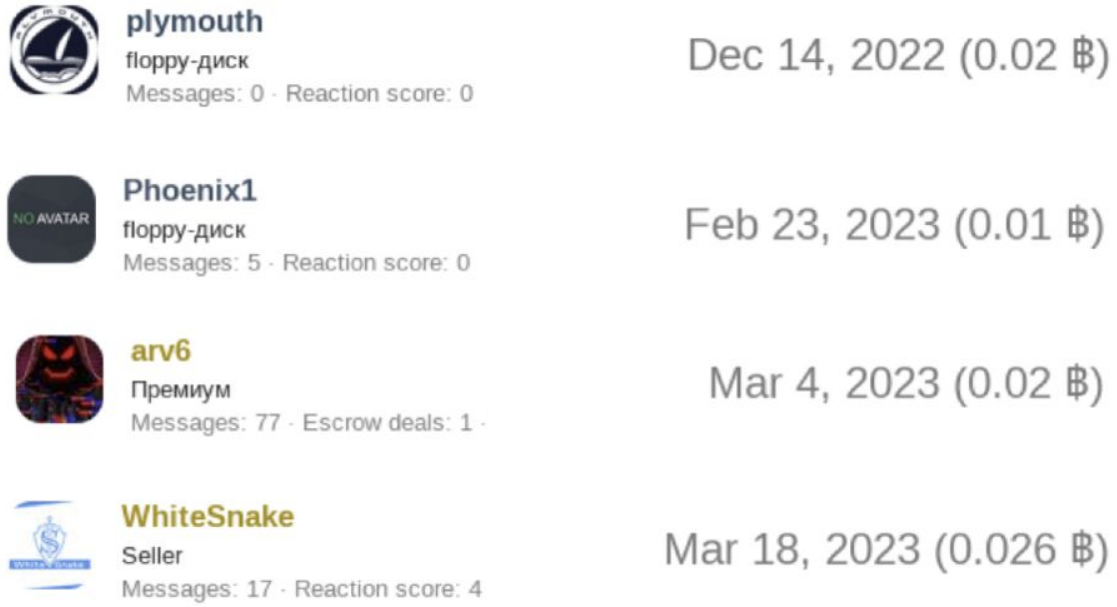
Méthodologie d'investigation et d'analyse
Monitoring et capitalisation

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



Méthodologie d'investigation et d'analyse
Recherche proactive de nouveaux samples

Méthodologie d'investigation et d'analyse

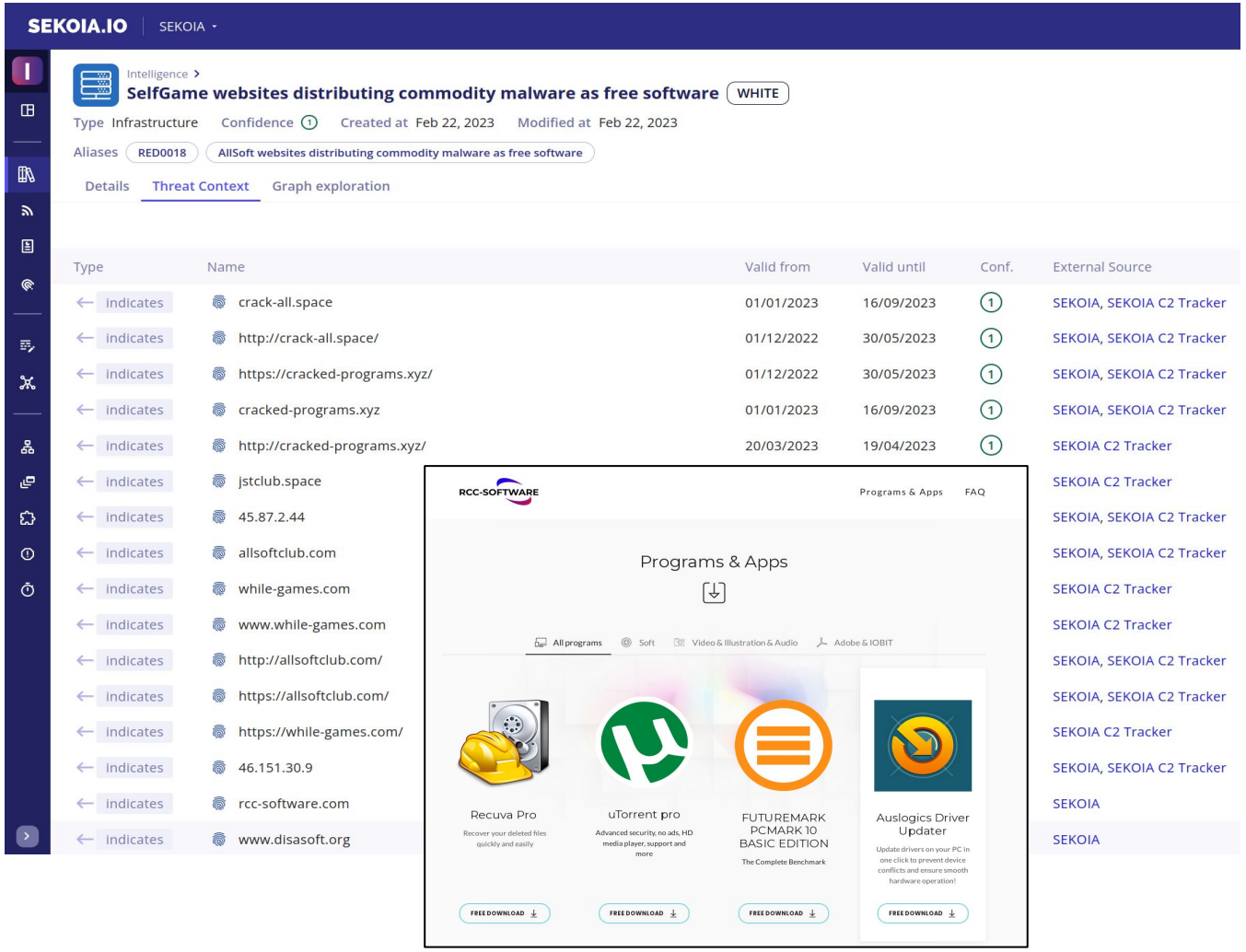
Recherche proactive de nouveaux samples

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



Méthodologie d'investigation et d'analyse

Recherche proactive de nouveaux samples

Écrire des signatures YARA basées sur les données ciblées des :

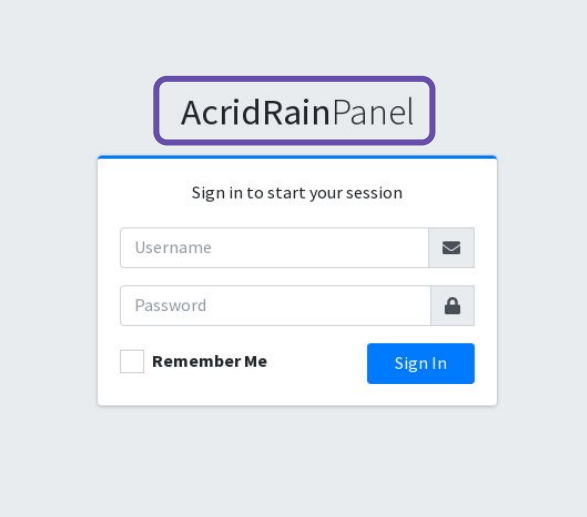
- navigateurs web
- portefeuilles de crypto monnaies (logiciel)
- portefeuilles de crypto monnaies (extensions de navigateur)

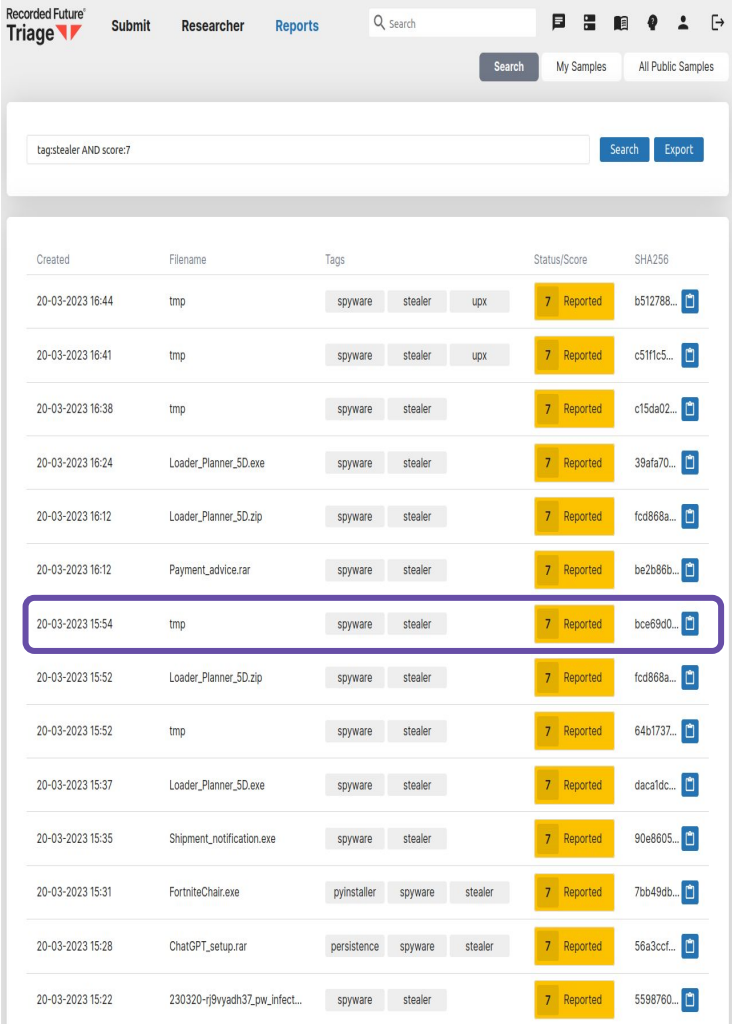
```
strings:
    $str01 = "wallet.dat" wide ascii
    $str07 = "logins.json" wide ascii
    $str08 = "Google\\Chrome\\User Data" wide ascii
    $str09 = "BraveSoftware\\Brave-Browser\\User Data" wide ascii
    $str10 = "Chromium\\User Data" wide ascii
    $str11 = "Opera Software\\Opera " wide ascii
    $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
```

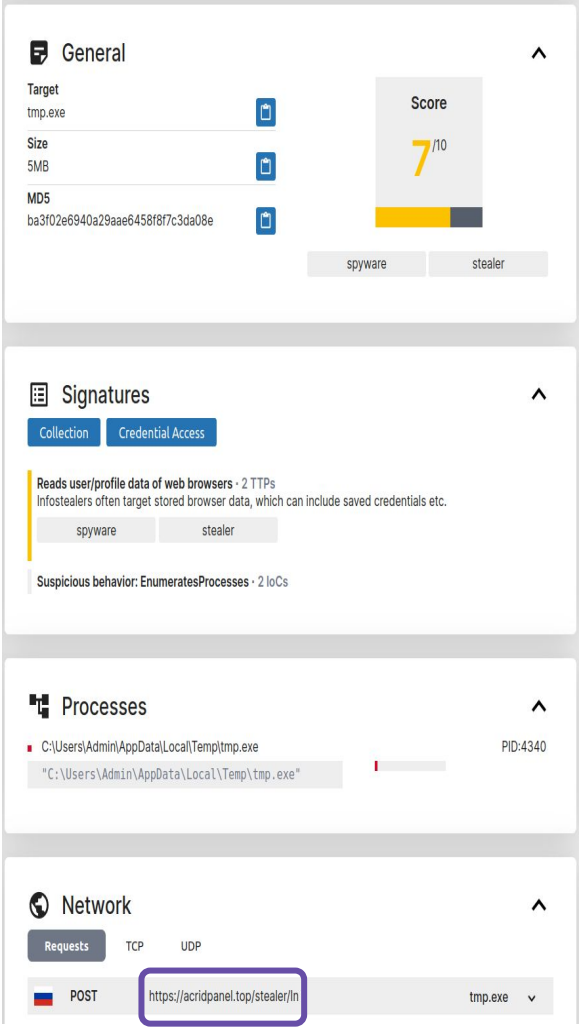
```
strings:
    $sql0 = "SELECT " wide ascii
    $sql1 = "username_value" wide ascii
    $sql2 = "password_value" wide ascii
    $sql3 = " FROM " wide ascii
    $sql4 = "logins" wide ascii
    $sql5 = "moz_cookies" wide ascii
    $sql6 = "moz_places" wide ascii

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







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

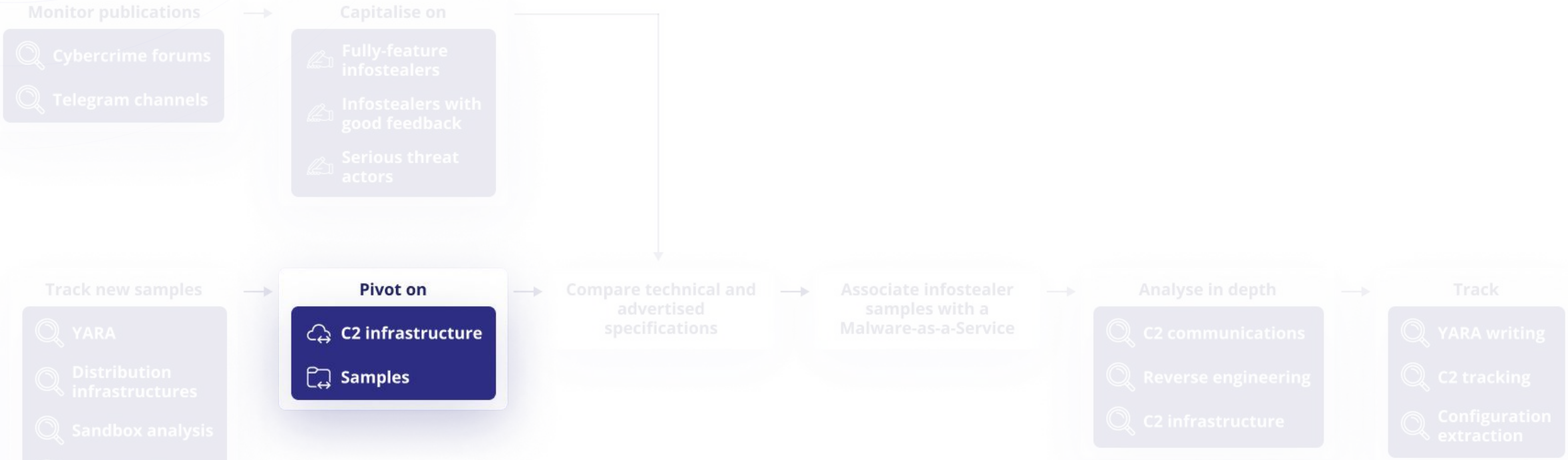
Exemple : bot de suivi des payloads distribués par le loader GCleaner

TDR - Cybercrime bot BOT 09:24

GCleaner PPI payloads tracking - 2023-03-17 09:19:42 - `hxxp://45.12.253.75/addons/_links.json`

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}\/msvcp140\.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/msvcp140.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

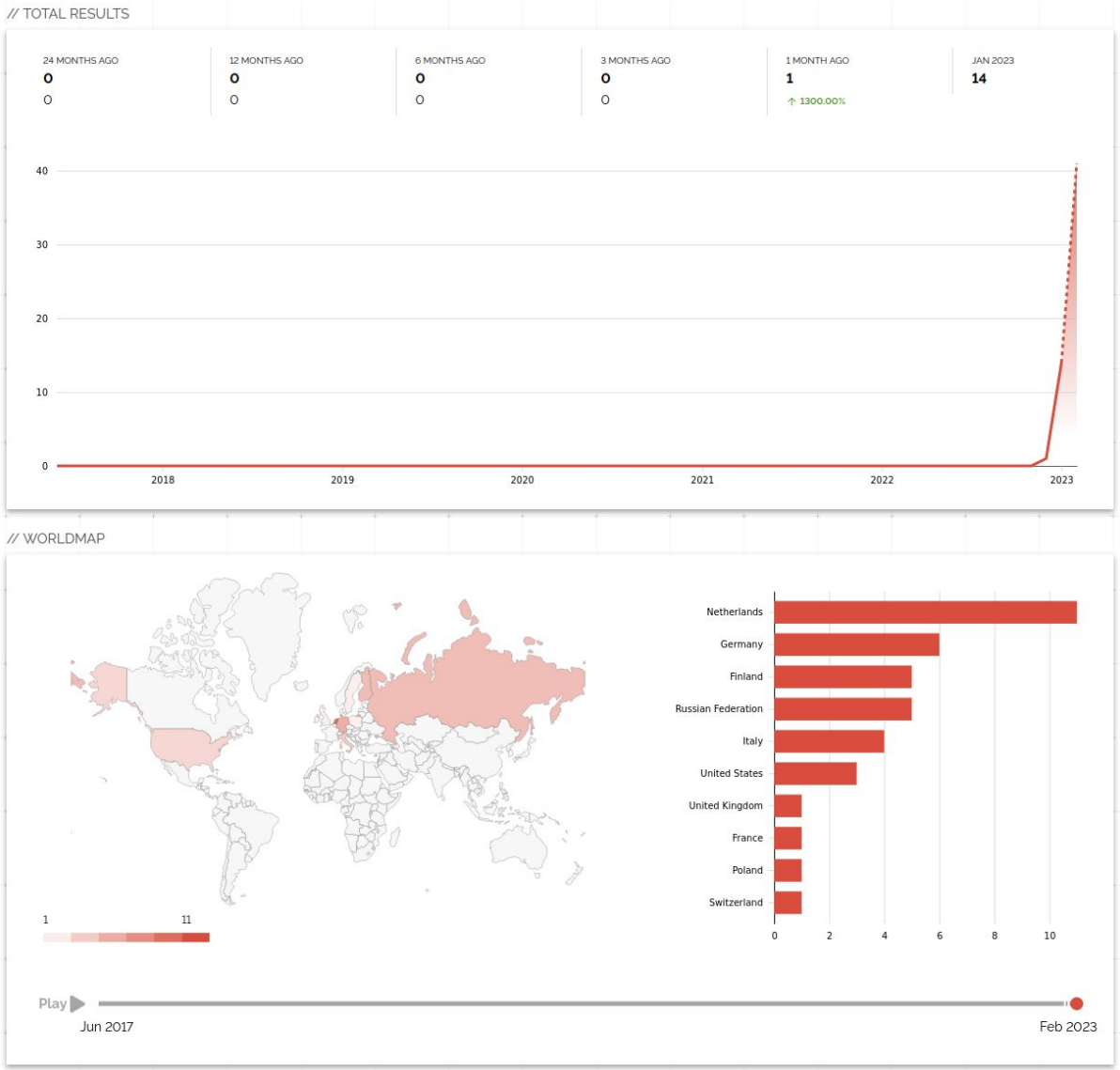
Pivot sur les nouveaux samples

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

- à partir des en-têtes HTTP et HTML :

Janvier 2023

```
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

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

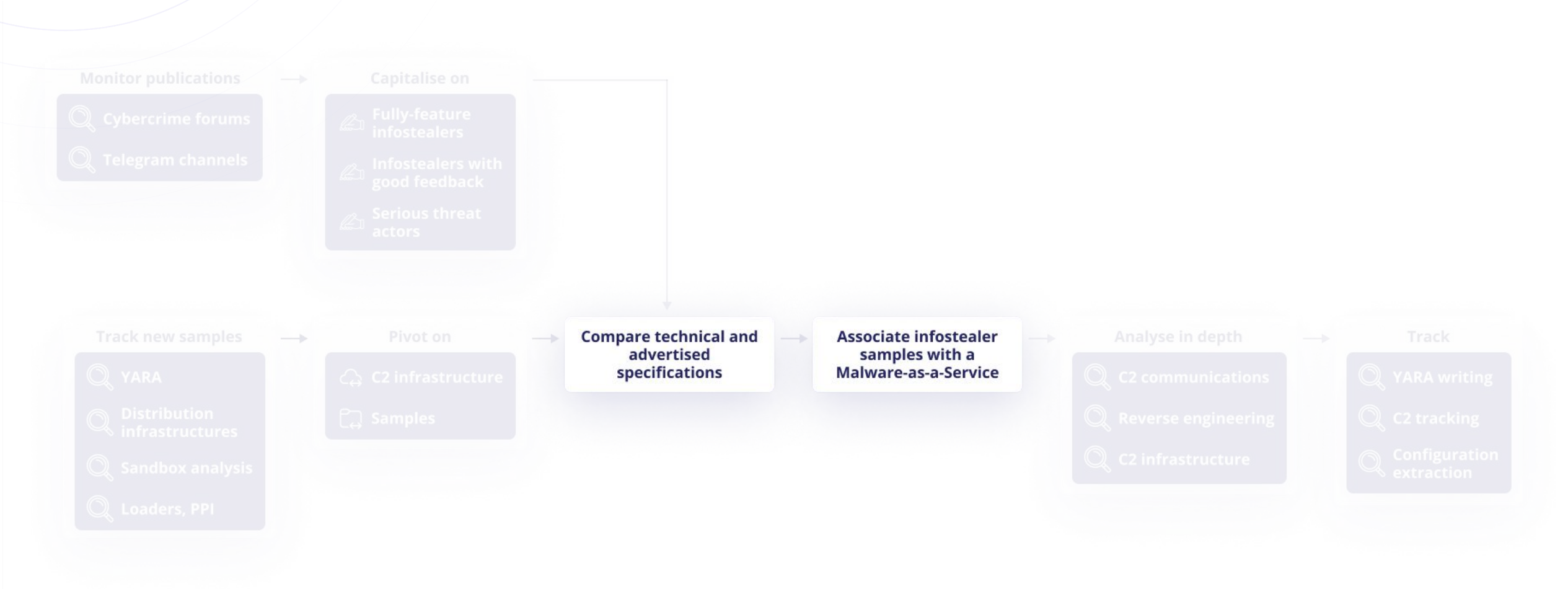


Méthodologie d'investigation et d'analyse

Pivot sur les nouveaux samples

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

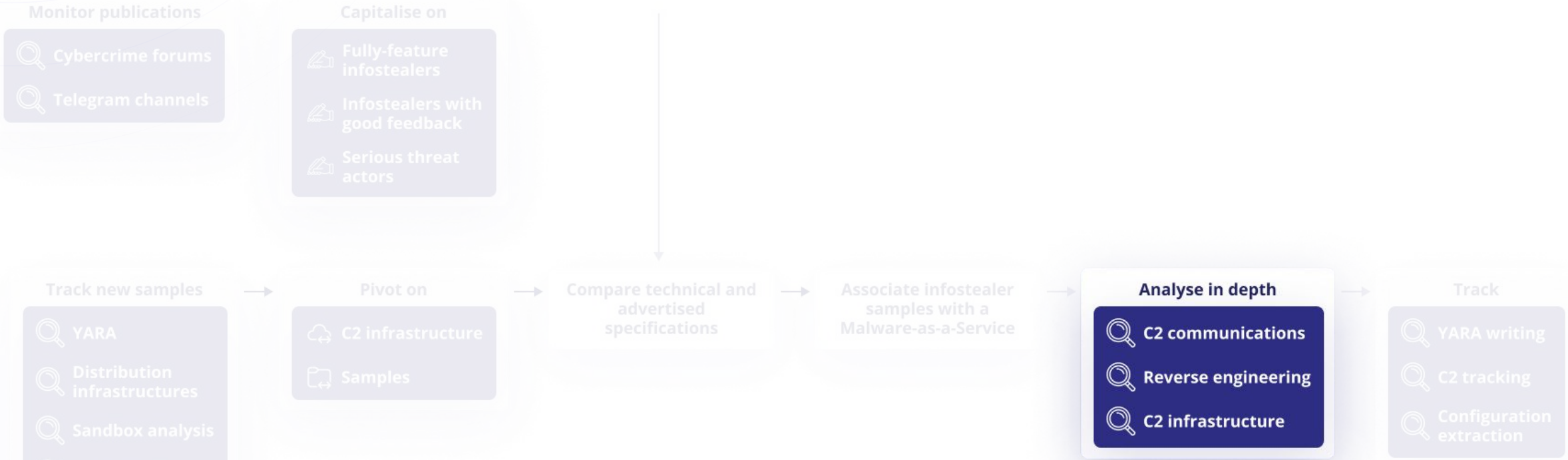
- comparer les caractéristiques techniques et annoncées
- confirmer l’association d’un MaaS et d’une famille d’infostealer

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

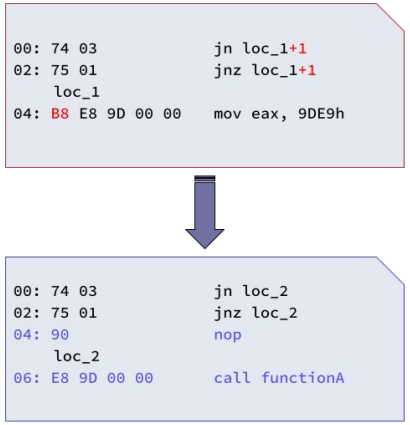
Objectif : comprendre le fonctionnement de l’infostealers d’un point de vue système et réseau

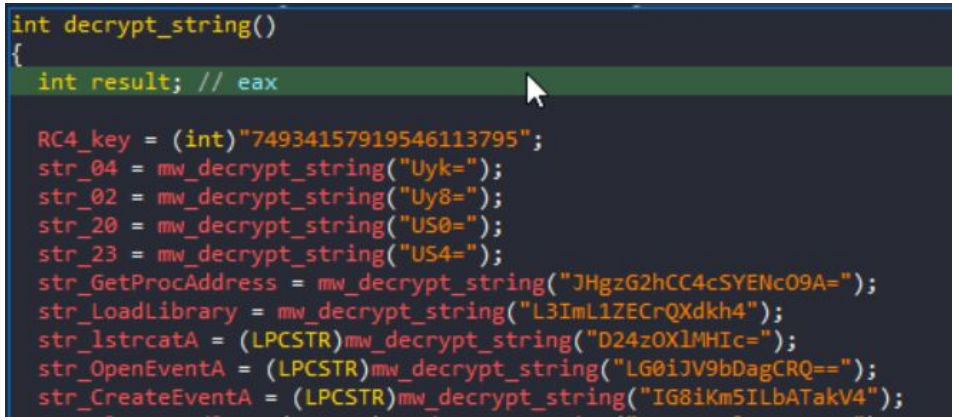
- comparer les caractéristiques techniques observées et celles annoncées
- documenter le malware
- identifier des similarités entre infostealers

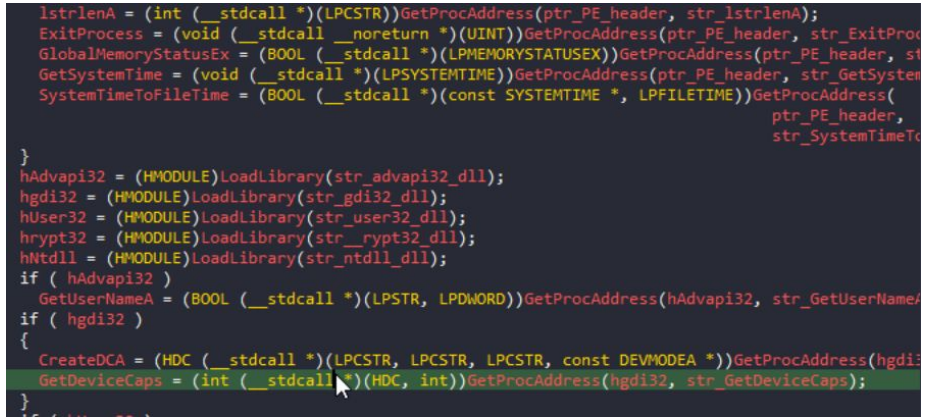
Méthodologie d'investigation et d'analyse

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

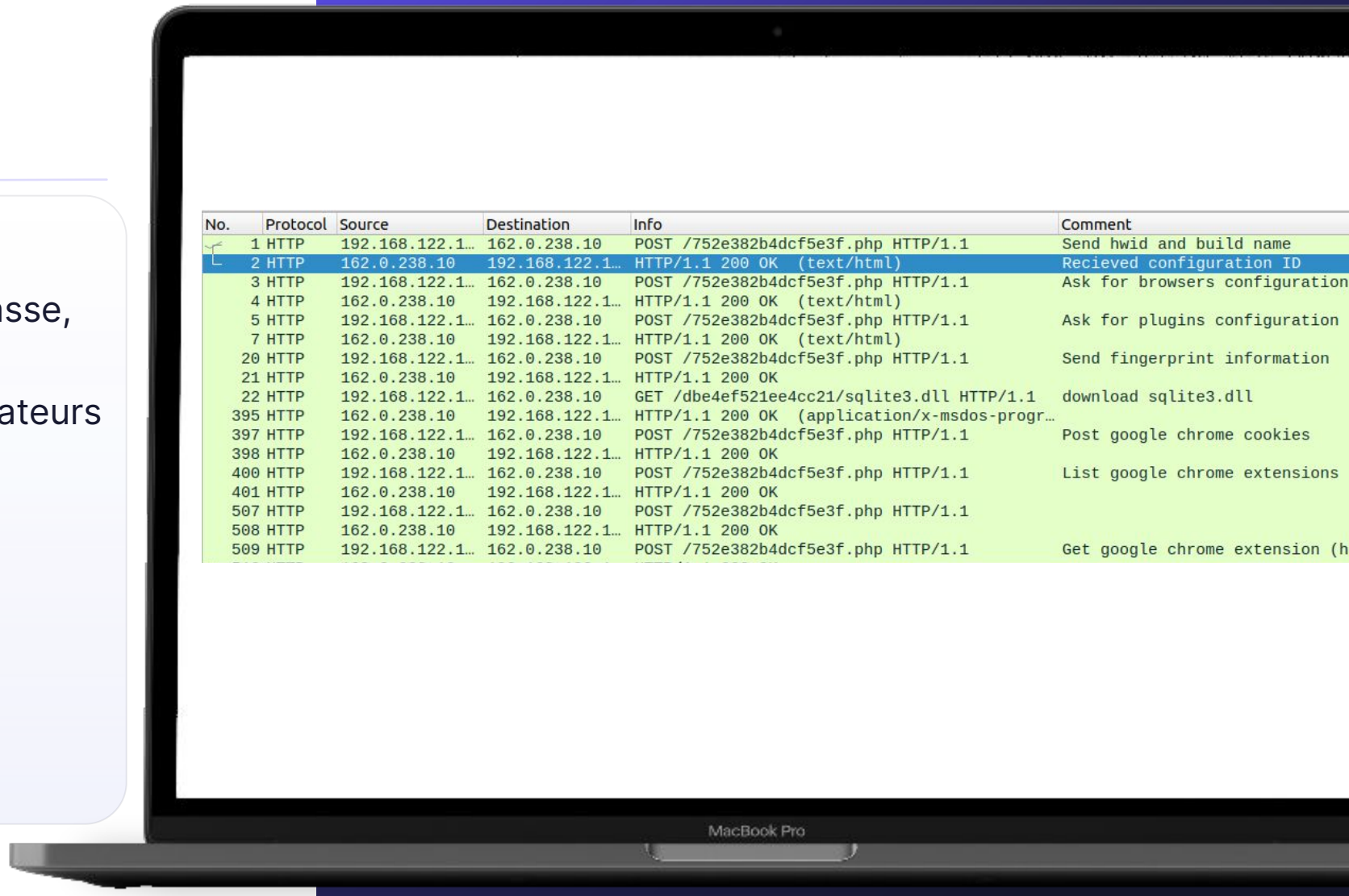






Rétro ingénierie : communications réseaux

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



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

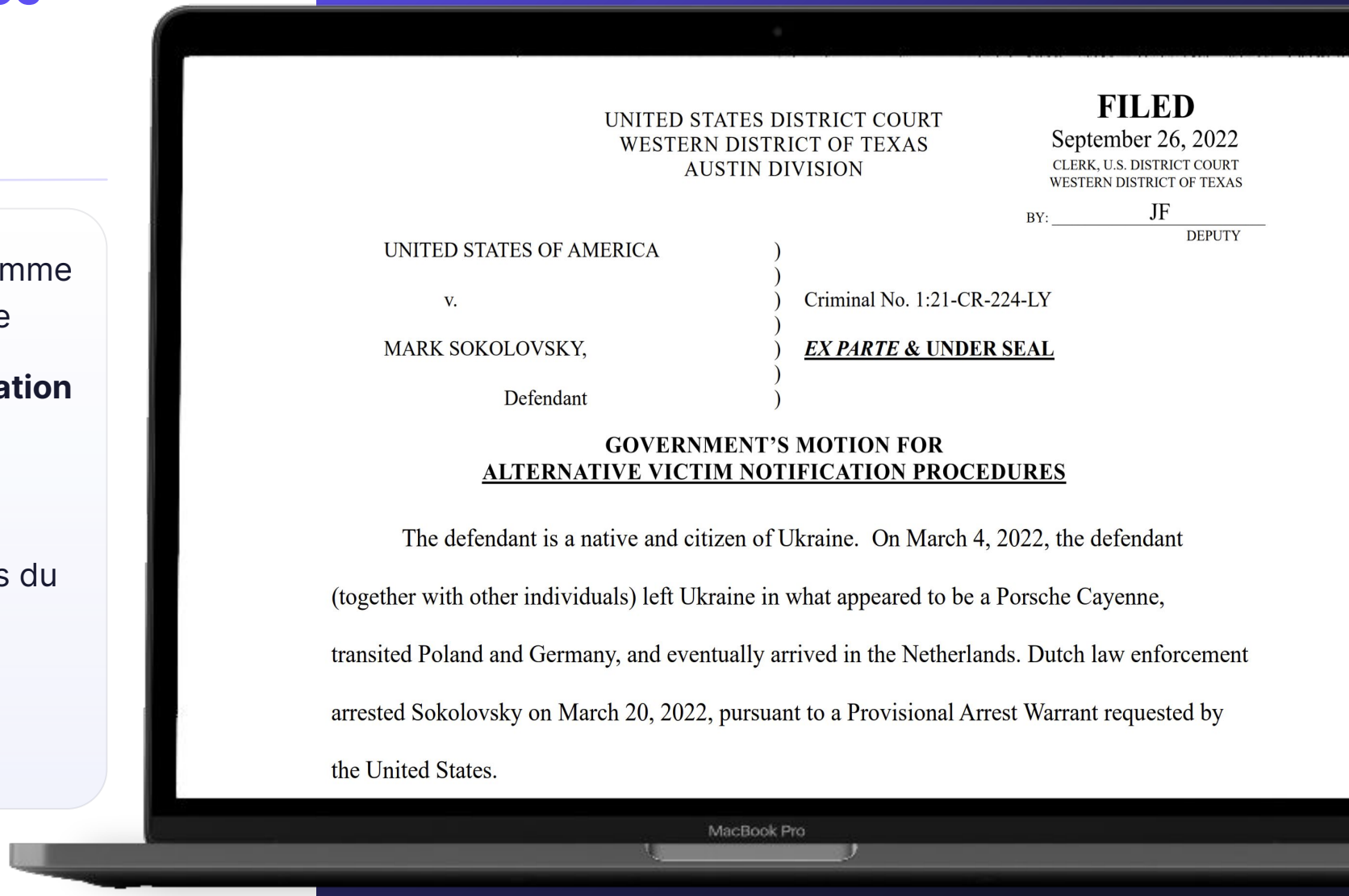
Méthodologie d'investigation et d'analyse
Suivi de la menace dans le temps

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

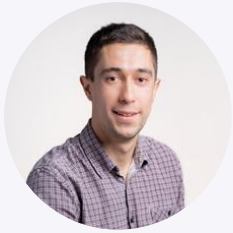
Conclusion : tendances et éléments-clés

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**"



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