GATEWATCHER

PURPLE TEAM
GATEWATCHER

The French stealer ecosystem: *The resurgence of skid gangs in cybercrime landscape*

#WHOAMI_

0xSeeker

Twitter: @Seeker0x
Purple Team @GATEWATCHER

> *Threat Intelligence/Threat Hunting*
> *Security analyst*

PURPLE TEAM
GATEWATCHER

Big Thanks!

Nicolas MF

Linkedin: Nicolas MF

Former intern @Gatewatcher

Genesis of this talk

→ 2024 French cyberattacks:
A wave of attacks saw credentials stolen from streamers to compromise major French companies.

→ Undocumented threat actors:
Our investigation uncovered new, smaller groups behind these attacks, about whom little information was publicly available.

→ Ignoring the smaller threat:
This focus overlooks the threat posed by smaller, more discreet groups, which target individual users and accumulate fewer victims.

Summary_

GATEWATCHER

1

Anatomy
of stealers

2

Anatomy of groups
and their lack of
awareness

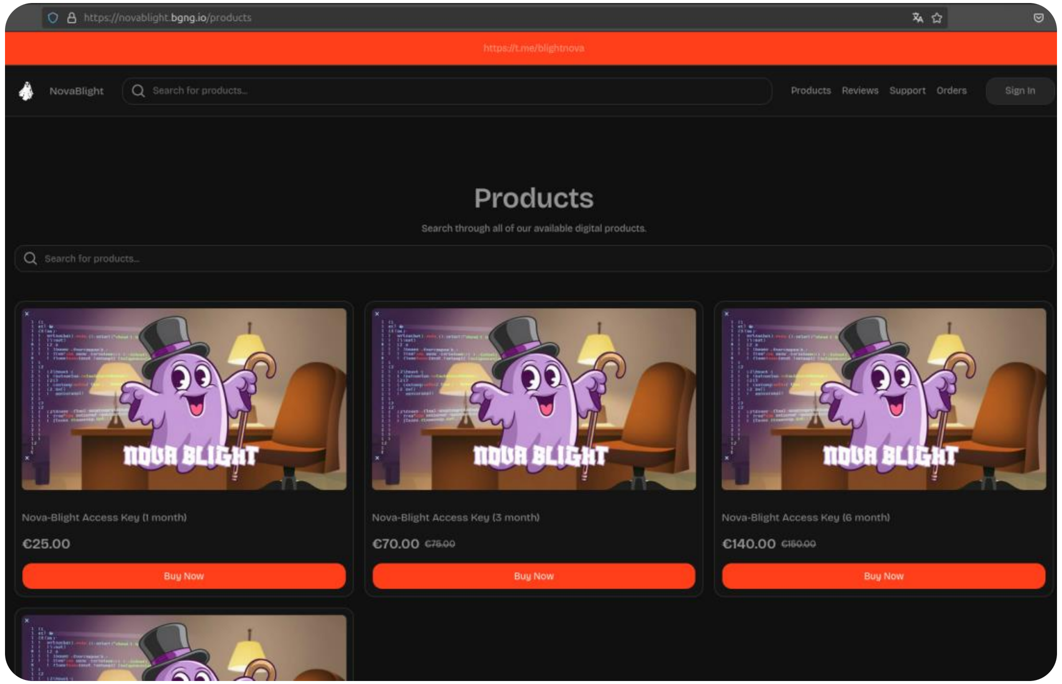
3

Why watching and
understanding them
matters

*Anatomy of Stealer_*

The example of Nova_

- > A representative French threat:
  The sordeal/Nova Group is an ideal case study.
- > Tracking their evolution:
  We've followed the group from their early, less-sophisticated days.



https://novablight.bgng.io/products

https://t.me/blightnova

NovaBlight Search for products... Products Reviews Support Orders Sign In

Products

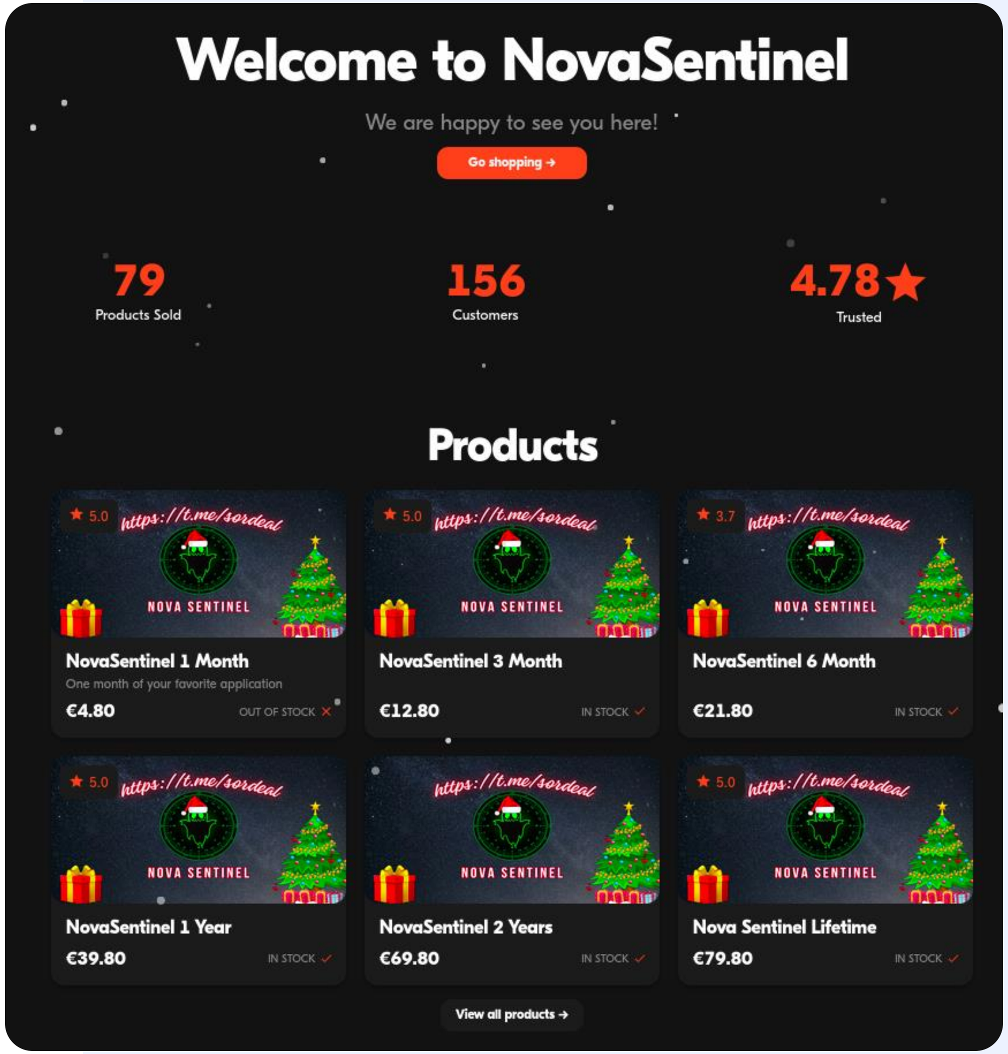
Search through all of our available digital products.

Search for products...

Nova-Blight Access Key (1 month)
€25.00
Buy Now

Nova-Blight Access Key (3 month)
€70.00 ~~€75.00~~
Buy Now

Nova-Blight Access Key (6 month)
€140.00 ~~€150.00~~
Buy Now



Welcome to NovaSentinel

We are happy to see you here!

Go shopping →

79 Products Sold

156 Customers

4.78★ Trusted

Products

★ 5.0 NovaSentinel 1 Month
One month of your favorite application
€4.80 OUT OF STOCK ✕

★ 5.0 NovaSentinel 3 Month
€12.80 IN STOCK ✓

★ 3.7 NovaSentinel 6 Month
€21.80 IN STOCK ✓

★ 5.0 NovaSentinel 1 Year
€39.80 IN STOCK ✓

NovaSentinel 2 Years
€69.80 IN STOCK ✓

★ 5.0 Nova Sentinel Lifetime
€79.80 IN STOCK ✓

View all products →

The evolution_

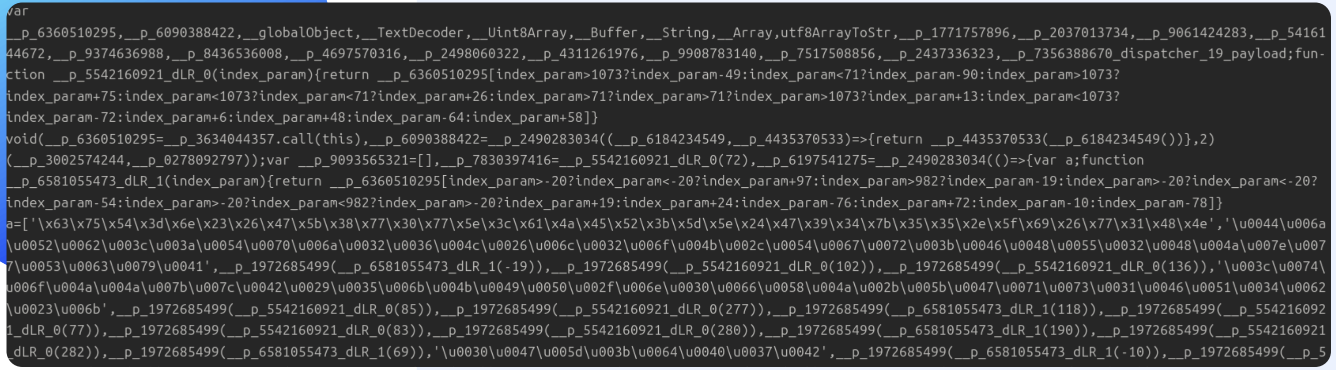
Nova stealer's evolution (2023-2025)

> Enhanced obfuscation:
JS obfuscation still reversible

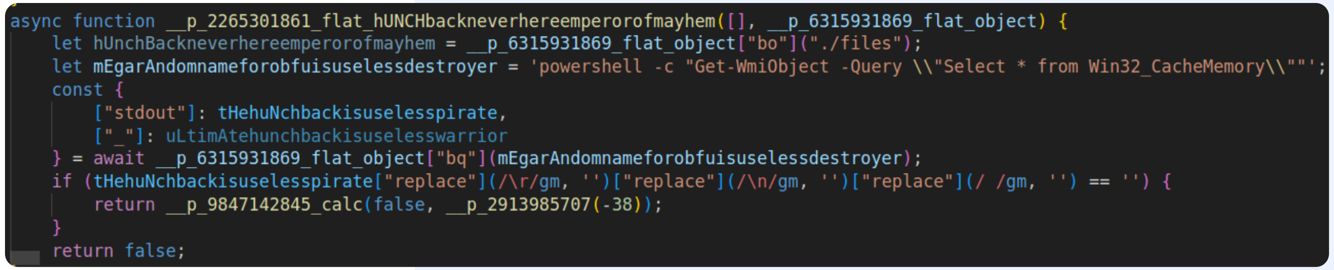
> Targeting high-value data:
cryptocurrency wallets, bank accounts, and password managers

> Frequent rebranding:
The group regularly rebrands its malware

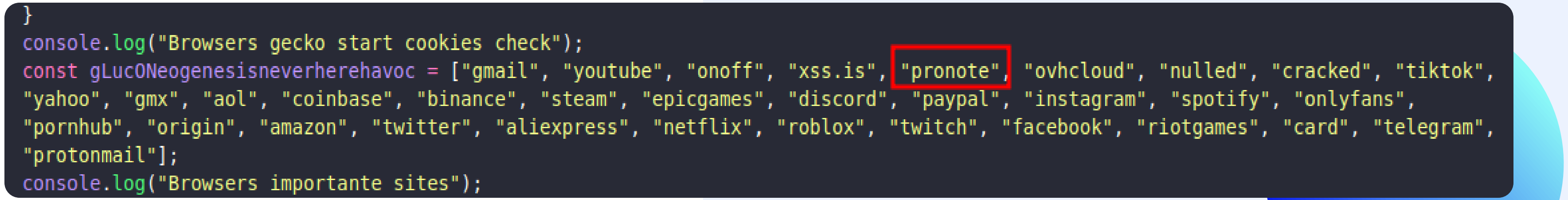
> Develop interfaces:
Better ergonomy and Ux



```
var
__p_6360510295,__p_6090388422,__globalObject,__TextDecoder,__Uint8Array,__Buffer,__String,__Array,utf8ArrayToStr,__p_1771757896,__p_2037013734,__p_9061424283,__p_54161
44672,__p_9374636988,__p_8436536008,__p_4697570316,__p_2498060322,__p_4311261976,__p_9908783140,__p_7517508856,__p_2437336323,__p_7356388670_dispatcher_19_payload;fun-
ction __p_5542160921_dLR_0(index_param){return __p_6360510295[index_param>1073?index_param-49:index_param<71?index_param-90:index_param>1073?
index_param+75:index_param<1073?index_param<71?index_param+26:index_param>71?index_param>71?index_param>1073?index_param+13:index_param<1073?
index_param-72:index_param+6:index_param+48:index_param-64:index_param+58]}
void(__p_6360510295=__p_3634044357.call(this),__p_6090388422=__p_2490283034((__p_6184234549,__p_4435370533)=>{return __p_4435370533(__p_6184234549())},2)
(__p_3002574244,__p_0278092797));var __p_9093565321=[],__p_7830397416=__p_5542160921_dLR_0(72),__p_6197541275=__p_2490283034(()=>{var a;function
__p_6581055473_dLR_1(index_param){return __p_6360510295[index_param>-20?index_param<-20?index_param+97:index_param>982?index_param-19:index_param>-20?index_param<-20?
index_param-54:index_param>-20?index_param<982?index_param>-20?index_param+19:index_param+24:index_param-76:index_param+72:index_param-10:index_param-78]}
a=['\x63\x75\x54\x3d\x6e\x23\x26\x47\x5b\x38\x77\x30\x77\x5e\x3c\x61\x4a\x45\x52\x3b\x5d\x5e\x24\x47\x39\x34\x7b\x35\x35\x2e\x5f\x69\x26\x77\x31\x48\x4e','\u0044\u006a
\u0052\u0062\u003c\u003a\u0054\u0070\u006a\u0032\u0036\u004c\u0026\u006c\u0032\u006f\u004b\u002c\u0054\u0067\u0072\u003b\u0046\u0048\u0055\u0032\u0048\u004a\u007e\u007
7\u0053\u0063\u0079\u0041',__p_1972685499(__p_6581055473_dLR_1(-19)),__p_1972685499(__p_5542160921_dLR_0(102)),__p_1972685499(__p_5542160921_dLR_0(136)),'\u003c\u0074\
u006f\u004a\u004a\u007b\u007c\u0042\u0029\u0035\u006b\u004b\u0049\u0050\u002f\u006e\u0030\u0066\u0058\u004a\u002b\u005b\u0047\u0071\u0073\u0031\u0046\u0051\u0034\u0062
\u0023\u006b',__p_1972685499(__p_5542160921_dLR_0(85)),__p_1972685499(__p_5542160921_dLR_0(277)),__p_1972685499(__p_6581055473_dLR_1(118)),__p_1972685499(__p_554216092
1_dLR_0(77)),__p_1972685499(__p_5542160921_dLR_0(83)),__p_1972685499(__p_5542160921_dLR_0(280)),__p_1972685499(__p_6581055473_dLR_1(190)),__p_1972685499(__p_5542160921
_dLR_0(282)),__p_1972685499(__p_6581055473_dLR_1(69)),'\u0030\u0047\u005d\u003b\u0064\u0040\u0037\u0042',__p_1972685499(__p_6581055473_dLR_1(-10)),__p_1972685499(__p_5
```



```
async function __p_2265301861_flat_hUNCHbackneverhereemperorofmayhem([], __p_6315931869_flat_object) {
    let hUnchBackneverhereemperorofmayhem = __p_6315931869_flat_object["bo"]("./files");
    let mEgarAndomnameforobfuisuselessdestroyer = 'powershell -c "Get-WmiObject -Query \\"Select * from Win32_CacheMemory\\""';
    const {
        ["stdout"]: tHehuNchbackisuselesspirate,
        ["_"]: uLtimAtehunchbackisuselesswarrior
    } = await __p_6315931869_flat_object["bq"](mEgarAndomnameforobfuisuselessdestroyer);
    if (tHehuNchbackisuselesspirate["replace"](/\r/gm, '')["replace"](/\n/gm, '')["replace"](/ /gm, '') == '') {
        return __p_9847142845_calc(false, __p_2913985707(-38));
    }
    return false;
```

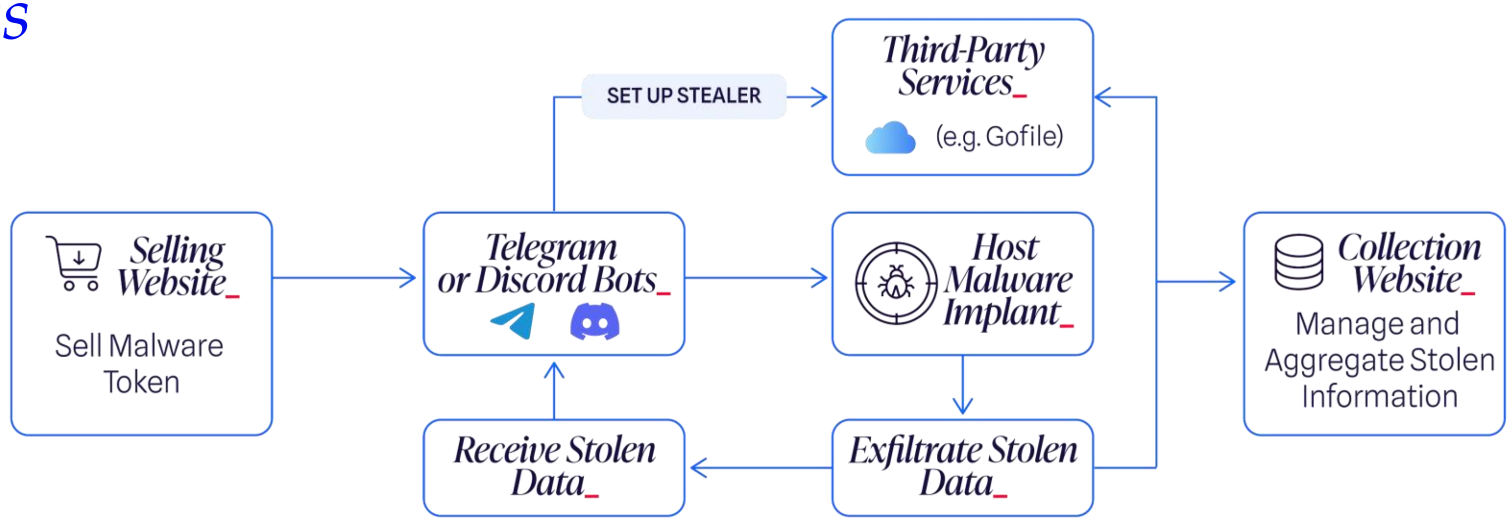


```
}
console.log("Browsers gecko start cookies check");
const gLucONeogenesisneverherehavoc = ["gmail", "youtube", "onoff", "xss.is", "pronote", "ovhcloud", "nulled", "cracked", "tiktok",
"yahoo", "gmx", "aol", "coinbase", "binance", "steam", "epicgames", "discord", "paypal", "instagram", "spotify", "onlyfans",
"pornhub", "origin", "amazon", "twitter", "aliexpress", "netflix", "roblox", "twitch", "facebook", "riotgames", "card", "telegram",
"protonmail"];
console.log("Browsers importante sites");
```

How it works (still pretty simple)_

Key Infrastructure Elements

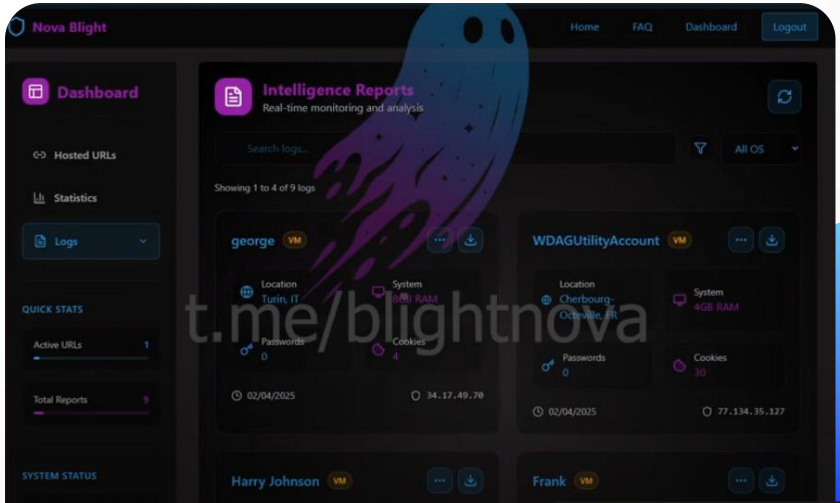
- Selling Website
- Telegram/Discord Bots: Used to set up the stealer and receive stolen data.
- Third-Party storage Services
- Data Collection Website: A dedicated platform for stolen information.



Process Flow_

P1 (Build Parameters via Bot) › P2 (Host Implant on Gofile) › P3(Collect Stolen Data via Website)

How it works (still pretty simple)_
Dashboard



Active URLs 1

Total Reports 9

● All Systems Operational

Intelligence Reports
Real-time monitoring and analysis

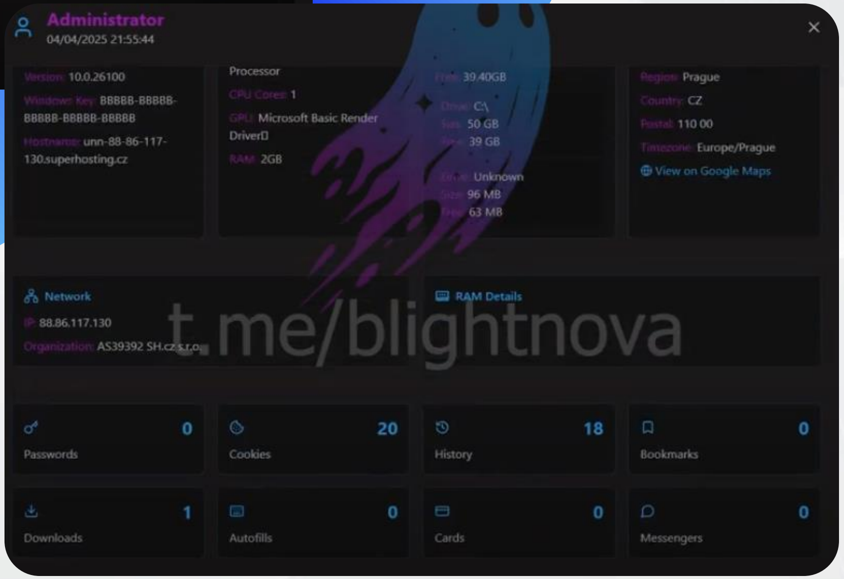
Showing 1 to 4 of 9 logs

george VM
Location Turin, IT
System 8GB RAM
Passwords 0
Cookies 4
02/04/2025 34.17.49.70

WDAGUtilityAccount VM
Location Cherbourg-Octeville, FR
System 4GB RAM
Passwords 0
Cookies 30
02/04/2025 77.134.35.127

Harry Johnson VM
Location Köln, DE
System 16GB RAM
Passwords
Cookies

Frank VM



Administrator
04/04/2025 21:55:44

Version: 10.0.26100
Windows Key: BBBBB-BBBBB-BBBBB-BBBBB-BBBBB
Hostname: unn-88-86-117-130.superhosting.cz

Processor
CPU Cores: 1
GPU: Microsoft Basic Render Driver□
RAM: 2GB

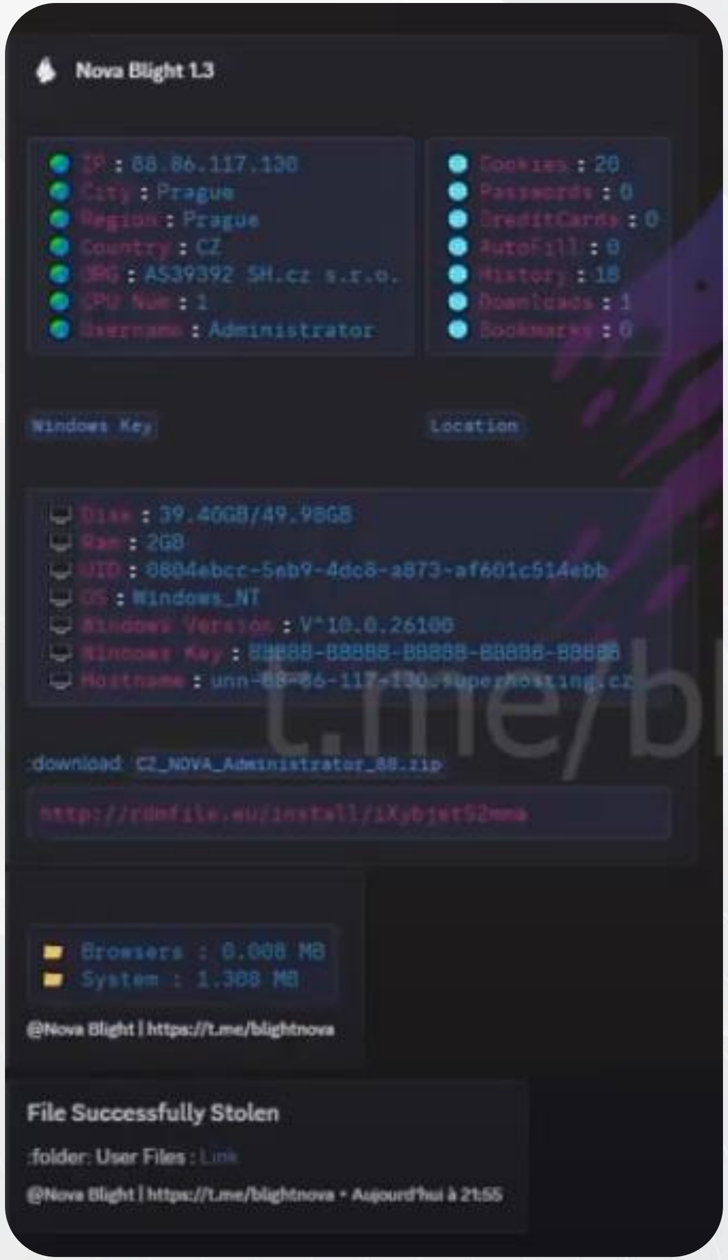
Free: 39.40GB
Drive: C:\
Size: 50 GB
Free: 39 GB
Drive: Unknown
Size: 96 MB
Free: 63 MB

Region: Prague
Country: CZ
Postal: 110 00
Timezone: Europe/Prague

Network
IP: 88.86.117.130
Organization: AS39392 SH.cz s.r.o.

RAM Details

Passwords	0
Cookies	20
History	18
Bookmarks	0
Downloads	1
Autofills	0
Cards	0
Messengers	0



Nova Blight 1.3

```
IP : 88.86.117.130              Cookies : 20
City : Prague                   Passwords : 0
Region : Prague                 CreditCards : 0
Country : CZ                    AutoFill : 0
ORG : AS39392 SH.cz s.r.o.      History : 18
CPU Num : 1                     Downloads : 1
Username : Administrator        Bookmarks : 0

Windows Key                     Location

Disk : 39.40GB/49.98GB
Ram : 2GB
UID : 0804ebcc-5eb9-4dc8-a873-af601c514ebb
OS : Windows_NT
Windows Version : V^10.0.26100
Windows Key : BBBBB-BBBBB-BBBBB-BBBBB-BBBBB
Hostname : unn-88-86-117-130.superhosting.cz
```

:download: CZ_NOVA_Administrator_88.zip

```
http://rdmfile.eu/install/iXybjet52mma
```

```
Browsers : 0.008 MB
System : 1.308 MB
```

@Nova Blight | https://t.me/blightnova

File Successfully Stolen

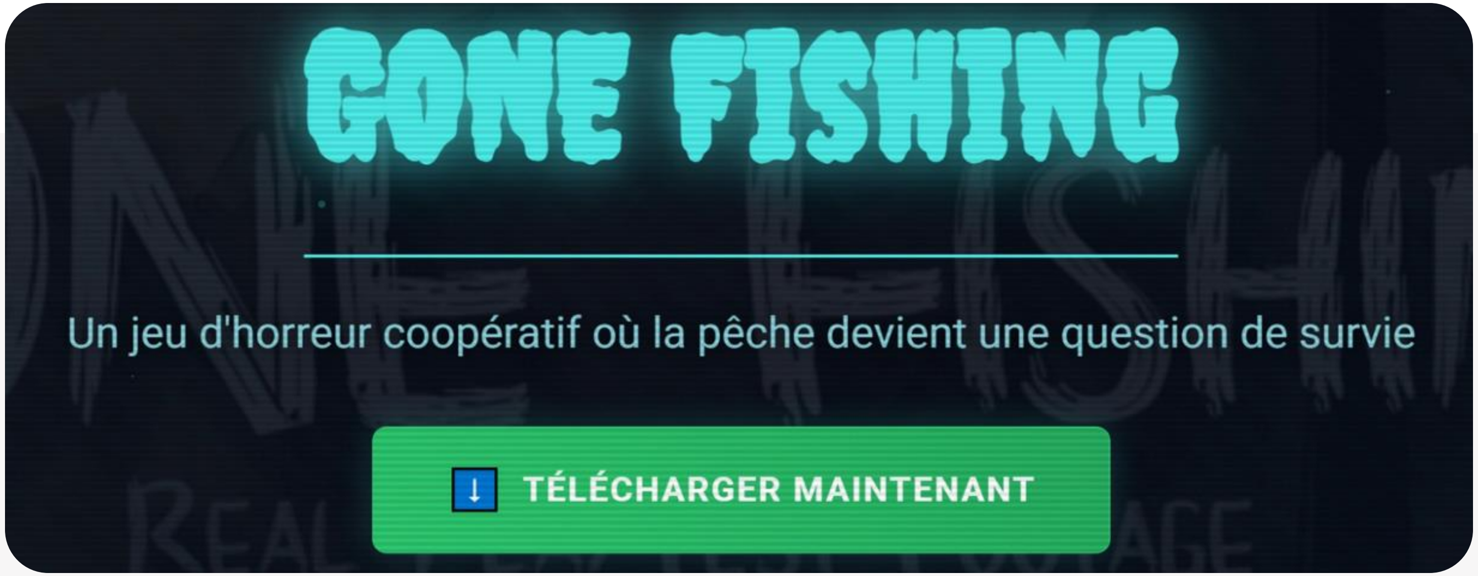
:folder: User Files : Link

@Nova Blight | https://t.me/blightnova • Aujourd'hui à 21:55

Spreading the malware_

Targeting and distribution

- Focus on personal users:
  Nova's distribution methods, such as fake video streaming sites and video game cheats, demonstrate a clear focus on individual, not corporate, targets.
- Corroborating evidence:
  The nature of the stolen data, a large volume of personal accounts and credentials, supports this conclusion, further distinguishing Nova from groups that target corporate networks.



GONE FISHING

Un jeu d'horreur coopératif où la pêche devient une question de survie

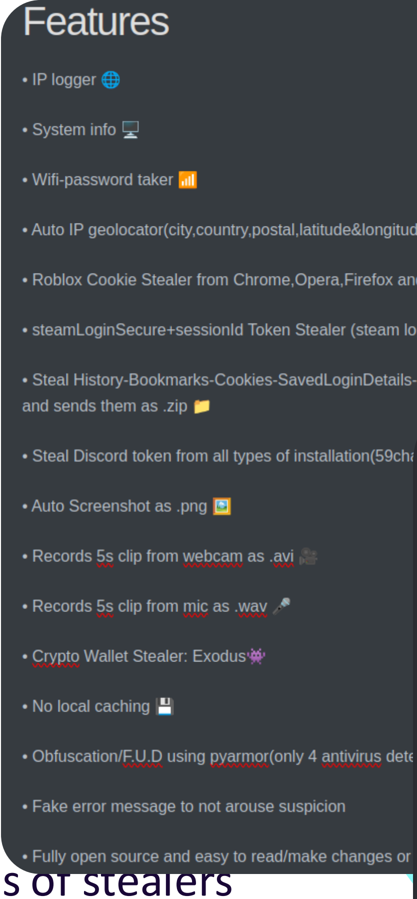
Similarities with opensource tools_

A broader ecosystem

> **Widespread Techniques**

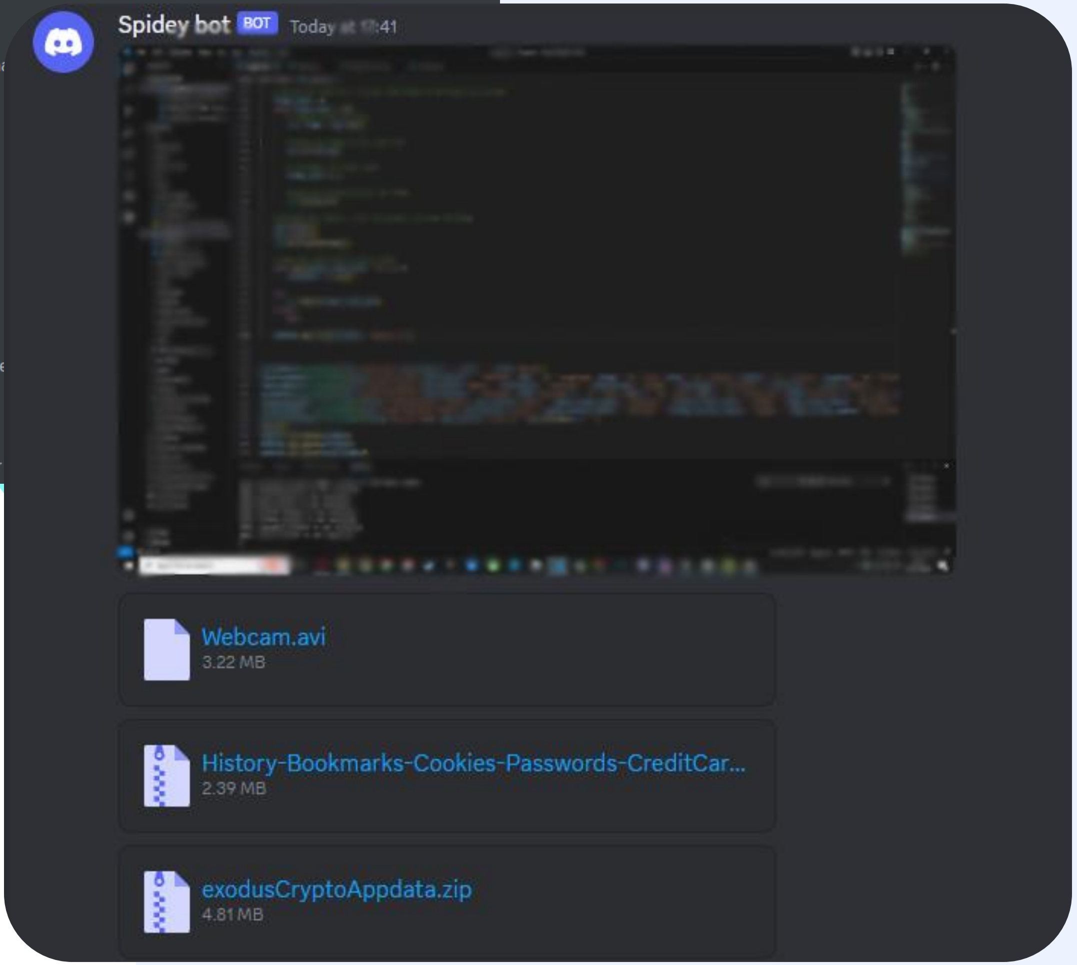
> **Common Infrastructure**

> **Shared Targets**



Features

- IP logger 🌐
- System info 🖥️
- Wifi-password taker 📶
- Auto IP geolocator(city,country,postal,latitude&longitude) 🌎
- Roblox Cookie Stealer from Chrome,Opera,Firefox and Edge 🍪
- steamLoginSecure+sessionId Token Stealer (steam login cookie) from Chrome(not a client) 🎧
- Steal History-Bookmarks-Cookies-SavedLoginDetails-BrowserAutofill-CreditCards from basically all chromium browsers and sends them as .zip 📁
- Steal Discord token from all types of installation(59cha
- Auto Screenshot as .png 🖼️
- Records 5s clip from webcam as .avi 🎥
- Records 5s clip from mic as .wav 🎤
- Crypto Wallet Stealer: Exodus👾
- No local caching 💾
- Obfuscation/F.U.D using pyarmor(only 4 antivirus dete
- Fake error message to not arouse suspicion
- Fully open source and easy to read/make changes or



Spidey bot BOT Today at 17:41

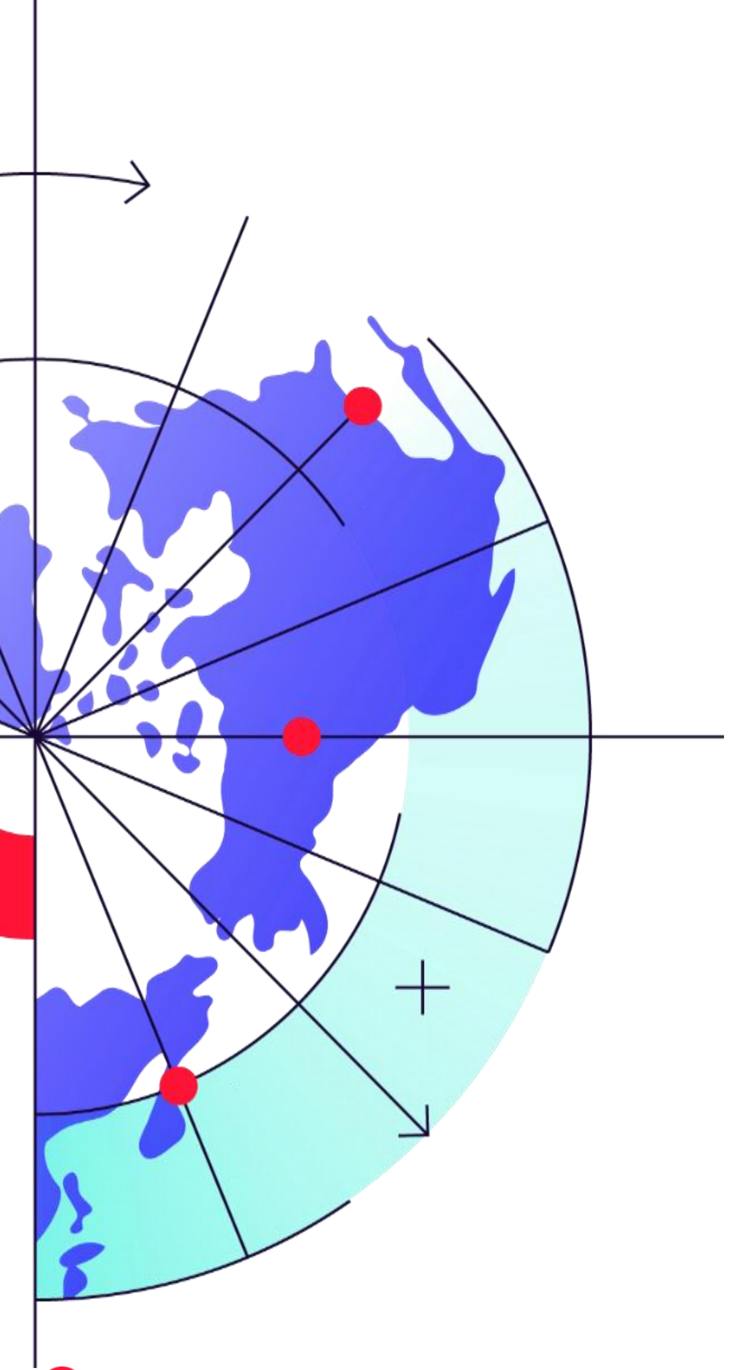
Webcam.avi
3.22 MB

History-Bookmarks-Cookies-Passwords-CreditCar...
2.39 MB

exodusCryptoAppdata.zip
4.81 MB

For example, a stealer called "*Bytestealer*" is one of many.

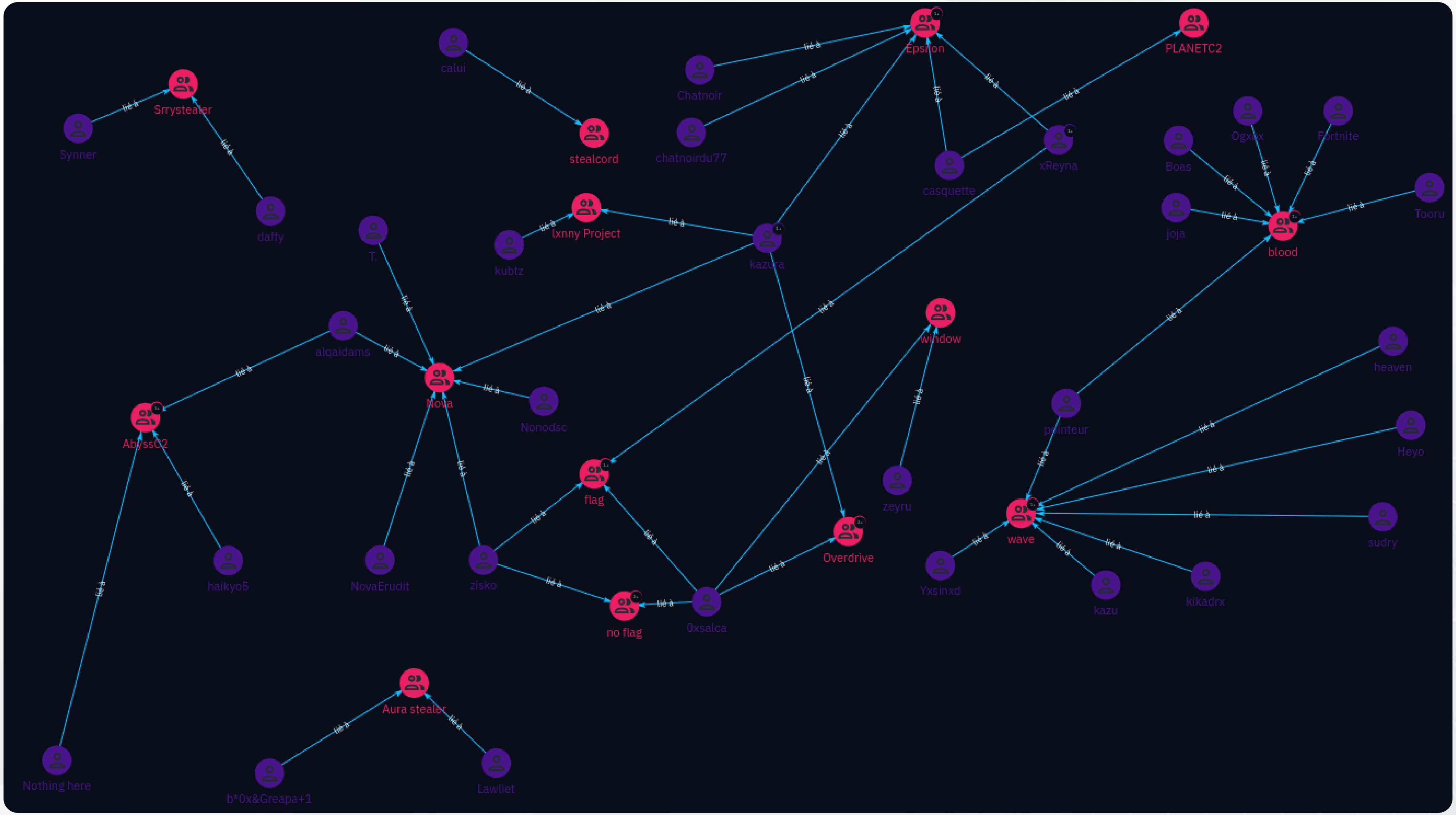
Because much of the source code for these types of stealers is often leaked or sold, it's possible to find thousands of them, each with slight or big variations.



GATEWATCHER

*Anatomy of groups and their lack of awareness_*

The ecosystem of French speaking cybercrime actors (2nd half of 2024)_



Group management_

Organizational structure

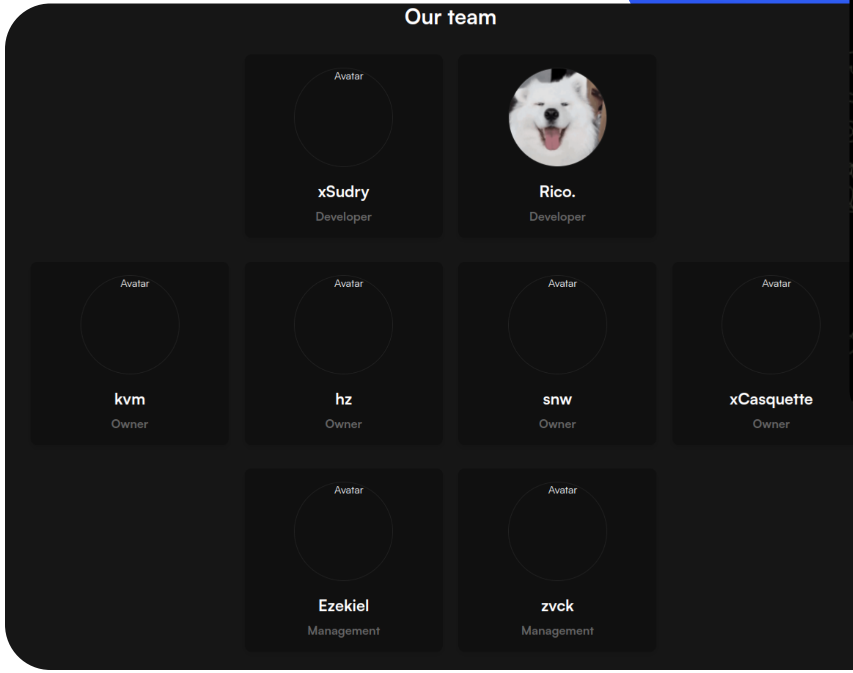
The cybercrime ecosystem has adopted a corporate-like structure with defined roles:

> **Dev/Owners**

> **Community Managers**

> **Support**

This centralized structure on platforms like Telegram and Discord allows these groups to scale their operations efficiently.



Our team

xSudry
Developer

Rico.
Developer

kvm
Owner

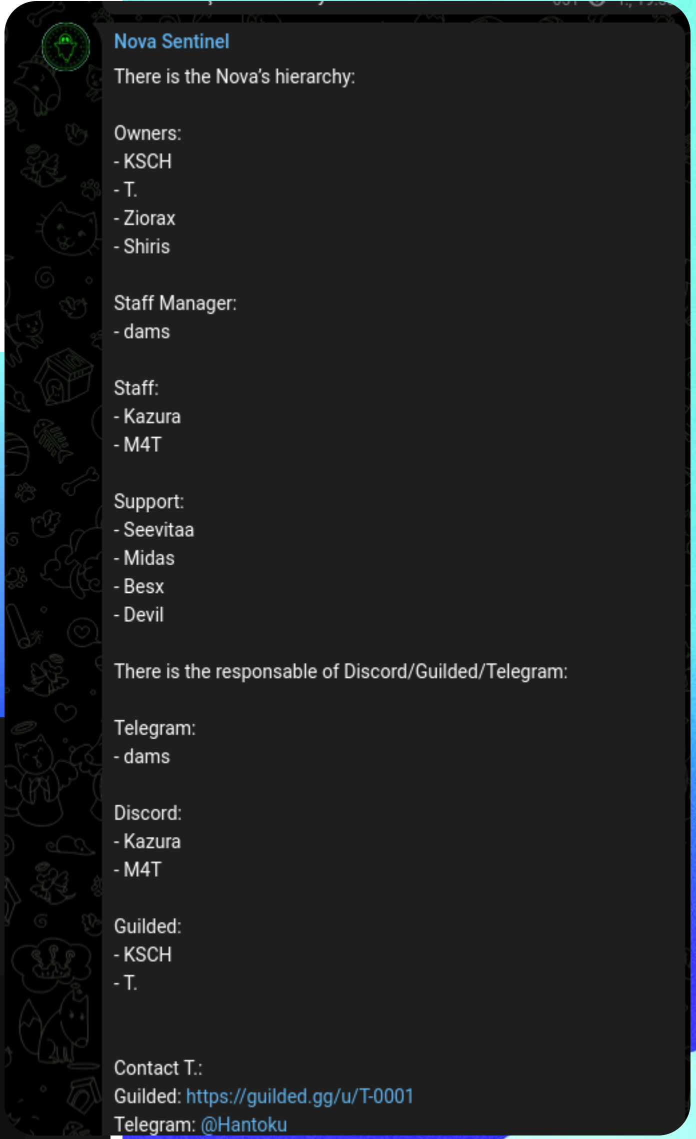
hz
Owner

snw
Owner

xCasquette
Owner

Ezekiel
Management

zvck
Management



Nova Sentinel

There is the Nova's hierarchy:

Owners:
- KSCH
- T.
- Ziorax
- Shiris

Staff Manager:
- dams

Staff:
- Kazura
- M4T

Support:
- Seevitaa
- Midas
- Besx
- Devil

There is the responsable of Discord/Guilded/Telegram:

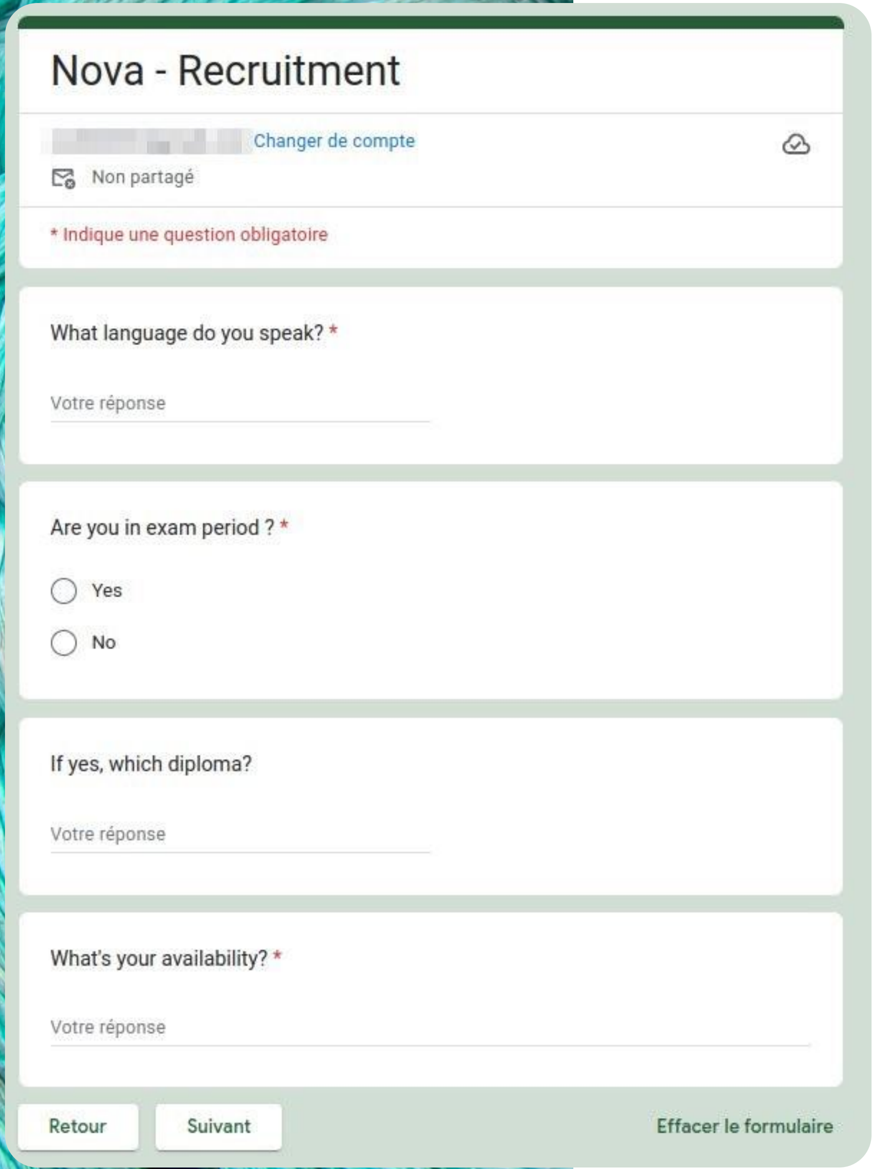
Telegram:
- dams

Discord:
- Kazura
- M4T

Guilded:
- KSCH
- T.

Contact T.:
Guilded: https://guilded.gg/u/T-0001
Telegram: @Hantoku

Who are they_



Nova - Recruitment

[redacted] Changer de compte

Non partagé

* Indique une question obligatoire

What language do you speak? *

Votre réponse

Are you in exam period ? *

○ Yes

○ No

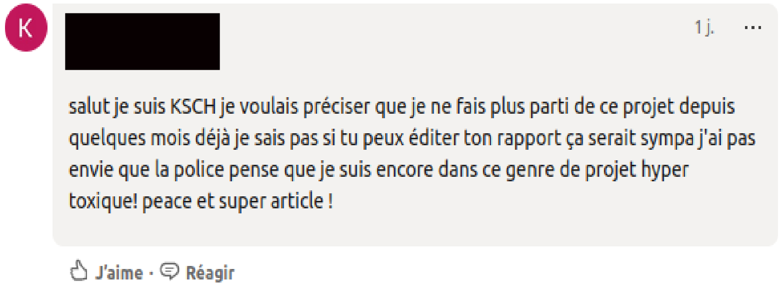
If yes, which diploma?

Votre réponse

What's your availability? *

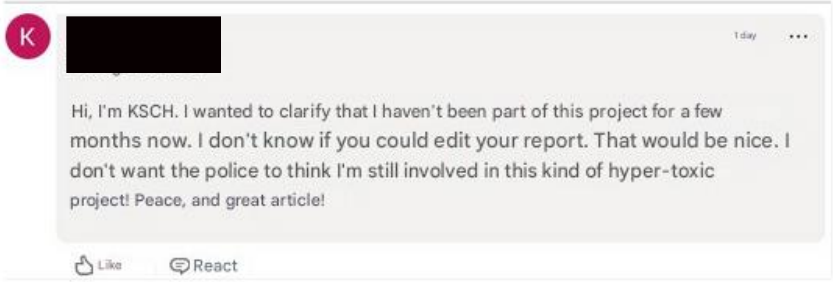
Votre réponse

- Methodology of research:
  We compiled information from their self-doxxed data, shared language, habits, and recruitment methods to establish these profiles.
- Background:
  Between 15 and 25 years old, still in school or university.
- Motivation:
  Primarily for "fun" and a small amount of profit, with little to no understanding of the real harm their actions cause.
- Identity:
  Drawn in by the "hacker myth," they see themselves as masters of their craft.



[redacted] 1 j.

salut je suis KSCH je voulais préciser que je ne fais plus parti de ce projet depuis quelques mois déjà je sais pas si tu peux éditer ton rapport ça serait sympa j'ai pas envie que la police pense que je suis encore dans ce genre de projet hyper toxique! peace et super article !



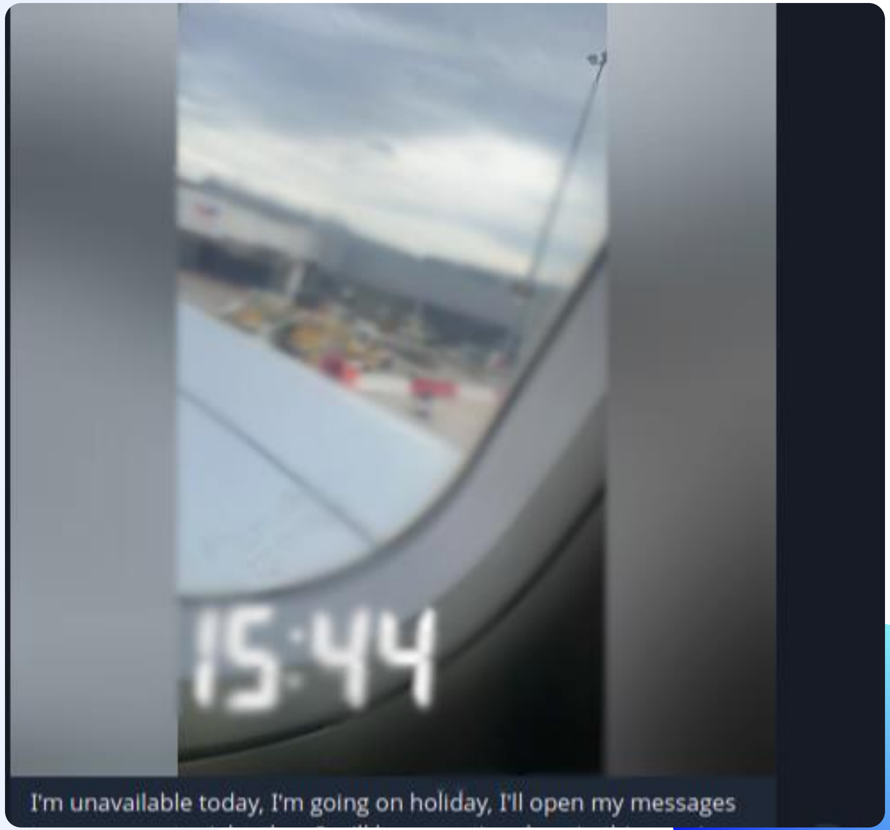
[redacted] 1 day

Hi, I'm KSCH. I wanted to clarify that I haven't been part of this project for a few months now. I don't know if you could edit your report. That would be nice. I don't want the police to think I'm still involved in this kind of hyper-toxic project! Peace, and great article!

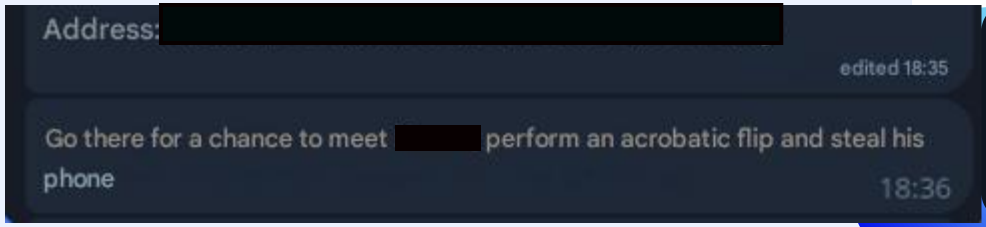
Few examples of how we managed to understand who are the admin_

Operational insights: Exploiting human weakness

- Lack of SecOps:
  A significant vulnerability is the poor security culture among group administrators.
- Careless personal sharing:
  Members often post personal photos and details from their holidays.
- The power of pseudonyms:
  Reused pseudonyms are a major weakness.

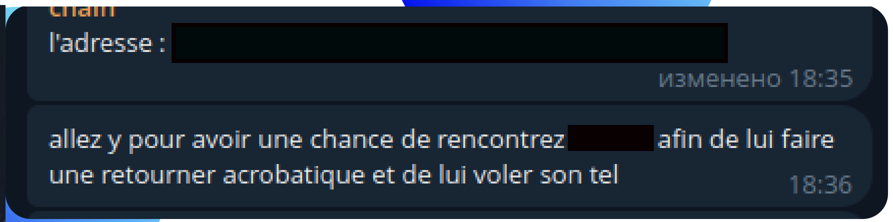


I'm unavailable today, I'm going on holiday, I'll open my messages



Address: [redacted]
edited 18:35

Go there for a chance to meet [redacted] perform an acrobatic flip and steal his phone
18:36



l'adresse : [redacted]
изменено 18:35

allez y pour avoir une chance de rencontrez [redacted] afin de lui faire une retourner acrobatique et de lui voler son tel
18:36

Diversification of cybercrime activities_

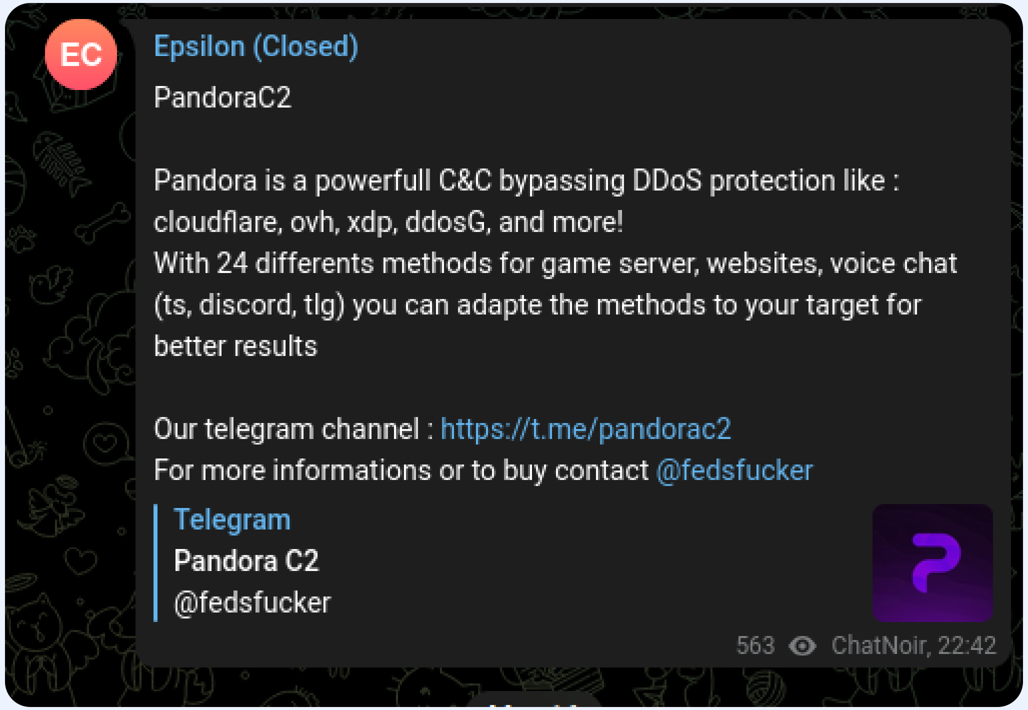
Additional administrator activities

- **Revenge porn groups:**
  Some administrators of these groups are also involved in revenge porn or Onlyfan leak groups.

Diversification of cybercrime activities_

Additional administrator activities

> **C2 for DDOS activities:**
They advertise these services on their Telegram channels and actively participate in the attacks.



EC Epsilon (Closed)

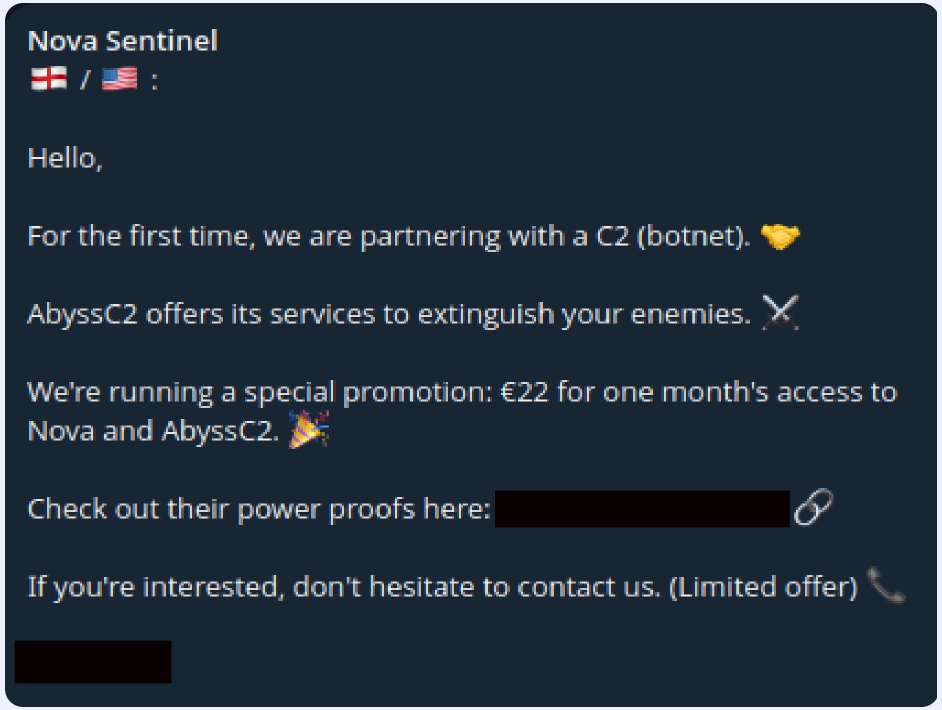
PandoraC2

Pandora is a powerfull C&C bypassing DDoS protection like : cloudflare, ovh, xdp, ddosG, and more!
With 24 differents methods for game server, websites, voice chat (ts, discord, tlg) you can adapte the methods to your target for better results

Our telegram channel : https://t.me/pandorac2
For more informations or to buy contact @fedsfucker

Telegram
Pandora C2
@fedsfucker

563 ChatNoir, 22:42



Nova Sentinel
🏴󠁧󠁢󠁥󠁮󠁧󠁿 / 🇺🇸 :

Hello,

For the first time, we are partnering with a C2 (botnet). 🤝

AbyssC2 offers its services to extinguish your enemies. ⚔️

We're running a special promotion: €22 for one month's access to Nova and AbyssC2. 🎉

Check out their power proofs here: [redacted] 🔗

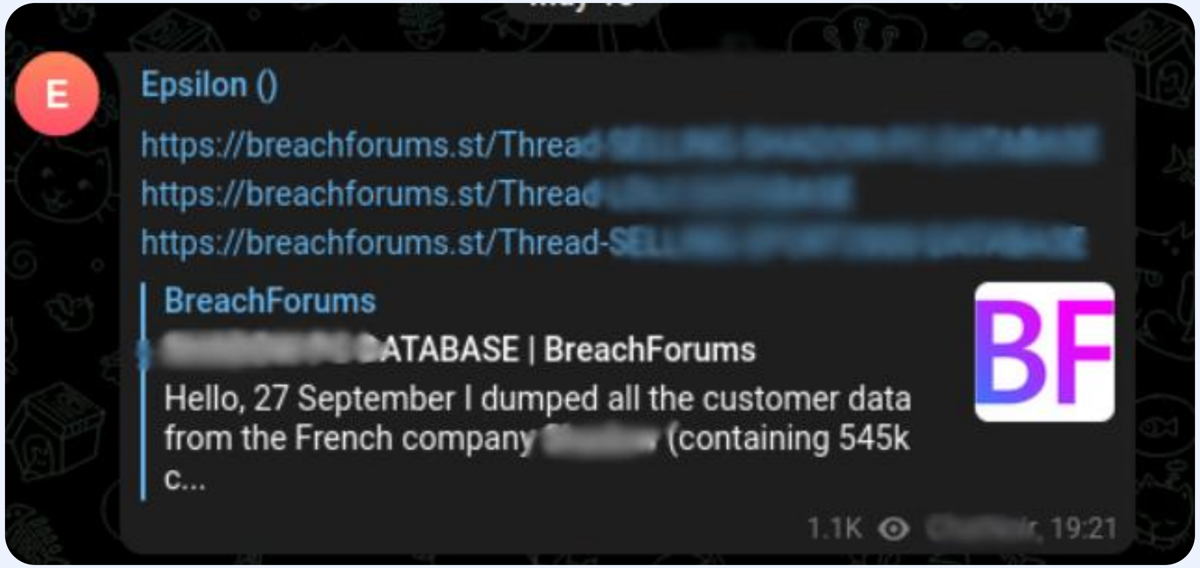
If you're interested, don't hesitate to contact us. (Limited offer) 📞

[redacted]

Diversification of cybercrime activities_

Additional administrator activities

- Hacking companies and reselling data:
  We found a specific case involving the Epsilon group,
  which was responsible for hacking media and other companies in France.
- This group was known for selling stolen data on the cyber black market,
  and their 2024 breach resulted in the exposure of millions of customer records.



Epsilon ()

https://breachforums.st/Thread[redacted]
https://breachforums.st/Thread[redacted]
https://breachforums.st/Thread-S[redacted]

BreachForums

[redacted]ATABASE | BreachForums

Hello, 27 September I dumped all the customer data from the French company [redacted] (containing 545k c...

1.1K [redacted], 19:21

Specific case of Epsilon regarding diversification_

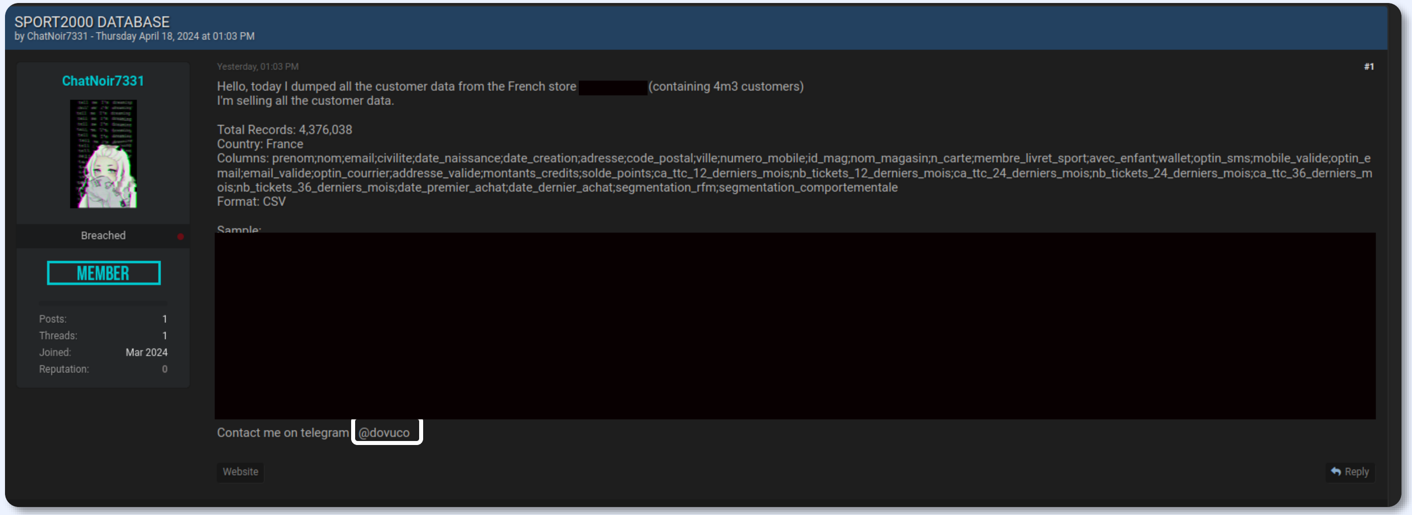
Epsilon: A case study

> Epsilon was a French stealer group that compromised and sold data from several companies.

> They sold their stolen data on multiple forum.

> The uniqueness of their messages across different forums is a key indicator.

> This consistency allows us to confidently attribute the messages to the same group.



SPORT2000 DATABASE
by ChatNoir7331 - Thursday April 18, 2024 at 01:03 PM

ChatNoir7331

Breached

MEMBER

Posts: 1
Threads: 1
Joined: Mar 2024
Reputation: 0

Yesterday, 01:03 PM #1

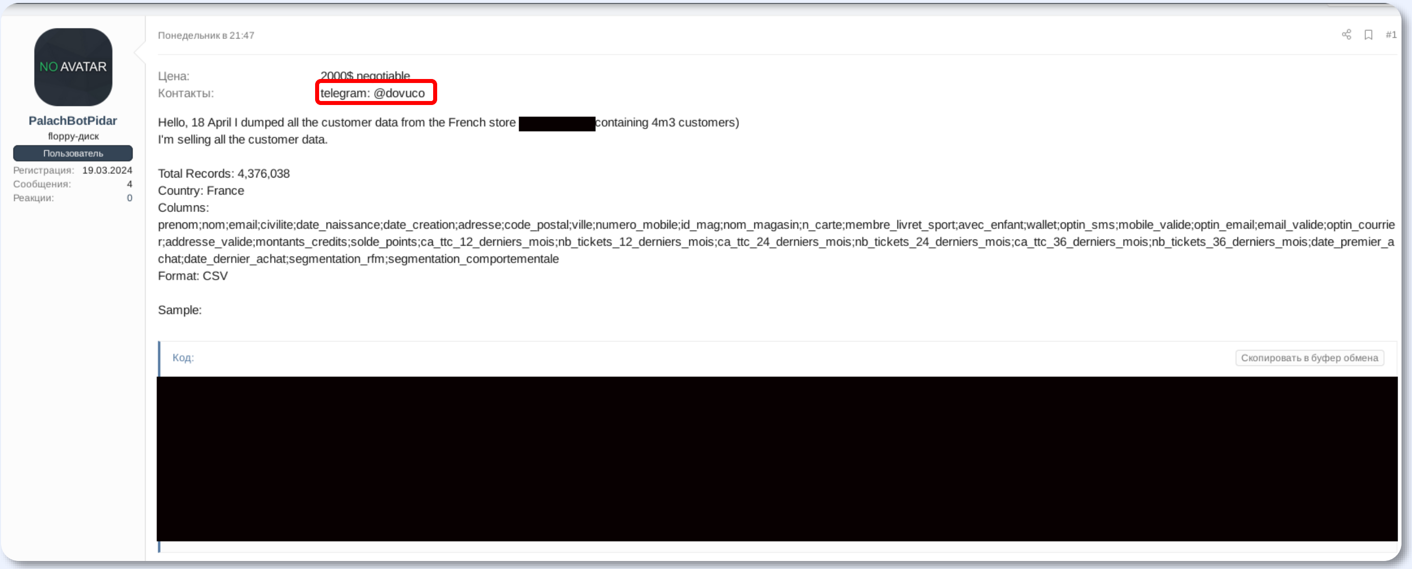
Hello, today I dumped all the customer data from the French store [redacted] (containing 4m3 customers)
I'm selling all the customer data.

Total Records: 4,376,038
Country: France
Columns: prenom;nom;email;civilite;date_naissance;date_creation;adresse;code_postal;ville;numero_mobile;id_mag;nom_magasin;n_carte;membre_livret_sport;avec_enfant;wallet;optin_sms;mobile_valide;optin_email;email_valide;optin_courrier;addresse_valide;montants_credits;solde_points;ca_ttc_12_derniers_mois;nb_tickets_12_derniers_mois;ca_ttc_24_derniers_mois;nb_tickets_24_derniers_mois;ca_ttc_36_derniers_mois;nb_tickets_36_derniers_mois;date_premier_achat;date_dernier_achat;segmentation_rfm;segmentation_comportementale
Format: CSV

Sample:

[redacted]

Contact me on telegram @dovuco



NO AVATAR

PalachBotPidar
floppy-диск
Пользователь
Регистрация: 19.03.2024
Сообщения: 4
Реакции: 0

Понедельник в 21:47 #1

Цена: 2000$ negotiable
Контакты: telegram: @dovuco

Hello, 18 April I dumped all the customer data from the French store [redacted] containing 4m3 customers)
I'm selling all the customer data.

Total Records: 4,376,038
Country: France
Columns:
prenom;nom;email;civilite;date_naissance;date_creation;adresse;code_postal;ville;numero_mobile;id_mag;nom_magasin;n_carte;membre_livret_sport;avec_enfant;wallet;optin_sms;mobile_valide;optin_email;email_valide;optin_courrier;addresse_valide;montants_credits;solde_points;ca_ttc_12_derniers_mois;nb_tickets_12_derniers_mois;ca_ttc_24_derniers_mois;nb_tickets_24_derniers_mois;ca_ttc_36_derniers_mois;nb_tickets_36_derniers_mois;date_premier_achat;date_dernier_achat;segmentation_rfm;segmentation_comportementale
Format: CSV

Sample:

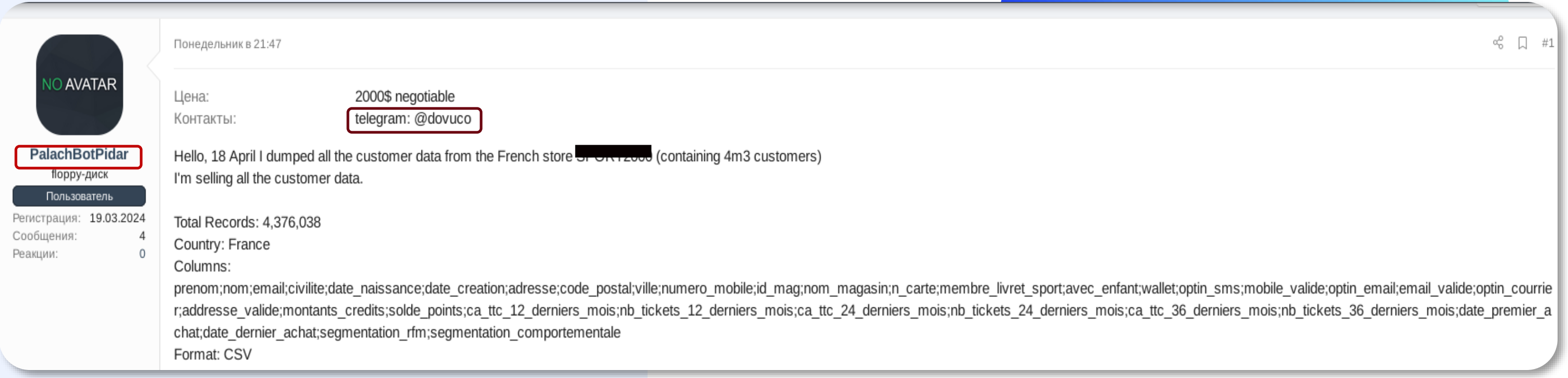
Код:

[redacted]

Specific case of Epsilon regarding diversification_

Revolut Pro accounts and money laundering

- This account has multiple interactions, including scam reports.
- The account holder attempted to purchase Revolut Pro accounts
- The link between the purchase request and previous activities (stealer or database sales) is currently unknown.



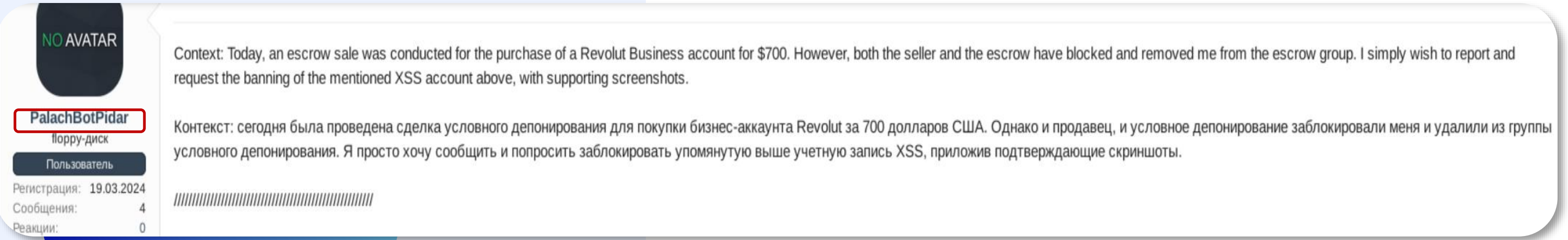
PalachBotPidar
floppy-диск
Пользователь
Регистрация: 19.03.2024
Сообщения: 4
Реакции: 0

Понедельник в 21:47

Цена: 2000$ negotiable
Контакты: telegram: @dovuco

Hello, 18 April I dumped all the customer data from the French store [redacted] (containing 4m3 customers)
I'm selling all the customer data.

Total Records: 4,376,038
Country: France
Columns:
prenom;nom;email;civilite;date_naissance;date_creation;adresse;code_postal;ville;numero_mobile;id_mag;nom_magasin;n_carte;membre_livret_sport;avec_enfant;wallet;optin_sms;mobile_valide;optin_email;email_valide;optin_courrier;addresse_valide;montants_credits;solde_points;ca_ttc_12_derniers_mois;nb_tickets_12_derniers_mois;ca_ttc_24_derniers_mois;nb_tickets_24_derniers_mois;ca_ttc_36_derniers_mois;nb_tickets_36_derniers_mois;date_premier_achat;date_dernier_achat;segmentation_rfm;segmentation_comportementale
Format: CSV



PalachBotPidar
floppy-диск
Пользователь
Регистрация: 19.03.2024
Сообщения: 4
Реакции: 0

Context: Today, an escrow sale was conducted for the purchase of a Revolut Business account for $700. However, both the seller and the escrow have blocked and removed me from the escrow group. I simply wish to report and request the banning of the mentioned XSS account above, with supporting screenshots.

Контекст: сегодня была проведена сделка условного депонирования для покупки бизнес-аккаунта Revolut за 700 долларов США. Однако и продавец, и условное депонирование заблокировали меня и удалили из группы условного депонирования. Я просто хочу сообщить и попросить заблокировать упомянутую выше учетную запись XSS, приложив подтверждающие скриншоты.

//

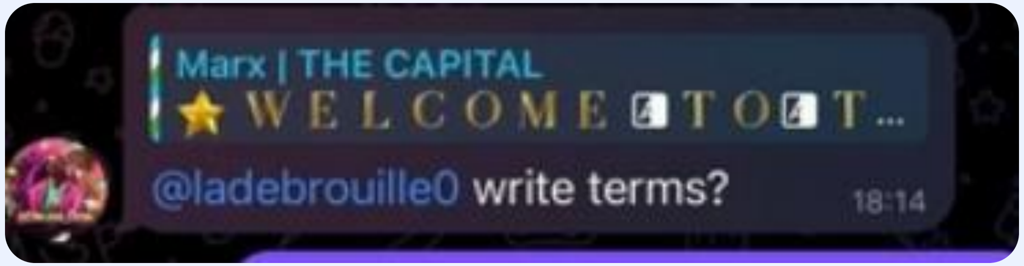
Specific case of Epsilon regarding diversification_

Connecting the dots

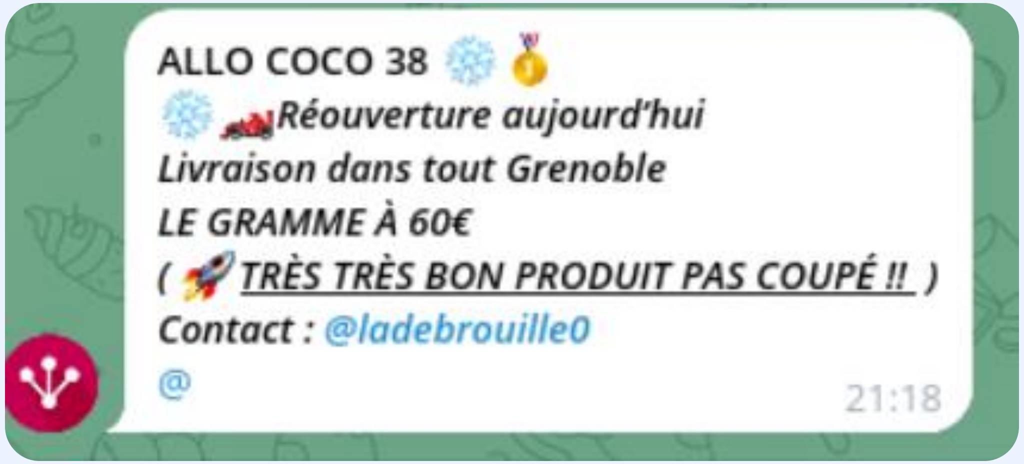
> A chat exchange between a scammer and a post publisher helped us identify his Telegram pseudonym.

> The pseudonyms `chatnoir` (@dovuco) and `La Debrouille` (@ladebrouille0) are connected by these posts, though we don't know if they are the same person.

> We believe an administrator or a member of the Epsilon group is involved in drug trafficking in Grenobles, France, and may be advertising these activities.



Marx | THE CAPITAL
⭐ WELCOME ▣ TO ▣ T…
@ladebrouille0 write terms? 18:14



ALLO COCO 38 ❄️ 🥇
❄️ 🏎️ *Réouverture aujourd'hui*
Livraison dans tout Grenoble
LE GRAMME À 60€
(🚀 TRÈS TRÈS BON PRODUIT PAS COUPÉ !!)
Contact : @ladebrouille0
@
21:18

*Reopening today
Delivery through all Grenoble
60€/gram
Very good uncut product

*Why watching and understanding them matters_*

The underestimated power of these groups_

- Risk to companies:
  While these groups see their activities as a "game"
  they create substantial risks for companies.

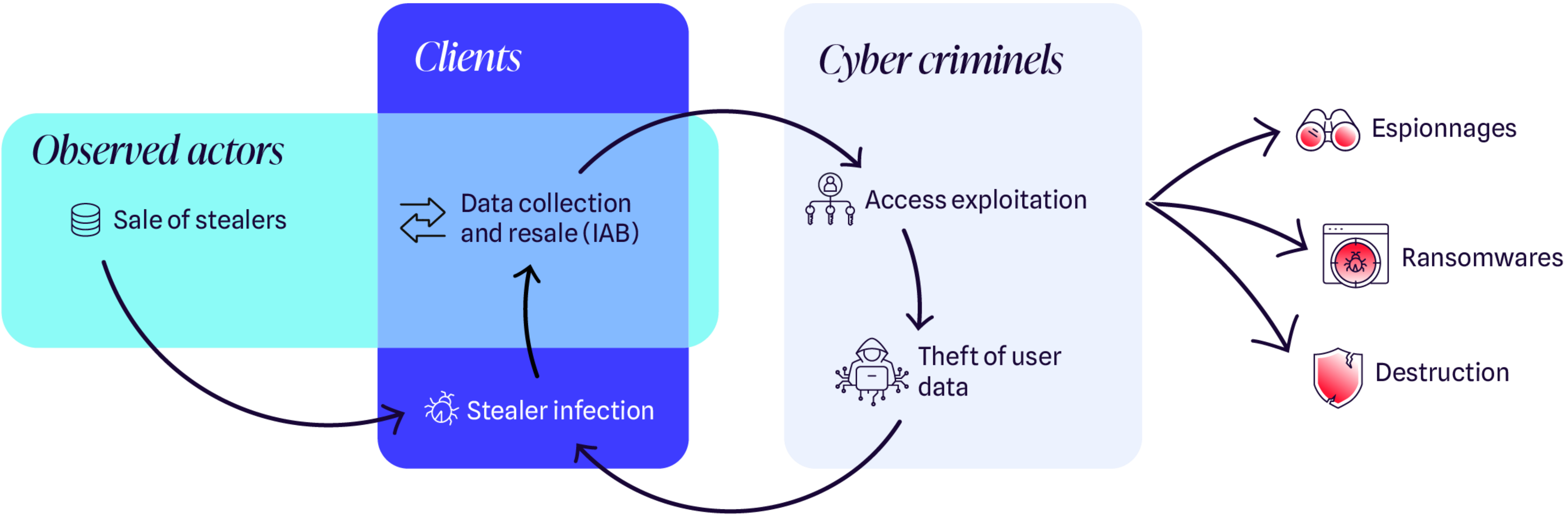
- Vulnerability through employees:
  The main threat comes from employees who reuse personal
  and professional passwords

- "Combolists" are a threat:
  These groups compile "combolists" (lists of usernames and passwords) from various breaches, which are then sold to more sophisticated attackers.

- Gateway to more serious attacks

- Importance of monitoring:
  Keep an eye onthese seemingly minor actors as part of an effective
  cybersecurity strategy.

The underestimated power of these groups_



Key takeaways and conclusion_

We mapped out the French Stealer ecosystem, revealing the structure and connections between the different French-speaking groups..

> Technical insights on stealers:
Learn how these stealers operate

> Profiling threat actors:
By analyzing cybercriminal interactions and OpSec errors, we can identify and disrupt these groups and better understand who they really are.

> Epsilon group case study:
See how one group’s activities extend into illicit fields like drug trafficking, underscoring the broader impact of these operations

This group still needs to be monitored sometime and authorities must explain by sensibilization that *these activities are illegal with big risks and are not a game!*

Sources_

[Stealing with flair: French young actors unveiled]

[Nova Stealer, The Malware Made in France]

[MaaS appeal: an infostealer rises from the ashes]

GATEWATCHER

Thank you