

Info-stealer: Most bang for the buck malware

S2W Jiho Kim

Threat Analysis Team (BLKSMTH)

@TALON

Who Am I?



- Jiho Kim
 - Junior Threat Intelligence Researcher
 - BLKSMTH, S2W Talon
 - Working hard always 🔥

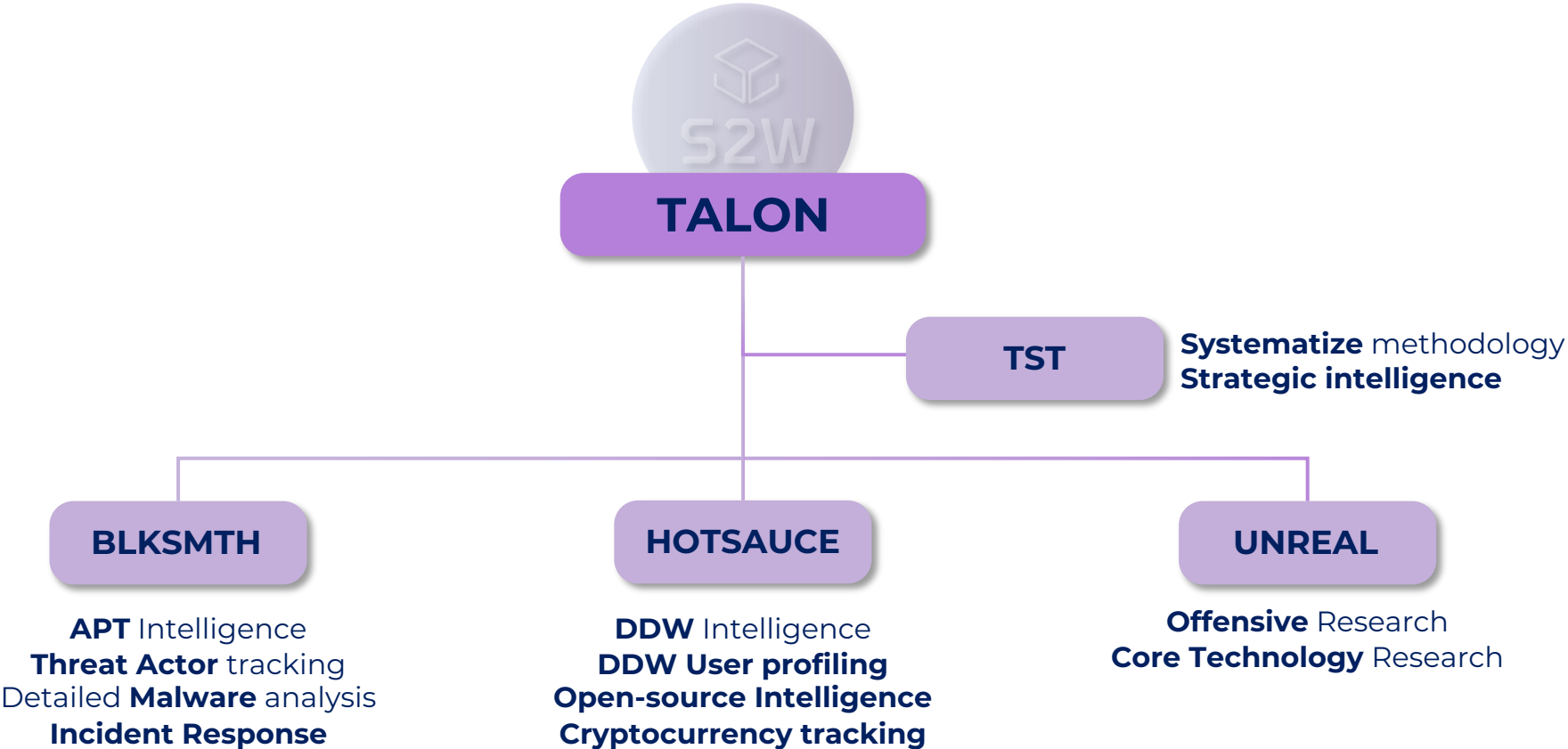
FIRSTCON 2023: First presentation of my life ever!

 @gimchesh

 [Kim Jiho](#)

Who are we & What we do?

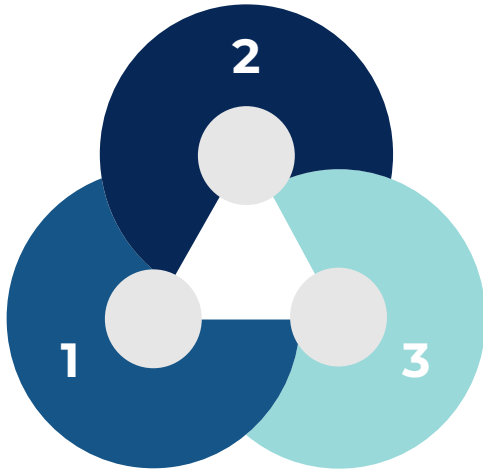
We are S2W TALON!



Abstract in 5W1H

WHO

A type of malware that steals all sensitive information, including credentials, after infiltrating a victimized system.



01. MaaS (Malware-as-a-Service)

A type that operates on **the deep & dark web** and **sells builder or license** that create stealer malware executables and **panels** for managing infection logs

02. Open-source

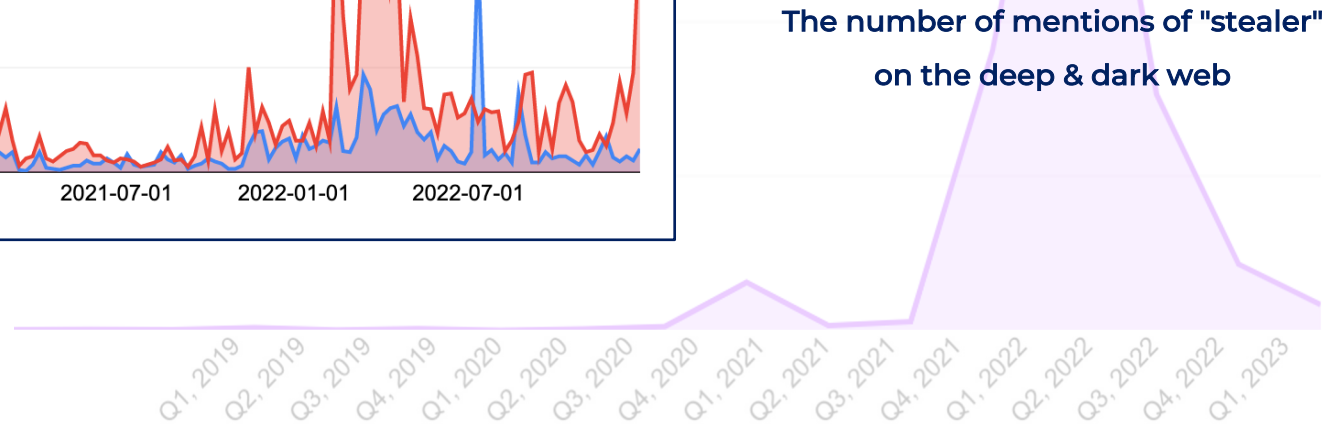
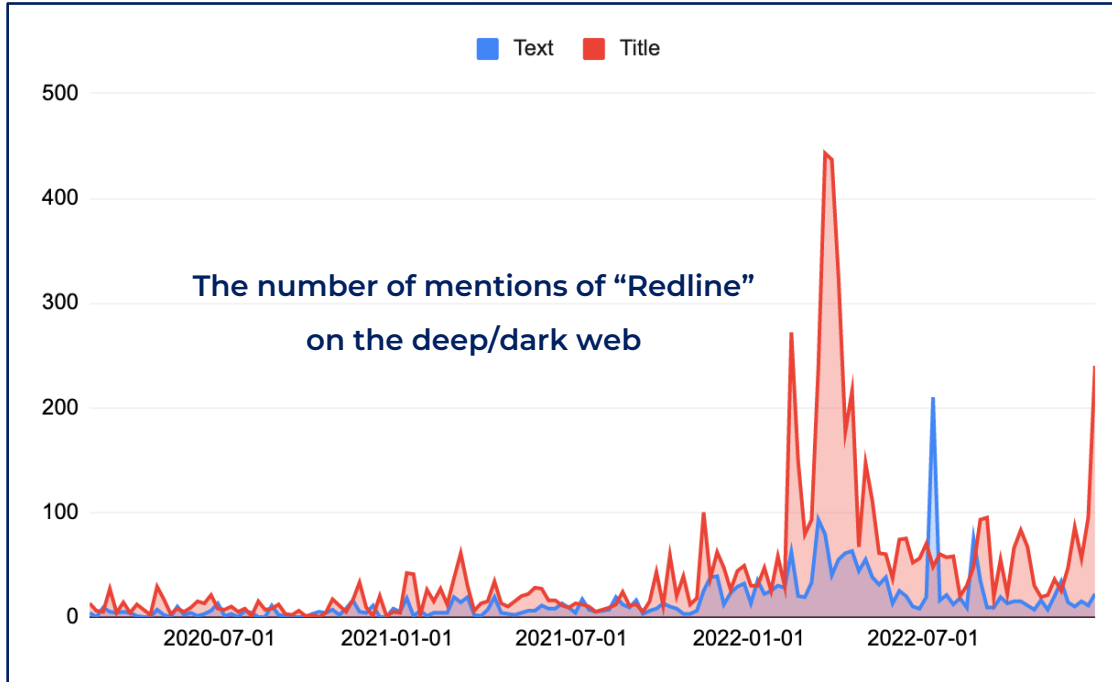
A type releasing the **source code** of the stealer created **for free**

03. Own

A type **that builds and use own stealer** without selling or disclosing it

WHEN

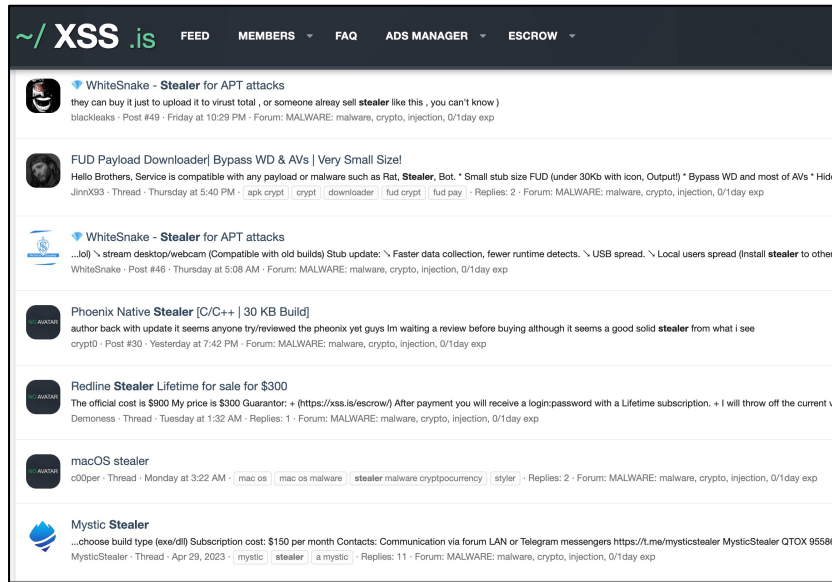
* Statistics by S2W's deep & dark web search engine, Xarvis



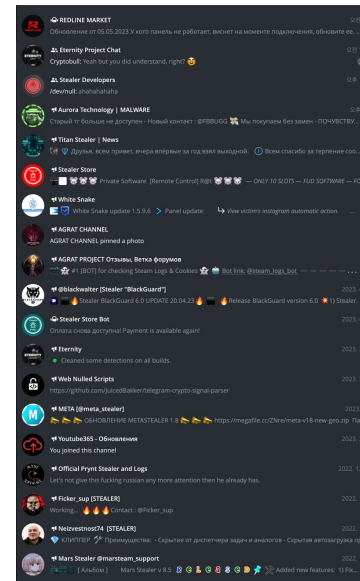
WHERE

They are most active on dark web forums and use their own Telegram channels for communication and customer care.

Dark web forums



Telegram channels



Channel for Support

Channel for Chat

Bot for sale

WHAT

They steal **the most valuable information**, and that information changes over time.

Browser

Telegram

FTP

Crypto Wallet

Steam

Email Client

VPN

Discord

IM Client

RDP

SystemInfo

Password Manager

WHY

Not all they have huge TTPs, but they are often used by attackers because the value of the items stolen is hundreds of times greater than the relatively small cost.



Spectacular Tactics

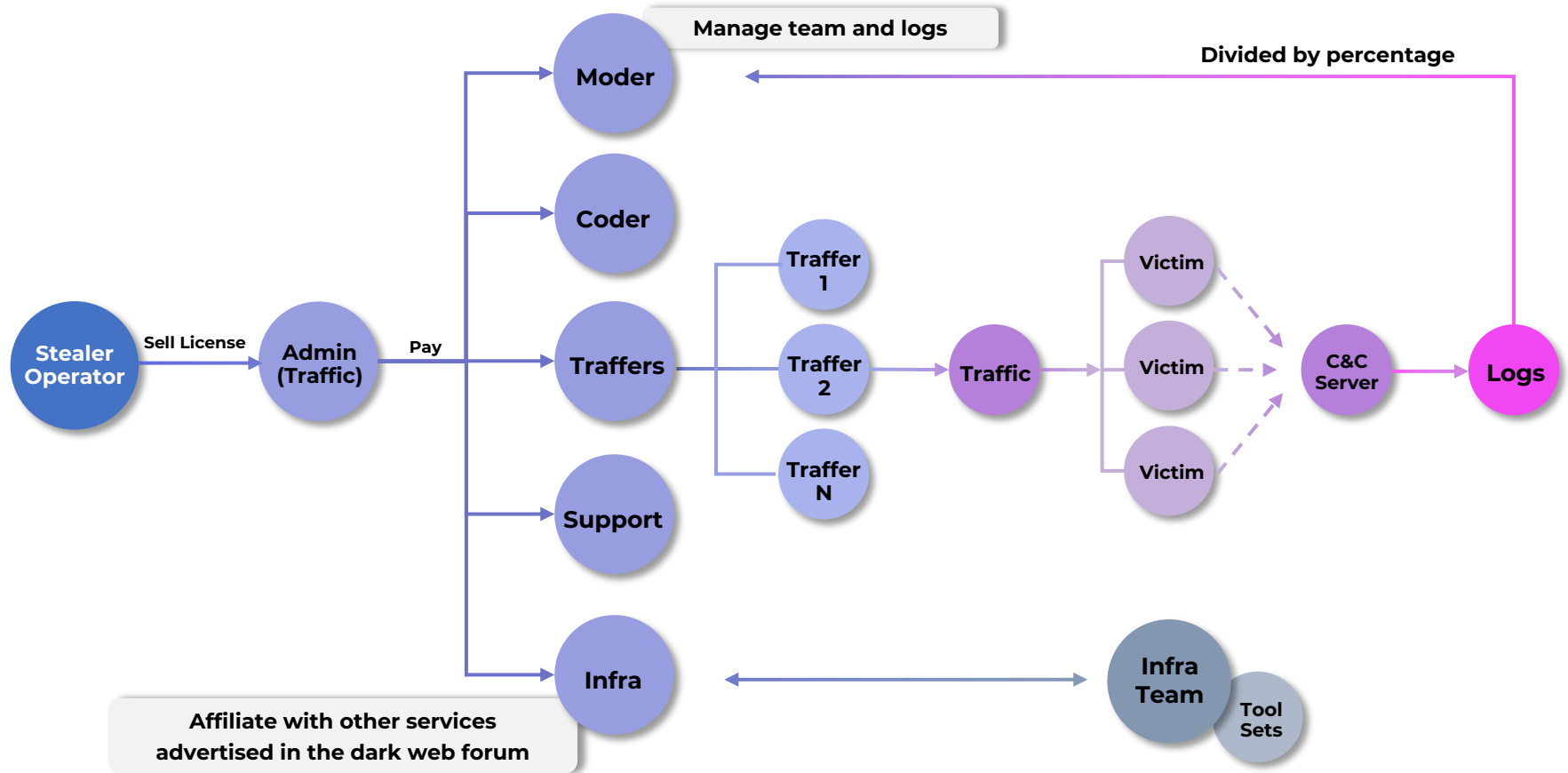


**0-day / 1-day
Vulnerability**



Amazing set of tools

HOW



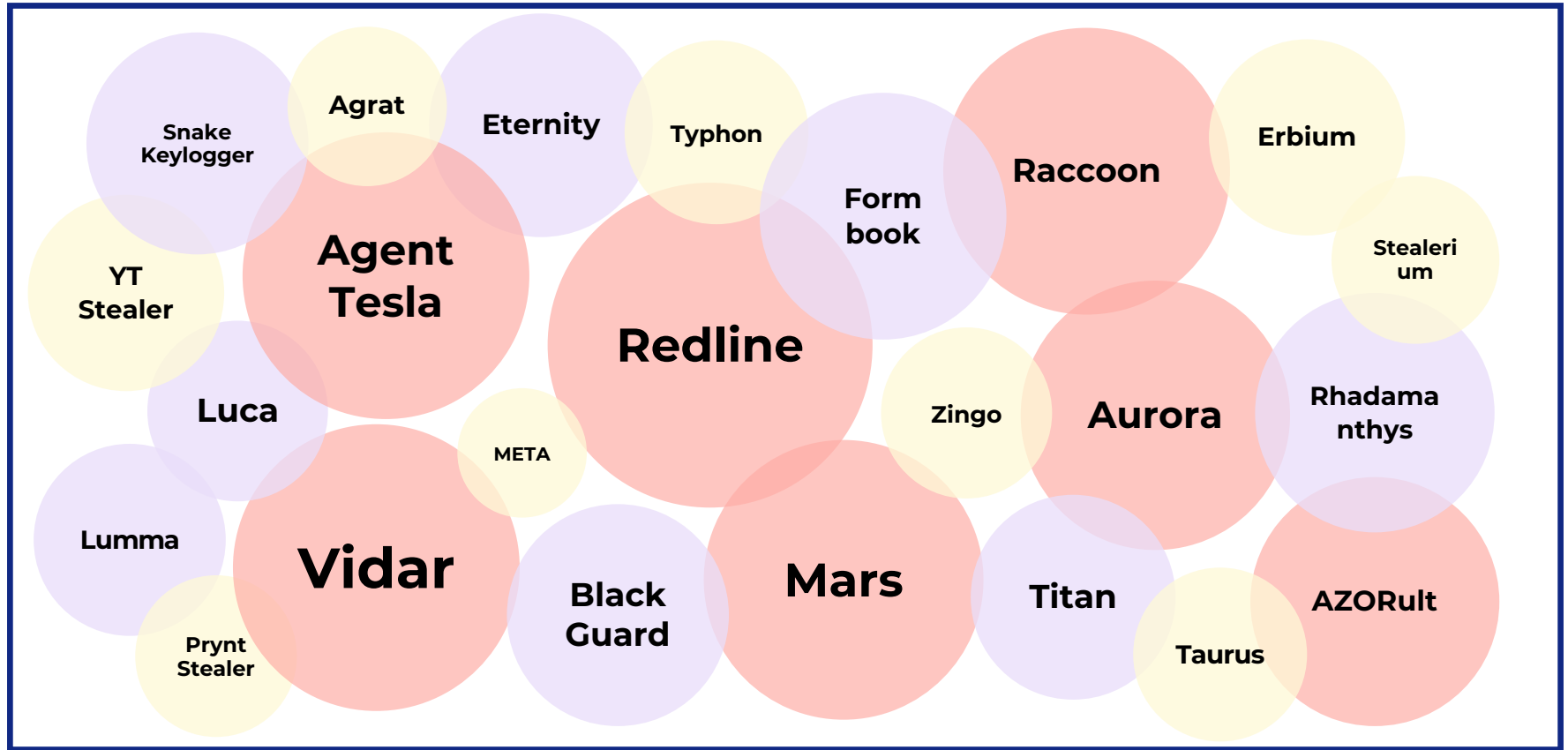
Changes

Activities of Stealer Operators in 2022

There are **more than 100 operators** in dark web forums and telegram channels, with over 40 of them being newly discovered on the dark web.

In addition to old favorites like Redline, Vidar, and Raccoon, newer stealers like Aurora, Meta, and Titan are making their mark.

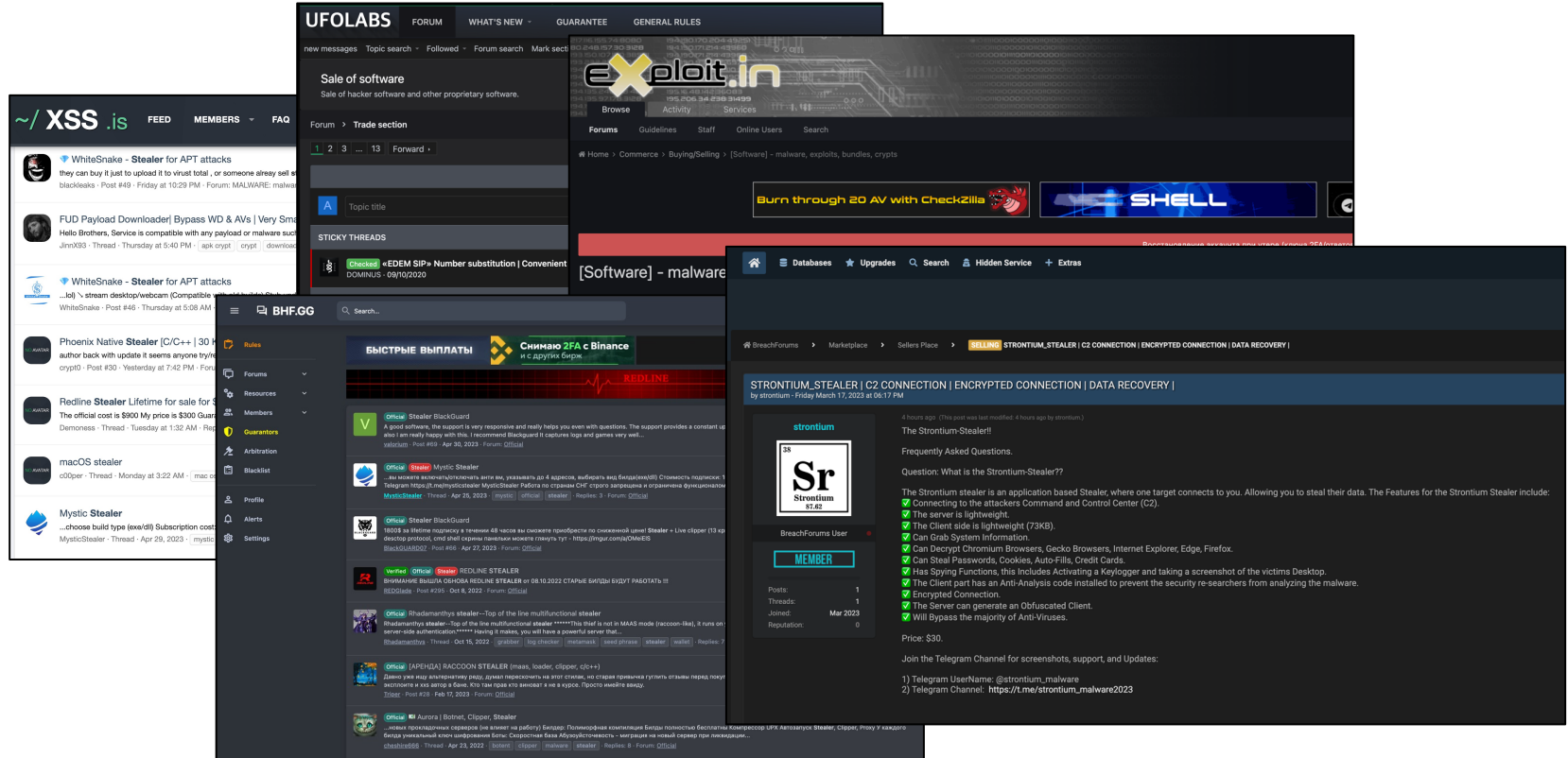
Activities of Stealer Operators in 2022



* Statistics by S2W's deep & dark web search engine, Xarvis (2020 ~ 2022)

Darkweb Forums: Sales for stealer

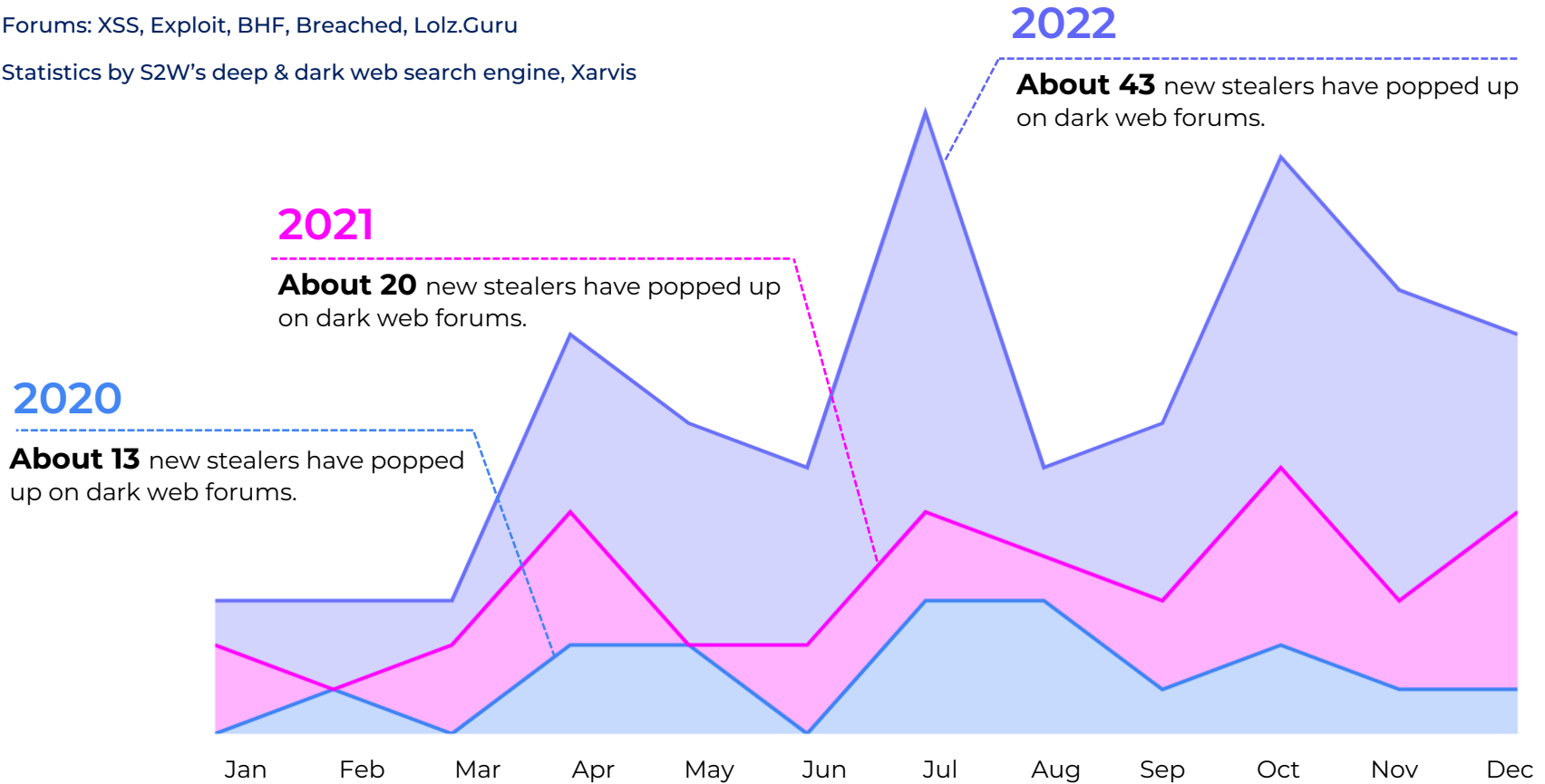
Stealer operators began to advertise on various dark web forums to sell stealers, and fierce competition ensued on forums like Breached, XSS, and Exploits.



Activities of Stealer Operators in 2022

* Forums: XSS, Exploit, BHF, Breached, Lolz.Guru

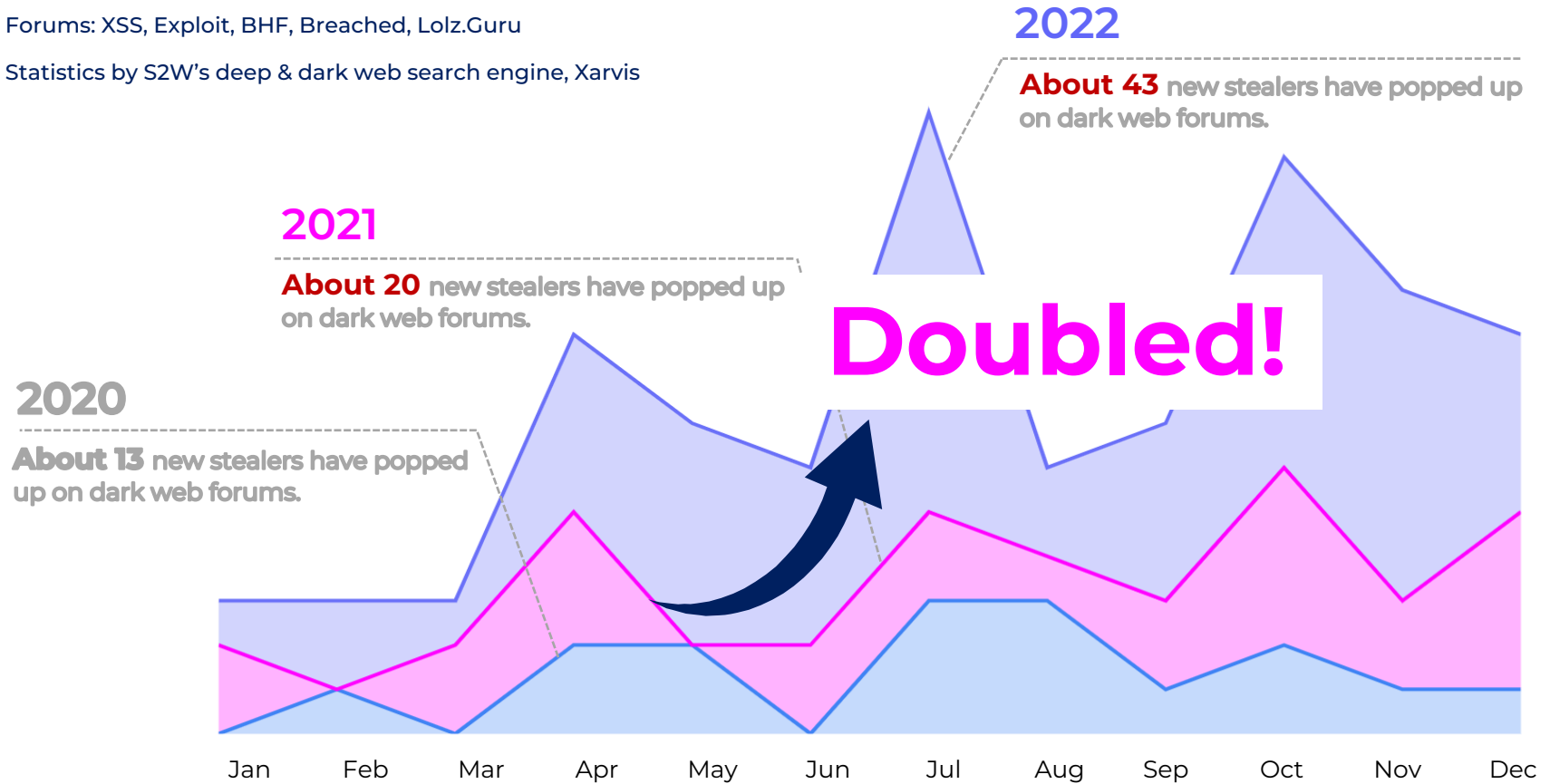
* Statistics by S2W's deep & dark web search engine, Xarvis



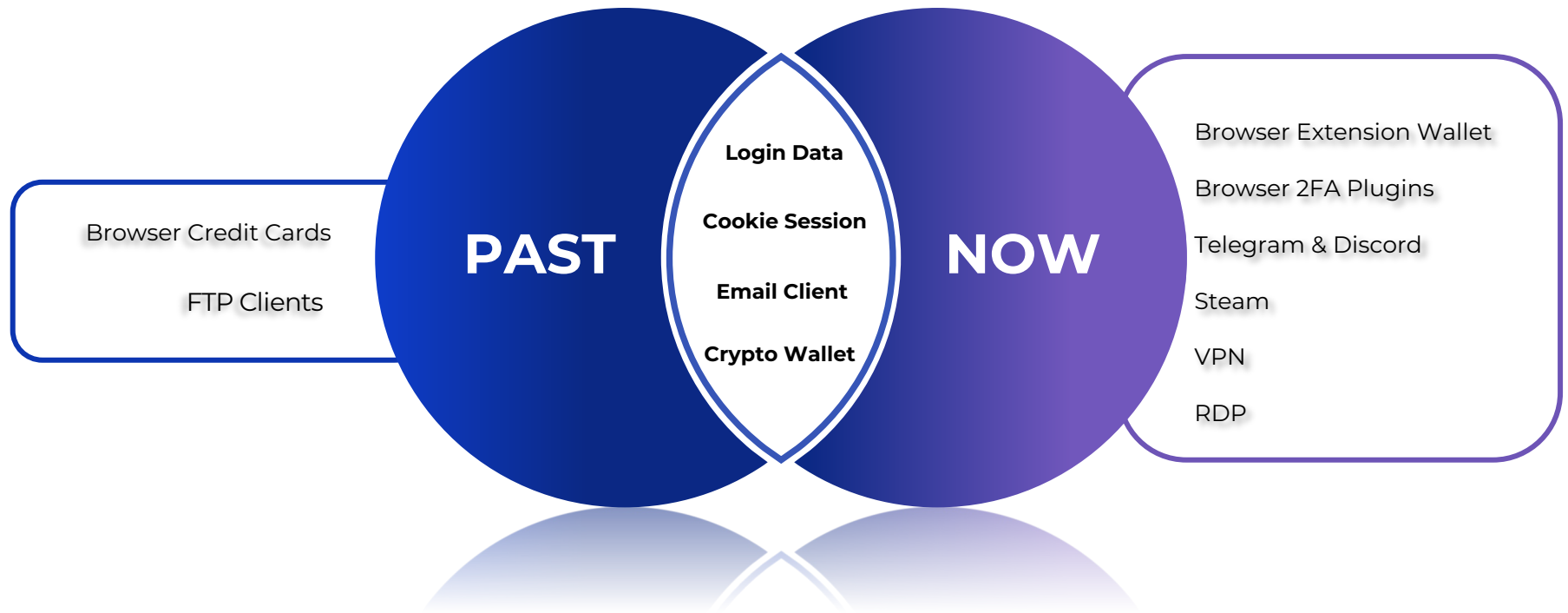
Activities of Stealer Operators in 2022

* Forums: XSS, Exploit, BHF, Breached, Lolz.Guru

* Statistics by S2W's deep & dark web search engine, Xarvis

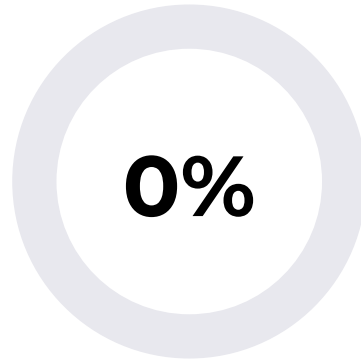


Activities of Stealer Operators in 2022

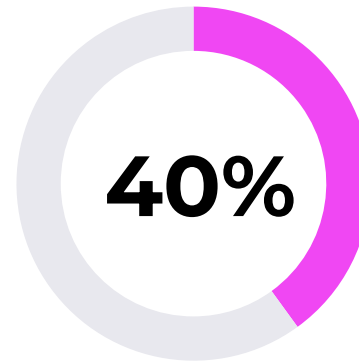


Exfiltrated Data

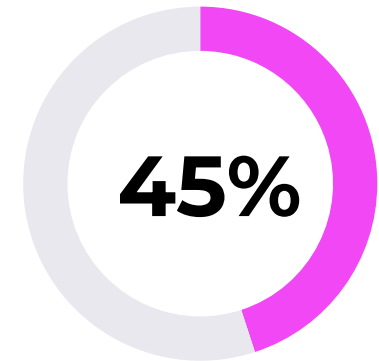
Browser Plugins



2020

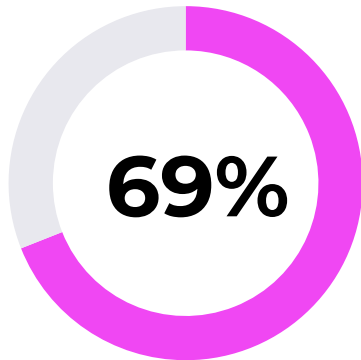


2021

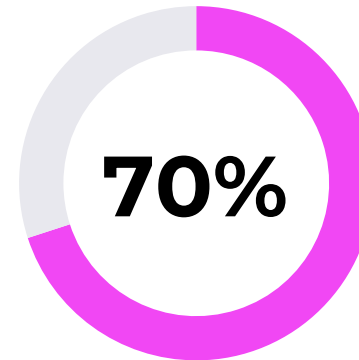


2022

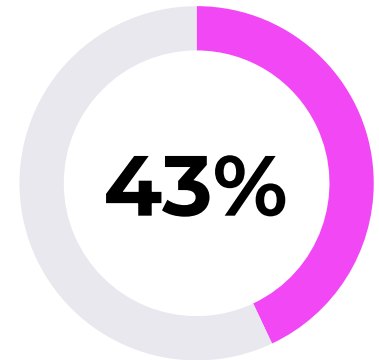
Browser
Credit Card



2020



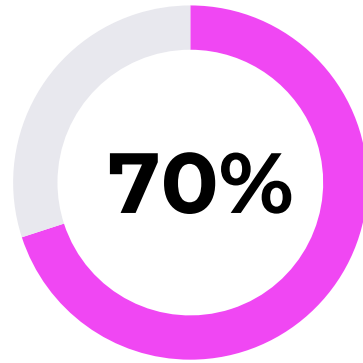
2021



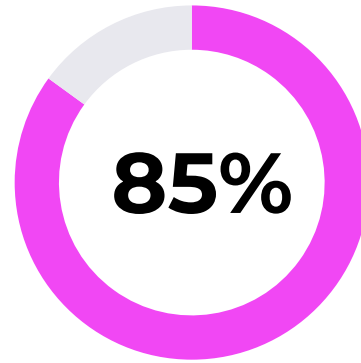
2022

Exfiltrated Data

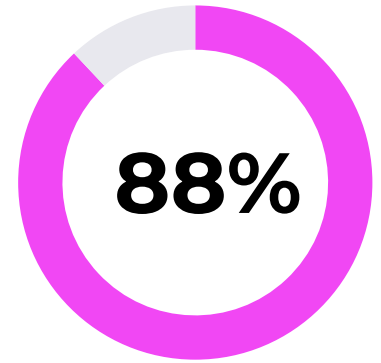
Crypto Wallet



2020

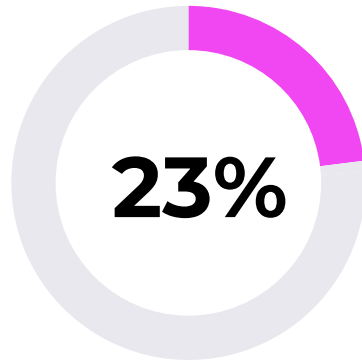


2021

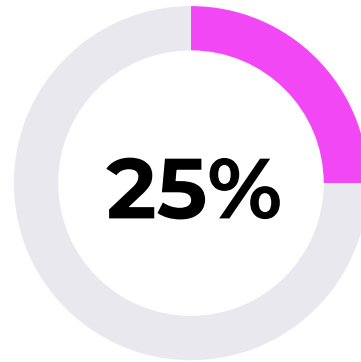


2022

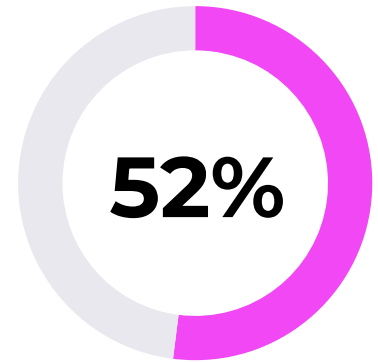
Steam



2020



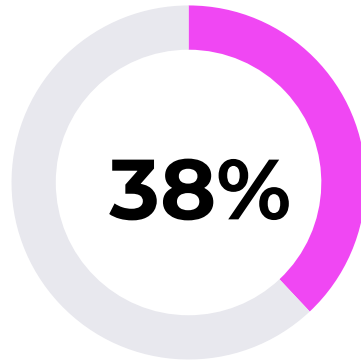
2021



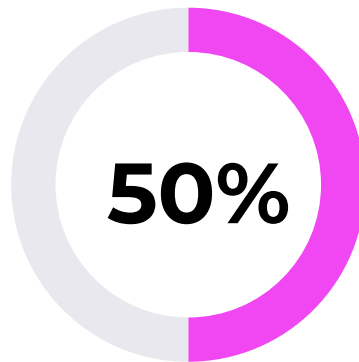
2022

Exfiltrated Data

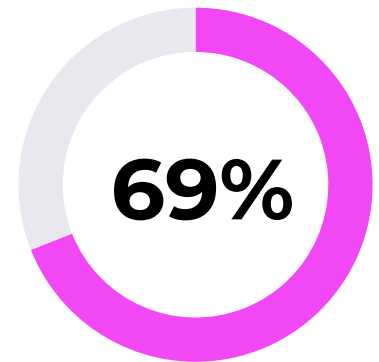
Telegram Session



2020

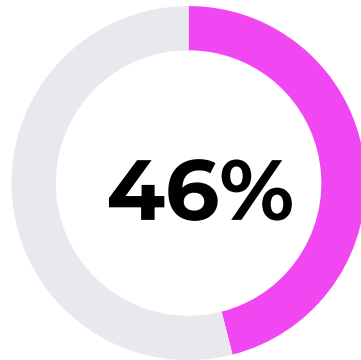


2021

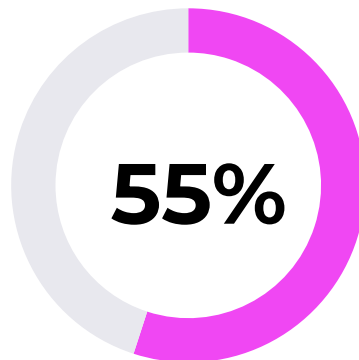


2022

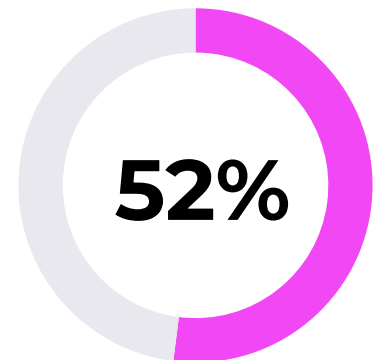
VPN



2020



2021



2022

Darkweb Forums: Sales for stealer log

- └─ Autofills
 - └─ CryptoTab Browser_[User Data]_Default.txt
 - └─ Google_[Chrome]_Default.txt
 - └─ Microsoft_[Edge]_Default.txt
 - └─ Opera GX_Unknown.txt
- └─ Cookies
 - └─ Google_[Chrome]_Default Extension.txt
 - └─ Google_[Chrome]_Default Network.txt
 - └─ Microsoft_[Edge]_Default Network.txt
 - └─ Opera GX_Unknown Network.txt
- └─ Discord
 - └─ Tokens.txt
- └─ DomainDetects.txt
- └─ FTP
 - └─ Credentials.txt
- └─ ImportantAutofills.txt
- └─ InstalledBrowsers.txt
- └─ InstalledSoftware.txt
- └─ Passwords.txt
- └─ ProcessList.txt
- └─ UserInformation.txt



```
*****
*
*
*  REDLINE
*
*
* Telegram: https://t.me/REDLINESELLER
*
*****

Build ID:[Redacted]
IP: [Redacted]
FileLocation: C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe
UserName: [Username]
Country: [Country]
Zip Code: [Zip Code]
Location: [Location]
HWID: [HWID]
Current Language: [Language]
ScreenSize: {Width=1920, Height=1080}
TimeZone: [Timezone]
Operation System: Windows 10 Enterprise x64
UAC: AllowAll
Process Elevation: False
Log date: 11/20/2022 8:29:07 AM

Available KeyboardLayouts:
[KeyboardLayouts#1]
[KeyboardLayouts#2]
[KeyboardLayouts#3]
..

Hardwares:
Name: AMD Ryzen 5 2600 Six-Core Processor , 6 Cores
Name: NVIDIA GeForce RTX 2060, 4293918720 bytes
Name: Total of RAM, 16312 MB or 17104371712 bytes

Anti-Viruses:
Windows Defender|
```

Darkweb Forums: Sales for stealer log

In addition, since 2022, forum categories and markets have emerged that sell only logs

The image is a collage of screenshots from various darkweb forums and markets. At the top left, a forum post header for '11K KOREA COMBOLIST' is shown, dated 24 March, 2023. To its right is a forum header for 'Stealer Logs' with the text 'Forum where you can post Stealer logs.' Below this, a 'genesis' dashboard is visible with navigation links for 'Dashboard', 'Home', and 'Wiki'. The bottom portion of the collage features a 'RUSSIAN MARKET' search interface. This interface includes a sidebar with categories like 'News', 'CVV', 'Dumps', 'RDP', and 'LOGS' (which is highlighted as 'pre-order'). The main search area has filters for 'Stealer', 'System', 'Country', 'State', 'City', 'Zip', 'ISP', 'Outlook', 'Per page', and 'Vendor'. A search bar contains the text 'accounts.google.com'. The interface also shows a 'Price' slider and a 'Search' button.

Activities of Stealer Operators in 2022

Logs are being sold for as little as \$1 and as much as \$10 on the Russian Market where logs are commonly sold.



\$ 1 ~ \$10

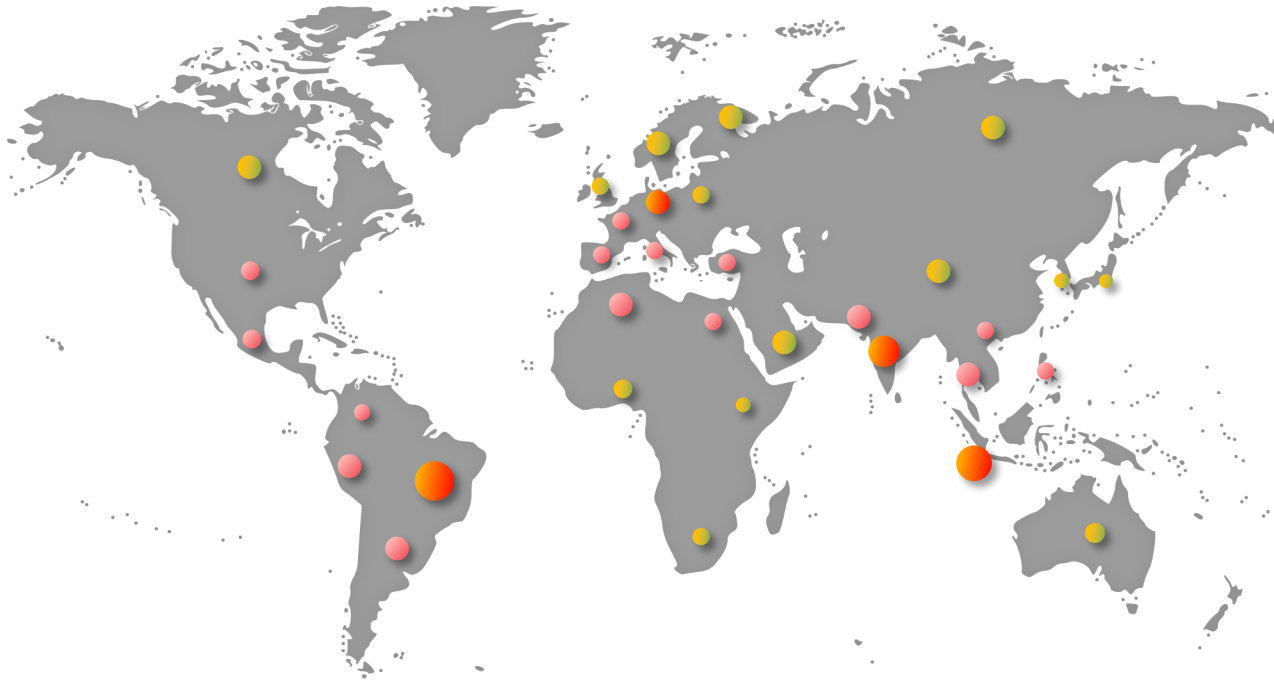


Activities of Stealer Operators in 2022

About **222 countries detected** by S2W, and **the number of logs** for sale is more than **12,426,205**.

Total Amount of Logs

12,426,205



Brazil	1,684,015
India	933,266
Indonesia	764,632
Germany	528,072
:	:
Thailand	311,246
France	290,625
Colombia	262,708
:	:
South Korea	104,087

Ecosystem of Stealer

Deep Dive in Stealer Ecosystem

The stealer ecosystem is becoming tighter and more organized.

People who specialize in each area of the offense are starting to team up and sell their services to the customer in the dark web forums and Telegram.

They make money through fees paid for using their services.

The image shows a screenshot of a Telegram chat interface. The chat title is "Need a traffer for the strait on the stiller!". The chat history includes a message from a user with a "NO AVATAR" profile picture, dated May 17, 2021. The message reads: "Hello, gentlemen of the forum! I realize that my proposal may seem strange, but I'll try anyway. We need a person who knows how to send high-quality traffic to the stealer. You spill, I give back in logs (70/30 or 80/20, in yo you need any specific requests from the logs, let me know, I can give them without touching. If anyone is interested in this offer, write to the forum PM or TG (@H4d3zzz).". Below this is a separator line and another message from the same user: "Hello! I realize that my proposal may seem strange, but I'll try anyway. We need a person who knows how to send high-quality traffic to the stealer. You spill, I give back in logs (70/30 or 80/20, in yo you need any specific requests from the logs, let me know, I can give them without touching. If anyone is interested in this offer, write to the forum PM or TG (@H4d3zzz).". A central text box with a black background and red text lists the following details:

- We collect traffers for Redline stealer**
- We take only cold wallets and pay 70% of them to the worker
- There is an auto-checker MetaMask , RoninWallet, PhantomWallet
- There is an auto-upload of videos directly in the bot / Cheat SEO .
 - We pay 200P for every 100 logs in the team
 - Any traffic without limits
 - Free FUD 0-3/26 private crypt
 - Instant automatic output of logs in the bot
- We also have contests and encourage good workers in the form of \$\$\$, we have the most friendly team that will not leave you in trouble and will always help.**

On the right side of the chat, there is a separator line and a message from the same user, dated Sunday at 9:25 PM: "Hello, Selling traffic & logs from different sources. Traffic is tested, good for phishing & spread. Logs are from Raccoon Stealer. Bank logs available. Any questions - PM or @BotLogs21".

Deep Dive in Stealer Ecosystem

Stealer operating Team

A group that makes stealer, licenses and builds it

Traffic Teams

A group that spreads stealer and other malware and monetizes logs



Ecosystem

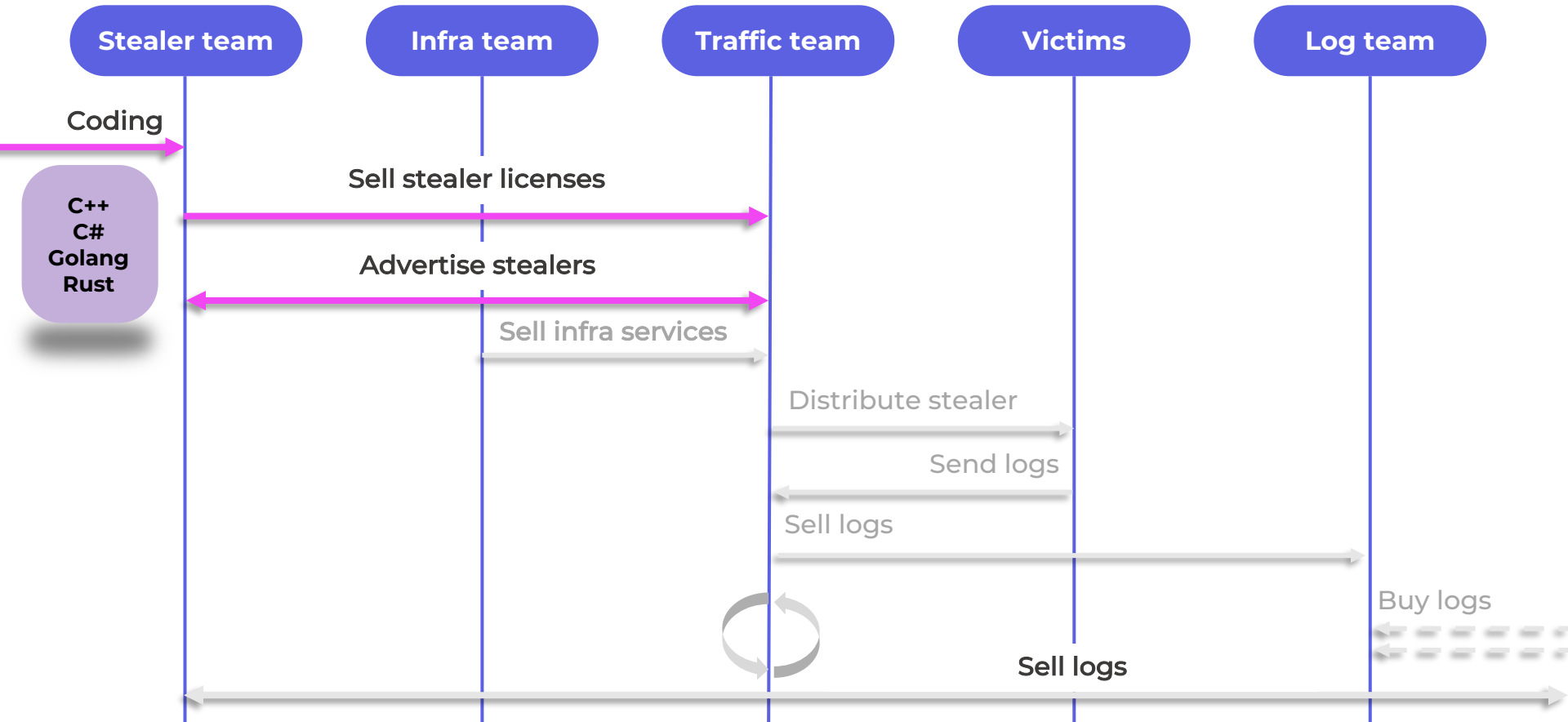
Infrastructure Team

A group that provides the panels, the hosting servers needed to run and distribute it, the tools to attack

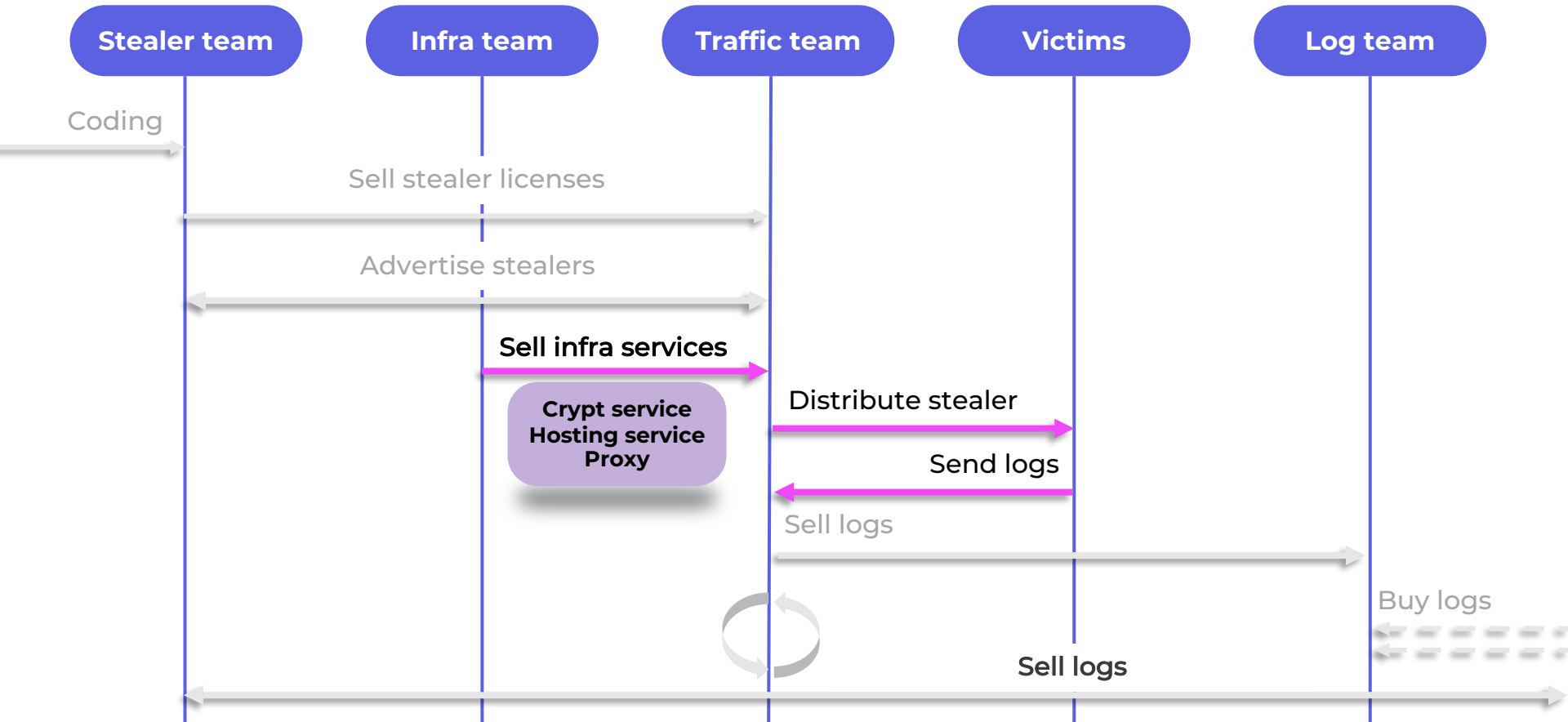
Log Team

A group that sells only logs, which can be sold per item, per country, or per stealer.

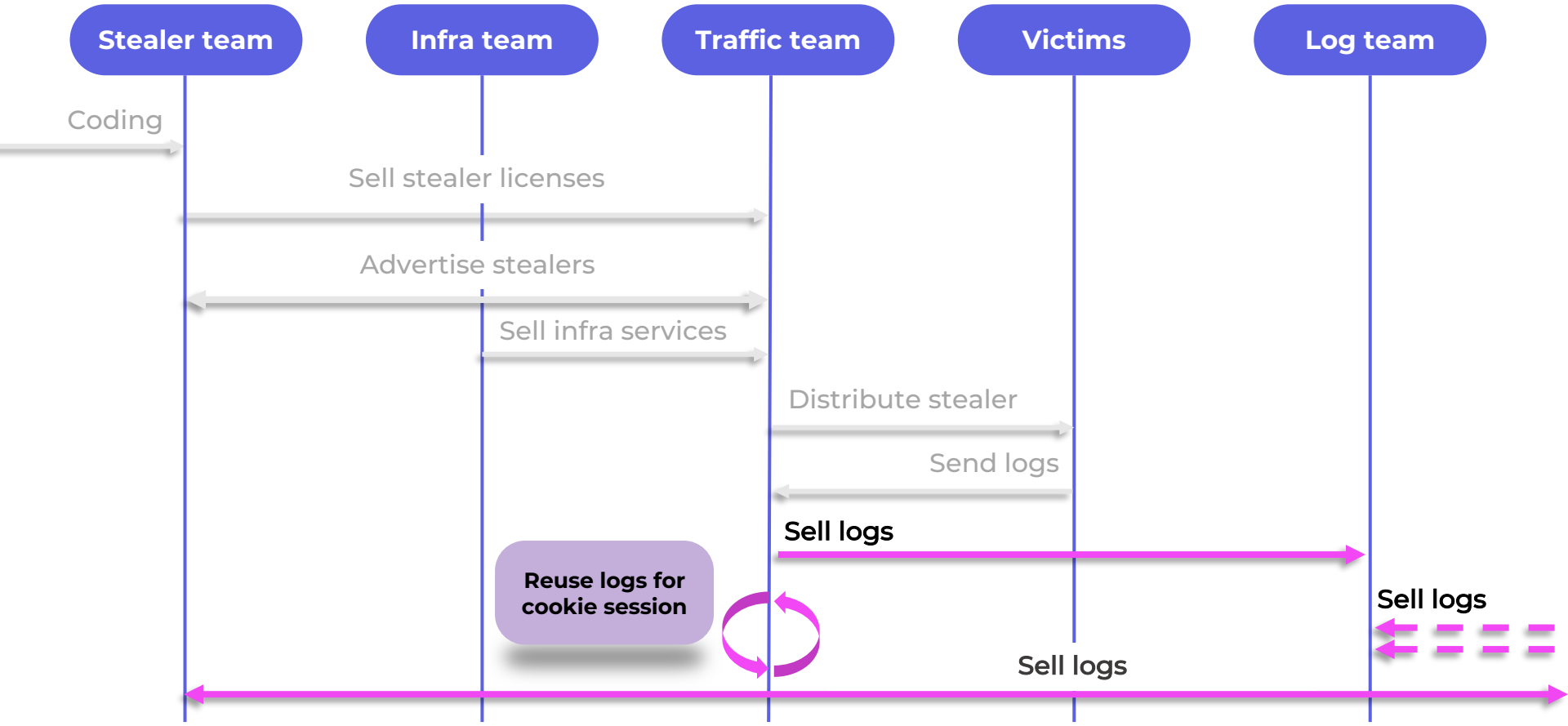
Deep Dive in Stealer Ecosystem



Deep Dive in Stealer Ecosystem

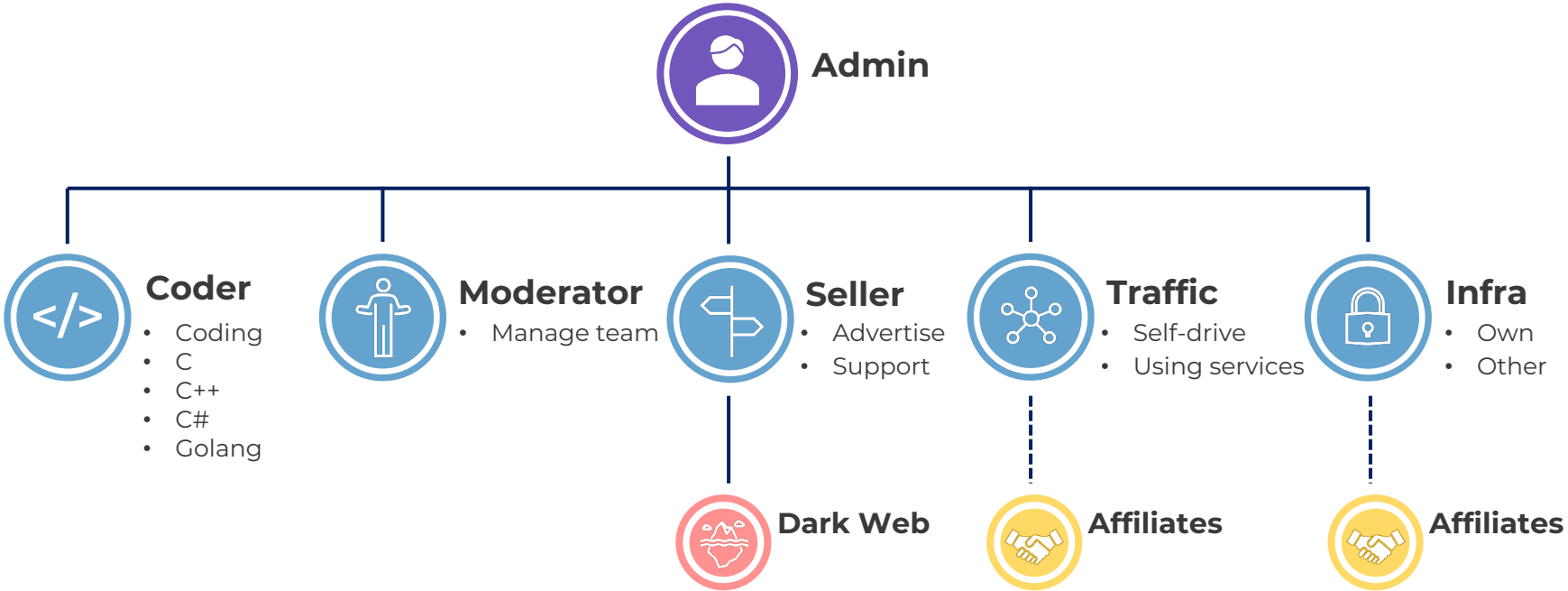


Deep Dive in Stealer Ecosystem



Stealer Operator

The operator group develops stealer, monetizes it as a service, and sells it on dark web forums.



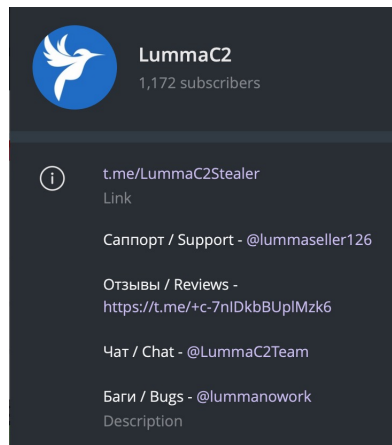
Stealer Operator

LummaC Stealer

Post Started: 2022-01-31

Contact Method: Telegram

Role: **Admin, Coder, Seller, Support, Advertisement**



LummaC2
1,172 subscribers

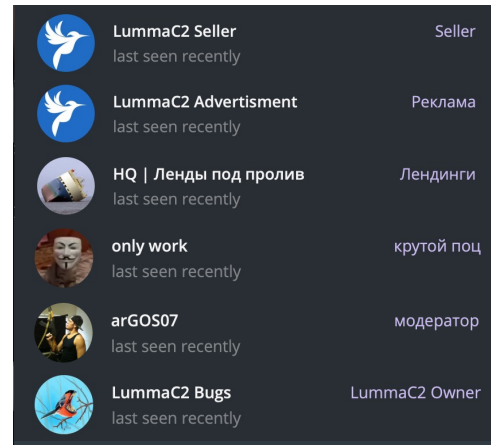
t.me/LummaC2Stealer
Link







Санпорт / Support - @lummaseller126

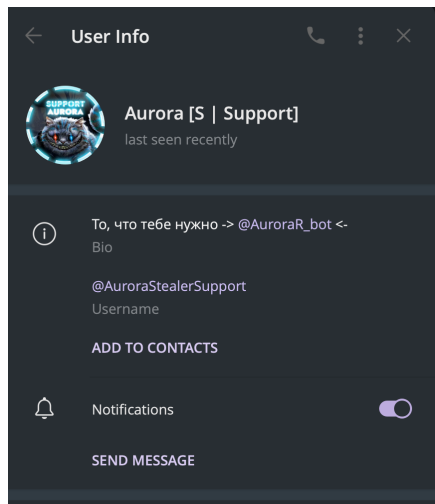
Отзывы / Reviews -
<https://t.me/+c-7nIDkbBUplMzk6>

Чат / Chat - @LummaC2Team


Баги / Bugs - @lummanowork
Description



	LummaC2 Seller last seen recently	Seller
	LummaC2 Advertisement last seen recently	Реклама
	HQ Ленды под пролив last seen recently	Лендинги
	only work last seen recently	крутой поц
	arGOS07 last seen recently	модератор
	LummaC2 Bugs last seen recently	LummaC2 Owner



User Info

 **Aurora [S | Support]**
last seen recently

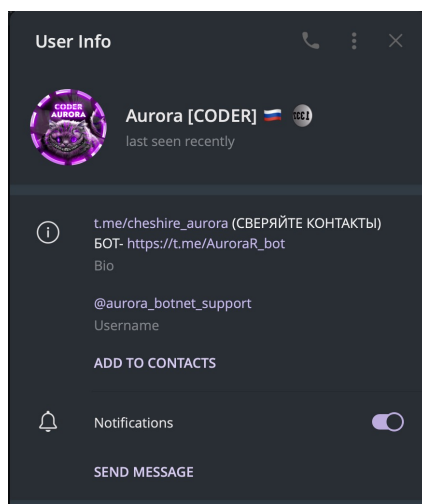
[To, что тебе нужно -> @AuroraR_bot <-](https://t.me/AuroraR_bot)
Bio

@AuroraStealerSupport
Username




ADD TO CONTACTS

Notifications

SEND MESSAGE



User Info

 **Aurora [CODER]**  
last seen recently

[t.me/cheshire_aurora \(СВЕРЯЙТЕ КОНТАКТЫ\)](https://t.me/cheshire_aurora)
БОТ- https://t.me/AuroraR_bot
Bio

@aurora_botnet_support
Username

ADD TO CONTACTS

Notifications

SEND MESSAGE

Aurora Stealer

Post Started: 2022-08-21

Contact Method: Telegram

Role: **Admin, Coder, Seller, Support**

Other Services: Install, Crypt, Traffic

Stealer Operator

Eternity Group

Started: 2022-02-02

Contact Method: Telegram

Role: **Admin, Coder, Seller, Support, Moderator**

Other Services: Install, Brute Force, Crypt, Traffic

Work: 09:00 ~ 00:00

AGRAT Group (same as Eternity)

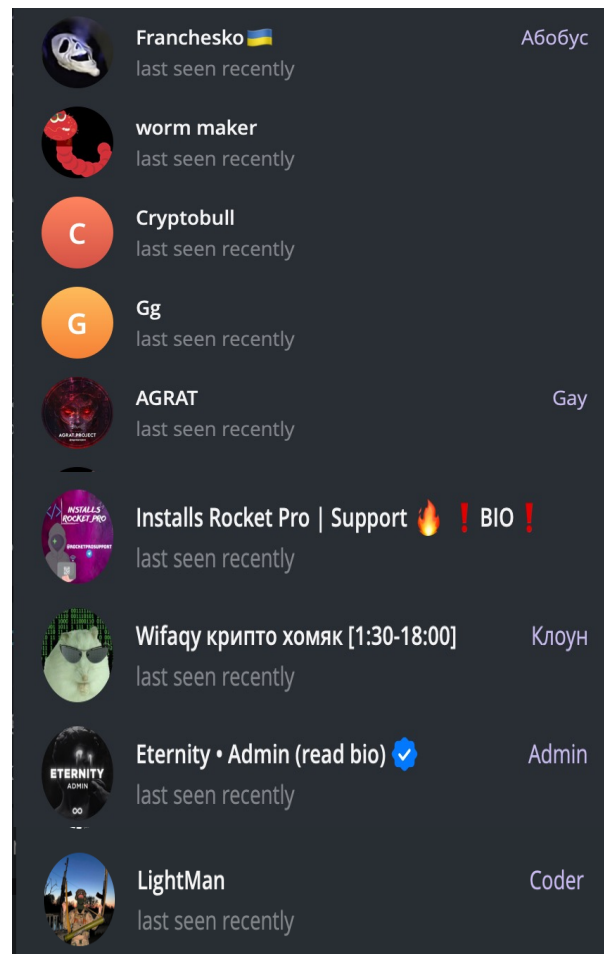
Started: 2022-02-09

Contact Method: Telegram

Role: **Admin, Coder, Seller, Support, Moderator**

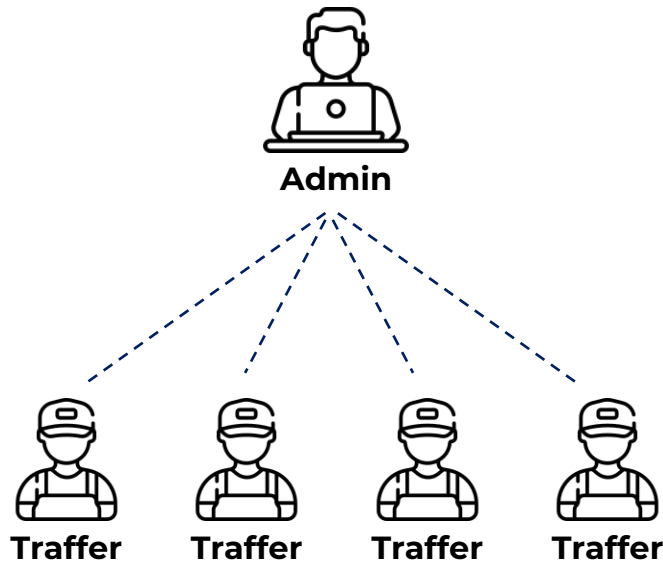
Other Services: Install, Brute Force, Crypt, Traffic

Work: 09:00 ~ 00:00

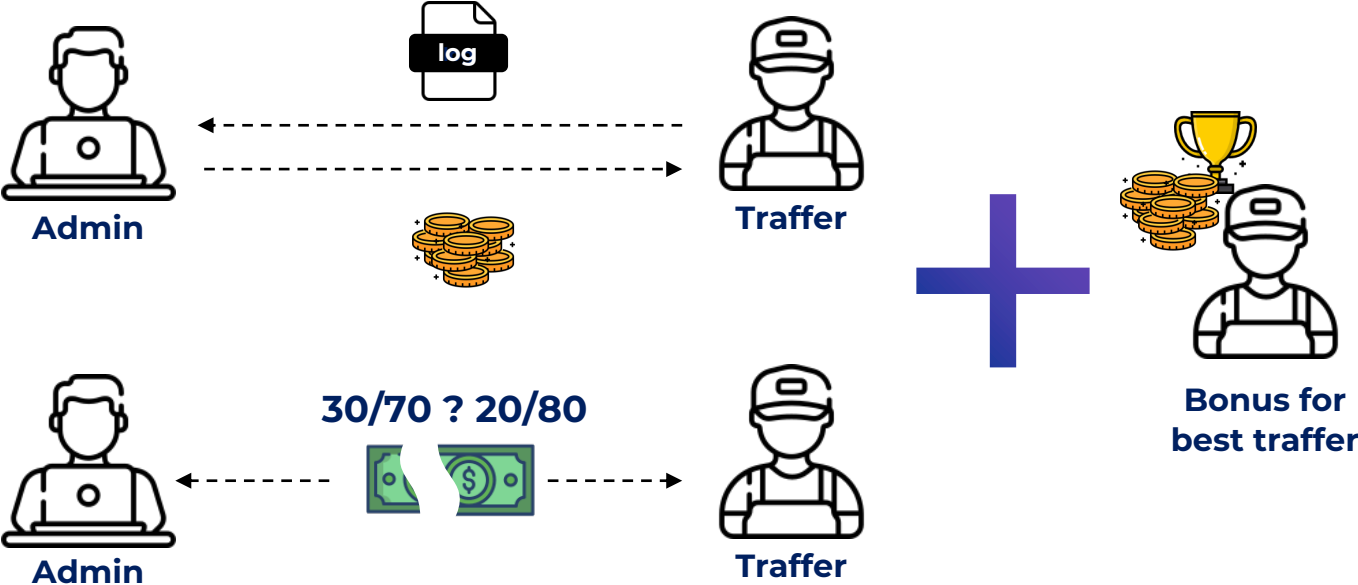


Traffic Team

A traffic team is a group whose primary purpose is to “distribute stealer” and “get Logs”. They purchase stealer licenses sold within the forums or affiliate with stealer operators and provide builds to members of the team, called *Traffers*.

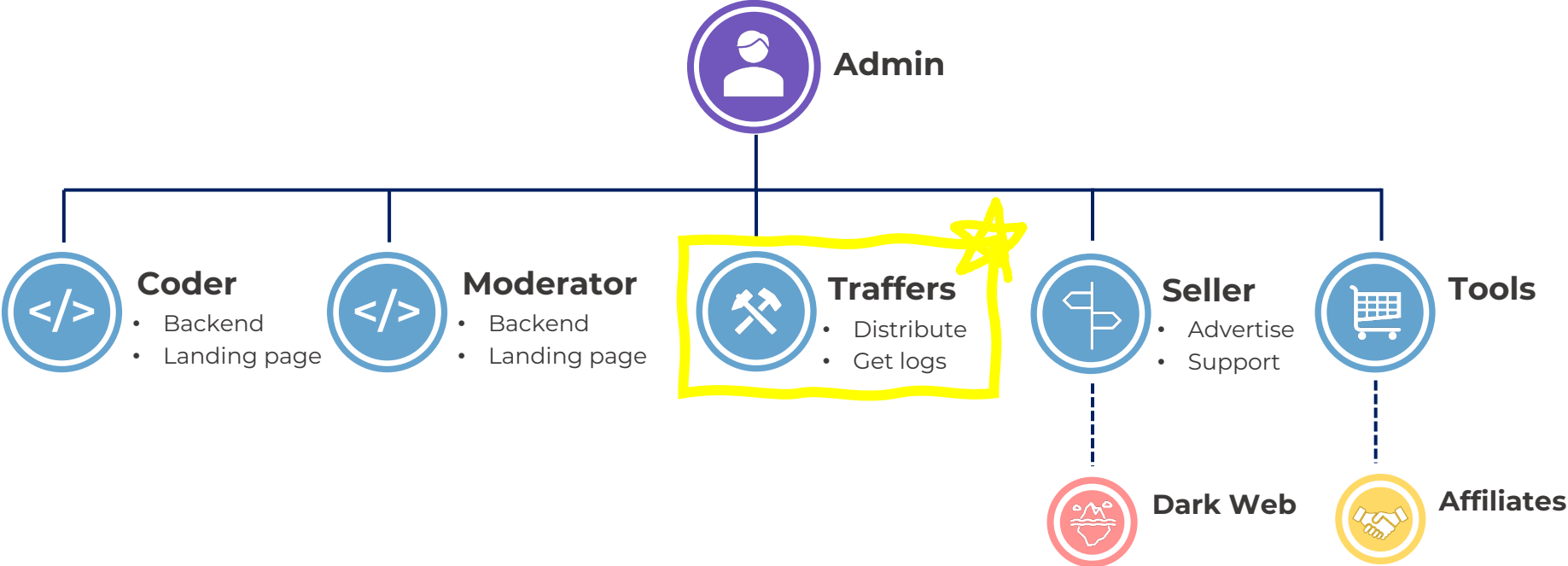


Traffic Team



Traffic Team

The operator group develops stealer, monetizes it as a service, and sells it on dark web forums.



Relation: Stealer Team – Traffic Team

Aurora	Meta	Raccoon
Amnesia Team	Crypton Team	BADMAN Team
Space Team	Keqing Team	ExTeam
HellRide Team	Ghostbusters	1377 Team
Sakura Team	Lucky Team	NETRUNNERLZT
KZ	HellRide Team	2x2Team
YungRussia	REQX Team	4fun-lolz
Shark Team	KZ	Fabbi-lolz
Xane Team	Dragon Advert	DevilTraff Team
DevilTraff Team	Shiba Traffer Team	
ARIZONA Team	Milky M1 team	
Milky M1 team		

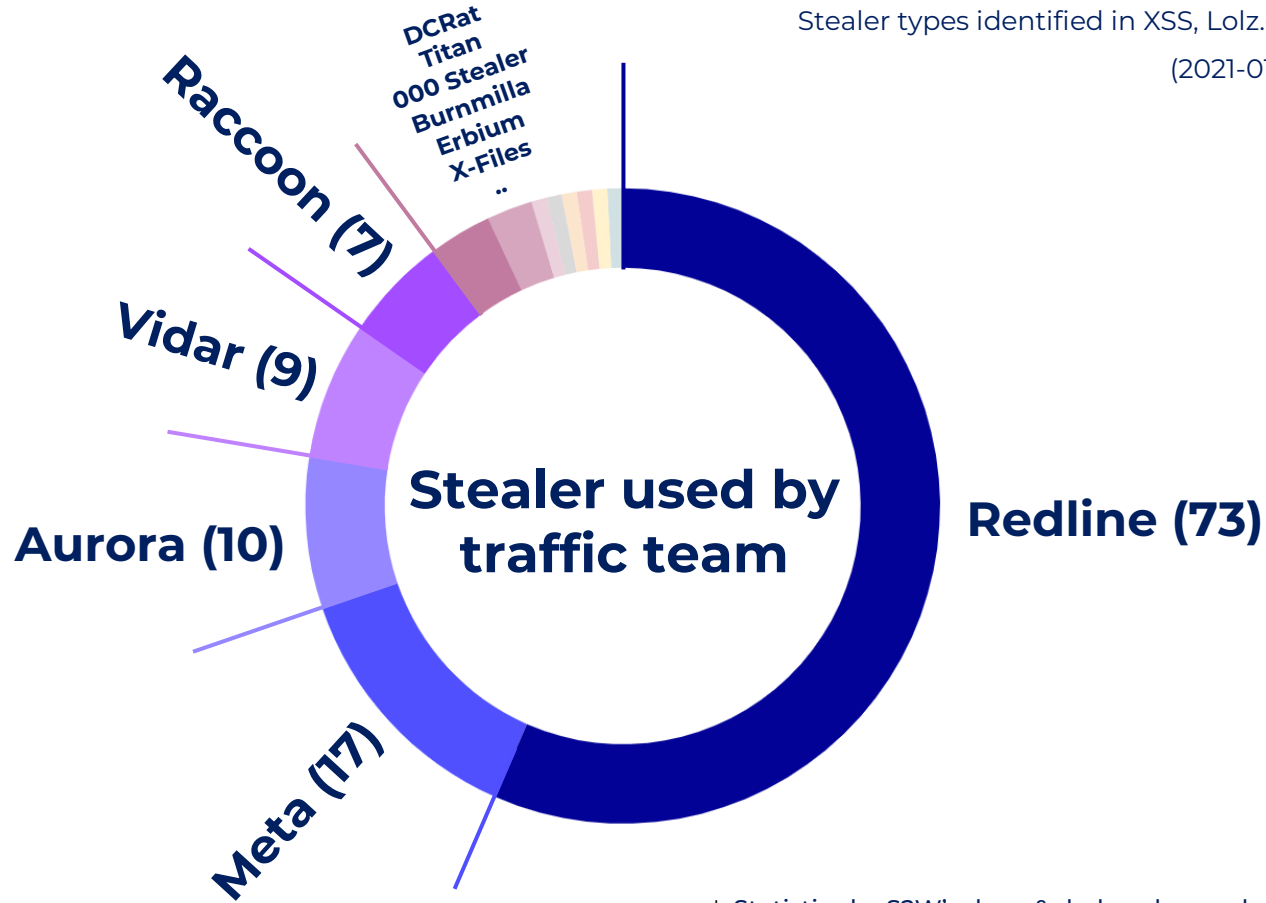
Traffic teams identified in XSS, Lolz.guru, and Exploit
(2021-01-01 to 2022-12-31)

Relation: Stealer Team – Traffic Team

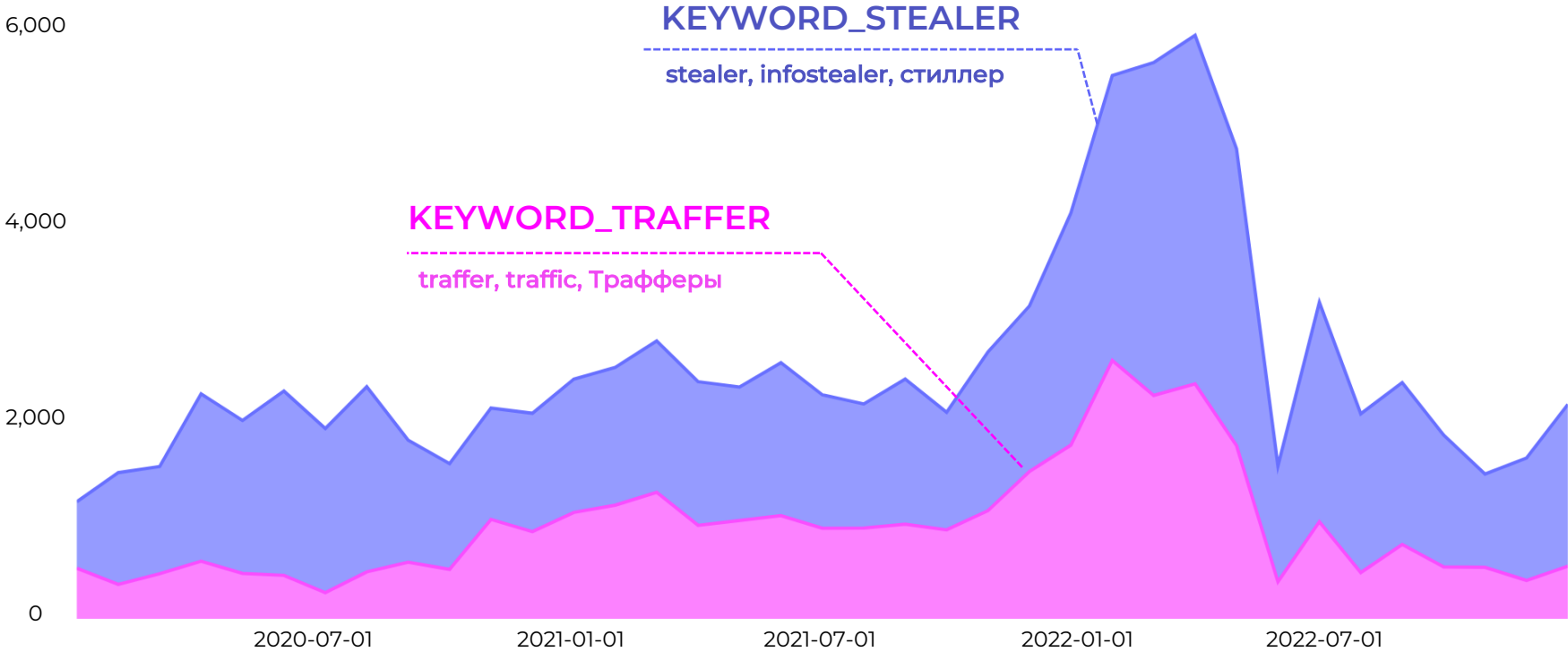
Redline				Titan
Strait of Traffic Team	CripsGang	War and Peace	WebCrew Logs Team	Xane Team
Darkweb Team	Universal Team	Invokere-lolz	Shark Team	
Sisky	Innovation Team	PPI Monster	SPACEUP Team	
eegrabber-lolz	Lelouch Team	Shadow Team	AIPachino	Erbium
SWEETYLOGS	BetterTraffic	Amnesia Team	Oblivion Team NFT	Minion Team
GMC team	Kekonaut-lolz	SQL-lolz	EuroLogs	
Soldbum Team	LeksKB-lolz	Paracetamol Team	Party team	
31 Boulevard Team	Game Square team	Santares Team	ExTeam	Vidar
BOMBSPAM Team	Dark Dynasty	Hydra Family	Awesome Team	
SADAX Team	1377 Team	Krek3621	Xanax	ARIZONA Team
Qwiks Team	Heavn's Bliss Team	Vertigos de Team	...	Shiba Traffer Team

Traffers identified in XSS, Lolz.guru, and Exploit
(2021-01-01 to 2022-12-31)

Relation: Stealer Team – Traffic Team



Number of Stealers \propto Number of Trafffers?



* Statistics by S2W's deep & dark web search engine, Xarvis
(2020.01.01 ~ 2022.12.31)

How do they distribute stealers?

Manual

The traffic team targets phishing pages and YouTube that are accessible to a large number of users to mass distribute the stealer.

Work manual from slide

Hello everyone, I'm glad that you came to see my manual, in which I put all my knowledge about traffic with all my heart. After reading it, I guarantee that everything will work out for you and you will have money

INTRODUCTION

What is the essence of the work?
We must spread the virus, which the victim will then launch. The virus can be disguised as a cheat for any game. Or you can disguise it as a program. Basically, everyone works on YouTube, uploading videos with a virus to them.
Examples: Crack Adobe Photoshop, fortnite hack, bandicam crack
I think you get the point. But everyone pours such garbage, so turn on your imagination.

AMNESIA | Library

Hello! I will tell you how to completely secure yourself on the network, and physically protect your data, both from a PC and from a phone.[Safety in life and network.](#)

You can fully set up your PC, but at the same time sit in your telegram from a regular phone, withdraw money to your card, distribute any personal information about yourself.

For each thread you can catch on and stretch the whole ball, every little thing is important. I won't teach you how to live, tell you what to do, what not to do, tell how safe the scheme is at the output, you yourself will understand everything in the end, and collect your config. [Entry](#)

Tools used by Traffic Team

- Proxy
 - Proxy list required for communication between C&C server and infected PCs.
 - Ex) *Space Proxy, Luxury Proxy, Proxy Store, etc..*
- YouTube Upload Tools
 - Automated uploading of videos to a specific YouTube account to perform malicious actions via browser cookie values and proxy values in captured logs.
 - Ex) *YouTube365, Proxy 911, @YT_TurboT*
- SEO
 - an indicator depending on what we take as an example. In terms of YouTube, this is a collection of tags, titles, descriptions, and more.
 - Ex) *@CheckSEOBot, VidiQ*

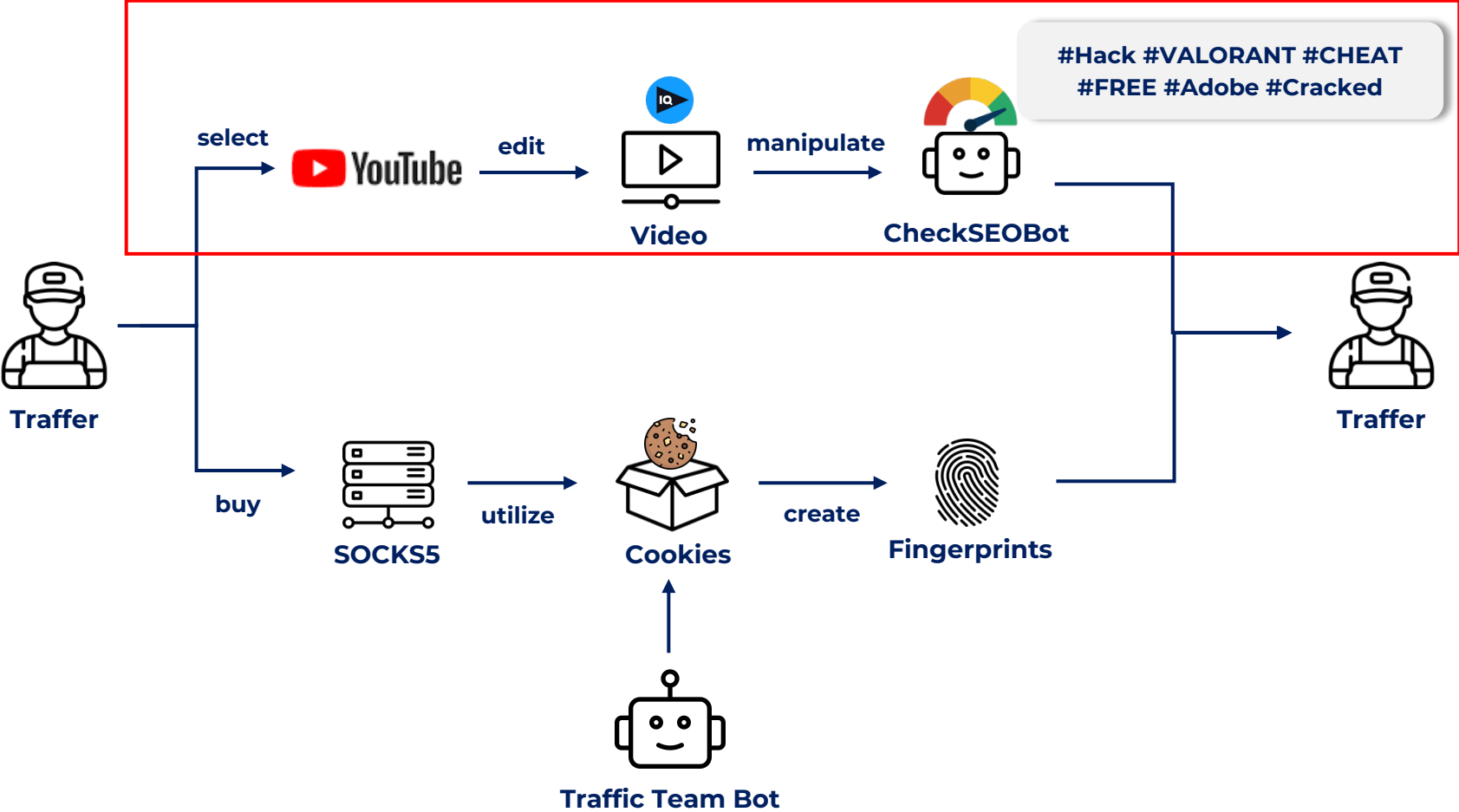
Tools used by Traffic Team

- Proxy
 - Proxy list required for communication between C&C server and infected PCs.
 - Ex) *Space Proxy, Luxury Proxy, Proxy Store etc..*
- YouTube upload tools
 - Automated uploading of videos to a specific YouTube account to perform malicious actions via browser cookie values and proxy values in captured logs.
 - Ex) *YouTube365, Proxy 911, @YT_TurboT*
- SEO
 - an indicator depending on what we take as an example. In terms of YouTube, this is a collection of tags, titles, descriptions, and more.
 - Ex) *@CheckSEOBot, VidiQ*

Tools used by Traffic Team

- Proxy
 - Proxy list required for communication between C&C server and infected PCs.
 - Ex) *Space Proxy, Luxury Proxy, Proxy Store etc..*
- YouTube Upload Tools
 - Automated uploading of videos to a specific YouTube account to perform malicious actions via browser cookie values and proxy values in captured logs.
 - Ex) *YouTube365, Proxy 911, @YT_TurboT*
- **SEO (Search Engine Optimization)**
 - In terms of YouTube, this is a collection of tags, titles, descriptions, and more that make video to be the top of the search result.
 - Ex) **@CheckSEOBot, VidiQ**

Traffer's process of spreading malware via YouTube



Traffer's process of spreading malware via YouTube

The image shows a YouTube video player on the left and search results on the right. The video player displays a video titled "[NEW] VALORANT HACK FREE \ VALORANT HACK 2023 DOWNLOAD \ VALORANT CHEAT DOWNLOAD \ FREE DOWNLOAD LINK IN COMMENTS!!!!". The video thumbnail features the text "BEST VALORANT CHEAT" and a woman's face. The video has 911 views, 53 likes, and a URL of "youtu.be/gcgjBTWNT4". The video description includes "Hot tags" such as "hack valorant", "valorant wallhack", "valorant cheat download", "valorant aimbot download", "valorant cheats", "valorant hack esp", "valorant hack download free", "valorant hack 2023", "valorant free hack", "valorant cheats free", "cheat valorant", and "valorant aimbot".

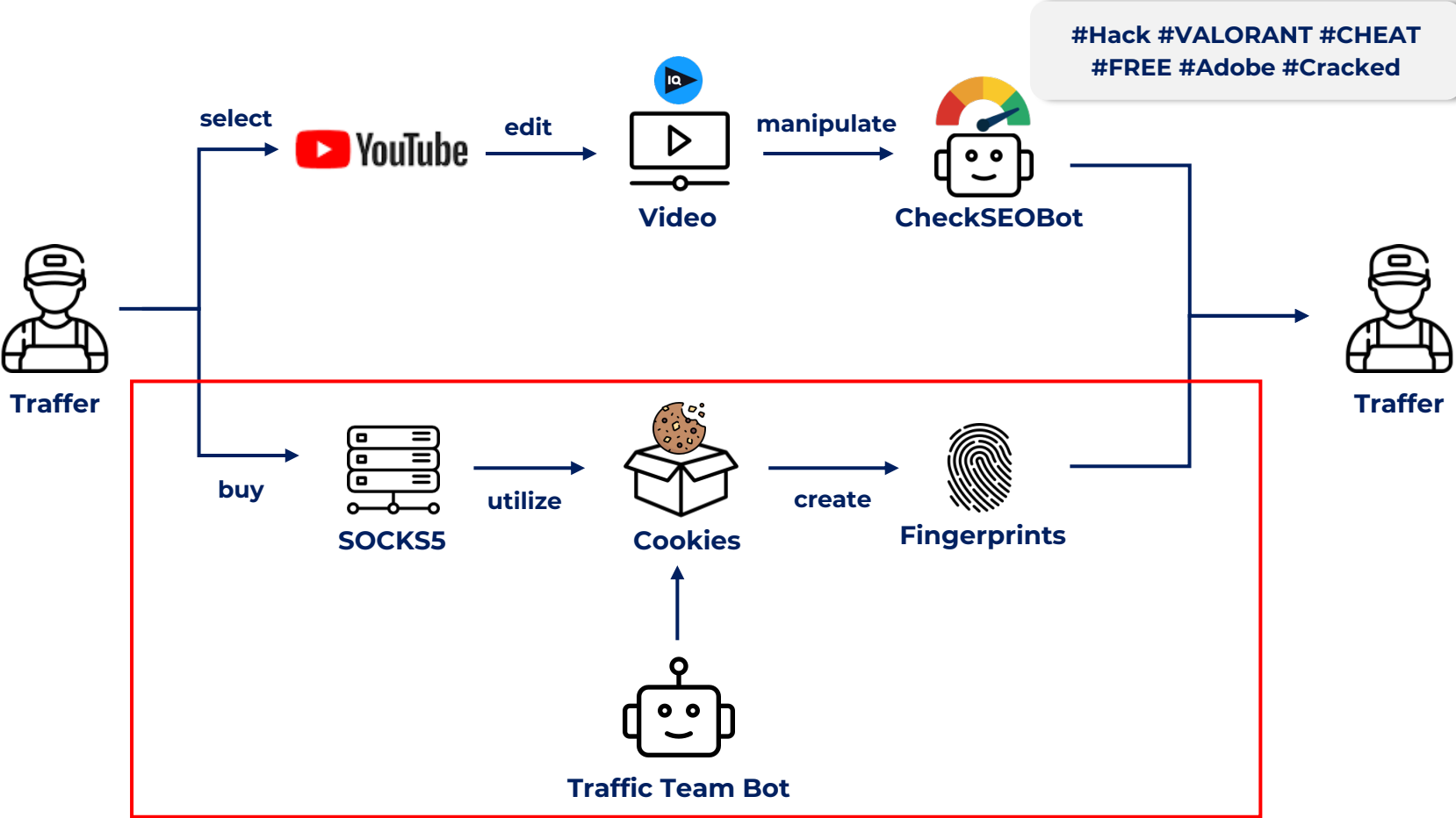
The search results on the right show a search for "adobe photoshop crack". The top result is a video titled "Download and Install Best Free Adobe Photoshop Express on Windows Laptops !! 2023" by Easy Classes, with 3.7K views. The video thumbnail features the text "INSTALL FREE ADOBE PHOTOSHOP" and the Adobe Photoshop logo. The video description includes "How to Download and Install Adobe Photoshop Express on any Windows Laptops 2023. Join this channel to get access to perks: ...".

The search results also show a video titled "INSTALACIÓN de ADOBE PHOTOSHOP 2022 V.23.3.2 en ESPAÑOL 100% ACTIVADO" by Técnico PCs, with 3.56 views. The video thumbnail features the text "INSTALACIÓN ADOBE PHOTOSHOP 2022 V. 23.3.2 100%ACTIVADO ULTIMA VERSION" and a woman's face. The video description includes "Actualiza tu plataforma de Photoshop 2022 :) Si te fue útil mi contenido, apóyame con una SUSCRIPCIÓN porfa :) Haciendo una ...".

The search results also show a "vidIQ" widget with a search panel, a "Get daily custom AI-generated ideas" section, a "Change from adobe acrobat to adobe photoshop crack" section, a "Never miss a trending video" section, and an "Overall score: High" section with a score of 75 out of 100. The widget also shows a "Volume" bar at 67 and a "Competition" bar at "Very low".

Show how high a trending index the video has

Traffer's process of spreading malware via YouTube



Traffer's process of spreading malware via YouTube

Новый профиль Массовый импорт 🔍 НОВЫЙ ОТПЕЧАТОК + СОЗДАТЬ ✕

ОСНОВНОЕ ДОПОЛНИТЕЛЬНО АНКЕТА

Название: Статус:

Теги:

WINDOWS MACOS LINUX

NONE FACEBOOK GOOGLE ТИКТОК CRYPTO

БЕЗ ПРОКСИ НОВЫЙ ПРОКСИ ВЫБРАТЬ ПРОКСИ

Вставьте куки или перетащите файл drag and drop
КУКИ ИЗ ФАЙЛА

Useragent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (

WebRTC: ВЫКЛ РЕАЛЬНЫЙ ПОДМЕНЯТЬ ВРУЧНУЮ

Canvas: ВЫКЛ РЕАЛЬНЫЙ ШУМ

WebGL: ВЫКЛ РЕАЛЬНЫЙ ШУМ

Название:

Статус:

Теги:

Платформа: Windows

UserAgent:

Прокси: Без прокси

WebRTC: Подменять

Canvas: Реальный

WebGL: Реальный

WebGL инфо:

Client Rects: Реальный

Часовой пояс: Авто

Язык: Авто

Геолокация: Авто

Процессор: 8 ядер

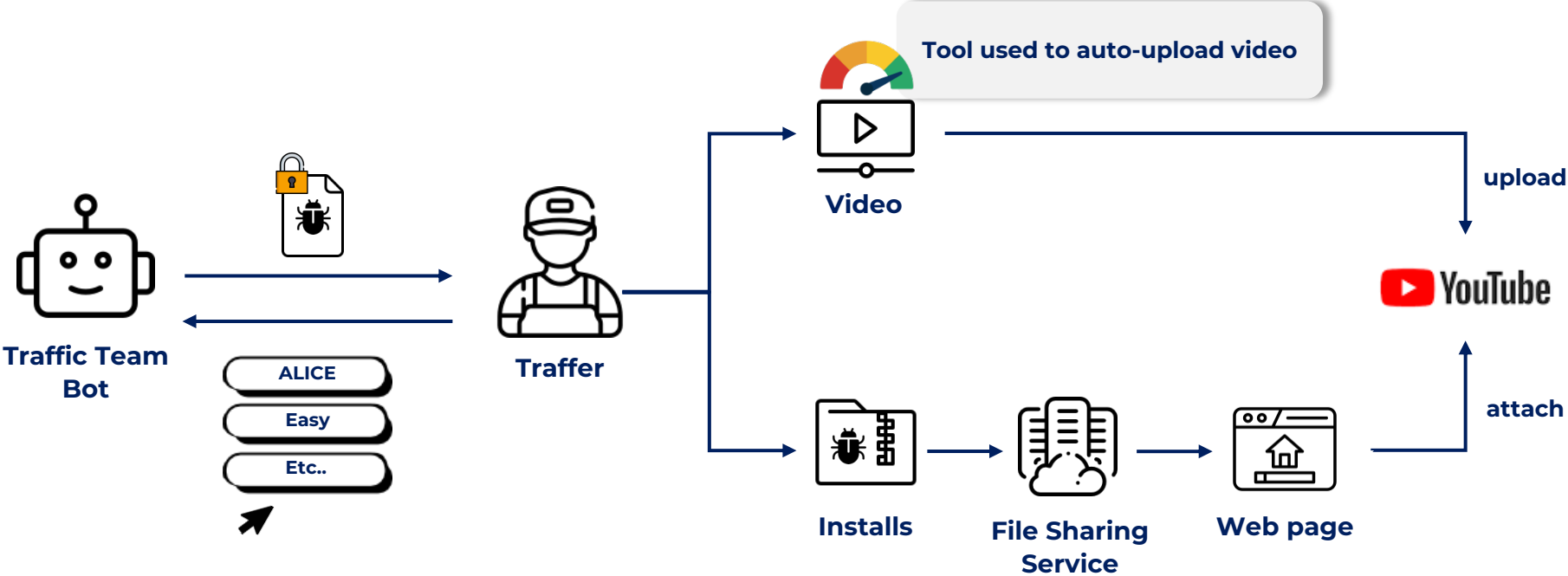
Память: 8 ГБ

Экран: Реальный

Аудио: Реальный

Set the browser fingerprints & proxy & session data

Traffer's process of spreading malware via YouTube



Traffer's process of spreading malware via YouTube

Valorant Hack
May 10, 2023


Valorant Hack

Download link ➔ **CLICK**

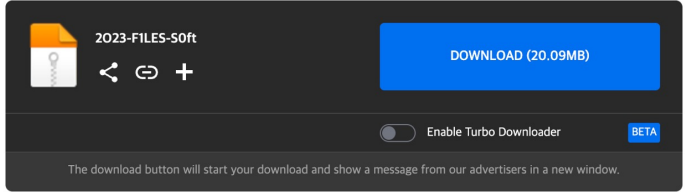
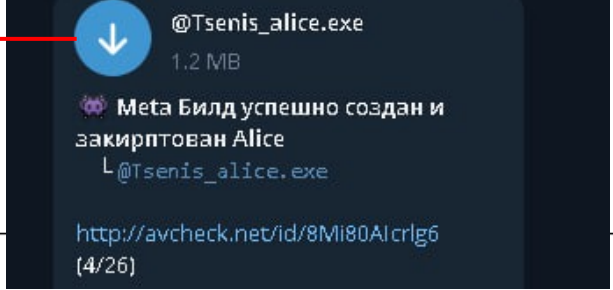
Password: 1234

🚫 IF YOU HAVE PROBLEMS DOWNLOADING / INSTALLING!
If you can't download / install the archive, you need to:

1. Disable / remove antivirus (files are completely clean)
2. Disable Windows Smart Screen, as well as update the Visual C++ package



MediaFire
SIGN UP LOG IN



To avoid detections, use a free web page to redirect download URL

Traffic Team: Threat cases

Among Us Cheat Free Download # Among Us Mod ... - YouTube



Download - <https://telegra.ph/Software-2023-02-21-6> Password - 2023 INSTRUCTIONS:1) Turn off Windows Defender2) Download the file from...
YouTube · Dedex NA ·

AccountEdge Pro Installation 2023 - YouTube



AccountEdge Pro Installation & Upgrade Download - <https://telegra.ph/Software-2023-02-21-6> ... Show more. Show more. Show...
YouTube · _Anant_ ·

Free Download QuickBook 2023 Full Version - YouTube



Hello everyone! This is my own app and website, so please enjoy! DOWNLOAD LINK: <https://telegra.ph/Software-2023-02-21-6> Password: ...
YouTube · The New World ·

Wallpaper Engine UNLOCK 2023 - YouTube



DOWNLOAD LINK: <https://telegra.ph/Software-2023-02-21-6> Wallpaper Engine CRACK 2023 | Wallpaper...
YouTube · sergio villagra · 2023. 2. 24. ·

youtube.com
<https://www.youtube.com/watch>

CSGO SKINCHANGER 2023 UNDETECTED - YouTube



CSGO SKINCHANGER UNDETECTED 2023 DOWNLOAD: <https://telegra.ph/Software-2023-02-21-6> PASSWORD: 2023- Off Defender...
YouTube · Tomás ·

Best PC up software/cheats 2023
February 21, 2023

↓ DOWNLOAD LINK ↓

Download Link : <https://>

Additional link : <https://>

Password : 2023



**SOFTWARE
CRACK
CHEATS**



INFO:
This is a great guide on how to install program crack for free. I bought this crack, but I give it to you for free.

How to install:
1.Unzip all files from archive
2.Run Installer
3.Complete full installation



Threat cases: Lumma Stealer targeted Korean YouTuber

전체 메일함 안읽음 9 / 28 <안내> 네이트 담당자를 사칭한 스팸

답장 | 전체답장 | 전달 | 간편답장 | 삭제 | 완전삭제 | 스팸신고 | 이동 | 추가

Re: Bandai Namco YT Offer 2023

보낸사람 : "DSADS" <bandai.namco.ma@kakao.com> 주소록추가 수신지단

Good morning, our esteemed partner! Bandai Namco Entertainment is happy to welcome you. If you've made it to this point, it means you're doing great work, and we're sure we can be useful to each other!

Below you'll find the keys to the materials in question in our response letter. The materials contain more detailed terms of cooperation.

A little bit about our game that you will be promoting.
A new RPG from the hugely popular manga and anime series ONE PIECE, commemorating the 25th anniversary of the series!
The famed pirate, Monkey.D.Luffy, better known as Straw Hat Luffy, and his Straw Hat Crew, are sailing across the New World in search of the next island and the next adventure that awaits them.
But during their voyage they are caught in a storm and shipwrecked. They find themselves washed up on a lush tropical island surrounded by constantly raging storms...

● Link to the game on Steam:
https://store.steampowered.com/app/814000/ONE_PIECE_ODYSSEY/

To read the PDF cooperation agreement, as well as the game trailer, please follow this link:
DROPBOX:<https://www.dropbox.com/s/rcrreonk17d0ah9/One%20Piece%20Odyssey%20Youtube%20Deal.zip?dl=1>

Tesla US 10시간 전
<굿즈 관련 재공지 드립니다>

우리 블루베리들의 사랑과 관심을 제가 너무 간과한 듯 합니다. 처음 굿즈 주문제작을 요청할 때, 각 제품마다 사실 많은 수량 제작을 요청하지 않았었거든요. 그런데 예상보다 굿즈 구매에 많은 관심을 주셔서 자세히 보기

533 👍 421

Tesla US
@tesla-us-23
구독자 312인명

실시간 | 재생목록 | 커뮤니티 | 채널 | 정보

Tesla US 10시간 전
<굿즈 관련 재공지 드립니다>

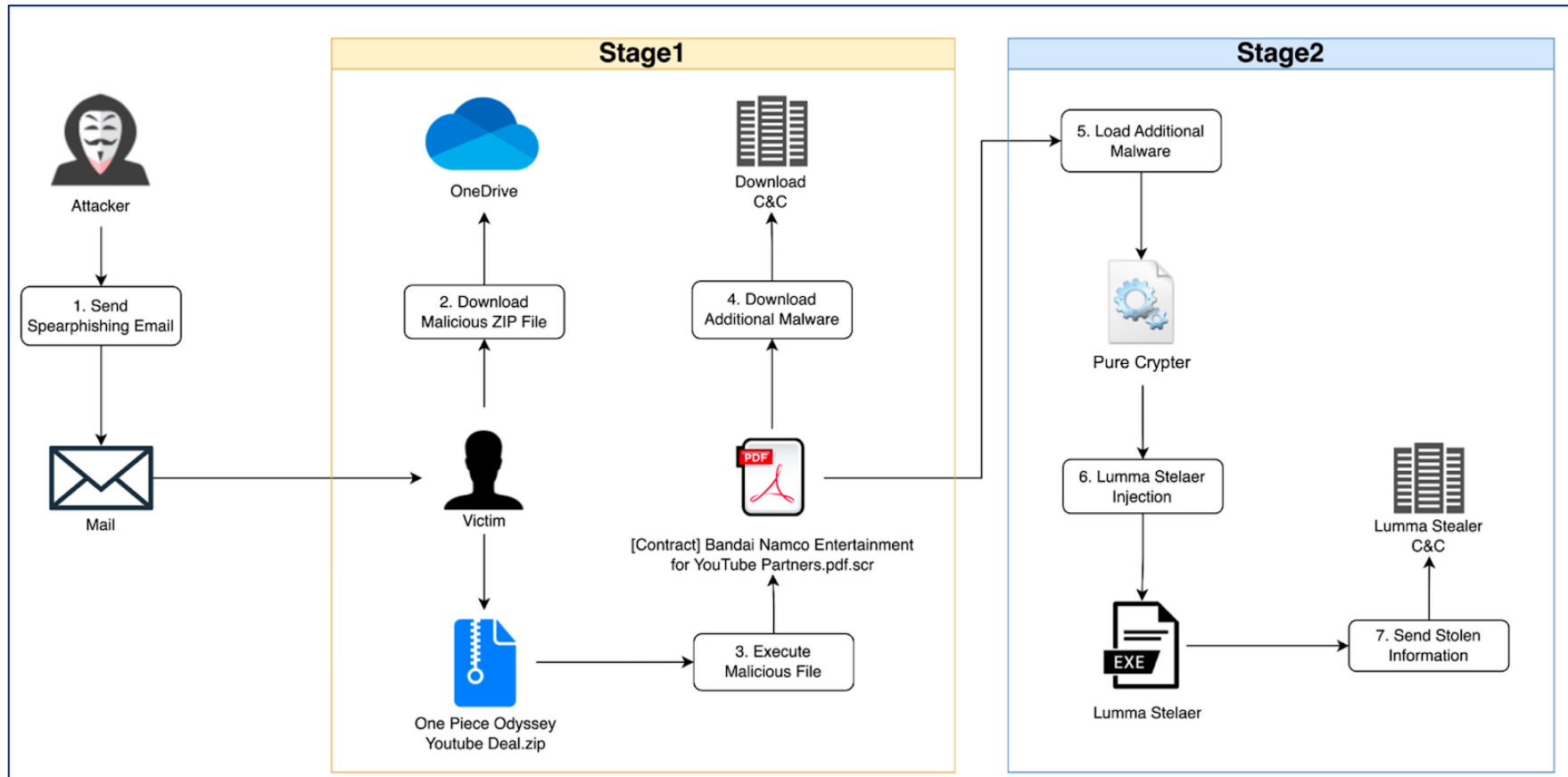
우리 블루베리들의 사랑과 관심을 제가 너무 간과한 듯 합니다. 처음 굿즈 주문제작을 요청할 때, 각 제품마다 사실 많은 수량 제작을 요청하지 않았었거든요. 그런데 예상보다 굿즈 구매에 많은 관심을 주셔서 자세히 보기

533 👍 421

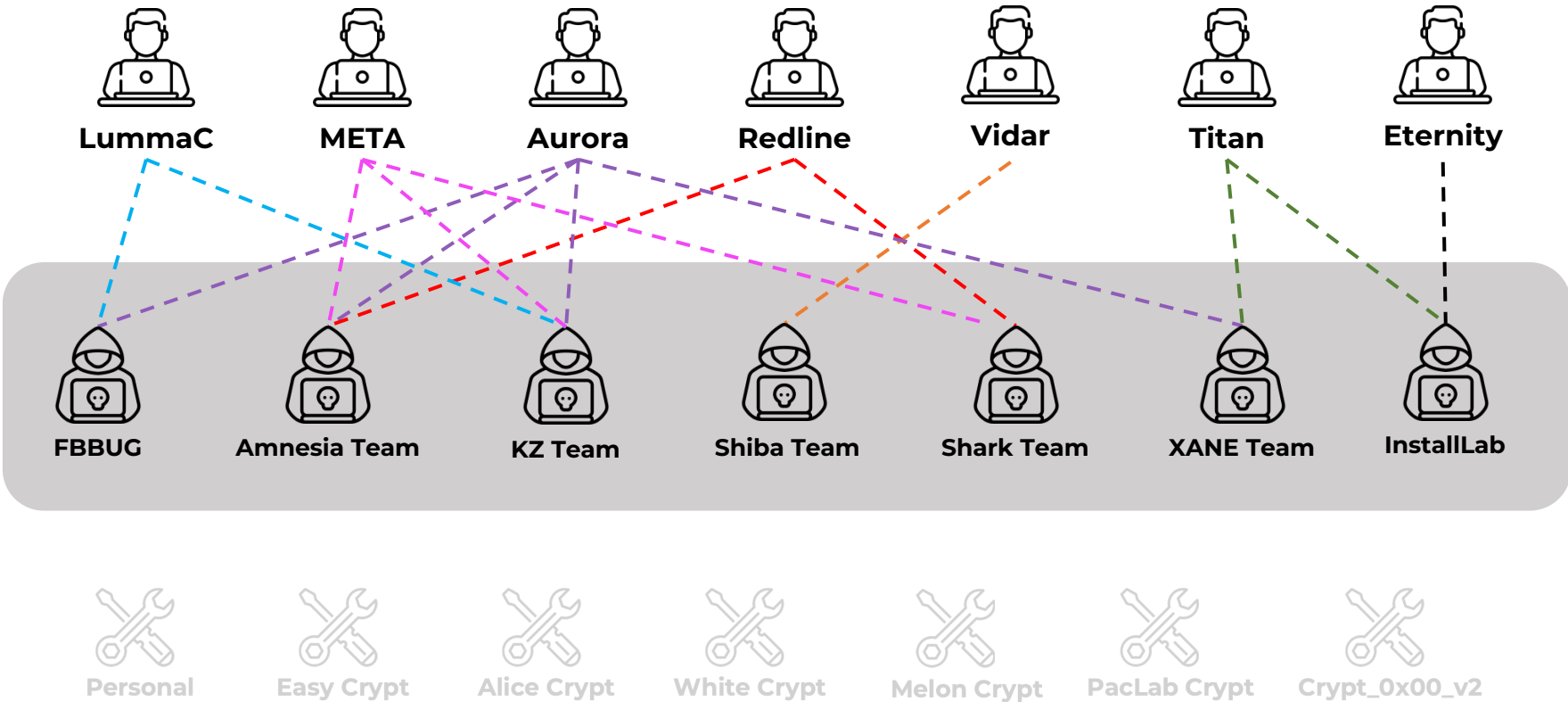
Tesla US 3일 전
<사연 포스트 관련 내용 수정 공지드려요~>

제일 중요한 걸 빼먹어서 수정글 공지드려요^^

Threat cases: Lumma Stealer targeted Korean YouTuber



Relationship with Stealer Operating Group



Relationship with Crypt



LummaC



META



Aurora



Redline



Vidar



Titan



Eternity



FBBUG



Amnesia Team



KZ Team



Shiba Team



Shark Team



XANE Team



InstallLab



Personal/Unknown



White Crypt



Alice Crypt



Easy Crypt



Melon Crypt



PacLab Crypt



Crypt_0x00_v2

Relationship with Tools



Case related Stealer Ecosystem

The string "**@im_HiLLi**" was present in the Build ID, which can be arbitrarily specified by the attacker when creating the stealer, and the same string was found in **another Meta** stealer and **Aurora** stealer.

The image shows a Telegram chat interface on the left and two expanded views on the right. The chat shows a message from 'Flora' containing a file 's368_r2015_v3k_9.zip' (144.6 KB) and purchase details. The expanded view on the top right shows the 'META STEALER' logo and a Telegram link, with the 'Build ID: @im_HiLLi' highlighted. The expanded view on the bottom right shows a JSON configuration for 'AURORA STEALER' with the 'BuildID' field set to '@im_HiLLi', also highlighted.

```
*****  
*                                     *  
*          ( M | E | T | A )          *  
*                                     *  
*          Telegram: https://t.me/metastealer_bot *  
*                                     *  
*****  
Build ID: @im_HiLLi
```


```
{ "Type": "Browser", "Info": { "Name": "User-PC", "BuildID": "@im_HiLLi", "GroupID": "ALL", "OS": "Windows" } }
```

META STEALER

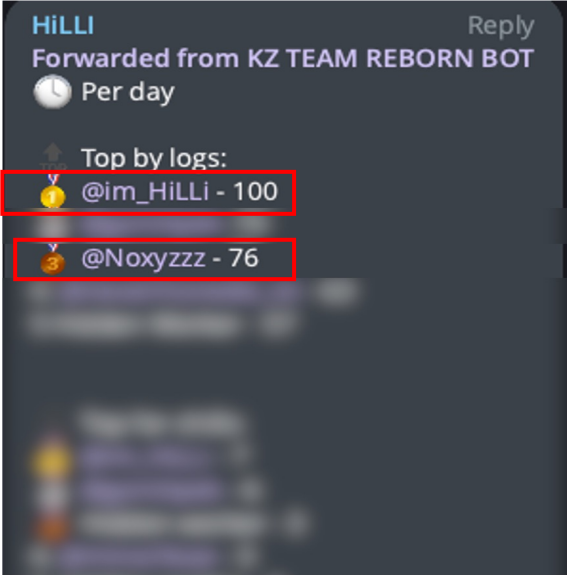
AURORA STEALER

Case related Stealer Ecosystem

The string "ALL" and the **same ICON hash** were found in a common set of samples identified them as the **KZ traffic team** by the Telegram ID used in the BuildID field.

BuildID	GroupID	Icon Hash
@punjet	ALL	 80c0dadadadac000
5713190558		
@Noxyzzz		
@relisek		
@im_HiLLi		

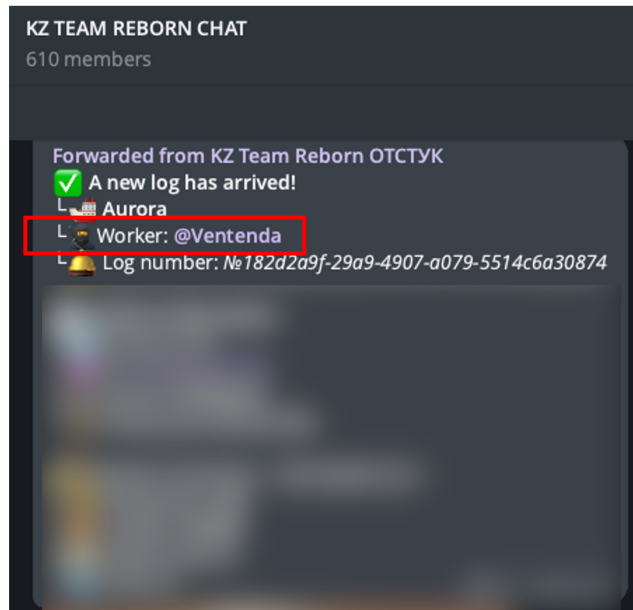
Identify value used in Aurora stealer



Best Traffer in KZ Team

Case related Stealer Ecosystem

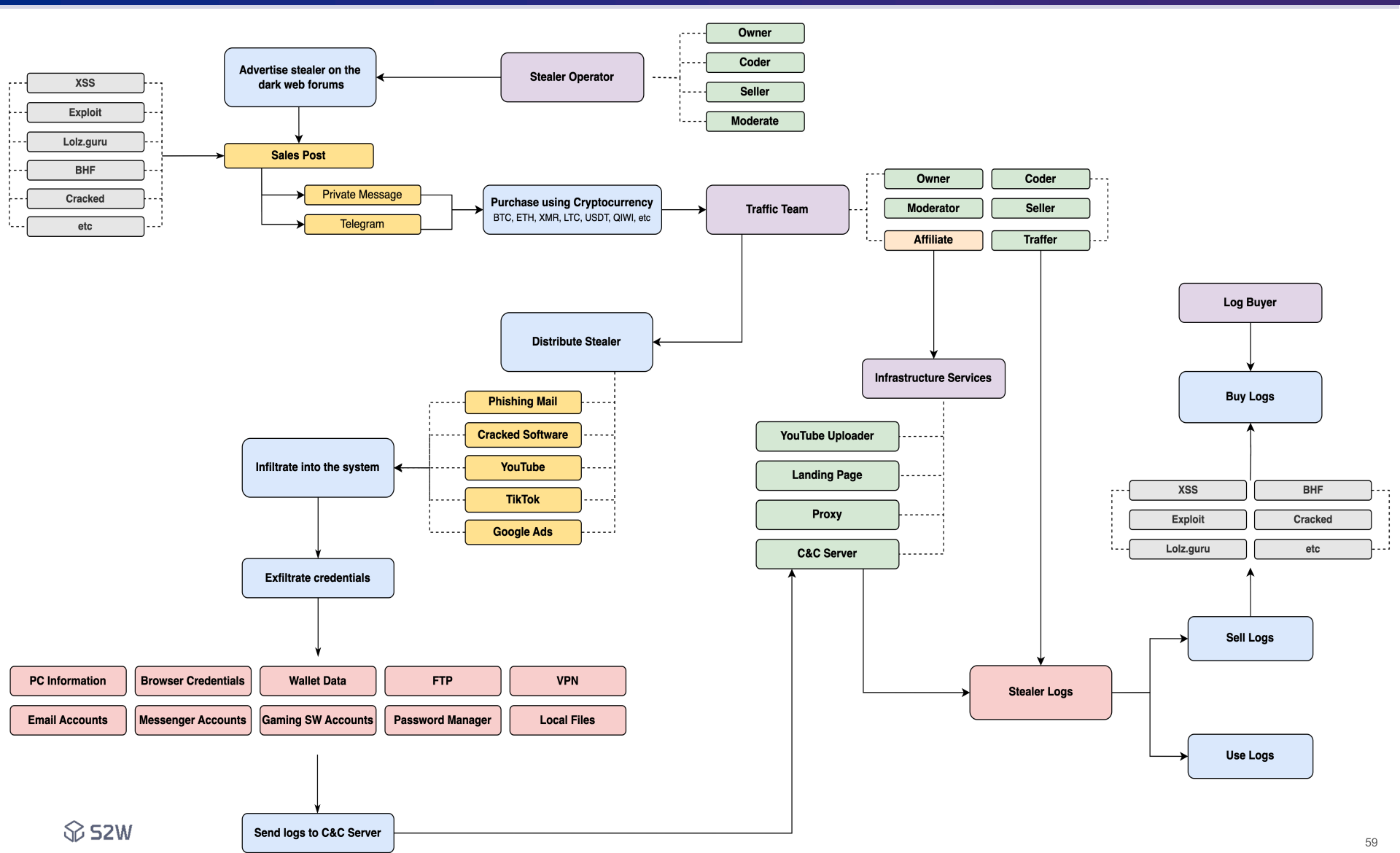
One of KZ Team's traffickers, user "Ventenda," uploaded log files to a Telegram channel that specializes in sharing only stealer logs.



KZ Team's Traaffer: @Ventenda

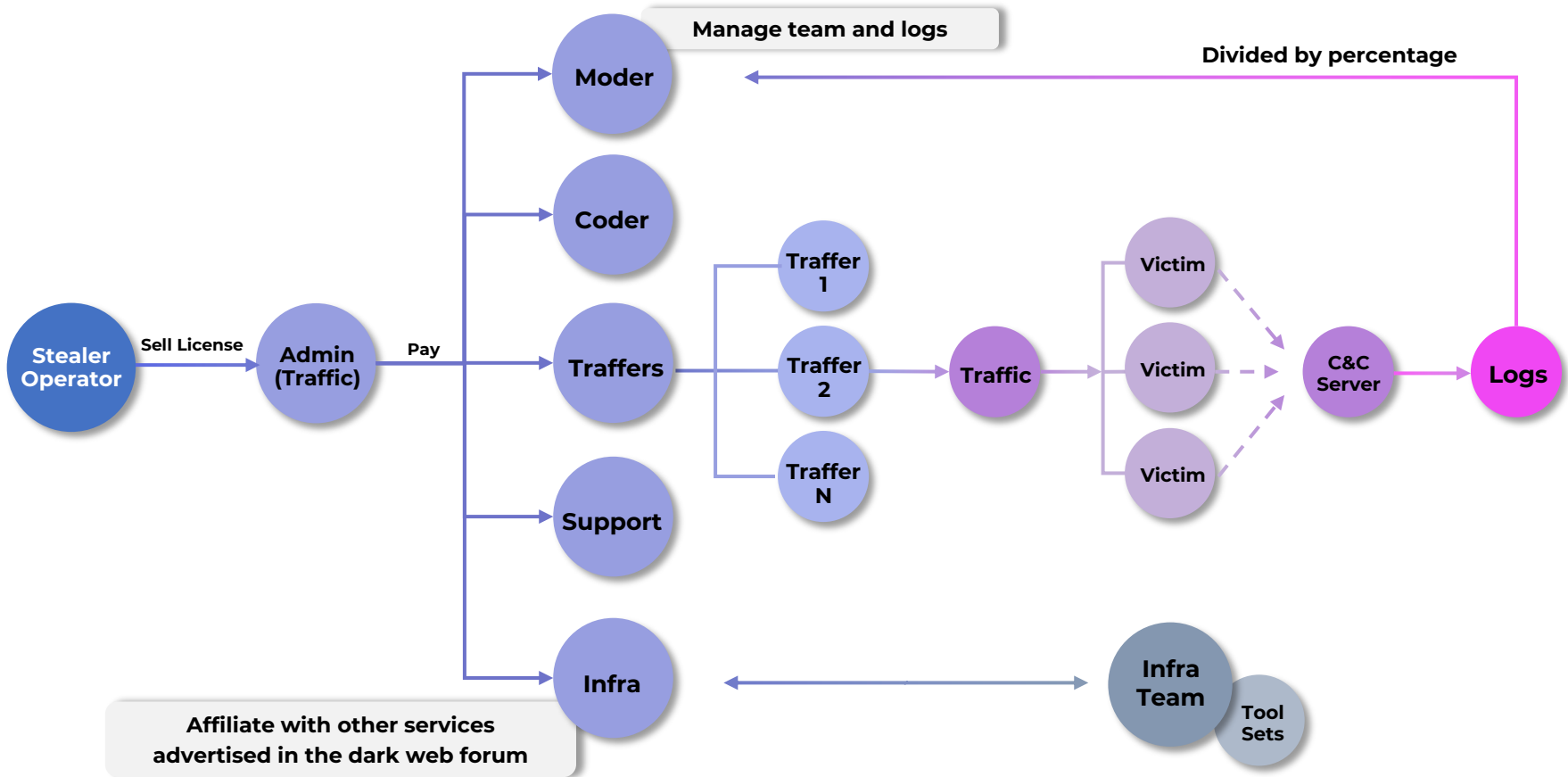


Some files in a shared stealer log

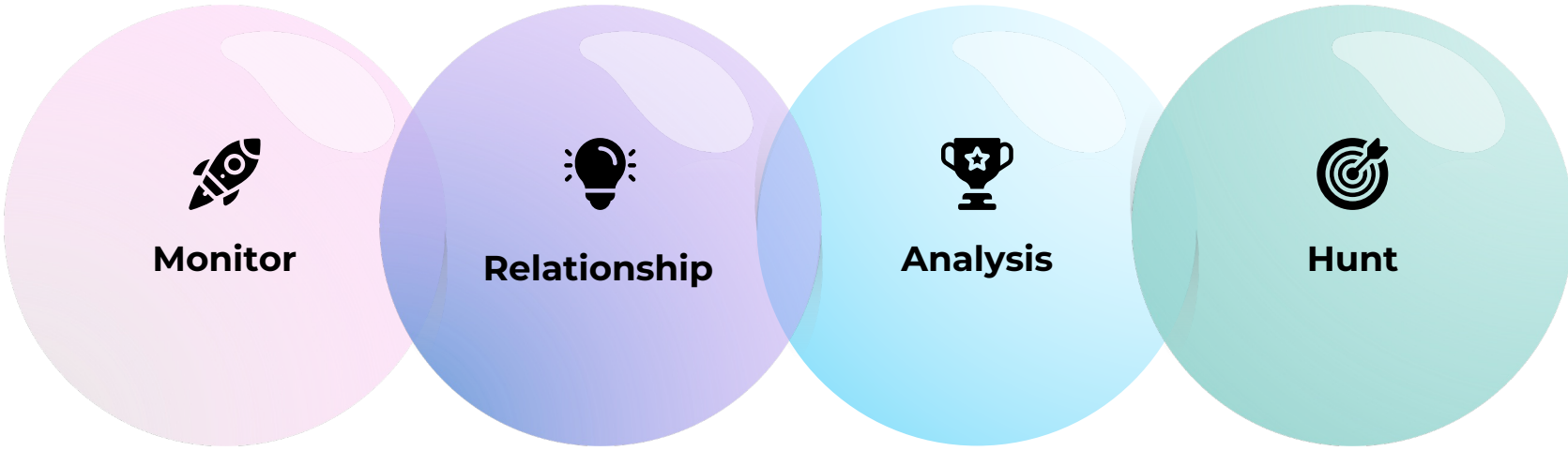


Takeaways

Lessons Learned: What to focus on to track down stealer groups



Lessons Learned: What to focus on to track down stealer groups



**Thanks,
Any Questions?**