C2 Active Monitoring

Collecting orders from Command and Control servers by impersonating an infected machine

@xanhacks

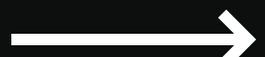
https://slides.com/xanhacks/c2-active-monitor/

whoami

@xanhacks

- Student at ENSIBS
- Malware Analyst at the French Post Office
- Play CTF in my free time (Web & Reverse)

How it works - Part 1



Downloader

Download samples

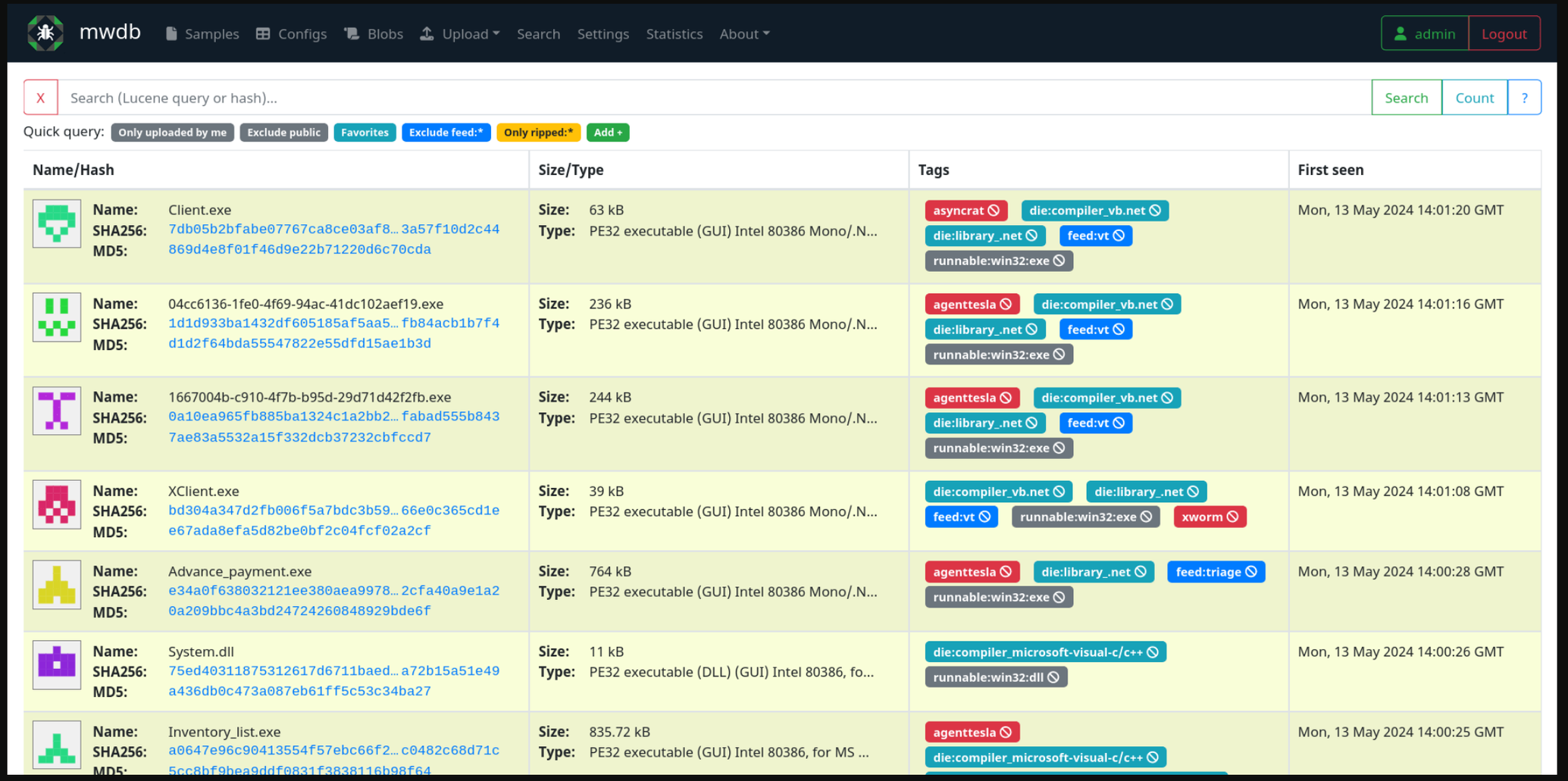
MWDB

Malware Database

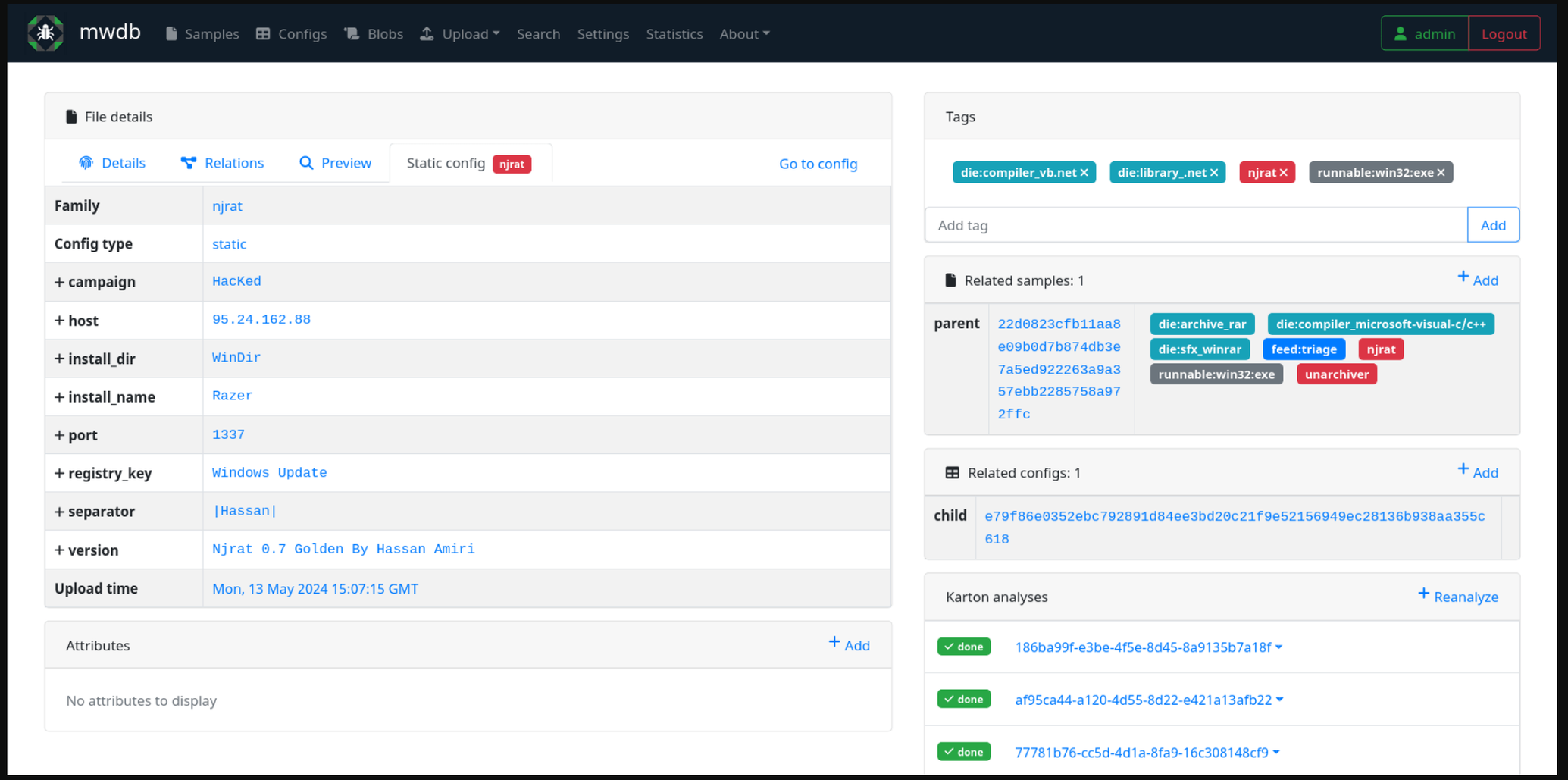
Karton

Configuration extraction

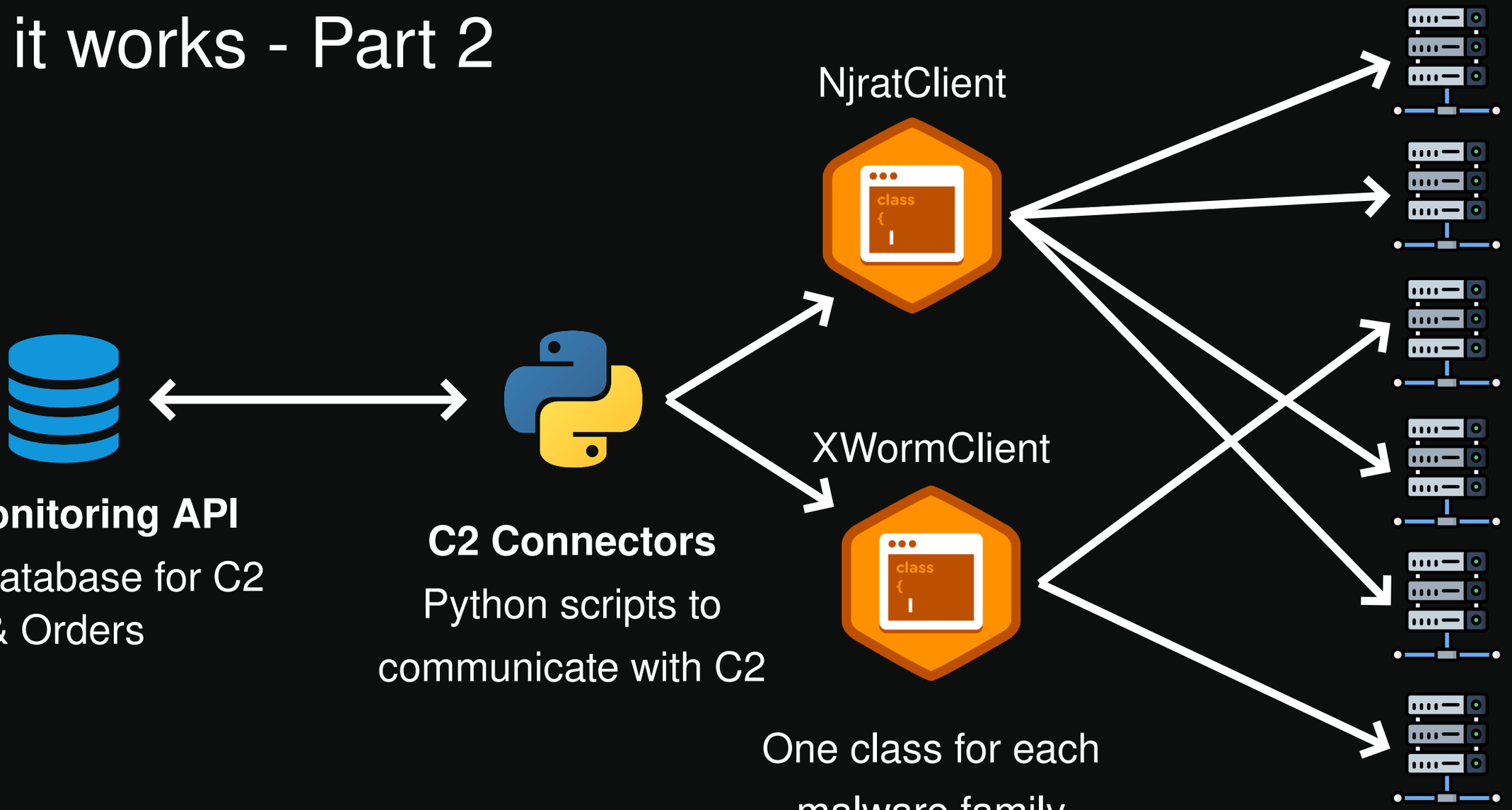
How it works - Part 1 - MWDB Sample List



How it works - Part 1 - MWDB Sample Overview



How it works - Part 2



C2 Monitoring API

API & database for C2 & Orders

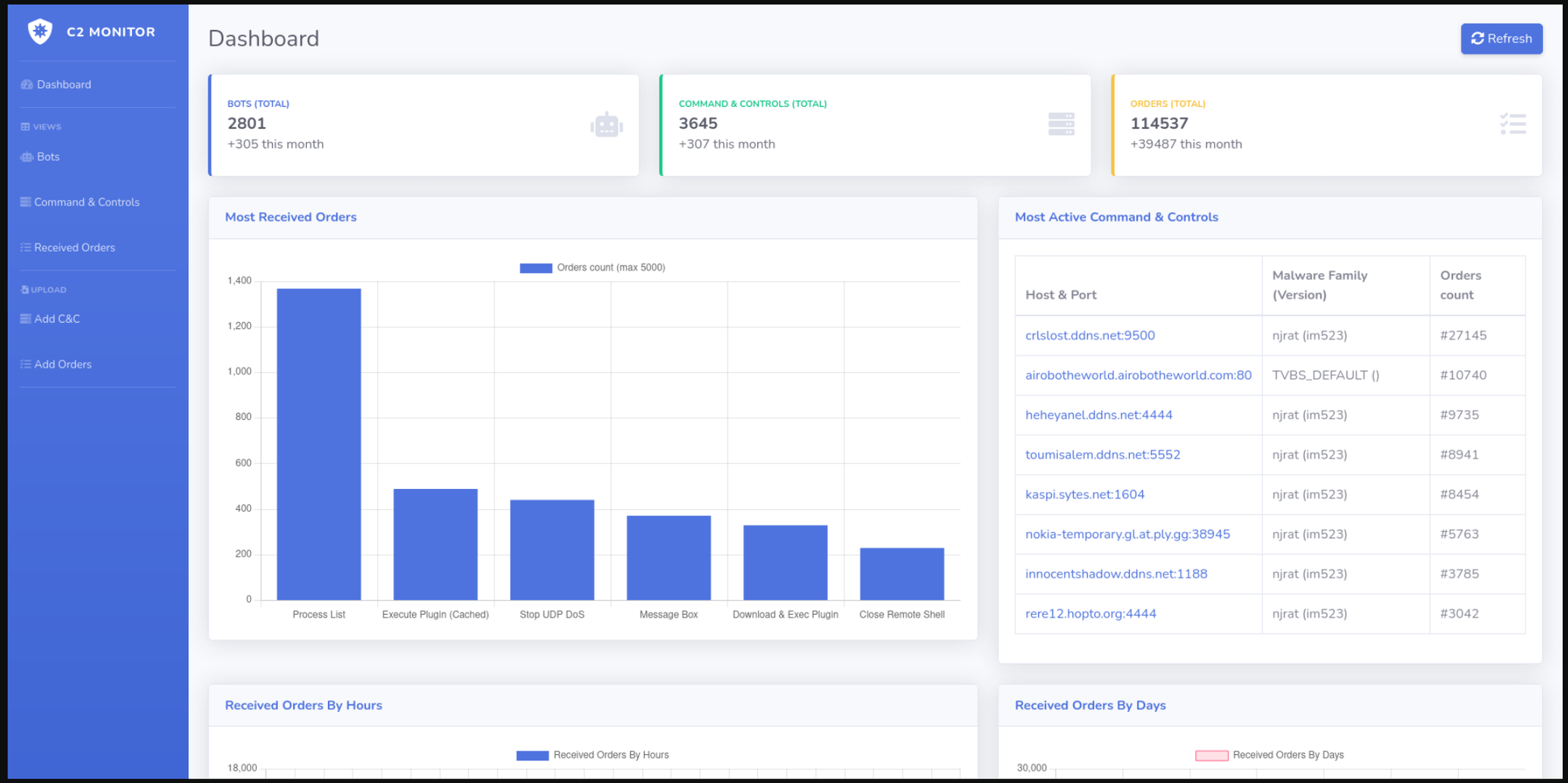
C2 Connectors

Python scripts to communicate with C2

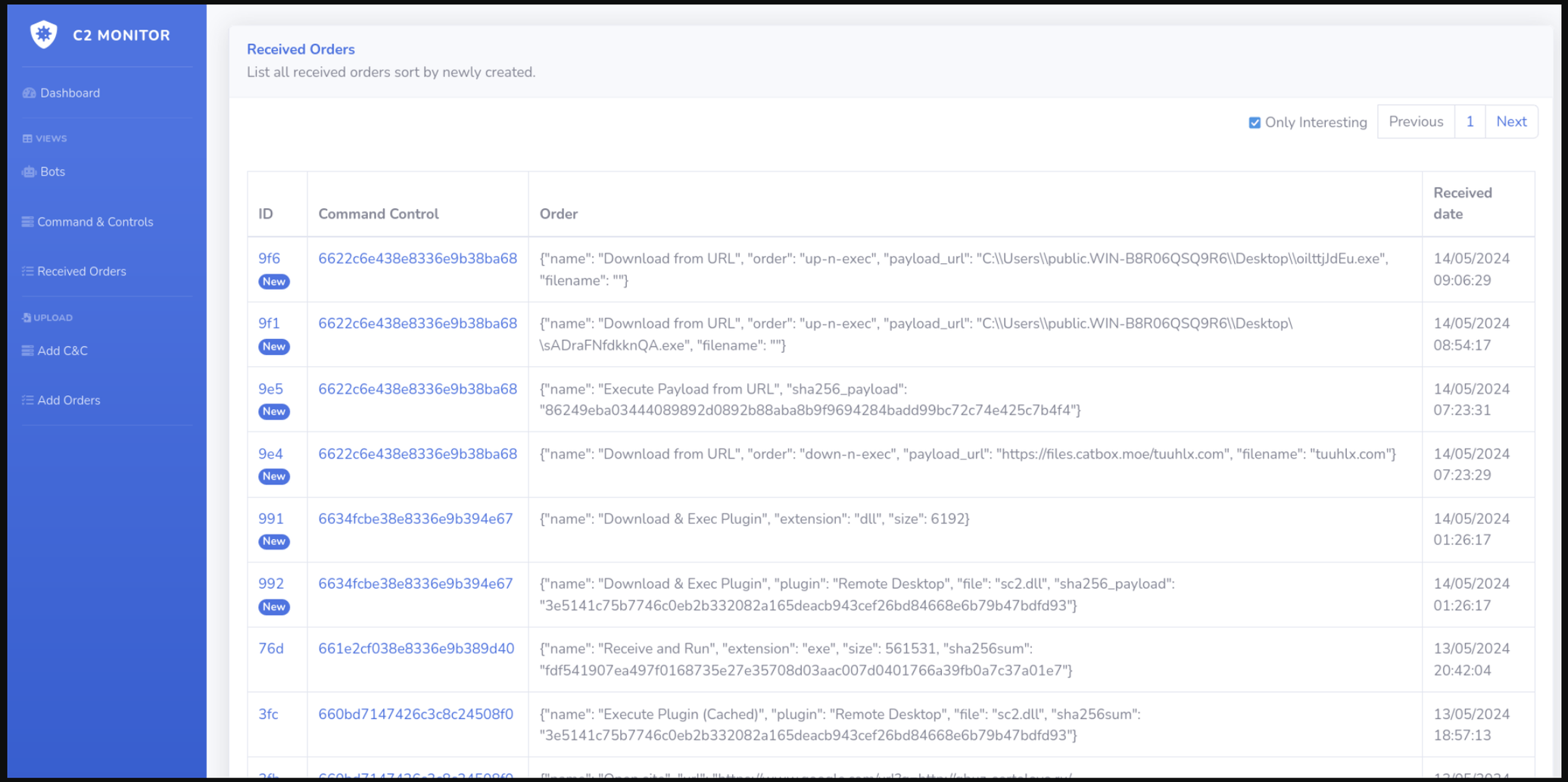
One class for each malware family

C2 Servers

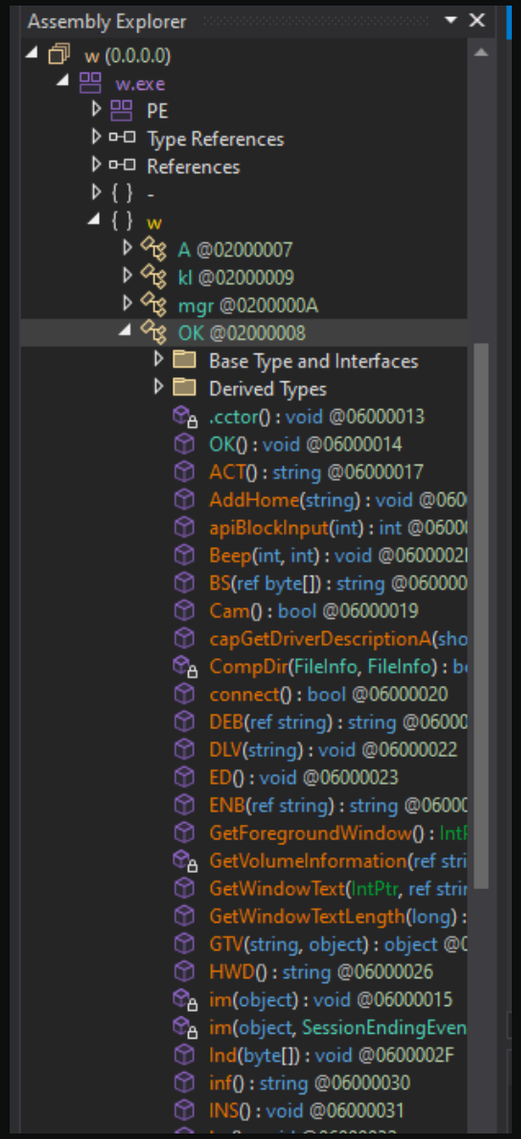
How it works - Part 2 - C2 Monitor Overview



How it works - Part 2 - C2 Monitor Orders

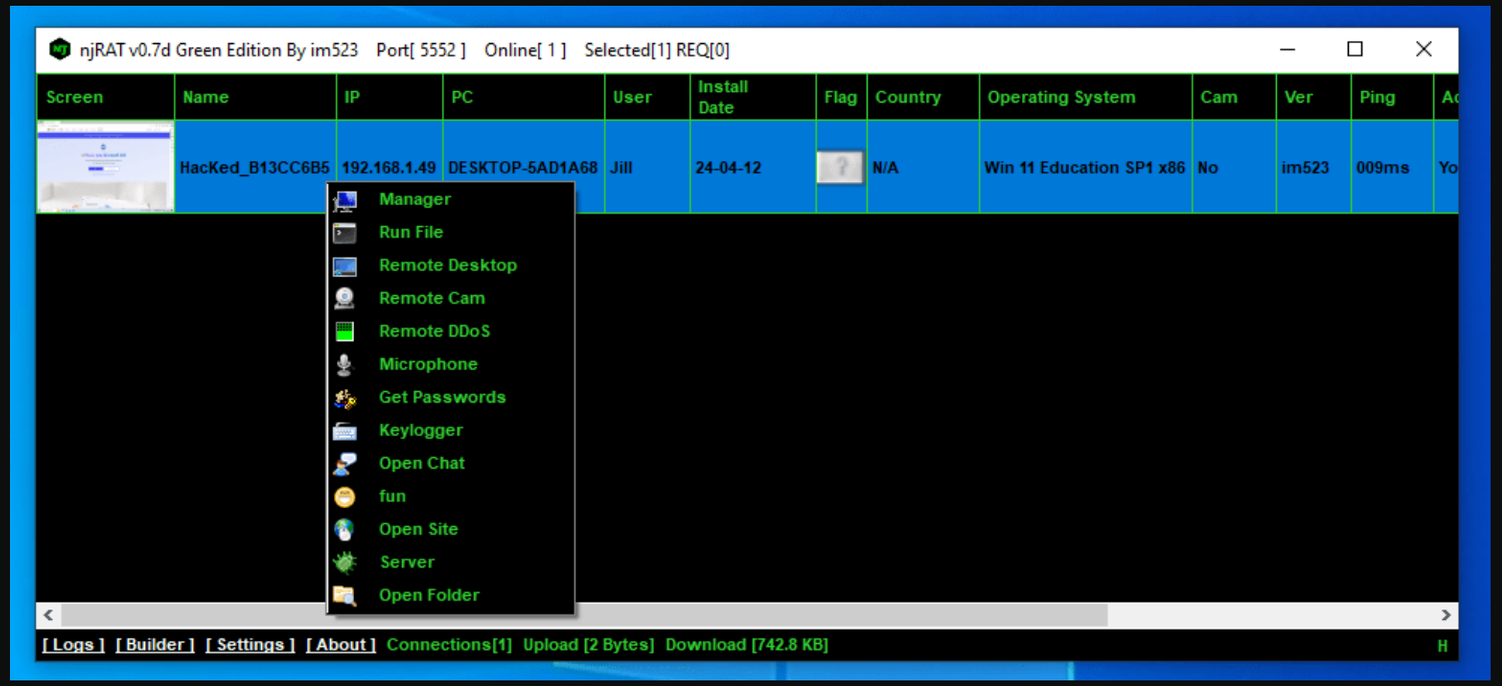


Case Study: NjRAT - Green Edition



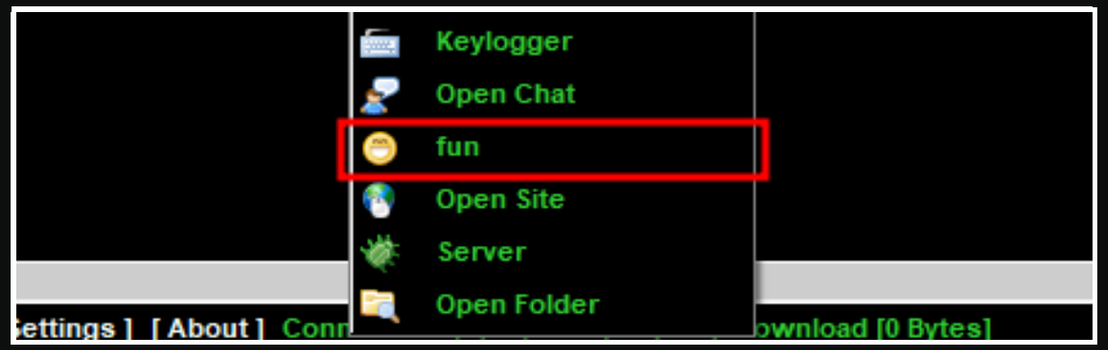
NjRAT is a Remote Access Trojan made in .NET that communicates through unencrypted TCP socket

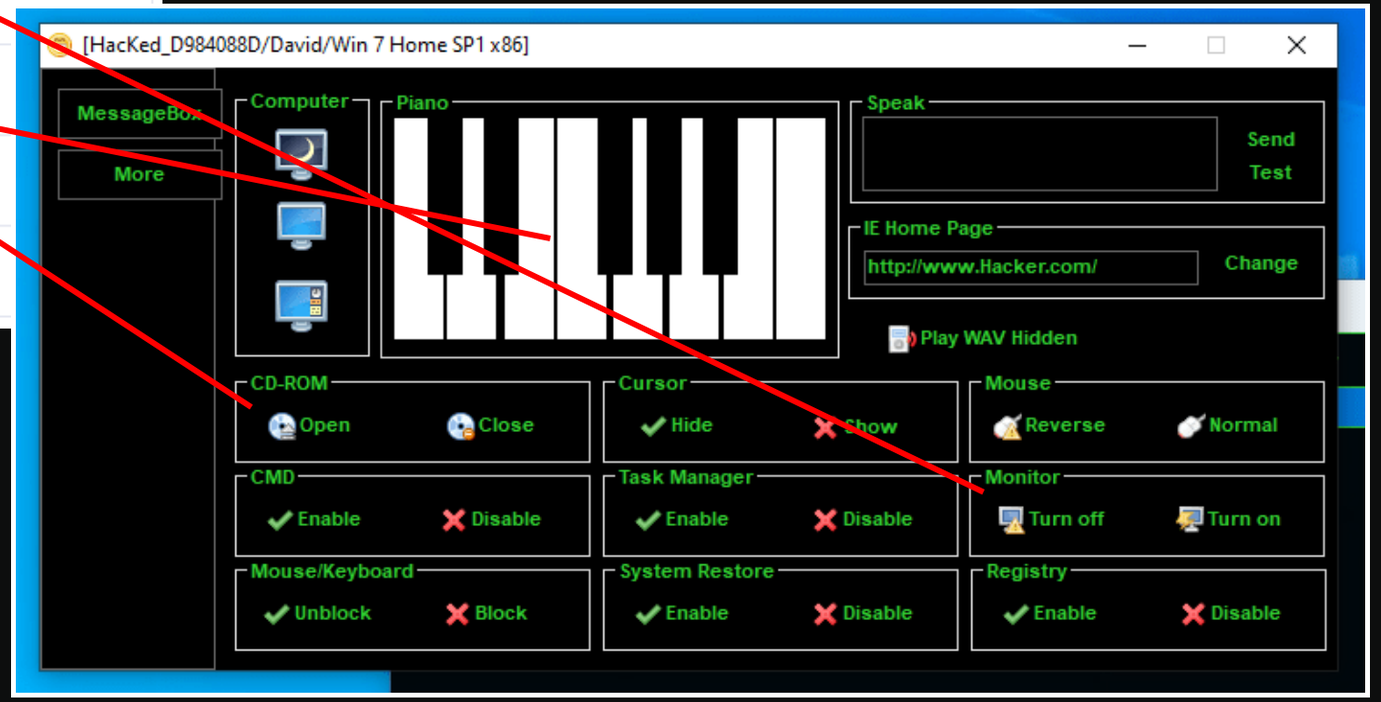
(default port: 5552)



Funny Orders - Fun Popup

{"name": "TurnOffMonitor"}	11/04/2024 23:56:21
{"name": "OpenCD"}	11/04/2024 23:55:33
{"name": "Piano", "key": "311"}	11/04/2024 23:55:28
{"name": "Piano", "key": "311"}	11/04/2024 23:55:28
{"name": "Piano", "key": "311"}	11/04/2024 23:55:28
{"name": "Piano", "key": "311"}	11/04/2024 23:55:27
{"name": "Fun popup"}	11/04/2024 23:55:26





Funny Orders - Chat Plugin

{"name": "Recv Chat Message", "message": "fuck you"}

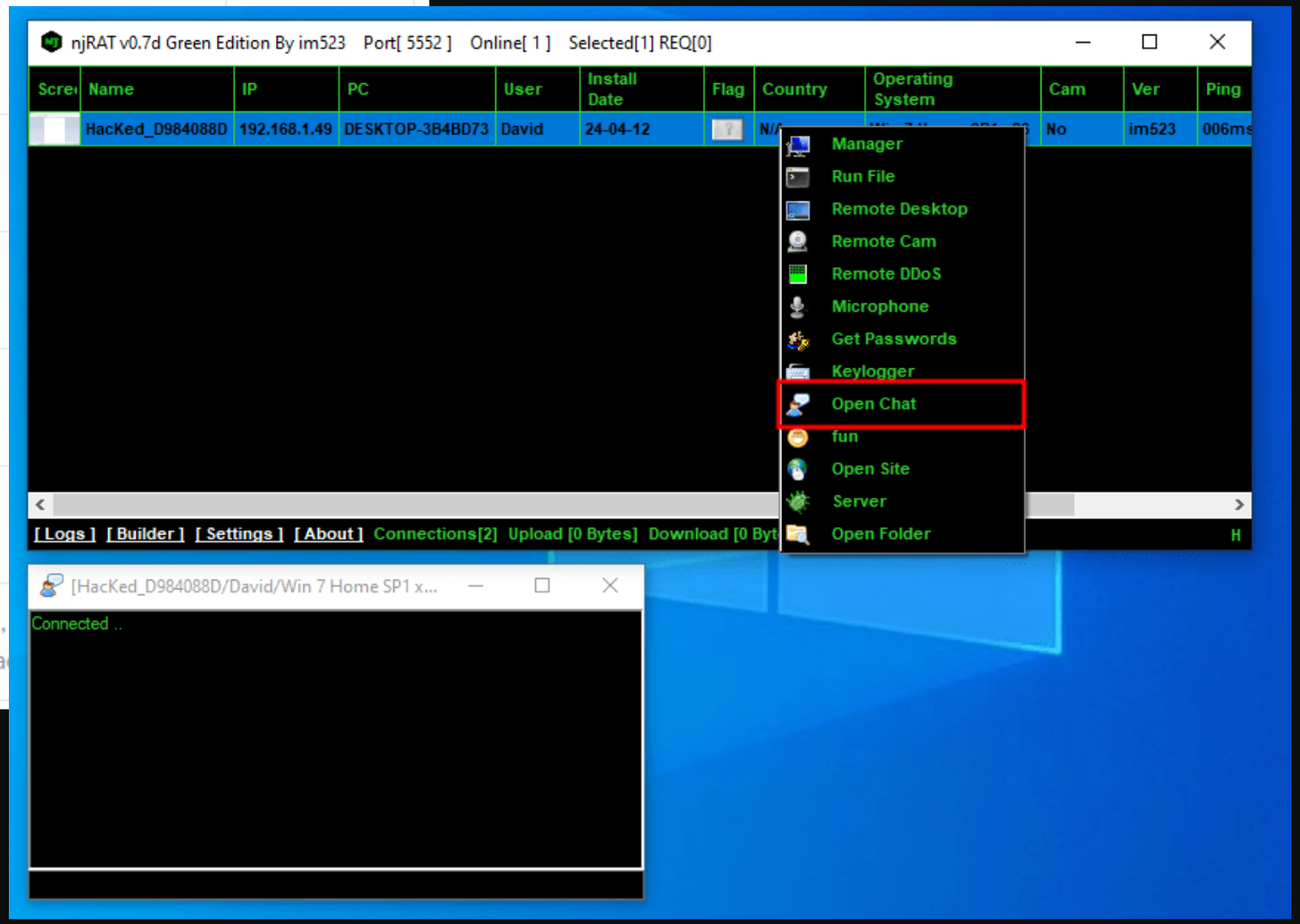
{"name": "Get Desktop Screenshot"}

{"name": "Get Desktop Screenshot"}

{"name": "Chat Hacker Username", "username": "!~Hacker~!"}

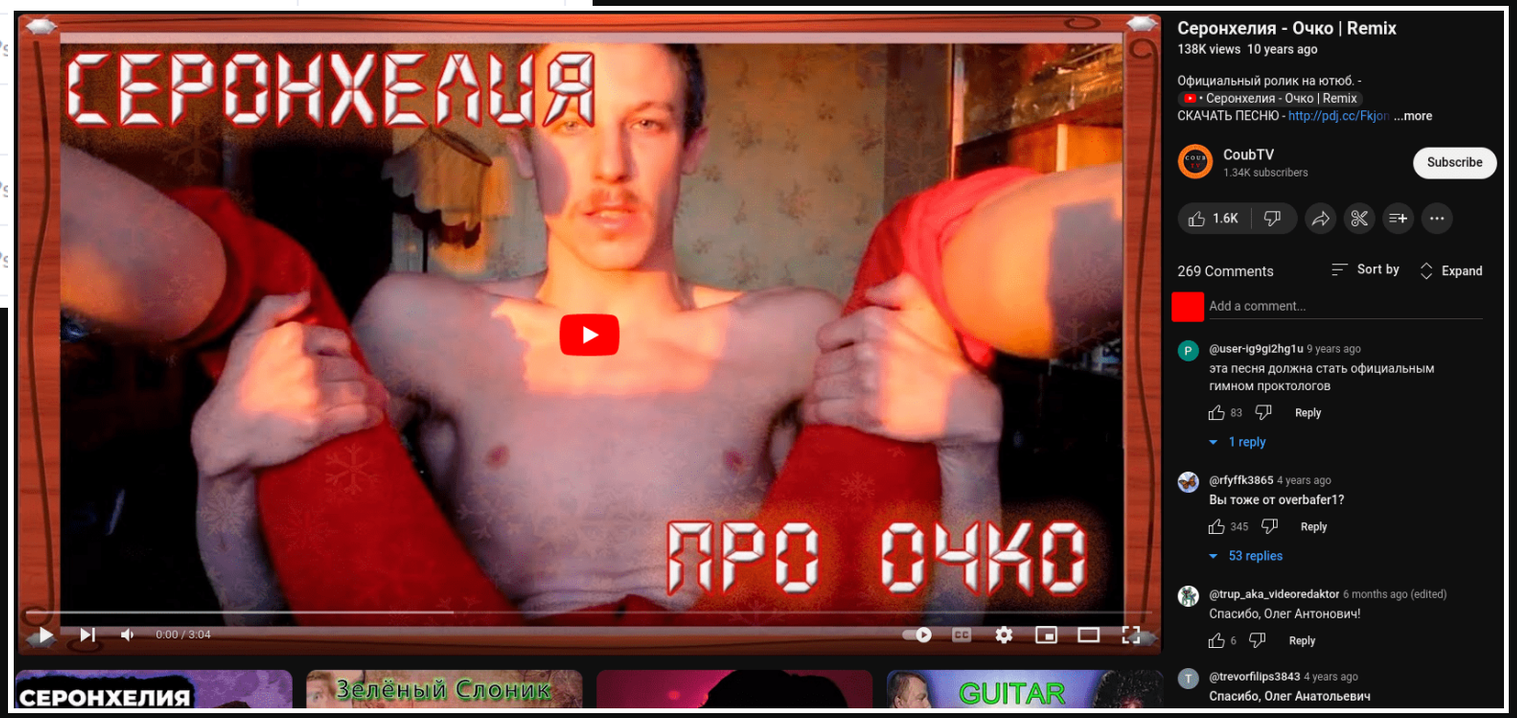
{"name": "Get Desktop Screenshot"}

{"name": "Download & Exec Plugin", "plugin": "Open Chat", "file": "ch.dll",
"7722206dba0cfb290f33093f9430cb770a160947001715ae11e6dbbfa

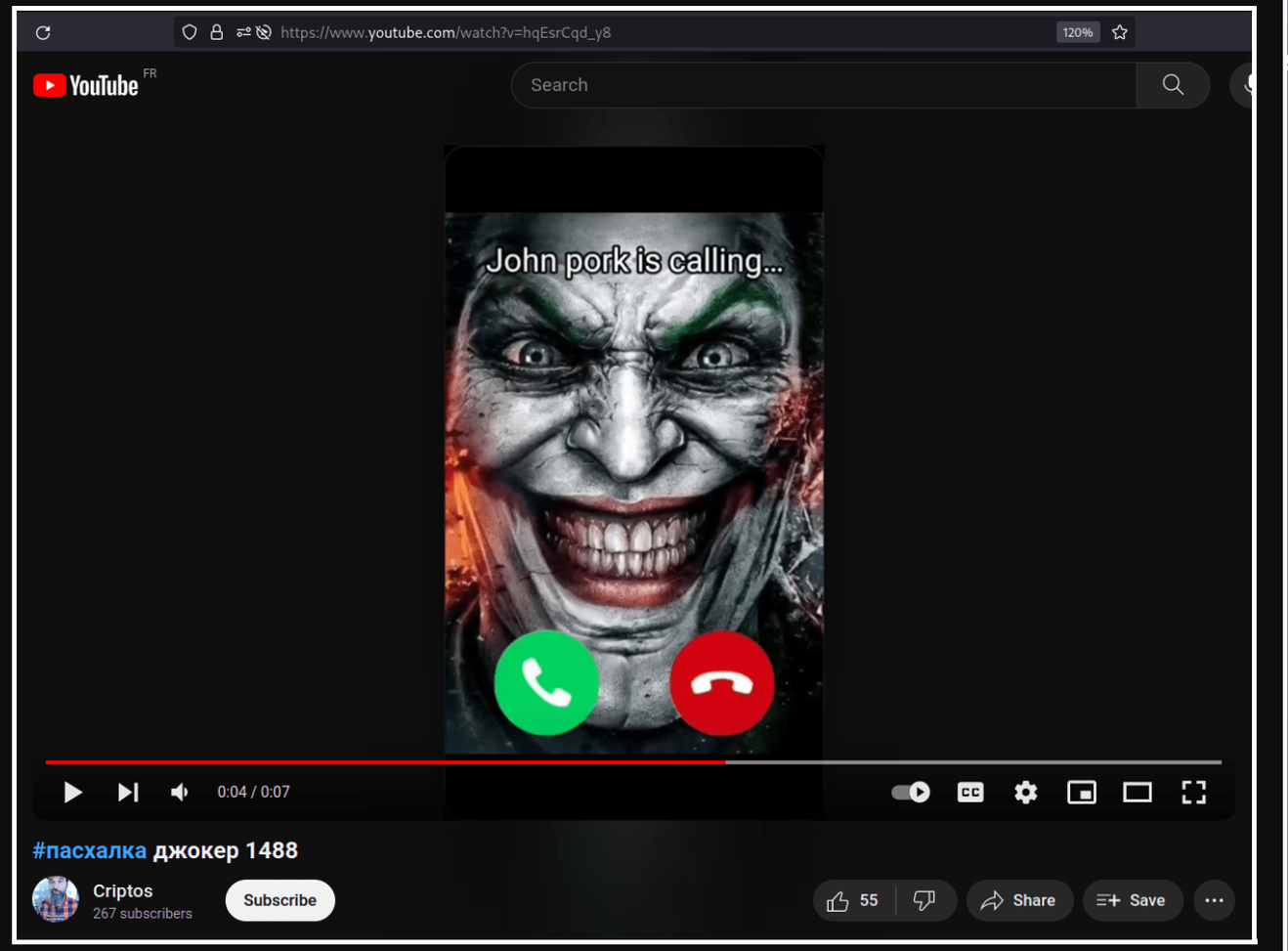


Funny Orders - Open Site - Russian Video

Order	Received date
{"name": "Get Desktop Screenshot"}	12/04/2024 02:54:34
{"name": "Open site", "url": ["OpenSite", "https://youtu.be/YSDCNV0RCG0?si=7vTppZ31jF3AviFl"]}	12/04/2024 02:54:29
{"name": "Open site", "url": ["OpenSite", "https://youtu.be/YSDCNV0RCG0?si=7vTppZ31jF3AviFl"]}	12/04/2024 02:54:29
{"name": "Open site", "url": ["OpenSite", "https://youtu.be/YSDCNV0RCG0?si=7vTppZ31jF3AviFl"]}	12/04/2024 02:54:29
{"name": "Open site", "url": ["OpenSite", "https://youtu.be/YSDCNV0RCG0?s	
{"name": "Get Desktop Screenshot"}	
{"name": "Open site", "url": ["OpenSite", "https://youtu.be/YSDCNV0RCG0?s	
{"name": "Open site", "url": ["OpenSite", "https://youtu.be/YSDCNV0RCG0?s	



Funny Orders - Open Site - Russian Video again...



Funny Orders - Open Site - P*rn website

ID	Command Control	Order	Received date
8b0	660bd7327426c3c8c2450b7f	{"name": "Open site", "url": "www.pornhub.com"}	11/05/2024 12:11:00
8b1	660bd7327426c3c8c2450b7f	{"name": "Open site", "url": "www.pornhub.com"}	11/05/2024 12:11:00
8b3	660bd7327426c3c8c2450b7f	{"name": "Open site", "url": "www.pornhub.com"}	11/05/2024 12:11:00
8b2	660bd7327426c3c8c2450b7f	{"name": "Open site", "url": "www.pornhub.com"}	11/05/2024 12:11:00
8b4	660bd7327426c3c8c2450b7f	{"name": "Open site", "url": "www.pornhub.com"}	11/05/2024 12:11:00
8aa	660bd7327426c3c8c2450b7f	{"name": "Open site", "url": "www.pornhub.com"}	11/05/2024 12:10:59
8af	660bd7327426c3c8c2450b7f	{"name": "Open site", "url": "www.pornhub.com"}	11/05/2024 12:10:59
8ab	660bd7327426c3c8c2450b7f	{"name": "Open site", "url": "www.pornhub.com"}	11/05/2024 12:10:59
8ad	660bd7327426c3c8c2450b7f	{"name": "Open site", "url": "www.pornhub.com"}	11/05/2024 12:10:59
8ae	660bd7327426c3c8c2450b7f	{"name": "Open site", "url": "www.pornhub.com"}	11/05/2024 12:10:59
8ac	660bd7327426c3c8c2450b7f	{"name": "Open site", "url": "www.pornhub.com"}	11/05/2024 12:10:59
8a8	660bd7327426c3c8c2450b7f	{"name": "Open site", "url": "www.pornhub.com"}	11/05/2024 12:10:58

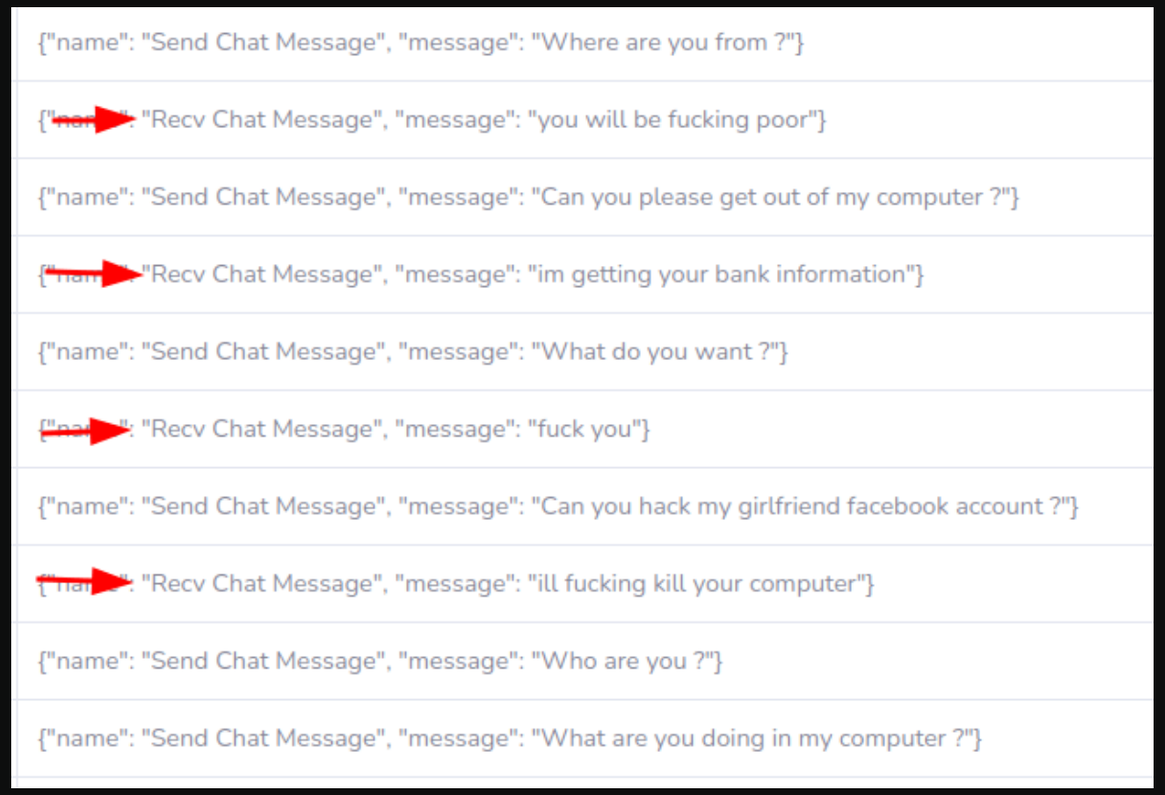
Campaign - "I am Furry"

Command & Control

Delete | Edit | Back

ID	661a87f5434a57a747dac86a
Host & Port	green-morrison.gl.at.ply.gg:17455
Malware Family	njrat
Version	im523
Enabled	True
Last Poll	15/04/2024 13:14:56
First Success Response	14/04/2024 18:46:27
Last Success Response	14/04/2024 22:24:03
MWDB Config ID	c6c38fa56c7b7ac9d357879b061ad8036f317f6d16b547a81af6e9be33cd96bb
Creation Date	13/04/2024 13:26:13
Metadata	{"host": "green-morrison.gl.at.ply.gg", "port": "17455", "version": "im523", "campaign": "I am Furry", "separator": "|'|'|", "install_dir": "AllUsersProfile", "install_name": "COM Surrogate.exe", "registry_key": "e14109296e01cf24bb9b7f72f64c4cb3"}

Campaign - "I am Furry"



"ill fucking kill your computer"
"im getting your bank information"
"you will be fucking poor"

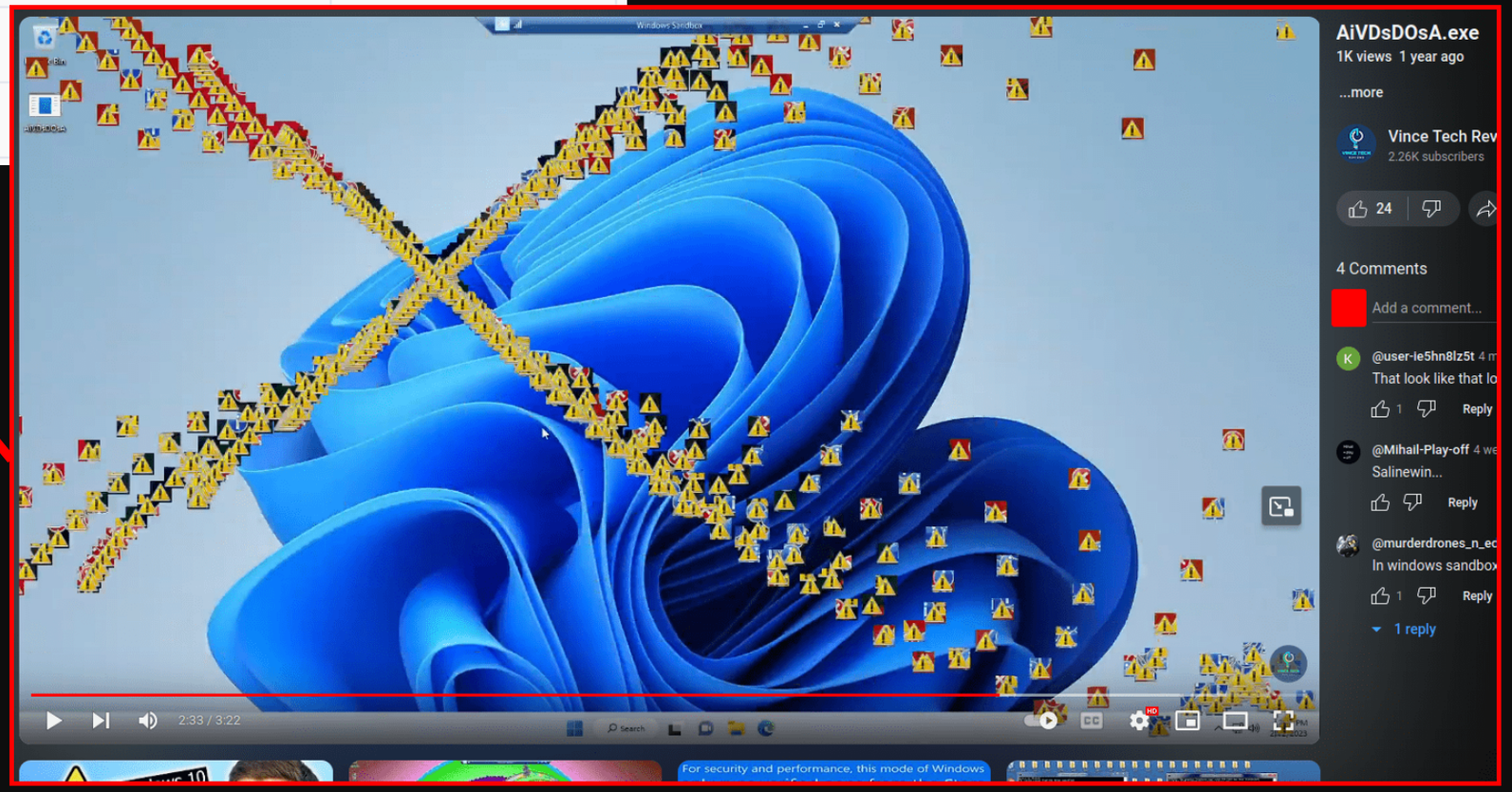
Timeline

Campaign - "I am Furry"

Order	Received date
{"name": "Recv Chat Message", "message": "im leaving ur pc ok"}	14/04/2024 22:32:09
{"name": "Receive and Run", "extension": "webp", "size": 43096}	14/04/2024 22:30:39
{"name": "Receive and Run", "extension": "exe", "size": 1176035}	
{"name": "Receive and Run", "extension": "exe", "size": 14750}	

Wiper #1:
AiVDsDOsA

https://www.youtube.com/watch?v=Xs3ukQql0H0



Campaign - "I am Furry"

Order	Received date
{"name": "Recv Chat Message", "message": "im leaving ur pc ok"}	14/04/2024 22:32:09
{"name": "Receive and Run", "extension": "webp", "size": 43096}	14/04/2024 22:30:39
{"name": "Receive and Run", "extension": "exe", "size": 1176035}	
{"name": "Receive and Run", "extension": "exe", "size": 14750}	

https://www.youtube.com/watch?v=jK1nRADpVnw

Wiper #2: Neptunium

Campaign - "I am Furry"

Order	Received date
{"name": "Recv Chat Message", "message": "im leaving ur pc ok"}	14/04/2024 22:32:09
{"name": "Receive and Run", "extension": "webp", "size": 43096}	
{"name": "Receive and Run", "extension": "exe", "size": 1176035}	
{"name": "Receive and Run", "extension": "exe", "size": 14750}	

Furry lover <3

Campaign - @gribojuy / ГРИБОЖУЙ / Champignon

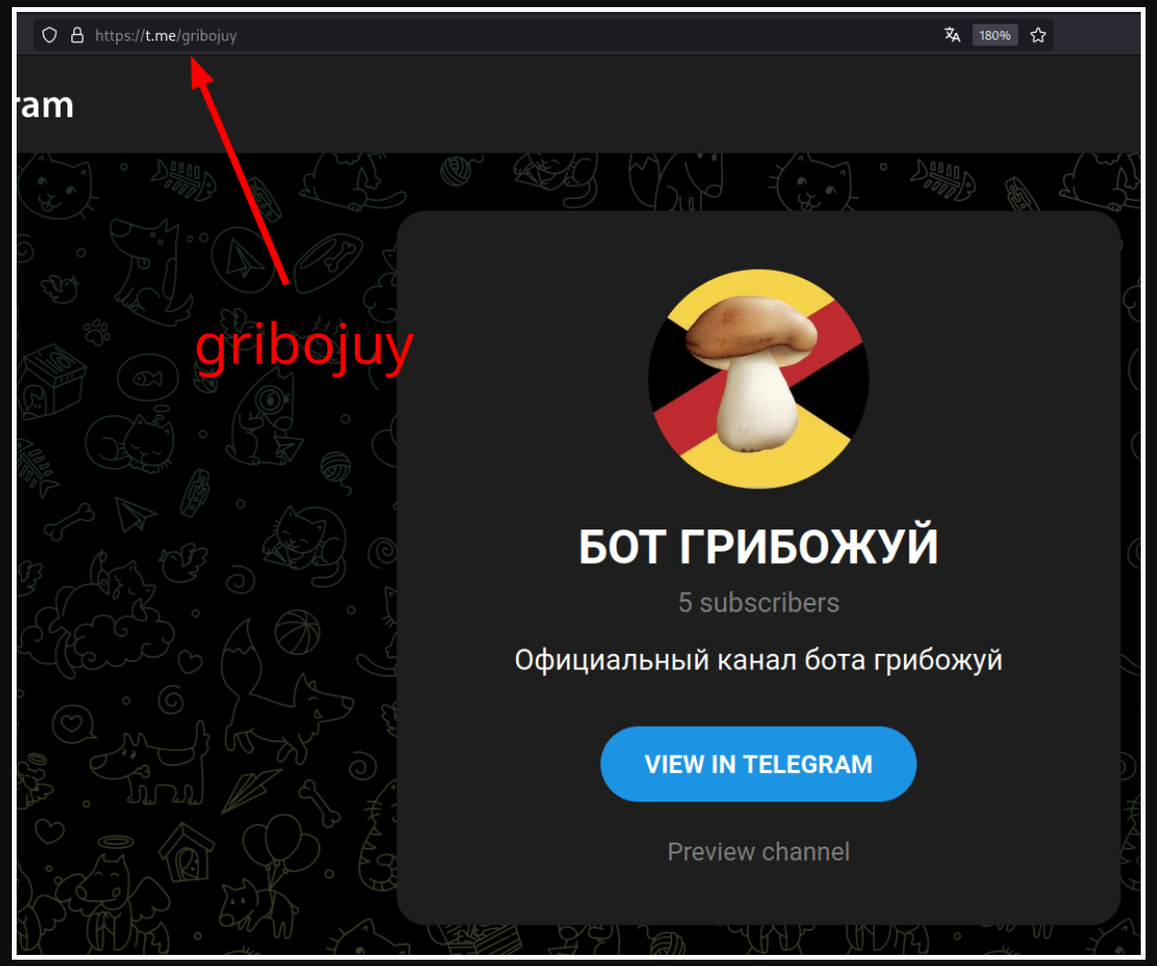
> "gribojuyy" enter the chat
gribojuyy: Bro, hello, do you have paypal?
me: What are you doing in my computer ?
gribojuyy: do you have a discord?
me: Where are you from ?
gribojuyy: America
gribojuyy: bro do you have telegram
gribojuyy: bro do you have telegram
gribojuyy: bro do you have telegram
gribojuyy: ...
gribojuyy: message me in telegram @gribojuy

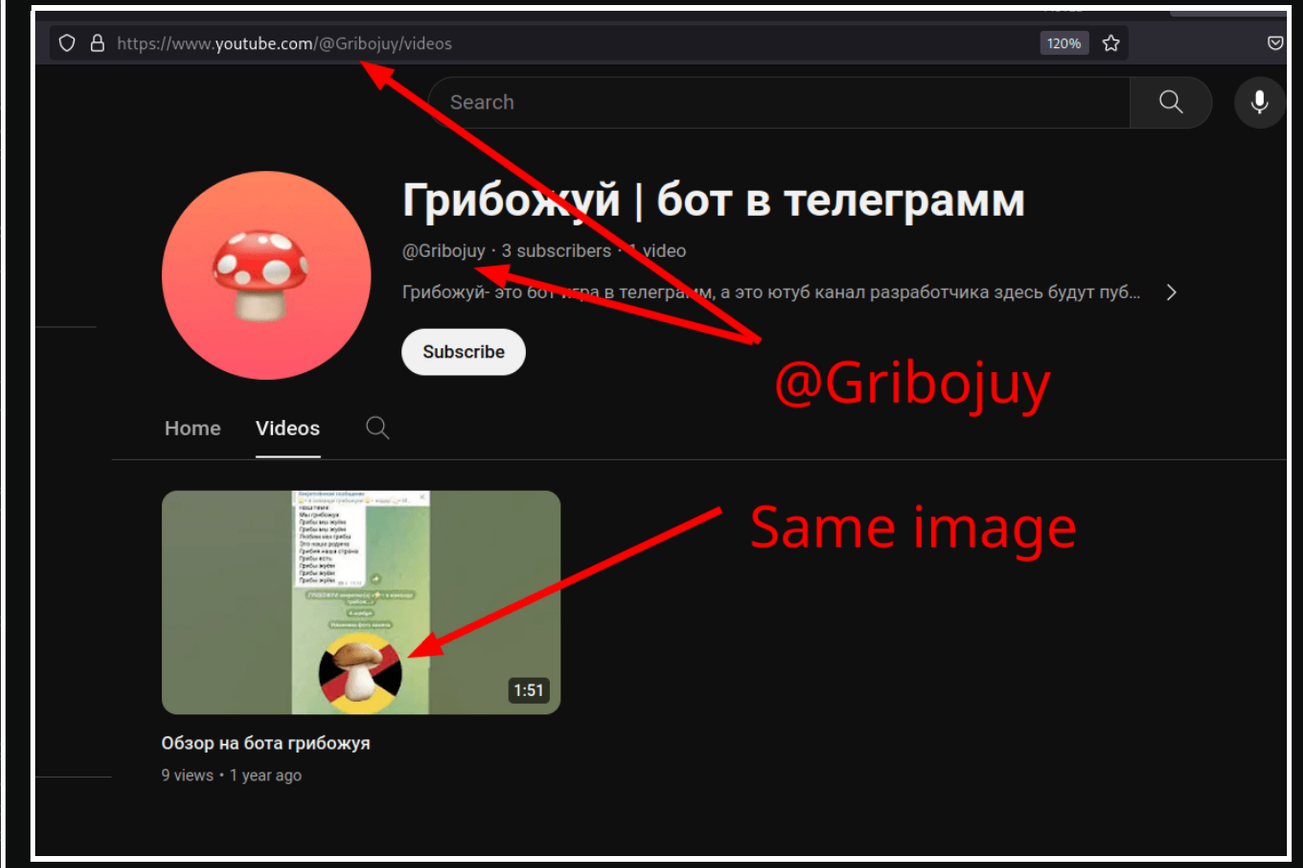
At the same time:

- Record Micro/Cam
- Open PH (also send index.html)
- Play piano
- Process List
- Text to Speech (if i do not answer to chat)

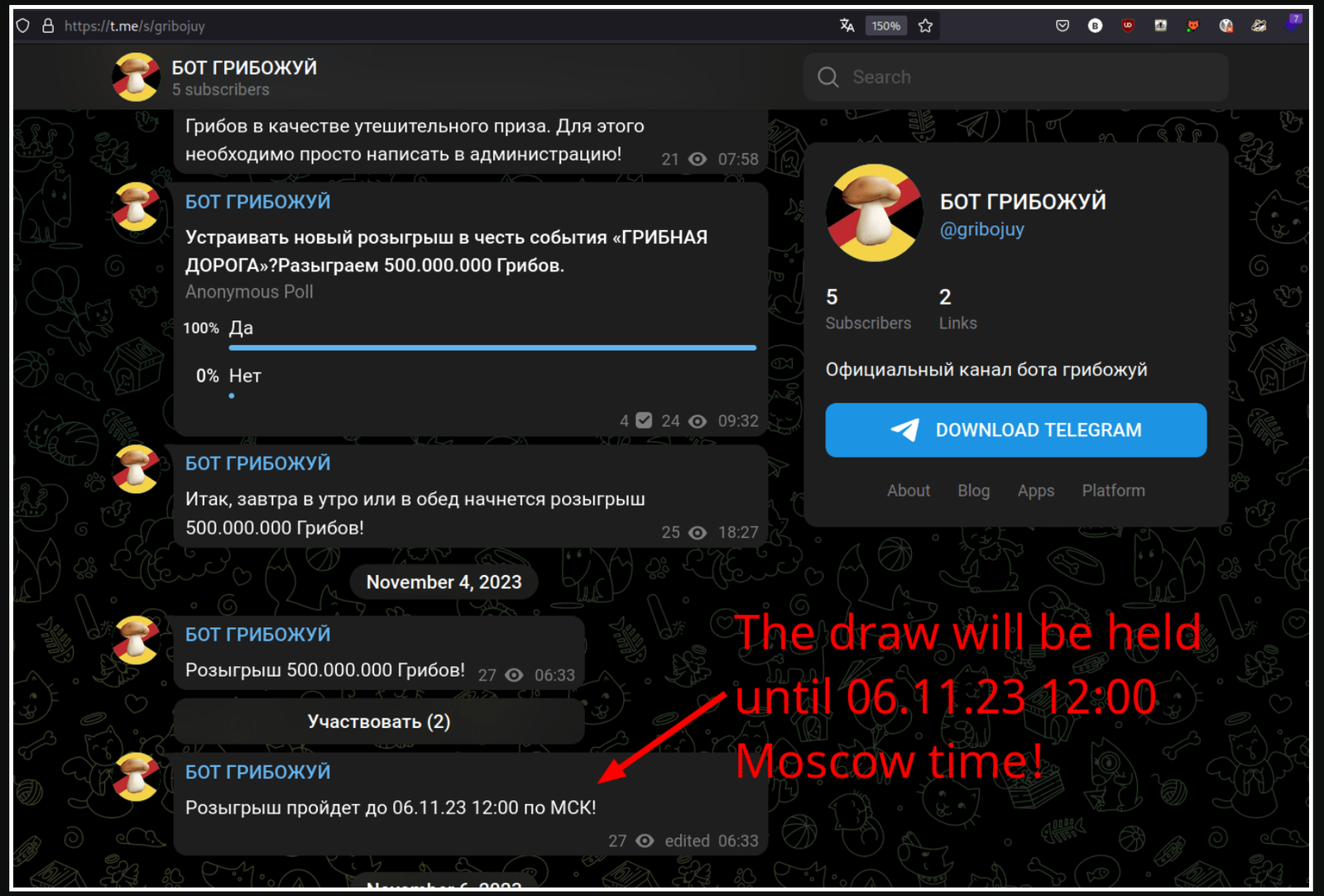
Chat exchange on 10/05/2024

Campaign - @gribojuy - Telegram & YouTube

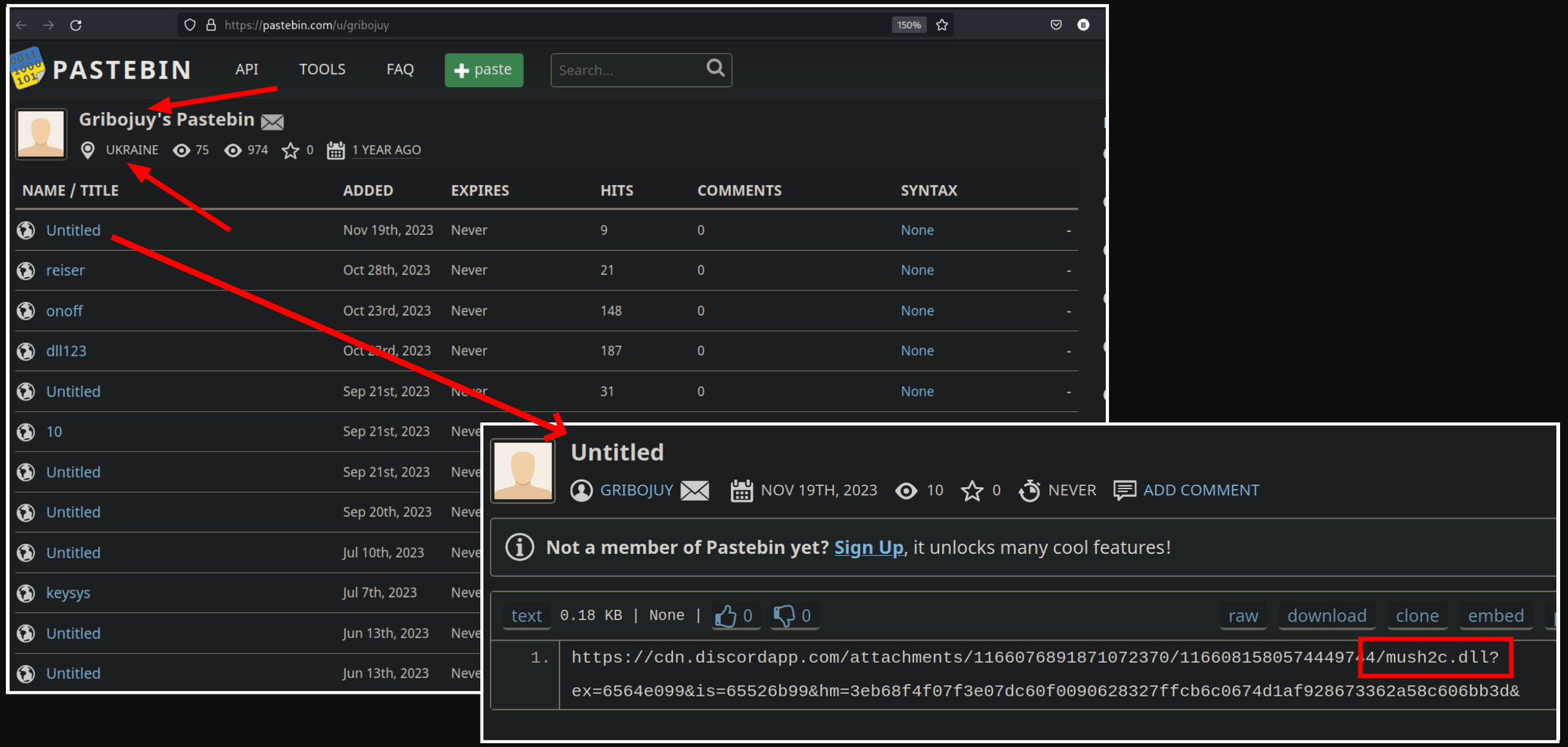




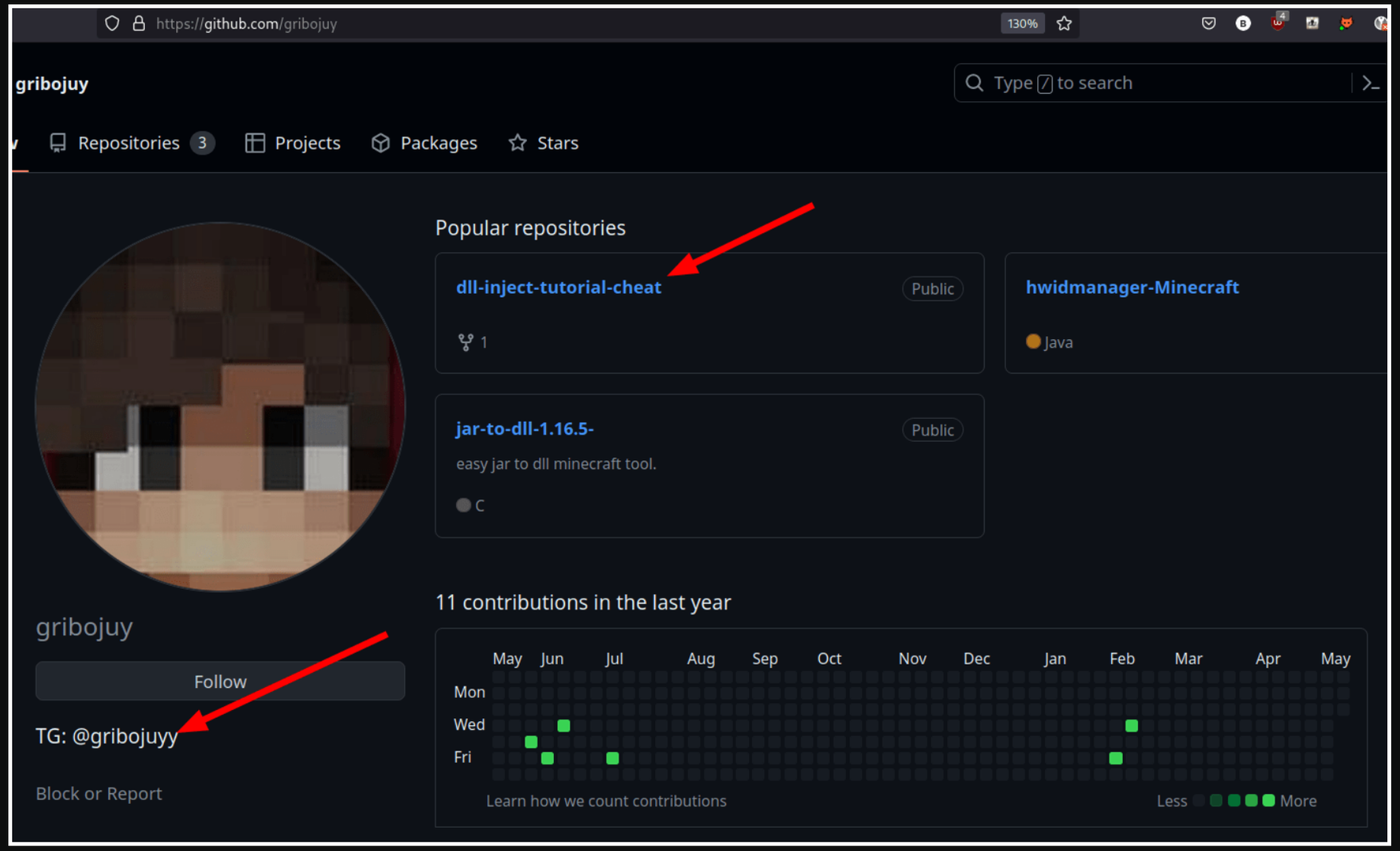
Campaign - @gribojuy - Telegram Preview



Campaign - @gribojuy - Pastebin Account



Campaign - @gribojuy - Github Account



The nice guy

"You installed a virus that I did not distribute"

"Please install antivirus"

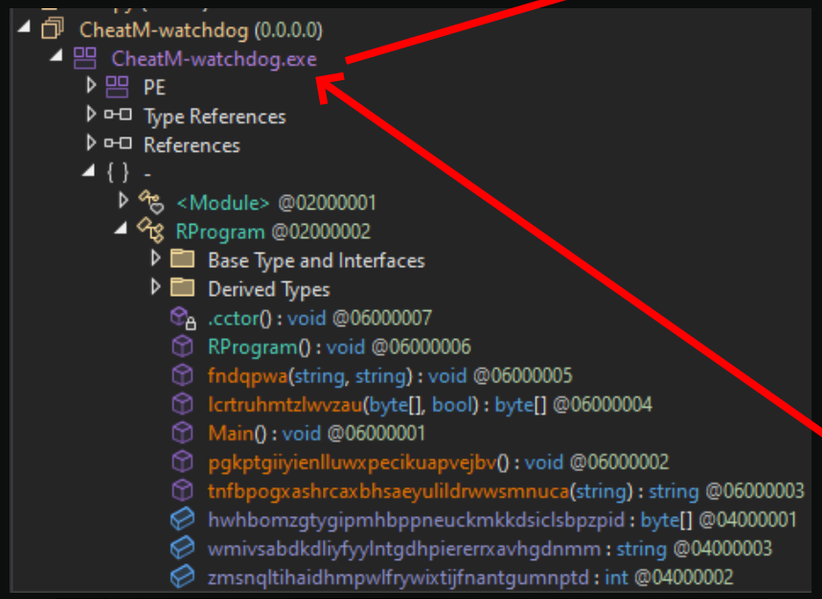
{"name": "Recv Chat Message", "message": "NO"}	17/04/2024 13:39:42
{"name": "Send Chat Message", "message": "I would like to talk to a real hacker. Are you a real hacker ?"}	17/04/2024 13:39:33
{"name": "Recv Chat Message", "message": "nothing"}	17/04/2024 13:39:24
{"name": "Send Chat Message", "message": "What do you want ?"}	17/04/2024 13:38:53
{"name": "Recv Chat Message", "message": "Please install antivirus or remove virus in startup"}	17/04/2024 13:38:47
{"name": "Send Chat Message", "message": "How much money do you make in a month ?"}	17/04/2024 13:34:31
{"name": "Recv Chat Message", "message": "you are from fance?"}	17/04/2024 13:34:24
{"name": "Send Chat Message", "message": "Can you please get out of my computer ?"}	17/04/2024 13:33:43
{"name": "Recv Chat Message", "message": "You yourself installed a virus that I did not distribute"}	17/04/2024 13:33:38
{"name": "Send Chat Message", "message": "Who are you ?"}	17/04/2024 13:31:29
{"name": "Recv Chat Message", "message": "I don`t know"}	17/04/2024 13:31:20

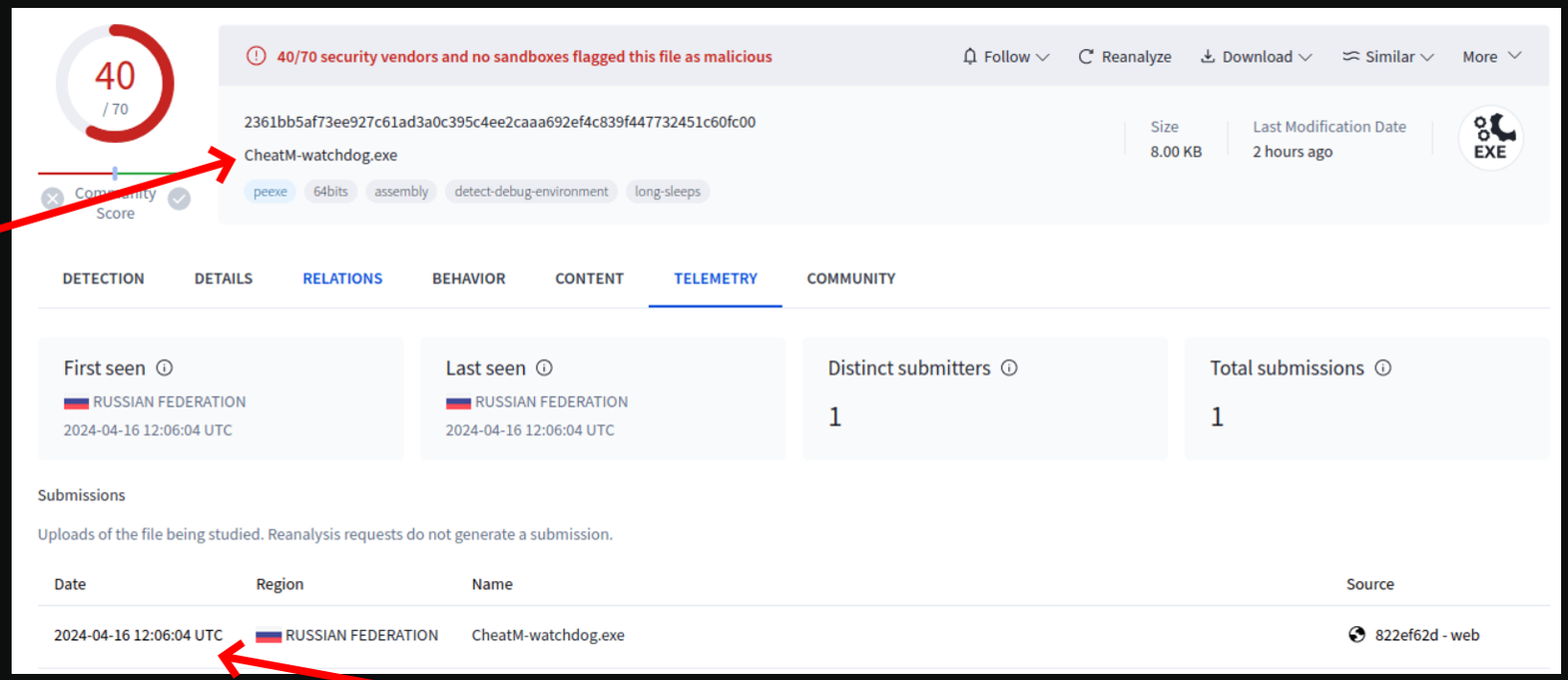
Timeline

{"name": "Message Box", "icon": "3", "button": "1", "title": "install antivirus", "content": "install antivirus or https://www.pcrisk.com/removal-guides/14768-njrat-malware"}	17/04/2024 13:45:02

MessageBox: Documentation to remove NjRAT

Coincidence??





14min interval

{"name": "Receive and Run", "extension": "exe", "size": 4929}	16/04/2024 11:52:56
{"name": "Get Desktop Screenshot"}	16/04/2024 11:52:52
{"name": "Get Desktop Screenshot"}	16/04/2024 11:52:35

Anydesk IT Support from Russia

SEND: Who are you ?

RECV: i m russian student

SEND: Can you hack my girlfriend facebook account ?

RECV: no i cant

SEND: How much money do you make in a month ?

RECV: 5000$

SEND: What do you want ?

RECV: bro i can delete this virus but you must download anydesk program and give me anydesk code

14/04/2024

End !

Any questions ?

@xanhacks

https://slides.com/xanhacks/c2-active-monitor/