SynapseX cracked virus UniqueGeese

Found on hacked youtube channel UniqueGeese in this download link. The video description was the following: Hi! There is SYNAPSE X CRACK!

HOW TO INSTALL IT:

1) Download the archive.
2) Unzip in new folder.
3) Open Executer.
4) Follow the instructions in the video.

⚠ LAUNCHER WILL NOT WORK IF YOUR WINDOWS DEFENDER IS ON! YOU NEED TO DISABLE IT! ⚠

Hope you will enjoy it!

💝Like and Subscribe to support me 💝
TAGS:
❌ Tags (IGNORE):
synapse x cracked, synapse x crack, synapse x cracked free, synapse x cracked 2022, synapse x cracked download, synapse x free, free synapse x, synapse x download, roblox exploit, free synapse x key, roblox hack, roblox synapse x, synapse x, roblox synapse x free, synapse cracked, roblox exploit download, synapse, synapse x roblox, roblox synapse x cracked, synapse crack, cracked synapse x, roblox exploit free, synapse free, roblox, how to download synapse x, free roblox exploit, download synapse x cracked 2022, roblox free exploit, synapse x cracked free 2022, free synapse x giveaway, synapse x free download cracked 2022, synapse x cracked free roblox exploit, synapse x free executor, synapse x free download cracked 2022, roblox script executor free, free synapse, free synapse x remake, synapse free account, free synapse x key giveaway, synapse x free account generator, synapse x free robux, synapse x free download roblox 2022 mac, roblox free synapse x key, free synapse x 2022, synapse roblox, roblox cheats, roblox script executor, roblox synapse x free account, crack synapse x, roblox cheat, synapse x free download, best roblox exploit, synapse x cracked 2021 mega, roblox synapse x cracked 2021, how to crack synapse x 2020, synapse x serial key, synapse download, synapse x cracked 2021 free download, how to download synapse, synapse x cracked roblox, synapse x free 2021, roblox executor, synapse x crack download, exploit, synapse x key, roblox script, synapse x cracked mega, synapse x cracked 2022 mega download, roblox synapse, roblox exploiting, synapse x cracked no virus, synapse x exploit cracked, roblox hacking, synapse x cracked 2022, synapse x remake, synapse x crack roblox, synapse free download 2022, synapse x crack with proof, synapse x crack roblox 2021, synapse x activation crack, synapse crack download, synapse x crack 2022, synapse x cracked no linkvertise, roblox synapse x cracked 2022, synapse x cracked may, synapse x crack july 2022, roblox synapse x download, hack, best synapse x crack 2021, synapse x scripts, hacks, roblox hack 2022, exploiting, cracked, free roblox hack, free, how to get synapse x for free, free lua executor roblox, synapse x discord, synapse x free license key, lua executor, script exector, roblox lua, how to crack synapse x 2022, script, synapse x cracked no login, synapse x cracked mega download 2021, synapse x cracked mega link, synapse x cracked no key mega, synapse x cracked account, synapse x cracked free download 2021, synapse x cracked mega.nz, synapse x cracked tutorial, roblox synapse x cracked free, synapse x cracked mega download, synapse cracked roblox, roblox synapse x free download 2021 mega, synapse x cracked with key, synapse roblox free download 2022, synapse x

activation, synapse x cracked free download mega 2021, scripting roblox, roblox scripts, synapsex, syanpsex, hacking, synapse x cracked free download, synapse x roblox exploit cracked, free roblox hacks, synapse x 2021, synapse roblox cracked

Virus information:

It came with several useless files, and an instruction to disable Windows Defender. It was easily decompiled with ScyllaHide PE unpacker, because it created an unprotected thread that could be unpacked. It had the following virus types: Vidar, ArkeiStealer, Invisimole, Mimikatz, and TeamSpy. It used several different crypto wallets to mine crypto.

It also sent the user's information to discord and telegram, the telegram's location was Amsterdam.

The following ips received TCP requests from the virus:

149.154.167.99
104.98.237.123
195.201.44.125
162.159.129.233
104.21.65.227

They were all forwarded either Discord, Telegram, or Akamai Technologies, which is a company that provides hosting, analytics and malware protection.

Possible reasons investigated by ChatGPT:

Command and Control (C2) servers: The malware may be using the servers as part of its infrastructure for receiving commands from the attacker and exfiltrating data from the infected system. The attacker may choose a well-known and reputable company such as Akamai to host these servers in order to make it harder for security researchers to detect and block the communication.

Evasion tactics: The malware may be communicating to Akamai's servers in order to evade detection by security tools that may be less likely to flag traffic to a trusted and well-known company.

Data exfiltration: The malware may be sending stolen data to the Akamai servers as a way of hiding the data transfer in the noise of legitimate traffic to the company's servers.

I was only able to reverse a few functions in the source code, as the program was really big and had a lot of garbage code in it. I had to use Intezer to check where exactly the malicious functions were. I identified the debugger detector and some text processing in the functions. The rest of the functions were unintelligible even with several Windows function signatures applied.

The virus also retrieves a zip file from a server: http://195.201.44.125/package.zip I have not been able to retrieve it.

The decompiled code, original virus and unpacked thread are in this link.