SynapseX cracked virus UniqueGeese

Found on hacked youtube channel UniqueGeese, available on a mediafire page which will probably be soon deleted so I won’t post it here, but the original file is available on this git repository. The video description was the following: Hi! There is SYNAPSE X CRACK!

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. Initially, when trying to access it you get a 403 forbidden response. But upon analyzing the PCAP file you can see the HTTP request for that file uses the user agent **“Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.0.0 Safari/537.36”**, so if you change your browser to that, it works, and you get the file. I have posted the contents of it on the github page.

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