SUBEX

CyberGate Threat Report

Date: 20/05/2021

Hussain Kathawala

CyberGate is a Remote Access Trojan (RAT) that allows an attacker to gain unauthorized access to the victim's system. Attackers can remotely connect to the compromised system from anywhere around the world. The Malware author generally uses this program to steal private information like passwords, files, etc. It might also be used to install malicious software on the compromised systems.

Overview

The initial Malware is a dropper that executes and drops a malicious file into the victim system without the consent of the user. The dropped file starts its execution and performs anti-VM checks to prevent the execution in any virtual environment. After which the Malware performs various malicious activities, like Keylogging, and stealing sensitive information. Then it creates a legitimate process to communicate with the C2 server.

Infection

The initial executable is a PE32 file, for Intel architecture compiled with .NET. It drops another executable in the temp folder with the name "`Qlezrhhlbmw.exe`".

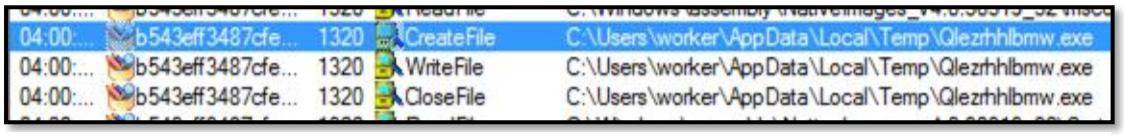

Figure 1

The dropper when disassembled, shows classes with random generated names like "`ADPRnBdJjt8XwX2FQm`" and "`eWANbC7fX237ucPNNr`" to avoid detection and analysis.

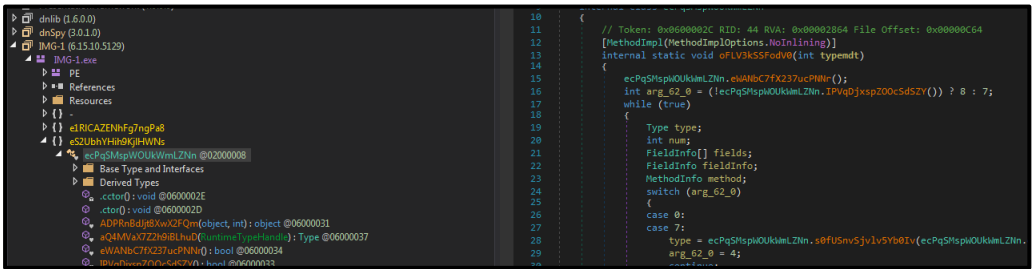

Figure 2

Once the actual RAT is dropped, its execution begins. To remain persistent in the system, the malware creates copies of itself in the folder "`c:\\programfiles(x86)\rdns`" as "`windows`" as shown in the figure below. The copy of the executable gets deleted after the execution gets completed.

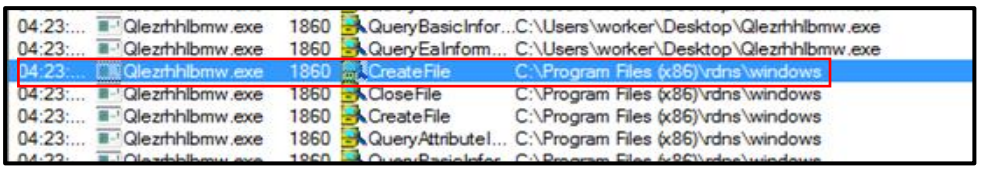

Figure 3

It creates a legitimate process in firefox.exe and it injects a code using various functions as seen in the below figure. It allocates memory through this step.

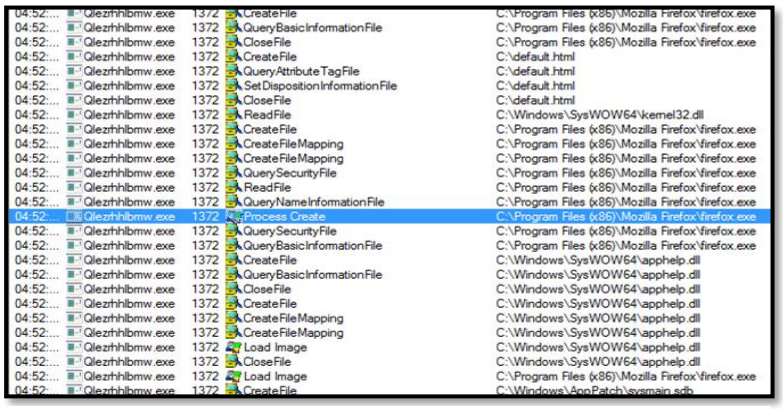

Figure 4

The malware contains functionality to read the clipboard data with the "`GetClipboardData`" function as seen below. The return value of this function is the handle to a clipboard object.

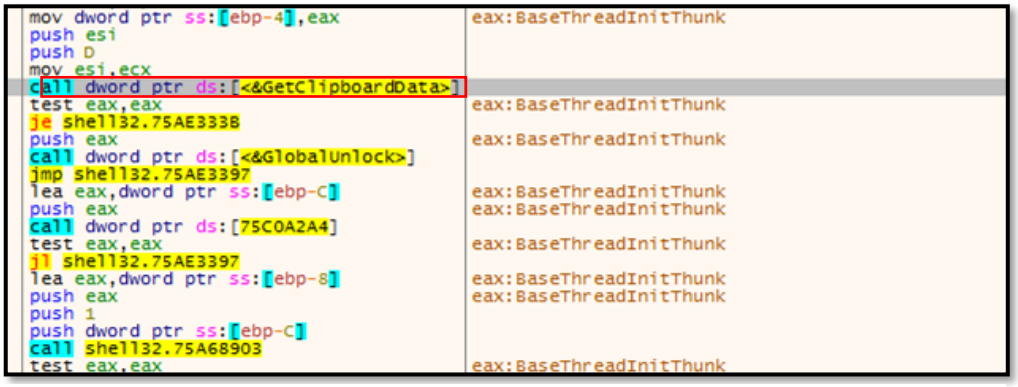

Figure 5

It also retrieves information about pressed keystrokes and acts as a Keylogger using the function "`GetKeyboardState`". It gives the status of the 256-virtual keys.

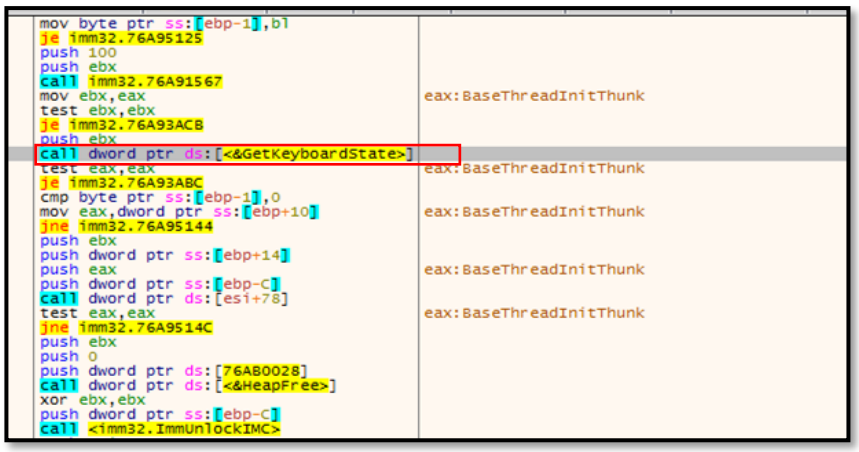

Figure 6

The malware also has a functionality to retrieve handle of the desktop window of the victim system using the functionality, "`GetDesktopWindow`".

Figure 7

Anti-VM & Anti-Debug Feature

The malware performs various anti-VM checks on the victim machine. This statement is supported with the figure shown below.

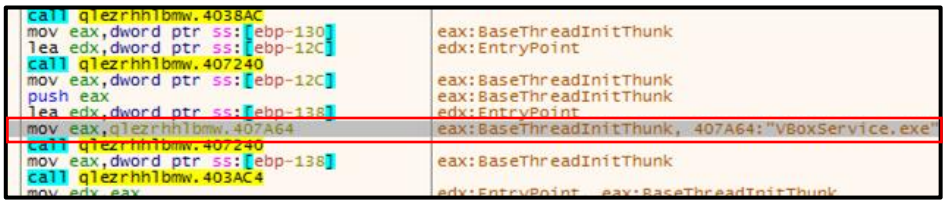

Figure 8

It also checks for the presence of kernel debugger in the system. This can be observed because of the strings like "`\\\\.\\Syser`", "`\\\\.\\SyserDbgMsg`" and "`\\\\.\\SyserBoot`".

Figure 9

Network Traffic Analysis

Once it captures the information, the malware tries to communicate with the C2 server "`aside.no-ip.org`" using the foreign process i.e., firefox.exe as we can see in the below figure.

Frame Number	Time Date Local Adjusted	Time Offset	Process Name	Source	Destination	Protocol Name	Description
5	06:29:23 18/05/2021	17.8567743	firefox.exe	10.0.2.15	asade.no-ip.org	TCP	TCP:Flags=.....S., SrcPort=49160, DstPort=25565,
7	06:29:26 18/05/2021	21.1631054	firefox.exe	10.0.2.15	asade.no-ip.org	TCP	TCP:[SynReTransmit #5]Flags=.....S., SrcPort=491
13	06:29:32 18/05/2021	27.1777299	firefox.exe	10.0.2.15	asade.no-ip.org	TCP	TCP:[SynReTransmit #5]Flags=.....S., SrcPort=491
19	06:29:51 18/05/2021	46.0359687	firefox.exe	10.0.2.15	asade.no-ip.org	TCP	TCP:Flags=.....S., SrcPort=49161, DstPort=25565,
21	06:29:54 18/05/2021	49.0500307	firefox.exe	10.0.2.15	asade.no-ip.org	TCP	TCP:[SynReTransmit #19]Flags=.....S., SrcPort=49
24	06:29:59 18/05/2021	54.2254584	firefox.exe	10.0.2.15	asade.no-ip.org	TCP	TCP:[SynReTransmit #19]Flags=.....S., SrcPort=49
26	06:30:19 18/05/2021	73.7196177	firefox.exe	10.0.2.15	asade.no-ip.org	TCP	TCP:Flags=.....S., SrcPort=49162, DstPort=25565,
28	06:30:22 18/05/2021	76.7183464	firefox.exe	10.0.2.15	asade.no-ip.org	TCP	TCP:[SynReTransmit #26]Flags=.....S., SrcPort=49
31	06:30:29 18/05/2021	83.9980817	firefox.exe	10.0.2.15	asade.no-ip.org	TCP	TCP:[SynReTransmit #26]Flags=.....S., SrcPort=49

Figure 10

MITRE Attack Techniques Used

Technique ID	Technique
T1497	Virtualization/Sandbox Evasion
T1055	Process Injection
T1056	Input Capture
T1115	Clipboard Data
T1113	Screen Capture
T1036	Masquerading

IOC's

4df346a12ef5679ec0b960d037c8f52a
2cad1ad59e145139cbab70260b1a2f19
hxxp://asade.no-ip.org
178.206.211.67

Subex Secure Protection

Subex Secure detects the sample as "SS_AI_Trojan_PE".

Our Honeypot Network

This report has been prepared from the threat intelligence gathered by our Honeypot network. This Honeypot network is today operational in 62 cities across the world. These cities have at least one of the following attributes:

- Are landing centers for submarine cables
- Are internet traffic hotspots
- House multiple IoT projects with a high number of connected endpoints
- House multiple connected critical infrastructure projects
- Have academic and research centers focusing on IoT
- Have the potential to host multiple IoT projects across domains in the future.

Over 3.5 million attacks a day is being registered across this network of individual Honeypots. These attacks are studied, analysed, categorized, and marked according to a threat rank index, a priority assessment framework that we have developed within Subex. The Honeypot network includes over 4000 physical and virtual devices covering over 400 device architectures and varied connectivity mediums globally. These devices are grouped based on the sectors they belong to for purposes of understanding sectoral attacks. Thus, a layered flow of threat intelligence is made possible.