SECTRIO

MALWARE REPORT

RevengeRAT

Date: 24/06/2021

Shikha Sangwan

RevengeRAT is a potential Remote-Access Trojan malware. Microsoft has issued an alert over a RAT dubbed RevengeRAT that it says has been used to target Aerospace and Travel sectors with spear-phishing emails. This RAT is used as a Crypter-as-a-Service.

Overview

This RAT once installed into the system, checks for any anti-virus or any security software in the system and drops multiple executables in the system for persistence. The dropped malware is a backdoor which looks like a genuine application. The malware connects to the C&C server and steals sensitive information about the system, physical memory, webcams, and the machine's user. It encodes the collected information, sends it to the C2 server and compromise the victim's machine.

Technical Analysis

Once we run the malware in the system, it drops and starts a program with name "win_service.exe" which is a backdoor, and it misleads the user as its name looks like a legitimate software.

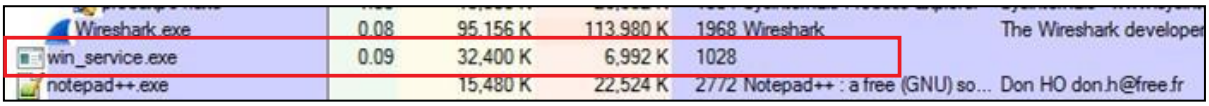

Figure 1 Trojan Backdoor

Persistence

It drops the PE file to the start-up folder (as shown in the figure below). Malware uses start-up items to automatically execute at boot to establish persistence. It also creates a start menu entry and stores files in the Windows start menu directory.

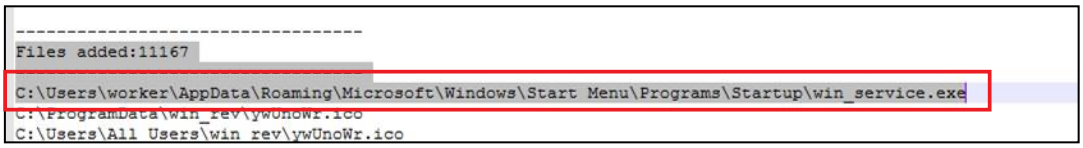

Figure 2 Dropped PE file in the start-up folder

Hooking

It creates files in the recycle bin andvolume driver for hiding and protection.

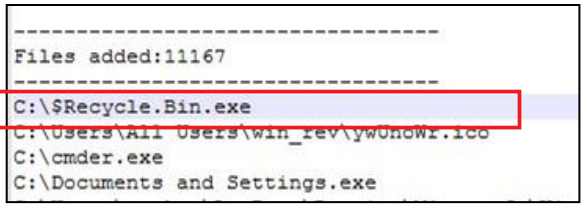

Figure 3 File created in the recycle bin

It turns off the Windows Error reporting for the current user, as shown below in the disassembly at address "0000000076F28FE6". This disables application error reporting messages to hide itself.

Figure 4 Address: 0000000076F28FE6 disabling application error reporting

Backdoor

It reads .ini files from the desktop to get the configuration information of different programs that runs in the system.

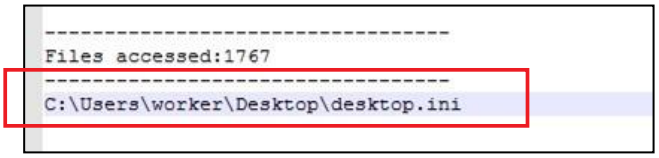

Figure 5 Read desktop's ini file

Then the backdoor steals critical system information like the victim's user name and computer name, Windows system information, capacity of the physical memory, type of security software installed in the system, and language used on the victim machine. (As shown in the disassembly below)

Figure 7 address:0000000076F1E568 reading computer's name

Figure 6 address:0000000076F72ABD reading user's name

Figure 8 address:0000000077117181 getting system's volume information

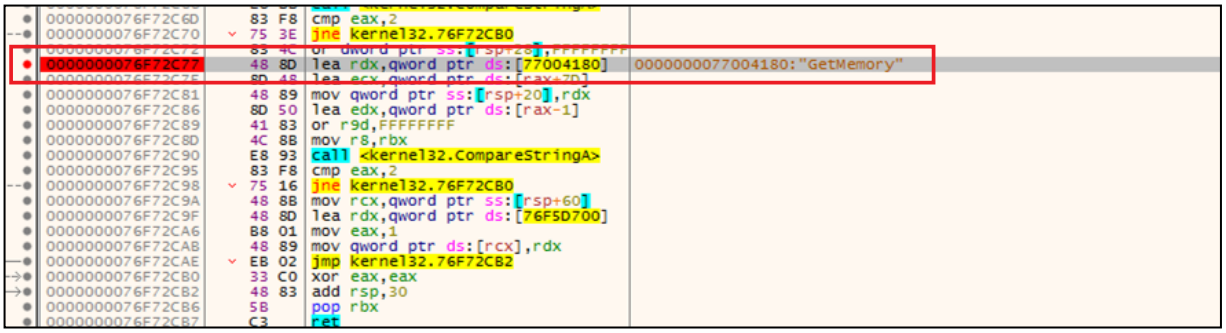

Figure 9 address:0000000076F72C77 getting system's physical memory

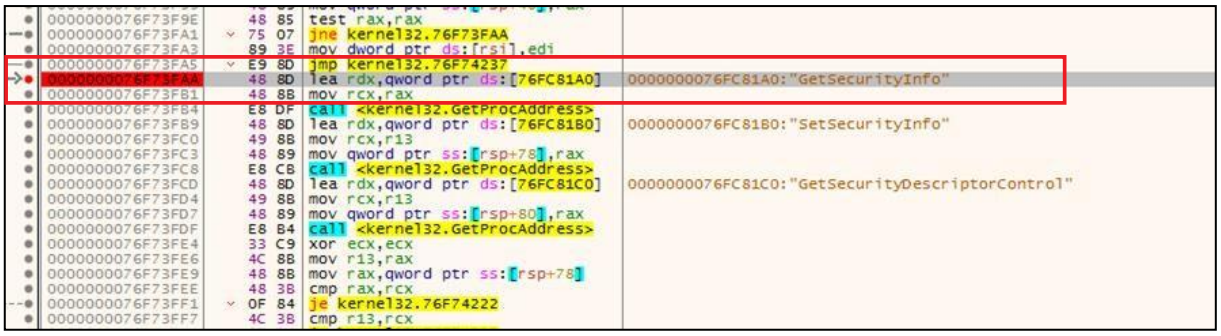

Figure 10 address:0000000076F73FAA getting system's security software information

Figure 11 address:000000007FEF284EEAA getting system's language information

It also reads the software policies to get the information of the software installed in the system.

Figure 12 address:0000000076F311AD reading software's policies

C&C Server

The RAT connects to the C2 server and sends the collected data from the victim's system to the C2 server, whose IP addresses are:

`192.3.122.73`
`45.61.48.65`

The server port numbers used are "1339" and "6767".
The malware keeps trying to make connections to the two IP addresses until the connection has been established.

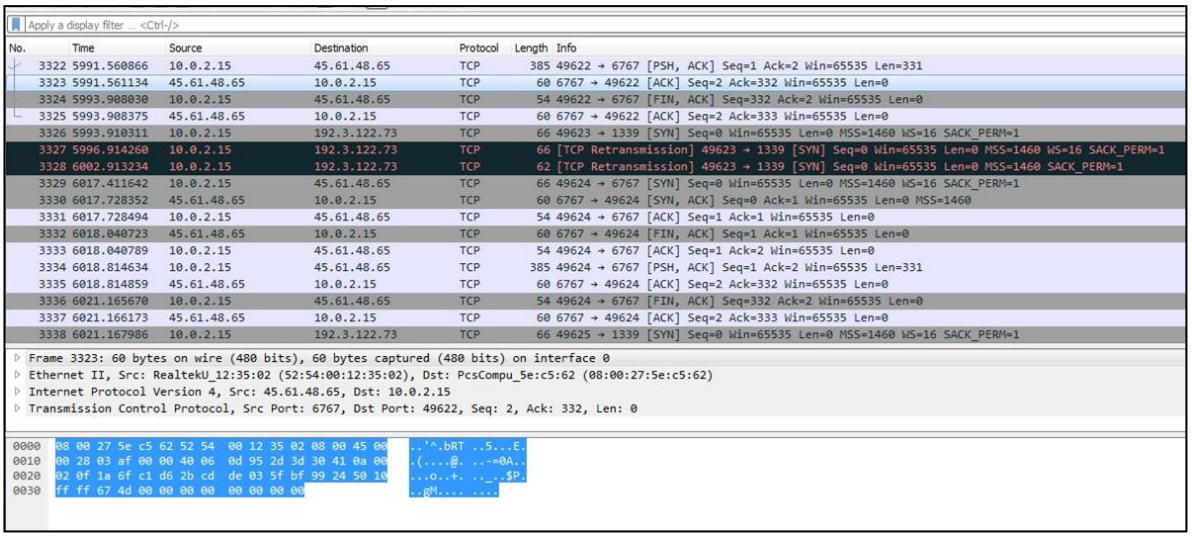

Figure 13 connecting to C2 server

Once the connection to the C&C server is established, the information that is collected by the malware is sent to its server. The packet that is sent from the victim's machine to the server looks like the image below:
Most of the strings in the packet are base64 encoded.

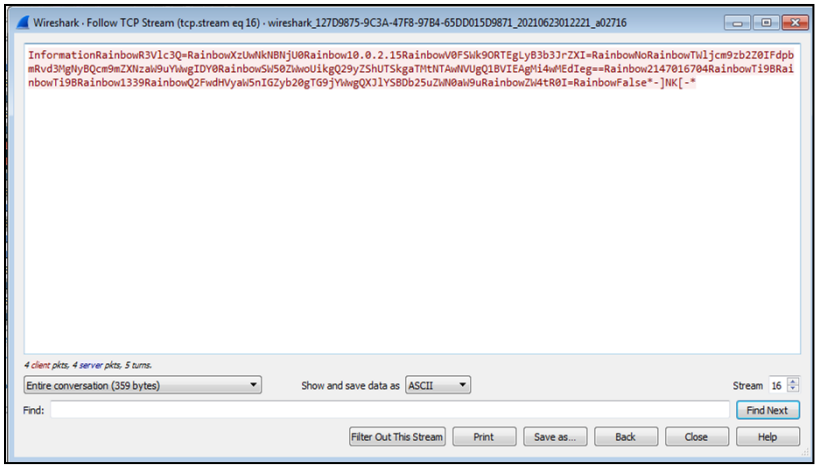

Figure 14 packet sent to server

InformationRainbowR3Vlc3Q=RainbowXzUwNkNBNjU0Rainbow10.0.2.15RainbowV0FSWk9ORTEgLyB3b3JrZXI=RainbowNoRainbowTWljcm9zb2Z0IFdpbmRvd3MgNyBQcm9mZXNzaW9uYWwgIDY0RainbowSW50ZWwoUikgQ29yZShUTSkgaTMtNTAwNVUgQ1BVIEAgMi4wMEdIeg==Rainbow2147016704RainbowTi9BRainbowTi9BRainbow1339RainbowQ2FwdHVyaW5nIGZyb20gTG9jYWwgQXJlYSBDb25uZWN0aW9uRainbowZW4tR0I=RainbowFalse*-]NK[-*

As we can see, the packet is split into different blocks which are separated by the string "Rainbow".
Below is the explanation of different blocks present in the packet:

- "Rainbow" is a separator here which splits the data in the packet.
- "Information" is always the first part of the packet.
- "R3Vlc3Q=" is decoded as "Guest".
- "XzUwNkNBNjU0" is decoded as "_506CA654", which is the volume information.
- "10.0.2.15" is the IP address of victim's machine.
- "V0FSWk9ORTEgLyB3b3JrZXI=" is decoded as "WARZONE1 / worker" is the victim's machine name nad username.
- "No" is whether the victim has a webcam or not.
- "Twljcm9zb2Z0IFdpbmRvd3MgNyBQcm9mZXNzaW9uYWwgIDY0" is decoded as "Microsoft Windows 7 Professional 64", which is the victim's Windows system information.
- "SW50ZWwoUikgQ29yZShUTSkgaTMtNTAwNVUgQ1BVIEAgMi4wMEdIeg==" is decoded as "Intel(R) Core(TM) i3-5005U CPU @ 2.00GHz", which is the CPU information.
- "2147016704" is the system physical memory.
- "Ti9B" is decoded as "N/A", which could be whether any antivirus or firewall is installed or not.
- "1339" is the port number of the C&C server it is connecting to.
- "Q2FwdHVyaW5nIGZyb20gTG9jYWwgQXJlYSBDb25uZWN0aW9u" is decoded as "Capturing from Local Area Connection" which could be the title of the top-most window, in mine it was Wireshark.
- "ZW4tR0I=" is decoded as "en-GB", which is the language used on the victim's machine.
- "*-]NK[-*" is used to define the end of packet.

Sandbox Evasion

It tries to detect if any VM or sandbox is running in the system to evade the virtual environment. It also drops some PE files which has not been started or loaded, to remove the attention from the actual backdoor.

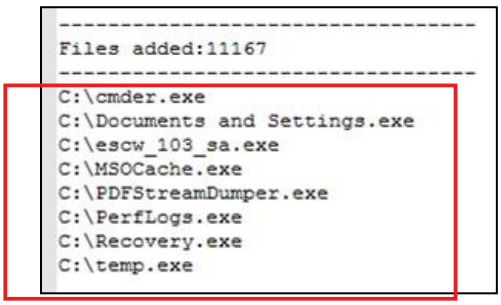

Figure 15 dropped PE files

MITRE Attack Techniques Used

Technique ID	Tactic	Technique
T1106	Execution	Native API
T1037.005	Persistence	Startup Items
T1547.001	Persistence	Registry Run Keys / Startup Folder
T1055	Privilege Escalation	Process Injection
T1036	Defensive Evasion	Masquerading
T1497	Defensive Evasion	Virtualization/Sandbox Evasion
T1564.001	Defensive Evasion	Hidden Files and Directories
T1027	Defensive Evasion	Obfuscated Files or Information
T1027.002	Defensive Evasion	Software Packing
T1518.001	Discovery	Security Software Discovery
T1083	Discovery	File and Directory Discovery
T1082	Discovery	System Information Discovery
T1560	Collection	Archive Collected Data
T1573	Command and Control	Encrypted Channel
T1571	Command and Control	Non-Standard Port
T1219	Command and Control	Remote Access Software

Sectrio Protection

Sectrio detects this malware as “SS_Gen_RevengeRAT_PE_A”.

IOC's

IPs
192.3.122.73
45.61.48.65

Sample
313afaedd435018403f358337115eb45

Dropped file
f3dd3b35b5ea9f30f946f86e6b3a4730
c2082df303350b29360581d4bf3e9d42
3199e7449063b2699b48cdf607357bfc
7fa50220d182c6ec9e223355e8daf2bd
3e2bfc63f1945a9c2bd43822ea609cda
3cab7117fcc6f319e2ccfc550e8b284a

Our Honeypot Network

This report has been prepared from the threat intelligence gathered by our honeypot network. This honeypot network is today operational in 72 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 12 million attacks a day is being registered across this network of individual honeypots. These attacks are studied, analyzed, categorized, and marked according to a threat rank index, a priority assessment framework that we have developed within Sectrio. 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.