
infinitum IT
Power of integrated Security
Shadow0x
Miner RAT
www.infinitumit.com.tr
infinitumitlabs

CONTENTS

Shadow Miner RAT and What You Need to Know

What is Shadow Miner RAT?

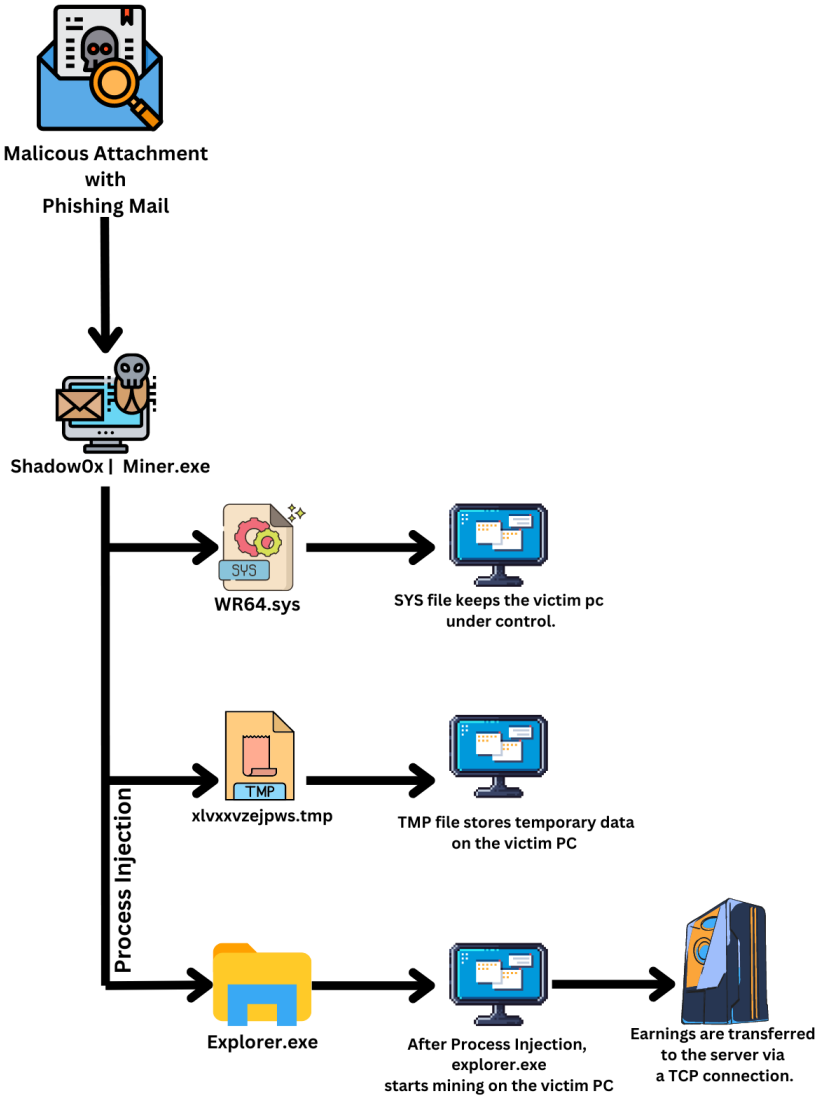
A Remote Access Trojan (RAT) constitutes a class of malicious software that affords an unauthorized infiltrator the capability to access a target computer or network. This form of software embeds itself surreptitiously within the targeted system, enabling the perpetrator to establish remote control, gain access to data, and execute various malicious activities.

A Crypto Miner denotes a software variant that leverages the resources of a victim's computer to generate revenue through cryptocurrency. Adversaries may employ such software to pilfer the victim's computational power and mine cryptocurrencies through a process that appropriates the victim's resources to respond to escalating demands.

The Shadow0x Miner RAT represents a pernicious software entity with an exceedingly inconspicuous detection rate, discretely implanting itself within the victim's computer. This software engenders an interface linking the perpetrator and victim systems, facilitating remote control by the former. Additionally, unauthorized access to the victim's data is achieved, thus empowering the exfiltration or malevolent exploitation of said data. Concomitantly, this RAT endows the perpetrator with the ability to harness the victim's Graphics Processing Unit (GPU) for cryptocurrency mining.

These genres of malicious software proffer substantial security risks for both individual users and enterprises. RATs crafted with sophisticated methodologies and possessing low detectability can circumvent conventional security measures, operating surreptitiously for extended durations. Vigilance demands fortification of defense mechanisms against such threats, along with regular updates to security software and stringent avoidance of downloading and executing files from unknown sources.

Infection Chain



Shadow0x Miner RAT Overview

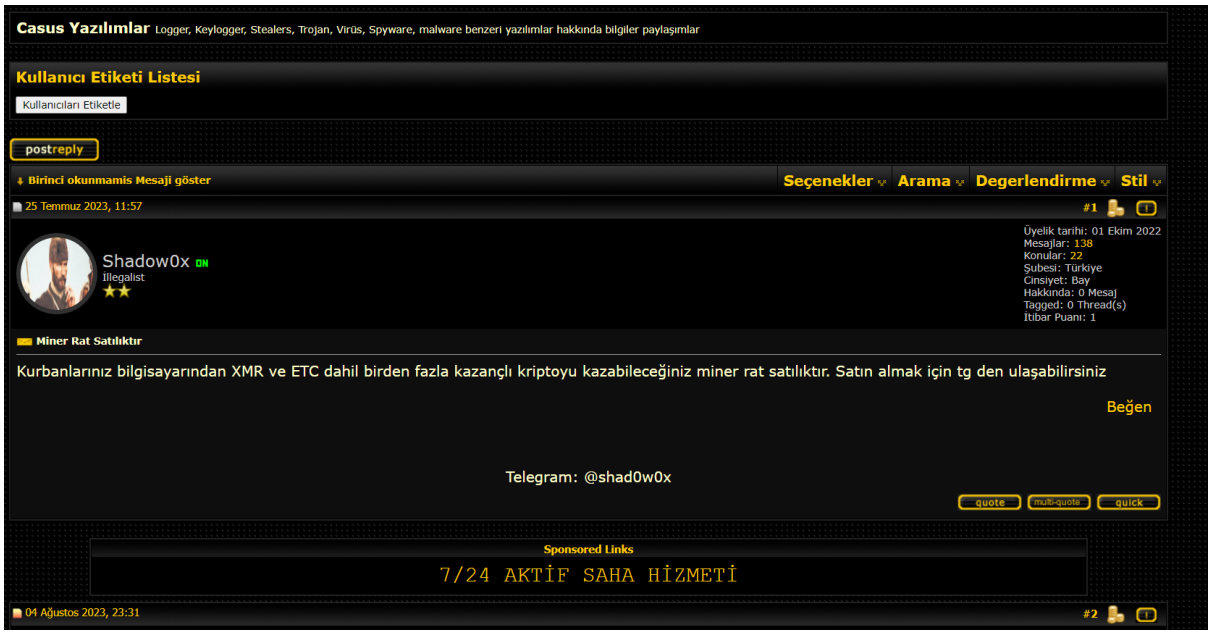


Figure 1- Dark Web forum info

The seller has a nickname called Shadow0x and selling this crypto miner on a darkweb forum. He's using Telegram for communication.

Figure 2- Malware features

The project has a very low detection rate and it bypasses most used antiviruses. The seller and its customers **mostly target Turkey** and he claims to have big illegal services for Turkey.

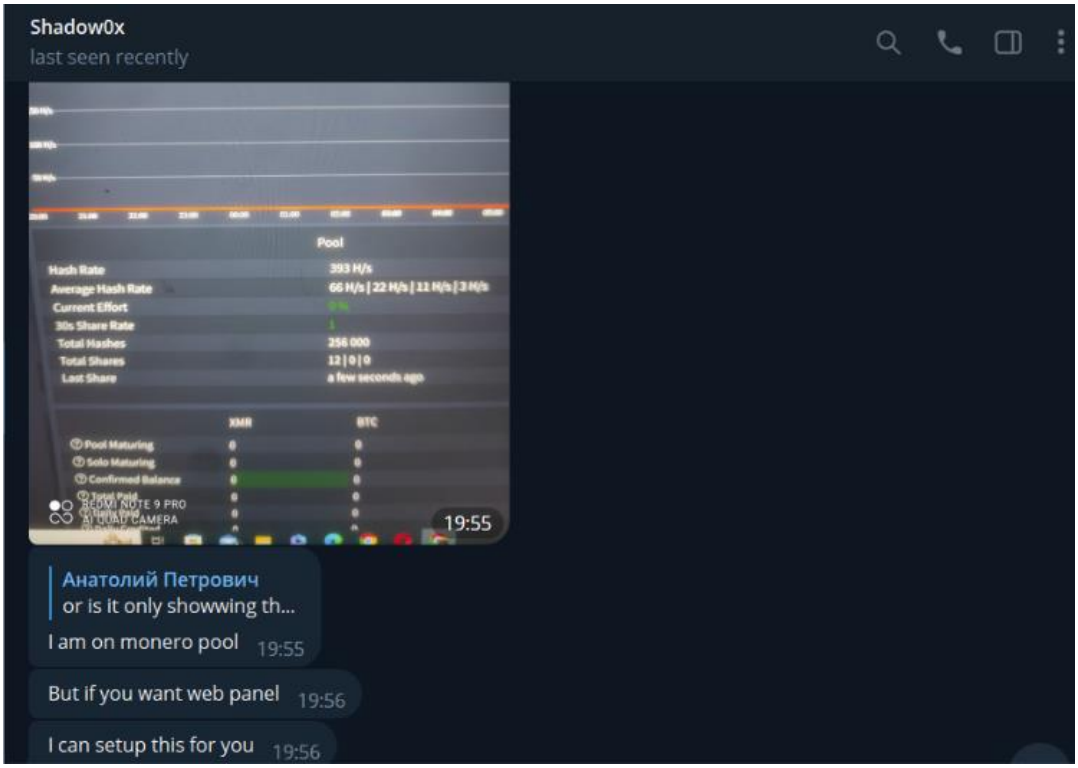


Figure 3- Web panel for bitcoin

The seller uses crypto pools by default but he can setup a web panel for a certain amount of bitcoin.

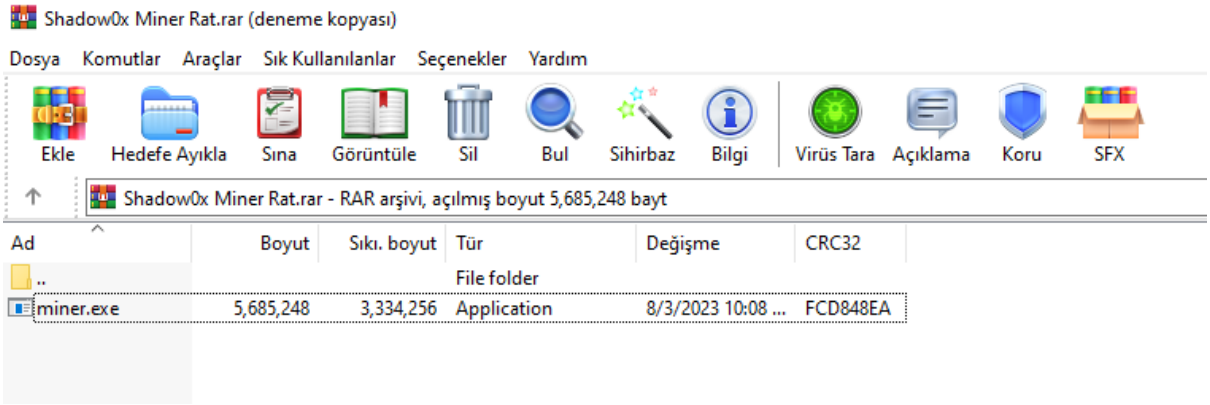


Figure 4- Information about file

The miner comes with a simple “EXE” file. It’s **5.42MB** and once the malicious file is executed, it starts mining using the victim's GPU.

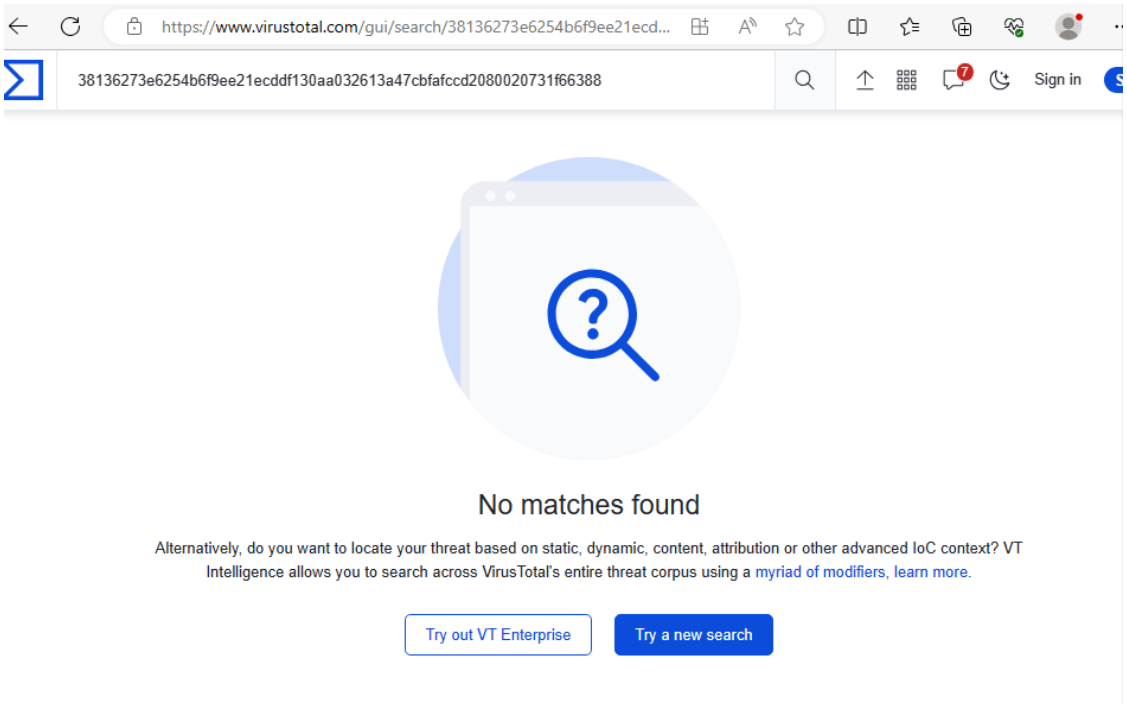


Figure 5- VirusTotal info

The project is quite new, the hash information is not available in the VirusTotal database.

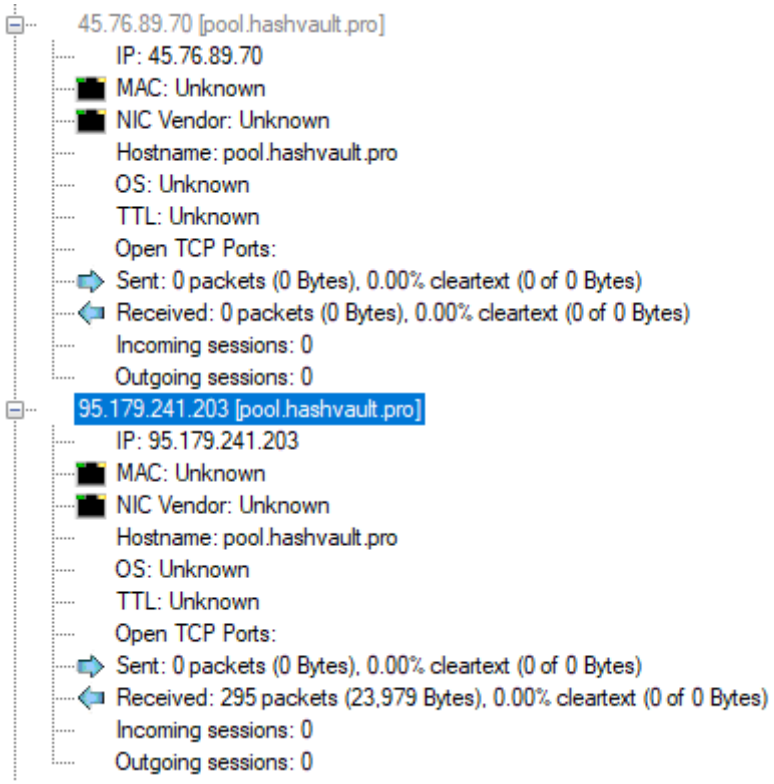


Figure 6- Network information

“miner.exe” does not establish a TCP connection but it sends UDP packets to **“pool.hashvault.pro”** which is the pool of cryptocurrency Shadow0x use.

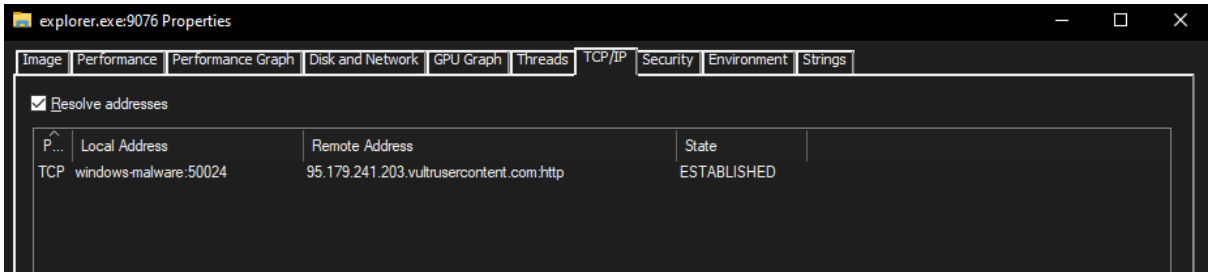


Figure 7- TCP connection

The "miner.exe" file shuts down after running for a period of time. Subsequently, a seemingly legitimate 2.4GB file named **"explorer.exe"** is executed, aiming to deceive the user. This "explorer.exe" enables communication between the attacker and the compromised device. It establishes a TCP connection with the IP address **"95.179.241.203"** of Shadow0x's VPS server.

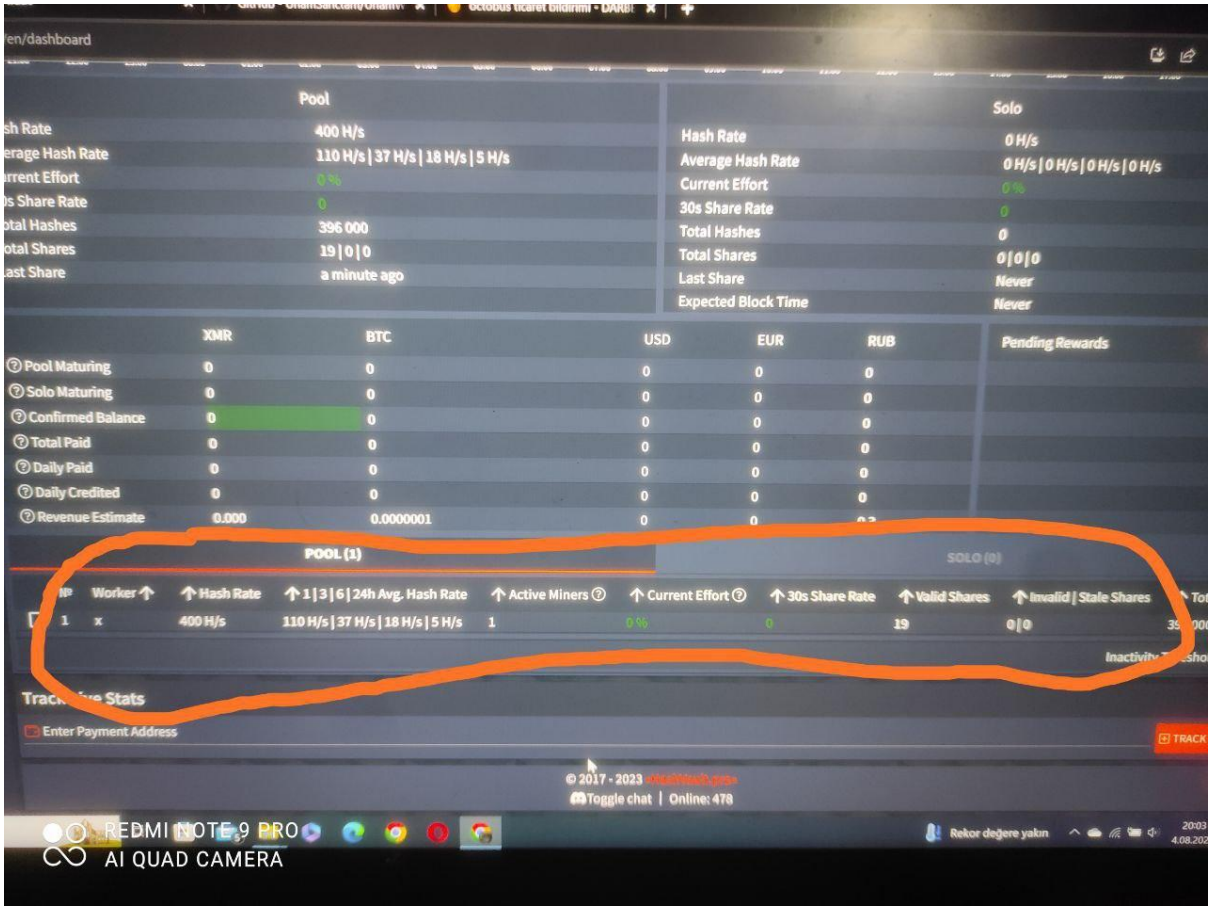


Figure 8- Hashvault pool of crypto information earned

The earnings that the crypto miner makes can be tracked from the hashvault pool dashboard.

Static Analysis

miner.exe Analysis

File Name	miner.exe
MD5	24d9219e4542504ace0faaa3a0305022
SHA256	38136273e6254b6f9ee21ecddf130aa032613a47cbfafccd2080020731f66388
File Type	PE/64

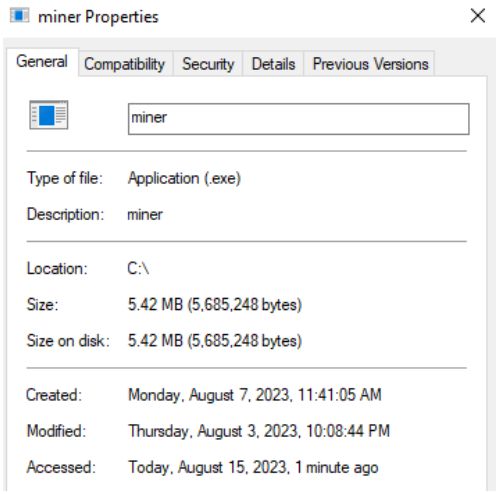


Figure 1- Information about malicious file

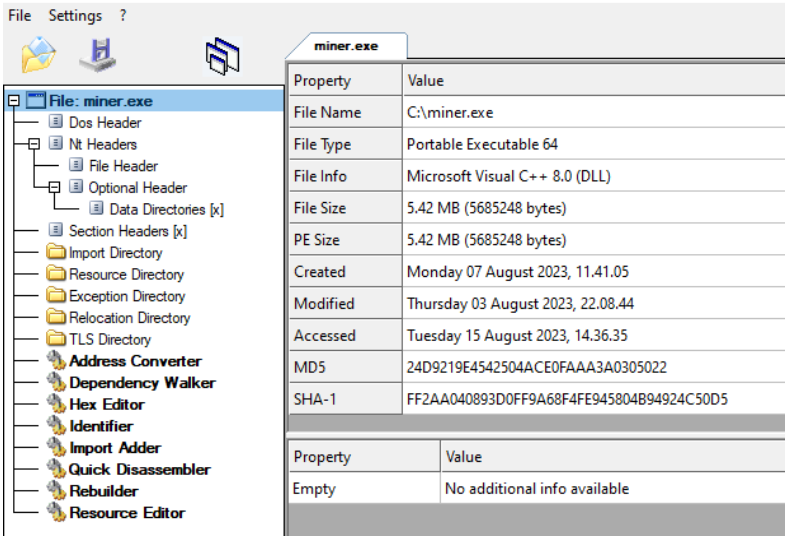


Figure 2- General Information

It has been determined that miner.exe is written in the C++ programming language.

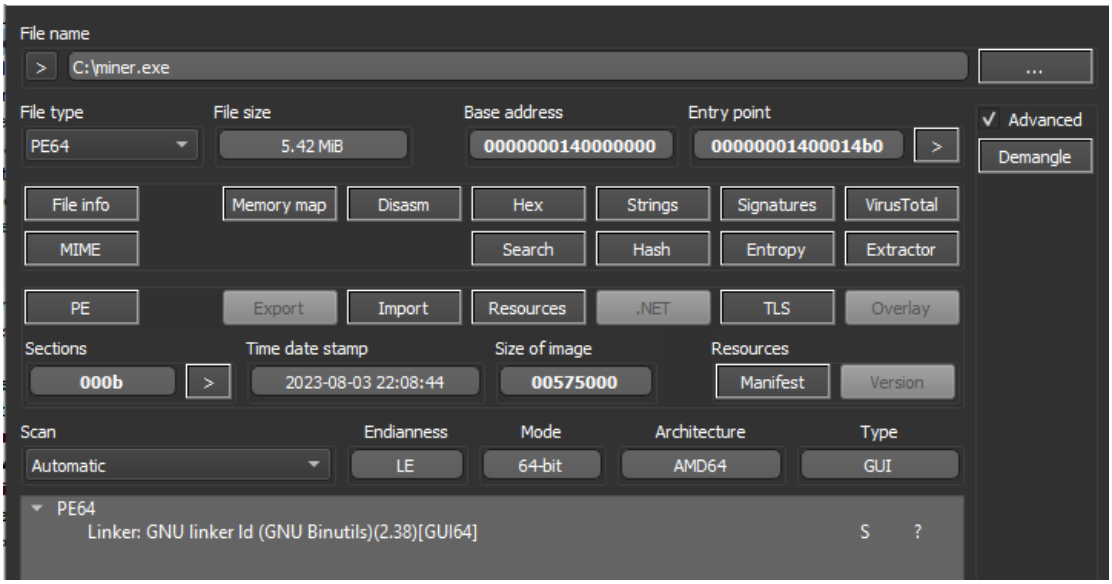


Figure 3- Executed malicious file

It was determined that no packaging technique was used.

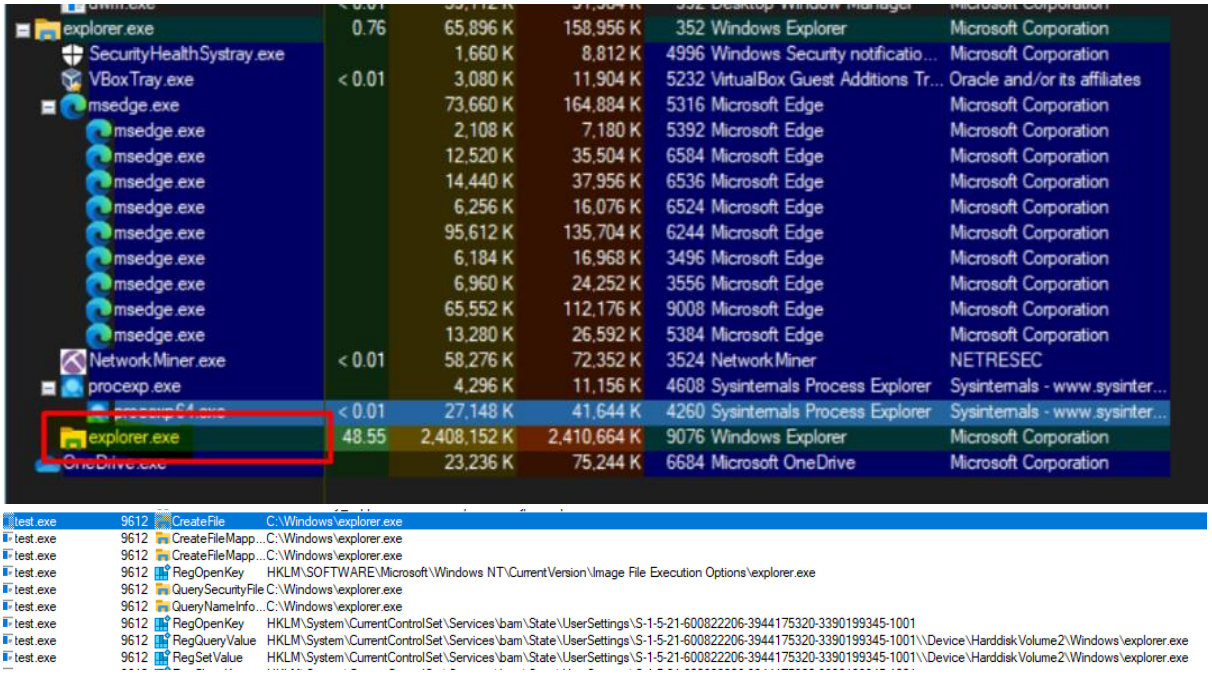


Figure 4- Executed malicious file

Once the malicious file is executed, it's running in background with the filename the victim opens it. The malicious file does not create any subfiles but it kills its process in a few seconds and it runs as **"explorer.exe".**

Dynamic Analysis

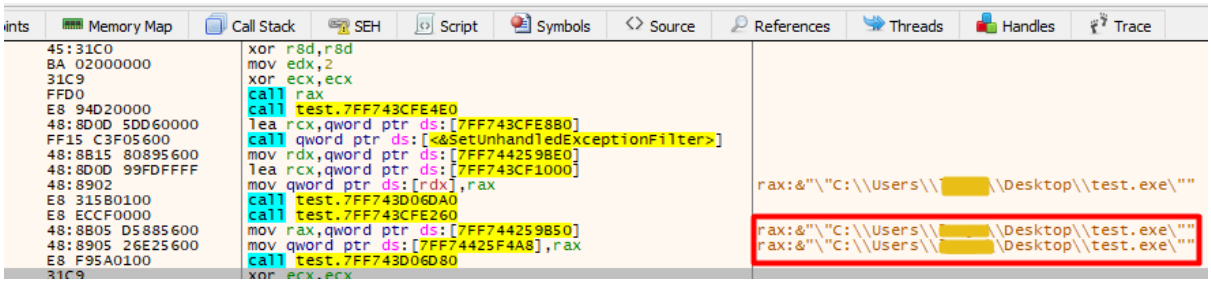


Figure 1- Gets location information

The malicious file gets the information in which location it is running.

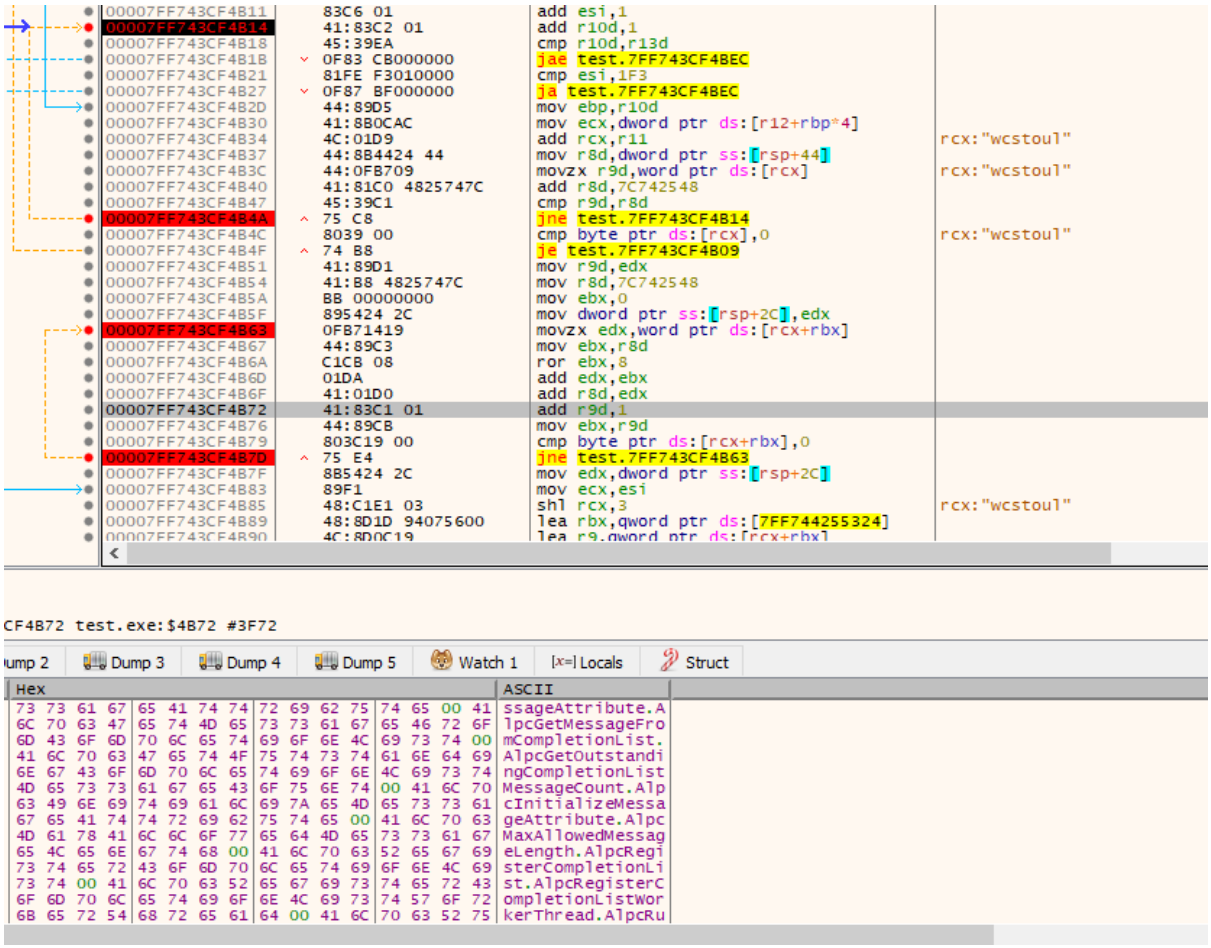


Figure 2- Loads Functions

It has been determined that the program parses strings in order to continue its operations. Some of the analyzed expressions are as shown in the figure.

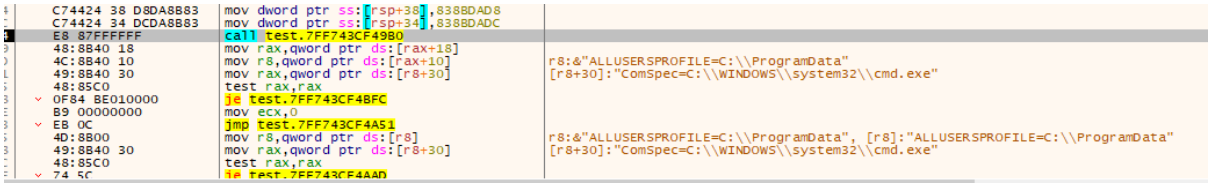


Figure 3- Using ALLUSERPROFILE

This directory is used to store data shared by programs. This expression means that programs can store data accessible to all users here. It calls the cmd.exe command client to process common data (for example, settings files or databases) under the ALLUSERPROFILE path. The malware uses the command prompt to perform complex operations or make system-level adjustments.

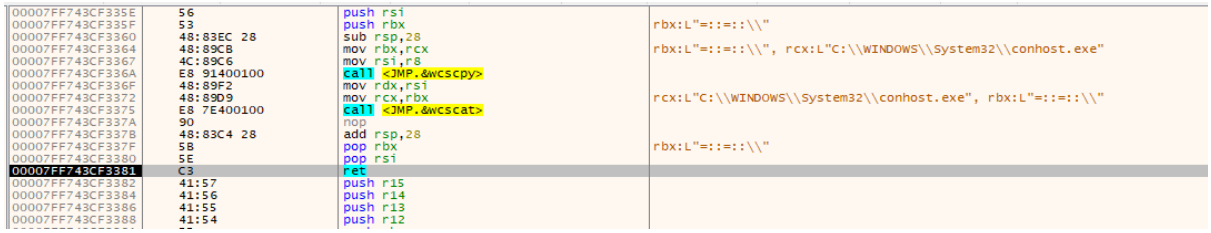


Figure 4- Conhost.exe

The miner uses conhost.exe to continue its malicious activities by performing command line operations in the background or displaying console-based output.

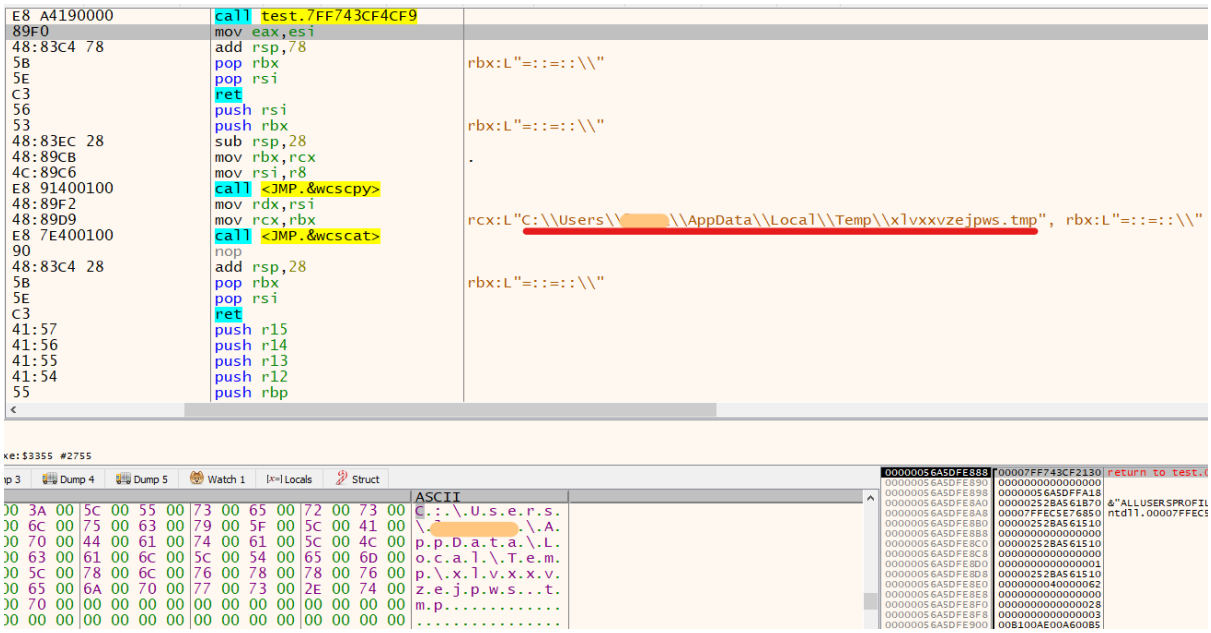


Figure 5- Creates xlvxxvzejpws.tmp file

The miner creates a temp file named **"xlvxxvzejpws.tmp"** that contains malicious code. The purpose of creating a temporary file in this directory is to bypass security products and avoid being scanned. The malware can stay for a while and continue its malicious activities silently.

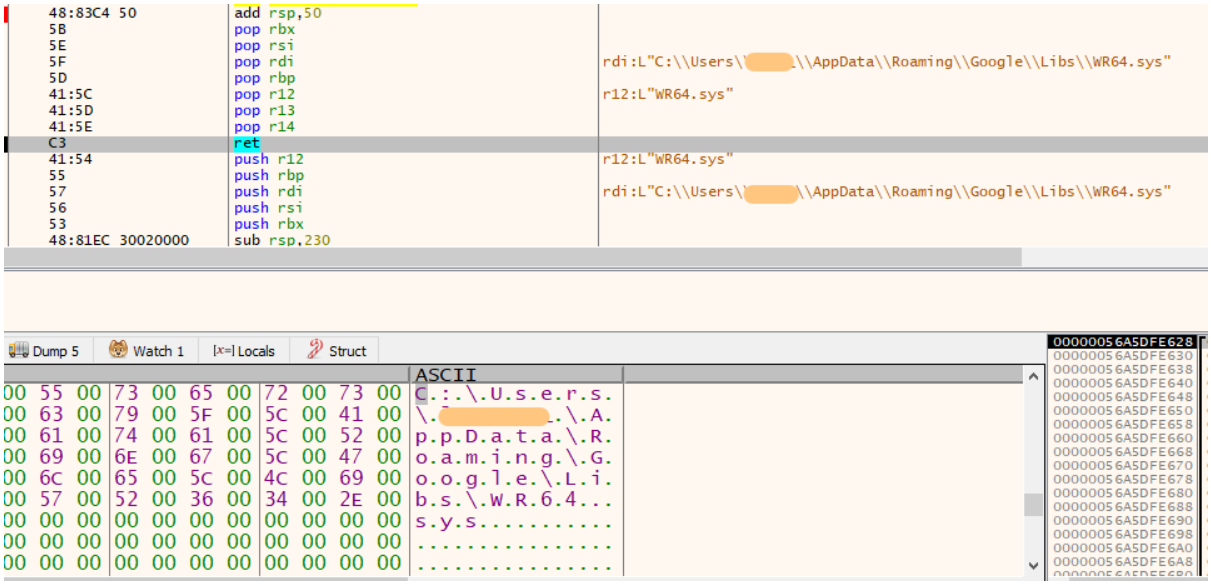


Figure 6- Creates malicious WR64.sys file

It creates the **"WR64.sys"** file in the directory **"C:\Users\Admin\AppData\Roaming\Google\Libs"** The generated fake **"WR64.sys"** file is used to perform various malicious actions on the infected computer, such as stealing sensitive information, installing malicious software, gaining unauthorized access and control over the system for malicious purposes.

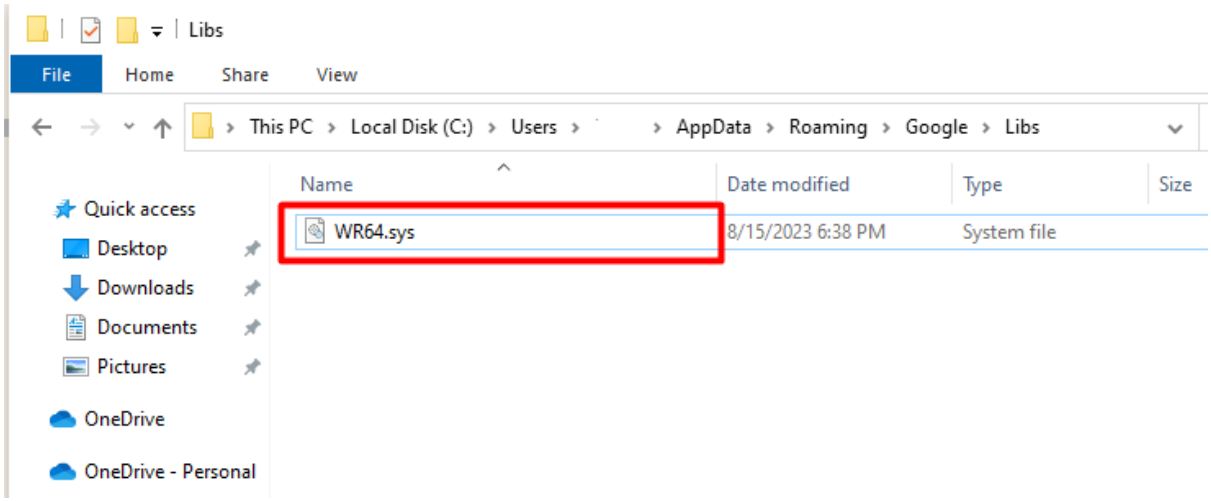


Figure 7- Created WR64.sys file

It can be observed that the created WR64.sys file is registered in the directory **"C:\Users\Admin\AppData\Roaming\Google\Libs".**

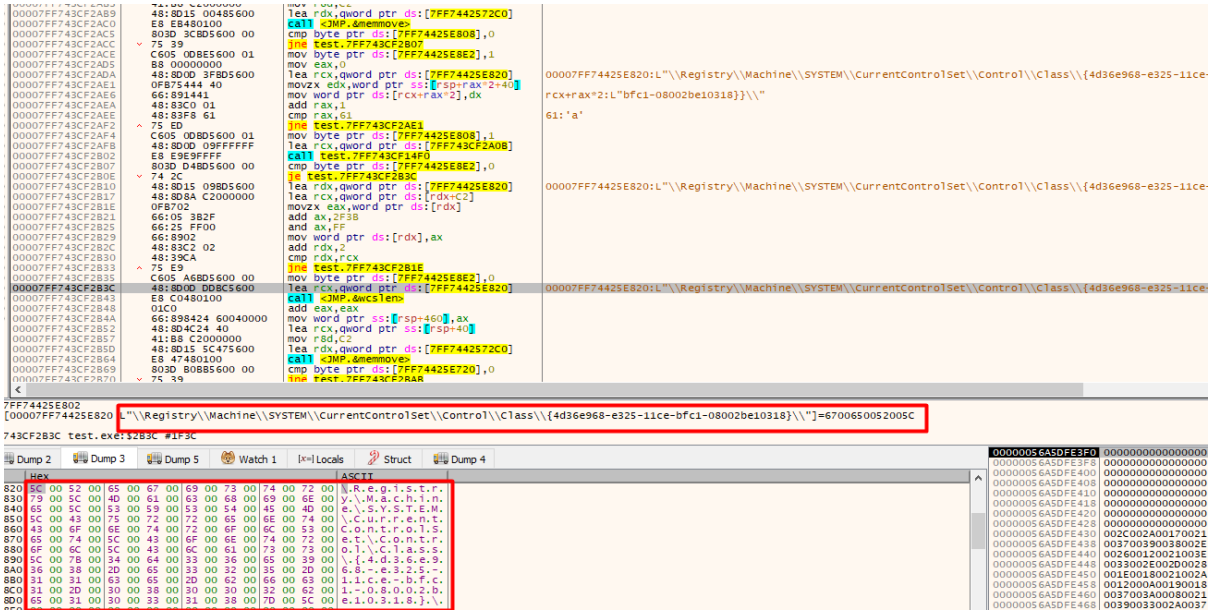


Figure 8- Using registry key

This Registry **("\\Registry\\Machine\\SYSTEM\\CurrentControlSet\\Control\\Class\\{{4d36e968-e325-11ce-bfc1-08002be10318}}")** operation is commonly used in Windows systems to manage drivers for hardware devices. The miner utilized the system-level access privileges of hardware devices to establish a persistent impact within the system.

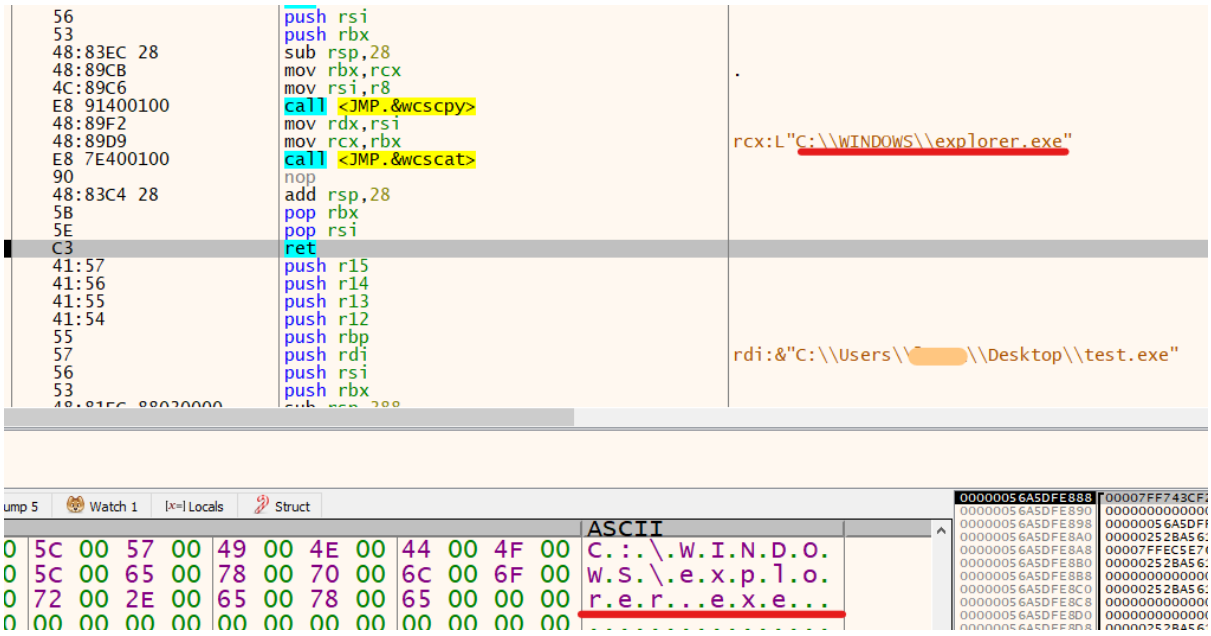


Figure 9- Creates explorer.exe

To silently persist within the system without being noticed by the user and to establish permanence within the system, **it continues as explorer.exe.** This is where **Command and Control (C2)** processes take place. Through this method, the attacker can remotely control compromised devices, execute desired actions, and enable covert transmission of sensitive data.

IOCs

IPs :

IOC Type	IOC
IPv4	45.76.89[.]70
IPv4	95.179.241[.]203

DOMAINs:

IOC Type	IOC
Domain	vultrusercontent[.]com
Domain	pool.hashvault[.]pro

HASHs:

IOC Type	IOC
MD5	24d9219e4542504ace0faaa3a0305022
MD5	f4976ef29e3ae6c8e0bfc2c3139a4ac5
MD5	718f54c5d2d887210b5d50e0a9cbc14c48901db1
SHA1	ff2aa040893d0ff9a68f4fe945804b94924c50d5
SHA1	80aef0cc3c3ec37b59f44d63b7e36bf52e81e904
SHA1	718f54c5d2d887210b5d50e0a9cbc14c48901db1
SHA256	38136273e6254b6f9ee21ecddf130aa032613a47cbfafccd2080020731f66388
SHA256	5a2602ba4027bb49e07a4cfd40ab3304c12e583d4e53981b0afa2215a394a02e
SHA256	767bec990ffbac2ff16d6ab929e5f72294e00dabcc5f39a9267648e70dda6f1d

YARA RULE

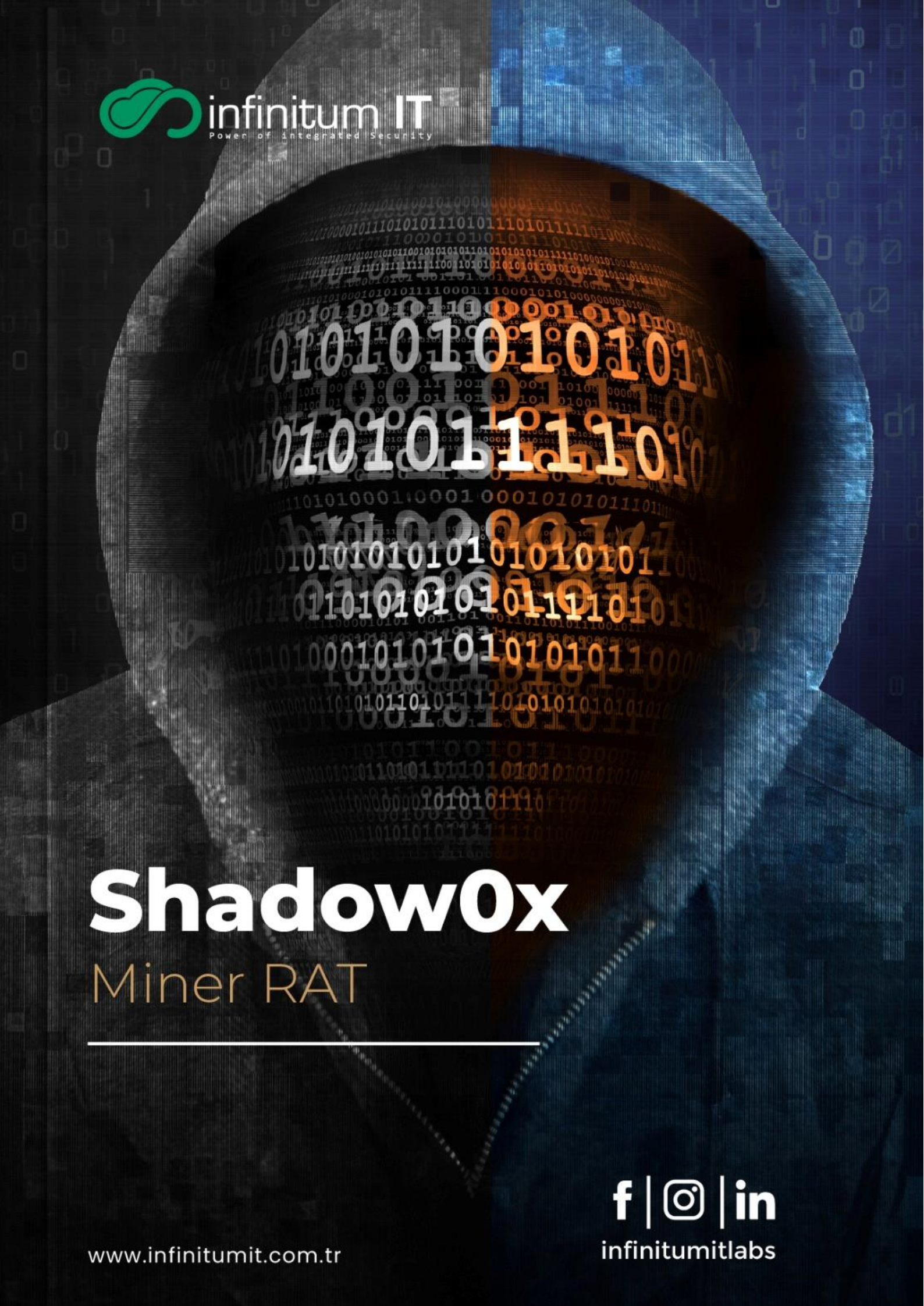
```
import "hash"
rule Shadow0x
{
meta:
        author = "Kerime Gencay"
        description = "Shadow0x Miner RAT Rule"
        file_name = "miner.exe"
        hash = "24d9219e4542504ace0faaa3a0305022"
strings:

        $opc1 = {E8 3F 5E 01 00 48 85 C0 0F 94 C0 0F B6 C0 F7 D8 48 83 C4 28}
        $opc2 = {0F B7 54 44 70 66 89 14 41 48 83 C0 01 48 83 F8 ?? 75 ED}
        $opc3 = {0F B7 02 66 2D 71 0A 66 25 FF 00 66 89 02 48 83 C2 02 48 39 CA 75 E9}


condition:

        uint16(0) == 0x5A4D and (any of ($opc*))

}
```

MITRE ATT&CK TABLE

Discovery	Command and Control	Defense Evasion	Persistence	Credential Access	Reconnaissance
T1012 Query Registry	T1102 Web Service	T1036 Masquerading	T1047 Create or Modify Systems	T1055 Process Injection	T1566 Phishing
T1082 Information Discovery		T1564.001 Hidden Files and Directories			

MITIGATIONS

- Configure firewalls on your network to block incoming and outgoing connections from suspicious IP addresses. This can prevent RATs from establishing communication with command and control servers.
- Keep your operating system, applications, and security software up-to-date. Updates often include patches that fix vulnerabilities exploited by RATs.
- Install antivirus and anti-malware software. Perform regular scans to detect and remove any RAT infections.
- If not needed, disable remote desktop services. If needed, ensure strong passwords and proper authentication methods are in place.
- Unplug or disable devices such as webcams, microphones, or USB drives when not in use. RATs can abuse these devices for surveillance.
- Whenever possible, enable 2FA for all accounts, including email and cloud services. This can thwart unauthorized access.
- Monitor your system's running processes for any unusual or unfamiliar ones. Use task managers or specialized tools to detect suspicious activity.
- Ensure strong and unique passwords for all accounts. Avoid using easily guessable information.
- Be cautious of unsolicited emails, attachments, or links. RATs can often be delivered through phishing emails.
- Allow only approved applications to run on your system. This can prevent RATs from executing even if they manage to infiltrate.
- Regularly review and update your firewall rules to ensure they're effective against RATs and other malicious traffic.
- Keep an eye on system performance and behavior. Unexpected slowdowns, crashes, or unusual network activity could indicate a RAT.


infinitum IT
Power of integrated Security
Shadow0x
Miner RAT
www.infinitumit.com.tr
infinitumitlabs