

# Shadow0x

## Miner RAT

---

# CONTENTS

<b>Shadow Miner RAT and What You Need to Know .....</b>	<b>3</b>
<b>What is Shadow Miner RAT?.....</b>	<b>3</b>
<b>Infection Chain .....</b>	<b>4</b>
<b>Shadow0x Miner RAT Overview.....</b>	<b>4</b>
<b>Static Analysis .....</b>	<b>9</b>
<b>miner.exe Analysis .....</b>	<b>9</b>
<b>Dynamic Analysis .....</b>	<b>11</b>
<b>IOCs .....</b>	<b>15</b>
IPs : .....	15
DOMAINs:.....	15
HASHs:.....	15
<b>YARA RULE .....</b>	<b>16</b>
<b>MITRE ATT&amp;CK TABLE .....</b>	<b>17</b>
<b>MITIGATIONS .....</b>	<b>18</b>

# Shadow Miner RAT and What You Need to Know

## What is Shadow Miner RAT?

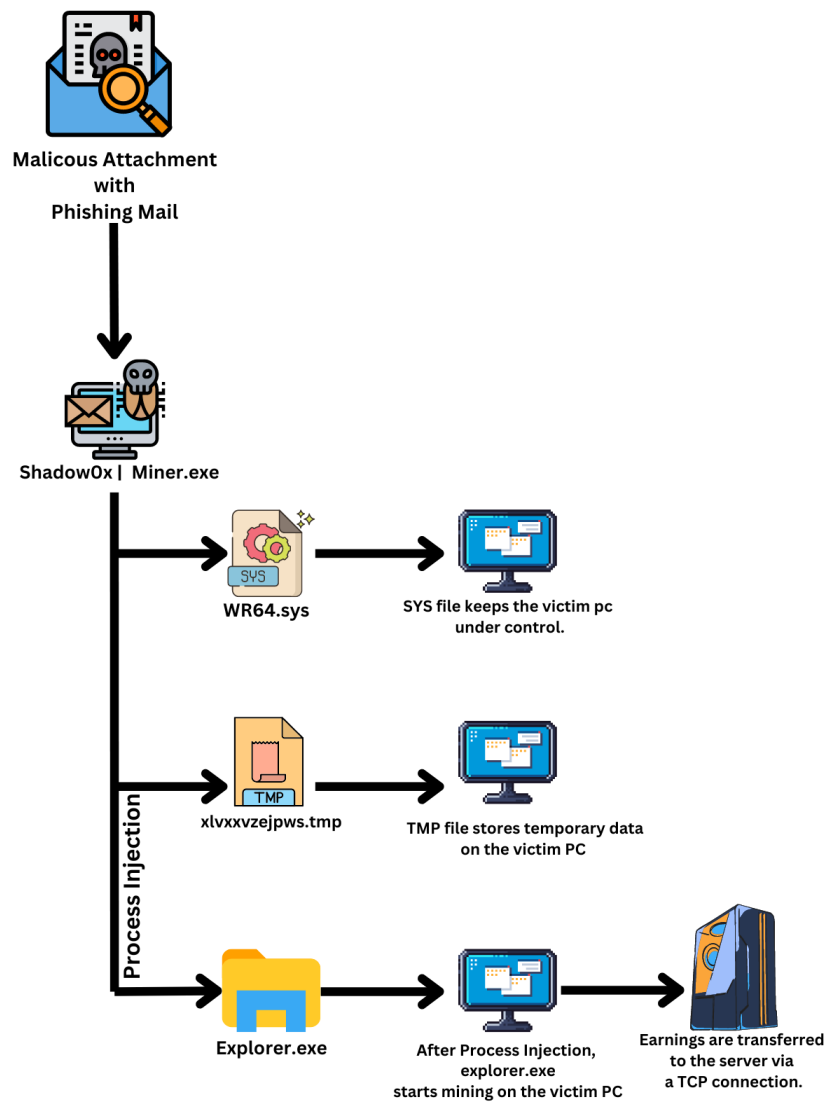
A Remote Access Trojan (RAT) constitutes a class of malicious software that affords an unauthorized infiltrator the capability to access a target computer or network. This form of software embeds itself surreptitiously within the targeted system, enabling the perpetrator to establish remote control,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

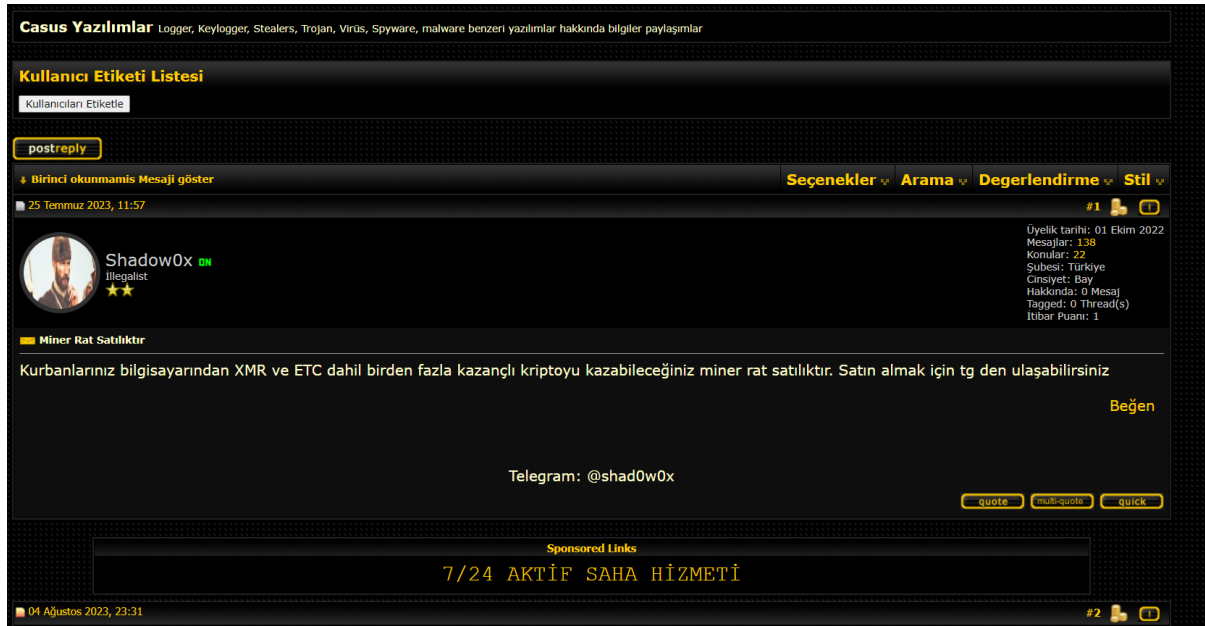


Figure 1- Dark Web forum info

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.



## Shadow0x Miner RAT

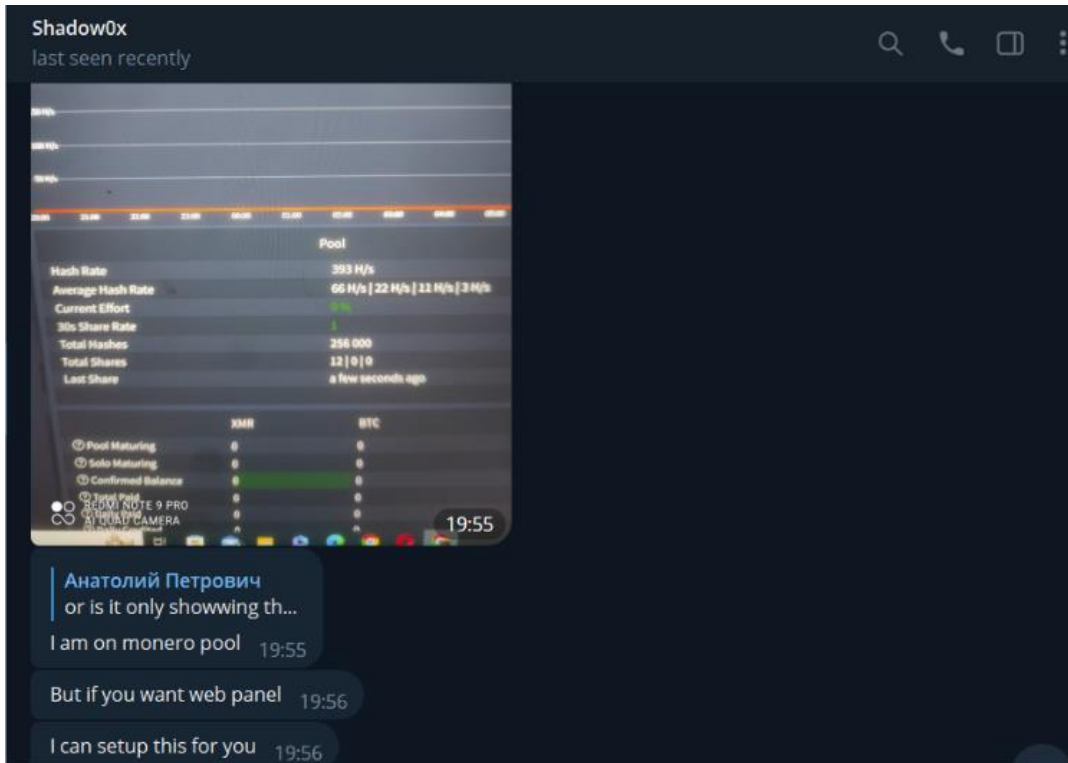


Figure 3- Web panel for bitcoin

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

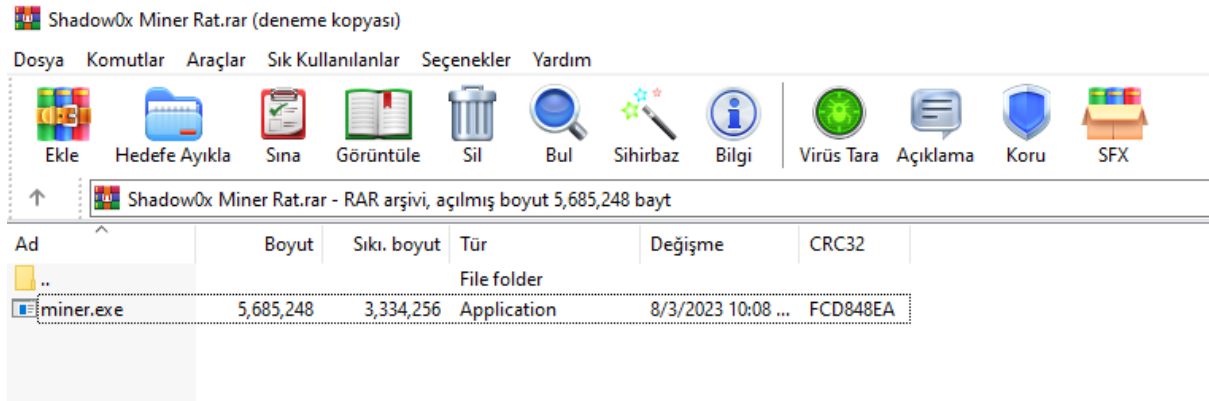


Figure 4- Information about file

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.

## Shadow0x Miner RAT

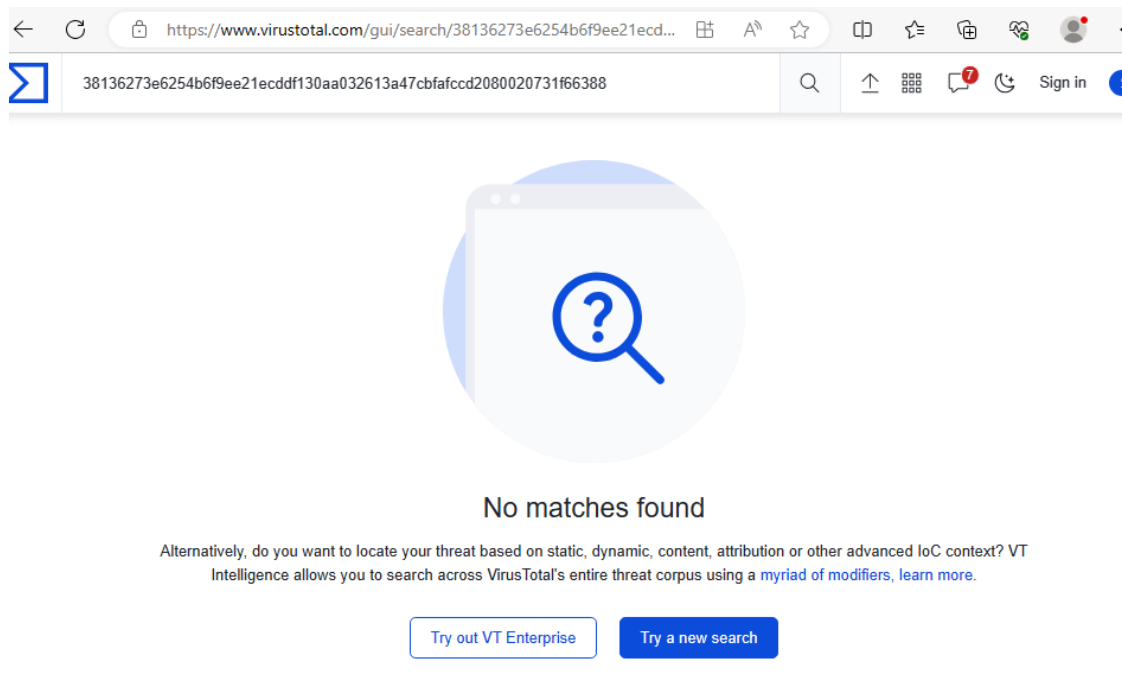


Figure 5- VirusTotal info

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

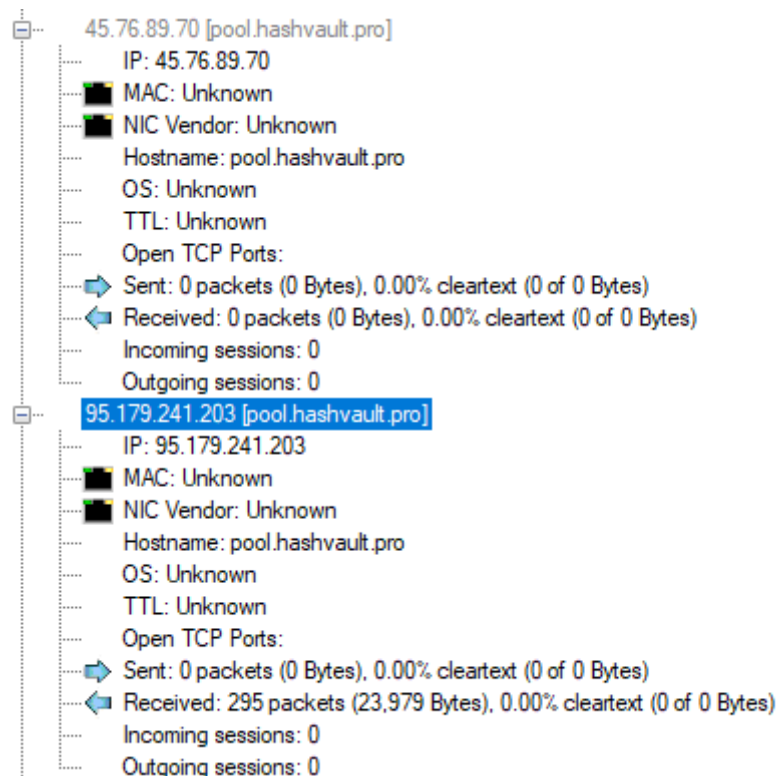


Figure 6- Network information

“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.

## Shadow0x Miner RAT

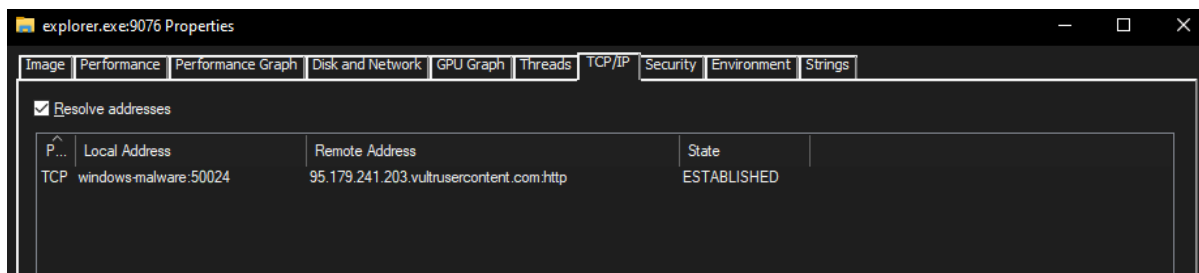


Figure 7- TCP connection

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.

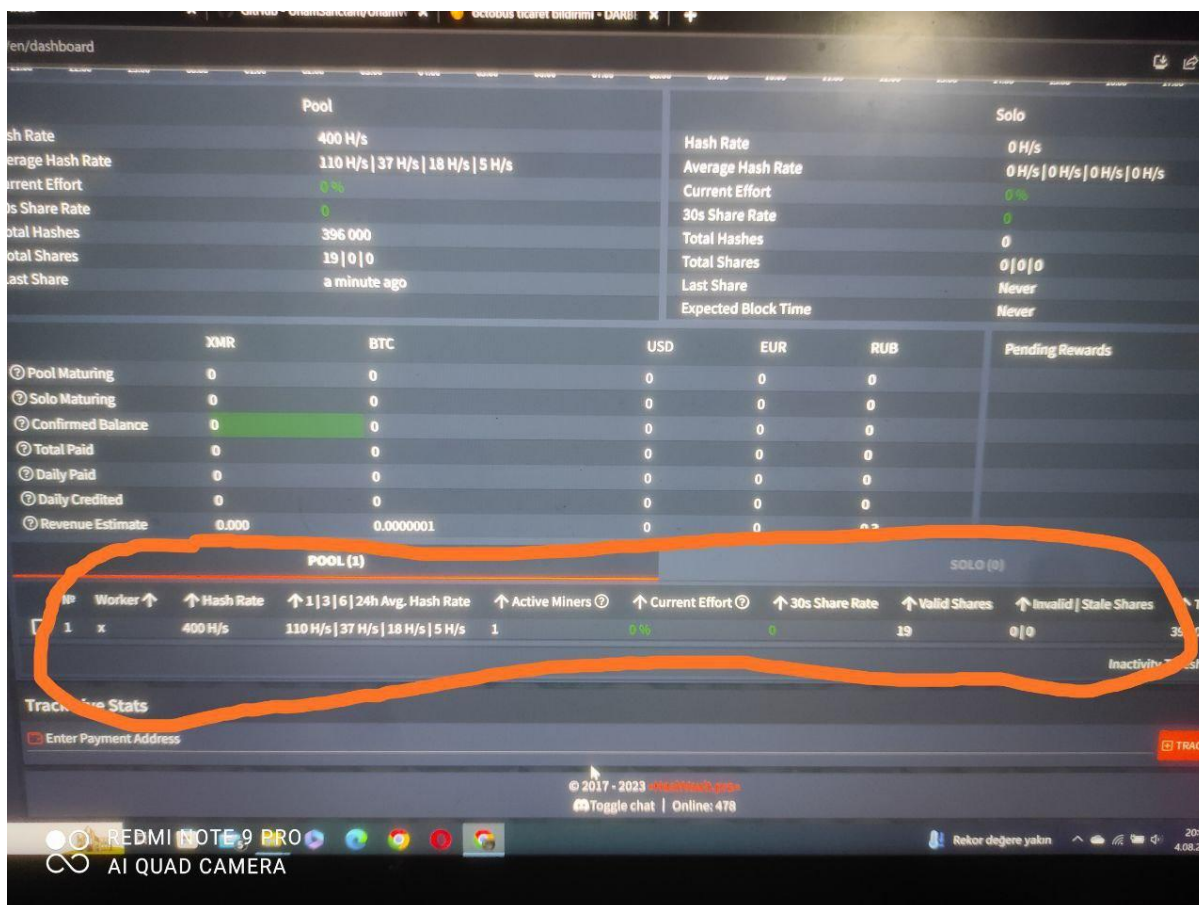


Figure 8- Hashvault pool of crypto information earned

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

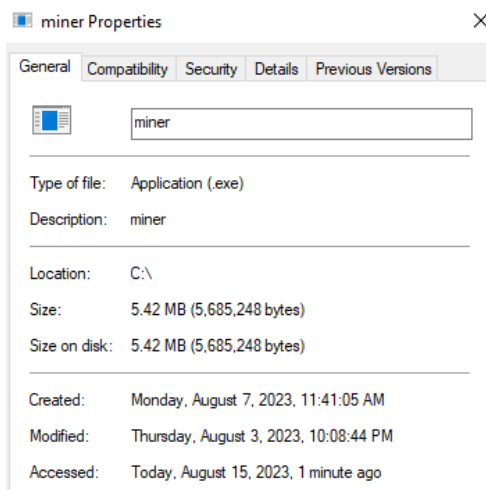


Figure 1- Information about malicious file

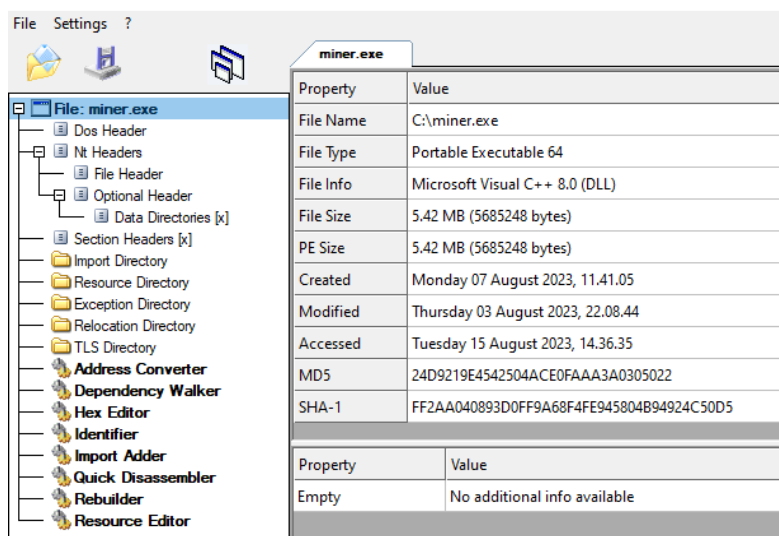


Figure 2- General Information

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

## Shadow0x Miner RAT

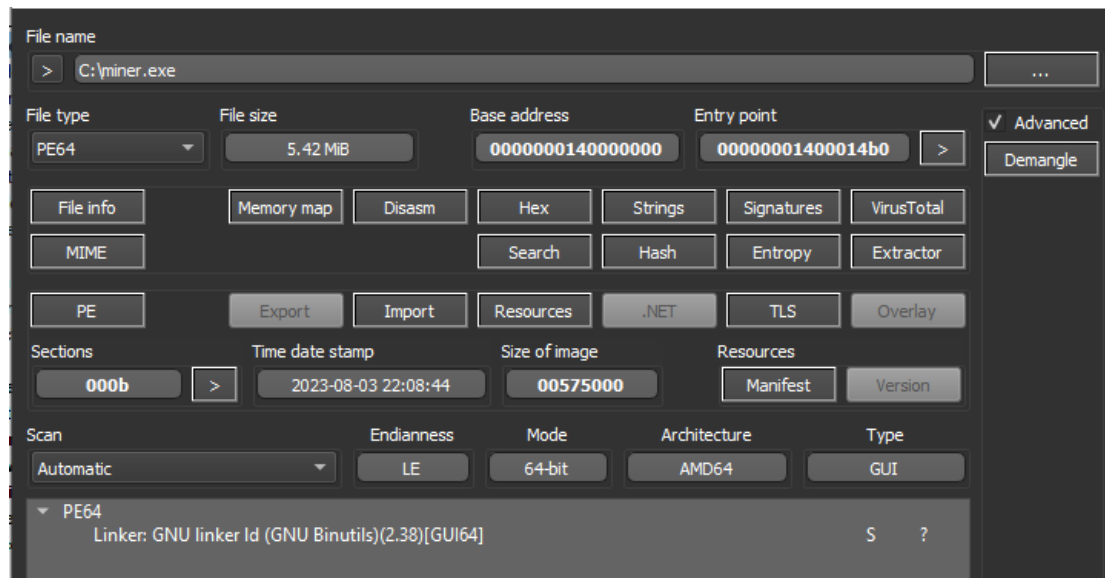


Figure 3- Executed malicious file

It was determined that no packaging technique was used.

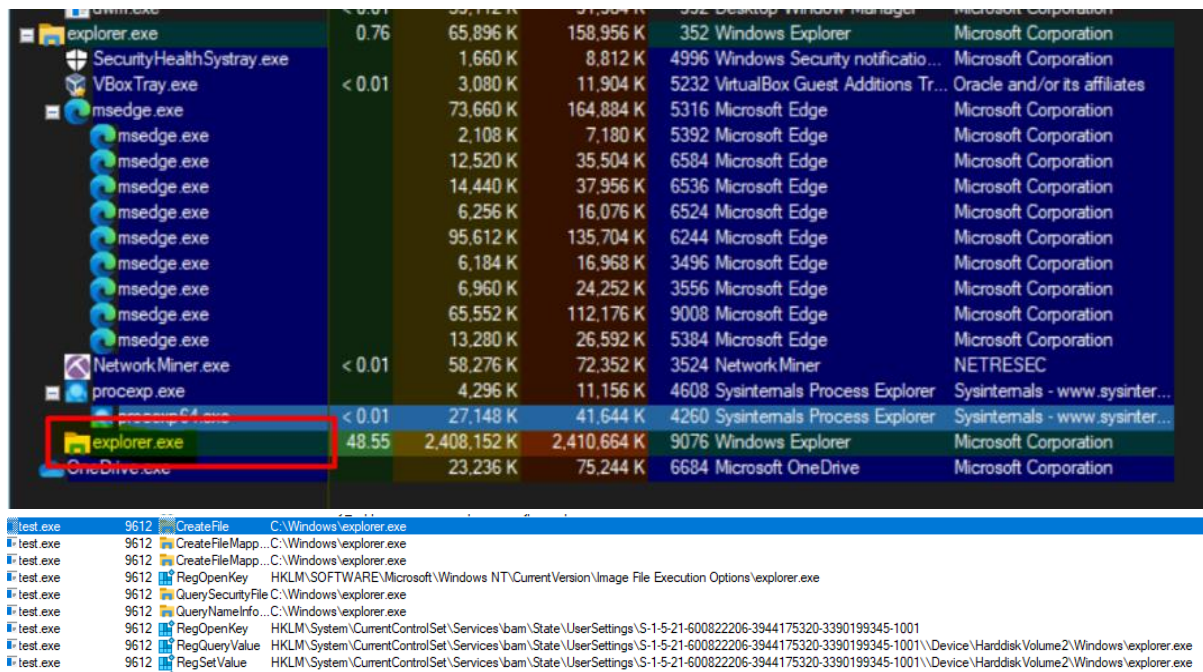


Figure 4- Executed malicious file

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

```

45:31C0 xor r8d,r8d
BA:02000000 mov edx,2
31C9 xor ecx,ecx
FFD0 call rax
E8:94D20000 call test.7FF743CFE4E0
48:8D0D 5DD60000 lea rcx,qword ptr ds:[7FF743CFE880]
FF15 C3F05600 call qword ptr ds:[K&SetUnhandledExceptionFilter>]
48:8B15 80895600 mov rdx,qword ptr ds:[7FF7442598E0]
48:8D0D 99FDFFFF lea rcx,qword ptr ds:[7FF743CF1000]
48:8902 mov qword ptr ds:[rdx],rax
E8:315B0100 call test.7FF743D06DA0
E8:ECCF0000 call test.7FF743CFE260
48:8B05 D5885600 mov rax,qword ptr ds:[7FF744259850]
48:8905 26E25600 mov qword ptr ds:[7FF74425F4A8],rax
E8:F95A0100 call test.7FF743D06D80
31C9 xor ecx,ecx

```

rax:&"C:\Users\...\Desktop\test.exe"

rax:&"C:\Users\...\Desktop\test.exe"

rax:&"C:\Users\...\Desktop\test.exe"

Figure 1- Gets location information

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

```

00007FF743CF4B11 83C6 01 add esi,1
00007FF743CF4B14 41:83C2 01 add r10d,1
00007FF743CF4B18 45:39EA cmp r10d,r13d
00007FF743CF4B1B 0F83 C8000000 jae test.7FF743CF4BEC
00007FF743CF4B21 81FE F3010000 cmp esi,1F3
00007FF743CF4B27 0F87 BF000000 ja test.7FF743CF4BEC
00007FF743CF4B2D 44:89D5 mov ebp,r10d
00007FF743CF4B30 41:8B0CAC mov ecx,dword ptr ds:[r12+rbp*4]
00007FF743CF4B34 4C:01D9 add rcx,r11
00007FF743CF4B37 44:8B4424 44 mov r8d,dword ptr ss:[rsp+44]
00007FF743CF4B3C 44:0FB709 movzx r9d,word ptr ds:[rcx]
00007FF743CF4B40 41:81C0 4825747C add r8d,7C742548
00007FF743CF4B47 45:39C1 cmp r9d,r8d
00007FF743CF4B4A 75 C8 jne test.7FF743CF4B14
00007FF743CF4B4C 8039 00 cmp byte ptr ds:[rcx],0
00007FF743CF4B4F 74 B8 je test.7FF743CF4B09
00007FF743CF4B51 41:89D1 mov r9d,edx
00007FF743CF4B54 41:8B 88 mov r8d,7C742548
00007FF743CF4B5A 8B 00000000 mov ebx,0
00007FF743CF4B5F 895424 2C mov dword ptr ss:[rsp+2C],edx
00007FF743CF4B63 0FB71419 movzx edx,word ptr ds:[rcx+rbx]
00007FF743CF4B67 44:89C3 mov ebx,r8d
00007FF743CF4B6A C1CB 08 ror ebx,8
00007FF743CF4B6D 01DA add edx,ebx
00007FF743CF4B6F 41:01D0 add r8d,edx
00007FF743CF4B72 41:83C1 01 add r9d,1
00007FF743CF4B76 44:89CB mov ebx,r9d
00007FF743CF4B79 803C19 00 cmp byte ptr ds:[rcx+rbx],0
00007FF743CF4B7D 75 E4 jne test.7FF743CF4B63
00007FF743CF4B7F 8B5424 2C mov edx,dword ptr ss:[rsp+2C]
00007FF743CF4B83 89F1 mov ecx,esi
00007FF743CF4B85 48:C1E1 03 shl rcx,3
00007FF743CF4B89 48:8D1D 94075600 lea rbx,qword ptr ds:[7FF744255324]
00007FF743CF4B90 4C:8D0C19 lea r9,qword ptr ds:[rcx+rbx]

```

rcx:"wcstoul"

rcx:"wcstoul"

rcx:"wcstoul"

rcx:"wcstoul"

rcx:"wcstoul"

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.

## Shadow0x Miner RAT

4	C74424 38 D8DA8883	mov dword ptr ss:[rsp+38],8388DAD8	
5	C74424 34 DCDA8883	mov dword ptr ss:[rsp+34],8388DADC	
6	E8 87FF743CF4980	call test.7FF743CF4980	
7	48:8840 18	mov rax,qword ptr ds:[rax+18]	
8	4C:8840 10	mov r8,qword ptr ds:[rax+10]	
9	49:8840 30	mov rax,qword ptr ds:[rax+30]	
10	48:85C0	test rax,rax	
11	0F84 9E010000	ja test.7FF743CF48FC	
12	B9 00000000	mov ecx,0	
13	E8 0C	jmp test.7FF743CF4A51	
14	4D:8800	mov r8,qword ptr ds:[r8]	
15	49:8840 30	mov rax,qword ptr ds:[r8+30]	
16	48:85C0	test rax,rax	
17	74 5C	je test.7FF743CF4A4F	

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.

00007FF743CF335E	56	push rsi	
00007FF743CF335F	53	push rbx	
00007FF743CF3360	48:83EC 28	sub rsp,28	
00007FF743CF3364	48:89C8	mov rbx,rcx	
00007FF743CF3367	4C:89C6	mov rsi,r8	
00007FF743CF336A	E8 91400100	call <JMP.&wcscpy>	
00007FF743CF336F	48:89F2	mov rdx,rsi	
00007FF743CF3372	48:89D9	mov rcx,rbx	
00007FF743CF3375	E8 7E400100	call <JMP.&wcscat>	
00007FF743CF337A	90	nop	
00007FF743CF337B	48:83C4 28	add rsp,28	
00007FF743CF337F	5B	pop rbx	
00007FF743CF3380	5E	pop rsi	
00007FF743CF3381	C3	ret	
00007FF743CF3382	41:57	push r15	
00007FF743CF3384	41:56	push r14	
00007FF743CF3386	41:55	push r13	
00007FF743CF3388	41:54	push r12	

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.

E8 A4190000	call test.7FF743CF4CF9	
89F0	mov eax,esi	
48:83C4 78	add rsp,78	
5B	pop rbx	
5E	pop rsi	
C3	ret	
56	push rsi	
53	push rbx	
48:83EC 28	sub rsp,28	
48:89CB	mov rbx,rcx	
4C:89C6	mov rsi,r8	
E8 91400100	call <JMP.&wcscpy>	
48:89F2	mov rdx,rsi	
48:89D9	mov rcx,rbx	
E8 7E400100	call <JMP.&wcscat>	
90	nop	
48:83C4 28	add rsp,28	
5B	pop rbx	
5E	pop rsi	
C3	ret	
41:57	push r15	
41:56	push r14	
41:55	push r13	
41:54	push r12	
55	push rbp	

ke:3355 #2755			
ip 3	Dump 4	Dump 5	Watch 1
30 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00	ASCII		
30 6C 00 75 00 63 00 79 00 5F 00 5C 00 41 00			
30 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00			
30 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00			
30 5C 00 78 00 6C 00 76 00 78 00 78 00 76 00			
30 65 00 6A 00 70 00 77 00 73 00 2E 00 74 00			
30 70 00 00 00 00 00 00 00 00 00 00 00 00			
30 00 00 00 00 00 00 00 00 00 00 00 00 00			

Figure 5- Creates xlxxvzejpws.tmp file

The miner creates a temp file named "xlxxvzejpws.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.

## Shadow0x Miner RAT

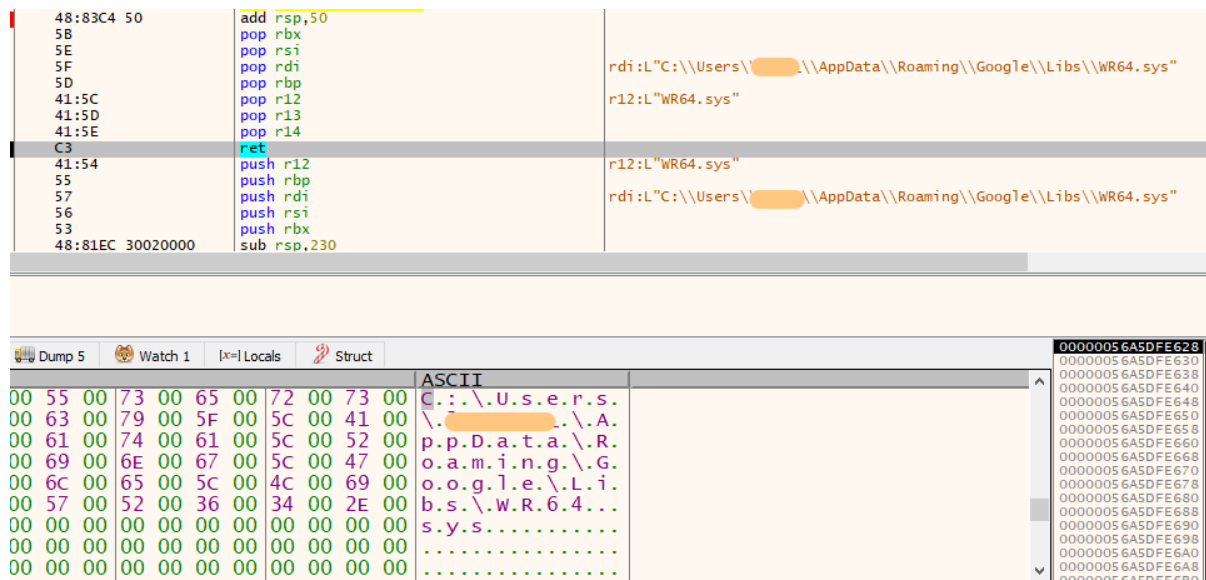


Figure 6- Creates malicious WR64.sys file

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.

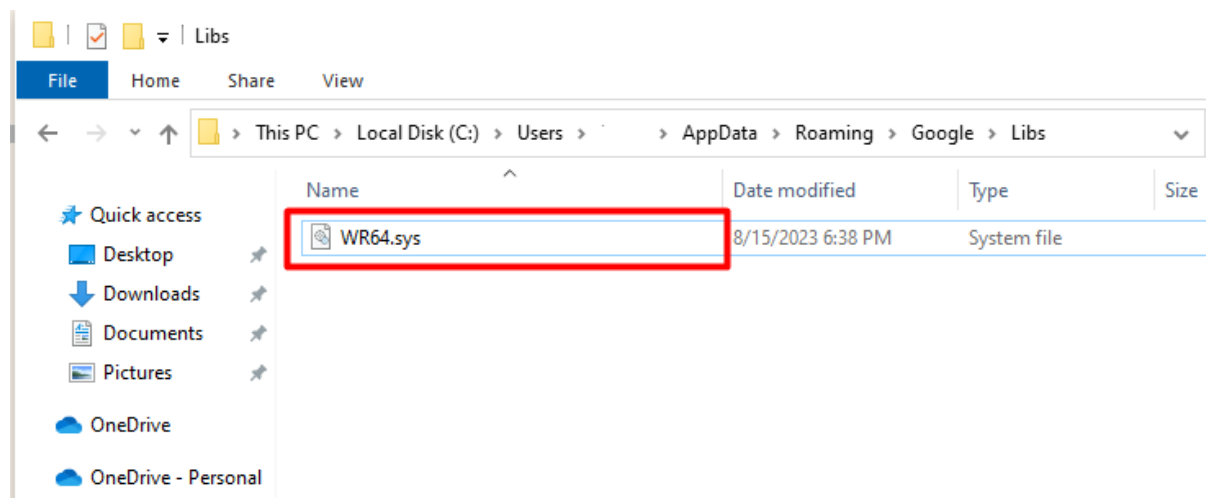


Figure 7- Created WR64.sys file

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



# Shadow0x Miner RAT

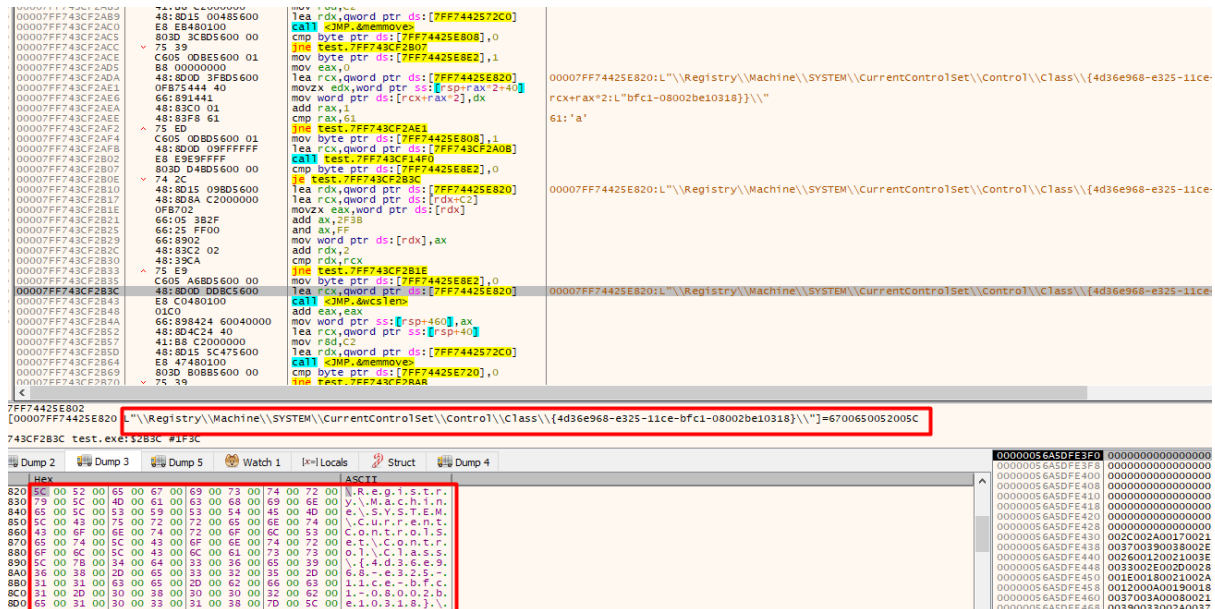


Figure 8- Using registry key

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.

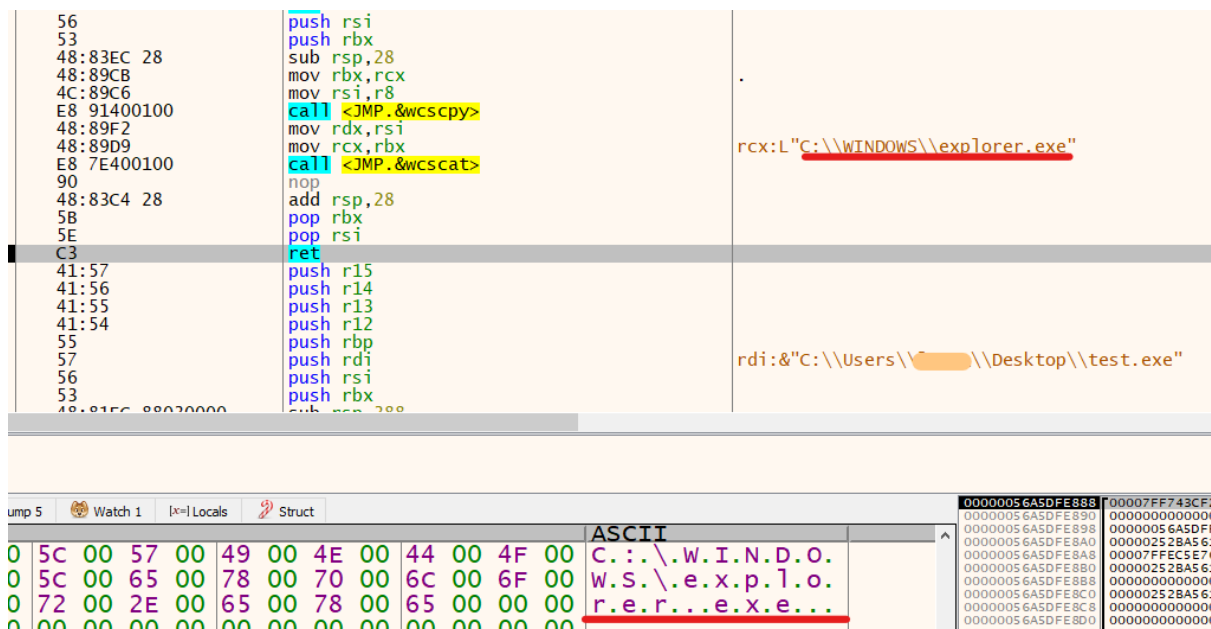


Figure 9- Creates explorer.exe

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	767bec990ffbacc2ff16d6ab929e5f72294e00dabcc5f39a9267648e70dda6f1d

## YARA RULE

```
import "hash"
rule Shadow0x
{
  meta:
    author = "Kerime Gencay"
    description = "Shadow0x Miner RAT Rule"
    file_name = "miner.exe"
    hash = "24d9219e4542504ace0faaa3a0305022"
  strings:
    $op1 = {E8 3F 5E 01 00 48 85 C0 0F 94 C0 0F B6 C0 F7 D8 48 83 C4 28}
    $op2 = {0F B7 54 44 70 66 89 14 41 48 83 C0 01 48 83 F8 ?? 75 ED}
    $op3 = {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 ($op*))
}
```

## 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.



# Shadow0x

## Miner RAT

---