

01010101010

Shadovox Miner RAT

f Ø in

www.infinitumit.com.tr

CONTENTS

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



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.

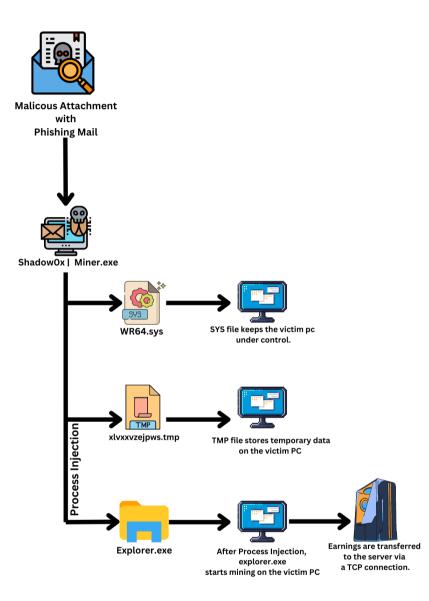
A Crypto Miner denotes a software variant that leverages the resources of a victim's computer to generate revenue through cryptocurrency. Adversaries may employ such software to pilfer the victim's computational power and mine cryptocurrencies through a process that appropriates the victim's resources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

Casus Yazılımlar Logger, Keylogger, Stealers, Trojan, Virüs, Spyware, malware benzeri yazılımlar hakkında bilgiler paylaşımlar			
Kullanıcı Etiketi Listesi			
Kullanıcıları Etiketle			
postreply			
↓ Birinci okunmamis Mesaji göster	Seçenekler 🗸	Arama 💀	Degerlendirme 🗸 Stil 🗸
25 Temmuz 2023, 11:57			#1 📙 🕕
Shadow0x IN Ilegalist			Üyelik tarihi: 01 Ekim 2022 Mesajlar: 138 Konular: 22 Şubesi: Türkiye Cinsiyet: Bay Hakkında: 0 Mesaj Tagged: 0 Thread(s) İtibar Puani: 1
🔤 Miner Rat Satılıktır			
Kurbanlarınız bilgisayarından XMR ve ETC dahil birden fazla kazançlı kriptoyu kazabileceğiniz miner rat	satılıktır. Satın a	lmak için t <u>ç</u>	ı den ulaşabilirsiniz
			Beğen
Telegram: @shad0w0x			
		C	quote (multi-quote) quick
Sponsored Links			
7/24 AKTIF SAHA HİZMETİ			
04 Ağustos 2023, 23:31			#2 📙 🔳

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								Q	e.	
last seen recently										
-										
	-		_							
		Pool								
Hash Rate		393 H/s								
Average Hash Rate Current Effort		66 H/s 22 H/s	118/6/38/							
30s Share Rate										
Total Hashes		256 000								
Total Shares Last Share		12 0 0 a few seconds ag								
			-							
	XMR	978								
C Pool Maturing		2								
Solo Maturing O Confirmed Balance		:								
CO ALUAD CAMERA			19:5	5						
aller the set										
Анатолий Петр	ович									
or is it only show										
l am on monero p	ool 19:55									
But if you want we	b panel	19:56								
I can setup this fo	r you 19:9	56								

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.

osya Komutlar A	raçlar 🛛 Sık Kull	anılanlar Seç	enekler Yardım			
				1		0
Ekle Hedefe Ay		Görüntüle - RAR arşivi, a	Sil Bul çılmış boyut 5,685	Sihirbaz Bilgi ,248 bayt	Virüs Tara Açıklama	Koru SFX
Ad ^	Boyut	Sıkı. boyut	Tür	Değişme	CRC32	
			File folder			
ininer.exe	5 685 248	3.334.256	Application	8/3/2023 10:08	. FCD848EA	

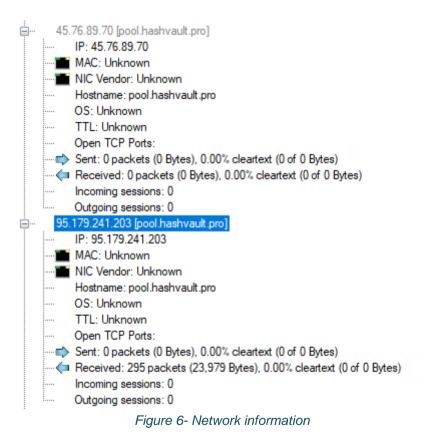
Figure 4- Information about file

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.



\leftarrow	C	θI	http	os://w	ww.v	irusto	tal.com	n/gui/s	search	h/3813	36273e	6254b6f	f9ee21	ecd	₿	Aø	☆		C)	€≣	Ē	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~		
Σ	3813627	273e6	6254	b6f9e	e21e	cddf13	30aa032	2613a4	47cbfa	afccd2	2080020	731f663	88				C	ζ	\pm		Ç 0	Ċ	Sign in	4
												C	?											
											No r	natch	hes	four	nd									
		A	Alter		-	-			-			on static, otal's ent	-									xt? VT		
									Тг	ry out	VT Ente	erprise		Try a	new se	earch								
									Fig	ure	5- V	′irusT	otal	info	2									

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



"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.



🛤 explorer.exe:9076 Properties			_	□ ×
Image Performance Performance Graph	Disk and Network GPU Graph Threads TCP/IP Secur	ity Environment Strings		
<mark>✓ <u>R</u>esolve addresses</mark>				
P Local Address	Remote Address	State		
TCP windows-malware:50024	95.179.241.203.vultrusercontent.com.http	ESTABLISHED		

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.

/dashboard								
			u.cu cu.cu cu.cu					6
		Pool					Solo	
Rate		400 H/s		H	ash Rate		0 H/s	
age Hash Rate		110 H/s 37 H/s 18 H/s 1	5 H/s		verage Hash Rate		0 H/s 0 H/s 0 H/s	1011/-
ent Effort					urrent Effort		000/3 [0 11/5] 0 11/5	sjun/s
Share Rate				30	s Share Rate			
ll Hashes		396 000		To	tal Hashes		0	
al Shares		19 0 0		To	tal Shares		01010	
t Share		a minute ago			st Share		Never	
				Ex	pected Block Time		Never	
	XMR	BTC			EUR	RUB	Pending Rewards	
Pool Maturing						0		
) Solo Maturing						0		
) Confirmed Balance								
D Total Paid								
② Daily Paid								
② Daily Credited								
② Revenue Estimate	0.000	0.0000001						
		POOL (1)					DLO (0)	
Nº Worker 1	1 Hash Rate	↑1 3 6 24h Avg. Hash Rate	↑ Active Miners ⑦	↑ Current	Effort ⑦ 个 30s S	ihare Rate 🔺 Valid S	hares 🏫 Invalid Stale S	ihares
V 1 x	400 H/s	110 H/s 37 H/s 18 H/s 5 H/s				19	010	3
								activity
Track Tre Stats								
Enter Payment Addres	5							
			-	-				
			© 2017 - @Togg	2023 - Continue de Continue de Continue de Continue de Continue de Continue de Continue de Continue de Continue Le chat Onli	ne: 478			
O O REDMI		RO 💿 💿 🧑 👩	3			81 R	ekor değere yakın 🛛 👄 🎢	e 🛥 🕁 💡
	D CAMER	٨						

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

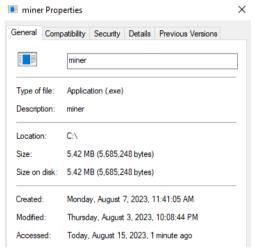


Figure 1- Information about malicious file

File Settings ?						
الل 💫	miner.exe					
	Property	Value	2			
File: miner.exe Jos Header	File Name	C:\m	iner.exe			
- I I Nt Headers	File Type	Porta	ble Executable 64			
II File Header	File Info	Micr	osoft Visual C++ 8.0 (DLL)			
Optional Header Interference [x]	File Size	5.42	MB (5685248 bytes)			
Section Headers [x]	PE Size	5.42 MB (5685248 bytes)				
Import Directory Directory Directory	Created	Monday 07 August 2023, 11.41.05				
Exception Directory	Modified	Thursday 03 August 2023, 22.08.44 Tuesday 15 August 2023, 14.36.35				
Contraction Directory Contractory Contractory	Accessed					
- Madress Converter	MD5	24D9	219E4542504ACE0FAAA3A0305022			
	SHA-1	FF2A	A040893D0FF9A68F4FE945804B94924C50D5			
- Mildentifier						
	Property		Value			
	Empty		No additional info available			
- SResource Editor						



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



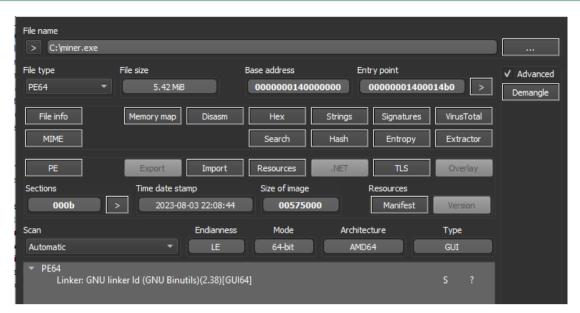


Figure 3- Executed malicious file

It was determined that no packaging technique was used.

	INIT.GAG	0.01	00,112 K	31,304 10	USE Dealtop Million Manager	microsoft corporation
= explo	orer.exe	0.76	65,896 K	158,956 K	352 Windows Explorer	Microsoft Corporation
÷ 5	SecurityHealthSystray.exe		1,660 K	8,812 K	4996 Windows Security notificatio	Microsoft Corporation
1 N	/BoxTray.exe	< 0.01	3.080 K	11,904 K	5232 VirtualBox Guest Additions Tr	Oracle and/or its affiliates
= 🧖 n	nsedge.exe		73,660 K	164.884 K	5316 Microsoft Edge	Microsoft Corporation
	msedae.exe		2.108 K	7,180 K	5392 Microsoft Edge	Microsoft Corporation
	msedge.exe		12.520 K	35.504 K	6584 Microsoft Edge	Microsoft Corporation
	msedge.exe		14,440 K	37.956 K	6536 Microsoft Edge	Microsoft Corporation
	msedge.exe		6.256 K	16.076 K	6524 Microsoft Edge	Microsoft Corporation
	msedge.exe		95.612 K	135,704 K	6244 Microsoft Edge	Microsoft Corporation
	msedge.exe		6.184 K	16.968 K	3496 Microsoft Edge	Microsoft Corporation
				24,252 K		
	msedge.exe		6,960 K	and the second se	3556 Microsoft Edge	Microsoft Corporation
	msedge.exe		65,552 K	112,176 K	9008 Microsoft Edge	Microsoft Corporation
	msedge.exe		13,280 K	26,592 K	5384 Microsoft Edge	Microsoft Corporation
	Network Miner.exe	< 0.01	58,276 K	72,352 K	3524 Network Miner	NETRESEC
🗖 🧾 P	rocexp.exe		4,296 K	11,156 K	4608 Sysinternals Process Explorer	Sysintemals - www.sysinter
	procesup 64 outo	< 0.01	27,148 K	41,644 K	4260 Sysinternals Process Explorer	Sysintemals - www.sysinter
- e	xplorer.exe	48.55	2,408,152 K	2,410,664 K	9076 Windows Explorer	Microsoft Corporation
Circ	Dilve.exe	-	23,236 K	75,244 K	6684 Microsoft OneDrive	Microsoft Corporation
est.exe		ows\explorer.exe		·		
est.exe est.exe	9612 🐂 CreateFileMappC:\Wind 9612 📷 CreateFileMappC:\Wind					
est.exe est.exe			osoft\Windows NT\Curr	rentVersion\Image File F	Execution Options\explorer.exe	
est exe	9612 RuerySecurityFile C:\Windo			childen anage hie i		
est.exe	9612 Tel QueryNameInfoC:\Windo	ows\explorer.exe				
	Soliz addition of the second		1.10.000 1.01.00	State\LleerSettinge\S-1	-5-21-600822206-3944175320-3390199345-1001	
est.exe est.exe	9612 RegOpenKey HKLM\S					
est.exe est.exe est.exe est.exe est.exe	9612 📫 RegÓpenKey HKLM\S 9612 🎬 RegQueryValue HKLM\S	ystem\CurrentCo	ntrolSet\Services\bam\	State\UserSettings\S-1	-5-21-600822206-3944175320-3390199345-1001\\De -5-21-600822206-3944175320-3390199345-1001\\De	

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

ints	Memory Map	🗐 Call Stack	SEH	Script	🐏 Symbols	<> Source	P	References	🛸 Threads	晶 Handles	🐔 Trace
	45:31C0	xor r80	l,r8d								
	BA 02000000	mov ed>	.2								
	31C9	xor ec	ecx								
	FFD0	call ra	1x								
	E8 94D20000	call te	st.7FF743	3CFE4E0							
	48:8D0D 5DD60000	lea rc	.gword pt	tr ds:[7FF7	43CFE8B0]						
	FF15 C3F05600	call qu	word ptr d	ds:[<&SetUn	handledExce	ptionFilter>	1				
	48:8B15 80895600	mov rd	, gword pt	tr ds:[7FF7	44259BE0]		-				
	48:8D0D 99FDFFFF	lea rc	, gword pt	tr ds:[7FF7	43CF1000]						
	48:8902	mov qwo	ord ptr ds	s:[rdx],rax	. –			rax:&"\"C	:\\Users\\1	\\Desktop	\\test.exe\"
	E8 315B0100	call te	st.7FF743	3D06DA0							
	E8 ECCF0000	call te	st.7FF743	3CFE260							
	48:8B05 D5885600	mov rax	, gword pt	tr ds:[7FF7	44259B50			rax:&"\"C	:\\Users\\	\\Desktop	\\test.exe\"
	48:8905 26E25600	mov qwo	ord ptr de	s:[7FF74425	F4A8],rax			rax:&"∖`"C	:\\Users\\	Desktop	\\\test.exe\'''
	E8 F95A0100	call te	st.7FF743	3D 0 6D 80	- /						
	3109	xor eco	.ecx								

Figure 1- Gets location information

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

00007FF743CF4811 00007FF743CF4818 00007FF743CF4818 00007FF743CF4821 00007FF743CF4821 00007FF743CF4821 00007FF743CF4820 00007FF743CF4834 00007FF743CF4834 00007FF743CF4834 00007FF743CF4834 00007FF743CF48454 00007FF743CF4859 00007FF743CF4879 00007FF743CF4879 00007FF743CF4879 00007FF743CF4879 00007FF743CF4879 00007FF743CF4875 00007FF743CF4874 00007FF743	83C6 01 41:83C2 01 45:39EA • 0F83 C8000000 81FE F3010000 • 0F87 BF000000 44:89D5 41:8B0CAC 4C:0D9 44:884424 44 44:0F8709 41:81C0 4825747C 45:39C1 • 75 C8 8039 00 • 74 B8 41:89D1 41:89D1 41:89D1 41:89D1 41:89D1 41:89C3 C1CB 08 01DA 41:01D0 41:83C1 01 44:89C8 803C19 00 • 75 E4 805C19 • 75 E4 805C19 • 75 E4 805C19 • 75 E4 805C19 • 75 E4 • 805C19 • 75 E4 • 7	<pre>add esi,1 add r10d,1 cmp r10d,r13d jae test.7FF743CF48EC cmp esi,1F3 ja test.7FF743CF48EC mov eby,r10d mov ecx,dword ptr ds:[r12+rbp*4] add rcx,r11 movz r8d,dword ptr ds:[rcx] add r8d,7C742548 cmp r9d,r8d jme test.7FF743CF48L4 cmp byte ptr ds:[rcx],0 je test.7FF743CF48L9 mov r8d,edx mov r9d,edx mov r9d,edx mov r9d,edx mov ebx,0 mov dword ptr ss:[rsp+2C],edx movz&,r8d add edx,ebx add r8d,edx add r9d,1 mov ebx,r9d cmp byte ptr ds:[rcx+rbx],0 jme test.7FF743CF48B8 mov ecx,esi sh1 rcx,3 lea rbx,qword ptr ds:[7FF744255324] lea r5.0word ptr ds:[rcx+rbx]</pre>	<pre>rcx: "wcstoul" rcx: "wcstoul" rcx: "wcstoul" </pre>
CF4B72 test.exe:\$4B72 #3F72		[x=] Locals 🌮 Struct	
Hex			
73 73 61 67 65 41 74 74 72 73 60 73 73 61 67 65 41 74 72 73 60 73 73 61 67 65 74 40 65 73 60 70 62 64 65 74 60 70 62 64 64 67 65 74 40 65 73 73 61 67 65 74 47 72 66 67 43 67 66 67 63 46 63 46 63 45 67 63 49 66 67 47 47 69 61 62 63 67 65 41 74 72 69 61 62 63 67 65 41 74 72 69 61 62 67 65 40 61 74 63 61 62<	69 62 75 74 65 00 41 ss 73 61 67 65 46 72 6F 1P 66 62 62 63 74 00 mC 74 73 74 61 65 64 69 A1 69 65 64 64 69 A1 65 46 73 74 ng 75 66 74 00 41 6C 70 81 74 65 40 65 73 73 161 17 75 66 74 00 41 6C 70 83 74 65 00 41 6C 70 63 96	ageAttribute.A CGetMessageFro ompletionList. pcGetOutstandi CompletionList ssageCount.Alp nitializeMessa Attribute.Alpc	

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.



4	C74424 38 D8DA8B83	mov dword ptr ss: rsp+38,838BDAD8	
	C74424 34 DCDA8B83	mov dword ptr ss: rsp+34,838BDADC	
	E8 87FFFFFF	call test.7FF743CF49B0	
9	48:8B40 18	mov rax, gword ptr ds: [rax+18]	
	4C:8B40 10	mov r8, gword ptr ds:[rax+10]	r8:&"ALLUSERSPROFILE=C:\\ProgramData"
L	49:8B40 30	mov rax, gword ptr ds: [r8+30]	[r8+30]:"ComSpec=C:\\WINDOWS\\system32\\cmd.exe"
5	48:85C0	test rax,rax	
3	 OF84 BE010000 	je test.7FF743CF4BFC	
1	B9 00000000	mov ecx.0	
3	EB 0C	jmp test.7FF743CF4A51	
5	4D:8B00	mov r8,qword ptr ds:[r8]	r8:&"ALLUSERSPROFILE=C:\\ProgramData", [r8]:"ALLUSERSPROFILE=C:\\ProgramData"
3	49:8B40 30	mov rax, qword ptr ds: [r8+30]	[r8+30]:"ComSpec=C:\\WINDOWS\\system32\\cmd.exe"
2	48:85C0	test rax,rax	
-	✓ 74 5C	ie test.7EE743CE4AAD	

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	rbx:L"=::=::\\"
00007FF743CF3360	48:83EC 28	sub rsp,28	
00007FF743CF3364	48:89CB	mov rbx,rcx	<pre>rbx:L"=::=::\\", rcx:L"C:\\WINDOWS\\System32\\conhost.exe"</pre>
00007FF743CF3367	4C:89C6	mov rsi,r8	
00007FF743CF336A	E8 91400100	call <jmp.&wcscpy></jmp.&wcscpy>	
00007FF743CF336F	48:89F2	mov rdx,rsi	
00007FF743CF3372	48:89D9	mov rcx,rbx	<pre>rcx:L"C:\\WINDOWS\\System32\\conhost.exe", rbx:L"=::=::\\"</pre>
00007FF743CF3375	E8 7E400100	call <jmp.&wcscat></jmp.&wcscat>	
00007FF743CF337A	90	nop	
00007FF743CF337B	48:83C4 28	add rsp,28	
00007FF743CF337F	5B	pop rbx	rbx:L"=::=::\\"
00007FF743CF3380	5 E	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	
I		and the second sec	

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	rbx:L"=::=::\\"
5E	pop rsi	
C3	ret	
56	push rsi	
53	push rbx	rbx:L"=::=::\\"
48:83EC 28	sub rsp,28	
48:89CB	mov rbx,rcx	
4c:89c6	mov rsi.r8	
E8 91400100	call <jmp.&wcscpy></jmp.&wcscpy>	
48:89F2	mov rdx,rsi	
48:89D9	mov rcx, rbx	<pre>rcx:L"C:\\Users\\\AppData\\Local\\Temp\\xlvxxvzejpws.tmp", rbx:L"=::=::\\</pre>
E8 7E400100	call <jmp.&wcscat></jmp.&wcscat>	
90	nop	
48:83C4 28	add rsp,28	
5B	pop rbx	rbx:L"=::=::\\"
5E	pop rsi	
C3	ret	
41:57	push r15	
41:56	push r14	
41:55	push r13	
41:54	push r12	
55	push rbp	
<		
xe:\$3355 #2755		
np 3 💷 Dump 4 💷 Dump 5 🥘	Watch 1 [x= Locals 2 Struct	00000056A5PE883 00007FF743CF2130 return to tes: 00000056A5PE859 0000000000
	ASCII	I 0000005 6A5DFE898 0000005 6A5DFFA18 0000005 6A5DFE898 0000005 6A5DFFA18 0000005 6A5DFE898 00000025 2BA5 61B70 & "ALLUSER SPROI
00 3A 00 5C 00 55 00 7	3 00 65 00 72 00 73 00 C.:.	U.s.e.r.s. 0000005 GASDFEBA8 00007FFEC5E76850 ntdl1.00007FF
	9 00 5F 00 5C 00 41 00 🔨 🧰	A. 0000005 6A50FE880 000002528A5 61510 0000005 6A50FE880 000000000000000000000000000000000
00 70 00 44 00 61 00 7	4 00 61 00 5C 00 4C 00 p.p.C	D.a.t.a.\.L. 00000056A5DFE8C0 00000252BA561510
00 63 00 61 00 6C 00 5	C 00 54 00 65 00 6D 00 0.c.a	a.l.\.T.e.m. 00000056450FE8C8 00000000000000000000000000000000000
00 5C 00 78 00 6C 00 7	6 00 78 00 78 00 76 00 p.\.>	x.1.v.x.x.v. 0000005 GASD FEBD 00000252BAS 61510
00 65 00 6A 00 70 00 7	7 00 73 00 2E 00 74 00 z.e.j	j.p.w.st. 00000056450FE8E0 000000000000000000000000000000000
	0 00 00 00 00 00 00 00 m.p	0000005 6A5DFE8F0 00000000000028 0000005 6A5DFE8F8 00000000000003
0 00 00 00 00 00 00 00 00	0 00 00 00 00 00 00 00 00 00 00	0000005 6A5DFE3F0 0000000000000000000000000000000000
	Figure	5- Creates xlvxxvzejpws.tmp file
	TIQUIE	

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.



48:83C4 50 58 55 55 41:50 41:55 41:55	add rsp,50 pop rbx pop rsi pop rdi pop rdp pop rl2 pop rl3 pop rl4	rdi:L"C:\\Users\\\\AppData\\Roaming\\Goog]e\\Libs\\WR64.sys" r12:L"WR64.sys"
C3 41:54 55 57 56 53 48:81EC 30020000	ret push r12 push r12 push rdi push rsi push rsi sub rsp.230	r12:L"WR64.sys" rdi:L"C:\\Users\\\\AppData\\Roaming\\Google\\Libs\\WR64.sys"
🕮 Dump 5 🛛 🛞 Watch 1	x=l Locals 🛛 🖉 Struct	00000056A5DFE628 00000056A5DFE628
00 63 00 79 00 5F 00 61 00 74 00 61 00 69 00 6E 00 67 00 6C 00 65 00 5C 00 57 00 52 00 36 00 00 00 00 00 00	00 5C 00 52 00 p.p.D.a.t.a.\.	A. 0000005 6A5DFE650 0000005 6A5DFE650 0000005 6A5DFE660 0000005 6A5DFE660 0000005 6A5DFE660 0000005 6A5DFE670 000005 6A5DFE670 0000005 6A5DFE678 0000005 6A5DFE688 0000005 6A5DFE688 0000005 6A5DFE688 0000005 6A5DFE688 000005 6A5DFE688 000005 6A5DFE688 000005 6A5DFE688 000005 6A5DFE68 000005 6A5DFE68 000005 6A5DFE68 000005 6A5DFE68 000005 6A5DFE68 000005 6A5DFE68 000005 6A5DFE67 00005 6A5DFE67 00005 6A5DFE67 000005 6A5DFE67 0000005 6A5DFE67 000000005 6A5DFE67 00000005 6A5DFE600000000000000000

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.

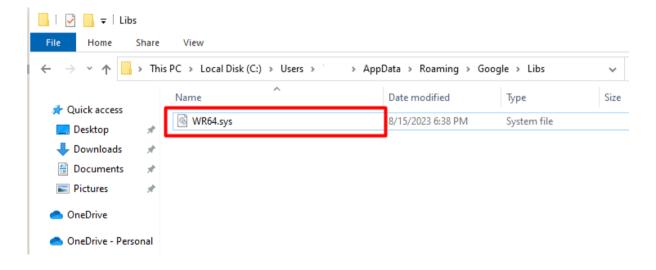


Figure 7- Created WR64.sys file

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



1000011173012000	1.00 02000000	100 100,02		
00007FF743CF2AB9	48:8D15 00485600	lea rdx, gword ptr ds: [7FF7442572C0]		
00007FF743CF2AC0	E8 EB480100	call <jmp.&memmove></jmp.&memmove>		
00007FF743CF2AC5	803D 3CBD5600 00	cmp byte ptr ds:[7FF74425E808],0		
00007FF743CF2ACC	75 39	jne test.7FF743CF2B07		
00007FF743CF2ACE	C605 0DBE5600 01	mov byte ptr ds:[7FF74425E8E2],1		
00007FF743CF2AD5	B8 00000000	mov eax,0		
00007FF743CF2ADA	48:8D0D 3FBD5600	lea rcx, qword ptr ds: [7FF74425E820]	00007FF74425E820:L"\\Registry\\Machine\\SYSTEM\\CurrentControlSet\\Control	\\Class\\{4d36e968-e325-11Ce-
00007FF743CF2AE1 00007FF743CF2AE6	0FB75444 40 66:891441	movzx edx,word ptr ss:[rsp+rax*2+40] mov word ptr ds:[rcx+rax*2].dx	rcx+rax*2:L"bfc1-08002be10318}}\\"	
00007FF743CF2AE6	48:83C0 01	add rax,1	rextrax-2:E bici=08002bel0318}}\\	
00007FF743CF2AEE	48:83F8 61	cmp rax.61	61: 'a'	
00007FF743CF2AF2	∧ 75 ED	jne test.7FF743CF2AE1		
00007FF743CF2AF4	C605 0DBD5600 01	mov byte ptr ds: [7FF74425E808],1		
00007FF743CF2AFB	48:8DOD 09FFFFFF	lea rcx, gword ptr ds: [7FF743CF2A0B]		
00007FF743CF2B02	E8 E9E9FFFF	call test.7FF743CF14F0		
00007FF743CF2B07	803D D4BD5600 00	<pre>cmp byte ptr ds:[7FF74425E8E2],0</pre>		
00007FF743CF2B0E	 74 2C 74 2C 	je test.7FF743CF2B3C		
00007FF743CF2B10 00007FF743CF2B17	48:8D15 09BD5600 48:8D8A C2000000	lea rdx, qword ptr ds: [7FF74425E820]	00007FF74425E820:L"\\Registry\\Machine\\SYSTEM\\CurrentControlSet\\Control	//01822//{40366368-6322-1106-
00007FF743CF2B1E	0FB702	<pre>lea rcx,qword ptr ds:[rdx+C2] movzx eax,word ptr ds:[rdx]</pre>		
00007FF743CF2B12	66:05 3B2F	add ax.2F3B		
00007FF743CF2B25	66:25 FF00	and ax, FF		
00007FF743CF2B29	66:8902	mov word ptr ds:[rdx].ax		
00007FF743CF2B2C	48:83C2 02	add rdx,2		
00007FF743CF2B30	48:39CA	cmp rdx,rcx		
00007FF743CF2B33	^ 75 E9	jne test.7FF743CF2B1E		
00007FF743CF2B35	C605 A68D5600 00 48:8D0D DD8C5600	mov byte ptr ds:[7FF74425E8E2],0		
00007FF743CF2B3C 00007FF743CF2B43	E8 C0480100	<pre>lea rcx,qword ptr ds:[7FF74425E820] call <jmp.&wcslen></jmp.&wcslen></pre>	00007FF74425E820:L"\\Registry\\Machine\\SYSTEM\\CurrentControlSet\\Control	//стазу//{+0366968-6325-1166
00007FF743CF2B48	0100	add eax.eax		
00007FF743CF2B4A	66:898424 60040000	mov word ptr ss:[rsp+460],ax		
00007FF743CF2B52	48:8D4C24 40	lea rcx, gword ptr ss: rsp+40		
00007FF743CF2B57	41:B8 C2000000	mov r8d,C2		
00007FF743CF2B5D	48:8D15 5C475600	<pre>lea rdx,qword ptr ds:[7FF7442572C0]</pre>		
00007FF743CF2B64	E8 47480100	call <jmp.&memmove></jmp.&memmove>		
00007FF743CF2B69 00007FF743CF2B70	803D B0BB5600 00 75 39	<pre>cmp byte ptr ds:[7FF74425E720],0 ine test.7EF743CE2BAB</pre>		
00007EE743CE28701	× 75 39	THE TEST. /EE/43CE/BAB	1	
7FF74425E802				
[00007FF74425E820	L"\\Registry\\Machine\\S	YSTEM\\CurrentContro1Set\\Contro1\\Class	\\{4d36e968-e325-11ce-bfc1-08002be10318}\\"]=6700650052005C	
743CF2B3C test.exe				
ABCE283C CESC. EXE	. 3283C #1F3C			
Dump 2 Dump 3	3 💷 Dump 5 💮 Watch 1	[x=] Locals 🖉 Struct 🕮 Dump 4		005 GASDEE3E0 0000000000000000
	watch 1	· · · · · ·		0056A5DFE3F8 000000000000000 0056A5DFE400 0000000000000000000000000000000000
Нех		ASCII		005 GASDFE408 00000000000000000000000000000000000
820 SC 00 52 00 65	00 67 00 69 00 73 00 74	00 72 00 N.R.e.g.i.s.t.r.		005 GASDFE410 00000000000000000000000000000000000
830 79 00 5C 00 4D	00 61 00 63 00 68 00 69	00 GE 00 y.\.M.a.c.h.i.n.	00000	005 GA5DFE418 00000000000000000
		00 4D 00 e.\.S.Y.S.T.E.M. 00 74 00 \.C.u.r.r.e.n.t.		005 6A5D FE 420 0000000000000000000000000000000000
860 43 00 6E 00 6E	00 74 00 72 00 65 00 66	00 53 00 C.o.n.t.r.o.l.S.		0056A5DFE428 000000000000000000000000000000000000
870 65 00 74 00 50	00 43 00 6F 00 6E 00 74	00 72 00 e.t.\.C.o.n.t.r.		0056A5DFE430 002C002A00170021
880 GF 00 GC 00 5C	00 43 00 6C 00 61 00 73	00 73 00 0.1.\.C.1.a.s.s.		005 6A5DFE438 003700390038002E
890 5C 00 7B 00 34	00 64 00 33 00 36 00 65	00 39 00 \.{.4.d.3.6.e.9.		005 6A5DFE440 002600120021003E 005 6A5DFE448 0033002E002D0028
8A0 36 00 38 00 2D	00 65 00 33 00 32 00 35	00 2D 00 6.8e.3.2.5		005 GASDFE448 0033002E002D0028
880 31 00 31 00 63	00 65 00 2D 00 62 00 66	00 63 00 1.1.c.eb.f.c.		0056A5DFE458 0012000A00190018
		00 62 00 10.8.0.0.2.b.		005 6A5DFE460 0037003A00080021
800 65 00 31 00 30	00 33 00 31 00 38 00 7D	00 5C 00 e.1.0.3.1.8.}.\.		005 6A5DFE468 00390033002A0037

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.

56 53 48:83EC 28 48:89CB 4C:89C6 E8 91400100 48:89F2 48:89D9 E8 7E400100 90 48:83C4 28 58 58 C3	<pre>push rsi push rbx sub rsp.28 mov rbx,rcx mov rsi,r8 call <jmp.&wcscpy> mov rdx,rsi mov rcx,rbx call <jmp.&wcscat> nop add rsp.28 pop rbx pop rsi ret</jmp.&wcscat></jmp.&wcscpy></pre>	rcx:L" <u>C:\\WINDOWS\\explorer.exe</u> "			
41:57 41:56 41:55 41:54 55 57 56 53	push r15 push r14 push r13 push r12 push rbp push rdi push rsi push rbx	rdi:&"C:\\Users\\\\Desktop\\test.exe"			
ump 5 👹 Watch 1 🛛 [x=] Locals 🍃	Struct	00000056A5DFE885 00007FF743CF3 00000056A5DFE890 0000000000			
	ASCII	0000005 6450 FE 898 0000005 6450 FE 800 0000025 2845 61 0000025 2845 61			
0 5C 00 65 00 78	00 4E 00 44 00 4F 00 c.:.\ 00 70 00 6C 00 6F 00 W.S.\ 00 78 00 65 00 00 00 r.e.r 00 00 00 00 00 00 00 1	.W.I.N.D.O. .e.x.p.l.o. .e.x.e. .e.x.e. 			
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:

ІОС Туре	IOC
Domain	vultrusercontent[.]com
Domain	pool.hashvault[.]pro

HASHs:

ЮС Туре	IOC
MD5	24d9219e4542504ace0faaa3a0305022
MD5	f4976ef29e3ae6c8e0bfc2c3139a4ac5
MD5	718f54c5d2d887210b5d50e0a9cbc14c48901db1
SHA1	ff2aa040893d0ff9a68f4fe945804b94924c50d5
SHA1	80aef0cc3c3ec37b59f44d63b7e36bf52e81e904
SHA1	718f54c5d2d887210b5d50e0a9cbc14c48901db1
SHA256	38136273e6254b6f9ee21ecddf130aa032613a47cbfafccd2080020731f66388
SHA256	5a2602ba4027bb49e07a4cfd40ab3304c12e583d4e53981b0afa2215a394a0 2e
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 (sopc^*))
}
```



MITRE ATT&CK TABLE

Discovery	Command and Control	Defense Evasion	Persistence	Credential Access	Reconnaissa nce
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.





020101010191

Shadowox Miner RAT

f Ø in

www.infinitumit.com.tr