Cryptocurrency Entities at Risk: Threat Actor Uses Parallax RAT for Infiltration

uptycs.com/blog/cryptocurrency-entities-at-risk-threat-actor-uses-parallax-rat-for-infiltration

Uptycs Threat Research

Parallax RAT (aka, ParallaxRAT) has been distributed through spam campaigns or phishing emails (with attachments) since December 2019. The malware performs malicious activities such as reading login credentials, accessing files, keylogging, remote desktop control, and remote control of compromised machines.

The Uptycs Threat Research team has recently detected active samples of the Parallax remote access Trojan (RAT) targeting cryptocurrency organizations. It uses injection techniques to hide within legitimate processes, making it difficult to detect. Once it has been successfully injected, attackers can interact with their victim via Windows Notepad that likely serves as a communication channel.

Malware operation

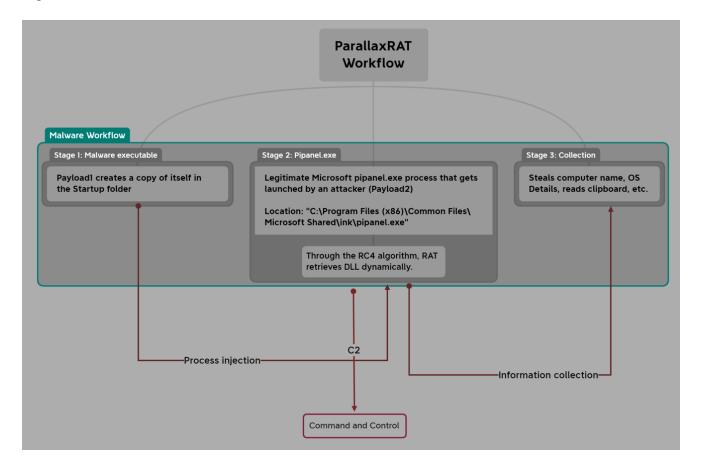


Figure 1shows the ParallaxRAT workflow.

Figure 1: ParallaxRAT workflow

Payload1

Compiled using Visual C++, payload1 is a binary file in the form of a 32-bit executable. It seems to have been intentionally obfuscated by threat actors (TA) wanting to hide something. Its fifth section (figure 2, highlighted) seems to have been altered and is unusually large compared to the remainder.

Moreover, this section has been marked with the "Code and Executable" flag, indicating it contains executable code. The TA was able to decrypt its content and use it to create a new binary, which we refer to as payload2 (i.e., Parallax RAT). Payload1 uses a technique known as <u>process-hollowing</u> to inject payload2 into a legitimate Microsoft pipanel.exe process that then gets launched by an attacker.

To maintain persistence, payload1 creates a copy of itself in the Windows Startup folder.

Eile : angle.exe	🔎 🖻		Nr	Virtual	Virtual s	RAW D	RAW size	Flags	Name	First bytes (hex)	First Ascii 20h b	sect. Stats
Entry Point : 0000AE1F 00 < EP Section : .text	01 ep	00001000	0000D60A	00001000	0000E000	60000020	.text	55 8B EC 81 EC A0 07 00 00	U 🗆 VE			
File Offset : 0000AE 1F First Bytes : 55.8B.EC.6A.FF	•	Plug	02 im	0000F000	00001300	0000F000	00002000	40000040	.rdata	20 FF 00 00 08 FF 00 00 F0		
Linker Info : 6,00 SubSystem : Windows GUI			03	00011000	00006068	00011000	00006000	C0000040	.data	00 00 00 00 00 00 00 00 00 00	@	
Linker Info : 6.00 SubSystem : Windows GUI	PE		04rs	00018000	00019884	00017000	0001A000	40000040	.rsrc	00 00 00 00 00 00 00 00 00 04	□ □ □	
File Size : 003EB000h < NO 00000000	0	5	05	00032000	0002E617	00031000	0002F000	60000020	.itext	BD 4A C2 33 CD B2 8A 02 B1	J3 {:□lQ	
	Q	1000000	06	00061000	00001014	00060000	00001000	42000040	.avinash .bharat	29 34 11 39 05 0D 1A 38 28 3C 41 26 20 2F 06 2F 33 2B)4□9□ □8()	
Image is 32bit executable RES/OVL : 2 / 0 % 2003	8	07	00063000	0000104E 000010A6	00061000	00001000	52000040 52000040	.onarat	3C 41 26 20 2F 06 2E 33 2B 35 08 16 47 35 35 09 08 4F	<a& □.3+\$□<br="">5□□G55□0</a&>		
Microsoft Visual C++ ver 5.0/6.0 - no sec. CAB/7z/Zip - 2003-10-23	09	00063000	000010A6	00062000	00001000	50000040	.giuditt	15 2C 04 20 02 2A 2A 00 1B	□,□ ** □&			
Lamer Info - Help Hint - Unpack info	10	00069000	0000107E	00064000	00001000	40000040	rgiolarce	43 47 0F 01 38 46 35 2F 16	CG === 8F5/=*			
Not packed , try OllyDbg v2 - www.ollydbg.de or IDA v7 www.hex-ray	11	0006B000	00386000	00065000	00386000	42000040	.halette	23 0F 15 27 0B 11 08 28 42	#00'00(B			
	<u></u>		Overla	ay: No over	rlav data							
	End of file : 00 00 00 00 00 00 00 00 00 00 00 00 0								00 00 00 00 00 00 00 00 00 00			
			Clip	Section 05	status : Executab	le ⊡Rea	dable	Writable	S		tions size : 2 MB	Cave S-

Figure 2: Payload1 binary

Payload2

ParallaxRAT is a 32-bit binary executable that gathers sensitive information from victimized machines, e.g., system information, keylogging, and remote control functionality.

It has null import directories and encrypted data is stored in the .data section. The attacker uses the RC4 algorithm to decrypt this data, revealing the DLLs required for further action.

	1	
text:00405D61	loc_405D61:	; CODE XREF: sub_405D09+E↑j
.text:00405D61 5E	pop esi	
.text:00405D62 83 EC 08	sub esp, 8	
text:00405D65 8D 64 24 08	lea esp, [esp+8]	
.text:00405D69 30 0E	xor [esi], dl	
Le .text:00405D6B EB DC	jmp short loc 405D49	
.text:00405D6B	sub 405D09 endp ; sp-analysis f	failed
.text:00405D6B		
.text:00405D6D		
.text:00405D6D	; ========== S U B R O U T	Г Т N F =================================
.text:00405D6D	,	
.text:00405D6D		
.text:00405D6D	sub 405D6D proc near	; CODE XREF: sub 405D6D+20↓p
.text:00405D6D	sub_400000 proc near	, CODE AREL: SUD_405000+200p
	and the standards of	
.text:00405D6D	arg_0= dword ptr 4	
.text:00405D6D		
.text:00405D6D	; FUNCTION CHUNK AT .text:00405	5B9D SIZE 00000007 BYTES
.text:00405D6D		
.text:00405D6D 8D 64 24 04	lea esp, [esp+4]	
.text:00405D71 33 C0	xor eax, eax	
.text:00405D73 8B 0C 24	mov <mark>ecx</mark> , [esp-4+arg_0]	
text:00405D76 EB 56	jmp short loc_405DCE	
.text:00405D76	;	
.text:00405D78 D3 4A E5 14 69 FD CC 5F A6 D1 50 AD	dd 14E54AD3h, 5FCCFD69h, 0AD50D	D1A6h
.text:00405D84 39 A9 C8	db 39h, 0A9h, 0C8h	
.text:00405D87	;	
.text:00405D87		
.text:00405D87	loc_405D87:	; CODE XREF: sub_405D09+37↑j
<pre>.text:00405D87 0F 85 10 FE FF FF</pre>	jnz loc_405B9D	
.text:00405D8D E8 DB FF FF FF	call sub 405D6D	
.text:00405D92 13 C9	adc ecx, ecx	
.text:00405D94 8E 68 CA	mov gs, word ptr [eax-36h]	
00005169 0000000000405D69: sub 405D09+60 (Synchronized with 1		
O Hex View-1		
0040C1A0 51 F5 5E D8 3D 5C 1E B7 AB 5F D5 E7 A3 37 BA CA 00^0=		
0040C1B0 21 7B 33 E4 A6 4E D2 0A 2F F9 6C 17 86 A8 2E 2A !{3ä!		
0040C1C0 2B 27 62 B4 F7 8A B8 8E 5C A9 16 C1 30 8F 20 56 + b +		
0040C1D0 C7 B2 DE 60 B0 E7 1F 33 BD F4 3D F3 54 92 78 E5 C ² P [°]		
0040C1E0 B8 F7 39 BC 58 CC FE 69 1C 0F 48 0B 36 0D 3E 39 .+9XX		
0040C1F0 EB A8 1F 97 01 D1 E8 15 0B 40 27 C6 F1 01 01 1D ë"		
0040C200 A9 E4 4C 43 72 79 70 74 33 32 2E 64 6C 6C A1 77 @äLCm		
0040C210 5E 49 8B 70 AB 5A 58 76 2B E2 09 F4 74 06 6D F7 ^I px		
0040C220 A1 84 23 23 4D 51 A6 EF FE 73 C9 98 2C FF FF FF in##M		
0040C230 FF 00 00 00 00 53 4F 46 54 57 41 52 45 5C 4D 69 ÿ		
0040220 11 00 00 00 00 00 35 4F 40 54 57 41 52 45 5C 4D 69 y	OF TWARE (FIT	

Figure 3: RC4 decryption algorithm

System information

An attacker can extract sensitive information from a victim's machine, including computer name and operating system (OS) version. And the attacker is able to read data stored in the clipboard.

🔘 Hex \	/iew-1																
005531F	0 AB	AB	AB	AB	AB	AB	AB	AB	00	00	00	00	00	00	00	00	««««««««
0055320		50							A2	B7	1E	A8	FA	C7	BA	DØ	\$PxÆ¢¢"úÇ≌Ð
0055321	0 72	7F	8F	01	D4	FA	12	13	87	47	21	9C	18	55	сс	ED	rÔú‡G!œ.UÌí
0055322	0 49	33	69	12	10	ØE	6F	93	34	2C	СВ	E9	66	C2	EA	00	I3io"4,ËéfÂê.
0055323	0 00	00	00	00	00	00	00	00	00	00	00	00	FF	FF	FF	FF	······ÿÿÿÿ
0055324	0 55	00	73	00	65	00	72	00	2F	00		_				00	U.s.e.r./.
0055325	0	00	2D	00	57	00	49	00	4E	00	44	00	4F	00	57	00	W.I.N.D.O.W.
0055326	0 53	00	2D	00				00	00	00	00	00	FF	FF	FF	FF	Sÿÿÿÿ
0055327	0 57	69	6E	64	6F	77	73	20	31	30	20	45	6E	74	65	72	Windows · 10 · Enter
0055328		72							61	6C	75	61	74	69	6F	6E	prise·Evaluation
0055329	0 20	00	FF	FF	FF	FF	78	36	34	00	FF	FF	FF	FF	49	00	·.ÿÿÿÿx64.ÿÿÿÿI.
005532A		00								00							D.Ap.a.y.
005532B		00								00							l.o.a.d.2i.6.
005532C		00								00							4. •. (.p.a.y.l.o.
005532D		00								00							a.d.2b.i.n.).
005532E		00								00							+.C.:.\.U.s.e.r.
005532F		00								00							s.\.U.s.e.r.\.D.
0055330		00								00							e.s.k.t.o.p.\.p.
0055331		00								00							a.y.l.o.a.d.2
0055332 0055333		00 00								00 00							1.6.4R.u.
0055334		00								00							n.n.i.n.gÿÿÿÿ " 00000 0000
0055335		00								00							"ÿÿÿÿ9ÿÿÿÿ kÿÿÿÿ
0055336		00								00							
0055337		00								00							
0055338		00								00							
0055339		00											00				
005533A		00	00	00	00	00	00	00	00	00	00	00	00	00	00		
005533R		00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	

Figure 4: Read victim machine

Uptycs has detected and recorded the same event.

IGNALS DETECTION GRAPH	Related Detections »	CONTEXT ACTIVITIES
ATT&CK Matrix ⑦ 504 signals ♥ Group All ▼ Search ■ P P D C D C C C C C A Signals (1). C.14710g1all1 Files/Google10/104 File Subeal1(0+0.47.01G00		empting to get system information - T1082 - rmation Discovery - Windows
✓ Signals (5): C\WINDOWS\Explorer.EXE	Code: ATTACK_SYSTI	M_INFORMATION_DISCOVERY_T1082_WINDOWS_API
 Signals (3): C:\Users\ \Desktop\ \angle.exe 02/21/2023 17:46:54 		
• 02/21/2023 17:46:54	Арі	GetComputerNameW
• 02/21/2023 17:46:53	Command line	\. 'angle.exe"
Signals (4) : C:\Users\ \Desktop\Procmon64.exe	File	C:\Users\ Desktop \ \angle.exe
0 📀 T1529 - IMPACT - WINDOWS	Login name	
Z_Beta_Process attempting to Shutdown the System	Process id	12104
∧ Signals (1): C:\windows\syswow64\shutdown.exe	Process name	angle.exe

Figure 5: Uptycs event detection

Keystrokes

The attacker has the ability to read and record their victim's keystrokes, which are then encrypted and stored in the %appdata%\Roaming\Data\Keylog_<Data> directory.

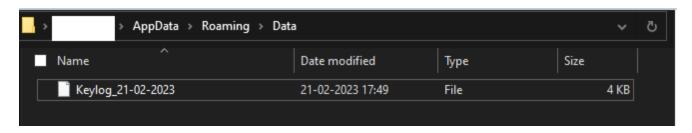


Figure 6: Keylogger data

Command and control

After successfully infecting a victim's machine, the malware sends a notification to the attacker. They then <u>interact</u> with the victim by posing questions via Notepad and instructing them to connect to a Telegram channel.

File Edit View	
The threat actor initiates a hey dude, can we talk? chat with the victim. comnpanyk you wor k for//	*README.txt - Notepad File Edit View
do yoou haaaveee teleggraamm//Yes	my telegram is @testapple123 The threat actor provided the victim with a Telegram ID.
You are from	okay
ggiiveee meee yourr teleegraamm contttaccttt Y	
iiii waantt t tooo unnddstndddyyyorr possitionn purpose of	
Your ID plz	
yyysss ysss yeesss i wnattt t knoww	
???	
	Ln 1, Col 30

Figure 7: Attacker shared Telegram ID via Notepad

Shutdown

The attacker is able to remotely shut down or restart the victim's machine. Here, they remotely restarted our test machine (figure 8).

SIGNALS DETECTION GRAPH	Kelated Determine	ctions >>	CONTEXT ACTIVITIES
ATT&CK Matrix 7 504 signals Group All Time * Search * * <td< th=""><th>Clear filters</th><th>T1529 -</th><th></th></td<>	Clear filters	T1529 -	
Isof6.001 - INPUT CAPTURE - WINDOWS Z_Beta_Process attempting to intercept keystrokes Signals (1): C:\WINDOWS\Explorer.EXE 0/221/2023 17:47:03		Api Arguments	InitiateSystemShutdownExW {"IpMachineName": "NULL" "IpMessage": "NULL" "dwTimeout": "30" "bForceAppsClosed": "0" "bRebotAtterShutdown": "1" "dwReason": "2147483903" }
0.1 C T1204 - USER EXECUTION - WINDOWS Process executed by user V Signals (1): CAUsers). (Desktoo) (angle.exe		Command li	ne shutdown-r C:\windowstsyswow64 \shutdown.exe

Figure 8: Attacker restarted victim machine

Script file

The ParallaxRAT binary was extracted from memory and independently executed, wherein it drops a UN.vbs file and runs that using the wscript.exe tool. The script deletes the payload and erases any traces of its existence.

On Error Resume Next Set DpxjzJffnNL = CreateObject("Scripting.FileSystemObject") while DpxjzJffnNL.FileExists("C:\Users\<username>\AppData\Local\Temp\<payload2>.exe") DpxjzJffnNL.DeleteFile "C:\Users\<username>\AppData\Local\Temp\<payload2>.exe" wend DpxjzJffnNL.DeleteFolder "C:\Users\<username>\AppData\Local\Temp\<payload2>.exe" DpxjzJffnNL.DeleteFolder "C:\Users\<username>\AppData\Local\Temp\<payload2>.exe"

Figure 9: Visual Basic script

Threat actor objective

The threat actor uses a commercially available remote access Trojan (RAT) tool. It grabs private email addresses of cryptocurrency companies from the website, dnsdumpster.com. ParallaxRAT subsequently disseminated malicious files via phishing emails and obtained sensitive data.

The Uptycs Threat Intel research team conducted a thorough analysis to gain a better understanding of the operations and goals of the actor modules, we have engaged with the threat actor. The following picture illustrates how the actor is utilizing Parallax RAT in his campaign targeting crypto companies.

The purchased Parallax/XAT and use the same for weaponization.		Intel collection Integlibratumpater com It was discovered that the attacker was searching In invitate omal address of targeted composition.	
The purchased Parallar/RAT and use the same for weaponization.	cryptocurrency organizations.	All and a fire 2,26 (%) (a) interface to the mask a fire 2,26 (%) If the top 30 logger (2) (%) If the top 30 logger	
	TA purchased ParallaxRAT and use the same for weaponization.	we lead thing you can do its printably (222 PM) workbulk some public rat source code (222 PM) object go through (z. 223 PM) doot even understand its printably (223 PM) doot even understand its printable (223 PM) doot even understand its prin	Crowna Crowna
Once TA collects the list of mails then, for delivery TA use phishing mail with weaponized ParallaxRAT as a attachment.	Once TA collects the list of mails then, for delivery mail with weaponized ParallaxRAT as a attachmer im currently campaigning against specific corporat	t the second s	

Figure 10: Telegram chat and attacker's mindmap

← → C	O A https://dnsdumpster.com							☆
		B3-1909,200,200,000.	210.233.30.10 ns3.google.com	United States				
		$M\!X$ $Records$ ** This is where email for the domain goes			*	¶ 0	•	
		30 alt3.gmail-smtp-in.1.google.com. Ⅲ 	142.250.27.26 ra-in-f26.1e100.net	GOOGLE United States				
		20 alt2.gmail-smtp-in.1.google.com. ∰ >4 ⊗ ∲	64.233.184.26 wa-in-f26.1e100.net	GOOGLE United States				
		10 alt1.gmail-smtp-in.1.google.com. ∰ ≯4 ⊚ ∲	209.85.203.27 dh-in-f27.1e100.net	GOOGLE United States				
		5 gmail-amtp-in.l.google.com. Ⅲ ズ 👁 🔶	172.253.115.27 bg-in-f27.1e100.net	GOOGLE United States				
		40 alt4.gmail-smtp-in.l.google.com. Ⅲ >4 ④ ∲	142.250.153.27 ea-in-f27.le100.met	GOOGLE United States				

Figure 11: ParallaxRAT grabs target company info from public source

Conclusion – Uptycs EDR detects and blocks ParallaxRAT attacks

It's important for organizations to be aware of this malware's existence and take necessary precautions to protect systems and data. With YARA built-in and armed with other advanced detection capabilities, Uptycs EDR customers can easily scan for ParallaxRAT. EDR contextual detection provides important details about identified malware. Users can navigate to the toolkit data section in a detection alert, then click the name of a detected item to reveal its profile (figure 12).

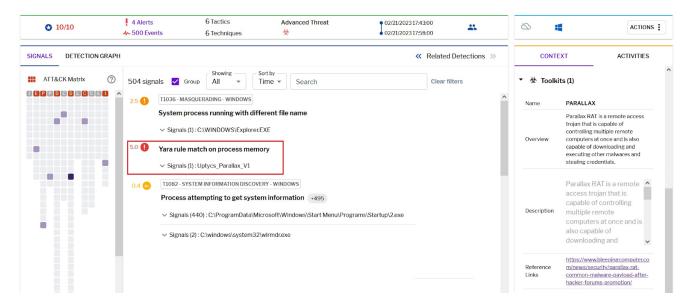


Figure 12: Uptycs EDR detection showing ParallaxRAT—YARA rule match

IOCs

File name	Md5 hash
Payload1	40256ea622aa1d0678f5bde48b9aa0fb
Payload2	698463fffdf10c619ce6aebcb790e46a
pipanel.exe(Legitimate)	3c98cee428375b531a5c98f101b1e063
milk.exe	40256ea622aa1d0678f5bde48b9aa0fb

Persistence

C:\users\<username>\appdata\roaming\microsoft\windows\start menu\programs\startup\milk.exe

Domain/URL

By analyzing the VirusTotal graph, we were able to identify a higher number of Parallax RAT samples spreading in recent days. All the files are communicating with the USA regions (144.202.9.245:80) as per vt report.

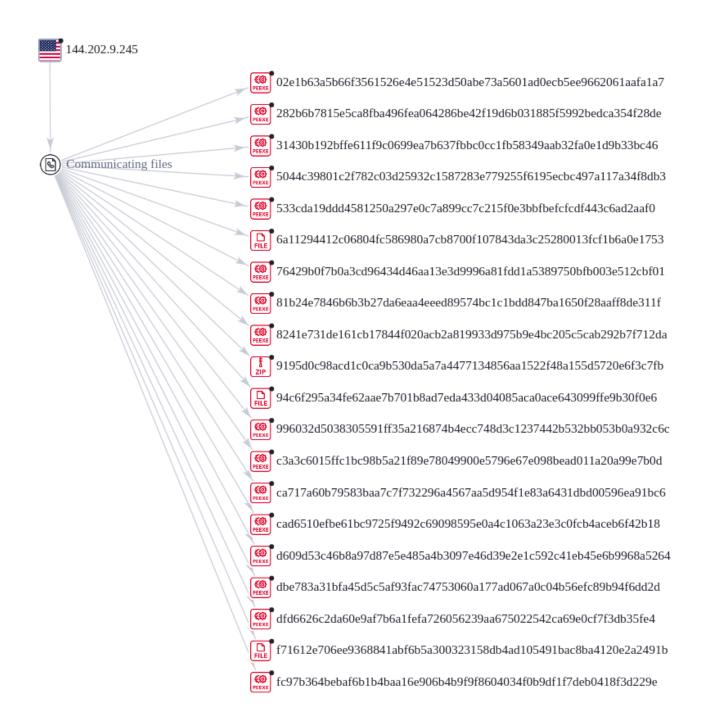


Figure 13: VirusTotal graph for ParallaxRAT

Tag(s): Threat Hunting , Threat Management , EDR , Threat Research , XDR

Uptycs Threat Research

Research and updates from the Uptycs Threat Research team.

Connect with the author