

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 1 shows the ParallaxRAT workflow.

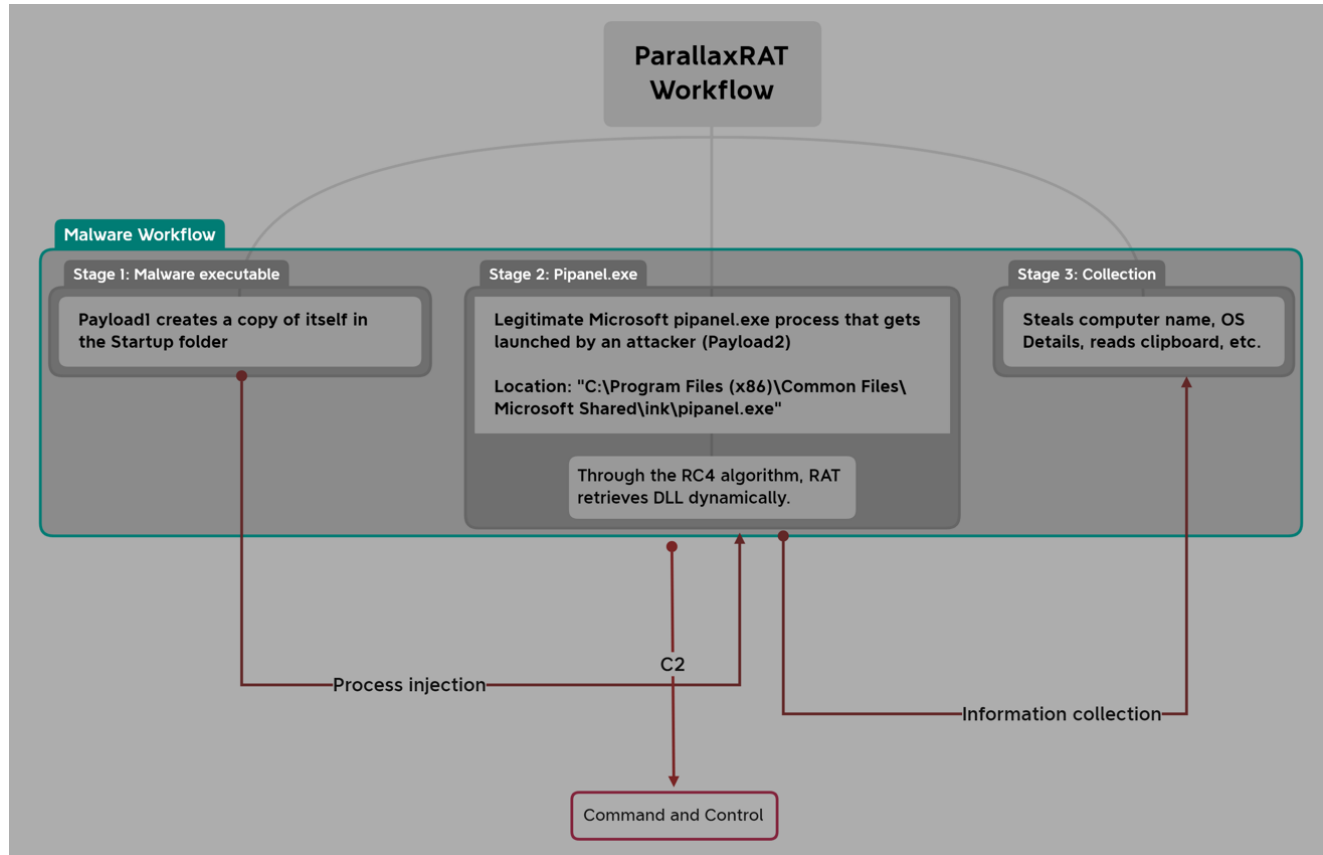


Figure 1: ParallaxRAT workflow

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 process-hollowing 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.

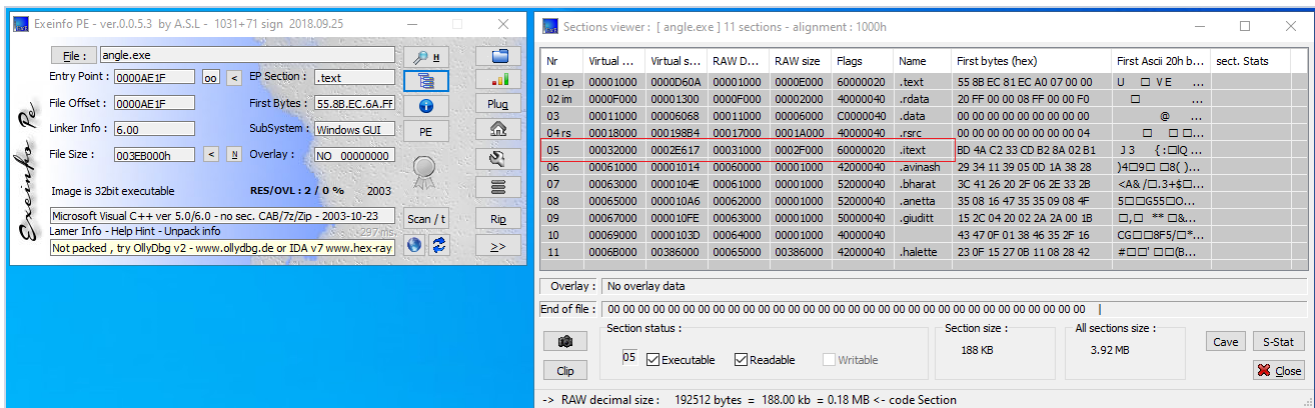


Figure 2: Payload1 binary

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.

```

.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]
RIP .text:00405D69 30 0E xor [esi], dl
.text:00405D6B EB DC jmp short loc_405D49
.text:00405D6B sub_405D09 endp ; sp-analysis failed
.text:00405D6B
.text:00405D6D
.text:00405D6D
; ===== SUBROUTINE =====
.text:00405D6D
.text:00405D6D sub_405D6D proc near ; CODE XREF: sub_405D6D+20↑p
.text:00405D6D arg_0= dword ptr 4
.text:00405D6D ; FUNCTION CHUNK AT .text:00405B9D 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 ecx, [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, 0AD50D1A6h
.text:00405D84 39 A9 C8 db 39h, 0A9h, 0C8h
; -----
.text:00405D87
.text:00405D87 loc_405D87: ; CODE XREF: sub_405D09+37↑j
RIP .text:00405D87 0F 85 10 FE FF FF jnz loc_405B9D
.text:00405D88 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 RIP)

```

```

Hex View-1
0040C1A0 51 F5 5E D8 3D 5C 1E B7 AB 5F D5 E7 A3 37 BA CA Q8^0=\.«_õçE7ºÊ
0040C1B0 21 78 33 E4 A6 4E D2 0A 2F F9 6C 17 86 A8 2E 2A !{3ã}NÒ./û1.+*.
0040C1C0 2B 27 62 B4 F7 8A B8 8E 5C A9 16 C1 30 8F 20 56 +'b'+š,ž\@.Á0.·V
0040C1D0 C7 B2 DE 60 B0 E7 1F 33 BD F4 3D F3 54 92 78 E5 Ç²p`°ç.3%ó=óT'xá
0040C1E0 B8 77 39 BC 58 CC FE 69 1C 0F 4B 0B 36 0D 3E 39 .+9%XÍpi..K.6.>9
0040C1F0 EB A8 1F 97 01 D1 E8 15 0B 40 27 C6 F1 01 01 1D ë".-ñë..@'ãñ...
0040C200 A9 E4 4C 43 72 79 70 74 33 32 2E 64 6C 6C A1 77 0ãL Crypt32.dll;w
0040C210 5E 49 8B 70 AB 5A 58 76 2B E2 09 F4 74 06 6D F7 ^I<p<ZXv+ã.ót.m+
0040C220 A1 84 23 23 4D 51 A6 EF FE 73 C9 98 2C FF FF FF j,##MQ;ìpsÉ",ÿÿÿ
0040C230 FF 00 00 00 00 53 4F 46 54 57 41 52 45 5C 4D 69 ý....SOFTWAREVMi

```

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.

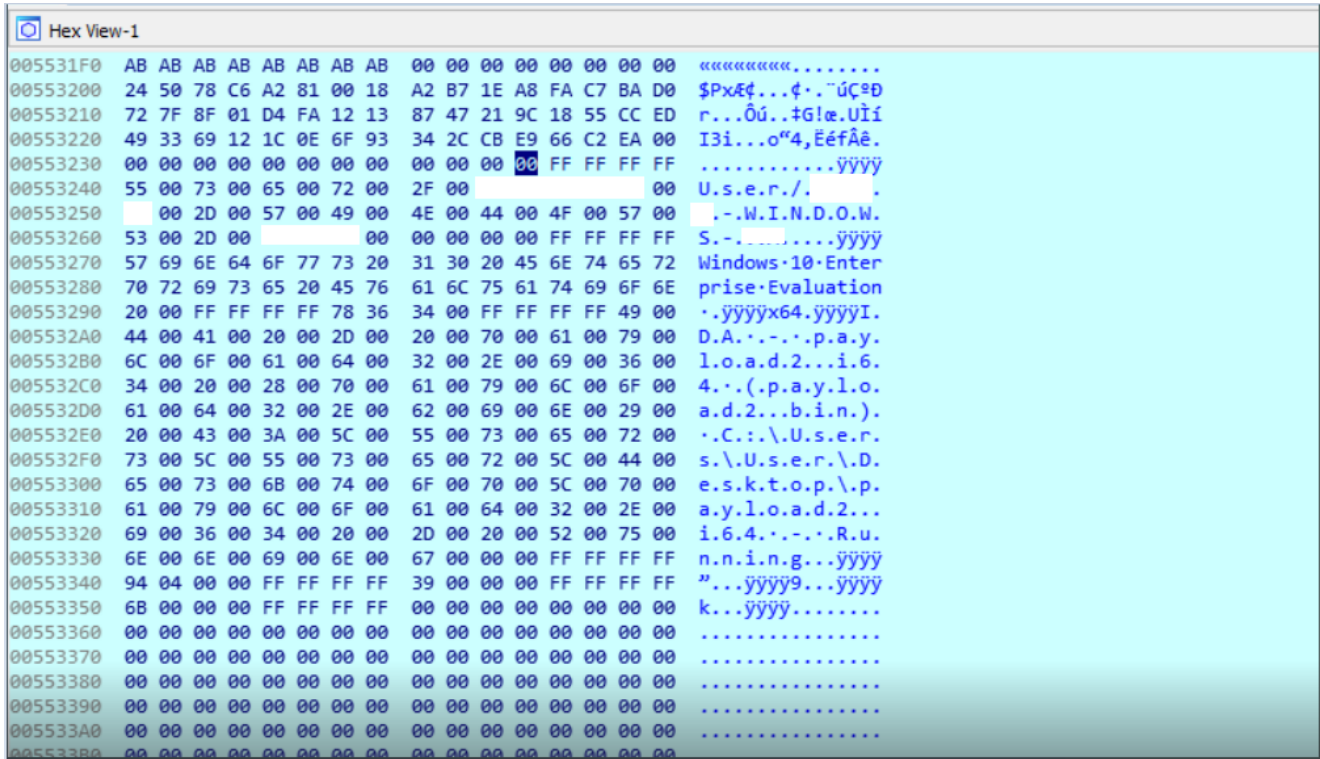


Figure 4: Read victim machine

Uptycs has detected and recorded the same event.

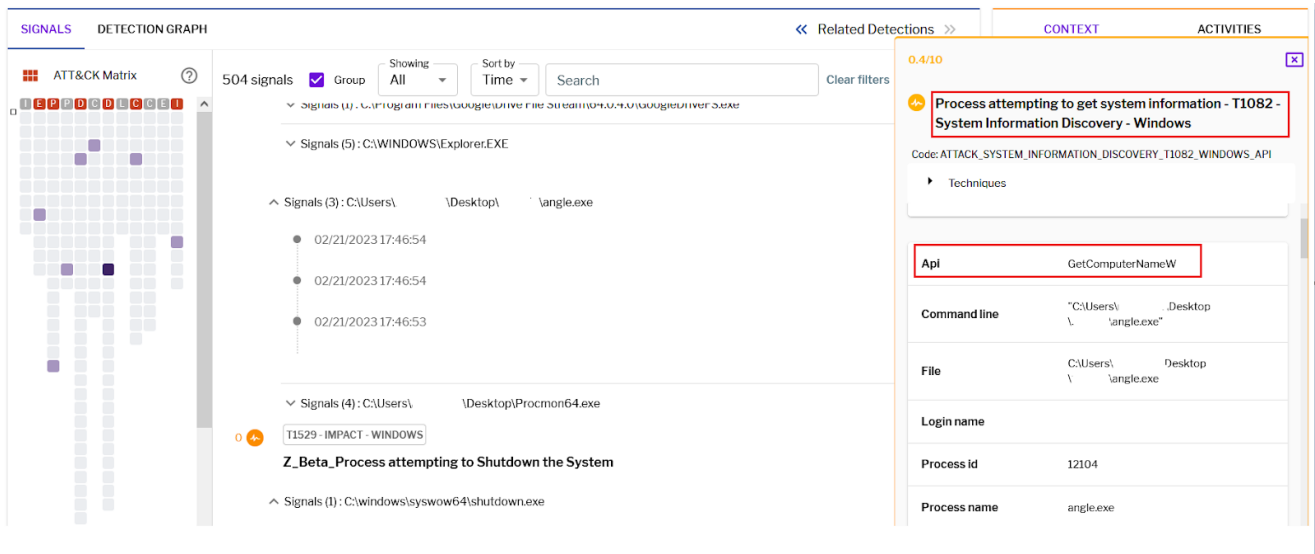


Figure 5: Uptycs event detection

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.

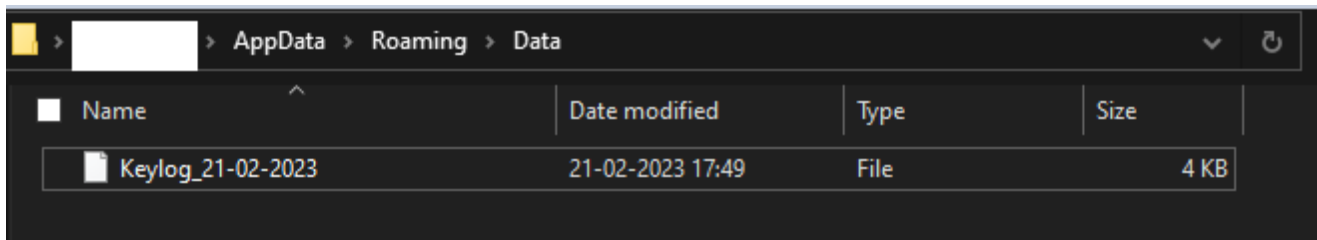


Figure 6: Keylogger data

Command and control

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

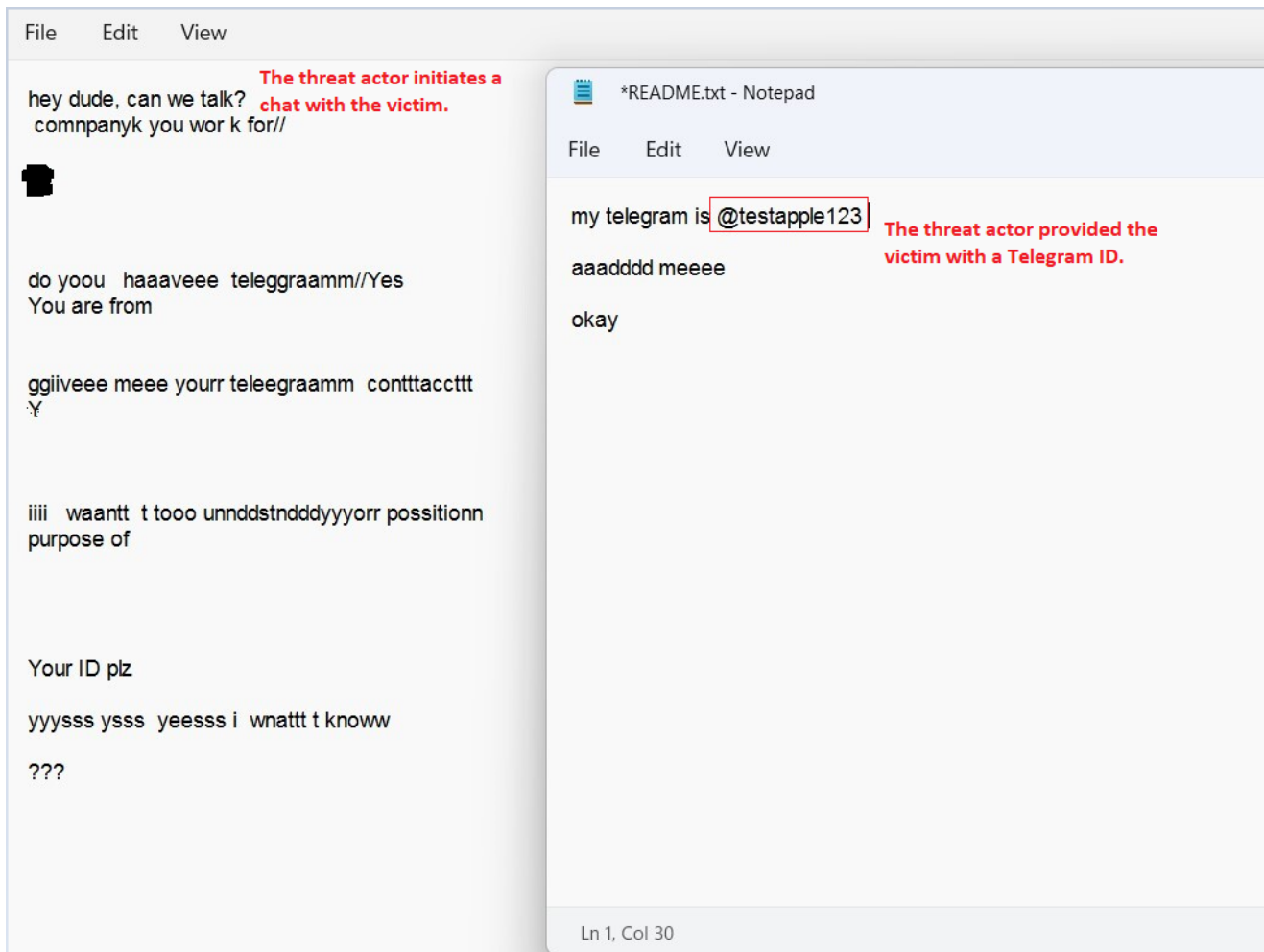


Figure 7: Attacker shared Telegram ID via Notepad

Shutdown

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

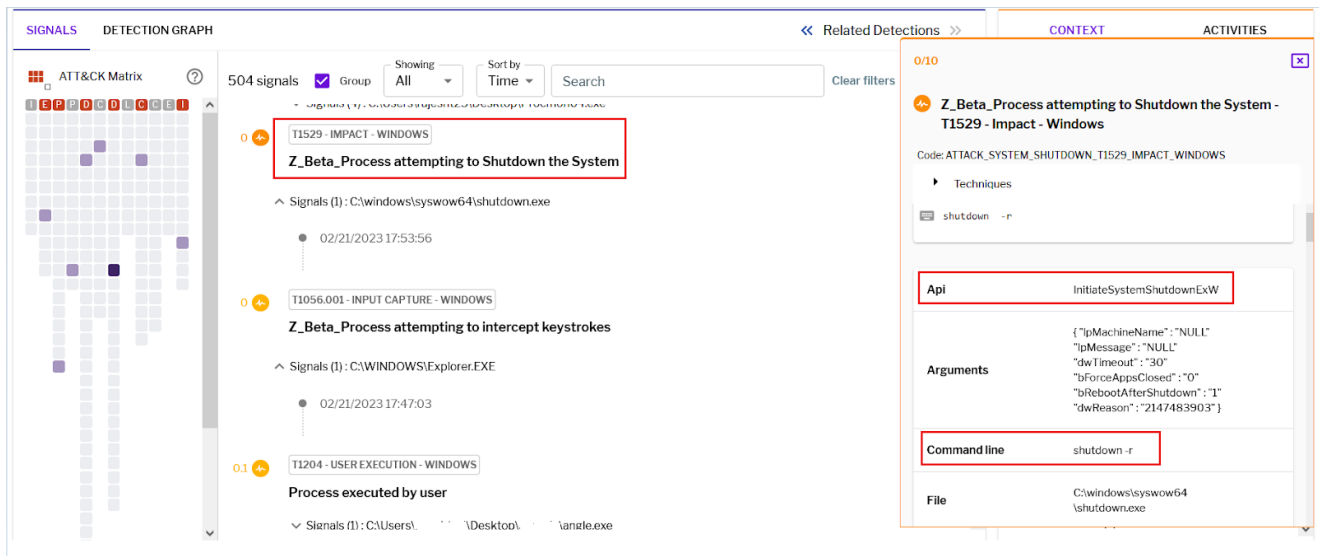


Figure 8: Attacker restarted victim machine

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\\AppData\Local\Temp\\AppData\Local\Temp\\AppData\Local\Temp\
```

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.

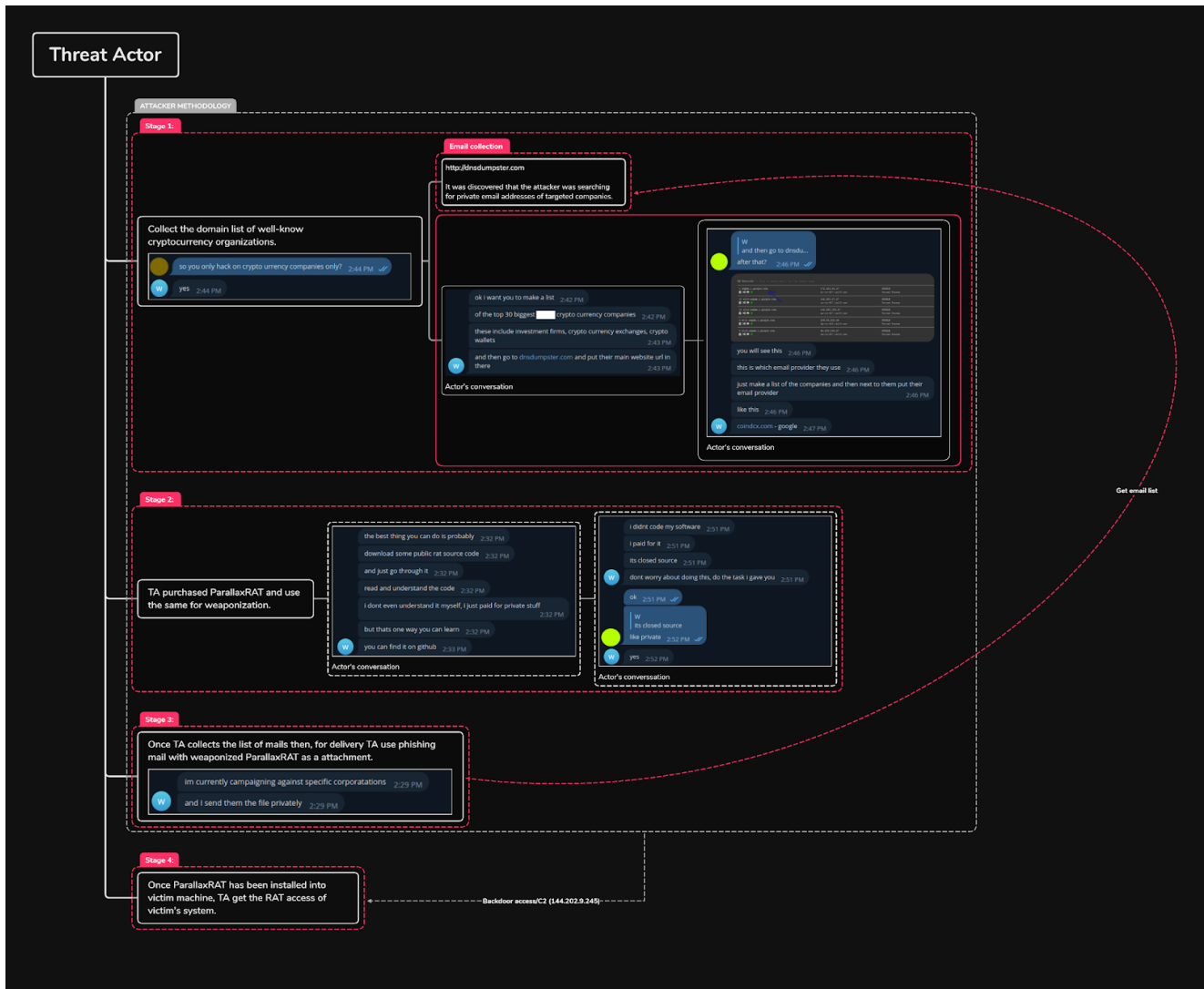


Figure 10: Telegram chat and attacker's mindmap

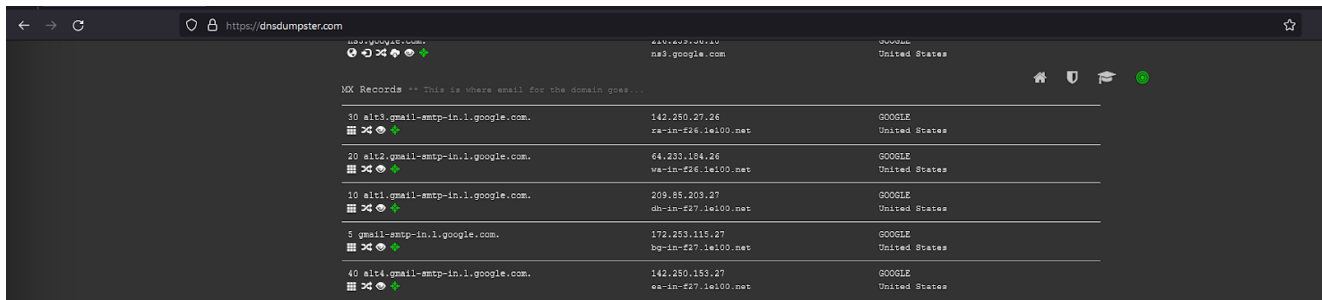


Figure 11: ParallaxRAT grabs target company info from public source

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).

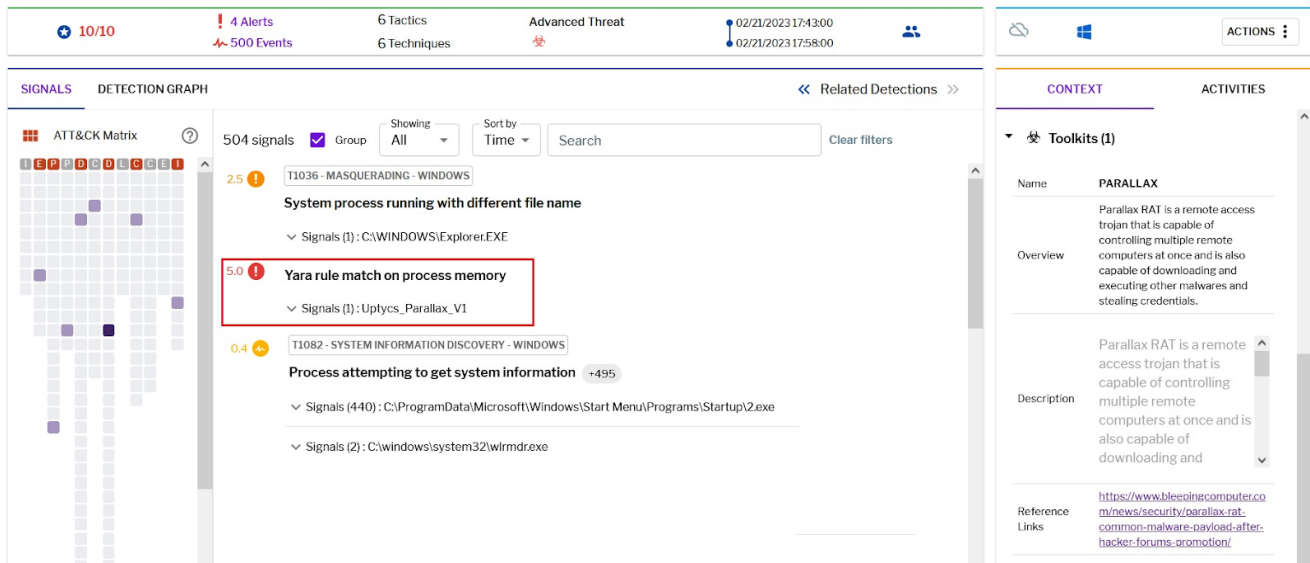


Figure 12: Uptycs EDR detection showing ParallaxRAT—YARA rule match

IOCs

File name	Md5 hash
Payload1	40256ea622aa1d0678f5bde48b9aa0fb
Payload2	698463ffdf10c619ce6aebcb790e46a
pipanel.exe(Legitimate)	3c98cee428375b531a5c98f101b1e063
milk.exe	40256ea622aa1d0678f5bde48b9aa0fb

Persistence

C:\users\\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