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.

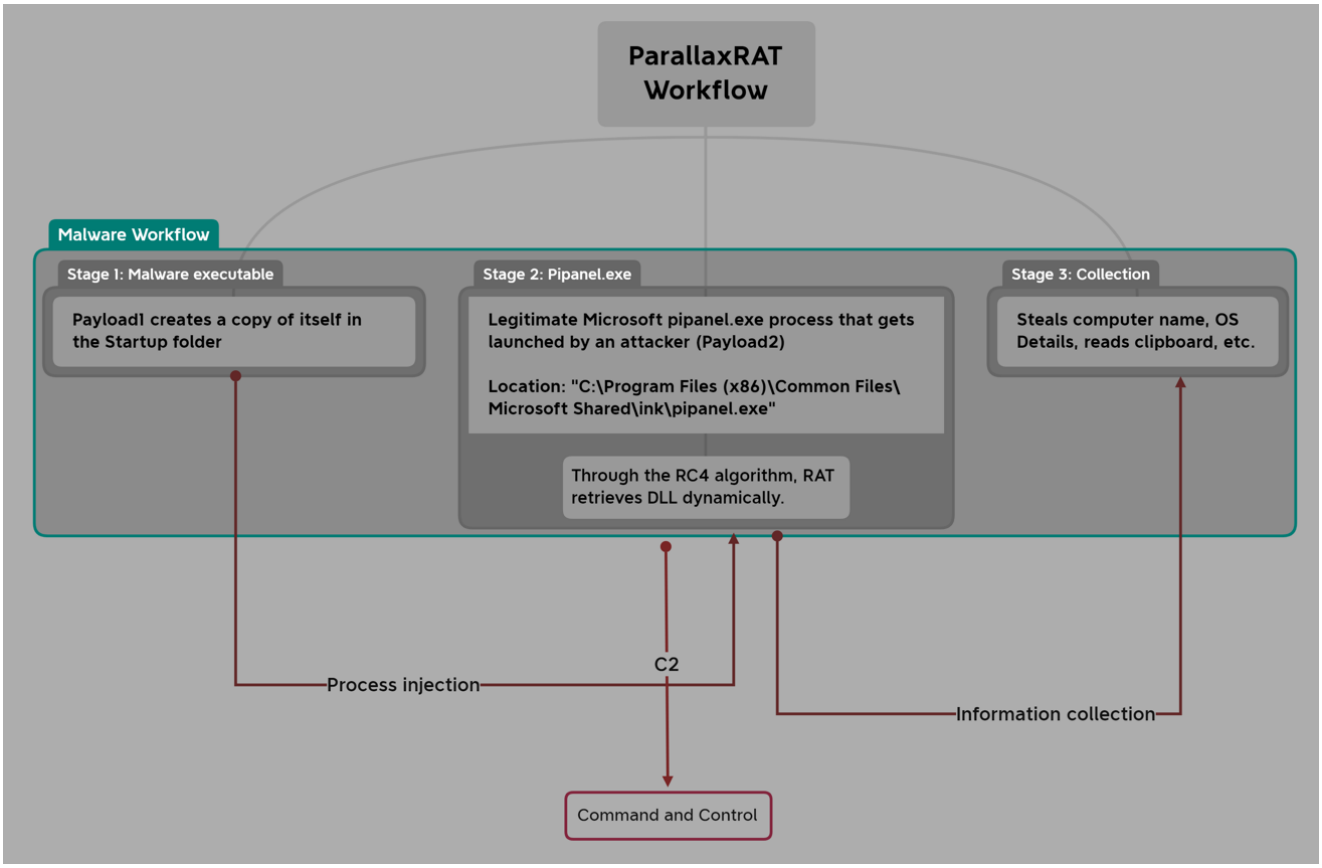

Figure 1: ParallaxRAT workflow

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 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.

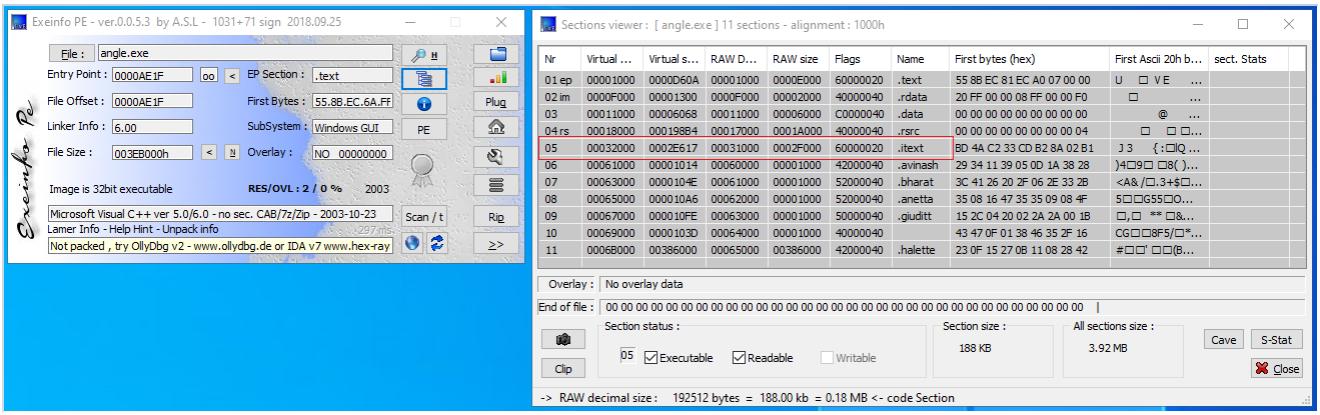

Figure 2: Payload1 binary

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.

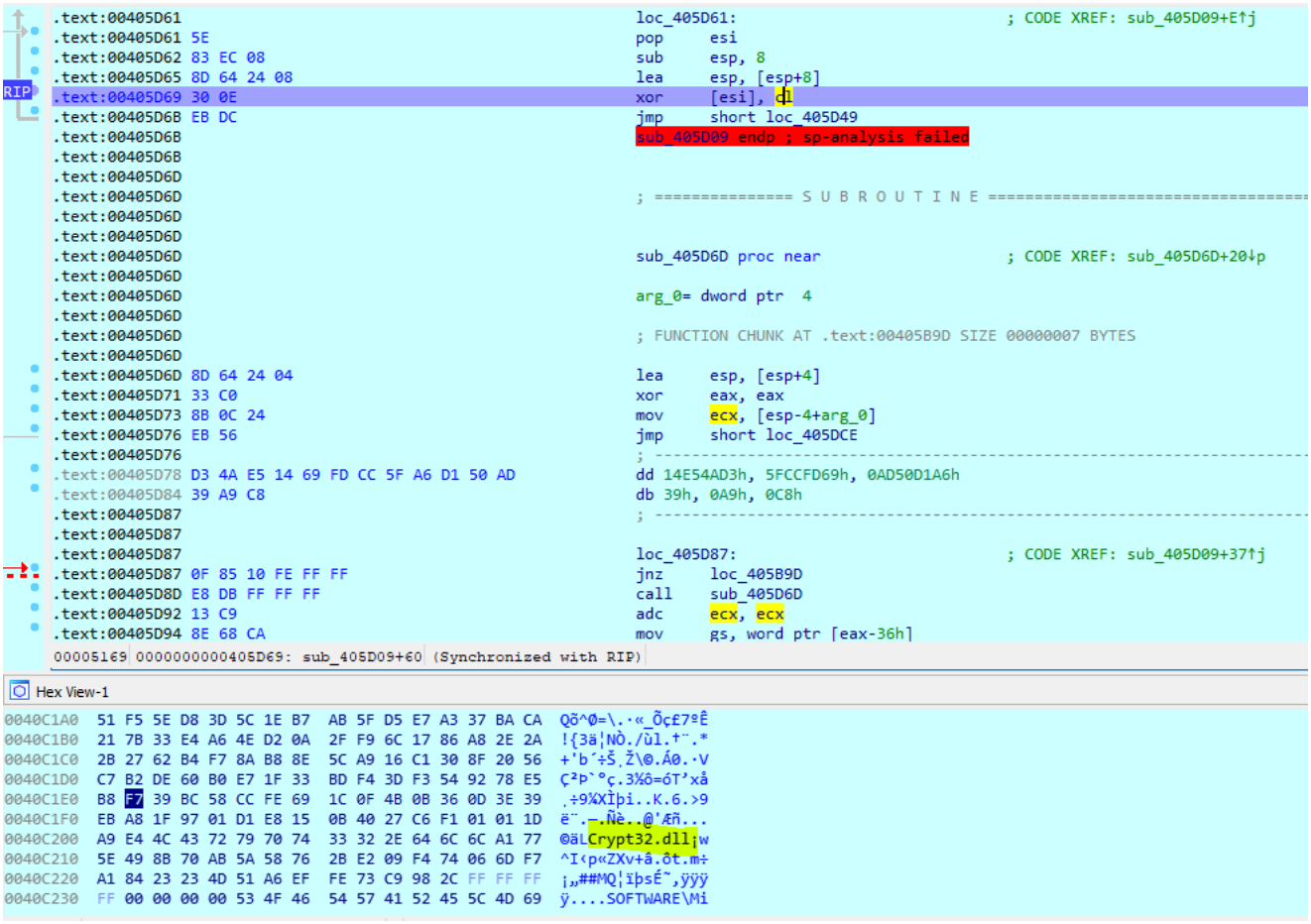

Figure 3: RC4 decryption algorithm

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.

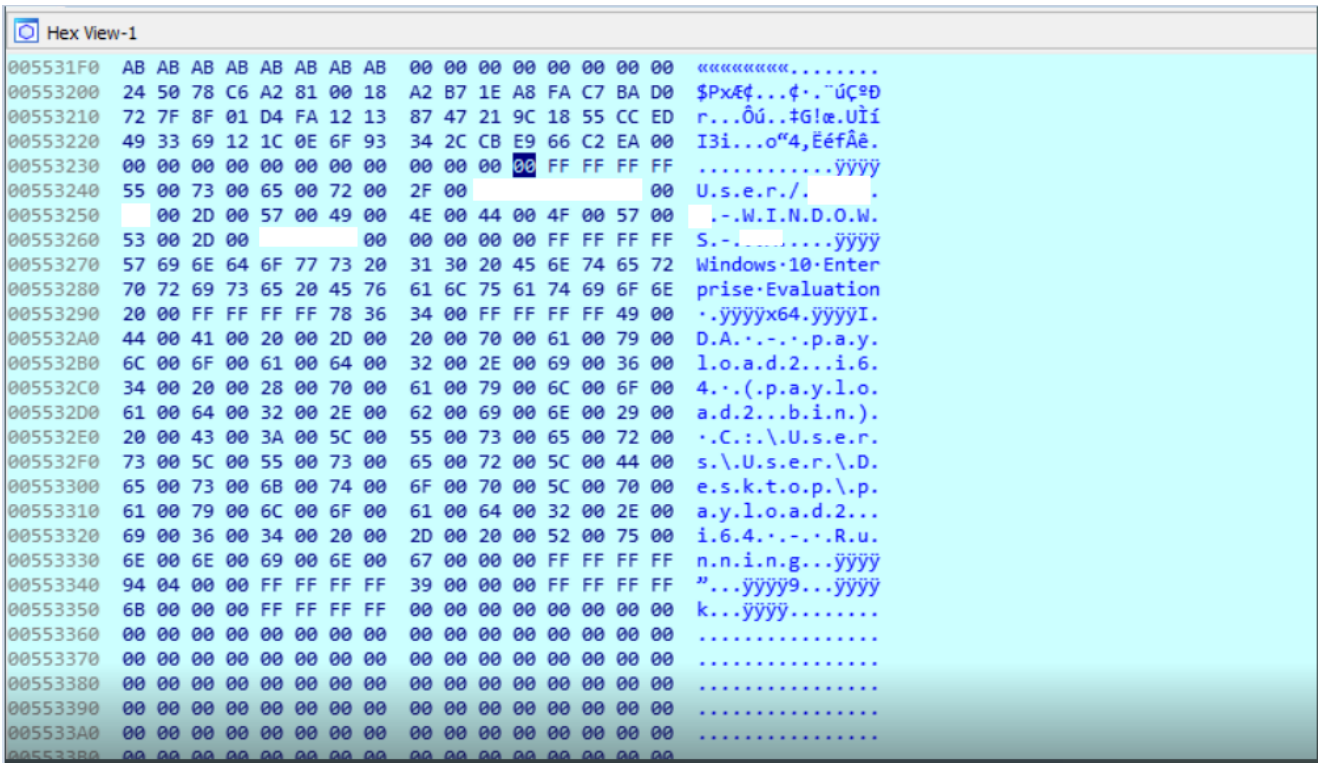

Figure 4: Read victim machine

Uptycs has detected and recorded the same event.

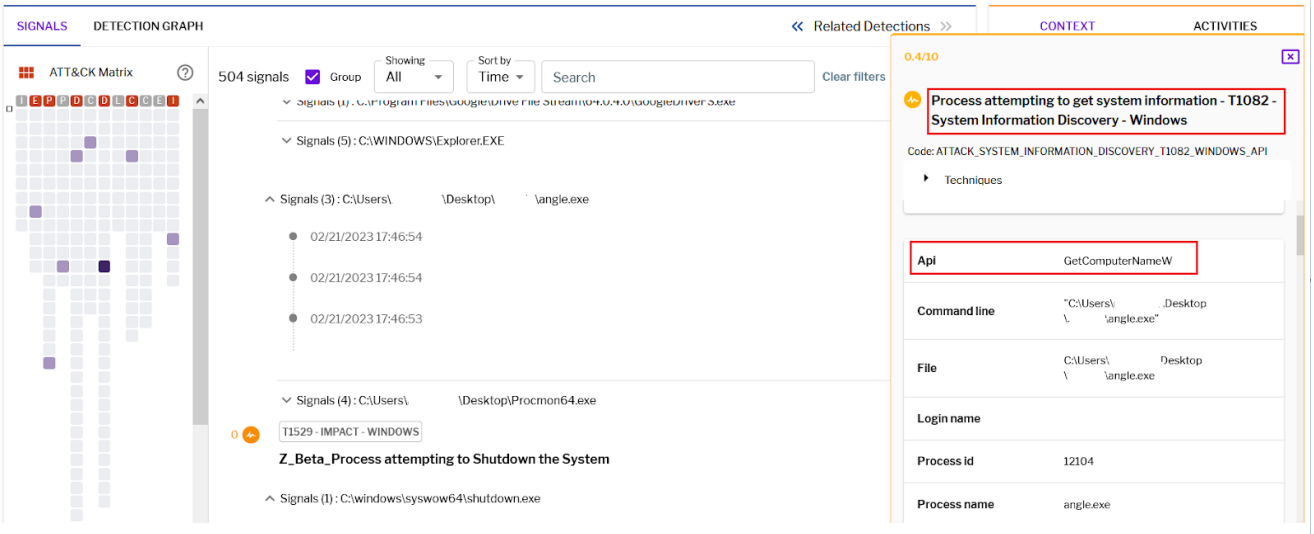

Figure 5: Uptycs event detection

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.

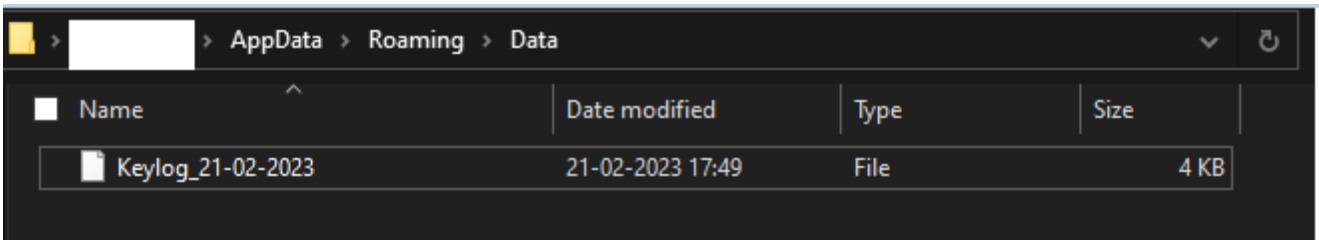

Figure 6: Keylogger data

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.

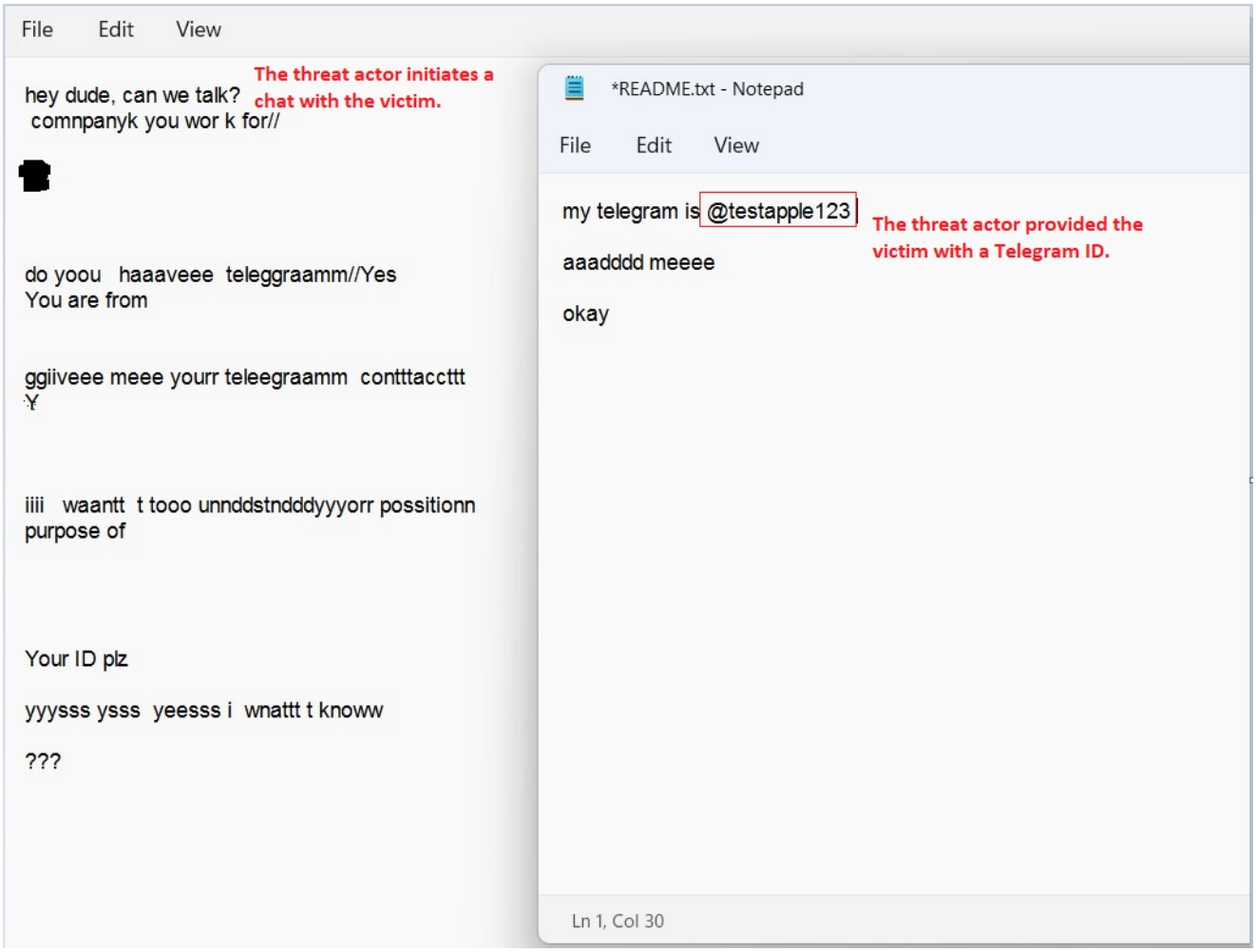

Figure 7: Attacker shared Telegram ID via Notepad

Shutdown

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

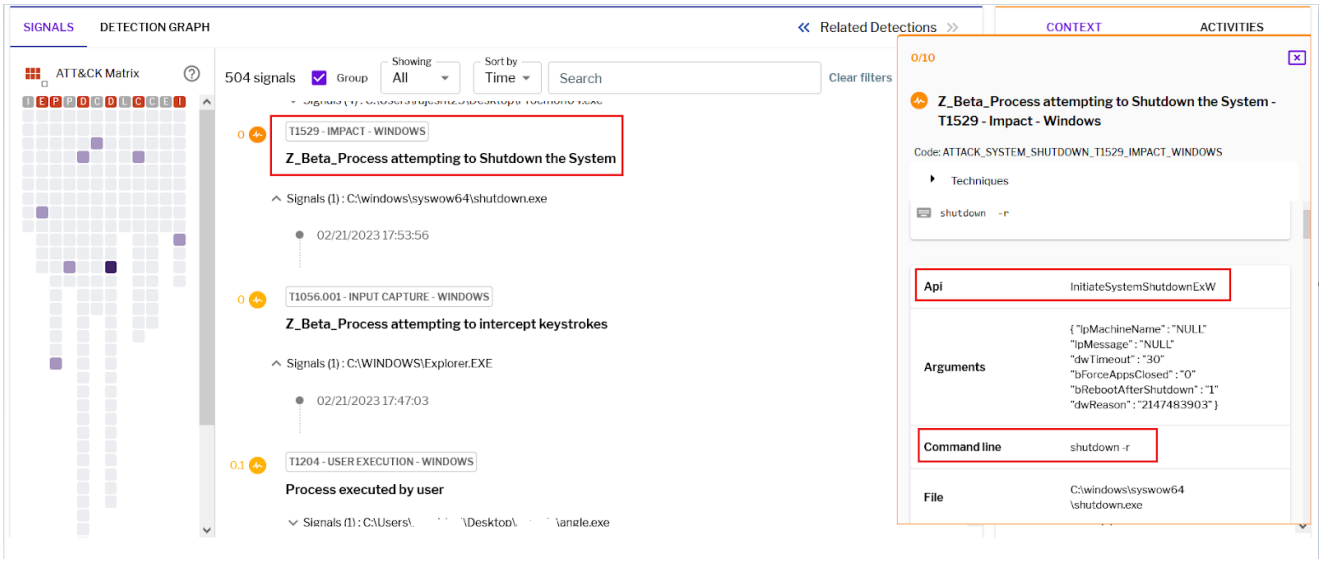

Figure 8: *Attacker restarted victim machine*

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\<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"
DpxjzJffnNLX
```

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.

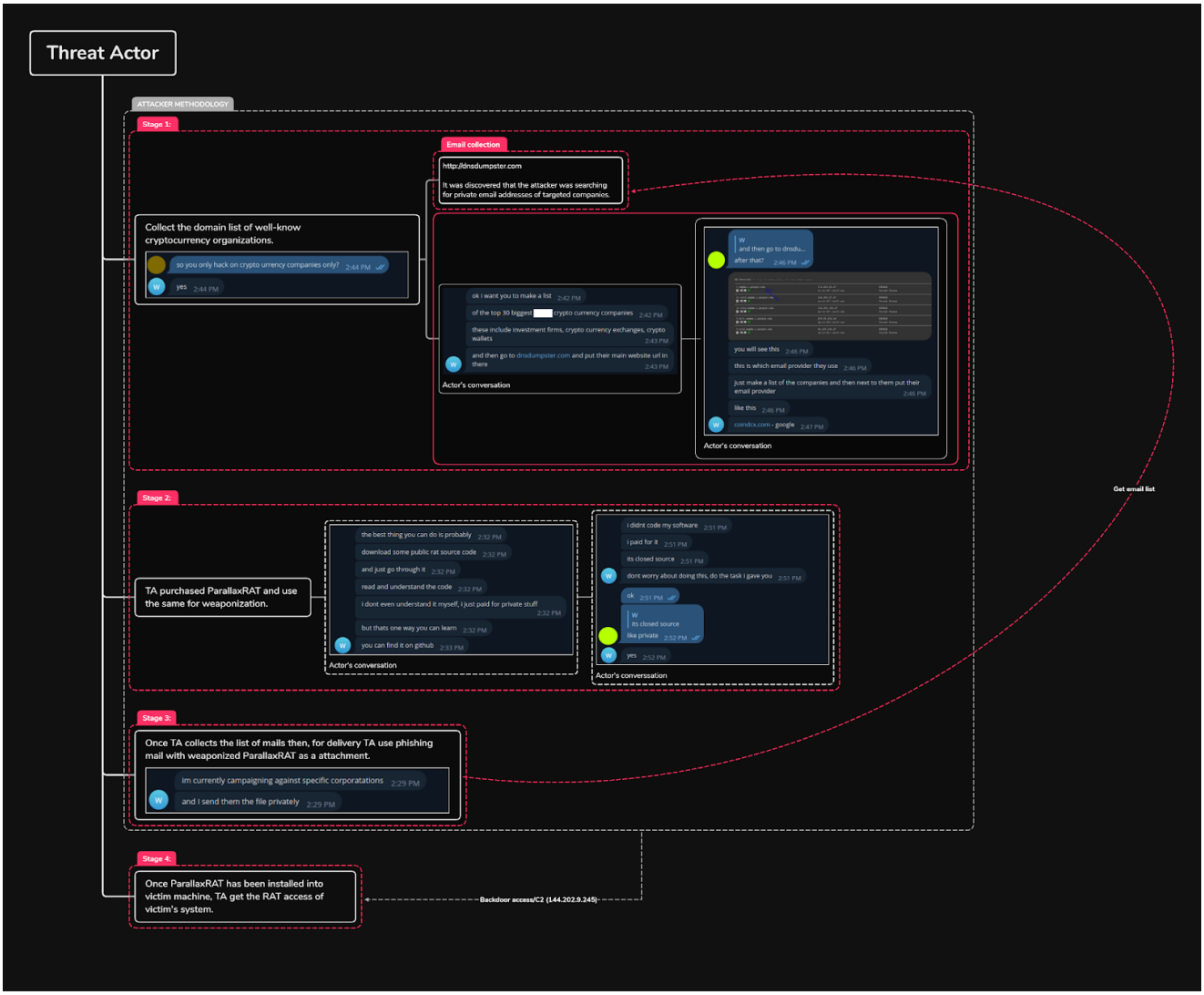

Figure 10: Telegram chat and attacker's mindmap

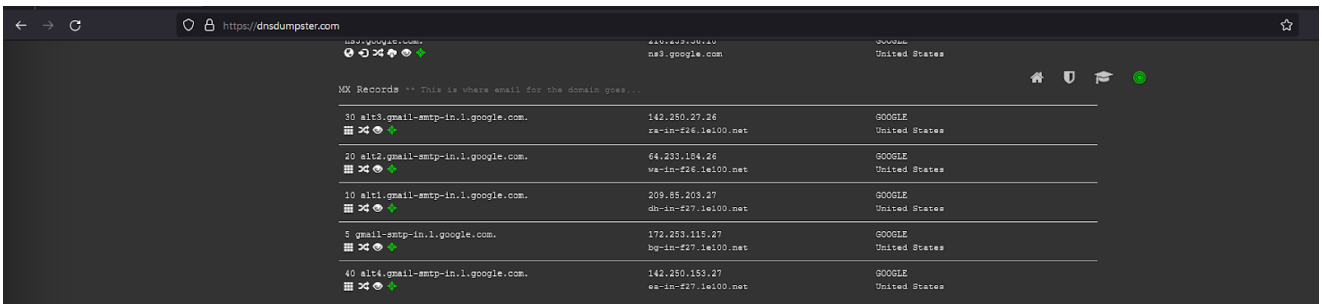

Figure 11: ParallaxRAT grabs target company info from public source

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).

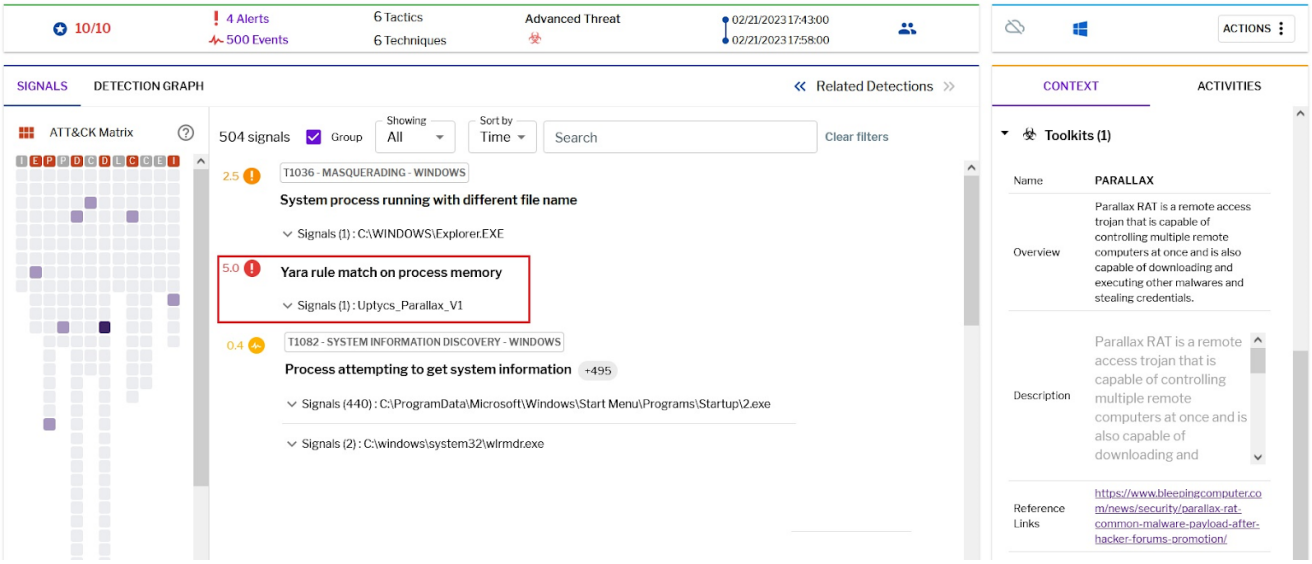

Figure 12: Uptycs EDR detection showing ParallaxRAT—YARA rule match

IOCs

File name	Md5 hash
Payload1	40256ea622aa1d0678f5bde48b9aa0fb
Payload2	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