QuasarRAT Dropper

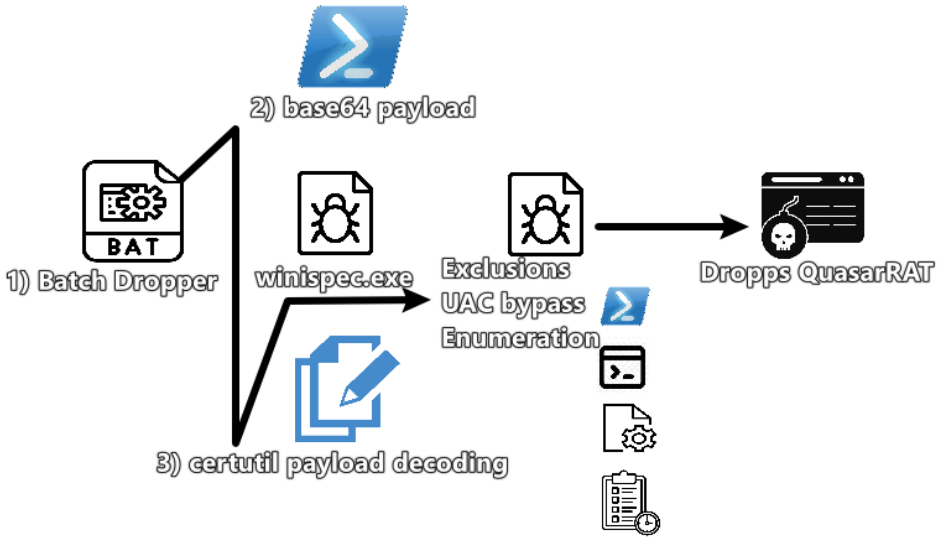
July 27, 2025
Author: BABAgala
https://www.linkedin.com/in/gal-akavia-7b1288201/

Key Takeaways

This report explores a newly identified dropper variant of QuasarRAT, a known remote access trojan, analysed for fun after downloading a malicious script from Bazaar.

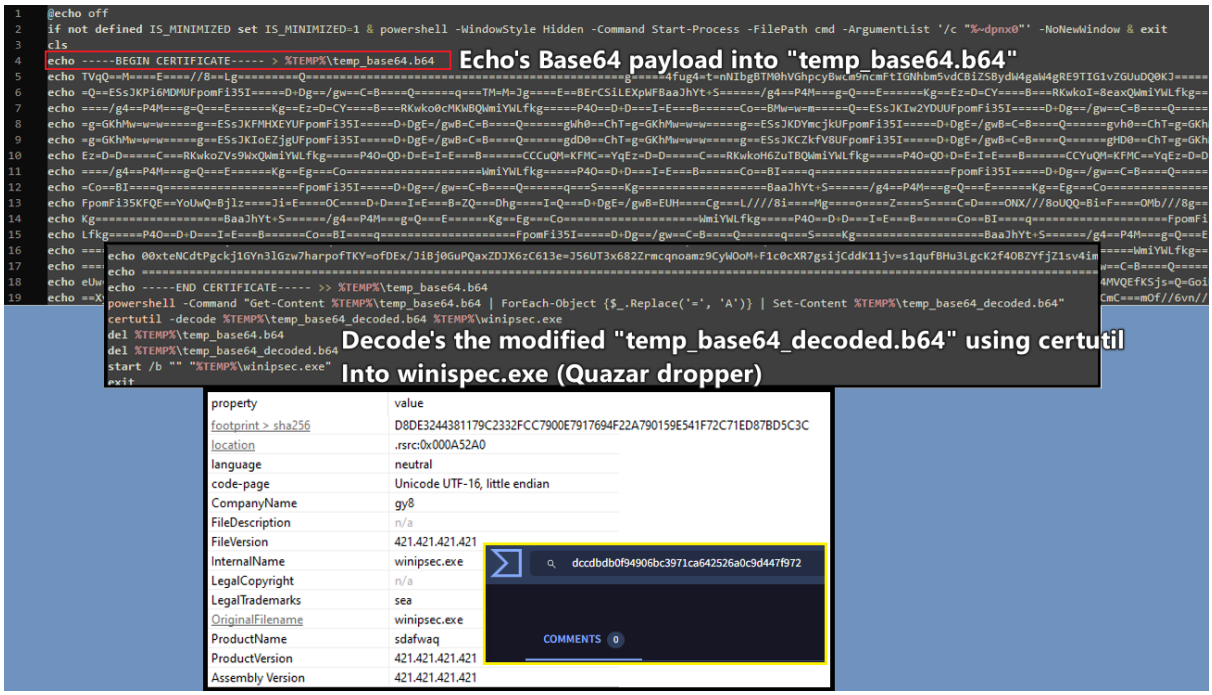
The investigation began with an unknown initial access method, but the attack chain unfolded through a batch script dropped and executed from the %temp% folder a highly obfuscated 64-bit .NET assembly written in C#, named “winispec.exe”. Subsequent stages execute entirely in memory, showcasing sophisticated evasion and persistence tactics.

- The malware (winispec.exe) modifies multiple registry keys to bypass UAC and elevate privileges, notably abusing ComputerDefaults.exe "LOLBAS" techniques, while establishing persistence through various methods.
- It enumerates device and user information via Hash Table techniques.
- Scans for security products by checking the etc/hosts file.
- Disrupt system settings by removing AppxPackage items.
- Finally, it deploys QuasarRAT as disgusted svchost.exe, which communicates with a Telegram bot and an attacker-controlled (C2) server.



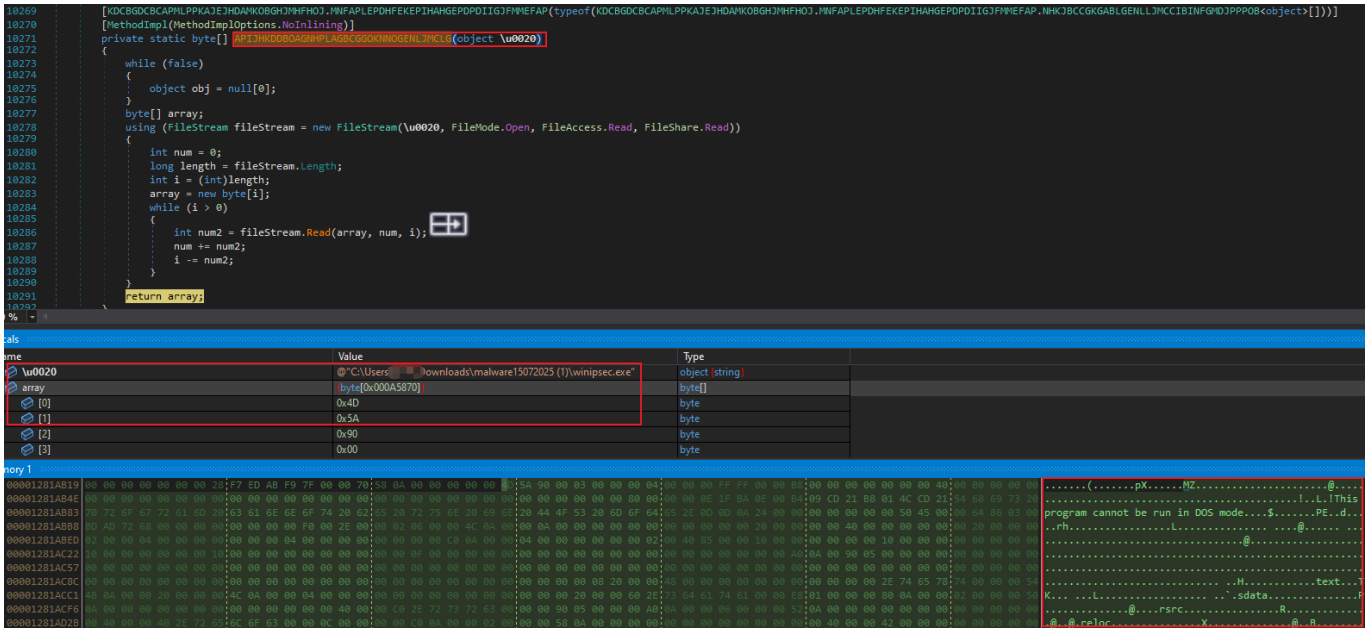
Analysis

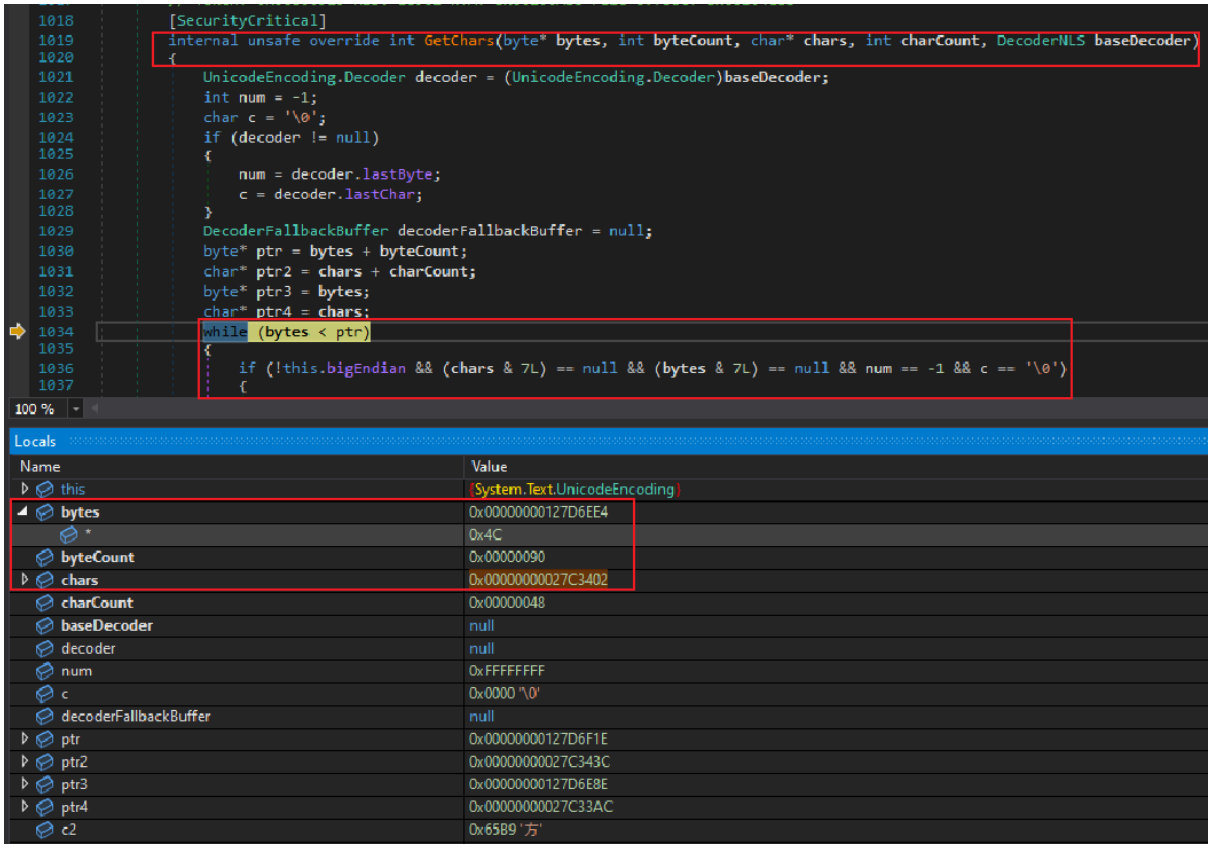
A batch script that decodes a Base64 payload using certutil.exe. The decoded output, a highly obfuscated 64-bit .NET assembly written in C# named winispec.exe, is dropped and executed from the %temp% folder. Correct for this analysis, the assembly isn't recognized in VT.



Unpacking

Upon execution, winispec.exe starts the unpacking process by pulling the entire byte stream into an array, using .NET `GetChars` Method, which decodes a sequence of bytes into a set of characters.

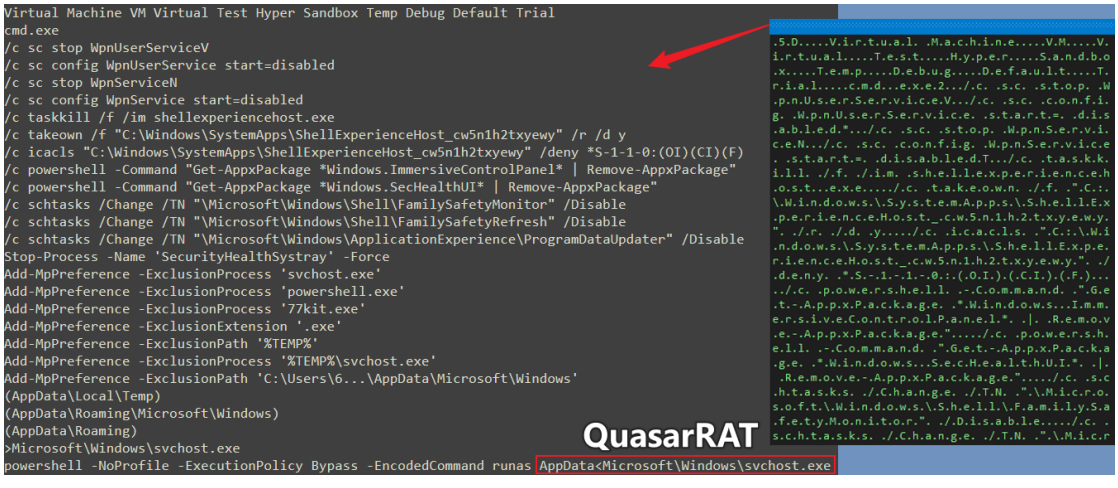




Defense Evasion

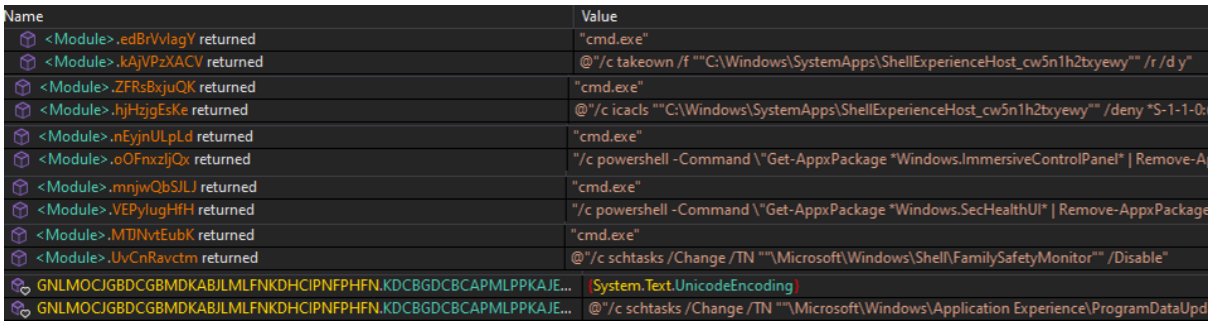
Then, winispec.exe will spawn cmd, PowerShell and Task-scheduler to execute a series of commands:

- Check for VM or sandboxing
- UAC bypass
- Disable user access to system and security settings
- Disable security notifications
- Adding exclusions to antivirus (svchost.exe - QuasarRAT)



Keep in mind, QuasarRAT will act from this stage as disguised svchost.exe, so I will refer to QuasarRAT as svchost.exe for the rest of the blogpost.

Obfuscated functions spawn more Microsoft native binaries.

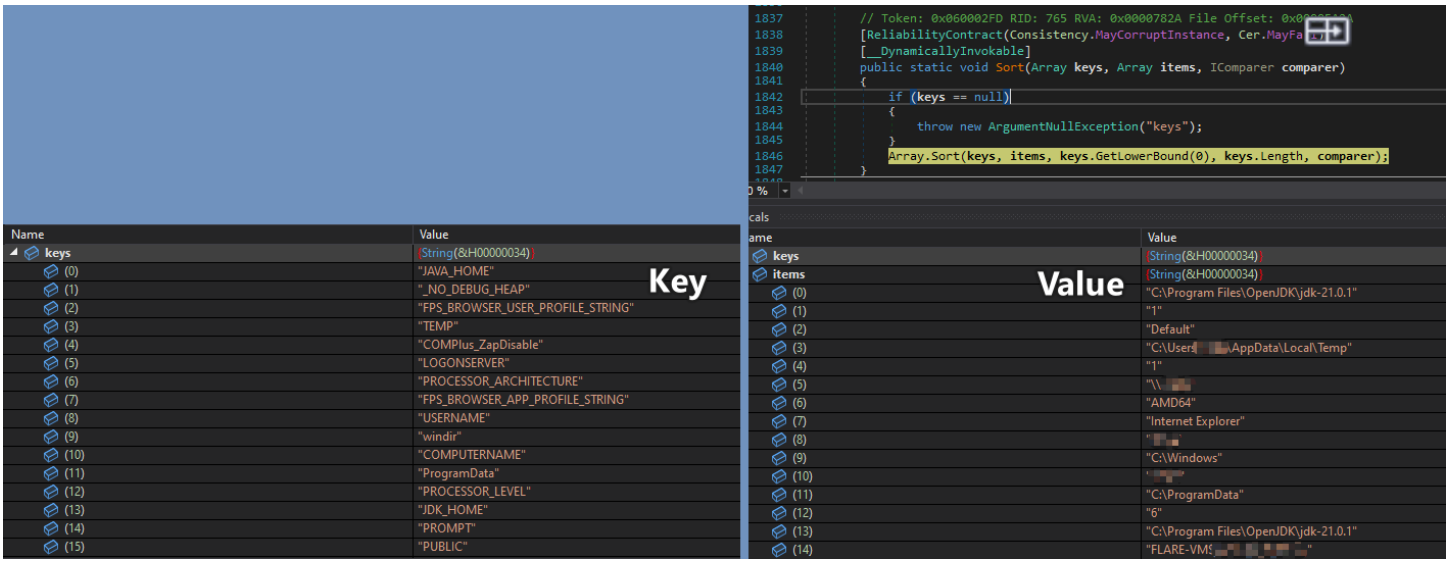


Full list –

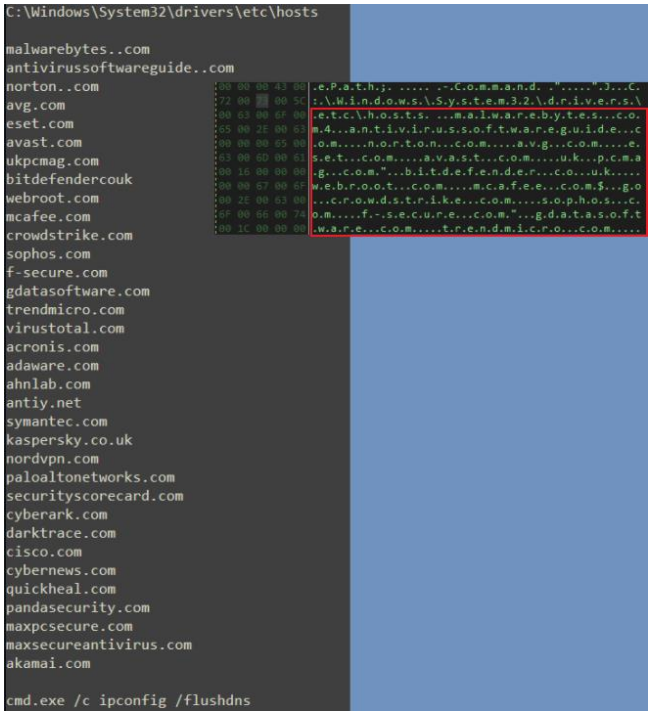
Command	Description
powershell –Command "Get–AppxPackage Windows.ImmersiveControlPanel	Remove–AppxPackage"
powershell –Command "Get–AppxPackage Windows.SecHealthUI	Remove–AppxPackage"
reg add "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" /v ConsentPromptBehaviorAdmin /t REG_DWORD /d 0 /f	Bypasses UAC for admin actions
reg add "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" /v EnableLUA /t REG_DWORD /d 0 /f	Disables UAC
reg add "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" /v PromptOnSecureDesktop /t REG_DWORD /d 0 /f	Disables UAC prompts
"cmd.exe" /c sc config WpnService start= disabled	Disables the Windows Push Notification Service (WpnService)
"cmd.exe" /c sc config WpnUserService start= disabled	Disables WpnUserService startup
"cmd.exe" /c sc stop WpnService	Stops security or system updates
"cmd.exe" /c sc stop WpnUserService	Stops real–time notifications to users
"cmd.exe" /c schtasks /Change /TN "\Microsoft\Windows\Application Experience\ProgramDataUpdater" /Disable	Prevents app compatibility updates
"cmd.exe" /c schtasks /Change /TN "\Microsoft\Windows\Shell\FamilySafetyMonitor" /Disable	Disable parents monitor and manage screen time and online activities.
"cmd.exe" /c schtasks /Change /TN "\Microsoft\Windows\Shell\FamilySafetyRefresh" /Disable	
Stop–Process –Name 'SecurityHealthSystray' –Force	Forces termination of the Security Health Systray (Windows Security tray icon)

Enumeration

Device enumeration performed by using the Hash-table key-value pairs data structure to map keys to indices for fast data retrieval and insertion.

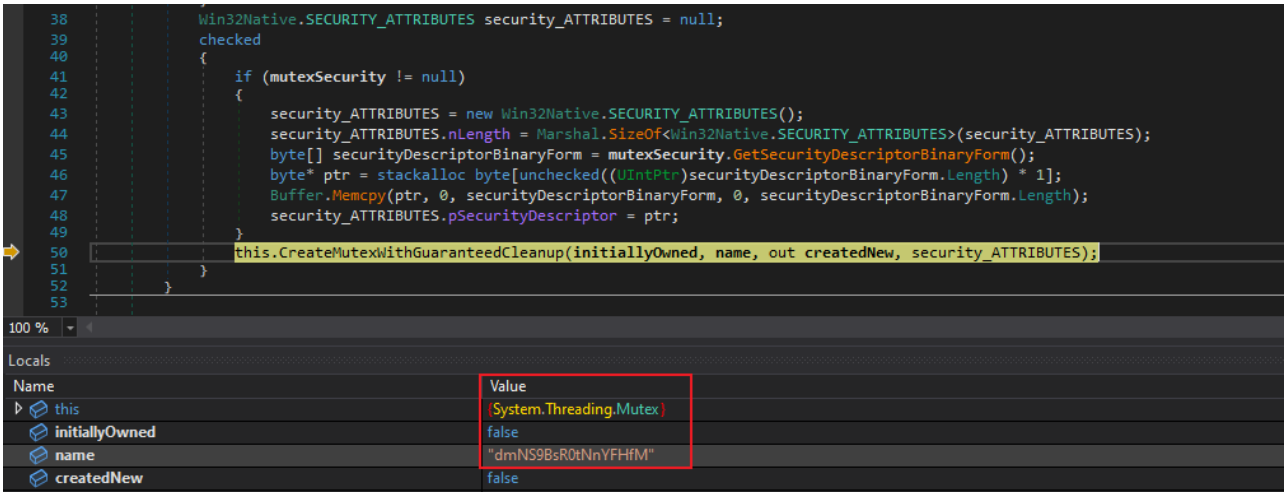


Next, winispec.exe access the local device DNS cache file in “/etc/hosts” and enumerates for a list of known security vendors, then it will flush the local DNS cache to potentially disrupt DNS caching using “ipconfig /flushdns”



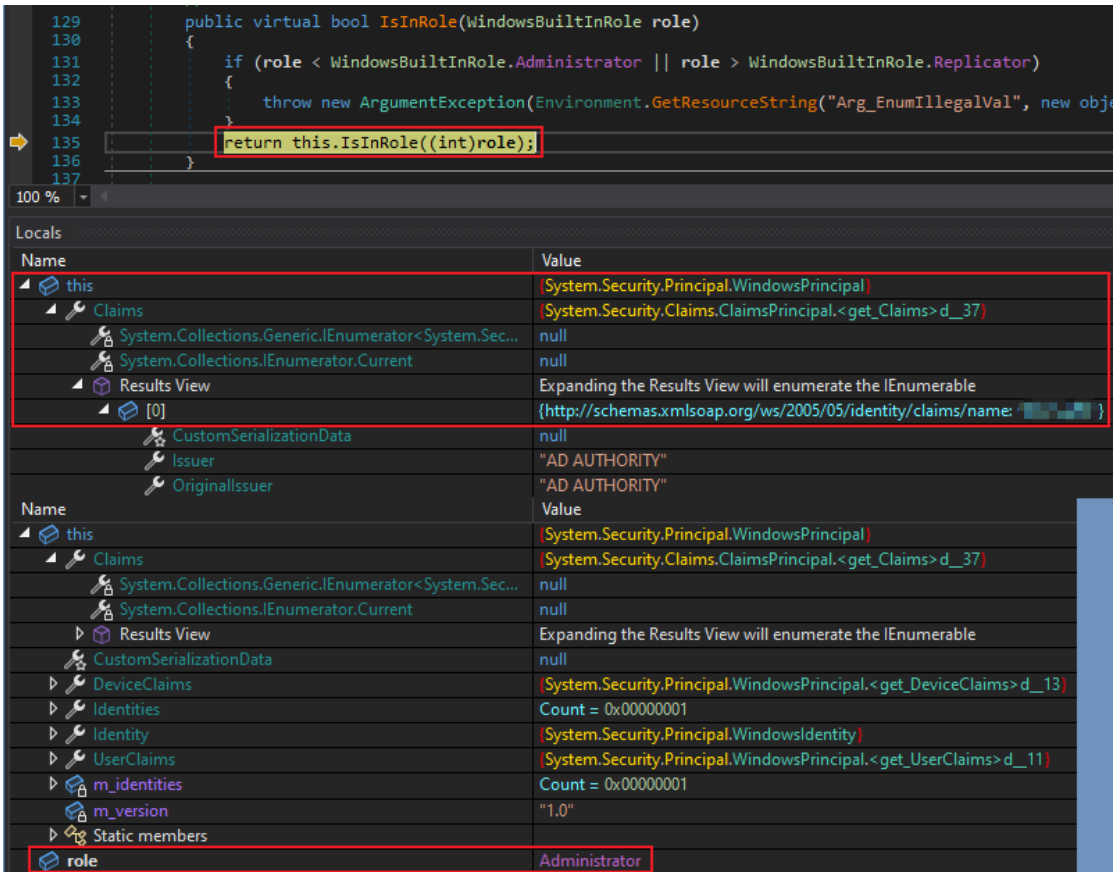
Snippets from the hosts file enumeration

Before it continues to the next stage, and performing registry manipulation, winispec.exe creates a Mutex, to ensure only one instance of itself runs at a time

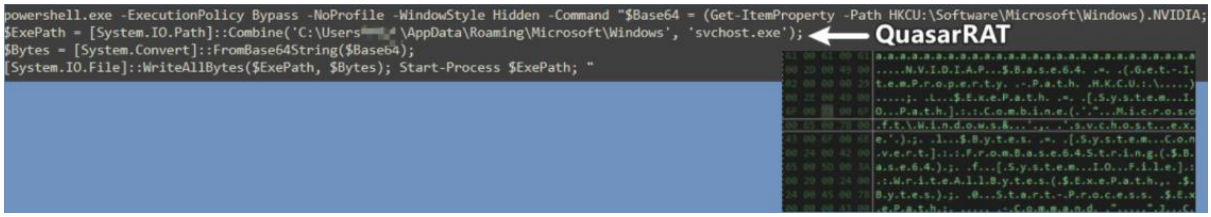


Execution

winispec.exe checks if the current user has an identity with specific security claims (e.g., Administrator role) using `IsInRole` and validates the user's identity claims (name, role, group SID, etc.) via `ClaimsIdentity`, likely to determine if it has elevated privileges or can escalate them.

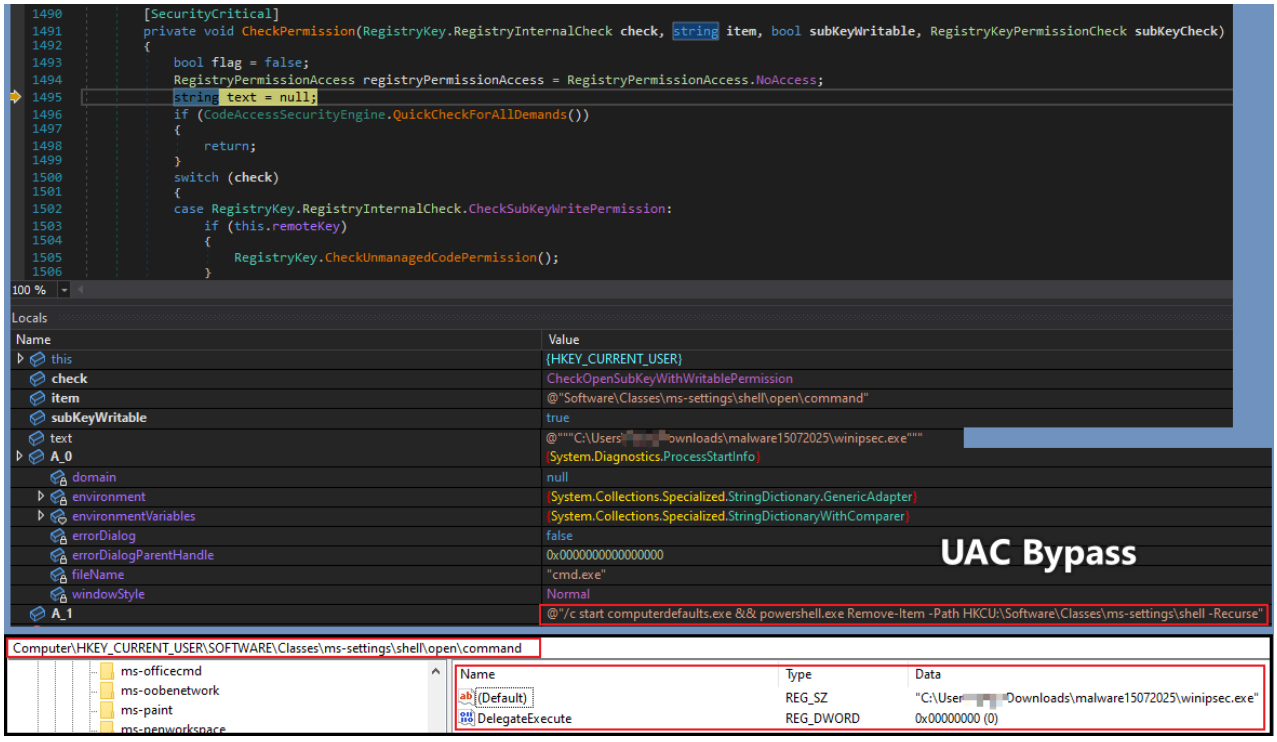


In the next stage, winispec.exe will decode a base64 payload written to HKCU:\Software\Microsoft\Windows\NVIDIA, use it to create a disguised svchost.exe.



Additionally, winispec.exe is added to HKEY_CURRENT_USER\Software\Classes\ms-settings\Shell\open\command.

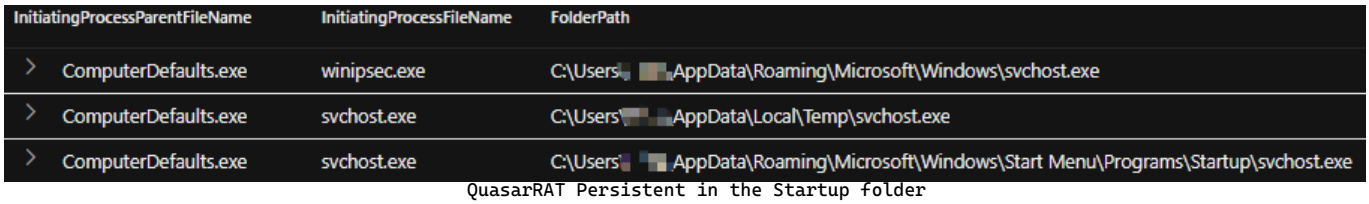
Known LOLBAS technique, upon execution, ComputerDefaults.exe checks this registry key, setting DelegateExecute to 0, allowing the custom command to execute instead, potentially running with elevated privileges without a UAC prompt.



Then it deletes the value in HKEY_CURRENT_USER\Software\Classes\ms-settings\Shell.

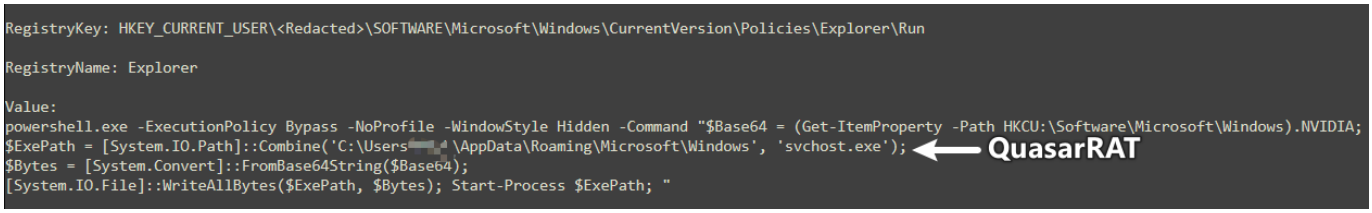
Persistent

ComputerDefaults.exe dropped “svchost.exe” from multiple locations on disk, maintained persistence in the Startup folder and the Run key –



InitiatingProcessParentFileName	InitiatingProcessFileName	FolderPath
ComputerDefaults.exe	winipsec.exe	C:\Users\ AppData\Roaming\Microsoft\Windows\svchost.exe
ComputerDefaults.exe	svchost.exe	C:\Users\ AppData\Local\Temp\svchost.exe
ComputerDefaults.exe	svchost.exe	C:\Users\ AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\svchost.exe

QuasarRAT Persistent in the Startup folder



QuasarRAT Persistent in the Run key

svchost.exe established network connection to Telegram and the attacker C2.

InitiatingProcessFolderPath	RemoteUrl	RemoteIP
c:\user \appdata\local\temp\svchost.exe	ip-api.com	208.95.112.1
c:\users \appdata\local\temp\svchost.exe	api.telegram.org	149.154.167.220
c:\users \appdata\local\temp\svchost.exe		104.248.130.195

Conclusion

Although this dropper is unknown to security vendors, defenders must monitor suspicious behavioral activity to detect and respond to threats effectively.

A Yara detection for that dropper on my GitHub

IOC’s

winispec.exe SHA1 dccdbdb0f94906bc3971ca642526a0c9d447f972

svchost.exe (QuasarRAT) SHA1 7f851a397bc819990ee1b6a1ebaaef6b08dd2e10

C2

104.248.130[.]195

api.telegram[.]org 149.154.167[.]220

Enjoy playing around with the sample – https://bazaar.abuse.ch/sample/46efff9950c02ea2c419f5aa19efa24cc9a7c6bdcf3e60497f59cedd0f00c86e/