Training Scenario - Data Enumeration

Group Name

Training Data - RAT Exfil (Quasar)

Scenario

In this training scenario, we will execute a RAT on the victim machine, and use it to enumerate the data on disk, with the goal of exfiltrating files.

While this is not a ransomware attack, the behaviors used by the RAT fall under the umbrella of the data extortion behaviors that Cyber Crucible detects. The response to the incident, and related data, look very similiar to that of the response to a ransomware payload, because to Cyber Crucible it’s all the same!

Identifying it

Number of Incidents	Machine Name	Program Path	Program Arguments
4	\\DESKTOP-GISR8SE	C:\Windows\System32\SubDir\Client.exe	

Created	Response Name	Untrusted Remote Threads	Modified Memory	No Trusted Cert
October 18, 2022 at 9:36:01 PM EDT	Polka-Dot-Plant Ferret Plum 868	False	False	True
October 18, 2022 at 9:38:54 PM EDT	Pearly-Everlasting Black-Footed-Rhino Aspar	False	False	True
October 18, 2022 at 9:39:03 PM EDT	Navy-Blue Sweet-Pea Ragdoll 542	False	False	True
October 18, 2022 at 9:39:07 PM EDT	Wildcat School-bus-yellow Balsam 541	False	False	True

This executable looks a bit odd, but it’s in system32 and triggering repeated responses. Some more investigation is required to figure out what happened here. We can start by looking for child paths related to the response path.

Parent Path	Parent Arguments	Child Path
C:\Windows\explorer.exe	C:\Windows\Explorer.EXE	C:\Users\user\Desktop\Client-built.exe
C:\Windows\System32\svchost.exe	C:\Windows\system32\svchost.exe -k netsvcs -p -s Appinfo	C:\Users\user\Desktop\Client-built.exe
C:\Users\user\Desktop\Client-built.exe	"C:\Users\user\Desktop\Client-built.exe"	C:\Windows\System32\SubDir\Client.exe

Here we get some more evidence to the story. A user ran the client-build.exe from the desktop, which is the RAT dropper. Then it looks like it privilege escalates via an svchost. There are still some missing pieces to the puzzle, though. How do we know this is a RAT and not just something interacting with svchost?

Parent Path	Parent Arguments	Child Path
C:\Windows\explorer.exe	C:\Windows\Explorer.EXE	C:\Users\user\Desktop\Client-built.exe
C:\Windows\System32\svchost.exe	C:\Windows\system32\svchost.exe -k DcomLaunch -p	C:\Windows\SysWOW64\dllhost.exe
C:\Windows\System32\svchost.exe	C:\Windows\system32\svchost.exe -k netsvcs -p -s Appinfo	C:\Windows\System32\consent.exe
C:\Windows\System32\svchost.exe	C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p	C:\Windows\System32\audiodg.exe
C:\Windows\System32\svchost.exe	C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s TabletInputService	C:\Program Files\Common Files\microsoft shared\ink\Tab
C:\Windows\System32\svchost.exe	C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s TabletInputService	C:\Program Files\Common Files\microsoft shared\ink\Tab
C:\Windows\System32\svchost.exe	C:\Windows\system32\svchost.exe -k netsvcs -p -s Appinfo	C:\Users\user\Desktop\Client-built.exe
C:\Users\user\Desktop\Client-built.exe	"C:\Users\user\Desktop\Client-built.exe"	C:\Windows\System32\schtasks.exe
C:\Windows\System32\schtasks.exe	"schtasks" /create /tn "Quasar Client Startup" /sc ONLOGON /tr "C:\Users\user\Desktop\Client-built.exe" /rl HIGHEST /f	C:\Windows\System32\conhost.exe
C:\Users\user\Desktop\Client-built.exe	"C:\Users\user\Desktop\Client-built.exe"	C:\Windows\System32\SubDir\Client.exe
C:\Windows\System32\SubDir\Client.exe	"C:\Windows\system32\SubDir\Client.exe"	C:\Windows\System32\schtasks.exe
C:\Windows\System32\schtasks.exe	"schtasks" /create /tn "Quasar Client Startup" /sc ONLOGON /tr "C:\Windows\system32\SubDir\Client.exe" /rl HIGHEST /f	C:\Windows\System32\conhost.exe

This opens up a whole lot more visibility! Not only do we know for sure that some suspicious activity is going on, and what paths are related, but we know there's persistence being created as well. And we even see that we're dealing with Quasar, a well known RAT.

Quasar is a sophisticated RAT, and does most of its behavior from within its own executable, choosing to bring its own statically compiled libraries rather than using Windows' default utilities for many things. But even Quasar gets caught using things like schtasks.

Relevant documentation

- Mitre T1566 - Phishing may be used to trick a user into performing an action they would not have done otherwise such as running a script or sharing a password.
- Mitre T1091 - Malware may replicate itself onto removable media so that the next machine to connect it may execute via autorun or driver vulnerabilities.
- Mitre T1204 - User execution, often gained via phishing, is the simplest way malware to begin execution.
- Mitre T1547 - Malware may instruct Windows to execute malicious programs on boot or when a user logs in.
- Mitre T1037 - Malware may instruct Windows to execute malicious scripts on boot or when a user logs in.

- Mitre T1543 - Creating or modifying a system process can disguise malicious code as a normal, trusted system process from malware detection.

Revision #2
Created 2026-07-13 18:48:57 UTC by Dennis Underwood
Updated 2026-07-13 18:49:01 UTC by Dennis Underwood