

Trainingsszenario – Datenenumeration

Gruppenname

Trainingsdaten - RAT-Exfiltration (Quasar)

Szenario

In diesem Trainingsszenario führen wir einen RAT auf der Opfermaschine aus und nutzen ihn, um die Daten auf der Festplatte zu enumerieren, mit dem Ziel, Dateien zu exfiltrieren.

Auch wenn es sich hierbei nicht um einen Ransomware-Angriff handelt, fallen die vom RAT verwendeten Verhaltensweisen unter die Kategorie der Datenerpressungsverhalten, die Cyber Crucible erkennt. Die Reaktion auf den Vorfall und die zugehörigen Daten sehen der Reaktion auf eine Ransomware-Payload sehr ähnlich, denn für Cyber Crucible ist das alles dasselbe!

Erkennung

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 Aspari	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

Diese ausführbare Datei sieht etwas eigenartig aus, befindet sich aber in system32 und löst wiederholte Reaktionen aus. Es sind weitere Untersuchungen erforderlich, um herauszufinden, was hier passiert ist. Wir können damit beginnen, nach untergeordneten Pfaden zu suchen, die mit dem Reaktionspfad in Zusammenhang stehen.

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

Hier erhalten wir weitere Hinweise zur Geschichte. Ein Benutzer hat client-build.exe vom Desktop aus ausgeführt, bei dem es sich um den RAT-Dropper handelt. Anschließend scheint eine Privilegienerweiterung über einen svchost stattzufinden. Es fehlen jedoch noch einige Teile des Puzzles. Woher wissen wir, dass es sich um einen RAT handelt und nicht nur um etwas, das mit svchost interagiert?

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\dlhost.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

Dies eröffnet eine ganze Menge mehr an Transparenz! Wir wissen nun nicht nur mit Sicherheit, dass verdächtige Aktivitäten im Gange sind und welche Pfade damit zusammenhängen, sondern auch, dass Persistenz erzeugt wird. Und wir sehen sogar, dass wir es mit Quasar zu tun haben, einem bekannten RAT.

Quasar ist ein hochentwickelter RAT und führt die meisten seiner Verhaltensweisen innerhalb seiner eigenen ausführbaren Datei aus, wobei er für viele Zwecke lieber seine eigenen statisch kompilierten Bibliotheken mitbringt, anstatt die Standardwerkzeuge von Windows zu verwenden. Aber selbst Quasar wird erwischt, wenn er Dinge wie schtasks verwendet.

Relevante Dokumentation

- [Mitre T1566](#) - Phishing kann verwendet werden, um einen Benutzer dazu zu bringen, eine Aktion auszuführen, die er sonst nicht durchgeführt hätte, wie z. B. das Ausführen eines Skripts oder das Weitergeben eines Passworts.
- [Mitre T1091](#) - Malware kann sich selbst auf Wechseldatenträger replizieren, sodass der nächste Rechner, an den dieser angeschlossen wird, sie über Autorun oder Treiber-Schwachstellen ausführen kann.

- [Mitre T1204](#) - Benutzerausführung, oft durch Phishing erreicht, ist der einfachste Weg für Malware, mit der Ausführung zu beginnen.
 - [Mitre T1547](#) - Malware kann Windows anweisen, bösartige Programme beim Booten oder bei der Benutzeranmeldung auszuführen.
 - [Mitre T1037](#) - Malware kann Windows anweisen, bösartige Skripte beim Booten oder bei der Benutzeranmeldung auszuführen.
 - [Mitre T1543](#) - Das Erstellen oder Verändern eines Systemprozesses kann bösartigen Code als normalen, vertrauenswürdigen Systemprozess vor der Malware-Erkennung tarnen.
-

Revision #1

Created 2026-07-24 03:55:40 UTC by Dennis Underwood

Updated 2026-07-24 03:55:40 UTC by Dennis Underwood