

Scénario de formation - Énumération de données

Nom du groupe

Training Data - RAT Exfil (Quasar)

Scénario

Dans ce scénario de formation, nous allons exécuter un RAT sur la machine victime, et l'utiliser pour énumérer les données présentes sur le disque, dans le but d'exfiltrer des fichiers.

Bien qu'il ne s'agisse pas d'une attaque par ransomware, les comportements utilisés par le RAT relèvent des comportements d'extorsion de données que Cyber Crucible détecte. La réponse à l'incident, ainsi que les données associées, ressemblent beaucoup à celles de la réponse à une charge utile de ransomware, car pour Cyber Crucible, tout cela revient au même !

Identification

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

Cet exécutable semble un peu étrange, mais il se trouve dans system32 et déclenche des réponses répétées. Une investigation plus approfondie est nécessaire pour comprendre ce qui s'est passé ici. Nous pouvons commencer par rechercher les chemins enfants liés au chemin de réponse.

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

Ici, nous obtenons davantage d'éléments pour reconstituer l'histoire. Un utilisateur a exécuté client-build.exe depuis le bureau, qui est le dropper du RAT. Ensuite, il semble qu'il y ait une élévation de privilèges via un svchost. Il manque toutefois encore quelques pièces au puzzle. Comment savons-nous qu'il s'agit d'un RAT et non simplement d'un élément interagissant avec 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\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\audiogd.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

Cela offre une bien meilleure visibilité ! Non seulement nous savons désormais avec certitude qu'une activité suspecte est en cours, ainsi que les chemins associés, mais nous savons également qu'une persistance est créée. Et nous constatons même que nous avons affaire à Quasar, un RAT bien connu.

Quasar est un RAT sophistiqué, qui exécute la majeure partie de ses comportements depuis son propre exécutable, préférant intégrer ses propres bibliothèques compilées statiquement plutôt que d'utiliser les utilitaires par défaut de Windows pour de nombreuses opérations. Mais même Quasar se fait repérer en utilisant des outils comme schtasks.

Documentation pertinente

- [Mitre T1566](#) - Le phishing peut être utilisé pour inciter un utilisateur à effectuer une action qu'il n'aurait pas effectuée autrement, comme exécuter un script ou partager un mot de passe.
- [Mitre T1091](#) - Un logiciel malveillant peut se répliquer sur un support amovible afin que la prochaine machine sur laquelle il est connecté puisse l'exécuter via l'exécution automatique ou des vulnérabilités de pilotes.

- [Mitre T1204](#) - L'exécution par l'utilisateur, souvent obtenue via le phishing, est le moyen le plus simple pour un logiciel malveillant de commencer son exécution.
 - [Mitre T1547](#) - Un logiciel malveillant peut demander à Windows d'exécuter des programmes malveillants au démarrage ou lorsqu'un utilisateur se connecte.
 - [Mitre T1037](#) - Un logiciel malveillant peut demander à Windows d'exécuter des scripts malveillants au démarrage ou lorsqu'un utilisateur se connecte.
 - [Mitre T1543](#) - La création ou la modification d'un processus système peut permettre de déguiser un code malveillant en un processus système normal et de confiance, afin d'échapper à la détection des logiciels malveillants.
-

Revision #1

Created 2026-07-24 06:20:50 UTC by Dennis Underwood

Updated 2026-07-24 06:20:51 UTC by Dennis Underwood