Escenario de Capacitación - Enumeración de Datos

Nombre del Grupo

Datos de Capacitación - Exfiltración mediante RAT (Quasar)

Escenario

En este escenario de capacitación, ejecutaremos un RAT en la máquina víctima y lo utilizaremos para enumerar los datos en disco, con el objetivo de exfiltrar archivos.

Si bien esto no es un ataque de ransomware, los comportamientos utilizados por el RAT se encuadran dentro de los comportamientos de extorsión de datos que Cyber Crucible detecta. La respuesta al incidente, y los datos relacionados, se parecen mucho a los de la respuesta a una carga útil de ransomware, ¡porque para Cyber Crucible todo es lo mismo!

Identificándolo

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

Este ejecutable se ve un poco extraño, pero está en system32 y está desencadenando respuestas repetidas. Se requiere más investigación para descubrir qué sucedió aquí. Podemos comenzar buscando rutas secundarias relacionadas con la ruta de respuesta.

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

Aquí obtenemos más evidencia de la historia. Un usuario ejecutó client-build.exe desde el escritorio, que es el dropper del RAT. Luego, parece que se produce una escalada de privilegios a través de un svchost. Sin embargo, todavía faltan algunas piezas del rompecabezas. ¿Cómo sabemos que esto es un RAT y no simplemente algo interactuando con 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

¡Esto abre mucha más visibilidad! No solo sabemos con certeza que hay actividad sospechosa en curso, y qué rutas están relacionadas, sino que sabemos que también se está creando persistencia. E incluso vemos que estamos tratando con Quasar, un RAT muy conocido.

Quasar es un RAT sofisticado, y realiza la mayor parte de su comportamiento desde dentro de su propio ejecutable, optando por traer sus propias bibliotecas compiladas estáticamente en lugar de utilizar las utilidades predeterminadas de Windows para muchas cosas. Pero incluso Quasar es detectado utilizando herramientas como schtasks.

Documentación relevante

- Mitre T1566 - El phishing puede utilizarse para engañar a un usuario para que realice una acción que de otro modo no habría llevado a cabo, como ejecutar un script o compartir una contraseña.
- Mitre T1091 - El malware puede replicarse a sí mismo en medios extraíbles para que la próxima máquina que se conecte a ellos pueda ejecutarlo mediante autorun o vulnerabilidades de controladores.
- Mitre T1204 - La ejecución por parte del usuario, a menudo obtenida mediante phishing, es la forma más sencilla en que el malware comienza su ejecución.

- Mitre T1547 - El malware puede indicarle a Windows que ejecute programas maliciosos al arrancar o cuando un usuario inicia sesión.
- Mitre T1037 - El malware puede indicarle a Windows que ejecute scripts maliciosos al arrancar o cuando un usuario inicia sesión.
- Mitre T1543 - Crear o modificar un proceso del sistema puede disfrazar código malicioso como un proceso del sistema normal y confiable, evitando así la detección de malware.

Revision #1
Created 2026-07-24 01:14:18 UTC by Dennis Underwood
Updated 2026-07-24 01:14:18 UTC by Dennis Underwood