

Escenario de Capacitación - Inyección de Procesos

Nombre del Grupo

Datos de Capacitación - Inyección de Procesos (Hive)

Escenario

En este escenario de capacitación, ejecutaremos una carga útil de ransomware mediante inyección de procesos en un Svchost.exe que ya está en ejecución. El Svchost en cuestión es una operación normal del sistema, de larga duración, firmada, y bajo la cuenta de usuario LocalSystem.

Debido a que el Svchost es 'real', a menudo se pasa por alto. Los administradores saben que se ejecutan muchas instancias de Svchost, y mientras los argumentos del programa parezcan correctos, se trata como una "caja negra" y se deja en paz. Este es un vacío obvio, y frecuentemente explotado, que los hackers aprovechan. Combinado con una carga útil de día cero, este enfoque tiene mucho éxito para ofuscar ataques de ransomware.

Identificándolo

Number of Incidents	Machine Name	Program Path	Program Arguments
▼ 1	\\CC-NOAH-TEST	C:\Windows\System32\svchost.exe	-k UnistackSvcGroup

Created	Response Name	Untrusted Remote Threads	Modified Memory	No Trusted Cert
October 18, 2022 at 9:16:41 PM EDT	    Royal-purple Komc	True	False	False



La situación en torno a esta respuesta automatizada no es evidente a primera vista. Los argumentos de la línea de comandos parecen válidos para Svchost, y el ejecutable está firmado por Microsoft.

El hecho de que exista un subproceso remoto no confiable es sospechoso, pero requiere más investigación. Muchos subprocesos remotos ocurren en un sistema, pero la mayoría permanecen "confiables" ya que se utilizan para la comunicación entre procesos normal, el uso compartido de datos, etc.

Cuando se crea un subproceso remoto en un proceso de manera anormal, y se marca como no confiable, es ahí donde debemos examinar con mayor detenimiento.

Injector Pid	Injector Path	Injectee Pid	Injectee Path ↑
3992	C:\Windows\System32\csrss.exe	8844	C:\Windows\System32\cmd.exe
4228	C:\Windows\System32\dwm.exe	3992	C:\Windows\System32\csrss.exe
3268	C:\Windows\System32\dwm.exe	5972	C:\Windows\System32\csrss.exe
4228	C:\Windows\System32\dwm.exe	3992	C:\Windows\System32\csrss.exe

Inyecciones de procesos inocuas que ocurren normalmente

Para poder clasificar las numerosas inyecciones de procesos que ocurren en un sistema en un momento dado, podemos referirnos tanto al momento del incidente como al pid del proceso marcado. Normalmente comenzaremos con algunos pids de respuestas sospechosas, y subiremos por la cadena de inyecciones y creación para obtener la historia completa.

Response Details



Description	Value
Response Name	Royal-purple Komodo-Dragon Lavender 848
Machine Name	\\CC-NOAH-TEST
Program Path	C:\Windows\System32\svchost.exe
Program Arguments	-k UnistackSvcGroup
Agent Name	
Ram usage	0
File access count	0
Number of threads	0
Pid	6224

[View Certificate Publisher Names](#)

Injectee Pid ▾

6224

⋮ ▾ ☰

Equals ▾

6224

Reset Apply

Filtrando inyecciones irrelevantes

Injector Pid	Injector Path	Injectee Pid ▾	Injectee Path ↑
9168	C:\svchost_injector.exe	6224	C:\Windows\System32\svchost.exe

¡La prueba irrefutable!

Ya sabemos que nadie debería inyectar en Svchost de esta manera, ¡pero definitivamente no en este proceso! A partir de aquí podemos tratar este proceso como si fuera "malware.exe" y ver quién lo ejecutó, ya que alguien debió haberlo hecho.

Created ↑	Child Pid ▾	Parent Path	Child Path
October 18, 2022 at 9:11:09 PM EDT	9168	C:\Windows\System32\services.exe	C:\Program Files (x86)\Dropbox\Update\DropboxUpdate.exe
October 18, 2022 at 9:16:04 PM EDT	9168	C:\Windows\explorer.exe	C:\svchost_injector.exe

Procesos iniciados con el pid 9168

Dado que hubo dos creaciones de procesos con el pid 9168, y son muy diferentes, podemos reducir la búsqueda basándonos en la marca de tiempo y/o la ruta secundaria, y ver que fue creado por un explorer.exe. Esto significa que alguien ejecutó manualmente el proceso inyector, y no puede ser alguna coincidencia de un comportamiento de Svchost que fue marcado incorrectamente.

Documentación relevante

- **Inyección de Procesos**

- [Mitre T1559](#) - La comunicación entre procesos puede proporcionar control sobre el proceso objetivo desde el inyector una vez que la inyección se ha completado.
- [Mitre T1106](#) - Las API nativas suelen ser el acceso más directo a la funcionalidad del sistema operativo para acceder a archivos, ejecutar procesos, y más.
- [Mitre T1569](#) - Inyectar en un servicio del sistema como un svchost existente puede disfrazar código malicioso para que se reporte como ejecutándose desde un proceso conocido y confiable.
- [Mitre T1055](#) - Inyección de procesos, generalmente utilizada para ejecutar código malicioso en un proceso objetivo mientras se permite que el proceso original continúe.

Revision #1

Created 2026-07-24 01:14:41 UTC by Dennis Underwood

Updated 2026-07-24 01:14:41 UTC by Dennis Underwood