Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

Cisco Talos comparte información relacionada con un ciberataque reciente a Cisco.

10/Agosto/2022

Contenido

INTRODUCCIÓN

Mediante este boletín, compartimos con usted la información brindada por Cisco en la cual confirman haber sido victimas de un ataque a su red interna y comparten sus hallazgos e indicadores de compromiso con toda la comunidad.

Ataque en contra de Cisco.

A continuación, se encuentra en cuadro de identificación de la amenaza.

ID de alerta:	DSOC-CERT_2022_08_10_01
Clasificación de alerta:	Noticia
Tipo de Impacto:	ALTO
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	08/10/2022
Es día cero (0 day):	NO

Resumen

El acceso inicial a Cisco VPN se logró mediante el compromiso exitoso de la cuenta personal de Google de un empleado de Cisco. El usuario había habilitado la sincronización de contraseñas a través de Google Chrome y había almacenado sus credenciales de Cisco en su navegador, lo que permitió que esa información se sincronizara con su cuenta de Google. Después de obtener las credenciales del usuario, el atacante intentó eludir la autenticación multifactor (MFA) utilizando una variedad de técnicas, incluido el phishing de voz (también conocido como "vishing") y la fatiga de MFA, el proceso de envío de un gran volumen de solicitudes de inserción al dispositivo móvil del objetivo. hasta que el usuario acepte, ya sea accidental o simplemente para intentar silenciar las notificaciones automáticas repetidas que está recibiendo. El vishing es una técnica de ingeniería social cada vez más común mediante la cual los atacantes intentan engañar a los empleados para que divulguen información confidencial por teléfono. En este caso, un empleado informó que recibió varias llamadas durante varios días en las que las personas que llamaban, que hablaban en inglés con varios acentos y dialectos internacionales, pretendían estar asociadas con organizaciones de apoyo en las que confiaba el usuario.

Una vez que el atacante obtuvo el acceso inicial, inscribió una serie de nuevos dispositivos para MFA y se autenticó con éxito en la VPN de Cisco. Luego, el atacante escaló a los privilegios administrativos, lo que le permitió iniciar sesión en múltiples sistemas, lo que alertó a nuestro Equipo de Respuesta a Incidentes de Seguridad de Cisco (CSIRT), quien posteriormente respondió al incidente. El actor en cuestión dejó caer una variedad de herramientas, incluidas herramientas de acceso remoto como LogMeIn y TeamViewer, herramientas de seguridad ofensivas como Cobalt Strike, PowerSploit, Mimikatz e Impacket, y agregó sus propias cuentas traseras y mecanismos de persistencia.

TTP POSTERIORES AL COMPROMISO.

Luego del acceso inicial al entorno, el actor de amenazas llevó a cabo una variedad de actividades con el fin de mantener el acceso, minimizar los artefactos forenses y aumentar su nivel de acceso a los sistemas dentro del entorno.

Una vez en un sistema, el actor de amenazas comenzó a enumerar el entorno, utilizando las utilidades comunes integradas de Windows para identificar la configuración de membresía de usuario y grupo del sistema, el nombre de host e identificar el contexto de la cuenta de usuario bajo la cual estaban operando. Periódicamente observamos que el atacante emitía comandos que contenían errores tipográficos, lo que indicaba que se estaba produciendo una interacción manual del operador dentro del entorno.

Después de establecer el acceso a la VPN, el atacante comenzó a usar la cuenta de usuario comprometida para iniciar sesión en una gran cantidad de sistemas antes de comenzar a adentrarse más en el entorno. Se trasladaron al entorno Citrix, comprometiendo una serie de servidores Citrix y finalmente obtuvieron acceso privilegiado a los controladores de dominio.

Después de obtener acceso a los controladores de dominio, el atacante comenzó a intentar volcar NTDS de ellos usando "ntdsutil.exe" de acuerdo con la siguiente sintaxis:

```
powershell ntdsutil.exe 'ac i ntds' 'ifm' 'create full c:\users\public' q q
```

Luego intentaron exfiltrar el NTDS descargado a través de SMB (TCP/445) desde el controlador de dominio al sistema VPN bajo su control.

Después de obtener acceso a las bases de datos de credenciales, se observó que el atacante aprovechaba las cuentas de las máquinas para la autenticación privilegiada y el movimiento lateral en el entorno.

De acuerdo con la actividad observada anteriormente en otros ataques separados pero similares, el adversario creó un usuario administrativo llamado "z" en el sistema usando los comandos integrados de Windows "net.exe". Luego, esta cuenta se agregó al grupo de administradores locales. También observamos instancias en las que el actor de amenazas cambió la contraseña de las cuentas de usuario locales existentes. En particular, se ha observado la creación de la cuenta "z" por parte de este actor en compromisos previos a la invasión rusa de Ucrania.

El atacante aprovechó con frecuencia las técnicas de omisión de inicio de sesión de Windows para mantener la capacidad de acceder a los sistemas del entorno con privilegios elevados. Con frecuencia confiaban en PSEXESVC.exe para agregar de forma remota los siguientes valores de clave del Registro:

```
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution
Options\narrator.exe /v Debugger /t REG_SZ /d C:\windows\system32\cmd.exe /f
```

```
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution
Options\sethc.exe /v Debugger /t REG_SZ /d C:\windows\system32\cmd.exe /f
```

Esto permitió al atacante aprovechar las características de accesibilidad presentes en la pantalla de inicio de sesión de Windows para generar un símbolo del sistema a nivel de SISTEMA, otorgándole el control completo de los sistemas. En varios casos, observamos que el atacante agregaba estas claves pero no interactuaba más con el sistema, posiblemente como un mecanismo de persistencia para ser utilizado más adelante cuando se revoca su acceso privilegiado principal.

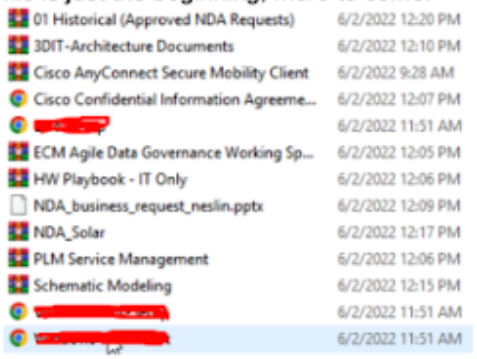
En las semanas posteriores a la expulsión del atacante del entorno, observamos continuos intentos de restablecer el acceso. En la mayoría de los casos, se observó que el atacante apuntaba a una higiene de rotación de contraseñas débil luego de los restablecimientos obligatorios de contraseñas de los empleados. Se dirigieron principalmente a usuarios que creían que habrían realizado cambios de un solo carácter en sus contraseñas anteriores, intentando aprovechar estas credenciales para autenticarse y recuperar el acceso a la VPN de Cisco. El atacante inicialmente estaba aprovechando los servicios de anonimización del tráfico como Tor; sin embargo, después de experimentar un éxito limitado, cambiaron para intentar establecer nuevas sesiones de VPN desde el espacio de IP residencial usando cuentas previamente comprometidas durante las etapas iniciales del ataque.

From: [redacted]
Date: Saturday, July 30, 2022 at 8:51 AM
To: [redacted]
Subject: Re: Cisco incident 5/28

We are giving you a very good deal. no one will know about the incident and information leakage if you pay us.

June 13, 2022 7:17:02 PM CEST [redacted] wrote:

> How are you?
>
> June 3, 2022 9:27:46 AM CEST [redacted] wrote:
>
> > This is just the beginning, more to come.



ANÁLISIS DE PUERTA TRASERA

El actor dejó caer una serie de cargas útiles en los sistemas, que continuamos analizando. La primera carga útil es una puerta trasera simple que toma comandos de un servidor de comando y control (C2) y los ejecuta en el sistema final a través del procesador de comandos de Windows. Los comandos se envían en blobs JSON y son estándar para una puerta trasera. Hay un comando "DELETE_SELF" que elimina completamente la puerta trasera del sistema. Otro comando, más interesante, "LIMPIAR", indica a la puerta trasera que elimine de la memoria el último comando ejecutado, probablemente con la intención de afectar negativamente el análisis forense en cualquier host afectado.

El malware también crea un archivo llamado "bdata.ini" en el directorio de trabajo actual del malware que contiene un valor derivado del número de serie del volumen presente en el sistema infectado. En los casos en que se ejecutó esta puerta trasera. se observó que el malware se ejecutaba desde la siguiente ubicación del directorio:

```
C:\usuarios\público\win\cmd.exe
```

Se observó con frecuencia que el atacante preparaba herramientas en ubicaciones de directorio bajo el perfil de usuario público en los sistemas desde los que estaba operando.

Según el análisis de la infraestructura C2 asociada con esta puerta trasera, se evalúa que el servidor C2 se configuró específicamente para este ataque.

ATRIBUCIÓN DE ATAQUE

Con base en los artefactos obtenidos, las tácticas, técnicas y procedimientos (TTP) identificados, la infraestructura utilizada y un análisis exhaustivo de la puerta trasera utilizada en este ataque, se evaluó con una confianza moderada a alta que este ataque fue realizado por un adversario que ha sido previamente identificado como un corredor de acceso inicial (IAB) con vínculos tanto con UNC2447 como con Lapsus$. Las IAB generalmente intentan obtener acceso privilegiado a los entornos de redes corporativas y luego monetizar ese acceso vendiéndolo a otros actores de amenazas que luego pueden aprovecharlo para una variedad de propósitos. También se observa actividad anterior que vincula a este actor de amenazas con la pandilla de ransomware Yanluowang, incluido el uso del sitio de fuga de datos de Yanluowang para publicar datos robados de organizaciones comprometidas.

UNC2447 es un actor de amenazas motivado financieramente con un nexo con Rusia que se ha observado anteriormente realizando ataques de ransomware y aprovechando una técnica conocida como "doble extorsión", en la que los datos se extraen antes de la implementación del ransomware en un intento de obligar a las víctimas a pagar el rescate. demandas. Informes anteriores indican que se ha observado que UNC2447 opera una variedad de ransomware, incluidos FIVEHANDS, HELLOKITTY y más.

Aparte de UNC2447, algunos de los TTP descubiertos durante el curso de la investigación coinciden con los de Lapsus$. Lapsus$ es un grupo de actores de amenazas que, según se informa, ha sido responsable de varias infracciones notables anteriores de entornos corporativos.

MAPEO DE MITRE ATT&CK

Todos los TTP descritos anteriormente que se observaron en este ataque se enumeran a continuación según la fase del ataque en la que ocurrieron.

Acceso inicial

Técnica ATT&CK: Phishing (T1566)

Técnica ATT&CK: Cuentas válidas (T1078)

Ejecución

Técnica ATT&CK: Servicios del sistema: Ejecución del servicio (T1569.002)

Persistencia

Técnica ATT&CK: Crear cuenta: Cuenta local (T1136.001)

Técnica ATT&CK: Manipulación de cuenta: Registro de dispositivo (T1098.005)

Escalada de privilegios

Técnica ATT&CK: Ejecución activada por evento: Inyección de opciones de ejecución de archivo de imagen (T1546.012)

Evasión de defensa

Técnica ATT&CK: eliminación del indicador en el host (T1070)

Técnica ATT&CK: eliminación del indicador en el host: Borrar registros de eventos de Windows (T1070.001)

Técnica ATT&CK: Enmascaramiento: hacer coincidir el nombre o la ubicación legítimos (T1036.005)

Técnica ATT&CK: Debilitar las defensas: deshabilitar o modificar el firewall del sistema (T1562.004)

Técnica ATT&CK: Modificar Registro (T1112)

Acceso a Credenciales

Técnica ATT&CK: volcado de credenciales del sistema operativo: memoria LSASS (T1003.001)

Técnica ATT&CK: volcado de credenciales del sistema operativo: administrador de cuentas de seguridad (T1003.002)

Técnica ATT&CK: volcado de credenciales del sistema operativo: NTDS (T1003.003)

Técnica ATT&CK: generación de solicitud de autenticación multifactor (T1621)

Movimiento lateral

Técnica ATT&CK: Servicios remotos (T1021)

Descubrimiento

Técnica ATT&CK: Registro de consultas (T1012)

Comando y control

Técnica ATT&CK: Protocolo de capa de aplicación: Protocolos web (T1071.001)

Técnica ATT&CK: Software de acceso remoto (T1219)

Técnica ATT&CK: Canal cifrado: Criptografía asimétrica (T1573.002)

Técnica ATT&CK: Proxy: Proxy multisalto (T1090.003)

exfiltración

Técnica ATT&CK: Exfiltración sobre protocolo alternativo (T1048)

RECOMENDACIONES

- Implemente un plan de recuperación que mantenga y conserve múltiples copias de datos confidenciales o de propiedad y servidores en una ubicación segura, segmentada y separada físicamente (es decir, disco duro, dispositivo de almacenamiento o la nube).

- Implemente la segmentación de la red y mantenga copias de seguridad fuera de línea de los datos para garantizar una interrupción limitada de la organización.

- Realice copias de seguridad de los datos con regularidad y proteja con contraseña las copias de seguridad almacenadas sin conexión. Asegúrese de que las copias de los datos críticos no sean accesibles para su modificación o eliminación desde el sistema donde residen los datos.

- Instale, actualice periódicamente y habilite la detección en tiempo real del software antivirus en todos los hosts.

- Instale actualizaciones para sistemas operativos, software y firmware siempre que estén disponibles y el historial de cambios no indique vulnerabilidades o bugs críticos.

- Revise los controladores de dominio, los servidores, las estaciones de trabajo y los directorios activos en busca de cuentas nuevas o no reconocidas.

- Auditar cuentas de usuario con privilegios administrativos y configurar controles de acceso según el principio de mínimo privilegio.

- Deshabilite los puertos no utilizados.

- Considere agregar un banner de correo electrónico a los correos electrónicos recibidos desde fuera de su organización.

- Hacer cumplir la autenticación multifactor (MFA).

- Considere instalar y usar una red privada virtual (VPN) para establecer conexiones remotas seguras.

- Examine el tráfico de red entrante y saliente, en busca de actividad sospechosa dentro de su red.

- Utilizar escritorio remoto solo cuando es necesario.

- Realizar capacitaciones de forma continua a su personal sobre detección y reporte de Phishing.

Noticia Completa

https://devel.group/cisco-talos-comparte-informacion-relacionada-con-un-ciberataque-reciente-a-cisco/

IOC's

https://github.com/develgroup/SOC_IOCs/tree/main/20220810_10_UNC2447

CONTACTOS DE SOPORTE

Correo electrónico: cert@develsecurity.com

Teléfonos directos:

Guatemala: +(502) 2307 5757
El Salvador: +(503) 2249 4252
Honduras: +(504) 2283 5904
República Dominicana: +1 829 734 2040

WhatsApp: +(502) 5124 9536

Sitio Web: https://www.devel.group/reporta-un-incidente