Autor:

11 de julio de 2024

Las operaciones del equipo rojo de la CISA contra una organización del Poder Ejecutivo Civil Federal resaltan la necesidad de una defensa en profundidad

RESUMEN EJECUTIVO

A principios de 2023, la Agencia de Ciberseguridad y Seguridad de la Infraestructura (CISA, por sus siglas en inglés) realizó una evaluación del equipo rojo SILENTSHIELD contra una organización del Poder Ejecutivo Civil Federal (FCEB, por sus siglas en inglés). Durante las evaluaciones de SILENTSHIELD, el equipo rojo primero realiza una simulación a largo plazo y sin previo aviso de operaciones cibernéticas de un estado-nación. El equipo imita las técnicas, las estrategias y los comportamientos de agentes de amenazas sofisticados y mide el tiempo de permanencia potencial que los agentes tienen en una red, lo que proporciona una evaluación realista de la postura de seguridad de la organización. Luego, el equipo trabaja directamente con los defensores de la red de la organización, los administradores del sistema y otro personal técnico para abordar las fortalezas y debilidades encontradas durante la evaluación. El objetivo del equipo es ayudar a la organización a perfeccionar sus capacidades de detección, respuesta y búsqueda, en particular la búsqueda de amenazas desconocidas.

En coordinación con la organización evaluada, la CISA publica este Aviso de ciberseguridad (CSA, por sus siglas en inglés) que detalla la actividad y las tácticas, técnicas y procedimientos (TTP, por sus siglas en inglés) del equipo rojo; la actividad de defensa de la red asociada; y las lecciones aprendidas para brindar a los defensores de la red recomendaciones para mejorar las capacidades de detección y la postura cibernética de su organización.

Durante la primera fase, el equipo de SILENTSHIELD obtuvo acceso inicial explotando una vulnerabilidad conocida en un servidor web sin parchear en el enclave Solaris de la víctima. Aunque el equipo comprometió completamente el enclave, no pudo ingresar a la parte de Windows de la red debido a la falta de credenciales. En un esfuerzo paralelo, el equipo obtuvo acceso a la red de Windows mediante phishing. Luego, descubrieron credenciales de administrador inseguras, lo que les permitió pivotar libremente por el entorno de Windows y resultó en la vulneración total del dominio y el acceso a activos de nivel cero. A continuación, el equipo identificó que la organización tenía relaciones de confianza con múltiples organizaciones asociadas externas y pudo aprovecharlas y pivotar a una organización externa. El equipo rojo permaneció sin ser detectado por los defensores de la red durante la primera fase.

Todas las organizaciones deben notificar incidentes y actividades anómalas al centro operativo de la CISA, disponible las 24 horas los 7 días de la semana, a Report@cisa.gov o al (888) 282-0870. Cuando esté disponible, incluyan la siguiente información sobre el incidente: fecha, hora y lugar del incidente; tipo de actividad; número de personas afectadas; tipo de equipo utilizado para la actividad; el nombre de la empresa u organización presentadora y un punto de contacto designado.

Los hallazgos del equipo rojo subrayaron la importancia de la defensa en profundidad y el uso de capas diversificadas de protección. La organización solo pudo comprender plenamente el alcance del ataque del equipo rojo al ejecutar diagnósticos completos de todas las fuentes de datos. Esto implicó analizar registros basados en el host, registros de red interna, registros de red externa (de salida) y registros de autenticación.

Los hallazgos del equipo rojo también demostraron el valor de utilizar indicadores de riesgo (IOC, por sus siglas en inglés) independientes de la herramienta y basados en el comportamiento, y de aplicar un enfoque de "lista blanca" al comportamiento y los sistemas de la red, en lugar de un enfoque de "lista negra", que sobre todo resulta en una cantidad inmanejable de ruido. Los hallazgos del equipo rojo destacaron las siguientes lecciones aprendidas para los defensores de la red sobre cómo reducir y responder al riesgo:

- **Lección aprendida:** la organización evaluada no contaba con controles suficientes para prevenir y detectar actividades maliciosas.
- **Lección aprendida:** la organización no recopiló, retuvo ni analizó registros de manera eficaz ni eficiente.
- **Lección aprendida:** los procesos burocráticos y los equipos descentralizados obstaculizaron a los defensores de la red de la organización.
- **Lección aprendida:** un enfoque de detección de "malo conocido" dificultó la detección de TTP alternativos.

Para reducir el riesgo de actividades cibernéticas maliciosas similares, la CISA anima a las organizaciones a aplicar las recomendaciones de la sección Medidas de mitigación de este aviso, incluidas las que se enumeran a continuación:

- **Aplicar principios de defensa en profundidad** mediante múltiples capas de seguridad para garantizar un análisis exhaustivo y la detección de posibles intrusiones.
- **Utilizar una segmentación de red robusta** para impedir el movimiento lateral a través de la red.
- **Establecer líneas de base de tráfico de red, ejecución de aplicaciones y autenticación de cuentas**. Utilizar estas líneas de base para aplicar una filosofía de "lista blanca" en lugar de rechazar IOC que se sabe que son malos. Asegurarse de que las herramientas y procedimientos de monitoreo y detección se basen principalmente en el comportamiento, en lugar de centrarse en el IOC.

La CISA reconoce que el software inseguro contribuye a estos problemas identificados e insta a los fabricantes de software a adoptar los principios de Seguridad desde el diseño e implementar las recomendaciones de la sección Medidas de mitigación de esta CSA, incluidas las que se enumeran a continuación, para fortalecer las redes de los clientes contra la actividad maliciosa y reducir la probabilidad de riesgo del dominio:

- **Eliminar las contraseñas predeterminadas.**
- **Proporcionar registros sin costo adicional**.
- **Trabajar con proveedores de gestión de eventos e información de seguridad (SIEM, por sus siglas en inglés) y orquestación, automatización y respuesta de seguridad (SOAR, por sus siglas en inglés)**, junto con los clientes, para comprender cómo los equipos de respuesta usan los registros para investigar incidentes.

ÍNDICE

INTRODUCTION **4**
INFORMACIÓN TÉCNICA **4**
Fase de emulación del adversario 5
Explotación del enclave Solaris 5
Explotación del dominio de Windows 8
Técnicas de evasión de defensa 12
Fase colaborativa 13
Recolección de registros 13
Análisis forense 14
Confianza en los IOC conocidos 14
Gestión de la vigilancia y la investigación periódicas 14
Configuraciones erróneas de Sysmon 15
LECCIONES APRENDIDAS Y HALLAZGOS CLAVE **15**
Lección aprendida: la organización evaluada no contaba con controles suficientes para prevenir y detectar actividades maliciosas 15
Lección aprendida: la organización no recopiló, retuvo ni analizó registros de manera eficaz ni eficiente 16
Lección aprendida: la comunicación burocrática y los equipos descentralizados obstaculizaron a los defensores de la red de la organización 17
Lección aprendida: un enfoque de detección de “malo conocido” dificultó la detección de TTP alternativos 17
FORTALEZAS DESTACADAS **18**
MITIGATIONS **18**
Defensores de la red 18
Fabricantes de software 22
VALIDAR LOS CONTROLES DE SEGURIDAD **23**
RESOURCES **24**
DISCLAIMER **24**
HISTORIAL DE VERSIONES **24**
APÉNDICE: TÁCTICAS Y TÉCNICAS DE MITRE ATT&ACK **25**

INTRODUCCIÓN

La CISA tiene autoridad para buscar e identificar, con o sin previo aviso o autorización de las agencias, amenazas y vulnerabilidades dentro de los sistemas de información federales (ver en general el Párrafo 3553[b][7] del Título 44 del Código de los Estados Unidos [USC, por sus siglas en inglés]). La organización objetivo de esta evaluación fue una gran organización del FCEB de EE. UU. La CISA llevó a cabo la evaluación SILENTSHIELD durante un período de aproximadamente ocho meses en 2023, y tres de esos meses consistieron en una fase de colaboración técnica:

- **Fase de emulación del adversario:** el equipo comenzó emulando un agente de estado-nación sofisticado simulando el acceso inicial conocido y las TTP posteriores a la explotación. El objetivo del equipo era comprometer el dominio de la organización evaluada e identificar rutas de ataque a otras redes. Una vez completados sus objetivos iniciales, el equipo diversificó las herramientas y la estrategia implementadas para imitar un conjunto más amplio y, a menudo, menos sofisticado de agentes de amenazas para atraer la atención de los defensores de la red. Los miembros del equipo rojo de la CISA no limpiaron ni eliminaron los registros del sistema, lo que permitió a los defensores investigar todos los artefactos e identificar el alcance completo de una violación.
- **Fase de colaboración:** el equipo de SILENTSHIELD se reunió periódicamente con personal superior y personal técnico para analizar problemas con las capacidades de defensa cibernética de la organización. Durante esta fase, el equipo:
  1. Propuso nuevas detecciones basadas en el comportamiento y ajenas a las herramientas para descubrir estrategias adicionales utilizadas durante la fase de emulación del adversario. También evaluó las mejoras de la organización de acuerdo con las prioridades actuales de la CISA y la orientación pública.
  2. Solucionó problemas con los pasos de detección existentes para mostrar cómo ciertas TTP evadieron las detecciones basadas en IOC.
  3. Diferenciaron eventos de la actividad del equipo rojo de la CISA, lo que indicó un comportamiento inesperado de la red/aplicación o la posible presencia de un adversario real en la red.

  Nota: el objetivo del equipo durante esta fase fue desarrollar la capacidad de la organización para detectar actividad maliciosa basada en el comportamiento del adversario (es decir, TTP) en lugar de confiar en IOC conocidos.

Este aviso, redactado en coordinación con la organización evaluada, detalla la actividad y las TTP del equipo rojo, la actividad de defensa de la red asociada y las lecciones aprendidas para brindar a los defensores de la red recomendaciones para mejorar la postura cibernética defensiva de su organización. El aviso también proporciona recomendaciones a los fabricantes de software para fortalecer las redes de sus clientes contra actividades maliciosas y reducir la probabilidad de que los dominios se vean comprometidos.

INFORMACIÓN TÉCNICA

Nota: Este aviso utiliza el marco MITRE ATT&CK para entornos empresariales, versión 15. Consulte la sección Tácticas y técnicas de MITRE ATT&CK para ver la tabla de la actividad de los agentes de amenazas asignada a las tácticas y técnicas de MITRE ATT&CK®. Para obtener asistencia con el seguimiento de las actividades cibernéticas maliciosas en el marco MITRE ATT&CK, consulte las prácticas recomendadas para el seguimiento de MITRE ATT&CK de la CISA y MITRE ATT&CK, y la herramienta Decider de la CISA.

Durante la fase de emulación del adversario, el equipo rojo obtuvo acceso inicial al enclave Solaris de la organización explotando una vulnerabilidad conocida en un servidor web sin parchear. Obtuvieron acceso independiente al entorno de Windows mediante phishing y pudieron comprometer el dominio completo y su dominio principal. Consulte la Figura 1 para ver una cronología de esta evaluación y las secciones a continuación para obtener detalles sobre la actividad del equipo y las TTP.

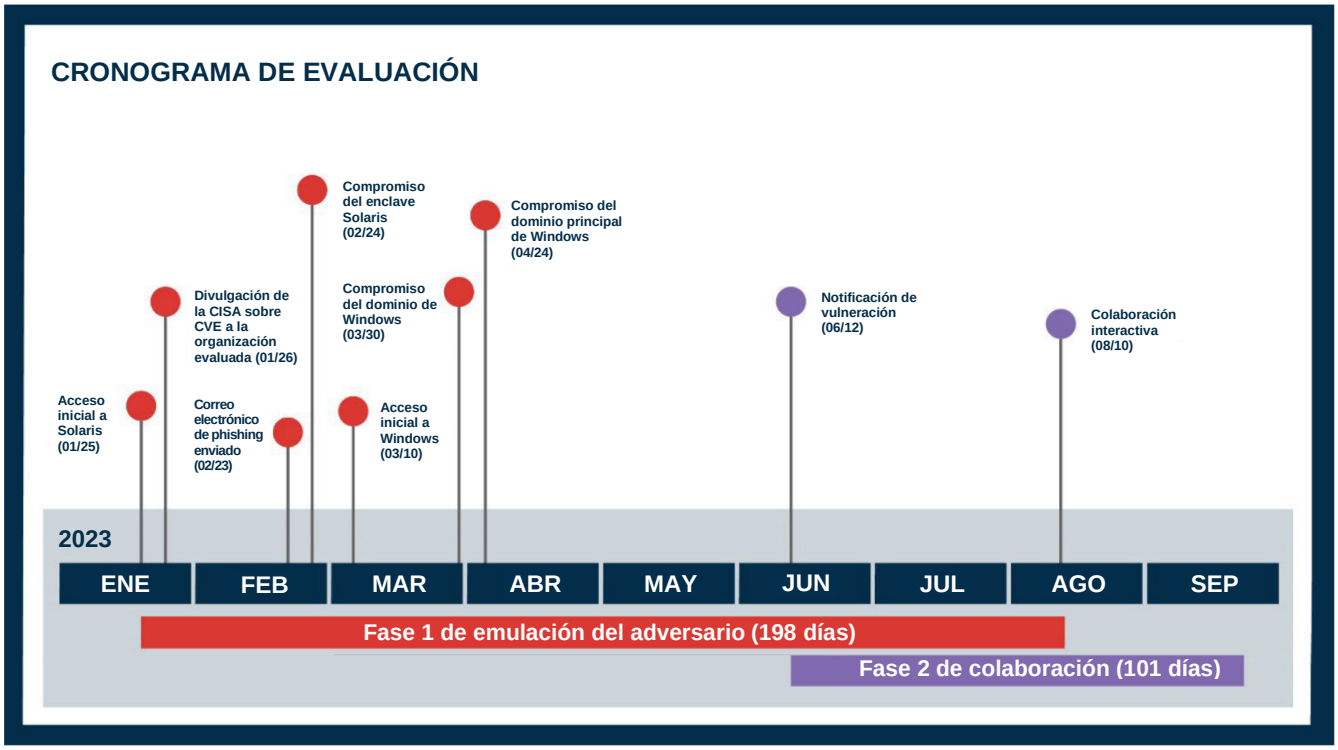

Figura 1: Cronograma de evaluación de SILENTSHIELD

Fase de emulación del adversario

Explotación del enclave Solaris

Reconocimiento, acceso inicial y mando y control

El equipo rojo de la CISA utilizó herramientas de código abierto y servicios de terceros para investigar la superficie expuesta a Internet de la organización [T1594]. Esto incluyó escaneos de puertos no intrusivos para puertos comunes y enumeración del Sistema de nombres de dominio (DNS, por sus siglas en inglés) [T1590.002]. Estos esfuerzos revelaron que el servidor web de la organización no estaba parcheado para CVE-2022-21587, una vulnerabilidad de ejecución remota de código (RCE, por sus siglas en inglés) no autenticada en Oracle Web Applications Desktop Integrator. Durante tres meses, la organización evaluada no logró reparar esta vulnerabilidad y el equipo la aprovechó para obtener acceso inicial.

El exploit permitía la ejecución de código en un servidor de aplicaciones backend (SERVIDOR 1) que manejaba las solicitudes entrantes del servidor web público. El equipo rojo utilizó este exploit para cargar y ejecutar una herramienta de acceso remoto (RAT, por sus siglas en inglés) segura de Python. Debido a que el servidor de aplicaciones tenía salida completa a Internet externa a través de los puertos `80` y `443` del Protocolo de control de transmisión (TCP, por sus siglas en inglés), la RAT habilitó tráfico de mando y control (C2) consistente [T1071.001].

Nota: después de obtener acceso, el equipo informó rápidamente a los agentes de confianza de la organización sobre el dispositivo sin parchear, pero la organización tardó más de dos semanas en aplicar el parche disponible. Además, la organización no realizó una investigación exhaustiva de los servidores afectados, lo que habría revelado IOC y debería haber conducido a una respuesta completa al incidente. Aproximadamente dos semanas después de que el equipo obtuvo acceso, el código de exploit se publicó en un popular marco de explotación de código abierto. La CISA identificó que la vulnerabilidad fue explotada por un tercero desconocido. La CISA agregó esta CVE a su Catálogo de vulnerabilidades explotadas conocidas el 2 de febrero de 2023.

Acceso a credenciales, mando y control, y aumento de privilegios

Una vez en el SERVIDOR 1, el equipo rojo investigó los archivos y la estructura de carpetas del host [T1005] e identificó varios archivos de respaldo `.tar` antiguos y accesibles globalmente, que incluían una copia legible de un archivo `/etc/shadow` que contiene el hash de una cuenta de servicio privilegiada (CUENTA 1). El equipo descifró rápidamente la contraseña débil de la cuenta utilizando una lista de palabras comunes [T1110.002]. Luego, establecieron una conexión de Protocolo Secure Shell (SSH) saliente a través del puerto TCP `80` y usaron un túnel inverso para volver a conectarse mediante SSH al SERVIDOR 1, donde se les solicitó restablecer la contraseña vencida de la CUENTA 1 [T1571] (ver Figura 2). El equipo identificó que la cuenta estaba habilitada en un subconjunto de contenedores, pero no se había utilizado activamente durante un período de tiempo significativo; el equipo cambió la contraseña de esta cuenta a una contraseña segura.

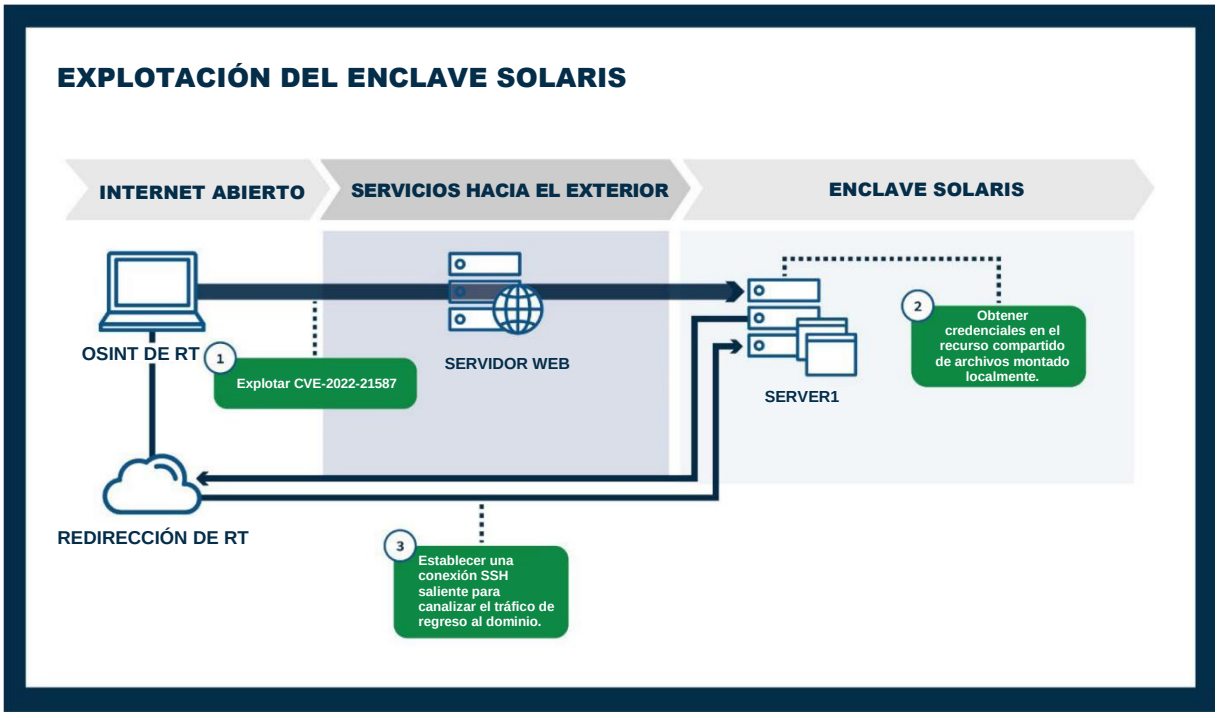

Figura 2: Explotación del enclave Solaris

El equipo descubrió que la CUENTA 1 era un administrador local con acceso `sudo/root` y la utilizó para moverse lateralmente (ver la siguiente sección).

Movimiento lateral y persistencia

Los servidores en el enclave Solaris no usaban autenticación centralizada, sino que tenían un conjunto mayoritariamente uniforme de cuentas y permisos locales [T1078.002]. Esto permitió que el equipo rojo usara la CUENTA 1 para moverse a través de gran parte del segmento de red a través de SSH [T1021.004].

Algunos servidores permitían el acceso externo a Internet, y el equipo implementó RAT en algunos de estos hosts para C2. Implementaron varias RAT diferentes para diversificar las firmas de tráfico de red y ocultar las huellas en el disco y en la memoria. Estas herramientas se comunicaron con un redirector del equipo rojo a través de TCP/`443`, mediante mensajes HTTPS válidos y a través de SSH mediante puertos no estándar (`80` y `443`) [T1571].Gran parte del tráfico no estaba bloqueado por un firewall y la organización carecía de firewalls de capa de aplicación capaces de detectar desajustes de protocolos en puertos comunes.

Luego, el equipo se trasladó lateralmente a varios servidores, incluidos activos de alto valor, que no permitían el acceso a Internet. Utilizando túneles SSH inversos, el equipo se trasladó al entorno y utilizó un proxy SOCKS [T1090] para avanzar a través de la red. Configuraron implantes con escuchas de enlace TCP vinculadas a puertos altos aleatorios para conectarse directamente con algunos de estos hosts sin crear nuevos eventos de inicio de sesión SSH (ver Figura 3).

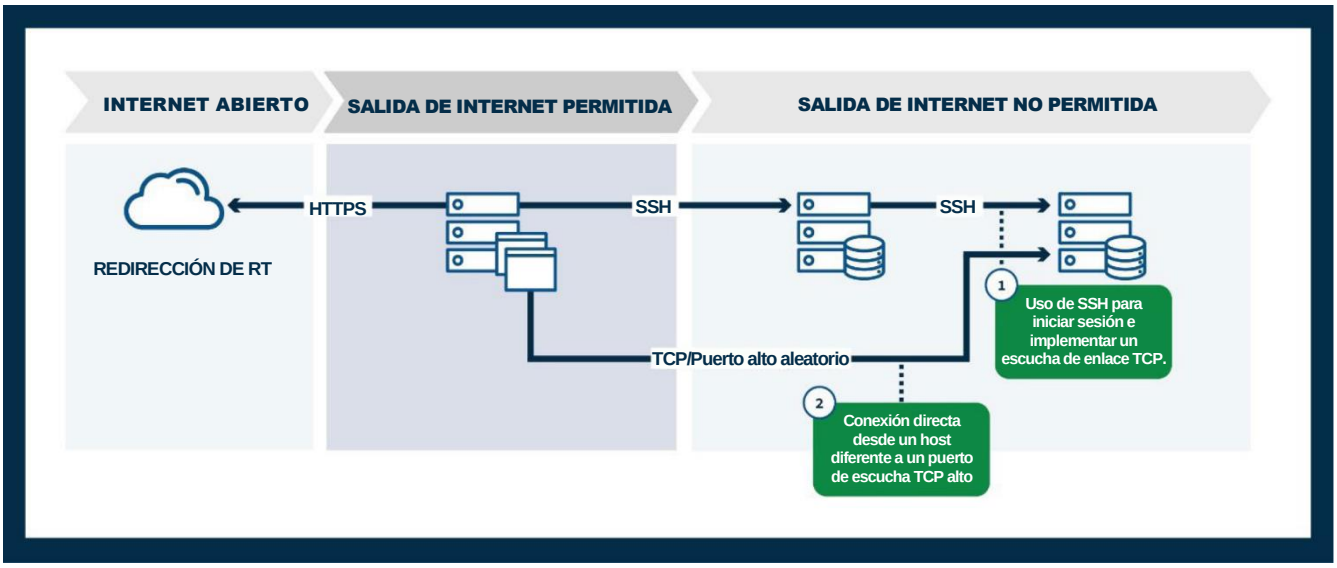

Figura 3: Ejemplo de movimiento lateral en el enclave Solaris

Una vez en otros hosts internos, el equipo extrajo datos de cada uno de ellos en busca de información confidencial y credenciales. Obtuvieron información de identificación personal (PII, por sus siglas en inglés), archivos ocultos, una clave SSH de administrador protegida por una contraseña de frase descifrable y una contraseña de texto sin formato [T1552.003] en el `.bash_history` de un usuario. Estas credenciales extraídas de datos proporcionaron más vías para el acceso sin privilegios a través de la red. El equipo también utilizó túneles SSH para montar de forma remota recursos compartidos de archivos del Sistema de archivos de red (NFS, por sus siglas en inglés), falsificando valores `uid` y `gid` para acceder a todos los archivos y carpetas.

Para protegerse contra reinicios u otras interrupciones, el equipo persistió principalmente en los hosts usando la utilidad de `cron` [T1053.003], así como la utilidad `at` [T1053.002], para ejecutar tareas programadas y mimetizarse con el entorno. Además, las claves privadas SSH proporcionaban acceso persistente a los hosts pivote internos y habrían seguido permitiendo el acceso incluso si se rotaban las contraseñas.

Vulneración de todo el enclave

Aunque la CUENTA 1 permitió al equipo moverse lateralmente a gran parte del enclave de Solaris, no proporcionó acceso privilegiado a todos los hosts de la red porque un subconjunto de hosts había cambiado la contraseña (lo que negaba el acceso privilegiado a través de esa cuenta). Sin embargo, el equipo analizó los inicios de sesión de usuarios recientes utilizando el comando `last` e identificó una cuenta de servicio de escaneo de dispositivos de seguridad de red (CUENTA 2) que iniciaba sesión regularmente en un host interno utilizando autenticación basada en contraseña. Como parte de su análisis periódico de vulnerabilidades, la CUENTA 2 se conectaría a cada host a través de SSH y ejecutaría `sudo` con una ruta relativa en lugar de la ruta absoluta `/usr/local/bin/sudo`. La ruta local creó una vulnerabilidad de secuestro de ruta, que permitió al equipo rojo secuestrar el flujo de ejecución y registrar la contraseña de la cuenta [T1574.007].

La contraseña obtenida otorgó acceso privilegiado sin restricciones a todo el enclave de Solaris.

Explotación del dominio de Windows

Si bien la vulneración del enclave Solaris facilitó meses de acceso persistente a sistemas sensibles, incluidas aplicaciones web y bases de datos, no condujo a la vulneración inmediata del entorno corporativo de Windows. Una vez en el dominio de Windows, el equipo rojo identificó varias cuentas de servicio con contraseñas débiles. Es probable que un adversario pudiera haber continuado la ruta de ataque de Solaris a través de ataques prolongados de rociado de contraseñas o aprovechando credenciales obtenidas externamente (p. ej., volcados de credenciales de la dark web) (ver Figura 4).

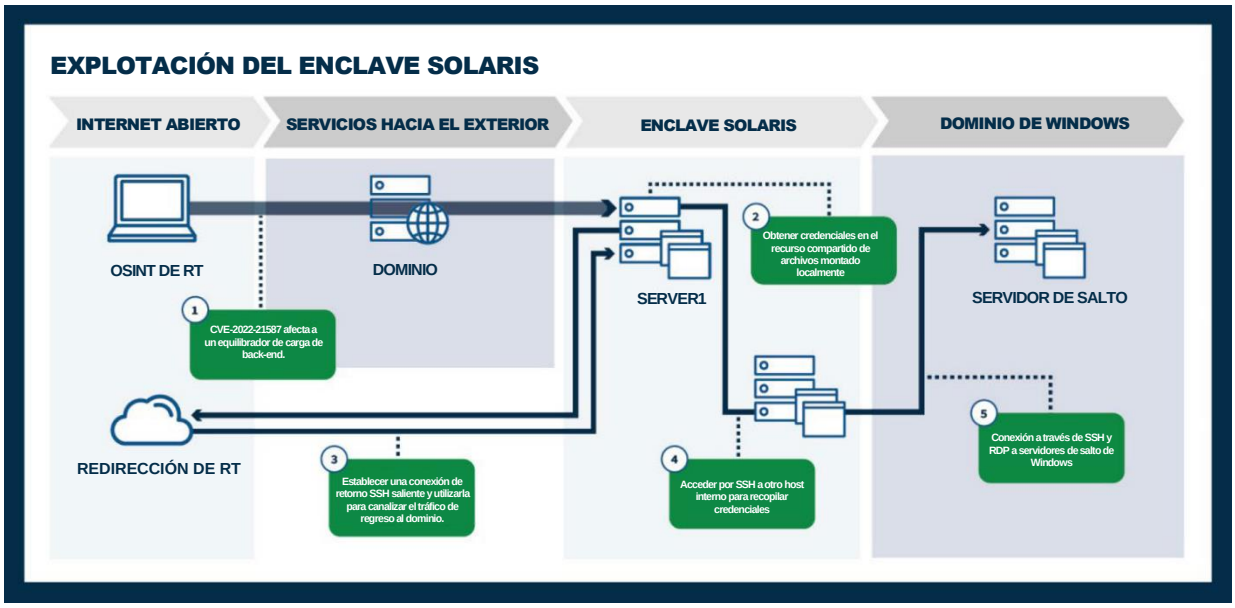

Figura 4: Explotación del enclave Solaris

El equipo explotó el dominio de Windows a través de otros vectores de acceso y, finalmente, demostró que el pivote no detectado entre los dominios podía realizarse después de obtener las credenciales de Windows.

Reconocimiento y acceso inicial

Al intentar pivotar de Solaris a Windows, el equipo rojo llevó a cabo una recopilación de información de código abierto sobre la organización. Recolectaron nombres de empleados [T1589.003] y utilizaron la información para derivar direcciones de correo electrónico basadas en el esquema de nombres de correo electrónico del objetivo. Después de identificar nombres, correos electrónicos y cargos laborales, el equipo seleccionó varios objetivos de phishing que interactuaban regularmente con el público [T1591.004]. Un usuario activó una carga útil de phishing que proporcionó acceso inicial a una estación de trabajo.

A continuación, el equipo colocó un RAT de acceso inicial simple en la estación de trabajo en una carpeta de escritura por usuario y obtuvo persistencia a nivel de usuario a través de una clave de ejecución de registro agregada, que llamó a un redirector del equipo rojo a través de HTTPS. El equipo evaluó lo que se estaba ejecutando en el host en términos de antivirus (AV) y detección y respuesta de puntos finales (EDR, por sus siglas en inglés) y utilizó el implante para inyectar un RAT más capaz y completo directamente en la memoria, que apuntaba a un redirector separado. Las herramientas de la organización evaluada no lograron categorizar el tráfico C2 como anómalo incluso cuando un error en uno de los implantes provocó que 8 GB de tráfico de red continuo fluyeran en una tarde.

Acceso con credenciales y aumento de privilegios

La información de la red interna estaba disponible libremente para usuarios sin privilegios unidos al dominio, y el equipo consultó cientos de megabytes de datos de Active Directory (AD) utilizando una reescritura personalizada de `dsquery.exe` en `.NET` y `ldapsearch` de Beacon Object File (BOF) desde la estación de trabajo del usuario suplantado. Luego, el equipo extrajo datos de numerosos servidores de archivos internos en busca de recursos compartidos accesibles [T1083]. El equipo encontró un archivo de contraseñas dejado por un empleado anterior en un recurso compartido de IT administrativo abierto, que contenía nombres de usuario y contraseñas en texto simple para varias cuentas de servicio privilegiadas. Con la información recopilada del Protocolo ligero de acceso a directorios (LDAP, por sus siglas en inglés), el equipo identificó que una de las cuentas (CUENTA 3) tenía privilegios de administrador de operaciones del centro del sistema (SCOM, por sus siglas en inglés) y privilegios de administrador de dominio para el dominio principal. Identificaron otra cuenta (CUENTA 4) que también tenía permisos administrativos para la mayoría de los servidores del dominio. Las contraseñas de ambas cuentas no se habían actualizado en más de ocho años y no estaban registradas en el sistema de gestión de identidad (IDM, por sus siglas en inglés) de la organización.

Movimiento lateral y persistencia

El equipo utilizó cuentas válidas o tokens con técnicas variadas para el movimiento lateral. Las técnicas incluían manipulación de tareas programadas, creación de servicios y secuestro de dominios de aplicaciones. [T1574.014]. Para el uso de credenciales, el IDM implementado en la red de la organización obstaculizó la capacidad del equipo rojo para pivotar, ya que bloqueó técnicas comunes de manipulación de credenciales como pass-the-hash [T1550.002] y pass-the-ticket [T1550.003]. El equipo rojo encontró formas de eludir el IDM, incluido el uso de contraseñas de texto simple para crear sesiones de inicio de sesión de red genuinas [T1134.003] para ciertas cuentas no registradas en el IDM, así como suplantar los tokens de los usuarios que actualmente han iniciado sesión para aprovechar sesiones válidas [T1134.001].

El equipo rojo adaptó las cargas útiles para que se mezclaran con el entorno de la red y no reutilizó los IOC como nombres de archivos o hashes de archivos, especialmente para implantes persistentes. Las consultas remotas de listados de directorios, tareas programadas, servicios y procesos en ejecución proporcionaron la información para que el equipo rojo se hiciera pasar por actividad legítima [T1036.004].

El equipo emuló la actividad normal de la red instalando agentes de señalización HTTPS en estaciones de trabajo donde los usuarios normales navegan por la web, estableciendo pivotes de red internos con enlaces TCP y escuchas SMB. Se basaron principalmente en la creación de servicios de Windows como su mecanismo de persistencia.

El equipo rojo utilizó las credenciales extraídas de la CUENTA 3 para moverse lateralmente desde la estación de trabajo a un servidor SCOM. Una vez allí, utilizaron la CUENTA 4 para atacar un servidor Systems Center Configurations Manager (SCCM), ya que era un punto de observación de red ventajoso. El servidor SCCM tenía administradores de servidor conectados existentes cuyos nombres de usuario seguían un patrón de nombres predecible (correlacionando funciones administrativas y niveles de privilegio), lo que les permitía determinar qué cuenta usar para pivotar a otros hosts.

El equipo atacó los servidores de salto de la organización frecuentados por cuentas administrativas con altos privilegios. Los operadores del equipo rojo utilizaron credenciales de administrador de servidor de SCCM robadas para comprometer uno de los hosts de salto de administrador de servidor de la organización. Se enteraron de que la organización separaba algunas cuentas, pero no todas, en servidores de salto separados por función (p. ej., los administradores de estaciones de trabajo y los administradores de servidores tenían puntos de salto separados, pero los administradores de servidores y dominios ocasionalmente compartían los mismos hosts de salto). Una vez que un administrador de dominio iniciaba sesión, el equipo rojo robaba el token de sesión del administrador y se movía lateralmente a un controlador de dominio donde extraía las credenciales de todo el dominio a través de `DCSync` [T1003.006], vulnerando todo el dominio (ver Figura 5).

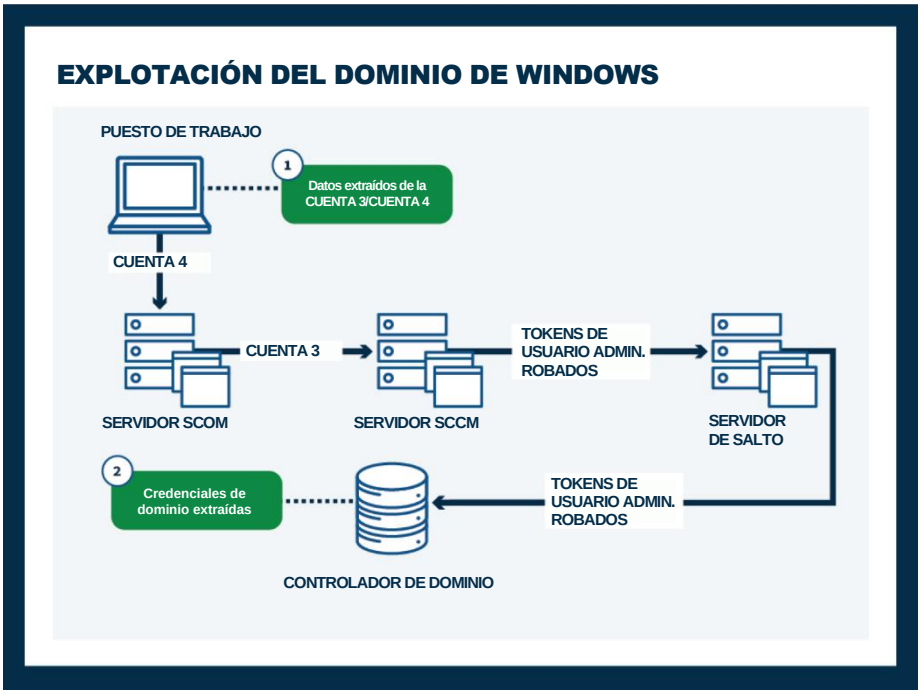

Figura 5: Explotación del dominio de Windows

Después de comprometer el dominio, el equipo confirmó el acceso a servidores sensibles, incluidos múltiples activos de alto valor (HVA, por sus siglas en inglés) y activos de nivel cero. Ninguno de los servidores a los que se accedió tenía protecciones adicionales notables ni restricciones de acceso a la red a pesar de su sensibilidad y funciones críticas en la red. La administración remota y el acceso a estos sistemas críticos deben restringirse a cuentas designadas y basadas en funciones que provengan de enclaves de red específicos o estaciones de trabajo. El aislamiento con estas limitaciones del vector de acceso los protege del riesgo y reduce drásticamente el ruido asociado, lo que permite a los defensores identificar más fácilmente el comportamiento anormal.

Pivotar hacia socios externos de confianza

El equipo inspeccionó las relaciones de confianza de la organización con otros dominios organizativos a través de LDAP [T1482] e identificaron conexiones con múltiples organizaciones externas asociadas del FCEB, una de las cuales posteriormente utilizaron para moverse lateralmente.

El equipo extrajo información LDAP de SOCIO DC 1 y aplicó Kerberos al dominio, lo que generó una cuenta de servicio válida con una contraseña débil que descifraron rápidamente, pero el equipo no pudo moverse lateralmente con esta cuenta porque carecía de los privilegios adecuados. Sin embargo, SOCIO 1 tenía relaciones de confianza con el controlador de dominio de un segundo socio (SOCIO DC 2). Usando las credenciales de SOCIO 1 adquiridas, el equipo rojo descubrió que SOCIO 2 también tenía una cuenta de servicio administrativo con privilegios altamente habilitados y vulnerable a Kerberoasting cuya contraseña fue descifrada, lo que le permitió al equipo moverse lateralmente a un host del SOCIO 2 desde la red de la víctima original (ver Figura 6).

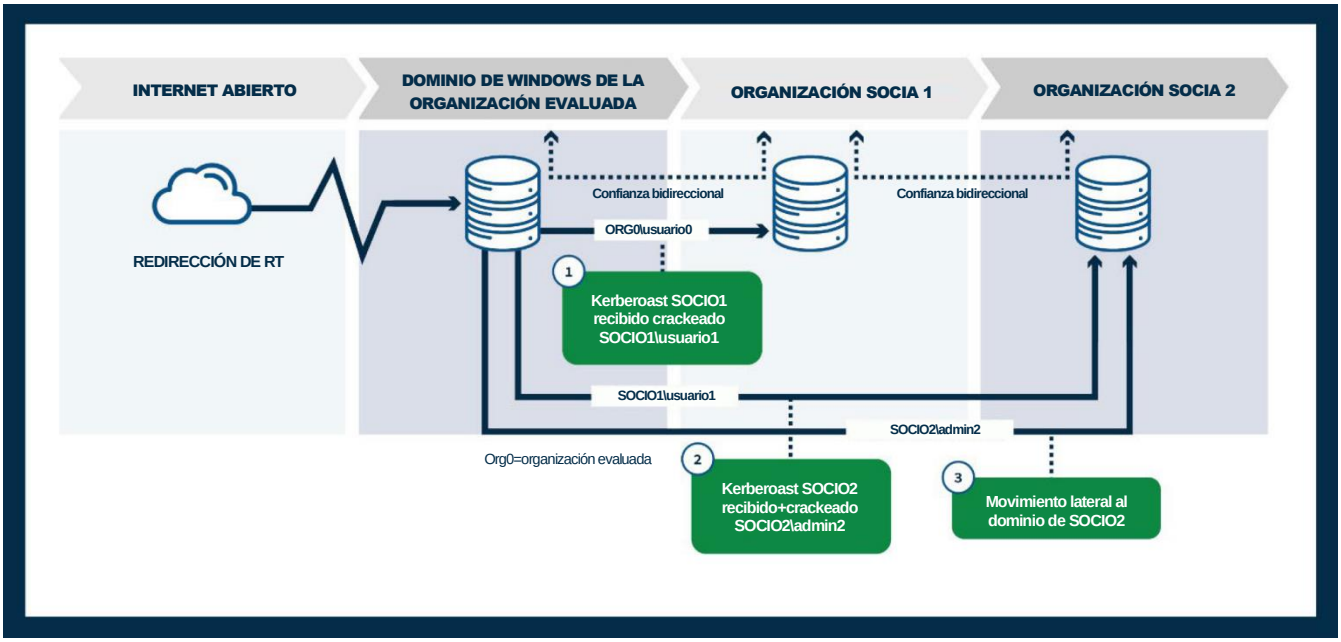

Figura 6: Ruta de explotación hacia organizaciones externas del FCEB

Estas rutas de ataque entre organizaciones rara vez se identifican o prueban en evaluaciones o auditorías regulares debido a la propiedad de la red, los acuerdos legales o la opacidad del proveedor. Sin embargo, siguen siendo un vector de acceso valioso para los agentes de amenazas persistentes avanzadas (APT, por sus siglas en inglés).

La experimentación con el acceso a dominios de socios confiables incluyó la modificación de las reglas de firewall del sistema local en el controlador de dominio de origen para permitir IP de origen y destino específicas. Los sistemas de monitoreo basados en el host de la organización no pudieron identificar la adición y eliminación de las excepciones de firewall del equipo rojo.

Técnicas de evasión de defensa

Enclave Solaris

Debido a la falta de una lista de aplicaciones permitidas, el equipo rojo se hacía pasar regularmente por software legítimo para pasar desapercibido para los defensores de la red de la organización [T1036]. Además, de forma predeterminada, la auditoría de comandos en Solaris a través del comando `lastcomm` solo captura el programa que se está ejecutando; no se registran la ruta completa del archivo ni los argumentos de la línea de comandos. Por ejemplo:

- Un archivo real: `/opt/splunkforwarder/bin/splunkd`
- Una copia maliciosa: `/opt/splunkforwarder/splunkd`
- Registros de auditoría de comandos: `splunkd`

El equipo también ocultó artefactos comunes para oscurecer su actividad operativa, incluida la modificación de marcas de tiempo de archivos [T1070.006] y permisos con los comandos `touch` y `chmod/chown` [T1222.002] para mezclarse con otros archivos del entorno.

Dominio de Windows

El equipo utilizó una amplia gama de cuentas, puertas traseras y canales C2 con diferentes huellas de red para ocultar la actividad [T1027].

La diversificación del uso de cuentas, las puertas traseras y los canales C2 ocultaron aún más la actividad del equipo rojo en el dominio. El movimiento lateral hacia nuevos hosts incluyó una variedad de cuentas para reducir el riesgo de detección. Al recopilar credenciales, el equipo seleccionó varias cuentas de respaldo para cada función (p. ej., administrador del servidor, administrador de la estación de trabajo, administrador del dominio, cuentas de servicio) en caso de que la cuenta prevista estuviera bloqueada, deshabilitada o marcada como comprometida.

Para enfatizar el valor de las detecciones basadas en el comportamiento y que no dependen de herramientas, el equipo rojo implementó más de siete implantes diferentes para imitar el uso diverso que hacen los adversarios del mundo real de RAT de código abierto, comerciales listos para usar (COTS, por sus siglas en inglés) y personalizados. Cada uno presentaba diferentes firmas de host y red para evadir las detecciones EDR listas para usar y cada implante tenía artefactos únicos tanto en el disco como en la memoria. El equipo también evadió la EDR/AV mediante el uso de cargadores propietarios y archivos de objeto beacon (BOF, por sus siglas en inglés) para realizar llamadas API directas y permitir la autoinyección de ejecutables `.NET` para ejecutar capacidades adicionales.

Todas las herramientas implementadas tenían diferentes huellas de canales de red C2. Algunos agentes de beaconing se conectaron a través de HTTPS a dominios legítimos propiedad del equipo rojo. Otros utilizaron el domain fronting [T1090.004] para aprovechar la funcionalidad común de la red de distribución de contenido (CDN, por sus siglas en inglés). El tráfico saliente enviado a sitios web públicos que no eran propiedad del equipo rojo tenía un encabezado de `Host` que le indicaba al proveedor de CDN que debía redirigir el tráfico a direcciones IP controladas por el equipo rojo. Los pivotes internos utilizaron SMB en el puerto `445` y escuchas de enlace TCP en puertos altos efímeros. El equipo adaptó ambos métodos para imitar las tuberías con nombre y las conexiones de red ya vistas en el dominio y evadir la detección.

Fase colaborativa

Cinco meses después de la evaluación, el equipo rojo notificó oficialmente al centro de operaciones de seguridad (SOC, por sus siglas en inglés) de la organización sobre la actividad en curso y comenzó a comunicarse directamente con el liderazgo del SOC. En este momento, la organización no había presentado resoluciones de conflicto y no parecía estar investigando activamente la actividad de evaluación SILENTSHIELD de la CISA.

Durante esta fase, la CISA se abstuvo de proporcionar TTP o IOC (como hosts concretos, nombres de archivos o dominios C2) para permitir que la organización desarrolle y pruebe sus propias métricas de detección. El equipo mantuvo debates semanales con el personal técnico superior de la organización, el SOC y los administradores de sistemas, lo que condujo a mejoras cuantificables en los tiempos de respuesta para técnicas conocidas y detecciones basadas en el comportamiento que descubrieron estrategias previamente desconocidas. En concreto, el equipo rojo trabajó con la organización para ayudarle a sintetizar las siguientes fuentes de datos para identificar el alcance de la vulneración del equipo rojo:

- Alertas de la EDR
- Escaneos YARA
- Dominios y técnicas C2
- Hosts de pivote interno
- Cuentas de administrador utilizadas para pivotar
- Volcados de memoria que revelan intentos de pasar credenciales
- Registros de correo electrónico que documentan la violación inicial a través de phishing

Cada agente de amenazas cibernéticas tiene un conjunto único de TTP. Sin embargo, casi todos los adversarios realizan los mismos pasos básicos:

- Ejecución de comandos (acceso inicial y movimiento lateral)
- Establecer canales C2 y exfiltrar datos
- Establecer persistencia
- Aumentar privilegios
- Usar y abusar de las credenciales

Todas las TTP tienen artefactos correspondientes, pero no todos los IOC son creados iguales. Concentrarse en un conjunto hiperconcentrado de IOC puede detectar amenazas conocidas, pero obstaculiza los esfuerzos por identificar adversarios desconocidos que emplean diferentes TTP.

Los principales temas analizados durante esta fase que mejoraron las capacidades de detección basadas en el comportamiento de la organización incluyeron la recopilación de registros, el análisis forense, la confianza en los IOC para la detección, el monitoreo y la gestión de la investigación, y las configuraciones erróneas de Sysmon.

Recolección de registros

Las organizaciones evaluadas tenían registros ineficaces e insuficientes, y los defensores de la red no utilizaban los registros para detectar de forma proactiva el comportamiento anómalo. Con la ayuda del equipo rojo, la organización identificó problemas de registro causados por fallas de hardware, copias de seguridad limitadas, ancho de banda de red y políticas limitadas de recopilación y retención de registros (solo 60 a 90 días). En otros casos, se registraron datos críticos, pero no se analizaron porque los artefactos se trasladaron a almacenamiento en frío.

Los defensores de la red de la organización identificaron obstáculos relativos al procedimiento y de otro tipo al intentar adquirir nuevos datos forenses. Por ejemplo, no se pudieron desconectar los servidores afectados para realizar imágenes porque no había ningún proceso establecido para hacerlo sin afectar las operaciones de la organización.

Además, los intentos de registrar datos forenses a través de capturas de paquetes ocurrieron directamente en los hosts de Solaris y Windows comprometidos, donde el equipo rojo observó que se recopilaban los datos y, por lo tanto, tuvo la oportunidad de interrumpir la recopilación, alterar los archivos de evidencia y adaptarse mejor a sus defensas y evadirlas.

Análisis forense

Los defensores no monitorearon la salida de C2 a través de DNS. Creían que su entidad matriz estaba monitoreando su tráfico DNS, lo que los liberaba de la necesidad de recopilar y monitorear registros para sus análisis.

Los analistas forenses confiaron ciegamente en las marcas de tiempo de los archivos y en los mecanismos de persistencia sin darse cuenta de que habían sido alterados. Los tiempos falsos agregados a los mecanismos de persistencia (como las tareas programadas) llevaron a los defensores a juzgar mal la cronología de la vulneración. Los operadores del equipo rojo ajustaban regularmente la marca de tiempo de la última modificación de archivos y carpetas, utilizando el comando nativo `touch -r` o el comando `timestomp` de los implantes para disfrazar la marca de tiempo de la última modificación registrada en la salida de `ls –la`. Las marcas de tiempo de archivos secundarios identificadas con `ls -lu` o `ls -lc` habrían revelado atributos de archivo anormales, además de anomalías más confiables encontradas durante una investigación forense adecuada.

Confianza en los IOC conocidos

El equipo rojo utilizó TTP diversificadas en la fase de emulación del adversario para reflejar la capacidad de los agentes de amenazas cibernéticas de eludir las estrategias de detección convencionales del mal conocido. Los defensores de la red no detectaron mucha actividad del equipo. Por ejemplo:

- Después de identificar una carga útil del equipo rojo, los defensores de la red escribieron reglas YARA personalizadas que definieron el comportamiento específico del cargador del equipo rojo, que descubrió varias cargas útiles similares, pero no logró detectar ninguno de los otros seis marcos C2.
- Los defensores de la red de la organización utilizaron una combinación de reglas de detección personalizadas y de código abierto (como `CommandLine=kerberoast*` o archivos llamados `bloodhound.zip`) y no detectaron la actividad de kerberoasting del equipo.

Gestión de la vigilancia y la investigación periódicas

Las conversaciones con los líderes del SOC revelaron varios problemas de procedimiento que llevaron a un análisis lento o incompleto de la intrusión y la actividad del equipo rojo. Por ejemplo:

- Si bien los productos de EDR detectaron y pusieron en cuarentena varias de las herramientas del equipo rojo, incluida la carga útil de phishing inicial, los procedimientos diarios de la organización no siempre incluían la revisión de las alertas de EDR. El equipo rojo trabajó con la organización para garantizar que la respuesta rápida a las alertas de EDR se convirtiera en una parte fundamental de los flujos de trabajo diarios de los defensores de la red. Esto permitió al personal del SOC identificar nuevos intentos de movimiento lateral.
- Los propietarios de redes Solaris descubrieron que varios firewalls se habían configurado de forma incorrecta o se habían desactivado por error. Los equipos técnicos de la organización trabajaron directamente con el equipo rojo para corregir errores y reorganizar y revalidar la topología de la red.
- Los defensores de la red tenían una seguridad operativa deficiente y alertaron al equipo rojo de investigaciones. Por ejemplo:

  - En un caso, después de recibir señales entrantes de lo que evidentemente era un entorno aislado, la carga útil no fue renombrada desde su archivo original, lo que permitió al equipo rojo identificar de inmediato qué parte de su acceso estaba bajo escrutinio. Las organizaciones deben garantizar que los entornos aislados sean seguros, estén protegidos y completamente aislados.
  - El equipo rojo observó a los administradores del sistema revisando artefactos forenses vinculados a la carga útil de Solaris del equipo: búsqueda de archivos, ejecución de capturas de paquetes para el tráfico C2 saliente y escaneo del puerto del redirector C2. Los miembros del equipo tan solo reinstalaron su persistencia con un nuevo redirector y ruta de archivo, eludiendo la investigación informal.
- Los equipos de IT estaban aislados del SOC, que no tenía conocimiento de la investigación que el administrador del sistema había llevado a cabo durante semanas sobre el comportamiento anómalo de la red.
- Si bien la organización compartimentó la mayor parte de su búsqueda de amenazas y respuesta a incidentes en un dominio separado, el personal aún utilizó las cuentas de dominio corporativo comprometidas para comunicar los detalles de las investigaciones y evaluaciones activas.

Configuraciones erróneas de Sysmon

El equipo rojo tuvo un intercambio productivo con la organización sobre su configuración de Sysmon, que el equipo abusó durante toda la evaluación. El equipo rojo identificó varias configuraciones erróneas:

- Los equipos de implementación enviaron el conjunto de reglas (almacenado como un archivo `.xml`) a un directorio `C:\Windows` legible globalmente. No existían reglas para atrapar a los adversarios que leían las configuraciones desde el disco o el registro. Como resultado, al equipo rojo de la CISA se le proporcionaron rutas de archivos explícitas para colocar sus cargas útiles de forma segura.
- Las reglas apuntaban a un único IOC específico de la herramienta en lugar de a una técnica (p. ej., `sc.exe` en lugar de eventos de creación de servicios).
- Las excepciones fueron demasiado permisivas (por ejemplo, excluir todas las entradas de imágenes en cualquier parte de `C:\Program Files (x86)\Google\Update\*`).

LECCIONES APRENDIDAS Y HALLAZGOS CLAVE

El equipo rojo tomó nota de las siguientes lecciones aprendidas y hallazgos clave relevantes para la seguridad de la red de la organización evaluada. Estos hallazgos específicos contribuyeron a la capacidad del equipo de obtener acceso persistente a toda la red de la organización. Consulte la sección Medidas de mitigación para obtener recomendaciones sobre cómo abordar estos hallazgos.

Lección aprendida: la organización evaluada no contaba con controles suficientes para prevenir y detectar actividades maliciosas.

- **Hallazgo n.º 1: la red perimetral de la organización no estaba adecuadamente protegida desde su red interna, lo que no pudo restringir el tráfico saliente.** La mayoría de los hosts de la organización, incluidos los controladores de dominio, tenían conectividad a Internet a amplios rangos AWC de EC2, lo que le permitió al equipo rojo realizar solicitudes web salientes sin activar respuestas de IDS/IPS. Estas conexiones exitosas revelaron la falta de un firewall de capa de aplicación capaz de detectar desajustes de protocolo en puertos comunes.

- **Hallazgo n.º 2: la organización evaluada tenía una segmentación de red insuficiente.** La falta de segmentación de la red permitió al equipo rojo entrar, salir y moverse por el dominio de Solaris y Windows. Esto también les permitió recopilar una enorme cantidad de datos sobre la organización y sus sistemas. Los servidores internos podrían llegar a casi cualquier otro host del dominio, sin importar el tipo (servidor o estación de trabajo), propósito (computadora portátil del usuario, servidor de archivos, servidor de IDM, etc.) o ubicación física. El uso de la traducción de direcciones de red (NAT, por sus siglas en inglés) entre diferentes partes de la red ocultó aún más los flujos de datos, lo que dificultó la respuesta a incidentes.
- **Hallazgo n.º 3: la organización tenía relaciones de confianza con múltiples organizaciones asociadas,** lo que, combinado con credenciales débiles y conectividad de red, permitió al equipo rojo explotar y moverse lateralmente a un controlador de dominio asociado. Esto resalta el riesgo de permitir ciegamente la conectividad de redes de terceros y la importancia de monitorear regularmente tanto el acceso privilegiado como el material de credenciales confiables transitivas**.**
- **Hallazgo n.º 4: el personal defensivo de la organización no aisló lo suficiente su actividad investigativa defensiva.** Las organizaciones siempre deben comunicar información relativa a incidentes sospechosos fuera de banda, en lugar de hacerlo desde dentro de un dominio que saben que está comprometido. Mientras que los sistemas defensivos fueron desviados a otro dominio con confianzas correctas (unidireccionales), el equipo rojo identificó un posible vector de ataque a ese dominio a través del mismo servidor del IDM previamente comprometido. Algunos analistas también realizaron un análisis dinámico de los implantes sospechosos desde un entorno aislado conectado a Internet, informando al equipo rojo sobre los archivos y hosts específicos que estaban bajo investigación.
- **Hallazgo n.º 5: los defensores de la red no estaban familiarizados con las complejidades de su solución del IDM.** El equipo rojo de la CISA identificó cuentas no inscritas en el IDM y las utilizó con éxito junto con los tokens de acceso de usuarios ya existentes para eludir el IDM. El dispositivo, en su configuración activa, no fue probado exhaustivamente contra técnicas comunes de manipulación de credenciales ni se monitorearon alertas sobre comportamiento anómalo.
- **Hallazgo n.º 6: la organización tenía cierta segmentación de host basada en funciones, pero no era lo bastante granular.** La organización utilizaba funciones claramente definidas (administrador del servidor y administrador del dominio), pero no separaba lo suficiente las cuentas en sus propios servidores o sistemas, lo que permitió el aumento de privilegios.

Lección aprendida: la organización no recopiló, retuvo ni analizó registros de manera eficaz ni eficiente.

- **Hallazgo n.º 7**: **los analistas defensivos no tenían la información que necesitaban** debido a una combinación de problemas con la recopilación, el almacenamiento y el procesamiento de registros. Otras políticas recopilaron demasiados datos inútiles, generando ruido y ralentizando la investigación.
- **Hallazgo n.º 8: los procedimientos diarios de los defensores de la red no siempre incluían el análisis de las alertas de EDR**, y las herramientas que se instalaban solo proporcionaban una retención de 30 días para los archivos en cuarentena. En consecuencia, los investigadores no pudieron acceder a información oportuna que podría haber llevado a una detección más temprana de la actividad del equipo rojo.
- **Hallazgo n.º 9: los analistas forenses confiaron en artefactos del host que podrían haber sido modificados por un adversario.** En particular, se examinaron las marcas de tiempo de los archivos y las capturas de paquetes sin considerar la posibilidad de manipulación maliciosa.

Lección aprendida: la comunicación burocrática y los equipos descentralizados obstaculizaron a los defensores de la red de la organización.

- **Hallazgo n.º 10: el personal técnico de la organización estaba distribuido en equipos descentralizados.** La estructura de equipo aislada significaba que los equipos de IT, seguridad y otros equipos técnicos carecían de coherencia con sus herramientas, lo que generaba demasiado ruido que los defensores no podían analizar.
- **Hallazgo n.º 11: el equipo del SOC carecía de la capacidad para actualizar o implementar rápidamente conjuntos de reglas a través de los equipos de IT fragmentados**. La organización distribuyó la responsabilidad de herramientas individuales, como Sysmon, entre múltiples grupos, lo que dificultó la puntualidad y el mantenimiento de una postura defensiva.
- **Hallazgo n.º 12**: **el equipo forense de la organización produjo un informe de respuesta a incidentes que documentó la explotación inicial del enclave de Solaris por parte del equipo rojo. Sin embargo, el informe tuvo un alcance limitado y no documentó de forma adecuada la capacidad del equipo rojo para expandirse y persistir**. El éxito de la primera fase del equipo rojo, utilizando TTP conocidas públicamente, ilustró el riesgo comercial para todos los hosts de Solaris y, por extensión, el entorno Windows. Además, el informe interno de la organización solo se centró en servidores vulnerables y no tuvo en cuenta la capacidad de un agente de amenazas cibernéticas de expandirse y persistir en el enclave de Solaris.
  - Las investigaciones del administrador de Solaris sobre el equipo rojo no aparecieron ni en el informe ni en las resoluciones del SOC. La investigación de un administrador sobre una actividad inusual y probablemente maliciosa, en particular en medio de una investigación de infracciones confirmadas de hosts adyacentes, debería haber sido considerada en el informe como evidencia de movimiento lateral.

Lección aprendida: un enfoque de detección de "malo conocido" dificultó la detección de TTP alternativos.

- **Hallazgo n.º 13**: **defensores hiperconcentrados en IOC específicos, como atributos de archivos, marcos C2 particulares o dominios C2.** Los defensores de la red de la organización inicialmente no emplearon detecciones independientes de las herramientas, lo que les llevó a identificar de forma positiva algunas herramientas del equipo rojo, pero permanecieron ciegos ante el alcance total de la vulneración. Estaban acostumbrados a atrapar equipos rojos internos que utilizaban TTP específicas; introducir un nuevo "agente de amenaza" con nuevas TTP evitó casi todas las detecciones.
- **Hallazgo n.º 14**: **las reglas de detección eran visibles desde los sistemas comprometidos**, Lo que permitía al equipo rojo eludir las detecciones basadas en reglas y excepciones codificadas.
- **Hallazgo n.º 15: no hubo suficiente restricción de herramientas administrativas.** El personal técnico carecía de un conjunto estandarizado de herramientas administrativas, lo que dejaba todos los protocolos de administración remota disponibles para que los usaran los administradores, el equipo rojo de la CISA o los adversarios. Esto también creó un ruido excesivo que los defensores tuvieron que analizar de manera efectiva para determinar qué actividad era esperada y cuál era anómala.
- **Hallazgo n.º 16: no hubo suficiente seguimiento del software**. No hubo un proceso aparente de aprobación o seguimiento para la instalación de software en todo el dominio, lo que impidió que los analistas defensivos identificaran software anormal colocado por el equipo rojo. Un inventario completo de software aprobado ayudaría a los defensores a identificar comportamientos anormales y facilitaría la implementación de listas de aplicaciones permitidas.

FORTALEZAS DESTACADAS

La organización evaluada planificó y resolvió rápidamente múltiples problemas identificados, entre ellos los siguientes:

- **Cuentas de servicio de Windows**: la organización eliminó más del 30 % de las cuentas de servicio que se consideraron innecesarias. Hay un esfuerzo en curso para cambiar las contraseñas de las cuentas de servicio y aplicar el cumplimiento de la Guía de implementación técnica de seguridad (STIG, por sus siglas en inglés) recomendado por el Departamento de Defensa (DoD, por sus siglas en inglés) (más del 85 % se han cambiado desde la publicación de este informe).
- **IDM**: la organización está estudiando cómo mejorar su implementación del IDM y aplicar alertas de seguridad y prevenciones adicionales para el posible uso indebido de credenciales. Planean implementar capacidades adicionales de monitoreo basadas en identidad frente a activos de nivel cero.
- **Salida**: la organización implementó nuevos procesos para detectar y evitar que los servidores salgan de manera anómala de la red hacia Internet.
- **Soluciones basadas en host**: la organización utilizó características adicionales de su software antivirus, como puntajes de reputación, para buscar todos los valores atípicos en los tipos de archivos ejecutables e identificar instancias anómalas.
- **Hosts**: la organización desmanteló grupos de servidores y los reconstruyó completamente desde cero después de identificar numerosos problemas irreparables y configuraciones erróneas.
- **Credenciales de Solaris**: la organización cambió contraseñas, eliminó claves SSH, restringió permisos y eliminó cuentas innecesarias.

MEDIDAS DE MITIGACIÓN

Defensores de la red

La CISA recomienda que las organizaciones implementen las recomendaciones de la Tabla 1 para mitigar los hallazgos enumerados en la sección Lecciones aprendidas y hallazgos clave de este aviso. Estas medidas de mitigación coinciden con los objetivos de desempeño en ciberseguridad (CPG, por sus siglas en inglés) intersectoriales que desarrollaron la CISA y el Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés). Los CPG proporcionan un conjunto mínimo de prácticas y protecciones que la CISA y el NIST recomiendan que todas las organizaciones implementen. La CISA y el NIST basaron los CPG en marcos y orientación de ciberseguridad establecidos para brindar protección contra las amenazas, las tácticas, las técnicas y los procedimientos más comunes e impactantes. Consulte los objetivos de desempeño en ciberseguridad intersectoriales de la CISA para obtener más información sobre los CPG y las protecciones de referencia recomendadas.

Tabla 1: Recomendaciones para mitigar los problemas identificados

Hallazgo	Recomendación
Cortafuegos inadecuado entre el perímetro y los dispositivos internos	• Implementar firewalls de red internos y externos para inspeccionar, registrar o bloquear el tráfico desconocido o no autorizado. • Realizar una inspección profunda de paquetes para detectar tráfico de aplicaciones no coincidentes o flujos de datos cifrados.

Hallazgo	Recomendación
	• Restringir la salida de Internet a los hosts siempre que sea posible. • Establecer una línea base de la actividad normal del usuario, incluidas direcciones IP o dominios únicos.
Segmentación insuficiente de la red	• Aplicar el principio del mínimo privilegio para limitar la exposición de sistemas y servicios en la zona desmilitarizada (DMZ, por sus siglas en inglés). • Segmentar la DMZ en función de la sensibilidad de los sistemas y servicios, así como de la red interna [CPG 2.F]. • Segmentar redes para proteger activos y estaciones de trabajo de la exposición directa a Internet, teniendo en cuenta la criticidad del activo para las funciones comerciales, la sensibilidad de los datos que atraviesan el activo y los requisitos de acceso a Internet del activo. • Implementar y probar periódicamente firewalls, listas de control de acceso y sistemas de prevención de intrusiones. • Aprovechar las oportunidades para crear una segmentación natural de la red. Las VPN configuradas de forma segura utilizadas para computadoras portátiles remotas, por ejemplo, crean un lugar fácil para filtrar y monitorear el tráfico entrante.
Las relaciones de confianza entre dominios eran demasiado permisivas	• Restringir la conectividad de red (entrada y salida) únicamente a los servicios necesarios entre dominios confiables [CPG 2.E]. • Supervisar periódicamente el acceso privilegiado a través de entidades de seguridad externas (FSP, por sus siglas en inglés).
La actividad defensiva no estaba lo bastante aislada	• Realizar investigaciones de defensa de red fuera de banda [CPG 3.A]. • Realizar auditorías de seguridad periódicas y pruebas de penetración por parte de partes internas y externas. • Desarrollar e implementar un Plan de Respuesta a Incidentes (IRP, por sus siglas en inglés) integral y realizar simulacros y simulaciones regulares [CPG 2.S].
Las soluciones del IDM no se comprendieron ni se utilizaron por completo	• Inscribir todas las cuentas en las soluciones del IDM y probarlas contra técnicas comunes de manipulación de credenciales. • Integrar la solución del IDM con otros sistemas y aplicaciones, permitiendo la agilización de los flujos de trabajo.
Segmentación de host basada en roles insuficiente	• Establecer controles de acceso basados en roles (RBAC, por sus siglas en inglés) para asignar sistemáticamente permisos según las funciones laborales [CPG 2.E]. • Implementar un modelo de seguridad integral que incorpore la microsegmentación a nivel de host.

Hallazgo	Recomendación
No se monitorizan diariamente las alertas de EDR	• Desarrollar y documentar procedimientos operativos estándar (SOP, por sus siglas en inglés) para manejar las alertas de EDR [CPG 5.A]. • Establecer y mantener manuales de respuesta a incidentes. • Realizar auditorías y revisiones periódicas del proceso de manejo de las alertas de EDR.
Se confiaba demasiado en los artefactos del host	• Aplicar e implementar soluciones de monitoreo de integridad de archivos (FIM, por sus siglas en inglés). • Revisar y ajustar periódicamente los permisos de acceso, adhiriéndose al principio del mínimo privilegio [CPG 2.E]. • Establecer procesos forenses adecuados para garantizar la integridad.
La burocracia y la descentralización de los defensores de la red obstaculizaron la comunicación y la coherencia	• Introducir iniciativas de capacitación cruzada para cultivar una cultura colaborativa. • Fomentar el establecimiento de proyectos multifuncionales. • Utilizar plataformas de colaboración que integren sin problemas diversas herramientas y sistemas.
Notificación insuficiente de respuesta a incidentes internos	• Promover una cultura de mejora continua, fomentando al mismo tiempo un enfoque proactivo entre los empleados para notificar rápidamente las actividades sospechosas. • Tratar los incidentes sospechosos de amenaza como una violación confirmada, y tener en cuenta la capacidad de un agente de amenazas de moverse lateralmente al definir el alcance de los esfuerzos de respuesta a incidentes.
Enfoque en IOC conocidos o comunes	• Utilizar registro centralizado y métodos de detección independientes de herramientas. • Aprovechar las fuentes de inteligencia sobre amenazas integrándolas en una herramienta SIEM. • Implementar actualizaciones periódicas para los IOC y las TTP, con capacidad de personalización para abordar el panorama de amenazas específico [CPG 3.A].
Las reglas de detección eran visibles desde los sistemas comprometidos	• Integrar mecanismos de detección en tiempo de ejecución mientras se eliminan archivos de configuración legibles por todos de las implementaciones del instalador cuando corresponda.

Hallazgo	Recomendación
Restricción insuficiente de las herramientas de administración	• Mejorar la postura de seguridad mediante la implementación de una lista blanca de aplicaciones para garantizar que solo se permitan aplicaciones confiables y aprobadas [CPG 2.Q]. • Aplicar el principio del mínimo privilegio, otorgando a los usuarios solo el nivel mínimo de acceso necesario para realizar las funciones laborales.
Seguimiento insuficiente del software	• Realizar un inventario completo de activos y establecer una línea de base para el comportamiento [CPG 1.A]. • Utilizar una solución de gestión de activos de software (SAM, por sus siglas en inglés) que ofrezca capacidades integrales de seguimiento, informes y gestión de cumplimiento. • Implementar herramientas de descubrimiento y monitoreo automatizados para escanear e identificar continuamente software nuevo y existente.

La CISA recomienda que las organizaciones implementen las recomendaciones de la Tabla 2 para mitigar otros problemas identificados que pueden descubrirse mediante pruebas de penetración tradicionales o evaluaciones de equipo rojo.

Tabla 2: Recomendaciones para mitigar los problemas identificados

Problema	Recomendación
Las cuentas tenían demasiados privilegios, y la red de la organización contenía cuentas de servicio innecesarias	• Aplicar el principio del mínimo privilegio al asignar permisos a las cuentas de usuario. Auditar las membresías de grupos existentes, eliminar privilegios innecesarios y eliminar los grupos/usuarios anidados innecesarios. • Supervisar el bloqueo de cuentas, especialmente en cuentas administrativas, y cambiar a una política de desbloqueo de cuentas manual. • Aumentar la supervisión de las cuentas de mayor riesgo, como las cuentas de servicio, que tienen muchos privilegios y un patrón de comportamiento predecible (p. ej., análisis que se ejecutan de manera confiable a una determinada hora del día). • Los usuarios privilegiados deben tener cuentas de usuario dedicadas basadas en funciones y hosts de salto asociados para iniciar sesión en recursos críticos.
Configuración de EDR insuficiente	• Asegurarse de que todos los hosts tengan algún tipo de EDR instalado. • Implementar una EDR capaz de detectar técnicas de ejecución u ocultación comúnmente conocidas.
Credenciales inseguras e insuficientes	• Asegurarse de que las credenciales y los documentos confidenciales no se almacenen en un lugar accesible. • Exigir contraseñas seguras y complejas [CPG 2.B]. Para obtener más información, consulte Secure Our World: Requerir contraseñas seguras de la CISA.

Nota: las medidas de mitigación anteriores se aplican a las organizaciones de infraestructura fundamental con entornos híbridos o en las instalaciones. La CISA anima a todas las organizaciones a **priorizar la compra de productos de fabricantes que demuestren principios de seguridad desde el diseño**, como lo evidencian las publicaciones de seguimiento de empresas que han firmado el Compromiso de seguridad desde el diseño.

Fabricantes de software

La CISA reconoce que el software inseguro es la causa principal de muchas fallas; la responsabilidad no debe recaer en el usuario final. La CISA insta a los fabricantes de software a implementar lo siguiente:

- **Eliminar las contraseñas predeterminadas** y determinar qué prácticas de contraseñas deben requerirse (como la longitud mínima de la contraseña y la prohibición de contraseñas violadas conocidas). Configurar el software para utilizar esquemas de autenticación más seguros de forma predeterminada.

- **Proporcionar registros sin costo adicional**. Los servicios en la nube y los productos en las instalaciones deben comprometerse a generar y almacenar registros relacionados con la seguridad sin costo adicional.
- **Trabajar con proveedores de gestión de eventos e información de seguridad (SIEM, por sus siglas en inglés) y orquestación, automatización y respuesta de seguridad (SOAR, por sus siglas en inglés)**, junto con los clientes, para comprender cómo los equipos de respuesta usan los registros para investigar incidentes. El objetivo es desarrollar registros que produzcan una historia completa del evento.
- **Eliminar dependencias de software innecesarias**. El software innecesario aumenta la superficie de ataque disponible para los adversarios y puede introducir vulnerabilidades adicionales. Mitigarlas requiere una inversión significativa, que consume recursos como tiempo y personal técnico, y aumenta el nivel de esfuerzo de seguridad.

Estas medidas de mitigación se alinean con las tácticas proporcionadas en la guía conjunta Cambiar el equilibrio del riesgo de la ciberseguridad: principios y enfoques para un software seguro desde el diseño. La CISA insta a los fabricantes de software a asumir la responsabilidad de mejorar los resultados de seguridad de sus clientes mediante la aplicación de estas y otras tácticas de seguridad desde el diseño. Utilizando tácticas de seguridad desde el diseño, los fabricantes de software pueden hacer que sus líneas de productos sean seguras desde el primer momento, sin necesidad de que los clientes gasten recursos adicionales en cambios de configuración, compras de registros y softwares de seguridad, supervisión y actualizaciones de rutina.

Para obtener más información sobre el concepto “seguridad desde el diseño”, consulte la página web Seguridad desde el diseño de la CISA. Para obtener más información sobre las configuraciones erróneas más comunes y orientación para reducir su prevalencia, consulte el documento consultivo conjunto Los equipos rojo y azul de la NSA y la CISA comparten las diez principales configuraciones erróneas de ciberseguridad.

VALIDAR LOS CONTROLES DE SEGURIDAD

Además de aplicar las medidas de mitigación, la CISA recomienda ejecutar, probar y validar el programa de seguridad de su organización frente a los comportamientos de amenazas asignados al marco MITRE ATT&CK para entornos empresariales que figuran en este aviso. La CISA recomienda que pruebe su inventario establecido de controles de seguridad para evaluar cómo se desempeñan frente a las técnicas de ATT&CK descritas en este aviso.

Para empezar:

1. Seleccione una de las técnicas de ATT&CK descritas en este aviso (consulte las tablas 3 a 11).
2. Alinee sus tecnologías de seguridad con la técnica.
3. Pruebe sus tecnologías con la técnica.
4. Analice el desempeño de sus tecnologías de detección y prevención.
5. Repita el proceso para todas las tecnologías de seguridad a fin de obtener un conjunto de datos completos sobre el desempeño.
6. Ajuste su programa de seguridad (esto incluye a las personas, los procesos y las tecnologías) en función de los datos que se generaron en este proceso.

La CISA recomienda probar su programa de seguridad de forma continua, a escala, en un entorno de producción para garantizar un desempeño óptimo frente a las técnicas de MITRE ATT&CK identificadas en este aviso.

RECURSOS

- Seguridad de la red en capas mediante segmentación
- Práctica recomendada: mejorar la ciberseguridad de los sistemas de control industrial con estrategias de defensa en profundidad
- Orientación sobre suplantación de identidad: Detener el ciclo de ataque en la fase uno
- BOF
- Detección de DCSync
- Descripción general del secuestro de dominios de aplicaciones

DESCARGO DE RESPONSABILIDAD

La información contenida en este informe se proporciona “tal cual” solo con fines informativos. La CISA no promociona a ninguna entidad comercial, producto, empresa o servicio, incluidas las entidades, los productos o los servicios vinculados en este documento. Cualquier referencia a entidades comerciales, productos, procesos o servicios específicos mediante marcas de servicio, marcas registradas, fabricantes, o de otro modo, no constituye ni implica la promoción, la recomendación ni la preferencia por parte de la CISA.

HISTORIAL DE VERSIONES

11 de julio de 2024: versión inicial.

APÉNDICE: TÁCTICAS Y TÉCNICAS DE MITRE ATT&ACK

Consulte las tablas 3 a 11 para conocer todas las tácticas y técnicas de agentes de amenazas a las que se hace referencia en este aviso.

Tabla 3: Reconocimiento

Nombre de la técnica	Identificación	Uso
Búsqueda de páginas web propiedad de la víctima	T1594	El equipo rojo de la CISA utilizó herramientas y servicios de código abierto para investigar la presencia de la organización en Internet y recopilar información, incluidos nombres, funciones e información de contacto.
Recopilar información sobre la red de la víctima: DNS	T1590.002	El equipo rojo recopiló información sobre los registros DNS de la organización, que revelaron varios detalles sobre la red interna de la organización.
Recopilar información sobre la identidad de la víctima: nombres de empleados	T1589.003	El equipo rojo de la CISA recopiló los nombres de los empleados de las organizaciones evaluadas para utilizar sus direcciones de correo electrónico para segmentaciones específicas basadas en funciones y responsabilidades.
Recopilar información sobre la organización de la víctima: funciones de identidad	T1591.004	El equipo rojo de la CISA seleccionó a individuos específicos de la organización evaluada y los atacó con cargas útiles de phishing.

Tabla 4: Mando y control

Nombre de la técnica	Identificación	Uso
Protocolo de capa de aplicación: protocolos web	T1071.001	El equipo rojo explotó CVE-2022- 21587 y ejecutó un RAT que proporcionaba C2 consistente a través de puertos abiertos del protocolo de control de transmisión (TCP, por sus siglas en inglés).

Nombre de la técnica	Identificación	Uso
Puerto no estándar	T1571	El equipo rojo usó SSH a través de los puertos `80` o `443` al establecer C2 saliente.
Proxy: domain fronting	T1090.004	El equipo rojo de la CISA aprovechó el domain fronting para redirigir y ocultar su tráfico.

Tabla 5: Acceso a credenciales

Nombre de la técnica	Identificación	Uso
Fuerza bruta: descifrado de contraseñas	T1110.002	El equipo rojo descifró la contraseña de una cuenta utilizando una lista de palabras comunes.
Volcado de credenciales de OS: DCSync	T1003.006	El equipo rojo de la CISA extrajo las credenciales del dominio a través de DCSync para obtener acceso completo al dominio.
Credenciales sin protección: historial bash	T1552.003	El equipo rojo obtuvo una contraseña buscando en el historial de comandos bash de un usuario, lo que proporcionó acceso adicional sin privilegios a toda la red.

Tabla 6: Descubrimiento

Nombre de la técnica	Identificación	Uso
Descubrimiento de confianza del dominio	T1482	El equipo rojo de la CISA inspeccionó las relaciones de confianza del dominio de la organización evaluada a través de LDAP e identificó conexiones potenciales en organizaciones externas a las cuales moverse lateralmente.

Nombre de la técnica	Identificación	Uso
Descubrimiento de archivos y directorios	T1083	El equipo rojo extrajo los datos de numerosos servidores internos y descubrió un recurso compartido mal configurado que contenía nombres de usuario y contraseñas en texto simple para varias cuentas de servicio privilegiadas.

Tabla 7: Aumento de privilegios

Nombre de la técnica	Identificación	Uso
Flujo de ejecución de secuestro: intercepción de ruta mediante la variable de entorno PATH	T1574.007	El equipo rojo secuestró el flujo de ejecución de un programa que utilizaba una ruta relativa en lugar de una ruta absoluta, lo que permitía la captura de la contraseña de la cuenta.
Manipulación de tokens de acceso: suplantación de identidad o robo de tokens	T1134.001	El equipo rojo de la CISA se hizo pasar por los tokens de los usuarios actuales para explotar sesiones válidas y eludir el IDM de la organización.
Manipulación de tokens de acceso: crear y suplantar tokens	T1134.003	El equipo rojo de la CISA creó nuevos tokens y sesiones de inicio de sesión para cuentas no registradas en el IDM para aumentar privilegios.

Tabla 8: Movimiento lateral

Nombre de la técnica	Identificación	Uso
Servicios remotos: SSH	T1021.004	El equipo rojo de la CISA utilizó SSH con una cuenta válida para moverse por el enclave.
Proxy	T1090	El equipo rojo utilizó un proxy SOCKS para evitar conexiones directas a su infraestructura y ocultar la fuente del tráfico malicioso.

Nombre de la técnica	Identificación	Uso
Uso de material de autenticación alternativo: Pass the Hash	T1550.002	Las operaciones del equipo rojo se vieron obstaculizadas por el IDM de la organización cuando bloqueó los intentos del equipo de eludir los controles de acceso al sistema utilizando diferentes tipos de hash para la autenticación.
Uso de material de autenticación alternativo: Pass the Ticket	T1550.003	Las operaciones del equipo rojo de la CISA se vieron obstaculizadas por el IDM de la organización cuando bloqueó los intentos del equipo de eludir los controles de acceso al sistema utilizando tickets de Kerberos para la autenticación.

Tabla 9: Recopilación

Nombre de la técnica	Identificación	Uso
Datos del sistema local	T1005	El equipo rojo de la CISA buscó en cada host archivos que contuvieran información sensible o interesante, como hashes de contraseñas, información de cuentas, configuraciones de red, etc.

Tabla 10: Persistencia

Nombre de la técnica	Identificación	Uso
Tarea/trabajo programado: Cron	T1053.003	El equipo rojo utilizó la utilidad `cron` para programar tareas y ejecutar código malicioso dentro de sistemas Unix en horas específicas.
Tarea/trabajo programado: At	T1053.002	El equipo rojo de la CISA utilizó la utilidad `at` para programar tareas y ejecutar código malicioso dentro de sistemas Unix a una hora y fecha específica.

Nombre de la técnica	Identificación	Uso
Flujo de ejecución de secuestro: AppDomainManager	T1574.014	El equipo rojo ejecutó cargas maliciosas secuestrando el modo en que `.NET AppDomainManager` carga los ensamblajes.
Cuentas válidas: cuentas del dominio	T1078.002	El equipo rojo de la CISA utilizó con regularidad cuentas de dominio válidas comprometidas administradas por Active Directory, dando acceso a los recursos del dominio.

Tabla 11: Evasión defensiva

Nombre de la técnica	Identificación	Uso
Enmascaramiento: tarea o servicio de enmascaramiento	T1036.004	El equipo rojo enumeró los archivos locales y los procesos en ejecución para recopilar información para que sus cargas útiles y mecanismos de persistencia parezcan una actividad legítima.
Información o archivos ocultados	T1027	El equipo rojo de la CISA cifró, codificó y ocultó sus ejecutables y canales C2 para evadir las defensas en toda la red.
Modificación de permisos de archivos y directorios: modificación de permisos de archivos y directorios de Linux y Mac	T1222.002	El equipo rojo modificó los permisos de los archivos con los comandos `touch` y `chmod/chown` para ocultar su actividad y mezclarse con otros archivos del entorno.
Eliminación del indicador: marca de tiempo	T1070.006	El equipo rojo de la CISA modificó las marcas de tiempo de los archivos para ocultar su actividad operativa.