TLP:CLEAR

ORIENTACIÓN CONJUNTA:

Identificación y mitigación de las técnicas “living off the land”

Publicación: 7 de febrero de 2024

Agencia de Ciberseguridad y Seguridad de Infraestructura de EE. UU. (U.S. Cybersecurity and Infrastructure Security Agency)
Agencia de Seguridad Nacional de EE. UU. (U.S. National Security Agency)
Oficina Federal de Investigaciones de EE. UU. (U.S. Federal Bureau of Investigation)
Departamento de Energía de EE. UU. (U.S. Department of Energy)
Agencia de Protección Ambiental de EE. UU. (U.S. Environmental Protection Agency)
Administración de Seguridad del Transporte de EE. UU. (U.S. Transportation Security Administration)
Centro Australiano de Ciberseguridad (Australian Cyber Security Centre) de la Dirección de Señales de Australia (Australian Signals Directorate)
Centro Canadiense de Ciberseguridad (Canadian Centre for Cyber Security; Centro Cibernético), parte del Establecimiento de Seguridad de las Comunicaciones (CSE, por sus siglas en inglés)
Centro Nacional de Ciberseguridad del Reino Unido (United Kingdom National Cyber Security Centre)
Centro Nacional de Ciberseguridad de Nueva Zelanda (New Zealand National Cyber Security Centre)

Este documento está marcado como TLP:CLEAR. Los receptores pueden compartir esta información sin restricciones. La información está sujeta a las normas estándar de derechos de autor. Para obtener más información sobre el protocolo de semáforo, consulte https://www.cisa.gov/tlp.

TLP:CLEAR

Resumen

Esta guía, elaborada por la Agencia de Ciberseguridad y Seguridad de Infraestructura de EE. UU. (CISA, por sus siglas en inglés), la Agencia de Seguridad Nacional (NSA, por sus siglas en inglés), la Oficina Federal de Investigaciones (FBI, por sus siglas en inglés) y las siguientes agencias (en lo sucesivo, denominadas "agencias autoras"), proporciona información sobre las técnicas "living off the land" (LOTL) comunes, así como de las deficiencias habituales en las capacidades de ciberdefensa.

- Departamento de Energía de EE. UU. (DOE, por sus siglas en inglés);
- Agencia de Protección Ambiental de EE. UU. (EPA, por sus siglas en inglés);
- Administración de Seguridad del Transporte de EE. UU. (TSA, por sus siglas en inglés);
- Centro Australiano de Ciberseguridad (ACSC, por sus siglas en inglés) de la Dirección de Señales de Australia (ASD, por sus siglas en inglés);
- Centro Canadiense de Ciberseguridad (Canadian Centre for Cyber Security; Centro Cibernético), parte del Establecimiento de Seguridad de las Comunicaciones (CSE, por sus siglas en inglés);
- Centro Nacional de Ciberseguridad del Reino Unido (NCSC-UK, por sus siglas en inglés);
- Centro Nacional de Ciberseguridad de Nueva Zelanda (NCSC-NZ, por sus siglas en inglés).

La guía conjunta para los defensores de redes se centra en cómo mitigar las deficiencias identificadas y detectar y buscar actividad de las técnicas LOTL. La información incluida en esta guía conjunta proviene de un aviso conjunto publicado anteriormente, las ejecuciones de respuesta a incidentes que llevaron a cabo varias de las agencias autoras, las evaluaciones del equipo rojo por parte de varias de las agencias autoras utilizando las técnicas LOTL para obtener un acceso persistente y no detectado, y los esfuerzos de colaboración con la industria.

Las agencias autoras han observado que los agentes de amenazas cibernéticas, como los patrocinados por el Estado de la República Popular China (PRC, por sus siglas en inglés) [1],[2] y la Federación de Rusia [3], aprovechan las técnicas LOTL para poner en riesgo a las organizaciones de infraestructura fundamental y mantener un acceso persistente a estas. Las agencias autoras publican esta guía conjunta para los defensores de redes (entre ellos, los buscadores de amenazas) porque el uso malicioso de las técnicas LOTL se manifiesta cada vez más en el entorno general de las amenazas cibernéticas.

Los agentes de amenazas cibernéticas que aprovechan las técnicas LOTL hacen mal uso de las herramientas y los procesos nativos en los sistemas, y a menudo utilizan binarios "living off the land". Utilizan las técnicas LOTL en varios entornos de tecnologías de la información (IT, por sus siglas en inglés), lo que incluye los entornos híbridos, en las instalaciones, en la nube o de Windows, Linux y macOS. Las técnicas LOTL permiten que los agentes de amenazas lleven a cabo sus operaciones de forma discreta, ya que pueden camuflar la actividad con comportamientos típicos del sistema y de la red. Al hacer esto, posiblemente eluden las capacidades básicas de seguridad de los puntos de conexión.

Las técnicas LOTL son particularmente efectivas por los siguientes motivos:

- Muchas organizaciones carecen de prácticas efectivas de administración de redes y seguridad (como referencias establecidas) que respalden la detección de actividades

maliciosas con las técnicas LOTL. Esto dificulta que los defensores de redes puedan distinguir el comportamiento legítimo del malicioso y llevar a cabo análisis de comportamiento, detección de anomalías y una búsqueda proactiva.
- Existe una falta general de indicadores de riesgo (IOC, por sus siglas en inglés) convencionales que se asocien con la actividad, lo que dificulta los esfuerzos de los defensores de redes para identificar, monitorear y categorizar los comportamientos maliciosos.
- Permiten a los agentes de amenazas cibernéticas evitar invertir en el desarrollo y la implementación de herramientas personalizadas.

Incluso para las organizaciones que adoptan las prácticas recomendadas, distinguir las actividades maliciosas con técnicas LOTL de los comportamientos legítimos es difícil, ya que, con frecuencia, los defensores de redes hacen lo siguiente:

- Operan en silos separados de los equipos de IT y sus flujos de trabajo operativos.
- Dependen principalmente de los sistemas de detección y respuesta de puntos de conexión (EDR, por sus siglas en inglés) no ajustados, que pueden no emitir alertas sobre la actividad de las técnicas LOTL, e IOC discretos que los atacantes pueden modificar u ofuscar para evitar la detección.
- Mantienen configuraciones de registro predeterminadas, que no registran de forma completa los indicadores de las técnicas LOTL ni información lo suficientemente detallada para diferenciar la actividad maliciosa de la actividad de administración de IT legítima.
- Tienen dificultades para identificar un volumen relativamente pequeño de actividad maliciosa dentro de grandes volúmenes de datos de registro.

Las agencias autoras instan encarecidamente a las organizaciones de infraestructura fundamental a aplicar las siguientes orientaciones de detección y prácticas recomendadas *priorizadas* para buscar posibles actividades de las técnicas LOTL. Estas recomendaciones son parte de una estrategia de ciberseguridad multifacética que permite la relación y el análisis de datos efectivos. No existe una solución infalible para evitar o detectar la actividad de las técnicas LOTL por completo, pero, si aplican estas prácticas recomendadas, las organizaciones pueden posicionarse mejor para lograr una detección y una mitigación más efectivas.

Prácticas recomendadas de detección:

1. Implemente registros detallados y agrupe los registros en una ubicación centralizada fuera de banda que sea de escritura única y lectura múltiple para evitar el riesgo de que los atacantes modifiquen o borren los registros.
2. Establezca y mantenga referencias de actividades administrativas, de red, de usuarios y de aplicaciones, así como restricciones de privilegios mínimos, de forma continua.
3. Cree o adquiera automatización (como modelos de aprendizaje automático) para revisar continuamente todos los registros a fin de comparar las actividades actuales con las referencias de comportamiento establecidas y emitir alertas sobre las anomalías especificadas.
4. Reduzca el ruido de las alertas ajustándolas según la prioridad (urgencia y gravedad) y revise de forma continua las detecciones en función de las tendencias de actividad.
5. Aproveche los análisis del comportamiento de usuarios y entidades (UEBA, por sus siglas en inglés).

Prácticas recomendadas para el refuerzo:

1. Aplique y consulte las orientaciones recomendadas por el proveedor para reforzar la seguridad.
2. Implemente listas de aplicaciones permitidas y supervise el uso de los binarios "living off the land" (LOLBins, por sus siglas en inglés) comunes.
3. Mejore la segmentación y la supervisión de las redes de IT y de tecnología operativa (OT, por sus siglas en inglés).
4. Implemente controles de autenticación y autorización para todas las interacciones entre softwares y entre humanos y softwares, independientemente de la ubicación de la red.

Para obtener detalles y recomendaciones adicionales, consulte las secciones "Sugerencias de prácticas recomendadas" y "Recomendaciones de detección y búsqueda". Si se identifica actividad de las técnicas LOTL, los defensores deben denunciar la actividad a las agencias relevantes, según corresponda, y aplicar la orientación de correcciones que figura en esta guía.

Además, esta guía ofrece recomendaciones para que los fabricantes de software reduzcan la prevalencia de las fallas explotables en software que posibiliten las técnicas LOTL. En muchos casos, los defectos de software o las configuraciones predeterminadas no seguras permiten que los agentes de amenazas cibernéticas lleven a cabo actividades cibernéticas maliciosas utilizando técnicas LOTL. Las agencias autoras exhortan encarecidamente a los fabricantes de software a responsabilizarse de los resultados de seguridad de sus clientes aplicando las recomendaciones de seguridad desde el diseño que figuran en esta guía y en la guía conjunta de seguridad desde el diseño de la CISA: Cambio del equilibrio de los riesgos de ciberseguridad: principios y enfoques para el software seguro desde el diseño.

Los fabricantes de tecnología pueden reducir la efectividad de las técnicas LOTL elaborando productos que sean seguros desde el diseño, lo que incluye lo siguiente:

- Deshabilitar o quitar protocolos innecesarios por defecto.
- Limitar la accesibilidad de la red en la medida posible.
- Limitar los procesos y programas que se ejecutan con privilegios elevados.
- Habilitar la autenticación de múltiples factores (MFA, por sus siglas en inglés) resistente a la suplantación de identidad como característica predeterminada.
- Proporcionar registros seguros de alta calidad sin costo adicional, más allá de los costos de procesamiento y almacenamiento.
- Eliminar las contraseñas y credenciales predeterminadas al instalar software.
- Limitar o quitar la ejecución de código dinámico.

Índice

Introducción

Las agencias autoras publican esta guía conjunta para advertir a los defensores de redes que los agentes de amenazas cibernéticas, como los agentes patrocinados por el Estado de la PRC [1],[2] y la Federación de Rusia [3], están aprovechando las técnicas "living off the land" (LOTL) para poner en riesgo a las organizaciones de infraestructura fundamental y mantener su persistencia en estas.

Esta guía proporciona información para los defensores de redes, como los buscadores de amenazas, sobre las técnicas LOTL y las debilidades de la defensa de redes que permiten a los agentes utilizar las técnicas LOTL sin que los detecten, además de brindar orientación para la detección. La información y la orientación provienen de lo siguiente:

- Un aviso conjunto publicado anteriormente.
- Las ejecuciones de respuesta a incidentes por parte de las agencias autoras, incluida una respuesta reciente por parte de la CISA, en la que los agentes de amenazas cibernéticas tenían acceso persistente y a largo plazo al entorno de la víctima y pusieron en riesgo el controlador de dominio (DC, por sus siglas en inglés). Los agentes utilizaron técnicas LOTL durante toda la intrusión.
- Las evaluaciones del equipo rojo de las agencias autoras, lo que incluye las evaluaciones del equipo rojo de la CISA para examinar las redes del Poder Ejecutivo Civil Federal (FCEB, por sus siglas en inglés) y, a pedido del propietario de la red, las redes no federales. (Los equipos rojos de la CISA utilizan con frecuencia técnicas LOTL conocidas públicamente para la ejecución, la persistencia, el movimiento lateral, el descubrimiento y el acceso a las credenciales, y los defensores de redes rara vez detectan su actividad).
- Los esfuerzos de colaboración con expertos de otras agencias y de la industria en ciberseguridad y respuesta a incidentes.

Técnicas "living off the land"

Las técnicas LOTL involucran el mal uso de herramientas y procesos nativos en los sistemas, especialmente de los binarios "living off the land" (a menudo denominados "LOLBins"), para camuflarse con las actividades normales del sistema y operar de forma discreta con una menor probabilidad de detección o bloqueo, debido a que estas herramientas ya están implementadas en el entorno y se consideran de confianza. Los agentes de amenazas cibernéticas utilizan las técnicas LOTL de manera efectiva en varios entornos, como los entornos híbridos, en las instalaciones, en la nube o de Windows, Linux y macOS, en parte porque estas permiten evitar invertir en el desarrollo y la implementación de herramientas personalizadas.

Los equipos de respuesta a incidentes de las agencias autoras observan principalmente que los agentes de amenazas cibernéticas aprovechan las técnicas LOTL en entornos de Windows debido al uso generalizado del sistema operativo en entornos corporativos y empresariales. En entornos de Windows, los agentes de amenazas cibernéticas utilizan herramientas, servicios y características nativos, y se basan en el hecho de que estos componentes son universales y generalmente confiables.

En entornos de macOS, las técnicas LOTL también se denominan "living off the orchard" (LOO, por sus siglas en inglés). Los agentes maliciosos explotan entornos de scripting nativos, herramientas integradas, configuraciones del sistema y binarios denominados "LOOBins". En entornos híbridos, los agentes de amenazas cibernéticas explotan cada vez más los sistemas físicos y basados en la

nube aprovechando sofisticadas técnicas LOTL. Consulte el "Apéndice A: Técnicas LOTL en entornos híbridos y de macOS" para obtener más información sobre los LOOBins.

Para obtener más información sobre los LOLBins que se sabe que se usan de forma maliciosa, consulte el "Apéndice C: LOLBins conocidos que se utilizan de forma maliciosa" y los siguientes recursos:

- Repositorio GitHub del proyecto LOLBAS: Binarios, scripts y bibliotecas "living off the land".
- Para obtener una lista de los binarios Unix que se pueden usar en las técnicas LOTL, consulte gtfobins.github.io.
- Para obtener una lista de los LOLBins de macOS que se pueden usar en las técnicas LOTL, consulte loobins.io.
- Para obtener una lista de los controladores "living off the land" de Windows, consulte loldrivers.io.

Además de LOLBins, los agentes de amenazas cibernéticas también usan software de acceso remoto de terceros, p. ej., administración y supervisión remota, administración de configuración de puntos de conexión, EDR, administración de correcciones, sistemas de administración de dispositivos móviles y herramientas de administración de bases de datos. Estas herramientas, algunas de las cuales se diseñaron para administrar y proteger dominios, vienen con una funcionalidad integrada que puede ejecutar comandos en todos los hosts de clientes en la red, lo que incluye a los hosts confidenciales, como los controladores de dominio. Por necesidad, estas herramientas tienen altos privilegios que se requieren para la administración del sistema objetivo. Consulte el "Apéndice B: Herramientas externas para técnicas LOTL" si desea obtener más información.

Debilidades de la defensa de redes

Las técnicas LOTL son efectivas porque muchas organizaciones no implementan capacidades de las prácticas recomendadas de seguridad que admitan la detección de actividades maliciosas. Los equipos rojos de la CISA con frecuencia aprovechan las técnicas LOTL para obtener un acceso persistente y no detectado. Estas evaluaciones del equipo rojo demuestran de qué forma un adversario podría lograr poner en riesgo todo el dominio con poca o ninguna inversión en herramientas. En muchos de estos casos, los equipos rojos de la CISA determinaron que la organización evaluada no contaba con referencias de seguridad, lo cual permitía que los LOLBins se ejecutaran y evitaba que los analistas pudieran identificar actividades anómalas. En otros casos, las organizaciones no ajustaron de forma adecuada sus herramientas de detección para reducir el ruido de las alertas, lo que produjo un nivel incontrolable de alertas que había que examinar y sobre las cuales había que tomar medidas. Los sistemas automatizados, como las funciones de administración continua que utilizan cuentas de servicio y escáneres de vulnerabilidades, con frecuencia llevan a cabo acciones posiblemente sospechosas con altos privilegios que llenan de eventos de registro a los analistas si no se categorizan de forma correcta.

Incluso en los casos en que las organizaciones con posturas cibernéticas más maduras han aplicado las prácticas recomendadas, distinguir las actividades maliciosas con técnicas LOTL de los comportamientos legítimos es difícil, ya que las técnicas LOTL permiten a los agentes camuflarse con las actividades normales del sistema y de la red.

- Los administradores de IT utilizan los LOLBins de forma legítima y, por lo tanto, estos binarios cuentan con atributos confiables (por ejemplo, hashes de archivos o firmas

digitales). Esto puede confundir a los defensores de redes y hacer que piensen que son seguros para todos los usuarios. Los administradores del sistema deben identificar el uso responsable y permitido de los LOLBins y aplicarlo como política.

- Un concepto erróneo común es pensar que, como un programa es una herramienta legítima de administración de IT, es seguro permitirlo de forma global. Las políticas generales de "permisión" para los LOLBins comunes amplían la superficie de ataque. Los administradores del sistema deben restringir las políticas de "permisión", limitar el uso de inicio de sesión y los intentos de uso, y crear alertas para los comportamientos que se desvíen del uso permitido.
- Por ejemplo, los equipos rojos de la CISA a menudo encuentran LOLBins accesibles para todos los usuarios, incluso para los usuarios estándar. Los equipos rojos de la CISA también encuentran excepciones demasiado amplias para la herramienta PsExec porque los administradores la utilizan con regularidad para sus tareas laborales. Los agentes maliciosos a menudo aprovechan la falta de restricciones para moverse lateralmente sin que los detecten.

Este asunto se agrava por las posturas defensivas y las capacidades de detección insuficientes. En muchos casos, los equipos de respuesta a incidentes y los equipos rojos de las agencias autoras descubren con frecuencia que los defensores de redes hacen lo siguiente:

- Operan en silos que separan a los profesionales de seguridad de los equipos de IT y sus flujos de trabajo operativos.
  - En silos, los defensores de redes no pueden crear una referencia del comportamiento de los usuarios (normales y privilegiados).
  - La falta de mecanismos de comunicación abierta y colaboración entre los profesionales de seguridad y los equipos de IT también aumenta el tiempo necesario para solucionar las vulnerabilidades o investigar comportamientos anormales. En organizaciones grandes, las investigaciones pueden llevar varios meses, durante los cuales los agentes de amenazas cibernéticas amplían su acceso.
  - Los silos también pueden afectar negativamente las decisiones empresariales (de recursos); por ejemplo, los equipos rojos de la CISA han observado que los líderes toman decisiones basadas en el riesgo comercial debido a sistemas heredados o softwares inseguros sin considerar lo suficiente las evaluaciones que presentan sus propios equipos de seguridad. Esto puede provocar que sistemas fácilmente explotables permanezcan en la red evaluada.
- Dependen principalmente de los sistemas de EDR no ajustados y los IOC discretos.
  - Las técnicas LOTL pueden evitar la activación de productos de EDR. Los proveedores de EDR pueden asumir que los LOLBins son "seguros", o los administradores preocupados por que el sistema de EDR bloquee sus herramientas solicitan configuraciones estándar para permitir los LOLBins.
  - Los agentes de amenazas pueden modificar con facilidad los IOC conocidos, como nombres de archivos y argumentos de líneas de comando, o modificar el contenido para cambiar el hash. Los agentes de amenazas cibernéticas modifican los IOC comunes, como nombres y rutas de archivos, y destinos de controles y comandos, para evitar las detecciones convencionales de "elementos maliciosos conocidos". Los agentes patrocinados por el Estado explotan la sintaxis alternativa en argumentos de líneas de comando convencionales o en aquellos que utilizan variables del entorno.[1] Por

ejemplo, `ntdsutil snapshot “activate instance ntds” create quit quit` también es efectivo cuando se acorta a `ntdsutil snapshot “ac i ntds” create quit quit`.

- Mantienen configuraciones de registro predeterminadas que carecen de un registro matizado, extenso y centralizado.
  - Las configuraciones de registro predeterminadas no reflejarán toda la actividad. Cada red es única con respecto a la actividad y los archivos benignos. Depender de las configuraciones predeterminadas y de las garantías de los proveedores nunca es suficiente para defender las redes por completo. Las pruebas y validaciones regulares de las configuraciones activas son esenciales para lograr una defensa proactiva. Además, los sistemas heredados o el software especializado (por ejemplo, hosts basados en Unix y dispositivos de infraestructura, como enrutadores) rara vez vienen con una funcionalidad de registro avanzada.
  - Muchas aplicaciones, incluso cuando se configuran correctamente, producen registros que requieren procesamiento adicional a fin de que puedan ser útiles para los defensores de redes.
  - Algunos registros que proporcionan los proveedores solo están disponibles para las organizaciones de los clientes con un costo adicional. Desafortunadamente, algunas actividades maliciosas solo pueden identificarse mediante registros “mejorados” (consulte el aviso conjunto sobre ciberseguridad [CSA, por sus siglas en inglés] Supervisión mejorada para detectar actividades de amenazas persistentes avanzadas [APT, por sus siglas en inglés] que atacan a Outlook en línea). Por lo tanto, es posible que las organizaciones que no pagan por el registro mejorado no puedan detectar determinadas actividades maliciosas. Nota: De conformidad con los principios de seguridad desde el diseño, la CISA insta encarecidamente a los fabricantes de software a que consideren el registro mejorado, más allá de los costos reales de procesamiento y almacenamiento, como una necesidad básica para la seguridad de la red, y a que lo incluyan en todos los niveles de servicio. De esta manera, todas las organizaciones, especialmente aquellas con menos recursos, pueden detectar las intrusiones y responder a estas. Consulte la sección “Seguridad desde el diseño” para obtener más información.
- Tienen amplias políticas de listas de permitidos para los rangos de direcciones de protocolos de Internet (IP, por sus siglas en inglés) que son propiedad de proveedores de alojamiento y de la nube.
  - Es importante tener en cuenta que estos rangos de IP son accesibles para cualquier organización que alquile espacio de IP al proveedor, incluso los agentes maliciosos. Identifique y priorice los rangos de IP esenciales para las operaciones organizacionales, aplique restricciones selectivas a los demás y revise y actualice periódicamente las listas de permitidos para obtener adaptabilidad y seguridad contra amenazas emergentes. Supervise los patrones de tráfico de la red para identificar desviaciones de la actividad normal.

Los defensores de redes deben garantizar que existan protecciones adecuadas para los dispositivos macOS, ya que, a menudo, se producen confusiones sobre la seguridad inherente de macOS.

- macOS carece de una orientación para reforzar el sistema que esté estandarizada y se promueva ampliamente, en comparación con otros sistemas operativos. Esta falta de énfasis en las prácticas de refuerzo puede generar que los sistemas macOS se implementen

con configuraciones predeterminadas, que pueden no estar optimizadas para la seguridad. Los profesionales cibernéticos a menudo pasan por alto la necesidad de contar con pautas de refuerzo integrales que aborden las prácticas recomendadas y las configuraciones de seguridad específicas de macOS. Para obtener orientación adicional, consulte la Orientación de seguridad de dispositivos del NCSC-UK y el Proyecto de Cumplimiento de Seguridad de macOS de GitHub.

- Existe la creencia predominante de que los dispositivos macOS son “seguros” debido a su diseño y sus funciones de seguridad integradas. Esta presunción puede producir que se subestimen los riesgos y las vulnerabilidades potenciales que se asocian con macOS. Como resultado, las medidas de seguridad que son estándar en otros entornos, como las evaluaciones de seguridad periódicas, los registros de alta fidelidad y las listas de aplicaciones permitidas, pueden perder prioridad o ignorarse en los entornos de macOS.
- En entornos de sistemas operativos mixtos, es común que los dispositivos Windows superen en número a los dispositivos macOS. Esta dinámica puede hacer que los administradores de sistemas den prioridad a Windows sobre macOS a la hora de buscar amenazas. Los equipos informáticos y de seguridad tienden a pasar por alto o prestar menos atención a macOS debido a su menor representación en algunos entornos, lo que potencialmente deja a estos sistemas más vulnerables a las intrusiones.

Estos factores a menudo contribuyen a un exceso de confianza al dedicar recursos adecuados para la administración de seguridad de los dispositivos macOS. Esto incluye asignar presupuesto y tiempo para implementar medidas de seguridad avanzadas, como los sistemas de EDR, e invertir en herramientas de seguridad específicas para macOS.

Sugerencias de prácticas recomendadas

La detección de técnicas LOTL requiere que las organizaciones realicen análisis contextuales de múltiples fuentes de datos para identificar ejecuciones de comandos, interacciones de archivos, elevaciones de privilegios y otras actividades de red que difieren de las acciones administrativas normales. La implementación de estas recomendaciones depende del panorama de riesgos y de las capacidades de recursos de cada organización. Sin embargo, establecer y mantener una infraestructura que recopile y organice datos para los defensores es esencial para detectar técnicas LOTL.

> Estas recomendaciones no son infalibles, pero son parte de un enfoque integral y multifacético para mitigar las amenazas cibernéticas con técnicas LOTL.
>
> Aunque se las clasifica por relevancia, las organizaciones deben implementar tantas como sea posible, ya que su efectividad radica en su implementación combinada, lo que permitirá la relación y el análisis de datos efectivos.

Las agencias autoras exhortan encarecidamente a los defensores de redes a implementar las siguientes recomendaciones *priorizadas de detección y refuerzo* para permitir el análisis de comportamientos, la detección de anomalías y la búsqueda proactiva.

Detección

1. **Implemente registros completos (es decir, de gran cobertura) y verbosos (es decir, detallados), y agrupe los registros** en una ubicación centralizada fuera de banda en la que los adversarios no puedan alterarlos para permitir el análisis de comportamientos, la detección de anomalías y la búsqueda proactiva. Además, la implementación de registros centralizados permite a los defensores mantener historiales de registro más largos.
    a. **Habilite el registro completo de todos los eventos relacionados con la seguridad**, lo que incluye las actividades de shells, las solicitudes de interacción del sistema y los registros de auditoría en todas las plataformas. Además, los defensores deben priorizar los registros y las fuentes de datos que tengan más probabilidades de detectar herramientas y actividades de las técnicas LOTL maliciosas. **Nota:** Las configuraciones de registro predeterminadas rara vez reflejan todos los eventos necesarios. Esto puede requerir la compra de capacidades de registro mejoradas, ya que algunas actividades maliciosas solo pueden identificarse mediante el registro mejorado. Como parte de la campaña Seguridad desde el Diseño (Secure by Design) de la CISA, esta agencia insta a los fabricantes de software a proporcionar registros de auditoría de alta calidad a los clientes sin costo adicional o a proporcionar registros que no requieran que los clientes realicen configuraciones adicionales. Consulte la sección "Seguridad desde el diseño" de esta guía para obtener más información. Si desea recomendaciones adicionales sobre la administración de registros, consulte NIST SP 800-92, rev. 1: Guía de planificación de la administración de registros de ciberseguridad.
        i. En el caso de los entornos en la nube, haga lo siguiente:
            1) Asegúrese de que el registro esté habilitado para todas las operaciones del plano de control, lo que incluye las solicitudes de interacción de la interfaz de programación de aplicaciones (API, por sus siglas en inglés) y los inicios de sesión

de usuarios finales, a través de ciertos servicios, como Amazon Web Services CloudTrail, Azure Activity Log y Google Cloud Audit Logs. Configure estos registros de modo que reflejen las actividades de lectura y escritura, los cambios administrativos y los registros de autenticación.

2) Configure las políticas de registro para todos los servicios de nube disponibles en el entorno de la organización, incluso si no se utilizan activamente. Los agentes de amenazas cibernéticas pueden aprovechar servicios o regiones no utilizados que no se supervisan activamente para evitar que los detecten.

b. **Habilite el registro verboso para los eventos relacionados con la seguridad,** como las líneas de comando, la actividad de PowerShell y el rastreo de eventos del Instrumental de administración de Windows (WMI, por sus siglas en inglés), a fin de obtener visibilidad del uso de herramientas dentro del entorno. Además, el sistema de EDR puede recopilar y centralizar registros.
   i. En el caso de los entornos de Microsoft, **habilite funciones del servidor de Microsoft específicas que tengan características de registro avanzadas opcionales**, como el registro avanzado de eventos de Microsoft Internet Information Services (IIS). Estas características favorecen la identificación de ciertos vectores de ataque y pueden ser necesarias para detectarlos. Por ejemplo, es posible que los web shells del módulo de IIS sean difíciles de detectar si no se habilitan estos registros. Para obtener más información, consulte el sitio de Microsoft Módulos de IIS: la evolución de los web shells y cómo detectarlos.
   ii. En el caso de las configuraciones específicas de la nube, **habilite el registro detallado para puertas de enlace de la red y equilibradores de carga a fin de monitorear el tráfico de entrada y salida**. Asimismo, configure las exportaciones de registros desde servicios de almacenamiento en la nube a una solución de administración de eventos e información de seguridad (SIEM, por sus siglas en inglés) o a un servidor de registro centralizado, como los eventos de datos de Amazon S3 CloudTrail (o registros de acceso de S3) o el registro de Azure Blob Storage, para supervisar los patrones de acceso a los datos.
   iii. En el caso de los sistemas macOS, **habilite los registros verbosos para los comandos de Terminal**, las actividades de AppleScript y el acceso a binarios clave, como `curl`, `osascript` y `launchctl`.

c. **Considere utilizar herramientas de administración de eventos e información de seguridad (SIEM)** para agrupar y administrar registros. Las herramientas de SIEM recopilan datos de registros de eventos de una variedad de fuentes, lo que facilita a los defensores de redes la capacidad de identificar actividades que se desvían de las referencias. La agrupación de registros es fundamental, porque se sabe que algunos agentes de amenazas cibernéticas borran o modifican los registros de eventos del sistema local. Además, la mayoría de los dispositivos de infraestructura de red disponibles en el mercado en la actualidad tienen capacidades de almacenamiento local tradicionalmente limitadas. La implementación de registros centralizados puede garantizar que los registros no se renueven tan rápido, lo que brinda a los defensores de redes un historial de registros que se puede mantener adecuadamente y que se puede relacionar entre eventos registrados desde múltiples sistemas.

   d. **Audite regularmente la integridad de los registros y la eficiencia de las alertas.** Verifique de forma rutinaria que los eventos se registren correctamente, se transmitan de forma segura a un repositorio centralizado y activen alertas de manera confiable. Esto es fundamental, ya que las actualizaciones de software y firmware, los ajustes de configuración o las alteraciones del sistema pueden afectar el registro y reenvío de eventos. Esto puede socavar la precisión de los registros y la eficacia de las alertas.
2. **Establezca y mantenga de forma continua una referencia de las herramientas y los softwares instalados**, el comportamiento de la cuenta y el tráfico de la red. De esta manera, los defensores de redes pueden identificar posibles valores atípicos, que pueden indicar actividad maliciosa.
   a. Aproveche **las soluciones de SIEM y los registros globales** para crear referencias del comportamiento de la cuenta, de las herramientas usadas con frecuencia, las mallas de servicios, el tráfico de la red, las intercomunicaciones del sistema y otros elementos, según corresponda.
   b. **Mejore la supervisión de la red, la retención de registros y la búsqueda de amenazas para identificar la presencia prolongada de adversarios.** Ampliar el almacenamiento de registros, ajustar la detección de anomalías y profundizar las tácticas de búsqueda de amenazas puede ayudar a descubrir agentes de amenazas que aprovechan las técnicas LOTL durante períodos de permanencia inmediatos y prolongados.
   c. **Seleccione un subconjunto mínimo de herramientas administrativas para usar en la red**, configúrelas con registros extensos y bloquee todas las demás o emita alertas sobre ellas. Aplique las restricciones correspondientes a los inicios de sesión de la red. Esto reduce el ruido del entorno que los defensores deben analizar y proporciona más detalles del comportamiento observado.
   d. **Cree referencias claras del comportamiento de las cuentas privilegiadas.** Establezca qué herramientas suelen utilizar los administradores, los comandos que ejecutan, sus períodos de actividad y los dispositivos específicos con los que interactúan. Modifique las políticas de inicio de sesión de la red para limitar las rutas de acceso innecesarias en función de este perfil bien definido de actividad legítima. Las referencias del comportamiento también deben incluir la secuencia de uso. Por ejemplo, suele haber una serie predeterminada de aplicaciones que se ejecutan cuando un usuario inicia sesión. Sin embargo, en otros momentos del día, la secuencia de aplicaciones puede indicar actividad sospechosa según la referencia, especialmente si las aplicaciones solicitan interacción con otras aplicaciones.
      i. **Utilice estaciones de trabajo de acceso privilegiado (PAW, por sus siglas en inglés)** para cuentas administrativas y exija su uso para funciones administrativas. En entornos de Windows, como mínimo, utilice primero las PAW para los administradores de Active Directory (AD). Para obtener más información, consulte el sitio de Microsoft Asegurar el dispositivo como parte de la historia de acceso privilegiado.
   e. **Defina claramente el comportamiento de las herramientas y los sistemas automatizados** (p. ej., aplicaciones y servicios que utilizan cuentas de servicio y escáneres de red). El uso debería limitarse de forma previsible en función de la hora del día, los hosts de origen y destino, y las cuentas de usuario que pueden verse afectadas por un servicio automatizado. Estas cuentas son el objetivo de los agentes de amenazas porque, con

frecuencia, tienen privilegios adicionales innecesarios y no utilizan la autenticación de múltiples factores (MFA).

f. **Cree un inventario de configuraciones, políticas y softwares instalados establecidos** en cada host. Si el host no requiere un software específico, desinstálelo a fin de limitar las herramientas disponibles para los agentes de amenazas cibernéticas. Las herramientas de EDR son especialmente adecuadas para esta función.

g. **Realice un escrutinio adicional a los hosts en riesgo**, como los servidores públicos en una zona desmilitarizada (DMZ, por sus siglas en inglés). Los agentes de amenazas cibernéticas que obtienen un punto de apoyo inicial mediante la explotación de servicios conectados a Internet, con frecuencia, dependen de los LOLBins para la ejecución inicial, el reconocimiento y la implementación de cargas útiles secundarias.

h. **Monitoree y registre qué infraestructura se ha inspeccionado**, verifique si hay problemas sin resolver y registre de forma continua qué se considera de alto riesgo para priorizar los esfuerzos de manera proactiva.

i. **Establezca una referencia para los LOLBins y supervise los cambios.** Comprenda de qué LOLBins los atacantes están haciendo mal uso y entienda los detalles del uso normal de esos binarios en el entorno. Por ejemplo, se puede utilizar un LOLBin particular, pero siempre con una línea de comando o un usuario específicos. Evalúe si se pueden crear alertas si esos LOLBins se utilizan fuera de la referencia e investigue las ejecuciones observadas.

j. En el caso de los entornos en la nube, haga lo siguiente:

   i. **Diseñe entornos en la nube para garantizar la separación adecuada de los enclaves** utilizando herramientas de grupos de seguridad o subred. Esto puede habilitar registros adicionales dentro del entorno y proporcionar más información. Asegúrese de que se creen copias de seguridad del entorno para incluir la infraestructura como código. Esto se puede utilizar para comparar cambios en el entorno.

3. **Utilice la automatización para revisar continuamente todos los registros y aumentar la eficiencia de las actividades de búsqueda.** Compare las actividades actuales con las referencias de comportamiento establecidas y preste especial atención a las cuentas privilegiadas y a los activos fundamentales, como los controladores de dominio. A medida que se identifiquen nuevas estrategias de búsqueda, aproveche la automatización y asegúrese de que el personal haya recibido la capacitación adecuada sobre su uso.

   a. En entornos de Linux, **realice auditorías periódicas de los `cron jobs` y los temporizadores `systemd` para detectar entradas imprevistas**. Si implementa supervisiones de la integridad de los archivos en archivos de configuración fundamentales, como archivos de unidad `/etc/crontab`, `/etc/cron.*/*` y `systemd`, eso puede alertar a los defensores sobre las modificaciones no autorizadas. Busque entradas imprevistas o desconocidas, especialmente aquellas que invocan scripts o binarios que no forman parte de las tareas estándar de mantenimiento del sistema.

   b. Para macOS, **realice comprobaciones de rutina de los archivos de lista de propiedades (PLIST, por sus siglas en inglés) y las tareas programadas de macOS** (use `launchd`). Busque entradas no autorizadas o modificadas que puedan indicar mecanismos de persistencia.

   c. Para Windows, realice auditorías periódicas del registro de Windows en busca de cambios en las ubicaciones de inicio automático, como las claves `Run` y `RunOnce`, y otras

áreas que se utilizan a menudo para la persistencia. Implemente la supervisión de la integridad de los archivos en estas claves. Además, cree detecciones para tareas programadas que se ejecutan en momentos inusuales, ejecutan scripts o binarios poco comunes, o que se han modificado recientemente sin autorización.

d. En los entornos en la nube, **supervise las solicitudes de interacción de la API inusuales**, especialmente aquellas que involucren cambios en los grupos de seguridad, la configuración de los recursos de la nube o el acceso a datos confidenciales. Esto se puede hacer utilizando herramientas nativas de la nube.
    i. **Investigue cualquier comportamiento inusual de la cuenta**, como inicios de sesión fuera de horario, inicios de sesión simultáneos desde ubicaciones geográficamente dispares y enumeraciones de redes internas.

e. **Considere aprovechar las capacidades de detección de anomalías con base en el aprendizaje automático** dentro de los servicios de seguridad del proveedor de la nube para mejorar el análisis de registros. Estos servicios procesan datos de registro de múltiples fuentes en tiempo real más allá del alcance de los métodos tradicionales y emplean el aprendizaje automático para detectar patrones anómalos y comportamientos que indican actividad maliciosa. Concéntrese en los patrones irregulares de solicitudes de interacción de la API, el acceso inusual al almacenamiento en la nube y el tráfico de red atípico.

4. **Reduzca el ruido de las alertas.** Perfeccione las herramientas de supervisión y los mecanismos de alerta para diferenciar entre acciones administrativas típicas y comportamientos de amenazas potenciales. Además, relacione las actividades de autenticación remota para identificar anomalías y valores atípicos, y, de este modo, poder centrarse en las alertas que probablemente indiquen actividades sospechosas.
    a. **Evite las reglas de detección demasiado amplias,** como `CommandLine=*` o `Filepath=C:\...\*`. Esto se aplica a las reglas de inclusión y exclusión.
    b. **Coordine con los equipos de IT para reducir la prevalencia de herramientas administrativas permitidas y tipos de inicio de sesión disponibles en la red**. Considere el host, el propósito previsto y el usuario asociado con la actividad. Por ejemplo, un usuario empresarial típico nunca abrirá un símbolo del sistema ni ejecutará ipconfig. Un servidor backend administrado a través de un shell seguro (SSH, por sus siglas en inglés) o una interfaz de protocolo de transferencia de hipertexto seguro (HTTPS, por sus siglas en inglés) no debería necesitar que el protocolo de escritorio remoto (RDP, por sus siglas en inglés) esté habilitado. Las cuentas de usuario con privilegios de administrador de dominio solo deben iniciar sesión en los controladores de dominio.
    c. Deshabilite la instalación y el uso de las herramientas de acceso remoto que su organización no requiera y emita alertas al respecto.
    d. **Considere implementar un modelo de madurez de detección de amenazas** para desarrollar, implementar, probar y ajustar los mecanismos de alerta habilitados dentro de la red y de los sistemas de detección de intrusiones del host o de la solución de SIEM. Considere implementar una convención de denominación estandarizada para las alertas, que incluya el nivel de madurez de la alerta y la fase de MITRE ATT&CK, con el fin de permitir una clasificación de respuestas a incidentes más rápida. A medida que se ajustan las alertas, se debe actualizar su madurez para reflejar la estabilidad de la regla, lo que genera, en definitiva, detecciones sólidas y confiables.

5. **Aproveche los análisis del comportamiento de usuarios y entidades (UEBA)** para analizar y relacionar actividades en múltiples fuentes de datos, identificar posibles incidentes de seguridad que las herramientas tradicionales pueden pasar por alto y perfilar y supervisar el comportamiento de los usuarios mediante la detección de amenazas internas o cuentas puestas en riesgo.

Refuerzo

1. Aplique la orientación para el refuerzo.
   a. **Fortalezca las configuraciones del software y del sistema** en función de la orientación para el refuerzo que proporcionó el proveedor o de la industria, el sector o el gobierno (p. ej., el Instituto Nacional de Estándares y Tecnología de EE. UU. [NIST, por sus siglas en inglés]) a fin de reducir la superficie de ataque. No confíe en configuraciones predeterminadas de software y dispositivos que puedan ser inseguras. Nota: Como parte de la campaña Seguridad desde el Diseño de la CISA, la agencia insta a los fabricantes de software a priorizar las configuraciones seguras por defecto para eliminar la necesidad de que el cliente implemente las pautas de refuerzo. Consulte la sección "Seguridad desde el diseño" de esta guía para obtener más información.
      i. En el caso de Windows**, aplique las actualizaciones y correcciones de seguridad que proporciona Microsoft**. Para obtener pautas completas de refuerzo, siga la Guía de referencias de seguridad de Windows elaborada por Microsoft o los Puntos de referencia del Center for Internet Security (CIS). Refuerce los servicios que con frecuencia son objetivo de explotación, como el bloque de mensajes del servidor (SMB, por sus siglas en inglés) y el RDP, y deshabilite cualquier servicio o característica superfluos.
      ii. En sistemas Linux, **compruebe qué permisos binarios están configurados**. Consulte los Puntos de referencia para Red Hat Enterprise Linux del CIS.
      iii. En el caso de macOS, **actualice periódicamente el sistema a la última versión y aplique todas las correcciones de seguridad**. Utilice las características integradas de seguridad de macOS, como Gatekeeper, XProtect y FileVault. Siga las pautas que establece el Proyecto de Cumplimiento de Seguridad de macOS de GitHub. Implemente listas de aplicaciones permitidas y aproveche el cortafuegos integrado para controlar el acceso a la red.
      iv. Las organizaciones con infraestructura en la nube de Microsoft deben consultar las guías de referencia de configuración de seguridad de Microsoft 365 que elaboró la CISA, las cuales proporcionan referencias mínimas y viables de configuración segura para Microsoft Defender para Office 365, Azure Active Directory, Exchange Online, OneDrive para la Empresa, Power BI, Power Platform, SharePoint Online y Teams. Para obtener orientación adicional, consulte el Plan para una Nube Segura de la Dirección de Señales de Australia.
      v. Las organizaciones con infraestructura en la nube de Google deben consultar las guías de referencia de configuración de seguridad de Google Workspace que elaboró la CISA, las cuales proporcionan referencias mínimas y viables de configuración segura para Groups for Business, Gmail, Google Calendar, Google Chat, Google Common Controls, Google Classroom, Google Drive y Docs, Google Meet y Google Sites.

   b. **Adopte medidas de** refuerzo **que sean de aplicación universal**, como minimizar los servicios en ejecución, aplicar principios de privilegio mínimo y asegurar las comunicaciones de la red. Para obtener recomendaciones adicionales, consulte los Objetivos de Desempeño de Ciberseguridad Intersectoriales de la CISA.
   c. **Asegure los activos fundamentales** aplicando medidas de refuerzo de los proveedores. Por ejemplo, en el caso de los activos fundamentales o el nivel 0 de Microsoft, como los Servicios de federación de Active Directory (ADFS, por sus siglas en inglés) y los Servicios de certificados de Active Directory (ADCS, por sus siglas en inglés), aplique la orientación que figura en la documentación de seguridad: Modelo de acceso empresarial de Microsoft. Los activos fundamentales incluyen los componentes de infraestructura multiplataforma, como proveedores de identidad, servicios de directorio, administración de dispositivos móviles (MDM, por sus siglas en inglés) y consolas de administración de la nube. Asegurar estos activos significa no solo reforzar sus configuraciones, sino también limitar las aplicaciones y los servicios que pueden utilizar o a los que pueden acceder. Esto reducirá su exposición e impondrá restricciones estrictas a todas las cuentas que tengan acceso administrativo a los activos.
   d. **Utilice herramientas administrativas que no almacenen las credenciales en el host remoto.** Si un agente de amenazas pone en riesgo un host con credenciales almacenadas, a menudo puede encontrar y reutilizar esas credenciales para obtener acceso a otros hosts y servicios.
2. **Implemente listas de aplicaciones permitidas** para restringir el entorno de ejecución y configure listas de permitidos para funciones empresariales. Esta estrategia canaliza toda la actividad administrativa y de los usuarios a través de una vía estrecha que es más fácil de supervisar, lo cual mejora la efectividad de los análisis del comportamiento y reduce el volumen de las alertas a aquellas que son más pertinentes. Para obtener recomendaciones adicionales, consulte el sitio Enfoques técnicos para descubrir y corregir actividad maliciosa de la CISA.
   a. En el caso de macOS, configure los ajustes de Gatekeeper para evitar la ejecución de aplicaciones sin firma o no autorizadas y supervise los intentos de eludir estos ajustes.
   b. En el caso de Windows, **utilice AppLocker y el Control de aplicaciones de Windows Defender para obtener una lista sólida de aplicaciones permitidas**. Estos mecanismos facilitan una regulación estricta de archivos ejecutables, scripts, archivos MSI, bibliotecas de vínculo dinámico (DLL, por sus siglas en inglés) y formatos de paquetes de aplicaciones. Los administradores pueden aplicar las políticas de seguridad elaborando reglas centradas en atributos del archivo, como nombre, versión, editor y ruta.
3. **Mejore la segmentación y la supervisión de la red** para limitar las posibilidades de movimiento lateral de los agentes de amenazas. El comportamiento anormal de la red puede indicar la presencia de un agente de amenazas que evadió las detecciones basadas en el host, posiblemente mediante técnicas LOTL. La implementación y administración adecuada de la segmentación de la red garantiza que los usuarios solo tengan acceso a la cantidad mínima de aplicaciones y servicios que se requieren para realizar sus tareas diarias. Cuando un agente de amenazas cibernéticas pone en riesgo credenciales legítimas, tener una segmentación de la red adecuada limita el “radio de explosión” de los sistemas accesibles.

a. **Utilice herramientas de análisis de tráfico de la red para supervisar el tráfico entre segmentos** y céntrese en patrones inusuales o comunicaciones con segmentos confidenciales.
b. **Coloque estratégicamente sensores de red y analizadores de tráfico de la red** en puntos fundamentales de la infraestructura de la red, como intersecciones entre diferentes segmentos de la red, redes privadas virtuales (VPN, por sus siglas en inglés) y puertas de enlace externas, y zonas desmilitarizadas (DMZ). Asegúrese de que estos sensores tengan capacidades de inspección profunda de paquetes para facilitar un análisis integral del tráfico.
c. **Utilice analizadores de metadatos del tráfico de la red** (p. ej., Zeek [anteriormente denominado Bro]) para lograr un análisis eficiente del tráfico de la red, lo que permite la identificación de patrones sospechosos y anomalías que indican actividades de las técnicas LOTL. Además, considere integrar sistemas de detección de intrusiones en la red (NIDS, por sus siglas en inglés) de código abierto (p. ej., Snort, Suricata) para mejorar la detección de amenazas de técnicas LOTL.
   Nota: Como estrategia a largo plazo, las agencias autoras recomiendan encarecidamente que las organizaciones implementen arquitecturas de confianza cero para garantizar que los binarios y las cuentas que los utilizan no se consideren confiables de forma automática. Además, su uso debe restringirse y examinarse a fin de confirmar un comportamiento confiable. Para obtener más información, consulte el Modelo de madurez de confianza cero de la CISA.

4. Implemente controles de autenticación:
   a. Aplique la autenticación de múltiples factores (MFA) resistente a la suplantación de identidad en todos los sistemas, especialmente para las cuentas privilegiadas.
   b. **Implemente una solución sólida de administración de acceso privilegiado (PAM, por sus siglas en inglés)** con acceso justo a tiempo mediante la restricción del acceso elevado a las necesidades y los períodos específicos. Utilice controles de PAM basados en el tiempo, lo que incluye el acceso según el día y la hora del día, y compleméntelos con un control de acceso basado en funciones (RBAC, por sus siglas en inglés) para lograr un acceso personalizado de acuerdo con los requisitos del trabajo. Esto garantiza que el acceso elevado se otorgue solo cuando sea necesario y por un tiempo limitado, lo que minimiza la oportunidad para el mal uso o la explotación de credenciales privilegiadas.
   c. En el caso de los entornos en la nube, **aplique políticas estrictas de administración de identidad y acceso a credenciales (ICAM, por sus siglas en inglés)**, lo que garantiza privilegios mínimos para cada usuario y cuenta de servicio. Realice auditorías periódicas de las configuraciones de ICAM para detectar funciones demasiado permisivas y corríjalas. Además, considere crear identificaciones de RBAC con identificaciones maestras de la nube asociadas y almacenarlas de forma segura fuera de Internet. Asegúrese de que las claves de acceso se alternen o tengan fechas de vencimiento.
   d. En el caso de macOS y Unix, **revise con frecuencia el archivo `sudoers` para detectar errores de configuración** que puedan permitir una elevación de privilegios. Asegúrese de que se adhiera al principio de privilegio mínimo.

Además, las agencias autoras recomiendan que, a fin de posicionarse mejor para mitigar las técnicas LOTL, los defensores de redes apliquen lo siguiente:

- **Ejerza la diligencia debida** al seleccionar software, dispositivos, proveedores de servicios en la nube y proveedores de servicios administrados. Seleccione proveedores que cuenten con principios de seguridad desde el diseño para reducir la disponibilidad de LOLBins que los agentes de amenazas pueden aprovechar.
  - Haga que los proveedores sean responsables de las configuraciones y los requisitos predeterminados de su software. Tenga cuidado con los productos que infrinjan el principio de privilegio mínimo, no indiquen con claridad el acceso necesario (p. ej., reglas de cortafuegos demasiado amplias, en lugar de puertos específicos del protocolo de control de transmisión [TCP, por sus siglas en inglés]) o requieran deshabilitar las herramientas antivirus.
  - Siga las prácticas recomendadas para la administración de riesgos de la cadena de suministro y solo obtenga los productos de proveedores acreditados.
- **Realice auditorías del software de acceso remoto y sus configuraciones** en dispositivos de su red para identificar los softwares de acceso remoto autorizados o utilizados actualmente.
  - Considere reducir los softwares de acceso remoto en los sistemas eligiendo una solución y una solución de respaldo. Esto ayudará a los defensores de redes a identificar posibles actividades anómalas, por ejemplo, si hay actividad de soluciones de acceso remoto no aprobadas.
  - Aplique las prácticas recomendadas para softwares de acceso remoto del documento conjunto Guía para asegurar el software de acceso remoto.
- **Limite la exposición de las configuraciones defensivas.** Los agentes maliciosos pueden leer configuraciones defensivas y ajustar su estrategia si la información está disponible. Por ejemplo, las reglas de Sysmon (lo que se registra o no) están disponibles por defecto en una clave de registro legible globalmente, y se pueden analizar con Sysmon.exe.
  - Realice una auditoría de los intentos de leer la configuración, deshabilitar el software de supervisión o alterar los artefactos de registro.
- Restrinja la conectividad a Internet saliente.
  - Los servidores back-end (especialmente las bases de datos, los controladores de dominio, etc.) no necesitan acceso a Internet. Si se restringe, por defecto, se evitan muchas cargas útiles iniciales, especialmente aquellas utilizadas en las puestas en riesgo de la cadena de suministro.
    - En el caso de los servidores o las aplicaciones que requieran salida a Internet, restrinja y supervise la conectividad saliente para que solo se produzca hacia destinos de salida esenciales.
  - Muchos servicios esenciales, como el de EDR, ahora están conectados a la nube. Garantice que los servicios tengan lo necesario, pero no conceda un acceso demasiado amplio (p. ej., permitir ciertos dominios/IP necesarios para los servicios en lugar de incluir en la lista de permitidos a todo el proveedor de servicios).
  - Busque conexiones sin procesar a direcciones IP que no tengan las correspondientes solicitudes de sistema de nombres de dominio (DNS, por sus siglas en inglés).

Recomendaciones de detección y búsqueda

General

Las agencias autoras recomiendan encarecidamente que los defensores de redes revisen y comparen periódicamente el comportamiento de las herramientas y los sistemas automatizados, las configuraciones y los softwares instalados en hosts, registros y otros elementos de su referencia para identificar posibles actividades maliciosas. Estas recomendaciones no son infalibles, sino que son pautas sobre las maneras de utilizar los registros como parte de un enfoque multifacético.

Registros de eventos de aplicaciones, seguridad y sistemas

Revise los registros de eventos de aplicaciones, seguridad y sistemas; para ello, céntrese en los registros de aplicaciones de la tecnología de motor de almacenamiento extensible (ESENT, por sus siglas en inglés) de Windows. Ciertas identificaciones de eventos del registro de aplicaciones de la ESENT (`216`, `325`, `326` y `327`) pueden indicar que los agentes copian `NTDS.dit`. Consulte el aviso conjunto Agentes patrocinados por el Estado de la PRC ponen en riesgo la infraestructura fundamental de EE. UU. y mantienen un acceso persistente a esta para obtener más información, incluidos ejemplos de ESENT y otros indicadores de registros clave que deben investigarse.

Registros de red

Los artefactos de la red para técnicas LOTL son mucho más difíciles de detectar y reflejar que los artefactos del host. Los defensores de redes pueden encontrar artefactos del host, a menos que el agente de amenazas los elimine, sin realizar cambios en la configuración del sistema. Sin embargo, los artefactos de la red requieren que los defensores de redes configuren y establezcan registros de manera adecuada para su detección. Además, los artefactos de la red para actividad de las técnicas LOTL son en gran medida transitorios, ya que derivan del tráfico de la red. Si no se implementan sensores para reflejar el tráfico, entonces no habrá forma de ver la actividad de las técnicas LOTL desde una perspectiva de red.

Rara vez hay un solo indicador de actividad de las técnicas LOTL, lo que presenta uno de los muchos desafíos que se encuentran al intentar detectar esta actividad a medida que ocurre. Más bien, se trata de una colección de posibles indicadores que ofrece una imagen más amplia del comportamiento del tráfico de la red.

Algunas formas de descubrir posible actividad de las técnicas LOTL y sus indicadores son las siguientes:

- Revise los intentos de acceso bloqueado en los registros del cortafuegos. En una red correctamente segmentada, el tráfico denegado (no permitido) puede ser un indicador de riesgo. Los intentos de descubrimiento y asignación de la red (especialmente desde el interior de la red que se originan en uno o más hosts) también pueden ser un indicador. Se debe tener cuidado para garantizar que este no sea un comportamiento normal asociado con muchas herramientas de administración de red diferentes. En lugar de definir umbrales de comportamiento, se debe investigar cualquier tráfico anormal, como el siguiente.
    - Solicitudes del protocolo ligero de acceso a directorios (LDAP, por sus siglas en inglés) a un DC desde hosts Linux unidos que no pertenecen al dominio en enclaves separados.

  - Solicitudes SMB en distintos sitios geográficos o segmentos de la red lógica, como un usuario que accede a servidores de archivos no relacionados con su función laboral.
  - Solicitudes de acceso a la base de datos desde una estación de trabajo del usuario a un servidor backend de base de datos. Únicamente el servidor frontend debe comunicarse con el servidor de base de datos.

Si las aplicaciones legítimas realizan esas solicitudes, considere tenerlo en cuenta en sus niveles de ruido de referencia.

- Además de los registros de dispositivos de red dedicados, examine los registros de ciertos servicios, como Sysmon, IIS y otros servicios de red en equipos host. Estos registros pueden proporcionar información sobre las interacciones del servidor web, las transacciones del protocolo de transferencia de archivos (FTP, por sus siglas en inglés) y otras actividades de la red que administra el host. Alinear estos datos con los registros del dispositivo de red puede revelar discrepancias o anomalías que indican un comportamiento malicioso de la red, como intentos inusuales de acceso externo o actividades de exfiltración de datos. Es importante recordar que los registros centrados en la red de los equipos host pueden ofrecer contexto y detalles valiosos que los dispositivos de red tradicionales no reflejan.
- Combine registros de tráfico de la red con registros basados en el host para incluir información adicional, como procesos y cuentas de usuario. Compare el destino con artefactos en la red, ya que la información que no coincide podría indicar tráfico malicioso. Por ejemplo:
  - Tráfico por el puerto `88`. Pocos procesos (como `lsass.exe`) deben comunicarse con Kerberos a través del puerto `88`.
  - Tráfico de acceso remoto, como el servicio de actualización de la supervisión y administración remotas (RMM, por sus siglas en inglés), que se dirige a un sitio no relacionado pero que parece legítimo.

Registros de autenticación

- **Adopte una estrategia sólida para la separación de privilegios**, que es fundamental para identificar técnicas LOTL a través de registros de autenticación. Restrinja las cuentas de administrador de dominio para que solo puedan iniciar sesión en controladores de dominio y, de esta manera, minimizar la exposición de las credenciales y el peligro de puesta en riesgo. En el caso de otras funciones administrativas, utilice PAW junto con hosts bastiones como puntos de salto controlados y predecibles para aplicar procedimientos de inicio de sesión estandarizados. Estos hosts bastiones, en conjunto con las PAW, son especialmente fundamentales en los entornos de sistemas de control industrial (ICS, por sus siglas en inglés). Actúan como puertas de enlace seguras y supervisadas que refuerzan la segmentación de la red, debido a que permiten el acceso a dispositivos fundamentales únicamente desde zonas de red designadas. Implemente la autenticación de múltiples factores como una capa adicional de protección.
- **Compare la actividad con el comportamiento normal del usuario**. Los comportamientos inusuales incluyen los horarios extraños de inicio de sesión, el acceso que entra en conflicto con los cronogramas de trabajo esperados o las vacaciones planificadas, la sucesión rápida o un gran volumen de intentos de acceso seguidos de un inicio de sesión exitoso, las rutas

de acceso inusuales, los inicios de sesión simultáneos desde varias ubicaciones geográficas y los casos de viajes en el tiempo imposibles.

Registros de Sysmon o basados en el host

- Utilice referencias establecidas de herramientas y actividades en ejecución para identificar comportamientos anormales o potencialmente maliciosos.
- Utilice registros privilegiados (más seguros) que tienen menos probabilidades de que un adversario los altere durante la explotación inicial. Por ejemplo, los usuarios sin privilegios pueden modificar los archivos `.bash_history` de Linux, pero los registros `auditd` a nivel del sistema serían inaccesibles.
- En entornos de Windows, los registros de Sysmon brindan visibilidad de las actividades del sistema y ofrecen un registro detallado de la creación de procesos, las conexiones de red, las modificaciones del registro, los hashes criptográficos y más. Esta información detallada permite a los equipos de seguridad buscar y detectar el uso malicioso de utilidades del sistema y herramientas legítimas. Para obtener más información, consulte la Orientación de configuración de Sysmon elaborada por Microsoft.
- Para la mayoría de las utilidades de Microsoft, use `OriginalFileName` a fin de identificar los archivos a los que se les cambió el nombre (por ejemplo, de `net.exe` a `net2.exe`), lo cual puede indicar actividad maliciosa (en el caso de la mayoría de las utilidades, los nombres de archivo originales se encuentran en el encabezado del archivo portable ejecutable [PE] con el nombre del archivo en el disco).
- Implemente técnicas de detección en entornos de Windows para identificar el uso malicioso de utilidades de líneas de comandos y scripting, en particular aquellas que aprovechan flujos de datos alternativos (ADS, por sus siglas en inglés). Configure Sysmon para registrar la actividad de la línea de comandos y céntrese en detectar comandos que indiquen explotación de ADS. Esto involucra la supervisión de sintaxis o argumentos de la línea de comandos específicos que se utilizan para interactuar con los ADS, como el uso de operadores `>` o `:` en scripts de PowerShell o `cmd.exe`. Por ejemplo, busque ciertos patrones, como `type file.txt > file.txt:hidden.exe` o `-command “&{Get-Content file.txt -Stream hidden}”` de PowerShell. Estos patrones indican intentos de ejecutar cargas útiles ocultas en los flujos del sistema de archivos de nueva tecnología (NTFS, por sus siglas en inglés) o de interactuar con estas.
- Desarrolle estrategias de detección específicas para técnicas de alta ofuscación en interfaces de línea de comandos (CLI, por sus siglas en inglés) y utilidades de scripting, como `cmd.exe`, en entornos de Windows. Mejore las configuraciones de Sysmon para registrar y examinar las ejecuciones de la línea de comandos, y preste especial atención a los patrones que indican ofuscación. Esto incluye detectar el amplio uso de caracteres de escape, la concatenación de comandos, el uso excesivo de variables del entorno o el empleo de la codificación Base64. Por ejemplo, supervise las ejecuciones de `cmd.exe` que contengan secuencias inusuales, como `^`, `%%` o `&`, o comandos de PowerShell codificados en Base64, como en `powershell.exe -EncodedCommand [Base64String]`. Los agentes de amenazas cibernéticas suelen utilizar estos métodos de ofuscación para eludir las herramientas de supervisión de seguridad y ejecutar cargas útiles maliciosas sin que los

detecten. Integre estos registros de Sysmon con análisis en sistemas de SIEM para automatizar el proceso de detección.

- Supervise las cadenas de procesos sospechosos, como documentos de Microsoft Office que inician procesos de scripting. Céntrese en monitorear las creaciones de procesos, especialmente cuando las aplicaciones de Office, como Word o Excel, generan comandos `cmd.exe`, `wscript.exe` o `cscript.exe`, o de PowerShell. Esta es una señal de alerta, ya que es poco común que estas aplicaciones inicien dichos procesos de scripting. Además, preste atención a estos procesos si comienzan a ejecutar comandos inusuales (p. ej., whoami, net y query, que son atípicos para las operaciones habituales de Office). Es posible que la ejecución aislada de estos comandos no indique una alerta, pero su inicio desde una aplicación de Office es anómalo y merece una investigación. Establezca referencias para las actividades normales de procesos primarios-secundarios a fin de detectar las desviaciones de forma efectiva. La integración de registros de Sysmon con sistemas de SIEM y la aplicación de reglas de relación ayudan a identificar escenarios de ataques avanzados que involucran aplicaciones de Office como conductos para la explotación y el reconocimiento basados en scripts.
- Compare la cuenta de usuario y el comportamiento normal. Por lo general, los usuarios normales (no técnicos) nunca abrirán un símbolo del sistema ni ejecutarán el comando ipconfig. En cambio, una cuenta de usuario puesta en riesgo podría hacerlo.
- En máquinas Linux, habilite `Auditd` o Sysmon para el registro de Linux y envíe los registros a una plataforma de SIEM; esto puede mejorar, en gran medida, la capacidad de una organización para identificar actividades anómalas. El registro `Auditd` se puede personalizar fácilmente, lo que brinda a las organizaciones la capacidad de supervisar comandos específicos, la sintaxis de comandos o los cambios en archivos o directorios. Configurar alertas para cambios no aprobados o comandos poco comunes ayuda a identificar actividades potencialmente maliciosas. Preste especial atención a los árboles de procesos inesperados, por ejemplo, un editor de texto, como Vim o Gedit, que inicia herramientas de red, como `curl` o SSH. Utilice herramientas, como SELinux o AppArmor, para la ejecución y la supervisión adicional del comportamiento estándar de las aplicaciones.
- En el caso de macOS, utilice determinadas herramientas, como Santa, un sistema de autorización binaria de código abierto, para supervisar las ejecuciones de procesos. Céntrese en detectar la generación anormal de procesos por parte de aplicaciones que suelen utilizarse para la productividad, como Pages o Numbers, que podrían iniciar utilidades de scripting, como bash, zsh o Python. Supervise las ejecuciones de comandos de shells o scripts poco comunes por parte de estas aplicaciones, ya que este comportamiento es inusual en las operaciones estándar.

Revisión de las configuraciones

- Revise las configuraciones de host establecidas comparándolas con una referencia conocida de software instalado y comportamientos esperados. Esto puede detectar IOC que quizás no se reviertan mediante actualizaciones periódicas de la política de grupo, como el software instalado, los cambios en el cortafuegos o las actualizaciones de archivos principales (p. ej., archivo Hosts que ayuda con la resolución de DNS).

  - Los agentes de amenazas cibernéticas pueden eludir los registros de eventos estándar para registrar servicios y tareas programadas simplemente escribiendo en el registro, ya que esto no crea eventos estándar del sistema. Consulte Alteración de tareas programadas | WithSecure™ Labs para obtener más información.
- Las auditorías periódicas del inventario del sistema pueden detectar el comportamiento del adversario que los registros de eventos omitieron, ya sea porque se reflejaron eventos incorrectos o porque la actividad ocurrió antes de que se implementaran los cambios en el registro.

Ejemplos de detección personalizados

Comprender el contexto de las actividades de las técnicas LOTL es fundamental para lograr una respuesta y detección precisa, por lo que esta sección incluye orientación personalizada sobre la detección a partir de ejemplos del mundo real, específicamente `ntdsutil.exe` y `psexec.exe`, que, con frecuencia, son empleados por agentes de amenazas persistentes avanzadas (APT) patrocinados por el Estado en entornos puestos en riesgo. Las agencias autoras recomiendan encarecidamente que los defensores de redes apliquen la siguiente orientación para detectar el uso potencial de estos LOLBins.

NTDSUtil.exe

Dada la capacidad de `ntdsutil.exe` para crear instantáneas de la base de datos de Active Directory, `ntdsutil.exe` es un objetivo prioritario en las tácticas LOTL debido al acceso que proporciona a datos confidenciales del usuario y configuraciones del sistema.

Entre las tácticas, las técnicas y los procedimientos (TTP, por sus siglas en inglés) distintivos que emplea un grupo de APT patrocinado por el Estado, se incluye la creación de una instantánea de volumen, seguida del volcado del archivo `ntds.dit`, que involucra los comandos `vssadmin.exe` y `ntdsutil.exe`. Los agentes inician el proceso con la creación de una instantánea de volumen de la unidad del sistema mediante un comando, como `vssadmin.exe Create Shadow /for=C:`. Este paso establece una instantánea del estado del sistema, incluida la base de datos de Active Directory. Posteriormente, se emplea `ntdsutil.exe` con la secuencia de comandos `ntdsutil snapshot “activate instance ntds” create quit quit` para interactuar con esta instantánea. Luego, los agentes acceden a la instantánea para extraer el archivo `ntds.dit` del directorio `\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy[X]\Windows\NTDS`. Esta secuencia organizada se diseñó para extraer credenciales confidenciales, como contraseñas con hash, de Active Directory, lo que pone en riesgo a todo el dominio. La ejecución exitosa de esta técnica proporciona a los agentes de APT privilegios elevados, facilita el movimiento lateral a través de la red y permite su acceso persistente a sistemas y datos fundamentales.

Tomando el ejemplo específico del comando `ntdsutil snapshot “activate instance ntds” create quit quit`, que crea una instantánea de la base de datos de Active Directory, se pueden aprovechar múltiples fuentes de registro para crear un contexto completo en torno a esta actividad. Además, los defensores de redes deben considerar que muchos comandos se pueden acortar, y la detección debe tener en cuenta esto. Por ejemplo, el comando `ntdsutil snapshot “ac i ntds” create quit quit` también funciona. Este enfoque es vital para distinguir entre el uso

administrativo legítimo y la posible explotación maliciosa. Los siguientes registros pueden agregar contexto y ayudar a detectar esta actividad:

- Registros de creación de procesos y líneas de comando: Los registros de seguridad con la identificación de evento `4688` y los registros de Sysmon con la identificación de evento `1` brindan visibilidad de la ejecución del comando `ntdsutil`. Estos registros indican los argumentos de la línea de comandos utilizados, lo que ofrece la primera capa de información. En un entorno empresarial típico, el uso de `ntdsutil` para crear instantáneas puede no ser habitual y podría indicar una actividad inusual.
- Registros de acceso y creación de archivos: La identificación de evento `11` de Sysmon registra los eventos de creación de archivos. La creación de una instantánea utilizando `ntdsutil` involucra generar archivos específicos, que pueden reflejarse en estos registros. Además, los registros de seguridad con la identificación de evento `4663`, que registra los intentos de acceder a objetos, pueden indicar el acceso a archivos confidenciales, como `NTDS.dit`, lo que proporciona más contexto al proceso de creación de instantáneas.
- Registros de uso de privilegios: La identificación de evento `4673` en los registros de seguridad indica el uso de servicios privilegiados. La ejecución de `ntdsutil` requiere privilegios elevados, y la supervisión de dicho aumento de privilegios puede ser un indicador clave de un posible uso indebido, especialmente cuando se relaciona con la ejecución del comando.
- Registros de autenticación y actividad de la red: Junto con estos registros, los registros de actividad de la red pueden proporcionar contexto sobre cualquier conexión remota simultánea o transferencia de datos, lo que podría indicar intentos de exfiltración de datos luego de la creación de la instantánea. Los registros de autenticación también pueden ser fundamentales para determinar quién ejecutó el comando `ntdsutil` y si la cuenta utilizada se alinea con el comportamiento administrativo típico.

En este ejemplo del mundo real, si una organización implementara y siguiera rigurosamente las sugerencias de prácticas recomendadas (indicadas anteriormente), el resultado de la actividad de APT podría mitigarse. Mediante una segmentación estricta de la red y la aplicación de principios de privilegio mínimo, una organización podría restringir la capacidad del agente de amenazas para moverse lateralmente en la red. Incluso si se extraen credenciales de alto nivel, la segmentación podría limitar el alcance del agente a segmentos aislados de la red. Además, una administración sólida del acceso privilegiado garantizaría que el acceso elevado se conceda con moderación y se supervise de cerca, lo que dificultaría que un agente de amenazas cibernéticas haga un uso indebido de las credenciales robadas. La lista de aplicaciones permitidas evitaría aún más la ejecución de software no autorizado, lo que reduciría el riesgo de que se implementen herramientas administrativas adicionales. Sin embargo, estas medidas son más efectivas cuando se combinan con una supervisión atenta, una respuesta rápida a incidentes y una reevaluación continua de los controles y las configuraciones de acceso a la red.

PSExec.exe

`PSExec.exe` forma parte del conjunto de Microsoft PsTools y es una herramienta común en las tácticas LOTL debido a su capacidad de ejecutar comandos de forma remota en sistemas en red, a menudo con privilegios elevados de `SYSTEM`. Comprender el contexto de las actividades de las

técnicas LOTL también es fundamental cuando se trata de ciertas herramientas, como `PSExec.exe`, comúnmente utilizada para la administración y ejecución remota de procesos.

Los agentes patrocinados por el Estado han utilizado el siguiente comando `PSExec.exe` para ejecutar comandos únicos, como este intento de quitar configuraciones de proxy de puerto en un host remoto:

- `"C:\pstools\psexec.exe" {REDACTED} -s cmd /c "cmd.exe /c netsh interface portproxy delete v4tov4 listenaddress=0.0.0.0 listenport=9999"`[1]).

Para detectar y contextualizar de forma efectiva dicho uso de `PSExec.exe`, los defensores de redes pueden confiar en varios registros:

- Registros de creación de procesos y líneas de comando: Los registros de seguridad con la identificación de evento `4688` y los registros de Sysmon con la identificación de evento `1` ofrecen información fundamental sobre la ejecución de `PSExec.exe` y cualquier comando asociado, como `Netsh`. Estos registros reflejan la línea de comando utilizada y brindan información esencial sobre la naturaleza y la intención del proceso.
- Registros de credenciales explícitas y uso privilegiado: Los registros de seguridad con la identificación de evento `4672` indican casos de privilegios especiales que se asignan a nuevos inicios de sesión. Esto es particularmente pertinente cuando PSExec se ejecuta con el modificador `-s`, que ejecuta el comando con privilegios de `SYSTEM`. Además, la identificación de evento `4648` en los registros de seguridad puede reflejar casos de usos de credenciales explícitas, lo que se produce cuando se ejecuta PSExec con credenciales de usuario específicas.
- Registros de Sysmon: La identificación de evento 3 de Sysmon es fundamental para registrar conexiones de red, ya que indican la ejecución remota, un componente central de la funcionalidad de PSExec. Estos registros pueden proporcionar información valiosa sobre la interacción de la red durante la operación de PSExec. Las identificaciones de evento `12`, `13` y `14` (eventos de registro) reflejarán cualquier cambio realizado al registro a causa del comando `Netsh`. En este caso específico, los registros probablemente mostrarían eventos de eliminación (identificación de evento `14`) para las claves de registro asociadas con la configuración del proxy de puerto. Por lo general, las claves afectadas estarían en rutas similares a `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\PortProxy\v4tov4`.
- Registros de auditoría del registro de Windows: Los registros de auditoría del registro de Windows (si se habilitan) indicarían las modificaciones realizadas a las claves del registro relacionadas con la configuración del proxy de puerto. Debido al comando específico `Netsh` utilizado, los registros indicarían la eliminación de entradas con la clave `v4tov4`, que administran la configuración del proxy de puerto para la dirección de escucha `0.0.0.0` y el puerto de escucha `9999`. Los registros incluirían ciertos detalles, como la marca de tiempo del cambio, la cuenta con la que se realizó el cambio (probablemente la cuenta de `SYSTEM` en este caso, debido al modificador en PSExec) y los valores de registro específicos que se modificaron o eliminaron.

- Registros de cortafuegos y red: Para el análisis del tráfico de la red, específicamente el tráfico de SMB, que es característico del uso de PSExec, son fundamentales los registros de dispositivos de red. Por lo general, los defensores de redes pueden identificar conexiones a recursos compartidos administrativos (como el recurso compartido) y otro tráfico de comunicación entre procesos (IPC, por sus siglas en inglés) a través del puerto TCP . Los registros de cortafuegos en el sistema objetivo, si el registro de cortafuegos local está habilitado, también pueden proporcionar información sobre los cambios en la configuración de red del sistema. Estos registros pueden reflejar modificaciones en la configuración del proxy de puerto o cambios en el estado o las reglas del cortafuegos, que correspondan al momento de la ejecución del comando.

Corrección

Si se detecta un riesgo, las organizaciones deben implementar las siguientes respuestas defensivas inmediatas:

1. **Investigue para determinar la cuenta con el nivel de privilegio más alto a la que tenía o tiene acceso el agente de amenazas.**
    a. **Si el agente de amenazas tiene el control de una cuenta administrativa, como el administrador de dominio de Windows Active Directory, restablezca las credenciales de las cuentas privilegiadas y no privilegiadas dentro del límite de confianza de cada cuenta puesta en riesgo.**
        i. Fuerce el restablecimiento de contraseñas, anule los certificados y emita nuevos para todas las cuentas o dispositivos.
        ii. En entornos de Windows:
            1. Si se sospecha que los agentes obtuvieron acceso al DC/AD, se deben restablecer las contraseñas de todas las cuentas locales, como `Guest`, `HelpAssistant`, `DefaultAccount`, `System`, `Administrator` y `kbrtgt`. Es esencial restablecer la contraseña de la cuenta `kbrtgt`, ya que esta cuenta es responsable de administrar las solicitudes de vales de Kerberos, así como de cifrarlas y firmarlas. La cuenta `kbrtgt` debe restablecerse dos veces (tiene un historial de dos contraseñas). Para evitar cualquier problema, es necesario permitir que se replique el primer restablecimiento de la cuenta `kbrtgt` antes del segundo. Consulte la Orientación de expulsión de redes que se vieron afectadas por el riesgo de SolarWinds y Active Directory/M365 elaborada por la CISA para obtener más información. Si bien las medidas se diseñaron para las agencias de FCEB puestas en riesgo en la cadena de suministro de SolarWinds Orion de 2020, son aplicables para las organizaciones con riesgo de Windows AD.
            2. Si se sospecha que el archivo `ntds.dit` se ha exfiltrado, deberán restablecerse todas las contraseñas de los usuarios del dominio.
            3. Revise las políticas de acceso para anular de forma provisoria los privilegios o el acceso para las cuentas o los dispositivos afectados. Si es necesario evitar alertar al agente de amenazas cibernéticas (p. ej., con fines de inteligencia), se pueden reducir los privilegios de las cuentas o los dispositivos afectados a fin de "contenerlo".

b. **Restablezca las claves de acceso o las credenciales de cuentas relevantes si la investigación determina que el acceso del agente de amenazas está limitado a permisos no elevados.**
   i. Supervise las cuentas relacionadas, especialmente las administrativas, para detectar cualquier señal adicional de acceso no autorizado.

2. **Realice una auditoría de todas las configuraciones de dispositivos de red y dispositivos perimetrales con indicadores de actividad maliciosa a fin de detectar señales de cambios no autorizados o maliciosos en la configuración.**
   Las organizaciones deben asegurarse de realizar una auditoría de la configuración actual del dispositivo de red en ejecución y cualquier configuración local que pueda cargarse en el momento del arranque. Si se identifican cambios de configuración:
   a. Cambie todas las credenciales que se utilizan para administrar dispositivos de red, con el propósito de incluir claves y cadenas utilizadas a fin de asegurar las funciones de los dispositivos de red (cadenas del protocolo simple de administración de redes [SNMP, por sus siglas en inglés] o credenciales de usuario, claves precompartidas del protocolo de seguridad de Internet [IPsec, por sus siglas en inglés] y del intercambio de claves de Internet [IKE, por sus siglas en inglés], secretos de enrutamiento, secretos del sistema de control de acceso del controlador de acceso a terminales [TACACS, por sus siglas en inglés] y del servicio de autenticación remota telefónica de usuario [RADIUS, por sus siglas en inglés], claves y certificados de RSA, etc.).
   b. Actualice todo el firmware y software a la última versión.
3. Denuncie el riesgo a una agencia autora, según corresponda.
   a. **Organizaciones de EE. UU.:** Para denunciar actividades sospechosas o delictivas relacionadas con información que se encuentra en esta guía conjunta, utilice los siguientes contactos:
      i. Comuníquese con el Centro de Operaciones (Operation Center) de la CISA, el cual está disponible las 24 horas, los 7 días de la semana, enviando un correo electrónico a Report@cisa.gov o llamando al (888) 282-0870, o bien, comuníquese con su oficina local de la FBI. Si es posible, incluya la siguiente información sobre el incidente: la fecha, la hora y la ubicación del incidente; el tipo de actividad; la cantidad de personas afectadas; el tipo de equipo utilizado para la actividad; el nombre de la empresa u organización que presenta la denuncia; y un punto de contacto designado.
      ii. Para conocer los requisitos de clientes de la NSA o realizar consultas generales de ciberseguridad, comuníquese con Cybersecurity_Requests@nsa.gov.
      iii. Las entidades de transporte reguladas por la TSA deben presentar su denuncia a la central de la CISA, de acuerdo con los requisitos que se encuentran en las directrices o los programas de seguridad, o en las órdenes de la TSA que correspondan.
      iv. Las entidades obligadas a denunciar los incidentes al DOE deben seguir los requisitos establecidos de presentación de denuncias, según corresponda. Para realizar otras consultas del sector de energía, comuníquese con EnergySRMA@hq.doe.gov.
      v. Las organizaciones del sector de sistemas de agua y aguas residuales deben comunicarse con la División de Infraestructura de Agua y Resiliencia Cibernética (Water Infrastructure and Cyber Resilience Division) de la EPA enviando un correo

electrónico a watercyberta@epa.gov para proporcionar información de la situación de forma voluntaria.

b. **Organizaciones de Australia:** Visiten cyber.gov.au o llamen al 1300 292 371 (1300 CYBER 1) para denunciar incidentes de ciberseguridad y acceder a las alertas y los avisos.
c. **Organizaciones de Canadá:** Denuncien los incidentes enviando un correo electrónico al Centro Canadiense de Ciberseguridad (CCCS, por sus siglas en inglés) a contact@cyber.gc.ca.
d. **Organizaciones de Nueva Zelanda:** Denuncien los incidentes de ciberseguridad a incidents@ncsc.govt.nz o llamen al 04 498 7654.
e. **Organizaciones del Reino Unido:** Denuncien un incidente importante de ciberseguridad en ncsc.gov.uk/report-an-incident (supervisado las 24 horas) o, para recibir asistencia urgente, llamen al 03000 200 973.

4. Las organizaciones con entornos híbridos o en la nube deben aplicar las prácticas recomendadas para la administración de identidad y acceso a credenciales.
5. **Minimice y controle el uso de las herramientas y los protocolos de acceso remoto** mediante la aplicación de las prácticas recomendadas del documento conjunto Guía para asegurar el software de acceso remoto y la hoja de información conjunta de ciberseguridad: Cómo mantener PowerShell: medidas de seguridad para implementar y adoptar.

Para obtener más información sobre la corrección y la respuesta de incidentes, consulte los siguientes recursos:

- Aviso conjunto Enfoques técnicos para descubrir y corregir actividad maliciosa. Este aviso proporciona las prácticas recomendadas de respuesta a incidentes.
- Manuales de respuesta a vulnerabilidades e incidentes de ciberseguridad del Gobierno federal de la CISA. Si bien se diseñaron para las agencias del Poder Ejecutivo Civil Federal (FCEB) de EE. UU., los manuales son aplicables para todas las organizaciones. El manual de respuesta a incidentes proporciona procedimientos para identificar, coordinar, corregir, recuperar y monitorear las medidas de mitigación exitosas de incidentes.

Seguridad desde el diseño: recomendaciones para fabricantes de software

Las secciones anteriores "Sugerencias de prácticas recomendadas" y "Recomendaciones para la detección" se aplican a las organizaciones de infraestructura fundamental con entornos híbridos o en las instalaciones. El software inseguro permite que agentes de amenazas aprovechen las fallas para habilitar técnicas LOTL, y la responsabilidad no debe recaer únicamente en el usuario final. La CISA insta a los fabricantes de software a implementar lo siguiente para reducir la prevalencia de configuraciones y contraseñas predeterminadas débiles, reconocer la necesidad de un registro mejorado de bajo costo o sin costo y otros problemas explotables identificados en esta guía.

- **Minimice las superficies de ataque que los agentes de amenazas cibernéticas pueden aprovechar utilizando técnicas LOTL.** Deshabilite los protocolos innecesarios por defecto, limite la cantidad de procesos y programas que se ejecutan con privilegios elevados y tome otras medidas para limitar la capacidad de los agentes de amenazas cibernéticas de aprovechar la funcionalidad nativa para realizar intrusiones.

- **Integre la seguridad en la arquitectura del producto** en todo el ciclo de vida de desarrollo de software (SDLC, por sus siglas en inglés).
- **Exija la MFA, idealmente la** MFA resistente a la suplantación de identidad, a los usuarios con privilegios y haga de la MFA una característica predeterminada, en lugar de una voluntaria.
- **Proporcione registros de alta calidad para plataformas y aplicaciones sin costo adicional.** Los servicios en la nube deben comprometerse a generar y almacenar registros relacionados con la seguridad sin costo adicional. Los productos locales también deberían generar registros relacionados con la seguridad sin costo adicional.
- **Busque y reduzca la "guía de refuerzo".** Reduzca el tamaño de las "guías de refuerzo" que se incluyen con los productos y esfuércese por garantizar que el tamaño se reduzca con el tiempo a medida que se lanzan nuevas versiones del software. Integre componentes de la "guía de refuerzo" como configuración predeterminada del producto.
- **Considere las consecuencias de la configuración de seguridad en la experiencia del usuario.** Cada nueva configuración aumenta la carga cognitiva de los usuarios finales, y debe evaluarse junto con el beneficio empresarial que deriva. Idealmente, no debería existir una configuración; en cambio, la configuración más segura debería integrarse en el producto de forma predeterminada. Cuando es necesaria la configuración, la opción predeterminada debe ser ampliamente segura contra amenazas comunes.
- **Quite las contraseñas predeterminadas.** Las contraseñas predeterminadas deben quitarse por completo o, si es necesario, deben generarse o configurarse en la primera instalación y, luego, alternarse periódicamente.
- **Quite o limite la ejecución de código dinámico.** La ejecución de código dinámico permite que los productos sean más versátiles, pero es una superficie de ataque extremadamente vulnerable, que puede explotarse con IOC difíciles de detectar.
- **Quite las credenciales codificadas de forma rígida.** Las aplicaciones y los scripts que contienen credenciales de texto sin formato codificadas de forma rígida permiten que los agentes maliciosos aprovechen las credenciales para acceder fácilmente a los recursos y ampliar su acceso en una red.

Estas medidas de mitigación se alinean con las tácticas proporcionadas en la guía conjunta Cambio del equilibrio de los riesgos de ciberseguridad: principios y enfoques para el 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 principios 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 la seguridad desde el diseño, consulte CISA: Seguridad desde el diseño, Dirección de Señales de Australia: Seguridad desde el diseño y Principios de seguridad desde el diseño: seguridad del Gobierno del Reino Unido.

Recursos

CISA: Herramienta de registro simplificado

NSA, CISA, NCSC-NZ y NCSC-UK: Cómo mantener PowerShell: medidas de seguridad para implementar y adoptar
NSA y CISA: Guía de refuerzo de Kubernetes
Microsoft: Aplicaciones que pueden eludir el Control de aplicaciones de Windows Defender (WDAC, por sus siglas en inglés) y cómo bloquearlas

Referencias

[1] CISA: People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection
[2] CISA: PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure
[3] Mandiant: Sandworm Disrupts Power in Ukraine Using a Novel Attack Against Operational Technology
[4] MITRE: Unsecured Credentials: Cloud Instance Metadata API
[5] MITRE: Event Triggered Execution
[6] MITRE: Automated Exfiltration: Traffic Duplication
[7] CISA: Scattered Spider
[8] Microsoft: cmd.exe
[9] Microsoft: Windows Management Instrumentation
[10] WMIC: WMI command-line utility
[11] Microsoft: What is PowerShell?
[12] MITRE: System Binary Proxy Execution: Mshta
[13] Man7: sh(1p)
[14] GNU: Bash Reference Manual
[15] Die.Net: csh(1)
[16] Zsh.org
[17] Stanford: vi
[18] Vim.org
[19] Man7: curl(1)
[20] Man7: tar(1)
[21] Microsoft: Controlling a Service Using SC
[22] Microsoft: Use the at command to schedule tasks
[23] Microsoft: New-Service
[24] Microsoft: Win32_Service class
[25] Microsoft: PsTools
[26] Microsoft: PsExec v2.43
[27] MITRE: PsExec
[28] Microsoft: Ntdsutil
[29] Microsoft: reg commands
[30] Microsoft: Detecting and Preventing LSASS Credential Dumping Attacks
[31] Man7: cat(1)
[32] Man7: less(1)
[33] Man7: more(1)
[34] Man7: head(1)

[35] Man7: tail(1)
[36] Man7: sudo(8)
[37] Die.net: gpg(1)
[38] Microsoft: Net.exe
[39] Microsoft: Dsquery
[40] Microsoft: Get-ADUser
[41] Microsoft: Ldifde
[42] Microsoft: ipconfig
[43] Microsoft: Dnscmd
[44] Microsoft: nslookup
[45] Die.net: nslookup(1)
[46] Die.net: dig(1)
[47] Man7: ifconfig(8)
[48] Man7: ip(8)
[49] Microsoft: dir
[50] Man7: ls(1)
[51] Microsoft: Get-ChildItem
[52] Microsoft: netstat
[53] Man7: netstat(8)
[54] Microsoft: Get-NetTCPConnection
[55] Microsoft: tasklist
[56] Microsoft: Get-Process
[57] Microsoft: whoami
[58] Man7: whoami(1)
[59] Man7: id(1)
[60] Man7: uname(1)
[61] Die.net: procinfo(8)
[62] Man7: lscpu(1)
[63] Microsoft: Understanding the Remote Desktop Protocol (RDP)
[64] Virtual Network Computing from ORL: VNC Documentation
[65] Microsoft: Windows Remote Management
[66] OpenSSH: Manual Pages
[67] Man7: ssh(1)
[68] Man7: scp(1)
[69] Man7: iptables(8)
[70] Debian: NFT

Descargo de responsabilidad

La información contenida en este informe se proporciona “tal cual” solo con fines informativos. Las agencias autoras no respaldan ninguna entidad comercial, producto, empresa o servicio, incluidas las entidades, los productos o los servicios vinculados o mencionados en este documento. Cualquier referencia a entidades comerciales específicas o productos, procesos o servicios mediante marcas de servicio, marcas comerciales, fabricantes o de otro modo no constituye ni implica respaldo, recomendación o favoritismo por parte de las agencias autoras.

Agradecimientos

Las siguientes organizaciones contribuyeron a esta guía:

- Amazon Web Services (AWS).
- Representantes de la industria energética, a través del piloto del Centro de Análisis de Amenazas Energéticas (ETAC, por sus siglas en inglés) de la Oficina de Ciberseguridad, Seguridad Energética y Respuesta a Emergencias (CESER, por sus siglas en inglés) del DOE.
- Nippon Telegraph and Telephone (NTT).

Historial de versiones

7 de febrero de 2024: versión inicial.

Apéndice A: Técnicas LOTL en entornos híbridos y de Windows, Linux y macOS

Windows

Algunos LOLBins comunes que los agentes de amenazas cibernéticas utilizan en entornos de Windows (híbridos y en las instalaciones) son `wmic.exe`, `ntdsutil.exe`, `Netsh`, `cmd.exe` y PowerShell para la ejecución. Por ejemplo:

- En un riesgo confirmado, la CISA observó el uso de `ntdsutil.exe` de manera potencialmente no autorizada en los DC. En un caso, el archivo `ntds.dit` se movió de su ubicación original a otra dentro del directorio `HarddiskVolumeShadowCopy`.
- En otro caso, la CISA observó posibles actividades de exfiltración de datos, incluida la ejecución del comando del Instrumental de administración de Windows (WMIC, por sus siglas en inglés), la creación de directorios provisorios, la iniciación del proceso de instantáneas de volumen y el montaje de la base de datos `ntds.dit`. Se hicieron modificaciones a las claves de registro `MountPoints2\CPC` para tres cuentas de usuario, lo que sugiere que los agentes de amenazas cibernéticas intentaron ocultar los indicios de exfiltración de datos.
- La CISA observó que los agentes de amenazas utilizan el comando `Netsh` para crear una modificación del registro del proxy de puerto en los dispositivos puestos en riesgo. Específicamente, la modificación se agregó a la clave de registro `HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\PortProxy\v4tov4\cp\0.0.0.0/49275 | {redacted IP address}/8443`. Esta configuración de registro provocó que el tráfico entrante en el puerto `49275` se reenviara a un servidor de comando y control sospechoso de un agente de amenazas en el puerto `8443`.

Linux

Algunos LOLBins comunes que los agentes de amenazas cibernéticas utilizan en entornos de Linux son `curl`, `systemctl`, `systemd` y Python. Por ejemplo, los agentes de amenazas cibernéticas hacen lo siguiente:

- Utilizan entornos de scripting, como Python, para obtener acceso al shell interactivo, generar un shell inverso, transferir archivos o ejecutar scripts personalizados en dispositivos puestos en riesgo.
- Utilizan certificados o credenciales de SSH para moverse lateralmente y camuflarse con las actividades normales del administrador, y así aprovechan las relaciones confiables entre los hosts de Linux.
- Explotan el software con permisos elevados o cron jobs elevados para aumentar los privilegios o mantener la persistencia.
- Explotan los binarios `Suid Bit` configurados para elevar privilegios o acceder a archivos del sistema asegurados.

macOS

- Se sabe que los agentes maliciosos utilizan las siguientes técnicas LOTL en entornos de macOS.

- Explotación de herramientas y entornos de scripting en macOS: Los agentes de amenazas cibernéticas explotan los lenguajes de scripting nativos y las herramientas integradas con fines maliciosos. Utilizan AppleScript y Bash para automatizar tareas, controlar aplicaciones y ejecutar comandos, y a menudo manipulan AppleScript a fin de interactuar con aplicaciones legítimas para la exfiltración de datos o la manipulación del sistema. Además, hacen mal uso de las herramientas integradas, como `osascript` para ejecutar AppleScripts y JavaScripts, `launchctl` para administrar demonios y agentes, y `curl` para las transferencias de archivos. De esta forma, aprovechan las funcionalidades inherentes de macOS con el propósito de realizar actividades maliciosas.
- Manipulación de archivos de lista de propiedades (PLIST) para lograr persistencia: Los agentes de amenazas cibernéticas pueden modificar archivos de PLIST a fin de ejecutar de forma automática cargas útiles maliciosas durante el arranque del sistema o el inicio de sesión del usuario.
- Elevación de privilegios mediante `sudoers` mal configurados: Los agentes de amenazas cibernéticas pueden explotar las configuraciones erróneas de `sudoers` que permiten ejecutar comandos como superusuario sin contraseña, lo que les posibilita obtener un acceso elevado.
- Elusión de Gatekeeper para la ejecución de malware: A fin de eludir Gatekeeper, los agentes de amenazas cibernéticas pueden aprovechar los certificados de desarrollador confiables o modificar la configuración del sistema para permitir la ejecución por parte de desarrolladores no identificados.

Entornos en la nube

Entre algunas de las técnicas LOTL que se sabe que los agentes maliciosos utilizan en entornos en la nube, se incluyen las siguientes:

- Mal uso de servicios nativos de metadatos de instancia (IMDS, por sus siglas en inglés) en la nube: La API de IMDS se puede consultar (sin autenticación) desde instancias en la nube para obtener una variedad de información útil, incluidas las credenciales que las aplicaciones utilizan para interactuar con otros servicios en la nube. Los agentes de amenazas cibernéticas que obtienen acceso a instancias virtuales pueden intentar consultar la API de IMDS para obtener credenciales y conseguir más acceso a los recursos de la nube [4].
- Obtención de la persistencia a través de tareas programadas: Los agentes de amenazas cibernéticas pueden utilizar los servicios de automatización de la nube para lograr la persistencia en el entorno mediante la creación o la modificación de un desencadenador de eventos para ejecutar scripts maliciosos cada vez que ocurre el evento. Los agentes de amenazas cibernéticas también pueden utilizar esta técnica a fin de aumentar los privilegios y aprovechar el hecho de que estas acciones automatizadas se pueden configurar para ejecutarse en una cuenta diferente a la del usuario (como una cuenta de servicio, que puede tener más privilegios que el agente de amenazas cibernéticas) [5].
- Obtención de la persistencia mediante cuentas de servicio: Las cuentas de servicio se utilizan comúnmente para proporcionar a las aplicaciones acceso a los recursos de la nube con los que necesitan comunicarse. Como estas cuentas se utilizan normalmente para aplicaciones, carecen de protección adicional, como MFA, que con frecuencia se requiere para las cuentas de usuario. Los agentes de amenazas pueden atacar estas cuentas para

lograr un acceso persistente al inquilino de la nube, en lugar de tener que eludir continuamente las protecciones de MFA en las cuentas de usuario, incluso con credenciales puestas en riesgo.

- Reflejo del tráfico mediante puertas de enlace de aplicaciones: Los proveedores de la nube suelen ofrecer servicios de reflejo del tráfico para duplicar y reenviar el tráfico a fin de que los defensores de redes lo analicen. Los agentes de amenazas cibernéticas pueden aprovechar estos servicios para exfiltrar el tráfico [6].
- Uso indebido de las herramientas de CLI de los proveedores de servicios en la nube (CSP, por sus siglas en inglés): Las herramientas de CLI que ofrecen los CSP, como la CLI de AWS y la CLI de Azure, son accesibles dentro de los entornos en la nube. Las herramientas de CLI pueden utilizarse indebidamente para actividades no autorizadas en recursos de la nube, incluida la exfiltración de datos y el establecimiento de amenazas persistentes.

Entornos híbridos

- Se sabe que, en entornos híbridos, los agentes maliciosos utilizan las técnicas LOTL que se detallan a continuación. **Nota:** Las organizaciones con entornos híbridos deben revisar el contenido de Windows y Linux, según corresponda.
- Explotación de sistemas de federación de identidades: Los entornos híbridos emplean con frecuencia los Servicios de federación de Active Directory (ADFS, por sus siglas en inglés) para la administración de identidades en plataformas en las instalaciones y en la nube. Los agentes de amenazas atacan los ADFS para poner en riesgo y manipular los tokens de federación, y para hacerse pasar por entidades o usuarios legítimos. Esto permite que los agentes de amenazas obtengan acceso no autorizado a una multitud de recursos.
- Manipulación de tokens y ataques de reproducción: En entornos híbridos, los agentes de amenazas explotan la confianza inherente entre los proveedores de identidades en las instalaciones y los servicios en la nube. Lo logran adquiriendo o fabricando tokens de federación, como tokens de lenguaje de marcado de aserción de seguridad (SAML, por sus siglas en inglés). Esta táctica elude de forma efectiva las medidas de seguridad que dependen de la verificación tradicional basada en credenciales.
- LOLBins en entornos híbridos: Los LOLBins de Windows, como PowerShell y `cmd.exe`, se utilizan para manipular sistemas tanto en las instalaciones como en la nube. **Nota:** Detectar el uso indebido es más difícil en estos entornos, ya que presentan una menor segmentación, en comparación con los sistemas independientes en las instalaciones o en la nube.
- Uso indebido de las herramientas de CLI de los proveedores de servicios en la nube (CSP): Las herramientas de CLI que ofrecen los CSP, como la CLI de AWS y la CLI de Azure, son accesibles dentro de los entornos híbridos. Las herramientas de CLI pueden utilizarse indebidamente para actividades no autorizadas en recursos de la nube, incluida la exfiltración de datos y el establecimiento de amenazas persistentes.
- Ataque a plataformas híbridas de administración en la nube: Las plataformas que supervisan los recursos tanto en las instalaciones como en la nube son posibles vectores de intrusión. Los agentes de amenazas pueden explotar estas plataformas para obtener información completa sobre la infraestructura híbrida, modificar configuraciones o implementar elementos maliciosos.

Apéndice B: Herramientas externas para técnicas LOTL

Para las técnicas LOTL, los agentes de amenazas cibernéticas usan softwares desplegados y softwares de acceso remoto, incluidos los siguientes:

- **Sistemas de administración de dispositivos móviles.** Los sistemas de administración de dispositivos móviles (MDM) son objetivos atractivos para los agentes de amenazas porque brindan acceso elevado a miles de dispositivos móviles.
- **Supervisión y administración remota/administración de configuración del centro del sistema (SCCM, por sus siglas en inglés).** El software de RMM presenta importantes capacidades para supervisar u operar dispositivos y sistemas, así como para obtener mayores permisos, lo que lo convierte en una herramienta atractiva para que los agentes de amenazas cibernéticas mantengan la persistencia y se muevan de forma lateral en redes puestas en riesgo.
- **Sistemas de administración de correcciones.** Los sistemas de administración de correcciones brindan acceso a miles de sistemas.
- **EDR:** Los agentes de amenazas cibernéticas aprovechan las herramientas comunes de EDR instaladas en las redes de la víctima para aprovechar las capacidades de shell remoto de las herramientas.[7]
- **Herramientas de administración de máquina virtual (VM, por sus siglas en inglés):** Los agentes de amenazas cibernéticas atacan las herramientas vitales de administración de virtualización para explotar las infraestructuras de VM. Utilizan estas plataformas para controlar VM, ejecutar comandos, facilitar el movimiento lateral en la red y acceder a datos confidenciales.
- **Herramientas de administración de bases de datos:** Los agentes de amenazas cibernéticas pueden atacar las herramientas de administración de bases de datos para ejecutar comandos de lenguaje de consulta estructurado (SQL, por sus siglas en inglés), extraer datos confidenciales o manipular las entradas de bases de datos.
- **Sistemas de administración de redes:** Los sistemas de administración de redes ofrecen amplia visibilidad y control sobre los dispositivos de red, y son objetivos principales. El riesgo de estos sistemas puede generar la capacidad del agente de amenazas cibernéticas para supervisar el tráfico de la red, modificar las configuraciones y potencialmente interrumpir las operaciones de la red, explotando las mismas herramientas utilizadas para garantizar la estabilidad y la seguridad de la red.
- **Sistemas de administración de identidad y acceso (IAM, por sus siglas en inglés).** Los sistemas de IAM, que son fundamentales para administrar las identidades de los usuarios y su acceso a la red, suelen ser el objetivo de los agentes de amenazas cibernéticas debido a su función esencial en el control del acceso a la red.
- **Administración de servicios de tecnologías de la información (ITSM, por sus siglas en inglés).** Los agentes de amenazas cibernéticas pueden manipular las plataformas de administración de servicios de tecnologías de la información (ITSM) y explotar estos sistemas para alterar vales, flujos de trabajo, y activar acciones automatizadas con fines maliciosos.
- Para obtener más información, consulte el documento conjunto Guía para asegurar el software de acceso remoto.

Apéndice C: LOLBins conocidos que se utilizan de forma maliciosa

Nota: Esta guía utiliza el marco MITRE ATT&CK para entornos empresariales, versión 14. Para obtener asistencia con la asignación de las actividades cibernéticas maliciosas al marco MITRE ATT&CK, consulte las prácticas recomendadas para la asignación de MITRE ATT&CK de la CISA y MITRE ATT&CK, y la herramienta Decider de la CISA.

Consulte de la Tabla 1 a la Tabla 5 para informarse sobre los LOLBins conocidos que se utilizan de forma maliciosa, así como la táctica y la técnica de MITRE ATT&CK asociadas. Varios de los LOLBins que se especifican más abajo demuestran la multitud de técnicas disponibles para que los adversarios logren la misma meta.

Dado que los administradores utilizan estas herramientas para funciones legítimas, los defensores de redes no deben bloquear ni limitar su uso indiscriminadamente. En cambio, los defensores de redes deben seguir la orientación de esta guía para identificar posibles usos maliciosos en función del comportamiento. En algunos casos, también hay disponibles argumentos de la línea de comandos alternativos, y los defensores de redes deben tener en cuenta otras opciones (consulte los indicadores de `/dom` y `/domain` de `net.exe` o los indicadores de `i` e `ifm` de `ntdsutil.exe`).

***Tabla 1: LOLBins utilizados para la ejecución** [TA0002]*

LOLBin	Entorno	Uso	Técnica de MITRE ATT&CK
`cmd.exe`, `wmic.exe`, `powershell.exe`, `Mshta.exe`	Windows	El programa `cmd.exe` es una interfaz de línea de comandos para sistemas operativos (OS, por sus siglas en inglés) Windows.[8] El Instrumental de administración de Windows (WMI) se utiliza para administrar datos y operaciones en sistemas operativos de Windows, y `wmic.exe`, que está obsoleto, proporciona una interfaz de línea de comandos para WMI.[9],[10] PowerShell es un lenguaje de scripting y una herramienta de línea de comandos para sistemas operativos Windows.[11] `Mshta.exe` ejecuta archivos de aplicaciones de lenguaje de marcas de hipertexto (HTML, por sus siglas en inglés) de Microsoft, que son aplicaciones independientes que se ejecutan con modelos y tecnologías de Internet Explorer fuera del navegador.[12]	Intérprete de comandos y scripting [T1059] Ejecución de proxy binario del sistema: Mshta [T1218.005] Instrumental de administración de Windows [T1047]

LOLBin	Entorno	Uso	Técnica de MITRE ATT&CK
		Los agentes de amenazas cibernéticas pueden utilizar estas herramientas para modificar los argumentos de la línea de comandos, ofuscar las relaciones de procesos principales-secundarios, aislar los procesos secundarios e, incluso, ejecutar código en otros hosts. Los agentes también pueden usar algunas de estas para ejecutar cargas útiles secundarias.	
sh, bash, csh y zsh	Unix	Los shells de Unix, como sh,[13] bash,[14] csh [15] y zsh[16], son intérpretes universales de la línea de comandos y están instalados en la mayoría de los sistemas Linux y macOS. Los agentes de amenazas cibernéticas pueden hacer mal uso de estos shells como LOLBins para llevar a cabo operaciones maliciosas.	Intérprete de comandos y scripting [T1059]
Perl, Python y Ruby	Windows o Unix	Los lenguajes Perl, Python y Ruby, así como otros intérpretes de scripting, suelen estar presentes en sistemas Windows y Unix, y, con frecuencia, poseen permisos excesivos. Los agentes de amenazas cibernéticas pueden utilizar estos intérpretes de scripting para realizar la ejecución arbitraria de código.	Intérprete de comandos y scripting [T1059]
vim, vi, `curl` y tar	Unix	El editor de texto vim tiene un indicador --cmd que se puede utilizar para ejecutar comandos de shell o Python.[17] De manera similar, se puede hacer que el binario vi ejecute comandos con `:!` seguido del comando.[18] El comando curl tiene una opción --exec que permite ejecutar scripts o binarios después de descargar archivos.[19] Se puede engañar a la utilidad tar para que ejecute código de forma arbitraria pasando archivos especialmente diseñados o generando un shell interactivo mediante el indicador --checkpoint-action=exec.[20]	Intérprete de comandos y scripting [T1059]

LOLBin	Entorno	Uso	Técnica de MITRE ATT&CK
		Los agentes de amenazas cibernéticas pueden hacer mal uso de estas utilidades como LOLBins para llevar a cabo actividades maliciosas.	
`Sc.exe`, `at.exe`, comando New-Service de PowerShell, clase WMI Win32_Service	Windows	Estos LOLBins se utilizan para crear, modificar o ejecutar servicios. El comando `sc.exe` es una utilidad de línea de comandos para controlar servicios.[21] `at.exe` es una utilidad de línea de comandos que se usa para programar tareas.[22] New-Service de PowerShell puede crear nuevos servicios.[23] Win32_Service es una clase WMI que representa servicios en hosts que ejecutan sistemas operativos Windows.[24] Los agentes de amenazas cibernéticas pueden utilizar estas herramientas para crear servicios y moverse lateralmente.	Servicios del sistema: ejecución de servicios [T1569.002]
`PsExec.exe`	Windows	El programa `PsExec.exe`, parte del conjunto de PsTools, ejecuta procesos de forma remota. `PsExec.exe` puede iniciar símbolos del sistema interactivos en sistemas remotos y herramientas de habilitación remota, como IpConfig.[25],[26] Los agentes de amenazas cibernéticas suelen usar PsExec.exe para la ejecución de servicios, la creación remota de cuentas y el movimiento lateral.[27]	Servicios del sistema: ejecución de servicios [T1569.002]

***Tabla 2: LOLBins utilizados para el acceso a credenciales** [TA0006]*

LOLBin	Entorno	Uso	Técnica de MITRE ATT&CK
`Ntdsutil.exe`	Windows	`Ntdsutil.exe` es una herramienta de línea de comandos para sistemas operativos Windows. Se utiliza para la administración de Servicios de dominio de Active Directory (AD DS, por sus siglas en inglés) y Servicios de directorio ligero de Active Directory (AD LDS, por sus siglas en inglés).[28]	Vuelco de credenciales del sistema operativo: Servicios de directorio de NT (NTDS, por sus siglas en inglés) [T1003.003]

LOLBin	Entorno	Uso	Técnica de MITRE ATT&CK
		Los agentes de amenazas cibernéticas pueden utilizar Ntdsutil.exe para obtener credenciales exfiltrando copias de ntds.dit de los controladores de dominio (DC). ntds.dit es el principal archivo de la base de datos de Active Directory (AD) y, por defecto, 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.	
`reg.exe`	Windows	El programa `reg.exe` se utiliza para realizar operaciones con información de subclaves de registro y valores en entradas de registro.[29] Los agentes de amenazas cibernéticas pueden exportar los subárboles de registro SAM y SYSTEM para buscar credenciales almacenadas localmente.	Credenciales sin protección: credenciales en registros [T1552.002]
`lsass.exe`	Windows	El archivo ejecutable `lsass.exe` guarda las credenciales almacenadas en la memoria mientras los usuarios acceden al sistema para facilitar el inicio de sesión único en los recursos de la red. Debido a que `lsass.exe` se ejecuta con un alto nivel de privilegios, los agentes de amenazas cibernéticas utilizan herramientas de inyección de memoria, como Procdump y Mimikatz, para extraer datos de credenciales de lsass.exe.[30]	Vuelco de credenciales del sistema operativo: memoria del Servicio de subsistema de autoridad de seguridad local (LSASS, por sus siglas en inglés) [T1003.001]
sudo, cat, less, more, head, tail, vi y vim	Unix	Dado que muchas configuraciones y credenciales se almacenan como archivos en sistemas basados en Unix, los agentes de amenazas aprovechan cada vez más las utilidades universales de Unix que pueden leer archivos para descubrir credenciales almacenadas en sistemas puestos en riesgo. Ciertos comandos, como cat,[31] less,[32] more,[33] head [34] y tail [35], cuando se los invoca en archivos que contienen secretos, como contraseñas con hash, claves privadas, tokens de API o cadenas de conexión de bases de datos, podrían permitir que el agente de amenazas cibernéticas robe	Vuelco de credenciales del sistema operativo: /etc/passwd y /etc/shadow [T1003.008] Credenciales sin protección [T1552.001]

LOLBin	Entorno	Uso	Técnica de MITRE ATT&CK
		de forma encubierta estas credenciales para explotarlas aún más. De manera similar, los editores de texto estándar, como vi y vim, podrían permitir que los agentes de amenazas cibernéticas accedan al contenido de archivos confidenciales. Finalmente, se pueden usar ciertas utilidades, como sudo, para elevar los privilegios y volcar archivos de credenciales como superusuario.[36]	
gpg	Unix	El binario gpg puede contener claves o credenciales descifradas si no se asegura correctamente.[37]	Credenciales sin protección [T1552.001]

***Tabla 3: LOLBins utilizados para el descubrimiento** [TA0007]*

LOLBin	Entorno	Uso	Técnica de MITRE ATT&CK
`net.exe`, `dsquery.exe`, cmdlets GET-AD* de PowerShell, `ldifde.exe`	Windows	El archivo ejecutable `net.exe` puede consultar Active Directory, administrar servicios en ejecución, enumerar recursos compartidos, entre otros elementos.[38] Dsquery es una herramienta de línea de comandos del sistema operativo Windows para consultar Active Directory.[39] Los cmdlets GET-AD* de PowerShell obtienen objetos del usuario de Active Directory.[40] `ldifde.exe` es una herramienta de línea de comandos de Windows que crea, modifica y elimina objetos del directorio.[41] Los agentes de amenazas cibernéticas los utilizan para realizar consultas del protocolo ligero de acceso a directorios (LDAP) a fin de enumerar grupos y usuarios del dominio. Es posible que ciertos ejecutables, como dsquery.exe y ldifde.exe, no estén presentes en todos los sistemas; solo se instalan junto con determinadas funciones (como controladores de dominio) o sistemas operativos obsoletos. La compatibilidad con versiones anteriores	Descubrimiento de cuenta: cuenta de dominio [T1078.002]

LOLBin	Entorno	Uso	Técnica de MITRE ATT&CK
		permite a los adversarios cargar y ejecutar estas herramientas legítimas de Microsoft de forma semi-LOTL.	
`ipconfig.exe`, `dnscmd.exe`, `nslookup.exe`, nslookup y dig	Windows o Unix	`ipconfig.exe` puede volcar los registros DNS almacenados del sistema, así como configuraciones actuales de la red. [42] `dnscmd.exe` es una interfaz de línea de comandos para administrar servidores DNS.[43] `nslookup.exe` en Windows o el binario nslookup en Unix muestran información de DNS.[44],[45] El binario dig se puede utilizar para interrogar a los servidores DNS. [46] Los agentes de amenazas cibernéticas pueden utilizarlos para enumerar el sistema de nombres de dominio (DNS) interno.	Descubrimiento de la configuración de la red del sistema [T1016]
ifconfig, ip	Unix	Los binarios ifconfig [47] e ip [48] son utilidades de configuración de red comunes en los sistemas Unix y Linux, y se pueden utilizar para ver y configurar las interfaces de red. Los agentes de amenazas cibernéticas pueden utilizar ifconfig o ip para enumerar la información de red del sistema o modificar las configuraciones de red.	Descubrimiento de la configuración de la red del sistema [T1016]
cmd.exe /c dir, cmdlet Get-ChildItem de PowerShell y ls	Windows o Unix	cmd.exe /c dir, el binario ls y Get-ChildItem de PowerShell muestran una lista de los archivos y subdirectorios de un directorio.[49],[50],[51] Los agentes de amenazas cibernéticas pueden utilizar estos LOLBins para enumerar archivos en el disco y los servidores internos de bloque de mensajes del servidor (SMB).	Descubrimiento de archivos y directorios [T1083]
netstat.exe, cmdlet Get-NetTCPConnection de PowerShell y netstat	Windows o Unix	El archivo ejecutable netstat.exe en Windows o el binario netstat de Unix enumera las conexiones de TCP activas, los puertos en los que el host está escuchando y la tabla de enrutamiento de IP.[52],[53] El cmdlet Get-NetTCPConnection puede obtener las conexiones de TCP actuales.[54]	Descubrimiento de las conexiones de red del sistema [T1049]

LOLBin	Entorno	Uso	Técnica de MITRE ATT&CK
		Los agentes de amenazas cibernéticas pueden usar estos LOLBins para enumerar las conexiones de red locales, incluidas las conexiones de protocolo de control de transmisión (TCP) activas.	
Tasklist.exe, cmdlet Get-Process de PowerShell y ps	Windows o Unix	La herramienta Tasklist.exe en Windows o el binario ps en Unix enumera los procesos que están actualmente en ejecución.[55] El cmdlet Get-Process de PowerShell pone en marcha los procesos.[56] Los agentes de amenazas cibernéticas pueden usar estos LOLBins para enumerar softwares, servicios y procesos en un sistema puesto en riesgo.	Descubrimiento del software [T1518] Descubrimiento de servicios del sistema [T1007] Descubrimiento de procesos [T1057]
Whoami.exe, whoami, id	Windows o Unix	El archivo ejecutable Whoami.exe muestra información de usuarios, grupos y privilegios para el usuario que actualmente ha iniciado sesión en el host local de Windows.[57] El binario whoami en Unix puede mostrar el nombre de usuario del usuario que ha iniciado sesión actualmente.[58] El binario id en Unix puede mostrar la información de usuarios y grupos para un usuario especificado o un proceso actual.[59] Los agentes maliciosos pueden usar estos binarios para identificar usuarios principales o comunes de sistemas puestos en riesgo.	Descubrimiento del propietario/usuario del sistema [T1033]
systeminfo.exe	Windows	El ejecutable systeminfo.exe se puede utilizar para recopilar información sobre el sistema operativo del sistema puesto en riesgo. Los agentes de amenazas cibernéticas pueden utilizar systeminfo.exe para enumerar información del sistema local.	Descubrimiento de información del sistema [T1082]
uname, lscpu, procinfo	Unix	El binario uname (usado comúnmente con el indicador -a) imprime información del sistema, como la versión del núcleo y la arquitectura del hardware.[60] Los binarios procinfo y lscpu imprimen información del sistema y de la	Descubrimiento de información del sistema [T1082]

LOLBin	Entorno	Uso	Técnica de MITRE ATT&CK
		unidad central de procesamiento (CPU, por sus siglas en inglés). [61],[62] Los agentes de amenazas cibernéticas pueden usar estos binarios para enumerar información del sistema local.	

Tabla 4: LOLBins utilizados para el movimiento lateral

LOLBin	Entorno	Uso	Técnica de MITRE ATT&CK
RDP, VNC, WinRM	Windows o Unix	Los agentes pueden usar el protocolo de escritorio remoto (RDP) [63], la computación de red virtual (VNC, por sus siglas en inglés) [64] y WinRM [65] con cuentas válidas para interactuar de forma remota con los hosts. Esta actividad produce artefactos de registro diferentes de otros tipos de inicio de sesión.	Servicios remotos: protocolo de escritorio remoto [T1021.001] Servicios remotos: VNC [T1021.005] Servicios remotos: administración remota de Windows [T1021.006]
Shell seguro (SSH), copia segura (protocolo de copia segura [SCP, por sus siglas en inglés])	Windows o Unix	El shell seguro (SSH) se utiliza para iniciar sesión de forma segura en sistemas Windows o Unix a través de una interfaz de línea de comandos, y los agentes maliciosos pueden usar el SSH para moverse lateralmente.[66] [67] La copia segura (SCP) es un protocolo de transferencia de archivos cifrados que utiliza el protocolo de transferencia segura de archivos (SFTP, por sus siglas en inglés) y el SSH para transferir datos.[68] Los equipos rojos de la CISA suelen utilizar el SSH para moverse lateralmente a través de redes puestas en riesgo luego de adquirir las claves privadas del SSH para cuentas de servicios con privilegios. Los agentes de amenazas podrían utilizar estos LOLBins para acceder de forma remota a sistemas puestos en riesgo, exfiltrar datos o moverse lateralmente.	Protocolo de capa de aplicaciones [T1071] Servicios remotos: SSH [T1021.004]

Tabla 5: LOLBins utilizados para comando y control

LOLBin	Entorno	Uso	Técnica de MITRE ATT&CK
`Netsh`, proxy de puerto de interfaz de Netsh	Windows	Netsh es una utilidad integrada de scripting de la línea de comandos de Windows que puede mostrar o modificar la configuración de red de un host, lo que incluye el cortafuegos de Windows. El proxy de puerto de la interfaz de Netsh permite reenviar puertos en los hosts.	Proxy [T1090] Defensas contra deterioros: desactivación o modificación [T1562.001] Cortafuegos del sistema [T1562.004]
Ldifde.exe, certutil.exe	Windows	Los agentes maliciosos pueden utilizar estos LOLBins para permitir que los agentes de amenazas carguen, descarguen y ofusquen archivos en el disco.	Transferencia de herramientas de ingreso [T1105] Exfiltración sobre servicio web [T1567]
iptables, nftables	Linux	Los binarios iptables [69] y nftables [70] permiten que los administradores del sistema configuren las reglas de filtrado de paquetes de IP de los cortafuegos Linux. Los agentes maliciosos pueden usar iptables para redirigir el tráfico desde hosts basados en Linux.	Proxy [T1090]
Shell seguro (SSH), copia segura (SCP)	Windows o Unix	El SSH se utiliza para iniciar sesión de forma segura en sistemas Windows o Unix, a través de una interfaz de línea de comandos. [66] [67] La copia segura (SCP) es un protocolo de transferencia de archivos cifrados que utiliza el SFTP y el SSH para transferir datos.[68] Los agentes maliciosos pueden utilizar los indicadores -L, -R, -D para crear túneles proxy cifrados (ya sea de punto a punto o dinámicos). Los agentes de amenazas podrían utilizar estos LOLBins para acceder de forma remota a sistemas puestos en riesgo, exfiltrar datos o moverse lateralmente.	Protocolo de capa de aplicaciones [T1071] Servicios remotos: SSH [T1021.004]