Amenazas explicadas

Explicaciones en lenguaje sencillo de las técnicas de ataque que Cyber Crucible está diseñado para detener: malware sin archivos, ataques en memoria, automatización de hackers, infostealers y robo de tokens de sesión.

¿Puede Cyber Crucible detener el movimiento lateral del atacante?

El motor de comportamiento del producto y las metodologías de Zero Trust recopilan eficazmente evidencia de movimiento lateral.

Esa evidencia puede ser de movimiento lateral de proceso a proceso en la propia máquina, o puede tratarse del descubrimiento del punto de entrada de un atacante al sistema desde un sistema remoto, durante la realización de un Análisis de Causa Raíz.

Los programas y sus argumentos asociados con métodos de inyección de procesos y procesos de “living off the land” que abren otros procesos son capturados y enviados a Cyber Crucible.

Debido a la analítica de comportamiento de procesos a nivel de kernel, no existen procesos demasiado privilegiados para la observación y notificación de Cyber Crucible (incluyendo otros controladores de kernel, o incluso otras herramientas de seguridad de endpoint).

Las respuestas automatizadas de contra-extorsión se producen cuando se inician acciones de extorsión de datos o de cifrado por ransomware.

Por ejemplo, aquí se muestra un video que demuestra el movimiento lateral a través de una máquina, utilizando técnicas en memoria, y el exploit de Log4J. Tenga en cuenta que la suspensión automatizada del/los proceso(s) afectado(s) ocurrió después de que se iniciaran comportamientos de robo de datos y ransomware.

rr-log4j-procinj-3mins.mp4

Otro ejemplo de esta dinámica demuestra el uso por parte de un atacante para abrir un shell de Windows. La observación capturó toda la evidencia, pero la actividad fue suspendida una vez que el shell de Windows comenzó a intentar actividades de extorsión de datos (en este caso, robo de datos)

rr-com-dll.mp4

Por último, también se observa la migración desde un navegador explotado, y en este caso el atacante nunca logró moverse con éxito desde el navegador Chrome explotado, debido al monitoreo del estado de memoria del navegador:

rr-untrusted-chrome.mp4

¿Funciona la lista blanca de aplicaciones?

¿Qué es la lista blanca de aplicaciones?

La lista blanca de aplicaciones es un concepto en el que se dispone de una lista de programas a los que se les permite operar, y todo lo demás no puede funcionar.

Las tecnologías de lista blanca de aplicaciones más avanzadas combinarán algún tipo de lógica de origen y destino. Por ejemplo, una lista blanca de aplicaciones puede indicar: “El Bloc de notas de Windows tiene permitido acceder a la carpeta de Impuestos en mi escritorio, pero Microsoft Word no.”

Analizaremos esto con mayor detalle, pero, de forma genérica, las estrategias defensivas de lista blanca de aplicaciones dependen fuertemente de estas dos variables:

1. Los atacantes aceptan seguir las reglas que usted ha establecido con respecto a su herramienta de ciberseguridad de lista blanca de aplicaciones.
2. Su entorno es muy pequeño, con pocas aplicaciones que se mantienen bastante estables y sin exploits.

Inconvenientes de las tecnologías de lista blanca de aplicaciones

Complejidad

Las redes de TI son como organismos complejos

Incluso las redes de TI pequeñas son entidades en constante cambio, con una infinidad de comportamientos. Los usuarios agregan y eliminan aplicaciones de manera constante. Los módulos dentro de las aplicaciones son añadidos y eliminados constantemente por los creadores de los programas, especialmente durante las actualizaciones. Por último, los comportamientos de las aplicaciones, además de los cambios en el código que resultan en cambios de comportamiento, son utilizados de diferentes maneras por distintos usuarios en distintos momentos. Ahora imagine el equipo que tendría que encargarse de rastrear esto constantemente, y los tickets de la mesa de ayuda de TI que tendrían que llegar de forma continua.

En términos realistas, el único entorno de TI estable es aquel impulsado por quioscos, en los que los programas se instalan sin la posibilidad de actualizarse, añadirse o eliminarse, y a los usuarios se les permite realizar de forma restringida solo una o dos funciones. Tal vez un quiosco para impresión de fotos o algo similar. En ese caso, la lista blanca de aplicaciones solo necesitaría actualizarse cada vez que se actualice la terminal del quiosco, quizás dos veces al año.

Listas blancas de aplicaciones más avanzadas significan mayor complejidad

Las listas blancas de aplicaciones más simples simplemente contienen listas de programas cuya existencia está permitida en el sistema de un usuario.

Esto en sí mismo puede ser difícil de gestionar, pero da lugar a una variedad de posibles mejoras.

Por ejemplo, solo porque el departamento de nómina tiene una aplicación para interactuar con el sistema de pago de sueldos de la empresa, ¿no debería existir un conjunto de reglas separado para el equipo del almacén, que tiene aplicaciones diferentes (no relacionadas con nómina)?

Por lo tanto, las mejoras relacionadas con qué divisiones o usuarios pueden ejecutar qué aplicaciones son una mejora obvia. Una mejora que ahora ha creado complejidad adicional, además de simplemente rastrear el número, tipo y versiones de los programas en su red.

Ahora, supongamos que necesitamos otro conjunto de mejoras: necesitamos decidir qué usuario tiene acceso a qué aplicación, para qué conjunto de datos.

Eso también tiene todo el sentido, ¿verdad? Usted no quiere que su equipo de almacén tenga acceso a los registros de RR. HH., y es probable que el equipo de RR. HH. no necesite acceso a los datos operativos del equipo de entregas del almacén.

Ese es un conjunto de combinaciones ridículamente complejo de rastrear, ahora que las ubicaciones de los datos se han añadido como una variable.

Entonces, con cada mejora necesaria para que las tecnologías de lista blanca de aplicaciones sean eficaces, la gestión, configuración y el soporte continuo (podría decirse que interminable y siempre en aumento) necesario para mantenerla funcional hace que la tecnología resulte inutilizable. El resultado, normalmente, es que se otorga acceso a grandes grupos de usuarios sobre grandes grupos de aplicaciones, y probablemente a casi todos los datos. Es decir, una configuración casi inútil de la tecnología, porque ninguna empresa cuenta con los recursos para mantenerla adecuadamente gestionada.

Las aplicaciones interactúan entre sí

Es común en los sistemas operativos modernos que las aplicaciones interactúen con otras aplicaciones. A veces, la interacción se debe a una integración entre dos aplicaciones que mejora la experiencia del usuario, como cuando un documento de Word abre Microsoft Photos. En otras ocasiones (esto es muy común), existen llamadas entre programas que se realizan de una manera que suele ser invisible para el usuario final.

¿Qué es el listado blanco de aplicaciones (Application Whitelisting)?

Introducción

El listado blanco de aplicaciones, en el contexto de Cyber Crucible, consiste en otorgar a una aplicación permiso para realizar alguna acción que de otro modo podría considerarse sospechosa o maliciosa.

La tecnología de listado blanco de aplicaciones se encuentra típicamente en el arte defensivo del análisis de comportamiento, aunque algunos atacantes también la utilizan (no se cubre aquí) en sus operaciones.

Piénselo como en la escuela, donde a los estudiantes normalmente no se les permitía caminar por los pasillos durante la clase. Sin embargo, si una figura de autoridad les daba un “pase de pasillo” de alguna forma, los estudiantes no eran devueltos a su salón de clases ni enviados a la oficina del director.

Tipos de listado blanco de aplicaciones - una descripción no técnica

Si continuamos con la analogía del “pase de pasillo”, puede haber diferentes técnicas que los funcionarios de la administración escolar han aprendido, las cuales ayudaron a formalizar los comportamientos que algunos estudiantes (definitivamente no nuestro CEO Dennis) pudieron haber intentado hacer sin ser descubiertos. Todo esto tiene una correlación directa con las operaciones de seguridad.

El pase de pasillo obvio y engorroso (algo bueno)

21987331.jpg?width=278
¿Recuerda alguna vez haber recibido un pase de pasillo, o una llave de alguna habitación, que era increíblemente grande y evidente?

Había un par de buenas razones para eso:

1. Para que no se perdiera.
2. Para reducir el tiempo y la energía invertidos por parte de una figura de autoridad, en la verificación rápida de las actividades aprobadas del estudiante.

Un buen software no “perderá” una lista blanca, pero el software de listado blanco de aplicaciones debe permitir una validación rápida y eficiente en recursos de que la aplicación ha sido inspeccionada.

El pase de pasillo genérico (probablemente no es algo bueno)

Esto probablemente sea lo menos útil tanto para el monitoreo de aplicaciones como para las escuelas, pero requiere la menor gestión o experiencia.

En este caso, al estudiante se le permite hacer su diligencia en el pasillo. El profesor puede saberlo, por ejemplo, pero no hay validación por parte de los monitores de pasillo sobre lo que el estudiante está haciendo. Además, si hay un intento de validación, existen dos niveles de inversión considerable de recursos:

1. el nivel de esfuerzo para acercarse al estudiante e interrogarlo sobre sus comportamientos e intenciones
2. el nivel de esfuerzo para asegurarse de que el estudiante está siendo honesto, para validar la explicación del estudiante

Con las aplicaciones, esto se observa con mayor frecuencia cuando un programa se agrega a una lista blanca y no hay más validación de los comportamientos o actividades permitidas. Desafortunadamente, la capacidad de obtener contexto sobre los comportamientos de una aplicación típicamente no está disponible para su adquisición si no es rastreada externamente por algún otro marco de trabajo.

El pase de pasillo genéricamente específico

No confundir con, “¡adelante, Aplicación, haz lo que quieras!”

Volvamos al pase para el baño, porque es muy apropiado aquí. Dada la visibilidad del pase, es relativamente fácil evaluar qué debería estar haciendo el estudiante. Los comportamientos flagrantes fuera de lo esperado con “ir al baño” pueden evaluarse sin mucha dificultad.

El listado blanco de aplicaciones que tiene límites genéricos de actividades es el más común, aunque en muchos casos esos límites equivalen a permitir que un estudiante con un pase para el baño juegue en el patio de recreo.

El pase de pasillo específico-específico

¡No confundir con el pase de pasillo “genéricamente específico”!

22642689.jpg?width=340
Si bien, con el pase de pasillo genéricamente específico, sabemos que el estudiante está usando el baño, en una escuela grande no sabemos
1. Quién le dio permiso al estudiante

2. De dónde acaba de venir.

3. En qué baño pensaba la figura de autoridad cuando dio su aprobación.

4. Cuánto tiempo ha estado el estudiante “fuera y por ahí”.

Esto requirió más trabajo por parte del marco de autoridad de la escuela.

Volviendo al listado blanco de aplicaciones, el análisis de comportamiento es más preciso cuantas más variables se agreguen a cualquier capacidad de toma de decisiones.

Además, al investigar un pase de pasillo que ha sido emitido, normalmente no es necesario rastrear una cadena de 5 profesores para llegar a la fuente. También casi siempre se puede confiar en que el profesor no era algún tipo de “mal profesor” que les dice a los estudiantes que se comporten de manera inapropiada. El listado blanco de aplicaciones, en un ejemplo de lista blanca específica-específica, requiere trabajar hacia atrás, para examinar cada aplicación padre o ancestro que abrió la siguiente aplicación. Por ejemplo, una pieza de malware puede haber abierto una utilidad legítima de Windows.

Las siguientes preguntas son aproximadamente equivalentes al “pase de pasillo estudiantil” mencionado anteriormente:

1. ¿Para qué se inició la aplicación, o qué se le indicó que hiciera? Necesitamos conocer el comportamiento previsto.
2. ¿Quién inició la aplicación? Esto típicamente es otro programa.
3. ¿Qué programas “padre” o “ancestro” resultaron en la apertura de este programa? ¿Qué estaba haciendo cada uno de ellos, o qué pretendía hacer?

La aplicación comprometida

Recuerde en varias obras de ciencia ficción, o literatura y películas de terror, cuando un impostor de alguna manera ha tomado

22413315.jpg?width=226
el control del comportamiento de un personaje? En las escuelas, no hay muchas posibilidades de que un instructor sea poseído por alienígenas.

La toma de control de aplicaciones es una técnica favorita de los atacantes porque, al igual que en las películas, la mayoría de los observadores no notan nada extraño hasta que es demasiado tarde.

En este caso, un atacante toma un programa en ejecución, que actualmente está cargado en memoria. Así, el programa completamente intacto en el sistema de archivos es ignorado. El programa en memoria se edita para agregar el código del atacante. Muy parecido a un alienígena dentro del cuerpo de un humano. El atacante realiza sus comportamientos delictivos, y cuando el programa termina de ejecutarse, la mayor parte de la evidencia desaparece. Cuando el programa legítimo se ejecuta nuevamente, si el atacante no edita el código otra vez, es tal como los codificadores legítimos originales lo pretendían. ¿Tal vez una mejor analogía, en ese caso, sería un hombre lobo?

Un listado blanco de aplicaciones, entonces, necesita trabajo adicional para garantizar que el programa, y cualquier ancestro o programa padre, estén intactos sin que un hacker edite los programas mientras se están ejecutando.

En resumen - Preguntas que hacer al investigar una capacidad de listado blanco de aplicaciones

Asegúrese de comprender los límites que permite una lista blanca al discutir el listado blanco de aplicaciones con su equipo de tecnología o proveedor.

1. ¿Esta capacidad examina y rastrea lo que se supone que un programa debe hacer, y compara los comportamientos esperados frente a los observados?
2. ¿Cuánto detalle captura la capacidad de listado blanco en su toma de decisiones? ¿Más o menos que un pase de pasillo estudiantil detallado?
3. ¿La capacidad de listado blanco rastrea e investiga los programas padre y ancestro en busca de comportamiento malicioso? (El Programa A abre B, abre C, abre D – muy común)
4. ¿La capacidad de listado blanco valida que el programa en ejecución no haya sido manipulado?

Lectura profunda del Instituto Nacional de Estándares y Tecnología (NIST)

Una publicación autorizada que no es para una lectura casual, pero que es muy descriptiva.

Aunque no cubre todos los escenarios, y los detalles no se actualizan con la frecuencia suficiente para mantenerse al día con cada escenario, las descripciones son lo suficientemente estratégicas como para ser valiosas en la mayoría de las circunstancias.

El equipo de Cyber Crucible siempre valora las ideas de las publicaciones del NIST, y dedica tiempo en consecuencia.

https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-167.pdf

¿Cómo Puedo Saber Qué se Habría Suspendido de no ser por el Comportamiento Personalizado?

Los usuarios pueden ver qué respuestas de extorsión se habrían suspendido si no existiera un comportamiento personalizado, dirigiéndose primero a la página de Respuestas de Extorsión, ubicada en la pestaña Operations de la barra lateral.

La columna Excluded muestra si una respuesta de extorsión ha sido excluida o no, y el filtro de columna predeterminado muestra las respuestas no excluidas y no silenciosas.

ExcludedColumn.png
Para mostrar las respuestas excluidas, abra el filtro de la columna Excluded y seleccione únicamente Excluded.

ExcludedFilter.png
Después de hacer clic en Apply, la cuadrícula mostrará las respuestas de extorsión excluidas que se habrían suspendido si el comportamiento personalizado no existiera.

Para ver qué comportamiento personalizado se aplicó a una respuesta, primero haga clic en la flecha de la columna Number of Incidents correspondiente a la fila específica. En la cuadrícula interna que se revela al hacer clic en la flecha, la columna Hiding Rule mostrará el nombre del comportamiento personalizado que se aplicó a la respuesta.

ExcludedResponses.png

Cómo administrar comportamientos personalizados

La página de Comportamientos Personalizados se encuentra en la pestaña Operaciones en la barra lateral. Tenga en cuenta que los usuarios deben tener el permiso “Ver Comportamientos Personalizados” para un grupo a fin de poder ver los comportamientos personalizados de ese grupo en esta página

Cómo crear un comportamiento personalizado

Después de navegar a la página de Comportamientos Personalizados, haga clic en el ícono de excluir proceso encima de esta cuadrícula.

Al hacer clic en este ícono se abrirá una ventana emergente para crear el comportamiento personalizado.

CreateTailoredBehaviorIcon.png
Create Exclusion.png

Los usuarios tienen la opción de especificar un programa principal con la excepción

94732291.png?width=504
Ingrese restricciones adicionales para aplicar

CreateTailoredBehaviorAdditionalRestrictions.png

Ahora los usuarios tienen la opción de limitar la excepción a activadores de acceso a archivos específicos; todos los activadores de acceso a archivos se incluyen de forma predeterminada. Tenga en cuenta que solo los agentes en la versión 4.4.6.2 o superior tienen esta capacidad de activador de acceso a archivos.

Los usuarios también tienen la capacidad de crear comportamientos temporales, vea más en la siguiente sección

Cómo crear y editar comportamientos personalizados temporales

Los usuarios pueden crear un comportamiento personalizado temporal siguiendo el proceso normal para crear un comportamiento como se explicó anteriormente, y luego activando el interruptor “Hacer Este Comportamiento Personalizado Temporal”. Los usuarios pueden entonces ingresar las horas hasta que el comportamiento temporal deba expirar (hasta un máximo de una semana).

Temporary Exclusion.png
La fecha de expiración del comportamiento se puede ver en la columna Fecha de Expiración de la cuadrícula.

Para editar un comportamiento temporal y extender la fecha de expiración, hacer que un comportamiento temporal sea permanente, o hacer que un comportamiento permanente sea temporal, haga clic en el ícono de editar en el comportamiento deseado en la columna Fecha de Expiración.

Edit Temp Behavior Icon.png

Al hacer clic en este ícono se abrirá una ventana emergente donde los usuarios pueden editar la fecha de expiración del comportamiento como lo deseen

Edit behavior modal.pngScreenshot from 2024-09-09 15-21-58.png

Cómo eliminar comportamientos personalizados

Para eliminar un comportamiento, o varios comportamientos al mismo tiempo, primero seleccione el(los) comportamiento(s) a eliminar en la cuadrícula y haga clic en el ícono de papelera encima de

la cuadrícula.

Segundo, escriba “delete” y haga clic en el botón Eliminar.

RemoveTailoredBehaviorIcon.pngRemoveTailoredBehaviorModal.png

Cómo copiar comportamientos personalizados a un grupo diferente

Para copiar un comportamiento (o varios comportamientos al mismo tiempo) a otro grupo, seleccione el(los) comportamiento(s) a copiar en la cuadrícula y haga clic en el ícono de copiar encima de la cuadrícula.

Al hacer clic en este ícono se abrirá una ventana emergente donde puede seleccionar el grupo al que se deben copiar el(los) comportamiento(s).

Esta ventana emergente también tiene una opción para eliminar los comportamientos existentes en el grupo seleccionado (excepto los comportamientos generados automáticamente), y contener solo los comportamientos copiados en el grupo seleccionado después de enviar la solicitud.

CopyTailoredBehaviorIcon.pngCopyTailoredBehaviorModal.png
Después de enviar la solicitud, los comportamientos copiados ahora aparecerán para el grupo seleccionado.

ResultGrid.png

Creación de un comportamiento personalizado desde la página de Respuesta a la Extorsión

Los usuarios tienen la capacidad de crear comportamientos personalizados desde la página de Respuestas a la Extorsión.

Primero, haga clic en la flecha en la fila de respuesta a la extorsión deseada en la columna Número de Incidentes para revelar la cuadrícula interna.

Segundo, haga clic en el ícono de excluir respuesta en la columna Nombre de la Respuesta, lo cual abrirá una ventana emergente para crear el comportamiento personalizado.

ExcludeResponseIcon.png
En esta ventana emergente, puede crear comportamientos usando las rutas de ejecutables sugeridas o enviar la respuesta para revisión si no encuentra lo que necesita entre las rutas sugeridas.

Exclude Modal.png

También puede hacer clic en el botón Llévame a la Página de Comportamientos Personalizados, lo cual lo redirigirá a la página de Comportamientos Personalizados y prellenará automáticamente la ventana emergente de creación de comportamiento con el mismo grupo, ruta y argumentos del programa provenientes de la respuesta.

AutofilledModal.png

Tenga en cuenta que, de forma predeterminada, la opción Limitar Excepción a Programa + Programa Principal está desactivada. La ruta y los argumentos del programa principal de la respuesta a la extorsión también se completarán automáticamente si activa esta configuración.

PrefilledArgs.png

La Exclusión de Comportamiento Personalizado después de hacer clic en Crear con la configuración Limitar Excepción a Programa + Programa Principal activada:

ExlusionResult.png

¿Qué es un ataque sin archivos (en memoria)?

Respuesta breve: Un ataque sin archivos es aquel que nunca escribe un programa en el disco. El atacante inyecta código malicioso directamente en la memoria de un proceso legítimo y de confianza, y construye allí su carga útil (payload). Como nunca se crea ningún archivo, las herramientas de seguridad que analizan archivos —incluida la mayoría de EDR— no tienen nada que encontrar.

Por qué derrota a las herramientas basadas en archivos

La protección tradicional de endpoints se construye sobre una suposición simple: el malware es un archivo, así que hay que inspeccionar archivos. Las técnicas sin archivos eliminan por completo el archivo.

En una implementación real, una empresa de servicios financieros utilizaba tres productos EDR líderes en la industria (Microsoft, CrowdStrike y Sophos) junto con un SOC gestionado del Top 50. Los atacantes comprometieron una herramienta de monitoreo remoto de confianza, inyectaron código en los procesos de administración de Microsoft SQL Server y compilaron su ransomware y malware de robo de datos directamente en la memoria del servidor. Como nada tocó el disco duro, los tres EDR, el MDR y el SOC quedaron completamente ciegos. Cyber Crucible interceptó de forma autónoma casi 10,000 procesos maliciosos —el 98% de ellos en la granja de servidores SQL— sin una sola alerta de la pila de herramientas heredada.

Cómo lo ve Cyber Crucible

Cyber Crucible observa el comportamiento y la intención a nivel del kernel en lugar de analizar archivos. Un proceso que actúa de manera maliciosa se detiene en menos de 200 milisegundos, se haya escrito un archivo o no.

¿Qué es la automatización de hackers y por qué anula las defensas tradicionales?

Respuesta breve: la automatización de hackers es el uso de scripts, IA y automatización robótica de procesos para ejecutar todas las etapas de un ataque a velocidad de máquina. Un ataque automatizado puede infiltrarse en una máquina, robar datos y eliminar sus propias herramientas en memoria en segundos, mucho más rápido de lo que cualquier analista humano puede responder.

Qué se automatiza

- **Reconocimiento:** las herramientas escanean internet en busca de sistemas vulnerables y mapean una red objetivo en segundos, además de generar phishing convincente a gran escala.
- **Explotación:** una vez detectada una debilidad, los frameworks despliegan el exploit de inmediato; una vulnerabilidad de día cero puede utilizarse en millones de máquinas antes de que un humano registre la alerta.
- **"Golpe y fuga":** el malware moderno no evalúa qué archivos son valiosos. Cifra o exfiltra todo lo que puede alcanzar, tan rápido como puede alcanzarlo.

Por qué los humanos no pueden ganar esta carrera

El límite no es la calidad del equipo ni la dotación de personal. Es la biología. El tiempo que necesita una persona para ver una alerta, procesarla y actuar es mayor que el que tarda el ataque en completarse. Enviar la telemetría a un servidor en la nube para su análisis y de vuelta añade aún más demora.

La única respuesta viable es una defensa que decida y actúe de forma autónoma, en el endpoint, en milisegundos.

¿Por qué los ataques automatizados apuntan a las mismas ubicaciones en cada computadora?

Respuesta breve: los atacantes no saben nada sobre su entorno específico, por lo que su automatización está escrita contra ubicaciones que existen prácticamente en todas las máquinas: carpetas de perfiles de usuario, letras de unidad y directorios de datos de aplicaciones. Esa previsibilidad es una debilidad que los defensores pueden aprovechar.

Los objetivos predecibles

- **Perfiles de usuario y escritorios:** en Windows, `C:\Users\[Username]` contiene de manera confiable datos valiosos. Un script recorre cada directorio de usuario sin necesidad de comprender el sistema.
- **Letras de unidad:** las herramientas automatizadas enumeran `C:\`, `D:\` y más allá para encontrar recursos compartidos de red, unidades externas y particiones montadas para cifrar.
- **Carpetas de datos de aplicaciones:** cada sistema operativo guarda credenciales, cookies y configuraciones en rutas conocidas, objetivos principales para el robo de credenciales.

Convertir la previsibilidad en contra del atacante

El patrón de ataque no es reflexivo; es un barrido contundente de ubicaciones bien conocidas. Cyber Crucible monitorea exactamente esos puntos de entrada conocidos de robo de identidad y robo de datos. Cualquier programa que acceda a datos en esas ubicaciones —junto con sus procesos principales y secundarios y las bibliotecas asociadas— tiene su intención evaluada en una fracción de segundo, y es interceptado si esa intención es maliciosa.

¿Qué es un infostealer y por qué el robo de tokens de sesión es tan peligroso?

Respuesta breve: Un infostealer es un malware diseñado para capturar material de identidad digital —contraseñas, tokens de sesión, claves de API y credenciales VPN— y exfiltrarlo rápidamente. Un token de sesión robado es peligroso porque a menudo evita por completo las contraseñas y la autenticación multifactor, permitiendo que un atacante inicie sesión como un usuario legítimo.

Por qué los atacantes ahora roban la identidad en lugar de permanecer residentes

Los atacantes modernos evitan cada vez más quedarse dentro de una red. Permanecer en el entorno aumenta las probabilidades de detección. En su lugar, toman el material de identidad y se marchan, lo que les otorga dos ventajas:

1. **Menor riesgo** — analizan lo que robaron desde un entorno seguro a su propio ritmo.
2. **Regreso sencillo** — con un token de sesión, contraseña o clave VPN válidos, pueden volver cuando quieran, apareciendo como completamente legítimos ante el sistema de autenticación.

Por qué la velocidad es todo el problema

Estas herramientas pasan de la infiltración a la autoeliminación en segundos —más rápido de lo que tarda una alerta en la nube en salir del edificio. Cyber Crucible interpreta la intención en el momento del acceso a los datos de identidad y suspende el proceso en menos de 200 milisegundos, antes de que comience la exfiltración.

¿Qué son los ataques de tipo Living-off-the-Land (LotL) y por qué falla la lista blanca de aplicaciones contra ellos?

Respuesta breve: Los ataques Living-off-the-Land utilizan software que ya está instalado y que ya es de confianza —utilidades del sistema, herramientas administrativas, navegadores— en lugar de introducir nuevos archivos maliciosos. La lista blanca de aplicaciones falla porque el atacante opera dentro de programas que la lista blanca permite explícitamente.

La lista blanca se convierte en una lista de objetivos

La lista blanca de aplicaciones responde a una sola pregunta: "¿está permitido ejecutar este archivo?" Las técnicas modernas de ataque hacen que esa pregunta sea irrelevante. Si los atacantes ocultan código malicioso dentro de la memoria de un proceso aprobado, la lista blanca ya ha dicho que sí. En la práctica, una lista blanca le indica a un atacante con precisión en qué procesos es más seguro esconderse.

La mejor pregunta

Una defensa eficaz debe pasar de "*¿está permitido este archivo?*" a "*¿qué está haciendo realmente este código en este momento?*" Esto requiere inspeccionar el comportamiento y la memoria a nivel del kernel, donde la actividad real es visible, y no a nivel de archivo, que el atacante ya ha eludido.

¿Qué es un ataque en memoria a una DLL de System32?

Respuesta breve: Es un ataque que infecta las bibliotecas de código central de Windows (DLL de System32) mientras se están ejecutando en memoria. Dado que casi todas las aplicaciones y herramientas de seguridad dependen de esas bibliotecas para funcionar, comprometerlas otorga al atacante un control casi total del endpoint con muy poco rastro.

Por qué esto representa la cúspide del oficio ofensivo en endpoints

Las DLL de System32 proporcionan las operaciones fundamentales de las que dependen Windows y sus aplicaciones: asignación de memoria, criptografía, redes. Fueron diseñadas para ofrecer velocidad y fiabilidad, nunca para ser parcheadas o interceptadas ("hooked") sobre la marcha en producción.

Un atacante capaz de alterarlas en memoria obtiene el poder de inspeccionar, crear, modificar o destruir datos y programas en el sistema, con un sigilo prácticamente imposible de rastrear.

Por qué la mayoría de las herramientas no pueden detectarlo

Los productos de seguridad que dependen de datos de sensores proporcionados por Microsoft están, por definición, apoyándose en las mismas bibliotecas que están siendo atacadas. Los sensores necesarios para detectar esta clase de ataque simplemente no existen en los conjuntos de herramientas estándar, por lo que la herramienta guarda silencio mientras informa que todo está en orden.

Cyber Crucible fue diseñado deliberadamente para ser independiente de las bibliotecas de Windows, de modo que un sistema operativo comprometido no pueda cegarlo ni deshabilitarlo.

¿Por qué el malware no siempre se activa en un laboratorio de pruebas de seguridad?

Respuesta breve: los atacantes diseñan el malware para que permanezca inactivo a menos que reciba una señal de validación de un servidor de comando y control (C2) en vivo que ellos controlan. Para cuando una muestra llega a una base de datos de malware, la infraestructura de C2 normalmente ya se ha movido, por lo que los investigadores a menudo están probando una muestra huérfana que no hace nada.

Por qué los atacantes incorporan la inactividad

- **Minimizar la inteligencia:** el malware inactivo no realiza ninguna acción maliciosa observable, lo que deja a los analistas con menos elementos para documentar y a los proveedores con menos base para crear firmas.
- **Prevenir el secuestro:** exigir un saludo secreto garantiza que un rival o investigador que se apodere del servidor C2 no pueda simplemente activar el malware y recolectar los datos robados.

Qué implica esto para la evaluación de herramientas de seguridad

Una prueba de laboratorio contra una muestra desconectada mide muy poco. La pregunta relevante no es si una herramienta reacciona ante malware inactivo que permanece inerte, sino si detiene ataques en vivo y de rápido movimiento a medida que ocurren. Cyber Crucible está diseñado para esto último: monitorea los puntos de entrada de robo de identidad y de datos que los ataques reales atacan, evalúa la intención en menos de 200 milisegundos y detiene el robo antes de que tenga éxito.