INFORME SOBRE CIBERAMENAZAS: RECONOCIMIENTO 2.0

Los atacantes han desarrollado un arsenal de técnicas y herramientas para penetrar en las redes de las organizaciones y robar información valiosa. Este informe revela las últimas tácticas que usan los atacantes para no ser descubiertos mientras realizan actividades de reconocimiento interno. También explica cómo la automatización ha permitido a los hackers más novatos llevar a cabo actividades de reconocimiento avanzado y acelerar sus ataques.

Atacantes en Búsqueda de Datos Valiosos

Los ataques dirigidos suelen comenzar por los puntos más débiles en las defensas de las organizaciones: sus endpoints. El paso inicial de un ataque dirigido puede ser tan simple como convencer a un usuario de abrir un adjunto en un correo electrónico. Con el 4 % de los usuarios que caen en la trampa de cualquier campaña de phishing[1] y con atacantes capaces de enviar una cantidad infinita de correos electrónicos de phishing y de ejecutar un sinnúmero de otros ataques (desde exploits de día cero hasta ataques de ingeniería social), las intrusiones golpean incluso a las organizaciones con las defensas más fortalecidas.

Cuando los atacantes comprometen un endpoint, deben establecer un canal de comunicación con un servidor de comando y control (C2). Luego, comienzan a explorar el entorno en busca de recursos valiosos. Durante esta etapa de reconocimiento interno, es posible que sigan caminos que los conduzcan a callejones sin salida, pero continuarán intentando nuevas rutas hasta lograr su objetivo.

Para evitar ser detectados, los atacantes actualizan constantemente sus herramientas y métodos. Aprovechan técnicas nuevas para determinar la disposición del terreno y ubicar los recursos clave como, por ejemplo, servidores Active Directory®, servidores de archivos y bases de datos.

Durante años, los atacantes han utilizado una combinación de escáneres de puertos, malware, herramientas de hackeo y de prueba y error para trazar mapas de las redes objetivo y expandir su campo de acceso una vez que se introdujeron en una red. Hoy en día, muchos atacantes han ampliado su repertorio de técnicas de reconocimiento interno para incluir aquellas que se muestran en la Figura 1.

Figura 1: Algunas técnicas de reconocimiento interno

Estas técnicas de reconocimiento interno permiten, a los atacantes, encubrir sus actividades y acelerar sus ataques. Entonces, ¿cómo trabajan? O, lo que es más importante, ¿podemos detectar y detener estos ataques antes de que se produzca algún daño? Creemos que la respuesta es un "sí" rotundo.

Ataques Sin Archivo

Dado que las tecnologías de seguridad mejoran su capacidad de detectar malware, los atacantes recurren a ataques sin archivo para comprometer endpoints y realizar tareas de reconocimiento interno sin generar sospechas. Las técnicas de ataque sin archivo incluyen lo siguiente:

- Malware de solo memoria (memory-only)
- Malware y herramientas basados en scripts
- Código malicioso incorporado en archivos benignos

Los atacantes realizan ataques sin archivo porque es mucho más probable que resulten exitosos de esta forma que con malware tradicional basado en archivos. De hecho, según una encuesta reciente, el 77 % de los ataques exitosos fueron gracias a ataques sin archivo o exploits, mientras que solo el 23 % de las veces que se comprometió la seguridad fue por ataques basados en archivos.[2]

Los ataques sin archivo pueden eludir los controles de seguridad porque el software antivirus tradicional fue diseñado para analizar archivos y buscar atributos o funciones de archivos a fin de determinar si son maliciosos. Sin embargo, en un ataque sin archivo, no hay archivos tradicionales que los antivirus puedan escanear o analizar; esto permite a los atacantes evadir la detección estática basada en discos.

El 77 % de los ataques exitosos fueron ataques sin archivo o exploits.

Los atacantes pueden empezar con un exploit distribuido por la web o por tráfico de correo electrónico, como un archivo malicioso de Adobe® Flash®, una macro en una hoja de cálculo o, incluso, una cadena JavaScript especialmente desarrollada que aprovecha la vulnerabilidad de un endpoint para ejecutar un código malicioso.

1. "2018 Data Breach Investigations Report", Verizon, marzo de 2018, https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_execsummary_en_xg.pdf.
2. "The 2017 State of Endpoint Security Risk Report", Ponemon Institute, octubre de 2017, https://www.barkly.com/ponemon-2018-endpoint-security-statistics-trends#form.

Los atacantes pueden forzar así las herramientas integradas de Windows®, como PowerShell® y Windows Management Instrumentation, o usar otras herramientas, como Metasploit®, para transferir malware desde una ubicación remota y cargarlo en la memoria. El contenido del malware nunca se escribe en el disco, sino que se ubica en las áreas volátiles del sistema como, por ejemplo, en los procesos dentro de la memoria o en las áreas de servicio. El malware de solo memoria (memory-only) es especialmente efectivo en aquellos servidores y dispositivos de red que no se reinician de manera frecuente.

Los atacantes también usan malware basado en scripts, usualmente en conjunto con malware de solo memoria (memory-only), para ejecutar comandos en equipos objetivo de ataques. Dado que los scripts son archivos de texto no estructurado, no es fácil para las herramientas de seguridad usar firmas de los ataques para detectarlos. Los atacantes pueden modificar fácilmente los parámetros, los nombres o el orden de los códigos de scripts para frustrar la detección de firmas.

*El **30%** de todos los ataques de 2017 fueron sin archivo. En 2019, se espera que lleguen al **38%**.*

Por último, los atacantes pueden incorporar código malicioso en archivos conocidos, en especial aplicaciones de código abierto o libre que no tienen firma digital. Incluso pueden inyectar código en procesos en ejecución. Si las herramientas antivirus llegan a detectar funciones maliciosas en estos archivos legítimos, los analistas de seguridad tienden a asumir que las alertas corresponden a falsos positivos para concentrarse en otras amenazas aparentemente de mayor prioridad. Una vez que los atacantes comprometieron un endpoint con un ataque sin archivo, pueden atravesar la red para buscar y exfiltrar datos.

Los kits de exploits y los marcos de trabajo (frameworks) preempacados han hecho que los ataques sin archivo sean más fáciles de implementar que nunca y sean más comunes en el actual escenario de amenazas. De todos los ataques en 2017, 30 % fueron sin archivo, y se espera que este número aumente a 38 % en 2019.[3]

Vivir de la Tierra

Una vez que los atacantes llevan a cabo un exploit en un endpoint (generalmente con un ataque sin archivo), intentan localizar, robar, manipular o destruir datos. En lugar de llamar la atención al instalar malware o herramientas de ataque, los atacantes sigilosos utilizan las aplicaciones ya existentes en los equipos de sus víctimas para llevar a cabo actividades de reconocimiento. Estas aplicaciones son de confianza y se utilizan en actividades diarias legítimas, por lo que los atacantes pueden usarlas en múltiples etapas del ciclo de vida del ataque, incluso en el reconocimiento interno, sin ser detectados.

Vivir de la tierra también consiste en abusar de los servicios conocidos, como GitHub®, Pastebin, Twitter®, Box o incluso Microsoft Office 365®. Los atacantes utilizan estos servicios para encontrar datos confidenciales cuando se comparten archivos en línea y en aplicaciones de correo electrónico. También usan estos servicios para actividades C2, así como para exfiltración de datos.

Para sondear la red, los atacantes astutos se aprovechan de aplicaciones de red como Ping, NetStat y IpConfig, así como de herramientas de escritorio remoto y servicios de administración. Para los atacantes, comprometer los equipos de los administradores de TI significa llevarse el premio gordo para "vivir de la Tierra" y, por lo general, son capaces de tomar posesión de múltiples aplicaciones (y credenciales) que puedan ayudarlos a lograr sus turbios objetivos.

Los equipos de seguridad no pueden desinstalar todas estas aplicaciones fácilmente. Los riesgos de seguridad se potencian dado que los atacantes que viven de la tierra generalmente logran eludir el software antivirus tradicional y las herramientas de listas blancas de aplicaciones porque no instalaron archivos nuevos en el sistema. Como consecuencia, no hay firmas que las herramientas antivirus puedan detectar y son pocas las huellas de sus actividades que se pueden usar para análisis forense.

Violación de los Sistemas de Respaldo

Muchas organizaciones invierten cantidades extraordinarias de recursos en proteger sus aplicaciones confidenciales. Implementan firewalls, robustos procesos de autenticación, prevención de amenazas, protección de endpoints y más para proteger sus aplicaciones y sus datos. Sin embargo, estas organizaciones conscientes de la seguridad típicamente no extienden sus mejores prácticas de seguridad cibernética a los servidores de respaldo. Suelen considerar que la protección de contraseñas y los parches regulares son suficientes como controles de seguridad. Como resultado, los servidores de respaldo pueden proporcionar auténticos tesoros de datos de fácil acceso a los hackers inescrupulosos.

A modo de ejemplo, "Phineas Fisher", el autoproclamado hacker de HackingTeam, la compañía de TI ubicada en Milán, informó que ha utilizado servidores de respaldo para obtener acceso a varias máquinas virtuales, incluso el servidor de Mail Exchange

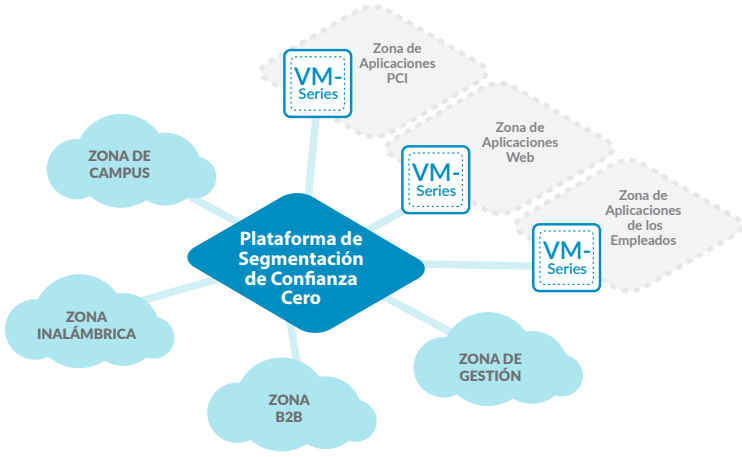

Figura 2: Modelo de Confianza Cero

3. "The 2018 State of Endpoint Security Risk Report", Ponemon Institute, consultado en febrero de 2019, https://www.barkly.com/ponemon-2018-endpoint-security-risk-report.

de la compañía. En su guía "Hack Back!", Fisher afirmó que "sus inseguros sistemas de respaldo fueron la vulnerabilidad que abrió sus puertas". El ataque a HackingTeam no fue el primero en explotar los sistemas de respaldo, pero sí creó consciencia entre la comunidad "black hat", sobre el uso de los sistemas y servicios de respaldo para ubicar y robar datos.

Como los servidores de respaldo contienen versiones anteriores de los datos activos, deben estar protegidos con el mismo nivel de seguridad que los servidores y las aplicaciones activos. Las organizaciones deben implementar el modelo de Confianza Cero, con segmentación de red y políticas minuciosas de firewall que limiten el acceso a usuarios autorizados. También deben implementar autenticación de múltiples factores para evitar que los atacantes accedan a los datos de respaldo con credenciales robadas. Por último, las organizaciones deben monitorear el acceso a los datos de respaldo para detectar actividades inusuales como usuarios que descarguen un gran volumen de datos o que descarguen datos sin subir o sincronizar ningún dato.

Automatización

En el pasado, solo los cibercriminales más sofisticados y los atacantes patrocinados por el estado podían llevar a cabo ataques dirigidos. Ahora, incluso el hacker más novato puede ejecutar ataques por múltiples etapas al utilizar una combinación de herramientas de ataque, scripts e información compartida. La automatización también permite que los atacantes realicen tareas de reconocimiento más rápido que nunca.

Las herramientas de pruebas de penetración, como Metasploit y PowerShell Empire, simplificaron los ataques dirigidos. Si bien estas herramientas no son precisamente nuevas (Metasploit se presentó por primera vez en 2003), con el tiempo han sumado nuevas funciones para explotar sistemas, descubrir vulnerabilidades nuevas y asistir a los hackers "white hat" (de sombrero blanco) o "black hat" (de sombrero negro) a través de cada etapa de un ataque. Dado que muchas de estas herramientas son impulsadas por comunidades activas en línea, se optimizan continuamente para incluir nuevas funciones y exploits.

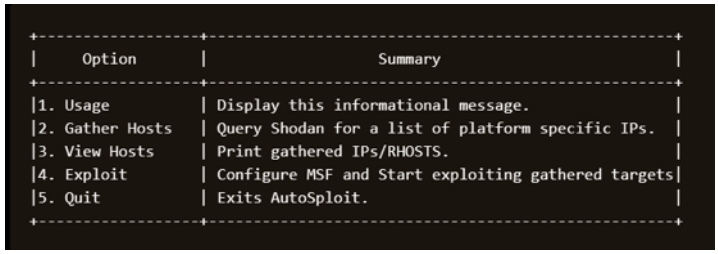

Figura 3: AutoSploit simplifica las actividades de reconocimiento y de explotación del sistema

Más recientemente, los desarrolladores han añadido interfaces gráficas y recomendaciones de exploits para sus herramientas, facilitando más que nunca las pruebas de penetración ("pen" testing) y el hackeo. Los desarrolladores también incluyeron scripts integrados que permiten que incluso los hackers o penetradores más novatos puedan ejecutar sus ataques. Por ejemplo, AutoSploit, presentado a comienzos de 2018, automatiza muchos de los pasos manuales de un ataque y permite prácticamente que cualquier atacante pueda ejecutar un asalto en múltiples etapas. AutoSploit combina Metasploit y Shodan®, un motor de búsqueda para dispositivos conectados a Internet, y permite a los atacantes localizar y explotar sistemas como los de dispositivos IoT inseguros.

Aunque los expertos en guerra cibernética puedan preferir los ataques manuales más sigilosos, la automatización de los ataques pone a los ataques avanzados al alcance de los hackers menos sofisticados. También permite, a los atacantes, detectar y explotar las vulnerabilidades apenas anunciadas muy rápidamente , lo que fuerza que las organizaciones apliquen parches a sus sistemas a la misma velocidad. Como los hackers utilizan cada vez más procesos automatizados, los equipos de seguridad deben fortificar sus defensas y automatizar las detecciones para adelantarse a los ataques.

Proteger su Organización contra Actividades de Reconocimiento

La actividad de reconocimiento interno de la red es un componente clave de la mayoría de los ataques dirigidos, pero también es cuando los atacantes quedan más expuestos. Para los atacantes, la intrusión inicial generalmente es solo el primer paso. Una vez que penetraron una red, deben tomar miles de acciones puntuales al explorar la red y moverse de forma lateral hasta acceder a los datos a los que apuntan. Si los defensores pueden recopilar y analizar aquellas señales como las que emiten los atacantes universales, podrán anticiparse a ellos.

Creemos que, con la tecnología correcta, los equipos de seguridad pueden evitar ciberataques exitosos. Al generar automáticamente perfiles de comportamiento de usuarios y dispositivos, los equipos de seguridad pueden detectar el comportamiento inusual que indica la presencia de una actividad de reconocimiento interno y de las demás etapas de un ataque dirigido. Con solo detectar una de las muchas acciones de los atacantes, los equipos de seguridad pueden identificarlos, expulsarlos fuera de la red e interrumpir el ataque.

Figura 4: Palo Alto Networks evita amenazas a través de todo el ciclo de vida del ataque

Proteger Su Organización con Cortex XDR

Cortex XDR™ es una aplicación de detección y respuesta basada en la nube que lo empodera para detener ataques sofisticados y adaptar las defensas para evitar futuras amenazas. Cortex XDR descubre amenazas con precisión al analizar los datos de sus redes, endpoints y nubes con aprendizaje automático. Brinda un panorama completo de cada incidente y revela causa raíz para acelerar las investigaciones. Una sólida integración con puntos de cumplimiento acelera la contención al permitirle detener los ataques antes de sufrir daños.

Cortex XDR detecta las actividades de reconocimiento interno, incluso cuando los atacantes no utilizan malware, porque identifica los cambios de comportamiento en la red. Como resultado, Cortex XDR puede atrapar a los atacantes que "viven de la tierra", que abusan de los sistemas de respaldo o que llevan a cabo actividades de reconocimiento automático. Cortex XDR también puede detectar a los atacantes que ejecutan ataques sin archivo y scripts para trasladarse de un host a otro dentro de la red.

Cortex XDR integra datos de redes, endpoints y nubes para generar el panorama completo de cada incidente. Al combinar los datos de tráfico de firewalls de nueva generación y endpoints provenientes de Traps™, la solución de protección de endpoints y respuesta, Cortex XDR puede determinar la causa raíz de los ataques. Este análisis integrado de endpoints ayuda a los analistas de seguridad a identificar qué aplicaciones o herramientas, como PowerShell o WMI, se utilizaron para los ataques en la red. Cortex XDR también puede analizar dispositivos corporativos en búsqueda de procesos extraños. Si Cortex XDR detecta herramientas de hackeo en un host, los equipos de seguridad pueden investigar más en profundidad para determinar si se ha comprometido el host.

Cortex es la única plataforma abierta de la industria que ofrece seguridad continua basada en Artificial Intelligence (Inteligencia artificial – IA). Proporciona una simplicidad incomparable para las operaciones de seguridad y mejora significativamente los resultados de seguridad mediante automatizaciones y una precisión nunca antes vista.

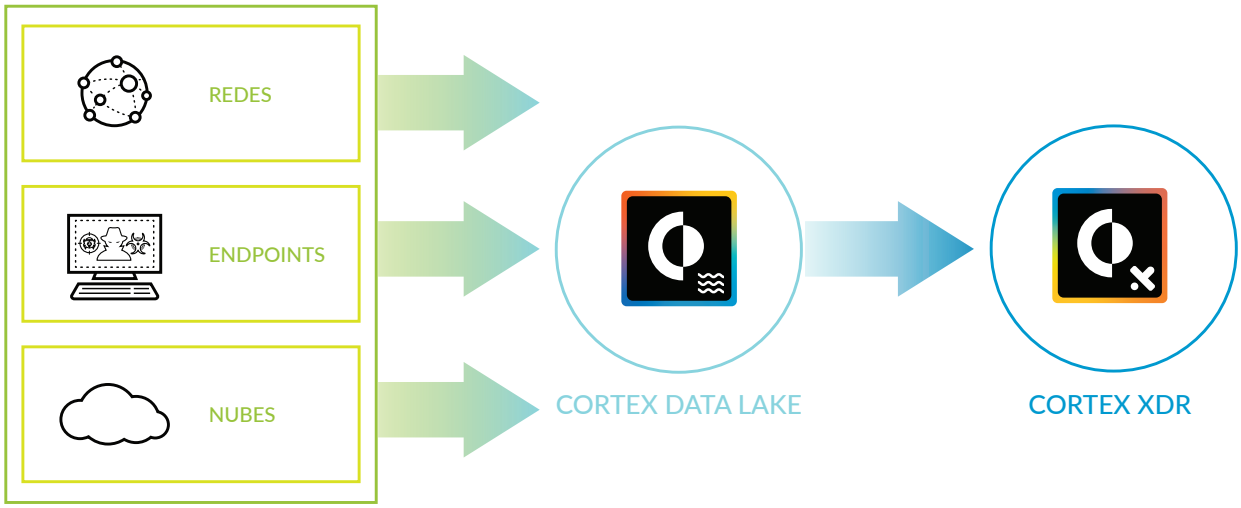

Figura 5: Cortex XDR acaba con la fragmentación al integrar datos de endpoints, redes y nubes

Anticiparse a los Atacantes

Los métodos de ciberataque cambian constantemente. Es solo cuestión de tiempo para que los atacantes encuentren nuevas formas para acelerar sus ataques y esconder sus actividades de las herramientas de seguridad. Las técnicas de reconocimiento actuales (como "vivir de la tierra", ataques sin archivo, violaciones de los sistemas de respaldo y la automatización) son peligrosas, pero los atacantes las reemplazarán eventualmente por nuevos métodos de ataque. De todas maneras, ellos aún van a necesitar recopilar información sobre sus entornos antes de poder localizar y robar datos. Al generar perfiles de comportamiento en la red de usuarios y dispositivos, los equipos de seguridad pueden detectar las actividades de reconocimiento interno incluso si los atacantes cambian sus herramientas y técnicas en el futuro.

3000 Tannery Way
Santa Clara, CA 95054

Línea principal: +1.408.753.4000
Ventas: +1.866.320.4788
Soporte técnico: +1.866.898.9087

www.paloaltonetworks.com

cyberthreat report-reconnaissance2.0-wp-022219