FORCEPOINT
POWERED BY Raytheon

Whitepaper

Tiempo de permanencia y movimiento lateral de los ataques cibernéticos

EL NUEVO PLAN DE SEGURIDAD CIBERNÉTICA

POR JOSHUA C. DOUGLAS, CTO, FORCEPOINT™

Contenido

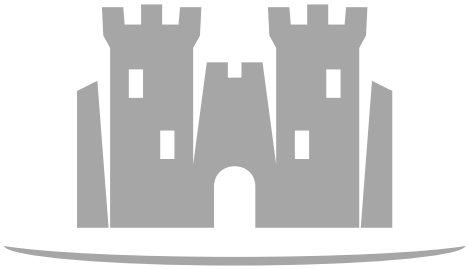
INTRODUCCIÓN

En 1971, Ray Tomlinson, un joven ingeniero que trabajaba en lo que ahora es Forcepoint BBN Technologies, presentó el omnipresente símbolo "@" y cambió las comunicaciones tal y como las conocemos. El lanzamiento del correo electrónico, la expansión de las redes y el intercambio de datos junto con la introducción del sistema de nombres de dominio han creado oportunidades tecnológicas innovadoras para personas, empresas y gobiernos en todo el mundo. Sin embargo, estas oportunidades también se les presentaron a los atacantes – delincuentes que esperaban aprovechar las ventajas de esta nueva apertura mediante la explotación de protocolos, aplicaciones y sistemas operativos.

En respuesta a esto, los defensores cibernéticos se encontraron dentro de un círculo interminable de intentos de llenar brechas de seguridad con parches, superposiciones y nueva tecnología. Aunque admirables, estos esfuerzos no fueron eficaces porque a menudo se aplican a lo que fundamentalmente es infraestructura tecnológica insegura.

Los profesionales de seguridad de TI y los ejecutivos al mando de las empresas solo desean mantener a los atacantes fuera de sus redes y sistemas, pero este plan de juego ha demostrado ser imposible. Las noticias en los medios son bien conocidas, y los datos son alarmantes: Según el informe Investigaciones sobre fugas de datos 2015 de Verizon, hubo más de 79,790 incidentes de seguridad en 2014[1].

En este contexto, la pregunta es: si es imposible prevenir las fugas, ¿cómo deben concentrar sus esfuerzos los profesionales de seguridad cibernética para minimizar el impacto de un ataque?



DESPLAZANDO LA CARGA HACIA EL ATACANTE

El enfoque de seguridad cibernética pasivo, en espera de un ataque, claramente no es suficiente; esto está más que claro. Mientras las organizaciones deben trabajar para fortalecer sus defensas, un enfoque pragmático incluye:

1. **Reconocer la realidad actual:** las fugas de datos existen, no se debe negar lo inevitable.
2. **Reconocer el panorama de amenazas:** los ataques provienen tanto desde adentro como desde afuera de una organización. Cuando se originan afuera, los atacantes imitarán a los empleados de la organización.
3. **Identificar las vías de ataque:** la ruta que siguen los atacantes dentro de una red –conocida como movimiento lateral– brinda información clave sobre la intención y el impacto potencial de una fuga.
4. **Limitar la duración de la fuga:** tomar las medidas necesarias para minimizar el tiempo del atacante dentro de su red – el tiempo de permanencia de un ataque cibernético – lo que limita el impacto potencial al reducir la exposición.

Los puntos 3 y 4 serán el foco de este documento y presentan los conceptos de movimiento lateral y **tiempo de permanencia de un ataque cibernético**. Entender estos conceptos les permite a las organizaciones desplazar el peso de la amenaza al atacante, convirtiendo sus bienes y su infraestructura en un blanco menos deseable.

1 Fuente: http://www.verizonenterprise.com/DBIR/2015/

Según el informe Investigaciones sobre fugas de datos 2015 de Verizon, hubo más de

79,790 incidentes de seguridad en 2014.[1]

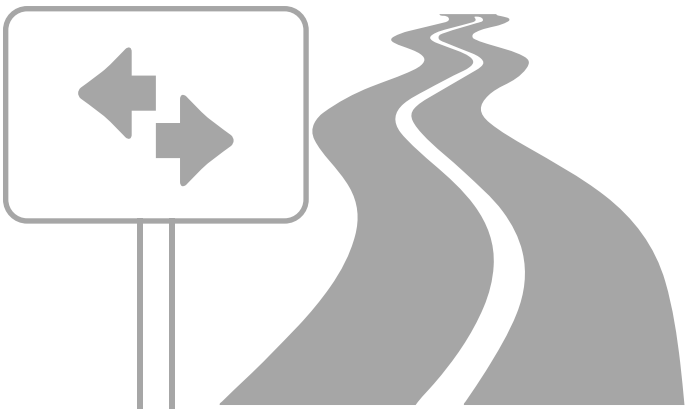
UN SENDERO EN EL BOSQUE: COMPRENSIÓN DEL MOVIMIENTO LATERAL

Los ataques avanzados ocurren con un propósito; son lanzados con una clara intención. Teniendo esto en mente, es importante que las organizaciones no tengan un punto de vista a corto plazo sobre el análisis de un ataque.

Por ejemplo, cuando se descubre que una máquina está en peligro, hay algunas preguntas fundamentales que deben hacerse siempre: ¿Por dónde ingresó el ataque? ¿Cómo fue posible el movimiento? ¿Cuál era el objetivo final? ¿Qué controles se realizaron para que la amenaza fuera persistente?

Al responder las preguntas planteadas, los encargados de la defensa de seguridad deben comprender que el *phishing* dirigido, los ataques de "pozo de agua" (*waterhole*) o cualquier otra metodología de envío de malware son todos medios para lograr un fin. Los sistemas infectados, si bien son importantes por derecho propio, son superfluos para los atacantes avanzados. Lo que en realidad les interesa es su capacidad para permanecer sin ser detectados mientras recorren las redes de la empresa.

El objetivo inicial del envío de malware normalmente no es extraer la mayor cantidad de información intelectual posible, sino establecer una puerta de entrada a los entornos que los atacantes no controlan. Ese sistema infiltrado se convierte en proxy para comenzar el proceso de movimiento lateral. Puede realizarse un solo paso lateral o 100 pasos para obtener la propiedad intelectual deseada o el control de un sistema. En muchos casos, los atacantes van en busca de las credenciales de una persona, lo que les permite moverse en la red aparentando ser un usuario legítimo. Es esencial comprender dónde y cómo ocurre esto, ya que brinda información sobre la intención y el impacto potencial de un ataque.



VIDA ÚTIL DE UN ATAQUE: CONTENCIÓN DEL TIEMPO DE PERMANENCIA DE UN ATAQUE CIBERNÉTICO

Como se comentó, las organizaciones pragmáticas comprenden bien que habrá fugas y que la prevención, aunque es muy necesaria, no puede ser su única táctica de seguridad. También deben enfocarse en la contención. Es primordial identificar y contener a un atacante lo antes posible.

Del mismo modo que los vándalos que ingresan a una escuela en horas de inactividad escolar, el objetivo de la contención del tiempo de permanencia de un ataque cibernético es asegurar de que los vándalos tengan el menor tiempo posible para provocar estragos y sacar bienes importantes de la organización. La investigación demuestra que los atacantes pasan un promedio de 200 días dentro de una red antes de ser erradicados.[2] Imagínense todo el daño que podría causar un atacante en ese período de tiempo. Si los atacantes pueden ser contenidos en menos tiempo y posteriormente tienen acceso a menos áreas de superficie de la empresa, agotarán más recursos para obtener lo que desean.

Para reducir el tiempo de permanencia de un ataque cibernético, es necesario comprender el concepto en su totalidad. El tiempo de permanencia de un ataque cibernético comienza cuando un atacante ingresa en su red y permanece hasta que usted lo expulsa o se va (presumiblemente después de haber completado las acciones deseadas). El objetivo debe ser reducir el tiempo de permanencia en la medida de lo posible y dar al atacante la menor oportunidad de lograr un movimiento lateral y extraer datos esenciales de su organización.

La siguiente pregunta probable es: "¿Cómo se mide el tiempo de permanencia de un ataque cibernético?". Esto solo se puede hacer rastreando la amenaza hasta su origen; determinar cuándo y dónde se originó la amenaza, además de seguir el rastro de los movimientos laterales.

2 Fuente: INFOSEC Institute: *The Seven Steps of a Successful Cyber Attack* (Los siete pasos de un ataque cibernético exitoso), 11 de julio de 2015

Áreas de enfoque para reducir el tiempo de permanencia de un ataque cibernético

- Controles de seguridad fundamentales
- Visibilidad granular e inteligencia correlacionada
- Monitoreo continuo de dispositivos finales
- Predicción demostrable del comportamiento humano
- Reconocimiento del usuario

CINCO PRÁCTICAS PARA CAMBIAR LA CARGA DE LUGAR

A medida que las organizaciones avanzan para reducir el tiempo de permanencia de un ataque cibernético, hay muchos conceptos fundamentales que deben considerarse. A continuación se detallan cinco prácticas que sirven para ayudar a las organizaciones a reducir el tiempo de permanencia de un ataque cibernético mediante la detección, la contención y el control de las amenazas cibernéticas.

1. **Controles de seguridad fundamentales.** El primer paso, particularmente relevante en el contexto de la contención del movimiento lateral, es asegurar que se estén implementando los controles básicos de seguridad. Al implementar controles fundamentales de seguridad – como la aplicación regular de parches, el acceso administrativo restringido, la autenticación de dos factores y la segmentación de la red donde corresponda – el atacante se verá obligado a invertir mayores recursos para encontrar una manera de ingresar. Al obligar al atacante a aumentar su inversión, este puede elegir buscar un blanco más atractivo.

   En el proceso de implementación de controles de seguridad de mejores prácticas, un paso fundamental debe ser identificar blancos de alto valor – los sistemas y las personas esenciales para el éxito de su organización. Estos son los blancos que los adversarios desean explotar con más frecuencia para obtener una ventaja financiera o intelectual. El control de seguridad debe aumentar para estos bienes. Un enfoque de este tipo permite que sus equipos de seguridad cibernética dediquen tiempo operativo a dar prioridad a las alertas y, al mismo tiempo, faciliten el proceso para aplicar controles enfocados en dispositivos finales, dispositivos de redes o los mismos blancos de alto valor.

2. **Visibilidad granular e inteligencia correlacionada.** Como se indicó anteriormente, las fugas ocurrirán independientemente de las medidas fundamentales de seguridad que se implementen.

   Sin embargo, las empresas pueden resistir fugas asegurando la visibilidad granular de su red y de las comunicaciones empresariales.

   Por lo tanto, las empresas deben implementar funcionalidades de control de redes como Netflow y recolectar registros de cualquier dispositivo que capte el uso de identidad. Esto les permite a las organizaciones crear indicadores relacionados con el robo de identidad, la pérdida de datos y la actividad anormal en forma diaria. Si bien estas alertas son importantes, una capacidad esencial es la correlación de acciones con cada máquina o usuario, dentro o fuera de la red. La información detallada relacionada con todos los mensajes de correo electrónico entrantes, como encabezados completos e incluso contenido, les permitirá a los equipos de seguridad cibernética llegar hasta el origen del incidente.

   La visibilidad forense es imperativa cuando los atacantes traspasan el perímetro y los controles de seguridad internos. Con los datos forenses, las organizaciones tienen una mayor capacidad para rastrear las amenazas hasta su origen y calcular el tiempo de permanencia. El tiempo de permanencia es un nuevo indicador para los encargados de responder a los incidentes, e incidentalmente es el único que Forcepoint utiliza para medir su postura de seguridad. ¿Qué tan eficaz es su equipo de respuesta para detectar, contener y controlar las amenazas avanzadas?

3. **Monitoreo continuo de dispositivos finales.** Con el monitoreo continuo de dispositivos finales, las organizaciones pueden tener una percepción aguda de las personas, los procesos y las máquinas – traduciendo la actividad de los usuarios en los dispositivos finales en políticas y viceversa prácticamente en tiempo real. ¿Por qué es importante esto? Cuando se hace correctamente, el reconocimiento contextual resultante permite a los equipos de seguridad juntar las piezas del marco de un incidente y correlacionar eventos aparentemente no relacionados. Esto significa tiempos de respuesta más rápidos y menos tiempo dedicado al trabajo forense tradicional para intentar comprender los movimientos y las intenciones de un atacante.

   Como se mencionó anteriormente, la mayoría de los ataques comienza con el huésped o el empleado, por lo tanto el monitoreo continuo de los dispositivos finales es una evolución importante en la postura de seguridad, y esencial para responder rápidamente a los incidentes. Esta información sobre dispositivos finales permite la detección más rápida de malware y de comportamientos anormales de los usuarios. Buscando no solo malware y prestando atención a la actividad anormal de los usuarios, las organizaciones podrán reducir el tiempo de permanencia. Esta reducción del tiempo de permanencia y la evidencia forense proporcionarán la capacidad para aplicar contexto y proteger más que sistemas individuales.

"...El reconocimiento contextual resultante permite a los equipos de seguridad juntar las piezas del marco de un incidente y correlacionar eventos aparentemente no relacionados".

4. **Predicción demostrable del comportamiento humano.** La predicción de perfiles de ataque sobre la base del plan probable de un adversario, una ciencia dentro del campo más amplio de la respuesta a incidentes, les permite a las organizaciones anticipar los movimientos que podría hacer un atacante para tener acceso a blancos de alto valor. Más específicamente, al comprender la ruta anterior de un atacante – a dónde viajó anteriormente – los profesionales de seguridad pueden comenzar a predecir su ruta futura.

   ¿Por qué es importante esto? La capacidad de predecir el movimiento futuro es esencial para contener el movimiento lateral y reducir el tiempo de permanencia. El equipo de seguridad cibernética puede anticipar mejor los próximos pasos de un ataque y aislarlo. Esto es similar al juego de ajedrez, en el sentido de que el adversario tiene varias piezas en el tablero y ha hecho muchas movidas. El atacante también tiene muchas movidas más planificadas para crear un escenario de "jaque mate". Los profesionales de seguridad pueden determinar los pasos que deben seguir, como sacar determinados recursos fuera de línea o notificar a los usuarios que estén atentos a comportamientos anormales, para asegurar que no haya "jaque mate".

   Para que este esfuerzo sea eficaz, los equipos de seguridad cibernética deben aceptar que los atacantes externos no son diferentes de un atacante interno. Saben tanto de sistemas internos como los administradores de TI. Sus actividades se mezclan con los comportamientos normales en la red, y gracias al malware personalizado, los usuarios afectados proporcionan una capacidad general de comportarse como un atacante interno. Las organizaciones deben asumir que todos los empleados de alto perfil (las personas conocidas fuera de la compañía debido a la exposición a los medios o a un nivel ejecutivo de visibilidad) son puntos de entrada a la empresa y una ruta que conduce a un destino final. Del mismo modo que un atacante, tienen acceso a determinados recursos y esos recursos tienen acceso a otros recursos. Esto puede crear predicciones útiles sobre el comportamiento humano normal y anormal para la creación de un marco para crear zonas, reducir privilegios y permitir que el equipo de seguridad tenga la capacidad de combatir a los atacantes una vez que estén dentro de la empresa.

5. **Reconocimiento del usuario.** Es imperativo que las organizaciones eduquen a sus empleados no solo sobre las políticas corporativas y los mandatos gubernamentales, sino también sobre el creciente riesgo que presentan las amenazas avanzadas para la organización. Al implementar programas educativos formales, los profesionales de seguridad obtienen un mayor respaldo de los usuarios finales, lo que aumenta la probabilidad de cambiar el comportamiento riesgoso.

   Asimismo, el equipo de seguridad también debe poder educar a los empleados para que estén atentos a situaciones excepcionales, como cuando los usuarios se convierten en blanco de los atacantes.

   Cuando se identifica un ataque, sea exitoso o no, es importante brindarles a los usuarios afectados información sobre el ataque para que conozcan qué aspecto pueden tener los ataques futuros. Si un ataque es exitoso, los profesionales de seguridad no deben castigar a los usuarios, sino darse cuenta de que siempre se cometerán errores. Esta es una oportunidad para guiar las acciones futuras en la dirección correcta. En efecto, los usuarios se convierten en "sistemas de detección de intrusiones" y brindan información que de otro modo podría perderse en el marco de la seguridad cibernética. No hay ningún producto en el mercado que detecte todo el malware o todos los malos comportamientos de los usuarios. Dicho esto, si se combina una buena tecnología y buenos procesos con buena gente, las empresas podrán aumentar la capacidad para combatir las amenazas avanzadas, reducir el tiempo de permanencia y detectar movimientos laterales.

"Si se combina una buena tecnología y buenos procesos con buena gente, las empresas podrán aumentar la capacidad para combatir las amenazas avanzadas, reducir el tiempo de permanencia y detectar movimientos laterales".

CONCLUSIÓN

Cuanto más tiempo permanecen los atacantes en la empresa (mayor tiempo de permanencia), más daño pueden causar y más propiedad intelectual pueden robar. Las organizaciones actuales no deben concentrarse únicamente en mantener a los atacantes fuera de sus redes, sino en garantizar que el atacante permanezca el menor tiempo posible en la red — y esforzarse constantemente por reducir aún más el tiempo de permanencia. Los atacantes pueden regresar, pero se darán cuenta de que sus esfuerzos son demasiado costosos y tienen poco retorno de inversión. Cuando los atacantes se encuentran con una empresa enfocada en el tiempo de permanencia, rápidamente se dan cuenta de que aunque encontraran una puerta abierta, la empresa los detectaría de inmediato y los expulsaría. Entonces se irán a otra parte, en busca de una empresa menos protegida.

CONTACTO

www.forcepoint.com/contact

ACERCA DE FORCEPOINT

[WHITEPAPER_CYBER_DWELL_TIME_ESLA] 200017.011416