¿Cuál es el siguiente nivel para los antivirus de nueva generación?

Hoy se perpetran más ciberataques que nunca y nada favorece más el acceso indebido a los datos confidenciales de las empresas que la gran variedad de endpoints que existe. Para protegerlos, todavía son demasiadas las empresas que siguen recurriendo a antivirus obsoletos basados en firmas. Desgraciadamente, los antivirus antiguos —e incluso su sucesor, el «antivirus de nueva generación»— no garantizan la protección de las empresas, ya que hoy en día los atacantes han desarrollado todo un arsenal de técnicas que no requieren archivos ni firmas, y se han vuelto auténticos expertos en crear y utilizar malware nuevo, la mayoría del cual no tiene ni 24 horas de vida. En este informe, hablaremos de cómo los equipos de seguridad pueden adaptar su estrategia de seguridad del endpoint para defenderse de todas estas amenazas.

El mercado de la ciberseguridad busca satisfacer la necesidad de herramientas capaces de identificar ataques avanzados y sofisticados para permitir a las empresas investigar lo ocurrido, darle seguimiento y localizar la causa principal para reparar los endpoints afectados. Estas herramientas suelen conocerse como «antivirus de nueva generación», «plataformas de protección del endpoint» y «soluciones de detección y respuesta en el endpoint» (NGAV, EPP y EDR, respectivamente, por sus siglas en inglés); categorías cuyas funciones hoy a menudo se solapan. Por eso, a la dificultad para decidir en qué invertir se suma el hecho de que ninguna de ellas haya demostrado ser eficaz a la hora de responder a las necesidades de seguridad de las empresas. Según el Ponemon Institute, cerca del 67 % de las empresas acusan falta de tiempo y recursos para proteger todas las vulnerabilidades que afectan a sus endpoints e impedir que se produzcan brechas de datos.[1] De hecho, según los resultados de las pruebas del SANS Institute, los productos EDR normalmente detectan tan solo el 26 % de los vectores de ataque iniciales.[2] Si las plataformas EPP no previenen los ataques y las soluciones EDR no los detectan, nos quedamos sin respuesta.

En este informe, nos ocuparemos de las funciones específicas que las empresas necesitan para proteger sus endpoints de las amenazas modernas. También examinaremos una serie de estrategias escalables para implementar estas funciones y optimizar tanto los flujos de trabajo como los resultados de los equipos de SecOps, ahora y en el futuro.

Una buena prevención sigue siendo la clave de una estrategia de seguridad eficaz

Los atacantes son muy mañosos y el volumen y la variedad de los endpoints potencialmente vulnerables no paran de crecer. Pero seamos realistas: detener el 100 % de las amenazas es prácticamente imposible, al menos sin bloquear otras actividades benignas ni interrumpir drásticamente las operaciones de la empresa.

Dicho esto, es necesario entender que, sin una prevención coherente y coordinada, la detección y la respuesta caen en saco roto. Hasta la solución EDR más eficaz solo detecta los ataques una vez iniciados, lo que sitúa a los equipos de SecOps en una posición pasiva que los obliga a localizar primero el daño para luego invertir recursos operativos en estudiarlo y valorarlo antes de, en último término, tratar de repararlo. Las soluciones EDR son como los sensores de colisión que disparan los airbags: aunque salvan vidas, es preferible prevenir el choque. Una metodología centrada en la prevención equivale a implementar una seguridad basada en evitar las colisiones. El primer paso hacia una buena prevención es revisar la forma en que las organizaciones responden a las amenazas.

Tres principales requisitos de la protección del endpoint

Los atacantes deben completar cierta secuencia de eventos, conocida como «ciclo de vida de los ataques», para lograr sus objetivos, ya se trate de robar información o de ejecutar ransomware. Casi todos los ataques empiezan poniendo en riesgo un endpoint y, aunque la mayoría de las organizaciones han implementado sistemas de protección del endpoint, lo cierto es que no son infalibles y las infecciones siguen siendo frecuentes.

En la actualidad, muchos de los atacantes más avezados fusionan dos métodos de ataque principales: los dirigidos a las vulnerabilidades en las aplicaciones y la implementación de archivos maliciosos. Estos métodos pueden utilizarse por separado o combinados de diversas maneras, aunque sus características esenciales son distintas:

- **Los exploits** son el resultado de técnicas diseñadas para obtener acceso a través de las vulnerabilidades del código del sistema operativo o de una aplicación.
- **El malware** es un archivo o fragmento de código que infecta, explora o sustrae información, o bien adopta el comportamiento que el atacante quiera.
- **El ransomware** es un subtipo de malware que secuestra archivos o datos valiosos. El atacante, por lo general, cifra los datos y solo entregará la clave de descifrado a cambio de un rescate.

Debido a las diferencias fundamentales entre el malware y los exploits, para que una estrategia de prevención sea efectiva es necesario, además de protegerse de ambos ataques, incluir las siguientes funciones.

1. Análisis de malware

La complejidad de las amenazas actuales —combinada con su diversidad, volumen y sofisticación cuando tienen como blanco el entorno empresarial moderno— dificulta enormemente su prevención. Por si no fuera suficiente, a esto se añade el desafío de detectar malware y exploits nunca vistos y de identificar contenido malicioso conocido.

Para bloquear estas amenazas sofisticadas, dirigidas y evasivas, la protección del endpoint debe integrarse con la inteligencia sobre amenazas compartida, lo que permitirá conocer y desarrollar las defensas que sean necesarias. IDC Research ha publicado un informe según el cual el 39 % de los profesionales de seguridad consideran que la inteligencia sobre amenazas compartida es una prioridad alta o muy alta a la hora de mejorar la estrategia de seguridad.[3] En relación con esto, cabe destacar que integrar la inteligencia sobre amenazas basada en la nube con la protección del endpoint permite realizar un análisis más profundo y detectar lo antes posible amenazas potencialmente desconocidas. El aprendizaje automático en el endpoint debería ayudar a evaluar rápidamente un archivo tanto para determinar si es sospechoso como para someterlo a análisis dinámicos más profundos y, si fuera necesario, aislarlo en sandboxes de hardware e impedir la entrada de malware aún más evasivo.

2. Prevención del ransomware

Aunque el ransomware no es algo nuevo, los ataques graves como WannaCry, Petya/NotPetya y TrickBot han demostrado que los métodos de prevención convencionales son ineficaces frente al ransomware avanzado. Los atacantes han desarrollado métodos que les permiten usar el malware en ataques cada vez más sofisticados, automatizados, dirigidos y evasivos.

Prevenir el ransomware requiere instalar en el endpoint una serie de funciones de «defensa en profundidad» que permitan detectarlo y eliminarlo en distintas etapas del ciclo de vida del ataque. En el caso de WannaCry, conviene contar con funciones de prevención de exploits para detectar, en primer lugar, la técnica que intenta asumir privilegios sobre el kernel más allá de los del nivel de usuario y, después, bloquear el ataque. Si esto falla, la protección del proceso secundario debería detectar el proceso principal y detenerlo cuanto antes para impedir que genere un proceso secundario. Si, con todo, las amenazas pasan desapercibidas, el agente debería ser capaz de utilizar el análisis local y el aprendizaje automático para identificar las características conocidas de WannaCry.

1. *Challenging State of Vulnerability Management Today: Gaps in Resources, Risk and Visibility Weaken Cybersecurity Posture* (disponible en inglés), Balbix, Inc. y Ponemon Institute, julio de 2018, https://www.balbix.com/app/uploads/Ponemon-Survey-Vuln-Management-.pdf.
2. *Endpoint Protection and Response: A SANS Survey* (disponible en inglés), SANS Institute, 12 de junio de 2018, https://www.sans.org/reading-room/whitepapers/analyst/membership/38460.
3. Konstantin Rychkov y Duncan Brown, *Bridging Security Gaps with Network-to-Endpoint Integration* (disponible en inglés), IDC Research, octubre de 2018, https://www.paloaltonetworks.com/resources/whitepapers/bridging-security-gaps-with-network-to-endpoint-integration.

WastedLocker: combinación de malware y exploits

El ransomware como WastedLocker, que ha sido utilizado para pedir rescates de millones de dólares, se sirve de una combinación de exploits y malware para lograr sus objetivos y está dotado de distintas funciones innovadoras que le ayudan a burlar los sistemas de protección del endpoint. Este ransomware funciona así: primero, engaña a los usuarios para que descarguen código malicioso de sitios web mediante actualizaciones de software falsas. Esto implanta en el sistema atacado un cargador de Cobalt Strike personalizado que permite cargar el ransomware. A continuación, WastedLocker se desplaza lateralmente por la red de la víctima, se infiltra en una o más herramientas de gestión de sistemas para garantizar que se ejecutará sin problemas y, por último, despliega la carga.

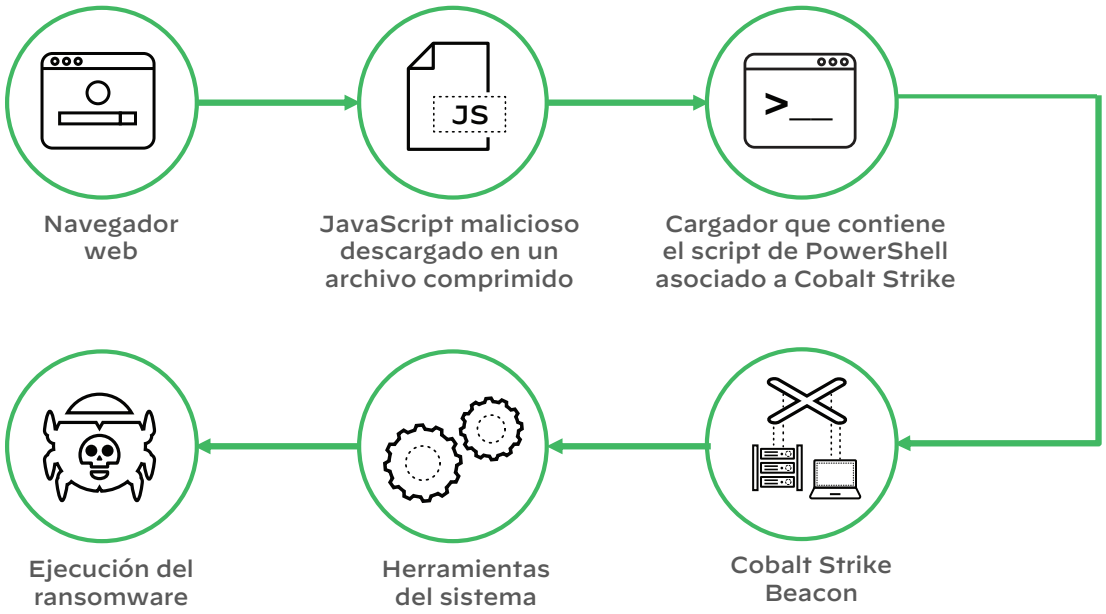

Figura 1: Secuencia simplificada del ataque de WastedLocker

3. Prevención de exploits

Cada año se descubren miles de vulnerabilidades y exploits de software nuevos, lo que exige, por un lado, que los proveedores de software distribuyan revisiones de software con diligencia y, por otro, que los administradores de seguridad y sistemas de las organizaciones las gestionen oportunamente. En resumidas cuentas, las revisiones se instalan para impedir la explotación de vulnerabilidades.

Claves de las técnicas de exploit

Muchas amenazas avanzadas insertan código malicioso en archivos de datos aparentemente inofensivos. Cuando estos archivos se abren, el código malicioso aprovecha, para ejecutarse, vulnerabilidades de la aplicación nativa utilizada para visualizar dichos archivos. Como las políticas de seguridad de TI permiten la aplicación vulnerable, este tipo de ataque esquivará los controles de listas de acceso.

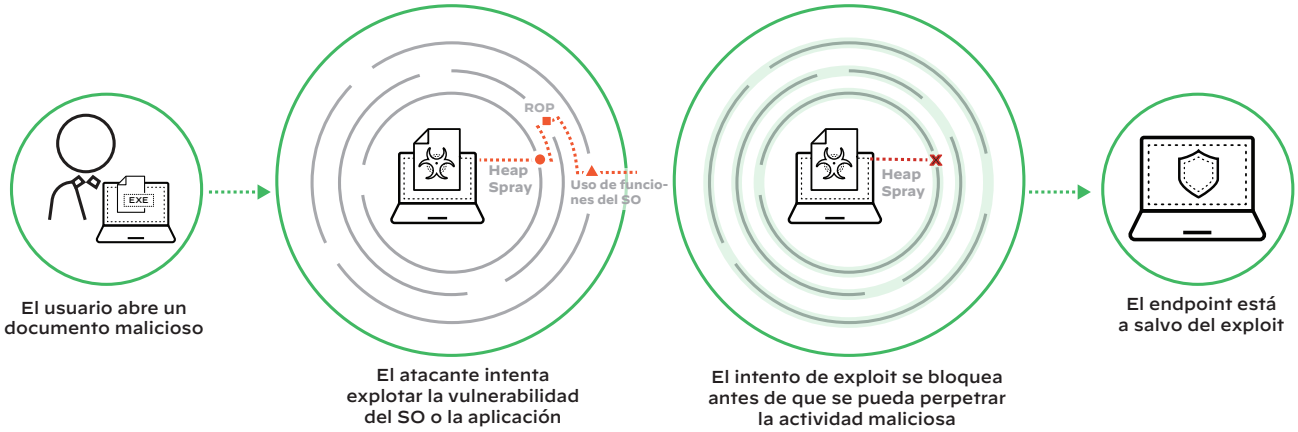

Figura 2: Protección frente a las técnicas de exploit (más que frente a los exploits en sí)

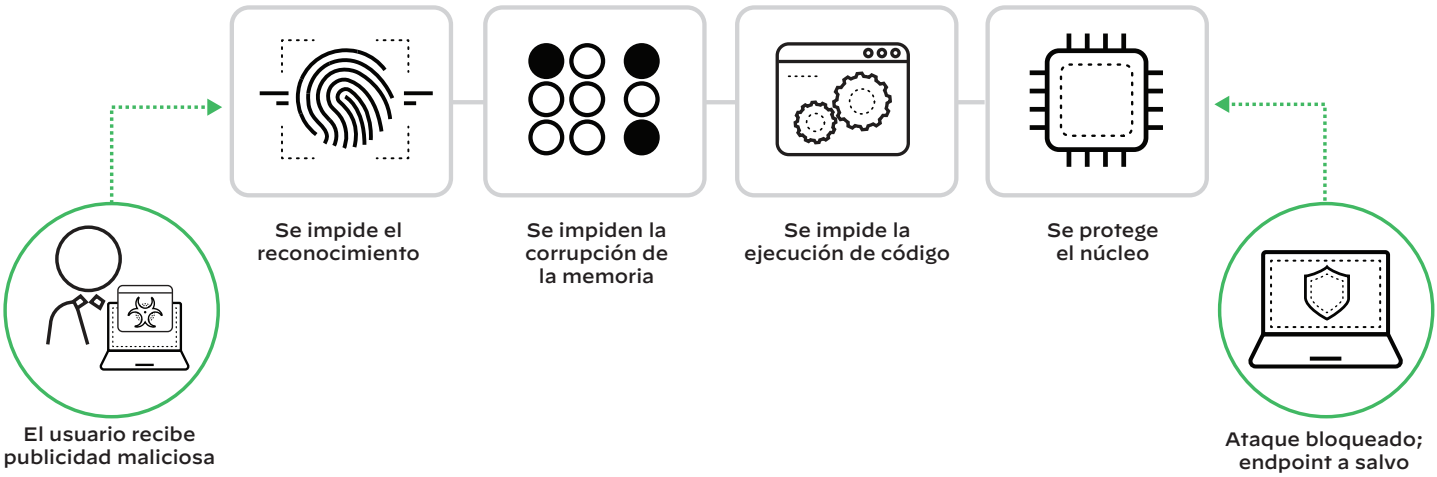

Figura 3: Diversos métodos de prevención de exploits

Aunque existen varios miles de exploits, todos ellos se basan en un reducido conjunto de técnicas básicas que apenas cambian. Independientemente del tipo de exploit o de su grado de complejidad, para que un ataque tenga éxito, quien lo perpetra debe emplear secuencialmente una serie de técnicas de exploit; es como encontrar la salida de un laberinto.

La prevención de exploits se centra en las técnicas básicas empleadas por todos los exploits y, al anular la utilidad de esas técnicas, neutraliza el riesgo que suponen las vulnerabilidades de las aplicaciones, tanto si están actualizadas como si no. Esta metodología resulta particularmente crucial a la hora de proteger entornos heterogéneos —como los que tienen cargas de trabajo en la nube—, donde los controles de los endpoints físicos pueden crear complicaciones imprevistas en los entornos virtuales.

Una estrategia de seguridad del endpoint válida a largo plazo

Es indiscutible que la prevención es crucial, pero por sí sola es insuficiente en la defensa frente a los ataques avanzados. Puede que su solución de protección del endpoint bloquee el 98 % de los intentos de brecha, pero ¿qué hay de ese 2 % por descubrir y mitigar?

Las funciones de detección y respuesta deben ir más allá del endpoint; después de todo, si los atacantes no se quedan en los endpoints, las herramientas de seguridad tampoco deberían hacerlo. Ahí es donde fallan las soluciones de EDR, lo que suele conducir a los equipos de seguridad infradotados a desperdiciar horas siguiendo el rastro de la actividad maliciosa para al final descubrir que un cortafuegos o punto de aplicación de políticas ya la ha bloqueado. Es preferible que las funciones de detección y protección del endpoint formen parte de una plataforma de detección y respuesta ampliadas (XDR, por sus siglas en inglés) integral que aplique el aprendizaje automático a una secuencia de datos centralizada. Esto permitirá disfrutar de visibilidad completa de los ataques en todas las fuentes de datos y coordinar la prevención en todos los puntos de aplicación de políticas. Las plataformas de XDR incorporan más funciones de prevención que los antivirus de nueva generación y las soluciones EDR, y ofrecen la visibilidad y la capacidad de análisis que los equipos de seguridad necesitan para combatir ataques sofisticados ahora y en el futuro.

Un estudio llevado a cabo por Forrester Consulting en 2020 muestra que solo el 49 % de las organizaciones consideran que sus herramientas de seguridad están bien integradas. Las organizaciones dedican muchísimo tiempo a obtener los datos que necesitan y a asegurarse de que dichos datos estén en el formato adecuado para que las herramientas de análisis puedan procesarlos. Otras veces necesitan recopilar datos de distintas fuentes para determinar qué usuarios, dispositivos, procesos o aplicaciones están asociados con según qué eventos. XDR automatiza todo esto reconstruyendo los incidentes de seguridad a partir de la correlación de alertas de distintas fuentes de datos y reduce drásticamente el número de alertas dispares que los analistas deben procesar cada día.

La reducción del volumen de alertas permite que los equipos de seguridad actúen más rápido. Las soluciones de XDR líderes del sector mejoran la seguridad porque integran funciones de protección del endpoint, detección y respuesta que apenas consumen recursos, prescinden de las firmas para la prevención, cuentan con una interfaz de gestión basada en la nube y aprovechan un gran volumen de datos de eventos y logs de alertas. Esto ofrece a los equipos de operaciones de seguridad la visibilidad necesaria para desarrollar operaciones centradas en la prevención sin descuidar la administración de los endpoints.

El próximo antivirus de nueva generación en el que invierta debe ser XDR

Las herramientas aisladas y los procesos manuales no tienen cabida en el futuro de las operaciones de seguridad. Para detener las amenazas sofisticadas y su creciente arsenal de herramientas va a ser necesaria mucha más inteligencia y el uso sistemático de la automatización, los datos masivos y el aprendizaje automático, así como un conjunto de herramientas más integrado que permita implementar las nuevas funciones de una forma más rápida y completa. Las inversiones en seguridad del endpoint ya no deberían depender únicamente de lo eficaz que sea la protección frente al malware ni del tamaño del agente del endpoint. Además, conviene tener en cuenta cómo facilitan los flujos de trabajo de las operaciones de seguridad, esenciales para la estrategia de seguridad general de una organización.

Su inversión en seguridad debe tener en cuenta si la solución elegida incluye:

- controles integrados de protección, detección y respuesta que se sirvan de la inteligencia artificial y el aprendizaje automático para resolver las deficiencias de seguridad automáticamente;
- controles unificados que hagan más fluida la comunicación entre los equipos de respuesta a incidentes y los administradores de SecOps, de los endpoints y de la red;
- un sistema que genere menos alertas de seguridad, y de mejor calidad;
- funciones que hagan visible toda la infraestructura —los endpoints, la red y la nube— para acelerar los tiempos de detección y respuesta, y reducir así el tiempo que los atacantes pasan en ella.

XDR es la única solución de seguridad del endpoint que cumple todos estos requisitos. Gracias a la combinación de datos de la red, los endpoints y la nube mejorados con tecnologías de análisis, XDR agiliza la clasificación de alertas y la respuesta a incidentes al proporcionar automáticamente una imagen completa de cada amenaza y su causa principal. De este modo, se reducen el tiempo y la experiencia del equipo de analistas necesarios en cada etapa de las operaciones de seguridad, desde la clasificación de las amenazas hasta su detección. La integración perfecta con los puntos de aplicación de políticas permite que los equipos de operaciones de seguridad respondan con rapidez a las amenazas y apliquen los conocimientos adquiridos para adaptar las defensas y evitar futuras amenazas, lo que agiliza aún más la siguiente respuesta. Además, como ventaja añadida, gracias a que XDR rebaja las exigencias en cuanto al nivel de conocimientos y cualificación que necesitan tener los analistas de seguridad de su equipo, se reduce el coste de las operaciones de seguridad.

Conclusión

Al adoptar un modelo orientado a la prevención con funciones de protección, detección y respuesta integradas, y al permitir que el equipo de SecOps no se centre en el «qué», sino en el «cómo», las organizaciones estarán en condiciones de resolver cuatro retos fundamentales: las carencias en materia de seguridad, el exceso de alertas, el aislamiento de las operaciones y el tiempo de permanencia de los atacantes en su entorno, que cada vez es más largo.

A la hora de elegir su próxima solución de seguridad del endpoint, estos son los objetivos que debería tener presentes: protección integrada; eliminación precoz de las alertas; detección y respuesta a través de un agente del endpoint ligero; cadenas de causalidades avanzadas que unifiquen los equipos de SecOps, administración del endpoint y respuesta a incidentes; y visibilidad completa de toda la infraestructura —los endpoints, la red y la nube— para aumentar los índices de detección y respuesta y, en última instancia, reducir el tiempo de permanencia del enemigo.

paloalto NETWORKS

Oval Tower, De Entrée 99 - 197
1101HE Ámsterdam
Países Bajos

Tel.: +31 20 888 1883

www.paloaltonetworks.es

what-is-the-next-step-for-next-gen-antivirus-wp-111220-es