FORTINET
NSE Training Institute

NSE 2 Endpoint Scripts—Spanish Version

¡Hola! En esta clase, hablaremos de la seguridad de los dispositivos terminales o endpoints, en qué consiste y cómo ha evolucionado.

Veamos qué es un endpoint. Anteriormente, se trataba de cualquier dispositivo personal utilizado por un usuario final, como una computadora de escritorio o portátil, o un dispositivo móvil. Hoy, los endpoints incluyen la internet de las cosas (Internet of Things, IoT), que abarca una gran variedad de aparatos, como termostatos inteligentes o refrigeradores domésticos.

¿Cómo hemos garantizado la seguridad de estos endpoints y por qué es tan importante? Los endpoints siempre han sido un punto de entrada fácil a una red. Por qué intentar burlar un firewall si, a través de la ingeniería social, es posible aprovecharse de los usuarios desprevenidos o ingenuos. A medida que las conexiones en línea han aumentado, la cantidad de vectores de ataque se ha multiplicado en los endpoints, lo que da a los atacantes más oportunidades para aprovechar.

Antes de que las redes estuvieran conectadas a internet, los agentes maliciosos utilizaban discos flexibles para esparcir un *malware*. Cuando un disco infectado se insertaba en una computadora, esta también quedaba infectada. Luego, la lista incluiría otros dispositivos de almacenamiento extraíbles, como los CD o DVD, o las unidades portátiles conectadas por USB. Como puede imaginar, este vector de ataque tenía un alcance bastante limitado. Los primeros productos de seguridad para endpoints fueron los antivirus o AV, es decir, programas para escanear dispositivos y discos duros en busca de *malware*. Estaban basados en firmas, lo que significa que los programas antivirus buscaban características, huellas digitales o firmas de los virus. Si encontraban algo que tuviera esas características, ponían el programa en cuarentena o lo eliminaban.

Todo esto cambió cuando las redes domésticas y las empresariales comenzaron a conectarse a internet. Los ciberdelincuentes empezaron a tener muchos más vectores de ataque a disposición, como los correos electrónicos de suplantación de identidad (*phishing*), los sitios web infectados, la práctica de llevar los dispositivos personales al trabajo (*bring your own*

device o BYOD) y las redes sociales. Estas nuevas oportunidades generaron una proliferación de *malware*, que pasaron de unas decenas de miles por año a cientos de miles por día. Además, los agentes maliciosos empezaron a explotar los agujeros de seguridad de los sistemas operativos y de aplicaciones como el navegador web o, incluso, otras relativamente inertes como los documentos de MS Word. Para agravar el problema de una superficie de ataque cada vez mayor, la propia naturaleza del *malware* cambió. El *malware* polimórfico está diseñado para cambiar por sí mismo e imita la mutación de los virus en el mundo natural. Así, los programas antivirus basados en firmas dejaron de ser completamente efectivos.

Fue así que llegó la plataforma de protección para endpoints (*endpoint protection platform*, EPP), cuyo fin era prevenir ataques de *malware* basados en archivos e implementar otros controles preventivos. Este método consistía en detener el *malware* antes de que se ejecutara e infectara el dispositivo. Un *malware* basado en archivos es un archivo que se descarga en un dispositivo y que, cuando se lo abre, ejecuta un código malicioso o un *script*.

Las EPP brindan muchos servicios orientados a la prevención, como los antivirus, los firewalls para dispositivos, los filtros de contenido web, la protección de datos mediante cifrado y el control de dispositivos. El control de dispositivos es una tecnología que proporciona seguridad integrada para detectar, autorizar y proteger los dispositivos de almacenamiento extraíbles. El filtro de contenido web es una tecnología que permite a los administradores de una red controlar el tipo de sitios a los que se puede acceder.

Sin embargo, ninguna de estas tecnologías ha demostrado ser el antídoto definitivo para la infección de endpoints. En ese entonces, se pensaba que los filtros de contenido web eran una solución porque se suponía que los *malware* de internet solo provenían de sitios maliciosos. También estaba la posibilidad de que el *malware* proviniera de una publicidad o de un sitio legítimo.

Debido a que los métodos de ataque eran cada vez más complejos y las superficies de ataque cada vez mayores, los profesionales de la seguridad se dieron cuenta de que era imposible prevenir todas las infecciones por *malware*. Así, se diseñó una nueva estrategia para proteger

los endpoints a la par del desarrollo de las EPP. Esta nueva estrategia es conocida como detección y respuesta para endpoints (*endpoint detection and response*, EDR).

Un EDR es un programa que sirve para detectar e investigar actividades sospechosas en endpoints y responder a ellas. Comenzó como una herramienta digital de investigación forense que brindaba a los analistas de seguridad la información sobre amenazas y las herramientas necesarias para analizar un ataque e identificar los indicadores de compromiso (IoC). De esta manera, los analistas podían detectar los *malware*, algunos de los cuales permanecían ocultos en las redes durante meses o años. En lugar de investigar un ataque para conocer su anatomía, esta herramienta también se utilizaba para detectar en tiempo real un ataque en curso. Además, se agregaron herramientas de remediación, que permitían a los analistas solicitar más información sobre endpoints o aislarlos, inhabilitar procesos o bloquear determinadas IP. Los EDR se convirtieron en una verdadera solución de detección y respuesta, pero no estaban exentos de problemas.

Los EDR de primera generación utilizaban en su mayoría métodos manuales que insumían mucho tiempo y eran demasiado lentos para las amenazas dinámicas como los *ransomware*. La falta de integración con otros programas de seguridad disminuía su capacidad para responder de manera efectiva y a tiempo. La configuración y el uso de los EDR requerían conocimientos avanzados, y el análisis de una gran cantidad de alertas, muchas de las cuales eran falsos positivos, llevaba mucho tiempo a los analistas. Los proveedores mitigaron parcialmente estos problemas al introducir una plataforma de detección y respuesta administrada (*managed detection and response*, MDR), que llevaba a cabo una clasificación básica de alertas y notificaba a los analistas por correo electrónico. Aun así, los EDR seguían siendo demasiado lentos y complicados para convertirse en una herramienta estándar dentro del arsenal de programas de seguridad para endpoints.

Los EDR de segunda generación apuntaban a estos aspectos. Se diseñaron para funcionar orientados a políticas y de manera automatizada. Mediante manuales personalizables, ahora los analistas pueden utilizar un EDR para remediar estos problemas de manera inmediata y

automática. También pueden ordenar proactivamente al EDR que responda de cierta manera cuando detecte un programa o *script* que se comporta de manera sospechosa. Las actividades maliciosas disparan bloqueos automáticos para prevenir la extracción y el cifrado de datos y los intentos de infiltraciones en la red. Los EDR pueden detener y revertir los ataques de *ransomware* en tiempo real y sin necesidad de quitar el dispositivo o de interferir en la continuidad de una actividad.

Los profesionales de la seguridad notaron de inmediato las ventajas de fusionar las tecnologías de EDR y EPP, y la mayoría de las definiciones de EPP ya incluyen ambas características. Un único agente integrado puede prevenir la mayoría de los ataques de *malware* basados en archivos en la etapa previa a la infección y ejecución. Asimismo, puede detectar un *malware* que haya evadido la prevención y responder en una etapa posterior a la infección. Una solución combinada de EPP y EDR también elimina las preocupaciones sobre la integración y simplifica a los analistas la configuración y administración.

Los programas de EPP y de EDR ahora incluyen otros controles preventivos para mejorar la higiene de seguridad y, por ejemplo, alertan a los analistas cuando un endpoint no tiene el parche de seguridad más reciente o está ejecutando aplicaciones inseguras. Al identificar vulnerabilidades críticas, los equipos de seguridad pueden mitigar las amenazas y aplicar parches virtuales o diseñar políticas que impongan restricciones a los dispositivos terminales hasta que se instale un parche en el programa. Además, el aprendizaje automático (ML) ahora está incluido como parte de las capacidades mejoradas de los antivirus, lo que ayuda a detectar malware en la fase previa a la ejecución.

Las capacidades de detección y respuesta no sólo se aplican a los endpoints, ahora se pueden ampliar a toda la infraestructura de seguridad. Esto se denomina detección y respuesta extendidas o XDR. XDR implementa tecnología de IA adicional para proporcionar capacidades de detección y respuesta a velocidad de máquina con el fin de proteger no sólo los endpoints, sino también la red, la capa de acceso y la nube.

Los productos de Fortinet para seguridad de los endpoints son FortiClient® y FortiEDRTM.

El endpoint que ejecuta FortiClient® está completamente integrado con otros productos de seguridad que comparten datos de inteligencia y que se administran de forma centralizada en el denominado Fortinet Security Fabric. El producto de detección y respuesta extendidas de Fortinet se llama FortiXDRTM.

Gracias por su tiempo, y no olvide responder las preguntas a continuación.