FORTINET
NSE Training Institute

NSE 2 Threat Intelligence Services Scripts—Spanish Version

En esta clase, veremos cómo los proveedores de seguridad recopilan información sobre amenazas y brindan acceso a ese conocimiento para detectar comportamientos sospechosos en línea.

En los primeros productos antivirus para dispositivos terminales, los proveedores debían catalogar los virus conocidos para que los productos pudieran confirmar si un archivo estaba infectado o no. Para ello, los equipos de información sobre amenazas tomaban una muestra de cada virus y generaban una firma, que representaba el contenido del archivo. En otras palabras, era una huella digital. La lista de firmas de virus se distribuía con el software antivirus. Con el tiempo y la aparición de nuevos virus, los servicios de información sobre amenazas de cada proveedor distribuían actualizaciones de su lista de firmas de virus. Las actualizaciones se enviaban en forma periódica y de distintas maneras. Se lanzaban con una frecuencia mensual o trimestral y, en algunos casos, solo una vez al año.

A medida que los desarrolladores de malware adquirían experiencia, los programas maliciosos se volvían más complejos e incluían mecanismos para burlar los tradicionales análisis basados en firmas, ya que era posible cambiar el contenido del archivo a discreción. Y, como el contenido cambiaba, las firmas también lo hacían, por lo que los malware podían evadir los antiguos productos antivirus. Así, un único tipo de malware se convertía en una familia entera de hasta cientos de miles de archivos diferentes. A este fenómeno se lo conocía como malware polimórfico, y cada uno tenía el mismo comportamiento malicioso. Este inconveniente también se presenta con la venta de kits para desarrollar malware en la red oscura o "dark web", por no mencionar la proliferación de organizaciones de malware como servicio. ¡El ciberdelito tiene su propio modelo de negocio!

Así que tenemos un nuevo problema: el clásico enfoque individual de firmas, en el que cada archivo de malware conocido se representa con una única firma en el archivo de firmas, obviamente *no puede* escalar bien, debido a que, potencialmente, un malware puede adoptar millones de formas por día. Para hacer frente a esta capacidad de

mutación del malware, los servicios de información sobre amenazas de los proveedores crearon métodos para detectar familias enteras de malware mediante **una** sola firma. Esto se logra de diversas maneras, pero todas sirven para identificar puntos en común en una familia de malware.

Hasta ahora, hemos hablado de malware ya visto y que, por lo tanto, es conocido para los investigadores de un proveedor. Pero ¿qué sucede con un malware cuyas nuevas formas aún no han sido detectadas? Los métodos de detección basados en firmas no sirven. Por eso, los proveedores crearon los productos de sandbox, que llevan los archivos sospechosos a un entorno seguro para analizar su comportamiento en detalle. Si el archivo tiene una actividad maliciosa en el sandbox, se marca como malware. Este método, conocido como detección heurística, busca comportamientos anómalos o poco habituales. De hecho, los proveedores crean algoritmos heurísticos propios que pueden detectar muestras desconocidas de malware polimórfico.

Según el producto de sandbox y su configuración, el usuario no solo puede propagar esta nueva información a través de su entorno de seguridad de red, sino que también puede enviar los detalles al servicio de información sobre amenazas del proveedor y compartirlos a escala global para proteger a más personas.

Más allá de los entornos de sandbox, en el futuro, el servicio de información sobre amenazas utilizará la inteligencia artificial y el aprendizaje automático para detectar malware desconocido y clasificar rápidamente el potencial de amenaza de seguridad de los archivos que atraviesan la red. Y no se trata solo de archivos. El servicio de información sobre amenazas cataloga el conocimiento sobre ataques existentes o emergentes, lo que incluye:

- los mecanismos específicos del ataque
- la evidencia de que el ataque ha ocurrido, también conocida como indicadores de compromiso o IoC
- las consecuencias del ataque
- la identificación del atacante

- y sus posibles motivaciones

A medida que las técnicas utilizadas por los agentes maliciosos evolucionan y se vuelven más complejas, es más importante que nunca compartir en tiempo real la información sobre amenazas en todo el entorno de seguridad de red. Si algunos componentes de seguridad detectan ataques mientras otros esperan actualizaciones periódicas de firmas, los atacantes pueden evadir las defensas y ocasionar daños. Los productos de seguridad y los servicios de información sobre amenazas que actúan juntos y en tiempo real tienen las mejores probabilidades de detener estos ataques.

Además, el intercambio de información sobre amenazas no se limita a la línea de productos de cada proveedor. Podría pensarse que, después del trabajo necesario para recopilar, analizar y catalogar la información sobre amenazas, cada proveedor la mantiene en secreto. Sin embargo, casi todos los proveedores comparten la información con la comunidad de seguridad en general. Esto es posible a través de membresías oficiales en organizaciones como la Cyber Threat Alliance, los equipos de respuesta ante emergencias informáticas o CERT, sean locales, nacionales o internacionales, así como numerosas asociaciones de confianza privadas con otros proveedores, investigadores de seguridad independientes y autoridades. El intercambio en tiempo real de la información sobre amenazas permite obtener un panorama más completo del ataque, dado que ningún proveedor por sí mismo tendrá todos los datos. Lo que distingue a los proveedores no es la información, sino lo que hacen con ella y con la tecnología de sus productos.

Aquí es donde Fortinet se destaca. Nuestro servicio de información sobre amenazas se conoce como FortiGuard® Labs. Cientos de investigadores de FortiGuard® Labs de diez disciplinas de seguridad distintas exploran el panorama de las ciberamenazas y buscan proactivamente nuevas vías de ataque a diario para descubrir (y, en el mejor de los casos, prevenir) las amenazas emergentes. La protección de seguridad de FortiGuard® Labs, que está probada y certificada, brinda servicios de seguridad integrales, actualizaciones y protección para toda la gama de soluciones de Fortinet Security Fabric.

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