¿QUÉ SIGUE PARA LOS ANTIVIRUS?

Traducción de white paper “WHAT'S NEXT FOR ANTIVIRUS?” de DeepSecure, Junio 2021

RESUMEN

Los antivirus están bajo asedio. Los enfoques basados en la detección en el que se han basado los últimos 40 años ya no es capaz de derrotar constantemente a los ciberdelincuentes actuales. En esta traducción de un breve libro electrónico, examinamos lo que nos ha traído hasta este punto y cómo un nuevo enfoque al problema del malware es el siguiente paso evolutivo lógico para los antivirus.

UN PROBLEMA DEL SIGLO XX

Desde el intercambio de correos electrónicos, las interacciones de los medios sociales en la web hasta los dispositivos habilitados en internet y las transacciones máquina a máquina, la tecnología genera la información digital que es el alma[1] de cualquier organización.

Por otro lado las organizaciones están fuertemente integradas unas con otras formando parte de una ecosistema tecnológico complejo, esta información digital es compartida y comunicada con socios, clientes, cadenas de suministro, así como con trabajadores locales y remotos.

La información compartida en esta escala crea un problema peculiar del siglo xxi: una potencial enorme superficie de ataque para los cibercriminales y que puede ser resumida en una única palabra, datos.

EL DILEMA DE LOS DATOS

La información del negocio que cualquier organización desea enviar o recibir - está envuelta en datos. Básicamente, las organizaciones quieren compartir información, pero para hacerlo deben aceptar los datos que la contienen y ahí es donde se oculta el malware. La información entrante está envuelta en datos y puede contener malware oculto.

Un formato de archivo, por ejemplo, es un contenedor de datos que representa la información comercial en una estructura predefinida. Para hacer esto, necesita poder soportar todos los diferentes elementos de información que podrían estar presentes en el archivo. Incluso para formatos de archivo simples como Windows Bitmaps, existen los datos

[1] 102,6 trillones de correos se envían y reciben cada año (OptinMosters). 63.2% de la población mundial tiene acceso a internet (Boadbandsearch.net). Se espera que el mercado de la transformación digital crezca a una tasa de crecimiento anual compuesto del 23% desde 2019 hasta alcanzar los $ 3.3 billones para 2025. (Research and Markets)

de píxeles reales: la imagen en sí, pero también información sobre el tamaño de la imagen y la paleta de colores que se debe representar.

Las aplicaciones complejas como por ejemplo Microsoft Office[2] pueden almacenar muchos más tipos de información junto con las palabras que componen el documento, desde metadatos hasta información sobre fuentes y registros de cambios. Todo esto debe estar representado de manera que las aplicaciones lo puedan acceder fácilmente y, por lo tanto, el formato de archivo debe ajustarse a eso. Los diferentes formatos manejan la información de diferentes maneras, algunos van de arriba hacia abajo, otros de abajo hacia arriba, algunos con encabezados que identifican el contenido y otros sin él. Algunos tienen relleno o contienen áreas del archivo que no se utilizan y no afectan la apariencia del archivo cuando se abre.

Este nivel de complejidad crea oportunidades para que los atacantes prueben crear exploits. Se necesita un software de aplicación complejo para manejar estos formatos. El software complejo puede fallar y, por lo tanto, puede ser explotado. Casi todos los ataques cibernéticos que aparecen en los titulares a diario se inician desde algún tipo de formato de archivo complejo, como un archivo PDF o un documento de Office. Algunos utilizan la funcionalidad que ofrecen estos formatos para ejecutar contenido activo como macros, mientras que otros aprovechan los errores de software en aplicaciones que manejan las estructuras complejas que permiten a un atacante ejecutar su propio código.

EL RETROCESO CON LA DETECCIÓN

La superficie de ataque de una organización promedio[3] ha crecido exponencialmente en los últimos años. En respuesta, ha aumentado el número de tecnologías defensivas. Pero todas estas defensas se basan hasta cierto punto en el concepto de detección.

Ya en el 2012, el periodista estadounidense y veterano de la industria Brian Krebs causó revuelo cuando observó que, en promedio, el software antivirus solo tenía un 25% de éxito en la detección de malware. Los tiempos han cambiado y las defensas se han vuelto más sofisticadas. Ahora, las estadísticas de la eficacia del software antivirus se encuentran en un rango entre el 82% y el 96%. ¿Suena bien? Bueno, si el promedio está alrededor del 90%, 1 de cada 10 intentos de penetrar las defensas antivirus basadas en la detección de una organización tendrá éxito. Dicho así las probabilidades no parecen tan geniales[4].

La razón por la que las probabilidades no son buenas es que el antivirus basado en la detección sólo puede detectar lo que ha "visto" antes. Ha habido intentos de mejorar las

---

[2] "El 70% de todas las infecciones provienen de vulnerabilidades de Microsoft Office". (Kaspersky Lab)

[3] Travelex Diciembre de 2019: un ataque obligó a la empresa a eliminar sus sitios web en 30 países en un intento por contener un virus y proteger sus datos. Muchos de ellos seguían sin conexión dos semanas después. En agosto de 2020, la compañía fue absorbida por un consorcio de acreedores, citando una combinación del ataque de ransomware y la pandemia de coronavirus como razones clave de su fracaso.

[4] Maersk 2017: un ataque de zero day provocó la destrucción de todos los dispositivos del usuario final, incluidas 49.000 computadoras portátiles. 1.200 aplicaciones quedaron inaccesibles y aproximadamente 1.000 fueron destruidas. Alrededor de 3500 de los 6200 servidores fueron destruidos. El presidente Jim Hagemann Snabe le dijo al Foro Económico Mundial en Davos que el ransomware le costó a Maersk entre $ 250 millones y $ 300 millones.

probabilidades. Los entornos de sandboxing pueden ayudar, pero los atacantes han aprendido a detectarlos y aún confían en la detección para intentar identificar las amenazas.

Los algoritmos de inteligencia artificial y aprendizaje automático son útiles, pero en realidad solo utilizan la potencia informática para tratar de detectar una amenaza que ya se había visto más rápidamente. El problema, por supuesto, es que los ciberdelincuentes buscan constantemente atacar una organización con malware que la defensa no ha visto antes y, por lo tanto, considera seguro.

Las defensas basadas en la detección por sí solas simplemente no pueden mantenerse al día.

ANTIVIRUS BAJO ASEDIO

Si bien casi todos los avances en las defensas de ciberseguridad de los últimos 40 años se han basado en el paradigma de detección[5], los ciberdelincuentes han estado desarrollando sistemáticamente nuevas formas de evadir el proceso de detección y entregar malware oculto en los datos de los formatos de archivo que todos usamos en nuestro trabajo diario.

- Ataques de día cero: en 2017, IBM estimó que hubo 4 nuevos ataques de día cero por segundo durante el año.
- Malware sin archivos: código ejecutable que utiliza software autorizado en la computadora host para ejecutarse en la memoria y que puede ser prácticamente imposible de detectar.
- Archivos polimórficos: por ejemplo, un archivo que se ve y se comporta como una imagen, pero se puede abrir como, por ejemplo, un archivo html y ejecutará un script ejecutable. De nuevo, imposible de detectar.
- Esteganografía de imagen: un exploit codificado en los datos de píxeles de una imagen (valores de color y transparencia). Los secretos ocultos mediante la esteganografía de imágenes no se pueden detectar. Solo aquellos que codifican el secreto original en el archivo saben que está ahí y tienen la clave para decodificar y extraer lo que está oculto en su interior.

Las técnicas adoptadas por los ciberdelincuentes en la actualidad están diseñadas para evitar la detección. A menudo, estos ataques se centran en organizaciones específicas, están dirigidos. Un ataque probablemente solo se usa una vez, por lo que tiene muy poco tiempo de vida. La próxima vez que se utilice, se realizará un cambio en el ataque y estará dirigido a una nueva organización. Frente a un ataque tan concertado, las defensas antivirus basadas en la detección están bajo asedio. Ellas necesitan ayuda.

Cuando los investigadores de Deep Secure enviaron una muestra del virus Emotet a un sitio web de detección de malware popular que aloja la mayoría de los principales motores antivirus del mercado, alrededor del 75% de ellos lo identificó correctamente como una amenaza. Pero el más mínimo cambio en la muestra de Emotet hizo que la tasa de éxito se desplomara. Al agregar una simple línea de comentarios HELLO WORLD al script de

[5] Punto de vista del líder de TI: "Todos los virus que he eliminado durante los últimos 20 años estaban en una computadora con un software antivirus comercial que lo protegía". Nick Ioannou, Líderes de TI en informática 2019 250, autor de ciberseguridad, bloguero y orador.

macro, el porcentaje que identifica correctamente la muestra como maliciosa cayó al 34%. Al tomar esta versión modificada y copiarla y pegarla en un documento de Word diferente con contenido de cuerpo diferente, la tasa de éxito cayó al 20%. Los cambios son triviales, pero destacan el hecho de que la detección simplemente no puede seguir el ritmo de un malware como Emotet que cambia y se perfecciona constantemente.

ORIENTACIÓN EXPERTA

Cuando se trata de protección contra ataques dirigidos o diseñados de forma única, tanto los analistas de la industria como los expertos gubernamentales reconocen la necesidad de soluciones que puedan reforzar los antivirus basados en la detección.

A principios del 2021, el National Cyber Security Centre (NCSC) del Reino Unido publicó pautas sobre cómo proteger sistemas confiables de ataques, recomendando técnicas defensivas como la transformación para tratar los tipos de datos complejos (por ejemplo, archivos de Office, imágenes y PDF) utilizados por los atacantes para transportar malware.

Estas pautas se basan en décadas de investigación cuidadosa sobre la mejor manera de proteger sistemas gubernamentales clasificados de los ataques de ciberdelincuentes expertos, incluidas las agencias de inteligencia de los estados nacionales. A primera vista, adoptarlos es una obviedad. Pero, ¿pueden transponerse fácilmente al mundo comercial convencional? ¿Cómo es una defensa basada en la transformación? ¿Y exactamente cómo ayudará?

UN ANTIVIRUS TRANSFORMADOR

Una tecnología antivirus basada en la transformación es diferente porque no utiliza detección. Cuando se le presenta un archivo (el tipo en el que a los atacantes les gusta ocultar el malware, como un documento de Microsoft Office o PDF), no busca la amenaza, sino que busca la información comercial válida y la entrega.

Entonces, en el caso de un PDF, la defensa extraerá la información comercial válida del archivo (palabras, imágenes, estructuras de píxeles), descartará el original, verificará el contenido extraído y luego creará un archivo nuevo con solo la información comercial válida para entregar únicamente eso. Es un enfoque que es el polo opuesto de una defensa basada en la detección y tiene el potencial de resolver el dilema de los datos de una vez por todas. No se basa en la detección de datos no seguros. En cambio, transforma los datos en algo que es simple y obviamente seguro, por lo que se elimina cualquier amenaza presente. Esta transformación ocurre incluso si no hay ninguna amenaza: los datos se transforman de todos modos, lo que garantiza una verdadera confianza cero.

Este enfoque basado en la transformación ofrece una serie de beneficios potenciales. Debido a que no utiliza la detección, el atacante no puede adivinar la defensa. Debido a que no utiliza definiciones de firmas para identificar amenazas, no necesita parches y actualizaciones constantes. Y debido a que siempre entrega archivos libres de malware, tiene el potencial de reducir los costos de SOC asociados con el monitoreo, la aplicación de parches y la reparación.

Las organizaciones que buscan agregar transformación a su arsenal defensivo deben observar detenidamente las tecnologías que se ofrecen. Al hacer una selección, deberán considerar soluciones que ofrezcan algunos o, idealmente, todos los siguientes:

- Velocidad: el proceso de transformación debe ser muy rápido. La ciberseguridad a menudo se percibe como un inhibidor del crecimiento y la tecnología elegida debe entregarse con una latencia cercana a cero si se quiere cumplir con las expectativas del usuario empresarial y facilitar el crecimiento empresarial.
- Transparencia: la transformación DEBE entregar un archivo de píxeles perfectos al usuario que no debe saber que se han aplicado controles de seguridad que han dado como resultado la entrega de un archivo desinfectado completamente nuevo.
- Facilidad de integración: Compatible con interfaces estándar de la industria para la integración con defensas antivirus basadas en detección existentes.
- Facilidad de implementación: debe admitir la integración en implementaciones locales, virtuales y nativas de la nube.
- Procesos separados: para la extracción, verificación y construcción, las fases de la transformación ayudan a proteger la defensa de ser explotada con éxito.
- Verificación (opcional) en hardware: el uso de FPGA para verificar la información comercial extraída en la lógica del hardware, evita que los atacantes eludan o tomen el control de la defensa.
- Roturas de protocolo: Para detener ataques en los protocolos utilizados para transferir la información.
- Flujos de datos unidireccionales: por ejemplo, para detener el uso de un canal de importación de datos como conducto para filtrar datos.

CONCLUSIÓN

Una defensa verdaderamente eficaz necesita utilizar tanto la transformación como la detección. El antivirus basado en la detección puede continuar monitoreando los límites del perímetro, en busca de amenazas "conocidas" o vistas anteriormente.

Si se parchea y mantiene de forma adecuada, probablemente funcionará con una eficacia de entre el 84 y el 96%. Paralelamente, la transformación someterá cada archivo e imagen a un proceso de desinfección que lo liberará de todas las amenazas, incluso el malware de día cero y completamente desconocido, operando con 100% de eficacia.

Este enfoque cambia las reglas del juego, un verdadero enfoque de confianza cero para el intercambio de información sin malware. Tiene el potencial de ofrecer inmunidad completa contra el malware ahora y en el futuro. La transformación es el siguiente paso evolutivo lógico para las defensas antivirus porque es la única manera de estar absolutamente seguro de que un archivo está libre de amenazas, robarle al atacante su capacidad para esconderse de la detección y reducir drásticamente los costos de monitoreo, parcheo y corrección.