STORMSHIELD

ARTÍCULOS DE OPINIÓN

SOLUCIONES DE PROTECCIÓN DE PUESTOS DE TRABAJO Y ANTIVIRUS: ¿CUÁL ES LA DIFERENCIA?

Julien Paffumi
Product Portfolio Manager,
Stormshield

Ha pasado casi una década desde que se anunciara la muerte de los antivirus tradicionales, pero siguen siendo muy populares entre el gran público. Aunque sigue siendo un término de uso común en el mundo de la informática, el antivirus ya no es lo que está de moda. He aquí por qué.

El uso de software antivirus tradicional parece ahora obsoleto, y los términos «Antivirus de nueva generación» (NGAV), «Plataforma de protección de puestos de trabajo» (EPP) y «Detección y respuesta en puestos de trabajo» (EDR) han ocupado su lugar. ¿Cuáles son las diferencias entre todas estas tecnologías de detección? ¿Seguimos necesitando un software antivirus hoy en día? En este documento respondemos a estas preguntas.

¿SIGUEN OFRECIENDO LOS ANTIVIRUS UNA PROTECCIÓN FIABLE?

El software antivirus es un programa informático diseñado para ser instalado en dispositivos individuales como ordenadores, tabletas y teléfonos con el objetivo de detectar y eliminar software malicioso. Desarrollado por primera vez por IBM en 1987 en respuesta al virus informático «Brain», **el término «antivirus» se ha popularizado a lo largo de los años con una gran notoriedad, convirtiéndose en la única defensa contra los virus informáticos en el imaginario colectivo.**

Estos programas antivirus funcionan según el principio de la búsqueda de firmas. «*Al igual que una vacuna, el antivirus dispone de una base de datos de firmas que le permite reconocer un virus informático. Por lo tanto, es esencial que la firma de este virus específico se haya generado previamente*», explica **Stéphane Prévost,** Product Marketing Manager Stormshield. Este método de funcionamiento genera diversos problemas y limitaciones. El primero de ellos es que ya es necesario estar familiarizado con el virus antes de poder identificar su firma (y ser capaz de combatirlo). El segundo problema – y no menor – es la aparición del polimorfismo, una técnica para generar archivos maliciosos cuya firma digital es única para cada archivo, pero cuyo método de infección y carga útil siguen siendo comunes. Esta limitación es tanto más significativa dado que cada día se crean 450.000 nuevos programas maliciosos, es decir, casi 4 millones al mes, según el Instituto AV-TEST. Como consecuencia directa de esta explosión, es técnicamente imposible que el software antivirus tenga conocimiento previo de todas las firmas... Peor aún para el software antivirus, el modus operandi de los ciberdelincuentes no ha dejado de evolucionar en los últimos años, hasta el punto de ocultarse en puntos ciegos de los algoritmos de detección, como el «malware sin archivos». ¿Y el resultado? Los mecanismos de detección basados en la búsqueda de huellas digitales en un archivo dejan pasar la inmensa mayoría de los programas maliciosos, y deben complementarse con otras técnicas de protección.

La evolución de los ciberataques, cada vez más sofisticados, está convirtiendo incluso al propio software antivirus en un objetivo. Por ejemplo, en la conferencia «Black Hat Europe» de diciembre de 2022, un investigador de seguridad reveló una vulnerabilidad nunca vista que afecta a varios programas antivirus. Este fallo permite apoderarse del software antivirus y eliminar archivos legítimos. Entonces, ¿qué podemos hacer cuando nuestra principal herramienta de protección ya no cumple su función?

LA LLEGADA DE LA DETECCIÓN DE COMPORTAMIENTO EN LOS PUESTOS DE TRABAJO

En respuesta a esta nueva situación, l**os fabricantes de ciberseguridad tuvieron que idear un nuevo enfoque, pasando de las huellas digitales al análisis heurístico basado en el comportamiento del usuario**. Denominados Next-Gen Antivirus o NGAV, estos nuevos tipos de antivirus constituyeron la base de lo que se conoció como Endpoint Protection Platform (EPP). Las soluciones EPP ofrecieron una respuesta inicial al polimorfismo y a los ataques sin archivos al integrar nuevas funciones como la supervisión de la memoria, el análisis del comportamiento y la verificación de los indicadores de

compromiso (IoCs). A pesar de este avance tecnológico, los ciberataques insidiosos seguían colándose por las rendijas. Por lo tanto, se hizo imperativo detectarlos, incluso después de que se hubieran producido, y responder a ellos.

Esta fue la observación que motivó la aparición de las soluciones *Endpoint Threat Detection & Response* (ETDR) en 2013 en los análisis de Gartner, basados en los temas de respuesta frente a incidentes e investigación. A partir de 2015, el acrónimo ETDR se sustituyó por EDR para *Endpoint Detection & Response*. La particularidad de este nuevo enfoque reside en la capacidad de detectar y responder a amenazas desconocidas en tiempo real de forma semiautónoma, como señala **Noël Chazotte**, Product Manager Stormshield: «*Si detecta una amenaza, un antivirus bloqueará el programa en la fase inicial, a veces poniéndolo en cuarentena. El EDR, por el contrario, entra en acción una vez que el incidente de seguridad se detecta o ya se ha producido en la máquina, e intenta determinar lo que ha sucedido a nivel de máquina para ayudar a los equipos operativos a evitar que la infección se propague*».

¿Cómo detecta la tecnología EDR los ataques sofisticados? «*El EDR identifica comportamientos anómalos mediante indicadores de compromiso (IoC), explica Stéphane Prévost. No siempre se trata de sucesos excepcionales; pueden ser acciones habituales, como abrir una conexión a un servidor externo*». De ahí la importancia de definir con precisión el marco de funcionamiento de la solución durante la fase de aprendizaje para evitar los «falsos positivos». Pero las soluciones EDR y EPP siguen siendo complementarias, como señala Stéphane Prévost: «*Se puede hacer una analogía con la seguridad física de una empresa. La solución EDR es como las cámaras de vigilancia: te permiten ver, por ejemplo, si un intruso está entrando en tu recinto industrial. Pero para impedirle la entrada, hace falta un guardia de seguridad in situ: es el EPP*».

Entonces, ¿dónde encaja el antivirus en todo esto? En 2023, según el sitio web security.org, tres de cada cuatro estadounidenses creen que necesitan un antivirus para poder utilizar su ordenador personal con tranquilidad. Dados los avances tecnológicos mencionados, surge la pregunta a nivel profesional: **¿por qué seguimos necesitando un software antivirus hoy en día?** Y la respuesta es: simplemente porque proporciona una primera capa de seguridad. Aunque esta solución no será eficaz contra todos los ciberataques, proporciona un nivel inicial de protección contra los ataques menos sofisticados – con la garantía de evitar el problema de los falsos positivos y de consumir muy pocos recursos en la estación de trabajo. Pero una primera capa de seguridad implica la existencia de otras. «*Estamos viendo varias soluciones de protección instaladas en la misma máquina, explica Noël Chazotte. Sin embargo, combinarlas no siempre es una estrategia acertada, ya que algunas de ellas pueden provocar conflictos, dejando otra puerta abierta a los ciberdelincuentes*».

NDR, XDR, MDR: UNA TENDENCIA HACIA LA ESPECIALIZACIÓN EN LA DETECCIÓN Y RESPUESTA

A pesar de la promesa de funcionamiento sin intervención humana de este tipo de soluciones, la gestión de estas herramientas debe ser supervisada por expertos, como demuestra el desarrollo de ofertas de EDR gestionado o mini-SOC. **Además de mejorar la detección, es esencial que las herramientas de protección de puestos de trabajo incluyan capacidades de detección y respuesta frente a incidentes.** Y dada la proliferación de puntos de recolección de incidentes, un analista SOC debe tener acceso a todos los equipos de red e infraestructura.

Por ejemplo, las soluciones Network Detection and Response (NDR) analizan los paquetes TCP/IP que pasan por la red para detectar actividades sospechosas. El sistema XDR (eXtended Detection and Response) pretende combinar todos los activos informáticos internos y externos (red, directorios, recursos en la nube, cortafuegos, etc.) para ofrecer una visión global de los eventos en el sistema de información. Según Noël Chazotte, «*una plataforma XDR es un conjunto de puntos de recolección y, sobre todo, una plataforma de correlación para ayudar a mitigar el riesgo y proporcionar un grado de respuesta y remediación*».

En los últimos años han surgido otros acrónimos, como MDR. En la práctica, «Managed Detection and Response» (MDR) es simplemente un modo de comercialización de un XDR en el que un equipo humano externo gestiona las alertas. Sea cual sea la herramienta y la tecnología, hay que tener en cuenta que el papel del analista sigue siendo central y que ninguna tecnología ofrece por sí sola una seguridad suficiente para un activo sensible.

Según un estudio de Survey Risk Alliance, solo el 12% de los profesionales de la ciberseguridad afirma haber adoptado una solución XDR en su organización para 2022. El 77% restante afirma que tiene previsto adoptar una en los próximos 24 meses. Por lo tanto, se espera que la demanda de expertos en seguridad especializados en detección y respuesta frente a incidentes siga creciendo en los próximos años. Porque a pesar de los avances tecnológicos, la intervención humana sigue siendo esencial para analizar y comprender los incidentes. Estos perfiles son muy solicitados en respuesta a la constante evolución de los métodos operativos, y sus servicios serán sin duda más fácilmente accesibles para las empresas a través de ofertas de EDR gestionadas o mini-SOC.