

Develando mitos sobre soluciones antivirus

En este artículo, revisaremos las falacias más importantes en torno a la moderna industria antivirus y analizaremos las capacidades reales y las limitaciones de dichas aplicaciones.

Introducción

Un programa antivirus es un componente importante de cualquier paquete completo de seguridad, que cualquier usuario que desee estar protegido, debería tener en su escritorio.

El antivirus lo ayudará a evitar diversos tipos de amenazas.

Es una herramienta indispensable para verificar la seguridad de todos los archivos y mensajes de correo electrónico entrantes antes que los mismos sean abiertos.

Sin embargo, el antivirus es considerado erróneamente una solución integral que lo defenderá para siempre contra todos los enemigos modernos que amenazan su seguridad.

Esta creencia no está ni siquiera cerca de la realidad, dado que el programa antivirus tiene serias limitaciones si se utiliza de manera aislada.

Tipos de amenazas

Virus, programas espía, troyanos y gusanos continúan siendo el foco de los problemas tanto para usuarios hogareños como corporativos.

Estas amenazas mejoran, constantemente, su resistencia contra verificaciones de seguridad y fortalecen su impacto disminuyendo los beneficios de los procedimientos de mitigación sobre los sistemas afectados.

Antes de lanzar su cría en la jungla, los fanáticos desarrolladores de virus verifican hasta el cansancio sus programas **maliciosos** en busca de una larga lista de programas antivirus y aplicaciones contra programas espía.

De esta forma, se aseguran que no serán detectados por la mayoría de las más recientes definiciones de firmas de virus / programas espía.

Este enfoque complica los esfuerzos de detección de las compañías de seguridad.

Una multitud de foros de piratas y *blogs* han surgido últimamente donde se analizan las vulnerabilidades de seguridad y se comparten las formas de sortear la detección antivirus.

Dicha industria está tratando de ponerse al día con esta comunidad clandestina, que tiende a estar un paso adelante (salvo escasas excepciones) contando con mayores datos sobre vulnerabilidades disponibles.

El año pasado, ciertos proveedores comenzaron a enviar una advertencia, que solicitaba a los usuarios, actualizar sus equipos con parches para evitar que sus sistemas se infectaran a través de un archivo especialmente diseñado después de realizar una verificación.

Lo extraño es que el problema se mantuvo recurrentemente durante un periodo de tres meses, creando la incertidumbre acerca de la incapacidad de la industria de crear productos seguros y sin virus.

Los agresores diseñan formas cada vez más crueles y maliciosas de intimidar a sus víctimas.

Realizan extorsiones en línea y actividades de crimen organizado.

Por ejemplo, envían programas maliciosos que encriptan los documentos de las víctimas y luego solicitan dinero para que sean descryptados y utilizados libremente.

Esos programas utilizan métodos de tipo viral para infectar los sistemas y pueden eliminarse solamente después que la víctima haya pagado un rescate o el programa antivirus lo haya desinfectado.

Es una tendencia nueva y alarmante que va un paso más allá de los esquemas de intimidación tradicionales.

El tiempo de reacción contra la epidemia de virus es otro problema grave de la actualidad.

Se estima que la brecha de tiempo entre el lanzamiento de un virus y la respuesta del proveedor más expeditivo (emitiendo una huella dactilar para detectar la nueva muestra de virus) oscila entre algunas horas y hasta varias semanas.

Eso es mucho tiempo y puede generar severos daños considerando la velocidad a la que se propagan las nuevas amenazas.

Los ataques de día cero y los ataques provenientes del olvido del usuario de realizar actualizaciones de firmas, en tiempo y forma, son las fuentes más importantes de las pandemias de virus.

Mientras los programas antivirus continúen dependiendo, en gran medida, de la detección por firmas, la defensa estará siempre rezagada con respecto a la ofensiva.

Esto convierte al programa antivirus en una herramienta poco efectiva para combatir las nuevas amenazas no contenidas.

El crecimiento de las técnicas de ingreso furtivo a sistemas vulnerables, también parece estar proliferando.

Estas técnicas, llamadas *rootkits*, esconden la presencia de un archivo en un sistema (es decir, código malicioso) al interceptar las funciones de la interfaz de programación de aplicaciones del sistema.

Los *rootkits* engañan a los programas tipo Explorador de Windows, al no mostrar los verdaderos contenidos de una carpeta.

La ejecución de tareas también se manipula, de forma tal que una aplicación maliciosa puede encubrir su presencia en la memoria y ejecutar procesos en el ordenador.

La mayoría de los modernos programas antivirus no ha aprendido a detectar de manera confiable y a combatir los *rootkits*.

Por lo tanto, la mayor parte del código malicioso complejo que utiliza métodos intrincados, pasará probablemente desapercibida.

Detección de código malicioso: donde la mayoría de los programas antivirus fallan

La detección de amenazas sigue siendo el control más importante para desafiar a los virus modernos.

Actualmente, las soluciones complementarias son también necesarias porque los analizadores de comportamiento (más conocidos como verificaciones heurísticas) en general, no detectan el 100% de las amenazas y muchos programas no son eficaces para desterrar *rootkits*.

A menudo el programa antivirus que detectó con éxito la versión anterior de un virus no lo logra con una versión posterior porque se ha modificado para evitar dicha detección.

Los falsos positivos siguen acechando a la industria. Si bien no se conocen las cifras concretas, los falsos positivos (objetos legítimos identificados erróneamente y tratados como maliciosos) representan más del 1% del total de los resultados de las verificaciones efectuadas.

Una cantidad muy importante, ya que un archivo borrado o modificado accidentalmente puede generar graves problemas, y costes.

No hace mucho tiempo, se decía que un importante programa antivirus corporativo había borrado, por error, un archivo ejecutivo de la dirección de administración de trenes en Japón.

El error paralizó el tráfico y se debió realizar un esfuerzo significativo para solucionar la situación.

Los problemas de rendimiento, si bien no son tan críticos, afectan seriamente la productividad laboral y la experiencia de los usuarios hogareños.

Es común que el módulo residente de cualquier antivirus moderno (análisis en el acceso), salvo escasas excepciones, utilice alrededor del 80% del total de la potencia del procesador y una buena parte de la memoria.

Puede ver claramente este agotamiento cuando instala un producto de más de 4Gb o ejecuta un juego que utiliza el procesador en gran medida con el control de virus activo.

La capacidad de juego se reducirá de manera visible.

Eliminación y mitigación de la amenaza

Después que el programa antivirus detectó un virus, el siguiente paso es eliminarlo.

Esto puede suponer un gran reto, dado que cada vez más virus tienden a replicarse en un sistema, mutar y descargar elementos hostiles adicionales desde Internet.

Un virus o gusano puede existir en cientos de lugares.

Varios virus pueden convivir e intercambiar componentes que eviten su eliminación y que sirvan como puntos de respaldo entre sí.

Dada la complejidad del problema, no es sorprendente que en algunos casos el programa antivirus no pueda erradicar por completo la amenaza.

La tarea de eliminar código hostil de un archivo, al mismo tiempo que se mantiene la integridad original, puede resultar engañosa.

A menudo el programa antivirus se excede, y deja al programa o componente sin funcionar o completamente inútil.

Desafortunadamente, esto les sucede a muchos usuarios, que se quedan con archivos dañados como resultado de un intento, sin éxito, de parte del programa antivirus para tratar la amenaza detectada.

Recomendaciones para reforzar su seguridad

- Instale un cortafuegos para proteger su ordenador contra conexiones ilegítimas o innecesarias (Obviamente, recomendamos [Outpost Firewall Pro](#), que ofrece protección adicional contra programas espía) y evita conexiones generadas por código malicioso.
- Si bien no es recomendable la utilización de varios antivirus de acceso simultáneamente, el uso de módulos diversos a petición del usuario, puede permitirle tener una mejor visión del grado de protección que cada uno puede ofrecerle, existiendo versiones gratuitas (como [ClamAV](#) o [Antivir](#)) y comerciales, como [Eset NOD32](#).
- La mayoría de los sitios de Internet de las soluciones antivirus le ofrecen la posibilidad de enviar archivos sospechosos para su análisis, lo cual también le dará una mejor perspectiva de las posibilidades de cada uno.
- Efectúe copias de respaldo con periodicidad y, si su información es crítica, consulte con su asesor técnico, quien le ayudará a diseñar una política de seguridad acorde con su actividad.
- No trabaje bajo la cuenta de administrador hasta que la situación sea segura (utilice la cuenta de usuario restringido para navegar en Internet).
- Actualice su sistema y aplicaciones con los parches que periódicamente lance su proveedor.
- Pruebe utilizar un navegador alternativo a Internet Explorer, como por ejemplo Opera o Firefox.

Conclusión

Para una mejor protección, el programa antivirus debe utilizarse junto con otras medidas de seguridad y actualizaciones rápidas para el programa existente.

La mejor seguridad se logra con el mejor conocimiento.

Le recordamos algunos vínculos para obtener más información:

- [Advertencias de seguridad](#)
- [Descarga de manuales y documentos](#)
- [Glosarios](#)
- [Documentos complementarios sobre tecnología antivirus, seguridad informática y otras medidas de protección adicionales](#)
- [Enciclopedia Virus, una completa enciclopedia en español sobre virus informáticos](#)

✍ Traducción y adaptación: Ontinet.com, S.L.