¿Son eficaces las soluciones antivirus? (I)

Hoy en día la tasa de detección inicial de un virus de reciente creación es de menos del 5% y, aunque las empresas fabricantes hacen lo posible por modernizar sus mecanismos, los productos disponibles en el mercado parecen incapaces de competir con la velocidad de propagación de los virus en Internet. A algunos les lleva un mes o más actualizarse tras la primera exploración, mientras que los proveedores con las mejores capacidades de alerta son los que distribuyen sus creaciones de manera gratuita. Al menos ésas son las principales conclusiones a las que llega **"Assessing the Effectiveness of Antivirus Solutions"**, algo así como "Evaluando la eficacia de las soluciones antivirus", **un estudio publicado hace unas semanas por** la compañía especializada en protección de datos **Imperva y un grupo de estudiantes de The Technion** (Instituto Israelí de Tecnología).

El mismo estudio que ha levantado ampollas entre las firmas de seguridad analizadas porque, entre otras cosas, asegura que el gasto de corporaciones y clientes individuales en antivirus no es proporcional a su efectividad y que ambos tipos de usuarios deberían plantearse la exploración de nuevas medidas de cara a la protección de sus sistemas, como el modelo freeware. "En 2011, Gartner informó que los consumidores gastaron 4.500 millones de dólares en antivirus, mientras que las empresas invirtieron 2.900 millones, lo que hace un total de 7.400 millones. Esto representa más de un tercio de los 17.700 millones destinados en conjunto a software de seguridad", señala la investigación, que añade que se deberían aprovechar cada vez más las tecnologías que detectan un comportamiento aberrante "como la velocidad de acceso inusualmente rápida o un gran volumen de descargas", en vez de seguir por los mismo derroteros.

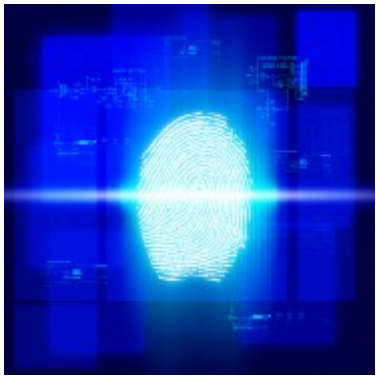
La metodología utilizada

Para armar este razonamiento, Imperva **enfrentó 82 muestras de malware con un total de 40 productos antivirus**, entre los que se encuentran ofertas tan conocidas como las de Microsoft, Symantec, McAfee o Kaspersky, tal y como os explicábamos al poco tiempo de su publicación. ¿Cómo se seleccionaron dichas muestras? Primero, se realizaron búsquedas en Google "con términos que nos acercaban a repositorios de malware esporádicos en páginas web de acceso público", explica ahora Amichai Shulman, CTO de la compañía. "Complementamos esto con algunos enlaces que obtuvimos a través de búsquedas esporádicas en foros de hackers soft-core. Nos centramos en foros de idioma ruso, sí, pero no creo que esto sea controvertido". Aunque **el conjunto de mayor peso fue suministrado por algunos enlaces "que tomamos de tráfico obtenido a través de servidores proxy anónimos"**, continúa describiendo el directivo. Todo este trabajo fue acometido **por personas "imparciales"**, no relacionadas con el negocio antivirus ni con el de la piratería.

¿Y cómo se rastreó todo este mejunje de malware? Imperva necesitaba una infraestructura para confrontarlo con el mayor número de productos antivirus posible, de forma repetida a lo largo del tiempo. Y esa infraestructura no fue otra que **VirusTotal, el conocido servicio (online y gratuito) de escaneo de archivos y URLs**, que permite identificar virus (como su nombre bien indica), gusanos, troyanos y demás categorías de contenido malicioso desde el punto de vista de las soluciones de protección. El experimento se repitió durante seis semanas, hasta almacenar un total de 13.000 entradas en una base de datos relacional para su posterior análisis. Cada una de estas entradas representa el resultado de analizar un archivo específico por un producto antivirus también específico, donde se indica si la muestra se identificó como malware y, en caso afirmativo, qué malware concreto fue detectado.

La opinión de los fabricantes

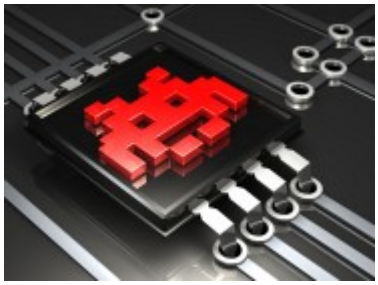
Precisamente, optar por VirusTotal como herramienta base ha sido uno de los principales flancos de ataque de los fabricantes de soluciones antivirus hacia un informe que ha recibido duros calificativos como **"broma de mal gusto"** (avast!), **"sesgado"** (Kaspersky) o **"insuficiente"** (Symantec), entre otras lindezas. "El estudio patrocinado por Imperva no evalúa ninguno de los productos en la forma en la que se utilizarían en situaciones reales en el ordenador de un usuario", señala César Cid, responsable de Tecnología para España y Portugal de la propia Symantec, una de las compañías más críticas en este asunto. "De hecho, la prueba está limitada en su alcance hasta el punto de proporcionar evaluaciones erróneas. El principal problema es que sólo examina uno de los aspectos de protección de los productos de seguridad -la basada en huellas dactilares- sin tener en cuenta todas las demás tecnologías de protección disponibles. En concreto, VirusTotal sólo explora cada archivo sometido al escáner de huellas dactilares de cada producto de seguridad".



"En un laboratorio podemos simular escenarios que creemos pueden ser similares a los reales pero, en realidad, difieren mucho de los entornos a los que usuarios domésticos y corporativos se enfrentan", añade María Ramírez, ingeniera de ventas sénior de Trend Micro, rechazando la validez de datos tan cerrados. "Las soluciones de protección frente a amenazas no pueden medirse en entornos simulados, ya que el máximo potencial de nuestras soluciones está en la nube, con nuestros servicios de reputación y detección en tiempo real". Y es que cuando un usuario tiene instalado un antivirus "cuenta con un gran número de medidas de seguridad adicionales", recuerda otro experto en la materia, Vicente Díaz, analista sénior de malware en Kaspersky Lab. "Esto es fácil de entender con una analogía: en Virus Total digamos que sólo se detecta un virus en caso que conozcamos su nombre y apellidos, mientras que en un sistema donde tengamos el antivirus instalado, a pesar de no conocerlo, lo detendremos cuando intente realizar una acción maliciosa".

Desde Fortinet también tiran de comparaciones: "testar antivirus basándonos en esta metodología es como esquiar en ropa interior para probar si ésta es efectiva. Sin llevar más capas, está claro que la ropa interior no va a mantenernos a salvo del frío. Lo que no implica que no sea útil", razona

el gerente sénior de su Equipo de Respuesta ante Amenazas para la región EMEA, Guillaume Lovet. "El objetivo de VirusTotal es ayudar a los usuarios a formarse una idea de si un archivo es o no malicioso, sometiéndole a uno de los filtros utilizados en productos antivirus, conocido como motor de análisis estático. Pero la superación de este filtro no significa que el archivo no pueda ser detectado por otro filtro de un antivirus real", concluye. O, dicho de otro modo, "**actualmente los antivirus cuentan con múltiples capas de protección** y el uso únicamente de las bases de firmas no muestra la protección real de la que disponen los usuarios", apunta Josep Albors, director del laboratorio de ESET España.



"Los antivirus utilizados hoy en día son mucho más que un motor anti-malware y medir su efectividad sólo en función de este elemento implica un enfoque muy limitado", opina por su parte Eddy Willems, portavoz de G Data. "**Que una amenaza no fuera detectada por VirusTotal no implica que otro módulo de ese mismo antivirus no lo hiciera**. Ningún fabricante de soluciones antivirus ofrece a sus clientes una solución basada exclusivamente en el escáner antivirus", sino que ésta se suele combinar con tecnologías anti-phising y anti-spam, sistemas IPS de prevención de intrusiones, heurísticas, cortafuegos y otros complementos no recogidos con dicha metodología. Y es que "los antivirus son una capa importante, pero deben ser complementados con otro tipo de soluciones de seguridad y, sobre todo, con la formación de los usuarios", observa David Ávila, manager de ecrime en S21sec.

[Página 2]

El aviso de VirusTotal

Lo cierto es que los propios responsables de VirusTotal advierten en la presentación del servicio colgada en su página web que esta herramienta no debería ser empleada para evaluar la eficacia del software, so riesgo de caer en inexactitudes. "**En VirusTotal estamos cansados de repetir que el servicio no fue diseñado como un instrumento para realizar análisis comparativos de antivirus**, sino como una herramienta que comprueba muestras sospechosas con varias soluciones y ayuda a laboratorios enseñándoles el malware que ellos no logran detectar. Aquellos que usan VirusTotal para realizar análisis comparativos de antivirus deben saber que están introduciendo muchos errores implícitos en su metodología", advierte el capítulo titulado como Mala Idea. "Por lo tanto, decir que al subir 'algunas' muestras a la página web de VirusTotal se puede evaluar un producto es, o bien estúpido, o bien una mentira absoluta", remacha Jindrich Kubec, director de Inteligencia de Amenazas de avast!.

Además de denunciar que Imperva no valoró los productos sino que simplemente cargó las muestras en una plataforma online, Kubec aduce que **la selección de malware fue "dudosa" y** que **el número de muestras era "demasiado bajo"**. En el mismo sentido se pronuncia Luis Corrons, director técnico de PandaLabs, que considera ridículo el hecho de mandar "unas docenas de muestras"

a VirusTotal, sobre todo "teniendo en cuenta que cada día detectamos 74.000 nuevas muestras de malware". Además, "si en las pruebas alguna compañía antivirus (o todas) hubiera detectado el 100% de las muestras enviadas, tampoco significaría nada", dice el directivo. "Este es un test, si se le puede llegar a llamar así, con tantos fallos en su metodología que cualquiera que sea la conclusión a la que llegue no debe ser tenida en cuenta".

Ambas críticas, la que deja en entredicho la selección de muestras de malware y la que descarta el método de evaluación de tal muestra, se reiteran de unas a otras compañía cuyos productos antivirus han sido analizados en "Assessing the Effectiveness of Antivirus Solutions" y con las que ha hablado *Silicon Week*. Sin embargo, el CTO de Imperva, tiene otra forma de ver las cosas. "Incluso entre los que han cuestionado nuestra metodología, parece haber un consenso en torno a nuestras conclusiones: que las soluciones antivirus estándar han llegado al punto de un rendimiento o utilidad decreciente y que las organizaciones deben virar sus inversiones hacia otras soluciones que protejan a las organizaciones frente a los efectos de la infección", escribe Shulman en un post titulado **"¿Todavía no les gusta nuestro estudio sobre soluciones AV? Una respuesta a los críticos"**. "Tengo que asumir", continúa, "que si nuestra metodología nos lleva de manera lógica a conclusiones que son tan ampliamente aceptables, no puede ser tan mala".

La defensa de Imperva

"Un muestreo malo sería un argumento justo si hubiésemos usado una técnica misteriosa de recogida de malware que sólo puede ser aplicada a las bandas criminales de alta gama. Éste, por supuesto, no es el caso", se defiende Imperva, que aprovecha para sugerir que en realidad las argumentaciones de los fabricantes de antivirus respecto a lo que se puede considerar un conjunto idóneo de ejemplares de software malicioso dan la razón a su empresa. Éstas afirman que, si se toma el tamaño de la muestra con la que trabajan, unos100.000 ejemplares por día, logran un ratio de acierto de más del 90%. "Es decir, **pierden 2.000 ejemplares de cada 100.000**", calculan Shulman. "¿Qué tan difícil creéis que es para un atacante (intencionalmente no he agregado el término "experto") poner sus manos en un par de esas 2.000 muestras no detectadas?", pregunta, añadiendo que todas las muestras incluidas en sus estadísticas fueron finalmente detectadas por una porción notable de productos antivirus, aunque ninguna de ellas era código malicioso de reciente creación, sino "más bien variaciones e instancias de malware existente".

"Somos conscientes de las limitaciones del uso de VirusTotal, y describimos dichas limitaciones en nuestra investigación", sigue justificando. "Sin embargo, **no somos los primeros en publicar estudios comparativos de eficacia antivirus basados en VT**, diversos informes recientes han estado utilizándolo para el mismo propósito. Sé que no se define como una herramienta de detección anti-malware y que no está diseñado para ser utilizado como reemplazo de los antivirus, pero tampoco se puede sostener que es sólo una herramienta de recolección para la industria con unos resultados por muestra completamente sin sentido". Es más, en la firma estadounidense insisten que han utilizado este servicio de una manera "prudente y cortés": sin hacer uso de funciones no documentadas, sin subvertir la API y sin alimentarla con datos para alterar los

resultados de las decisiones de los proveedores. “Así que, básicamente, **nuestro delito es la forma en la que interpretamos los resultados y las conclusiones que sacamos de ellos. Ir en contra de esto no tiene ningún otro término que ‘policía del pensamiento’**”.

Otra premisa en contra de la validez del estudio de Imperva sobre la efectividad de los antivirus es que recurre a la versión de línea de comandos, por lo que su configuración no es la ideal. “Esto afecta al contexto de ejecución, lo que quiere decir que un producto podría fallar en la detección de algo que sería capaz de detectar en condiciones normales de funcionamiento”, concreta el investigador David Harley en el blog oficial de ESET NOD32. ¿La contestación de Shulman? “Me encantaría ver a los vendedores de antivirus explicar qué tipos de malware no se detectan por su versión de línea de comandos y sí se detectan con la otra versión, y por qué. Ciertamente **estoy dispuesto a aceptar que nuestros resultados habrían sido algo diferentes si hubiésemos probado una versión instalada del producto que no fuese la versión de línea de comandos**, aunque creo que es una buena aproximación”.

** *Este informe sigue en la* ***segunda parte***.