



ENJOY SAFER TECHNOLOGY™

LA TECNOLOGÍA DE ESET

Protección efectiva en múltiples capas

Versión del documento:

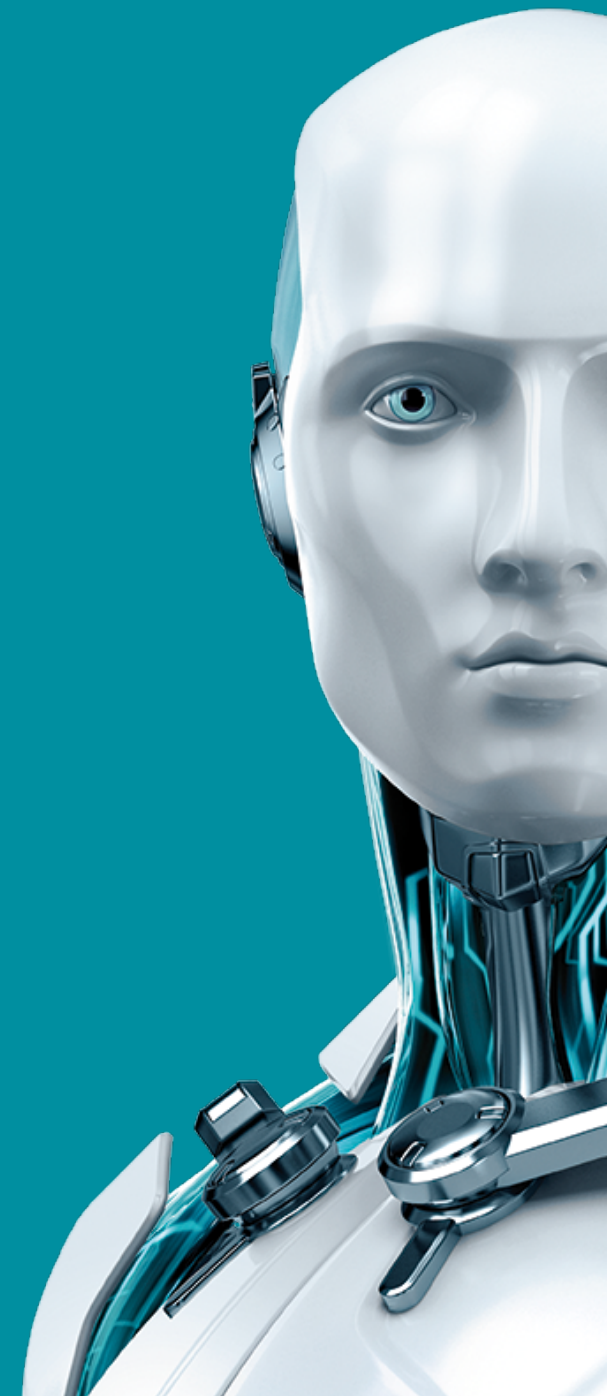
1.1

Autores:

Jakub Debski, Head of Core Technology Development

Juraj Malcho, Chief Research Officer

Peter Stancik, Security Researcher



LA TECNOLOGÍA DE ESET

¿Por qué la protección en múltiples capas es efectiva?

Contenido

Objetivos	2
Por qué el antivirus aún no ha muerto	2
Múltiples amenazas; múltiples capas de protección	3
Múltiples amenazas; múltiples plataformas	3
Diferentes vectores de distribución	3
Diseño del malware	3
Los beneficios de la tecnología base de ESET	4
Protección contra ataques de red	5
Reputación y caché	5
Detecciones de ADN	5
Bloqueo de exploits	7
Exploración avanzada de memoria	7
Sistema en la nube de protección contra malware	8
Protección ante Botnets	8
Procesamiento automatizado y manual de muestras	10
Sobre los falsos positivos y los indicadores de sistemas comprometidos	11
Conclusión	12

Objetivos

En el presente documento detallamos y resumimos las distintas tecnologías en múltiples capas que utiliza ESET para brindar una seguridad integral y mucho más completa que con las características antivirus básicas. Para ello, explicaremos cuáles son los niveles de protección involucrados en la resolución de problemas específicos y qué beneficios le aportan al usuario.

¿Por qué el antivirus aún no ha muerto?

La mayoría de las compañías antivirus surgieron a partir de la necesidad de ayudar a los usuarios con inconvenientes relacionados a malware, y con el paso de los años, su tecnología fue evolucionado a la par de la creciente variedad de amenazas que los fabricantes de seguridad comenzaban a investigar. En la actualidad, el antivirus ya se considera un producto básico y la seguridad es una preocupación de todos, más allá de que entiendan o no realmente su significado. En el último tiempo, surgieron nuevas empresas de seguridad que aseguran ser "de la próxima generación", y que si bien no suelen tener gran experiencia en el desarrollo de soluciones antimalware, utilizan una campaña de marketing fuerte para promover sus soluciones como "innovadoras". No obstante, su capacidad de detección suele estar basada en un motor de terceros adquirido a un fabricante consolidado, ya que, de todos los proveedores de soluciones que se encuentran actualmente en el mercado, son muy pocos los que realmente cuentan con la experiencia o la capacidad para desarrollar su propio núcleo de tecnologías de detección. Todas las tecnologías de ESET son propias de la empresa y se desarrollaron internamente.

El antivirus no ha muerto. Sin embargo, si bien la detección simple mediante firmas estáticas (que, según la opinión de las nuevas empresas en el mercado, está perjudicando la eficacia de la industria antimalware establecida) aún no está obsoleta, constituye tan solo una pequeña porción de la gran variedad de tecnologías que los productos de seguridad modernos despliegan contra las amenazas actuales.

Múltiples amenazas. Múltiples capas de protección

Las empresas antimalware consolidadas que aún se mantienen activas lograron mantener su cuota de mercado gracias a la evolución de sus tecnologías, lo que les permitió enfrentar las amenazas actuales. Las amenazas no son estáticas y su evolución no se frenó a principios de la década de 2000. Por lo tanto, las amenazas actuales no se podrían combatir con eficacia si las empresas de seguridad sólo actualizaran las tecnologías empleadas en la década de 1990. Por eso, las empresas de seguridad deben perfeccionar sus productos de manera constante, tanto de forma reactiva como también proactiva, para ofrecer soluciones eficaces, incorporando diferentes capas de protección capaces de detectar y/o bloquear el malware moderno. Un único punto de protección o un único método de defensa no alcanza. Esa es una de las razones por las que ESET también pasó de ser un proveedor de productos antivirus a una empresa de TI que ofrece seguridad integral.

Múltiples amenazas. Múltiples plataformas

Los sistemas operativos de Microsoft no son las únicas plataformas a las que el malware está dirigido en la actualidad. El campo de batalla está cambiando rápidamente a medida que los atacantes tratan de tomar el control de plataformas y procesos aún no explorados.

- Todo lo que se pueda controlar para realizar actividades maliciosas se puede utilizar en ataques.
- Todo lo que ejecute códigos para procesar datos externos puede ser potencialmente secuestrado.

Los servidores Linux constituyen un importante objetivo para los atacantes ([Operación Windigo](#), [Linux/Mumblehard](#)), los equipos Mac con OS X alojaron una de las botnets más grandes de la historia ([OSX/Flashback](#)), los teléfonos móviles son objetivos muy comunes ([Hesperbot](#)) y los ataques a routers se están convirtiendo en una grave amenaza ([Linux/Moose](#)). Los rootkits están cada vez más cerca del hardware (ataques contra firmware o el uso del [rootkit de UEFI](#)) y la virtualización abre nuevos vectores de ataque (Bluepill, vulnerabilidades de escape de máquinas virtuales). Además, los navegadores Web y otras aplicaciones se han vuelto tan complejos como los sistemas operativos, y sus mecanismos de scripting se utilizan a menudo con fines maliciosos ([Win32/Theola](#)).

Diferentes vectores de distribución

Históricamente, el primer malware apareció en forma de procesos autoreplicantes, al principio dentro de los mismos sistemas y luego como un virus que infectaba archivos y/o el disco, y que se propagaba de una PC a otra. Como Internet tiene un uso prácticamente universal, la cantidad de maneras de distribuir software malicioso ha aumentado enormemente. Los objetos maliciosos también se pueden enviar por correo electrónico como archivos adjuntos o enlaces, descargar desde páginas Web, instalar mediante scripts presentes en documentos, compartir en dispositivos extraíbles, desplegar en forma remota a través del aprovechamiento de contraseñas débiles o la falta de políticas de autorización, ejecutar por exploits o instalar por los usuarios finales que caen en el engaño de las técnicas de ingeniería social.

Diseño del malware

La época en que al malware lo creaban principalmente los jóvenes para hacer una broma o presumir, quedó en el pasado hace tiempo. Hoy en día, el malware se escribe con otros motivos: ganar dinero o robar información, y se invierten importantes sumas en su desarrollo, tanto por los delincuentes como por los gobiernos.

Con la esperanza de hacer más difícil su detección, los desarrolladores de malware utilizan diferentes lenguajes de programación, compiladores y lenguajes interpretados. Además, ocultan el código y lo protegen con software personalizado para dificultar aún más su detección y análisis. Los atacantes suelen inyectar el código malicioso en procesos no infectados para tratar de evitar la detección por los monitores de conducta (diseñados para detectar actividad sospechosa) y obstaculizar así su extracción, asegurando la persistencia del malware dentro del sistema. También utilizan scripts para evadir las técnicas de control de aplicaciones, y usan malware que solo está presente en memoria para que la seguridad basada en archivos los pase por alto.

Para evitar ser detectadas, las bandas criminales llenan la Internet con miles de variantes de su malware. Otra de sus estrategias consiste en distribuir malware a un pequeño número de objetivos específicos para evitar atraer la atención de las empresas de seguridad. Utilizan indebidamente los componentes de software no infectados o firman el código malicioso con certificados robados a empresas legítimas, dado que un código autorizado es más difícil de detectar.

Además, en el nivel de la red, el malware está dejando de usar direcciones de servidores de comando y control (C&C) codificadas en forma rígida, desde donde se envían instrucciones y se reciben datos de los sistemas comprometidos. Ahora es más común que los atacantes elijan el control descentralizado de las botnets que utilizan las redes de pares *peer to peer*, donde las comunicaciones cifradas dificultan la identificación de los ataques. Los algoritmos para la generación de dominios reducen la eficacia de la detección basada en el bloqueo de direcciones URL conocidas. Los atacantes toman el control de sitios Web legítimos de buena reputación e incluso usan servicios de publicidad legales para distribuir contenido malicioso.

NOTA IMPORTANTE Son muchas las maneras en que los atacantes logran evadir la detección, por eso una sola capa de seguridad no es suficiente para proteger un sistema. En ESET creemos que una protección constante, en tiempo real y en múltiples niveles es imprescindible para garantizar la máxima seguridad.

Los beneficios de la tecnología base de ESET

El **motor de análisis de ESET** constituye el núcleo de nuestros productos y, aunque la tecnología subyacente es heredada de nuestro antiguo antivirus, se extendió y perfeccionó, y se encuentra **en desarrollo e innovación constante para cubrir las nuevas amenazas**. El propósito del motor de análisis es identificar los posibles casos de malware y tomar decisiones automatizadas sobre la probabilidad que tienen de ser maliciosos.

Durante muchos años, el rendimiento de ESET se basó en algoritmos inteligentes y código ensamblador elaborado en forma manual para hacer frente a los problemas de rendimiento causados por el análisis de código en profundidad que utilizaba la tecnología sandboxing integrada al producto. Sin embargo, renovamos este enfoque. Ahora, para lograr el máximo rendimiento, utilizamos **la traducción binaria junto con la emulación interpretada**.

Con el **modo de sandbox incorporado en el producto** es necesario emular diferentes componentes de hardware y software para ejecutar un programa en un entorno virtualizado. Estos componentes incluyen la memoria, el sistema de archivos, las API del sistema operativo y la CPU (unidad de procesamiento central).

En el pasado, se utilizaba un código ensamblador hecho a medida para emular la CPU. De todas formas, servía meramente para interpretar código, es decir que cada instrucción se tenía que emular por separado. Con la traducción binaria, se ejecutan instrucciones emuladas en forma nativa en una CPU real. Esto es muchas veces más rápido, especialmente en el caso de los bucles del código: la introducción de múltiples bucles es una técnica de protección común de los ejecutables maliciosos (para protegerlos ante el análisis de productos de seguridad e investigadores de malware).

Los productos de ESET exploran cientos de formatos de archivos diferentes (archivos ejecutables, archivos de instalación, scripts, archivos comprimidos, documentos y códigos de bytes) con el fin de detectar con precisión los componentes maliciosos incrustados.

La siguiente imagen muestra las distintas tecnologías que conforman el núcleo de protección de ESET, y cuándo y cómo pueden detectar y/o bloquear una amenaza durante su ciclo de vida en el sistema:

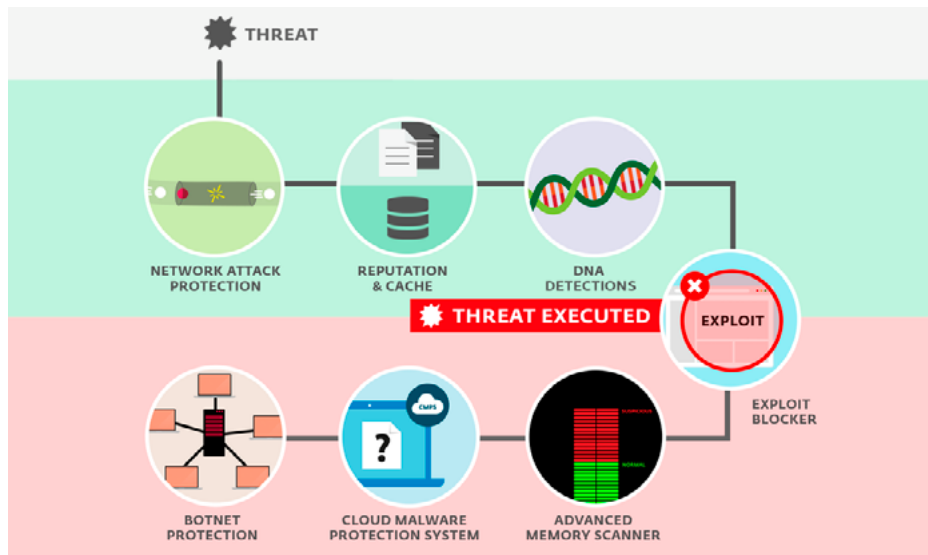
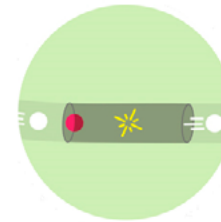


Imagen 1: Capas de protección de ESET

Protección contra ataques de red



La Protección contra ataques de red es una **extensión de la tecnología de firewall** que mejora la detección de las vulnerabilidades conocidas en el nivel de la red. Al implementar la detección de las vulnerabilidades comunes en los protocolos de uso más frecuente, como [SMB](#), [RPC](#) y [RDP](#),

constituye otra importante capa de protección ante el malware en propagación, los ataques que circulan por la red y el aprovechamiento de vulnerabilidades para las cuales aún no se lanzó al público o no se desarrolló la revisión correspondiente.

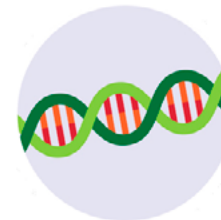
Reputación y caché



Al inspeccionar un objeto, como un archivo o una URL, antes de que se lleve a cabo cualquier exploración, nuestros productos revisan la caché local (y la **ESET Shared Local Cache**, en el caso de ESET Endpoint Security) para ver si ya hay objetos maliciosos conocidos u objetos no infectados en la lista blanca. De esta forma, se **mejora el rendimiento de la exploración**. Luego se consulta el **Sistema de reputación de archivos ESET LiveGrid®** para conocer la **reputación de los objetos** (es decir, si el objeto ya se ha encontrado en otros lugares y si se clasificó como malicioso). Esto **mejora la eficiencia de la exploración y acelera el intercambio de la inteligencia de malware con nuestros clientes**. El hecho de aplicar listas negras de direcciones URL y comprobar la reputación de los objetos evita que los usuarios accedan a sitios con contenido malicioso y/o a sitios de phishing.

De esta forma, se **mejora el rendimiento de la exploración**. Luego se consulta el **Sistema de reputación de archivos ESET LiveGrid®** para conocer la **reputación de los objetos** (es decir, si el objeto ya se ha encontrado en otros lugares y si se clasificó como malicioso). Esto **mejora la eficiencia de la exploración y acelera el intercambio de la inteligencia de malware con nuestros clientes**. El hecho de aplicar listas negras de direcciones URL y comprobar la reputación de los objetos evita que los usuarios accedan a sitios con contenido malicioso y/o a sitios de phishing.

Detecciones de ADN



Los tipos de detecciones varían desde *hashes* muy específicos (que resultan útiles, por ej., para detectar binarios maliciosos específicos o versiones específicas de malware, con propósitos estadísticos, o simplemente para darle un nombre de detección más preciso a un tipo de malware que

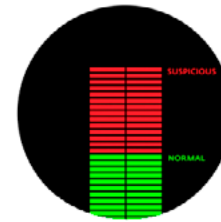


Bloqueo de exploits

Las tecnologías de ESET brindan protección ante varios tipos de vulnerabilidades en diferentes niveles: nuestro motor de exploración detecta los exploits que aparecen en los archivos de documentos con formato incorrecto; la protección contra ataques de red se concentra en el nivel de la comunicación; y finalmente, el Bloqueo de exploits detiene el proceso mismo de aprovechamiento de vulnerabilidades.

El Bloqueo de exploits monitorea las aplicaciones que suelen ser atacadas por exploits con mayor frecuencia (navegadores, lectores de documentos, clientes de correo electrónico, Flash, Java, etc.) y, en lugar de enfocarse solamente en ciertos [identificadores de CVE](#), se centra en las técnicas de explotación. Cada exploit es una anomalía en la ejecución del proceso, y nosotros buscamos anomalías que sugieran la presencia de técnicas de aprovechamiento de vulnerabilidades. Como las tecnologías de detección están en desarrollo constante, se añaden nuevos métodos con regularidad para cubrir las nuevas técnicas de los exploits. Al accionarse, se analiza el comportamiento de los procesos y, si se considera sospechoso, se puede **bloquear la amenaza de inmediato en la máquina**, y enviar metadatos sobre el ataque a nuestro sistema en la nube ESET LiveGrid. Estos datos se siguen procesando y se correlacionan entre sí, lo que **nos permite detectar las amenazas desconocidas hasta el momento y los ataques 0-day**. Además, le proporciona a nuestro laboratorio la valiosa inteligencia sobre amenazas.

El Bloqueo de exploits agrega una capa de protección adicional que emplea una tecnología completamente diferente a las tecnologías de detección enfocadas en el análisis de los códigos maliciosos en sí.



Exploración avanzada de memoria

La Exploración avanzada de memoria es una **tecnología exclusiva de ESET** que aborda con eficacia un problema importante del malware moderno: **el uso intensivo de técnicas de ofuscación y/o cifrado**.

Estas tácticas de protección de malware, de uso frecuente en los empaquetadores de tiempo de ejecución y los protectores de código, causan problemas a los tipos de detección que emplean técnicas de desempaquetamiento, como la emulación o el modo sandbox. Es más, si la comprobación se realiza mediante un emulador o sandbox virtual/físico, no hay ninguna garantía de que durante el análisis el malware muestre un comportamiento malicioso que permita calificarlo como tal. El malware se puede ofuscar de forma que no todas sus rutas de ejecución se puedan analizar; también puede incluir condiciones o un reloj para accionar el código, y con mucha frecuencia, puede descargar nuevos componentes durante su vida útil. Para afrontar estos problemas, la Exploración avanzada de memoria monitorea el comportamiento del proceso malicioso y lo explora cuando se muestra en memoria. Esto complementa la funcionalidad más tradicional de análisis proactivo del código, ya sea en forma previa a la ejecución o durante la misma.

Además, los procesos no infectados de pronto pueden convertirse en maliciosos debido al aprovechamiento de vulnerabilidades o a la inyección de código. Por estas razones, hacer una sola exploración no es suficiente. Es necesario hacer un monitoreo constante, y ese es justamente el papel de la Exploración avanzada de memoria. **Cada vez que un proceso hace una llamada del sistema desde una nueva página ejecutable, la Exploración avanzada de memoria analiza el comportamiento del código utilizando las Detecciones de ADN de ESET.**

El análisis de código no solo se realiza en la memoria ejecutable estándar, sino también en el Lenguaje Intermedio de Microsoft (MSIL) de .NET, utilizado por los creadores de malware para obstaculizar el análisis dinámico. Debido a la implementación de almacenamiento inteligente en caché, la Exploración avanzada de memoria prácticamente no afecta el rendimiento del sistema y no causa ningún deterioro notable en la velocidad de procesamiento.

La Exploración avanzada de memoria es muy efectiva cuando trabaja junto con el Bloqueo de exploits. A diferencia del Bloqueo de exploits, este método detecta el malware después de su ejecución; es decir, existe el riesgo de que ya se haya llevado a cabo alguna actividad maliciosa. No obstante, es un paso más en la cadena de protección, y **constituye un último recurso de seguridad** en caso de que un atacante logre eludir las demás capas de protección.

Además, el malware avanzado presenta una nueva tendencia: algunos de los códigos maliciosos que ahora opera son exclusivos para la memoria, es decir que no necesitan componentes persistentes en el sistema de archivos que se pueden detectar de forma convencional. En un principio, este tipo de malware apareció sólo en servidores, debido a que sus períodos de actividad ininterrumpida son prolongados (como los sistemas de servidores permanecen encendidos durante meses o años, los procesos maliciosos podrían permanecer en la memoria de forma indefinida sin necesidad de sobrevivir a un reinicio de sistema). Sin embargo, los recientes ataques a empresas indican un cambio en esta tendencia, y ahora comenzamos a encontrar endpoints que son víctimas de estos ataques. **Únicamente la exploración de la memoria puede descubrir con éxito este tipo de ataques maliciosos y ESET ya está preparado para la nueva tendencia.**

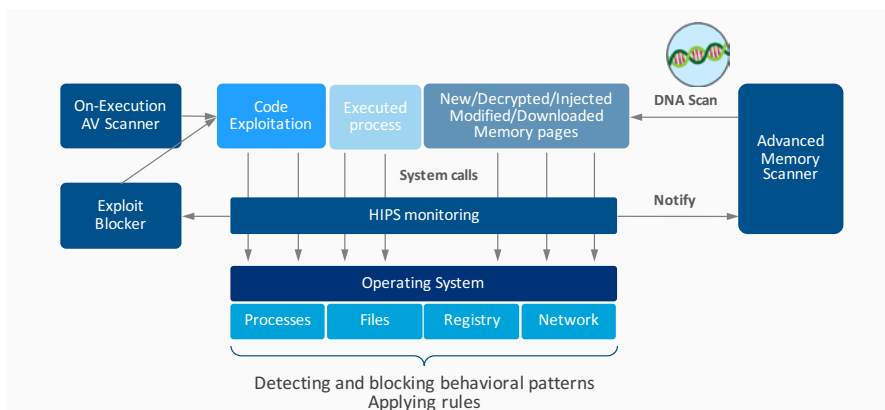
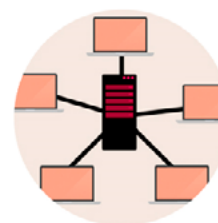


Imagen 2: Funcionamiento de la detección del comportamiento



Sistema en la nube de protección contra malware

El sistema en la nube de protección contra malware provisto por ESET es una de las muchas **tecnologías basadas en ESET LiveGrid**. Las aplicaciones desconocidas potencialmente maliciosas y otras posibles amenazas se monitorean y se envían a la nube de ESET a través del sistema de recopilación de datos ESET LiveGrid. **Las muestras recopiladas se verifican automáticamente en el modo sandbox y se someten al análisis de su comportamiento** y, si se confirman las características maliciosas, se crean nuevas detecciones automatizadas. A los clientes de ESET les llegan estas nuevas detecciones automatizadas a través del Sistema de reputación de archivos ESET LiveGrid, sin necesidad de esperar a la próxima actualización del motor de detección. El tiempo de respuesta de los mecanismos normalmente es menor a 20 minutos, lo que permite la detección eficaz de las nuevas amenazas incluso antes de que se entreguen las detecciones regulares a los equipos de los usuarios.



Protección ante Botnets

Uno de los elementos del malware que a sus creadores les resulta muy costoso cambiar es la comunicación con los servidores de C&C. Está comprobado que **la Protección ante botnets suministrada por ESET detecta con éxito la comunicación maliciosa** utilizada por las botnets, y al mismo tiempo identifica los procesos ofensivos.

Las Detecciones de redes de ESET extienden la tecnología de Protección ante botnets para abordar los problemas generales asociados con el análisis de tráfico de red. Permiten una **detección más rápida y flexible del tráfico malicioso**. Las firmas estándares de la industria como Snort o Bro detectan muchos ataques, pero las Detecciones de redes de ESET están diseñadas específicamente para detectar vulnerabilidades de la red, exploit kits y particularmente las comunicaciones que establece el malware avanzado.

La capacidad de realizar análisis del tráfico de red en las endpoints ofrece ventajas adicionales. Nos permite identificar exactamente qué proceso o módulo es el responsable de la comunicación maliciosa, tomar las medidas necesarias contra el objeto identificado y a veces incluso permite pasar por alto el cifrado de las comunicaciones.

Protección reactiva vs. proactiva en la actualidad

Mientras que las detecciones de ADN son excelentes para detectar hasta familias enteras de malware, primero deben distribuirse a los usuarios para que cuenten con su protección. Lo mismo ocurre con el motor de exploración, la heurística o cualquier tecnología que se centre en nuevas amenazas. Hoy en día, la comunicación con el sistema basado en la nube ESET LiveGrid es necesaria para garantizar el más alto nivel de protección por muchas razones:

- **La exploración offline es mayormente reactiva.** En la actualidad, ser proactivo ya no consiste en tener la mejor detección heurística. Si las herramientas de protección están disponibles para un atacante, no importa que sean firmas, heurística o clasificadores de aprendizaje automático: un creador de malware puede experimentar con la tecnología de detección, modificar su malware hasta que no sea detectado y, recién entonces, liberarlo. ESET LiveGrid contrarresta esta estrategia del atacante.
- **Las actualizaciones no son en tiempo real.** Las actualizaciones pueden lanzarse con mayor frecuencia y hasta se podrían enviar a los equipos de los usuarios cada pocos minutos. Pero ¿no habrá una manera más eficaz de hacerlo? Sí. ESET LiveGrid suministra protección instantánea, ya que proporciona la información en todo momento que se necesite.
- **El malware hace lo posible por pasar desapercibido.** Los autores de malware, especialmente en el caso del espionaje cibernético, tratan de evitar la detección por tanto tiempo como sea posible. Los ataques dirigidos (a diferencia de las distribuciones masivas, por ejemplo, con gusanos de correo electrónico) envían

piezas exclusivas de malware a una pequeña cantidad de objetivos, a veces incluso a uno solo. Nosotros hacemos que esta característica se vuelva en contra de los autores de malware: asumimos que los objetos que no son populares y que no tienen una buena reputación son potencialmente maliciosos y los analizamos en detalle, ya sea en la endpoint o enviándolos a nuestro sistema de recopilación de datos LiveGrid para un análisis automatizado en profundidad. El Sistema de reputación ESET LiveGrid contiene información sobre los archivos, sus orígenes, similitudes, certificados, y direcciones URL e IP.

Protección mediante ESET LiveGrid

La forma más sencilla de suministrar protección mediante un sistema en la nube es creando listas negras con hashing de coincidencia perfecta (exact hashing). Esto funciona bien tanto para archivos como direcciones URL, pero solo es capaz de bloquear los objetos que coincidan exactamente con el hash. Esta limitación condujo a la creación del hashing difuso (fuzzy hashing). El hashing difuso tiene en cuenta la similitud binaria de los objetos, dado que objetos similares tienen el mismo hash o un hash similar.

ESET llevó el hash difuso al siguiente nivel. Nosotros no hacemos hashing de los datos, sino del comportamiento descrito en las detecciones de ADN. Al usar el hashing de ADN, somos capaces de bloquear miles de variantes diferentes de malware al instante.

Unique files detected by DNA hashes

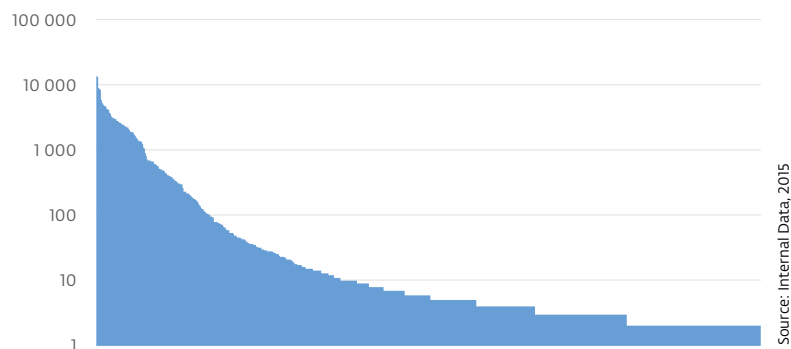


Imagen 3: Cantidad de archivos únicos (eje y) detectados por el hashing de ADN (eje x).

El suministro instantáneo de listas negras a los usuarios no es el único propósito del Sistema de ESET en la nube para protección contra malware. Si un usuario decide participar en el proceso de envío de muestras, cada vez que se identifique una nueva muestra cuya reputación es dudosa, se enviará a ESET para un análisis en profundidad. Para aprovechar todo el potencial del sistema en la nube de protección contra malware, los usuarios primero deben habilitar el sistema de recopilación ESET LiveGrid, lo que nos permite recoger las muestras sospechosas de reputación dudosa para realizar un análisis detallado.

Procesamiento automatizado y manual de muestras

Cada día, ESET recibe cientos de miles de muestras preprocesadas y agrupadas, que se procesan de forma automática, semiautomática y manual. **El análisis automatizado se lleva a cabo mediante herramientas desarrolladas internamente en una gran variedad de máquinas virtuales y físicas.** Su clasificación se realiza utilizando diferentes atributos extraídos durante la ejecución, según el análisis

de códigos estáticos y dinámicos, los cambios hechos en el sistema operativo, los patrones de comunicación de red, las similitudes con otras muestras de malware, las características de su ADN, la información estructural y la detección de anomalías.

Todos los clasificadores automáticos presentan inconvenientes:

La elección de características diferenciadoras para la clasificación no es trivial y requiere emplear el conocimiento de personas expertas en el campo de malware.

- Los clasificadores de aprendizaje automático requieren la participación de personas expertas para verificar las entradas utilizadas en el aprendizaje. Si el procesamiento fuera totalmente automatizado y las muestras clasificadas por el sistema se utilizaran directamente como entradas en el sistema, las entradas positivas irían creando un bucle con efecto exponencial que dejaría al sistema rápidamente inestable. Es decir, la integridad del rendimiento de un sistema o proceso depende de la integridad de los datos de entrada.

- Los algoritmos de aprendizaje automático no entienden los datos e incluso cuando la información es estadísticamente correcta no significa que sea válida. Por ejemplo, el aprendizaje automático no puede distinguir las nuevas versiones de software no infectado de las versiones alteradas, no puede distinguir un programa de actualización de una aplicación no infectada o de un downloader utilizado por el malware, ni es capaz de reconocer cuándo se utilizan componentes de software no infectados con fines maliciosos.

- Con el aprendizaje automático, añadir nuevas muestras a un proceso de aprendizaje puede causar falsos positivos, y eliminar falsos positivos puede reducir la eficacia de una detección positiva real.

- Mientras que el procesamiento automatizado permite obtener respuestas inmediatas ante nuevas amenazas gracias a su detección con ESET LiveGrid, es crucial que los ingenieros de detección lleven a cabo un procesamiento

adicional de dichas muestras para garantizar la mayor calidad y las mejores tasas de detección, así como el menor número de falsos positivos.

Servicios de reputación

ESET LiveGrid también les otorga a los objetos una reputación. Calificamos la reputación de varias entidades, incluyendo archivos, certificados, direcciones URL y direcciones IP. Como se describió anteriormente, la reputación se puede utilizar para identificar nuevos objetos maliciosos o fuentes de infección. Sin embargo, también tiene otros usos.

Uso de listas blancas en la exploración

El uso de listas blancas reduce la cantidad de veces que el motor de exploración inspecciona un mismo objeto. Si estamos seguros de que un objeto en particular no se modificó y no está infectado, directamente no hay necesidad de volver a explorarlo. Esto tiene un impacto sumamente positivo en el rendimiento y ayuda a hacer que los productos de ESET no sean intrusivos. Como solemos decir: "el código más veloz es aquel que no se ejecuta". Nuestras listas blancas se adaptan constantemente a la realidad cambiante del mundo de software.

Recopilación de inteligencia

Si un usuario decide participar en el envío de estadísticas a ESET LiveGrid, utilizamos la información enviada para hacer un seguimiento y monitoreo de las amenazas globales. Esta información nos da una valiosa cantidad de datos para investigación y nos permite concentrarnos en los casos más urgentes y problemáticos, observar las tendencias del malware, y planificar y priorizar el desarrollo de tecnologías de protección.

Sobre los falsos positivos y los indicadores de sistemas comprometidos

Los indicadores de sistemas comprometidos son vistos como algo muy importante en la seguridad corporativa contemporánea, pero están lejos de ser tan especiales o avanzados, a pesar de que a veces los proveedores de seguridad "de la nueva generación" insisten en ellos por demás. Más abajo mostramos un desglose de los indicadores de sistemas comprometidos más prevalentes y en qué se basan.* Como podemos ver, los problemas que abordan son muy básicos: en una cuarta parte de los casos se trata de hashes MD5 conocidos, luego siguen los nombres de archivo, etc. Estos resultados dejan en claro que no es un método adecuado para la prevención y el bloqueo, aunque puede ser útil para la informática forense. Es irónico que algunos de los vendedores "de la nueva generación" que rechazan las detecciones basadas en firmas de los "viejos antivirus" por considerarlas "obsoletas", hablen tan bien de los indicadores de sistemas comprometidos, a pesar de ser el método basado en firmas más débil que existe para detectar archivos o eventos maliciosos.

*Fuente: IOC Bucket, abril de 2015. IOC Bucket es una plataforma gratuita desarrollada por la comunidad que se dedica a compartir la inteligencia sobre amenazas con la comunidad de seguridad.

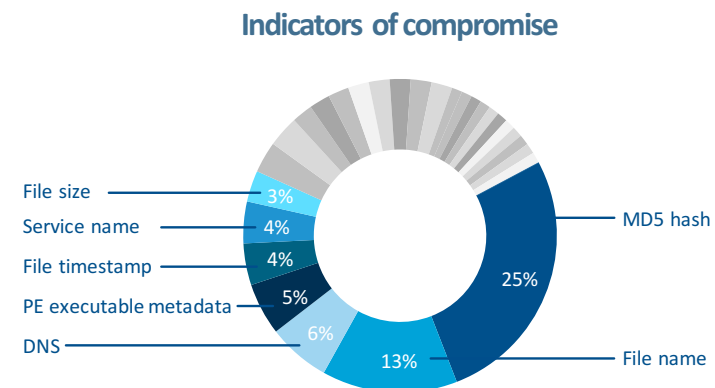


Imagen.4: Análisis de los indicadores de sistemas comprometidos, IOC Bucket (ejemplar de abril de 2015).

Conclusión

No hay ninguna solución infalible cuando se trata de seguridad. El malware de hoy, por su naturaleza dinámica para responder a las continuas investigaciones, requiere una protección de múltiples capas basada en tecnologías proactivas e inteligentes que tengan en cuenta los petabytes de datos de inteligencia recopilados durante muchísimos años por investigadores experimentados. Ya pasaron 20 años desde que ESET reconoció que el antivirus (el enfoque tradicional) era una solución incompleta, por eso desde aquel entonces ya empezamos a incorporar tecnologías proactivas a nuestro motor de exploración y gradualmente implementamos diferentes capas de protección para combatir el malware en las distintas etapas de la cadena maliciosa cibernética.

ESET es una de las pocas empresas de seguridad capaces de proporcionar un alto nivel de protección con una trayectoria de más de 25 años de investigación. Esto nos permite estar siempre un paso adelante del malware, mejorando constantemente nuestras tecnologías para ir más allá de las firmas estáticas estándar. Nuestra combinación exclusiva de tecnologías basadas en endpoints y de servicios en la nube ofrece la seguridad contra malware más avanzada del mercado.

