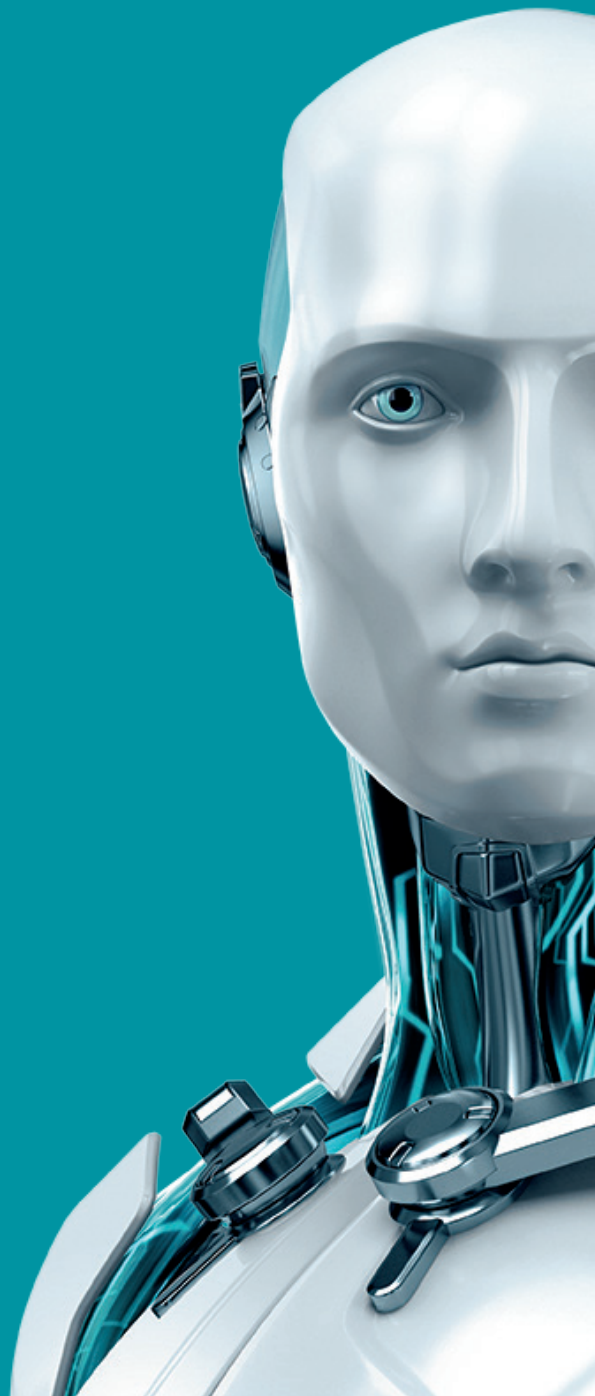
ENJOY SAFER TECHNOLOGY™

TECNOLOGÍA ESET

El enfoque multicapa y su eficacia



Versión del documento:
1.1

Autores:
Jakub Debski, Responsable de Desarrollo de la Tecnología del Núcleo
Juraj Malcho, Responsable de Investigación
Peter Stancik, Investigador de Seguridad

TECNOLOGÍA ESET

El enfoque multicapa y su eficacia

Índice

Objetivos

En este documento resumimos de qué forma usa ESET las tecnologías multicapa para ir mucho más allá de las posibilidades de un antivirus básico. Para ello, explicamos qué capas están implicadas en la solución de determinados problemas y qué ventajas proporcionan al usuario.

¿Por qué el antivirus no está muerto?

La mayoría de empresas antivirus nacieron de la voluntad de ayudar a los usuarios que tenían problemas con los virus o malware, y su tecnología fue evolucionando para adaptarse a un amplio rango de amenazas que los fabricantes de seguridad estaban empezando a solucionar. Hoy en día, la industria antivirus es percibida como un producto de consumo y la seguridad es un tema del que todo el mundo habla, aunque no se entienda realmente su significado. Últimamente, hemos observado una proliferación de nuevas empresas que se denominan a sí mismas "next-generation" o "next-gen". Éstas cuentan con poca experiencia en el desarrollo de soluciones antimalware, pero venden sus productos agresivamente como "innovadores" menospreciando a los fabricantes con larga trayectoria . Al igual que muchos vendedores que prometen la panacea, muchos de sus argumentos son contradictorios e, irónicamente, su capacidad de detección se basa normalmente en un motor de terceros que procede de un proveedor tradicional, puesto que muy pocos de entre las docenas de proveedores de soluciones tienen la experiencia o la capacidad ahora en el mercado de poder desarrollar su propia tecnología núcleo de detección. Las tecnologías de ESET son todas propietarias y han sido desarrolladas en la compañía.

El antivirus no está muerto. Sin embargo, la detección simple con base de firmas estáticas que -según los nuevos fabricantes- está poniendo en riesgo la eficacia de la industria antimalware tradicional es, si no está obsoleta o ha desaparecido, solo un componente minúsculo de la batería de tecnologías que un producto de seguridad moderno desarrolla contra las amenazas actuales.

Múltiples amenazas, protección multicapa

Las empresas antimalware tradicionales que aún están en el negocio hoy en día han mantenido su cuota de mercado adaptando su estrategia a las amenazas actuales. Estas amenazas no son estáticas y su evolución no se detiene desde el año 2000. Las amenazas actuales no pueden combatirse eficazmente añadiendo funcionalidades a la tecnología de los 90. La lucha contra las amenazas actuales es un juego del gato y el ratón en el que nos enfrentamos a equipos de tipos malos hábiles y motivados económicamente. Por tanto, las compañías de seguridad deben refinar sus productos de seguridad constantemente, tanto de forma reactiva y proactiva, para ofrecer soluciones eficaces añadiendo diferentes capas con las que detectar y/o bloquear las amenazas modernas. Un único punto de protección o un único método de defensa simplemente no es suficiente. Esta es una de las razones por las que ESET también ha pasado de ser un fabricante antivirus a una compañía de seguridad informática.

Múltiples amenazas, múltiples plataformas

Los sistemas operativos de Microsoft no son las únicas plataformas en las que puede ejecutarse malware hoy en día. El campo de batalla está cambiando rápidamente porque los atacantes intentan obtener el control de plataformas y procesos que no han sido explorados anteriormente.

- Cualquier cosa que pueda ser controlada para realizar actividades maliciosas puede utilizarse para atacar.
- Cualquier cosa que ejecute código para procesar datos externos puede ser potencialmente secuestrada por códigos maliciosos.

Los servidores Linux se han convertido en un objetivo importante para los atacantes *(Operación Windigo, Linux/Mumblehard)*, los Mac con sistema operativo OS X formaron parte de una de las mayores botnets de la historia *(OSX/Flashback)*, los móviles son objetivos comunes *(Hesperbot)* y los ataques a routers se están convirtiendo en una amenaza importante *(Linux/Moose)*. Los Rootkits se están acercando al hardware *(ataques al firmware o utilizando el rootkit UEFI)* y la virtualización abre nuevos vectores de ataque *(Bluepill, vulnerabilidades que permiten al malware escapar de entornos controlados como máquinas virtuales)*. Asimismo, los navegadores web y otras aplicaciones se han hecho tan complejas como los sistemas operativos y sus mecanismos de scripting se usan a menudo con fines maliciosos *(Win32/Theola)*.

Diferentes vectores de distribución

Históricamente, las primeras muestras de malware aparecieron como procesos de autorreplicación, al principio dentro de los sistemas y después como virus de infección de archivos y/o de disco que se propagaban de equipo a equipo. Como el uso de Internet se ha hecho casi universal, el número de formas de distribución de malware ha crecido enormemente. Los objetos maliciosos también pueden enviarse por correo electrónico como documentos adjuntos o enlaces, descargarse de páginas web, insertarse mediante scripts en documentos, compartirse en dispositivos extraíbles, instalarse remotamente aprovechando permisos de administración o contraseñas débiles, ejecutarse mediante exploits o hacer que los usuarios finales los instalen engañándolos mediante técnicas de ingeniería social.

Diseño de malware

La era de cuando el malware era programado por adolescentes como broma o para presumir ya ha pasado. Hoy en día, el malware se programa para obtener beneficios económicos o robar información, y los cibercriminales y gobiernos invierten mucho dinero en su desarrollo.

Con la esperanza de dificultar su detección, el malware se programa en distintos lenguajes, usando diferentes compiladores y lenguajes interpretados. El código se ofusca y protege usando programas personalizados para hacer que la detección y el análisis sean más difíciles.

El código se inyecta en procesos legítimos para intentar evitar la monitorización del comportamiento –diseñada para detectar actividades sospechosas– y dificultar su eliminación, garantizando así su persistencia en el sistema. Se utilizan scripts para evitar técnicas de control de aplicaciones y el malware que "solo se ejecuta en memoria" se salta la seguridad basada en análisis de archivos.

Para evitar la protección anterior, los malos inundan Internet con miles de variantes de su malware. Otra forma es distribuir el malware a un pequeño grupo de objetivos para evitar atraer la atención de las empresas de seguridad. Para evitar su detección, se aprovechan los componentes de programas legítimos o se firma el código malicioso usando certificados robados de empresas legítimas para que el código no autorizado sea más difícil de detectar.

Asimismo, a nivel de red el malware utiliza menos servidores de control y comando (C&C) hardcodeados para enviar instrucciones y recibir información de equipos puestos en riesgo. Se utiliza frecuentemente el control descentralizado de botnets que utilizan comunicaciones de red entre iguales, y las comunicaciones cifradas hacen que la identificación de los ataques sean más difíciles. Los algoritmos de generación de dominios reducen la eficacia de la detección basada en el bloqueo de URLs conocidas. Los atacantes toman el control de páginas web legítimas con buena reputación e incluso se utilizan servicios legales de promoción de anuncios para distribuir el contenido malicioso.

NOTA IMPORTANTE

Existen muchas maneras por las cuales los atacantes pueden evitar ser detectados, por lo que una solución simple con una sola capa no es suficiente para protegerte adecuadamente. En ESET creemos que la protección constante, en tiempo real y multicapa es esencial para garantizar el máximo nivel de protección.

Las ventajas de la tecnología ESET

El motor de análisis ESET se encuentra en el núcleo de nuestros productos, mientras que la tecnología base procede de un "antivirus tradicional", ha sido ampliada y mejorada y se encuentra **en desarrollo constante para proteger contra las amenazas más actuales.**

El objetivo del motor de análisis es identificar el posible malware y tomar decisiones automáticas sobre el grado de probabilidad de que el código inspeccionado sea malicioso.

Durante muchos años, el rendimiento de ESET se basaba en algoritmos inteligentes y código de ensamblaje programado a mano para solucionar los cuellos de botella en el rendimiento causados por el análisis profundo de código usando la tecnología de sandboxing (aislamiento de procesos) integrada en el producto. Sin embargo, hemos mejorado este enfoque. Ahora, para un rendimiento máximo, usamos **traducción binaria junto con la emulación interpretada.**

El aislamiento de procesos en el producto provoca que tengas que emular diferentes componentes del hardware y software del equipo para ejecutar un programa en un entorno virtualizado. Estos componentes pueden incluir memoria, el sistema de archivos, APIs del sistema operativo y la CPU.

Por lo que respecta a la CPU, ésta se emulaba usando código de ensamblaje hecho a medida. Sin embargo, era un "código interpretado", que significa que cada instrucción tenía que emularse por separado. Con la traducción binaria, ejecutas instrucciones emuladas de forma nativa en una CPU real. Esto es mucho más rápido, especialmente en caso de bucles en el código: introducir múltiples bucles es una técnica de protección común a todos los ejecutables donde se han aplicado medidas para protegerlos del análisis de productos e investigadores de seguridad.

Los productos ESET analizan cientos de formatos de archivo diferentes (ejecutables, instaladores, scripts, ficheros, documentos y bytecodes) para detectar de forma precisa los componentes incrustados.

El gráfico inferior muestra varias tecnologías del núcleo ESET y una aproximación de cuándo y cómo pueden detectar y/o bloquear una amenaza durante su ciclo de vida en el sistema:

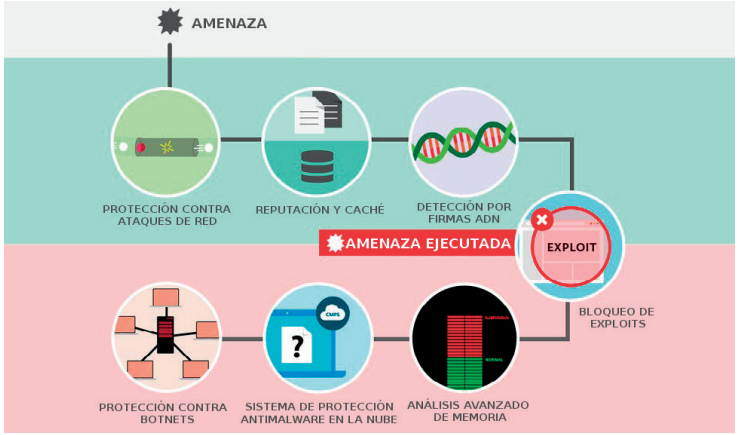
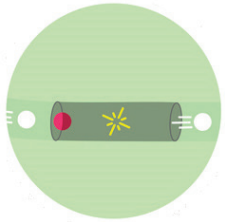


Fig. 1: Capas de protección ESET

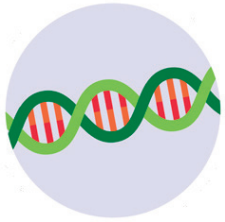


Protección contra ataques de red

La protección contra ataques de red es una **extensión de la tecnología del cortafuegos y mejora la detección de vulnerabilidades conocidas a nivel de la red**. Implementando la detección para vulnerabilidades comunes en protocolos usados ampliamente, tales como *SMB*, *RPC* y *RDP*, **constituye otra capa de protección importante** contra el malware que se propaga, los ataques de red y el aprovechamiento de vulnerabilidades para las que todavía no existe o se ha implementado un parche.

Reputación y caché

Al inspeccionar un objeto como un archivo o URL, antes de llevar a cabo un análisis nuestros productos revisan la caché local (y **ESET Shared Local Cache**, en el caso de ESET Endpoint Security) en busca de objetos maliciosos u objetos benignos en una lista blanca. Esto **mejora el rendimiento del análisis**. Posteriormente, **nuestro sistema de reputación ESET LiveGrid® analiza su reputación** (esto es, si el objeto ya ha sido visto en otro lugar y clasificado como malicioso o no). Esto **mejora la eficacia del análisis y permite compartir más rápidamente información del malware con nuestros clientes.** Aplicar las listas negras de URLs y comprobar su reputación evita que los usuarios accedan a sitios con contenido malicioso o páginas de phishing.



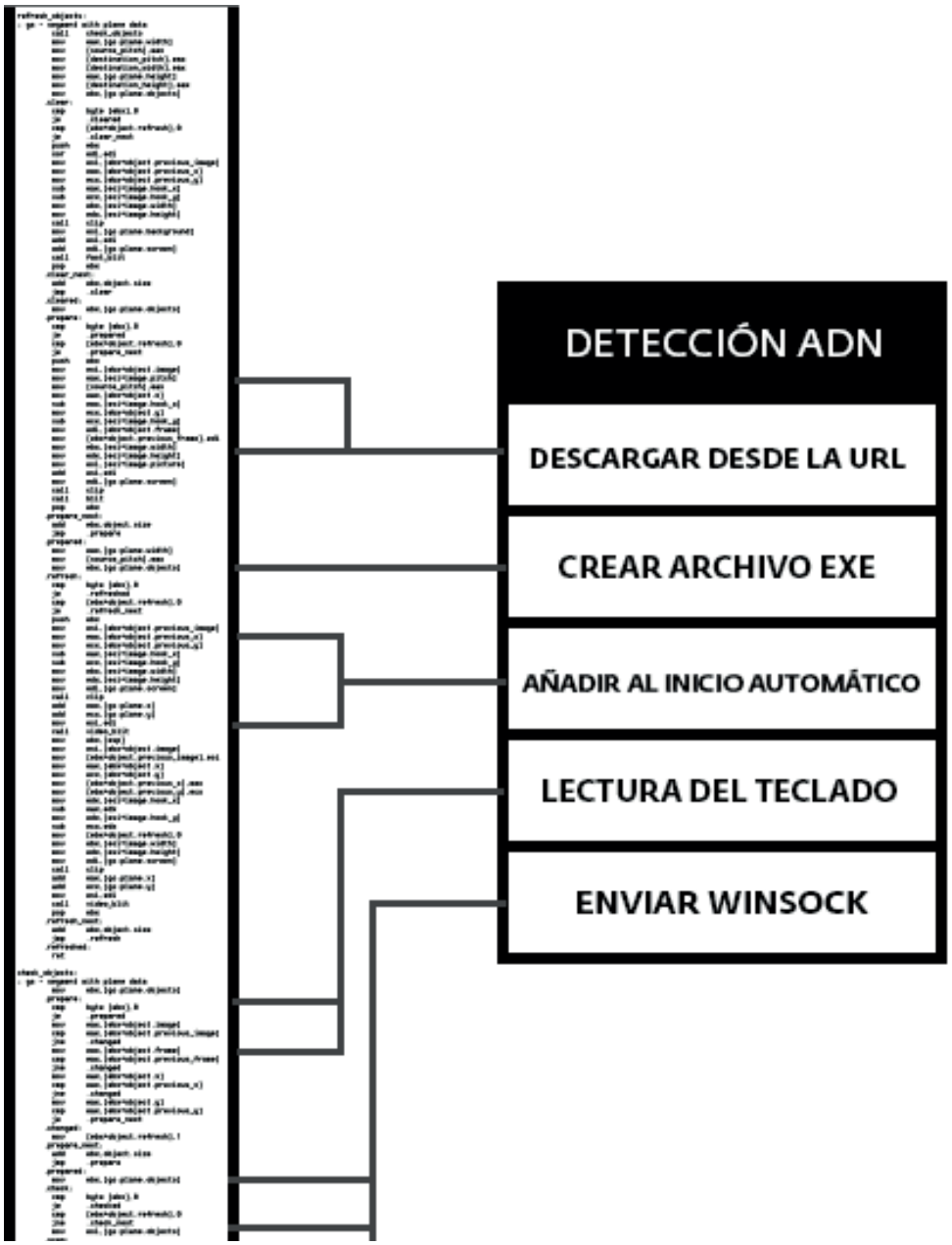
Detecciones por firmas ADN

Los tipos de detección varían desde funciones hash muy específicas (útiles, por ejemplo, para buscar determinados binarios maliciosos o versiones determinadas de malware, para objetivos estadísticos o simplemente para dar un nombre de detección más preciso al malware que hemos detectado previamente por heurística) hasta las **detecciones por ADN**, que **son definiciones complejas de comportamiento malicioso y características de malware.**

La correlación de modelos que utilizan los productos antivirus de la vieja escuela puede saltarse fácilmente con una simple modificación del código o el uso de técnicas de ofuscación. Sin embargo, el comportamiento de los objetos no puede cambiarse tan fácilmente. Las detecciones por ADN de ESET han sido diseñadas precisamente para sacar el máximo partido a este principio. Llevamos a cabo un análisis profundo del código, extrayendo los "genes" que son responsables de su comportamiento. Estos **genes de comportamiento contienen mucha más información que los indicadores de compromiso (IOCs, por sus siglas en inglés)** a los que algunas de las soluciones llamadas "next-gen" consideran "la mejor alternativa" a la detección por firmas. Los genes de comportamiento ESET se utilizan para construir Detecciones ADN, que se usan para analizar el código potencialmente sospechoso, tanto si se encuentra en el disco o en la memoria de los procesos en ejecución.

Adicionalmente, nuestro motor de análisis extrae muchos genes discriminadores, que se utilizan para la detección anómala: cualquier cosa que no tenga un aspecto legítimo es potencialmente maliciosa.

Dependiendo del nivel umbral ajustable y las condiciones de correlación, las detecciones por ADN pueden identificar determinadas muestras de malware conocido, nuevas variantes de una familia de malware conocida o incluso malware nunca antes visto o desconocido que contiene genes que indican comportamiento malicioso. En otras palabras, **una única descripción de comportamiento por ADN bien ensamblada puede detectar decenas de miles de variantes de malware** relacionadas y permitir que nuestro antivirus no solo detecte el malware ya conocido o visto anteriormente, sino **también nuevas variantes desconocidas**. Además, la clusterización automática y la aplicación de algoritmos de aprendizaje de máquinas a nuestro conjunto de muestras maliciosas nos permite identificar nuestros genes maliciosos y modelos de comportamiento para la detección de nuestro motor de análisis. Estos genes pueden compararse fácilmente contra una lista blanca enorme para asegurarse de que no generen falsos positivos.

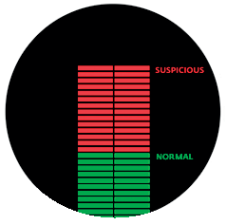


Bloqueo de exploits

La tecnología ESET protege contra varios tipos de vulnerabilidades a diferentes niveles: nuestro motor de análisis protege contra los exploits que aparecen en archivos de documentos malformados; la Protección contra ataques de red se dirige a nivel de la comunicación; y finalmente, el Bloqueo de exploits bloquea el proceso de aprovechamiento de vulnerabilidades en sí.

El Bloqueo de exploits monitoriza las aplicaciones típicamente aprovechables (navegadores, lectores de documentos, clientes de correo electrónico, Flash, Java y más) y en vez de dirigirse a identificadores *CVE particulares*, **se centra en las técnicas de aprovechamiento de las vulnerabilidades**. Cada exploit es una anomalía en la ejecución del proceso y buscamos anomalías que sugieran la presencia de técnicas de aprovechamiento de las vulnerabilidades. Como la tecnología está en constante desarrollo, se añaden regularmente nuevos métodos de detección para protegerse contra las nuevas técnicas de aprovechamiento de vulnerabilidades. Cuando se activan, se analiza el comportamiento del proceso, y si se considera sospechoso, **se puede bloquear la amenaza inmediatamente en el equipo**, con el envío adicional de metadatos al sistema en la nube ESET LiveGrid. Esta información se procesa y correlaciona, lo cual **nos permite detectar amenazas desconocidas hasta entonces llamadas ataques zero-day**, y nos proporciona al laboratorio información muy valiosa.

El Bloqueo de exploits añade otra capa de protección, un paso más cerca de los atacantes, utilizando tecnología que es completamente diferente a las técnicas de detección que se centran en analizar el código malicioso en sí.



Análisis avanzado de memoria

El Análisis avanzado de memoria es **una tecnología única de ESET** que **soluciona** una incidencia importante del malware más reciente: el fuerte uso de la **ofuscación del código o cifrado**.

Estas tácticas de protección del malware, a menudo utilizadas en empaquetadores en el momento de ejecución y protectores del código, causan problemas para tipos de detección que emplean técnicas de desempaquetado como la emulación o el sandboxing (aislamiento de procesos). Más aún, si la comprobación se realiza usando un emulador o sandboxing virtual/físico, no existe ninguna garantía de que durante el análisis el malware muestre comportamientos maliciosos que permitan que sea clasificado como tal. El malware se puede ofuscar de forma que no se analicen todas las rutas de exclusión; puede contener activadores condicionales o temporales para el código; y, muy frecuentemente, puede descargar nuevos componentes durante su ciclo vital. Para solucionarlo, el Análisis avanzado de memoria monitoriza el comportamiento de un proceso malicioso y lo analiza cuando se ejecuta en memoria. Esto complementa la funcionalidad más tradicional de análisis proactivo del código antes de ejecutarse o durante la ejecución.

Asimismo, los procesos legítimos se pueden volver maliciosos repentinamente debido al aprovechamiento de vulnerabilidades (exploitation) o la inyección de código. Por estas razones, realizar un análisis solo una vez no es suficiente. Se necesita una monitorización constante, y esta es la función del Análisis avanzado de memoria. **Siempre que un proceso realice una llamada al sistema desde una nueva página ejecutable, el Análisis avanzado de memoria realiza un análisis conductual del código usando las Detecciones ADN de ESET.**

El análisis del código se realiza no solo para la memoria ejecutable estándar, sino también para el código .NET MSIL (Microsoft Intermediate Language) usado por los creadores de malware para evitar el análisis dinámico. Debido a la implementación de la caché inteligente, el Análisis avanzado de memoria no tiene casi carga y no ocasiona ninguna disminución perceptible en la velocidad de los procesos.

El Análisis avanzado de memoria se lleva bien con el Bloqueo de exploits. A diferencia del último, es un método posterior a la ejecución, lo cual implica que existe el riesgo de que ya haya ocurrido alguna actividad maliciosa. Sin embargo, **participa en la cadena de protección como último recurso** si un atacante consigue saltarse otras capas de protección.

Además, existe una nueva tendencia en el malware avanzado: algunos códigos maliciosos operan ahora "solo en memoria", sin necesidad de componentes persistentes en el sistema de archivos que puedan detectarse de forma convencional. Inicialmente, este tipo de malware aparecía solo en servidores, debido a su largo periodo de actividad –puesto que los servidores están conectados durante meses o años sin apagarse, los procesos maliciosos podrían permanecer en memoria de forma indefinida sin necesidad de sobrevivir a un reinicio del equipo– pero los ataques recientes en empresas indican un cambio en esta tendencia, y estamos observando ataques de este tipo a equipos convencionales. **Solo el análisis de memoria puede descubrir con éxito estos ataques maliciosos y ESET está preparado para esta nueva tendencia con el Análisis avanzado de memoria.**

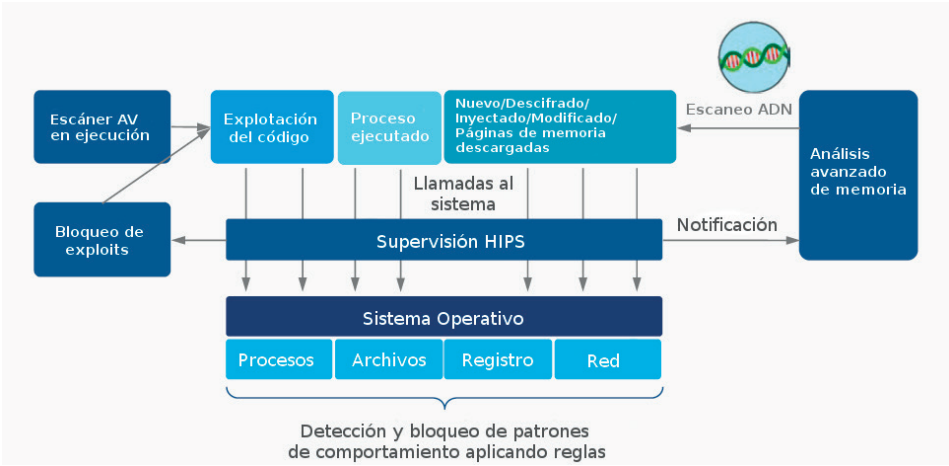
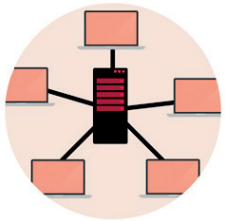


Fig.2: Cómo funciona la detección por comportamiento de ESET

Sistema de protección contra el malware en la nube

El sistema de protección contra el malware en la nube es una de las diversas tecnologías de ESET basadas en la nube, ESET LiveGrid. Las aplicaciones desconocidas y potencialmente maliciosas y otras posibles amenazas se monitorizan y envían a la nube de ESET mediante el sistema de respuesta ESET LiveGrid. **Las muestras recopiladas se someten al aislamiento de procesos (sandboxing) automático y al análisis de su comportamiento**, que finalizan con la creación de detecciones automáticas si se confirman sus características maliciosas. Los clientes de ESET reciben estas detecciones automáticas mediante el sistema de reputación en la nube ESET LiveGrid sin necesidad de esperar a la próxima actualización del motor de detección. El tiempo de este ciclo es típicamente inferior a 20 minutos, lo cual permite una detección eficaz de amenazas emergentes incluso antes de lanzar la actualización regular a los equipos de los usuarios.



Protección contra botnets

Un elemento caro para los creadores de malware es cambiar la comunicación con servidores C&C. **La protección contra botnets de ESET ha demostrado eficazmente ser capaz de detectar la comunicación maliciosa que utilizan las botnets, y al mismo tiempo identificar los procesos ofensivos.**

Las detecciones de red de ESET amplían la tecnología contra botnets para solucionar problemas generales asociados con el análisis del tráfico de red. **Permiten una detección más rápida y flexible del tráfico malicioso**. Las firmas estándar de la industria como Snort o Bro permiten la detección de muchos ataques, pero las detecciones de red de ESET están específicamente diseñadas para detectar las vulnerabilidades de la red, los kits de exploits y la comunicación del malware avanzado en particular.

La capacidad de realizar análisis del tráfico de red en equipos tiene ventajas adicionales. Permite identificar exactamente qué proceso o módulo es responsable de la comunicación maliciosa y también permite tomar decisiones contra el objeto identificado, y algunas veces permite incluso evitar el cifrado de la comunicación.

Protección reactiva vs proactiva en la actualidad

Aunque las Detecciones de ADN son excelentes para detectar incluso familias enteras de malware, deben distribuirse a los usuarios para protegerlos. Lo mismo sucede con el motor de análisis, la heurística o cualquier cambio centrado en las nuevas amenazas. Hoy en día, es necesaria la comunicación con el sistema ESET LiveGrid en la nube para garantizar el nivel más elevado de protección por muchas razones:

- **El análisis offline es en su mayoría reactivo.** Ser proactivo hoy en día ya no significa tener la mejor heurística en el producto. Mientras estén disponibles las herramientas de protección para un atacante, no importa si estás usando firmas, heurística o aprendizaje de máquinas: un creador de malware puede experimentar con tu tecnología de detección, modificar el malware hasta que no se pueda detectar y solo entonces lanzarlo. ESET LiveGrid contraataca esta estrategia del malware.
- **Las actualizaciones no son en tiempo real.** Pueden lanzarse actualizaciones más a menudo, y pueden incluso instalarse remotamente cada pocos minutos. Pero, ¿esto puede mejorarse? Sí, ESET LiveGrid permite la protección instantánea, proporcionando información cuando sea necesaria.
- **El malware intenta volar bajo el radar.** Los creadores de malware, especialmente en el caso del ciberespionaje, intentan evitar su detección al máximo. Los ataques dirigidos, a diferencia de las distribuciones masivas como los gusanos por correo electrónico, envían piezas únicas de malware a un pequeño número de objetivos, y a veces solo a uno. Usamos este hecho contra los creadores de malware: los objetos que no son populares y no tienen buena reputación asumimos que son potencialmente maliciosos y se analizan en detalle en el equipo o se envían para su análisis automatizado mediante el sistema de respuesta LiveGrid Feedback. El sistema de reputación ESET LiveGrid contiene información de archivos, su origen, similitudes, certificados, URLs e IPs.

Protección usando ESET LiveGrid

La forma más simple de ofrecer protección usando un sistema en la nube es mediante la creación de listas negras exactas usando hashing (resúmenes criptográficos). Esto funciona bien tanto para archivos como URLs, pero solo es capaz de bloquear objetos que coincidan exactamente con el hash. Esta limitación ha llevado a la invención de hashes borrosos. Los hashes borrosos tienen en cuenta el parecido binario de objetos, porque los objetos semejantes tienen el mismo hash o similar.

ESET ha elevado los hashes borrosos a un nivel superior. No llevamos a cabo hashes de datos, sino hashes del comportamiento descrito en las detecciones de ADN. Usando los hashes de ADN podemos bloquear miles de variantes diferentes de malware al instante.

Fig.3: Número de archivos únicos (eje X) detectados por hashes ADN individuales (eje Y).

Proporcionar una lista negra instantánea a los usuarios no es el único objetivo del Sistema de protección contra el malware en la nube. Si un usuario decide participar en el proceso de envío de muestras, siempre que se identifique una nueva muestra de dudosa reputación se envía a ESET para un análisis profundo. Para aprovechar al máximo el potencial del Sistema de protección contra el malware en la nube, los usuarios deberían también habilitar el Sistema de respuesta de ESET LiveGrid, que nos permite recopilar muestras sospechosas de dudosa reputación para llevar a cabo un análisis profundo.

Procesamiento automatizado y manual de muestras

Cada día, ESET recibe cientos de miles de muestras, que se procesan automáticamente, semiautomáticamente y manualmente después de preprocesarlas y agruparlas en clústeres. **El análisis automatizado se realiza mediante herramientas desarrolladas internamente en una selección de equipos virtuales y reales**. La clasificación se realiza usando diferentes atributos extraídos durante la ejecución según análisis estáticos y dinámicos de código, cambios introducidos en el sistema operativo, modelos de comunicación de la red, el parecido con otras muestras de malware, características ADN, información estructural y la detección de anomalías.

Todos los clasificadores automáticos tienen inconvenientes:

- **Elegir características de discriminación para la clasificación no es trivial** y debe llevarse a cabo usando el conocimiento de humanos expertos en el campo del malware.
- **Los clasificadores de aprendizaje de máquinas requieren la participación de humanos expertos** para comprobar la información utilizada para el aprendizaje. Con el procesamiento totalmente automatizado, donde las muestras clasificadas por el sistema se utilizarían como información para el sistema, el efecto bola de nieve del círculo de información positiva lo volvería rápidamente inestable. "Basura dentro, basura fuera."
- Los algoritmos del aprendizaje de máquinas no entienden la información e **incluso si la información es estadísticamente correcta, eso no significa que sea válida**. Por ejemplo, el aprendizaje de máquinas no puede distinguir nuevas versiones de programas legítimos frente a las versiones no legítimas, no puede distinguir un actualizador vinculado a una aplicación legítima de una aplicación de descarga utilizada por el malware y no sabe reconocer cuándo se utilizan componentes de programas legítimos con objetivos maliciosos.
- Con el aprendizaje de máquinas, añadir nuevas muestras a un proceso de aprendizaje puede causar falsos positivos, y eliminar falsos positivos puede reducir la efectividad de la detección de casos positivos reales.
- Mientras que el procesamiento automático permite respuestas automáticas a nuevas amenazas con la detección mediante ESET LiveGrid, el procesamiento adicional de muestras mediante ingenieros de detección es crucial para asegurar la máxima calidad en la tasa de detección y el menor número de falsos positivos.

Servicios de reputación

ESET LiveGrid también proporciona reputación para objetos. Valoramos la reputación de varias entidades, entre ellas archivos, certificados, URLs e IPs. Como se ha descrito antes, la reputación puede utilizarse para identificar nuevos objetos maliciosos o fuentes de infección. Existen, además, otros usos.

Lista blanca del análisis

La creación de listas blancas de análisis es una característica que reduce el número de veces que el motor de análisis necesita inspeccionar un objeto. Si estamos seguros de que un objeto no ha sido modificado y es legítimo, no existe necesidad de realizar ningún análisis. Esto tiene un impacto muy positivo en el rendimiento y contribuye a hacer que los productos ESET sean tan poco intrusivos. Como decimos nosotros, "el código más rápido es el código que no se ejecuta". Nuestras listas blancas están en constante adaptación a la realidad cambiante del mundo del software.

Recopilación de inteligencia

Si un usuario decide participa enviando estadísticas a ESET LiveGrid, usamos esta información para el rastreo global y la monitorización de amenazas. Esta información nos proporciona abundantes datos de investigación con los que trabajar y **nos permite centrarnos en los casos más urgentes y problemáticos, observar tendencias en el malware y planificar y priorizar el desarrollo de tecnologías de protección.**

Sobre FPs e IOCs

Los Indicadores de compromiso (IOCs, en inglés) se consideran algo muy importante en el mundo de la seguridad corporativa actual. Sin embargo, distan mucho de ser especiales o avanzados aunque se ponga el acento sobre ellos por parte de los fabricantes autodenominados como "next-gen". En el gráfico adjunto puede observarse un desglose de los IOCs más relevantes y en qué se basan*. Como podemos observar, las características en las que se centran son extremadamente básicas: en el 25% de los casos se trata de MD5 conocidos, nombres de archivos, etc. Estos resultados demuestran que no es un método apropiado para la prevención y el bloqueo, aunque pueden resultar útiles para el análisis forense. Resulta irónico que algunos de los fabricantes "next-gen" que desechan las detecciones basadas en firmas por considerarlas "obsoletas" alaben tanto a los IOCs a pesar de que estos sean, de hecho, la manera más débil de detectar archivos maliciosos o eventos mediante bases de firmas.

*Fuente de la información: IOC Bucket, abril de 2015. IOC Bucket es una plataforma gratuita llevada por la comunidad dedicada a proporcionar a la comunidad de seguridad una forma para compartir información sobre amenazas.

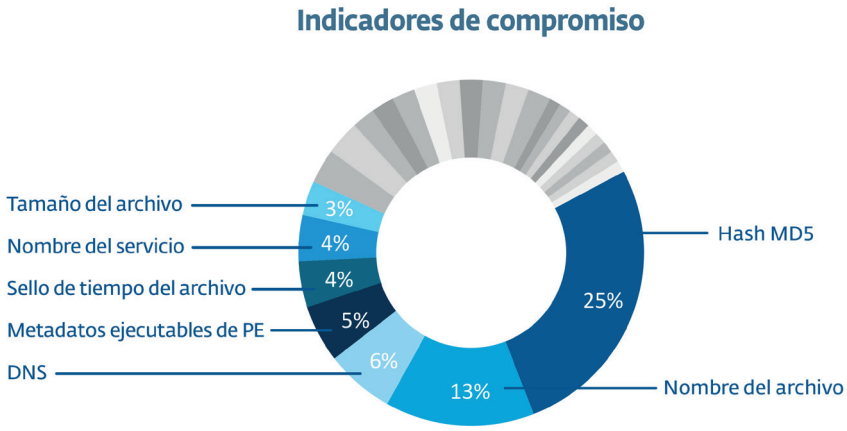


Fig.4: Análisis de indicadores de compromiso de IOC Bucket (muestra de abril 2015).

Conclusión

No existe ningún remedio infalible en la seguridad. El malware actual –dinámico y a veces dirigido– requiere un enfoque multicapa basado en tecnologías proactivas e inteligentes que tienen en cuenta petabytes de información recopilada a lo largo de muchos años por investigadores experimentados. Hace ya 20 años, ESET reconoció que el antivirus –el enfoque tradicional– era una solución incompleta, un punto en el que empezamos a incorporar tecnologías proactivas a nuestro motor de análisis e implementamos gradualmente diferentes capas de protección para dar en el blanco en diferentes fases de la cadena del cibercrimen.

ESET es uno de los pocos fabricantes de seguridad capaces de proporcionar un alto nivel de protección basado en 30 años de investigación. Esto nos permite ir por delante del malware, mantener nuestras tecnologías en constante evolución para ir más allá del uso de firmas estándar estáticas. Nuestra combinación única de tecnologías basadas en los equipos y aumentadas en la nube proporciona la seguridad más avanzada del mercado contra el malware.