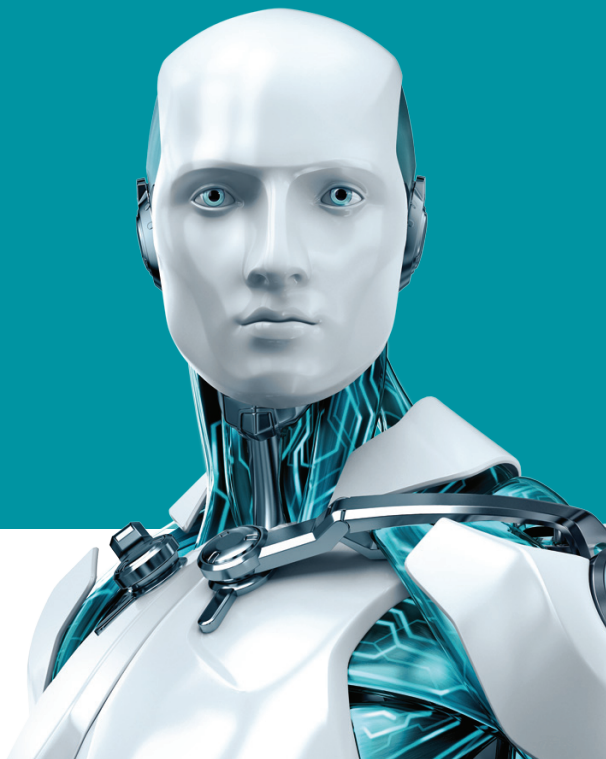
ESET vs CRYPTORANSOMWARE

¿Qué, cómo y por qué?



ENJOY SAFER TECHNOLOGY™

Índice

INTRODUCCIÓN

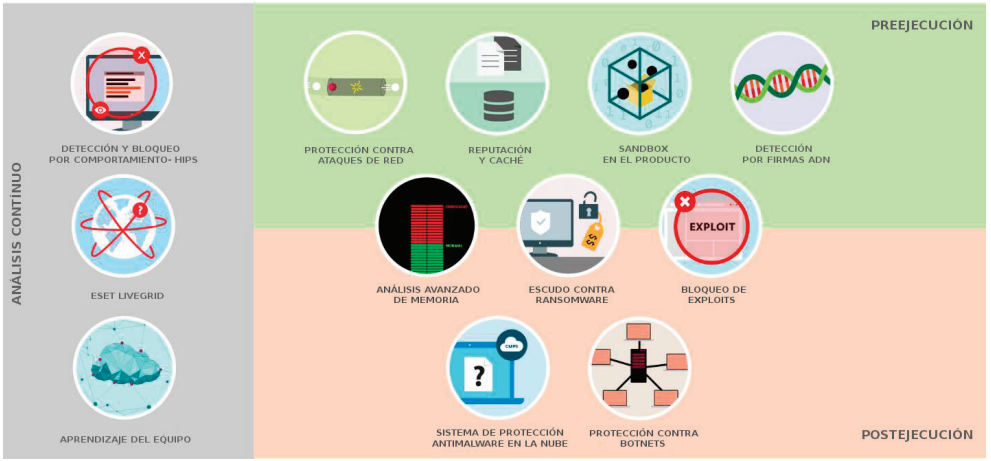
El cryptoransomware (o filecoders) ha ido creciendo ininterrumpidamente desde el 2013, cuando apareció el tristemente célebre CryptoLocker. Desde entonces, los cibercriminales han recaudado millones de dólares extorsionando a las víctimas a cambio de descifrar la información previamente robada. En 2016, *las previsiones a partir de los hallazgos del FBI* sugerían que el ransomware iba a convertirse en el crimen de los **1000 millones de dólares al año.**

Las ganancias de los cibercriminales demuestran el impacto de esta tendencia exponencial y son el principal motivo de por qué el cryptoransomware se ha convertido en el malware elegido en muchas campañas de virus. No debe sorprendernos que la mayoría de campañas de ransomware usen kits de exploits y correos electrónicos con mensajes de ingeniería social como vector de infección, lo cual también contribuye a su gran crecimiento. De hecho, según el servicio PhishMe, *"más del 97% de los correos de phishing enviados en 2016 contenían ransomware..."*

ESET ha estado monitorizando la amenaza del ransomware muy de cerca y respondiendo a su rápida evolución. En 2016, hubo pocos días en los que los investigadores de ESET no encontraran una nueva familia de ransomware.

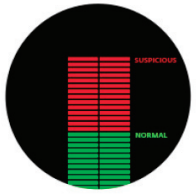
Sin embargo, a pesar de ser uno de los tipos de malware más importantes en actividad, es tan solo un tipo de malware más. Esto significa que ESET está combatiéndolo como lo hace con cualquier otro malware, mediante múltiples capas.

TODAS LAS CAPAS ACTIVADAS



La gran mayoría de ataques de ransomware son bloqueados por *la tecnología multicapa de ESET* antes incluso de que la infección en sí llegue a los equipos de las víctimas. Un buen ejemplo de esto es la detección de mensajes de correo electrónico que contienen "droppers" que podrían eventualmente descargar y ejecutar el ransomware.

Otro ejemplo es la detección de intentos de aprovechamiento de vulnerabilidades que permiten a los atacantes conseguir control remoto de los equipos de las víctimas y en muchos casos conducen a la extorsión por ransomware. Las Detecciones de red de ESET están diseñadas para prevenir esos intentos centrándose en las vulnerabilidades de red y en los kits de exploits. Además, el **Bloqueo de exploits** de ESET monitoriza los procesos de las aplicaciones en ejecución y busca anormalidades en su comportamiento. Su diseño permite a ESET detectar y bloquear eficazmente el aprovechamiento de vulnerabilidades, incluso las desconocidas llamadas zero-day, que podrían ser utilizadas por el cryptoransomware para acceder al equipo.



Para reforzar más los equipos de los usuarios, el **Análisis avanzado de memoria de ESET** está diseñado para descubrir la verdadera naturaleza de los procesos fuertemente escondidos, a menudo detectando el cryptoransomware antes de que pueda llegar a cifrar archivos valiosos. Este malware ofuscado constituye una parte significativa del tráfico malicioso actual, en su mayoría debido a los servicios de rempaquetado/ofuscación automáticos, disponibles en los "black markets". Pero incluso el código más ofuscado del mundo necesita revelarse en algún punto para poder ser ejecutable, y ese es exactamente el punto en el que nuestro Análisis avanzado de memoria lo atrapa, que es activado por el Sistema de prevención de intrusiones basado en el host de ESET (HIPS) justo en el momento adecuado.

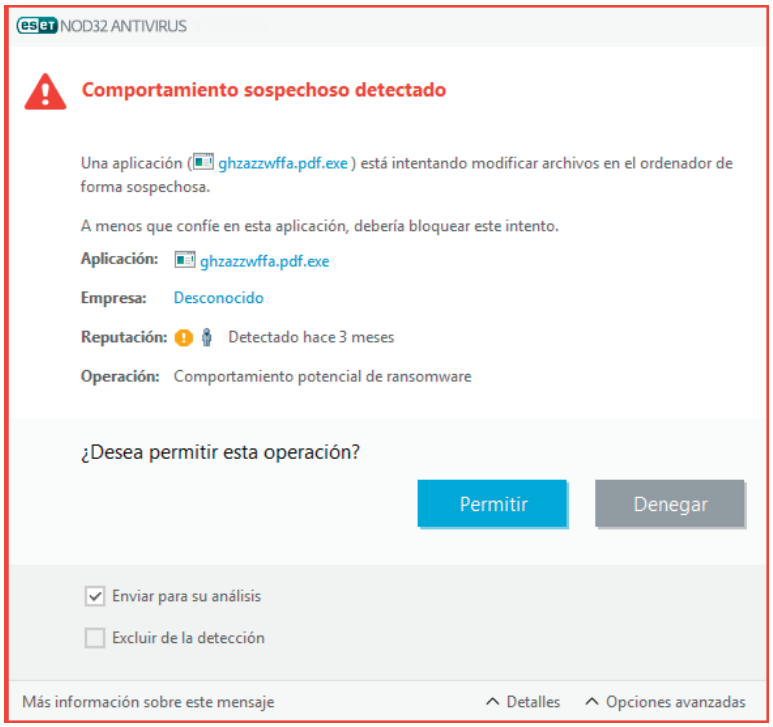
En resumen, cada capa de la tecnología multicapa de ESET usa diferentes medios para colaborar en un bloqueo eficaz del cryptoransomware. Además, los metadatos de cada una de estas capas pueden enviarse a nuestro sistema en la nube **ESET LiveGrid®**, que proporciona inteligencia avanzada a nuestros algoritmos de aprendizaje de los equipos. Estos sistemas automatizados, junto con la experiencia de nuestros investigadores e ingenieros, nos permiten acortar el tiempo de reacción frente a nuevas amenazas emergentes a unos minutos.

En nuestro empeño por alcanzar lo máximo posible la seguridad perfecta, ESET ha añadido otra capa adicional dirigida al fenómeno del ransomware.

Escudo contra ransomware ESET

El escudo contra ransomware ESET monitoriza y evalúa las aplicaciones ejecutadas usando heurística de comportamiento. Ha sido diseñado para detectar y bloquear comportamientos que puedan ser similares al ransomware.

Esta tecnología está activada por defecto. Si una actividad sospechosa activa el escudo antiransomware de ESET, se le solicitará al usuario que apruebe/deniegue una acción de bloqueo.



Además, el cuadro de diálogo permite al usuario enviar la aplicación sospechosa para su análisis, o excluirla de una futura detección.

¿POR QUÉ DE ESTA FORMA Y NO DE OTRA?

Entre las diversas formas posibles de combatir el ransomware, creemos que nuestro enfoque multicapa es el correcto. Y no solo lo creemos nosotros, su eficacia ha sido demostrada en innumerables análisis independientes por reputadas instituciones de análisis. Por ejemplo, en un *análisis por la organización de análisis independiente SE Labs, centrada en detección de ransomware, ESET obtuvo una puntuación del 100%. La palabra* "reputado" es muy importante: hay análisis que no proporcionan ningún tipo de valor informativo en absoluto. Algunos de ellos son incluso confusos, por ejemplo el llamado *RanSim.*

RanSim

Este programa podría ser un simulador, pero ciertamente NO simula el comportamiento de un cryptoransomware. Solo modifica los archivos que ha creado él mismo, de hecho solo simula un "ransomware" que solicita el pago por descifrar sus propios archivos. Ni incluso en el caso que todas las cientos de familias de ransomware "in the wild" compartieran este diseño tan ingenioso, no sería un ransomware real en absoluto.

Los productos ESET no detectan –ni lo harán jamás- este comportamiento como malicioso, por lo tanto "fallan" repetidamente en estos análisis. De hecho, si tuviera que detectarlo también tendría que detectar las técnicas de administración de permisos digitales usadas por plataformas de difusión digitales como Steam. Estas se comportan de forma parecida, descargando sus propios archivos cifrados –juegos en el caso de Steam- y los descifran en el momento adecuado.

La lista blanca de aplicaciones no es una solución infalible

La idea de listas blancas simples de aplicaciones seguras conocidas se discute como candidata para un tratamiento potente del cryptoransomware. Independientemente del objetivo de mantener el número de falsos positivos lo más bajo posible, existen varios temas que necesitan solución.

Los casos problemáticos, por ejemplo, incluyen cryptoransomware que se inyecta a sí mismo a un proceso que pertenece a una aplicación en una lista blanca. O cuando algunas de las aplicaciones de la lista blanca podrían interpretar comandos como wscript, autoit o cmd, y podría suponer un problema permitir o bloquear su ejecución, puesto que el código que están a punto de interpretar podría ser malicioso. Sin mencionar casos donde una aplicación legítima que sea capaz de cifrar archivos (un archivador, por ejemplo) se use incorrectamente para cifrar archivos.

No estamos afirmando que las listas blancas de aplicaciones no tengan sentido. Contribuyen a la capacidad general de detección de los productos ESET, sin embargo, sin otras capas de protección serían significativamente más débiles.

Shadow Copy es útil, pero no contra el cryptoransomware

Shadow Copy es una tecnología que permite realizar copias de seguridad manuales o automáticas o snapshots de archivos o volúmenes del equipo, incluso estando en uso. Sin embargo, hay algunos hechos a considerar antes de intentar usar este método como solución después de una infección por cryptoransomware.

En primer lugar, deberíamos tener en cuenta la posible pérdida de rendimiento en relación con la creación de volúmenes shadow copy y su almacenamiento. En segundo lugar, los volúmenes "shadow copy" pueden ser eliminados o cifrados por ransomware si no están protegidos. Además, si el ransomware empieza a cifrar los archivos repetidamente, el búfer dedicado a almacenar los cambios de archivos incrementales podría llegar a su límite. Y lo más importante, no deberíamos olvidar el ransomware de cifrado de discos (como *Petya*) contra el cual los volúmenes shadow copy serían totalmente inservibles.

¿Por qué no volver a una versión anterior como último recurso?

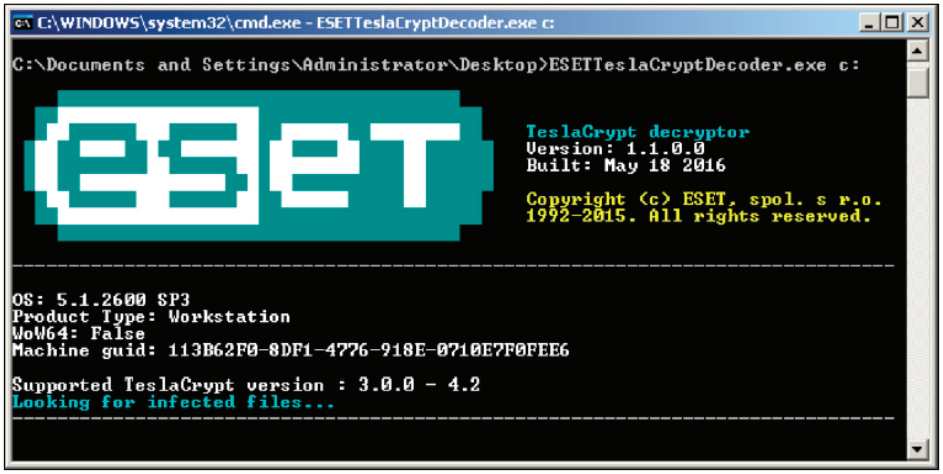
Existe una ventaja clara al tener la posibilidad de poder volver a una versión anterior implementada directamente en una solución de seguridad. Estamos continuamente probando y evaluando el impacto general de una solución así y podríamos implementar una en el futuro. En este punto, sin embargo, nuestros análisis sugieren que el enfoque actual, centrado principalmente en medidas proactivas, proporciona resultados óptimos.

OTRAS FORMAS CON LAS QUE ESET COMBATE EL RANSOMWARE

En ESET somos conscientes de que la lucha contra el malware, especialmente los tipos tan molestos como el cryptoransomware, necesita ir más allá de nuestras soluciones de seguridad estándar y la tecnología implementada en ellos. Por ese motivo nuestros investigadores están continuamente buscando oportunidades para dificultar la actividad de los cibercriminales.

En el caso del cryptoransomware, esto significa encontrar errores en su implementación o agujeros en la infraestructura de los cibercriminales. Aprovechamos cada oportunidad de crear herramientas de descifrado de ransomware que ayudan a las víctimas a conseguir recuperar su información. En la mayoría de los casos, desarrollamos herramientas de descifrado a medida del caso específico de la víctima, puesto que existen muchas variables específicas del sistema a tener en cuenta. Sin embargo, siempre que es posible creamos esas herramientas de descifrado y las ofrecemos gratuitamente al público en general. Nuestra herramienta de descifrado TeslaCrypt, que ha sido descargada más de 100.000 veces, es uno de esos casos.

De forma parecida al enfoque proactivo que toman nuestros productos para combatir el cryptoransomware, también compartimos los resultados de nuestras investigaciones llevadas a cabo en diversos centros de investigación de ESET.



Publicamos frecuentemente artículos de investigación sobre el cryptoransomware en nuestro blog corporativo *www.blogs.protegerse.com*, para concienciar a los usuarios sobre esta amenaza global.

Compartimos nuestros hallazgos con investigadores de todo el mundo, tanto si trabajan para nuestra competencia más directa o fuerzas y cuerpos de seguridad como el FBI. Ser una de las primeras empresas privadas en apoyar el *proyecto "No more ransom"* es una de las muchas formas en las que ESET ha demostrado su dedicación a luchar contra el cryptoransomware.

CONSEJOS BÁSICOS PARA PROTEGERTE CONTRA EL RANSOMWARE

El ransomware es tan solo otra familia de malware. La única diferencia es que va en busca de tus archivos, por lo que además de todo lo que hagas para evitar infectarte (los vectores de ataque son en su mayoría correos electrónicos y kits de exploits), necesitas tener una política de copias de seguridad razonable, pudiendo restaurar rápidamente. Las soluciones de "journaling" utilizan mucha CPU/disco y realmente no quieres usarlas hasta que aparece una infección por ransomware (lo cual ya es demasiado tarde). Para limitar los vectores de ataque:

1. Configura de forma apropiada los equipos y tu producto de seguridad.
2. Actualiza y parchea el sistema operativo y programas regularmente, puesto que el ransomware a menudo usa vulnerabilidades conocidas. Presta especial atención a los navegadores en este aspecto.
3. Las soluciones de seguridad en los equipos y a nivel perimetral son obligatorias, y deben estar configuradas apropiadamente para poder usar todo el conjunto de características, como las detecciones rápidas en la nube.
4. Usa todas las posibilidades que tu sistema ofrezca para fortalecerlo:
    a. Elimina la capacidad de ejecutar código que no es de confianza con AppLocker o Políticas de restricción de programas.
    b. Deshabilita el scripting en sistemas operativos y navegadores web;
    c. Deshabilita servicios innecesarios como RDP.
    d. Haz que el sistema operativo muestre las extensiones de los archivos;
    e. Sopesa la posibilidad de deshabilitar Windows Script Host.
    f. Configura "Abrir con..." para las extensiones que se usan a menudo para infecciones con un lector (como el Bloc de notas) en vez de un programa que interprete el código.
    g. Bloquea la ejecución de aplicaciones de las carpetas %LocalAppDa ta% y %AppData%.
5. Deshabilita el acceso innecesario a unidades de red compartidas.
6. No utilices servidores como equipos de escritorio (por ej., para navegar por internet).

ENJOY SAFER TECHNOLOGY™