Tácticas y técnicas de delito cibernético: estado del malware en el 2017

Presentado por

Malwarebytes LABS

Índice

Resumen ejecutivo

El 2017 fue un año tumultuoso en cuestión de política, medios, género, problemas raciales... y la ciberseguridad no se quedó atrás. El año pasado estuvo lleno de giros inesperados en el mundo del crimen cibernético, con importantes brotes, nuevos métodos de infección y la evolución de la industria del crimen de criptomonedas que dejó a los investigadores no solo en alerta, sino completamente perplejos.

Tratando de encontrar algún sentido a tanto caos, obtuvimos información a través de nuestros equipos de ciencia, investigación e inteligencia de datos a lo largo del año y estuvimos al pendiente de las tendencias, las vicisitudes de las familias de malware, los métodos de distribución y más. Para crear el informe, analizamos la telemetría que recopilamos de nuestros productos en los periodos de enero a noviembre del 2016 y de enero a noviembre del 2017. Además de esto, combinamos los datos recopilados por nuestros sistemas señuelo (honeypots) en el 2017 con las observaciones y los análisis de los investigadores de Malwarebytes. Lo que un obtuvimos fue un panorama más completo de las amenazas del 2017 que nos mostró lo mucho que las cosas pueden cambiar en tan solo un año.

Este informe especial de fin de año abordará las tácticas de infección, los métodos de ataque y las técnicas cambiantes de desarrollo y distribución que los criminales cibernéticos han utilizado en los últimos 12 meses. Profundizaremos en el aumento exponencial en el volumen y la severidad del malware que se presenta año con año (y los tipos de malware que experimentaron reducciones), así como las tendencias en amenazas de alto impacto como el ransomware y la criptominería. En última instancia, mostraremos una evolución del crimen cibernético que seguramente nos traerá más problemas en el 2018.

Puntos clave para empresas y consumidores

El volumen de ransomware subió en el 2017, pero su actual tendencia es a la baja.

El año pasado quedó claro que, al menos cuando se trató de ataques a empresas, el ransomware fue la herramienta predilecta. Nuestra telemetría muestra que en el 2017 las detecciones de ransomware aumentaron en un 90 por ciento para los clientes empresariales, rebasando las cifras del año pasado para convertirse en la quinta amenaza más detectada. El ransomware también tuvo un año récord entre los consumidores con índices de detección de hasta 93 por ciento en el 2016.

A pesar de haber tenido un año destacado con brotes significativos, el desarrollo de nuevas familias de ransomware se vio estancado. Conforme se aproximaba el fin de año, hubo un gran cambio de distribución debido a la diversificación de la carga en muchas de las vías conocidas para la distribución del ransomware, donde se optó en lugar de este último por los troyanos bancarios y los mineros de criptomonedas.

Si no pueden pedir rescate por algo, los criminales recurrirán al robo.

Con el lento declive del ransomware, los criminales recurrieron a los troyanos bancarios, el spyware y los hijackers en el 2017 para atacar a las empresas. Estos tipos de malware se utilizaron para robar datos, credenciales de ingreso, listas de contactos, datos de tarjetas de crédito, así como para distribuir más malware y espiar a la víctima con el fin de obtener información sobre su empresa o sobre cómo infiltrarse más en su red. Vimos un aumento del 40 por ciento en detección de hijackers y un 30 por ciento en detección de spyware en el 2017. La segunda mitad del año también marcó un aumento promedio de 102 por ciento en la detección de troyanos bancarios.

Las 10 detecciones principales para empresas		
2016	vs.	2017
Herramienta de fraude	1	Hijacker
Adware	2	Adware
Hijacker	3	Herramienta riskware
Herramienta riskware	4	Backdoor
Backdoor	5	Ransomware
Herramienta hack	6	Spyware
Gusano	7	Gusano
Herramienta crack	8	Herramienta hack
Troyano bancario	9	Herramienta de fraude
Ransomware	10	Troyano bancario

Figura 1. Las 10 principales amenazas del 2016 y el 2017

Las amenazas a los consumidores van en aumento.

Desde el punto de vista del consumidor, cada año, sin falta, el malware se está convirtiendo en un problema aun más severo. En el 2017, las detecciones totales de amenazas para los consumidores aumentaron en un 12 por ciento. Esto concuerda con la observación de que evolucionaron los métodos de desarrollo y distribución en el 2017, lo cual permitió que se crearan y se distribuyeran más amenazas a las víctimas.

El volumen de adware ha aumentado, pero hay menos participantes en la actividad.

Las detecciones de adware en el 2017 mostraron un volumen inmenso de distribución de hasta 132 por ciento año con año. Subió del puesto número dos en nuestra lista de amenazas más comunes para el consumidor en el 2016 al número uno en nuestra lista del 2017. El adware representa actualmente casi el 40 por ciento de nuestras detecciones de amenazas al consumidor, mientras que en el 2016 representaba el 20 por ciento. Sin embargo, debido a que más compañías de seguridad están detectando programas potencialmente no deseados, existen menos creadores que estén produciendo adware nuevo. A pesar de esto, los desarrolladores que siguen en pie están utilizando tácticas de malware para evitar la detección y persistir.

La criptominería está fuera de control.

Aprovechando la nueva popularidad de las criptomonedas, los maleantes han empezado a utilizar herramientas de criptominería para su propio beneficio, utilizando los recursos del sistema de la víctima en el proceso. Este proceso incluye sitios web comprometidos que utilizan códigos de minería de tipo drive-by, un incremento significativo en la distribución de mineros a través de spam malicioso y exploit kits, así como paquetes de adware que distribuyen mineros en lugar de barras de herramientas. Hacia finales del 2017, prácticamente cualquier persona que realizara algún tipo de delito cibernético estaba también participando de alguna forma en la criptominería.

Las 10 detecciones principales para consumidores		
2016	vs.	2017
Herramienta de fraude	1	Adware
Adware	2	Herramienta de fraude
Herramienta riskware	3	Herramienta riskware
Backdoor	4	Backdoor
Herramienta hack	5	Herramienta hack
Hijacker	6	Gusano
Herramienta crack	7	Hijacker
Gusano	8	Herramienta crack
Troyano bancario	9	Ransomware
Rootkit	10	Spyware

Figura 2. Las 10 principales amenazas al consumidor en el 2016 y el 2017

Los criminales cibernéticos implementaron métodos de distribución más creativos en el 2017.

El 2017 será conocido como un año con vectores interesantes de infección, tal como observamos con los exploits filtrados del gobierno, tales como el EternalBlue, utilizado en el brote de ransomware WannaCry, procesos de actualización comprometidos y el aumento en el uso de la geolocalización para realizar ataques. Es probable que estas tácticas se hayan adoptado para evadir los métodos de detección tradicional que buscan las vías de infección más comunes.

Los exploit kits estuvieron a la baja, pero llegó el spam malicioso.

En un giro inesperado, los exploit kits no tuvieron mucho desarrollo en el 2017, ya que los exploit kits que siguen activos no utilizaron ningún exploit de día cero nuevo. Esto constituye un cambio significativo respecto a años anteriores, en los cuales los exploits fueron el principal método de infección. En lugar de esto, el desarrollo de tácticas de evasión de detección de spam malicioso, junto con la inclusión de múltiples exploits para los documentos de Microsoft Office, impulsaron el aumento en la entrega de malware a través de estos vectores.

Los estafadores pasaron de los bloqueos de navegador tradicionales a otras tácticas distintas.

Las estafas del 2017 se distinguieron por su cambio de táctica, ya que se alejaron de los tradicionales bloqueadores de navegadores e implementaron los correos electrónicos de suplantación de identidad y la publicidad maliciosa. Además, a finales de año vimos un alza en contenido relacionado con Bitcoin, en donde las estafas de soporte técnico pasaron a suplantar monedas populares como nueva treta.

Predicciones para el 2018

Como dijo alguna vez Mark Twain en *Viaje alrededor del mundo, siguiendo el Ecuador*, “La profecía es una buena línea de negocio, pero está llena de riesgos”. Somos conscientes de que hacer predicciones sobre el crimen cibernético tiene un poco más de arte que de ciencia, pero apoyándonos en años de patrones, datos y experiencia, podemos hacer pronósticos bien informados sobre hacia dónde pensamos que nos estamos dirigiendo.

Nuestras predicciones para el 2018 cubren bastante terreno, incluyendo el futuro de la minería de criptomonedas, posibles ataques al Internet de las cosas y malware para Mac. Los cibercriminales hicieron enormes esfuerzos en el 2017 para expandir las capacidades de las amenazas existentes y utilizarlas en formas nunca antes vistas. Es probable que esta tendencia continúe a lo largo del 2018; sin embargo, consideramos que habrá nuevas familias de malware y nuevas técnicas de infección que seguirán siendo implementadas. Mientras tanto, podemos aprender de las experiencias del año pasado y no solo implementar soluciones para proteger a nuestros sistemas de la siguiente gran amenaza, sino también concientizar a nuestros usuarios sobre cómo cuidarse de ella y evitarla.

Malware

Ransomware

Si ha estado siguiendo nuestros informes trimestrales del 2017, sabrá que ya hemos cubierto la peligrosidad y la escala de las amenazas ransomware este año. Esto incluye los brotes a gran escala de malware en forma de gusanos de ransomware, las familias dominantes de ransomware que se distribuyeron a lo largo del año y la consolidación del poder de unos cuantos grupos destacados.

Sin embargo, si analizamos el año entero, podemos ver que fue estadísticamente un año récord para el ransomware. De acuerdo con la telemetría recopilada de los productos de Malwarebytes, las detecciones de ransomware para empresas y consumidores aumentaron en un 90 y 93 por ciento, respectivamente, en el 2017. Esto se debe principalmente a familias como WannaCry, Locky, Cerber y GlobeImposter. De hecho, el índice mensual de ataques de ransomware contra empresas es hasta 10 veces mayor que el índice del 2016.

Un fuerte inicio

Mientras que a principios de año vimos principalmente a Locky y Cerber, el verano introdujo una oleada de infecciones de ransomware de nuevos participantes como GlobeImposter y Jaff. Entre julio y septiembre del 2017, hubo un aumento del 700 por ciento en ransomware (de acuerdo con la telemetría de Malwarebytes), con solo dos familias dominando la mayor parte de esas cifras:

- GlobeImposter aumentó en un 341 por ciento de julio a agosto del 2017.
- WannaCry tuvo un incremento del 375 por ciento de agosto a septiembre del 2017.

Además, casi el 7 por ciento de los ataques contra empresas en septiembre del 2017 involucró el uso de ransomware, mientras que en el 2016, el índice promedio de ataques de ransomware fue del 1.11 por ciento en total.

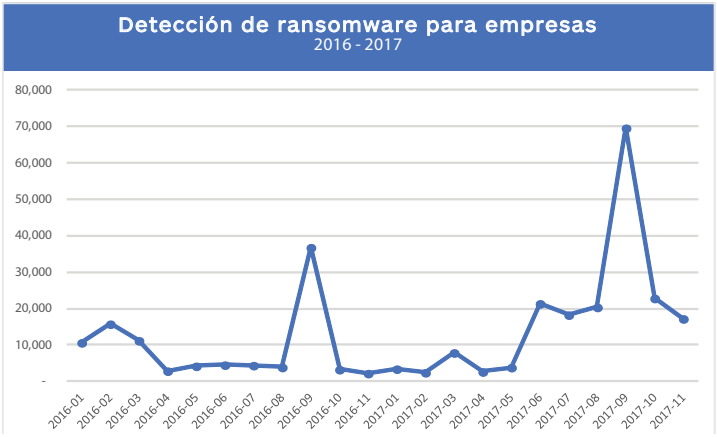

Figura 3. Detección de ransomware en empresas, 2016–2017

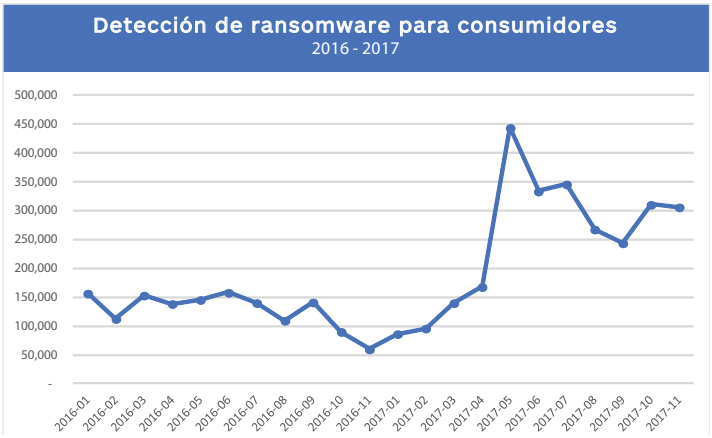

Figura 4. Detección de ransomware en consumidores, 2016–2017

Desarrollo estancado

A pesar de la gran cantidad de ataques de alto perfil, así como del increíblemente alto volumen de ransomware que se muestra en las figuras anteriores, el desarrollo de nuevo ransomware se ha visto un poco estancado. Los principales traficantes de ransomware están conformados por unas cuantas familias que acaparan la mayor parte del mercado, ya sea debido a que cuentan con un mejor producto en general que venden en la red oscura o porque tienen una relación especial con los portadores y distribuidores de botnets de spam malicioso y exploit kits (los métodos principales para la distribución de malware).

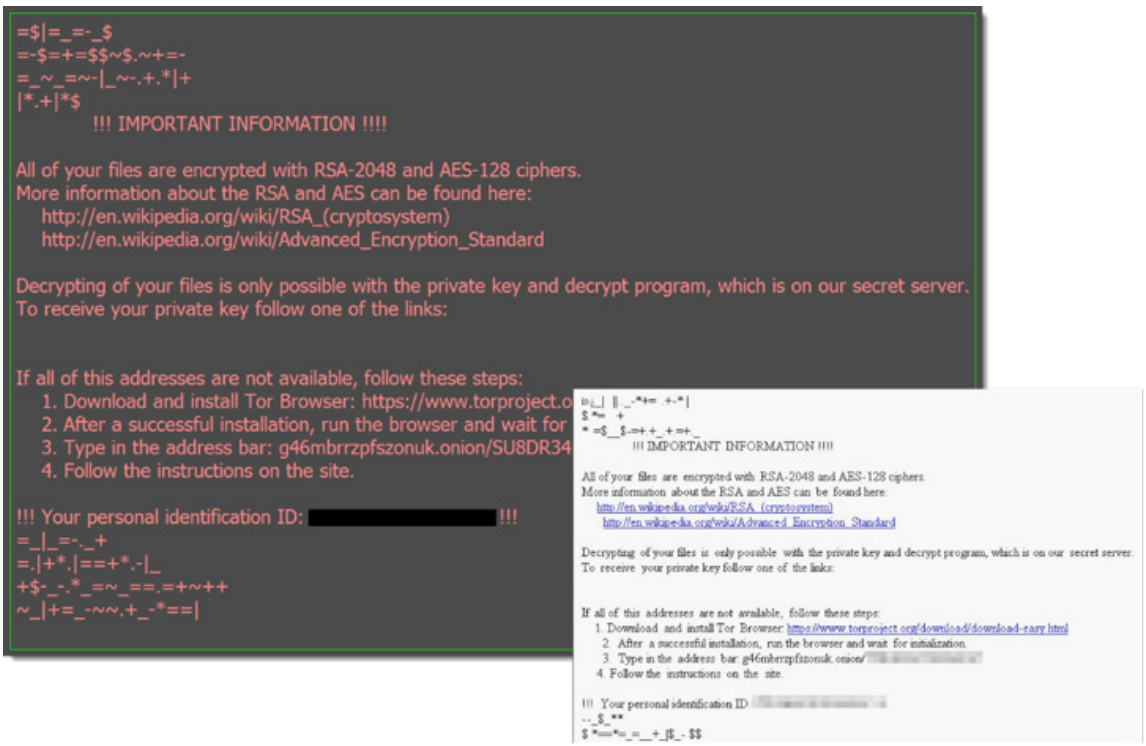

Figura 5. Pantalla de Locky y nota de rescate

La excepción a esta mala racha de innovación es la inclusión de la funcionalidad de gusano encontrada en familias de ransomware como WannaCry y NotPetya, algo sobre lo que estaremos discutiendo con mayor detalle en nuestra sección sobre EternalBlue.

Ransomware pasado de moda

A principios de año, la dominación que tenía el ransomware sobre los vectores de infección primaria hacía que pareciera que lidiar con este tipo de malware sería la norma de ahí en adelante. Sin embargo, las tendencias en los últimos meses han dejado atrás al ransomware. De hecho, muchos mecanismos de distribución de malware han optado por regresar a los viejos favoritos, como los troyanos bancarios y el spyware, o por unirse a la más reciente tendencia de los mineros de criptomonedas.

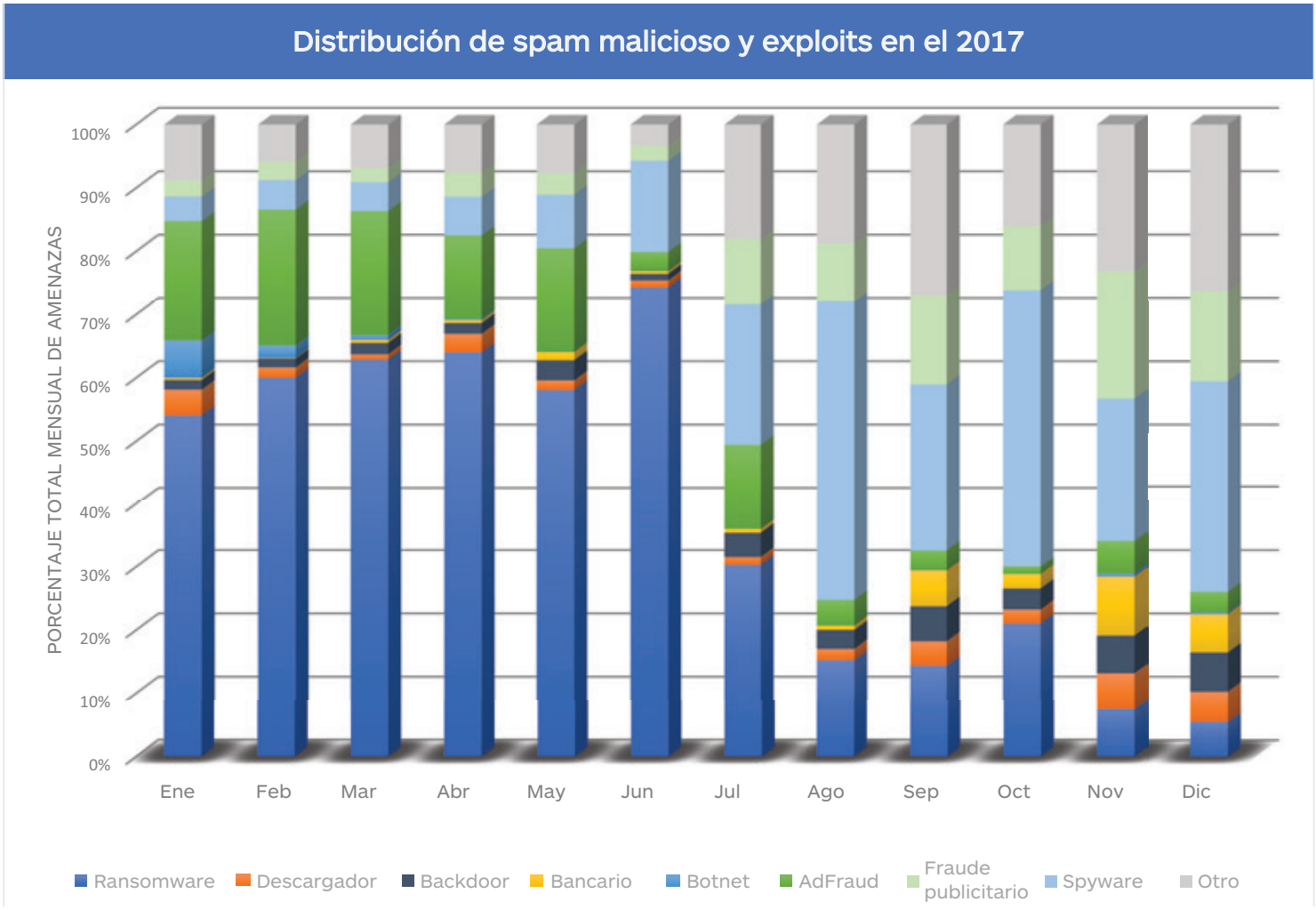

Figura 6. Distribución de spam malicioso y exploits en el 2017

La motivación más probable detrás de esta acción tiene que ver con un menor retorno de inversión para los grupos que se encuentran detrás de las familias más grandes de ransomware. La adopción y el uso de tecnología antiransomware, los respaldos de precaución y un mayor conocimiento general sobre las amenazas y los métodos de protección han tenido como resultado menos casos en los cuales se termina pagando el rescate. Por lo tanto, actualmente es más económico para los criminales utilizar criptomineros, malware de fraude publicitario y el tradicional robo de credenciales en lugar del ransomware.

Spyware

El spyware tuvo su mayor impacto tanto para empresas como para consumidores en la segunda mitad del 2017. Esto probablemente se debe a que los cibercriminales han tenido menos éxito con los ataques de ransomware.

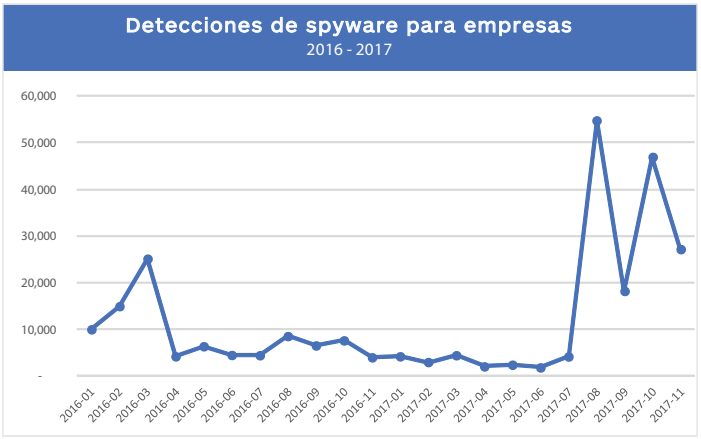

Figura 7. Detecciones de spyware para empresas en 2016-2017

El spyware, cuyo nombre incorpora el vocablo "spy" (o "espiar", en inglés), es una categoría de software malicioso que se crea con el fin de espiar al usuario. Esto se puede realizar a través de diversos métodos, incluyendo la captura de datos a través de capturas de imagen, capturas de cámara web, keylogging o robo de datos de los sitios web que el usuario visita.

La tabla anterior muestra las detecciones de spyware para clientes empresariales en el 2016 y el 2017. El incremento a finales del 2017 concuerda con la alta y baja en detecciones de ransomware durante ese mismo periodo. Esto indica que los criminales diversificaron su estrategia de ataque para incrementar su éxito utilizando diferentes tipos de malware.

El impacto empresarial de una fuerte campaña de ataque de spyware podría tener como resultado el robo de propiedad intelectual; sin embargo, también se podría utilizar para explorar la red corporativa e identificar los mejores puntos de ataque para lanzar formas más peligrosas de malware.

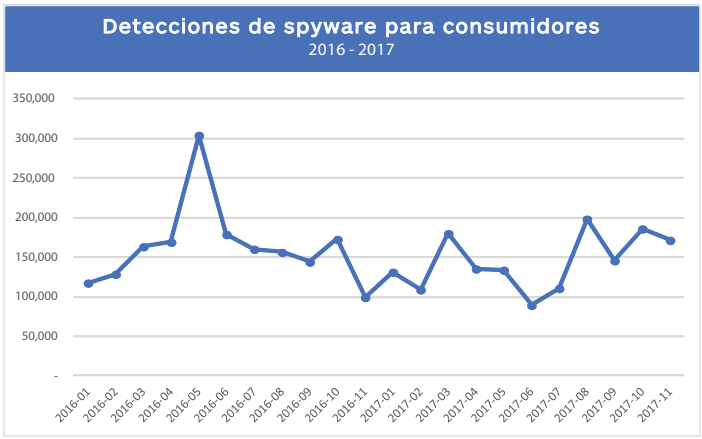

Figura 8. Detecciones de spyware para consumidores en 2016-2017

La tabla anterior muestra las detecciones de spyware para consumidores en los últimos dos años. Para los consumidores, el spyware se ha mantenido como una amenaza constante, terminando la segunda mitad del 2017 más fuerte que en la primera. Esta tendencia, que permanece generalmente constante, tiene sentido si tomamos en cuenta que el spyware que se utiliza contra un consumidor habitual es mucho más entretenido y probablemente satisfactorio que el que se utiliza con una víctima empresarial.

Consideramos que seguiremos viendo un flujo constante y continuo de spyware para consumidores e incrementos significativos en los ataques a empresas en el 2018.

Hijackers

Las tendencias de los hijackers fueron altamente contrastantes este año, ya que las empresas vieron un incremento significativo en las detecciones de hijackers, pero los consumidores experimentaron una caída dramática.

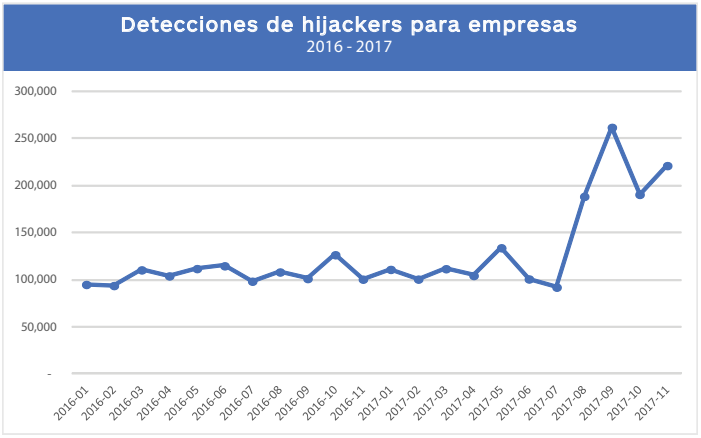

Figura 9. Detecciones de hijackers para empresas en 2016-2017

El mes de agosto del 2017 tuvo una cantidad nunca antes vista de detecciones de malware en forma de hijackers en el caso de empresas. Esta es una tendencia interesante tomando en cuenta que el principal método de infección de los hijackers es a través de la instalación de paquetes de programas de dudosa procedencia y potencialmente no deseados.

Los hijackers interactúan con y modifican las operaciones del navegador de la víctima para ejecutar publicidad y redirigir al navegador hacia buscadores de terceros o sitios de compras. Dependiendo de la familia de hijackers, también es posible que instalen malware adicional o que roben información personal.

Los hijackers tienen un fuerte impacto en las empresas principalmente al ocasionar tiempo de inactividad; sin embargo, también pueden propiciar otra infección adicional o algo peor. Por lo tanto, es altamente recomendable protegerse contra estos fastidiosos, pero engañosamente peligrosos tipos de malware.

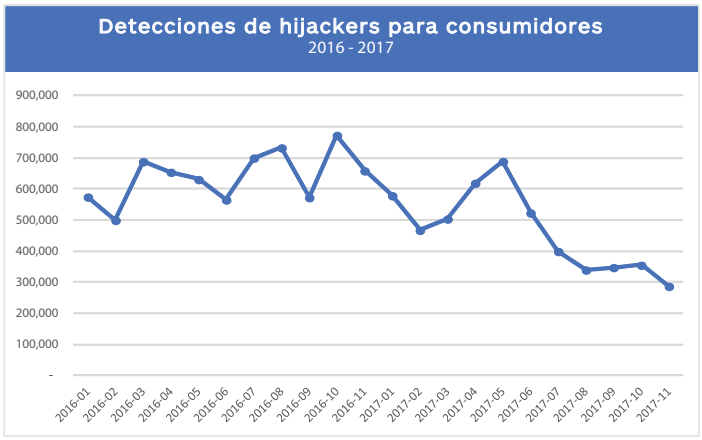

Figura 10. Detecciones de hijackers para consumidores en 2016-2017

Los consumidores se enfrentaron al problema opuesto, ya que las detecciones de malware en forma de hijackers tuvieron un declive en la segunda mitad del año. Esto concuerda con las observaciones que se hicieron anteriormente en el año, las cuales indicaban que había menos desarrolladores activos de paquetes de software diseñados para estafas, ya que estos paquetes son el principal método de distribución de estos hijackers.

Con esta caída continua en detecciones de hijackers, es poco probable que veamos un aumento significativo en el 2018, o, al menos, no llegará a la magnitud que en el 2016.

Troyanos bancarios

Antes del 2016, los troyanos bancarios estaban en todos lados. Algunas de las características más avanzadas utilizadas por el malware fueron diseñadas por familias con el propósito de robar información bancaria y financiera. Con el paso de los años, se fue haciendo menos y menos común, probablemente debido al aumento de medidas de seguridad tomadas por los bancos para evitar el fraude, así como la optimización de sus medidas de recuperación. Por ejemplo, si alguien le roba su tarjeta, usted la puede bloquear, solicitar que le envíen una nueva y revertir los cargos sin mucho esfuerzo.

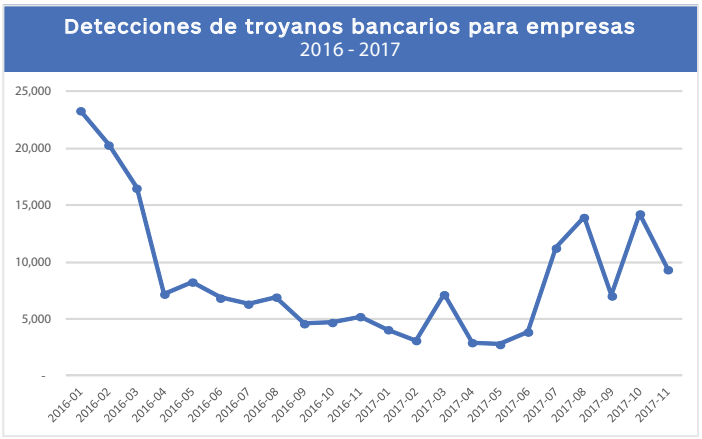

Figura 11. Detecciones de troyanos bancarios para empresas en 2016-2017

A pesar de la tendencia a la baja en los últimos años en la detección de troyanos bancarios para empresas, el fin de año experimentó un gran incremento en ataques con este tipo de malware. Como lo muestra la figura 11, se puede ver un incremento que empieza en julio del 2017 seguido por una reducción significativa en septiembre. Esto concuerda casi a la perfección con nuestras estadísticas de detección de spyware para clientes empresariales, lo cual probablemente significa que esta misma campaña que distribuía estos troyanos bancarios también distribuía spyware. Otra teoría es que un tipo de malware instalaba al otro, lo cual es bastante común.

El mayor impacto empresarial que podría tener este tipo de amenaza sería el robo de información financiera corporativa y personal por parte de criminales, la cual podrían utilizar para tratar de robar dinero o para vender en el mercado negro. El uso de este tipo de malware contra empresas a finales del año indica un declive en el retorno de inversión del ransomware que lleva a los cibercriminales a retomar los métodos de ataque tradicionales ya comprobados.

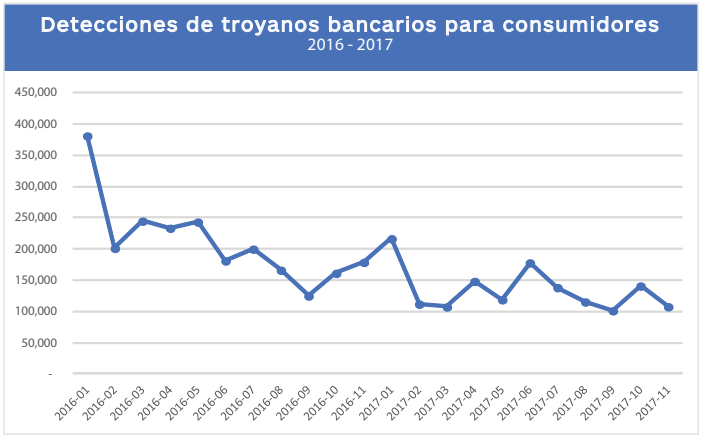

Figura 12. Detecciones de troyanos bancarios para consumidores en 2016-2017

El caso es el mismo para los consumidores, pero con un final distinto. El declive en la detección de troyanos bancarios a lo largo del año presagia el fin de este método de ataque y hace muy poco probable que regrese fortalecido en el 2018. Los avances en la seguridad bancaria y financiera contra el fraude y el robo han sido extraordinarios; es muy probable que estos hayan sido los factores contribuyentes más importantes que marcaron el declive de los troyanos bancarios. Sin embargo, todavía falta mucho por hacer para evitar que la información personal de las víctimas se utilice para abrir cuentas bancarias y tarjetas de crédito.

Adware

El volumen de adware sigue incrementando año con año. El adware constituye el 40 por ciento de las detecciones de amenazas para consumidores, con un incremento del 132 por ciento solo durante el año pasado. Es la amenaza que más detectamos actualmente. Sin embargo, igual que con el ransomware, existen menos familias activas. La mayor parte del trabajo que se está realizando es por parte de unos cuantos desarrolladores activos de adware para Windows, macOS y Android.

¿Qué está ocasionando esta baja en desarrolladores de adware? La industria de la tecnología ha implementado los bloqueadores de publicidad de una manera mucho más agresiva. Google, Mozilla y Microsoft han tomado medidas para introducir herramientas de bloqueo de publicidad más sofisticadas en sus navegadores. Otros plugins para bloquear publicidad se han vuelto más ubicuos. De esta manera, los creadores de adware que disponían de menos recursos y menos adaptabilidad terminaron por extinguirse mediante el darwinismo técnico.

Lo que esto significa es que si estos perpetradores querían seguir distribuyendo adware, tuvieron que ponerse las pilas para evitar ser bloqueados. Para lograrlo, tuvieron que redoblar esfuerzos y mejorar sus tácticas. Solo sobrevivieron los más fuertes.

Adware para Windows

Un buen ejemplo de esta tendencia más agresiva de adware es un programa de Windows llamado Smart Service. Smart Service se empaqueta con adware y programas potencialmente no deseados (PUP) que sirven como protección contra desinstalaciones. Utiliza dos métodos para obtener su objetivo.

En primer lugar, Smart Service se engancha a la función de CreateProcess de Windows para inspeccionar procesos nuevos antes de permitir su ejecución. Para evitar la eliminación del adware del sistema afectado, bloquea los programas de seguridad y evita que estos se ejecuten o incluso que se instalen. Hace esto a partir de sus certificados de seguridad y los nombres de sus procesos. El usuario ve un mensaje de error que indica "El recurso solicitado está actualmente en uso".

En segundo lugar, el programa protege a ciertos procesos para evitar su finalización y evita que el usuario elimine sus archivos críticos y claves de registro. El usuario ve un mensaje de error que indica "No es posible eliminar" al intentar realizar esta acción.

Smart Service incluye un componente de fraude publicitario que permite a los creadores de la amenaza obtener ganancias a partir de él. Los empaquetadores incluyen gustosamente este paquete, ya que evita que las víctimas sean capaces de eliminar el programa no deseado.

Gracias a esto, todos estos maleantes salen ganando.

Poder luchar contra esta infección es una batalla constante, ya que los creadores de Smart Service monitorean activamente los avances de la comunidad investigadora con el fin de desarrollar contramedidas en cuanto se implementen nuevas defensas. El escáner de malware en tiempo real de Malwarebytes es capaz de detectar y bloquear a Smart Service; sin embargo, es muy difícil eliminar esta infección una vez adquirida.

Adware para Android

En los últimos seis meses, ha habido muchos clickers y adware empaquetado que se han infiltrado a la tienda Google Play. Aquellos que se infiltran son agresivos y utilizan nuevas tácticas creativas para ofuscar su verdadero propósito.

En el otoño del 2017, se encontró una nueva variante de malware móvil en Google Play conocida como Android/Trojan.AsiaHitGroup. Este malware se instala bajo un nombre genérico de aplicación, Download Manager, el cual es diferente al nombre que proporciona Google Play. Una vez instalada, la aplicación crea un ícono de acceso directo, pero este se elimina rápidamente después de abrir la aplicación por primera vez.

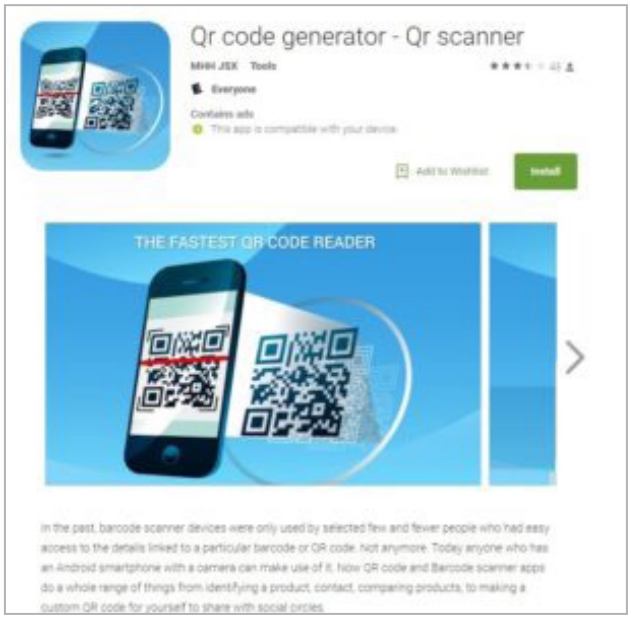

Figura 13. Trojan.AsiaHitGroup

Esta aplicación maliciosa identifica la ubicación del dispositivo móvil a través de un sitio web de geolocalización que utiliza la dirección IP del dispositivo. Si determina que su ubicación está dentro de un perímetro específico, descarga e instala un SMS troyano. Este SMS troyano se utiliza para propagar todavía más el malware. Además de esto, la aplicación maliciosa contiene adware oculto, el cual se ejecuta independientemente de la ubicación. Consideramos que el principal objetivo de este malware es ejecutar este adware para obtener ingresos a partir de él.

Este enfoque avanzado de ocultar el adware es una tendencia que se ha estado popularizando en el malware móvil. Este enfoque utiliza SDK de publicidad legítimos de los cuales obtiene una pequeña ganancia por cada anuncio publicitario mostrado. El malware ejecuta engañosamente estos anuncios publicitarios para obtener ganancias más rápidamente.

Adware para Mac

Para Mac, vimos una interesante técnica utilizada por el adware VSearch (o Pirrit). La gran mayoría del adware (y malware) para macOS utiliza los métodos de persistencia más populares y recomendados; es decir, los agentes/daemons de ejecución y los elementos de inicio de sesión. Estos son fáciles de implementar y son totalmente compatibles con Apple, pero también son de fácil detección.

Se detectaron algunas variantes de VSearch que utilizaban tecnología más antigua, probablemente con el fin de evitar ser detectadas. Específicamente, utilizaban el antiguo proceso cron, un programa de Unix diseñado para programar tareas recurrentes. Ya que Apple ha estado recomendando el uso de agentes/daemons de ejecución en lugar de las mucho más sencillas tareas cron desde hace tiempo, pocas personas se acuerdan de cron y no les interesa mucho investigar su estado actual. Ya que cron aún tiene un estado funcional en las últimas versiones de macOS, esto lo convierte en un buen objetivo para el adware o el malware que busca mantenerse vigente, pero, a la vez, pasar desapercibido.

```
$ sudo crontab -l
50 * * * * /Library/stateliness.hu/stateliness.hu cr
```

Figura 14. Adware VSearch

Botnets

El año pasado pudimos apreciar un declive continuo en la detección de malware en forma de botnets, un gran cambio respecto de lo que vimos en el 2016. Esto concuerda con la telemetría que recopilamos de nuestros clientes, tanto de empresas como de consumidores. Esta disminución probablemente se debe a un cambio de enfoque, el cual se ha alejado de la computadora de escritorio para concentrarse en los dispositivos del Internet de las cosas como ruteadores y dispositivos inteligentes. Los cibercriminales cambian frecuentemente de plataforma para sacar provecho de las oportunidades de infección más accesibles. Los dispositivos del Internet de las cosas son mucho más vulnerables a este tipo de ataques.

Los botnets son básicamente un grupo de malware poco inteligente que infecta numerosos sistemas. La parte poco inteligente, o el bot, está conformada por una aplicación ligera y a veces silenciosa que se ejecuta en el fondo del sistema de la víctima, esperando recibir instrucciones del atacante.

Los botnets se utilizan para lanzar ataques de denegación distribuida de servicio (Distributed Denial of Service, DDoS), los cuales distribuyen correos electrónicos maliciosos e instalan aun más malware. Sin embargo, dependiendo de la familia de bots, pueden ser capaces también de incorporar métodos más tradicionales de spyware, tales como keylogging y capturas de pantalla.

Las amenazas más significativas a las empresas cuando se trata de botnets son principalmente las familias de malware en forma de botnets que llevan a cabo operaciones más invasivas de robo de datos. Sin embargo, la infección de los puntos finales de una empresa con malware puede tener como resultado el uso de esos sistemas para un ataque de denegación distribuida de servicio (DDoS) en contra de alguien más, lo cual no solo afecta a otros usuarios legítimos, sino que también agota los recursos de la red de origen infectada.

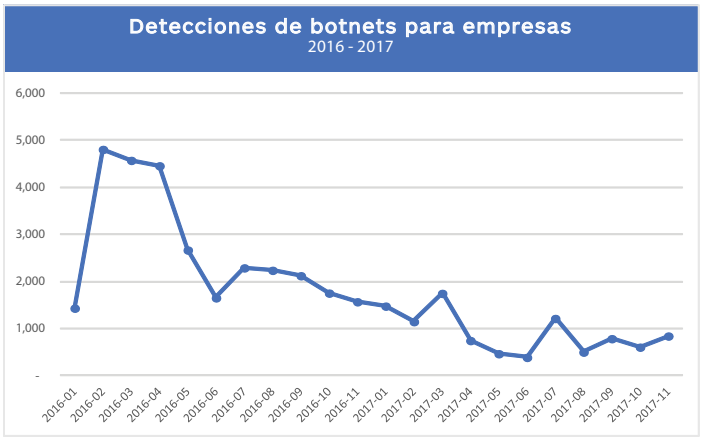

Figura 15. Detecciones de botnets para empresas en 2016-2017

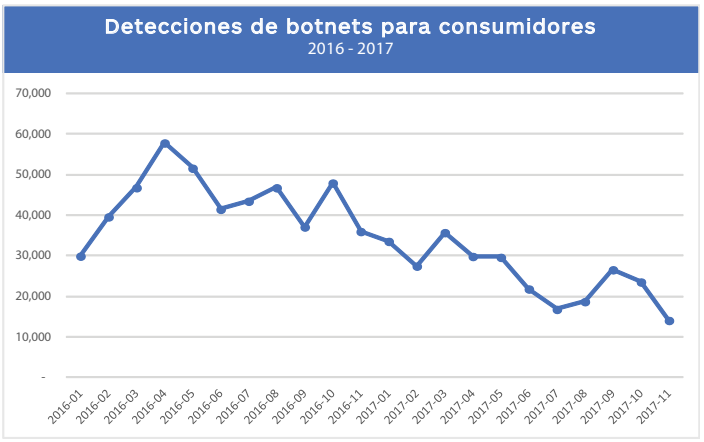

Figura 16. Detecciones de botnets para consumidores en 2016-2017

Mineros de criptomonedas

Las criptomonedas: la última moda. En el 2017, los mineros de criptomonedas experimentaron una rápida evolución, así como una mayor distribución a través de diversos medios.

Debido al aumento en la popularidad y el valor de mercado de las criptomonedas, hemos visto un incremento no solo en la cantidad de ataques maliciosos a través de criptomineros, sino también en la cantidad de métodos utilizados para llevar a cabo estos ataques. Definimos el uso malicioso de criptomineros para englobar cualquier método que utiliza los recursos del sistema de una víctima desprevenida para minar criptomonedas. A esto le llamamos minería de tipo drive-by.

La moneda más popular para la minería de tipo drive-by en el 2017 fue Monero, lo cual se debe a que:

- Procesa transacciones a velocidades más altas, incluso al procesar cantidades pequeñas.
- La anonimidad que incorpora automáticamente la cadena de bloques de Monero.
- El algoritmo de minería no favorece a las fichas especializadas.

Minería de tipo drive-by

En el otoño del 2017, una nueva empresa llamada Coinhive revivió un antiguo concepto fallido de minería basada en el navegador a través de JavaScript. Para capitalizar la popularidad de las criptomonedas, Coinhive les proporcionó una API sencilla a los administradores web para que la adoptaran en sus sitios web y con la cual convertían a cada visitante en un minero de la moneda digital Monero.

Desafortunadamente, esta tecnología sufrió inmediatamente de abusos por parte de administradores web que la ejecutaban de manera oculta, así explotando los CPU de sus visitantes para su propia ganancia. Con el tiempo, los criminales también tomaron nota y empezaron a vulnerar sitios con código de criptominería.

Durante este periodo, Malwarebytes bloqueó en promedio 8 millones de intentos de minería de tipo drive-by de sitios web y visitantes de todo el mundo. Coinhive es ahora uno de los muchos imitadores nuevos que presumen haber sido capaces de ejecutar su código sin ser descubiertos por los bloqueadores de publicidad y los antivirus.

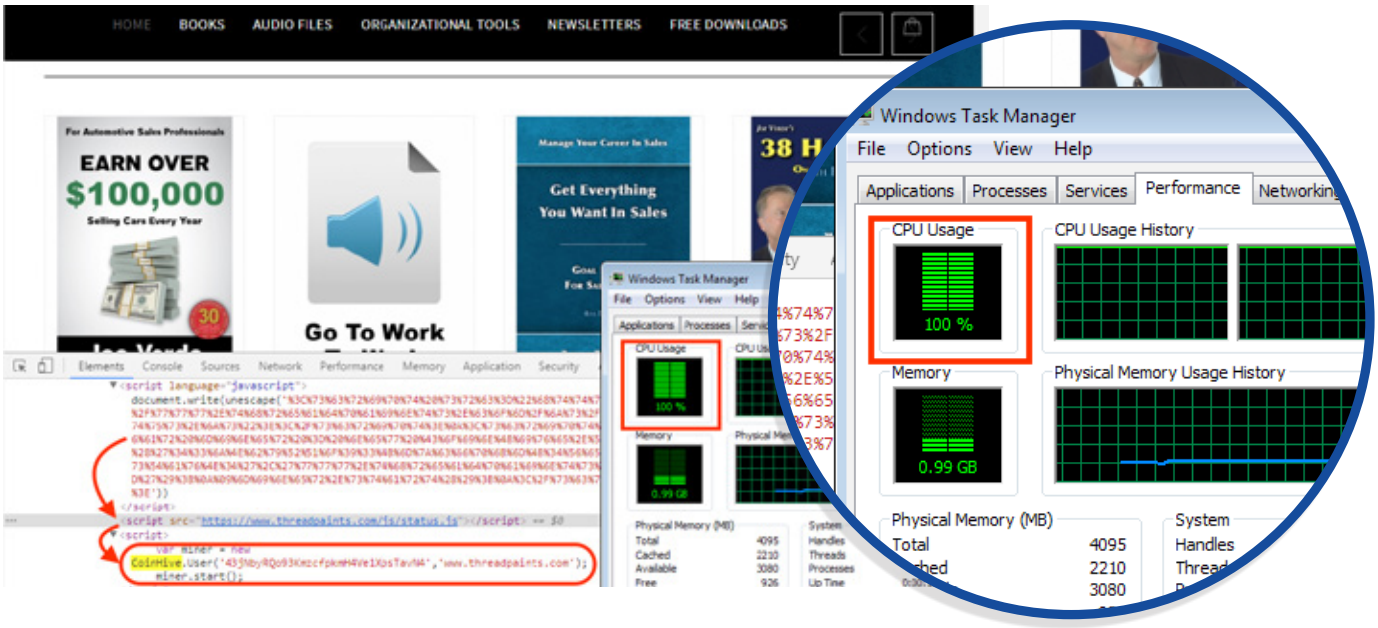

Figura 17. Un ejemplo de abuso de la minería a partir de script

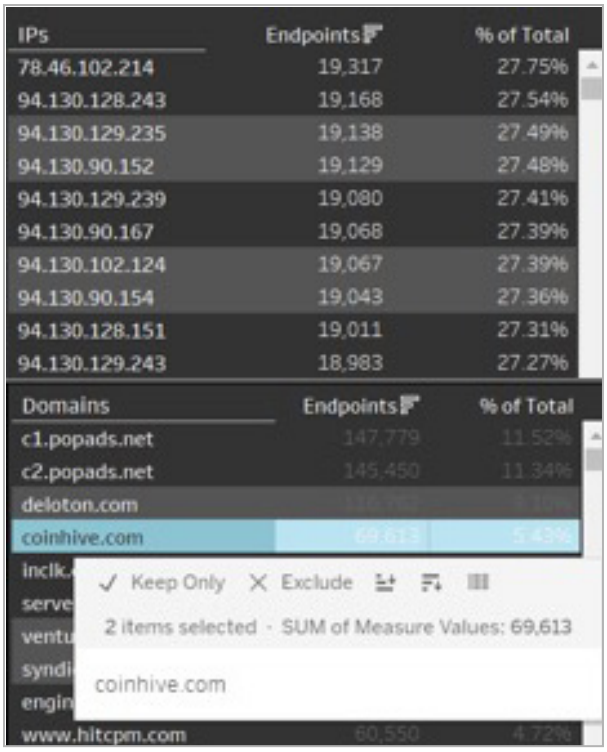

Figura 18. Cantidad de bloqueos de coinhive.com que realizó Malwarebytes en cinco días

Las anteriores estadísticas muestran cinco días de bloqueos de coinhive.com. La actividad de solo este dominio representa más del 5 por ciento del total de nuestros dominios bloqueados y equivale al 27 por ciento de las direcciones IP bloqueadas. Si a esto le sumamos dominios relacionados como coin-hive.com, authedmine.com y cnhv.co, obtenemos 100 millones de bloqueos mensuales.

Métodos de los ataques de minería de tipo drive-by

Wrappers de programas potencialmente no deseados (PUP)

Se ha descubierto que una gran variedad de paquetes y wrappers de programas potencialmente no deseados (PUP) instalan mineros, y parece que están sustituyendo al adware como forma de pago. IStartSurf, un programa potencialmente no deseado (PUP) que se ha hecho popular por sus hijackers para navegadores, ha empezado a incluir mineros en sus instalaciones silenciosas. Es el mismo caso con InstallMonster, un paquete de uso más general.

Exploit kits y publicidad maliciosa

La carga del exploit kit RIG empezó a incluir criptomineros en el 2017. Es el mismo caso con Terror EK, aunque en menor grado. Profundizaremos en este tema en la sección sobre exploit kits.

Incluso el exploit EternalBlue, que fue lanzado a la fama gracias a WannaCry, fue utilizado para distribuir un minero detectado como Trojan.BitcoinMiner que utilizaba Windows Management Instrumentation para ocasionar una infección persistente sin archivos.

Además de esto, los perpetradores mezclaron las técnicas de publicidad maliciosa con las de fraude publicitario para hacer al proceso de minería más persistente, incluso después de que los usuarios cerraran la ventana del navegador. Lo que podría haber sido un modelo empresarial que ofreciera una alternativa a la publicidad en línea se convirtió en un gran yermo de oportunidades desaprovechadas.

Spam malicioso

Los distribuidores de spam se han divertido a lo grande con las criptomonedas. No solo han utilizado la red de pruebas de Ethereum para llevar a cabo una campaña de spam, sino que también han aprovechado las fluctuaciones en el valor de Bitcoin para sus campañas de suplantación de identidad, todo esto mientras distribuyen criptomineros o instaladores para estos mineros como spam malicioso.

Figura 19. Spam malicioso de Bitcoin

Ingeniería social

La ingeniería social es otro vector de ataque que se utiliza en la minería de tipo drive-by. La llamada campaña Roboto utilizó la ingeniería social para que los usuarios pensaran que debían instalar una nueva fuente cuando, en realidad, les entregaba un criptominero.

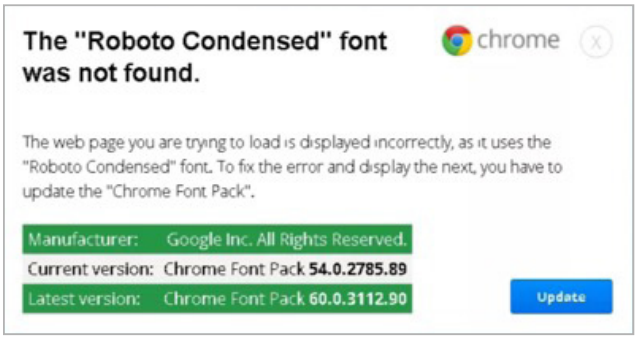

Figura 20. Instalación de un minero mediante la ingeniería social

También hemos visto algunos mineros (como Cloud Packager) que se ofrecieron como versiones piratas de programas populares.

Los bancarios van por el robo de carteras de Bitcoin

Los troyanos bancarios también han expandido su portafolio para incluir el robo de criptomonedas directamente de las carteras virtuales de las personas. Coinbase es una cartera virtual que realiza intercambios de diversas monedas, entre ellas Bitcoin. Se detectó una variante de Trickbot que incorpora el intercambio mediante Coinbase para robar credenciales de los sitios que monitorea. Se han detectado otros troyanos que roban criptomonedas sobre la marcha, entre ellos CryptoShuffler, un troyano que monitorea el portapapeles, el área de almacenamiento temporal para operaciones de cortar/pegar. En cuanto encuentra la dirección de la cartera virtual en el portapapeles, la sustituye por la de la amenaza. Sigilosos. Engañosos. Falsos.

Técnicas de distribución

En esta sección que sigue, profundizaremos en las principales técnicas de distribución que utilizaron los criminales para distribuir sus cargas en el 2017. Desde el uso creativo de exploits filtrados de la NSA hasta los archivos CCleaner troyanizados y el ransomware diseñado específicamente para Corea del Sur, los perpetradores no perdieron tiempo en el 2017 y crearon diversas formas innovadoras para evadir la detección y mantener a los investigadores en alerta.

Quizás la inspiración creativa para estos hijinks surge del hecho de que los exploit kits y los ataques de botnets tuvieron un declive, lo cual permitió el regreso de los métodos tradicionales como la publicidad maliciosa y las estafas de soporte técnico.

Exploit SMB/EternalBlue

Uno de los ataques más poderosos y sorprendentes del 2017 fue posible gracias a un exploit filtrado de la NSA conocido como EternalBlue. Tanto el ransomware WannaCry como el NotPetya utilizaron este exploit para sus ataques a mediados del año.

El exploit

EternalBlue (CVE-2017-0144) explota una vulnerabilidad que se encuentra en una gran variedad de sistemas operativos de Windows, específicamente un bug de manejo del Server Message Block (SMB). Los atacantes pueden utilizar este exploit para ejecutar un código en el sistema objetivo al enviarle unos paquetes de red especialmente diseñados con una versión vulnerable de SMB versión 1 instalada.

Figura 21. MS17-010, boletín de seguridad que anuncia un parche para EternalBlue

Esta vulnerabilidad se reportó a Microsoft meses antes de que ocurriera el primer ataque público en mayo; Microsoft emitió un boletín de emergencia (MS17-010) el 14 de marzo del 2017. Estos parches se implementaron en cada versión compatible de Windows. A pesar de haber contado con dos meses de ventaja, cientos de miles de sistemas seguían sin estar actualizados y, por lo tanto, aún eran vulnerables al exploit EternalBlue que se detectó como activo en pareja con WannaCry.

Amenaza activa

WannaCry

WannaCry se clasifica como ransomware con funcionalidad de gusano, también llamado ransomworm. En el brote de mayo, utilizó a EternalBlue para infectar sistemas con conexión a Internet en todo el mundo. Después de la infección, WannaCry utilizaría a EternalBlue, en conjunto con otros exploits filtrados de la NSA, para recorrer rápidamente la red conectada al sistema de la víctima, encriptar sus archivos y exigir un pago.

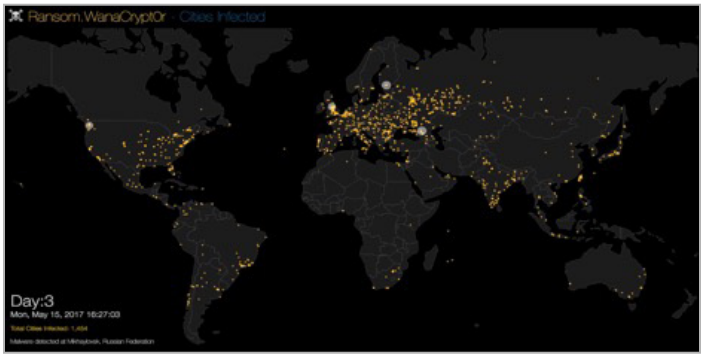

Figura 22. Mapa de la infección WannaCry

La versión inicial de WannaCry incluía un monitor de tráfico de red que servía como detonador. El malware podía comunicarse con un dominio codificado sin esperar ninguna respuesta. Sin embargo, si recibía una respuesta, el malware no encriptaba ningún archivo. Cuando un investigador de seguridad registró este dominio, la versión original de WannaCry se volvió benigna.

NotPetya

La llegada de NotPetya en junio, solo un mes después de WannaCry, podría parecer un mal chiste, solo que nadie se estaba riendo.

NotPetya parecía estar fuertemente influenciado por Petya y WannaCry. De manera similar a otras cepas que le precedieron, NotPetya fue capaz de esparcirse explotando dos vulnerabilidades de Server Message Block (SMB): EternalBlue (CVE-2017-0144) y EternalRomance (CVE-2017-0145). También atacó las estructuras de bajo nivel de los sistemas afectados encriptando sus tablas maestras de archivos (MFT) y sus registros de arranque maestro (MBR).

A diferencia de otras cepas anteriores, NotPetya contaba con recursos adicionales que favorecían su propagación, tales como el robo de credenciales y la usurpación de la personalidad mediante archivos compartidos en la red y WMI (Windows Management Instrumentation) o PSEXEC.

La evidencia recopilada por múltiples investigadores de seguridad y las autoridades señalan a Intellect Service, una pequeña compañía de software de Ucrania, como "paciente cero" de este brote o el lugar donde se originó este malware.

Adicionalmente, nuestros amigos de ESET revelaron que los perpetradores habían contaminado ilegalmente al menos tres archivos de actualización del popular programa de contabilidad de impuestos de la firma, M.E.Doc, incorporando en él un backdoor.

La evidencia más reciente señala que NotPetya no es en realidad ransomware, sino un malware destructivo. ¿Por qué?

El ransomware fue esencialmente ineficaz al cobrar su rescate. Se les aconsejó a los usuarios afectados por NotPetya que no se molestaran en pagar, ya que el servicio de correo electrónico que alojaba la dirección en la cual se les indicaba a las víctimas que enviaran sus pagos estaba cerrado. Por lo tanto, la recuperación de archivos a través de un pago ya no era posible. Otros investigadores de seguridad aconsejaron el uso de una vacuna para recuperar el sistema afectado. Finalmente, se les aconsejó a todos los usuarios de M.E.Doc que cambiaran todas las contraseñas de sus proxies y cuentas de correo electrónico.

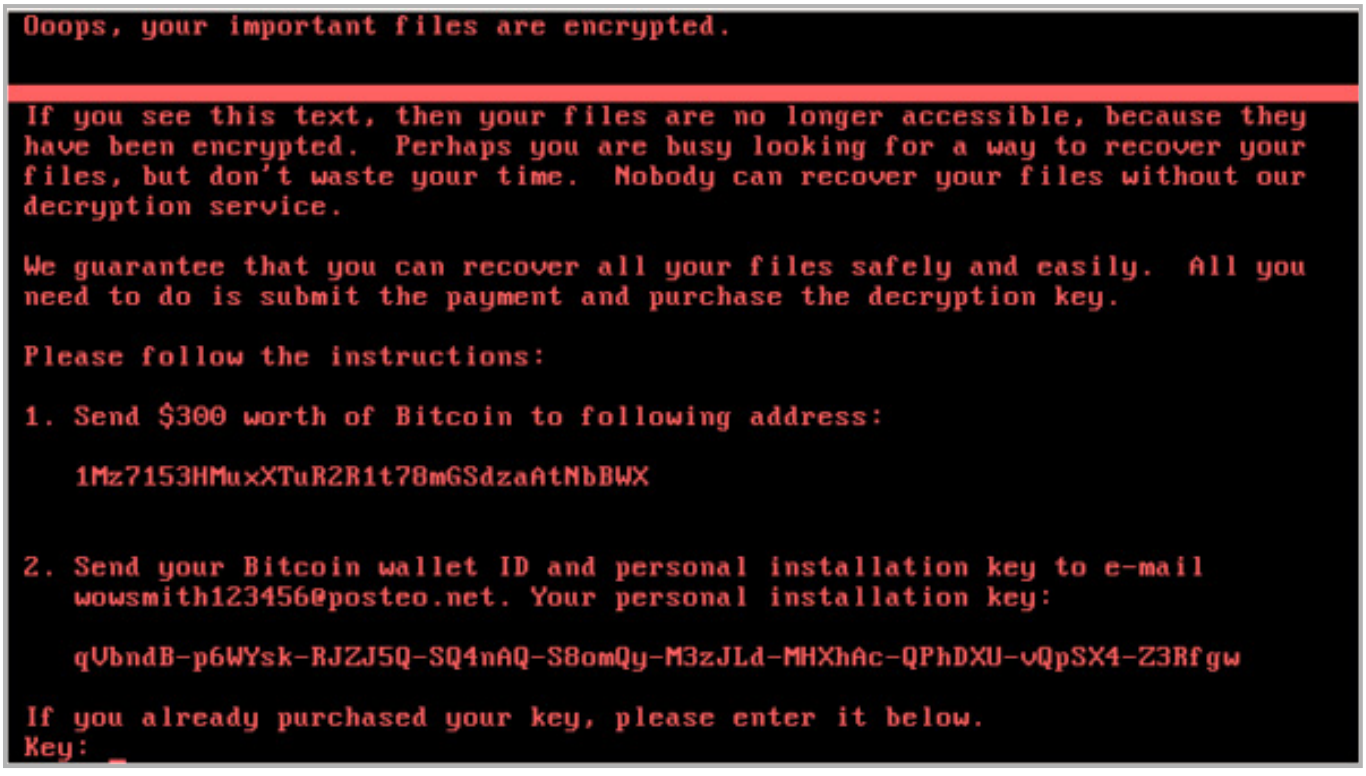

Figura 23. Nota de rescate de NotPetya

Otras

Mientras que WannaCry y NotPetya llegaron a los titulares y provocaron confusión en la comunidad de la seguridad, existían entonces, y aún existen, otras formas de malware que han utilizado EternalBlue y otros exploits filtrados para su beneficio. Por ejemplo:

- Adylkuzz es una familia de mineros de Bitcoin que no solo utilizó el exploit EternalBlue para infectar sistemas semanas antes de que lo hiciera WannaCry, sino que también instalaba parches en los sistemas de sus víctimas para que no fuera posible instalar ningún otro malware.
- CoinMiner es otra familia de mineros que utiliza EternalBlue para infiltrarse a las redes; sin embargo, en lugar de instalar un malware ejecutable, se ejecuta en la memoria activa del sistema. Esta práctica se conoce como infección sin archivos y resultó ser un método efectivo para evitar la detección de las soluciones de seguridad en el pasado. CoinMiner tiene la gran distinción de ser uno de los primeros mineros sin archivos de Bitcoin.
- Retefe (no Covfefe) es una familia de malware en forma de troyanos bancarios con un enfoque geográfico en Austria, Suecia, Suiza y Japón. Adoptó el exploit EternalBlue en nuevas variantes de malware que recorrieron las redes después de una infección inicial de código malicioso incrustado en un documento de Word y adjunto en un correo electrónico no deseado (spam).

Ataques a la cadena de suministro

Como si mantener segura la cadena de suministro física de una empresa no fuera lo suficientemente desafiante y complicado, la amenaza de ser blanco de los ataques de ciberseguridad solo lo hace más difícil. Que los cibercriminales aprovechan la parte más vulnerable de la cadena de suministro de una organización no es algo nuevo; sin embargo, esta práctica se volvió más popular en el último trimestre del 2017 en comparación con los trimestres anteriores del mismo año.

A continuación, resumimos algunos de los principales ataques a la cadena de suministro en el 2017, enfocándonos en cómo iniciaron y qué motivaciones tenían.

Archivo CCleaner troyanizado

CCleaner ha existido por más de una década. Con más de 2 mil millones de descargas, ha sido una de las principales herramientas gratuitas de limpieza y mantenimiento para la PC.

A mediados de septiembre, se descubrió que la versión 5.33.6162 de CCleaner y la versión 1.07.3191 de CCleaner Cloud contenían una carga de backdoor que le permitía perfilar agresivamente a los equipos en los cuales se instalaba, enviar la información a su servidor de comando y control (C&C) y, si se cumplían ciertos requisitos predefinidos, instalar una carga secundaria.

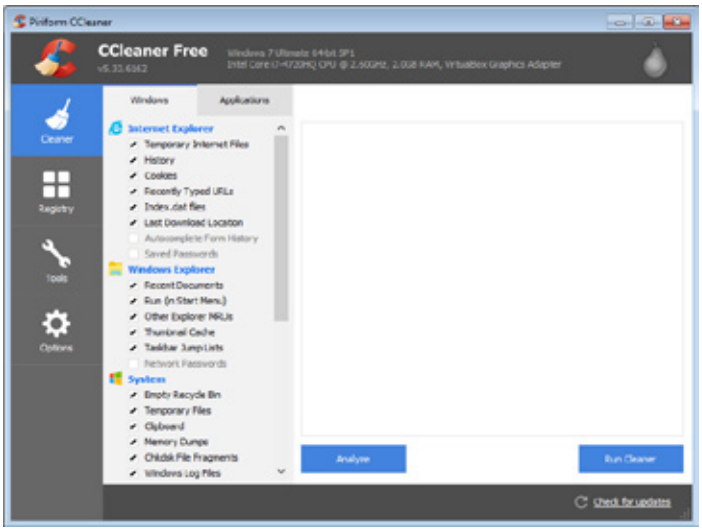

Figura 24. La versión afectada de CCleaner para PC

Los perpetradores de este ataque demostraron claramente una planeación meticulosa y un alto nivel de sofisticación, desde la modificación ilegal del archivo de actualización de CCleaner durante su proceso de compilación hasta el resultado final que buscaban, el cual era infiltrarse eventualmente en ciertas organizaciones de alto perfil, entre ellas Samsung, Sony y Microsoft. Esto sugiere que su objetivo era obtener propiedad intelectual invaluable.

Al momento de la elaboración de este informe, las investigaciones siguen en curso y los perpetradores aún no han sido identificados y muy posiblemente están fugitivos.

Archivo Elmedia Player troyanizado

El malware Proton para Mac OSX.utilizó los ataques a la cadena de suministro para infectar dos veces a los usuarios en el 2017. La primera ocasión fue en mayo, cuando un servidor mirror que distribuye su popular software de extracción de DVD, Handbrake, empezó a distribuir una copia maliciosa de esta aplicación. Más tarde, en octubre, el sitio web de Eltima Software se vio comprometido y dos de sus aplicaciones, Elmedia Player y Folx, fueron víctimas de modificaciones maliciosas.

El programa Elmedia Player, que contaba con un diseño muy característico, parecía ser completamente legítimo, incluso al abrirlo. Esto debido a que el software troyanizado era un wrapper que contenía la aplicación legítima. Así que, una vez abierto, el reproductor se ejecutaba en primer plano y parecía funcionar de manera normal para los usuarios desprevenidos, mientras que el código malicioso se ejecutaba en segundo plano.

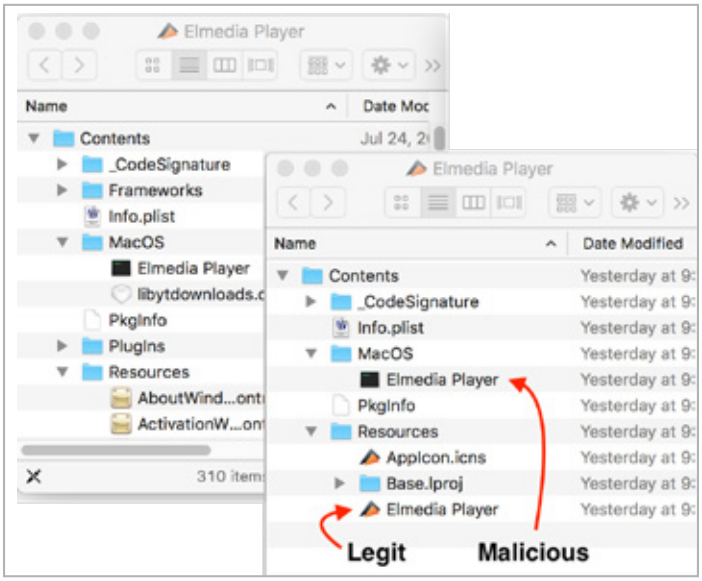

Figura 25. Una comparación: la aplicación legítima Elmedia Player y el wrapper malicioso

La variante Proton que corrompió a Elmedia Player fue capaz de extraer sigilosamente los llaveros del sistema, las bóvedas de 1Password que contenían contraseñas de usuarios y demás información delicada, así como las credenciales de inicio de sesión almacenadas de quienes utilizaban la función de recordar la contraseña del navegador. También fue tras las carteras de criptomonedas, lo cual sugiere que puede robar monedas digitales como Bitcoin y otros datos que los criminales pueden utilizar para acceder a recursos potencialmente delicados del usuario afectado.

Ya que el objetivo principal del malware Proton es robar credenciales de cualquier tipo, es probable que estos ataques se sigan llevando a cabo a través de cuentas comprometidas. Es extremadamente fácil que la gente caiga en este tipo de ataques, incluso los expertos.

Ataques geoespecíficos

Los ataques geoespecíficos, aquellos en los cuales los grupos de hackers seleccionan un blanco y hacen todo lo posible por deteriorar, desestabilizar o comprometer sus datos, siguen siendo un método popular de desmantelar agresivamente a un oponente.

En los últimos meses, hemos visto la ejecución metódica y clínica de muchas amenazas que han tenido resultados caóticos para gobiernos, organizaciones, periodistas y hasta consumidores tratando de afinar sus PC.

Magniber (Corea del Sur)

En octubre, el ransomware Magniber se convirtió en la carga predilecta del antes latente exploit kit Magnitude, que atacó solamente a sistemas que utilizaban los paquetes del idioma coreano, pero también tomaba en cuenta la dirección IP y la geolocalización para asegurarse de que su distribución estuviera lo más confinada posible dentro de la región de Corea del Sur.

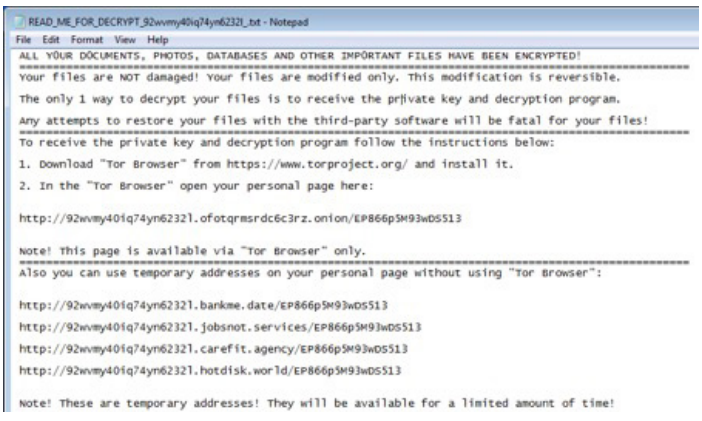

Figura 26. Ransomware Magniber

Este ransomware, cuya distribución fue a través de sitios de publicidad maliciosa propiedad de los hackers responsables del ataque, trató de encriptar una larga lista de archivos, entre ellos documentos, código fuente, etc. Si el archivo determinaba que la víctima se encontraba fuera de Corea del Sur, se autoeliminaba sin causar ningún problema, lo cual es interesante, ya que se podría suponer que los hackers aprovecharían cualquier oportunidad de obtener ganancias extras, pero, al parecer, estos no estaban interesados. Este ataque se enfocaba en Corea del Sur con una precisión extraordinaria.

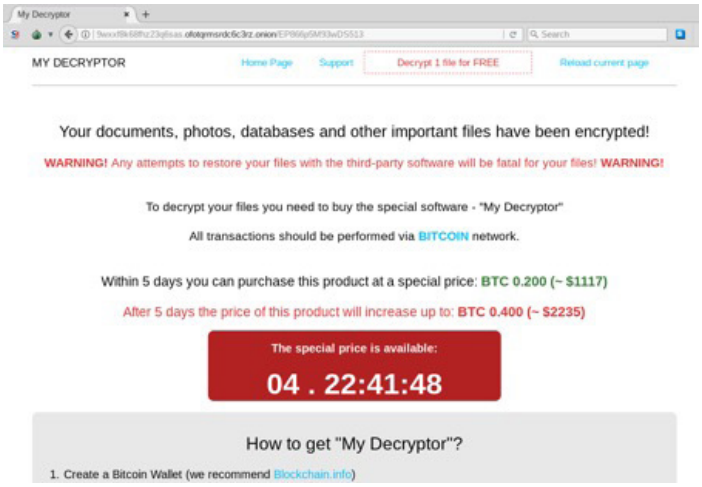

Figura 27. Desencriptador para Magniber

Magnitude tuvo una distribución centrada en Asia en los últimos años, después de haber tenido un enfoque mundial de infección. Pero el notable hecho de que haya regresado a la vida con un ataque tan focalizado nos hace preguntarnos quién exactamente tenía una enemistad contra Corea del Sur de tal nivel que lo llevaría a resucitar un exploit kit latente.

Finfisher (Medio Oriente)

En otra parte del mundo, también en octubre del 2017, se detectó que un grupo de hackers conocidos por su espionaje, BlackOasis, tenía como blanco de ataque a organizaciones e individuos vinculados a la política en el Medio Oriente, entre ellos corresponsales de noticias, activistas y hasta miembros de las Naciones Unidas.

BlackOasis atraía a sus víctimas hacia una trampa de exploit con un correo electrónico señuelo que parecía ser una serie de documentos políticos de oficina. Los documentos incluían objetos de ActiveX incrustados, lo cual desencadenaba un ataque de exploit mediante Flash y ponía en marcha la trampa.

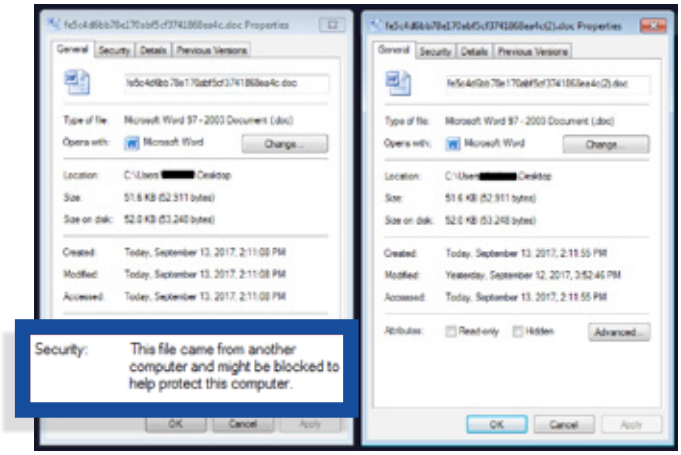

Figura 28. Documento de Microsoft Word infectado

La carga final del ataque era el malware FinSpy, el cual se vende normalmente a las autoridades o las naciones para fines de vigilancia legal. Se dice que estos archivos fueron creados por el llamado grupo Gamma, aunque no se sabe si BlackOasis ha estado comprando spyware y exploits de manera masiva a Gamma o si los ha obtenido de una gran variedad de fuentes distintas.

Gran parte del objetivo de estos atacantes parece estar relacionado con el petróleo, ya que todas las regiones afectadas estaban conectadas a Arabia Saudita, quien también compra presuntamente spyware, lo cual complica aún más las cosas.

Estafas de soporte técnico en francés

Las estafas multilingües de soporte técnico han existido desde hace mucho tiempo y los estafadores se han diversificado para abarcar el español, alemán, japonés y más idiomas en busca de generar ganancias. En el 2017, pudimos ver una campaña enfocada hacia los francoparlantes, con operaciones basadas en Quebec y Mauricio.

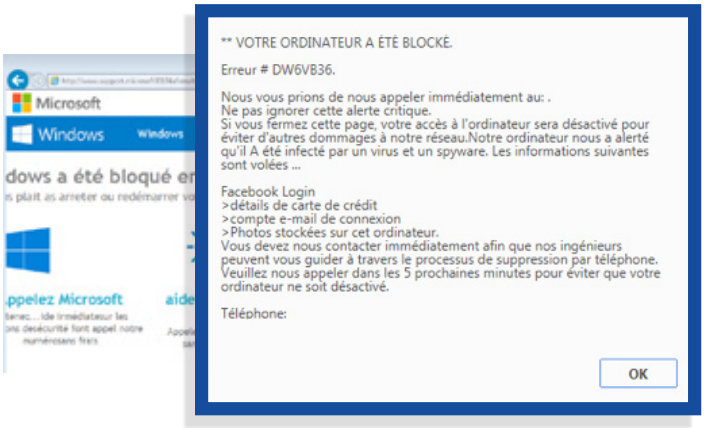

Figura 29. Una estafa de soporte técnico en francés

Como con las estafas actuales más populares, las tácticas que se utilizaron para dirigir a las víctimas hacia las ventanas de pago involucraban publicidad maliciosa y páginas falsas personalizadas que los llevaban hacia los operadores, quienes hablaban francés fluido (aunque con un ligero acento). Las estafas de este tipo a veces dan pistas sobre su ubicación, como podría ser el nombre de una ciudad en su URL, pero en todos los demás aspectos, han hecho lo necesario para mantenerse anónimas. Son comunes los registros web chinos, números gratuitos difíciles de rastrear comprados en masa e información de registro oculta detrás de proxies.

BadRabbit y NotPetya (Ucrania)

Los sistemas de transporte, entre ellos aeropuertos y vías férreas subterráneas, se vieron severamente afectados por un brote de ransomware BadRabbit en Ucrania en octubre, el cual exigía €220 para restaurar el acceso a los sistemas comprometidos. Distribuido a través de los llamados ataques de aguadero (en los cuales los sitios frecuentados por una organización resultan comprometidos y se utilizan para distribuir malware), los instaladores falsos de Flash instalaban el ransomware al activarse.

Este enfoque relativamente sencillo tenía como resultado un registro de arranque maestro encriptado y una solicitud de rescate una vez reiniciado. A partir de ahí, BadRabbit se diseminaría a través de redes y ocasionaría más problemas a los administradores al intentar acceder, hasta por fuerza bruta, a cualquier recurso administrativo con el cual se llegara a topar.

BadRabbit tenía una gran similitud con NotPetya, llamado así por estar diseñado para parecerse a un malware conocido como Petya.

NotPetya obtuvo su renombre por los estragos que ocasionó en Ucrania en junio, cuando afectó a grandes empresas de envíos y firmas energéticas; incluso aseguró haber contribuido a la caída de una red eléctrica. Algunos analistas consideran que uno o ambos ataques se implementaron desde Rusia, lo cual Rusia niega fervientemente.

El potencial para ataques focalizados contra una región, o contra individuos trabajando en recursos importantes o inteligencia vinculados a esa región, es enorme y constituye una fuente constante de explotación por parte de hackers, naciones y grupos criminales profesionales.

Exploit kits

Ataques de tipo drive-by

El panorama de los ataques de tipo drive-by ha cambiado mucho en los últimos años. En el 2017, se vio un retroceso en la actividad de exploit kits; sin embargo, surgieron nuevos esquemas con el aumento general de ataques basados en la ingeniería social. Existen muchas razones para estos cambios, pero quizás el principal factor está vinculado con la cuota de mercado de los navegadores y el desarrollo (o falta de desarrollo) de los exploits para la web.

Continúa la caída de los exploit kits

Los exploit kits perdieron su atractivo desde hace tiempo. Solo unos cuantos siguen activos en el 2017 y se utilizan en cadenas de publicidad maliciosa. Aprovechar las vulnerabilidades de los tradicionales Internet Explorer y Flash ya no es una manera eficiente de infectar a los usuarios a escala masiva.

RIG EK sigue siendo el exploit kit más visible y estable que hemos detectado en todo el año. Después de una operación de desmantelamiento contra su infraestructura de dominio sombreado, sus distribuidores no han intentado volver a recurrir a cuentas host hackeadas y subdominios para evadir las listas negras. Es uno de los pocos (o tal vez el único) en utilizar URI de IP literal, lo cual lo hace más fácil de detectar y bloquear.

Protocol	Host	URL	Body	Content-Type
HTTP	free.joshualanglais.com	/?q=wXbQMvXcJwDQCYbGMvrESLtANknQA0KK2Ir2_dqyEo...	118,619	text/html;charset=UTF-8
HTTP	free.joshualanglais.com	/?yus=souls.87od69.406e1l6n2&oq=vQ9acsfuBQbwrliUKC...	16,433	application/x-shockwave-flash
HTTP	free.joshualanglais.com	/?ct=mart&fix=mart.128ub69.406f4a1f3&q=wXrQMvXcJw...	409,502	application/x-msdownload
Domain shadowing to IP literals				
HTTP	81.177.140.59	/?q=z37QMvXcJwDQDoTBMvrESLtEMU_OGUKK2OH_783VC...	32,962	text/html;charset=UTF-8
HTTP	81.177.140.59	/?yus=sound.89sc65.406y2q6s3&ct=sound&biw=sound.1...	14,854	application/x-shockwave-flash
HTTP	81.177.140.59	/?biw=april.106al62.406u2n0h2&q=wH_QMvXcJwDPFYbG...	288,768	application/x-msdownload

Figura 30. URI de IP literal

Quizás debido a su lugar prominente entre los exploit kits, RIG ha estado distribuyendo una gran variedad de cargas, entre las cuales está el ransomware, el cual sorprendentemente no es la carga más popular que los exploit kits han estado distribuyendo a lo largo del año (esa sería la de los criptomineros).

Un exploit kit que ha tenido bastante actividad es Terror EK. A pesar de que la escala de distribución es mucho más limitada que la de RIG, sus operadores se han dedicado a editar constantemente su código y probar ciertas características, tales como SSL.

EKFiddle v.0.5.3 (Fiddler)

File Edit Rules Tools View Help Links

QuickSave VPN Import SAZ/PCAP View/Edit Regexes Run Regexes Clear Markings Advanced UI on/off WinConfig Replay

Server IP	Protocol	Host	URL	Body	Comments
188.226.179.53	HTTPS	yakset.accountant	/spex.php?[redacted]	413	Terror_EK (Decoy Page)
188.226.180.230	HTTPS	dimplethan.stream	/serve.mfaif.popads.net/picture.gif?dongdong=4934311698	114,990	Terror_EK (IE exploits)
188.226.180.230	HTTPS	dimplethan.stream	/serve.mfaif.popads.net/serve.ebbnhf.popads.net/tihv.doc	4,614	Terror_EK (Flash calls)
188.226.180.230	HTTPS	dimplethan.stream	/serve.mfaif.popads.net/serve.ebbnhf.popads.net/ipha.jng	1	Terror_EK (empty Flash)
188.226.180.230	HTTPS	dimplethan.stream	/serve.mfaif.popads.net/serve.ebbnhf.popads.net/oxey.jng	44,392	Terror_EK (Flash Exploit)
188.226.180.230	HTTPS	dimplethan.stream	/serve.mfaif.popads.net/serve.ebbnhf.popads.net/bzti.jng	18,997	Terror_EK (Flash Exploit)
188.226.180.230	HTTPS	dimplethan.stream	/serve.mfaif.popads.net/vqzn-makei.gif	120,006	Terror_EK (Malware Payload)

Figura 31. Terror EK mediante SSL

Fraude publicitario y el poderoso Kovter

El fraude publicitario sigue siendo un gran problema para los publicistas debido a que gran parte de los gastos de las empresas se desperdician gracias a los botnets que fingen ser usuarios reales. El equipo detrás de Kovter tiene fama por involucrarse en este negocio lucrativo haciendo uso tanto de campañas de publicidad maliciosa de alto perfil como de malware sin archivos que evaden la detección.

Un ejemplo de estas campañas se implementó en la red de publicidad de Yahoo! y engañó a los usuarios para que descargaran un parche falso para el navegador Firefox. El archivo descargado era en realidad un JavaScript, el cual Kovter extraía y hacía más persistente utilizando el registro de Windows, casi sin dejar rastro.

El grupo Kovter ha evolucionado con el tiempo y tiene conocimiento pleno de cuáles son los métodos de distribución más efectivos. Mientras que alguna vez utilizó exploit kits impulsados por la publicidad maliciosa, ha desarrollado sus propios trucos de ingeniería social respaldados por múltiples técnicas de evasión para infectar a millones y mantenerse fuera del radar.

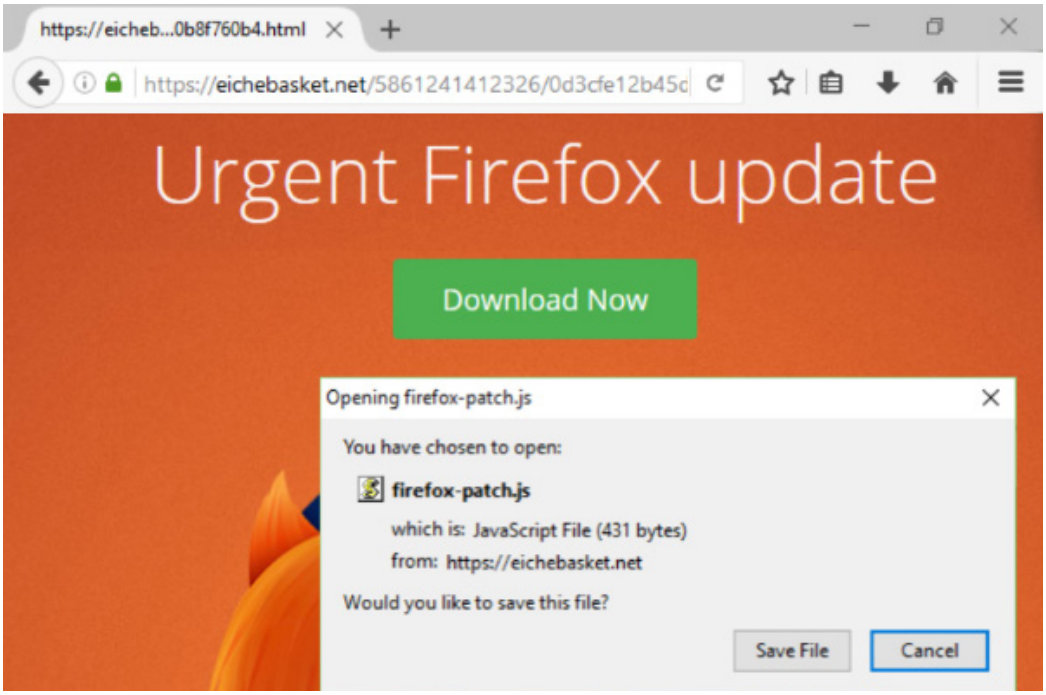

Figura 32. Actualización falsa de Firefox

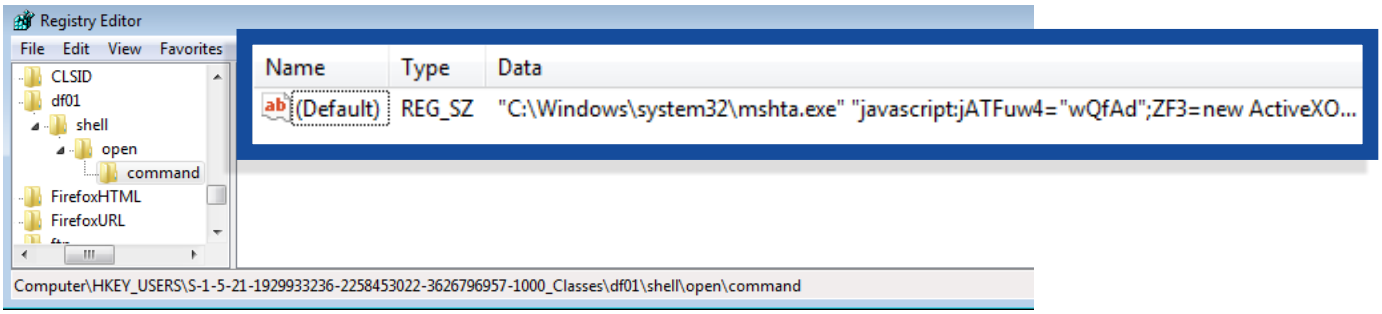

Figura 33. Registro Kovter

Ataques de ingeniería social

Quizás relacionado con la baja en la actividad de los exploit kits, también ha disminuido la cantidad de sitios web hackeados que redirigen a ataques de descargas de tipo drive-by. Sin embargo, todavía hay muchas formas en que los criminales aprovechan los sitios comprometidos, y una de ellas se apoya en la ingeniería social.

Esta campaña de larga duración, a la cual llamamos EITest en el 2014, no solo está al tanto de la geolocalización, sino que también se basa en el navegador, implementando actualizaciones falsas de fuente o estafas de soporte técnico.

Alterando de manera inteligente el texto de la página y sustituyéndolo con caracteres falsos, los maleantes dan a los visitantes la impresión de que les falta una fuente para poder ver correctamente el contenido del sitio. Por supuesto, el instalador de fuentes no es lo que dice ser y, en muchos casos, resulta ser ransomware, como Spora.

Vale la pena mencionar que los sitios web hackeados distribuyen con frecuencia más de una sola carga y, al instalar un bloqueador de navegador, podrían fácilmente utilizarlo para alojar malware, plantillas de suplantación de identidad y spam farmacéutico.

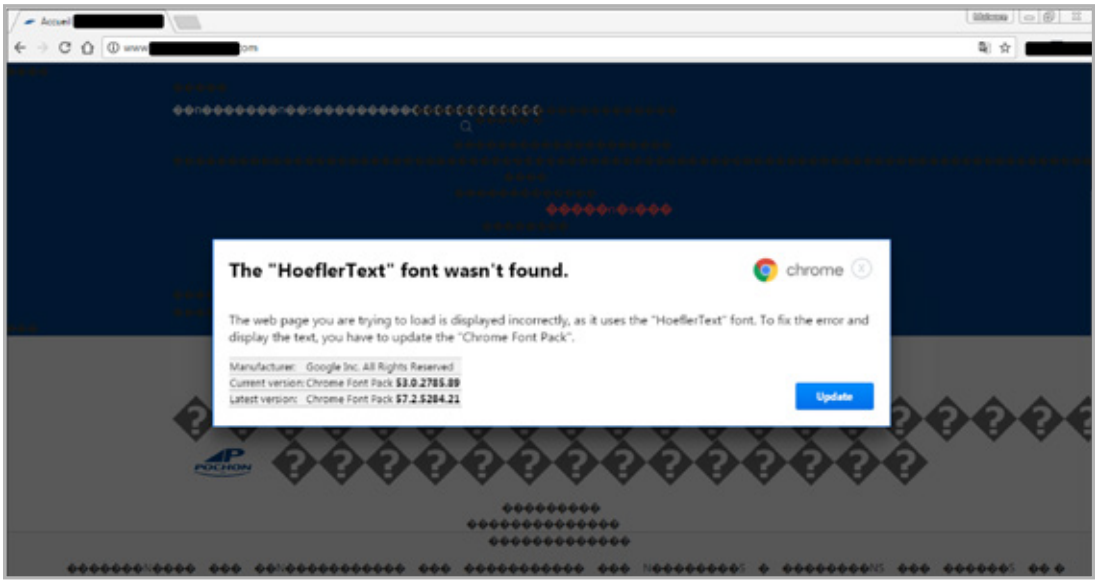

Figura 34. Mensaje de "fuente faltante" de EITest

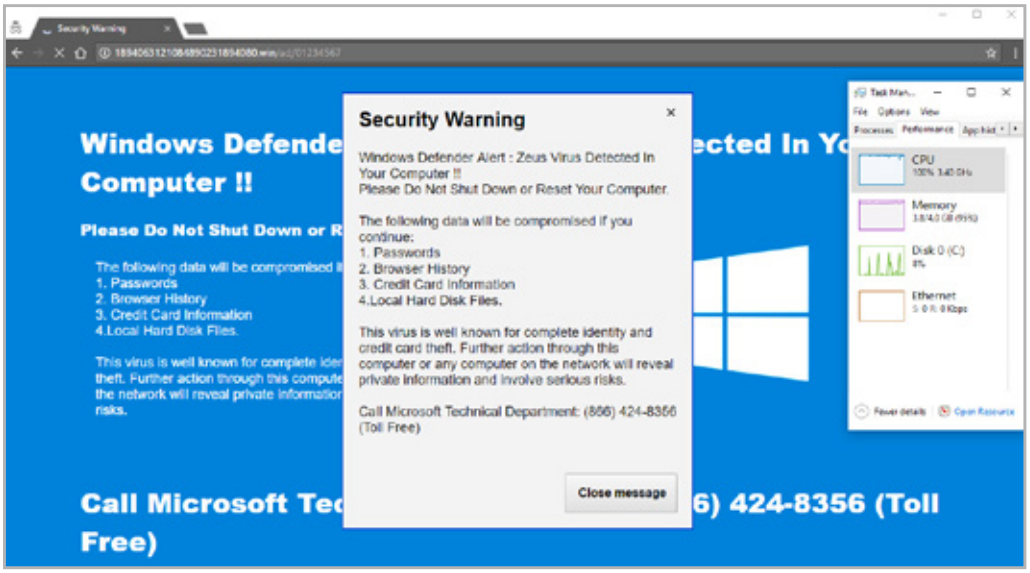

Figura 35. Estafa de soporte técnico de EITest

Spam malicioso

A pesar del inicio lento del año, con una reducción en la cantidad de correos electrónicos que contenían malware debido a la hibernación inesperada del botnet Necurs, el 2017 terminó bien para el spam malicioso. Los atacantes se vieron recompensados con una fuente continua de exploits aprovechables durante el 2017 y muchos tomaron ventaja del correo electrónico como vector para lanzar ataques contra millones de personas.

Este año, también vimos un incremento en el fraude de soporte técnico por correo electrónico en una gran variedad de idiomas y ubicaciones. Además, hicimos un viaje al mundo de los recuerdos con el resurgimiento a gran escala de un antiguo tipo de compresión.

Documentos maliciosos enviados por correo electrónico

Mientras que el 2016 fue víctima de ataques masivos utilizando vulnerabilidades de día cero para ataques de publicidad maliciosa y exploit kits, el 2017 nos trajo en cambio una cantidad comparable de métodos explotables que favorecían la distribución por correo electrónico y se enfocaban en los productos de Microsoft.

No faltaron las vulnerabilidades de Microsoft Office que permitieron la inyección maliciosa y arbitraria de código de cargas maliciosas y los atacantes no perdieron tiempo y aprovecharon las ya comprobadas fortalezas del correo electrónico para facilitar la entrega de documentos maliciosos mediante correos electrónicos cuidadosamente redactados.

Es particularmente notable la adopción de las vulnerabilidades CVE-2017-0199 y CVE-2017-8759 por parte de los autores de malware para facilitar la instalación de cargas maliciosas con poca o nula interacción.

CVE-2017-0199 es una vulnerabilidad que responde a una falla en el objeto olelink de Microsoft Office, la cual puede ocasionar que se emita una solicitud http y se ejecute el código .hta como respuesta. Los autores de malware rápidamente tomaron ventaja de esta vulnerabilidad para enviar correos electrónicos especialmente diseñados que contenían una gran variedad de cargas. Profundizamos en uno de estos ejemplos en nuestro blog Labs, titulado Fake IRS notice delivers customized spying tool (Notificación falsa de IRS instala herramienta personalizada de espionaje).

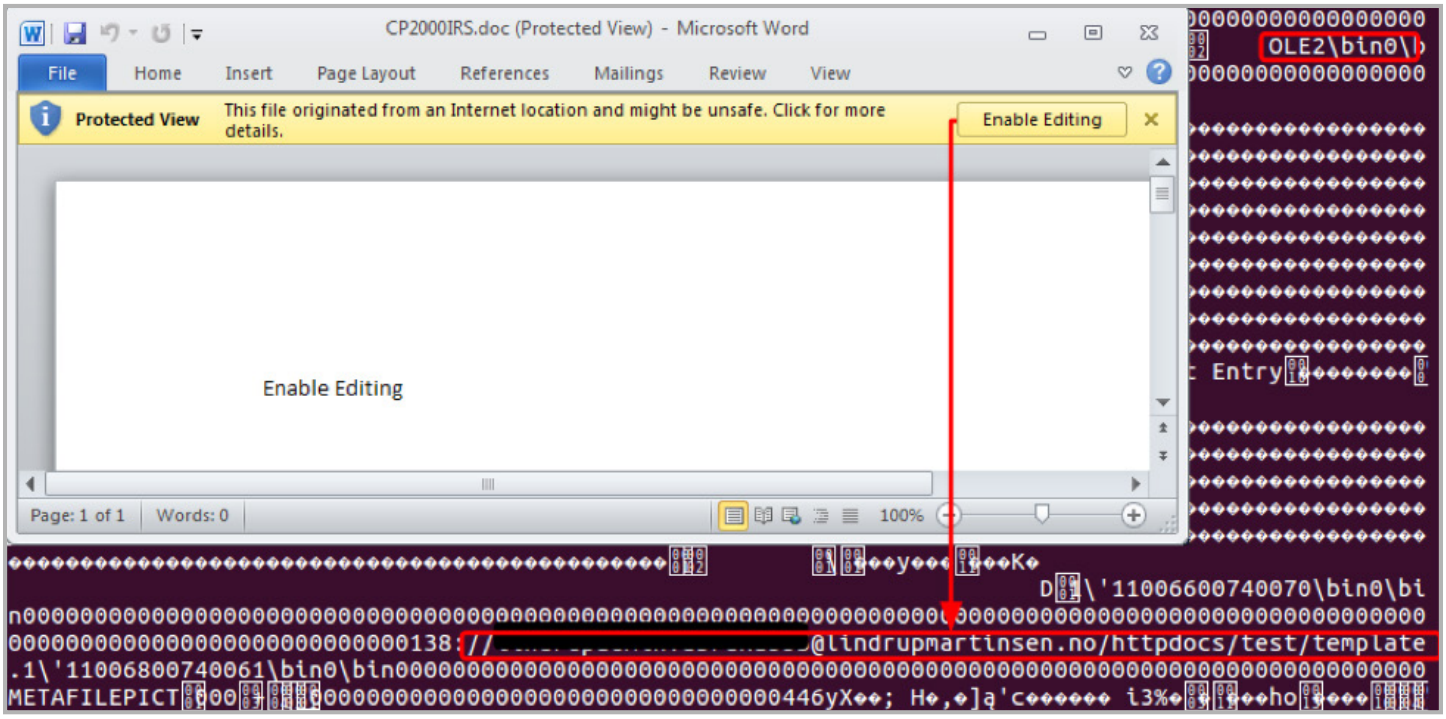

Figura 36. Ejemplo de un documento que utiliza la CVE-2017-0199

CVE-2017-8759 también atrajo la atención de los atacantes por la metodología que utiliza para descargar y ejecutar automáticamente código malicioso. Esta vulnerabilidad de .NET permite a los atacantes aprovechar una falla en los mecanismos de protección del motor Web Services Description Language. Esta falla permite a los atacantes enviar documentos bien redactados que, una vez abiertos en un equipo vulnerable, pueden automáticamente descargar e instalar contenido malicioso. Ya hemos visto a este exploit instalar el infame malware FinSpy, y Malwarebytes cuenta con un análisis detallado sobre este ataque en su publicación Decoy Microsoft Word document delivers malware through a RAT (Documento señuelo de Microsoft Word instala malware a través de RAT).

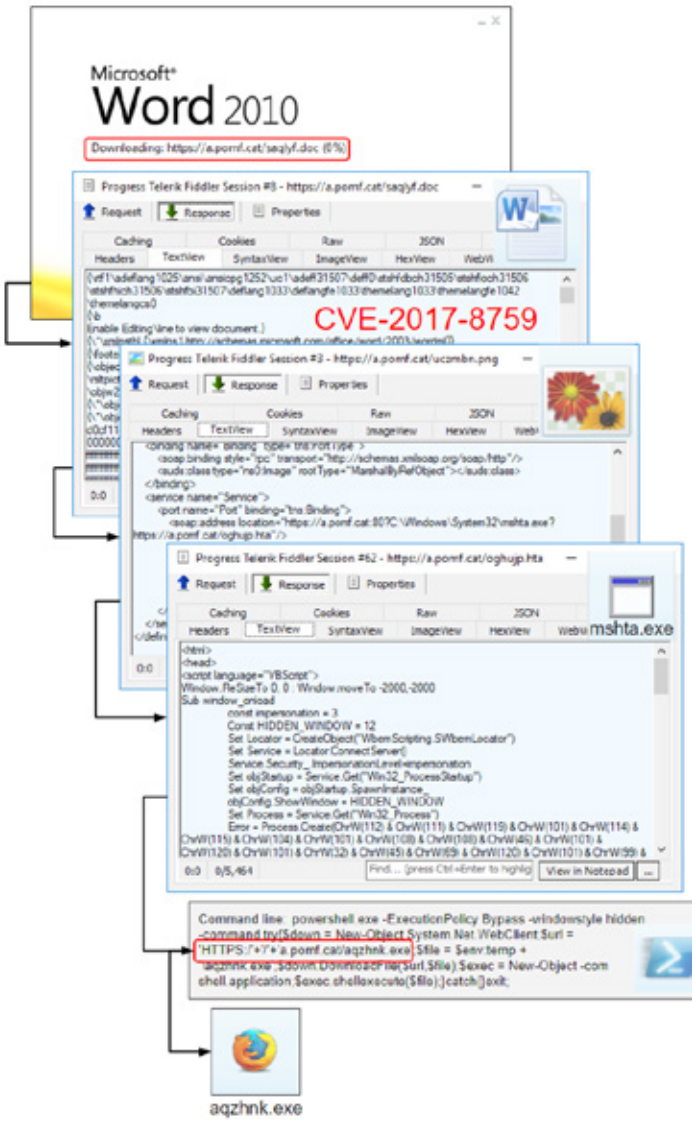

Figura 37. Flujo de CVE-2017-8759

Regresa el formato .ace

Durante el 2017, el spam ha sido uno de los motores de cambio dominantes detrás de la distribución de malware. Los atacantes utilizarán cualquier mecanismo que conozcan para facilitar la instalación de cargas maliciosas. Mientras que esto normalmente incluye exploits novedosos y llamativos que atacan a los equipos vulnerables, en otras ocasiones, los atacantes pueden utilizar tecnologías antiguas y obsoletas con la esperanza de evadir a los sistemas automatizados y las herramientas de detección de spam.

Uno de estos mecanismos, que proliferó en el 2017, fue el uso de archivos .ace para comprimir las cargas de malware malicioso a formatos aceptados en los correos electrónicos. Mientras que el formato .ace ha existido desde hace mucho tiempo, este formato de compresión perdió popularidad al emerger soluciones más comunes y accesibles.

Los atacantes pueden utilizar herramientas que ya existen, pero que tienen índices bajos de adopción, para evadir a los sistemas de automatización y detección, ya que estos sistemas pueden no ofrecer una compatibilidad nativa para estos formatos. Un descuido como este durante el desarrollo puede ser exactamente lo que un creador de malware necesita para lograr una implementación exitosa; así que los atacantes añaden esta metodología a su arsenal.

Tendencias en estafas

Las estafas en el 2017 se destacaron por sus éxitos moderados en actividades de aplicación, un cambio de táctica que se alejó de los tradicionales bloqueadores de navegadores, y por un auge en el contenido relacionado con Bitcoin. En general, conforme los defensores mejoran sus esfuerzos corporativos contra los estafadores, enfocándose en la identificación y eliminación de la infraestructura que les sirve de apoyo, los estafadores se han adaptado, ya sea al cambiar de táctica hacia las llamadas de salida dirigidas o al desarrollar formas de ingreso alternativas, dejando de lado la infraestructura para implementar otras formas de estafa.

Éxito de los defensores

Una mejor comunicación entre las agencias de leyes estatales y federales y las empresas privadas ha tenido como resultado unos juicios extraordinarios contra grupos de estafadores, de los cuales se ha obtenido al menos una compensación parcial para miles de víctimas. Un caso notable es el de agosto, en el cual la FTC obtuvo $10,000,000 de la compañía de estafas Advanced Tech Support y creó un fondo para compensar a las víctimas. Además, los procuradores generales estatales han obtenido más éxitos a nivel local, lo cual contribuye a crear un entorno menos hospitalario para estos estafadores. Como resultado, los grupos de estafas basados en los Estados Unidos y los procesadores foráneos de pagos de soporte técnico experimentaron un declive continuo durante el 2017. Los grupos de estafadores se han visto reducidos, en algunos casos, a tener que solicitar cheques físicos de sus víctimas.

Attorney General Bondi Continues Efforts to Shut Down Tech Scams

TALLAHASSEE, Fla.—Attorney General Pam Bondi today announced the filing of three complaints, including one filed jointly with the Federal Trade Commission, against companies allegedly involved in the operation of tech support scams. Tech support scams trick consumers into believing their computers are infected with viruses and malware in an effort to bilk users out of hundreds of dollars.

"Tech support scams prey on people's fear of losing important work, family photos or sensitive identification information. Using that fear, scammers trick thousands of consumers in to paying millions of dollars to fix problems that never existed," said Attorney General Bondi. "These scams will not be tolerated in Florida and that is why we are bringing more cases against more tech support scammers than any other state in the country—to protect consumers and recover money for victims."

Figura 38. Procurador general de Florida procesa más casos contra las estafas de soporte técnico

El declive de los bloqueadores de navegadores

Conforme la sofisticación y las defensas integradas en los navegadores hacían menos sostenible el uso de bloqueadores de navegadores, los estafadores tuvieron que implementar nuevos vectores hacia el final del 2017, como los correos electrónicos maliciosos y la publicidad maliciosa. La publicidad maliciosa fue especialmente efectiva a lo largo del año debido a la dificultad de reproducir los ataques para fines de análisis y a la poca disposición o capacidad de las grandes compañías publicitarias de monitorear este problema. Ya que implementar una seguridad efectiva al evaluar y vender publicidad ocasionaría pérdidas de ganancias en todos los ámbitos, prevemos que la publicidad maliciosa sea un fuerte vector para la implementación de estafas de soporte técnico durante el 2018.

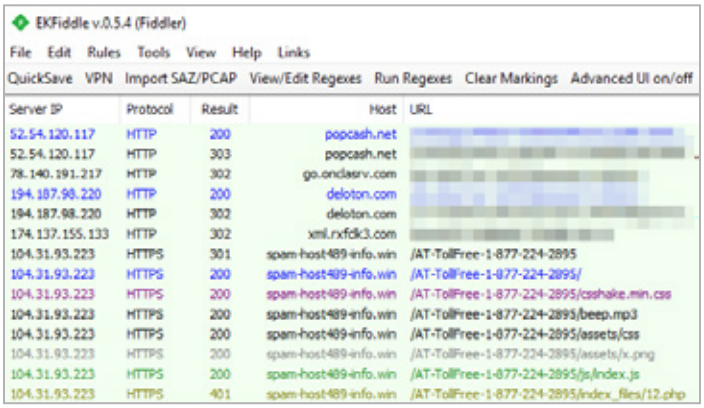

Figura 39. Fiddler EK implementa estafas

Suplantación de identidad mediante estafas de soporte técnico

El torrente de ataques exitosos de malware implementados por correo electrónico ha atraído también a los que se dedican al negocio de las estafas de soporte técnico. El 2017 marcó un aumento en la cantidad de estafas que se originaron por correo electrónico.

Se sabe que los estafadores utilizaron una muy variada selección de tretas para persuadir a las víctimas de hacer clic en enlaces maliciosos.

A lo largo del año, vimos ataques por correo electrónico que aprovechaban nombres de marcas como Amazon, Walmart, Walgreens, USPS y UPS.

Y aunque puede cambiar el contenido del correo electrónico, su objetivo sigue siendo el mismo: persuadir a sus víctimas a hacer clic. Independientemente del método implementado, los usuarios deben siempre evitar ponerse en contacto con empresas que utilicen este tipo de publicidad.

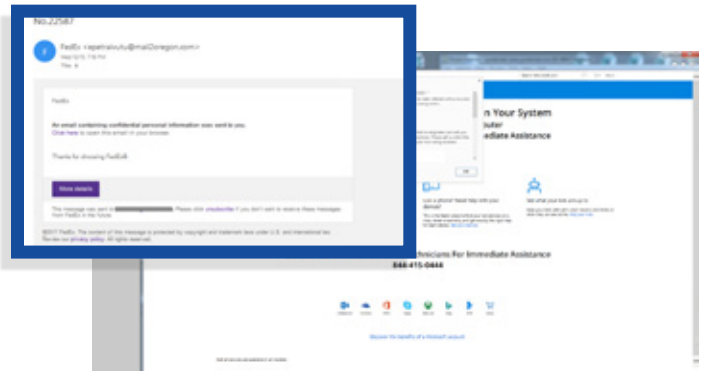

Figura 40. Ejemplo de un correo electrónico que contiene un aviso de Fedex, pero que dirige a una estafa de soporte técnico al hacer clic en el enlace

Bitcoin: llega un nuevo desafío

Conforme la valoración de Bitcoin iba a la alza a finales de año, las estafas de soporte técnico se convirtieron en suplantaciones de monedas populares. Un grupo de estafas que fue especialmente exitoso fue Coinbase, quien presuntamente robó cantidades de hasta cinco cifras a sus víctimas. Utilizando una combinación de ingeniería social y suplantación de identidad de datos personales, los estafadores han dejado a estas víctimas más desamparadas y sin recursos que aquellas que sufren de pérdidas en los medios tradicionales de inversión.

Figura 41. Estafa de Bitcoin

Predicciones para el 2018

El año pasado nos enfrentamos con varios problemas inesperados, con ataques masivos de ransomware, cambios en la distribución del malware y un sorpresivo interés en los mineros de criptomonedas. Nunca ha sido más difícil tratar de predecir qué va a pasar durante todo el año que nos espera. Pero queremos intentarlo de todas formas. Estas son nuestras predicciones para el 2018.

La fiebre por la minería de criptomonedas engendrará nuevas y peligrosas amenazas.

Nuestra primera predicción llega durante un periodo de fiebre por las criptomonedas, durante el cual la minería de tipo drive-by y el alza de valores están despertando el interés tanto de los usuarios como de los criminales. Si continúa este furor, es probable que sigamos viendo la evolución de las herramientas de minería de tipo drive-by, nuevas plataformas de minería (para dispositivos de Android y del Internet de las cosas) y nuevas formas de malware diseñadas para minar y/o robar criptomonedas.

Un año lento para el Internet de las cosas augura más ataques para el 2018.

En octubre del 2016, pudimos ver con el botnet Mirai lo que sucede si se explota el poder del Internet de las cosas. Aunque no hubo ataques masivos al Internet de las cosas en el 2017, los atacantes han estado invirtiendo su tiempo en el desarrollo de nuevas herramientas para aprovechar el Internet de las cosas a través de la minería de criptomonedas, los botnets que distribuyen spam y, probablemente, más ataques de denegación distribuida de servicio (DDoS).

No es descabellado pensar que es posible que veamos ataques de denegación distribuida de servicio (DDoS) contra grandes organizaciones, como aerolíneas y empresas de servicios energéticos, en los que se exija el pago de un rescate para retirar a un ejército de dispositivos del Internet de las cosas infectados por botnets. De acuerdo con la baja que se observó en infecciones de ransomware a finales del 2017, probablemente debido a un menor retorno de inversión, los criminales podrían seguir utilizando el mismo enfoque de exigir rescates, pero, en lugar de encriptar archivos, sus ataques desestabilizarán a las empresas y sus operaciones hasta que el pago se haya hecho.

Continuará la serie de ataques a la cadena de suministro y esto llevará a nuevos métodos de infección de malware.

El año pasado, se experimentaron dos notables ataques a la cadena de suministro: la distribución de NotPetya mediante el proceso de actualización del software de contabilidad MeDoc y la vulneración del software CCleaner. Esta seguirá siendo una vía predilecta de los cibercriminales mientras sigan siendo capaces de infiltrar las defensas de las redes de las empresas de desarrollo de software. Esto podría tener como resultado infecciones a través de actualizaciones y mejoras, el reemplazo de descargas legitimas con malware, exploits de tipo drive-by e incluso actualizaciones de bases de datos para software de seguridad.

El malware en los sistemas Mac tomará diversas formas.

Las amenazas para las Mac han aumentado drásticamente en los últimos años. El uso de malware basado en scripts, los ataques a la cadena de suministro y un aumento en el desarrollo de programas potencialmente no deseados (PUP) en el 2017 nos dieron un ejemplo de lo que seguramente veremos en el 2018. A la vez, conforme las amenazas a las Mac se vuelven cada día más comunes, los escáners y los limpiadores falsos se harán más populares.

Las filtraciones de gobiernos y empresas privadas tendrán como resultado la armamentización de más vulnerabilidades de día cero.

El ataque WannaCry en mayo confundió a muchos profesionales de la seguridad, principalmente debido a su método inesperado de infección: el uso de un código de exploit filtrado. Dos años antes, ya se habían filtrado exploits de una firma privada de seguridad a los exploit kits populares activos. A menos que los gobiernos y las empresas den a conocer las vulnerabilidades que detectan de manera rápida y pública, seguiremos viviendo en un entorno vulnerable sin ser conscientes de ello.

Conclusión

Y con esto concluimos este informe. Estos han sido nuestros aprendizajes, observaciones y predicciones más importantes a partir de lo que vimos en el 2017. La industria del crimen cibernético crece de manera acelerada y muchos de los desarrolladores se han unido para consolidar esfuerzos y crear amenazas más peligrosas. Sin embargo, junto con la constante evolución del malware, cada vez más usuarios aprenden sobre cómo protegerse a sí mismos a través de software, la lectura de artículos e informes y la implementación de tácticas comunes de seguridad en cada sistema que utilizan. Los criminales no pueden obtener ganancias a partir de sus esfuerzos mas que victimizando a los usuarios. Si podemos disminuir la cantidad de posibles víctimas mediante el conocimiento y el desarrollo de software, es posible que todo salga bien en el 2018.

Colaboradores:

- Adam Kujawa, director de Malwarebytes Labs: ransomware/exploits SMB/predicciones para el 2018
- Wendy Zamora, directora de Contenido, Malwarebytes Labs: editora en jefe/resumen ejecutivo/adware
- Jérôme Segura, director de Investigaciones, Malwarebytes Labs: exploits/minería de tipo drive-by
- William Tsing, director de Operaciones, Malwarebytes Labs: tendencias en estafas
- Adam McNeil, analista ejecutivo de inteligencia de malware: spam malicioso
- Pieter Artnz, analista de inteligencia de malware: mineros de criptomonedas/programas potencialmente no deseados (PUP)
- Chris Boyd, analista ejecutivo de inteligencia de malware: ataques geoespecíficos
- Jovi Umawing, analista de inteligencia de malware: cadena de suministro
- Nathan Collier, ingeniero ejecutivo de investigación móvil: Android
- Thomas Reed, director de Mac y Móvil: Mac
- Marcelo Rivero, analista de inteligencia de malware: ransomware