EUIPO
OFICINA DE PROPIEDAD INTELECTUAL DE LA UNIÓN EUROPEA

IDENTIFICACIÓN Y ANÁLISIS DE PROGRAMAS MALIGNOS EN DETERMINADOS SITIOS WEB SOSPECHOSOS DE INFRINGIR LOS DERECHOS DE AUTOR

RESUMEN EJECUTIVO

Septiembre de 2018

Resumen

Los contenidos sospechosos de infringir los derechos de autor representan una vulneración importante de los derechos de propiedad intelectual. Existen algunos sitios web que comparten dichos contenidos públicamente, a veces incluso de forma gratuita, sin ningún registro. Junto con estos contenidos, los sitios web suelen distribuir diversos tipos de programas malignos y programas potencialmente no deseados (PUP, *potentially unwanted programs*), práctica que invita a los usuarios a descargar y lanzar estos archivos. El estudio proporciona una visión general de los ejemplos más actualizados de programas malignos y PUP encontrados en sitios web sospechosos de infringir los derechos de autor. Estos programas utilizan técnicas e ingeniería social engañosas, como instalaciones vacías de juegos y *software* pretendidamente «útil», para incitar a los usuarios finales a que revelen su información confidencial. Durante el estudio, se detectó una serie de programas potencialmente no deseados, tales como *software* «útil», instaladores de juegos falsos y clientes para plataformas de transmisión de vídeo. Este *software* no representa, necesariamente, un peligro directo para el *software* o *hardware* del usuario. Sin embargo, a través de trucos de ingeniería social, se puede convencer a un usuario para que revele información personal confidencial o datos de su tarjeta de pago. Además, podría filtrarse la propia información relativa al ordenador a otras partes sin el consentimiento explícito del usuario.

Equipo de investigación

El equipo de investigación estuvo integrado por Francesca Bosco, responsable de programas del UNICRI, y Andrii Shalaginov, investigador doctoral en seguridad de la información del Departamento de Seguridad de la Información y Tecnología de la Comunicación (Grupo Forense Digital), Facultad de Informática e Ingeniería Eléctrica, Universidad Noruega de Ciencias y Tecnología.

Cláusula de exención de responsabilidad

En este contexto, debe hacerse hincapié en que el único objetivo de la investigación es determinar las características técnicas de los programas malignos y los PUP que se detectaron durante el estudio, y que podrían afectar a los usuarios de internet que naveguen por contenidos sospechosos de infringir los derechos de autor. Las muestras documentadas de programas malignos y PUP no pueden considerarse exhaustivas, ni el objetivo del estudio (o sus resultados) es proporcionar evaluación alguna de la probabilidad o riesgo general de infección por programas malignos y PUP a los que un usuario de internet se enfrenta al buscar material sospechoso de infringir los derechos de autor.


EUIPO
OFICINA DE PROPIEDAD INTELECTUAL
DE LA UNIÓN EUROPEA

Preámbulo

Las actividades sospechosas de infringir los derechos de autor en línea se pueden financiar de diversas formas, inclusive mediante las tarifas de suscripción, las donaciones, el pago de servicios auxiliares y los ingresos de la publicidad gráfica en línea.

Sin embargo, no todos los medios de financiación son tan benignos como los ejemplos anteriores. Durante años, la divulgación de infecciones por programas malignos y otros tipos de programas potencialmente no deseados (PUP) ha sido de importancia clave en relación con la financiación de actividades sospechosas de infringir los derechos de autor en internet.

Los usuarios habituales de internet están comenzando a tomar conciencia de los riesgos de infección cuando acceden a sitios web o aplicaciones móviles sospechosos de infringir los derechos de autor.

El Barómetro de la propiedad intelectual entre los jóvenes de la EUIPO, de 2015, indicó que el 52 % de los jóvenes considera que la seguridad en un sitio web es importante a la hora de acceder a contenidos en línea. En total, el 78 % de los jóvenes afirmó que se lo pensaría dos veces antes de utilizar un ordenador o aplicación si supiera que está infectado por virus o programas malignos. En total, el 84 % declaró que se lo pensaría dos veces antes de utilizar tarjetas de crédito si conociera el riesgo de que se roben sus datos.

En la investigación para este estudio, la Oficina emprendió una tarea que plantea muchos desafíos desde el punto de vista técnico: detectar y documentar ejemplos de programas malignos y PUP que un usuario de internet podría encontrarse al intentar acceder a películas, música, videojuegos y programas de televisión conocidos entre el gran público, y pirateados.

En este contexto, debe hacerse hincapié en que el único objetivo de la investigación fue determinar las características técnicas de los programas malignos y PUP que se detectaron durante el estudio y que podrían afectar a los usuarios de internet que buscan contenidos sospechoso de infringir los derechos de autor. Las muestras documentadas de programas malignos y PUP no pueden considerarse exhaustivas, ni el objetivo del estudio (o sus resultados) era proporcionar evaluación alguna de la probabilidad o riesgo general de infección por programas malignos y PUP a los que un usuario de internet se enfrenta al buscar material sospechoso de infringir los derechos de autor.

La investigación se llevó a cabo en varias fases, en estrecha cooperación con el Centro Europeo de Ciberdelincuencia (EC3) de Europol.

Los resultados muestran una serie de diferentes amenazas relativas a los programas malignos y los programas potencialmente no deseados que un usuario de internet puede encontrarse al navegar por contenidos sospechoso de infringir los derechos de autor. La mayoría de los programas malignos y PUP documentados se pueden describir como troyanos u otro *software* no deseado capaz de obtener acceso injustificado a los datos personales de los usuarios de internet. Estos ejemplos serán relevantes y de interés no solo para la comunidad de titulares de derechos de PI, sino también para las autoridades policiales y aduaneras y, por último, pero no menos importante, para los consumidores que estén preocupados por el acceso a sus datos personales sin su autorización.

Resumen ejecutivo

El estudio proporciona una visión general de los ejemplos más recientes de programas malignos y programas potencialmente no deseados (PUP) detectados en sitios web sospechosos de infringir los derechos de autor. Estos programas utilizan técnicas e ingeniería social engañosas, como instalaciones vacías de juegos y *software* pretendidamente «útil», para incitar a los usuarios finales a que revelen su información confidencial.

El objetivo de este estudio es descubrir y documentar *software* malintencionado o no deseado diseminado en sitios web seleccionados sospechosos de infringir los derechos de autor y clasificar las muestras encontradas en línea según varias categorías de programas malignos. En este contexto, debe hacerse hincapié en que el estudio tuvo como único objetivo determinar las características técnicas de los programas malignos y los PUP que se detectaron durante la investigación y que podrían encontrarse los usuarios de internet que buscaran contenido sospechoso de infringir los derechos de autor. Las muestras documentadas de programas malignos y PUP no pueden considerarse exhaustivas, ni el objetivo del estudio (o sus resultados) era proporcionar evaluación alguna de la probabilidad o riesgo general de infección por programas malignos y PUP a los que un usuario de internet se enfrenta al buscar material sospechoso de infringir los derechos de autor. A los fines de este estudio, se consideran contenidos protegidos por derechos de autor los programas de televisión, las películas, la música y los videojuegos.

Resultados del estudio

Los contenidos sospechosos de infringir los derechos de autor representan una vulneración importante de los derechos de propiedad intelectual. Existen algunos sitios web que comparten dichos contenidos públicamente, a veces incluso de forma gratuita, sin ningún registro. Junto con estos contenidos, los sitios web suelen distribuir diversos tipos de programas malignos y PUP, práctica que invita a los usuarios a descargar y lanzar estos archivos. Durante la identificación de sitios web basada en la clasificación de Alexa Top 500 y una simulación de búsquedas promedio de usuarios que utilizaban motores de búsqueda muy conocidos, como Google, Yahoo y Bing, se descubrió que el conjunto de sitios web cambió en el transcurso de las dos rondas del estudio. Este cambio es, probablemente, el resultado de los esfuerzos de los motores de búsqueda por eliminar enlaces a sitios web sospechosos de infringir los derechos de autor, mientras siguen apareciendo nuevos sitios web sospechosos. En relación con la identificación de sitios web, un hallazgo interesante tiene que ver con el hecho de que la abrumadora mayoría de los sitios web está alojada en los Estados Unidos o tiene nombres de dominio vinculados al alojamiento en ese país. Por el contrario, solo unos pocos se encuentran en servidores dentro de la UE. Además, .com y .net son los nombres de dominio de nivel superior más frecuentes utilizados en sitios web sospechosos de infringir los derechos de autor, lo cual puede derivarse de que, a diferencia de los dominios específicos del país, es posible que no requieran la identificación del usuario con un pasaporte u otros documentos de identificación. En promedio, se añadió un 20 % de sitios web nuevos y se eliminó el 20 % de los sitios web antiguos entre las dos rondas de identificación. Además, casi el 8 % de los sitios web identificados en ambas rondas fue considerado malicioso por la plataforma VirusTotal. Con la ayuda de varios sistemas de administración de contenidos, ahora casi no

supone esfuerzo crear un sitio web y entregar contenido a los usuarios, incluso aplicaciones maliciosas.

Antes de la recopilación de programas malignos, este estudio realizó un control documental de amenazas de programas malignos en 2017 y una clasificación de la situación actual. Se utilizó este conjunto de conocimientos durante el análisis delos programas malignos para observar los principios aceptados por la comunidad sobre la identificación de los tipos y las familias de programas malignos. En total, se recopilaron 106 archivos durante las dos rondas de recopilación de datos. Entre ellos se incluyen archivos descargados directamente de sitios web sospechosos de infringir los derechos de autor, así como archivos que se crearon durante la ejecución de los archivos descargados. Durante el estudio, se descubrió una serie de programas potencialmente no deseados, tales como *software* «útil», instaladores de juegos falsos y clientes para plataformas de transmisión de vídeo. Dicho *software* no supone, necesariamente, un peligro directo para el *software* o *hardware* del usuario. Sin embargo, a través de trucos de ingeniería social, se puede convencer a un usuario para que revele información personal confidencial o datos de su tarjeta de pago. Además, podría filtrarse la propia información relativa al ordenador a otras partes sin el consentimiento explícito del usuario.

Los programas malignos recopilados se analizaron, en un principio, utilizando herramientas de código abierto para comprender la lógica interna, detectar posibles actividades maliciosas y evaluar su relevancia para el presente estudio sobre programas malignos. Además del análisis preliminar con herramientas de código abierto, las muestras de programas malignos recopiladas se analizaron por la plataforma de solución de análisis de programas malignos de Europol (EMAS, *Europol Malware Analysis Solution*), lo que dio lugar a la detección de una gran cantidad de dispositivos y actividades maliciosas diferentes. Los informes de la EMAS incluyen un análisis exhaustivo de los archivos que utilizan cuatro versiones de MS Windows, en las que el tráfico de la red, las llamadas a funciones y las actividades del disco se registran exhaustivamente para su posterior análisis. Además, la plataforma destaca cualquier actividad sospechosa detectada durante las rutinas de ejecución de archivos. Después de analizar todos los informes, la EMAS localizó 35 tipos de actividades maliciosas, agrupadas en 17 clases de eventos maliciosos, que oscilaban entre anomalías generales (como procesos del sistema de lanzamiento o búsqueda de procesos en memorias) y acciones inconfundiblemente maliciosas (como *keylogger*, *rootkit* y alteración del tráfico de red).

En general, las muestras binarias de programas malignos y PUP recopiladas revelaron algunos modelos comerciales generales diferentes: programas «útiles» que pretenden limpiar archivos viejos en el ordenador de un usuario con una suscripción pagada; simuladores de instalación de juegos que exigen los datos personales del usuario; y programas gratuitos que ofrecen acceso a plataformas que distribuyen contenido pirateado, como a través del rastreador BitTorrent. Las dos rondas de identificación de sitios web y la recopilación de programas malignos produjeron resultados prometedores en términos de comprensión de los métodos de diseminación de programas malignos e ingeniería social para atraer información personal e identificable. Además, resulta evidente la creciente popularidad de los dispositivos móviles en los últimos años, a la luz de la detección de muchos programas potencialmente no deseados para el sistema operativo Android, disponibles a través de las plataformas de distribución de contenidos sospechosas de infringir los derechos de autor. Como resultado de la correlación de los análisis, se llegó a la conclusión de que el panorama de amenazas para los programas malignos distribuidos a través de sitios web que infringen los derechos de autor es más sofisticado de lo que podría parecer a primera vista. Entre los tipos de *software* descubiertos, algunos pueden clasificarse, además, como troyanos, *adware*, puertas traseras y agentes. Esta situación se ve agravada por el hecho de que también se encontraron muchas familias específicas de programas malignos, como WisdomEyes, DealPly y FileRepMalware. Asimismo, una clasificación tan completa también es válida para la plataforma Android, no solo para Microsoft Windows. Existe una amplia gama de amenazas para los activos de los usuarios que incluye, entre otros, el robo de credenciales confidenciales, datos personales, información de configuración de *hardware* y modificaciones del tráfico de la red. Por lo tanto, aunque el *software* identificado sea PUP, es posible, no obstante, que tenga un impacto en los usuarios, especialmente en casos que involucran a un consumidor medio que podría no estar completamente al tanto de las prácticas y medidas básicas de seguridad en línea.

Se muestra, a continuación, un ejemplo de los hallazgos del estudio.

Sitio web 03

El sitio web engaña a los usuarios para que utilicen una instalación de juegos falsa; todo el proceso de obtención de información confidencial de un usuario ha cambiado entre la primera y la segunda ronda de recopilación de programas malignos.
El usuario de este servicio descarga un archivo que contiene contenido enmascarado como archivos relacionados con el juego y no un archivo binario explícitamente ejecutable, que cualquier antivirus podría detectar como malicioso. El archivo cifrado otorga acceso solo a los nombres de archivo, pero no al contenido sustantivo de los archivos.

Sitio web 09

El sitio web ofrece acceso a cualquier tipo de contenido de vídeo disponible a través de rastreadores de «torrents» con la ayuda de una herramienta de *software*. Esta herramienta requiere menos interacciones del usuario en comparación con otros rastreadores de BitTorrent.
Solo se requieren unos pocos clics para descargar contenidos de fuentes desconocidas, mientras que el usuario no está protegido ni tiene control sobre lo que se está descargando.

Sitio web 08

(Android) El sitio web proporciona acceso a una gama de aplicaciones móviles gratuitas sin registro. Una aplicación proporciona acceso ilimitado a la transmisión de programas de televisión y películas. No hay una solicitud explícita para proporcionar información confidencial del usuario o datos de pago para comprar acceso a vídeos protegidos por derechos de autor. Sin embargo, un usuario tiene que deshabilitar las configuraciones de seguridad que permitirán la instalación de aplicaciones distintas de las de un comercio de aplicaciones oficial.

Metodología

Con el fin de llevar a cabo la investigación, se tuvo que adoptar una metodología sólida para tratar la selección de títulos y sitios web, así como la tarea de detectar y documentar los ejemplos de programas malignos y PUP encontrados, la cual representa un desafío desde el punto de vista técnico. Se describe, a continuación, una breve descripción de la metodología:

1. En la fase I de la investigación del UNICRI, en colaboración con el Observatorio Europeo de las Vulneraciones de los Derechos de Propiedad Intelectual (Observatorio), se estableció un grupo de de expertos para prestar apoyo y dar asesoramiento sobre la metodología de investigación, la selección de sitios web utilizados para el análisis y para evaluar la investigación realizada dentro de cada fase de aplicación del proyecto. El grupo de expertos de apoyo se compuso de representantes de las partes interesadas del Observatorio, organizaciones de titulares de derechos, el mundo académico, las fuerzas del orden y las agencias de la UE.

2. Al mismo tiempo, se seleccionó el equipo de investigación. En el marco de este informe, técnicamente no fue posible[1] investigar en todos los Estados miembros de la UE; por lo tanto, se seleccionó al azar una muestra de 10 países de los 28 Estados miembros de la UE en la fase II.

[1] El número de países seleccionados tendrá un impacto (aumento) directo sobre el número de sitios sospechosos de infringir los derechos de autor seleccionados y los correspondientes archivos binarios que se analizarán. Así pues, se optó concentrarse únicamente en una muestra de países a fin de poder de realizar, con éxito, la parte práctica del estudio dentro de un periodo de tiempo determinado.

3. En la fase III se identificaron películas, programas de televisión, canciones y videojuegos populares. La popularidad incluyó la popularidad mundial y la popularidad en solo uno o más de los 10 países de la muestra al comienzo del período de recopilación de datos, el 23 de junio de 2017. En las fases subsiguientes del estudio, estos títulos de muestra se utilizaron sistemáticamente en búsquedas web en línea para encontrar sitios web y aplicaciones móviles que infringen los derechos de autor. Cada título cumple dos o más de los siguientes criterios:

   - ser popular en el momento de la recopilación de datos en los Estados miembros de la UE,
   - ser popular en el momento de la recopilación de datos a escala mundial,
   - ser popular históricamente a escala mundial, y
   - clasificarse como película, programa de televisión, canción o videojuego.

   Se seleccionaron cinco títulos de películas, cinco títulos de programas televisión, cinco títulos musicales y cinco títulos de videojuegos, lo que arroja un total de 20 títulos de muestra. Se prestó especial atención a las fuentes utilizadas para identificar la popularidad de un título en particular, lo que implicó un proceso de selección sistemático con el fin de garantizar que los datos de origen estuvieran disponibles para todos o la mayoría de los Estados miembros.

4. La fase IV identificó los sitios web sospechosos de proporcionar acceso ilegal a material protegido por derechos de autor que fueran populares en todo el mundo o en los 10 países de la muestra, a fecha de 26 de junio de 2017 (primera ronda de recopilación de programas malignos). En una fase posterior del estudio, estos sitios web se analizaron en busca de programas malignos y programas potencialmente no deseados.

   La metodología para identificar sitios web sospechosos de infringir los derechos de autor se desarrolló con las aportaciones del grupo de expertos de apoyo identificado en la fase I, así como con una revisión por parte del UNICRI de la literatura existente. Se diseñó, específicamente, para generar una muestra de sitios web que:

   - sean populares en los diferentes Estados miembros de la UE, lo que garantiza una amplia cobertura geográfica;
   - representen diferentes tipos de sitios web sospechosos de infringir los derechos de autor, incluidos sitios web de transmisión de datos, enlaces de sitios web, sitios web de alojamiento, *cyberlockers* y sitios web de *torrents*;
   - representen una amplia gama de contenido sospechoso de infringir los derechos de autor, incluidos películas, títulos de programas de televisión, música y videojuegos; y
   - representen sitios web con los que el usuario promedio de internet se encuentra cuando intenta acceder a material sospechoso de infringir los derechos de autor.

   Se utilizaron cinco pasos para seleccionar sitios web sospechosos de infringir los derechos de autor. Los tres primeros pasos se diseñaron para identificar los sitios sospechosos de infringir los derechos de autor más populares en los Estados miembros de la UE. Este método imitaba aquellos escenarios en los que un usuario promedio podría buscar sitios web sospechosos de infringir los derechos de autor sin especificar, por ejemplo, el título de una película o una canción. Los dos pasos finales se diseñaron para identificar sitios sospechosos de infringir los derechos de autor que un usuario promedio podría encontrar al buscar formas de descargar un título popular específico, sin especificar un sitio web. Este paso fue particularmente significativo, dada la presencia de presuntos sitios web maliciosos que envenenan los resultados de las búsquedas, explotando los temas destacados a través de la optimización de los motores de búsqueda. Juntos, los dos enfoques cubrieron las diferentes formas en que un usuario de internet promedio intentaría encontrar material sospechoso de infringir los derechos de autor en línea.

   Se hizo hincapié en el análisis simultáneo de programas malignos y PUP específicos para aplicaciones móviles en dispositivos; por ejemplo, teléfonos inteligentes y tabletas, como una de las principales amenazas emergentes de ciberdelincuencia. El análisis se limitó a los dispositivos

Android debido a las indicaciones, en la literatura existente, de una mayor presencia de programas malignos en las tiendas de aplicaciones de Android (es decir, Google Play) que en la tienda iTunes de Apple. La metodología se diseñó para generar una muestra de aplicaciones móviles que:

- fueran populares en el momento de la recopilación de datos a escala mundial;
- representasen diferentes tipos de aplicaciones (para incluir aplicaciones de transmisión, aplicaciones de *torrents* y aplicaciones de alojamiento);
- contuviesen o proporcionaran acceso a una amplia gama de contenidos que, presuntamente, infringen los derechos de autor (incluyendo películas, títulos de programas de televisión, música y juegos móviles); y
- representen lo que un usuario promedio de un dispositivo móvil encontrará al intentar descargar o usar una aplicación que facilite el acceso a contenidos sospechosos protegidos por derechos de autor.

5. La fase V consistió en la recopilación de programas malignos y PUP, además de las aplicaciones móviles en los sitios web identificados, que se examinarían en una etapa posterior para una clasificación adecuada. La fase de adquisición de datos incluyó dos rondas de recopilación y análisis de programas malignos, realizadas durante el verano de 2017. La primera ronda de recopilación de programas malignos dio como resultado 1 054 nombres de dominio únicos, y la segunda ronda reveló 1 057 nombres de dominio únicos en los 10 Estados miembros de la UE seleccionados. Los programas malignos se recopilaron de forma manual y automática para simular la experiencia de un usuario promedio.

Recopilación manual. Este método implicó revisar manualmente los dominios identificados en la fase previa. Mediante la recopilación manual, el experto pudo simular la experiencia de un usuario promedio de internet que hace clic en anuncios e interactúa con sitios web que requieren indicaciones.

Recopilación automatizada. Este método empleó un rastreador web automatizado diseñado por un experto para seguir todos los enlaces disponibles en un sitio web sospechoso de infringir los derechos de autor. En primer lugar, en cualquier sitio web determinado, el rastreador primero recopiló información de los enlaces en la página de inicio. En segundo lugar, el rastreador siguió cada uno de esos enlaces a sitios web secundarios. En tercer lugar, el rastreador siguió cada uno de esos enlaces a sitios web terciarios. En cada paso, el rastreador recuperó archivos binarios de interés para el posterior análisis manual, incluidos los programas potencialmente malignos o sospechosos y los programas potencialmente no deseados. Este proceso continuó hasta alcanzar unos 1 000 enlaces por sitio web.

6. Una vez que se recopilaron los archivos binarios, se analizaron en un entorno informático seguro, para comprender su funcionalidad interna y para su adecuada clasificación. El análisis preliminar se llevó a cabo utilizando herramientas de código abierto para poder correlacionar los hallazgos con informes de amenazas cibernéticas. Las muestras de *software* recopiladas se entregaron a la EMAS para su análisis; el análisis de la EMAS se comparó luego con los resultados preliminares.

Visión general de la metodología

Detección de muestras de programas malignos y PUP

A 28 de julio de 2017, se habían revisado automáticamente 5 240 sitios web (1 054 únicos) durante la primera ronda de recopilación, con 617 archivos relevantes recuperados (música, vídeo, archivos *torrent* y *software*) y un tamaño total de 47 GB. Este lote de archivos sin clasificar requirió un análisis adicional para decidir qué archivos recopilados eran relevantes para el estudio. Las muestras de los sitios web que infringen los derechos de autor fueron similares en los 10 países de muestra respecto de cada uno de los tipos de medios (programas de televisión, películas, música y videojuegos). Como resultado, Bélgica fue elegida al azar a partir de los países de la muestra, y todos los sitios web identificados como sitios web que infringen los derechos de autor para Bélgica se verificaron manualmente para descartar la presencia de *software* malicioso o no deseado. El 10 de agosto de 2017, después de la segunda ronda de recopilación, se recuperó automáticamente un total de 3 665 archivos de los sitios web de todos los países, con un tamaño total de 167 GB. El número total de URL exclusivas extraídas para todos los países fue de 1 057 de los 5 606 sitios web, lo que impidió verificarlas todas manualmente.

Después de un análisis preliminar de los archivos recopilados, se extrajeron 106 archivos binarios únicos para MS Windows, Android y Mac OS como resultado de ambas rondas de recopilación de programas malignos. Más específicamente, se seleccionaron 41 archivos durante la primera ronda y 65 se seleccionaron durante la segunda ronda, en particular: 2 para Mac, 15 para Android y 89 para MS Windows. De estos archivos, 21 se pueden considerar programas maliciosos bien conocidos y señalados por varios proveedores de antivirus como añadidos por la plataforma VirusTotal. Estos incluyen archivos descargados directamente de sitios web seleccionados sospechosos de infringir los

derechos de autor, así como archivos que se crearon durante la ejecución de los archivos descargados. Posteriormente, las muestras de *software* recopiladas se analizaron en un entorno de prueba limitado y se entregaron a la EMAS para un análisis más avanzado de posibles actividades maliciosas. En general, se descubrieron 821 eventos maliciosos distintos en cuatro informes de la EMAS (Windows 7 SP1, Windows7 SP1 de 64 bits, Windows 10 de 64 bits, Windows XP SP3) para todos los archivos binarios. Algunos de los informes no informaban sobre actividades sospechosas y algunos de ellos tenían hasta 10 actividades maliciosas previamente conocidas. Durante la etapa final del estudio se correlacionaron los resultados del análisis preliminar y de los informes de la EMAS. El resumen cuantitativo de los resultados se presenta en la tabla a continuación.

	Ronda 1	**Ronda 2**
Fecha	28 de julio de 2017	10 de agosto de 2017
Sitios web descubiertos en 10 países de la UE	5 240	5 606
Sitios web únicos	1 054	1 057
Archivos relevantes	617	3 665[2]
Tamaño de los archivos relevantes, GB	47	167
Entregados a la EMAS		
Android	3	12
Mac OS	2	–
MS Windows	36	53
Tamaño total, *bytes*	175 600 117	522 991 095

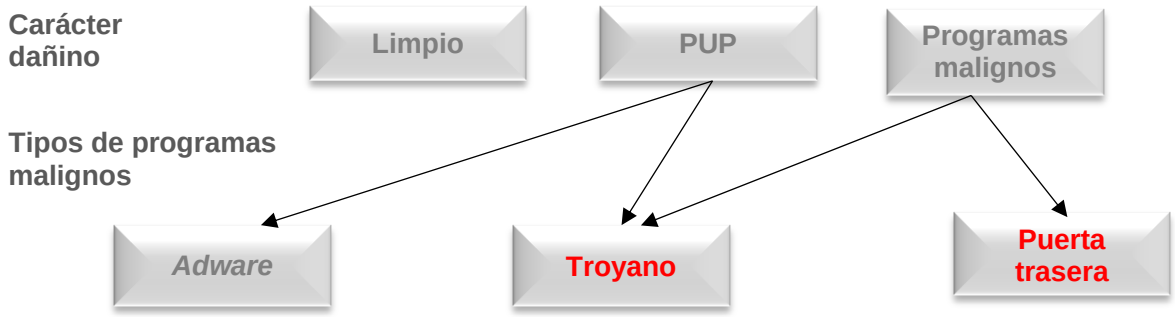
Solución para el análisis de programas malignos de Europol (EMAS)

La solución para el análisis de programas malignos de Europol (EMAS) es una solución dinámica y automatizada de análisis de programas malignos proporcionada por Europol a los Estados miembros de la UE. La EMAS ofrece la posibilidad de crear informes de análisis, pero su característica más revolucionaria es producir inteligencia para los investigadores policiales. Las verificaciones cruzadas automatizadas pueden mostrar enlaces entre ataques realizados en diferentes países con los mismos programas malignos o por la misma organización criminal que promueve la misma familia de programas malignos, que se conectan a los mismos dominios y están relacionados con diferentes investigaciones dentro o fuera de la UE. En 2015, la EMAS se automatizó por completo para permitir el acceso directo a las fuerzas del orden con las que Europol ha suscrito acuerdos operativos. En 2015, se analizaron 525 108 archivos en la EMAS, de los cuales 356 863 fueron identificados como maliciosos.

Como se muestra en la cifra a continuación, los archivos binarios recopilados se pueden clasificar, en general, según su carácter dañino, como: benignos (archivos que no causan ningún daño), PUP y programas malignos dañinos. Además, no solo se descubrieron PUP para Microsoft Windows, sino que también se encontraron para Android y Mac OS, lo que sugiere que los desarrolladores de programas malignos intentan afectar a tantos usuarios como sea posible mediante el uso de diferentes plataformas. Los PUP y los programas malignos se pueden diferenciar aún más según los principales tipos de programas malignos; es decir, troyano, *adware* y puerta trasera. La mayoría del *software* que se encontró quedó comprendido en la categoría de PUP. El funcionamiento de los PUP puede

[2] Para explicar la diferencia en los números entre la ronda 1 y la ronda 2, durante la ronda 2 de recopilación automatizada hubo sitios web que publicaron múltiples conjuntos de archivos en cada una de sus páginas web.

asociarse a uno de los siguientes modelos comerciales: la instalación de juegos falsos que requieren datos de cuentas personales y bancarias, la descarga de programas «útiles» que obligan a los usuarios a comprar una suscripción a una versión pagada o la instalación de programas gratuitos para acceder a plataformas que infringen los derechos de autor. Estas aplicaciones podrían comprometer los datos personales de los usuarios y la configuración del ordenador. A través de trucos de ingeniería social, también se podrían divulgar diversos tipos de datos privados, como datos de tarjetas de pago, información de identificación personal y credenciales de cuentas de redes sociales. Del mismo modo, la investigación identificó 15 aplicaciones de Android de mercados de aplicaciones de terceros y, después del análisis preliminar, se concluyó que dichas aplicaciones podrían estar involucradas en la distribución de contenido que infringe los derechos de autor y en la divulgación de datos personales.



Amenazas para los usuarios finales

Durante las dos rondas de identificación de sitios web y análisis de programas malignos, no se encontraron binarios de *ransomware*. En general, la mayoría de los programas malignos recopilados se puede caracterizar como troyanos, lo que significa que podrían estar representados en los sitios web como *software* benigno de uso común o popular, mientras que, en realidad, pueden robar o divulgar información privada. Un usuario inexperto puede depositar un alto grado de confianza en el *software* y es posible que no perciba ninguna anormalidad. Además, el análisis estático y las observaciones conductuales dinámicas de dicho *software* podrían no revelar su funcionalidad completa sin tener un código fuente. Tras el análisis preliminar de programas malignos, el análisis de la EMAS mostró actividades maliciosas más específicas. El impacto de tener este *software* instalado en el ordenador de un usuario final puede ser considerable, ya que es posible que cause no solo pérdidas financieras, sino también el robo de datos personales, y suponga otros riesgos de acceso y control no deseados. Es de esperar que estas actividades den lugar a la recopilación y transmisión de información personal a terceros en formato de texto cifrado o abierto. Tales datos podrán consistir, por ejemplo, en las credenciales de la cuenta bancaria del navegador, datos de la configuración del *hardware/software* del ordenador o, básicamente, cualquier cosa escrita con el teclado.

IDENTIFICACIÓN Y ANÁLISIS DE PROGRAMAS MALIGNOS EN DETERMINADOS SITIOS WEB SOSPECHOSOS DE INFRINGIR LOS DERECHOS DE AUTOR

RESUMEN EJECUTIVO

Septiembre de 2018