VÍDEO intypedia006es

LECCIÓN 6: MALWARE

AUTOR: Bernardo Quintero

Hispasec – VirusTotal Founder

ALICIA

Hola, bienvenidos a intypedia. Hoy vamos a hablar del apasionante mundo de los códigos maliciosos y el negocio que existe alrededor de ellos. ¡Acompáñanos!

ESCENA 1. INTRODUCCIÓN AL MALWARE: CONCEPTOS

ALICIA

Hola Bernardo, quería consultarte una cosa sobre mi ordenador. Últimamente aparecen muchas ventanas de publicidad de forma aleatoria, sin que yo haga nada. También lo noto especialmente lento cuando navego por Internet… ¿crees que podría estar infectado por un virus?

BERNARDO

Podría ser algún tipo de malware. Si quieres déjame que lo estudie un momento para ver si encontramos al culpable de ese comportamiento extraño.

ALICIA

Claro, toma, aquí lo tienes. Me has dicho que puede ser un malware, ¿eso qué es, un tipo de virus?

BERNARDO

Malware es un término genérico para referirse a cualquier tipo de software malicioso o molesto que se instala en los sistemas, también se caracterizan porque llevan a cabo acciones no deseadas sin el consentimiento del usuario. Los virus informáticos son en realidad un subtipo dentro de la gran familia del malware, al igual que otros especímenes como son los gusanos, troyanos, adware, keyloggers, dialers, etc.

ALICIA

Vaya, no sabía que hubiera tantos tipos de software malicioso. ¿Qué diferencias hay entre ellos?

BERNARDO

Los virus informáticos tienen la capacidad de adjuntarse o incrustarse en otro software, es decir, se auto-replican infectando otros programas.

De esta forma una aplicación legítima, por ejemplo un juego de ordenador o un programa de contabilidad, podría estar infectado por un virus si ha tenido contacto con él en un sistema infectado. En el caso de los gusanos, no tienen esa capacidad de introducirse e infectar a otros programas, y en su lugar se replican haciendo copias de sí mismos. Por ejemplo, uno de los casos más conocidos fue el gusano ILOVEYOU, que se replicaba enviando una copia de sí mismo por correo electrónico simulando ser una carta de amor. Si alguien abría el fichero que contenía la supuesta carta de amor, el gusano se ejecutaba y se auto-enviaba de nuevo en un mensaje a toda la lista de contactos de correo electrónico de ese usuario.

Por otro lado, el adware es todo aquel software que presenta publicidad no deseada ni consentida por el usuario, los keyloggers son programas que permiten capturar las pulsaciones de teclado de manera que actúan como espías de lo que el usuario infectado escriba en su sistema, y los dialers realizan llamadas de tarificación adicional a través de un módem, con el consecuente incremento en la factura telefónica de los usuarios afectados. Una atención especial merecen los troyanos por su difusión actual. Los troyanos, a diferencia de los virus y los gusanos, no son capaces de infectar a otros programas ni auto-replicarse por sí mismos, y suelen presentarse como un programa legítimo a la espera de que el usuario lo acepte y ejecute.

De hecho, su nombre proviene del famoso caballo de madera que los griegos utilizaron para infiltrarse en la ciudad de Troya, haciéndoles creer que se trataba de un regalo, cuando en realidad en su interior se encontraban escondidos los soldados dispuestos a atacar. Hoy día los troyanos representan la familia más extensa dentro del malware y a su vez se dividen en muchas subespecies. Así, hablamos de troyanos backdoor aquellos que instalan una puerta trasera que permite a un intruso acceder al sistema, troyanos bancarios aquellos que están especializados en el robo de credenciales de acceso a la banca por Internet, etc.

ALICIA

¡Qué interesante! Entonces las ventanas que salen en mi ordenador pueden estar provocadas por un adware… ¿Existen más tipos de malware?

BERNARDO

Sí, hay muchos más, y además podemos tener varias clasificaciones de malware según diferentes criterios. Por ejemplo atendiendo a los mecanismos de distribución, a los métodos de instalación en el sistema, a la forma en que son controlados remotamente, etc. Hoy día los especímenes de malware suelen poseer muchas funcionalidades y se suelen clasificar según la más destacada. Por ejemplo, podríamos hablar de un troyano que tiene funciones de rootkit si posee técnicas específicas para permanecer oculto ante usuarios avanzados y soluciones de seguridad, además puede ser un bot si forma parte de una red de equipos infectados que son controlados de forma centralizada y remota. Al mismo tiempo también podría hacer aparecer publicidad no deseada y capturar las pulsaciones de teclado, por lo que también entraría en la familia adware y keylogger. Es decir, sería un troyano-rootkit-bot-adware-keylogger… ¡todo en uno! En realidad este escenario es bastante común.

ESCENA 2. DIFUSIÓN DEL MALWARE. ¿CÓMO SE INFECTA?

ALICIA

Bernardo me ha quedado bastante más claro los diferentes tipos de malware que existen. Quizás los troyanos y el adware sean los más comunes. ¿Cómo hacen para infectar ordenadores?

BERNARDO

A día de hoy la mayor parte del malware se distribuye a través de Internet. Uno de los métodos más usuales es el conocido como "drive-by download" que consiste en descargar y ejecutar el fichero malicioso, por ejemplo a través de la Web o ejecutando un fichero adjunto recibido por correo electrónico, por ejemplo, un fichero PDF malicioso. En muchas ocasiones se le engaña al usuario haciéndole creer que es un programa o información útil para él, por ejemplo, para un software para reproducir vídeos. En otras ocasiones, la infección es transparente al usuario; sólo es necesario visitar una página Web que aproveche alguna vulnerabilidad del navegador Web para descargar y ejecutar el malware. No obstante, en general cualquier protocolo de Internet puede ser utilizado para distribuir malware, por ejemplo las redes P2P o la mensajería instantánea. No debe olvidarse, además, que también los medios de almacenamiento físico pueden propagarlos; por ejemplo, es común la distribución de ellos a través de memorias USB.

ESCENA 3. EL NEGOCIO DEL MALWARE

ALICIA

Bernardo, hay algo que no entendiendo, ¿por qué alguien querría crear malware? ¿Quizás para demostrar que es más inteligente?

BERNARDO

Bueno, más o menos. Cuando aparecieron los primeros virus informáticos, los creadores de malware eran personas que tenían mucha destreza programando en lenguaje ensamblador y el único fin era experimentar y demostrar su capacidad ante terceros. Digamos que en su comienzo fue una década "romántica", en cuanto a que no existía un fin económico por parte de los creadores de virus. Hoy día el panorama es bien diferente; existe todo un negocio alrededor del malware, hay verdaderas mafias detrás de estos bichos.

ALICIA

¿Pero cómo pueden ganar dinero con el malware? ¿Cuál es el negocio?

BERNARDO

Hay muchas vías para ganar dinero a través del malware. Por ejemplo, existen los especímenes especializados en delitos financieros, como los troyanos que roban credenciales de acceso a la banca electrónica, de forma que los atacantes pueden realizar transferencias en nombre de la víctima. A este tipo de malware también se le conoce por el nombre de "crimeware". Por ejemplo, el adware produce dinero mediante la venta de publicidad intrusiva en los ordenadores infectados, en muchas ocasiones los anunciantes no son conscientes de estas prácticas, sino que creen que están pagando campañas de publicidad legítimas. De manera similar hay malware cuya función es enviar spam, mensajes masivos de publicidad a través de los sistemas infectados. Las botnets, o redes de sistemas controladas de forma central, son utilizadas en muchas ocasiones para realizar ataques distribuidos de negación de servicio contra sitios Web, como por ejemplo comercios electrónicos. Básicamente los miles de sistemas infectados, o incluso millones, reciben órdenes de visitar o enviar tráfico a un sitio Web, produciendo su colapso. En esos casos los sitios sufren chantajes a cambio de no ser atacados.

Pero la cosa no se queda ahí… existen otras muchas estafas relacionadas con el malware. Por ejemplo, está el tipo de malware "ransomware" que se basa en el chantaje; por ejemplo cifra los documentos y fotos de los sistemas infectados para luego pedir un rescate al usuario si quiere recibir la contraseña que permita descifrarlos y recuperarlos.

Otro modelo de fraude en auge es el malware clasificado como "rogueware", que paradójicamente son falsos antivirus que cobran al usuario para eliminar supuestas infecciones. Evidentemente estos productos no eliminan nada, toda las detecciones y supuestas desinfecciones son falsas; lo único cierto es que el usuario habrá pagado por un software que es un timo.

ESCENA 4. CONTRAMEDIDAS: DETECCIÓN Y ELIMINACIÓN DE MALWARE

ALICIA

¿Qué tal va el análisis de mi ordenador Bernardo? ¿Has descubierto algo?

BERNARDO

Sí, he encontrado dos especímenes de malware instalados: “AdWare.Win32.Axarq.a” y “Trojan.Bredolab”. El primero era el que provocaba que aparecieran esas molestas ventanas de publicidad. El segundo era un troyano que recibe órdenes de forma remota; tu ordenador estaba formando parte de una botnet. Es probable que primero te infectaras con “Trojan.Bredolab” y que este troyano, días más tarde, descargara e instalara el adware en tu equipo. Una hipótesis es que te infectaras de forma automática navegando por Internet, ya que estás utilizando una versión antigua de Internet Explorer que tiene vulnerabilidades.

ALICIA

¿Pero yo tengo un antivirus instalado y actualizado? ¿No debería haberme protegido?

BERNARDO

Los antivirus son una solución de seguridad recomendable, pero no son infalibles. Aunque muchos implementan sistemas heurísticos, firmas genéricas y detecciones basadas en el comportamiento para tratar de detectar los especímenes nuevos, la realidad es que buena parte de la protección que ofrecen contra el malware de nueva generación sigue siendo reactiva. Es decir, siempre hay un número indeterminado de casos donde el antivirus no podrá proteger de forma efectiva.

ALICIA

¿A lo mejor instalándome un sistema operativo distinto de Windows estaría más segura? ¿Quizás Linux o Mac?

BERNARDO

Todos los sistemas operativos son proclives a tener software malicioso; de hecho existen muchos especímenes especialmente diseñados para Linux y Mac. No obstante, es cierto que la gran mayoría del malware se diseña para Windows ya que es un sistema de uso mayoritario; no olvidemos que el malware es un negocio y por tanto los creadores intentan maximizar su beneficio afectando al mayor número de víctimas. Es decir, aunque puedes infectarte con cualquier sistema operativo, sí es cierto que a efectos prácticos tienes más posibilidades con Windows. Mi recomendación es que uses el sistema operativo y el software en general que mejor se adapte a tus necesidades.

ALICIA

¿Entonces qué me recomiendas para prevenir este tipo de infecciones?

BERNARDO

Hoy lo más importante es actualizar el sistema operativo y las aplicaciones de tu ordenador, especialmente algunas aplicaciones críticas como el visualizador de archivos en formato PDF o el paquete de ofimática. No debes olvidar de actualizar la versión de tu navegador Web y de aquellas extensiones más populares que permiten ver contenido multimedia, vídeos flash, etc. Lógicamente, aunque no es una medida infalible, tener instalado un antivirus actualizado constituye una capa más a añadir a la seguridad de tu ordenador. En cualquier caso, a todo esto hay que sumarle sentido común y actitud crítica antes de ejecutar programas de desconocidos o pinchar en enlaces recibidos por correo electrónico. Estas simples medidas permitirán prevenir muchas situaciones de riesgo.

ALICIA

¡Gracias Bernardo! Seguiré tus consejos.

BERNARDO

Bueno Alicia, ya he eliminado el malware de tu sistema y he actualizado el sistema operativo y todas tus aplicaciones. Por hoy ya es suficiente. En la página Web de intypedia encontrarás documentación adicional a esta lección. ¡Adiós!

ALICIA

¡Hasta la próxima lección!

Guión adaptado al formato intypedia a partir del documento entregado por D. Bernardo Quintero.

Madrid, España, marzo de 2011

http://www.intypedia.com

http://twitter.com/intypedia