No. 30 / octubre - noviembre 2017

.Seguridad®

Cultura de prevención para TI

30

La seguridad es responsabilidad de todos

Buenas prácticas para prevenir incidentes

Contenido

.Seguridad
Cultura de prevención para TI

Universidad Nacional Autónoma de México. Dirección General de Cómputo y Tecnologías de Información y Comunicación. Coordinación de Seguridad de la Información/UNAM-CERT. Revista .Seguridad Cultura de prevención para TI M.R., revista especializada en temas de seguridad del UNAM-CERT.

Editorial

.Seguridad
Cultura de prevención para TI

La seguridad es responsabilidad de todos:

Buenas prácticas para prevenir incidentes

En el segundo trimestre del 2017 se detectó un aumento en los ciberataques con respecto al mismo periodo en el 2016. Según PandaLabs, hubo un incremento de 40% en los ataques, lo cual nos sitúa en "los tres meses más trepidantes en seguridad informática de los últimos años".

En este contexto, la demanda de profesionales en ciberseguridad aumenta dramáticamente para enfrentar los retos crecientes. De acuerdo con la asociación sin fines de lucro (ISC)[2], para el 2020 se teme que habrá un déficit de profesionales en ciberseguridad de 1.5 millones, lo que implica que muchas organizaciones buscarán contratar de manera externa a los profesionales que hagan falta.

Sin embargo, no solo hacen falta más profesionales en ciberseguridad, sino difundir buenas prácticas de seguridad entre los usuarios del presente. Según una encuesta del Instituto SANS, las amenazas internas son el principal temor de las organizaciones, dado que las personas aún requieren de una comprensión de las amenazas que existen, por ejemplo, en el manejo de contraseñas y el uso de credenciales privilegiadas para mejorar la seguridad de los ambientes en las organizaciones.

A la falta de profesionales y el problema de las amenazas internas se suma una inquietud que quedó manifiesta a partir de ataques como WannaCry y la nueva versión de Petya: la falta de vinculación entre los equipos de TI y los encargados de la seguridad, quienes están alejados por la carencia de procesos adecuados que permitan detectar amenazas. Como se puede apreciar en el artículo "Después de WannaCry", 90% de los ataques utilizan vulnerabilidades comunes que podrían evitarse si se efectuaran actualizaciones de sistemas a tiempo. Esto podría mostrar que no basta con realizar grandes inversiones para mitigar los problemas de ciberseguridad, sino que hace falta invertir en la capacitación del personal para formar un frente sólido ante las amenazas crecientes.

Por estas razones, creemos que la ciberseguridad adquirió mayor relevancia en los equipos de trabajo dedicados a las tecnologías de la información y comunicación, quienes ahora deberán enfrentar el reto de compartir con los usuarios finales la preocupación por cuidar de los recursos informáticos.

UNAM-CERT

.Seguridad Cultura de prevención para TI, revista bimestral, octubre-noviembre 2017 / Certificado de Reserva (en trámite), Certificado de Licitud de Título (en trámite), Certificado de Licitud de Contenido (en trámite), Número ISSN (en trámite), Registro de Marca 1298292 | 1298293 / Universidad Nacional Autónoma de México, Circuito Exterior s/n edificio de la Dirección General de Cómputo y de Tecnologías de Información y Comunicación, Coordinación de Seguridad de la Información, Cd. Universitaria, Coyoacán Ciudad de México, México, C.P. 04510, Teléfono: 56228169

DIRECCIÓN GENERAL DE CÓMPUTO Y DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

DIRECTOR GENERAL
Dr. Felipe Bracho Carpizo

DIRECTOR DE SISTEMAS Y SERVICIOS INSTITUCIONALES
Act. José Fabián Romo Zamudio

COORDINADOR DE SEGURIDAD DE LA INFORMACIÓN/ UNAM-CERT
M. en C. José Roberto Sánchez Soledad

DIRECTORA EDITORIAL
L.A. Célica Martínez Aponte

EDITOR
Raúl Abraham González Ponce

ASISTENTE EDITORIAL
Rocío de Abril Pérez López

ARTE Y DISEÑO
L.D.C.V. Alicia M. Manjarrez Ceron

REVISIÓN DE CONTENIDO
Angie Aguilar Domínguez
Demian Roberto García Velázquez
Manuel Ignacio Quintero Martínez
Roberto Sánchez Soledad
Célica Martínez Aponte
Paulo Santiago de Jesús Contreras Flores

COLABORADORES EN ESTE NÚMERO
Marco Antonio Ruano Muñoz
Said Ramírez Hernández
Camilo Gutiérrez Amaya
Francisco Carlos Martínez Godínez
Miguel Ángel Mendoza
Sergio Anduin Tovar Balderas

Torrents: compartiendo información legítima y también amenazas

Camilo Gutiérrez Amaya

Sin lugar a dudas el uso de torrents es una de las herramientas más populares para compartir información entre los usuarios, pero como muchas tecnologías exitosas y de uso masivo, suele ser aprovechada por atacantes para propagar campañas maliciosas.

Los torrents tienen muchos usos legítimos en varios segmentos e industrias. Los sistemas operativos y el software de código abierto los utilizan para poner a disposición sus nuevas versiones; los *gamers* los ven como su centro de actualización y entretenimiento, mientras que algunos músicos incluso lo usan para hacer llegar su material a sus oyentes.

Sin embargo, su popularidad entre usuarios los convierte un interesante vector de propagación de amenazas para los ciber-criminales. Desde comienzos de 2016, la telemetría de ESET ha detectado casi 15 millones de registros en los que la descarga de código malicioso se relacionada a uno de los clientes punto a punto (P2P) o servicios para compartir archivos más populares.

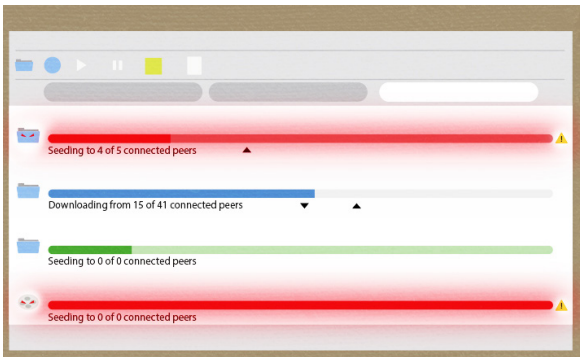
Entendiendo la tecnología de los torrents

Antes de entrar en detalle de la forma en que los torrents son usados en campañas de propagación de amenazas, vamos a explicar brevemente de qué se trata esta tecnología. Torrent es un formato de archivo que almacena los datos necesarios para que una aplicación comparta el contenido a través el protocolo BitTorrent, uno de los más populares dentro de los sistemas de intercambio P2P.

La aplicación utilizada se conoce como cliente torrent. Cuando el usuario tiene instalada dicha aplicación, logra que su dispositivo interprete los datos de los archivos .torrent, puede conectarse a la red P2P con otros usuarios, también es capaz de gestionar la velocidad de transferencia de archivos, realizar descargas múltiples, así como comprobar y montar los archivos y carpetas una vez que la descarga se ha completado.

Compartiendo amenazas a través del intercambio P2P

Al ser una tecnología popular para intercambiar archivos e información entre redes de usuarios, en ocasiones algunos de los archivos descargados también puedan ser una amenaza, ya que se pueden hacer pasar por software, juegos, música o películas populares, pero pueden terminar siendo algo completamente distinto (y a menudo malicioso).



Esto fue lo que hizo el Sathurbot (ESET, 2017a), un código malicioso que infectaba dispositivos a través de archivos que eran descargados por redes P2P, con lo cual dichos sistemas eran añadidos a una botnet, cuya principal actividad consistía en buscar cuentas de administrador de sitios en WordPress. Dentro de las técnicas de propagación de esta amenaza, se aprovechaban las cuentas comprometidas de WordPress para colocar el torrent malicioso en ubicaciones atractivas para usuarios que buscaran información para descargar.

Si el usuario iniciaba la descarga de los archivos, generalmente asociados con películas, obtenía un paquete que contenía un archivo con extensión de video, acompañado por un aparente instalador de códecs y un archivo de texto con explicaciones. En este caso al ejecutar el archivo, era cargada la biblioteca de enlace dinámico (DLL) de Sathurbot.

Pero el caso anterior no ha sido el único relacionado con la descarga de amenazas a través de torrents. A principios de este año, cibercriminales se aprovecharon de redes BitTorrent para distribuir campañas de ransomware como la de Patcher (M.Léveillé , 2017), haciéndose pasar por software legítimo, principalmente Adobe Premiere Pro y Microsoft Office para Mac.

En este caso la amenaza consistía en un único archivo ZIP y si bien el malware no estaba muy bien desarrollado, además de no contar con ningún código para comunicarse con un servidor de comando y control (C&C), la rutina de cifrado utilizada era lo suficientemente efectiva como para evitar que las víctimas accedieran a sus archivos afectados. Además, no se enviaba la clave usada para cifrar los archivos a los operadores del malware y tampoco podrían proveer una clave de descifrado a las víctimas.

No solamente archivos, también clientes torrent son comprometidos

Siguiendo con las amenazas relacionadas, no son solo los archivos de torrents los que pueden ser utilizados con fines maliciosos, ya que ocasionalmente se comprometen los propios clientes de BitTorrent. Por ejemplo, durante el año pasado los usuarios de macOS fueron blanco de este tipo de amenazas cuando fue comprometida una versión de la aplicación Transmission, un cliente de BitTorrent legítimo y muy popular; posteriormente fue utilizado para propagar malware.

El primer ataque se documentó en marzo de 2016 y descargaba el ransomware KeRanger (Stanick), el cual usaba un algoritmo criptográfico prácticamente imposible de romper, y por lo tanto dejaba inaccesible la información de las víctimas. A pesar de la rápida reacción de los desarrolladores de Transmission, que eliminaron la versión troyanizada del programa apenas unas horas después de que apareciera en el sitio oficial, hubo miles de víctimas en todo el mundo.

Otro caso se dio con la variante del malware llamado OSX/Keydnap (ESET, 2017b) que se propagó usando una versión alterada del software Transmission, insertando un *backdoor* permanente en los dispositivos infectados y robando credenciales almacenadas en la aplicación Keychain. Sin duda, el software utilizado para la transferencia de archivos, también puede ser comprometido, lo que representa otro riesgo de seguridad asociado a esta tecnología.

Engaños que aprovechan la popularidad de los torrents

Además de las campañas anteriores, hemos visto algunas más que aprovechan la popularidad del uso de torrents para sacar ventaja de diferentes situaciones que suelen llamar la atención utilizando técnicas de Ingeniería Social, específicamente para la descarga de material malicioso a través de engaños.

Por ejemplo, antes de que saliera a la venta la versión en Blu Ray de uno de los últimos episodios de la saga Star Wars, se anunció que se había filtrado en Internet una copia de la producción. Desde ese momento muchos usuarios se volcaron a descargar, principalmente por redes P2P, la copia ilegal de la película (Gutiérrrez, 2017).

Aprovechando lo anterior, se observaron varias campañas maliciosas que dentro de las búsquedas que hacían los usuarios para obtener la película a través de sitios de torrents, no los dirigían a este tipo de contenido, sino a la descarga de otras aplicaciones maliciosas, suplantando la identidad de sitios conocidos para el intercambio a través de redes P2P.

En estos sitios, se instaba al usuario para la descarga de un falso códec y ejecutarlo. Este software únicamente mostraba una ventana con términos y condiciones de uso, pero una vez que el proceso continuaba, no sucedía nada más de forma visible en su máquina. Sin embargo, al analizar las capturas de tráfico en la máquina, era posible verificar que este supuesto códec en realidad estaba enviando información del usuario a un servidor.

En realidad, se trataba de una amenaza de las que denominamos Potencialmente Peligrosas (PUA) (ESET, 2017c), ya que si bien el usuario está aceptando unas condiciones y términos de uso antes del proceso, el resultado final no corresponde con lo que espera.

Lecciones aprendidas: piensa antes de descargar

Lo anterior son solo algunos ejemplos de distintas campañas de propagación de amenazas que se valen de la popularidad de los torrent para poner en práctica diferentes tipos de vectores de propagación, buscando llegar a grandes cantidades de usuarios, para infectarlos con malware u obtener acceso a sus computadoras y usarlas con fines maliciosos.

Es importante destacar que el uso de esta tecnología no necesariamente puede mostrarse como algo peligroso, pero si se emplea la descarga de torrents, es importante conocer que los atacantes lo usan frecuentemente como medio para propagar sus amenazas. Al mismo tiempo, es importante tomar en cuenta estos posibles escenarios de riesgo y prestar mucha atención antes de descargar.

Sin duda, conocer estas amenazas es el primer paso para evadirlas, así como evitar caer en los engaños que suelen emplear los atacantes, que se valen de esta herramienta para intentar afectar a los usuarios. La aplicación de buenas prácticas, el uso de la tecnología de seguridad y la concientización nos permitirá disfrutar de la tecnología en un ambiente cada vez más seguro.

Referencias

ESET Research. (2017a). Sathurbot: ataque distribuido apunta a contraseñas de WordPress. WeLiveSecurity en español. Recuperado el 8 de agosto de 2017, de https://www.welivesecurity.com/la-es/2017/04/06/sathurbot-ataque-contrasenas-wordpress/

ESET Research. (2017b). OSX/Keydnap se propaga en una aplicación firmada de Transmission. WeLiveSecurity en español. Recuperado el 8 de agosto de 2017, de https://www.welivesecurity.com/la-es/2016/08/30/osxkeydnap-aplicacion-firmada-transmission/

ESET Research. (2017c). Glosario. WeLiveSecurity en español. Recuperado el 8 de agosto de 2017, de https://www.welivesecurity.com/la-es/glosario/#G

Gutiérrez, C. (2017). Historias de engaños en la web: Star Wars y falsos torrents. WeLiveSecurity en español. Recuperado el 8 de agosto de 2017, de https://www.welivesecurity.com/la-es/2016/04/01/star-wars-falsos-torrents/

M.Léveillé, M. (2017). Nuevo ransomware criptográfico afecta a macOS. WeLiveSecurity en español. Recuperado el 8 de agosto de 2017, de: https://www.welivesecurity.com/la-es/2017/02/22/nuevo-ransomware-criptografico-afecta-macos/

Stanick, P. (2017). KeRanger: nuevo ransomware para Mac se propaga vía Transmission. WeLiveSecurity en español. Recuperado el 8 de agosto de 2017, de https://www.welivesecurity.com/la-es/2016/03/07/keranger-ransomware-mac-transmission/

Si quieres saber más, consulta:

- Tips de seguridad para el cómputo en nube
- Piensa antes de copiar software
- Copyright prevent copy: protocolo BPS

Camilo Gutiérrez Amaya

Se desempeña actualmente como Head of Awareness & Research, liderando el equipo de investigadores de ESET Latinoamérica. Es Ingeniero Electrónico egresado de la Universidad de Antioquia e Ingeniero Administrador graduado de la Universidad Nacional de Colombia.

Cuenta con una especialización en Sistemas de la Información en la Universidad EAFIT y actualmente opta al título de Magister en Data Mining en la Universidad de Buenos Aires, Argentina.

Anteriormente se desempeñó como Coordinador de Riesgo Operativo para una importante compañía de financiamiento y se ha desarrollado modelando y generando sistemas de información.

Ransomware, ¿quién secuestra nuestra información?

Miguel Ángel Mendoza López

En mayo pasado una noticia recorrió el mundo entero. Por primera vez, una nota relacionada con la ciberseguridad acaparó los titulares, debido a un código malicioso conocido como *WannaCry*. Se trataba de otra familia de ransomware. Aunque el secuestro y la extorsión en el ámbito digital a través del software malicioso no es un tema nuevo, este *malware* contaba con la característica de gusano informático, es decir, la facultad de propagarse de forma automática a través de la explotación de vulnerabilidades en el software, algo que podemos denominar *ransomworm*.

Los propósitos por los cuales se desarrollan y propagan los códigos maliciosos han cambiado; desde modificar la funcionalidad de los sistemas y dar reconocimiento a sus creadores, hasta causar daños, corromper la información y conseguir algún otro tipo de beneficio para sus desarrolladores (principalmente ganancias económicas) en un periodo cada vez menor. En esta publicación haremos un recuento de la evolución del ransomware, desde sus primeras versiones hasta casos más recientes y los pronósticos relacionados con esta amenaza informática.

El inicio del secuestro de información

Mucho se ha hablado de las distintas campañas de propagación a nivel global. Aunque no se trata de una idea nueva, el secuestro de la información ha tomado relevancia debido al impacto que ha

representado para los usuarios y empresas que se han visto afectadas negativamente. Los primeros casos de ransomware se remontan a 1989, cuando apareció el troyano PC Cyborg, un programa que ocultaba los directorios y cifraba los nombres de los archivos de la unidad de almacenamiento. Posteriormente solicitaba al usuario "renovar su licencia" con un pago en dólares. Su propagación se presentó principalmente en Europa y Estados Unidos.

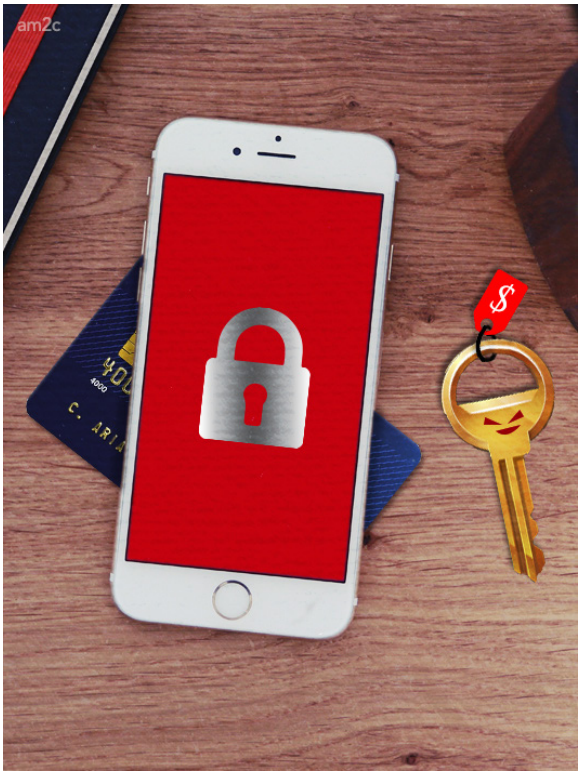
En los siguientes años se identificaron nuevas versiones de programas que buscaban extorsionar a los usuarios, que a diferencia del cifrado simétrico de PC Cyborg, utilizaban algoritmos de cifrado asimétrico con claves cada vez de mayor tamaño. Por ejemplo, en 2005 se conoció GPCoder y, más tarde, sus variantes, que luego de cifrar archivos con extensiones específicas pedía un pago como rescate de la información codificada.

Bloqueo de pantalla, nuevas variantes del ransomware

Eventualmente, aparecieron más códigos maliciosos que funcionaban bajo el principio de la inaccesibilidad a la información, a partir de bloquear los sistemas. Estas variantes son las denominadas LockScreen, que en lugar de modificar los archivos mediante el cifrado, se enfocaban en bloquear el acceso al equipo y la información.

Dentro de esta categoría aparece Winlock, programa malicioso que se conoció en 2010 y que luego de infectar el equipo, lo bloqueaba desplegando un mensaje en la pantalla, al tiempo que se demandaba un pago. Para obtener el código de desbloqueo, el usuario afectado debía enviar un mensaje SMS con un costo aproximado de 10 dólares.

Bajo este mismo principio, en 2012 se conoció a Reveton, el denominado "virus de la policía" que bloqueaba el acceso al sistema del usuario afectado. El programa malicioso permitía mostrar un falso mensaje supuestamente del cuerpo policiaco del país donde se propagaba la amenaza, que indicaba al usuario haber infringido una ley, por lo que debía pagar una "multa" para restaurar el acceso normal.



Aumento de la cantidad y complejidad del ransomware

En años recientes, comenzó a observarse la proliferación de los códigos maliciosos creados de forma específica para generar ganancias económicas a sus desarrolladores. El crecimiento es tal que diariamente los Laboratorios de ESET a nivel mundial reciben alrededor de 200 mil nuevas variantes. El aumento puede identificarse en tres variables: cantidad, complejidad y diversidad.

Por ello, han aparecido nuevas oleadas de programas maliciosos que operan bajo el principio del cifrado de la información, también conocido como *criptoransomware* o FileCoders, ya que su principal propósito es codificar los archivos mediante algoritmos de cifrado. Para 2013 conocimos la relevancia de CryptoLocker, en gran medida

debido a la cantidad de infecciones generadas en distintos países. Entre sus principales características se encuentra el cifrado a través de algoritmos de clave pública, enfocado únicamente de algunos tipos de extensiones de archivos y el uso de comunicaciones con el comando y control (C&C) del atacante a través de la red anónima Tor.

Casi de manera simultánea, hizo su aparición CryptoWall (una variante de Cryptolocker), que logró superar a su predecesor en el número de infecciones, en cierta medida, debido a los vectores de ataque empleados: desde *exploit kits* en navegadores y ataques *drive-by-download*, hasta el más común mediante archivos maliciosos adjuntos en correos electrónicos.

A principios de 2015 se identificaron nuevas campañas con la aparición de CTB-Locker, mismo que podía ser descargado al equipo de la víctima utilizando un TrojanDownloader; el término *downloader* se aplica para programas maliciosos cuyo propósito (generalmente único) es descargar y ejecutar software malicioso adicional e infectar un sistema. Entre sus distintas versiones, una estaba enfocada a los usuarios hispanohablantes, con mensajes escritos completamente en español.

Entre sus peculiaridades, el malware también conocido como Citrioni cifraba los archivos en el disco, unidades extraíbles y unidades de red, utilizando un algoritmo de curva elíptica no reversible para el cifrado de la información. Para mantener el anonimato del creador, se conecta a través de Tor y solicita un rescate en *bitcoins*, una de las criptomonedas más conocidas.

Posteriormente, durante 2016 nuevas familias de ransomware comenzaron a propagarse por Latinoamérica, tal es el caso de Cerber, Locky o TeslaCrypt, con importantes repercusiones en las empresas y usuarios de la región. Durante 2017, el código malicioso de mayor renombre sin duda ha sido WannaCry, también conocido como WannaCryptor que, a diferencia de sus predecesores, se puede propagar automáticamente a través de la explotación de vulnerabilidades en el sistema operativo, lo que aumenta su potencial de infección.

El caso más reciente fue el brote del malware Diskcoder.C, también conocido como ExPetr, PetrWrap, Petya, o NotPetya, el cual tiene como objetivo sobrescribir los archivos, sin cobrar el dinero del rescate. De hecho, no brinda información de contacto de los cibercriminales ni puede proveer una clave de descifrado. Por ello, las nuevas familias de malware son diseñadas para causar daño, corromper la información y afectar de forma negativa a objetivos de interés y con un alcance global.

La diversidad del ransomware en aumento

En los últimos años, hemos visto el desarrollo de una mayor cantidad de ransomware, con mecanismos cada vez más complejos, que hacen casi imposible la recuperación la información, ya que los intentos por obtener las claves de descifrado requieren de mucho tiempo y procesamiento, debido que los algoritmos de cifrado tienen como base la resolución de problemas matemáticos complejos.

Por ello, la última alternativa que tienen las víctimas de ransomware es el pago del rescate al cibercriminal, sin embargo no se recomienda por dos razones principales. En primer lugar, al realizar el pago del rescate no se tiene garantía ni la certeza de recuperar la información, puesto que es probable que el ciberdelincuente no realice la entrega de las claves de descifrado y por otro lado, con el pago se financia una industria cibercriminal que con más recursos puede generar más amenazas informáticas.

Aunado al crecimiento en la cantidad y complejidad del ransomware, su diversidad también ha ido en aumento. Por ejemplo, en 2014 conocimos el primer caso de malware de la familia FileCoder para Android. SimpLocker apareció en escena; su función consistía en escanear la tarjeta de almacenamiento del dispositivo móvil en busca de archivos con extensiones específicas. Del mismo modo, aparecieron más códigos maliciosos como AndroidLocker, que suplantaba soluciones de seguridad y

aplicaciones legítimas para Android, con el propósito de ganar la confianza de los usuarios.

Además, otras plataformas se han convertido en objetivo de los atacantes. Durante 2015 aparecieron los primeros casos de ransomware diseñado especialmente para sistemas operativos Linux, CTB-Locker o KillDisk. Durante 2016 apareció una muestra de ransomware conocida como KeRanger, un ransomware especialmente diseñado para OS X, así como otras familias enfocadas en macOS, como la familia de ransomware Patcher durante 2017.

¿Estamos ante una amenaza que llegó para quedarse?

Es evidente que la proliferación del ransomware va en aumento y es muy probable que continúe creciendo. Los hechos y los datos nos hacen pensar que estamos ante una amenaza que estará presente en los siguientes años, entre los principales motivos, por las ganancias ilícitas que representa para sus creadores, así como la cantidad de dispositivos y usuarios que podrán verse afectados.

Una tendencia de los últimos meses es el crecimiento de ransomware que tiene como foco el denominado Internet de las cosas (IoT). Distintos dispositivos como relojes o televisores inteligentes son susceptibles de ser afectados por software malicioso de esta naturaleza, en lo que se ha denominado ransomware de las cosas (RoT). Es probable que en el futuro próximo seamos testigos de ataques a dispositivos que se conectan a Internet, incluso se vislumbran nuevos conceptos, como el *jackware*, es decir, el secuestro de automóviles que se conectan a Internet.

Aunque el escenario parece pesimista, sin duda existen cuestiones positivas dentro del conjunto de descalabros. Podemos destacar que la seguridad de la información fue el foco de atención en el orbe, a raíz de estos ataques, lo que debería traducirse es mayores iniciativas de protección en diferentes ámbitos, teniendo como punto de partida la prevención.

Ante este panorama, la ciberseguridad se convierte en un tema cada vez más relevante en distintos ámbitos y niveles, que involucra a la iniciativa privada, los gobiernos, instituciones académicas, y por supuesto, a los usuarios. Las buenas prácticas, la tecnología de protección y la educación en temas seguridad resultan necesarios en la actualidad, todo con un objetivo fundamental: disfrutar de la tecnología en un ambiente cada vez más seguro.

*Este texto es una actualización del artículo "La evolución del *ransomware*: del ochentero PC Cyborg a un servicio en venta", publicado el 21 de agosto de 2015 en https://www.welivesecurity.com/la-es/2015/08/21/evolucion-del-ransomware/

Referencias

Cobb, S. (2017). Jackware: cuando los autos conectados conocen al ransomware. WeLiveSecurity en español. Recuperado el 23 de agosto de 2017, de https://www.welivesecurity.com/la-es/2016/07/21/jackware-autos-conectados-ransomware

Lipovsky, R. (2017). KillDisk apunta a Linux: demanda $250K de rescate pero no descifra los archivos. WeLiveSecurity en español. Recuperado el 24 de agosto de 2017, de https://www.welivesecurity.com/la-es/2017/01/05/killdisk-linux-rescate-no-descifra

Longstaff, T. (1989). Information about the PC CYBORG (AIDS) trojan horse. SecurityFocus. Recuperado el 24 de agosto de 2017, de http://www.securityfocus.com/advisories/700

Mendoza M. (2017). Panorama de ransomware en México tras el impacto de WannaCryptor. WeLiveSecurity en español. Recuperado el 24 de agosto de 2017, de https://www.welivesecurity.com/la-es/2017/07/26/panorama-de-ransomware-mexico/

M.léveillé, M. (2017). Nuevo ransomware criptográfico afecta a macOS. WeLiveSecurity en español. Recuperado el 20 de agosto de 2017, de https://www.welivesecurity.com/la-es/2017/02/22/nuevo-ransomware-criptografico-afecta-macos

Pagnotta, S. (2016). Locky, un ransomware ya presente en Latinoamérica. WeLiveSecurity en español. Recuperado el 24 de agosto de 2017, de https://www.welivesecurity.com/la-es/2016/02/19/locky-nuevo-ransomware-latinoamerica

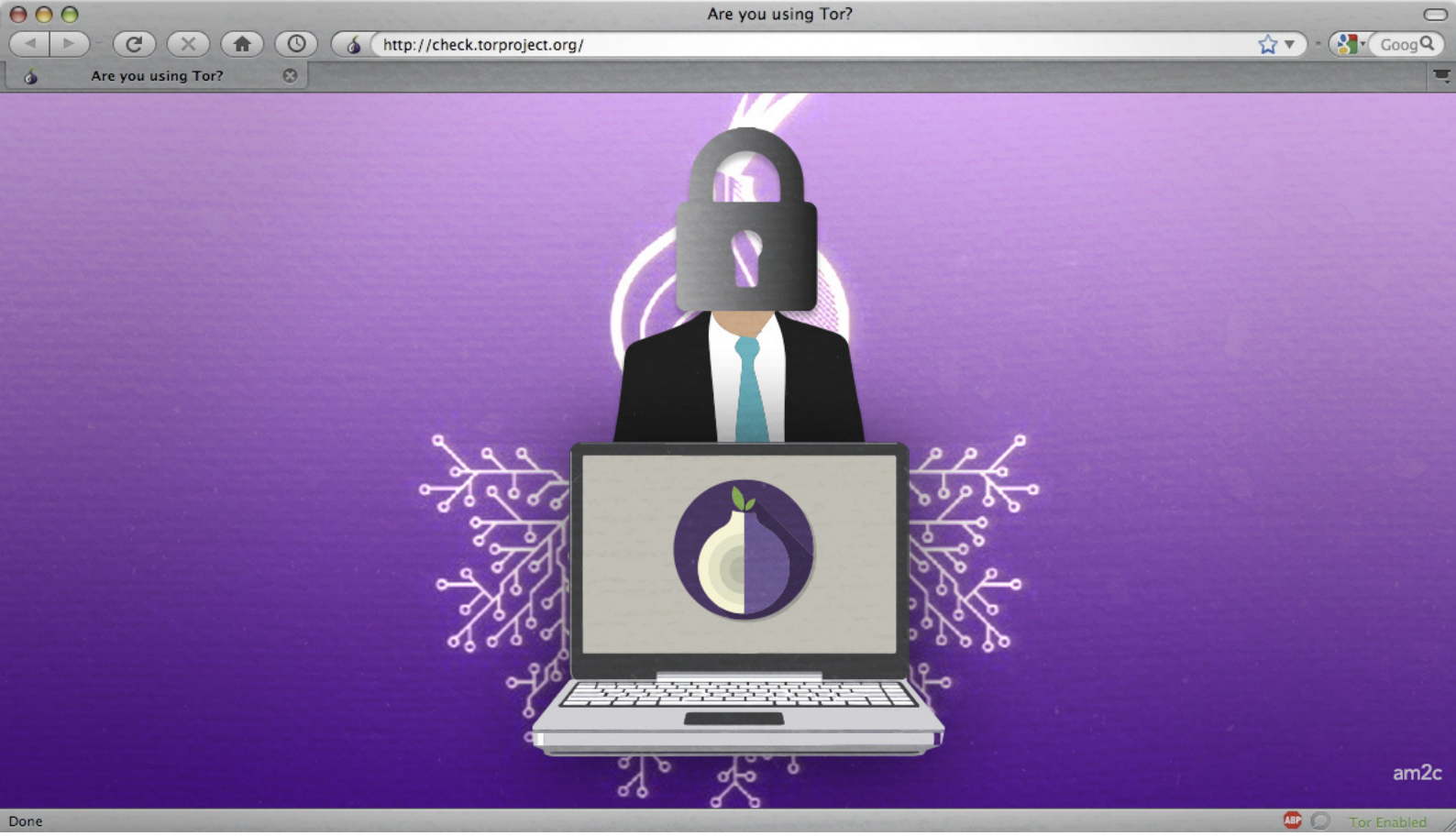
Si quieres saber más, consulta:

- Wannacry: ataque mundial y consideraciones sobre ciberseguridad
- Macro malware, campañas de propagación vigentes en México
- Tendencias de seguridad 2017, ¿estás preparado?

Miguel Ángel Mendoza López

Ingeniero en Computación por la Facultad de Ingeniería de la UNAM, Miguel Ángel Mendoza se desempeña actualmente como Security Researcher en ESET Latinoamérica, compañía dedicada al desarrollo, investigación y comercialización de soluciones de protección antivirus y seguridad informática. Además se desempeña como vocero de ESET Latinoamérica y representa a la empresa en todo tipo de actividades tales como seminarios, conferencias, capacitaciones internas y otros eventos de exposición pública.

Colaboró en la DGCCH de la UNAM, en la Facultad de Ingeniería y formó parte de la Coordinación de Seguridad de la Información/UNAM-CERT en el área de Auditoría y nuevas tecnologías, donde desarrolló actividades de implementación de estándares, mejores prácticas y auditorías de seguridad informática.



La red Tor como elemento de privacidad en nuestras vidas

Marco Antonio Ruano Muñoz

Con el incremento de servicios en la nube, el abaratamiento de dispositivos tecnológicos y la reducción de su tamaño, se ha elevado de forma abrumadora la facilidad para conectarse a Internet y realizar tareas cotidianas, permitiendo comunicarse con personas al otro lado del planeta en instantes, realizar operaciones bancarias sin necesidad de hacer una fila, enviar importantes correos con información sensible o hacer las compras del supermercado desde el hogar. Sin embargo, cuando una persona aprende a utilizar una de estas plataformas no recibe un curso enfocado a la seguridad y protección de su información, por tanto, es de suma importancia considerar aspectos como la privacidad y el anonimato a la hora de sumergirnos en la red.

El navegdaro Tor

Tor es una herramienta utilizada en todo el mundo por características que la hacen particularmente atractiva para aquellas personas que deseen "enmascarar" su actividad en línea, así como acceder a ciertas áreas que no se encuentran indexadas por la mayoría de los motores de búsqueda.

Típicamente, la red en la que navega un usuario consiste en una arquitectura cliente-servidor, la cual permite que el navegador (es decir el cliente) haga una petición a un servidor solicitando cierta información, como puede ser una página web, una imagen, video, etcétera, y el servidor devolverá una respuesta por medio

del protocolo HTTP con el resultado, siendo este visualizado en el navegador.

La red Tor (The Onion Routing) funciona de forma análoga. Sin embargo, la gran diferencia radica en que esta es una red distribuida, es decir, está compuesta por varios nodos además del cliente y el servidor con el que desea comunicarse. Estos nodos conformados por voluntarios que aportan una porción de su ancho de banda para permitir el funcionamiento brindan la posibilidad de navegar por Internet de forma anónima, ya que cuando un usuario envía datos para establecer una comunicación, esta información es cifrada con 3 llaves distintas, de modo que el primer nodo únicamente es capaz de descifrar una de estas llaves para reenviar la información al segundo nodo, que a su vez removerá una "capa" más del cifrado y de nuevo trasladará el contenido al último nodo (nodo de salida), el cual descifra la última llave y redirige la petición hacia el servidor objetivo.

Cada uno de estos nodos cuenta con la localización de los puntos más cercanos, es decir, de donde viene la información y a donde se dirige, y este camino que se recorre se configura de forma aleatoria constantemente, lo cual dificulta el análisis de tráfico proveniente hacia algún usuario.

Este proyecto de software libre, entre algunas otras funcionalidades desarrolladas, cuenta con un navegador listo para trabajar con esta red, el cual trabaja con el protocolo HTTPS que asegura la comunicación de principio a fin. Sin embargo, vale la pena mencionar que Tor no cuenta con cifrado de extremo a extremo, por lo que, si no se usa HTTPS, el nodo de salida es un punto vulnerable en el cual se puede perder el anonimato deseado.

En la figura 1 podemos observar el funcionamiento de la red Tor y el uso de HTTPS, en donde un usuario intenta acceder a un sitio, ingresando sus credenciales para autenticarse, y enviando cierta información, así como su localización gracias a la dirección IP. Suponiendo que alguna persona o incluso el proveedor de servicios de Internet (ISP en el recuadro rojo, que se encarga de proveer a personas y compañías la posibilidad de conectarse a Internet) monitorea el tráfico proveniente de la red del usuario, únicamente podrán revelar su localización. Para hacerlo requieren de ciertos permisos y procesos legales interpretados por abogados (icono rosa en la figura 1) y autoridades (icono azul). El primer nodo de Tor solo sabe de dónde proviene la información, pero no tiene acceso a esta, ni sabe cuál es el destino; el segundo nodo no cuenta con información alguna de la petición, y solo el nodo de salida conocerá el sitio al que se intenta acceder. Mientras que, del lado del servidor (interpretado en el recuadro negro), al recibir los datos no tendrá conocimiento de dónde proviene la petición gracias al funcionamiento de la red.

Por otro lado, resulta contraproducente acceder a sitios que solicitan al usuario ingresar cierta información para identificarse, como su nombre, correo electrónico, números de tarjetas bancarias, etcétera, y se perderá la dosis de anonimidad buscada.

Podemos también observar las figuras en azul que representan a organizaciones de seguridad nacional, típicamente agencias del gobierno, las cuales monitorean este tipo de infraestructura de forma periódica, debido al gran número de actividades criminales que se llevan a cabo a costa del anonimato que da la red.

Este esquema realizado por la Electronic Frontier Foundation, organización sin fines de lucro y cuyo objetivo es defender la libertad de expresión en el mundo digital, pretende mostrar que Tor por su cuenta no es perfecto, y solo garantiza anonimidad cuando se utiliza HTTPS.

A diferencia de otros navegadores que cuentan con una configuración predeterminada que permite la recolección y envío de cierta información sobre el usuario y su actividad (a menos que sean desactivadas dichas características manualmen-

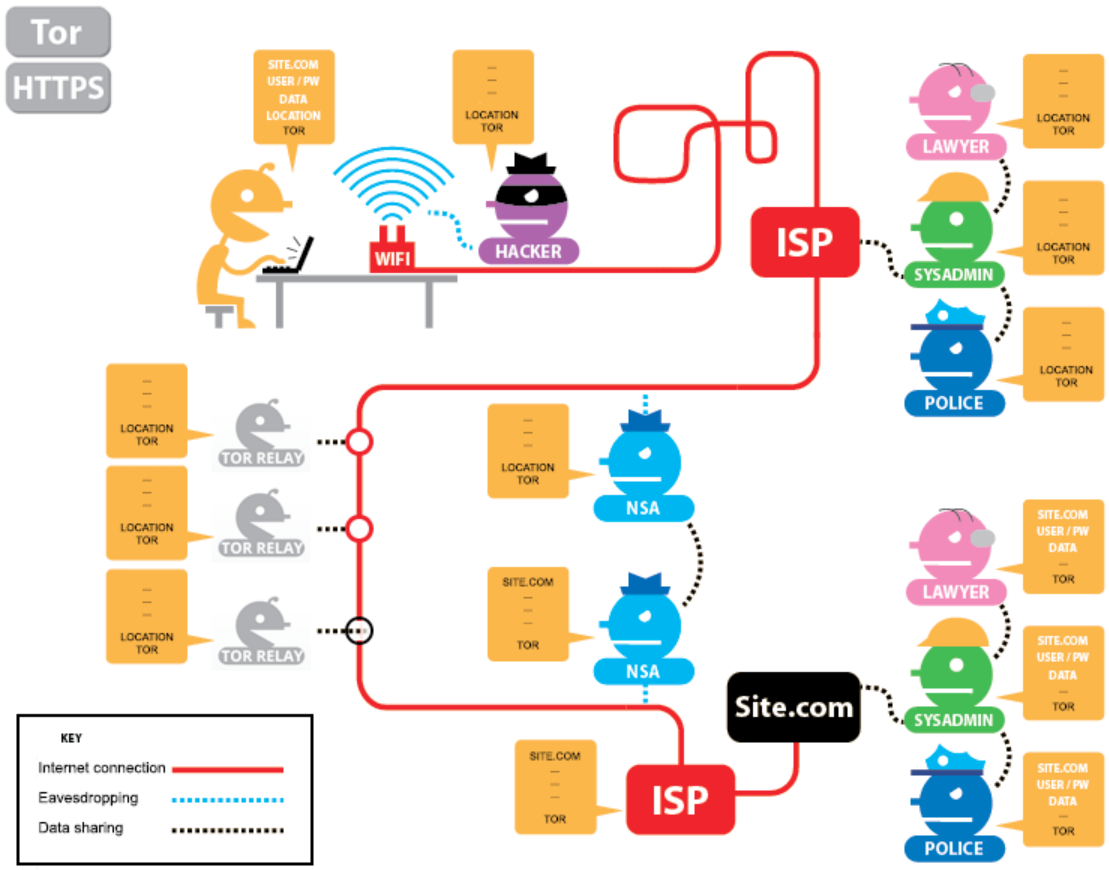


Figura 1

te cuando es posible), el navegador Tor promueve su uso advirtiendo sobre ciertos hábitos que se suelen arraigar, los cuales pueden ser inconvenientes para el objetivo esperado de la red, por ejemplo: compartir archivos mediante Torrent, instalar o activar *plugins* en el navegador, no usar el protocolo HTTPS en sitios web, o abrir documentos descargados por medio de la red Tor mientras se encuentre en línea, por mencionar algunos.

Incluso, ya hay disponible una versión para móviles con sistema operativo Android, y no es para menos, ya que "los dispositivos móviles se utilizan más que las computadoras tradicionales para búsquedas en la Web" (Gibbs, 2016). Esta herramienta llamada Orbot, permite utilizar un proxy local inmerso en la red Tor, y también brinda la habilidad de cifrar la información saliente del *smartphone* o *tablet* e incluso de otras aplicaciones instaladas compatibles.

Por supuesto al pasar la información por una serie de nodos en una red distribuida, es claro que la velocidad no será la misma que al navegar por Internet de forma tradicional, ya que en vez de seguir una ruta directa el tráfico se tiene que desviar hacia los nodos intermediarios, por lo que no es recomendable para algunas tareas cuya eficiencia dependa de la velocidad, como el *streaming*.

Otra desventaja es que algunos proveedores de Internet bloquean nodos de la red Tor, debido a la presión que ejercen los gobiernos de algunos países, por ejemplo, China y Rusia, quienes no están de acuerdo con su uso, debido a la complejidad que implica para sus organizaciones de inteligencia al monitorear a usuarios que pueden hacer uso de la red para actividades

delictivas. Este hecho puede dificultar conectarse a ciertos sitios al estar conectado a la red.

Afortunadamente, hay nodos distribuidos por muchos países que no cuentan con este tipo de políticas, ya que su uso no representa ningún tipo de problema, siempre y cuando no se realicen actividades ilegales.

Conclusiones

Claramente, si una herramienta resulta benéfica para incrementar el nivel de privacidad en línea, la combinación con otras más, como el sistema operativo Tails, servicios de mensajería como Tor Messenger, el uso de redes virtuales privadas (VPN), entre otras, puede ofrecer una solución que, sumada con un uso correcto, responsable y seguro, significará un buen escudo para proteger la información de cada persona.

Sin embargo, la red Tor no solo consiste únicamente en un medio para mantener las comunicaciones privadas, sino también funge como un acto de colaboración entre personas en muchos países que están dispuestos a ceder una porción de su ancho de banda para mantener esta red activa y que todos puedan ser partícipes de ella.

¿Cómo se puede colaborar? Una forma de fortalecer la red es aumentar el número de nodos, es decir ser partícipe de la misma, ya que, a mayor número de nodos, incrementará la disponibilidad de conexiones posible y la secuencia de los tres posibles nodos a seleccionar para una conexión resultará más cambiante, añadiendo complejidad a un posible análisis estadístico que permita conocer información sobre un usuario.

Referencias

Caddy, B. (2017). Google tracks everything you do: here's how to delete it. Recuperado el 28 de julio de 2017, de http://www.wired.co.uk/article/google-history-search-tracking-data-how-to-delete

Electronic Frontier Foundation. (s/f). How HTTPS and Tor Work Together to Protect Your Anonymity and Privacy. Recuperado el 28 de julio de 2017, de https://www.eff.org/pages/tor-and-https

Gibbs, S. (2016). Mobile web browsing overtakes desktop for the first time. Recuperado el 28 de julio de 2017, de https://www.theguardian.com/technology/2016/nov/02/mobile-web-browsing-desktop-smartphones-tablets

How HTTPS and Tor Work together to Protect Your Anonymity and Privacy. (2017). Recuperado el 28 de julio de 2017, de https://www.eff.org/es/pages/tor-and-https

Orbot: Tor for Andorid. (2017). Recuperado el 28 de julio de 2017, de https://www.torproject.org/docs/android.html.en

TOR Download. (2017). Want Tor to really work? Recuperado el 28 de julio de 2017, de https://www.torproject.org/download/download-easy.html.en#warning

Este artículo se desarrolla vinculado con el proyecto PE102718 PAPIME/DGAPA/UNAM.

Si quieres saber más, consulta:

- Mitos y realidades de la Internet profunda.
- El cifrado web (SSL/TLS)
- Ningún navegador es seguro

Marco Antonio Ruano Muñoz

Es estudiante de la carrera de Ingeniería en Computación en la Facultad de Ingeniería de la Universidad Nacional Autónoma de México (UNAM). Fue analista de información y programador

de bases de datos en International Data Corporation (IDC).

Posteriormente se desempeñó como Technical Account Manager de empresas públicas y privadas en Microsoft México y actualmente labora como gerente de producto, desarrollador y administrador de bases de datos en la misma compañía.

Es miembro del Laboratorio de Investigación y Desarrollo de Software Libre (LIDSOL) en la Facultad de Ingeniería.

La vida después de WannaCry

Francisco Carlos Martínez Godínez

"Como en la mayoría de incidentes de seguridad, este no es un problema tecnológico, es un problema de procesos y de gente" (Litan, 2017).

Es cada vez más común ver a organizaciones invertir en dispositivos y herramientas de seguridad, adquirir soluciones para mantener a la empresa segura, y diseñar campañas informativas y de concientización. Lo que ocurrió en mayo de 2017 significó una sacudida mayor para los programas de seguridad de la información en compañías de todos los tamaños alrededor del mundo, y reveló una verdad irrefutable: las organizaciones no están preparadas.

Se trató de un incidente de seguridad como no se había visto antes, al menos en cuanto a impacto y alcance, y deja varias preguntas en el aire que deberán ser respondidas en varios niveles dentro de las organizaciones. ¿Cómo una vulnerabilidad conocida pudo ser aprovechada a estos niveles? ¿Pudo hacerse algo más? ¿Dónde se está fallando? Y lo más importante, ¿qué lecciones se aprendieron?

El mundo secuestrado

WannaCry es un ransomware que explota la vulnerabilidad de SMB (MS17-010), la cual es considerada crítica por Microsoft, y afecta a todas las versiones de los sistemas operativos Windows. Este tipo de malware no es nuevo, de hecho el secuestro de equipos se ha vuelto cada vez más

frecuente. Sin embargo, la aparición de WannaCry representa un evento importante en el mundo de la seguridad a nivel global, pues lo que se presenció con este malware no tiene precedentes principalmente por tres factores.

Primero, el alcance. Cinco continentes, más de 179 países y más de 300,000 equipos infectados (Tovar, González, y García, 2017); 16 hospitales en Reino Unido, Renault, FedEx, el operador español de telefonía móvil Telefónica, la estación de trenes alemana en Frankfurt, el ministerio interior y el banco Sberbank rusos, son solo algunas de las instituciones que fueron golpeadas por este malware (Times Media, 2017). El ataque, cuyos primeros indicios fueron detectados en España y Reino Unido, se propagó en minutos alrededor del mundo.

Segundo, la arquitectura del ataque. Wannacry está formado por dos componentes clave: un gusano y un ransomware. El gusano utiliza un *exploit* que aprovecha una vulnerabilidad en SMB y se propaga sin la necesidad de la interacción de usuarios (Williams, 2017).

Tercero, la utilización de una herramienta creada originalmente por una institución gubernamental. Resulta interesante el hecho de que WannaCry utiliza para propagarse SMBv1 Eternalblue, un exploit que, se asume, fue robado a la Agencia de Seguridad Nacional de los Estados Unidos (NSA, por sus siglas en inglés), y el cual se hizo público apenas un mes antes de la propagación del ransomware (Williams, 2017). Eternalblue implanta una pieza específica de *shellcode* llamada Doublepulsar, la cual tiene la particularidad de ejecutarse en el espacio de kernel. Eternalblue forma parte del grupo de herramientas de *hacking* desarrollado por la NSA y que fue filtrado por el grupo de hackers Shadow Brokers (Ullrich, 2017). Existen fuentes que apuntan a la existencia de este grupo con los servicios de inteligencia rusos, lo que resulta interesante y paradójico, siendo que instituciones rusas fueron de las primeras afectadas tras este ataque (Price, 2016).

Una verdad incómoda

Existe una preocupación detrás de ataques como WannaCry, y es el hecho de que se ha dejado en evidencia una profunda desconexión entre el trabajo realizado por los equipos de TI, encargados de la operación, y los de seguridad, encargados de prevenir ataques contra la organización, así como la falta de procesos adecuados en ambas partes. De acuerdo con Avivah Litan, analista de Gartner, más del 90% de los ataques utilizan vulnerabilidades comunes y que pueden ser prevenidos manteniendo los sistemas actualizados, lo que indica que los procesos, como el de la instalación de actualizaciones, están fallando (Litan, 2017).

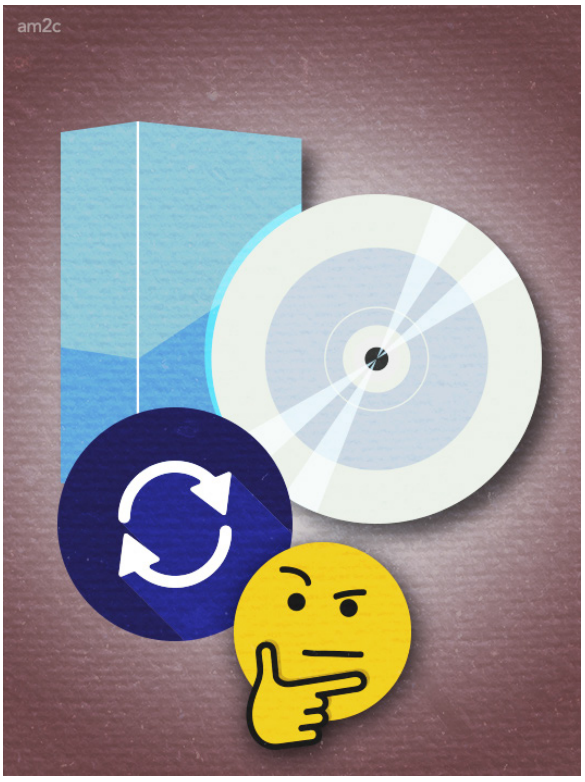
En el caso de WannaCry, las áreas de seguridad de las compañías debieron tener una visibilidad mínima de los sistemas vulnerables y por lo menos sugerir alguna acción acorde con el nivel de la amenaza. Sin embargo, es indudable que los encargados de la gestión de actualizaciones y la instalación de las mismas son las áreas operativas. Falta de seriedad o conocimiento respecto a la amenaza o falta de mecanismos y recursos para mitigarla son algunos de los posibles factores que desembocaron en el resultado ya conocido. La forma de enfrentar un incidente de seguridad debe estar soportada por procesos sólidos, y es ahí donde se están encontrando carencias. Se sigue invirtiendo todo tipo de recursos en cubrir necesidades tecnológicas olvidando que el eslabón más débil de la cadena sigue siendo las personas. Sin un plan de acción adecuado dominado por todos los involucrados, inevitablemente se volverán a cometer los mismos errores.

¿Existe un plan B?

Si la falta de actualizaciones fue lo que abrió la puerta a WannaCry, ¿por qué no simplemente actualizarlo todo? ¿Por qué no deshacerse de una vez por todas de sistemas con Windows XP y/o mantener actualizados sistemas operativos y aplicaciones en cuanto nuevas actualizaciones

son liberadas? Suena bien, pero el mundo real es mucho más complejo que eso. Muchas veces sistemas y aplicaciones no pueden ser actualizados sino hasta después de meses debido a la propia demanda de la operación, y existe infraestructura crítica que no puede ser ni actualizada ni migrada a nuevas versiones simplemente porque la interrupción del servicio que brinda es impensable, y tendría un impacto mayor en la salud, las finanzas o la seguridad de una organización o incluso de una nación entera.

Si la remediación no puede ocurrir por medio de actualizaciones, entonces, ¿no hay nada por hacer? Anton Chuvakin, analista de Gartner, señala que "si las organizaciones no pueden corregir el problema y no pueden aceptar el riesgo, ¿por qué no mitigan más? Generalmente porque el mitigar requiere controles y los controles cuestan dinero y/o tiempo" (Chuvakin, 2017). Así que, ¿cómo mitigar? ¿Cómo mantener seguros sistemas obsoletos y que no pueden ser actualizados? Ese es el reto. En ese sentido, el establecimiento de controles compensatorios, como el deshabilitar servicios, limitar el acceso a la red, endurecer configuraciones o implementar controles a nivel de red, de host o de aplicación, pueden ayudar a reducir el riesgo inherente a sistemas que no pueden ser actualizados (Chuvakin, 2013).



Conclusiones

Meses han pasado desde la aparición de WannaCry y aún parece poco tiempo para saber qué lecciones se aprendieron. Un mes después de este ataque, apareció un nuevo ransomware conocido como NotPetya, una variante del malware Petya, el cual aprovechaba la misma vulnerabilidad que WannaCry para su propagación, sin embargo, el impacto y los tiempos de respuesta ante este incidente fueron mucho menores. A primera vista, este hecho no representa una mejora significativa en la forma en que se afrontan incidentes de seguridad, ya que las compañías estaban preparadas para un ataque con esas características específicas. Sin embargo, este hecho parece demostrar que una vez que se cuentan con planes y procesos adecuados, el impacto y los riesgos pueden ser disminuidos. Los niveles de sofisticación y alcance de los ataques está creciendo día con día, y este crecimiento no va a detenerse. El siguiente gran ataque está gestándose en estos momentos en algún lugar del mundo y las organizaciones deberán estar preparadas, si es que algo se ha aprendido.

Referencias

Chuvakin, A. (2017). WannaCry or Useful Reminders of the Realities of Vulnerability Management. Gartner. Recuperado el 14 de agosto de 2017, de http://blogs.gartner.com/anton-chuvakin/2017/05/18/wannacry-or-useful-reminders-of-the-realities-of-vulnerability-management/

Chuvakin, A. (2013). Cannot Patch? Compensate, Mitigate, Terminate! Gartner. Recuperado el 14 de agosto de 2017, de http://blogs.gartner.com/anton-chuvakin/2013/10/28/cannot-patch-compensate-mitigate-terminate/

Litan, A. (28 de junio de 2017). Wannacry and Petya point to dangerous disconnects between IT operations and security. Gartner. Recuperado el 14 de agosto de 2017, de http://

blogs.gartner.com/avivah-litan/2017/06/28/wannacry-and-petya-ransomware-point-to-dangerous-disconnects-between-it-operations-and-security/

Price, R. (16 de agosto de 2016). EDWARD SNOWDEN: Russia might have leaked alleged NSA cyberweapons as a 'warning'. Business Insider Deutschland. Recuperado el 14 de agosto de 2017, de http://www.businessinsider.de/edward-snowden-shadow-brokers-russia-leaked-nsa-equation-group-files-warning-dnc-hacking-2016-8

Times Media (6 de mayo de 2017). Infographic: The impact of WannaCry in numbers. Recuperado el 14 de agosto de 2017, de https://www.businesslive.co.za/fm/fm-fox/numbers/2017-05-26-infographic-the-impact-of-wannacry-in-numbers/

Tovar, S., González, R. y García D. (Junio 2017). Wannacry: Ataque mundial y consideraciones sobre ciberseguridad. Revista .Seguridad Cultura de Prevención para TI . Recuperado el 14 de agosto de 2017, de https://revista.seguridad.unam.mx/numero29/wannacry

Ullrich, J. (15 de mayo de 2017). WannaCry/WannaCrypt Ransomware Summary. SANS Internet Storm Center. Recuperado el 14 de agosto de 2017, de https://isc.sans.edu/forums/diary/ /WannaCryWannaCrypt+Ransomware+Summary/22420

Williams, J. (12 de mayo de 2017). Special Webcast: WannaCry Ransomeware Threat - What we know so far. SANS. Recuperado el 14 de agosto de 2017, de https://www.sans.org/webcasts/special-webcast-wannacry-ransomeware-threat-105160?msc=wannacry

Si quieres saber más:

- Wannacry: ataque mundial y consideraciones sobre ciberseguridad
- Concienciar para prevenir
- Ransomware, ¿quién secuestra nuestra información

Francisco Carlos Martínez Godínez

Es egresado de la Facultad de Ingeniería de la UNAM de la carrera de Ingeniería en Computación, del módulo terminal de Redes y Seguridad. Se desempeñó como Administrador de Servidores Windows en el Departamento de Operación Interna y PKI de la Subdirección de Seguridad de la Información/UNAM-CERT. Formó parte de la Primera Generación del Diplomado de Ciberseguridad impartido por la Facultad de Ingeniería de la UNAM y Mnemo. Actualmente forma parte de Hewlett Packard Enterprise, desempeñándose como Administrador de Active Directory, Servidores Windows e Infraestructura de Correo en el Corporativo Televisa. Cuenta con las certificaciones de Certified Ethical Hacker, GIAC Certified Windows Security Administrator y Microsoft Certified Solutions Expert.

Una contraseña para gobernarlos a todos

Said Ramírez Hernández

Hoy en día, la mayoría de las personas se encuentran registradas en al menos una red social o tiene acceso a una cuenta de correo electrónico. Por esta razón, la mayoría de las aplicaciones y plataformas han decidido integrar el concepto de *single sign on*, el cual es un método utilizado para permitir a los usuarios acceder a múltiples recursos o instancias mediante una sola identificación, que por lo general es un usuario y una contraseña. Este tipo de mecanismos es de gran utilidad debido a que se simplifican los procesos de registro y de autenticación, pues únicamente se debe otorgar autorización a la aplicación y listo.

Sin embargo, ¿alguna vez te has detenido a pensar sobre qué pasaría si un atacante lograra apoderarse de tu usuario y contraseña de Facebook, de Google o cualquier otra de tus redes sociales? La respuesta más obvia sería que tendría la capacidad de vulnerar la privacidad de tus mensajes, notas personales, fotografías y todo tipo de información que tengas almacenada en esa red; incluso también podría dañar tu imagen y reputación. Si tienes cuentas vinculadas el impacto no se queda ahí.

Pensemos por un momento en una compañía de la cual han comprometido sus credenciales de LinkedIn con el objetivo de publicar contenido inapropiado o que va en contra de sus políticas. Si esta cuenta está configurada para publicar automáticamente en Facebook y Twitter, el contenido de dichas publicaciones tendrá

una mayor audiencia, lo cual provocará que el nombre de esta compañía esté en boca de todos, inclusive podrían llegar a perder la confianza de sus clientes, lo que se traduciría en una pérdida económica para la organización.

El punto es que podemos concentrar una cantidad finita de aplicaciones vinculadas con una sola identificación, y eso no tiene nada malo, siempre y cuando se tomen las medidas apropiadas para protegerlas. Tomemos como ejemplo a Facebook; si un atacante se apoderara de tus credenciales, solamente tendría que ir a la sección de Apps dentro de la pestaña de configuración para obtener el listado de aplicaciones que has autorizado, y así poder autenticar en cada una de ellas y causar un daño mucho mayor. Interesante, ¿no? Como J. R. R. Tolkien escribió en sus obras para referirse al "anillo único" y haciendo una analogía con este tema, se podría decir:

"Una contraseña para gobernarlos a todos, una contraseña para encontrarlos, y causarles mucho daño"

Lo ideal sería contar con una contraseña para cada sitio web o aplicación que utilices en tu vida diaria, de esta forma, se minimizaría la superficie de ataque en caso de que la seguridad de tus credenciales se viera comprometida. Actualmente existen un sinfín de gestores de contraseñas, algunos son nativos del sistema operativo como el Keychain de macOS y otros son multiplataforma, como Buttercup, KeePass o 1password por mencionar algunos.

Pero al final estamos cayendo en la misma situación, depositamos todos nuestros accesos en un solo contenedor protegido por una contraseña maestra, una huella dactilar o cualquier otro tipo de elemento biométrico. Hay que recordar que, por definición un sistema no es 100% seguro y siempre existirá una vulnerabilidad asociada con este, imagina por un momento que olvidas la contraseña maestra de tu gestor de contraseña, toda aquella información que hayas almacenado se perderá. También existen las fallas de seguridad asociadas con el desarrollo de software, basta con recordar algunas aplicaciones como LastPass, Keeper Password Manager o Dashlane Password Manager, entre muchas otras, que han sido afectadas por vulnerabilidades que permiten comprometer la seguridad de la información almacenada y "protegida" por ellos.

Es importante mencionar que la mayoría de las plataformas, aplicaciones y servicios que utilizamos día a día, cuentan con un apartado dedicado a la seguridad dentro de sus opciones generales. En la mayoría de ellos se pueden habilitar acciones como el envío de alertas por correo o mensaje de texto ante eventos como inicios de sesión o nuevas autorizaciones o cambios de contraseña. Incluso puedes habilitar un segundo factor de autenticación (2FA) mediante la integración de un tercero como Google Authenticator, Microsoft Authenticathor o Authy por mencionar algunos. Con esta medida de seguridad, además de autenticarte con tu usuario y contraseña en la forma tradicional, tendrás que ingresar un código que se actualiza cada cierta cantidad de segundos (60 segundos es el valor más común).

Desafortunadamente, muchas de estas opciones de seguridad vienen deshabilitadas por defecto y requieren que el usuario le dedique unos minutos para su configuración. Además, atiende estas recomendaciones para mejorar tu seguridad.

- Revisa el apartado de seguridad de todas las aplicaciones y plataformas con las que trabajas en tu vida diaria.
- Recuerda que es importante cambiar tus contraseñas con frecuencia, no compartirlas con los demás, y si por alguna razón lo tienes que hacer, cámbiala inmediatamente después de que la hayan terminado de ocupar.
- No uses palabras que aparezcan en un diccionario o que sean fáciles de adivinar (tu nombre, fecha de nacimiento o aniversario, letras o números consecutivos), no las escribas en un papel y

no las guardes en un archivo de texto plano sin protección en tu computadora, si lo llegas a hacer, recuerda que hay mecanismos para cifrar su contenido como PGP (Pretty Good Privacy).
- Revisa el historial de los dispositivos en los que has iniciado sesión, y si no reconoces alguno, siempre tendrás la opción de forzar el cierre de sesión.

Sin embargo, existe un problema común con el que te puedes enfrentar al momento de habilitar el 2FA y que tiene que ver principalmente cuando se utiliza una aplicación desarrollada por un tercero para acceder a un determinado servicio como el correo electrónico o un dispositivo como una consola de videojuegos o un reproductor de contenidos digitales. Pero no te preocupes, porque siempre podrás generar una "contraseña específica por aplicación" y evitarte este problema, la cual mantiene un nivel alto de seguridad y sin la necesidad de memorizarla.

Recuerda que la seguridad la hacemos todos, no simplifiques el trabajo de los atacantes y protege tu información siempre.

Referencias

Apple. (2017). Uso de contraseñas específicas de la aplicación. Recuperado el 15 de septiembre del 2017 de https://support.apple.com/es-mx/HT204397

Facebook. (2017). Consejos de seguridad. Recuperado el 15 de septiembre del 2017 de https://es-la.facebook.com/help/379220725465972/

Google. (2017a). Aumentar la seguridad de tu cuenta. Recuperado el 15 de septiembre del 2017 de https://support.google.com/accounts/answer/46526?hl=es

Google. (2017b). Acceso mediante la contraseña de la aplicación. Recuperado el 15 de septiembre del 2017 de https://support.google.com/accounts/answer/185833?hl=es-419

LinkedIn. (2017). Recomendaciones de seguridad y privacidad de una cuenta. Recuperado el 15 de septiembre del 2017 de https://www.linkedin.com/help/linkedin/answer/889?lang=es

Microsoft. (2017). Contraseñas de aplicaciones y verificación en dos pasos. Recuperado el 15 de septiembre del 2017 de https://support.microsoft.com/es-mx/help/12409/microsoft-account-app-passwords-two-step-verification

Pontiroli, S. (2013). PGP – Privacidad, seguridad y autenticación fiables para todos. Recuperado el 15 de septiembre del 2017 de https://www.kaspersky.es/blog/pgp-privacidad-seguridad-y-autenticacion-fiables-para-todos/1781/

Twitter. (2017). Consejos de seguridad de la cuenta. Recuperado el 15 de septiembre del 2017 de https://support.twitter.com/articles/349068?lang=es

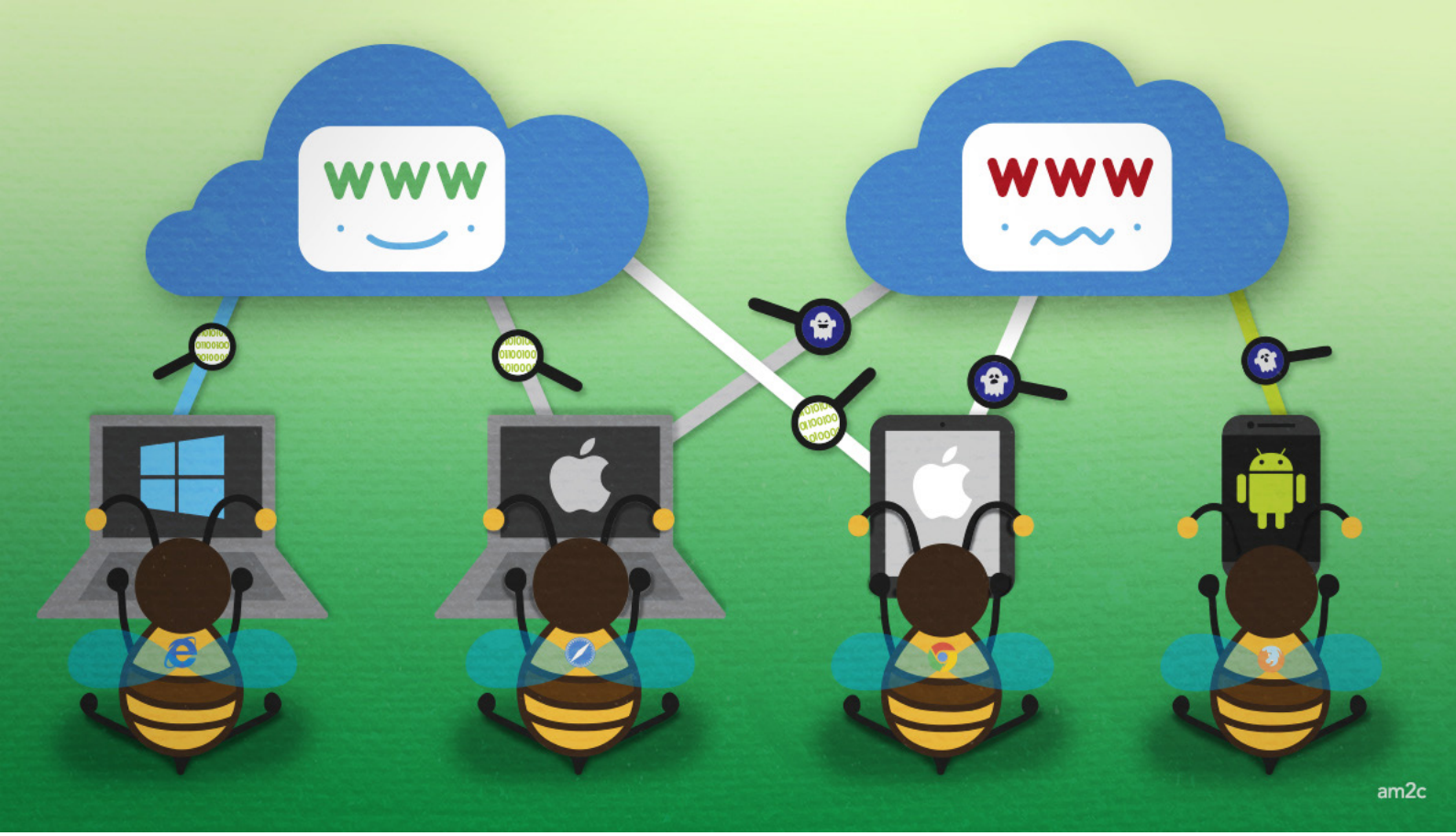
Wei, W. (2017). 9 Popular Password Manager Apps Found Leaking Your Secrets. Recuperado el 15 de septiembre del 2017 de http://thehackernews.com/2017/02/password-manager-apps.html

Si quieres saber más:

- 5 consejos prácticos para mejorar la seguridad en redes sociales
- Redes sociales, entre la ingeniería social y los riesgos a la privacidad

Said Ramírez Hernández

Es egresado de la 7ª generación del plan de becarios de UNAM-CERT. Actualmente es cofundador y consultor de ARSEN – Protegiendo tu información, una consultora especializada en servicios de TI, seguridad informática y privacidad de la información. En su trayectoria como consultor, ha colaborado con tres de los principales bancos en México, bancos emergentes e instituciones financieras, universidades públicas y privadas, proveedores de telecomunicaciones, secretarías de gobierno, empresas del sector privado y con clientes en Estados Unidos, Malasia, Sri Lanka, Noruega y Australia.



Thug Honeyclient: Atrapando sitios web maliciosos

Sergio Anduin Tovar Balderas

Muchas veces hemos escuchado la frase "el usuario es el eslabón más débil de la cadena", lo cual implica múltiples causas que son aprovechadas por los ciberdelincuentes por medio de diferentes técnicas para comprometer los equipos de los usuarios. ¿Imaginas que tu dispositivo podría ser comprometido con tan solo visitar una página web en Internet?, esto se debe a que los ciberdelincuentes comprometen sitios web con poca seguridad e ingresan código malicioso que explota vulnerabilidades en nuestros navegadores. Estos códigos maliciosos forman parte de un paquete de *exploits*.

En este artículo explicaré el panorama general de los paquetes de exploits y una prueba de concepto que consiste en el análisis de tres sitios maliciosos usando Thug. La implementación del cliente honeypot (honeyclient) Thug se puede consultar aquí. Conoce más sobre honeypots en el portal del Proyecto Honeynet UNAM.

En 2016 las aplicaciones más explotadas fueron, en primer lugar, los navegadores web, en segundo lugar, los sistemas operativos Windows, seguido en tercer lugar por los sistemas operativos Android y en cuarto lugar, el conjunto de aplicaciones de Microsoft Office. Además, más de 297 mil usuarios en el mundo fueron atacados por exploits desconocidos (de día cero o conocidos pero muy ofuscados), según el reporte Ataques con exploits: de amenazas diarias a campañas dirigidas de Kaspersky Lab.

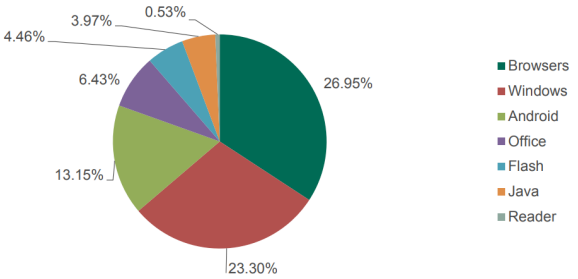


Figura 1. Distribución de usuarios atacados con exploits dirigidos a diferentes aplicaciones en 2016 (Kaspersky Lab)

Una de las principales técnicas utilizadas por los ciberdelincuentes son los ataques del lado del cliente (client side attacks), estos ataques aprovechan vulnerabilidades en las aplicaciones para ejecutar código malicioso (por ejemplo, descargar y ejecutar malware) sin la intervención del usuario. El navegador web es uno de los principales vectores de ataque contra usuarios. De acuerdo a las estadísticas de los sitios NetMarketShare, W3Counter y StatCounter basado en el análisis del comportamiento de los usuarios en Internet, el navegador más utilizado es Google Chrome, seguido principalmente de Safari o Internet Explorer(IE)/Edge y Firefox. Continuamente son identificadas vulnerabilidades en los navegadores (Chrome, Internet Explorer/Edge, Safari y Firefox) y complementos (Adobe Reader, Adobe Flash Player, Adobe Shockwave Player, Java Runtime Environment, Microsoft Silverlight) que son aprovechadas por los atacantes con el fin de llevar acabo su actividad maliciosa.

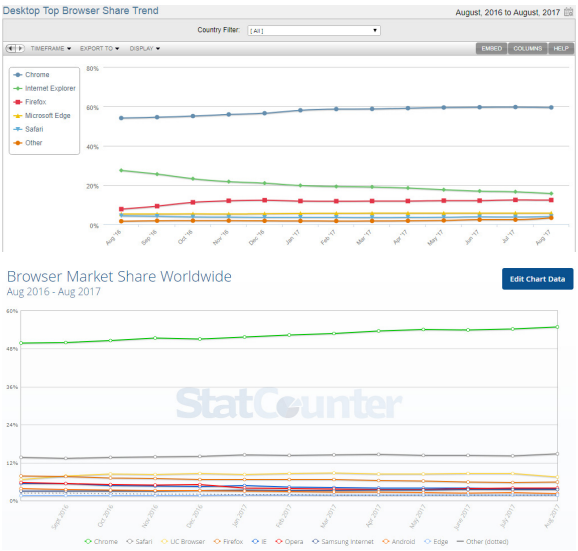


Figura 2. Gráficas de navegadores usados de agosto 2016 a agosto 2017 de NetMarketShare (superior) y StatCounter (inferior)

Paquete de exploits

Un exploit es un programa o código que al ejecutarse se aprovecha de una vulnerabilidad en un sistema, programa o protocolo, para que el creador de dicho programa lo utilice en su beneficio, por ejemplo, para crear una puerta trasera, concebir un equipo zombie (bot), escalar privilegios, instalar un rootkit, robar información u otras actividades maliciosas. Existen dos tipos básicos de exploits que pueden identificarse como conocidos o no conocidos (este último también recibe el nombre de exploits de día cero o *0day*). Para los exploits conocidos existe un registro de divulgación de vulnerabilidades (Vulnerability Disclosure) en las páginas oficiales de los programas, por ejemplo, Apache HTTP Server o Security TechCenter, en donde se encuentra una solución o forma de mitigar la amenaza. Para los exploits de día cero no existe un registro de la vulnerabilidad, esta es aprovechada por los ciberdelincuentes para obtener algún beneficio. Por esa razón es importante mantenerse informado sobre la divulgación de vulnerabilidades y buscar las Vulnerabilidades y Exposiciones Comunes (CVE, Common Vulnerabilities and Exposures) de los sistemas y aplicaciones para tomar las medidas necesarias con el fin de mitigar o reparar el problema de seguridad.

Un paquete de exploits (EK, por sus siglas en inglés) o algunas veces llamado *exploit pack*, son un conjunto de herramientas (páginas de redirección, páginas de aterrizaje, *payloads*, exploits, malware, *gates*, etcétera) que los ciberdelincuentes emplean para automatizar sus ataques. Sirven para aprovecharse de vulnerabilidades en diferentes navegadores web y complementos como Adobe Reader, Flash Player, Shockwave, Java, Microsoft Silverlight en diferentes sistemas operativos para obtener algún beneficio, como pedir una recompensa o realizar otras actividades maliciosas. Algunos EK cuentan con consolas de administración que ayudan al ciberdelincuente a conocer el estado de su operación o campaña.

De acuerdo al Reporte de Amenazas de Seguridad en Internet (ISTR, Internet Security Threat Report) número 22 de Symantec, el exploit kit Angler fue el más común en 2016. Además, existen otros como Magnitude, Neutrino, Rig, Nuclear, Sundown y Fiesta que han afectado considerablemente a usuarios en todo el mundo. Continúan surgiendo otros como Neptune, Disdain y Terror, este último se muestra en la prueba de concepto (PoC, Proof of Concept) de este artículo.

Funcionamiento de un EK

Existen diferentes formas de infección y funcionamiento de los paquetes de exploits, dependiendo de las características particulares que tiene cada EK, la infraestructura del EK empleada para los ataques, campaña y objetivo de los ciberdelincuentes. A continuación, se explican de forma general las etapas de una infección con un paquete de exploits y se pueden observar en la figura 3.

Los ciberdelincuentes colocan anuncios publicitarios con malware (*malvertising*) o introducen código malicioso en sitios web con poca seguridad. Existen diferentes técnicas utilizadas por los ciberdelincuentes para atraer a los usuarios a visitar un sitio, por ejemplo, a través de correos no solicitados o basura (SPAM), mensajes por medio de clientes de mensajería (Whatsapp, Telegram, Snapchat, Facebook Messenger), redes sociales, SMS, etcétera.

Posteriormente, los usuarios dan clic en el anuncio malicioso del sitio o en el vínculo del correo SPAM, o visitan el sitio comprometido y son redirigidos al sitio malicioso. Estos sitios maliciosos obtienen información del equipo de la víctima, una vez que detectan alguna versión vulnerable del navegador web o complementos, envían los exploits; algunos EK envían instrucciones (payload) que produce la descarga de programas sin el consentimiento de los usuarios (*drive-by download*) logrando infectar el equipo con algún tipo de malware como un ransomware y esto se logra simplemente al visitar el sitio.

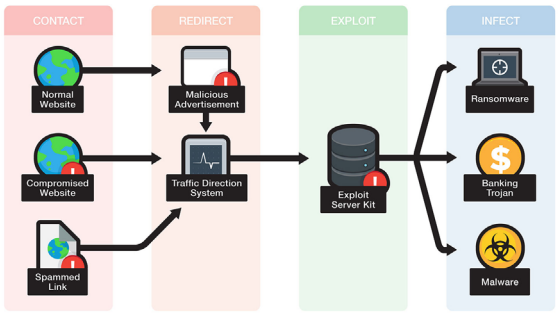


Figura 3. Cadena de infección de un paquete de exploits (Trend Micro)

Si observamos un poco más a detalle los componentes de un ataque con paquetes de exploits podemos encontrar:

- *Landing page*: son las páginas de aterrizaje o destino del EK. Es un componente principal de la infraestructura de los EK ya que esta página es enviada a los usuarios (no es visible en el navegador debido a que se ocultan con código HTML y CSS o utilizan código ofuscado). Estas páginas pueden identificar diferentes versiones de los sistemas operativos, navegadores web y complementos con el fin de identificar una vulnerabilidad específica y poder enviar el exploit adecuado. Una vez explotada la vulnerabilidad, se ejecutan las instrucciones contenidas en el payload permitiendo descargar e instalar algún programa o biblioteca de enlace dinámico para infectar al equipo con ransomware u otro tipo de malware.
- Gate o *gateway server*: el propósito de estas páginas es evaluar a las víctimas, concediendo o negando el paso a cierto tipo de equipos. Evalúan las cabeceras de los protocolos para identificar si son sistemas reales y detectar si se está ejecutando en una *sandbox* o en un honeypot, en cuyo caso se puede detener su actuación para evitar ser analizado. También son utilizados entre el sitio comprometido y la página de aterrizaje (landing page) para controlar la campaña, por ejemplo, esta-

blecer los países, lenguajes, sistemas operativos, navegadores, entre otras características.

- Panel de administración (Management Panel): estas páginas son utilizadas por los ciberdelincuentes para conocer el estado actual de la campaña, ver estadísticas (por navegador web, sistema operativo, complementos, país o versión), tasas de infección, administrar payloads y exploits, generación de nuevas páginas de redirección, realizar búsquedas, crear y seguir campañas, etcétera.

La figura 4 muestra el esquema de la infraestructura utilizada por Magnitude, en donde se aprecian los componentes de este paquete de exploits.

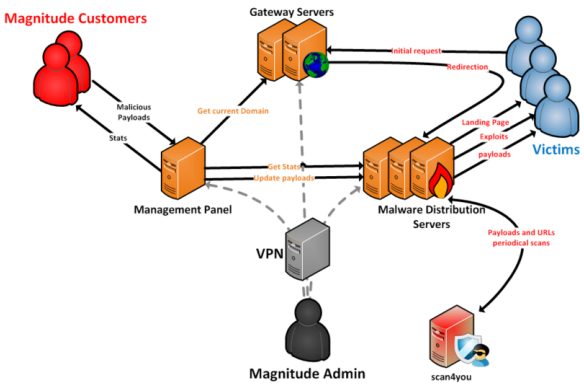


Figura 4. Arquitectura de Magnitud (Trustwave)

Cabe mencionar que existen infraestructuras más complejas detrás de los paquetes de exploits que pueden llegar a tener servidores maestros, de panel de administración, gateway y de distribución de malware.

THUG

Un honeypot es un equipo señuelo configurado e instalado en una red de investigación o producción para poder obtener información de ataques, atacantes o intrusos. A diferencia de los honeypots, los clientes honeypot o honeyclients permiten analizar los ataques del lado del cliente, e igual que los honeypot, estos también pueden ser de alta o baja interacción. Los honeyclient de baja interacción están diseñados para imitar el comportamiento de una aplicación del lado del cliente. PhoneyC es un cliente honeypot virtual (de baja interacción) debido a que solo emula la función principal de un cliente web sin ninguna característica del sistema operativo y cuenta con soporte de lenguajes dinámicos como JavaScript y Visual Basic Script. Fue creado por José Nazario en 2009.

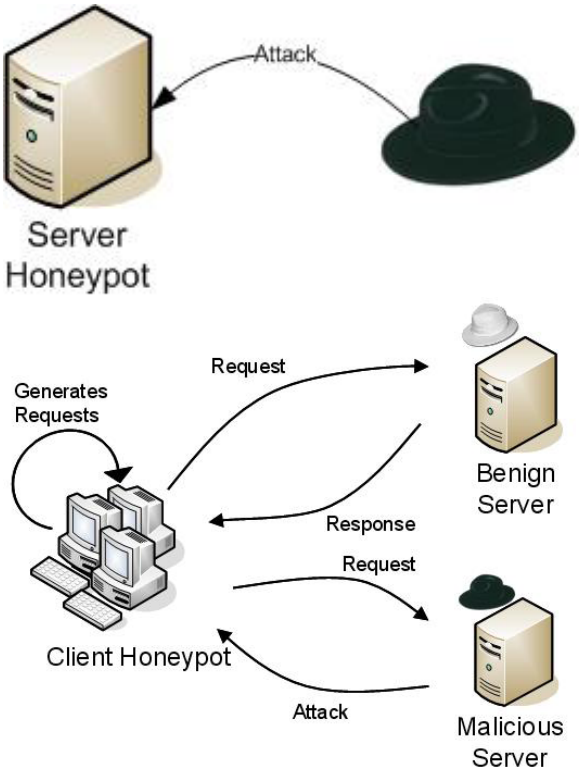


Figura 5. Diferencias entre un Honeypot (superior) y un Honeyclient (inferior)

Angelo Dell'Aera comenzó a contribuir en el desarrollo de PhoneyC a finales del 2009. Mientras Angelo trabajaba en PhoneyC encontró limitaciones en el diseño original. Durante los primeros meses de 2011, pensó en un nuevo diseño y desarrolló Thug, liberó la versión 0.1.0 en julio de ese año. Actualmente Thug se encuentra en la versión 0.9.5, las últimas actualizaciones se pueden encontrar en el proyecto de Github, así como su documentación.

Thug es un honeyclient de baja interacción hecho en Python, está basado en un enfoque híbrido de análisis (estático y dinámico) con el propósito de imitar el comportamiento de un navegador web, así como detectar y emular contenidos maliciosos cuando intentan explotar alguna vulnerabilidad.

Thug proporciona una implementación del Modelo de Objetos del Documento (DOM, Document Object Model) que es (casi)

Document Object Model) que es (casi) compatible con las especificaciones DOM, HTML, eventos, vistas y estilo de W3C (nivel 1, 2 y parcialmente 3). También usa el motor de Javascript V8 de Google embebido en PyV8 para analizar el código Javascript malicioso y de la biblioteca Libemu embebido en Pylibemu para detectar y emular los shellcodes.

Además, el honeyclient Thug cuenta con múltiples "personalidades", aparenta ser diferentes dispositivos como una computadora, celular o tableta. Cada dispositivo puede utilizar diversas versiones de sistemas operativos con diferentes navegadores web, cada navegador con una versión particular. También es posible especificar la versión de los complementos que utilizará el navegador web e incluso puede enviar información emulando movimientos del ratón. Los navegadores web que personaliza son Internet Explorer, Firefox, Safari y Chrome. También cuenta con múltiples módulos de vulnerabilidades (controles ActiveX, principales funcionalidades del navegador, complementos de navegador). Estas características permiten mejorar la emulación y extender la interacción del honeyclient, haciéndole pensar a los ciberdelincuentes que son un navegador y usuario reales; esto posibilita la ejecución de código malicioso como scripts y exploits de los atacantes logrando obtener mayor información y mejores resultados al procesar y analizar los sitios maliciosos.

Thug envía una solicitud a la página web con versiones específicas de un navegador web y complementos (personalidad), la página web procesa la solicitud y genera una respuesta. Thug procesa la respuesta del servidor con los módulos de análisis (estático y dinámico) y de vulnerabilidades, durante este proceso se identifican lenguajes de programación y se detecta código malicioso (payloads y shellcodes). Estos son ejecutados en el honeyclient y si el código malicioso requiere algo más, se genera una nueva solicitud para descargar algún otro recurso, como podría ser un malware. El honeyclient registra el análisis en las bitácoras dependiendo de la configuración (estos datos se toman de los archivos de configuración y de los argumentos pasados a través de la línea de comandos). Este proceso se repite por cada elemento de la página web durante la visita. La figura 6 muestra el panorama general del funcionamiento de Thug.

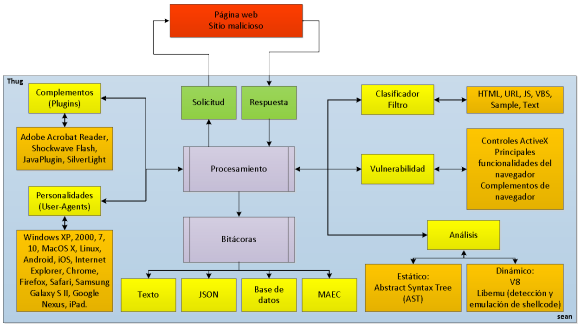


Figura 6. Panorama general de funcionalidad (de Sergio Anduin Tovar Balderas)

Prueba de concepto

En esta PoC (Proof of Concept) se muestra el análisis de tres sitios maliciosos usando Thug. Las diferentes opciones que tiene el honeyclient permite realizar el análisis de sitios con diferentes personalidades que incluyen diferentes versiones de navegadores web, complementos y sistemas operativos e inclusive emular ser un dispositivo móvil. Las opciones nos ayudan a precisar versiones específicas para lograr una emulación lo más cercana a un navegador web para que el paquete de exploits se ejecute de forma exitosa. Las personalidades de Thug se pueden ver en la siguiente figura.

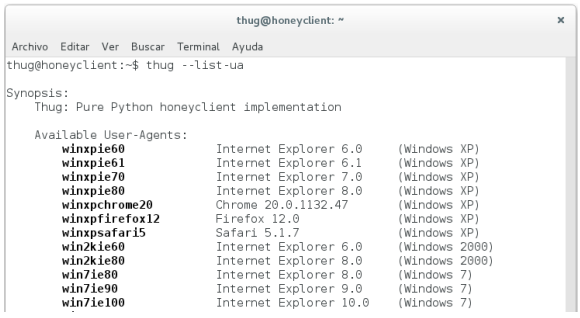


Figura 7. Personalidades de Thug

Un escenario posible es el siguiente: el usuario recibe y lee un correo electrónico no solicitado (SPAM) y da clic en el enlace. Se

inicia el navegador web prestablecido y muestra el sitio http://dominioMalicioso1.com; este sitio a simple vista no realiza ninguna acción o simplemente presenta una página en blanco, pero cuando la página es cargada en el navegador web del usuario se ejecutan instrucciones no entendibles (ofuscadas) que explotan una vulnerabilidad, esta es aprovechada para descargar y ejecutar un archivo binario.

El primer sitio analizado con Thug es http://dominioMalicioso1.com, donde se utilizan las siguientes opciones (figura 8):

- -u win7ie100: especifica el agente de usuario (personalidad), sistema operativo Windows 7 con Internet Explorer 10.0
- -n poc1: indica la ruta de salida de los archivos y bitácoras del análisis
- -v: habilita el modo verbose, muestra mayor detalle de la ejecución
- -F: habilita el modo de registro de bitácoras en archivo de texto
- -Z: habilita el modo de registro de bitácoras en formato JSON

Si no se especifican los complementos a través de la línea de comandos, Thug emplea los prestablecidos (Java versión 1.6.0.32, Adobe Acrobat Reader versión 9.1.0 y Shockwave Flash versión 10.0.64.0).

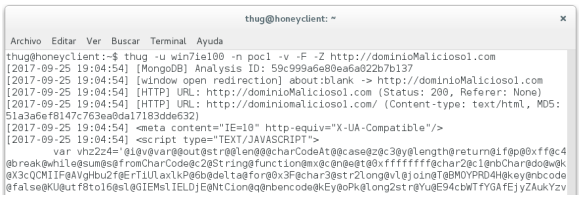


Figura 8. Ejecución y código ofuscado en el primer sitio

En la siguiente figura se puede apreciar parte del código de Visual Basic Script (VBS) utilizado en este sitio malicioso.

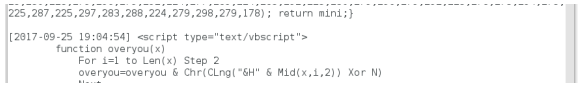


Figura 9. Ejecución, análisis y gráfica del primer sitio

Durante la revisión del sitio, Thug emplea los módulos de vulnerabilidades y realiza un análisis híbrido (estático y dinámico) del código de la página principal. Durante el análisis Thug detecta un código ofuscado, interpreta e identifica una URL (http://4-ever.co.kr/4ever/data/m/win.exe) en el código ofuscado, que resulta en una redirección para descargar el un archivo ejecutable (win.exe).

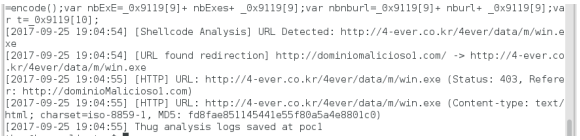


Figura 10. Detección de código ofuscado y redirección a un archivo ejecutable

Cuando Thug está analizando el sitio, obtiene los archivos y los guarda en la carpeta especificada (poc1, se puede apreciar en última línea de la figura anterior), cada archivo es nombrado con su firma MD5. La estructura que crea el honeyclient para este análisis es el siguiente.

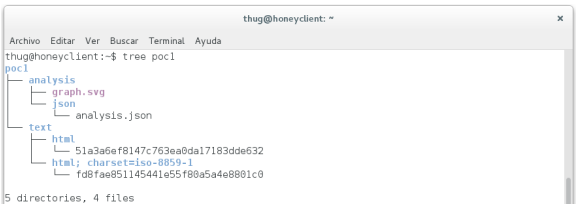


Figura 11. Estructura de archivos y bitácoras generadas por Thug

Se puede consultar las firmas MD5 generadas por Thug en VirusTotal o subir el archivo para tener otra opinión de múltiples antivirus. Thug obtuvo un archivo principal del sitio (index.html) con la firma MD5 51a3a6ef8147c763ea0da17183dde632 y también la URL sospechosa (http://4-ever.co.kr/4ever/data/m/win.exe). Para determinar si el archivo sospechoso es algún tipo de malware es necesario realizar un análisis de malware.

El honeyclient Thug genera una imagen de la interacción con la página maliciosa facilitando en análisis de forma gráfica, esta imagen puede contener redirecciones a otras páginas u otros archivos, iframe (sirven para insertar un documento o mostrar contenidos externos al sitio web), scripts, etcétera.

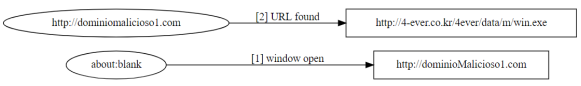


Figura 12. Gráfica de análisis del primer sitio

Configuración

El segundo sitio analizado es http://dominioMalicioso2.com, se utiliza la personalidad de un sistema operativo Windows 10 con Internet Explorer 11.0 empleando los complementos preestablecidos y opciones antes mencionadas. Durante el análisis se identificaron dos iframe que redirigen a las URL http://159.203.15.85/3c5284133c62313b6b28a34f8cdfa328/a39401275d1b300aa789fb22aea4148a y http://159.203.15.85/3c5284133c62313b6b28a34f8cdfa328/9526e055c9757becf45c5190facfd9f2. En la figura 13 se pueden apreciar estos detalles.

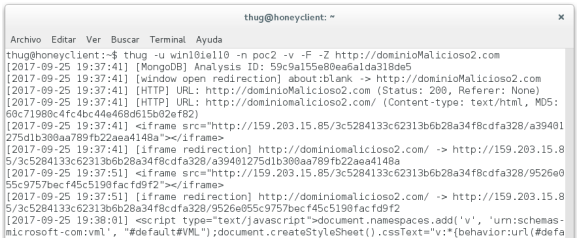


Figura 13. Ejecución y URL detectadas en el segundo sitio

Thug analiza un shellcode y detecta una URL que redirecciona a http://159.203.15.85/d/3c5284133c62313b6b28a34f8cdfa328/?q=r4&r=62ba5e67f14ed186d58fc171909e09ba&e=cve20132551 que intenta explotar la vulnerabilidad CVE-2013-2551 (esta vulnerabilidad también la explota Terror, se revisará en el siguiente ejemplo), esta URL y las anteriores también fueron consultadas en VirusTotal.

Figura 14. Detección y redirección a URL maliciosa

En esta imagen se pueden ver los 2 iframe que tiene la página y la redirección a una URL que intenta explorar una vulnerabilidad particular.

Figura 15. Gráfica de análisis del segundo sitio

El paquete de exploits Terror (Terror EK) evalúa a sus potenciales víctimas determinando el sistema operativo, navegador web y complementos con el fin de enviar los exploits más adecuados para comprometer el equipo.

El último sitio que se analizará con Thug utiliza el paquete de exploits Terror, y se utiliza la personalidad de un sistema operativo Linux con Chrome versión 54.0.2840.100 (figura 26). Durante el análisis el paquete de exploits utiliza un applet.

Figura 16. Análisis del tercer sitio

Terror EK utiliza iframe para insertar un documento o mostrar contenidos externos al sitio web, en la figura se puede observar que hace redirección a la página http://dominiomalicioso3.com/exploits/adobe1.html.

Figura 17. Redirección a través de iframe

Esta página contiene código JavaScript que sirve para obtener información de las potenciales víctimas. La información que obtiene es la plataforma (win, linux y unix) y sistema operativo (Windows 2000, XP, Vista, 7, 8, 8.1, Mac/iOS, UNIX, Linux).

Figura 18. Identificación de plataforma y sistema operativo

Posteriormente se identifica una línea que valida el navegador web, esta verificación sirve para ejecutar el código y mostrar un archivo shockwave o flash si no es Internet Explorer (if !IE).

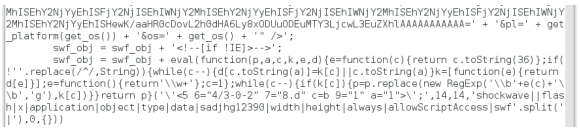


Figura 19. Validación de navegador

Nuevamente el EK utiliza una redirección para cargar y ejecutar código JavaScript en el equipo (exploit) enfocado al navegador web Firefox.

Figura 20. Redirección a JavaScript malicioso

En la primera línea se puede apreciar que se hace una validación para ejecutar el código en Windows. El código malicioso carga instrucciones para realizar una consulta a http://kitempowernetwork.com/test/q.php y ejecutarlas en el equipo víctima utilizando wscript.exe o cmd.exe.

Figura 21. Código malicioso usando JavaScript

El EK utiliza otros iframe y redirecciones para ejecutar código malicioso en Internet Explorer. Se puede observar que Thug identifica un programa vbscript (Visual Basic Script) que utiliza powershell.exe para realizar la consulta a la página de la figura anterior, esto muestra una forma diferente de ejecutar código malicioso.

Figura 22. Código malicioso usando Visual Basic Script

La figura 23 muestra la estructura de archivos creada por Thug durante el análisis, en ella se encuentran los archivos obtenidos del sitio malicioso y bitácoras.

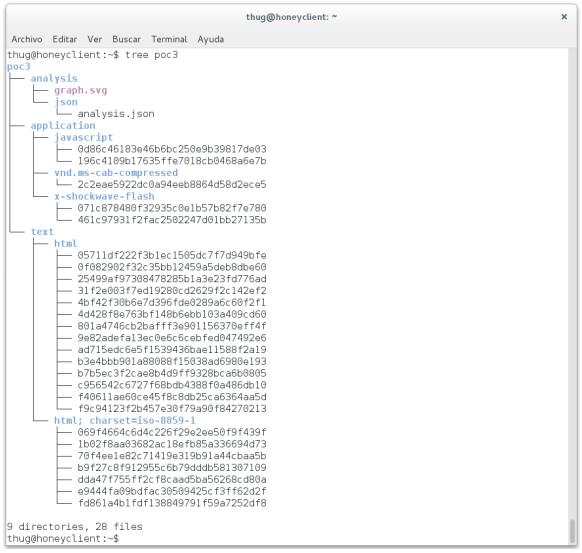


Figura 23. Estructura de archivos del análisis

Se ha identificado que los exploits utilizados en el sitio http://dominiomalicioso3.com/ forman parte del EK Terror y explotan diferentes vulnerabilidades; en la tabla 1 se especifican los CVE y muestra el reporte de VirusTotal de algunos de los archivos que obtuvo Thug durante el análisis del sitio.

Tipo de archivo	MD5	CVE
JavaScript	0d86c46183e-46b6bc250e9b-39817de03	-
JavaScript	196c4109b-17635ffe7018c-b0468a6e7b	2014-1510

Tipo de archivo	MD5	CVE
HTML	31f2e003f7e-d19280cd2629f-2c142ef2	2016-0189
HTML	4d428f8e-763bf148b6eb-b103a409cd60	2012-3993
HTML	ad715edc6e5f-1539436bae-11588f2a19	2014-6332
HTML	b3e4bbb901a-88088f15038a-d6980e193	2014-6332

Tabla 1. Archivos analizados y CVE identificados en el reporte de VirusTotal (de Sergio Anduin Tovar Balderas)

En esta imagen generada por Thug se pueden apreciar de forma gráfica el comportamiento cuando la víctima visita el sitio y todas las acciones que emplea el EK para identificar el sistema operativo, navegador y complementos.

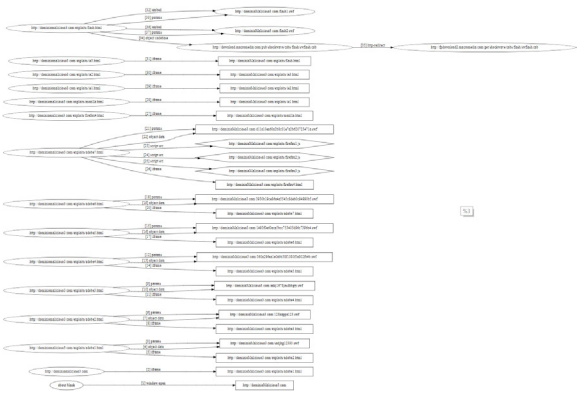


Figura 24. Imagen de análisis del tercer sitio

Si deseas ver el video del artículo ingresa al canal SeguridadTV de UNAM-CERT o entra directamente aquí.

Conclusiones

Thug ayuda a los analistas de malware a examinar detalladamente un sitio sospechoso pretendiendo ser un navegador real ya que realiza un análisis estático y dinámico en conjunto de los módulos de vulnerabilidades. Además, es capaz de detectar shellcode e identificar URL, recolectar archivos del sitio como scripts, ejecutables, PDF, applets, archivos flash (swf), exploits o payloads que utiliza el sitio, así como generar una imagen con el flujo de comportamiento e interacción. Este honeyclient ayuda a los investigadores de seguridad a obtener evidencia para reportar y dar de baja los sitios maliciosos. También es posible realizar un análisis de malware ya que se cuenta con los archivos del sitio, esto permitirá determinar a detalle las vulnerabilidades que explota, obtener indicadores de compromiso, firmas para la detección y prevención en sistemas antivirus, sistemas de detección (IDS) y prevención intrusos (IPS), antispam y otras soluciones.

Es muy importante como usuarios mantener actualizados los sistemas operativos, antivirus y aplicaciones de nuestros dispositivos (computadora, celular y tableta), así como aplicar los parches de seguridad críticos. No dar clic en vínculos, no abrir mensajes ni adjuntos de correos electrónicos o mensajes instantáneos sospechosos (asegurarse de que la persona que nos envía la información es un conocido). Los navegadores cuentan con tecnologías para detectar y evitar phishing, programas o sitios maliciosos, pero hay que estar atentos en las advertencias de seguridad que muestra el navegador, así como realizar configuraciones de seguridad y establecer preferencias de privacidad para limpiar nuestros datos de navegación como cookies y datos de formularios.

En nuestra organización es importante realizar campañas de concientización para que los usuarios conozcan los métodos y técnicas que utilizan los ciberdelincuentes para evitar que sean víctimas de algún ataque.

También se recomienda:

- Utilizar soluciones de administración de parches de seguridad y actualizaciones (por ejemplo, WSUS)
- Crear una política para descargar e instalar las actualizaciones del sistema operativo
- Prohibir la instalación de programas no autorizados en la organización
- Utilizar soluciones endpoint, NAC, firewall e IPS
- Programar la descarga de base de firmas y escaneo de los equipos cliente desde consolas antivirus

Es muy importante siempre estar atento a las vulnerabilidades de los servicios y sistemas para aplicar las actualizaciones, parches de seguridad o aplicar un mecanismo de protección para mitigar el impacto.

Para conocer otras herramientas visita nuestra página del Proyecto Honeynet UNAM.

Si identificaste algún sitio sospechoso, malware o phishing puedes reportarlo a UNAM-CERT aquí. A través de Google también es posible denunciar páginas de phishing: (https://safebrowsing.google.com/safebrowsing/report_phish/); o sitios maliciosos (https://safebrowsing.google.com/safebrowsing/report_badware/).

Conoce OUCH!, el boletín de seguridad preventiva del Instituto SANS, consejos del UNAM-CERT, mantente al día en noticias de seguridad e inscríbete al boletín de noticias. Conoce nuestro portal y revisa la sección de divulgación.

Referencias

Dell'Aera, Angelo. (2017). Thug - Python low-interaction honeyclient. GitHub Pages. Recuperado el 11 de octubre de 2017, de https://buffer.github.io/thug/

Dell'Aera, Angelo. (2017). Thug 0.9.3 documentation. GitHub Pages. Recuperado el 11 de octubre de 2017, de https://buffer.github.io/thug/doc/index.html

Dell'Aera, Angelo. (2017). Thug - Python low-interaction honeyclient. GitHub. Recuperado el 11 de octubre de 2017, de https://github.com/buffer/thug

Dell'Aera, Angelo. (2012). Thug: a new low-interaction honeyclient. Recuperado el 11 de octubre de 2017, de https://www.honeynet.org/files/HPAW2012-Thug.pdf

Dell'Aera, Angelo. (2015). Thug and the art of web client tracking inspection. The Honeynet Project. Recuperado el 11 de octubre de 2017, de https://www.honeynet.org/node/1200

Seifert, Christian. Steenson, Ramon. Holz, Thorsten. Yuan, Bing. Davis, Michael A. (2007). Know Your Enemy: Malicious Web Servers. The Honeynet Project. Recuperado el 11 de octubre de 2017, de http://www.honeynet.org/papers/mws

Seifert, Christian. The Honeynet Project. (2007). Know Your Enemy: Behind the Scenes of Malicious Web Servers. The Honeynet Project. Recuperado el 11 de octubre de 2017, de https://www.honeynet.org/papers/wek

Nazario, Jose. (2009). PhoneyC: A Virtual Client Honeypot. Recuperado el 11 de octubre de 2017, de https://www.usenix.org/legacy/events/leet09/tech/full_papers/nazario/naz...

Seifert, Christian. (2011). PhoneyC: A virtual client honeypot. The Honeynet Project. Recuperado el 11 de octubre de 2017, de https://www.honeynet.org/project/PhoneyC

Chuvakin, Anton. (2011). The Honeynet Project Releases New Tool: PhoneyC | The Honeynet Project. Recuperado el 11 de octubre de 2017, de https://www.honeynet.org/node/605

Nazario, Jose. Dell'Aera, Angelo. (s.f). PhoneyC. GitHub. Recuperado el 11 de octubre de 2017, de https://github.com/buffer/phoneyc

Baecher, Paul. Koetter, Markus. (2008). libemu - shellcode detection. GitHub. Recuperado el 11 de octubre de 2017, de https://github.com/buffer/libemu

Dell'Aera, Angelo. (2016). A Libemu Cython wrapper. GitHub. Recuperado el 11 de octubre de 2017, de https://github.com/buffer/pylibemu

Kaspersky Lab. (2017). Attacks with exploits: From everyday threats to targeted campaigns. Recuperado el 11 de octubre de 2017, de https://go.kaspersky.com/rs/802-IJN-240/images/Report_Exploits_in_2016_e...

NetMarketShare. (2017). Market Share Reports. Recuperado el 11 de octubre de 2017, de https://www.netmarketshare.com/

Awio Web Services LLC. (2017). W3Counter: Global Web Stats. Recuperado el 11 de octubre de 2017, de https://www.w3counter.com/globalstats.php

StatCounter. (2017). Browser Market Share Worldwide. StatCounter Global Stats. Recuperado el 11 de octubre de 2017, de http://gs.statcounter.com/browser-market-share/all/

MITRE. (2017). CVE. Common Vulnerabilities and Exposures (CVE). Recuperado el 11 de octubre de 2017, de https://cve.mitre.org/

The Apache Software Foundation. (2017). Reporting Security Problems with Apache. Recuperado el 11 de octubre de 2017, de https://httpd.apache.org/security_report.html

Microsoft. (2017). Microsoft Security. Coordinated Vulnerability Disclosure. Report a Vulnerability. MSRC. Recuperado el 11 de octubre de 2017, de https://technet.microsoft.com/en-us/security/dn467923.aspx

Symantec Corporation. (2017). Internet Security Threat Report 2017. Symantec. Recuperado el 11 de octubre de 2017, de https://www.symantec.com/security-center/threat-report

Symantec Corporation. (2017). ISTR Volume 22. Recuperado el 11 de octubre de 2017, de https://digitalhubshare.symantec.com/content/dam/Atlantis/campaigns-and-... Protection/ISTR22_Main-FINAL-JUN8.pdf

Duncan, Brad. (2016). EITest Campaign Evolution: From Angler EK to Neutrino and Rig. Palo Alto Networks Blog. Recuperado el 11 de octubre de 2017, de https://researchcenter.paloaltonetworks.com/2016/10/unit42-eitest-campai...

SpiderLabs Research. (2017). Magnitude Exploit Kit Backend Infrastructure Insight Part III. Recuperado el 11 de octubre de 2017, de https://www.trustwave.com/Resources/SpiderLabs-Blog/Magnitude-Exploit-Ki...

Segura, Jérôme. (2016). A look into Neutrino EK's jQueryGate. Malwarebytes Labs. Recuperado el 11 de octubre de 2017, de https://blog.malwarebytes.com/threat-analysis/exploits-threat-analysis/2...

Segura, Jérôme. (2016). Nuclear EK Leveraged In Large WordPress Compromise Campaign. Malwarebytes Labs. Recuperado el 11 de octubre de 2017, de https://blog.malwarebytes.com/threat-analysis/2016/02/nuclear-ek-leverag...

Biasini, Nick. Brumaghin, Edmund. Chiu, Alex. (2017). Cisco's Talos Intelligence Group Blog: Threat Spotlight: Sundown Matures. Recuperado el 11 de octubre de 2017, de http://blog.talosintelligence.com/2017/03/sundown-matures.html

Elisan, Christopher. (2017). The Fiesta Exploit Kit. Not So Festive After All. Recuperado el 11 de octubre de 2017, de https://www.rsa.com/en-us/blog/2017-04/fiesta-exploit-kit

Gardezi, Zain. Sardiwal, Manish. Threat Research. (2017). Hiking Club Malvertisements Drop Monero Miners Via Neptune Exploit Kit. Threat Research Blog. FireEye Inc. Recuperado el 11 de octubre de 2017, de https://www.fireeye.com/blog/threat-research/2017/08/neptune-exploit-kit...

Unterbrink, Holger. Tacheau, Emmanuel. (2017). Cisco's Talos Intelligence Group Blog: Terror Evolved: Exploit Kit Matures. Recuperado el 11 de octubre de 2017, de http://blog.talosintelligence.com/2017/05/terror-evolved-exploit-kit-mat...

Gooley, Derek. Hegde, Rohit. (2017). Top Exploit Kit Activity Roundup Summer 2017. Zscaler Blog. Recuperado el 11 de octubre de 2017, de https://www.zscaler.com/blogs/research/top-exploit-kit-activity-roundup-...

Segura, Jérôme. (2017). RIG exploit kit distributes Princess ransomware. Malwarebytes Labs. Recuperado el 11 de octubre de 2017, de https://blog.malwarebytes.com/cybercrime/2017/08/rig-exploit-kit-distrib...

Segura, Jérôme. (2017). Enemy at the gates: Reviewing the Magnitude exploit kit redirection

chain. Malwarebytes Labs. Recuperado el 11 de octubre de 2017, de https://blog.malwarebytes.com/cybercrime/2017/08/enemy-at-the-gates-revi...

Trend Micro. (2017). exploit kit - Definition - Trend Micro USA. Recuperado el 11 de octubre de https://www.trendmicro.com/vinfo/us/security/definition/exploit-kit

Kaspersky. (2017). Adware. Internet Security Threats. Recuperado el 11 de octubre de 2017, de https://latam.kaspersky.com/resource-center/threats/adware

W3C. (2005). W3C Document Object Model. Recuperado el 11 de octubre de 2017, de https://www.w3.org/DOM/

Ecma International. (2017). Standard ECMA-262. Recuperado el 11 de octubre de 2017, de https://www.ecma-international.org/publications/standards/Ecma-262-arch.htm

Malwarebytes Labs. (2016). Exploit kits. Malwarebytes Labs. Threats. Recuperado el 11 de 2017, de octubre de https://blog.malwarebytes.com/threats/exploit-kits/

US-CERT. (2015). Securing Your Web Browser. Recuperado el 11 de octubre de 2017, de https://www.us-cert.gov/publications/securing-your-web-browser

VirusTotal. (s.f.). VirusTotal. Recuperado el 11 de octubre de 2017, de https://www.virustotal.com

UNAM-CERT. (2017). Exploit. Recuperado el 11 de octubre de 2017, de https://www.seguridad.unam.mx/taxonomy/term/1063

Frank, Daniel. (2017). Dissecting Sundown Exploit Kit | RSA Link. Recuperado el 11 de octubre de 2017, de https://community.rsa.com/community/products/netwitness/blog/2017/08/14/...

F-Secure. (2017). Exploit Kits. Recuperado el 11 de octubre de 2017, de https://www.f-secure.com/en/web/labs_global/exploit-kits

Antoniewicz, Brad. (2017). Catching Exploit Kit Landers. OpenDNS Umbrella Blog. Recuperado el 11 de octubre de 2017, de https://umbrella.cisco.com/blog/2017/01/11/catching-exploit-kit-landers/

McAfee. (2015). Browser Network Attack Methods. Recuperado el 11 de octubre de 2017, de https://www.mcafee.com/mx/resources/solution-briefs/sb-browser-network-a...

Kaspersky Lab. (2012). El exploit día-cero de Java en la web - Securelist. Recuperado el 11 de octubre de 2017, de https://securelist.lat/el-exploit-da-cero-de-java-en-la-web/65791/

Krebs, Brian. (2013). What You Need to Know About the Java Exploit - Krebs on Security. Recuperado el 11 de octubre de 2017, de https://krebsonsecurity.com/2013/01/what-you-need-to-know-about-the-java...

Goujon, André. (2012). Alerta: exploit 0 day afecta Java y propaga malware. Recuperado el 11 de octubre de 2017, de https://www.welivesecurity.com/la-es/2012/08/27/alerta-exploit-0-day-afe...

Catoira, Fernando. (2012). ¿Cómo funciona el exploit 0-day de Java? Recuperado el 11 de octubre de 2017, de https://www.welivesecurity.com/la-es/2012/08/30/como-funciona-explot-0-d...

ESET. (2017). Glosario. Recuperado el 11 de octubre de 2017, de https://www.welivesecurity.com/la-es/glosario/#E

Albors, Josep. (2015). Exploits: What are they and how do they work? Recuperado el 11 de octubre de 2017, de https://www.welivesecurity.com/2015/02/27/exploits-work/

Lopes, Ilya. (2014). Malvertising, ¿la evolución del adware? Recuperado el 11 de octubre de 2017, de https://www.welivesecurity.com/la-es/2014/09/11/malvertising-evolucion-a...

Zeltser, Lenny. (2015). Three Web Attack Vectors Using the Browser. Recuperado el 11 de octubre de 2017, de https://zeltser.com/web-browser-attack-vectors/

Microsoft. (2016). Deploy Windows Server Update Services | Microsoft Docs. Recuperado el 11 de octubre de 2017, de https://docs.microsoft.com/en-us/windows-server/administration/windows-s...

Si quieres saber más, consulta:

- Proyecto Honeynet en la UNAM
- Glastopf: Honeypot de aplicaciones web – I
- Glastopf: Honeypot de aplicaciones web – II
- Cowrie Honeypot: Ataques de fuerza bruta
- Conpot: Honeypot de Sistemas de Control Industrial

Sergio Anduin Tovar Balderas

Es egresado de la carrera de Ingeniería en Computación con módulo de salida en Redes y Seguridad por la Facultad de Ingeniería de la Universidad Nacional Autónoma de México (UNAM).

Labora desde 2014 en la Coordinación de Seguridad de la Información (CSI/UNAM-CERT) en el área de Detección de Intrusos y Tecnologías Honeypot, donde lleva a cabo actividades de desarrollo, instalación y pruebas de tecnologías honeypot para análisis y detección de actividad maliciosa. Fue instructor de la línea de especialización Detección de Intrusos y Tecnologías Honeypot en el Congreso Seguridad en Cómputo UNAM 2014.

Egresado de la octava generación del Plan de Becas en Seguridad Informática de UNAM-CERT. Ha participado como instructor de nuevas generaciones en este mismo plan de capacitación. Laboró en el proyecto Seguridad en UNIX de la misma organización, además ha impartido cursos y participado en proyectos con dependencias de la UNAM y entidades externas del sector público.

Cuenta con la certificación IPS-ESE (*IPS Express Security for Engineers*) de Cisco.

DGTIC

DIRECCIÓN GENERAL DE CÓMPUTO Y DE
TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

UNAM CERT®

Revista .Seguridad *Cultura de prevención para* TI
No.30 /octubre- noviembre 2017