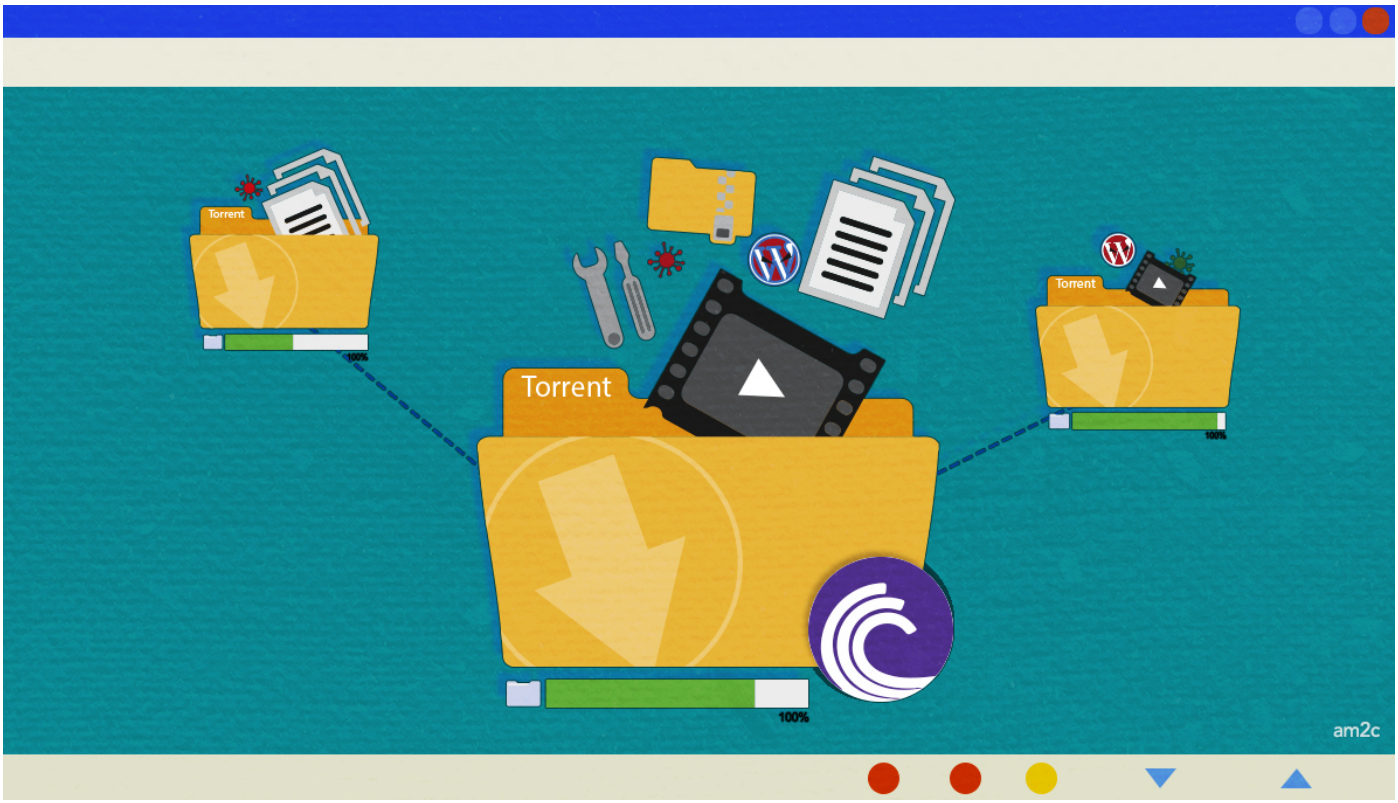
.Seguridad
Cultura de prevención para TI
Published on *Revista .Seguridad* (http://revista.seguridad.unam.mx)

TORRENTS: COMPARTIENDO INFORMACIÓN LEGÍTIMA Y TAMBIÉN AMENAZAS

Camilo Gutiérrez Amaya

numero-30



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 cibercriminales. 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
