Press release

NOTA DE PRENSA

PARA PUBLICACIÓN INMEDIATA

Madrid, 13 de octubre, 2011

Desvelando el lado oscuro de BitTorrent

Con decenas de millones de usuarios, descargas diarias, el 60% del tráfico upstream y el 20% del tráfico downstream en Europa, BitTorrent es la aplicación de intercambio de archivos P2P (Peer to Peer) más popular del mundo y representa una parte significativa del tráfico actual en Internet. Sin embargo, esta gran popularidad no sólo atrae a usuarios habituales del intercambio de archivos, sino también a usuarios malintencionados.

Autores: Michal Kryczka del Institute IMDEA Networks y Rubén Cuevas de la Universidad Carlos III de Madrid

La investigación desarrollada por el Institute IMDEA Networks, la Universidad Carlos III de Madrid y el Institut Telecom Sud Paris, "TorrentGuard: stopping scam and malware distribution in the BitTorrent ecosystem", se enfocó en el fenómeno de la publicación de contenidos falsos y maliciosos en el ecosistema BitTorrent. Se examinaron treinta mil torrents publicados en el portal PirateBay durante un período de dos semanas. Los resultados mostraron que el 35% de los torrents analizados se asociaban a contenidos falsos. Esto significa que uno de cada tres torrents tiene un contenido distinto al que se describe en el título.

PirateBay, el portal más popular de BitTorrent, elimina todos los torrents que se demuestra que son falsos, junto con la cuenta de usuario que publicó el contenido. Los torrents falsos son identificados por los usuarios que efectúan descargas, quienes informan a PirateBay, el cual, a su vez, elimina el torrent y la cuenta de usuario.

Press release

Pese a este mecanismo de detección/eliminación, una de cada cuatro descargas de BitTorrent tiene contenidos falsos. Esto supone una grave amenaza que todavía no se ha resuelto.

El estudio muestra que sólo 20 editores son responsables de la inyección del 90% de los contenidos falsos que aparecen en el ecosistema BitTorrent. La mayoría de estos editores utilizan servidores dedicados de empresas extranjeras, con el fin de tener suficientes recursos para sus actividades, así como para ocultar su identidad. Se dedica un enorme esfuerzo a distribuir estos contenidos falsos, porque los portales eliminan todas las cuentas desde las cuales se publican dichos contenidos, y se han de crear cuentas nuevas continuamente. El estudio también describe distintas técnicas utilizadas por los editores para atraer a los usuarios a sus contenidos. Estas técnicas incluyen el uso de títulos de películas de éxito o la falsificación de las estadísticas de rendimiento de un torrent para que parezca más popular. Esta enorme inversión de dinero y recursos sólo puede explicarse por las fuertes motivaciones que impulsan la distribución de contenidos falsos.

Con el fin de identificar estas motivaciones, los investigadores examinaron a fondo una gran cantidad de contenidos falsos. Su análisis demostró que los editores de contenidos falsos se ajustan a tres perfiles distintos. Un sesenta y cinco por ciento de ellos explotan la popularidad del sistema BitTorrent para propagar rápidamente malware entre miles de usuarios. El contenido publicado puede ser malware en sí mismo, pero algunos editores utilizan técnicas más sofisticadas. Publican películas con títulos atrayentes, que se abren en un reproductor con ventanas emergentes. En éstas se le pide al usuario que instale nuevos codecs, y proporcionan el enlace a una URL donde pueden descargarse. El software de seguridad y antivirus detecta el archivo que contiene los codecs falsos como malware.

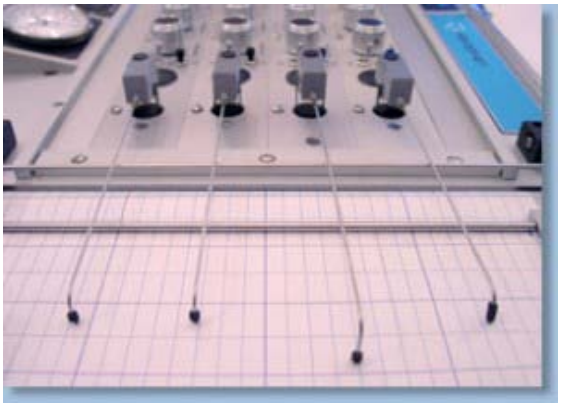
Press release

Por otra parte, el 35% de los editores de contenidos falsos son estafadores. Utilizan el ecosistema *torrent* para atraer a los usuarios a sus páginas web, donde llevan a cabo distintos tipos de fraudes. Por ejemplo, pueden pedir a las víctimas que proporcionen su número de tarjeta de crédito o que participen en concursos con SMS premium. Por tanto, lo que motiva a estos editores es el dinero. El resultado es que un porcentaje muy reducido de los torrents falsos se origina en las agencias antipiratería. Al contrario que los otros dos tipos de editores, que tienen motivaciones fraudulentas, las agencias antipiratería publican versiones falsas de los contenidos bajo derechos de autor que desean proteger. Las medidas de las agencias antipiratería se ven limitadas por la cantidad de contenido (a solicitud de una empresa) y el tiempo disponible (en las semanas antes y después de que el contenido, por ejemplo una película, se estrene).

El intercambio de archivos P2P representa una parte significativa del tráfico actual en Internet

Con el fin de protegerse contra los torrents falsos, los investigadores desarrollaron y evaluaron un software llamado “TorrentGuard”. Este programa utiliza el portal PirateBay para recopilar las direcciones IP utilizadas para distribuir los contenidos falsos. Estas direcciones se ponen luego en una lista negra. El software también controla cada torrent publicado en PirateBay y lo marca como falso si se ha utilizado una dirección IP de la lista negra para servir el contenido. Con este método es posible identificar los contenidos falsos poco después de que se publiquen por primera vez, lo cual acelera el proceso de detección. El software está a disposición del público y se puede acceder a él a través de una página web o de un popular plug-in para los clientes de BitTorrent. El uso generalizado de esta herramienta podría evitar hasta 35 millones de descargas de contenidos falsos cada año, contribuyendo así a reducir el número de infecciones informáticas y episodios fraudulentos a los que se enfrentan los usuarios de BitTorrent.

Press release



El software propuesto en este trabajo tiene un propósito similar al del polígrafo

El estudio fue realizado por Michal Kryczka, del Institute IMDEA Networks, Rubén Cuevas, Roberto González y Arturo Azcorra, de la Universidad Carlos III de Madrid, y Ángel Cuevas, del Institut Telecom Sud Paris (Francia).

Michal Kryczka

Institute IMDEA Networks

Rubén Cuevas

Universidad Carlos III de Madrid

Press release

SOBRE INSTITUTE IMDEA NETWORKS

Institute IMDEA Networks es un Instituto de investigación respaldado por el Gobierno de la Comunidad de Madrid y por la Unión Europea. El Instituto atrae a distinguidos y jóvenes investigadores científicos de todo el mundo con el fin de desarrollar ciencia y tecnología punta en el campo de las redes. Para asegurarse una perspectiva auténticamente internacional, el lenguaje de trabajo del Instituto es el inglés. Al promover la colaboración interdisciplinaria, el Instituto, establecido en Madrid, trabaja en sociedad con empresas y científicos líderes de todo el mundo. Sus actividades generan nuevo saber y conocimientos, con los que el Instituto apoya el continuo desarrollo de Madrid y de España como centros de referencia internacional para la investigación científica y tecnológica.

www.networks.imdea.org

INFORMACIÓN DE CONTACTO – CON PROPÓSITOS MERAMENTE INFORMATIVOS

Amablemente solicitamos que no publique los siguientes datos de contacto. Gracias por su cooperación.

Si desea más información sobre este particular, por favor, contacte con:

Contacto:
Rebeca De Miguel, Operations Support Manager
Tel: +34 91 481 6977
Email: rebeca.demiguel@imdea.org

Más información:
Tel: +34 91 481 6210
Email: info.networks@imdea.org

Institute IMDEA NETWORKS
Avda del Mar Mediterráneo, 22
28918 – Leganés
Madrid (Spain)