BOLETÍN DE ALERTA

Boletín Nro.: 2015-13
Fecha de publicación: 26/10/2015
Tema: Drive-by-Download

Descripción:

Drive-by-Download es una técnica utilizada por ciberdelincuentes en la que un software malicioso (malware) se instala en un equipo con el sólo hecho de visitar una página en Internet que está infectada por este tipo de amenaza. No se requiere interacción de parte de la víctima ya que el malware (o una pieza del mismo) se encuentra en el mismo código de las páginas infectadas y el sólo hecho de cargarlas en el navegador hace que se infecte el equipo.

Por lo general, los ciberdelincuentes utilizan la técnica de *drive-by-download* explotando vulnerabilidades en complementos de navegadores (*plugins*), como Java, Adobe Reader y Adobe Flash. Si el equipo cuenta con alguna vulnerabilidad, el código malicioso de la web infectada podrá explotarla para instalar el malware de forma automática.

Para infectar un sitios web los atacantes por lo general **inyectan código** que utilizan *iframes* y/o javascripts maliciosos para conectarse a sitios remotos y descargar el malware. Generalmente el código se encuentra al final del sitio web y utiliza etiquetas propiamente configuradas, como por ejemplo la etiqueta *style* con el valor *hidden*, para ocultarse de la vista del usuario.

Por lo tanto cuando un usuario navega por el sitio comprometido, automáticamente comienza la descarga de la amenaza.

Las páginas infectadas no sólo se limitan a páginas de alto riesgo (como páginas pornográficas, por ejemplo), sino que también pueden ser páginas legítimas y confiables que han sido comprometidas por ciberdelincuentes y que hospeden el código malicioso sin saberlo.

Esta técnica de *drive-by-download* puede ser utilizado contra equipos de cualquier sistema operativo: Windows, OS X (Apple), Linux, Android, iOS, etc.

CERT-PY Equipo de Respuestas ante Emergencias Cibernéticas
Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)
Gral. Santos y Concordia – Complejo Santos – Ofic. E14
cert@cert.gov.py | +595 21 201014 | +595 21 3276902
Asunción - Paraguay | www.cert.gov.py
@CERTpy
/CERT-Py

Impacto:

La técnica de *drive-by-download* se utiliza para la distribución de software malicioso (malware), tales como virus, software espía (spyware), gusanos, ransomware, etc.

Se ha observado un importante aumento de ransomware, un tipo de malware que encripta los archivos de la víctima y solicita un pago de "rescate" para desencriptar los archivos. Este tipo de malware frecuentemente es distribuido a través de la técnica de drive-by-download.

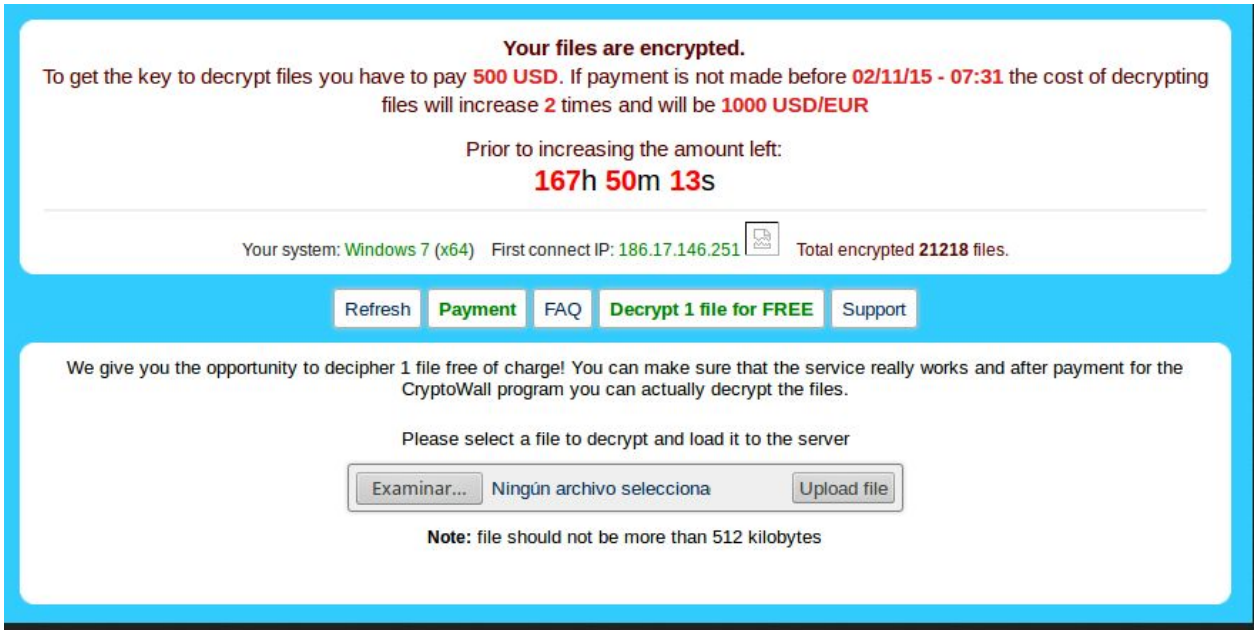

Figura 2: Ejemplo de una variante de Ransomware (CryptoWall 3.0)

Mitigación y Prevención:

Para evitar que un equipo quede infectado por malware distribuido mediante *drive-by-download*, las acciones preventivas son fundamentales:

- Contar con soluciones de antivirus y mantenerlo actualizado, de modo a **prevenir** la infección. Cuando un equipo ya está infectado, el antivirus muchas veces ya no es efectivo.
- Mantener su sistema operativo y el software siempre actualizado, con los últimos parches. El *drive-by-download* explota vulnerabilidades del software, si el software no contara con dicha vulnerabilidad, el malware no podría instalarse.
- No ingresar a enlaces dudosos que le son enviados a través de correo electrónico, servicios de mensajería, redes sociales, etc.

CERT-PY Equipo de Respuestas ante Emergencias Cibernéticas
Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)
Gral. Santos y Concordia – Complejo Santos – Ofic. E14
cert@cert.gov.py | +595 21 201014 | +595 21 3276902
Asunción - Paraguay | www.cert.gov.py
@CERTpy
/CERT-Py

- Evitar la ejecución automática de plugins como Adobe Flash Player, Java, etc. La mayoría de los navegadores modernos permiten configurarlo de modo a que se solicite permiso al usuario cada vez que un sitio web intente ejecutar un plugin. Para ello puede ir a la Configuración u Opciones de su navegador.
    - En Google Chrome, escribir "chrome://settings/content/" en la barra de navegación y en la sección "Complementos", seleccionar “Permitirme decidir cuándo ejecutar contenido de plugins”.
    - En Mozilla Firefox, escribir "about:addons" en la barra de navegación y en cada plugin deseado, seleccionar la opción "Preguntar para activar".
- Contar con mecanismos de protección contra la publicidad invasiva, muy ligada al malvertising (anuncios maliciosos embebidos en la web). Existen complementos muy útiles como AdBlock Plus, disponible para varios sistemas operativos y navegadores: https://adblockplus.org/es/

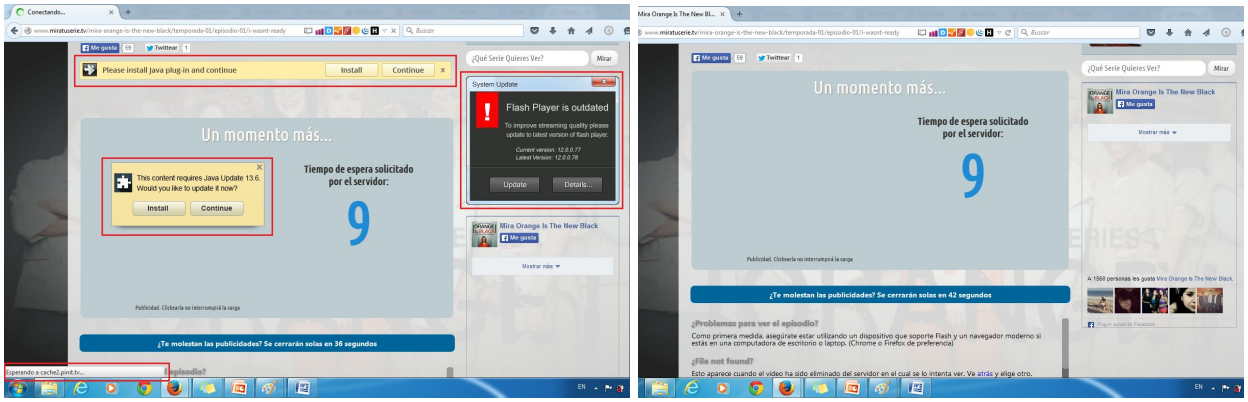

Figura 3: Ejemplo de filtrado de publicidad maliciosa con AdBlock Plus

- Evitar la ejecución automática de Javascript. Existen complementos como No-Script y ScriptSafe que deshabilitan por defecto la ejecución de Javascript, permitiendo al usuario habilitarlo sólo en las páginas en las que confía.
  https://addons.mozilla.org/es/firefox/addon/noscript/
  https://chrome.google.com/webstore/detail/scriptsafe/oiigbmnaadbkfbmpbfijlflahbdbdgdf

CERT-PY Equipo de Respuestas ante Emergencias Cibernéticas
Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)
Gral. Santos y Concordia – Complejo Santos – Ofic. E14
cert@cert.gov.py | +595 21 201014 | +595 21 3276902
Asunción - Paraguay | www.cert.gov.py
@CERTpy
/CERT-Py

En caso de sospechar que una página web puede estar infectada, se recomienda realizar la denuncia a los organismos correspondientes; puede reportarlo al Centro de respuestas ante Incidentes Cibernéticos (CERT-PY).

Información adicional:

https://sophos.files.wordpress.com/2014/03/webc2a0threatsc2a0infographic.pdf
http://www.welivesecurity.com/la-es/2008/08/20/paginas-web-condicen-nada/
http://www.welivesecurity.com/la-es/2012/05/03/android-primer-malware-drive-by-download/
http://www.welivesecurity.com/la-es/2015/06/30/cryptowall-3-vulnerabilidad-flash-player/

CERT-PY Equipo de Respuestas ante Emergencias Cibernéticas
Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)
Gral. Santos y Concordia – Complejo Santos – Ofic. E14
cert@cert.gov.py | +595 21 201014 | +595 21 3276902
Asunción - Paraguay | www.cert.gov.py
@CERTpy
/CERT-Py