SDIGITALES

- Sistemas
- Software a Medida
- Soporte Corporativo
- Consultoría Informática

Pueyrredón 935 - (2630) Firmat
Tel. 03465-420494
Web: http://www.sdigitales.com.ar
Email: informacion@sdigitales.com.ar

Virus de Facebook que etiqueta personas en videos

El tema de este virus es complejo, pero en la gran mayoría de los casos, es involuntaria la participación de la persona etiquetada, quedando sin etiquetar, y obviamente, sin identificar, el infectado, y por lo tanto, el generador del problema.

El virus se ofrece como un video (puede ser pornografía, o cualquier otra cosa). Cuando se lo comienza a reproducir, muestra unos segundos de video, y se detiene, con un cartel que indica que se ha dañado el Flash Video Player (un plugin que se utiliza para reproducir videos), y ofrece un enlace para descargar una actualización y arreglarlo.

Obviamente, la actualización no es tal, sino que es un malware, que infecta la máquina. Según el blog de ESET:

"A diferencia de otras amenazas similares descubiertas anteriormente donde se enviaban mensajes a los contactos de la víctima con enlaces maliciosos, en esta ocasión se opta por etiquetar directamente a un número determinado de contactos de la víctima para que este vídeo se muestre también en sus perfiles, si estos no tienen activada la opción de revisar etiquetas."

"Además, el malware inyecta procesos en Google Chrome, que suelen encontrarse por defecto en C:\users\user\appdata\roaming\chromium.exe*. Al cerrar el navegador el proceso continúa activo, es decir, que el troyano sigue propagándose."*

Entre las funciones que posee el malware podemos destacar las siguientes:

- *Crea varias hooks (tareas) que monitorean y capturan las entradas del teclado y mouse. Esto le permite* ***tener capacidad de keylogger*** *(registra todo lo que se tipea en el teclado).*
- ***Roba información confidencial*** *contenida en el navegador.*
- *Se* ***autoinstala*** *en el arranque de Windows."*

Este virus, como tanto malware que se difunde a través de las redes sociales, usa conceptos de ingeniería social para infectar y copiarse, entre otras cosas:

- La curiosidad de las personas, al ser tentadas
- La falta de cuidado, o de prevención de riesgos, en función de esa curiosidad
- El desconocimiento del correcto uso de las redes sociales
- La falta de seguridad en los perfiles, debido a falta de conocimiento de los usuarios.
- La falta de seguridad en navegadores y equipos.

Es muy importante recalcar que las redes sociales son absolutamente inseguras, y tanto la misma red social, como las aplicaciones que habitualmente se corren en ellas tienen absoluto acceso a toda la información del perfil del usuario, incluido todo aquello considerado como privado (o sea, todo es público).

Esto es porque el objetivo de una red social es facturar, en función de venta de publicidad, y análisis de mercado basado en la información almacenada en los perfiles. Por ello hay tantas aplicaciones y juegos. No son gratis. Se cobran con información. (Tengan en cuenta que el desarrollo de un juego, por más simple que sea, puede tener un costo de varios miles de dólares).

Un malware de este tipo, entonces, aprovecha la ingenuidad del usuario, y las vulnerabilidades de la red social, nuestro navegador e instalación, para hacer su trabajo.

Por eso, recomiendo:

- No acepten ninguna sugerencia de actualización de software, si no es de la página del desarrollador del mismo.
- No compartan, ni acepten absolutamente nada sin estar 100% seguros de su origen.

Pueyrredón 935 - (2630) Firmat
Tel. 03465-420494
Web: http://www.sdigitales.com.ar
Email: informacion@sdigitales.com.ar

- No usar aplicaciones ni juegos de facebook. NO son gratis. Tienen acceso a nuestro equipo, a nuestra información (pública y privada), y siempre la usan para algo.
- Utilicen un navegador seguro. Recomiendo Maxthon, que no permite ejecutar plugins ni complementos. Mozilla Firefox, Google Chrome e Internet Explorer son MUY INSEGUROS.
- Manténganse protegidos con un buen antivirus. Recomiendo ESET (licencia paga) o Kaspersky (Licencia Paga). Los gratuitos son normalmente muy poco efectivos.

Hay forma de bloquear y prevenir el etiquetado. Fundamentalmente, usando y configurando correctamente Facebook.

Para ara configurar Facebook, de manera que cualquier etiqueta pase por nuestra supervisión antes de publicarse se deben seguir los siguientes pasos:

- Hacer click en el último ícono de la barra superior
- Tocar "Configuración"
- Tocar "Biografía y Etiquetado"
- Donde dice: "¿Quieres revisar las publicaciones en las que tus amigos te etiquetan....?" tocar "Editar" y seleccionar "Activado".
- También es conveniente, el el item "¿Quién puede publicar en tu biografía?" que este seleccionado "Amigos"
- Donde indica "¿Quieres revisar las etiquetas que otros agregan a sus publicaciones..." también dejar en "Activado".
- En "Cuando se etiqueta en una publicación, ¿a quién quieres agregar...", colocar en "Solo yo".
- En "Quien recibe sugerencias para etiquetarte en fotos..." configurar en "Nadie".

Lamentablemente, las etiquetas son un punto nefasto de Facebook, muy mal usado, y que hace muy vulnerable a cualquier perfil de ser incluido en contenido poco apropiado (como está pasando con este virus).

Cómo actuar ante algo que no queremos ver en Facebook:

Cuando detecten una publicación fraudulenta, sea resultante de este virus, u de otra clase, o con contenido ofensivo o perturbador, proceder de la siguiente manera:

- Tocar el símbolo de la fecha hacia abajo, en el ángulo superior derecho de la publicación.
- Del menú que aparece, hay que tocar "No quiero ver esto"
- Luego, elegir "Reportar publicación".
- Del nuevo menú, elegir la opción que mejor describe porque les parece que no se debe publicar, y tocar "Continuar". Puede aparecer un nuevo menú, para que especifiquen el motivo. Háganlo, y toquen nuevamente "Continuar".
- Finalmente, elijan "Enviar a Facebook para su revisión".
- Eventualmente, le pueden enviar un mensaje a la persona que hizo la publicación.
- Luego, tocar "Cerrar"

Con esto, mantendremos limpia de basura a la red social.

Enlaces de interés:

Blog de ESET:
NUEVO TROYANO SE PROPAGA POR FACEBOOK INFECTANDO A MÁS DE 100.000 USUARIOS

5 CONSEJOS PARA CONSEGUIR MEJOR PRIVACIDAD Y SEGURIDAD EN FACEBOOK

Pueyrredón 935 - (2630) Firmat
Tel. 03465-420494
Web: http://www.sdigitales.com.ar
Email: informacion@sdigitales.com.ar

Y TÚ, ¿CÓMO TIENES CONFIGURADA LA PRIVACIDAD DE TU FACEBOOK?

VECTORES DE PROPAGACIÓN MODERNOS: FACEBOOK, VÍDEOS IMPACTANTES Y COMPLEMENTOS DEL NAVEGADOR