VERSIÓN EN ESPAÑOL

UNAM CERT

OUCH! | Mayo 2014

Boletín mensual de seguridad para usuarios de computadoras

OUCH!

En esta edición...

- Resumen
- Indicadores de ataque
- Cómo actuar

Me hackearon ¿Ahora?

Resumen

Sabemos que te preocupa proteger tu computadora y tu información así como tomar las medidas necesarias para mantenerlos seguros. Aún así (igual que cuando conduces) no importa con qué tanta precaución lo hagas, tarde o temprano podrías verte involucrado en un accidente. En este boletín queremos enseñarte en qué debes fijarte para determinar si tu computadora fue hackeada, y en caso de ser así, qué puedes hacer al respecto. A fin de cuentas, mientras más rápido detectes si has sido hackeado y mientras más rápida sea tu respuesta, podrás mitigar de mejor manera el daño, tanto a tu organización como de forma personal.

Editor Invitado

Jake Williams (**@MalwareJake**; **malwarejake.blogspot.com**) es Científico en Jefe en CSR, Grupo Computer security Consultants, también es autor de los cursos Memory Forensics (FOR526) y Malware Reverse Ingineering (FOR610) del Instituto SANS.

Indicadores de ataque

Primero, es necesario que entiendas que no hay un paso único para determinar si tu computadora ha sido atacada, en lugar de ello, existen algunos indicadores. Si detectas algunos de ellos en tu equipo, esto indica que ha sido comprometido, aquí hay algunos ejemplos.

- Tu programa antivirus lanza una alerta que dice que tu equipo está infectado, principalmente si dice que no pudo remover o poner en cuarentena los archivos comprometidos.
- La página de inicio de tu navegador cambió sin razón alguna o bien, te lleva a sitios en los que no querías navegar.
- Hay nuevas cuentas de usuario en tu computadora que tú no creaste.
- Hay nuevos programas corriendo que tú no instalaste.
- Tu computadora colapsa continuamente o corre muy lento.
- Un programa en tu computadora solicita autorización para hacer cambios en el sistema, sin embargo, tú no estás actualizando o instalando aplicación alguna en ese momento.
- El firewall lanza alertas de un programa que no reconoces y que solicita conectarse a Internet.

Me hackearon ¿Ahora?

Cómo actuar

Si tú crees que tu computadora ha sido comprometida, mientras más pronto reacciones, será mejor. Si el equipo que tienes es propiedad de tu empresa o lo usas para tu trabajo, no trates de reparar el daño tú mismo y tampoco apagues el equipo. Probablemente no solo estarías causando más daño que beneficios, sino que podrías destruir evidencia cuantiosa que puede ser usada para investigación. En lugar de eso, reporta el incidente a tu organización de inmediato, usualmente sería contactando al servicio de mantenimiento, al quipo de seguridad o a tu jefe directo. Si por alguna razón no puedes contactar a tu compañía o te preocupa que se generen atrasos, desconecta tu computadora de Internet y ponla en modo de reposo, suspensión o en modo hibernación. Incluso si no estás seguro de haber sido hackeado, es mucho mejor reportarlo para evitar sorpresas. Tu compañía tiene mejor conocimiento y personal para manejar este tipo de situaciones, permíteles hacer ese trabajo.

Tarde o temprano tu computadora podría estar bajo ataque, cuanto más rápido detectes un incidente y reacciones ante él, el resultado será mucho mejor.

Si tu computadora, al contrario, es para uso personal, aquí hay algunos pasos que puedes realizar:

- **Respaldos**. El paso más importante es prepararte para lo que viene con una copia de seguridad. Específicamente te recomendamos resguardar tus datos de forma regular y periódica, además, verifica que tus respaldos sí son recuperables en caso de que tengas que usarlos. En algunas ocasiones, la única forma de recuperarse de un ataque es restablecer el sistema desde cero o bien, comprar un nuevo equipo, para estos casos es mejor estar preparado con una copia de seguridad.
- **Cambia tus contraseñas**. Asegúrate de cambiarlas todas. Esto incluye, además de las contraseñas de tus equipos de cómputo y dispositivos móviles, todas las contraseñas de servicios en línea. Asegúrate de cambiarlas desde un equipo que sepas que es seguro.
- **Antivirus**. Si tu software antivirus te informa de un archivo infectado, puedes seguir las siguientes acciones que te recomienda. Usualmente consisten en poner el archivo en cuarentena, limpiar el archivo o borrarlo, la mayoría de los antivirus tienen ligas con más información de la amenaza que te está atacando. Si tienes dudas, pon el archivo en cuarentena, si no es posible, entonces bórralo.
- **Reinstalar**. Si no fue posible limpiar la computadora por medio del antivirus, una de las formas más seguras de recuperarse es reinstalar el sistema por completo. Primero desconecta tu equipo de la red. Sigue las instrucciones

Me hackearon ¿Ahora?

que vienen con él, en la mayoría de los casos esto implica usar la partición de recuperación que viene en el disco duro para reinstalar el sistema operativo. Si la partición de recuperación está dañada o infectada, contacta al fabricante y solicita un disco de recuperación, no reinstales el sistema operativo desde los respaldos. Estos respaldos podrían tener las mismas vulnerabilidades con las que el atacante logró entrar en tu sistema. Los respaldos sólo deben usarse para recuperar tu información personal. Si tu computadora o sistema operativo están descontinuados, es mucho más sencillo y a veces barato comprar un equipo nuevo que intentar recuperar el dañado.

- **Ayuda profesional**. Si estás preocupado por haber sido hackeado, pero crees que no tienes las habilidades o conocimientos para resolverlo, podrías llevar tu equipo con un profesional. Por ejemplo, después de ser hackeado, podrías darte cuenta de que tus respaldos están incompletos o demasiado obsoletos y podrías sentirte tentado a transferir algunos documentos entre tu computadora infectada y la nueva, podría ser que sin darte cuenta, estés transfiriendo malware en tu equipo nuevo al mismo tiempo que tus documentos. En este caso podrías llevar tu equipo con un profesional que logre recuperar tu información sin transferir la amenaza al nuevo equipo.

Conoce más

Suscríbete al boletín mensual de conciencia sobre seguridad OUCH!, consulta los archivos OUCH! y aprende más acerca de las soluciones de seguridad SANS visitando: http://www.securingthehuman.org

Versión en español

UNAM-CERT, Equipo de Respuesta a Incidentes de Seguridad de la Información en México reconocido ante FIRST, es una referencia en la materia en este país.

Sitio web: http://www.seguridad.unam.mx

Síguelo en Twitter @unamcert

Recursos

OUCH! Respaldos:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201309_sp.pdf
OUCH! Contraseñas:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201305_sp.pdf
OUCH! Qués es el malware:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201402_sp.pdf
Detecting Evil Poster:	https://digital-forensics.sans.org/media/poster_2014_find_evil.pdf

Consejo editorial: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Traducción al español por: Erika Ródriguez e Israel Rubí