VERSIÓN EN ESPAÑOL
UNAM CERT

OUCH! | Abril 2016

Boletín mensual de seguridad para usuarios de computadoras

OUCH!

En esta edición...

He sido hackeado, ¿y ahora qué?

Resumen

Sabemos que te importa la protección de tu computadora y tus dispositivos móviles, así como tomar medidas para asegurarlos. Sin embargo, no importa qué tan segura sea la tecnología que utilizas, tarde o temprano tu equipo podría ser comprometido o "hackeado". En este boletín aprenderás cómo determinar si has sido hackeado y, si es así, qué puedes hacer al respecto. En última instancia, entre más rápido detectes que algo está mal, es más probable que reduzcas el daño que un ciberatacante pueda causar.

Editor Invitado

Samantha Davison es la Directora del Programa de Educación y Conciencia sobre Seguridad en Uber, dedicado a educar a los empleados de la compañía en más de 350 ciudades en todo el mundo. Puedes encontrar a Samantha en Twitter como **@Sam_E_Davison**.

Pistas de que has sido hackeado

Si bien puede ser difícil determinar si has sido hackeado, ya que a menudo no hay una forma única de averiguarlo, los ciberatacantes suelen dejar varias pistas a menudo llamadas indicadores. Cuanto más cerca estés de coincidir con alguna de estas pistas en tu sistema, es más probable que hayas sido hackeado:

- Tu programa antivirus ha emitido una alerta de que tu sistema está infectado, sobre todo si dice que es incapaz de eliminar o poner en cuarentena los archivos afectados.
- La página de inicio de tu navegador se ha cambiado inesperadamente o el navegador te lleva a sitios web que no quieres ir.
- Hay nuevas cuentas en tu computadora o dispositivo que no has creado o nuevos programas en ejecución que no instalaste.
- El equipo o las aplicaciones fallan constantemente, hay iconos para aplicaciones desconocidas o aparecen ventanas extrañas.
- Un programa solicita tu autorización para realizar cambios en el sistema, aunque no estás instalando o actualizando de forma activa alguna de tus aplicaciones.
- Tu contraseña ya no funciona cuando intentas iniciar sesión en el sistema o una cuenta en línea, a pesar de saber que la contraseña es correcta.
- Tus amigos te preguntan sobre correos electrónicos que tú no enviaste.
- Tu dispositivo móvil realiza cargos no autorizados a números premium de SMS.

He sido hackeado, ¿y ahora qué?

- El dispositivo móvil registra un alto e inexplicable uso de datos o de batería.

Cómo responder

Si sospechas que tu computadora o dispositivo ha sido comprometido, mientras más rápido respondas, mejor. Si ocurre en el equipo que te fue proporcionado por tu empresa o que usas para el trabajo, no trates de solucionar el problema por ti mismo. No sólo puedes causar más daño, sino que podrías destruir evidencia valiosa para una investigación. En su lugar, reporta el incidente a tu empresa inmediatamente contactando al soporte técnico, al equipo de seguridad o al supervisor. Si por alguna razón no puedes contactar a tu organización o estás preocupado por un retraso, desconecta tu computadora o dispositivo de la red y luego activa la hibernación, suspensión o modo avión. Incluso si no estás seguro de que tu equipo ha sido comprometido, es mejor reportarlo pronto, por si acaso. Si la computadora o dispositivo es de uso personal, aquí hay algunos pasos que te ayudarán:

Tarde o temprano tu dispositivo podría ser comprometido, mientras más rápido detectes un incidente y pronto respondas, mejor.

- **Cambia tus contraseñas**: Esto incluye no sólo cambiar las contraseñas en tus computadoras y dispositivos móviles, sino también para todas tus cuentas en línea. Asegúrate de no usar la computadora comprometida para cambiar las contraseñas.
- **Antivirus**: Si tu programa antivirus te informa sobre un archivo infectado, puedes seguir las acciones recomendadas. Usualmente incluye poner el archivo en cuarentena, desinfectarlo o eliminarlo. La mayoría de los programas antivirus proporcionan vínculos para aprender más sobre la infección en cuestión. Ante la duda, deja el archivo en cuarentena. Si no es posible, elimínalo.
- **Reconstruir**: Si eres incapaz de reparar la infección o quieres estar absolutamente convencido de que tu sistema está reparado, una opción más segura es reconstruirlo. En el caso de las computadoras, sigue las instrucciones del fabricante. En la mayoría de los casos, significa usar las utilidades precargadas para reinstalar el sistema operativo. Si dichas utilidades están ausentes, corrompidas o infectadas, contacta a tu proveedor para recibir orientación o visita su sitio web. No reinstales el sistema operativo usando respaldos, ya que podrían tener las mismas vulnerabilidades que permitieron al atacante obtener acceso originalmente. Los respaldos sólo deben ser usados para recuperar tu información. En dispositivos móviles, sigue las instrucciones del fabricante del dispositivo o proveedor del servicio, las cuales deberían estar en su sitio web. En varias ocasiones, esto puede ser tan simple como restaurar tu dispositivo móvil a los valores de fábrica. Si te sientes incómodo con el proceso, considera contratar un servicio profesional para ayudarte. Si tu computadora o dispositivo es antiguo, podría ser más simple

He sido hackeado, ¿y ahora qué?

e incluso más barato comprar uno nuevo. Finalmente, una vez que has reconstruido tu computadora o dispositivo, o comprado uno nuevo, asegúrate de que esté completamente actualizado y sea lo más reciente posible y activa las actualizaciones automáticas para instalarse cuando estén disponibles.

- **Respaldos**: El paso más importante que puedes realizar para protegerte a ti mismo es prepararte ante eventualidades con respaldos regulares. Mientras más respaldos generes regularmente, mejor. Algunas soluciones generan automáticamente, cada hora, respaldos de cualquier archivo nuevo o modificado. Sin importar que solución utilices para generar respaldos, verifica periódicamente que eres capaz de restaurar los archivos. Con frecuencia usa los respaldos para recuperar información, ya que es la única forma en que puedes restablecer el equipo comprometido.
- **Aplicación de las leyes**: Si te sientes amenazado de alguna forma, reporta el incidente a las autoridades locales.

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

Software antivirus:	http://www.seguridad.unam.mx/usuario-casero/eduteca/main.dsc?id=116
Respaldos y recuperación:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201508_sp.pdf
Consejos para una navegación segura:	
http://revista.seguridad.unam.mx/numero-09/consejos-para-una-navegaci%C3%B3n-segura	
Buenas prácticas de seguridad:	http://www.seguridad.unam.mx/usuario-casero/eduteca/main.dsc?id=149
Consejos de seguridad UNAM-CERT:	http://www.seguridad.unam.mx/usuario-casero/consejos/

Consejo editorial: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Traducción: Mario Vasquez, Oscar Flores, Katia Rodríguez