HSBC

Juntos prosperamos

HSBC*net*
Malware

Riesgos para sus negocios: Pérdida de datos | Pérdida financiera | Daños al hardware | Paralización de la actividad empresarial

El software malicioso está codificado con la intención de perjudicar a su objetivo. Afecta a usuarios particulares y corporativos por igual, y puede robar información, dañar los datos, apropiarse de las visitas a sitios web y espiar la actividad en Internet. Actualmente, una de las formas de ataque más frecuentes es la redirección fraudulenta de los usuarios de banca por Internet.

¿Qué es el malware?

El malware puede ocultarse dentro de un software de aspecto inofensivo (troyanos) o diseminarse entre máquinas sin depender de la interacción de los usuarios (gusanos). Puede estar diseñado específicamente para evadir las defensas y ejecutar tareas determinadas.

Una vez instalado sin que el usuario lo perciba, el malware puede realizar muchas actividades invisibles. Puede espiar los sitios web que visita, destruir datos o reconstituir sus contraseñas. Los delincuentes lo utilizan cada vez más para cifrar la información empresarial importante hasta que la organización pague un "rescate" por ella. Además, los usuarios de banca por Internet podrían ser redirigidos a sitios falsos que registran sus datos de inicio de sesión para facilitar los robos financieros.

Los malware normalmente se envían a través de correos electrónicos o links fraudulentos. Las aplicaciones malintencionadas y las memorias USB también pueden poner en peligro a teléfonos inteligentes y computadoras, respectivamente. El malware puede permanecer oculto durante meses hasta que se active.

68% de las infracciones de seguridad de negocios **se deben a virus, spyware y malware.**

El Instituto AV-Test registra 390,000 **programas maliciosos cada día.**

Tipos de malware:

- **Spyware**
- **Ransomware**
- **Troyanos**
- **Keyloggers**

Cómo mantener su negocio seguro:

- Tome medidas de respuesta sólidas, como procesos de recuperación y copias de seguridad.
- Ejecute un software de antivirus actualizado en todos los equipos de su organización en forma regular y programada. Realice análisis de antivirus a menudo puede servir para minimizar el riesgo de ataques de malware.
- Mantenga sus computadoras, servidores y hardware asociados actualizados, instale los parches de seguridad más recientes a medida que estén disponibles.
- Asegúrese de que su personal evite sitios web cuestionables y que no descarguen software o aplicaciones gratuitas, que no ejecuten macros de MS Office en archivos adjuntos de correo electrónico ni utilicen memorias USB de fuentes no verificadas.
- Considere utilizar listas de aplicaciones de confianza (que bloquean cualquier software que no esté autorizado).
- Utilice contraseñas diferentes para diferentes inicios de sesión de negocios.
- Si sospecha que fue víctima de un fraude, comuníquese con su representante de HSBC inmediatamente.

Si sospecha que fue víctima de un fraude, comuníquese con su representante de HSBC inmediatamente.

Fuentes: https://www.gov.uk/government/publications/cyber-security-breaches-survey-2016; http://www.clearswift.com/blog/2016/05/24/10-shocking-malware-and-ransomware-statistics