¿Sabe cómo se roban sus datos?

Lunes, 05 de Octubre de 2015 09:19 **Redacción Canal Informático**

Rees Johnson

Intel Security concluyó recientemente una investigación para poder responder a estas preguntas y se obtuvieron descubrimientos muy interesantes.

Son las 11:00 p.m. ¿Sabe dónde están sus datos o quién se los está robando? ¿Sabe cómo los robaron? o al menos, ¿sabe dónde estaban cuando fueron sustraídos?

La mayoría de los informes de robo de datos se concentran en cómo se infiltraron a la organización los delincuentes, en lo que no funcionó para detenerlos, y en qué información fue robada. Es frecuente preguntarse cómo se pudo sustraer la información ¿Cómo se sacó, o se exfiltró?, y ¿quién probablemente lo hizo?

Intel Security concluyó recientemente una investigación para poder responder a estas preguntas y se obtuvieron descubrimientos muy interesantes.

La más probable es que los ladrones pertenezcan a la delincuencia organizada, o sean hackers activistas, aunque se ha descubierto que algunas personas que pertenecen a la organización son cómplices en el 40% de los robos, según un estudio que Intel Security publicó el 15 de septiembre.

Cuando las personas que pertenecen a una organización estuvieron involucradas en un robo de datos, incluyendo a empleados, contratistas, y proveedores, la mitad de las violaciones fueron intencionales, y la otra mitad accidentales.

Hemos preguntado a los profesionales de seguridad de medianas y grandes empresas sus preocupaciones y desafíos en relación al robo de datos. Los dos primeros lugares correspondieron a la cada vez mayor sofisticación de los atacantes, y al predominio de las amenazas externas maliciosas.

En promedio, los profesionales a los que encuestamos sufrieron seis violaciones de seguridad de datos que generaron exfiltración de datos a lo largo de sus carreras, y cuatro de esos incidentes fueron lo suficientemente graves como para afectar negativamente a las finanzas de la compañía o requerir de divulgación pública. Sólo la mitad de las violaciones fueron descubiertas por los equipos de seguridad interna. La otra mitad se encontró en diversas entidades externas, como hackers éticos, organismos de seguridad pública, y compañías de tarjetas de crédito.

Los ladrones de datos están interesados en cada uno de los fragmentos de información de carácter personal que su compañía recolecta de clientes y empleados, desde nombres y direcciones hasta números de cuenta e información de su institución de salud. Más del 60% de los incidentes de robo de datos involucraron información personalmente identificable, siendo que el resto involucró otra información valiosa de carácter financiero y de pagos (25%) o de propiedad intelectual (14%). Los datos estructurados, robados de bases de datos, son los más susceptibles de robo cuando se miden por cantidad. Sin embargo, cuando se les pregunta cuál es la proporción de incidentes que involucraron distintos formatos de datos, los documentos de Microsoft Office fueron el formato más robado, seguido

de archivos CSV y PDF.

Cómo se extraen los datos es quizás uno de los descubrimientos más interesantes de la encuesta. La sustracción física estuvo involucrada en un 50% de los robos, se informó que fueron realizados por gente que pertenece a la organización, especialmente laptops y unidades USB, y en un 40% de los robos realizados, fueron por personas ajenas a la organización. Cuando se aprovecharon las redes para robar datos, los protocolos de archivos y túneles fueron el mecanismo principal de transporte (25%), seguido de protocolos web (24%), y correo electrónico (14%). Sin embargo, los cada vez más sofisticados atacantes están utilizando una gran variedad de protocolos y técnicas para sacar los datos, incluyendo peer-to-peer, secure shell, mensajería instantánea, voz sobre IP, y datos ocultos dentro de imágenes o video. También están disfrazando los datos para pasarlos a través de las defensas, utilizando cifrado, compresión y otras técnicas de camuflaje, haciendo que sea cada vez más desafiante evitar el robo de datos. Para obtener una explicación detallada de los motivos que tienen los atacantes, sus objetivos y sus métodos de exfiltración, lea "Exfiltración de datos: un paso importante en la jornada del ciberladrón" en el recién publicado Informe de Amenazas de McAfee Labs: Agosto de 2015.

El comprender los objetivos, motivos y técnicas de los ciberladrones es importante para detectar la exfiltración de datos y prevenir la fuga de éstos.

Algunos de los pasos más importantes que le ayudarán a combatir el robo de datos son:

· Crear un inventario de datos para ayudar a priorizar las defensas.

· Identificar los flujos de datos normales para información delicada. El movimiento anormal de datos frecuentemente es el primer signo de que hay riesgo.

· El software de Data Loss Prevention (DLP) añade controles adicionales a los movimientos de datos y, junto con los sistemas de detección y prevención de intrusiones, representa la mayor parte de descubrimientos de violaciones de datos.

· El software de gestión de políticas y riesgos proporciona la revisión y supervisión que se necesitan para proteger sus datos sensibles, al mismo tiempo que los mantiene accesibles para las personas que los necesitan para realizar su trabajo.

Juntas, estas herramientas defienden a profundidad su red y le ayudan a saber dónde están sus datos y dónde han estado, y de esta forma evitar que los roben.

Comentarios

No hay comentarios publicados aún. ¡Sé el primero!

Publicar un nuevo comentario

¡ingresa el texto justo aquí!

Comentar como invitado o iniciar sesión:

Nombre

Se muestra junto a tus comentarios.

Correo electrónico

No se muestra públicamente.

Sitio web (opcional)

Si tienes un sitio web, ingresa la liga aquí.

Suscribirse a Ninguno

Enviar comentario