MANDIANT
A FireEye® Company

PANORAMA DE LAS AMENAZAS: EN NÚMEROS

2015 fue un año en el que se rompieron todos los récords. Más ataques se hicieron públicos que cualquier otro año, y más grupos de ciberdelincuentes fueron identificados operando a nivel mundial, incitados por una mayor diversidad de motivos. Estos grupos infiltraron y destruyeron sistemas, sustrajeron información personal y atacaron dispositivos de comunicación de red. Esto dio lugar a más estrés para los responsables de prevenir la pérdida de datos y la reputación; más tiempo y más dinero fueron necesarios en la recuperación de cada ataque y más razones estimularon a las organizaciones para fortalecer su posición de seguridad.

TRES NUEVAS TENDENCIAS APARECIERON EN 2015:

- Interrupción al negocio
- Robo de información personal de identificación
- Ataques a ruteadores y switches

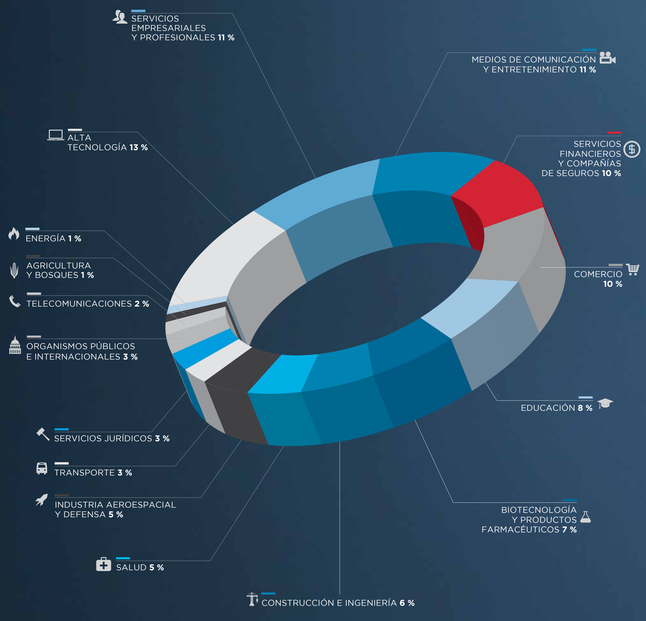
DOS TENDENCIAS ANTERIORES PERSISTIERON:

- Uso de mecanismos de persistencia
- Ataques a proveedores de servicios externos

EL AÑO EN ATAQUES

SECTORES INVESTIGADOS POR MANDIANT

Porcentaje del total de ataques por sector.



MÁS Y MENOS

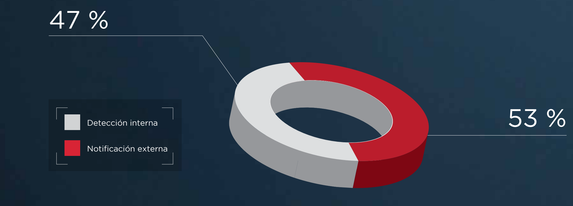
Algunos sectores han experimentado más ataques en relación a 2014, mientras que otros han sufrido menos.

ALTA TECNOLOGÍA	SERVICIOS EMPRESARIALES Y PROFESIONALES
6 % ↑	6 % ↓

MÁS ATAQUES DESCUBIERTOS INTERNAMENTE

Comparado con 2014, el porcentaje de víctimas que descubren un ataque internamente ha aumentado un 16 %.

16 % ↑



LAS ORGANIZACIONES MEJORAN LA VIGILANCIA

En 2015, el tiempo promedio desde cuando un ataque sucede hasta cuando es descubierto se redujo en 59 días (205 en 2014).

TIEMPO DESDE EL ATAQUE HASTA EL DESCUBRIMIENTO		
PROMEDIO	NOTIFICACIÓN EXTERNA	DETECCIÓN INTERNA
146 DÍAS	320 DÍAS	56 DÍAS

MÁS LECCIONES APRENDIDAS

Un año marcado por ataques con importantes consecuencias ha dejado nuevas lecciones en cuanto a defensa y respuesta.

1. **Confirme** que se ha producido un ataque.
2. No olvide que los adversarios son **seres humanos**. Sus reacciones pueden ser imprevisibles.
3. **El tiempo es crítico:** valide y evalúe la amplitud del ataque lo antes posible.
4. **Esté atento** : se verá inmerso en una carrera contrarreloj.
5. **Evalúe cuidadosamente** la posibilidad de enfrentarse a un agresor (véase el punto 2).
6. Involucre a expertos **antes** de un ataque, para obtener ayuda sobre análisis forense, cuestiones legales y relaciones públicas.
7. **Considere todas las opciones** cuando le soliciten el pago de un rescate. No existe garantía alguna de que recupere lo robado.
8. **Asegure** una fuerte segmentación y controles eficaces en sus copias de seguridad.
9. **Una vez** solucionado un incidente, debe centrarse en una mejora general de la seguridad.
10. Si consigue eliminar a los agresores, esté preparado: **ellos pueden volver en cualquier momento.**

MÁS INFORMACIÓN

Obtenga el informe M-Trends 2016 en **fireeye.com/M-Trends-2016.html**

FireEye, Inc.
1440 McCarthy Blvd. Milpitas, CA 95035
408.321.6300 / 877.FIREEYE (347.3393) / info@FireEye.com
fireeye.com

FireEye