# Ransomware: la realidad

¡Ya está aquí, es sofisticado y es astuto!

Pérdida de datos confidenciales y de propiedad exclusiva

Pérdidas financieras

Interrupciones

Daño a la reputación

## Malware con un precio elevado.

## **Reconozca** la creciente amenaza

### 2015

**NÚMERO 3** en la lista[1] de "Temas Centrales para 2015" del FBI

**Tomando impulso**

**USD 24 millones** extorsionados en más de 2400 reclamos al FBI[2]

Campaña frustrada por **USD 60 millones** del Kit de Ataque Angler[3]

### 2016

**"El año del rescate"**

**USD 209 millones** extorsionados en los primeros tres meses[4]

Se esperan ganancias **USD 1000 MILLONES** por en 2016[5]

**Un aumento sextuplicado** en ataques a usuarios corporativos[6]

## **Conozca** los vectores de ataque

Los kits de ataque son herramientas utilizadas por atacantes para distribuir malware. A menudo, se envían a través de:

- **Correo electrónico:** mensajes de suplantación de identidad y correo electrónico no deseado con enlaces o adjuntos maliciosos
- **Servidores Web:** puntos de ingreso para acceso a la red
- **Aplicaciones en línea:** archivos cifrados propagados por medios sociales y mensajería instantánea
- **Publicidad maliciosa:** descargas desapercibidas a través de un sitio infectado

| Vector de Infección | Comando y Control | Cifrado de Archivos | Solicitud de Rescate |
|---|---|---|---|
| Utiliza con frecuencia la web y el correo electrónico | Toma el control de sistemas dirigidos | Los archivos se tornan inaccesibles | El propietario/empresa paga el rescate (bitcoins) para liberar el sistema |

## **Evite ataques** con un enfoque arquitectónico:

- Protección en la capa DNS, terminales, correo electrónico, web y red
- Asegure los dispositivos tanto dentro como fuera de la red
- Prepárese para detectar y contener el movimiento de malware rápidamente

## **Detecte e interrumpa el** ransomware

Cisco Talos interrumpe un ataque de ransomware anual por **USD 60 millones**

Uno de los kits de ataque más grandes y más avanzados, conocido como Angler, se utilizó en campañas de publicidad maliciosa dirigidas

Se detuvo el ataque a **90 000 víctimas** por día por **USD 30 millones** anuales en casi **150 servidores proxy**

## Obtenga más información hoy mismo

Ingrese en **cisco.com/go/ransomware** para consultar el enfoque simple, abierto, automatizado y eficaz de Cisco para la seguridad.

CISCO

[1]EE.UU. Ministerio de Justicia, Oficina Federal de Investigación, Informe de Delitos de Internet de 2015, https://pdf.ic3.gov/2015_IC3Report.pdf
[2]La Oficina Federal de Investigación, "Ransomware: Última Herramienta de Extorsión Cibernética", abril de 2016 https://www.fbi.gov/cleveland/press-releases/2016/ransomware-latest-cyber-extortion-tool
[3]Talos, Threat Spotlight: Cisco Talos impide el acceso al Kit de Ataque Internacional Masivo, lo cual genera USD 60 m anuales solamente de ransomware, octubre de 2015, http://www.talosintelligence.com/angler-exposed/
[4]CNN Money, "Se disparan las pérdidas por extorsión cibernética", afirma el FBI," David Fitzpatrick y Drew Griffin, abril de 2016, http://money.cnn.com/2016/04/15/technology/ransomware-cyber-security/
[5]Ibid.
[6]Security Week, "Historia y Estadísticas de Ransomware," Kevin Townsend, junio de 2016, http://www.securityweek.com/history-and-statistics-ransomware
[7]Cisco Talos, Threat Spotlight: Cisco Talos impide el acceso al Kit de Ataque Internacional Masivo, lo cual genera USD 60 m anuales solamente de ransomware, octubre de 2015, http://www.talosintelligence.com/angler-exposed/