

Ransomware: la realidad

¡Ya está aquí, es sofisticado y es astuto!



Pérdida de datos confidenciales y de propiedad exclusiva



Interrupciones



Pérdidas financieras



Daño a la reputación

Malware con un precio elevado.



Reconozca la creciente amenaza



NÚMERO 3 en la lista¹ de "Temas Centrales para 2015" del FBI

USD 24 millones extorsionados en más de 2400 reclamos al FBI²

Campaña frustrada por

USD 60 millones del Kit de Ataque Angler³

2015

Tomando impulso



2016

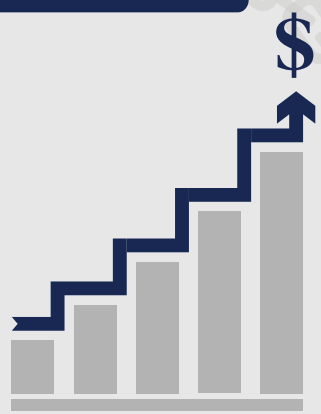
"El año del rescate"

USD 209 millones

extorsionados en los primeros tres meses⁴

Se esperan ganancias **USD 1000 MILLONES** por en 2016⁵

Un aumento sextuplicado en ataques a usuarios corporativos⁶



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



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.



¹EE.UU. Ministerio de Justicia, Oficina Federal de Investigación, Informe de Delitos de Internet de 2015, https://pdf.ic3.gov/2015_IC3Report.pdf

²La 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>

³Talos, 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/>

⁴CNN 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/>

⁵Ibid.

⁶Security Week, "Historia y Estadísticas de Ransomware," Kevin Townsend, junio de 2016, <http://www.securityweek.com/history-and-statistics-ransomware>

⁷Cisco 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/>