# El interior del *ransomware*

La evolución de esta amenaza la ha convertido en el tipo de *malware* más rentable en la historia.

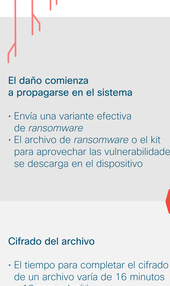

Por años los cibercriminales lo han usado para obtener grandes cantidades de dinero. Por ejemplo,en 2016 reportó ganancias por más de 1,000 millones de dólares a los cibercriminales.[i]

**+50%** de las compañías en Estados Unidos han experimentado un incidente de *ransomware*.

**60%** de los ataques a empresas exigen 1,000 dólares o más.[iii]

**50%** de las víctimas de *ransomware* en Estados Unidos paga el rescate.

**40%** de las víctimas de *ransomware* en todo el mundo paga el rescate.[iv]




## Noticia:

***Orange County Transportation Authority***[v]

Un ataque de *ransomware* encriptó los archivos de 88 servidores

Se exigió el pago de un rescate por 8,500 dólares

OCTA eligió no pagar. Tiempo para restaurar la información: 2.5 días

Costo total: 600,000 dólares

# Cómo funciona el *ransomware*

### Vector de infección

El usuario hace clic en la liga de un sitio afectado, publicidad maliciosa (*malvertising*), una liga en un correo electrónico de phishing o un archivo adjunto infectado con un virus informático.

Los vectores de ataque más comunes son:

- Correo electrónico: El 46% de los ataques de *ransomware* de todo el mundo se originan por este medio[vi]
- Vulnerabilidades de software popular: Flash ha sido el medio de aproximadamente el 80% de los intentos de ataque exitosos causados por vulnerabilidades[vii]

### El daño comienza a propagarse en el sistema

- Envía una variante efectiva de *ransomware*
- El archivo de *ransomware* o el kit para aprovechar las vulnerabilidades se descarga en el dispositivo

### Comunicaciones de comando y control (*C2 comms*) y el intercambio de llaves asimétricas

- Se realiza una devolución de llamada (*callback*) hacia la infraestructura con el *ransomware* malicioso
- Aparecen en promedio más de 1,000 nuevas variantes de código de *ransomware* por día[viii]

### Cifrado del archivo

- El tiempo para completar el cifrado de un archivo varía de 16 minutos a 18 segundos[ix]
- La información del dispositivo es cifrada cuando el *ransomware* recupera las llaves privadas, codificando tantos archivos como le sea posible

### Petición de rescate

- Cuando el cifrado ha sido completado, el código despliega un mensaje de rescate
- La víctima paga el rescate o busca hacer una recuperación, o ambos

*"Aunque el ransomware es una amenaza que crece y evoluciona constantemente, existen maneras de remediar sus ataques. Una de las mejores maneras de combatir este problema es contar con grandes herramientas en su arsenal. Cisco Umbrella ofrece la visibilidad necesaria para bloquear el tráfico hacia sitios maliciosos y provee las herramientas para investigar un problema existente."*

– **Freud Alexandre**, Gerente de Seguridad y Arquitectura Empresarial, Ciudad de Nueva Orelans

# Una estrategia multicapa de defensa



Prevenga:

- Respalde toda su información crítica
- Proteja a los usuarios sin importar en dónde se encuentren ellos o sus laptops
- Gestione los parches de manera consistente e integral

Detecte y detenga:

- Monitoree sus redes continuamente
- Identifique los kits de *malware* que aprovechan vulnerabilidades y evite que se ejecute el código malicioso
- Bloquee el tráfico malicioso de comando y control, los archivos maliciosos y los URLs maliciosos en correos electrónicos





Reduzca el riesgo de infección:

- Desarrolle un plan de seguridad proactiva que aproveche una defensa multicapa
- Use inteligencia predictiva para entender en qué parte de Internet se encuentran los ataques
- Mejore continuamente la higiene de la red y evalúe su postura de seguridad



*"La primera protección contra el ransomware es el entrenamiento de los usuarios. Cuando esta falla, usted necesita tener sistemas como Cisco Umbrella y Cisco ASA with Firepower para establecer capas de protección en el momento en que sus usuarios inevitablemente hagan clic sobre un archivo adjunto o una liga."*

– **Tyker Warren**, Consultor de Seguridad, Prologis

Para más información sobre cómo proteger a su negocio contra las amenazas del *ransomware*, visite:

https://www.cisco.com/c/es_mx/solutions/security/ransomware-defense/index.html



[i] David Fitzpatrick and Drew Griffin, "Ransomware is expected to gross cybercriminals $1 billion in 2016 says FBI," CNN Money, 11 de abril, 2016 (http://money.cnn.com/2016/04/15/technology/ransomware-cyber-security/)

[ii] "40 Percent of Enterprises Hit by Ransomware in the Last Year," Security Magazine, 4 de agosto, 2016 (http://www.securitymagazine.com/articles/87332-percent-of-enterprises-hit-by-ransomware-in-the-last-year)

[iii] Ibid.

[iv] Ibid.

[v] Nick Gerda, "Transportation Authority Kept Secret Cyber Attack That Cost $600,000," VoiceQC, 2 de agosto, 2016 (https://voiceofqc.org/2016/08/transportation-authority-kept-secret-cyber-attack-that-cost-600000/)

[vi] "40 Percent of Enterprises Hit by Ransomware in the Last Year," Security Magazine, 4 de agosto, 2016 (http://www.securitymagazine.com/articles/87332-percent-of-enterprises-hit-by-ransomware-in-the-last-year)

[vii] Cisco, "Cisco 2016 Midyear Cybersecurity Report," 2016

[viii] Rick Correa, "How Fast Does Ransomware Encrypt Files? Faster than You Think," Barkly, 2016 (https://blog.barkly.com/how-fast-does-ransomware-encrypt-files)

[ix] Ibid.