OWASP
Open Web Application Security Project
Perú Chapter

Anatomía de un ataque ransomware

Jorge Córdova Pelayo

En seguridad, no existen segundas oportunidades

Lima, 23 de noviembre de 2016

Agenda

- Objetivos de la charla
- ¿Qué es un ransomware?
- ¿Cómo nos afecta?
- Métodos de infección
- Explotación
- Comunicación a un Centro de Control
- Cifrado del documentos
- Pago de chantaje
- Descifrado
- Contramedidas

¿Listos?

Objetivos

- Entender cómo el ransomware está afectando a las organizaciones actuales.
- Entender cómo funciona un ransomware y las contramedidas para mitigar los riesgos de infección y pérdida de información.

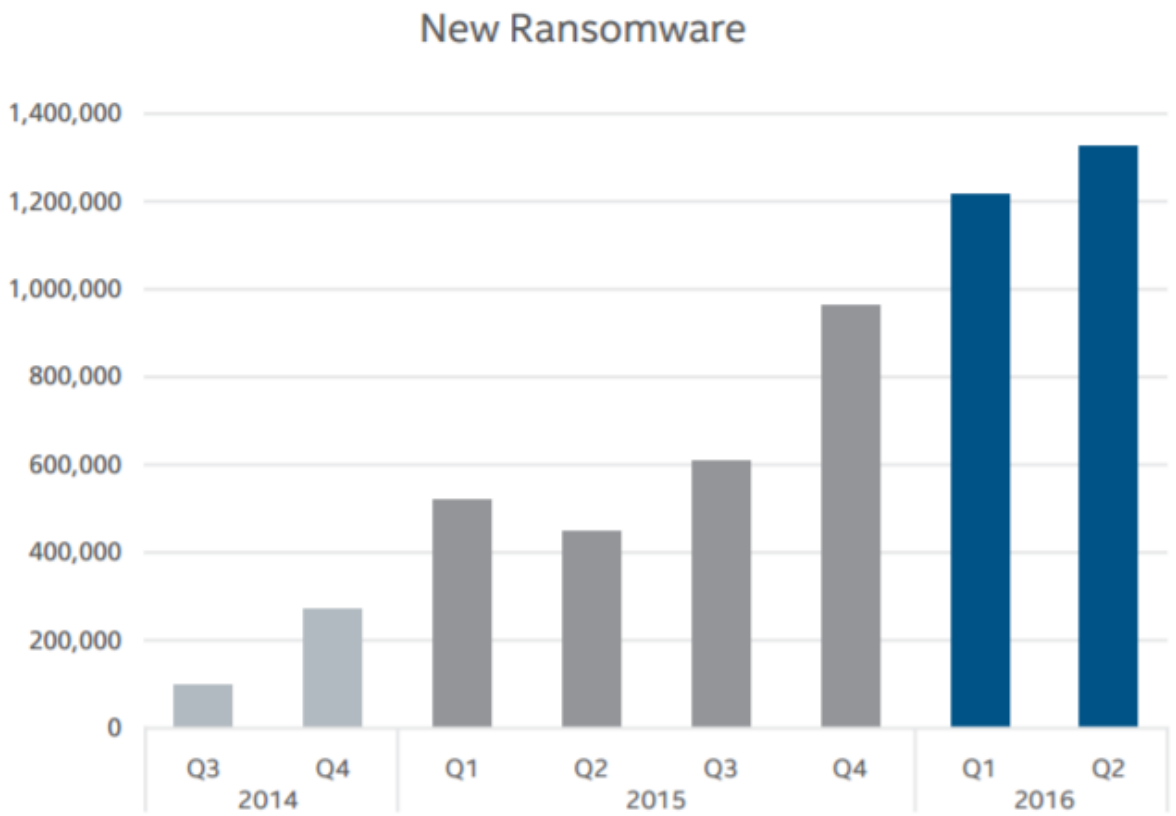
¿A quién le apareció una ventana así?

¿Qué es un ransomware?

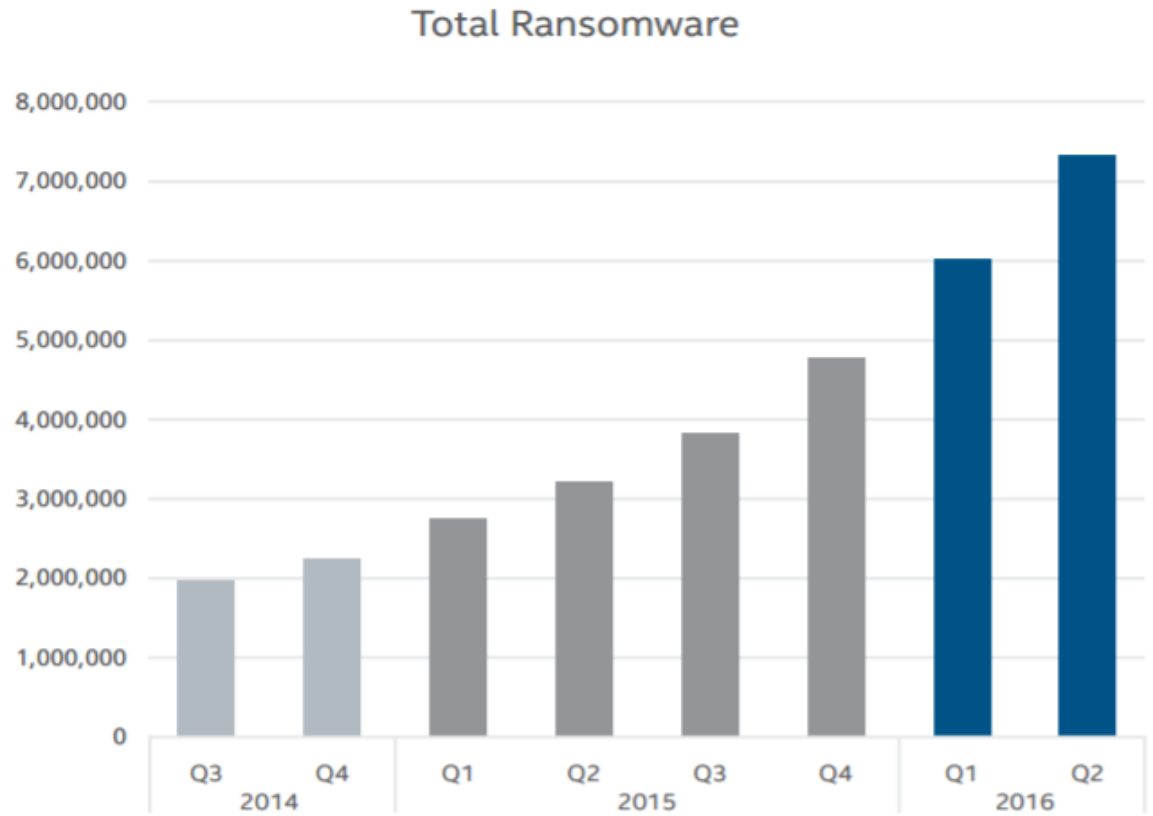
- El Ransomware es un software malicioso que al infectar nuestro equipo le da al ciberdelincuente la capacidad de bloquear el PC desde una ubicación remota y encriptar nuestros archivos quitándonos el control de toda la información y datos almacenados. Para desbloquearlo el malware lanza una ventana emergente en la que nos pide el pago de un rescate.
- Fuente: Panda Labs

¿Cómo nos afecta?

- Principalmente afecta la confidencialidad y disponibilidad de la información.



Source: McAfee Labs, 2016.



Source: McAfee Labs, 2016.

Métodos de infección

Correo - phishing

Aplicación infectada

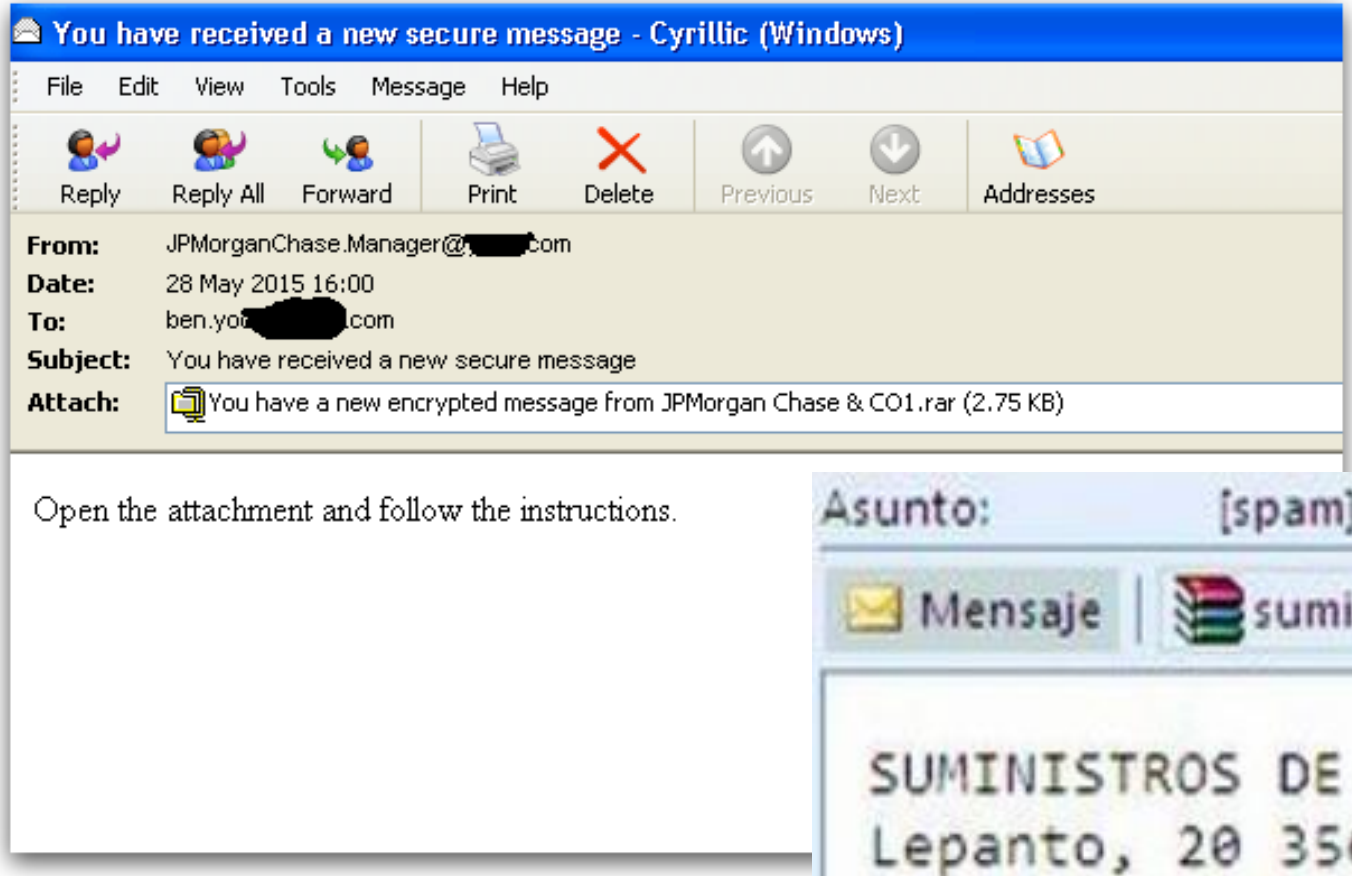
Botnet

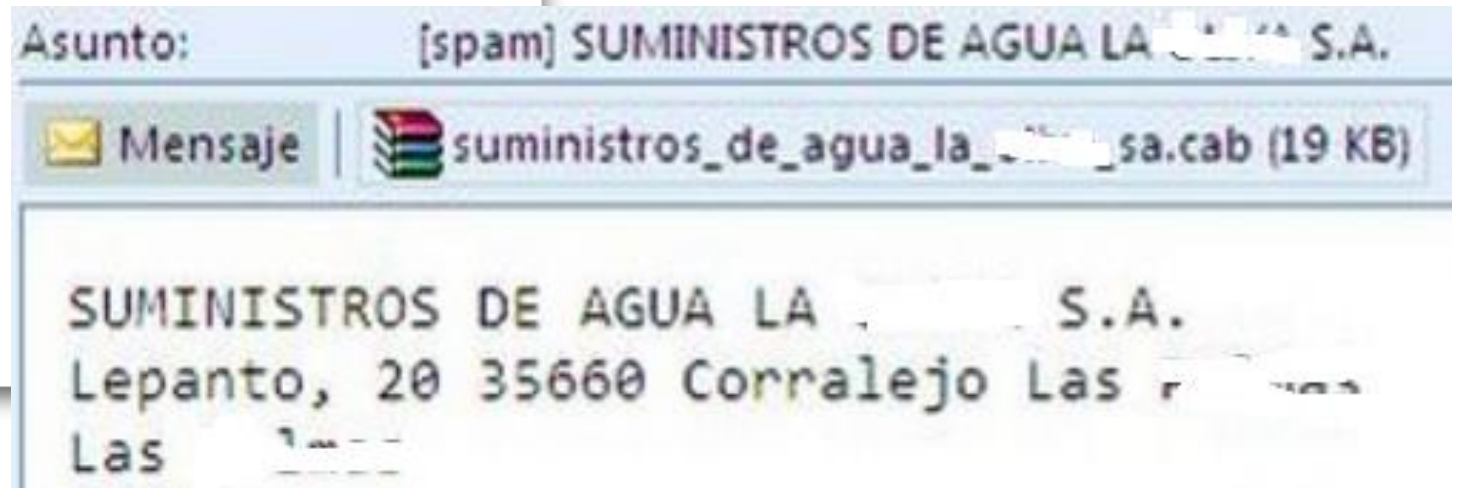
Descargas

Banners - publicidad

Sitios web comprometidos

Métodos de infección





Explotación

- Identifica una vulnerabilidad a explotar en la PC víctima.

Sistemas operativos y software instalado

Navegadores, plugins (flash, entre otros)

Explotación

- Luego de instalarse y utiliza un proceso del sistema operativo (por ejemplo el explorer.exe o svchost.exe).
- Empieza a ejecutar tareas que desprotegen nuestra información.

Deshabilita y elimina las shadow copies (versiones previas)

Deshabilita mensajes

Manipula configuraciones (p. e. proxy)

Comunicación a un CC

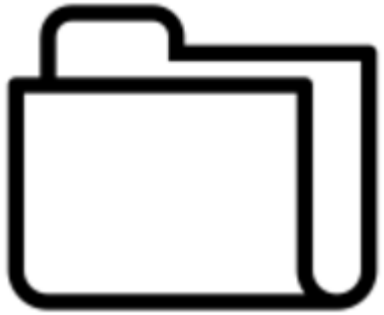
- Se conecta a un Centro de Control con el fin de recibir los siguientes pasos.

Se conecta al CC para recibir instrucciones. Puede ser un sitio web de internet, red TOR o I2P. Suele recibir la llave publica de un cifrado asimétrico (RSA)

Identifica las características del equipo infectado y envía ordenes de acuerdo al tipo de equipo

Cifrado de documentos

- Encripta documentos y contenido multimedia.



Encriptación de los contenidos de carpetas en orden alfabético

Puede encriptar documentos en red si existen unidades mapeadas

Utiliza una llave robusta para el cifrado de los documentos

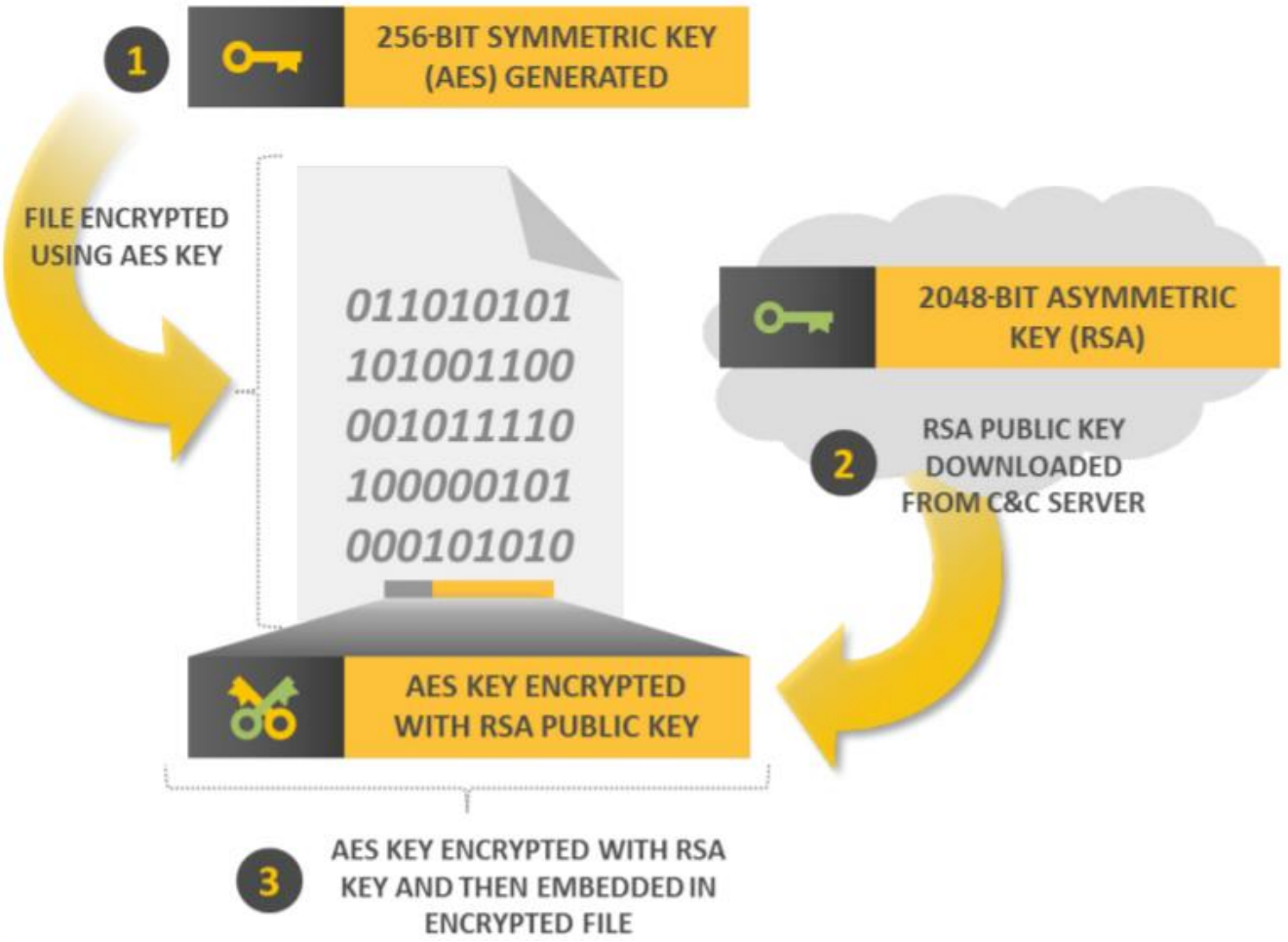
Cifrado de documentos

- El cifrado es el proceso de aplicar un algoritmo a los datos para ocultarlos de cualquier persona.
- Cifrado simétrico
  - Advanced Encryption Standard (AES), Rivest Cipher 4 (RC4) y Data Standard Encryption Standard (DES) son ejemplos. La misma clave se utiliza para el cifrado como para el descifrado. Sólo es efectivo cuando la clave simétrica es mantenida en secreto por las dos partes involucradas.

Cifrado de documentos

- Claves Públicas (clave asimétrica)
  - Rivest, Shamir y Aldeman (RSA) usan dos claves. Una clave pública a la que todos tienen acceso y una clave privada controlada por la persona con la que desea comunicarse.

Cifrado de documentos



- Las últimas muestras de ransomware utilizan cifrado simétrico para los archivos (p.e AES) y cifran la clave privada del cifrado simétrico con un algoritmo de llave pública (p.e RSA). La clave privada se almacena en el servidor de CC.
- Se requiere la clave privada del cifrado simétrico para volver acceder a los archivos.

Cifrado de documentos

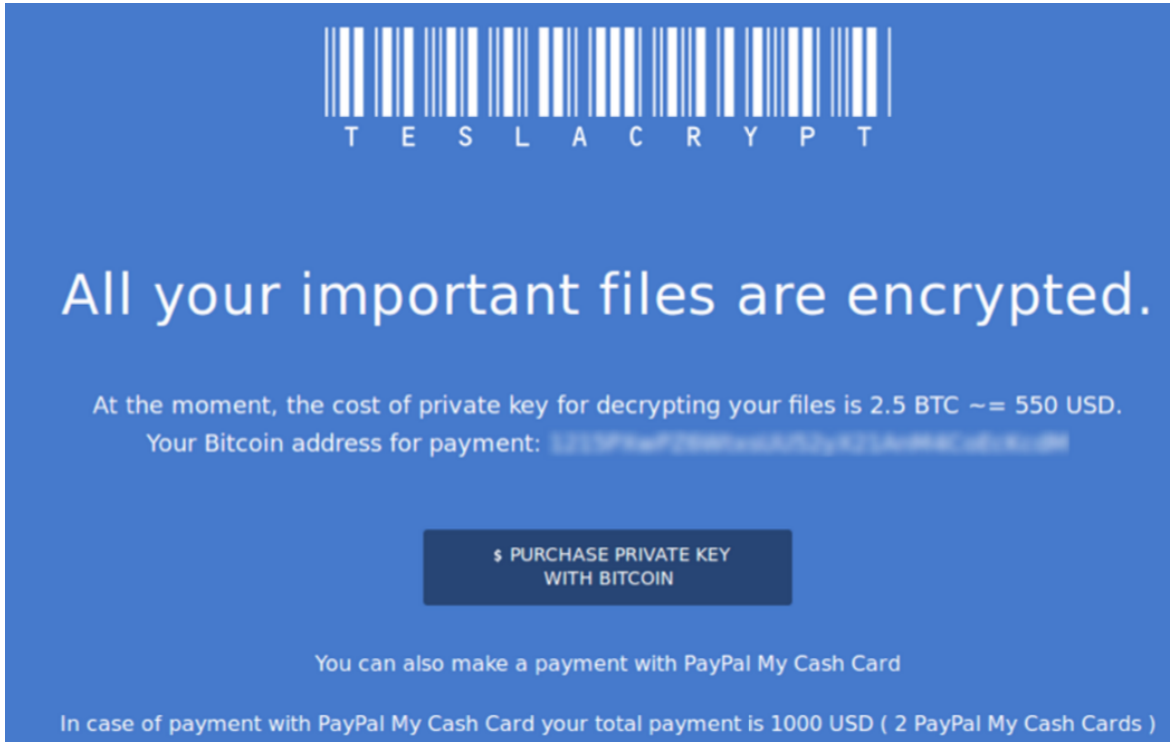
- Robustez de un cifrado
  - Hay que observar el tipo de encriptación que se utiliza (ya sea simétrica o pública/asimétrica) y la longitud de la clave.
  - Dos factores importantes: cuanto más larga es la clave, más fuerte es el cifrado y la longitud de la clave se mide en bits.
- Rompiendo un cifrado
  - Para un algoritmo simétrico, necesitará un par de horas de tiempo de una computadora para una clave de 20 bits o años para una clave de 128 bits (2128 = 340282366920938463463374607431768211456 posibles claves de 128 bits)

Pago de chantaje

- Después de cifrar los archivos aparece un mensaje (imagen, nota de texto o página html) que indica que tu información ha sido cifrada y debes pagar un ransom.

Pago de chantaje

Pago de chantaje



Descifrado

- Casi imposible, debido a la robustez del cifrado de la llave. Para algunos casos, existen herramientas para descifrar los archivos.
- Depende de cada organización si decide pagar el chantaje para recuperar su información.
- Existen casos donde se paga y no se logra obtener la clave para descifrar la información.
- Es posible utilizar herramientas forenses para recuperar datos de las "versiones previas" y del sistema de archivos (no siempre funciona)

Variant	Locky	Cerber	Cryptowall	SamSam	CryptXXX
Infection methods observed	Exploit kit[14],[15] (Magnitude, Nuclear) Spam emails[16]	Exploit kit[17] (Magnitude) Compromised website	Spear-phishing emails[18] Spam emails[19] Exploit kits[20] (Angler[21], Magnitude[22], Neutrino[23], Nuclear[24])	Exploitation of unpatched vulnerabilities in external-facing servers[25]	Exploit kit (Angler, Neutrino)[26]
Evidence of targeted / untargeted campaigns	**Semi-targeted** Spam emails using a fake invoice as a social engineering lure[27]	**Untargeted** Mass infection of victims	**Untargeted to highly targeted** Spear-phishing emails to company executives with names and job titles[28] Small to medium businesses - email lures relating to resumes, orders and passport copies[29]	**Highly targeted** Network intrusion techniques employed (vulnerable JBoss application servers)	**Untargeted** Mass infection of victims
Encryption techniques (latest)	RSA-2048 and AES-128[30]	AES-256[31]	AES 256 CBC and RSA-2048[32]	Rijndael and RSA-2048[33]	RSA4096
Action	Encrypts local and mounted or networked drives[34]	Encrypts networked devices and files[35]	Encrypts local and mounted or networked drives[36]	Lateral movement by threat actor on the network	Encrypts files and harvests information and credentials
Ransom demands	approx. $220 - $1770[3738]	approx. $500[39]	approx. $200 - $10,000[40]	approx. $440 - $750 per machine	approx. $500 - $1000

Contramedidas

- Entrenamiento a los usuarios.
- Aseguramiento de configuración de navegadores y S.O. (hardening)
- Antivirus, antispam actualizados y configurados adecuadamente.
- Lista blanca de aplicaciones.
- Menor cantidad de privilegios posibles (no administrador local).
- Mantener los sistemas operativos y software base actualizado.
- Backups o respaldos de información.
- Firewalls de tipo NGFW.
- Filtro de URLs.
- SIEM (correlación de eventos, identificación de incidentes y respuesta).
- Monitoreo de integridad de archivos.
- Sistemas de prevención de intrusos (IPS, IDS, entre otros)
- Sistemas antimalware basados en comportamiento. Entre otras.

Contramedidas

- Durante un ataque:
  - Identificar, aislar los sistemas infectados o posiblemente infectados.
  - Deshabilitar las unidades de red compartidas conectadas a los sistemas infectados.
  - Considerar la posibilidad de suspender las copias de seguridad de (backups) de esos sistemas para evitar la propagación del virus.
  - Enviar una advertencia al personal de la organización informándoles de la amenaza y advirtiéndoles que no abran correos electrónicos con archivos adjuntos de dudosa procedencia.
  - Copia integral (bit a bit) y recuperación de datos en ambiente aislado.

Contramedidas

- A nivel de seguridad en aplicaciones, se recomienda incorporar lo siguiente:

1. Incluir la seguridad antes y durante el desarrollo de una app.
2. Parametrizar Queries.
3. Codificar Datos.
4. Manejo adecuado de sesiones.
5. Validar parámetros de entrada.
6. Implementar controles de identificación y autenticación efectivos.
7. Protección de de datos (p.e. cifrado).
8. Logging y detección de intrusos
9. Uso de frameworks de seguridad
10. Manejo de errores y excepciones

Fuente: https://www.owasp.org/index.php/OWASP_Proactive_Controls

Demo

Preguntas

- SNmKx3TvIlJOhA2

Recursos adicionales

- OWASP Anti-Ransomware Guide Project. https://www.owasp.org/index.php/OWASP_Anti-Ransomware_Guide_Project
- Mitigación y prevención. http://resources.infosecinstitute.com/ransomware-mitigation-and-prevention/

Contacto

- Jorge Córdova Pelayo, CISSP, CISM, ISO 27001 LA, C|EH, C)PTE, BNS, MCSA+M, MCTS
  - Celular: +51 988070443
  - Correo: jcordova@inticyber.com
  - http://www.inticyber.com

Existen dos tipos de organizaciones

1. Las que han sufrido ciberataques o brechas y toman acciones

2. Las que creen no haber sido afectadas por brechas y no toman acciones