

**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 de 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?



**Your personal files are encrypted!**

Private key will be destroyed in:

Time left  
**95:52:36**

Pay Now \$

The image shows a ransomware warning window. It has a red background and a blue shield icon with a white cross. The text reads: "Your personal files are encrypted!". Below this is a white box with five horizontal lines, likely for a message or instructions. To the left of this box, it says "Private key will be destroyed in:" followed by a large yellow timer showing "95:52:36". At the bottom right, there is a blue button that says "Pay Now \$".

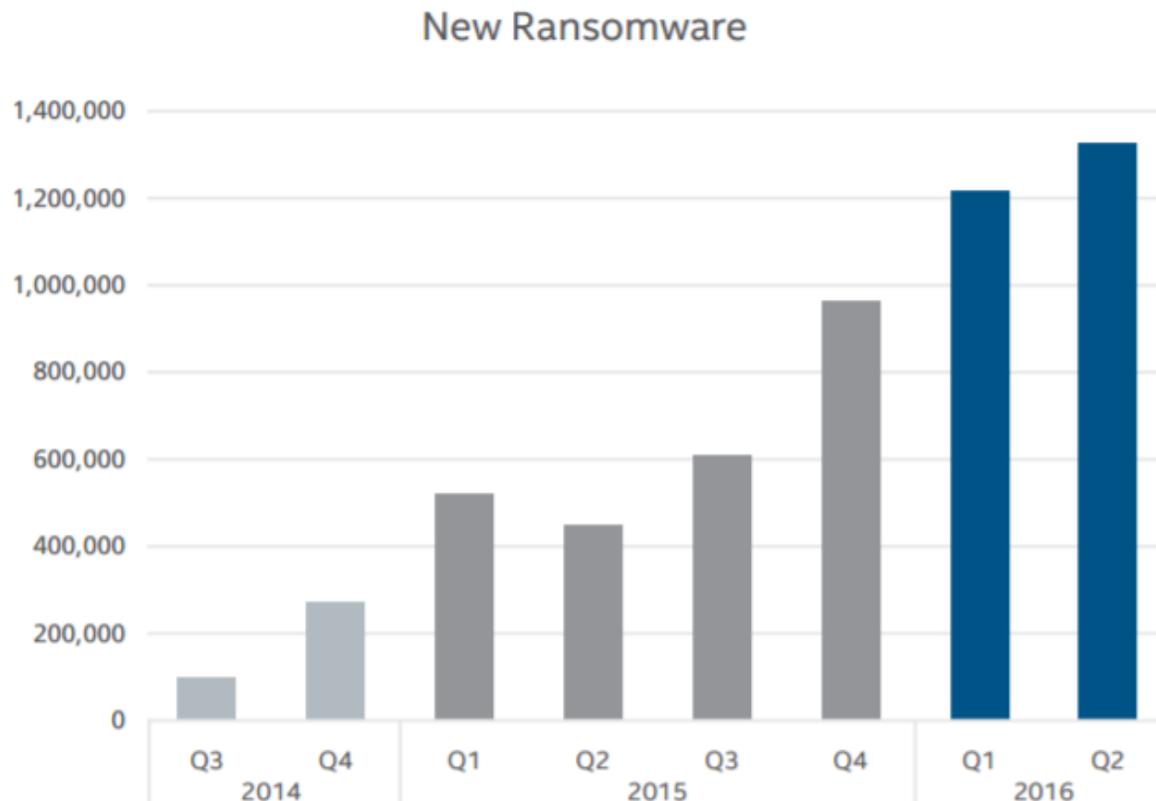
# ¿Qué es un ransomware?

- 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

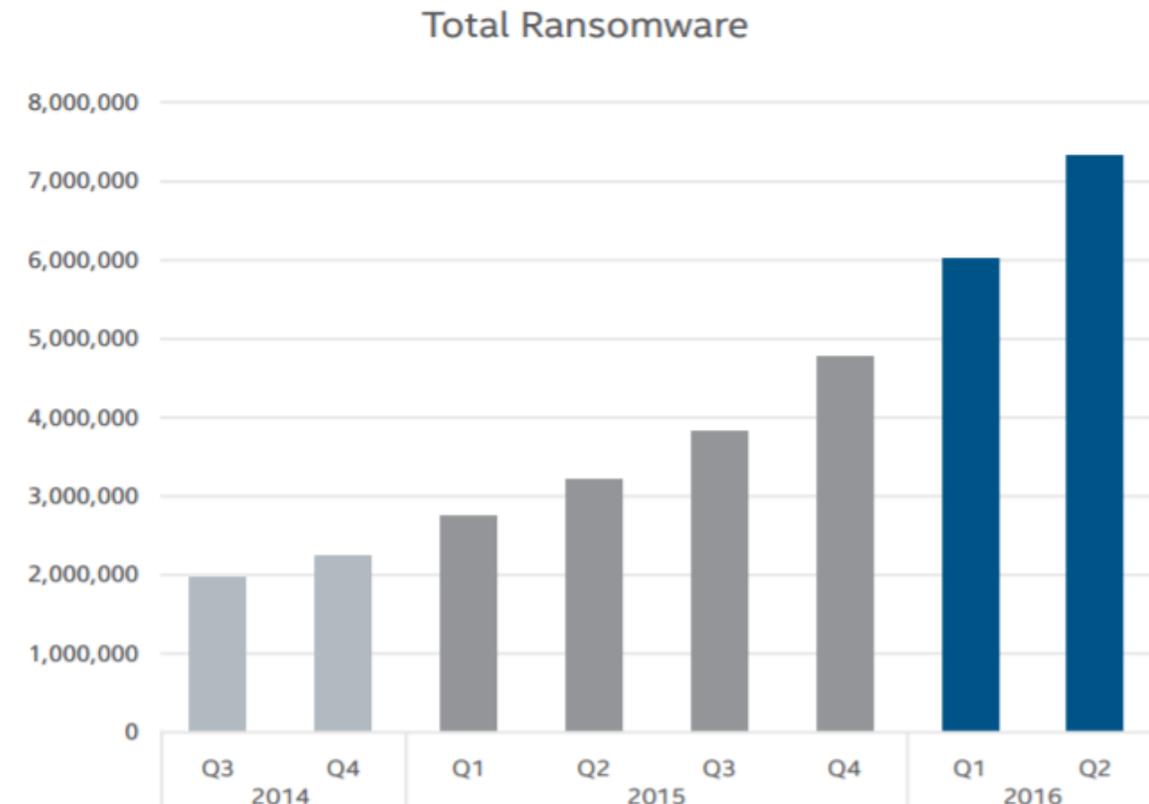


# ¿Cómo nos afecta?

- Principalmente afecta la confidencialidad y disponibilidad de la información.



Source: McAfee Labs, 2016.



Source: McAfee Labs, 2016.

# Métodos de infección



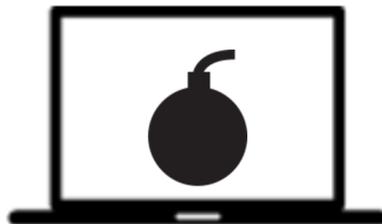
Correo -  
phishing



Aplicación  
infectada



Botnet



Descargas



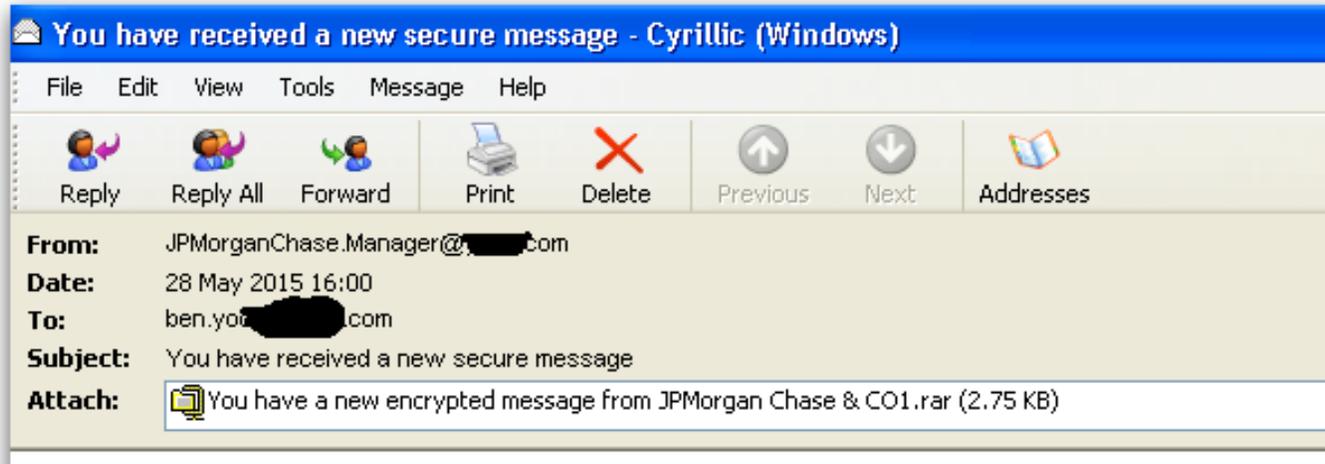
Banners -  
publicidad



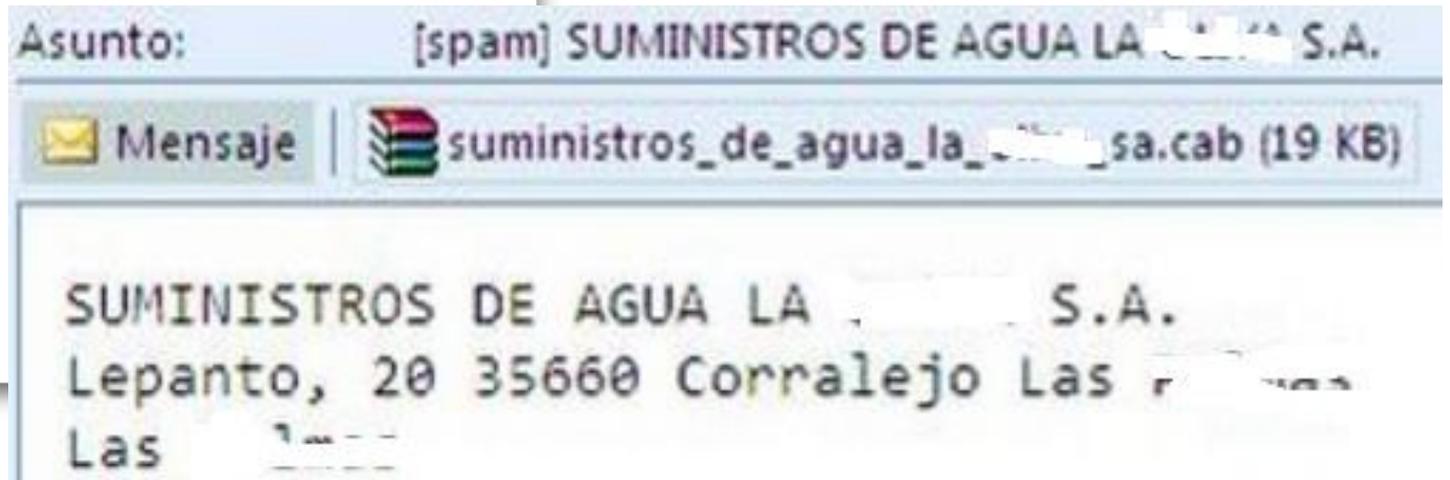
Sitios web  
comprometidos



# Métodos de infección



Open the attachment and follow the instructions.



# 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.



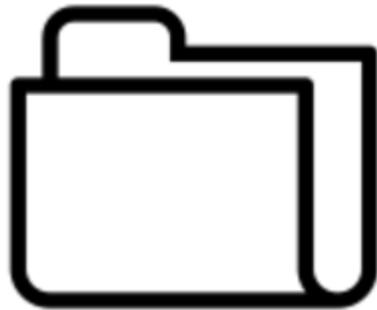
Se conecta al CC para recibir instrucciones. Puede ser un sitio web de internet, red TOR o I2P. Suele recibir la llave pública de un cifrado asimétrico (RSA)



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.

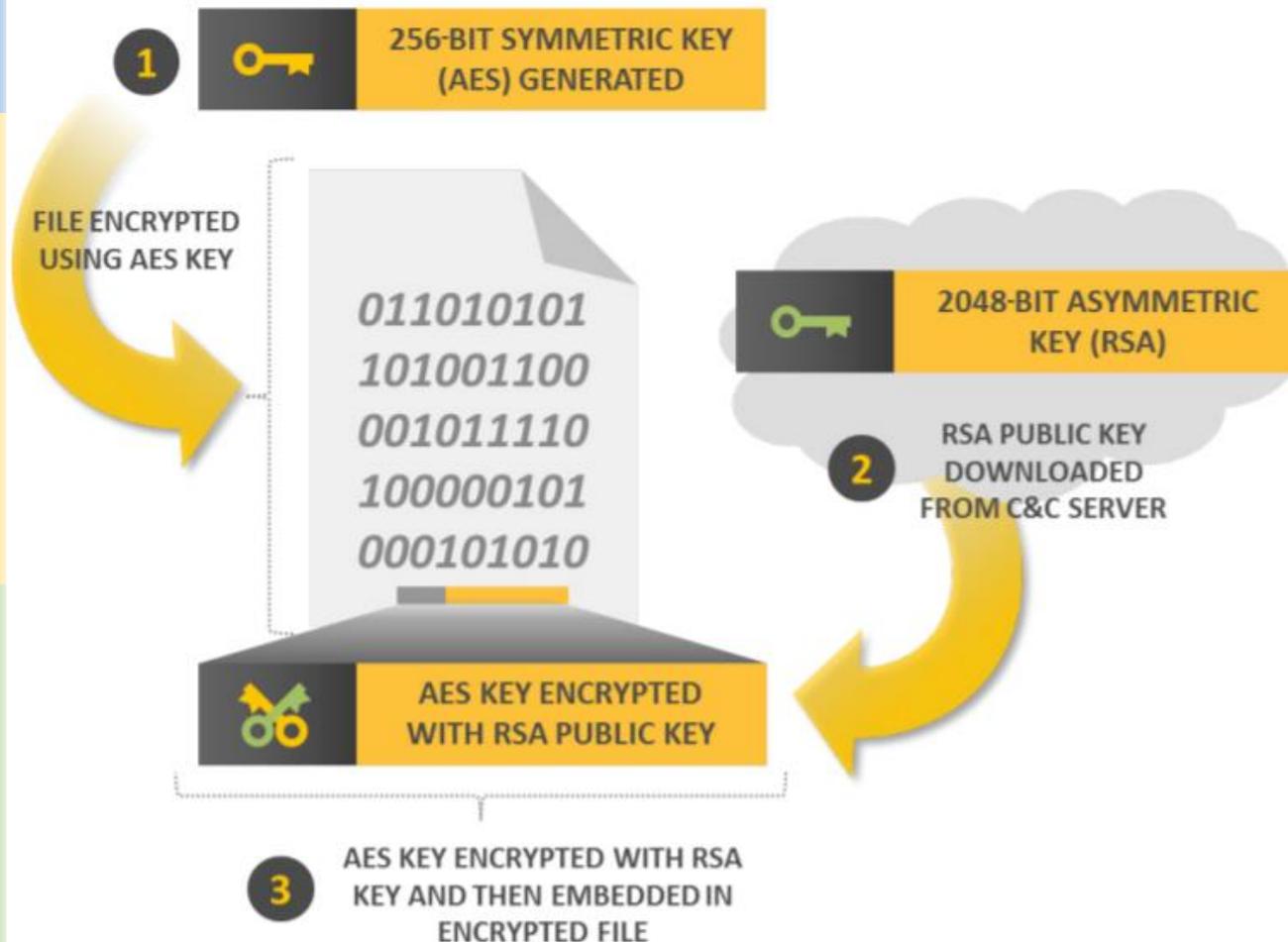


# Cifrado de documentos

- 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 ( $2^{128} = 340282366920938463463374607431768211456$  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

## YOUR COMPUTER HAS BEEN LOCKED!

This operating system is locked due to the violation of the federal laws of the United States of America! (Article 1, Section 8, Clause 8; Article 202; Article 210 of the Criminal Code of U.S.A. provides for a deprivation of liberty for four to twelve years.)

Following violations were detected:

Your IP address was used to visit websites containing pornography, child pornography, zoophilia and child abuse. Your computer also contains video files with pornographic content, elements of violence and child pornography! Spam-messages with terrorist motives were also sent from your computer.

This computer lock is aimed to stop your illegal activity.

To unlock the computer you are obliged to pay a fine of \$200.

You have 72 hours to pay the fine, otherwise you will be arrested.

You must pay the fine through

To pay the fine, you should enter the digits resulting code, which is located on the back of your in the payment form and press OK (if you have several codes, enter them one after the other and press OK).

If an error occurs, send the codes to address [fine@fbi.gov](mailto:fine@fbi.gov).



OK

## Tus archivos personales se cifran por CTB-Locker.

Tus documentos, fotografías, bases de datos y otros archivos importantes han sido cifrados con el cifrado más fuerte posible y con una clave única, generada para este equipo.

La clave de descifrado privada se almacena en un servidor de Internet en secreto y nadie puede descifrar tus archivos hasta que pagues y obtengas la clave privada.

Tienes solo 96 horas para enviar el pago. Si tú no envías el dinero dentro del tiempo proporcionado, todos tus archivos se mantendrán permanentemente cifrados y nadie será capaz de recuperarlos.

Haz clic en 'Ver' para ver la lista de archivos que han sido cifrados.

Presiona 'Siguiente' para ir a la siguiente página.



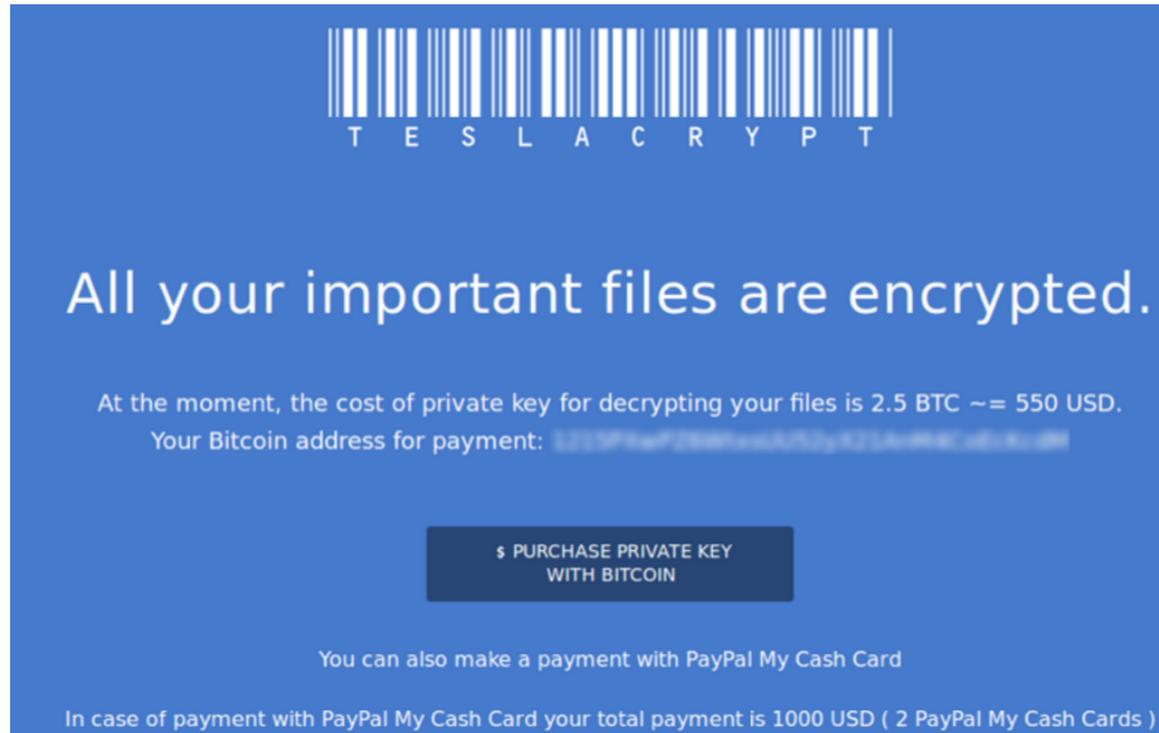
**¡ADVERTENCIA! NO TRATES DE DESHACERSE DEL PROGRAMA POR TI MISMO. CUALQUIER ACCIÓN TOMADA CONLLEVA A QUE LA CLAVE DE DESCIFRADO SEA DESTRUIDA. PERDERÁS TUS ARCHIVOS PARA SIEMPRE. LA ÚNICA MANERA DE MANTENER TUS ARCHIVOS ES SEGUIR LAS INSTRUCCIONES.**

Ver

95:52:59

Siguiente >>

# Pago de chantaje



  
T E S L A C R Y P T

## All your important files are encrypted.

At the moment, the cost of private key for decrypting your files is 2.5 BTC ≈ 550 USD.  
Your Bitcoin address for payment: `1213P7haP288F44A52yK21A494C461A48H`

[\\$ PURCHASE PRIVATE KEY WITH BITCOIN](#)

You can also make a payment with PayPal My Cash Card

In case of payment with PayPal My Cash Card your total payment is 1000 USD ( 2 PayPal My Cash Cards )





## Pago requerido.

El servidor acepta el pago solamente en Bitcoin (BTC).

1. Paga la cantidad de 2.5 BTC (alrededor de 575 EUR) para a la dirección:  
`13h[REDACTED]TyV`
2. La transacción tardará cerca de 15-30 minutos para que sea confirmada.

El descifrado se iniciará automáticamente. No puede: apagar la computadora, ejecutar el antivirus, deshabilitar la conexión a Internet. Fallos durante la recuperación de claves y descifrado de archivos puede conducir a daños accidentales en los ficheros.

Si no tienes Bitcoins haz clic en 'Cambiar'.

**69 49 39** [Cambiar >>](#)

# 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 <sup>14,15</sup> (Magnitude, Nuclear) Spam emails <sup>16</sup>	Exploit kit <sup>17</sup> (Magnitude)  Compromised website	Spear-phishing emails <sup>18</sup>  Spam emails <sup>19</sup>  Exploit kits <sup>20</sup> (Angler <sup>21</sup> , Magnitude <sup>22</sup> , Neutrino <sup>23</sup> , Nuclear <sup>24</sup> )	Exploitation of unpatched vulnerabilities in external-facing servers <sup>25</sup>	Exploit kit (Angler, Neutrino) <sup>26</sup>
Evidence of targeted / untargeted campaigns	<b>Semi-targeted</b>  Spam emails using a fake invoice as a social engineering lure <sup>27</sup>	<b>Untargeted</b>  Mass infection of victims	<b>Untargeted to highly targeted</b>  Spear-phishing emails to company executives with names and job titles <sup>28</sup>  Small to medium businesses - email lures relating to resumes, orders and passport copies <sup>29</sup>	<b>Highly targeted</b>  Network intrusion techniques employed (vulnerable JBoss application servers)	<b>Untargeted</b>  Mass infection of victims
Encryption techniques (latest)	RSA-2048 and AES-128 <sup>30</sup>	AES-256 <sup>31</sup>	AES 256 CBC and RSA-2048 <sup>32</sup>	Rijndael and RSA-2048 <sup>33</sup>	RSA4096
Action	Encrypts local and mounted or networked drives <sup>34</sup>	Encrypts networked devices and files <sup>35</sup>	Encrypts local and mounted or networked drives <sup>36</sup>	Lateral movement by threat actor on the network	Encrypts files and harvests information and credentials
Ransom demands	approx. \$220 - \$1770 <sup>37,38</sup>	approx. \$500 <sup>39</sup>	approx. \$200 - \$10,000 <sup>40</sup>	approx. \$440 - \$750 per machine	approx. \$500 - \$1000

# Contramiedidas

- 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.



# Contra medidas



- 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.

# Contra medidas

- 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](https://www.owasp.org/index.php/OWASP_Proactive_Controls)



# Demo

# Preguntas

- SNmKx3TvIIJOhA2



# Recursos adicionales

- OWASP Anti-Ransomware Guide Project.  
[https://www.owasp.org/index.php/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](mailto:jcordova@inticyber.com)
  - <http://www.inticyber.com>



Existen dos tipos de organizaciones

¿Qué tipo 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

