
COLEGIO DE INFORMÁTICOS
COCHABAMBA - BOLIVIA
Personería Jurídica R.A. N°069/1998 del 7 mayo de 1.998
AFILIADO A LA FEDERACION DE PROFESIONALES DE COCHABAMBA
coloquio
RANSOMWARE
MIGUEL ANGEL PACO ESCOBAR

COLEGIO DE INFORMATICOS DE COCHABAMBA

Analizaremos las siguientes cuestionantes:

- Qué es y cómo se produce?
- Sus impactos en la empresa y organizaciones?
- Cómo evitar ser afectado?
- Importancia de contar con un Sistema de Gestión de Seguridad de la Información ISO:27001

COLEGIO DE INFORMATICOS DE COCHABAMBA

Todos quisiéramos que la vida sea una taza de leche

COLEGIO DE INFORMATICOS DE COCHABAMBA

Pero no lo es!!
Existen villanos que raptan a las “niña de sus ojos”

COLEGIO DE INFORMATICOS DE COCHABAMBA

Qué es RANSONWARE?

Ransomware se puede traducir como "**cibersecuestro de datos**"

Consiste en que un software malicioso infecta nuestro equipo (Windows) y encripta nuestros archivos, obligándonos a realizar el pago de una determinada cantidad para poder recuperarlos.

Fuente: COMPUTERHOY (2017)

COLEGIO DE INFORMATICOS DE COCHABAMBA

Cómo se produce RANSONWARE?

- Este tipo de malware se camufla dentro de otro archivo apetecible (usando la ingeniería social) para que el usuario haga click. Por ejemplo, puede ocultarse en documentos adjuntos en e-mails, vídeos de páginas de dudoso origen o, incluso, en actualizaciones de sistema o de programas, a priori, confiables.
- Una vez que ha penetrado en el ordenador (se ha instalado), el malware se activa y provoca el bloqueo de todo el sistema operativo.

COLEGIO DE INFORMATICOS DE COCHABAMBA

Ejemplo Ingeniería social

no deseado | Limpiar Mover a Categorías •••

Hola!

LM [redacted]@gmail.com>

lun 13/10/2014, 14:03

Usted

Bandeja de entrada

Espero que esto te llegue a tiempo, hice un viaje a Newcastle, In
Tarjetas de Crédito dentro. La Embajada está deseando ayudarr
pagar por el billete y cubrir las cuentas del Hotel. Para mi desgr
contacte con mi Banco pero necesitan más tiempo para los proc
pensado en pedirte un préstamo rápido de fondo que puedo d
vuelo.Necesito como 900 libra para cubrir mis gastos.Western u
enviarte los detalles en cómo hacer llegar los fondos a mí.

Espero ansiosamente tu respuesta.

Saludos.

--
Cordialmente,

[redacted]

Cochabamba - Bolivia

COLEGIO DE INFORMATICOS DE COCHABAMBA

COLEGIO DE INFORMATICOS DE COCHABAMBA

Tecno:Codigo

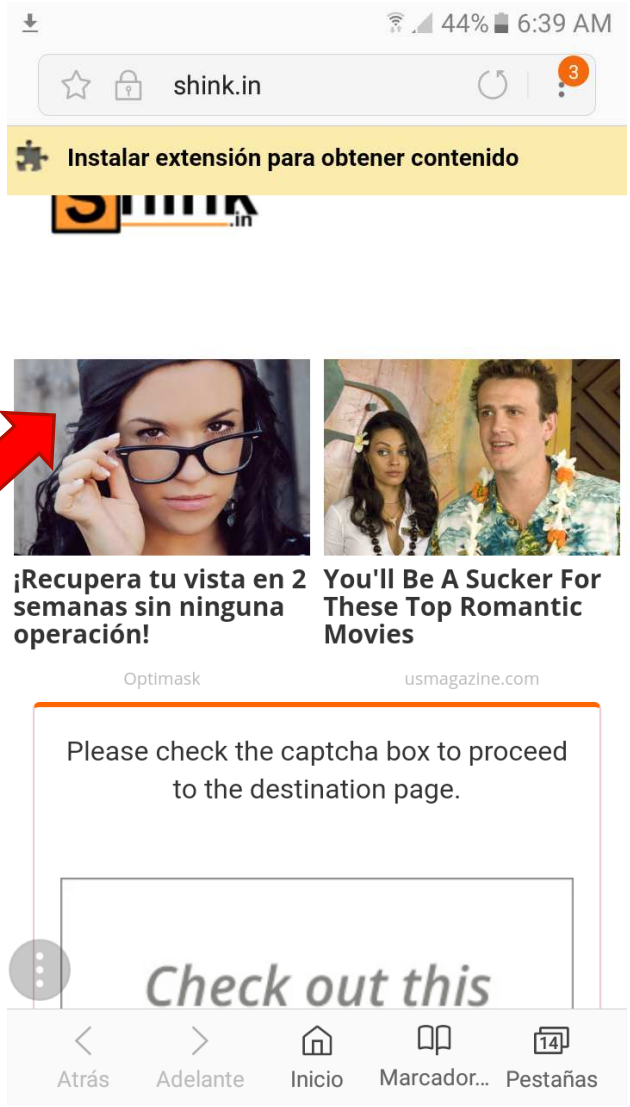
ALGORITMOS RESUELTOS CON DIAGRAMAS DE FLUJO Y PSEUDOCÓDIGO Descarga: http://shink.in/QTZKC

Contiene: 172 paginas Año: 2014. Disfruta confirmando el captcha y dando en click en GET LINK.

Fotos de la biografía · 20 de diciembre de 2016 ·

Ver en tamaño grande · Más opciones

Me gusta Comentar Compartir



COLEGIO DE INFORMATICOS DE COCHABAMBA

Cómo se produce RANSONWARE?

- Existen dos tipos de bloqueo: sin y con encriptación. El primero de ellos es una toma del sistema **sin encriptar** los datos. Lo normal es que este malware desactive el Administrador de tareas, blinda el acceso al registro e infecta el fichero EXPLORER.EXE para que desaparezcan los iconos de escritorio. Esto te impedirá usar sus programas.
- Por otra parte también está la variante que **encripta** los datos del disco duro con códigos casi imposibles de descifrar si no conoces la clave. Si la encriptación sólo afecta a archivos del sistema, un antivirus puede recuperar el control reinstalándolos. Pero si está encriptado **todo el sistema operativo** o, aún peor, los datos del usuario, la única solución es formatear el disco duro, con la inevitable pérdida de datos.
- A continuación, lanza el mensaje de advertencia con la amenaza y el importe del rescate que se ha de pagar para recuperar la información. Éste se suele enviar al cibercriminal mediante transferencia, llamada o SMS.

COMPUTERHOY (2017)

COLEGIO DE INFORMATICOS DE COCHABAMBA

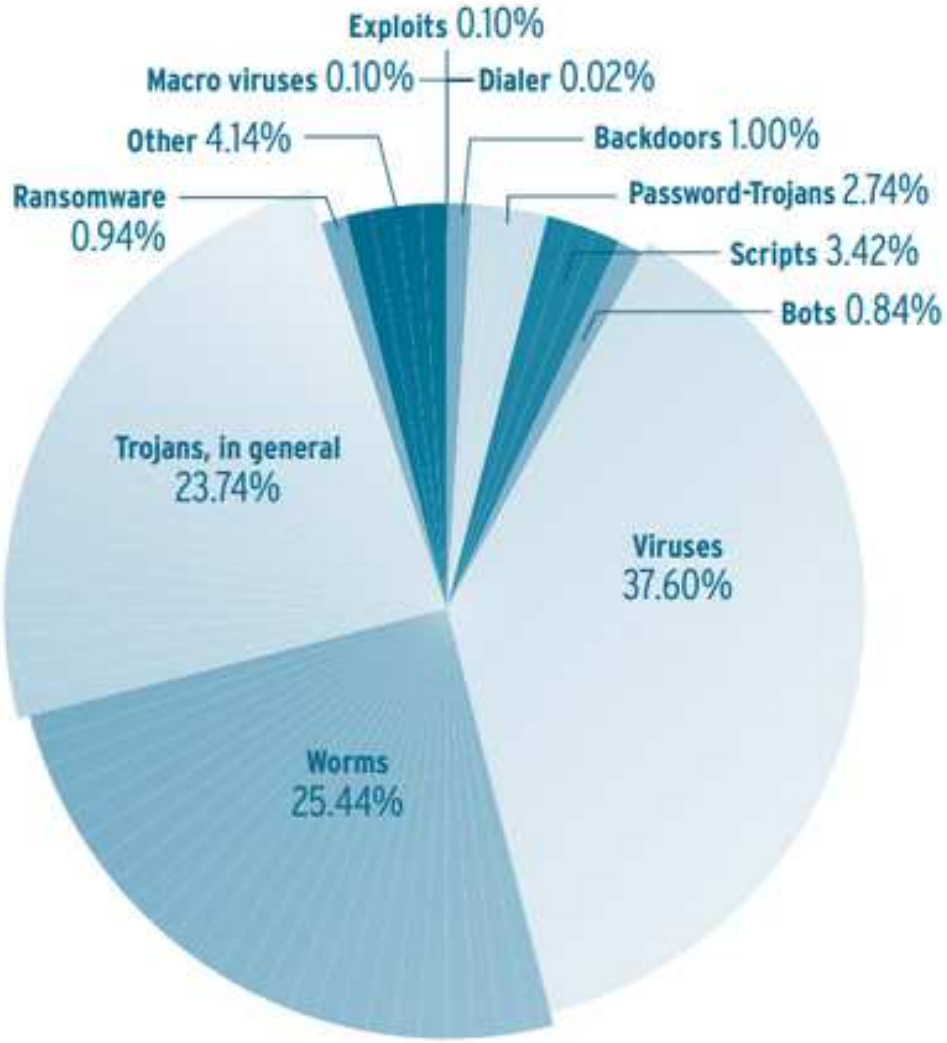
Petya, el ransomware que encripta el disco duro de tu PC

- Para potenciar la incertidumbre y el miedo de la víctima, en ocasiones incluyen en la amenaza la dirección IP, la compañía proveedora de Internet y hasta una fotografía captada desde la webcam.
- En muchos casos, aunque pagues, no te devolverán el control del ordenador y tendrás que formatearlo.
- Si quieres evitar ser una **víctima del ransomware como el reciente WannaCry** utilizado para **atacar a Telefónica**, te recomendamos seguir esta serie de consejos: el primero, mantener tu sistema operativo actualizado para evitar fallos de seguridad e instalar un antivirus; por otra parte, también debes evitar abrir correos o archivos de remitentes desconocidos; finalmente, no debes acceder a las páginas no seguras con contenido no verificado.

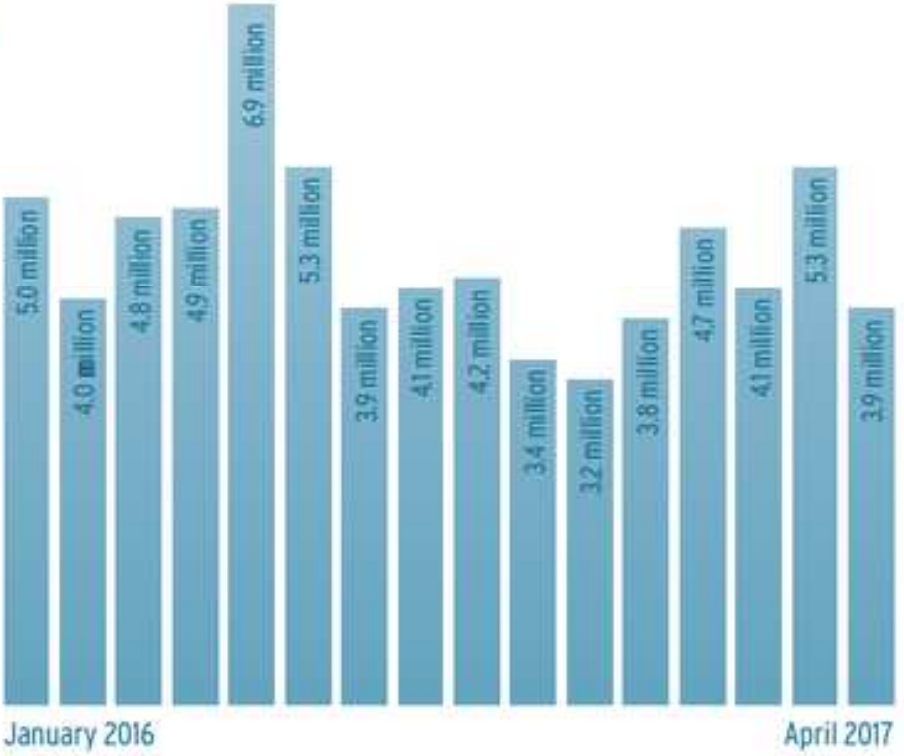

You became victim of the PETYA RANSOMWARE!
The harddisks of your computer have been encrypted with an military grade encryption algorithm. There is no way to restore your data without a special key. You can purchase this key on the darknet page shown in step 2.
To purchase your key and restore your data, please follow these three easy steps:
1. Download the Tor Browser at "https://www.torproject.org/". If you need help, please google for "access onion page".
2. Visit one of the following pages with the Tor Browser:
http://pety .onion/g
http://pety .onion/g
3. Enter your personal decryption code there:
a6
nF y1
If you already purchased your key, please enter it below.
Key: _

COLEGIO DE
INFORMATICOS
DE COCHABAMBA

Distribution of malware under Windows in 2016



Development of new malware for Windows in 2016 and 1st quarter of 2017



ZDNET (2017)

COLEGIO DE INFORMATICOS DE COCHABAMBA

Causas

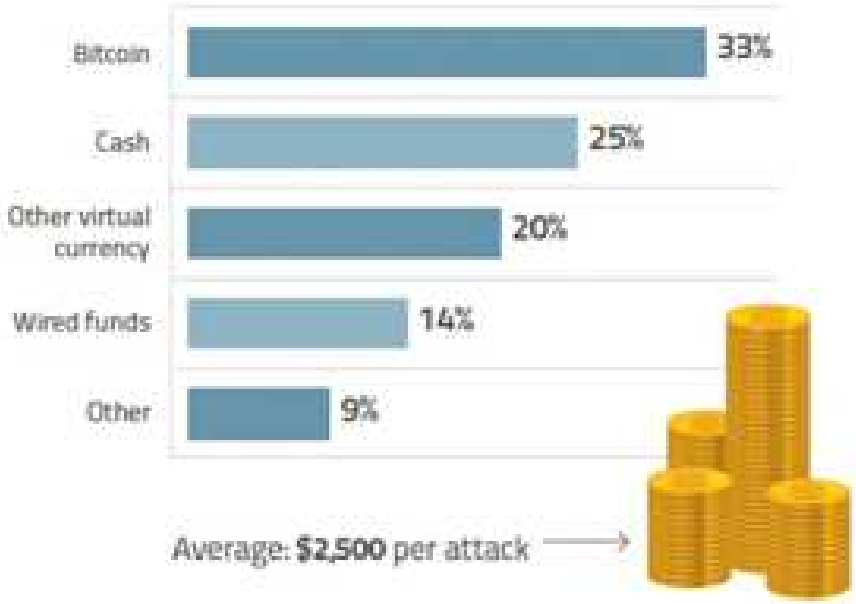
- El usuario instaló un programa infectado.
- No se actualizó sistema operativo (“parches” de seguridad)
- No se cuenta o no se actualiza el antivirus
- Dispositivos conectados a la computadora están infectados (flash usb, celulares, etc)
- Se propagó virus por la red
- …

Many Companies Pay Ransoms

The financial fallout from ransomware involves more than bitcoins, one study found. BY KATHLEEN RICHARDS

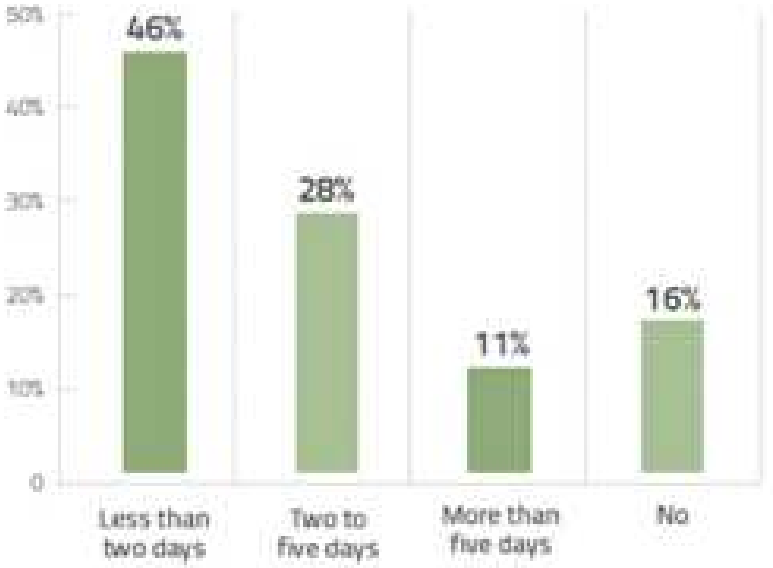
48% Paid the Attackers

How did your company pay the ransom?



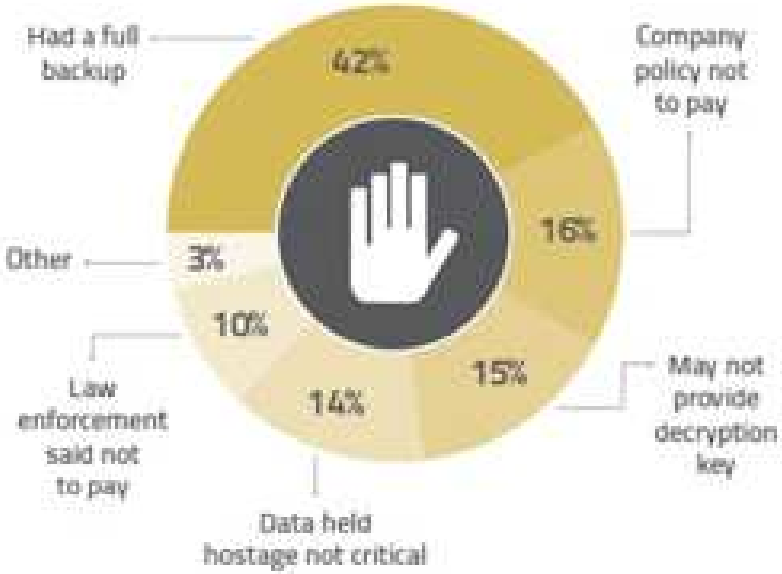
Speed Required

Did the ransomware place a time limit for payment?



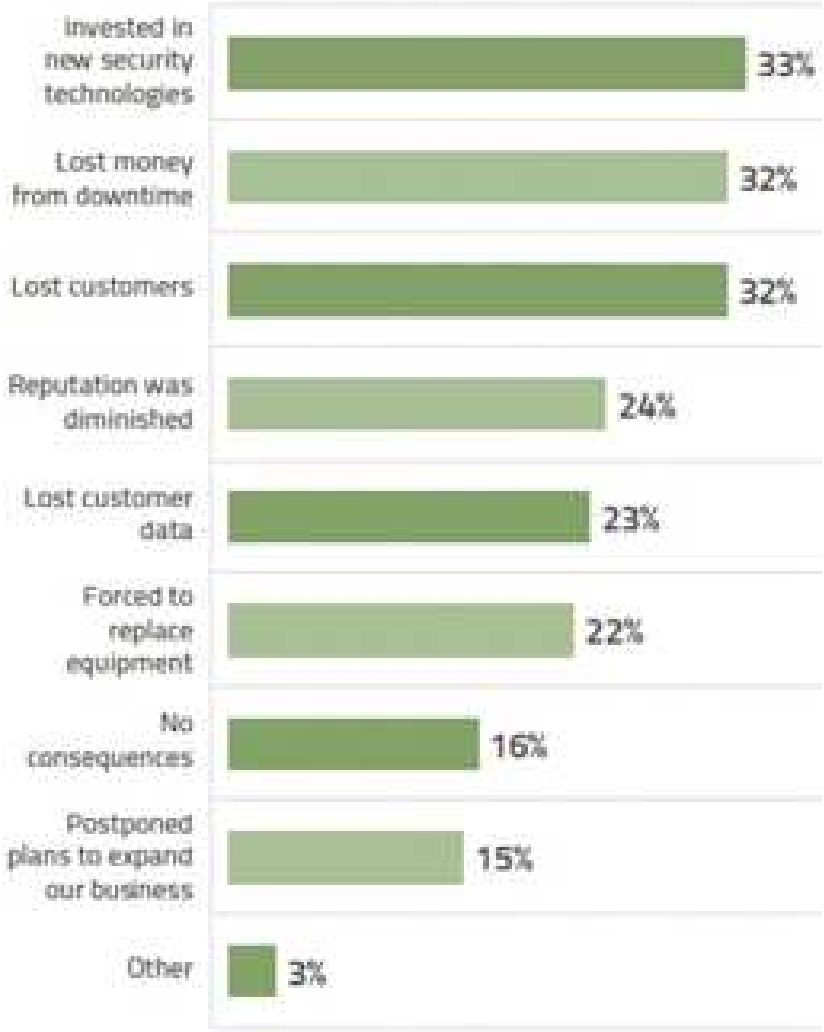
52% Did Not Pay

Why was the ransom not paid?



Financial Fallout

What are the consequences of the ransomware attack?*



Stolen Data

Did the ransomware exfiltrate data from the compromised device(s)?

Fuente: SearchSecurity 2017

COLEGIO DE INFORMATICOS DE COCHABAMBA

Sus impactos en las empresas y organizaciones?

- Continuidad de procesos se ve afectada
- Descenso en los ingresos
- Pérdida de clientes
- Pérdida de credibilidad
- Afectación de la reputación

COLEGIO DE INFORMATICOS DE COCHABAMBA

Sus impactos en las empresas y organizaciones? PEOR CASO

- … banca rota
- … cierre de empresas
- … pérdida de fuentes laborales

COLEGIO DE INFORMATICOS DE COCHABAMBA

En búsqueda de soluciones integrales

- **Inversión en la formación de:**
  - Recursos humanos de las empresas o particulares
  - Personal técnico IT
  - La alta gerencia sobre estos aspectos.
- Inversión en medios y equipamiento tecnológico para mitigar estos incidentes (hardware / software)
- **Sistema de Gestión de Seguridad de la Información**

COLEGIO DE
INFORMATICOS
DE COCHABAMBA

COLEGIO DE INFORMATICOS DE COCHABAMBA

Bibliografía

- COMPUTERHOY (2017). *¿Qué es ransomware y cómo funciona el secuestro de datos?*. Recuperado de http://computerhoy.com/noticias/software/que-es-ransomware-como-funciona-secuestro-datos-43513
- ZDNET (2017) recuperado de http://www.zdnet.com/article/windows-ransomware-found-to-be-incredibly-rare/
- MALWAREBYTES LABS (2917). Petya and Mischa – Ransomware Duet (Part 1) Recuperado de https://blog.malwarebytes.com/threat-analysis/2016/05/petya-and-mischa-ransomware-duet-p1/