ISBCorp
Information Security Bolivia
Business Continuity Security & Risk Management

# ransomware

# wanacry / wannaCrypt / petya

ISBCorp
Information Security Bolivia
Business Continuity Security & Risk Management

# Ransomware ?

## Programa malicioso / malware
## (secuestra, encripta tus datos y solicita rescate)

**ransom = rescate**
**ware = software**
**rescate x software**

ISBCorp
Information Security Bolivia
Business Continuity Security & Risk Management

# EternalBlue / CVE-2017-0144

Common Vulnerabilities and Exposures (CVE)

**Echemos un vistazo a la historia de la vulnerabilidad que ha dado lugar al exploit de EternalBlue**

**25 de octubre de 2001:** Microsoft lanza el sistema operativo Windows XP, uno de los mayores éxitos de la historia de la compañía. Contiene, sin que nadie lo supiera, un crítico agujero de seguridad que ha sido heredado por el resto de versiones del sistema operativo.

**14 de marzo de 2017:** Microsoft publica una actualización que soluciona dicha vulnerabilidad (MS17-010) / Para todos sus sistemas operativos, incluido Windows XP (Oficialmente sin soporte), algo insólito !!

ISBCorp
Information Security Bolivia
Business Continuity Security & Risk Management

# EternalBlue / CVE-2017-0144

Common Vulnerabilities and Exposures (CVE)

**Echemos un vistazo a la historia de la vulnerabilidad que ha dado lugar al exploit de EternalBlue**

**El 8 de abril de 2017**, el grupo The Shadow Brokers luego de haber ingresado a los sistemas de la NSA, filtro en su Github las herramientas que encontraron. Dentro de las herramientas filtradas, se encuentra un **exploit (EternalBlue)** que permite aprovechar una vulnerabilidad en el protocolo SMB versión 1, y de esta manera poder Ejecutar Código Remoto (RCE) sobre la máquina víctima consiguiendo acceso al sistema.

**12 de mayo de 2017:** Aparece WannaCry, un gusano de red que utiliza el ataque de EternalBlue para propagarse y además ejecuta ransomware en las máquinas atacadas

**28 de junio de 2017:** Se reporta la aparición de Petya ransomware que también utiliza el exploit EternalBlue para propagarse.

ISBCorp
Information Security Bolivia
Business Continuity Security & Risk Management

# WannaCry / WannaCrypt / WannaCrypt0r

ISBCorp
Information Security Bolivia
Business Continuity Security & Risk Management

# WannaCry / WannaCrypt / WannaCrypt0r

**Características :**

1. **Encripta archivos en Sistemas Windows Infectados / AES 128**
2. **Esta compuesto por dos componentes o funcionalides a nivel software - un gusano con capacidad de autoreplicarse (usa exploit eternalblue) y el paquete ransomware que realiza el cifrado de archivos**
3. **El malware se distribuye entre los equipos de la red que tengan sistemas operativos windows vulnerables a eternalblue**
4. **El malware también se distribuye a través de adjuntos de email (viaje en crucero al caribe u otros similares parte de ingeniería social)**
5. **Solicita un rescate por los datos encriptaos en Bitcoins por el equivalente de 300 USD o 600 USD**
6. **Estable un contador de tiempo de descuento para efectivizar pago antes que los datos sean destruidos**

ISBCorp
Information Security Bolivia
Business Continuity Security & Risk Management

# WannaCry / WannaCrypt / WannaCrypt0r

**Sistemas Operativos Afectados**

Microsoft Windows XP *
Microsoft Windows Server 2003 *
Microsoft Windows Vista SP2
Windows Server 2008 SP2 and R2 SP1
Windows 7
Windows 8.1
Windows RT 8.1
Windows Server 2012 and R2
Windows 10
Windows Server 2016

**Archivos comúnmente afectados**

- Commonly used office file extensions (.ppt, .doc, .docx, .xlsx, .sxi).
- Less common and nation-specific office formats (.sxw, .odt, .hwp).
- Archives, media files (.zip, .rar, .tar, .bz2, .mp4, .mkv)
- Emails and email databases (.eml, .msg, .ost, .pst, .edb).
- Database files (.sql, .accdb, .mdb, .dbf, .odb, .myd).
- Developers' sourcecode and project files (.php, .java, .cpp, .pas, .asm).
- Encryption keys and certificates (.key, .pfx, .pem, .p12, .csr, .gpg, .aes).
- Graphic designers, artists and photographers files (.vsd, .odg, .raw, .nef, .svg, .psd).
- Virtual machine files (.vmx, .vmdk, .vdi).

ISBCorp
Information Security Bolivia
Business Continuity Security & Risk Management

# WannaCry / WannaCrypt / WannaCrypt0r

**Mas de 100 países afectados, actualmente el ataque ha sido contenido (kill switch)**
**Reporte by Kaspersky Labs.**

ISBCorp
Information Security Bolivia
Business Continuity Security & Risk Management

# Petya / Not Petya / GoldenEye

```
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://petya37h5tbhyvki.onion/P9VVR3
   http://petya5koahtsf7sv.onion/P9VVR3

3. Enter your personal decryption code there:

   cdSPP4-JUZrRr-pMSxia-gXpmfB-vGWoRf-FfMph1-XTUzVn-QmFeeV-ofb94y-HuScaa-
   rB1gmV-djYAEH-8WEakz-wrQ85W-BbsCzw

If you already purchased your key, please enter it below.

Key: 8x3qrMHjmkrN9jfd
Decrypting sector 83234 of 126464 (65%)
```

ISBCorp
Information Security Bolivia
Business Continuity Security & Risk Management

# Petya / Not Petya / GoldenEye

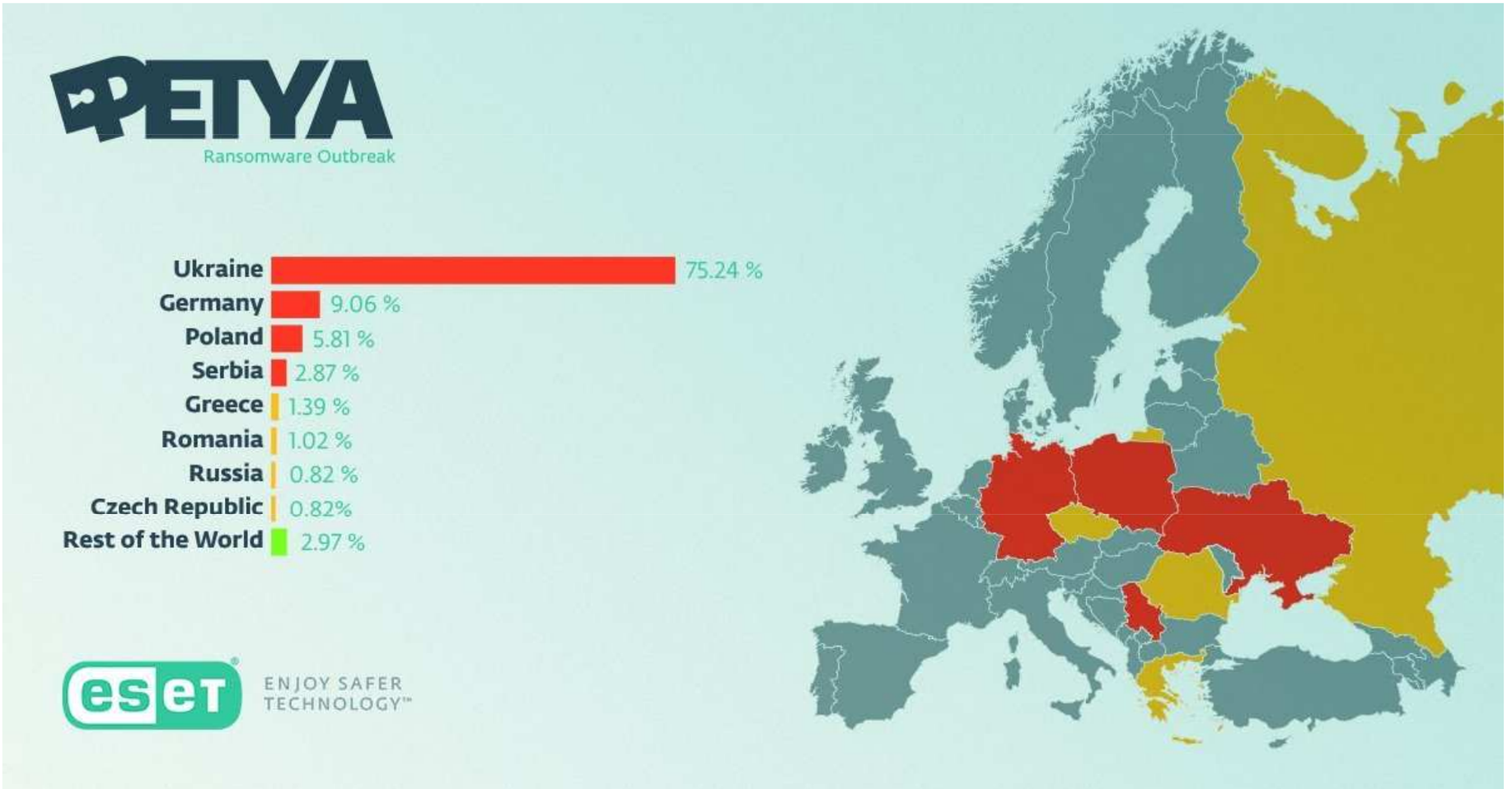
**Características :**

1. **Encripta la tabla MFT en particiones NTFS para posteriormente, sobrescribir el MBR y modificar el *loader para de esta forma anular toda forma opcional de booteo y* para proyectar mensaje de secuestro.**
2. **Esta compuesto por dos componentes o funcionalides a nivel software - un gusano con capacidad de autoreplicarse (usa exploit eternalblue) y el paquete ransomware que realiza la modificación de MBR y el cifrado de la tabla de particiones**
3. **El malware se distribuye entre los equipos de la red que tengan sistemas operativos windows vulnerables a eternalblue / alternativamente el malware explota la vulnerabilidad CVE-2017-0145 (EternalRomance)**
4. **El malware también se distribuye a través de adjuntos de email (archivo rtf u otros similares parte de ingeniería social)**
5. **Solicita un rescate en Bitcoins por el equivalente de 300 USD, para facilitar la llave de decriptacion.**

ISBCorp
Information Security Bolivia
Business Continuity Security & Risk Management

# Petya / Not Petya / GoldenEye

**Mas de 25 países afectados, actualmente el ataque esta controlado se filtro la llame maestra de decrepitación AES 256 : 38dd46801cec61883433048d6d8c6ab8be18654a2695b4723**



ISBCorp
Information Security Bolivia
Business Continuity Security & Risk Management

# Estrategia de Seguridad de Información & Continuidad del Negocio para la gestión del riesgo de ransomware

## Buenas Practicas
## Sistema de Gestión de Seguridad de Información / Sistema de Gestión de Continuidad del Negocio
## ISO 27001 :2013 / ISO 223001

ISBCorp
Information Security Bolivia
Business Continuity Security & Risk Management

# Antes de Ransomware

**Política y/o Procedimientos de Seguridad de Información:**

Licenciamiento de Software
Gestión de Vulnerabilidades Técnicas / Ethical Hacking
Gestión y actualización de Parches de Seguridad
Inventario de Activos de Información (Conocer la criticidad de los activos críticos)
Gestión de Backups / Copias de Seguridad (activos críticos)
Gestión del mail corporativo
Sensibilización corporativa multinivel para todo el personal (ransomware y otros riesgos)

**Planes de Continuidad del Negocio**

Plan de contingencia Bases de Datos (incluya el escenario ransomware)
Procedimiento para la respuesta de incidentes de seguridad de información (ransomware)
Plan de crisis ante la materialización de ransonware
Plan de comunicación  (incluya el escenario ransomware)

ISBCorp
Information Security Bolivia
Business Continuity Security & Risk Management

# Antes de Ransomware

## Controles Técnicos

- Implementación Antivirus / End Point Security - Actualizado, con capacidad de detección de ransomware / antispam
- Implementación de VLANS / Segmentos de Red
- Configuración de Firewalls (Protocolo 455 SMB / reglas específicas sobre lo permitido y denegado)
- Repositorio de información en alta disponibilidad

## Actividades Técnicas

- Deshabilitar macros en Office
- Análisis de Vulnerabilidades / Ethical Hacking a intervalos regulares
- Actualizar con parches de seguridad todos los sistemas operativos
- Reguardo de información en sitio principal y alterno a intervalos regulares
- Pruebas de los planes de continuidad del negocio
- Registro de incidentes relacionados a violaciones de la política y/o procedimientos de seguridad deinformación

ISBCorp
Information Security Bolivia
Business Continuity Security & Risk Management

# Durante ransomware / Procedimiento respuesta incidente

**Actividades Técnicas**

- Usuario : notificar inmediatamente todo mal funcionamiento de software
- Seguridad de Información : Confirmar o descartar la materialización de ransomware
- [Si y solo si se confirma ransomware]

|_ Notificar formalmente la activación de :

**Planes de contingencia**

Plan de crisis, si fuera oportuno

Plan de comunicación, si fuera oportuno

Seguridad de Información: Fin de Crisis

ISBCorp
Information Security Bolivia
Business Continuity Security & Risk Management

# Durante ransomware / Procedimiento respuesta incidente

**PLAN DE CONTINGENCIA**

**[Si se cuenta con Backup]**
|_ Apagar / desconectar computadores de la RED para evitar propagación
|_ Desconectar VLAN / Afectada
|_ Eliminar la infección
|_ Formateo de equipos
|_ Reinstalación de Software
|_ Actualización de Data / (Backup)
|_ Fin incidente

**[Si no se cuenta con Backup]**
|_ Apagar / desconectar computadores de la RED para evitar propagación
|_ Desconectar VLAN / Afectada
|_ Resguardar el equipo hasta que potencialmente se encuentre una solución ,
alternativamente se debe considerar el escenario de perdida de información y sus potenciales impactos (Plan de Crisis / Plan de Comunicaciones)

ISBCorp
Information Security Bolivia
Business Continuity Security & Risk Management

# Después de ransomware / Procedimiento respuesta incidente

**LECCIONES APRENDIDAS / MEJORA CONTINUA DE LA SEGURIDAD**

Documentación de los incidentes de seguridad de información

- Causas
- Efectos
- Estimación de Impactos (Financiero, Legal, Reputacional)
- Recomendaciones para la mejora continua de controles de seguridad de información

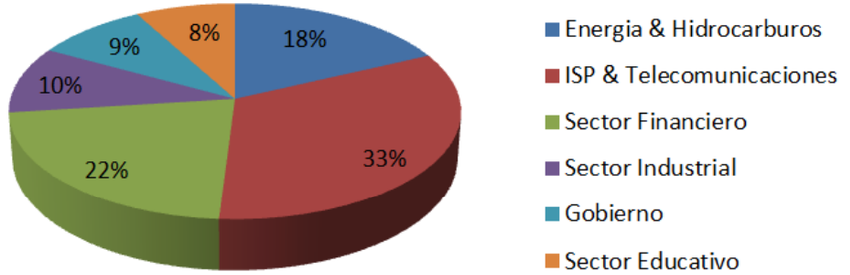
# ISBCorp
Information Security Bolivia
Business Continuity Security & Risk Management

# QUIENES SOMOS - A QUE NOS DE DEDICAMOS -



**ISB es una empresa especialista en Seguridad de la Información, Continuidad del Negocio y Gestión de Riesgo.**

## NUESTRO ENFOQUE POR SECTORES





Subscribe

www.isb.com.bo InformationSecurityBolivia

CyberSecurityXperts
CertifiedEngineers

ISBCorp
Information Security Bolivia
Business Continuity Security & Risk Management

# CAPACITACIONES Y CERTIFICACIONES EN SEGURIDAD DE LA INFORMACIÓN






Subscribe

www.isb.com.bo InformationSecurityBolivia

CyberSecurityXperts
CertifiedEngineers

# GRACIAS POR SU ATENCIÓN

**www.isb.com.bo**