Honeypots

Sergio Anduin Tovar Balderas

Coordinación de Seguridad de la Información

UNAM-CERT

Agenda

- UNAM-CERT y su historia
- Introducción
- Honey(pots|nets)
- Tipos
- Clasificación

Agenda

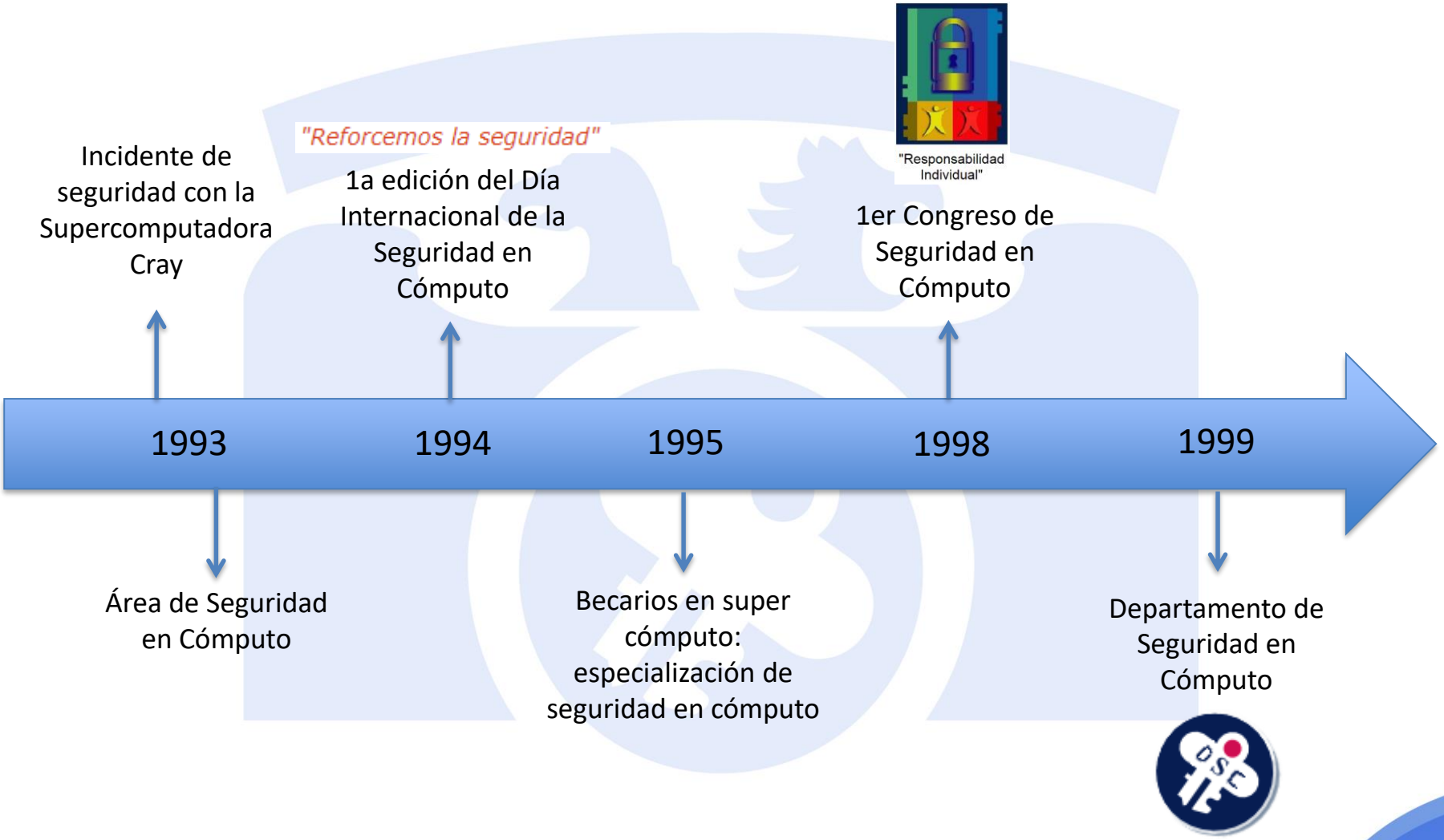
- Proyecto Honeynet UNAM – PHU
- PSTM
- SMART
- RDH

Coordinación de Seguridad de la Información/UNAM-CERT

Contribuir al desarrollo de la UNAM, a través de la prestación de **servicios especializados**, la **formación** de capital humano y el fomento de la **cultura de seguridad de la información**.

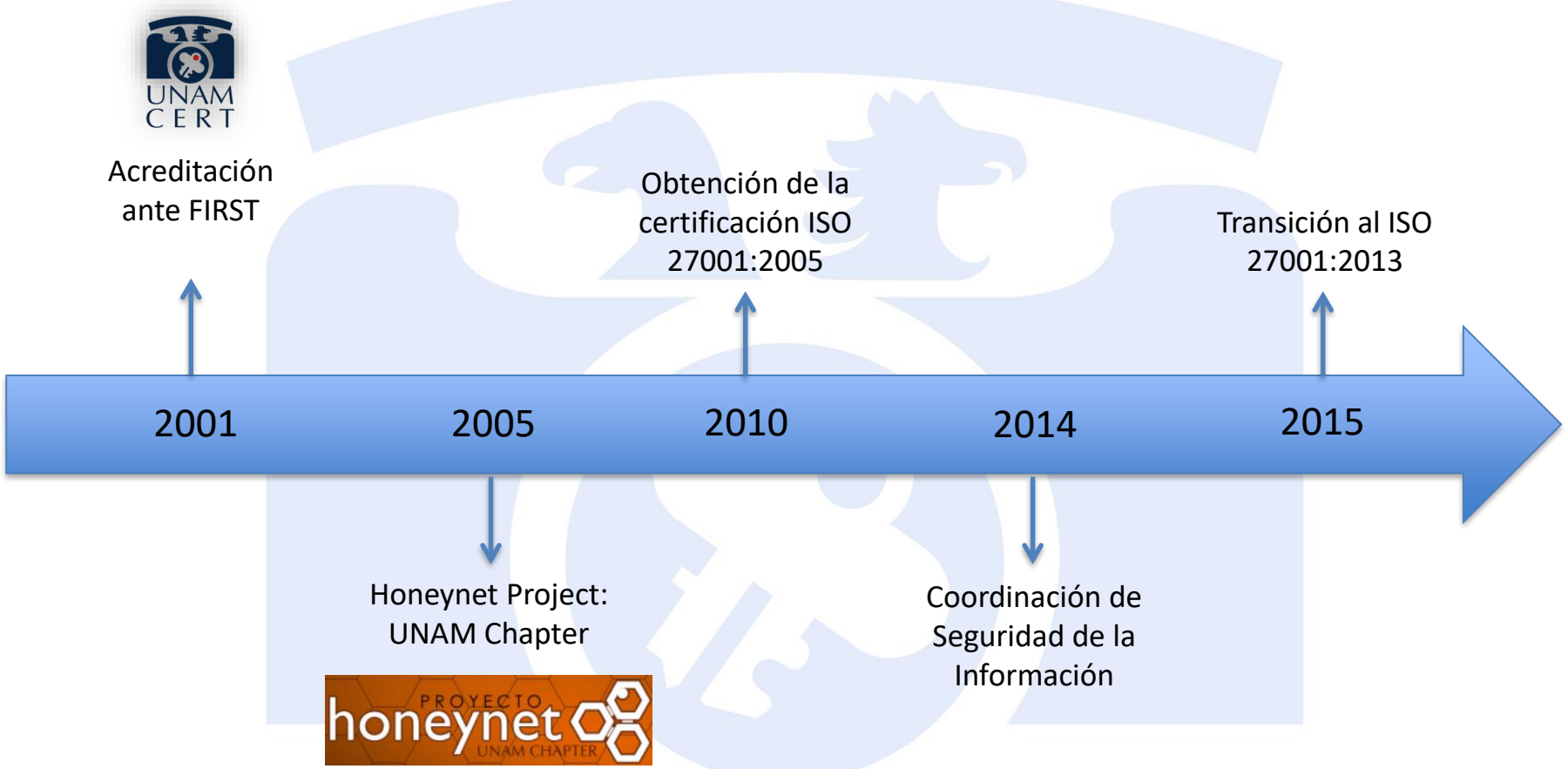
DGTIC

Historia



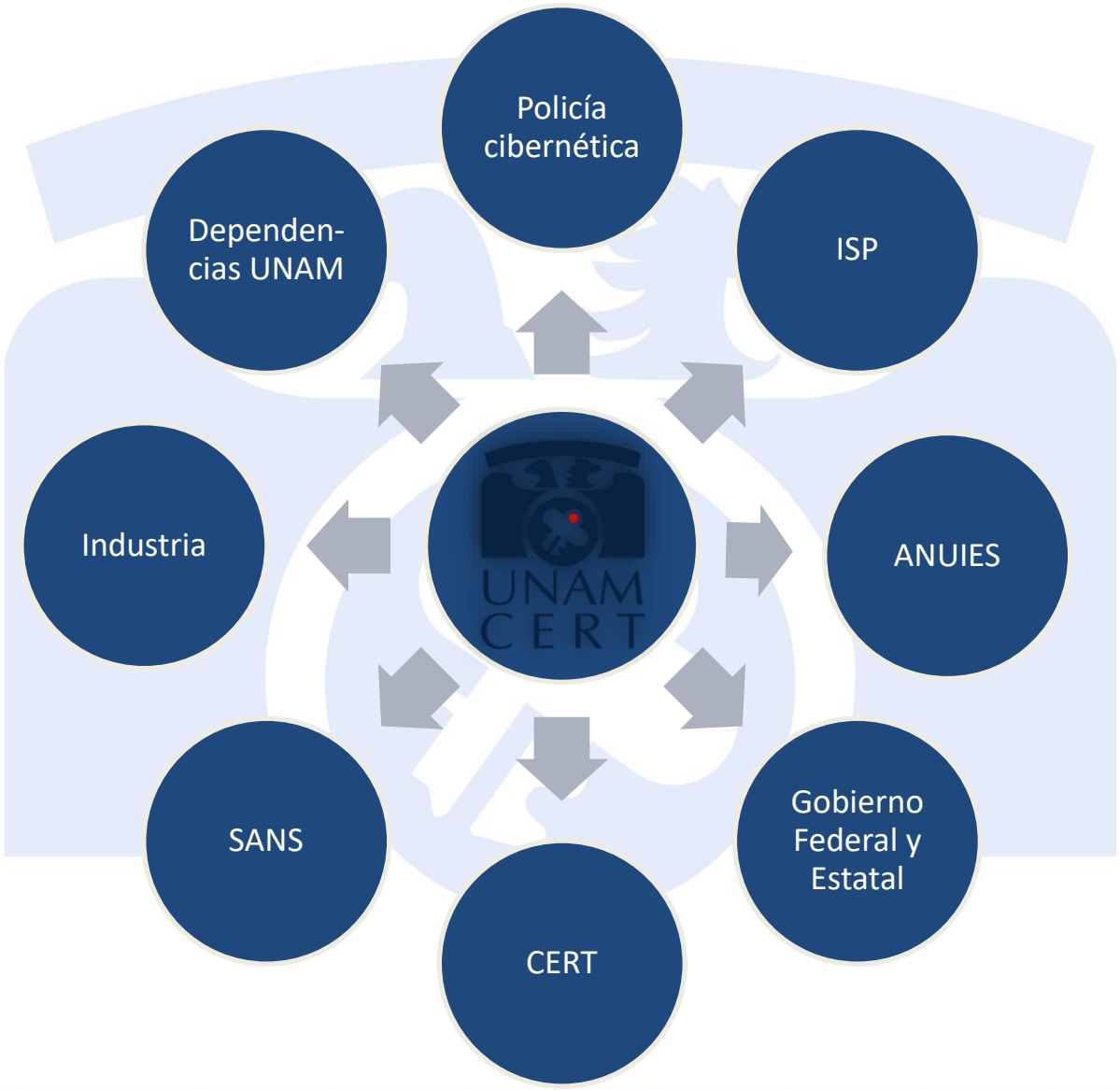
DGTIC

Historia



DGTIC

Colaboración



DGTIC

Universidad Nacional Autónoma de México

La UNAM en números (2017-2018)

- **80 mil 777** computadoras propiedad de la UNAM con conexión a Internet
- **156,701** cuentas activas en la Red Inalámbrica Universitaria
- Capacidad de supercómputo de **232 mil millones** de operaciones aritméticas por segundo

http://www.estadistica.unam.mx/numeralia/

DGTIC

Amenazas

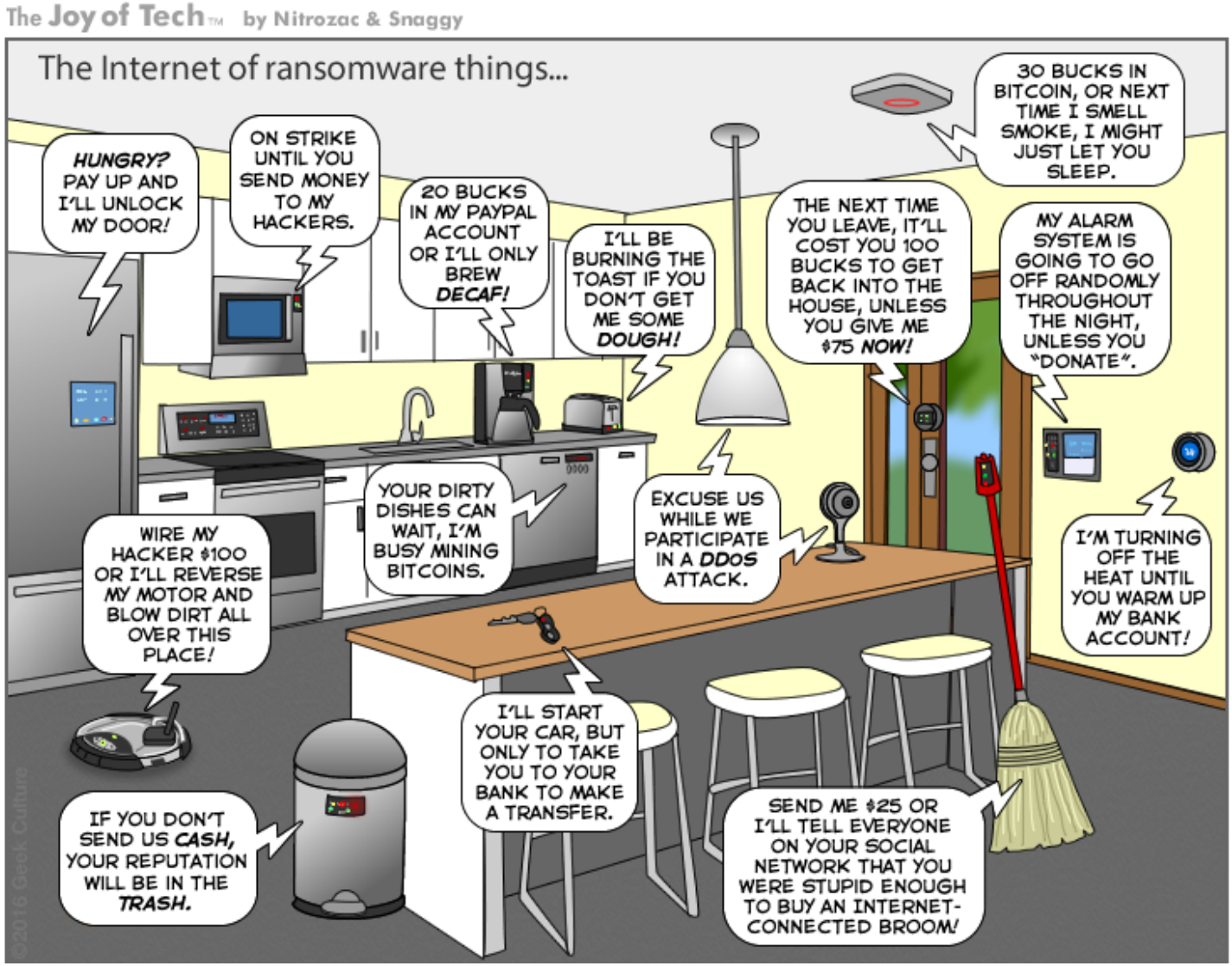
DGTIC

IoT

Internet de las cosas (IoT por sus siglas en inglés)

- Objetos cotidianos conectados a Internet
  - Cámaras
  - Televisores
  - Biométricos
  - Automóviles
- Falta de seguridad (escasa)
  - Contraseñas (hardcode)

IoT



http://www.geekculture.com/joyoftech/joyimages/2340.png

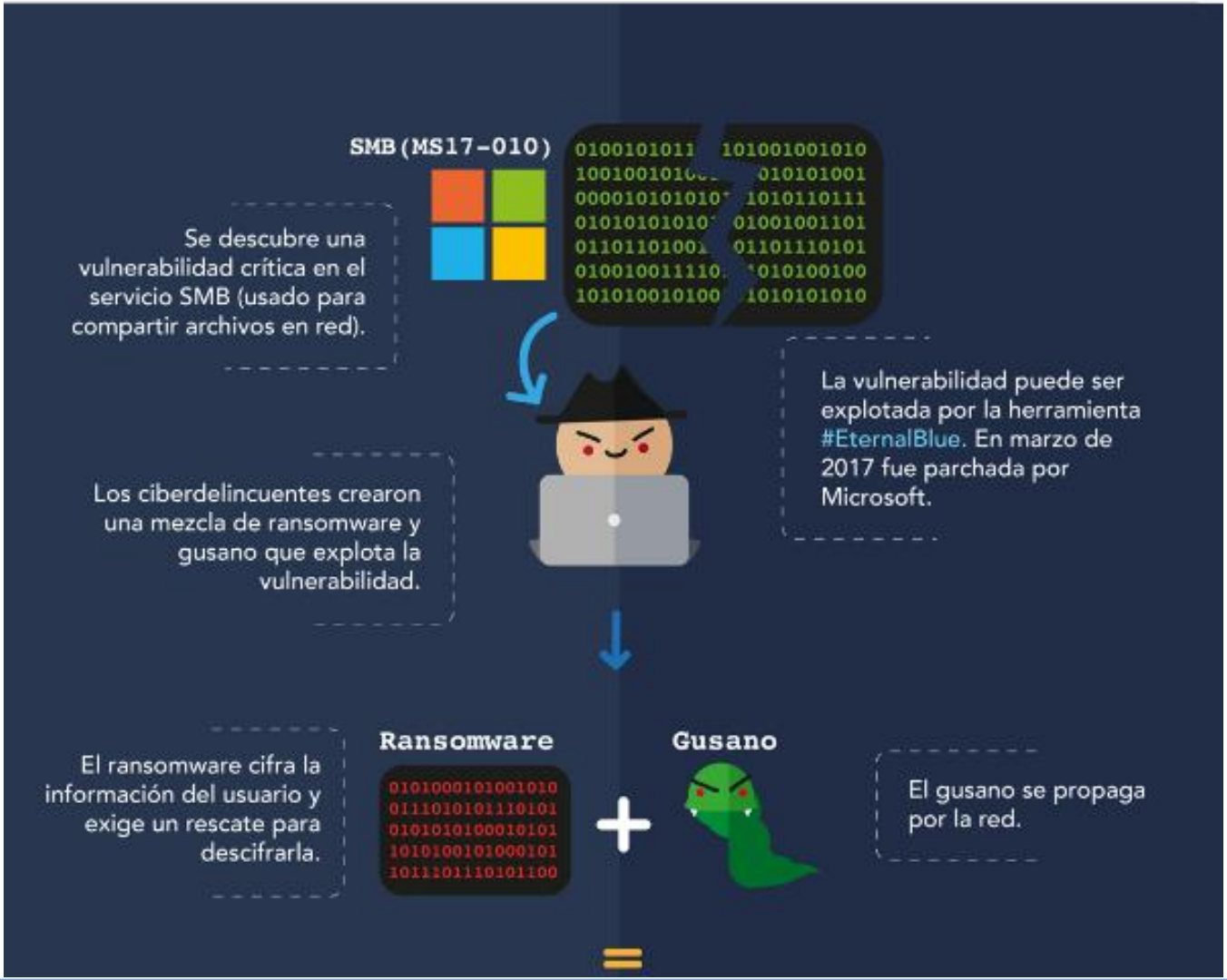
DGTIC

Mirai

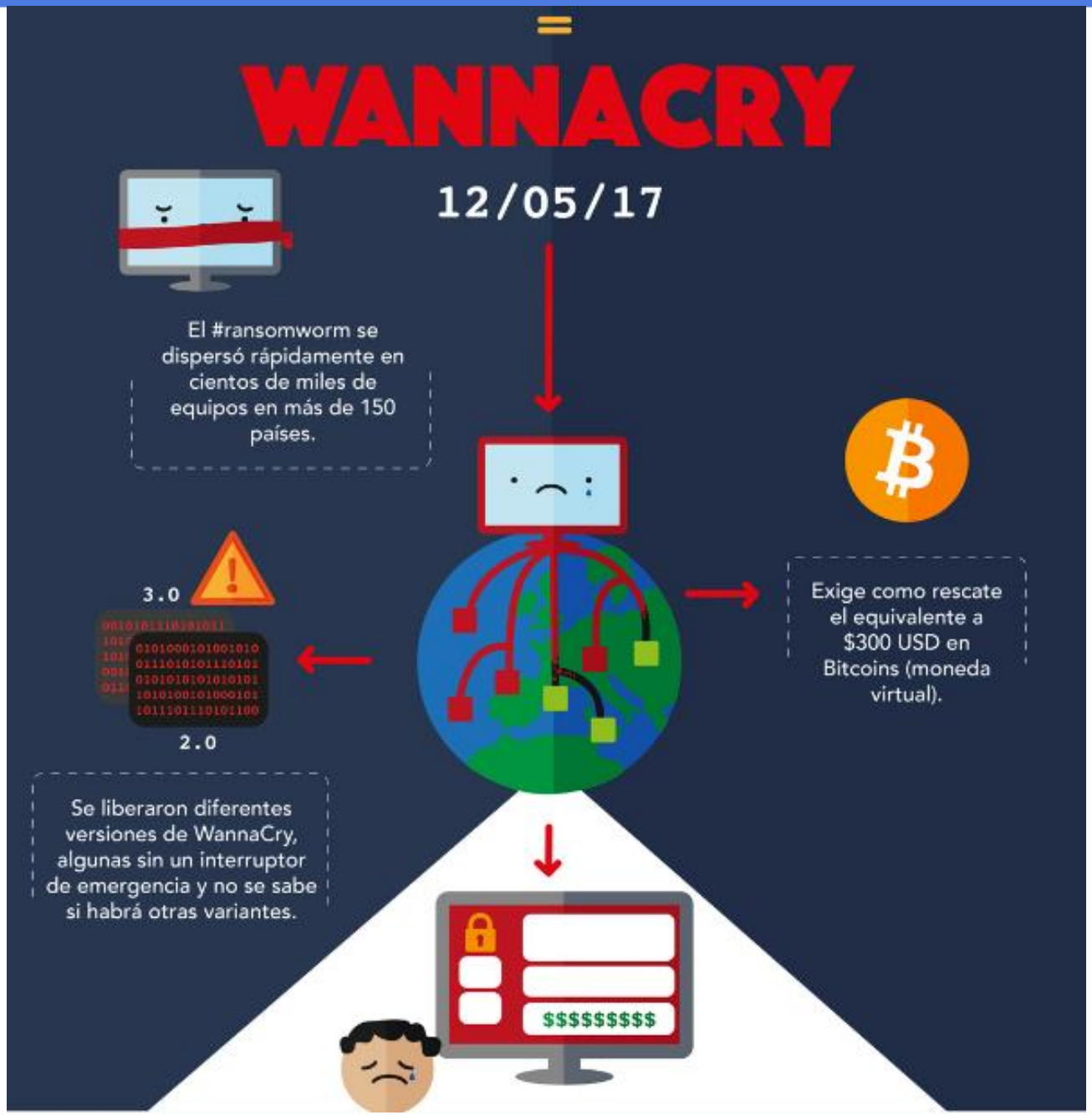
- Malware
  - Ataques de diccionario
- Botnet IoT
- Infectó dispositivos de IoT
  - Cámaras
  - Routers

root	xc3511
root	vizxv
root	admin
admin	admin
root	888888
root	xmhdipc
root	default
root	juantech
root	123456
root	54321
support	support

¡Ataque! WannaCry

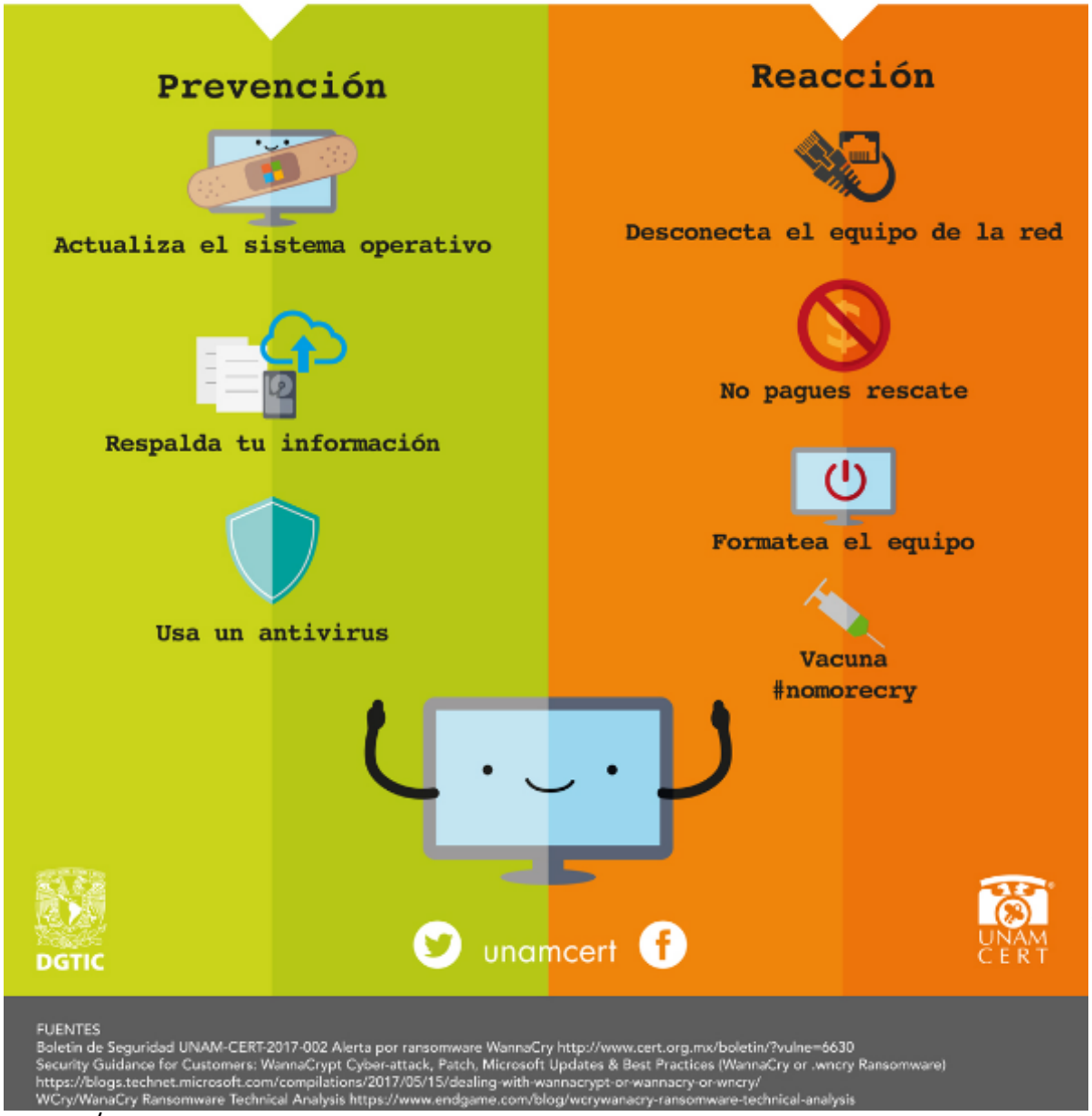


DGTIC


WANNACRY
12/05/17
El #ransomworm se dispersó rápidamente en cientos de miles de equipos en más de 150 países.
Exige como rescate el equivalente a $300 USD en Bitcoins (moneda virtual).
3.0
2.0
Se liberaron diferentes versiones de WannaCry, algunas sin un interruptor de emergencia y no se sabe si habrá otras variantes.
$$$$$$$$

DGTIC

¿Qué hago?



https://www.seguridad.unam.mx/ataque-wannacry

DGTIC

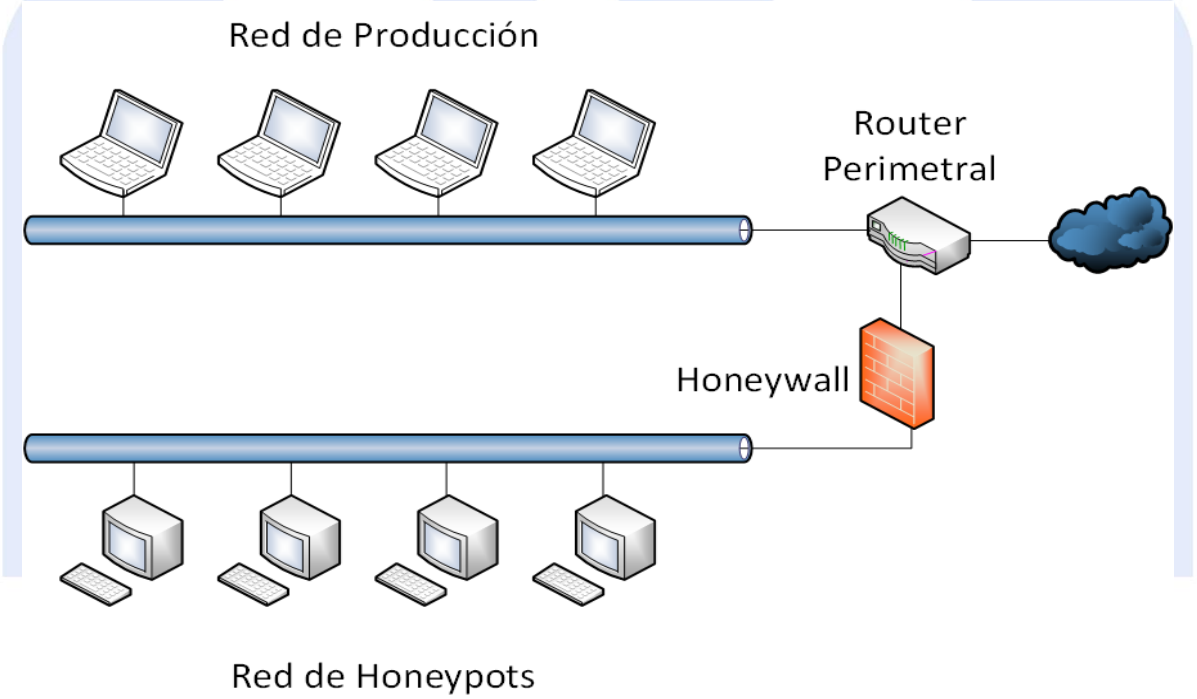
Honeypots

Es un recurso computacional (servicio, aplicación, sistema, etcétera) cuyo único objetivo es ser sondeado, atacado, comprometido o usado de manera no autorizada.

- Surgieron a finales de los años 90
- Mecanismo de detección
- Lance Spitzner introdujo el término honeynet

Honeynets

- Una honeynet está formada por uno o más honeypots desplegados bajo un esquema de control y análisis de tráfico de red.



Tipos

Por su entorno:

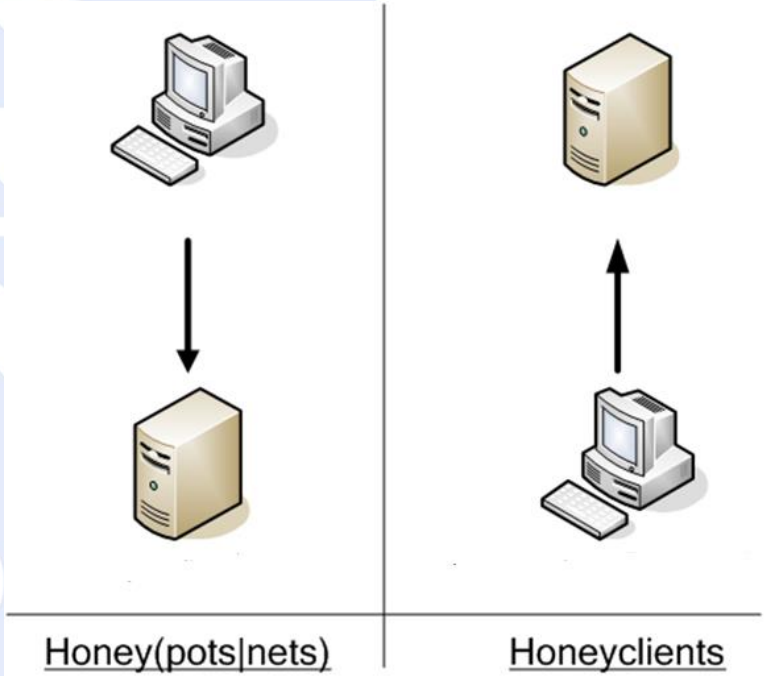
- Honeypots de producción
- Honeypots de investigación

Por su modo de funcionamiento:

- Honeypots de baja interacción
- Honeypots de alta interacción

Por el tipo de recurso:

- Honeypots tipo servidor
- Honeypots tipo cliente



Tecnologías de engaño

Las técnicas de deception como los honeypots no son un nuevo concepto en seguridad.

El engaño se utiliza como una técnica con fines defensivos.

Estas tecnologías están definidas por el uso de:

- Engaños
- Trucos
- Señuelos
- Crean falsas vulnerabilidades/sistemas/servicios
- Generan una respuesta engañosa

Tecnologías de engaño

Propósito

- Detectar
- Frustrar
- Interrumpir
- Obtener información del atacante

Se integran con otras tecnologías

- NGFW
- NGIPS
- Sandbox
- SIEM

Honeypots

- Kippo
- Cowrie
- Glastopf
- Conpot
- Nepenthes
- Dionaea
- Amun
- Elastic honey
- Shockpot
- Wordpot
- HiHat
- IoTCandyJar
- MysqlPot
- telnet-oit-honeypot
- Potd
- HoneyThing

Glastopf: Honeypot de aplicaciones web

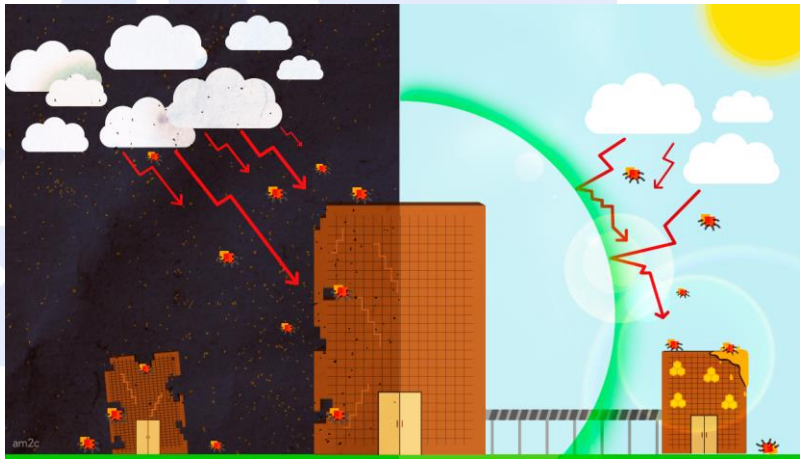
- Baja interacción
- Emular miles de vulnerabilidades web
  - Inserción remota de archivos (RFI)
  - Inyección SQL
  - Inserción local de archivos (LFI)

https://revista.seguridad.unam.mx/numero25/glastopf-honeypot-de-aplicaciones-web-i
https://revista.seguridad.unam.mx/numero26/glastopf-honeypot-de-aplicaciones-web-ii

Cowrie Honeypot: Ataques de fuerza bruta

Diseñado para registrar los ataques de fuerza bruta y la interacción realizada por el atacante

- Media interacción
- Simula un servidor de Secure SHell (SSH) y Telnet
- Registra la actividad del atacante
- Usuario/Contraseña
- Comandos ejecutados



https://revista.seguridad.unam.mx/numero-28/cowrie-honeypot
https://www.youtube.com/watch?v=ZDcCp2-Ezk0&feature=youtu.be

DGTIC

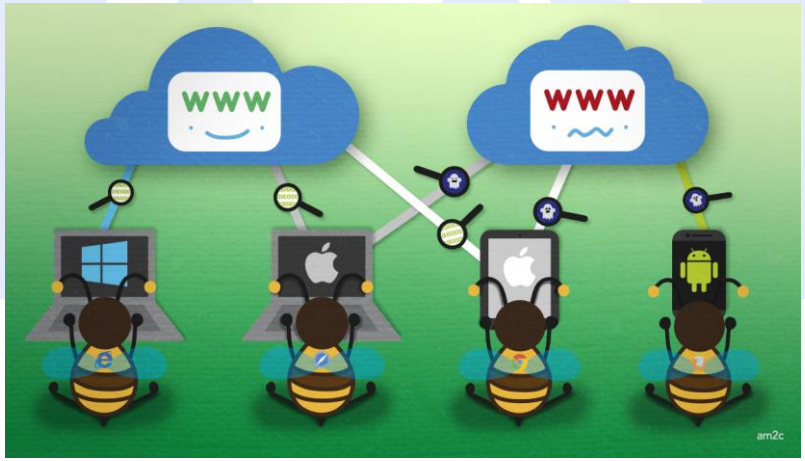
Conpot: Honeypot de Sistemas de Control Industrial

- Honeypot de baja interacción
- Simular Sistemas de Control Industrial (SCADA)
- Obtener los métodos de ataque más comunes a estas plataformas
- Simula un PLC de la compañía Siemens modelo SIMATIC S7-200

https://revista.seguridad.unam.mx/numero29/conpot-honeypot-de-sistemas-de-control-industrial

Thug Honeyclient: Atrapando sitios web maliciosos

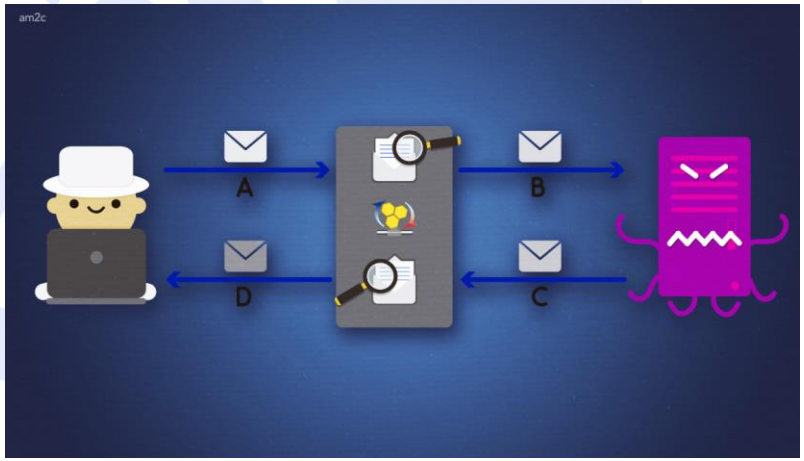
- Cliente honeypot (Honeyclient)
- Análisis híbrido de análisis (estático y dinámico)
- Imitar el comportamiento de un navegador web
- Detectar y emular contenidos maliciosos cuando intentan explotar alguna vulnerabilidad



https://revista.seguridad.unam.mx/numero30/thug-honeyclient-atrapando-sitios-web-maliciosos
https://www.honeynet.unam.mx/es/content/implementacion-del-honeyclient-thug

HoneyProxy: análisis de tráfico HTTP

- Proxy de hombre en el medio
- Permite la inspección y análisis de tráfico HTTP(S) en tiempo real
- Aplicación web o de un dispositivo móvil
- Análisis de tráfico de red durante el análisis dinámico de malware



https://revista.seguridad.unam.mx/content/honeyproxy-analisis-de-trafico-http
https://www.honeynet.unam.mx/es/content/implementacion-de-honeyproxy

DGTIC

¿Qué información obtenemos?

- Comandos ejecutados
- Direcciones IP
- Sitios maliciosos
- Malware
- Exploits

```
stovar@darknet:~$ sudo ls -l /opt/dionaea/var/dionaea/binaries/
total 72
-rw------- 1 nobody nogroup 71168 nov  4 21:06 657598044ddab4537ec2ecae0f14188a
stovar@darknet:~$ sudo md5sum /opt/dionaea/var/dionaea/binaries/657598044ddab4537ec2ecae0f14188a
657598044ddab4537ec2ecae0f14188a  /opt/dionaea/var/dionaea/binaries/657598044ddab4537ec2ecae0f14188a
stovar@darknet:~$ sudo sha256sum /opt/dionaea/var/dionaea/binaries/657598044ddab4537ec2ecae0f14188a
5b2aa53001c0884222bebf931b8235e80cc798c46e3e28c5a4026ccd5590fabf  /opt/dionaea/var/dionaea/binaries/657598044ddab4537ec2ecae0f14188
stovar@darknet:~$
```

https://www.virustotal.com/#/file/5b2aa53001c0884222bebf931b8235e80cc798c46e3e28c5a4026ccd5590fabf/detection

Search or scan a URL, IP address, domain, or file hash

EXE

53 / 66

53 engines detected this file

SHA-256	5b2aa53001c0884222bebf931b8235e80cc798c46e3e28c5a4026ccd5590fabf
File name	1486886645055_rbhdz_dionaea-nyc1_657598044ddab4537ec2ecae0f14188a
File size	69.5 KB
Last analysis	2018-10-19 00:12:22 UTC
Community score	-71

Detection | Details | Relations | Behavior | Community 4

Ad-Aware	Gen:Win32.NetworkWorm.emGfa8dK...	AhnLab-V3	Worm/Win32.MyDoom.C2693347
ALYac	Gen:Win32.NetworkWorm.emGfa8dK...	Antiy-AVL	Worm[Net]/Win32.Agent
Arcabit	Gen:Win32.NetworkWorm.emGfa8dK...	Avast	Win32:Malware-gen
AVG	Win32:Malware-gen	Avira	TR/Dropper.Gen

¿Qué hacemos con la información que obtenemos?

- Anticipación de ataques
- Técnicas y tendencias de ataques
- Análisis de malware
- Mejorar la seguridad

Proyecto Honeynet UNAM

DGTIC

Implementación de HoneyProxy

published by stovar on Jue, 12/14/2017 - 12:03

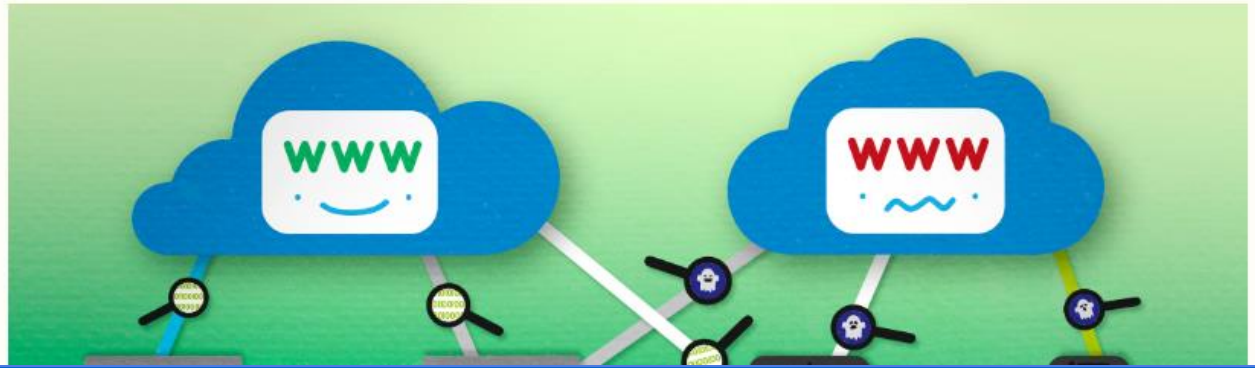
Tags:

honeyproxy HTTP HTTPS proxy mitm man in the middle URL exploit kit malware caché forward proxy de envío reverse proxy inverso transparent proxy transparente

Leer más

Implementación del honeyclient Thug

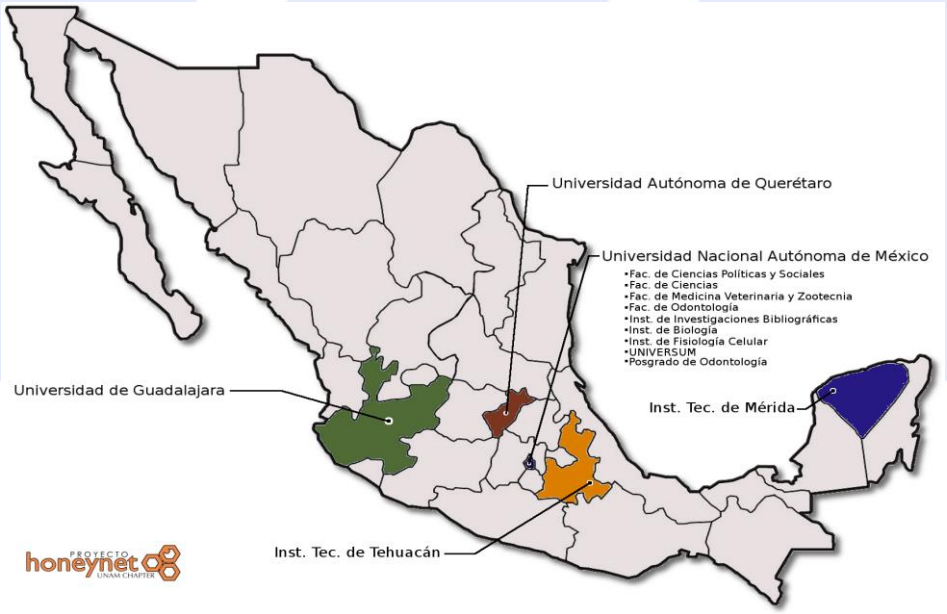
published by stovar on Vie, 10/13/2017 - 16:07



PSTM

Plan de Sensores de Tráfico Malicioso

- Iniciativa del UNAM-CERT
- Crear una red de sensores para la identificación de actividad maliciosa en las redes de datos



DGTIC

SMART

Sensor de Monitoreo, Análisis y Recolección de Tráfico

Compuesto por:

- Honeytrap
- Dionaea
- IDSmod
- Sensorview

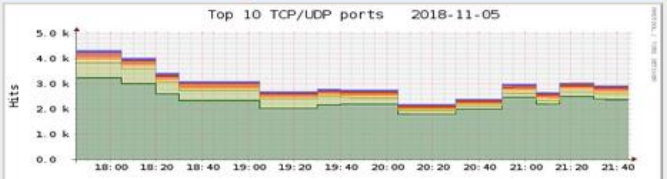
SMART

RedUNAM

PROYECTO honeynet UNAM CHAPTER

Reportes | Tráfico info | Incidentes info | Sistema info | Procesos info | Honeypot | Búsqueda Inc | Eventos | Incidentes | Rules | RedUNAM | Home

Top de Puertos TCP/UDP

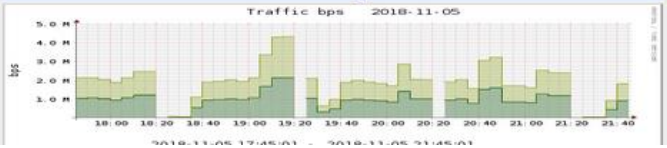


2018-11-05 17:45:01 - 2018-11-05 21:45:01

Protocol	Port	Last	Max	Average
udp	111	2383	3246	2342
tcp	3389	201	601	311
tcp	23	98	108	80
tcp	22	66	83	59
udp	137	46	71	50
tcp	5900	39	56	42
udp	5060	36	55	36
tcp	5901	21	37	27
udp	65535	20	36	25
tcp	5908	19	36	23

honeynet.unam.mx

Tráfico bps



Información actualizada últimos 10 min

Actividad de puertos

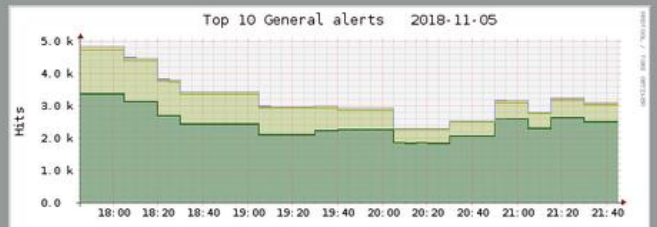
Hits	TCP/UDP
2383	udp/111
201	tcp/3389
98	tcp/23
66	tcp/22
46	udp/137
39	tcp/5900
36	udp/5060
21	tcp/5901
20	udp/65535
19	tcp/5908

Hits	IP
13	5.188.206.247
10	103.207.36.91
10	42.51.38.138
9	185.209.0.3
9	115.42.138.42
7	132.248.10.2
7	104.128.144.131
7	103.1.95.8
6	223.83.252.104
6	196.52.43.53

Actividad de incidentes

Descripcion | Alertas

Incidentes	Descripcion
2513	Unclassified incident
533	General scan port or service (honeypot detection)
55	IP sending SSH Scan/Attack

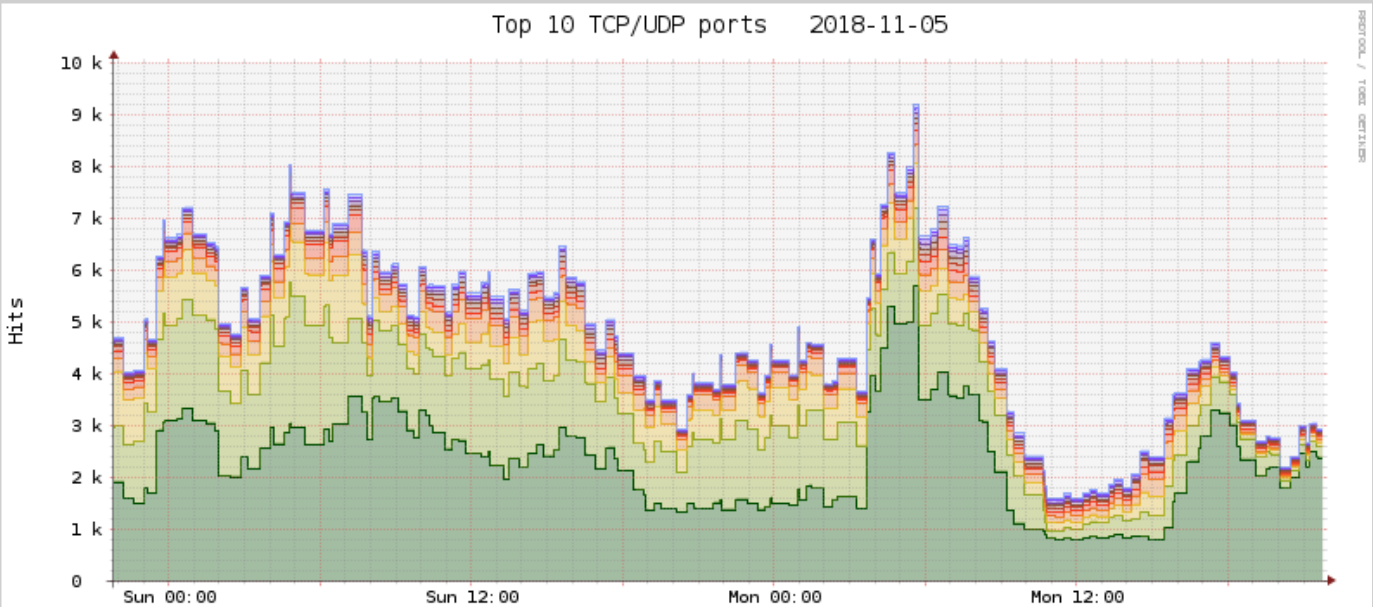


2018-11-05 17:45:01 - 2018-11-05 21:45:01

Alert	Last	Max	Average
Unclassified incident	2513	3378	2441
General scan port or service (	533	1361	741
IP sending SSH Scan/Attack	55	86	59

DGTIC

SMART



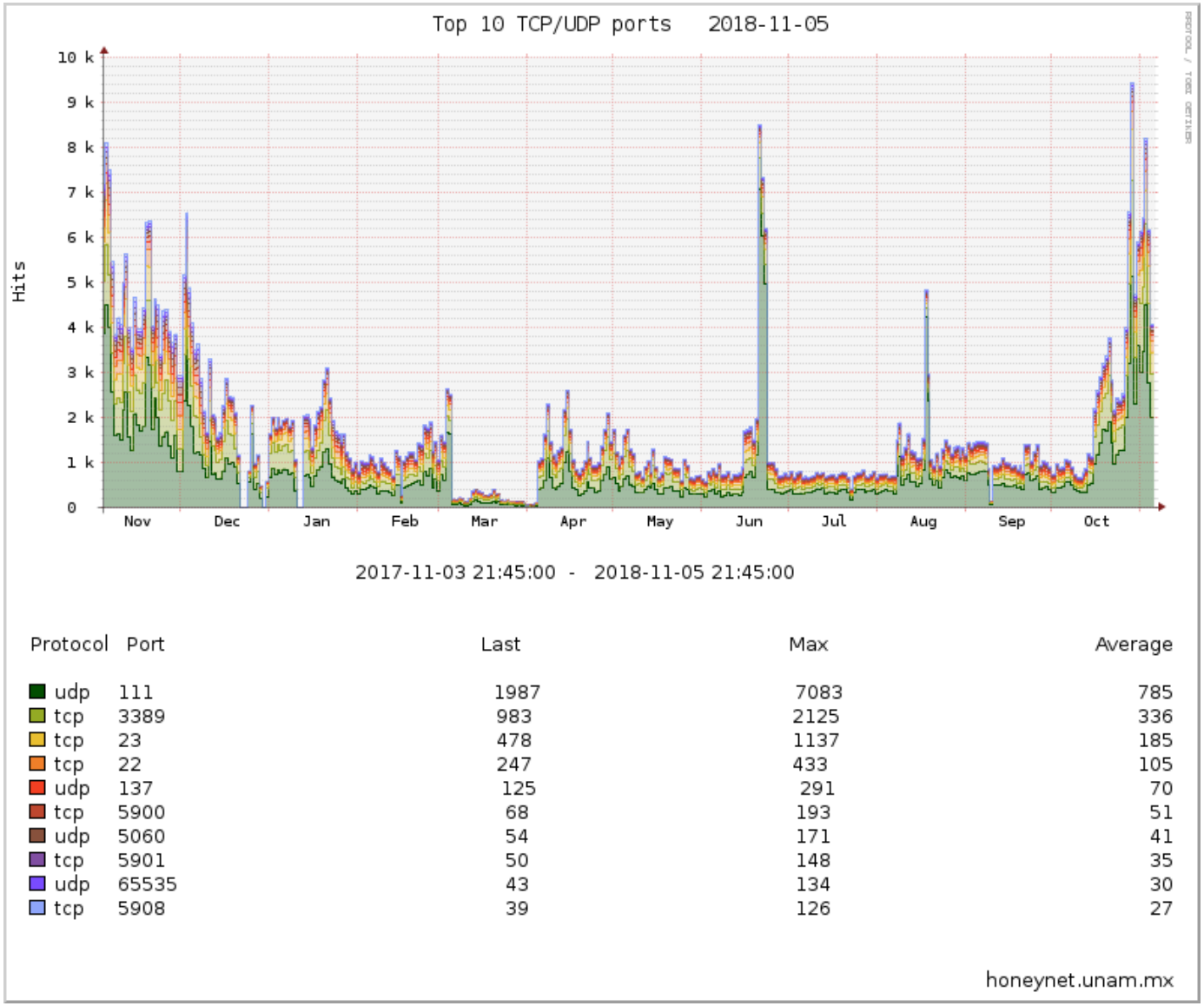
2018-11-03 21:45:01 - 2018-11-05 21:45:01

Protocol	Port	Last	Max	Average
udp	111	2383	5706	2291
tcp	3389	201	2725	1198
tcp	23	98	1311	556
tcp	22	66	473	270
udp	137	46	332	139
tcp	5900	39	165	75
udp	5060	36	135	61
tcp	5901	21	135	54
udp	65535	20	84	44
tcp	5908	19	78	39

honeynet.unam.mx

DGTIC

SMART


Top 10 TCP/UDP ports 2018-11-05
Hits
10 k
9 k
8 k
7 k
6 k
5 k
4 k
3 k
2 k
1 k
0
Nov
Dec
Jan
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep
Oct
2017-11-03 21:45:00 - 2018-11-05 21:45:00
Protocol Port Last Max Average
udp 111 1987 7083 785
tcp 3389 983 2125 336
tcp 23 478 1137 185
tcp 22 247 433 105
udp 137 125 291 70
tcp 5900 68 193 51
udp 5060 54 171 41
tcp 5901 50 148 35
udp 65535 43 134 30
tcp 5908 39 126 27
honeynet.unam.mx

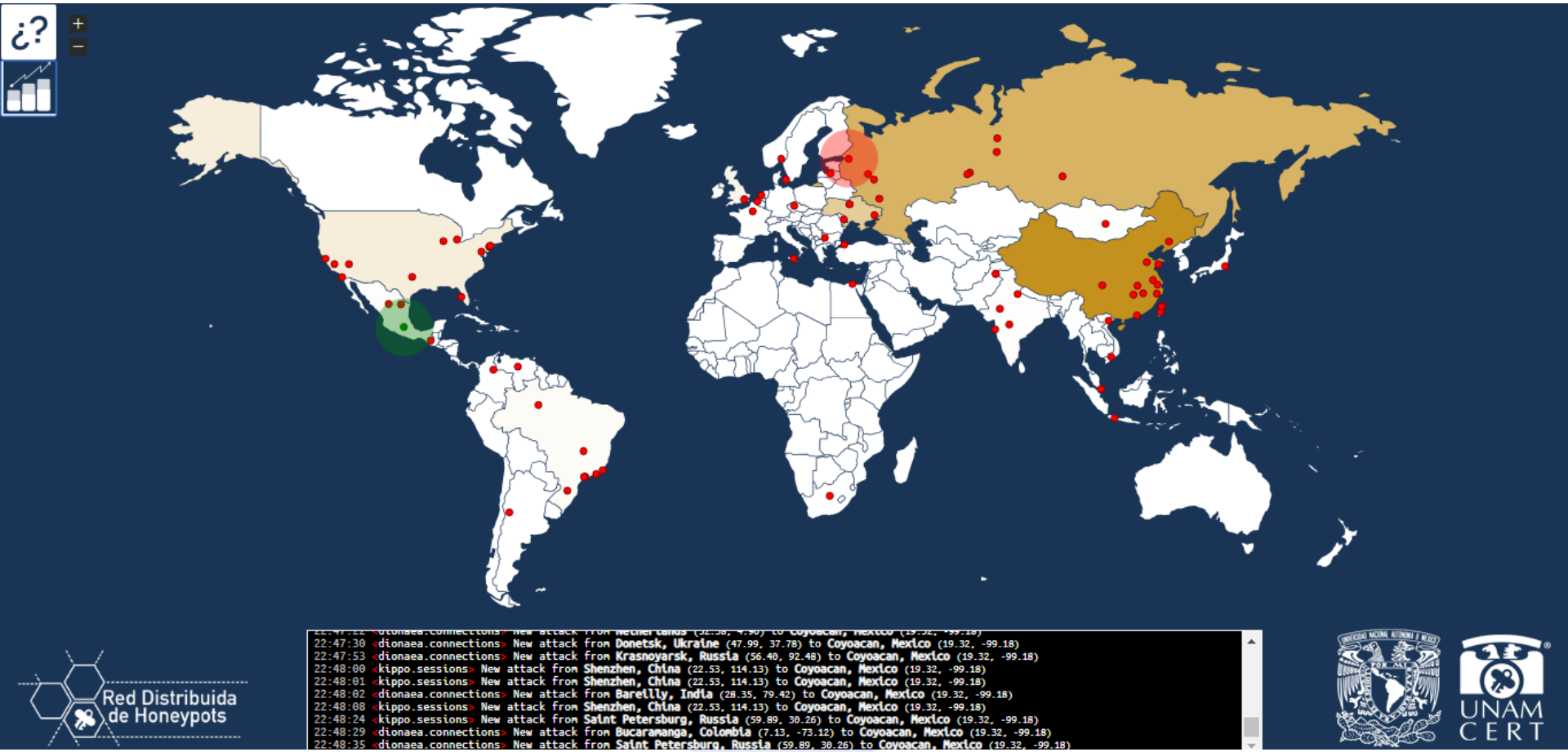
DGTIC

RDH

Red Distribuida de Honeypots

- Ataques en tiempo real
- Honeypots de UNAM-CERT e IES
- Los puntos rojos representan a los atacantes
- Los puntos verdes representan los objetivos

RDH



Red Distribuida de Honeypots

UNAM CERT

DGTIC

Difusión

- Sitio de UNAM-CERT
  - www.cert.unam.mx
  - www.seguridad.unam.mx
- Revista .Seguridad Cultura de prevención para TI
  - revista.seguridad.unam.mx
- Boletín Ouch! (colaboración con SANS Institute)
  - www.seguridad.unam.mx/ouch

Difusión

- Proyecto Honeynet UNAM Chapter
  - www.honeynet.unam.mx
- Red Distribuida de Honeypots
  - map.cert.unam.mx

Redes sociales

Twitter:

@unamcert

Facebook:

/unamcert

YouTube:

/user/SeguridadTV

DGTIC

¡Gracias!

Sergio Anduin Tovar Balderas

anduin.tovar@cert.unam.mx

UNAM CERT

DGTIC

DIRECCIÓN GENERAL DE CÓMPUTO Y DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN