El Ciber-Observatorio y su impacto en la seguridad de redes IP de República Dominicana

James Pichardo. Fundador/Analista Senior
Fundación DO-CSIRT

XVI Congreso Nacional de Seguridad. La Romana, Agosto 2014

CNS
CONGRESO NACIONAL DE SEGURIDAD

DØ-C5IRT

Agenda

- Introducción
- Misión del Ciber-Observatorio
- Metodología y arquitectura
- Números característicos del Ciber-Observatorio
- Estadísticas por puerto escaneado
- Mecanismos de colaboración y resolución de hallazgos
- Proyectos en proceso y futuro
- Conclusiones y próximos pasos

CNS
CONGRESO NACIONAL DE SEGURIDAD

DØ-C5IRT

Introducción

- Misión del Ciber-Observatorio
- Relación DO-CSIRT / Ciber-Observatorio
- Penetración del Internet en República Dominicana y su importancia en el contexto de la investigación
- Presencia del Ciber-Observatorio en LAC
- Próximas presentaciones relacionadas al Ciber-Observatorio

DØ-C5IRT

Internet Fast Scanning

Paper seminal:
"On the Mismanagement and Maliciousness of Networks"
Jing Zhang, Zakir Durumeric, Michael Bailey, Manish Karir, and Mingyan Liu

Network and Distributed System Security Symposium (NDSS), San Diego, CA, February 2014

- Aunque ya existían técnicas y herramientas de gran escala, es el año pasado que se producen hitos importantes
- La idea es escanear con el menor tráfico posible
- Escaneo responsable es clave
- Se usa un conjunto de herramientas: zmap, nmap, python y shell scripts propietarios

CNS CONGRESO NACIONAL DE SEGURIDAD

DØ-C5IRT

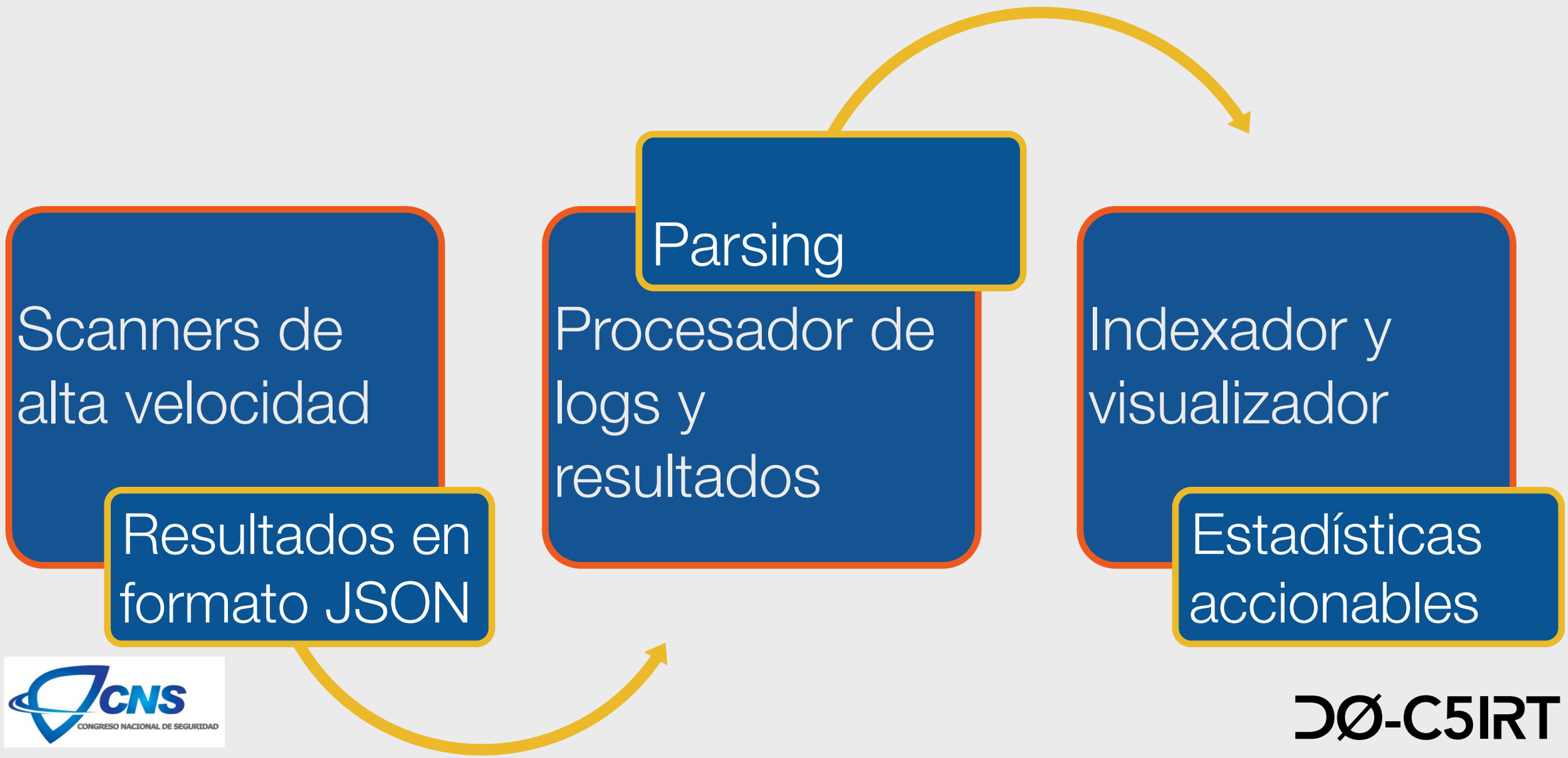
Escaneo Responsable

- Estipula una base procedimental sobre la cual basar actividades de investigación genuinas
- Principios:
  - Transparencia acerca de la naturaleza investigativa de los escaneos
  - Evitar tácticas de investigación que puedan afectar de manera adversa las redes que se investigan
  - Respeto a la solicitud de exclusiones
  - Evitamos a toda costa la explotación de vulnerabilidades (aunque nos topemos de frente con una)

DØ-C5IRT

Arquitectura y metodología

- Escaneo responsable ejecutado de manera periodica
- Anomalías son investigadas



CNS CONGRESO NACIONAL DE SEGURIDAD

DØ-C5IRT

Números del Ciber-Observatorio

- 993,273 direcciones IP escaneadas (0.02% del total)
- Entre 10 y 15 puertos (UDP/TCP) escaneados
- Cada 15-20 minutos se escanea
- Entre 2-4 Mbps de tráfico de los scanners por aproximadamente 2 minutos. Esto es por cada puerto escaseado

DØ-C5IRT

Números del Ciber-Observatorio

- 15 scanners localizados en cuatro continentes
- Capacidad de mas 10TB de tráfico
- 2 probes por cada IP
- Sólo 3 “quejas” en 6 meses. Una solicitud de eliminación de la lista
- Mas de 350,000 archivos de datos
- Mas de 1TB de datos (raw) de escaneo

DØ-C5IRT

HTTP (TCP/80)

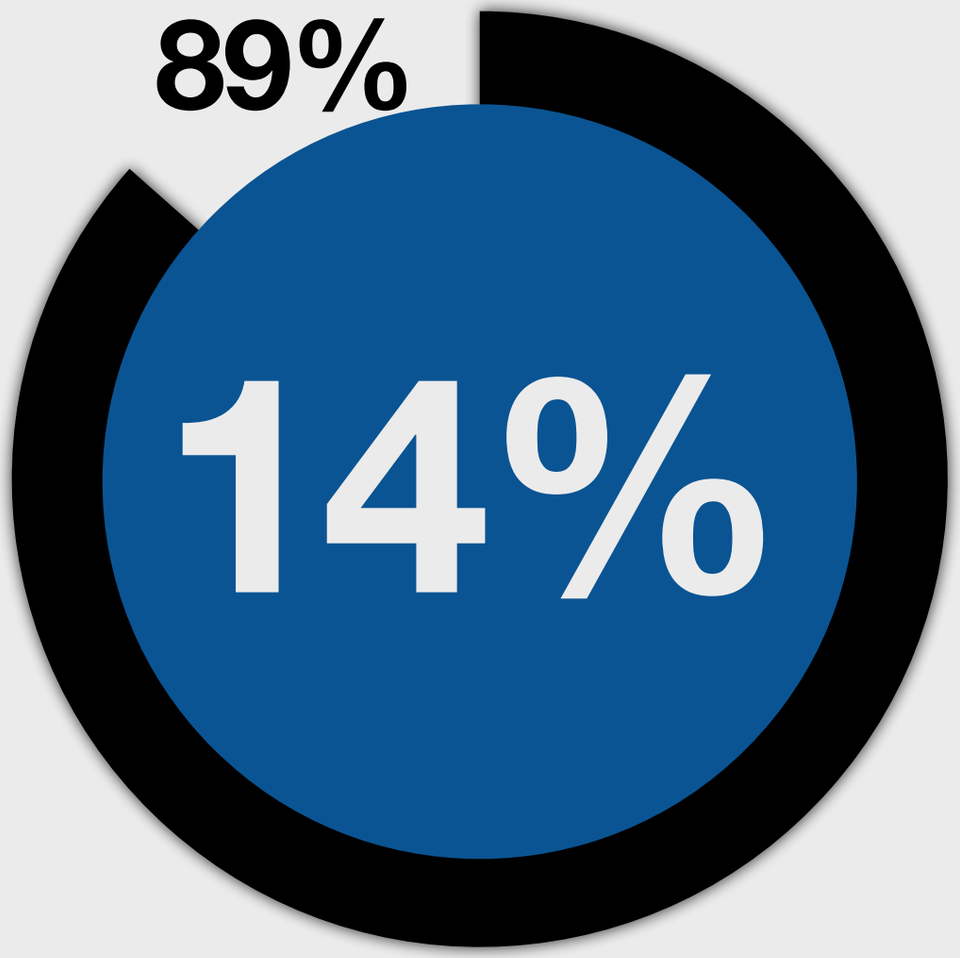
Un alto porcentaje de la cantidad de IPs con el protocolo HTTP son CPEs (dispositivos de accesso a Internet en premisas del cliente).

Infraestructura expuesta

Proxies abiertos

- **Cantidad promedio de servidores: 141,861 (14% del total)**
- **Categorización**
  - **Microsoft: 796 con 13 categorías**
  - **Thomson: 13,303**
  - **micro_httpd: 10,314**
  - **“sharer”: 7,638**
  - **Speedtouch: 14,096**
  - **HG532e: 45,314**
  - **Cisco: 1,247**

HTTP (TCP/80)

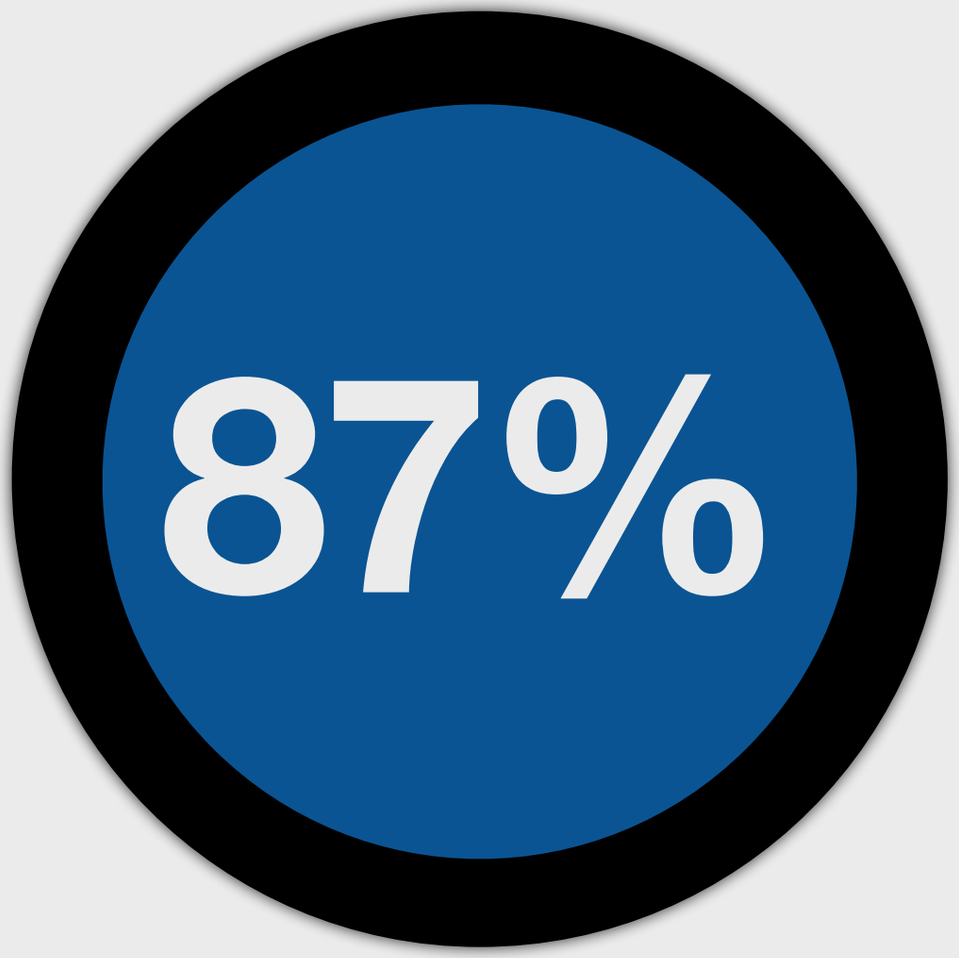


Porcentaje de IPs exponiendo servicios Web y porcentaje de IPs que representan CPEs

CNS
CONGRESO NACIONAL DE SEGURIDAD

DØ-C5IRT

DNS (UDP/53)

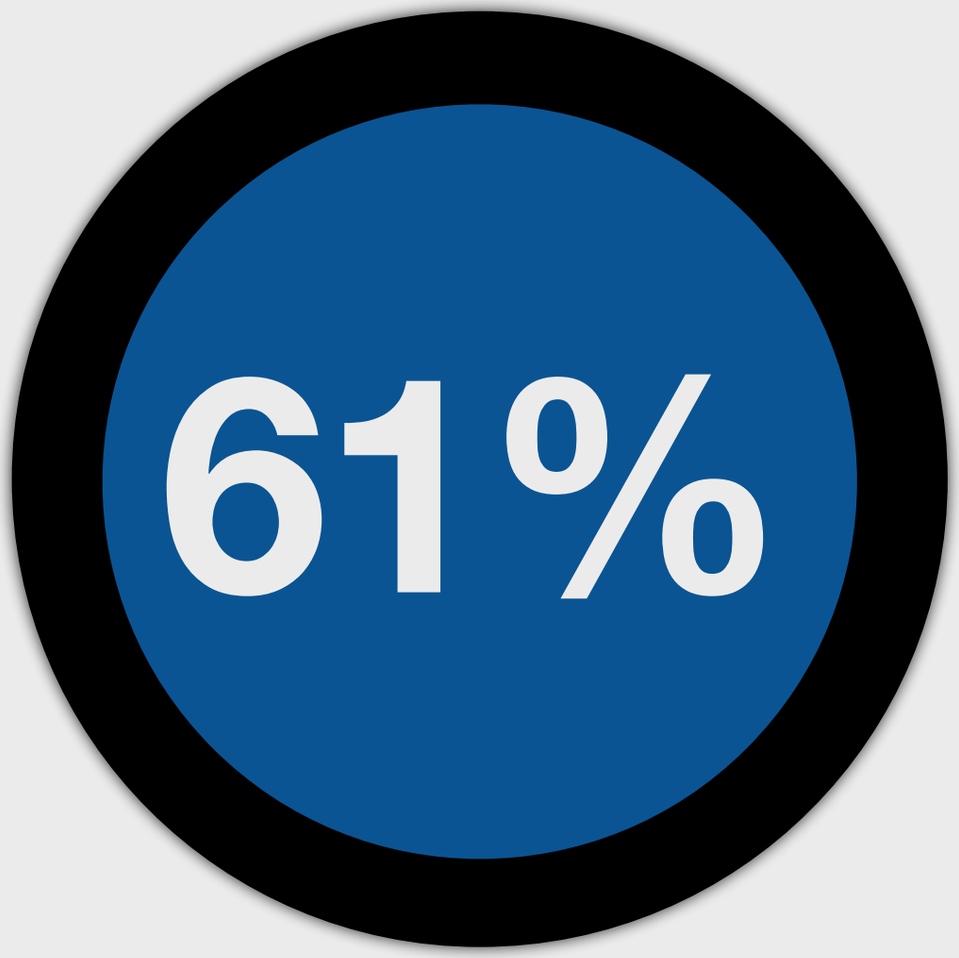


- 1,889 direcciones IPs exponiendo servicios de DNS
- 1,649 son “open resolvers”
- Problemas para la superficie de ataque: amplificación DNS, fast flux domains, etc.
- Validez de las respuestas a queries?

CNS
CONGRESO NACIONAL DE SEGURIDAD

DØ-C5IRT

RDP (TCP/3389)



- 1,816 direcciones IPs exponiendo servicios de Remote Desktop (Windows
- 1,118 tienen encriptamiento débil
- Indicador de que no hay un so extensivo de VPN como mecanismo de gestión remota (malas prácticas)
- Cuantos son Windows XP

CNS
CONGRESO NACIONAL DE SEGURIDAD

DØ-C5IRT

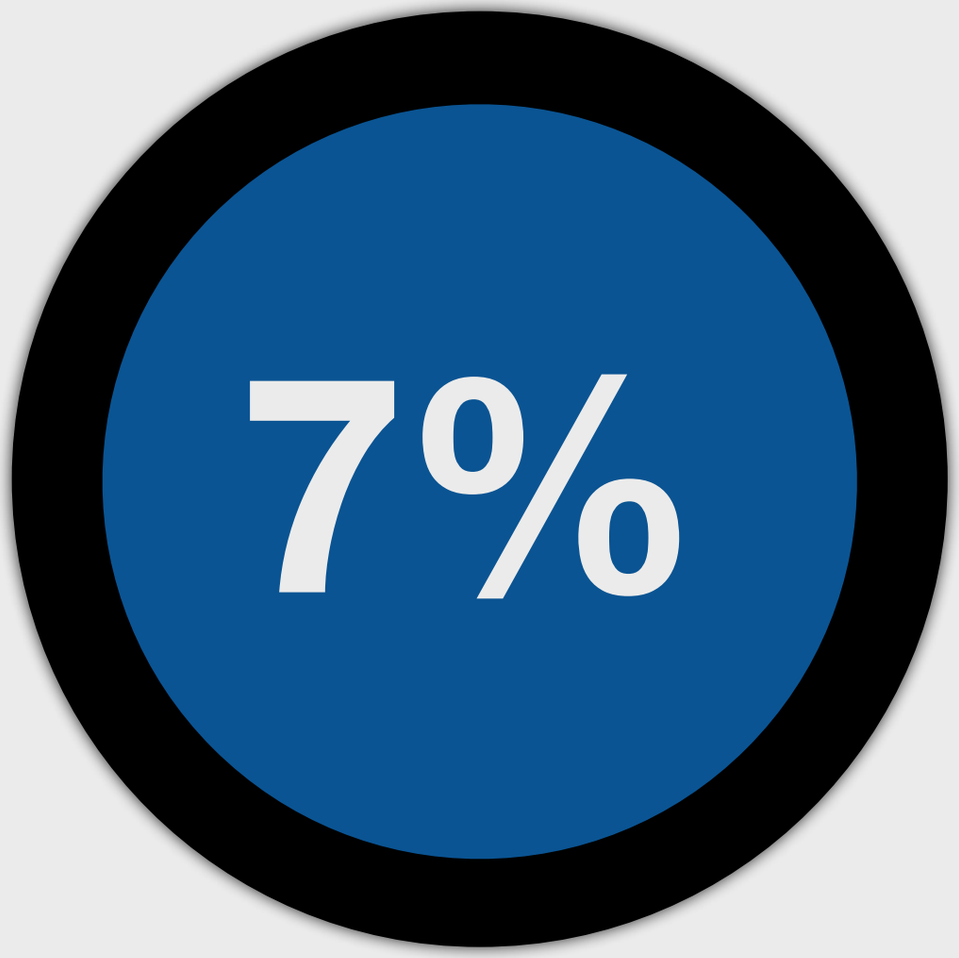
Windows/SMB (TCP/445)

- 493 direcciones IPs exponiendo servicios SMB (comúnmente asociados a Windows)
- Windows XP: 124
- Windows 7: 121
- Windows 8: 18
- Windows XP ya no tiene soporte de Microsoft. Muy faciles de comprometer

CNS
CONGRESO NACIONAL DE SEGURIDAD

DØ-C5IRT

SMTP (TCP/25)

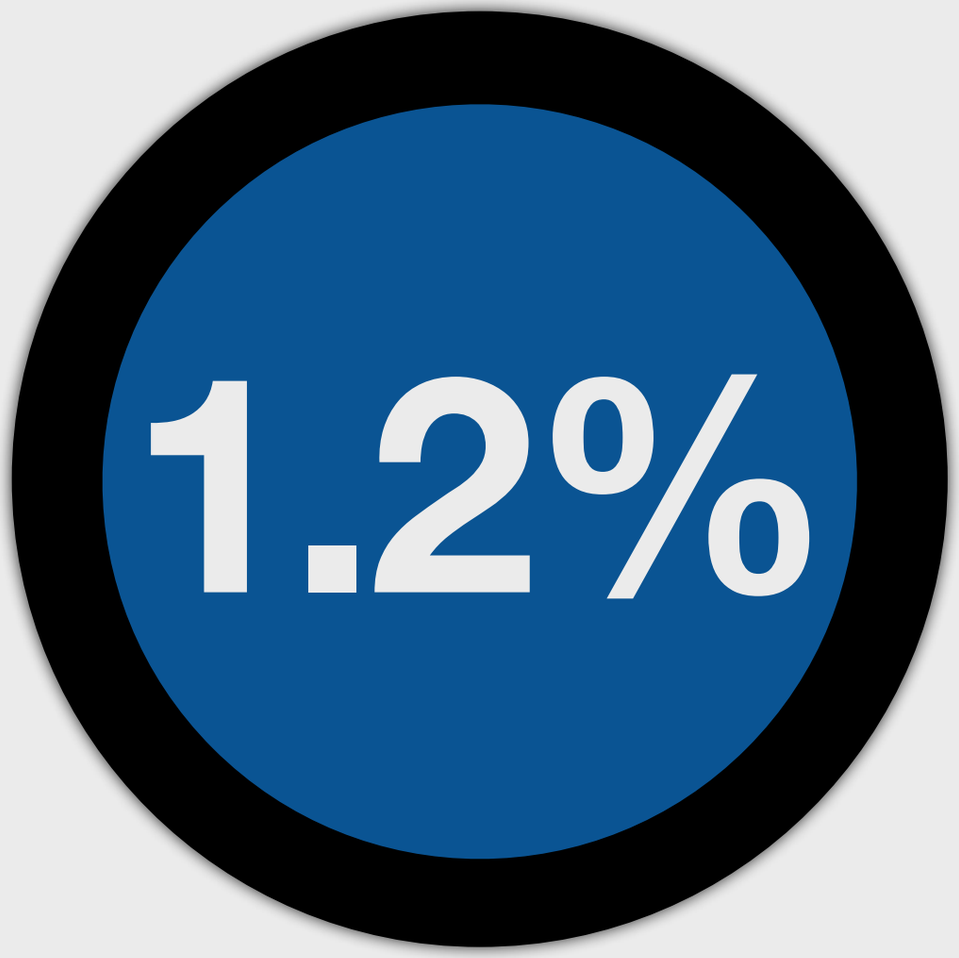


- 642 direcciones IPs exponiendo servicios SMTP (servidores de correo electrónico)
- 45 identificados como open SMTP relays (SPAM)
- Algunos relays identifican compañías comerciales y del estado

CNS
CONGRESO NACIONAL DE SEGURIDAD

DØ-C5IRT

HTTPS (TCP/443)



- 13,111 direcciones IPs exponiendo servicios HTTPS (transacciones seguras vía web)
- 159 servidores con vulnerabilidad HeartBleed
- Muchos de los dispositivos encontrados son firewalls o appliances VPN

CNS
CONGRESO NACIONAL DE SEGURIDAD

DØ-C5IRT

Aspectos críticos

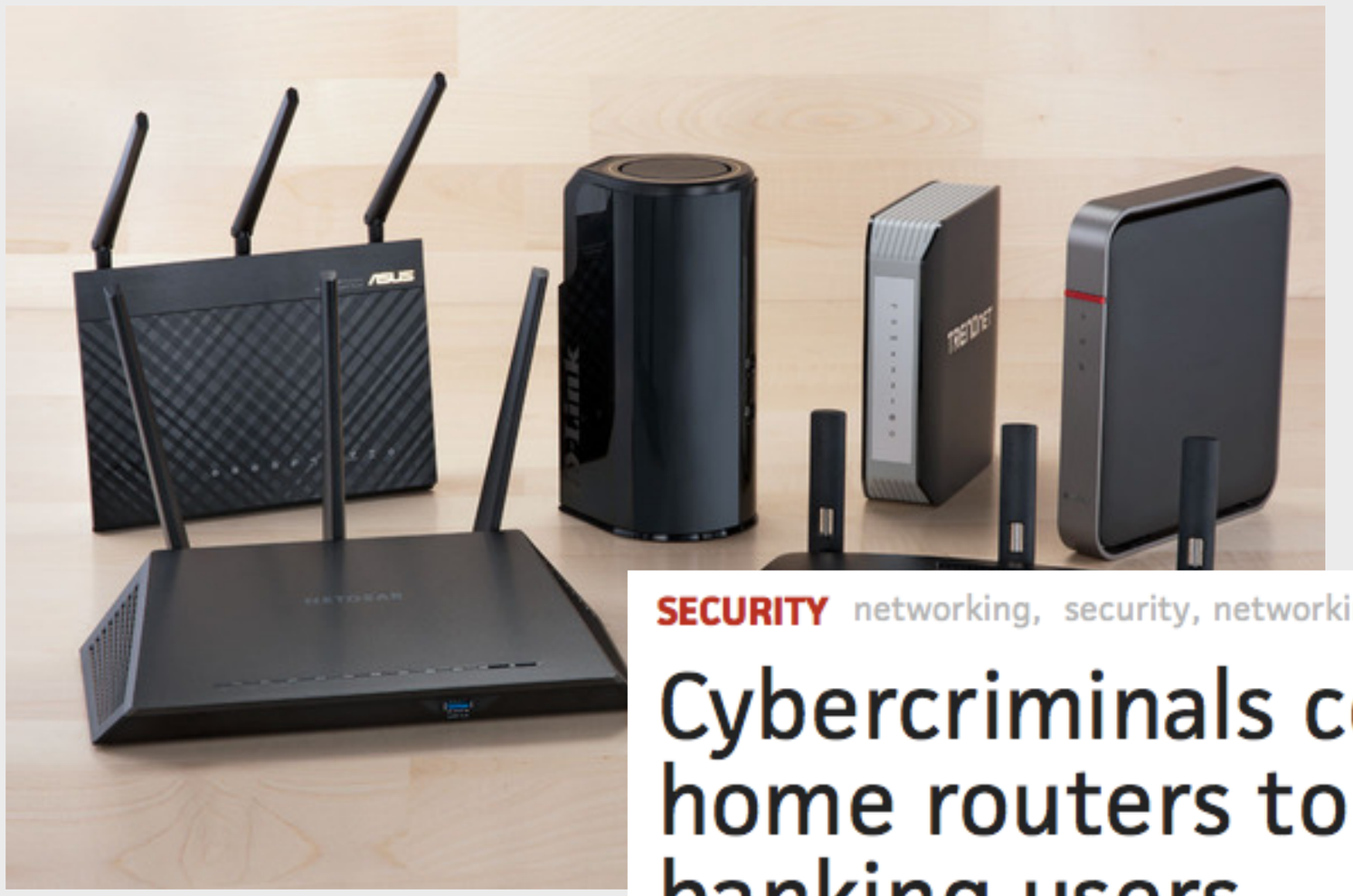
CPEs sin passwords

CPEs con passwords por defecto

CNS
CONGRESO NACIONAL DE SEGURIDAD

DØ-C5IRT

Problemas para los clientes de bancos



SECURITY networking, security, networking, network security, routers, phishing

Cybercriminals compromise home routers to attack online banking users

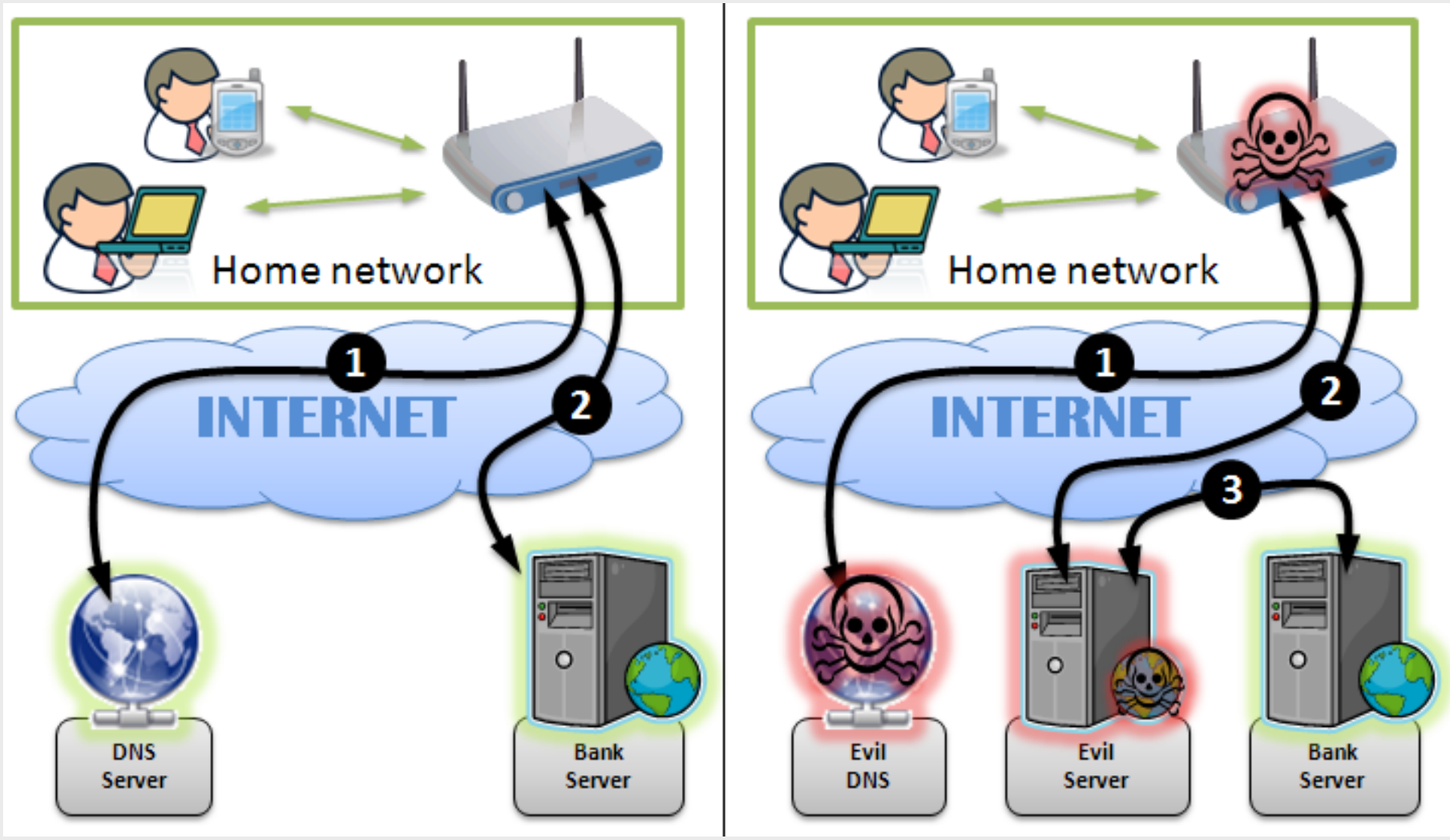
Lucian Constantin

Feb 7, 2014 12:24 PM

CNS CONGRESO NACIONAL DE SEGURIDAD

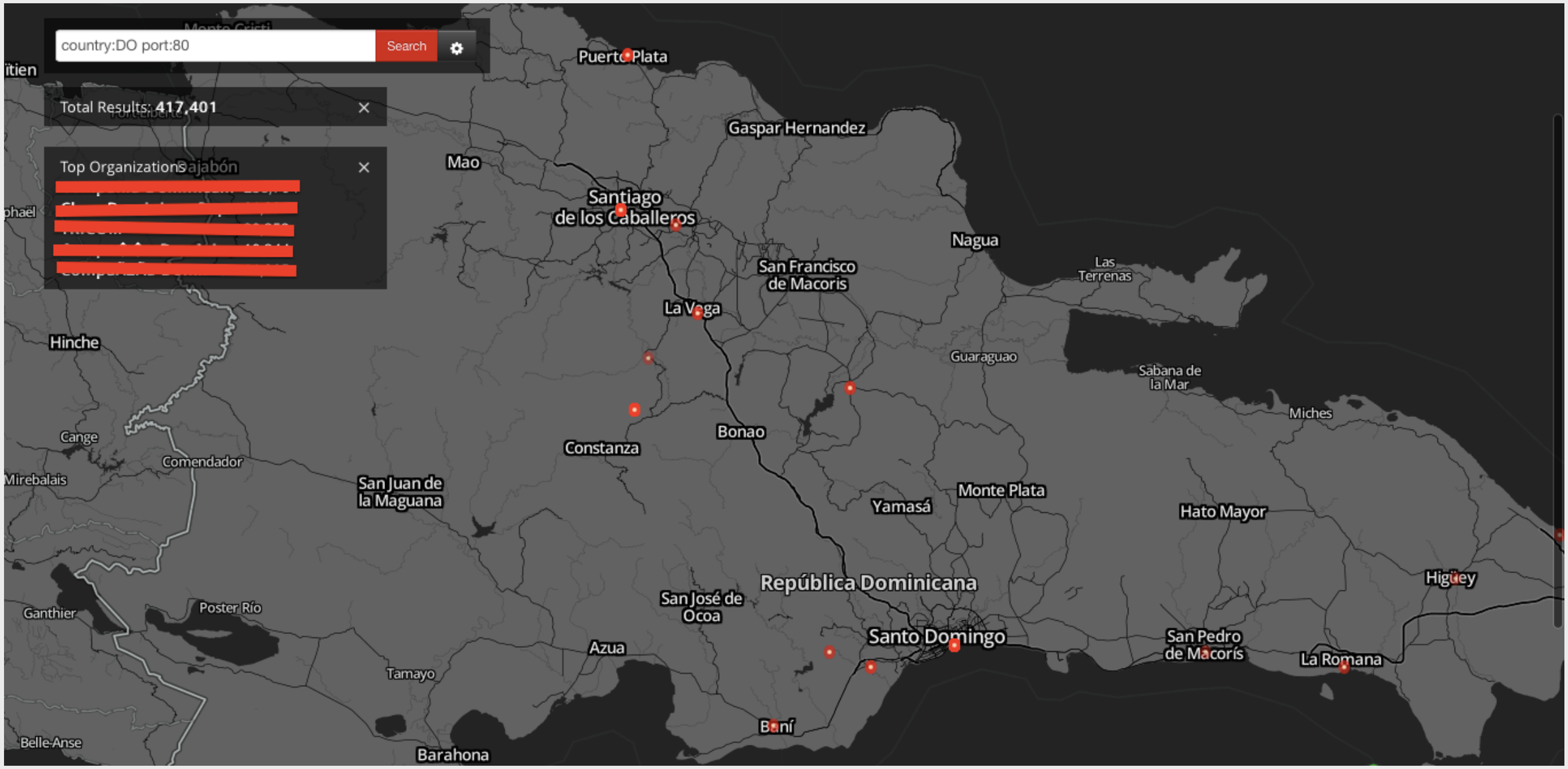
DØ-C5IRT

Problemas para los clientes de bancos



Gráfica cortesía de CERT.PL

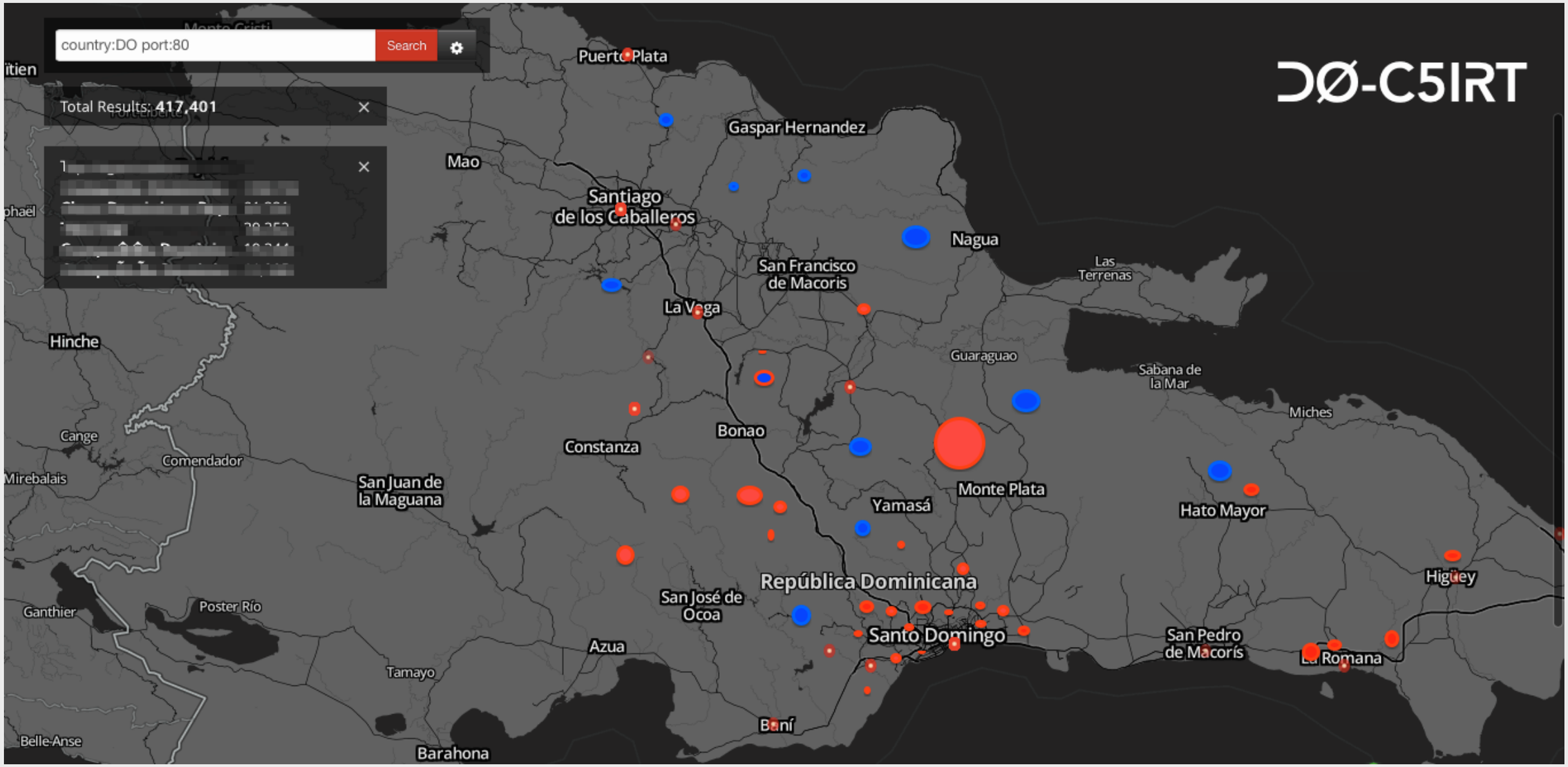
En proceso: interfaz de acceso



CNS
CONGRESO NACIONAL DE SEGURIDAD

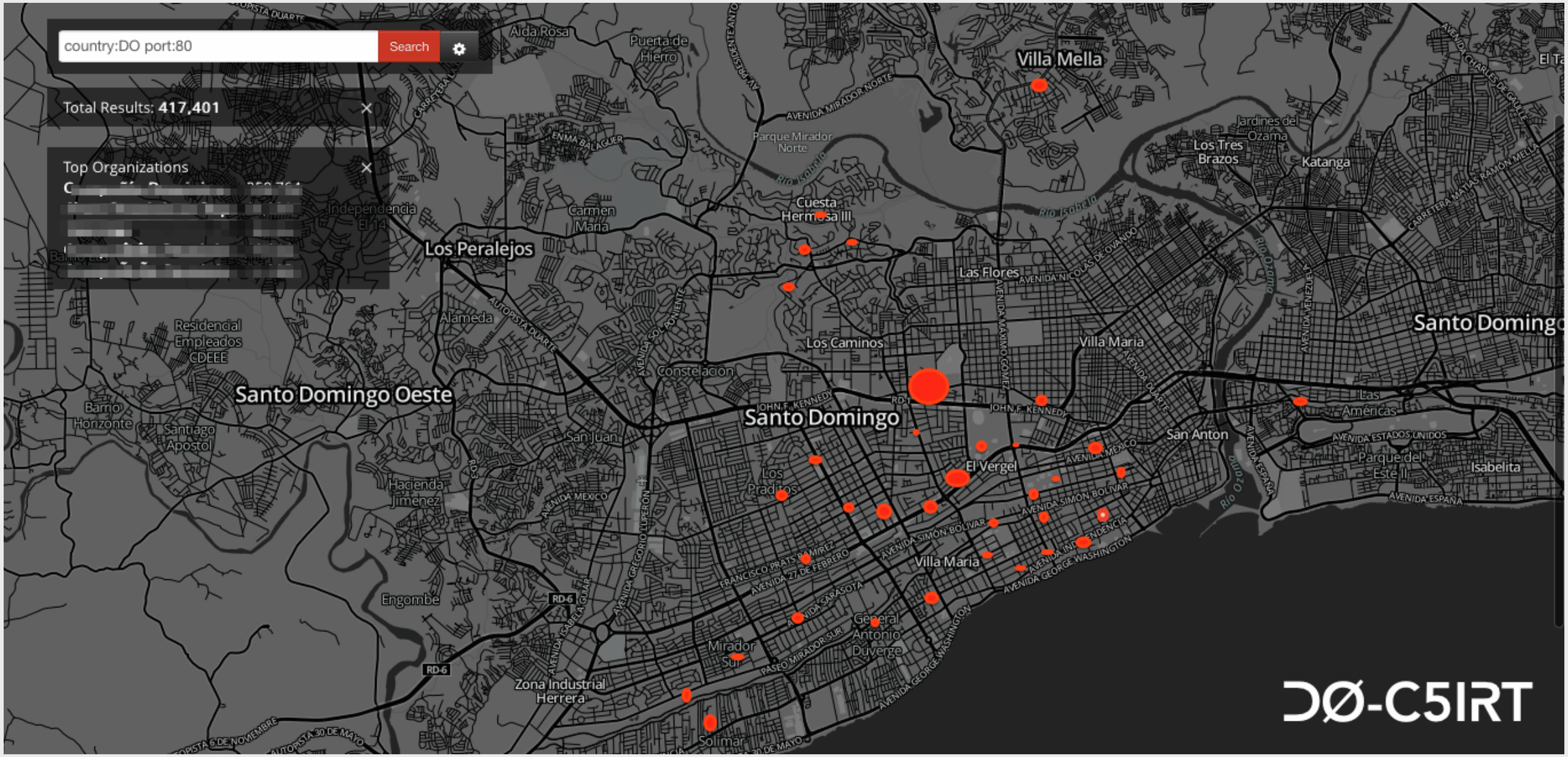
DØ-C5IRT

En proceso: interfaz de acceso



CNS
CONGRESO NACIONAL DE SEGURIDAD

En proceso: interfaz de acceso



CNS
CONGRESO NACIONAL DE SEGURIDAD

Hallazgos y colaboración con Telcos

- Las estadísticas que genera el Ciber-Observatorio proporcionan una visión única del uso del espacio de direcciones
- Uso de PGP (encriptamiento) para enviar alertas
- Las alertas deben generar una respuesta satisfactoria
- Posibilidad de colaborar en la solución del problema

DØ-C5IRT

Conclusiones y siguientes pasos

- La metodología de escaneo y de obtención de estadísticas ha probado ser facilmente obtenibles y reproducibles
- Debemos discutir y acordar mecanismos de colaboración para ayudar a mejorar la seguridad a nivel de infraestructura
- Creación de una interfaz con acceso público?
- Inspección de netflows de parte de los telcos?
- Creación de un CSIRT nacional?

CNS CONGRESO NACIONAL DE SEGURIDAD

DØ-C5IRT