CCN
Centro Criptológico Nacional

CCN-CERT
centro criptológico nacional

XVIII JORNADAS SOBRE TECNOLOGÍA: CIBERSEGURIDAD Y LAS ACTIVIDADES FINTECH.

INSTITUTO IBEROAMERICANO DE MERCADOS DE VALORES

SIN CLASIFICAR

CCN
Centro Criptológico Nacional

CCN-CERT
centro criptológico nacional

"CIBERAMENAZAS"

¿ QUIEN NOS ESTÁ ATACANDO?

SIN CLASIFICAR

El cambio es exponencial

Sociedad agraria

4000 a.C. ~ 1763

Consumo medio de proteínas per cápita

Sociedad industrial

1764 ~1970

Consumo medio de electricidad per cápita

Sociedad de Internet

1971 ~ 2014

Penetración de internet

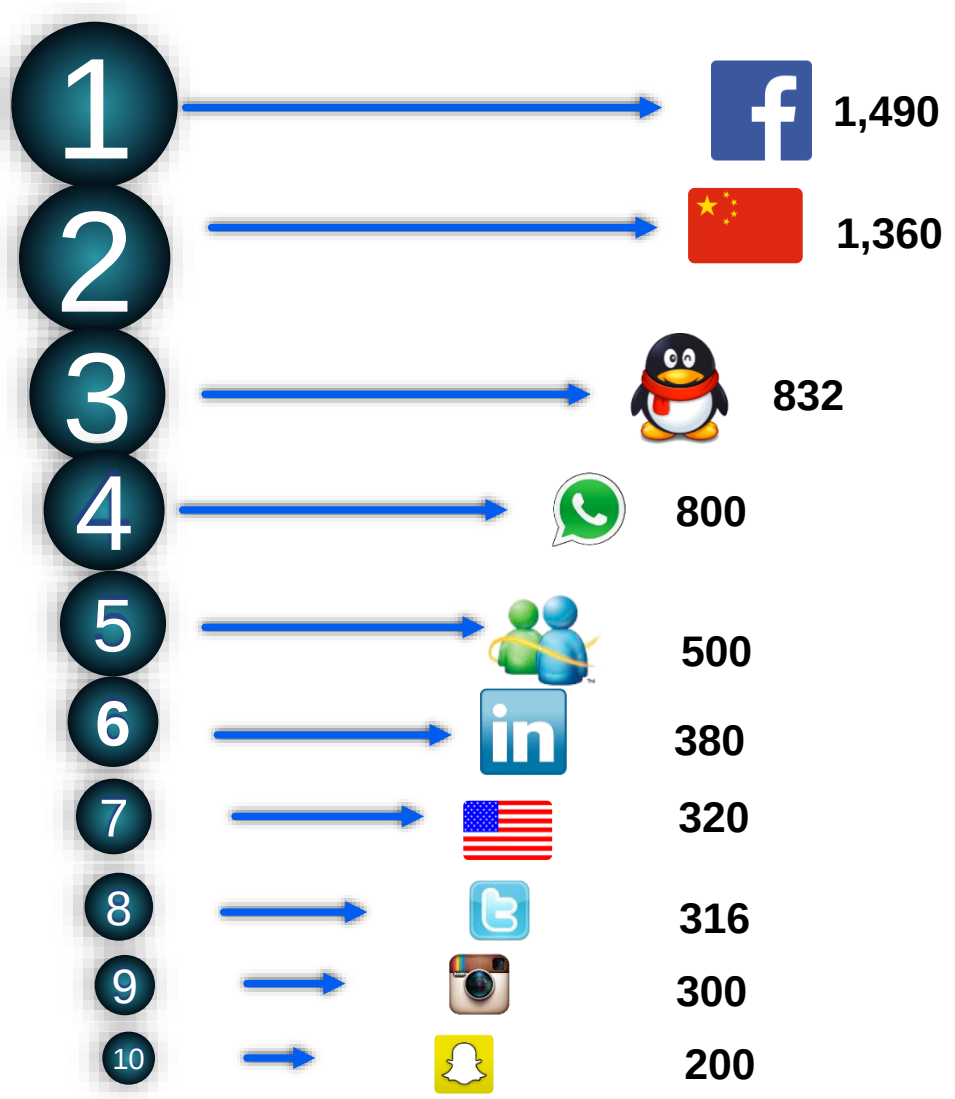
Sociedad de los datos

Después de 2015

Consumo medio de información per cápita

OCT 2015

Las **REDES SOCIALES** tienen un **IMPACTO** instantáneo y masivo



La disrupción en servicios es cada vez más rápida

Tiempo necesario para alcanzar 100 millones de usuarios

El ordenador en tu MANO es más POTENTE que el que cargaban estos 13 hombres en 1957

1991

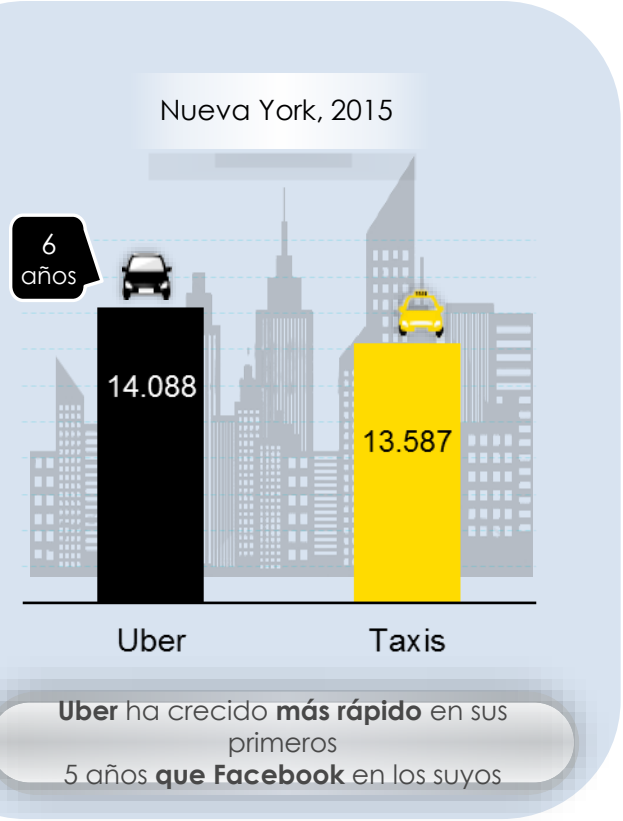
Ser disruptivos o no ser

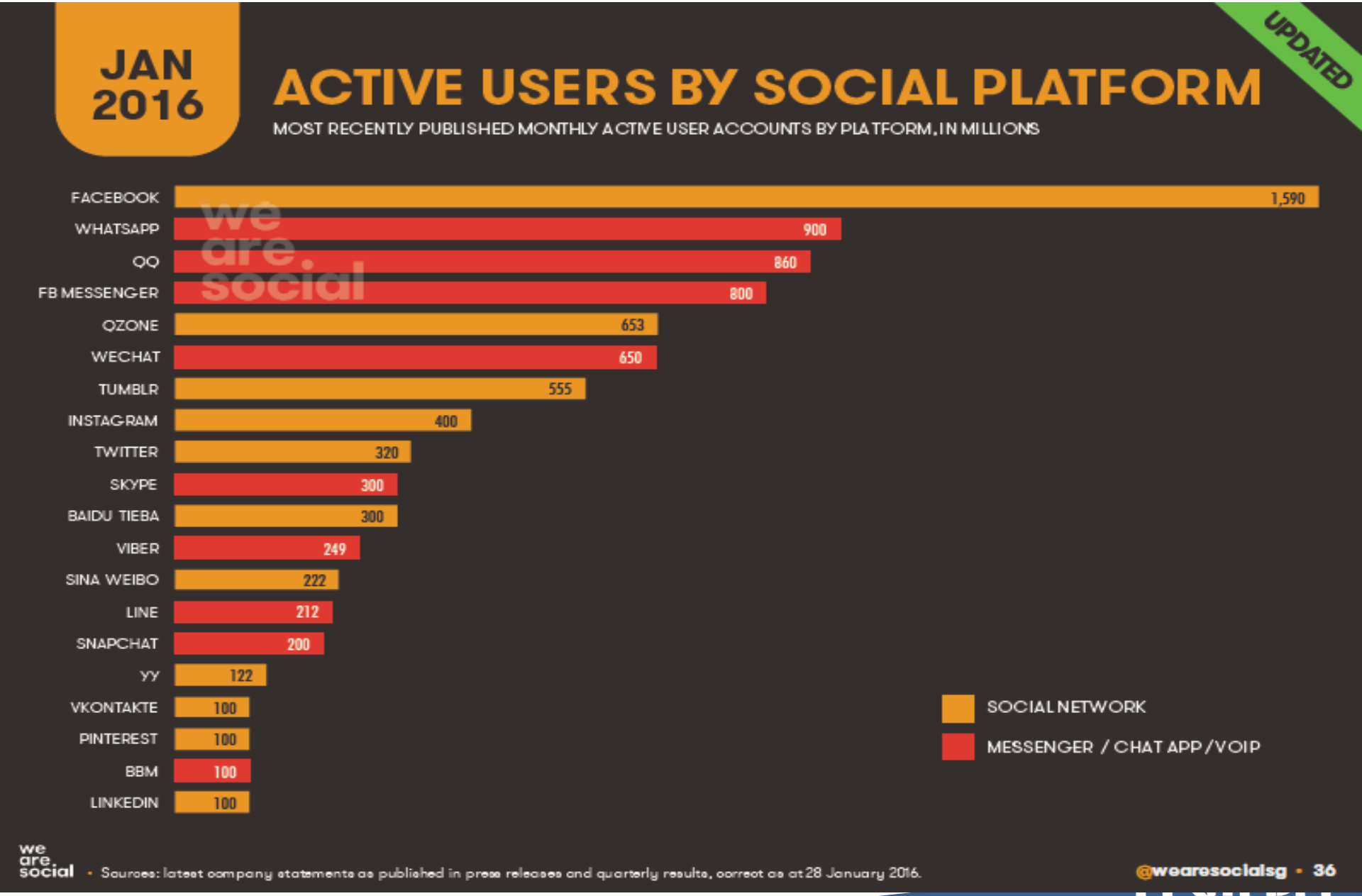
UBER — La mayor compañía de taxis del mundo, no tiene ningún coche

facebook — El mayor dueño de contenidos del mundo, no los genera

Alibaba.com — El minorista más valorado, no tiene inventarios

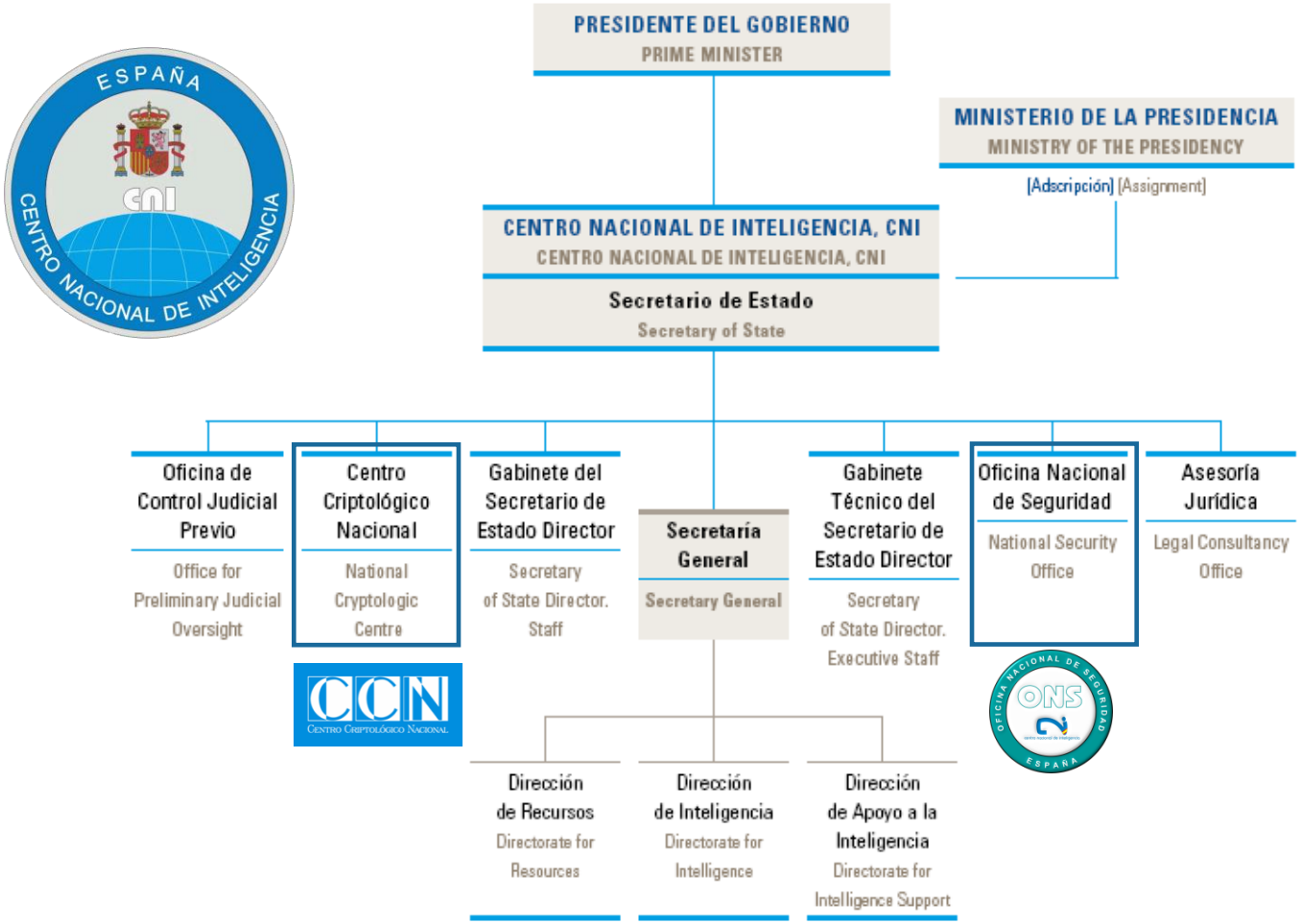
airbnb — El mayor proveedor de alojamientos, no posee ninguna propiedad



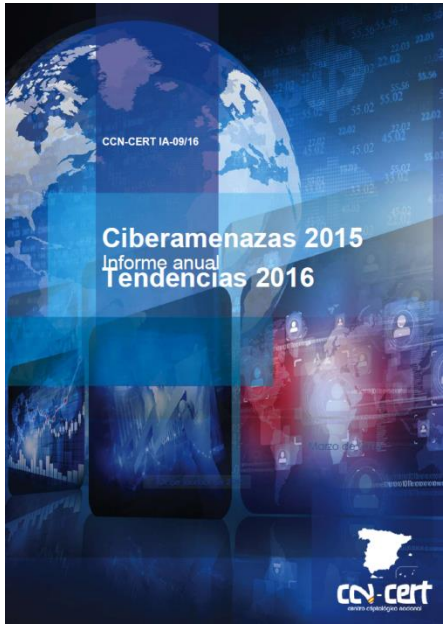

JAN 2016
UPDATED
ACTIVE USERS BY SOCIAL PLATFORM
MOST RECENTLY PUBLISHED MONTHLY ACTIVE USER ACCOUNTS BY PLATFORM, IN MILLIONS
FACEBOOK 1,590
WHATSAPP 900
QQ 860
FB MESSENGER 800
QZONE 653
WECHAT 650
TUMBLR 555
INSTAGRAM 400
TWITTER 320
SKYPE 300
BAIDU TIEBA 300
VIBER 249
SINA WEIBO 222
LINE 212
SNAPCHAT 200
YY 122
VKONTAKTE 100
PINTEREST 100
BBM 100
LINKEDIN 100
we are social
SOCIAL NETWORK
MESSENGER / CHAT APP / VOIP
we are social • Sources: latest company statements as published in press releases and quarterly results, correct as at 28 January 2016.
@wearesocialsg • 36

*"Usted le otorga a Facebook el derecho irrevocable, perpetuo, no exclusivo, transferible y **mundial** (con la autorización de acordar una licencia secundaria) de utilizar, copiar, publicar, difundir, almacenar, ejecutar, transmitir, escanear, modificar, editar, traducir, adaptar, redistribuir cualquier contenido depositado en el portal".*

La **"huella digital" de nuestra vida, consciente o desapercibida, tendrá un enorme valor económico en el futuro,** y se podrá vender e intercambiar por efectivo, descuentos, productos o servicios que cada vez están más personalizados y adaptados al cliente.



(*) La estructura básica del CNI está definida en los Reales Decretos 436/2002, de 10 de mayo y 612/2006, de 19 de mayo.
The basic structure of the CNI is established by Royal Decree 436/2002 of May 10th, and 612/2006 of May 19th.



INFORME ANUAL DE AMENAZAS 2015
TENDENCIAS 2016

Informes de Amenazas Ejecutivo

RECOMENDACIONES PROTECCIÓN AVANZADA

1. Aumentar la capacidad de Vigilancia.
2. Herramientas de Gestión Centralizada.
3. Política de seguridad.
4. Aplicar configuraciones de seguridad.
5. Empleo de productos confiables y certificados.
6. Concienciación de usuarios.
7. Compromiso de dirección (Aceptación Riesgo)
8. Legislación y Buenas Prácticas.
9. Intercambio de Información.
10. Trabajar como si se estuviera comprometido.

CCN-CERT IA-09/16 Ejecutivo (17 páginas)

Definiciones. Agentes de la amenaza

CIBERSEGURIDAD

La habilidad de proteger y defender las redes o sistemas de los **ciberataques.** Estos según su motivación pueden ser:

CIBERESPIONAJE

Ciberataques realizados para obtener secretos de estado, propiedad industrial, propiedad intelectual, información comercial sensible o datos de carácter personal.

CIBERDELITO / CIBERCRIMEN

Actividad que emplea las redes y sistemas como medio, objetivo o lugar del delito.

CIBERACTIVISMO o HACKTIVISMO

Activismo digital antisocial. Sus practicantes persiguen el control de redes o sistemas (sitios web) para promover su causa o defender su posicionamiento político o social.

CIBERTERRORISMO

Actividades dirigidas a causar pánico o catástrofes realizadas en las redes y sistemas o utilizando éstas como medio.

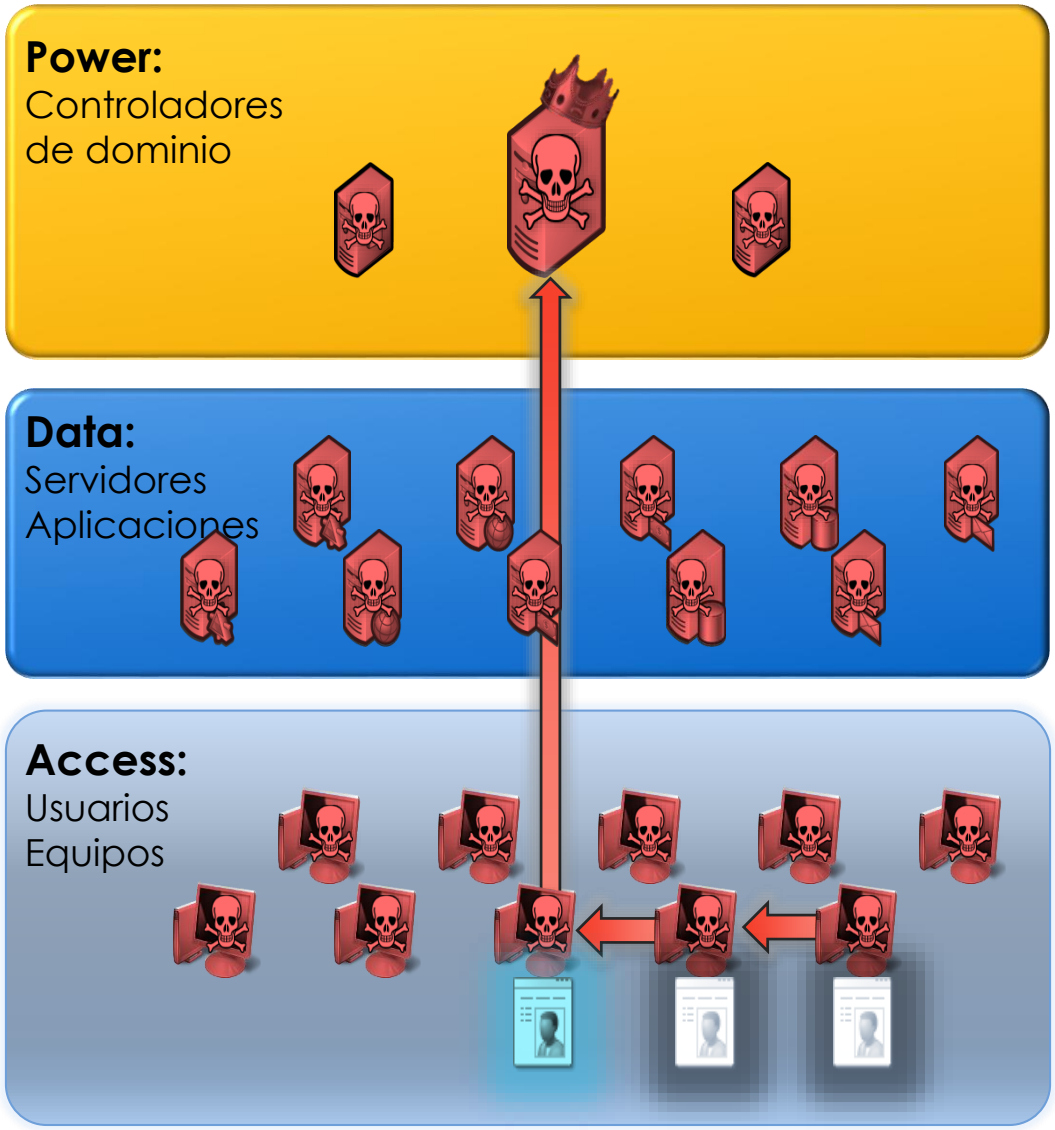
CIBERCONFLICTO / CIBERGUERRA

CIBERATAQUE

Uso de redes y comunicaciones para acceder a información y servicios sin autorización con el ánimo de robar, abusar o destruir.

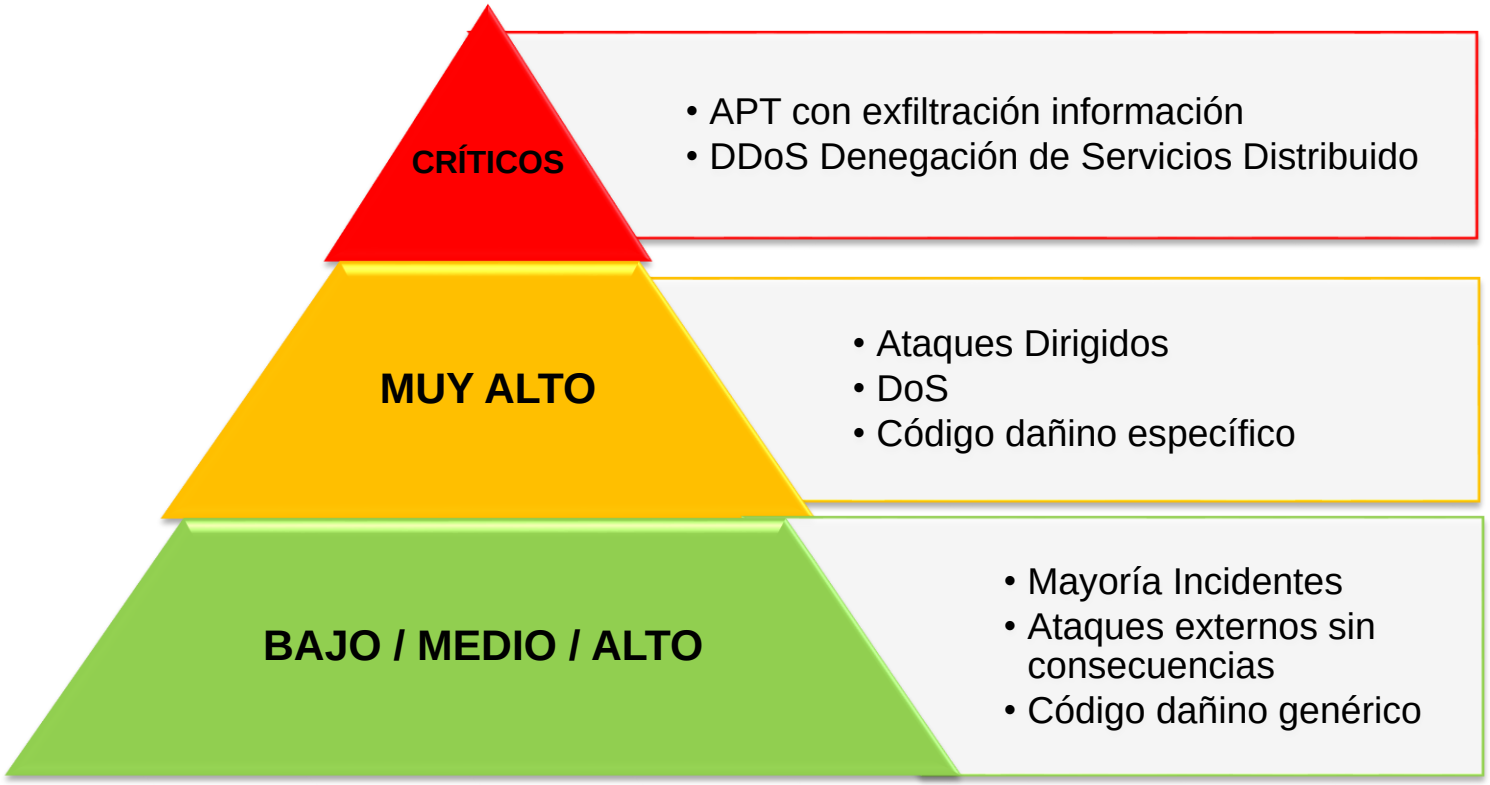
Año	Concepto Seguridad	Amenaza	Cambios Tecnológicos
1980-90	Compusec Netsec Transec	Naturales	Telecomunicaciones Sistemas Clasificados
1990-2004	Infosec Info. Assurance	Intencionadas	Redes corporativas Sist. Control industrial Infraestructuras Criticas
2005-2010	Ciberseguridad Ciberdefensa	Ciberespionaje Ciberterrorismo	Telefonía móvil Redes sociales Servicios en Cloud
2010-2015	Ciberresiliencia Seg. Transparente Defensa activa	Ciberguerra APT Hacktivismo Ciberactivismo	BYOD Shadow IT …//…

Tomando el control



1. Objetivos en masa / definidos
2. Usuarios con altos privilegios son el principal objetivo
3. Buscan credenciales "de lo que sea"
4. Búsqueda de credenciales cacheadas, cuentas de acceso a dominio, correo electrónico, etc..
5. Si logran acceder a toda la red, la empresa está perdida

Gestión de Ciberincidentes (CCN-STIC-817)



Ciberamenazas. Agentes. Conclusiones 2015

+
+

1. Ciberespionaje / Robo patrimonio tecnológico, propiedad intelectual
   - China, Rusia, Irán, otros…
     Servicios de Inteligencia / Fuerzas Armadas / Otras empresas

+

2. Ciberdelito / cibercrimen
   - HACKERS y crimen organizado

Usuarios internos

=

3. Ciberactivismo
   - ANONYMOUS y otros grupos

+

4. Uso de INTERNET por terroristas
   - Objetivo : Comunicaciones , obtención de información, propaganda, **radicalización** o financiación

-

5. Ciberterrorismo
   - Ataque a Infraestructuras críticas y otros servicios

¿CIBERYIHADISMO?

AGENTES DE LA AMENAZA TENDENCIAS

- **Ciberespionaje** continuará en **ascenso** al tiempo que lo hace en **sofisticación y peligrosidad**.
- **Ciberdelito** los **beneficios** obtenidos propiciará el **incremento de estas acciones**
- **Ciberterrorismo** gran peligrosidad **potencial**
- **Ciberyihadismo** no ha hecho sino empezar a mostrarse es de esperar **más ataques**
- Resto amenazas y actores internos no se prevén alteraciones sustanciales de comportamiento

HERRAMIENTAS UTILIZADAS POR LOS ATACANTES

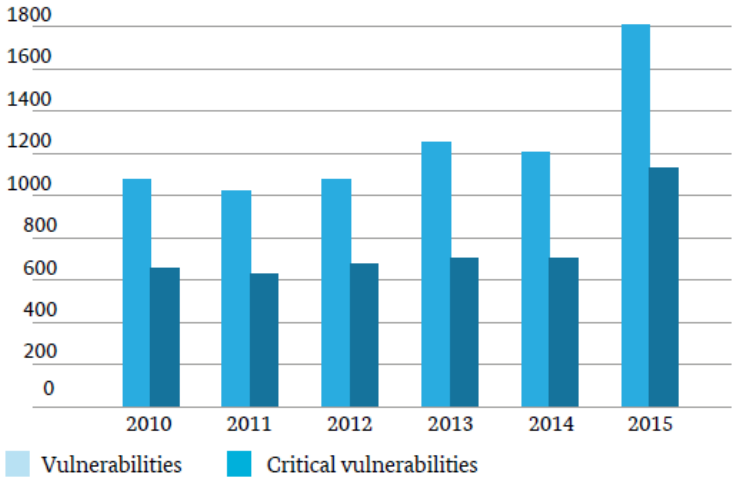
- En comparación con 2014 el **nivel de amenazas se ha agravado considerablemente**
- Los **ciberatacantes están invirtiendo** en el desarrollo de **nuevas herramientas (exploits-kits)** y en la **búsqueda de nuevas vulnerabilidades**

Vulnerabilidades. Precios

- **Criticidad ALTA = Ejecución de código**
- **Desmotivación de los investigadores de seguridad**
- **Vulnerabilidades DIA CERO**
  - **Mercado Negro**
  - **Mercado Gris**

2013

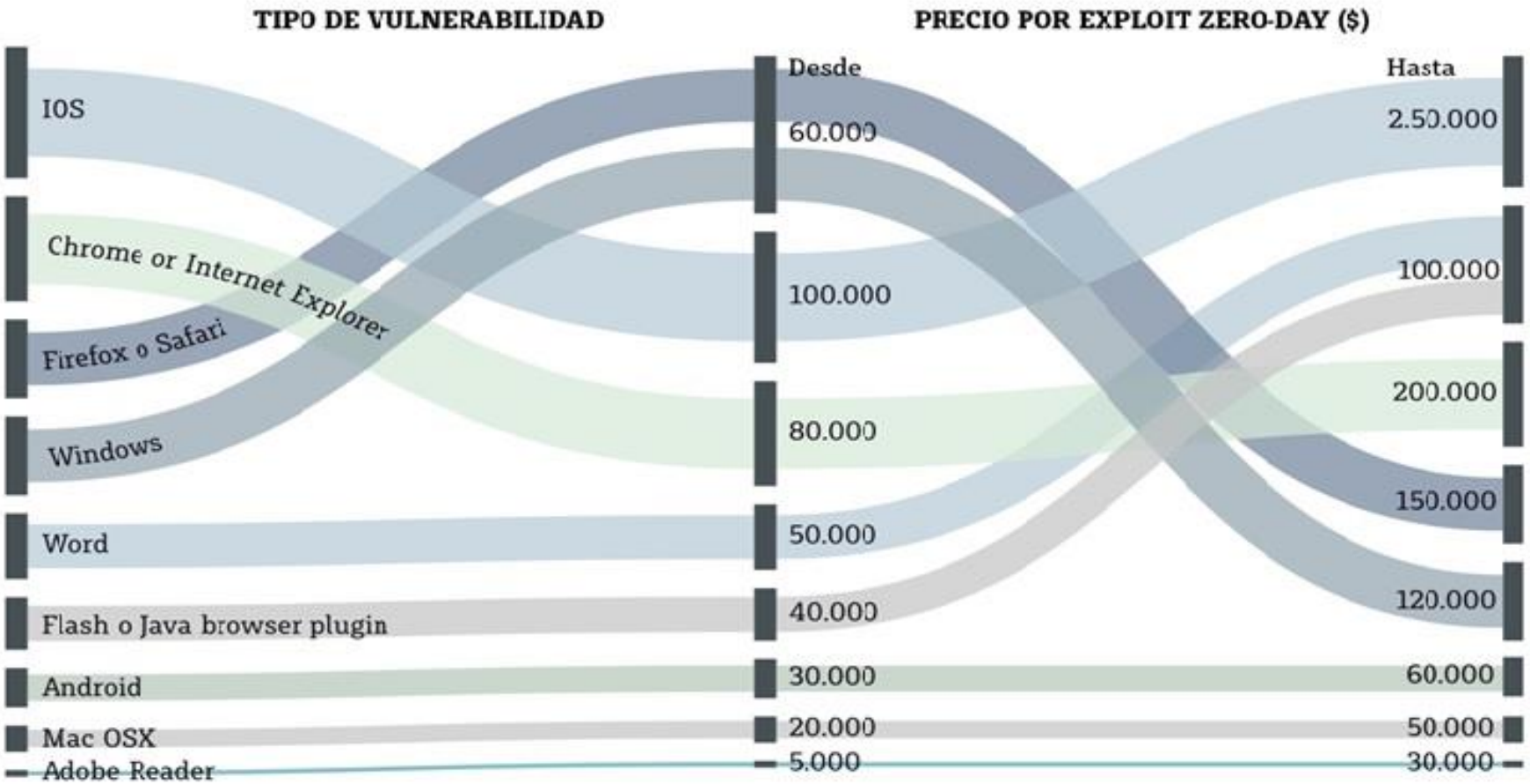
Producto	Rango de precios
Adode Reader	3.800 – 23.000€
Mac OS X	15.300 – 38.300 €
Android	23.000 – 46.000 €
Plug-ins Java para navegador	30.600 – 76.700 €
Plug-ins Flash para navegador	30.600 – 76.700 €
Microsoft Word	38.300 – 76.700 €
Windows	46.000 – 92.000 €
Firefox	46.000 – 122.600 €
Safari	46.000 – 225.000 €
Chrome	61.300 – 153.000 €
Internet Explorer	61.300 – 153.000 €
iOS	76.700 – 191.600 €



2015

Vulnerability Type	Price for Zero-Day Exploit
Adobe Reader	$5,000–$30,000
Mac OS X	$20,000–$50,000
Android	$30,000–$60,000
Flash or Java Browser Plug-ins	$40,000–$100,000
Word	$50,000–$100,000
Windows	$60,000–$120,000
Firefox or Safari	$60,000–$150,000
Chrome or Internet Explorer	$80,000–$200,000
IOS	$100,000–$250,000

HERRAMIENTAS UTILIZADAS exploits día cero



McAfee Labs Threats Report (Aug. 2015)

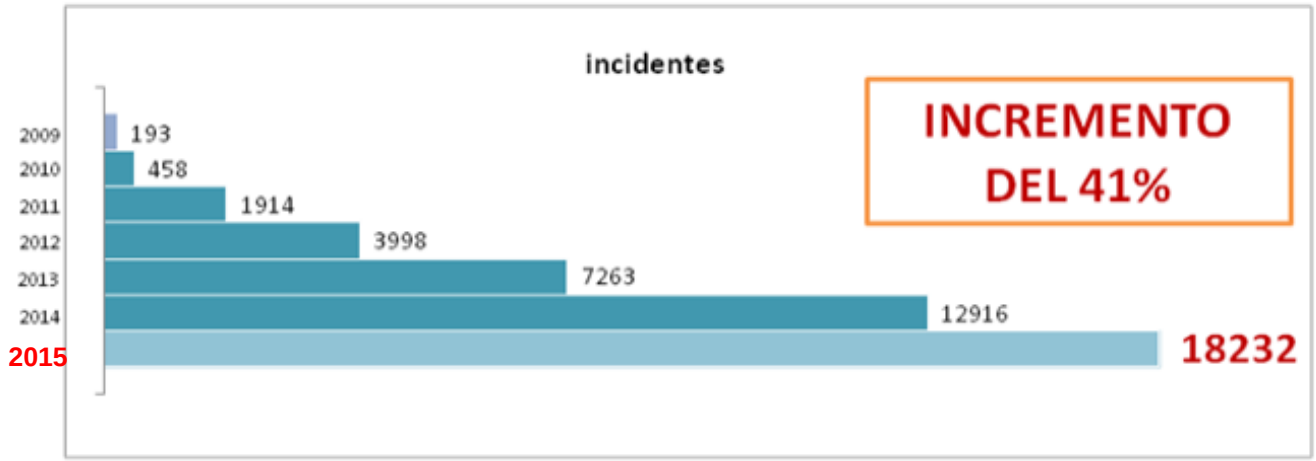
Código Dañino. Nivel complejidad

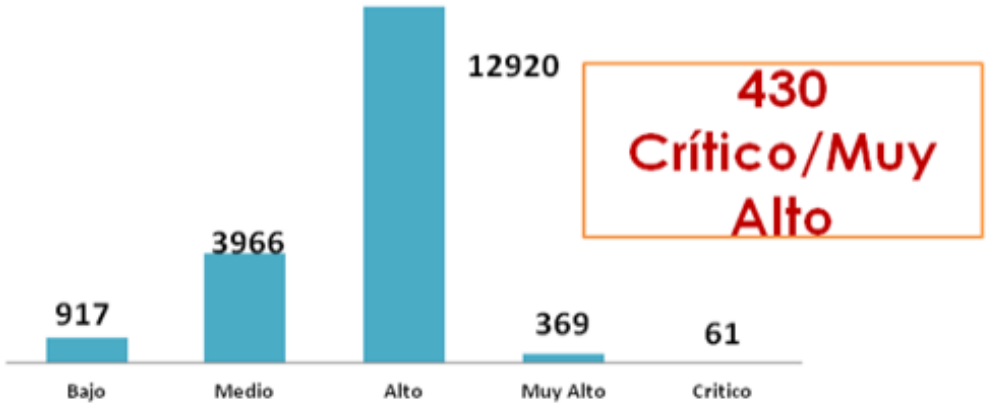
	Clasificación por capacidades	
Nivel 1	Profesionales que emplean desarrollos de código dañino y mecanismos de infección de terceros (usan exploits conocidos).	GRUPOS CHINOS
Nivel 2	Profesionales de gran experiencia que desarrollan herramientas propias a partir de vulnerabilidades conocidas.	10^3 euros
Nivel 3	Profesionales que se focalizan en el empleo de código dañino desconocido. Usan Rootkits en modo usuario y kernel. Usan herramientas de minería de datos. Atacan personal clave en las organizaciones para robar datos personales / corporativos para su venta a otros criminales.	OCTUBRE ROJO
Nivel 4	Grupos Criminales / esponsorizados por Estados organizados, con capacidades técnicas y financiados para descubrir nuevas vulnerabilidades y desarrollar exploits.	10^6 euros
Nivel 5	Grupos esponsorizados por Estados que crean vulnerabilidades mediante programas de influencia en productos y servicios comerciales durante su diseño, desarrollo o comercialización o con la habilidad de atacar la cadena de suministro para explotar redes / sistemas de interés.	SNAKE REGIN EQUATION GROUP
Nivel 6	Estados con la capacidad de ejecutar operaciones conjuntas (ciber, de inteligencia y militares) para conseguir sus objetivos políticos, económicos, militares…	10^9 euros

Fuente: Resilient Military Systems and the Advanced Cyber Threat. Enero 2013

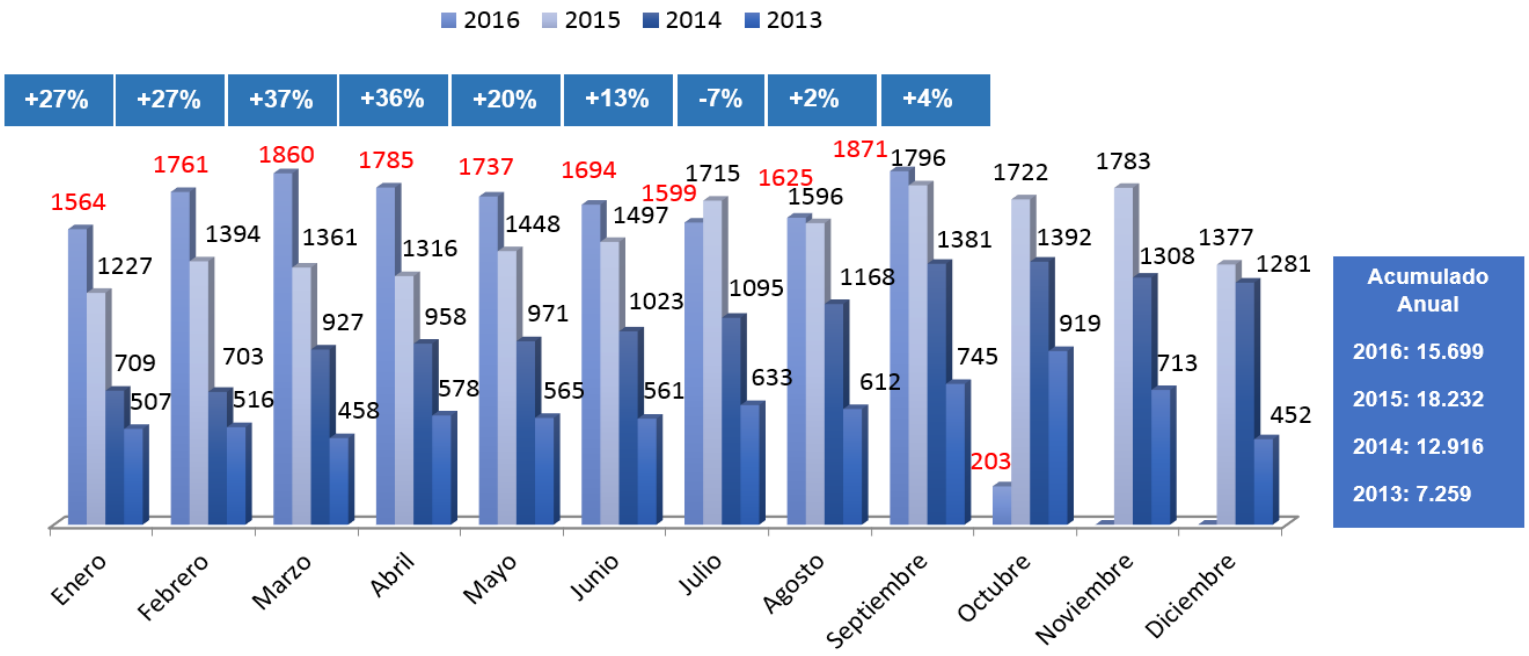
Incidentes detectados por los sistemas de alerta temprana del CCN-CERT

Total de incidentes gestionados por año

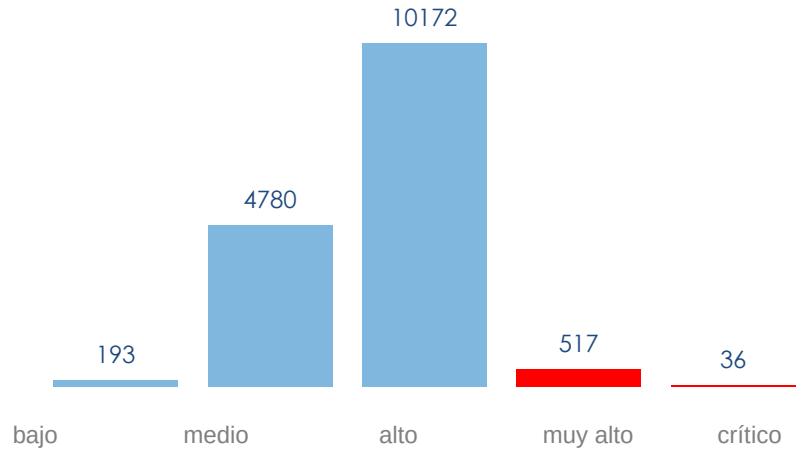




14.10.2016
16.156 INC.

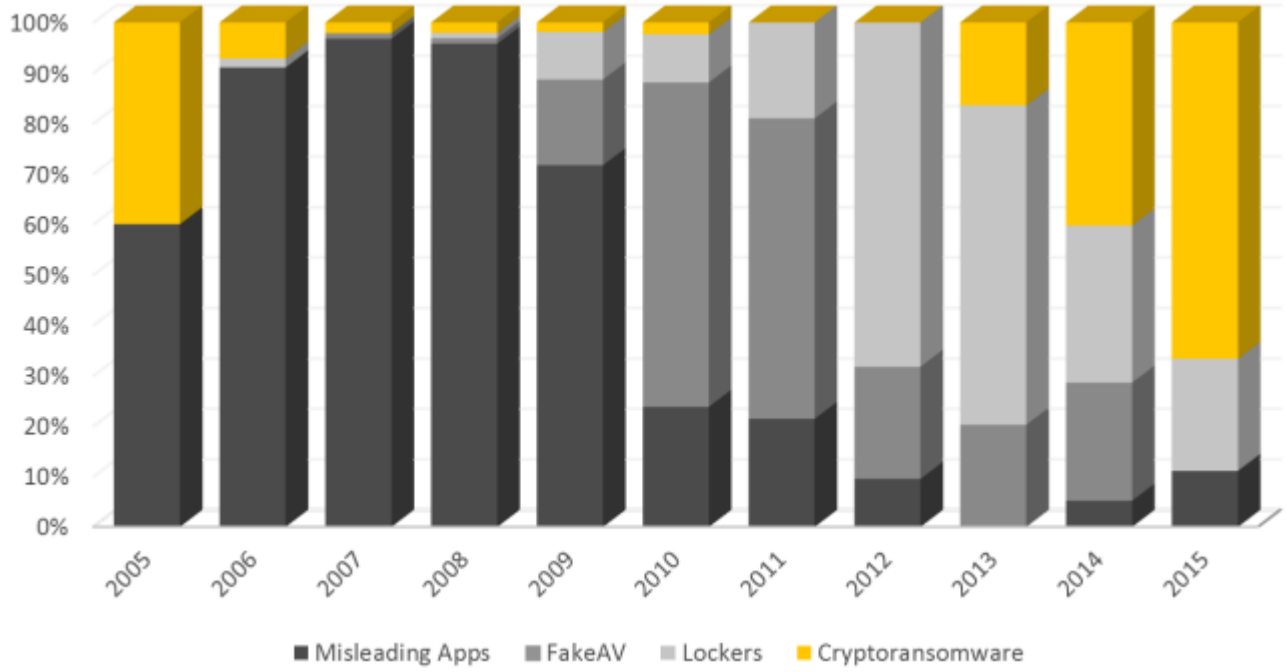


553 críticos
y muy altos



75 % SAT INTERNET
15 % SAT SARA
10 % OTROS

Ramsonware



Cryptoware
Locky
…//…

2015

Tipo	Nº incidentes
Cryptolocker	93
Torrentlocker	89
Teslacrypt	73
Cryptowall	109
Otros	73

Total: 427

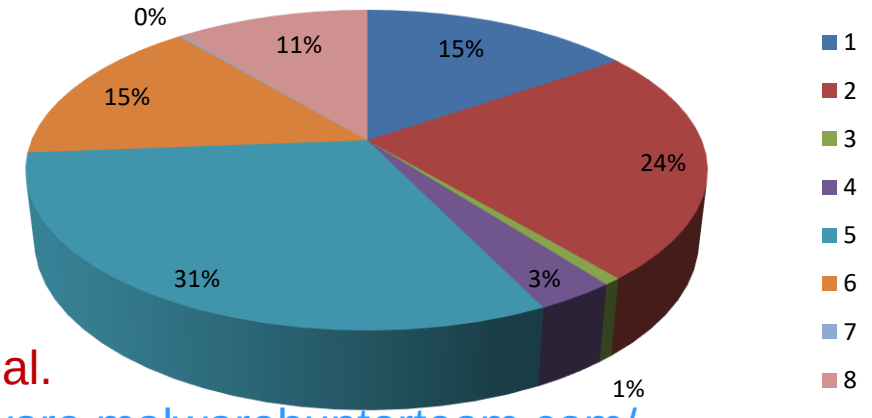
2016

Tipo	Nº incidentes
Locky	308
Teslacrypt	234
Torrentlocker	151
Cryptolocker	108
Cryptowall	153

Total: 954

RAMSONWARE

PAGO DE RESCATE TRAS EL SECUESTRO DEL SISTEMA INFORMATICO.

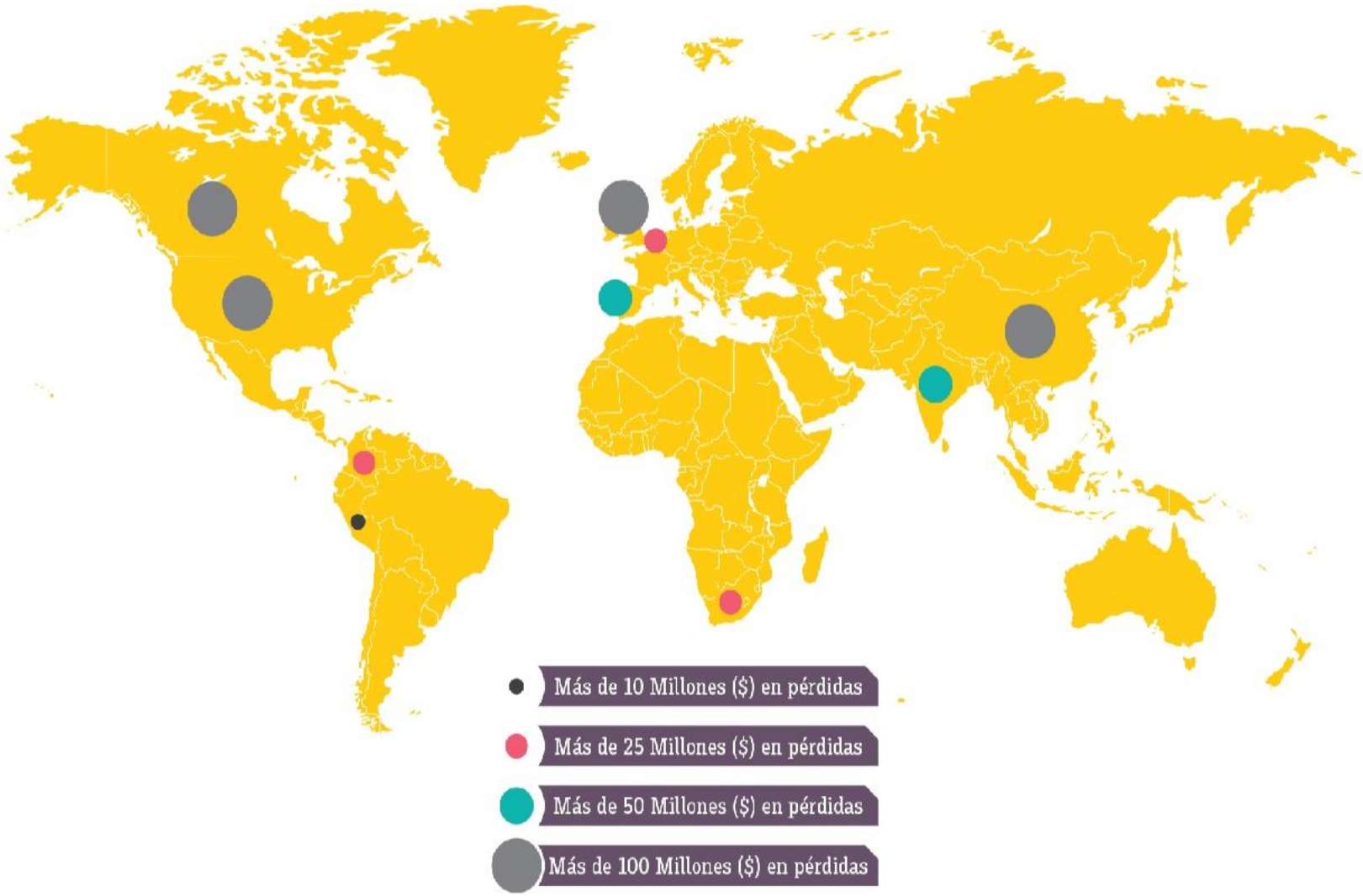


Ransomware is helping make the cyber threat real.

Familia/Versión Ransomware: https://id-ransomware.malwarehunterteam.com/

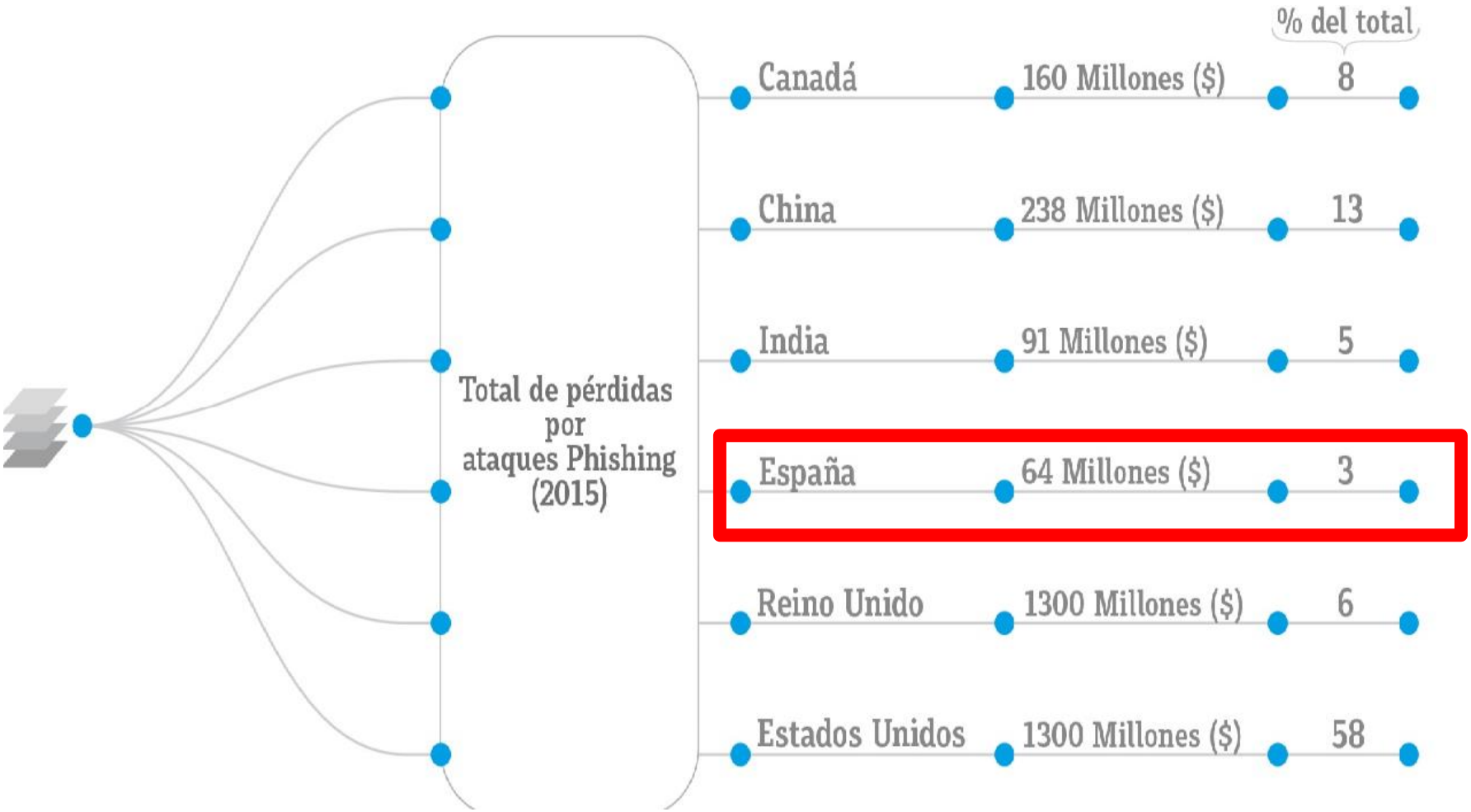
Herramientas descifrado: https://www.nomoreransom.org/decryption-tools.html

HERRAMIENTAS UTILIZADAS phishing paises con mayores perdidas



EMC-RSA http://spain.emc/microsites/rsa/phishing/index.htm

HERRAMIENTAS UTILIZADAS phishing paises con mayores perdidas



EMC-RSA http://spain.emc/microsites/rsa/phishing/index.htm

AGENTES DE LA AMENAZA

	ORIGEN DE LA AMENAZA	MOTIVACIÓN	NIVEL DE CONOCIMIENTO
1	Estados	Mejora de su posición geopolítica o estratégica. Ciberterrorismo como falsa bandera Contraterrorismo o protección de la seguridad nacional.	ALTO
2	Ciberdelincuentes	Beneficio económico (directo o indirecto)	ALTO > MEDIO
3	Hacktivistas	Acercarse a sus objetivos ideológicos.	MEDIO
4	Grupos Yihadistas	Lograr la penetración de su ideología.	BAJO>MEDIO
5	Grupos terroristas	Lograr cambios en la sociedad, mediante el uso del terror, o influir en la toma de decisiones políticas. Objetivos de alto impacto.	MEDIO > BAJO
6	Cibervándalos	Picardía. Búsqueda de desafíos.	BAJO
7	Actores internos	Venganza o beneficios económicos o ideológicos (en ocasiones, dirigida desde el exterior).	ALTO > BAJO
8	Ciberinvestigadores	Revelación de debilidades (y su propio perfil)	MEDIO
9	Organizaciones privadas	Obtener o vender información valiosa.	ALTO > BAJO

OBJETIVOS

SECTOR PÚBLICO	SECTOR PRIVADO	CIUDADANOS
Ciberespionaje político	Ciberespionaje económico	Ciberespionaje instrumental
Cibercapacidades ofensivas	Cibercapacidades ofensivas	
Sustracción, publicación o venta de información	Sustracción, publicación o venta de información	Sustracción, publicación o venta de información
Manipulación de información	Manipulación de información	Manipulación de información
Interrupción de sistemas	Interrupción de sistemas	Interrupción de sistemas
Toma de control de sistemas	Toma de control de sistemas	Toma de control de sistemas
Sustracción y publicación de la información sustraída	Sustracción y publicación de la información sustraída	
Desfiguraciones	Desfiguraciones	
Interrupción de sistemas	Interrupción de sistemas	
Toma de control de sistemas	Toma de control de sistemas	
Interrupción de Sistemas / Toma de control	Interrupción de Sistemas / Toma de control	Propaganda y reclutamiento
Desfiguraciones	Desfiguraciones	
Interrupción de Sistemas / Toma de control	Interrupción de Sistemas / Toma de control	
Sustracción de información	Sustracción de información	Sustracción de información
Interrupción de sistemas	Interrupción de sistemas	
Sustracción, publicación o venta de información	Sustracción, publicación o venta de información	
Interrupción de sistemas	Interrupción de sistemas	
Recepción y publicación de información	Recepción y publicación de información	
	Sustracción de información (espionaje industrial)	Uso/abuso o reventa de información de clientes o público en general

BAJO

- No se han observado nuevas amenazas o tendencias, o
- Se dispone de medidas suficientes para neutralizar la amenaza, o
- No ha habido incidentes especialmente significativos en el periodo analizado.

MEDIO

- Se han observado nuevas amenazas o tendencias, o
- Se dispone de medidas (parciales) para neutralizar la amenaza, o
- Los incidentes detectados no han sido especialmente significativos.

ALTO

- Las amenazas o su tendencia se ha incrementado significativamente.
- Las medidas adoptadas tienen un efecto muy limitado, por lo que la amenaza permanece.
- Los incidentes detectados han sido especialmente significativos.

¿Qué hemos aprendido todos este tiempo sobre las **APT**?


Saben más…

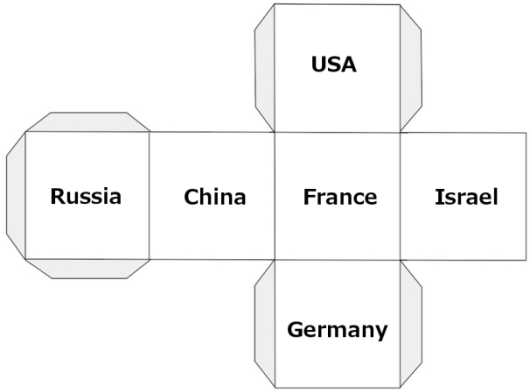

Son más…


Son muy insistentes…


Están especializados…

Características Generales

- Estados/Industrias/Empresas.
- Ataques Dirigidos.
- Dificultad de atribución.
- **Contra los Sectores Privado y Público**.
- Ventajas políticas, económicas, sociales…



Rusia

- Utilización de **herramientas diseñadas específicamente** contra el objetivo
- **Conocimiento técnico muy elevado**
- Evitar **atribución**
- Esfuerzo **HUMINT**
- **AA.PP.**

China

- Interés en Propiedad intelectual EMPRESAS
  Aeroespacial/Energía/Defensa/Gubernamental/Farmacéutico/Químico/Financiero/TIC/Transporte
- **Uso de herramientas comerciales**
- Diferentes grupos con nivel técnico diverso

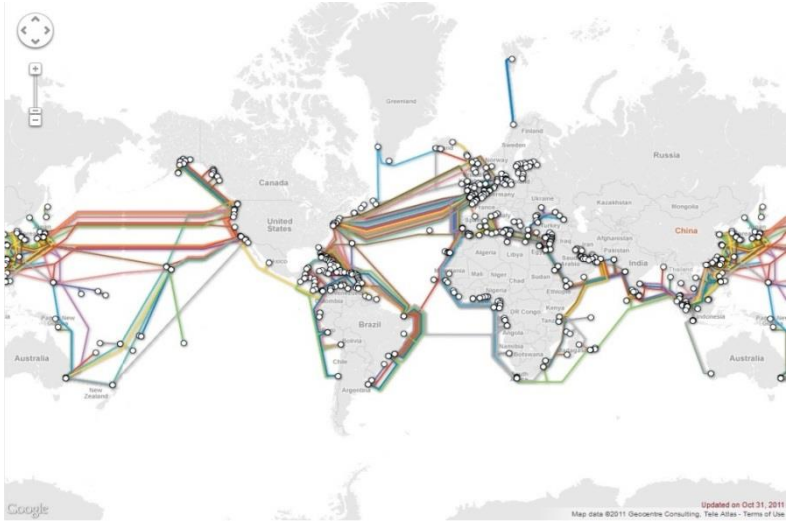
Otros países?

Otros actores con grandes capacidades

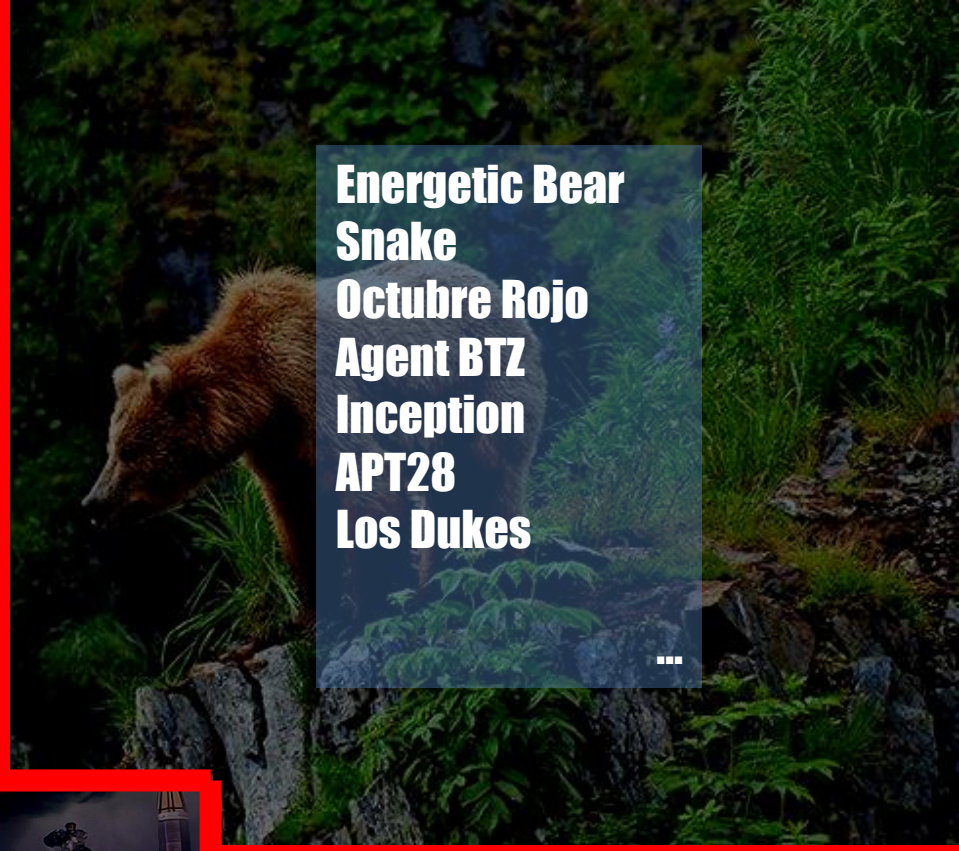
- Estados Unidos (NSA)
- Reino Unido (GCHQ)
- Canadá (CSC)
- Francia (DGSE)
- Australia (DSD)
- Alemania (BND)
- Países Bajos

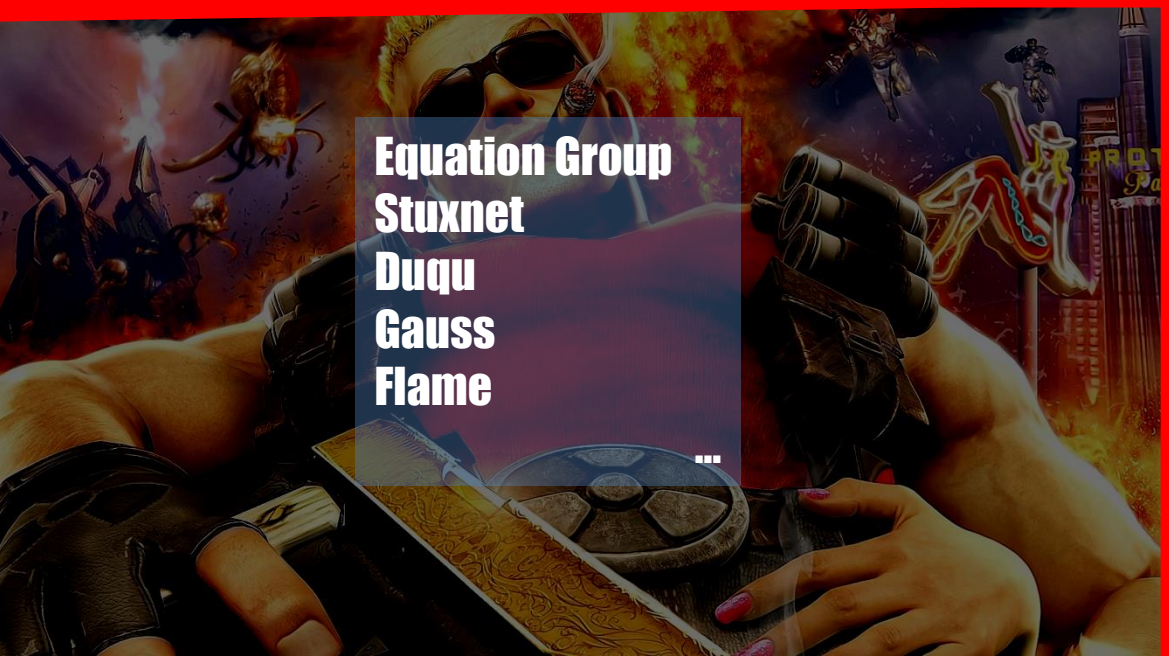
Otros actores adquiriendo grandes capacidades

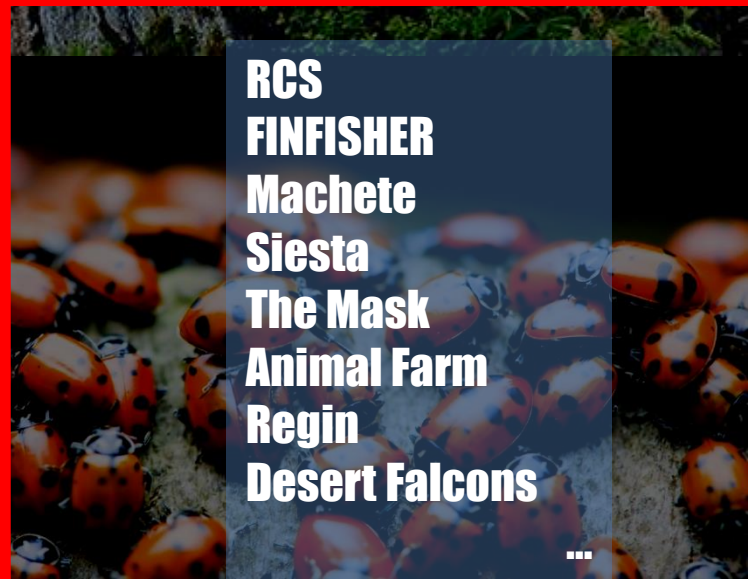
- Marruecos
- Irán
- Corea del Norte
- Pakistán
- India
- Colombia
- Venezuela



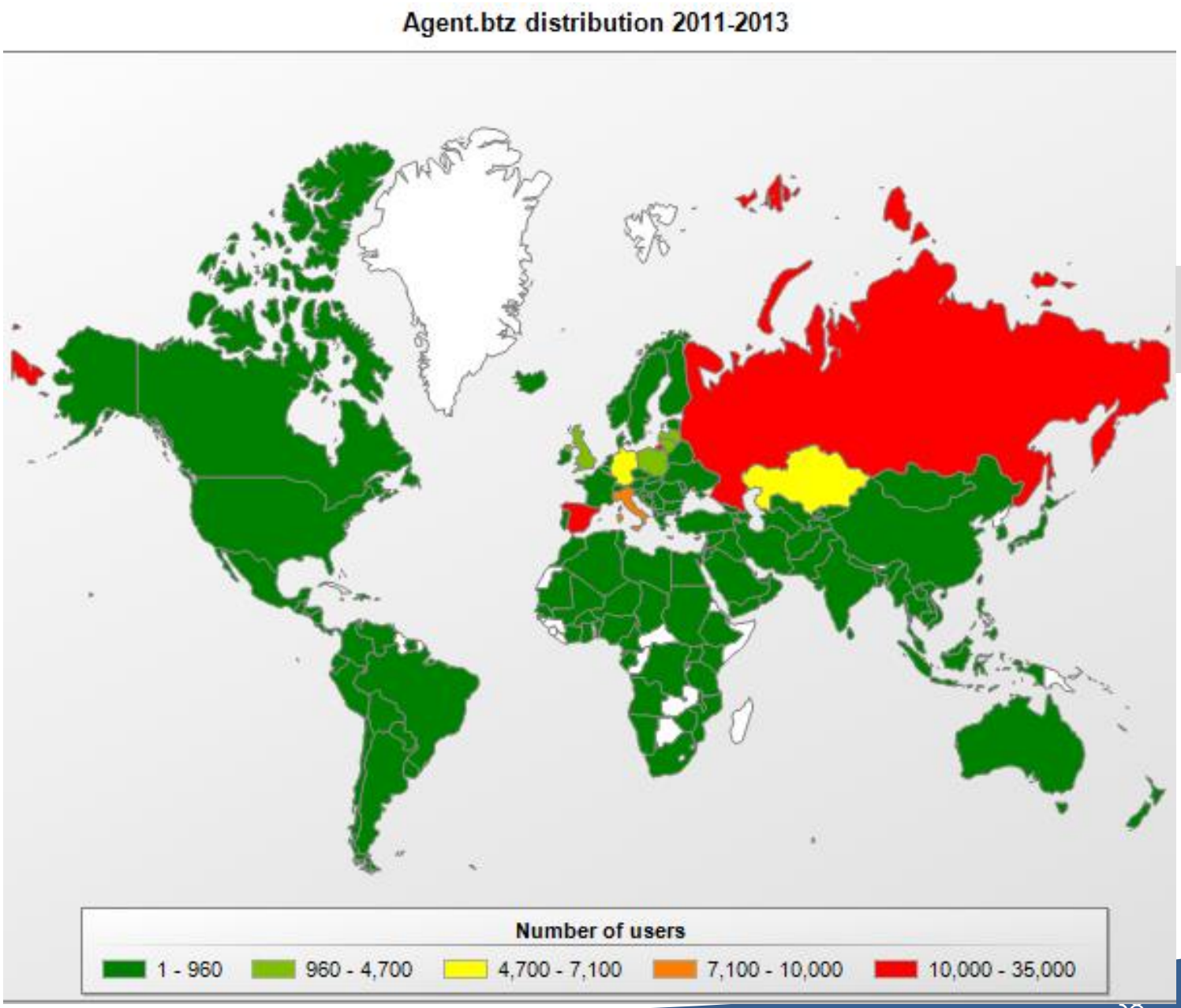

Goblin Panda
Vixen Panda
Deep Panda
Emissary Panda
Pirate Panda
Numbered Panda
Lotus Panda
Pitty Panda
Gothic Panda
Predator Panda
Dynamite Panda
Temper Panda
Pale Panda
Violin Panda
Hurricane Panda
Sabre Panda
Samurai Panda
Dagger Panda
Aurora Panda
Maverick Panda
Keyhole Panda
Stone Panda
Spicy Panda
Comment Panda ...


Energetic Bear
Snake
Octubre Rojo
Agent BTZ
Inception
APT28
Los Dukes
...


Equation Group
Stuxnet
Duqu
Gauss
Flame
...


RCS
FINFISHER
Machete
Siesta
The Mask
Animal Farm
Regin
Desert Falcons
...

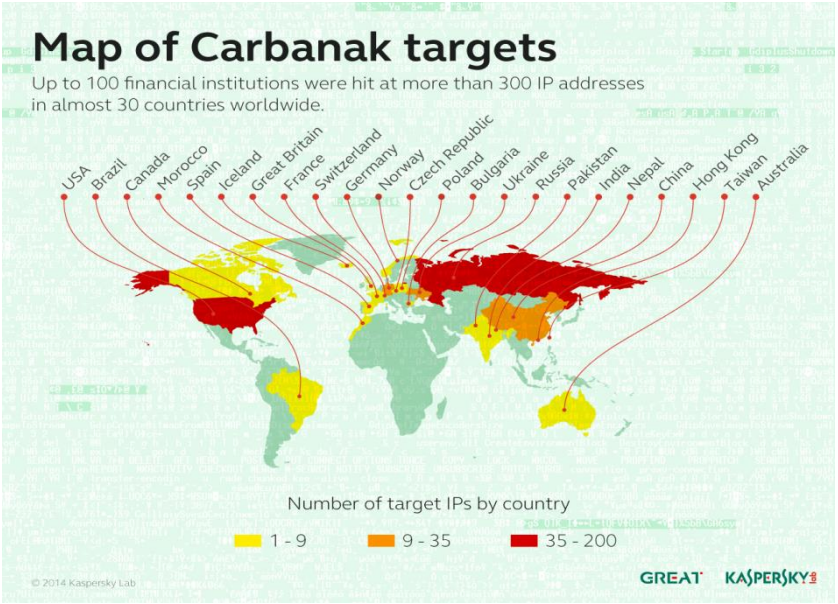


AGENT BTZ

Más de 900 IP,s en España

CARBANAK

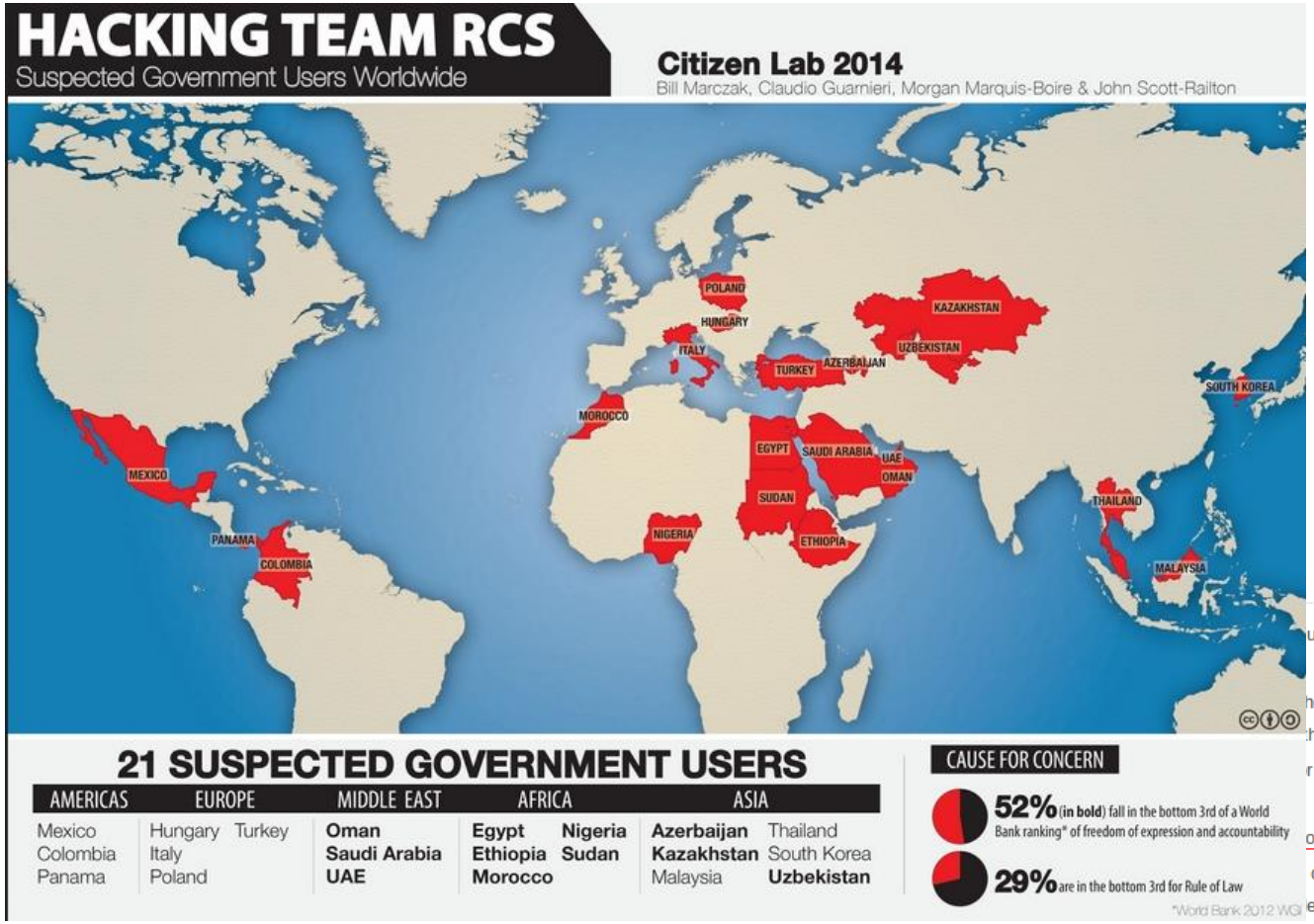


- Carbanak ejemplo claro del cibercrimen utilizando técnicas APT.
- "Spear phishing" simulando comunicaciones bancarias.
- Movimientos laterales: Ammyy RAT y comprometimiento de servidores SSH.
- Grabaciones vídeo de empleados (particualermente admisnitradores).
- Utilización de red SWIFT, actualización balances y mecanismos de desembolso (ATM).
- Fondos transferidos a cuentas bancarias de USA y China.

Remote Control System (RCS)

RCS

Versiones Windows, *Mac OS, Linux, Windows Mobile 5, Windows Mobile 6, iPhone, BlackBerry* y *Symbian*,



Funciones 2011:

- Monitorizar el navegador
- Ficheros abiertos / cerrados / eliminados
- Pulsaciones de teclado
- Documentos impresos
- Logs de chats
- Correos electrónicos
- Conversaciones de *Skype*
- Grabación de webcam.

understood the power of our software in law enforcement and

he surveillance technologies that we produce, and so we take a
hat abuse.

r government agencies. We do not sell products to individuals or

ountries blacklisted by the U.S., E.U., U.N., NATO or ASEAN.

determine whether or not there is objective evidence or credible
ed to the customer will be used to facilitate human rights violations.

We have established a panel of technical experts and legal advisors, unique in our industry, that reviews potential sales.

NSO GROUP PEGASUS

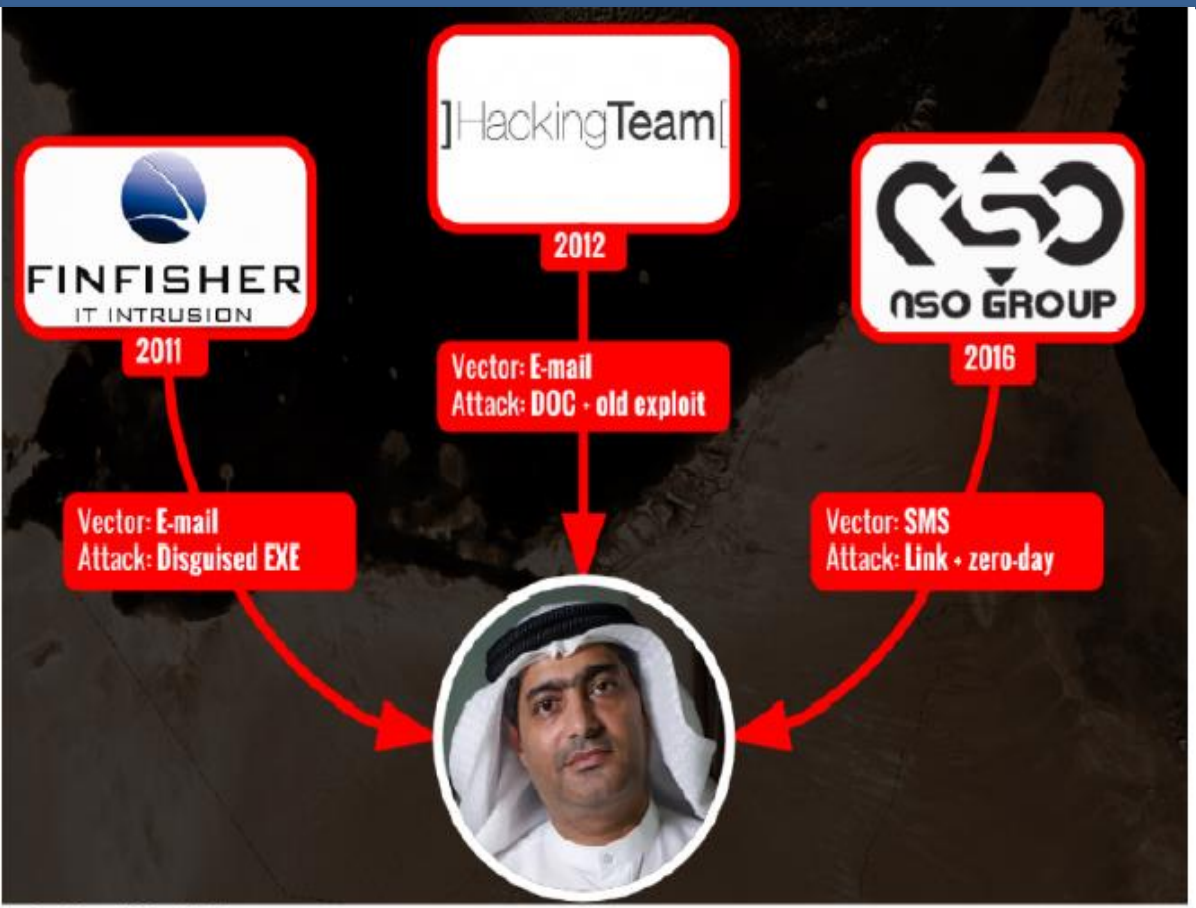


Figure 1: Ahmed Mansoor, the "Million Dollar Dissident."

Ejecución remota de código

Sectores que reciben más ataques en ESPAÑA

Disponibilidad

Energético

Industria Nuclea

Administración

Espacio

Financiero

Hídrico

Al ón

Transporte

Sanid ndustria Química

ones de Investigación

Tecnologías de la Información

Infraestructuras Críticas

Confidencialidad

Protección del Patrimonio

Energético

Ae al

Administración

Defensa

armacéutico

Minería

Financi

Marítimo

Qu

Ingeniería

aciones

Derechos Humanos

Sectores Más atacados

CNPIC

CENTRO NACIONAL PARA LA PROTECCIÓN DE LAS INFRAESTRUCTURAS CRÍTICAS

- **CASO 1:** EMPRESA ESTRATÉGICA (Junio 2013/ Enero / Octubre 2014)

  - Vector de infección: **spear phishing**
  - Malware utilizado: **Poison Ivy**, **malware propio**

- Canal de exfiltración de información: **Amazon C3**
  - Servidor de Mando y Control: **servidor web español hackeado**
  - Uso de **mimikatz** y **gsecdump** para el robo de credenciales

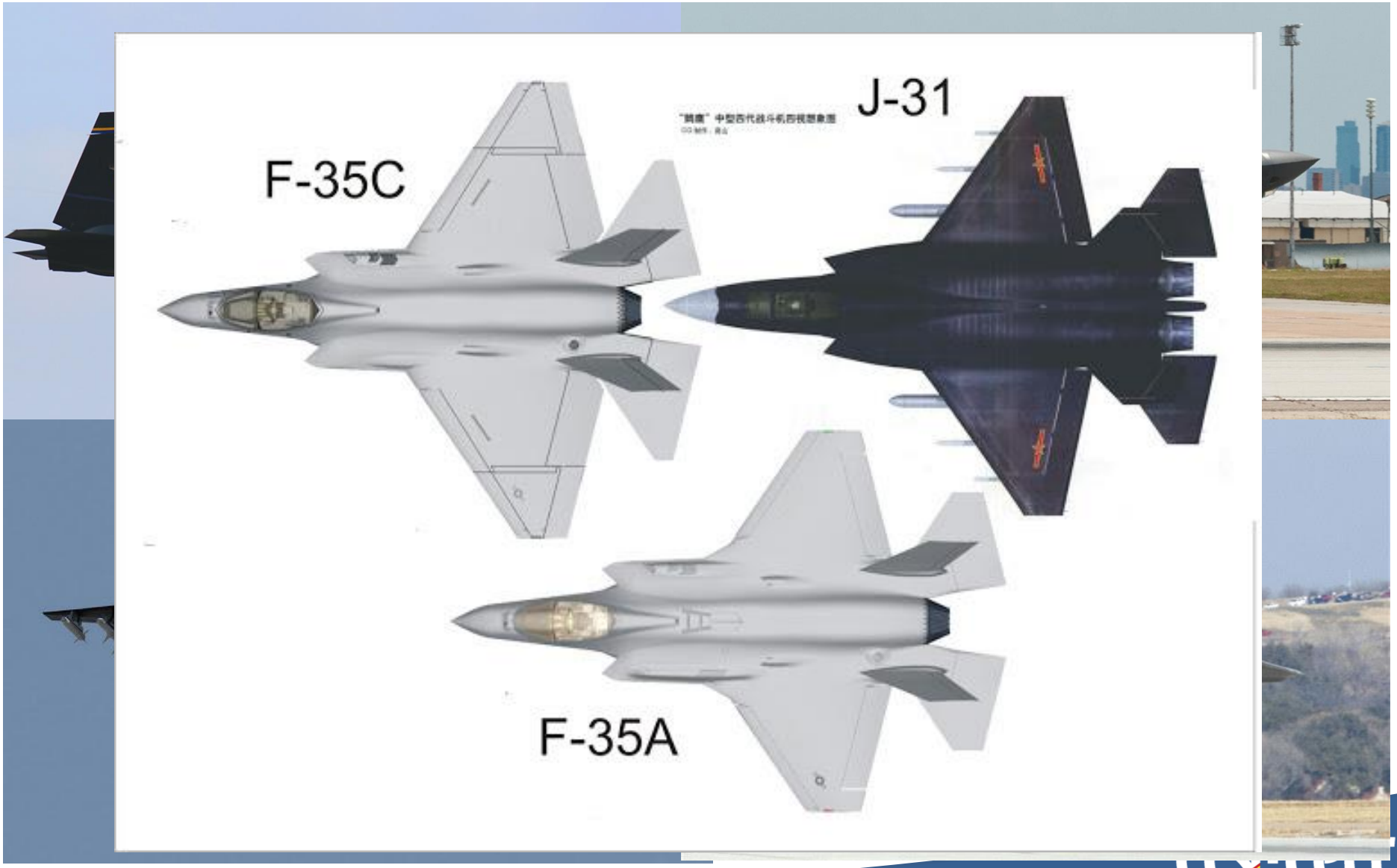
Servidor C2	Puerto usado	Geolocalización
av.ddns.us	443	China
usa.got-game.org	443	China
yeahyeahyeahs.3322.org	443	China
za.myftp.info	53	China

- **CASO 2:** ORGANISMO GUBERNAMENTAL (Abril 2013 / Nov 2014 / Ene 2015….)
  - Vector de ataque: **Spear Phishing**
  - Código dañino: **malware específico**

  - **Canal de exfiltración: HTTP POST / DNS Dinámicos / ¿HTTPS?**
  - **Canal exfiltración: CORREO ELECTRÓNICO**

  - Uso de **cifrado asimétrico** : PGP y GPG
  - Infraestructura: **Varios saltos**
  - Server C2: **Servidores web comprometidos (al menos 15)**
  - Otras herramientas: **mimikatz** y **gsecdump** para robo de credenciales

EJEMPLOS



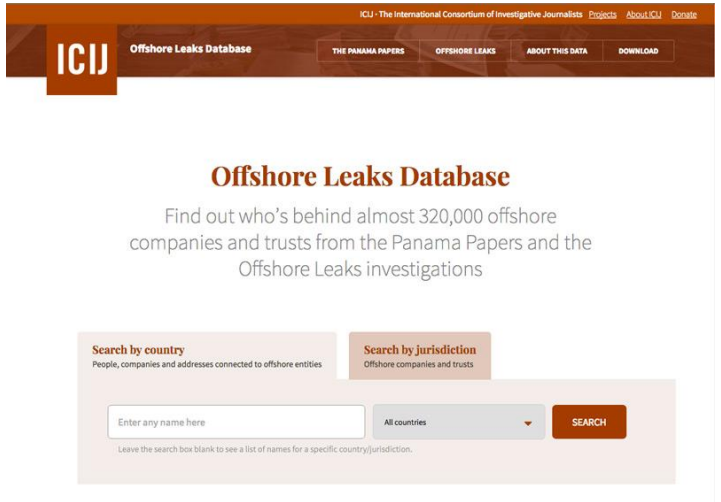
¿Me puede **pasar a mí**?

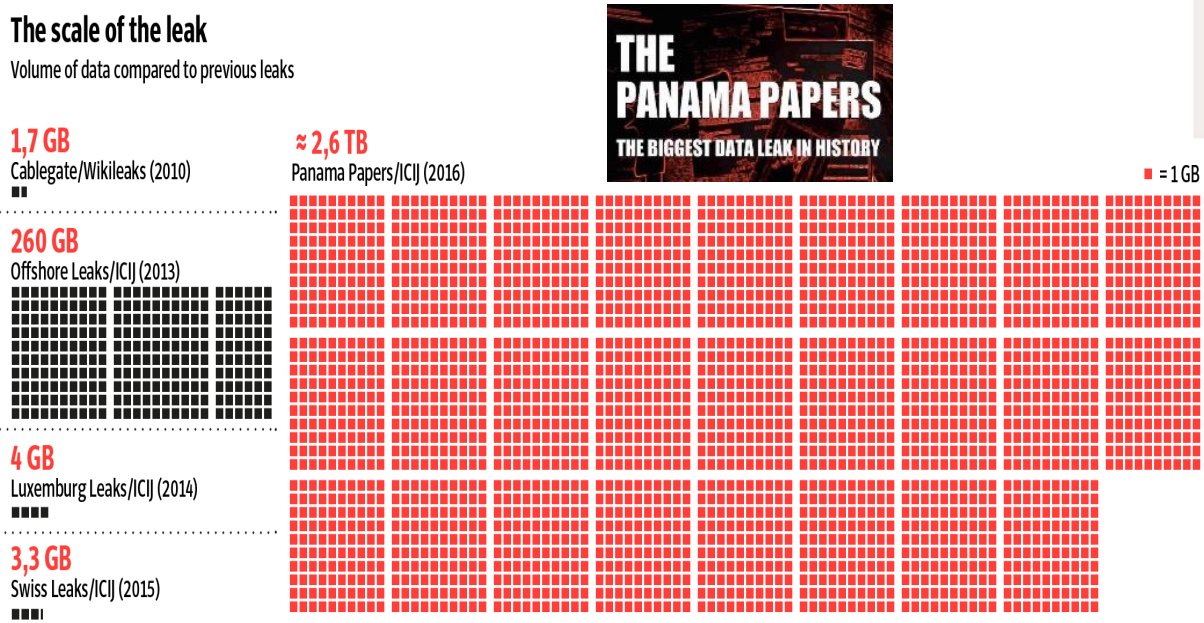
¿ Impacto en las organizaciones?

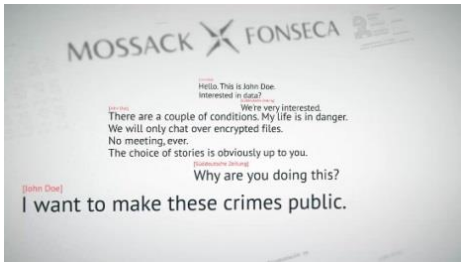
Debilidades de Nuestros Sistemas de Protección

- ✓ **Falta de concienciación** y **desconocimiento del riesgo**
- ✓ **Somos objetivos blandos**: Sistemas con Vulnerabilidades, escasas configuraciones de seguridad y Seguridad Reactiva.
- ✓ **Poco personal de seguridad y escasa vigilancia**
- ✓ **Ausencia herramientas faciliten investigación**
- ✓ **Mayor superficie de exposición (Redes sociales, Telefonía móvil (BYOD) y Servicios en nube)**
- ✓ **Afectados NO comparten información.**
- ✓ **NO comunican incidentes**

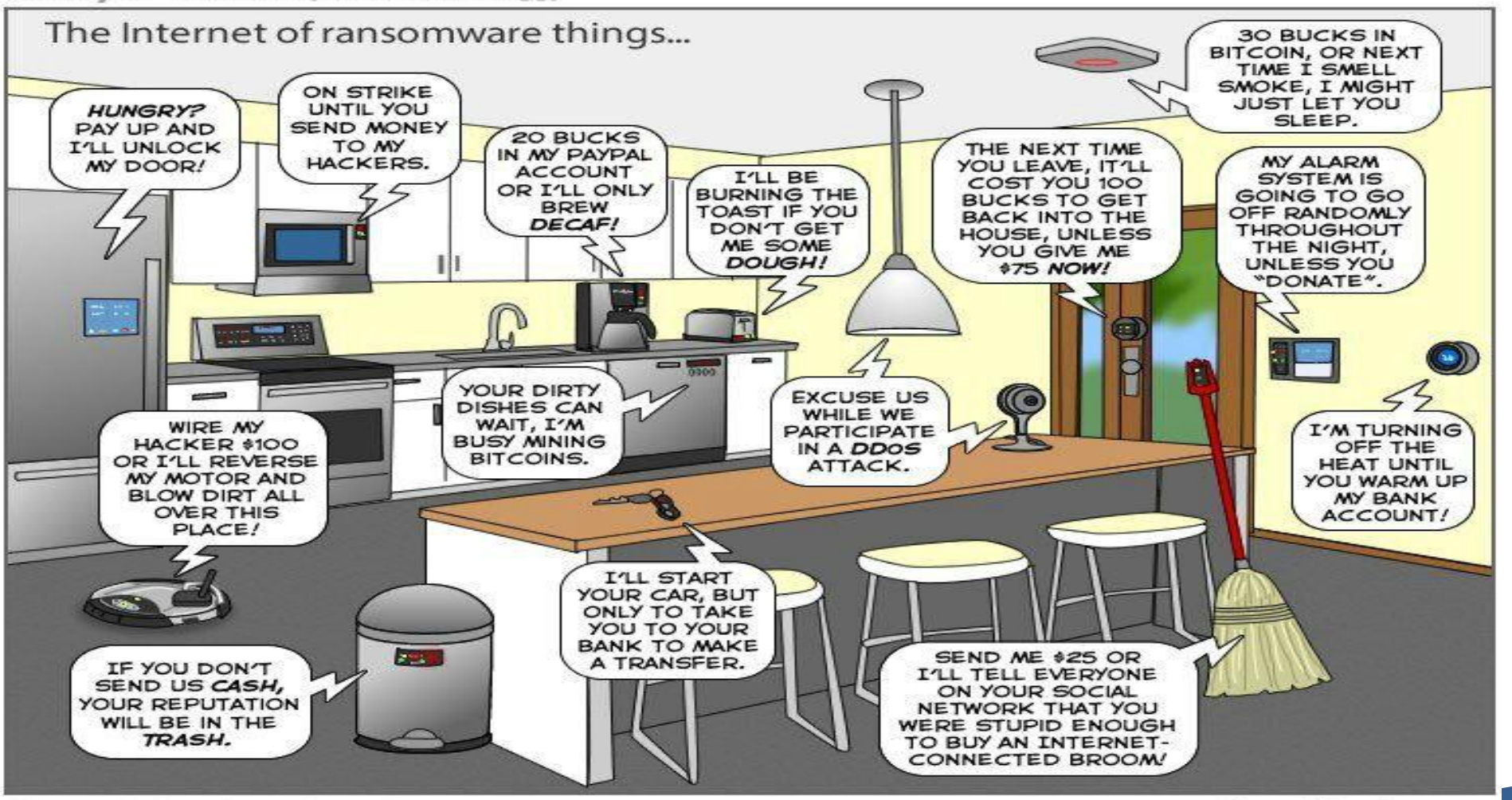
Los beneficios obtenidos y el acceso cada vez más fácil a las herramientas de ataque propicia el incremento del número de ciberdelincuentes y, en consecuencia, el de sus acciones.



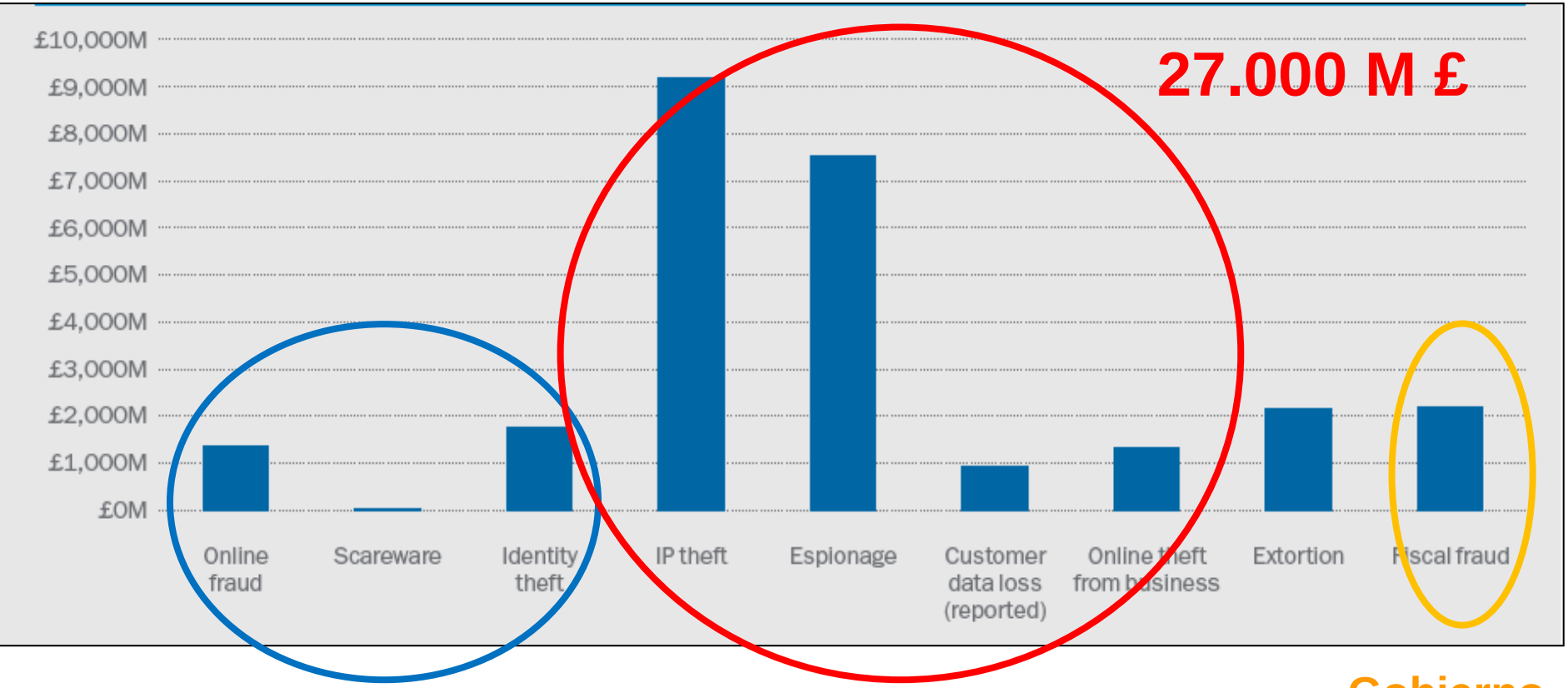




INTERNET DE LAS COSAS (IoT)



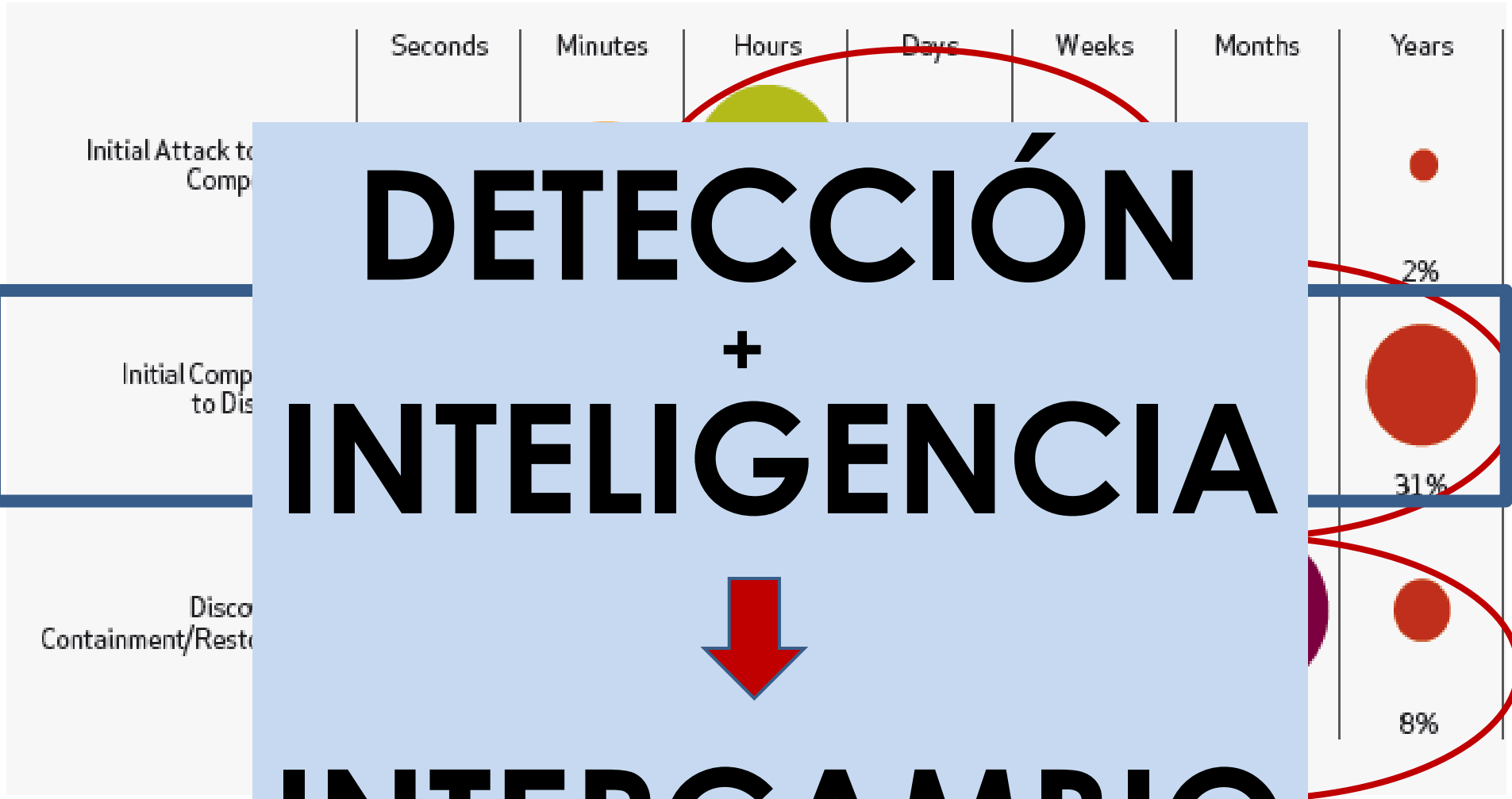
Coste CIBERESPIONAJE. UK



Ciudadanos …… 3.100 M£

Empresas…… 21.000 M£

Gobierno 2.200 M£



DETECCIÓN
+
INTELIGENCIA
⇓
INTERCAMBIO

VERIZON rp_dat

CONCLUSIONES

- Incremento constante del **número, sofisticación y complejidad** de los **ciberataques**
- **El ciberespionaje** sobre las administraciones públicas y las empresas estratégicas **es la amenaza más importante** para los intereses nacionales y la seguridad nacional
- La **dificultad de atribución** es el factor que caracteriza esta amenaza en relación con otras.
- La **amenaza procede** tanto de países con intereses encontrados como de países con intereses afines (¿amigos?).
- Es preciso reforzar la capacidad de **prevención y protección** en todas las instancias del Estado (ciudadanos, empresas y administraciones públicas)
- Es preciso reforzar las **capacidades de INTELIGENCIA y de PERSECUCIÓN DEL DELITO TECNOLÓGICO** para la identificación de atacantes, determinación de sus objetivos y aplicar la legislación vigente al respecto.

Invertir en CIBERSEGURIDAD al menos una cantidad equivalente que en SEGURIDAD FÍSICA.

¿PREGUNTAS?

La **"huella digital" de nuestra vida, consciente o desapercibida, tendrá un enorme valor económico en el futuro,** y se podrá vender e intercambiar por efectivo, descuentos, productos o servicios que cada vez están más personalizados y adaptados al cliente.

- **E-Mails:** José Antonio Mira
  - **ccn-cert@cni.es**
  - **info@ccn-cert.cni.es**
  - **ccn@cni.es**
  - sat-inet@ccn-cert.cni.es
  - sat-sara@ccn-cert.cni.es
  - **incidentes@ccn-cert.cni.es**
  - organismo.certificacion@cni.es
- **Websites**
  - www.ccn.cni.es
  - **www.ccn-cert.cni.es**
  - www.oc.ccn.cni.es

Gracias