Deloitte.

CyberSOC *Academy*

# Hacking & Cybersecurity for Fun and Profit

#somauditors 

26è Fòrum de l'Auditor Professional

**Deepak Daswani**
ddaswani@deloitte.es

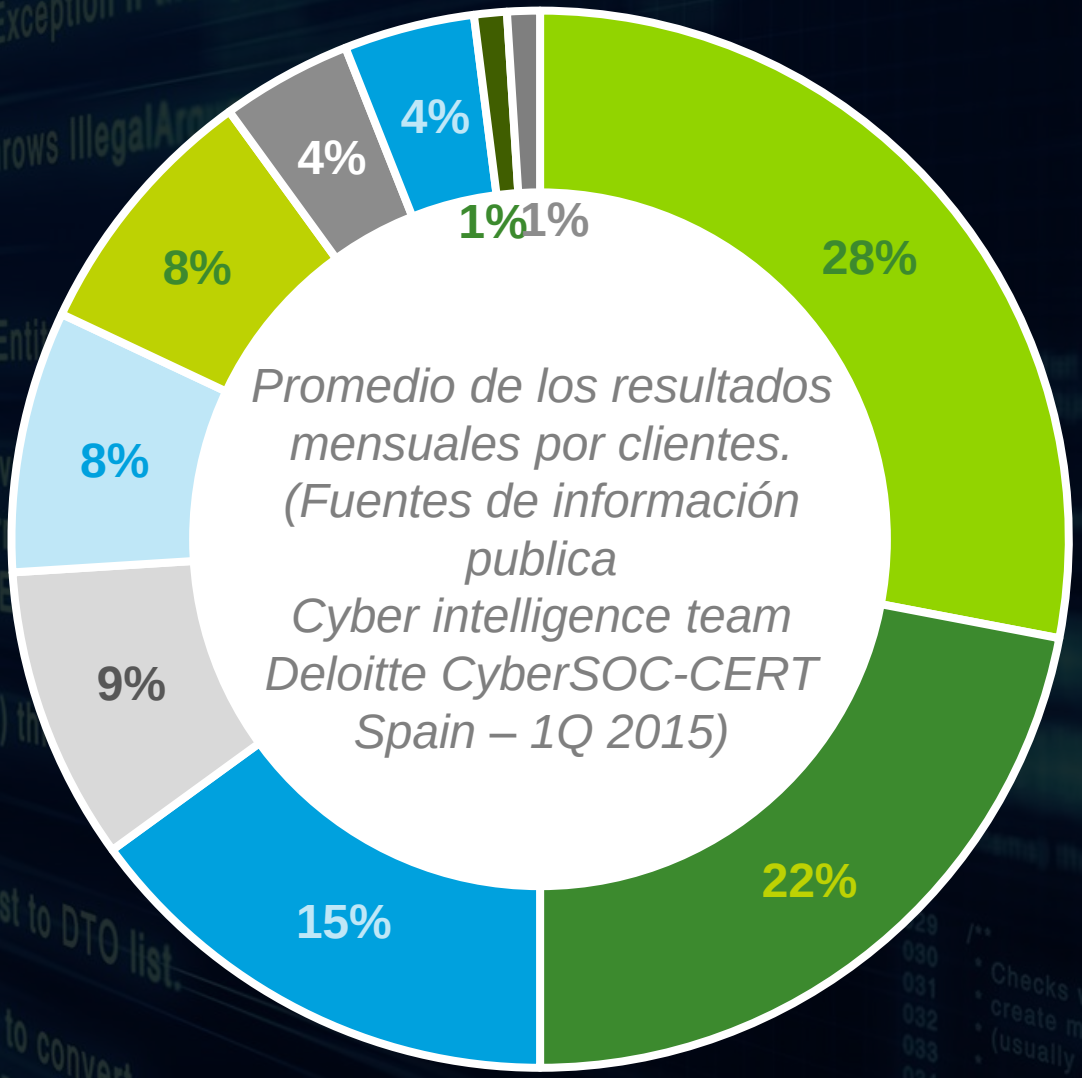
**Sergi Gil López**
sgillopez@deloitte.es

# deepak@daswani:/$ whoa

Deloitte. CyberSOC Academy

- Ingeniero Superior en Informática (ULL) y Experto en Seguridad Informática y Hacking Ético (URJC)
- Actividad profesional en el sector TIC en Canarias (2004-2013)
- Docente en cursos y postgrados universitarios además de formación especializada a empresas particulares
- Investigador de Seguridad. Publicación en blogs especializados y escritor de libros de seguridad con el equipo de MundoHacker
- Security Evangelist de INCIBE (MINETUR, Gobierno d España (Octubre de 2013 – Julio 2015)
- Colaborador fijo de medios de comunicación a nivel autonómico, nacional e internacional:
- *Diario de Avisos (Columna Defiéndete Online)*
- *Televisión Autonómica de Canarias (Buenos días Canarias y Canarias2punto*
- *Radio Autonómica de Canarias (Galaxias y Centellas)*
- *Cadena SER*
- *CNN*
- *…*
- Cybersecurity Expert Deloitte CyberSOC Academy
- Cofundador de HACKRON

# Tendencias en ciberataques




- Malware (excluyendo botnets)
- Otros fraudes
- Phising global
- Credenciales filtradas
- Botnets
- Información corporativa
- Spear phising
- Información financiera
- Información personal (no credenciales)
- Bases de datos

# Motivaciones

Lucro económico

Posicionamiento geopolítico

Inoperatividad

Extorsión

Robo de información

# De venta en los mercados negros

Hospedaje ($10 a $200) en servidores anónimos

Malware personalizado para atacar una empresa ($12 a $3,500)

Spam a **1 millón** de direcciones de email válidas ($70 a $150)

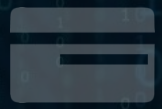
Tarjetas SIM activas para móviles ($100)

Cuentas de juego y apuestas ($10 a $15), las cuales representan un valor real

1,000 de **seguidores** en RRSS ($2 a $12)

1,000 **cuentas de email válidas** ($0.50 a $10)

Cuentas en la nube ($7 a $8), que pueden server para hospedar servidores de command-and-control (C&C)



Tarjetas de crédito comprometidas ($0.50 a $20)

Ataques de denegación de servicio distribuidos (DDoS) $10 a $1,000 al día

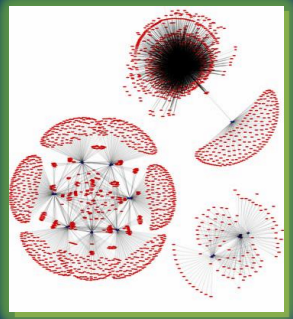
**Los equipos de ciberinteligencia se encargan de detectar qué información robada de una empresa se encuentra en la deep web.*

# Ciberamenazas

***APT: Amenazas Avanzadas Persistentes***

***Malware***

***Botnets***



***DDoS***

# Malware

- Un malware es un programa que se instala en un sistema informático sin que nadie sepa que está ahí, con el objetivo de llevar a cabo actividad maliciosa.
- Malware es la gran amenaza del 2015!
  - Comunicarse con otros equipos y recibir instrucciones del mando de control del malware (Command and Control panel - C&C).
  - Ciberespionaje.
  - Robo de identidad.
  - Lanzar ataques contra otros sistemas o enviar malware a otros usuarios y/o dispositivos.
  - Almacenar contenido ilegal en equipos.
  - Espiar dispositivos (keyloggers, cámaras, micrófonos del dispositivo).
  - Cifrado no autorizado de datos (ransomware).
  - Construir patrones de comportamiento y usos.
  - Proliferación del cibercrimen.

**Malware nuevo es generado a un ratio de 160,000 - 225,000 nuevas muestras cada día.*

# Advanced persistent Threats

Las diferencias principales con ataques tradicionales:

**Selección de la víctima:**

En la mayoría de estos ataques existe un blanco determinado; en ataques tradicionales se utilizan objetivos que estén disponibles y sin determinar.

**Silencio :**

Estos tipos de ataques intentan pasar inadvertidos por un periodo de tiempo mayor.

**Duración del ataque :**

A pesar de todos los esfuerzos , el tiempo medio que se tarda en detectar un APT es de meses.

**Las brechas de seguridad son inevitables. Los actores más resueltos siempre encontrarán una manera.*

# Botnets es un tipo de malware
## (2014 – Deloitte CyberSOC Spain)


**Botnets, a través de servidores de Command and Control, controlan PCs zombies de usuarios de todo el mundo.*

# Hacktivismo

Inicialmente estuvo ligado a acciones sociales en favor de los derechos y la libertad de expresión.

Actualmente, representa un arma cibernética de primer orden.

La detección de campañas de hacktivismo puede ayudar en la prevención de ataques de DDoS (Denial of service attacks).

Los ataques de DDoS se dirigen normalmente a portales o páginas web a los que se le realizan peticiones de manera masiva hasta conseguir colocarlas offline.

**El número de ataques de DDoS creció en 2014, un 240% con respecto al año anterior (Deloitte CyberSOC Spain).*

# Puntos de entrada de malware

## Ingeniería Social

Los atacantes llevan a usuarios legítimos a realizar tareas según sus órdenes. La falta de concienciación, la curiosidad, el exceso de confianza y el ego, son las claves del éxito de estas técnicas.

## SPAM y PHISHING

Envío masivo e indiscriminado de emails, con contenido falso (**phishing**) que normalmente personifica a una entidad de confianza.

**Spear phishing** es un tipo de phishing, personalizado y dirigido a individuos concretos o a un colectivo dentro de una misma organización. El asunto y el cuerpo del mensaje también están personalizados.

**El malware se suele encontrar como fichero adjunto de un phishing o como un enlace dentro del cuerpo del mensaje.*

# Robo de Credenciales

## ¿Cómo sucede?

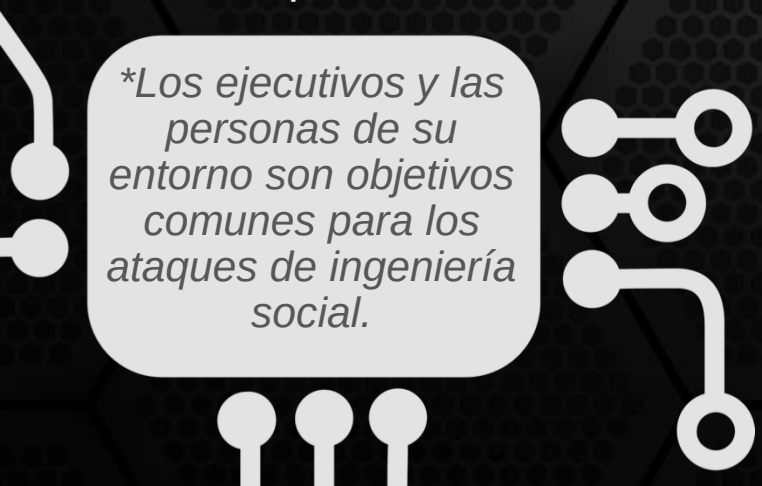
1. Una entidad de confianza es suplantada como emisora de un email falso, o un whatsapp, un mensaje de texto, etc.
2. Una campaña de spam distribuye el email con un enlace a una página web falsa de la entidad suplantada (**phishing**)
3. 1 de cada 10 empleados expuestos a spam malicioso hará click en el enlace
4. El usuario accede a la página web falsa con su login y password
5. Los datos robados son vendidos en el mercado negro

**La generación, almacenamiento, custodia y distribución de credenciales son tareas críticas en ciberseguridad.*

# Ingeniería Social

- La ingeniería social es la manera más efectiva y fácil de entrar a un sistema.
- Consiste en recoger información mediante la manipulación legítima de los usuarios.
- El factor clave para utilizar la técnicas de ingeniería social con éxito se basa en la naturaleza humana: ego, empatía y modos de pensamiento.
- Educar para saber dónde, cuándo y en quién confiar, si se trata de otra persona, un sitio web o un dispositivo de comunicación.

**Los ejecutivos y las personas de su entorno son objetivos comunes para los ataques de ingeniería social.*



A todos nos gusta mostrar que estamos bien informados y documentados.

La mayoría de las personas reutilizan contraseñas.

No queremos parecer mal educados o groseros ante otras personas.

Siempre estamos dispuestos a dar detalles y hablar de nuestros logros personales.

# Los ejecutivos como vector de entrada a un ataque

**Ejecutivos** son **objetivos** obvios y claves

Sus contraseñas sueles habilitar el acceso a las áreas más sensibles de la empresa.

La información en sus PCs, portátiles y móviles es clave para defines y planear APTs.

La suplantación de ejecutivos es una manera efectiva de lograr que alguien realice algo que normalmente no le está permitido.

Conocen gente constantemente, recogen tarjetas y no tienen el tiempo para revisar identidades falsas.

Suelen ser usuarios privilegiados en las bases de datos.

Tradicionalmente, managers y directivos han valorado a sus colaboradores en base a la resolución rápida de tareas, no en base a qué niveles de seguridad aplican.

**Dirigirse a un líder puede crear un vector de entrada fácil para realizar un ataque dirigido a una compañía.*

# Buenas prácticas en el ciberespacio

## Mecanismos para combatir un ciberataque:

- Medidas administrativas
- Medidas técnicas
- Marco legal

## Factores claves para preparase ante un ciberataque:

- Concienciación
- Inversión
- Formación técnica especializada

# Buenas prácticas en el ciberespacio (Oficina, Viajes, Hogar)

Usar contraseñas seguras, robustas y custodiarlas con rigor

Mantener todas las aplicaciones de software y anti-virus al día

Adquirir licencias originales de software y aplicaciones

Evitar las conexiones a redes Wifi públicas

Realizar frecuentemente copias de seguridad y gestionarlas correctamente


No hacer click sobre enlaces. Siempre escribir la URL en el navegador y forzar https://

No confiar en dispositivos de almacenamiento (USB) externos

Utilizar un antivirus de prestigio y reputación contrastada

No enviar información del trabajo al email personal ni viceversa

Establecer una polícita para el correcto uso de redes sociales

Contacto:

ES ERS IT CyberSOC Academy
deloittecybersocacademy@deloitte.com

CyberSOC Academy

Deloitte.