jtsec

BEYOND IT SECURITY

jtsec
BEYOND IT SECURITY

ASPECTOS TÉCNICOS DE PREVENCIÓN Y SOLUCIÓN

JORNADA Claves en la ciberseguridad empresarial y ayudas a su implantación

TIC Cámaras

Unión Europea
Fondo Europeo
de Desarrollo Regional
"Una manera de hacer Europa"

Cámara de Comercio de España

Cámara Granada

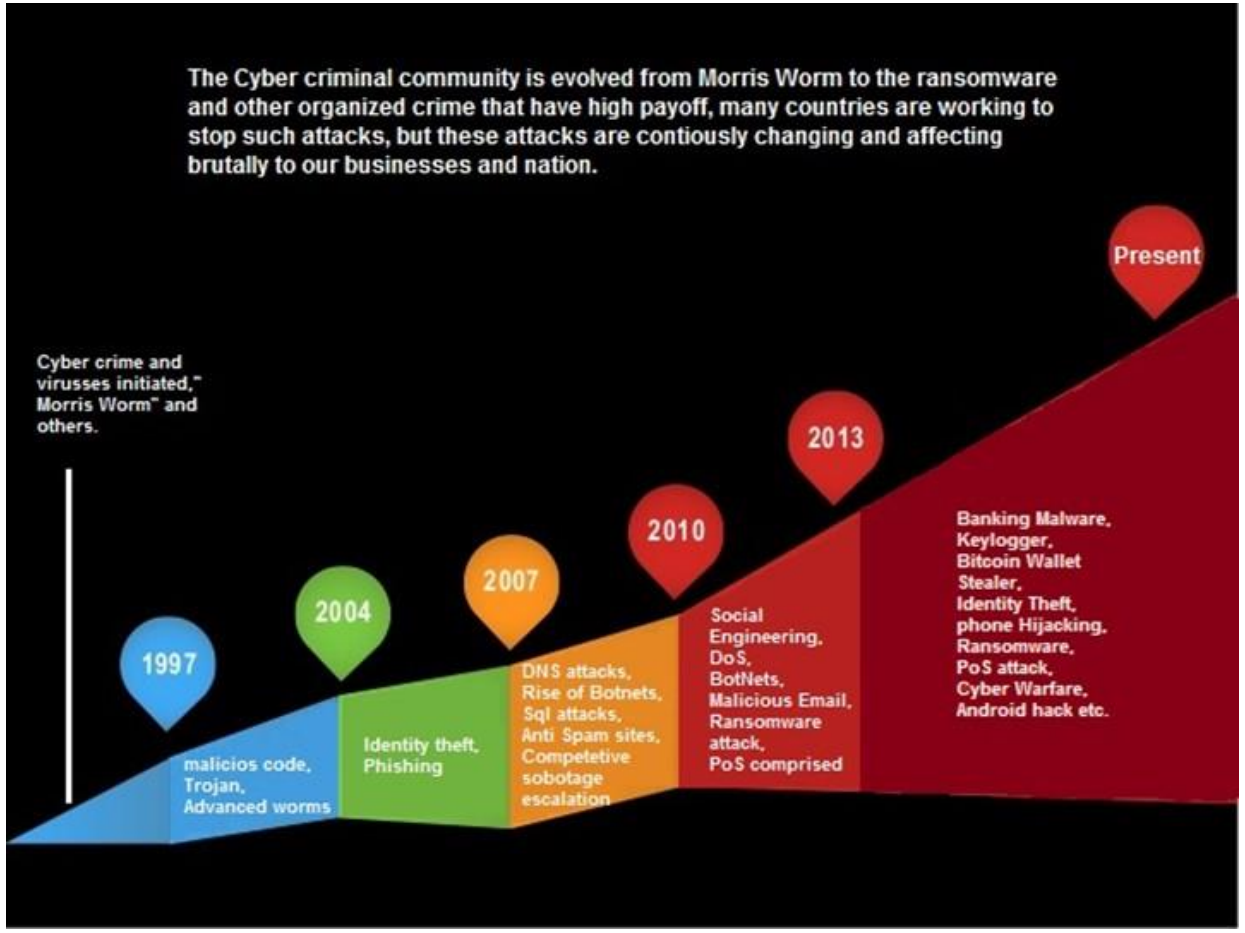
Sobre mí

- **José Manuel Pulido**
- Ingeniero en Informática (Universidad de Granada)
- Consultor en certificación ciberseguridad, en **jtsec Beyond IT Security S.L.**
- Experto en certificación Common Criteria y LINCE
- Evaluador de ciberseguridad de productos y sistemas
- Miembro contribuidor del grupo para la estandarización ISO/IEC JTC 1/SC 27/WG3 para la definición de criterios de evaluación de vehículos conectados
- Miembro vocal del grupo CNT320 para el estudio de la ciberseguridad en vehículos conectados

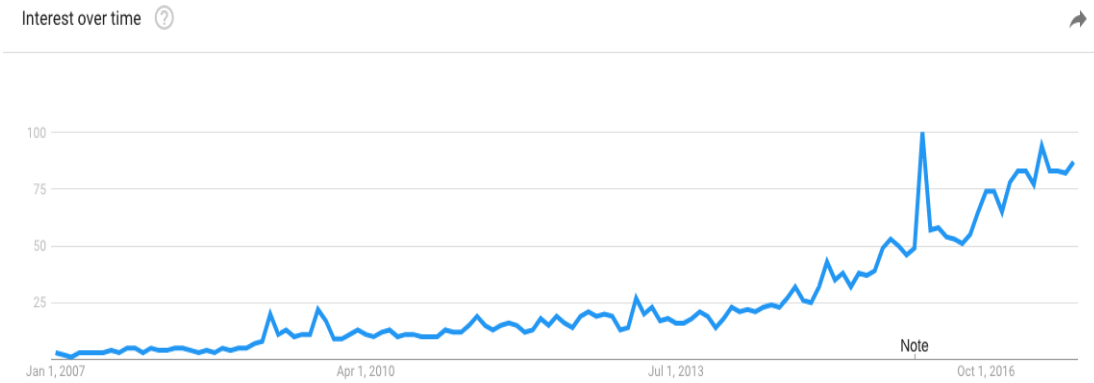
Prevención y solución

- Los sistemas TIC son fundamentales para el funcionamiento de la empresa
- Almacenamos y usamos información valiosa, servicios críticos y sistemas de alto valor económico
- ¿Estamos preparados para defendernos de un ciberataque?
- ¿Sabemos que probablemente seamos objetivo de un ciberataque?

Evolución histórica

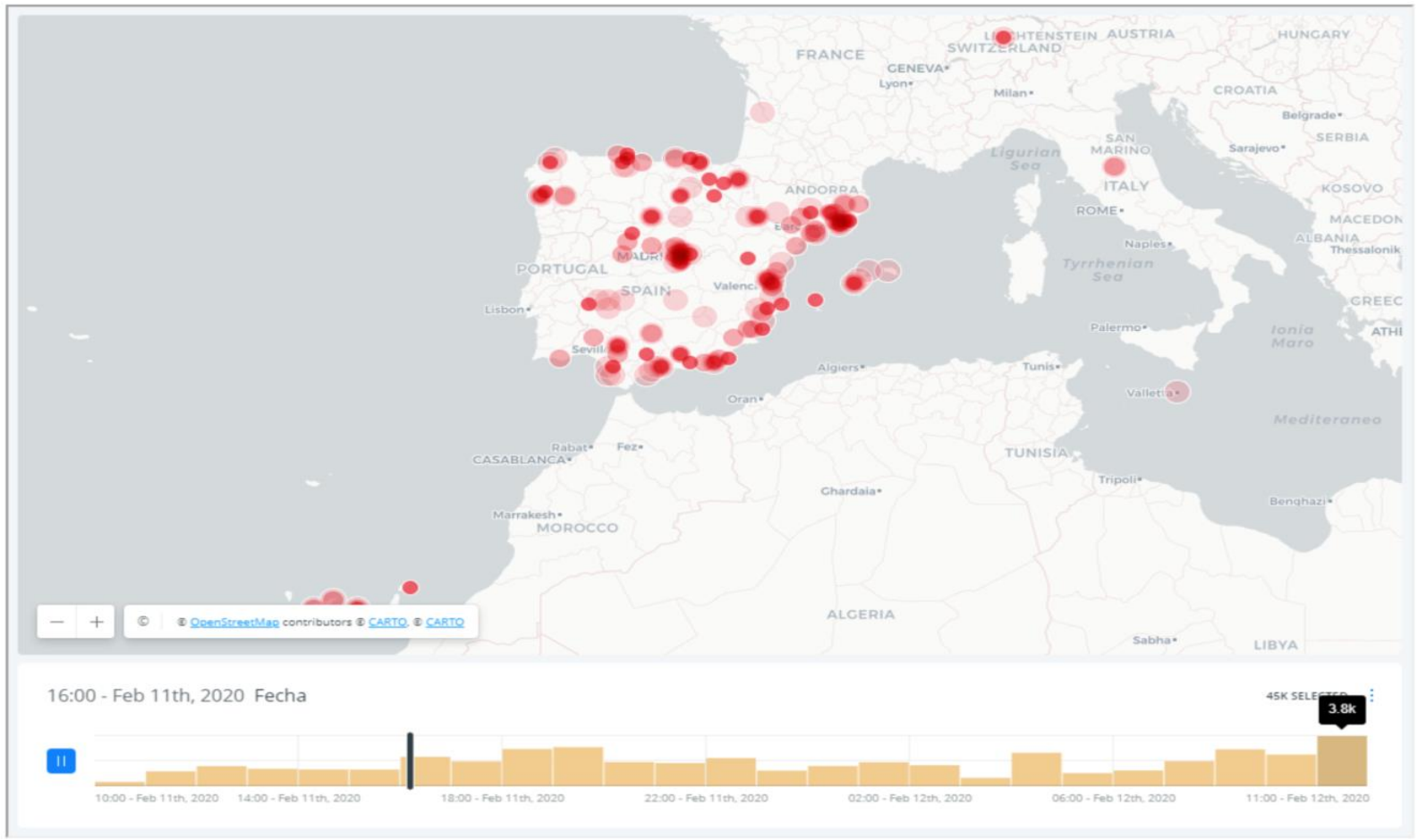


A medida que los atacantes han ido evolucionando y depurando sus métodos, se han desarrollado nuevas defensas y sobre todo concienciación global.



Fuente: https://resources.infosecinstitute.com/evolution-in-the-world-of-cyber-crime/#gref

¿Puede ocurrirle a mi empresa?



INCIBE registra decenas de ataques diarios a sistemas ligados a la administración.

Los ataques a la mayoría de entidades privadas no se contabilizan.

Fuente: https://www.incibe-cert.es/respuesta-incidentes/nivel-impacto-espana

Cómo afectan a las empresas

- **El 43% de los ciberataques tienen como objetivo empresas pequeñas o medianas**
- El **coste medio** de filtraciones de datos en 2020 será superior a 150 millones de dólares
- Las compañías tardan unos **seis meses** en **detectar** una brecha de datos (incluso grandes compañías)
- El **precio de las acciones** cae un 7% de media después de una brecha de datos.

Fuente: https://www.cybintsolutions.com/

La importancia de la ciberseguridad

¿Son tan preocupantes las ciber-amenazas?

"El cibercrimen es la mayor amenaza para cualquier compañía del mundo"

Ginni Rometty,
CEO y presidenta de IBM

El camino de la prevención

- Conocerse a **uno mismo**
  - Qué debo proteger y cuánto valor tiene
  - Cuántos recursos emplear en proteger
  - Cuáles son nuestras debilidades
  - Cuáles son nuestras fortalezas
- Conocer a nuestros **enemigos**
- Conocer a nuestros **aliados**
- ACTUAR

¿Qué debo proteger?

INFORMACIÓN

- Propiedad intelectual
- Datos de clientes
- Datos bancarios
- Datos de negocio
- Información privilegiada

SERVICIOS

- Páginas web
- Correo electrónico
- Comercio online
- Portales de cliente
- Servicios internos

SISTEMAS IT

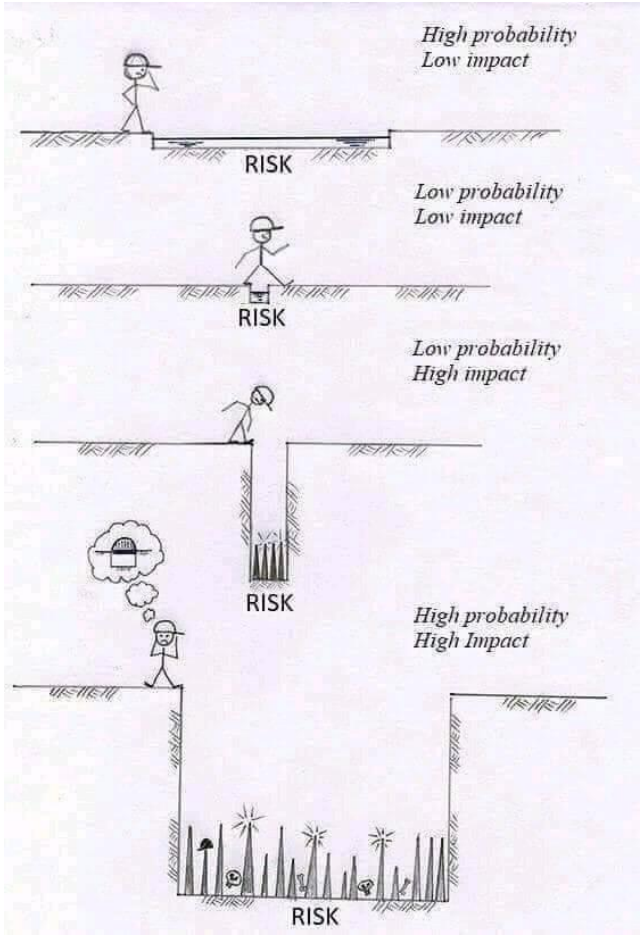
- Servidores web
- Portátiles y móviles
- Equipamiento de red
- Webcams
- CPDs

ACTIVOS DE LA EMPRESA

¿Cuánto invertir en proteger la seguridad?

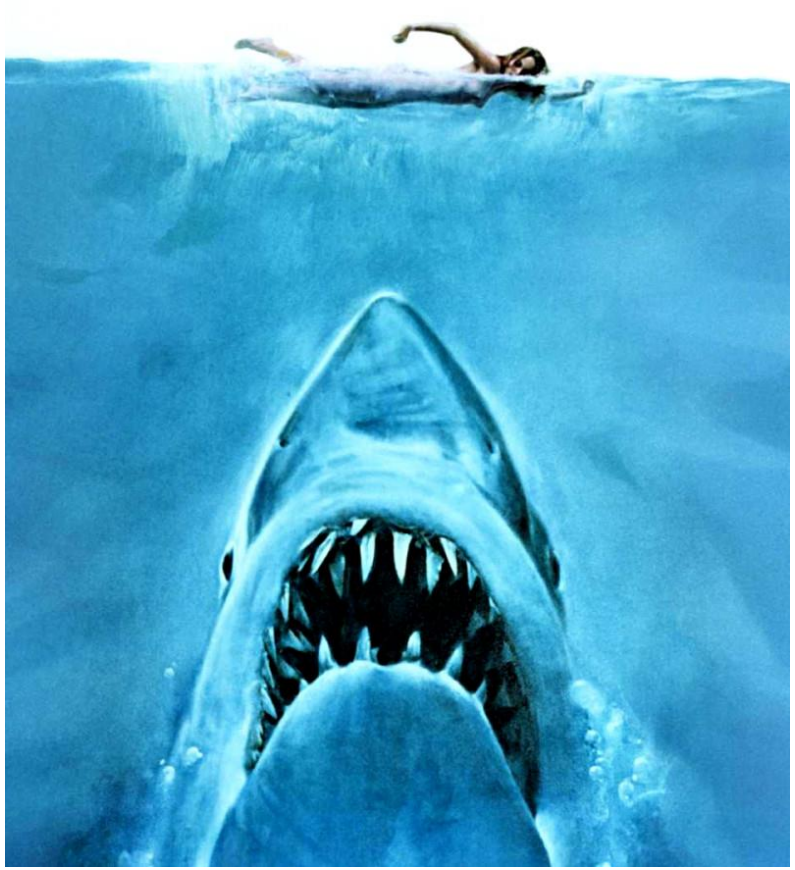
- Según el **valor** de los activos a proteger, según:
  - Impacto: ¿qué ocurre si se compromete?
  - Probabilidad: ¿cómo de probable?

- **Regla general: l**a inversión en ciberseguridad debería ser equivalente a la inversión en seguridad física.



¿Cuáles son nuestras debilidades?

No ser conscientes del peligro



No estar preparados para defendernos

El factor humano es el eslabón más débil

¿Cuáles son nuestras debilidades?

- **Superficie de exposición cada vez mayor**
  - Más tipos de dispositivos conectados
  - Más formas de acceder a la información
  - Más servicios en la nube
  - Los usuarios usan sus propios dispositivos (móviles, tablets, teletrabajo)
  - El correo corporativo en los móviles personales es un peligro
  - Dispositivos seguros e inseguros en la misma red
  - No siempre es posible controlar la seguridad

¿Cuáles son nuestras fortalezas?

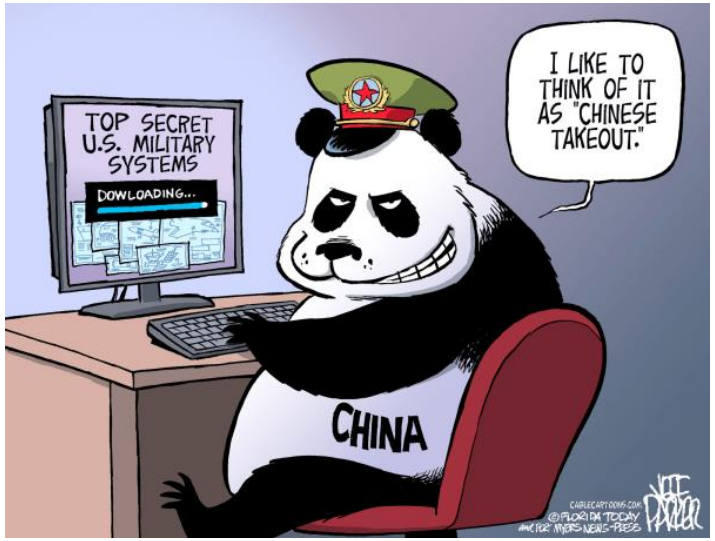
- Contamos con **más información y recursos formativos** que nunca…
  - Para personal técnico encargado de la protección
  - Para la concienciación de los usuarios
- Canales de avisos de ciberseguridad
- Gran cantidad de herramientas gratuitas

Conocer al enemigo

¿Quiénes son?

Ciberespías

- Roban información para vender a competidores
- Alta capacitación técnica
- Ligados a organizaciones o gobiernos



Cibercriminales

- Cometen ciberdelito y fraude para obtener beneficios económicos
- Organizados o en solitario
- A veces ligados a movimientos ideológicos

Conocer al enemigo

¿Qué quieren de nosotros?

Nuestra información

ROBAR

Secretos industriales, Propiedad intelectual
Datos de clientes
Información de mercado o negocio

SECUESTRAR

Cifrar y pedir un rescate a cambio de la clave

FILTRAR

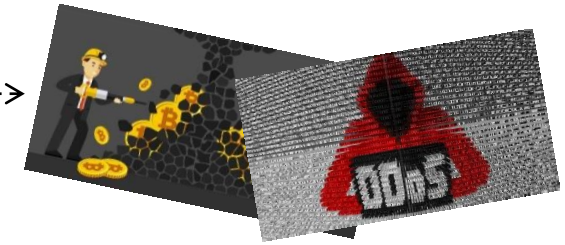
Generar pérdida de imagen y de reputación
Generar problemas legales y económicos

Conocer al enemigo

¿Qué quieren de nosotros?

Nuestros sistemas y servicios

USO ILÍCITO



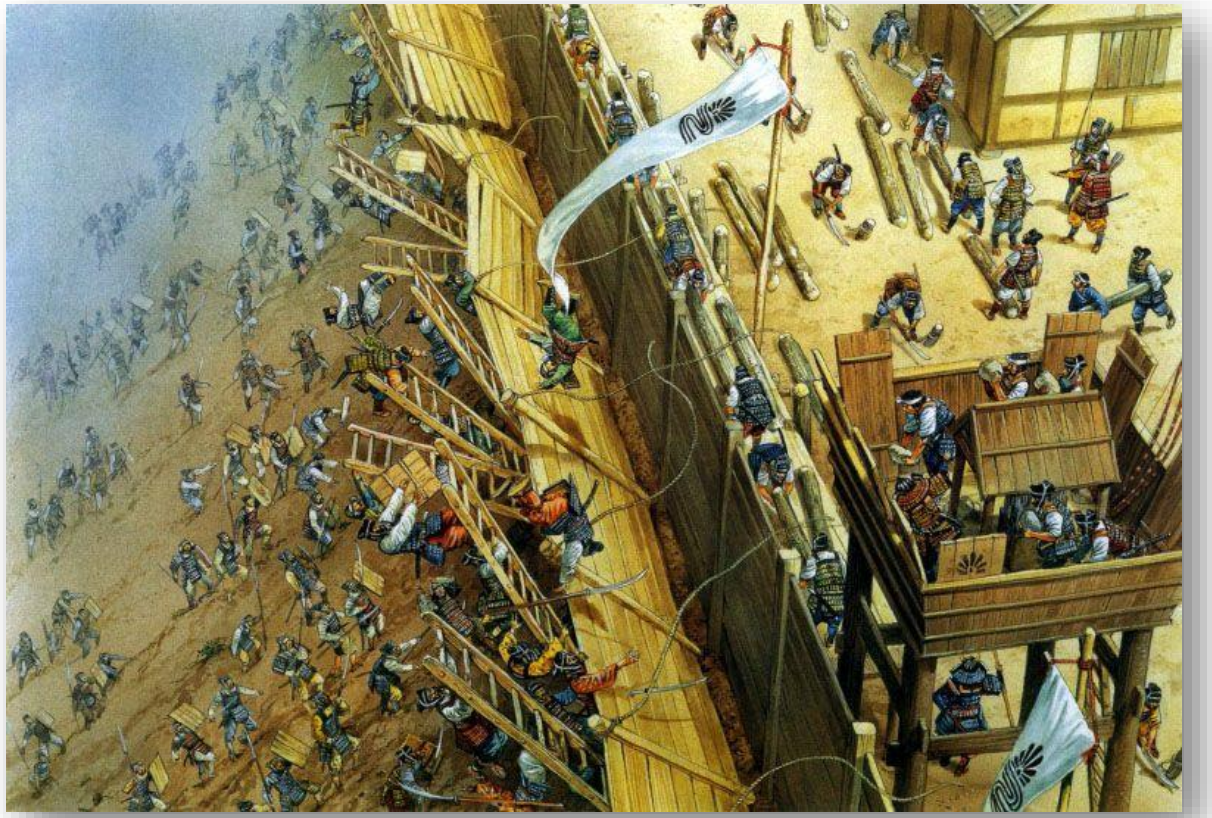
- Minado de criptodivisas
- Cyberataques desde nuestros equipos

INTERRUMPIR

- Interrumpir los servicios al público
- Generar perjuicio a clientes y a empresa
- Deteriorar la imagen de la empresa

Conocer al enemigo

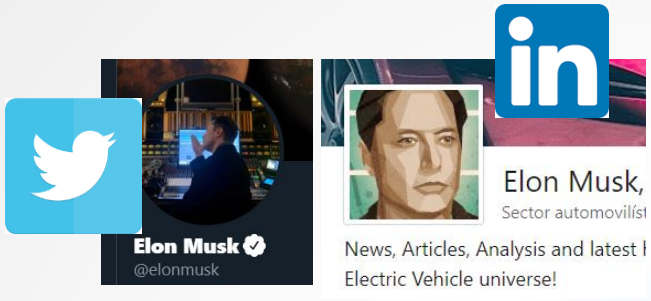
¿Cómo nos atacan?



- Existen multitud de métodos y vectores de ataque
- Es difícil protegerse de todos.
- Pero unos pocos son:
  - Los más **comunes**
  - Los más **efectivos**
  - Los más **conocidos**

Spear phishing a través de e-mail

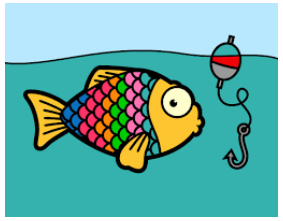
El 75% de los ataques son a través de spear phishing a través de correo electrónico.



Se estudia a la víctima: su trabajo, sus proveedores, sus intereses, sus aficiones..

Se diseña un e-mail para que parezca de un tercero confiable: su banco, su teleoperadora, Google…

Nos urge a resolver un problema: fondos, password cambiado…
Contiene campos y un enlace para robar credenciales, instalar malware...



El usuario ¿hace click?

Ataques a sistemas desactualizados

Los sistemas desactualizados contienen **vulnerabilidades públicas fácilmente explotables**

Sistemas accesibles desde el exterior

Webs con CMS y sus plugins

Sistemas internos desactualizados

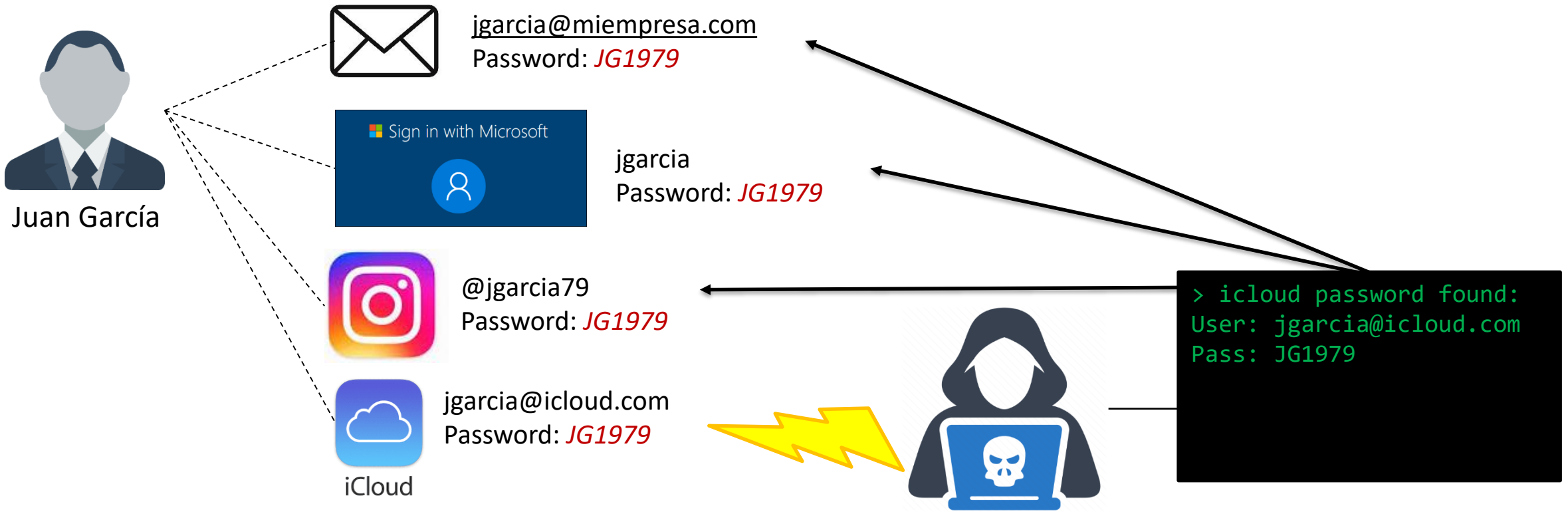
Aplicaciones de uso común

Hardware con firmware vulnerable

Uso de librerías vulnerables

Ataques a contraseñas inseguras

- Una contraseña corta, sencilla o deducible es INSEGURA
- Una contraseña **reutilizada** es INSEGURA^{N} (N = número de servicios donde se usa)



¿Y si el enemigo está en casa?

- **Usuarios:**
  - Poco formados
  - Poco prudentes, vulnerables a ingeniería social
  - Con demasiados permisos de acceso
- **Administradores de sistemas:**
  - Poco formados en seguridad
- **Directiva:**
  - Se consideran por encima de la seguridad
  - ¿Proporcionan los recursos necesarios para proteger?
  - ¿Promueven la cultura de seguridad en la empresa?
  - ¿Promueven auditorías de seguridad?

Conocer a nuestros aliados

- No solo existen **multitud de recursos** formativos online
- También existen **entidades públicas y privadas** que publican abundantes recursos para formación, concienciación, detección y solución
  - **INCIBE –** boletines de noticias, blogs, artículos, guías de seguridad.
    - Línea de atención **017** ante incidentes de ciberseguridad
  - **AEPD –** Guías para implementar protección de datos personales
  - **nomoreransom.org –** Ayuda a recuperarse de ataques de ransomware conocidos.
  - **haveibeenpwned.com –** Comprobar si nuestra clave de e-mail ha sido filtrada

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

NO MORE RANSOM!

';--have i been pwned?
Check if you have an account that has been compromised in a data breach

Conocer a nuestros aliados

Recurrir a **profesionales** que nos ayuden a evaluar y mejorar la seguridad de nuestros sistemas

- **Auditorías de seguridad** (tests de intrusión).
  - Expertos en seguridad realizan pruebas de penetración para comprobar si un atacante podría entrar con éxito en nuestros sistemas.
  - Evaluan la seguridad a nivel técnico, a nivel humano (ingeniería social) y a nivel de gestion de la seguridad.
  - Identifican los problemas, proponen soluciones y forman al personal.
- **Consultoría de seguridad.**
  - Profesionales que ayudan a diseñar una arquitectura segura y líneas de defensa adecuadas.

Prevención mediante buenas prácticas

El conocimiento en prevención se puede aplicar con una serie de reglas sencillas

Decálogo de buenas prácticas de seguridad

1. Implantar la cultura de la ciberseguridad en la empresa

- La directiva debe promover la ciberseguridad
- Fomentar la formación y concienciación
- Desarrollar políticas, normativas y procedimientos de seguridad
- La ciberseguridad debe tomarse como una inversión
- Estar al día: boletines de noticias, avisos INCIBE
- Diseñar plan de recuperación ante ataques

Decálogo de buenas prácticas de seguridad

2. No abrir enlaces ni descargar ficheros sospechosos

- El phishing se evita con precaución
- Evitar abrir adjuntos en correos, pueden contener virus
- Revisar dominio del remitente en los correos
- Revisar URL de los enlaces en los correos
- Nunca introducir nuestras credenciales en enlaces recibidos
- Ante la duda, consultar con el personal de IT

Decálogo de buenas prácticas de seguridad

3. Utilizar software y hardware de seguridad

- Antivirus instalado y actualizado en todos los equipos
- Protección en tiempo real activada
- Escanear ficheros descargados
- Utilizar un cortafuegos para la salida a internet

Decálogo de buenas prácticas de seguridad

4. Utilizar contraseñas seguras

- Más larga = más segura (mínimo 10)
- Combinar números, mayúsculas, minúsculas y símbolos
- Mejor una frase que una palabra
- NO reutilizar contraseñas en varios sitios
- Cambiarlas periódicamente
- No recordar contraseñas en el navegador
- No introducirla en webs que miden la complejidad!

Decálogo de buenas prácticas de seguridad

5. Limitar superficie de exposición

- Instalar sólo el software necesario
- No tener servicios innecesarios corriendo en servidores
- Limitar al mínimo necesario los permisos
- No usar la nube como carpeta de trabajo
- No usar red WIFI si no es estrictamente necesario
- Desconectar tomas de red sin uso del switch

Decálogo de buenas prácticas de seguridad

6. Cifrar información sensible y borrado seguro

- La información más crítica debería estar cifrada
- Los equipos portátiles de trabajo deben estar cifrados
- La información en discos extraíbles debe cifrarse
- Antes de tirar o reutilizar equipos, hacer borrado seguro

Decálogo de buenas prácticas de seguridad

7. No usar software ilegal

- El software pirata descargado de internet suele contener malware
- El software pirata puede permitir acceso remoto al equipo
- No usar cracks ni keygens: suelen estar infectados
- El software ilegal termina en auditorías y multas económicas

Decálogo de buenas prácticas de seguridad

8. Hacer copias de seguridad periódicas

- Si la información se borra por accidente, necesitas un backup
- Si un equipo se estropea, necesitas un backup
- Permiten recuperarse de un ataque Ransomware
- Muy recomendable almacenarlas en otra ubicación
- Muy recomendable almacenarlas cifradas
- No usar la nube para backups de información privada

Decálogo de buenas prácticas de seguridad

9. Mantener los sistemas actualizados

- Los sistemas desactualizados son vulnerables
- Las actualizaciones deben ser periódicas y programadas
- No ignorar avisos de actualizaciones!
- Prioridad:
    1. Antivirus
    2. Sistema operativo
    3. Aplicaciones

Decálogo de buenas prácticas de seguridad

10. Revisiones periódicas - auditorías

- Revisar periódicamente el estado de la seguridad
- Revisar permisos de carpetas
- Revisar si hay usuarios obsoletos antiguos
- Realizar auditorías de seguridad (tests de intrusión) periódicamente

Un breve resumen

- La ciberseguridad es una inversión
- La ciberseguridad debe estar en la cultura de la empresa
- Formación y concienciación: conocer al enemigo para defendernos
- Usar el decálogo de buenas prácticas
- Contratar profesionales para auditar y mejorar nuestra seguridad

Contact

jtsec: Beyond IT Security

Granada & Madrid – Spain

hello@jtsec.es

@jtsecES

www.jtsec.es

"Any fool can make something complicated. It takes a genius to make it simple."
Woody Guthrie