

Seguridad Informática

Tema 10 – Presente y futuro de la Seguridad informática



- Seguridad en entornos cloud.
- Blockchain.
- Seguridad en dispositivos móviles y BYOD.
- APTs.
- Ciberguerra.
- Protección de infraestructuras críticas.
- 5G.
- IoT/Industria.
- Deepweb.
- IA y ciberseguridad.
- Deepfakes.

- Seguridad en entornos cloud.
- Blockchain.
- Seguridad en dispositivos móviles y BYOD.
- APTs.
- Ciberguerra.
- Protección de infraestructuras críticas.
- 5G.
- IoT/Industria.
- Deepweb.
- IA y ciberseguridad.
- Deepfakes.

- Entorno cloud (*Cloud Computing*) es un modelo tecnológico que permite el acceso ubicuo, adaptado y bajo demanda a un conjunto compartido de recursos de computación.
- Hay tres modelos:
 - **Infrastructure as a service (IaaS)**: ordenadores físicos o máquinas virtuales. Los usuarios instalan sistemas operativos y sus aplicaciones.
 - **Platform as a service (PaaS)**: plataformas de cómputo.
 - **Software as a service (SaaS)**: acceso a aplicaciones y bases de datos. El proveedor de cloud gestiona la infraestructura y la plataforma.
- Ha surgido el modelo SECaaS: Security as a Service. Empresas que proporcionan servicios relacionados con la seguridad.

- Algunas aspectos a tener en cuenta:
 - Pérdida de control sobre los activos (datos, aplicaciones, sistemas de información,...) que provoca la externalización.
 - Esto influye en la confidencialidad y disponibilidad.
 - Necesidad de conectarse con los servicios contratados a través de internet.
 - Ya no se pueden utilizar los esquemas de seguridad de protección del perímetro.
 - Dependencia de los proveedores para garantizar la seguridad de sus sistemas.
 - La convivencia de los datos, procesos, aplicaciones, sistemas,... de diferentes organizaciones sobre las mismas máquinas físicas.

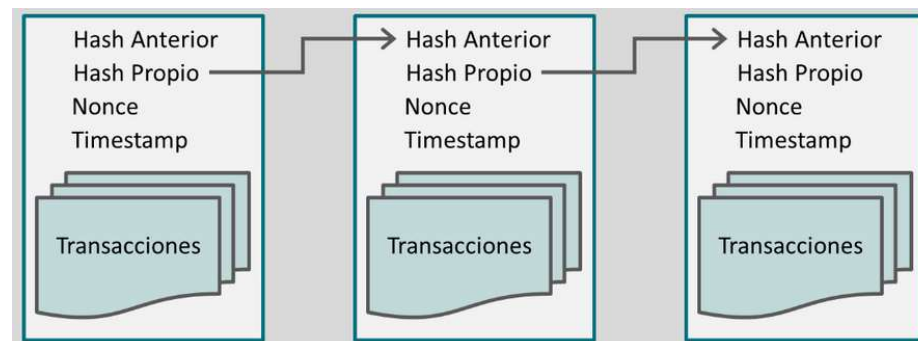
- La seguridad en entornos cloud se proporciona mediante:
 - Protocolos de red seguros.
 - Encriptación de los datos.
 - Sistemas de gestión de identidades y control de accesos.
- Siguen esquemas “Triple A” que tienen cuatro funcionalidades:
 - Identificación de un usuario asignándole una entidad digital.
 - **Autenticación:** verificar que un usuario es quien dice ser.
 - **Autorización:** control de acceso del usuario a los diferentes recursos.
 - **Auditoría:** trazabilidad de lo que el usuario hace.

- Para evitar saturar a los usuarios con una gran número de contraseñas se han creado los esquemas de IAAA federados con sus correspondientes aplicaciones federadas.
- Estas aplicaciones se caracterizan por confiar la autenticación y autorización de un usuario en un tercer servidor central.
- Parecido al protocolo Kerberos pero mejorado, y orientado a web.
- De esta manera evitan el almacenar un gran número de usuarios.

- Seguridad en entornos cloud.
- **Blockchain.**
- Seguridad en dispositivos móviles y BYOD.
- APTs.
- Ciberguerra.
- Protección de infraestructuras críticas.
- 5G.
- IoT/Industria.
- Deepweb.
- IA y ciberseguridad.
- Deepfakes.

- Generalmente se asocia el blockchain al tema de bitcoins y criptomonedas.
- Fue descrito en 1991 en un trabajo sobre bloques asegurados criptográficamente.
- Pero se hizo popular en 2008 con la llegada del bitcoin.
- Sin embargo su utilización se está extendiendo a otros ámbitos, como las instituciones financieras, servicios médicos o el Internet de las Cosas.

- Es un registro único, consensuado y distribuido en varios nodos de una red.
- En cada bloque se almacena:
 - Una cantidad de registros o transacciones válidas.
 - Información referente a ese bloque.
 - Su vinculación con el bloque anterior (hash).
- Cada bloque tiene un lugar específico en la cadena.
- La cadena completa se guarda en cada nodo → hay una copia exacta de la cadena en todos los participantes.



¿Por qué es tan seguro?

- Al haber una copia de la cadena en cada nodo, se asegura la disponibilidad de la información.
 - Una denegación de servicio necesitaría inhabilitar todos los nodos de una red.
- Como todos los nodos tienen la misma información, es casi imposible alterar algún dato (asegura la integridad).
- Además con el uso del hash, al añadir un nodo a la red su información es inmutable.
- Cada nodo tiene certificados y firma digital para verificar la información y validar los datos almacenados. Permite asegurar la autenticidad de la información.

- Los datos están distribuidos en todos los nodos de la red.
- Al no haber un nodo central, todos participan por igual almacenando y validando la información.
- Permite comunicar y almacenar información de manera confiable.
- Un modelo descentralizado donde la información es de los propios nodos que participan y no dependen de una compañía que proporcione el servicio.

Usos del Blockchain:

- Salud:
 - Los registros de salud podrían ser unificados y almacenados en blockchain. El historial médico de cada paciente estaría seguro y disponible para cada médico.
- Documentos:
 - El uso de blockchain permite registrar compras, escrituras, documentos o cualquier elemento digital evitando que pueda ser falsificado.
- Industria:
 - Generalmente para el control, o automatización, de líneas de producción, o aplicado a sistemas de almacenamiento y distribución de productos.

- Seguridad en entornos cloud.
- Blockchain.
- **Seguridad en dispositivos móviles y BYOD.**
- APTs.
- Ciberguerra.
- Protección de infraestructuras críticas.
- 5G.
- IoT/Industria.
- Deepweb.
- IA y ciberseguridad.
- Deepfakes.

- Desde hace años se estaba trabajando para implantar el teletrabajo... pero hasta el 2020 no se ha implantado de manera efectiva.
- La idea es trabajar desde cualquier lugar, y con cualquier dispositivo como si estuvieras en la oficina.
- Por lo que hay que dotar de cierta seguridad:
 - A la propia red para permitir dicha conexión.
 - A los dispositivos móviles para permitir conexiones desde cualquier dispositivo.

- El teletrabajo ha tenido una gran implicación en la cantidad de ataques que se han producido en los últimos años.
- Sin embargo, la vuelta a la “normalidad” ha traído otro problema asociado, y está relacionado con el BYOD.
- BYOD: *Bring Your Own Device*.

- Es una apuesta que se puso de moda antes de la pandemia, y consiste en permitir que los empleados usen sus propios dispositivos.
- Como consecuencia: los dispositivos móviles se han convertido en el nuevo objetivo de los ciberdelincuentes.
- El objetivo no es acceder al dispositivo para robar información personal, sino ser capaces de acceder a la información de la empresa para la que trabaja.

- El problema: el usuario es uno de los problemas de seguridad más importantes.
- Puede ser que esos dispositivos contengan malware o usen aplicaciones vulnerables.
- Algunas empresas proporcionan smartphones corporativos
 - Los empleados quieren usar las aplicaciones y servicios que usan en su entorno personal

ESCÁNDALO

Multa a LaLiga de fútbol por usar el móvil de 50.000 españoles para espiar

El organismo presidido por Javier Tebas ha anunciado que recurrirá la sanción impuesta por la Agencia Española de Protección de Datos.



El presidente de LaLiga, Javier Tebas. EFE

El Gobierno denuncia que los móviles de Sánchez y Robles fueron espiados con el programa Pegasus

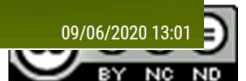
MIGUEL GONZÁLEZ | Madrid

Los atacantes extrajeron 2,6 gigas de datos del teléfono del presidente y nueve megas de la ministra de Defensa. El Ejecutivo no sabe aún cuál es la información robada y su grado de sensibilidad

en Google Play de
que contenía



09/06/2020 13:01



- Seguridad en entornos cloud.
- Blockchain.
- Seguridad en dispositivos móviles y BYOD.
- **APTs.**
- Ciberguerra.
- Protección de infraestructuras críticas.
- 5G.
- IoT/Industria.
- Deepweb.
- IA y ciberseguridad.
- Deepfakes.

- Amenaza Persistente Avanzada (*Advanced Persistent Threat*)
- Conjunto de procesos **sigilosos** con la intención y capacidad de atacar de forma avanzada y **continuada en el tiempo**.
- Son creados por grupos organizados con muchos recursos y con un gran interés en el objetivo. Ejemplos: mafias organizadas, ejércitos, grupos terroristas, grupos activistas... etc.

- El objetivo suele ser tener el control del ordenador de la víctima de forma continuada.
- Algunas características de las APTs son:
 - Persistencia: el software malicioso se suele instalar en varias máquinas para tener esa consistencia en caso de sustitución, formateo o rotura.
 - Sigilo: usan Técnicas de Evasión Avanzadas para evitar ser descubiertos.
 - Suelen evitar ser localizados: tiene la capacidad de ante la duda de detección el malware se borra y se reorganiza en otros equipos.
 - Si es descubierto, su análisis revela la mínima información por medio de código cifrado u ofuscado, borrar la información enviada, no usar comentarios... etc.

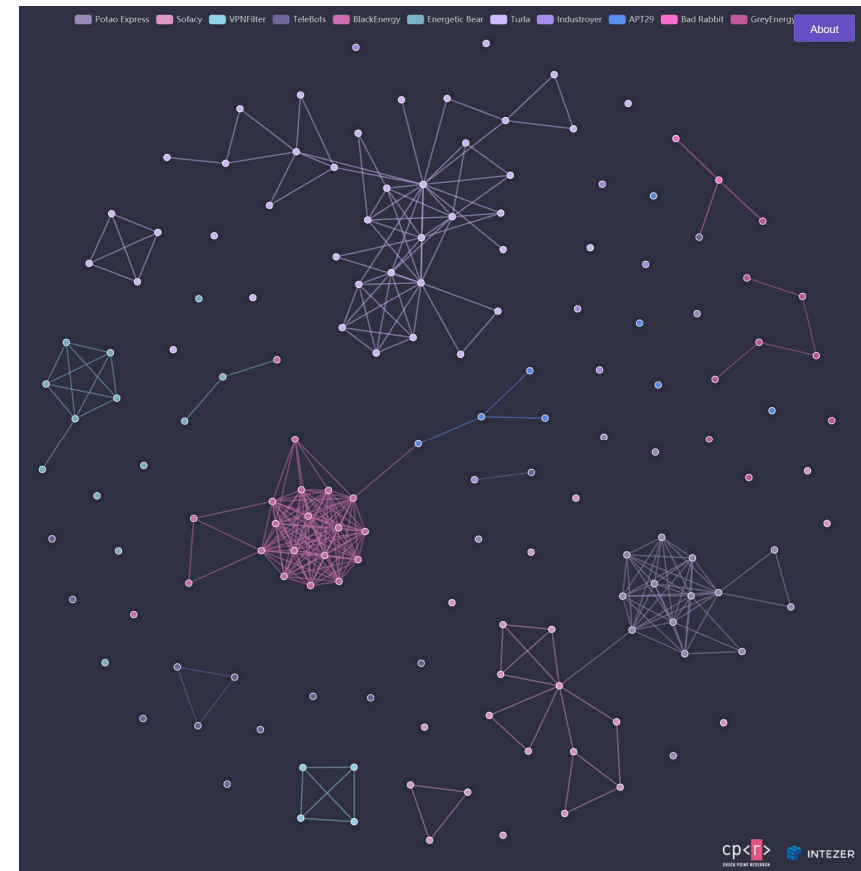
- Hay una gran variedad de grupos que desarrollan APTs, pero una gran cantidad son grupos de China, Rusia e Irán, donde presuntamente son apoyados por los gobiernos.
- Por ejemplo:
 - APT1: supuestamente apoyado por China.
 - TAO (*Tailored Access Operations*): revelada por Snowden y supuestamente apoyada por Estados Unidos.

■ Ejemplos de grupos organizadores de APTs:

■ Rusia:

- APT28: objetivo militar, farmacéutico, financiero...
- APT29: objetivo aeroespacial, defensa, energía...
- DragonFly: objetivo sector energético.
- Black Energy: apagón en Ucrania el 23 de diciembre 2015.

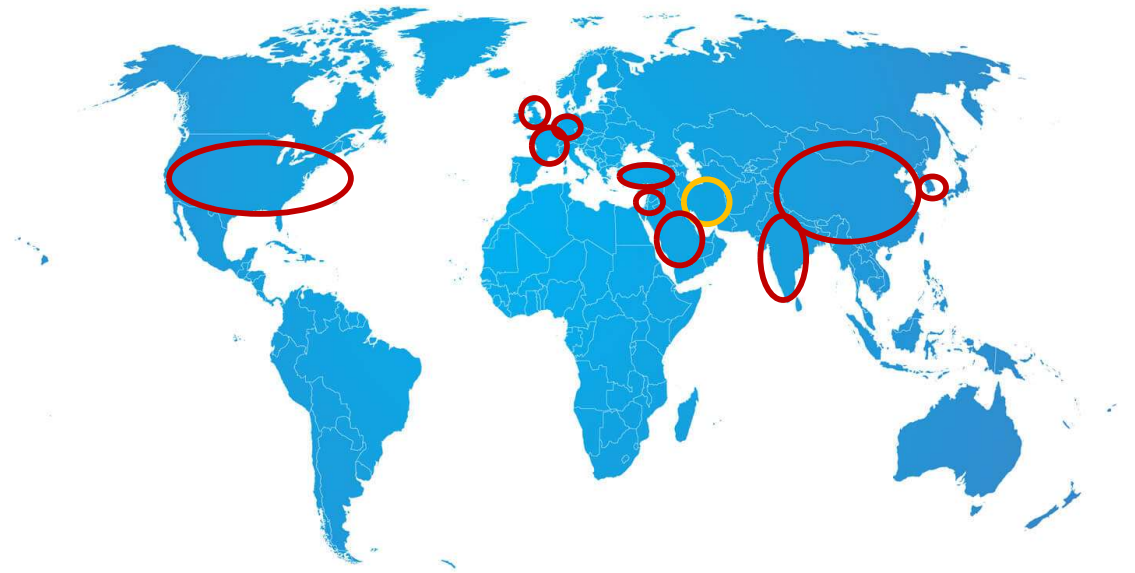
<https://apt-ecosystem.com/russia/map/>



- Ejemplos de grupos organizadores de APTs:

- Irán:

- APT33: ataques contra USA, Corea del Sur, Arabia Saudí, y con objetivos en el sector aeroespacial, petroquímico y defensa.
 - Cleaver: USA, Israel, China, India, Francia, Reino Unido y Arabia Saudí.
 - CopyKittens: USA, Jordania, Turquía, Israel, Arabia Saudí y Alemania.
 - Leafminer: Arabia Saudí, Líbano, Israel y Kuwait.





Careto / The mask.

- Conjunto de troyanos de reconocimiento y robo de datos.
- Monitoriza muchos datos de las operaciones de un sistema, las teclas que se pulsan y la monitorización de red.
- La información se guarda en local, y después se recolecta en un servidor externo.

Careto / The mask

- Es un malware muy modular y cada módulo tiene una función muy particular.
- Tiene una instalación en varias etapas con diferentes pasos intermedios.
- Se descubrieron dos variantes: SGH y Careto.
- Cuando se analizaron los informes, se determinó que el ataque podría estar activo desde el 2007 hasta mediados del 2013.

Careto / The mask

- Los objetivos de careto:
 - Instituciones gubernamentales, cuerpos diplomáticos / embajadas, empresas de energía, petróleo y gas, instituciones de investigación, organizaciones activistas...
- Se detectaron más de 380 víctimas repartidas en 31 países diferentes.

Careto / The mask

- La mayor característica de careto era la complejidad del conjunto de herramientas que podían usar los atacantes:
 - Un malware extremadamente complicado
 - Un rootkit
 - Un bootkit
 - Versiones para Windows 32 y 64
 - Versiones para Mac OS X, Linux, y posiblemente para Android y Apple iOS.

Careto / The mask

- ¿Qué extraía de las víctimas?
 - Interceptaba el tráfico de red.
 - Conversaciones de Skype.
 - Claves PGP.
 - Analiza el tráfico WiFi.
 - Busca toda la información de dispositivos Nokia, Android, iOS.
 - Capturas de pantalla.
 - Recopila archivos del sistema infectado: claves de cifrado, configuraciones VPN, claves SSH, archivos de escritorio remoto, y otros archivos relacionados con herramientas de cifrado a nivel militar / gubernamental.

Careto / The mask

- ¿Quién estaba detrás de Careto?
- No se sabe... pero hay sospechas.
- Las muestras no mostraban información de la localización, pero algunas muestras tenían información de la página de códigos.
- El valor era 0x4E4, cuyo valor decimal es 1252.
- Esta página de códigos la utiliza Microsoft para productos que utilizan el alfabeto latino de Europa occidental.

Careto / The mask

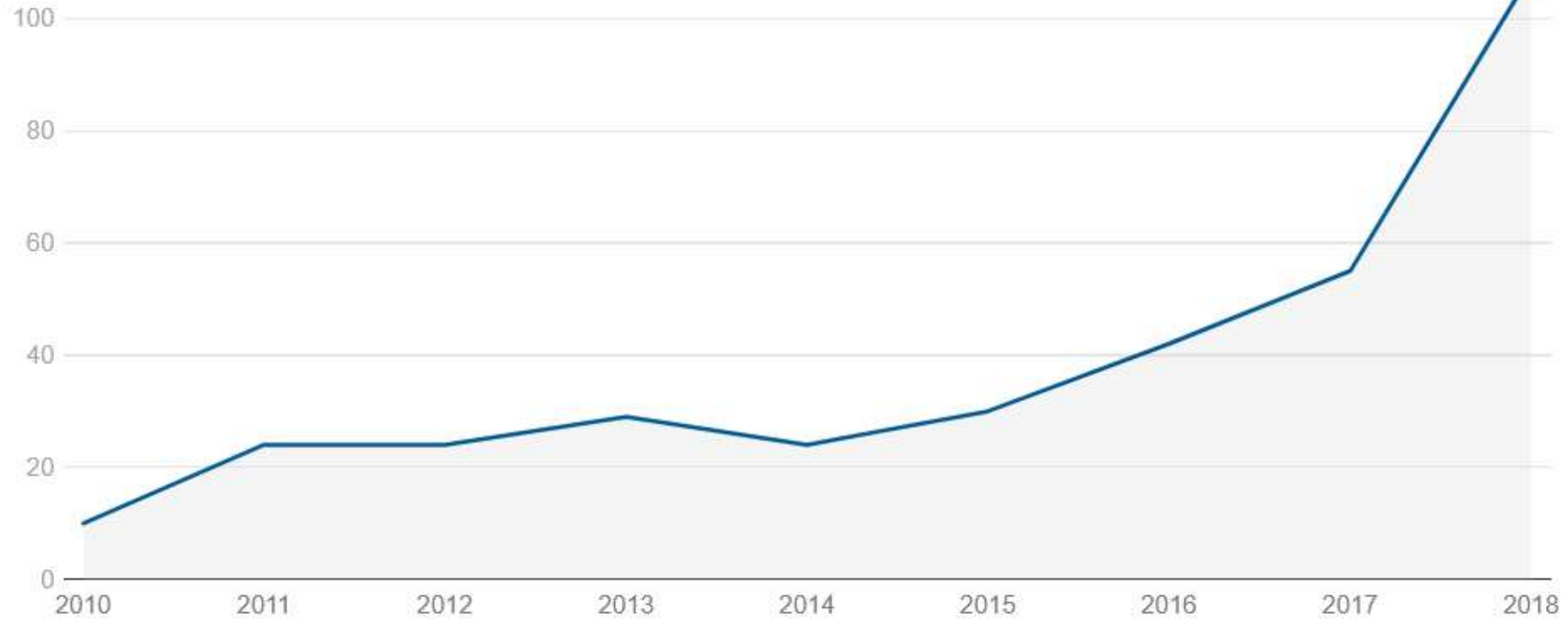
- ¿Quién estaba detrás de Careto?
- Además hay expresiones que hacen pensar que Careto es de origen español:
 - “Careto”
 - La configuración de los datos tenía: “Accept-Language: es Accept-Encoding: gzip”
 - Cuando se debugearon los desinstaladores encontraron paths de los desarrolladores a carpetas llamadas “Pruebas”.
 - Y además encontraron una clave RC4 usada por las comunicaciones command and control.
 - Al descifrarla, la clave en claro era: “*Caguen1aMar*”.



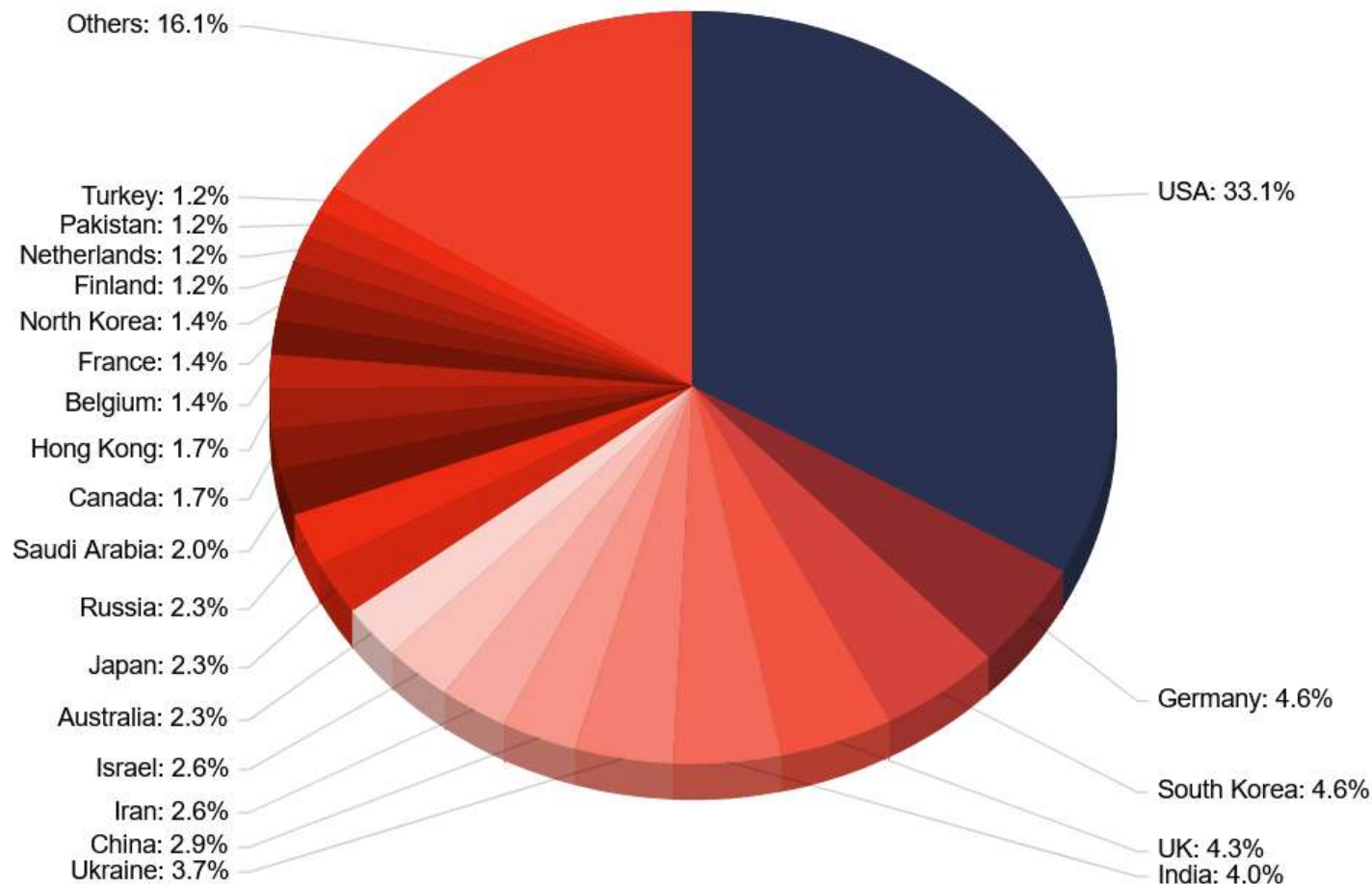
- Seguridad en entornos cloud.
- Blockchain.
- Seguridad en dispositivos móviles y BYOD.
- APTs.
- **Ciberguerra.**
- Protección de infraestructuras críticas.
- 5G.
- IoT/Industria.
- Deepweb.
- IA y ciberseguridad.
- Deepfakes.

- El concepto se refiere al uso de ataques digitales por un país para interrumpir los sistemas informáticos vitales de otro.
- Los ataques informáticos son cada vez más frecuentes en los conflictos internacionales.
- No todos los ciberataques contribuyen a la “ciberguerra”:
 - Sólo se consideran aquellos ataques realizados por grupos que son supuestamente apoyados, o respaldados, por el Estado.

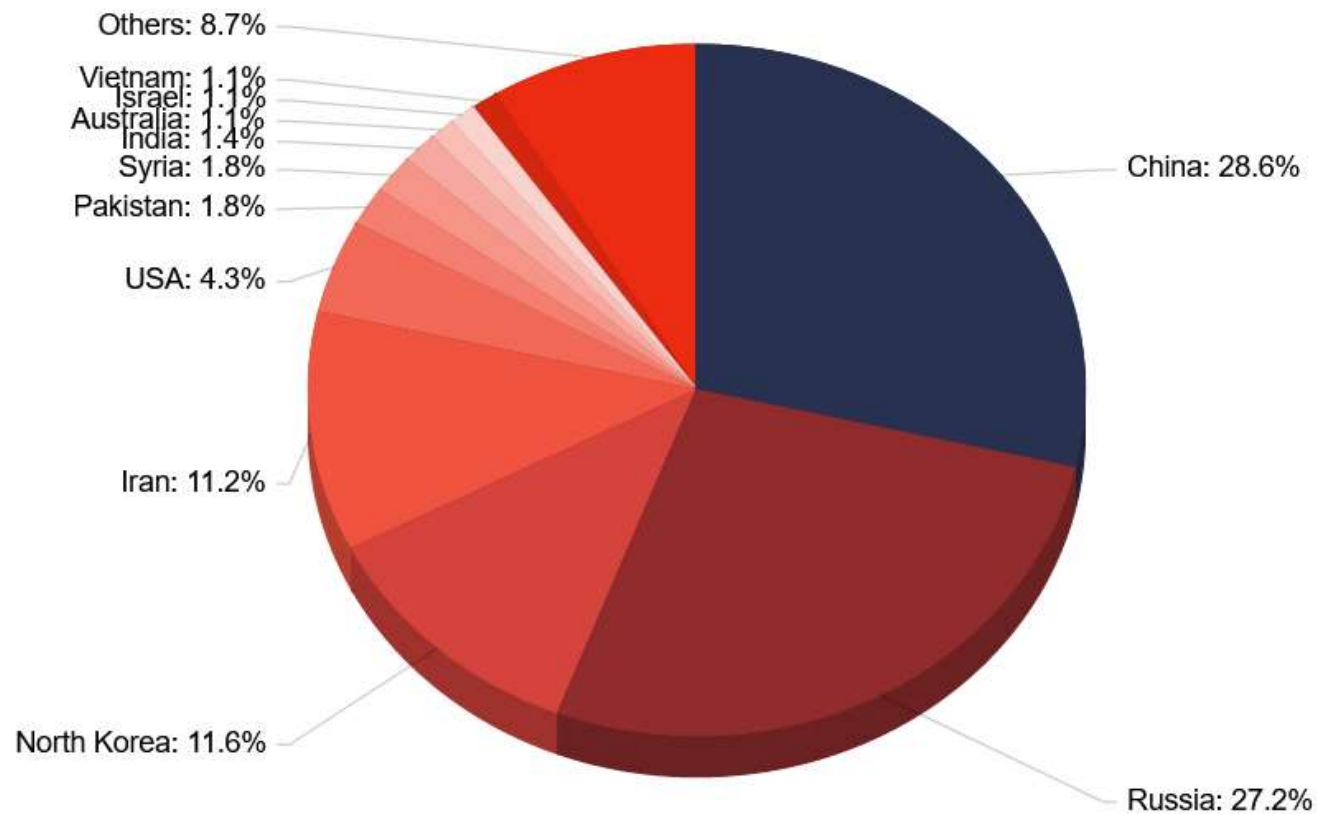
Ciberataques geopolíticos en todo el mundo (2009-2019)



■ Los países más atacados:



■ Origen de esos ataques:



- Usando la ciberguerra los estados son menos “evaluados” por la ciudadanía.
- Invadir un país o iniciar una guerra necesita la aprobación por un Congreso, y además es un acto visible, lo que permitirá a los ciudadanos (y otros países) juzgar ese gobierno.
- En cambio, un ataque cibernético pasa desapercibido ya que no se suele hacer público quiénes son los estados que han participado.

- La financiación para crear un ciberataque es mucho menor que la que se necesita para iniciar una guerra.
- Esto hace que cualquier país (por pequeño que sea) tenga la capacidad de atacar a otro.
- “Solo” se necesita disponer de un grupo de hackers con los conocimientos necesarios y estén dispuestos a ayudar a su país.
- ¿Qué pasaría si un país es capaz de convencer a la ciudadanía para que le preste capacidad de cómputo?

- Seguridad en entornos cloud.
- Blockchain.
- Seguridad en dispositivos móviles y BYOD.
- APTs.
- Ciberguerra.
- **Protección de infraestructuras críticas.**
- 5G.
- IoT/Industria.
- Deepweb.
- IA y ciberseguridad.
- Deepfakes.

- Todos estos ataques se suelen realizar contra infraestructuras críticas.
- Las infraestructuras críticas son aquellas instalaciones, redes, servicios y equipos físicos y de tecnología de la información cuya interrupción o destrucción tendría un impacto en la salud, la seguridad o el bienestar económico de los ciudadanos.
- Todas aquellas infraestructuras cuyos sistemas, medios y servicios son fundamentales para el progreso de la sociedad.

INFRAESTRUCTURAS CRÍTICAS

.....



Energía



Agua



Finanzas



Investigación



TIC



Salud



Energía Nuclear



Administración



Transporte



Química



Alimentación



Telecomunicaciones



- El Centro Nacional de Protección de Infraestructuras y Ciberseguridad (CNPIC): responsable del impulso, coordinación y supervisión de todas las políticas y actividades relacionadas con la protección de las infraestructuras críticas españolas.
- Tres objetivos fundamentales:
 - Prevenir los ataques informáticos contra las infraestructuras de información críticas
 - Reducir la vulnerabilidad nacional a los ciberataques.
 - Reducir al mínimo los daños y el tiempo de recuperación cuando estos ataques se producen.

- Ejemplos de ataques a infraestructuras críticas:
 - 2000 (Australia) – Un empleado, con claves de acceso, tomó el control de la compañía de agua y provocó un vertido de aguas residuales a parques y ríos de la región.
 - 2006 – 2011 (China) – NightDragon realizó una serie de ataques desde China a compañías de Utilities para obtener información sensible y espiar las actividades.
 - 2008 (Polonia) – Un chico de 14 años logró descarrilar 4 trenes.
 - 2015 (Ucrania) – BlackEnergy dejó a toda Ucrania sin luz durante 6 horas, por un ataque a más de 30 plantas eléctricas del país.
 - 2017 (Reino Unido) – WannaCry paralizó el funcionamiento de 16 hospitales, restringiendo el acceso a los historiales médicos.
 - 2021 – *Zeppelin ransomware que atacó el servicio en la nube de ASAC dejó sin servicio al ayuntamiento de Oviedo, Cáceres, Vinaròs, FECYT, el Tribunal de cuentas...*



- Los problemas más frecuentes a los que se enfrenta la protección de infraestructuras críticas son los siguientes:
 - Sistemas desactualizados o sin seguridad alguna.
 - Hardware obsoleto.
 - Falta de talento.
 - Vulnerabilidades y agujeros de seguridad desde el diseño.
 - Falta de preparación y concienciación.
 - Mayor número de ciberataques.
 - Aumento del número de dispositivos conectados.

- Seguridad en entornos cloud.
- Blockchain.
- Seguridad en dispositivos móviles y BYOD.
- APTs.
- Ciberguerra.
- Protección de infraestructuras críticas.
- **5G.**
- IoT/Industria.
- Deepweb.
- IA y ciberseguridad.
- Deepfakes.

- Nueva tecnología móvil.
- Presenta varias ventajas:
 - Velocidad optimizada: de hasta 100 veces mayor que el 4G.
 - Baja latencia.
 - Mayor flexibilidad: permite gestionar mejor los dispositivos conectados al mismo tiempo.
 - Menor consumo: permite la utilización de la tecnología en dispositivos pequeños.

- Aunque es un avance tecnológico supone algunos retos de cara a la seguridad:
 - Aumenta el número de dispositivos → aumenta la exposición a los ataques y tenemos más puntos entrada para los ataques.
 - El 5G tiene una nueva arquitectura cuya característica y las nuevas funcionalidades, ciertos equipos se convierten en nodos “críticos” dentro de la red.
 - Una mayor exposición a los riesgos relacionados con la dependencia de los operadores de redes móviles respecto a los proveedores.

- Se prevé que las redes 5G se conviertan en la espina dorsal de muchas aplicaciones informáticas cruciales.
- Por eso, la integridad y la disponibilidad serán un aspecto clave.
- Además, deberemos prestar mucha atención a los ataques por DDoS.

- Seguridad en entornos cloud.
- Blockchain.
- Seguridad en dispositivos móviles y BYOD.
- APTs.
- Ciberguerra.
- Protección de infraestructuras críticas.
- 5G.
- **IoT/Industria.**
- Deepweb.
- IA y ciberseguridad.
- Deepfakes.

- Está aumentando de manera considerable el número de dispositivos que nos rodean.
- Tanto en el terreno industrial como en el doméstico.
- Un aspecto clave es que los dispositivos funcionan, o se comunican, sin intervención de los usuarios.
- Los sensores recolectan, comunican, analizan y trabajan con la información → nueva forma de crear valor.

- También se crean nuevas oportunidades para comprometer toda esa información.
- No sólo son más datos compartidos entre diferentes dispositivos, sino que los datos pueden ser mucho más sensibles.
- El despliegue de estos sistemas en una gran variedad de dominios conllevan a una gran cantidad de datos e información que puede ser explotada, o utilizada.

Terreno industrial

- Generalmente son sensores que miden o controlan el proceso industrial de una compañía, o fábrica.
- Miden aspectos como la velocidad, presión, temperatura, brazos robóticos, turbinas, ventiladores...
- Un ataque a este sistema podría suponer varias cosas:
 - Que los atacantes tengan control total sobre la cadena de producción, o sobre alguna máquina.
 - Que dispongan de dicha información:
 - Espionaje.
 - Venta de datos.

Ciudades

- Muchos de estos sensores se están instalando en ciudades (*Smart cities*).
- Se incluye en edificios HVAC (*heating, ventilation and air conditioning*), pero también se usan en el transporte público, control del tráfico, o parking inteligentes.
- Tener acceso a estos sistemas pueden ser graves consecuencias:
 - Medios de transporte autónomos.
 - Control del tráfico.



Sistemas Sanitarios

- Las posibilidades del IoT se están empezando a utilizar en centros sanitarios.
- Ejemplos de aplicaciones: cuidado de pacientes, sistemas de diagnóstico remoto, *bio wearables*, monitorización de personas mayores,...
- Al igual que el caso anterior, hay que prestar especial atención a la seguridad dentro de estos entornos.

Hogar


- El hogar es el entorno donde más se está utilizando las tecnologías basadas en IoT (además del sector industrial) y también es el entorno con mayor riesgo.
- Tenemos sensores y dispositivos para controlar el termostato, alarmas, las luces, sistema de alimentación de animales, cámaras de seguridad, puertas, o incluso vehículos eléctricos.

- Una página interesante es shodan:

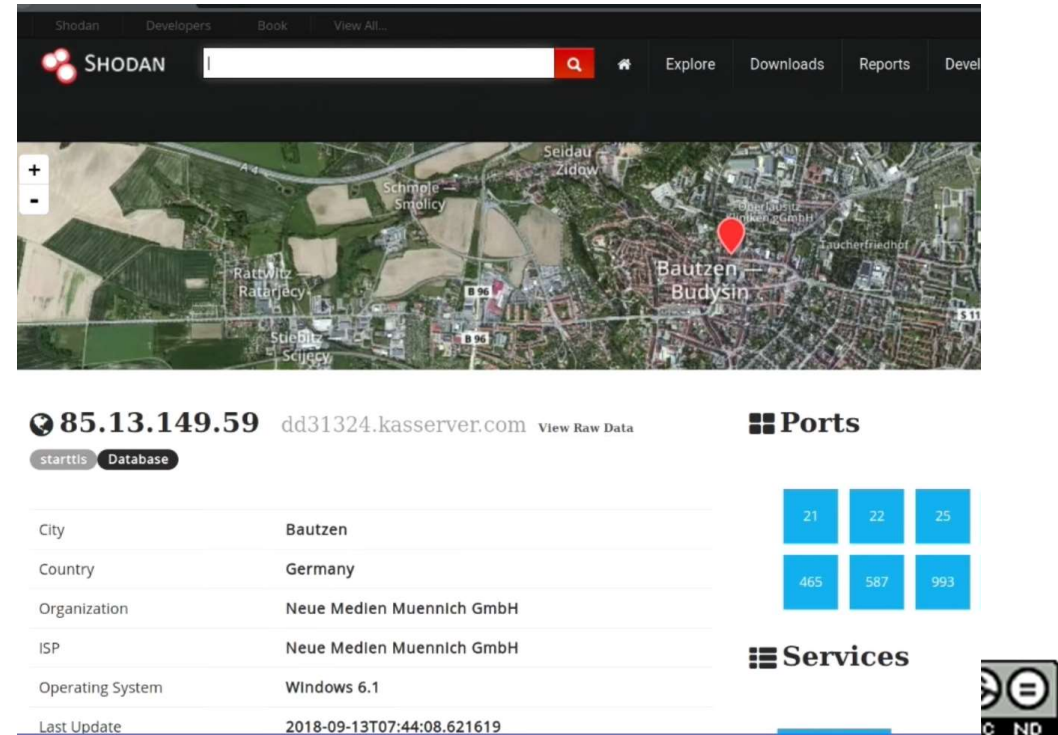
<https://www.shodan.io/>

- Shodan es un motor de búsqueda de sistemas.
 - para localizar todo tipo de dispositivos que estén conectados a internet.
- Es considerado uno de los motores de búsqueda más peligrosos por el tipo de información que podemos recuperar.

- Como cualquier motor de búsqueda tiene distintos dorks.
- Podemos buscar por países, por dispositivo, por sistema operativo, por vulnerabilidad (CVE).
- Por dispositivo específico.
- Y ver la información de la IP.

85.13.149.59
dd31324.kasserver.com
Windows 6.1
Neue Medien Muennich GmbH
Added on 2018-09-13 07:44:08 GMT
 **Germany, Bautzen**
[Details](#)

SMB Status
Authentication: enabled
SMB Version: 1
Capabilities: unicode,large-files,nt-smb,rpc-remote-api,nt-status, itex,unix,extended-security



85.13.149.59 dd31324.kasserver.com [View Raw Data](#)


[starttls](#) [Database](#)

City	Bautzen
Country	Germany
Organization	Neue Medien Muennich GmbH
ISP	Neue Medien Muennich GmbH
Operating System	Windows 6.1
Last Update	2018-09-13T07:44:08.621619

Ports

21	22	25
465	587	993

Services



- Podemos buscar servidores específicos:

52.175.205.43

Microsoft Azure

Added on 2018-09-13 07:57:46 GMT



United States

Details

videogame

cloud

Minecraft Server

Players: 0 online - 10 maximum

Version: 1.12.2 (protocol 340)

Description: Homeslice **Server**

150.95.201.41

v150-95-201-41.a0f7.gtyo1.static.cnode.io

GMO Internet,Inc

Added on 2018-09-13 07:56:38 GMT



Japan

Details

videogame



Minecraft Server

Players: 0 online - 20 maximum

Version: 1.13 (protocol 393)

Description: PIPPI **Server**

- O incluso webcams:

webcamXP 5 
68.231.64.215
985.231.64.215.ph.ph.cox.net
Cox Communications
United States, Tucson

HTTP/1.1 200 OK
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 7327
Cache-control: no-cache, must revalidate
Date: Tue, 03 May 2022 01:51:04 GMT
Expires: Tue, 03 May 2022 01:51:04 GMT
Pragma: no-cache
Server: webcamXP 5

2022-05-03T01:51:06.571607



- Bluescanner:
 - Se utiliza para rastrear dispositivos Bluetooth y extraer información sin tener que emparejarse con el dispositivo.

- Bluesniff:
 - Sirve para rastrear redes Bluetooth ocultas y ataca a los dispositivos vulnerables.

- Seguridad en entornos cloud.
- Blockchain.
- Seguridad en dispositivos móviles y BYOD.
- APTs.
- Ciberguerra.
- Protección de infraestructuras críticas.
- 5G.
- IoT/Industria.
- **Deepweb.**
- IA y ciberseguridad.
- Deepfakes.

- Hay que diferenciar Deep web y dark web.
- En ambos casos son zonas de internet que no están indexadas en ningún buscador.
- La Deep web contiene información que no es accesible de manera pública: páginas normales protegidas por un paywall, archivos guardados de Dropbox o correos electrónicos almacenados en los servidores de los proveedores.
- A la Dark web hay que acceder con un navegador específico: Tor.

- La Dark web se suele utilizar para vender información robada.
- Esto se puede hacer gracias al anonimato de la propia red.
- Además se utilizan criptomonedas por lo que es imposible de rastrear.
- Toda esta información puede ser información personal, pero también información de diferentes empresas.

- Existen foros dedicados al comercio de exploits y vulnerabilidades.
- Según un estudio de Recorded Future el 75% de las vulnerabilidades descubiertas, aparecieron en la dark web antes de publicarse en sitios oficiales.
- También hay páginas donde se debate el desarrollo de exploits, o debates sobre nuevas vulnerabilidades.

- Por último, existen páginas o lugares destinados a empleados descontentos con su empresa.
- El objetivo podría ser realizar actos delictivos
- Podría suponer la fuga de datos sensibles de la propia empresa o el acceso desautorizado a la red interna de la compañía.
- Mucha desinformación → surgen empresas encargadas de monitorizar la dark web.

- Seguridad en entornos cloud.
- Blockchain.
- Seguridad en dispositivos móviles y BYOD.
- APTs.
- Ciberguerra.
- Protección de infraestructuras críticas.
- 5G.
- IoT/Industria.
- Deepweb.
- **IA y ciberseguridad.**
- Deepfakes.

- La Inteligencia Artificial es un elemento clave en cualquier desarrollo software.
- Esto se debe gracias a la gran variedad de aplicaciones que se pueden desarrollar con IA y la gran capacidad de cómputo que tenemos.
- Se prevé que el papel que juega la inteligencia artificial en el mercado de la ciberseguridad pase de 8.800 millones de dólares en 2019 a 38.200 millones de dólares en 2026, con una tasa de crecimiento anual del 23,3%.

- Dentro del área de la ciberseguridad podríamos desarrollar diferentes sistemas basados en IA para realizar diferentes tareas.
- Detección de intrusiones.
- Protección de la privacidad.
- Defensa pro-activa.
- Identificación de comportamientos anómalos.
- Detección de amenazas.

- La IA puede usarse en todas las etapas de una seguridad integral inteligente:
 - Identificación
 - Protección
 - Detección
 - Respuesta
 - Recuperación ante incidentes.

- Pero también la IA se puede utilizar por parte de los atacantes.
- Existen aplicaciones conocer los patrones de comportamiento de usuarios y diseñar campañas comerciales.
- No tiene sentido pensar que los atacantes no usen algo similar para conocer mejor a sus víctimas e identificar el mejor momento para realizar el ataque.
- También se puede usar la IA para desarrollar sistemas relacionados con el ciberterrorismo, ciberespionaje o la ciberguerra.

- Seguridad en entornos cloud.
- Blockchain.
- Seguridad en dispositivos móviles y BYOD.
- APTs.
- Ciberguerra.
- Protección de infraestructuras críticas.
- 5G.
- IoT/Industria.
- Deepweb.
- IA y ciberseguridad.
- **Deepfakes.**

- Son vídeos manipulados para hacer creer a los usuarios que están viendo a una determinada persona realizar declaraciones o acciones que nunca ocurrieron.
- Los deepfakes se utilizan con diversos propósitos:
 - Generación de desinformación.
 - Fake News.
 - Desacreditar a la persona.

- La creación de estos vídeos utilizan técnicas de *Deep learning* y el entrenamiento de arquitecturas de redes neuronales generativas como los autoencoders o las GANs (*generative adversarial networks*).
- Ejemplos de uso:
 - Rogue One: Una historia de Star Wars (2016). Permitieron recuperar a Peter Cushing y a Carrie Fisher.
 - Pornografía.
 - Política.



Few-shot learning (2019, Samsung)

Training frames:



Face landmarks



Learned talking head

Nicromancia digital

- Consiste en revivir a personas que han fallecido por medio de técnicas de deepfakes.

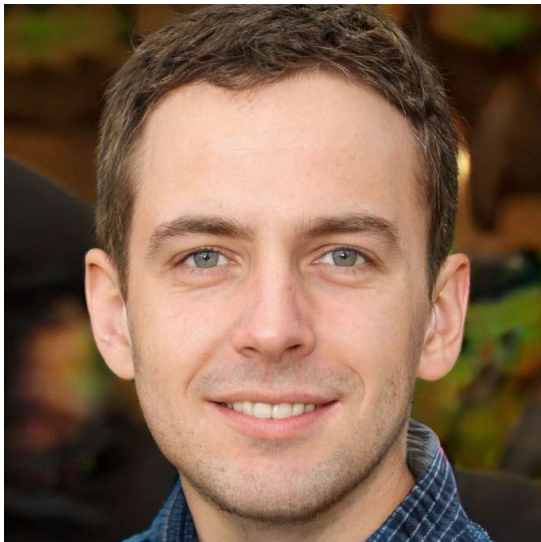
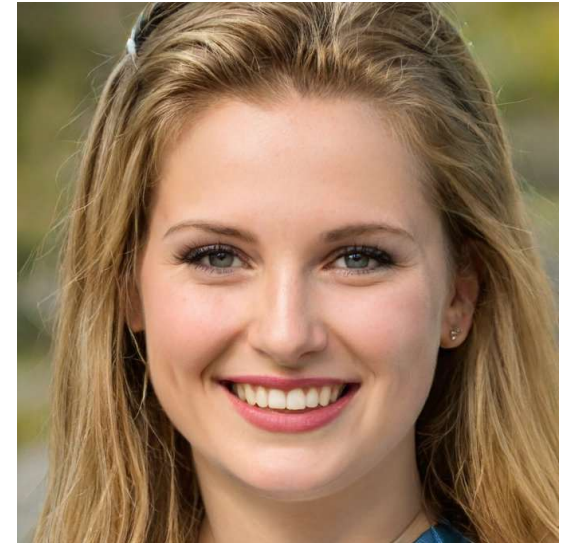


- Algunas cuestiones:
 - ¿Hasta qué punto es moral seguir explotando la imagen pública de una persona que ha fallecido para obtener beneficio y/o entretenimiento de la sociedad?

- En el caso de MyHeritage, ¿estarían de acuerdo estas personas con el uso que se está dando de su imagen?



Deepfakes



- Lo que tienen en común... es que ninguna de estas personas existen.
- Cuenta de twitter: @wedontexistthere
- Web: <https://thispersondoesnotexist.com/>
- Son retratos generados por GANs (Generative Adversarial Networks)

