ESTUDIANTE DE FP HACKEA DGT

Adrián Navarro Barroso
Alberto Moreno Carrero
Alex Carrero Sánchez
Ana Orozco Asensio

TABLA DE CONTENIDOS

1 Introducción

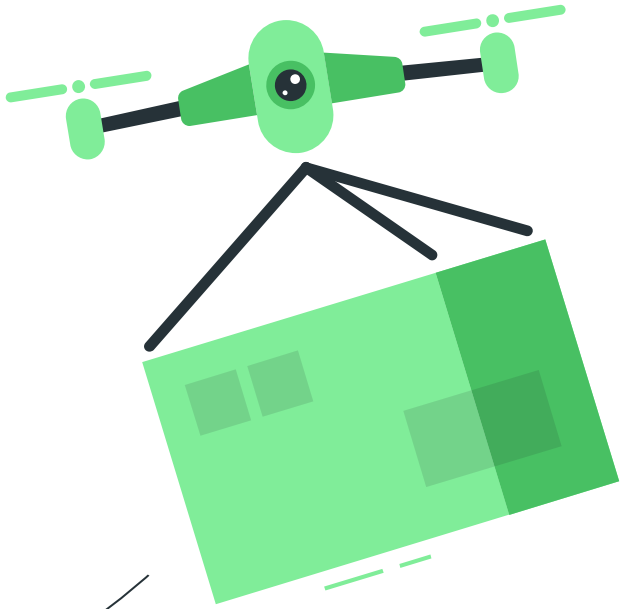
2 Noticia

3 Diccionario

4 Bibliografía

INTRODUCCIÓN

Un poco de historia y enlace de la criptografía con la actualidad.



AVANCES

La **ciberseguridad** es un conjunto de prácticas destinadas a **proteger** sistemas, redes y datos de ataques o accesos no autorizados. La **criptografía** juega un papel fundamental dentro de la ciberseguridad, asegurando el **cifrado** de los datos.

Con el avance de las tecnologías, nuestra dependencia de sistemas informáticos ha aumentado considerablemente, desde teléfonos móviles hasta infraestructuras esenciales como redes eléctricas y sistemas financieros.

Todo esto nos ha permitido realizar actividades comerciales, llevar a cabo transacciones económicas y mejorar la comunicación, entre otras cosas. No obstante, este incremento en la conectividad también ha incrementado la **exposición a diversas amenazas y vulnerabilidades.**

UN POCO DE HISTORIA

A lo largo de la historia la criptografía ha ido evolucionando desde métodos antiguos de cifrado como la ***escítala espartana***, utilizada por Julio César, y continuando con innovaciones más complejas, como la ***máquina Enigma***, que fue clave en las comunicaciones de Alemania durante la Segunda Guerra Mundial.

En los años 90, el aumento de las amenazas cibernéticas impulsó el **desarrollo de software antivirus y firewalls**, y en 2004 Estados Unidos formuló su **primera estrategia nacional** de ciberseguridad.

En 2018, la Unión Europea implementó el ***Reglamento General de Protección de Datos (RGPD)***, estableciendo estándares rigurosos para la protección de datos personales. Este desarrollo **resalta la evolución** de la criptografía y la ciberseguridad, que han avanzado de técnicas simples a tecnologías complejas para **enfrentar las necesidades** de un mundo digitalizado.

LÍNEA DE TIEMPO

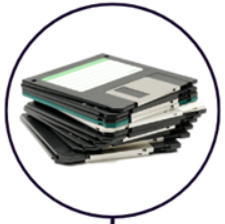
SIGLO IV A.C

ESCÍTALA ESPARTANA

1918

MÁQUINA ENIGMA

DÉCADA DE LOS 90



PRIMEROS FIREWALLS Y ANTIVIRUS

2004

ESTRATEGIA NACIONAL DE CIBERSEGURIDAD EEUU

2018

RGPD

NOTICIA

UCO

Detenidos un estudiante de FP y su cómplice por hackear la DGT, ayuntamientos, bancos, universidades y más de 100 administraciones

Los arrestados compartían identidades como "GUARDIACIVILX" y además atacaron la Red SARA, el eje de la administración digital

SUCESO

Nuevo caso en España de ciberdelitos dirigidos hacia las administraciones públicas. Según datos del CCN-CERT, hasta el 34% de los ciberdelitos en España son dirigidos a estas entidades del sector público. En 2023 las administraciones públicas experimentaron 107.000 ciberataques y solo en los dos primeros meses de 2024 la cifra se eleva a 25.000.

Los ciberataques de este grupo en concreto se cuentan por más de 200 en el periodo de un año.

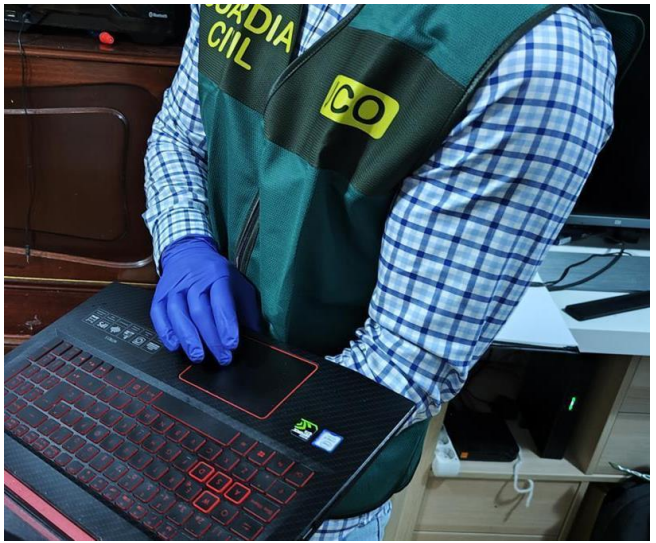
Los ataques se llevaban a cabo con el propósito de robar datos y credenciales para así poder venderlos. El móvil de estos era únicamente sacar dinero.

ATACANTES

Los protagonistas de esta noticia son **2 jóvenes** de 18 y 27 años que llevan haciendo ataques a instituciones públicas y privadas desde **octubre de 2022**. Uno de ellos era muy habilidoso con la **programación** y el otro destacaba en detectar **vulnerabilidades de seguridad**.

Ambos usaban **múltiples identidades** para delinquir, como por ejemplo «GUARDIACIVILX», que es la más conocida o «9bands», «banz9», «TheLich», «Crystal_MSF», «OUJA» o «unlawz», actuando como una sola persona, y compartían tanto los delitos como sus beneficios.

Utilizaban un canal de **Telegram** para promocionar algunos de sus éxitos.



METODOLOGÍA

Su modus operandi era **vender datos** de empresas y particulares en foros utilizados por cibercriminales y en la Dark Web al **mejor postor**, que después usaban para delinquir, propagar malware, secuestrar servidores o pedir rescates de datos a empresas o instituciones para enviar mensajes masivos con los que engañar a sus víctimas y obtener datos confidenciales (Ejemplo: “Bancos Falsos”).

Curiosidad: La UCO comprobó que uno de los dos arrestados había ofrecido vender un ordenador con acceso a la Red SARA y privilegios de administrador a Skull (Alcasec).

AFECTADOS

Ejemplos de entidades atacadas:

- **Red SARA**
- **DGT**:

  Se robaron los siguientes datos de la Dirección General de Tráfico: Nombres y apellidos, fechas de nacimiento, número y fecha del carnet de conducir, DNI, dirección del domicilio, vehículos y detalles (marca, modelos, matricula, nº de bastidor, compañía de seguros...)

- **ITV** Asturias
- **Ayuntamientos**: Sevilla, Zaragoza, Jaén...
- **Sede electrónica del Ministerio de Industria y Turismo**
- **Empresas farmacéuticas**

Más de **100** organismos han sido expuestos.

DICCIONARIO

Recopilación de algunas palabras, organismos o términos que pueden ser confusos o desconocidos.

DISTINTOS ATAQUES

- **Phishing:** Envío de correos electrónicos o mensajes falsos que parecen legítimos para robar credenciales.

- **Malware:** Programas maliciosos como virus, troyanos, ransomware y spyware diseñados para infiltrarse y dañar sistemas, además de robar datos sensibles.

- **Ransomware:** Bloquea el acceso a los datos del sistema, generalmente cifrándolos, y exige un pago (ransom) para liberarlos.

DISTINTOS ATAQUES

- **Ataque fuerza bruta:** Probar múltiples combinaciones de contraseñas o claves hasta encontrar la correcta. Afecta a cuentas protegidas por contraseñas débiles.

- **Man-In-The-Middle (MITM):** Interceptar y manipular la comunicación entre dos partes sin que estas lo sepan, pudiendo robar datos sensibles transmitidos.

- **SQL Injection:** Inyectan código malicioso en una aplicación web a través de una consulta SQL para obtener acceso a la base de datos.

DISTINTOS ATAQUES

- **Session Hijacking:** Los atacantes roban cookies de sesión que permiten autenticarse como otro usuario en sitios web, robando información personal y credenciales.

- **Ataque a la Ingeniería Social:** Los atacantes manipulan psicológicamente a las víctimas para que entreguen información confidencial, sin necesidad de usar software malicioso.

DISTINTOS ATAQUES

- **Keylogging:** Se instala un software que registra todas las pulsaciones de teclas del usuario, permitiendo al atacante capturar contraseñas y otros datos sensibles.

- **Ataque de Denegación de Servicio (DDoS):** Estos ataques sobrecargan un servidor o red con tráfico para interrumpir su funcionamiento. En algunos casos, sirven como distracción para otros tipos de ataques.

ORGANISMOS

- **Red SARA:** conjunto de infraestructuras de comunicaciones y servicios básicos que conecta las redes de las Administraciones Públicas Españolas e instituciones europeas.

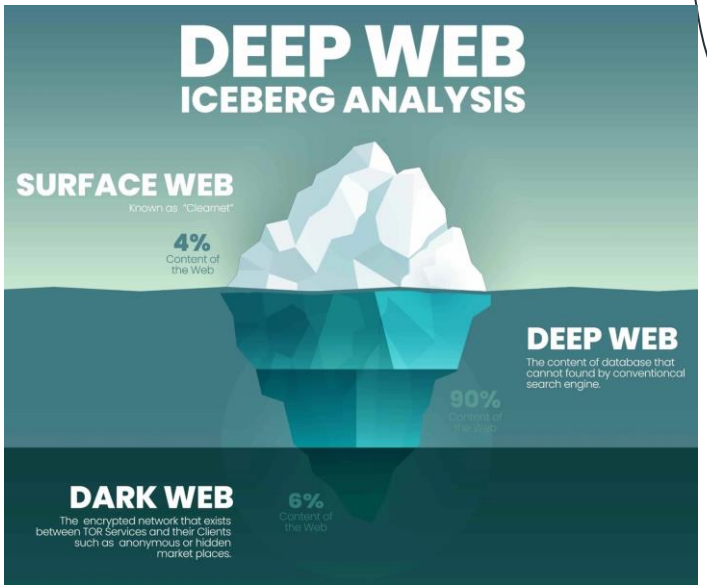
- **Punto Neutro Digital:** Red de servicios que ofrece a los órganos judiciales los datos necesarios en la tramitación judicial mediante accesos directos a aplicaciones y bases de datos del propio Consejo, de organismos de la Administración General del Estado y de otras instituciones.

LA DARK WEB

Es el contenido de la World Wide Web que existe en darknets o redes oscuras, que son redes que se superponen a la internet pública y requieren de software específico y configuraciones o autorización para acceder.

Constituye el 0,1% de la World Wide Web, al contrario que la Deep Web que supone el 90% y alberga contenido oculto sin motivación ilegal.

Suele contener una gran cantidad de contenido ilegal como puede ser la compra/venta de armas y datos, alquileres de sicarios, hackers e incluso páginas de alquileres o venta de personas (con motivos de asesinato y violaciones).



¿QUÉ PODEMOS HACER?

Esta filtración masiva de datos representa un riesgo significativo para la privacidad y la seguridad de los conductores españoles en el caso de los datos robados a la DGT. Las autoridades deben tomar medidas urgentes para proteger a los afectados y prevenir futuros incidentes similares.

En esta ocasión la filtración no son credenciales de usuario y contraseñas del portal de la DGT sino una filtración de la base de datos interna. No hay opción de cambiar contraseña o cerrar la cuenta para dejar de ser vulnerable.

Como se prevé que esos datos puedan acabar en manos de ciberdelincuentes debemos estar alerta ante posibles ciberestafas.

¿QUÉ PODEMOS HACER?

Ejemplos de ciberestafas en España:

- Correos que parecen provenir de bancos como BBVA o Caixabank, solicitando que el usuario actualice sus datos a través de un enlace falso.
- Ofertas demasiado buenas para ser ciertas en productos como smartphones, videojuegos o entradas para eventos.
- Un comprador dice haber enviado el dinero pero el vendedor nunca lo recibe; o se utiliza un supuesto servicio de transporte o pago que resulta ser fraudulento.
- Esquemas Ponzi o piramidales donde prometen inversiones en criptomonedas con ganancias inmediatas, que luego desaparecen con el dinero.

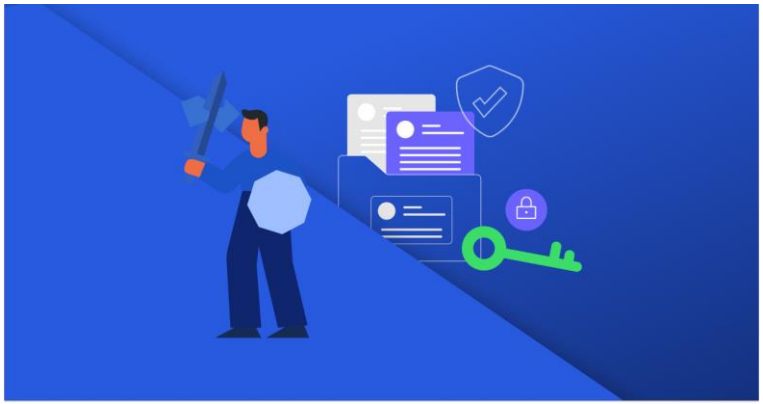
¿QUÉ PODEMOS HACER?

Ejemplos de ciberestafas en España:

- Mensajes falsos de Correos o DHL indicando que hay un paquete pendiente de entrega y que se necesita pagar una pequeña cantidad para liberarlo.
- Ofertas de trabajo como "mistery shopper" o trabajo desde casa que resultan ser falsas y tienen como fin obtener datos bancarios o cobrar una tarifa de inscripción.

¿QUÉ PODEMOS HACER?

Para evitar caer en este tipo de ciberestafas, es fundamental desconfiar de correos, SMS o llamadas inesperadas que soliciten datos personales o financieros, verificar siempre la autenticidad de las webs y anuncios, y utilizar herramientas de seguridad como antivirus y contraseñas seguras.



CONCLUSIÓN

La ciberseguridad no solo implica la implementación de medidas técnicas y herramientas de protección, sino también la **concienciación y educación** de usuarios y organizaciones para **reconocer y prevenir amenazas**.

Es importante que tanto los gobiernos como las empresas adopten un enfoque proactivo para **proteger sus sistemas y datos**, desarrollando políticas robustas, realizando auditorías de seguridad y fomentando **una cultura de ciberseguridad.**

Solo a través de una colaboración efectiva y la innovación constante se podrá mitigar el riesgo de la ciberdelincuencia y **asegurar un entorno digital más seguro** para todos.

BIBLIOGRAFÍA

- https://www.elconfidencial.com/tecnologia/2024-06-28/hackers-ciberseguridad-robo-datos-dgt-itv-guardia-civil_3912381/
- https://www.abc.es/espana/andalucia/malaga/dos-detenidos-asturias-sevilla-centenar-ciberataques-organismos-20240628105755-nts.html?ref=https%3A%2F%2Fwww.google.com%2F
- Véliz, C. (2021). *Privacidad es poder: datos, vigilancia y libertad en la era digital.* Debate
- https://es.euronews.com/my-europe/2024/06/01/que-datos-tuyos-tienen-los-hackers-de-la-dgt-tras-la-filtracion-de-345-millones-de-usuario
- https://www.elmundo.es/papel/2023/04/03/642a6bd9fc6c83fc678b456d.html