CIBERINTELIGENCIA Y EVALUACIÓN DE RIESGOS FRENTE A AMENAZAS PERSISTENTES AVANZADAS EN EL ENTORNO CORPORATIVO

Daniel Blanco Aranda

16 DE MAYO DE 2025

GOODJOB

BLANCO ARANDA DANIEL - 31008342H

Firmado digitalmente por BLANCO ARANDA DANIEL - 31008342H
Fecha: 2025.05.16 18:00:32 +02'00'

Contenido

Marco introductorio 4
Módulo 1 Estrategia 5
Introducción 5
Información Relevante sobre la empresa 5
Activos principales 6
Organigrama 7
Estrategia 8
Inventario de amenazas 8
Matriz de riesgos (valoración) 9
Análisis de inteligencia/OSINT 11
Objetivos del análisis OSINT 11
Fuentes utilizadas: 11
Ejemplo aplicado a SUPERTECH: 11
Módulo 2 Inteligencia de Amenazas. 12
Identificación del actor 12
Posibles Actores de Amenazas. 13
APT34(OILRIG) 13
APT35(Mint-Sandstorm) 14
APT44(Sandworm) 15
Comparativa Estratégica de Grupos APT: Perfil de Capacidades Cibernéticas 16
Perfil de Atracción de SUPERTECH S.A. para Grupos APT Elegidos 17
Probabilidad del ataque por APTs 18
Conclusión del APT atacante 19
Estudio de APT44 19
Ataques conocidos y TTPs 20
Evolución y sofisticación del grupo 22
Contexto geopolítico 22
Perspectivas futuras 22
Medidas a tomar contra APT44. 23
Conclusión Módulo 2 24
Módulo 3 EJERCICIOS ESPECÍFICOS 25

Mapa de riesgos 25
Investigación OSINT de un activo expuesto 27
Identificación del activo 27
Objetivo del análisis 27
Fuentes y herramientas utilizadas 27
Resultados obtenidos 28
Resumen de la búsqueda 30
Simulación de ataque dirigido 31
Medidas defensivas frente al ataque simulado 32
Hacking 33
Ejercicio 1 33
Ejercicio 2 35
Ejercicio 3 37
Conclusión del TFC. 40
Bibliografía 41
Anexos 42
Anexo 1 Uso de IA en el desarrollo del TFC 42
Anexo 2 Glosario de términos 43
Anexo 3: Herramientas utilizadas en retos 43

Ilustración 1-Organigrama de SUPERTECH 7
Ilustración 2-Mapa de calor de nivel de riesgo 10
Ilustración 3-Gráfica de radar entre APTs 16
Ilustración 4-Gráfica de atracción hacia SUPERTECH 17
Ilustración 5-Mapa de influencia APT44 21
Ilustración 6-Matriz de riesgos con datos de Módulo 1 y 2 26
Ilustración 7-Captura de reto 1, se muestra la ejecución del comando exiftool 34
Ilustración 8-Captura de reto 1, se muestra la ejecución del comando exiftool 34
Ilustración 9-Captura de reto 1, se muestra la ejecución del comando pdfimages 34

Ilustración 10-Captura de reto 1, se muestra la ejecución del comando mutool..... 34
Ilustración 11-Captura 1 Ejercicio 2, Wireshark..... 36
Ilustración 12-Captura 2 Ejercicio 2, Registro de Wireshark 36
Ilustración 13-Captura 3 Ejercicio 2, Registro de Wireshark 36
Ilustración 14-Captura 4 Ejercicio 2, Información de Registro de Wireshark..... 36
Ilustración 15-Captura 1 Ejercicio 3 Ejecución comando strings..... 38
Ilustración 16-Captura 2 Ejercicio 3, Ejecución de comando r2, con solución de reto.. 38

Marco introductorio

En este proyecto se recogerán 3 módulos relacionados con el entorno de la ciberseguridad.

- Módulo 1, se pondrá en juego una empresa ficticia puntera en el sector, se hará un documento de estado y se evaluarán los objetivos, líneas de negocio, posibles vulnerabilidades y soluciones a estas y otros aspectos necesarios en el sector.
- Módulo 2, en este apartado se hará un estudio de distintos actores de amenazas (APTs) y se intentará identificar cual podría ser el más propenso a atacar nuestra empresa y evaluar las medidas para evaluar el ataque.
- Módulo 3, en este apartado se llevarán a cabo ejercicios prácticos específicos con el objetivo de aplicar los conocimientos teóricos adquiridos en los módulos anteriores. También se investigará y se evaluará el grado de exposición de un activo importante de nuestra empresa con el objetivo de evitar que este mismo pueda ser atacado.

Módulo 1 Estrategia

Introducción

En este módulo se elaborará un plan de gobierno de seguridad para la organización SUPERTECH S.A., con sede principal en Madrid, dedicada a servicios de tecnología y ciberseguridad para clientes muy importantes en el sector.

Información Relevante sobre la empresa

Sus principales líneas de negocios son:

- Servicios de hacking y revisiones de seguridad.
- Servicios de INTeligencia.
- Servicios de fortificación y aseguramiento de empresas.

El principal objetivo corporativo es la obtención de ingresos mediante la prestación de servicios de ciberseguridad de alta calidad.

Sus clientes son bancos, aseguradoras, particulares con grandes fortunas, gobiernos, agencias de inteligencia.

La empresa posee un desarrollo tecnológico consolidado, sustentado en inversiones estratégicas en tecnologías emergentes como:

- Blockchain
- IA
- Criptomonedas

La compañía presenta una facturación anual aproximada de 2.000 millones de euros, con unos costes operativos que rondan los 980 millones de euros.

Activos principales

En SUPERTECH S.A., los objetivos principales son:

Infraestructura tecnológica y datos sensibles

Este activo incluye servidores, redes, bases de datos y sistemas que soportan los servicios hacking y de inteligencia.

Mantener la confidencialidad, integridad y disponibilidad de esta infraestructura es vital para la seguridad y confianza de los cliente.

Capital humano especializado

El equipo humano conformado por expertos en ciberseguridad, analistas y desarrolladores representan un activo estratégico.

Su conocimiento y habilidades permiten desarrollar tecnologías avanzadas y brindar servicios de calidad, siendo clave para la innovación y respuesta efectiva frente a amenazas.

Organigrama

Organizada en tres puntos geográficos: Barcelona, Madrid y Dubái.

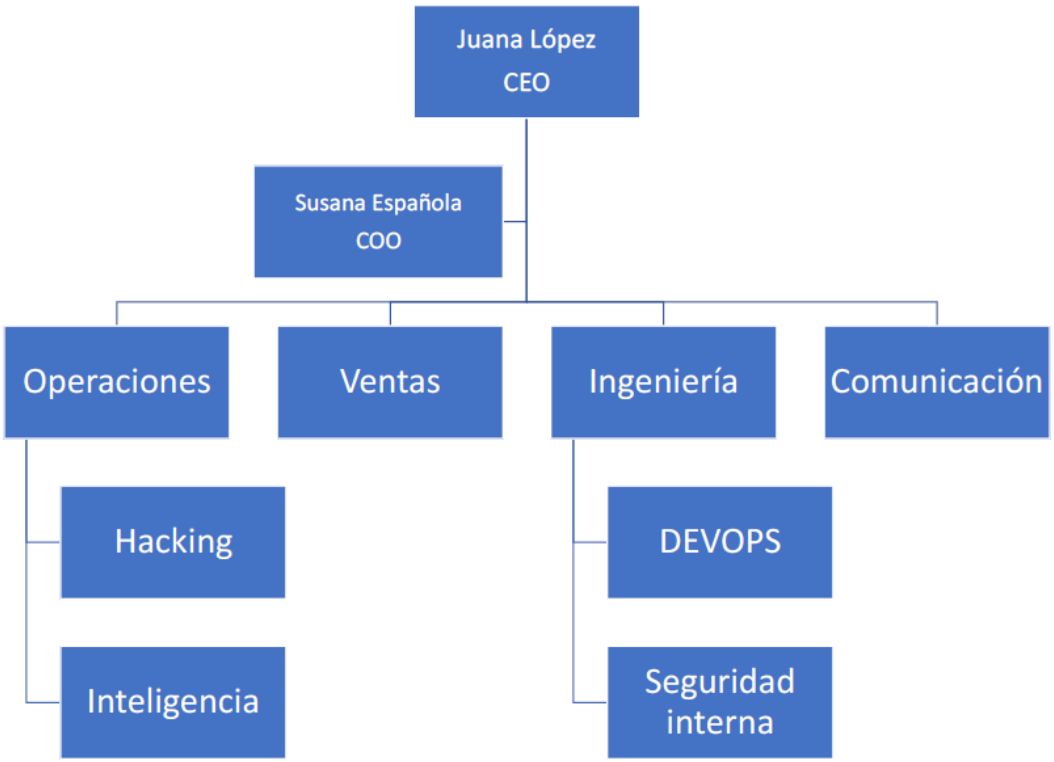

Ilustración 1-Organigrama de SUPERTECH

La ilustración presenta un organigrama en el que se indica que el cargo de CEO (Directora General) está ocupado por Juana López

Estrategia

A continuación, se presenta un resumen del inventario de amenazas y de la matriz de riesgos identificados para la organización:

Inventario de amenazas

Se han identificado cinco amenazas relevantes para SUPERTECH S.A., en función de su actividad, perfil de clientes y tecnologías empleadas.

N.º	Amenazas identificadas	Descripción Breves
1	APTs	Ciberataques prolongados y dirigidos, ejecutados por actores con recursos y motivación estratégica.
2	Fuga de información	Exfiltración de datos por malware o acciones internas
3	Vulnerabilidades en tecnologías emergentes	Fallos en IA, blockchain o criptomonedas aún sin madurez normativa/técnica.
4	Ataques DDoS	Inundación de tráfico que puede afectar la disponibilidad de los servicios.
5	Ingeniería social y phishing	Ataques enfocados en el personal con el fin de sustraer credenciales o desplegar software malicioso.

Matriz de riesgos (valoración)

A continuación, se valoran los 10 riesgos principales, considerando:

- **Probabilidad (P)**: Baja (1), Media (2), Alta (3)
- **Impacto (I)**: Bajo (1), Medio (2), Alto (3)
- **Nivel de riesgo (R)**: P x I

Nº	Riesgo Identificado	P	I	R	Nivel
1	Pérdida de datos sensibles (clientes/infraestructura)	3	3	9	Alto
2	Compromiso de sistemas por vulnerabilidad en IA o blockchain	2	3	6	Medio
3	Ataques dirigidos a ejecutivos (spear phishing)	2	3	6	Medio
4	DDoS afectando servicios de clientes críticos	3	2	6	Medio
5	Acceso no autorizado por errores en configuraciones	2	2	4	Bajo
6	Empleados descontentos con acceso privilegiados	2	3	6	Medio
7	Brecha reputacional por filtración de datos	2	3	6	Medio
8	Uso indebido de herramientas de hacking	2	2	4	Bajo
9	Ataques a la cadena de suministro	1	3	3	Bajo
10	Incumplimiento normativo (RGPD,etc.)	2	3	6	Medio

Aquí se expone un mapa de calor de riesgos dentro de nuestra empresa.

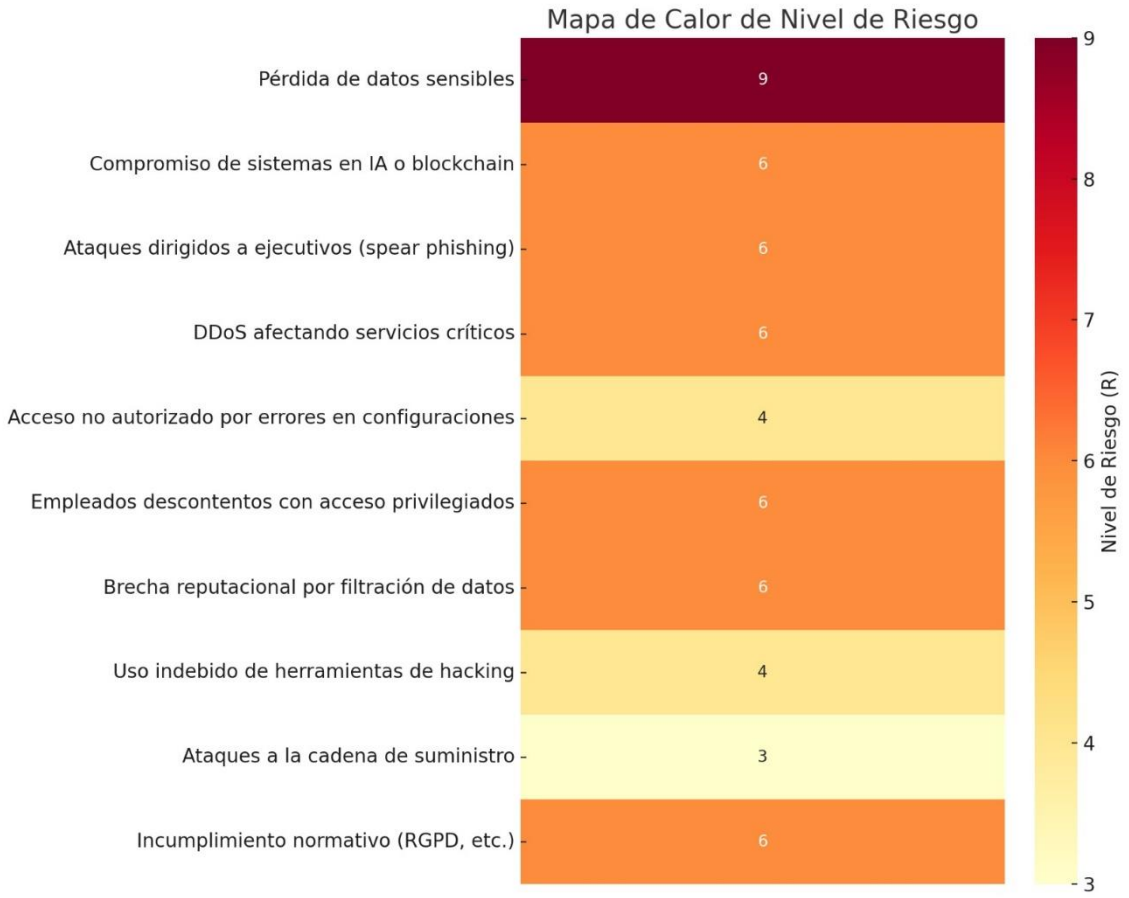

Ilustración 2-Mapa de calor de nivel de riesgo

Análisis de inteligencia/OSINT

La búsqueda de información y fuentes externas (OSINT) ayudará a la empresa a anticiparse a estar al tanto de la información pública y semipública.

Este proceso resulta fundamental para identificar actores hostiles, patrones de ataque y posibles filtraciones de información que puedan impactar tanto a la organización como a sus clientes.

Objetivos del análisis OSINT

- Identificar posibles campañas de phishing dirigidas a empleados o altos cargos.
- Detectar filtraciones de datos en foros, pastebins o dark web.
- Monitorear menciones a SUPERTECH S.A. o sus servicios en redes sociales y medios especializados.
- Analizar perfiles de grupos APT y ciberdelincuentes que operan en sectores financieros y tecnológicos.

Fuentes utilizadas:

- Motores OSINT como **Shodan**, **Censys**, **HaveIBeenPwned**, **Recon-ng**.
- Plataformas de inteligencia como **ThreatFox**, **VirusTotal**, **AlienVault OTX**.
- Foros y marketplaces del **darknet** (vigilancia pasiva mediante herramientas).
- Redes sociales (X, LinkedIn) y servicios de alerta.

Ejemplo aplicado a SUPERTECH:

Durante el análisis, se descubrió una posible filtración de correos corporativos vinculados a empleados de ingeniería en *HaveIBeenPwned*. También se identificaron menciones a la empresa en foros de hacking que ofrecían accesos RDP posiblemente asociados a terceros proveedores con permisos internos.

Esta información será útil para:

- Activar procesos de respuesta ante incidentes.
- Fortalecer las autenticaciones y políticas de acceso.
- Reforzar la protección a través de ejercicios de concienciación.

Módulo 2 Inteligencia de Amenazas.

Este módulo se focaliza en el análisis de un actor de amenaza concreto, potencialmente un grupo **APT,** que pudiera atacar a nuestra empresa. El análisis se hará mediante técnicas de inteligencia.

Los grupos **APT** son grupos de ciberdelincuentes altamente sofisticados que llevan a cabo ataques cibernéticos **prolongados** y **dirigidos**, con el objetivo de sustraer información confidencial o interrumpir operaciones críticas

Analizaremos una serie de adversarios con el objetivo de identificar al actor principal, realizando un estudio exhaustivo de sus TTPs (Tácticas, Técnicas y Procedimientos), características y posibles contramedidas

Identificación del actor

Una vez confirmada el actor de amenaza, el primer paso sería recopilar toda la información posible que nos ayude a reconocerlo de manera efectiva.

Esto incluye el origen, sus motivaciones, su historial de ataques, objetivos habituales, y patrones identificables de comportamiento.

Se procederá a un análisis comparativo de diversos grupos APT que podrían representar una amenaza potencial para la organización.

Posibles Actores de Amenazas.

APT34(OILRIG)

Aspecto	Descripción
Procedencia	Irán. Vinculado al Ministerio de Inteligencia y Seguridad de Irán (MOIS).
Motivaciones	Ciberespionaje, vigilancia y obtención de información estratégica regional.
Ataques conocidos	- Ataques a sectores financieros y de telecomunicaciones en Oriente Medio. - Compromiso de redes gubernamentales y petroleras.
TTPs destacadas	- Phishing dirigido y uso de macros maliciosas. - Creación de dominios falsos para campañas de ingeniería social. - Acceso remoto y movimiento lateral.
Herramientas comunes	POWBAT, BondUpdater, ValueVault, múltiples scripts PowerShell personalizados.
Técnicas MITRE ATT&CK	T1566.001 (spearphishing), T1059.001 (PowerShell), T1071.001 (C2 sobre HTTP), T1082 (descubrimiento de sistema).
Tipo de objetivos	Empresas de telecomunicaciones, energía, gobiernos y entidades diplomáticas en Oriente Medio y Asia Central.

APT35(Mint-Sandstorm)

Aspecto	Descripción
Procedencia	Irán. Conexiones con el IRGC (Cuerpo de la Guardia Revolucionaria Islámica).
Motivaciones	Propaganda, ciberespionaje, robo de credenciales y operaciones de influencia.
Ataques conocidos	- Campaña de spearphishing contra disidentes, ONGs y sectores académicos. - Uso de dominios falsos y correos con temas políticos o de investigación.
TTPs destacadas	- Envío de correos maliciosos con enlaces falsos. - Uso de credenciales robadas para acceso a correos institucionales. - Recolección y exfiltración de datos personales.
Herramientas comunes	Charming Kitten Malware, PowerShell-based backdoors, herramientas personalizadas de vigilancia.
Técnicas MITRE ATT&CK	T1566.002 (phishing con enlaces), T1059.001 (PowerShell), T1041 (exfiltración), T1203 (explotación de cliente).
Tipo de objetivos	Periodistas, investigadores, ONGs, defensores de derechos humanos, y sectores académico y gubernamental.

APT44(Sandworm)

Aspecto	**Descripción**
Procedencia	Rusia. Asociado a la Dirección Principal del Estado Mayor de las Fuerzas Armadas de la Federación de Rusia (GRU).
Motivaciones	Ciberataques con fines militares, políticos y de desestabilización. Sabotaje y guerra de información.
Ataques conocidos	- Ataque a la red eléctrica de Ucrania (2015, 2016). - NotPetya (2017), considerado uno de los ciberataques más destructivos. - Ataques a los Juegos Olímpicos de Invierno 2018.
TTPs destacadas	- Despliegue de wipers como NotPetya. - Uso de exploits de día cero. - Movimientos laterales rápidos y destrucción de infraestructura crítica.
Herramientas comunes	BlackEnergy, Industroyer, NotPetya, KillDisk, GreyEnergy.
Técnicas MITRE ATT&CK	T1485 (destrucción de datos), T1027 (ofuscación), T1210 (explotación de servicios remotos), T1046 (descubrimiento de red), T1569.002 (Ejecución remota).
Tipo de objetivos	Infraestructura crítica, gobiernos, energía, transporte, organizaciones internacionales, especialmente en Europa y EE.UU.

Comparativa Estratégica de Grupos APT: Perfil de Capacidades Cibernéticas

Esta gráfica de radar compara los tres grupos **APT** estudiados: **APT34 (OilRig)** de Irán, **APT35 (Mint-Sandstorm)** de Irán y **APT44 (Sandworm)** de Rusia.

La comparación se basa en cinco aspectos clave de sus operaciones cibernéticas: su nivel de destructividad, la variedad de objetivos que atacan, el nivel técnico de sus herramientas, su capacidad de mantenerse dentro de sistemas comprometidos (persistencia), y las técnicas que usan para ocultarse y evadir detección.

La imagen ayuda a ver las fortalezas de cada grupo: APT44 se destaca por ser el más destructivo y técnicamente avanzado, APT35 tiene buena persistencia y evasión, mientras que APT34 muestra un enfoque más equilibrado, aunque con menor sofisticación técnica.

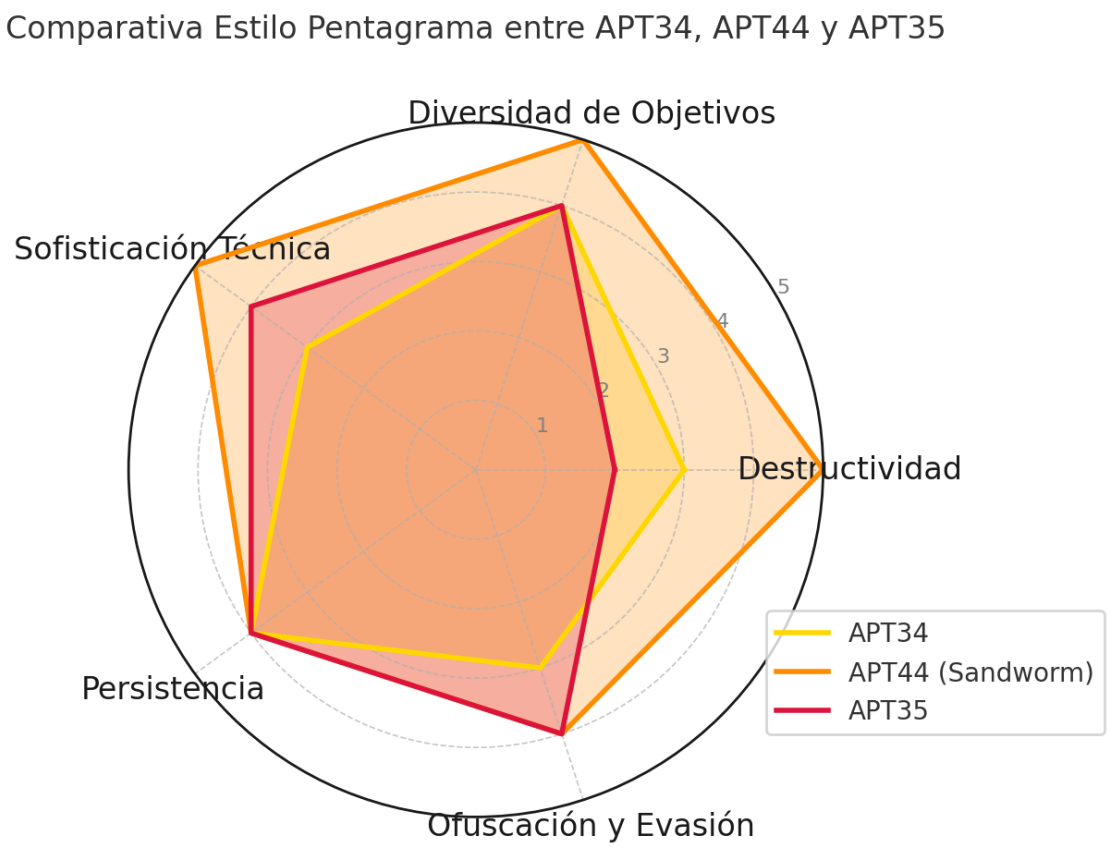

Ilustración 3-Gráfica de radar entre APTs

Perfil de Atracción de SUPERTECH S.A. para Grupos APT Elegidos

La gráfica ilustra cómo las principales características de SUPERTECH S.A.—como su elevada facturación, su apuesta por tecnologías avanzadas (IA, blockchain) y su ubicación estratégica en España (Unión Europea)—la convierten en un objetivo particularmente atractivo para **APT44 (Rusia)**.

Este grupo, impulsado por motivaciones geopolíticas y económicas, posee un historial de ataques a entidades críticas en Europa, lo que lo posiciona como la mayor amenaza.

Le sigue **APT34 (Irán)**, que presenta un interés considerable debido al perfil sensible de los clientes de SUPERTECH (bancos, gobiernos), aunque con un enfoque más técnico. En tercer lugar, se encuentra **APT35 (Irán)**, cuyo interés es más moderado, centrado en campañas de espionaje y desinformación, y menos enfocado en la obtención de tecnología avanzada.

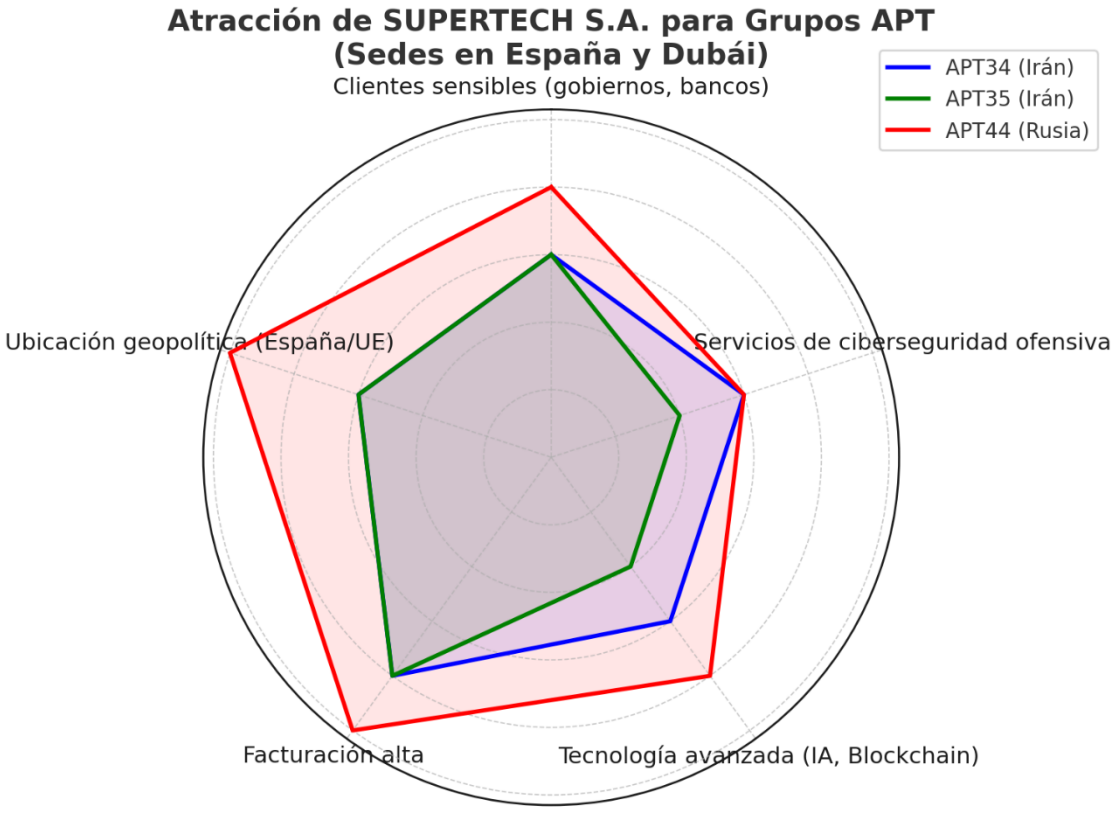

Ilustración 4-Gráfica de atracción hacia SUPERTECH

Probabilidad del ataque por APTs

Este apartado expone la probabilidad estimada de ataque por parte de los tres grupos APT analizados

APT44 (Rusia) – Mayor probabilidad de ataque

- **Motivación geopolítica y estratégica:** Rusia considera a empresas de ciberseguridad de países de la OTAN y la UE como objetivos prioritarios.
- **Enfoque en infraestructuras críticas y tecnología avanzada:** SUPERTECH maneja clientes gubernamentales, bancos y tecnologías como IA y blockchain, todos blancos típicos para APT44.
- **Alta capacidad técnica y operativa**: Tiene los recursos, experiencia y antecedentes para comprometer objetivos complejos como SUPERTECH.
- **Ubicación del objetivo:** La sede en Madrid (UE/OTAN) aumenta significativamente el atractivo para Rusia por razones de ciberespionaje estatal y desestabilización**.**

APT34 (Irán) – Moderada probabilidad-

Aunque tiene interés en el espionaje corporativo, generalmente su alcance es más local o enfocado en sectores energéticos y diplomáticos. Podría estar interesado en los clientes de SUPERTECH, pero sus motivaciones y capacidades son más limitadas en comparación con APT44.

APT35 (Irán) – Baja probabilidad

Este grupo se centra en campañas de desinformación, manipulación social y vigilancia de disidentes. Por ello, su perfil no encaja directamente con el entorno tecnológico y financiero de SUPERTECH.

Como resultado del análisis de probabilidad de ataque por **APTs**, se ha determinado que el grupo que representa el mayor riesgo para SUPERTECH S.A. es **APT44**(Sandworm). Esto se debe a su avanzada capacidad técnica, sus motivaciones geopolíticas, su enfoque en objetivos estratégicos y el interés que genera la ubicación y el perfil tecnológico de la empresa. Por ello, debe ser considerado la principal amenaza en materia de ciberseguridad.

Conclusión del APT atacante

Basándonos en el estudio realizado y en el análisis efectuado sobre SUPERTECH S.A., así como en las motivaciones de los distintos grupos APT, se concluye que el grupo con mayor probabilidad de atacar a nuestra empresa es **APT44 (Sandworm)**.

Estudio de APT44

APT 44 (Sandworm) es un grupo de ciberatacantes respaldado por la inteligencia militar rusa (GRU), específicamente la Unidad 74455. Activo desde al menos 2009, se especializa en ataques destructivos y de espionaje, y ha sido vinculado a operaciones como el apagón en Ucrania (2015), el malware NotPetya (2017) y la interferencia en elecciones extranjeras. Su actividad se centra en infraestructuras críticas como energía, transporte y telecomunicaciones.

En 2024, la empresa Mandiant lo clasificó oficialmente como APT44, destacando su papel como una de las amenazas cibernéticas más serias a nivel global. Sus acciones combinan sabotaje técnico con campañas de propaganda para maximizar el impacto.

Ataques conocidos y TTPs

En este punto se hace referencia de nuevos a los ataques y **TTPs** de **APT44**

Aspecto	**Descripción**
Procedencia	Rusia. Asociado a la Dirección Principal del Estado Mayor de las Fuerzas Armadas de la Federación de Rusia (GRU).
Motivaciones	Ciberataques con fines militares, políticos y de desestabilización. Sabotaje y guerra de información.
Ataques conocidos	- Ataque a la red eléctrica de Ucrania (2015, 2016). - NotPetya (2017), considerado uno de los ciberataques más destructivos. - Ataques a los Juegos Olímpicos de Invierno 2018.
TTPs destacadas	- Despliegue de wipers como NotPetya. - Uso de exploits de día cero. - Movimientos laterales rápidos y destrucción de infraestructura crítica.
Herramientas comunes	BlackEnergy, Industroyer, NotPetya, KillDisk, GreyEnergy.
Técnicas MITRE ATT&CK	T1485 (destrucción de datos), T1027 (ofuscación), T1210 (explotación de servicios remotos), T1046 (descubrimiento de red), T1569.002 (exec remota).
Tipo de objetivos	Infraestructura crítica, gobiernos, energía, transporte, organizaciones internacionales, especialmente en Europa y EE.UU.

A continuación, se muestra un mapa de Europa y Asia Central con los niveles de actividad del grupo **APT44**, indicando alta influencia en Europa del Este.

También detalla las tácticas cibernéticas empleadas, como acceso inicial, movimiento lateral y sabotaje en sectores estratégicos.

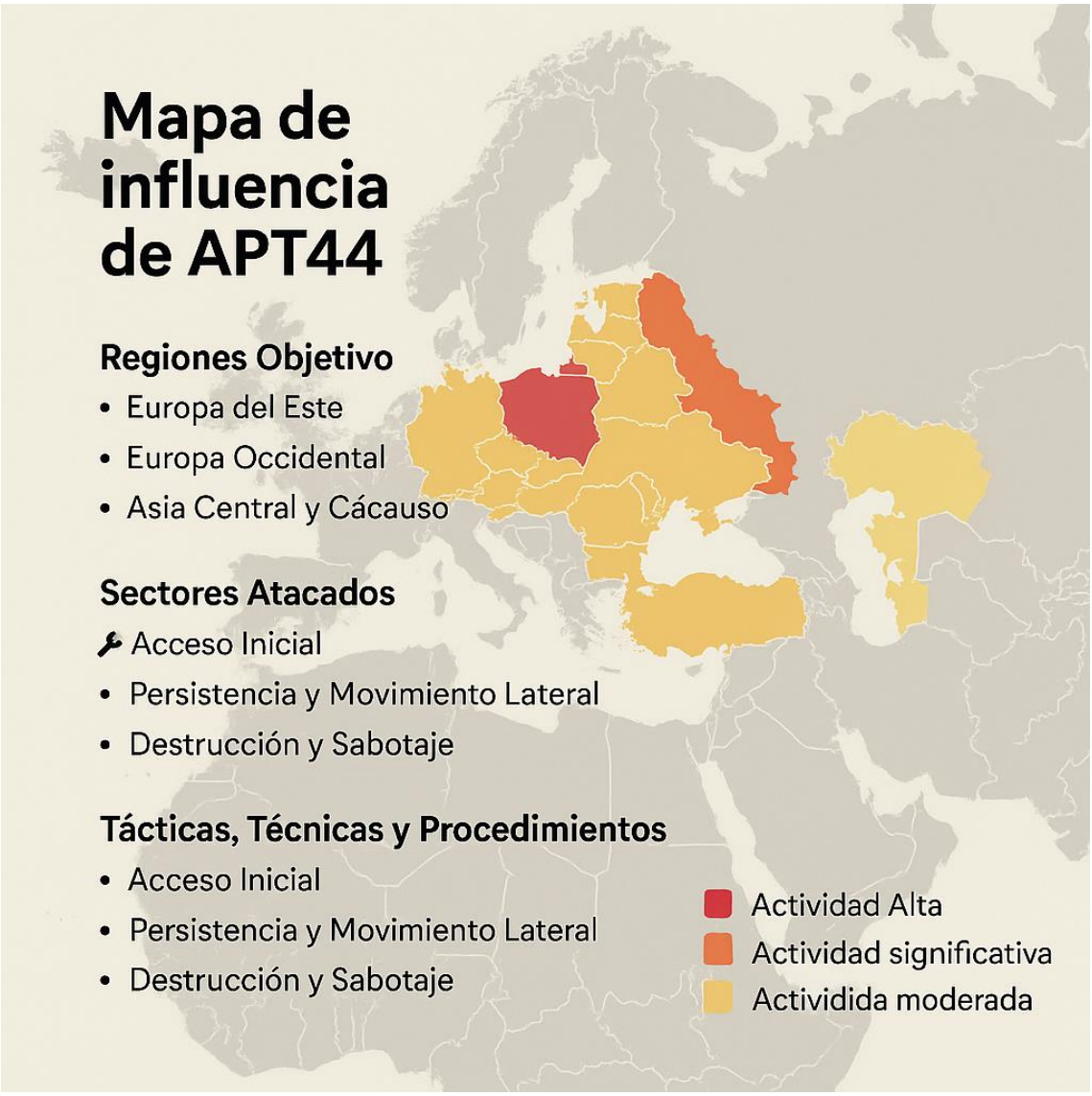

Ilustración 5-Mapa de influencia APT44

Evolución y sofisticación del grupo

A lo largo del tiempo, APT44 ha evolucionado sus capacidades técnicas. Ha adaptado sus tácticas y herramientas según el objetivo y el entorno tecnológico.

Su nivel de sofisticación no solo se refleja en la variedad de malware que desarrollan, sino también en la persistencia de sus operaciones, que suelen mantenerse activas durante largo periodos sin ser detectadas.

Esto se debe a una importante inversión en investigación, desarrollo y operaciones por parte del estado ruso.

El grupo ha demostrado una capacidad increíble para operar en muchos ámbitos, como el ciberespacio y en el ámbito de la información.

Esto se refleja en operaciones de guerra psicológica y campañas de desinformación, ampliando el alcance del ataque más allá del ciberespacio.

Contexto geopolítico

La actividad de **APT44,** no puede ser entendida sin considerarse en el entorno geopolítico en el que opera.

Rusia ha adoptado la ciberseguridad ofensiva como una extensión de su doctrina militar.

Es un marco en el cual los grupos como **APT44** actúan como brazos ejecutores de estrategias de influencia, desestabilización y sabotaje digital.

Las tensiones con Occidente, especialmente tras la anexión de Crimea en 2014, han intensificado ese tipo de operaciones encubiertas.

Perspectivas futuras

A medida que las tecnologías emergentes como la inteligencia artificial, el aprendizaje automático y los sistemas cibernéticos avanzan, se espera que **APT44** continúe adaptando sus capacidades.

El grupo probablemente ampliara su repertorio técnico para incluir ataque a entornos OT/ICS(sistemas de control industrial) y a nuevas superficies de ataque como redes 5G o dispositivos IoT críticos.

Además es probable que combine aún más sus operaciones técnicas con campañas de desinformación ampliando el impacto estratégico de sus acciones a nivel global.

Medidas a tomar contra APT44.

A continuación, se detallan las medidas de mitigación propuestas frente a la amenaza representada por APT44.

APT 44 (SandWorm), es un grupo avanzado vinculado a operaciones de ciberataque destructivo, sabotaje y ciberespionaje, con actividad en Europa y el ámbito geopolítico ucraniano.

Para poder mitigar el impacto, se prevén las siguientes medidas:

1. **Fortalecimiento de la infraestructura crítica**
    - Segmentación de redes **OT** (Operational Technology) e **IT**((Information Technology).
    - Supervisión activa de sistemas **SCADA(**Sistemas de Control Industrial) y Protocolos Industriales.
2. **Endurecimiento del acceso**
    - Uso obligatorio de **MFA** en accesos privilegiados(Autenticación Multifactor).
    - Auditoría y limitación de cuentas con privilegios excesivos
3. **Detección y respuesta avanzada**
    - Implementación de soluciones **EDR/XDR** para detectar movimientos laterales y comportamiento anómalo.
    - Monitorización de patrones relacionados con herramientas como **Mimikatz, Credential Dumping,** o ejecución de scripts maliciosos en **PowerShell.**
4. **Resiliencia y backup**
    - Copias de seguridad offline y pruebas regulares de restauración
    - Protección contra **wipers(**borradores) como NotPetya, mediante segmentación de sistemas y uso de snapshots.

5. **Inteligencia y actualización**
    - Integración de fuentes de inteligencia (**CTI)** para detectar **TTPs** recientes del grupo
    - Aplicación acelerada de parches ante vulnerabilidades conocidas explotadas previamente por el grupo (p. ej., **CVE-2022-30190 “Follina”)**
6. **Concienciación y simulacros**
    - Formación sobre **spear phishing** y ataques de **ingeniería social.**
    - Simulacros de respuesta a incidentes destructivos y **ransomware.**

Conclusión Módulo 2

El análisis de diferentes **actores APT** nos ha llevado paso a paso a la identificación del verdadero responsable: **APT44**.

Este método comparativo ha sido fundamental para descartar otras opciones y concentrar nuestros esfuerzos en entender mejor al grupo más probable.

Tras confirmar que era **APT44**, realizamos un estudio profundo de sus formas de actuar (tácticas, técnicas y procedimientos), así como de los ataques más importantes que ha llevado a cabo.

Este análisis permitió comprender en profundidad el comportamiento operativo, los objetivos estratégicos y el perfil de amenazas asociado al grupo.

Gracias a toda esta información, pudimos definir medidas de seguridad específicas y ajustadas a su perfil.

Estas acciones están diseñadas para detectar, bloquear y responder de manera efectiva a las técnicas que utiliza APT44, especialmente en áreas críticas o que tienen un gran valor estratégico.

Módulo 3 EJERCICIOS ESPECÍFICOS

Este módulo tiene como objetivo poner en práctica los conocimientos adquiridos en los módulos anteriores a través de ejercicios específicos relacionados con tres áreas clave: **mapa de riesgos**, **inteligencia de amenazas** y **hacking técnico**.´

Este módulo permite consolidar el análisis previo mediante representaciones visuales, simulaciones estratégicas y soluciones técnicas ante vulnerabilidades reales.

Mapa de riesgos

Continuando con el análisis realizado en **Módulo 1**, se ha desarrollado un mapa de riesgos que ofrece una visión clara y cuantificable de las principales amenazas detectadas en **SUPERTECH S.A.**

Este mapa integra las amenazas identificadas y el actor confirmado (**APT44)** en el **Módulo 2,** permitiendo una representación visual precisa y estratégica para la gestión de riesgos.

Para ello, se han evaluado los riesgos según dos criterios:

- **Probabilidad de ocurrencia**
- **Impacto sobre la organización**

Se han representado gráficamente en una matriz de calor que permite ver rápidamente qué amenazas requieren mayor prioridad de mitigación.

Amenaza / Riesgo	**Probabilidad (1-5)**	**Impacto (1-5)**	**Riesgo total (P x I)**	**Nivel**
Ataque de APT44 con malware destructivo	5	5	25	Crítico
Phishing dirigido a empleados clave	4	4	16	Alto
Robo de credenciales y movimiento lateral	4	5	20	Crítico
Pérdida de datos sensibles	3	5	15	Alto
Acceso a red interna a través de servicios MSP	3	4	12	Medio
Fuga de información por fallo humano	2	3	6	Bajo

A continuación se muestra una matriz más visual

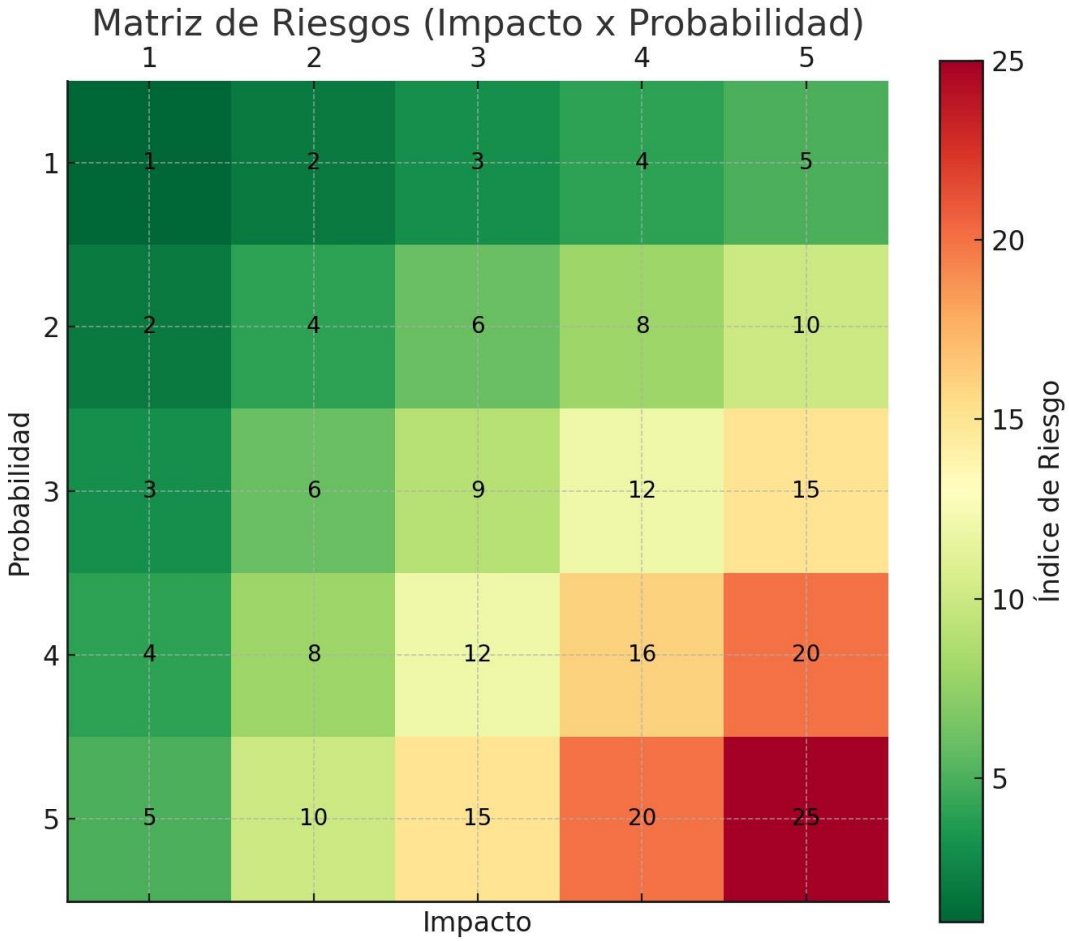

Ilustración 6-Matriz de riesgos con datos de Módulo 1 y 2

Investigación OSINT de un activo expuesto

En el siguiente apartado se evaluará el nivel de exposición de uno de nuestros activos más importantes antes posibles y futuros ataques.

Identificación del activo

La persona a la cual debemos de analizar es **Helena Herrero**, Directora de Operaciones de nuestra empresa.

Objetivo del análisis

Antes los posibles ataques a los que nuestra empresa se enfrenta, hemos decidido evaluar contramedidas para que nuestro factor humano no se vea expuesto a futuros ataques y tanto ellos como su entorno estén seguros.

Fuentes y herramientas utilizadas

Se utilizarán las siguientes herramientas para nuestra evaluación.

- **LinkedIn-** Para analizar su puesto, funciones, tecnologías con las que trabaja, personas con la que se conecta, etc.
- **Wikipedia-** Para ver qué información podría haber de ella
- **Google + Dorking**- Para buscar posible información asociada con publicaciones, documento o menciones.
- **Facebook, Instagram y Twitter-**Para detectar posibles exposiciones de vida social.

Resultados obtenidos

Aquí se muestran los resultados obtenidos, los que servirán para conocer el grado de exposición y toma medidas para evitar los posibles ataques.

LinkedIn:

Campo	Información
Nombre Completo	**Helena Herrero Starkie**
Lugar de Residencia	**Las Rozas, Madrid**
Estudios Realizados	**- Licenciatura en Químicas, Universidad Complutense de Madrid (1977–1982) - Gestión y Dirección Empresarial, INSEAD - PADE, IESE Business School**
Información Laboral Actual	**- Miembro del Consejo de Administración de Naturgy - Vocal-Consejera en Mutua Madrileña (Comisiones de Auditoría y Control, y de Cumplimiento) - Vicepresidenta de AmChamSpain - Miembro de Fundación Consejo España-EE.UU y de la Junta Directiva del American Business Council - Patrono de Fundación COTEC para la Innovación - Colaboradora de la Fundación Princesa de Girona**
Distinciones Obtenidas	**- Premio a la Trayectoria (Forinvest)** **– Personalidad del Año (Revista Byte) - Ejecutiva del Año (Revista Ejecutivos y FEDEPE)** **- Mujer Directiva (Fundación Madrid Woman's Week) - Premio a la Profesionalidad (EVAP)** **- Premio Gestor de Personas (Asociación Española de Directores de RRHH)** **- Premio ANQUE 2018 (Asociación Nacional de Químicos e Ingenieros Químicos de España)**

Mantiene un perfil bajo en LinkedIn, que utiliza de forma profesional.

Comparte publicaciones relacionadas con la tecnología, la innovación, la sostenibilidad y causas de impacto social, en línea con su trayectoria como alta directiva y su participación en diversas organizaciones empresariales y fundaciones

Wikipedia

En Wikipedia, no se logra obtener gran información de nuestro activo, salvo su fecha de nacimiento habiendo nacido esta en 1959 y teniendo actualmente 66 años.

En Wikipedia, tambien se obtiene su trayectoria profesional y estudiantes, como lo recogido en LinkedIn.

Google + Dorking

La información más relevante encontrada con los distintos Dorks es la siguiente:

- Casada y madre de dos hijos (Universitarios): No se atisba nivel de exposición de su pareja ni hijos (Nombres ni ninguna otra información.
- Muy Activa en entrevistas sobre tecnología y activismo feminista y sobre las mujeres en el sector tecnológico

En Google tampoco se encuentra gran información sobre nuestro activo, salvo entrevistas hechas enfocadas al trabajo y hablando en bajo nivel de su familia y activos personales.

Facebook, Instagram y Twitter

Tiene un bajo perfil en redes sociales, casi nulo, no se puede desgranar gran información de ella.

Resumen de la búsqueda

Categoría	**Descripción / Qué buscar**
Datos de contacto	Linkedin
Información profesional	Varios trabajos en el sector tecnológico
Red familiar / social	Casada, con dos hijos universitarios
Intereses personales	Sostenibilidad y innovación. Desarrollo educativo y formación de futuros líderes. Empoderamiento de la mujer en el entorno corporativo. Redes internacionales y colaboración empresarial.
Orientación política o ideológica	Se atisba una orientación política de izquierdas
Publicaciones o filtraciones	No se encontró nada referente a la información requerida
Actividades en foros o redes técnicas	No participa activamente en foros o redes técnicas como profesional técnica, sino que su actividad se centra en el liderazgo estratégico en innovación, sostenibilidad y transformación digital dentro del ámbito corporativo..
Uso de herramientas / entornos	No se encontró nada referente a la información requerida
Geolocalización o rutina diaria	Vive en Las Rozas, Madrid, sin ninguna otra ubicación conocida.

Simulación de ataque dirigido

En el siguiente apartado se simulará un posible ataque.

Fase 1- Reconocimiento

El atacante identifica a Helena Herrero como una figura de alto nivel dentro de la empresa con presencia en LinkedIn y una imagen asociada a innovación, sostenibilidad y liderazgo estratégico.

Su correo podría estar disponible mediante fuentes como “Hunter.io” o filtraciones antiguas.

Fase 2- Acceso inicial

Se diseña un ataque de **spear phishing personalizado,** utilizando un mensaje aparentemente enviado desde una organización relacionada con sostenibilidad o empoderamiento femenino, temáticas afines a su perfil.

El correo incluiría un enlace o documento con carga maliciosa (ej. Macro, PDF con exploit o enlace a web clonada).

Fase 3- Ejecución

Si Helena accede al enlace o abre el archivo, se ejecuta un script que instale un malware tipo **RAT(Remote Acces Trojan)** o beacon (C2) en su equipo corporativo.

A partir de ahí, el atacante puede realizar reconocimiento interno, robo de credenciales o escalar privilegios en la red de **SUPERTECH.**

Fase 4- Resultados esperados

- Acceso a documentos confidenciales
- Compromiso de cuentas de correo corporativo
- Obtención de credenciales de acceso privilegiado
- Expansión lateral dentro de la red si el Endpoint no está segmentado o protegido adecuadamente.

Medidas defensivas frente al ataque simulado

Aquí se exponen medidas frente al posible ataque.

- **Formación en concienciación para personal directivo**
  - Campañas periódicas de phishing simulado.
  - Charlas específicas sobre ingeniería social dirigida a figuras de alto perfil.
- **Filtrado avanzado de correos electrónicos**
  - Uso de soluciones anti phishing con análisis de comportamiento y reputación de enlaces adjuntos.
  - Bloqueo de archivos ejecutables y macros en correos entrantes.
- **Implementación de EDR/XDR**
  - Herramientas de monitorización y respuesta para detectar RATs o comportamientos anómalos en endpoints.
- **Segmentación de red**
  - Aislar puestos de trabajo de usuarios clave del resto de la red corporativa para limitar movimientos laterales.
- **MFA en todos los accesos sensibles**
  - Activar autenticación Multifactor especialmente en cuentas de correo, VPN y acceso remoto.
- **Gestión de la exposición pública**
  - Auditoría de huella digital de directivos.
  - Control de la información personal o profesional publicada en redes públicas.

Hacking

En este apartado se recogen 3 de todos los retos que nos hemos encontrado a lo largo del curso, en él se recogerán los siguientes puntos.

- Descripción del reto
- Herramientas usadas
- Solución aplicada
- Capturas
- Erros y Dificultades encontradas

Ejercicio 1

Ejercicio 1: “Más que un Despiste”

Descripción del reto:

El reto consistía en utilizar técnicas de OSINT (Open Source Intelligence) para identificar una "flag" a partir del análisis de un único documento PDF.

Herramientas utilizadas o consideradas

Puesto que teníamos el documento pdf, lo primero que se probó fue el uso de las siguientes herramientas:

- Exiftool, la cual permite leer, modificar y borrar los metadatos de cualquier archivo(foto, video, documentos, etc.). — Referencia en imagen 1 y 2.
- Pdfimages, la cual se usa para poder extraer imágenes visibles u ocultas de archivos PDF — Referencia en imagen 3.
- Mutool, el cual nos sirve para ver el contenido de cada objeto del PDF— Referencia en imagen 4

Solución aplicada

En este caso no se puede llegar hasta la flag

Capturas de pantalla

Capturas 1 y 2

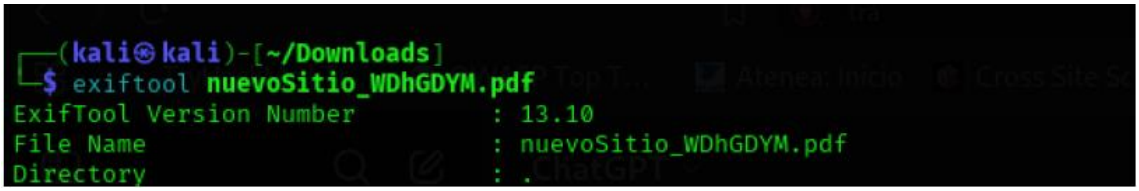

Ilustración 7-Captura de reto 1, se muestra la ejecución del comando exiftool

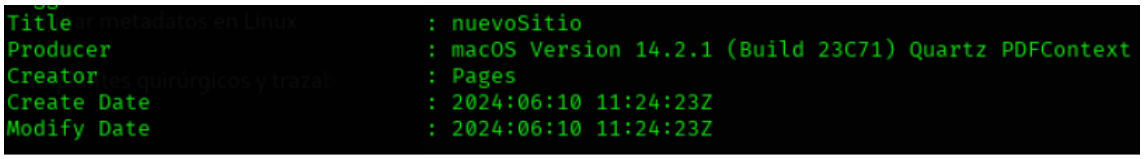

Ilustración 8-Captura de reto 1, se muestra la ejecución del comando exiftool

Captura 3

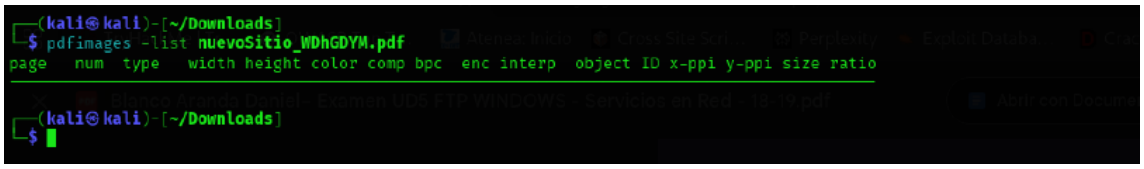

Ilustración 9-Captura de reto 1, se muestra la ejecución del comando pdfimages

Captura 4

Ilustración 10-Captura de reto 1, se muestra la ejecución del comando mutool

Errores o dificultades encontradas

Aunque no se logró resolver el reto, se exploraron diversas herramientas OSINT, lo cual enriqueció el aprendizaje

Ejercicio 2

Ejercicio 2: Zerologon

Descripción del reto

El reto consistía en encontrar el nombre de un servidor de Active Directory, valiéndome de un archivo de tráfico en Wireshark, con información de una conexión OpenVPN.

Herramientas utilizadas o consideradas

En este reto se usó solamente la herramienta Wireshark, la cual sirve para capturar y analizar el tráfico de red en tiempo real. Permite ver qué datos se envían y reciben en una red, lo que es útil para diagnosticar problemas, detectar intrusiones o aprender sobre protocolos de red. **— Referencia imagen 1**

Solución aplicada

Revisando los registros de OpenVPN, identificamos al atacante con la IP 192.168.100.128 y al servidor con la IP 192.168.100.6.
Buscamos tramas donde el origen sea la IP del atacante y el destino el servidor.
En una de ellas observamos un intento de autenticación a través del protocolo Netlogon.

Al desplegar la información de dicha trama, se revela actividad sospechosa relevante.

Esto sugería que aquí se encuentra la información clave del ataque. —**Referencia imagen 2, 3 y 4**

Solución aplicada

Se usó Wireshark y mediante las pistas proporcionadas, por el propio reto, se pudo identificar al registro exacto que contenía la solución.

Capturas de pantalla

Captura 1

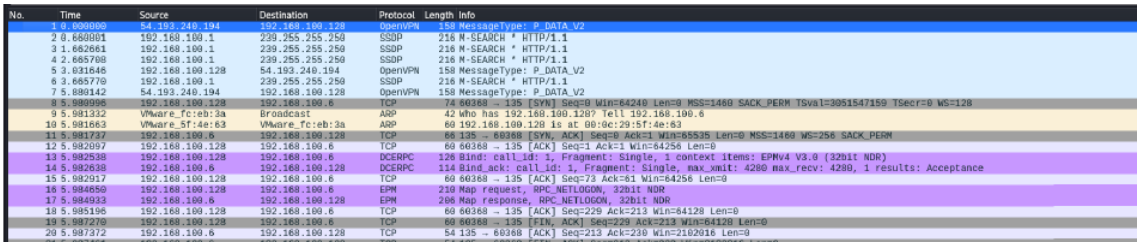

Ilustración 11-Captura 1 Ejercicio 2, Wireshark

Captura 2, 3 y 4

Ilustración 12-Captura 2 Ejercicio 2, Registro de Wireshark

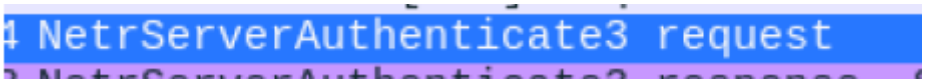

Ilustración 13-Captura 3 Ejercicio 2, Registro de Wireshark

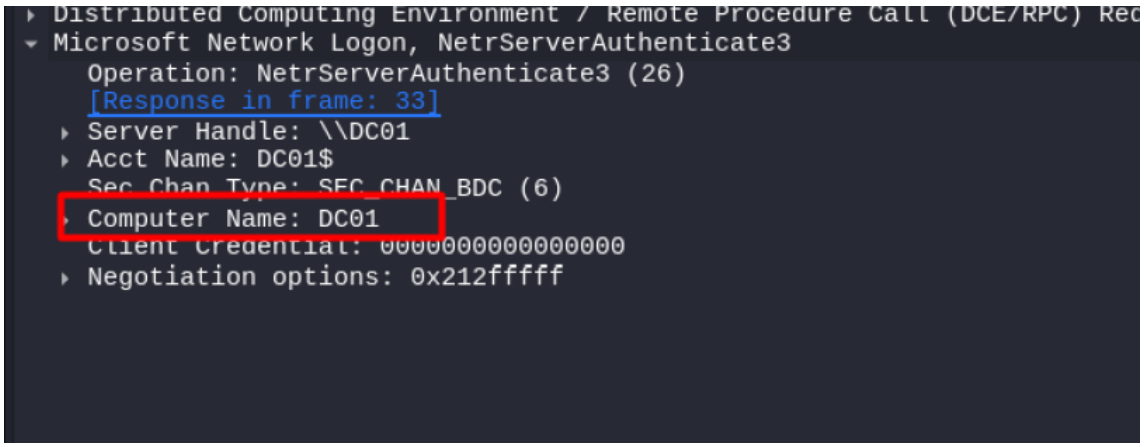

Ilustración 14-Captura 4 Ejercicio 2, Información de Registro de Wireshark

Errores o dificultades encontradas

La única dificultad encontrada fue que el archivo tenía gran cantidad de registros, y para usuarios que no están acostumbrados a usar Wireshark podría haber sido un gran reto.

Ejercicio 3

Ejercicio 3: El acechador nocturno

Descripción del reto

En este reto, te proporcionaban un programa que a primera vista parecía una simple calculadora, pero dentro de su código se encontraba nuestro flag.

Herramientas utilizadas o consideradas

Las herramientas que pudimos usar en este reto fueron las siguientes:

- file, la cual sirve para obtener información de todo tipo de archivos
- strings, se usa para extraer cadenas de texto legibles (ASCII o Unicode) desde archivos binarios o ejecutables y se usa para analizar archivos binarios para ver si contienen texto oculto o incrustado. —**Referencia imagen 1**
- radare2 (r2), herramienta española la cual sirve para hacer análisis y reversa de binarios muy potentes y de código abierto. —**Referencia imagen 2**

Solución aplicada

Primero se usó el comando *"file"* para averiguar el tipo de archivo el cual era un archivo binario de 64 bits, seguidamente usamos *"strings"* para ver los entresijos del programa y encontramos un flag codificada aún en binario (**Referencia imagen 1)**, una vez conseguido esto se usó r2 para realizar ingeniería inversa a dicha información y conseguir la clave en el formato deseado (**Referencia imagen 2).**

Capturas de pantalla

Captura 1

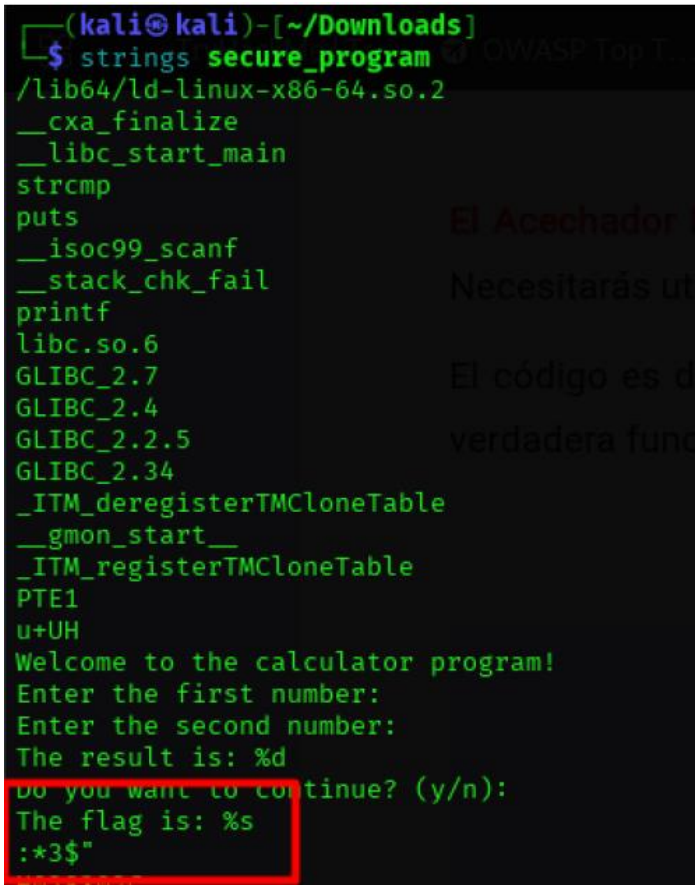

Ilustración 15-Captura 1 Ejercicio 3 Ejecución comando strings

Captura 2

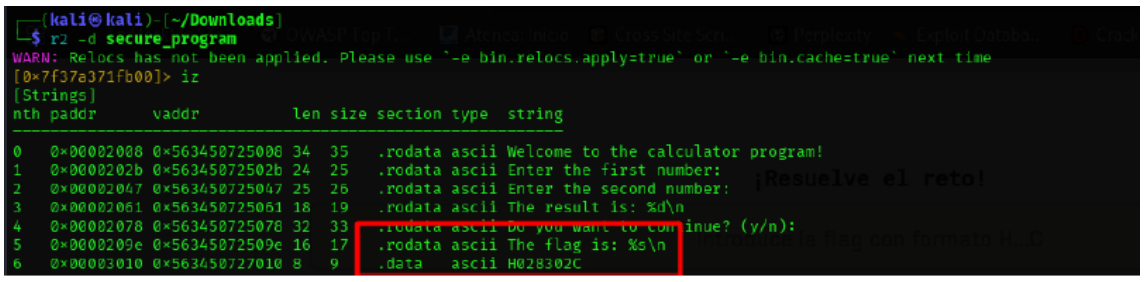

Ilustración 16-Captura 2 Ejercicio 3, Ejecución de comando r2, con solución de reto

Errores o dificultades encontradas

La dificultad de este reto es el conocimiento que se tenga de comando de Linux, archivos binarios, etc.

Pero con ayuda de información procedente de foros, herramientas de IA, entre otros recursos se puede resolver sin ningún problema.

Conclusión del TFC.

Gracias a este trabajo, considero que se han consolidado en gran medida los conocimientos adquiridos a lo largo del curso.

Ha resultado ser una práctica útil y realista para futuros informes o situaciones profesionales en el ámbito de la ciberseguridad.

Aunque la identificación del actor de amenazas no fue una tarea sencilla, la experiencia ha permitido no solo reconocer a APT44 como posible atacante, sino también explorar y comprender las características de otros grupos relevantes.

Por último, el análisis OSINT aplicado al personaje ha reforzado las habilidades de investigación y ha demostrado la importancia de saber dónde y cómo obtener información valiosa en escenarios reales.

Bibliografía

Google Cloud. (2024, febrero 20). *APT44: Unearthing Sandworm*. Google Cloud Blog. https://cloud.google.com/blog/topics/threat-intelligence/apt44-unearthing-sandworm

MITRE. (n.d.). *APT34*. MITRE ATT&CK. https://attack.mitre.org/groups/G0034/

Wikipedia contributors. (n.d.). *Charming Kitten*. Wikipedia. Retrieved May 15, 2025, from https://en.wikipedia.org/wiki/Charming_Kitten

Wikipedia contributors. (n.d.). *Sandworm (grupo de hackers)*. Wikipedia. Recuperado el 15 de mayo de 2025, de https://es.wikipedia.org/wiki/Sandworm_(grupo_de_hackers)

MITRE. (n.d.). *Groups*. MITRE ATT&CK. https://attack.mitre.org/groups/

Anexos

Anexo 1 Uso de IA en el desarrollo del TFC

En este anexo se recogen los prompts, que he usado con la IA (chatgpt) para completar este trabajo.

- Dame un mapa de influencia de APT44
- Creame una matriz de riesgos con datos de Módulo 1 y 2
- Necesito una gráfica de radar entre APTs
- Haz una gráfica de atracción de los APTs hacia SUPERTECH
- Haz una matriz de calor para el mapa de riesgos.
- Corrígeme las faltas de ortografía.
- Creame una tabla con la siguiente información.
- Dame más información sobre APT 44.

Anexo 2 Glosario de términos

- **APT**: Grupos de ciberdelincuentes altamente sofisticados que llevan a cabo ataques cibernéticos prolongados y dirigidos, con el objetivo de sustraer información confidencial o interrumpir operaciones críticas.
- **CTI (Cyber Threat Intelligence)**: Inteligencia de amenazas cibernéticas basada en análisis de datos y comportamientos maliciosos.
- **EDR (Endpoint Detection and Response)**: Tecnología para monitorizar, detectar y responder a amenazas en dispositivos finales.
- **MITRE ATT&CK**: Base de datos de conocimiento sobre tácticas y técnicas utilizadas por atacantes, actores maliciosos y sus TTPs.
- **OSINT (Open Source Intelligence)**: Proceso de recopilación y análisis de información pública para obtener información útil.
- **Phishing**: Técnica de ingeniería social para engañar a usuarios y robar datos confidenciales mediante correos o enlaces falsos.
- **SCADA (Supervisory Control and Data Acquisition)**: Sistemas de control industrial utilizados en infraestructuras críticas.
- **TTPs**: Tácticas, Técnicas y Procedimientos, usados por atacantes.
- **Wiper**: Tipo de malware diseñado para eliminar o inutilizar datos de forma irreversible.
- **XDR (Extended Detection and Response)**: Expande las capacidades del EDR unificando detección en endpoints, redes y servidores.
- **Spear phishing**: ataque dirigido que engaña a una persona específica para robar información sensible.
- **Exploit**: código o técnica que aprovecha una vulnerabilidad para ejecutar acciones maliciosas.
- **RAT(Remote Acces Trojan)** : Es un malware que permite el control remoto total de un sistema comprometido.

Anexo 3: Herramientas utilizadas en retos

- **exiftool** → para leer y analizar metadatos del PDF.
- **pdfimages** → para extraer imágenes visibles u ocultas del documento PDF.
- **mutool** → para explorar los objetos internos del archivo PDF.
- **Wireshark** → herramienta de análisis de tráfico de red.
- **file** → para identificar el tipo de archivo (binario de 64 bits).
- **strings** → para extraer texto legible incrustado en el binario.
- **radare2 (r2)** → herramienta de análisis y reversa de binarios

---Fin del documento---