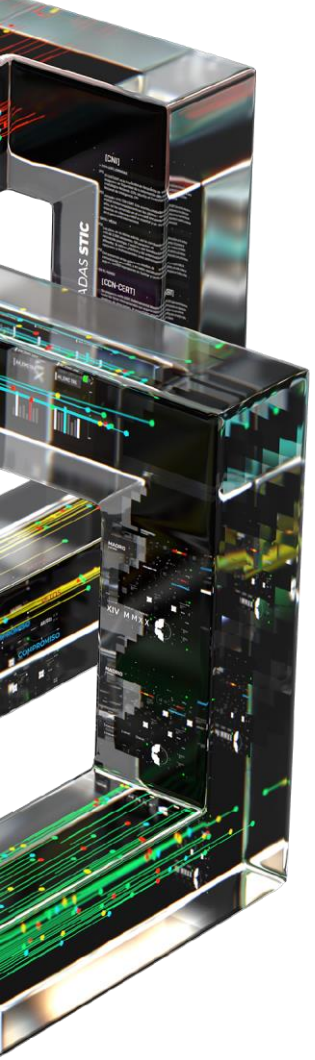


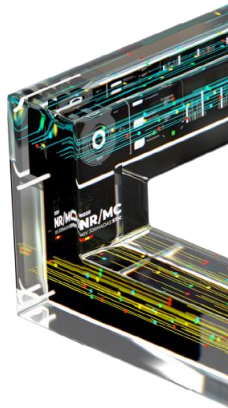
GOBIERNO DE ESPAÑA MINISTERIO DEL INTERIOR

Guardia Civil

UNIDAD CENTRAL OPERATIVA UCO GUARDIA CIVIL

# #XIVJORNADASCCNCERT

## “Threat Hunting Scenario: Insider Hunting”



cn-cert centro criptológico nacional

Teniente Coronel
D. Juan Antonio
Rodríguez
Álvarez de Sotomayor

**Jefe del Departamento de Delitos Telemáticos.**

**Unidad Central Operativa**

***GUARDIA CIVIL***

# El Reto:

A través de un caso real, veremos la importancia de conformar un **equipo ganador contra el Cibercrimen**: los equipos **CSIRT**, **la Guardia Civil** y **el ámbito judicial:**

*"Mediante un trabajo conjunto y coordinado en el desarrollo de una investigación tecnológica y criminal, se procedió a dar caza del "Insider" responsable de la exfiltración"*

# Ejemplo de trabajo conjunto CSIRTs-GC-Judicial

**DETECCIÓN**

**CSIRT** detecta un incidente que pudiera revestir carácter delictivo y lo comunica a la **GC**

La **GC** solicita los detalles y posibles evidencias

**RECOGIDA EVIDENCIAS**

**CSIRT** recoge datos relevantes de tráfico y de localización que puedan ser usados como evidencia judicial (GC)

**INVESTIGACIÓN ADICIONAL**

En el casos de un incidente a gran escala, se necesitará información adicional del operador de Red, a través de requerimientos de **GC** y la experiencia del equipo **CSIRT**

**ANÁLISIS DE EVIDENCIA, TRATAMIENTO, VALIDACIÓN POR EL TRIBUNAL**

En este momento, la **GC** puede usar herramientas forenses avanzadas y la experiencia del personal del **CSIRT**

# El caso

- El CEO de la compañía ACME, con base en España, tiene conocimiento de que un competidor, la empresa Eiffel (de un país europeo) ha tenido **acceso a información interna** de la empresa.
- Esta información versa sobre un proyecto de 700 millones de euros por los que están licitando ahora mismo en un país de América Latina (AL), a la vez que Eiffel.
- Ha sido el Country Manager (CM) de ACME en ese país de América Latina quien lo ha sabido.
- En una de las múltiples reuniones del proyecto, una persona le dice que la compañía Torre Effiel, en un chat de WhatsApp ha mostrado la estrategia de la compañía ACME.
- Esta persona cede las capturas del WhatsApp al CM.

# Empresa ACME

- Se trata de una empresa española, con varias sedes en el mundo.
- Su principal foco está en la **tecnología y las infraestructuras**.
- Se está **expandiendo de manera internacional**, su plan estratégico marca que para el año 2023 el 60% de su facturación debería ser fuera de España.
- En época Covid, mantiene a la mayoría de la plantilla teletrabajando, aunque no ha cerrado sus oficinas.

# La empresa Eiffel

- Se trata de una empresa europea, de similares características que ACME.
- A diferencia de la anterior, ésta ya tiene **mucha presencia internacional**.
- Su core de negocio se encuentra en **infraestructuras e ingeniería**.
- Cuenta con mucha presencia en América y Asia, que son sus principales mercados.

# La ayuda

# La ayuda

- Tras **muchas deliberaciones internas** de la empresa, ésta acude a la Guardia Civil explicando el problema, puesto que han tenido sospechas anteriormente de que habían sido objeto de **espionaje industrial**, pero no tan claro como esto.

- La idea de ACME es **denunciar** a partir de las capturas de la conversación de whatsapp.

- Sospechan también que ha sido un **malware** u otro software malicioso lo que ha podido extraer la información, pero ¿cómo ha llegado a manos de la empresa Eiffel?, por lo tanto, es necesario **conformar un equipo junto al CSIRT y la GC**.

# Empieza la investigación..

- La Guardia Civil, mediante **Cooperación Policial Internacional**, solicita la asistencia de la policía de ese país de AL.
- Éstos se entrevistan con el Country Manager de ACME.
- A la par, el CSIRT de ACME comienzan a realizar **análisis a los equipos informáticos**, tanto en España como en ese país de AL.

INTERPOL

# Entonces Eiffel…

- Al enterarse de estas novedades, decide comunicar oficialmente estos hechos a la empresa ACME, dado que ambas están concursando en ese proyecto de 700 millones de dólares.

- La empresa informa que la documentación le llegó a través de un **correo electrónico anónimo de Gmail**.

- También comunica el asunto al **organismo regulador del país**, cuya normativa obliga a reportar cualquier incidente que afecte al concurso de licitación.

- Hace entrega de un email y cinco documentos ofimáticos.

# La investigación

# ¿Por donde empezamos?

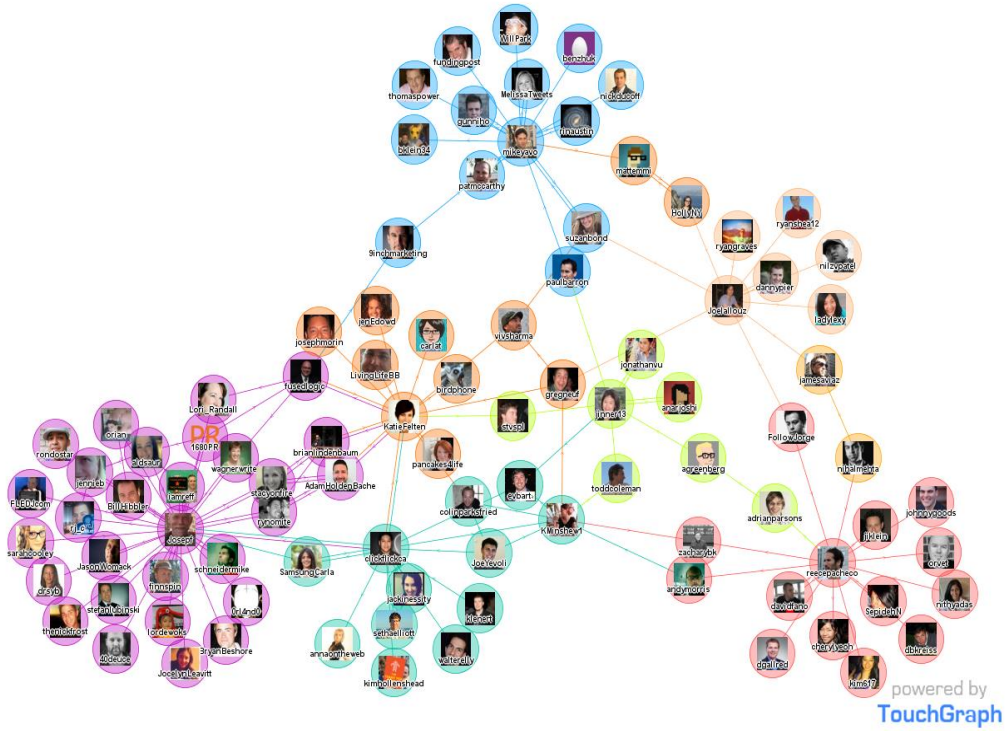
- Se solicita un mandamiento judicial sobre la **cuenta de Gmail**. Esto lo hacen las autoridades del país de AL

- A través de los sistemas informáticos de ACME, se detectó **qué personas tenían acceso a esa información**, mediante sistemas DLP y los registros de actividad de los equipos informáticos.

- En total hay **10 personas** que tienen acceso y trabajan con esa información.

# Análisis de Redes Sociales

- A la par, mediante un análisis en RRSS, se **perfila a las personas** involucradas.
- Como es normal, en la **red Linkedin** existen contactos profesionales entre empleados y ex empleados de ambas mercantiles.
- Pero destaca que una de las **10 personas** mantiene amistad en varias redes sociales con un antiguo empleado de la compañía Eifell, actualmente trabajando para otra compañía del sector.
- El análisis de **RRSS puede ser una pieza fundamental** en cualquier investigación de estas características.



# Análisis Técnico

- Tras un análisis inicial, se detecta que hubo una conexión de un pendrive al **equipo del comercial del proyecto** que copió esos y otros archivos. El comercial está de baja de paternidad y su equipo está en uso porque contiene documentación esencial del proyecto.

- La Policía de AL indica a la Guardia Civil que el CSIRT ha detectado un malware en el equipo del CM, remitiendo los **IoC y muestra del malware** a España.

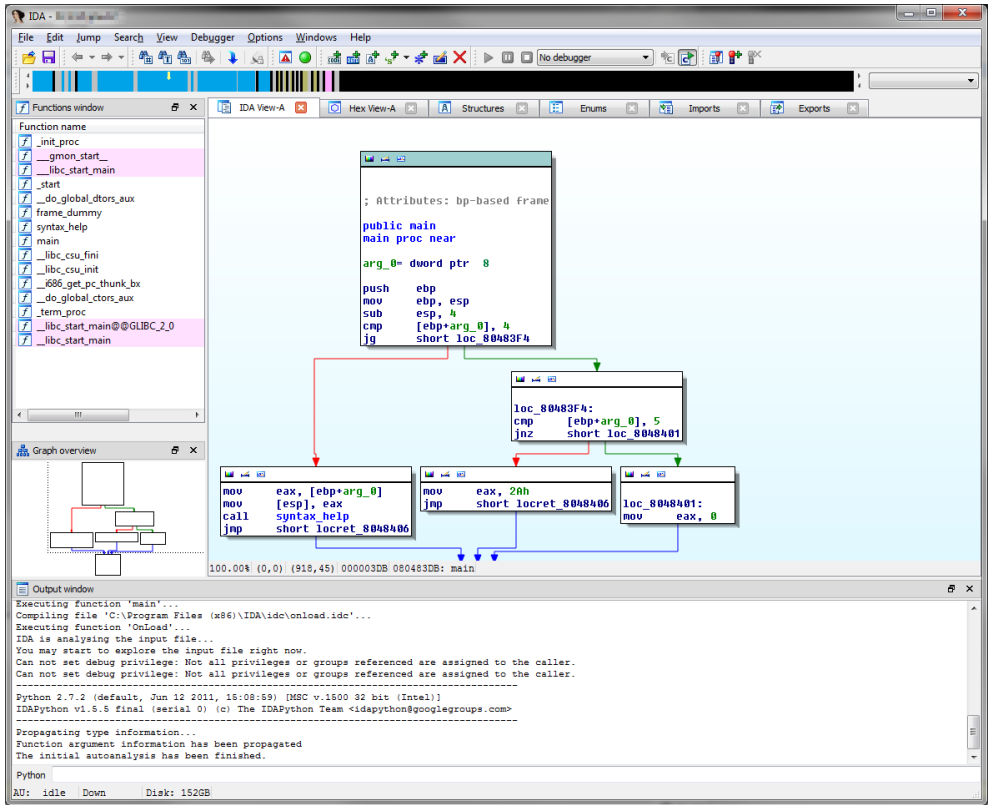
- Dicho malware no es conocido por los antivirus, y lo que hace es recoger documentación y teclas pulsadas.

# El malware

- En España, el CSIRT comienza a buscar ese malware en la infraestructura tecnológica de la compañía ACME, detectándose que en dos equipos ese malware existe.
  - ✓ Un equipo de secretaría.
  - ✓ El **equipo del trabajador** que tiene un amigo en RRSS ex-empleado de la empresa Eiffel.

- El malware se conecta a un **chat de Slack** donde va dejando los documentos, información, etc.

- Tiene capacidad de evasión de AV y la conexión es a través de http hacia el citado canal de Slack.



# Medidas proactivas de investigación

# Petición a la empresa Eiffel

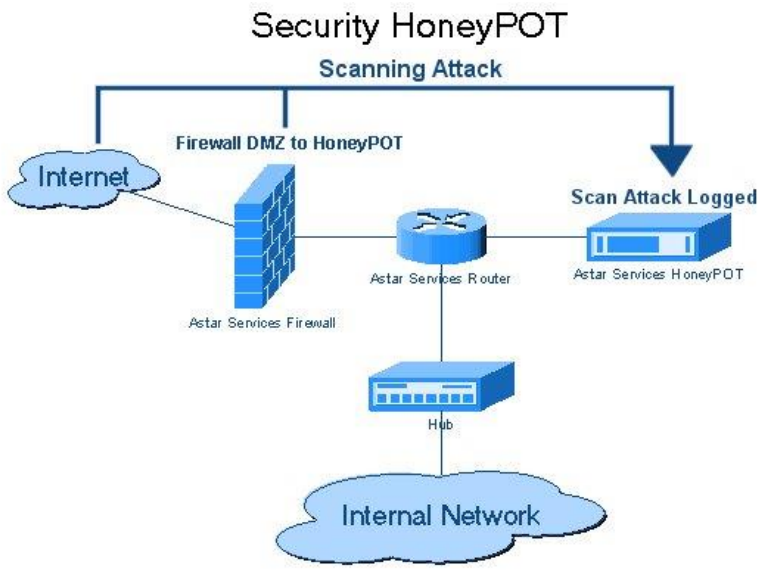
- Se pide su colaboración al objeto de contactar con el Gmail, y que **pida al sospechoso la siguiente documentación:**
  - ✓ Información de otros proyectos en la zona.
  - ✓ Información sobre nuevas contrataciones.

- Se le indica que va a ser remunerado por toda esta información.

- Incluso se le ofrece un puesto de trabajo en la empresa Eiffel si consigue la información que se le pide.

# El HoneyPot / Deception

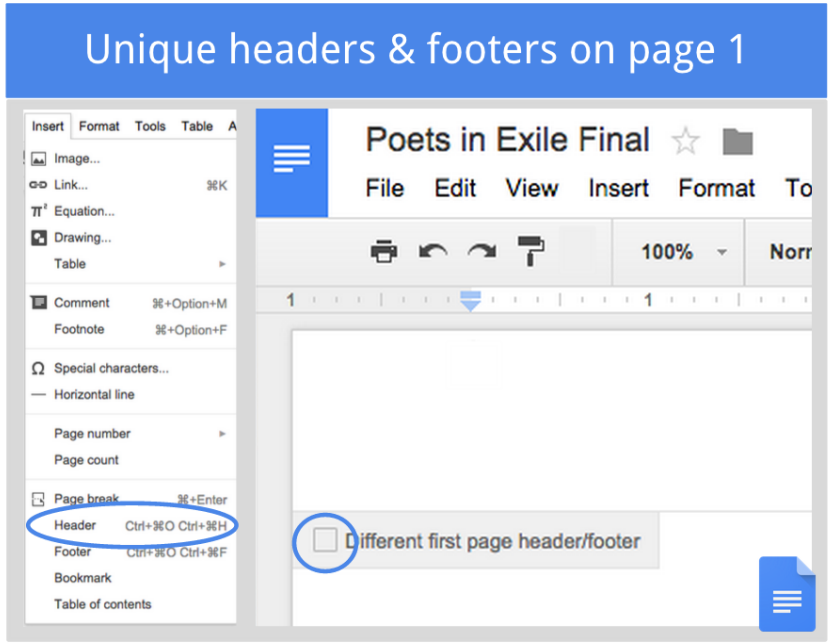
- Junto con el CSIRT, se decide desplegar en la red una serie de documentos ofimáticos relacionados con el proyecto.
  - ✓ Aprovechando que esta empresa es externa.
  - ✓ No se puede contar con recursos internos de la compañía por confidencialidad.
- Estos documentos llevan **un baliza digital** que indica los siguientes datos:
  - ✓ Cuando se abre el documento (fecha/hora)
  - ✓ Dirección IP // Nombre del ordenador
  - ✓ Listado de archivos en la carpeta “Mis Documentos”
- La idea es **monitorizar quién está accediendo** a los documentos y donde va.



# Acceso a la documentación

- En los siguientes días, se detecta lo siguiente
  - ✓ Se detecta el acceso a esta documentación desde una **dirección VPN**.
  - ✓ Sin embargo, de uno de los trabajadores objetivo.
  - ✓ Además, recoge el **nombre del equipo** que se conecta.
  - ✓ Ruta de la carpeta de mis documentos:

    C:/Users/**Nombre_Usuario**/Documents



# La judicialización

# Las IPS y análisis técnico equipos

- El proveedor **Slack aporta varias IPs** de interés.
  - ✓ Ips de la compañía ACME e IPs de VPN
  - ✓ Tres **Ips españolas** desconocidas
- Se resuelve la IP española, correspondiendo a un hotel en una zona del norte de Madrid, que con el covid19 ha sido cerrado.
  - ✓ Cerca de donde vive el empleado ya citado.
- La otra IP, pertenece a una persona cuyo nombre coincide con uno de los contactos en RRSS del empleado
- El pendrive que ha sido conectado en el equipo del comercial, también se ha conectado en el equipo de ese empleado de la IP.

# Las manifestaciones

- En la primera manifestación dice que no tiene ni idea de qué le están hablando, pero que el ex-empleado es amigo suyo y que de vez en cuando va a su casa.

- En una segunda manifestación, **ante las evidencias,** decide contar lo sucedido:
  - ✓ Está cansado de la Cía y está pasando por un mal momento, se siente maltratado.
  - ✓ Contacta con Eiffel a través del ex-empleado amigo y contacto en RRSS.
  - ✓ Le mandaron un email con un adjunto, que se descargó y contenía un malware con el que se infectaron los tres ordenadores.

# Las manifestaciones (II)

- Mandó ese documento a más personas, entre ellas al Country Manager, sólo él lo abrió.
- De vez en cuando se iba a trabajar a la cafetería de un hotel, que es precisamente el mismo que resuelve la IP.
- Reconoció que leyó el email que mandaron desde Eifell para acceder a la documentación que se le pidió, y que era la que estaba balizada.
- Se imaginó que podrían haber usado un software malicioso, pero no sabía el funcionamiento.
- Y….todo por venganza y la promesa de un mejor trabajo.

Los **CSIRT**, la **GC** y el **ámbito judicial** tienen sus propios roles, estructuras y responsabilidades

Uso de **herramientas comunes**: comunicación de incidentes, obtención de "e-evidence", análisis e investigación, coordinación e intercambio de información

Bajo el **control judicial** de la investigación y el acceso a la **e-evidence** a través de las herramientas de legales

La lucha contra el cibercrimen requiere una **perspectiva global, mayor inversión** y un **esfuerzo conjunto**

# Propuestas para luchar contra el Cibercrimen

**CIBERSEGURIDAD BASADA EN EL INTERCAMBIO DE INFORMACIÓN ENTRE ORGANISMOS**

**Centro de Fusión contra el Cibercrimen**

**ACCESO A LA E-EVIDENCE Y ATRIBUCIÓN MÁS EFECTIVA**

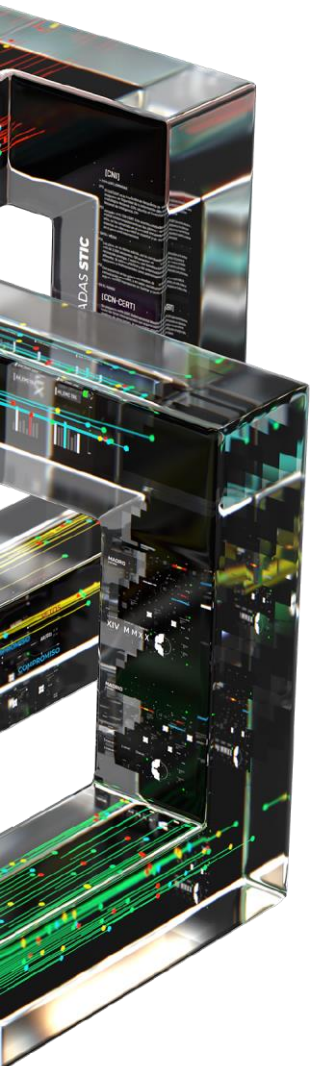
**Punto Neutro Judicial de Resolución WHOIS**

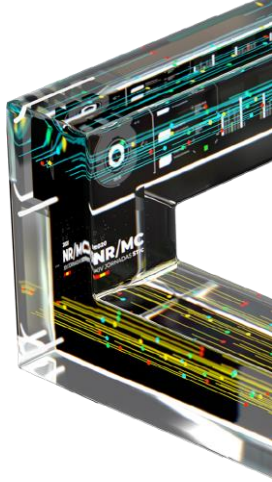
**CERTIFICACIÓN DE HERRAMIENTAS Y PROTOCOLOS**

**Centro Nacional de Certificación**

**FORMACIÓN Y CAPACTACIÓN AL ÁMIBITO JUDICIAL**

**Jurisdicción propia en el Ciberespacio**





GUARDIA CIVIL

CIBERCRIMEN

# MUCHAS GRACIAS

#XIVJORNADASCCNCERT