Cómo te levantan 100.000€ sin pestañear

Investigando una estafa al CEO desde el punto de vista forense

Maite Moreno - @mmorenog
Cybersecurity Intelligence Analyst - CERT Team Manager

Antonio Sanz - @antoniosanzalc
Senior Incident Response & Forensics Analyst

Agenda

- Cibercrimen
- Fraude al CEO
- Ejemplo: Caso real
- Caso Práctico: Estafa al CEO
- Conclusiones

Evidencias para el taller

bit.ly/estafaCEO

Reto forense

bit.ly/CTF_DFIR_Exchange

Cibercrimen

GRUPO

La vanguardia de la ciberseguridad

Impacto económico del cibercrimen

Las ganancias globales del cibercrimen alcanzan los 1.5$ trillones

Según un estudio de la Universidad de Surrey (Inglaterra):

$860 billion – Illicit/illegal online markets
$500 billion – Theft of trade secrets/IP
$160 billion – Data trading
$1.6 billion – Crimeware-as-a-Service
+ Zero-day Adobe exploits, up to $30,000
+ Zero-day iOS exploit, $250,000
+ Malware exploit kit, $200-$600 per exploit
+ Blackhole exploit kit, $700 for a month's leasing, or $1,500 for a year
+ Custom spyware, $200
+ SMS spoofing service, $20 per month
+ Hacker for hire, around $200 for a "small" hack
$1 billion – Ransomware

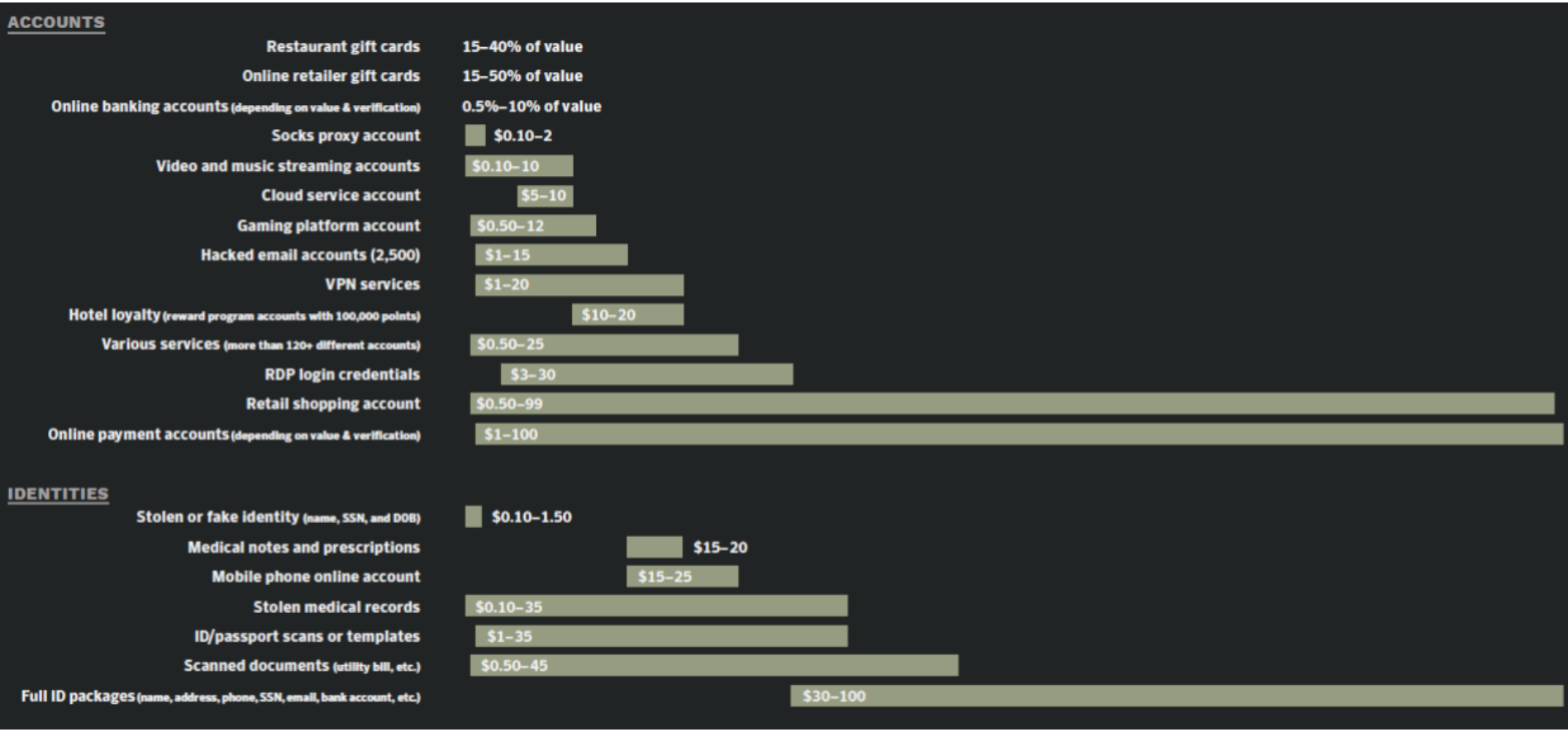
Impacto económico del cibercrimen

Europol EC3 – European Cybercrime Centre

Europol asiste a los 28 Estados miembros de la Unión Europea en su lucha contra la delincuencia internacional y el terrorismo. Colabora asimismo con numerosos estados asociados no pertenecientes a la UE y organizaciones internacionales

El cibercrimen cuesta a los Estados miembros de la UE 265,000 millones de euros al año. Para la economía mundial esa cifra ronda los 900.000 millones de euros

Economía underground



Cibercrimen organizado

Así operaba el Bandidos Revolution Team, la banda de hackers de México que robaba millones de los bancos todos los meses

Redacción
BBC News Mundo

5 junio 2019 Compartir

A Bandidos Revolution Team se la acusa de estar detrás del mayor ciberataque de la historia de México.

Un par de cajeros automáticos que de repente empezaron a escupir dinero fueron clave para que las autoridades mexicanas lograran desmantelar a la principal banda de cibercriminales del país.

Ocurrió el pasado 3 de marzo en León (Guanajuato) y Tijuana (Baja California Norte), luego de que los cibercriminales que debían recoger los billetes aparentemente faltaran a la cita.

- Cibercriminales manipularon el Sistema de Pagos Electrónicos Interbancarios del Banco de México para enviar dinero a varias cuentas fraudulentas, procediendo luego a retirar el dinero, principalmente a través de cajeros
- Cerca de 30M$ en pérdidas para el Sistema bancario mexicano
- Ransomware contra la aseguradora AXA (1 millón $)
- Clonación de tarjetas, etc…

Cibercrimen: Percepción del riesgo

World Economic Forum Global (2018-2019)

- El fraude y el robo masivo de datos fue clasificado como el cuarto riesgo más importante a nivel mundial
- Ataques disruptivos a infraestructuras y operaciones aparece como quinto riesgo más importante
- Aparecen por detrás de confrontaciones económicas o políticas entre grandes potencias

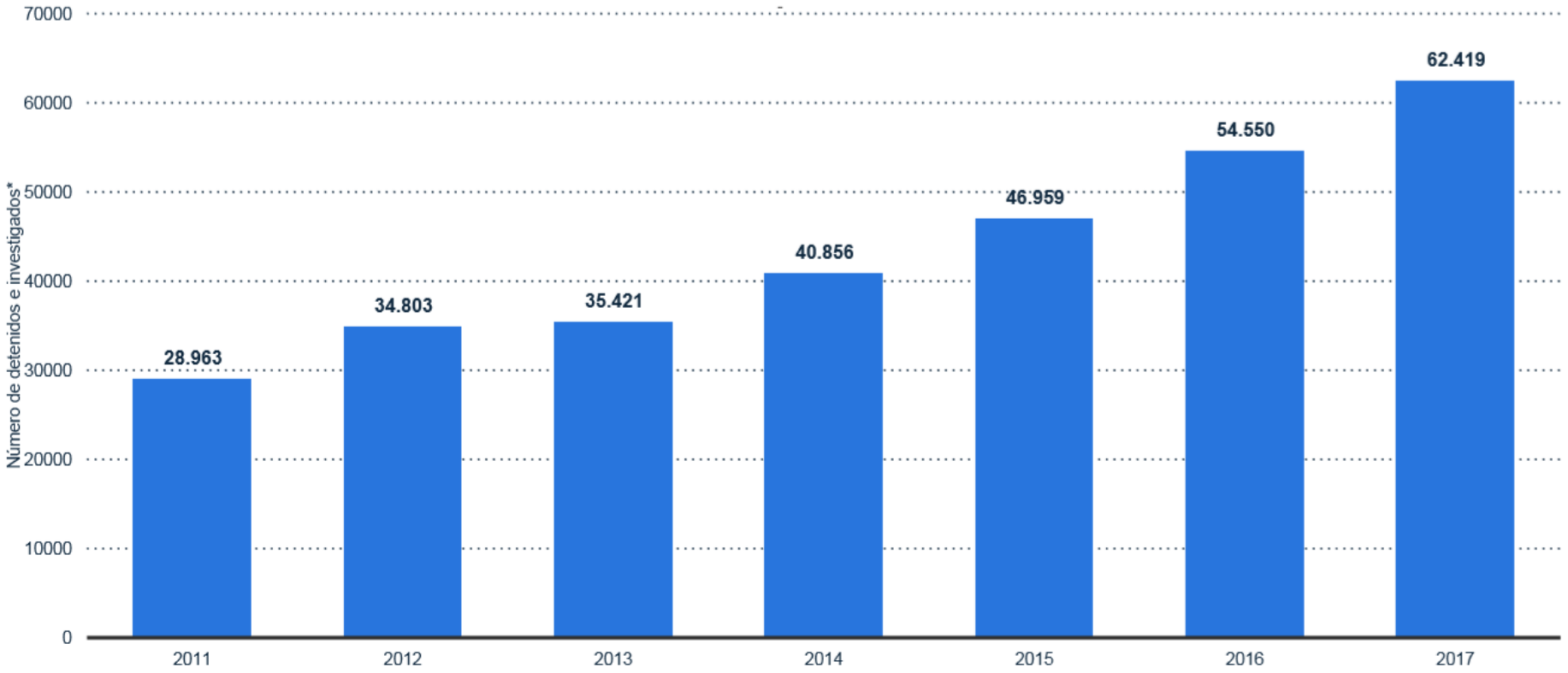
Amenazas y tendencias (CCN, 2019)

- Más del 60% del tráfico mundial del correo electrónico en 2018 contenía carga dañina y estuvo involucrado en más del 90% de los ciberataques
- Ataques phishing refinados mediante el uso de técnicas de ingeniería social y la innovación permanente para persuadir a los usuarios de la autenticidad de las estafas
- Los riesgos de delinquir en el ciberespacio, si se usan las herramientas adecuadas son muy bajos, al contrario que los beneficios que pueden ser muy elevados.

Cibercrimen: Cifras

Número de victimizaciones por ciberdelitos en España de 2011 a 2017

Cibercrimen: número de victimizaciones España 2011-2017

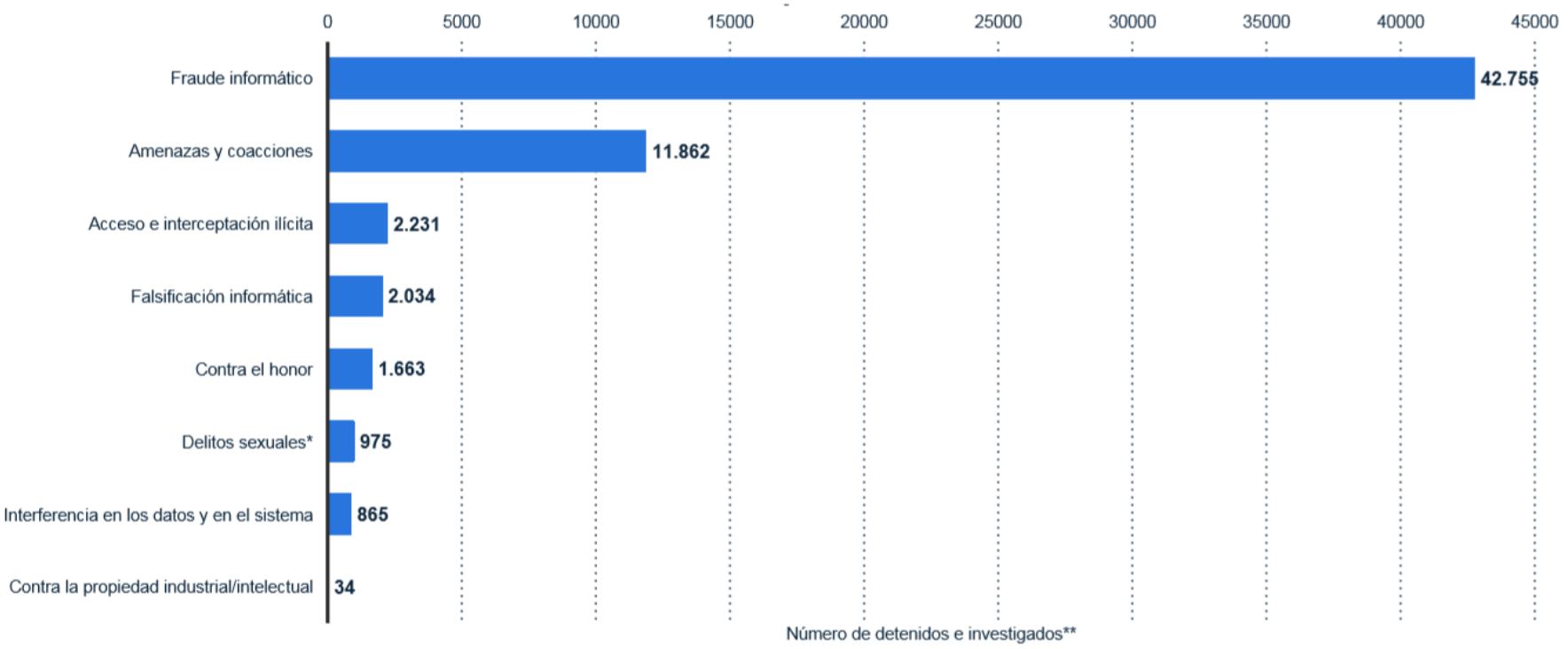


Notas: España; 2011 - 2017
Hay disponibles más datos y comentarios sobre esta estadística en la página 58.
Fuente(s): Ministerio del Interior (España); ID 814010

Cibercrimen: Cifras

Número de victimizaciones por ciberdelitos en España en 2017, por grupo penal

Cibercrimen: número de victimizaciones por grupo penal España 2017



Notas: España; 2017
Hay disponibles más datos y comentarios sobre esta estadística en la página 60.
Fuente(s): Ministerio del Interior (España); ID 884901

Estafas al CEO

S2 GRUPO

Business Email Compromise - BEC

OBJETIVO

Cualquier empleado de una compañía, en especial aquellos que tengan **accesos a los recursos financieros** de la empresa o estén habilitados para emitir pagos por transferencia a su nombre

ESCENARIO

El objetivo recibe un correo, supuestamente de su jefe/CEO/Director/Presidente de la empresa, en la que le **pide ayuda para una operación financiera**. El empleado víctima cae en el engaño y desvela datos confidenciales como el saldo de la cuenta, accede a hacer una transferencia, etc.

Los cibercriminales suelen aprovechar ocasiones en las que el **jefe no está disponible** para que la víctima no tenga la oportunidad de verificar su autenticidad

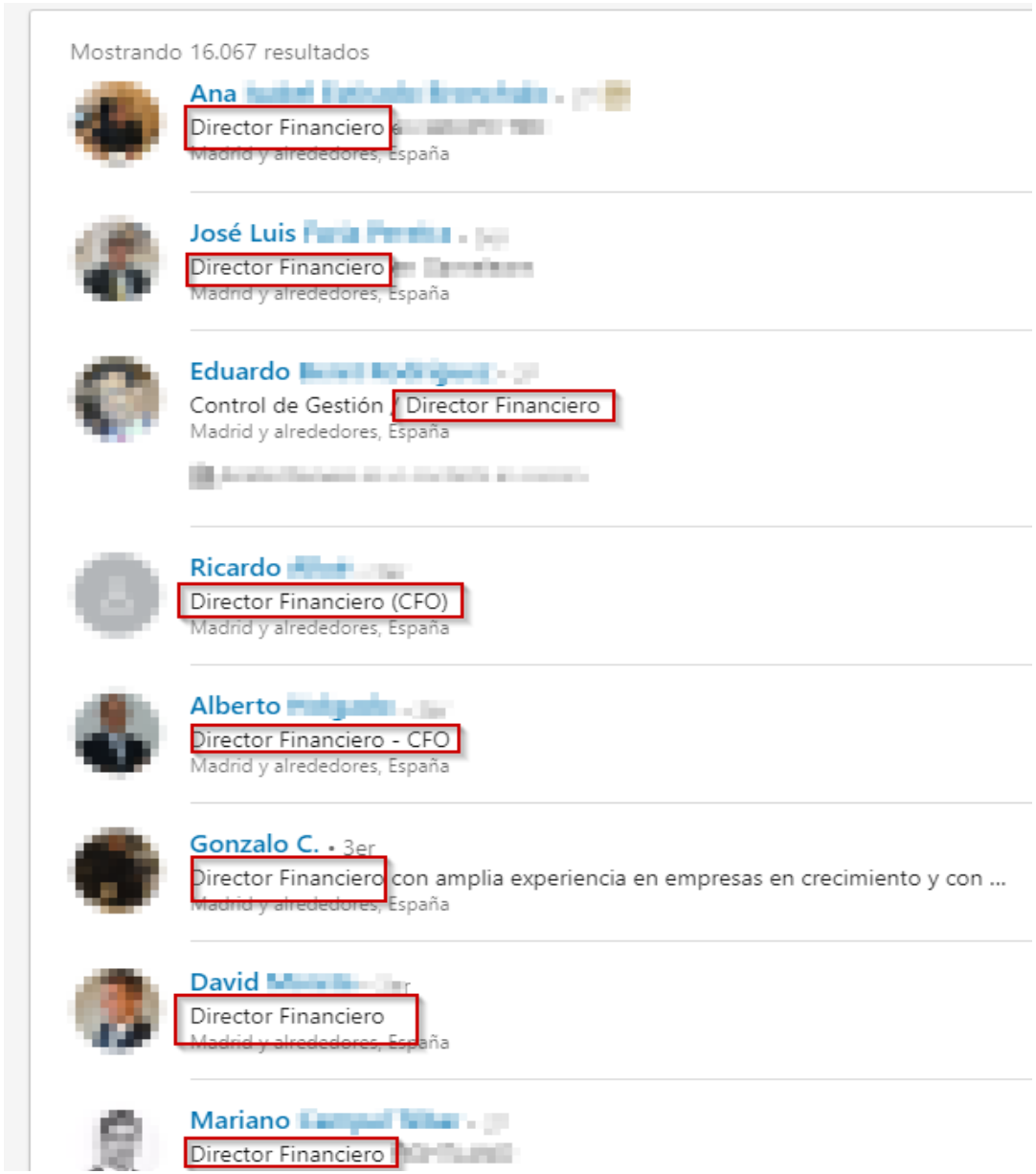
En casos más sofisticados los criminales interceptan las comunicaciones y estudian los correos electrónicos intercambiados durante tiempo de manera concienzuda, para suplantar de forma eficaz a los altos cargos

Estafas al CEO: Fases

Identificar al objetivo. Reconocimiento

- Buscar empresa objetivo
- Buscar empleados de la empresa objetivo
- OSINT: Hunter.io, LinkedIn, Facebook, Twitter, Badoo, Meetic…
- Localizar a las personas de interés (empleados con acceso directo o indirecto al dinero)

Estafas al CEO: Reconocimiento



Comprometer el objetivo/s

- Generación de un **phishing dirigido** a los objetivos (Director Financiero, Director ejecutivo, etc.)
- Ataque al **servidor de correo**:
  - Password Spraying (fuerza bruta por diccionario) contra el servidor de correo y las cuentas para los atacantes
  - Credential Stuffing/Credential reuse: los atacantes prueban de manera automatizada pares de nombres de usuario y contraseñas extraídas de alguna filtración con el fin de obtener acceso a una cuenta. Es posible que se reutilicen contraseñas de por ejemplo redes sociales en cuentas corporativas de la empresa.
  - Fuerza bruta tradicional (poco usada ya que bloquea las cuentas de usuario y puede alertar a los objetivos)

Ejecución de la operación

- Una vez dentro los atacantes **leen los correos de la victima** (CEO,CFO,etc)
  - Existen incluso kits de herramientas como MailSniper que nos permiten hacer búsquedas de palabras clave en entornos como Microsoft Exchange
  - Identifican interlocutores, estudian forma de redacción de los implicados, detalles, etc.
- Una vez llegado el momento adecuado (por ejemplo que el responsable este ausente, de viaje, sin acceso a correo ni móvil, etc.) **suplantan a su objetivo**
- El atacante ha estudiado la forma de redactor de la víctima, conoce las relaciones con sus proveedores, utiliza una situación ficticia en la que se tiene que **actuar con urgencia** y se muestran **precisos e imperativos**

Estafas al CEO: Ejecución

Los cibercriminales se hacen con el botín

- Los atacantes solicitan realizar una o **varias transferencias de dinero**
- El lenguaje es **urgente**: tienen que hacerse ahora mismo
- Habitualmente logran su objetivo
- Se suelen usar **transferencias internacionales**
- Si el fraude no se descubre a tiempo **el dinero es dificil de recuperar** gracias a técnicas de blanqueo de dinero, “mulas”, etc.

Volumen de negocio de las estafas al CEO

Delitos informáticos		Procedimientos judiciales incoados	%
Contra la libertad	Amenazas/coacciones a través de TICs (arts. 169 y ss. y 172 y ss)	568	8,51
	Acoso a través de TICs (art 172 ter)	200	3,00
Contra la integridad moral	Trato degradante a través de TICs (art. 173)	67	1,00
Contra la libertad sexual	Pornografía infantil/discapaces a través de TICs (art. 189)	825	12,36
	Acoso menores a través de TICs (art. 183 ter)	159	2,38
	Otros delitos c/libertad sexual a través TIC	93	1,39
Contra la intimidad	Ataques/interceptación sistemas y datos (art. 197 bis y ter)	87	1,30
	Descubrimiento/revelación secretos a través TIC (art. 197)	466	6,98
Contra el honor	Calumnias/injurias autoridades a través TIC (art. 215)	91	1,36
Contra el patrimonio y el orden socio-económico	Estafa cometida a través de las TICs (arts. 248 y 249)	3.714	55,63
	Descubrimiento secretos empresa a través TIC (arts. 278 y ss.)	43	0,64
	Delitos c/ servicios de radiodifusión/ interactivos (art. 286)	13	0,19
	Delitos de daños informáticos (art. 264, 264 bis y 264 ter)	90	1,35
	Delitos c/ propiedad intelectual a través TIC (arts. 270 y ss.)	53	0,79
De falsedad	Falsificación a través de las TICs	69	1,03
Contra Constitución	Discriminacion a través TIC (art. 510)	77	1,15
Otros		61	0,91
Total		6.676	100,00

- El impacto financiero mundial es importante, en 2017 el FBI hablaba de más de **$3 billones** en pérdidas

Memoria de 2018 de la Fiscalía General del Estado

Estafas al CEO: Noticias

Fraudes en línea

En una operación conjunta entre INTERPOL y la Comisión contra Delitos Económicos y Financieros de Nigeria llevada a cabo en 2016, la policía detuvo al cabecilla de una red delictiva internacional responsable de fraudes en línea por un valor superior a 60 millones de dólares estadounidenses. La red, dirigida por un ciudadano nigeriano conocido como «Mike» y formada por al menos 40 individuos de Nigeria, Malasia y Sudáfrica, tenía como objetivo cientos de víctimas de todo el mundo con varios sistemas de fraude que ponían en compromiso correos electrónicos de empresas.

Estafas al CEO: Noticias

CORRIERE DELLA SERA

MILANO / CRONACA

IL CASO

Tecnimont truffata, la mail del capo era falsa: persi 17 milioni di dollari

Bonifici ordinati da account fittizi. Il manager non vede che nel mittente manca una vocale e fa partire i soldi. Il Gruppo raggirato in India e Arabia. E i giudici di Milano devono fermarsi «per difetto di giurisdizione»

di Luigi Ferrarella

Estafas al CEO: Caso real

S2 GRUPO

Víctima: Fabricantes SL

José Salamanca pregunta a Bea Monreal (ambos de Fabricantes SL) sobre el estado de un pago referente a un pedido, el 120201, al proveedor (chino) Tornillos SA.

Hola Bea,

[redacted] lo pregunto por mail.

necesito saber:

1.- Hemos pagado 3182,04 dolares al prov. 3054 que se llama [redacted]? Este pago debe ser reciente de este año 2012. Es el 30% de la profor
[redacted] 120201.

			7280	$22.546,48
			30% deposit	$3.182,04
			Sticker cost	$400,00
			Blance payment	$19.764,44

Víctima: Fabricantes SL

Bea responde a José que no, así que se paga el 30% acordado al pedido 120201, al proveedor. Este indica que ha recibido el dinero y que comienza su producción. El contacto del cliente es Teresa@tornillos.cc

Dear [redacted]

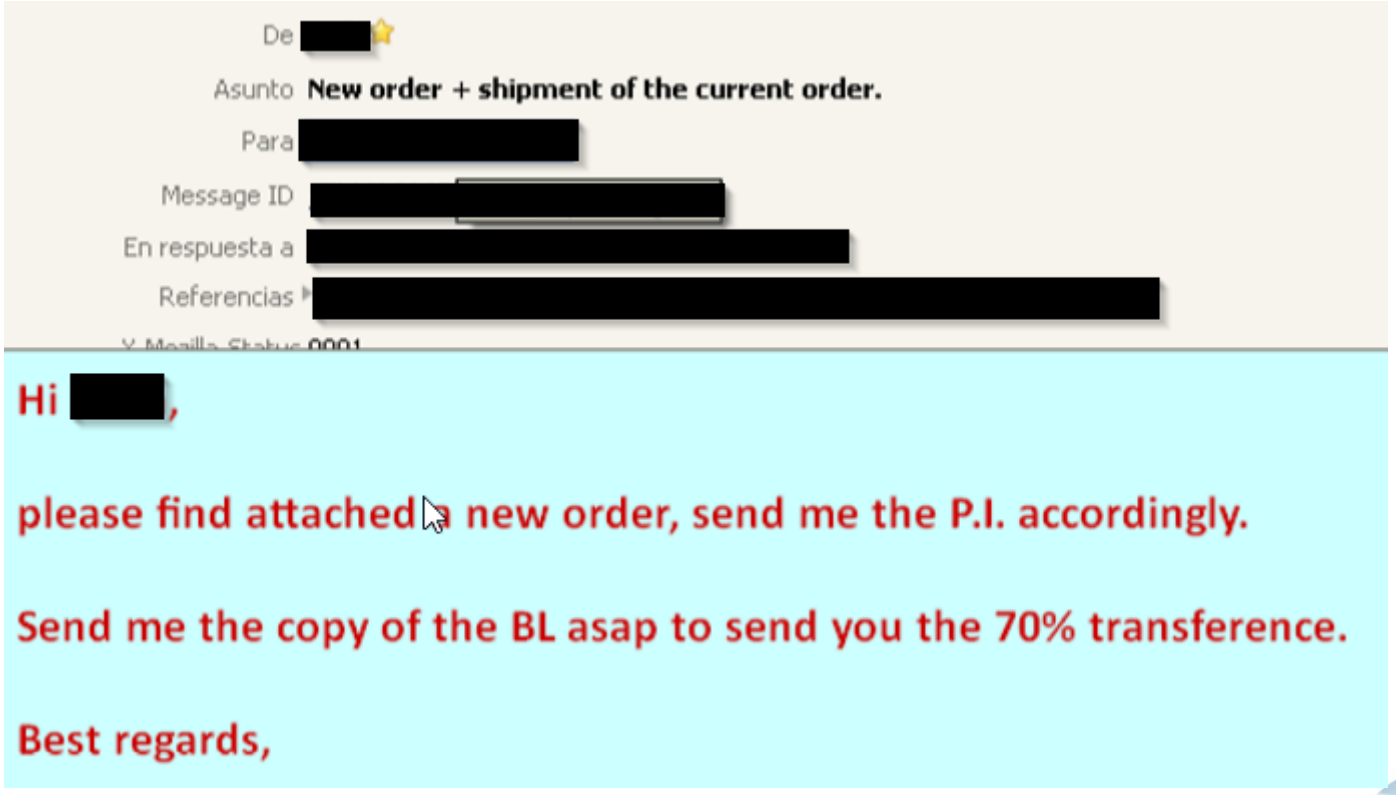
You payment is received eventually , thanks for that . We have started the order , and plan to ship in early June , kindly be noted .

Best regards

2012-04-10

Víctima: Fabricantes SL

Días posteriores, José envía un correo a Teresa@tornillos.cc haciendo un nuevo pedido con código 210612 (anexa el detalle del mismo en un .odt) y le dice que le va a pagar el 70% restante del primer pedido 120201



Víctima: Fabricantes SL

Teresa@tornillos.cc envía un correo a José, poniendo en copia una dirección de correo no reconocida por ellos (Caroltornillos@yahoo.cn) e indicando que no puede abrir el .odt. En la respuesta no viene el .odt

Dear [redacted] ,

Thanks for your new order , but i can not open it , pls could you send me by PDF ? Thanks

To keep you updated , we have just received the S/O from your forwarder , and we will arrange shpt around Jun 26 . Once the shpt is made , we will start send you B/L against balance payment .

Best regards

Se investiga la IP desde donde se envía el correo, cabeceras, etc. y coincide con correos anteriores así que es probable que Teresa haya sido la que ha puesto por primera vez ese nuevo contacto. Pero existe la posibilidad de que se esté usando el equipo de Teresa para suplantar su identidad y comenzar el fraude.

Víctima: Fabricantes SL

caroltornillos@yahoo.cn envía otro correo a José de Fabricantes SL y pone en copia a teresatornillos@yahoo.cn indicando información sobre el segundo pedido que venía descrita en el .odt del correo anterior… en la respuesta no iba anexo el correo así que ¿cómo ha conseguido ese fichero?

1. caroltornillos@yahoo.cn es un correo lícito de la empresa y es la propia Teresa la que se lo hace llegar
2. Un atacante tiene acceso al PC/correo de Teresa@tornillos.cc y ha obtenido el fichero
3. Un atacante tiene acceso al PC/correo de José

Víctima: Fabricantes SL

[redacted]

Responder | Responder a todos | Reenviar | Arch

Asunto **Re: New order + shipment of the current order.**

Para [redacted]

Cc [redacted]@yahoo.cn <[redacted]@yahoo.cn>

Este mensaje puede ser fraudulento.

Desactivar detección de mensajes fraudulentos

Dear [redacted]

This is [redacted] from [redacted] Glad to meet you via E-mail .

Firstly, we no longer use our previous because our webmail is down due to some technical problems. You can contact us anytime on our new email.

Attached herewith,pls find the PI for your new order which has been received yesterday (22-June) and kindly note below :

1. item 1552010500 (our item DB-05B-S) ,we adjust it order qty as 320pcs for each color to make even carton since they are packed as 40pcs/carton .

2. item 1555011500 (our item DB-01-L),to meet with MOQ of color box & sticker ,we adjust order qty as 200pcs for each color

3. item 1555012000 (our item DB-01-XL),the same as above point 2 .

4. At the moment there is about 3cbm space left in one 20ft container . Pls kindly help check whether some items can be added to meet with one 20ft container .

5. ETD : the delivery time is within 70-75 days after 30% deposit is received .

Awaiting your kind confirmation so that we can arrange the mass-production .

Also please take note of our new banking information.

Thanks & best regards

Víctima: Fabricantes SL

El correo se envía desde el Webmail de Yahoo China pero se registra la IP originaria del mensaje:

"Received: from **[41.138.180.104]** by web92412.mail.cnh.yahoo.com **via http**"

"X-Mailer: YahooMailWebService/0.8.118.349524"

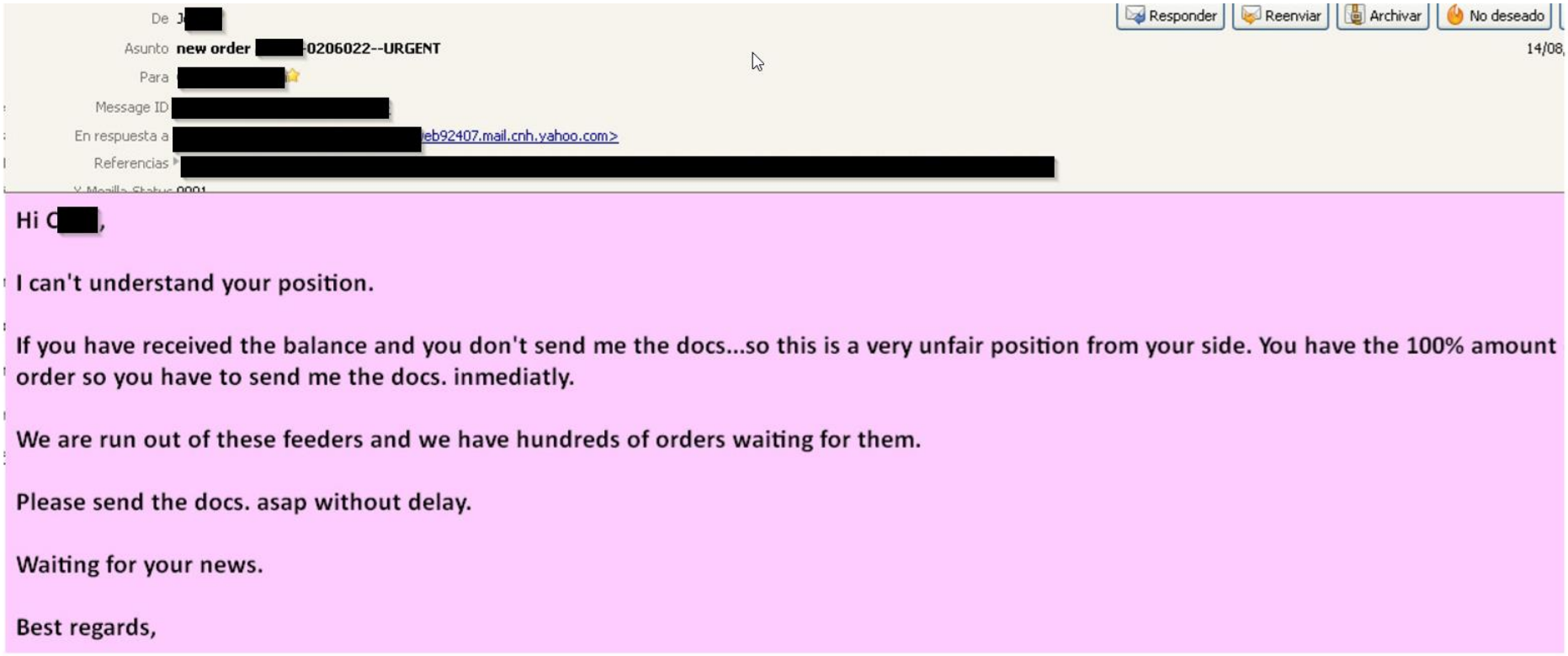
La IP originaria pertenece a Lagos (Nigeria)

Ejecución del engaño

Carol y José se intercambian varios correos recordando incluso que el dinero del primer pedido pendiente se ingrese a la nueva cuenta bancaria

Ejecución del engaño

Fabricantes SL ingresan cerca de $24.000 pero nadie les envía los papeles para que puedan ir al puerto a recoger su pedido…



Ejecución del engaño

Por otro lado también descubrimos que los criminales habían estado haciendo el mismo engaño con la verdadera Teresa de Tornillos SA suplantando a José para que ella no le recriminara el pago de los envíos que tenían pendiente …

Tras la investigación se concluye que el proveedor Tornillos SA situados en China estaba comprometido por una grupo de estafadores aparentemente localizados en Lagos (Nigeria) los cuales tenían acceso a la infraestructura de su red corporativa.

Se revisó la infraestructura de Fabricantes SL y estaba limpia.

PÉRDIDAS DIRECTAS	$30.000
PERDIDAS INDIRECTAS (sin calcular)	Retrasos en la fabricación Desconfianza en el proveedor etc.

Estafas al CEO: Caso práctico

S2 GRUPO

Energía del presente y el futuro

- **MINAF** (Minerías Alcazar y Ferrán)
- Empresa minera que factura 40M€+
- Presencia **internacional**

*Nota: Este caso es 100% ficticio. Lo que no nos hemos inventado son las herramientas y técnicas empleadas por los cibercriminales para llevar a cabo estos ataques

Preparación

- Sistemas y antivirus (razonablemente) actualizados
- Logs activados en el proxy de navegación y correo
- Concienciación de seguridad de usuarios: en proceso....

- El **CEO** va a Estambul a firmar un acuerdo comercial
- Mientras está fuera, se ordenan una serie de **transferencias**
- El CFO realiza las transferencias… que NO fueron pedidas por el CEO

Timeline del incidente

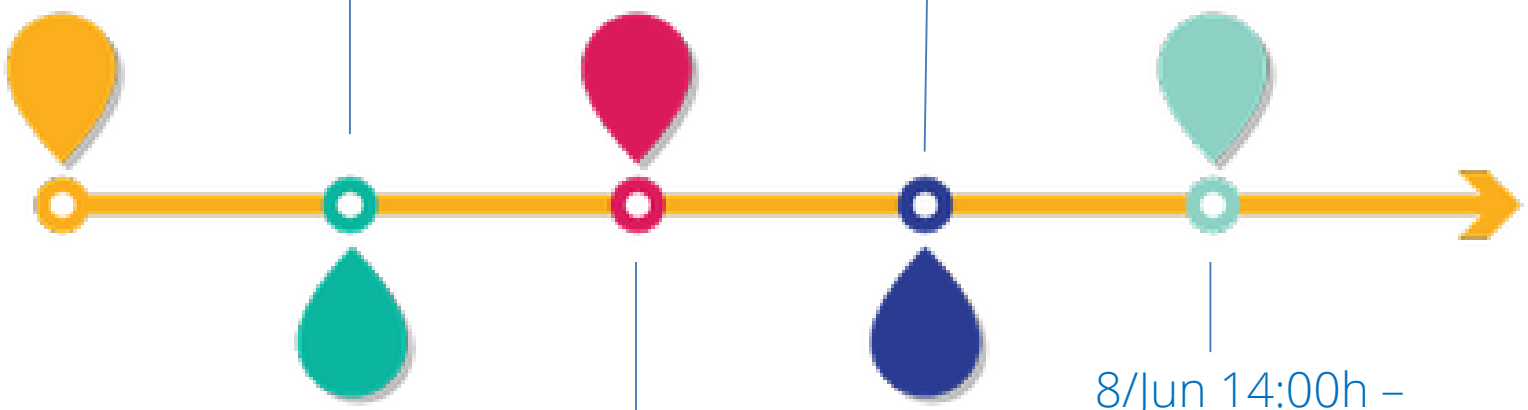
7/Jun 13:00h - Llegada a Estambul

14:00h - Comienzo de las negociaciones

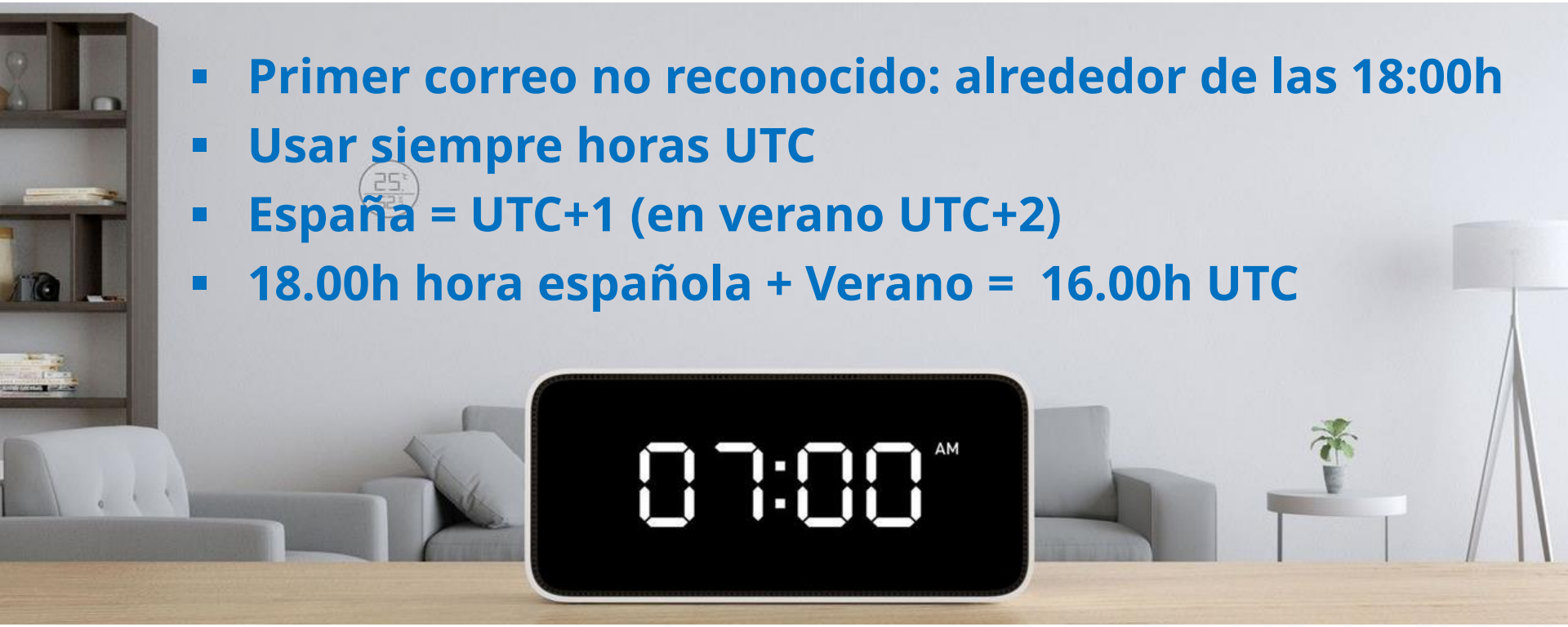
17.00h - Solicitud de transferencias

17:30h - Realización de las transferencias

8/Jun 14:00h – Detección del incidente



Inicio de los eventos sospechosos

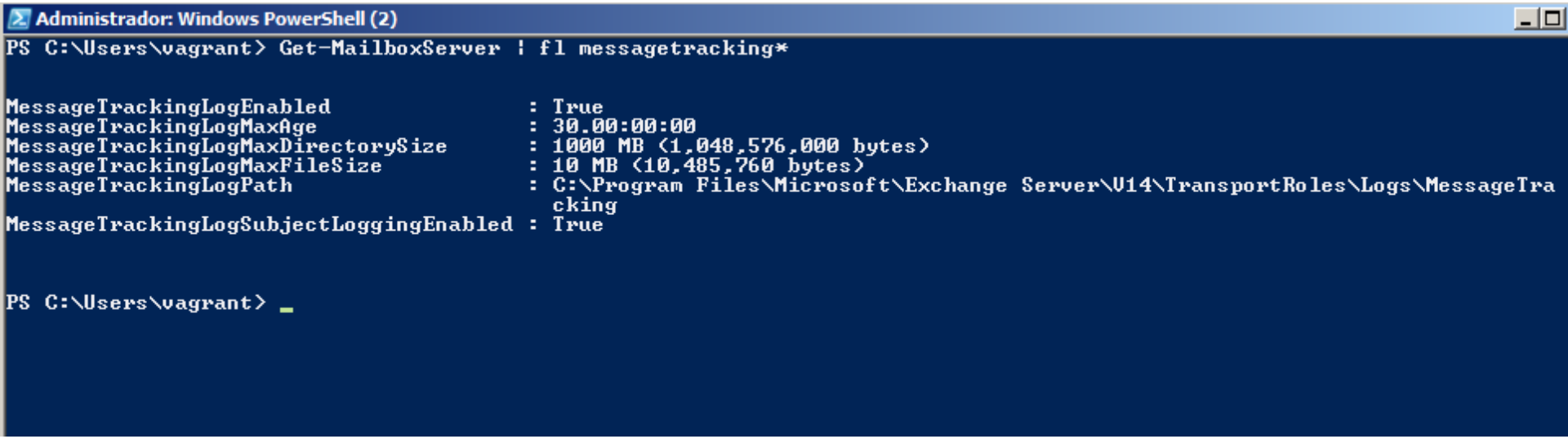


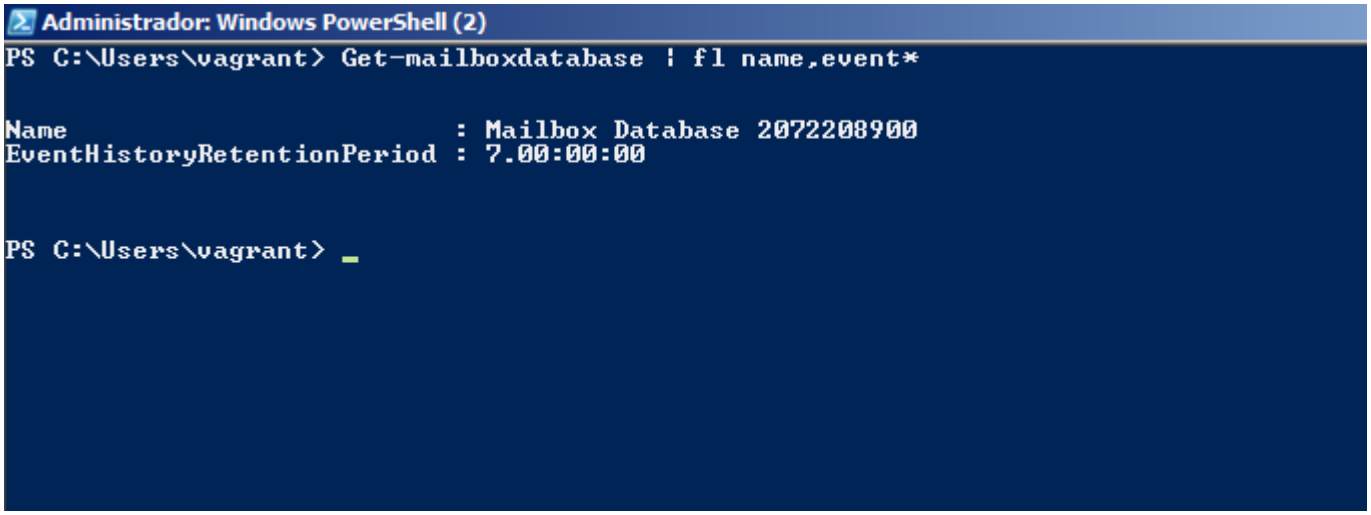
- **Primer correo no reconocido: alrededor de las 18:00h**
- **Usar siempre horas UTC**
- **España = UTC+1 (en verano UTC+2)**
- **18.00h hora española + Verano = 16.00h UTC**

Adquisición de evidencias

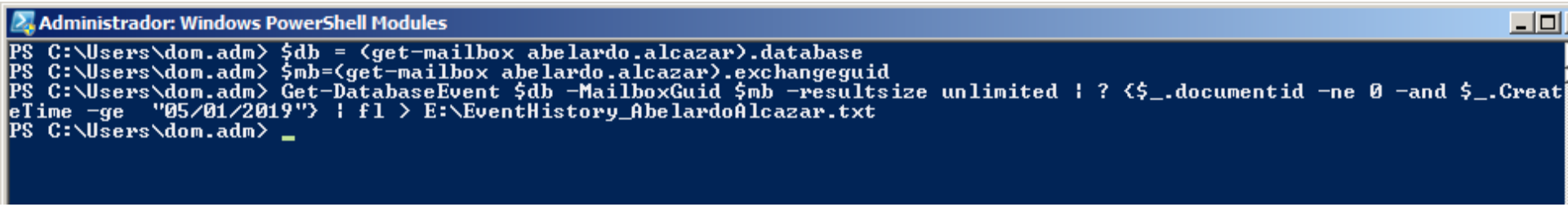
- Volcado de RAM: **winpmem**
- Datos de triage: **CYLR**
- Datos de Exchange: **buzones + MessageTracking + EventHistoryDB**

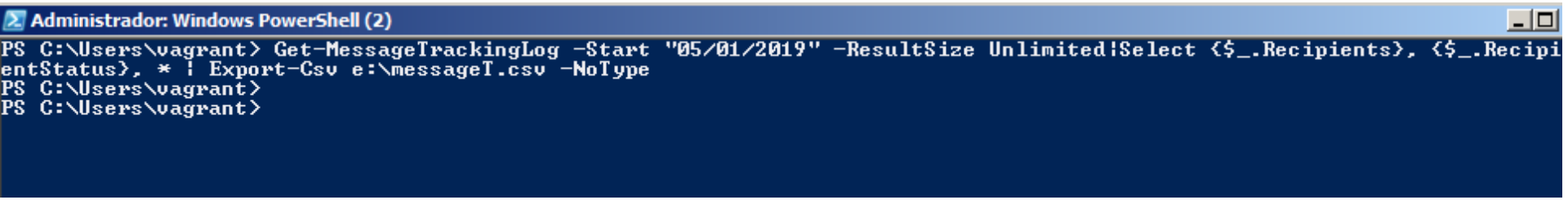
Comprobamos disponibilidad de datos

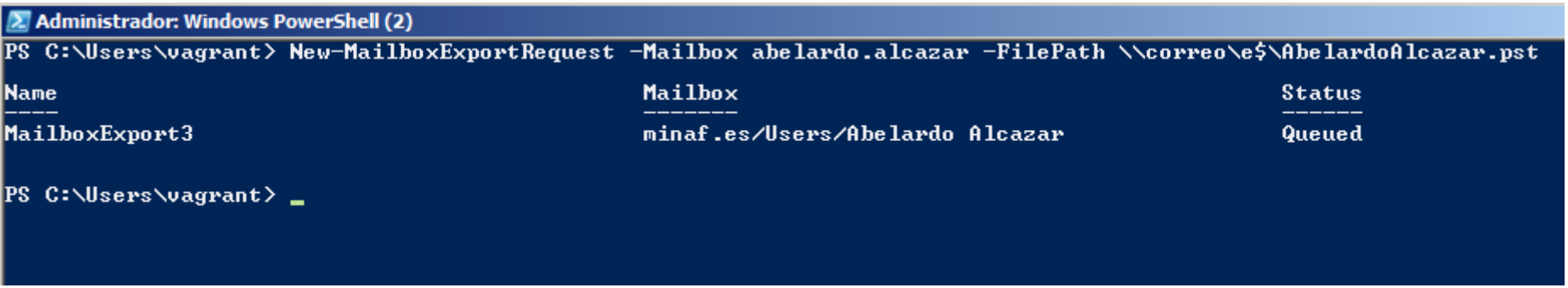




Adquirimos logs de Exchange





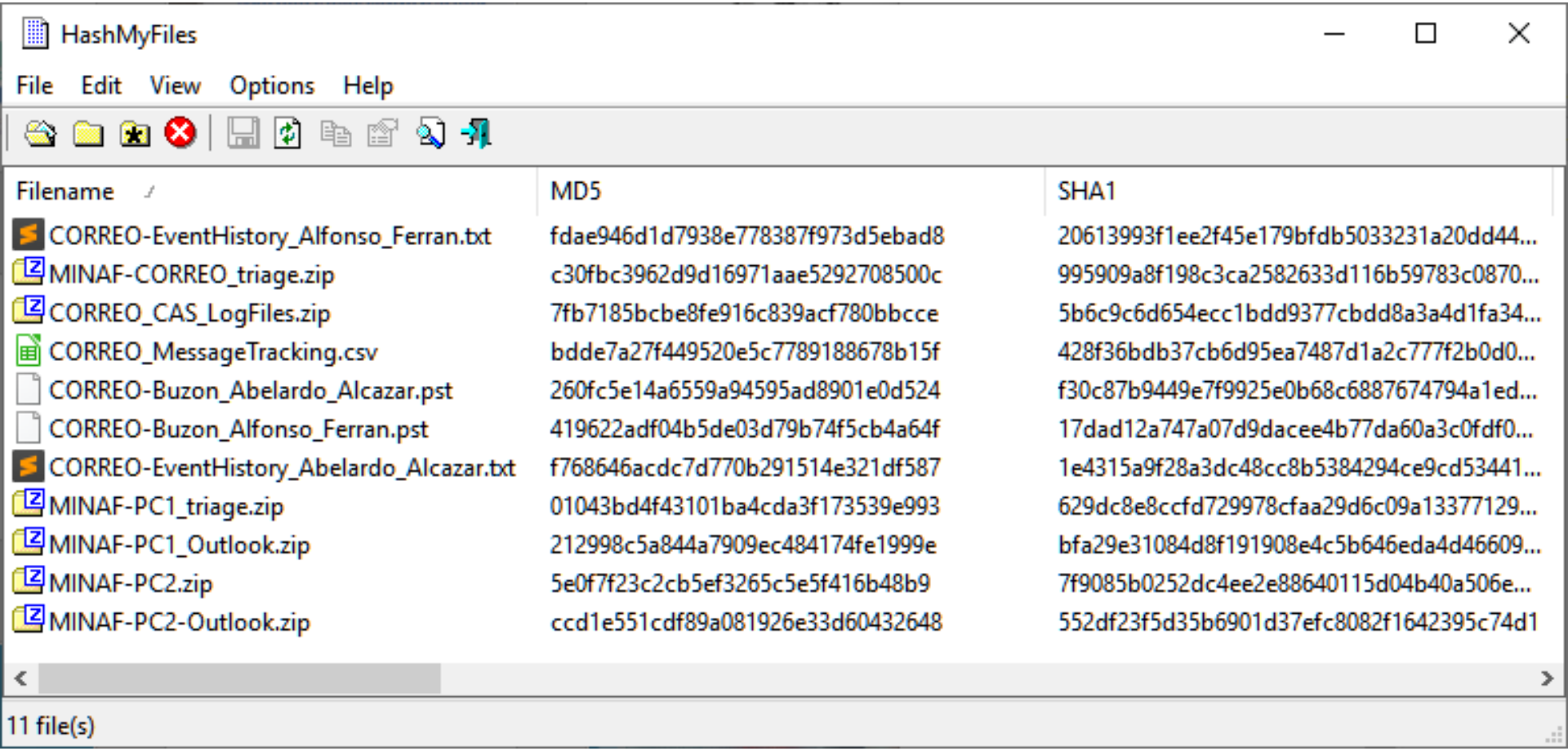


Adquisición

- Entorno sintético en la nube
- !USB → Disco añadido a VM
- Jump the shark with me ☺

Se documenta la adquisición

```
########################################
Ficha de Adquisición de evidencias
########################################

* Caso:  MINAF-001
* Número de adquisición: MINAF-2019-001
* Fecha de captura: 08/07/2019
* Hora de captura: 19:00h
* Persona que realiza la adquisición: Salvador Bendito (técnico de sistemas del MINAF)
* Personas presentes durante la adquisición: Abelardo Alcazar (CEO del MINAF), Alfonso Ferrán (CFO del MINAF),
#074 (analista de respuesta ante incidentes)
* Equipo adquirido: MINAF-PC1, IP 10.11.0.11, MINAF-PC2, IP 10.11.0.12, CORREO, IP 10.11.0.101
* Evidencias adquiridas: Volcado de memoria a través de la herramienta winpmem,
datos de triage a partir de la herramienta CyLR, ejecución de comandos de Powershell en el servidor CORREO
* Ficheros de evidencia (consultar hashes en el fichero hashes.txt):
MINAF-PC1_triage.zip
MINAF-PC1-Outlook.zip
MINAF-PC2_triage.zip
MINAF-PC2-Outlook.zip
MINAF-CORREO_triage.zip
CORREO_CAS_LogFiles.zip
CORREO-MessageTracking.csv
CORREO-EventHistory_Abelardo_Alcazar.txt
CORREO-EventHistory_Alfonso_Ferran.txt
CORREO-Buzon_Abelardo_Alcazar.pst
CORREO-Buzon_Alfonso_Ferran.pst

Procedimiento seguido
---------------------------
Para los puestos de usuario:
- Se inserta un USB con las herramientas en el equipo.
- Se abre un terminal de línea de comandos con privilegios de administrador.
- Se ejecuta la herramienta winpmem.exe con estas opciones:
winpmem --output MINAF-PC1_RAM.mem
```



Verificamos los hashes...

HashMyFiles

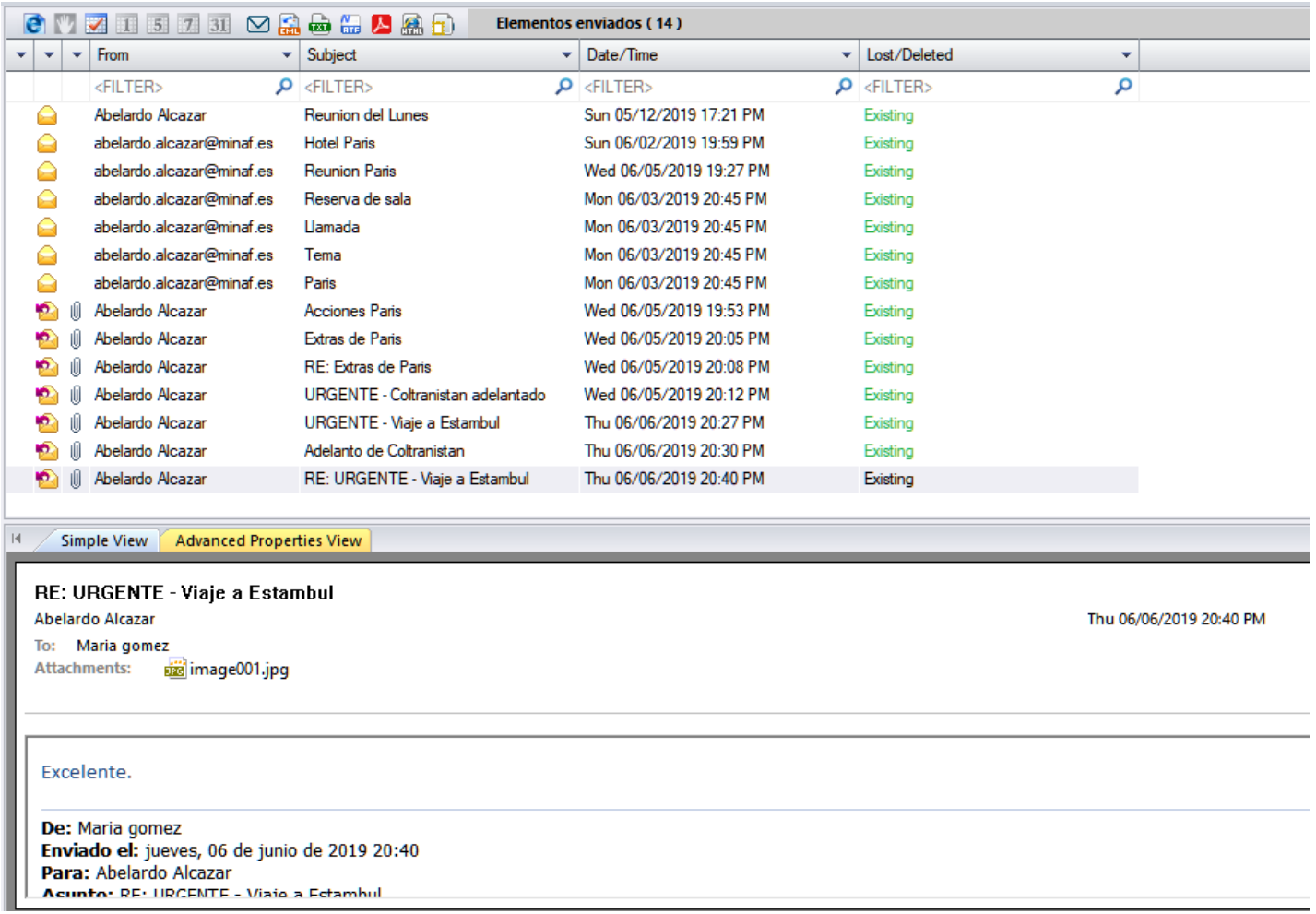
File Edit View Options Help

Filename	MD5	SHA1
CORREO-EventHistory_Alfonso_Ferran.txt	fdae946d1d7938e778387f973d5ebad8	20613993f1ee2f45e179bfdb5033231a20dd44...
MINAF-CORREO_triage.zip	c30fbc3962d9d16971aae5292708500c	995909a8f198c3ca2582633d116b59783c0870...
CORREO_CAS_LogFiles.zip	7fb7185bcbe8fe916c839acf780bbcce	5b6c9c6d654ecc1bdd9377cbdd8a3a4d1fa34...
CORREO_MessageTracking.csv	bdde7a27f449520e5c7789188678b15f	428f36bdb37cb6d95ea7487d1a2c777f2b0d0...
CORREO-Buzon_Abelardo_Alcazar.pst	260fc5e14a6559a94595ad8901e0d524	f30c87b9449e7f9925e0b68c6887674794a1ed...
CORREO-Buzon_Alfonso_Ferran.pst	419622adf04b5de03d79b74f5cb4a64f	17dad12a747a07d9dacee4b77da60a3c0fdf0...
CORREO-EventHistory_Abelardo_Alcazar.txt	f768646acdc7d770b291514e321df587	1e4315a9f28a3dc48cc8b5384294ce9cd53441...
MINAF-PC1_triage.zip	01043bd4f43101ba4cda3f173539e993	629dc8e8ccfd729978cfaa29d6c09a13377129...
MINAF-PC1_Outlook.zip	212998c5a844a7909ec484174fe1999e	bfa29e31084d8f191908e4c5b646eda4d46609...
MINAF-PC2.zip	5e0f7f23c2cb5ef3265c5e5f416b48b9	7f9085b0252dc4ee2e88640115d04b40a506e...
MINAF-PC2-Outlook.zip	ccd1e551cdf89a081926e33d60432648	552df23f5d35b6901d37efc8082f1642395c74d1

11 file(s)

!Y comprobamos que un hash no coincide!

Análisis del correo del equipo del CEO



Elementos enviados (14)

From	Subject	Date/Time	Lost/Deleted
<FILTER>	<FILTER>	<FILTER>	<FILTER>
Abelardo Alcazar	Reunion del Lunes	Sun 05/12/2019 17:21 PM	Existing
abelardo.alcazar@minaf.es	Hotel Paris	Sun 06/02/2019 19:59 PM	Existing
abelardo.alcazar@minaf.es	Reunion Paris	Wed 06/05/2019 19:27 PM	Existing
abelardo.alcazar@minaf.es	Reserva de sala	Mon 06/03/2019 20:45 PM	Existing
abelardo.alcazar@minaf.es	Llamada	Mon 06/03/2019 20:45 PM	Existing
abelardo.alcazar@minaf.es	Tema	Mon 06/03/2019 20:45 PM	Existing
abelardo.alcazar@minaf.es	Paris	Mon 06/03/2019 20:45 PM	Existing
Abelardo Alcazar	Acciones Paris	Wed 06/05/2019 19:53 PM	Existing
Abelardo Alcazar	Extras de Paris	Wed 06/05/2019 20:05 PM	Existing
Abelardo Alcazar	RE: Extras de Paris	Wed 06/05/2019 20:08 PM	Existing
Abelardo Alcazar	URGENTE - Coltranistan adelantado	Wed 06/05/2019 20:12 PM	Existing
Abelardo Alcazar	URGENTE - Viaje a Estambul	Thu 06/06/2019 20:27 PM	Existing
Abelardo Alcazar	Adelanto de Coltranistan	Thu 06/06/2019 20:30 PM	Existing
Abelardo Alcazar	RE: URGENTE - Viaje a Estambul	Thu 06/06/2019 20:40 PM	Existing

Simple View | Advanced Properties View

RE: URGENTE - Viaje a Estambul

Abelardo Alcazar

Thu 06/06/2019 20:40 PM

To: Maria gomez

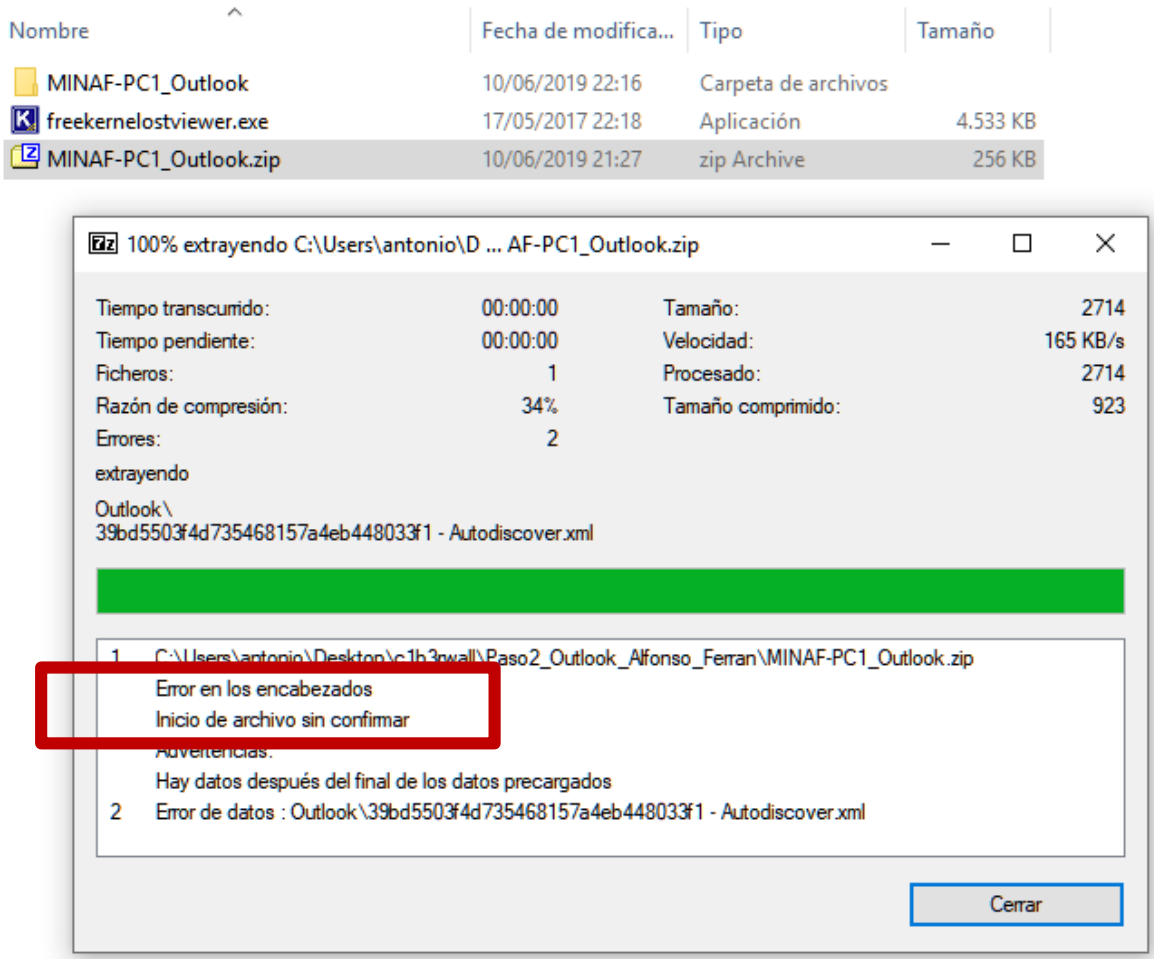
Attachments: image001.jpg

Excelente.

De: Maria gomez
Enviado el: jueves, 06 de junio de 2019 20:40
Para: Abelardo Alcazar
Asunto: RE: URGENTE - Viaje a Estambul

No hay nada enviado el 7 de Junio…

Análisis del correo del equipo del CFO



El fichero está corrupto … ☹

MessageTracking

	A	B	C	D	E	F
1	Timestamp	Sender	$_.Recipients	MessageSubject	Source	EventId
2	02/06/2019 19:33:37				STOREDRIVER	NOTIFYMAPI
3	02/06/2019 19:33:38	alfonso.ferran@minaf.es	maria.gomez@minaf.es	Reunion con Abelardo	STOREDRIVER	RECEIVE
4	02/06/2019 19:33:38	alfonso.ferran@minaf.es		Reunion con Abelardo	STOREDRIVER	SUBMIT
5	02/06/2019 19:33:39	alfonso.ferran@minaf.es	maria.gomez@minaf.es	Reunion con Abelardo	STOREDRIVER	DELIVER
6	02/06/2019 19:59:38	abelardo.alcazar@minaf.es	maria.gomez@minaf.es	Hotel Paris	STOREDRIVER	RECEIVE
7	02/06/2019 19:59:38	abelardo.alcazar@minaf.es	maria.gomez@minaf.es	Hotel Paris	STOREDRIVER	DELIVER
8	02/06/2019 19:59:38				STOREDRIVER	NOTIFYMAPI
9	02/06/2019 19:59:38	abelardo.alcazar@minaf.es		Hotel Paris	STOREDRIVER	SUBMIT
10	02/06/2019 20:03:02	maria.gomez@minaf.es	abelardo.alcazar@minaf.es	RE: Hotel Paris	STOREDRIVER	RECEIVE
11	02/06/2019 20:03:02	maria.gomez@minaf.es	abelardo.alcazar@minaf.es	RE: Hotel Paris	STOREDRIVER	DELIVER
12	02/06/2019 20:03:02				STOREDRIVER	NOTIFYMAPI
13	02/06/2019 20:03:02	maria.gomez@minaf.es		RE: Hotel Paris	STOREDRIVER	SUBMIT
14	03/06/2019 20:45:53				STOREDRIVER	NOTIFYMAPI

- Log de **alto nivel** de la actividad del servidor
- Recoge fecha, origen, destino, asunto
- Recoge metadatos de bajo nivel
- Excelente para una **primera toma de contacto**

MessageTracking

MDB:36477b65-a1ba-47a8-9970-2d856e87dd2c, Mailbox:9fee0121-8902-4013-81f9-6eb7a2d19a9f, Event:7372, MessageClass:IPM.Note.Exchange.ActiveSync.RemoteWipeConfirmation, CreationTime:2019-06-07T18:47:03.970Z, ClientType:AirSync

Confirmacion de la eliminacion remota de datos del dispositivo movil

abelardo.alcazar@minaf.es

- Miles de eventos repetidos
- Se ha solicitado el **borrado remoto** del terminal de abelardo.alcazar (CEO del MINAF)
- Fecha: 07/Jun – 18:47:05 UTC

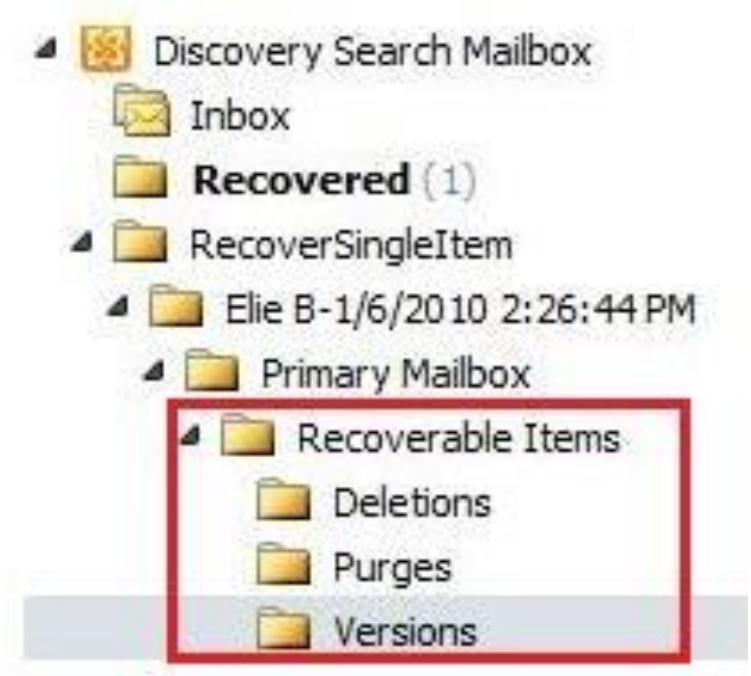
MessageTracking

07/06/2019 17:54:42	alfonso.ferran@minaf.es	abelardo.alcazar@minaf.es	RE: Adelanto de Coltranistan	STOREDRIVER	DELIVER
07/06/2019 17:54:42	alfonso.ferran@minaf.es		RE: Adelanto de Coltranistan	STOREDRIVER	SUBMIT
07/06/2019 18:02:01	abelardo.alcazar@minaf.es	alfonso.ferran@minaf.es	Transferencias COBALTO	STOREDRIVER	RECEIVE
07/06/2019 18:02:01	abelardo.alcazar@minaf.es	alfonso.ferran@minaf.es	Transferencias COBALTO	STOREDRIVER	DELIVER
07/06/2019 18:02:01				STOREDRIVER	NOTIFYMAPI
07/06/2019 18:02:01	abelardo.alcazar@minaf.es		Transferencias COBALTO	STOREDRIVER	SUBMIT
07/06/2019 18:04:44	alfonso.ferran@minaf.es	abelardo.alcazar@minaf.es	RE: Transferencias COBALTO	STOREDRIVER	RECEIVE
07/06/2019 18:04:44	alfonso.ferran@minaf.es	abelardo.alcazar@minaf.es	RE: Transferencias COBALTO	STOREDRIVER	DELIVER
07/06/2019 18:04:44				STOREDRIVER	NOTIFYMAPI
07/06/2019 18:04:44	alfonso.ferran@minaf.es		RE: Transferencias COBALTO	STOREDRIVER	SUBMIT
07/06/2019 18:05:26	abelardo.alcazar@minaf.es	alfonso.ferran@minaf.es	Re: Transferencias COBALTO	STOREDRIVER	RECEIVE
07/06/2019 18:05:26	abelardo.alcazar@minaf.es	alfonso.ferran@minaf.es	Re: Transferencias COBALTO	STOREDRIVER	DELIVER
07/06/2019 18:05:26				STOREDRIVER	NOTIFYMAPI
07/06/2019 18:05:26	abelardo.alcazar@minaf.es		Re: Transferencias COBALTO	STOREDRIVER	SUBMIT
07/06/2019 18:06:53	alfonso.ferran@minaf.es	abelardo.alcazar@minaf.es	RE: Transferencias COBALTO	STOREDRIVER	RECEIVE
07/06/2019 18:06:53	alfonso.ferran@minaf.es	abelardo.alcazar@minaf.es	RE: Transferencias COBALTO	STOREDRIVER	DELIVER
07/06/2019 18:06:53				STOREDRIVER	NOTIFYMAPI
07/06/2019 18:06:53	alfonso.ferran@minaf.es		RE: Transferencias COBALTO	STOREDRIVER	SUBMIT
07/06/2019 18:08:02	abelardo.alcazar@minaf.es	alfonso.ferran@minaf.es	Re: Transferencias COBALTO	STOREDRIVER	RECEIVE
07/06/2019 18:08:02	abelardo.alcazar@minaf.es	alfonso.ferran@minaf.es	Re: Transferencias COBALTO	STOREDRIVER	DELIVER
07/06/2019 18:08:02				STOREDRIVER	NOTIFYMAPI
07/06/2019 18:08:02	abelardo.alcazar@minaf.es		Re: Transferencias COBALTO	STOREDRIVER	SUBMIT
07/06/2019 18:18:45				STOREDRIVER	NOTIFYMAPI
07/06/2019 18:18:46	alfonso.ferran@minaf.es	abelardo.alcazar@minaf.es	RE: Transferencias COBALTO	STOREDRIVER	RECEIVE
07/06/2019 18:18:46	alfonso.ferran@minaf.es	abelardo.alcazar@minaf.es	RE: Transferencias COBALTO	STOREDRIVER	DELIVER
07/06/2019 18:18:46	alfonso.ferran@minaf.es		RE: Transferencias COBALTO	STOREDRIVER	SUBMIT
07/06/2019 18:19:08	abelardo.alcazar@minaf.es	alfonso.ferran@minaf.es	Re: Transferencias COBALTO	STOREDRIVER	RECEIVE
07/06/2019 18:19:08				STOREDRIVER	NOTIFYMAPI
07/06/2019 18:19:09	abelardo.alcazar@minaf.es	alfonso.ferran@minaf.es	Re: Transferencias COBALTO	STOREDRIVER	DELIVER
07/06/2019 18:19:09	abelardo.alcazar@minaf.es		Re: Transferencias COBALTO	STOREDRIVER	SUBMIT
07/06/2019 20:39:16	abelardo.alcazar@minaf.es	alfonso.ferran@minaf.es	Coltranistan ok	STOREDRIVER	RECEIVE
07/06/2019 20:39:16	abelardo.alcazar@minaf.es	alfonso.ferran@minaf.es	Coltranistan ok	STOREDRIVER	DELIVER
07/06/2019 20:39:16				STOREDRIVER	NOTIFYMAPI
07/06/2019 20:39:16	abelardo.alcazar@minaf.es		Coltranistan ok	STOREDRIVER	SUBMIT
07/06/2019 20:45:26	alfonso.ferran@minaf.es	abelardo.alcazar@minaf.es	RE: Coltranistan ok	STOREDRIVER	RECEIVE
07/06/2019 20:45:26	alfonso.ferran@minaf.es	abelardo.alcazar@minaf.es	RE: Coltranistan ok	STOREDRIVER	DELIVER
07/06/2019 20:45:26				STOREDRIVER	NOTIFYMAPI

Qué sabemos hasta ahora…

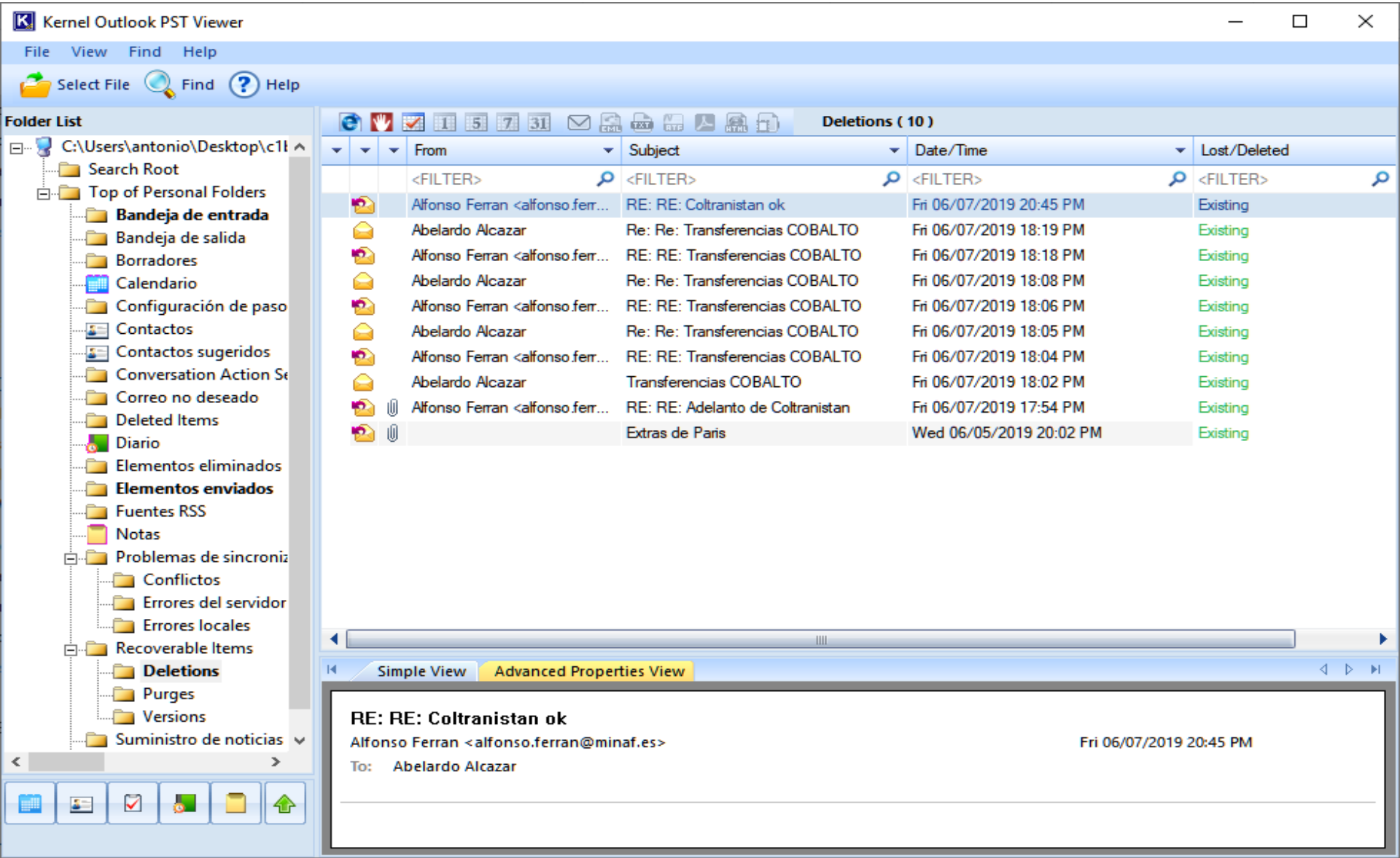
- El CEO **no** reconoce los correos de COBALTO
- **Sí** que envió el correo de “Coltranistán OK”
- Asegura **no** haber recibido la respuesta del CFO (alfonso.ferran)
- Su móvil dejó de funcionar poco después….

Exchange: Elementos recuperables

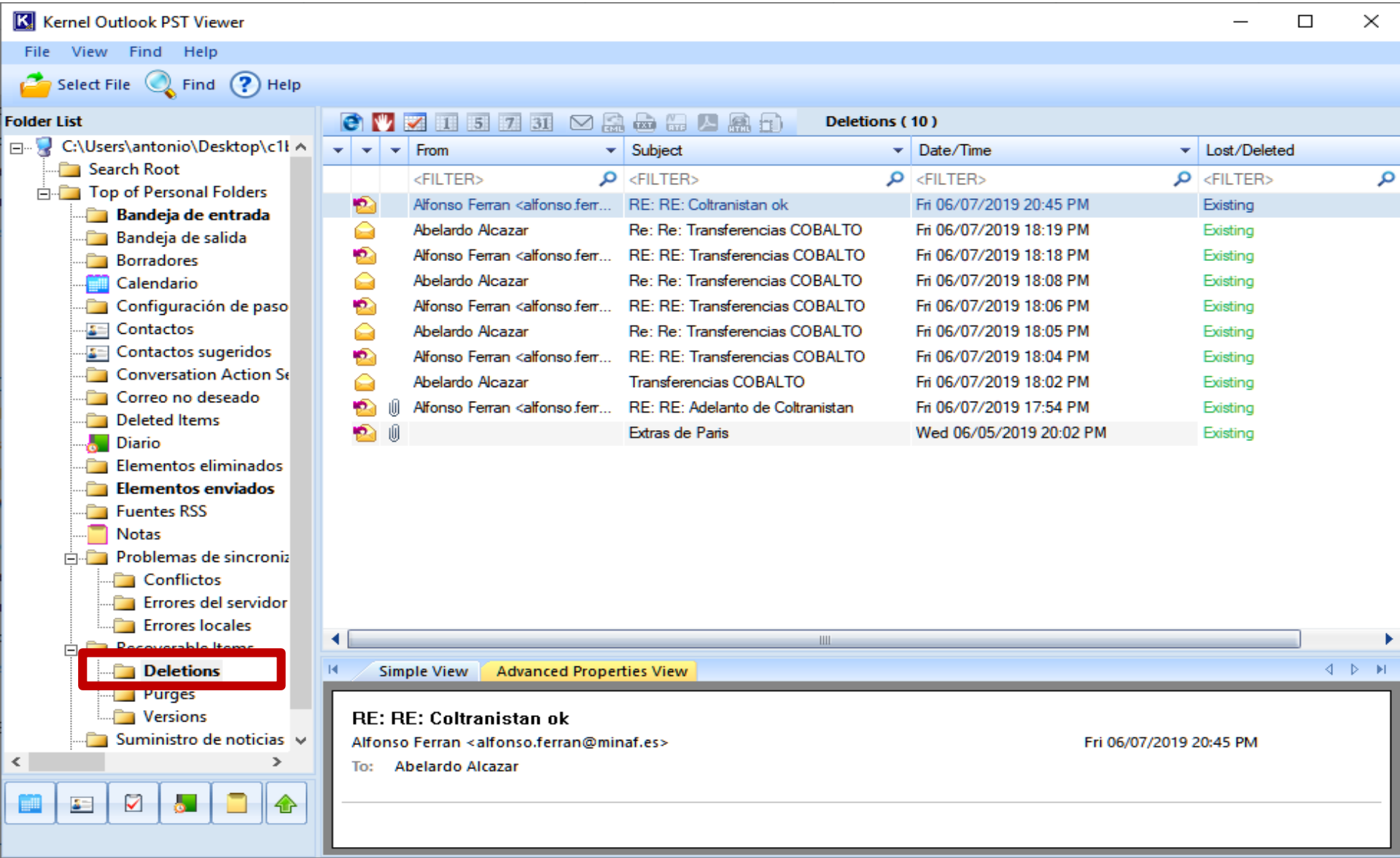


- "**Papelera**" de Exchange
- **Invisible** al usuario
- Guarda correos y ++
- Valor por defecto: **14 días / 30Gb**

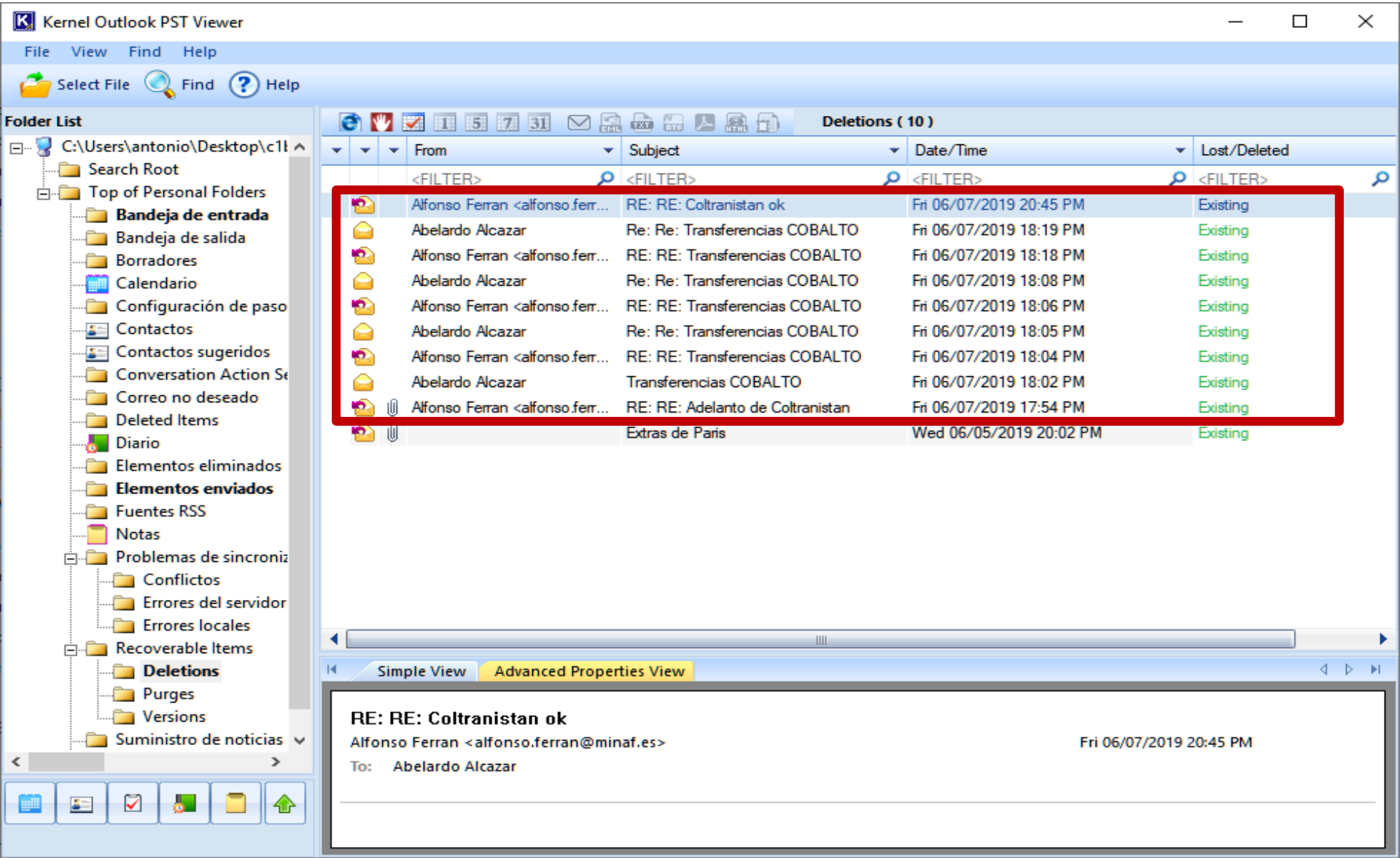
Recuperamos el buzón del CEO



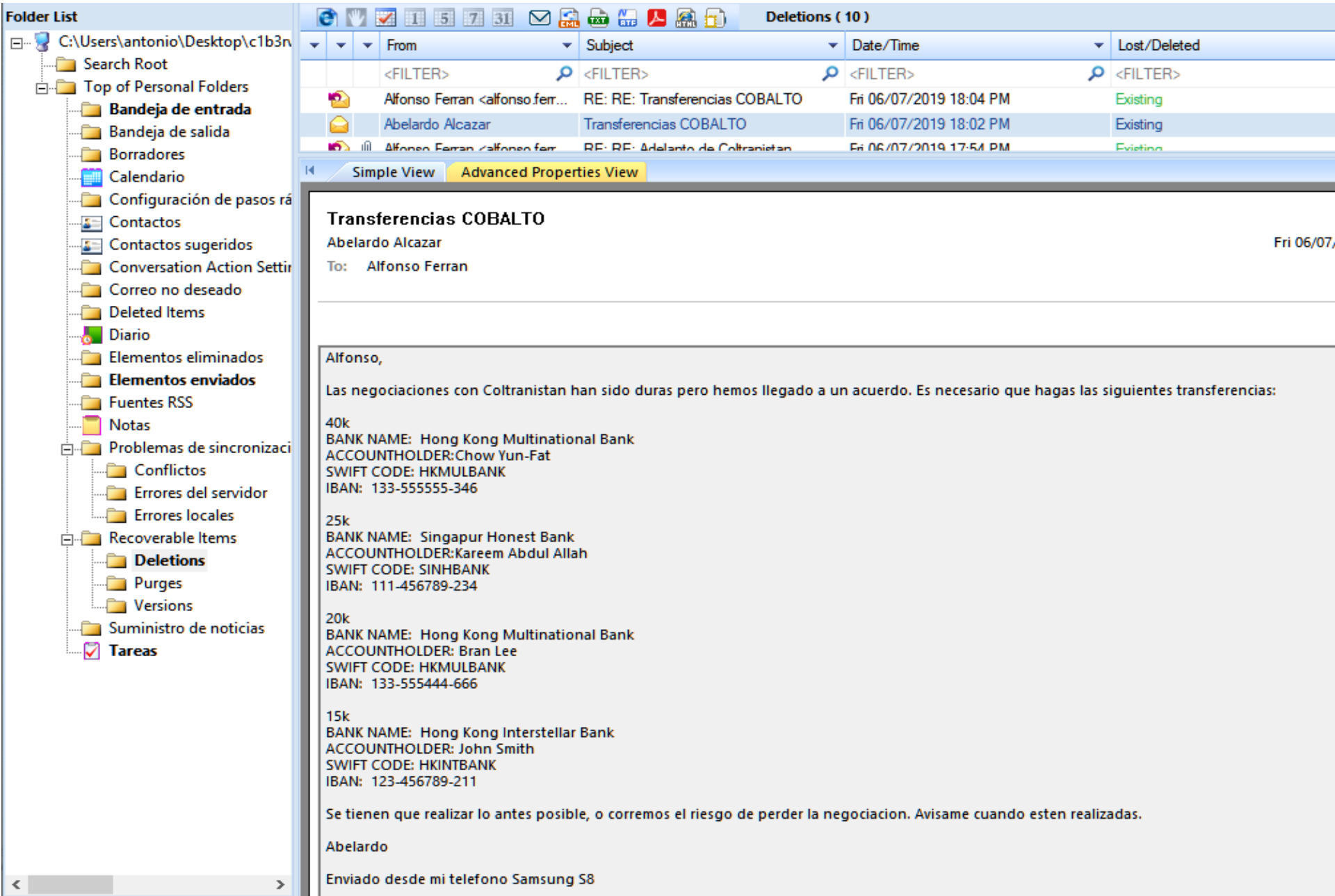
Recuperamos el buzón del CEO



Recuperamos el buzón del CEO



Paso 4: Exchange CEO



Paso 4: Exchange CEO

RE: RE: Transferencias COBALTO

Alfonso Ferran <alfonso.ferran@minaf.es> Fri 06/07/2019 18:04 PM

To: Abelardo Alcazar

Estimado Abelardo,

Es un importe bastante elevado. ¿Estamos seguros de que es absolutamente necesario?

Saludos,

Alfonso Ferran

Re: Re: Transferencias COBALTO

Abelardo Alcazar Fri 06/07/2019 18:05 PM

To: Alfonso Ferran

Alfonso,

Nos estamos jugando un contrato de muchos millones. Hazlo.

Abelardo.

Paso 4: Exchange CEO

RE: RE: Transferencias COBALTO

Alfonso Ferran <alfonso.ferran@minaf.es> Fri 06/07/2019 18:06 PM

To: Abelardo Alcazar

Estimado Alfonso

Realizar tal volumen de transferencias va a ser luego complicado de explicar en nuestras cuentas o si tenemos una auditoria seria. De verdad, no lo recomiendo.

Atentamente,

Alfonso

Re: Re: Transferencias COBALTO

Abelardo Alcazar Fri 06/07/2019 18:08 PM

To: Alfonso Ferran

Alfonso,

Haz las transferencias. Ya veremos luego como lo arreglamos.

Abelardo

Paso 4: Exchange CEO

RE: RE: Transferencias COBALTO

Alfonso Ferran <alfonso.ferran@minaf.es> Fri 06/07/2019 18:18 PM

To: Abelardo Alcazar

Estimado Abelardo,

Ya están realizadas las transferencias.

Atentamente,

Alfonso

Re: Re: Transferencias COBALTO

Abelardo Alcazar Fri 06/07/2019 18:19 PM

To: Alfonso Ferran

Excelente

Paso 4: Exchange CEO

Coltranistan ok

abelardo.alcazar@minaf.es

Fri 06/07/2019 20:39 PM

To: Alfonso Ferran

Alfonso,

Las negociaciones han ido como la seda. Al final no vamos a necesitar nada de COBALTO, estan ansiosos de trabajar con nosotros.

Me quedo a dormir aqui y vuelvo a Madrid el sabado, el lunes concretamos.

Abelardo

Enviado desde mi Samsung S9

RE: RE: Coltranistan ok

Alfonso Ferran <alfonso.ferran@minaf.es>

Fri 06/07/2019 20:45 PM

To: Abelardo Alcazar

Pero no me habias dicho hace un par de horas que realizara 4 transferencias?

Exchange: **EventHistoryDB**

- Recoge **eventos** del correo
- Extremadamente **minucioso**
- Accesible con **Powershell**
- Por defecto: **7 días**

EventHistoryDB: Ejemplo

```
Counter          : 2938
CreateTime       : 02/06/2019 17:08:44
ItemType         : MAPI_MESSAGE
EventName        : ObjectModified
Flags            : FolderAssociated, ObjectClassTruncated
MailboxGuid      : 9fee0121-8902-4013-81f9-6eb7a2d19a9f
ObjectClass      : IPM.Microsoft.OSC.SyncLock.{BC2F3794-4509-4896-83CA-352D354
ItemEntryId      : 0000000004494C2A79DA0243970AABE82DA0BDE50700255F532116B8DC41A61899E7574052690000000032D22C0000255F5321
                   16B8DC41A61899E757405269000000334E640000
ParentEntryId    : 0000000004494C2A79DA0243970AABE82DA0BDE50100255F532116B8DC41A61899E757405269000000032D22C0000
OldItemEntryId   :
OldParentEntryId :
ItemCount        : 0
UnreadItemCount  : 0
ExtendedFlags    : 2147483843
ClientCategory   : MOMT
PrincipalName    : NT AUTHORITY\SYSTEM
PrincipalSid     : S-1-5-18
Database         : Mailbox Database 2072208900
DocumentId       : 10021
```

- ItemEntryID: Identificador único
- EventName: Lo que le sucede al mensaje
- ClientCategory: Desde dónde se ha hecho

Metadatos de correos interesantes del MessageTracking

```
Mensaje 1: (Supuesto primer mensaje de los atacantes)

* Fecha: 07/06/2019 18:02:01
* From: abelardo.alcazar@minaf.es
* To: alfonso.ferran@minaf.es
* Asunto: Transferencias COBALTO
* EventData:
[ItemEntryId, 0000000004494C2A79DA0243970AABE82DA0BDE50700255F532116B8DC41A61899E7574052690000032D22
D0000255F532116B8DC41A61899E7574052690000D3CE75E0000]

Mensaje 2: (Mensaje enviado por Alfonso Ferrán y no recibido por Abelardo Alcazar)

* Fecha: 07/06/2019 20:45:26
* From: alfonso.ferran@minaf.es
* To: abelardo.alcazar@minaf.es
* Asunto: RE: Coltranistan ok
*EventData:
[ItemEntryId, 00000000086EC9F1EB309E49BAEB131E3F7B951C0700D4484CCEA6D15C44936B0FD468845C2C00000024D48
00000D4484CCEA6D15C44936B0FD468845C2C00000D2ECF9B0000]
```

Primer correo falso: 7/Jun 18:02:01h

```
C:\Users\antonio\Desktop\c1b3rwall\Paso5_EventHistoyDB>grep 1899E75740526900000D3CE75E0000 CORREO-EventHistory_Abelardo
Alcazar.txt

C:\Users\antonio\Desktop\c1b3rwall\Paso5_EventHistoyDB>less CORREO-EventHistory_Abelardo_Alcazar.txt
"CORREO-EventHistory_Abelardo_Alcazar.txt" may be a binary file.  See it anyway?

C:\Users\antonio\Desktop\c1b3rwall\Paso5_EventHistoyDB>type CORREO-EventHistory_Abelardo_Alcazar.txt > EventHistoryDB_A
elardo_Alcazar_convertido.txt

C:\Users\antonio\Desktop\c1b3rwall\Paso5_EventHistoyDB>grep 1899E75740526900000D3CE75E0000  EventHistoryDB_Abelardo_Alc
zar_convertido.txt
                  16B8DC41A61899E75740526900000D3CE75E0000
                  16B8DC41A61899E75740526900000D3CE75E0000
                  16B8DC41A61899E75740526900000D3CE75E0000
                  16B8DC41A61899E75740526900000D3CE75E0000
                  16B8DC41A61899E75740526900000D3CE75E0000
                  16B8DC41A61899E75740526900000D3CE75E0000
                  16B8DC41A61899E75740526900000D3CE75E0000
                  16B8DC41A61899E75740526900000D3CE75E0000
                  16B8DC41A61899E75740526900000D3CE75E0000
                  16B8DC41A61899E75740526900000D3CE75E0000
                  16B8DC41A61899E75740526900000D3CE75E0000

C:\Users\antonio\Desktop\c1b3rwall\Paso5_EventHistoyDB>grep -B 8 -A 11 3CE75E0000 EventHistoryDB_Abelardo_Alcazar_conve
tido.txt > primer_mensaje_historia.txt

C:\Users\antonio\Desktop\c1b3rwall\Paso5_EventHistoyDB>
```

- Existen caracteres binarios en la salida
- Hay que convertir el fichero

!Encontramos el correo!

```
--
Counter          : 6572
CreateTime       : 07/06/2019 16:02:01
ItemType         : MAPI_MESSAGE
EventName        : ObjectModified
Flags            : None
MailboxGuid      : 9fee0121-8902-4013-81f9-6eb7a2d19a9f
ObjectClass      : IPM.Note
ItemEntryId      : 0000000004494C2A79DA0243970AABE82DA0BDE50700255F532116B8DC41A61899E7574052690000032D22D0000255F5321
                   16B8DC41A61899E7574052690000D3CE75E0000
ParentEntryId    : 0000000004494C2A79DA0243970AABE82DA0BDE50100255F532116B8DC41A61899E7574052690000032D22D0000
OldItemEntryId   :
OldParentEntryId :
ItemCount        : 0
UnreadItemCount  : 0
ExtendedFlags    : 2147483843
ClientCategory   : Transport
PrincipalName    : NT AUTHORITY\SYSTEM
PrincipalSid     : S-1-5-18
Database         : Mailbox Database 2072208900
DocumentId       : 14386
--
```

EventHistoryDB sabe cuándo se empezó a escribir el correo

```
Counter          : 6558
CreateTime       : 07/06/2019 15:56:07
ItemType         : MAPI_MESSAGE
EventName        : ObjectCreated
Flags            : SearchFolder
MailboxGuid      : 9fee0121-8902-4013-81f9-6eb7a2d19a9f
ObjectClass      : IPM.Note
ItemEntryId      : 0000000004494C2A79DA0243970AABE82DA0BDE50700255F532116B8DC41A61899E7574052690000032D22D0000255F5321
                   16B8DC41A61899E75740526900000D3CE75E0000
ParentEntryId    : 0000000004494C2A79DA0243970AABE82DA0BDE50100255F532116B8DC41A61899E75740526900000BD71B0A0000
OldItemEntryId   :
OldParentEntryId :
ItemCount        : 0
UnreadItemCount  : 0
ExtendedFlags    : 1073741824
ClientCategory   : OWA
PrincipalName    : NT AUTHORITY\SYSTEM
PrincipalSid     : S-1-5-18
Database         : Mailbox Database 2072208900
DocumentId       : 14386
--
Counter          : 6559
CreateTime       : 07/06/2019 15:56:07
ItemType         : MAPI_MESSAGE
EventName        : ObjectCreated
Flags            : None
MailboxGuid      : 9fee0121-8902-4013-81f9-6eb7a2d19a9f
ObjectClass      : IPM.Note
ItemEntryId      : 0000000004494C2A79DA0243970AABE82DA0BDE50700255F532116B8DC41A61899E7574052690000032D22D0000255F5321
```

Paso 5: EventHistoryDB

```
--
CreateTime        : 07/06/2019 16:04:50
ItemType          : MAPI_MESSAGE
EventName         : ObjectMoved
Flags             : None
MailboxGuid       : 9fee0121-8902-4013-81f9-6eb7a2d19a9f
ObjectClass       : IPM.Note
ItemEntryId       : 0000000004494C2A79DA0243970AABE82DA0BDE50700255F532116B8DC41A61899E7574052690000032D2250000255F5321
                    16B8DC41A61899E7574052690000D3D17540000
ParentEntryId     : 0000000004494C2A79DA0243970AABE82DA0BDE50100255F532116B8DC41A61899E7574052690000032D2250000
OldItemEntryId    : 0000000004494C2A79DA0243970AABE82DA0BDE50700255F532116B8DC41A61899E7574052690000032D2240000255F5321
                    16B8DC41A61899E7574052690000D3CEF830000
OldParentEntryId  : 0000000004494C2A79DA0243970AABE82DA0BDE50100255F532116B8DC41A61899E7574052690000032D2240000
ItemCount         : 0
UnreadItemCount   : 0
ExtendedFlags     : 2147483648
ClientCategory    : OWA
PrincipalName     : S-1-5-21-4217457921-347679429-1194348710-1141
PrincipalSid      : S-1-5-21-4217457921-347679429-1194348710-1141
Database          : Mailbox Database 2072208900
DocumentId        : 14386
--
CreateTime        : 07/06/2019 16:20:41
ItemType          : MAPI_MESSAGE
EventName         : ObjectMoved
Flags             : None
MailboxGuid       : 9fee0121-8902-4013-81f9-6eb7a2d19a9f
ObjectClass       : IPM.Note
ItemEntryId       : 0000000004494C2A79DA0243970AABE82DA0BDE50700255F532116B8DC41A61899E7574052690000032FBC60000255F5321
                    16B8DC41A61899E7574052690000D3CFAD70000
ParentEntryId     : 0000000004494C2A79DA0243970AABE82DA0BDE50100255F532116B8DC41A61899E7574052690000032FBC60000
OldItemEntryId    : 0000000004494C2A79DA0243970AABE82DA0BDE50700255F532116B8DC41A61899E7574052690000032D2250000255F5321
                    16B8DC41A61899E7574052690000D3D17540000
OldParentEntryId  : 0000000004494C2A79DA0243970AABE82DA0BDE50100255F532116B8DC41A61899E7574052690000032D2250000
ItemCount         : 0
UnreadItemCount   : 0
ExtendedFlags     : 2147483648
ClientCategory    : OWA
```

Correo no leído por el CEO: 7/Jun 18:45:26h

```
--
Counter          : 7326
CreateTime       : 07/06/2019 18:45:32
ItemType         : MAPI_MESSAGE
EventName        : ObjectModified
Flags            : SearchFolder
MailboxGuid      : 9fee0121-8902-4013-81f9-6eb7a2d19a9f
ObjectClass      : IPM.Note
ItemEntryId      : 0000000004494C2A79DA0243970AABE82DA0BDE50700255F532116B8DC41A61899E7574052690000032D2220000255F5321
                   16B8DC41A61899E75740526900000D3CFCF70000
ParentEntryId    : 0000000004494C2A79DA0243970AABE82DA0BDE50100255F532116B8DC41A61899E75740526900000BD71B0A0000
OldItemEntryId   :
OldParentEntryId :
ItemCount        : 0
UnreadItemCount  : 0
ExtendedFlags    : 1073741824
ClientCategory   : OWA
PrincipalName    : S-1-5-21-4217457921-347679429-1194348710-1141
PrincipalSid     : S-1-5-21-4217457921-347679429-1194348710-1141
Database         : Mailbox Database 2072208900
DocumentId       : 14496
--
```

- Se ha leído por OWA
- No hay acceso ActiveSync → El CEO no lo leyó

… y ahora entendemos porqué

```
--
CreateTime        : 07/06/2019 18:45:35
ItemType          : MAPI_MESSAGE
EventName         : ObjectMoved
Flags             : None
MailboxGuid       : 9fee0121-8902-4013-81f9-6eb7a2d19a9f
ObjectClass       : IPM.Note
ItemEntryId       : 0000000004494C2A79DA0243970AABE82DA0BDE50700255F532116B8DC41A61899E7574052690000032D2250000255F5321
                    16B8DC41A61899E7574052690000D3D175D0000
ParentEntryId     : 0000000004494C2A79DA0243970AABE82DA0BDE50100255F532116B8DC41A61899E7574052690000032D2250000
OldItemEntryId    : 0000000004494C2A79DA0243970AABE82DA0BDE50700255F532116B8DC41A61899E7574052690000032D2220000255F5321
                    16B8DC41A61899E7574052690000D3CFCF70000
OldParentEntryId  : 0000000004494C2A79DA0243970AABE82DA0BDE50100255F532116B8DC41A61899E7574052690000032D2220000
ItemCount         : 0
UnreadItemCount   : 0
ExtendedFlags     : 2147483648
ClientCategory    : OWA
PrincipalName     : S-1-5-21-4217457921-347679429-1194348710-1141
PrincipalSid      : S-1-5-21-4217457921-347679429-1194348710-1141
Database          : Mailbox Database 2072208900
DocumentId        : 14496
--
CreateTime        : 07/06/2019 18:45:46
ItemType          : MAPI_MESSAGE
EventName         : ObjectMoved
Flags             : None
MailboxGuid       : 9fee0121-8902-4013-81f9-6eb7a2d19a9f
ObjectClass       : IPM.Note
ItemEntryId       : 0000000004494C2A79DA0243970AABE82DA0BDE50700255F532116B8DC41A61899E7574052690000032FBC60000255F5321
                    16B8DC41A61899E7574052690000D3CFAD90000
ParentEntryId     : 0000000004494C2A79DA0243970AABE82DA0BDE50100255F532116B8DC41A61899E7574052690000032FBC60000
OldItemEntryId    : 0000000004494C2A79DA0243970AABE82DA0BDE50700255F532116B8DC41A61899E7574052690000032D2250000255F5321
                    16B8DC41A61899E7574052690000D3D175D0000
OldParentEntryId  : 0000000004494C2A79DA0243970AABE82DA0BDE50100255F532116B8DC41A61899E7574052690000032D2250000
ItemCount         : 0
UnreadItemCount   : 0
ExtendedFlags     : 2147483648
ClientCategory    : OWA
```

Qué sabemos hasta ahora…

- Correos escritos y enviados **al momento**
- **Borrados** del buzón nada más ser enviados
- Se **vacía la papelera** al final de la acción
- **Monitorización** constante del correo
- **RemoteWipe** del terminal
- Origen: !! **OWA** !!

CAS (Client Access Server)

- Recoge actividad del correo
- OWA, ActiveSync, ECP → **CAS**
- En realidad, un IIS
- Formato de logs **estándar**
- **Sin periodo** de retención

Buscamos el correo de OK del CEO → CFO el 7/Jun

```
2019-06-07 18:39:15 10.11.0.101 POST /Microsoft-Server-ActiveSync/default.eas Cmd=SendMail&
User=abelardo.alcazar%40minaf.es&DeviceId=androidc1290513397&DeviceType=Android&Log=V141_Ld
apC6_LdapL31_RpcC30_RpcL47_Ers1_Pk2658248895_ClsName:IPM.Note_As:AllowedG_Mbx:CORREO.minaf.
es_Dc:dc.minaf.es_Throttle0_Budget:(A)Conn%3a0%2cHangingConn%3a0%2cAD%3a%24null%2f%24null%2
f0%25%2cCAS%3a%24null%2f%24null%2f1%25%2cAB%3a%24null%2f%24null%2f1%25%2cRPC%3a%24null%2f%2
4null%2f1%25%2cFC%3a1000%2f0%2cPolicy%3aDefaultThrottlingPolicy%5Fee93b4b2-4f01-41b6-b341-6
99759376ac7%2cNorm_ 443 abelardo.alcazar@minaf.es 10.11.0.210
Android-Mail/7.5.7.156101332.release 200 0 0 203
```

- Uso de ActiveSync (DeviceId:androidc1290513397)
- User-Agent: Android-Mail/7.5.7.156101332.release (concurrente con Android 8.1, SO de los S9)
- IP correcta (10.11.0.210, VPN del MINAF)

Buscamos el primer correo malicioso del 7/Jun

```
2019-06-07 16:02:00 10.11.0.101 POST /owa/forms/basic/BasicMessageView.aspx
ae=PreFormAction&t=IPM.Note&a=Send&Initial+Budget>>Conn:1,HangingConn:0,AD:18000/18000/
0%,CAS:90000/90000/0%,AB:18000/18000/0%,RPC:90000/90000/0%,FC:1000/0,Policy:DefaultThrot
tlingPolicy_ee93b4b2-4f01-41b6-b341-699759376ac7,Norm&mbx=CORREO.minaf.es&sessionId=88af
c1b05cf54b2e97272bc9091e5bc3&prfltncy=281&prfrpccnt=13&prfrpcltncy=63&prfldpcnt=0&prfldp
ltncy=0&prfavlcnt=0&prfavllltncy=0&End+Budget>>Conn:1,HangingConn:0,AD:18000/18000/
0%,CAS:90000/89719/1%,AB:18000/18000/0%,RPC:90000/89940/1%,FC:1000/
0,Policy:DefaultThrottlingPolicy_ee93b4b2-4f01-41b6-b341-699759376ac7,Norm[
Resources:(Mdb)Mailbox+Database+2072208900(Health:-1%,HistLoad:0),] 443
MINAF\abelardo.alcazar 101.132.122.100 Mozilla/5.0+(Linux;+Android+7.0;+PLUS+Build/
NRD90M)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/61.0.3163.98+Mobile+Safari/537.36
200 0 0 281
```

- Uso de OWA, no ActiveSync
- User-Agent fake: Mozilla/5.0+(Linux;+Android+7.0; +PLUS+Build/NRD90M)+AppleWebKit/537.36 …
- IP maliciosa (101.132.122.100)

Pivotamos sobre la IP maliciosa el 7/Jun

```
2019-06-07 15:04:12 10.11.0.101 GET /ecp/ rfr=owa&p=Organize/AutomaticReplies.slab 443 - 101.132.122.100
Mozilla/5.0+(X11;+Linux+x86_64)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/61.0.3163.100+Safari/537.36 302 0 0 46
2019-06-07 15:04:12 10.11.0.101 GET /owa/auth/logon.aspx url=https://10.11.0.101/ecp/%3Frfr=owa%26p=Organize/AutomaticReplies.slab&reason=3 443 -
101.132.122.100 Mozilla/5.0+(X11;+Linux+x86_64)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/61.0.3163.100+Safari/537.36 200 0 0 109
2019-06-07 15:04:46 10.11.0.101 GET /owa/auth/logon.aspx url=https://10.11.0.101/ecp/%3Frfr=owa%26p=Organize/AutomaticReplies.slab&reason=3 443 -
101.132.122.100 Mozilla/5.0+(Linux;+Android+7.0;+PLUS+Build/NRD90M)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/61.0.3163.98+Mobile+Safari/537.36 200 0 0 15
2019-06-07 15:05:14 10.11.0.101 POST /owa/auth.owa - 443 MINAF\abelardo.alcazar 101.132.122.100 Mozilla/5.0+(Linux;+Android+7.0;+PLUS+Build/
NRD90M)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/61.0.3163.98+Mobile+Safari/537.36 302 0 0 171
2019-06-07 15:05:14 10.11.0.101 GET /ecp/ rfr=owa&p=Organize/AutomaticReplies.slab 443 MINAF\abelardo.alcazar 101.132.122.100
Mozilla/5.0+(Linux;+Android+7.0;+PLUS+Build/NRD90M)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/61.0.3163.98+Mobile+Safari/537.36 200 0 0 765
2019-06-07 15:05:15 10.11.0.101 GET /ecp/Organize/AutomaticReplies.slab showhelp=false& 443 MINAF\abelardo.alcazar 101.132.122.100
Mozilla/5.0+(Linux;+Android+7.0;+PLUS+Build/NRD90M)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/61.0.3163.98+Mobile+Safari/537.36 200 0 0 140
2019-06-07 15:05:34 10.11.0.101 GET /ecp/MyGroups/PersonalGroups.aspx showhelp=false& 443 MINAF\abelardo.alcazar 101.132.122.100
Mozilla/5.0+(Linux;+Android+7.0;+PLUS+Build/NRD90M)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/61.0.3163.98+Mobile+Safari/537.36 200 0 0 8859
2019-06-07 15:05:36 10.11.0.101 POST /ecp/MyGroups/MemberOfGroups.svc/GetList
msExchEcpCanary=W1llB3pkrEGvb0FMfLio-WXPUkZR7NYIAtzJPDyNngENfhFk_xkZEns8NaAEKQTk3TXnQ58FqLI. 443 MINAF\abelardo.alcazar 101.132.122.100
Mozilla/5.0+(Linux;+Android+7.0;+PLUS+Build/NRD90M)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/61.0.3163.98+Mobile+Safari/537.36 200 0 0 1750
2019-06-07 15:05:52 10.11.0.101 GET /ecp/Customize/Messaging.aspx showhelp=false& 443 MINAF\abelardo.alcazar 101.132.122.100
Mozilla/5.0+(Linux;+Android+7.0;+PLUS+Build/NRD90M)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/61.0.3163.98+Mobile+Safari/537.36 200 0 0 15031
2019-06-07 15:06:02 10.11.0.101 GET /ecp/PersonalSettings/Password.aspx showhelp=false& 443 MINAF\abelardo.alcazar 101.132.122.100
Mozilla/5.0+(Linux;+Android+7.0;+PLUS+Build/NRD90M)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/61.0.3163.98+Mobile+Safari/537.36 200 0 64 21656
```

- Los atacantes entran a las 15:04:12 UTC
- Están permanentemente monitorizando el correo
- Envían los 4 correos maliciosos desde el OWA
- Ordenan el borrado remoto

Pivotamos sobre la IP maliciosa días anteriores

```
u_ex190604.log:2019-06-04 20:33:30 10.11.0.101 GET /owa/ - 443 - 101.132.122.100
Mozilla/5.0+(Windows+NT;+Windows+NT+10.0;+es-ES)+WindowsPowerShell/5.1.17134.590 401 2 5 6265
u_ex190604.log:2019-06-04 20:33:30 10.11.0.101 GET /owa/auth/logon.aspx url=https://10.11.0.101/owa/&reason=0 443 -
101.132.122.100 Mozilla/5.0+(Windows+NT;+Windows+NT+10.0;+es-ES)+WindowsPowerShell/5.1.17134.590 200 0 0 187
u_ex190604.log:2019-06-04 20:33:34 10.11.0.101 POST /owa/auth.owa - 443 - 101.132.122.100
Mozilla/5.0+(Windows+NT;+Windows+NT+10.0;+es-ES)+WindowsPowerShell/5.1.17134.590 302 0 0 218
u_ex190604.log:2019-06-04 20:33:34 10.11.0.101 GET /owa/auth/logon.aspx url=https://10.11.0.101/owa/&reason=2 443 -
101.132.122.100 Mozilla/5.0+(Windows+NT;+Windows+NT+10.0;+es-ES)+WindowsPowerShell/5.1.17134.590 200 0 0 62
u_ex190604.log:2019-06-04 20:35:17 10.11.0.101 GET /owa - 443 - 101.132.122.100
Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/74.0.3729.131+Safari/537.36 301 0 0 15
u_ex190604.log:2019-06-04 20:35:17 10.11.0.101 GET /owa/ - 443 - 101.132.122.100
Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/74.0.3729.131+Safari/537.36 401 2 5 15
u_ex190604.log:2019-06-04 20:35:17 10.11.0.101 GET /owa/auth/logon.aspx url=https://10.11.0.101/owa/&reason=0 443 -
101.132.122.100
Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/74.0.3729.131+Safari/537.36 200 0 0 125
u_ex190604.log:2019-06-04 20:35:17 10.11.0.101 GET /owa/auth/logon.aspx replaceCurrent=1&url=https%3a%2f%2f10.11.0.101%2fowa%2f
443 - 101.132.122.100
Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/74.0.3729.131+Safari/537.36 200 0 0 0
u_ex190604.log:2019-06-04 20:35:23 10.11.0.101 GET /owa/ - 443 - 101.132.122.100
Mozilla/5.0+(Windows+NT;+Windows+NT+10.0;+es-ES)+WindowsPowerShell/5.1.17134.590 401 2 5 15
u_ex190604.log:2019-06-04 20:35:23 10.11.0.101 GET /owa/auth/logon.aspx url=https://10.11.0.101/owa/&reason=0 443 -
101.132.122.100 Mozilla/5.0+(Windows+NT;+Windows+NT+10.0;+es-ES)+WindowsPowerShell/5.1.17134.590 200 0 0 0
u_ex190604.log:2019-06-04 20:35:23 10.11.0.101 POST /owa/auth.owa - 443 - 101.132.122.100
Mozilla/5.0+(Windows+NT;+Windows+NT+10.0;+es-ES)+WindowsPowerShell/5.1.17134.590 302 0 0 218
u_ex190604.log:2019-06-04 20:35:24 10.11.0.101 GET /owa/auth/logon.aspx url=https://10.11.0.101/owa/&reason=2 443 -
101.132.122.100 Mozilla/5.0+(Windows+NT;+Windows+NT+10.0;+es-ES)+WindowsPowerShell/5.1.17134.590 200 0 0 93
```

- User-Agent: Powershell
- Intentos de acceso repetidos
- Posible password spraying con MailSniper

Pivotamos sobre la IP maliciosa días anteriores

```
u_ex190604.log:2019-06-04 20:41:46 10.11.0.101 GET /owa/auth/logon.aspx url=https://correo.minaf.es/owa/&reason=2 443 - 101.132.122.100 Mozill
/5.0+(Windows+NT;+Windows+NT+10.0;+es-ES)+WindowsPowerShell/5.1.17134.590 200 0 0 125
u_ex190605.log:2019-06-05 18:15:14 10.11.0.101 GET /owa/auth/logon.aspx url=https://10.11.0.101/owa/&reason=2 443 - 101.132.122.100 Mozilla/5.
+(Windows+NT+10.0;+Win64;+x64)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/74.0.3729.169+Safari/537.36 200 0 0 46
u_ex190605.log:2019-06-05 18:15:14 10.11.0.101 GET /owa/auth/logon.aspx replaceCurrent=1&reason=2&url=https%3a%2f%2f10.11.0.101%2fowa%2f 443 -
101.132.122.100 Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/74.0.3729.169+Safari/537.36 200 0 0 15
u_ex190605.log:2019-06-05 18:15:43 10.11.0.101 GET /owa/auth/logon.aspx url=https://10.11.0.101/owa/&reason=2 443 - 101.132.122.100 Mozilla/5.
+(Windows+NT+10.0;+Win64;+x64)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/74.0.3729.169+Safari/537.36 200 0 0 46
u_ex190605.log:2019-06-05 18:15:43 10.11.0.101 GET /owa/auth/logon.aspx replaceCurrent=1&reason=2&url=https%3a%2f%2f10.11.0.101%2fowa%2f 443 -
101.132.122.100 Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/74.0.3729.169+Safari/537.36 200 0 0 0
u_ex190605.log:2019-06-05 18:15:50 10.11.0.101 GET /owa/auth/logon.aspx url=https://10.11.0.101/owa/&reason=2 443 - 101.132.122.100 Mozilla/5.
+(Windows+NT+10.0;+Win64;+x64)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/74.0.3729.169+Safari/537.36 200 0 0 62
u_ex190605.log:2019-06-05 18:15:50 10.11.0.101 GET /owa/auth/logon.aspx replaceCurrent=1&reason=2&url=https%3a%2f%2f10.11.0.101%2fowa%2f 443 -
101.132.122.100 Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/74.0.3729.169+Safari/537.36 200 0 0 15
u_ex190605.log:2019-06-05 18:15:56 10.11.0.101 GET /owa/auth/logon.aspx url=https://10.11.0.101/owa/&reason=2 443 - 101.132.122.100 Mozilla/5.
+(Windows+NT+10.0;+Win64;+x64)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/74.0.3729.169+Safari/537.36 200 0 0 31
u_ex190605.log:2019-06-05 18:15:56 10.11.0.101 GET /owa/auth/logon.aspx replaceCurrent=1&reason=2&url=https%3a%2f%2f10.11.0.101%2fowa%2f 443 -
101.132.122.100 Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/74.0.3729.169+Safari/537.36 200 0 0 15
u_ex190605.log:2019-06-05 19:40:14 10.11.0.101 GET /owa/auth/logon.aspx replaceCurrent=1&reason=2&url=https%3a%2f%2f10.11.0.101%2fowa%2f 443 -
101.132.122.100 Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/74.0.3729.169+Safari/537.36 200 0 0 31
~
```

- User-Agent: Chrome
- Intentos de acceso repetidos pero a través del OWA
- Tiempo aleatorio entre peticiones ← no automatizado
- Posible credential stuffing manual

Pivotamos sobre la IP maliciosa días anteriores

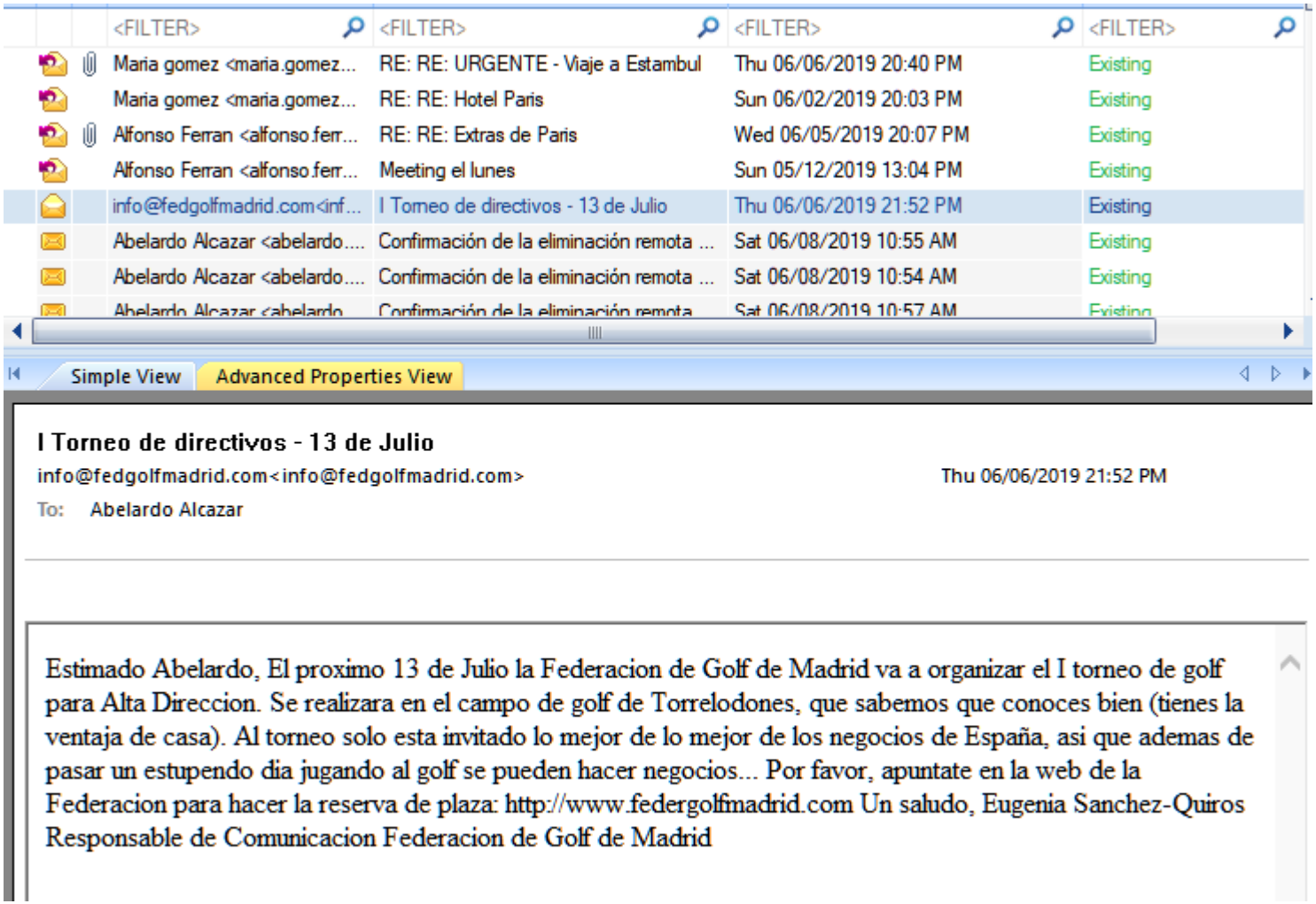
```
u_ex190606.log:2019-06-06 20:05:25 10.11.0.101 POST /owa/auth.owa - 443 MINAF\abelardo.alcazar
101.132.122.100 Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/74.0.3
729.169+Safari/537.36 302 0 0 1234

u_ex190606.log:2019-06-06 20:05:32 10.11.0.101 GET /owa/forms/premium/StartPage.aspx
&Initial+Budget>>Conn:1,HangingConn:0,AD:18000/18000/0%,CAS:90000/90000/0%,AB:18000/18000/0%,RPC:90000/90000/
0%,FC:1000/0,Policy:DefaultThrottlingPolicy_ee93b4b2-4f01-41b6-b341-699759376ac7,Norm&mbx=CORREO.minaf.es&sess
ionId=2c791f212f3448c097f8542b895da015&prfltncy=6786&prfrpccnt=71&prfrpcltncy=109&prfldpcnt=18&prfldpltncy=92&
prfavlcnt=0&prfavllltncy=0&End+Budget>>Conn:1,HangingConn:0,AD:18000/17970/1%,CAS:90000/85579/8%,AB:18000/18000
/0%,RPC:90000/89709/1%,FC:1000/0,Policy:DefaultThrottlingPolicy_ee93b4b2-4f01-41b6-b341-699759376ac7,Norm[
Resources:(Mdb)Mailbox+Database+2072208900(Health:-1%,HistLoad:0),(DC)dc.minaf.es(Health:-1%,HistLoad:0),]
443 MINAF\abelardo.alcazar 101.132.122.100 Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64)+AppleWebKit/537.36+(KHTML
,+like+Gecko)+Chrome/74.0.3729.169+Safari/537.36 200 0 0 6843
```

- User-Agent: Chrome
- Logran el acceso el día anterior al ataque
- Se dedican a leer TODO el correo de AA

Qué sabemos hasta ahora…

- Los atacantes prueban varios ataques contra el Exchange
- Logran las **credenciales** de abelardo.alcazar y leen **todo su correo**
- El 7/Jun mandan los correos desde el OWA, monitorizando el correo
- Borran el móvil desde el OWA

Localizamos el phishing



<FILTER>	<FILTER>	<FILTER>	<FILTER>
Maria gomez <maria.gomez...	RE: RE: URGENTE - Viaje a Estambul	Thu 06/06/2019 20:40 PM	Existing
Maria gomez <maria.gomez...	RE: RE: Hotel Paris	Sun 06/02/2019 20:03 PM	Existing
Alfonso Ferran <alfonso.ferr...	RE: RE: Extras de Paris	Wed 06/05/2019 20:07 PM	Existing
Alfonso Ferran <alfonso.ferr...	Meeting el lunes	Sun 05/12/2019 13:04 PM	Existing
info@fedgolfmadrid.com<inf...	I Torneo de directivos - 13 de Julio	Thu 06/06/2019 21:52 PM	Existing
Abelardo Alcazar <abelardo....	Confirmación de la eliminación remota ...	Sat 06/08/2019 10:55 AM	Existing
Abelardo Alcazar <abelardo....	Confirmación de la eliminación remota ...	Sat 06/08/2019 10:54 AM	Existing
Abelardo Alcazar <abelardo...	Confirmación de la eliminación remota ...	Sat 06/08/2019 10:57 AM	Existing

Simple View | Advanced Properties View

I Torneo de directivos - 13 de Julio

info@fedgolfmadrid.com<info@fedgolfmadrid.com> Thu 06/06/2019 21:52 PM

To: Abelardo Alcazar

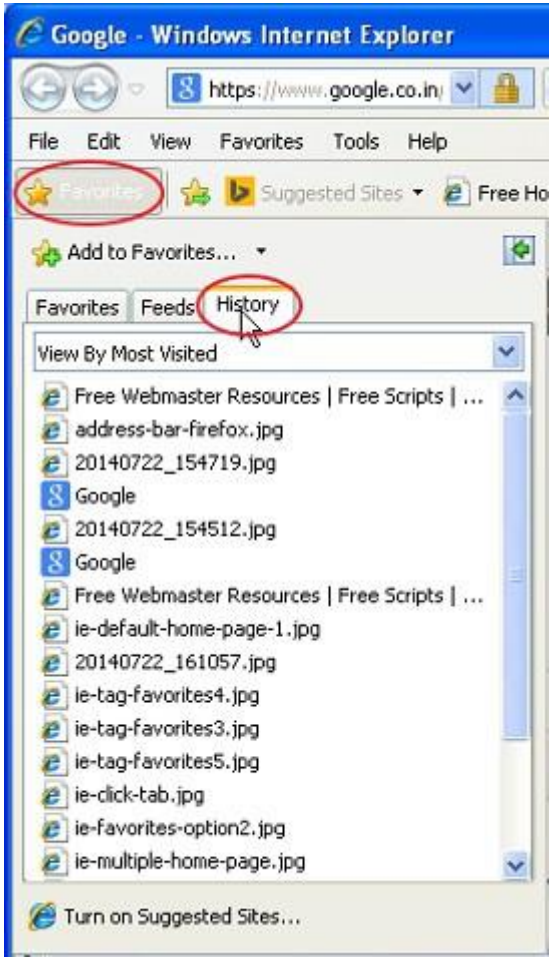
Estimado Abelardo, El proximo 13 de Julio la Federacion de Golf de Madrid va a organizar el I torneo de golf para Alta Direccion. Se realizara en el campo de golf de Torrelodones, que sabemos que conoces bien (tienes la ventaja de casa). Al torneo solo esta invitado lo mejor de lo mejor de los negocios de España, asi que ademas de pasar un estupendo dia jugando al golf se pueden hacer negocios... Por favor, apuntate en la web de la Federacion para hacer la reserva de plaza: http://www.federgolfmadrid.com Un saludo, Eugenia Sanchez-Quiros Responsable de Comunicacion Federacion de Golf de Madrid

Comprobamos los metadatos

PR_RCVD_REPRESENTING_EMAIL_ADDRESS	0x0078001F	UTF-16 Unicode string	/O=MINAF/OU=EXCHANGE ADMINISTRATIVE...
PR_TRANSPORT_MESSAGE_HEADERS	0x007D001F	UTF-16 Unicode string	Received: from correo.mina.es (10.11.0.211) by c...
PR_SENDER_ENTRYID	0x0C190102	Binary data	00 00 00 00 81 2B 1F A4 BE A3 10 19 9D 6E 00...
PR_SENDER_NAME	0x0C1A001F	UTF-16 Unicode string	info@fedgolfmadrid.com
PR_SENDER_SEARCH_KEY	0x0C1D0102	Binary data	53 4D 54 50 3A 49 4E 46 4F 40 46 45 44 47 4F ...
PR_SENDER_ADDRTYPE	0x0C1E001F	UTF-16 Unicode string	SMTP

Hex Preview | Txt Preview | Unicode Txt Preview

```
Received: from correo.mina.es (10.11.0.211) by correo.minaf.es (10.11.0.101)
 with Microsoft SMTP Server id 14.3.439.0; Thu, 6 Jun 2019 21:52:21 +0200
Received: from [127.0.1.1] (localhost [127.0.0.1])  by correo.mina.es (Postfix)
 with ESMTPS id 14BB28318B            for <abelardo.alcazar@minaf.es>; Thu,  6 Jun 2019
 21:52:20 +0200 (CEST)
Content-Type: multipart/mixed;
        boundary="==========725457947981936846 8=="
MIME-Version: 1.0
From: =?utf-8?b?aW5mb0BmZWRnb2xmbWFkcmlkLmNvbQ==?= <info@fedgolfmadrid.com>
To: <abelardo.alcazar@minaf.es>
X-Priority:
X-MSMail-Priority:
Subject: =?utf-8?b?SSBUb3JuZW8gZGUgZGlyZWN0aXZvcyAtIDEzIGRlIEp1bGlv?=
Message-ID: <20190606195220.14BB28318B@correo.mina.es>
Date: Thu, 6 Jun 2019 21:52:20 +0200
Return-Path: info@fedgolfmadrid.com
X-MS-Exchange-Organization-AuthSource: correo.minaf.es
X-MS-Exchange-Organization-AuthAs: Anonymous
```



Historial de navegación web

- Guardado en el **perfil** de cada usuario
- Navegación, búsquedas, cache…
- IE10+ → **WebCache**
- Webcache = **ESE Database**
- Tool: **ESEDatabaseView.exe**

Se comprueba que AA abrió el phishing

06/06/2019 19:49:08	0	05/05/18...	0	Visited: abelardo.alcazar@file:///C:/Users/abelardo.alcazar/AppData/Local/Microsoft/Windows
06/06/2019 19:49:08	0	05/05/18...	0	Visited: abelardo.alcazar@file:///C:/Users/abelardo.alcazar/AppData/Local/Microsoft/Windows
06/06/2019 19:49:08	0	05/05/18...	0	Visited: abelardo.alcazar@file:///C:/Users/abelardo.alcazar/AppData/Local/Microsoft/Windows
06/06/2019 20:02:29	0	0	0	Visited: abelardo.alcazar@http://www.federgolfmadrid.com/
06/06/2019 19:57:54	0	0	0	Visited: abelardo.alcazar@http://www.federgolfmadrid.com/favicon.ico
06/06/2019 19:59:20	0	0	0	Visited: abelardo.alcazar@https://www.colectivosvip.com/banners/banner.action?bannerId=12
06/06/2019 19:59:20	0	0	0	Visited: abelardo.alcazar@http://www.fedgolfmadrid.com/files/decalogo/index.html?v=12h2
06/06/2019 19:59:20	0	0	0	Visited: abelardo.alcazar@http://www.fedgolfmadrid.com/files/circuito_amateur/index.html?V
06/06/2019 19:59:21	0	0	0	Visited: abelardo.alcazar@https://www.youtube.com/embed/6kaotCmBR3k?list=PLOUpJc-W0
06/06/2019 20:10:39	0	0	0	Visited: abelardo.alcazar@about:blank
06/06/2019 20:10:03	0	0	0	Visited: abelardo.alcazar@https://staticxx.facebook.com/connect/xd_arbiter.php?version=44
06/06/2019 19:59:21	0	0	0	Visited: abelardo.alcazar@https://platform.twitter.com/widgets/widget_iframe.d753e00c3e838
06/06/2019 19:58:04	0	05/05/18...	0	Visited: abelardo.alcazar@https://www.facebook.com/v3.0/plugins/page.php?adapt_container
06/06/2019 19:58:13	0	05/05/18...	0	Visited: abelardo.alcazar@https://platform.twitter.com/widgets/widget_iframe.d753e00c3e838
06/06/2019 19:58:13	0	05/05/18...	0	Visited: abelardo.alcazar@https://www.facebook.com/v3.0/plugins/page.php?adapt_container

Conclusiones del análisis forense I

- Los atacantes realizan el **5/Jun** varios ataques contra **cuentas de correo** del MINAF
- El dia 6/Jun lanzan un **spear-phishing** dirigido al **CEO** según sus gustos sociales
- Poca superficie de ataque y dirigido → **OSINT previa** por parte de los atacantes
- El CEO pica en el phishing y **reusa credenciales**, dando a los atacantes **acceso a la cuenta**

Conclusiones del análisis forense II

- El 7/Jun, entran a la cuenta simulando ser un Android y envían un correo al **CFO**, solicitando unas **transferencias**
- Aprovechan la **no disponibilidad** del CEO (en las negociaciones)
- Hacen uso de **conocimiento previo** → Atacantes profesionales
- **Borran los correos** al enviarlos para que el CEO no los lea en el terminal móvil

Conclusiones del análisis forense III

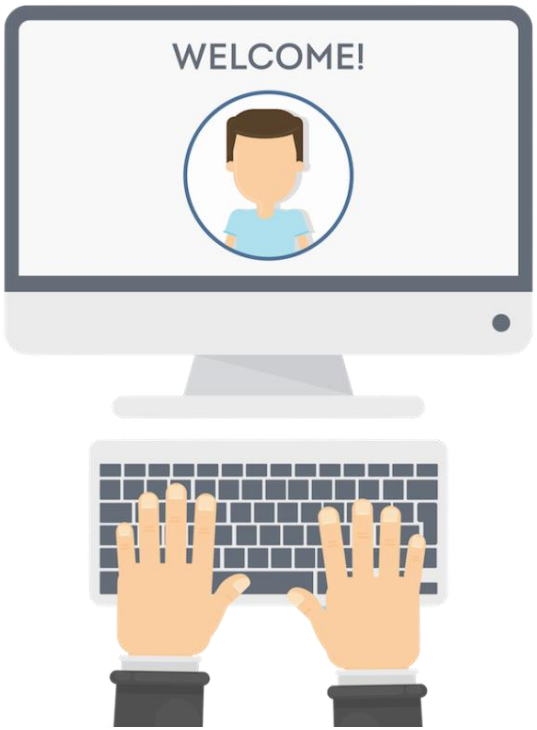
- Vacían la **papelera** al terminar los envíos
- **Monitorizan** la cuenta en busca de posibles correos
- **Borran** la respuesta del CFO al CEO
- Realizan un borrado remoto para ganar tiempo
- Ejecución limpia y casi sin fisuras → Grupo de **atacantes profesionales**
- La infrestructura del MINAF **no ha sido comprometida**

Conclusiones

GRUPO

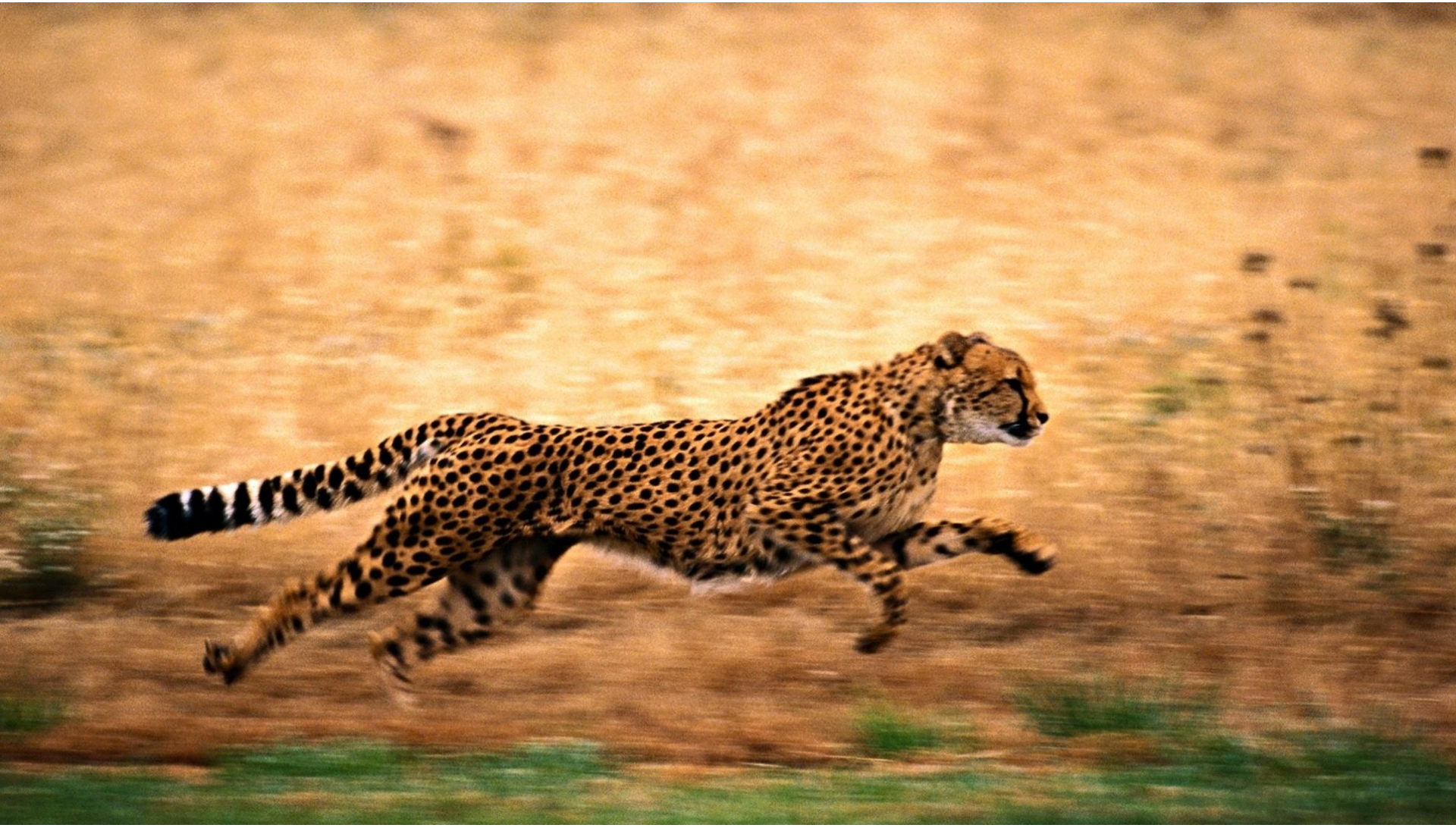
La vanguardia de la ciberseguridad

Usa doble factor de autenticación (2FA)



Los logs son tus mejores amigos

Reacciona con rapidez



Conciencia a tus usuarios

Controla el dinero

Trabaja como si estuvieras COMPROMETIDO

Evidencias para el taller / Reto forense

bit.ly/estafaCEO / bit.ly/CTF_DFIR_Exchange

Maite Moreno - @mmorenog
Antonio Sanz - @antoniosanzalc

S2 GRUPO

MADRID

Velázquez, 150, 2ª planta, 28002
T. (+34) 902 882 992

BARCELONA

Llull, 321, 08019
T. (+34) 933 030 060

VALENCIA

Ramiro de Maeztu 7, 46022
T. (+34) 902 882 992

info@s2grupo.es
www.s2grupo.es
www.securityartwork.es

MÉXICO, D.F.

Monte Athos 420
D.F., 11000
México
T. (+52) 15521280681

BOGOTÁ

Calle 89, nº 12-59,
T. (+57) 317 647 10 96