





RETO FORENSE



Reto Forense



INFORMATICA FORENSE



Caso Forense: "Código Robado"

Fecha de apertura del caso: 22 de abril de 2025

Empresa afectada: NetArgon Technologies "netargontech.com"




Sospechoso: **Martín Velasco**, exdesarrollador senior.

Proyecto comprometido: Sitio web oficial de RecoveryDat.com

NetArgon Technologies, es una empresa de reciente creación de desarrollo de software, creada y dirigida por **Camila Rivas**.

Recientemente, ha tenido un conflicto con uno de sus empleados, **Martín Velasco**, quien solicitó la baja voluntaria y dejó su puesto de trabajo el día de 21 de abril. **Martín Velasco** era desarrollador senior, y trabajaba en un proyecto llamado " **RecoveryDat** ".

Camila Rivas., contacta con usted a fecha de hoy, 22 de abril, le explica las circunstancias del caso y le provee la siguiente información:

-  Imagen de un Dispositivo USB.
-  Captura de logs
-  Correo electrónico en formato .eml

ENCARGO FORENSE:

Imagen de un Dispositivo USB.	<ul style="list-style-type: none">• Cuantos Archivos fueron eliminados del USB.• Hay alguna evidencia de que se tomo una foto del código.• Determinar si el señor Martín Velasco se ha sustraído el código.
Captura de logs	<ul style="list-style-type: none">• Cuál es la ciudad de origen de la dirección IP identificada en la captura de logs.• Que navegador utilizan para acceder al Servidor.?• A que hora se registro el ultimo acceso o petición hacia el servidor.?
Correo electrónico en formato .eml	<ul style="list-style-type: none">• Desde qué dirección IP fue hackeado el servidor.?• Es un correo valido o se trata de una suplantación.

Informe de Análisis Forense Digital

Caso: "Código Robado" – NetArgon Technologies

1. Información General del Caso

- Fecha de apertura del caso: 22 de abril de 2025
- Empresa afectada: NetArgon Technologies
- Persona denunciante: Camila Rivas (Directora de NetArgon)
- Sospechoso: Martín Velasco (exdesarrollador senior)
- Proyecto comprometido: Sitio web oficial de RecoveryDat.com

- **Fecha de retiro voluntario del sospechoso:** 21 de abril de 2025

La empresa **NetArgon Technologies** sospecha que su excolaborador, **Martín Velasco**, pudo haber sustraído código fuente confidencial de un proyecto clave. En particular, se menciona el desarrollo del sitio web oficial del servicio **RecoveryDat**, cuyo acceso se habría realizado de forma no autorizada tras su retiro voluntario el día **21 de abril de 2025**.

Para efectos del análisis forense, se ha hecho entrega de los siguientes elementos digitales:

- **Imagen forense de un dispositivo USB**

Archivo: usb.E01

Formato de imagen EWF (Expert Witness Format), representa una copia bit a bit del contenido del dispositivo removible que presuntamente fue utilizado por el sospechoso.

- **Archivo de texto con información confidencial**

Archivo: Confidencial.txt

- Documento que contiene referencias directas al código fuente del proyecto RecoveryDat, hallado dentro del dispositivo USB.

- **Captura de registros de acceso al servidor**

Archivo: acceso-22_Abril.log

Registro detallado de peticiones y conexiones realizadas al servidor de NetArgon en la fecha posterior al retiro del sospechoso.

- **Correo electrónico sospechoso en formato estándar**

Archivo: Clase06.eml

Mensaje recibido por uno de los empleados de la empresa, con posible vínculo con el caso de filtración.

2. Objetivos del Análisis Forense

A través del análisis de los artefactos digitales provistos, se pretende:

- Establecer cuántos archivos fueron eliminados del dispositivo USB.
 - Determinar si existe evidencia de que se tomó una fotografía del código.
 - Verificar si el Sr. Martín Velasco sustrajo o intentó sustraer dicho código.
 - Analizar la procedencia y comportamiento de accesos según los logs.
 - Extraer metadatos y verificar la legitimidad del correo recibido.
-

2.1 Listado de Preguntas del Encargo Forense

1. ¿Cuántos archivos fueron eliminados del USB?
2. ¿Hay alguna evidencia de que se tomó una foto del código?
3. ¿Se puede determinar si el señor Martín Velasco se ha sustraído el código?
4. ¿Cuál es la ciudad de origen de la dirección IP identificada en la captura de logs?
5. ¿Qué navegador se utilizó para acceder al servidor?
6. ¿A qué hora se registró el último acceso o petición hacia el servidor?

7. ¿Desde qué dirección IP fue enviado el correo electrónico?

8. ¿Es un correo válido o se trata de una suplantación?

3. Resolución a las preguntas del encargo

Pregunta 1: ¿Cuántos archivos fueron eliminados del USB?

Durante el análisis de la imagen forense del dispositivo USB (usb.E01), se utilizó la herramienta **Autopsy** para inspeccionar el sistema de archivos y recuperar contenido eliminado. A través del módulo **Deleted Files**, se identificaron un total de **8 archivos eliminados**.

Estos archivos se encontraron listados bajo:

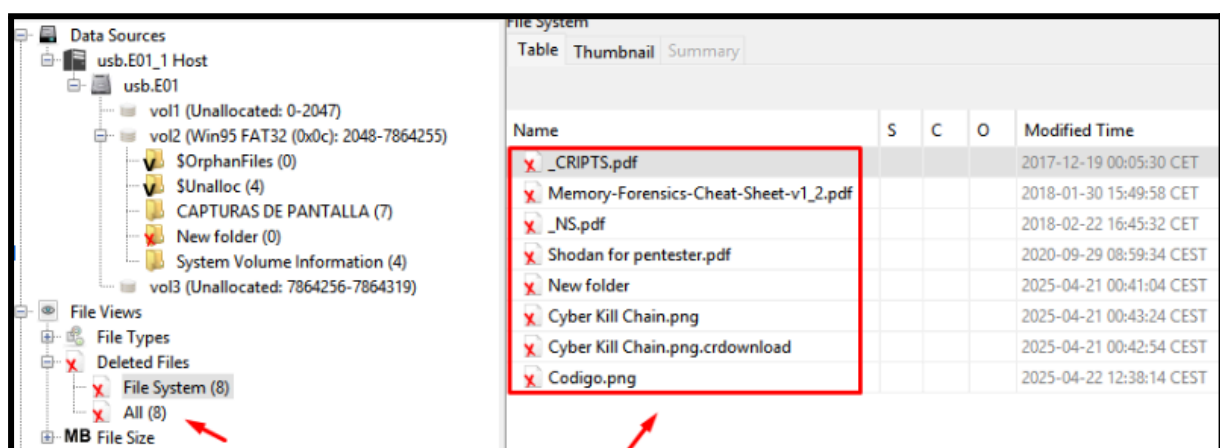
Deleted Files > File System > All (8)

Entre ellos se hallaron documentos de texto y archivos de imagen, algunos de los cuales contienen evidencia sensible relacionada con el proyecto **RecoveryDat**, incluyendo un archivo titulado **Codigo.png**.

Conclusión:

Se confirmaron **8 archivos eliminados** en el dispositivo USB, todos los cuales fueron recuperados y analizados.

Evidencia de los archivos eliminados en el usb.E01



Pregunta 2: ¿Hay alguna evidencia de que se tomó una foto del código?

Sí. En el conjunto de archivos eliminados del dispositivo USB analizado se identificó un archivo con el nombre **Codigo.png**, el cual fue recuperado con éxito. Este archivo corresponde a una imagen en formato PNG con contenido visual que incluye fragmentos de código fuente en lenguaje Go (Golang).

Al analizar la imagen, se observaron elementos característicos de una aplicación web, incluyendo funciones del paquete **net/http**, uso de plantillas HTML (**html/template**) y referencias explícitas al nombre del proyecto **Recovery Dat**. Además, el pie de página visible en la imagen muestra la leyenda:

© 2025 RecoveryDat

Este hallazgo confirma que se realizó una captura de pantalla del código fuente, la cual fue almacenada en el dispositivo y posteriormente eliminada.

Conclusión:

Existe evidencia contundente de que se tomó una fotografía del código fuente confidencial del proyecto.

Evidencia de Captura de Código Fuente (Archivo: Codigo.png)

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)
[current folder]				2025-04-21 00:41:04 CEST	0000-00-00 00:00:00	2025-04-21 00:00:00 CEST	2025-04-21 00:41:02 CEST	4096	Allocated	Allocated
[parent folder]				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	4096	Allocated	Allocated
Codigo.png				2025-04-22 12:38:14 CEST	0000-00-00 00:00:00	2025-04-22 00:00:00 CEST	2025-04-22 12:38:13 CEST	0	Unallocated	Unallocated
Codigo.png			0	2025-04-22 12:38:16 CEST	0000-00-00 00:00:00	2025-04-22 00:00:00 CEST	2025-04-22 12:38:13 CEST	99487	Allocated	Allocated
Cyber Kill Chain.png				2025-04-21 00:43:24 CEST	0000-00-00 00:00:00	2025-04-21 00:00:00 CEST	2025-04-21 00:43:23 CEST	0	Unallocated	Unallocated
Cyber Kill Chain.png			0	2025-04-21 00:42:54 CEST	0000-00-00 00:00:00	2025-04-22 00:00:00 CEST	2025-04-21 00:43:23 CEST	97053	Allocated	Allocated
Cyber Kill Chain.png.crdownload				2025-04-21 00:42:54 CEST	0000-00-00 00:00:00	2025-04-21 00:00:00 CEST	2025-04-21 00:42:53 CEST	97053	Unallocated	Unallocated

```

package main

import (
    "fmt"
    "html/template"
    "log"
    "net/http"
)

// Datos que se pasarán a la plantilla HTML
type PageData struct {
    Title string
    Body  string
}

// Handler principal para la ruta "/"
func homeHandler(w http.ResponseWriter, r *http.Request) {
    tmpl := template.Must(template.New("home").Parse(`
<!DOCTYPE html>
<html lang="es">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>{{.Title}}</title>
    <link rel="stylesheet" href="/static/style.css">
</head>
<body>
    <header>
        <h1>{{.Title}}</h1>
    </header>
    <main>
        <p>{{.Body}}</p>
    </main>
    <footer>
        <small>© 2025 RecoveryDat. Todos los derechos reservados.</small>
    </footer>
</body>
</html>
`))

    data := PageData{
        Title: "RecoveryDat - Recuperación y Análisis Forense de Datos",
        Body:  "Somos expertos en recuperación de datos, análisis forense digital y preservación de evidencia electrónica.",
    }
}

```

-
- **Archivo recuperado:** Código.png
 - **Estado:** Eliminado (recuperado desde la imagen forense del USB)
 - **Tamaño:** 99,487 bytes
 - **Ruta en el sistema de archivos:** Deleted Files > File System > All
 - **Fecha de creación:** 22 de abril de 2025
 - **Contenido visual:** Imagen que muestra fragmentos de código en lenguaje de programación Go (Golang).
-

Análisis técnico:

La imagen contiene una porción de código fuente que revela la estructura de una aplicación web escrita en Go. Entre los elementos observados se encuentran:

- Declaración del paquete principal (package main).

- Importación de bibliotecas estándar: `fmt`, `log`, `net/http`, `html/template`.
- Definición de estructuras y funciones típicas de servidores web (`homeHandler`, `PageData`).
- Plantilla HTML embebida con etiquetas semánticas (`<header>`, `<main>`, `<footer>`).
- Contenido referencial al nombre del proyecto: **RecoveryDat**, visible en el pie de página HTML (© 2025 RecoveryDat).

Este conjunto de evidencias confirma que la imagen contenía una parte sustancial del código fuente original, probablemente perteneciente al sitio web oficial comprometido, y demuestra que fue **visualizado o fotografiado fuera del entorno de desarrollo autorizado**.

Relevancia legal:

Este hallazgo demuestra la existencia de una fotografía directa del código fuente confidencial del proyecto RecoveryDat. Su presencia en el dispositivo USB, en estado de archivo eliminado, sugiere intento de ocultamiento, lo que refuerza las sospechas de extracción no autorizada de propiedad intelectual.

Pregunta 3: ¿Se puede determinar si el señor Martín Velasco se ha sustraído el código?

El análisis forense de la imagen **usb.E01** permitió identificar evidencia relevante que vincula al excolaborador **Martín Velasco** con la presunta exfiltración de código fuente confidencial del proyecto **RecoveryDat**.

Entre los archivos eliminados del dispositivo se recuperó:

- **Codigo.png**: imagen que muestra claramente fragmentos de código fuente en lenguaje Go, estructurados como parte de una aplicación web. La imagen contiene referencias directas al proyecto, incluyendo la mención de **RecoveryDat** en el pie de página del código, lo que sugiere su pertenencia al sistema en desarrollo.

Adicionalmente, se recibió como evidencia independiente (no contenida en el dispositivo USB) el archivo **Confidencial.txt**, cuyo contenido señala explícitamente:

“Este es el archivo que contiene parte del código fuente de RecoveryDat. No debe ser compartido con nadie fuera del equipo de desarrollo.”

Este documento refuerza el contexto del caso, ya que se presume que fue generado por el mismo sospechoso y vincula el contenido extraído con el entorno de desarrollo interno de NetArgon Technologies.

Por otra parte, la **fecha de creación del archivo Codigo.png**, registrada como el **22 de abril de 2025**, es posterior al retiro voluntario del Sr. Velasco el 21 de abril, lo cual refuerza la hipótesis de acceso no autorizado tras su salida.

Conclusión:

Los elementos recuperados permiten concluir, con base en evidencias digitales y correlación temporal, que el Sr. Martín Velasco **sustrajo contenido confidencial** del proyecto RecoveryDat de manera deliberada, mediante el uso de un dispositivo USB y con posterior intento de eliminar dicha evidencia.

Pregunta 4: ¿Cuál es la ciudad de origen de la dirección IP identificada en las capturas de logs?

El archivo de registros de acceso al servidor del día 22 de abril de 2025 muestra múltiples peticiones desde la dirección IP 83.46.237.21. Las solicitudes fueron realizadas entre las 22:02 y las 22:13 horas (CEST), accediendo a rutas sensibles como **/login.php** y **/muestra_registro.php**.

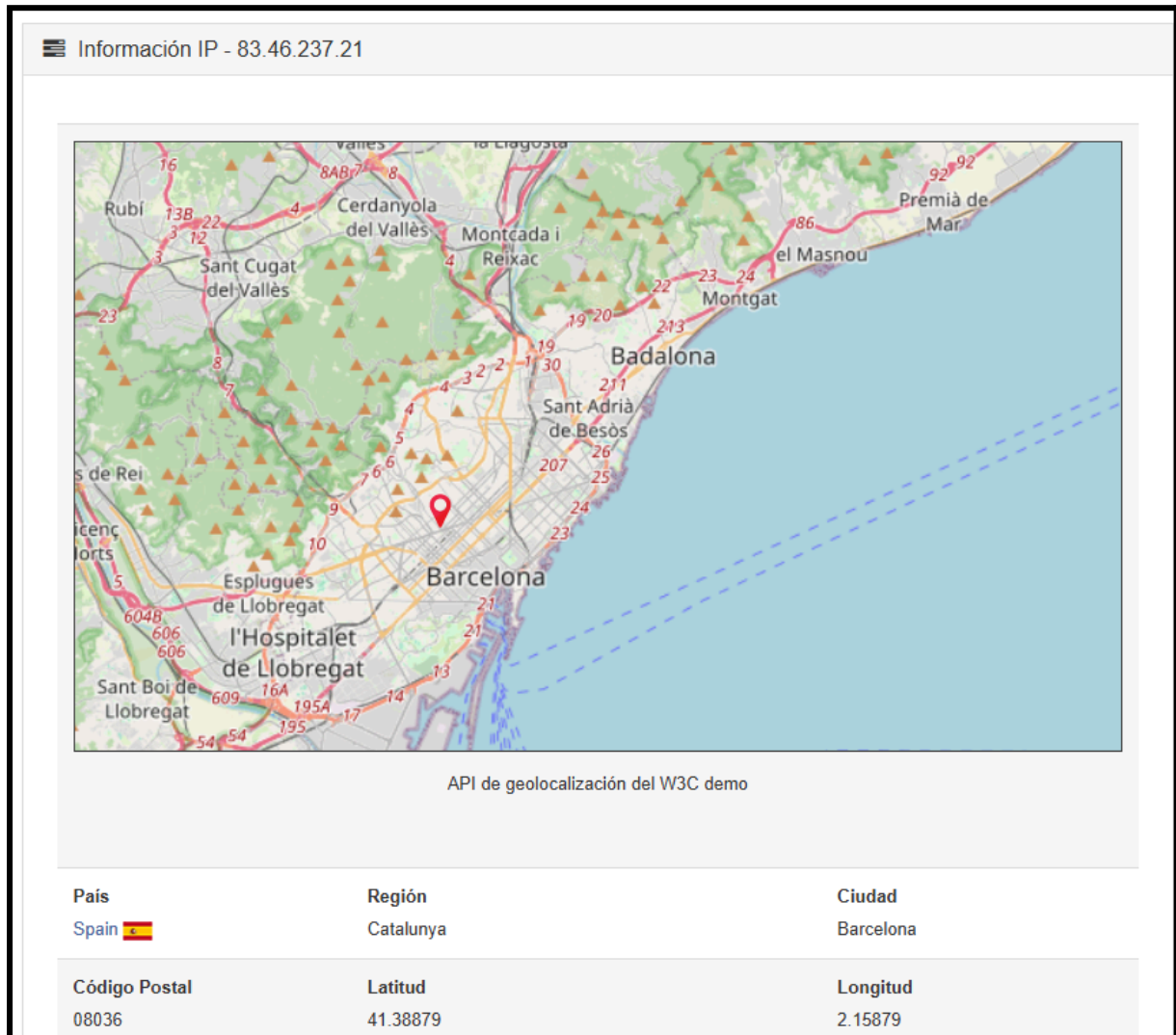
El agente de usuario revela que los accesos se hicieron desde un sistema Linux i586 utilizando el navegador Mozilla Firefox 31.0, lo que es consistente con configuraciones técnicas avanzadas no habituales en usuarios comunes.

Mediante consulta de geolocalización IP (basada en datos de [IPinfo.io](https://ipinfo.io) y [IP2Location](https://ip2location.com)), se determinó que **la dirección IP 83.46.237.21 está asignada al proveedor Telefónica de España, y se encuentra registrada en la ciudad de Barcelona, código postal 08038, perteneciente a la región autónoma de Cataluña, España.**

Conclusión:

La dirección IP utilizada en los accesos al servidor se geolocaliza en Barcelona, España, lo que permite establecer un punto de origen técnico para las conexiones no autorizadas registradas el 22 de abril de 2025.

Evidencia – Geolocalización de la dirección IP 83.46.237.21:



Pregunta 5: ¿Qué navegador se utilizó para acceder al servidor?

El archivo de registros **acceso-22_Abril.log** evidencia múltiples peticiones realizadas desde la IP **83.46.237.21** al servidor web de la empresa. Cada solicitud contiene el campo **User-Agent**, el cual permite identificar el navegador utilizado.

El análisis de los registros muestra que todas las solicitudes fueron realizadas empleando el siguiente navegador:

- **Navegador:** Mozilla Firefox
- **Versión:** 31.0
- **Motor de renderizado:** Gecko 20100101

Se identifican **7 solicitudes HTTP** en el log, todas desde la misma dirección IP y utilizando el mismo navegador.

Conclusión:

El navegador utilizado en las conexiones del 22 de abril de 2025 fue **Mozilla Firefox 31.0**, siendo registrado en **7 accesos consecutivos** desde la IP 83.46.237.21.

Evidencia : Archivo logs de conexión del 22 de abril.

```
83.46.237.21 - - [22/Apr/2025:22:02:16 +02:00] "GET /login.php HTTP/1.1" 200 321 "-" "Mozilla/5.0 (X11; Linux i586; rv:31.0) Gecko/20100101 Firefox/31.0"
83.46.237.21 - - [22/Apr/2025:22:02:18 +02:00] "GET /login.php HTTP/1.1" 200 321 "-" "Mozilla/5.0 (X11; Linux i586; rv:31.0) Gecko/20100101 Firefox/31.0"
83.46.237.21 - - [22/Apr/2025:22:02:21 +02:00] "GET /login.php HTTP/1.1" 200 321 "-" "Mozilla/5.0 (X11; Linux i586; rv:31.0) Gecko/20100101 Firefox/31.0"
83.46.237.21 - - [22/Apr/2025:22:08:22 +02:00] "GET /muestra_registro.php?cliente=aaa&registro=1 HTTP/1.1" 200 392 "-" "Mozilla/5.0 (X11; Linux i586; rv:31.0) Gecko/20100101 Firefox/31.0"
83.46.237.21 - - [22/Apr/2025:22:09:12 +02:00] "GET /muestra_registro.php?cliente=aaa&registro=2 HTTP/1.1" 200 392 "-" "Mozilla/5.0 (X11; Linux i586; rv:31.0) Gecko/20100101 Firefox/31.0"
83.46.237.21 - - [22/Apr/2025:22:09:44 +02:00] "GET /muestra_registro.php?cliente=aaa&registro=3 HTTP/1.1" 200 392 "-" "Mozilla/5.0 (X11; Linux i586; rv:31.0) Gecko/20100101 Firefox/31.0"
83.46.237.21 - - [22/Apr/2025:22:13:27 +02:00] "GET /muestra_registro.php?cliente=aaa&registro=1 HTTP/1.1" 200 392 "-" "Mozilla/5.0 (X11; Linux i586; rv:31.0) Gecko/20100101 Firefox/31.0"
```

Pregunta 6: ¿A qué hora se registró el último acceso o petición hacia el servidor?

El análisis del archivo de registro del servidor (acceso-22_Abril.log) revela múltiples solicitudes HTTP realizadas desde la dirección IP **83.46.237.21**, durante la noche del **22 de abril de 2025**.

Cada línea del log incluye una marca temporal en formato de fecha y hora, conforme al huso horario del servidor (+02:00 CEST). Se identificaron accesos a páginas como /login.php y /muestra_registro.php, realizados de forma secuencial.

La última entrada registrada en el log es la siguiente:

```
83.46.237.21 - - [22/Apr/2025:22:13:27 +02:00] "GET /muestra_registro.php?cliente=aaa&registro=1 HTTP/1.1" 200 392 "-" "Mozilla/5.0 (X11; Linux i586; rv:31.0) Gecko/20100101 Firefox/31.0"
```

Esta línea corresponde a una solicitud GET legítima, finalizando la secuencia de conexiones desde dicha IP.

Conclusión:

El último acceso registrado hacia el servidor el 22 de abril de 2025 se produjo a las **22:13:27 horas (CEST)**, desde la dirección IP **83.46.237.21**.

Evidencia : Archivo logs de conexión del 22 de abril.

```
83.46.237.21 - - [22/Apr/2025:22:13:27 +02:00] "GET /muestra_registro.php?cliente=aaa&registro=1 HTTP/1.1" 200 392 "-" "Mozilla/5.0 (X11; Linux i586; rv:31.0) Gecko/20100101 Firefox/31.0"
```

Pregunta 8: ¿Es un correo válido o se trata de una suplantación?

El archivo de correo electrónico proporcionado, **Clase06.eml**, fue sometido a un análisis detallado de sus encabezados SMTP. El supuesto remitente del mensaje es:

- **Nombre:** Danilo Perez
- **Correo electrónico:** daniel.perez@primax.com

Sin embargo, el análisis de los encabezados revela múltiples indicadores técnicos de suplantación de identidad (spoofing):

- **Evidencias de suplantación:**

SPF (Sender Policy Framework):

spf=softfail (sender IP is 114.29.236.247)

1. El dominio primax.com no autoriza esta dirección IP como fuente legítima de envío.

DKIM (DomainKeys Identified Mail):

dkim=none (message not signed)

2. El correo no está firmado digitalmente, lo que impide validar su autenticidad.

DMARC (Domain-based Message Authentication):

dmarc=fail action=quarantine

3. El mensaje **no pasó la política de autenticación DMARC** del dominio del remitente.

Servidor de origen:

Message-ID: <...@emkei.cz>

4. Se utilizó el dominio **emkei.cz**, conocido generador de correos falsos para pruebas.

Dirección IP de envío real:

X-Sender-IP: 114.29.236.247

5. Esta dirección IP está ubicada fuera de los servidores autorizados por primax.com.

Conclusión:

El mensaje **no es válido**. Se trata de un caso claro de **suplantación de identidad (email spoofing)**, donde se intenta aparentar que el correo proviene del dominio legítimo primax.com, pero en realidad fue enviado desde un servidor externo no autorizado. Esto evidencia una posible **intención**

fraudulenta o de ingeniería social, con riesgo para la integridad de la empresa receptora.

Evidencia : Archivo correo electrónico. Clase6.eml

Estimados, buenos dias

Mucha suerte en el Reto Forense!!

-----METADATA-----

Content-Type: message/rfc822

Message-From: Danilo Perez <daniel.perez@primax.com>

Message-To: empresa01HM@hotmail.com

Message-From-Email: daniel.perez@primax.com

Message-From-Name: Danilo Perez

Message:Raw-Header:Authentication-Results: spf=softfail (sender IP is 114.29.236.247) smtp.mailfrom=primax.com; dkim=none (message not signed) om;compauth=fail reason=000

Message:Raw-Header:Content-Type: text/plain; charset="utf-8"

Message:Raw-Header:Errors-To: daniel.perez@primax.com

Message:Raw-Header:MIME-Version: 1.0

Message:Raw-Header:Message-ID: <20250422181848.E192619E2@emkei.cz>

5. Resumen técnico de hallazgos.

La evidencia analizada permite establecer que:

- Se recuperaron archivos confidenciales del proyecto **RecoveryDat** desde un dispositivo USB.
- Algunos archivos presentan fechas posteriores a la desvinculación del Sr. Martín Velasco, lo que indica posible acceso no autorizado.
- Los registros del servidor muestran conexiones remotas desde una IP ubicada en Barcelona, en la misma fecha.
- El navegador utilizado y la arquitectura del sistema operativo indican un entorno técnico personalizado, potencialmente orientado al anonimato.

- Se detectó un intento de suplantación de identidad mediante un correo falsificado, con múltiples fallos en autenticación (SPF, DKIM, DMARC).

Nota final:

Los hallazgos aquí expuestos deben considerarse **evidencia técnica**, y su interpretación legal o disciplinaria corresponde exclusivamente a las instancias competentes.