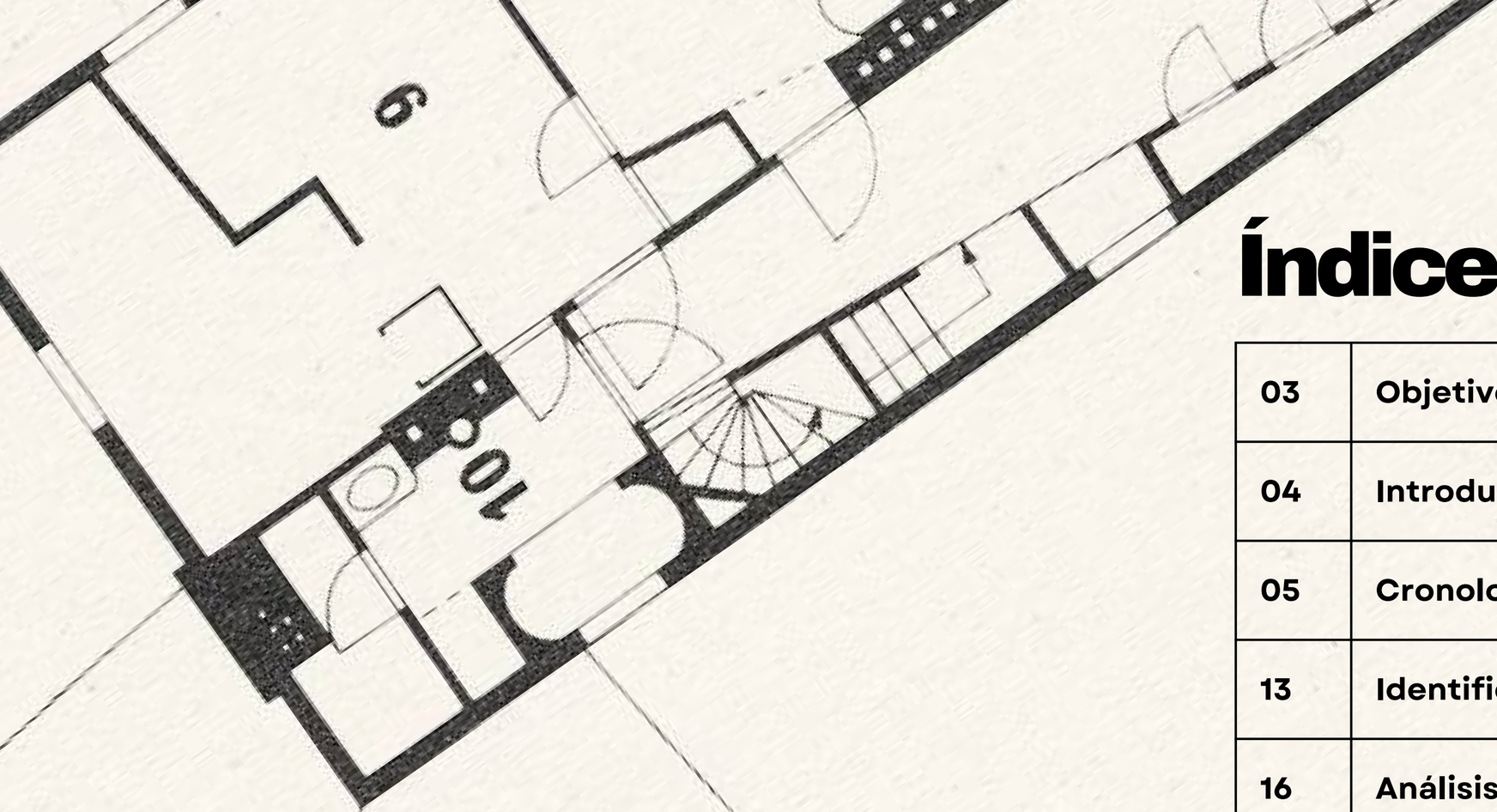
ROBO EN EL LOUVRE

Reconstrucción OSINT

PRESENTACIÓN DE:
Jon Ormaechea Caro



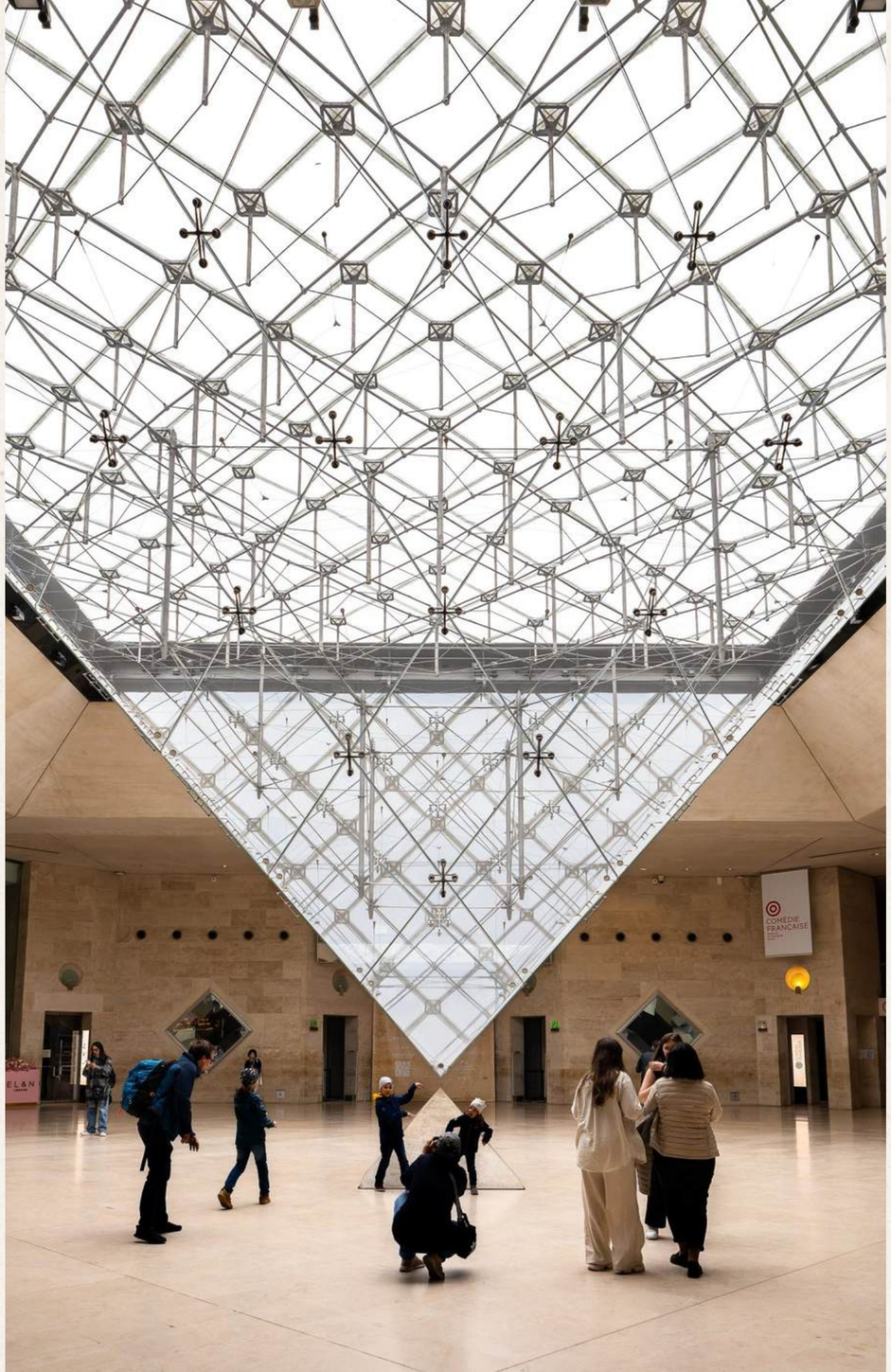
Índice

Objetivos

01 Analizar el robo usando información OSINT y extraer lecciones de ciberseguridad y gestión de riesgos físicos/digitales.

02 Cómo reconstruir el ataque paso a paso usando fuentes abiertas.

03 Simulación de como un atacante podría comprometer el sistema principal del museo



¿Por qué es relevante para la ciberseguridad?

Este caso evidencia cómo unas infraestructuras tecnológicas desactualizadas y una gestión desatendida de los sistemas pueden generar fallos críticos en la seguridad. Además, veremos cómo un atacante puede aprovechar información pública, rutinas operativas previsibles y debilidades organizativas para explotar una infraestructura que, pese a su apariencia de fortaleza, carece de la resiliencia tecnológica necesaria para responder de forma eficaz.

Introducción

¿Qué ocurrió?

El 19 de octubre de 2025, un grupo de cuatro ladrones disfrazados de obreros accedió a la Galería de Apolo del Museo del Louvre y robó nueve piezas de las Joyas de la Corona francesa en una operación que duró apenas siete minutos, con un botín valorado en unos 88 millones de euros.

Le Monde

FRANCE • LOUVRE HEIST

Forgotten Louvre security report highlighted specific balcony used by crown jewel thieves

Le Monde has learned that a 2018 security audit explicitly identified the balcony used by the thieves as a point of vulnerability, even noting the possibility that a freight lift could be used to access it.

By Jacques Follorou
Published on November 25, 2025, at 9:01 pm (Paris) · 4 min read · Lire en français

The New York Times

Inside the Heist That Shocked the World

More than a week after thieves made off with treasures from the Louvre, a picture is emerging of a seemingly well-planned burglary that exploited security lapses at the museum and outpaced the police.

The Guardian

Explainer

How the Louvre museum robbery happened in video, photographs and maps

Eight pieces stolen, but crown of Napoleon III's wife dropped by the fleeing thieves

europapress

INTERNACIONAL

El Gobierno francés confirma un robo en el Louvre y declara el cierre provisional del museo

La ministra de Cultura lamenta la sustracción de un botín de "un valor incalculable"

THE TIMES

Louvre museum security 'outdated and inadequate' at time of heist

A leaked report reveals a lack of CCTV equipment in rooms where priceless French artefacts were displayed

EL PAÍS

MUSEO DEL LOUVRE >

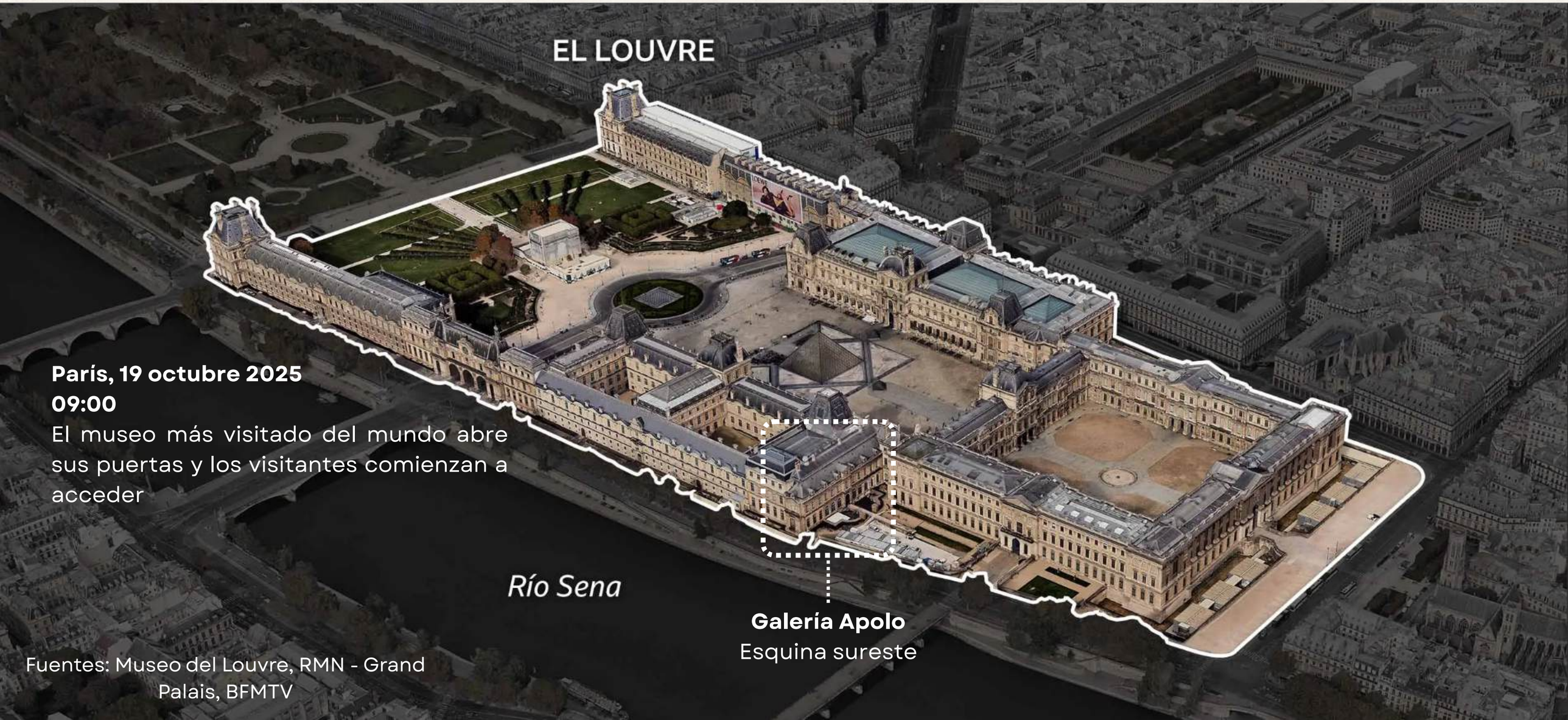
Robo en el Louvre: unos encapuchados se llevan ocho joyas de la Corona francesa con una radial

El valor de las piezas desaparecidas es "inestimable", entre ellas broches, tiaras y collares de la emperatriz Eugenia de Montijo y las reinas María Amelia y Hortensia

BBC

El paso a paso del espectacular robo al museo del Louvre en París

Cronología



París, 19 octubre 2025
09:00
El museo más visitado del mundo abre sus puertas y los visitantes comienzan a acceder

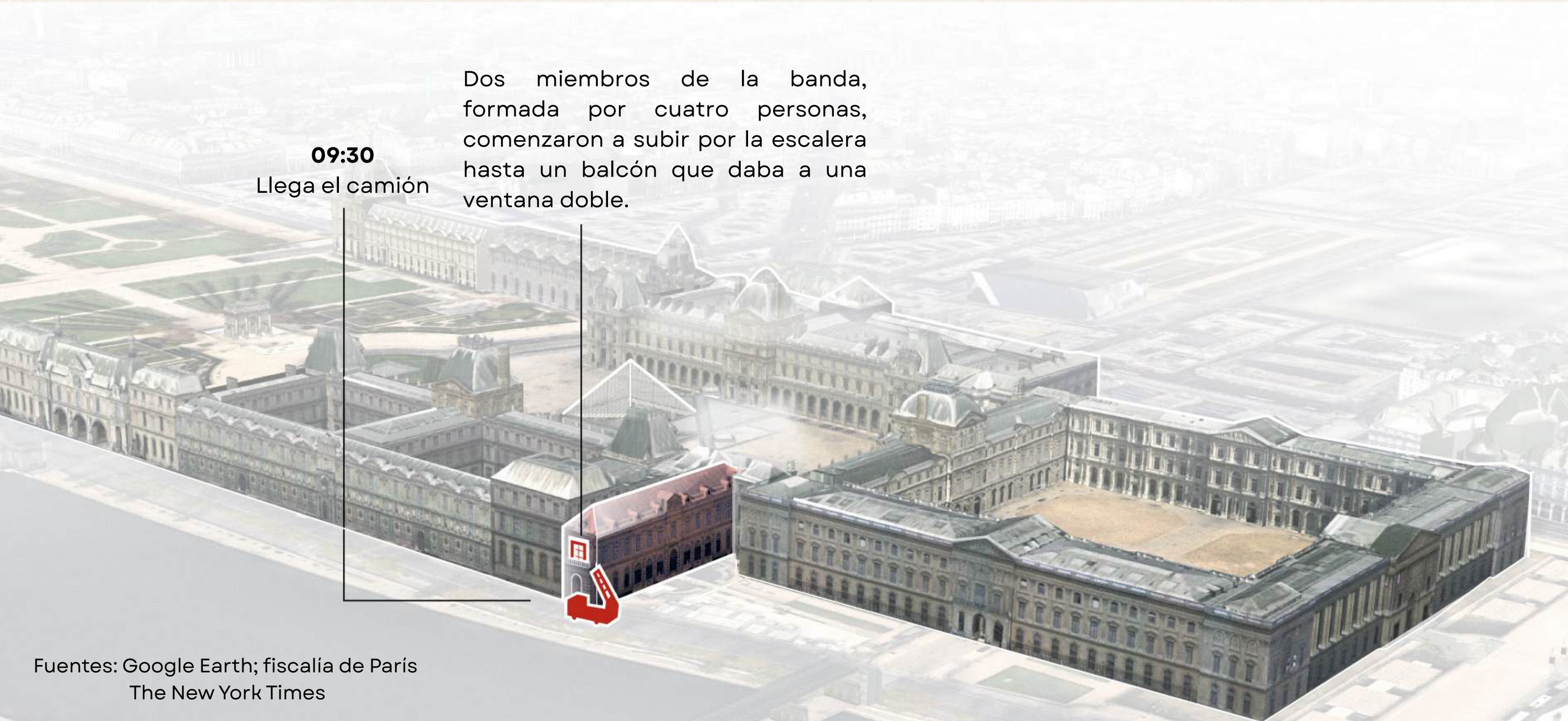
Galería Apolo
Esquina sureste

Fuentes: Museo del Louvre, RMN - Grand Palais, BFMTV

Cronología

09:30
Llega el camión

Dos miembros de la banda, formada por cuatro personas, comenzaron a subir por la escalera hasta un balcón que daba a una ventana doble.



Fuentes: Google Earth; fiscalía de París
The New York Times

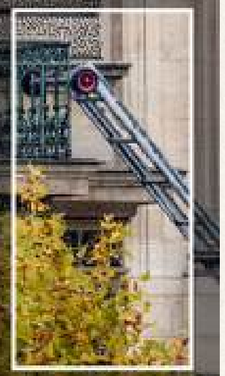
Cronología

Cámara de seguridad apuntaba en la otra dirección, hacia el oeste

09:34
Intrusión

Ventana cortada

Montacargas eléctrico



Fuentes: fiscalía de París
The New York Times

Alarms began sounding in the guards' control room when the window was breached, and new alerts were sent as the thieves

Cinco miembros del personal del museo se encontraban en la Galería Apolo o cerca de ella. Siguieron el protocolo de seguridad del Louvre y se pusieron en contacto con la policía, "dando prioridad a la protección de las personas", según un comunicado del Ministerio de Cultura francés.

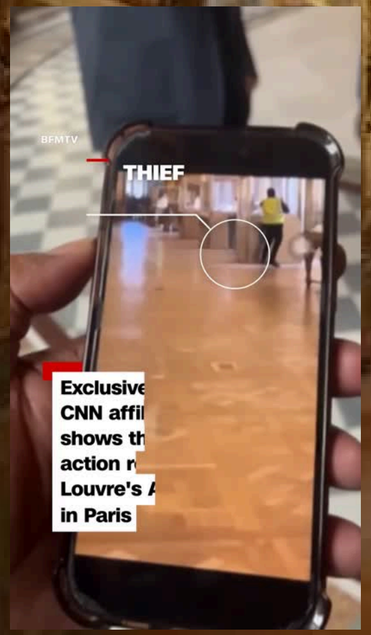
Los guardias de seguridad evacuaron el museo.

Cronología

BBC Verify confirmó que las imágenes se grabaron desde la esquina suroeste de la galería.

Las imágenes de las cámaras de seguridad del interior del museo confirman que les llevó no más de tres minutos y 57 segundos para forzar dos vitrinas, hacerse con las joyas y huir, según declaró un ministro francés.

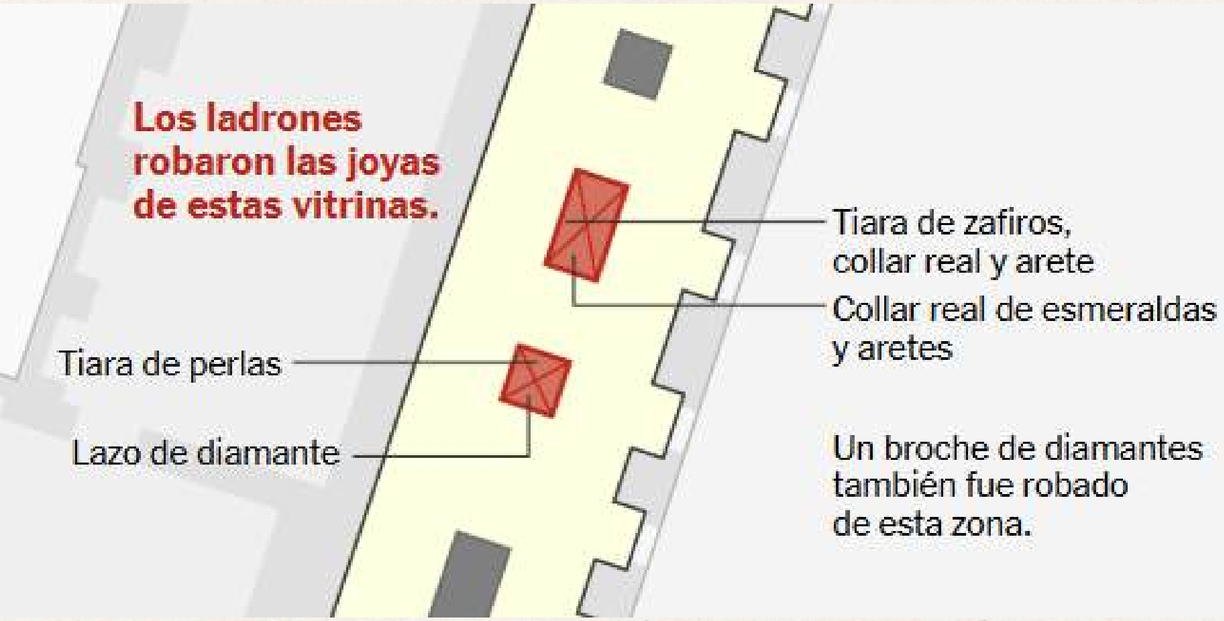
Los ladrones fueron rápidos y determinados: sabían exactamente lo que buscaban.



Fuentes:BFMTV, BBC, fiscalía de París, The New York Times

Vitrinas robadas

Cronología



Tras irrumpir en la galería, **el primer ladrón se dirigió directamente a la quinta vitrina de una fila de 200 pies**, que contenía el regalo de boda de Napoleón junto con un collar de zafiros y una tiara y pendientes que habían pertenecido a la última reina de Francia, María Amelia. **El segundo ladrón, que llevaba un casco de motocicleta, atacó la vitrina contigua.**

Fuentes: Le Parisien, BBC, fiscalía de París, The New York Times

1-3 Tiara, collar y un par de pendientes usados por la reina Hortensia de Holanda y la reina María Amelia

4-5 Collar y pendientes de esmeraldas regalados por Napoleón Bonaparte a su segunda esposa, María Luisa, como regalo de boda

6-7 Tiara de perlas y diamantes y broche de diamantes de la emperatriz Eugenia

8 Broche conocido como el "broche relicario"

Cronología

Fuentes: Le Parisien, The New York Times

09:36 Aviso a la policía

> attacked the two cases, according to the museum director's testimony. From that room, the museum's chief operations manager called the closest police station, just over half a mile away, the Louvre's head of security, Dominique Buffin, told

Nuevas alertas se activaron mientras los ladrones atacaban las dos vitrinas. Según declaró el director del museo, desde esa sala **el responsable de operaciones llamó a la comisaría** más cercana, situada a poco más de medio kilómetro.

09:37 Se solicita cierre de puertas

> The footage seen by Le Parisien showed what happened next in the gallery, the newspaper reported. The thieves remained calm while working, even as two museum guards tried to scare them off. One approached with a metal pole, but one of the intruders waved him back.

Los ladrones siguieron trabajando con calma incluso cuando **dos guardias intentaron ahuyentarlos**. Uno se acercó con una barra metálica, pero **uno de los intrusos lo hizo retroceder con un gesto.**

Cronología

09:38 Huida

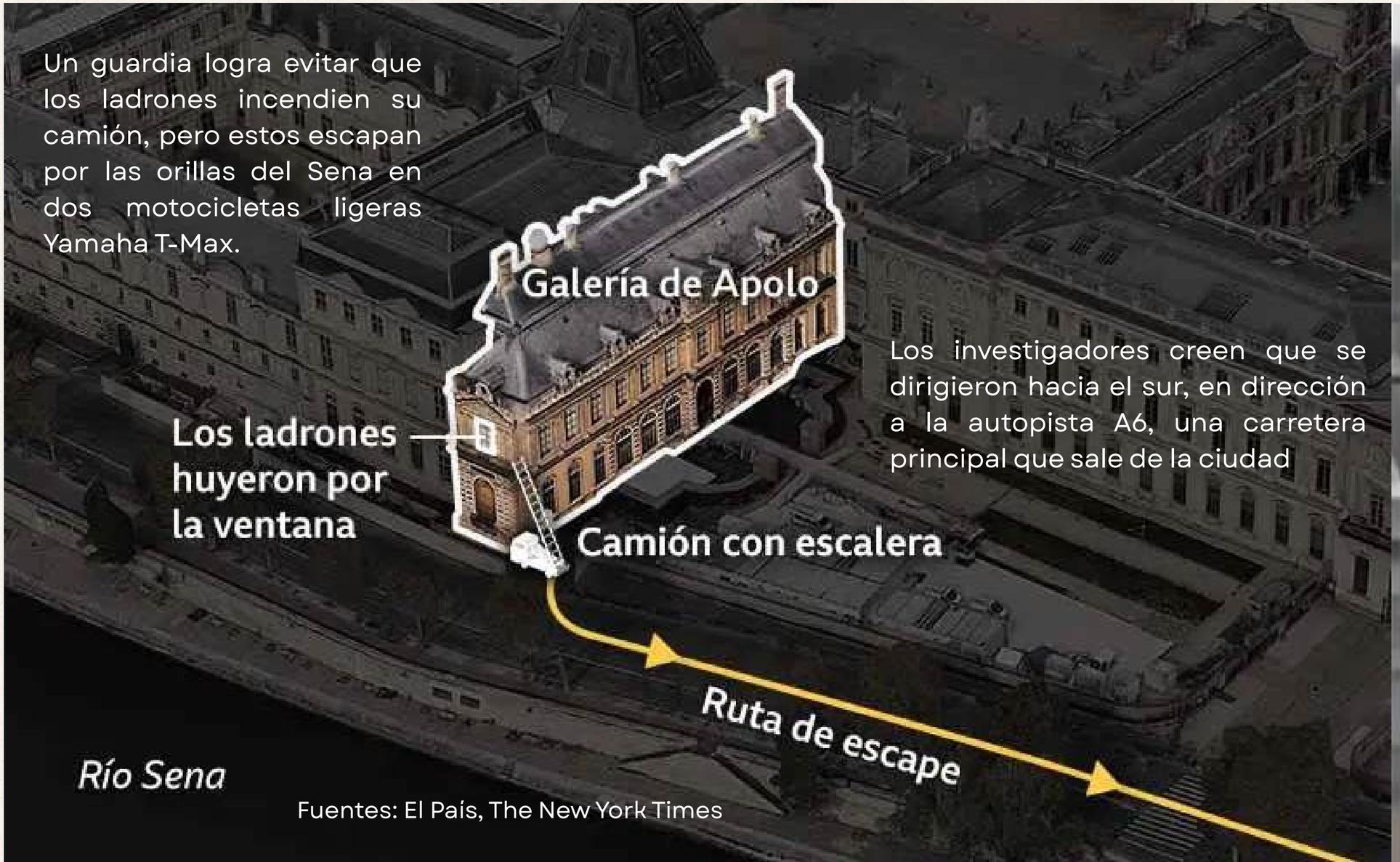
No todo salió según lo previsto: la policía confirmó que posiblemente a los ladrones **se les cayó la corona de la emperatriz Eugenia** y, aunque dañada, la encontraron en la ruta de escape.

Fuentes: BBC, fiscalía de París, The New York Times

> Then the burglars' composure seemed to crack; they got sloppy. One dropped some jewelry and stopped to stuff it back into his bag, but the burglars left a glove and jeweled brooch behind. The footage also showed the helmeted thief diving head first into the ladder's basket, the newspaper reported.

"Entonces, la compostura de los ladrones pareció quebrarse; se volvieron descuidados. ***Uno dejó caer algunas joyas y se detuvo para volver a meterlas en su bolsa****, pero los ladrones dejaron atrás un guante y un broche con incrustaciones. Las imágenes también mostraron al* ***ladrón con casco lanzándose de cabeza dentro de la cesta de la escalera****, según informó el periódico."*

Cronología



Fuentes: El País, The New York Times

Identificación de sospechosos

Operario de limpieza de 34 años
Arrestado el 25 de octubre, mientras intentaba abordar un avión hacia Argelia en el aeropuerto París-Charles de Gaulle.

Su ADN fue recuperado de un scooter utilizado en la huida.

Hombre de 37 años
Arrestado el 29 de octubre en el suburbio parisino de Seine-Saint-Denis.

Su ADN fue hallado en el elevador mecánico utilizado para entrar al museo.

Mujer de 38 años
Arrestada el 29 de octubre en Seine-Saint-Denis.

Es pareja desde hace tiempo del sospechoso de 37 años y ha negado su implicación en el robo.

Taxista de 39 años
Arrestado el 25 de octubre en su domicilio en el suburbio parisino de Aubervilliers.

Había sido arrestado anteriormente por robo con agravantes.

Su ADN fue encontrado en una ventana del Louvre.

Niakate Abdoulaye
Había trabajado como vigilante de seguridad en el Centro Pompidou.

Poseía antecedentes por 15 delitos, incluido un robo de joyería en 2014.

Conocido en redes sociales como **“Doudou Cross Bitume”** publicaba vídeos de acrobacias en moto, entrenamiento callejero y contenido de fitness.

Fuentes: The Guardian, abc news,
The New York Times

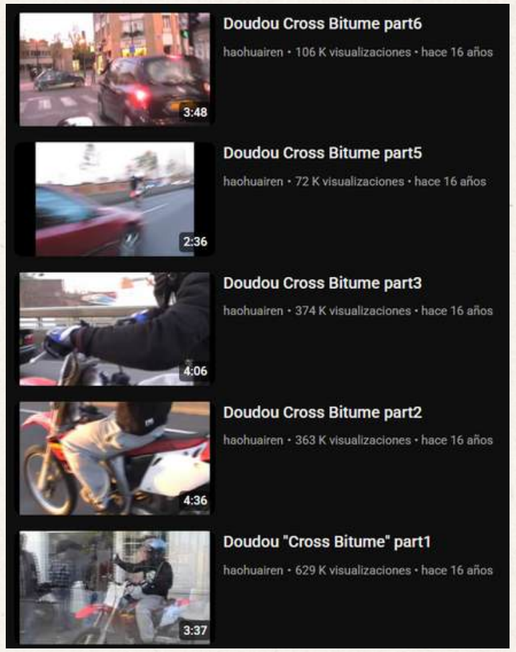
Identificación de sospechosos

Actualmente todas sus redes sociales personales permanecen privadas o eliminadas, sólo he podido acceder a su contenido a través de terceros.

“ DOUDOU CROSS BITUME AUBER 93”
TikTok @doudou.cross.bitu
Instagram @doudoucross6
Youtube haohuarien
Vimeo haohuai / antho-4 (contenido relacionado)

Sus redes sociales giran en torno al motocross urbano. Se volvió viral por sus acrobacias en moto en pleno centro de París, incluyendo vídeos haciendo caballitos en los Campos Elíseos, una de las imágenes más difundidas antes de su detención. Le Point lo describe como una “leyenda urbana del motocross de los años 2000”, famoso por recorrer el asfalto del barrio del Landy. En conjunto, su presencia digital está dominada por maniobras arriesgadas y contenido de calistenia

Fuentes: Telemadrid, Beauxarts

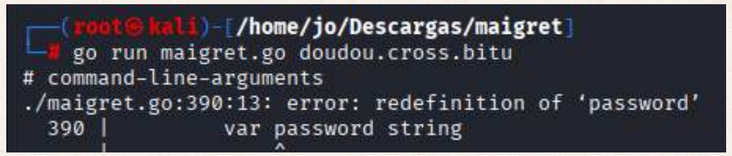


Identificación de sospechosos

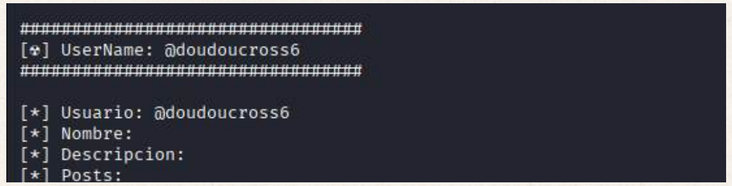
Las búsquedas OSINT realizadas a partir del nombre de usuario no han obtenido resultados relevantes, ya que ninguna de las herramientas empleadas ha identificado perfiles activos.

TikTok-OSINT

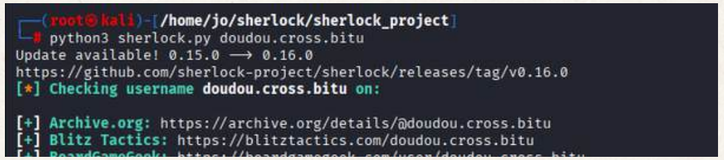
Maigret



NetSoc-OSINT

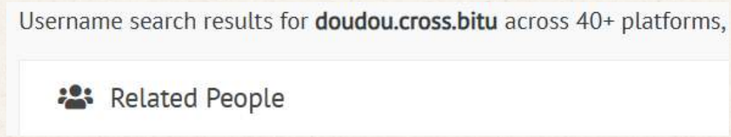


Sherlock

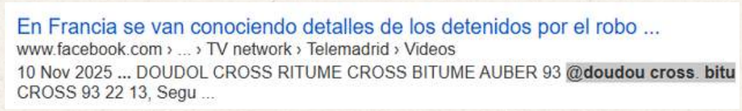


Mr.Holmes

idcrawl.com

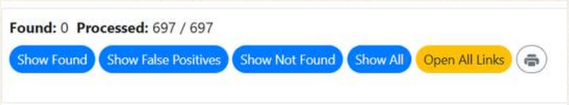


Social-searcher.com

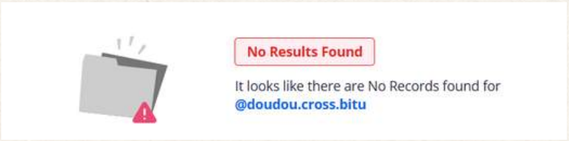


instantusername.com

whatsmyname.app

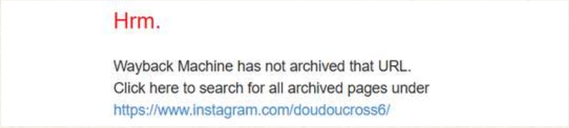


Socialcatfish.com



megalodon.jp

Waybachmachine



Análisis OSINT

Fuentes: The Hill, Swissinf.ch, AFP, ABC

Böcker, la empresa del montacargas le dijo a la agencia de noticias francesa AFP que reconoció el aparato de su empresa por las noticias, y afirmó que la máquina fue vendida "hace unos años a un cliente francés que alquila este tipo de equipos en París y alrededores".

A ese cliente, que desea estar anónimo, dijo Böcker, ***los ladrones del Louvre pidieron una demostración de la máquina la semana pasada y la robaron durante la muestra****. "Retiraron el logo del cliente y cambiaron la placa de matrícula", añadió*

Además la plataforma elevadora usada por los ladrones era idéntica a las que se usan en las restauración de fachadas periódicas del museo.

El robo del Louvre, convertido en motivo publicitario para la empresa del montacargas

«El robo del museo más famoso y visitado del mundo podría servir para llamar la atención sobre la calidad de los productos de nuestra compañía», dijo el director de la empresa

Análisis OSINT

Búsqueda de información a través de la matrícula **EV - 698 - HA**
Debido a la legislación francesa no se puede obtener información concluyente con el SIV de la matrícula. Lo he confirmado usando distintas herramientas como:

Gideon

```
[Gideon/main/carNphone/category] >> 2
Enter Car Number(a111aa77) >> EV-698-HA
[no result]
http://avto-nomer.ru/ru/gallery.php?fastsearch=ev-698-ha
```

Siv-auto.fr

Gateway Timeout

The gateway did not receive a timely response from the upstream server or application.

Lo único que he podido obtener ha sido información genérica a por medio de **Licencesplatesmania.com**, como el código **75** y el símbolo rojo con forma de estrella a la derecha de la matrícula hacen referencia a la ciudad París.

Région îledeFrance

Análisis OSINT

los sistemas de seguridad ya eran evidentes en 2014 y 2017, según auditorías de seguridad confidenciales anteriores revisadas por Libération . Por ejemplo, el museo aún utilizaba Windows 2000 en la red de su oficina cuando la Agencia Nacional de Ciberseguridad francesa (ANSSI)

La **Agencia Nacional de Ciberseguridad francesa** (ANSSI) realizó su auditoría de **2014** y determinó que:

· El museo aún utilizaba **Windows 2000** en la red de su oficina.

· Un servidor de videovigilancia funcionaba con la contraseña "**LOUVRE**".

· El nombre de usuario "**THALES**" otorgaba acceso a la aplicación de videovigilancia Thales.

En **2017** se realizó una segunda auditoría, a cargo del **Instituto Nacional de Estudios Superiores en Seguridad y Justicia (INHESJ)**

· Estaciones de trabajo están equipadas con sistemas operativos obsoletos como **Windows 2000/XP** y **servidores Windows Server 2003**

Fuentes: Le monde, Liberation, bbc, Solutions-numeriques,The New York Times

Análisis OSINT

El Tribunal de Cuentas, que examinó el período comprendido entre **2019 y 2024**, observó **retrasos significativos en la modernización de los sistemas de seguridad**. Los proyectos de renovación de los sistemas de videovigilancia y control de acceso, planificados ya en 2017, se han pospuesto repetidamente debido a limitaciones presupuestarias, trabas burocráticas y falta de coordinación entre los departamentos técnicos del museo.

El informe de la **ANSSI** destaca un riesgo importante: **la interconexión de las redes de oficinas y los sistemas de seguridad**. Esta arquitectura, en caso de intrusión, **permitía la manipulación física mediante acceso informático**.

Este caso ilustra un problema más amplio: tanto en edificios patrimoniales como en infraestructuras complejas, **la ciberseguridad ya no es un ámbito separado de la seguridad**, sino que ahora es un pilar fundamental de esta.

Fuentes: Le monde, Liberation, bbc, Solutions-numeriques,The New York Times

Análisis OSINT

Fuentes: PVPP (2009-2011),Libération, TechSpot, The Independent

Reprise des partenariats existants : forum des Halles - carrousel du Louvre - parc des expositions de la porte de Versailles - palais des congrès de la porte Maillot - Printemps Haussmann - musée du Louvre. Les arrêtés préfectoraux d'autorisation sont modifiés dès lors qu'un déport d'images est envisagé avec la PP sur la base

El PVPP es el Plan de Videoprotección para París, diseñado para integrar y coordinar los sistemas de cámaras urbanas de múltiples entidades públicas y privadas bajo una arquitectura común de seguridad y gobernanza.

El **informe del Comité d'éthique du PVPP** (2009-2011) muestra que **el Louvre se integran como socios de videoprotección** cuyos flujos de imágenes pueden ser desviados hacia la Prefectura de Policía, mediante convenios específicos y modificaciones de los arrêtés préfectoraux. Aunque **no existen pruebas públicas de que este sistema comprometido haya servido de vector hacia el PVPP**, **la combinación de interconexión estructural y debilidades internas convierte al Louvre en un eslabón débil potencial dentro del ecosistema de videoprotección parisino**, con un riesgo escalable teórico hacia la videovigilancia combinada si las segmentaciones de red y las barreras técnicas no fueran suficientes.

Análisis OSINT

Fuentes: abc news, fiscalía de París, The New York Times

Vestidos con chalecos reflectantes y pasamontañas los ladrones ascendieron al segundo para cortar el vidrio del balcón.
Los cristales y los paneles de madera no resistieron las **amoladoras eléctricas**: las autoridades francesas confirmaron que las ventanas de la opulenta galería no están reforzadas.

> And they cut hand-sized holes with specialized tools that the Louvre's own firefighting manual says are efficient for opening cases if there's a blaze. Experts said the cases that display museums' most valuable items are normally designed to withstand some 140 hammer blows or ax strikes, enough to exhaust a thief, and they called the use of disc grinders innovative.

Los ladrones emplearon herramientas especializadas para cortar agujeros del tamaño de una mano en las vitrinas, **las mismas que el manual contra incendios del Louvre** recomienda como eficaces para abrirlas en caso de fuego. Estas vitrinas, diseñadas para proteger objetos de gran valor, están construidas para resistir hasta 140 golpes de martillo o hacha, una barrera pensada para agotar físicamente a cualquier intruso.

Análisis OSINT

Les salles

La galerie d'Apollon, fermée en mars 2019, a rouvert au public fin décembre. Le dépoussiérage des peintures et des décors de stuc s'est accompagné de celui des tapisseries. Les Diamants de la Couronne et les bijoux historiques ont été regroupés au cœur de la galerie, désormais accessible des deux côtés, dans trois nouvelles vitrines,

d'exposition d'œuvres. Le SPSI, épaulé par les sapeurs-pompiers de la huitième compagnie, a su s'adapter aux situations avec rapidité et efficacité. Les plans de sauvegarde des œuvres ont été déclenchés avec une mise en place d'un éventail de modes d'action : protection et évacuation des œuvres, découpe de vitrines… Ces exercices illustrent l'importance de la prise en compte du plan de sauvegarde des œuvres par le SPSI.

Fuentes: Informe de actividades Museo Louvre 2019

*"**La Galería de Apolo**, cerrada desde marzo de 2019, volvió a abrir al público a finales de diciembre tras un proceso de limpieza que incluyó pinturas, decoraciones de estuco y tapices. **Los Diamantes de la Corona y otras joyas históricas se reunieron en el centro de la galería**, ahora accesible por ambos lados, dentro de **tres nuevas vitrinas**. La colección de gemas de la Corona también recibió una presentación renovada en las vitrinas históricas. Tanto la iluminación como **los sistemas de seguridad fueron completamente modernizados**, al igual que las antiguas vitrinas de madera dorada y su interior."*

El plan de salvaguarda de las obras (PSO)

*"Se activaron los planes de protección de las obras, aplicando distintas medidas como **la protección y evacuación de piezas, así como la apertura o corte de vitrinas** cuando fue necesario."*

Análisis OSINT

« LE CHARIOT EST UN ÉLÉMENT DE PREMIÈRE INTERVENTION »

SERGENT-CHEF MATTHIEU LELOUP, INVENTEUR DU CHARIOT DE SAUVEGARDE

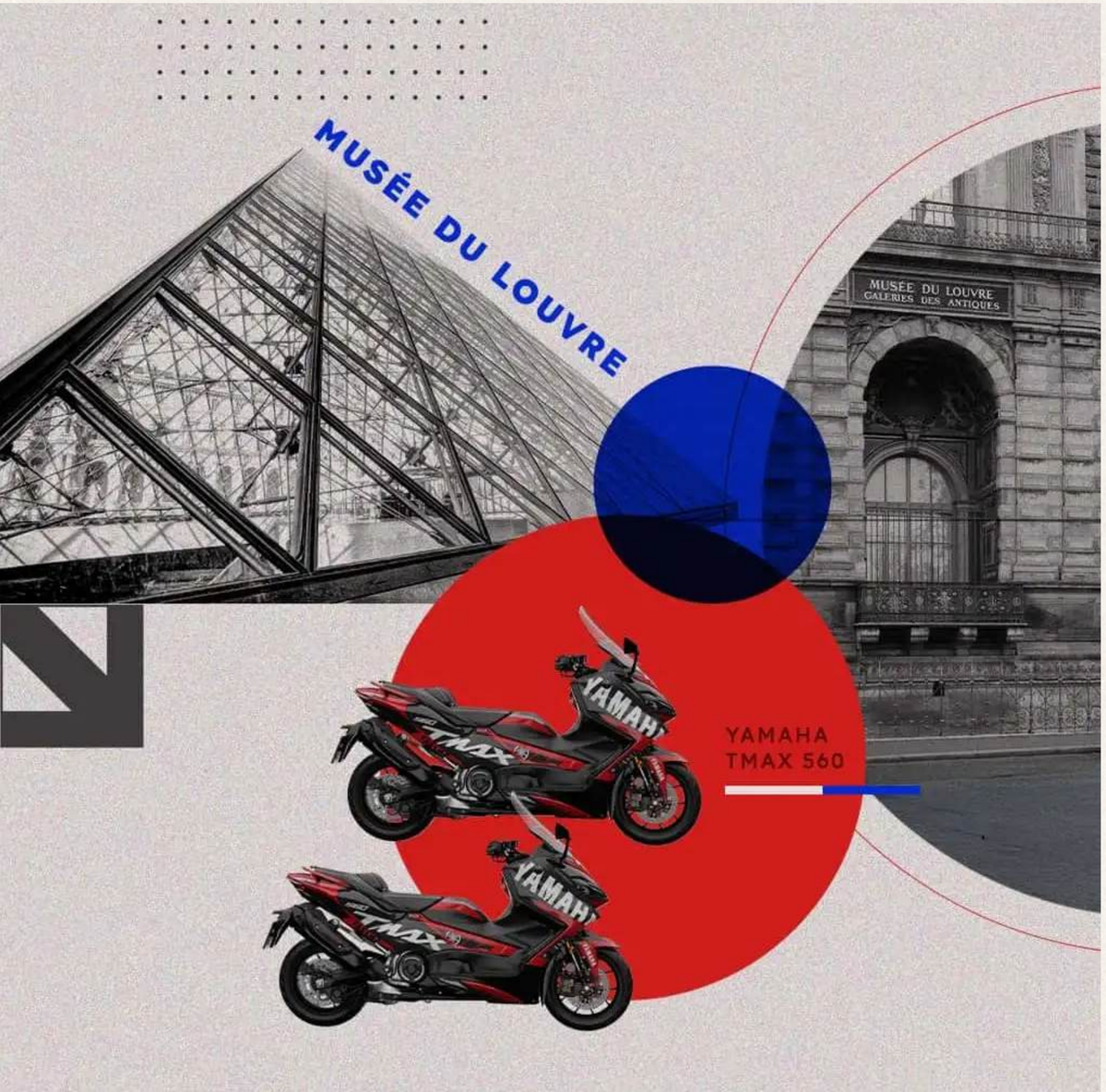
«El carro es un elemento de primera intervención»
Sargento jefe Matthieu Leloup, inventor del carro de salvaguarda

Las amoladoras eléctricas utilizadas por los ladrones en el reciente robo al Museo del Louvre –herramientas que les permitieron abrir vitrinas blindadas y cortar cristales en cuestión de minutos– **coinciden con las que aparecen en un reportaje de mayo de 2021** dedicado a los bomberos del museo. En aquel artículo, se presentaba un innovador carro de intervención rápida diseñado para rescatar obras de arte en situaciones de emergencia, como incendios o inundaciones.

Fuentes: Allo18.fr

Les éléments du chariot de sauvegarde des œuvres

Análisis OSINT



Según informes, los investigadores encontraron su ADN en uno de los escaparates rotos y en objetos abandonados en el lugar. El ADN de su presunto cómplice se encontró en uno de los dos scooters Tmax utilizados en la huida.

La policía francesa confirmó que los autores **huyeron en dos scooters de gran cilindrada, unos Yamaha TMAX**, vistas en las cámaras de seguridad abandonando el perímetro del museo hacia la autopista A6. Es la misma combinación (rapidez,

Aunque existe un vídeo difundido por la prensa que muestra a varias motocicletas alejándose del museo, las imágenes no permiten identificar modelos ni matrículas, y las fuentes abiertas no detallan la dirección exacta que tomaron. El único elemento firme y consistente en todas las crónicas es la utilización de varias motos Yamaha Tmax como vehículo de fuga y la velocidad con la que abandonaron la zona del Louvre.

Fuentes: rideapart, Indianexpress, Mundodeportivo.

Análisis OSINT

CGI Group, una firma israelí de inteligencia que anteriormente ayudó a resolver un robo multimillonario en la Bóveda Verde de Dresde, Alemania, también ha sido incorporada para colaborar.

> Zvika Nave, chief executive, said he would not comment about its operations or clients.
>
> "However, as an exceptional case, we were approached by parties connected to the Louvre museum to assist in identifying those involved in the robbery, as well as in recovering the stolen treasures," he said.

Zvika Nave, director ejecutivo, *dijo que no comentaría sobre las operaciones ni los clientes.*
"Sin embargo, como caso excepcional, fuimos contactados por partes vinculadas al museo del Louvre para ayudar en la identificación de los implicados en el robo, así como en ***la recuperación de los tesoros sustraídos***", *declaró.*

Fuentes: BBC, CNN

Análisis OSINT

An Israeli security company says it has been contacted by the thieves behind the Louvre jewel heist, offering secret negotiations to sell the stolen items via the dark web.

La empresa, dijo que recibieron un mensaje cifrado a través de su sitio web cinco días después del robo, enviado por una persona que afirmaba representar a los ladrones.

*"Nos ofreció **negociar en la dark web para comprar las joyas robadas,** limitando el contacto a solo 24 horas", señaló Naveh.*
"La empresa mantuvo una serie de conversaciones codificadas con un representante de los ladrones y recibió indicios de que efectivamente poseía al menos parte de los objetos robados. Estaban huyendo y necesitaban deshacerse de su botín rápidamente"

CGI Group contactó con el Louvre a través de un intermediario y afirma que el museo no respondió.

Fuentes: Telegrafi, Il Tempo

"Perdimos credibilidad ante los ladrones y el Louvre perdió una oportunidad real de recuperar las joyas"

*Asegura que, hace unos meses, en una entrevista con el periódico italiano **Il Tempo**, advirtió sobre conversaciones en redes que sugerían planes para robar el Louvre.*

Según el director general, los países europeos más expuestos a los delitos contra el patrimonio artístico son Italia, Francia y Alemania: "La Mona Lisa del Louvre es uno de los objetivos más discutidos en los foros de la dark web. Los tesoros italianos son igualmente vulnerables, pero a menudo están insuficientemente asegurados o protegidos".

*"Lo que hace única la estrategia de CGI Group es el **uso de inteligencia artificial para monitorear la actividad delictiva** en línea, **especialmente en la dark web**. "Hace cinco años iniciamos diálogos estratégicos con personas sospechosas en línea.*
La IA nos permite cruzar datos, rastrear conversaciones e identificar amenazas de forma rápida y eficaz".

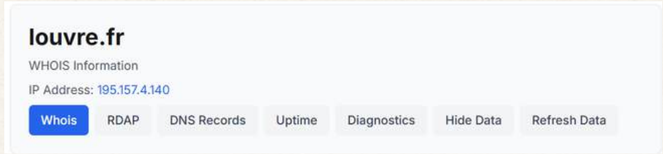
Análisis Web

Louvre.fr

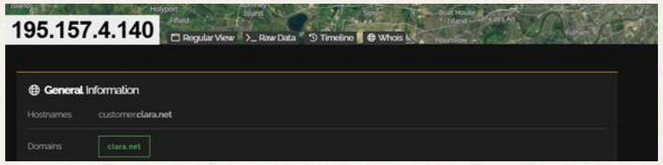
IP principal	195.157.4.140
Proveedor	Claranet
ASN	AS8426
Servidores NS autoritativos	ns0.fr.claradns.net ns2.fr.claradns.net ns1.fr.claradns.net
Seguridad web	Certificado HTTPS válido (Let's Encrypt) Redirección automática a HTTPS
Tecnologías detectadas	Servidor web basado en nginx nginx (backend) Varnish / WADP (capa de caché/proxy)
Ubicación del servidor	TW15, Ashford, Inglaterra

louvre.fr está alojado en una infraestructura gestionada por Claranet, **protegido con WAF**, con un enfoque en disponibilidad y delegación a un proveedor especializado a través de un DNS y hosting externalizados.

Whois



Shodan

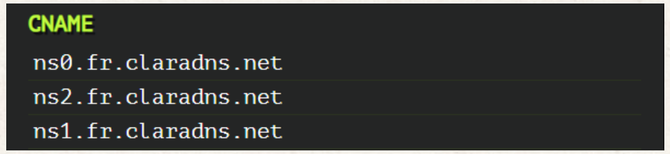


DNSDumpster

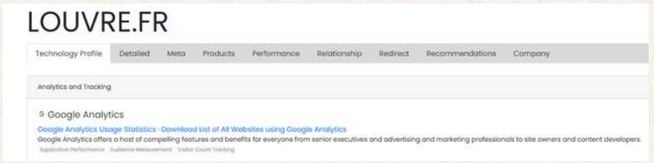
Whois Kali Linux

```
nserver:        ns0.fr.claradns.net
nserver:        ns1.fr.claradns.net
nserver:        ns2.fr.claradns.net
source:         FRNIC

registrar:      GANDI
address:        63-65 boulevard Massena
address:        75013 PARIS
country:        FR
phone:          +33.170377661
fax-no:         +33.143731851
e-mail:         support@support.gandi.net
website:        https://www.gandi.net/fr/tlds/fr/
anonymous:      No
registered:     2004-03-08T00:00:00Z
source:         FRNIC
```

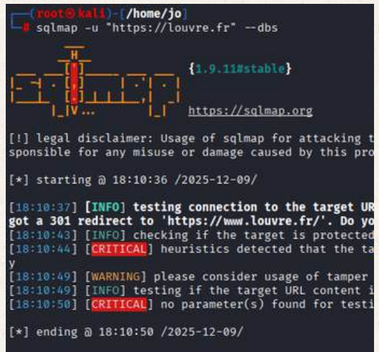
Webcheck



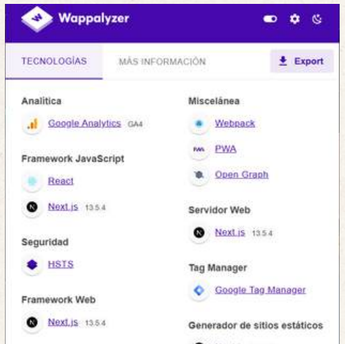
Builtwith



SQLmap



Wappalyzer



Análisis Web

Gobuster

```
┌──(root㉿kali)-[/home/jo]
└─# gobuster dir -u https://www.louvre.fr -w /usr/share/wordlists/dirb/common.txt
═══════════════════════════════════════════════════════════════
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
═══════════════════════════════════════════════════════════════
[+] Url:                     https://www.louvre.fr
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.8
[+] Timeout:                 10s
═══════════════════════════════════════════════════════════════
Starting gobuster in directory enumeration mode
═══════════════════════════════════════════════════════════════
Progress: 0 / 1 (0.00%)
2025/12/09 19:25:22 the server returns a status code that matches the provided options for non exi
status code or set the wildcard option.. To continue please exclude the status code or the length
```

Dirb

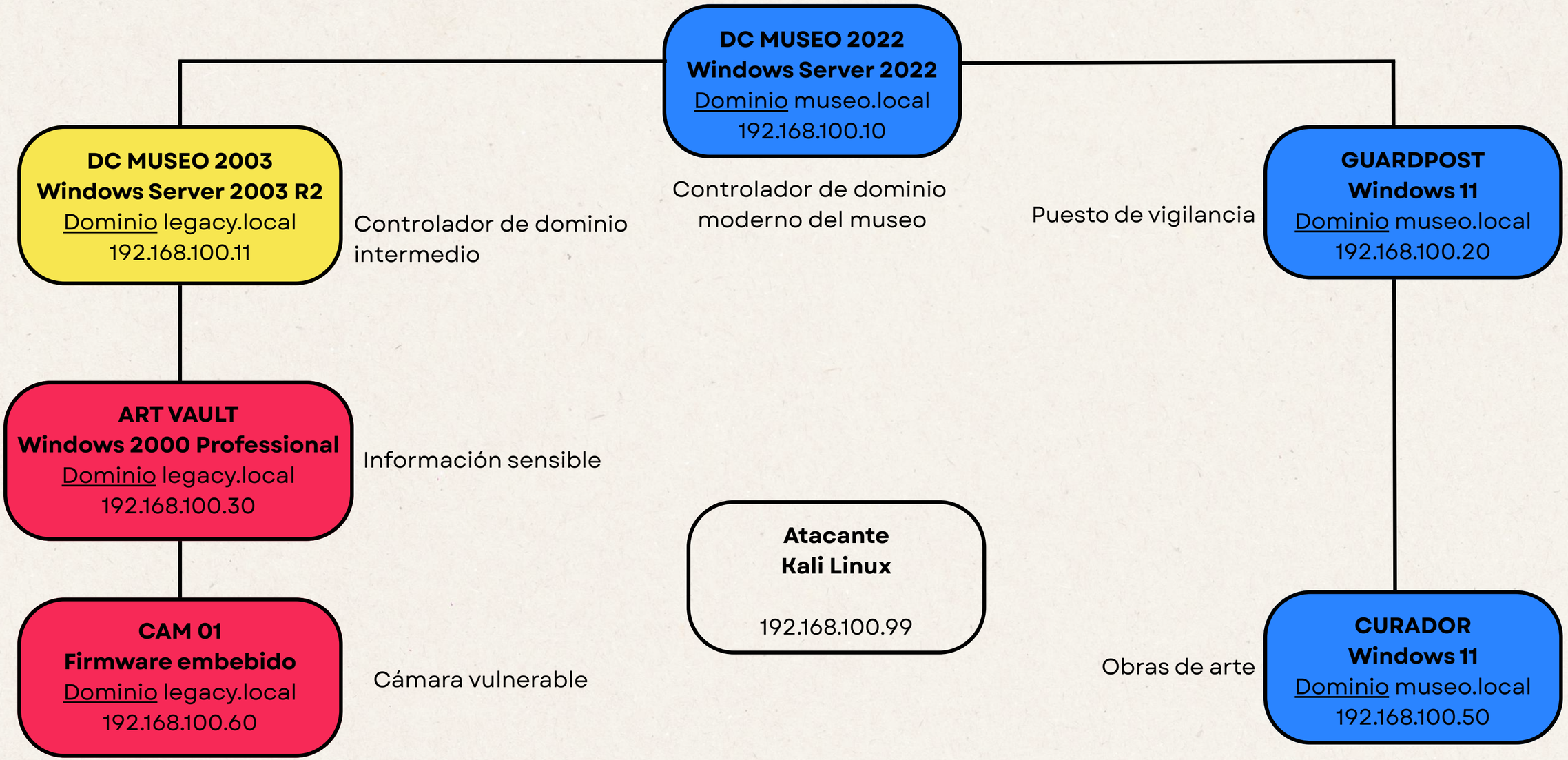
```
┌──(root㉿kali)-[/home/jo]
└─# dirb https://www.louvre.fr -o louvrefr.txt

-----------------
DIRB v2.22
By The Dark Raver
-----------------

OUTPUT_FILE: louvrefr.txt
START_TIME: Tue Dec  9 19:17:58 2025
URL_BASE: https://www.louvre.fr/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
```

Subfinder

```
┌──(root㉿kali)-[/home/jo/Descargas/subfinder]
└─# subfinder -d louvre.fr -o louvre.txt

                __             __
   _____  __  _/ /_  _____  __/ /_  ____
  / ___/ / / / / __ \/ ___/ / __ \/ __ \/ __/
 (__  ) /_/ / / /_/ / /__ / /_/ / /_/ / /
/____/\__,_/_/_.___/\___/ /_/ /_/\__,_/_/

                projectdiscovery.io

[INF] Current subfinder version v2.6.0 (outdated)
[INF] Loading provider config from /root/.config/subfinder/provider-config.yaml
[INF] Enumerating subdomains for louvre.fr
```

El servidor bloquea cualquier petición sospechosa, **no permite enumeración de directorios mediante fuerza bruta** e incluso rutas válidas podrían estar configuradas para devolver 403 si el User-Agent o el patrón de acceso parece automatizado

Esquema laboratorio



Esquema laboratorio

Objetivo: Acceder a la máquina CURADOR partiendo desde CAM 01

1. Explotación inicial: CAM 01
Dispositivo embebido con firmware vulnerable
Posible vector: RCE vía interfaz web o protocolo inseguro
Acceso como usuario limitado

2. Pivoting hacia ART VAULT
Mismo dominio: legacy.local
Enumeración de red interna
Explotación de vulnerabilidad conocida
Acceso como usuario local o SYSTEM

3. Escalada a DC MUSEO 2003
Controlador de dominio legacy.local
Volcado de credenciales
Acceso a hashes de usuarios del dominio

4. Movimiento lateral a GUARDPOST
Enlace entre dominios
Uso de credenciales reutilizadas o Kerberoasting
Enumeración
Acceso como usuario del dominio museo.local

5. Acceso final a CURADOR
Enumeración de servicios expuestos
Uso de credenciales válidas o pass-the-hash
Acceso como usuario CURADOR
Exfiltración de datos y persistencia