

Reto#4

Un cliente cuya red se vio comprometida y desconectada te ha encargado que investigues el incidente y determines la identidad del atacante.

Los servicios de respuesta a incidentes y los investigadores forenses digitales se encuentran actualmente en el lugar y han llevado a cabo una investigación preliminar. Sus hallazgos muestran que el ataque se originó en una única cuenta de usuario, probablemente una persona privilegiada.

Investiga el incidente a partir de las evidencias obtenidas y encuentra al informante:

1. ¿Cuál es la clave API que el *insider* agregó a sus repositorios de GitHub? Fichero de evidencias: Github.txt

Buscando el contenido del primer repo que sale se encuentra lo siguiente

API Key = ajFRaLHijMXvYZgLPwiJkroYLGRkNBW. En el primer repositorio dentro del archivo

<https://github.com/EMarseille99/Project-Build---Custom-Login-Page/blob/master/Login%20Page.js>

2. ¿Cuál es la contraseña en texto plano que el *insider* agregó a sus repositorios de GitHub?

En la misma página que el ejercicio anterior hay un bloque de código con una contraseña en texto plano.

Password: UGljYXNzb0JhZ3VldHRIOTk=

Con [CyberChef](#) se puede descifrar aplicando en este caso Base64:

The screenshot shows the CyberChef interface with the following details:

- Operations:** A sidebar on the left containing various conversion tools like "To Base64", "From Base64", "To Hex", etc.
- Recipe:** Set to "From Base64".
 - Alphabet: "A-Za-z0-9%2B%3D"
 - Remove non-alphabet chars
 - Strict mode
- Input:** The input text is "UGljYXNzb0JhZ3VldHRIOTk=". This text is highlighted in yellow.
- Output:** The output text is "PicassoBaguette99".

3. ¿Qué herramienta de minería de criptomonedas utilizó el informante?

xmrig

The screenshot shows a GitHub repository page for the 'xmrig' project. At the top, there's a navigation bar with tabs for Overview, Repositories (which is the active tab), Projects, Packages, and Stars. Below the navigation bar, it says 'PowerShell' and 'GNU General Public License v3.0'. The date 'Updated on May 17, 2020' is also present. The main content area contains three entries: 'XploitSPY' (Public, Forked from XploitWizer-Community/XploitSPY, XploitSPY is an Android Monitoring Tool), 'xmrig' (Public, Forked from xmrig/xmrig, RandomX, CryptoNight, AstroBWT and Argon2 CPU/GPU miner), and another entry that is partially visible. A red box highlights the 'xmrig' entry.

4. ¿A qué universidad fue el informante?

Sorbonne Université (el perfil de linkedin que aparecía al buscar).

5. ¿En qué sitio web de juegos tenía una cuenta el informante?

En Steam <https://steamcommunity.com/id/emarseille99/>

6. ¿Cuál es el enlace al perfil de Instagram del *insider* ?

<https://www.instagram.com/emarseille99/>

7. ¿Adónde fue el informante durante las vacaciones? (Solo país)

A Singapur. Entrando en el perfil de Instagram

<https://www.instagram.com/emarseille99/> se encuentra una foto de un edificio con una descripción que dice que fue de vacaciones. Se hace un Google Lens de la foto y aparece el edificio en maps y urls de tipo TripAdvisor etc que identifican al edificio como un complejo turístico llamado Marina Bay Sands.

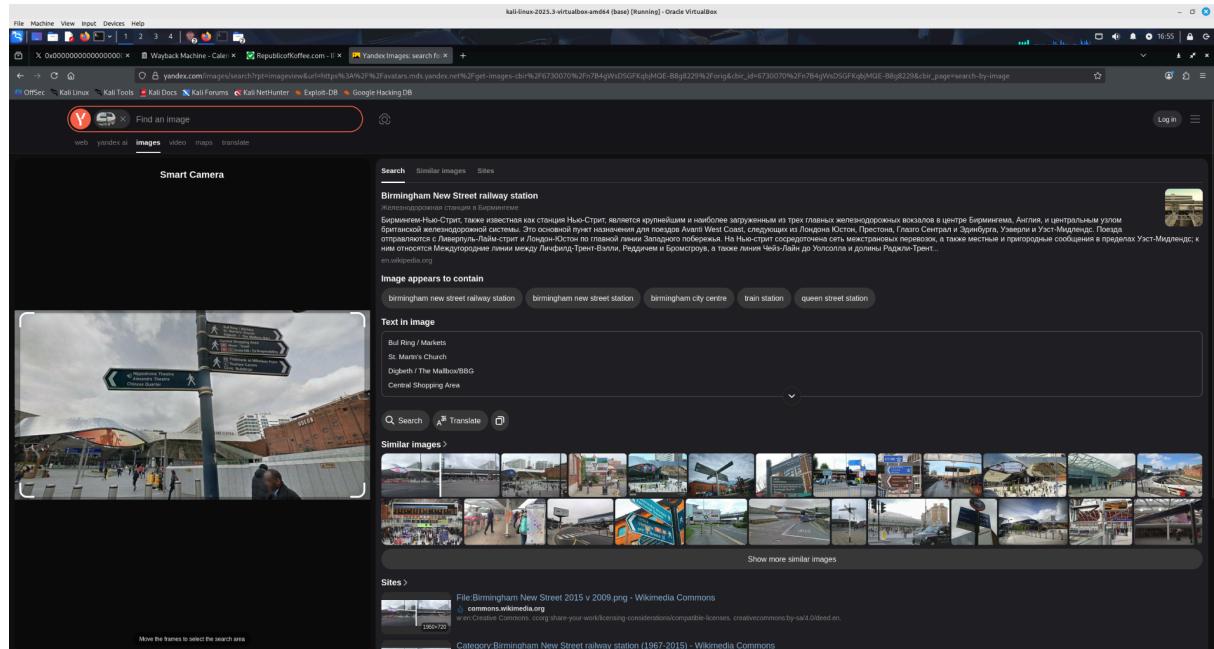
8. ¿Dónde vive la familia del informante? (Solo ciudad)

Haciendo búsquedas con fotos de instagram

<https://www.instagram.com/emarseille99/> en yandex o google lens, identifica directamente la torre Burj Khalifa, ubicada en Dubai, ciudad en la que vive la familia.

9. Se le ha proporcionado una fotografía del edificio en el que la empresa tiene oficinas. ¿En qué ciudad está ubicada la empresa?. Fichero de evidencias: office.jpg

Cargamos la imagen en Yandex y nos da la ciudad exacta en la que se encuentra la empresa: Birmingham.



10. El sospechoso ha abandonado el país pero un equipo de inteligencia cree haber detectado el objetivo con esta cámara IP. ¿En qué estado se encuentra esta cámara?. Fichero de evidencias: Webcam.png

Cargamos la imagen en Yandex y nos da la ubicación exacta en la que se encuentra: el estado de Indiana.

