CYCLOPES JLE Scenario for Vendors: The Black Veil Attack

Table of Contents

Funded by the European Union

CYCLOPES
CYBERCRIME LAW ENFORCEMENT PRACTITIONERS NETWORK

Scenario: An Isolated Cyber Attack?

Approach:

This Joint Live Exercise (JLE) will challenge participants to investigate a ransomware attack against a mid-sized logistics company, initially appearing to be an isolated incident. As teams conduct OSINT, cryptocurrency tracing, and digital forensics, they will uncover unexpected links to previous large-scale ransomware operations. The exercise will emphasise intelligence-sharing, cross-border cybercrime investigations, and assessing criminal adaptation strategies.

Background

A **mid-sized logistics company** in a European recently suffered a ransomware attack. The ransom demand—€150,000 in Monero (XMR).

Initial Investigation Team Tasks (Part 1)

Participants will be split into **three core investigative teams** to examine the logistics company attack and determine its origins.

🔎 OSINT Team:

- Identify any **dark web chatter** referencing the logistics company attack.
- Investigate **potential threat actor aliases and ransomware groups** known to target similar businesses.
- Track **social media or underground forum discussions** about the ransom demand.

💰 Cryptocurrency Tracing Team:

- Map out the **Monero ransom payment flow** and attempt to follow any **conversion points**.
- Identify any **patterns in past ransom transactions** from similar attack methods.
- Determine if any **known cryptocurrency laundering services** have been used.

💻 Digital Forensics Team:

- Analyse the **ransomware sample** to identify its encryption methods and possible weaknesses.
- Examine system **logs and artefacts** to determine the attack vector and how the breach occurred.
- Investigate **seized devices or forensic images** to assess the attacker's tactics and techniques.

Funded by the European Union

A Multi-Jurisdictional Ransomware Investigation (Part 2)

Background

In recent years, **three European countries** have suffered chaos in the form of Ransomware attacks. Critical IT systems have been **locked down**, with ransom notes flashing across screens, and key files **encrypted**. Among the affected organisations:

- A **regional healthcare authority** in Germany, halted access to digital patient records.
- A **municipal transport network** in France, disrupted ticketing systems and city-wide operations.
- A **government data centre** in Spain, shutting down critical public services, including tax administration and civil records.

All victims received the same **ransom demand**—€5 million in **Monero (XMR)**, with a strict **72-hour deadline** before stolen data was released.

Due to the significant disruption, each incident was considered a national priority, with the return of service being the number one priority.

The Attacker: Black Veil

Intelligence suggested the attacks as the work of **Black Veil**, a well-organised **ransomware-as-a-service (RaaS) syndicate** operating out of Eastern Europe. Known for **double extortion tactics**, Black Veil encrypts victim data while **stealing** sensitive information, threatening to leak it on their **dark web leak site** if demands are not met.

Key details from past attacks suggest:

- **Initial Access**: Exploitation of **compromised VPN credentials** and **phishing emails** targeting senior IT staff.
- **Ransomware Deployment**: Executed remotely using **previously compromised admin accounts**, requiring **no direct malware analysis** in this exercise.
- **Cryptocurrency Flow**: Payments funnelled through **privacy wallets and mixing services** before reaching offshore exchanges.
- **Communication Channels**: Black Veil operates via **Telegram**, underground forums, and their **Tor-hosted ransom portal**.

Funded by the European Union