Day 3: OSINT Investigation Using WHOIS Lookup

Introduction

On Day 3, I learned how to investigate a suspicious website using a technical and legal method instead of guessing. The case involved a fake crypto investment website that was promising very high returns in a short time. Such promises are usually a sign of online scams. To verify whether the website was real or fake, I used a WHOIS lookup. This helped me understand how cybersecurity professionals start investigations using open-source information.

Fake Crypto Investment Website

A fake crypto investment website is a fraudulent website created to trick people into investing money. These websites often promise guaranteed profits or extremely high returns, which is not realistic in real financial markets. They usually look professional and attractive to gain the trust of users. Many people lose money because they believe these false promises without verifying the website.

why the website was Suspicious

The website raised suspicion because it promised unrealistic returns with no risk. It did not provide clear information about the company, such as registration details or physical address. There was also pressure to invest quickly, which is a common trick used by scammers. These warning signs made it necessary to investigate the website technically instead of trusting it blindly.

what is WHOIS?

WHOIS is a public database that stores information about domain names. It tells us who registered a domain, when it was registered, and when it will expire. WHOIS is completely legal and is widely used by cybersecurity experts, ethical hackers, and investigators. It is often the first step in website investigation and OSINT analysis.

Why WHOIS is Used in Cybersecurity

WHOIS helps convert an unknown website into traceable technical information. By using WHOIS, investigators can find out whether a website is newly created or long-standing. Many scam websites use new domains that exist only for a short period. This makes WHOIS a powerful tool for identifying suspicious online platforms.

Domain Registrar

A domain registrar is the company where a domain name is registered. WHOIS reveals the name of the registrar used by the website owner. Some scammers repeatedly use the same registrars to create fake websites. Identifying the registrar helps investigators find patterns across multiple scam websites.

Hosting Provider

The hosting provider is the service that stores the website files and makes the website accessible on the internet. WHOIS can help identify the hosting provider associated with a domain. Many fake websites are hosted on low-cost or poorly regulated hosting services. Knowing the hosting provider helps in reporting the website for abuse.

Domain Registration and Expiry Dates

WHOIS shows the date when the domain was registered and when it will expire. Fake websites are often registered very recently and for a short duration, such as one year. This indicates that the website may be temporary and created only for scamming purposes. These dates help investigators understand the timeline of the website.

Registrant Contact Details

Registrant details include the name, email address, or organization used to register the domain. Sometimes these details are real, but often scammers hide them using privacy protection services. Even hidden or fake details can be useful because the same information may appear across multiple scam domains. This helps in linking different websites together.

WHOIS as a Starting Point for OSINT

OSINT stands for Open-Source Intelligence, which means collecting information from publicly available sources. WHOIS is one of the most important OSINT tools in cybersecurity investigations. It provides initial technical data that can be combined with other OSINT techniques. WHOIS helps investigators move from a suspicious website to deeper analysis.

Identifying Scam Networks

Scam networks are groups of fake websites controlled by the same attackers. By comparing WHOIS data of different domains, investigators can identify common patterns such as same registrar, hosting provider, or registrant details. This helps expose not just one fake website, but an entire scam operation.

Linking Multiple Fake Websites

WHOIS allows investigators to link multiple fake websites together using shared technical details. For example, if several websites use the same registrar or contact email, they may belong to the same scammer. Linking websites strengthens the investigation and provides better evidence of organized cybercrime.

Evidence Collection and Preservation

WHOIS information can be saved as screenshots or reports and used as digital evidence. This evidence is useful for cybercrime complaints, academic research, or legal investigations. Preserving WHOIS data is important because scammers often delete or change websites quickly to avoid detection.