Use case - Compromised websites distributing child abuse material

One line summary:

Find information on the registrar of compromised websites distributing child abuse material (CAM).

Primary actor: Law enforcement.

Other stakeholders: Registrars, hosting providers.

Data elements: Domain names, DNS data (IP address of the website hosting CAM), WHOIS data (email address of the domain name's administrative contact) .

Story:

A number of websites on the clear web, controlled by organised crime groups, distribute child abuse material. For a monthly fee of approximately 99$/month, clients can have unlimited access to child abuse material. They can also pay per download.

Investigators gathered the **domain names** linked to those websites using open source monitoring or on the basis of contribution from law enforcement partners or NGOs.

They then gathered the **DNS information** linked to those domain names (the IP associated to the domain names) using Python DNS scripts or domain tools API. They also gathered the **WHOIS data** associated to those identified domains.

They then cross-match the three data sets to identify any commonalities between the sets.

Most of the time, on the basis of domain names and DNS information there is no connection between the domains: Domain A will have specific DNS information which will indicate that this Domain A is registered to IP A. Domain B has DNS information indicating that Domain B is registered to IP B. Etc. **BUT**, when cross-matched against **WHOIS data**, investigators can identify one valid email address that is used by the registrant to register all the different domains.

In that specific case they could identify a **valid email address** that linked the three sets of information. This email address was used by the registrants to register the different domains. The registrants needed to provide at least one valid email address to communicate with the registrar for billing purposes.

Unfortunately, the websites are hosted in an uncooperative jurisdiction so the websites are still up but the investigations in the criminal groups continue.

Privacy implication:

WHY would registrants use the same email address to register different domains?

- Laziness: registrant can't be bothered to create 10 different email addresses to register 10 different domains.
- Can't they use **privacy and proxies** to hide their credential? YES but since most of the time the server are hosted in a jurisdiction that does not cooperate and privacy and proxies services means additional costs – they don't care.

Main take-away:

This case shows that when WHOIS data is accurate (email address), not only investigators save precious time and resources but, cross-checked against other data sets, it is a useful tool for crime attribution.