Find Domains Registered by Miscreant Use Case

Domain Registration Data - Use Case Exposition

LE/Anti-abuse

Find malicious domains created by a particular miscreant

Goal/Scenario

Miscreants will often register multiple domain names, both concurrently and over time. LE/Ops-Sec personnel (investigators) typically desire to find all domains registered for a "campaign" or over time by a miscreant, based on determining one or more initial domains are malicious. Investigators will then take further actions based on their findings.

NOTE: This is a use-case based on current practices that doesn't typically involve today's whois system directly, but are performed using universal whois databases collected by outside organizations, including "whowas" type services.

NOTE 2: This use case is very similar to the open-source research use case.

Brief Format Use Case

Use Case: Find malicious domains created by a particular miscreant

Main Use Case: LE/Ops-Sec type person (investigator) accesses the RDS via their credentials. The investigator enters one or more domain names or particular details tied to domain names registered by a particular miscreant to determine if there are other domain names potentially related to the same miscreant. The system returns list of domain names and potentially other information the investigator is entitled to given their credentials. The investigator may iterate on this case many times based on the information various searches reveal.

Casual Format Use Case

Title: Find malicious domains created by a particular miscreant

Primary Actor: LE/Ops-Sec person investigating a potential miscreant and their involvement with the domain name system.

Other stakeholders: Operator of the RDS

Scope: Interacting with Domain Name Directory Service

Level: User Task

Data Elements:
Nameservers assigned to the domain names identified
e-mail addresses used to control the domain(s)

registrar(s)/reseller(s) of domain names identified
contact info used by the miscreant
- Name/Org Name
- e-mail address
- phone
- physical address

Story: LE/Ops-Sec person investigating (investigator) a potential miscreant desires to find domain names tied to that actor.

The system should be accessible via a website or some other electronic processing means.

Investigator provides access credentials and the system authenticates them and their access privileges.

The investigator enters domain names and/or data related to domain names that are under investigation and requests any domain names or other information tied to that input via a search capability.

The system returns domain names and other information the investigator is entitled to given their credentials. Information that would likely be stored by the RDS that could be useful in an investigation includes lists of related domains along with the full contact information (proxy and non-proxy) for the listed registrant, the e-mail addresses used to control the domain name, nameservers utilized by the domain name, and the relevant registrar (and reseller) of the domain name.

The investigator will examine the returned information, potentially move their investigation forward, and/or may request further information about the domain names revealed. It is likely that the investigator will iterate over this use case several times, and put the RDS to other use cases as a result of information obtained.

The investigator will then use the information provided to further their investigation, tying that information into other clues and information in their case.