Investigate Abusive Domain Use Case

Domain Registration Data - Use Case Exposition

LE/Anti-abuse

Find owner of abusive domain - potential miscreant

Goal/Scenario

LE/Ops-Sec personnel investigating a maliciously registered domain name desire to find identity of person who registered name. It is unlikely that miscreants will put their own information into a registration record, but telltales may be found in resources used to register the domain. Information that could be useful in an investigation includes the IP address used to perform the registration, any credentials used (access or financial), e-mail addresses used to control the domain, nameservers utilized by the domain name, or standard personas used by the miscreant. With that information, the LE/Ops-Sec person can take further steps to track down the person responsible for creating the abusive domain name.

Brief Format Use Case

Use Case: Find owner/information about owner of abusive domain - potential miscreant

Main Use Case: LE/Ops-Sec type person (investigator) accesses the RDS via their credentials. The investigator enters a domain under investigation domain name and requests full details on the registrant and any captured domain registration data from the system. The system returns contact information and other information the investigator is entitled to given their credentials. The system may return pointers to a registry/reseller/reseller contacts (TBD) for the domain who may have more information related to the registration of the domain. If technical contact details are being tracked for the domain name (e.g. DNS, web hosting, e-mail, etc.) in the RDS, then the system may return pointers to those contacts as well.

Casual Format Use Case

Title: Find owner/information about owner of abusive domain - potential miscreant

Primary Actor: LE/Ops-Sec person investigating a maliciously registered domain name.

Other stakeholders: Operator of the RDS, registry operator for the TLD of the domain name, registrar of the domain name, reseller of the domain name, registrant of the domain name, providers for Internet services (web/e-mail/messaging/etc.) for the domain name.

Investigate Abusive Domain Use Case

Scope: Interacting with Domain Name Directory Service, Interacting with the registry/registrar/reseller of the domain name that is being investigated, interacting with service providers for the domain name.

Level: User Task

Data Elements:
Timestamp of the domain registration activity
Nameservers assigned to the domain name
IP address used to perform the registration
Credentials used (access or financial) to perform the registration
e-mail addresses used to control the domain
standard personas used by the miscreant
- Name
- e-mail address
- phone
- physical address

Story: LE/Ops-Sec person investigating a maliciously registered domain name (investigator) desires to find identity of person who registered a domain name.

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 a domain name under investigation and requests full details on the registrant and any captured domain registration data from the system.

The system returns contact information 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 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 technical provisioning of the domain name. If technical contact details are being tracked for the domain name (e.g. DNS, web hosting, e-mail, etc.) in the RDS, then the system may return pointers to those contacts as well.

The investigator will then use the information provided to further their investigation, tying that information into other clues and information in their case. The investigator may use the contact information they have obtained from the RDS to reach out to various providers to obtain further investigatory

information. Such information would include data stored by those various stakeholders that is not present in the RDS. For example, this may include information about account access, payment information, and other data logged by the entities that the potential miscreant interfaced with.