Criminal Investigation or DNS Abuse Mitigation

GNSO RDS PDP – Drafting Team 7

ICANN60 | November 1, 2017

Definition

The broad category of criminal investigation or DNS abuse mitigation covers all use of an RDS to support criminal and other investigations, abuse prevention, security incident response, and other activities to protect people, systems, and networks from detrimental activities.

These activities range from criminal activities like extortion, phishing, and provision of child abuse materials to abusive activities including denial-of-service attacks, spam, and harassment.

Users

- Law enforcement
- Cybersecurity professionals
- IT administrators
- Automated protection systems
- Other actors pursuing abuse issues

Tasks

- Depend upon the circumstances!
- Contact domain owners and/or the entities that provide services for an affected domain to
  - Mitigate problems
  - Gather evidence
  - Notify them of compromises
- Expand investigations and associations to fully understand the scope of an abuse issue
- Identify Internet infrastructure involved with detrimental activities
- Inform protection systems to take protective actions
- Request suspension of domain names

Categories of Actors

- Individuals or small teams making ad-hoc data requests for single or small sets of domains
- Automated processes that may query for information about thousands to millions of domains

Categories of Actions

- Determination of domain compromise vs. exclusive control
- Notification of appropriate parties to security and abuse issues
- Understanding scale and scope of incidents and campaigns

Other RDS Touchpoints in the Category

- Indirect involvement of a domain name in some other criminal and/or abuse case
- Infrastructure affected by but not involved in an incident

Sample use Cases – Individual Investigations

- Manual determination of domain status (malicious/compromised)
- Notify parties responsible for a domain name that has had its website compromised
- Notify parties responsible for a domain name that has had its management account compromised
- Notify registrar of malicious domain name registration for mitigation and/or evidence gathering
- Expand knowledge from malicious domain to other domains involved in incident

Sample use Cases – Automated Processes

- Automatically determine if a domain used for an attack is registered maliciously
- Automatically create reputation score for domain names
- Automated notifications of abuse
- Automatically expand knowledge from one or more known malicious domains to other domains potentially part of the same issue

Sample use Case – Domain Related to Other

- Determine domain ownership or involvement with operating a domain name tied to real-world criminal/abuse activities