RDS Purpose: Criminal Activity or DNS Abuse Mitigation
DT7 Answers to Questions – First Draft for DT Review

Criminal Activity/ DNS Abuse Mitigation

Definition: The broad category of criminal activity 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.

Criminal Activity/DNS Abuse Mitigation – Investigation

From https://community.icann.org/download/attachments/74580010/DraftingTeam7-CrimInvAbuseMit-10%20Nov%202017%20clean.pdf?version=1&modificationDate=1510442602000&api=v2

> Purpose Summary: The following information is to be made available to regulatory authorities, law enforcement, cybersecurity professionals, IT administrators, automated protection systems and other incident responders for the purpose of enabling identification of the nature of the registration and operation of a domain name linked to abuse and/or criminal activities to facilitate the eventual mitigation and resolution of the abuse identified: Domain metadata (registrar, registration date, nameservers, etc.), Registrant contact information, Registrar contact Information, DNS contact, etc..

1. ***Who associated with the domain name registration needs to be identified and/or contacted for investigation of Criminal Activity/DNS Abuse?***

During investigation of Criminal Activity/DNS Abuse, users of registration data, such as regulatory authorities, law enforcement, cybersecurity professionals, IT administrators, automated protection systems and other incident responders, may wish to identify the entity or individual who is in control of the domain name registration or who can provide information that would lead to the identification of the entity or individual who is controlling the domain name registration. Generally, this use case isn't for contact but is focused instead on identification. Accurate RDS data is important and can be critical in determining if the registrant is a victim of abuse or the abuser. While accurate data is preferred even bad data can be useful in identifying trends, showing patterns or association with known bad actors.

2. ***What is the objective achieved by identifying and/or contacting each of those entities?***

Identification of the entity responsible for criminal activity could lead to prosecution. The RDS data may be used in conjunction with other data points to build a case. As previously noted even bad data can be useful and may help demonstrate patterns or trends of abuse.

The objectives are:

1) Prevention of criminal activity and DNS abuse
2) Mitigation of impacts from criminal activity and DNS abuse
3) When it does occur providing data points to help build a case for prosecution of those responsible for the criminal activity

This use case generally uses the RDS data for identification but not for contact. In cases where a reseller or privacy/proxy service is used however, then contact with the objective of identifying domain owner (for purposes specified above) applies.

3. What might be expected of that entity with regard to the domain name?

If the entity or individual who is in control of the domain name registration cannot be identified, the party with access to that information (e.g. the privacy/proxy service or registrar) is expected to provide information concerning the entity or individual who is in control of the domain name registration so that the investigation can establish what role the entity or individual played in the DNS abuse and further abuse can be mitigated.

If the entity can be identified, it is expected that the entity will either want to be notified of and mitigate any associated crime/abuse, or the entity is the abuser and subject to further investigation.

RDS Purpose: Criminal Activity or DNS Abuse Mitigation
DT7 Answers to Questions – First Draft for DT Review

Criminal Activity/DNS Abuse Mitigation – Notification

From https://community.icann.org/download/attachments/74580010/DraftingTeam7-CrimInvAbuseMit-10%20Nov%202017%20clean.pdf?version=1&modificationDate=1510442602000&api=v2

> Purpose Summary: The following information is collected and made available for the purpose of enabling notification by regulatory authorities, law enforcement, cybersecurity professionals, IT administrators, automated protection systems and other incident responders of the appropriate party (registrant, providers of associated services, registrar, etc), of abuse linked to a certain domain name registration to facilitate the mitigation and resolution of the abuse identified: Registrant contact information, Registrar contact Information, DNS contact, etc..

1. ***Who associated with the domain name registration needs to be identified and/or contacted for Notification of Criminal Activity/DNS Abuse?***

During Notification of Criminal Activity/DNS Abuse, users of registration data, such as regulatory authorities, law enforcement, cybersecurity professionals, IT administrators, automated protection systems and other incident responders, may need to contact the entity or individual who is in control of the domain name registration or who can provide information that would lead to notification of the entity or individual who is controlling the domain name registration. This entity could be the domain name registration holder (the Registrant), the privacy/proxy service and/or the registrar. This is often an entity being harmed by Criminal Activity or DNS Abuse associated with a domain name – for example, when a domain name has been hijacked or compromised. The who may be another entity associated with the domain name registration (e.g., registrar, proxy) that can help notify the harmed entity. The who in this use case is often the victim of criminal activity or DNS abuse and needs to be someone authoritative for the domain who if necessary can take corrective action to mitigate or stop the abusive activity.

2. ***What is the objective achieved by identifying and/or contacting each of those entities?***

In some cases, the victim may not be aware of any issues, so the primary objective is notification of the problem. The secondary objective is that by notifying the appropriate party of an issue it can be corrected or otherwise mitigated. Enabling notification of the appropriate party (registrant, providers of associated services, registrar, etc), of crime or DNS abuse linked to a certain domain name registration is intended to facilitate the mitigation and resolution of the crime/abuse identified. Mitigation of criminal activity or DNS abuse associated with domain names is essential to promote the security and stability of the Internet, and thus of potential benefit to both victims of crime/abuse and indirectly to all Internet users.

3. ***What might be expected of that entity with regard to the domain name?***

Following notification, the entity in control of the domain name registration is expected to mitigate and resolve the abuse identified. In some instances, action might be expected of an entity other than the owner of the domain name registration. For example, when notified of certain types of abuse, a registrar might be expected to take down a domain name registration or otherwise prevent it from resolving.

RDS Purpose: Criminal Activity or DNS Abuse Mitigation
DT7 Answers to Questions – First Draft for DT Review

Criminal Activity/DNS Abuse – Reputation

From https://community.icann.org/download/attachments/74580010/DraftingTeam7-CrimInvAbuseMit-10%20Nov%202017%20clean.pdf?version=1&modificationDate=1510442602000&api=v2

> Purpose Summary: The following information is to be made available to organizations running automated protection systems for the purpose of enabling the establishment of reputation for a domain name to facilitate the provision of services and acceptance of communications from the domain name examined: Domain metadata (registrar, registration date, nameservers, etc.), Registrant contact information, Registrar contact Information, DNS contact, etc..

1. ***Who associated with the domain name registration needs to be identified and/or contacted for Reputation Analysis associated with Criminal Activity/DNS Abuse Mitigation?***

During reputation analysis to mitigate Criminal Activity/DNS Abuse, various data points are used to determine a reputation score. Who is but one of the elements that may be used by the scoring algorithm. Data needed will typically be those attributes that tend to cluster for abusive domain names including nameservers, registrar, creation date, registrant contact info (particularly e-mail, phone, and name), other contact information.

2. ***What is the objective achieved by identifying and/or contacting each of those entities?***

Enabling the establishment of reputation for a domain name to facilitate the provision of services and acceptance of communications from the domain name examined.

A company might make use of a reputation service to determine whether to allow traffic to a site. The objective here would be to protect users of the reputation service from Criminal Activity / DNS Abuse.

3. ***What might be expected of that entity with regard to the domain name?***

No contact would be expected for this use case; however, a domain name owner might be expected to provide accurate and up to date information if he/she is motivated to obtain a higher reputation score.