Framework for Registry Operator to Respond to Security Threats

Objective

The objective of this framework is to deliver on the New gTLD Program Committee of the ICANN board's (NGPC) commitment to the GAC regarding ICANN soliciting community participation to develop a framework for how a Registry Operator (RO) may respond to identified security threats. This framework is a voluntary and non-binding document designed to articulate the ways registries may respond to identified security threats.

This framework does not address situations where a registry operator does not have discretion to respond (such as subject to a Court Order from a court of competent jurisdiction over the Registry)." It does not reflect any consensus policy affecting registries.

Scope

This framework addresses Registries' responses to notifications of security threats.

Categories of Action by Registries in Response to Security Threats

The Registry Operator's generic Top-Level Domain (gTLD) policies or Terms of Service typically govern the types of responses available to the Registry Operator. These policies are developed based on applicable legal, operational and technical requirements, which vary across registries and jurisdictions. Policies may be amended at the discretion of the RO and in line with consensus policies and legal requirements, to address new circumstances and lessons learnt from previous security threats.[1]

1 This Framework does not cover the duty of Registry Operators to periodically conduct a technical analysis to assess whether domains in its gTLD are being used to perpetrate security threats, such as pharming, phishing, malware, and botnets, nor does it cover the requirement for Registry Operators to maintain statistical reports on the number of security threats identified and the actions taken as a result of the periodic security checks. As a consequence, the framework does not cover the response to any security threat that may be discovered by the Registry Operator itself in the process of the required periodic technical analysis. Registry Operators may however choose to apply the same framework to their response to those security threats.

This list, whilst not comprehensive, represents many of an RO's potential abuse response options.

Existing domain names

- Refer the issue to the Registrar.

Referral is often the first response employed by a RO because it is the Registrar that has the contractual relationship with the Registrant of the domain name. The Registrar should be given a time-bound opportunity to investigate the security threat and respond appropriately. A negative or non-existent response from the Registrar should not preclude the Registry from taking action.

- Hold the domain name so it does not resolve.

Applying *serverHold* status removes the domain name from the TLD zone file, with the consequence that the domain name will no longer resolve on the public Internet.[2] .An additional benefit is that this action is easy to reverse in case of mistake.

- Lock the domain name so it cannot be changed.

Although rarely used for security threats, applying lock status[3] means that a domain cannot be transferred, deleted or have its details modified, but will still resolve. It is occasionally seen as part of an action where a domain is locked in conjunction with the seizure of its name servers.

- Redirect name services for the domain name.

A Registry has the technical ability to change a domain name's nameservers. By changing the nameservers for the domain name, services associated with the domain name can be redirected for "sink-holing" (logging traffic) to identify victims for the purposes of remediation.

- Transfer the domain name.

The transfer of a domain to a suitably-qualified Registrar may prevent exploitation, whilst allowing for management of lifecycle, EPP status codes, and expiration.

- Delete the domain name.

Deletion is an extreme action and not generally recommended without careful due diligence and direction from the appropriate authorities. Restoring a domain name, if the deletion is found to be inappropriate, may involve additional burdens that are not manifest when placing a domain name on *serverHold*. Deletion is generally not as effective at mitigating security threats as suspension, as a registrant is free to re-register the domain name after it is purged from the zone.

2 Commonly known as "suspension", the effect will be to stop relevant DNS services which are under control of the RO – without seizure of the domain.

3 Registry 'lock' status is in fact a combination of these three EPP status codes: *serverTransferProhibited, serverDeleteProhibited,* and *serverUpdateProhibited*.

- Take no action.

This option is always available. Registry policy may limit action under specific circumstances or it may be the default action if no other response is appropriate. Similarly, a RO may reach the conclusion that a referred matter does not constitute a security threat or that the consequences of action outweigh the threat itself. As a matter of courtesy, the RO should respond to the originator of a security threat indicating why this is the response to the reported security threat.

Unregistered (DGA-type) domain names

A security threat may be associated with a domain name that is not yet registered. This can happen when the domain name is the result of an automatic Domain Generation Algorithm (DGA) associated with botnet activity. Often the threat will involve thousands or more domain names.

- Create the domain name.

Registering a potentially malicious domain name seems counterintuitive; but when done in controlled conditions, it enables researchers and public safety organizations such as CERTs to take appropriate action (such as sinkholing) on a domain name. Similarly, to the *transfer* option above, this helps identify victim computers for mitigation purposes. Additionally, use of the domain name is denied to bad actors as with the *block* option below.[4]

The RO generally has discretion as to whether it delegates previously unregistered domains to a suitably-qualified registrar, or its own internal registrar. ROs should be sure that they seek any appropriate or necessary waiver(s) from ICANN with regards to certain contractual provisions of the RO's respective Registry Agreement. This is currently achieved through ICANN's Expedited Registry Security Request (ERSR) process. The timing of the receipt of the waiver is dependent upon ICANN.

- Block registration of the domain name.

Where agreed, the RO may reserve the requested domain name. Requestor should work with the RO to establish an appropriate time limit for the block, if any.

4 Logged data may contain Personally Identifiable Information (PII). Any action should be carried out in line with the appropriate requirements of the RO's jurisdiction.

Reporting security threats

Whilst assessing source credibility is a matter for the individual RO, there exists a hierarchy of the severity of security threats. An RO must also pay attention to the quality and standard of the information provided in a source's report, together with previous reports. A straightforward example of where priority should be given and actions taken more quickly, subject to the RO's policies and determinations, are for those reports properly made by relevant national law enforcement authorities (LEAs) where the RO is located, or where a request is grounded by court order from a court with jurisdiction over the RO.

A) Reports from Law Enforcement Authorities

Where the notifying party is confirmed as a government Law Enforcement Authority (including national law enforcement or other government public safety agency of suitable jurisdiction over the RO) this framework encourages ROs to consider such reports to be of a higher fidelity, and as such are afforded with all due priority. While ROs should proceed with a higher degree of certainty with respect to referrals from LEAs, they should still conduct any investigation they deem necessary to ensure that the referrals properly constitute a security threat and to confirm the validity of the referral source.

B) Reports from RO Recognized Sources

At its own discretion, an RO may choose to prioritize reports from entities that it recognizes as having the requisite expertise in the appropriate field, such as national CERTs and security reporting organizations.

C) Reports from other sources

ROs are encouraged to adequately address reports of technical abuse of the DNS from public sources, as appropriate. ROs are further encouraged to ensure that appropriate procedures are put in place, so that proper attention may be given to any verified threat. This includes reports and requests from users, members of the public, or those identified via the RO's own choice of technical analysis. For the absence of doubt, any reports received from anonymous sources should never be discounted solely due to the fact that the report was made anonymously. ROs should undertake to review all reports, made in good faith, whether anonymously made or not, based on the merits and evidence presented.

Registry Response

For clarity, 'response' in the following context is taken to mean the action, or actions, following receipt of a report about a security threat specifically identified by the RO as posing an actual risk of harm in accordance with the RO's policies, including, but not limited to, a response to the reporting Public Safety Authority that reported the security threat is under investigation by the RO.

Upon receipt of the referral, ROs are encouraged to provide a prompt, initial affirmative receipt response, indicating that the request is being considered. Within 24 hours after acknowledging initial receipt, the RO should make reasonable efforts to respond with its assessment of the request and, where possible and appropriate, its chosen course of action, based on that assessment. If possible, the inclusion of a potential timeline for action would be beneficial in managing expectations on both sides.

ROs can assess the request, in accordance with their policies, and their subsequent response based on the following factors:

1. Level of Priority

Initial judgment of a request being "High Priority" should be self-evident and require no unique skills in order to determine a public safety nexus. "High Priority" should be considered an imminent threat to human life, critical infrastructure or child exploitation. A significant threat of disruption to the DNS may also be considered as a "High Priority" issue. Registries should use their own internal policies to make these determinations. Any other incident not categorized as "High Priority", related to technical abuse of the DNS, will be handled according to the Anti-Abuse policy of the registry when they have the appropriate legal discretion.

2. Origin of Report

Each RO should scrutinize, question or otherwise inquire about the legitimacy of the origin of a request, in accordance with their own internal policies and processes.

3. Content

The content of each request should be reviewed in full as it may contain verifying information, or come with specific requests for the RO. Priority reports should be substantiated with information demonstrating a self-evident potential for harm to human life, critical infrastructure or child exploitation. Such content, including any such RO specific requests, should be assessed based on the internal policies of each respective RO and, where appropriate to do so, identify any remediating steps.

4. Responsible Parties

ROs are not necessarily the best parties to address certain security threats. The identification of the parties considered as being most relevant and appropriate in resolving the security threat is critical to the prompt resolution of the matter. For example, in the case of abusive registrations, the registrar or reseller is best placed to review and address registration issues. Whereas, in the case of compromised systems, the registrant or their hosting provider maintain administrative access to affected systems and are best able to address issues; however, the Registry operator may be the best party to address large-scale threats that span many registrants or registrars.

If and when requests are categorized as “High Priority” and of a legitimate and credible origin, then as soon as possible and no later than 24 hours of acknowledging receipt, the Registry Operator can acknowledge the threat and communicate its planned steps to mitigate the security threat. When incidents are not “High Priority,” the ROs are encouraged to respond within 24 hours with details of what they will be doing moving forward, to include that they may be doing nothing. It is encouraged that ROs communicate the analysis of the threat to the requestor in order to clarify why they may or may not be taking further action or that mitigation should be handled through a different party.

ROs are encouraged to engage with one or more competent law enforcement agencies in their jurisdiction (e.g. national high-tech crime unit) or suitable public safety agencies that may:

- help assess reports about security threats,
- help with identification and verification of applicable Law Enforcement and public safety agencies.
- serve as facilitators between ROs and investigating law enforcement officers.

ROs are encouraged to share information of abused domain names with other ROs and competent law enforcement agencies when appropriate to prevent DNS abuse.

5. Respecting Privacy & Confidentiality

The reporting and resolution of an identified security threat will ordinarily involve the processing of personally identifiable information (PII) by the RO, Law Enforcement, or a competent and relevant authority. When responding to an identified security threat, ROs should be mindful of their respective privacy policies, accepted best practices with regards to confidentiality, data security, data transfer, and data retention, as well as any local laws, contractual requirements, or otherwise binding requirements.

Future iterations and updates to this framework may occur as appropriate, pursuant to ICANN process.