Framework for Registry Operators to Respond to Security Threats

20 September 2016

Contents

1 Introduction

Background

The Governmental Advisory Committee (GAC) Beijing Communique contained GAC Advice to the ICANN Board, notes that a number of safeguards should be applicable to all new gTLDs and that such safeguards should be subject to contractual oversight[1]. Among these safeguards, the GAC advised that new gTLD Registry Operators be required to periodically conduct a technical analysis to assess whether domains in their respective gTLDs are being used to perpetrate security threats such as pharming, phishing, malware, and botnets and, where the Registry Operator identifies security risks that pose an actual risk of harm, notify the relevant Registrar and where appropriate, suspend the domain. [2].

The GAC Advice set forth in the Beijing Communique led ICANN's New gTLD Program Committee (NGPC) to propose additional language to the baseline new gTLD Registry Agreement: Specification 11, the Public Interest Commitments, applicable to all new gTLD Registry Operators.[3] To address the GAC Advice regarding the technical analysis for security threats, Specification 11 included new language encapsulating requirements that Registry Operators:

- Periodically conduct a technical analysis to assess whether domains in the TLD are being used to perpetrate security threats;
- Maintain statistical reports on the number of security threats identified and the actions taken as a result of the periodic security checks; and
- Provide these reports to ICANN upon request.[4]

Notably, the language did not introduce any requirements for *how* Registry Operators ought to respond to identified security threats. Within the same resolution, the NGPC generally called on ICANN to "*solicit*

[1] What constitutes GAC Advice: https://newgtlds.icann.org/en/applicants/gac-advice#what
[2] See GAC Beijing Communique, https://www.icann.org/en/system/files/correspondence/gac-to-board-11apr13-en.pdf
[3] See NGPC Resolution 2013.06.25.NG02 – 2013.06.25.NG03, https://www.icann.org/resources/board-material/resolutions-new-gtld-2013-06-25-en#2.b
See NGPC Resolution 2014.06.06.NG02, https://www.icann.org/en/system/files/files/resolutions-new-gtld-annex-2-06jun14-en.pdf
[4] See ICANN Base New gTLD Registry Agreement, http://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-09jan14-en.pdf

community participation… to develop a framework for Registry Operators to respond to identified security risks that pose an actual risk of harm."

Objective

The objective of this framework is to deliver on the NGPC's commitment to the GAC regarding ICANN soliciting community participation to develop a framework for Registry Operators to respond to identified security threats. This framework serves as the product of ICANN's efforts to solicit community participation in this regard.

Furthermore, this framework is intended to provide the wider community with an understanding of the Registry Operator's role in the Domain Name System (DNS) ecosystem including the parameters and constraints at play. This understanding will inform and enrich subsequent discussions regarding the types of responses to identified security threats considered appropriate for Registry Operators.

Finally, this framework is intended to assist New gTLD Registry Operators with navigating the complexities inherent in mitigating security threats by serving as, just one of many, educational tools.

Scope

In order to facilitate a well-informed discussion regarding the types of responses to identified security threats considered appropriate for Registry Operators, the framework contains an overview of the Registry Operator's role in the Domain Name System (DNS) ecosystem and the typical phases of action in relation to security threats.

The body of the framework encompasses non-binding mitigation principles and accompanying rationale that may be employed by Registry Operators in determining how to respond to security threats, identified pursuant to a technical analysis conducted by the Registry Operator, that pose an actual risk of harm. Principles and accompanying rationale are discussed with respect to the following areas:

- Responses to security threats;
- Notifications procedures in the face of an identified security threat; and
- Privacy and confidentiality.

Limitations

The NGPC's resolution of June 2013 clearly sets out the scope of the framework.[5] As this resolution is the raison d'être of the framework, a conscientious effort has been made to limit the scope of this framework to that articulated in the resolution. For the purposes of clarity, the framework is limited to Registry Operator's responses to security threats such as pharming, phishing, malware and botnets and does not include a discussion on how to detect, investigate, analyse and report on security threats.

Moreover, the following are specifically considered to be out of scope for this framework:

1 **Clarification of Existing Requirements**

As noted above, the base new gTLD Registry Agreement does not specify a requirement for how Registry Operators ought to respond to identified security threats. This framework cannot therefore be considered as 'clarification' of Registry Operator's requirements – there is no applicable requirement to clarify. This framework is independent of the obligations in the new gTLD Registry Agreement.

2 **Creation of New Requirements**

This framework does not, and is not intended to, introduce new contractual requirements for Registry Operators in the form of SLAs or otherwise. The introduction of new contractual requirements with respect to how Registry Operators ought to respond to security threats must be through the mechanisms established in the new gTLD Registry Agreement. This framework is no way intended to circumvent those mechanisms.

3 **Purpose**

This framework, by way of a statement of non-binding principles, is intended to assist registries in addressing, or where more appropriate, referring security threats to the relevant party to resolve. It must be emphasized that the framework encompasses non-binding mitigation principles and accompanying rationale regarding how a Registry Operator *may* respond to security threats.

The limited scope of this framework has in no way inhibited efforts in the wider community to discuss and address matters beyond scope as evidenced by the recent creation of industry led initiatives in the area of malicious activity management.

Guiding Principles of the Framework

The following guiding principles are applicable to the framework as a whole:

[5] See NGPC Resolution 2013.06.25.NG02 – 2013.06.25.NG03, https://www.icann.org/resources/board-material/resolutions-new-gtld-2013-06-25-en#2.b

1 **General Objective to Reduce Time to Harm**

The general objective of the framework is to provide a platform to foster the adoption of practices that ultimately serve to reduce the time to harm for security threats.

2 **Universal Applicability**

The New gTLD Program has led to the introduction of new gTLDs that differ in terms of registration model, business model, size, restrictions, or other variables. Examples of such variables include:

Incorporation of Specification 13 into the New gTLD Registry Agreement i.e. '.Brand TLDs';

Designation as a Community Based New gTLD;

New gTLDs that represent Geographic Names;

Exemption to Specification 9 of the New gTLD Registry Agreement;

High registration fee and low volume new gTLDs;

Low registration fee and high volume new gTLDs;

Restricted eligibility new gTLDs.

The framework is intended to be both universally relevant and applicable to new gTLD Registry Operators regardless of these variables. This is achieved by providing for sufficient flexibility in the framework such that it is informative rather than prescriptive in nature.

3 **Standardization Not An Objective**

Given the nuanced nature of security threats and the differing types of new gTLDs as described above, all responses by Registry Operators to identified security threats will be based on an analysis of the specific set of facts and circumstances applicable to the threat and to the Registry Operator, thus rendering void any application of a 'one size fits all' approach to responses. This framework is conscious of this reality and in no way attempts to standardize Registry Operator responses to security threats by, amongst other things, mapping responses to threat types.

4 **Cognizance of Registry Operator Role**

The framework intends to ensure that any discussion of responses considered appropriate for Registry Operators is grounded in an understanding of the respective roles and capabilities of Registry Operators and registrars, as well as other third parties such as hosting or network providers.

5 **Registry Operator's Policies Govern Responses**

The framework recognises that it is ultimately the Registry Operator's policies that govern how a Registry Operator responds to an identified security threat. The framework intends to inform rather than prescribe these policies.

Outreach

In line with the NGPC's commitment to the GAC regarding ICANN soliciting community participation to develop a framework for Registry Operators to respond to identified security threats, ICANN conducted a preliminary consultation with a group of Registry Operators and GAC representatives between December 2014 and March 2015.

In July 2015, based on the feedback received and discussions during ICANN 53 in Buenos Aires, ICANN formed a Framework Drafting Team to develop the '*Framework for Registry Operators to Respond to Security Threats*'. As of 30 November 2015, the Drafting Team was composed of a total of 44 representatives from:

- The GAC Public Safety Working Group (9)
- Registry Operators (30); and
- Registrars (5).

Previous efforts

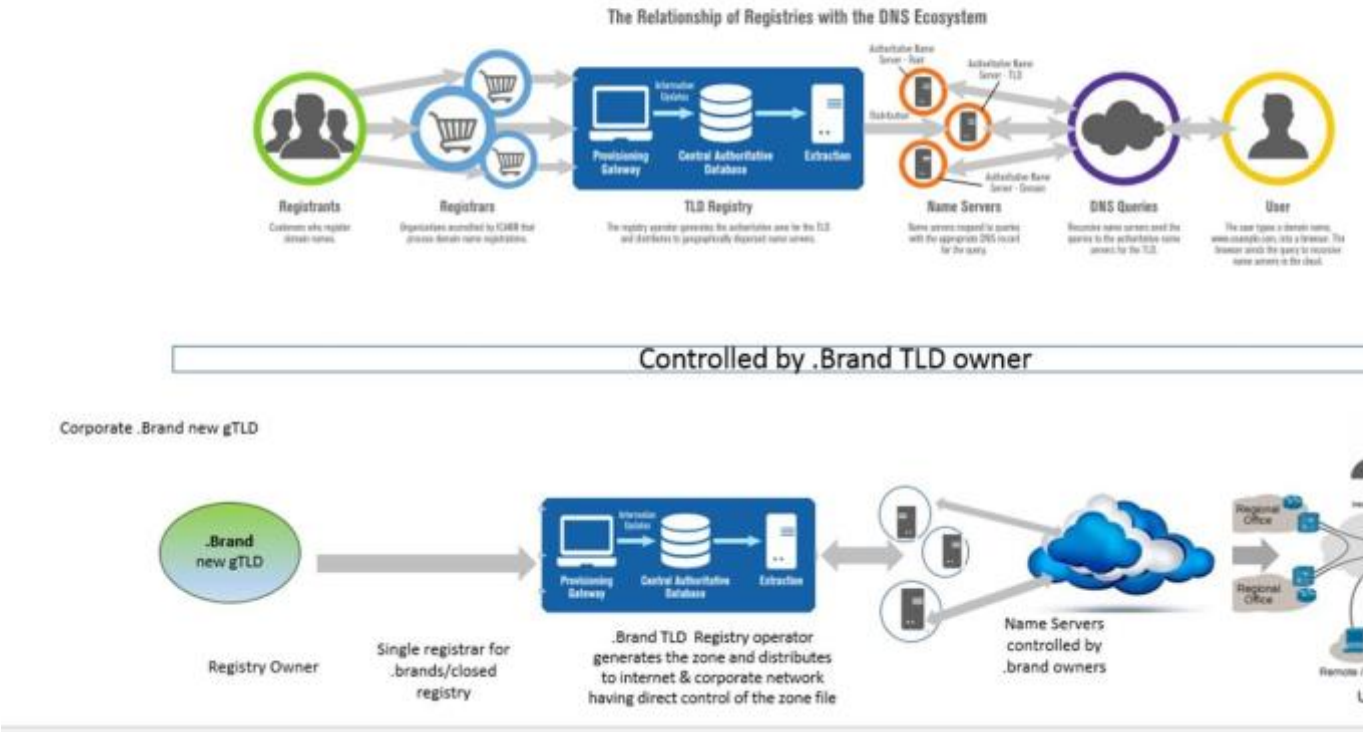
The ICANN community has discussed the mitigation of domain names used for abuse on several occasions, including:

- Discussion Paper on the Creation of non-binding Best Practices to help Registrars and Registries address the Abusive Registrations of Domain Names (September 2011)[6]
- Registration Abuse Policies Working Group Final Report (May 2010)[7]
- Mitigating Malicious Conduct - New gTLD Program Explanatory Memorandum (October 2009)[8]
- ICANN Security and Stability Advisory Committee Reports: SAC 007, SAC 028, SAC 038, SAC040, SAC044 and SAC 049 [9]

[6] http://gnso.icann.org/en/issues/rap/discussion-paper-rap-best-practices-28sep11-en.pdf
[7] http://gnso.icann.org/en/issues/rap/rap-wg-final-report-29may10-en.pdf
[8] https://archive.icann.org/en/topics/new-gtlds/mitigating-malicious-conduct-04oct09-en.pdf
[9] http://www.icann.org/en/committees/security/ssac-documents.htm

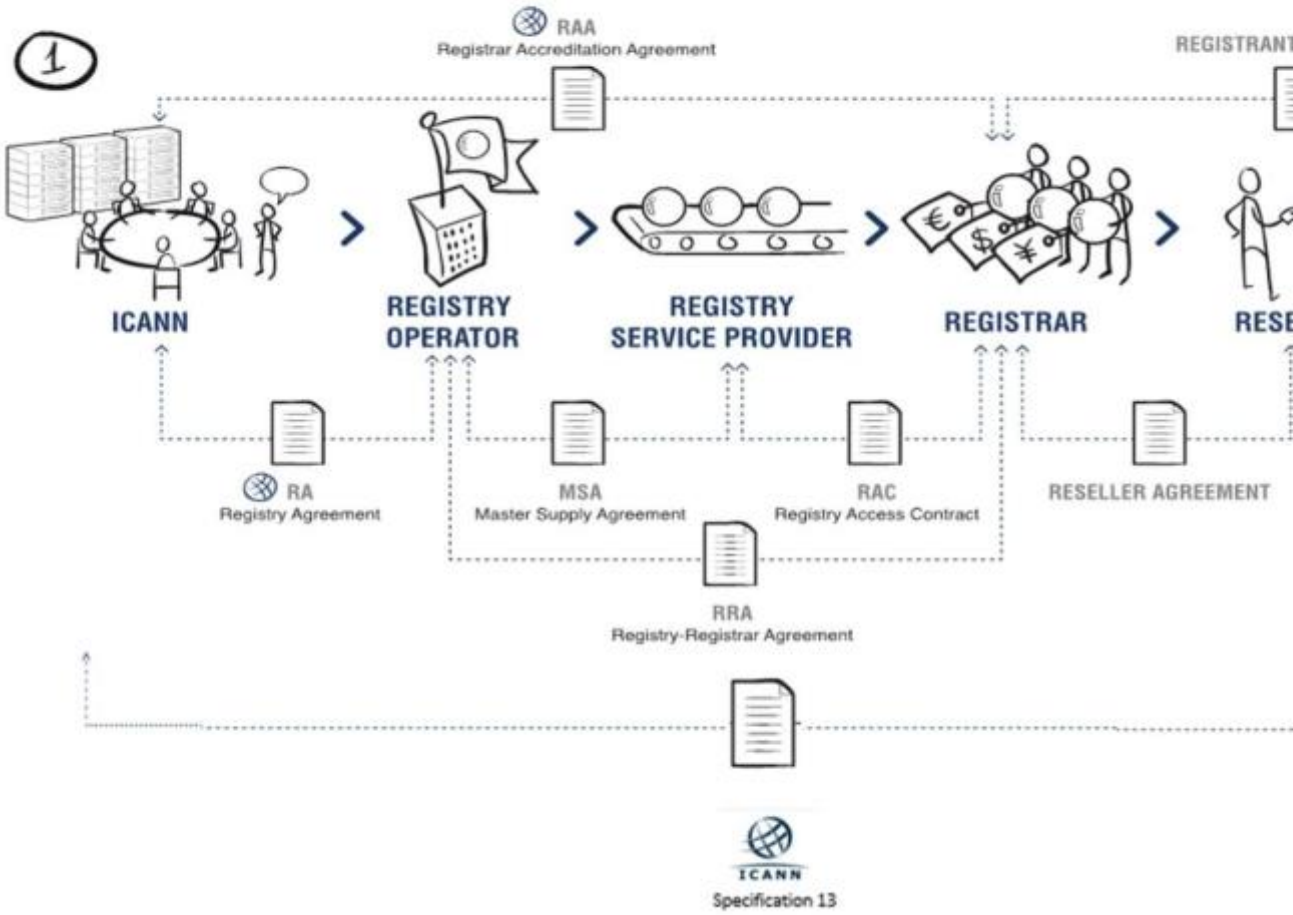
2 Registry Operator's role in DNS Ecosystem

The info-graphic below illustrates the role of the Registry Operator in the DNS Ecosystem:



Notably, the info-graphic highlights the limited operational interaction between commercial Registry Operators and registrants. In the first example it is the registrar, and not the Registry Operator, that owns the Registrant relationship and interaction. This limited interaction is supported by the contractual relationships typically in place between Registry Operators, registrar and registrants as illustrated on the following page.

The second example highlights the differences in the process, as experienced by Brand Registries, whose only registrant, is in effect themselves.



As described above, the registrant's contractual relationship is with the registrar and not the Registry Operator. This limited interaction between Registry Operators and Registrants and the commercial, operational and legal parameters and constraints inherent therein must be taken into account in any discussion regarding how Registry Operators respond to identified security threats. Specifically, it must

be recognized that the limited interaction, limits the Registry Operator's capabilities and therefore potential scope of actions.

3 Typical Phases of Action in Relation to Security Threats

While the scope of this framework is limited to Registry Operator responses to security threats, an overview of what occurs immediately prior to and following such is necessary to ensure a holistic approach to the framework. This overview will also serve as an educational tool for New gTLD Registry Operators by describing the typical phases of action in relation to security threats from detection to reporting.

Overview

Typical phases of actions taken in relation to security threats include:

1 Receive Data .

2 Analyze Data .

3 Identifying action.

4 Taking action and recording.

5 Reporting on the activity.

Note: The framework is applicable only to phases three and four.

Phase 1 - Receive Data

The receipt of information related to a security threat may be from a report to a abuse point of contact; or from a data feed or an automated analysis of domain names within a TLD.

Abuse Point of Contact

As per the terms of the new gTLD Registry Agreement, Registry Operators are required to provide to ICANN and publish on their website the accurate contact details including a valid email and mailing

address as well as a primary contact for handling inquiries related to abuse in the TLD. Security threats may be identified from information provided to this contact from a range of sources.

Data Feeds

Registry Operators, are encouraged to use public and/or private data feeds to identify security threats in the TLD. These feeds are often published by trusted security organizations based on reports from information security researchers, incident responders and automated systems. Should a Registry Operator opt for the use of such a data feed, it is advised that prior to incurring both cost and resources, a registry operator should consider, for guidance, the contents of the ICANN Advisory on Specification 11, 3.b.

As the characteristics of feeds vary, each Registry Operator may develop a different approach to using feeds, if indeed the use of feeds is considered appropriate. Common feed characteristics which may be reviewed before acceptance include the following:

1 **Accuracy**

In reviewing feeds, Registry Operators may consider accuracy as the most important criterion. The false positives rate, defined as non-abusive domain names listed as being involved in security threats, will be a significant indicator of feed accuracy and may impact a Registry Operator's use of feeds.

2 **Timeliness**

Timeliness of feed data may be measured based on the time lapsed from listing to delisting. Ideally domain names involved in security threats are identified as quickly as possible and published within the feed. As the underlying sources of feeds differ, this time varies significantly. Once domain names are no longer involved in security threats, they should also promptly be delisted from feeds.

3 **Volume**

The volume of feed data, defined by the number of identified security threats per time period, is a significant consideration when evaluating feeds. Registry Operators may evaluate feeds based on this criterion particularly to identify high volume feeds with low accuracy, which generate significant cost with limited benefit.

4 **Cost**

The usage costs of feeds are also a significant consideration when evaluating feeds. Ideally feeds will be available free of charge or at a low cost. This cost does not include the Registry Operator's costs to add new feeds to existing process and systems.

-

Automated Analysis

Registry Operators may use automated analysis of domains for security threats. This includes monitoring zone file changes and crawling web services on domain names for malware or phishing activity.

Phase 2 - Analyse Data

Once information relating to a security threat is received, the information is typically analysed to facilitate the identification of appropriate responses. Such analyses should be conducted in a timely manner, based on factors such as the severity of the threat. This analysis may include validation of threat information and documentation of findings. An analysis may also be conducted to identify the type of security threat; whether it is an abusive domain name registration or if it is as a result of compromised systems. The following parameters may be considered in this analysis.

Relevance

A Registry Operator may review the received security threat information for relevance to their TLD. This review may include verification that the domain names involved in the security threat are within the TLD and that the Registry Operator is the appropriate party for follow-up action. **Accuracy**

Registry Operators may employ multiple methods to measure the accuracy of reports regarding security threats. These methods may include manual or automated processes such as review by information security researchers or automated tools such as anti-virus scanners.

In the event that the Registry Operator lacks the resources, expertise or authority to review and make a determination regarding a security threat, it may elect to, or request that the reporter, forward the information to the relevant government public safety and or Law Enforcement Agency for investigation and follow-up.

Policies

The Registry Operator may review security threat information regarding domain names to identify any TLD policy implications with respect to the behaviour and circumstances at hand. For example, have the TLD's Registration and/or Anti-Abuse policies been violated? Furthermore, Registry Operators may utilize any reported cases of security threat to refine their policies.

Phase 3 - Identify Action – Framework Applicable to this State

Where the security threat is identified as posing an actual risk of harm, an identification of the response is required. The following parameters may be considered in this phase:

Responsible Parties

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. This step requires an understanding of the Registry Operator's role in the DNS Ecosystem as described in section 2 of this document. For example, , in the case of abusive registrations, the registrar 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.

Escalation Targets

Escalation targets will depend on the type of security threat identified and purpose of the domain name. In the case of abusive registrations, the Registry Operator may contact the registrar, as the registrar is both able to address the registration for a specific domain name and identify related domain names within a potentially abusive account. In the case of compromised systems within a domain, the registrant and their hosting provider are most capable of remedying the underlying security threat.

As the Registry Operator does not maintain a direct relationship with the registrant or hosting providers, the Registry Operators may notify the registrar in these cases to support remediation efforts.

Interpretation of Policies

The Registry Operator's TLD policies typically govern the types of responses available to the Registry Operator. Given the unique nature of TLD policies that are developed based on applicable legal, operational and technical requirements, consultation of existing policies may be required to ensure coverage. TLD policies may also be updated to address new circumstances and lessons learnt from previous security threats.

Phase 4 - Take Action – Framework Applicable to this State

Where the Registry Operator has identified the appropriate action, such action may be taken by the Registry Operator or referred to a third party organization such as a relevant law enforcement agency.

Notification

Registry Operator may communicate with the registrar of the domain name or other parties to support remediation efforts

Record Action

The Registry Operator's documenting of the results of any review of reports of security threats will support reporting needs and allow research in the event that details on a specific security threat are needed.

Communications

Registry Operator communications with registrar or other parties may be archived. This includes initial and follow up emails.

Supporting Documentation

Supporting documentation, including technical details, such as identified malware details, may also be recorded by Registry Operators.

Results

Registry Operators may record actions taken and final status of domains involved in security threats. Categorization such as 'reported to registrar', 'false positive' and 'cleaned' may assist in reporting.

Phase 5 - Report on Action

Registry Operators may report on activities in relation to security threats. These reports may include:

- common metrics such as the number of identified security threats classified by;

category, for instance, phishing or malware; or

registrar; and

- the number of instances where actions, such as reporting to registrars, are taken.

Reports may be created annually or may be created more frequently based on the reporting capabilities and needs of the Registry Operator.

4 Responses to Security Threats

The principles herein stated are intended to support Registry Operators in adequately responding to an identified security threat. For clarity, 'response' in this context is taken to mean the action, or actions, following receipt of a security threat specifically identified by the Registry Operator as posing an actual risk of harm in accordance with the TLD policies.

Underlying the response to any such identified security threat must be the understanding that an appropriate response for one Registry Operator may differ from that of another. Further, each security threat is unique and therefore not capable of being addressed by a single static process. Various considerations such as localized legislative requirements, TLD specific requirements (e.g. Public Interest Commitments), and individual Registry Operator's Acceptable Use / Anti-Abuse policies provide that there can be no specific and universal approach in responding to security threats. The annunciation of principles, across the spectrum of all Registry Operators, therefore, must remain that of a high level guidance with an aim of uniformity of result achieved and not of the approach used to achieve it.

Single Point of Contact

Principle

To effectively ensure that all relevant security threats are responded to in an adequate fashion, a Registry Operator may ensure that all such matters are reviewed centrally, under the guidance of a Single Point of Contact (SPOC).

Rationale

A SPOC, either being an identified person and/or department ensures:

1 **Internal Uniformity**

A properly identified central recipient for all reports and subsequent review and action of identified security threats promotes consistency, ensuring the uniform application of the process and procedure of that Registry Operator.

2 **External Consistency**

For external parties conveying the notification of security threats to a Registry Operator, the availability of a SPOC provides confidence in communication, review and response.

Proportionality of Response

Principle

Any action taken in response to an identified security threat should have the intended effect of mitigating that security threat; however, any such mitigation should, wherever possible, be proportionate to the scope of threat and account for the anticipated results including potential consequential loss. [10]

Rationale

This principle is based on the fact that the mitigation of the security threat should only be considered achieved when actions taken are done so with due regard to the principles of proportionality:

1 the action must be proportionate to the result desired, and not overbroad in ambit;

2 the action must achieve the desired result with the least possible disruption; and

3 the action must adequately consider competing interests or collateral effects, if any; and

4 if the function of a given domain name is unclear the Registry Operator may forward the details to local public safety or law enforcement agencies before taking any action, even if it contradicts the principle of timeliness as described in 4.4.

In essence, any response to a security threat should represent the least invasive and least disruptive course of action for all parties involved, whilst still being capable of achieving the objective i.e. the mitigation of the identified security threat. Any actions therefore should be undertaken within a reasonable timeframe, by the appropriate party, and should be measured in their ambit so as to not over-reach the ultimate objective of the remediation. .

Actions taken should be conscious of the likely culpability of the registrant such that, where possible, an effort is made to educate the registrant and an opportunity granted to remedy the threat where the situation indicates the registrant is likely not culpable. In a similar vein, Registry Operators should, unless the severity of the threat dictates otherwise, consider adopting an escalation process rather than taking immediate severe action in responding to a security threat. Furthermore, considerations should be given where the registry operator will want to work with public safety agencies to ensure evidence of criminality can be preserved.

[10] Please note that 'mitigation' in this context is defined as the completion of any action, by a Registry Operator, which they believe is sufficient to satisfy the statement that the identified security threat is either no longer valid, no longer existing, or has been escalated as appropriately, such that it is no longer within the power or responsibility of the Registry Operator to further action.

It is recommended that, any action by a Registry Operator[11], should ideally remain reversible in the event of a mistake, innocent actor, etc. (e.g. placing a domain name on 'serverhold' versus the deletion of the domain name), ensuring that any potential errors, omissions, or unforeseen repercussions are capable of being remedied with minimum effort and effect on all parties.

Response Grounded in the TLD Policies

Principle

Both the Registry Operator's identification of a security threat as posing an actual risk of harm and the response to the threat should be grounded in the Registry Operator's TLD policies, with due regard to the requirements of Spec 11 3 (a), where applicable.

Rationale

While there may be varied and competing views and interests regarding as to what an identified security threat is and as to what actions should be taken in response to an identified security threat, it is imperative that the registrant is granted access to an authoritative source of information in relation to both these matters. This source is typically the Registry Operator's TLD policies. The transparent publication of the TLD policies, and the Registry Operator's adherence to such, grants the registrant with a degree of predictability regarding what actions may be taken in relation to its domain name. It also serves to protect the registrant against the taking of arbitrary action with respect to its domain name.

Timely Response

Principle

In the interests of proportionality, Registry Operators should respond to any identified security threat within a timely and reasonable time frame. .. Many security threats are time-sensitive and need to be addressed in the most expeditious manner, not only for the safety and security of the DNS, but in the interests of public safety. It is understood not all security threats should be handled in the same manner and timeframe; the relevant timings should take into account both the source and the severity of the reported threat.

[11] An 'action' is a direct action taken by the Registry Operator, through use of the Shared Registry System or equivalent, which is considered to remove the security threat.

This framework identifies 3 categories of Security Threats, for which it defines what constitutes a timely response:

1. Imminent Threat to life or limb, and child exploitation[12]: 24 hours
2. Threats to Internet Infrastructure and Critical Infrastructure[13]: 48 hours
3. Use of domain name for furtherance of non-life threatening crimes: 72 hours

The notifying party (including law enforcement or public safety agency) shall provide Registry Operators with:

1. Verifiable credentials for reliable identification
2. Sufficient and specific information related to the nature of the Security Threat allowing for assessment of categorization

Rationale

The priority allocated and the speed with which a Registry Operator reviews and actions, as appropriate, an identified security threat, should be linked to the identified threat itself.

Given the shared responsibility of all Registry Operators in attaining the desired result, which is the mitigation of an identified security threat, so too should all parties share, in principle, the achievement of such a result within in a reasonable and timely manner

This framework does not purport to identify the specific timeframe required for individual security threats; however, any such limits should be justifiable and directly linked to the following:

1 **Source of the Identified Security Threats**

Although a matter for the individual Registry Operator, there exists a natural hierarchy of the severity of security threats and quality and standard of the evidence provided in a source's report. The obvious example is where priority should be given and actions taken perhaps more quickly are for those reports properly made by national authorities or where a request is grounded by court order.

[12] See for instance the Council of Europe's Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (Lanzarote Convention) for relevant definitions of related crimes at https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/201

[13] Such threat include Botnet, Malware and intrusions into Critical Infrastucture may include Chemical facilities, Commerical facilities, Communications, Manufacturing, Dams, Defense Industry facilities, Emergency Services, Energy, Financial Serivces, Food and Agriculture, Government facilities, Healthcase and Public Health, Information Technology, Nuclear facilities materials and waste, Transportation systems and Water and Wastewater Systems (inspired from the US PPD-21 on Criticlal Infrastructure Security and Relience (https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil)

That is not to say however that a report, duly evidenced, received from any other source shall not be given due attention or regard. Registry Operators should ensure that adequate procedures are put in place, to ensure proper attention is given to any received report.

2 **Severity of the Security Threat**

Objectively, certain identified security threats, by their nature shall require a prioritized review: e.g. threats which have the potential to disrupt or damage the stability of the DNS and/or threats which have the potential to cause actual or substantial harm. Subjectively, the identification of a hierarchy of such security threats are a matter for the individual Registry Operator, with consultation with other parties such as Law Enforcement and Public Safety organizations, as appropriate, and may vary based on the nature of the TLD(s) controlled.

Appropriate Actions Taken By Appropriate Parties

Principle

In the interests of proportionality, any action, where possible, should be taken by the most appropriate party (Registry Operator, registrar, reseller, registrant, hosting provider, ISP, etc...) with due regard to matters such as, but not necessarily limited to, proximity to the security threat, relevant policies, local legislative requirements and/or legal climate.

Rationale

Security threats are capable of being initially reported to any one of the parties in the domain name registration and operation chain; however, being the point of initial complaint, does not necessarily qualify that party to be the most appropriate to take action. It is further reasoned that perhaps due to policy or local legislation, a party may be unable or unwilling to take action in a particular instance, whereas other related parties are not equally constrained.

The degree of relationship to the registrant must be a key consideration in framing a response to any security threat. A Registry Operator may be capable of taking action in any given situation; however that does not necessarily mean they ought to. Where possible, the party with the direct relationship to the registrant should, at the very least be invited to review and action.

Justification, Transparency and Retention

Principle

All actions taken by parties in the response to identified security threats must not be arbitrary. Where remediation has been achieved, all parties must be mindful of the need to retain supporting

documentation and/or other evidence. Any and all such data should be retained for no more than is considered necessary to the party retaining such records.

Rationale

The effectiveness of any framework for response to security threats, must also consider the need to ensure that all parties remain good actors. As a necessary element in ensuring all parties act in the spirit of openness and transparency, they should be capable of providing adequate justification for any action taken. Although this framework does not purport to require such justification, or indeed does propose a mechanism for the testing of such, on principle, all parties to the framework must be firm in their commitment to not act in an arbitrary and unfair manner. Out of necessity therefore, this principle is enunciated, but only at a very high level. Its application and relevance is heavily dependent on factors such as the strength of commitment to the voluntary framework, and hinges on elements such as the specific types of information held, the countries of residence of the parties, and has particular applicability to the holding and/or processing of data, which may or may not be considered personal data.

From a practical point of view, regardless of the framework's guidance, as a matter of good business, each party should ensure accurate and sufficient records are always available as required; for example litigation, in contemplation of complaint etc.

5 Notification Procedures

With specific reference to the principles previously noted regarding the response to identified security threats, a key element of any response to such security threats includes the appropriate notification of the related and /or relevant parties affected.

Common to the principles regarding response to identified security threats, notifications of the various stakeholders must be equally aligned with the principles of proportionality. In the interests of minimal impact, with maximum effect, the following principles are noted:

Sufficiently Identified Contacts / Communication with the Appropriate Parties

Principle

Notification should always be issued to the relevant and correct party, unless such notification is to a malicious actor, willing participant/accessory or party who is the past has been unresponsive. Notifications should not be used if such notification will harm or negatively impact the prevention, mitigation or termination of a security threat in any way. Although it is a matter for the individual Registry Operator to notify any party they deem necessary, such inclusions should, where possible, be directly related and relevant to the matter at hand.

Rationale

In order to ensure timely response and action, the parties to whom a Registry Operator sends any notification should be limited to those who are relevant to the matter at hand. The inclusion of several parties on any notification may lead to confusion, delay and indicate a less meaningful engagement for the mitigation of an identified security threat.

Registry Operators should ensure that relevant abuse contacts are identified as a matter of course with their registrar channel and/or if appropriate, their resellers. Again mirroring the availability of a SPOC within Registry Operators, this should be implemented at all levels of the chain of mitigation, to ensure direct and timely remediation as appropriate.

Detailed and Clear Notifications

Principle

Notifications issued should be written, clear and provide all relevant and appropriate detail, providing such information to enable the recipient to review and escalate as appropriate.

Rationale

If a security threat has been identified, any recipient of a notification should be provided with the information that has grounded such an identification, so as to enable them to review and/or action as appropriate. The absence of sufficiently clear information would likely lead to delay and cause confusion.

Responsiveness of the Parties

Principle

On receipt of a notification, a response should be issued. Responses should be timely, and should issue, as appropriate, within a reasonable time frame which has been set with due regard to both the source and the severity of the reported threat.

Rationale

For certainty, and in order to prevent undue delay, all notifications issued should be the subject of a response. It is not within the function or scope of this framework to identify the content of any such response; however as a general guideline, such responses should be written, clear, relevant and timely.

Errors regarding any notification, or recipients therein included, should be also raised as appropriate to ensure ongoing streamlining of the process of security threat notifications.

Limited direct Contact with Resellers and Registrants

Principle

Registry Operators are not precluded from making direct contact with any relevant party including, but not necessarily limited to, a reseller or a registrant. Registry Operators should always consider carefully any such direct contact, with particular reference to instances where it is clear that such contact may harm or negatively impact the prevention, mitigation or termination of a security threat in any way. Such contact should be ordinarily limited to, and exercised on occasions where the source or severity of the identified security threat warrants the contact. Unless otherwise precluded from doing so, the registrar should be advised that such a contact has been made.

Rationale

In the case of Registry Operators attempting to prevent, mitigate or terminate an identified security threat, timely action and responsiveness of the parties are vital to ensuring an appropriate priority is allocated to mitigation.

Where, as in the majority of cases, a registrar is identified as the appropriate party to whom escalation should occur, the Registry Operator should direct notifications to the relevant registrar. If, after a reasonable period of time has passed and such a registrar remains either non-responsive, or have indicated that they are either unwilling and/or unable to review a matter as notified, the Registry Operator shall not be prevented from making contact with the reseller, and/or the registrant directly. It is a matter for the individual Registry Operator to decide when, if at all, such communications should issue.

Although not expected to be a common occurrence, regardless of whether or not a Registry Operator first notifies the relevant registrar, it remains at the discretion of that Registry Operator whether or not to make direct contact with any other connected party in priority to that registrar. In reaching such a decision, a Registry should take into account the source and severity of the security threat, the appropriateness of such a communication and any other matters it believes to be relevant.

Notification to ICANN

Principle

Depending on the severity of the security threat, a Registry Operator may initiate the Expedited Registry Security Request Process with ICANN in order to obtain mitigation assistance and alert the community of the potential threat

Rationale

A process exists for Registry Operators to inform ICANN of a present or imminent security incident to their TLD and/or the DNS to request a contractual waiver for actions it might take or has taken to mitigate or eliminate an incident[14].

Intelligence Sharing

Principle

There may be instances in which Registry Operators should consider the sharing of appropriately sanitized intelligence regarding identified security threats. Intelligence sharing should be limited in circulation to between registry operators, registrars (including, where appropriate, resellers), members of Law Enforcement (LE), and public safety authorities, with specific reference to avenues existing to the

[14] https://www.icann.org/resources/pages/ersr-2012-02-25-en

members of the Public Safety Working Group (PSWG).The sharing of this Intelligence should be aimed at the development of a dynamic and more effective detection and reporting process for the mitigation of security threats.

Rationale

Given the expertise of industry colleagues, LE and the members of the PSWG in matters regarding security threats, Registry Operators may find ongoing engagement to be of great benefit in effectively and efficiently responding to identified security threats.

Shared information should relate to, but not necessarily be limited to the nature of the threats identified, the details of actions taken, outcomes of actions and any lessons learned.

With the ever evolving methods and mediums by which security threats, old and new, are perpetrated, such an intelligence sharing endeavour can be of great assistance in identification, response, limitation of actual harm caused, and the reach and uptime of security threats, both present and future.

Safeguards

Given the sensitive nature of information regarding security threats, such information cannot be freely and publically available. Stakeholders should work towards identifying appropriately secure methods of 'Intelligence Sharing', in order to minimize the chance that shared information has a detrimental effect in ongoing security threat mitigation efforts.

6 Appropriate Consequences

As explored in the guiding principles, any discussion regarding appropriate consequences with respect to an identified security threat must be grounded in the understanding that such consequences will always be based on an analysis of the specific set of facts and circumstances pertaining to the threat. An appropriate consequence for one Registry Operator may differ from that of another. Further, each security threat is unique and therefore not capable of being addressed by a single static process. Various considerations such as localized legislative requirements, TLD specific requirements (for example, Public Interest Commitments), and individual Registry Operator's Acceptable Use / Anti-Abuse policies provide that there can be no specific and universal approach in responding to security threats.

The limited interaction between Registry Operators and registrants and the commercial, operational and legal parameters and constraints inherent therein must also be taken into account in any discussion regarding appropriate consequences with respect to an identified security threat. Specifically, it must be recognized that the limited interaction, restricts the Registry Operator's capabilities and therefore potential scope of actions. It is the registrar that typically owns the relationship with the registrant and is therefore best placed to review and address registration issues at the registrar level. Owing to this fact, the role of the Registry Operator, in the majority of cases, is limited to referring a security threat to the registrar. This reality is reflected in the robustness of processes implemented in the registrar community regarding how registrars respond to complaints regarding abuse and illegal activity. Some of these processes are captured in a set of registrar best practices in the document titled 'Unified Registrar Approaches to Abuse'. This document, along with the principles described in this framework, should sufficiently serve to provide Registry Operators with a holistic view of appropriate consequences with respect to an identified security threat.

Annex A

Examples of Responses to Abusive Activity

Abusive registrations, by their nature, vary widely in scope, severity and urgency. Accordingly, there cannot be a "one size fits all" approach as to how those registrations are handled when referred to Registries. That being said, it is important that abusive registrations are addressed and done so appropriately.

Here is one appropriate way (of many) that an Abuse referral can be handled, using a hypothetical referral alleging spam:

1) John Doe (the "Referrer") writes to the ICANN Abuse contact listed for our ".example" TLD, "Abuse@registry.example." The Referrer states that he has received spam from the domain "www.spam.example." The Abuse@registry.example email address directs to employees at our Registry who are empowered to act on Abuse referrals.

2) The Registry evaluates the complaint and determines whether the Referrer has alleged enough to warrant further investigation into the domain (as opposed to, for example, a referral that alleges some sort of copyright infringement which is outside of the Registry's Abuse mitigation purview). Given that the Referrer directly alleged that the domain in question has engaged in spam, the Registry determines that further investigation is warranted.

3) The Registry (or perhaps a Reputation Service Provider acting on the Registry's behalf) conducts research on the domain, including for example, whether the domain is listed on reputable and trusted blacklist providers and/or otherwise definitely exhibits technical indicia that it is engaged in spam. In our example, the domain "registry.example" is determined to be likely engaged in active spamming. The Registry retains the right to determine whether the domain is likely to be engaged in abusive activity.

4) If the Registry determines that the domain is likely an abusive registration, then the Registry will refer the matter to the sponsoring Registrar for investigation and action. The Registrar has the direct commercial relationship with the domain name Registrant and, in most instances, the Registry should provide the Registrar the opportunity to address and attempt to mitigate any abusive registrations. Consistent with the Registry's remit to address and remediate technical Abuse as a threat to the security and stability of the Internet, the Registry informs the Registrar that if it does not take action to address the spam, the Registry reserves the right to do so.

5) Registrars often (upon conducting and confirming their own investigation) act upon Abuse referrals from Registries. That being said, there are instances in which a Registrar either (i) disagrees with the Registry's conclusions; or (ii) fails to respond or act on the Registry's referrals. For this hypothetical, the Registrar did not respond to the Registry's referral and did not act on the domain in question.

6) Given the Registrar's inaction in this hypothetical, the Registry, being satisfied that it has been presented with sufficient evidence, suspends the domain (via EPP commands at the Registry level). In most instances, suspending the domain is preferable to terminating the domain name registration because such an action remains easily reversible, should a valid appeal be made. In addition should the Registry delete the registration, the same domain name becomes available again for registration (perhaps by the same registrant for the same Abusive purposes).

Case Example: Registries – Key to Frontline Action: The Takedown of the Cryptolocker Malware/Gameover ZeuS Botnet

Background

CryptoLocker is a malware believed to have emerged on the Internet in 2013 and responsible for encrypting files of an infected computer before demanding a ransom payment to the owner in exchange for keys to decrypt the affected files. It was spread via infected emails by relying on the Gameover ZeuS Botnet infrastructure, itself a by-product of malicious computer program that turned an estimated 1 million infected computers globally into agents of this botnet (Source: FBI). It is estimated that Cryptolocker made 500,000 victims and extorted up to 3M$ from those willing to pay the ransom[15].

Operation Tovar is credited with disrupting the Gameover ZeuS Botnet infrastructure, which eventually led to the neutralization of Cryptolocker. It was a coordinated effort conducted by law enforcement agencies in North America, Europe, Japan and Russia, with contributions from various countries' CERTs, private companies, financial institutions and researchers, which led to take down of infected computers, command & control servers, as well as the arrest of criminals. In particular, collaboration between law enforcement agencies, gTLD Registries (Afilias, Neustar, Public Interest Registry and Verisign) and ICANN was a key contributing factor to this operation.

Challenges

Cryptolocker and Gameover ZeuS, like other botnets and malware types, make use of steps in the domain registration process, as implemented by each particular registrar and its resellers, that are exploited by criminals for the registration of algorithmically generated domain names (DGA domains). As examples, criminal abuse of reseller or registrar APIs, lack of verification of credit card data against stolen data traded in underground forums, use of crypto currencies that allow for increased anonymity, use of Whois data points already flagged as malicious (for example, the name servers have already been seen in association with other botnet, or the Admin Contact's email address has been used for registering domains in a previous malicious campaign), use of privacy/proxy services as another anonymization vector that aids criminals in their malicious campaigns.

[15] http://www.bbc.com/news/technology-28661463

The spread of such cyber threats abusing DNS resources require the response against them to be a coordinated community ~~international~~ effort, usually on an international scale. Single actions or single actors in a single jurisdiction will not be able to effectively mitigate or contain threats.

Additionally, the fast pace with which malicious activity occurs, very frequently means that by the time the malicious domains are detected and suspended or canceled, the criminals have already used them, profited from them and even discarded them. This requires prompt information sharing between interested parties as well as specific prevention and mitigation measures.

Notification of Threats

Considering the scale and complexity of the Cryptolocker/GameverZeuS threats, involvement of Registries was a key contributing factor to the success of the threats' mitigation.

While communications between trusted law enforcement agencies relevant to the Registries' respective jurisdictions were efficient once the threat was identified and communication channels established, several factors could improve future collaboration:

- Pre-established relationships between law enforcement agencies and Registry Operators facilitate the timely exchange of threat information.
- Prompt information sharing between registries and trusted interveners for the processing of abuse reports accelerates the mitigation of the threat.

In addition to collaborating with relevant law enforcement agencies in prevention or curation of threats, Registries may also wish to consider collaborating with programs such as the APWG's Malicious Domain Suspension Program (AMDoS)[16], where vetted security researchers can submit reports of abuse to registrars and the registrars commit to quickly mitigate the threats, if within the program's guidelines. While the AMDoS Program is initially aimed at registrars, nothing prevents Registries to engage with the APWG and sign-up to the program themselves or offer incentives to its accredited registrars that decide to sign-up.

Response and Actions Taken

Registries

While most Registries did not require a court order to take action because available evidence proved compelling enough to constitute abuse as defined in their Anti-Abuse Policy, some Registries did require a court order to take action.

Actions taken by registries involved suspension of domain names, as well as sinkholing of DNS resolution which is a technique that re-directs malicious traffic coming from hosts infected with malware to services controlled by researchers and/or law enforcement agencies to collect intelligence, conduct analysis and take appropriate actions. In addition to the identification of a botnet's command and

[16] https://apwg.org/apwg-news-center/amdos/

control infrastructure, this technique also allows for the immediate disruption of communications between the infected hosts and the botnet's command and control servers thus preventing further spreading of the related threats.

When immediate action is deemed necessary, prompt sinkholing, which involves updating the DNS Records or targeted domain delegations, may be achieved by Registries under the auspices of the Expedited Security Request (ERSR) process available at ICANN.

ICANN

An important factor in allowing Registries to mitigate the Gameover ZeuS/Cryptolocker threats was in fact the use of the ERSR process by several registries. In the context of abusive domains based on Domain Generation Algorithms (or DGA domains) that criminals use for command and control of their botnets, ICANN's Expedited Registry Security Request (ERSR) procedure proved effective for purposes of preemptively blocking or sinkholing the domains associated with a given botnet and effectively taking the malicious infrastructure away from the criminals' control.

The Expedited Registry Security Request (ERSR) was developed by ICANN to provide a path for gTLD registries who inform ICANN of a present or imminent security incident to their TLD and/or the DNS to request a waiver from compliance with a specific provision of the Registry Agreement for the time period necessary to respond to the incident, for actions it might take or has taken to mitigate or eliminate an Incident. Such incidents include "Malicious activity involving the DNS of scale and severity that threatens systematic security, stability and resiliency of a TLD or the DNS; or Unauthorized disclosure, alteration, insertion or destruction of registry data, or the unauthorized access to or disclosure of information or resources on the Internet by systems operating in accordance with all applicable standards;"

Registrars

While Registrars were not directly involved in mitigation of the Gameover ZeuS/Cryptolocker threats, Algorithmically Generated Domains (DGAs) require the community to consider matters related to registry/registrar prediction of abusive registrations so the malicious domains can be prevented from registration right at their point of creation.

Network Administrators and End-Users

Administrators of networks of all sizes, from that of individuals to that of large organizations, should monitor and analyze their internal network's DNS traffic since it is one of the most effective ways to detect compromised machines: Usually as soon as the botnet compromises a device, it will attempt to contact its command and control server via DNS. Such monitoring also helps determine the type of malware, enhances the effectiveness of the response efforts and aids in information sharing across organizations.

Administrator of mail servers should consider the inclusion of SPF, DKIM and DMARC records in the DNS information of their domain names, which help prevent receipt of spoofed email messages and can provide useful insight in mitigating malware threats by acting as a 'virtual handshake' between email sender and receiver, ensuring only authenticated email is delivered to customers. In the case of

Cryptolocker, DMARC information for one known attack reveals how criminals attempted to use a well-known domain to send a malicious email containing a malware attachment (Soucre: http://www.infosecurity-magazine.com/opinions/threat-intelligence-fuelling/)

End-Users should be continuously trained on awareness and phish-spotting. No matter how much an organization invests in the protection of its informational assets, it must always invest in the human resource. The assumption must be that users will click on malicious links simply because that's human nature – either the user is tired late at night or in a rush, or simply under a huge amount of stress. So, effectively increasing their awareness will reduce the likeliness of occurrence.

Annex B – Registry Operator Policies

Registry Operators are required to publish and maintain clear registration policies. Such policies are available on the respective website of each applicable registry operator, a listing of which is available from ICANN at: https://www.icann.org/resources/pages/listing-2012-02-25-en

It must be noted that although the individual Registry Agreements may dictate the inclusion of common elements across registration policies of all Registry Operators, it is ultimately at the sole discretion of the relevant registry operator as to the manner and method of such inclusions. Beyond any such common elements, registry operators may also include any term that they see fit, as long all inclusions remain transparent and in a manner consistent with the general principles of openness and non-discrimination. A registration policy of single registry operator therefore should not be considered as universally applicable and/or directly comparable to that of another. Likewise, the policies and business practices of one Registry should not be used as grounds for any claim that a separate registry operator is not adhering to this Framework.