ICANN66 Prep Week: DNS Abuse Webinar
17 OCTOBER 2019

GAC Public Safety Working Group
Registries Stakeholder Group
Registrars Stakeholder Group
Current Concerns and Issues Regarding DNS Abuse (PSWG)

DNS Abuse Webinar
October 15, 2019

Laureen Kapin, US Federal Trade Commission, Counsel for International Affairs for Consumer Protection, PSWG Co-Chair

Gregory Mounier, Europol, European Cybercrime Centre (EC3)

Gabriel Andrews, US Federal Bureau of Investigation, Cyber Initiative Resource Fusion Unit
Road Map

1. Combatting Domain Name System Abuse
2. “DNS Abuse” as seen by Law Enforcement
3. Best practices to create a safer DNS eco-system
1. Combatting DNS Abuse

Why Mitigation of DNS Abuse is a Vital Topic

- Global cost of Cybercrime: $600 billion in 2018 (Source: CCT Review)
- The public relies on the DNS for communications and transactions; so do cyber-criminals
- GDPR is causing challenges for investigating cyber-threats that use the DNS
- Potential second round of gTLDs offers opportunities for improvements
1. Combatting DNS Abuse

Why ICANN and Contracted Parties Must Take Steps

- ICANN operates “for the benefit of the Internet community as a whole” [Bylaws, Commitments]
- Administration of the DNS requires ensuring the DNS infrastructure is safe and secure
- ICANN Bylaws include duty to assess the effectiveness of various efforts to address threats to the security and stability of the DNS, and to meet the needs of law enforcement and promote consumer trust
- Registration policies influence abuse (CCT Review conclusions)

As you’ll hear, these steps can be systemic and pro-active to both aim at bad actors that pollute the DNS and encourage mechanisms that promote a more secure DNS
ICANN’s Domain Abuse Activity Reporting tool (DAAR) has identified categories of abuse such as:

“Phishing, Malware, Botnet command-and-control & Spam”
2. Where DNS Abuse meets Law Enforcement

DAAR has identified categories of abuse such as: “Phishing, Malware, Botnet command-and-control & Spam”

From: CEO’s True Name
[mailto:redacted@flyietedge.com]
Sent: Wednesday, August 19, 2015 12:13 PM
To: CFO’s True Name
<redacted@flyjetedge.com>
Subject: Fwd: Payment

Please find the attached invoice to be settled today, confirm receipt of mail

CEO’s True Name

Sent from my iPhone
2. Where DNS Abuse meets Law Enforcement

- DAAR has identified categories of abuse such as:
  “Phishing, Malware, Botnet command-and-control & Spam”

Source = CyberReason
2. Where DNS Abuse meets Law Enforcement

Quantification of “Abuse” is tough… but essential to shared understanding of facts.

- Competition, Consumer Trust, and Consumer Choice commissioned Study on DNS Abuse,
- DAAR,
- Identifier Technology Health Indicators,
- Quality Performance Index
etc

Quantify what actions inhibit abusive behavior, and incentivize them

Quantify what factors encourage abuse, and disincentivize them
3. Best Practices - Systemic

Competition, Consumer Trust and Consumer Choice Review Team (CCT RT) generated Recommendations aimed at DNS Abuse:

- **Recommendation 14:** incentivize the adoption of proactive anti-abuse measures in Registry Agreements

- **Recommendation 15:** contractual provisions aimed at preventing systemic use of specific registrars or registries for DNS Security Abuse, including thresholds of abuse at which compliance inquiries are automatically triggered.

- **Recommendation 17:** publication of the chain of parties responsible for domains (including resellers)
3. Best Practices – ccTLDs

Pro-active anti-abuse measures – examples from ccTLD space

- ccTLDs Proactive anti-abuse measures
- Do it because they want to be trusted place for users. No content. Scams, malware, phishing
- Simple, innovative measures => substantial impact on rate of abuse.

- Examples from ccTLDs registries:
  - EURid / .EU
    - Machine learning - Estimation of possibly abusive domains before their delegation
    - Identification of possibly abusive domain names after their delegation (Clones of bank login pages, fake eShops, C2-like domains, IP infringements etc.)
  - SIDN / .NL
    - Artificial Intelligence (AI) to predict malicious registrations
  - DIFO / .DK
    - Strong authentication and KYC. Close cooperation with LEA. Reduced abuse rate from 7% to 0.1% in 8 months.

Pro-active identification of abusive registrations
- Strict KYC and authentication methods
- Close cooperation with LE and judiciary for takedowns/seizing

=> Tried and tested methods that should inspire gTLDs
3. Best Practices - gTLDs

- **Economic incentives and cooperation on takedowns and notices**
  - Service providers are attractive to scammers due to a combination of low prices, high convenience and a slack attitude to abuse reports.
  - Contracted Parties can take affirmative steps to make their domains safer and more secure.
  - Some CPs are committed to a healthy domain name environment and a safe and secure namespace.

- Examples from regular gTLDs
  - **Donuts Trusted Notifier Program** => Voluntary agreements to facilitate notice and takedown of malicious domains
  - **Verified top level domains consortium** => processes and policies that preserve the integrity of their vTLDs (.bank; .insurance, .pharmacy) – verification of eligibility prior to use; adherence to standards; ongoing verification.
  - **PIR Quality Performance Index (QPI)** => Measure the quality of individual registrars = determine eligibility for marketing programs = incentivize good domain names: (1) Abuse score; (2) renewal rates; (3) domain name usage; (4) DNSSEC; and (5) SSL Certificate usage.
Webinar on DNS Abuse
ICANN66 Preparation Week
Summary: Abuse may not mean the same thing to everyone

Key Items

- Registrar activity is generally limited to DNS and excludes content
- Some registrars also offer additional services such as hosting or email which can be used for abusive purposes
- Presentation focused on abuse dealt with as a registrar (and later, registry)
- DNS Abuse comprises 5 general categories
  - Malware
  - Botnets
  - Phishing
  - Pharming
  - Spam (when used as delivery mechanism for above)
Registrars - Contractual Requirements

**Key Items**

- Registrar shall maintain abuse email and telephone number in RDDS (Whois Specification Section 1.4)
- Registrar shall provide abuse contact on website and take reasonable and prompt steps to investigate and respond appropriately to any reports of abuse (Section 3.18.1)
- Registrar must maintain dedicated law enforcement abuse contact 24/7, and review complaints within 24 hours (Section 3.18.2)
- Registrar must publish abuse handling process on website (Section 3.18.3)

**Key Concerns**

- “Respond” can mean “take action” or “reply” - so a registrar may not always send a response to an abuse complaint
- For invalid abuse complaints, a registrar may take no action
- “Law enforcement” refers to jurisdiction(s) of the registrar - not worldwide
- Published abuse email address likely to get a lot of spam, etc.
Registry Agreement Specification 11(3)(b)

“Registry Operator will periodically conduct a technical analysis to assess whether domains in the TLD are being used to perpetrate security threats, such as pharming, phishing, malware, and botnets. Registry Operator will maintain statistical reports on the number of security threats identified and the actions taken as a result of the periodic security checks. Registry Operator will maintain these reports for the term of the Agreement unless a shorter period is required by law or approved by ICANN, and will provide them to ICANN upon request.”

Requirements

• Technical analysis to identify potential security threats
• Maintain records of threats identified and actions taken
ICANN Advisory re: R A Spec 11 (3)(b)

• “[O]ffers one voluntary approach registry operators may adopt to perform such technical analyses to assess security threats and produce statistical reports as required by Spec 11 (3)(b).”

• Technical analysis: (1) reviewing data feeds; and/or (2) automated analyses that provide data equal to “Domain Reputation Service Providers” (RBLs).

• Analysis should be not less than monthly basis.

• Technical Analysis:
  o Consider use of one or more domain reputation service providers (RBLs) for a leading indication of potential problems.
  o Consider review of RR/RY transaction summaries (EPP and DNS) to identify potential problems.
Security Framework

Aim is to deliver on the ICANN Board's GAC:

“regarding ICANN soliciting community participation to develop a framework for how a Registry Operator (RO) may respond to identified security threats.”

• Voluntary framework developed over 2 years ago between PSWG and Registries
• Presents a registry response to Security Threats
• Notes a hierarchy of the severity of security threats, noting difference in quality in a report
  o Who is the reporter? (higher priority LEA/public safety agencies)
• ROs should provide prompt response and should within 24 hours communicate contemplated steps
• Notes that “ROs are not necessarily the best parties to address certain security threats”
Website Content Abuse

Website Content Abuse is generally outside the scope of Registrar and Registry agreements with ICANN.

- Registries and Registrars often cover certain forms of Website Content Abuse in their Acceptable Use Policies/Anti-Abuse Policies.

- Generally, things like Child Sexual Abuse Materials are prohibited and Registrars and Registries will act upon this at the DNS level.
  - Many AUPs are much more expansive.
Why Hosting Provider Before Registrar

**Key Items**

- Specific laws provide hosting providers with safe harbor provisions (e.g. DMCA, Electronic Commerce Directive).
- Registrar only has a nuclear option (suspend whole domain ... not specific content).
- Domain suspension not fully effective. Hosting content may remain available via IP and other domains.
- Hosting Provider has access to additional information that can indicate whether the website may have been compromised.
Proportionality / Collateral Damage

• Because of limited options, acting at the DNS level can have huge impact
• Acting on a domain for a piece of website content renders every other piece of content, subpage, information, email accounts for the whole domain inaccessible
• Example: Craigslist post
What can a Registry do?

**Existing Registrations**
1. Refer to registrar
2. Suspend the domain (e.g. apply ServerHold status)
3. Lock the domain so it can’t be changed
4. Redirect* the domain
5. Transfer* the domain
6. Delete

**Unregistered Domains***
1. Create and typically redirect (DGAs)
2. Block/reserve

* Typically for DGAs
Examples of Typical Registrar Actions

Key Items

• Attempt to confirm alleged abuse
• Determine what services are being provided (if more than registrar)
• Determine (if possible) if compromised
• Determine possible scale of abuse
• (As appropriate) Contact / work with customer to resolve
• (If needed) Request additional data from complainant
• Take appropriate action to disrupt abuse
• For IP abuse, registrars will comply with UDRP, URS procedures, and court orders, but are not competent to adjudicate disputes
Additional Registrar Best Practices

Key Items

• Provide Law Enforcement with a possible path to enact a takedown in advance of formal Legal Process when domain is shown to be part of criminal investigation in order to reduce additional harm.

• Facilitate direct communication between complainant and Registrant when appropriate.

• If abusive domain is confirmed and appears to be intentional abuse, Registrar may be able to find additional domain relating to the same Registrant / account.

• Support MFA and best current password and security practices on Registrant accounts to prevent hijacking, domain shadowing, etc. (See SAC074).

• Refer complainants to the most appropriate party to mitigate issue (Hosting Provider, etc.).
Common Issues in Abuse Investigations

- Not the most appropriate level to investigate / act
- Only have the “nuclear option” for removal
- Actions can cause collateral damage to legitimate parties / sites
- Abuse email overload
  - Delays
  - Filtering issues
  - Separating out the noise
- Lack of available evidence
- Sense of urgency differences
- Resourcing for unexpected volumes and threats
- “Potential Abuse”
Questions?