DNS TECHNICAL ABUSE : CHOICE OF ACTION

REF: 20-114 | November 2, 2020

Once technical abuse[1] has been identified, evaluated and confirmed, Domain Name System ("DNS") Operators must decide whether and how to act to address the abuse. While action at the DNS level may be appropriate to address certain types of technical abuse, DNS-level action has a major impact not only on the domain name, itself, but potentially on other activities linked to the domain name, such as email, name servers, databases and other services which are linked to the domain. DNS-level action to address alleged technical abuses must be therefore not only effective, but efficient and proportionate to the harm(s) alleged.

Malware and Phishing are technical abuses that can be delivered through websites or via email (in the form of spam). In such cases, acting on the attendant domain can be used to stop or interrupt its activity within the DNS. Conversely, pharming, while a form of technical abuse, cannot be remedied through DNS-level action by DNS Operators. Pharming involves the redirection of unknowing users to fraudulent sites or services, typically through DNS hijacking or poisoning. DNS hijacking occurs when attackers use malware to redirect victims to the attacker' site instead of the one initially requested. DNS poisoning causes a DNS server [or resolver] to respond with a false IP address bearing malicious code. These activities do not involve the use of domain name(s) to propagate abuse. Therefore, action at the DNS level is ineffective to address pharming. Signing domains with DNSSEC and enabling validation on resolvers is a systemic approach that can be effective in preventing pharming.

As noted below, the LOCK and HOLD commands are most often used in tandem to address malware and phishing, as, respectively, these commands appropriately prevent the resale or transfer of domains engaged in abuse and remove the domain name from the TLD zone file, thereby preventing the domain from resolving on the public internet. Conversely, as explained below, the Transfer, Redirect and Create commands are of limited use in stopping DNS abuse and are usually implemented by DNS operators only pursuant to formal requests from law enforcement or courts.

The charts below are based on Criteria F of the Operational Approaches document[2] and address respectively:

- HOLD and LOCK, most often indicated to remediate technical abuse
- REDIRECT and TRANSFER, generally used as additional measures upon specific requests.
- DELETE and CREATE, exceptional actions mainly used in the case of botnets and Domain Generation Algorithms (DGA's)

[1] For scope of technical abuse, Refer to Annex in Domains & Jurisdiction Program Outcome on DNS Operators' Decision-making Guide To Address Technical Abuse

[2] Domains & Jurisdiction Operational Approaches 2019

TYPE OF ACTION	APPLICABLE AGAINST	EFFECT OF ACTION
LOCK	*Malware, Phishing, Botnets, Fast Flux Hosting, Spam (as a delivery mechanism)*	Locking a domain name preserves the status quo in terms of ownership, contact information and server configuration. This can assist investigators and fact-finders (e.g. courts) in investigating alleged abuse. The Lock command also prevents the resale or transfer of domains involved in abuse to unsuspecting third parties. A locked domain cannot be transferred, deleted or have its details modified, but will still resolve through the DNS (i.e. enabling access to the attendant website(s) via the domain name).
HOLD/ SUSPENSION	*Malware, Phishing, Botnets, Fast Flux Hosting, Spam (as a delivery mechanism)*	The *Hold or Suspension command* removes the domain name from the TLD zone file and prevents it from resolving on the public internet (i.e. enabling access to the attendant website(s) or other services including emails or 3rd party domains linked via nameservers via the domain name). This helps prevent distribution of malware and exposure to phishing including its distribution via email. The Hold or Suspension action is the strongest action applicable to a domain name and can be used to address most technical abuse. It is important to note however, that the attendant website will still remain reachable, albeit only through its IP address.

The actions *Redirect* and *Transfer* **do not stop or impede ongoing technical abuse**. DNS Operators generally apply these commands only when compelled to do so by a formal request from law enforcement, a court order or other compulsory instruments.

TYPE OF ACTION	APPLICABLE AGAINST	EFFECT OF ACTION
REDIRECT	*Malware, Phishing, Botnets*	A DNS Operator 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 upon request for "sink-holing" (logging traffic), for instance to identify victims for the purposes of remediation.
TRANSFER	*Malware, Phishing, Botnets, Fast Flux Hosting, Spam (as a delivery mechanism)*	DNS Operators may be compelled to Transfer domain names without the registrant's consent in certain limited circumstances, for instance in order to prevent further abuse. This command effects a change in control (administration and ownership rights) of a domain to a third party to prevent exploitation, whilst allowing for management of lifecycle, EPP status codes, and expiration.

When a domain is deleted, it is removed from the TLD (Top Level Domain) zone file. As a result however, the domain becomes available again to be registered on a first-come, first-served basis.

REF: 20-114

This may potentially be done by the very registrant[3] who was using the domain to commit abuse. For this reason, the Delete command is generally not widely used to address abuse. The *Create* command may be also sparingly used for specific forms of technical abuse, such as botnets, but the use of this command raises very important and specific issues.[4]

TYPE OF ACTION	APPLICABLE AGAINST	EFFECT OF ACTION
DELETE	*Botnets*	Deleting a domain name is an extreme action and not generally recommended without careful due diligence and direction from the appropriate authorities. The *Delete* command may assist in interrupting a Botnet by interrupting the command and control path set by the Botnet's controllers. Deletion has a dramatic effect on the domain name holder and related services and cannot be undone in the circumstances when this choice of action is erroneously implemented. However, as noted above, the *Delete* command generally is not as effective at mitigating abuses as other actions such as *Hold* because the domain(s) can be quickly re-registered by a bad actor.
CREATE	*Botnets, Domain Generation Algorithms*	DNS Operators are sometimes asked to create and then redirect/sinkhole domains that are part of a predictive sequence of a Domain Generation Algorithm ("DGA"). DGAs are algorithms seen in various families of malware used to periodically generate a large number of domain names to be used as rendezvous points with their command and control servers. Once created, the actions *Hold, Redirect* or *Delete* might be used to interfere with the domain names pointing to the servers that form the botnet. In some cases, this may effectively hinder a botnet, as the infected machines require the path provided by the control domain names in order to "call home".

[3] In some instances, DNS Operators are required (by court order) to place deleted domain names "on reserve" so that they cannot be re-registered by the perpetrator(s) of abuse. However, DNS Operators who operate pursuant to contractual agreements with ICANN are generally contractually prohibited from placing domains on reserve, except in limited circumstances outside of abuse mitigation efforts. Likewise, certain ccTLD (country code Top Level Domains) may also be subject to restrictions or prohibition when placing domains on reserve.

[4] Criteria F in the Domains & Jurisdiction Operational Approaches does not include 'Create', but is included here due to its relevance to the topic. Create has however two important consequences in the ICANN environment: 1) It requires a contractual waiver for DNS Operators and 2) The newly created domains may entail the payment of a recurring fee.