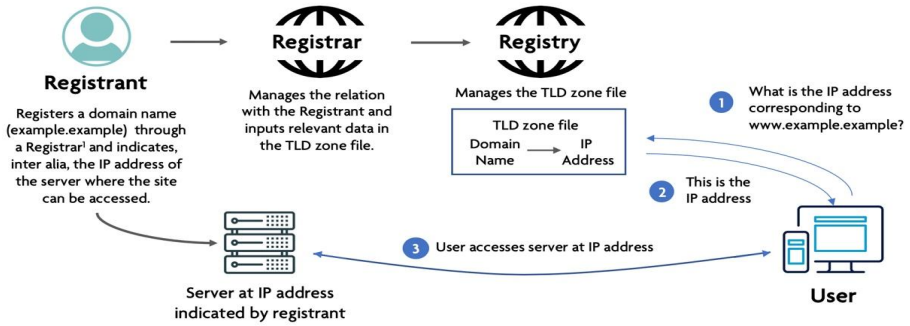
EFFECTS OF ACTIONS AT THE DNS LEVEL

REF: 20/301 | February 20, 2020

Action at the Domain Name System (DNS) layer is neither a fully effective way - nor should be considered as the natural tool - to address technical abuses or problematic content. Acting at the DNS level should only be considered when it can be reliably determined that the domain itself is used with a clear intent of significant abusive conduct. Furthermore, because the suspension of a domain has by definition a global impact, proportionality requires that only a particularly high level of abuse and/or harm can potentially justify resorting to such a measure.[1]

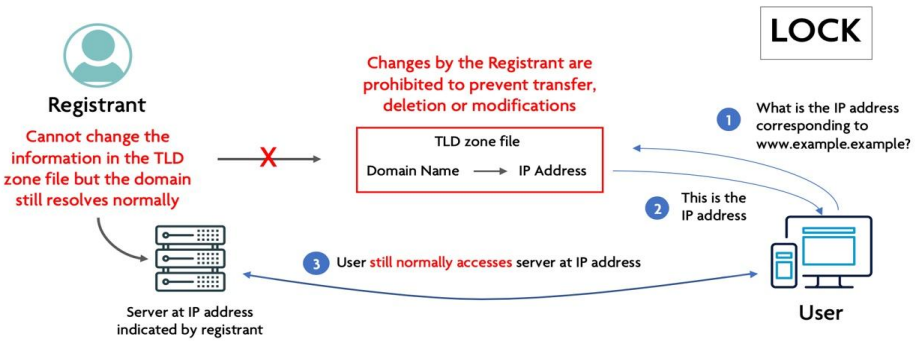
In any case, requests for action should be directed first to parties that are closest to the abusive activity, including by contractual relationship, in order to minimize impact on the functioning of the DNS. If attempts to reach the registrant or the hosting provider are unsuccessful, requestors should consider the different types of actions listed below that Registry operators (who manage the Top Level Domains ("TLDs")) and Registrars may take, as appropriate, in response to cross-border suspension requests. It is important that the functioning of the DNS and the impact of each specific action at DNS level are well understood.

The basic functioning of the Domain Name System



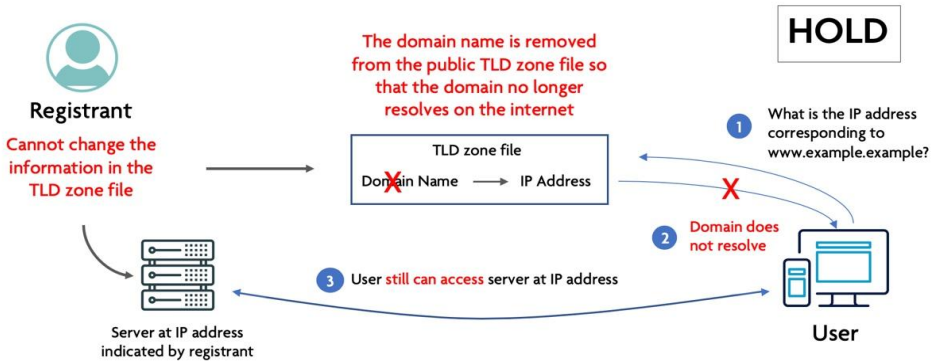
ACTIONS

ACTION 1: LOCK A locked domain cannot be transferred, deleted or have its details modified, but still resolves.

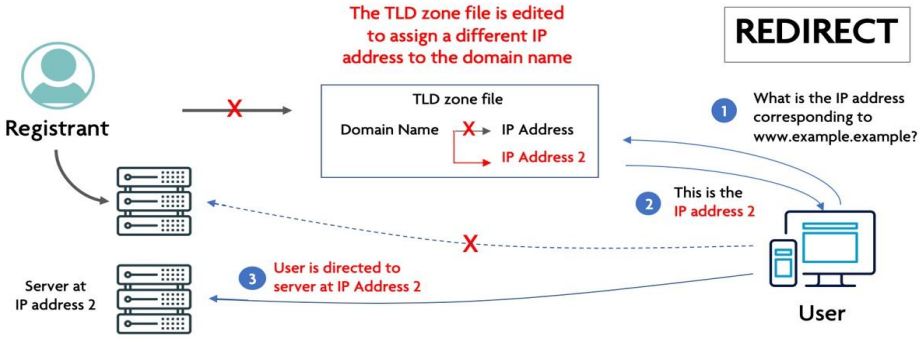


[1] This infographic details Criteria F of the Operational Approaches developed by the 2018-19 Domains & Jurisdiction Contact Group of the Internet & Jurisdiction Policy Network. The full document is accessible at: www.internetjurisdiction.net/operationalapproaches

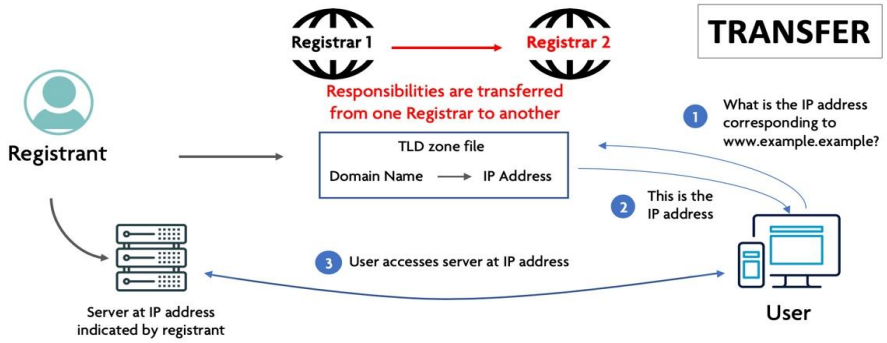
ACTION 2: HOLD This action removes the domain name from the TLD zone file, so the domain name will no longer resolve on the public internet. In the event that the request was made in error, this action may be reversed. Importantly, the site still remains accessible through the IP address.



ACTION 3: REDIRECT By changing the nameservers for the domain name, associated services can be redirected without consent of the registrant, for instance for "sink-holing" (logging traffic) to identify victims for the purposes of remediation.



ACTION 4: TRANSFER Transfer of the domain name to a qualified Registrar may prevent exploitation, whilst allowing for management of lifecycle, EPP status codes, and expiration.



ACTION 5: DELETION Deleting a domain name is an extreme action and **not generally recommended** without careful due diligence. Restoring the domain name would involve additional burdens absent when placing a domain name on hold. More importantly, **registrants are free to re-register the domain name** after it is purged from the zone.

REF: 20/301