

Guidance for Preparing Domain Name Orders, Seizures & Takedowns

Abstract

This “thought paper” offers guidance for anyone who prepares an order that seeks to seize or take down domain names. Its purpose is to help preparers of legal or regulatory actions understand what information top level domain name (TLD) registration providers such as registries and registrars will need to respond promptly and effectively to a legal or regulatory order or action. The paper explains how information about a domain name is managed and by whom. In particular, it explains that a seizure typically affects three operational elements of the Internet name system – domain name registration services, the domain name system (DNS) and WHOIS services – and encourages preparers of legal or regulatory actions to consider each when they prepare documentation for a court action.

Table of Contents

GUIDANCE FOR PREPARING DOMAIN NAME ORDERS, SEIZURES & TAKEDOWNS	1
PURPOSE OF THIS PAPER	2
WHAT INFORMATION SHOULD ACCOMPANY A LEGAL OR REGULATORY ORDER OR ACTION?.....	4
CHECKLIST OF INFORMATION TO SUBMIT WITH A LEGAL OR REGULATORY ACTION .	5
ADDITIONAL CONSIDERATIONS.....	12
CONTACT US.....	13
REFERENCES.....	16

Purpose of this paper

Recent legal actions resulting in disrupting or dismantling major criminal networks (Rustockⁱ, Corefloodⁱⁱ, Kelihosⁱⁱⁱ) have involved seizures of domain names, domain name system (DNS) name server reconfiguration, and transfers of domain name registrations as part of the take down actions. These activities have been taken to mitigate criminal activities and will likely continue to be elements of future anticrime efforts.

Generally, court-issued seizure warrants or restraining orders in the United States or similar governmental jurisdictions identify the required, immediate actions a party must take and accompany these with sufficient information for domain name registration providers such as registry operators or registrars to comply. Domain name registration providers can promptly obey complaints or legal or regulatory actions (or voluntarily cooperate with law enforcement agents and the private sector) when the instructions of the court or regulatory entity specify the immediate and long-term actions required as completely and unambiguously as possible.

Providing all of the information that registry operators or registrars need to comply with an order or request requires some familiarity with Internet protocols, technology and operations. Law enforcement agents, attorneys, officers of courts and others who are not familiar with the operation and interrelationship of domain name registration services, the domain name system (DNS), and WHOIS services can benefit from a reference list of questions and guidance for “answers” (information) that ideally would be made available when action is specified in a court order.

We offer a list of questions and encourage preparers to answer each when the legal or regulatory action seeks to seize or take down a domain name. For each question, a checklist or explanation of information that preparers should make available to registry operators or registrars is provided. Note that it may not necessarily be the case that all of the information identified in this list will be relevant for all types of seizure or take down actions.

The information discussed here is not exhaustive, nor are these questions prescriptive. However, the preparation and execution of actions or orders may be expedited if these details are considered during the preparation of a legal or regulatory action or during the onset of an incident involving the DNS, including domain name registrations.

The comments and recommendations made in here are based on experience with actions and orders that have been prepared and executed by U.S. courts. This is a lay document. Its authors and contributors are technical and operational staff, not attorneys [although persons with legal expertise were consulted in the preparation

of this document for publication]. We offer no legal advice here. Our purpose is to share “field experience” so that these can be taken into consideration for future actions and orders involving domain name seizures and take downs.

Domain name seizures are typically ordered in association with criminal acts. Preparers of orders should consider whether disputes concerning alleged abusive registrations of domain names (e.g., bad faith use, confusing similarity) may be handled through the Uniform Domain Name Dispute Resolution Policy and administrative procedure, found at [^{iv}].

ICANN Security Team

What information should accompany a legal or regulatory order or action?

Domain name registration is a multi-step process. An organization or individual that wants to use a domain name first checks availability of the string of characters in a given Top Level Domain (TLD), and if available, must register the domain name. ICANN accredited registrars process registrations for ICANN generic TLDs (gTLD). Country-specific TLDs (ccTLDs) are not under obligation to use ICANN accredited registrars and may use any registration provider or they may provide registration services directly.

A fee for a term of use is commonly paid to register a domain. Upon completing a domain name registration, the domain name is made active in the TLD registry, a registration record is created, and the Domain Name System is configured to allow name to Internet address resolution for the domain and services such as email or web. Often, several business entities coordinate to perform these actions on behalf of the registering party (the registrant) and to manage all the information associated with a domain throughout that domain's life cycle. Nearly all of this information may be relevant or essential to a successful execution of a legal or regulatory order or action.

Domain name registration providers such as registries or registrars require certain information to enable them to satisfy a court order or investigate a legal or regulatory action. As you prepare one of these documents, consider the following high-level questions:

- 1) Who is making the legal or regulatory action or issuing a request?

Examples: a court of law, a law enforcement agent/agency, a registry, a registrar, an attorney, or an intervener (e.g., a trusted or contracted agent of a complainant who has assisted in the technical or operational investigation of criminal activity).

- 2) What changes are required to the **registration** of the domain name(s) listed in the legal or regulatory order or action?

Individuals or organizations register and pay an annual fee to use a domain name. The individual or organization then becomes the *registrant on record* of the domain. Parties that perform domain name registrations as a service ("registrars" or "registries") collect contact, billing and other information from the registrant. A legal or regulatory action should describe if this information is to be altered, and how.

A domain name registration also identifies the *status* of the domain^v. Status indicates the operational state of a domain name in a registry, i.e., whether or not the domain name is active or not. Status also serves as an access control, i.e., whether or not the registration of a domain name can be transferred, modified, or deleted. A legal or regulatory order or action should specify the status a registrar or registry should assign to the domain name(s) listed in the legal or regulatory order or action. [Note that status also preserves the state of information associated with a domain name in services such as data escrow and registration data information services such as WHOIS].

In cases where the registration of a domain name is to be transferred away from a party named in a legal or regulatory action to law enforcement or an agent operating on behalf of law enforcement, the legal or regulatory action should provide the “replacement” domain name registration data as described in ICANN’s registrar accreditation agreement (RAA^{vi}).

- 3) Should the Domain Name System (DNS) continue to **resolve the domain name(s)** listed in the legal or regulatory action?

Provisions must be made in the DNS to make the name usable, i.e., to make it possible for Internet users to locate (determine the Internet address of) web, mail, or other services the registrant intends to host. The process of locating hosts using the DNS is called domain name resolution. The legal or regulatory action should indicate whether and how the DNS is to be configured, whether domain name(s) listed in the order or action are to resolve, and how.

- 4) What changes are required to the **WHOIS information** associated with the domain name(s) listed in the legal or regulatory action?

Certain information about a domain name registration – the registrant on record, point of contact information, domain status, sponsoring registrar, name server address – may be available via an Internet service called **WHOIS**. The legal or regulatory action should identify what information WHOIS services should provide in response to queries about domain name(s) identified in the legal or regulatory action.

Checklist of information to submit with a legal or regulatory action

Preparers of legal or regulatory actions are encouraged to consider whether the questions presented below have been answered in an order or action. For each question, there is an accompanying checklist or explanatory text to help preparers. The table considers a single domain. When legal or regulatory orders identify multiple domains, preparers can expedite handling of the order by grouping the domain names by Top Level Domain type (e.g., COM, NET, BIZ, INFO...).

<p>Who is making the request?</p>	<p><input type="checkbox"/> Complainant (plaintiff)</p> <p><input type="checkbox"/> Respondent (defendant)</p> <p><input type="checkbox"/> Court of Record</p>
<p>Who are the primary points of contact?</p>	<p>Contact information for court officers, attorneys, technical/operational staff or agents, line or senior management of parties to the legal or regulatory action:</p> <ul style="list-style-type: none"> • Name • Postal address • Telephone number(s) • Fax numbers(s) • Email address(es) <p>These prove beneficial should issues be identified that require a technical or operational action, legal consultation or business decisions; in particular, call attention to any person designated as the coordinator, lead or responsible party to the action.</p> <p><i>Important:</i> Issuers of requests are encouraged to provide some form of official, verifiable contact information. Recipients of a court order may require a method to verify the legitimacy of the issuer of the request. The inability to validate a request, especially when the request comes from a foreign law enforcement agency, court, or other entity can delay action by the recipient.</p> <p><i>Indicate whether any contact information provided is to be kept confidential.</i></p>

<p>What kind of request is this?</p>	<p>The request should clearly indicate whether this is a court order or request for action. For example,</p> <ul style="list-style-type: none"> <input type="checkbox"/> Court order (attached) or regulatory action <input type="checkbox"/> 3rd party request for action. Examples: <ul style="list-style-type: none"> <input type="checkbox"/> Algorithmically generated domain name HOLD request <input type="checkbox"/> Child abuse material <input type="checkbox"/> Copyright infringing materials <input type="checkbox"/> Malware Command & Control host <input type="checkbox"/> ... <p>Note: 3rd party requests should be accompanied by verifiable evidence supporting the third party request.</p>
<p>What is the expected response time?</p>	<ul style="list-style-type: none"> <input type="checkbox"/> Date and time by which the actions indicated in the legal or regulatory action must be executed. <p>Document should make clear when the actions must be executed. This is particularly important when multiple parties must coordinate execution so that their actions are “simultaneous”.</p>
<p>Is there a desire to obtain records related to the domain at the same time the domain is seized?</p>	<ul style="list-style-type: none"> <input type="checkbox"/> Records and documents sought <p>The legal or regulatory action should list and describe all forms of records sought and indicate the span of time. Make clear whether or not the request is part of the action.</p> <p>Important: The issuer should always seek to direct requests to the party who is in possession of the information sought, especially when preparing sealed orders. For generic TLDs, registrars typically possess billing information and other customer (registrant) information that cannot be accessed using WHOIS services (e.g., information associated with privacy protection services).</p>

<p>How is the domain name registration record to be changed?</p> <p>Note: Identify all the changes ordered or requested.</p>	<p><input type="checkbox"/> change domain name registrant</p> <p>The party identified as the domain name registrant is to be changed to the party specified in the complaint. The “gaining” party may be responsible for future registration fees.</p> <p><input type="checkbox"/> Change domain name registration point of contact information as specified</p> <p>The point of contact information recorded in the domain name registration is to be changed to the contact information specified in the complaint. The legal or regulatory action should indicate how each point of contact (registrant, administrative contact, technical contact) is to be altered.</p> <p><input type="checkbox"/> Disable DNSSEC</p> <p>DNS information that has been cryptographically protected with a digital signature will be altered so that is no longer protected</p> <p><input type="checkbox"/> Replace existing DNSSEC keys with new key(s) supplied</p> <p>DNS information that has been cryptographically protected with a digital signature will be altered so that is now protected using the key(s) supplied by the requesting entity.</p>
<p>How is domain name status to be changed?</p>	<p><input type="checkbox"/> prevent transfer of domain name</p> <p><input type="checkbox"/> prevent updates to domain name registration</p> <p><input type="checkbox"/> Delete domain name</p> <p>Deleting a domain name “releases” the name into the pool of names available for registration by any party.</p>

<p>Is the domain name to be transferred to a different sponsoring registrar?</p>	<p><input type="checkbox"/> Transfer domain to new registrar specified</p> <p>If the legal or regulatory action wants the domain name transferred from the current sponsoring registrar to a registrar identified in the order or action, the requesting entity should supply the “losing” registrar and the “gaining” registrar for this action. A unique authorization code (Auth-Code) may be required for this action. This is obtained from the losing registrar and provided to the gaining registrar as proof of consent to transfer the domain name.</p>
<p>Is the party that provides name resolution service (DNS) to be changed?</p>	<p><input type="checkbox"/> Change authority for DNS</p> <p>Authority identifies the party that is responsible for managing and providing DNS for a domain name. A legal or regulatory action should identify parties that will assume authority for name resolution of domain names listed in the document.</p> <p>This is a change to the DNS configuration of the registry (TLD) zone file. Specifically, the DNS records that identify the authoritative name server(s) for the domain name must be changed to point to IP address(es) under administrative control of the parties named in the legal or regulatory action (or request).</p> <p><input type="checkbox"/> Change DNS configuration of the domain</p> <p>This is a change to the DNS configuration of the zone file for the domain specified in the order or action. Requesting entities provide this information to registrars or 3rd party DNS providers. The requesting entity should provide current and desired values for all zone data (resource records, TTL values) that is to be changed.</p>

<p>Is name resolution service (DNS) to be suspended?</p>	<p><input type="checkbox"/> Suspend name resolution (DNS): “seize and take down”</p> <p>The legal or regulatory action should specify that domain name(s) should not resolve. In this case, the TLD registry operator will take action so that the DNS will return a non-existent domain response to any queries for any delegation in this domain.</p> <p>This action implies that the domain name is to be “locked”; i.e., that no party (e.g., registrar, registrant) can modify the status and cause the DNS to resume name resolution of the domain name).</p>
<p>Is redirection to a text of notice page required?</p>	<p><input type="checkbox"/> Redirect domain name to text of notice page: “seize and post notice”</p> <p>If the requesting entity intends to post a text of notice on a web page, the legal or regulatory action should provide the domain name(s) and IP address(es) for the name server that will perform name resolution for the domain names listed in the order or action. The legal or regulatory action should indicate the intended duration of time that redirection is to be performed.</p>

ICANN SECRET

<p>Is redirection of Internet hosting required?</p>	<p><input type="checkbox"/> Redirect to host operator: “seize and operate”</p> <p>If the legal or regulatory action seeks to replace an Internet host¹ with one that is operated under the requesting entity’s purview, provide the domain name(s) and IP address(es) for the name server that will perform name resolution for the domain names listed in the legal or regulatory action. In other situations, the requesting entity may seek to keep the name (and name resolution) operational. This can happen when a problematic service is operational on the same domain name that also serves non-problematic services. The legal or regulatory action should indicate the intended duration of time that redirection is to be performed.</p> <p>¹ The requesting entity may operate a “command and control (C&C)” for the purpose of monitoring or intercepting communications, substituting commands or responses or other actions to remotely disable or supervise software executing without authorization or consent on compromised computers. (Note that the requesting entity could operate any service it chooses. This will have no bearing on what information to provide to registries or registrars.</p>
<p>What should WHOIS for the domain name display?</p>	<p><input type="checkbox"/> WHOIS information display change</p> <p>The legal or regulatory action should specify the information that the registry or registrar should use in response to queries for domain name registration data via a WHOIS service (See Appendix A for an example WHOIS response).</p> <p><input type="checkbox"/> Reveal private/proxy registration</p> <p>Individuals or organizations that register domain names may pay a fee to a registrar or 3rd party to protect part or all of the information displayed via WHOIS services from display. A legal or regulatory action should indicate when it requires the disclosure of “privacy protected” registration information.</p>

Additional Considerations

The nature and complexity of domain name seizures and takedown operations has evolved over time. Moreover, as criminals have demonstrated that they will adapt to technical measures to thwart crime, they are likely to adapt as they study legal measures. This section calls attention to some of the issues that past seizures and takedown actions have exposed.

Legal or regulatory actions are typically specific with respect to the immediate obligation; for example, they will enumerate domain names, IP addresses, and equipment that are to be seized. A legal or regulatory action can be less clear with regard to how long an action is to remain ongoing, or can impose a constraint on a registry that creates an obstacle to satisfying the instructions in the order. Certain legal or regulatory actions identify domain names that are hosted in countries outside the U.S., where the offense is not against the law.

Certain legal or regulatory actions create long-term administrative responsibilities for registries; for example, if a botnet algorithmically generates domain names, a registry may need to block registrations of these names as frequently as the algorithm generates to comply with an order. The number of domain names identified in these orders can accumulate to (tens of) thousands over a span of 1-2 years (100 algorithmically generated domains per day reaches 10,000 in 3 months' time). Legal or regulatory actions do not always indicate how long seizure or hold actions are to persist. Domain seizures (holds) also demand "zero error": should any party in the chain fail to identify or block even one domain name, a botnet that was successfully contained for months can be resurrected.

Algorithmically generated domain names may also conflict with already registered domains. Registries would typically seek to protect a legitimate registrant that has the misfortune of having registered a second level label that is identical to one algorithmically generated, but if the court order seizes the domain, registries could note the conflict but ultimately would obey the order. Moreover, domain generation algorithms used in criminal activities may (are likely to) adapt to defeat blocking techniques; for example, blocking registrations may not be practical if an algorithm were to generate tens of thousands of domains per day.

Sealed court orders pose operational challenges to TLD registry operators who rely on registrars to manage registrant contact information. The order prohibits the registry to communicate with the registrar of record but the registry cannot modify the contact information unless the registrar of record is engaged.

Legal or regulatory actions may order registries, registrars, Internet (web or mail) hosting companies, and ISPs to take specified steps at a specified date and time.

Such steps require considerable coordination and preparers of legal or regulatory actions should consider how “lead” as well as “execution” time may affect outcome.

Orders can create administrative responsibilities for registrars as well (for example, inter-registrar transfers of seized domain name registrations).

Orders generally do not consider fee waivers, nor do they typically consider the ongoing financial obligation of the “gaining” registrant to pay annual domain registration fees.

Contact Us

Dave Piscitello, Senior Security Technologist at ICANN, prepared this thought paper, with the assistance of the ICANN Security Team. Information. Reviews and comments from Internet security, technical and operational community members were essential in preparing this initial paper, and the Security Team thanks all who contributed. We welcome additional comments. Please forward all comments by electronic mail to dave.piscitello@icann.org

Appendix A. Sample WHOIS response

This is a sample response to a WHOIS query. The data labels and display format varies across registries and registrars. Values for registration data elements in **BOLD** should be provided by the requesting entity.

Domain ID: D2347548-LROR
Domain Name: **ICANN.ORG**
 Created On: 4-Sep-1998 04:00:00 UTC
 Last Updated On: 10-Jan-2012 21:32:13 UTC
 Expiration Date: 07-Dec-2017 17:04:26 UTC
 Sponsoring Registrar: GoDaddy.com, Inc. (R91-LROR)
 Status: CLIENT DELETE PROHIBITED
 Status: CLIENT RENEW PROHIBITED
 Status: CLIENT TRANSFER PROHIBITED
 Status: CLIENT UPDATE PROHIBITED
 Status: DELETE PROHIBITED
 Status: RENEW PROHIBITED
 Status: TRANSFER PROHIBITED
 Status: UPDATE PROHIBITED
 Registrant ID: CR12376439
Registrant Name: **Domain Administrator**
Registrant Organization: ICANN
Registrant Street1: **4676 Admiralty Way #330**
Registrant City: **Marina del Rey**
Registrant State/Province: California
Registrant Postal Code: **90292**
Registrant Country: **US**
Registrant Phone: **+1.4242171313**
Registrant FAX: **+1.4242171313**
Registrant Email: **domain-admin@icann.org**
 Admin ID: CR12376441
Admin Name: **Domain Administrator**
Admin Organization: ICANN
Admin Street1: **676 Admiralty Way #330**
Admin City: **Marina del Rey**
Admin State/Province: California
Admin Postal Code: **90292**
Admin Country: **US**
Admin Phone: **+1.4242171313**
Admin FAX: **+1.4242171313**
Admin Email: **domain-admin@icann.org**
 Tech ID: CR12376440
Tech Name: **Domain Administrator**
Tech Organization: ICANN

Tech Street1: 4676 Admiralty Way #330
Tech City: Marina del Rey
Tech State/Province: California
Tech Postal Code: 90292
Tech Country: US
Tech Phone: +1.4242171313
Tech FAX: +1.4242171313
Tech Email: domain-admin@icann.org
Name Server: NS.ICANN.ORG
Name Server: A.IANA-SERVERS.NET
Name Server: B.IANA-SERVERS.NET
Name Server: C.IANA-SERVERS.NET
Name Server: D.IANA-SERVERS.NET
DNSSEC: Signed
DS Created 1: 26-Mar-2010 15:12:06 UTC
DS Key Tag 1: 41643
Algorithm 1: 7
Digest Type 1: 1
Digest 1: 93358db22e956a451eb5ae8d2ec39526ca6a87b9
DS Maximum Signature Life 1:1814400 seconds
DS Created 2: 26-Mar-2010 15:12:28 UTC
DS Key Tag 2: 41643
Algorithm 2: 7
Digest Type 2: 2
Digest
2:b8ab67d895e62087f0c5fc5a1a941c67a18e4b096f6c
622aefae30dd7b1ea199
DS Maximum Signature Life 2:1814400 seconds

References

- i Defeating Rustock in the Courts
http://www.microsoft.com/security/sir/story/default.aspx#!rustock_defeating
- ii “Coreflood” Temporary Restraining Order
http://www.fbi.gov/newhaven/press-releases/pdf/nh041311_5.pdf/at_download/file
- iii “Kelihos” ex parte temporary restraining order
<http://www.noticeofpleadings.com/images/FAC-EN.pdf>
- iv Uniform Dispute Resolution Policy and procedures
<http://www.icann.org/en/dndr/udrp/policy.htm>
- v EPP Status Codes: What do they mean and why should I know?
<http://www.icann.org/en/transfers/epp-status-codes-30jun11-en.pdf>
- vi ICANN Registrar Accreditation Agreement 21 May 2009
<http://www.icann.org/en/registrars/ra-agreement-21may09-en.htm>