The value of assessing collateral damage before requesting a domain seizure

David Piscitello, on behalf of the ICANN Security Team

In our Thought Paper on Domain Seizures and Takedowns, we offer guidance to anyone who prepares an order that seeks to seize or take down domain names. By offering this guidance, we do not endorse such actions as a prescriptive measure, nor do we consider seizures or takedowns the appropriate remedy for every misuse or abuse. We only acknowledge that actions of these kinds have and will continue to be taken to combat criminal or abusive use of the DNS, and given this, we lend guidance to preparers so that orders they issue can be met expeditiously *and* with as little collateral harm as possible.

We are keenly aware that seizures or takedowns can have unintended consequences. Incidents involving Jotform.com and Mooo.com serve as noteworthy examples:

Jotform.com. On 15 February 2012, a domain name registrar suspended name service for Jotform.com, an online forum for web forms creation and sharing. Jotform claims it did not receive notice of a court order but was informed by the registrar that the site had been suspended as part of an ongoing investigation. The investigation of a single user account caused a service interruption for the entire Jotform.com community, estimated at over 100,000 users. Jotform's users not only create but host forms at Jotform's site. Other third party services that relied on forms hosted at Jotform could not operate as intended.

Mooo.com. A US government agency seeking to seize domains associated with counterfeit goods and child abuse material seized multiple domain names and ordered registry operators to redirect name service to a notice of seizure web page. Mooo.com, a dynamic domain name-sharing project, was named in the order. Name service was suspended for over 84,000 "subdomain" websites using mooo.com's services (e.g., example.mooo.com) that were not involved in counterfeiting or hosting child abuse material; further, visitors to these sites were redirected to a notice of seizure page identifying the site as having been seized for hosting child pornography.

Checklist of information to submit with a legal action

Domain name registration providers 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 action or issuing a request?
2) What changes are required to the **registration** of the domain name(s) listed in the legal or regulatory order or action?
3) Should the Domain Name System (DNS) continue to **resolve the domain name(s)** listed in the legal action?
4) What changes are required to the Domain Name Registration Data **(WHOIS) information** associated with the domain name(s) listed in the legal or regulatory action?

For more information see Guidance for Preparing Domain Name Orders, Seizures & Takedowns

In these cases, the seizure caused harm to website operators or entire communities who depend on multi-user sites. We are also concerned that, where possible, actions taken by one investigator or team should avoid interfering with redirection or surveillance by other investigators. Operation b71 is a case on point: a private corporation seized domain names allegedly affiliated with the notorious ZeuS botnet crime ring. Security companies or nongovernment organizations had registered a number of the seized domain names for traffic monitoring and analysis ("sinkholing"). As a consequence of the seizures, these investigators lost some of their intelligence feeds; further, the orders incorrectly associated the investigators with criminal activities.

To minimize unintended consequences of these kinds, we recommend that investigators assess the potential for collateral damage when requesting a seizure or takedown, and ask that you consider the following as you prepare an order.

Name Resolution Considerations

Upon completing a domain name registration, a 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. If you intend to request that a registrar or registry operator cease domain name resolution in an order, bear in mind that domain names are used for purposes other than naming websites. Before you make this request,

Check whether your action will disrupt name service for other reputable domains. It is common for a domain registrant to deploy a name server that is assigned a host name from a different or *out of bailiwick* domain; for example, a registrant may assign a host name of `ns1.example.net` to the name server of a domain `example.com`. More importantly, potentially many registrants may host name service at `ns1.example.net`. Ceasing name resolution for `example.net` will cause `ns1.example.net` to stop resolving and thus may also affect name service of one or thousands of domains also employing `ns1.example.net` as their name server. Passive DNS can often assist investigators in identifying name server dependencies (both legitimate and criminal). In circumstances where your action will disrupt name service for legitimate domains, consider whether it is appropriate or possible to (temporarily) support name resolution for reputable domains (i.e., domains not listed in your order, as was the case for DNSChanger).

Check whether your action will disrupt hosting services for parties other than those named in your order. Suspending name resolution for a domain will affect all users who host web or other types of accounts on hosts assigned names in domains you seize or take down. Note that in cases like the aforementioned Jotform, users may depend on scripts, web services, or content

that may be exclusively hosted on a hosting site affected by your order and will not have access to these once the domain is suspended. Consider whether it is appropriate or possible to (temporarily) support hosting service for any reputable domains.

Check what services other than web are affected. Some actions may seek the removal of content published on the World Wide Web or file sharing. For example, while the specific target for your action may be illicit content hosted at `www.example.com`, it is possible that legitimate email service is being hosted at `mail.example.com`. While suspending name resolution for `example.com` will accomplish the objective of preventing access to the web content, this action will also disrupt (in this case) email but more generally any other services hosted at this domain for potentially large user populations. Use DNS zone query tools (dig, nslookup) to check the zone files of domains in the order for resource records that may indicate the domain supports services other than those you seek to suspend. For example, to determine whether the domain is hosting mail services you can use `dig <domain name> MX`. If your dig or nslookup queries reveal services other than web, consider investigating what affect or harm you will cause to users that rely on these potentially legitimate services.

Check whether reputable naming services such as URL shorteners are affected. Familiarity with popular URL shortening services like bit.ly, TinyURL or goo.gl is commonplace; however, many organizations or website owners offer custom, vanity, or private label link shortening abilities. Suspending name resolution for a domain that is used for reputable URL shortening of this kind potentially affects thousands of links, sites, and users. Investigators can consult lists maintained by any of several organizations that attempt to enumerate these shorteners, e.g. VanityURLshorteners.com.

Check for interference. Without disclosing your action beyond a comfortable web of trust, attempt (to the extent possible) to make certain that your action will not adversely affect other active investigations, monitoring, sinkholing, or other surveillance.

Domain Name Registration (Whois) Considerations

Your order may request the registry operator or registrar to modify the registration record (Whois) of a domain name, or transfer ownership of the domain from the current owner of record to you or a party you identify. When making such requests, consider:

Check for interference. To the best of your ability (i.e., without disclosing your action beyond a comfortable web of trust), are you certain that a transfer or change in registration data will not adversely affect other active investigations or surveillance?

What action do you expect the criminal to take in response? Are you giving notice to the criminal that this registration information has been revealed as fraudulent and thus providing an opportunity to modify data that identifies him in other attack contexts; for example, a spammer who is running multiple spam campaigns but using the same registration data across all malicious registrations may take notice of the change and in response, modify Whois for domains you have not included in the order. (This may be unavoidable but it may affect other investigations.)

Domain Name Registry Considerations

Your order may request the registry operator to delete a domain from its registry database. This action is rare. When making such requests, consider:

What expectation do you have that the domain name will not be registered again? Restoring the domain name to the pool of available names creates an opportunity for a criminal to register the name again. The alternative is to transfer the registration to your organization or agency, or to authorize a party in your order to assume transfer of the registration.

What action do you expect a registry operator to take if the request involves a domain that is not yet registered? Criminals may use algorithmically generated domain names (DGAs) to support botnets or other criminal activities. Such names may be generated at regular intervals. In the Conficker case, registry operators collaborated with security researchers to identify algorithmically generated domain names in advance so that attempts to register any of the names could be blocked. Identify and work closely with all registry, registrar, and security researchers to coordinate activities of this scale and complexity.

What action do you expect the criminal(s) to take in response? While it is not possible to know exactly how criminals will respond when you have disrupted a criminal enterprise, discuss scenarios involving retaliation (e.g., DDOS attacks) or changes of tactics (e.g., an increase of algorithmically generated names generated daily and expansion of the registries targeted, as was the case with Conficker) with trusted parties.

Closing Remarks

All parties involved combatting Internet crime have vested interests in seeking the most effective outcomes. Where misuse or abuse of the DNS, we are keenly interested in minimizing collateral harm as well. Not all of these checks may affect the actions you request in an order or the information you submit, but assessing how you will manage the consequences of these actions could mean the difference between having a popular and successful outcome or an adverse one.

Appendix

Conficker – an Internet worm that compromises computer systems that operate Microsoft Windows and uses these computers to form a criminal attack network

DGA, domain generation algorithm – a method criminals use to create lists of domain names that a criminal botnets can use to contact a supervisory system (known as command and control or rendezvous systems)

DNS – domain name system, a distributed system that provides mappings between user friendly names and Internet addresses

DNSchanger – a Trojan horse malware that modifies DNS server settings on the computer system it infects

Jotform (jotform.com)- a multi-user web developer collaboration site whose domain name was suspended February 2012, interrupting service for all users.

Mooo.com - a dynamic domain name-sharing project whose name resolution service was suspended February 2011, disrupting web service for 84,000 site operators.

Operation b71 – name of a global action by Microsoft Corporation, FS-ISAC, and NACHA taken to dismantle a ZeuS criminal enterprise

Passive DNS – a technique used to identify DNS server query and response traffic

Sinkholing – a technique used to disrupt communications between infected computers ("bots") and the systems (command and control or C&C) that criminals use to remotely control them

URL shortener – a service or program that algorithmically converts a long universal resource locator (URL) into a shorter one, commonly used to save character space in text messaging services

Whois – a service that provides information associated with registered domain names

ZeuS, ZeuS Botnet – a Trojan horse malware used to infect and operate criminal networks of computers ("botnet") used to attack financial institutions