Software Engineering Institute
Carnegie Mellon University

Finding Site Contacts

CERT Division

http://www.sei.cmu.edu

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by Carnegie Mellon University or its Software Engineering Institute.

This report was prepared for the

SEI Administrative Agent
AFLCMC/AZS
5 Eglin Street
Hanscom AFB, MA 01731-2100

DM17-0052

Table of Contents

1 Introduction

The ability to contact sites is an important step in responding to computer security incidents. It allows you to exchange information about security incidents, better understand intruder activity, become aware of potential vulnerabilities, and improve security at your site. Contacting a site may also help them become aware of a previously unknown security incident and respond appropriately. Ultimately, contacting sites to discuss security incidents helps to improve computer security for the entire Internet community.

This document describes contact methods, converting between domain names and IP numbers, finding contact information based on domain names, and finding contact information based on IP numbers.

2 Methods of Contacting Internet Sites

Site point of contact information is usually available in the form of an email address, telephone number, or FAX number. There are advantages and disadvantages to using each method in the context of a security incident.

1. Contacting a site using email

Email communication has several advantages, such as:

- providing a ready means of communicating electronically- stored information, such as log files
- enabling you to share information with multiple contacts
- allowing a site to analyze information received and respond at their own rate
- offering more controlled, clear messages than other forms of communication

When you send email to a site involved in a security incident, take care to ensure the communication is secure in that it reaches the intended site contact. If the target host is compromised, there is a possibility that an intruder will intercept the email communications you send and they will not reach the site contact.

Section C of this document describes several ways to find site point of contact information using publicly-accessible information on the Internet. Email contact information for a site is only accurate if it is regularly updated and maintained by the site. Unfortunately, the email contact information you find on the Internet is sometimes out-of-date or inaccurate.

Standard mailboxes can be used when the site email contact information listed in public databases is invalid. Many Internet sites employ the use of several standard and de facto email addresses. RFC 2142, "Mailbox Names for Common Services, Roles, and Functions", specifies a basic set of mailbox names which sites on the Internet are encouraged to support. RFC 2142 is available at:

http://info.internet.isi.edu/in-notes/rfc/files/rfc2142.txt

Basic mailbox names commonly used for security communication include:

```
security      - Security incident reporting mailbox
abuse         - Network abuse reporting mailbox
root          - The administrative user for a UNIX host
postmaster    - The administrator in charge of e-mail
```

E-mail is addressed using the mailbox name and the site's domain name, or sometimes the hostname, as follows:

```
To: security@domain.name
To: abuse@domain.name
To: root@domain.name
```

```
To: postmaster@domain.name
To: security@host.domain.name
To: abuse@host.domain.name
To: root@host.domain.name
To: postmaster@host.domain.name
```

Because the availability and functional state of standard mailbox names is not a widely reliable means of reaching a site contact, standard mailboxes should only be used as a last resort in the absence of valid publicly available contact information.

2. Contacting a site using the telephone

Telephone communication has the advantage of being a more immediate form of communication than email and is useful for dialogues. If you need to speak with the administrator of a compromised site, telephone communication is less likely to be intercepted by an intruder. This makes it a good way to initiate contact with a site for highly sensitive or critical issues. You can then establish secure email communication to share information.

Telephone communication has disadvantages, including:

- time zone differences between sites may make telephone contact difficult
- differences in language abilities may exist
- the call may catch a site off-guard causing the site contact to be defensive or unwilling to talk

Similar to email contact information, site telephone contact information is only accurate if the site maintains and updates it. Unfortunately, publicly-available telephone information is sometimes out-of-date or inaccurate.

3. Contacting a site using a FAX machine

FAX communication is typically insecure as an initial form of contact because a FAX machine in a typical office is not private and because a FAX may not reach the appropriate site contact. We do not recommend that you use a FAX machine to initially contact a site; use it to contact a site only when the other methods have failed.

Once you have used email or the telephone to initiate contact with a site, you can use a FAX machine to exchange documented information effectively and with a certain degree of security. Using a FAX machine to transmit communication after you make telephone contact is useful when the privacy of email communication is suspect due to a compromised host.

FAX contact information is only accurate if the site keeps it up-to-date. If you can avoid it, don't use a FAX for initial contact; however if could be useful to ask the site contact for his or her FAX number and use it to exchange information during subsequent communication.

3 Domain names and IP numbers

You can often locate site point of contact information using publicly-available databases maintained by Internet registry organizations.

The key information you need to find contact information for a site are its domain name and/or the IP number of a host on the site's network. In the context of a security incident, the attacked host's log files typically provide an IP number or a domain name in association with logged events.

After you know a domain name or an IP number, you can use the Domain Name System (DNS) to convert from a domain name to an IP number, or from an IP number to a domain name.

It is important to note that the information in the Domain Name System is dynamic. Converting between IP numbers and domain names after an incident has occurred may yield different results than you would obtain before or during the incident. Factors influencing the dynamic nature of the DNS include changes made by an intruder, normal changes made by a network or system administrator, or changes made in response to an incident.

Refer to Appendix B of this document for more information about problems when converting between IP numbers and domain names.

1. Converting from a domain name to an IP number

Given a domain name or host name you can derive the IP number using a DNS query tool such as 'nslookup', which is a common tool available on many UNIX hosts. Other operating system platforms may have similar tools for querying DNS information. For example, the Windows NT 4.0 operating system includes an 'nslookup' command which can be used from a command prompt window in a fashion similar to UNIX versions of 'nslookup'. In general, DNS query tools are available for most popular operating systems.

Below are examples of converting from domain name to IP number. These examples use nslookup in a UNIX environment.

Example 1:

Given the domain name "example.com", convert the domain name into an IP number.

```
$ nslookup example.com
Server:  localhost
Address:  127.0.0.1
Name:    example.com
Address:  10.125.214.12
```

The IP number associated with the name "example.com" in this example is 10.125.214.12.

Example 2:

Given the fully qualified domain name "somehost.example.com", convert the domain name into an IP number.

```
$ nslookup somehost.example.com
Server:  localhost
Address:  127.0.0.1
Name:    somehost.example.com
Address:  10.125.214.13
```

The IP number associated with the name "somehost.example.com" in this example is 10.125.214.13.

2. Converting from an IP number to a domain name

Likewise, given an IP number, the 'nslookup' tool can be used to convert the IP number into a domain name.

Example 1:

Given the IP number "10.125.214.12", convert the IP number into a domain name.

```
$ nslookup 10.125.214.12
Server:  localhost
Address:  127.0.0.1
Name:    example.com
Address:  10.125.214.12
```

The domain name in this example is example.com.

Example 2 :

Given the IP number "10.125.214.13", convert the IP number into a domain name.

```
$ nslookup 10.125.214.13
Server:  localhost
Address:  127.0.0.1
Name:    somehost.example.com
Address:  10.125.214.13
```

The fully qualified domain name in this example is somehost.example.com. For the purposes of finding point of contact information, the fully qualified domain name is shortened to the second-level domain name, which is example.com in this case.

4 Finding a point of contact using a domain name

Several methods are available on the Internet to locate site contact information based on a domain name. Four common methods are discussed below.

1. Contacting incident response teams

There are a number of security incident response teams located in different states, regions, and countries which serve defined constituencies. For sites that are within the defined constituency of an incident response team, we recommend that you contact the response team representing that constituency rather than contacting a site directly. The response team can then provide direct assistance where needed.

The Forum of Incident Response and Security Teams (FIRST) is a coalition of incident response teams around the world. Please refer to the FIRST web site for a list of incident response teams, their constituencies, and appropriate contact information.

http://www.first.org/team-info/

2. Using Whois

Whois is a common directory service provided by registry entities. A registry is an organization which is responsible for the allocation of domain names and/or IP numbers. A registry may also be referred to as a registrar or a network information center (NIC). The Whois databases provided by registries typically contain, among other things, point of contact information for domain names registered with that particular registry.

The CERT/CC maintains a list of pointers to known registry databases for top-level domains, including known Whois server names for use with local whois clients, URL's for web-based query forms, and in some cases, an email address to obtain contact information from the registry. Please see Appendix A of this document for more information.

The general syntax for using a local whois client is :

```
$ whois -h whois.server.name domain.name
```

Example:

Given the domain name "EXAMPLE.CA", query the Canadian registry Whois database to locate contact information:

```
$ whois -h whois.cdnnet.ca example.ca
Subdomain:      example.ca
Date-Received:  1998/11/24
Date-Approved:  1998/12/01
Organization:   Example Construction Inc
Type:           For-Profit Corporation
```

```
Description:    Construction company
Admin-Name:     Jane Q. Admin
Admin-Title:    Owner
Admin-Postal:   Example Construction Inc
                123 Example Rd Industrial Park
                P.O.Box 9876
                Exampleplace NB
                E2L3V9
Admin-Phone:    +1 555-123-1234
Admin-Fax:      +1 555-123-9876
Admin-Mailbox:  jane@example.ca
Tech-Name:      ExampleISP Domain Name Registrar
Tech-Title:     ExampleISP Domain Name Registrar
Tech-Postal:    ExampleISP Inc
                One ExampleISP Parkway
                Exampleplace, N.B.
                E2L3V9
Tech-Phone:     +1 (555) 987-6543
Tech-Fax:       +1 (555) 987-1234
Tech-Mailbox:   hostmaster@exampleisp.ca
NS1-Hostname:   ns1.exampleisp.ca
NS2-Hostname:   ns2.exampleisp.ca
```

Using this information, you can contact the site via email or telephone.

Contact information for many top-level domains can be located at a single registry Whois database serving the top-level domain. The top-level domains .COM, .ORG, and .NET are notable exceptions that are served by multiple registrars and a single shared registry. Domain names in .COM, .ORG, and .NET can be registered with any one of a number of registrars. It is up to each registrar to provide contact information for the domains served by the particular registrar.

In order to obtain contact information for a domain name in .COM, .ORG, or .NET, you must first determine the proper registrar to query for information. Whois can be used to query the shared registry Whois database to determine the proper registrar.

Example:

Given the domain name "EXAMPLE.COM", query the shared registry Whois database to determine the proper registrar.

```
$ whois -h whois.internic.net example.com
Whois Server Version 1.1
   Domain Name: EXAMPLE.COM
   Registrar: NETWORK SOLUTIONS, INC.
   Whois Server: whois.networksolutions.com
   Referral URL: www.networksolutions.com
   Name Server: NS1.EXAMPLE.COM (10.128.9.32 )
   Name Server: NS2.EXAMPLE.COM (10.128.9.128 )
   Updated Date: 14-jun-1999
```

Using this information, we can determine that the proper registrar Whois database to query for "EXAMPLE.COM" is whois.networksolutions.com.

```
$ whois -h whois.networksolutions.com example.com
Registrant:
Example Internet Site, Inc. (EXAMPLE2-DOM)
   1234 Noname Blvd., Suite 987
   Exampleburgh, PA 10000-1111
   Domain Name: EXAMPLE.COM
   Administrative Contact, Technical Contact, Zone Contact:
      Example.com NOC noc@example.com
      (311) 555-1111
   Record last updated on 03-Nov-98.
   Record created on 31-Aug-95.
   Database last updated on 9-Nov-98 04:37:06 EST.

   Domain servers in listed order:
   NS1.EXAMPLE.COM              10.128.9.32
   NS2.EXAMPLE.COM              10.128.9.128
```

Using this information, you can contact the site via email or telephone.

3. Using the DNS SOA record

Each domain name in the Domain Name System has a resource record called the Start of Authority Record, or SOA. The SOA record includes a field for the email address of the point of contact for the domain name. The DNS tool 'nslookup' can be used in interactive mode to query the DNS for SOA records.

Example:

```
$ nslookup
Default Server:  localhost
Address:  127.0.0.1
> set query=soa
> example.com
Server:  localhost
Address:  127.0.0.1
example.com
        origin = NS1.EXAMPLE.COM
        mail addr = noc.example.com
        serial = 950301
        refresh = 43200 (12H)
        retry   = 3600 (1H)
        expire  = 1209600 (2W)
        minimum ttl = 86400 (1D)
example.com     nameserver = NS1.EXAMPLE.COM
example.com     nameserver = NS2.EXAMPLE.COM
NS1.EXAMPLE.COM internet address = 10.128.9.32
NS2.EXAMPLE.COM internet address = 10.128.9.128
```

The email address specified in the example SOA record is notated using the format "mailbox.domain.name". So, the point of contact for the domain name EXAMPLE.COM, according to the SOA record in the example, is noc@example.com.

4. Using traceroute to find the upstream Internet service Provider

In the absence of secure contact information for a site, sometimes you can contact the site's upstream Internet service provider, which may be able to provide assistance with security incidents involving their downstream sites.

Tools such as 'traceroute' can be used to identify the network path to a site, from which the site's upstream Internet service provider can be identified. The 'traceroute' tool is available on many UNIX platforms. Variations of 'traceroute' are generally available on other operating systems, such as most Windows 95/98/NT systems which include a command prompt tool called 'tracert' which is similar in function to 'traceroute'. Because 'traceroute' can trigger other sites's intrusion detection systems, we recommend you only use 'traceroute' if you have no other method of obtaining secure contact information for a site.

The following is an example of how to use the UNIX 'traceroute' to identify a site's upstream Internet service provider. The domain names and IP numbers used are non-functional examples.

Example:

Assume we have a hostname of host3.example-site.edu and wish to identify the upstream provider for this site.

```
$ traceroute host3.example-site.edu
traceroute to host3.example-site.edu (10.72.0.176), 30 hops max
1 hop1.reporting-site.com (10.112.1.2) 2 ms 2 ms 1 ms
2 hop2.transit-network.net (10.288.114.254) 2 ms 2 ms 2 ms
3 hop3.transit-network.net (10.224.137.21) 3 ms 3 ms 5 ms
4 hop4.transit-network.net (10.224.46.74) 4 ms 2 ms 3 ms
5 hop5.transit-network.net (10.224.46.93) 18 ms 20 ms 21 ms
6 hop6.transit-network.net (10.224.46.5) 26 ms 21 ms 27 ms
7 hop7.example-upstream.net (10.224.32.30) 19 ms 16 ms 16 ms
8 hop8.example-upstream.net (10.4.1.122) 25 ms 24 ms 24 ms
9 hop9.example-upstream.net (10.4.1.202) 24 ms 25 ms 26 ms
10 hop10.example-site.edu (10.192.33.3) 24 ms 26 ms 26 ms
11 hop11.example-site.edu (10.72.0.11) 27 ms 25 ms 27 ms
12 host3.example-site.edu (10.72.0.176) 26 ms 27 ms 26 ms
```

The last host in the traceroute appearing before any host in the EXAMPLE-SITE.EDU domain is in the EXAMPLE-UPSTREAM.NET domain. Locating site contact information for EXAMPLE-UPSTREAM.NET would involve a query to the appropriate Whois database, as discussed in section C.2. For example:

```
$ whois -h whois.internic.net example-upstream.net
Whois Server Version 1.1
   Domain Name: EXAMPLE-UPSTREAM.NET
   Registrar: NETWORK SOLUTIONS, INC.
   Whois Server: whois.networksolutions.com
   Referral URL: www.networksolutions.com
   Name Server: NS1.EXAMPLE-UPSTREAM.NET (10.4.100.12 )
   Name Server: NS2.EXAMPLE-UPSTREAM.NET (10.5.154.9 )
   Updated Date: 13-oct-1998
$ whois -h whois.networksolutions.com example-upstream.net
Example Internet, Inc. (EXAMPLE-UPSTREAM-DOM)
   4422 Boogy Boogy Ave.
   Exampleburgh, PA 15555
   Domain Name: EXAMPLE-UPSTREAM.NET
   Administrative Contact, Technical Contact, Zone Contact:
   Network Operations Center, Example Internet (EXI)
   noc@example-upstream.net  (311) 555-1111
   Record last updated on 13-Oct-98.
   Record created on 02-Dec-95.
   Database last updated on 13-Oct-98 03:50:14 EDT.
   Domain servers in listed order:
   NS1.EXAMPLE-UPSTREAM.NET     10.4.100.12
   NS2.EXAMPLE-UPSTREAM.NET     10.5.154.9
```

5 Finding a point of contact using an IP number

Several methods are available on the Internet to locate site contact information based on an IP number. Three common method are discussed below.

1. Using Whois

Like domain names, Whois directory service databases are also used by IP number registries to provide, among other things, point of contact information for IP numbers allocated by the particular registry.

The CERT/CC maintains a list of pointers to known registry databases for IP number registries, including known Whois server names and URL's for web-based query forms. Please see Appendix A of this document for more information.

This document covers the use of a local whois client to perform registry database queries against Whois servers.

The general syntax for using a whois client is:

```
$ whois -h whois.server.name X.X.X.X
```

where X.X.X.X is the IP number being queried.

Example:

Given the IP number 10.128.9.32, query the ARIN Whois database for contact information.

```
$ whois -h whois.arin.net 10.128.9.32
Example Internet Site, Inc. (NET-EXAMPLE-NET)
   1234 Noname Blvd., Suite 987
   Exampleburgh, PA 10000-1111
   Netname: EXAMPLE-NET
   Netnumber: 10.128.9.0
Coordinator:
   Example.com (EXNOC)  noc@example.com
   (311) 555-1111
   Domain System inverse mapping provided by:
   NS1.EXAMPLE.COM              10.128.9.32
   NS2.EXAMPLE.COM              10.128.9.128
   Record last updated on 26-Oct-94.
   Database last updated on 13-May-98 16:09:10 EDT.
```

Using this information, you can contact the site via email or telephone.

2. Using the DNS SOA record

IP numbers are usually mapped to domain names in the DNS using resource records known as PTR records. IP number mappings are located in the IN-ADDR.ARPA domain, and are listed with the IP number represented in reverse order. Each PTR record in the DNS is tied to a Start of Authority, or SOA, record which includes a field for the email address of the point of contact for the IP number. The DNS tool 'nslookup' can be used in interactive mode to query the DNS for SOA records.

Example:

Given an IP number of 10.128.9.32, query the DNS to find the email point of contact for the IP number.

```
$ nslookup
Default Server:  localhost
Address:  127.0.0.1
> set query=soa
> 32.9.128.10.in-addr.arpa
Server:  localhost
Address:  127.0.0.1
9.128.10.in-addr.arpa
origin = example.com
mail addr = noc.example.com
serial = 97112514
refresh = 3600 (1H)
retry   = 900 (15M)
expire  = 86400 (1D)
minimum ttl = 86400 (1D)
```

The email address specified in the example SOA record is notated using the format "mailbox.domain.name". So, the point of contact for the IP number 10.128.9.32, according to the SOA record in the example, is noc@example.com.

3. Using traceroute to find the upstream Internet Service Provider

In the absence of secure contact information for a site, sometimes you can contact the site's upstream Internet service provider, which should be able to provide assistance with security incidents involving their downstream sites.

Tools such as 'traceroute' can be used to identify the network path to a site, from which the site's upstream Internet service provider can be identified. The 'traceroute' tool is available on many UNIX platforms. Variations of 'traceroute' are generally available on other operating systems, such as most Windows 95/98/NT systems which include a command prompt tool called 'tracert' which is similar in function to 'traceroute'. Because 'traceroute' can trigger other sites's intrusion detection systems, we recommend you only use 'traceroute' if you have no other method of obtaining secure contact information for a site.

The following is an example of how to use the UNIX 'traceroute' to identify a site's upstream Internet service provider. The domain names and IP numbers used are non-functional examples.

Example:

Assume we have an IP number of 10.72.0.176 and wish to identify the upstream provider for this site.

```
$ traceroute 10.72.0.176
traceroute to host3.example-site.edu (10.72.0.176), 30 hops max
1 hop1.reporting-site.com (10.112.1.2) 2 ms 2 ms 1 ms
2 hop2.transit-network.net (10.288.114.254) 2 ms 2 ms 2 ms
3 hop3.transit-network.net (10.224.137.21) 3 ms 3 ms 5 ms
4 hop4.transit-network.net (10.224.46.74) 4 ms 2 ms 3 ms
5 hop5.transit-network.net (10.224.46.93) 18 ms 20 ms 21 ms
6 hop6.transit-network.net (10.224.46.5) 26 ms 21 ms 27 ms
7 hop7.example-upstream.net (10.224.32.30) 19 ms 16 ms 16 ms
8 hop8.example-upstream.net (10.4.1.122) 25 ms 24 ms 24 ms
9 hop9.example-upstream.net (10.4.1.202) 24 ms 25 ms 26 ms
10 hop10.example-site.edu (10.192.33.3) 24 ms 26 ms 26 ms
11 hop11.example-site.edu (10.72.0.11) 27 ms 25 ms 27 ms
12 host3.example-site.edu (10.72.0.176) 26 ms 27 ms 26 ms
```

The IP number 10.72.0.176 is associated with the EXAMPLE-SITE.EDU domain. The last host in the traceroute appearing before any host in the EXAMPLE-SITE.EDU domain is in the EXAMPLE-UPSTREAM.NET domain. Locating site contact information for EXAMPLE-UPSTREAM.NET would involve a query to the appropriate Whois database, as discussed in section C.2. For example,

```
$ whois -h whois.internic.net example-upstream.net
Whois Server Version 1.1
   Domain Name: EXAMPLE-UPSTREAM.NET
   Registrar: NETWORK SOLUTIONS, INC.
   Whois Server: whois.networksolutions.com
   Referral URL: www.networksolutions.com
   Name Server: NS1.EXAMPLE-UPSTREAM.NET (10.4.100.12 )
   Name Server: NS2.EXAMPLE-UPSTREAM.NET (10.5.154.9 )
   Updated Date: 13-oct-1998
$ whois -h whois.networksolutions.com example-upstream.net
Example Internet, Inc. (EXAMPLE-UPSTREAM-DOM)
   4422 Boogy Boogy Ave.
   Exampleburgh, PA 15555
   Domain Name: EXAMPLE-UPSTREAM.NET
   Administrative Contact, Technical Contact, Zone Contact:
      Network Operations Center, Example Internet (EXI)
      noc@example-upstream.net  (311) 555-1111
   Record last updated on 13-Oct-98.
   Record created on 02-Dec-95.
   Database last updated on 13-Oct-98 03:50:14 EDT.
   Domain servers in listed order:
   NS1.EXAMPLE-UPSTREAM.NET     10.4.100.12
   NS2.EXAMPLE-UPSTREAM.NET     10.5.154.9
```

Appendix A: Resources for finding point of contacts

1. Registry databases by domain name

   Please refer to the following URL for the HTML version: http://www.cert.org/tech_tips/whois_by_domain.html

2. Registry databases by IP number allocation

   Please refer to the following URL: http://www.cert.org/tech_tips/whois_by_ipaddr.html

Appendix B: Possible problems when converting between IP numbers and domain names

When you work with domain names and IP numbers in the context of responding to a security incident, you must determine the authenticity and integrity of the available domain name or IP number information.

In TCP/IP network communications, hosts communicate using IP numbers. IP numbers may be recorded by activity logging mechanisms, by hosts, or by other network devices. In other cases, IP numbers are converted to domain names using the DNS before being recorded by activity logging mechanisms. The following examples highlight some situations which may result in untrustworthy IP number or domain name information.

- IP spoofing - Some intruder attacks, particularly denial-of-service attacks, may consist of intruder-crafted packets which contain false source IP number information in an attempt to mask the true origin of the attack. In such cases, activity logging mechanisms may record false IP numbers, or perform DNS queries on the IP numbers that cause false domain names to be recorded.
- Intruder control of authoritative nameserver - If an intruder controls the nameserver for an IN-ADDR.ARPA delegation, it may be possible for the intruder to set bogus PTR records which cause nameserver IP number queries to return answers containing false domain names. Activity logging mechanisms, which rely on resolving IP numbers to domain names before recording information, may record the false domain names.
- Intruder poisoning of nameserver information - In some instances, it may be possible for an intruder to "poison" the information contained in a nameserver resulting in the nameserver providing bogus answers to queries. Activity logging mechanisms which rely on resolving IP numbers to domain names may record poisoned domain name information.
- Validate IP number and domain name information during the investigation of a security incident. In doing so, be sure to be aware of the following issues:
- The information contained in the DNS can be (and is often) legitimately changed to meet the evolving needs of organizations and individuals. It may be the case that nameserver queries resolve differently at the time an incident is investigated than they do when the incident actually took place.
- In some cases, DNS zone administrators do not maintain complete or accurate DNS information for delegated zones. For example, PTR records may be missing or inaccurate for some or all IP numbers in a delegated IN-ADDR.ARPA zone. This may lead to inaccurate results when converting from IP numbers to domain names. Also, it's possible that the A record for a domain name does not match the PTR record for the corresponding IP number, resulting in a mismatch between IP number and domain name.
-