The Continuing Denial of Service Threat Posed by DNS Recursion (v2.0)

US-CERT

Summary

US-CERT has been alerted to an increase in distributed denial of service (DDoS) attacks using spoofed recursive DNS requests. These attacks are troublesome because all systems communicating over the internet need to allow DNS traffic. The attacks work in the following manner: a malicious attacker sends several thousand spoofed requests to a DNS server that allows recursion. The DNS server processes these requests as valid and then returns the DNS replies to the spoofed recipient (i.e., the victim). When the number of requests is in the thousands, the attacker could potentially generate a multi-gigabit flood of DNS replies. This is known as an amplifier attack because this method takes advantage of misconfigured DNS servers to reflect the attack onto a target while amplifying the volume of packets.

A recent survey[1] conducted by the Measurement Factory, sponsored by the DNS appliance vendor InfoBlox, found that 75% of DNS servers they polled (roughly 1.3 million) allowed recursion. A similar study using a smaller sample size was conducted by the CERT Coordination Center (CERT/CC). It found 80% of DNS servers still enabled recursion.[2]

An organization could be used as a DNS recursion amplifier if its DNS server is misconfigured. Consequently, its DNS server could be misused in a DDoS attack against another organization. An organization could still be targeted by a DDoS attack from misconfigured recursive DNS servers even if it is not running a vulnerable name server.

Background

The domain name system (DNS) is the internetwork of name servers and protocols that allow computers to resolve hostnames to IP addresses. Commonly referred to as the workhorse of the internet, it provides name resolution services for other core protocols. For detailed information on DNS, consult RFC 1035.[3]

---

1 http://dns.measurement-factory.com/surveys/sum1.html

2 http://cyber.law.harvard.edu/icann/mdr2001/archive/pres/Cert.pdf

3 http://www.ietf.org/rfc/rfc1035.txt

DNS requests can be either recursive or non-recursive. A recursive DNS server processes a domain name request on a domain name for which it is not authoritative (or has not already cached) by querying the root name servers for the IP address of the requested domain name. The root name server will then "delegate" the query to the appropriate top level domain (TLD) server (.com, .org, .net, etc.), which in turn delegates to the authoritative nameserver for the domain in question. A non-recursive server only provides the information it has available locally. However, depending on its configuration, it may also return delegation information for the requested domain.

Potential Targets and Risks

Any system configured to provide DNS recursion is susceptible to this attack, including

- Windows systems running Domain Name Services
- Unix systems running Domain Name Services (BIND)
- DNS appliances (Infoblox, MiningWorks, BlueCat)
- Apple Macintosh OS X. Recursion cannot be filtered in the DNS implementation shipped with Macintosh OS X 10.3.x
- Any device capable of proxying DNS lookups recursively, such as customer premises equipment (CPE)

In addition, the inbound network transport infrastructure is put at risk during such an attack because of the volume of traffic generated.

A DNS recursion attack is essentially an amplification DoS attack. Therefore, the attack affects multiple impact points:

- DNS servers configured to provide recursion receive the spoofed requests and generate replies to the spoofed address (i.e., the victim). The performance of these systems may be negatively affected when processing the spoofed requests.
- The spoofed DNS requests query the root name servers, part of the internet's critical infrastructure, indirectly affecting them.
- The traffic then traverses the internet backbone, affecting the internet service provider and any upstream providers until it reaches the intended target.
- The intended target receives large amounts of inbound DNS replies that could consume all available resources on its router, depending on available bandwidth. Even if the traffic is reduced through rate limiting or other bandwidth throttling measures, the attack could impact other legitimate business along the path of the attack.

What can I do to protect my DNS servers from abuse?

Typically, DNS servers only provide DNS services to machines within a trusted domain. Restricting recursion and disabling the ability to send additional delegation information can help prevent DNS-based DoS attacks and cache poisoning. It can also improve performance on your network by reducing the vulnerability of your DNS servers to use as a reflector in such an attack. The following sections provide guidance on mitigating this threat.

Follow Security Best Practices for Configuring DNS

For additional information on secure DNS practices, see the “Resources” section of this paper.

Microsoft

Server 2003

Consult Microsoft’s *Securing DNS for Windows 2003*

http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/Operations/fea46d0d-2de7-4da0-9c6f-2bb0ae9ca7e9.mspx

Windows 2000

Consult the *Windows 2000 Secure DNS Configuration Guide*:

http://nsa2.www.conxion.com/win2k/guides/w2k-6.pdf

Unix

The Berkeley internet Name Domain (BIND) server is distributed with most UNIX variants and provides name services to many networks. BIND, however, has a number of vulnerabilities that can, among other things, allow it to be exploited to launch DoS attacks. Team Cymru’s Secure BIND Template provides guidance on securing BIND from such abuse. The template is available at the following URL:

http://www.cymru.com/Documents/secure-bind-template.html

Team Cymru also provides templates for additional border protection: the Secure IOS Template and the Secure BGP Template.

Disable Recursive DNS

Consult the following documentation to learn about disabling recursive DNS in your environment.

Microsoft

Server 2003

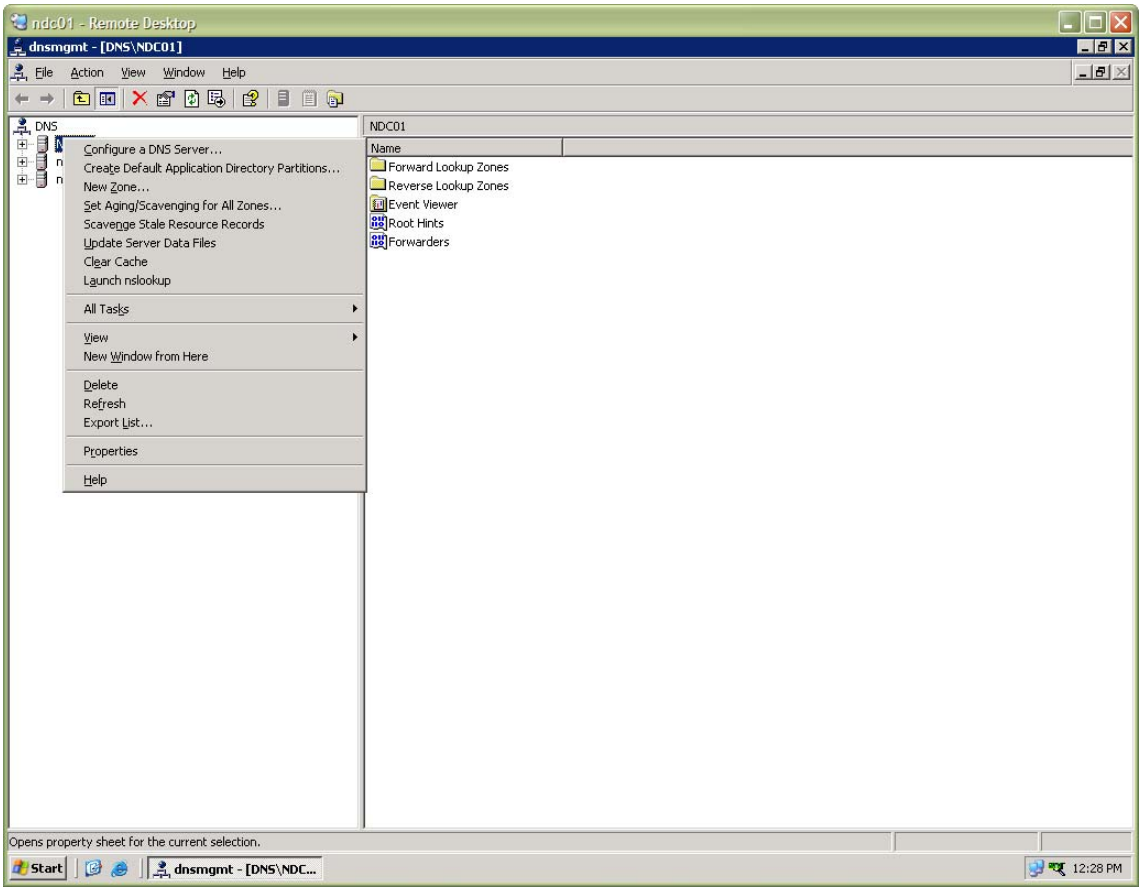
Information on how to disable recursive queries on the DNS server can be found at the following URL:

http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/ServerHelp/e1fe9dff-e87b-44ae-ac82-8e76d19d9c37.mspx

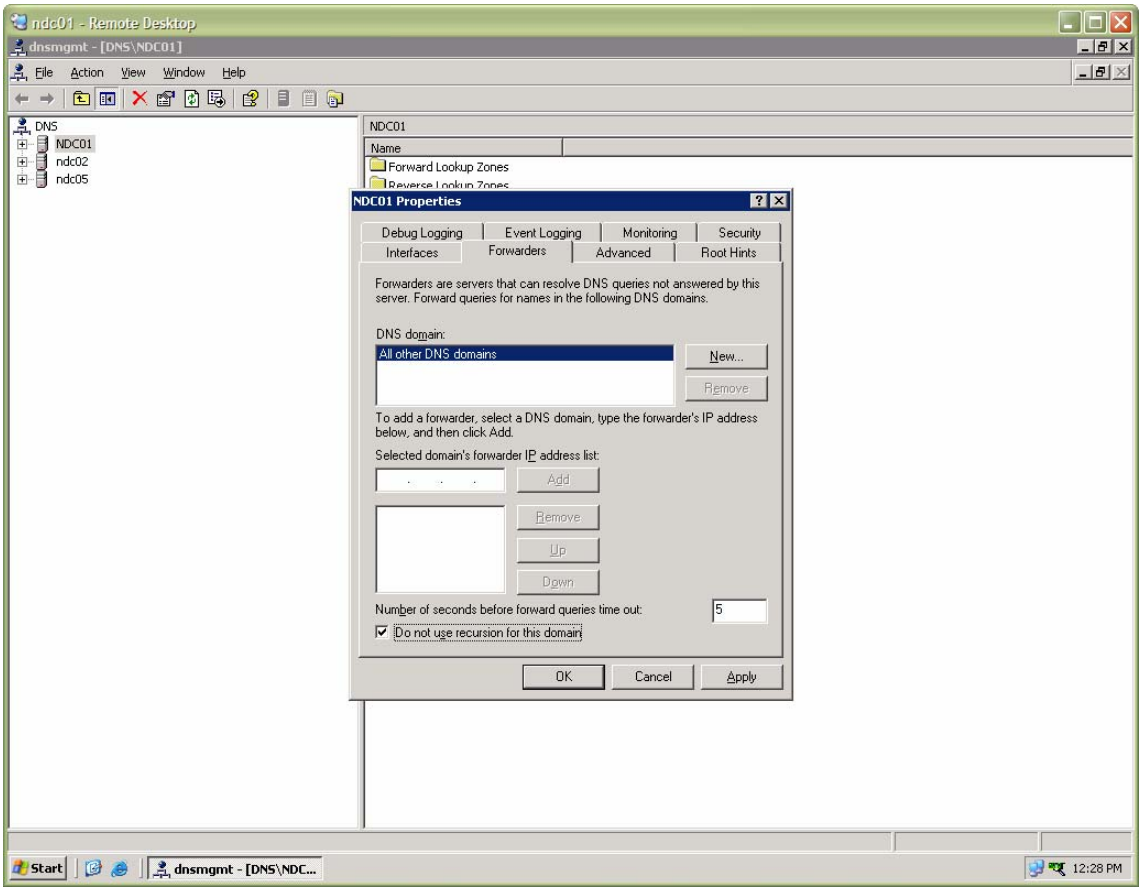
Instructions taken from the above URL have been provided here. Screen shots have also been provided for illustrative purposes.

To disable recursion using the Windows interface:

- Open the DNS snap-in (To open the DNS snap-in, click **Start**, point to **Administrative Tools**, and then click **DNS**).
- In the console tree, right-click the applicable DNS server, then click **Properties**:



- Click the **Advanced** tab.
- In **Server options**, select the **Disable recursion (also disables forwarders)** check box, and then click **OK**:



To disable recursion using the command line:

- At a command prompt, type the following command, and then press ENTER:

  dnscmd*ServerName*/Config/NoRecursion {1|0}

Value	Description
ServerName	Required. Specifies the DNS host name of the DNS server. You can also type the Internet Protocol (IP) address of the DNS server. To specify the DNS server on the local computer, you can also type a period (.).
/NoRecursion	Required. Disables recursion.
{1|0}	Required. To disable recursion, type 1 (off). To enable recursion, type 0 (on). By default, recursion is enabled.

Windows 2000

Information on how to disable recursive queries on the DNS server can be found at the following URL:

http://www.microsoft.com/windows2000/en/advanced/help/default.asp?url=/windows2000/en/advanced/help/sag_DNS_imp_ModifyServerDefaults.htm

Instructions taken from the above URL have been provided here.

To disable recursion on the DNS server

- Open DNS (click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **DNS**).
- In the console tree, click the applicable DNS server.
- On the **Action** menu, click **Properties**.
- Click the **Advanced** tab.
- In **Server options**, select the **Disable recursion** check box, and then click **OK**.

Unix

For information on disabling recursive DNS on Unix systems, see Team Cymru's BIND Template (noted above).

In the current version of BIND, DNS recursion is enabled by default. Internet Systems Consortium (ISC) has agreed to disable recursion by default in the next release of BIND. For current versions of BIND, these instructions, taken from Team Cymru's BIND Template (http://www.cymru.com/Documents/secure-bind-template.html) are provided for disabling recursion.

```
// Create a view for external DNS clients.
view "external-in" in {
   // Our external (untrusted) view. We permit any client to access
   // portions of this view. We do not perform recursion or cache
   // access for hosts using this view.

   match-clients { any; };
   recursion no;
   additional-from-auth no;
   additional-from-cache no;

        // Link in our zones
        zone "." in {
           type hint;
```

```
        file "db.cache";
    };

    zone "ournetwork.net" in {
        type master;
        file "master/db.ournetwork";

        allow-query {
            any;
        };
    };

    zone "8.8.8.in-addr.arpa" in {
        type master;
        file "master/db.8.8.8";

        allow-query {
            any;
        };
    };


};
```

Test your existing configuration

The Measurement Factory web site provides pointers to a number of third-party tools available for validating DNS. The list is available at the following URL:

http://dns.measurement-factory.com/tools/third-party-validation-tools/

Conclusion

Where possible, organizations should secure their DNS servers to ensure that they do not allow recursion or, at a minimum, restrict access to only trusted domains and disable the ability to send additional delegation information.

References

Bellovin, Stephen M. *Using the Domain Name System for System Break-ins.* <http://www.cs.columbia.edu/~smb/papers/dnshack.ps> (1990).

Boran, Sean. *Hardening the BIND DNS Server.* < http://www.boran.com/security/sp/chrooting_bind.html > (October 2, 2000).

DynDNS. *The Dangers of Open Recursive DNS*. <http://www.dyndns.com/about/company/notify/archives/the_dangers_of_open_recursive_dns.html> (November 3, 2005).

Espiner, Tom. *Old software weakening Net's backbone, survey says.* < http://news.com.com/Old+software+weakening+Nets+backbone,+survey+says/2100-7347_3-5913771.html > (October 25, 2005).

Householder, Allen et al. *Securing an Internet name server.* <http://www.cert.org/archive/pdf/dns.pdf> (August 2002).

Leydon, John. *Most DNS Servers 'wide open' to attack.* < http://www.theregister.co.uk/2005/10/24/dns_security_survey/ > (October 24, 2005).

LURHQ Threat Intelligence Group. *DNS Cache Poisoning – The Next Generation.* < http://www.lurhq.com/cachepoisoning.html > .

Mirkovic, Jelena; Dietrich, Sven; Dittrich, David; and Reiher, Peter. *Internet Denial of Service: Attack and Defense Mechanisms*. New York, NY: Prentice Hall PTR, 2004 (pp. 51-52).

Myser, Michael. *DNS Survey Finds Widespread Vulnerability.* <http://www.eweek.com/article2/0,1895,1877177,00.asp> (October 25, 2005).

Rampling, Blair; Dalan, David. Walking through DNS Request Processing (adapted from *DNS for Dummies*). < http://www.dummies.com/WileyCDA/DummiesArticle/id-1701.html > (February 2003).

RUS CERT. Permitting recursion can allow spammers to steal name server resources (discussion thread). http://cert.uni-stuttgart.de/archive/bugtraq/2003/09/msg00164.html > (September 9, 2003).

Schuba, Christoph. *Addressing Weaknesses in the Domain Name Protocol.* < http://ftp.cerias.purdue.edu/pub/papers/christoph-schuba/schuba-DNS-msthesis.pdf > (August 1993).

UNISOG. Discussion thread concerning a DNS reflector DoS attack against a major provider of

global domain name registration services.
<http://staff.washington.edu/dittrich/misc/ddos/register.com-unisog.txt> (January 2001).

Wikipedia. *An example of theoretical DNS recursion.*
<http://en.wikipedia.org/wiki/Domain_Name_System#An_example_of_theoretical_DNS_recursion>.

Zytrax Communications. *DNS BIND Query Statements.* <
http://www.zytrax.com/books/dns/ch7/queries.html > .