May 8, 2013

To: IT Security Staff, Network Administrators, and DNS Administrators
(a CIO version of this Alert is available at http://www.ren-isac.net/alerts.html)

REN-ISAC ALERT:

Prevent your institution from being an unwitting partner in denial of service attacks

The REN-ISAC [1] wants to raise awareness and drive change concerning common network and domain name system (DNS) configurations that fall short of accepted best practice and which, if left unchecked, open the door for your institution to be exploited as an unwitting partner to crippling denial of service attacks against third parties.

Please note important, specific recommended **ACTIONS** included below.

Although attacks exploiting the network and DNS configuration weaknesses have been around for a long time, the frequency and impact of attacks have grown over the past year. These attacks may exploit thousands of institutional DNS servers to create an avalanche of network traffic aimed at a third-party victim. The traffic sourced by any single institutional system may be small enough to go unnoticed at the institution; however, the aggregate experienced at the target can be crippling. A recent attack [2] generated over 300 gigabits per second of traffic aimed at the victim organization. To put that in context, most universities and organizations connect to the Internet at 1 Gbps or less. In this incident not only was the intended victim crippled, Internet service providers and security service providers attempting to mitigate the attack were adversely affected.

Given history and the success of recent attacks, we expect that attacks will rise in frequency and magnitude in the months ahead.

The network configuration issue concerns the ability for a machine on your network to send packets marked with a source IP address that doesn't belong to you ("spoofed") to outside your network. The DNS issue concerns a configuration that allows outsiders to exploit your DNS servers to send high volumes of traffic at arbitrary target machines.

=== ACTIONS ===

In a companion note to CIOs [3], the REN-ISAC recommends the following four actions:

1. Distribute a copy of this message to your network administrators, information security staff, DNS administrators, and other relevant personnel.

2. Ensure your institutional network(s) are unable to originate Internet traffic with spoofed source addresses.

3. Do not permit any DNS server on your networks to answer queries from the public Internet, with the exception of the institution's authoritative servers, which should only answer queries about data they are authoritative for.

4. Investigate rate limiting for your authoritative DNS servers. Rate limiting becomes even more important for DNSSEC-enabled zones.

TECHNICAL AND POLICY CONTROLS

===== Overview =====

Open recursive resolvers, authoritative DNS severs (especially when zones are DNSSEC signed), and networks that do not prevent source address spoofing create an environment on the Internet where DNS amplification DDoS attacks [4] of great magnitude can be achieved.

Too many higher education institutions contribute to this known and avoidable problem.

Unfortunately, this problem goes unsolved because organizations targeted in the attacks are not the same organizations failing to follow best common practices and being exploited to conduct the attacks. The exploited organization often experiences little ill effect; therefore, motivation to solve the problem depends on good Internet citizenship.

===== Solutions =====

[DNS]

Highly Recommended:

- Ensure recursive resolvers [5] are accessible only to authorized/intended users, such as by limiting access to your recursive resolvers to just your enterprise's IP addresses.

- Manage DNS traffic (port 53 tcp/udp), e.g. by using router ACLs, so queries from outside the enterprise can only go to permitted authoritative name servers. This mitigates risk from various uncontrolled devices, such as Internet appliances that have an embedded DNS service.

- Investigate rate limiting [6][7] for your authoritative name servers, and develop a plan for implementation as possible. Rate limiting becomes even more important for DNSSEC-enabled zones.

- Run recursive resolver and authoritative name servers on separate machines [8] thereby allowing proper controls for each.

Recommended:

- Provide a means to monitor DNS traffic, including the ability to detect anomalous changes in DNS query patterns.

Other related good practices:

- Manage DNS traffic (port 53 tcp/udp), e.g. by using router ACLs, so queries from inside the enterprise can only go to intentionally permitted enterprise or external (e.g. Google Public DNS or OpenDNS) recursive resolvers.

- Check your DNS configuration for other issues, e.g. using http://dnscheck.iis.se/

[Network]

Highly Recommended:

- Apply BCP38 filtering to prevent spoofed source address traffic from leaving your network. [9][10]

Recommended:

- Collect and store network flow (NetFlow/Sflow/J-Flow) data. Real time network flow allows backtracking spoofed network traffic. Historical network flow facilitates incident response capabilities.

===== More In-Depth =====

[Recursive Resolvers]

If you allow unrestricted access to your recursive resolvers, those resolvers are known as "open recursive resolvers" and are subject to abuse by any attacker connected to the Internet.

To understand how attackers abuse open recursive resolvers, assume attacker A wants to flood target T with an overwhelming volume of network traffic. Attacker A generates fake DNS queries, pretending (using spoofed IP source addresses) to be target T. The attacker sends those queries to open recursive resolvers located all over the Internet, potentially including yours if it's open for their use. Those open recursive resolvers then send answers to the forged DNS queries to target T, filling up T's network capacity and potentially knocking T's users off the network. The size of the DNS query is much smaller than the size of the answer, hence "DNS amplification".

It is absolutely critical all university recursive resolvers are properly configured so they only answer queries for the local users they're meant to be serving. You can request a free report of open recursive resolvers on your campus from these resources [11][12].

[Rate Limiting Authoritative DNS Servers]

Authoritative DNS servers should be accessible to everyone on the Internet; however, authoritative servers can also be exploited for DNS amplification attacks, especially with DNSSEC-enabled zones. Rate limiting prevents your authoritative server from answering the same (spoofed) question tens or hundreds of thousands of times per second. You should investigate rate limiting, and implement as possible. See http://www.redbarn.org/dns/ratelimits for more information.

[Network Filtering to Prevent Source-Spoofed Packets]

Systems should not be permitted to send spoofed traffic to the Internet, pretending to be from some other site's IP addresses. Roughly 80% of all networks have already installed filtering rules on their network routers to ensure any spoofed network traffic won't hit the Internet, but some networks -- including potentially yours -- have not yet done so. We need your help. Please ensure your institutional networks prevent traffic with spoofed source addresses from leaving your network.

Blocking spoofed network traffic from leaving your network is an IETF Best Common Practice ("BCP"), see:
http://tools.ietf.org/html/bcp38 and
http://tools.ietf.org/html/bcp84

The text of this message and the CIO version (along with clobber-free long URLs) can be found at [3].

We'd appreciate your input on additional means to protect from this threat, and general feedback concerning the Alert.

If you have any questions, please don't hesitate to e-mail us at soc@ren-isac.net.

Special thanks go to the members of the REN-ISAC Technical Advisory Group [13] for their work on this Alert.

On behalf of the REN-ISAC team,

Doug Pearson
dodpears@ren-isac.net
Technical Director, REN-ISAC
http://www.ren-isac.net
24x7 Watch Desk +1(317)278-6630

References

In addition to the references made in the text above, the following may be useful:

DNSSEC and DNS Amplification Attacks
http://technet.microsoft.com/en-us/security/hh972393.aspx

Explaining Distributed Denial of Service Attacks to Campus Leaders
http://pages.uoregon.edu/joe/ddos-exec/ddos-exec.pdf

Preventing Use of Recursive Nameservers in Reflector Attacks
http://www.ietf.org/rfc/rfc5358.txt

US-CERT Alert (TA13-088A) DNS Amplification Attacks
http://www.us-cert.gov/ncas/alerts/TA13-088A

[1] REN-ISAC
http://www.ren-isac.net

[2] Firm Is Accused of Sending Spam, and Fight Jams Internet
http://www.nytimes.com/2013/03/27/technology/internet/online-dispute-becomes-internet-snarling-attack.html?pagewanted=all

[3] REN-ISAC DNS Amplification Alert
http://www.ren-isac.net/alerts.html

[4] What is a DNS Amplification Attack?
https://deepthought.isc.org/article/AA-00897/0/What-is-a-DNS-Amplification-Attack.html

[5] Section 2 DNS Architectural Components provides definition of recursive resolver
http://www.dhs.gov/sites/default/files/publications/dns_reference_architecture_0.pdf

[6] Response Rate Limiting in the Domain Name System (DNS RRL)
http://www.redbarn.org/dns/ratelimits

[7] DNS Response Rate Limiting (DNS RRL)
http://ss.vix.su/~vixie/isc-tn-2012-1.txt

[8] Domain Name System (DNS) Security Reference Architecture
http://www.dhs.gov/sites/default/files/publications/dns_reference_architecture_0.pdf

[9] Network Ingress Filtering
http://tools.ietf.org/html/bcp38

[10] Securing the Edge
http://www.icann.org/en/groups/ssac/documents/sac-004-en.pdf

[11] For a list of open resolvers by ASN, e-mail dns-scan /at/ puck.nether.net
http://openresolverproject.org/

[12] List open resolvers on your network
http://dns.measurement-factory.com/cgi-bin/openresolverquery.pl

[13] REN-ISAC Technical Advisory Group
http://www.ren-isac.net/about/advisory.html#technical