May 8, 2013

To: CIOs
(a TECH 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.

CIOs, 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.

The higher education and research community needs to do its part to ensure that we are not helping to facilitate these attacks. The REN-ISAC recommends the following actions:

=== 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.

We're sharing a version of this letter, with additional technical depth and recommendations, to campus security officers, network administrators, and DNS administrators. This note and related technical notes are available at the REN-ISAC web site, and have been sent directly to REN-ISAC members and to the public EDUCAUSE Security and CIO mailing lists.

Reference: http://www.ren-isac.net/alerts.html

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 [3] 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

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

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