

Windows Enterprise Announcement

April 15, 2013 – Proposed Changes to DNS Service for Off-campus Users

Iowa State University DNS servers have participated in DDoS (Distributed Denial of Service) attacks against other systems on the Internet in the recent past. These attacks do not originate on the DNS servers at ISU, but the ISU DNS servers serve as a middle-man in the attack, amplifying a flood of DNS requests from an attacker's group of systems through ISU DNS servers forged as if from the victim site. This causes an overload at the victim site receiving the request and a subsequent denial of service.

ISU is being scanned for recursive DNS servers by two groups – the attackers who want to use our servers in attacks and Internet watch-dogs (such as REN-ISAC) who want us to properly configure our DNS services.

There are two things that must be done to eliminate ISU DNS servers from participating in the attack. First, ISU DNS servers should NOT do recursive lookups unless absolutely necessary. A recursive lookup occurs when the local DNS service cannot resolve the address requested and must refer it to another site. Second, port 53 (the DNS port) must be blocked at the campus border so that only the main DNS servers (DNS-
<n>.iastate.edu) are open to the internet and rate-limited (to reduce the efficiency of any attack).

A timeline for these changes has yet to be determined, though ITS intends to act as quickly as possible to aid in the reduction of these attacks. Watch for further information the main public mailing lists and meetings (CCSG, WinAdmin, etc.).

It should be noted that DNS service is running on all five domain controllers. This service is needed to be able to provide DNS resolution for critical domain services like LDAP, the KDC, etc. By default this DNS service is configured to do recursive lookups. However, this is unnecessary and recursion will be turned off May 16, 2013. If you have correctly configured your systems to point to the main NS-
<n>.iastate.edu servers on the IP configuration tab the change will have no impact on you.

Questions and concerns can be directory to Tracy Di Marco White [ITSYS] (gendalia@iastate.edu).