IS&T addresses concerns about MIT's network

Information Services & Technology sheds light on recent service interruptions, as well as steps taken to mitigate risks to the MIT network.

February 5, 2013

Since Jan. 13, MIT's campus network has experienced a series of outages that have temporarily affected a number of web services.

The network interruptions, which resulted in delays in email delivery and losses of Internet connectivity, have been caused by denial-of-service (DoS) attacks, misconfigurations to external systems and loss of control of the mit.edu domain to external parties. A Denial of Service (DoS) or Distributed Denial of Service (DDos) is focused on rendering a device or network inaccessible and unavailable to its intended users.

In response, Information Services & Technology (IS&T) has taken several measures, such as installing filters to block problematic traffic or content. "We understand that it can be unsettling to have a number of outages and service interruptions in a short period of time," says Christine C. Fitzgerald, manager of communications for IS&T. "The corrective and preventive measures that IS&T has put in place as a result of these outages have mitigated the risk of similar attacks or threats to the MIT network."

Problems and solutions

The first DoS or DDoS attack, on Jan. 13, caused the MIT campus to lose Internet access; MIT email and various MIT Web pages were also inaccessible externally. The outage lasted about three hours before IS&T stabilized the network by adding filters to block the attack.

Five days later, MIT experienced an email outage lasting four to six hours. This outage — caused by a misconfigured list-management system at MIT — resulted in an infinite email loop with delays in delivery of messages from outside MIT or to addresses outside MIT. Those using MIT email addresses (@mit.edu) experienced delays in sending and receiving messages from external addresses; internal e-mail exchanges were unaffected. To rectify the issue, IS&T used filters to block e-mails that were causing the loop and worked with system administrators to properly configure the list-management software.

On Jan. 28, the MIT website and other online services were rendered inaccessible from off campus. External messages to and from MIT email addresses were again delayed and, in some instances, lost. Some users experienced problems accessing online services, or had to reboot or restart machines that were not running properly. These issues were the result of another attack, this time on the MIT domain name — mit.edu. The mit.edu domain registration was administratively compromised by an attacker and re-pointed to Domain Name System (DNS) servers under the attacker's control.

The mit.edu domain name is managed by EDUCAUSE, a nonprofit association that is the registrar for all .edu domains. The attack rerouted MIT traffic destined for mit.edu hosts to different servers, causing MIT's Internet service to malfunction. After an hour of work with EDUCAUSE, IS&T regained administrative control of the domain. Although IS&T worked with Internet service providers to limit the period of impact as much as possible, the effects of this outage may have lasted up to 24 hours (due to the time information is cached/stored in the DNS servers around the Internet).

MIT's open network is essential to collaboration in teaching and learning at the Institute, Fitzgerald says. "IS&T is working to identify and address other vulnerabilities that present a risk to the campus network and key services — although the nature of these complex systems makes it difficult to eliminate risk completely," she says. "Community members should be assured that particular attention is being paid to minimizing risks and outages in the future."

If you are experiencing any service issues that you believe may be associated with the network outages, please contact the IS&T Help Desk at helpdesk@mit.edu or 617-253-1101. Members of the MIT community may also submit service requests online.