Are you ready for a DDoS attack?

DDoS threat preparedness tips

Distributed Denial of Service (DDoS) attacks are among one of the most disruptive and vicious activities passing over the Internet. DDoS attacks can overwhelm web servers and saturate a company's connections to the Internet resulting in the inability to maintain efficient communications and connectivity and can ultimately impact business operations. By integrating the predictive and early warning capabilities of AT&T DDoS Defense, AT&T is delivering one of the most potent tools against denial of service attacks, which have crippled entire networks and brought businesses to a halt.

Are you prepared if and when it happens to you? Read through the AT&T Top Readiness Tips below and see if you're prepared for a DDoS attack and if not, what actions you can take today to get ready.

Ready Yourself for a DDoS Attack

- Have a reaction plan ready to implement
- Document the key technical players to help remediate an attack. Use small focused groups to make good decisions quickly
- Test your DDoS service annually and ensure all notifications are received as expected
- Engineer resources to accommodate attack scenarios above and beyond normal, anticipated loads
- Keep mitigation settings current with gateway architecture (i.e. circuits, IP addresses, servers, services, etc.
- Be sure your DDoS Service Provider is experienced and well versed in current attack vectors
- Understand your ISP's capabilities for dealing with attacks
- You may need an alternate form of communication during an attack in the event that other IP based services are impacted i.e., VoIP, email
- Understand and document your gateway architecture as it evolves, and know how to implement routing changes quickly

During a DDoS Attack

- Refer to your documented plan
- Document all mitigation/corrective steps taken
- Save logs and packet captures for post mortem reviews

Threat Landscape

- Attacker's motives include political, financial, and bragging rights – every corporation is susceptible to an attack
- A DDoS attack is often a diversionary tactic to enable other illicit activities such as data theft, fraud, etc.
- All attacks are different – some attack volumetrically, while others exploit Transmission Control Protocol (TCP) Layer 7 vulnerabilities. Some attacks exploit both.
- Attacks tend to change and adapt to defensive measures put into place

For more information about AT&T DDoS Protection, visit us at www.att.com/ddos-protection or call us at 877 542-8666

To learn more about AT&T Managed Security Services, visit www.att.com/network-security or have us contact you.

Scan this code to learn more.

Share this with your peers

07/24/13 AB-2557-01