Limiting the Damage from a Denial of Service Attack

From the Experts
Andrew M. Hinkes, Corporate Counsel

In early 2013, a wave of denial of service (DoS) attacks reportedly caused U.S. banks to be knocked offline for 249 hours, at an estimated cost of over $12 million. Sony reportedly spent more than $170 million to clean up a DoS attack and associated loss of client data.

DoS attacks can impair your business’ ability to reach its customers, conduct online commerce and communicate with business partners, costing billions of dollars. Although attacks may be impossible to prevent, planning for a DoS attack can minimize the likelihood of an attack and limit the damage to assets and business goodwill.

What Is a DoS Attack?

A DoS attack is the purposeful overload of an Internet-connected device, aiming to make the device or a service provided by that device unavailable to its intended users. DoS attacks cause a targeted device to be flooded with a synchronized torrent of communication that paralyzes the device. A DoS typically emanates from large numbers of compromised computers (called a “bot” or “zombie”), which are under the control of one central machine (collectively called a “botnet”) in a Distributed Denial of Service attack (DDoS). DoS attacks have affected private business, governments, banks, gaming sites, e-commerce vendors and end-user computers, and are a favored tool in cyberwarfare. One industry survey commissioned by Neustar revealed that 39 percent of retailers and 41 percent of ecommerce businesses experienced an attack in 2012.
The tools and software necessary to launch a DoS attack are increasingly inexpensive and widely distributed. These tools have quickly increased in sophistication and ease of use; more modern DoS clients are available for download online, and are even available on a “for hire” basis through a DDoS-as-a-Service model. Studies show that victims of DoS attacks tend to be assaulted repeatedly, suffering attacks of escalating power and duration. Overall, DoS attacks continue to grow in frequency, duration and volume. These DoS attacks typically result in lost system access, extended system downtime, consumer complaints, lost sales, emergency system repairs and upgrades, and loss of brand goodwill.

**Why Can't Anyone Stop DoS Attacks?**

DoS attacks are made possible by the very structure of the Internet. To communicate with other machines, a device must open a line of communication (a port) to send and accept information. A DoS attack forces data into an open port at a speed and volume that overwhelms the receiving computer. The only distinguishing characteristic between a DoS attack and legitimate communication to that port is the bulk and the intent behind the traffic. The only sure way to protect a computer from a DoS attack is to disconnect it from the Internet. So, while prevention is impossible if connectivity is required, mitigation strategies can save your business from significant losses when a DoS attack strikes.

**What Are the Business Consequences of a DoS Attack?**

According to Neustar, organizations that depend on the Internet for their revenue stream suffered an estimated average daily revenue loss of $2,000,000—nearly $100,000 per hour—for Internet downtime, while other businesses’ losses average about $10,000 per hour. While these hourly losses are significant, they fail to incorporate the costs of reputational damage. Businesses hate to admit to any event that jeopardizes public trust. Acknowledgement of a DoS attack can cause a PR crisis, and sometimes require replacement of IT leadership, corporate rebranding and significant PR expenditures to recapture public confidence.

Aside from costs to remedy the damage caused by an attack, to restore system access and to repair a damaged reputation, a victim business may find itself facing legal claims. Customers who can prove damages due to e-commerce system downtime may sue for financial restitution, claiming the victim business took insufficient measures to safeguard the availability of the affected e-commerce website against DoS attacks. Those customer claims would likely be based upon an alleged breach of contract under the victim business’ Terms of Service (TOS) with its users.

**What Claims May Be Brought by the Victim Business?**

A victim business may attempt to recover against the parties responsible for the DoS attack, but will likely be limited to claims against the mastermind behind the DoS attack. Although foreign
jurisdictions have enacted laws directly addressing DoS attacks, there is no law directly punishing DoS attacks in the U.S., leaving victim businesses with few viable options for legal relief. A victim business may, however, pursue a remedy under the Computer Fraud and Abuse Act (CFAA), which generally provides both civil and criminal relief upon proof that a defendant accessed a computer without authorization and knowingly and with intent to defraud obtained something of value, resulting in damages of $5,000.00 or more. In Pulte Homes Inc. v. Laborers’ Int’l. Union of N. Am., the court ruled that a flood of phone calls and emails directed against an employer with the intention of rendering its telephone and email systems inoperative stated a claim under the CFAA. Pulte’s claim was brought against the known ringleader of the DoS attack. While a CFAA claim may be available against the mastermind of a DoS attack, these claims are less effective against individual bots that actually created the attack, because a victim business will have difficulty proving any one bot was the proximate cause of its injury when hundreds or thousands of bots attacked the device. Thus, while a CFAA claim may provide relief when the mastermind is easily identifiable, it may not facilitate relief against bots, and such claims are rarely pursued. Likewise, a negligence cause of action against a bot owner would likely fail, as there is no recognized duty of computer owners to secure their Internet-connected device from malware that would convert it into a bot. Claims against the coders who wrote the malware that launched the attack are rarely pursued, because most malware writers are unknown or difficult to identify, and based upon security statistics are likely not residents of the United States. The victim business may also attempt to sue its Internet Service Provider (ISP) for allowing the DoS traffic. The success of that claim would rely upon the specific terms of the business’ Service Level Agreement (SLA) with the ISP. Finally, although an e-commerce site TOS may expressly bar DoS attacks, from a practical standpoint, barring users whose machines were unwittingly controlled by a botnet from subsequent good faith access to engage in commerce, or suing active clients for the actions of their bots makes little business sense. Unless the mastermind of an attack is identified, victims of DoS attacks are left with few appealing options for relief. When the mastermind is known, however, both criminal and civil remedies may be available under the CFAA. **How Can Your Business Prepare for and Mitigate Damage Caused by a DoS Attack?** Although DoS attacks can be expensive, disruptive and create a public relations nightmare, there are steps your business can take to become a less attractive or more challenging target.
Technical maintenance and upkeep will help you reduce your IT systems’ vulnerability to DoS attacks. Stress testing the business’ network can simulate an attack, and allow your IT department to understand your devices’ load tolerances and identify which devices are “easy targets.” Then, with simple planning, your business can bolster its defenses. Redundancy and co-location and geographic distribution of resources will help your business avoid a loss of a critical service or function as a result of a DoS attack directed upon a single device.

Likewise, ensure that your IT department follows best practices when configuring servers, and maintains control over configuration changes on any Internet-facing device configurations. All Internet-facing devices should regularly be updated with all firmware and software updates. This includes simple fixes such as requiring complex passwords, disabling unused ports, updating firmware and updating spam filters.

Your business can also consider contracting for on-demand expandability of network and/or processing power from vendors to accommodate sudden surges of demand for network resources. Finally, an IT professional can set up a system that detects abnormal traffic patterns, which will provide early warning of an attack in progress.

Of course, legal and compliance should be involved in planning for DoS attacks. Your business should maintain written procedures for risk, legal, compliance and IT during an attack, including clear specification of which group is responsible to contact affected personnel, law enforcement, ISP and tech support, etc. Legal and IT should both be familiar with your business’ ISP SLAs, which explain your ISP’s obligations, if any, to protect your network from DoS. The SLA will typically explain the ISP’s obligations, if any, to notify your business upon detection of abnormal fluctuations in network traffic. The SLA may also contain key emergency contact information which will be needed during an attack. Finally, your business should consider purchasing cyberliability insurance to cover for losses caused by DoS and other cybercrime.

**My Business Is Being Attacked Right Now. What Should I Do?**

Most businesses learn they are being attacked shortly after they receive and fail to act on a ransom demand, or when they detect a service interruption. If your business is under attack, immediately call your ISP via its emergency support line. Your ISP should immediately monitor the traffic to your network and alert “upstream” connectivity providers of the attack. If you cannot find a responsive contact with your ISP, consider contacting a Computer Incident, Emergency or Security Incident Response Team (CIRT, CERT, CSIRT) or other similar organizations that assist with investigation of an attack.

Obviously, if a ransom demand was received or other threat made precedent to an attack, your business should report the threat to law enforcement. Law enforcement will help you document and investigate the attack, but will not assist in mitigating any damage. Finally, capturing information
about the attack will help diagnose the source of the attack and expedite recovery. An IT professional can set up a packet capture to sample the traffic flow directed at the device. The data collected can be forensically useful to identify any telltale characteristics of the attack and attempt to identify to its origin.

The Bottom Line

Although the effects of Denial of Service attacks can be devastating, strategic planning can make your business a less-enticing target, can minimize the impact of an attack on your business' Internet infrastructure and can reduce the severity of the interruption to your business.

Andrew M. Hinkes is an attorney with the Florida business law firm Berger Singerman. He concentrates his practice in business litigation, real estate-related litigation, representation of court-appointed fiduciaries, and is skilled in large scale electronic discovery management in civil litigation. He can be reached at ahinkes@bergersingerman.com.