

Viewpoint

CLOSE

Combating Cyberterrorismby [Arun Srinivasan](#)

Tuesday, February 01, 2005



Cyber terrorism. Extortion. Malicious attacks. Rogue nations.

No, this isn't the ad campaign for a big-budget Hollywood movie. It's the new reality for companies operating in an always-on online world.

Making strikes and boycotts seem like the quaint equivalent of a baby trying to hurt an Olympic wrestler with his tiny fist, the tactics employed by those known as "cyber terrorists" can bring a company to its knees in mere hours. It used to take the agreement and mutual action of thousands of people to even put a small dent in a company's bottom line. But in today's online business environment -- where a simple mouse click connects businesses to their suppliers, to their customers, even to their competitors -- one single individual wields the power to accomplish what once required the unified voices of many.

The cyber terrorists' weapon of choice? "Denial-of-service" attacks (DoS), in which a website is maliciously flooded with requests for information, overloading the system and shutting down the site. Attacks originate in places like the former Eastern Bloc, China or Libya, from attackers who can control thousands of machines simultaneously. Motives may be economic or political. Companies under such attack either submit to extortion, paying thousands of dollars to their attackers, or don't and suffer millions of dollars in lost revenue as a result.

Sound far-fetched? Consider this:

Three men were arrested in Russia in July for participating in a global extortion racket that targeted the Web sites of British and other bookmakers. The group overwhelmed the Web sites with DoS attacks that prevented legitimate users from accessing the sites -- sometimes for several days at a time -- then demanded payments of up to \$50,000. Estimates place total losses for the gambling sites at about \$70 million.

Companies that suffer business disruptions from Internet-based attacks are losing an average of \$2 million in revenue per incident, according to a recent study by the Aberdeen Group. The study also found that organizations on average suffered one disruptive incident a year from worms, viruses, spyware or other security-related causes, and that corporate systems were down an average of 22 hours in each attack.

And things may be about to get worse. According to the research director of the Washington-based SANS Institute, an estimated 7,000 organizations are now paying online extortion demands, and for cyber criminals, success begets success. "The epidemic of cybercrime is growing," said SANS research director Alan Paller in CNET. "You don't hear much about it because it's extortion, and people feel embarrassed to talk about it."

Denial-of-Service Attacks

The increasingly familiar scenario is this: potential attackers troll the Internet looking for vulnerable Web sites. Small- to mid-sized businesses are not immune; in fact, they may be the most vulnerable to a hit. These sites often are the least prepared to defend themselves against such an attack, lacking the resources to devote to sophisticated security measures.

Once the attackers find a vulnerability, they launch a mini attack just to let the company know they're serious and they have what it takes to overwhelm the server. Then they send an email taking responsibility for the attack and asking for cash payments to stop a larger, full-scale DoS attack launched from a distributed network of thousands of unwitting computers.

The results of an attack include a downed Web site, the inability to take and process orders from customers (potentially fatal for e-commerce sites), damaged customer relationships and an injured brand reputation. Hoping to avoid such consequences, many companies submit to the extortion and pay their attackers.

DoS attacks have become a grim fact of life. But while this may seem a daunting trend, companies and hosts are not powerless against it. Along with the many security related products available today -- including firewalls, automated systems patching, vulnerability notification services, Internet threat assessment and notification systems, intrusion prevention and anti-spyware software -- there are some basic steps every company and host can take to limit the possibility of attack and diminish the effectiveness of an attack, if launched.

Keep virus detection software and Windows Updates current. While this might seem obvious, it's striking how many companies and personal users still do not follow this most basic preventative step. Cyber terrorists know this and take advantage of it.

Attackers scan all computers that haven't been patched with the latest Windows updates. They send worms to infiltrate those computers through a vulnerability that hasn't been patched, and then use them to launch the phony requests that bog down companies' Web sites. DSL routers can block a great many of these, but many holes remain -- and can be exploited. When these computers with "holes" are unwittingly left on at night, they're open to being used in these schemes.

Develop company-wide security procedures. Create a list of rules that includes shutting down computers every night, specific back-up procedures, a schedule of regular updates and patches, periodic password changes, rules about opening email attachments, guidelines on how to protect data while working in public places (like airplanes or Starbuck's), and tips on how to ensure the physical security of laptop computers and actual office buildings.

Additionally, companies and hosts can work together to develop redundancies that will protect a website in case of a successful DoS attack. For example, some hosts will create mirror images of the site -- copying the site to various locations, making it much more difficult for an attacker to bring it down.

Train your employees. Individual users are security's weakest link. Having proper procedures in place is only effective if all employees know them and follow them. Yet in 2003, the Human Firewall Security Awareness Index Survey found that 48 percent of companies had never provided formal security training for their workforce.

Train employees in information security and anti-virus techniques, including how and when to use and update virus prevention software, to never open an email attachment from an unfamiliar address, and to turn off their computers before leaving the office. Make sure they know, understand and follow the company's security procedures.

Choose your Web host wisely. Selecting a good host is critical when it comes to preparing for and reacting to a DoS attack. And for hosts, this is a great opportunity to differentiate and add value.

Many hosts actually are resellers of other hosting companies -- marketing front-ends for other hosts -- and don't actually have the experience or the control to be able to really help in a DoS situation.

Companies need to thoroughly research hosts before making a selection, and always reassess their current hosting relationship to make sure it fits. A good host takes preventative measures up front, and the experienced ones often can see a DoS attack coming. In fact, the effects of a DoS attack can be mitigated at the network level if the host sees the attack coming and can re-route that traffic to help prevent slow-downs and outages.

What If You're Attacked?

If you receive an extortion email threatening a DoS attack, immediately notify the FBI by contacting your local field office. Often the attackers use free Web email services like Yahoo! and Hotmail, which the FBI can trace.

Then, take steps to protect your business and minimize the impact of the attack. Companies and hosts should review options together. There are products and services that companies can purchase to help filter out the bogus network traffic and reduce the stress on the system, but at prices that range from \$30,000 to \$200,000 they could be cost-prohibitive for some businesses. Still, this approach can provide both tangible security and peace of mind; while the terrorists' methods continually evolve and they don't typically use the same attack procedure twice, responding aggressively to even one attack means you're no longer an easy mark.

Alternatively, you can choose to block (a.k.a. null-route) the malicious traffic at the host level, but you'll probably still be responsible for the costs involved with the extra bandwidth. If you start blocking you also run the risk of casting aside legitimate requests and potentially losing some customers.

Perhaps the most common means of defeating a DOS attack involves using a caching service, such as Akamai or Mirror Image, which enables you to distribute your sites around the planet, so you don't have a single point of vulnerability. Microsoft successfully used this technique to defeat a large DOS attack earlier this year. As an added plus, it's possible to turn this capability on in rather short order, should the need arise.

While the DoS is occurring, of course, it's too late, which makes it all the more imperative to work with a host that already has these kinds of relationships in place. Find out about these capabilities in advance, so you can have them at the ready -- and perhaps even be proactive, preventing that next attack from ever reaching your doorstep.
So you actually can have your Hollywood ending.

Arun Srinivasan is COO of BroadSpire, Inc. (www.broadspire.com), a Web hosting firm in Los Angeles.

Find this article at: <http://www.line56.com/articles/default.asp?articleid=6315>