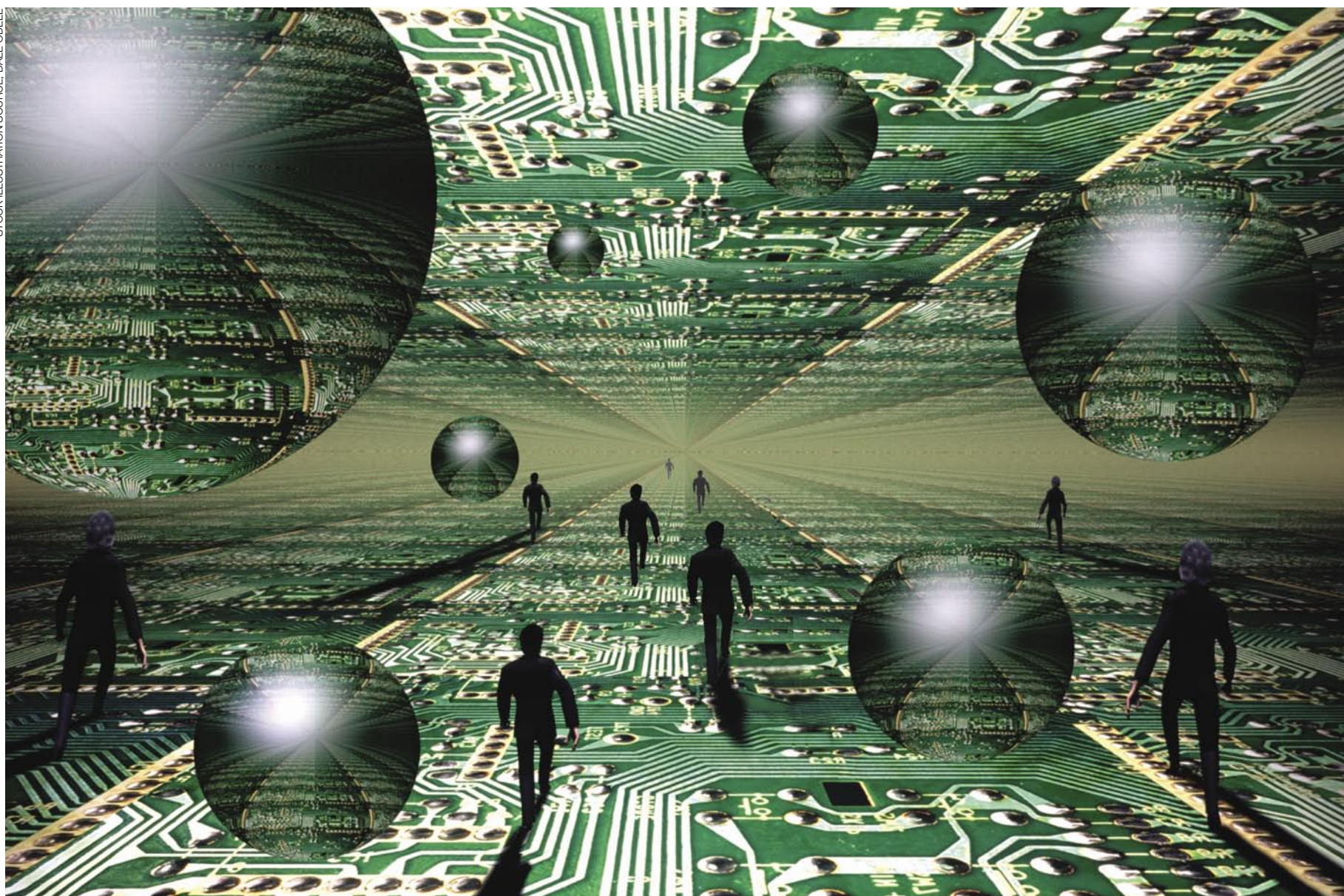


STOCK ILLUSTRATION SOURCE: DALE ODELL



March of the Zombies

Yeomen of silicon armies, 'Bots' soldier forth helped in their quest to decimate computer networks into data wastelands by the interdependence of systems and the lower cost of fast Internet connections. *By Mark Greisiger*

Thousands of companies operate in a network-dependent business environment. To thrive they rely more and more on Internet service providers, application services providers and partners.

By doing so, corporations have become more efficient. But by doing so, they have also placed themselves at greater jeopardy of extortion from thieves skilled at threatening entire corporate networks.

This emerging risk exposure has the potential to wreak havoc on a company's professional reputation and destroy customer and partner trust, while also decimating their bottom line.

Criminal hackers love to hijack porous and vulnerable corporate computer networks to build a silicon army of malicious "Bots," sometimes known as "slave" or "zombie" computers, linked to form a remotely controlled network that can ruin a corporate computer system targeted for attack by the bad guy, the Bot owner or manager.

We're not talking about fire and brimstone here. We're talking about attacks by wave after wave of messages and data from the belligerent Bots. Some networks may crash. More vulnerable ones collapse entirely.

Behind the evil Bots, often from some obscure locale offshore, sits a criminal hacker controlling

the attack in a way that is hard to detect, and even more difficult to trace. Like Darth Vader at the command of killer star destroyers, hackers send out wave upon wave of attack Bots with instructions to infect and cripple business networks.

The campaign, in computer talk, is what's known as a massive "Denial of Service" against a vulnerable corporate system. These events can wreak havoc with electronic funds transfer networks, for example, or can destroy an online retailing operation.

Criminal hackers need not go as far as crippling a corporate network. Instead, the mere threat of an attack will provoke a company to pay a ransom to keep the system up and running. Sophisticated criminals search out easy ways to "hold up" their victims. When they find a company with deep pockets, they pounce.

Take an online retailer who depends upon sales during November and December to make the difference between profits and losses. Those retailing Web servers and desktops must be operational 24 hours a day, seven days a week, especially during the critical Christmas season.

Online casinos or gambling also can ill afford an outage during a peak season, such as the Super Bowl.

Faced with the choice of paying a ransom of \$20,000 or absorbing a loss equivalent of \$2 million in online orders, management may well be happy to pay the ransom. Keeping the Bots at bay saves the peak season and avoids embarrassing media coverage.

Assessing Exposure

Network risk exposure would likely be considered a first-party risk, because revenues to a corporation would suffer as a result of a significant business-interruption loss. There is also potential liability exposure if corporate customers are dependent on your network and/or your applications for some business need.

This risk exposure should also be elevated on the list of concerns for the risk manager whose company requires 24-hour networking availability in order to conduct business and meet the demands of customers or partners.

Thus, a risk manager may want to answer these questions: How important is the corporate computer network in terms of ensuring that the network is always on and connected? Should an attack occur, how long can the business afford to have the network down before it becomes a serious issue? Might other networks or services contribute to or cause a future loss? Might customers or partners be affected should the network crash for a sustained period?

For the risk manager seeking to cede all or part of the exposure, he or she may want to consider a cyberrisk policy that specifically covers “cyberextortion.”

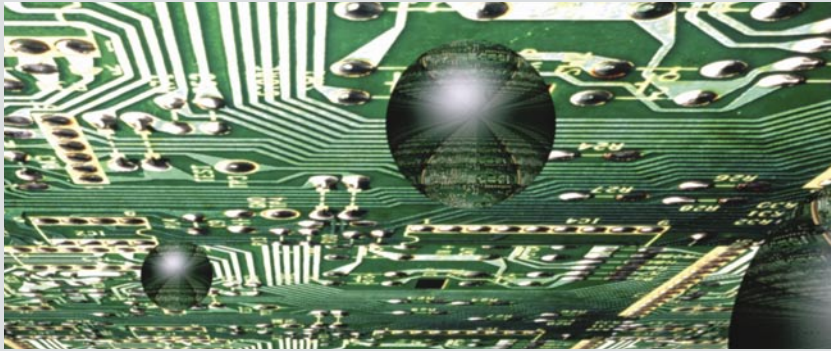
Carriers starting to cover this exposure include Ace USA, AIG, Arch (Digital Risk Managers), Chubb, Zurich, and various London syndicates, such as Hiscox and JLT Risk Solutions. Policies often reimburse the insured for the financial payout to an extortion attack. Limits or sublimits range from \$250,000 to more than \$20 million.

There are few conditions and exclusions that would degrade coverage beyond some commonsense elements, such as the immediate notice and written approval by the insurer.

Three example policies that cover this peril include the “WebNet” form from Digital Risk Managers (Arch), which offers to pay for extortion monies and/or extortion expenses incurred as a result of any extortion threat that began during the policy period. No deductible applies to this coverage.

Ace USA offers its version, known as the “Digitech” form, and AIG’s version is the “NetAdvantage Security” form.

—Mark Greisiger



Attackers are clever, and parse out their greed. They may launch a small attack designed just to show the victim what could happen if they don’t cooperate and pay the ransom, nor do they typically ask for a huge amount in ransom. They demand just enough to make sure they can fly under the radar, get paid and move on to the next victim. These demands serve as a warning, and send a message to the

victims that if they don’t cooperate, the attacker has the ability to bring the network to its knees.

Indeed, once launched, a denial-of-service campaign can result in a network outage spanning hours, days or even weeks.

Here’s an example of how such a denial-of-service attack works. An initial attack is launched against a business transaction server, one that belongs to, for instance,



CRIMINAL HACKERS LOVE TO HIJACK POROUS AND VULNERABLE CORPORATE COMPUTER NETWORKS WITH AN ONSLAUGHT FROM A SILICON ARMY OF MALICIOUS ‘BOTS’ ... THAT CAN RUIN A CORPORATE COMPUTER SYSTEM.

—Mark Greisiger, president, NetDiligence

a bank’s Internet platform. This results in a “short crash” of the electronic-banking application server. Retail and small-business customers can’t connect to the servers to complete transactions. The attack is immediately followed by an e-mail from the villain to the CEO demanding a \$20,000 wire transfer into a foreign bank account, *or else*. The explicit threat is—if you do not pay now, you risk yet another, even more powerful and longer-lasting attack, which will bring your network operations down for weeks, rather than just minutes. This belligerent tactic is effective, and companies often pay rather than fight. This also creates a major dilemma for the risk management department. It brings up an ethical issue: Should corporations pay and trust criminals not to attack their network during a peak season again? If a corporation pays, does that help them buy time to address and remedy this crisis for a later date? What should you do? How does the corporation stave off future attacks?

MITIGATION STRATEGIES

Unfortunately, there are no clear answers. Professional opinions

differ on courses of action, mainly because there are no real experts in this niche area yet.

Be that as it may, risk managers can start with an independent security assessment to understand their company’s preparedness and to understand their organization’s strengths and weaknesses.

Risk management departments need to find out if their information technology security team is confident in their existing prevention controls and if their company’s public-facing transaction Web sites can deflect a massive denial-of-service attack.

Regardless of whether they have cyberextortion insurance coverage in their network risk policy, risk managers may want to take some measures before Bots do damage.

Risk management departments should deploy an internal incident/emergency team and IR/BCP plan, and contact the legal department for counsel on any legal ramifications.

Risk managers, working with their IT counterparts, should also contact their corporation’s Internet service provider to address bandwidth consumption and attack issues.

If network availability is vital to

their business, they should ensure that prudent security controls—including network/application redundancies—are in place which can help keep networks functional during a sustained attack.

If a company's ISP/ASP has firsthand experience in defeating denial-of-service incidents in the past, the ISP might be able to help in mitigating the attack.

One tactic is to thwart the attack long enough for the perpetrator to either give up and move on to an easier target. This might not work, however, with a determined attacker wielding a large Bot network.

Risk managers work with ISPs to increase a company's bandwidth, and to assist in the deflection of such attacks. Upward of 10 times more bandwidth than normal might be needed during the peak periods of an attack.

Paul Williams, president and chief technology officer of Gray Hat Research Corp., says that for companies looking to design their own defense, that among other defenses bandwidth-on-demand agreements with Internet service providers are essential. He recommends checking with ISPs to see if they offer denial-of-service mitigation equipment.

As another defensive step, "the firewall should have denial-of-service defense rules added to limit the maximum number of permitted and attempted connections to each Internet-facing server and resource," he says.

Vendors such as Akamai, Riverhead Networks (now part of Cisco Systems), Top Layer, Mazu Networks, Arbor Networks, Captus Networks, Foundry and Juniper

Networks offer firewall devices.

When dealing with an actual case of extortion where attackers ask for money, risk managers should be sure to contact police and local FBI cybercrime special agent for help. This is vital, as they deal with these issues on a daily basis.

The FBI will most likely advise against making any type of extortion payment for many reasons, the first being that it sets a precedent and corporations may be locking themselves into a payment plan for life.

The FBI, unfortunately, will probably not be able to help you defend your network from an attack, nor will they be responsible for the impact of such an attack to bottom lines and shareholders.

If risk managers have a network risk policy that covers the payment for an extortion demand, they may want to check with their broker to see if there are any applicable conditions, such as contacting the FBI, or other limitations.

And, finally, to defend against any future sustained denial-of-

service threat, risk professionals need to prepare and invest in software and systems designed to prevent denial-of-service incidents, such as from Cisco Systems and Mazu Networks. Prevention solutions start at \$30,000. It's expensive, sometimes too expensive, but at the very least it should be factored into any risk management strategy designed to protect a company.

MARK GREISIGER is the president of NetDiligence. He can be reached at riskletters@lrp.com.

Two of an Evil Kind: Denial of Service Defined

A denial-of-service attack is an attack in which a company is deprived of its network/computer application or connection resources. The most common kind of denial-of-service attack is when the bad guys simply send more data traffic to a network Web site than its data buffers can handle. This may result in slower computers. Other times computers may crash outright. For example, a Web site accessed by millions of hits can be forced to temporarily cease operation.

This attack often can morph into a "distributed" threat, a distributed denial-of-service attack when the attacker's Bot network can number in the tens of thousands of slave computers, and are located anywhere in the world. Such an attack is harder to defend against because security firewalls need to be strong enough to decipher valuable data traffic—customer orders, for example—from malicious data. Herein lies the problem.

—Mark Greisiger