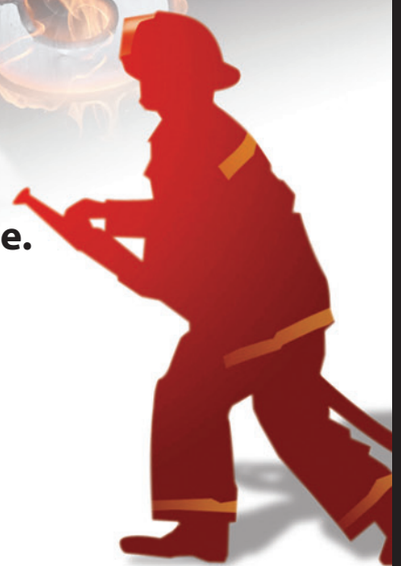
SECURITY
dark READING
JULY 2012
Protect The Business Enable Access

Next

DDoS Mitigation

Save Your ASSETS



Distributed denial-of-service attacks can do serious damage. Get ready before there's a flare-up. >>

By Kurt Marko

PLUS

UBM TechWeb

darkreading.com

dark READING

July 2012 Issue 7

CONTENTS

COVER STORY

Save Your Assets

Distributed denial-of-service attacks can do serious damage. Get ready before there's a flare-up. p. 8

DARK DOMINION

New Age Of Political Hacktivism

Next-gen attackers aren't out to steal your money, and your old style of defense isn't going to stop them p. 3

QUICKTAKES

DNSChanger Threat Could Re-Emerge

Temporary servers and efforts from ISPs have helped fight the Trojan, but problems aren't over p. 4

Critical Infrastructure Targeted

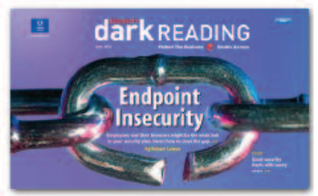
Banks, utilities, and other parts of the U.S. critical infrastructure face more cybersecurity threats p. 6

More From Dark Reading

Close The Door On Data Leaks

Stop insider theft and accidental disclosure with network and host controls—and don't forget to keep employees on their toes.

darkreading.com/issue/april2012



Endpoint Insecurity

Employees and their browsers might be the weak link in your security plan. Here's how to strengthen them and keep your company safe.

darkreading.com/issue/may2012

IN-DEPTH REPORTS

Measuring Risk: A Security Pro's Guide

One of the biggest challenges facing IT is risk assessment. Check out the tools available for evaluating security risks and get ideas on how to use the resulting data.

darkreading.com/reports/measurerisk

Lessons Learned From Duqu

While your company may be able to avoid the malware known as Duqu, variants and copycats are real, imminent threats.

darkreading.com/reports/duqu

DARK DOMINION

The New Age Of Political Hacktivism

TIM WILSON

Not so long ago, there were only two types of attackers aiming at enterprise systems: cybercriminals seeking to steal money and data, and hacker hobbyists trying to penetrate corporate defenses to get recognition from other hackers.

Ah, the good old days.

Today, the threats have radically changed. In addition to cybercriminals and cyberpunks, there's a range of politically motivated attackers, including disgruntled individuals, loosely organized "hacktivist" groups, and organized attacks by nation states.

These new-style attackers aren't out to steal money or customer data. Instead, they want to get your goat, disrupt your operations, publish your sensitive information, or steal your intellectual property. Their purposes and their methods differ, but one thing is clear: Defenses designed to stop cybercriminals and joy riders aren't enough anymore.

In the past, companies have followed a simple security premise: Follow the money. If the systems and applications involved funds transfer, personally identifiable information, or company secrets, they got top priority. If they didn't, you could get by with minimum defenses.

The follow-the-money strategy may not work anymore. Politically motivated attackers use distributed denial-of-service attacks as a form of protest, a way to make a statement against a company or other organization. DDoS isn't usually about money; it's about showing up the victim.

Whether DDoS is a legitimate form of protest or a cowardly criminal act is up for debate—and the subject of a different column. For now, we must accept that these attacks will happen. Several studies indicate that companies are regularly experiencing them, and Verizon Business' Data Breach Investigation Report suggests that hacktivism is one of the fastest-growing causes of major security breaches.

And it's not just DDoS. In recent months, we've seen many organizations being "doxed," where their email or other sensitive documents are stolen and published on the Internet. The criminals don't get money or fame from these attacks; they simply expose the victim organization and make it look bad.

We've also seen instances of cyber espionage, including repeated attacks on U.S. government systems by entities in China and the Stuxnet attack on Iranian nuclear facilities. Those are only the tip of the problem. If your organization harbors data that might be useful in some way to another country, you could be the target of a politically motivated intrusion by a foreign government or terrorist or nationalist group.

To cope with these new motives and methods, rethink your defenses. You'll need to doubly protect all Internet-facing systems and watch for attacks designed to disrupt your operations. Politically motivated attacks can be just as damaging as financial and data theft. Be sure that your security architecture protects you from them—or be prepared to explain why it didn't.

Tim Wilson is editor of DarkReading.com. Write to him at wilson@darkreading.com.

QUICKTAKES

QUICKFACT
210,000 DNSChanger Trojan victims that remain

CYBERSECURITY

DNSChanger Threat Could Re-Emerge

When the FBI recently shut down the temporary DNS servers keeping users infected with the DNSChanger Trojan online, just over 210,000 unique IP victims remained around the world, according to the DNSChanger Working Group, which was formed to support the cleanup after the DNSChanger attack. That's a far cry from the millions of victims initially estimated to have been hit by the nasty malware. But the threat is far from over, security experts say.

In addition to the FBI's temporary servers, many ISPs have waged aggressive campaigns to alert users and offer help to clean up their machines. And some deployed their own DNS backup servers for stragglers.

"The message about endpoint security is the real issue—is the underlying malware on your system and how did it get there?"

—Dan Brown, Bit9

These ISP backup servers are potentially a problem, says Paul Vixie, chairman and founder of the Internet Systems Consortium, which ran and managed the servers for the FBI. While they're keeping infected users from losing their DNS, he says, they're also masking the danger. It's like pulling off a Band-Aid slowly "The idea is to rip it off" instead, Vixie says.

The temporary DNS servers and the ISP awareness campaigns were successful—Infections went down 50%. But diminishing returns have set in, Vixie says. "Every one of those still-infected machines is a danger to its owner and to the rest of us. Given how easily targetable they are, I'm worried about the 210,000 still out there," he says.

The ISPs are essentially expanding the deadline on their own, says Dan Brown, director of security research at Bit9, a security products provider. But that's extending the infection, he says. It's enabling victims and obscuring the real lessons. "Some of the more important security lessons were pushed under the rug," he says. "One thing that happens is when you find malware, it's often not the only malware on that system."

That's the case with DNSChanger, which experts say was often a secondary infection to the TDSS malware with its botnet that instructed the machine to download DNSChanger.

The Shutdown

July 9 was the deadline for turning off the temporary servers that have been keeping infected users on the Internet. ISP efforts to find and help infected users have yielded results: Internet Identity, a provider of Internet security technology and services, saw a 10% to 20% decrease in the number of infected IP addresses in the week leading up to the server shut-off.

The FBI's "Operation Ghost Click" last year dismantled DNSChanger and led to the indictment of six Estonians and one Russian allegedly involved in infecting users and redirecting their computers to phony websites in a click-fraud scam. There were initially millions of infected machines, and the malware has been around

QUICKTAKES

for several years, initially targeting home routers.

Comcast says it received a "miniscule" number of calls from infected users right after the shutdown; it initially estimated that less than one-tenth of 1% of its customers would be affected. "For months, we have been emailing, mailing letters, sending in-browser notifications, and even calling customers who we thought might be impacted and urged them to take action," a spokesman says. They could download a free security patch or get fee-based professional help. Comcast didn't provide a backup DNS service for infected machines.

Another factor that may have lit a fire under some complacent victims was a "brownout" of the temporary FBI DNS servers that occurred a couple of months ago, says Rod Rasmussen, president and CTO of IID. That got some people to pay attention, he says.

But like any other potent malware, DNSChanger is likely to be recycled and retooled, so this won't be the last of it.

"The good news is that it was not the Armageddon that some had predicted," Bit9's Brown says. "The message about endpoint security is the real issue—is the underlying malware on your system and how did it get there?" And if this malware ended up in your corporate environment, Brown says, even though it was intended for consumers, it says something about your security posture.

—Kelly Jackson Higgins (higgins@darkreading.com)

QUICKTAKES

CYBERATTACKS

Critical Infrastructure Industries Targeted

U.S. critical infrastructure companies, including utilities, banks, and communications and transportation companies, have seen a dramatic increase in the number of reported cybersecurity incidents since 2009, according to a report from the U.S. Industrial Control Systems Cyber Emergency Response Team.

The response team handled nine incident reports in 2009. That number increased to 41 in 2010 and 198 in 2011. Of those 198, seven resulted in ICS-CERT deploying incident response teams on-site, and another 21 required remote analysis by ICS-CERT's Advanced Analytics Lab.

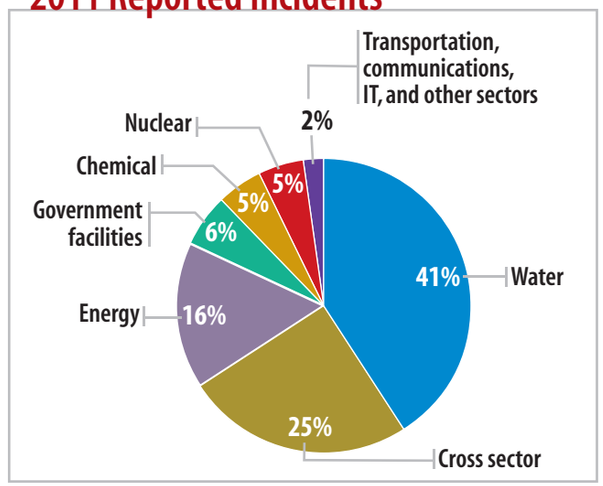
Eighty-one of the incidents (41%) were specific to the water sector. The prevalence of incidents in that sector is thought to be due to a larger number of Internet-facing control system devices used, the report says.

While not all of the reported incidents turned out to be actual attacks, the magnitude of the increase in reports is somewhat surprising, says Kim Legelis, VP of marketing at Industrial Defender, which provides industrial control systems. People close to critical infrastructure cybersecurity were aware of the increase in threats, she says, but the level of the increase was "more severe than expected."

All told, ICS-CERT performed 17 on-site assessments during the three years covered by the report. Spear phishing—email spoofing that targets a specific group of people or an organization—was the most common attack vector for network intrusion; it accounted for seven of the 17 incidents. "Sophisticated threat actors" were tied to 11 of the incidents, the report says, with the goal in several cases being data theft.

No actual intrusions into control system networks were identified. But, the report

2011 Reported Incidents



Data: ICS-CERT

QUICKTAKES

says, given the flat and interconnected nature of the networks in many of these organizations, once attackers gain access they can move into other parts of the network, including the control system, where they could compromise critical infrastructure operations.

In 12 of the 17 cases involving on-site assessments, implementing security best practices such as login limitations and properly configured firewalls could have deterred the attack, minimized the time taken to detect it, or reduced its impact, ICS-CERT says. Ten organizations could have detected an intrusion by using ingress/egress filtering of known bad IP addresses and domain names. In three cases, asset owners had been notified of a cyberattack or intrusion by external organizations, and in two other cases, the incidents had been identified by a third-party consultant or an integrator.

People close to critical infrastructure cybersecurity were aware of the increase in threats, but the level of the increase was "more severe than expected."

—Kim Legelis, Industrial Defender

—Brian Prince (editors@darkreading.com)

DDoS Mitigation

Save Your ASSETS

Distributed denial-of-service attacks can do serious damage. Get ready before there's a flare-up.

By Kurt Marko

Late last month, two members of the hacker group LulzSec pleaded guilty to launching distributed denial-of-service (DDoS) attacks against entities ranging from the state of Arizona to Nintendo to the CIA. Yet despite extensive media coverage of such attacks, chief information security officers are still surprised when their companies get hit.

This is not an unforeseeable lightning bolt from the blue, people. The cyber world is full of anonymous arsonists, and too many businesses are operating without a fire department on call. A few sprinklers won't cut it when things flare out of control. Firewalls and intrusion-

prevention system appliances are no substitute for specialized DDoS backup when an attack escalates.

Proactively securing a mitigation service can be a good insurance policy—in fact, it's better than insurance, which pays off only after damage is done. That's because mitigation services are designed to prevent destruction from occurring in the first place. Not only can a mitigation service act as a deterrent—many attackers will move on to easier prey when they see an initial DDoS attack fail—but these providers have the capacity and expertise to rapidly scale DDoS countermeasures against coordinated, professional attacks. That can mean keeping your website online even under heavy bombardment.

Big And Small Companies At Risk

Denial-of-service attacks used to be something that happened to other people, those with high online visibility. Not anymore. "We've seen very small companies come to us and they can't figure out why they're under attack," says Chris Richter, VP of security products and services at Savvis. They ask, " 'What have we done?' "

Blame the proliferation of prepackaged DDoS toolkits, such as the Low Orbit Ion Cannon and Dirt Jumper, for the fact that no one's safe. Like any brute-force tactic, DDoS relies on the fact that any attack, even the most rudimentary, repeated with sufficient volume and frequency, can effectively shut down a network or website. Botnets often span thousands or millions of systems worldwide; Akamai, for example, provides a real-time attack heat map. In early July, attack rates were almost 30% above normal, with hot spots in Delaware and Italy. Geographic dispersion, coupled with network traffic crafted to look like legitimate connections from normal users, makes DDoS attacks both extremely effective and difficult to defeat if you're not an expert with the right tools.

There are three main distributed denial-of-service categories:

>> Volumetric attacks overwhelm WAN circuits with tens of gigabits per second of meaningless traffic—so-called ICMP or UDP floods.

>> Layer 3 attacks abuse TCP. For example,

DDoS By The Numbers

10 Maximum sentence in years on second conviction under U.S. Computer Fraud and Abuse Act.

$5K CFAA threshold for damages to constitute a felony.

$240K Average cost, in revenue per day, of an attack for 65% of 1,000 respondents to a Neustar poll.

25% Increase in DDoS attacks for 1Q 2012 over 1Q 2011, according to Prolexic's most recent Attack Report.

SYN floods overload network equipment by starting but never completing thousands of TCP sessions using forged sender addresses. SYN floods can be in excess of 1 million packets per second, largely in response to the wider deployment of hardware countermeasures on firewalls and other security appliances, says Neal Quinn, COO of DDoS mitigation specialist Prolexic.

>> Layer 7 floods use HTTP GET or POST requests to overload application and Web servers. From the attacker's perspective, L7 exploits aren't anonymous. The attacking client's identity (IP address) is exposed because a TCP handshake must be completed. Attackers who use this approach consider the risk outweighed by the technique's effectiveness at much lower volumes and the traffic's stealthy nature. Requests are designed to look like normal Web traffic, factors that make L7 attacks hard to detect.

Our *InformationWeek* 2012 Strategic Security Survey shows that the increasing sophistication of threats is the most-cited reason for worry among respondents who say their orgs are more vulnerable now than in 2011, and L7 attacks are certainly sophisticated. They're also getting more common: Mark Teolis, founder and CEO of DOSarrest, a DDoS mitigation service, says 85% of the attacks his company sees have a Layer 7 component. Attackers leveraging L7 are often developers; they may do some reconnaissance on a website, looking for page requests that aren't cacheable and are very CPU-intensive—things like filling a shopping cart, searching a database, or posting a complex form.

Teolis says that a mere 2 to 3 Mbps increase in specially crafted L7 traffic can be crippling. "We've had gaming sites tell us they can handle 30,000 customers, but if 100 hit this one thing, it'll bring down the entire site," he says.

Layer 7 attacks are tough to defeat not only because the incremental traffic is minimal, but because it mimics normal user behavior. Teolis has seen attacks where an individual bot may hit a site only once or twice an hour—but there are 20,000 bots involved. Conventional network security appliances just can't handle that kind of scenario. And meanwhile, legitimate customers can't reach your site.

Biggest Threats

Security threats ranked from 1, "greatest threat," to 6, "lowest threat"

	Rank
Organized cybercriminals or hacktivists	1
Insiders	2
Foreign states	3
Accidental disclosure from service providers or partners	4
Terrorists	5
Lone-wolf hackers	6

Data: *InformationWeek* 2012 Federal Government Cybersecurity Survey of 106 federal government technology professionals, March 2012

Why Us?

The motivations for a DDoS attack are as varied as the perpetrators. For many, it's just business, with targets strategically chosen by cyber criminals. Others are political—a prime example is LulzSec hitting the Arizona Department of Public Safety to protest the state's strict immigration law, SB 1070. And for some, it's just sport.

Given this randomness, it's impossible to predict the need for professional distributed denial-of-service mitigation. For example, Teolis says one of DOSarrest's customers was the Dog Whisperer, that guru of man's best friend. "If Cesar Millan can get at-

tacked, anyone is fair game," he says.

Purchasing mitigation services requires the same kind of budgeting as any form of IT security: What you spend on controls should be proportional to the value of the data or website. So, while any organization with an online presence is at some risk, those with financial or reputational assets that could be seriously damaged by going dark should take DDoS mitigation most seriously.

Everyone should take these preparatory steps.

>> Do online reconnaissance: Follow what's being said about your company online, particularly on public social networks, and look for chatter that might hint at extortion or hacktivism. Subscribe to security threat assessment reports covering the latest DDoS techniques and incidents. Prolexic is one source for threat advisories; US-CERT also has overviews, like this one on Anonymous.

>> Heed threat mitigation recommendations: DDoS threat reports typically include details about the attack signature and recommended mitigation steps. For example, a recent Prolexic report on the High Orbit Ion Cannon identifies specific attack signatures, in this case HTTP requests, and content filter rules to block them. For L3/L4 attacks, incorporate these rules into your firewall; do likewise for L7 attacks if your firewall supports application-layer filtering.

>> Have a communications strategy: Know what you'll tell employees, customers, and the media

should you be the victim of an attack. Don't wait to make statements up on the fly.

>> Have an emergency mitigation backup plan: Although most DDoS mitigation services operate on a monthly subscription basis, if you haven't signed up and an attack overwhelms your defenses, at least know who you're gonna call. Quinn and Teolis say their services can be operational and filtering DDoS traffic within minutes, though of course it will cost you.

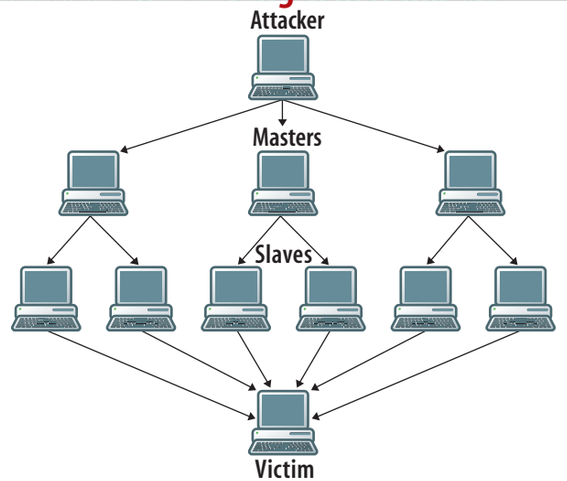
What To Look For In DDoS Mitigation

At the risk of oversimplification, DDoS mitigation services are fundamentally remote network traffic filters. Once your system detects an attack affecting your network or servers, you redirect traffic to the service; the service filters out the junk and passes legitimate packets to their original destinations. In this sense, it's like a cloud-based spam filter for websites.

This traffic redirection, so-called on-ramping, is typically done via DNS. The mitigation provider creates a virtual IP address, the customer makes a DNS A record (hostname) change pointing to the remote VIPA, traffic flows through the mitigation provider's filters, and the provider forwards only legitimate traffic on to the original site. Those facing attacks on multiple systems can divert entire subnets using Border Gateway Protocol advertisements, using Generic Routing Encapsulation tunneling to direct traffic to the mitigation provider. Advertising a new route to an entire address block protects an entire group of machines and, says Quinn, has the advantage of being asymmetrical, in that the mitigation service is used only for inbound traffic.

The most important DDoS mitigation features are breadth of attack coverage, speed of service initiation (traffic on-ramping), and traffic capacity. Given the increasing popularity of application-layer attacks, any service should include both L3/4 and L7 mitigation technology. Services may segment features into proactive, before-the-attack monitoring and

DDoS Botnet: Strength In Numbers



The most common distributed denial-of-service attack source is a botnet. Traffic comes from slave systems, typically PCs compromised with malware. The attack is initiated by instructions sent to one or more master servers, which could also be malware-infected systems running control software. These servers instruct the slaves about the type, target, and duration of attack.

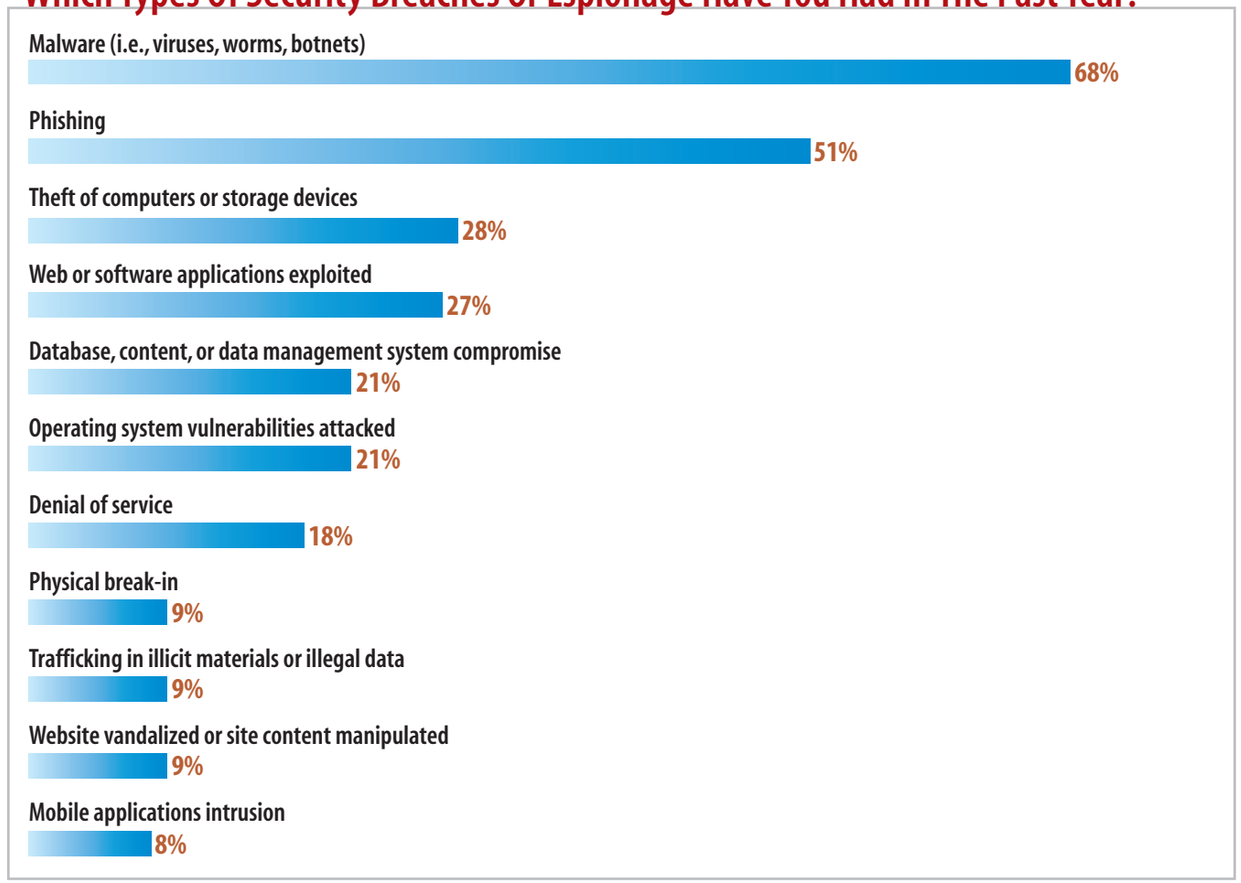
reactive, during-the-incident mitigation.

Customers with monthly subscriptions should demand typical and maximum mitigation times—measured in minutes, not hours—backed up by a service-level agreement with teeth. Even those procuring emergency mitigation services should expect fairly rapid response. Most DDoS specialists staff operations centers 24/7.

With DDoS mitigation, procrastination can be expensive. For those 70% of customers who first turn to DOSarrest in an emergency, the setup fee for the first month is around $3,500 to $4,000, depending on the complexity of the site. In contrast, an average monthly cost on a subscription basis is $700 per public-facing IP address.

Filtered bandwidth is another way to differentiate between services. Some, like Prolexic, adopt an all-you-can-eat pricing model. For a flat fee per server, customers can use the service as often as they need with as much bandwidth as required. Others, like DOSarrest, keep the "use as often as you like" model but include only a certain amount of clean bandwidth (10 Mbps in its case) in the base subscription, charging extra for higher-bandwidth tiers. Teolis says 10 Mbps is sufficient for at least 90% of his company's customers.

Which Types Of Security Breaches Or Espionage Have You Had In The Past Year?



Data: *InformationWeek* 2012 Strategic Security Survey of 183 business technology and security professionals at organizations with 100 or more employees experiencing a security breach within the past year, March 2012

A few services use a pricing model akin to an attorney's retainer, with a low monthly subscription but hefty fees for each DDoS incident. Richter says Savvis is moving to this model, saying that customers want usage-based pricing that resembles other cloud services. Prolexic's Quinn counters that this pricing structure leads to unpredictable bills.

Bottom line, there's a DDoS service to suit

your tolerance for risk and budgetary volatility.

Optional services available from some providers include postattack analysis and forensics (what happened, from where, and by whom) and access to a managed network reputation database that tracks active botnets and sites linked to fraudulent or criminal activity, a feature that facilitates automated blacklisting to help prevent attacks in the first place.

Aside from looking at service features, evaluate each company's technical expertise and track record. DDoS mitigation specialists, for whom this is a core business (or perhaps their only business) arguably have more experience and focus than Internet service providers or managed security providers for which DDoS mitigation is just a sideline. Not surprisingly, Quinn, whose company was among the first to offer DDoS mitigation as a service, suggests customers should make vendors show evidence that DDoS mitigation is something they do regularly, not as a rare occurrence.

Make sure the service has highly qualified staff dedicated to the task. Ask whether the provider has experts available 24/7 and how long it will take to access someone with the technical ability and authority to work on your problem.

Unfortunately there's no rule of thumb for measuring the DDoS mitigation return on investment; it's really a case-by-case calculation based on the financial value of the site being attacked. It relies on factors

such as the cost in lost revenue or organizational reputation for every minute of downtime. Quinn cites a common analyst cost estimate, which Cisco also uses in its product marketing, of $30 million for a 24-hour outage at a large e-commerce site.

There's a cruel asymmetry to DDoS attacks: They can cost thousands to mitigate, inflict millions in damage, and yet attackers can launch them on the cheap. A small botnet can be rented for as little as $600 a month, meaning a serious, sustained attack against multiple targets can be pulled off for $5,000 or $10,000.

With damages potentially two or three orders of magnitude higher than the DDoS mitigation costs, many organizations are finding mitigation a worthwhile investment. In fact, three-quarters of DOSarrest's customers don't wait for a DDoS attack to flip the switch, but permanently filter all of their traffic through the service. That makes sense, particularly if it's a high-value or high-visibility site, if your traffic fits within the cap, or if you're using an uncapped service like Prolexic. These services use the same sorts of colocation hosting centers where companies would typically house public-facing websites, and they do geographically distributed load balancing and traffic routing to multiple data centers. That makes the risk of downtime on the provider's end minimal. And this approach could actually reduce WAN costs since it filters junk before it ever touches your systems.

Recommendations

If a mitigation service is too expensive, there are things IT can do to lower the exposure and limit the damage from DDoS attacks (discussed more in more depth in our full report):

1. Fortify your edge network: Ensure that firewall and IDS systems have DoS features turned on, including things like dropping spoofed or malformed packets, setting SYN, ICMP, and UDP flood drop thresholds, limiting connections per server and client, and dynamically filtering and automatically blocking (at least for a short time) clients sending bad packets.

2. Develop a whitelist of known good external systems: These include business partner gateways, ISP links and cloud providers. This ensures that stringent edge filtering, whether done on your firewall or by a DDoS service, lets good traffic through.

3. Perform regular audits and reviews of your edge devices: Look for anomalies like bandwidth spikes. This works best if the data is centrally collected and analyzed across every device in your network.

4. Understand how to identify DDoS traffic: Research attack signatures and have someone on your network team who knows how to use a packet sniffer to discriminate between legitimate and DDoS traffic.

5. Prepare DNS: Lower the DNS TTL for public-facing Web servers, since these are most likely to be attacked. If you need to protect an entire server subnet, have a plan to readvertise BGP routes to a mitigation service.

6. Keep public Web servers off your enterprise ISP link: With Web servers being the most common DDoS target, Michael Davis, CEO of Savid Technologies and a regular *InformationWeek* contributor, recommends Web hosting with a vendor that doesn't share your pipes. "Your website may be down, but at least the rest of your business is up," says Davis.

7. Practice good server and application security hygiene: Layer 7 attacks exploit operating system and application security flaws, often using buffer overflows to inject attack code into SQL databases or Web servers, so keep systems patched.

Kurt Marko is an IT pro with broad experience, from chip design to IT systems. Write to us at editors@darkreading.com.

dark READING *Online, Newsletters, Events, Research*

Tim Wilson Dark Reading Site Editor
wilson@darkreading.com 703-262-0680

Kelly Jackson-Higgins Dark Reading Senior Editor
higgins@darkreading.com 434-960-9899

Rob Preston VP and Editor In Chief
rpreston@techweb.com 516-562-5692

Chris Murphy Editor
cjmurphy@techweb.com 414-906-5331

Stacey Peterson Executive Editor, Quality
speterson@techweb.com 516-562-5933

Lorna Garey Content Director, Reports
lgarey@techweb.com 978-694-1681

Jim Donahue Chief Copy Editor
jdonahue@techweb.com

Mary Ellen Forte Senior Art Director
mforte@techweb.com

Sek Leung Associate Art Director
sleung@techweb.com

Business Contacts

VP of Group Sales, InformationWeek Business Technology Network, Martha Schwartz
(212) 600-3015, mschwartz@techweb.com

Sales Assistant, Salvatore Silletti
(212) 600-3327, ssilletti@techweb.com

SALES CONTACTS—WEST

Western U.S. (Pacific and Mountain states) and Western Canada (British Columbia, Alberta)

Western Regional Sales Director, Kevin Bennett
(415) 947-6139, kbennett@techweb.com

Account Manager, Ashley Cohen
(415) 947-6349, aicohen@techweb.com

Strategic Accounts

Account Director, Sandra Kupiec
(415) 947-6922, skupiec@techweb.com

SALES CONTACTS—EAST

Midwest, South, Northeast U.S. and Eastern Canada (Saskatchewan, Ontario, Quebec, New Brunswick)

District Manager, Jenny Hanna
(516) 562-5116, jhanna@techweb.com

District Manager, Michael Greenhut
(516) 562-5044, mgreenhut@techweb.com

District Manager, Cori Gordon
(516) 562-5181, cgordon@techweb.com

Inside Sales Manager East, Ray Capitelli
(212) 600-3045, rcapitelli@techweb.com

Strategic Accounts

District Manager, Mary Hyland
(516) 562-5120, mhyland@techweb.com

Account Manager, Tara Bradeen
(212) 600-3347, tbradeen@techweb.com

SALES CONTACTS—MARKETING AS A SERVICE

Director of Client Marketing Strategy, Jonathan Vlock
(212) 600-3019, jvlock@techweb.com

Director of Client Marketing Strategy, Julie Supinski
(415) 947-6887, jsupinski@techweb.com

SALES CONTACTS—EVENTS

Senior Director, InformationWeek Events, Robyn Duda
(212) 600-3046, rduda@techweb.com

MARKETING

VP, Marketing, Winnie Ng-Schuchman
(631) 406-6507, wng@techweb.com

Senior Marketing Manager, Monique Kakegawa
(949) 223-3609, mkakegawa@techweb.com

Promotions Manager, Angela Lee-Moll
(516) 562-5803, aleemoll@techweb.com

UBM TECHWEB

John Dennehy CFO

David Michael CIO

Scott Vaughan CMO

David Berlind Chief Content Officer, TechWeb, and Editor in Chief, TechWeb.com

Ed Grossman Executive VP, InformationWeek Business Technology Network

Martha Schwartz VP, Group Sales, InformationWeek Business Technology Network

Joseph Braue Sr. VP, Light Reading Communications Network

Beth Rivera Senior VP, Human Resources

John Ecke VP of Brand and Product Development, InformationWeek Business Technology Network

Fritz Nelson VP, Editorial Director, InformationWeek Business Technology Network, and Executive Producer, TechWeb TV

UBM LLC

Pat Nohilly Sr. VP, Strategic Development and Business Admin.

Marie Myers Sr. VP, Manufacturing

READER SERVICES

DarkReading.com The destination for the latest news on IT security threats, technology, and best practices

Electronic Newsletters Subscribe to Dark Reading's daily newsletter and other newsletters at darkreading.com/newsletters/subscribe.jhtml

Events Get the latest on our live events and Net events at informationweek.com/events

Reports reports.informationweek.com for original research and strategic advice

How to Contact Us
darkreading.com/aboutus_editorial.jhtml

Editorial Calendar informationweek.com/edcal

Back Issues
E-mail: customerservice@informationweek.com
Phone: 888-664-3332 (U.S.)
847-763-9588 (Outside U.S.)

Reprints Wright's Media, 1-877-652-5295
Web: wrightsmedia.com/reprints/?magid=2196
E-mail: ubmreprints@wrightsmedia.com

List Rentals Specialists Marketing Services Inc.
E-mail: PeterCan@SMS-Inc.com
Phone: (631) 787-3008 x30203

Media Kits and Advertising Contacts
createyournextcustomer.com/contact-us

Letters to the Editor E-mail editors@darkreading.com. Include name, title, company, city, and daytime phone number.

Subscriptions
Web: informationweek.com/magazine
E-mail: customerservice@informationweek.com
Phone: 888-664-3332 (U.S.)
847-763-9588 (Outside U.S.)

UBM TechWeb