Sponsored by

VERISIGN™

WEB THREATS, SECURITY, AND DDoS

Due to the constantly changing threat landscape, keeping corporate networks secure is particularly tricky these days. Threats continue to increase and evolve as attackers attempt to stay one step ahead of their targets, employing new technology, social engineering scams, and the element of surprise. Distributed Denial-of-Service (DDoS) attacks continue to plague organizations, while newer strategies such as advanced persistent threats (APTs) and spear phishing are becoming more common. In these articles, *Network World* and its sister publications *CSO, CIO, InfoWorld*, and *Computerworld* offer news, advice, and commentary on securing modern enterprise IT environments.

IN THIS eGUIDE

WHAT IT'S LIKE TO GET HIT WITH A DDoS ATTACK

Bill Brenner • CSO

Akamai often finds itself scrambling to stop a DDoS attack against one or more of its clients

Google. Twitter. Government websites. Fortune 500 companies. All have been victims of crippling distributed denial-of-service (DDoS) attacks. The attacks have grown in reach and intensity thanks to botnets and a bounty of application flaws. And Akamai Technologies has a seen it all firsthand.

Many people use Akamai services without even realizing it. The company runs a global platform with thousands of servers that customers rely on to do business online. The company currently handles tens of billions of daily Web interactions for such companies as Audi, Fujitsu and NBC, and organizations like the Department of Defense and Nasdaq. There's rarely a moment—if there are any—when an Akamai customer is not under the DDoS gun.

So what's it like to be in charge of this much computing power when the attacker decides to strike? Akamai Security Evangelist Michael Smith recently took an audience at the SecTor security conference through a blow-by-blow account of some recent high-profile cases.

Taking center stage is the massive cyberattack on government websites and others around the world during the Fourth of July long weekend in 2009. In that onslaught, a botnet of some 180,000 hijacked computers hammered U.S. government websites and caused headaches for businesses here and in South Korea.

The attack started that Saturday, knocking out websites for the Federal Trade Commission and the Department of Transportation. U.S. Bancorp, the nation's sixth-largest commercial bank, also took a direct hit. Attackers have also targeted the likes of Amazon, Google and Yahoo. Attacks against Google didn't last long, but when one considers that Google content accounts for about 5 percent of all Internet traffic, the prospect of better-sustained attacks against it is sobering.

When a DDoS is underway, Smith said, customers panic some, but it's not the freak-out you might expect.

"There is a bit of panic if the traffic starts hitting your infrastructure because things start failing over. So you're doing the usual 'restore service' drill, but it's going in multiple directions, and then it seems like all of your infrastructure is in a cascade failure," he said. "Maybe a better way to describe it is that you're scrambling to fix stuff and you don't really have time to panic."

Even in an Akamai environment, if the attackers target dynamic content—which is set to not cache—that goes through

Akamai back to your origin, you'll see a traffic spike with your servers, Smith said. "Obviously we have ways to respond after that by caching the dynamic traffic for a small amount of seconds—most dynamic content is actually cacheable for a small period of time because the browser isn't loading it every 3 milliseconds like you might think," he says.

And some people don't panic because they may have been warned of the attack. If you're the target of an activist or protester attack, you might hear about it beforehand as they make plans via online forums.

"There has to be some panic, but then you calm down and realize it's manageable because you have time to react," Smith says. "But during the first 30 minutes of the attack, you're still sitting with your fingers crossed watching to see if anything gets through your defenses." •

PONEMON STUDY: CYBER ATTACKS MORE FREQUENT, SEVERE

Tim Greene • Network World

Most respondents say they expect to be hit again this year

Cyber attacks are becoming more frequent and severe, and the vast majority of businesses have suffered at least one data breach in the past year, a Ponemon Institute survey says.

According to the survey, 77% of respondents say attacks have been more severe or more difficult to prevent over the past 12 to 18 months, while 78% say attacks are more frequent. The survey was sponsored by Juniper Networks.

Only 10% of those who answered the survey say they had no data breaches and 53% say they had one to three.

Given these numbers, 53% have low confidence that their networks would avoid attacks in the next year; 24% say they have high confidence they won't suffer attacks, the survey says. A third (34%) have low confidence their network infrastructure can protect against attacks.

"We believe the fact that so many organizations are having multiple breaches is resulting in a low opinion about security preparedness and a low level of confidence they have to prevent a future attack," the survey says.

The cost of 55% of the breaches was between $250,000 and $1 million, with 19% saying the cost was more than that, and 16% saying they couldn't determine what their breaches cost.

Most of the incursions took place on mobile devices (28%) or on devices owned by business partners (27%). Another 20% took place in corporate branch offices and 16% at headquarters.

Of those companies that did suffer attacks, 40% don't know where the attacks came from. The top three causes of security breaches are insider abuse, malicious software downloads and malware from a Web site.

Employee laptops were the most common (34%) endpoint from which security breaches occurred followed by mobile devices such as tablets and smartphones (29%) and corporate desktops (28%). •

PAYPAL CISO: DDoS ONE BIG SECURITY THREAT AMONG MANY

Tim Greene • Network World

PayPal CISO Michael Barrett also urges other security pros to advise Congress on Internet security legislation

Stung by a high-profile denial-of-service attack in December, PayPal's CISO says application layer attacks remain a major threat to businesses in general, which need better defenses and actual testing of the DDoS tools they have.

"We need better planning as an industry," says Michael Barrett, the CISO of PayPal, whose blog site was knocked offline late last year by the political hacking group Anonymous.

During a recent interview with Network World about his major security concerns and priorities for 2011, Barrett also listed advanced persistent threats (APT) as a major worry and the need for legislation to improve Internet security. In addition, he says that the payment card industry (PCI) standards for protecting credit card information need some tweaking to give businesses more flexibility without hurting security.

But as for DDoS attacks, businesses need to plan defenses and confirm how well they will handle real attacks to live networks, Barrett says, because tests in simulated environments don't scale large enough to adequately stress the defenses.

Another problem is that testing the actual network gets in the way of doing business. "We have to do more testing, but we haven't figured out how," Barrett says. "You can't shut off the Internet for a significant length of time."

As for APTs, Barrett says they pose two big problems: how to detect them since they are typically hard to find with signature-based tools, and what to do about them when they are found. APT code is designed to burrow into networks and resist eradication so even if one instance is discovered and cleaned, others remain to carry out malicious activity, he says.

A piece of malware found on a PC, for example, could be a simple virus infecting one machine or it could be the sign of something more sinister trying to steal intellectual property or customer records. An APT sent by a determined adversary likely means there is also a backdoor to let in more malware, he says.

"If you react to one backdoor at a time, you wind up

IT'S WHAT YOU DON'T KNOW

"Many CISOs have been operating on the assumption that since they didn't know of anything, there wasn't anything,"

— Michael Barrett, CISO, PayPal

playing a game of whack-a-mole," he says. Plus taking down just one instance of an APT and leaving the rest may tip off the attacker that it's time to enter the next phase of the attack, he says. Honey pots can help determine the nature of discovered threats and whether they represent random infections or sophisticated targeted attacks, Barrett says.

One piece of the solution is better network-based detection tools to augment e-mail, Web proxies, antivirus and anti-malware applications. These additional detection tools should seek anomalous behaviors networkwide so corrupted machines can be found and cleaned all at once to eradicate the APT, he says.

The true size of APT infection is difficult to know because it is so stealthy. "Many CISOs have been operating on the assumption that since they didn't know of anything, there wasn't anything," Barrett says.

On the matter of PCI standards, he feels that businesses need more flexibility in implementing security measures that guard against identified threats. The standards which have been criticized for driving the bulk of security spending for those companies that must comply with them, could use some refinement, he says.

Overall they address important concerns and impose security measures that can only benefit network security, he says. "I simply do not believe that these absolute minimum thresholds will force you to do things you shouldn't be doing already anyway," he says.

But the standards are vague in some areas and others are too specific, he says. For example, under the regulations certain traffic requires stateful packet-inspection firewalls. "What if you used another technology that was the equivalent? Then you'd get in an argument with your QSA [qualified security auditor required by PCI]," he says. "PCI should be more risk-based with more options and less that is prescriptive – it's both too prescriptive and too vague at the same time."

2011 is a good time for security professionals to help shape needed Internet-security laws, Barrett says. "Technology is not legislators' strong point," he says. "The industry needs to spend some time educating Congress and its staff on issues to ensure what they do makes computing and the Internet safer and not less safe. They need to avoid the law of unintended consequences."

The top issue they should address is enforcement of cybercrime laws. Theft of $10,000 worth of goods online using fraudulent credit cards is unlikely to attract an aggressive prosecution, even if prosecutors knew who did it. The same theft from a brick-and-mortar retail store would attract an aggressive investigation, he says. "It's not lack of interest. It's that prior cases have been based

BUREAUCRATIC LATENCY

"I've never seen a cyber investigator who asked for help [from another country] and got it in less than six months. The bureaucracy needs to be fixed."

— Michael Barrett, CISO, PayPal

on financial loss. $10,000 is not enough." In prosecuting real-world vs. online crime, there should be no significant difference, Barrett says.

Barrett says the industry should also support creation of a presidential commission to study cybercrime and find out how much is really lost directly or indirectly to cybercrime. He says he's heard estimates ranging from $2 billion to $26 billion in the U.K. alone, and estimates as high as $2 trillion worldwide.

Along with that, the commission should assess how seriously other nations treat cybercrime. For example, he says many people say Russia doesn't investigate cybercrime because of corruption, but that isn't always true. "There may be problems, but it does prosecute and sometimes punishes," he says. The goal should be to figure out how to encourage more reliable prosecutions. "Like terrorism, we need to study other governments and see how seriously they'll treat it."

The Convention on Cybercrime, an international treaty signed by the European Union and the U.S., sets encourages international cooperation in prosecuting cybercrime and setting up appropriate laws to do so. Signed in 2006, it doesn't yet have the teeth to be effective, Barrett says. "The mechanisms are 19th century," he says. "I've never seen a cyber investigator who asked for help [from another country] and got it in less than six months. The bureaucracy needs to be fixed." •

THE INTERNET NEEDS ITS OWN WEATHER CHANNEL

Roger A. Grimes • InfoWorld

An Internet early-warning system would help organizations stay a step ahead of cyber criminals

Living on the East Coast, I often wonder how the early pioneers lived without Doppler radar and the Weather Channel. Today, we know about hurricanes weeks ahead of time, and you have days to batten down the hatches, gas up the car, and buy strawberry Pop-Tarts at Wal-Mart. Think I'm kidding about the last item? It's a consumer behavior proven to be an early indicator of where a hurricane will actually strike. Just look up the phrase "hurricane poptarts walmart" in your favorite search engine.

We often say that security should be baked in to any system from the start, but we usually don't do it – especially with the Internet. In the early days, the architects of the Internet were just trying to get a few separated computers to communicate with each other. By the time the miscreants began showing up to wreak havoc and commit cyber crimes, it was too late to rebuild the Internet's basic underpinnings. It's been a hardscrabble fight ever since, with the good guys and end-users losing most of the way.

One of the best things we could do for the Internet is to create an early-warning system (EWS) to warn us against rapidly spreading malware, spam attacks, and the like. Having thought about this for years, I envision this EWS as being a free, centralized, Internet-wide service – a DNS where participants could report and keep abreast of security events.

Here's how it would work: First, trusted devices or people would post notifications about malicious events to the service the moment they're noticed. Examples include the following:

- "IP address x.x.x.x is currently serving up a botnet"
- "XYZ Company is currently under attack by a spam worm and any email coming from them should be investigated more thoroughly"
- "Company X's website is currently hosting a malicious JavaScript redirect"

From there, any person or device could query the health status of any destination or origination point. Thus, when my email server receives an email from a given domain, it would send a one-packet query to the "Internet health service" to see if the sender's domain has been reported as healthy or ill. In either case, it would require only one packet to be sent and one packet in reply.

When the EWS reports something as unhealthy, it would

WORLDWIDE TATTLETALE

Most antivirus companies already have daily feeds telling them where bad traffic is coming from. That information could easily be shared with the world, immediately and for free, from a DNS-like service.

generate a warning message; alternatively, devices could be instructed to handle the incoming traffic appropriately. Your organization could choose to drop traffic from very ill places immediately, accept traffic without further inspection from very healthy places, or further investigate traffic reported in between the two reputation scores.

That reputation score could be based on a confluence of factors, such as written security policies, authentication method, patch status, secure code development, and demonstrated health over years.

To prevent information blockage early on, the EWS could be designed for such legacy systems to be allowed by default, although treated as untrusted, until all the new software and devices start using the centralized security defense.

There are some clear benefits to this sort of system. I know people who want to block wholesale a particular country's IP address space because they are tired of all the maliciousness coming from that nation. But why throw the good out with the bad? What they truly want is an easy way to see if the traffic is originating from a good, healthy part of that country versus one of the thousands of bad IP addresses. An EWS as I've described would make that far easier.

Additionally, such a system would help company's protect themselves against their weakest security link: end-users. As it stands, the average end-user can't be expected to make all the necessary reputation decisions that they are being asked to make on a daily basis. How can they be expected to know if a proposed download from a website they've been visiting for years is malicious? Thus, a centralized reputation service that could be queried to see if the website was compromised and respond accordingly would be welcome.

As to the plausibility of building a service that would rely on reports from various participating organizations, consider this: Most antivirus companies already have daily feeds telling them where the bad traffic is coming from. That information could easily be shared with the world, immediately and for free, from a DNS-like service.

Moreover, all the protocols we need to make this service happen today (HTML, XML, WS-*, IF-MAP, and so on) currently exist. It would just take a few dozen smart people sitting down in a room to figure out values in a table, agree on the service, and implement it.

The Weather Channel and Doppler radar have helped countless people protect themselves, their loved ones, and their belongings from imminent threat. It's high time to extend that early-warning model to the Internet. •

SPEAR PHISHERS SHARPEN SKILLS, CRAFT `INCREDIBLE' ATTACKS, SAYS EXPERTS

Gregg Keizer • Computerworld

But rash of targeted attacks may also mean more companies coming clean

Recent break-ins at high-profile targets like the International Monetary Fund (IMF) demonstrate just how proficient hackers have become at "spear phishing," researchers said recently.

"Today's spear phishing is not only more prevalent but also much more technically proficient," said Dave Jevans, chairman of the Anti-Phishing Working Group (APWG), an industry association dedicated to fighting online identity theft. Jevans is also the founder and chairman of IronKey, a Sunnyvale, Calif. security company.

"They're not going for a password, anymore, they're getting people to install crimeware on their computers," said Jevans.

Like the more common phishing, spear phishing attacks are launched as emails that try to con the recipient into clicking a link that leads to a malicious Web site. Those sites can take almost infinite forms, from fake account log-in screens to ones that tout a software upgrade to widely-used software, such as Adobe Flash.

In the second scenario, the file is not as advertised, but instead is attack code that infects the computer, giving criminals access to that machine – and through it, others – or to confidential information, like account passwords obtained by secretly monitoring the PC's keystrokes.

According to reports by the likes of Bloomberg, the IMF suspected that a phishing attack against one of its workers planted malware on a machine, which was then presumably used to scout the network for data to steal.

But the IMF incident was only the most recent in a series of specialized attacks this year aimed at targets from the Oak Ridge National Laboratory and the French foreign ministry to Google's Gmail.

All have one thing in common: They relied on spear phishing to fool users into installing malware or revealing account information.

The difference between phishing and spear phishing is while the former floods thousands or even millions of inboxes, the latter targets a small group of previously-identified people, sometimes only a handful who work at the same company or in the same organization.

It's like the difference between two letters asking for a loan: One addressed to "Occupant," the other from a best friend.

A key element of spear phishing is the reconnaissance hackers conduct before they launch their attacks, using the information they find on individuals to personalize the messages or to spoof the sending address of a colleague.

"They're doing a lot more legwork," said Jevans. "There's a lot more data on the Internet, on Facebook, on LinkedIn, that make these emails highly believable. And the malware that they're installing continues to evade antivirus software."

Kevin Haley, director of Symantec's security response team, agreed that cyber criminals have stepped up their spear phishing game.

"Social engineering has always been around," said Haley, referring to the term that describes the hacker strategy of manipulating victims into divulging information or doing something actually against their interest, like downloading malware. "But now [criminals] have perfected it."

Haley cited the example of the targeted attacks against Gmail users that Google said last week it had disrupted. Those attacks, which ran for months, were aimed at senior U.S. and South Korean government officials, military personnel, Chinese activists and journalists.

"You could have looked pretty hard [at the phony Gmail log-in screen] and not found any problems," said Haley.

"We used to say, 'Those stupid users, they're falling for obvious attacks,' but we can't do that anymore, maybe we shouldn't have done that in the first place," said Haley. "The social engineering [in targeted attacks] has reached a point where it's pretty incredible."

But unlike Jevans, Haley isn't ready to give hackers' spear phishing expertise all the credit for the rash of big-name break-ins this year.

Haley argued that while spear phishing has become more insidious, it hasn't become more frequent. But the fact that more companies and organizations are willing to retroactively acknowledge an attack or proactively disclose one has created that perception.

He pointed to Google's very public disclosure in early 2010 that it had been hacked, allegedly by Chinese attackers, for kick-starting the trend. "Google seems to be the first to come out and talk publicly [about an attack]," Haley said. "Credit to them."

But he also traced the change to Stuxnet, the worm found by researchers in 2010 that most experts believe was built as a digital weapon, then aimed at Iran's nuclear program.

"Stuxnet made us more aware of these types of attacks and the stakes of those attacks," Haley said. "It was no longer a discussion about the theoretical, but made everyone realize that these kind of attacks could be very serious."

Some security experts have said that the IMF attack smelled of state-sponsored hacking – attacks that were either government-run or government-financed. While Jevans and Haley were willing to rule that out, they noted that sophisticated spear phishing was well within the capabilities of cyber crime gangs.

"Although it's plausible, I'm not sure I buy it," said Jevans. "Governments certainly don't have more talent at their disposal than do the more sophisticated crimeware gangs."

As for defending against spear phishing, neither expert had a clear-cut answer. "There's no silver bullet," said Jevans, though he noted that isolating browsers and email clients in anti-malware "sandboxes" shows promise.

"There's not one thing that will stop this," echoed Haley. "All it takes is one user who goes into their junk mail folder and clicks on a link. We have to continue developing technical solutions, but if we ignore user education about targeted attacks we do ourselves a disservice." •

THE DDoS HALL OF SHAME

Tim Greene • Network World

Distributed denial-of-service attacks like those against WordPress now part of the political guerilla's toolkit

Distributed denial of service (DDoS) attacks like the ones that nailed WordPress blogs recently have been around for decades, but it's only in the last dozen years that they've had enough impact to grab public attention.

With the rise and commercial availability of botnets that provide a distributed platform from which to launch these attacks the means to carry them out are accessible.

Due to the cost, though, they have to be carried out by a motivated adversary bent on harm since there is little way to reap monetary profit from them aside from blackmailing potential victims with threats of crippling their servers.

Here are some of the notable DDoS attacks of the past few years:

Windows PCs as tools for DDoS attacks

In 2000, DDoS attacks on Yahoo!, eBay, eTrade, Amazon.com and CNN were launched from commandeered Unix machines in businesses and universities, but a few weeks later the malware directing the attacks called Trinoo shifted to Windows PCs.

DDoS attack highlights 'Net problems

Internet root servers were attacked in 2002, but the attacks were blunted enough for the servers to recover without a major take-down of the Internet itself. After the attack, limits on the Internet Control Message Protocol (ICMP) messages these servers will accept were set to ensure that type of attack in the future wouldn't succeed. The 13 root servers targeted run as the master directory for lookups that match domain names with their corresponding IP addresses.

Estonia suffers massive DDoS attack

A spree of DDoS attacks against Web sites in Estonia in May of 2007 crippled Web sites for the prime minister, banks, and less-trafficked sites run by small schools. But most of the affected Web sites were restored quickly, and the government called for greater response mechanisms to cyber attacks within the European Union. Russia was accused of the attacks, but they could not be traced back to a single source there.

Storm worm strikes back at security pros

During the height of the Storm worm attacks in 2007, a security researcher revealed that the people behind it or the worm itself was launching DDoS attacks against researchers trying to figure out a way to defeat it. The worm was able to figure out which users were trying to probe its com-

mand-and-control servers, and it retaliated by launching DDoS attacks that shut down their Internet access for days, said Josh Corman, now an analyst with the 451 Group.

Georgia cyberattacks linked to Russian organized crime

DDoS attacks against the country of Georgia were seen as a way to soften up the country in preparation for a five-day military invasion by Russia in 2007. About a year later the U.S. Cyber Consequences Unit, an independent research institute concluded the attacks were launched by Russian criminal gangs in sympathy with the Russian government.

Twitter DDoS attack determined to be politically motivated

DDoS attacks in August of 2009 that affected Twitter, Facebook, LiveJournal and several Google sites may have been an attempt to silence a blogger named Cyxymu from the Eastern European country of Georgia who was an outspoken supporter of his country. Facebook CSO Max Kelly has said the attack was coordinated to keep the blogger's voice from being heard.

Mikko Hypponen, the Chief Research Officer of Internet security firm F-Secure, said of the attacks, "Launching DDoS attacks against services like Facebook is the equivalent of bombing a TV station because you don't like one of the newscasters."

Pre-Christmas DDoS attack hits Amazon and others

Amazon.com and Amazon Web Services servers were hit by a DDoS attack Dec. 23, 2009 , as North American consumers rushed to finish online shopping ahead of the end-of-year holiday season.

Anonymous takes down Visa.com in WikiLeaks protest

A loosely organized group of Internet hacktivists called Anonymous took down Visa's website Dec. 7, 2010 after organizing similar attacks on MasterCard and PayPal. Anonymous, had been encouraging volunteers to download software called LOIC (Low Orbit Ion Cannon), which let them centrally control these systems and direct them into a DDoS. The point of the attacks was to put pressure on financial companies that recently cut ties with the WikiLeaks website over its publication of more than a quarter million U.S. Department of State classified cables. •

PHISHING STILL RULES, BECAUSE WE'RE STILL GULLIBLE

George V. Hulme • CSO

Depsite more than a decade of warnings, users readily fall for phishing attacks

For years, phishing attacks were viewed largely as a consumer security problem. Attackers would target users with an email that tempted them into a fraudulent 411 scam, or to share their account numbers and sign on credentials with a bogus Web site.

Not anymore.

It's become clear, going to back to the so-called 2009 Operation Aurora attacks that phishing attacks work. Regarding those attacks, a Forrester Research (FORR) analyst quoted an aerospace company employee who was familiar with the exploit-laced Adobe (ADBE) PDF files that came attached to the spear-phished emails.

"This kind of stuff is driving the defense contractors nuts. They should know better, yet they are still affected," the source said at the time.

Spear-phishing attacks – those that use information about someone to target them directly as part of an attack – are all the more successful. The viability of phishing attacks were revealed more recently with the successful attack against RSA Security and then the related attack on defense contractor Lockheed-Martin.

Internet security awareness training firm KnowBe4, LLC recently conducted a test to see what percentage of Inc. 5000 companies would be susceptible to phishing attempts. In one phase of the test, the firm hired a reputable bulk email service to send simulated phishing emails to employees at 81 companies. Of those 81 companies, only two blocked the phishing attack, and of those 45 percent of firms had one employee or more click on the link. In a follow-up test, a one-time mail server was set up to send the phish. That netted a 15 percent response rate in less than a day.

"The success rate of the attacks is surprisingly low," says Pete Lindstrom, research director at Spire Security. "I thought the results would [have] been higher for a test like that," he says.

Security experts are divided on whether security awareness training would have much success in driving the number of successful phishing attacks down. While some experts purport security awareness training would lessen the viability of such attacks, others strongly disagree.

"We find that most security advice simply offers a poor cost-benefit tradeoff to users and is rejected. Security advice is a daily burden, applied to the whole population, while an upper bound on the benefit is the harm suffered by the fraction that become victims annually. When that fraction is small, designing security advice that is beneficial is very hard. For example, it makes little

COST/BENEFIT

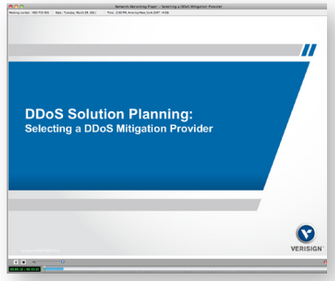
"Security advice is a daily burden, applied to the whole population, while an upper bound on the benefit is the harm suffered by the fraction that become victims annually. When that fraction is small, designing security advice that is beneficial is very hard."

— Cormac Herley, Microsoft

sense to burden all users with a daily task to spare 0.01 percent of them a modest annual pain," wrote Microsoft (MSFT) Research's Cormac Herley in his paper, " So Long, and No Thanks for the Externalities. The Rational Rejection of Security Advice by Users."

Such costs could be everything from using strong passwords to never clicking on links embedded within email. A certain percentage of the population will ignore this advice, no matter how many times they're told not to, because the direct cost to them for ignoring it is so low. "The value to risk ratio for people clicking on links is way too high. People are going to click on links," says Lindstrom. •

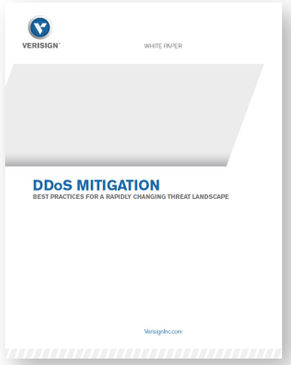
INTERNET SECURITY RESOURCES



Selecting a DDoS Mitigation Provider On-Demand Webinar

Learn how Verisign manages and helps protect the internet against DDoS attacks. This webinar will also provide you with best practices for business continuity and key considerations for DDoS protection in your organization.

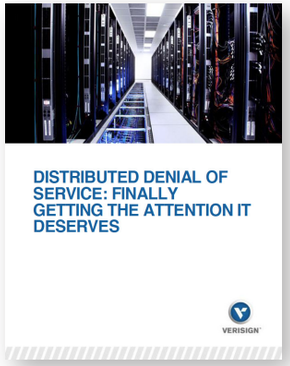
View now



Best Practices for a Rapidly Changing Threat Landscape

This paper describes how Verisign draws on their success and hands-on engagements with customers in a range of industries to identify a set of best practices that enables organizations to keep pace with DDoS attacks while minimizing impact on business operations.

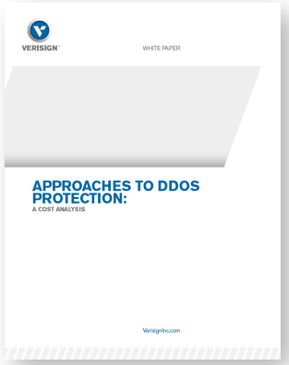
Download now



DDoS: Finally Getting the Attention it Deserves

Verisign commissioned a market research study to investigate just how concerned IT decision makers are with the threat of DDoS attacks and what - if anything - they are doing to prepare for the increased threats in todayís ever evolving cyber landscape. The results in this paper are very revealing.

Download now



Approaches to DDoS Protection - A Cost Analysis

All organizations with an online presence or dependence on internet-based systems need to fortify their defenses against DDoS attacks. Read this paper to learn what an attack can cost an organization, how to develop a DDoS mitigation strategy and how to get maximum protection from your investment.

Download now

Protecting Your Critical Information Infrastructure

A strategy that assures the availability and reliability of vital resources while protecting them from malicious attacks is at the core of network operations and security. This paper defines four key components of such a strategy, and offers a practical set of guidelines for ensuring its success.

Download now