Executive Suite Series

A Prolexic White Paper

‘Tis the Season – for DDoS Attacks

PROLEXIC
DDoS Attacks End Here.

‘Tis the season – for DDoS attacks

The holiday season is fraught with a bit more stress and worry than usual. Along with the joys of families coming together to celebrate these happy times, there’s always an elevated level of anxiety involved in planning, logistics and making sure budgets don’t crack under the weight of gifts and festivity.

Website load and the holidays

Interestingly, the holidays present many of the same challenges to businesses. It’s a time of great anticipation – the final months of the calendar year are often make-or-break times for companies, particularly those in the retail sector. A big holiday shopping season can, at one stroke, make up for a lackluster rest of the year, while a poor one can doom a company’s bottom line.

Retailers and other firms are increasingly dependent on online commerce to provide a substantial share – in many cases, the majority – of holiday sales. The rise of e-Commerce has provided a significant boost to the retail sector, but like any major technological advance, it demands a new set of competencies and security measures to prevent mishaps.

The spike in business, often seen during the holiday season, combined with the increasingly central role of e-Commerce for many companies, means that IT infrastructures can be easily overloaded by legitimate or spurious traffic.

Simply being unprepared for the holiday rush is often enough to do real damage to the bottom line. As more visitors push site response times up, growing user frustration means that additional business is driven away. Research from Forrester Consulting performed in 2009 found that even minor spikes in load times are enough to seriously impact the user experience for many.[1]

According to that study, just over half – 52 percent – of respondents said that load time was a critical factor in their online shopping experience, and 47 percent told researchers they expected an e-Commerce page to load in two seconds or less. Another 40 percent of those surveyed said they would wait “no more than three seconds” on a page before giving up and looking elsewhere.

What’s more, the Forrester experts found this type of dissatisfaction tended to irreparably damage a company’s image among affected users. Nearly four out of five respondents said they were measurably less likely to use such a site again and almost two-thirds stated that they would go to a competitor.

DDoS in the mix

It is clear that it is a significant challenge managing even the normal strains on a company's computing hardware during a busy holiday season. Nevertheless, this type of heavy traffic pales in comparison to the threat posed by a Distributed Denial of Service (DDoS) attack striking during the holidays.

DDoS is a potentially catastrophic issue for businesses even under the best of conditions. Coupled with spikes in traffic and the massive importance of the holiday season to many companies, such attacks become both more likely and potentially more damaging.

Beyond the obvious revenue losses from taking a website offline for anywhere from minutes to days, a holiday DDoS attack can wreck a company's brand perception on multiple levels. Not only is the competition likely to look a great deal safer and more reliable by comparison, a prolonged outage can shape the flow of web commerce in a way that completely omits a business unfortunate enough to suffer through one.

An examination of chat boards by Prolexic on Internet forums reveals that hackers are well aware of the potential impact of the DDoS technique, especially with the holiday season on the horizon. Indeed, one of the biggest threats to e-Commerce is driven by another type of online business, as hackers build networks of hijacked computers (botnets) for use in DDoS attacks and sell or rent them to each other.

A brief look at some not-so-happy holidays

It's important to realize that size alone is no protection from a sufficiently determined DDoS attacker. Technological advances in DDoS techniques mean that even a huge infrastructure with the capacity to handle immense amounts of traffic does not guarantee immunity. This was graphically demonstrated last year as online "hacktivists" managed to knock none other than Visa, MasterCard, PayPal and American Express offline during the height of the holiday season.

The attacks of early December 2010 were motivated by political factors, centering on the controversial website WikiLeaks. After the arrest of the site's founder and operator, Julian Assange, many online activists decried the case against him as politically motivated and intended to prevent him from disclosing uncomfortable facts about many international corporations and world governments. When PayPal and the other companies suspended accounts set up to provide a legal defense fund for Assange, a group of liberal hackers was outraged. This included the hackers who now make up the now infamous hacktivist collective known as Anonymous.

The first target of the massive DDoS attack was Swiss bank PostFinance, which froze one of Assange's accounts. According to the New York Times,[2] that company's website was offline within minutes of Anonymous' call to arms.

In and of itself, this would not have caused the type of negative publicity the group was looking for. However, the perceived complicity of the larger financial institutions in preventing funds from flowing to Assange broadened Anonymous' campaign considerably.

Hundreds of activists using the Low-Orbit Ion Cannon DDoS tool managed to direct enough excess traffic to the websites of Visa, MasterCard, American Express and PayPal, knocking those companies offline for various lengths of time and briefly preventing them from processing payments. This tool is still available to hackers who want to target legitimate e-Commerce businesses.

Although the direct financial effect of the attacks on those companies was likely minimal – stock prices for each company dipped temporarily during the actual assaults, but recovered quickly[3] – the potential damage should be clear. Smaller firms without the kind of exhaustive track record of a major multinational corporation aren't likely to weather such a storm nearly as easily.

Even before the politically motivated attacks of Anonymous in 2010, the 2009 season provided its own glimpse into the possibilities available to DDoS attackers during the holidays. On December 23, a confirmed DDoS attack on a major DNS service responsible for the domains of Amazon and Wal-Mart, among many others, briefly brought substantial amounts of the web's shopping traffic to a halt.[4] Although the hiccup was a short one, changes to any of several variables could have made it much more destructive.

How much coal in your stocking? Potential DDoS exposure

The process of assessing a company's DDoS risks and the potential damage that can be inflicted via such an attack is not a simple one. A host of different factors can affect both the ease with which a given IT infrastructure can be slowed down or derailed, and the severity of the consequences for the business in the long term.

One important consideration is the extent to which a company depends on its online operations to drive revenues, which varies considerably among different firms. One example of a business that is less reliant on online activity might be a mid-sized retail chain with several different locations in a given area. Customers are more likely to be confined to this geographic region, meaning that a physical outlet is probably somewhere nearby. Although a DDoS attack may mean significant disruption for such a business' website – particularly in light of the fact that its web presence could be less developed – it is more likely to be viewed as an annoyance than a crucial service interruption, though this is still not a possibility to take lightly.

However, other firms are not so lucky. Companies with a major web presence that are either completely or largely dependent on e-Commerce to drive revenues are effectively closed for hours or even days if a DDoS attack takes down their site. In this nightmare scenario, the bottom line impact can be devastating.

The technical challenges involved in such an attack are also a major consideration for firms looking to protect themselves against DDoS attacks and are not limited to a consideration of the defensive measures already in place. The way a business prepares for the holiday season, in fact, can be a determining factor in how much impact a potential DDoS attack may have.

Ironically, companies whose holiday traffic exceeds the levels they had anticipated could become victims of their own success. While the growth in sales and revenue are positive for any business, this increased strain placed on the IT infrastructure could lower the level of malicious traffic a DDoS attack will need to cause disruptions. This illustrates the importance of advanced preparation for the holidays.

None of this is to say that the defensive and recovery measures in place are not important to a company's calculation of its DDoS risk profile. To best understand how these measures will impact the overall effect of such an attack, it's often helpful for IT decision-makers to map out what will likely happen as a result of a DDoS attack, and what subsidiary effects it could have on a company's systems.

The usual defenses, including firewalls, can offer some protection, but a sufficiently high volume of traffic can quickly overwhelm them as well. Routers provide a defense against one of the most basic types of attack traffic – a simple flood of pings – but most modern DDoS techniques will simply bypass this. Unfortunately, most of the ways to configure a company's basic infrastructure to defend against DDoS attacks results in severely degraded performance for legitimate traffic – effectively doing the attackers' job for them with the same damage to the business' bottom line.

The same is true of so-called "blackholing" or "sinkholing" techniques, which redirect traffic away from an attacked website. The first tactic is a highly effective one if the precise IP addresses of attacking machines are known, enabling all traffic from those sources to be sent to a null interface to be discarded and ignored by the target system, according to research from the National Technical University of Athens.[5] Early in the evolution of denial-of-service attacks, this might have been a sufficiently robust defense, but the growing sophistication of DDoS techniques makes it increasingly difficult to pinpoint the sources of malicious traffic. In these cases, blackholing simply siphons off attacking packets and those from legitimate users alike, effectively taking the web site offline and helping the attackers achieve their objective. Blackholing is a common technique used by hosting providers, ISPs and DNS providers that offer DDoS mitigation as an add on service. When the size of an attack starts to overwhelm their network and impact their core business services the site under attack will be sacrificed so other services and clients can be served.

Sinkholing, the researchers added, is slightly more sophisticated, allowing for an analysis of the traffic on the victim's end and more effective filtering. However, despite this additional capability, sufficiently high-volume attacks can quickly overwhelm a sinkholing router even more easily than a blackhole system, making it also of limited use against modern DDoS techniques.

What will happen to the business' security systems in the wake of an attack? This is an excellent hypothetical question to ponder as it can help IT groups plan for the unpredictable aftereffects of a large-scale system outage. Although it's uncommon for general security measures to be compromised by a DDoS attack, it's always wise to make sure that some important access control won't be knocked out along with a business' web server. Losing the ability to conduct business online is one thing, but having private company information exposed as well is adding insult to injury.

Importantly, this issue is never far from the minds of the public, many of whom might not realize how rare such an event is. While DDoS attacks generally don't compromise payment data or client information, consumers without a detailed knowledge of online security may automatically assume that a website that fell victim to a DDoS attack is inherently insecure. This perceived issue can quickly become a real one, as scared-off consumers are effectively missed opportunities who can very well become customers of competitors.

Even among better-informed customers, a successful DDoS attack creates the perception, correct or not, that a victimized company doesn't have web security issues firmly under control. "If they can get taken down like that," the thought process might go, "what's to stop someone from hacking their way in and grabbing my credit card number?"

Holiday DDoS protection: Barricading the chimney while still letting Santa in

It's clear that the holiday season makes it more important than ever for businesses to protect themselves against DDoS attacks. Unfortunately, we've already seen that some of the simplest protection methods have crippling drawbacks or are simply ineffective.

With this in mind, what's a company to do when trying to keep its mission-critical services online? There are two basic considerations in DDoS defense that lead to measurably better success in repelling such attacks: system capacity and active defense.

The first issue is the simpler of the two. Systems with more available bandwidth, more memory and more computing resources can soak up more punishment from a DDoS attack without slowing down or crashing. Overprovisioning, as the technique is sometimes known, involves bringing additional capacity online in order to provide a buffer against both heavy legitimate holiday traffic and potential malicious activity. This can be treated as a permanent extension of a business' capabilities or a temporary cushion for anticipated seasonal need.

Trying to beat DDoS with overprovisioning alone, however, has potential downsides. The most obvious issue is the cost involved, as it is extremely expensive to install extra servers. While this can make the technique impracticable by itself, the less evident but potentially more serious issue is that just throwing more capacity at the problem doesn't account for the nature of the modern DDoS attack.

A technically knowledgeable and resourceful hacker can direct gigantic amounts of traffic at a target without too much trouble, and none but the wealthiest companies are likely to be able to pay for extra computing muscle to cope.

In addition, this type of protective measure fails to incorporate some of the most effective and efficient features of the second major technique: active defense. With the use of dedicated systems to quickly identify potential DDoS activity, coupled with the capability to redirect attack traffic through services provided by an expert third party provider for filtering, specialized DDoS protection services are likely the best bet for those who are serious about their defenses.

The "clean pipe" technique is probably the most advanced anti-DDoS tool available because it solves the central problem posed by such attacks. While there are a number of ways for companies to throttle back their connectivity to avoid their systems being overloaded by attack traffic, these tend to affect legitimate users just as badly as malicious ones. Specialist DDoS proxy providers use advanced detection techniques to identify when an attack is occurring and provide sophisticated analysis capabilities, enabling them to filter traffic much more efficiently than in-router sinkholing systems.

This alone is a substantial improvement over most other DDoS protection methods, but the clean pipe technique also allows for on-demand overprovisioning, leveraging dedicated servers from the provider to lessen the impact of an attacker's traffic.

An unconventional idea of naughty or nice: Reasons for DDoS attacks

The rise of hacktivist groups like Anonymous provide an illustration of the politically motivated threat. Even businesses tangentially involved in an issue in which Anonymous has expressed interest should factor this into the calculation of their DDoS vulnerability, since this is one of the group's most popular techniques. Fortunately, the increased visibility of the group and its heavy coverage in the mainstream media makes it more likely that companies will have plenty of warning that the hacktivist community is becoming involved in some matter related to their interests.

Other groups, like the now-infamous LulzSec, are far more difficult to predict. Their modus operandi seems to harken back to the earlier days of hacking, making them less political group and more of a partially organized band of online pranksters. "Because it is there," appears to be as good a reason for an attack as LulzSec requires, meaning companies should be on their guard. However, the group has been far less active of late and reports indicate that it has been at least partially absorbed by the more political Anonymous.

Regardless of the threat's source, however, the importance of awareness and effective protection against DDoS attacks during the holiday season is clear. The risk-reward analysis for companies should be relatively simple – while such attacks are relatively rare, they are becoming less so each year, and the damage that can be caused by a successful attack may be enough to drastically affect the fortunes of some businesses. Therefore, it is prudent to expect and plan for the worst while hoping for the best holiday season of online sales yet.

About Prolexic

Prolexic is the world's largest, most trusted Distributed Denial of Service (DDoS) mitigation provider. Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission critical Internet facing infrastructures for global enterprises and government agencies within minutes. Six of the world's ten largest banks and the leading companies in e-Commerce, payment processing, travel/hospitality, gaming and other at-risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world's first "in the cloud" DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida and has scrubbing centers located in the Americas, Europe and Asia. For more information, visit **www.prolexic.com**.

[1] http://www.akamai.com/html/about/press/releases/2009/press_091409.html

[2] http://thelede.blogs.nytimes.com/2010/12/06/latest-updates-on-leak-of-u-s-cables-day-9/#hackers-take-down-swiss-banks-web-site

[3] http://www.forbes.com/sites/schifrin/2010/12/09/are-wikithreats-a-traders-dream/2/

[4] http://www.darkreading.com/security/attacks-breaches/222100176/index.html

[5] http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_7-4/dos_attacks.html

A Prolexic White Paper

The Executive's Guide to DDoS

PROLEXIC
DDoS Attacks End Here.

On the front page

Distributed Denial of Service (DDoS) attacks have been all over the news lately – although it seems like we've been reading about them for years. A long parade of websites, some of them the biggest and – one would think – best-protected on the entire internet, have been taken offline by hackers, blasted from the web by a blizzard of unsolicited requests coordinated by shadowy networks of attacking PCs. Most of the attackers have no idea they are part of a DDoS attack, but the target, when the technique is properly executed, most certainly does.

Even the most muscularly provisioned services are vulnerable. The popular online multiplayer videogame Eve Online has sufficient capacity to support tens of thousands of simultaneous, real-time connections from its players, all of whom are potentially interacting with many others at any given time. The company behind Eve, Crowd Control Productions, runs the game on a specialized server farm, with dozens and dozens of machines devoted solely to keeping the online game functioning.[1] Even so, a major DDoS attack managed to quickly cause the entire system to grind to a halt.[2]

Beyond damage to a company's website and online services, DDoS attacks can even cause havoc deeper inside IT infrastructure. A sufficiently large-scale assault can knock whole sectors of an organization's network offline, and, in rare cases, can even affect regional internet connectivity.

The monetary costs of a DDoS attack – in terms of lost sales, damage to reputation and an inability to perform basic functions, in many cases – vary widely, but research from the Yankee Group, Forrester, and IDC estimate the total loss for every hour of downtime at anywhere from US$90,000 for a catalog sales center up to nearly US$6.5 million for a retail brokerage.[3] Clearly, DDoS can be an existential threat to many businesses.

THE WALL STREET JOURNAL

Hackers Claim MasterCard Web Crash

By Deal Journal

Mastercard's website is down, and hacker groups on Twitter are claiming responsibility, citing the financial company's role in cutting off payments to the document-leaking site WikiLeaks.

CNN Money

A Service of CNN, Fortune & Money

Wordpress hammered by massive DDoS attack

Forbes

DDoS: coming to a network near you

CNN Tech

Cyberwarfare finds a captive audience

(CNN) – From scanning news headlines over the last couple of

Bloomberg Businessweek

Internet Hacker Attacks at an All-Time High

Online networks suffered their heaviest attacks to date this year, with more sites than ever coming under sustained assault

COMPUTERWORLD

News

Anonymous claims LulzSec members, steps up attacks

By John Ribeiro

June 27, 2011 03:14 AM ET

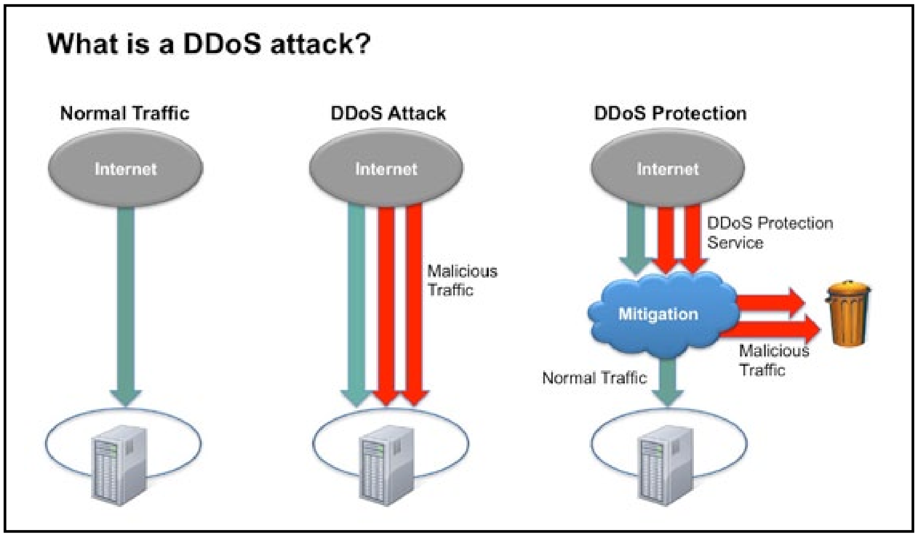
InformationWeek Government

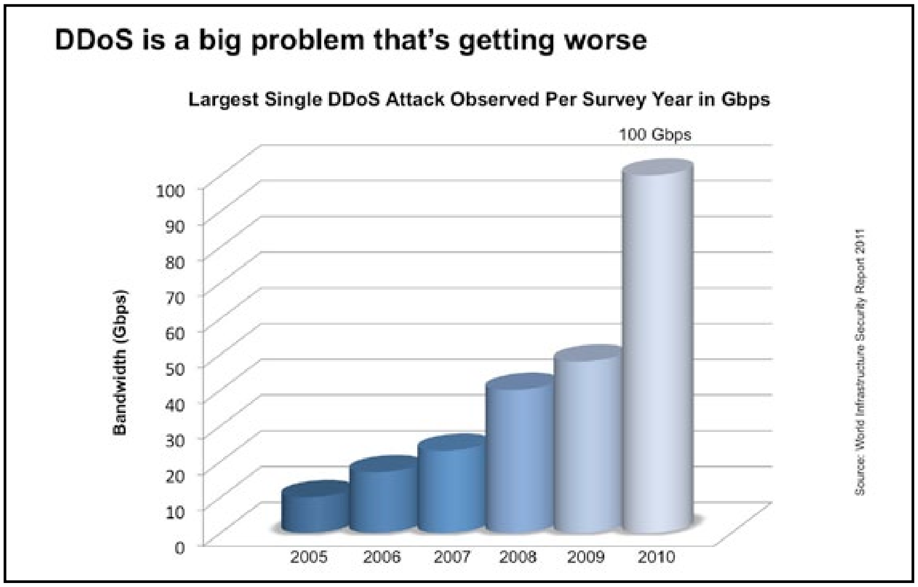
LulzSec, Anonymous: Feds Most Wanted

While the hacker groups have drawn attention with public boasts, federal investigators have set up shop in numerous social media sites, going undercover where necessary to root cyber criminals.

How it works

The basic idea behind a denial-of-service attack is quite simple. An attacker wishing to prevent a website or server from functioning correctly directs a large amount of requests – sometimes meaningless and sometimes legitimate – or other traffic to the target. This forces the target website to respond, taking up small amounts of its computing resources. Enough traffic and the target's performance will begin to suffer as it is forced to devote increasing amounts of its capacity to dealing with the flood of requests. Pile on more requests and all traffic comes to a halt, drowned out by the chorus of the attacker's digital noise.





Source: World Infrastructure Security Report 2011

As with so much in the world of digital security, however, the basics only tell a small fraction of the story. If an attacker simply configures his or her computer to blast a target site with information in an attempt to knock it offline, two problems will arise immediately.

The first is that a single machine is unlikely to be able to generate the volume of garbage traffic needed to cause trouble to anything but the simplest of targets. More importantly, the target will be able to clearly identify the source of the noise – the attacker might as well paint a "here I am" sign on his or her back. In light of the probability of a prosecution under the Computer Fraud and Abuse Act[4], as well as any number of other laws, stand-alone DoS attacks have proved unpopular.

Adding the extra "D" to "DoS"

However, malware writers have added the all-important extra "D" – for "distributed"– to the DoS attack with the advent of botnet technology. Instead of using one's own system to attack a target with meaningless but damaging noise, why not get a group of strangers to do it instead? Botnet malware allows online criminals to do just that.

The technique is based on infecting unsuspecting users with a malicious program that connects them to a hidden server and enables hackers to issue certain commands to them. A group of compromised machines linked together in this way is known as a botnet. Botnets have a number of functions beyond DDoS attacks, including acting as difficult-to-trace sources of illegal spam email and a means to perpetrate fraud via pay-per-click online advertisements.[5] They are frequently treated as a commodity by digital criminal groups, who lease them out to customers to use as they see fit.

An attacker, then, can command all the machines in a botnet to target a single site or server at the same time and flood it with traffic, drastically increasing the amount of data that can be flung at a victim in a given time period.

This solves the two basic problems with DoS as an attack technique simultaneously, making the perpetrators both much more powerful in terms of the white-noise traffic they can direct at their targets and more difficult to detect by several orders of magnitude. An IT staff trying to identify the attacker will see, instead of a single machine, a list numbering in the tens of millions in the case of the biggest botnets. And even if they are somehow able to identify the control servers being used to coordinate the attack, there will likely be no clue provided as to the actual identity of the people behind it.

A new wrinkle: Reflection

Botnets of such a size, however, are few and far between. They tend to be difficult to construct, as well as making for fat targets for law enforcement and white-hat security researchers, who will devote significant amounts of resources to a network that grows to the size of, say, BredoLab. (This gigantic botnet was seriously damaged by a Dutch government enforcement action that seized nearly 150 command-and-control servers in 2010, heavily undermining its capabilities.[6])

BredoLab is thought to be the record-holder for botnet size, but getting precise measurements of the number of infected computers in a given network is difficult, in part because their patterns of activity vary widely. The infamous Gumblar botnet, for example, is noted for manipulation of Google search results and its spreading of malicious programs disguised as antivirus solutions that in reality infect victims with additional malware, while the Conficker worm uses the Waledac spambot system to continually propagate itself.[7] The latter also displays a high level of sophistication, encrypting its payloads with either 512-bit or 1024-bit hashes, and delaying any activity beyond widespread infection until the fifth identified variant.

Nevertheless, even the most sophisticated of these malicious networks are often victims of their own success, drawing a great deal of unwanted attention from researchers at digital security companies and major computing firms. Microsoft reportedly had a significant role in the effective destruction of the Rustock botnet, which at one time had been thought to be responsible for a sizable fraction of the total worldwide volume of spam messages.[8]

However, clever hackers have a way to effectively multiply their hordes of zombie machines. Instead of simply telling the botnet to flood a target directly, each of the infected PCs sends requests to a long list of other, uninfected computers. Ordinarily, this would simply lead to a flood of responses to the botnet machines, but there's a twist – hackers can spoof the internet addresses of the infected computers to instead point to the real target.

This causes all of the response traffic from all of the machines queried to redirect onto the victim, creating a digital tsunami of confusing information that creates the desired DDoS effect, enabling higher traffic volumes – often made up of garbage data and requests – and an additional layer of anonymity between the attacker and the target.

Other variants

Not all DDoS techniques are focused on a one-time, full-scale takedown of the target's systems, however. Some attackers aim to degrade and harass, rather than completely knock out their victims. This is known as degradation of service, and it carries its own set of headaches for its targets. Accomplished by multiple smaller-scale DDoS traffic spikes designed to create a long-term, systemic slowdown in performance and availability, the technique can be difficult to distinguish from a legitimate surge in user activity.

Victims could assume, for example, that their site traffic numbers show significant interest in their organization's products or services, and consequently make substantial changes to a business plan based on this false assumption. The financial fallout from such an attack could be disastrous.

That said, others take the DDoS attack in the opposite direction, aiming for not just a shutdown of the victim's web services, but the actual destruction of valuable IT hardware. So-called permanent denial-of-service attacks were brought to prominence by a 2008 presentation at a European security convention by HP researcher Rich Smith, who stated that embedded systems were vulnerable to malicious firmware updates that could damage them irreparably.[9] This technique, however, is highly uncommon, and UK tech publication the Register reported at the time that no such attack had yet been seen operationally.[10]

This doesn't mean, of course, that PDoS is destined to remain a footnote of history. Awareness of the potential damage that can be caused by the use of cyberwarfare has caused serious concern not just for the security of corporate data, but for national security as well. The Stuxnet worm's release – and reported subsequent destruction of Iranian nuclear research hardware – has demonstrated the potential for computer software to inflict real-world damage. The similarity of PDoS' supposed ability to render various types of network hardware unusable is plain, and the possibility of its use in the future remains a real one.

The effects

Once a DDoS attack is active, the effects on an organization's IT infrastructure can be wide-ranging and severe. In many cases, the first sign that something is wrong is a rapid degradation of web server performance, manifesting as increasing difficulty in accessing the site and serious slowdowns in page loading speed.

The goal of most DDoS attacks, however, is to knock websites or services completely offline, and this can happen quite quickly if there is enough junk traffic being sent. Visitors to the site or users of the service will get error messages of various types, depending on the exact nature of the hosting in use.

While many consumers and workers may simply experience these outages as an annoyance, the consequences can be severe. An organization's reputation for stability and technical expertise can suffer greatly as a result of a significant DDoS attack, causing real but difficult-to-measure damage to the bottom line and granting a potential competitive advantage to rivals.

The trust of consumers in the organization's brand can also be substantially eroded as a result, and multiple incidents can create the hugely damaging perception of technical incompetence or a lack of organizational emphasis on security. Particularly for businesses in a highly technical field or one that places a high premium on reliability and safety – like healthcare or finance – consumer trust can be a make-or-break consideration.

Moreover, the damage can be compounded by media attention to such an incident, particularly if the victim of a DDoS attack is already in the public eye. While an active, responsible reaction to the event will go a long way toward mitigating this effect, there are no guarantees for how a publicized attack will play out in the press, and negative coverage can quickly exacerbate the reputational damage involved, fairly or unfairly.

Regardless of whether an organization is to blame for lackluster protective measures in place to defend against DDoS attacks, fault can easily be ascribed to the victim. This makes post-incident image management an essential concern for organizations affected.

This tendency in and of itself is worsened by the generally poor understanding of DDoS outside of the technical sphere. While the technique is undeniably damaging, non-experts may erroneously jump to the conclusion that company information or customer data stored on the organization's systems has been compromised, which further complicates the aftermath.

In sum, the combination of real and perceived fallout from a DDoS attack can spell major problems for many victims. Companies in a competitive market sector – again, particularly one related to or reliant upon technology – could find themselves suddenly playing catch-up or relegated to a smaller corner of their field. If their position is already tenuous, such an event might even affect a business' basic viability.

Mitigation

Fortunately, there are a number of ways to either mitigate the worst effects of a DDoS attack or ward them off completely. Beyond having the right protective systems in place and ensuring sufficient overflow capacity is available, much depends on an active, well-informed response to an incident.

Our demands are these.

- Sony must allow for end user modification of the PS3, as was available prior to the 3.21 update.
- Sony must end any attempts to bring legal action to those wishing to alter a product they own.
- Sony must not pursue legal action against the collected IP addresses.

We are not being unreasonable in our demands; we ask only that Sony restore the features that were originally found on the Playstation 3.

When IT staff notice the telltale symptoms of DDoS, including sudden performance degradation and system load spikes, the most important thing is to make sure that the problem really is a DDoS attack. There are a number of errors and technical failures that can look superficially like a DDoS attack, so it's critical to ensure that staff is acting to tackle the right kind of problem. A highly publicized outage of BBC websites earlier this year had many speculating that an attack from noted hacktivist group Anonymous was responsible – due to negative coverage of the group from the British state broadcaster – but the news outlet stated publicly that a rare simultaneous failure of both primary and backup routing systems was to blame instead.[11]

If it is, in fact, a deliberate attack, IT personnel should move quickly but with clear purpose. An investigation of an organization's log files can help reveal important details about an incoming DDoS, both in the volume of the garbage traffic and the specific technique being used to flood systems. Certain types of incoming instructions could be vulnerable to settings changes in a company's network systems, potentially choking off a significant proportion of the attack's strength.

Additionally, if there are identifiable sources of attack code, acting to block off the worst ones can help mitigate the damage and increase the team's chances of keeping systems in working order. This might be particularly useful in the case of reflected DDoS attacks using a large third-party site as a redirect to focus harmful traffic onto a target. While such a site is unlikely to be the only one in use by the attackers, all avenues that can be closed off – especially major ones – can alleviate at least some of the strain.

Getting ready for next time

The well-coordinated use of multiple forms of defense is necessary to provide meaningful protection against DDoS attacks. Given the high level of sophistication displayed by modern cybercriminals, there is no single catch-all technique or system that will offer any reasonable assurance of safety.

However, intelligently deployed protection utilizing the multitude of technologies available to IT departments can dramatically decrease the potential of a DDoS attack knocking an organization's services offline.

At the most basic level, the use of a firewall can help protect against DDoS by validating traffic, which prevents some types of junk requests from getting through. Any reduction in the amount of meaningless instructions that must be handled by the target server is likely to at least partially mitigate the effects of an attack.

However, firewalls need to be configured in highly specific ways to provide much defense against DDoS. Without expert handling, they are unlikely to provide meaningful amounts of protection from floods of malicious traffic. Properly set up, though, the tools are an adequate first line of defense.

Of course, even the most skillfully configured firewalls won't provide standalone defense against any but the most rudimentary types of denial-of-service attack, which are relatively uncommon today. The protective capabilities of a firewall, however, can be greatly enhanced by the use of network hardware with specialized features designed for DDoS defense.

Many of these devices use a technique called traffic shaping to actively prioritize some types of instructions and requests above others, using a host of different – and highly customizable – rules and guidelines to cause some traffic deemed more important to flow freely, while slowing other types to make room in available bandwidth.

This functionality is useful for more than just DDoS defense as well, granting the ability to provide better network performance for important tasks without the need to add new raw capacity.

Unfortunately, this type of mitigation is more of a speed bump to major DDoS attacks than a true barrier. The capacity for bandwidth shaping can be easily overwhelmed by the raw volume of traffic produced by a serious botnet.

What's needed, then, is something that can combine the protective features of a firewall with the traffic analysis capabilities of advanced network infrastructure. Specialized front-end devices are on the market, as are systems that look for identifiable signs of DDoS activity in an organization's general traffic. Superficially, this offers some level of protection against these attacks.

The intrusion prevention system has grown more advanced in recent years, with increasingly impressive abilities to analyze traffic patterns and potential attack techniques to protect web resources from the threat of a DDoS. Should they continue to improve at a similar pace, these products could become a more robust line of defense in the future.

Nevertheless, even these systems are insufficient when deployed on their own. Just as with firewall-based protection, the ability to accurately separate legitimate traffic from a DDoS attack is central to their functionality. In light of the fact that DDoS attacks frequently take the form of legitimate traffic themselves, there is no guarantee that such signature-based defenses can provide a high level of assurance against the technique.

In the final analysis, the only way to provide truly robust DDoS protection to an organization's web assets is through the use of a carefully coordinated, multi-level system for identifying bad traffic and patterns, blocking out attack attempts and keeping legitimate functions running. Given the high level of technical and organizational expertise and specialization needed to get such a framework operational and keep it running, many companies opt to take advantage of specialist service providers instead of trying to construct this type of DDoS defense in-house. These specialists can offer emergency defenses like temporary bandwidth, expert traffic analysis and in some rare cases the ability to develop attack signatures in real time to block new or changing attacks.

Preparing a sturdy defense against DDoS attacks has become critical, especially for businesses with a strong online presence. In a recent Gartner report[12], the analyst firm states that client calls on DDoS have increased and DDoS services are nearing "must-have" status. The report goes on to state, "DDoS mitigation services should be a standard part of business continuity/disaster recovery planning and be included in all Internet service procurements when the business depends on the availability of Internet connectivity. Any Internet-enabled application that requires guaranteed levels of availability should employ DDoS protection to meet those requirements.

For more information on DDoS as well as attack monitoring and mitigation strategies, look for other Prolexic white papers in the Executive Suite Series.

About Prolexic

Prolexic is the world's largest, most trusted Distributed Denial of Service (DDoS) mitigation provider. Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission critical internet-facing infrastructures for global enterprises and government agencies within minutes. Six of the world's ten largest banks and the leading companies in e-Commerce, payment processing, travel/hospitality, gaming and other at risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world's first "in the cloud" DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida and has scrubbing centers located in the Americas, Europe and Asia. For more information on DDoS as well as attack monitoring and mitigation strategies, look for other Prolexic white papers in the Executive Suite Series, visit **www.prolexic.com** or call +1 (**954) 620 6002**.

1. http://news.softpedia.com/news/EVE-Online-Readies-the-Largest-Supercomputer-in-the-Gaming-Industry-35225.shtml
2. http://massively.joystiq.com/2011/06/14/eve-online-server-offline-due-to-ddos-attack/
3. http://cdn1.level3.com/App_Data/MediaFiles/4/C/C/%7B4CCD4BA3-4894-479D-9DE1-27A757395A0E%7Dmanaged_ddos_protection_whitepaper_001.pdf
4. http://cyber.law.harvard.edu/studygroup/cybercrime.html
5. http://news.cnet.com/Exposing-click-fraud/2100-1024_3-5273078.html
6. http://www.zdnet.com/news/dutch-police-take-down-bredolab-botnet/478818
7. http://www.reuters.com/article/2009/04/24/us-security-virus-idUSTRE53N5I820090424
8. http://arstechnica.com/microsoft/news/2011/03/how-operation-b107-decapitated-the-rustock-botnet.ars
9. http://www.darkreading.com/security/client-security/211201088/permanent-denial-of-service-attack-sabotages-hardware.html
10. http://www.theregister.co.uk/2008/05/21/phlashing/
11. http://www.bbc.co.uk/blogs/theeditors/2011/03/total_outage_of_bbc_websites.html
12. "Hype Cycle for Infrastructure Protection, 2011", John Pescatore, Gartner, 08/10/11