In today’s world, Distributed Denial of Service (DDoS) attacks on organizations are becoming more prevalent. The number of attacks are increasingly annually with no end in sight, and the damage these attacks inflict grows more severe. Because these attacks essentially disconnect an organization from the Internet, the after effects can be ruinous, particularly if these attacks are staged to cover other malevolent acts going on in the background. Who should be concerned? Any organization with a website and/or Internet-based service.

There are steps enterprises can take beforehand to help prevent a DDoS attack, as well as to recover from an event in a way that minimizes the damage and pain, however. Here, Computerworld sister publications CIO, CSO, Network World and IT World explain why DDoS attacks are becoming a serious threat, what kind of protection enterprises should put in place, and how to prepare themselves to respond if an attack should happen.
Open DNS Resolvers Increasingly Abused to Amplify DDoS Attacks, Report Says

The frequency of DNS-based DDoS amplification attacks has increased By Lucian Constantin, IDG News Service

OPEN AND MISCONFIGURED DNS (Domain Name System) resolvers are increasingly used to amplify distributed denial-of-service (DDoS) attacks, according to a report released by HostExploit, an organization that tracks Internet hosts involved in cybercriminal activities.

In the latest edition of its World Hosts Report, which covers the third quarter of 2012, the organization included data about open DNS resolvers and the Autonomous Systems – large blocks of Internet Protocol (IP) addresses controlled by network operators – where they are located. According to HostExploit, incorrectly configured open DNS resolvers – servers that can be used by anyone to resolve domain names to IP addresses – are increasingly abused to launch powerful DDoS attacks.

DNS amplification attacks date back more than 10 years and are based on the fact that small DNS queries can result in significantly larger DNS responses. An attacker can send rogue DNS requests to a large number of open DNS resolvers and use spoofing to make it appear as if those requests originated from the target’s IP address. As a result, the resolvers will send their large responses back to the victim’s IP address instead of the sender’s address.

In addition to having an amplification effect, this technique makes it very hard for the victim to determine the original source of the attack and also makes it impossible for name servers higher up on the DNS chain that are queried by the abused open DNS resolvers to see the IP address of the victim.

“The fact that so many of these unmanaged open recursors exist allow the attackers to obfuscate the destination IPs of the actual DDoS targets from the operators of the authoritative servers whose large records they’re abusing,” said Roland Dobbins, solutions architect in the Security & Engineering Response Team at DDoS protection vendor Arbor Networks.

“The fact that so many of these unmanaged open recursors exist allow the attackers to obfuscate the destination IPs of the actual DDoS targets from the operators of the authoritative servers whose large records they’re abusing,” said Roland Dobbins, solutions architect in the Security & Engineering Response Team at DDoS protection vendor Arbor Networks. “It’s also important to note that the deployment of DNSSEC has made DNS reflection/amplification attacks quite a bit easier, as the smallest response the attacker will stimulate for any query he chooses is at least 1300 bytes.”

Even though this attack method has been known for years, “DDoS amplification is used far more frequently now and to devastating effect,” Bryn Thompson of HostExploit wrote in a blog post. “We have seen this recently and we see it increasing,” added Neal...
Quinn, the chief operating officer of DDoS mitigation vendor Prolexic, via email. “This technique allows relatively small botnets to create large floods toward their target. The problem is serious because it creates large volumes of traffic, which can be difficult to manage for many networks without use of a cloud mitigation provider.”

Dobbins couldn’t immediately share any data about the recent frequency of DNS-based DDoS amplification attacks, but noted that SNMP (Simple Network Management Protocol) and NTP (Network Time Protocol) reflection/amplification attacks “can also generate very large, overwhelming attack sizes.”

In its report, HostExploit ranked the Autonomous Systems with the largest number of open DNS resolvers in their IP address spaces. The top one, controlled by Terra Networks Chile, contains more than 3,200 open resolvers in a pool of around 1.3 million IPs. The second one, controlled by Telecomunicacoes de Santa Catarina (TELESC) – now part of Oi, Brazil’s largest telecom operator – contains nearly 3,000 resolvers in a space of 6.3 million IP addresses. “It should be stressed open recursive nameservers are not a problem in themselves; it is the mis-configuration of a nameserver where the potential problem lays,” HostExploit said in its report.
Latest DDoS Attacks on Banks: A Teachable Moment

Strikes failed to disrupt banks’ online operations – but gave enterprises a better idea of how to tighten defenses

**By Antone Gonsalves, CSO**

The websites of major U.S. banks were attacked last December in an ongoing campaign that reflects the changing tactics used in distributed denial of service (DDoS) strikes, a security expert says.

The attackers, who call themselves the Izz ad-Din al-Qassam Cyber Fighters, launched attacks against the websites of U.S. Bankcorp, JPMorgan Chase & Co., Bank of America, PNC Financial Services Group and SunTrust Banks. The group, which has been targeting banks since September, warned of the latest assault on Pastebin the day before the attacks.

While the DDoS strikes failed to disrupt the banks’ online operations, they did provide some important lessons for enterprises faced with such a threat, said Dan Holden, director of security research at Arbor Networks, which performs DDoS mitigation for some of the targeted banks.

First off, the attacks showed that perimeter defenses such as firewalls and intrusion prevention systems can filter traffic for malware, but are useless against today’s complex DDoS attacks. Instead, corporations need on-premise technology that can provide up-to-the-minute information on an attack before it takes down a website or business application.

Security providers that offload DDoS traffic generated to overwhelm a website need to take another look at their capacity levels, Arbor said. The latest bank attacks show perpetrators are capable of targeting multiple organizations in the same industry, which can strain the capacity of mitigation service providers.

Another lesson learned is over the changing tactics of attackers. DDoS no longer means just flooding a site with traffic. Instead, attackers like the ones targeting the banks are bombarding sites to divert attention away from the application layer, so they can look for vulnerabilities more susceptible to a targeted attack. “The big lesson learned on the enterprise side is the fact that application DDoS can still take you out, even if the traffic is mitigated,” Holden said.

The focus on web applications has changed the profile of attackers. “While these [bank attacks] are not the most sophisticated attacks in the world, it’s obvious these guys are fluent in the web application side of things, as well as the DDoS side,” Holden said.

The application layer attacks were on HTTP, HTTPS and DNS, while the large-scale traffic was on a variety of Internet protocols, including TCP, UDP and ICMP, Arbor said. Login pages or any oth-
Poorly maintained sites are easy targets for deploying attack tools. With the exception of a few tweaks in the latest attacks, the tools used against the banks since September have been similar. The most prominent attack tool is one called Brobot, also called itsoknoproblembro, Arbor said. Two other tools used less often are KamiKaze and AMOS. So far, none of the attacks have been catastrophic. Interruptions have been brief and intermittent, at best.

The perpetrators and their motives remain unclear. The group has claimed it is protesting YouTube video trailers denigrating the Prophet Muhammad. The crude trailers promoted an amateurish film called the “Innocence of Muslims,” and sparked violent protests in many Muslim countries.

The sophistication of the attacks indicates more than just a grassroots campaign. Theories on the motivation include Iran striking back for U.S.-led economic sanctions and cybercriminals trying to distract banks from noticing fraudulent wire transfers.
AT&T Hit by DDoS Attack, Suffers DNS Outage

There are few details on the outage that appeared to hit companies across the U.S.

By Martyn Williams, IDG News Service

A DISTRIBUTED DENIAL-OF-SERVICE ATTACK aimed at AT&T’s DNS (Domain Name System) servers last summer disrupted data traffic for some of the company’s customers.

“Due to a distributed denial of service attack attempting to flood our Domain Name System servers in two locations, some AT&T business customers are experiencing intermittent disruptions in service,” an AT&T spokesman told IDG News Service by email at the time. “Restoration efforts are underway and we apologize for any inconvenience to our customers.”

The attack appeared to have affected enterprise customers using AT&T’s managed services DNS product. “Our highest level of technical support personnel have been engaged and are working to mitigate the issue,” AT&T said in a message on its service status page. But it had added there is “no estimated time” for restoring the service.

DNS is responsible for converting human-friendly domain names into the numeric IP (Internet protocol) addresses that computers use to route data. When it fails, computers are unable to route data to its intended destination, even though the destination server remains online and accessible.

A distributed denial-of-service (DDoS) attack attempts to flood a server or system with so many packets of data that it becomes difficult or impossible to reach for legitimate traffic. It doesn’t necessarily stop the server from working, but the overload of data results in the system being all but unusable. Service is returned to normal when the attack stops or when engineers find a way to absorb or deflect the nuisance traffic.

“We got our first report of problems at 6:31 a.m. Pacific time,” said Daniel Blackmon, director of software development, at Worldwide Environmental Products. The company tests vehicle emissions and has remote units deployed that report back to central servers. “The problems mean none of the equipment we have in the field can contact our servers, and there is a limit to the amount of information they can hold offline.” •
4 Ways to Prepare for and Fend Off DDoS Attacks

Distributed Denial of Service events and other cyber-attacks are an unfortunate inevitability of doing business on the Web today. The four steps presented here will help your company prepare for and respond to a DDoS attack. By Jonathan Hassell, CIO

CYBER ATTACKS OF ALL KINDS are on the rise. It is a trend you ignore at your own peril. National Security Agency and U.S. cyber-command chief Keith Alexander said last year that Internet attacks of all sorts surged 44 percent in 2011 and are responsible for what he terms the “greatest transfer of wealth in history.”

In a world where you can rent an already-hacked botnet for about $20 to start your attack, and in a world where a criminal enterprise industry has developed to support amplifying attacks in progress, it is important to understand that these types of attacks are simply not going away. Are you ready for them? Are you considering the right points? Here are four strategies to help your organization prepare for and defend against Distributed Denial of Service (DDoS) events in the future.

1. Consider Over-Provisioning a Service in Advance

Most of us develop systems on strict budgets. There is a general resistance among financial types as well as information executives to pay for unused capacity. This makes good sense in and of itself—why waste your dollars on capacity, either bandwidth or compute, that you are not using? Many companies scale their systems to match a predictable but legitimate peak, such as Black Friday, Cyber Monday or another annual peak load.

In a DDoS attack, however, your site or resource can experience loads many times greater than even your highest peak activity—on the order of 10 or 20 times, if not more. Mind you, I’m not suggesting you budget capacity to pay hackers to blast your network with packets. While you are specing bandwidth and compute resources, though, it makes sense to give yourself a healthy margin of error, even on top of your peak.

With the advent of cloud computing, this has become easier. In most cases, it’s simple to spin up additional resources to either meet legitimate demand or ensure access to your services in the event your primary hosting site is under attack. Internet service providers and other providers are also usually quick to offer burst capabilities with their contracts. This way, you can access an assured, ready, additional amount of capacity in the
event you need it while not nec-
essarily paying full price for it dur-
ing those times when your load doesn’t demand it.

2 Don’t Be Bashful About Asking for Help

Many companies and businesses specialize in assisting customers before, during and after a cyber attack, and they serve all levels of clients. Akamai Technologies, Level 3 Communications and LevelLight Networks, for example, all serve large customers with highly trafficked sites, but their rates begin north of $10,000 per month just for a basic level of assistance. On the other hand, startups such as CloudFlare offer to take onto themselves the load of distributing your site across multiple data centers. They then engage in detection and mitigation services without involving your team. CEO Matthew Prince says CloudFlare datacenters see “more traffic than Amazon, Wikipedia, Zynga, Twitter, Bing and AOL combined.” If true, this certainly puts the company in the first tier of network experience and engagement.

With attacks increasing yearly and with no relief in sight, it’s important to engage a firm that meets your needs and get its assistance before an event. DDoS attacks are an expensive problem, but now a day’s defense against them is becoming simply a price of doing business on the web. After all, consider the revenue loss if your site were to become unavailable to the Internet. Every minute your page can’t be reached, dollars destined for your company’s coffers spill away to other businesses. The protection should seem justified when you think about it that way.

3 During a DDoS Attack, Be Quick to Dump Log Files

As network capacity increases, attacks become cheaper to mount, so attackers can scale the severity of their activities quite easily. According to Alex Caro, CTO and vice president of services for Asia Pacific and Japan for Akamai, “the biggest attack that we’ve seen is around 150 Gbps, and we expect much larger attacks in the future.”

As you can imagine, at that level logging explodes—on your servers themselves, as well as on the attendant devices that care for and feed your network. Firewalls, unified threat monitoring devices, servers and other systems usually can’t keep up with logging each individual request when an actual attack is in progress. Typically these devices begin falling over under the sheer load of logging each and every request, and their failures cause chain reactions with linked devices and systems, making the attack much more severe than just a lot of traffic. (That is much of the secret to DDoS attacks in the first place: causing enough load that other systems than the one initially targeted begin failing.)

These chain reactions are often difficult to predict and recover from. Consider the botched recovery job Amazon suffered with its Elastic Compute Cloud service after the power outages in the Washington, D.C. area in early 2012. While not an attack, once servers in the datacenter began recovering after utility power was restored, the large number of reboot requests created its own little denial of service and prevented many virtual instances from powering back up until the load lightened. The moral of this story: Don’t hesitate to dump your logs quickly once you know you’re under attack and they’re not giving you any more useful information.

4 Have a Good Response Plan Ready

If you experience a DDoS attack, you likely won’t have a chance to develop a response plan at the time of impact. Your services will be degraded, if not
disabled completely, and your highest priority will be restoring service and stopping the attack. These actions are aided by a detailed plan of mitigation developed in advance of an event.

Blogger Lenny Zelster has created a good-looking template for an incident response plan. His DDoS Cheat Sheet includes steps such as preparing contact lists and procedures in advance, analyzing the incident as it happens and spinning up your response processes, perform mitigation steps you’ve outlined for your action team and, finally, performing a thorough post-mortem to document lessons learned and amend the response plan with that experience for future incidents.

One takeaway here: Everyone works better during a crisis when there is a predefined procedure, with checklists and next actions already clearly laid out. Don’t deprive your incident response team of this wisdom. This is something you can do today at no cost. Get a team together, talk about your response and write the plan down. Be prepared.

DDoS attacks, cyber-intrusion events and other nefarious acts are simply a fact of life in an Internet-connected world. The key responsibility you have as a CIO is to make sure you have prepared for attacks, have a plan to mitigate them when they occur and have done your best to make your company able to withstand the attacks. The prospect of facing an attack with anything less should be a scary thought that kicks you into gear.
Earlier this year, the activist group Izz ad-Din al-Qassam Cyber Fighters was several weeks into Operation Ababil 2, and, as promised, once again directed distributed denial-of-service (DDoS) attacks at U.S. banks. The group has vowed to continue disrupting online and mobile banking sites until all instances of the movie “Innocence of Muslims” are removed from YouTube.

Numerous banks have been attacked, including PNC Bank, Fifth Third, HSBC, JPMorgan Chase, Citibank and others. For the financial institutions, it’s déjà vu all over again, as they were similarly attacked last September and October. The banks have all suffered daylong slowdowns and, at times, complete outages. Security experts say these are the largest cyberattacks they’ve ever seen.

It’s disturbing that this second round of attacks has had even a modicum of success in disrupting banking services. After all, the banks were forewarned that the DDoS attacks would be coming, and thus they had ample time to put preventive measures in place. There are anti-DDoS technologies that can mitigate these types of attacks and lessen the effects on the victim businesses.

Every company with a website and any type of online service should take notice of these attacks; they aren’t exclusive to financial institutions. DDoS attacks can be initiated by anyone with motivation and a few dollars. In fact, it’s incredibly easy for anyone to get DDoS as a service. There’s a series of advertisements running on YouTube for something called “Gwapo’s Professional DDoS Service.” These ads boldly describe how “Gwapo” will perform a denial of service against any target website for a fee. The cost depends on the strength and duration of the desired attack. Gwapo simply aims a botnet at the target website and fires excessive traffic to achieve the objective of an outage.

Why would someone attack a website? Some people, like Cyber Fighters, use DDoS to make a political statement. Others do it to extort money, holding the website hostage via an outage until a ransom is paid. Unscrupulous people use DDoS to disable a competitor. Some security experts believe that DDoS attacks are often a smoke-screen to cover up other illicit activity. While administrators are focused on getting their website functioning again, the perpetrator is planting malware or stealing information. In fact, this proved to be the case in some of the earlier attacks on the U.S. banks.

Best Practices to Mitigate DDoS Attacks

How can you protect your company’s Web presence? Here are a few tips on what you can do now to head off a potential problem later. By Linda Musthaler, Network World
How can you protect your company’s Web presence? Here are a few tips on what you can do now to head off a potential problem later.

**Don’t count on a firewall to prevent or stop a DDoS attack.** The first step is to recognize that your firewall is insufficient protection against the types of DDoS attacks that are increasingly common today. Even a next-generation firewall that claims to have DDoS protection built-in cannot deal with all types of attacks. The best protection against DDoS attacks is a purpose-built device or service that scrutinizes inbound traffic before it can hit your firewall or other components of the IT infrastructure. This type of solution has one mission: to prevent excessive or malicious traffic from making your Web-based applications inaccessible to legitimate customers or users.

**Bake DDoS into your business continuity and disaster recovery plan.** Your company probably has a business continuity/disaster recovery (BC/DR) plan that outlines what to do in the event of some sort of business interruption or outage. You need to include procedures for DDoS mitigation in this plan. This will help to minimize any delay in responding to an attack and help assure that your company executives will commit the necessary resources for prevention and mitigation.

**Know the signs of an active attack.** Not all disruptions to service are the result of a denial-of-service attack. There may be technical problems with a particular network, or system administrators may be performing maintenance. However, the United States Computer Emergency Readiness Team (US-CERT) advises that the following symptoms could indicate a DDoS attack:

- Unusually slow network performance (opening files or accessing websites)
- Unavailability of a particular website
- Inability to access any website
- A dramatic increase in the number of spam emails received

**Know your customers and lock out unexpected transactions.** Most companies have a limited geography for where they do business—even if that geography is the entire country. If your company isn’t expecting people from, say, Eastern Europe or China to be placing orders via your website, the presence of inbound traffic from those geolocations may indicate trouble. If your anti-DDoS solution has the feature, restrict transactions that originate in locations where you don’t typically do business.

**Measure the financial impact of being offline for a period of time.** How much would it cost your company if no Web transactions could take place for four hours? Eight hours? A full day? The cost of an outage varies greatly by company. Calculate what the financial impact would be to your company so that you can justify to executives the expense of DDoS mitigation services.

If you are the victim of a DDoS attack, look for fraud, data breaches or other criminal activity. Many security experts believe that DDoS attacks may be smokescreens to hide other cybercrimes, including data breaches or financial fraud. Payloads in the attack traffic could be dropping malware on your servers. If your company does experience a DDoS attack, do a very thorough inspection of all system logs to determine if other malicious activities took place during the attack period. If your website supports credit transactions, be especially mindful of your PCI/credit processing environment. Be sure to deploy defenses at the perimeter of your card holder data environment as required by PCI-DSS.

**Know who to call to stop an attack.** If you don’t have an anti-DDoS so-
lution in place, then at least know who to contact immediately if you suspect your company is under attack. It's prudent to explore the dedicated anti-DDoS solutions on the market and decide which vendor/solution provider to call if the need arises. It's like choosing your doctor before you get sick so you don't waste valuable time figuring out what to do in emergencies. DDoS attacks are on the rise. Every good security plan has to include mitigation in order to minimize the effects of a service outage.
DDoS & Downtime: Considerations for Risk Management

This paper draws on Verisign’s DDoS mitigation expertise to examine the threat of DDoS in the context of IT availability and enterprise risk management.

▶ Download

DNS: Risk, Reward and Managed Services

An active DNS management strategy is increasingly important to enterprises due to the mounting requirements around protection and availability of critical web systems. In this report, Yankee Group Research outlines the pros and cons of in-house, ISP and managed service provider DNS management options.

▶ Download

Combining Cloud-based DDoS Protection and DNS Services to Thwart the Threat of DDoS

First published in SC Magazine, this article discusses the threat of Distributed Denial of Service (DDoS), Domain Name System (DNS) as a common attack vector for DDoS, and makes the case for combined, cloud-based DNS and DDoS protection services to thwart the risks.

▶ Download

DDoS Mitigation - Best Practices for a Rapidly Changing Threat Landscape

Given the extraordinary and rapid changes in the DDoS terrain, traditional DDoS mitigation tactics are no longer sufficient to protect an organization’s critical web systems. Verisign has identified a set of best practices that enables organizations to keep pace with DDoS attacks while minimizing impact on business operations.

▶ Download

DDoS Malware – A Verisign iDefense Research Paper

Recently updated to include new attack vectors observed in late 2012/early 2013 with regard to highly publicized and targeted DDoS attacks. This technical brief covers DDoS-enabled malware and several DDoS-specific tools, their capabilities and the network indicators they generate while performing the attack methods.

▶ Download