FORRESTER®

For: Security &
Risk Professionals

Develop A Two-Phased DDoS Mitigation Strategy

by John Kindervag, May 17, 2013

KEY TAKEAWAYS

DDoS Attacks Are A Real Threat

Companies often worry that DDoS attacks are more hype than reality. But just because you haven't experienced a DDoS attack to date doesn't mean it won't happen. DDoS is a brutal and unexpected attack. Remember to plan for failure.

DDoS Requires A Two-Phased Mitigation Strategy

DDoS is a complex problem that requires a thoughtful solution. You will need a strategy that keeps your local connection up at the beginning of an attack and then cleans the upstream traffic prior to it reaching your network.

Start Planning To Defend Yourself Against A DDoS Attack

The great WWII General Dwight D. Eisenhower once said, "In preparing for battle I have always found that plans are useless, but planning is indispensable." Planning is preparation. In the fog of war, your plans may well need to change, but the planning you've done will still provide value and help you respond more effectively.

Develop A Two-Phased DDoS Mitigation Strategy

Protect Yourself From Hacktivists And Other Cybercriminals

by John Kindervag
with Rick Holland, Heidi Shey, Stephanie Balaouras, and Jessica McKee

WHY READ THIS REPORT

Until recently, distributed denial of service (DDoS) attacks had been part of infosec lore: something you heard about but rarely experienced. With the rise of hacktivist groups and other cybercriminal organizations, DDoS has once again raised its ugly head. Today, these attacks are one of the most prevalent cyberassaults in our constantly changing threat landscape. Bank of America, MasterCard, PayPal, Sony, Visa, and many more of the world's largest companies have all been victims of DDoS attacks. These unpredictable attacks continue to increase and grow in sophistication by the day. The availability of an organization's critical systems depends on its ability to adapt and scale across its online infrastructure and protect it from these types of incidents. This report will provide an overview of the DDoS threat and provide insights into how to protect your organization from these attacks.

Table Of Contents

Notes & Resources

Forrester interviewed nine vendor companies: Akamai, Arbor Networks, AT&T, BT, Fortinet, Neustar, Prolexic, VeriSign, and Verizon.

Related Research Documents

Develop Your Road Map For Zero Trust Network Mitigation Technology
May 9, 2012

Planning For Failure
November 9, 2011

Defend Your Business From The Mutating Threat Landscape
November 1, 2011

DDOS ATTACKS DOMINATE THE HEADLINES

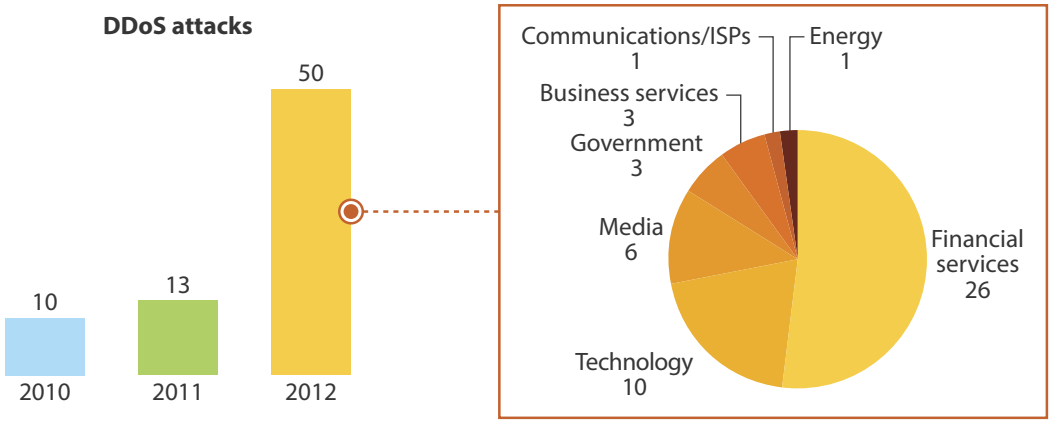
In October 2012, James Rohr, PNC CEO, was live on CNBC discussing his anxiety around cyberthreats and the company's run-in with a 58-GB-a-second DDoS attack that lasted 38 straight hours. This attack dramatically slowed processes and essentially "pummeled" his organization. He went further to say that the attack was most likely a test: "The stated goal was to disrupt the systems, but if you are really very paranoid about it, it is to test the vulnerabilities so you can come back with a stronger attack." This attack on PNC was part of a sequential set of attacks that also affected Bank of America, JP Morgan Chase, and Wells Fargo.[1] To help combat this trend in the US, the federal government created the Financial Services Information Sharing and Analysis Center (FS-ISAC) as part of President Obama's Cyber Security Executive Order to share threat information about the DDoS attacks on financial services public-facing websites.[2]

Once Dormant, DDoS Attacks Are The New Status Quo

The ability to access and use data on corporate networks and the Internet is fundamental to our modern data economy. This data has value, and today's cybercriminals are becoming more aggressive in their attempts to steal that data or disrupt access to it. Denial of service (DoS) attacks have been around for as long as networks have existed. These types of attacks prevent users from accessing applications or services — hence the name. Typically, they generate too much traffic for a site or network to handle, thereby effectively shutting it down. By the early 2000s, these types of attacks had become relatively dormant. This was because: 1) a DoS attack from a single machine was fairly trivial to trace, which left the attacker vulnerable to arrest and prosecution; and 2) there was not a real financial motivation to perform DoS attacks, as it is generally not an avenue for perpetrating data theft.

All of this has changed during the past few years. There has been a significant resurgence of a more-sophisticated mutation of this threat, known as a distributed denial of service attack. DDoS attacks have become prevalent because the software used to perform DDoS has advanced and because cybercriminals create massive botnets that use more machines in a distributed manner. Therefore, DDoS attacks are now at the forefront of today's cyberattacks (see Figure 1).[3]

Figure 1 DDoS Attacks Are On The Rise



Base: Publicly reported DDoS attacks*

Source: CyberFactors, a wholly owned subsidiary of CyberRiskPartners and sister company of CloudInsure.com
*Countries where these attacks occurred and were reported include: Australia, Brazil, China, France, Germany, India, Myanmar, Russia, Sweden, Thailand, Turkey, the US, and the UK

86101 Source: Forrester Research, Inc.

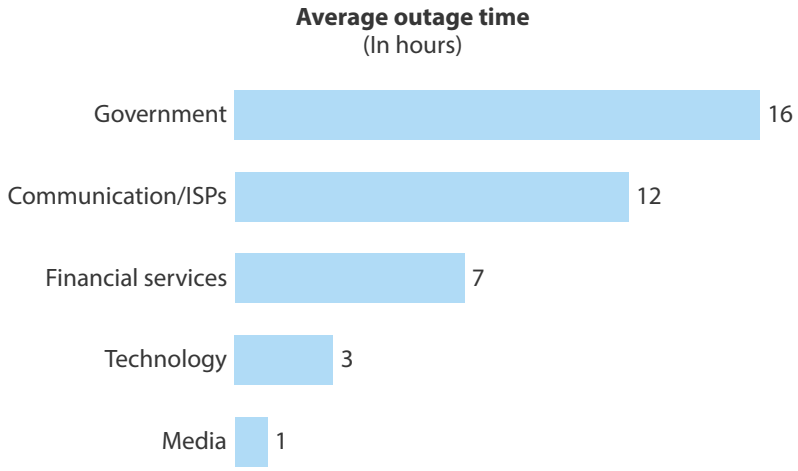
DDoS Attacks Create Extended Outages, Lost Revenue, And Customer Defection

DDoS attacks have become a quick and relatively easy way to disrupt your services, and the impact on the business and customer perception is enormous. DDoS attacks:

- **Create extended outages and cost millions.** The attack can last anywhere from hours to days, depending on how long it takes the victim to mitigate the traffic and how long the attacker can keep blasting the traffic at the victim's site and network.[4] The estimated financial impact is $2.1 million dollars lost for every 4 hours down and $27 million for a 24-hour outage. This is real money your company is losing, not to mention that downtime also damages your brand and causes customers to go your competitors.[5]

- **Frequently target financial services firms.** Statistically, the frequency of DDoS attacks across all industries is once a month, while the financial service industry suffers an attack as frequently as once a week (see Figure 2). Out of the 50 publicly documented DDoS attacks reported in 2012, cybercriminals targeted financial services firms 26 times. Despite being the hardest hit industry, because of preventive and mitigation measures, they suffered 7 hours of outage time on average per incident (see Figure 3). In contrast, government entities were the highest, at 16 hours of outage time on average per incident.[6] More often than not, downtime because of DDoS comes with a financial loss. Based on publicly reported cost estimates provided by DDoSed organizations, financial services firms suffered an estimated $17 million loss, on average, per incident in 2012 (see Figure 4).[7]

Figure 2 Downtime Caused By DDoS In 2012 Varied By Industry

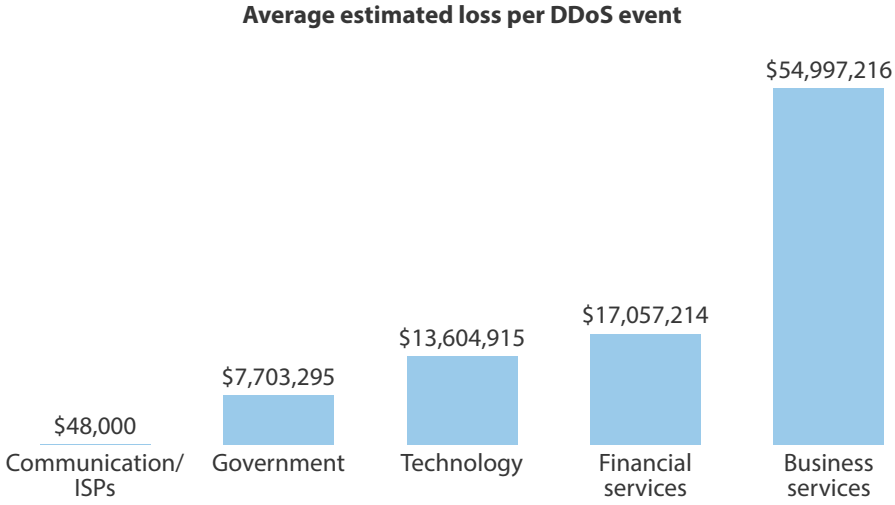


Base: 50 publicly reported DDoS attacks in 2012*

Source: CyberFactors, a wholly owned subsidiary of CyberRiskPartners and sister company of CloudInsure.com
*Countries where these attacks occurred and were reported include: Australia, Brazil, Germany, Myanmar, Russia, Sweden, the US, and the UK

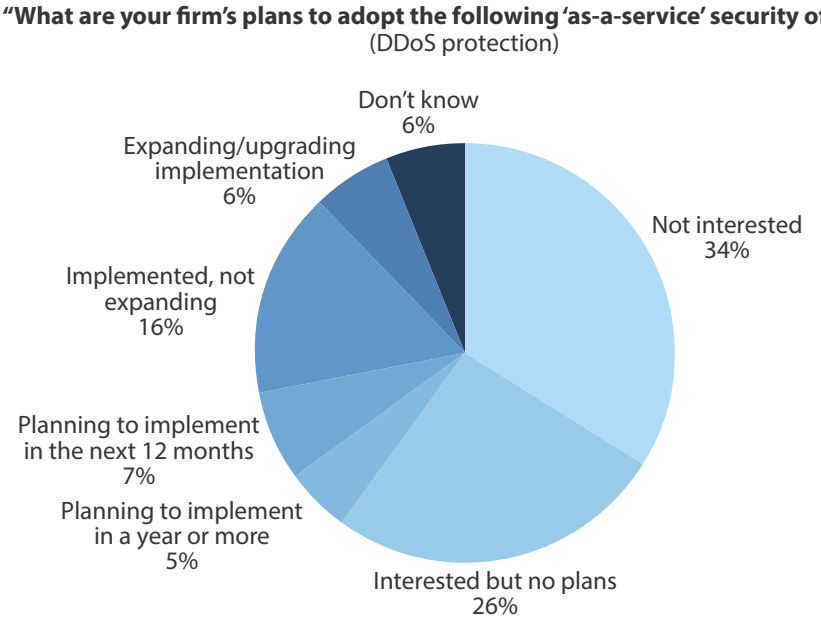
86101 Source: Forrester Research, Inc.

Figure 3 Average Losses In 2012 Caused By DDoS And Resulting Downtime Were Costly



86101 Source: Forrester Research, Inc.

Figure 4 DDoS Protection Services Are Not Widely Adopted



Base: 2,154 North American and European SMB and enterprise IT security decision-makers

Source: Forrester Forrsights Security Survey, Q2 2012

86101 Source: Forrester Research, Inc.

We All Live In The Same Bad Neighborhood, Yet Most Don't Prepare For DDoS Attacks

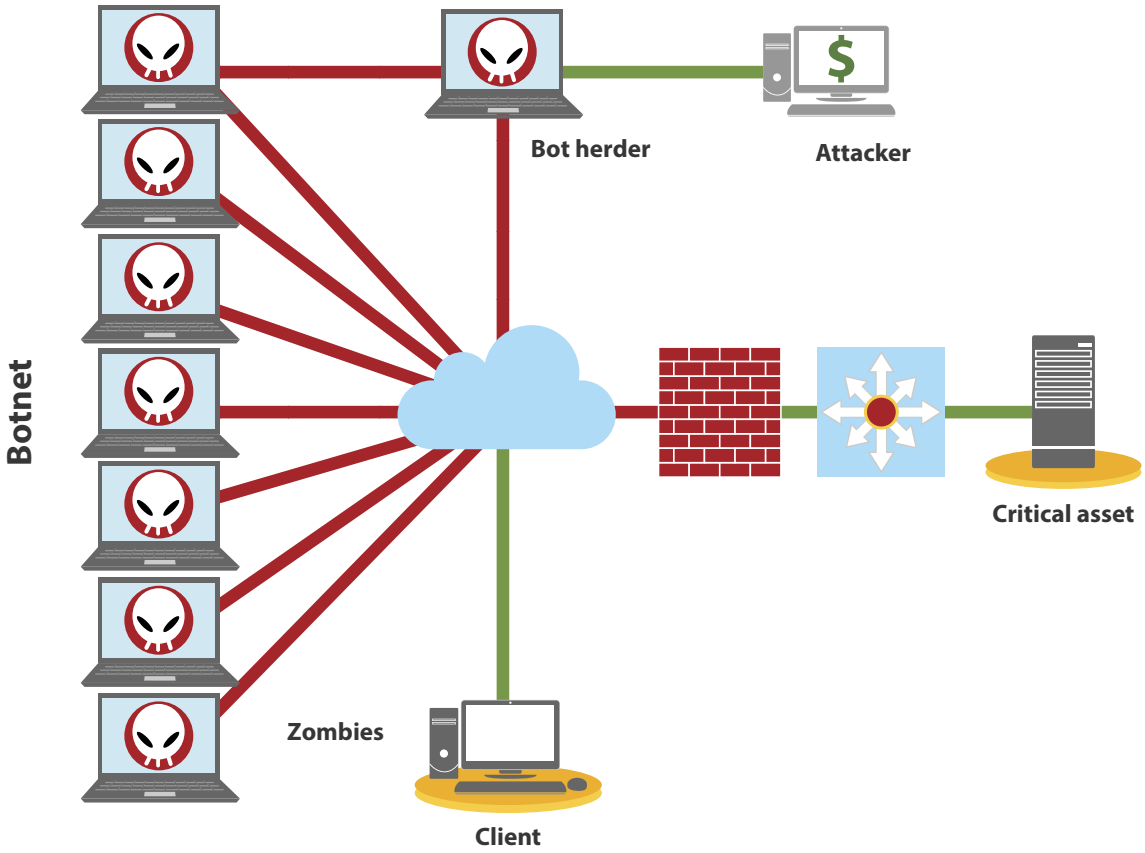
Does your organization connect to the Internet? Then yes, a DDoS attack can happen to you. These attacks are both random and prevalent. It's difficult to predict your risk of a DDoS attack. Do you have data that has value? Do you have intellectual property that might benefit an attacker? Have you angered someone who may want revenge? These are among the many reasons that cybercriminals perpetrate DDoS attacks. Although it's impossible to say with 100% certainty that your network will be the victim of a DDoS attack, it's easy to suggest that you should be prepared to defend yourself against this type of attack should it occur. Remember, we all live in the same bad neighborhood — the Internet — and if criminals were breaking into your neighbors' homes, it would be foolish to assume that for some unknown reason, they would spare you from their neighborhood crime spree. Unfortunately, we have found that:

- **Enterprise adoption of DDoS mitigation controls is quite low.** Forrester attributes the rise in DDoS attacks partially to the gap in DDoS mitigation controls. Despite the increasing prevalence of these attacks and the financial impact, according to Forrester's 2012 Security Survey, only 22% of organizations have implemented protection services.[8] Even more alarming,

60% of respondents had no plans to buy DDoS protection services (see Figure 5). This indicates that most companies will not be able to respond effectively should they suffer a DDoS attack. Trying to determine how to mitigate these attacks after they've begun is too late and will become very costly. You can't just flip a switch and have DDoS protection without prior planning.

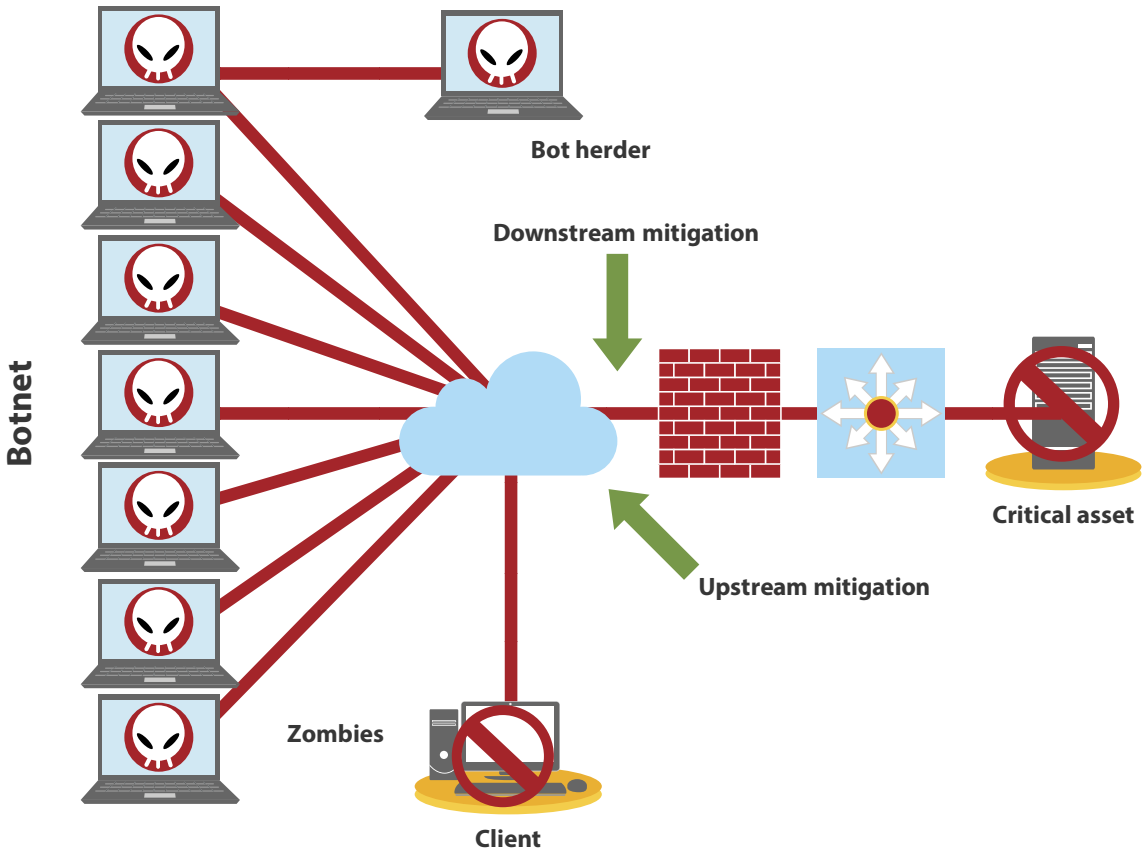
- **Enterprises are not learning from the experiences of the financial services industry.** As rampant as DDoS attacks are in this industry, their recovery time isn't bad relative to other sectors such as the government, which has the longest average outage time. A major factor behind the resiliency of the financial services sector is the adoption of advanced DDoS mitigation tools and reliance on third-party managed security providers.

Figure 5 Anatomy Of A Botnet



86101 Source: Forrester Research, Inc.

Figure 5 Anatomy Of A Botnet (Cont.)



86101 Source: Forrester Research, Inc.

UNDERSTANDING DDOS

A DDoS attack starts with the creation of a botnet. A botnet is a vast collection of remote computers that cybercriminals can use to perform attacks such as DDoS. What's interesting about a botnet is that the individual who controls it — known as a bot herder — does not own the computers — at least not financially. The bot herder has infected these remote machines with some type of malware that allows the bot herder to control each machine in the botnet without the machine owner's knowledge. Known as zombies, these bots exist all over the Internet, and the bot herder can control them as a single malicious entity.

The bot herder then makes the botnet available to a wide range of attackers who can rent out a portion or the entire botnet for an hourly or daily fee. This protects both the attacker and bot herder from discovery. In the case of the bot herder, it's true because traffic created by the bot will be traced

to zombie machines that typically mask the bot herder. In the case of the attacker, it's true because he has merely provided targeting information to the botnet — essentially outsourcing cybercrime to a third party. Reportedly, cybercriminals can rent botnets for as little as $100 a day.[9] In fact, launching this type of attack today is as easy as signing up for Gmail and as cheap as paying an attacker $9.10 an hour to administer a DDoS on your target of choice.[10]

Another factor has been the creation of DDoS toolkits, which has made launching a DDoS attack easier than ever. The game changed when the hactivist group Anonymous used a simple DDoS attack tool known as "Low Orbit Ion Cannon" (LOIC). LOIC was easy to download, install, and use and became responsible for the takedown of a vast array of websites.

DDoS Attacks Target Your Networks And Applications — On-Premises Or In The Cloud

There are two primary ways that attackers deny services to your users and customers — by attacking your network or attacking your applications — and one emerging way:

- **Network-level attacks.** In these attacks, cybercriminals target the network. Attackers will send so much illegitimate traffic to the network that it will become overloaded and unable to respond to valid service requests. By manipulating the underlying network protocols such as ICMP or TCP, an attacker can use DDoS techniques to effectively bring the network down. Sometimes called volumetric attacks, the industry often gives them adorable names such as "The Ping of Death" or "Smurf."[11]

- **Application-level attacks.** As the world has become more web-dependent, application attacks targeted at specific websites have become more common. For example, in an eCommerce application layer attack, the attacker replicates an unsupportable flood of the "add to cart" feature. This generates more traffic than the site can handle and causes legitimate users to receive error messages. Applications are more vulnerable to performance-related issues and bandwidth. According to a recent DDoS study from Arbor Networks, application-layer attacks have become increasingly common during the past few years, with 86% of the survey's 193 respondents reporting application-layer attacks targeting web services. Interestingly, during the past few years, there has been a significant increase in HTTPS attacks, with 37% of the respondents seeing application-layer attacks targeting this service, up from 24% the previous year.[12]

- **Cloud-level attacks.** Another type of DDoS attack is on the horizon. As applications continue to move outside the network, an interesting opportunity exists for attackers. By zombieing-out a machine inside a corporation's cloud, they can use a cloud-based botnet to launch DDoS attacks against victims outside the cloud. While no provider or customer has publicly reported cloud-level attacks, the advent and rapid adoption of cloud-based services makes this a real possibility.

Understanding DDoS Attack Motivations

There is a degree of randomness when it comes to the motivations behind DDoS attacks. With prepackaged toolkits widely available and relatively cheap, just about anyone can launch an attack on-demand. It would seem that any person with any number of incentives can deploy a DDoS. The main motivations for DDoS seen today include:

- **Hactivists driven by political and ideological goals.** This type of attacker often acts when angry or as a response to a perceived injustice. In January 2011, George Hotz found a way to jailbreak Sony's Play Station 3, which he publicly shared.[13] Sony subsequently sued him for publicly posting his PS3 hacking resources. In retaliation, Anonymous launched a DDoS attack on the company as a response to what they viewed as an infringement of Hotz's freedom of speech.[14]

  A similar case was the DDoS attack on MIT's website in January 2013. Anonymous brought down the university's site over their treatment of Reddit cofounder Aaron Swartz, a programmer and online activist, who committed suicide while facing charges for allegedly mass downloading nearly 5 million documents from online journal database JSTOR via the MIT campus network. Swartz was facing more than 35 years in prison if convicted. It's thought that Swartz wanted to liberate the data as a radical contribution to the open access movement, and Anonymous felt the university did not do enough to reduce the accusations against Schwartz.[15]

- **Criminals trying to extract money from victims.** It has been a common practice for certain types of cybercriminals to use DDoS attacks as a way to hold websites hostage for ransom. In this type of digital kidnapping, the attacker claims that he will release a website once the organization pays the ransom. Experts recommend never paying this extortion fee, as the act of doing so elevates a company on target lists.

- **Diversionary attacks that hide the real threat.** Earlier this year, San Francisco's Bank of the West suffered an intense DDoS attack. While the bank was investigating that attack, cybercriminals stole approximately $900,000.[16] The bank was distracted by the noisy DDoS attack; meanwhile, the hackers used digital sleight-of-hand to steal real money.

- **Competitive attacks using DDoS to gain an advantage.** Competitive attacks are where a company pays an attacker to DDoS a business competitor. This cybercriminal tactic is often seen in the online gaming world where anticompetitive DDoS can be used strategically. By bringing down a competitor's site and denying them anticipated revenue, an attacker can gain a competitive advantage. One new trend to keep watch on is the use of DDoS attacks in stock manipulation schemes. Attackers can place "bets" on the share price of a company and then launch a DDoS attack against that company to make certain they win their bet.

- **Political attacks making statements.** DDoS attacks achieve widespread notice — they're noisy and brutish. As such, they can be a very valuable political tool for governments, the politically disenfranchised, and even terrorists. A recent example is the arrival of a hacktivist group known as Izz ad-Din al-Qassam Cyber Fighters. Reportedly originating in Iran, these attackers have taken credit for a number of DDoS attacks on Western banks.[17] In posts on the website www.pastebin.com, the group said the DDoS attacks were in retaliation to a YouTube video insulting the Prophet Muhammad and many Muslims.

  Other examples of politically motivated attacks have occurred in countries in turmoil. A controversial election might lead to DDoS attacks against newspapers and voting systems in an attempt to sway the election to one side or another. This happened in Russia in 2011 during the height of elections; victims who were critical of the ruling United Russia party believed that the central government coordinated the attacks.[18]

ADOPT A TWO-PHASED DDOS MITIGATION APPROACH

DDoS mitigation requires a two-phased solution. To fully defend against these determined attackers, you will need a local short-term solution and a third-party service to provide long-term protection:

- **Downstream mitigation provides immediate defense at the point of attack.** The downstream portion of the attack occurs at your Internet or web farm gateway. To protect these fragile, yet critical, connections, it's imperative that you have some type of on-premises solution to keep your network and websites up during the initial attack. Thankfully, DDoS protection today is built into most of the network security platforms, such as the firewalls and IPS systems that you already use. Double-check that your devices have DDoS mitigation features. If they don't, it may be time to upgrade. While this type of downstream response might suffice for short-lived or small-scale attacks, it will be insufficient for longer-term or more-determined assaults. Since you will most likely only control the connection from your edge router inward, your on-premises equipment can't scrub the entire connection. To get clean pipes, you will have to rely on a third-party service that has access to the traffic upstream from your connection.

  Firewall vendors such as Check Point, Dell Sonicwall, Fortinet, and Palo Alto Networks have some level of denial of service mitigation built in. Intrusion prevention solutions such as those from Corero, HP TippingPoint, and IBM offer similar functionality.

- **Upstream services can help stop DDoS in the cloud.** Upstream protection provides DDoS mitigation much closer to the attacker and well before the threat traffic reaches your network's edge. There are distinct advantages to having one of these services as part of your overall DDoS mitigation strategy. These services see wide swaths of the Internet, so they're often aware of potential attacks before they ever pounce on your network and they have skilled operators who understand DDoS attack methodologies much more deeply than the typical security generalists.

When these services engage, they can stop the threat traffic and allow your network to go back to normal. There are a number of different types of anti-DDoS services available according to your individual needs. These include services offered by: 1) Internet service providers (ISPs) such as AT&T, BT, and Verizon, which can often bundle some level of DDoS mitigation service with the connectivity that they provide; 2) managed DNS services Neustar, Prolexic, and VeriSign, which use certain DNS scrubbing and redirection techniques to send threat traffic into a black hole; and 3) cloud services providers such as Akamai, which leverage a content delivery network (CDN) or similar private network to provide clean transport services to their clients.

RECOMMENDATIONS

CREATE A DDOS PLAN THAT CONNECTS TO YOUR INCIDENT RESPONSE STRATEGY

DDoS attacks are part of the modern threat landscape, and you can't ignore them. They provide a very powerful and damaging tool for malicious actors to use with ease and impunity. DDoS is a cost-effective attack methodology that we can expect to see continue to evolve as cybercriminals develop new techniques and new toolkits. In addition to the two-phased approach described above, Forrester also recommends that you:

- **Create a "plan of attacked."** The Internet is a very dangerous neighborhood, and your neighbors are under attack. Don't assume cybercriminals will decide to pass over your house. Start with the assumption that you will suffer a DDoS attack, and develop a response plan that helps you respond in a timely manner and without panic. You should create and test a policy detailing DDoS response procedures before you suffer an attack. Because a DDoS attack is often very public and affects your customers, this is a business and communication issue as well as a technical one. Make certain you identify all potential stakeholders and involve them in the plan's development.

- **Connect your plan to your incident response processes.** Consider DDoS mitigation a part of your incident response (IR) strategy.[19] While keeping your network or website up and running is your first priority, make sure that you tie this mitigation into your overall IR effort so that your IR team can analyze these attacks in the context of other threats. Remember, a DDoS attack might well be a feint for an even more dangerous attack coming on your flanks.

SUPPLEMENTAL MATERIAL

Methodology

Forrester collaborated with CyberFactors to obtain the data in this report. The data may contain publicly available information and/or proprietary data collected by CyberFactors. The analysis of the data is exclusively Forrester's. More information about CyberFactors is available at www.cyberfactors.com.

Companies Interviewed For This Report

Akamai

Arbor Networks

AT&T

BT

Fortinet

Neustar

Prolexic

VeriSign

Verizon

ENDNOTES

[1] There has been a surge in repetitive cyberattacks on banks. PNC CEO James Rohr spoke with CNBC about what he thought was motivating these hackers; here's a link to the entire interview. Source: Javier David, "Cyberattacks 'Huge Security Issue' for the US: PNC CEO," CNBC, October 18, 2012 (http://www.cnbc.com/id/49461040/Cyberattacks_039Huge_Security_Issue039_for_the_US_PNC_CEO).

[2] The Financial Services Information Sharing and Analysis Center gathers threat, vulnerability, and risk information about cyber and physical security risks faced by the financial services sector. Source: FS-ISAC (https://www.fsisac.com/).

[3] A note about the data source: CyberFactors aggregates data and information from publicly available sources on data breaches and incidents that are referred to as cyberevents in their database. If an organization suffers a DDoS attack, but for whatever reason this does not become public knowledge (e.g., reported in a media outlet, referenced in an annual report, or other public filing), it will not be counted in this database. As a result, the actual number of DDoS events is likely higher than what we show here.

[4] While researching for this report, Forrester spoke with John Jellema, global security product manager at Verizon Business, who gave insight into how costly extended outages are.

[5] Forrester Principal Analyst John Kindervag and Sean Leach, VP Technology at VeriSign, presented a webinar, "Assessing the Risk of DDoS: A Path to Proactive Protection." Source: VeriSign (https://www.verisigninc.com/en_US/forms/riskofddoswebinar.xhtml).

[6] Source: CyberFactors, a wholly owned subsidiary of CyberRiskPartners and sister company of CloudInsure.com.

[7] Operating expenses generally comprise the bulk of this cost, but other factors can also include regulatory fines if applicable, as well as legal settlements and outbound contact costs.

[8] Source: Forrsights Security Survey, Q2 2012.

[9] While researching for this report Forrester spoke with DDoS experts at Prolexic: Michael Donner, SVP, CMO; Stuart Scholly, president; Paul Sop, technology evangelist; and Neal Quinn, COO. They broke down the simplicity of launching DDoS specific cyberattacks and how important it is to invest in third-party mitigation tools.

[10] Forrester Principal Analyst John Kindervag and Sean Leach, VP Technology at VeriSign, presented a webinar, "Assessing the Risk of DDoS: A Path to Proactive Protection." Source: VeriSign (https://www.verisigninc.com/en_US/forms/riskofddoswebinar.xhtml).

[11] For a detailed taxonomy of DDoS attacks, read the report. Source: Jelena Mirkovic, Janice Martin, and Peter Reiher, "A Taxonomy of DDoS Attacks and DDoS Defense Mechanisms," UCLA Computer Science Department technical report (http://www.lasr.cs.ucla.edu/ddos/ucla_tech_report_020018.pdf).

[12] This report provides the results of Arbor Networks' eighth annual Worldwide Infrastructure Security Report. The survey covers a 12-month period from October 2011 through the end of September 2012. It was designed to collect the experiences, observations, and concerns of the operational security community. Source: Arbor Networks (http://www.arbornetworks.com/research/infrastructure-security-report).

[13] The term "jailbreak" refers to removing protections against running unauthorized software on an electronic device.

[14] The infamous hacking group Anonymous, which takes moral and ethical stances on certain issues, attacked Sony for its lawsuit against George Hotz, who essentially found a way to back up Sony games and play them from non-Sony hard drives. George Hotz made this information public, and Anonymous felt that once a Sony game was purchased it was the property of the owner and should be used wherever and however the owner saw fit. Source: "'Anonymous' hackers hit PlayStation and Sony websites in revenge for lawsuit," Mail Online, April 6, 2011 (http://www.dailymail.co.uk/sciencetech/article-1373621/Anonymous-hackers-hit-Playstation-Sony-websites-revenge-lawsuit.html#ixzz2OwcBK4T0, http://www.dailymail.co.uk/sciencetech/article-1373621/Anonymous-hackers-hit-Playstation-Sony-websites-revenge-lawsuit.html).

[15] Another hack by Anonymous was against the Massachusetts Institute of Technology for its involvement in the suicide of 26-year-old Aaron Swartz. Source: Noam Cohen, "A Data Crusader, a Defendant and Now, a Cause," The New York Times, January 13, 2013 (http://www.nytimes.com/2013/01/14/technology/aaron-swartz-a-data-crusader-and-now-a-cause.html?pagewanted=all&_r=0).

[16] A Christmas Eve cyberattack against the website of a regional California financial institution helped distract bank officials from an online account takeover and resulted in a financial loss of $900,000. Source: Brian Krebs, "DDoS Attack on Bank Hid $900,000 Cyberheist," KrebsonSecurity, Feburary 13, 2013 (https://krebsonsecurity.com/2013/02/ddos-attack-on-bank-hid-900000-cyberheist/).

[17] The hacktivist group Izz ad-Din al-Qassam Cyber Fighters has been launching DDoS attacks on US banks and credit unions; the motivation behind these attacks is still not clear. Source: Tracy Kitten, "DDoS Hacktivists: No U.S. Bank is Safe," Bank Info Security, January 2, 2013 (http://www.bankinfosecurity.com/ddos-hacktivists-no-us-bank-safe-a-5401/op-1).

[18] Websites of the Ekho Moskvy (Moscow Echo) radio station, the news portal Slon.ru, and election monitor Golos were taken down by cyberattacks during the height of the 2011 elections. Source: "Russian media, election watchdog silenced through cyberattacks," Info Security, December 5, 2011 (http://www.infosecurity-magazine.com/view/22444/russian-media-election-watchdog-silenced-through-cyberattacks/).

[19] An incident response plan, like a business continuity (BC) or an IT disaster recovery (DR) plan, is your organization's immediate response to a specific threat. IT security professionals should talk with their counterparts in BC/DR; the fundamentals of strategy development and response planning are very similar as are the lessons learned. Your organization wouldn't want to learn how to cut over from a failed primary site to a backup hot site after the outage occurred. You have created a DR plan to handle this scenario. By the same token, you don't want to develop your incident response plan in real time while cybercriminals are pilfering your intellectual property. A well-defined incident management program provides organizations a script to follow when incidents occur. See the November 9, 2011, "Planning For Failure" report.

About Forrester

A global research and advisory firm, Forrester inspires leaders, informs better decisions, and helps the world's top companies turn the complexity of change into business advantage. Our research-based insight and objective advice enable IT professionals to lead more successfully within IT and extend their impact beyond the traditional IT organization. Tailored to your individual role, our resources allow you to focus on important business issues — margin, speed, growth — first, technology second.

FOR MORE INFORMATION

To find out how Forrester Research can help you be successful every day, please contact the office nearest you, or visit us at www.forrester.com. For a complete list of worldwide locations, visit www.forrester.com/about.

CLIENT SUPPORT

For information on hard-copy or electronic reprints, please contact Client Support at +1 866.367.7378, +1 617.613.5730, or clientsupport@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.

Forrester Focuses On Security & Risk Professionals

To help your firm capitalize on new business opportunities safely, you must ensure proper governance oversight to manage risk while optimizing security processes and technologies for future flexibility. Forrester's subject-matter expertise and deep understanding of your role will help you create forward-thinking strategies; weigh opportunity against risk; justify decisions; and optimize your individual, team, and corporate performance.

« **SEAN RHODES,** client persona representing Security & Risk Professionals