SUCCESSFULLY COMBATING DDoS ATTACKS

NTT Communications | NTT America

AN NTT COMMUNICATIONS WHITE PAPER
AUGUST 2012

Executive Summary

The nearly limitless connectivity, information flow and transactional freedom of the digital age defy hyperbole and opportunities are practically boundless for businesses, organizations, governments and individuals.

But such online opportunities come with a cost—an expanded potential for ill-intentioned destruction of network assets. Establishing and developing an online presence carries with it a certain amount of vulnerability. Many leading global companies, prominent government entities, advocacy groups and small businesses alike have fallen prey to virtual attacks that exploit such vulnerability.

Distributed Denial-of-Service (DDoS) attacks are among the most prevalent and costly forms of such attacks, posing a serious threat to e-commerce and online businesses. During a DDoS attack, remote attackers or assailants generate a flood of traffic to a specific destination to disrupt a targeted website or server. The attack can come from one or multiple compromised machines or large networks of infected computers (i.e. botnets) to flood the target with high volumes of illegitimate traffic. As the targeted systems strain to keep up with the inundation, the ensuing slowdown or shutdown blocks legitimate users from access. The goal of most DDoS attacks is to force the targeted computing resources completely offline. They frequently succeed.

The business costs of such attacks are substantial. They range from monetary damage directly associated with the disruption itself to the longer term implications for the company's reputation, competitiveness and brand.

This white paper explores the scope, characteristic targets, and consequences of DDoS attacks. It also discusses the keys to mitigating such attacks, and discusses the attributes that differentiate NTT America's approach to solutions.

Scope of DDoS Attacks & Threats

All online businesses and organizations are at risk for DDoS attacks. It is estimated that there are an average of 7,000 such attacks every day, although not all are detected or reported by their targets. Many online entities are unaware of such attacks, erroneously associating spikes in traffic and system slowdowns with normal fluctuations or changes in demand patterns. But DDoS attacks are ubiquitous, constantly preying on the websites and servers of a wide variety of online businesses and organizations from all points on the Internet spectrum.

DDoS attacks are rising in number, size, frequency and complexity. With continuing Internet growth, the numbers of attacks are increasing proportionally as new targets are created every day. This means attacks are readily available to anyone with a PC and Internet connection. DDoS attack tools and services are openly sold and botnets can be rented through such common channels as YouTube.

Broader vulnerability to attacks has been further heightened by the explosive growth in mobile phones, tablets, and other devices. These advances have taken the Internet off the desktop and allow practically unlimited online access to increasing numbers of users—and more target opportunities for DDoS attackers. Some projections envision Internet-connected mobile devices hitting the 10-billion mark in coming years. This expanded connectivity opens the door further to DDoS attacks, especially since many mobile device users tend not to regard these devices as portable computers. Such users are less likely to be aware of or concerned about possible DDoS attacks.

DDoS attacks are rising in number, size, frequency and complexity

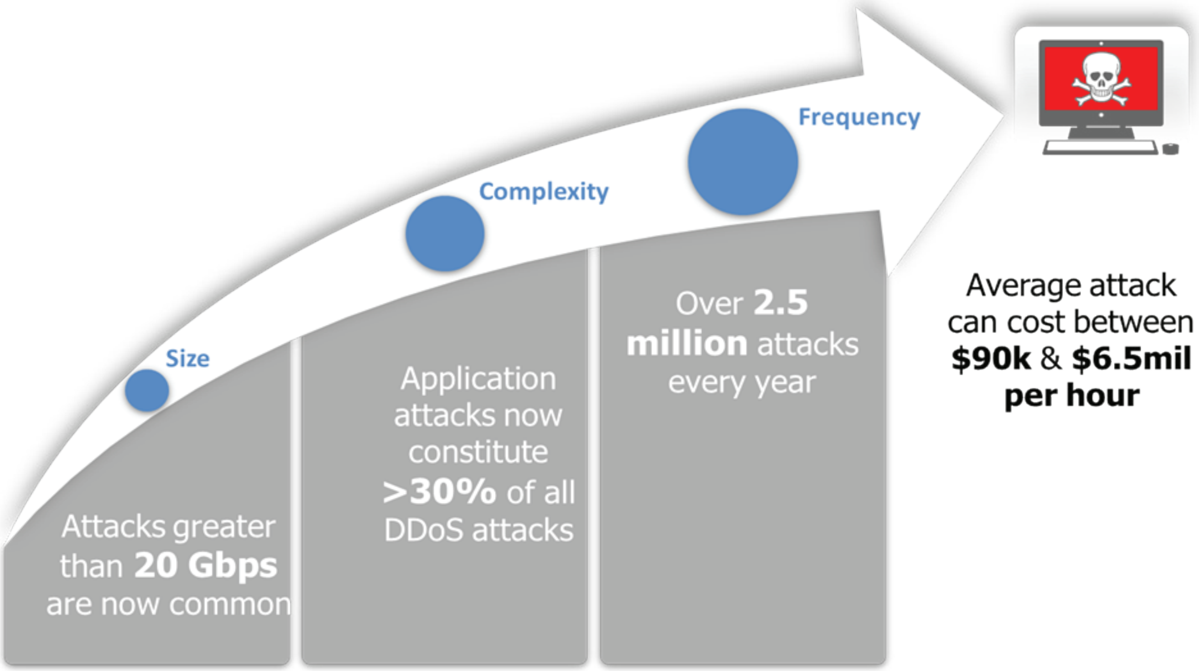
Reports from industry sources show that 9.5 petabytes of data were mitigated during the first quarter of 2012—the same amount of data it handled for all of 2011. “Hacktivism,” the term coined for attacks inspired by political, ideological or social beliefs and causes, increased 25 percent in the first quarter of 2012 compared to the first quarter of 2011. Because of the often public nature of hactivism and the media attention it consequently commands, such numbers will only escalate.

DDoS attack tools and services are openly sold and botnets can be rented through such common channels as YouTube

Besides the disturbing numbers, frequency and universal reach of DDoS attacks, the problem is further compounded by the ever-evolving sophistication, technical savvy and complexity of the attacks. DDoS attacks can range from simple network attacks to Domain Name System attacks to HTTP attacks. They can be volumetric, designed to overwhelm a host and make it unreachable, or attack application layers, targeting a specific service on the host. The use of multiple devices to amplify attacks means traffic can appear to be coming from all over the world. This makes it more difficult to block—and to trace to the perpetrators.

Attackers have also been able to move to smaller, more efficient botnets that make detection, analysis and mitigation even more challenging. Even as the quantity of attacks continues to rapidly increase, the intensity of attacks are increasing too. Attackers are relying on shorter, more powerful bursts of traffic for online onslaughts.

Widespread ignorance about DDoS attacks compounds the gravity of the problem. Many online enterprises are unaware that they have been attacked or are targets of such attacks. As


Frequency
Complexity
Size
Attacks greater than **20 Gbps** are now common
Application attacks now constitute **>30%** of all DDoS attacks
Over **2.5 million** attacks every year
Average attack can cost between **$90k** & **$6.5mil per hour**

Source: NTT Communications

a result, precautions, protections and mitigation efforts are inadequate. False confidence or arrogance can be an issue too, as many businesses and organizations believe their defenses to be sufficient when they are not.

Common Targets of DDoS Attacks

Understanding the most common motivators for DDoS attacks confirms the reality that all online businesses and organizations are at risk. There are four major categories within which nearly all DDoS attacks fall. All online businesses and organizations are potentially susceptible to most of these typical “motivators.”

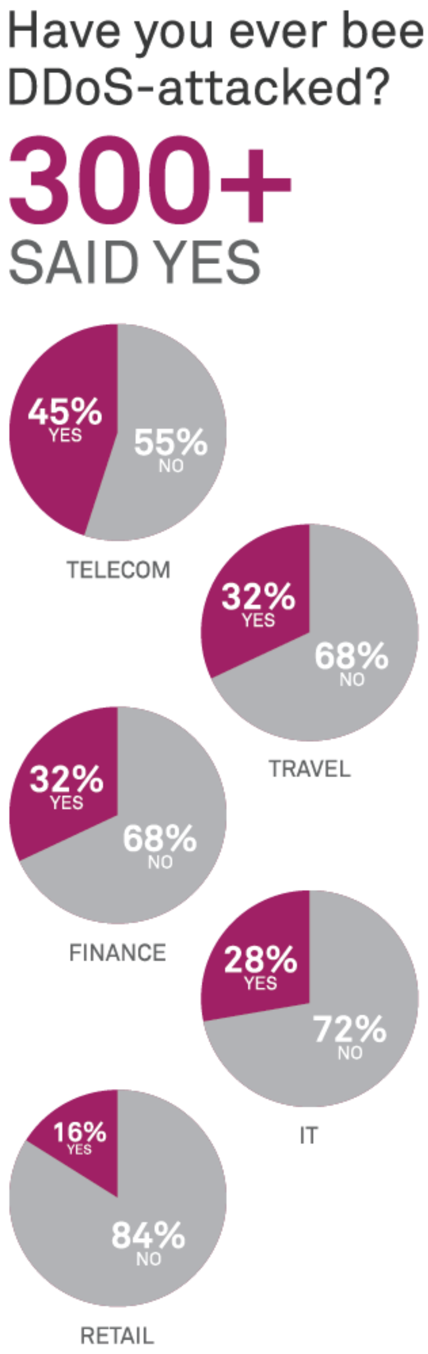
One common motivator is hactivism, in which social and political protests take the form of DDoS attacks. Groups like Anonymous have gained some measure of media notoriety by taking down some of the world’s most prestigious companies and brands.

A second reason DDoS attacks occur is extortion and other financial motivators. Extortion attempts typically involve a threatened DDoS attack if a ransom is not paid by a specific deadline. The attacker seeks a substantial ransom payment by threatening the online business with the even more substantial financial loss that will be incurred in a DDoS attack.

A third motivator for DDoS attacks is cybercrime, cyber espionage and hate crimes. Such attacks can come from competitors, disgruntled customers, former employees, or a group of hackers intending a hate crime.

A fourth major category of DDoS attack motivators is “just because”—instances of hacker experimentation, challenges between hackers, or attempts to gain prestige among peers.

There are some obvious likely targets suggested by such analysis. High profile business or government entities, or any online organization engaged in or representing activities or causes which might be construed as controversial, are often targets of hactivism. Financial institutions and e-commerce sites with substantial assets controlled by online systems are promising victims for extortionists. Companies in highly



Source: Neustar® Insights: DDoS Survey Q1 2012

competitive businesses, gaming sites (where large sums of money are lost or membership privileges can be suspended) and online organizations tied to specific minority, religious or alternative lifestyle groups may be more vulnerable to cybercrime and hate crimes. The "just because" class of DDoS attacks are more random, making any online business or organization a potential target. And obviously any company or organization that depends on web, DNS and email servers to reach large groups of people is a high-potential target for attackers.

No business or organization with an online presence is immune from DDoS attacks

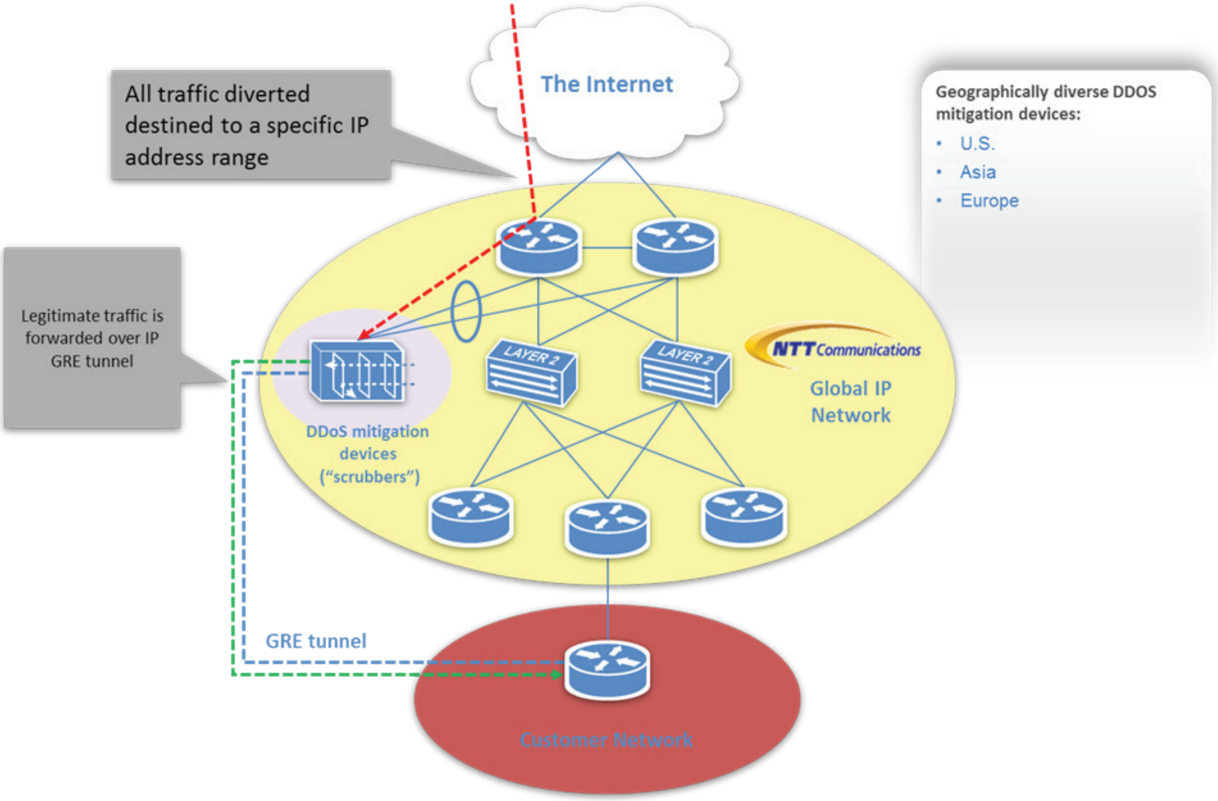
Importantly, all online businesses and organizations are potentially subject to most of these motivators from somewhere or someone, which means that all are at risk.

Some specific industries are witnessing especially acute accelerations in DDoS threats. Most notably, a DDoS attack report found that the financial services industry experienced nearly three times the number of attacks during the first quarter of 2012 compared to the same period in 2011. A Neustar Insights survey conducted during Q1 2012 found that telecommunications companies suffer the most DDoS attacks as an industry, with 45 percent of such participants positively responding when asked if they had ever been DDoS-attacked. This was followed by the financial and travel industries, both with 32 percent positive responses, the IT industry with a 28 percent positive response, and retail with 16 percent.

No business or organization with an online presence is immune from DDoS attacks, and all are potential targets. By understanding the mentality and motives of most attackers, a business or organization is in a better position to gauge its risk—and develop a strategy to minimize it.

Severity of the Threat—Damages

While reports and estimates about the monetary costs of a DDoS attack vary widely, all agree that such costs are substantial. Research indicates that such losses can range from $90,000 per hour to $6.5 million per hour, and that the


All traffic diverted destined to a specific IP address range
The Internet
Geographically diverse DDOS mitigation devices:
• U.S.
• Asia
• Europe
Legitimate traffic is forwarded over IP GRE tunnel
LAYER 2
LAYER 2
NTT Communications
Global IP Network
DDoS mitigation devices ("scrubbers")
GRE tunnel
Customer Network

Source: NTT Communications

average loss of revenue per hour during a Layer 7 DDoS attack is $220,000. The Neustar survey revealed that 70 percent of retailers state that outages cost more than $100,000 an hour—more than $2 million a day. These and other findings indicate that the damages caused by DDoS attacks are high, and depend on the specific operational features of the target.

While the costs of service outages are unique to every business, certain common elements can be considered in assessing immediate potential damage. These include operational costs to address the attack, help desk costs during a crisis, recovery costs, the value of lost employee output during downtime, lost business, lost customers, and penalties (including service level agreement credits).

But immediate financial costs are only part of the damage. Outages can cause significant damage to a company or organization's reputation and future business. It can instantly confer an advantage to competitors. Customer confidence and brand loyalty can be compromised. Such losses are not easily quantified, but can be much more significant in the long run than the immediate, quantifiable financial loss.

More importantly, the damage caused by DDoS attacks can be prevented and mitigated with the right strategy, planning, capabilities and resources.

Keys to Effective Mitigation of DDoS Attacks

A critical starting point for any business or organization is awareness. Conducting a baseline analysis to identify potential system vulnerabilities, understanding the signs that an attack is in progress, and making DDoS protection an organization-wide initiative are good first steps. Learning about industry-specific trends in DDoS attack activity, changing attack trends and the motivators behind attacks will also help in preparing for possible threats.

A second critical factor in successfully mitigating

DDoS attack is anticipation and planning. Every online business or organization needs a contingency plan for DDoS attacks. Such a plan should incorporate strategies for detection, defenses to be raised when an attack occurs, methods for monitoring attacks in progress, attack recovery provisions and post-attack notification of law enforcement. The plan should also specifically assign responsibility for DDoS protection, identify key contact people, and establish a process for managing communications through a single point of contact. Anticipating and planning for attacks enables a more orderly and rapid response when attacks occur. And speed is essential during an attack as damages rapidly accumulate.

Another key to effective mitigation is a comprehensive approach. DDoS attack methods evolve and adapt as rapidly as technology itself, and there is no single technique, system or tool capable of handling the broad spectrum of potential threats. Rather, a layered approach to security that integrates the most effective approaches and technologies gives target organizations the best response to DDoS attacks. Such a comprehensive approach enables the target to detect and identify bad traffic, stabilize the situation, identify root causes and key attack vectors, and filter traffic until the threat subsides.

Finally, expertise is an essential element in effectively mitigating DDoS attacks. There is no substitute for extensive experience and knowledge in preparing for and handling such attacks. The multi-level framework required for reliable protection is difficult for most online businesses and organizations to develop and manage in-house. When an attack is in progress, decisive and rapid action is required to minimize losses. These actions require extensive technical knowledge and an experienced grasp of the direction an attack is taking in the moment. A trusted mitigation service provider with the requisite security expertise is an invaluable partner, assuring that online assets and network availability are aggressively protected.

The damage caused by DDoS attacks can be prevented and mitigated with the right strategy, planning, capabilities and resources

NTT America DDoS Solutions

NTT America is uniquely positioned to partner with online businesses and organizations in protecting against DDoS attacks. NTT America's comprehensive solutions are based on state-of-the-art DDoS mitigation infrastructure, industry-leading protection platforms, best of breed technologies and a team of expert security engineers.

NTT America is fully prepared to combat large-scale attacks with instant analysis of the nature and extent of the attack, rapid redirection of the threat though the NTT America mitigation platform, and the ability to scrub attack data simultaneously at multiple points across Asia, North America and Europe. This geographical diversity means attack traffic can be filtered out close to where it enters the NTT Communications Tier-1 Global IP network for rapid, efficient protection.

NTT America uses the Arbor Peakflow SP Threat Management System, which is capable of surgical mitigation. This system ejects attack traffic and passes legitimate "clean" traffic through to the customer under attack, allowing business to continue to function during the attack. Once the DDoS attack subsides, original inbound routing is restored. Data collected during the mitigation is used to address any underlying issues revealed as a result of the attack.

Unlike many companies that offer protection services against attacks through automated processes, the NTT America team of expert security engineers monitors and guides the attack response, standing ready on a 24 x7 basis. This assures rapid and effective action when DDoS attacks occur.

Conclusion

DDoS attacks pose a threat to any business or organization with an online presence. These attacks are increasing in number, size, frequency and complexity. While certain industries have been harder hit than others, the common motivators for attacks readily apply to all online enterprises. The damages caused by such attacks are typically substantial.

Mitigating DDoS attacks requires awareness, planning, a comprehensive approach and expertise. A trusted mitigation service provider is an invaluable partner, assuring that online assets and network availability are aggressively protected.

NTT America is uniquely positioned to assist companies with their network security needs by protecting against and mitigating DDoS attacks. NTT America offers comprehensive solutions and the expertise to handle these attacks—and keep online businesses up and running.

NTT Communications | NTT America

About NTT Communications

NTT Communications provides consultancy, architecture, security and cloud services to optimize the information and communications technology (ICT) environments of enterprises. These offerings are backed by the company's worldwide infrastructure, including leading global tier-1 IP network, Arcstar Universal One™ VPN network reaching over 150 countries, and over 120 secure data centers. NTT Communications' solutions leverage the global resources of NTT Group companies including Dimension Data, NTT DOCOMO and NTT DATA.

Further information: **www.ntt.com | www.twitter.com/nttcom | www.facebook.com/nttcomtv**
For U.S. product and service information, please visit **www.us.ntt.net**.