VERISIGN™

WHITE PAPER

DISTRIBUTED DENIAL OF SERVICE (DDOS) ATTACKS:

EVOLUTION, IMPACT, & SOLUTIONS

VerisignInc.com

VERISIGN™

DENIAL-OF-SERVICE (DOS) ATTACKS HAVE EXISTED SINCE THE EARLY DAYS OF COMPUTING AND HAVE EVOLVED INTO COMPLEX AND OVERWHELMING SECURITY CHALLENGES. ORGANIZATIONS HAVE HAD TO WORRY NOT JUST ABOUT DOS ATTACKS, BUT DISTRIBUTED DOS ATTACKS (DDOS), AND MORE RECENTLY, DISTRIBUTED REFLECTOR DOS (DRDOS) ATTACKS. AS THE SOPHISTICATION OF TECHNOLOGY AND ITS SAFEGUARDS INCREASE, THE COMPLEXITY OF THE ATTACKS LEVELED AGAINST THAT TECHNOLOGY ALSO INCREASES.

As such, other more powerful DDoS variants are on the horizon. The problem is so wide-spread, fast-evolving, and confounding, that network security researchers, vendors, administrators, and law enforcement agencies are scrambling to keep up. DDoS attacks of multiple Gigabits per second (Gbps) are now routinely observed. After analyzing one DRDoS attack in early 2006, it was determined that the attack could have easily reached 120 Gbps. This is a staggering number since the largest non-multiplexed backbone connections today are 40 Gbps (OC-768) connections[1]. This paper will outline the evolution of DDoS attacks, discuss the current state and likely future state of the situation, and present some ideas for more comprehensive solutions.

As the threat has changed, so too must the strategy for defending against it. Traditional, network border devices are no longer sufficient to provide protection. Organizations must look at a security-in-depth approach in order to fully prepare for attacks. Part of that strategy is employing an "in-the-cloud" DDoS security service that identifies and filters traffic upstream of the organizational network. The solution should incorporate:

- Notification and alerting mechanism
- Sufficient bandwidth to absorb the attack
- Filtering technology that excludes only unwanted traffic
- A distributed model to create and maintain redundancy
- A logging/correlation system to collect detailed attack data

THE EVOLUTION OF DENIAL OF SERVICE ATTACKS

Although the methods and motives behind Denial of Service attacks have changed, the fundamental goal of attacks, to deny legitimate users of some resource or service, has not. Similarly, attackers have always, and will continue to look for methods to avoid detection. The evolution in the technology of DoS attacks originates from this fundamental premise: establish a denial of service condition without getting caught.

Malicious actors constantly explore new ways to leverage today's technology to meet their goals. Attackers work hard to engineer new techniques to distance themselves from the victim while amplifying the impact of their attack. Much of the evolution in DoS attacks goes hand-in-hand with the use and popularity of botnets. Botnets provide the perfect tool to help magnify the impact of an attack while distancing the attacker from the victim.

1 AT&T News Room: www.att.com/gen/press-room?pid=4800&cdvn=news&newsarticleid=24888

Building a Botnet

The earliest DoS attacks utilized one host machine to create the denial of service condition. Because of the ease of detection and, in turn, mitigation of this type of attack, attackers rapidly migrated to a more distributed model.

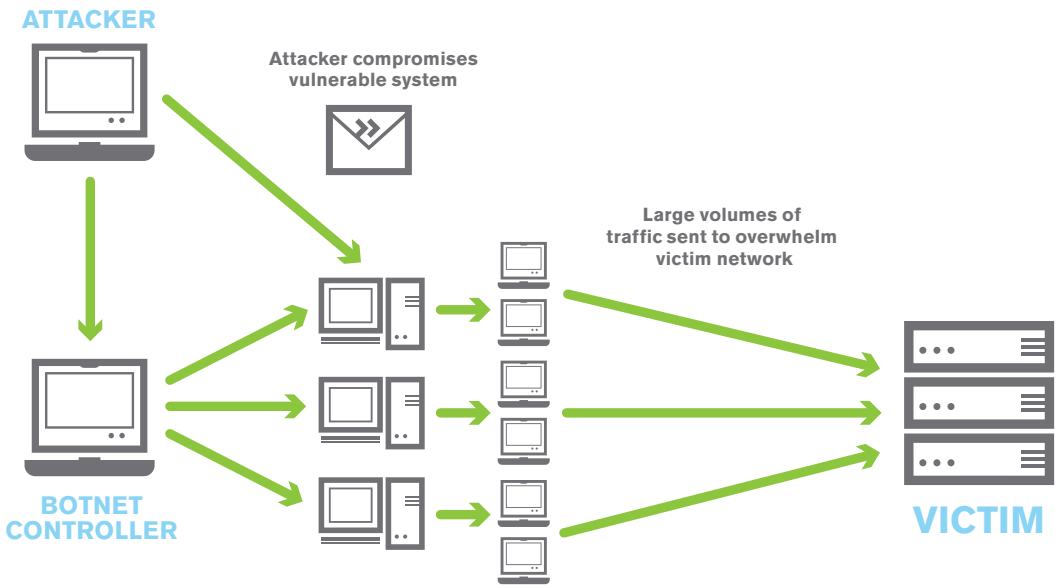
The Distributed Denial of Service (DDoS) attack leverages multiple sources to create the denial-of-service condition. By using multiple sources to attack a victim, the mastermind is not only able to amplify the magnitude of the attack, but can better hide his or her actual source IP address. The more layers that the attacker can place between him and the victim, the greater the chances of avoiding detection.

Today's DoS attacks are generally all distributed in nature because of the ease in which malicious actors can compromise other devices and leverage them for their purposes. Once a computer is compromised, the controller can leverage it to engage in nefarious activities. This collection of compromised devices, or a "botnet," is the launching pad for many of today's Internet threats. From spam to phishing, compromised devices sit at the core of many of today's Internet security challenges.

Attackers gain control of other computers by exploiting vulnerabilities in their operating system or other software. The rapid expansion of the Internet, lack of sufficient security tools, and illegally copied operating systems makes the landscape ripe for malicious actors to prey upon a host of system vulnerabilities. As a result, "botherders" are gathering and organizing attack machines in record numbers.

Individually, each compromised device, or "bot," can send small volumes of traffic that may do little harm. Collectively though, the network of compromised devices are capable of launching devastating DDoS attacks. Malicious actors have automated the "harvesting" process in order to compromise vast numbers of systems in a relatively short period of time. The largest botnets are amassed via Internet worms which compromise the victim computer and then use it as a launching pad to immediately compromise other computers.

FIGURE 1: SAMPLE ANATOMY OF A DDOS ATTACK



The 'Kraken' botnet, which reportedly overtook 'Storm' as the largest botnet on the Internet, is suspected to have 400,000 active bots, according to researchers at security firm Damballa[2].

Botnets and DDoS

The connection between botnets and DDoS attacks is so intertwined it is difficult to separate the two. According to a recent Yankee Group study of Tier 1 ISPs[3], DDoS attacks ranked first on a list of security threats, with botnets a close second.

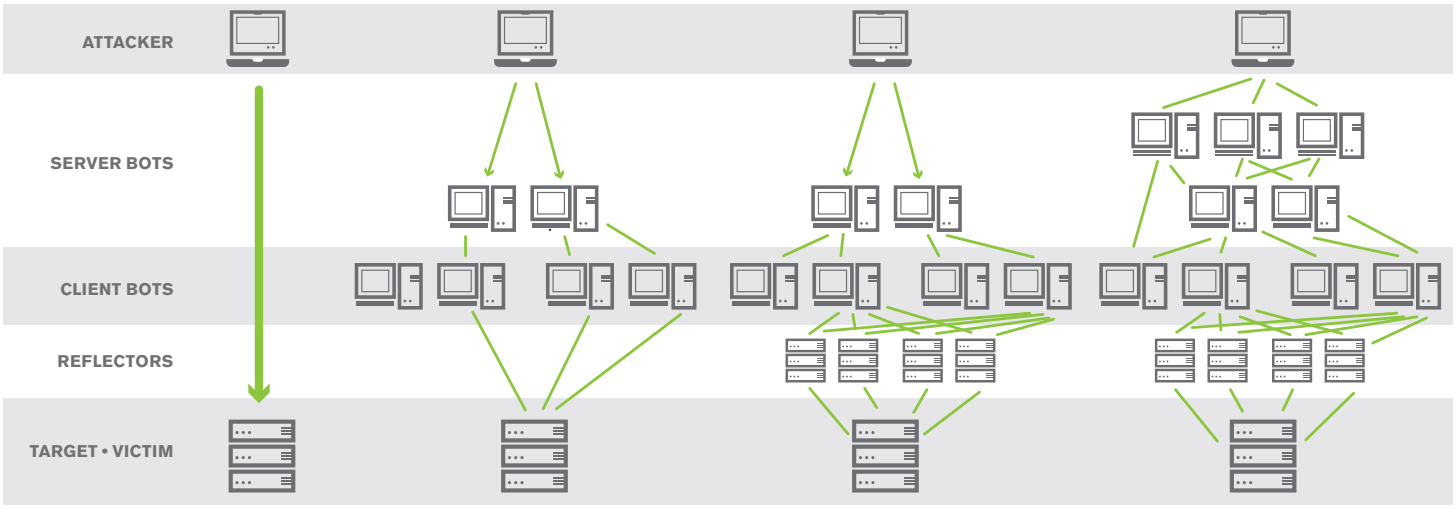
Malicious actors continue to leverage botnet technology to enhance the effectiveness of DDoS attacks. Over time, attack profiles have changed enabling the mastermind to distance himself or herself from the actual attack. The first phase of this evolution was the shift from standard DoS to DDoS attacks. Attackers soon realized that they could further separate themselves from the attack by introducing server bots for command and control purposes. By communicating with a few command and control server bots, attackers could manage hundreds and even thousands of client bots.

Recently, malicious actors complicated the attack by introducing new layers to the architecture. Distributed Reflector Denial-of-Service Attacks (DRDoS) take advantage of uncompromised devices that unwittingly participate in the attack. Typically seen through use of DNS servers that act as the reflector, the design of the attack sends several times more traffic to the victim than what was sent to it.

Researchers are attempting to keep ahead of the curve by trying to predict how botnets will evolve in the future. Research on what tomorrow's attacks will look like will help security providers today build solutions to mitigate them. As attackers start to use peer-to-peer technology to command and control a botnet, predictions on the next generation "Hybrid P2P" botnet do not seem far off[4].

Figure 2 shows how botnet architecture, specifically as used in DDoS attacks, has evolved over time.

FIGURE 2:EVOLUTION OF BOTNET CONFIGURATIONS AND DDOS ATTACKS



2 Dark Reading: www.darkreading.com/document.asp?doc_id=150292
3 Narus Software: www.narus.com/extras/yankee_ROI/ROI%20methodology.pdf
4 USENIX, hwww.usenix.orgevents/hotbots07/tech/full_papers/wang/wang_html

VERISIGN™

Using Technology Against Us

DDoS attackers are using all aspects of networking technology to perform their assaults. Some of the very tools that were designed to help support the growth of the Internet are now being leveraged to conduct attacks. From misuse of the TCP three-way "handshake" to incorporating the Domain Name System into attack scenarios, malicious actors are constantly evolving.

- **SYN Flood**
  During the early days of network protocol development, few envisioned attackers utilizing the three-way "handshake" of a TCP connection's establishment (the SYN, SYN-ACK, ACK sequence) to perform DDoS attacks. Today, SYN-flood attacks are one of the most common DDoS attack profiles on the Internet. Although more sophisticated variants of the attack are evolving[5], some organizations still fall victim to the basic approach that earlier attackers discovered (opening multiple connections with illegitimate SYN requests that deny legitimate users connection capability).

- **UDP Misuse**
  Misuse of UDP is another great example of repurposing legitimate Internet technologies for malicious purposes. User Datagram Protocol was designed to be a quick, easy method of transferring small amounts of data like DNS queries and answers. Unfortunately, "quick and easy" is ripe for attacker misuse. Forging the header information, specifically the source IP address, within UDP's packets has also become easy and attackers readily use the technique to mask their identity from legitimate users.

- **Encryption**
  Although encryption is a necessary security tool to protect the data of organizations and individuals, criminals have used it for decades to hide the secrets of their misdeeds. After security analysts and law enforcement agencies discovered that botmasters utilize unencrypted IRC channel directives to control botnets, attackers now encrypt the command and control signals of their botnets.

- **Fast-Flux**
  The evolution of the technology that attackers are taking advantage of continues today with the recent trend in fast-flux networks. Here, botnets manipulate DNS records to hide malicious Web sites behind a rapid-changing network of compromised hosts acting as proxies. The fast-flux trend reflects the need for attackers to try to mask the source of their attacks so that they are able to sustain the botnet for as long as possible.

Case Study: Analyzing an Attack

In 2006, a DRDoS attack illustrated the potential size of the security challenge facing network operators. More importantly, the attack highlighted some key shortcomings in traditional approaches to network security. Although the attack itself generated 5 Gbps against the victim network, "wargaming" and post-event analysis uncovered some telling tales of what attackers are capable of.

The perpetrator utilized a combination of compromised and uncompromised devices to help facilitate the attack. The attacker first infiltrated a DNS name server and published a zone with a 4,028-byte record. Then, using a botnet of unknown size, queried approximately 30,000 uncompromised DNS servers for the record. Since each bot had the spoofed source IP address of the victim, the uncompromised DNS servers returned the answer to the victim, thus creating a denial of service condition by overwhelming the victim network with traffic.

Because the attacker did not have to compromise the reflectors, he was able to save time and distance himself from the attack. Further, while the maximum bandwidth observed by the victim's ISP was approximately 5 Gbps, the attacker had to generate traffic at an estimated rate of only 79 Mbps (a 72:1 attack amplification). In other words, each bot sent only a 56-byte DNS query, but the response sent to the victim was 4,028 bytes. Multiplied by the thousands of bots querying thousands of DNS servers, the attacker is able to reflect enormous traffic loads.

5 Crossroads, The ACM Student Magazine: www.acm.org/crossroads/xrds10-1/tracingDOS.html

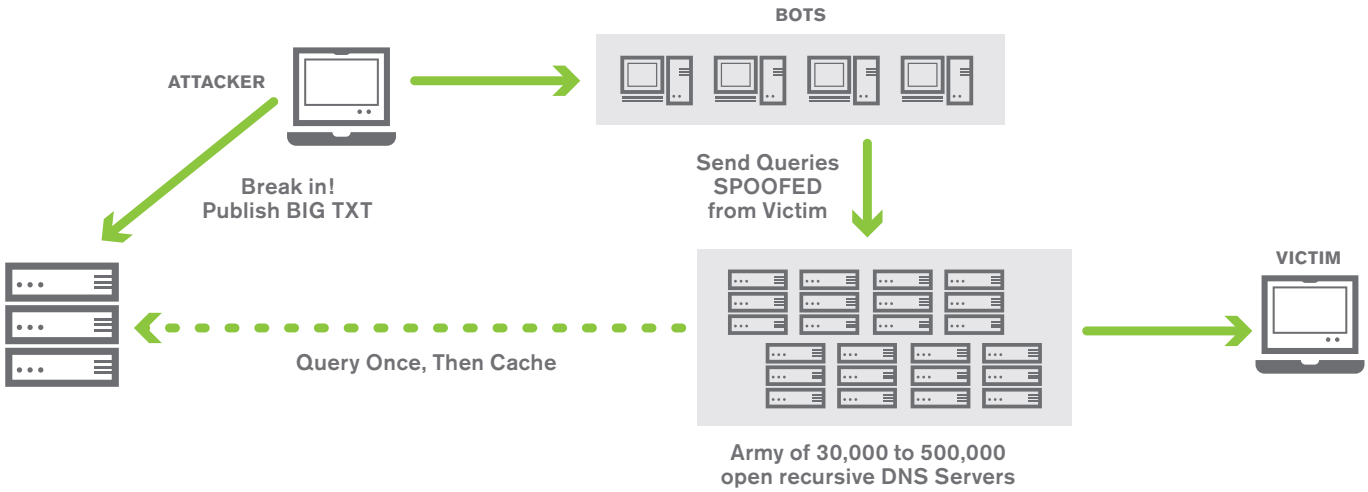
An attacker could have easily increased the total bandwidth of this attack by generating more originating traffic, using a larger DNS response, or utilizing more reflectors. While 5 Gbps was enough to bring down the victim in this case, other targets may have been more resilient. Total traffic could have easily been increased to more than 100 Gbps by utilizing approximately 600,000 DNS server reflectors. This may seem like an unreasonable number until one learns that the 30,000 reflectors used in the attack were pulled only from the 200.0.0.0 to 217.255.255.255 address space. Similar increases would be observed if other parameters of the attack were expanded.

It should be noted that while the DNS servers utilized in this attack were not compromised, they did have a flaw that allowed them to be used as reflectors: they were open, recursive DNS servers. That is, they did all of the recursion queries necessary to service a DNS client without requiring that client to be from the same network as they were. This poses a similar problem to that of open mail relays. As such, network operators should view open, recursive DNS servers as being just as important to secure.

Law Enforcement

Law enforcement agencies have had difficulties on numerous fronts in their attempts to bring cyber-criminals to justice. First, reporting on DDoS attacks is limited because of the reputation damage caused by a network outage. As result, there are limited cases to establish legal precedent. To add to the problem, anti-cyber crime legislation in the U.S. and abroad is rapidly trying to keep pace with the changing threat landscape. While cooperation between the law enforcement agencies of different countries is difficult, attackers can move through the virtual borders of the Internet with ease. Fortunately, the FBI has started to win cases against the more notorious botmaster cyber-criminals in the U.S.[6] which should help establish legal precedents for future cases.

FIGURE 3: ANATOMY OF A DRDOS ATTACK



6 Department of Justice: losangeles.fbi.gov/dojpressrel/pressrel08/la041608usa.htm

VERISIGN™

THE SOLUTIONS

Because of the rapid transformation of attack profiles and the demonstrated ability of malicious actors to launch devastating attacks, the nature of network security has changed. Network operators are reviewing the viability of traditional, edge security solutions focused on protecting organizations at and within the firewall. The fundamental question that security teams are addressing is how to deal with 10+Gbps attacks when the pipes to the organizational network are much smaller (an OC3 or OC12 connection or perhaps only a few T1s). Similarly, how does a security team keep up with the dynamic nature of attack profiles?

Organizations are correctly continuing to use a combination of security techniques to address the treat. Many security experts will contest that the best approach is to provide a layered approach in which the organization looks at security in-depth. Part of this approach asserts that some threats are better resolved in-the-cloud, or closer to the core of the Internet while others are still better handled at the organizational firewall. DDoS mitigation is a great example of a threat better mitigated in-the-cloud.

A comprehensive DDoS security solution should include the following components:

- Notification and alerting mechanism
- Sufficient bandwidth to absorb the attack
- Filtering technology that excludes only unwanted traffic
- A distributed model to create and maintain redundancy
- A logging/correlation system to collect detailed attack data

Network Security Devices: Firewalls and IDS/IPS Devices

While network security devices have matured and are extremely capable of thwarting certain attacks, they are insufficient when it comes to mitigating DDoS attacks. The primary reason is that on-premise security devices alone do not address the reserve bandwidth issue. Very few organizations have sufficient excess capacity to absorb a multiple Gigabit DDoS attack in addition to their normal traffic load. The best security devices in the world are rendered ineffective if the traffic never gets to them. Additionally, organizations that look to network security devices alone must continue to invest in the security teams that are able to adapt to the dynamic threat landscape. As a result, organizations are looking upstream of their network borders for solutions.

In-the-Cloud Network Security

The shift to ITC network security reflects the logical and necessary evolution for DDoS mitigation. Because of the size of attacks, an organization must identify and mitigate the attack before it has the chance to overwhelm its network. ITC security provides organizations this opportunity. As a result, some organizations have turned to their Internet Service Provider or a Managed Security Service Provider (MSSP) to afford DDoS protection.

Since ISPs provide bandwidth and connectivity to the Internet, they are generally the first place that organizations look to for a DDoS solution. Although some do offer a DDoS detection or mitigation services, many focus on maximizing reliability and not security. As Merike Kaeo writes in RFC 4778, “Some large ISPs do not concern themselves with attack streams that are less than 1Gbps in bandwidth.” For organizations suffering a 500 Mbps attack, the approach is not sufficient. Unfortunately, many organizations simply assume that their Internet Service Provider (ISP) affords DDoS protection without inquiring specifically about it.

Additionally, organizations should look carefully at how the ISP manages attacks. Simply “black hole routing” in many cases accomplishes the same result the attacker hoped to achieve (denying resources to legitimate users). While essentially disconnecting a victim may be acceptable for the ISP or for non-critical networks, most organizations cannot long survive without Internet connectivity, regardless of whether it is directly related to their core business.

Depending upon the needs of the organization, an MSSP may offer a better alternative. Although not providing packets to and from the organization as the ISP does, an MSSP does offer several advantages:

- **Security Expertise**
  MSSPs are fully staffed with security experts to that provide a service that is so integral to the core business that it is the core business.
- **ISP Agnostic**
  Unlike ISPs, MSSPs can provide one solution for enterprises that utilize multiple ISPs. Whereas an ISP can filter traffic traversing its network, it has no visibility into Internet traffic on redundant links from other providers. Enterprises with multiple ISPs can purchase multiple solutions, or look to an MSSP to provide the service.

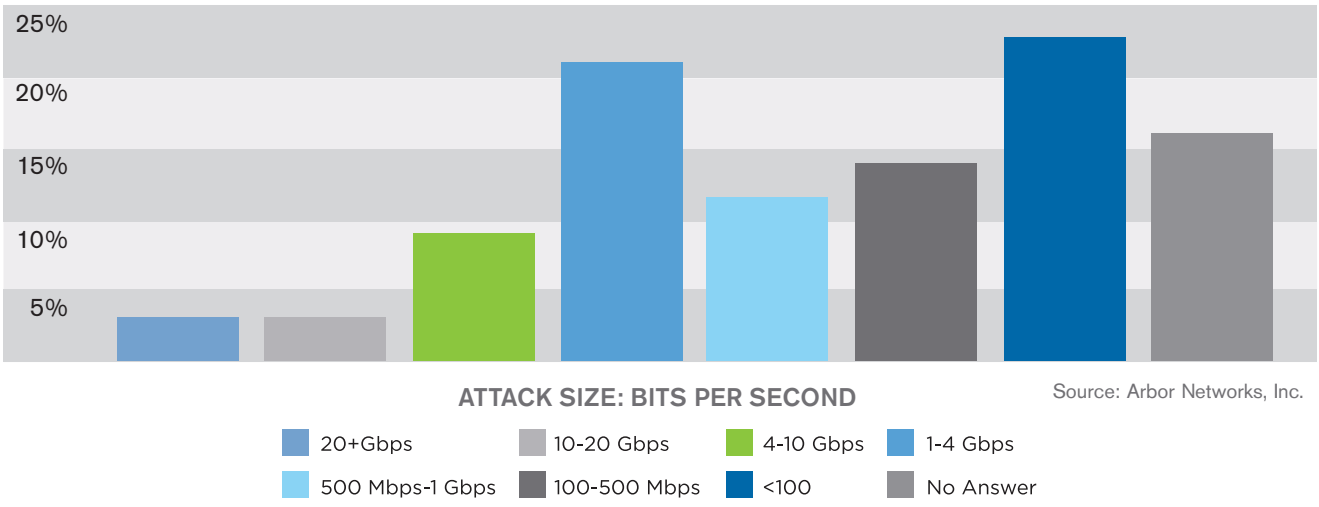
The critical question for any MSSP offering a DDoS mitigation solution is if they have the capacity and scale to mitigate the largest attack vectors. According to a survey conducted by Arbor Networks, attacks in excess of 20 Gbps are seen today while multi-Gbps attacks are becoming more prominent. The MSSP must be able to not only scale to meet these demands, but also the demand of attacks in the future.

CONCLUSION

Although DDoS attacks have largely escaped the front page of major news organizations over the past few years, replaced by elaborate identity theft, spam, and phishing schemes, the threat still remains. In fact, attack architectures and technology have evolved so rapidly that enterprises large and small should be concerned. Unfortunately, it appears the attacks will only increase in complexity and magnitude as computer network technology permits.

Whether attackers are driven by financial, political, religious, or technical motives, the tools that they have at their disposal have changed the dynamics of network security. Whereas firewall management used to be a sufficient strategy to manage attacks, botnets and reflectors have since reduced the effectiveness of blocking attacks at the network edge. The shift to in-the-cloud security for the detection and mitigation of DDoS attacks reflects the need to prevent attacks closer to the core of the Internet rather than waiting until it is too late.

FIGURE 4: ATTACK SIZE



Source: Arbor Networks, Inc.

VERISIGN™

As organizations look to make DDoS protection and mitigation a primary security initiative, they must choose the appropriate approach that suits their needs. Organizations vary in shapes in sizes, but one constant is that they should employ a layered approach to their security challenges. For organizations that have one ISP and great confidence in their ability to provide security solutions, a value-added DDoS service through the service provider may be the best alternative. Larger, multi-homed enterprises may prefer a network agnostic MSSP with the infrastructure, experience and technology to mitigate large-scale attacks. One thing is certain that many organizations can attest to: preparing for the attack while it is occurring is too late.

GLOSSARY

- **Bot/Zombie**
  A computer compromised with the intention of using it to commit cyber-crimes.
- **Botnet**
  A collection of compromised, networked computers used to commit cyber-crime.
- **Botmaster**
  A cyber-criminal that uses botnets to commit his crimes.
- **DoS Attack**
  Denial of Service Attack– a criminal attack where the goal is to prevent a computing resource from being used.
- **DDoS Attack**
  Distributed Denial of Service Attack–a DoS attack where the source attacker is not one computer or device, but several of them, typically located in disparate locations.
- **DRDoS Attack**
  Distributed Reflector Denial of Service Attack–a DDoS attack that is "amplified" by a reflector. A reflector is typically an uncompromised device that unwittingly participates in a DDoS attack. Due to the design of the attack, it sends several times more traffic to the victim than what was sent to it.

LEARN MORE

For more information, please email Learnmore@verisign.com.

ABOUT VERISIGN

Verisign is the trusted provider of Internet infrastructure services for the digital world. Billions of times each day, companies and consumers rely on our Internet infrastructure to communicate and conduct commerce with confidence.