E-Retailers: How to Protect Sales from DDoS Attacks

By Michael E. Donner, Senior Vice President, Chief Marketing Officer, Prolexic Technologies

Prolexic, the largest and most trusted provider of distributed denial of service (DDoS) protection services, advises e-retailers to put strong DDoS protection measures in place in advance of the peak shopping season. DDoS attacks are easier than ever to launch and can take an online business down for several days.

DDoS attacks and other cyber threats are a disaster for which preparedness can minimize damage. These malicious Internet-based attacks have become an unfortunate fact for e-retailers, especially during the holiday shopping season. December 2012 saw a 29 percent increase in the number of DDoS attacks compared to a year earlier.

It's not likely to get any better in Q4 2013, since other trends for the year show DDoS attacks that are bigger, stronger, longer – and more numerous – than in the past. As a result, e-retailers should expect a greater number of DDoS attacks during December 2013.

We've found that minutes count when DDoS attackers strike. Being prepared with a DDoS mitigation service vendor engaged and a plan in place can make the difference between having a brief site outage that lasts only a few seconds and having your business disappear from the Internet for days – or even a week.

Based on Prolexic's experience defending some of the world's leading e-Commerce sites against DDoS attacks, we have identified the DDoS mitigation playbook as a significant action e-retailers can take to minimize site downtime caused by a denial of service attack.

The importance of planning – and a DDoS mitigation playbook

Like any winning team, enterprise IT needs a playbook (an action plan) that reminds everyone what to do in the event of a denial of service attack. It's one thing to make a plan, and quite another to execute it. Smooth execution requires practice, practice, and more practice.

Practice will also help refine the plan and make it better. At Prolexic, we work with our customers to run simulated DDoS attack scenarios that help a customer's management team work out the best plan for managing their internal and external communications during a denial of service attack. After the simulation, management knows how long it will take to put their DDoS mitigation plan into action – and each step to take.

We've seen a simple relationship: the faster an effective DDoS mitigation service can be deployed, the shorter the outage and the smaller the revenue loss.

Fast, reliable, and controlled DDoS mitigation services delivered by an experienced DDoS mitigation service provider are the key to minimizing site downtime and financial loss for e-Commerce websites, both during the Q4 2013 holiday shopping season and year around.

e-Commerce businesses that take proactive measures to create a DDoS mitigation playbook with their mitigation vendor will have a competitive advantage as an online business that will always be open for business – on Cyber Monday as well as throughout the year – despite the escalating threats of DDoS denial of service attacks and other types of cyber crime.

You can learn more about Prolexic DDoS mitigation services, DDoS protection best practices and the value of safeguarding your holiday season e-retail revenues in Prolexic's whitepaper, *Safeguarding e-Commerce Revenues from DDoS Attacks in Q4.*

DDoS Attacks Can Take Your e-Commerce Sales Season from Ho, Ho, Ho to Ho-Hum

By Michael E. Donner, Senior Vice President, Chief Marketing Officer, Prolexic Technologies

What does the fourth quarter holiday e-retail season and the Grinch have in common? Distributed denial of service (DDoS) attackers would like nothing better than to sabotage your joyous holiday sales. Unlike the Grinch, though, malicious actors rarely have a change of heart.

If your business depends on Q4 revenue, now is the time to protect your income by arranging for DDoS mitigation service. Q4 is prime time for denial of service attacks against e-tailers, because attackers know that they can extract the greatest damage during your peak sales season.

Like the proverbial Grinch, malicious actors launch attacks that can result in lengthy service outages that disrupt sales and services on your website or any Internet-facing network infrastructure – with the aim to devastate your profits and your brand reputation.

Think it won't happen to you? There is often no rhyme or reason to who malicious actors choose to attack. In fact, it might even be a case of mistaken identity – but the damage to your business is all the same. Most online businesses think it won't happen to them – and that is a critical mistake. Your preparation for DDoS mitigation service can make the difference between a highly profitable or truly miserable online holiday sales.

In my experience gained from mitigating denial of service attacks launched against leading e-Commerce sites, it's a linear relationship: the longer a website is beset by extreme latency or crashed due to denial of service attacks, the more revenue is lost. A popular e-Commerce website told us that it lost US$1,000 per second (per second!) when it was brought down by DDoS attackers. Even if your business isn't that big, DDoS protection can offer a big payoff in keeping revenues flowing and customer satisfaction high.

This problem of denial of service attacks against e-Commerce businesses isn't going away. In fact, it's getting worse. The number of DDoS attacks increased 29 percent in December 2012 compared to December 2011. DDoS mitigation experts expect even more attacks in Q4 2013. If your business is like most e-tailers, the Q4 holiday shopping season is the most profitable quarter of the year. Taking action now can help keep it that way.

You see, the emergence of easy-to-use DDoS toolkits makes it simple for malicious actors to launch DDoS attacks – using computers or even mobile apps. Stopping the attacks is much more difficult and requires extensive experience with DDoS mitigation techniques. Firewall devices won't stop DDoS attackers, because malicious actors can subvert the devices to bring down your network anyway. And many of the DDoS toolkits have built-in randomization, so fighting these attacks means adjusting to a constantly moving target.

The faster that DDoS mitigation services can be deployed, the shorter the outage experienced and the less money is lost. Minutes count. Lining up your DDoS mitigation strategy and service provider in advance is a huge time saver (it could prevent days or a week of downtime). You can learn more about Prolexic DDoS mitigation services, DDoS protection best practices and the value of safeguarding your holiday season e-tail revenues in our free whitepaper, Safeguarding e-Commerce Revenues from DDoS Attacks in Q4.

No fun and games: DDoS attacks use game servers

By Michael E. Donner, Senior Vice President, Chief Marketing Officer, Prolexic Technologies

Each day 145 million people play online video games. Many of the servers they use are insecure and misconfigured, making online gaming networks easy-to-exploit by criminals who launch distributed denial of service (DDoS) attacks. What does this problem have to do with non-gamers? DDoS attackers use gaming servers to enhance their attacks, but their targets aren't limited to the gaming industry. Many attackers simply use the gaming servers to make their denial of service attacks more powerful. Regardless of your industry, a malicious actor could use gaming servers to attack your business.

The attacks keep coming and new techniques keep evolving. Using gaming servers to strengthen DDoS attacks is not new. Gamers and those who exploit multiplayer gaming infrastructures have been up to bad ends for a long time – since at least the 1990s.

Denial of service attacks involving gaming servers are launched by criminals who are outside of the gaming industry – and by gamers themselves. Criminals and players have different reasons for DDoSing. Criminals use gaming servers to boost their attacks against non-gaming businesses, especially against (but not limited to) the financial industry. Disgruntled gamers, on the other hand, may use a DDoS attack to knock a fellow gamer off a game network as a strategy to gain a temporary in-game advantage. Other gamers may use DDoS attacks to target other gaming systems to damage the playing experience of gamers on rival platforms.

One common type of denial of service attack that often involves the online gaming infrastructure is

called amplified distributed reflection denial of service attacks, or DrDoS attacks. This type of attack has been used for decades. Early DrDoS attacks that involved gaming servers took advantage of misconfigurations within the servers that hosted Counter-Strike, Quake and Half Life – and they still do.

One of the reasons gaming servers are so popular among criminals is that gaming-server aggregators provide a good source of server IP addresses to employ in DrDoS attacks. Although aggregators exist to provide a legitimate service for players to find a gaming server to play on, criminals use the server addresses maliciously. With the IP addresses, an attacker can identify which of them can be exploited and cause them to produce outsized responses directed the attacker's target, overwhelming the target with network traffic and slowing it or shutting it down.

Gamers tend to use different attack techniques. They often track down the IP address of an individual rival and use a DDoS method called packeting to slow or stop Internet service at the target. Although packeting attacks are relatively weak, gamers also have more sophisticated attacks at their disposal: For a fee, enterprising developers offer ready-to-use DDoS toolkits that are pre-configured to take advantage of insecure and misconfigured gaming servers.

Even non-gamers are at risk from DDoS attacks that abuse gaming servers. You can learn more about attacks and tools that exploit the multiplayer gaming infrastructure in Prolexic's white paper, *DrDoS and DDoS Attacks Involving the Multiplayer Video Gaming Community.*

DDoS Attackers New Tactics Amplify Attack Sizes and Hide Identities

By Michael E. Donner, Senior Vice President, Chief Marketing Officer, Prolexic Technologies

Distributed denial of service (DDoS) perpetrators changed tactics in Q3 2013 to boost denial of service attacks against websites and other Internet-facing technologies and to hide the identities of the cyber-attackers. By employing a type of DDoS attack called a reflection attack, which leverages the capabilities of vulnerable servers on the Internet, malicious actors launched high-bandwidth attacks with fewer of their own resources. These DDoS cyber-attacks are designed to cause outages at their intended targets, which are usually websites, and can prevent legitimate users from online shopping, banking, bill payment, information retrieval, use of social media, and more.

The reflection attack method grew in popularity among malicious actors by 265 percent year-over-year compared to Q3 2012 and by 70 percent in just the past quarter. Attackers are flocking to distributed reflection denial of service (DrDoS) attacks because this type of attack method provides them with significant benefits.

One benefit of DrDoS attacks for a malicious actor is the obscuring of the source of the attack (anonymity). By going through third-party servers, which are called victims because they are used for illegal purposes and without consent, the perpetrator's identity is hidden. Instead, it looks like the victim servers initiated the attack against the target.

The other benefit of DrDoS attacks for malicious actors is the ability to use the

bandwidth of the victim servers to make the attack more powerful. Because the amplification factor is so large – for one type of protocol attack the amplification factor is 17 – less outbound bot traffic is needed and the botnet of victim servers can be much smaller.

In DrDos attacks there are always two or more casualties: the malicious actor's intended target and the victim servers. The victims usually participate unknowingly. They aren't infected with malicious code as was more common in past botnets. Instead, they may have a server feature turned on that DrDoS attackers have learned to exploit opportunistically – typically a common network protocol such as Domain Name System (DNS) or Character Generator (CHARGEN).

In Q3 2013 there was a big jump in DDoS attacks involving the UDP protocol and a corresponding drop in DDoS attacks involving the SYN protocol. The increase in UDP attacks is part of the reflection attack trend, because UDP can be used to hide the perpetrator's identity.

Other DDoS trends identified in Q3 were related to the number of attacks. The total number of DDoS attacks in Q3 2013 remained high and represented the highest total ever for one quarter. Usually Q3 is a relatively quiet month, but the DDoS attack trend showed a consistently heightened level of DDoS activity around the world over the last six months.

Since Q3 2013, we have seen a 58 percent increase in total DDOS attacks, 101 percent increase in application layer (Layer 7) attacks, 48 percent increase in infrastructure (Layer 3 & 4) attacks and 12.3 percent increase in the average attack duration.

These attack statistics were extracted from Prolexic's Q3 2013 Global DDoS Attack Report, which also examines the problem of CHARGEN attacks being integrated into the DDoS threatscape – and explains how to remediate CHARGEN attacks.

Underground Market Fuels Reflected DDoS Attacks

By Michael E. Donner, Senior Vice President, Chief Marketing Officer, Prolexic Technologies

New tools and services have emerged in the underground market for distributed denial of service (DDoS) products. These website attack tools offer would-be attackers easy-to-use – and sometimes free – software to amplify attacks against websites and other Internet-facing technology using distributed reflection DDoS (DrDoS) attack techniques.

The sites that sell these malicious attack tools have slick user interfaces and convenient payment methods, opening up the market to malicious actors who can easily inflict damage on small-to-medium businesses for as little as US$5. As DrDoS attack suites leak into the public realm, underground tools developers make use of

publicly circulating code to create competing attack kits and services, fueling availability. With greater supply come lower prices. Unfortunately, it costs far less for a malicious actor to generate a denial of service attack than it does for a legitimate business to mitigate the attack.

Scanners, one type of newly available attack tool, can test broad IP address ranges, revealing vulnerable servers that can be used to amplify DDoS attacks. While IP address scanner tools had been found previously for sale on private underground forums, not only are scanners available publicly now, some are free.

Alternately, ready-to-use lists from the output of the IP address scanners are also available for sale, simplifying matters for attackers who don't want to use a scanner to make their own lists. The availability of lists could affect the underground market for scanner tools, because compilations of server IP addresses that are vulnerable to attack may reduce the demand for private scanners, allowing attackers to save time, effort and money by acquiring ready-made lists.

In addition to scanners and lists, the underground marketplace offers many DDoS-as-a-service tools that use reflection techniques, some for as little as $45 per month. One high-profile example of an attack suite is the RAGE booter, which has been hacked and leaked into the public realm numerous times, attracting mainstream media attention. The Prolexic Security Engineering and Response Team (PLXsert) has been tracking the emerging DDoS trend toward powerful DrDoS reflection attacks, which are being used more frequently.

Payment for DrDoS attack tools and services can be as simple as PayPal, which suggests a low-level of sophistication on the part of the vendors of these new tools, since more experienced DDoS tools developers would use lesser-known underground payment methods. Not surprisingly, DDoS tools and services vendors change names and locations often to avoid detection by authorities, following the pattern set by fraudulent e-Commerce sites.

Although lists of vulnerable servers have long been a commodity on the underground market, the surge in availability and demand for lists of servers specifically vulnerable to reflection attacks was new in the third quarter, as reported in the Q3 2013 Prolexic Global Attack Report from Prolexic. DrDoS scanner tools had not been widely available previously.

Who buys DrDoS reflection attack tools and services? Customers range from legitimate webmasters and system administrators who want to stress-test their own infrastructure to inexperienced script kiddies, sophisticated hackers looking to thwart and overtake rival services, and even state-sponsored malicious actors with ample resources.

The sites that sell these malicious attack tools have slick user interfaces and convenient payment methods, opening up the market to attackers who can easily

inflict damage on small-to-medium businesses for as little as US$5. The addition of amplification modules to these DDoS-for-hire sites highlights a growing problem: It costs far less to generate a DDoS attack than it does to mitigate one.

Server Configuration Can Protect Against Fast-Growing CHARGEN Attacks

By Michael E. Donner, Senior Vice President, Chief Marketing Officer, Prolexic Technologies

Hundreds of thousands of Internet servers sit at risk of being used in a fast-growing website attack technique to reflect and amplify distributed denial of service (DDoS) attacks. Server administrators can eliminate the threat with a simple change to server configuration. Without action, however, the server will be vulnerable due to a risk inherent in the default server configuration of many Windows servers.

Incidences of DDoS attacks using the character generator CHARGEN protocol rose sharply in the third quarter of 2013, according to data reported in the Q3 2013 Global Attack Report from the Prolexic Security Engineering and Response Team (PLXsert).

Attacks using the CHARGEN protocol, which was noted as vulnerable to these types of attacks as early as 1999, were the fastest-growing type of DDoS attack method in Q3 2013, with attackers using vulnerable servers around the world to reflect and amplify data onslaughts at target servers.

The CHARGEN protocol was initially created to enable testing and measurement of servers. Today, it is obsolete, and it should be disabled. Many legacy servers, especially those running the Microsoft Windows Server operating system, have it turned on by default.

Despite the age of the protocol , the re-emergence of CHARGEN attacks within the underground DDoS-as-a-Service marketplace suggests the abuse of this internet protocol retains value to malicious actors engaging in distributed reflected denial of service (DrDoS) attacks.

In Q3, Prolexic observed CHARGEN DrDoS attacks against its customers in the gambling and entertainment industries. Prolexic's experts mitigated these attacks before they affected the availability of the customers' servers. A subsequent forensic analysis found similar CHARGEN attack patterns in each case.

In the gambling industry attack, most of the reflected CHARGEN traffic originated from Asia, particularly China. The attack lasted 1.5 hours and reached a peak rate of 2 Gbps.

In the entertainment industry incident, although much of the traffic originated in China, CHARGEN servers from all continents except Antarctica were engaged by malicious actors in the attack, which lasted a half-hour and reached the same peak rate of 2 Gbps.

Because vulnerable servers used to reflect CHARGEN data may respond with as much as 17 times more data than they receive, attackers find the approach attractive. An attack launched with just one or two servers can overwhelm a standard 1GB virtual private server in a matter of seconds. In addition, the use of the UDP CHARGEN enables spoofing of IP addresses, which provides pseudo-anonymity for attackers.

Meanwhile, hundreds of thousands of CHARGEN servers are susceptible to use as attack vectors, a situation that could be readily addressed with a simple change by a network administrator to the server configuration. Of 1,000 attack events involving CHARGEN analyzed by PLXsert, more than 99 percent were found to have taken advantage of Windows servers – from Windows NT to Windows 2008 R2.

Step-by-step instructions on how to disable the CHARGEN protocol on a Windows server to prevent use in DDoS attacks is available in a case study on emerging DDoS reflection and amplification techniques in the Q3 2013 Global Attack Report from Prolexic.

DDoS Trends for Q4 2013

By Michael E. Donner, Senior Vice President, Chief Marketing Officer, Prolexic Technologies

Fall 2013 was a record-setting quarter for distributed denial of service (DDoS) cyber attacks. In one quarter we saw both the highest number of attacks and the largest-ever attack (179 Gbps) faced by Prolexic. In addition, we detected the use of mobile devices and mobile apps participating in DDoS attacks for the first time.

Infrastructure layer and application layer attacks were split similarly to the previous quarter, with infrastructure attacks accounting for 76 percent of all attacks and application attacks accounting for almost 24 percent of all attacks. A significant change, however, was an increase in the use of the CHARGEN protocol in infrastructure attacks. This was first noted in the summer of 2013, when CHARGEN was used in about 3 percent of all DDoS attacks. Through the fall quarter, it accounted for about 6 percent of all DDoS attacks, which represents a substantial increase.

Another recent development was the emergence of the use of the Network Time Protocol (NTP) in application attacks. NTP is used to synchronize the time on networked devices, but DDoS attackers have figured out how to use it in DDoS

reflection attacks. The misuse of the NTP protocol is increasing, although it is still very small, accounting for about one quarter of one percent of all DDoS attacks.

Examining attack vector metrics shows which attacks are currently favored by malicious actors. For infrastructure DDoS attacks, the UDP protocol was most commonly used in Q4 2013, with a combined 30 percent. SYN floods placed second with a total of 15 percent. In third and fourth place were ICMP protocol and DNS attacks with 10 percent each.

HTTP GET floods were the most commonly used application layer attack vector in Q4 2013, representing 20 percent of Layer 7 attacks.

Overall, the trend toward the use of reflected amplification-style (DrDoS) attacks over traditional DDoS attack methods continued with a persistent decline in ICMP floods (10 percent) and the rise in DNS, CHARGEN, and UDP/UDP fragment attacks.

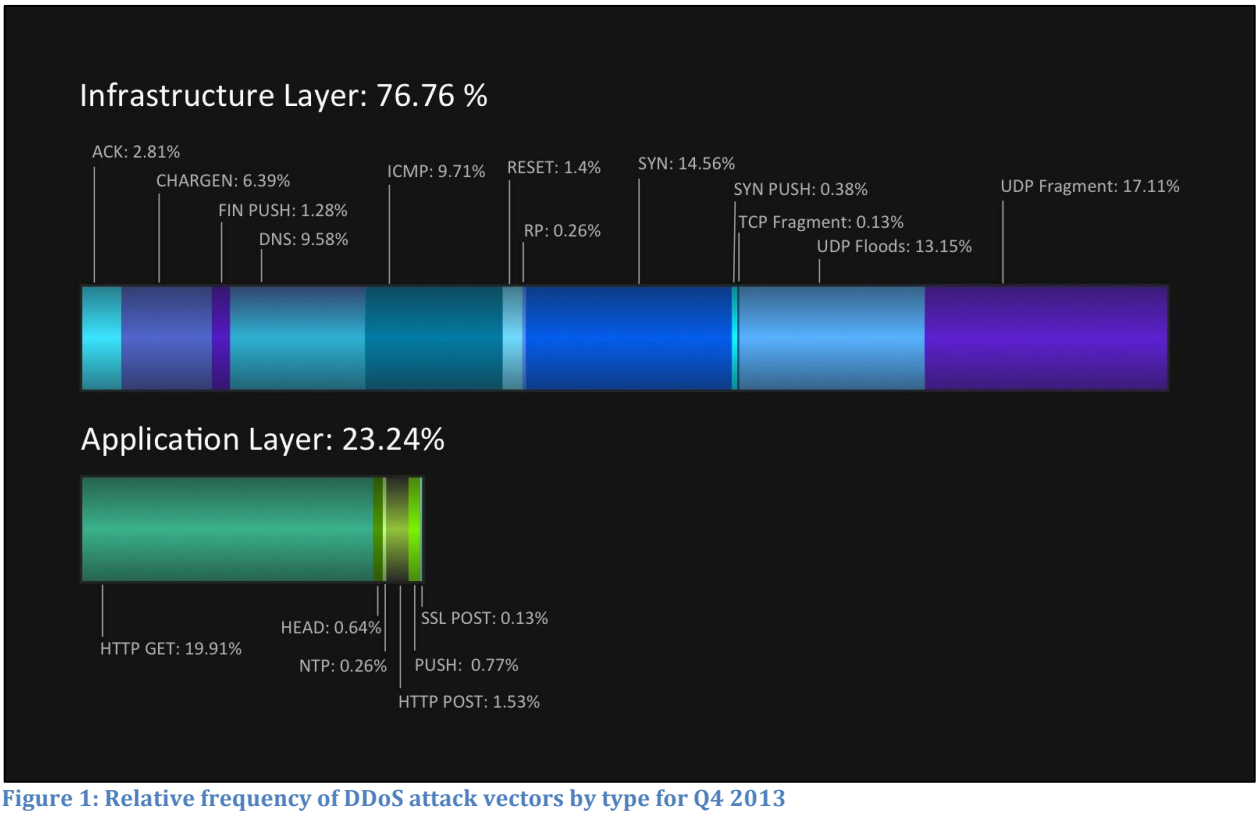

Figure 1: Relative frequency of DDoS attack vectors by type for Q4 2013

Top 10 source countries for DDoS attacks

The United States was the main source of DDoS attacks during Q4, accounting for 24 percent of all attacks. China, frequently ranked first, came in second by originating 19 percent of all DDoS attacks. Thailand not only rejoined the top 10 source countries after several quarters of not appearing on the list, but ranked third with

13 percent.

There was a noticeable presence of Asian countries in the top 10 source countries during this period. Growing economies and an expanding information technology infrastructure, plus large numbers of people online, are fueling DDoS attack campaigns coming out of Asia. It also appears there may be an increasing number of hacktivist groups becoming active in DDoS campaigns from Asia.

Man, Machine and DDoS Mitigation: The Case for Human Cyber Security Expertise

By Michael E. Donner, Senior Vice President, Chief Marketing Officer, Prolexic Technologies

DDoS mitigation appliances are network devices used by IT departments that are intended to prevent an outage caused by a DDoS attack. But today's DDoS attacks are often large and complex – too large and complex for automated DDoS mitigation. As a result, many businesses find real-time monitoring and analysis of network traffic by experienced DDoS mitigation engineers during an attack is necessary to ensure effective DDoS mitigation, especially when live attackers change attacks throughout an event.

A DDoS attack is an attempt to make a computer resource (i.e. website, e-mail, voice, or a network) unavailable to its intended users. By overwhelming it with data, requests or both, the target system either responds so slowly as to be unusable or crashes completely. Attackers typically reach these data volumes by harnessing a network of remotely controlled zombie or botnet (robot network) computers. Botnets are made up of computers that have fallen under the control of an attacker, generally through the use of a Trojan virus or other malware.

The financial damage from DDoS attacks is growing. Gartner predicts a 10 percent growth in the financial impact that cybercrime will have on online businesses through 2016, as DDoS attackers take advantage of new software vulnerabilities that are introduced via new cloud services and employee-owned devices used in the workplace. ("Gartner Reveals Top Predictions for IT Organizations and Users for 2012 and Beyond," December 1, 2011)

As a result, many organizations have made big investments in automated defensive tools such as firewalls, intrusion prevention systems (IPS), intrusion detection systems (IDS), and router appliances. Unfortunately, these automated tools can fail to block large or complex DDoS attacks.

Growing attack size and complexity

DDoS mitigation equipment cannot stop all DDoS attacks. Typically, a local DDoS

mitigation appliance can handle less than 10 gigabits per second (Gbps) of attack traffic, while a firewall solution offered by an ISP can usually handle less than 20 Gbps. A typical solution from a cloud-hosting provider can handle less than 40 Gbps. Yet, many of today's DDoS attacks are bigger than that.

In 2013, there were many attacks larger than 100 Gbps, and the largest peaked at 179 Gbps, as reported in the white paper, *Man, Machine and DDoS Mitigation,* from Prolexic.

DDoS attacks also continue to increase in complexity. DDoS attackers may target the network layer, described in the Open Systems Interconnection model (OSI model) as Layer 3, the transport layer (Layer 4) and the application layer (Layer 7) – and often all three in the same campaign. Even simple application layer attacks can critically overload web servers and databases, and they often resemble legitimate traffic, making them more difficult to detect and block.

Many DDoS attacks are live and dynamic, with a human attacker at the helm executing attacks and counterattacks in a real-time effort to outwit DDoS mitigation efforts. As such, the signatures, bandwidth, encryption and size of DDoS attacks can change constantly while the attack is ongoing.

Unfortunately, no automated system currently exists that can identify every DDoS attack and adjust the defense in real-time each time the attacker modifies a signature. Because DDoS attacks are launched by human attackers, human DDoS mitigators are needed to provide the intelligence, experience and creative decision-making abilities for effective DDoS mitigation.

A Multi-Vector Denial of Service Campaign Targeting a Financial Firm

By Michael E. Donner, Senior Vice President, Chief Marketing Officer, Prolexic Technologies

My firm recently mitigated a notable distributed denial of service (DDoS) attack campaign that shows how sophisticated hackers use multiple types of DDoS attacks in a single campaign in effort to cause an outage at the target website. In this case, the attackers used a dozen different DDoS attacks and every device at their disposal, including mobile phones belonging to other people. The attack, which targeted a global financial firm, and was ultimately unsuccessful, but it is an interesting attack to examine.

Multi-vector DDoS attack campaigns make DDoS mitigation more difficult. Multiple attack vectors make it less likely the attack can be blocked with automated devices. In addition, a DDoS mitigation team has to track more details and to fight the campaign on multiple fronts simultaneously.

In this case, the attacks continued for four days, during which time the DDoS mitigation team monitored and responded to the attack in real-time around the clock. Every time the attack changed, the DDoS mitigation engineers crafted a response to block the attack. In an emerging trend seen in other recent DDoS attacks, mobile phones played a pivotal role in boosting the strength of this attack.

The attack campaign spanned the globe, with Asian botnets playing a large role. The malicious actors used botnets in Indonesia, China, U.S. and Mexico. The source was hidden behind a *super proxy* – an IP address that acts as an intermediary for tens of thousands of other computer systems. To avoid blocking traffic from legitimate users of the super proxy, the DDoS mitigation team had to isolate the malicious network traffic from legitimate traffic.

The campaign comprised at least twelve different attacks, some of which attempted to take down the target by overwhelming the network layer (Layer 3) while others struck via the application layer (Layer 7). The attack signatures indicated the malicious actors recruited voluntary and involuntary participants in the botnet. In addition, unwitting domain name servers were victimized via spoofing to launch distributed reflection denial of service (DrDoS) attacks against the target.

Botnets are usually formed when servers and personal computers are infected with a Trojan virus or other malware that cause them to become unwitting participants in a DDoS botnet. Low Orbit Ion Cannon, also known as LOIC, is a DDoS tool that takes a different approach. LOIC lets supporters lend their computing resources by opting into a campaign. LOIC was used in this campaign.

To become part of the LOIC botnet, a participant simply downloads the tool and voluntarily connects to the attacker's command and control server. Once connected, the members of the Anonymous cooperative who lead an attack can control the participating devices remotely via Internet relay chat (IRC) or a URL shortening service, such as Bit.ly.

My firm has observed an increasing use of mobile devices in DDoS campaigns, including this one. This DDoS trend is most notable in markets such as Asia where the main means of access to the Internet is a mobile phone.

Attack signatures matching AnDOSid, a DDoS attack tool for Android devices, and mobile LOIC (Low Orbit Ion Cannon), a new Android app that was available from the official Google Play appstore in December 2013, were observed during the campaign. It seems likely that an increasing number of mobile devices will participate in future DDoS campaigns as the availability and adoption of these tools becomes widespread.

Actual attack signatures and details of recent DDoS trends such as the use of mobile devices and the role of Asian botnets in DDoS attacks were reported in the Q4 2013 Global Attack Report by Prolexic.