White Paper

Automating Defenses Against Increasingly Sophisticated DDoS Attacks

Prepared by

Patrick Donegan
Senior Analyst, Heavy Reading
www.heavyreading.com

on behalf of

www.radware.com

November 2014

Executive Summary

The distributed denial-of-service (DDoS) landscape has rapidly evolved in the last few years, and attackers have become much more sophisticated. The executive summary table below summarizes the findings in this paper regarding the changing landscape from volumetric to application-focused attacks, as well as the need for a fast and fine-grained automatic mitigation solution.

	LEGACY ENVIRONMENT	TODAY'S ENVIRONMENT
Threat Environment	Wireline-dominated Fixed IP addresses Individual attackers Sandbagged perimeter Connectivity-focused	Millions of new mobile endpoints Dynamic IP addresses Thousands of coordinated attackers Distributed perimeter App availability-focused
Detection	L2/3 rate-based	Application-based
Mitigation	Static signatures Manual analysis IP address blocking	Dynamic signatures Auto analysis
Time to Mitigate	Minutes or hours	Seconds or minutes
Mitigation Granularity	Coarse (may block good traffic)	Fine-grained
Mitigation Process	Manual	Automatic

DDoS Attacks Threaten Our Digital Lifestyle

There was a time when DDoS attacks were small-scale affairs. An antisocial individual with computing skills, looking to exact revenge on an organization that had crossed him, would swamp that organization's IT resources with high volumes of messages, to overwhelm those resources and take them out of service. These early attacks were rare, often amateurish, and often driven by personal grudges. Since these first attacks were launched in an era that preceded mass-market penetration of fixed broadband, e-commerce, mobile broadband and social networking, they tended to have a fairly limited impact.

In developed countries, the digital landscape has changed so dramatically in recent years that we now think in terms of the majority of people in these countries leading a "digital lifestyle." And that digital lifestyle has become increasingly vulnerable to DDoS attacks and both their short- and longer-term impacts. For example:

- **Businesses now store huge amounts of highly valuable intellectual property in digital format, as well as millions or tens of millions of customer account details, including bank-account details.** Any compromise in data security can cripple a business or dramatically reduce its competitiveness. Loss of customer data can trigger lawsuits from impacted customers.
- **Global business-to-consumer e-commerce sales are now heading toward $2 trillion per year.** This sales channel is entirely suspended for the duration of any outage inflicted by a DDoS attack. This ensures immediate loss of revenue and invites customers to shop online with a competitor instead.

- **The impact of DDoS attacks can be compounded by the power of social networking to instantly spread details of an attack and fan the flames of customer anger.** A successful DDoS attack can now cause huge damage to the reputation of any organization or organizations that are identified by as being responsible for failing to protect them from the impact. That can impact the attacked business itself, the service provider or providers that served as the conduit for the attack, or a managed security service provider that was meant to protect against such attacks, but failed to.
- **Large segments of Internet users have zero tolerance for any service interruption.** Both business users and regular consumers, whether fixed or mobile, are now heavily dependent on being able to access the Internet anytime, anywhere, and from any device. Some service providers can demonstrate a direct correlation between service outages and customer churn rates.
- **Botnets have greatly increased the power of DDoS attacks.** The increased use of botnets makes it possible to coordinate vastly more powerful DDoS attacks from hundreds or thousands of malware-infected machines that are remotely controlled by criminals.

Service providers are a key market players when it comes to protecting against DDoS attacks. They are the unwitting conduit of most attacks on third-party business, government or consumer targets. As managed security service providers (MSSPs), many have created a line of business in protecting their enterprise customers against DDoS attacks. And of course, service providers are themselves vulnerable to their own infrastructure being the direct target of a DDoS attack.

Heavy Reading's annual mobile network security survey shows that the number of DDoS attacks on mobile operators' own infrastructure is increasing: While 8 percent of mobile operator respondents stated in October 2012 that their infrastructure was seeing three or more attacks per month, 20 percent of respondents reported such high attack volumes in our October 2013 survey.

The fact that high-profile Tier 1 service providers feature so prominently among the victims in **Figure 1** reflects the asymmetric nature of the DDoS attack threat – namely that service providers and other organizations in developed countries tend to be a lot more vulnerable to these types of attacks than their counterparts in poorer countries, where the digital economy has yet to take hold.

Figure 1: DDoS Attack Incidents on Leading Service Providers & Their Customers

DATE	COUNTRY	VICTIM	DDOS ATTACK INCIDENT
May 2012	U.K.	Virgin Media	Service down for one hour, highly variable service in subsequent hours as well
August 2012	U.S.	AT&T	Attack on DNS servers caused Intermittent service disruption lasting several hours
March 2013	U.S.	Spamhaus	Largest-ever attack, peaking at 300 Gbit/s, causing worldwide disruption of the Internet
July 2014	Norway	Telenor	Attack impacted company's website
Sept. 2014	New Zealand	Spark (formerly TCNZ)	Customer suffered several hours of disruption to fixed and mobile broadband services

Source: Heavy Reading

DDoS Attacks Are Getting More Sophisticated

The last few years have seen a transformation in the profile of the attackers themselves, as well as the types of DDoS attacks that they are carrying out. Our increasingly digital lifestyle has created new motivations and opportunities for criminal organizations, terrorist groups and hostile nation-states to provide resourcing for a whole new breed of increasingly daring, sophisticated and lethal DDoS attacks. Such heavily resourced attackers are now generating the bulk of DDoS attacks, and they are no longer just looking to take infrastructure resources out of service, but also to enable theft or exfiltration of high-value information.

A May 2014 survey of IT managers by British Telecommunications (BT) shows that attackers are increasingly leveraging multiple attack vectors in orchestrated attacks. (See **sidebar**.) Due in large part to this, they are increasingly capable of bypassing or subverting security systems and delivering increasingly effective attacks.

Sidebar: BT Survey Research on Global DDoS Trends

In May 2014, BT published a survey of 640 IT decision makers worldwide. Among the key findings were:

- 59 percent agree that DDoS attacks are becoming more effective at subverting their organization's IT security measures.
- Attackers adopting multi-vector attack tactics have increased by 41 percent over the past year.

BT's survey was undertaken by Vanson Bourne, a technology research company focused on IT managers and consumers. They carried out 640 interviews with IT decision-makers in midsize and large organizations (1,000+ employees) across 11 countries and regions – the U.K., France, Germany, the U.S., Spain, Brazil, the Middle East, Hong Kong, Singapore, South Africa and Australia – and in a range of sectors, including finance, retail and public sector.

The Growth in Attackers & Intensifying Attack Impacts

The last few years have seen a marked increase in the number of attackers leveraging DDoS attacks and the severity of what these attacks can achieve. In addition to the increased use of botnets, new factors that are increasing the security threat include the following:

- **The simplification of attack-generation techniques and the professionalization of attack kits.** This is dramatically lowering the technical and financial barriers to entry for people wanting to perpetrate attacks.
- **A huge increase in the scale of volumetric attacks.** From a few hundred Mbit/s, attacks in the tens of Gbit/s are now regularly being reported.
- **The growth in 3G and 4G penetration has greatly expanded the footprint of IP end points that attackers are able to reach.** Smartphones and other mobile-connected devices pose two threats to the rest of the network. First, they can be used to attack the mobile carrier's own internal network infrastructure, such as the Evolved Packet Core (EPC). Second, mobile-connected devices are also vulnerable to infection by malware and becoming additional sources of coordinated large-scale botnet attacks themselves. This is already true of mobile-connected Windows devices and will be true of Android and other devices in the future.
- **The shift from volumetric-type to application-layer and encrypted attacks.** Whereas volumetric attacks, which directly send large volumes of messages at the end target, are fairly easy to detect with the right equipment, application-layer attacks target specific vulnerabilities in server resources, such as the Domain Numbering System (DNS), Session Initiation Protocol (SIP) and HyperText Transfer Protocol (HTTP) with low volumes of malicious traffic. When aimed at the right network resources, relatively low volumes of malicious software can randomly input administrator login credentials at the rates of hundreds of attempts per second, with the aim of bringing those

server resources down. These attacks render the target service unavailable, rather than merely seeking to block the ability to connect to it.

- **Targeting the unique vulnerabilities of a specific network.** Very importantly, application-layer attacks don't just exploit the unique vulnerabilities of the target application. Some of the most sophisticated ones rely on researching, identifying and targeting the unique vulnerabilities of a specific enterprise or service provider's network architecture.
- **The blending and coordination of different attack vectors to achieve a specific criminal objective.** For example, the use of a DDoS attack to bring down a network resource has the initial effect of preoccupying the security team of the attacked organization. While this diversionary attack absorbs the security team's attention, a second, undetected phase of the attack is then launched. This second phase might consist of, for example, exfiltrating the organization's propriety data from a completely different set of application servers somewhere else in the network.
- **Increased use of encryption by attackers in the design of their attacks.** This helps to avoid detection in two main ways. First, encrypted traffic will automatically escape detection by many conventional threat detection solutions. Second, encrypted sessions consume a lot more resources than unencrypted sessions, so by encrypting the attack, the attacker can achieve the same impact as an unencrypted attack, albeit with less volume.

This paper has already noted that the overall volume of DDoS attacks is increasing, and it has explained why. On average, around three quarters of DDoS attacks on service providers and enterprises are still of the volumetric type today. But around a quarter are now targeting the application layer, and that proportion appears to be growing inexorably.

For example, one network security professional at a large European network operator told Heavy Reading earlier this year that "we're seeing a lot more diversity in attack types now, for example increasing numbers of application-layer attacks."

Defenses for New Application-Layer Attacks

Significant changes in the telecom networking landscape tend to drive service providers to adjust either their organizational structures, the technologies and techniques that they use – or both – in order to adapt to them. And the ongoing changes in the characteristics of new cyber threats – including changes in DDoS attack characteristics – are doing just that.

The first imperative of adapting to these new application-layer threats is that service providers need to invest to ensure that their detection and mitigation capabilities are able to keep up with the changes in the threat landscape. But with most service providers still striving to break out of persistently flat revenue performance, the second, equally important imperative is that this cannot be done in a way that allows capex or opex to spike upward.

The Conventional Protection Model Approach

Take a look under the hood of most traditional service provider threat protection environments, and one would see a very small security operations team interacting at arm's length with the much larger network operations team. In a small service

provider, that security operations team may consist of as few as two or three people. In a larger service provider, they may number perhaps 20 or 30.

The network operations team was (and still is) charged with maintaining network availability in the face of network configuration errors, natural disasters and fiber cuts. The security team had responsibility for government liaison, such as Legal Intercept, as well as supporting the operations team when a cyber-attack posed any kind of threat to the availability of the network.

Initially, service providers experienced DDoS attacks as a rare occurrence. A market in third-party DDoS protection solutions grew out of building the ability to detect and mitigate malicious traffic based on volumetric threat signatures. That has typically meant blocking IP addresses. Some service providers also developed their own in-house solutions to that end. Some large service providers in developed markets started taking their own netflow statistics from routers in the network and generating their own manual attack signatures, either as their primary means of defending against DDoS attacks, or as a supplement to third-party solutions.

As the volume and variety of volumetric DDoS attacks has started to grow, most leading service providers have become quite adept at detecting and mitigating them. These days, many service providers routinely recognize and mitigate a high percentage of the attacks that they see. In some cases, these can run into several attacks a week, or even a day. In extreme cases, they can run into dozens per day.

Most service providers do routinely enjoy a high success rate in detecting and mitigating traditional, volumetric DDoS attacks with little or no impact on network availability. But it's also critical to consider that detecting and mitigating 99 percent of attacks doesn't amount to a successful security operation if the 99 percent that are blocked are potential low-impact attacks, while the 1 percent that gets through are high-impact attack types.

The Conventional Protection Model Is Under Pressure

As previously discussed, new patterns and types of security threats tend to be visited first on businesses and service providers in the world's most developed countries. For example, Heavy Reading research consistently shows that service providers in the U.S. tend to see advanced attacks long before they are seen in most other countries. And the experience of the last couple of years in the U.S. suggests that the conventional service provider DDoS defense model is coming under strain in a number of ways, including:

- **DDoS attacks are increasingly capable of escaping detection,** especially if they don't bear a conventional volumetric attack signature. When a website that normally sees 1 Gbit/s worth of traffic is suddenly inundated with 10 Gbit/s, that will inevitably capture the service provider's attention. When it sees 1.1 Gbit/s of traffic, that can easily escape notice.
- **Most threat protection solutions have particular difficulty dealing with application-layer attacks.** These are harder to detect because of the way they use relatively low volumes and because some are customized to exploit a vulnerability in the unique way that the specific target's network resources are configured. It's clear from Heavy Reading research that many service providers have malicious traffic in their network that they don't know about, and which is manifesting itself as reduced network performance, albeit without necessarily generating an outright outage.

- **The conventional approach tends to be too coarse-grained, which can reduce revenue from legitimate traffic.** In order to block malicious traffic emanating from a website or ISP, many service providers still block *all* traffic originating from that source, rather than filtering legitimate requests from malicious ones.
- **A model in which security analysts are increasingly relied upon to manually generate application-level attack signatures is not scalable.** Arriving at a resolution can also take a long time. Given the financial imperative to reduce opex, the case for investing in high-end automated detection and mitigation of application-layer attacks should usually be stronger than the case for hiring more skilled security personnel.
- **The limitations of simple IP address blocking are being further exposed by the growth in networking in the cloud and in 3G and 4G adoption.** Mobile operators have to dynamically share their limited IPv4 address pool across many millions or tens of millions of subscribers. These then have to be converted into public Internet addresses via Network Address Translation (NAT) gateways. In the cloud environment, a content delivery network (CDN) will often carry out its own internal NAT function. Hence, in the case of the increasing proportion of sessions in today's environment, the service provider receiving that incoming traffic can no longer count on having visibility of the originating IP address, as it could in the early ISP era of days gone by.

Protecting Against Application-Layer Attacks

In addition to protecting against volumetric attacks, it's clear that DDoS protection solutions need to defend against application-layer attacks. One approach is to leverage behavioral analytics and application logic to observe, store and correlate the unique traffic patterns in a given network.

This allows a baseline of traffic behaviors to be developed and applied that are uniquely associated with that specific network. When significant anomalies to the baseline are identified pointing to malicious traffic, an attack signature that is unique to that service provider can be automatically generated. This allows the service provider's cyber defenses to be customized to its unique requirements, rather than detection and mitigation responding solely to generic templates.

The baseline itself should take into account a lot of different network and traffic parameters for maximum accuracy. Among these can be volumetric patterns of different interfaces and at different network endpoints; the volumes and patterns of requests associated with the different types of application server; and variations according to time of day and type of subscriber. The baseline also needs to be constantly updated over time, so that at any given point in time it represents an accurate model of the behaviors that are associated with the service provider's own network.

It's reasonable to question whether a machine-generated signature will necessarily be as good as one generated by a human security expert. Viewing the detection and mitigation process as one end-to-end process, one can argue that, when it's done well, an automated signature generation process can be superior, in the sense that human analysis of a multi-element alert is liable to lead to different interpretations, and hence potentially different responses. By contrast, an automated response to a known signature should ensure the same, appropriate response each and every time.

This focus on the application layer also enables more fine-grained filtering per user or per flow. Instead of facing a choice of blocking traffic from all of another ISP's customers or allowing all of it into its network, the service provider can then filter out good traffic from bad.

Optimal Use of Skilled Personnel

Automation of attack signature generation can meet the network operator's opex and security goals by investing in purpose-built technology, rather than adding headcount exponentially. That should further enhance network security goals by freeing up those security specialists that are kept on the books to focus on readying the business for future generations of cyber threats, rather than engaging in day-to-day firefights against what they face today.

By bringing together the traditional objectives of the security organization with those of the network operations organization, service providers can look to align their organizations optimally to maintain high security and availability in the face of these growing challenges – and do so without raising opex.

Alignment With SDN & NFV Software Trends

Security is among the network applications that lends itself most favorably to new network trends toward software-defined networking (SDN) and network functions virtualization (NFV).

If ever there were a network domain characterized by a variety of specialized hardware platforms, currently needing expensive renewal every three years, it's the security domain. And if ever there were a security threat that presented itself as demanding little or no scaling of defenses for long periods of time, before suddenly requiring those defenses to scale up dramatically to mitigate that threat according to a virtualization model, it would be the DDoS attack. NFV promises the opportunity to markedly reduce the operator's dependency on proprietary security hardware.

Recognizing that the transition to the all-IP network ultimately exposes all network interfaces to security threats – not just those that directly face the public Internet – SDN can also have a role to play in the service provider's network security roadmap. For example, leveraging a centralized SDN control plane to provide a network-wide security service, rather than relying on in-line platforms protecting specific interfaces, is one application that can ensure that threats are detected and routed optimally throughout the network.

SDN-based security applications will also have the potential to make superior security decisions, by virtue of being able to draw on multiple telemetry feeds from classical or virtual software instances – be they routing, DPI, application servers or other – from throughout the network. And by enabling increased automation of the security operations center, SDN can be a key tool in containing opex while simultaneously increasing network and service availability.

In pursuit of the maximum flexibility, service providers will increasingly look for solutions to be available in any networking format, whether it be in classic hardware, as NFV instances or as SDN applications. That means being compliant with available standards such as OpenFlow and OpenStack today, and potentially other standards as they evolve.

Background to This Paper

About Radware

Radware (Nasdaq: RDWR) is a global leader of application delivery and application security solutions for virtual and cloud data centers. Its award-winning solutions portfolio delivers full resilience for business-critical applications, maximum IT efficiency and complete business agility. Radware's solutions empower more than 10,000 enterprise and carrier customers worldwide to adapt to market challenges quickly, maintain business continuity and achieve maximum productivity while keeping costs down. For more information, please visit www.radware.com.

Radware encourages you to join our community and follow us on LinkedIn, the Radware Blog, Twitter, YouTube and the Radware Connect app for iPhone.