Arbor Special Report

Worldwide Infrastructure Security Report

Volume IX

ARBOR NETWORKS

About Arbor Networks

Arbor Networks, Inc. helps secure the world's largest enterprise and service provider networks from DDoS attacks and advanced threats. Arbor is the world's leading provider of DDoS protection in the enterprise, carrier and mobile market segments, according to Infonetics Research. Arbor's advanced threat solutions deliver complete network visibility through a combination of packet capture and NetFlow technology, enabling the rapid detection and mitigation of malware and malicious insiders. Arbor also delivers market-leading analytics for dynamic incident response, historical analysis, visualization and forensics. Arbor strives to be a "force multiplier," making network and security teams the experts. Our goal is to provide a richer picture into networks and more security context—so customers can solve problems faster and reduce the risk to their business. To learn more about Arbor products and services, please visit our website at arbornetworks.com. Arbor's research, analysis and insight, together with data from the ATLAS global threat intelligence system, can be found at the ATLAS Threat Portal.

Table of Contents

List of Figures

Overview

This report provides the results of Arbor Networks' ninth annual *Worldwide Infrastructure Security* Survey. The survey covers a 12-month period from November 2012 through the end of October 2013. This report documents the collective experiences, observations and concerns of the operational security community in 2013.

The information within this report should be viewed as a general resource for all network operators, whether Tier-1 service providers or enterprises. It provides insights into the key trends in threats and the techniques to detect and mitigate them.

The majority of those completing the survey are directly involved in day-to-day operational security incident handling. This report is intended to provide a real-world view of the security threats that organizations face and the strategies they adopt to address them.

Survey Methodology

The 2013 Infrastructure Security Survey is comprised of 131 free-form and multiple-choice questions, a marked decrease from the 193 questions in the 2012 survey. As in previous iterations of the survey, Arbor has taken the feedback from last year's participants and made changes. This year the survey was designed to be quicker to complete, with extraneous or outdated questions and sections removed, and improved logic to prevent respondents from seeing irrelevant questions (based on their earlier answers). This year Arbor collected 220 responses to the Infrastructure Security Survey, a significant increase from 130 last year.

As in previous years, the survey addresses topics such as threats against infrastructure and customers, techniques employed to protect infrastructure, and mechanisms used to manage, detect and respond to security incidents.

The survey is organized into sections that focus on the threats that participants have experienced in 2013 and the threats they are concerned about for 2014. The survey asks detailed questions regarding any DDoS attacks experienced or monitored, as well as security issues on the corporate (internal, non-service delivering) network. Specific sections cover IPv6 strategy, DNS services, data center services, mobile services and overall security practices.

Arbor made further refinements to clarify questions in this year's survey, and added some questions to capture information on current topics of interest in the operational security community.

Key Findings

Threats and Attacks

- Multiple respondents report very large DDoS attacks above the 100Gbps threshold.
- DDoS attacks against customers remain the number one operational threat seen by respondents during the survey period, with DDoS attacks against infrastructure being the top concern for 2014.
- Over 60 percent of service provider respondents are seeing increased demand for DDoS detection and mitigation services from their customers, with just over one-third seeing the same demand as in previous years.
- Ideological hacktivism is still the top commonly perceived motivation behind the DDoS attacks monitored or experienced by survey respondents.
- Although customers of respondents are the most common targets of DDoS attacks, there has been an increase in attacks targeting network infrastructure.
- Cloud services stayed relatively unscathed by DDoS, with fewer than one-fifth of respondents seeing any attacks. For those who did report attacks, IaaS services were the most common target.
- Application-layer attacks were seen by almost all respondents during this survey period.
- Growth remained strong in the proportion of respondents seeing application-layer attacks targeting encrypted Web services (HTTPS)—up 17 percent over last year.
- HTTP GET floods remain the most common application-layer DDoS attack vector. HTTP POST floods have become much more common, along with Slowloris. Fewer respondents are seeing tools such as LOIC, HOIC and Apache Killer being used.
- Respondents identified NetFlow analyzers as the most effective and most commonly deployed threat detection mechanism. Firewall logs, the second most commonly used detection mechanism, rank fourth in terms of effectiveness behind SNMP tools and in-house developed scripts.
- When mitigating DDoS attacks, the percentage of respondents utilizing ACLs and intelligent DDoS mitigation systems (IDMS) is now almost equal, at just under two-thirds. This represents a slight drop in the proportion of respondents using ACLs for mitigation, and a slight rise in the proportion using IDMS.
- The proportion of respondents able to mitigate DDoS attacks in less than 20 minutes has increased again this year, to 60 percent. This is likely due to the increased use of scripts and tools for automatic mitigation.
- Advanced persistent threats (APT) are increasingly common, with nearly one-third of respondents reporting them on their networks during the survey period.
- The proportion of respondents allowing employees to use their own devices on internal networks (BYOD) has increased slightly, but more than half of respondents do not have ANY solution deployed to identify these devices.

Key Findings (continued)

IPv6

- This year, 60 percent of respondents indicated that they either have already deployed IPv6 or have plans to deploy within the next 12 months. This is surprising, given that the corresponding number for last year was around 80 percent. This decrease may be due to the broader mix of respondents to this year's survey.
- While getting visibility of the IPv6 traffic on their networks is critical for survey respondents, only about one-half of respondents have actually deployed a visibility solution for IPv6 traffic.
- When considering projected IPv6 traffic growth, the majority of respondents anticipate a 20 percent rise over the next 12 months, with less than 10 percent expecting more than 100 percent growth.
- This year the largest reported volume of IPv6 traffic monitored by a survey respondent was 20Gbps. This is a significant increase over last year, which topped out at 3Gbps.

Data Center

- Over 70 percent of respondents operating data centers reported DDoS attacks this year, up dramatically from under half last year.
- Over one-third of respondents who operate data centers experienced attacks that exceeded total available Internet connectivity, nearly double last year.
- Data center operators reported an increased frequency of DDoS attacks during this survey period. For the first time, nearly 10 percent of respondents saw over 100 attacks per month.
- Data center operators continue to rely on firewalls and are increasingly using IDS/IPS devices to deal with DDoS attacks. There are significant risks involved in relying on firewalls and IPS for DDoS protection. This year the proportion of respondents seeing an impact to their firewalls/IPS from DDoS attacks rose to 42 percent.

DNS

- Just over one-third of respondents have experienced customer-impacting DDoS attacks on their DNS infrastructure during the survey period—an increase from one-quarter last year.
- Approximately 26 percent of respondents indicated that there is no security group within their organizations with formal responsibility for DNS security, up from 19 percent last year. This increase is surprising given the number of high-profile DNS reflection/amplification attacks seen during the survey period.

Mobile

- Adoption of LTE mobile services continued its rapid expansion this year, reaching 63 percent with another 21 percent planning deployments in the next two years.
- Over 20 percent of respondents offering mobile services indicated that they have suffered a customer-visible outage due to a security incident, down slightly from about one-third last year.
- Respondents offering mobile services have massively improved their visibility into the traffic on their packet cores.
- Over one-quarter of respondents offering mobile services indicated that they have seen DDoS attacks impacting their mobile Internet (Gi) infrastructure—more than double the proportion seen last year.

Demographics of Survey Respondents

The number of respondents to the survey has been trending up over the past few years, with a mixture of Tier 1, Tier 2/3, hosting, mobile, enterprise and other types of network operators from around the world participating. More than 68 percent of respondents this year are service providers, giving us a global view into the traffic and threats targeting their networks, services and customers.

Looking first at the type of organizations responding to the survey, from a primary function perspective, respondents this year had a very similar make-up to that of last year's survey (Figure 1), with one notable exception: there was a significant increase in the proportion of enterprise respondents, up from 8 percent to 18 percent.

Survey Respondents by Organizational Type

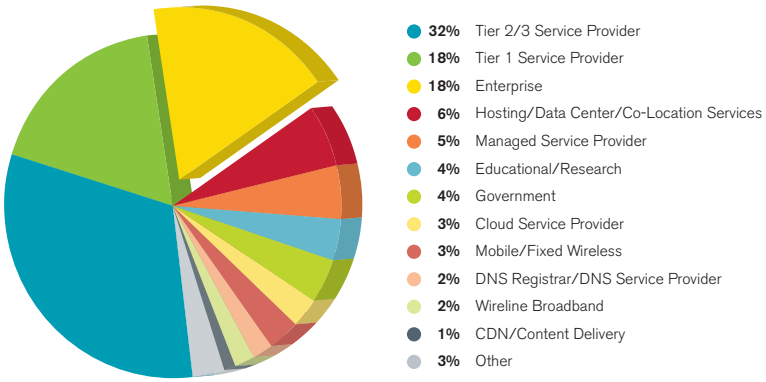

Figure 1 *Source: Arbor Networks, Inc.*

Network operators who participated in the survey are headquartered all around the world (Figure 2). This year, however, there was some shift in the geographic mix of respondents. The proportion of respondents from the Middle East, Asia Pacific and Latin America stayed similar to last year; however, a larger proportion are now based in Western, Central and Eastern Europe—up from 29 percent last year to 38 percent this year. The actual number of respondents from the U.S. and Canada was significantly up from last year; however, given the increase in overall respondent numbers, their proportion decreased.

Geographic Distribution of Organizational Headquarters

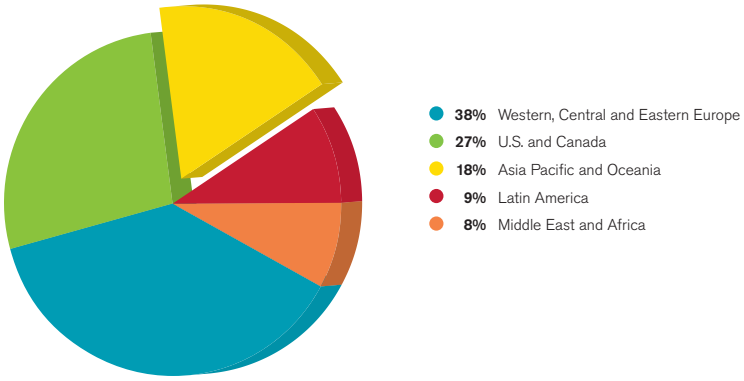

Figure 2 *Source: Arbor Networks, Inc.*

This year's survey also queried the services offered by participating network operators (Figure 3). Most operators offer multiple services, with the most common being business Internet access and hosting co-location services. The survey indicated a marked fall in the proportion of respondents offering DNS services, down to just over half of respondents from nearly three-quarters last year. Analysis of the data does not show any clear reason for this decrease based on changes in respondent mix, as a broad mix of operator types seem to NOT offer DNS services this year (although the increased number of enterprise respondents does contribute to some degree). The "Other" category includes wireless hotspot providers, on-line gaming companies and media organizations.

Services Offered

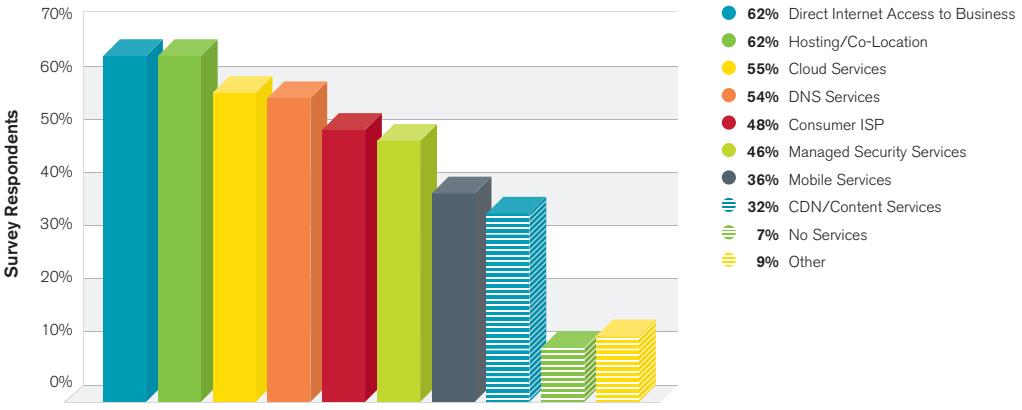

Figure 3 *Source: Arbor Networks, Inc.*

Figure 4 shows the proportion of respondents offering service coverage in each geographic region; this is consistent with the results from previous years.

Geographic Coverage of Respondent Network

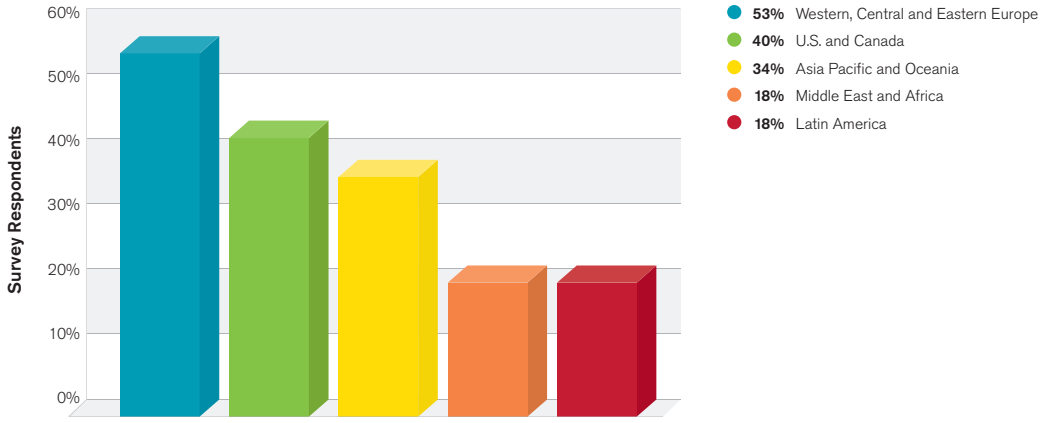

Figure 4 *Source: Arbor Networks, Inc.*

The Infrastructure Security Survey targets individuals involved in operational security, either from an engineering or management perspective. This year 58 percent of respondents are network, security or operations engineers who are involved directly in day-to-day operational security issues (Figure 5). This is a similar proportion to last year's survey.

Role of Respondent

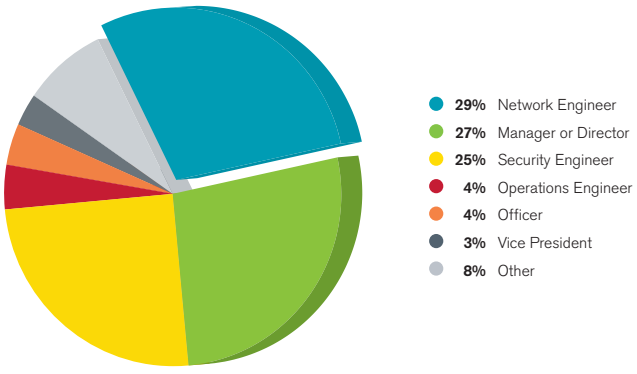

Figure 5 *Source: Arbor Networks, Inc.*

This year 81 percent of respondents indicated that their organization has dedicated operational security resources, a slight increase over last year (78 percent) but still not back up to the 85 percent from two years ago (Figure 6). As in previous years, the majority of respondents continue to work within small security operations teams, with over half of respondents having fewer than 10 dedicate resources. On a more positive note, a much higher proportion seem to have larger OPSEC teams this year—with 21 percent having teams of more than 30, up from 10 percent last year. Most of the respondents with large OPSEC teams are Tier 1 or Tier 2/3 service providers.

Over half of the respondents maintain an internal SOC, rather than outsourcing this function. The key challenges facing respondents when building and maintaining an effective operational security team (Figure 7) are identical to last year: "lack of head count and resources" and "difficulty in finding and retaining skilled personnel." Lack of both operating expenses and capital funding were cited as issues by roughly the same proportion of respondents as last year, indicating that tighter financial controls remain in place.

OPSEC Team Head Count

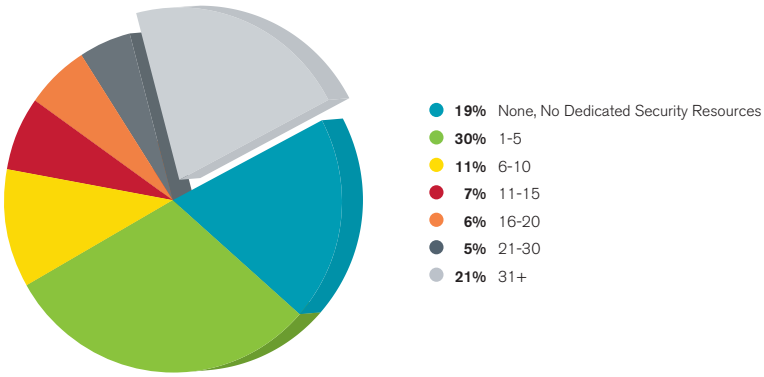

Figure 6 *Source: Arbor Networks, Inc.*

OPSEC Team Challenges

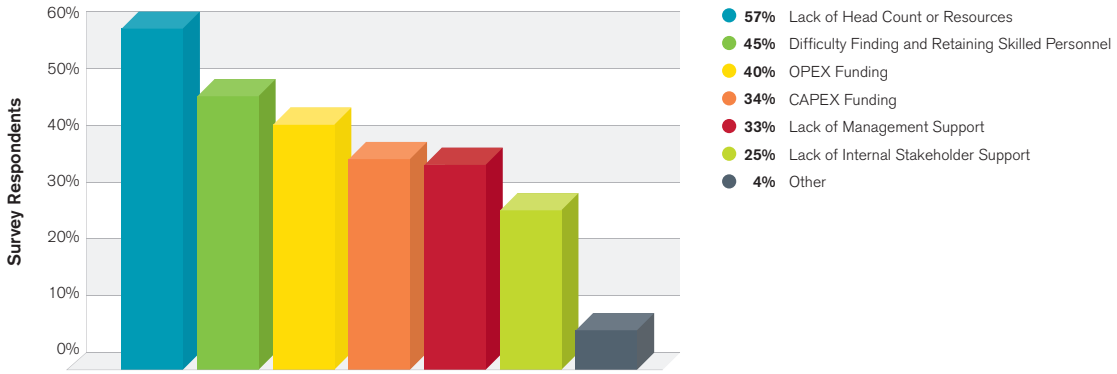

Figure 7 *Source: Arbor Networks, Inc.*

Arbor ATLAS® Introduction

As last year, Arbor is incorporating data in this report from its ATLAS® Active Threat Level Analysis System. ATLAS is unique, as it is the only globally scoped threat analysis system in existence. ATLAS leverages Arbor's service provider customer base, the Arbor Security Engineering & Response Team (ASERT) and relationships with other organizations in the security community to collate and correlate information pertaining to current security threats.

Arbor ATLAS® Introduction (continued)

This report makes use of ATLAS data for comparison and correlation with survey responses. ATLAS data relies upon (at time of writing) 290+ Peakflow® SP customers from around the world anonymously sharing statistics on a peak of over 80Tbps of traffic during 2013 (Figures 8 and 9). The data shared includes information on the traffic crossing the boundaries of the participating network operators. In addition, it includes anonymized information on the DDoS attacks they are seeing crossing their networks and targeting both their and their customers' infrastructure. The received data is collated and trended to deliver a detailed picture of the way in which DDoS attacks are evolving.

ATLAS Participants: Geographic Distribution

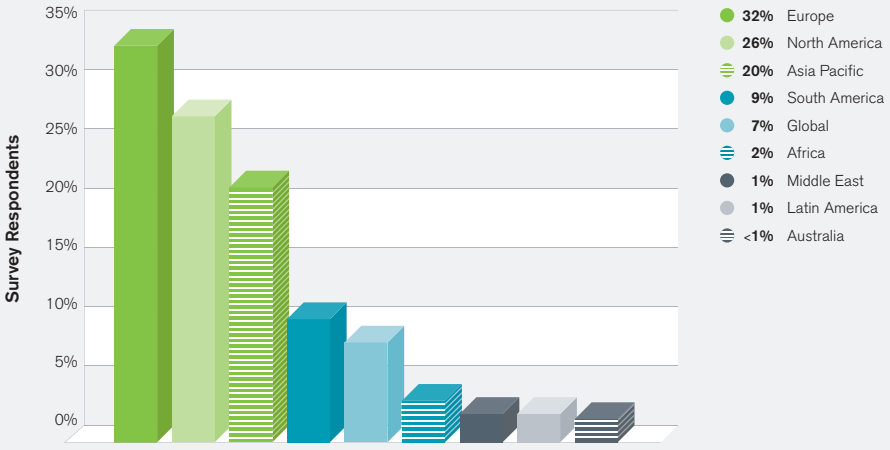

Figure 8 *Source: Arbor Networks, Inc.*

ATLAS Participants: Operator Type

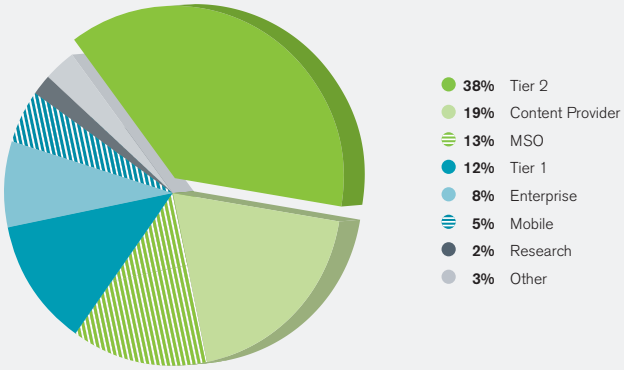

Figure 9 *Source: Arbor Networks, Inc.*

Most Significant Operational Threats

DDoS attacks against customers remain the number one operational threat seen during the survey period, with DDoS attacks against infrastructure being the top concern for 2014. DDoS remains a key issue; therefore, it should be no surprise that nearly two-thirds of service provider respondents are seeing increased demand for DDoS detection/mitigation services from their customers.

During this survey period, DDoS attacks against customers still remain the most commonly experienced security threat, with nearly two-thirds of respondents experiencing attacks. However, this does represent a drop in the percentage experiencing these attacks—from just over three-quarters last year (Figure 10). Percentages are down across the board for the top four experienced threats, but significantly up for others (e.g., bandwidth saturation, which is up from 21percent last year to 44 percent this year).

As mentioned above, nearly two-thirds of respondents experienced DDoS attacks toward their customers during the survey period, with just under half also reporting attacks against their infrastructure and/or services—down a little from last year. As in previous years, DDoS has taken up three of the top four spots, clearly illustrating the continued threat that DDoS poses to service providers and their customers alike. While DDoS ranked numbers 1, 3 and 4, the number two threat experienced by respondents in the last 12 months was outage due to failure or misconfiguration. This has been consistently experienced by around 60 percent of respondents for the three previous iterations of this survey; this year's survey is comparable at 55 percent, again indicating that this problem does not appear to be going away or improving substantially year over year.

One clear change in this year's report is in the proportion of respondents experiencing bandwidth congestion due to over-the-top (OTT) applications, unique events, flash crowds, etc. As mentioned above, the proportion experiencing this issue has more than doubled this year to 44 percent. This should be a key area of concern for all network operators.

Most Significant Operational Threats Experienced

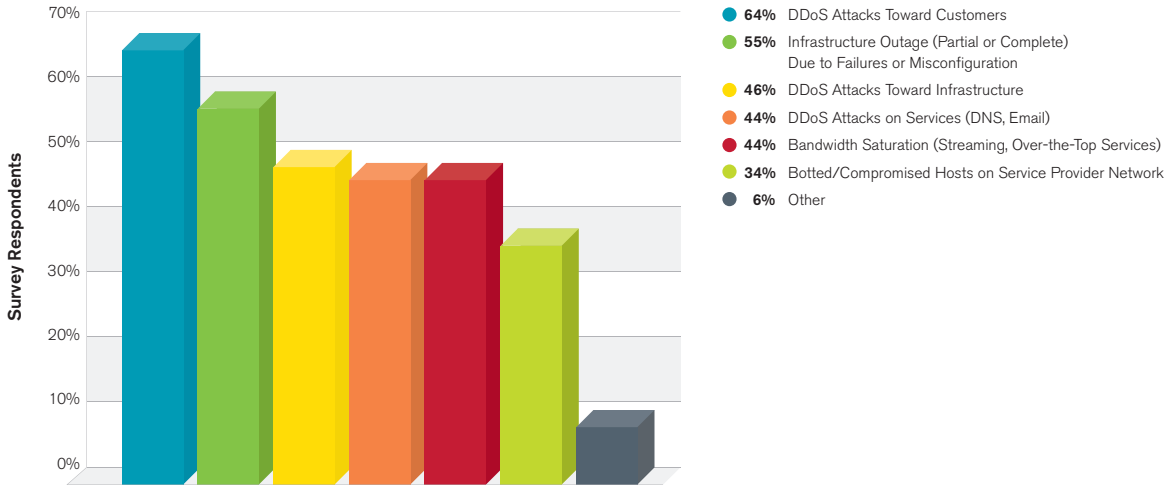

Figure 10 *Source: Arbor Networks, Inc.*

Looking at security concerns for the next 12 months, DDoS attacks continue to be top of mind; this is consistent with the data from the last two surveys. However, the number one and two concerns have swapped places from last year, with DDoS attacks against infrastructure now at number one and attacks targeting customers at number two (Figure 11). This shift may be due to the increase in amplification attacks targeting infrastructure. The number of reflection/amplification attacks seems to have increased significantly since the widely reported Spamhaus attack that occurred last year.

Interestingly, concerns about outages due to failure or misconfiguration continue to be ranked fourth, even though they have consistently been the second most commonly experienced threat over the past four years.

Bandwidth congestion is also a growing concern, possibly due to the increased experience of this issue during the survey period. Just under half of respondents are concerned about experiencing bandwidth congestion in the next 12 months, up from just under one-quarter last year. This may indicate that service providers are now running their networks with less spare capacity than they have done in the past, potentially making them more vulnerable to transient spikes in traffic.

Operational Security Concerns in the Next 12 Months

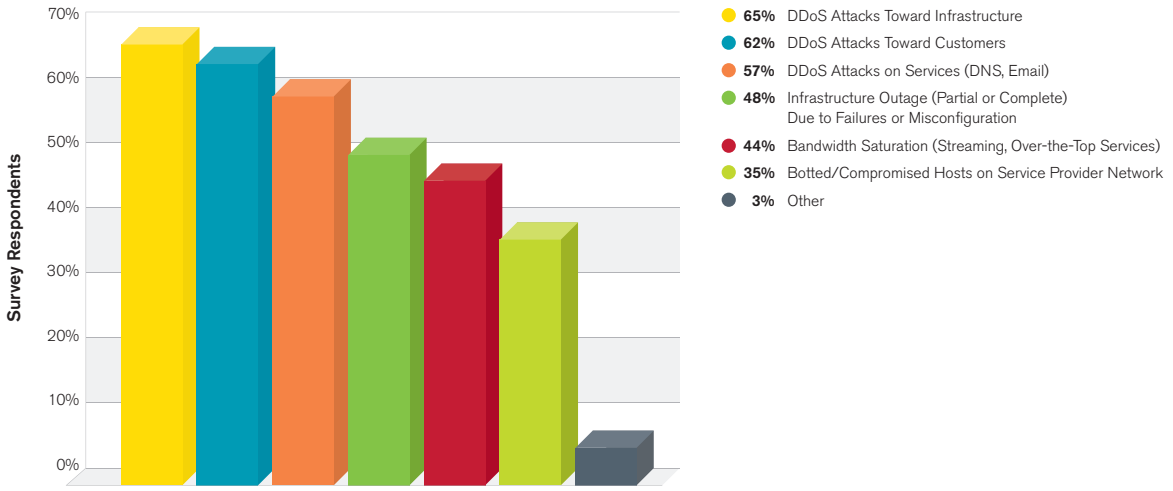

Figure 11 *Source: Arbor Networks, Inc.*

Given that DDoS is the top experienced threat and concern for survey respondents, it should come as no surprise that over 60 percent of service providers are seeing increased demand for DDoS detection and mitigation services from their customers, with just over one-third seeing the same demand as in previous years (Figure 12). Looking at the types of customer organizations expressing an interest in these services, the overwhelming majority of respondents mentioned financial service and government customers, which is to be expected given the number of well-publicized attacks against theses verticals in the recent past.

Demand for DDoS Detection and Mitigation Services

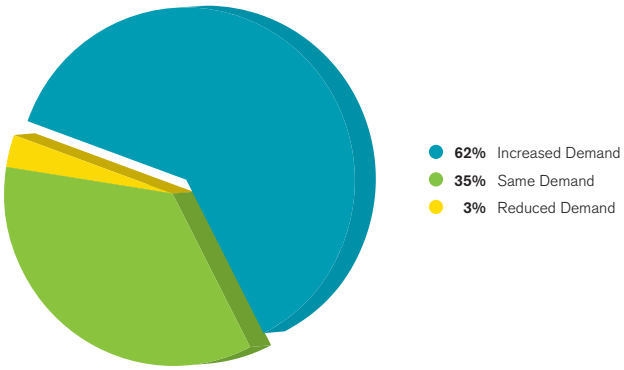

Figure 12 *Source: Arbor Networks, Inc.*

Respondents were queried regarding whether or not they saw, or expected to see, more state-sponsored attacks occurring. Just over half of respondents do NOT expect to see an increase here, which echoes last year's result.

Motivation, Scale, Targeting and Frequency of DDoS Attacks

During this survey period, the size of the largest DDoS attacks reported by respondents has increased dramatically. Historically, the largest reported attack was 100Gbps; this year multiple respondents reported attacks in excess of 100Gbps, with the largest attack reported at a whopping 309Gbps.

As in previous years, the survey queried respondents regarding the motivations they perceive to be behind the DDoS attacks they experienced or monitored (Figure 13). Ideological hacktivism continues to be the top commonly perceived motivation behind attacks. At number two this year is "Unknown," based on the responses of just over one-third of survey participants, up from one-quarter last year. This demonstrates that the range of motivations behind attacks—and the number that are occurring—are making it increasingly difficult for respondents to ascertain what is behind a given incident.

In joint third position this year, we have "Nihilism/Vandalism" and "Online Gaming-Related Attacks," with one-third of respondents seeing these as common or very common motivations. This year, to clarify our results, online gambling-related attacks were split out from online gaming. Only about one-fifth of respondents see gambling as a common or very common motivation.

Like last year, some of the motivations seen as common or very common by smaller (but growing) proportions of respondents are also interesting. This year between 16 percent and 18 percent saw DDoS attacks being used as a distraction from other criminal activity, such as financial market manipulation or a competitive takeout. This echoes anecdotal information Arbor has received indicating that DDoS attacks are increasingly being used as a "tool" by attackers as a part of broader campaigns.

Most Common Motivations Behind DDoS Attacks

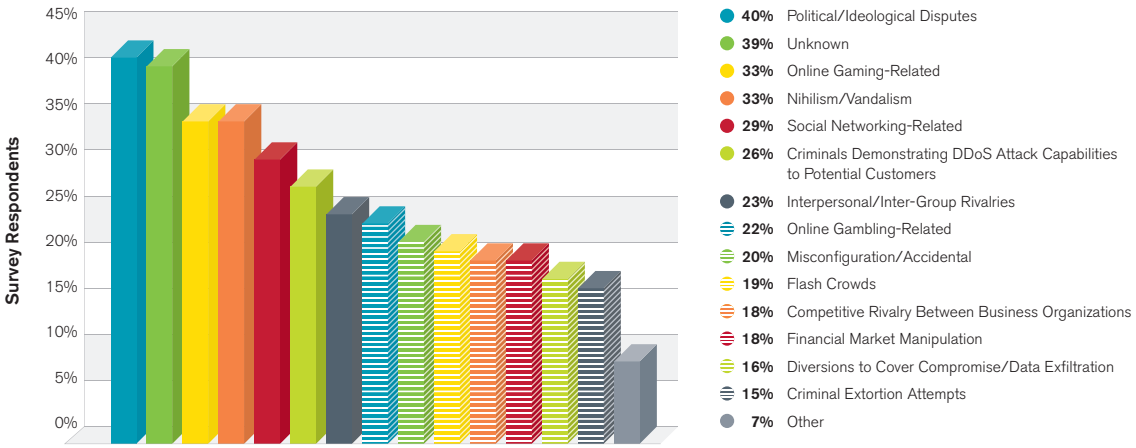

Figure 13 *Source: Arbor Networks, Inc.*

Given the well-publicized Spamhaus attack last year, and the attack sizes that the Arbor ATLAS system has been tracking, it was expected that the largest attack size reported would be significantly larger than the 60Gbps peak reported last year and the year before (Figure 14). Indeed, this year multiple respondents experienced attacks exceeding the previous largest reported attack of 100Gbps, which was recounted in our 2010 survey. This year's survey participants reported attacks ranging from 309Gbps at the top end, through 200Gbps, 191Gbps, 152Gbps, 130Gbps and 100Gbps. (Arbor is also aware that some respondents saw multiple events above the 100Gbps level, but only reported the largest of these.)

Size of Largest Reported DDoS Attack (Gbps)

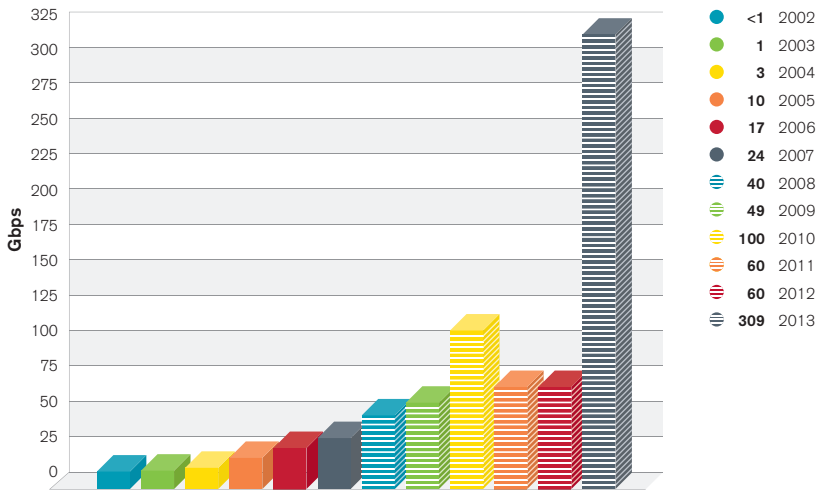

Figure 14 *Source: Arbor Networks, Inc.*

This sharp increase in attack traffic once again proves that attackers are continuing to shift methodology to make use of the latest attack capabilities available to them and to focus attacks on the most vulnerable areas of a network. As operators have changed their focus to building out defenses against application-layer and slow attacks, attackers have once again raised the bar in volumetric attacks.

The targets of these largest reported attacks of over 100Gbps have all been UDP/53 or TCP/80, or a combination of both of these in two cases. Attacks of this scale can cause issues for both service providers and end-user organizations alike. ATLAS data indicates that large attacks (above 20Gbps) have been much more common during 2013 (see ATLAS statistics section).

ATLAS-Monitored Attack Sizes

The Arbor ATLAS system gathers statistics from 290+ Peakflow SP customers all around the world. These statistics include anonymized details of the DDoS attacks monitored by participants. Arbor's ASERT team then collates and analyzes this rich dataset to determine key trends in DDoS attack activity. This data is then released quarterly to the broader operational security community.

The largest attacks reported by survey respondents have shown significant growth this year, and ATLAS data also shows this trend. The largest verified, monitored attack in 2013 was 245Gbps (Figure 15), as compared to 100Gbps in 2013. It should also be noted that the number of large attacks monitored by ATLAS (defined as being over 20Gbps) has increased massively in 2013—up more than eight times over 2012.

ATLAS Peak Monitored Attack Sizes Month-By-Month (January 2009 to Present)

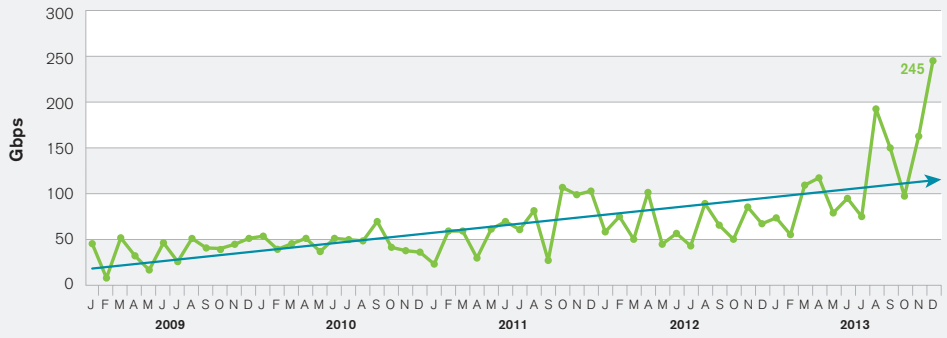

Figure 15 *Source: Arbor Networks, Inc.*

ATLAS-Monitored Attack Durations

As well as tracking attack sizes, ATLAS also allows Arbor to track the duration of attacks monitored by the 290+ network operators participating in the ATLAS initiative. In 2013, short and sharp attacks appeared to be more common, with 88 percent of attacks lasting less than one hour (Figure 16), up from 78 percent last year. This demonstrates the need for Internet operators to adopt new techniques and technologies to decrease the time it takes to detect and mitigate threats.

ATLAS-Monitored Attack Durations

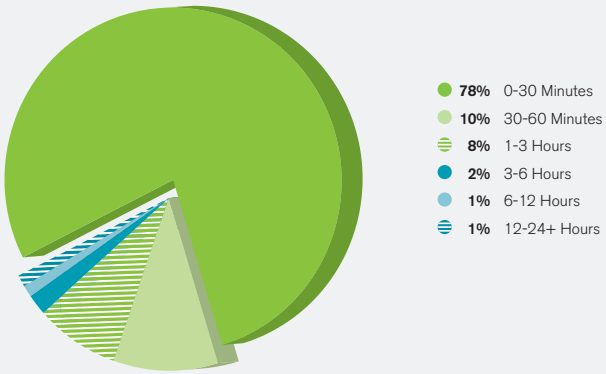

Figure 16 *Source: Arbor Networks, Inc.*

Survey participants reported a broad spread in the duration of their largest reported attack, with durations below six hours accounting for nearly half of the responses (Figure 17). Around 11 percent did, however, experience durations of over one week for their largest monitored attack, indicating how persistent attacks can be in some cases.

Duration of Largest DDoS Attack

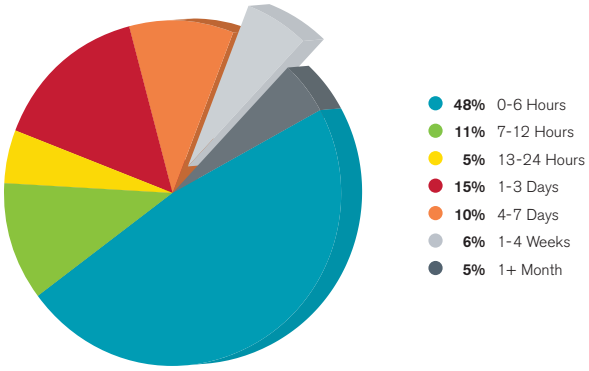

Figure 17 *Source: Arbor Networks, Inc.*

This year customers of survey respondents were by far the most common targets for the largest reported attacks (Figure 18). This is consistent with previous surveys. However, the proportion of respondents seeing their largest attacks target network infrastructure grew significantly—from 8 percent to nearly 20 percent.

Target of Largest DDoS Attack

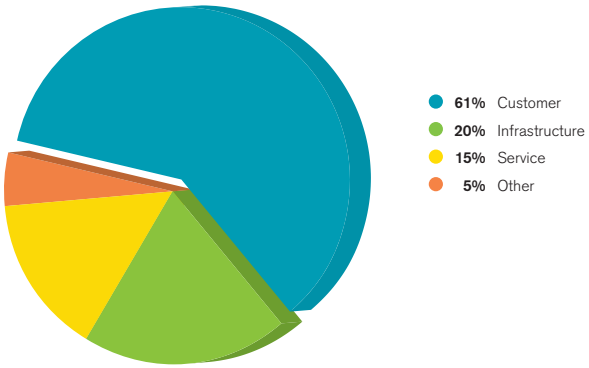

Figure 18 *Source: Arbor Networks, Inc.*

Customers of the survey's respondents are the most common targets of attacks overall (Figure 19). Service infrastructure (DNS servers, mail servers, Web portals, etc.) is the second most common target. These results are very similar to last year, but it is worth highlighting an increase in the percentage of attacks targeting network infrastructure—up from 11 percent to 17 percent. Clearly, attackers are predominantly targeting end users (as shown above), but in some cases where DDoS protection is in place, attackers are moving on to target service and network infrastructure to try and achieve their goals. For example, the Spamhaus attack initially targeted a customer and then migrated to service-provider infrastructure over the course of the event.

Monitored Attack Targets

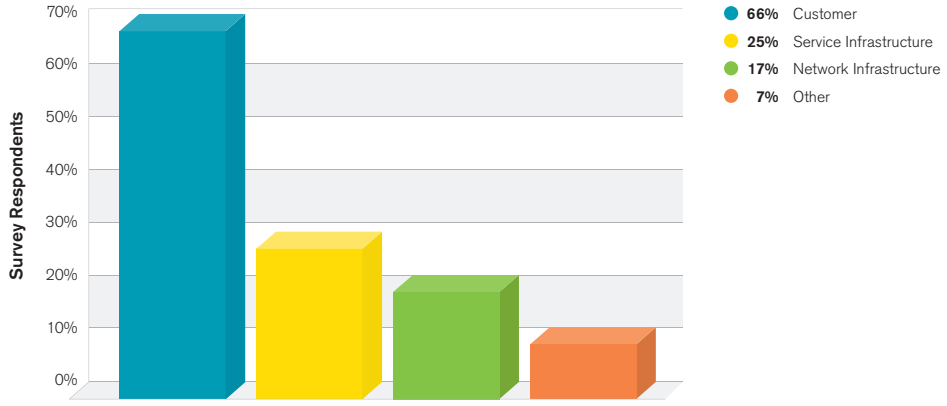

Figure 19 *Source: Arbor Networks, Inc.*

Looking at the types of customers being targeted by DDoS attacks (Figure 20), some changes have occurred from last year's results. Just under half of respondents reported attacks targeting end users or subscribers, with e-commerce and financial services customers being slightly behind in joint second place. This represents significant growth in the proportion of respondents seeing DDoS attacks targeting end users, up from just under one-third last year to nearly one-half this year.

Last year we highlighted our surprise that attacks targeting government and financial services organizations were not more widely reported (15 percent and 19 percent respectively) given their media coverage in 2012. The proportion reporting these attacks this year has predictably increased substantially (34 percent and 43 percent respectively). In fact, percentages of respondents seeing attacks against all specified verticals have increased over last year.

Targeted Customer Types

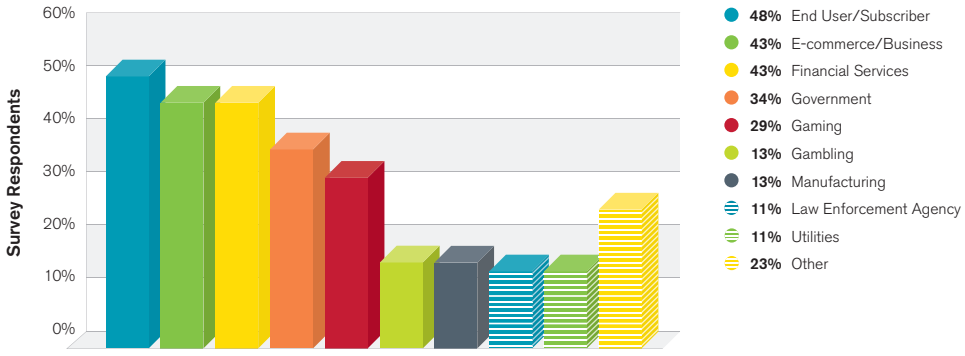

Figure 20 *Source: Arbor Networks, Inc.*

Cloud has remained a hot topic through this survey period, with anecdotal reports of a growing number of organizations embracing cloud-based data and application services. As these services are typically reached via the Internet, a DDoS attack could prevent customers from accessing these services. Last year only 14 percent of respondents had seen attacks targeting any form of cloud service; this year that has increased to 19 percent (Figure 21). Interestingly, however, nearly one-third of respondents answered "Do Not Know." This could indicate poor visibility of these services. For those who did report attacks, IaaS services seem to be the most common target.

Attacks Against Cloud Services

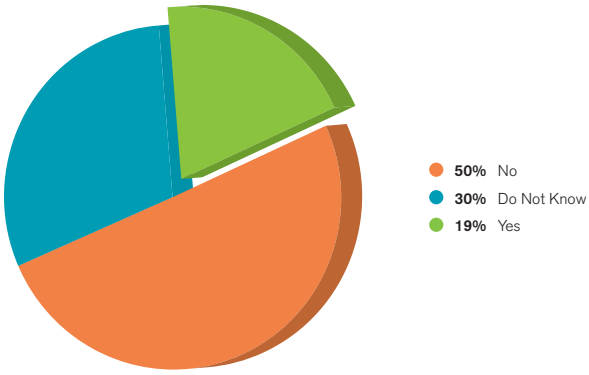

Figure 21 *Source: Arbor Networks, Inc.*

This year the survey included a new question to establish the proportion of respondents who have CGN (Carrier Grade NAT) deployed within their infrastructure. Attackers can target the state tables within CGN infrastructure, and almost half of respondents have some CGN deployed. However, only around 10 percent of respondents have seen attacks causing any impact to CGN—with a further 18 percent seeing attacks but with no discernible effect (Figure 22).

Impact of Attacks Against NAT Infrastructure

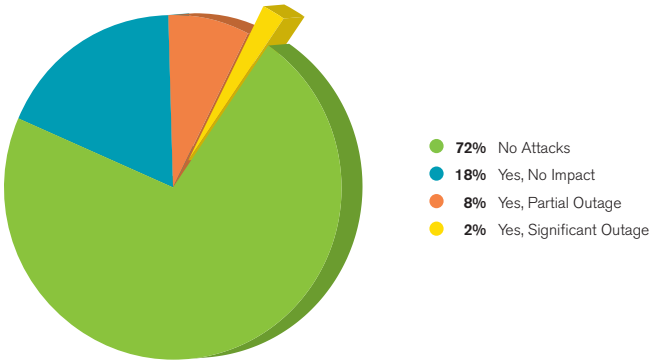

Figure 22 *Source: Arbor Networks, Inc.*

DDoS attack vectors vary significantly between attacks. Attack vectors tend to fall into one of three broad categories:

1. **Volumetric Attacks:** These attacks attempt to consume the bandwidth either within the target network or service, or between the target network or service and the rest of the Internet. These attacks are simply about causing congestion.

2. **TCP State-Exhaustion Attacks:** These attacks attempt to consume the connection state tables that are present in many infrastructure components, such as load balancers, firewalls and the application servers themselves. They can take down even high-capacity devices capable of maintaining state on millions of connections.

3. **Application-Layer Attacks:** These target some aspect of an application or service at Layer 7. They are the most sophisticated, stealthy attacks because they can be very effective with as few as one attacking machine generating a low traffic rate. This makes these attacks very difficult to proactively detect with traditional flow-based monitoring solutions. To effectively detect and mitigate this type of attack in real time, it is necessary to deploy an in-line or other packet-based component to your DDoS defense.

Within these categories, the actual attack vectors being used are evolving continuously, with attackers producing new and more complex attack tools all the time.

This year's survey asked respondents how the attacks they monitored or experienced during the survey period were split between the categories above (Figure 23). Based on the responses, volumetric DDoS attacks are still the most common form of attack, and ATLAS data seems to indicate that these "simpler" attacks have seen renewed interest from the attacker community in 2013. That said, the more sophisticated application-layer attacks have become increasingly common in recent years. Respondents reported that, on average, just under one-quarter of attacks targeted the application layer, with roughly 86 percent providing a non-zero result regarding application-layer attacks.

Attack Category Break-Out

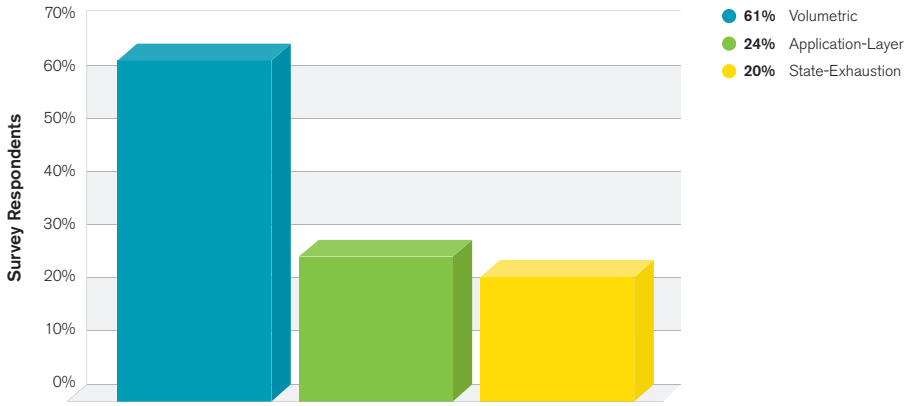

Figure 23 *Source: Arbor Networks, Inc.*

In terms of the services being targeted by application-layer attacks (Figure 24), over three-quarters of respondents reported attacks against Web services (HTTP). The break-out of services being targeted by volumetric attacks can be seen in the ATLAS inset. Looking at other services such as DNS and SMTP, the results were similar to last year—with a small increase (from 70 percent to 77 percent) for DNS and a decrease (from 31 percent to 25 percent) for SMTP. What is clear, though, is the continued strong growth in the proportion of respondents seeing application-layer attacks targeting encrypted Web services (HTTPS)—up to 54 percent this year, from 37 percent last year and 24 percent in 2011. This continued growth should be a key concern for e-commerce and financial services organizations that make substantial use of HTTPS in their Web properties.

Targets of Application-Layer Attacks

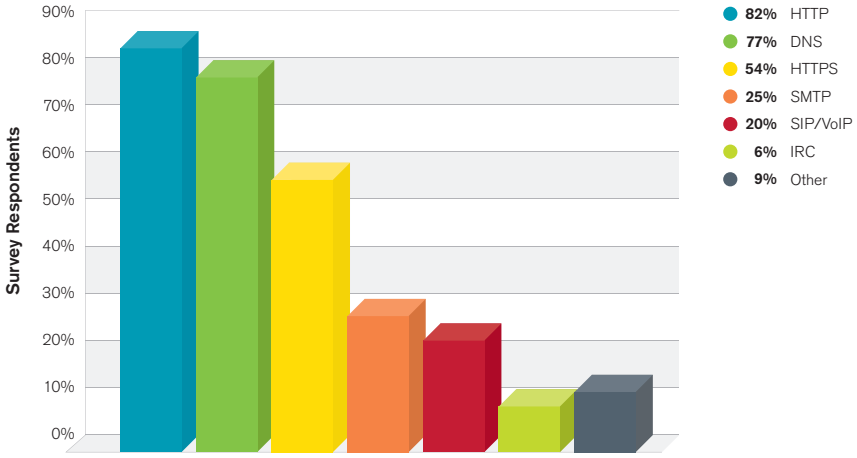

Figure 24 *Source: Arbor Networks, Inc.*

ATLAS-Monitored Services Targeted by Volumetric Attacks

Looking at the ports and protocols being targeted by the volumetric attacks tracked by ATLAS, as expected TCP/80 (HTTP) receives the most attacks—with just under one-third of monitored events, down from just over one-third last year (Figure 25). The second most common target is UDP/53 (DNS) at 10 percent, roughly the same percentage as last year.

Where there has been very significant growth, though, is in the proportion of attacks utilizing non-initial-fragments. In 2012, roughly 10 percent of attacks utilized non-initial-fragments; in 2013, this has grown to 25 percent.

This increase reflects the trend, monitored through 2013, of attackers utilizing reflection/amplification techniques (such as DNS, Chargen, NTP, SNMP, etc.) to magnify the volume of traffic that can be generated during an attack (e.g., the Spamhaus event, and many others).

ATLAS-Monitored Volumetric Service Targets

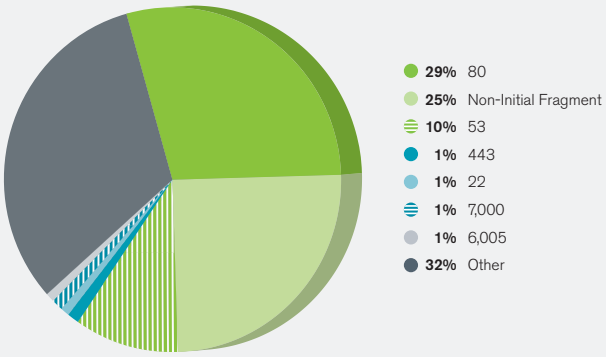

Figure 25 *Source: Arbor Networks, Inc.*

Looking in more detail at the attacks targeting encrypted services (Figure 26), we see three clear attack mechanisms, with roughly an equal split among respondents. Interestingly, one-third of respondents reported attacks targeting an encrypted service at the application layer, rather than the protocol or transport layer. This is higher than Arbor would have expected based on anecdotal information that customers provided outside of this survey.

Attacks Targeting Encrypted Web Services

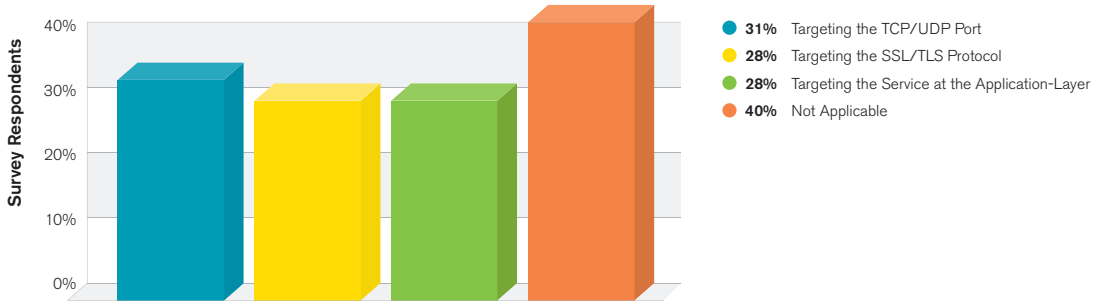

Figure 26 *Source: Arbor Networks, Inc.*

As mentioned previously, Web services remain the most popular target for application-layer attacks, with respondents seeing a broad range of attack vectors being used (Figure 27). HTTP GET floods remain the most commonly experienced attack vector, with more than three-quarters reporting this—as was the case last year. However, respondents did note some changes. HTTP POST floods appear to have become much more common in this survey period, with over half of survey participants reporting this attack vector, up from just under one-third last year. Slowloris has also seen an increase, with 43 percent experiencing this attack vector, up from 34 percent last year. Conversely, fewer respondents are seeing attacks using tools such as LOIC, HOIC and Apache Killer. This illustrates the importance of deploying defenses that can keep pace with the changing attack vectors (and variants) that attackers are using.

Application-Layer Attack Vectors

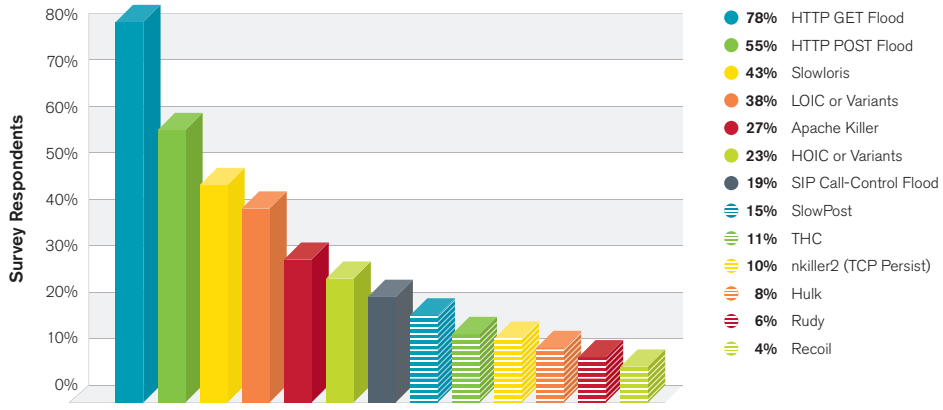

Figure 27 *Source: Arbor Networks, Inc.*

Multi-vector attacks have been a key concern over the past year, especially given their well-publicized use by the Qassam Cyber Fighters in Operation Ababil. Multi-vector attacks involve combinations of volumetric, state-exhaustion and application-layer attack vectors targeting an organization at the same time. In last year's survey, nearly half of all respondents had experienced these attacks, up from just over one-quarter in the previous year. This year, the proportion reporting these attacks has dropped to 39 percent (Figure 28). However, the proportion of respondents who "Do Not Know" if they have experienced these attacks has increased from 26 percent to 40 percent, which may account at least partially for the decrease in respondents reporting multi-vector attacks.

Multi-Vector DDoS Attacks

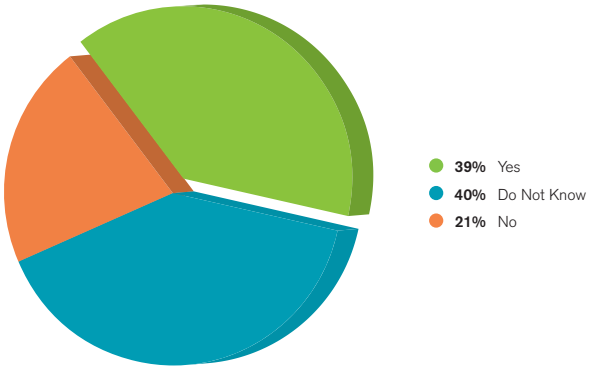

Figure 28 *Source: Arbor Networks, Inc.*

Lastly, looking at attack frequencies (Figure 29), the number of attacks monitored by respondents continues to increase year over year. Over one-quarter are now seeing more than 21 attacks per month, a significant rise from around 18 percent last year.

Attack Frequency Per Month

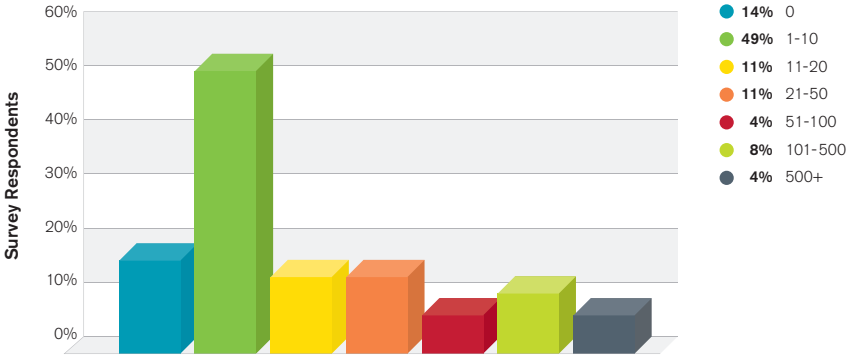

Figure 29 *Source: Arbor Networks, Inc.*

Network, Customer and Service Threat Detection

NetFlow analyzers are the most commonly deployed, and most effective, threat detection mechanism based on survey responses. Firewall logs are the second most commonly used threat detection mechanism, but only rank fourth when it comes to effectiveness.

Participants were asked which tools they use to detect threats targeting their networks, customers and services. This year the survey included a supplemental question for respondents to assess the relative effectiveness of these tools.

Figure 30 shows that most respondents are utilizing multiple tools to detect threats, with the three most common devices being NetFlow analyzers, firewall logs and SNMP-based tools. At first glance, this represents a change from last year's results. Last year, the most commonly deployed threat detection mechanism was firewall logs, used by just under three-quarters of all respondents. Commercial NetFlow analysis tools were in second place and in-house developed scripts in third. This year, however, the differentiation between commercial and open-source NetFlow and SNMP tools was removed from the survey response options, and this has shifted the results. NetFlow analyzers are now collectively most common, used by just over three-quarters of respondents, with firewall logs in second place having a similar percentage result to last year, and SNMP tools in third—again due to the amalgamation of the commercial and open-source results.

Tools Used to Detect Threats

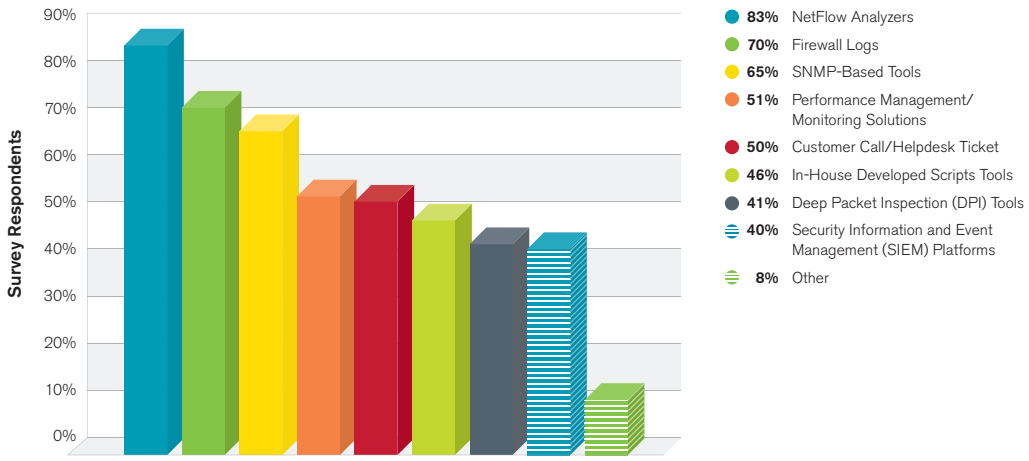

Figure 30 *Source: Arbor Networks, Inc.*

Looking at the effectiveness of deployed threat detection mechanisms (Figure 31), we can clearly see that NetFlow analyzers are viewed as most effective, as well as being the most commonly deployed threat detection mechanism. However, firewall logs, the second most commonly used detection mechanism, rank fourth in terms of effectiveness behind SNMP tools and in-house developed scripts.

Effectiveness of Detection Mechanisms

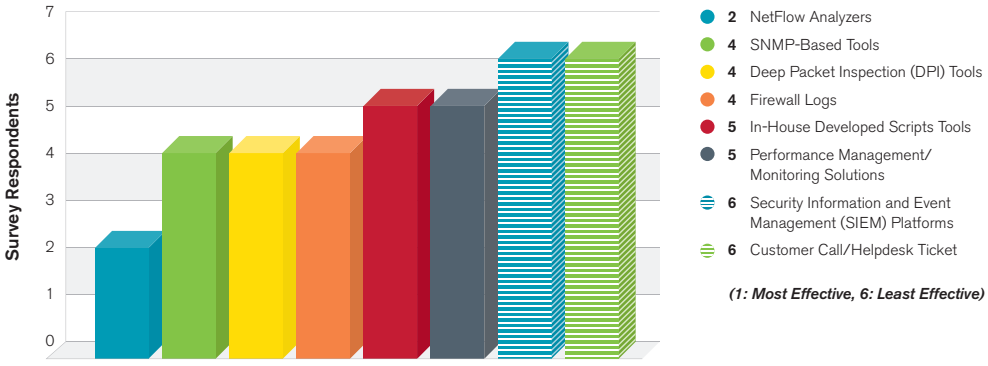

Figure 31 *Source: Arbor Networks, Inc.*

Looking at the results above, over three-quarters of respondents are using NetFlow analyzers to detect threats, illustrating how survey participants are leveraging this technology to gain cost-effective visibility of their network traffic. Traditionally, flow technologies provide visibility at Layers 3 and 4; however, some router vendors are now starting to provide Layer 7 visibility. Figure 32 shows that just over one-quarter of survey respondents are already leveraging this capability, with another half looking to do so when their infrastructure supports Layer 7 flow telemetry.

Layer 7 Flow Telemetry

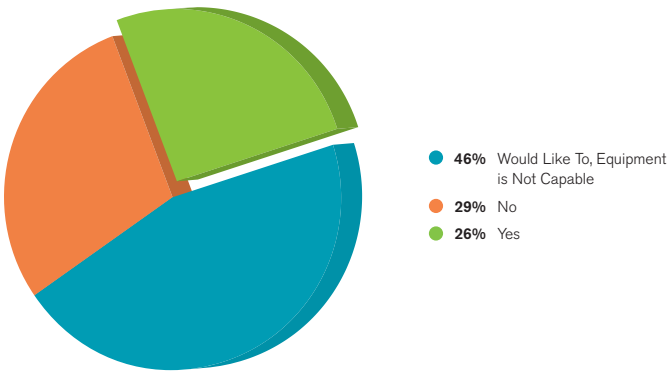

Figure 32 *Source: Arbor Networks, Inc.*

This year there was a welcome but small increase in the proportion of respondents capable of detecting outbound or cross-bound attacks on their networks. The proportion detecting these attacks had fallen over the past two years, but has now recovered slightly to 54 percent. This is encouraging because the monitoring of attack sources provides operators with the ability to locate and address infected hosts on their network, block attacks before they affect other Internet operators and provide attribution for the actions of individuals in the network.

Attack Mitigation Techniques

ACLs and intelligent DDoS mitigation systems (IDMS) are the two most popular DDoS attack mitigation mechanisms, with the proportion of respondents using firewalls reducing. The proportion able to mitigate attacks in less than 20 minutes has increased again this year, to nearly 60 percent.

The percentage of respondents utilizing ACLs and IDMS is now almost equal, at just under two-thirds (Figure 33). This represents a slight drop in the proportion using ACLs for mitigation, and a slight rise in the proportion using IDMS. This is encouraging because IDMS platforms offer more intelligent, surgical mitigation capabilities. There are a couple of other notable changes: the proportion using firewalls for DDoS mitigation has dropped from 57 percent to 47 percent; and, the proportion using destination-based remote triggered black hole (D-RTBH) filtering has increased from 39 percent to 45 percent.

Attack Mitigation Techniques

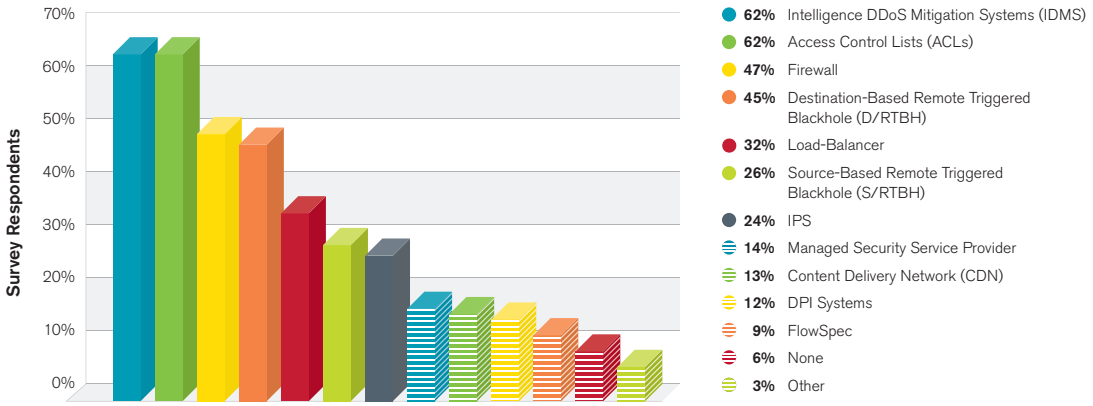

Figure 33 *Source: Arbor Networks, Inc.*

Interestingly, the two changes above are the reverse of what was noted between the 2011 and 2012 survey results. In 2012, our survey indicated that the use of firewalls had increased over 2011. This year the trend is reversed. This is positive because a reliance on maintaining session state can lead to firewalls being the targets of some state-exhaustion attacks (or being impacted due to state exhaustion as attack traffic passes through them). Firewalls have a role in a layered-security model, but relying on them to deal with all manner of DDoS attacks can put service availability at risk.

The increase in the use of D-RTBH among respondents also reverses the trend seen last year. Utilizing D-RTBH is positive in that respondents are exercising the capabilities of their network infrastructure to protect their service availability. However, because D-RTBH usually drops all traffic toward a target to protect the overall network availability and that of other customers and services at the expense of the attack target, it is not an ideal solution.

The proportion of respondents able to mitigate attacks in less than 20 minutes has increased again this year to 60 percent (Figure 34). This seems to be mainly due to the increased proportion of respondents who can automatically mitigate attacks using scripts and tools, up from 5 percent to 16 percent. Given this, the proportion taking more than 30 minutes to mitigate an attack has continued to drop to just over 20 percent, from 25 percent last year and 33 percent in 2011. The continued improvement in mitigation times is very positive, especially given the increased reliance many organizations have on Internet connectivity for day-to-day business activities.

Time to Mitigate Attacks

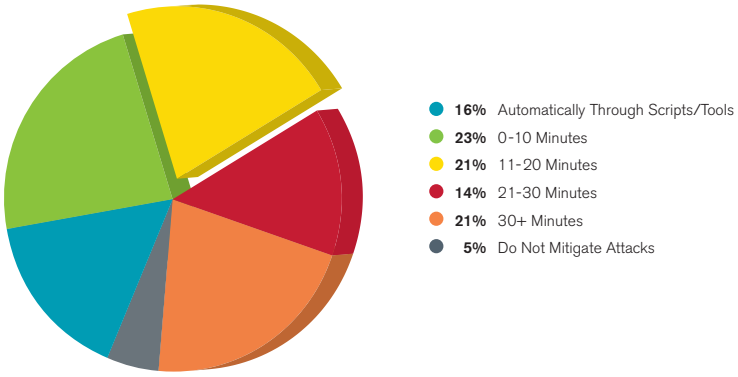

Figure 34 *Source: Arbor Networks, Inc.*

Looking at the mitigation of outbound attacks, just over 40 percent of respondents indicated that they had mitigated an attack—up from one-third last year, which is encouraging. Mitigation of outbound attacks is important because they can alter peering ratios, cause congestion and lead to other network and service issues.

The mechanisms used to mitigate outbound attacks vary from those used for inbound attacks (Figure 35), with ACLs and firewalls once again being the two most common mechanisms, as they were last year and the year before. What is concerning is the increase in the percentage of respondents who have no mechanism for mitigating outbound attacks, up from 30 percent to 40 percent this year.

Outbound Attack Mitigation Techniques

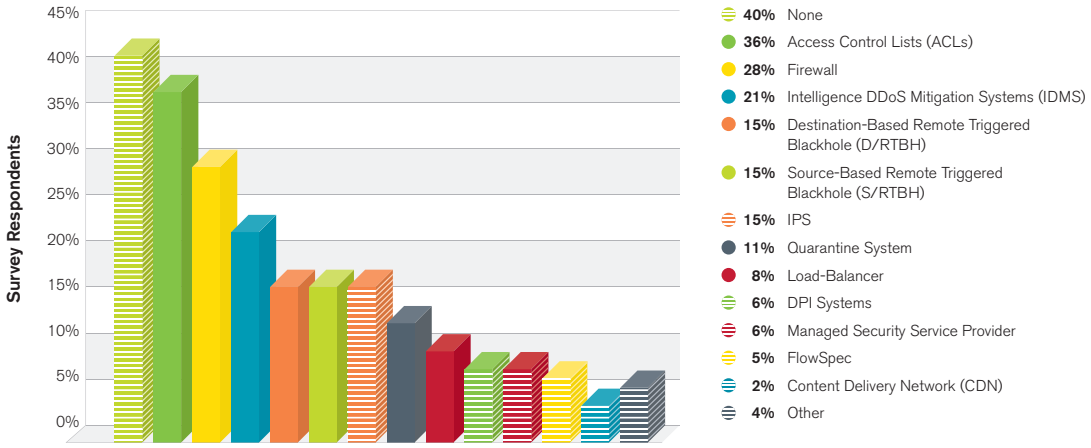

Figure 35 *Source: Arbor Networks, Inc.*

Corporate Network Threats

The proportion of respondents seeing advanced persistent threats (APTs) on their networks has increased from 20 percent to 30 percent—indicating the broadening spread of organizations being targeted by APTs. The proportion allowing employees to use their own devices on internal networks (BYOD) has increased from 63 percent to 71 percent, but 57 percent do not have any solution deployed to identify these devices.

This year's survey included a section to capture the specific threats and concerns around respondents' non-service-providing corporate or command-and-control networks.

The top threats experienced on corporate networks were "botted compromised hosts" and "under capacity for Internet bandwidth." These results are identical to last year's survey, with very similar percentages experiencing these issues (Figure 36). The most interesting change in this area is in the proportion seeing APTs on their networks, up from 22 percent to 30 percent. This illustrates the broadening spread of organizations being targeted by APTs. Attackers are aware of the value of intellectual property and customer information and use the tools available to them to bypass traditional perimeter security with relative ease. The fact that almost one-third of respondents are seeing APTs on their networks illustrates this, and focuses attention on the need for detection "inside" the network perimeter to identify suspicious and malicious host behavior wherever it occurs.

Internal Network Security Threats

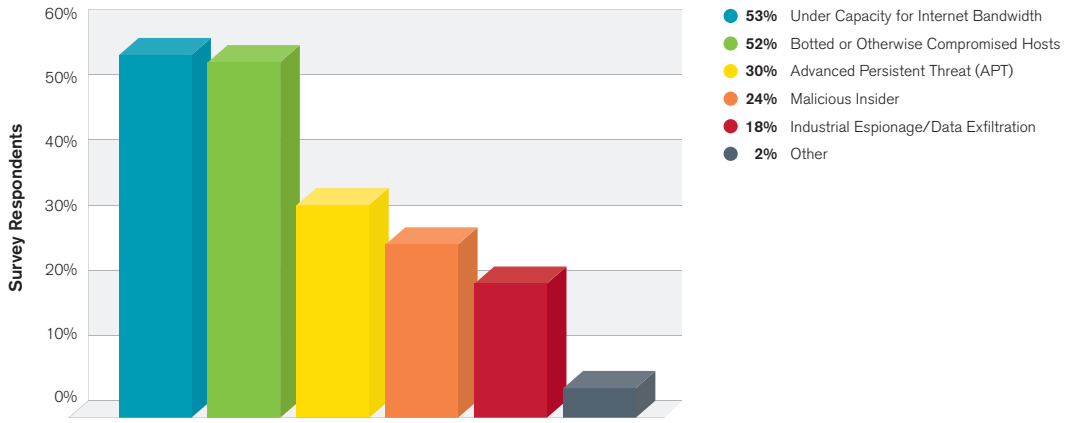

Figure 36 *Source: Arbor Networks, Inc.*

Looking at internal network security for 2014, respondents ranked botted hosts as their number one concern (Figure 37). The results for this question were almost identical to last year's. APTs came in second place—no surprise given the increased experience of these threats, noted above, and the continued media and operational security community focus on this type of threat.

Internal Network Security Concerns

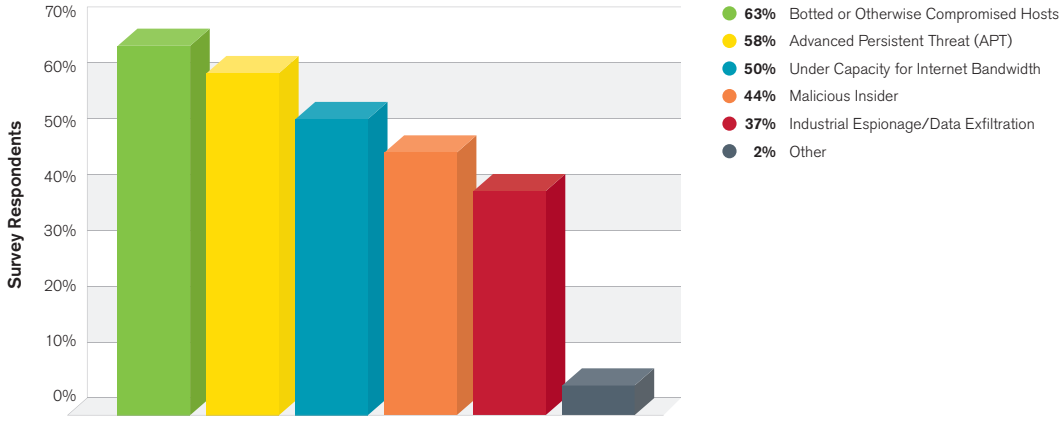

Figure 37 *Source: Arbor Networks, Inc.*

Looking at the threat detection devices used by organizations on their internal networks, firewall logs, NetFlow analyzers and SNMP tools represent the three most common mechanisms (Figure 38). This is consistent with the results from the previous survey, given that the distinction between open-source and commercial NetFlow and SNMP tools has been removed from the response options. One interesting result to note here is the doubling in the proportion of respondents who have outsourced threat monitoring—from 5 percent in last year's survey to 12 percent during this survey period. This may indicate that organizations are becoming more willing to trust internal security to external organizations, ridding themselves of the problem of maintaining in-house security expertise.

Internal Network Threat Detection Mechanisms

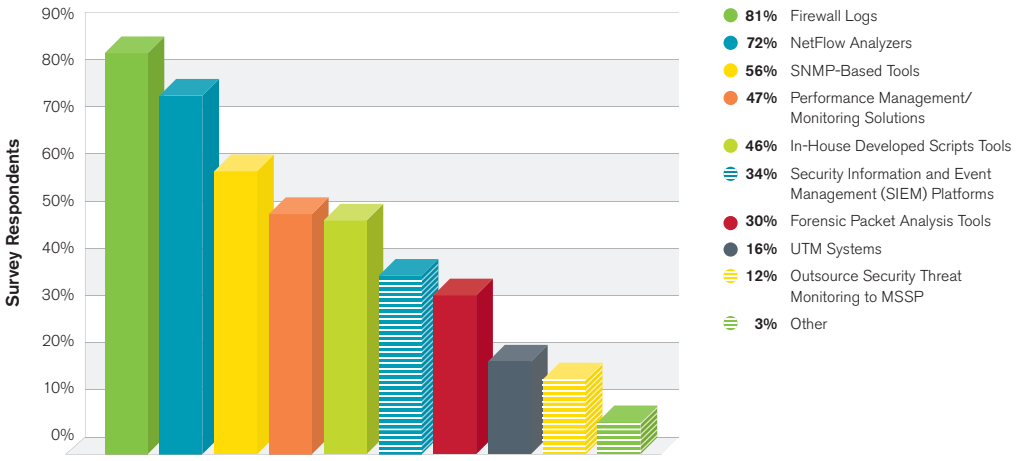

Figure 38 *Source: Arbor Networks, Inc.*

This year's survey included an additional question to ascertain whether the threat detection systems used by respondents augmented alert data with user-identity information (Figure 39). Just over one-third reported that this functionality was in place, with a similar proportion indicating that this facility would be very useful for them (but was not in place currently). This matches the current direction of security solution vendors, who are increasingly looking to add more context to detected events to assist incident response and policy definition.

Threat Data Augmented with User Identity

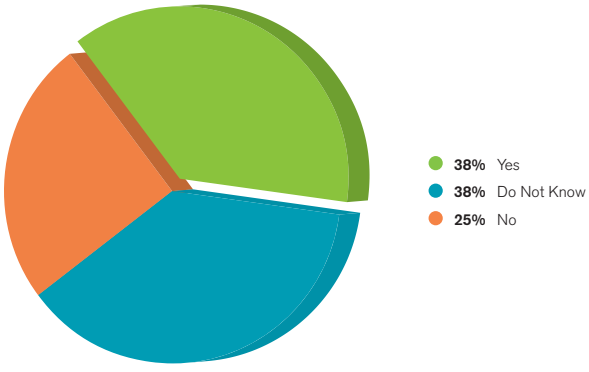

Figure 39 *Source: Arbor Networks, Inc.*

The survey also asked what tools respondents used to investigate threats detected on their internal networks. Firewall logs were the number one tool, followed by NetFlow analyzers and forensic packet recording and analysis tools (Figure 40).

Threat Analysis Tools

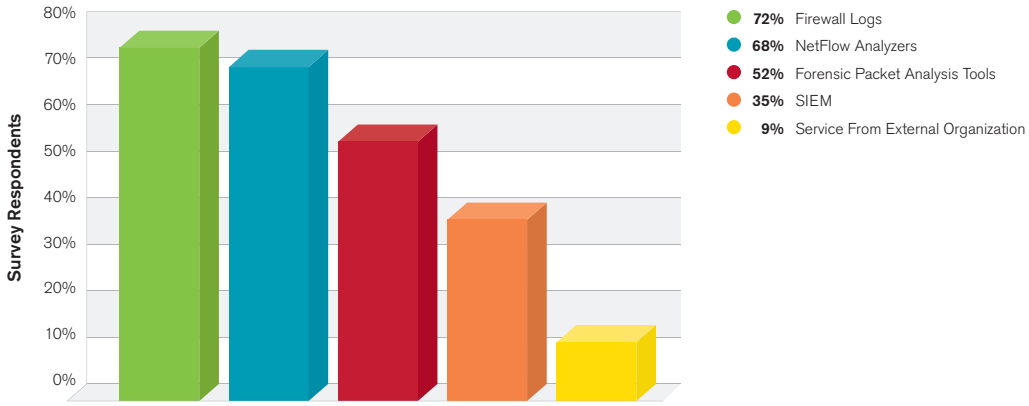

Figure 40 *Source: Arbor Networks, Inc.*

Looking at broader security policies, over three-quarters of respondents allow users to access social media sites from their internal networks. This is an almost identical result to last year. When looking at access to instant messaging applications, just over half of respondents allow this—again, an almost identical proportion to last year.

The proportion of respondents allowing employees to use their own devices on internal networks (BYOD) has, however, increased from 63 percent to 71 percent (Figure 41), illustrating how pervasive BYOD has now become. Organizations are increasingly looking to take advantage of the cost-savings and operational efficiency gains that can come from BYOD; but the loss of device and data control does pose risks.

Use of BYOD

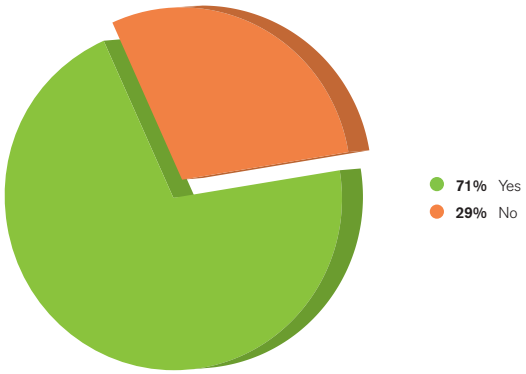

Figure 41 *Source: Arbor Networks, Inc.*

To minimize the risks posed by BYOD, organizations should be able to identify employee-owned devices on their networks, and then control their access appropriately. Surprisingly given the large and growing percentage of organizations that allow employee devices on their networks, 57 percent of survey respondents do not have ANY solution deployed to identify these devices (Figure 42). For those that do, the two most popular solutions are network access control and identity management systems.

Identification of Employee-Owned Device

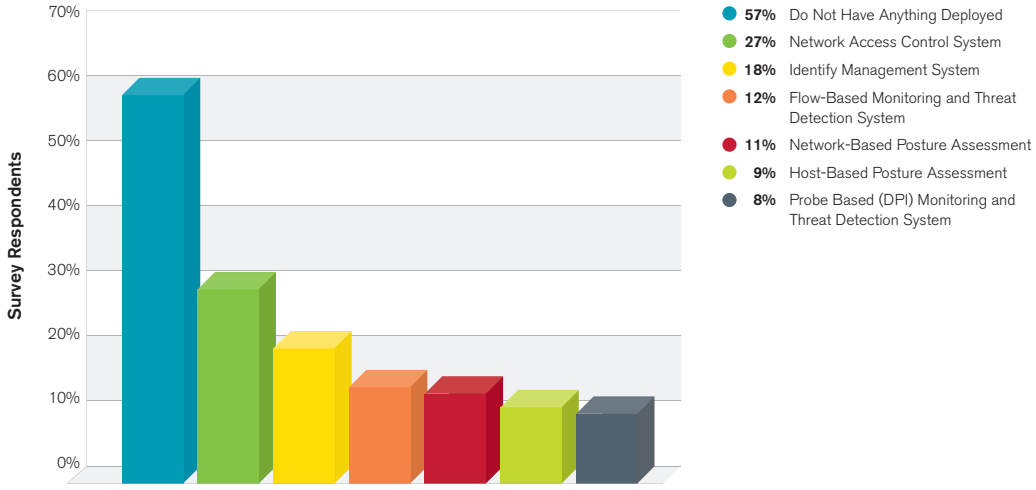

Figure 42 *Source: Arbor Networks, Inc.*

There are multiple options available to organizations seeking to monitor and restrict employee-owned devices. Organizations can implement specific security policies once a device is identified, limit access to internal resources or require the installation of specific security software or mobile device management (MDM) solutions (Figure 43). The implementation of specific security policies and segmentation of the network (to prevent access to critical internal resources) are the two most common options taken by survey respondents, with around two-thirds of them utilizing one or both of these mechanisms.

BYOD Access Restrictions

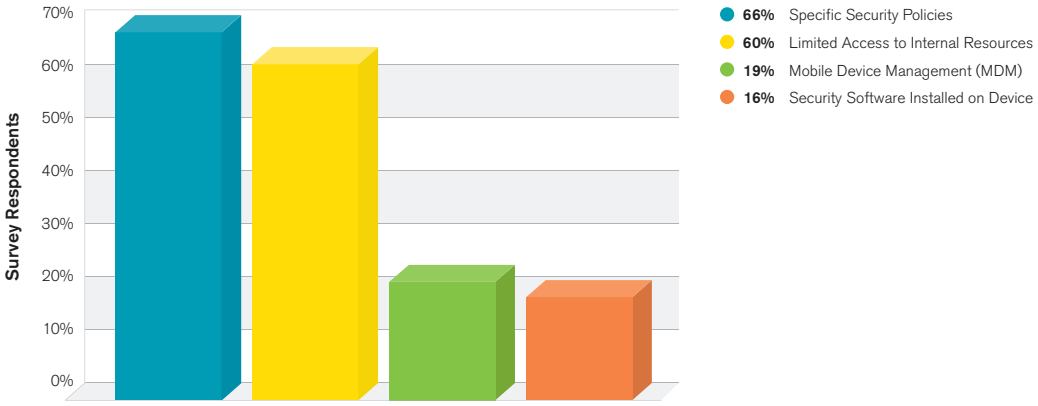

Figure 43 *Source: Arbor Networks, Inc.*

When it comes to allowing employee-owned devices to access cloud services for synchronization and backup, 60 percent of respondents do not allow this—comparable to last year's result.

Undoubtedly, there are risks to allowing BYOD on a corporate network, but only 13 percent of respondents experienced a security breach that could be attributed to BYOD during the survey period. More concerning is the fact that nearly 40 percent of respondents indicated they do not know if they had a security breach due to BYOD, which ties in with the lack of visibility of employee-owned devices in some organizations.

BYOD Security Breach

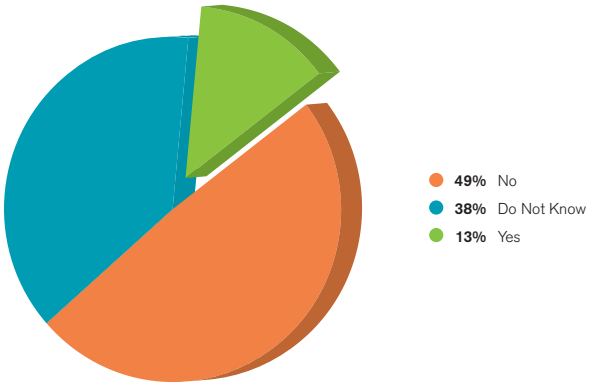

Figure 44 *Source: Arbor Networks, Inc.*

IPv6 Observations

IPv6 deployments continue, with dual stack being the most common migration strategy. Visibility of IPv6 traffic is still important to respondents, with over half having either full or partial support for flow telemetry from their infrastructure. Just over 50 percent of respondents have an IPv6 visibility solution in place.

This year, 60 percent of survey respondents reported that they either have already deployed IPv6 or have plans to deploy within the next 12 months. This is surprising, given that the corresponding number for last year was around 80 percent. Assuming that already deployed IPv6 infrastructure is not being removed, this would seem to indicate less urgency on the part of the respondents to implement IPv6. However, this change is more likely due to a shift in the survey demographics since last year. This year Arbor received responses from a higher proportion of network operators who are not service providers. In particular, the proportions of "Enterprise" and "Mobile" respondents were higher, perhaps indicating a shift towards respondents who are less far along in their IPv6 preparations.

This is an interesting reflection on the slow overall adoption of IPv6 through the entire IP industry. While a high percentage of service providers have it ready to go, networks at the edge of the Internet are adopting IPv6 much more slowly.

Of the respondents who have IPv6 plans, 29 percent have completed their deployment of IPv6 (up 4 percent from last year) with a further 54 percent in process. The rest are planning for a deployment soon (Figure 45). This breakdown does show a slight acceleration in IPv6 take-up, but it is not significantly different from last year's figures.

IPv6 Deployment Progress

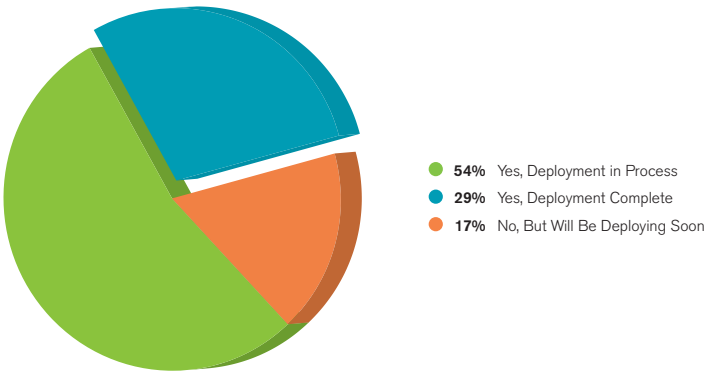

Figure 45 *Source: Arbor Networks, Inc.*

This year just over half of respondents indicated that IPv4 address availability is NOT an issue for them, and will not be within the next 12 months. This is very similar to last year. A number of respondents indicated that they still have sufficient IPv4 address availability for a period of time. This, coupled with the lack of an IPv6 "event" in 2013, may explain the somewhat reduced focus on IPv6 migration.

In terms of IPv6 migration strategies (Figure 46), over 97 percent of respondents have opted for dual-stack deployments (up 7 percent over last year); however, a percentage of them are also planning on using tunneling and/or address translation, which may increase their threat surface. The further shift towards dual stack as the dominant methodology would seem to be mostly at the expense of tunneling, although the proportion of respondents who indicated they plan to use translation has also reduced slightly.

IPv6 Migration Strategy

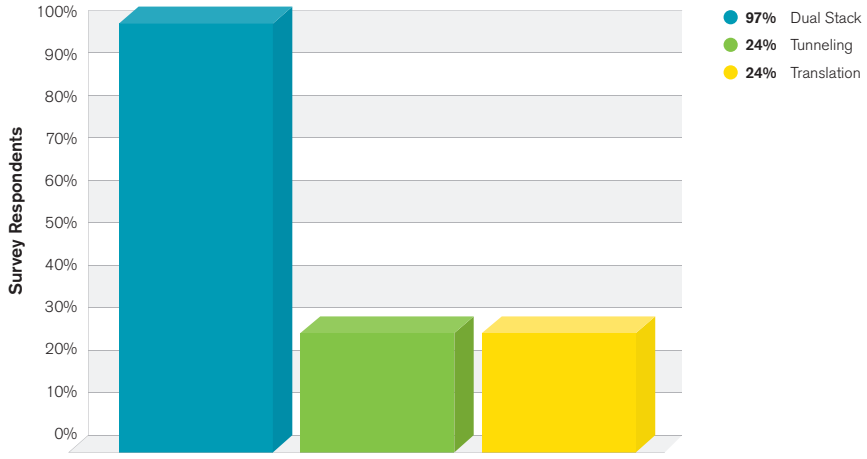

Figure 46 *Source: Arbor Networks, Inc.*

While getting visibility of the IPv6 traffic on networks is becoming increasingly important, just over half of respondents actually have a visibility solution for IPv6 traffic deployed (Figure 47). However, it is encouraging that the proportion of respondents with visibility solutions deployed has remained similar to last year, despite the larger respondent pool.

Prevalence of IPv6 Traffic Visibility

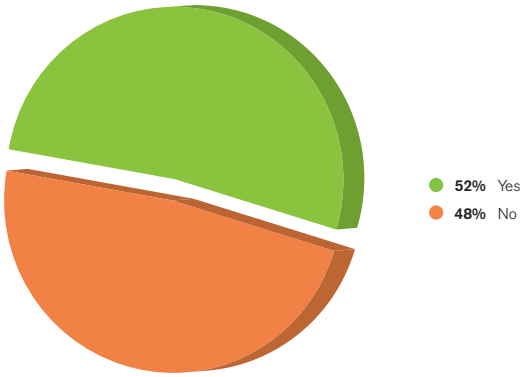

Figure 47 *Source: Arbor Networks, Inc.*

This year's results do show a small decrease in the proportion of respondents who have either partial or full support for IPv6 flow telemetry from their network infrastructure (Figure 48)—a decrease from 75 percent last year to 69 percent this year. Flow telemetry remains important for scalable, cost-effective threat detection and visibility, and overall the remaining high level of support for flow telemetry remains encouraging. The slight decrease is possibly attributable to the increased proportion of "Enterprise" and "Hosting" respondents who may have routing equipment with poorer IPv6 telemetry support. This is somewhat corroborated by the fact that the "Roadmap" category (defined as vendor support being more than 12 months away) has risen from 4 percent to 6 percent and the "Will not support" category has risen from 0 percent to 1 percent this year.

IPv6 Flow Telemetry Support

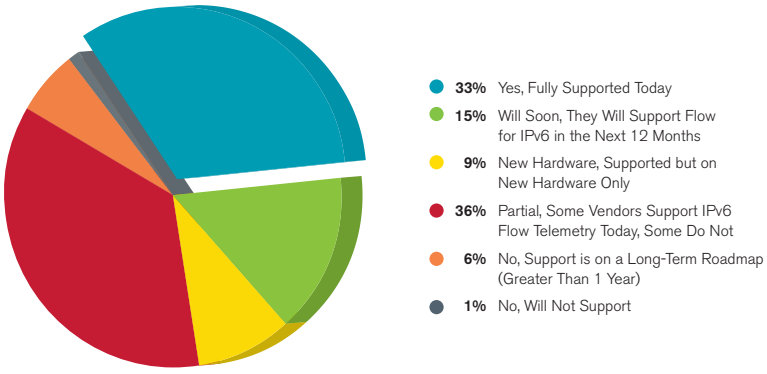

Figure 48 *Source: Arbor Networks, Inc.*

In terms of providing IPv6 addresses to customers, as last year, more respondents offer IPv6 services to their business customers as compared to their consumer customers (Figures 49 and 50). This year, the numbers are slightly up at 73 percent for business and 53 percent for consumers vs. 70 percent and 48 percent respectively. This year Arbor also gathered statistics on the reported uptake percentages in each category. As can be seen, even where available, uptake is still relatively low, with the vast majority of respondents reporting uptake in the 1 percent to 25 percent range.

IPv6 Addresses for Business Customers

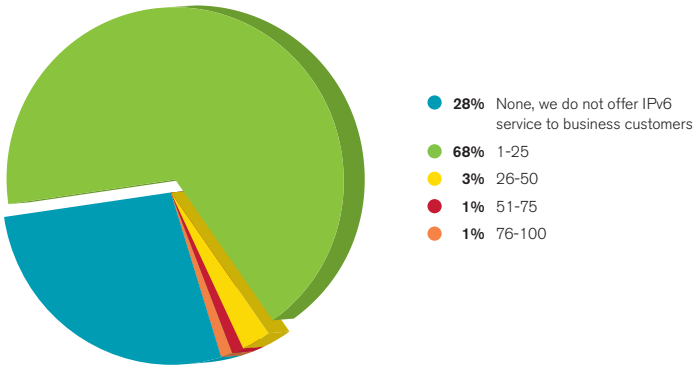

Figure 49 *Source: Arbor Networks, Inc.*

Again this year, the survey asked respondents for the peak daily rate of IPv6 traffic on their network. The highest reported traffic rate was 20Gbps—a significant increase over last year when 3Gbps was the highest reported volume. There were also several answers in the >1Gbps range and many responses in the 100Mbps range. The largest IPv6 traffic rates were reported in European countries. This is likely a direct result of aggressive IPv6 adoption policies in place within the European community.

IPv6 Addresses for Consumer Customers

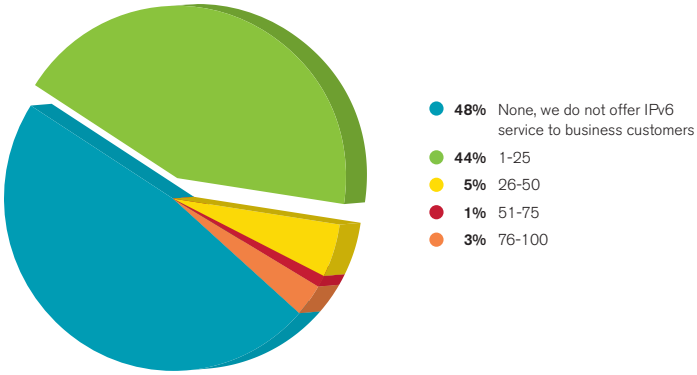

Figure 50 *Source: Arbor Networks, Inc.*

Although IPv6 traffic is still growing relatively quickly, the actual volume of traffic is still very low compared to IPv4, although climbing rapidly (see ATLAS insert). The slightly increased adoption of IPv6 by consumers is a likely cause for this growth, especially given the continuing availability of IPv6 services post-World IPv6 Launch day.

When considering projected IPv6 traffic growth (Figure 51), over half of respondents anticipate a 20 percent rise over the next 12 months (up from 42 percent last year), with 9 percent expecting more than 100 percent growth (down from 25 percent last year). This is interesting given the strong growth exhibited over the last year looking at ATLAS statistics and may demonstrate that respondents are underestimating the take-up of IPv6.

Anticipated IPv6 Traffic Growth

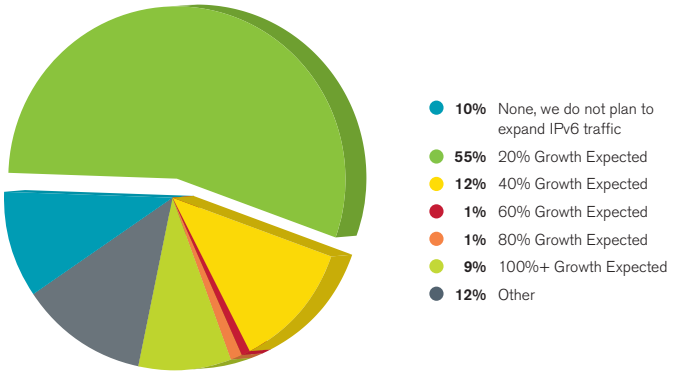

Figure 51 *Source: Arbor Networks, Inc.*

Last year there was a significant shift in the threats to IPv6 services that concerned survey respondents, and this year's results are fairly consistent with last year's data (Figure 52). The top perceived threat is still traffic floods or other DDoS attacks, with 72 percent of respondents showing a concern here—up slightly from 70 percent last year.

Also this year, IPv4 and IPv6 feature parity moved into second place, to top misconfiguration as the second-largest concern. The proportion of respondents concerned about feature parity has not shifted significantly though; rather, this change is more due to other concerns reducing significantly.

IPv6 Security Concerns

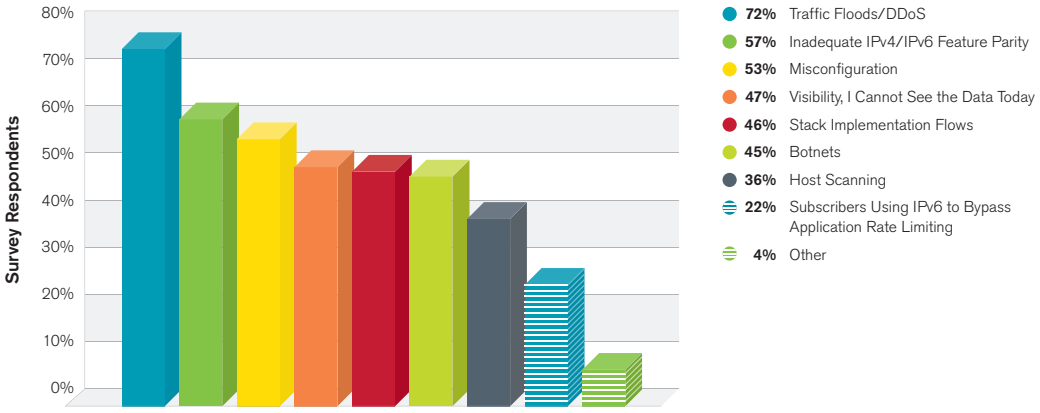

Figure 52 *Source: Arbor Networks, Inc.*

The reduced ranking of misconfiguration as an IPv6 security concern—53 percent of respondents this year, down from 60 percent last year—may speak to increasing familiarity with the protocol on the part of the respondents or bolstered confidence due to some successful initial deployments.

This year the survey also asked about concerns over attacks against dual-stack services (Figure 53). Just under half of respondents are either concerned or very concerned. This reflects the fact that in a dual-stack environment, the exploitation of more immature IPv6 infrastructure can have a very real effect on associated IPv4 infrastructure. The implication here is that dual-stack implementations increase risk to the existing IPv4 infrastructure.

IPv6 Dual-Stack Security Concerns

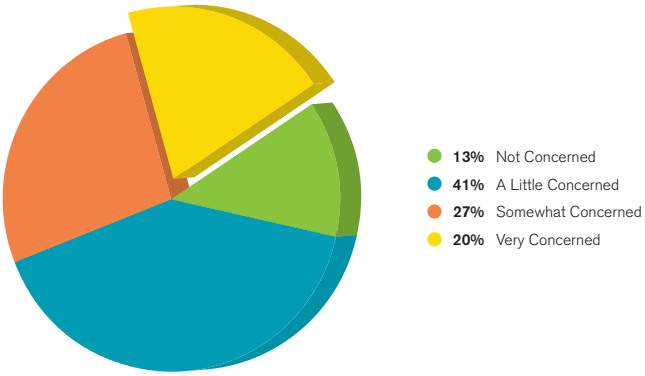

Figure 53 *Source: Arbor Networks, Inc.*

For the first time this year, IDMS systems have become the most important attack mitigation technique for dealing with IPv6 attacks, with 70 percent of respondents relying on these systems (Figure 54). Use of ACLs remains strong though (down from 67 percent to 61 percent). ACLs are a useful technique, especially if utilized as an adjunct to an IDMS.

Source- and destination-based remote triggered blackholes have both risen in popularity. This is likely due to the extensive use of such techniques in the hosting space. The proportion of respondents using FlowSpec remains the same, probably due to the still limited support for this promising diversion and blackholing technique by major router vendors, although this is improving.

IPv6 Mitigation Capabilities

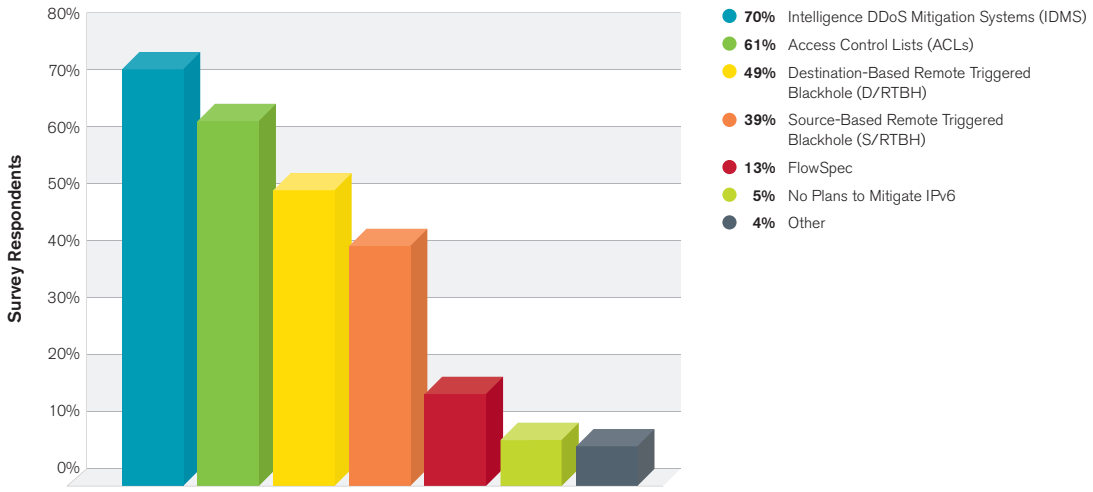

Figure 54 *Source: Arbor Networks, Inc.*

The percentage of respondents who do not intend to mitigate attacks against IPv6 services remains low at 5 percent, a very slight increase. This indicates that IPv6 services remain important to Internet operators.

ATLAS-Monitored IPv6 Growth

The ATLAS system, as well as tracking DDoS attacks, gathers traffic statistics from participants. One of the statistics gathered is the amount of native IPv6 traffic crossing the boundaries of participant networks.

The peak, cumulative, native IPv6 traffic volume monitored by ATLAS across approximately 290 participating network operators during this survey period was around 445Gbps, more than 10 times the peak monitored last year. This is a significant gain even against a backdrop of more than double the peak amount of IPv4 traffic (peak of over 80Tbps in 2013, versus just under 40Tbps in 2012). However, even with this growth, it still remains clear that IPv6 traffic is a small percentage of overall traffic, less than 1 percent.

However, it is still the case that not all ATLAS respondents have the capability of monitoring native IPv6 traffic due to their configuration or network infrastructure. This year around 27 percent of ATLAS participants provided statistics on native IPv6 traffic, up around 7 percent from last year. Figure 55 shows the geographic distribution of these participants. Based on the statistics reported by these participants, native IPv6 traffic is, on average, responsible for 0.11 percent of their total Internet traffic.

ATLAS IPv6 Native Traffic Reporters by Region

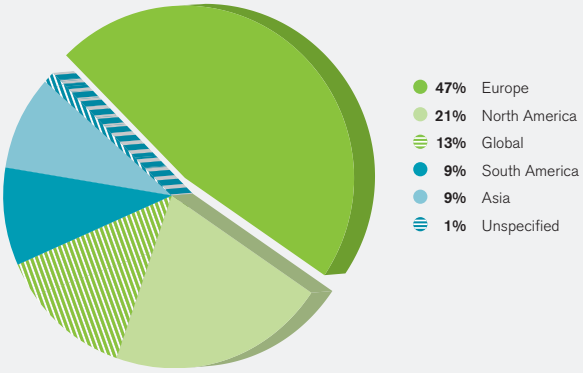

Figure 55 *Source: Arbor Networks, Inc.*

ATLAS-Monitored IPv6 Growth (continued)

This year IPv6 traffic has grown significantly despite a lack of specific consciousness-raising events such as World IPv6 Lauch Day (Figure 56). Native IPv6 traffic is by far the most prevalent traffic type seen, which tends to corroborate dual stack as the preferred mechanism for the majority of respondents.

Really taking off in the last half of the year, IPv6 traffic growth of 10x has been observed during this year, perhaps indicating that IPv4 address exhaustion is really starting to strain some geographies. If this rapid growth trajectory continues, 2014 could well be the breakout year for IPv6.

ATLAS-Monitored IPv6 Traffic Growth

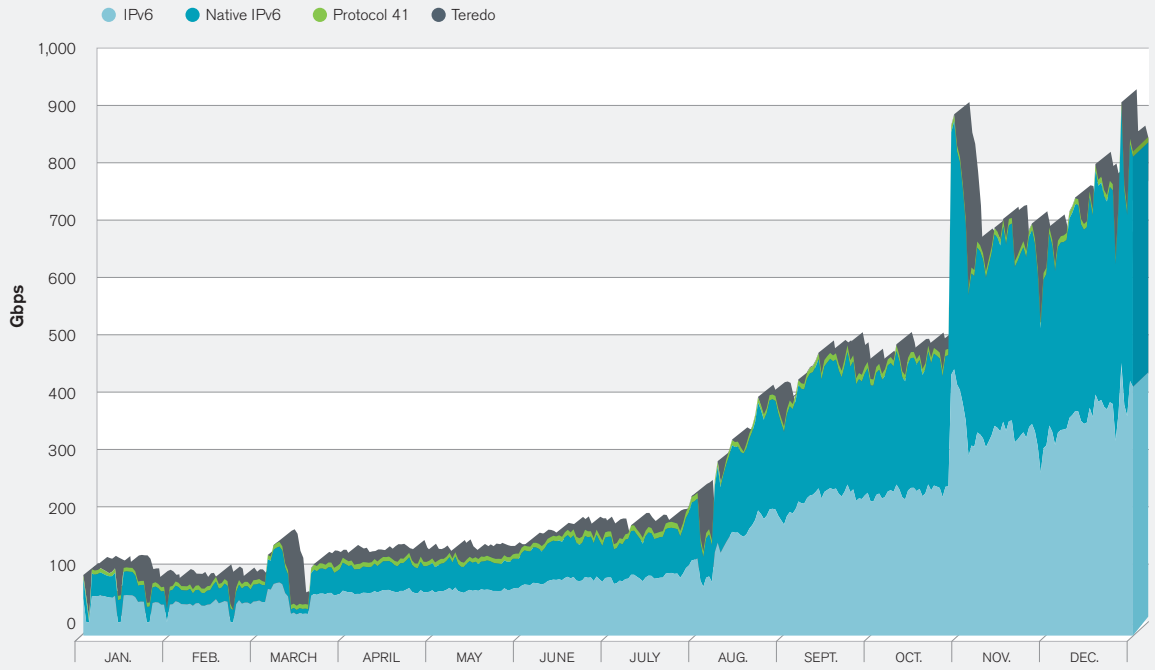

Figure 56 *Source: Arbor Networks, Inc.*

DNS and DNSSEC Operators

Approximately 26 percent of respondents have no security group within their organizations with formal responsibility for DNS security. Eighty percent of respondents have implemented the best practice of restricting recursive lookups by their DNS servers to queries from hosts located either on their own networks or on those of their end users, while 20 percent have not yet done so. Just over one-third of respondents have experienced customer-impacting DDoS attacks on their DNS infrastructure during the survey period.

Nearly 85 percent of respondents operate DNS servers on their networks (up slightly from last year), and almost three-quarters have either assigned responsibility for this infrastructure to their main OPSEC group or to a dedicated DNS security team (Figure 57).

DNS Security Responsibility

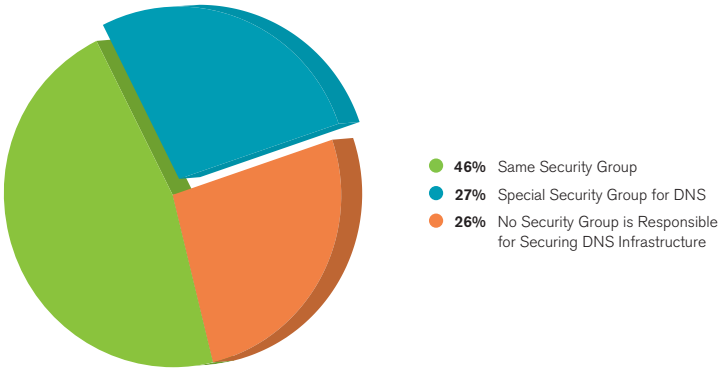

Figure 57 *Source: Arbor Networks, Inc.*

Just over one-quarter of respondents indicated that there is no security group within their organizations with formal responsibility for DNS security, up from 19 percent last year. This is possibly due to consolidation of security personnel, and may also reflect the expansion of the respondents outside the more traditional carrier base. Either way, the lack of security focus is probably a contributing factor to the significant number of unsecured, open DNS resolvers on the Internet today that can be abused to launch extremely high-bandwidth DNS reflection/amplification attacks, as have been seen over the last year.

When asked if they have good visibility of the traffic into or out of their DNS infrastructure, just over two-thirds of respondents reported good visibility at Layers 3 and 4, while just over one-third reported having full Layer 7 visibility (Figure 58). The fact that Layers 3 and 4 remained similar to last year, coupled with a significant gain in Layer 7 visibility (up 10 percent), is encouraging against a background of increasingly sophisticated attacks.

DNS Traffic Visibility

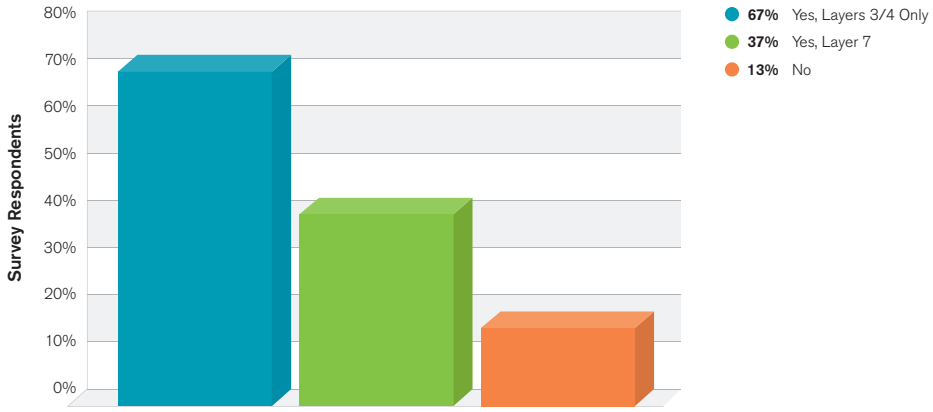

Figure 58 *Source: Arbor Networks, Inc.*

Eighty percent of respondents have implemented the best practice of restricting recursive lookups to their DNS servers to hosts located either on their own networks or on those of their end users (Figure 59). This is an almost identical result to last year's survey. While still a high percentage, this lack of improvement is disappointing against the backdrop of last year's Spamhaus attack and the renewed awareness of DNS reflection/amplification this has created. Twenty percent of respondents having open resolvers on their network open up ample opportunity for continued large DNS reflection attacks.

DNS Recursive Lookups Restricted

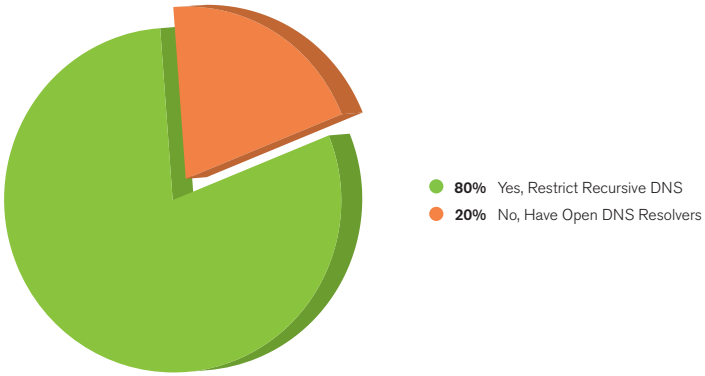

Figure 59 *Source: Arbor Networks, Inc.*

The Spamhaus Attack: A Massive DNS Amplification Attack in Action

In March of 2013, Spamhaus, an organization that maintains lists of spammers, came under a massive DNS reflection DDoS attack. The attack volume was reportedly as high as 300Gbps. Although not monitored directly by ATLAS, this number has been verified by the service provider community and represents the largest reported DDoS attack ever seen.

Although DNS reflection/amplification is not a new kind of attack, this event is noteworthy because of the extreme amounts of bandwidth brought to bear upon the victim, and later the fabric of the Internet itself. It is this latter activity that prompted exaggerated claims of this being an attack that brought down the Internet.

Previously, the largest reported (and verified) attacks of this type were around 100Gbps. This year, however, there have been several examples of large (damaging) DNS reflection/amplification attacks above the 100Gbps level (Figure 60).

Peak DDoS Attack Size (January 2010 to March 2013)

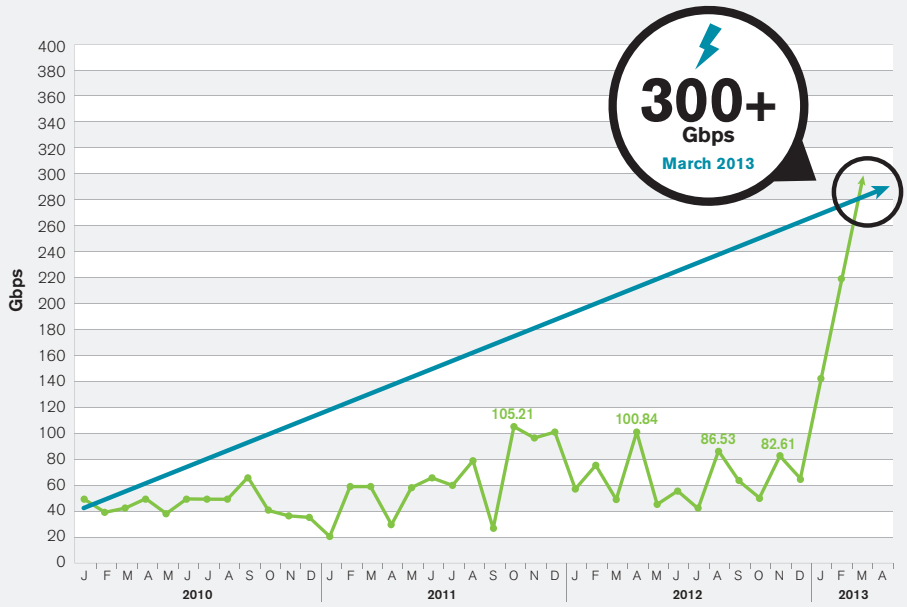

Figure 60 *Source: Arbor Networks, Inc.*

ASERT

The Spamhaus Attack: A Massive DNS Amplification Attack in Action (continued)

A DNS reflection/amplification attack leverages the DNS infrastructure of the Internet to magnify the traffic that an attacker is capable of generating.

DNS is a critical part of Internet infrastructure. It is primarily used for hostname to IP address resolution. In a DNS reflection/amplification attack, an attacker sends DNS queries (60 bytes or so) to open DNS resolvers, spoofing the source IP address of the query to be that of the intended attack victim. The DNS query usually asks for a large record set (for example, any queries, or queries for TXT records containing PGP public keys, etc.). This results in the server generating a response that is many times larger than the initial query. By using multiple client machines (bots) to send queries to multiple open DNS resolvers, an attacker can generate very large volumes of attack traffic from widely distributed sources. In fact, over 30K open resolvers were used during the Spamhaus attacks.

The DDoS attacks originally targeted Spamhaus on the 16th of March. Spamhaus engaged the services of CloudFlare (blog.cloudflare.com), which was able to mitigate the initial attacks successfully. (At this time, the traffic levels were around 85Gbps.) The attacks then escalated between the 19th and 21st of March—exhausting the capabilities of CloudFlare, targeting next-hop addresses at Internet exchanges around the world, and causing congestion and a perceived Internet slowdown in some geographies. Such attacks on the fabric of the Internet itself are somewhat unusual, and in dealing with this phase of the attack, some important lessons were learned.

Two things make these kinds of attacks possible: lack of ingress filtering on service provider networks (allowing traffic from spoofed source addresses to be forwarded), and the number of open DNS resolvers on the Internet (which will respond to queries from any IP address).

In order for the attack above to be possible, an attacker must be able to spoof the source address of DNS queries to be that of the intended attack victim. All organizations should implement BCP38/84 anti-spoofing at all edges of their networks.

tools.ietf.org/html/bcp84
tools.ietf.org/html/bcp38

Unfortunately, in this year's survey, only 51 percent of respondents indicated that they currently have BCP 38/84 implemented at their network edges.

The second key component of these attacks is the large number of open DNS resolvers available on the Internet. Currently, it is estimated that there are around 27 million open DNS resolvers on the Internet (openresolverproject.org).

Looking again at the 2013 survey data, approximately 26 percent of respondents indicated that there is no security group within their organizations with formal responsibility for DNS security. This undoubtedly contributes to the fact that 20 percent of survey respondents have not implemented the best practice of restricting their DNS servers to only respond to queries from hosts located either on their own networks or on those of their end users. In addition, it opens up a big opportunity for attackers to deploy rogue open DNS resolvers in these networks without the operator knowing of their existence.

In addition to the DNS attack, Spamhaus also suffered from other attacks during this period. Part of Spamhaus' assigned IP address ranges were hijacked for a period of time via illegitimate BGP announcements, also known as route hijacks, apparently by a "rogue" ISP. After hijacking the Spamhaus routes, which succeeded in diverting some proportion of legitimate network traffic intended for Spamhaus, the attacker then set up a bogus DNS server that gave poisoned answers to all queries intended for the Spamhaus DNS server.

These poisoned answers falsely claimed that all email from various sources was spam. This caused false positives for users of Spamhaus' anti-spam reputation service, whose traffic traversed ISPs who incorrectly accepted the hijacked routes.

As indicated in Figure 61, over one-third of respondents have experienced customer-impacting DDoS attacks on their DNS infrastructure during the survey period—an increase of 10 percent over last year's survey. This increase is a worrying trend and demonstrates the need for increased visibility and better mitigation tools in this space.

Attacking the authoritative DNS servers for a given domain can be an effective way to make the domain unreachable for end users. In many cases, it also requires fewer attack resources to disrupt service than attacking the target servers or applications directly. Collateral damage is a major issue with these kinds of attacks because all the domains for which a server is authoritative may become unresolvable.

Customer-Impacting DNS Attacks

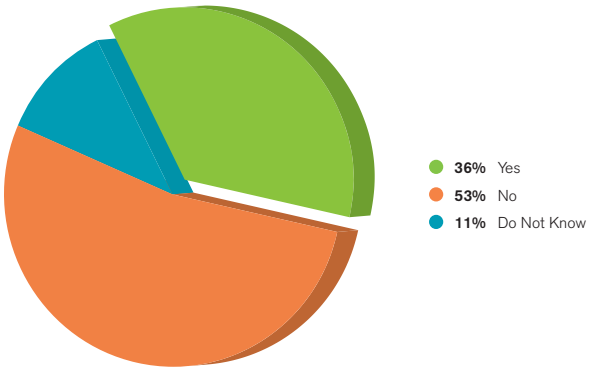

Figure 61 *Source: Arbor Networks, Inc.*

As noted in Figures 62 and 63 respectively, just over one-third of respondents indicated they have experienced DDoS attacks against their authoritative DNS servers. Just under one-quarter indicated they have experienced attacks against their recursive DNS servers during the survey period. These numbers are both down from last year, with attacks against authoritative servers down 10 percent. Given that customer reports of attacks have increased, this could be indicative of diminished overall visibility across respondents.

Operators of DNS infrastructure should continue to prioritize improvements to their DNS traffic visibility and threat detection capabilities to ensure the security of this critical service. The following are some respondent descriptions of DNS attacks in the past year:

- Direct attacks aimed at denying name resolution for customers.
- Direct DDoS attacks, 100Kpps, 400Mbps.
- Mostly SYN floods on TCP/UDP 53.

DDoS Attacks Against Authoritative DNS Servers

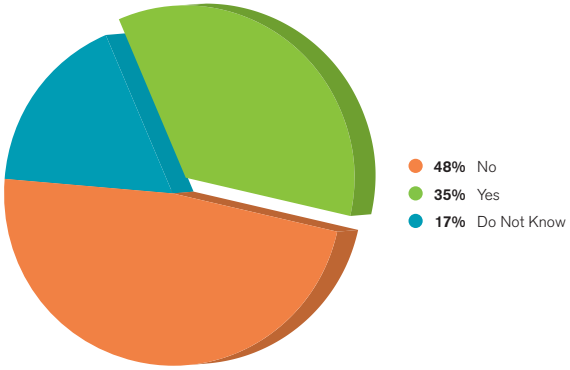

Figure 62 *Source: Arbor Networks, Inc.*

DDoS Attacks Against Recursive DNS Servers

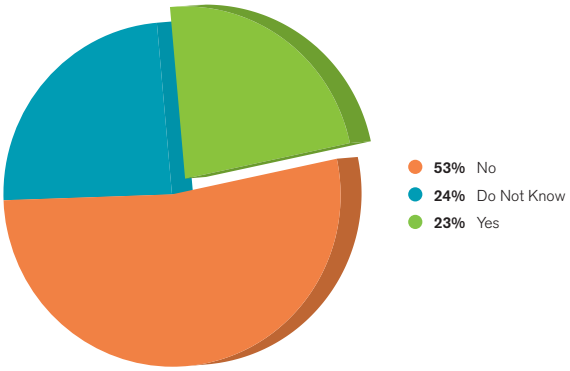

Figure 63 *Source: Arbor Networks, Inc.*

Just under one-quarter of respondents reported experiencing DNS cache-poisoning attacks directed to, or through, their DNS infrastructures during the survey period (Figure 64), up from 18 percent last year. Also, just under one-third indicated that they do not know whether or not they have experienced DNS cache-poisoning attacks, an identical proportion to last year. These figures reveal that some operators still have a serious lack of visibility into the traffic on their DNS servers, and that little progress has been made in this area despite a high-profile year for DNS attacks.

DNS Cache-Poisoning Attacks

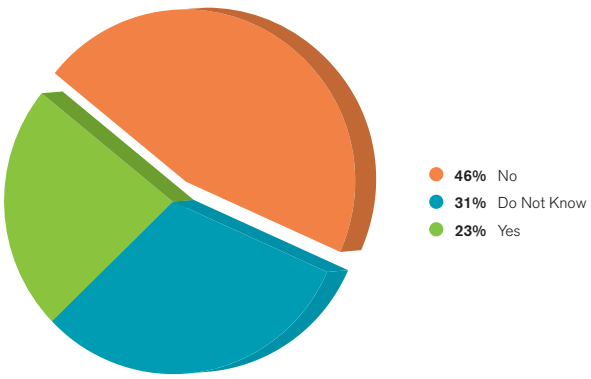

Figure 64 *Source: Arbor Networks, Inc.*

As illustrated in Figure 65, just under half of respondents stated that they do not observe any issues with DNSSEC functionality due to the lack of EDNS0 and/or TCP/53 DNS support on the Internet at large, a slight reduction over last year. However, just over one-third indicated that they have insufficient visibility to make this determination. Both figures are trending negatively, and indicate that a serious gap in the traffic analysis capabilities of DNS operators remains a big issue.

Issues with DNSSEC Functionality

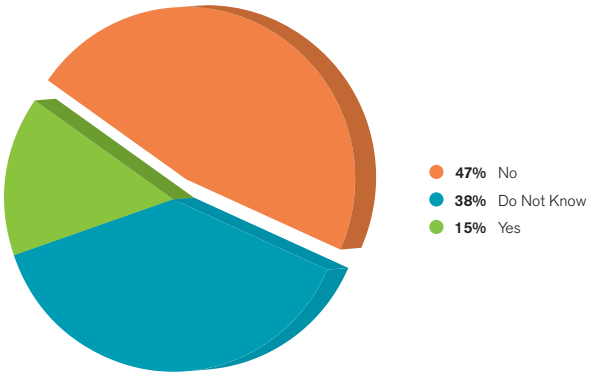

Figure 65 *Source: Arbor Networks, Inc.*

ATLAS-Monitored DNS DDoS Attacks

The ATLAS system shows that the proportion of monitored attacks targeting port 53 has stayed fairly steady over the whole of 2012/2013 at around 10 percent, although this percentage did dip significantly in the first half of 2013 (to just over 6 percent), but has since recovered.

The largest attack tracked by ATLAS targeting port 53 was 58Mpps (with multiple others only slightly smaller in the 40Mpps to 58Mpps range). Also of interest are attacks reported against port 0; in some cases, these could be indicative of DNS amplification attacks as Netflow reports non-initial fragments as port 0. Numerous large attacks of this type were reported to ATLAS in 2013, the largest being of 191Gbps/17.5Mpps.

Exactly 40 percent of respondents indicated that they do not believe drastically increased DNS response sizes have resulted in larger, more damaging DNS reflection/amplification attacks (Figure 66). This is a 10 percent reduction from last year, and correlates exactly to a 10 percent increase in respondents who say they believe increased response sizes is an issue. As noted in last year's report, DDoS attack amplification leveraging DNSSEC has been observed in the wild, and the increased reporting of these types of attacks in this year's survey tends to bear this out.

DNSSEC Response Size Impact

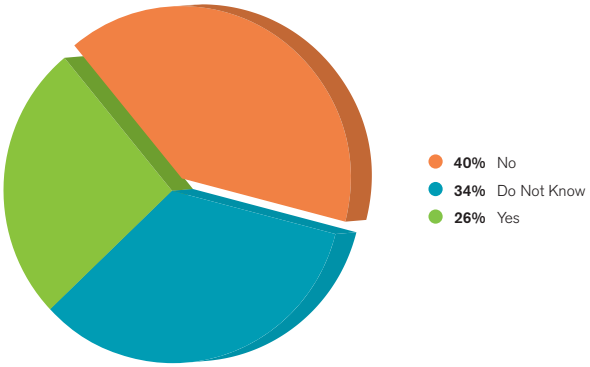

Figure 66 *Source: Arbor Networks, Inc.*

When asked if they had additional concerns regarding DNSSEC deployment, respondents provided the following feedback:

- Heavy operational complexity.
- New and exciting ways for critical infrastructure service to break.
- Disappointing amplification potential.
- Breakages due to lack of EDNS0.
- Evolving standards and adapting operations to support and deploy.

Respondents indicated they are using a variety of security measures and tools to protect their DNS infrastructure from DDoS attack (Figure 67). Just over half of respondents said they have deployed an IDMS, and nearly 60 percent have employed iACLs. Disappointingly, the proportion using iACLs is lower than last year's 67 percent, despite the effectiveness of this technique in protecting critical infrastructure.

Like last year, significant numbers of respondents are also using firewalls, IPS/IDS and other measures to protect their DNS infrastructure, but usage of uRPF has declined significantly from over one-third to less than one-quarter. Interestingly, this is also true of source-based blackhole, possibly indicating that the effectiveness of this technique is declining as attacks grow more distributed.

DNS Security Measures

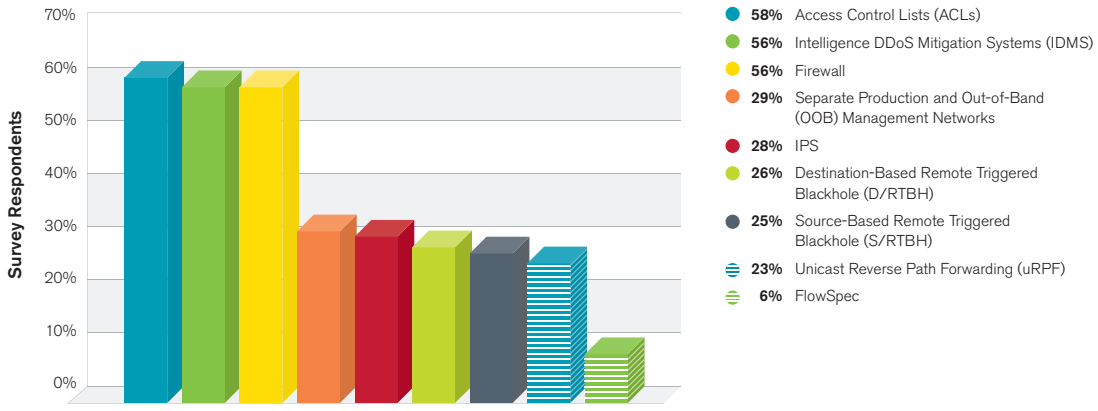

Figure 67 *Source: Arbor Networks, Inc.*

Data Centers

Data centers routinely experience DDoS attacks, with both infrastructure and customers targeted. Traditional security appliances cannot prevent these disruptions, which can cause significant loss of revenue.

With the current trends toward cloud computing and data center consolidation, it is important to understand the key trends relating to traffic analysis techniques, DDoS attacks, DDoS mitigation and other points of interest regarding data centers. Approximately 69 percent of survey respondents offer data center services to their end customers, a small increase from last year.

When asked how much visibility data center operators have into their networks, just over 83 percent indicated that they have good visibility up to Layer 4, while slightly less than one-quarter indicated they have visibility up to Layer 7 (Figure 68). This shows that the majority of operators are likely blind to attacks above Layer 4 until there is a service impact, making it difficult to effectively defend against such attacks. Layer 7 DDoS attacks are especially dangerous as they can be "low and slow," and are often undetected by traditional volumetric detection mechanisms.

Visibility of Traffic in the Data Center

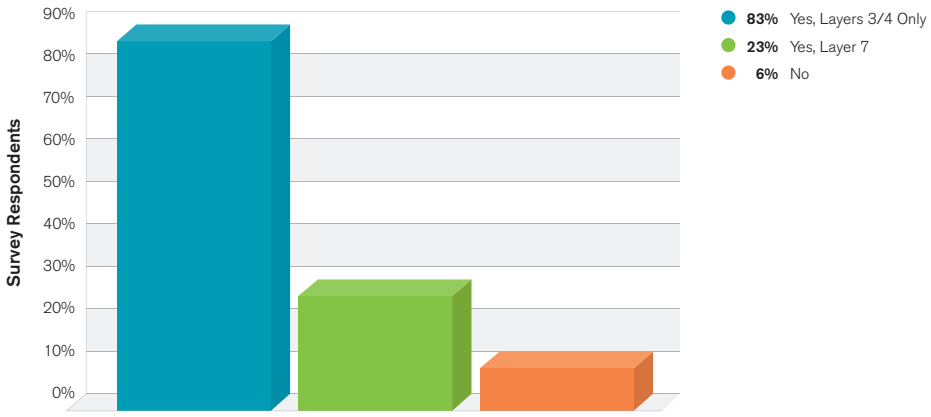

Figure 68 *Source: Arbor Networks, Inc.*

In terms of actively utilized security devices, firewalls are standard practice in data centers, as one would expect, with almost all respondents utilizing them. The second most commonly deployed technology is IDS/IPS, used by two-thirds of respondents (Figure 69). Interestingly, we saw an increase in all types of security mechanisms used in the data center this year. This may be the result of the more varied business types of respondents. It may also indicate a more conservative defense-in-depth strategy used by these new respondents.

Security Devices and Techniques in the Data Center

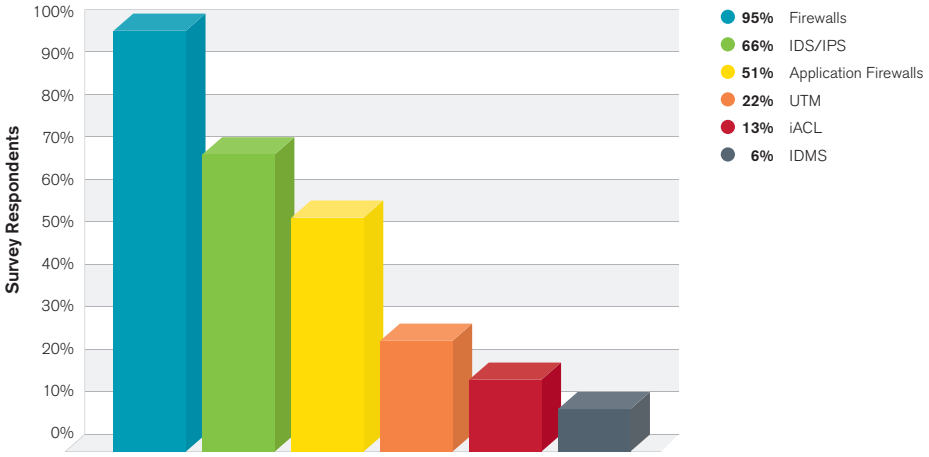

Figure 69 *Source: Arbor Networks, Inc.*

Over 70 percent of respondents reported observing DDoS attacks in the data center this year, up dramatically from under half last year (Figure 70). This illustrates that data centers are magnets for DDoS activity.

DDoS Attacks in the Data Center

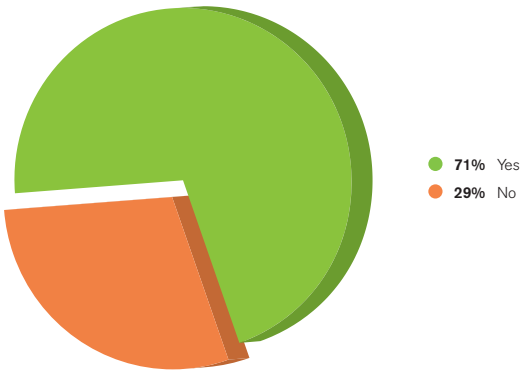

Figure 70 *Source: Arbor Networks, Inc.*

Over one-third of respondents experienced attacks that exceeded the total bandwidth available to the data center (Figure 71). This is nearly double the proportion that reported this last year, demonstrating the increased size of DDoS attacks seen during this survey period.

Attacks Exceeding Total Data Center Bandwidth

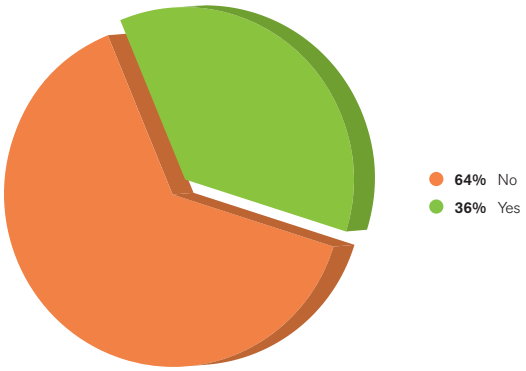

Figure 71 *Source: Arbor Networks, Inc.*

While data center infrastructure continues to be heavily targeted, the proportion of respondents who saw attacks against data center customers declined this year—from over three-quarters to slightly over half (Figure 72).

Targets of DDoS Attacks in the Data Center

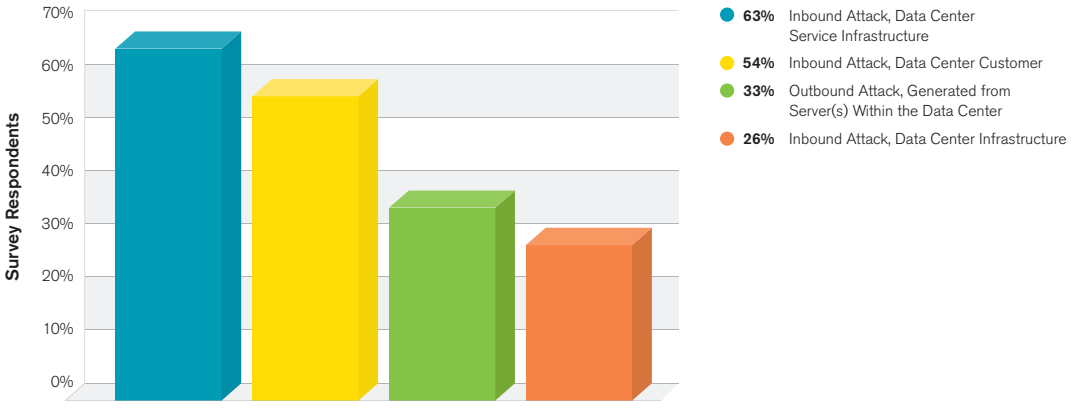

Figure 72 *Source: Arbor Networks, Inc.*

For data center operators who reported being the victims of a DDoS attack, the observed frequency of the attacks increased over last year's survey (Figure 73). Just under three-quarters of respondents experienced between one and 10 attacks per month. This is a similar result to last year. However, more of the respondents witnessed a very high number of attacks per month. For instance, for the first time this year, 9 percent saw over 100 attacks per month.

Frequency of DDoS Attacks in the Data Center

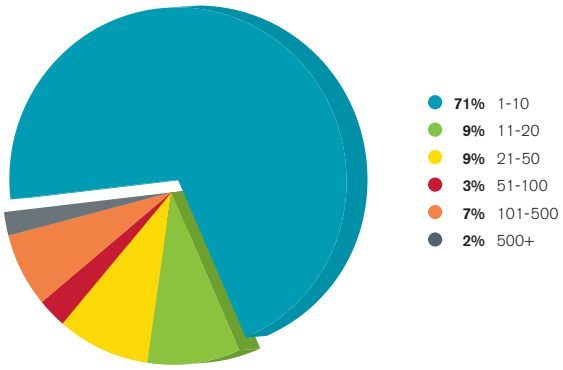

Figure 73 *Source: Arbor Networks, Inc.*

About 81 percent of data center operators reported operational expenses as a business impact due to DDoS attacks, compared to 90 percent last year (Figure 74).

Business Impact of DDoS Attacks in the Data Center

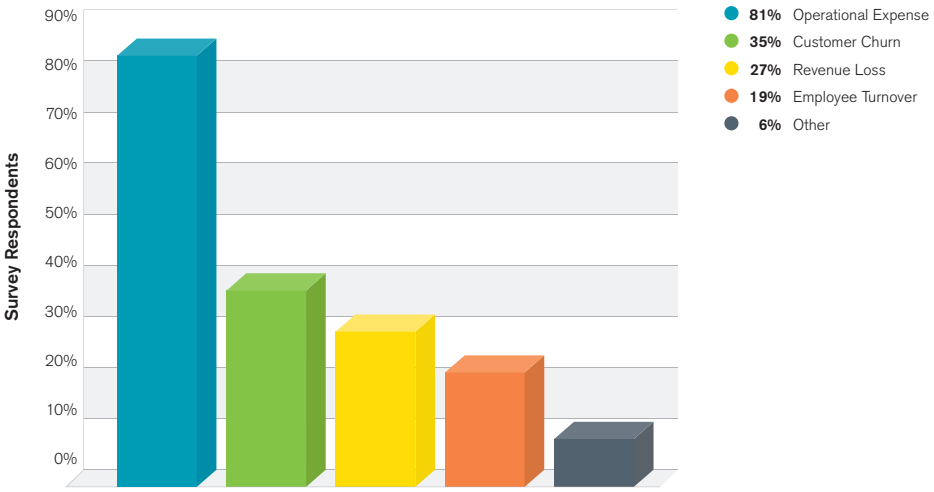

Figure 74 *Source: Arbor Networks, Inc.*

Similar to last year, customer churn was reported by approximately one-third of operators as a consequence of attacks. Customer confidence in the availability of data center services can be shaken should services become unavailable. This is especially true if a customer is not targeted directly and experiences an outage due to collateral damage from attacks targeting other data center customers or shared infrastructure. Finally, just over one-quarter of operators reported revenue loss due to DDoS attacks, down slightly from last year.

DDoS attacks can negatively impact firewalls and IPS devices due to state exhaustion. Similar to firewalls and IPS devices, load balancers also maintain session state and may be adversely impacted by a DDoS attack. More than 25 percent of respondents indicated that a DDoS attack impacted their load balancers during the survey period (Figure 75). This is a slight decline from 2012, when 29 percent indicated that attacks impacted their load balancers. This may be due to a change in the attack vectors used by attackers or to improved load-balancer stability when under attack conditions.

Load Balancers Affected by Attacks

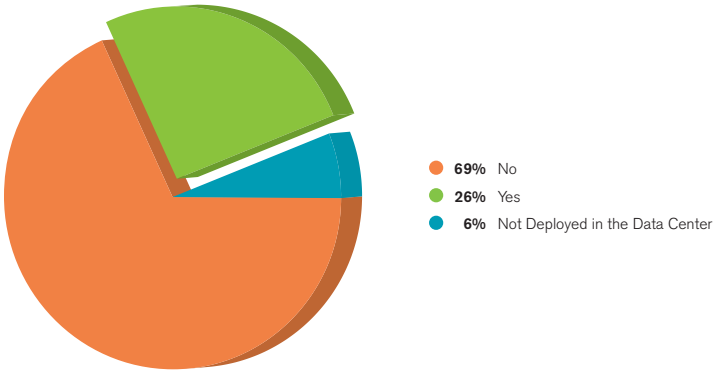

Figure 75 *Source: Arbor Networks, Inc.*

Data center operators use a wide variety of DDoS prevention/mitigation techniques (Figure 76). Looking at the results from this year's survey compared to last, the percentage of respondents using the majority of the DDoS protection mechanisms has decreased. Where this reduction is most apparent is in the use of Unicast Reverse-Path Forwarding (uRPF), FlowSpec on gateway routers and source-based remote triggered blackhole (sRTBH)—each of which has seen the proportion of respondents using the mechanism reduced by approximately half. The only mechanism that has seen a significant increase is IPS/IDS.

Overall, the continued use of firewalls and IDS/IPS devices to deal with DDoS attacks is very concerning. There are significant risks involved in relying on firewalls and IPS for DDoS protection. Although these devices can deal with some kinds of DDoS attacks, they are primarily designed to ensure confidentiality and integrity, rather than service availability.

Security Measures Used to Defend Against DDoS Attacks

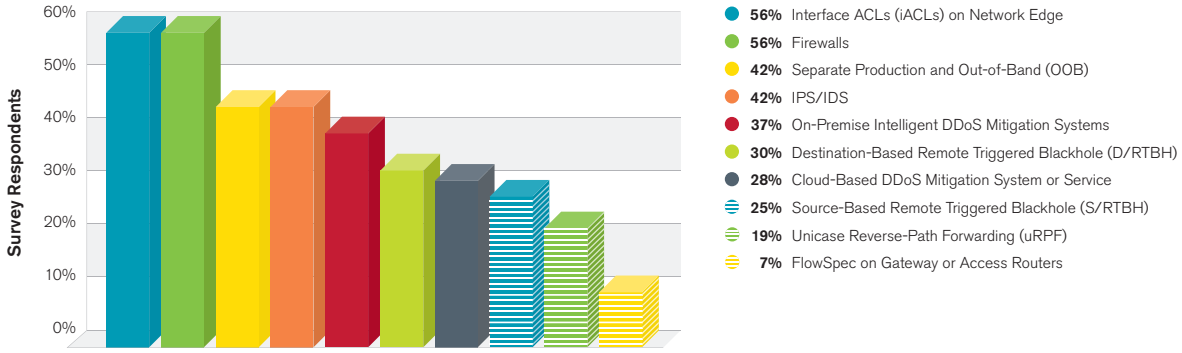

Figure 76 *Source: Arbor Networks, Inc.*

It is worth noting that 42 percent of respondents indicated that their firewalls or IDS/IPS systems were compromised by a DDoS attack during the survey period (Figure 77). Last year 35 percent experienced this issue, so there has been some increase in the impact to firewalls or IDS/IPS over the past year.

Firewalls and IPS Affected by DDoS Attacks

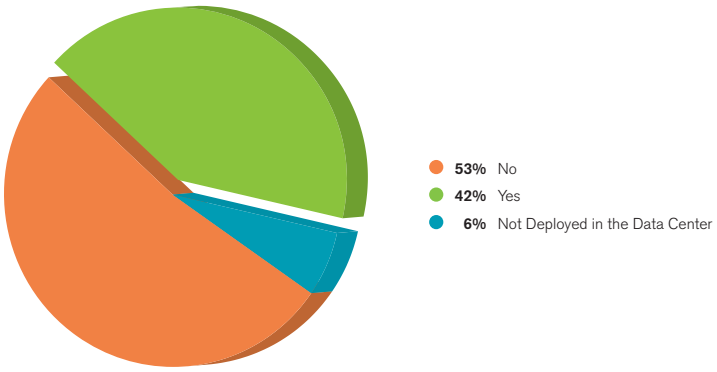

Figure 77 *Source: Arbor Networks, Inc.*

Looking at the provision of DDoS protection services to data center customers (Figure 78), around 40 percent of operators currently offer this (either bundled or as an additional cost option), with nearly one-third planning to do so in the future. This latter statistic should drive up the use of IDMS, as these systems are an intrinsic part of a DDoS protection service.

Managed DDoS Services Offered

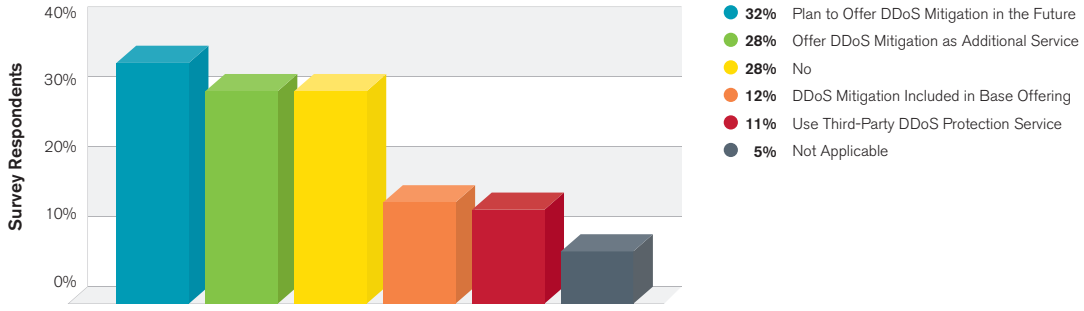

Figure 78 *Source: Arbor Networks, Inc.*

Lastly, about 60 percent of respondents indicated that they monitor either intra-data center traffic or outbound traffic for signs of compromised devices. This is a positive trend as last year only half indicated that they monitor such traffic. Perhaps lessons have been learned from the Operation Ababil attacks against American financial institutions in late 2012 and 2013, which used compromised servers to launch DDoS attacks from data centers.

Mobile/Wireless Networks

This fast-paced and extremely competitive industry continues to struggle with constant pressure to increase network speed, capacity and reach. Operators are doing a great job meeting these primary demands, but still have visibility limitations and a reactive stance on subscriber security.

With the increased worldwide dependence on wireless networks, it is no surprise that 42 percent of survey respondents operate mobile networks, up incrementally from 32 percent last year and 25 percent in 2011. The number of subscribers on respondent networks is impressive and underscores the importance of the availability of these networks (Figure 79). Mobile infrastructure long ago transitioned from being a luxury to a necessity. In fact, over 60 percent of respondents now have more than one million subscribers, and nearly one-fifth report networks with more than 25 million subscribers.

Mobile Network Subscribers

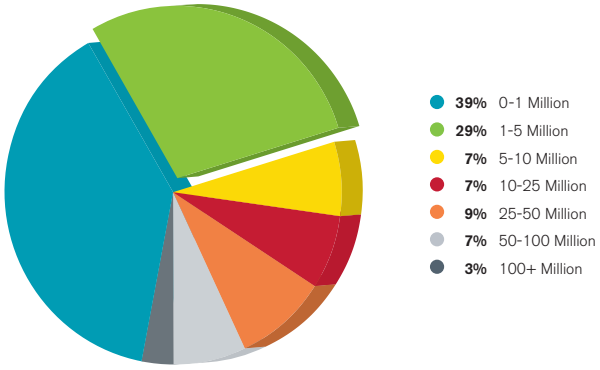

Figure 79 *Source: Arbor Networks, Inc.*

As expected, most respondents operate traditional GSM 2G and 3G networks. However, LTE deployments continue to increase, with over 63 percent indicating that they have LTE deployed, versus only 53 percent in 2012 and approximately 29 percent in 2011 (Figure 80). Almost a half of respondents already offer LTE services to their customers, with a further 14 percent planning to offer them in 2014 (Figure 81) illustrating the continued rapid adoption of this technology.

Mobile Technologies Deployed

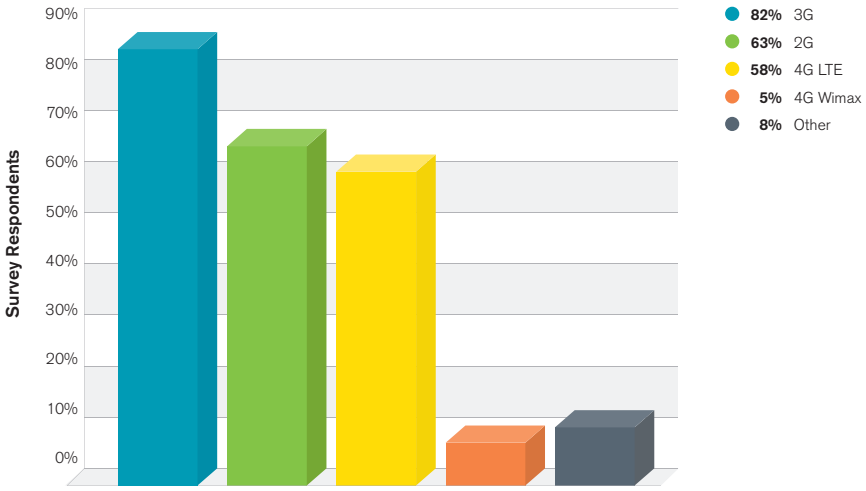

Figure 80 *Source: Arbor Networks, Inc.*

WiMax deployments have plateaued at around 5 percent over the last three years, showing that LTE is the clear winner in 4G technology. A few operators this year indicated they also offer WiFi, fixed microwave and other services.

Deployment Timeline for 4G Service

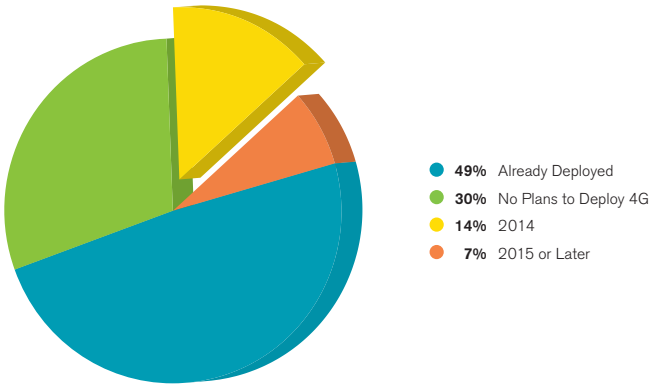

Figure 81 *Source: Arbor Networks, Inc.*

Only 46 percent of respondents indicated that they have NAT in place, down from 72 percent last year (Figure 82). This is surprising given the amount of IPv4 address space required for networks to operate without NAT. Also, providing mobile subscribers with public Internet addresses increases the risk of unsolicited traffic-consuming capacity—affecting bills, etc.

Mobile NAT Deployment

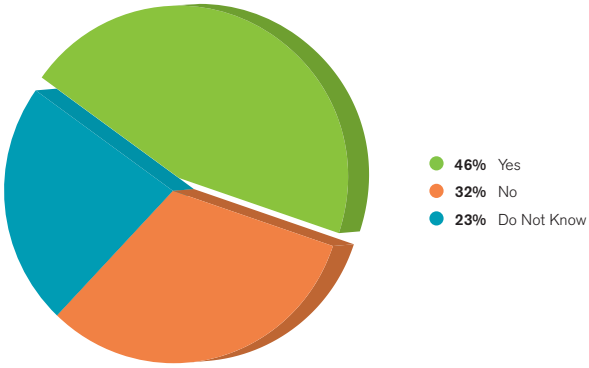

Figure 82 *Source: Arbor Networks, Inc.*

In the 2012 survey, nearly 18 percent of respondents indicated they were using IPv6 either for subscriber or mobile infrastructure addressing. In this year's survey, the number dropped to only 8 percent (Figure 83). Also last year, 30 percent indicated that they were planning to implement IPv6 over the next year. The number that now says they're planning IPv6 deployments also dropped to only 25 percent this year. This downward trend may indicate a broader acceptance of NAT as a longer-term solution within mobile networks, but the decrease in respondents using NAT (mentioned above) does seem contradictory here. The reduction in focus on IPv6 does, however, seems consistent with other areas of the survey.

Subscriber IPv6 Deployment

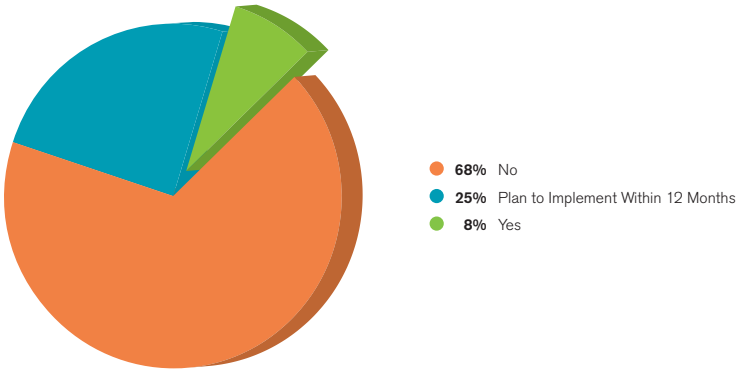

Figure 83 *Source: Arbor Networks, Inc.*

Over 20 percent of respondents indicated that they have suffered a customer-visible outage due to a security incident, down slightly from about one-third last year. While this is a positive trend, 25 percent do not know if they had outages caused by security incidents, which shows a continued lack of visibility and detection capabilities on mobile networks.

Over 63 percent of respondents do not know what proportion of subscriber devices on their networks are compromised and are participating in botnets or other malicious activities. This is an increase over last year's 57 percent, and is also indicative of limited subscriber threat detection capabilities.

Mobile malware is growing at an astonishing rate. Android-based mobile malware and high-risk apps have reached the one million mark, according to a recent study from a leading AV vendor (Source: Trend Micro). As LTE adoption increases, the potential for compromised mobile devices to consume significant amounts of capacity—impacting service availability and subscriber quality-of-experience—is a key concern.

Misbehaving user applications can also pose a real problem for mobile operators (Figure 84). This problem is likely to become more significant as operators increasingly use LTE/3G services for wire-line replacement. A widely deployed misbehaving user application can present a significant availability threat, similar in some ways to a DDoS attack. Anecdotally, multiple operators have reported significant outages or performance issues caused by non-malicious but misbehaving user applications. Our respondents corroborate this, with over one-third experiencing this issue.

Impact of Poorly Written Applications

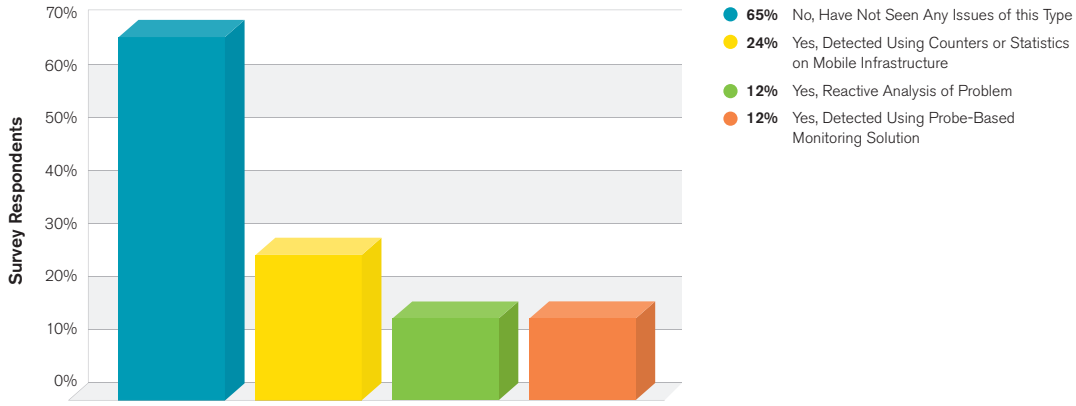

Figure 84 *Source: Arbor Networks, Inc.*

On an encouraging note, it appears that the proportion of respondents taking a reactionary approach to dealing with these issues has fallen dramatically, from nearly one-third last year to 12 percent this year. Quality of experience is a KPI for most mobile operators, and these results seem to show an increased interest in proactively monitoring network activity to meet that KPI.

In a huge improvement this year, only 35 percent of respondents do not have visibility into the traffic on their mobile/evolved packet cores (Figure 85), compared to 60 percent last year. About half now have visibility into the user/data-plane traffic, up from one-third last year. Finally, 57 percent now have visibility into the control-plane traffic, over double last year's 27 percent.

Visibility in Packet Core

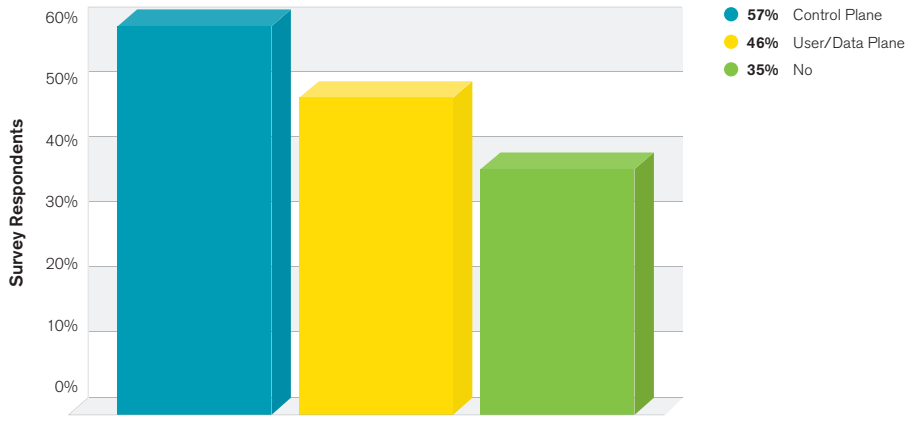

Figure 85 *Source: Arbor Networks, Inc.*

Of those respondents who have visibility into traffic on their mobile packet core, the majority use counters and statistics available directly from the mobile infrastructure itself, while 40 percent of operators use existing mobile vendor-supplied probe-based monitoring solutions (Figure 86). The remainder use third-party probes or a flow-monitoring device to visualize traffic. These latter two methods have seen an increase in adoption of about 50 percent during this survey period.

Visibility Solutions Deployed

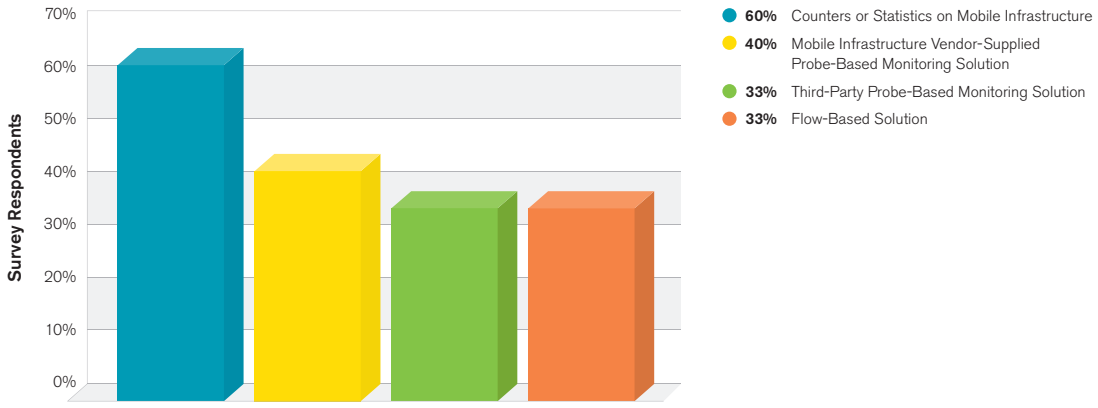

Figure 86 *Source: Arbor Networks, Inc.*

Mobile operators utilize a wide variety of tools and techniques to protect their infrastructure against availability threats (Figure 87). As with last year, iACLs and NAT/PAT technology are still the most common protective measures, although there has been a significant decrease in the proportion of respondents using iACLs (down from 69 percent to 47 percent). Interestingly, 62 percent of respondents indicated they use NAT/PAT as a security solution, compared to only 45 percent using NAT/PAT for subscriber address translation. This inconsistency may indicate that respondents are thinking about NAT/PAT more as a security solution than a mechanism for scaling their available public address space.

While the use of IDMS remained fairly steady, there was a large increase in the proportion of respondents using GTP firewalls, up from 19 percent to 32 percent. There was also a significant rise in the proportion using security gateways (SEG) between the radio access network (RAN) and the mobile packet core (MPC), up from 6 percent to 18 percent.

Security Measures Used to Defend Against DDoS Attacks

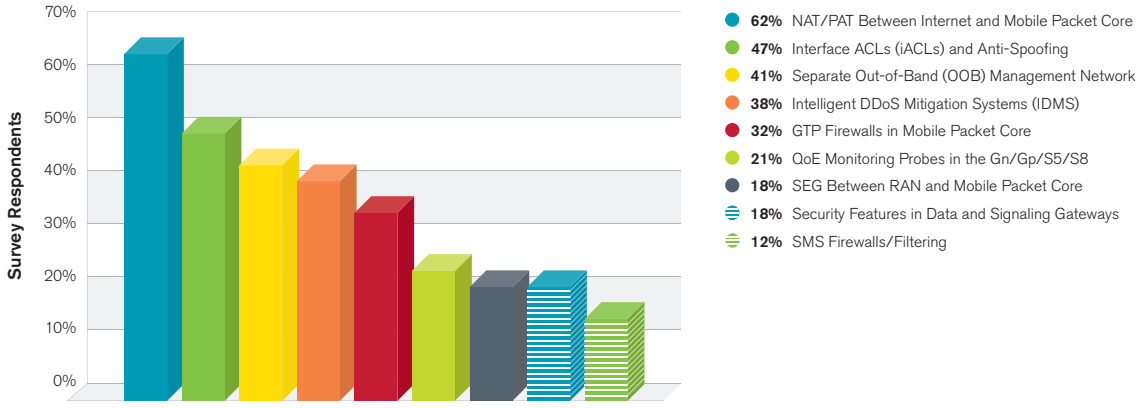

Figure 87 *Source: Arbor Networks, Inc.*

Approximately 25 percent of respondents have seen DDoS attacks targeting their mobile users, RAN, back-haul or packet core, while nearly 46 percent have not seen any attacks (Figure 88). Roughly 29 percent do not know if these attacks are occurring due to a lack of visibility. While reported attacks are slightly down from last year, the number of respondents reporting a lack of visibility has correspondingly increased. This may indicate that although mobile operators have improved their visibility into the traffic on their packet cores, a significant number do not have threat detection capabilities in place.

DDoS Attacks on Mobile Network

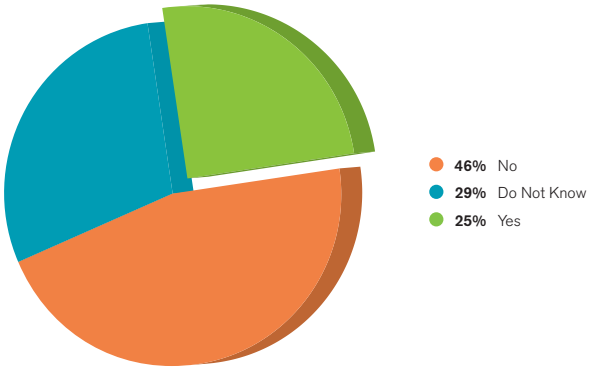

Figure 88 *Source: Arbor Networks, Inc.*

The vast majority of respondents who did see DDoS attacks on their mobile users, RAN, back-haul or packet core reported between one and 10 events per month. This is in line with last year's results. However, some network operators reported seeing 500 or more attacks in a single month (Figure 89).

Frequency of DDoS Attacks on Mobile Network

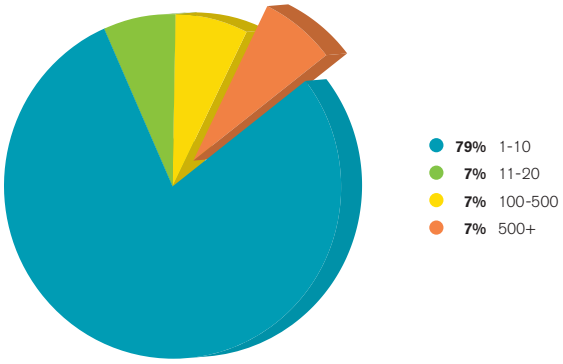

Figure 89 *Source: Arbor Networks, Inc.*

In terms of the targets of these attacks, subscriber handsets, computers and tablets are the most commonly affected devices. Additional targets include operator firewalls, data and signaling gateways, and other infrastructure.

Fewer than 13 percent of respondents indicated that they currently mitigate outbound DDoS attacks from subscribers. However, another one-quarter plan to do so in the next year. This shows great progress from last year, when nearly three-quarters indicated no plans in this regard (Figure 90).

Outbound DDoS Attack Mitigation

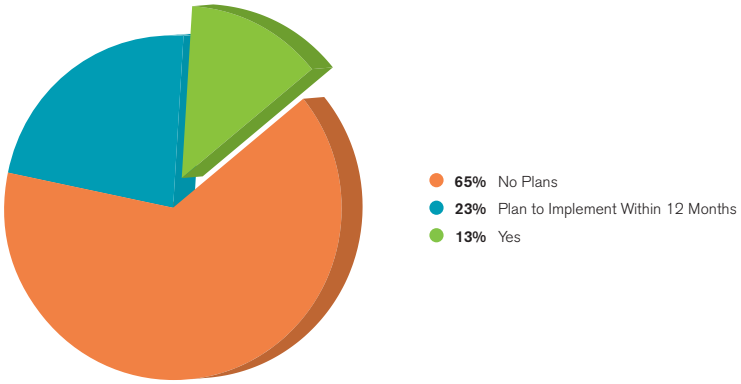

Figure 90 *Source: Arbor Networks, Inc.*

Mobile Internet (Gi) infrastructure visibility remains very similar to last year. About three-quarters of respondents indicated that they have visibility into traffic at Layers 3 and 4, but only 23 percent have Layer 7 visibility and over 20 percent report no visibility at all (Figure 91).

Internet (Gi) Traffic Visibility

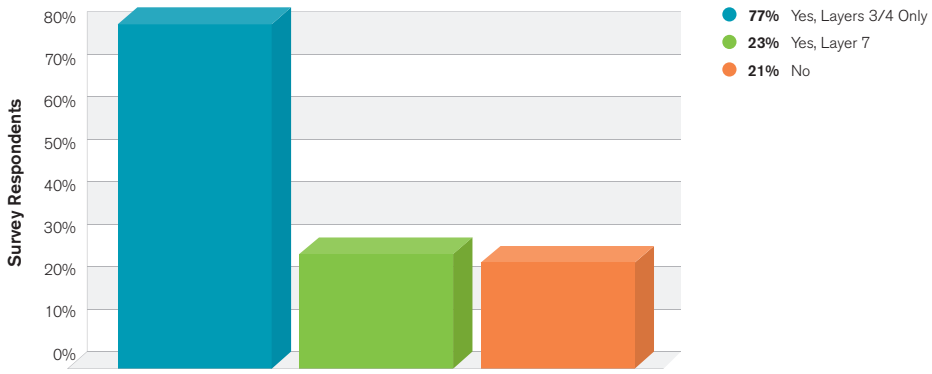

Figure 91 *Source: Arbor Networks, Inc.*

Respondents reported using a variety of solutions to gain visibility into traffic, with infrastructure counters and statistics being the most common mechanism (Figure 92). Flow-based solutions are the second most common mechanism, as solutions developed to operate in generic ISP environments are applicable here.

Visibility of Internet (Gi) Traffic

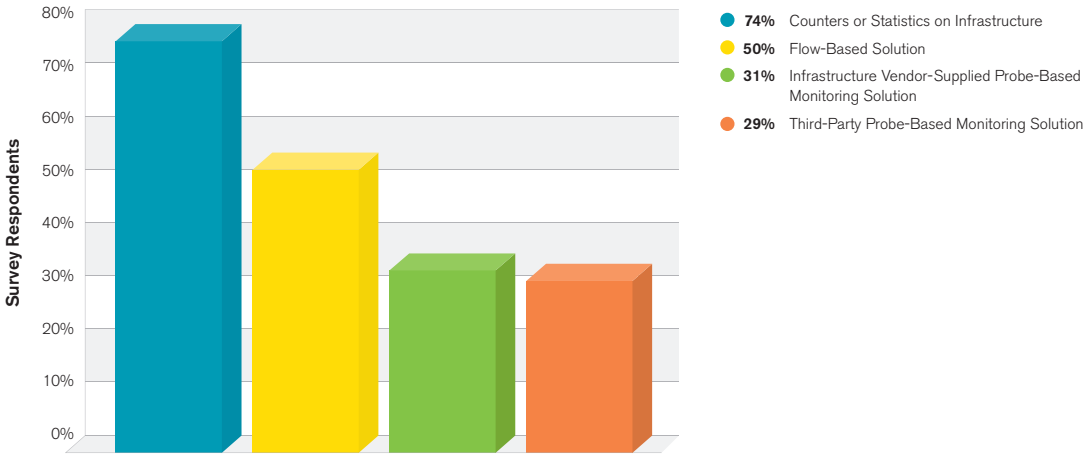

Figure 92 *Source: Arbor Networks, Inc.*

This year over one-quarter of respondents indicated that they have seen DDoS attacks impacting their mobile Internet (Gi) infrastructure. This represents more than double last year's result. Nearly half indicated that they have not seen attacks, and almost one-quarter do not know if attacks are going on (Figure 93). While still high, this latter number is a significant improvement from 45 percent last year. Lack of monitoring and threat detection capabilities still seem to be an issue for a significant minority of mobile operators.

DDoS Attacks on Internet (Gi) Infrastructure

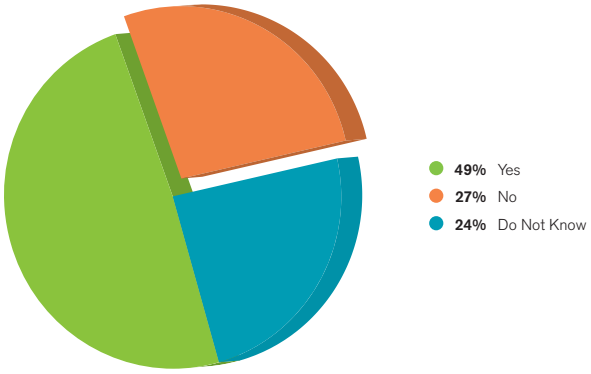

Figure 93 *Source: Arbor Networks, Inc.*

For respondents seeing attacks targeting their Gi infrastructure, 63 percent saw between one and 10 attacks per month (Figure 94).

Frequency of DDoS Attacks on Internet (Gi) Infrastructure

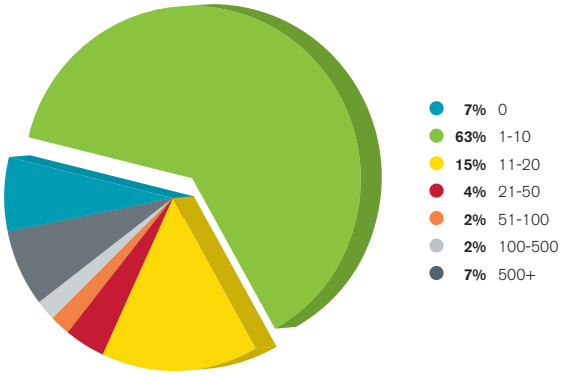

Figure 94 *Source: Arbor Networks, Inc.*

Attack targets were varied this year. DNS servers were once again the most common target, followed closely by routers and switches (link saturation). Other targets included firewalls, gateways and proxies (Figure 95).

Mobile Internet access is continuing to grow strongly. Bandwidth requirements continue to increase as subscribers use their devices for a mixture of personal and business activities, access to video, etc. Perceived quality and availability of services are now of great importance. Mobile operators appear to be improving the visibility they have into their network traffic, but there are still limitations in the threat detection capabilities of some respondents.

Internet (Gi) Resources Affected by DDoS Attacks

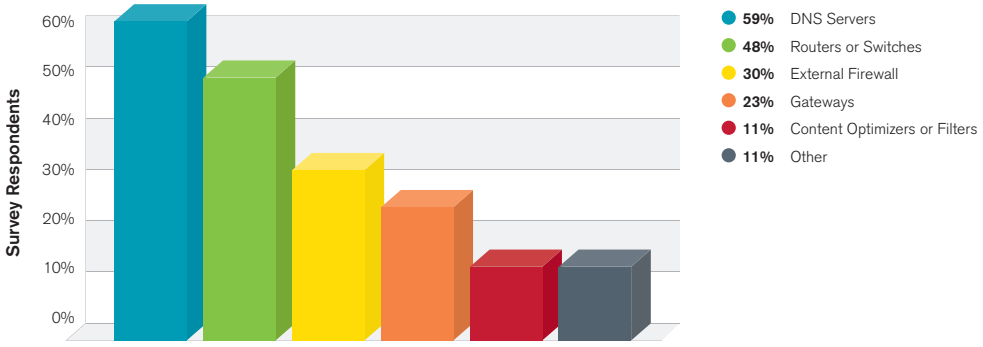

Figure 95 *Source: Arbor Networks, Inc.*

Organizational Security Practices

The ability to respond effectively to a security incident is very important, but this year's survey results show that steps are not always being taken to improve in this area. The proportion of respondents who practice DDoS attack and defense simulations has decreased from 49 percent to 45 percent. The proportion implementing anti-spoofing filters at the edge of their networks has also dropped from 57 percent to 51 percent.

The majority of respondent organizations continue to implement one or more best current practices (BCPs) within their network infrastructure (Figure 96). These BCPs include routing protocol authentication; iACLs to keep undesirable traffic away from network infrastructure devices; and anti-spoofing measures at the edges of their networks. However, the proportion of respondents implementing anti-spoofing filters at the edge of their networks has dropped from 57 percent to 51 percent. While not a significant change, this is movement in the wrong direction—especially given that a lack of these filters makes it easier for attackers to leverage reflection/amplification DDoS techniques. Also falling is the proportion having an out-of-band management network. This represents another important aspect of overall security that all organizations should look to implement.

Infrastructure BCPs Followed

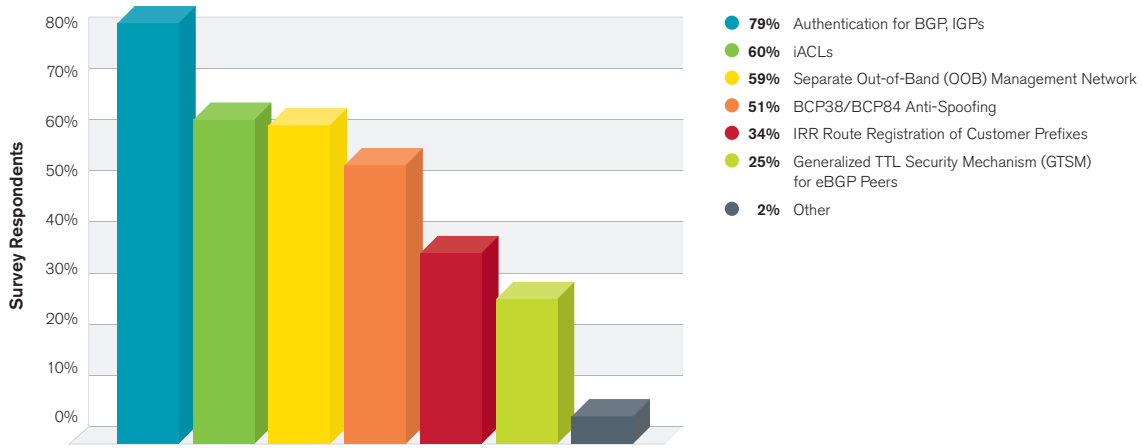

Figure 96 *Source: Arbor Networks, Inc.*

The ability to respond effectively to a security incident is critical so that organizations can minimize the business impact of any attack. The proportion of respondents who practice DDoS attack and defense simulations decreased this year from 49 percent to 45 percent—a relatively small change, undoing some of the gains shown in the last survey.

DDoS Defense Practice

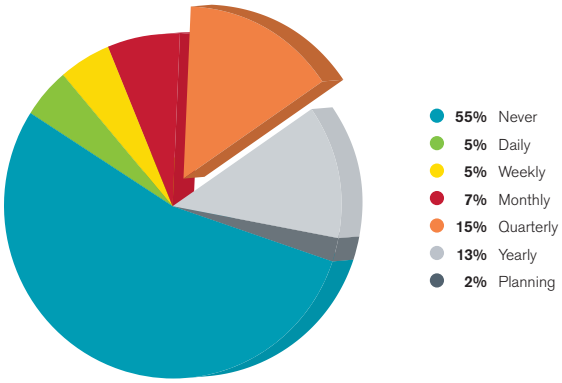

Figure 97 *Source: Arbor Networks, Inc.*

Things improved generally this year in the area of routing security precautions. Eighty-one percent of respondents explicitly filter their customers' route announcements, up moderately from 76 percent last year (and reversing the decline from the previous year).

More than 63 percent explicitly filter inbound routing advertisements from peers and upstream transit providers (Figure 98), up from 55 percent last year (again reversing the reduction from the previous year).

Just as last year, a little over half of respondents now monitor for route hijacking (Figure 99). In 2013, a number of purposeful attacks utilized route hijacking, where a return path for traffic was provided to mask the re-direction. Network operators should be aware of this and implement detection mechanisms accordingly.

BGP Peer Route Filters

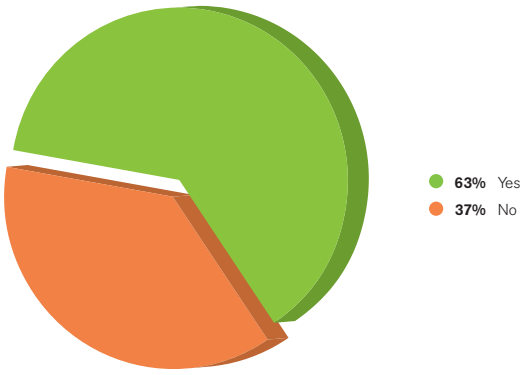

Figure 98 *Source: Arbor Networks, Inc.*

Route Hijack Monitoring

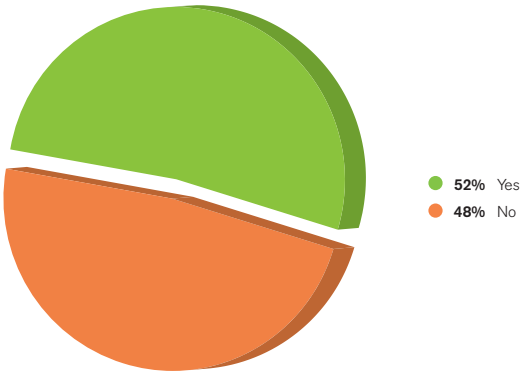

Figure 99 *Source: Arbor Networks, Inc.*

The proportion of respondents who proactively block traffic to known botnet C&C servers, malware drop sites, etc. remained practically the same as last year at 38 percent (Figure 100). The large increase seen from 2011 to 2012 does not appear to have continued.

Participation in closed or vetted global OPSEC groups is down slightly this year, with only 39 percent of respondents active. By contrast, 77 percent indicated that they believe these groups are highly effective in handling OPSEC issues on an inter-organizational basis. Compared to last year's survey, both participation and confidence in these groups are marginally down.

Proactive Known Threat Blocking

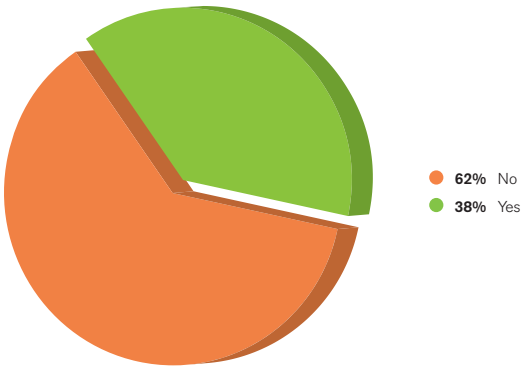

Figure 100 *Source: Arbor Networks, Inc.*

The challenges preventing full participation in closed/vetted global OPSEC groups persist (Figure 101). Lack of time or resources is the most frequently cited challenge, along with lack of management support, legal concerns and unclear benefits. This has been consistent over the last few years.

Challenges Preventing Participation in OPSEC Community

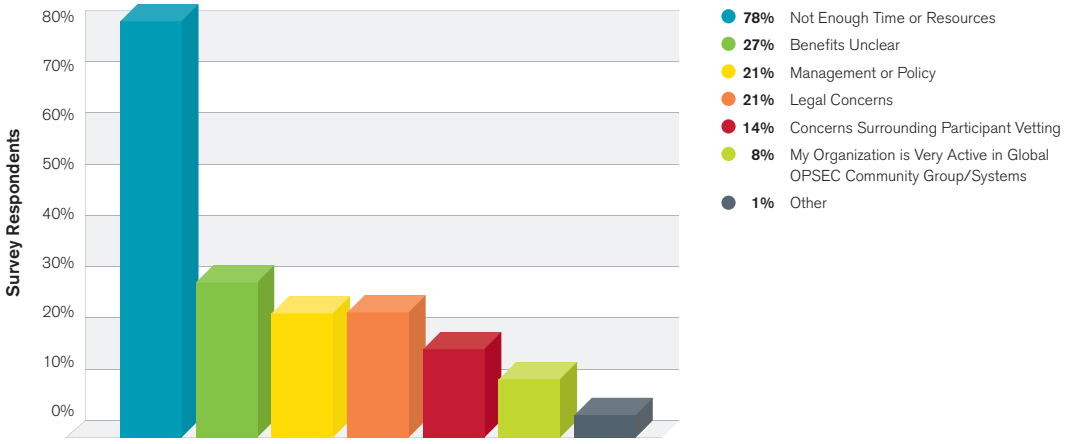

Figure 101 *Source: Arbor Networks, Inc.*

Nearly 80 percent of respondents indicated that their OPSEC team maintains current contact information for key OPSEC resources and/or other empowered groups within their peer, transit provider and customer organizations (Figure 102). This represents a slight decrease over last year. Maintaining up-to-date contact information for OPSEC teams is of paramount importance—especially with DDoS attack sizes growing rapidly, as this makes it more likely that multiple organizations will need to be involved in any mitigation effort.

Current Contact Information Maintained

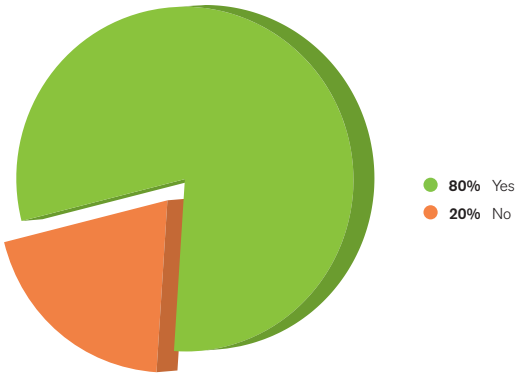

Figure 102 *Source: Arbor Networks, Inc.*

Conclusions

Arbor Networks' ninth annual *Worldwide Infrastructure Security Report* highlights some significant trends. This year, with a record number of respondents, the report has identified some broad trends in the threats facing organizations, as well as some more specific changes. In many cases, the data is consistent with previous surveys, but there are some key areas of change.

Higher Magnitude and Application-Layer DDoS Attacks

The previous largest attack was 100Gbps, as reported in our 2010 survey. This year's respondents reported attacks ranging from 309Gbps at the top end through 200Gbps, 191Gbps, 152Gbps, 130Gbps and 100Gbps. Arbor is also aware that some respondents saw multiple events above the 100Gbps level, but only reported the largest of these. This is consistent with Arbor's ATLAS data, which shows that there were more than eight times the number of attacks over 20Gbps in 2013, as compared to 2012. Through 2013, attackers do seem to have been resorting to large, volumetric DDoS attacks to achieve their goals.

Application-layer attacks have been seen by almost all respondents. This is no surprise given that application-layer attacks have been trending up for the last couple of years. However, there have been some changes in the attack vectors being used, with HTTP POST floods becoming much more common. In terms of the services being targeted, HTTP is still number one, but we have seen continued strong growth in application-layer attacks targeting encrypted Web services (HTTPS)—up 17 percent over last year. Interestingly, one-third of respondents are reporting attacks targeting an encrypted service at the application layer, rather than the protocol or transport layer. This may be attributable to the Operation Ababil attacks that plagued U.S. financial institutions for the majority of the survey period. Ababil routinely employed sophisticated multi-vector, multi-stage attacks with encrypted traffic.

DDoS is definitely top-of-mind for the customers of our survey respondents. Over 60 percent of respondents are seeing increased demand for DDoS detection and mitigation services from their customers. DDoS remains the top experienced threat and concern for network operators.

Corporate Network Threats

Advanced persistent threats (APT) are increasingly common, with nearly one-third of respondents experiencing them on their networks during the survey period. It is not surprising to see this trend continue from the previous year considering the renewed focus on these types of threats from security vendors and network operators alike.

Another key area of discussion in many organizations is BYOD/mobility. Nearly three-quarters of respondents now allow employees to use their own devices on internal networks, but more than half of them do not have any solution deployed to identify or monitor these devices. This represents a serious hole in the security of many organizations.

Data Centers

Data centers have become a magnet for DDoS activity, given that they represent a target-rich environment. This year nearly 9 percent of data center respondents reported seeing more than 100 attacks per month. More generally, over 71 percent of data centers operators reported DDoS attacks this year—up dramatically from less than half last year.

Even more concerning, over one-third of data center operators experienced attacks that exceeded total available Internet connectivity—nearly double last year. Shared infrastructure brings an inherent risk of collateral damage if not properly protected.

DNS

Slightly more than one-third of DNS operators have experienced customer-impacting DDoS attacks on their DNS infrastructure during the survey period—a modest increase from last year.

More than one-quarter of respondents indicated that there is no security group within their organizations with formal responsibility for DNS security—up from 19 percent last year. This is surprising given the number of high-profile DNS reflection/amplification attacks seen during the survey period, which would have been expected to renew focus in this area. The most notorious of these attacks targeted Spamhaus and tipped the scales at over 300Gbps. It is not surprising, however, that many attackers took note and followed suit with their own DNS reflection/amplification campaigns.

Organizations need to implement best practices and adequately secure and monitor their DNS infrastructure to protect their own customers and the broader Internet community.

Mobile

As expected, most respondents operate traditional GSM 2G and 3G networks. However, LTE deployments continue to increase, with 63 percent indicating that they have LTE deployed, versus only 53 percent in 2012 and approximately 29 percent in 2011. Almost a half of respondents already offer LTE services to their customers, with a further 14 percent planning to offer them in 2014 illustrating the continued rapid adoption of this technology. The rollout of higher speed data services combined with increasing security issues is clearly focusing some mobile operators on the need for better monitoring and threat detection solutions. Over one-quarter, according to Figure 93 of respondents indicated they have seen DDoS attacks impacting their mobile Internet (Gi) infrastructure—more than double last year. And, over 20 percent of respondents indicated that they have suffered a customer-visible outage due to a security incident.

IPv6

The volume of IPv6 traffic on the Internet appears to be growing very strongly, as shown by both survey responses and ATLAS data. However, more broadly there appears to have been less focus on IPv6 during this survey period, with fewer than 10% of respondents, according to Figure 51 of respondents expecting IPv6 traffic to more than double next year. This seems a bit pessimistic in light of evidence to the contrary over the past year.

About the Authors

Darren Anstee, Solutions Architect for EMEA, Arbor Networks

danstee@arbor.net

Darren Anstee is the Director of Solutions Architects for Arbor Networks, based in the UK. Anstee has over 18 years of experience in the pre-sales, consultancy and support aspects of telecom and security solutions. Currently in his eleventh year at Arbor, Anstee is involved in both research and operational activities at Arbor in relation to its network threat detection, mitigation and traffic visibility solutions. Prior to joining Arbor, Anstee spent eight years working in both pre- and post-sales for core routing and switching product vendors.

Andrew Cockburn, Consulting Engineer, Carrier Group North America, Arbor Networks

acockburn@arbor.net

With over 25 years in the IT industry, Andrew Cockburn has broad experience in roles ranging from software design and development, pre-sales and consulting, to engagement and project management in various industry sectors including online transaction processing, billing and mediation, Layer 7 parser development and other security products. Previously working for companies such as Honeywell, AT&T GIS, IBM and Narus, he is currently in his second year at Arbor Networks, and specializes in pre- and post-sales focused on anti-DDoS solutions for Tier 1 and 2 carriers in North America, where he strives to educate potential buyers in industry trends as well as propose creative ways to solve their problems.

Gary Sockrider, Solutions Architect for the Americas, Arbor Networks

gsockrider@arbor.net

Gary Sockrider is the Arbor Networks Solutions Architect for the Americas. He seeks to understand and convey the constantly evolving threat landscape as well as the techniques and solutions that address it. He works across the organization to ensure customers experience an optimal deployment and their needs and interests are best represented.

Sockrider is an industry veteran with over 20 years of broad technology experience ranging from routing and switching to network security, data center, and collaboration. He has diverse experience in multiple roles including support, IT, security SME and product management. Prior to joining Arbor Networks, Sockrider spent 12 years at Cisco Systems and held previous positions with Avaya and Cable & Wireless.

CONTRIBUTOR

Carlos Morales, Vice President, Global Sales Engineering and Consulting, Arbor Networks

cmorales@arbor.net

Carlos Morales is responsible for pre-sales technical support, design, consulting and implementation services for Arbor customers and partners worldwide. He is also responsible for sales approvals, sales processing, maintenance contracts, forecasting, data analysis and reporting for Arbor. Morales works closely with Arbor's customers and strategic and integration partners to ensure ongoing product interoperability and to set the direction for new product features. He has more than 15 years of experience implementing security, routing and access solutions in service provider, cloud and enterprise networks. Morales' background includes management positions at Nortel Networks, where he served as the director of systems engineering for Nortel's access products. Formerly, he was systems engineering director for Tiburon Networks and held systems engineering roles at Shiva Corporation, Crescent Networks and Hayes Microcomputer.

GLOSSARY

Glossary

A

ACL Access Control List
APT Advanced Persistent Threat
ASERT Arbor Security Engineering & Response Team
ATLAS Active Threat Level Analysis System
AV Anti-Virus

B

BCP Best Current Practice
BGP Border Gateway Protocol
BYOD Bring Your Own Device

C

C&C Command-and-Control
CGN Carrier Grade NAT

D

DDoS Distributed Denial of Service
DNS Domain Name System
DNSSEC Domain Name System Security Extensions
D-RTBH Destination-based Remotely Triggered Blackholing
S-RTBH Source-based Remotely Triggered Blackholing

E

EDNS0 Extension Mechanisms for DNS

G

Gbps Gigabits-per-second
Gi Global Internet

H

HOIC High Orbit Ion Cannon
HTTP Hypertext Transfer Protocol
HTTP/S HTTP Secure

I

IAAS Infrastructure As A Service
iACL Infrastructure ACL
ICMP Internet Control Message Protocol
IDMS Intelligent DDoS Mitigation System
IDS Intrusion Detection System
IPS Intrusion Prevention System
IPv4 Internet Protocol version 4
IPv6 Internet Protocol version 6

K

KPI Key Performance Indicator

L

LOIC Low Orbit Ion Canon
LTE Long Term Evolution

M

Mbps Megabits-per-second
MDM Mobile Device Management
MPC Mobile Packet Core

N

NAT Network Address Translation
NMS Network Management System

Glossary (continued)

O

OPSEC Operational Security
OTT Over the Top

P

PAT Port Address Translation

Q

QoE Quality of Experience

R

RAN Radio Access Network

S

SEG Security Gateways
SIEM Security Information Event Management
SLA Service Level Agreement
SMTP Simple Mail Transfer Protocol
SNMP Simple Network Management Protocol
SOC Security Operations Center
SPF Sender Policy Framework
S/RTBH Source-based Remotely Triggered Blackholing
SYN Synchronize

T

TCP Transmission Control Protocol
Tbps Terabits per second

U

UDP User Datagram Protocol
uRPF Unicast Reverse Path Forwarding

V

VoIP Voice over Internet Protocol
VPN Virtual Private Network

W

WAN Wide Area Network
WiMAX Worldwide Interoperability for Microwave Access

Corporate Headquarters

76 Blanchard Road
Burlington, MA 01803 USA

Toll Free USA +1 866 212 7267
T +1 781 362 4300

North America Sales

Toll Free +1 855 773 9200

Europe

T +44 207 127 8147

Asia Pacific

T +65 68096226

www.arbornetworks.com

ARBOR® NETWORKS

SR/WISR2013/EN/0114-LETTER