SPECIAL REPORT

Worldwide Infrastructure Security Report

Volume XI

ARBOR® NETWORKS

The Security Division of NETSCOUT

About Arbor Networks

Arbor Networks, the cyber security division of NETSCOUT, 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 risks 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.

CONTENTS

Attack Sizes 27

Attack Durations 29

Targeted Services 30

Source and Target Countries 31

Reflection Amplification Update 32

Type, Frequency and Motivation of DDoS Attacks 36

ASERT DD4BC: Summary 41

DDoS Threat Mitigation 44

Corporate Network Security 47

Data Center Operators 57

Mobile Network Operators 63

Organizational Security Practices 70

Service Provider IPv6 73

3. Enterprise 77

Enterprise Network Security 78

ASERT Malware Trends 90

intro

SECTION 1

1

INTRODUCTION

OVERVIEW

Welcome to our 11th annual *Worldwide Infrastructure Security Report* (WISR). The data within this document is based on the collective experiences, observations and concerns of the global operational security community. Arbor Networks has collected this data through a survey conducted in October 2015.

For the past 11 years, Arbor has produced the WISR — collecting detailed information on the threats and concerns of a variety of network operators, collating this data and then presenting it as a free-to-access repository of information.

This document is intended to highlight the key trends in the threats and concerns facing today's organizations, and the ways in which these organizations are mitigating those threats.

Since its inception, the WISR has been based upon survey data collected from those who are directly involved in day-to-day operational security, and this is our continued approach. The WISR has changed immeasurably in terms of its scope and scale over 11 years, but the core goal is still to provide real insight into infrastructure security from an operational perspective.

SURVEY METHODOLOGY

The 2016 *Worldwide Infrastructure Security Report* (WISR) is based on a survey comprised of 172 free-form and multiple choice questions, a slight decrease from 182 last year.

However, the small reduction in the number of questions belies the fact that this year's survey has specific logic flows that enable service providers and enterprise/government/education respondents to see a different set of questions depending upon their self-classification. This change has proved necessary as the number of non-service-provider respondents continues to grow. The questions we need to ask diverge depending upon the nature of the respondent, and we are addressing feedback from last year's respondents to reduce the number of irrelevant questions asked.

As in previous years, we have modified the survey questions to reflect changes in the threat landscape and to address responses from last year's survey. The current survey is divided into sections that address specific topics such as DDoS attacks, corporate network security, IPv6, data centers, mobile networking, etc. Each section establishes the observations and concerns of respondents and, where appropriate, the mechanisms put in place to manage their concerns.

Arbor distributes the WISR survey by specifically targeting individuals within the operational security community to get as accurate a picture as possible. We saw a significant increase in the number of respondents to this year's survey, up to 354 from 287 last year, which in turn was up from 221 in 2013. Survey participation continues to grow strongly, making the data presented within this report an even more valuable repository of information on the realities of operational security.

DEMOGRAPHICS OF SURVEY RESPONDENTS

The number of respondents to the WISR survey continues to grow year-over-year. The majority of responses (52 percent) came from service provider organizations. For the first time, nearly half came from other types of organizations representing a more diverse view of different types of networks. Enterprise organizations are very well represented by 38 percent of total respondents. The remaining respondents represent government (6 percent) and education (4 percent).

The United States and Canada represent the lead region for participation at 38 percent of respondents, further ahead of Western, Central and Eastern Europe compared to last year. This year, 95 percent of respondents report they have dedicated security resources. This represents a slight increase over last year's 94 percent, indicating continued focus on security across all types of network operators.

As in previous years, the majority of responses (52 percent) came from service provider organizations. However, for the first time in the 11-year history of this survey, nearly half came from other types of organizations. Enterprise organizations are very well represented by 38 percent of total respondents. The remaining respondents represent government (6 percent) and education (4 percent).

Also for the first time this year, we collected more details on the verticals from which our respondents bring their unique perspectives. Among service providers, well over half represent Tier 1, Tier 2/3 and regional ISPs offering multiple services, while the next largest group come from hosting and data center operators (Figure 1).

Service Provider Type

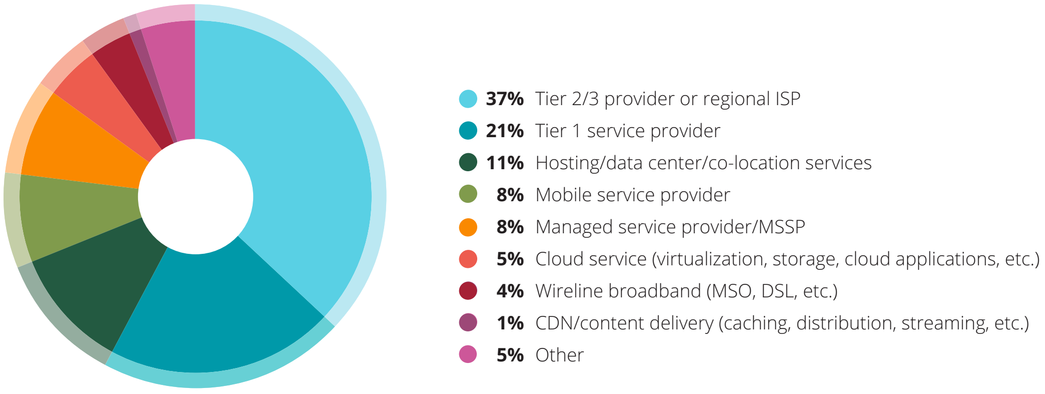


Figure 1 *Source: Arbor Networks, Inc.*

Among enterprise, government and education respondents, it's no surprise that the greatest number of responses come from the technology vertical, followed closely by banking/finance and government (Figure 2).

Enterprise Verticals

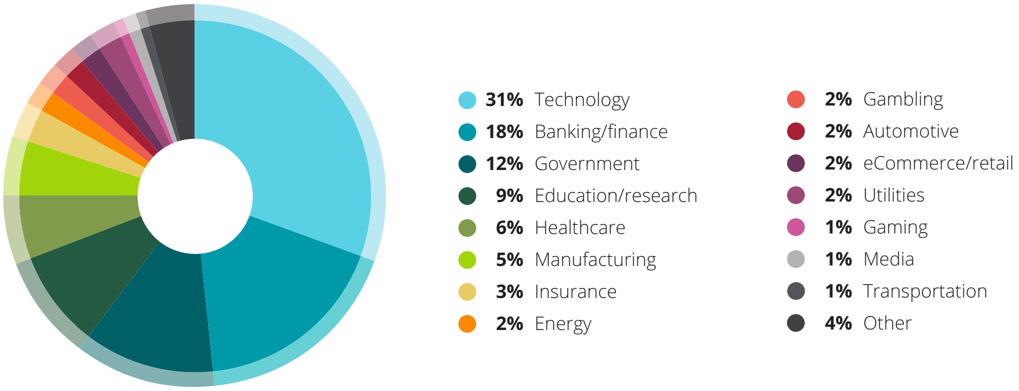


Figure 2 *Source: Arbor Networks, Inc.*

This year, just over two-thirds of respondents are security, network or operations professionals (Figure 3) — down slightly from 71 percent last year. The remainder are managers, directors or executives focused within the security and networking space.

Respondent's Role in Organization

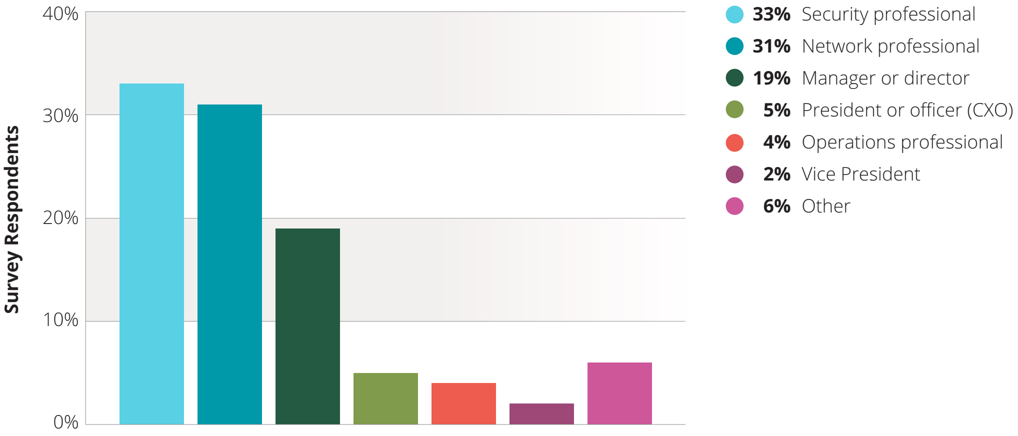


Figure 3 *Source: Arbor Networks, Inc.*

The WISR represents data collected from organizations that are headquartered — and that operate networks — all around the world (Figure 4). This year, the highest proportions of respondents are headquartered either in the United States and Canada or in Western, Central and Eastern Europe. This year, there are small increases in the proportions of respondents from Latin America and the Middle East, with a corresponding reduction in the proportion from Asia Pacific.

Many respondents offer services in multiple regions around the globe (Figure 4), with nearly half of respondents offering services either in the United States and Canada or in Western, Central and Eastern Europe.

Respondent’s Geographic Information

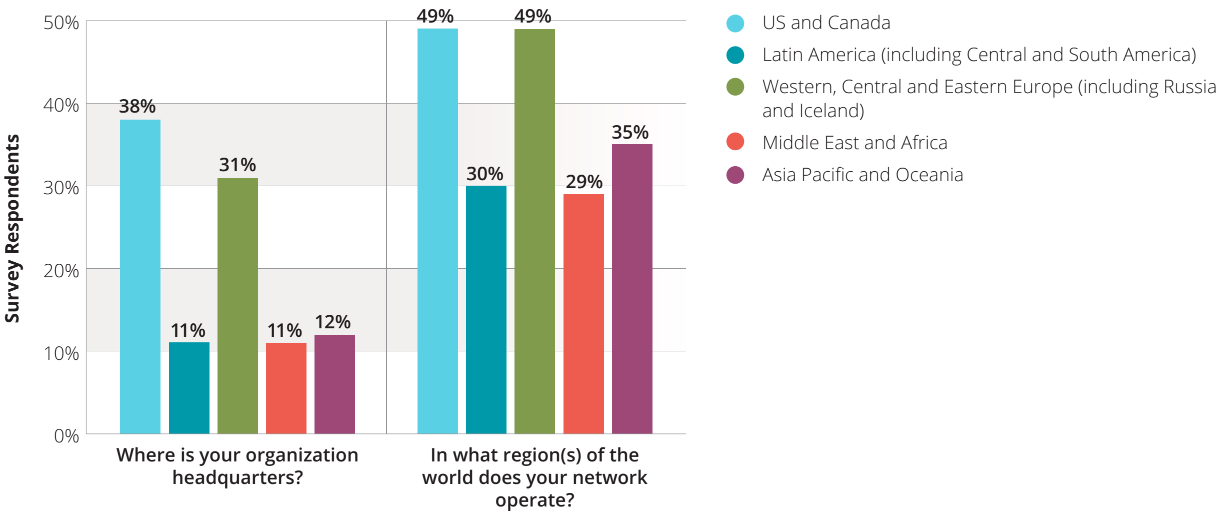


Figure 4 Source: Arbor Networks, Inc.

More than half of respondents maintain an internal security operations center (SOC), with 14 percent taking a hybrid approach (Figure 5). Hybrid SOCs are a mix of internal SOC resources supplemented by third-party SOC resources primarily for additional coverage on off hours and weekends. This is a growing trend that enables organizations to achieve 24x7 coverage, even if they are not staffed for this. Outsourcing the SOC entirely has increased, with 8 percent of respondents taking this approach — up from 5 percent last year. Just over one-fifth of respondents indicate that they have no SOC provision at all, a small improvement from last year’s 25 percent.

Looking more generally at dedicated security resources, 95 percent of respondents indicate they have personnel in place (Figure 6). This is a slight improvement from 94 percent last year. However, most organizations continue to work with relatively small teams of dedicated security personnel. Just over half of respondents have fewer than 10 dedicated resources — an almost identical percentage to last year. We have again seen a slight increase in the proportion of respondents with very large security teams (over 30 engineers) — up to 26 percent this year from 25 percent last year and 21 percent the year before.

Security Operations Center

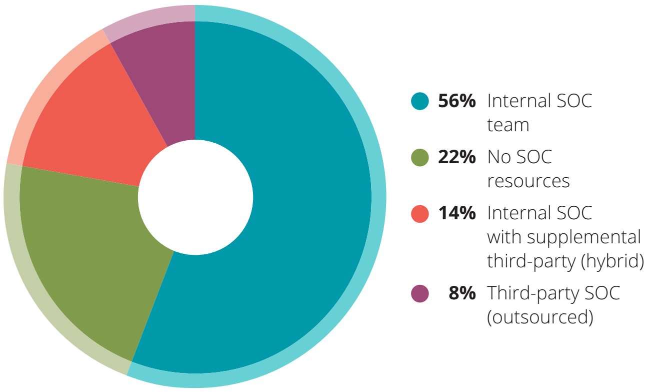


Figure 5 Source: Arbor Networks, Inc.

Dedicated Security Personnel

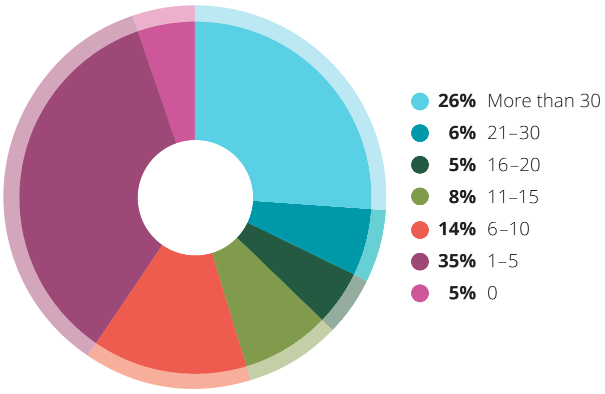


Figure 6 Source: Arbor Networks, Inc.

SERVICE PROVIDER KEY FINDINGS

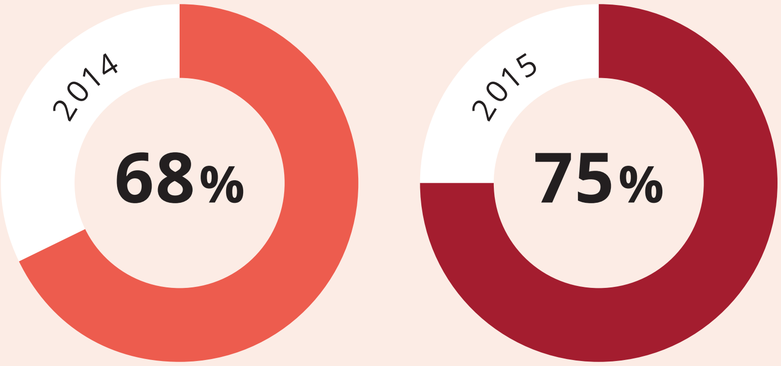
Threats and Concerns

- While DDoS attacks against customers remain the most commonly experienced threat, an increasing number of service provider respondents are experiencing bandwidth saturation due to streaming, OTT, unique events, etc.
- Encouragingly, the percentage of respondents seeing infrastructure outages due to failure or misconfiguration continues to fall.
- Looking at the security concerns of service provider respondents for the coming year, DDoS attacks continue to dominate, but there is less concern across all threat types.
- According to this year's respondents, NetFlow analyzers remain the most effective way of detecting threats; they are also the most commonly deployed. However, firewall logs — the second most commonly used detection mechanism — once again rank sixth in terms of effectiveness.
- About half of respondents cite both operational/ business support system integration and interoperability as their top concerns preventing the adoption of SDN/NFV.
- Similar to last year, 10 percent of respondents indicate that they are already implementing SDN/NFV technologies. However, an additional 39 percent are currently investigating or testing these technologies.

DDoS

- The largest attack reported by a respondent this year was 500 Gbps, with others reporting attacks of 450 Gbps, 425 Gbps and 337 Gbps.
- The trend of significant growth in the top-end size of DDoS attacks continues year-over-year. Last year, 20 percent of service provider respondents reported attacks over 50 Gbps. This year, nearly one-quarter report peak attack sizes over 100 Gbps. This emphasizes the scale of the DDoS problem.
- Customers remain the number one target for DDoS attacks, with over two-thirds of attacks targeting them.
- The proportion of respondents seeing attacks targeting cloud-based services has grown from 19 percent two years ago, to 29 percent last year and now 33 percent this year — a clear trend.
- The proportion of respondents seeing application-layer attacks continues to increase, up to 93 percent this year, from 90 percent last year and 86 percent in 2013.
- This year, there is a significant increase in those seeing multi-vector attacks, up to 56 percent from 42 percent last year.
- The most common service targeted by application-layer attacks is now, for the first time, DNS.

Three-quarters of respondents plan to deploy SDN/NFV in their data centers, up from just over two-thirds last year.



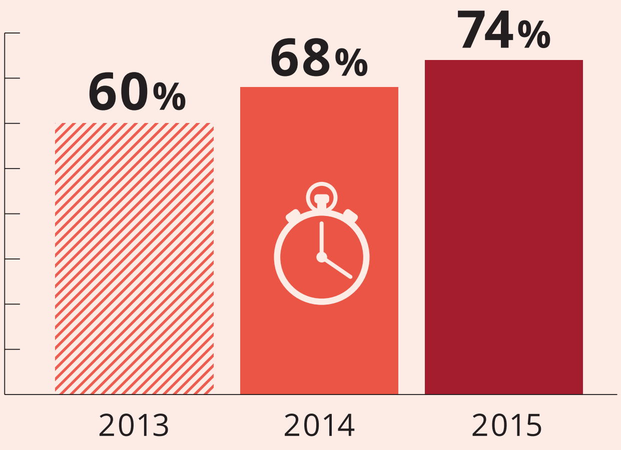
DDoS (continued)

- There is strong growth in those seeing attacks targeting SIP/VoIP services, up from 9 percent last year to 19 percent this year.
- This year, 44 percent of service providers indicate they have seen more than 21 attacks per month, up from 38 percent last year.
- Nine percent of respondents indicate they have witnessed IPv6 DDoS attacks. This is a significant increase over the 2 percent seen in previous iterations of this survey.
- This year, the top motivation behind DDoS attacks is “criminals demonstrating attack capabilities,” with “gaming” and “criminal extortion attempts” in second and third place respectively.
- A growing proportion of respondents are seeing DDoS attacks being used as a distraction for either malware infiltration or data exfiltration. This year, 26 percent see this as a common or very common motivation, up from 19 percent last year.
- Again this year, more respondents (73 percent) are using IDMS rather than ACLs to mitigate DDoS attacks. However, this gap has narrowed.
- Increased interest in DDoS detection and mitigation services continues this year, with 74 percent of service providers seeing more demand from customers, up 4 percent over last year.

Corporate Networks

- This year, there is a small increase in those respondents who have incident response handling plans in place, up 2 percent to 82 percent.
- Fewer respondents have well-resourced incident response handling teams, down from just under one-third to 25 percent.
- This year, the number of those who have contracted with external organizations to assist during incident response has increased 11 percent year-over-year.
- The most common threat seen by service providers against their corporate networks is Internet congestion due to DDoS, with an even greater proportion expressing concern about this in the future.
- The number who have experienced an APT on their corporate networks this year is around 10 percent, similar to last year. However, 44 percent are concerned about APT activity in the coming year, up from just over one-third last year.
- Almost one-third of service providers have reduced the time taken to discover an APT in their networks to under one week.
- Fifty-two percent state that they also have their discovery-to-containment time down to under one month.

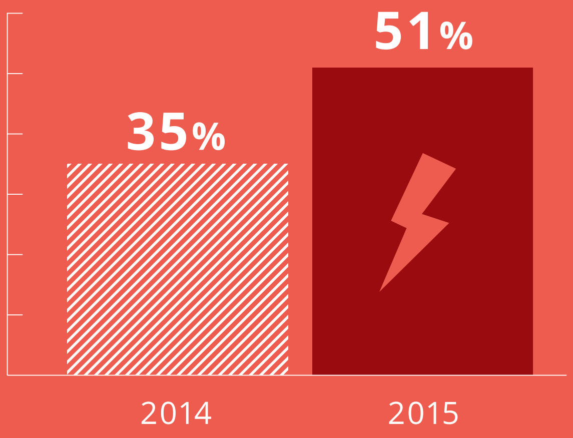
Nearly three quarters of service providers can now mitigate DDoS attacks in less than 20 minutes, up from 68 percent last year and 60 percent in 2013.



70% of service provider respondents feel their user community is properly educated around cyber security.

Almost 60% regularly update their security education and require re-certification of employees.

Last year, just over one-third of data center operators saw DDoS attacks that completely saturated their Internet connectivity. This year, that proportion has grown to 51 percent.



Corporate Networks (continued)

- Looking at the risks associated with a successful incursion by an APT, loss of personal information is the number one concern for service provider organizations, with reputation damage and disruption to business processes not far behind.
- Again this year, over half of respondents see an increase in incidents on the corporate network, with only 6 percent reporting a decrease.
- Over half of respondents state that they are reasonably well-prepared to deal with a security incident, a 12 percent increase from last year.
- As in previous years, NetFlow analysis and firewalls are the two most popular mechanisms used to detect threats within the corporate network, with firewalls growing by 8 percent. In contrast, the use of NetFlow analysis tools has fallen by 9 percent.
- In past surveys, manual detection was the number one way that respondents actually detected breaches. While manual detection is still in the top three methods, detection via routine checks and controls has replaced manual detection as the number one mechanism for actually detecting a security incident.
- This year, 20 percent of respondents indicate that they have cyber security insurance in place, an increase from 13 percent last year.
- In a significant increase over last year, 11 percent of respondents indicate that they have seen a breach or security incident related to a BYOD device.

Data Center Operators

- Visibility of traffic into or out of the data center at Layer 7 has continued to improve, with 44 percent of data center operator respondents having visibility at the application-layer — up from 38 percent last year and 23 percent in 2013.
- Only 15 percent of respondents have visibility of intra-data-center traffic that allows the detection of compromised devices. This is a key concern, as cyber criminals are increasingly using compromised devices within data centers to launch DDoS attacks, host C&C capabilities, etc.

Data Center Operators (continued)

- The proportion of respondents implementing anti-spoofing filters for some or all of their customers is consistent with last year. However, the proportion who have no plans to do this has fallen from 20 percent to 12 percent, which is encouraging.
- Firewalls, IDS/IPS and application firewalls are the three most commonly deployed security technologies at the data center perimeter. The use of iACLs has increased substantially from 30 percent last year to 46 percent this year.
- This year, 55 percent of respondents indicate they have seen DDoS attacks, down from two-thirds last year and 71 percent in 2013.
- Of those seeing attacks, 70 percent experience between 1 and 10 attacks per month, but 9 percent indicate they are seeing in excess of 50 attacks per month. None indicated this level of activity last year.
- Customers remain the most common target of DDoS attacks within the data center, similar to last year.
- There has been a sharp increase in the proportion of respondents seeing outbound attacks from servers within data centers, up to 34 percent from 24 percent last year.
- This year, as in the last two years, the number one business impact from DDoS is increased operational expense.
- This year, 56 percent of respondents indicate that they offer DDoS protection services to their customers, compared to only 37 percent last year.

Mobile Network Operators

- The exponential growth in mobile devices and applications is reflected in the high percentage deployment of LTE technology, where 84 percent of mobile network operator respondents now offer LTE services.
- Thirteen percent of MNO respondents have more than 100 million subscribers
- Thirty-eight percent of respondents indicate that they have experienced a security incident on the packet core that has led to a customer-visible outage.
- Seventy percent have observed DDoS attacks targeting their subscribers or infrastructure.

Organizational Security

- Implementation of anti-spoofing filters among service provider respondents is up to 44 percent this year, from 37 percent last year, but this is still less than half. It was hoped there would be a more significant increase, given the continued storm of reflection amplification DDoS attacks on the Internet.
- This year, 46 percent of respondents indicate that they carry out DDoS defense simulations, up from 34 percent last year. Even more positive is that 31 percent of service providers now run rehearsals at least on a quarterly basis, up from 21 percent last year.
- Encouragingly, the proportion of service providers who monitor for route hijacks has risen to 54 percent this year, from 40 percent last year.
- Participation in global OPSEC groups has improved slightly this year to 41 percent, from 36 percent last year.

Service Provider IPv6

- This year, nearly 70 percent of service provider respondents indicate that they have deployed IPv6 within their networks or plan to deploy it within the next 12 months.
- Thirty-three percent have completed their IPv6 deployment.
- More than 70 percent have subscribers utilizing IPv6 based services offerings.
- Continuing last year's trend, the number of respondents having IPv6 visibility continues to rise, this year to 70 percent.
- The top IPv6 security concerns are DDoS attack, followed by misconfiguration and botnets.

ENTERPRISE, GOVERNMENT AND EDUCATION (EGE) KEY FINDINGS

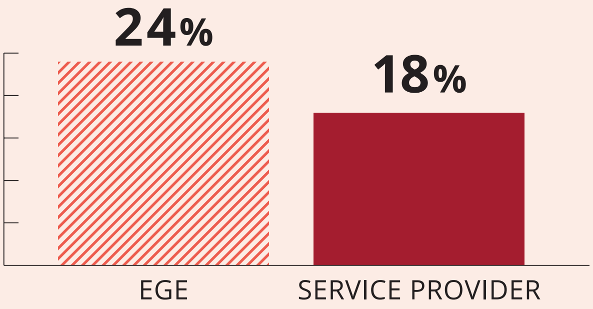
EGE Network Threats

- DDoS is once again the most common threat experienced by EGE respondents, similar to last year's results. The proportion experiencing malicious insiders increased from 12 percent last year to 17 percent this year. Those seeing APTs also grew from 18 percent to 23 percent.
- Less than 5 percent of respondents say incidents took more than three months to resolve.
- Eighty-two percent have either external or internal notification policies in place.
- Looking at the risks associated with a successful incursion by an APT, loss of personal information and disruption of business are the top concerns.
- This year, we see an increase in those with an incident response plan and at least some resources, up from around two-thirds last year to 75 percent this year.
- In this survey period, just over one-quarter of respondents indicate they have seen an increase in incident frequency.
- In terms of improving incident response, deploying solutions that speed up the incident response process is seeing significant interest, up from 45 percent last year to 57 percent this year.
- On a more negative note, there has been a big drop in those looking to increase their internal resources to improve incident preparedness, down from 46 percent to 38 percent.
- Similar to last year, firewalls and SIEM are the most commonly utilized tools to detect threats among EGE respondents. In third place are NetFlow analyzers. It should also be noted that the use of forensic packet analysis tools has increased by 9 percent this year — a big jump.
- This year, the proportion of respondents who have seen security incidents relating to BYOD has doubled to 13 percent, from 6 percent last year.

EGE DDoS

- More than half had firewall or IPS devices experience a failure or contribute to an outage during an attack, a significant uptick from last year.
- Over one-quarter indicate they suffered more than 10 attacks per month, and about half say attacks have exceeded their total Internet capacity.
- The most commonly perceived motivations behind DDoS attacks are now "criminals demonstrating attack capabilities" and "criminal extortion attempts."
- On a very encouraging note, 43 percent indicate they are using intelligent DDoS mitigation systems (IDMS), compared to around one-third last year.
- In a significant improvement over last year, nearly twice the percentage of respondents indicate they have the ability to immediately mitigate DDoS attacks via an "always-on" device or service.
- Just over one-quarter of EGE respondents are able to mitigate DDoS attacks in less than 15 minutes.
- Operational expenses, reputation/brand damage and direct revenue loss are the top business impacts of DDoS attacks.

This year's EGE respondents indicate that 24 percent of attacks targeted the application layer, significantly higher than the 18 percent reported by service providers.



EGE Organizational Security Practices

- The percentage of EGE respondents implementing infrastructure security best practices is lower in general when compared to service provider respondents.
- Thirty-eight percent indicate that they carry out DDoS defense simulations, a lower percentage than within the service provider respondents.
- Seventy percent of EGE respondents proactively filter known botnet command-and-control servers, malware drop servers, etc., as opposed to only just over one-half of service providers.

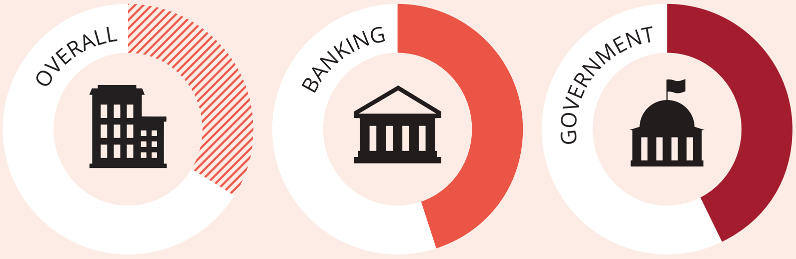
EGE IPv6

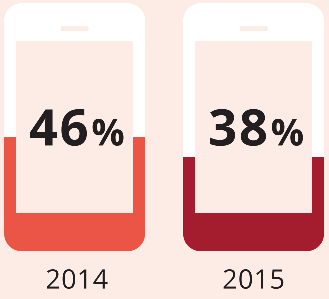
- Around one-quarter of EGE respondents indicate that they have already deployed IPv6 in their networks or plan to deploy it within the next 12 months.
- Fifty-eight percent have Internet-facing services available over IPv6.
- Half of those who have deployed IPv6 use it in their internal (private) networks.
- More than 60 percent have solutions deployed that provide visibility of IPv6 traffic.
- The top security concern around IPv6 is DDoS attack. Concerns around IPv4/IPv6 feature parity have fallen back this year.

DNS Operators

- Overall, 22 percent have NO security group responsible for their DNS infrastructure, down from one-third last year. However, 26 percent of enterprise respondents are still in this situation, as opposed to only 17 percent of service providers.
- Just under one-third of all respondents saw DDoS attacks against DNS infrastructure that resulted in a customer-visible outage. However, this percentage rises to just over one-half if we look purely at service provider respondents.
- The security mechanisms used to defend DNS infrastructure from DDoS attack are similar to last year, with firewalls, ACLs and IPS/IDS being the three most common technologies deployed within respondent networks.
- Only 19 percent of enterprise respondents utilize IDMS to protect DNS infrastructure, compared to just over half of service providers.

Thirty-four percent of this year's EGE respondents report that their organizations have experienced DDoS attacks over the past year. However, for the banking and government verticals, the percentages are higher, at 45 percent and 43 percent respectively.





Thirty-eight percent of all EGE respondent indicate they have *no* tools deployed to monitor BYOD on their networks. This is an improvement from 46% last year.

servi

SECTION 2

SERVICE PROVIDER

MOST SIGNIFICANT OPERATIONAL THREATS

DDoS attacks against customers remain the most commonly experienced threat among service provider respondents. An increasing proportion of these respondents are experiencing bandwidth saturation due to streaming, OTT, unique events, etc. Encouragingly, the percentage seeing infrastructure outages due to failure or misconfiguration continues to fall. Looking at security concerns for the next year, DDoS attacks continue to dominate, but there is an overall drop in the proportion of respondents concerned across all threat types. Consistent with last year, NetFlow analyzers are the tools most commonly used to detect threats, followed by firewall logs. NetFlow analyzers also remain the most effective way of detecting threats, while firewall logs once again rank sixth in terms of effectiveness.

Similar to last year, 10 percent of service provider respondents indicate they are already using SDN/NFV in production. However, an additional 39 percent are currently investigating or testing these technologies. Three-quarters of respondents plan to deploy these technologies in their data centers, up from just over two-thirds last year. Forty-two percent are considering deployment for value-added services, up from one-third last year. About half of respondents cite both operational/ business support system integration and interoperability as their top concerns preventing the adoption of SDN/NFV.

DDoS attacks against customers are increasingly the most commonly experienced security threat (Figure 7). The percentage seeing these attacks reached a new high of 77 percent; this exceeds last year's result by four percentage points. DDoS attacks targeting service infrastructure were seen by a lower proportion than last year, in contrast to an increase in those seeing bandwidth saturation (e.g., due to streaming, over-the-top services, unique events, flash crowds, etc.). Interestingly, we are once again seeing a declining trend in those experiencing infrastructure outages due to equipment failures or misconfiguration. The percentage has fallen steadily over the past few years from 60 percent, to 55 percent, to 53 percent and finally 49 percent this year.

Service Provider Experienced Threats

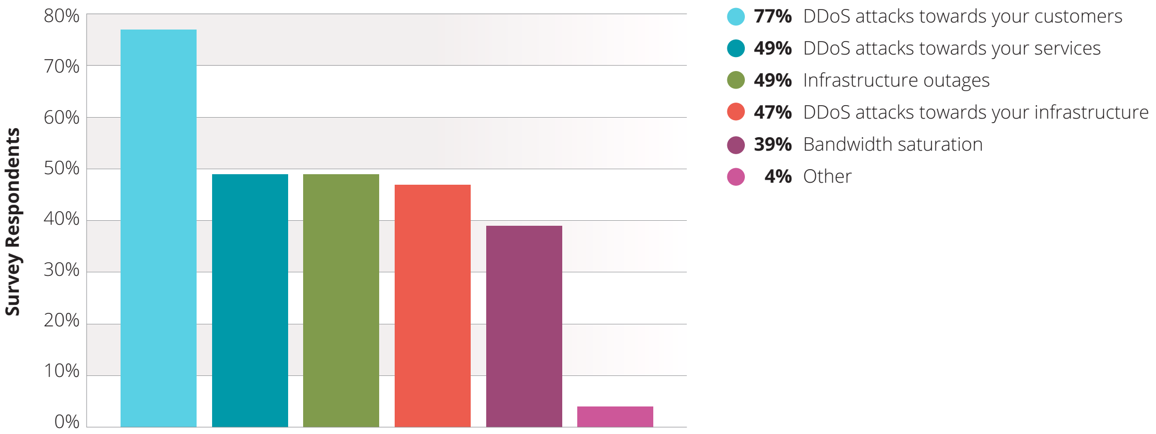


Figure 7 *Source: Arbor Networks, Inc.*

Looking at security concerns for the next 12 months (Figure 8), DDoS attacks continue to dominate, but there is an overall drop in those concerned across all threat types. In a reversal from last year, attacks targeting customers have regained the top spot at 69 percent. This is likely due to the increased proportion of respondents who have experienced attacks, as noted above. The results this year also indicate a decline in those concerned about DDoS attacks against infrastructure and services, with both dropping by about 10 percentage points. Concerns over bandwidth saturation and infrastructure outages due to equipment failures or misconfiguration are both on the rise this year. The former is likely due to the increased proportion of respondents who have experienced this issue in the last 12 months. The latter may be due to the continued focus on preventable failures and outages as demonstrated by the convergence of respondents experiencing and showing concern around these issues over the past few years.

Service Provider Expected Threats

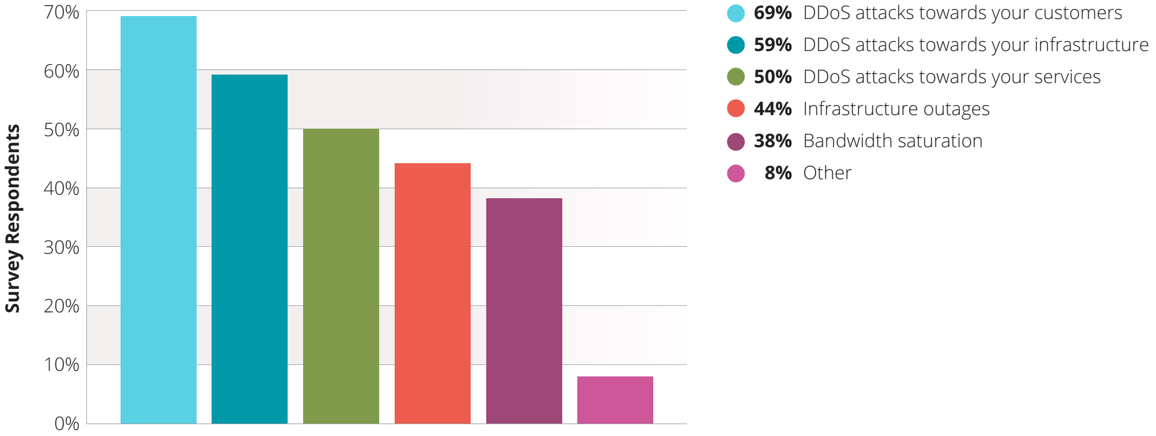


Figure 8 *Source: Arbor Networks, Inc.*

We asked participants which tools they use to detect threats targeting their networks, customers and services (Figure 9). Consistent with last year, NetFlow analyzers are the most commonly used tools, followed by firewall logs. However, both lost a few percentage points this year. While the proportion using SNMP tools has remained essentially the same as last year, SNMP now shares the third spot, tied with IDS/IPS.

Threat Detection Tools

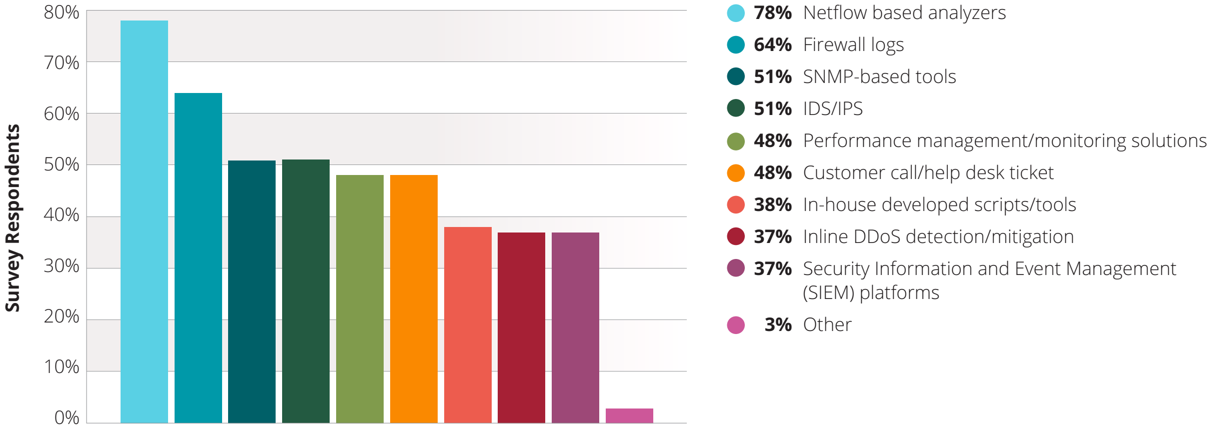


Figure 9 *Source: Arbor Networks, Inc.*

Looking at the effectiveness of deployed threat detection mechanisms (Figure 10), NetFlow analyzers remain the most effective way of detecting threats, as well as being the most commonly deployed. However, firewall logs — the second most commonly used detection mechanism — once again rank sixth in terms of effectiveness. These results are almost identical to last year.

In-line DDoS detection/mitigation systems are ranked second in effectiveness. However, the scalability requirements within the service provider space will likely mean that NetFlow will always be the most commonly deployed threat detection mechanism, with in-line devices used to protect key infrastructure and customers. Lastly, SIEM solutions are once again in second-to-last place in terms of effectiveness, despite their broad industry acceptance.

Effectiveness of Threat Detection Tools

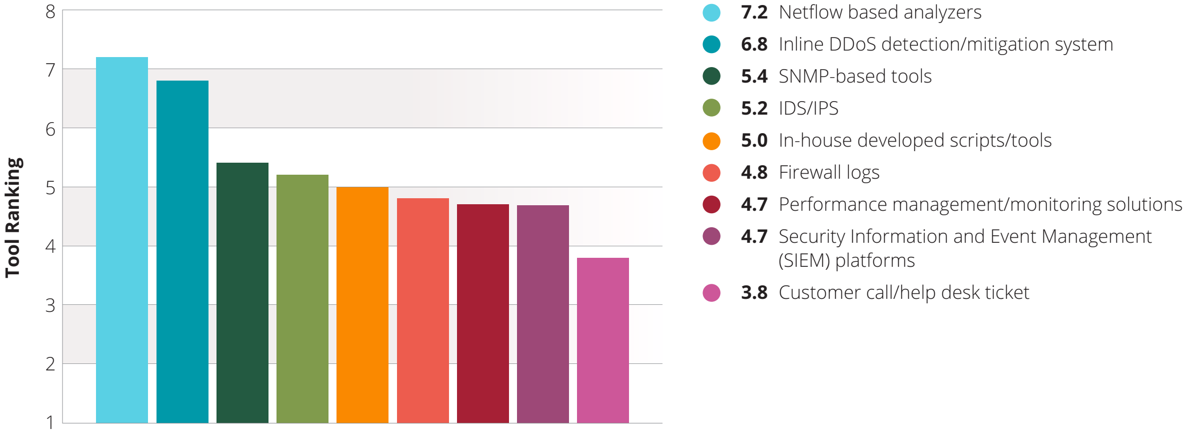


Figure 10 *Source: Arbor Networks, Inc.*

For the second year, we asked our service provider respondents if they plan on implementing SDN or NFV in a production environment. As expected, we see a significant increase in activity this year. Similar to last year, 11 percent indicate that they are already implementing these technologies (Figure 11). However, an additional 39 percent report that they are currently investigating or testing the technologies, with only 28 percent having no current plans to deploy SDN or NFV in the next few years.

SDN/NFV Deployment

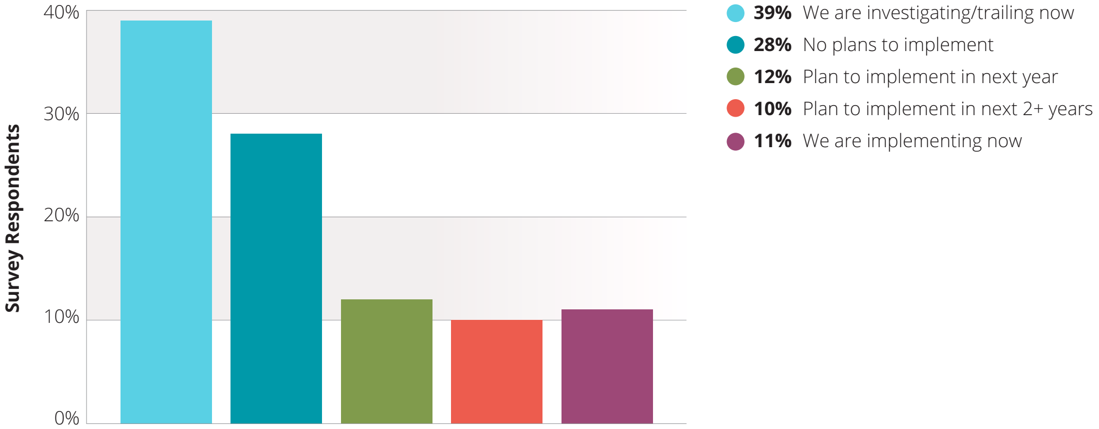


Figure 11 *Source: Arbor Networks, Inc.*

In terms of the locations within networks where these technologies are seeing the most interest, data centers are the clear leader again this year. Three-quarters of respondents plan to deploy these technologies in their data centers (Figure 12), up from just over two-thirds last year. This year also saw increased interest in utilizing SDN/NFV in value-added service infrastructure, with 42 percent of respondents considering deployment in this arena, up from one-third last year. Similar to last year, about one-third of respondents indicate that they plan to use SDN or NFV within their fixed-line infrastructure.

SDN/NFV Network Domains

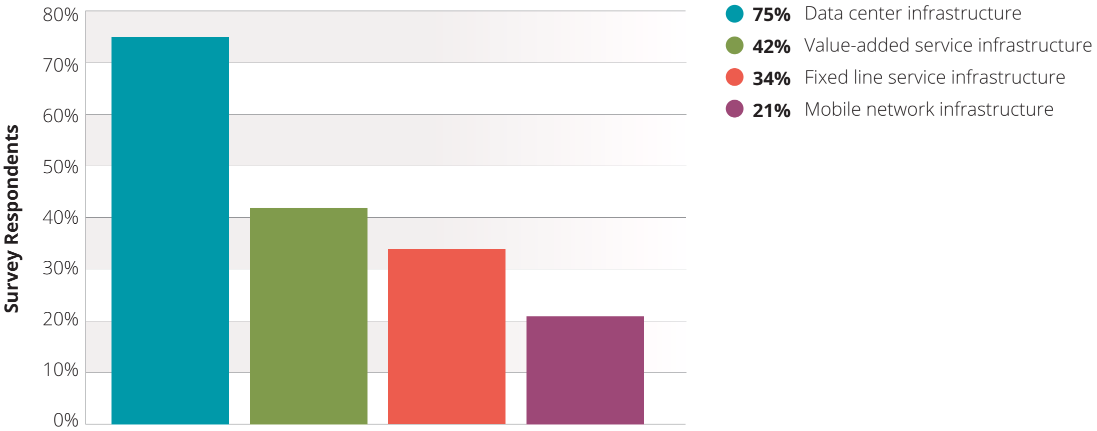


Figure 12 *Source: Arbor Networks, Inc.*

Finally in this area, we asked respondents what barriers are preventing the deployment of SDN and NFV technologies at this time. About half of respondents cite both operational/business support system integration and interoperability as top concerns (Figure 13). Around one-third indicate that security and vendor support are key barriers, and about one-quarter reference scalability. Other concerns beyond telemetry acquisition include cost, stability and performance.

SDN/NFV Key Barriers

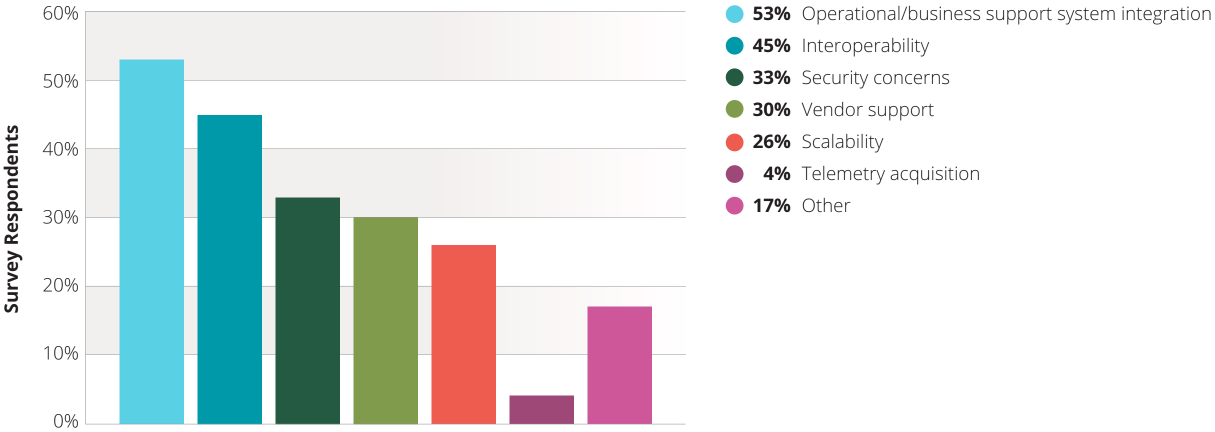


Figure 13 *Source: Arbor Networks, Inc.*

SERVICE PROVIDER DDoS ATTACKS

The largest attack reported by a respondent this year was 500 Gbps, with other respondents reporting attacks of 450 Gbps, 425 Gbps and 337 Gbps. This continues the trend of significant growth in the top-end size of DDoS attacks year-over-year. Last year, we highlighted that 20 percent of respondents reported attacks over 50 Gbps. In contrast, this year nearly one-quarter of respondents report peak attack sizes over 100 Gbps, emphasizing the scale of the DDoS problem. Customers remain the number one target for DDoS attacks, with over two-thirds of attacks targeting them. Again this year, the proportion of respondents seeing attacks targeting cloud-based services has grown, up from 19 percent two years ago, to 29 percent last year and now 33 percent this year — a clear trend.

This year, attackers have continued the 2014 trend of using reflection/amplification techniques to exploit vulnerabilities in NTP, SSDP and other protocols. The largest attack reported by a respondent this year was 500 Gbps, with other respondents reporting attacks of 450 Gbps, 425 Gbps, and 337 Gbps (Figure 14). Another five respondents reported events at 200+ Gbps. This continues the trend of significant growth in the top-end size of DDoS attacks year-over-year.

Last year, 20 percent of respondents reported attacks over 50 Gbps. This year's survey results indicate a sharp uptick, with nearly 25 percent of respondents seeing peak attack sizes over 100 Gbps. In general, peak attack sizes and large attack frequency seem to have increased dramatically over last year. The record number of 100 Gbps+ attacks tracked by the Arbor ATLAS system during 2015 confirms this; please see the ATLAS attack sizes section for further details.

Survey Peak Attack Size Year Over Year

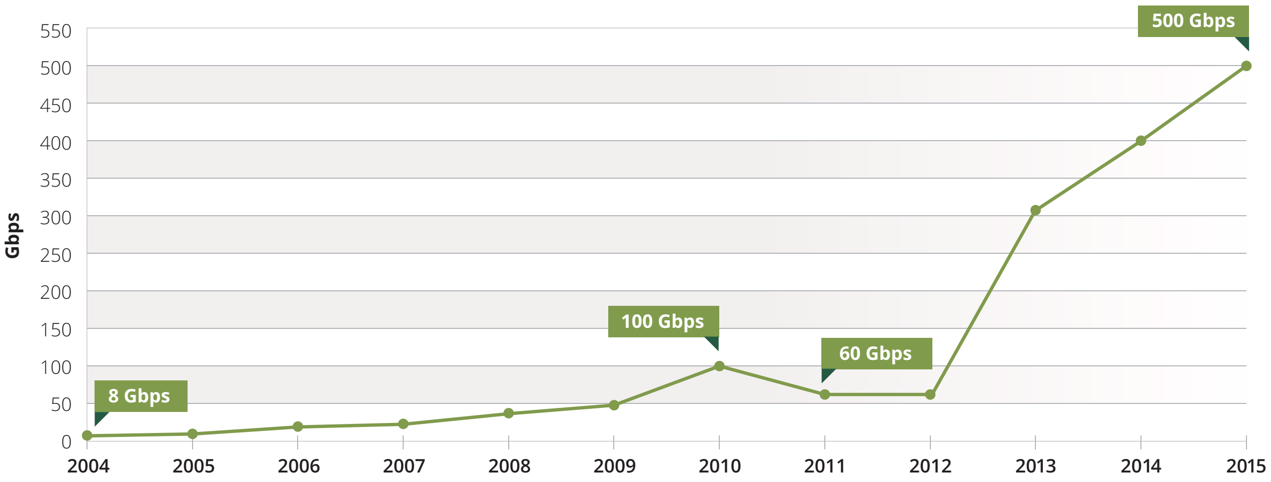


Figure 14 *Source: Arbor Networks, Inc.*

Once again, this year's survey asked a specific question about the protocols used for reflection/amplification (Figure 15). While all of these protocols have increased activity this year, DNS remains the most commonly used, with NTP close behind. However, the results also show significant use of SSDP, SNMP and Chargen. Of those respondents citing "other" protocols, the majority indicate they have seen attacks exploiting RIP. Similar to last year, attackers continue to leverage poorly configured or protected infrastructure to magnify their capabilities. Please see the ATLAS Reflection Amplification update section for further details.

Protocols Used for Reflection/Amplification

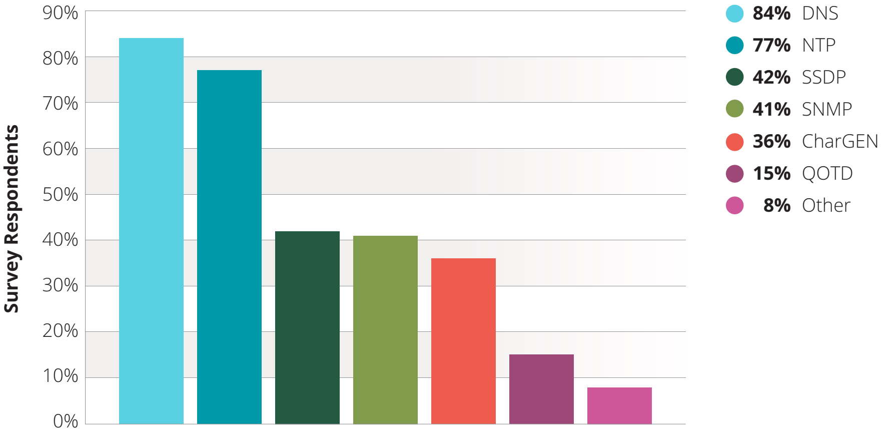


Figure 15 *Source: Arbor Networks, Inc.*

Looking more generally at the targets of DDoS attacks monitored by survey participants (Figure 16), the results are very similar to recent years. Customers remain the number one target, with two-thirds of attacks targeting them. The proportions of attacks targeting service and network infrastructure also remain consistent with last year.

Attack Target Mix

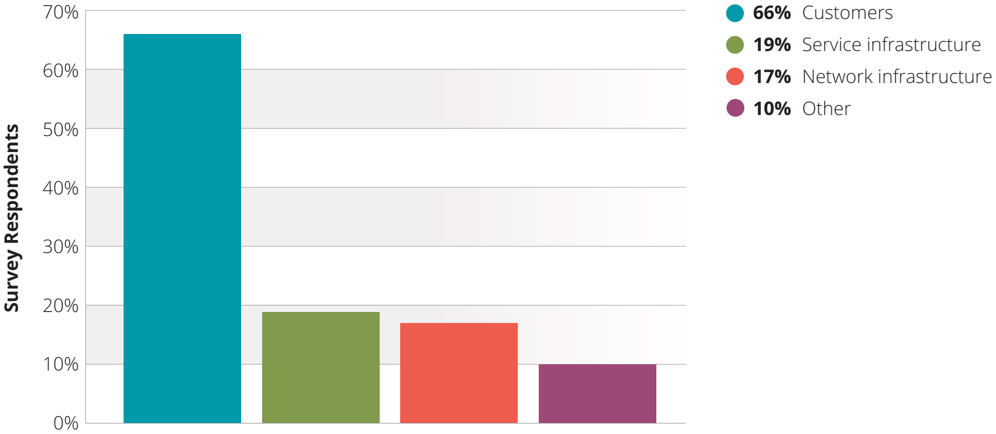


Figure 16 *Source: Arbor Networks, Inc.*

Similar to last year, end-user subscribers take the top spot as the most common type of customer targeted. Finance, which was in fifth place last year, has moved up into a three-way tie for second place with government and hosting (Figure 17). Meanwhile, e-commerce, which garnered second place last year, was pushed down to third place in a near tie with gaming. Other significant targets include education and gambling organizations, both of which were reported by about one-quarter of respondents.

Attack Target Customer Vertical

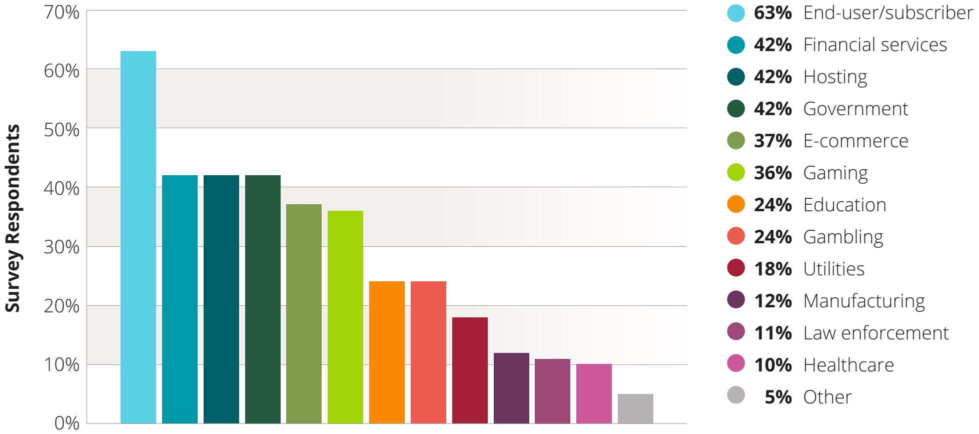


Figure 17 *Source: Arbor Networks, Inc.*

The use of cloud services continues to grow, with many organizations now adopting public, private or hybrid cloud solutions. Cloud services can offer significant performance, flexibility and cost advantages to business. However, they are generally reached via the Internet (even if a VPN is in place) and are therefore susceptible to DDoS attacks targeting their connectivity. When users cannot reach a cloud-based service, all of the business benefits are irrelevant. This year, the proportion seeing attacks targeting cloud-based services has grown again (Figure 18), up from 19 percent two years ago, to 29 percent last year and now 33 percent this year – a clear trend.

Given that cloud services are frequent targets of attacks, they warrant protection from the DDoS threat, especially given the multi-tenant nature of some infrastructure. Attacks targeting one customer can impact others and cause collateral damage if appropriate defenses are not in place. This can lead to significant, and potentially costly, problems for the cloud service provider.

Attacks Targeting Cloud Services

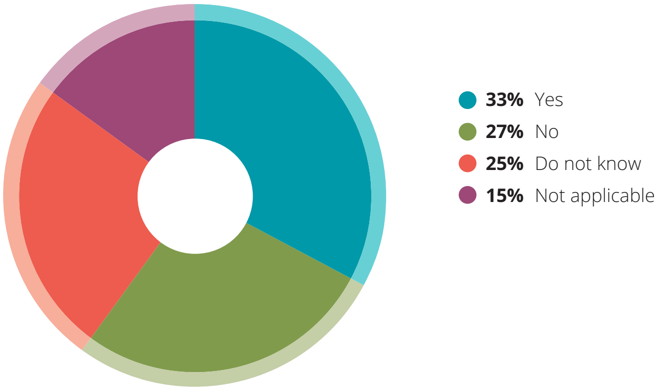


Figure 18 *Source: Arbor Networks, Inc.*

ARBOR ATLAS

ATTACK SIZES

The ATLAS® system gathers statistics from 300+ customers who use Arbor Networks® Peakflow SP all around the world. These statistics include anonymized details of the DDoS attacks monitored by these participants, along with summary information on the traffic crossing their network boundaries. ATLAS provides a view into approximately 30 percent of all Internet traffic. Arbor's team collates and analyzes this unique data set to determine key trends in DDoS attack activity. This data is then released quarterly to the broader operational security community, and referenced within the WISR on an annual basis.

In line with the results from the WISR survey, ATLAS data shows an increase in peak attack sizes monitored during 2015. The largest attack monitored by ATLAS was 334 Gbps, a small increase from the 2014 peak of 325 Gbps. Anecdotally, however, some Arbor customers who do not currently participate in the ATLAS system indicate they have seen even larger attacks in the latter half of the year. This is consistent with the data provided by WISR survey respondents.

However, the ATLAS data makes it very clear that the average size and frequency of very large DDoS attacks continue to grow. ATLAS data (Figure A.1) clearly demonstrates that, in 2015, peak monthly attack sizes were larger in many cases than in 2014. In fact, the number of attacks over 100 Gbps grew significantly this year. In 2013, ATLAS tracked 39 attacks over 100 Gbps. In 2014, we monitored 159. This year, we are up to 223, with 16 of those being over 200 Gbps.

Peak Attack Sizes 2014/2015

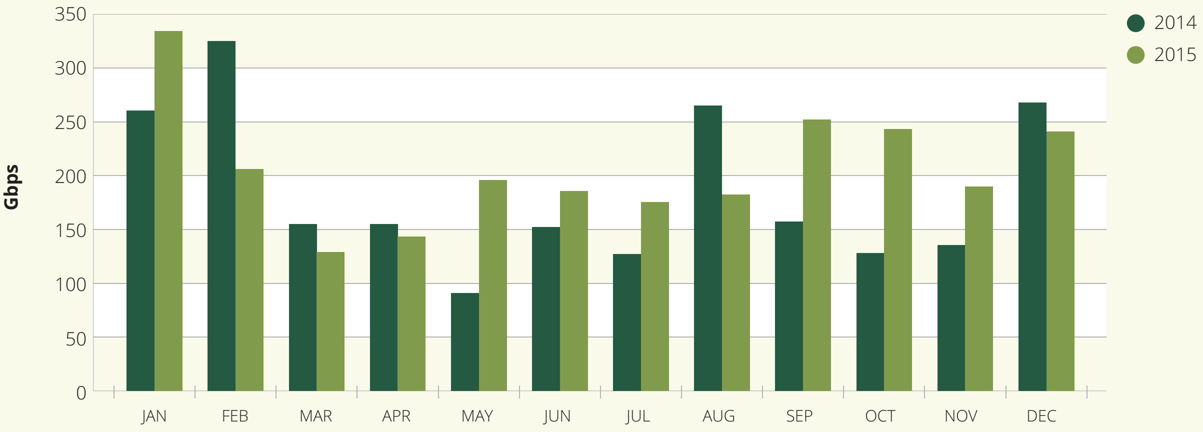


Figure A.1 *Source: Arbor Networks, Inc.*

The majority of monitored DDoS attacks are, however, still relatively small, with 84 percent of monitored events less than 1 Gbps in size (Figure A.2). The mean attack size this year was 760 Mbps. This does not seem like a huge amount of traffic, but attacks of this magnitude are still capable of causing significant problems for businesses that do not have the relevant preparations in place.

DDoS Attacks by Size

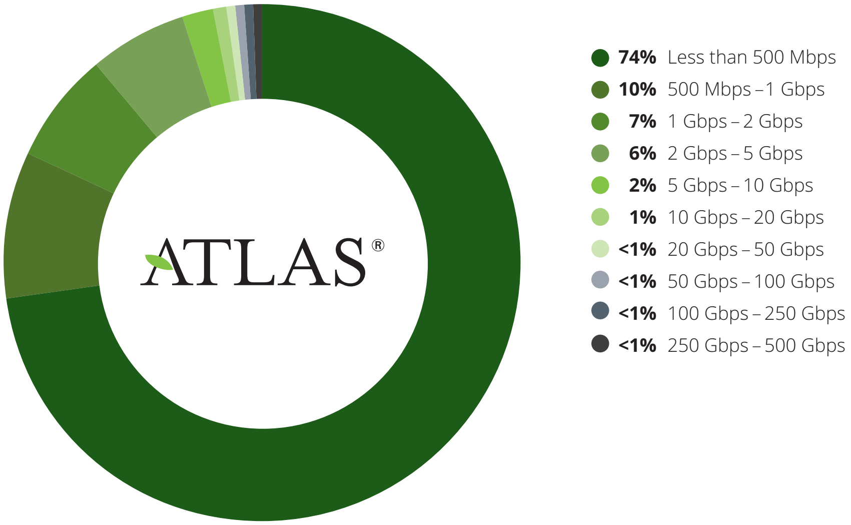


Figure A.2 *Source: Arbor Networks, Inc.*

Looking at the distribution of attacks in the 2-50 Gbps range through most of the year, we can see a clear upward trend in frequency (Figure A.3). This has been highlighted earlier this year in our quarterly ATLAS updates. Interestingly, however, we do not see a linear pattern when looking at the distribution of larger attacks (Figure A.4). This may indicate that these are generated in waves by specific attack campaigns or bad actor groups.

Attack Frequency (2–50 Gbps)

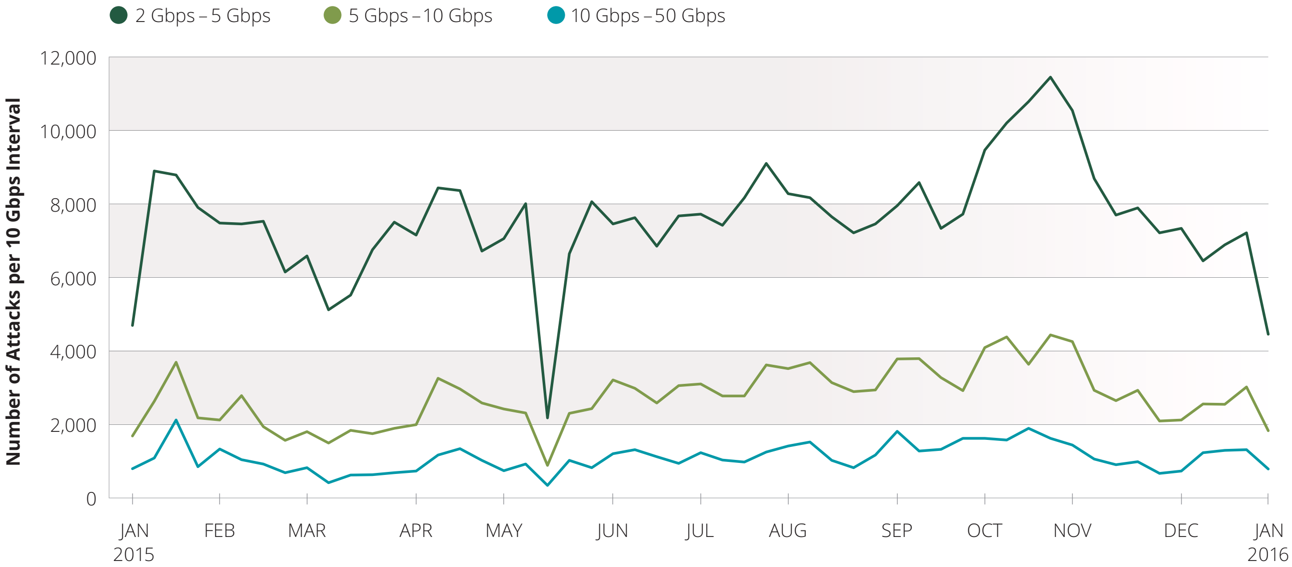


Figure A.3 *Source: Arbor Networks, Inc.*

Attack Frequency (50 – 300 Gbps)

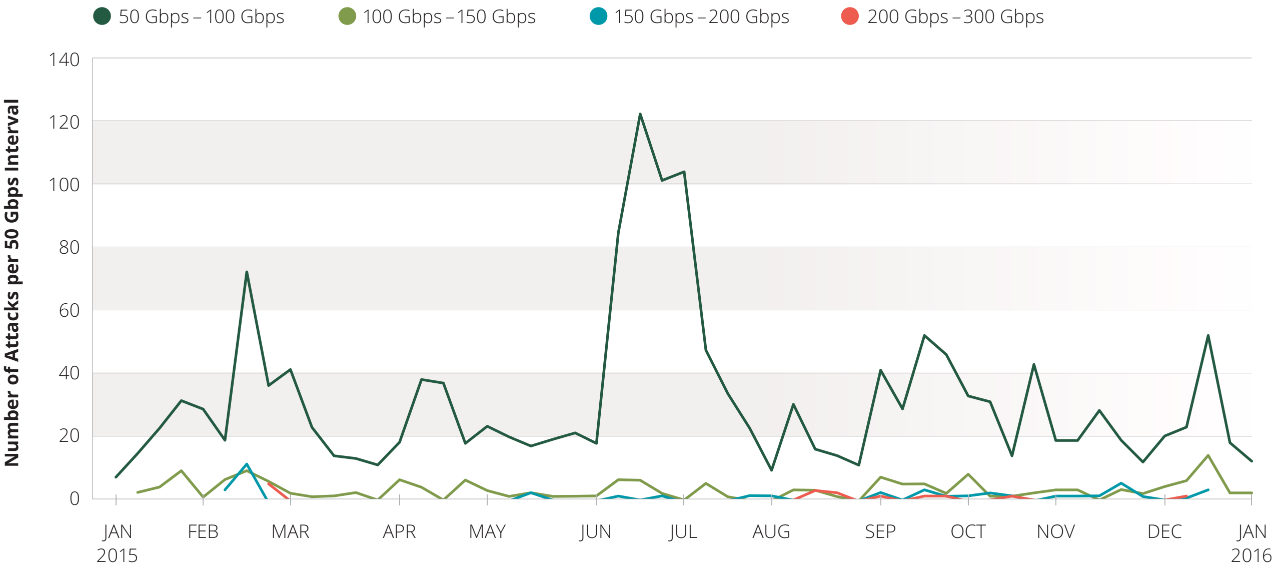


Figure A.4 *Source: Arbor Networks, Inc.*

ATTACK DURATIONS

In addition to tracking attack sizes, ATLAS also allows Arbor to track the duration of attacks monitored by participating network operators. During this survey period, the downward trend in attack durations appears to have stabilized.

This year, ATLAS data showed that 91 percent of events lasted less than one hour, a very small increase from the 88 and 90 percent seen in 2013 and 2014, respectively (Figure A.5). The average attack duration in 2015 was 58 minutes, which is relatively consistent with previous results.

It should be noted, however, that although the majority of individual ATLAS events lasted less than one hour, they can, in many cases, be part of multi-event campaigns where attackers will start/stop the attack sporadically over an extended period. This is done deliberately to make mitigation more complex, as organizations that do not operate a layered DDoS defensive strategy will need to divert their traffic to a cloud/service provider DDoS mitigation service for each and every event.

DDoS Attack Durations

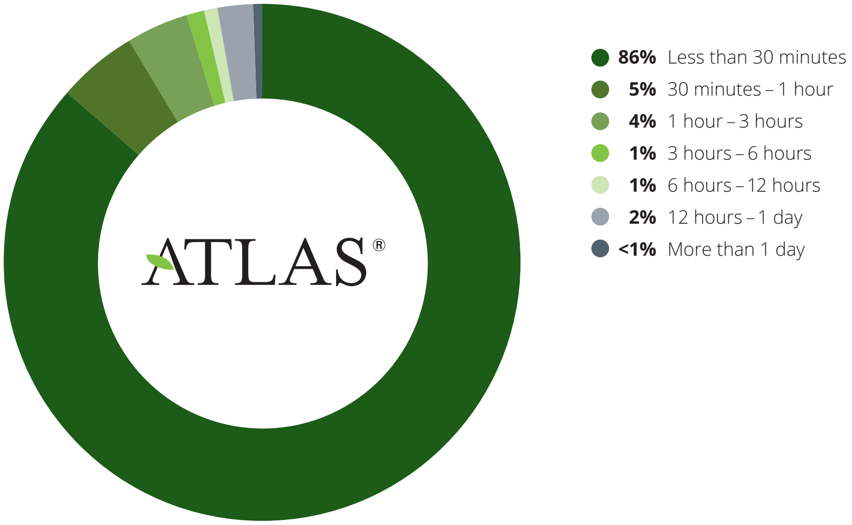


Figure A.5 *Source: Arbor Networks, Inc.*

TARGETED SERVICES

The top service port targeted during the survey period was HTTP, as in previous years. The proportion of attacks targeting UDP/80 throughout 2015 stands at 18.8 percent (Figure A.6). This is nearly four times the level of the next most commonly targeted service, DNS.

It should also be noted that ATLAS has seen an the proportion of attacks targeting port 443 stay relatively static at around 3 percent. Also interesting is the fact that ports 3074 and 25565, Xbox and Minecraft respectively, are among the top 10 targets — illustrating how much gaming-oriented DDoS is taking place.

Ports Targeted by DDoS Attacks

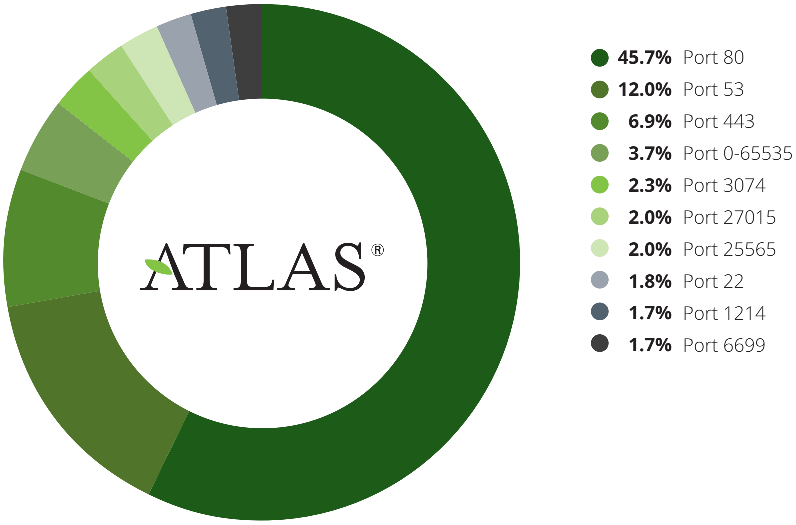


Figure A.6 *Source: Arbor Networks, Inc.*

SOURCE AND TARGET COUNTRIES

For the first time this year, Arbor is including ATLAS data in the WISR that aligns monitored attacks to the IP location of the source or destination. It should be noted that although a commercial database is used to map IP addresses to locations, the accuracy is limited. Therefore, this data should only be taken as a rough guideline.

As expected, the top two target countries are the USA and China (Figure A.7). The third most common target is France, which may come as a surprise to some. However, data centers in France provide hosting for many organizations based all around the world, and so the actual target businesses are, in many cases, not of French origin.

Looking at the targets of attacks in excess of 10 Gbps, the USA remains in the top spot, with France in third place. However, Canada is the second most popular target. China is, in fact, all the way down in 11th place.

Moving on to look at the sources of DDoS attacks (Figure A.8), we can see that the USA, South Korea and China hold the top spots. This is consistent with data from 2014. For attacks larger than 10 Gbps, the top three source countries are USA, China and Great Britain. Note: source country break-outs can add up to more than 100 percent as attack traffic for a single attack can be sourced from multiple countries.

Top 10 Target Countries

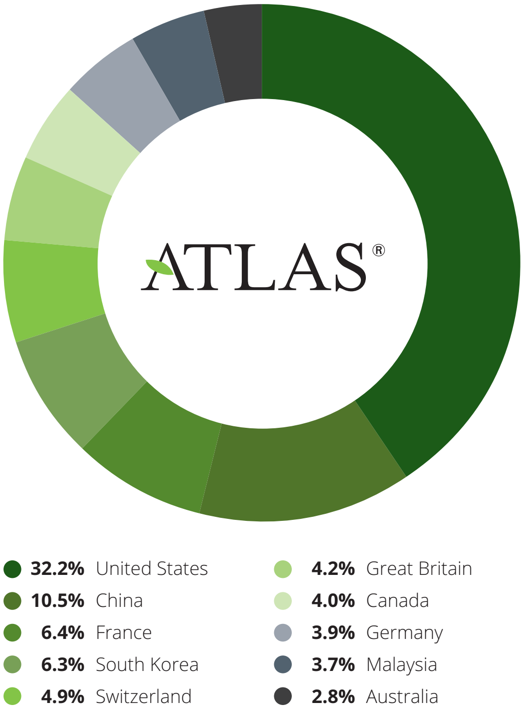


Figure A.7 *Source: Arbor Networks, Inc.*

Top 10 Source Countries

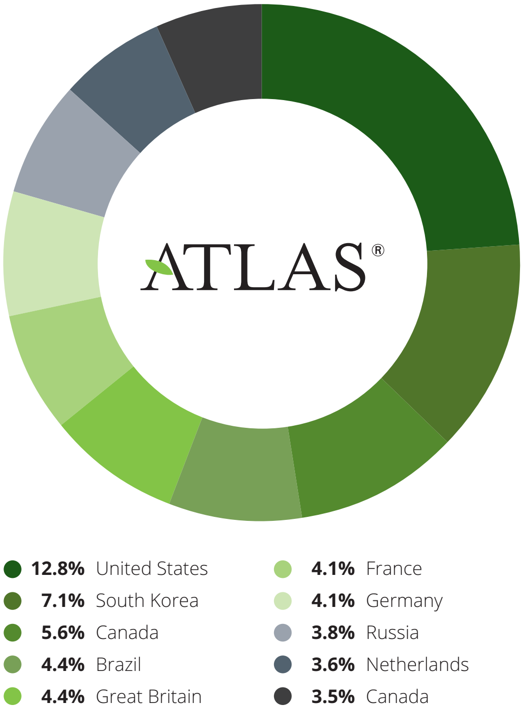


Figure A.8 *Source: Arbor Networks, Inc.*

REFLECTION AMPLIFICATION UPDATE

In last year's WISR, Arbor reported on the storm of reflection amplification DDoS activity across the Internet in 2014. During 2015, high levels of reflection amplification DDoS activity have continued. The concentration of very large attacks has not rivaled that seen in the first part of 2014, but there continue to be very large numbers of very large attacks.

In the early part of 2015, the most common protocol being leveraged for reflection amplification attacks was SSDP (Simple Service Discovery Protocol), with very high levels of activity seen in Q1 (Figure A.9). ATLAS tracked more than 50,000 attacks per month during this period. The use of SSDP, however, trailed off significantly in the latter part of the year. As of Q4, we are tracking around 10,000 to 15,000 attacks per month. However, as can be seen on the following page, there was renewed focus on NTP in the latter half of the year, with over 55,000 attacks per month monitored in September and October.

Protocols Used in Reflection Amplification Attacks (Attacks Per Week)

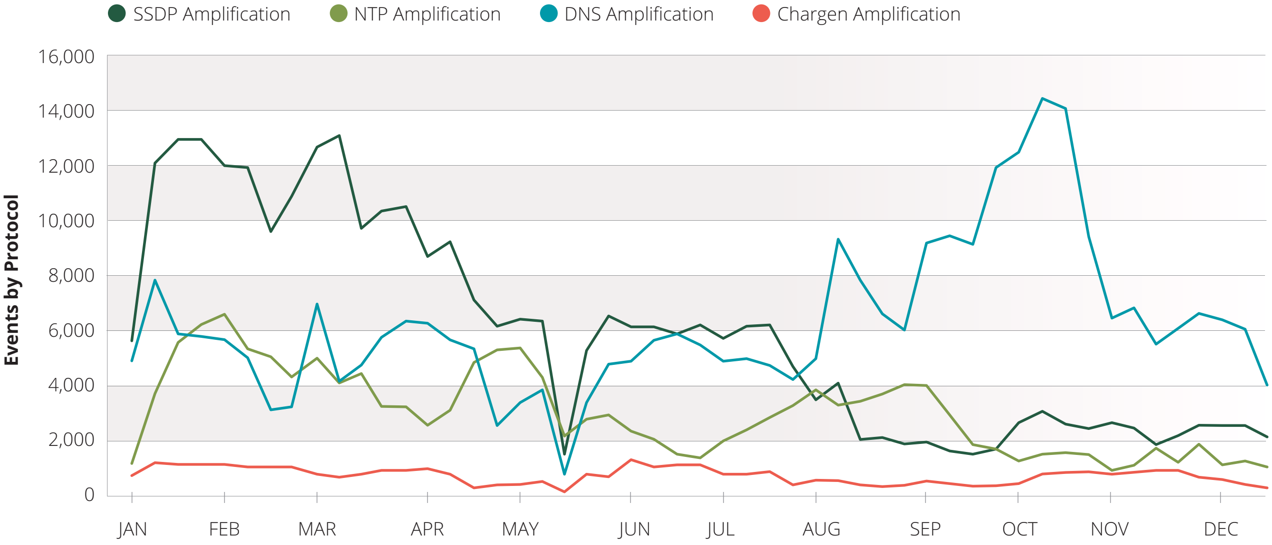


Figure A.9 *Source: Arbor Networks, Inc.*

The media has also given some focus to the use of other protocols, such as Portmap. While Portmap has seen growth over the last few months, it has only been responsible for around 300 attacks per month since September. The overall breakout of reflection amplification attacks by protocol throughout the year can be seen in Figure A.10.

Protocols Used in Reflection Amplification Attacks

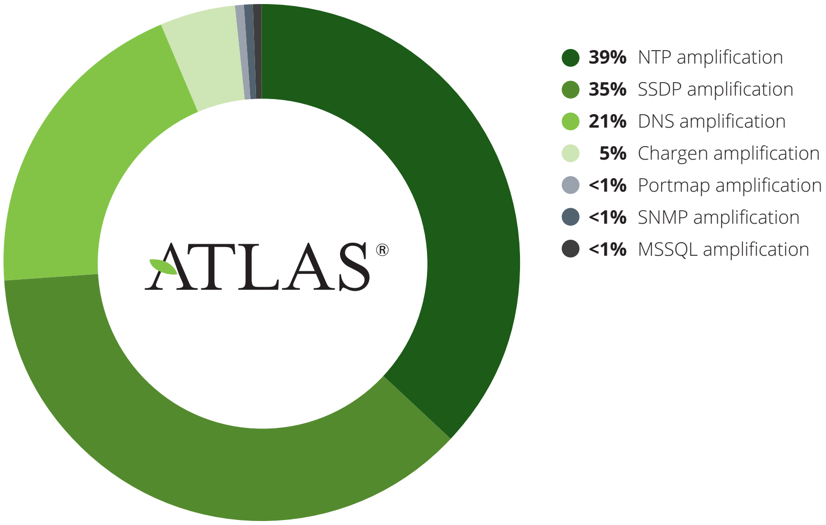


Figure A.10 *Source: Arbor Networks, Inc.*

The average size of reflection amplification attacks during 2015 was around 1.97 Gbps, significantly above the more general average attack size. This is expected, given that the aim of reflection amplification is usually to saturate the connectivity of the target. Attacks of 1.97 Gbps may not seem large, but they are still sufficient to saturate the Internet connectivity of many enterprises. Figure A.11 tracks the average size of reflection amplification attacks through 2015 on a week-by-week basis.

Average Size of Reflection Amplification Attacks

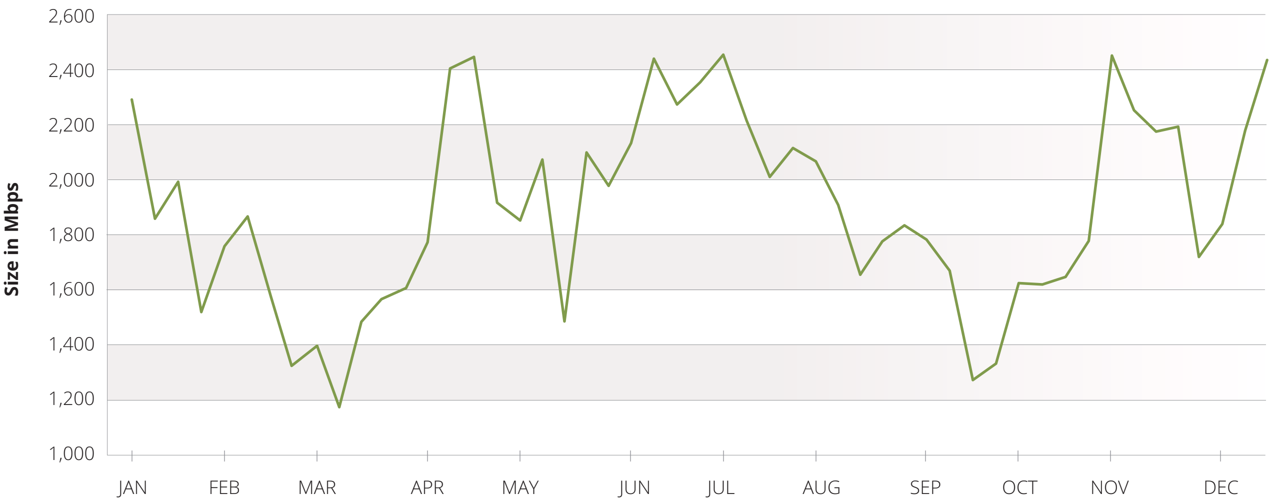


Figure A.11 *Source: Arbor Networks, Inc.*

The largest reflection amplification attack tracked in 2015 was monitored at 252.64 Gbps. This was an SSDP reflection attack in September that targeted a destination in the USA. Figure A.12 tracks the peak size of reflection amplification attacks through 2015 on a week-by-week basis.

Peak Size of Reflection Amplification Attacks

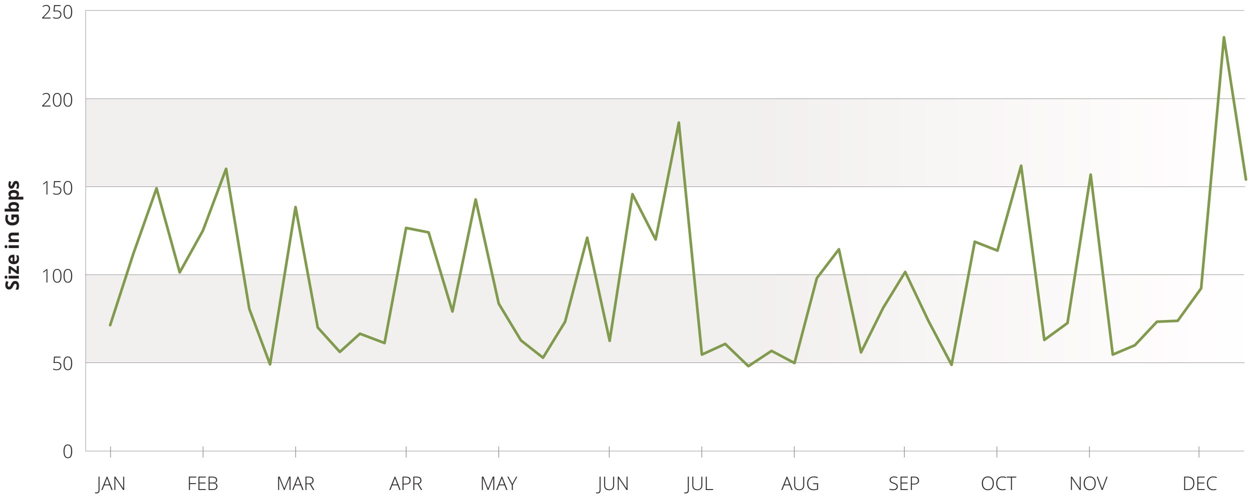


Figure A.12 *Source: Arbor Networks, Inc.*

It is also interesting to note the differences in the trends of mean attack size across the protocols used for reflection amplification. Figure A.13 clearly shows the increase in the average size of attacks utilizing Chargen, SSDP and DNS through 2015. With the average size of DNS reflection amplification attacks growing most substantially. No trends could be discerned for peak attack sizes across reflection amplification protocols.

Average Size Growth of DNS and SNMP Reflection Amplification Attacks

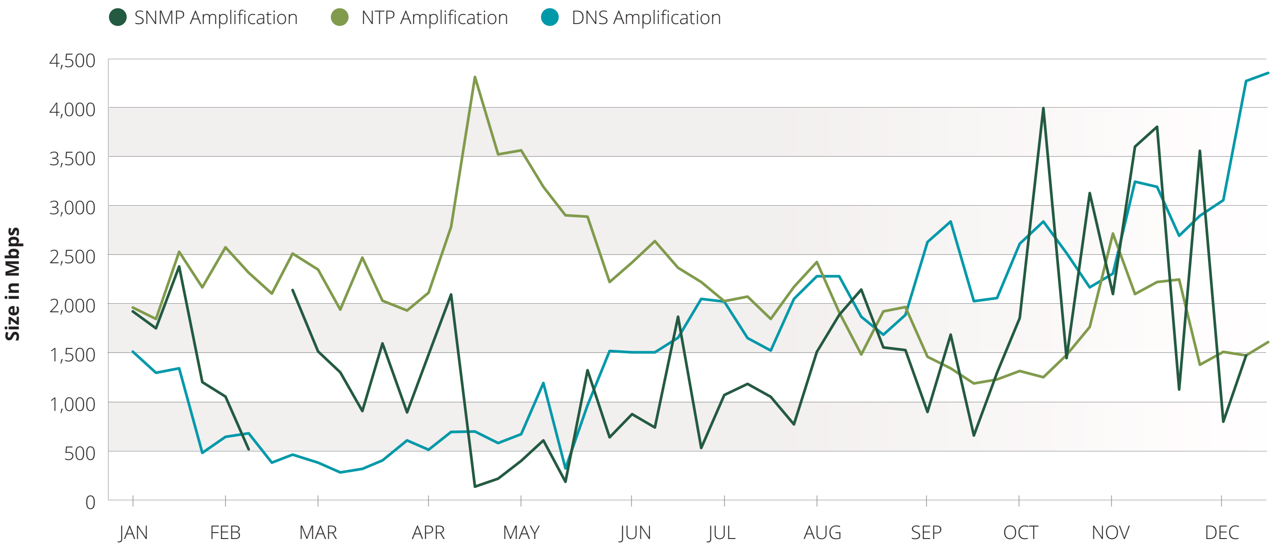


Figure A.13 *Source: Arbor Networks, Inc.*

The top targets of reflection amplification attacks (Figure A.14) are the USA, Canada and France. The most common targets for larger, greater than 10 Gbps reflection amplification attacks, are the same.

Reflection Amplification Target Countries

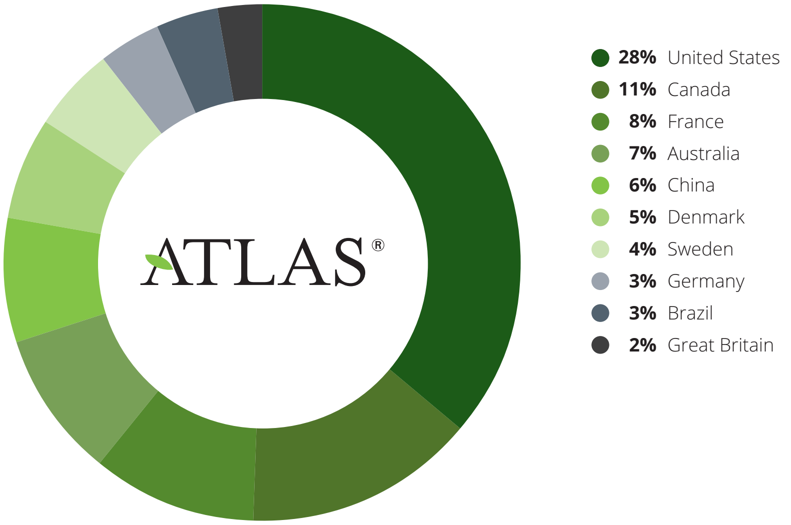


Figure A.14 *Source: Arbor Networks, Inc.*

TYPE, FREQUENCY AND MOTIVATION OF DDoS ATTACKS

In last year's report, we highlighted a resurgence of volumetric attacks in 2013 and 2014. This trend has continued and escalated in 2015, with more and larger volumetric attacks. ATLAS data confirms this, with a clear upward trend in the frequency of attacks in the 2 – 50 Gbps range. The proportion of respondents seeing application-layer attacks has continued to increase, up to 93 percent this year, from 90 percent last year and 86 percent in 2013. This year, we also have a significant increase in those seeing multi-vector attacks on their networks, up to 56 percent from 42 percent last year.

The most common service targeted by application-layer attacks is DNS this year. There is also strong growth in attacks targeting SIP/VoIP services, up from 9 percent last year to 19 percent this year. Last year, 38 percent indicated they experienced more than 21 attacks per month. This year, that has risen to 44 percent. Nine percent of respondents indicate they have witnessed IPv6 attacks. This is a significant increase over the 2 percent seen in previous iterations of this survey.

This year, the top motivation behind DDoS attacks is "criminals demonstrating attack capabilities," with "gaming" and "criminal extortion attempts" in second and third place. In line with other surveys, a growing proportion of respondents are seeing DDoS attacks being used as a distraction for either malware infiltration or data exfiltration. Last year, 19 percent of respondents saw this as a common or very common motivation; this has increased to 26 percent.

DDoS attack vectors vary significantly, and attackers are constantly evolving the methodologies they use to evade defenses and achieve their goals. 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, IPS and the application servers themselves. They can take down even high-capacity devices capable of maintaining state on millions of connections.
3. A**pplication-Layer Attacks:** These target some aspect of an application or service at Layer 7. They are the most sophisticated and stealthy attacks because they can be very effective with as few as one attacking machine generating traffic at a low rate. This makes these attacks very difficult to proactively detect with traditional flow-based monitoring solutions. To effectively detect this type of attack in real time, it is necessary to deploy an in-line or other packet-based component to your DDoS defense.

Looking at the split of attack types experienced by our survey participants (Figure 19), we can see that volumetric attacks are still the most common type of attack. In last year's report, we highlighted a resurgence of volumetric attacks in 2013 and 2014, and this has continued. This year's results show that the proportion of attacks that are volumetric in nature has remained consistent, with the results overall being very similar to last year. It should be noted, however, that although the overall proportion of attacks targeting the application layer has stayed relatively static, the proportion of respondents seeing application-layer attacks has continued to increase, up to 93 percent this year, from 90 percent last year and 86 percent in 2013.

DDoS Attack Types

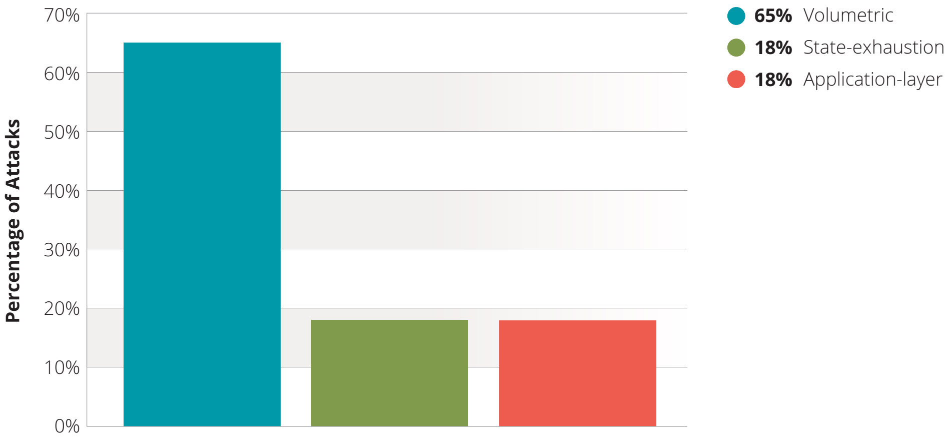


Figure 19 *Source: Arbor Networks, Inc.*

Multi-vector attacks have now been around for many years, and their increased complexity can make it more difficult for defenders to successfully mitigate them. This year, we have a significant increase in those seeing multi-vector attacks on their networks (Figure 20), up to 56 percent from 42 percent last year. Multi-vector attacks are more difficult to deal with, and layered defenses are the best solution. A layered defense lets you proactively deal with more stealthy attacks closer to the target, while the higher magnitude portions of an attack are handled inside the service provider or cloud infrastructure where sufficient capacity is available.

Multi-Vector DDoS Attacks

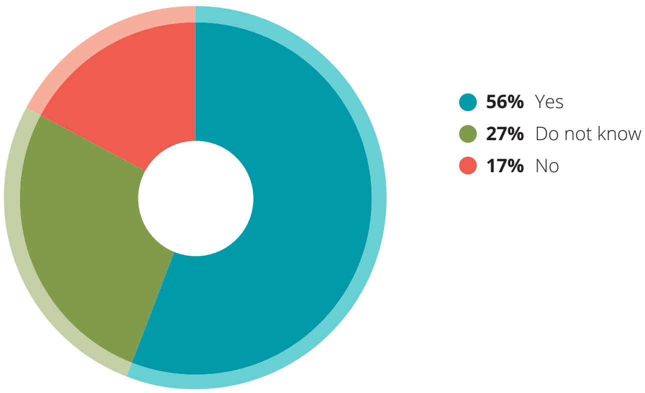


Figure 20 *Source: Arbor Networks, Inc.*

If we focus on the stealthier and more sophisticated (low-and-slow) application-layer attacks, the most common service targeted is DNS this year (Figure 21), with 78 percent seeing attacks. HTTP has been the top targeted service for the past few years, with DNS gaining ground year-over-year to tie for first place last year. Over three-quarters of respondents are now seeing application-layer attacks targeting DNS and HTTP services. This is a common problem. Additionally, there is strong growth in the proportion of respondents seeing attacks targeting SIP/VoIP services, up from 9 percent last year to 19 percent this year.

Targets of Application-Layer Attacks

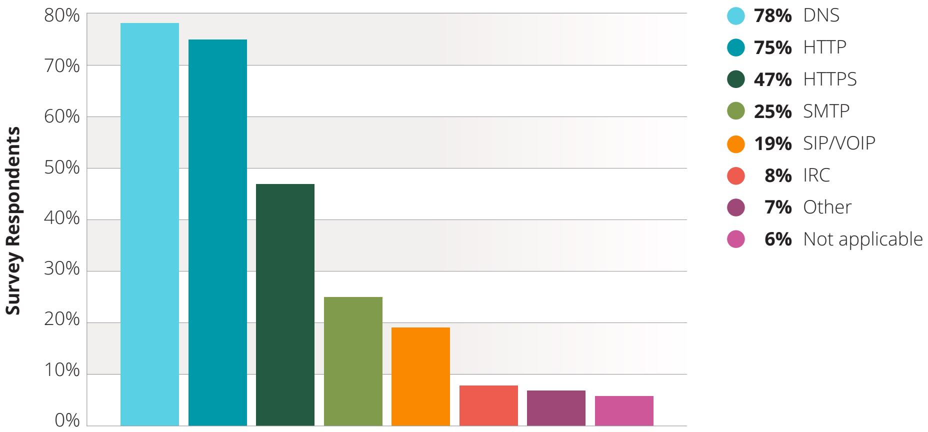


Figure 21 *Source: Arbor Networks, Inc.*

Looking in more detail at the attacks targeting encrypted services (Figure 22), we can organize them into four different categories:

1. Attacks that target the SSL/TLS negotiation.
2. Attacks that target connection state (number of connections).
3. Volumetric attacks that simply flood traffic at service ports.
4. Application-layer attacks that target the underlying service directly over fully negotiated SSL/TLS connections.

Roughly one-fifth of respondents are experiencing attacks in at least one category — but just over half do not know what kind of attacks are happening. While this is an improvement over last year, it still may indicate limited visibility and detection for attacks targeting encrypted services. Given the prevalence of encryption in many services today, especially those provided by financial and e-commerce organizations, a successful attack can have significant impact. Deploying the appropriate defense mechanisms is very important.

Types of Attacks Targeting Encrypted Services

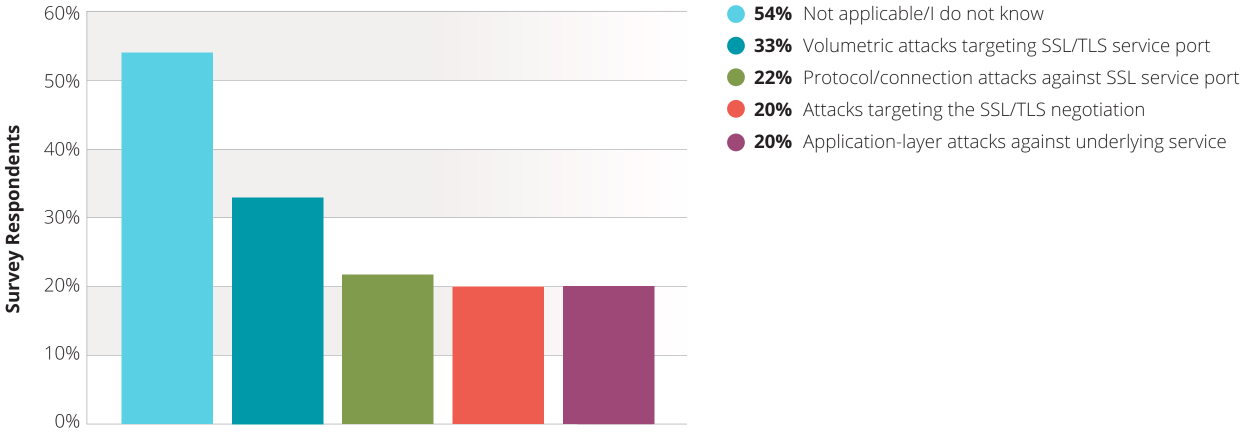


Figure 22 *Source: Arbor Networks, Inc.*

Looking at attack frequency, the number of attacks experienced per month has increased again (Figure 23), revealing a trend of very rapid attack frequency growth. Two years ago, only 25 percent reported seeing more than 21 attacks per month. Last year, that proportion increased to 38 percent, and this year it has risen to 44 percent. This trend backs up anecdotal feedback from Arbor customers, who indicate they have seen significantly more and larger attacks during this survey period.

Attack durations generally remained about the same as last year. Just over half indicate that the longest duration attack they have monitored over the last year was six hours or less (Figure 24). However, the proportions of respondents seeing attacks lasting longer than a week or a month have increased this year.

Attack Frequency

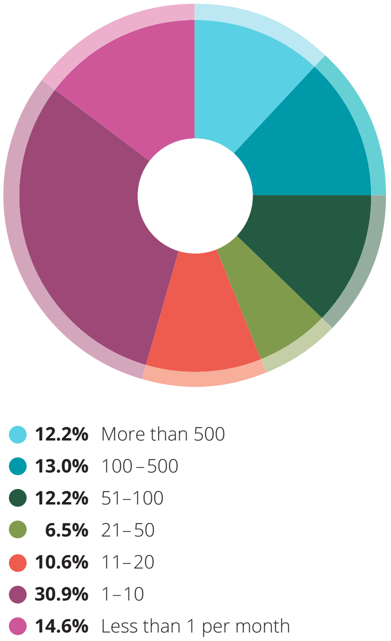


Figure 23 *Source: Arbor Networks, Inc.*

Longest Attack Duration

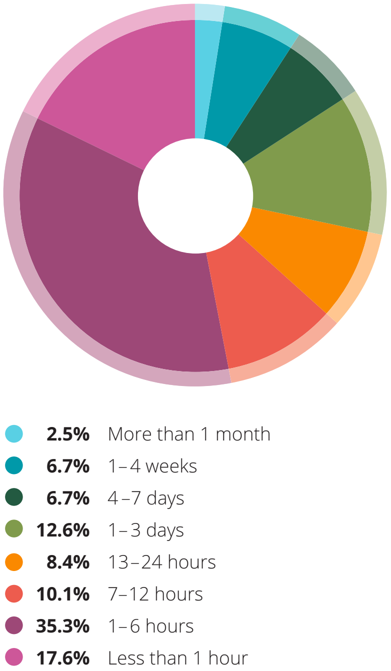


Figure 24 *Source: Arbor Networks, Inc.*

As in previous iterations of this survey, we asked respondents what they feel are the common or very common motivations behind the DDoS attacks they have monitored on their networks. Historically, ideological hacktivism has commonly been the top motivation, only displaced last year by nihilism/vandalism. This year, however, things have changed.

The top motivation is “criminals demonstrating attack capabilities,” with “gaming” and “criminal extortion attempts” in second and third place (Figure 25). Gaming is not a surprise, as the various storms of attacks surrounding gaming providers and users have been ongoing for the last 18 months, and are well known. The rise of extortion is also expected given the broad use of DDoS in this regard — e.g., in the DD4BC attack campaign (see ASERT DD4BC insert).

The rise of “criminals demonstrating their capabilities” is indicative of the ease with which DDoS attacks can now be procured and carried out for any and all reasons. The proliferation of booter/stresser services is a growing and serious problem.

In line with other surveys, a growing proportion of respondents are seeing DDoS attacks being used as a distraction for either malware infiltration or data exfiltration. Last year, 19 percent saw this as a common or very common motivation; this has increased to 26 percent — backing up other surveys and reports that have shown growth in this area.

DDoS Attack Motivations

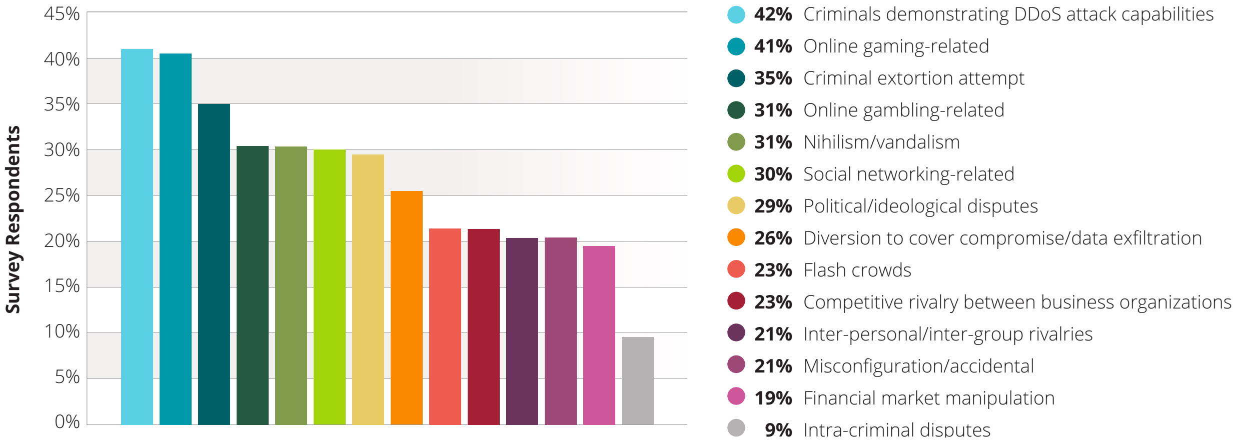


Figure 25 *Source: Arbor Networks, Inc.*

Last but not least, we asked service providers if they have monitored any IPv6 DDoS attacks during the survey period. While the majority have not (Figure 26), 9 percent indicate they have witnessed IPv6 attacks. This is a significant increase over the 2 percent seen in previous iterations of this survey.

Among those service providers reporting IPv6 DDoS attacks, the largest reported was 6 Gbps. Only one other large attack was reported at 2 Gbps, with other respondents indicating much smaller attacks.

IPv6 DDoS Attacks

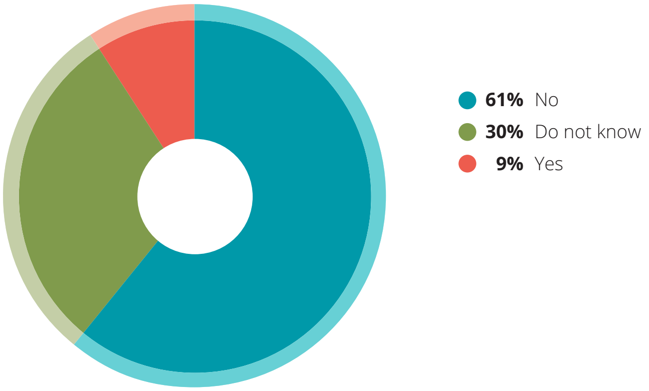


Figure 26 *Source: Arbor Networks, Inc.*

ASERT DD4BC: SUMMARY

For the last year or so, an individual or organization calling itself DD4BC ("DDoS for Bitcoin") has been rapidly increasing both the frequency and the scope of its DDoS extortion attempts. Over time, DD4BC has shifted its target demographics from Bitcoin exchanges, to online casinos and betting shops and, most recently, to prominent financial institutions (banks, trading platforms, payment acquirers) across the United States, Europe, Asia, Australia and New Zealand. Other verticals receiving extortion threats include ISPs and publishing, with indicators that higher education may have also been targeted. This section is a summary of a previously published ASERT Threat Intelligence Brief (2015-4 DD4BC DDoS Extortion Activity). It provides an overview of these attacks and outlines the tactics, techniques and procedures (TTPs) utilized by the threat actor(s). For further details, please consult the full ASERT Threat Intelligence Brief.

Executive Summary

News and other security organizations have been discussing the DD4BC (DDoS for BitCoin) attacker or attack group that has been subjecting various targets to extortion-based DDoS attacks. Despite a bounty of at least $26,000 (110 BTC) for information about DD4BC, these attacks persist. A higher volume of extortion letters continue being sent as of mid/late May and early June 2015.

Indicators show that DD4BC extortion DDoS attacks started sometime around July of 2014 and continue as of this writing in early June 2015. Extortion demands have increased recently to 100 BTC, depending upon the targeted vertical. Initial targets were in the online gambling arena. However, ASERT is aware of more recent attacks that have focused on other organizations, including several financials (banks, trading platforms and payment acquirers), publishers and potentially higher education targets. This suggests that DD4BC is diversifying in its attempt to generate funds.

Initial warning/assessment attacks are smaller, typically 10-15 Gbps. But the full attack launched after the victim refuses to pay the extortion demand has been reported as high as 40–60 Gbps. DD4BC has consistently advertised 400–500 Gbps of DDoS capacity. Yet if this capacity is available, it is not being used. The more likely scenario is that capabilities are being overstated. Despite this probable scenario, organizations should be aware that the potential for 400+ Gbps attacks clearly exists within the overall DDoS threat landscape, even if DD4BC does not wield such capabilities at this time. Organizations that are not prepared are highly likely to experience outages.

The bulk of observed attacks launched by DD4BC are SSDP and NTP reflection/amplification attacks, along with the occasional SYN flood and, most recently, Wordpress XML-RPC reflection/amplification attacks.

While the potential for threat actor evolution and increased DDoS capability is present, well-prepared organizations shouldn't have any trouble defending against such attacks using a combination of organic detection/classification/traceback/mitigation techniques, as well as cloud-based DDoS mitigation services. Indeed, ASERT originally warned about such attacks well over a year ago. Subsequently, ASERT provided its customers, as well as the community at large, with insights and a prolific amount of information regarding reflection/amplification attacks, along with information on what can happen when targeted organizations are unprepared. These materials provide in-depth information about how these attacks work, why they work, and precisely how to mitigate them using Arbor products and services, together with other network-based mitigation strategies. For more details, please see asert.arbornetworks.com.

Attack Tactics, Techniques and Procedures (TTPs)

Multiple indicators suggest that DD4BC may be using booter/stresser services to perform its attacks. Booter and stresser services are plentiful in the underground. While many operators of booter/stresser services overstate their capabilities, they are still a force to be reckoned with, especially if the network and hosts are unprepared for the various attacks that can be easily and cheaply launched. All of the commodity DDoS attacks from the past are now available in the stresser services, and as new attack techniques are discovered, they eventually make their way into the stressers. Booter code gets stolen, leaked, modified and re-used, which results in a lot of the same types of attacks being available to a wide population of miscreants. Lists of servers vulnerable to the various types of UDP reflection/amplification attacks are also known to be shared among some of the services, which results in more widespread abuse. At least one booter service advertises an API that allows users and site administrators to find reflection/amplification servers.

Before or during the delivery of the extortion payment message, the attacker(s) often launch a small attack which they reference in the extortion letter. This first "warning shot" is designed to send a message that the attack is real, but it may also serve as a generic test to assess DDoS defenses. If the site falls over easily, then the attacker(s) may have found a lucrative target. It should be obvious that no one should pay the ransom. Doing so only encourages the criminals to return to a soft target to extort more money, and further encourages their continued criminal campaigns.

If the site experiences an outage, or if the target does not pay the ransom, then a larger attack will typically commence, which may involve more in-depth attack techniques. In many cases in 2014, the heavier attacks would arrive shortly after the deadline had passed, although recent trends suggest a longer delay may be experienced. In some cases, the attacker(s) do not bother the target again after issuing the initial extortion email, even if the victim does not respond. In other cases, attacks have caused serious outages. In one instance (Exco.in), another attacker(s) (or related attacker(s)) took advantage of the confusion caused by the DDoS to deeply penetrate the business and engage in theft of all the bitcoins. This represented a painful financial loss for site operators and all users who had trusted the site with their funds.

Ransom Payment Infrastructure

Other researchers have speculated that DD4BC is using a new BTC address for each victim. In some cases, however, the same BTC addresses have been used for more than one attack. It is also possible that these addresses are used for other financial transactions that are not related to the extortion campaigns, because various transactions have been observed that fall far below even the apparently negotiated/reduced extortion amounts that have been shared publicly. This suggests other transactions are taking place that might provide for some opportunity for research and/or law enforcement investigation. In other cases, it's possible that a negotiated amount was decided upon in private.

Attribution

Attribution is sometimes a very helpful process to help locate miscreants and bring them to justice. In other cases, the attention of being identified is enough to cause an attacker to modify its behavior. Professional criminals aren't as likely to change their ways, however, and won't be scared off as easily. Although we cannot be absolutely certain of this assessment, we believe that DD4BC is one person. The volume of attacks, frequency of attacks, lack of follow through in several cases and the fact that the earlier extortion mails tend to be written in first-person singular are all factors in this assessment. Later extortion mails used the phrasing "we," perhaps in an attempt to overstate the threat and increase extortion payments by positioning the threat actor as part of a group. However, the continually observed TTPs still suggest a singular threat actor at play.

Mitigation

Even though DD4BC seemingly can't deliver on the threatened hundreds of Gbps promised in extortion emails, it often doesn't matter. Much lower volume attacks often succeed due to the unpreparedness of defenders. On the other hand, well-prepared organizations shouldn't have any trouble defending against these and even much larger attacks that may come from DD4BC, copycats or other adversaries. ASERT originally warned about the potential scale of reflection/amplification attacks well over a year ago. This was well documented in last year's Worldwide Infrastructure Security Report. Subsequently, ASERT provided its customers, as well as the community at large, with insights and a prolific amount of information regarding reflection/amplification attacks. These materials provide in-depth information about how these attacks work, why they work and precisely how to easily mitigate them using Arbor products and services, as well as other network-based mitigation strategies.

Conclusion

Despite the arrest of individuals in relation to DD4BC, attacks will continue. Copycat attackers have already emerged and are actively engaged in attack campaigns (e.g. The Armada Collective). A perfect storm of network architecture weaknesses due to misconfiguration, ease of launching attacks, unprepared targets and anonymized digital currency sets the stage for lucrative criminal gain with minimal risk to the perpetrators. The key is to be prepared, because even if DD4BC is prosecuted, attacks will likely increase in intensity and volume over time as trends from the last several years indicate. As a result of the painful downtime experienced by the targets in these campaigns, organizations should realize that they must institute defenses sooner rather than later, and begin taking steps to avoid devastating service disruptions. Organizations that are threatened should also report the threats and attacks to their law enforcement contacts. We invite such organizations to share meaningful attack data with Arbor ASERT, if possible.

DDoS THREAT MITIGATION

Again this year, more respondents (73 percent) are using intelligent DDoS mitigation systems (IDMS) rather than ACLs to mitigate DDoS attacks. However, the gap has narrowed. The proportion of respondents able to mitigate attacks in less than 20 minutes has increased once again this year to 74 percent, up from 68 percent last year and 60 percent the year before. The trend of increased interest in DDoS detection and mitigation services continues this year, with 74 percent of service providers seeing more demand from customers, up 4 percent over last year.

Looking at the techniques used by respondents to mitigate DDoS attacks, once again more respondents (73 percent) are using IDMS rather than ACLs this year (Figure 27) — although the gap has narrowed. IDMS usage has increased in percentage terms, which is a very encouraging trend in the application of the surgical mitigation technologies needed to deal with today's DDoS threat.

Also encouraging is the decreasing trend in those using IPS to mitigate DDoS events, down to only 22 percent from 31 percent last year. And, last but not least, it is also positive that the percentages using either source or destination-based black hole to mitigate attacks have increased.

Attack Mitigation Techniques

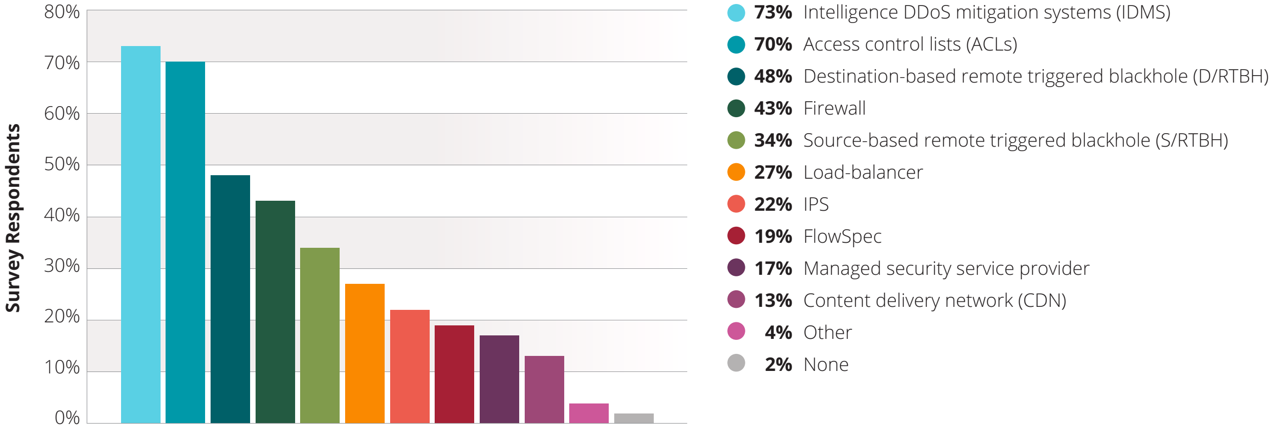


Figure 27 *Source: Arbor Networks, Inc.*

One negative finding is that the use of firewalls for DDoS mitigation has increased slightly, from 40 percent of respondents last year to 43 percent this year. While firewalls can deal with some DDoS attacks, these devices can suffer from state-exhaustion issues — making them susceptible to DDoS attack.

The proportion of respondents able to mitigate attacks in less than 20 minutes has increased once again to 74 percent this year (Figure 28), up from 68 percent last year and 60 percent the year before. This is a very positive finding. Interestingly, the 6 percent increase in those who can mitigate in less than 20 minutes is mirrored by a 6 percent increase in those using automated mitigation techniques.

Average attack durations are relatively short for volumetric reflection amplification attacks (20 minutes), although they can be repeated periodically to form longer attack “stop-start” cycles. This gives service providers a relatively short time to react, as they are the ones that need to mitigate these higher magnitude attacks. Overall, it appears that things are continuing to move in the right direction.

Time to Mitigate

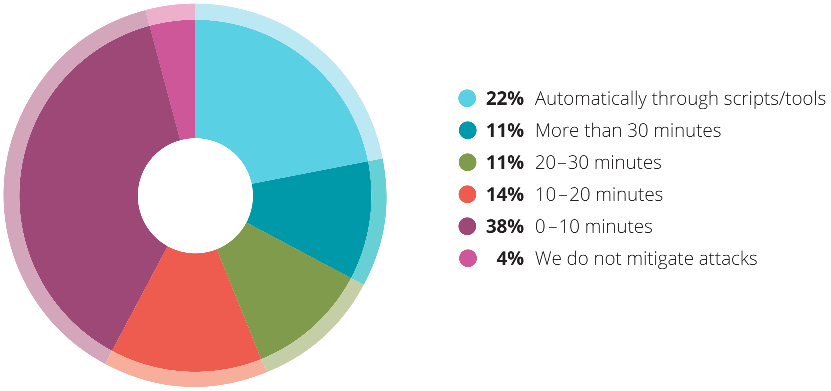


Figure 28 *Source: Arbor Networks, Inc.*

We asked respondents what proportion of the attacks detected on their networks were outbound or cross-bound. About 40 percent (Figure 29) indicate that they do NOT detect outbound or cross-bound attacks at all. While this is an improvement over last year, it still indicates a lack of visibility in this area. This is a concern, as these attacks can impact customer aggregation routers, peering and transit capacity. Ideally, organizations should detect and deal with outbound and cross-bound attacks in the same way as inbound attacks. Among respondents who do detect outbound or cross-bound attacks, 41 percent report them as less than 10 percent of all events detected on their networks.

Looking at the mitigation of outbound attacks, 39 percent of respondents indicate that they have mitigated an attack — an almost identical result to last year.

Outbound/Cross-Bound Attack Detection

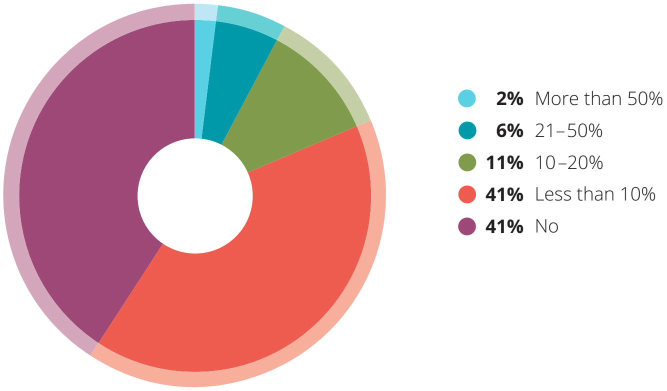


Figure 29 *Source: Arbor Networks, Inc.*

The trend of increased interest in DDoS detection and mitigation services continues this year, with 74 percent of service providers seeing more demand from customers, up 4 percent over last year (Figure 30). More interestingly, no respondents indicate reduced demand for DDoS detection and mitigation services this year. This should come as no surprise, given the increasing enterprise focus and awareness around availability threats.

Demand for DDoS Detection/Mitigation Services

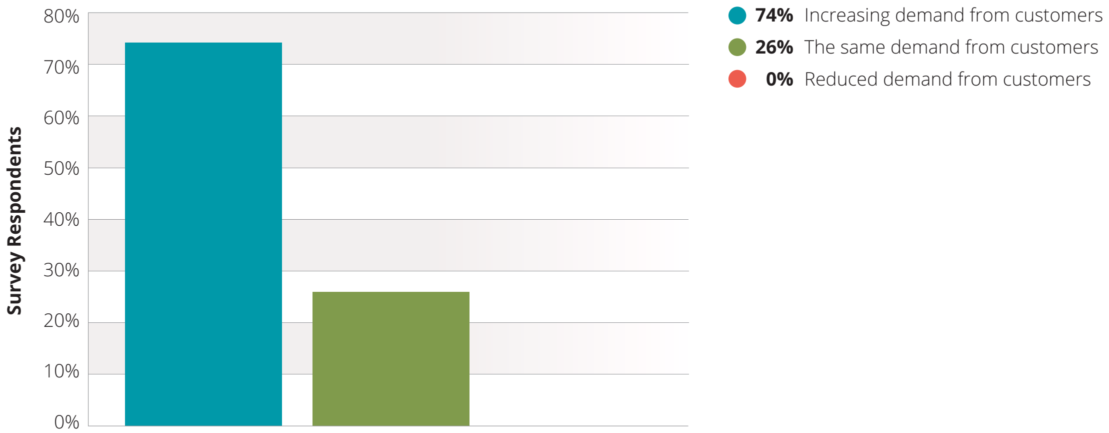


Figure 30 *Source: Arbor Networks, Inc.*

As with last year's survey, we drilled into the demand for these services in more detail to try to establish which verticals are driving the increase (Figure 31). Finance, government and cloud/hosting providers are in the top tier of verticals interested in these services, as per last year's results. One surprising development is the 10 percent reduction in those citing demand from e-commerce companies. However, we did see an increase in demand across virtually all of the other verticals over last year. This indicates that a wide variety of organizations are now aware of — and looking for — solutions to the DDoS threat.

Business Verticals for DDoS Services

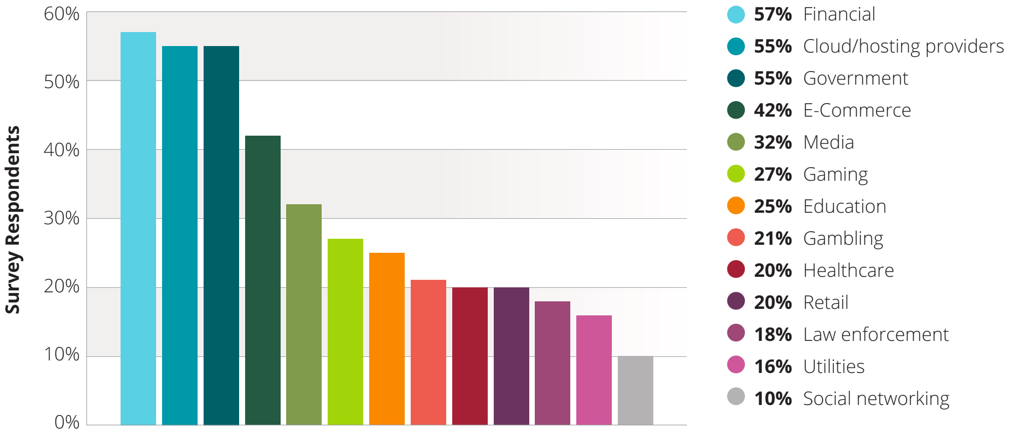


Figure 31 *Source: Arbor Networks, Inc.*

CORPORATE NETWORK SECURITY

This year, we see a small increase in the proportion of service provider respondents who have incident response plans in place, up 2 percent to 82 percent. More organizations having plans is positive, but this is tempered by the fact that fewer respondents have well-resourced teams — down from just under one-third to 25 percent. This year, the proportion of respondents who have contracted with external organizations to assist with incident response has increased by 11 percent. This shows willingness in the industry to seek external help as needed.

The most common threat seen by service providers against their corporate networks is Internet congestion due to DDoS attacks, with an even greater proportion expressing concern about this in the future. The proportion that has experienced advanced persistent threats (APTs) on their corporate network is around 10 percent, similar to last year. However, last year just over one-third of respondents were concerned about APT activity in the next year; this year, that has increased to 44 percent.

Almost one-third of respondents have reduced the time taken to discover an APT in their network to under one week. Even more positively, 52 percent of respondents state that they also have their discovery-to-containment time down to under one month. Looking at the risks associated with a successful incursion by an APT, loss of personal information is the number one concern, with reputational damage and disruption to business processes not far behind.

Again this year, over half of respondents saw an increase in incidents on their corporate networks, with only 6 percent reporting a decrease. Over half state that they are reasonably well prepared to deal with a security incident, a 12 percent increase from last year. As in previous years, NetFlow analysis and firewalls are the two most popular mechanisms used to detect threats within the corporate network, with the proportion of respondents using firewalls growing by 8 percent. In contrast, the use of NetFlow analysis tools has fallen by 9 percent this year. In past surveys, manual detection was the number one way respondents detected breaches. While manual detection is still in the top three, detection via routine checks and controls has replaced manual detection as the number one mechanism for detecting a security incident. This year, 20 percent of respondents indicate that they have cyber security insurance in place, an increase from 13 percent last year.

Seventy percent of service provider organizations feel their corporate network user community is properly educated around cyber security, with almost 60 percent regularly updating their security education and requiring re-certification of employees. This year, 11 percent of respondents indicate that they have seen a breach or security incident related to a BYOD device, a significant increase to previous surveys.

Last year was the first time this survey dedicated a section on the capabilities of service providers in dealing with incidents on their own internal corporate networks. This year, we observed some changes. However, it is too early to be able to identify long-term trends.

This year, we see a small increase in those who have incident response plans in place, up 2 percent to 82 percent (Figure 32). However, 2 percent of organizations now outsource their incident response plans, as opposed to zero last year. More organizations having plans in place is positive, but this is tempered by the fact that fewer respondents have well-resourced teams — down from just under one-third to 25 percent. Anecdotally, based on recent visits to major banks and media companies, Arbor has observed a doubling (or more) in IR team headcount, with the establishment of dedicated hunting teams — enabling more proactive security — becoming more common.

Incident Response Posture

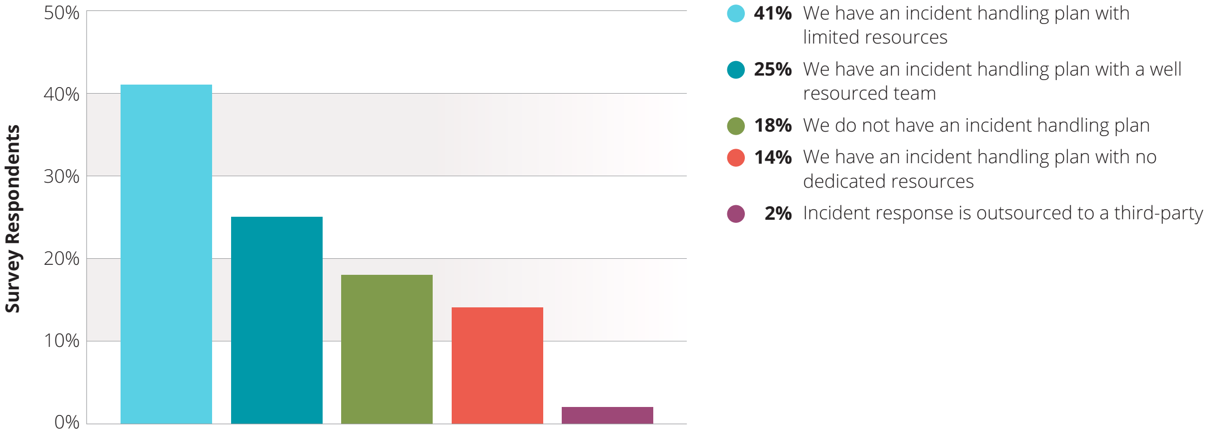


Figure 32 *Source: Arbor Networks, Inc.*

This year, the proportion of those who have contracted with external organizations to assist during incident response has increased 11 percent (Figure 33). This is a positive sign, and shows willingness in the industry to seek external help as needed. It is also in line with studies conducted by the Ponemon Group and the Economist Intelligence Unit that also indicate a growing number of organizations seeking outside help.

Incident Response Assistance

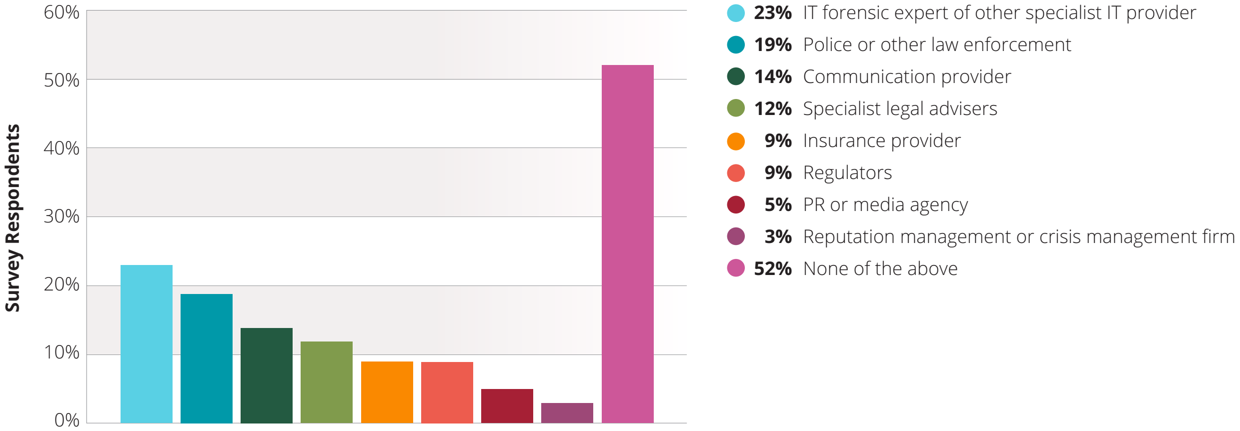


Figure 33 *Source: Arbor Networks, Inc.*

Looking at the types of organizations our respondents have contracted with, it is interesting to note that the most common type — "IT forensic expert or other specialist IT" — has remained at a similar level. However, there have been increases in those working with law enforcement (up from 12 percent to 19 percent), specialist legal advisers (up from 7 percent to 12 percent) and communication providers (up from 8 percent to 14 percent). Although all of these percentages are still relatively low, they are growing.

The most commonly observed threat vector experienced on the corporate networks of service providers is Internet connectivity congestion due to DDoS attack, similar to last year (Figure 34). This is reported by 57 percent, a 2 percent increase over last year. Interestingly, the second most commonly observed threat this year is Internet connectivity congestion due to genuine traffic. This was experienced by 34 percent of respondents, up 6 percent from last year — pushing botted or otherwise compromised hosts down into third place.

The proportion of respondents experiencing APT remains about the same as last year, at around 10 percent. It is important to point out that given other recent studies, as well as feedback from Arbor customers and potential customer interactions, there is significant concern that cyber criminals can use DDoS activity to mask as yet undiscovered APTs or other forms of orchestrated attacks. All organizations should be conscious of this.

This year, we also see small increases in the proportion of respondents experiencing accidental data loss, web defacement and theft. The proportion experiencing no issues has dropped from 21 percent to 18 percent.

Threats Observed on Corporate Networks

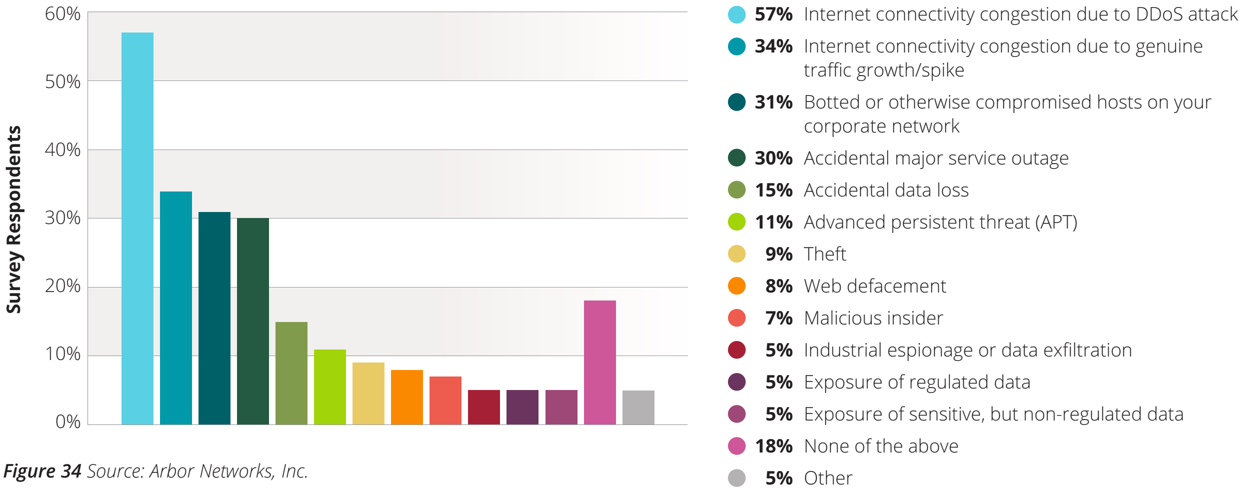
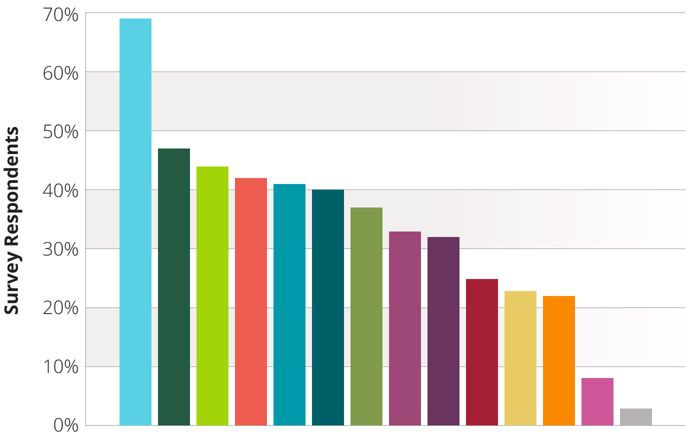


Figure 34 *Source: Arbor Networks, Inc.*

In terms of forward-looking concerns, DDoS attacks remain at the top, with an almost identical proportion of organizations to last year worried about this area (Figure 35). Concerns around accidental data loss and exposure of data also remain fairly steady, but there are some significant changes elsewhere.

This year, the proportion of organizations concerned about malicious insiders has increased by 16 percent, to just under one-half of respondents. Anecdotally, the industry has a healthy respect for this threat and is acting accordingly. This year, concerns around APT have also continued to increase. Last year, just over one-third of respondents were concerned about APT activity during the next year. This year, that has increased to 44 percent.

Corporate Network Concerns



- ● **69%** Internet connectivity congestion due to DDoS attack
- ● **47%** Accidental major service outage
- ● **44%** Advanced persistent threat (APT)
- ● **42%** Malicious insider
- ● **41%** Internet connectivity congestion due to genuine traffic growth/spike
- ● **40%** Botted or otherwise compromised hosts on your corporate network
- ● **37%** Accidental data loss
- ● **33%** Exposure of sensitive, but non-regulated data
- ● **32%** Exposure of regulated data
- ● **25%** Industrial espionage or data exfiltration
- ● **23%** Theft
- ● **22%** Web defacement
- ● **8%** None of the above
- ● **3%** Other

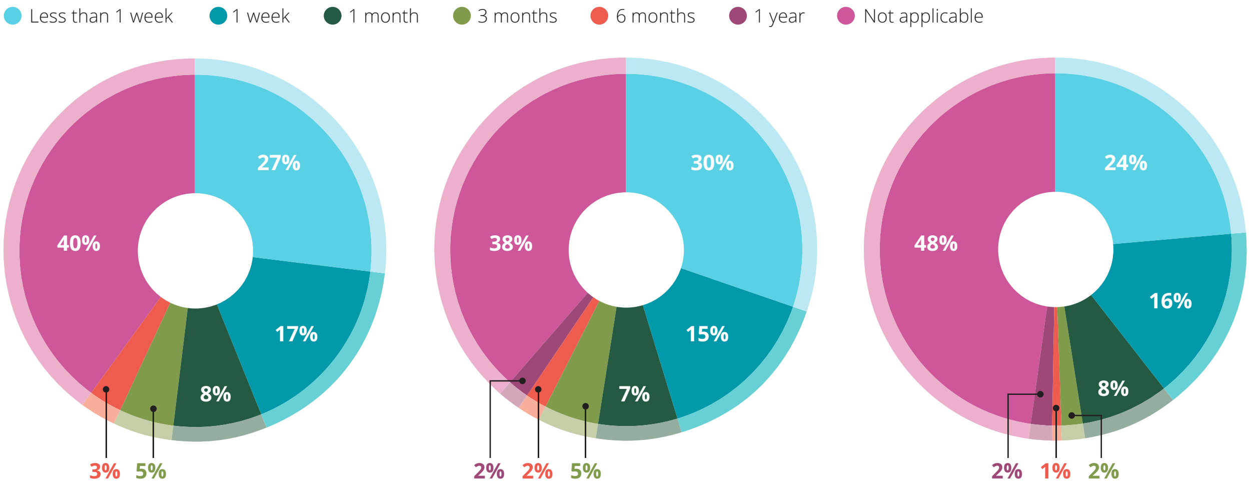
Figure 35 *Source: Arbor Networks, Inc.*

Last year, for the first time, the WISR attempted to capture some metrics around incident response time. This year, the questions are more focused and clearly stated.

Time-to-discovery of compromise has steadily improved in the last few years. Just two years ago, a nine-month compromise-to-discovery time was considered normal in many organizations. This year, the survey shows that almost one-third of respondents have reduced this time to under one week, with more than half reducing it to less than a month (Figure 36).

Even more positively, 52 percent state that they also have discovery-to-containment time down to one month or less. And, almost half of respondents state that their discovery-to-external-notification time is now a month or less. These results are a huge improvement and good news for consumers who entrust their personal data to service provider organizations. With the continued investments occurring, we expect to see further improvements here in the future.

Response Times for APT



Average time from compromise to discovery

Average time from discovery to containment

Average time from discovery to external notification

Figure 36 *Source: Arbor Networks, Inc.*

Looking at the risks associated with a successful incursion by an APT, loss of personal information is the number one concern for organizations, with reputation damage and disruption to business processes not far behind (Figure 37). The appreciation of the key risks of a successful APT attack is positive, and indicates that service providers have a "tackle it now" rather than a "wait and see" attitude in this area. It is interesting to note that loss of intellectual property came in as the lowest risk, but this could be due to the fact that service providers have intellectual property that would be more difficult to convert into monetary gain for a third party.

Risk of APT Incursion

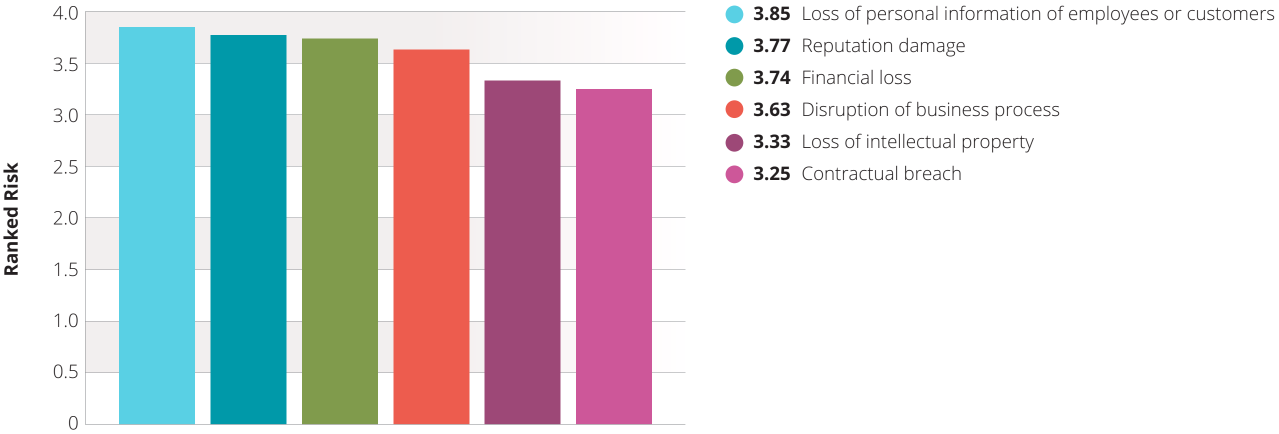


Figure 37 *Source: Arbor Networks, Inc.*

Similar to last year, over half of respondents indicate they have seen more incidents in this survey period than they had previously (Figure 38). There are, however, fewer respondents reporting a significant increase — a drop from 14 percent to 9 percent this year. This indicates that although fewer organizations are seeing pronounced rises in incident volume, the number of incidents is still increasing in many cases.

Because the costs associated with successful attacks continue to rise, organizations should be prepared to reverse the current trend of reducing onsite team funding. Note the reduction in well-resourced IR plans discussed earlier in this section. Obviously, preventing a breach is far more cost-effective than dealing with one.

Incident Rate Change

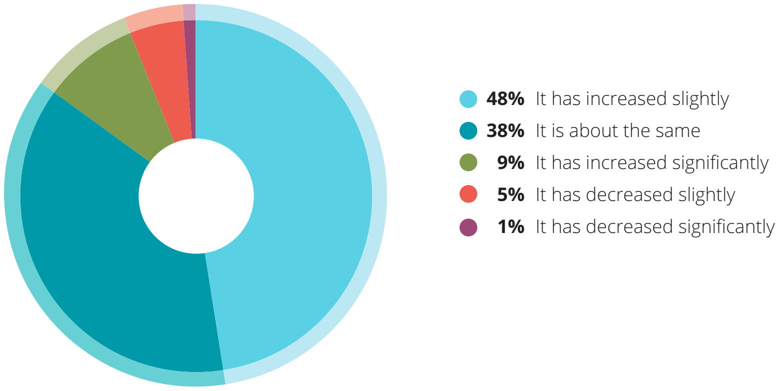


Figure 38 *Source: Arbor Networks, Inc.*

Similar to last year, most organizations say they have some level of IR preparedness, and the majority — 56 percent — report that they are reasonably prepared (Figure 39). This is a 12 percent increase from last year, and is very positive. Additionally, the proportion of respondents who feel "totally unprepared" dropped by 3 percent, not a radical change but still an improvement.

As a final note, the proportion of organizations that state they are fully prepared fell by 1 percent this year, possibly due to respondents either gaining additional experience or seeing reductions in funding. Anecdotal evidence suggests that executives in many service provider organizations fully understand the imperative to secure customer data, and funding issues are improving.

Incident Response Preparedness

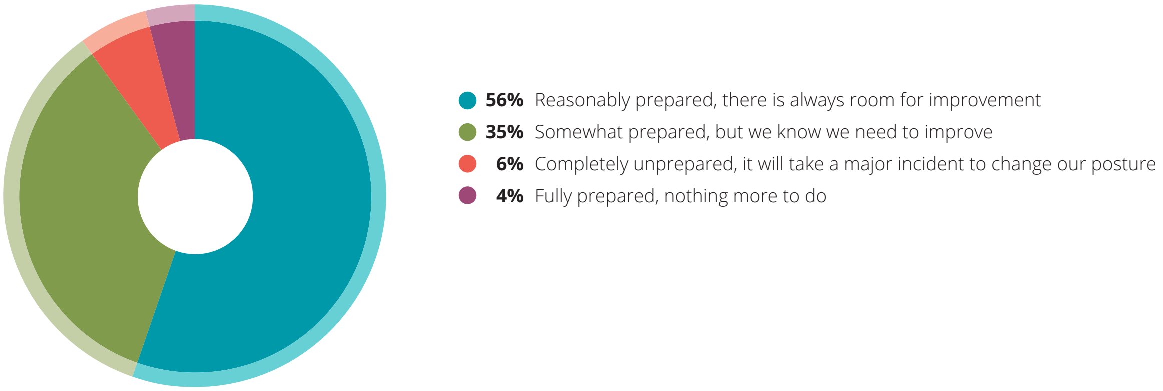


Figure 39 *Source: Arbor Networks, Inc.*

When we asked service providers how they would improve their incident handling, the responses are very similar to last year (Figure 40). This consistency illustrates that the four most important aspects of IR in the IT security world — automated tools, better intelligence, end user education and faster tools — are well-known and accepted standards. This does not mean the problem is solved, but a framework can be derived and strong recommendations for improvement postulated in many organizations.

A three-tier system of IR responders and a two-tier system of tools are becoming viewed as a best-practice approach for incident response. Tier-one IR analysts monitor commodity tools and report to a central repository for action. When an alert does not have a related, predefined procedure, it is passed on to a tier-two IR analyst, who then uses non-commodity tools such as PCAP and NetFlow analyzers to dig further into the incident. When an event surpasses the tier-two IR responder's knowledge, it is passed on to a tier-three analyst. Tier-three analysts also train tier-two analysts for career progression, knowledge dissemination, etc.

Using a model like the above, organizations can properly scale resources and reverse the commodity triangle of increasing support costs versus buying new tools and investing in training to allow promotion and skills conservation within an organization.

Incident Response Improvements

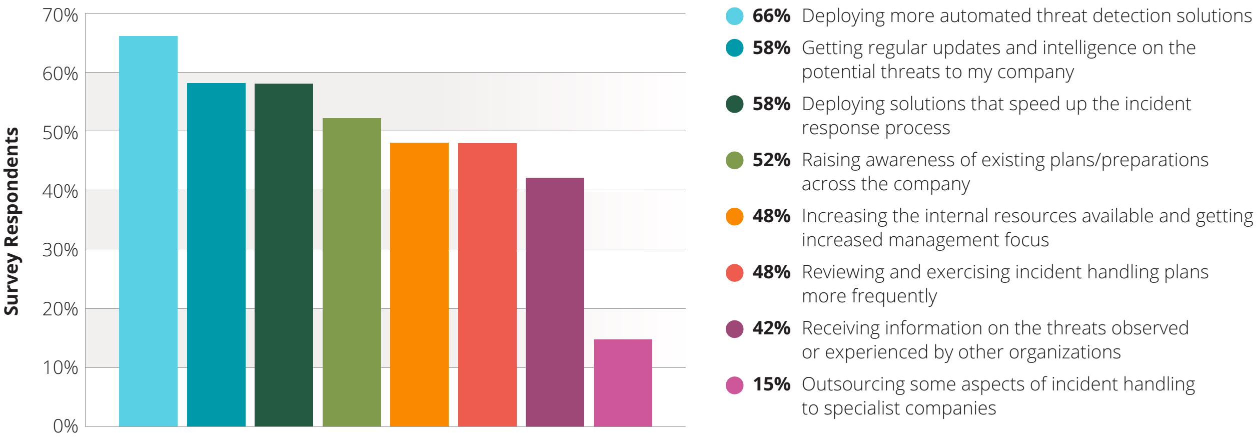


Figure 40 *Source: Arbor Networks, Inc.*

When it comes to detecting threats within the corporate network, the variety of tools being used by many respondents make it obvious that security is like an onion in many organizations (Figure 41). The more layers we have, the safer we feel. As in previous years, NetFlow analysis and firewalls are the two most popular mechanisms used, with the proportion of respondents using firewalls growing by 8 percent. In contrast, the proportion using NetFlow analysis tools has fallen by 9 percent this year. Even with this reduction, NetFlow is still more than twice as widely used as packet analysis, which seems to have fallen back this year.

As expected, technologies such as sandboxes continue to see incremental deployment, with 27 percent using these devices this year, up from 14 percent last year. SIEM is also more widely deployed at 50 percent, up from 43 percent last year.

SIEM is a part of the commodity tool layer discussed above, as are firewalls, UTM and NGFW. Both commodity tools and point solutions are required to give organizations the level of protection and visibility they need to deal with today's threats. SIEM was supposed to be the "single pain of glass" view into our environments, but has proven too costly to maintain in terms of both money and people for most companies. The biggest companies do more with SIEM than the smaller, but as evidenced below, direct analysis tools are far and away the preferred method of choice for threat detection.

Internal Network Threat Detection

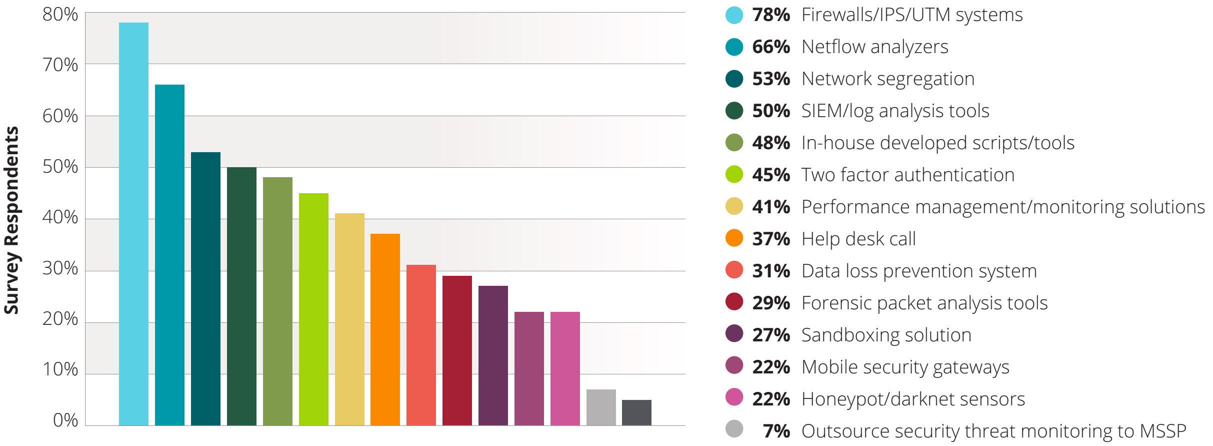


Figure 41 *Source: Arbor Networks, Inc.*

In past surveys, manual detection was the number one way most respondents actually detected security incidents. While manual detection is still in the top three methods, detection via routine checks and controls has replaced manual detection as the number one mechanism (Figure 42). Automated tools, such as SIEM and other security products, move down to number three this year. This indicates that processes put into place to respond to threats are becoming more effective, which in turn may indicate that end-user education is helping to protect our networks and data. The rest of the detection methods queried basically remain the same or see a nominal increase, the only exception being that customer and media notification declined about 6 percent. This drop may indicate that organizations are getting better at policing their own data, preferring to avoid the embarrassment of external notification of security issues.

Historically Detected Incidents

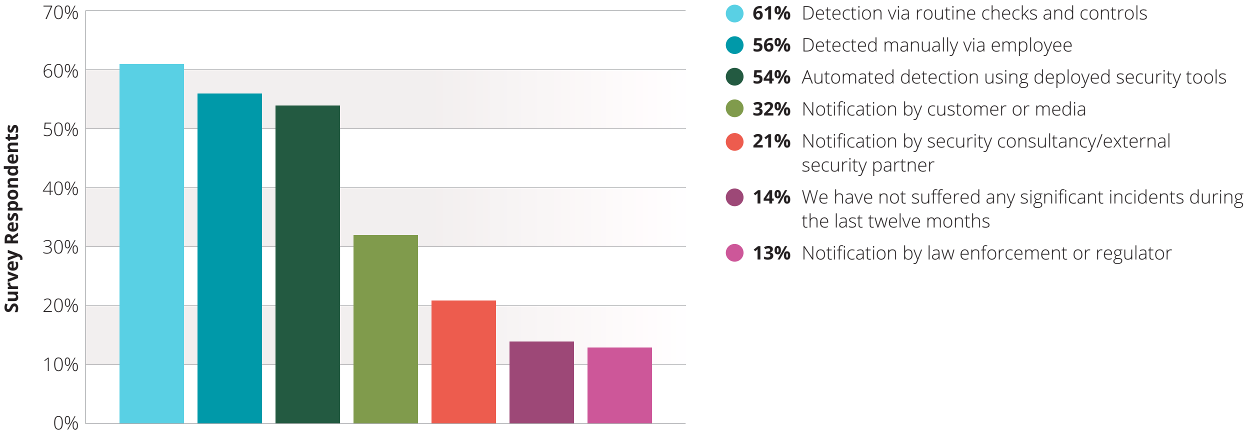


Figure 42 *Source: Arbor Networks, Inc.*

This is the second year the survey has asked about cyber security insurance, giving some historical frame of reference around the adoption of this particular practice. This year, 20 percent of respondents indicate that they have insurance in place (Figure 43), an increase from 13 percent last year. Nine percent indicate that they plan to look into insurance over the next 12 months. Anecdotally, we know that some executives are considering some form of cyber insurance after speaking with their peers about it. These engagements are mostly with financial service organizations, but discussions are propagating rapidly across all industries, as evidenced later in this survey.

Cyber Security Insurance

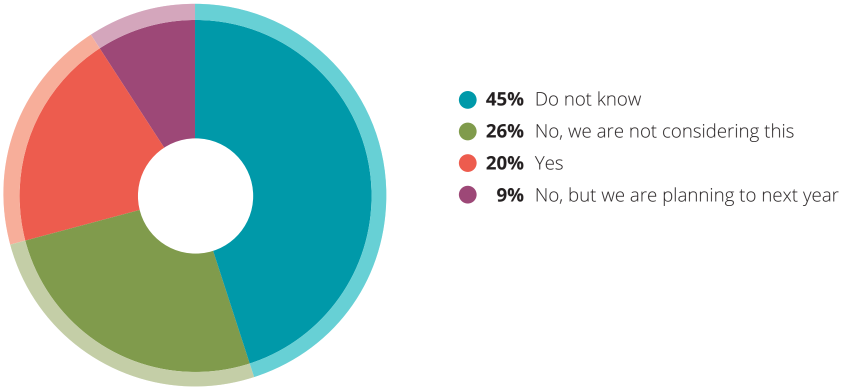


Figure 43 *Source: Arbor Networks, Inc.*

This year, we introduced some new questions directed at the end user community within respondent organizations. First, we inquired about the state of end user education on basic security — i.e., are users taught not to click on email links, not to disable the local firewall or AV, etc.? Encouragingly, 70 percent of service provider organizations feel their corporate network user community is properly educated.

It is important to keep current security issues top of mind for employees. As a result, we added a second question to this year's survey to establish if organizations regularly update their employees' security training and require periodic re-certification. Almost 60 percent of respondents update their security education and require regular re-certification. This is a positive result, but is unsurprising in the service provider space, given the technical nature of the business.

The Internet of Things (IoT) makes most networks (except for the most firmly controlled) much more vulnerable to APT, AT and the whole alphabet of threats out there today. Some organizations have a policy of only allowing devices that are registered with an internal MDM system to connect to the network. Some also retain the right to remotely wipe any device if it is suspected of being compromised. These are valid approaches.

Within service providers, just under one-third of respondents utilize MDM and/or require the installation of specific security software on user devices, with both of these percentages increasing from last year (Figure 44). The most popular method of reducing risk remains limiting access to internal resources from employee-owned devices, which garnered an almost identical result to last year.

BYOD Access Restrictions

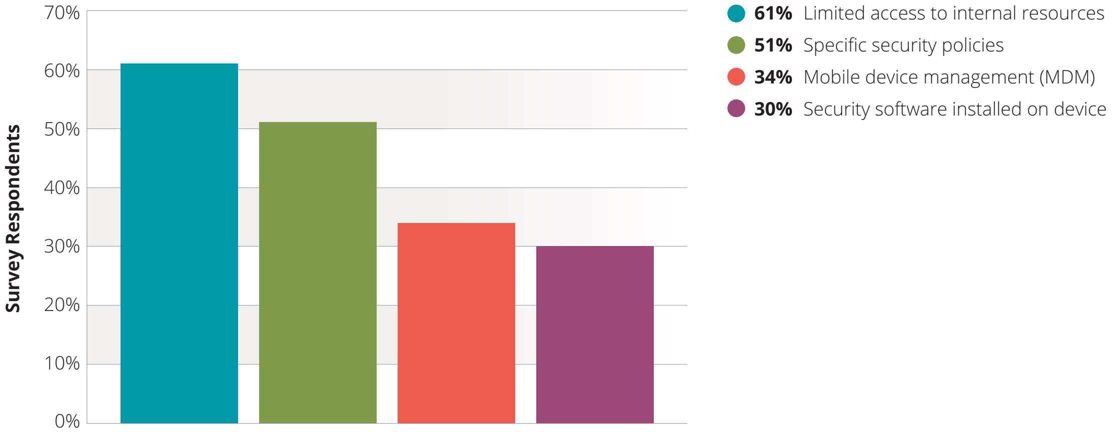


Figure 44 *Source: Arbor Networks, Inc.*

The question of sharing company data over public cloud services is of particular interest. This year, only 60 percent of respondents prohibit this type of data sharing, an identical result to two years ago, but down from 66 percent last year.

The risks of security incidents around BYOD are in constant discussion, but in previous iterations of this survey, the proportion of respondents seeing issues was well below 10 percent. This year, 11 percent of respondents indicate that they have seen a breach or security incident related to a BYOD device, a significant increase (Figure 45). It is also likely that the true percentage is higher, because over one-third of respondents indicate they simply don't know. As BYOD and IoT become ever more widely adopted, it will be interesting to see how these results change.

BYOD Security Breach

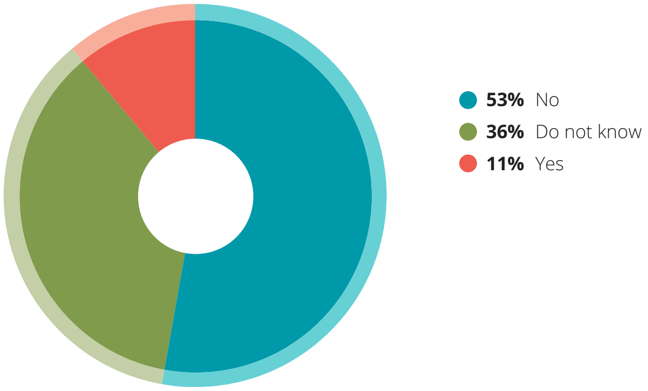


Figure 45 *Source: Arbor Networks, Inc.*

DATA CENTER OPERATORS

Visibility of traffic into or out of the data center at Layer 7 has continued to improve, with 44 percent having visibility at the application layer — up from 38 percent last year and 23 percent in 2013. Only 15 percent of data center operators have visibility of intra-data-center traffic that allows the detection of compromised devices. This is a key concern, as cyber criminals are increasingly using compromised devices within data centers to launch DDoS attacks, host command-and-control capabilities, etc. The proportion of respondents implementing anti-spoofing filters for some or all of their customers is consistent with last year. However, the proportion with no plans to do so has fallen from 20 percent to 12 percent, which is encouraging. Firewalls, intrusion detection systems/intrusion protection systems (IDS/IPS) and application firewalls are the three most commonly deployed security technologies at the data center perimeter. The use of iACLs has increased substantially, from 30 percent of respondents last year to 46 percent this year. This increase in the use of network infrastructure to protect customers and services from security threats is very positive.

Of those witnessing attacks, 70 percent see between 1–10 attacks per month, but 9 percent indicate they are seeing in excess of 50 attacks per month. None indicated this level of activity last year. Customers remain the most common target of DDoS attack within the data center; this is consistent with last year. The proportion of respondents seeing outbound attacks from servers within their data centers has increased sharply over the past year, up to 34 percent from 24 percent. Last year, we highlighted that just over one-third of data center operators had seen DDoS attacks that completely saturated their Internet connectivity. This year, that proportion has grown to 51 percent. This year, as in the last two years, the number one business impact from DDoS is increased operational expense. However, the proportion of respondents experiencing this and other impacts such as customer churn or revenue loss has dropped. This year, 56 percent indicate that they offer DDoS protection services to their customers, compared to only 37 percent last year.

This year, 67 percent of service provider respondents offer hosting, co-location or cloud services. This is consistent with the results for the last three years. Anecdotally, it appears that traffic volumes and enterprise use and reliance on these services continue to grow strongly.

Visibility is the first step to security, and around three-quarters of respondents have visibility of traffic into or out of their data centers at Layers 3 and 4 (Figure 46). This is consistent with last year's results. Visibility at Layer 7 has continued to improve, with 44 percent having visibility at the application layer — up from 38 percent last year and 23 percent in 2013.

Data Center Visibility

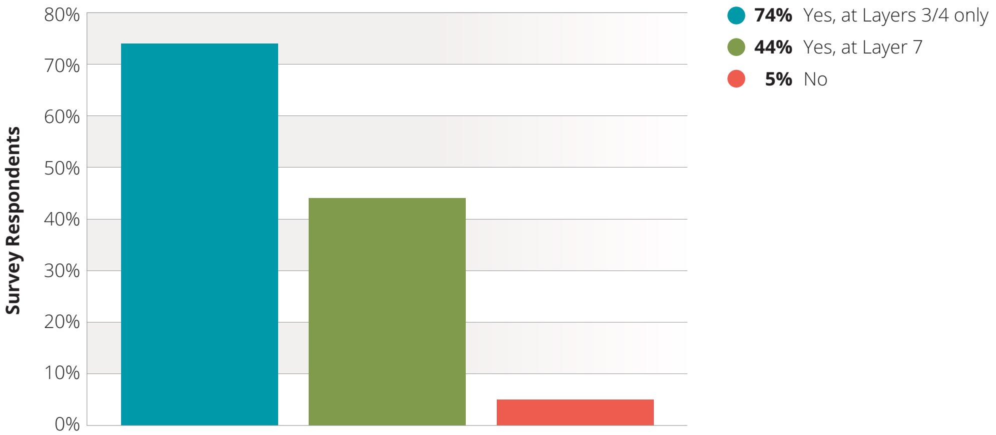


Figure 46 *Source: Arbor Networks, Inc.*

This year, we added a question to the survey to look at intra-data-center traffic visibility. Encouragingly, only 5 percent of respondents indicate that they have no visibility of intra-data-center traffic (Figure 47). Around 40 percent have visibility for performance monitoring and baselining of normal operations. However, only 15 percent have visibility that allows the detection of compromised devices. This is a key concern, as cyber criminals are increasingly using compromised devices within data centers to launch DDoS attacks, host command-and-control capabilities, etc.

Data Center Traffic Visibility

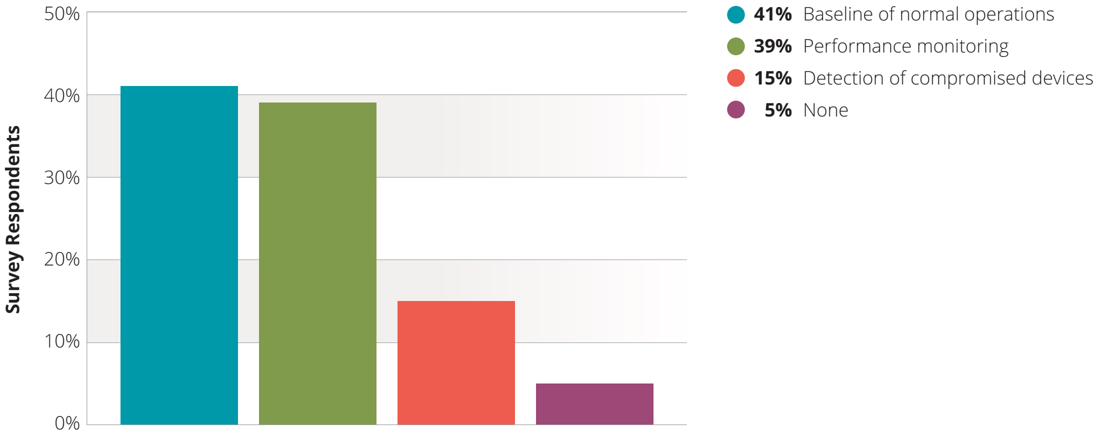


Figure 47 *Source: Arbor Networks, Inc.*

Given that the storm of reflection amplification DDoS attacks has continued in 2015 (although not to the same degree as in early 2014), it is imperative that service providers put steps in place to minimize the resources available to attackers. One way to do this is to implement anti-spoofing filters on customer-facing interfaces. This is especially important within data centers, given the high packet rates that servers can generate and the high bandwidth typically available to them.

The proportion implementing anti-spoofing filters for some or all of their customers is consistent with last year (Figure 48), indicating that there has not been much progress in this regard. However, the proportion of respondents who have no plans to do this has fallen from 20 percent to 12 percent this year, which should lead to improvements in the next survey.

Data Center Anti-Spoofing Filters

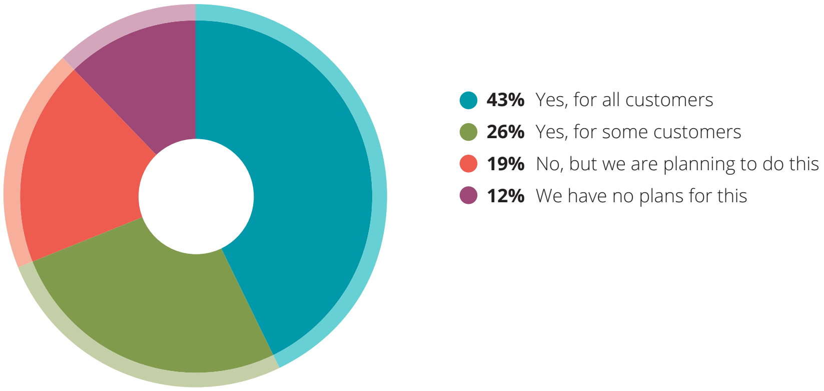


Figure 48 *Source: Arbor Networks, Inc.*

In terms of data center perimeter security, most organizations have multiple technologies deployed to address the different threats they face (Figure 49). The results this year are almost identical to last, with firewalls, intrusion detection systems/intrusion protection systems (IDS/IPS) and application firewalls being the three most commonly deployed technologies. The use of intelligent DDoS mitigation systems (IDMS) has increased slightly this year to 48 percent, from 45 percent last year. The biggest change is in the use of infrastructure ACLs (iACLs). This has increased substantially, from 30 percent last year to 46 percent this year. This increase in the use of network infrastructure to protect customers and services from security threats is very positive.

Data Center Perimeter Security Technologies

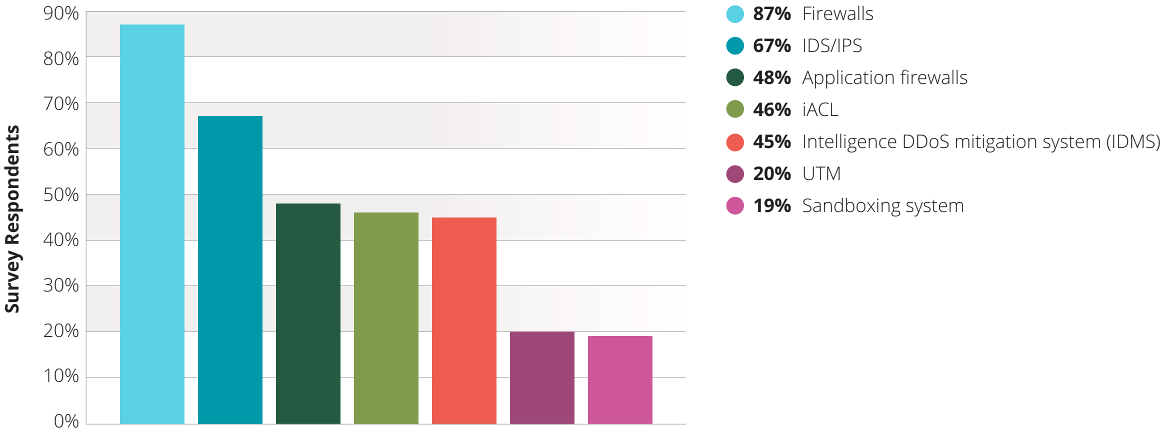


Figure 49 *Source: Arbor Networks, Inc.*

Again this year, the proportion of respondents seeing DDoS attacks targeting their data centers has dropped. This year, 55 percent of respondents indicate they have seen attacks, down from two-thirds last year and 71 percent in 2013. Anecdotally, this is inconsistent with what we are hearing from Arbor customers.

Of the respondents seeing attacks, 70 percent see between 1–10 attacks per month, up from 64 percent last year (Figure 50). However, more respondents report that they are witnessing higher attack frequencies. This year, 8 percent indicate they are seeing in excess of 50 attacks per month. No respondents reported over 50 attacks per month last year.

Data Center DDoS Attack Frequency

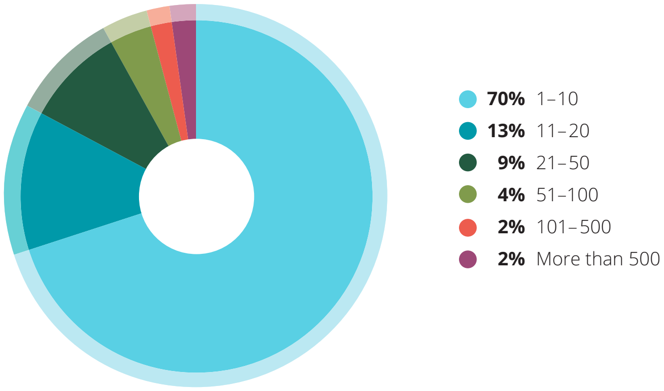


Figure 50 *Source: Arbor Networks, Inc.*

Customers remain the most common target of DDoS attacks within the data center (Figure 51). Interestingly, the proportion of respondents seeing attacks targeting service infrastructure within the data center has gone down significantly, falling from 61 percent last year to 50 percent this year. There has, however, been a sharp increase in those seeing outbound attacks from servers, up to 34 percent from 24 percent last year.

Data Center DDoS Attack Targets

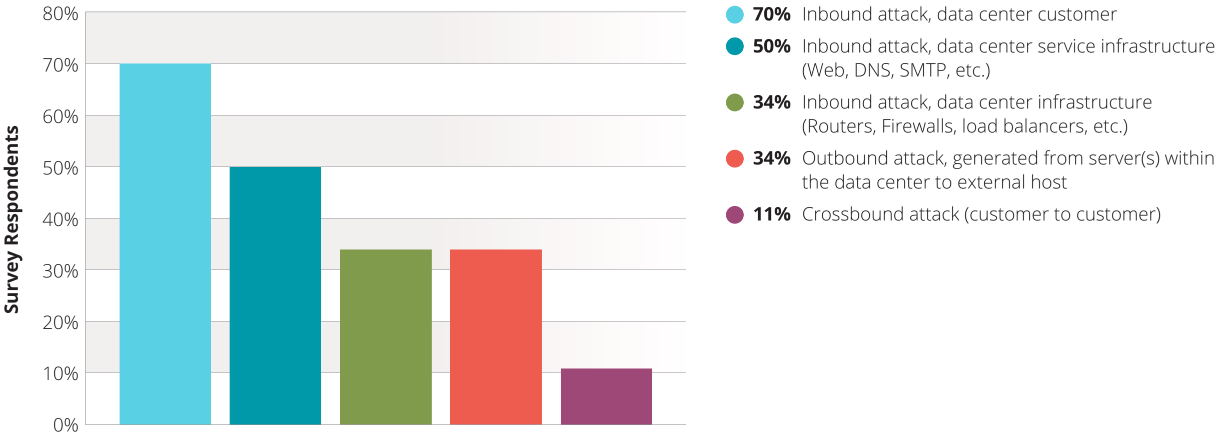


Figure 51 *Source: Arbor Networks, Inc.*

DDoS attacks have continued to grow over the last year, with significant numbers of very large attacks being tracked around the world. Last year, we highlighted that just over one-third of data center operators had seen DDoS attacks that completely saturated their Internet connectivity. This year, that proportion has grown to 51 percent (Figure 52). This growth is a major concern, as attacks that saturate Internet connectivity impact ALL customers and services within the data center — even those that aren't specifically targeted.

To deal with attacks that saturate Internet connectivity, data center operators need protection from an upstream DDoS protection service. It is, therefore, no surprise that cloud and hosting providers are the second most common vertical driving increased interest in service provider DDoS protection services (see the Service Provider DDoS section of this report for further details).

Data Center DDoS Attacks Exceeding Internet Connectivity

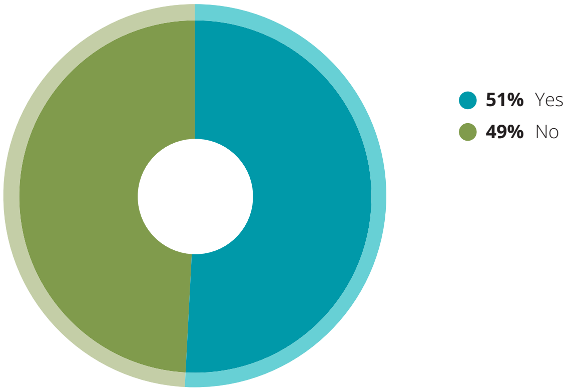


Figure 52 *Source: Arbor Networks, Inc.*

High-magnitude attacks are a significant concern for data center operators, as are attacks that target infrastructure components that maintain per session state. Fifty-six percent indicate that they have seen their firewalls experience or contribute toward an outage during a DDoS attack over the survey period, an increase from just below 50 percent last year. Load balancers also saw increased issues, with 47 percent of respondents seeing problems during DDoS attacks, up from just over one-third last year.

DDoS attacks can have significant business impact if organizations aren't prepared. This year, as in the last two years, the number one business impact from DDoS attacks is increased operational expense (Figure 53). However, the proportion of respondents reporting this has dropped from 81 percent to 69 percent. In fact, there is good news across the board, with lower percentages seeing revenue loss and/or customer churn. The only exception here is in relation to employee turnover, which has seen a huge jump from 2 percent last year to 14 percent this year.

Data Center DDoS Business Impact

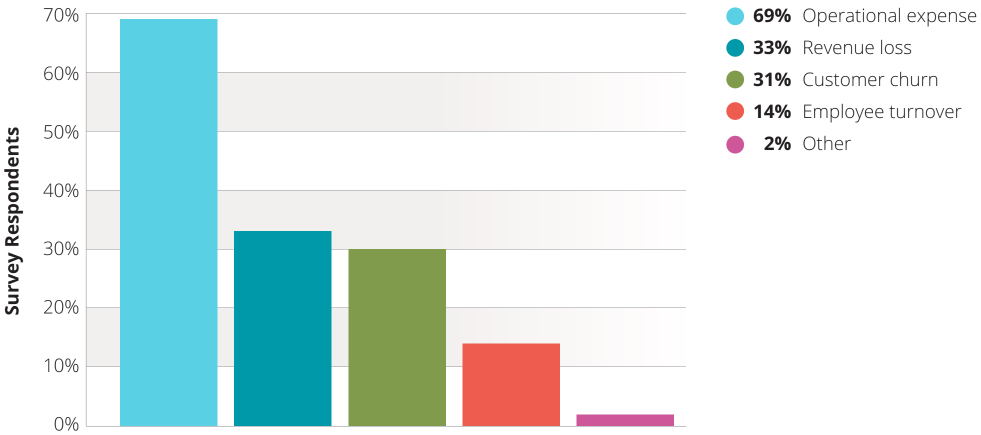


Figure 53 *Source: Arbor Networks, Inc.*

To protect themselves from DDoS attacks, most data center operators deploy multiple technologies (Figure 54). Firewalls remain the most commonly deployed security measure. This remains a concern, especially given the growing proportion of data center operators experiencing issues with firewalls during DDoS attacks (see above). Overall, this year's data is very consistent with last year's but with two notable exceptions. First, the proportion of respondents using perimeter IDMS solutions has increased slightly from 54 percent to 60 percent. Second, the proportion of respondents using iACLs for protection from DDoS has dropped from 70 percent to 56 percent. This is mixed news, as both IDMS and iACLs can be very effective in mitigating the impact of DDoS attacks.

Data Center DDoS Protection Technologies

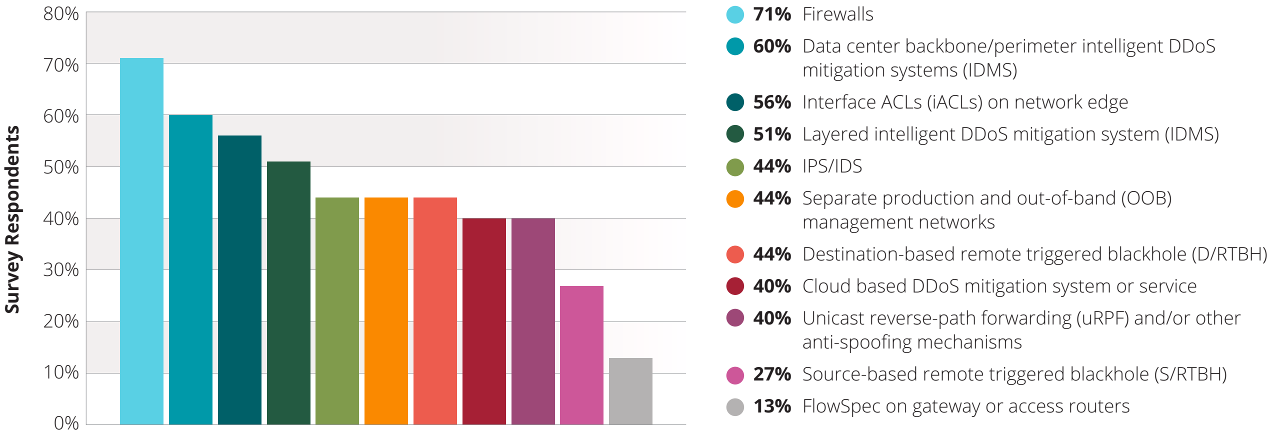


Figure 54 *Source: Arbor Networks, Inc.*

Data center operators are also increasingly offering DDoS protection services to their customers as a way of leveraging their investment in defensive technologies and expertise. Fifty-six percent indicate they offer DDoS protection services this year, compared to only 37 percent last year.

MOBILE NETWORK OPERATORS

The exponential growth in mobile devices and applications is reflected in the high-percentage deployment of LTE technology among this year's respondents, where 84 percent offer LTE service. Thirteen percent of MNO respondents have more than 100 million subscribers. Thirty-eight percent indicate that they have experienced a security incident on the packet core that has led to a customer-visible outage. Seventy percent have observed DDoS attacks targeting their subscribers or infrastructure.

Similar to last year, around 29 percent of respondents offer mobile services. Among those, there is significant growth in the size of the subscriber base (Figure 55). Eighty-two percent indicate that they have more than one million subscribers — much higher than last year's 68 percent. Even more impressive is that 13 percent have more than 100 million subscribers.

Number of Subscribers

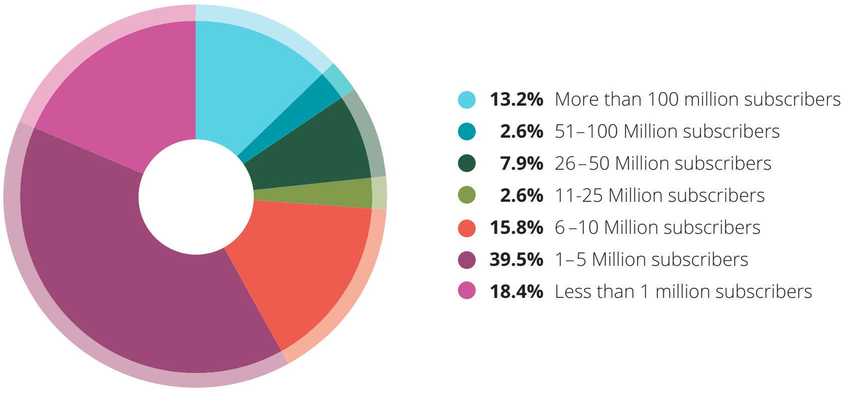


***Figure 55** Source: Arbor Networks, Inc.*

Mobile service operators are continuously building up their infrastructure to support LTE service. This year, more than 84 percent of respondents offer LTE service (Figure 56), much more than last year's 74 percent. Another point to note is that 28 percent of respondents now use WiMax, indicating mobile network operators are adopting new technology to offer better services to their customers.

Radio Technologies

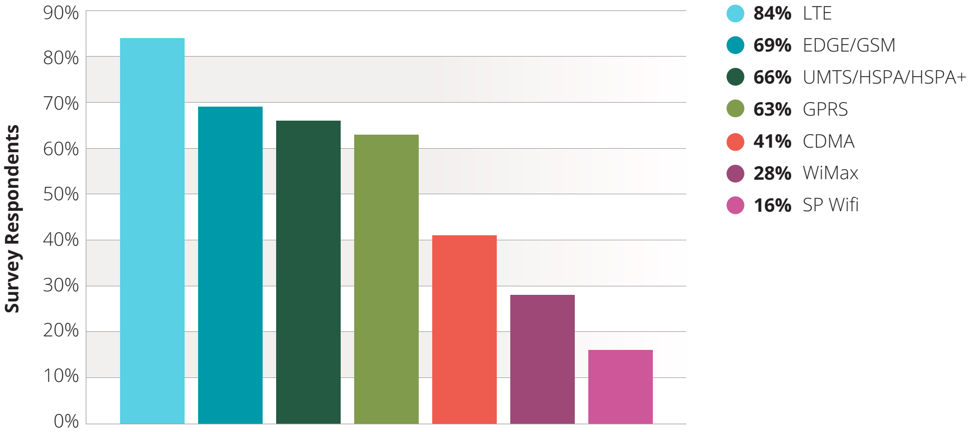


Figure 56 Source: Arbor Networks, Inc.

Regarding security incidents related to the packet core, 38 percent report they have experienced an incident that has led to a customer-visible outage (Figure 57). This is much higher than last year, which is a concern given the continuous growth in the mobile user population.

Security Incidents

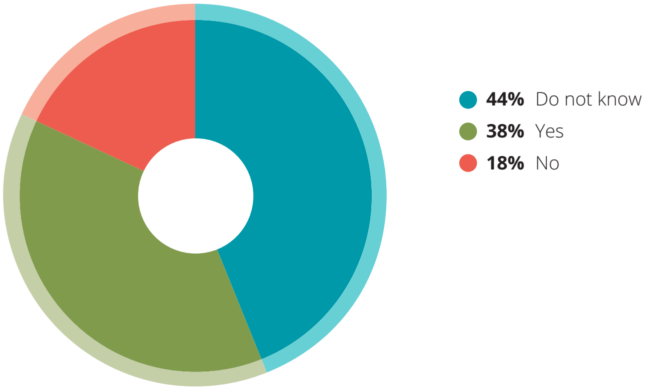


Figure 57 Source: Arbor Networks, Inc.

Regarding the tools and techniques MNOs deploy to protect their infrastructure against availability threats, we see quite a few differences between this year and last. While NAT/PAT and iACL are still the most common protective measures, both have decreased from last year (Figure 58). NAT/PAT usage has dropped to just 67 percent this year from 89 percent last year. In a similar decline, iACL usage has dropped from 79 percent last year to only 57 percent this year.

The use of GTP firewalls has seen significant growth, to 50 percent from just 37 percent in 2014. The increased use of firewall based security technology for availability assurance is of concern. On a positive note, 53 percent indicate that they have deployed IDMS, up from 47 percent last year.

Security Measures

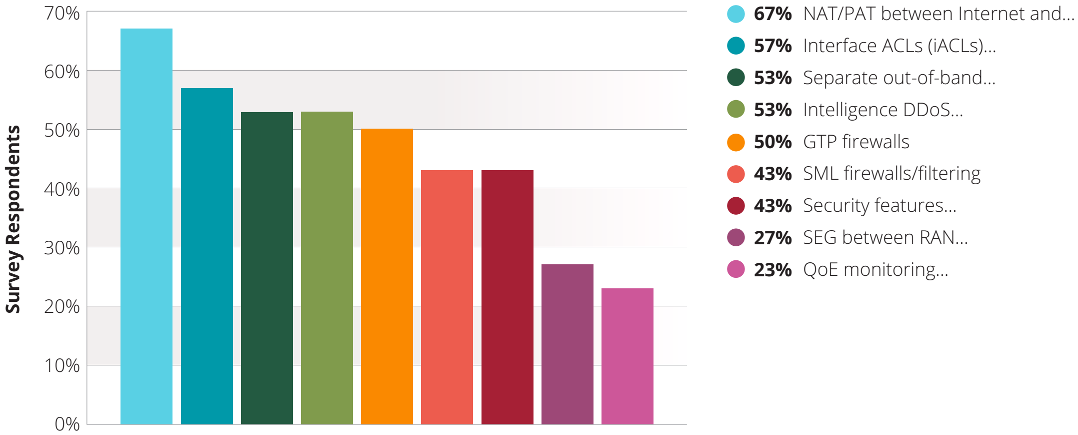


Figure 58 Source: Arbor Networks, Inc.

As with all networks, visibility is an important requirement for the MNO. However, 38 percent still do not have visibility into their packet core network (Figure 59), a slight increase from last year's 33 percent.

According to this year's respondents, Diameter leads the protocols for visibility support, standing at 42 percent. Only twenty-seven percent have visibility for SIP, as well as GTP-C.

Visibility in the Packet Core

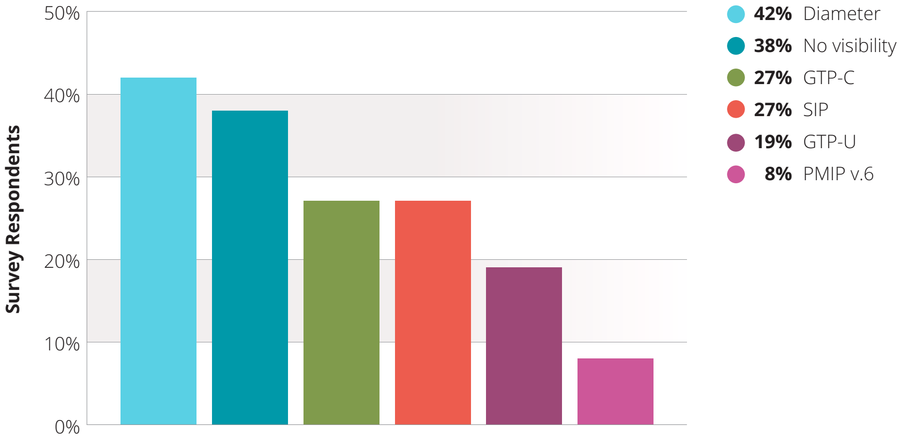


Figure 59 Source: Arbor Networks, Inc.

When asked about visibility on data-roaming interfaces, only 18 percent believe they have adequate visibility, while 62 percent do not know (Figure 60).

Roaming Data Monitoring

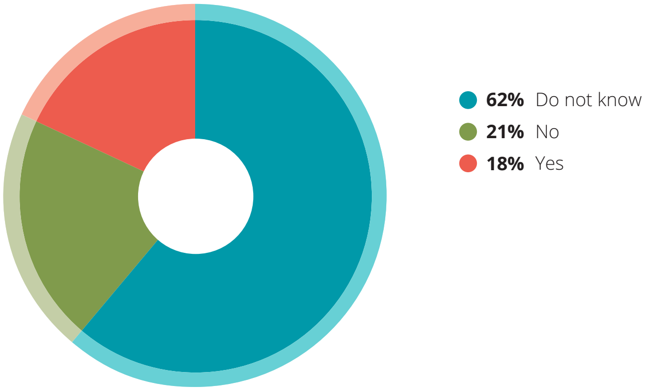


Figure 60 *Source: Arbor Networks, Inc.*

Poorly implemented applications can pose a real problem for mobile operators — causing signaling storms, spikes in DNS traffic and other network congestion issues (Figure 61). Fifty-two percent indicate that they have experienced this issue, up from only 36 percent last year.

Impact of Poorly Implemented Applications

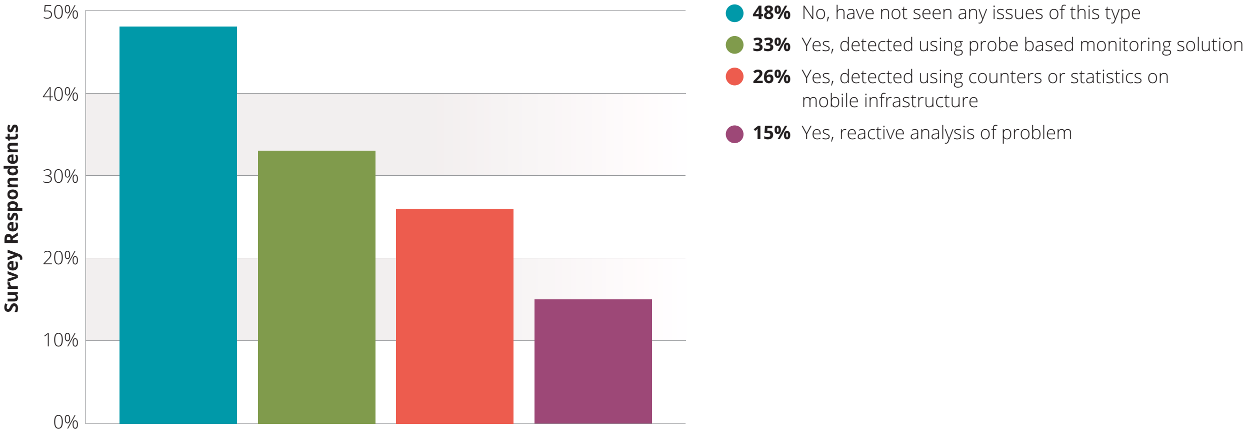


Figure 61 *Source: Arbor Networks, Inc.*

The adoption of IPv6 across mobile networks has increased significantly this year. Nearly one-third of respondents indicate they have adopted IPv6, including 13 percent who have adopted IPv6 for both subscriber services and mobile infrastructure (Figure 62).

In a slight improvement over last year, 27 percent of respondents are now able to detect a compromised subscriber device on their network. Given the rate of LTE adoption, this relatively low percentage remains a serious concern considering the potential bandwidth at the disposal of compromised devices.

Similarly, three-quarters of respondents indicate that they do not know whether any of their subscribers are part of a botnets (Figure 63). Among those who are aware of compromised hosts, the majority estimate them to make up 5 percent or less of the subscriber base. Anecdotally, there are some estimates that anywhere from one-quarter to one-half of all subscribers could be compromised.

Beginning last year, we introduced a question about DDoS threats observed in the mobile network. This year, 15 percent indicate they have identified DDoS attacks initiated by mobile users on their network, but 59 percent lack the visibility necessary to identify these threats (Figure 64).

Mobile IPv6 Adoption

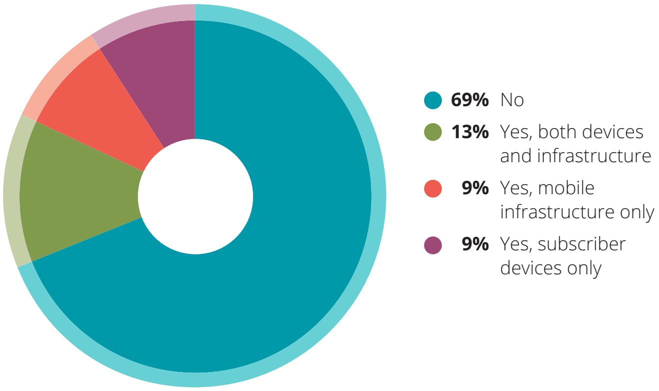


Figure 62 *Source: Arbor Networks, Inc.*

Compromised Subscribers

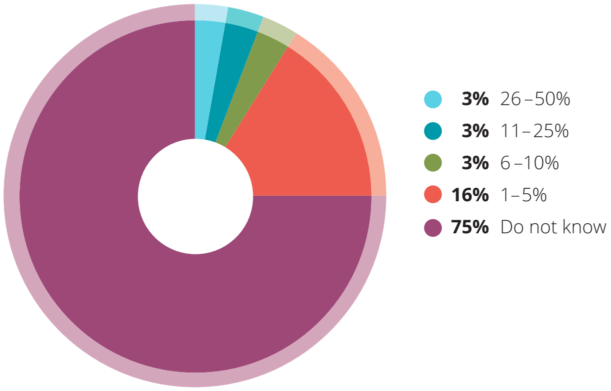


Figure 63 *Source: Arbor Networks, Inc.*

DDoS Attacks from Mobile Users

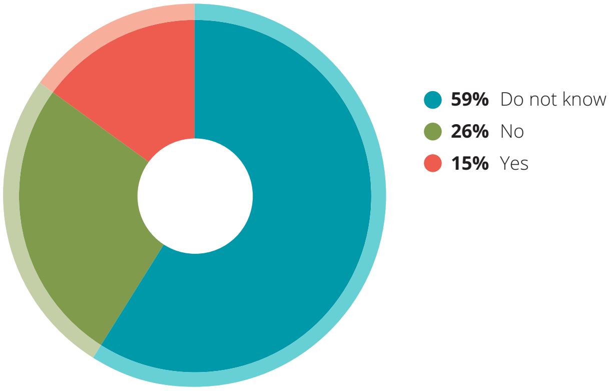


Figure 64 *Source: Arbor Networks, Inc.*

In terms of mitigation of outbound DDoS attacks from mobile subscribers, 9 percent indicate they are currently mitigating attacks — nearly double the percentage from last year (Figure 65). However, 62 percent still have no plan to undertake such action. This is a serious concern. Many subscribers are “NAT’ed” to the same source IP address; therefore, it is very difficult for upstream providers to successfully mitigate attack traffic from one subscriber without affecting other subscribers.

Outbound Attack Mitigation

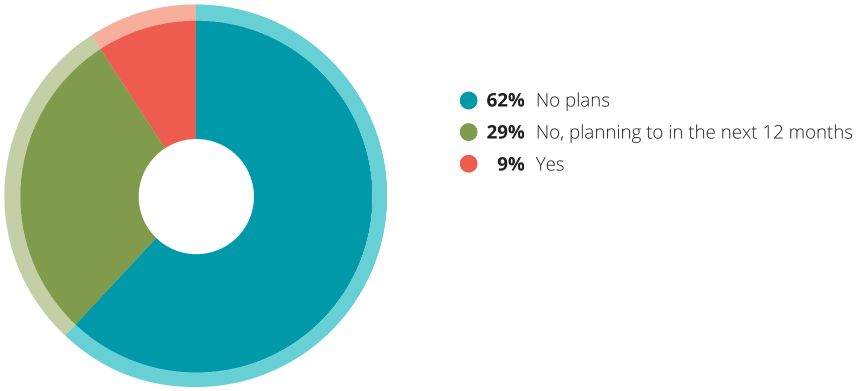


Figure 65 *Source: Arbor Networks, Inc.*

In a massive increase over last year, 68 percent of respondents indicate they have observed DDoS attacks targeting their mobile users or infrastructure, compared to just 36 percent previously (Figure 66). Interestingly, nearly one-third report over 20 attacks per month, with a few even indicating more than 500 monthly attacks.

DDoS Attacks Per Month Targeting Infrastructure or Users

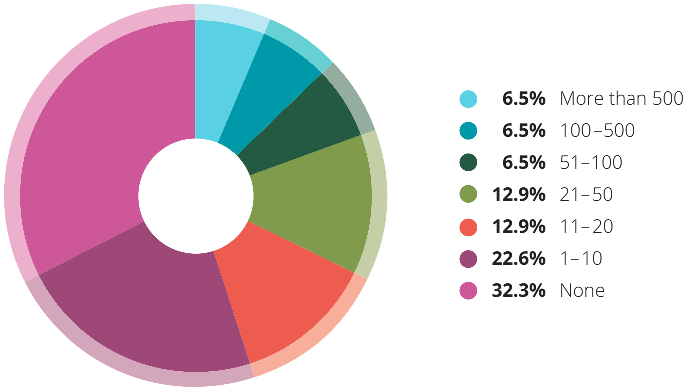


Figure 66 *Source: Arbor Networks, Inc.*

The proportion of organizations with visibility into the mobile Internet (Gi/SGi) infrastructure has gone down again this year (Figure 67). Forty-four percent indicate that they have NO visibility at all — up from 30 percent in 2014 and 20 percent in 2013. While respondents indicate a modest increase in traffic visibility at Layer 7, only 41 percent report visibility at Layers 3 and 4. This lack of visibility continues to be a challenge in protecting mobile IP infrastructure from security threats.

Visibility at (Gi/SGi) IP Backbone

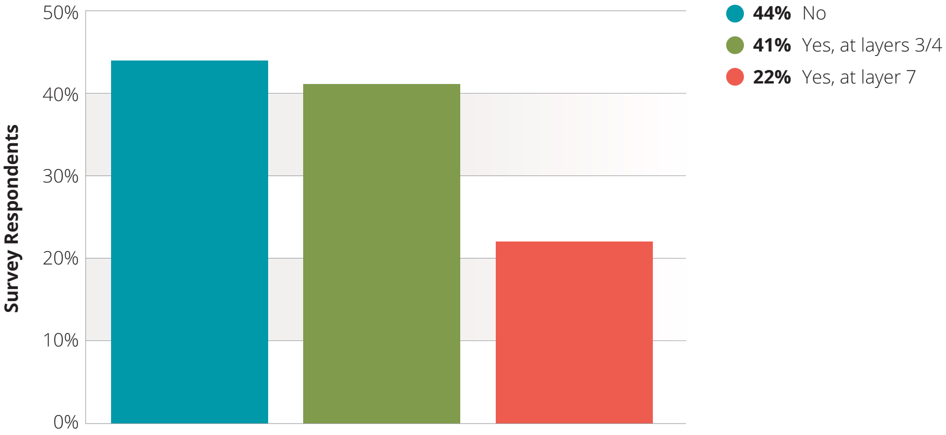


Figure 67 *Source: Arbor Networks, Inc.*

Fifty-nine percent of respondents indicate they have seen DDoS attacks targeting their mobile Internet (Gi/SGi) infrastructure, compared to only 7 percent last year (Figure 68). More interestingly, 28 percent report more than 20 attacks per month, with some indicating over 100 attacks per month.

DDoS Attacks Per Month Targeting (Gi/SGi) IP Infrastructure

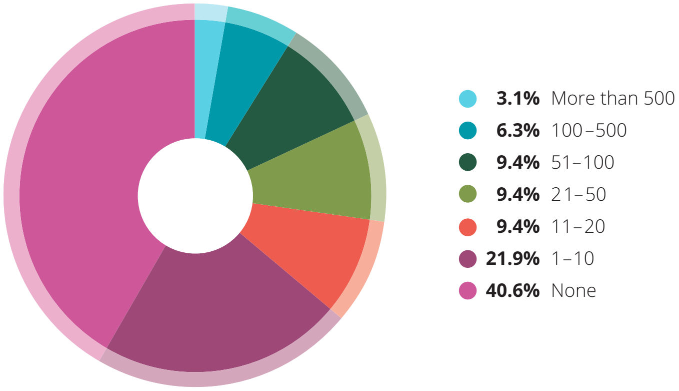


Figure 68 *Source: Arbor Networks, Inc.*

ORGANIZATIONAL SECURITY PRACTICES

Last year, we reported a broad decline in the proportion of service provider respondents implementing best practices in infrastructure security. This year, that trend has reversed, and we see significant increases in the use of most mechanisms. Implementation of anti-spoofing filters is up to 44 percent, from 37 percent last year — but this is still less than half. It was hoped there would be a more significant increase, given the continued storm of reflection amplification DDoS attacks on the Internet.

This year, 46 percent of respondents indicate that they carry out DDoS defense simulations, up from 34 percent last year and back to the level seen in 2013. Even more positive is that 31 percent of service providers now run rehearsals at least on a quarterly basis, up from 21 percent last year. Encouragingly, there has been an increase in those monitoring for route hijacks, up to 54 percent this year from 40 percent last year. Participation in global OPSEC groups has improved slightly this year to 41 percent, from 36 percent last year.

Last year, we reported that those implementing infrastructure security best practices broadly declined. This year, that trend has reversed. We see significant increases in the use of most best practices (Figure 69). Use of authentication for BGP and IGP — the most widely deployed best practice for the past few years — has seen further adoption, with 73 percent now using this, up from 65 percent last year. The use of separate OOB management networks and the generalized TTL security mechanism (GTSM) also saw increases in adoption of over 10 percent. However, although the implementation of anti-spoofing filters is up to 44 percent this year from 37 percent last year, this is still less than half of respondents. Given the continued storm of reflection amplification DDoS attacks raging across the Internet over the past two years, it was hoped that anti-spoofing filters, which can reduce the capability available to attackers, would be more widely implemented.

Security Best Practices

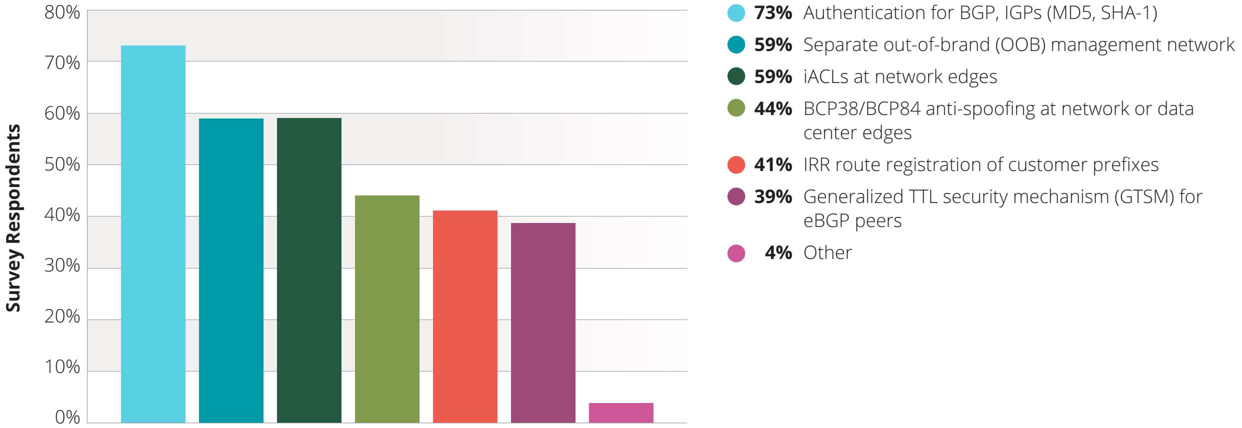


***Figure 69** Source: Arbor Networks, Inc.*

Dealing with a DDoS attack can be hugely stressful if teams and processes are not well rehearsed. The impact of attacks can be exacerbated if errors are made that result in the over-blocking of traffic or other service problems. To streamline the effectiveness of security teams and tools, regular DDoS defense exercises should be carried out. This year, 46 percent of respondents indicate that they carry out DDoS defense simulations (Figure 70), up from 34 percent last year and back to the level seen in 2013. Even more positive is that 31 percent of service provider respondents now run rehearsals at least on a quarterly basis, up from 21 percent last year.

DDoS Simulations

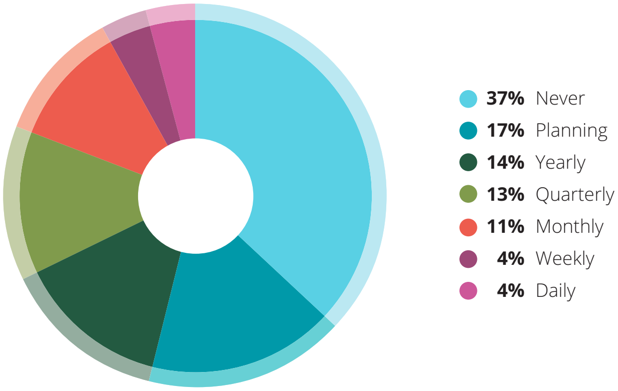


Figure 70 *Source: Arbor Networks, Inc.*

The proportion of respondents who filter routes from their customers and/or peers has increased this year; last year, that proportion dropped sharply. This year, 67 percent filter routes advertised from customers, and 62 percent filter routes advertised by peers — up from 49 percent and 48 percent respectively.

Encouragingly, the proportion of those monitoring for route hijacks has also increased, up to 54 percent this year from 40 percent last year. This represents a recovery to the level seen in 2013 — possibly driven by media coverage of route hijacks in the last year. The number proactively filtering known botnet C&C traffic, etc. has remained static this year at 56 percent. Significant growth was seen from 2013 to 2014, but plateaued this year.

Participation in Global OPSEC Groups

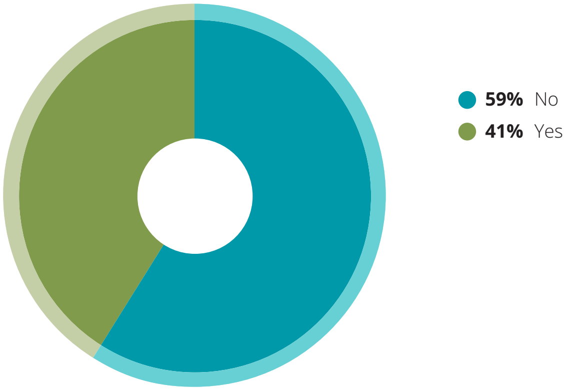


Figure 71 *Source: Arbor Networks, Inc.*

Participation in global OPSEC groups has improved slightly this year to 41 percent (Figure 71), from 36 percent last year. This year's result is also a slight improvement over the 2013 level of 39 percent. As in previous iterations of this report, over 80 percent believe that participation in these groups is an effective way of identifying and mitigating security incidents.

There are, however, a number of perennial challenges that prevent organizations from participating in these groups, with "not enough time" being the most significant reason (Figure 72). Most results in this area are consistent year-over-year, but we have seen a significant increase in respondents citing "legal concerns," up from 11 percent last year to 20 percent this year. This is worrying, as the sharing of appropriate data within closed communities for security purposes can be highly effective.

Reasons for Non-Participation in Global OPSEC Groups

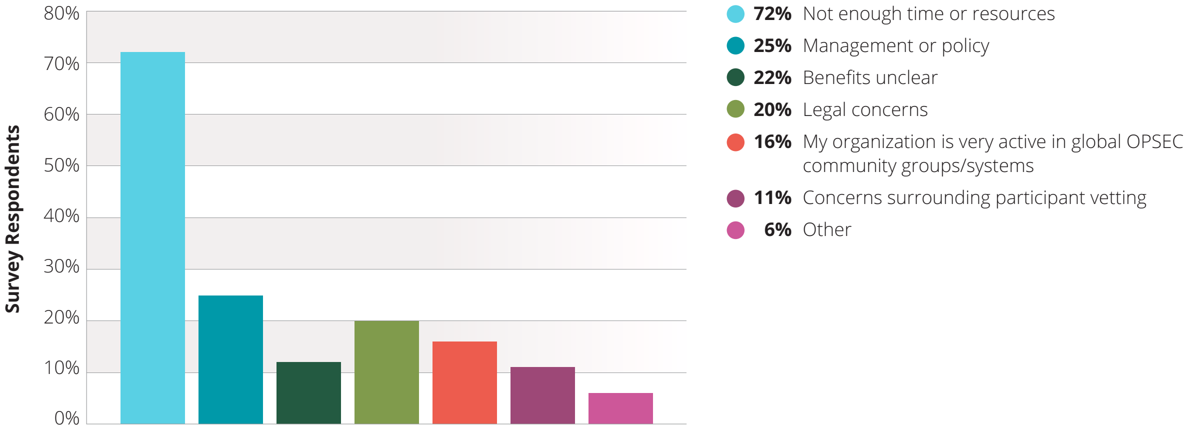


***Figure 72** Source: Arbor Networks, Inc.*

SERVICE PROVIDER IPv6

This year, nearly 70 percent of service provider respondents report that they have deployed IPv6 within their networks or plan to deploy it in the next 12 months. Thirty-three percent have completed their IPv6 deployment. More than 70 percent have subscribers utilizing IPv6 services offered by the service provider. Similar to last year, the number of respondents with IPv6 visibility is increasing, this year to 70 percent. The top security concern is DDoS attack, followed by misconfiguration and botnets.

Similar to last year's report, the IPv6 sections in this year's survey have been separated into service provider responses and enterprise, government and education responses. This separation provides better insight into how IPv6 technology is being deployed in different network types.

This year, 68 percent of service providers indicate that they have deployed IPv6 or plan to deploy it in their network in the next 12 months. This percentage remains unchanged from last year. At the same time, around 33 percent have already completed their IPv6 transition, which is again the same percentage reported last year. The percentage for "deployment in progress" also remains roughly the same, an indication that service providers are steadily deploying IPv6 in their networks.

Regarding IPv4 address shortage, roughly 44 percent of respondents indicate that this may be an issue for them in the next 12 months. This number will rise if respondents don't finish their IPv6 deployments, as the expansion of the IoT could increase the requirement for IP addresses by billions yearly.

According to last year's report, the proportion of subscribers and business customers using IPv6 increased from 2013 to 2014. This year, only 80 percent of service providers have business users who utilize IPv6 services, down from 88 percent in 2014 (Figure 73).

Business Customer IPv6 Service Usage

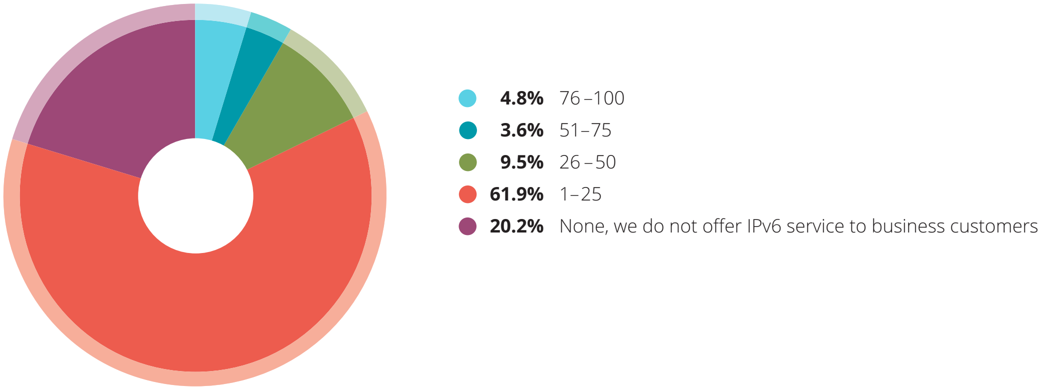


Figure 73 *Source: Arbor Networks, Inc.*

Meanwhile, the proportion of subscribers using IPv6 has risen slightly from 68 percent to 71 percent (Figure 74). Despite a lower growth rate this year, IPv6 has a relatively higher adoption rate than a few years ago.

With the increasing adoption of IPv6 by customers within service provider networks, IPv6 traffic visibility is a major requirement. The good news is that 70 percent of service providers indicate that they have good IPv6 visibility; this is a 6 percent increase from last year.

Flow telemetry is still the most cost-effective way to gather network-wide traffic information. Last year, nearly half of respondents indicated that they have full IPv6 flow telemetry support on their network infrastructure. This year, that number dropped slightly to 43 percent, with 19 percent indicating that they will have full IPv6 flow support over the next 12 months (Figure 75).

This year, IPv6 traffic has grown significantly compared to last year. Thirteen percent of respondents report over 30 Gbps of IPv6 traffic within their network. The highest reported traffic rate for an individual respondent is 5 Tbps, which represents a huge percentage increase from previous years.

Regarding future IPv6 traffic growth, nearly half indicate that they expect a mere 20 percent growth rate, which is similar to last year's survey (Figure 76).

Subscriber IPv6 Usage

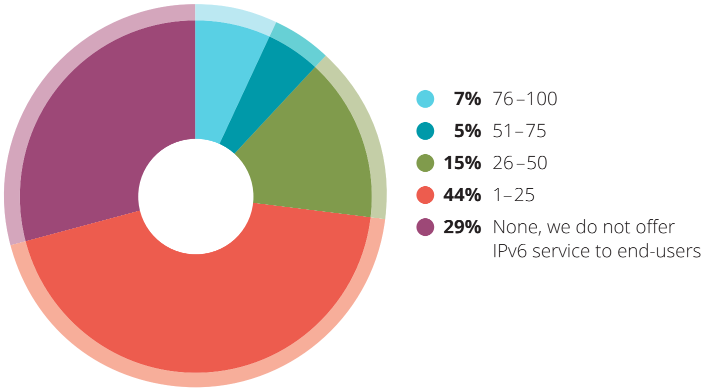


Figure 74 *Source: Arbor Networks, Inc.*

IPv6 Flow Telemetry

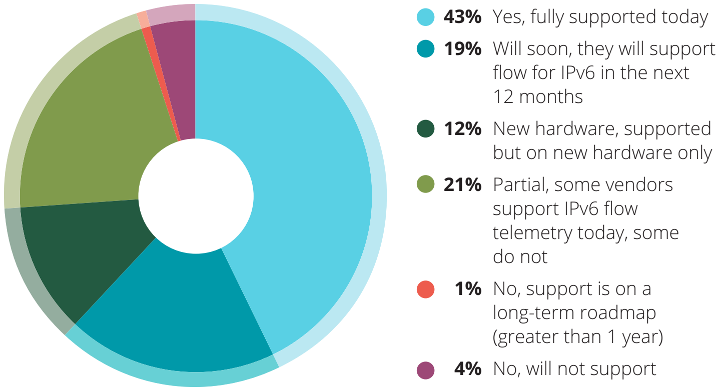


Figure 75 *Source: Arbor Networks, Inc.*

Anticipated IPv6 Traffic Growth

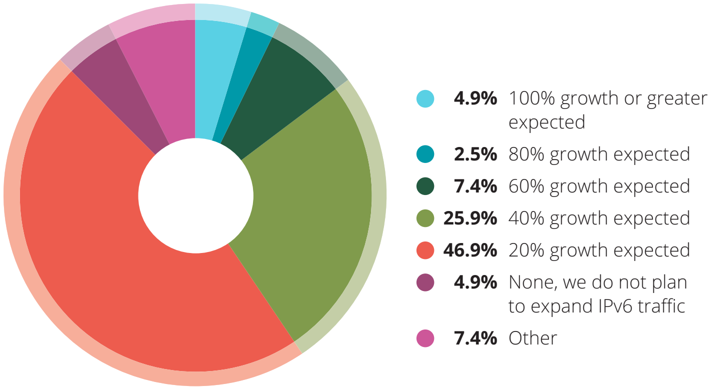


Figure 76 *Source: Arbor Networks, Inc.*

While IPv6 traffic is growing, security concerns related to IPv6 have gathered attention from service providers. This year, 75 percent of respondents are concerned with IPv6 DDoS, a significant increase from last year's 52 percent (Figure 77).

IPv6 Security Concerns

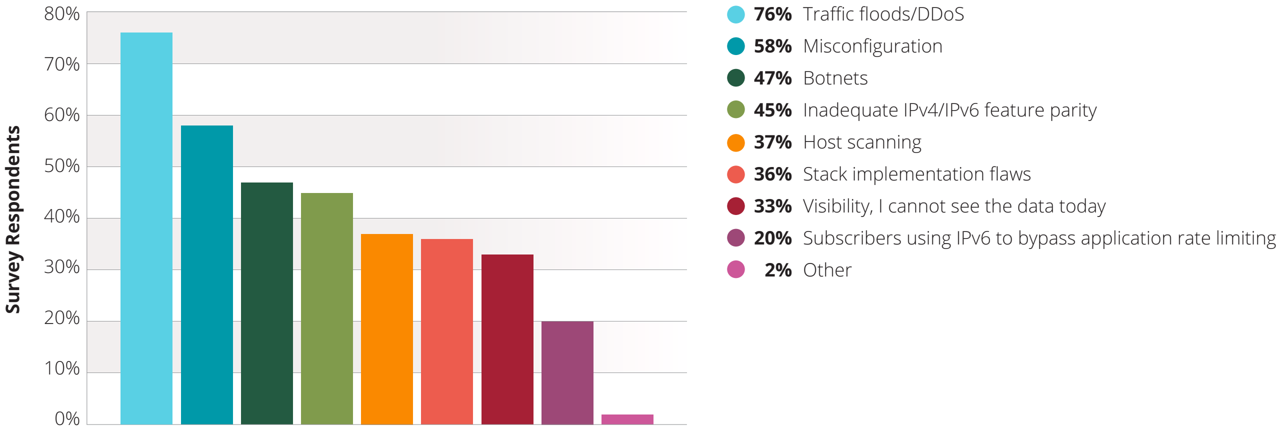


Figure 77 *Source: Arbor Networks, Inc.*

When asked what mitigation measures service providers deploy against IPv6 attacks, the top three mitigation options are (Figure 78):

- Intelligent DDoS mitigation system (IDMS)
- Access control list (ACL)
- Destination-based remote-triggered blackhole (D/RTBH)

IPv6 Mitigation Capabilities

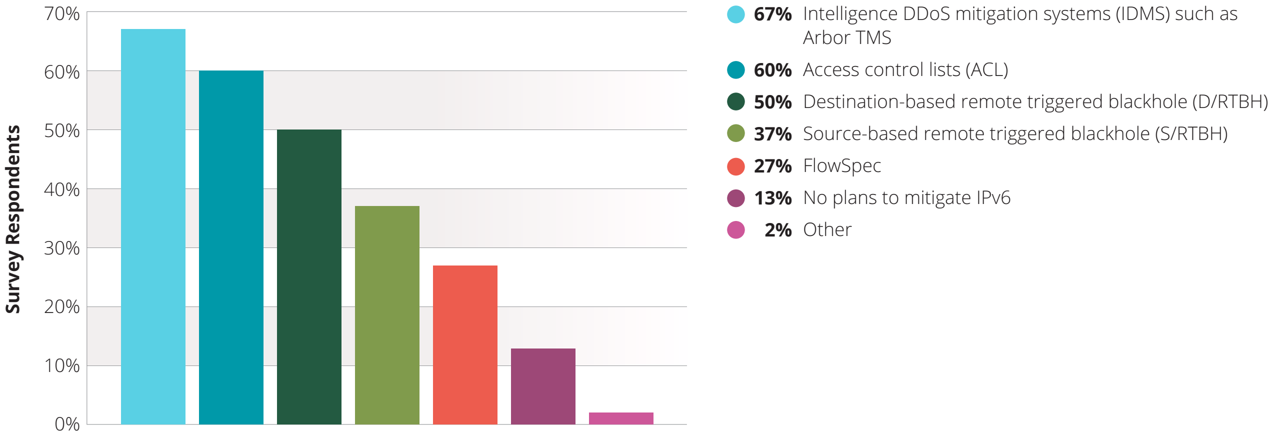


Figure 78 *Source: Arbor Networks, Inc.*

ente

3

SECTION 3

ENTERPRISE

ENTERPRISE NETWORK SECURITY

DDoS is the most common threat experienced by enterprise, government and education (EGE) respondents during this survey period, similar to last year. Respondents seeing malicious insiders increased from 12 percent last year to 17 percent this year; the proportion experiencing APT also grew from 18 percent to 23 percent. The statistics reported by EGE for discovery, reporting and remediation of threats are very encouraging. Less than 5 percent say incidents took more than three months to resolve. This year, we asked respondents about their notification processes in the event of a breach. The responses indicate that almost 85 percent of all participants have either formal external or internal notification policies in place.

Looking at the risks associated with a successful incursion by an APT, loss of personal information or disruption of business are the top concerns, with both ranked number one by around one-quarter of respondents. On a positive note, this year we saw an increase in those with an incident response plan and at least some resources in place, up from around two-thirds last year to 75 percent this year. In this survey period, just over one-quarter of respondents indicate they have seen an increase in incident frequency.

Looking at how EGE respondents rate their preparedness for dealing with an incident, results are broadly similar to last year. And, positively, the proportion of respondents indicating they have made no preparations has decreased, from 10 percent last year to 6 percent this year. In terms of improving incident response, deploying solutions that speed up the incident response process saw significant growth in interest, up from 45 percent to 57 percent of respondents. On a more negative note, there has been a big drop in those who are looking to increase their internal resources to improve preparedness, down from 46 percent to 38 percent.

Similar to last year, firewalls and SIEM are the most commonly utilized tools to detect threats within EGE respondents' networks. In third place are NetFlow analyzers, again with a similar result to last year. However, the use of forensic packet analysis tools has increased by 9 percent this year — a big jump.

Nearly 40 percent of all enterprises still do not have anything deployed to monitor BYOD devices on the network, this represents a 6 percent improvement over last year, but is still quite shocking. This year, the proportion of respondents who have seen security incidents relating to BYOD doubled, to 13 percent from 6 percent last year. This mirrors the increase seen from our service provider respondents.

Last year, for the first time, Arbor introduced a survey section dedicated to enterprise, government and education (EGE) respondents with a more tailored set of questions. The provision of this section allowed us to remove irrelevant questions (for this respondent group) and more easily compare and contrast the differences in observations between service provider and EGE respondents. This year, we have gone one step further to gain additional insight into the industries represented by respondents so that we can provide further analysis.

As mentioned in the demographic section, we received a record number of EGE responses this year, and those responses represent over 16 different verticals. Some of these verticals do overlap, but it is good to see diversity in the respondent space. The biggest verticals represented are technology, banking /finance and government — together making up over 60 percent of responses (Figure 79).

EGE Vertical Breakout

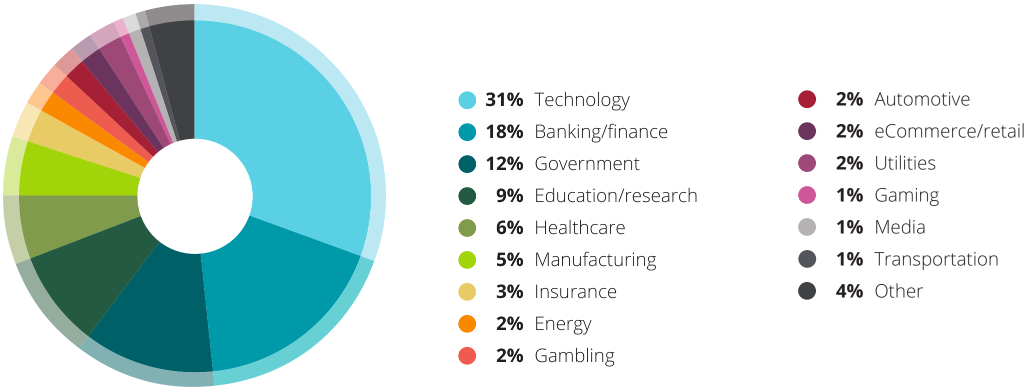


Figure 79 *Source: Arbor Networks, Inc.*

As this is the second year the survey has included a section of questions specifically aimed at EGE respondents, we can now begin to identify changes and trends. DDoS is the most common threat experienced by respondents during this survey period, similar to last year, followed by Internet connectivity congestion due to genuine traffic, accidental data loss and botted or compromised hosts (Figure 80). The percentage of respondents experiencing congestion due to genuine network traffic increased this year to 29 percent, from 26 percent last year, pushing it into second place. However, looking at the data, this shift is also due to reductions in the proportions of respondents seeing both accidental data loss and compromised hosts on their networks, which fell from 33 percent to 28 percent and from 32 percent to 26 percent respectively. This is a positive change.

Other changes are also noteworthy. The proportion of respondents seeing malicious insiders increased from 12 percent last year to 17 percent this year. The proportion experiencing APT also grew from 18 percent to 23 percent. Interestingly, the proportion of EGE respondents experiencing these threat types are roughly double those of service providers. These two threat types should be a key concern for EGE respondents.

This year's survey results regarding concerns in the coming year do not hold any big surprises (Figure 81). Concerns around DDoS attack and APT clearly remain top-of-mind. Interestingly, if we look at data for individual verticals, there are some clear differences. Sixty-four percent of banking/finance organizations are concerned about the disclosure of regulated data, the top concern for this organization type. This is not surprising, given the regulatory framework in place and the amount of data held. For government organizations, accidental data loss is much more significant, with 52 percent of these organizations registering their concern here.

EGE Threats

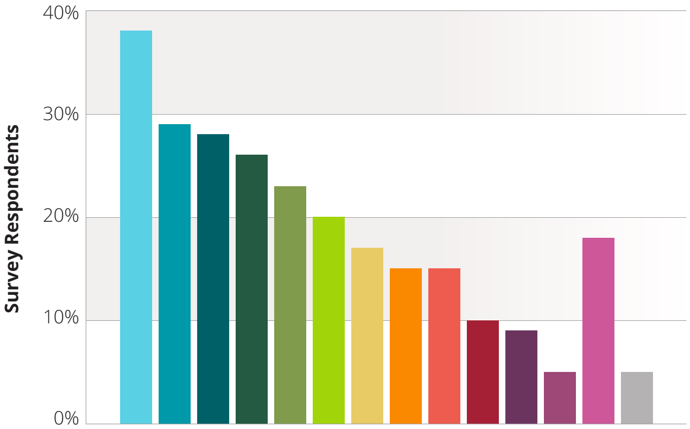


Figure 80 *Source: Arbor Networks, Inc.*

●	**38%**	Internet connectivity congestion due to DDoS attack
●	**29%**	Internet connectivity congestion due to genuine traffic growth/spike
●	**28%**	Accidental data loss
●	**26%**	Botted or otherwise compromised hosts on your corporate network
●	**23%**	Advanced persistent threat (APT) on corporate network
●	**20%**	Accidental major service outage
●	**17%**	Malicious insider
●	**15%**	Exposure of sensitive, but non-regulated data
●	**15%**	Theft
●	**10%**	Exposure of regulated data
●	**9%**	Web defacement
●	**5%**	Industrial espionage or data exfiltration
●	**18%**	None of the above
●	**5%**	Other

EGE Concerns

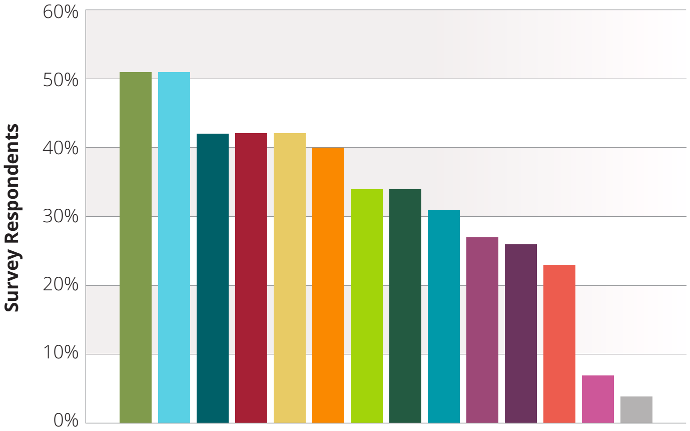


Figure 81 *Source: Arbor Networks, Inc.*

●	**51%**	Advanced persistent threat (APT)
●	**51%**	Internet connectivity congestion due to DDoS attack
●	**42%**	Accidental data loss
●	**42%**	Exposure of regulated data
●	**42%**	Malicious insider
●	**40%**	Exposure of sensitive, but non-regulated data
●	**34%**	Accidental major service outage
●	**34%**	Botted or otherwise compromised hosts on your corporate network
●	**31%**	Internet connectivity congestion due to genuine traffic growth/spike
●	**27%**	Industrial espionage or data exfiltration
●	**26%**	Web defacement
●	**23%**	Theft
●	**7%**	None of the above
●	**4%**	Other

Last year, for the first time, we attempted to capture metrics around incident response time. The survey questions provided room for free-form answers and did not specify the incident type — leading to a huge variation in the responses and making the data very difficult to interpret. This year, the questions have been focused around response times for advanced threat or advanced persistent threat, and time bands have been provided.

The statistics reported by EGE respondents for discovery, reporting and remediation of threats are very encouraging (Figure 82). Less than 5 percent say incidents took more than three months to resolve. While this does not match anecdotal information from IR teams outside of this survey, it does appear consistent across both EGE and service provider respondents. Looking at the contrast between EGE and service provider respondents, it is interesting to note that far higher proportions of EGE respondents take less than one week for all of the incident stages enumerated below. This difference is even more profound if we look at the banking and government responses; these organizations appear to have very effective response processes in place.

Response Times for APT

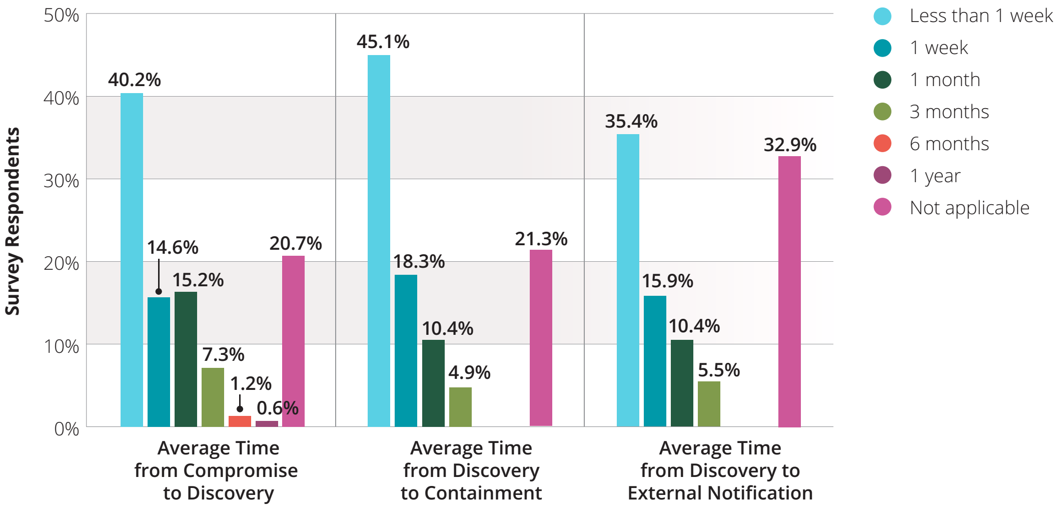


Figure 82 *Source: Arbor Networks, Inc.*

This year, we also asked respondents about their notification processes in the event of a breach. The responses indicate that almost 85 percent have either formal external or internal notification policies in place (Figure 83). This is a high percentage, but realistically it should be 100 percent. Many countries, states or industry verticals now have rules in place governing notification, and not having a process could prove very costly indeed. Organizations like the Identity Theft Resource Center (http://www.idtheftcenter.org), and many others, have good information to help assess if notification is required. Determining if notification is required is as important as the actual notification. Sharing information around a breach, if it does not involved regulated data, can be as damaging and costly to an organization as failing to disclose a breach of regulated information.

Breach Notification

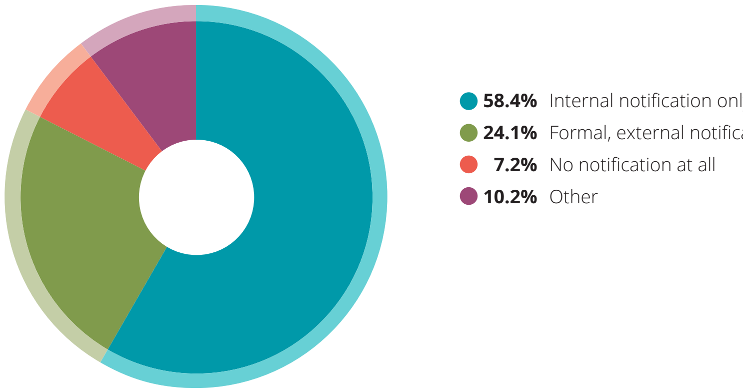


Figure 83 *Source: Arbor Networks, Inc.*

This year, we added questions to establish how respondents are looking to reduce the time it takes them to both discover and contain threats. The responses are very similar. The top three mechanisms in both cases are implementing new forensic tools, improving the triage process and integrating threat intelligence into the IR function (Figures 84 and 85). These areas could not be more important; anecdotally Arbor is hearing the exact same message at every meeting, whether it is with the executive board or frontline security practitioners. In most organizations, the message is very clear: "We are building a hunting team and require better tools with more intelligence."

The data for specific verticals is fairly consistent in this area. However, the implementation of new forensic tools is even more of a focus for banking and government respondents, who may have more developed IR processes and teams.

Improving Compromise and Discovery Time

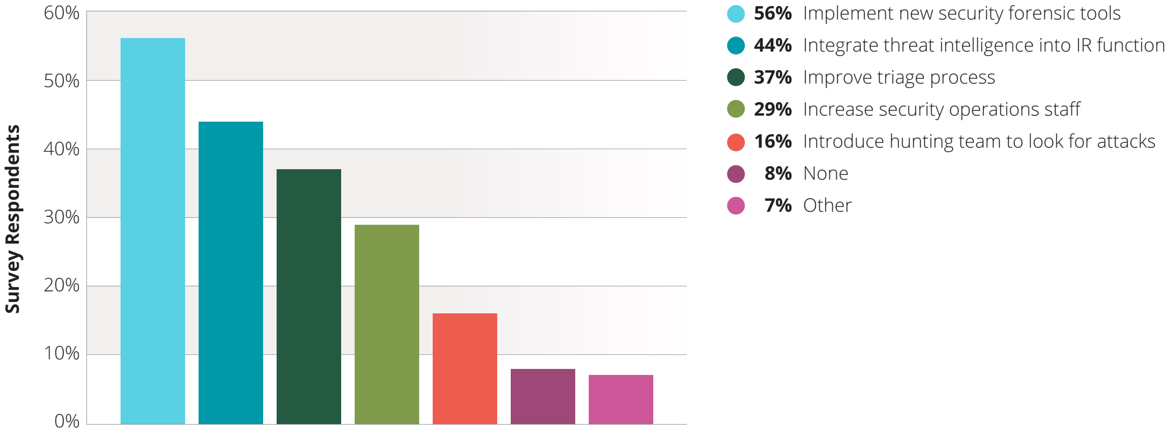


Figure 84 Source: Arbor Networks, Inc.

Improving Discovery and Containment Time

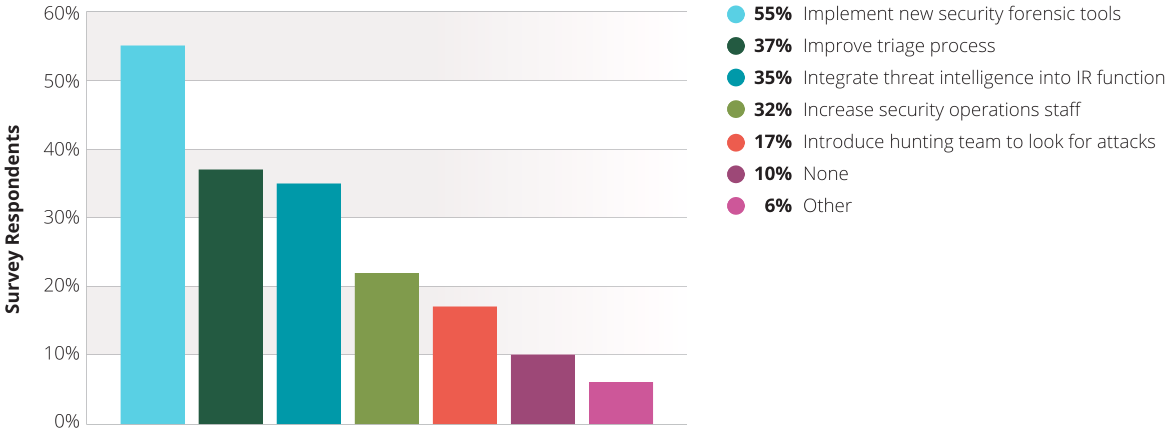


Figure 85 Source: Arbor Networks, Inc.

APT/AT and orchestrated attacks are a major concern for all enterprise operations. Looking at the risks associated with a successful incursion by an APT, loss of personal information or disruption of business are the top concerns, (Figure 86). Of all six major categories included, contractual breach is ranked lowest. This supports the theory that loss of personal data is king in the financial world. It is surprising to see only 12 percent of respondents concerned with loss of intellectual property, when it can be the cause of a business failing in a highly competitive market. Many hand-held device manufactures would be in much better shape if they had protected their intellectual property better from outside forces, as would a few green energy companies.

Ranking of APT Risk

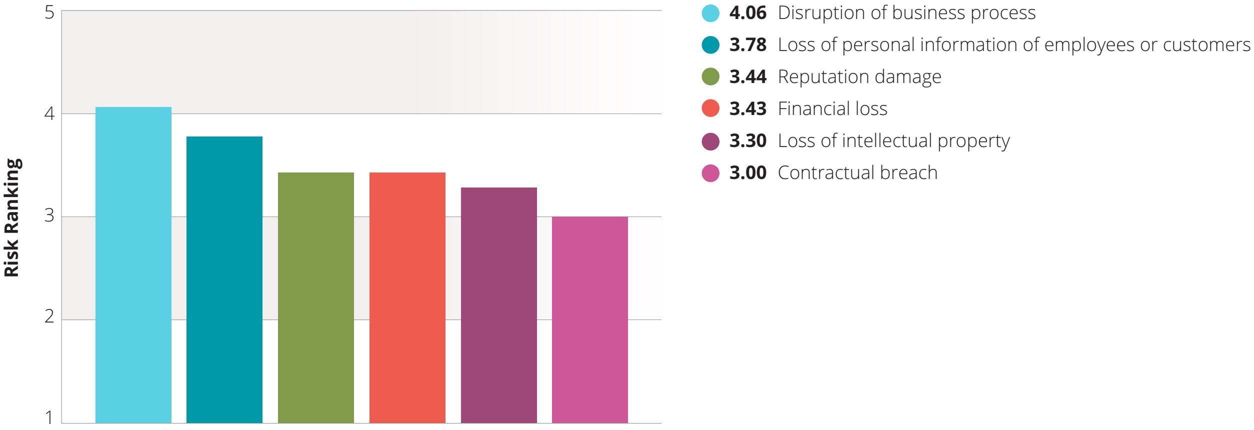


Figure 86 *Source: Arbor Networks, Inc.*

On a positive note, this year we see an increase in those with an incident response plan and at least some resources in place, up from around two-thirds last year to 75 percent this year (Figure 87). The proportion with no plan is down 5 percent from last year. This is a small change, but coupled with the above data and the 4 percent growth in respondents with a well-resourced team, this year's results represent a large step in the right direction for incident handling. Service providers also report improvements in this area but, in general, there are greater improvements amongst EGE organizations.

Incident Response Posture

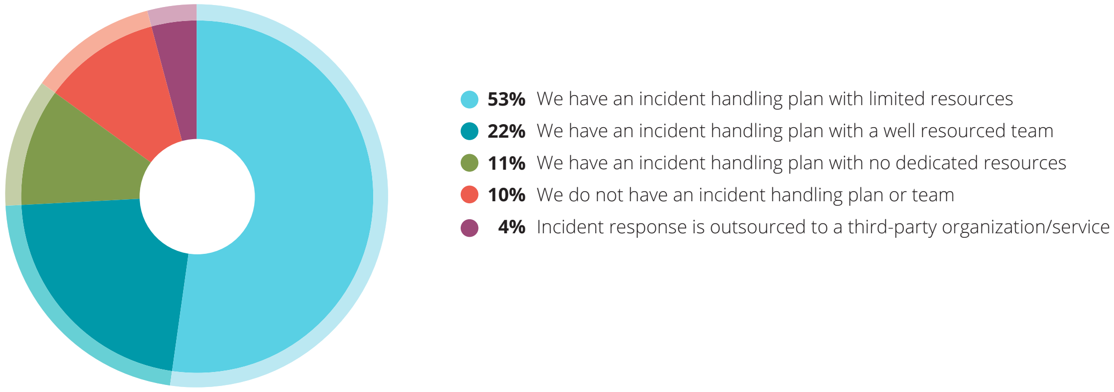


Figure 87 *Source: Arbor Networks, Inc.*

Outsourcing of incident handling stayed static. This possibly indicates that the industry is aware that incidents must be handled internally, to some degree, to deal with the alphabet soup of today's threats and the regulatory requirements that are either in place or coming down the pipe.

The question of contracting with external organizations to assist with incident response can go against the grain for security professionals. However, given the complexity of the threat landscape and the difficulty in finding skilled security professionals, it is becoming a necessity for many. Almost 50 percent of EGE respondents indicate that they have contracted with an external organization. This is around 10 percent higher than within the service provider space. The most common area where respondents seek external assistance is in specialist IT forensics, at 42 percent (Figure 88); within the banking vertical, this is up to 60 percent. Interestingly, for service provider respondents, IT forensics is also at the top, but only 23 percent of respondents have an external arrangement in place. This difference is expected, given the likely higher availability of technical resources within most service providers.

Another key area of difference between EGE and service provider respondents is in their engagement with regulators/government agencies. Nine percent of service providers indicate they use these bodies, as opposed to 17 percent of EGE respondents. This result is skewed somewhat by the government vertical, where 38 percent of respondents indicate they engage with regulators and other government bodies.

As internal IR teams receive additional investment and grow, it will be interesting to see if the percentage of organizations contracting for external, specialist assistance continues to grow. Many analysts predict that it will. However, disruptive forensics and threat detection technologies, along with wider use of high-fidelity threat intelligence feeds, may also have an impact.

Incident Response Assistance

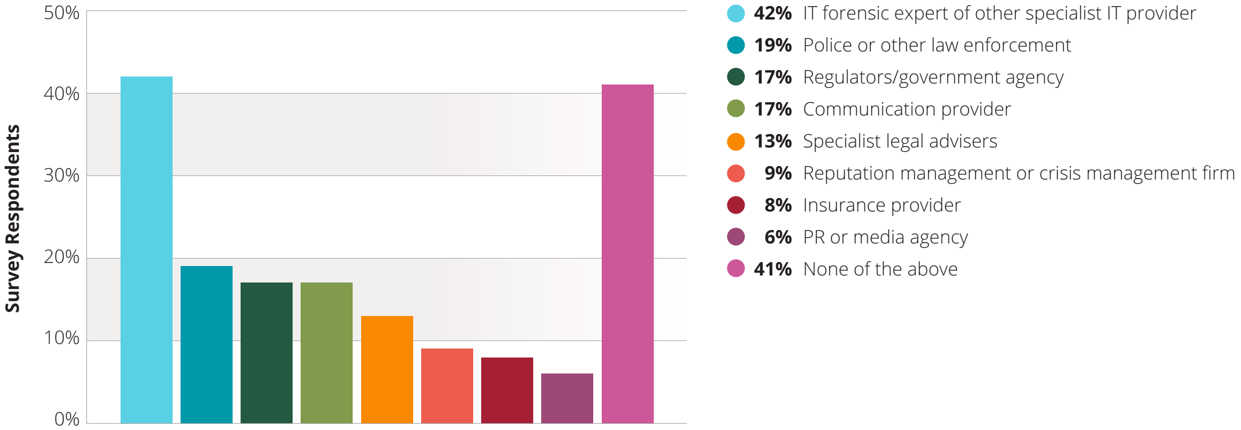


***Figure 88** Source: Arbor Networks, Inc.*

Just over one-quarter of EGE respondents indicate they have seen an increase in incident frequency (Figure 89). In general, the results this year are broadly similar to last year, with the rate of change much lower than seen with service provider responses. It appears that incident frequencies have been more stable for EGE organizations.

Incident Response Rate

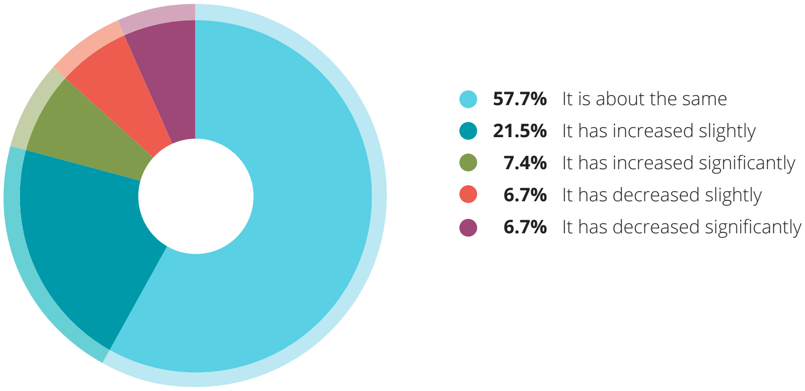


Figure 89 *Source: Arbor Networks, Inc.*

Looking at how EGE respondents rate their preparedness for dealing with an incident, results are broadly similar to last year (Figure 90). They are also similar to those seen from service provider responses this year. On a positive note, the proportion of EGE respondents indicating they have made no preparations has dropped, from 10 percent last year to 6 percent this year, but the fact that any organizations have stated this is a surprise. The costs of preparing are much lower in the long run than becoming a victim.

How Prepared Are You?

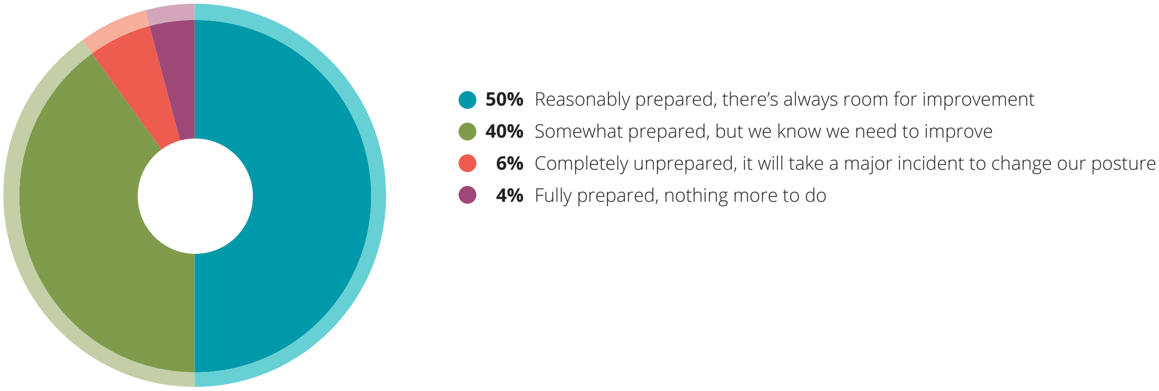


Figure 90 *Source: Arbor Networks, Inc.*

In terms of improving preparedness, we see some changes in the results. Last year, deploying more automated threat detection solutions was the most common response. This year, it is deploying solutions that speed up the incident response process (Figure 91). A significantly higher proportion are now looking at this, up from 45 percent to 57 percent. This emphasizes the problems that many security teams face: too many events, too few resources and slow/poorly integrated toolsets. It is encouraging that EGE respondents are looking for solutions here.

On a more negative note, we see a big drop in the proportion of respondents who are looking to increase their internal resources to improve preparedness, down from 46 percent to 38 percent. However, compared to our service provider segment, a far higher proportion of EGE respondents is looking at outsourcing to fill the gap — 27 percent versus 15 percent. Looking for help externally is likely a better choice for EGE respondents in the short term as they look to build internal teams. However, utilizing internal teams is likely cheaper and more effective in the longer term.

Improving Preparedness

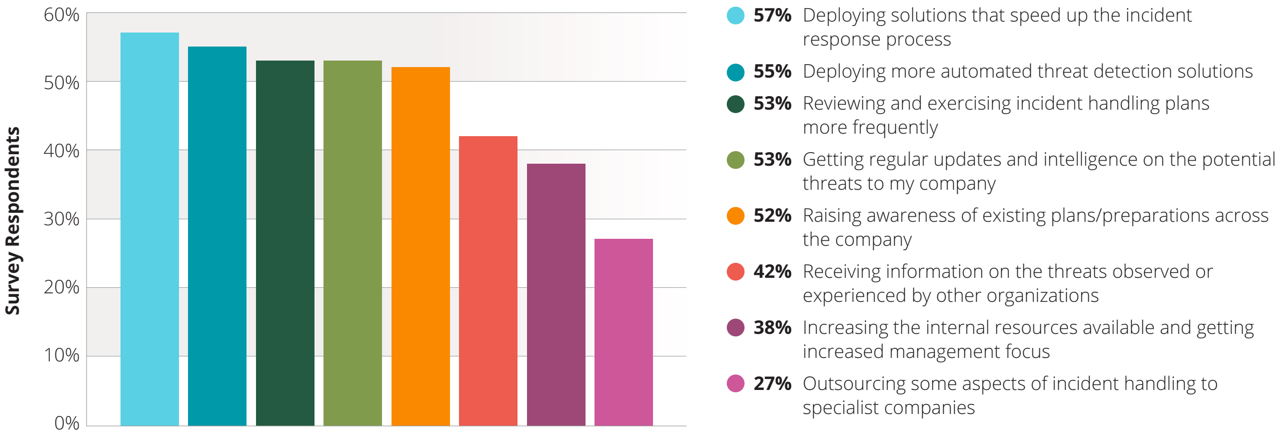


Figure 91 *Source: Arbor Networks, Inc.*

Moving on to look at the tools used to detect threats, as we stated earlier in the service provider section, the use of multiple tools means that defense in depth is an actuality, not just a good idea. Similar to last year, firewalls and SIEM are the most commonly utilized tools (Figure 92). In third place are NetFlow analyzers, again with a similar result to last year. However, the use of forensic packet analysis tools increased by 9 percent this year — a big jump. It is also interesting to note that far more EGE respondents than service provider respondents appear to be adopting forensic packet analysis tools. Looking at specific verticals, it is noteworthy that only 25 percent of banking respondents use forensic packet analysis, as opposed to 47 percent of government organizations.

Technologies such as sandboxes have continued to see incremental deployment. It is interesting that the results here seem to indicate continued investment in multiple point detection solutions. This ties in with the fact that although “deploying solutions that speed up incident response” is now the top approach EGE organizations are looking at to improve incident response, the proportion looking to invest in additional automated detection tools has not reduced.

Threat Detection

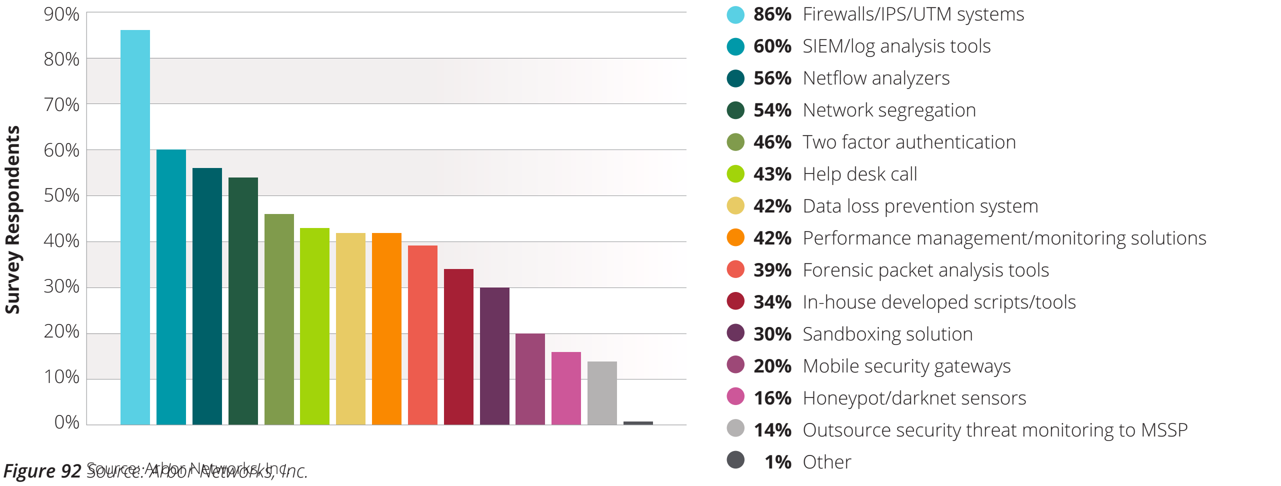


Figure 92 *Source: Arbor Networks, Inc.*

Source: Arbor Networks, Inc.

This year, when asking how organizations have "actually" detected incidents, we see a reduction in the proportion of respondents citing almost every mechanism. However, automated detection is still the most common way in which EGE respondents have detected incidents (Figure 93). In fact, the results from EGE respondents are quite different from those of service providers. The service provider results show an increase in routine checks and controls being used to detect incidents, moving it into the top spot. For EGE respondents, the utility of this mechanism appears lower, with only 46 percent detecting incidents in this way, down from 52 percent last year. This may indicate that the processes service providers have in place to detect unusual or suspicious activity are more advanced.

Actual Detection Methods and Sources

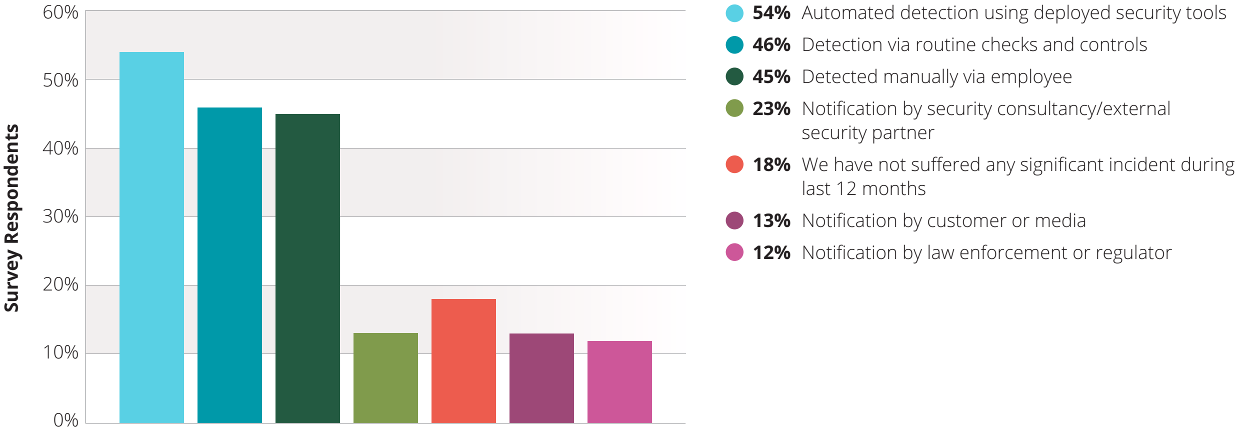


Figure 93 *Source: Arbor Networks, Inc.*

For the first time this year, the survey asked EGE respondents whether they have taken out insurance regarding cyber security incidents (Figure 94). Twenty-three percent indicate that they already have something in place, with a further 8 percent planning for next year. These results are almost identical to those of our service provider respondents.

Interestingly, the EGE insurance adoption rate is lower than expected given anecdotal information obtained by Arbor during recent meetings. However, these meetings were mainly within the financial sector, which does have a higher adoption rate (29 percent, according to survey data). It will be interesting to see if the rapid growth in the adoption of insurance among service provider respondents will continue and surpass insurance use in the EGE segment.

Insurance Against Cyber Incidents

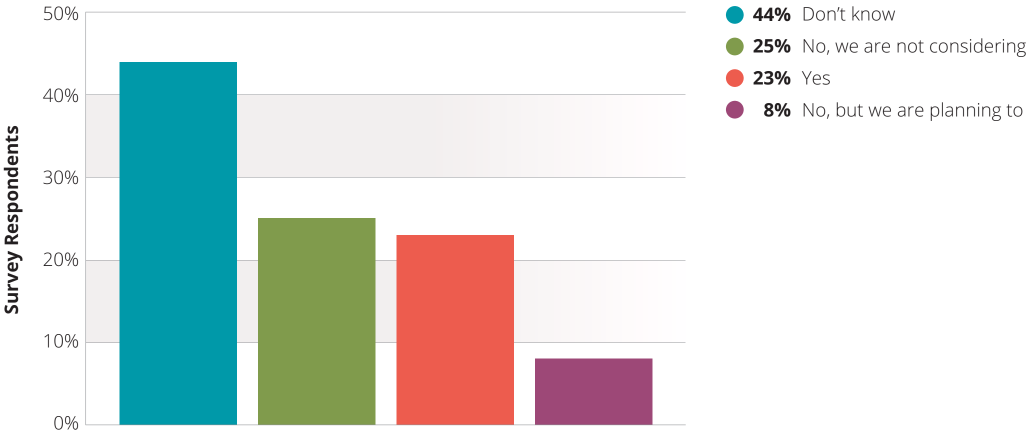


Figure 94 *Source: Arbor Networks, Inc.*

Intelligence sharing is a commonly heard term in the industry, and has become somewhat of a "hot topic." Most vendors with threat detection solutions have a community they want their customers to join. Some are free, others are not; all propose to keep your submission of information anonymous, and claim to have the best intel sharing and analysis in the market. We asked survey respondents which intelligence sharing organizations they currently work with. Surprisingly, there was very little commonality in the responses. ISSA (Information Systems Security Association) is the only very common organization mentioned, with around one-third of participants working with them.

This year, we introduced some new questions directed at the end user community. First, we inquired as to the state of end user education on basic security — i.e., are users taught not to click on email links, not to disable the local firewall or AV, etc.? Encouragingly, 70 percent of EGE organizations feel their user community is properly educated, a 6 percent higher result than our service provider respondents.

It is important to keep current security issues top of mind for employees. As a result, we added a second question to this year's survey to establish if organizations regularly update their employees' security training and require periodic re-certification. Sixty-two percent update their security education and require regular re-certification. This is a slightly higher proportion than seen within the service provider space, and may indicate that enterprises are more focused and process-oriented when it comes to employee education around security.

As a frame or reference, NETSCOUT, Arbor's parent company, has an annual re-certification program designed to help ensure that the company has the right policies, processes and procedures to protect both the company's confidential information and trade secrets, as well as the personal information of its employees, customers and partners.

BYOD and the IOT have made perimeter security a moving target since even organizations with the highest security and the most to lose must allow access, even if it is limited and closely monitored. This is true in both service provider and enterprise organizations. Nearly 40 percent of all enterprise respondents still do not have anything deployed to monitor BYOD devices on the network, this represents a 6 percent improvement over last year but is still quite shocking (Figure 95).

Monitoring BYOD Devices

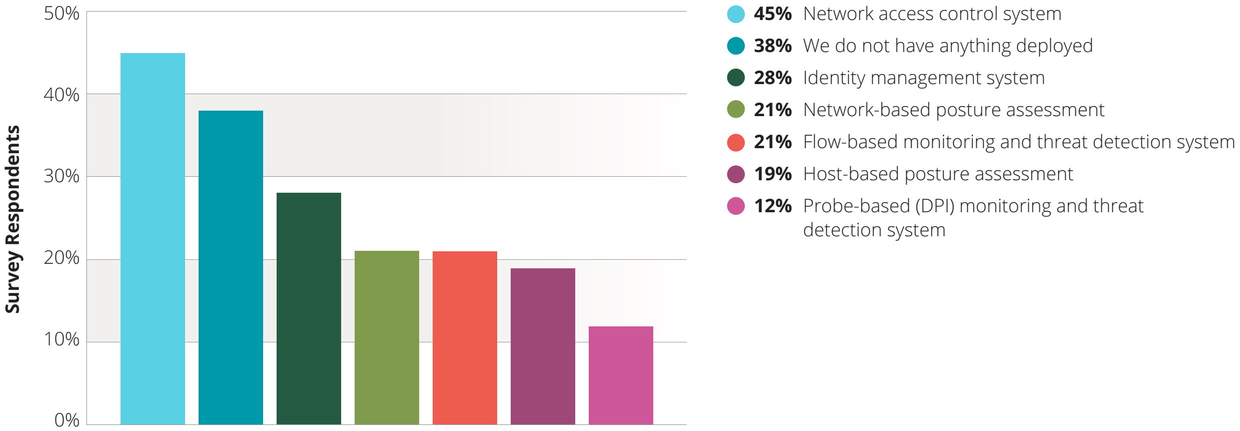


Figure 95 *Source: Arbor Networks, Inc.*

How enterprises restrict BYOD devices is more in line with what one would expect. However, these results do illustrate that the service provider world is more advanced in its use of policy-based restrictions for BYOD network access and also security software installed on devices (Figure 96). While implementing access limitations for employee-owned devices has increased among enterprises this year, most other categories have remained static. The only other change of note is in the reduced use of MDM by over 10 percent. This could be a cost issue, but it needs to be addressed, as BYOD is not going away.

Restricting BYOD

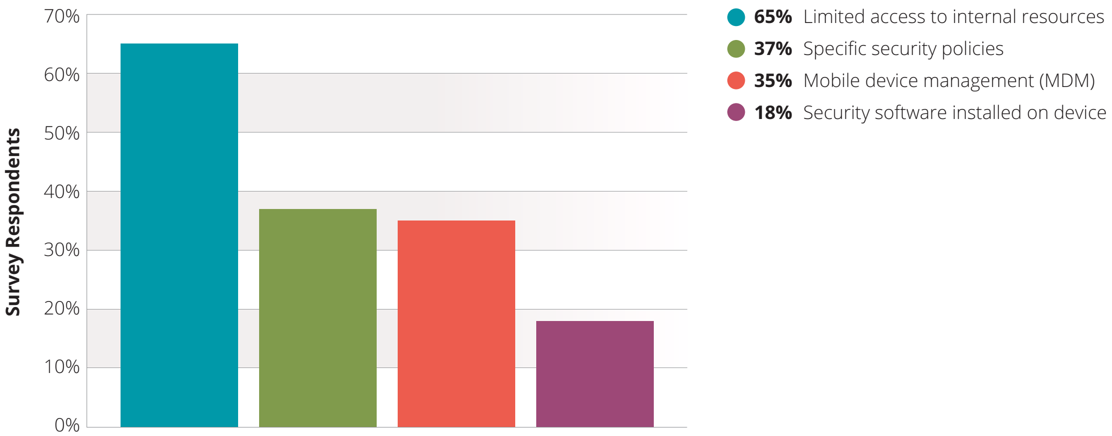


Figure 96 *Source: Arbor Networks, Inc.*

A lower proportion of EGE respondents prohibit the sharing of company data over public cloud services, down to 55 percent this year from over 60 percent last year. This is a concerning move in the wrong direction. The increased acceptance of cloud data synchronization is more likely due to the proliferation of BYOD, rather than actual company policies allowing or approving it. Each year, as we see more security issues around cloud or BYOD, companies should gain more leverage to implement adequate security policies.

This year, the proportion of respondents who have seen security incidents relating to BYOD has doubled, to 13 percent from 6 percent last year. This mirrors the increase seen from our service provider respondents. These increases support the standpoint many security professionals have taken for years: BYOD can represent a significant risk. As we can see here, data is now starting to become available that clearly supports this viewpoint, and that should allow the implementation of stricter controls around BYOD.

ASERT MALWARE TRENDS

The Arbor Security Engineering & Response Team (ASERT) at Arbor Networks delivers world-class network security research and analysis for the benefit of today's enterprise and network operators. ASERT engineers and researchers are part of an elite group of institutions that are referred to as "super remediators." Our team represents the best in information security. This is a reflection of having both visibility and remediation capabilities at a majority of service provider networks globally.

ASERT shares operationally viable intelligence with hundreds of international computer emergency response teams (CERTs) and with thousands of network operators via intelligence briefs and security content feeds. ASERT also operates the world's largest distributed honeynet, actively monitoring Internet threats around the clock and around the globe via ATLAS®, Arbor's global network of sensors (atlas.arbor.net). This mission and the associated resources that we bring to bear to the problem of global Internet security are an impetus for innovation and research.

Continued Use of HTTP in Malware

While it is common to see malware use HTTPS to communicate with command and control, we expected to see a major shift away from HTTP to HTTPS this year. However, when we look at the trend for usage of port 80 or 443 within malware, we see both as trending flat through the year. (Figure AS.1 has been normalized against the total number of new malware samples imported.)

Normalized Samples Communicating via Port 80

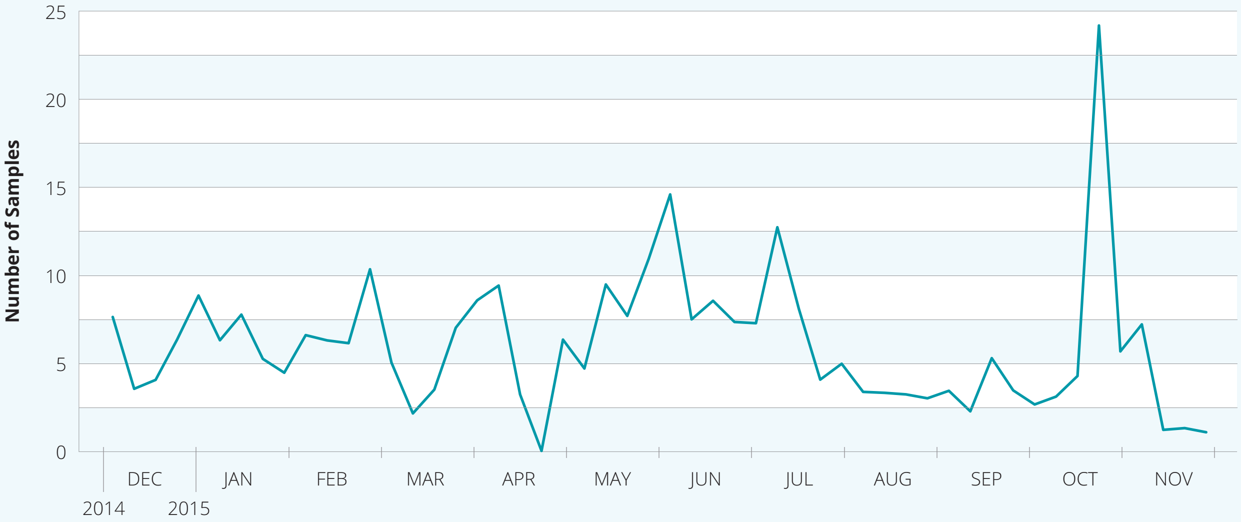


Figure AS.1 *Source: Arbor Networks, Inc.*

Russian Domains Still A Large Portion of Botnet-Based DDoS Targets

ASERT collects detailed information about the daily workings of many malware command and control systems. By collecting information sent to botnet drones, we are able to see who is being targeted by DDoS attacks launched from those drones (Figure AS.2). RU domains still dominate the total number of distinct domains targeted by DDoS bots in 2015. However, it does appear that the differential with other country TLDs has decreased somewhat, but it is not currently known why this fallout was observed.

Many smaller sites (gaming, gambling, etc.) seem to be the popular targets. And DDoS seems to be a cost of doing business in this area.

Botnet-Based DDoS Targets by TLD

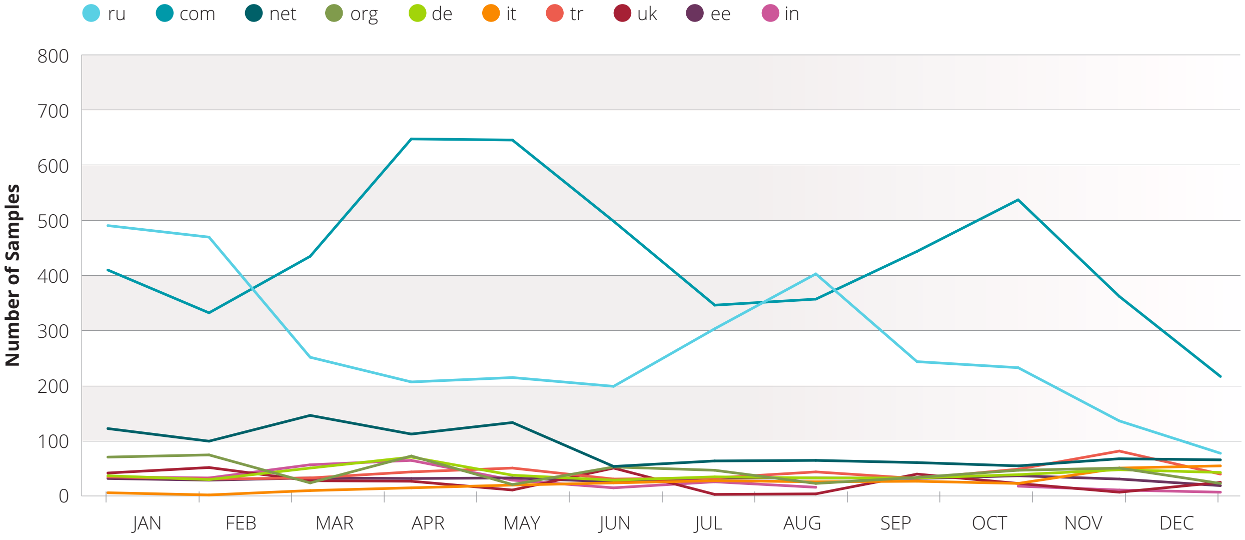


Figure AS.2 *Source: Arbor Networks, Inc.*

Iterative Malware Development

Over weeks and years, we witness a constant churn of malware development. As old samples are analyzed and detected by security vendors and their products, new variants are developed by malware authors and deployed. Two examples of this can be seen in Dyreza and Upatre.

In Figures AS.3 and AS.4, you can clearly see older variants fall out of popularity as the next variant starts to gain in popularity. This illustrates the breakneck pace of the arms race that pits security vendors against malware authors.

Upatre

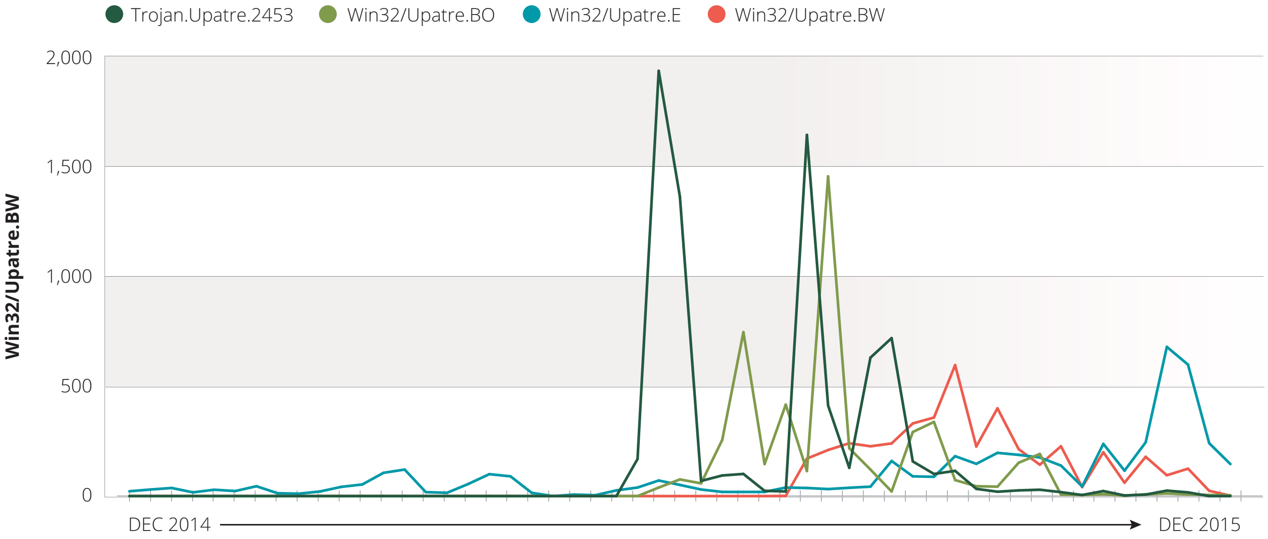


Figure AS.3 *Source: Arbor Networks, Inc.*

Dyreza

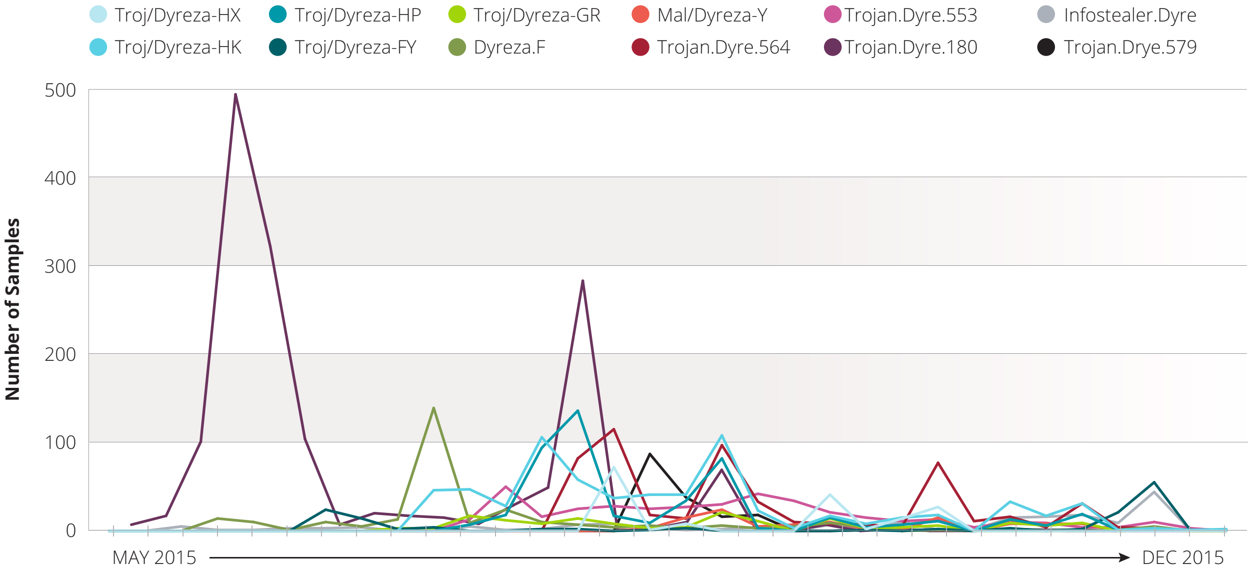


Figure AS.4 *Source: Arbor Networks, Inc.*

ASERT ANALYSIS SUMMARY: COREBOT

This section is a summary of an ASERT threat intelligence brief called "Dumping Core: Analytical Findings on Trojan CoreBot," and is included as an example of current malware trends and behaviors.

The CoreBot malware family is relatively new and was first documented by Security Intelligence in August 2015. Since then, the malware has evolved fairly rapidly and has added new capabilities. CoreBot now appears to be in the same league of full-blown banking trojans such as Dyreza, Neverquest/Vawtrak, Zeus, etc.

This summary documents some of ASERT's recent findings regarding CoreBot's cryptography, network behavior and banking targets. For further details, please see asert.arbornetworks.com.

Command and Control

CoreBot uses HTTP POST requests to communicate with its command and control (C&C) infrastructure; various APIs provided by the WinHTTP library are used to perform these communications. The underlying plain text format of CoreBot C&C request data varies, depending on the nature of the request. However, in all cases, the POSTed data undergoes RC4 encryption and is then Base64-encoded.

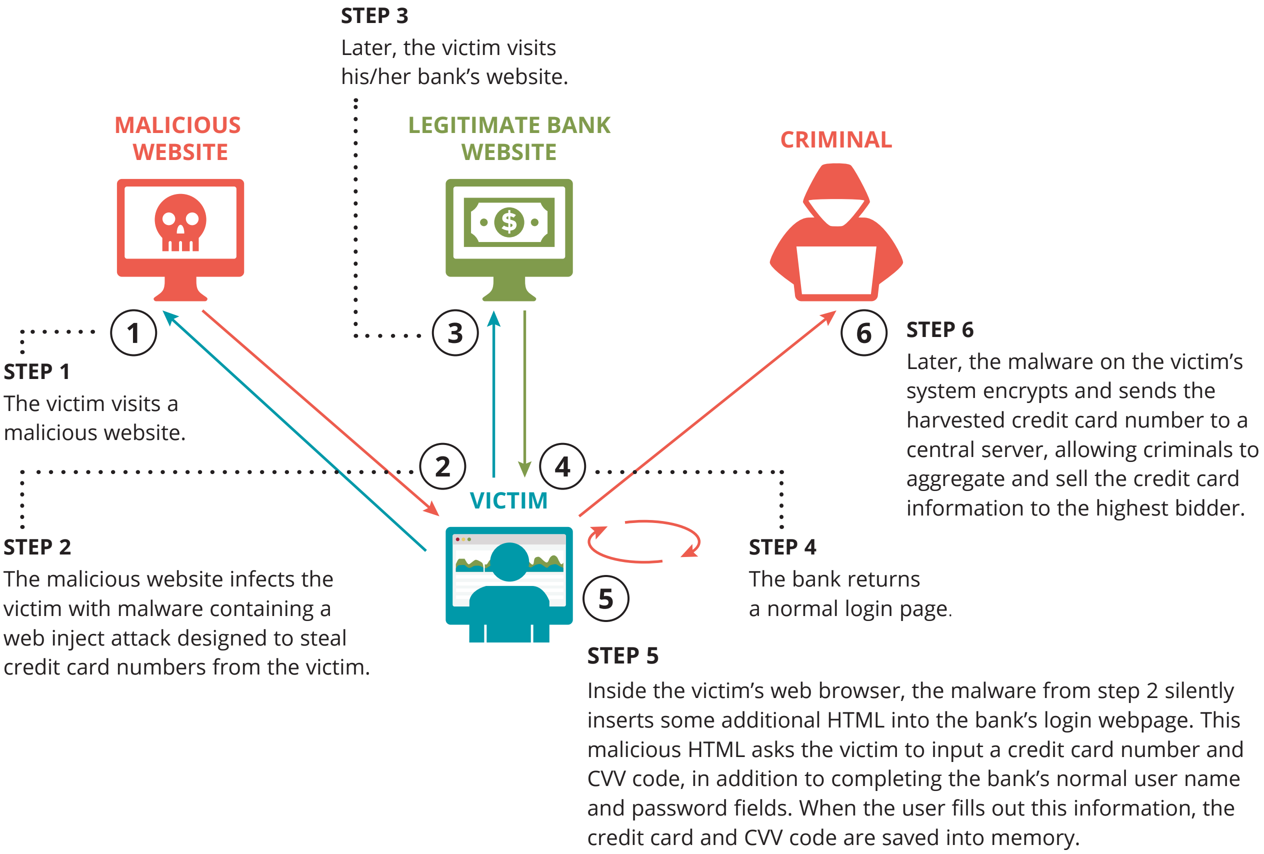
Responses from the C&C are also RC4-encrypted using the same key. However, instead of being Base64-encoded, they are sent in binary form. These binary responses are broken up into reasonably sized chunks via HTTP-chunked transfer encoding. CoreBot's network communications protocol also supports the ability for the C&C to push a new C&C URL to the bots. In this case, the response from the C&C will contain the new URL as a string token.

Capabilities

One of the distinguishing characteristics of CoreBot is its plugin-centric architecture in which most malicious functionality is implemented in the form of modular plugins. A brief overview of the capabilities of CoreBot appears below.

- **Screenshot Upload:** The core CoreBot engine supports the ability to capture screenshots of the infected host's desktop and upload them back to the C&C.
- **Stealer Mechanism:** The stealer plugin contains a lengthy list of approximately 134 different information-pilfering routines. Each routine is customized for stealing a particular type of information, such as FTP credentials, passwords, etc., from specific applications or locations on the infected host.
- **Man-in-the-Middle (MITM) Mechanism:** The MITM plugin's listening code can inspect and modify all browser traffic before forwarding it to its original destination (hence the name of the plugin). This allows it to perform web injections against a variety of targeted financial institutions.

The web injection's "style" of data theft usually takes the following form:



STEP 1
The victim visits a malicious website.

STEP 2
The malicious website infects the victim with malware containing a web inject attack designed to steal credit card numbers from the victim.

STEP 3
Later, the victim visits his/her bank's website.

STEP 4
The bank returns a normal login page.

STEP 5
Inside the victim's web browser, the malware from step 2 silently inserts some additional HTML into the bank's login webpage. This malicious HTML asks the victim to input a credit card number and CVV code, in addition to completing the bank's normal user name and password fields. When the user fills out this information, the credit card and CVV code are saved into memory.

STEP 6
Later, the malware on the victim's system encrypts and sends the harvested credit card number to a central server, allowing criminals to aggregate and sell the credit card information to the highest bidder.

CoreBot: The Future

Because of the number of features and well-written code of CoreBot, we expect to see a large increase in the number of malware samples in the coming months. Figure AS.5 is a graph of the samples we have received so far this year.

CoreBot Sample Rate

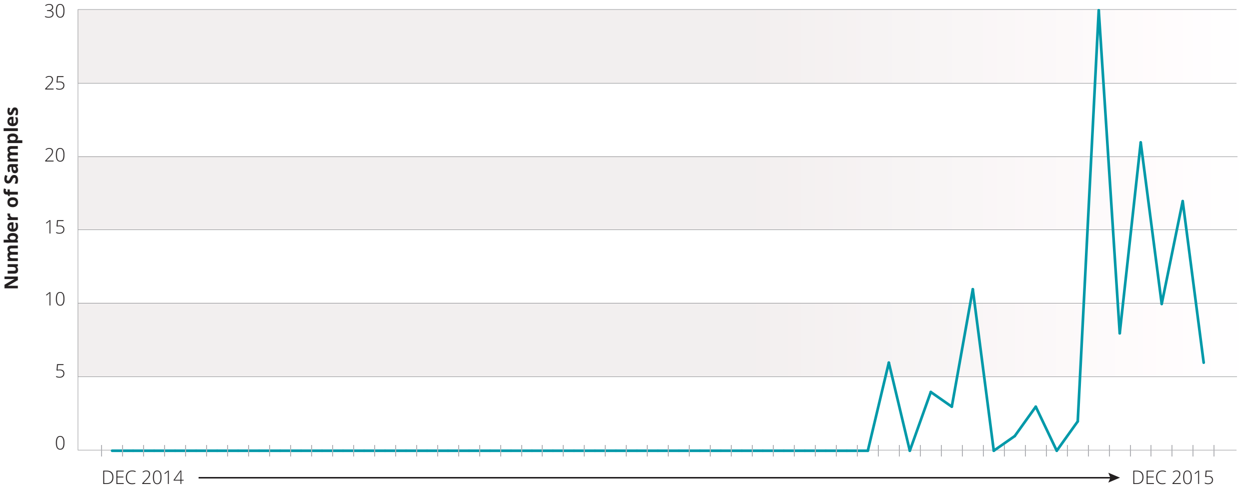


Figure AS.5 *Source: Arbor Networks, Inc.*

We expect CoreBot samples to increase rapidly in the coming months. Eventually, we expect it to mirror other similar malware such as Neverquest, whose sample graph can be seen in Figure AS.6.

Neverquest Samples

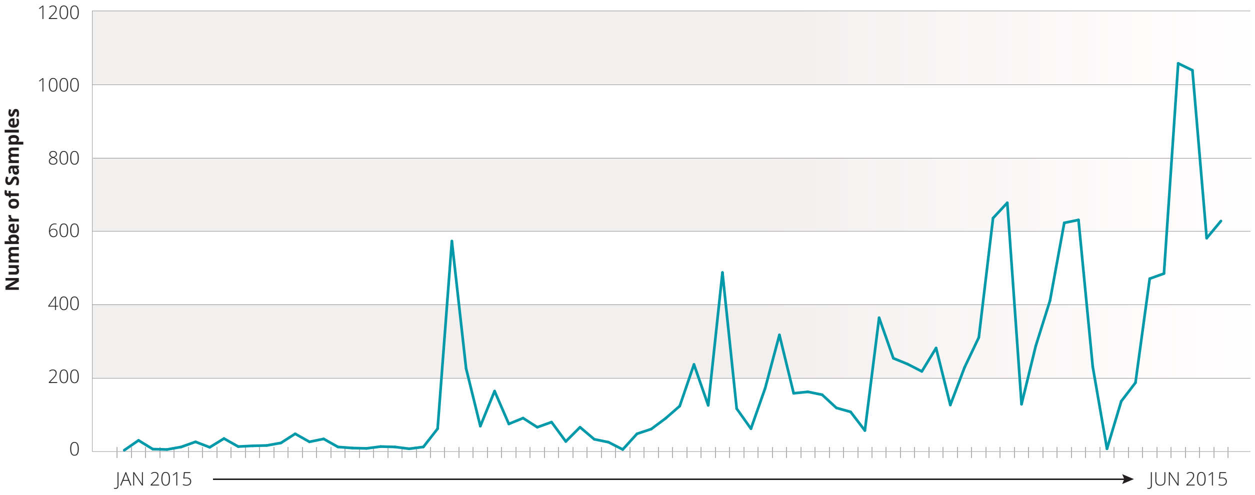


Figure AS.6 *Source: Arbor Networks, Inc.*

Conclusion

As stated earlier, the CoreBot malware family is relatively new. It has evolved fairly rapidly and now appears to be ready to join the ranks of other full-blown banking trojans such as Dyreza, Neverquest/Vawtrak, Zeus, etc. ASERT will continue to monitor and track CoreBot over time, and may have already released additional information since this document was published. To catch up on the latest developments in the CoreBot malware family and other active threats, please check out the ASERT blog here: asert.arbornetworks.com.

ENTERPRISE, GOVERNMENT AND EDUCATION DDOS ATTACKS

Thirty-four percent of the enterprise, government and education organizations report that they have experienced DDoS attacks over the past year. Among those, over one-quarter indicate they suffered more than 10 attacks per month, and about half say the attacks exceeded their total Internet capacity. Over half of organizations had firewall or IPS devices experience a failure or contribute to an outage during an attack, a significant uptick from last year. Respondents report that 24 percent of attacks targeted the application layer, a significantly higher proportion than the 18 percent reported by service providers. The most commonly perceived motivations behind DDoS attacks are now "criminals demonstrating attack capabilities" and "criminal extortion attempts."

On a very encouraging note, 43 percent of respondents indicate they are now using intelligent DDoS mitigation systems (IDMS), compared to around one-third last year. In a significant improvement over last year, nearly double the percentage of respondents indicate that they can immediately mitigate DDoS attacks via an "always-on" device or service. Further, just over one-quarter are able to mitigate in less than 15 minutes. Operational expenses, reputation/brand damage and direct revenue loss are the top business impacts of DDoS attacks.

This year, 34 percent of respondents representing enterprise, government and education (EGE) organizations have witnessed DDoS attacks during the past year. However, this percentage does vary by vertical; for the banking and government verticals, the percentages are higher, at 45 percent and 43 percent respectively.

Among those that have seen attacks, over one-quarter indicate they suffered more than 10 attacks per month (Figure 97), and about half say the attacks exceeded their total Internet capacity. This represents a significant increase from 40 percent last year and also aligns with the increased demand for cloud/service provider DDoS mitigation services seen from service provider respondents to this survey. The successful mitigation of such attacks requires the use of a cloud or service provider-based service.

DDoS Attack Frequency

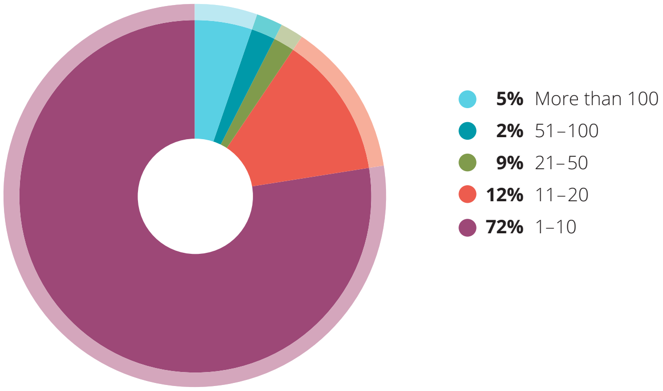


Figure 97 *Source: Arbor Networks, Inc.*

Looking at the targets of DDoS attacks (Figure 98), the majority are aimed at customer-facing services and applications, as last year. However, over half of respondents also indicate that they have seen attacks targeting infrastructure such as routers, load balancers, firewalls and overall network bandwidth. This again reinforces the fact that attackers are more frequently targeting infrastructure when they realize that services are well defended.

Targets of DDoS Attacks

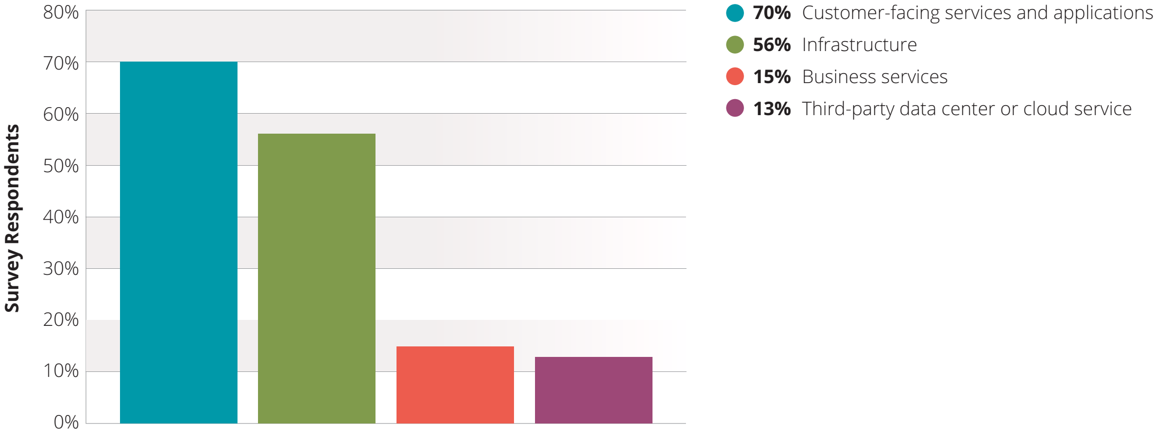


Figure 98 *Source: Arbor Networks, Inc.*

Over half of EGE respondents had firewall or IPS devices experience a failure or contribute to an outage during an attack. This is concerning, given that only 35 percent reported these failures last year. While firewalls provide a valuable layer in defensive strategies, they can become the target of DDoS attacks due to their stateful nature, and need to be protected themselves.

Concerning the duration of the longest DDoS attacks, the vast majority (88 percent) of organizations report attacks lasting less than one day (Figure 99). Nearly 60 percent report seeing their longest attack end in seven hours or less.

DDoS Attack Duration

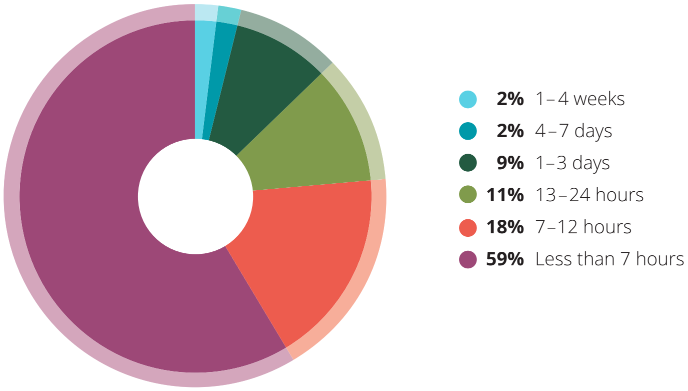


Figure 99 *Source: Arbor Networks, Inc.*

DDoS attacks can be broken out into one of three main categories: volumetric, state-exhaustion and application-layer. Of the attacks reported by EGE organizations this year, 58 percent were volumetric in nature (Figure 100) — less than the 65 percent reported by service providers. However, 24 percent of attacks targeted the application layer, a significantly higher level than the 18 percent reported by service providers. This may be due to the fact that service providers are not aware of all the application-layer attacks traversing their networks, given their macroscopic network view. This reinforces the need for a layered DDoS defense for EGE organizations.

It should also be noted that last year's EGE respondents saw 29 percent of attacks targeting the application layer, a higher percentage than this year. Anecdotally, Arbor is not aware of any reduction in application-layer attack frequency based on conversations with customers.

Attack Category Breakout

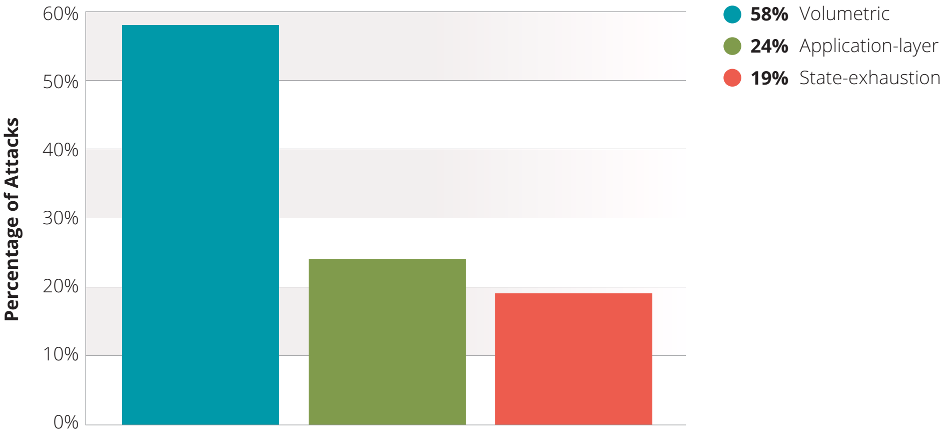


Figure 100 Source: Arbor Networks, Inc.

The primary target for application-layer attacks reported by EGE respondents is web services. Over 80 percent saw attacks targeting HTTP (Figure 101), and over half saw attacks against HTTPS and DNS. Overall, these results are almost identical to last year. Interestingly, service providers have seen DNS become the top application-layer target this year, but this difference is likely due to the types of infrastructure supported and monitored by the different respondent categories.

Targets of Application-Layer Attacks

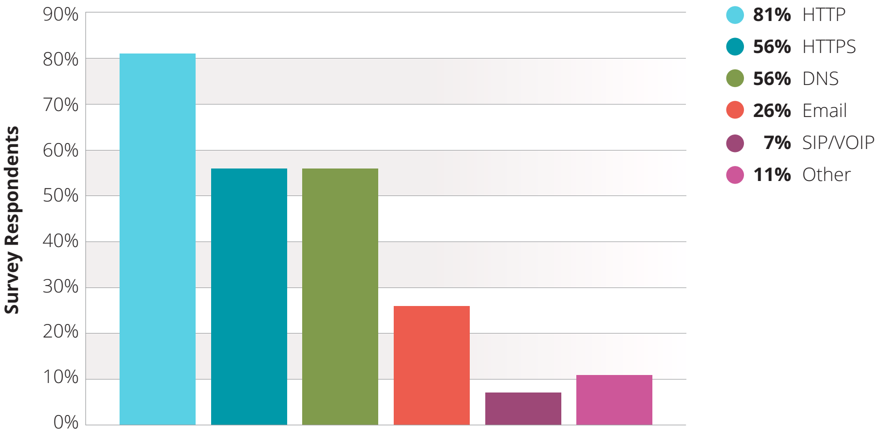


Figure 101 Source: Arbor Networks, Inc.

Regarding DDoS attacks targeting encrypted web services, these have become increasingly common in recent years. Nearly half of this year's EGE respondents have observed volumetric attacks targeting UDP/TCP port 443 (Figure 102). Thirty-seven percent have seen attacks targeting the encrypted service at the application layer — a much higher level than seen by our service provider respondents (20 percent). A higher proportion of EGE respondents have also seen attacks targeting the SSL/TLS protocol — 42 percent compared to just 20 percent of service providers. The variation in results between end user and service provider respondents is, as noted above, likely due to the higher granularity of visibility available when the monitoring solution is closer to the services being attacked (and potentially the ability to look inside encrypted traffic).

Encrypted Application-Layer Attacks

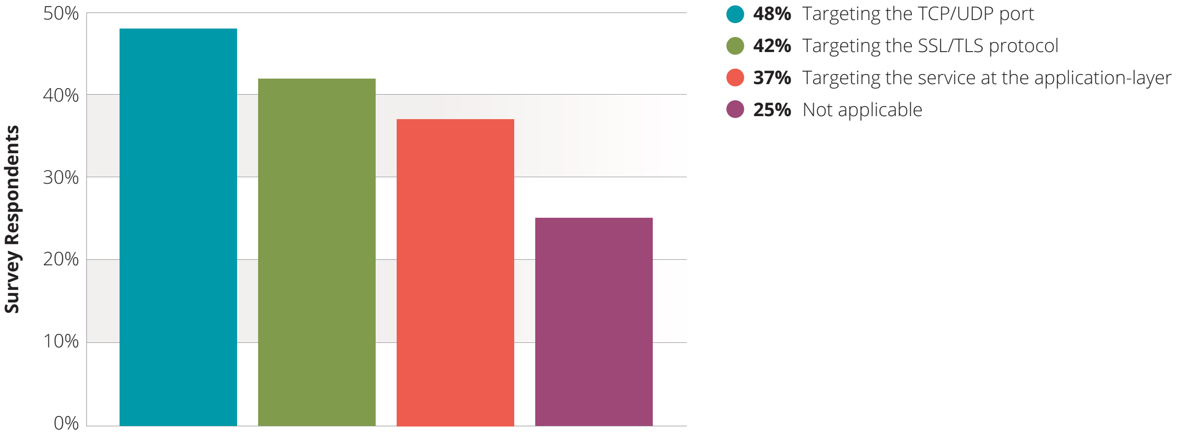


Figure 102 *Source: Arbor Networks, Inc.*

Multi-vector DDoS attacks combine multiple attack techniques concurrently, aimed at the same target, to increase both the attacker's chance of success and the mitigation complexity. Forty-three percent of EGE respondents report seeing multi-vector DDoS attacks in the past year (Figure 103), an identical result to last year. As mentioned earlier in this report, the proportion of service providers seeing multi-vector attacks jumped substantially. The fact that this is not mirrored among EGE organizations may be the result of attacks (or some portions of attacks) being mitigated upstream.

Multi-Vector Attacks

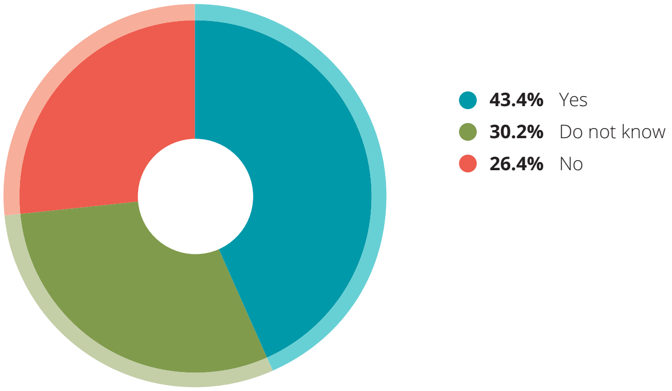


Figure 103 *Source: Arbor Networks, Inc.*

DDoS attack motivation continues to cover a wide and varied spectrum, as in previous iterations of the survey. However, we have seen some big changes in the most common motivations perceived by EGE respondents. These changes are consistent with those noted by service provider respondents. The most commonly perceived motivations behind DDoS attacks are now “criminals demonstrating attack capabilities” and “criminal extortion attempts” (Figure 104). Both of these motivations have seen significant growth in the last year among EGE respondents. The previous number one motivation, “political/ideological hacktivism,” is now only perceived as common by 16 percent of respondents, down from 36 percent last year. Anecdotally, this ties in with a perceived reduction in activity in this area.

The rise in the proportion of respondents who cite extortion as a common motivation is expected, given the broad use of DDoS in this regard, including the DD4BC attack campaign (see ASERT insert).

The rise of “criminals demonstrating their capabilities” is indicative of the ease with which DDoS attacks can now be procured and carried out for any and all reasons. The proliferation of booter and stresser services (DDoS for hire) is a growing and serious problem.

Finally, and in contrast to the trend seen from service providers, a lower proportion of EGE respondents are seeing “diversion to cover other criminal activity” as a common motivation for attack — down from 16 percent to 12 percent this year. This is surprising, especially given the big increase in service providers citing this motivation, as well as other independent surveys that have seen this as a key area of growth.

DDoS Attack Motivations

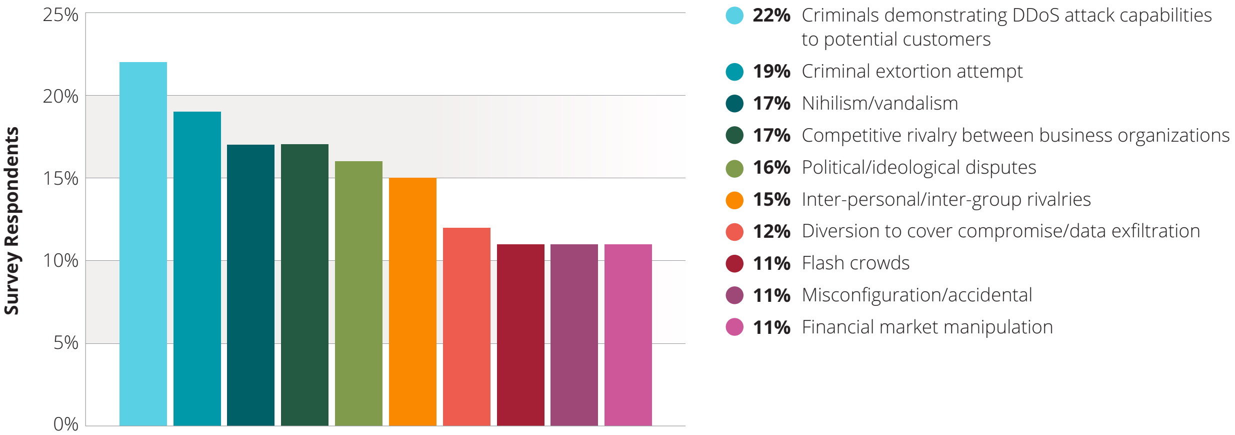


Figure 104 *Source: Arbor Networks, Inc.*

Given the continued growth in reliance on cloud services, their availability has become paramount. We asked enterprise, government and education participants whether they have seen DDoS attacks against the cloud services they use. One-quarter of respondents indicate that they have seen attacks, compared to about one-third of service providers. It is logical that the operators of cloud services are more likely to witness these attacks.

Regarding DDoS mitigation techniques deployed in enterprise, government and education networks, firewalls remain the most common mechanism (Figure 105), with 53 percent citing their use. However, this percentage has fallen substantially from 72 percent last year.

Access control lists are in second place, with an identical proportion of respondents using them as last year. In third place, IPS/WAF has seen growth in use from 43 percent last year to 47 percent this year. The continued use of firewalls and IPS/WAF for DDoS mitigation is a concern; it is well known that they are susceptible to state-exhaustion DDoS attacks, as evidenced by the 53 percent of EGE respondents who saw their firewalls fail due to DDoS attack during the survey period.

On a very encouraging note, 43 percent indicate they are using intelligent DDoS mitigation systems (IDMS), compared to around one-third last year. However, in a slight decline from last year, only 23 percent report having a layered DDoS mitigation strategy, which is the current best practice.

DDoS Mitigation Techniques

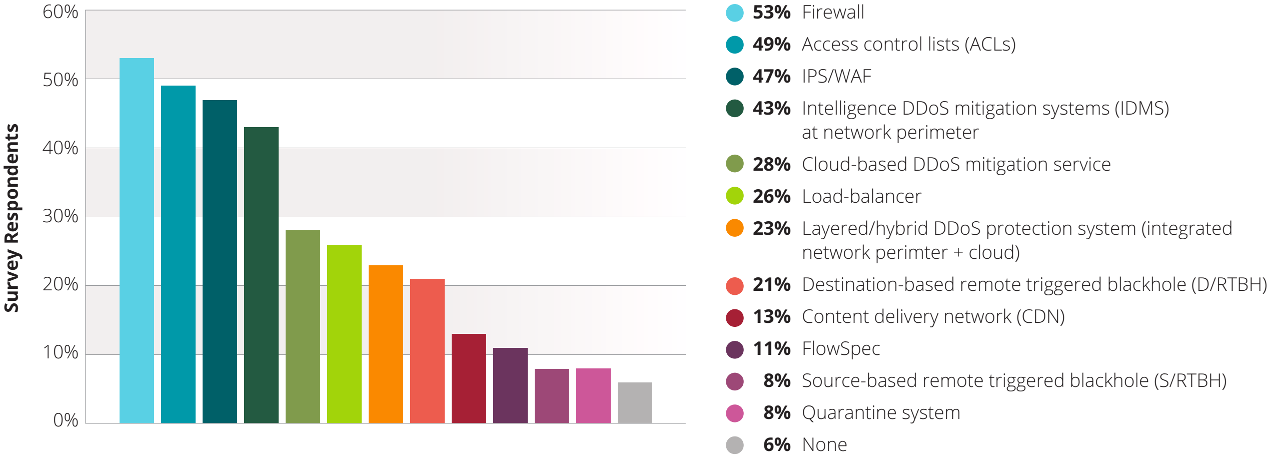


***Figure 105** Source: Arbor Networks, Inc.*

Mitigation time is key for DDoS attacks, as it can be a critical factor in controlling the cost of an attack to an organization. In a significant improvement over last year, nearly twice the percentage of EGE respondents indicate they can immediately mitigate an attack via an "always-on" device or service (Figure 106). Further, just over one-quarter are able to mitigate in less than 15 minutes. However, nearly as many measure their response time in hours, not minutes. Reducing mitigation times and deploying proactive defenses are becoming increasingly important. As more organizations become dependent on the Internet for business continuity, downtime becomes more costly.

DDoS Attack Mitigation Time

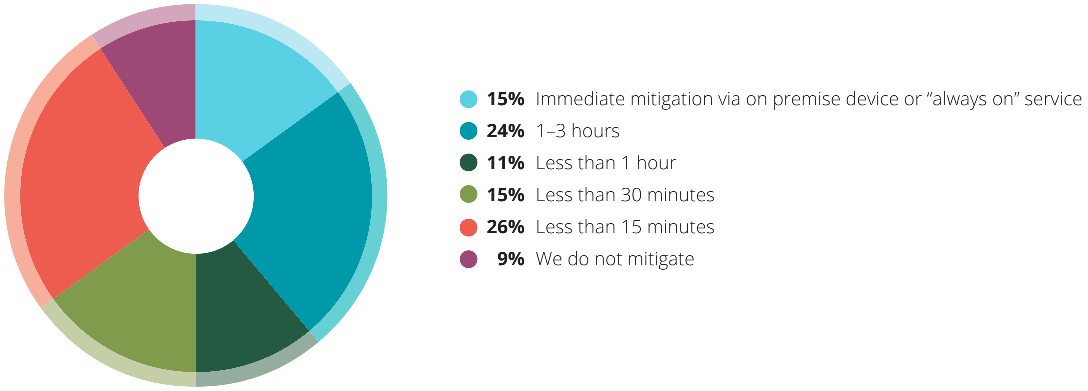


***Figure 106** Source: Arbor Networks, Inc.*

Organizations have observed a number of different business impacts as a direct result of DDoS attacks (Figure 107). About two-thirds cite operational expenses, and 36 percent indicate reputation/brand damage due to DDoS attacks. Nearly a third indicate direct revenue loss, and 17 percent cite customer loss. Another major impact is the cost of specialized IT security remediation and investigation services. Organizations should factor all of these costs into their calculations when looking at their investment strategies for defensive solutions.

Business Impacts of DDoS Attacks

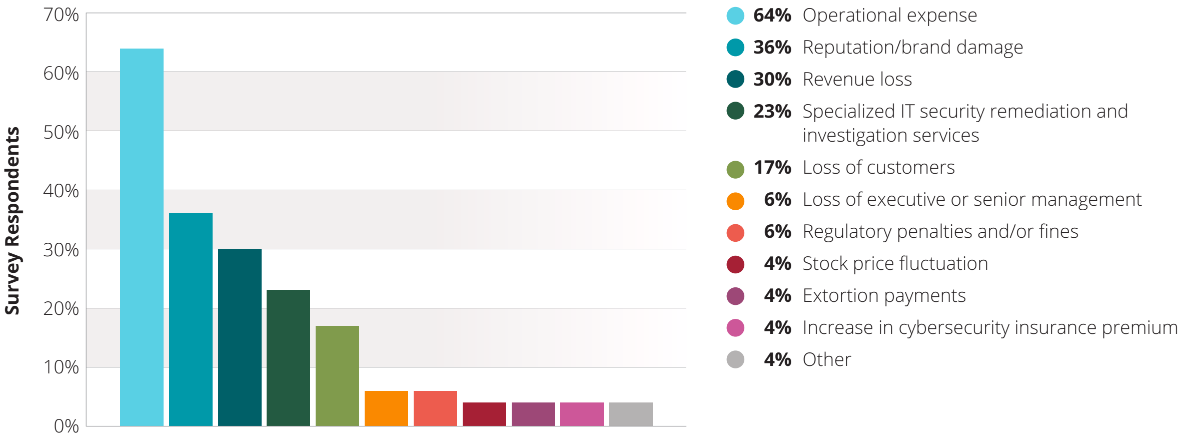


Figure 107 *Source: Arbor Networks, Inc.*

For the first time this year, we asked enterprise, government and education organizations to estimate the cost of Internet downtime (Figure 108). The vast majority of respondents to this section skipped this question, potentially indicating that they do not have a method to quantify the cost impact associated with the loss of Internet connectivity. Among those that did answer the question, nearly two-thirds estimate their costs above $500/minute, with some indicating much greater expense.

Cost of Internet Downtime

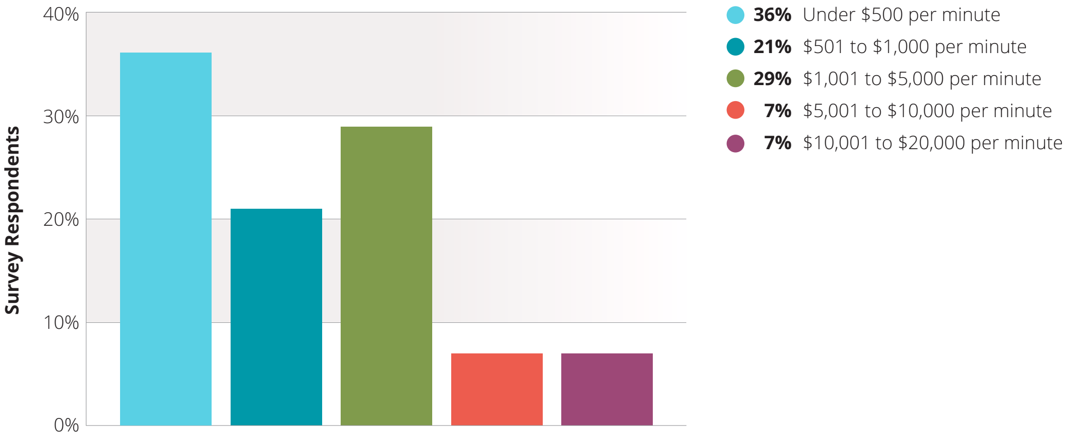


Figure 108 *Source: Arbor Networks, Inc.*

ENTERPRISE ORGANIZATIONAL SECURITY PRACTICES

This year, we added a specific section to this report covering organizational security practices for enterprise, government and education (EGE) respondents. The percentage implementing infrastructure security best practices is lower in general compared to service provider respondents. Only thirty-eight percent of EGE respondents indicate that they carry out DDoS defense simulations. Given that EGE respondents will likely see fewer attacks targeting their organizations, exercises are hugely important and should be scheduled at least quarterly.

A new section of this year's report covers organizational security practices for non-service provider respondents. The proportion of enterprise, government and education (EGE) respondents implementing infrastructure security best practices is lower in general compared to service provider respondents (Figure 109). This is expected, given that the focus on security best practices — especially around routing protocols and infrastructure — is usually less prevalent outside of the service provider space.

Interestingly, although the adoption rates for all best practices are lower for EGE respondents, the order of the mechanisms employed is almost identical to that seen within service providers. Fifty-six percent implement authentication for routing protocols, as opposed to 73 percent for service providers. This difference in adoption is fairly consistent across all best practices.

Best Current Security Practices

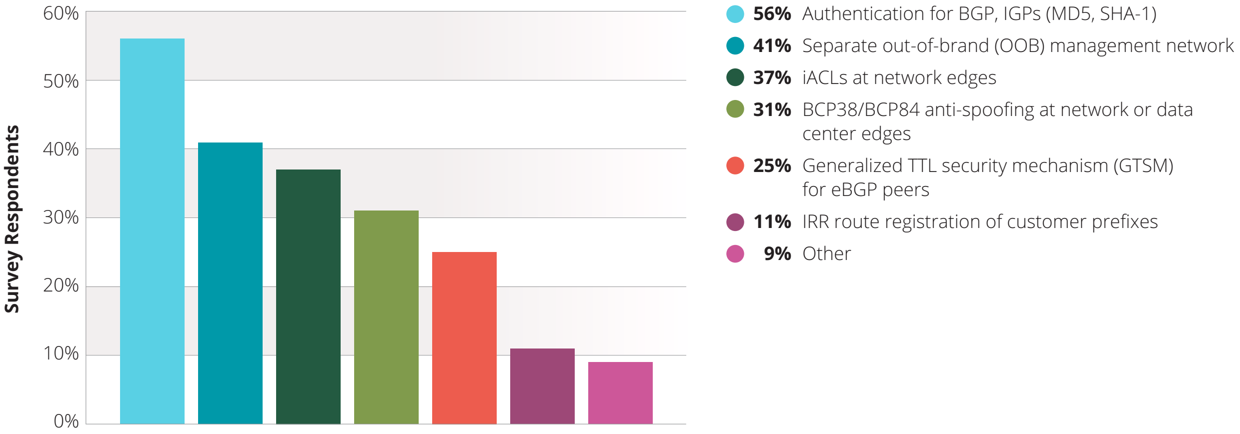


Figure 109 *Source: Arbor Networks, Inc.*

Dealing with a DDoS attack can be hugely stressful if teams and processes are not well rehearsed. Errors that result in the over-blocking of traffic or other service problems can exacerbate the impact of attacks. To streamline the effectiveness of security teams and tools, organizations should carry out regular DDoS defense exercises. Thirty-eight percent of EGE respondents indicate that they carry out DDoS defense simulations (Figure 110), a lower percentage than among service provider respondents (46 percent). Given that EGE respondents will likely see fewer attacks targeting their organizations, exercises are hugely important and should be scheduled at least quarterly. In the service provider space, 31 percent schedule exercises with at least a quarterly cadence. However, only 24 percent of EGE respondents adhere to this best practice.

With most organizations now dependent upon Internet services for their business continuity, DDoS attacks can have a significant operational and business impact. As a result, being adequately prepared is extremely important.

DDoS Simulations

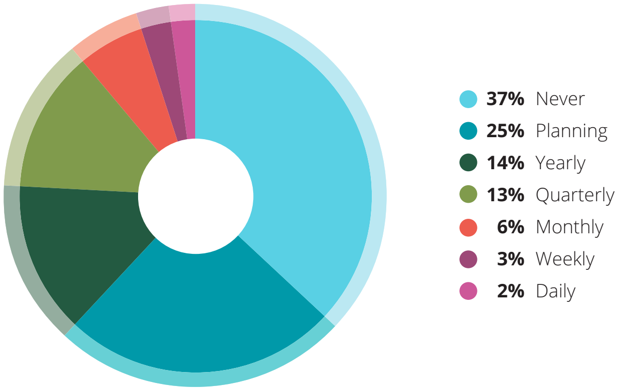


Figure 110 *Source: Arbor Networks, Inc.*

We also examined the proportion of respondents proactively filtering known botnet C&C traffic, etc. Seventy percent of EGE respondents filter this traffic, as opposed to only just over half of service providers. This is both expected and positive; it shows that EGE respondents are taking proactive steps to block threats that are directly applicable to their networks and business systems.

ENTERPRISE, GOVERNMENT AND EDUCATION IPv6

Around a quarter of enterprise, government and education (EGE) respondents indicate that they have already deployed IPv6 in their networks or plan to deploy it within the next 12 months. Fifty-eight percent have Internet-facing services available over IPv6. Half of the respondents have deployed IPv6 in their internal (private) network. More than 60 percent have deployed a solution to provide visibility of IPv6 traffic. The top security concern around IPv6 is DDoS attacks.

This year, only 26 percent of EGE respondents report that they have already deployed IPv6 or plan to deploy it in their network, compared to 30 percent last year. Within this group more than 55 percent have either completed their IPv6 deployment, or their deployment is already in progress.

When asked whether any of their Internet-facing services are available over IPv6, 58 percent answered "Yes," which is significantly higher than last year's 38 percent (Figure 111). The increase in IPv6 traffic seen in service provider networks is almost certainly due to the increase in enterprise provided services being made available over IPv6.

IPv6 Service Availability

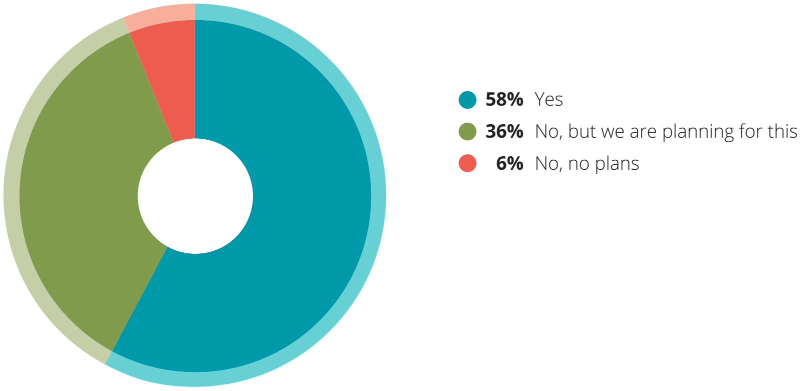


Figure 111 *Source: Arbor Networks, Inc.*

Fifty percent of enterprise EGE respondents report that they have already deployed IPv6 in their internal (private) network, with another 42 percent planning to do so in the future (Figure 112). This represents a general acceptance of IPv6 within corporate network infrastructure. With the number of devices connected to the IoT expected to reach 30 billion over the next five years, IPv6 will soon become a requirement for both service providers and enterprises alike.

Internal IPv6 Deployment

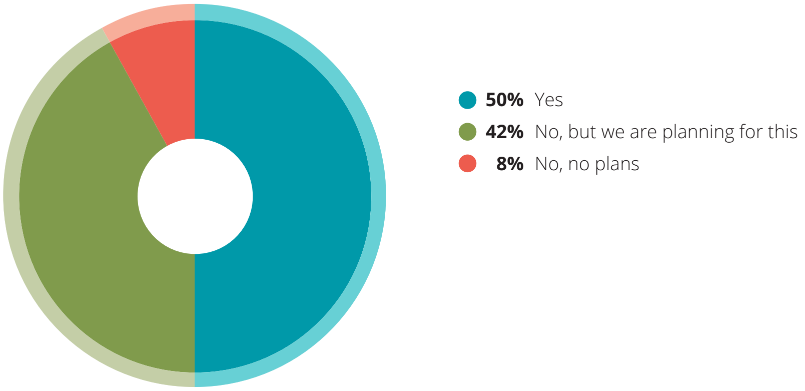


Figure 112 *Source: Arbor Networks, Inc.*

More than 60 percent of respondents indicate they have a solution that provides them with IPv6 traffic visibility, a slight increase from last year. However, only 30 percent report that their network equipment fully supports IPv6 flow telemetry. This is similar to last year, but still much lower than seen within service providers.

Regarding security concerns around IPv6 (Figure 113), the top three concerns are:

- DDoS attacks (58 percent)
- Misconfiguration (55 percent)
- Host scanning (52 percent)

Last year, the top concern was IPv4/IPv6 feature parity, at 68 percent. This year that concern has fallen to fourth place, with only half of respondents worried about this issue. This could be an indication that equipment vendors have further improved their IPv6 feature support.

IPv6 Security Concerns

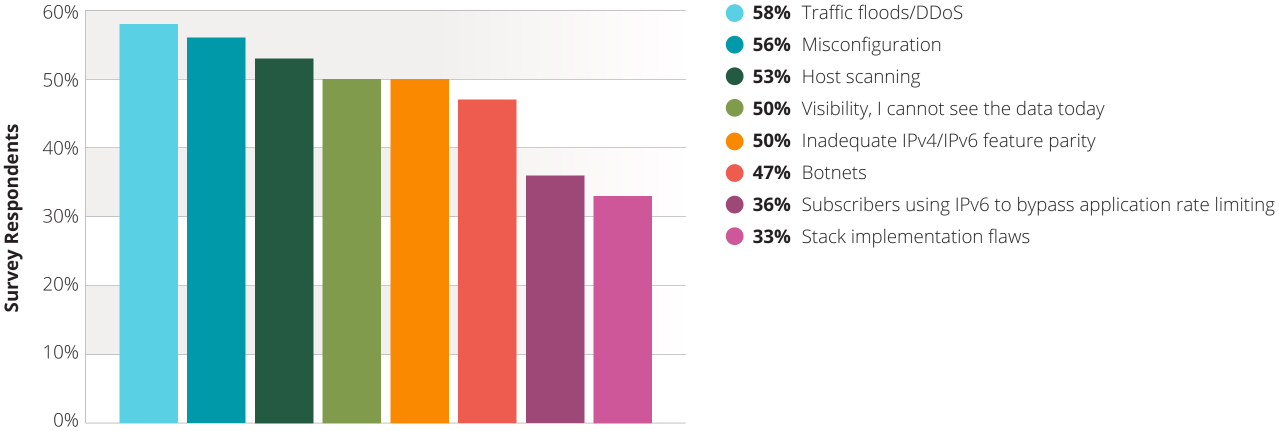


Figure 113 *Source: Arbor Networks, Inc.*

DNS OPERATORS

The overall proportion of respondents who have NO security group responsible for their DNS infrastructure has dropped to 22 percent, from one-third last year. However, 26 percent of EGE respondents are still in this situation, as opposed to only 17 percent of service providers. Just under one-third of overall respondents saw DDoS attacks against their DNS infrastructure that resulted in a customer-visible outage. However, this percentage rises to just over one-half if we look purely at service provider respondents. The security mechanisms used to defend DNS infrastructure from DDoS attack are similar to last year, with firewalls, ACLs and IPS/IDS being the three most common technologies deployed within respondents' networks. Only 19 percent of EGE respondents utilize IDMS to protect DNS infrastructure, compared to just over half of service providers.

In this year's survey, the DNS section was open to both enterprise and service provider respondents. Overall, 70 percent of respondents operate DNS servers in their networks. Looking at enterprise and service provider data separately, 65 percent of enterprises and 76 percent of service providers operate their own DNS infrastructure — high proportions in both cases.

In previous iterations of the survey we highlighted a growing proportion of respondents with NO security group responsible for their DNS infrastructure. Over the past three years, that proportion has grown from 19 percent to 33 percent. This year, however, there has been a very positive shift in the right direction, with only 22 percent of respondents indicating that there is no group responsible for the security of their DNS infrastructure (Figure 114).

DNS Security Responsibility

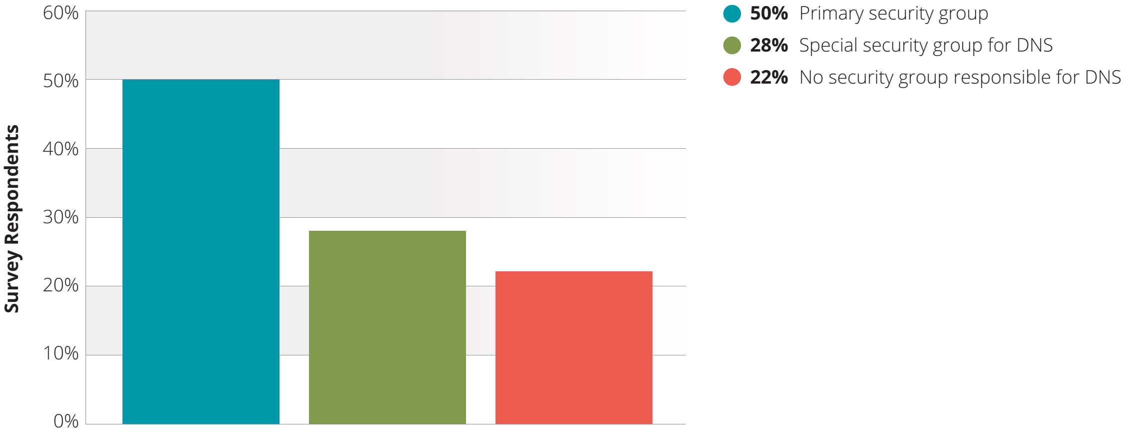


Figure 114 *Source: Arbor Networks, Inc.*

If we break out this data for EGE and service provider respondents, there is a marked difference: 17 percent of service providers have no security group responsible for DNS, as opposed to 26 percent of EGE respondents. Given the importance of DNS for all Internet-connected organizations, and its use as both a weapon and a target by attackers, it is imperative that ALL organizations put relevant security in place for their DNS infrastructure.

DNS infrastructure can be used to launch reflection amplification DDoS attacks, and organizations should restrict recursive look-ups to prevent their infrastructure from being abused. This year, we have seen a small increase in the proportion of respondents implementing this best current practice, up to 82 percent from around 80 percent in previous years.

In terms of visibility into DNS traffic, there has been an improvement in the proportion of respondents with visibility at Layers 3 and 4, up to 63 percent from 56 percent last year (Figure 115). This is still not as high as the 67 percent seen in 2013, which may be due to increased EGE participation in the survey skewing some results. If we filter this year's data to include only service provider respondents to this question, we see that 67 percent have Layer 3/4 visibility into DNS.

Visibility at Layer 7 continues to improve, up to 43 percent this year from 41 percent last year and 27 percent in 2013. Visibility at Layer 7 is important for DNS traffic because understanding and mitigating attacks, either targeting or utilizing DNS infrastructure, often require application-layer visibility.

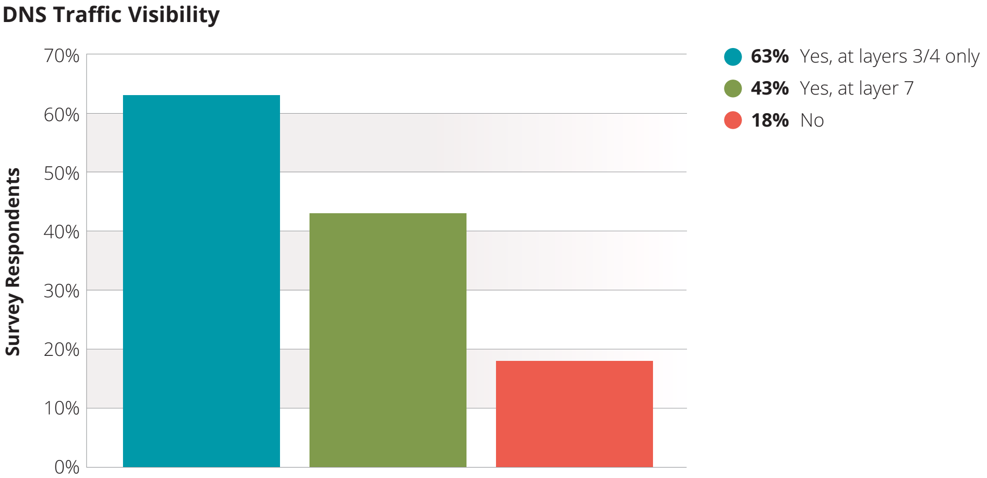


Figure 115 *Source: Arbor Networks, Inc.*

This year, we see a significant increase in the proportion of respondents experiencing DDoS attacks against their DNS infrastructure that resulted in a customer-visible outage. This proportion rose from 17 percent last year to 30 percent this year (Figure 116) — a return to a level last seen in 2013. Interestingly, if we narrow our view to look at EGE respondents and service providers independently, we see that only 11 percent of EGE witnessed an attack that led to a customer-visible outage, compared to 51 percent of service providers. Attackers are targeting DNS infrastructure as a means of impacting well-protected end-customer services. For service providers, this can lead to collateral damage if the appropriate protections aren't in place.

DNS Infrastructure DDoS Attack

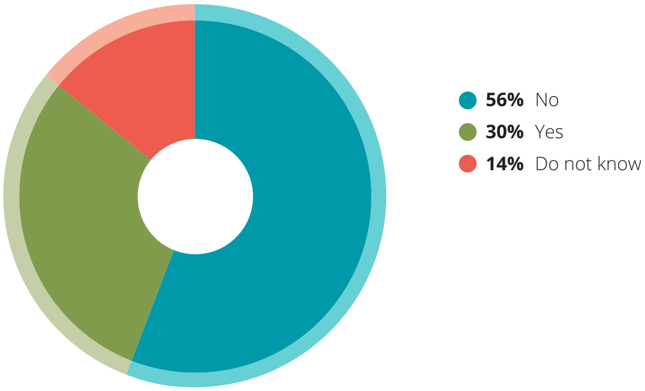


Figure 116 *Source: Arbor Networks, Inc.*

Given the increase cited above, it is no surprise that the proportions of respondents seeing attacks targeting recursive and authoritative DNS servers have increased. Last year, only 16 percent saw attacks targeting recursive DNS servers, and 21 percent saw attacks targeting authoritative DNS servers. This year, these proportions have increased to 29 percent and 34 percent respectively.

The security mechanisms used to defend DNS infrastructure from DDoS attack are similar to last year, with firewalls, ACLs and IPS/IDS being the three most common deployed technologies (Figure 117). However, there are some significant differences in the defensive mechanisms used by EGE and service providers.

A higher proportion of EGE organizations utilize firewalls to protect their DNS infrastructure — 80 percent versus 62 percent of service providers. A much higher proportion of service providers utilize ACLs for protection — 70 percent versus 50 percent of EGE. The big difference, though, is in the use of IDMS to protect DNS infrastructure. Only 19 percent of EGE respondents utilize IDMS, compared to 54 percent of service providers. IDMS provides the functionality needed to deal with DDoS attacks that either leverage or target DNS infrastructure. Given the ever-increasing business reliance on Internet services, the protection of DNS infrastructure is critical.

DNS DDoS Security Measures

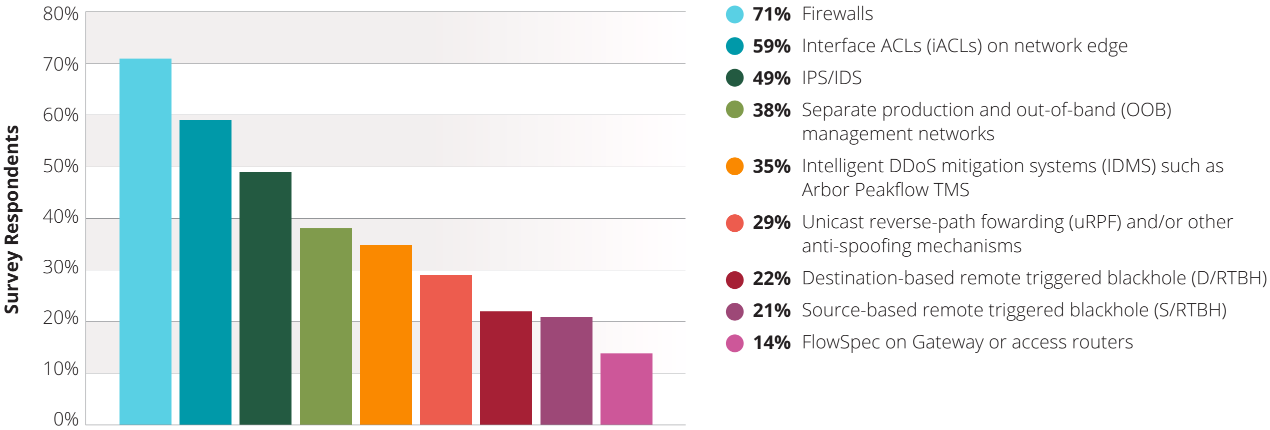


Figure 117 *Source: Arbor Networks, Inc.*

closi

SECTION 4

4

CLOSING REMARKS

CONCLUSION

In 1965, Gordon Moore, co-founder of Intel, famously predicted that the number of transistors in microchips would continue to double year over year for the next decade. After 10 years, he further predicted that the transistors in microchips would continue to double every two years for the next decade. His bold predictions have proven true over multiple decades, and have led to the accelerating level of both innovation and miniaturization of technology. This has made previously impossible things possible — smartphones, "big data" computing, complex medical procedures, intelligent appliances and much more. Technology has enabled just about every electronic device we own to become "smart" — connected to the Internet and able to interact with other devices. This, in turn, has led to the new phenomenon known as the Internet of Things (IoT). The IoT is already leading to exponential growth in the number of connected devices we use, and this is fueling reliance on the Internet among consumers and businesses alike. The challenges involved in securing our networks are getting that much bigger and more complex. Miscreants, criminals and even government intelligence groups are taking advantage of this environment to achieve their goals.

In this year's survey, enterprises, governments and education institutions report a rise in DDoS, malicious insiders and advanced threats, so they are feeling the brunt of these threats. They also have accelerated their use of IPv6, creating a more volatile network environment with a wider attack surface. Over one-third of these respondents experienced DDoS attacks over the past 12 months. Criminal extortion in DDoS has risen sharply thanks to DD4BC and the Armada Initiative. Fortunately, organizations are making a strong investment in protection to offset these challenges. Nearly half of respondents have now deployed intelligent DDoS mitigation systems (IDMS), and there is a significant rise in the deployment of always-on DDoS mitigation to ensure service availability. Organizations are also giving more attention to their incident response planning than ever before, and are investing more in forensic tools to investigate breaches.

Within service providers, mobile providers and data center operators, DDoS continues to be the biggest security threat. Almost every respondent saw application-layer attacks, and volumetric attack sizes in the hundreds of Gbps are now common. Similar to the enterprise, government and education segment, the top DDoS motivation reported among service providers is criminal extortion. This overtook vandalism/nihilism and ideological hacktivism, which have been the top motivations for the last few years. There is also a great deal of innovation in the service provider space; SDN/NFV deployments are growing quickly as providers are looking for ways to launch new cloud-based services. IPv6 has now become almost pervasive as most networks now support dual IPv4/IPv6 services. Both of these changes provide new target areas for attackers. The good news is that there seems to be an equal amount of focus put on defense in this segment. General network visibility, use of IDMS, participation in OPSEC communities, use of anti-spoofing, route hijack monitoring and DDoS simulation practice are all on the rise. And, more service providers are now offering DDoS protection services to their customers, where there is continued increasing interest in these services. These are all positive trends.

Arbor Networks is proud to release the 11th annual *Worldwide Infrastructure Security Report.* This report is designed to help network operators understand the breadth of the threats that they face, gain insight into what their peers are doing to address these threats, and comprehend both new and continuing trends. This year's report features responses from 354 respondents, the most ever by a significant margin, with over half of respondents representing enterprise, government or education. A good global distribution of respondents rounds out what has been our broadest representation of the Internet community ever. We hope that you find the information useful in preparing your defenses. Thank you for reading.

The Arbor Team

ABOUT THE AUTHORS

Darren Anstee

Chief Security Technologist, Arbor Networks

danstee@arbor.net

Darren Anstee has 20 years of experience in pre-sales, consultancy and support for telecom and security solutions. As Chief Security Technologist at Arbor Networks, Darren works across the research, strategy and pre-sales aspects of Arbor's traffic monitoring, threat detection and mitigation solutions for service providers and enterprises around the world. Prior to joining Arbor, he spent over eight years working in both pre- and post-sales for core routing and switching product vendors.

Paul Bowen

Principal Security Technologist, Arbor Networks

pbowen@arbor.net

Paul Bowen, Principal Security Technologist for Arbor Networks, brings 21+ years of experience to his role at the company where his primary focus is on advanced threats. Previously he was an Architect for advanced threat solutions at Fortinet. He also was The Architect for Mandiant Cloud based SIEM, called TAP. Spent 2 years as a security and compliance conference speaker for HP as a member of Office for advanced solutions, spent 7 years as a principal Engineer for Arcsight, and 10 years as a manager of global security for Estee Lauder.

C.F. Chui

Principal Security Technologist, Arbor Networks

cfchui@arbor.net

With more than 20 years of experience in the networking industry, C.F. Chui is a veteran in designing, implementing and supporting highly available network systems and solutions. In his current role with Arbor Networks, C.F. works closely with customers in the Asia Pacific region to develop and optimize approaches for their network security solutions to ensure the most effective deployment and highest customer satisfaction. He is also actively involved in Arbor's global research projects.

Before joining Arbor, C.F. held different regional positions in pre- and post-sales for various large core routing and switching vendors. His expertise lies mainly in the areas of Internet routing technology, network threat detection and network visibility solutions.

Gary Sockrider

Principal Security Technologist, Arbor Networks

gsockrider@arbor.net

Gary is an industry veteran bringing over 25 years of broad technology experience ranging from network security to routing and switching, data center, mobility and collaboration. His previous roles include security SME, consultancy, customer support, IT and product management. He seeks to understand and convey the constantly evolving threat landscape, as well as the techniques and solutions that address the challenges they present. Prior to joining Arbor in 2012, he spent 12 years at Cisco Systems and held previous positions with Avaya and Cable & Wireless.

GLOSSARY

A

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

B

BCP	Best Current Practice
BYOD	Bring Your Own Device

C

CDN	Content Delivery Network
C&C	Command-and-Control

D

DCN	Data Communication Network
DNS	Domain Name System
DDoS	Distributed Denial of Service
D-RTBH	Destination-based Remotely Triggered Blackholing
S-RTBH	Source-based Remotely Triggered Blackholing

E

EGE	Enterprise, Government, Education

G

Gbps	Gigabits-per-second
Gi	Global Internet
GTP-C	General Packet Radio Service (GPRS) tunneling protocol (GTP)
GTP-U	GPRS Tunnelling Protocol User Plane
GTSM	Generalized TTL Security Mechanism

H

HTTP	Hypertext Transfer Protocol
HTTP/S	HTTP Secure
iACL	Infrastructure ACL

I

ICMP	Internet Control Message Protocol
IDMS	Intelligent DDoS Mitigation System
IDS	Intrusion Detection System
IGP	Interior Gateway Protocol
IoT	Internet of Things
IPS	Intrusion Prevention System
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IR	Incident Response
IRC	Internet Relay Chat
ISP	Internet Service Provider

K

KPI	Key Performance Indicator

L

LTE	Long Term Evolution

M

Mbps	Megabits-per-second
MDM	Mobile Device Management
MITM	Man in the Middle
MNO	Mobile Network Operator
MPC	Mobile Packet Core
MSSP	Managed Security Service Provider

N

NAT	Network Address Translation
NFV	Network Functions Virtualization
NGFW	Next Generation Firewall
NMS	Network Management System
NTP	Network Time Protocol

O

OOB	Out of band
OPSEC	Operational Security
OTT	Over the Top

P

PAT	Port Address Translation
PCAP	Packet Capture

Q

QoE	Quality of Experience

R

RAN	Radio Access Network

S

SDN	Software-defined networking
SEG	Security Gateways
SIEM	Security Information Event Management
SIP	Session Initiation Protocol
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SOC	Security Operations Center
S/RTBH	Source-based Remotely Triggered Blackholing
SSDP	Simple Service Discovery Protocol
SSL	Secure Socket Layer
SYN	Synchronize

T

TLD	Top Level Domain
TLS	Transport Layer Security
Tbps	Terabits per second

U

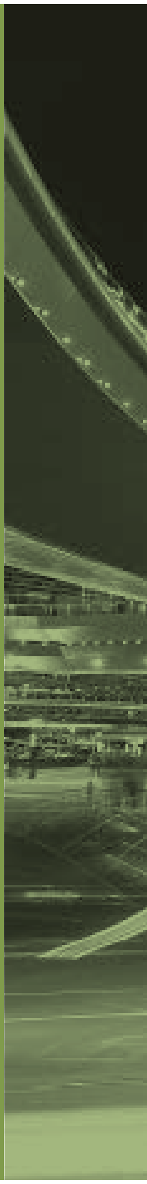
UDP	User Datagram Protocol
uRPF	Unicast Reverse Path Forwarding
UTM	Unified Threat Management

V

VoIP	Voice over Internet Protocol

W

WAF	Web Application Firewall
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

The Security Division of NETSCOUT

SR/WISR2015/EN/0116-LETTER