Ponemon INSTITUTE

The State of DDoS Attacks against Communication Service Providers

Sponsored by A10 Networks

Independently conducted by Ponemon Institute LLC

Publication Date: April 2019

The State of DDoS Attacks against Communication Service Providers

Ponemon Institute, April 2019

Part 1. Executive Summary

The State of DDoS Attacks against Communication Service Providers, sponsored by A10 Networks, specifically studies the threats to Internet Services Providers (ISPs) Mobile and/or Cloud Services Providers (CSPs). Ponemon Institute surveyed 325 IT and IT security practitioners in the United States who work in communication service provider companies and are familiar with their defenses against DDoS.

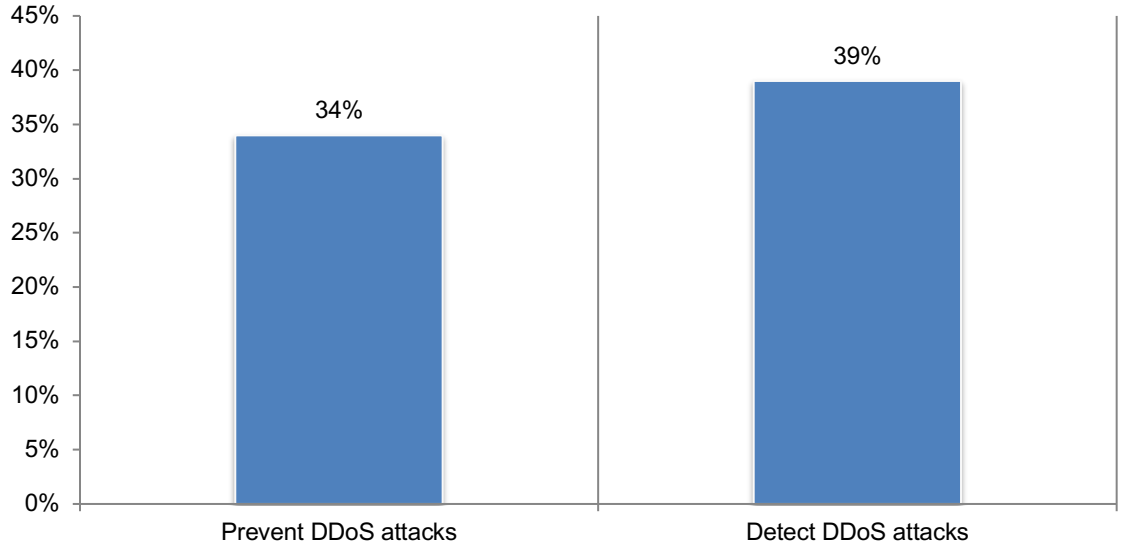
According to the research, communication service providers (CSPs) are increasingly vulnerable to DDoS attacks. In fact, 85 percent of respondents say DDoS attacks against their organizations are either increasing or continuing at the same relentless pace and 71 percent of respondents say they are not or only somewhat capable of launching measures to moderate the impact of DDoS attacks. The increase in IoT devices due to the advent of 5G will also increase the risk to CSPs.

Based on the findings, the most common DDoS attacks target the network protocol, flood the network with traffic to starve out the legitimate requests and render the service unavailable. As a result, these companies will face such serious consequences as diminished end user and IT staff productivity, revenue losses and customer turnover.

The most serious barriers to mitigating DDoS attacks are the lack of actionable threat intelligence, the lack of in-house expertise and technologies. As a result of these challenges, confidence in the ability to detect and prevent DDoS attacks is low. As shown in Figure 1, only 34 percent of respondents say their organizations are very effective or effective in preventing the impact of the attack and only 39 percent of respondents say they are effective in detecting these attacks.

Figure 1. How effective is your organization in detecting and preventing the impact of DDoS attacks?

Very effective and Effective responses combined



Following are the most salient findings from the research.

The most dangerous DDoS attackers are motivated by money. The DDoS attacker who uses extortion for financial gain represents the greatest cybersecurity risk to companies, according to 48 percent of respondents. These criminals make money offering their services to attack designated targets or to demand ransomware for not launching DDoS attacks. Forty percent of respondents fear the attacker who executes a DDoS attack to distract the company from another attack. Only 25 percent of respondents say a thrill seeker and 21 percent of respondents say an angry attacker pose the greatest cybersecurity risk.

Attacks targeting the network layer or volumetric floods are the most common attacks experienced. The most common types of DDoS attacks are network protocol level attacks (60 percent of respondents) and volumetric floods (56 percent of respondents). In a volumetric flood, the attacker can simply flood the network with traffic to starve out the legitimate requests to the DNS or web server.

DDoS attacks pose the greatest threat at the network layer. Respondents were asked to allocate a total of 100 points to seven layers in the IT security stack. The layer most at risk for a DDoS attack is the network layer followed by the application layer. The findings suggest how organizations should allocate resources to prevent and detect DDoS attacks.

DDoS attacks can have severe financial consequences because they cause a loss of productivity, customer turnover and damage to property, plant and equipment. DDoS attacks affect the bottom line. Respondents consider the most severe consequences are diminished productivity for both end users and IT staff.

Threat intelligence currently used to mitigate the threat of a DDoS attack is stale, inaccurate, incomplete and does not integrate well with various security measures. Seventy percent of respondents believe their DDoS-related threat intelligence is often too stale to be actionable and 62 percent of respondents say it is often inaccurate and/or incomplete. Other issues include the difficulty in integrating DDoS threat intelligence with various security measures and the high false positive rate, say 60 percent and 58 percent of respondents respectively.

To improve prevention and detection of DDoS attacks, organizations need actionable threat intelligence. Sixty-three percent of respondents say the biggest barrier to a stronger cybersecurity posture with respect to DDoS attacks are a lack of actionable intelligence. To address this problem, 68 percent of respondents say the most effective technology in mitigating DDoS threats is one that provides intelligence about networks and traffic.

Scalability, integration and reduction of false positives are the most important features to prevent DDoS attacks. As part of their strategy to address DDoS security risks, companies want the ability to scale during times of peak demand, integrate DDoS protection with cyber intelligence solutions, integrate analytics and automation to achieve greater visibility and precision in the intelligence gathering process and reduce the number of false positives in the generation of alerts.

Most organizations plan to offer DDoS scrubbing services. Sixty-six percent of respondents either have a DDoS scrubbing service (41 percent) or plan to in the future (25 percent). Benefits to offering these services are revenue opportunities, enhanced customer loyalty and lower support tickets with subscribers.

Best practices of communication service providers effective in moderating the impact of DDoS attacks

As part of this study, we conducted a special analysis of those organizations that are most capable of launching measures that moderate the impact of DDoS attacks. Twenty-nine percent of the total sample of respondents self-reported that their organizations have a high level of ability to accomplish this in order to reduce the impact and consequences of a DDoS attack. We refer to this sample as high performers and in this section, we compare the findings from this group to the overall sample.

Communication service providers that are most effective in dealing with DDoS attacks have the following four characteristics:

1. High performing companies are very effective in their ability to launch measures that moderate the impact of DDoS attack.

2. High performing companies are more positive about the use of threat intelligence in their organizations. Specifically, these respondents cite their companies' ability to manage the process, integrate threat intelligence with various security measures and reduce the high false positive rate.

3. High performing organizations are more likely to have advanced features in their threat intelligence operations that provide actionable information about DDoS for hire botnets or the reflected amplification of DDoS weapons locations.

4. High performing companies are more likely to offer DDoS scrubbing services to subscribers.

Part 2. Key findings

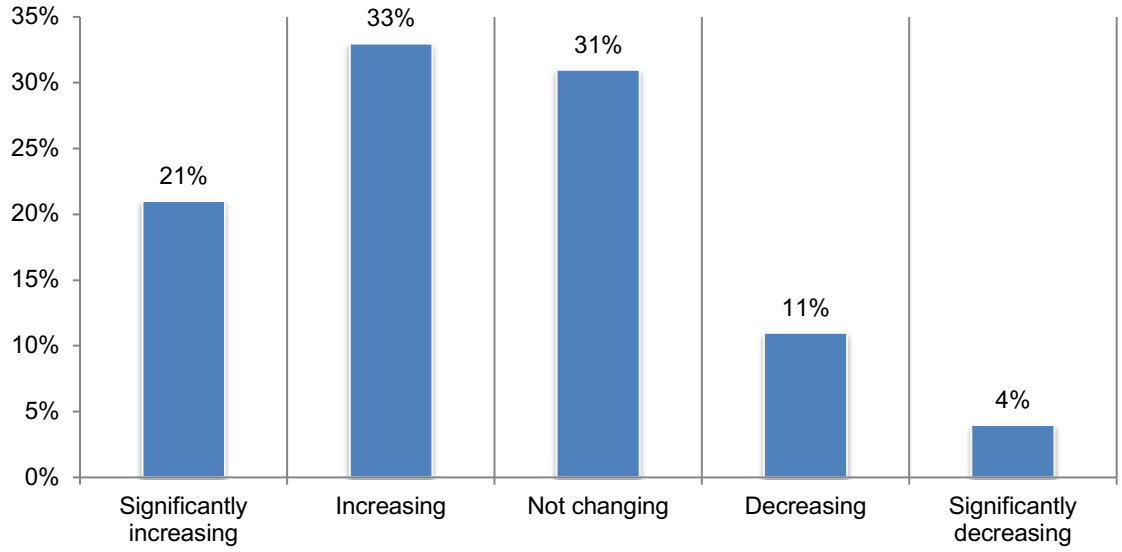
In this section, we provide a deeper analysis of the research findings. The complete audited findings are presented in the Appendix of this report. We have organized the report according to the following themes.

- DDoS attacks continue to be intense and pervasive
- The value of scalability, automation, integration and precision in DDoS solutions
- The importance of the Cyber Kill Chain in shaping DDoS threat mitigation tactics
- Best practices of organizations effective in moderating the impact of DDoS attacks

DDoS attacks continue to be intense and pervasive

Organizations are not optimistic DDoS attacks will decrease. According to Figure 2, 85 percent of respondents say DDoS attacks will either increase or stay the same. Because these attacks are not going away, organizations need to enhance their security defenses to fight these intense and pervasive threats.

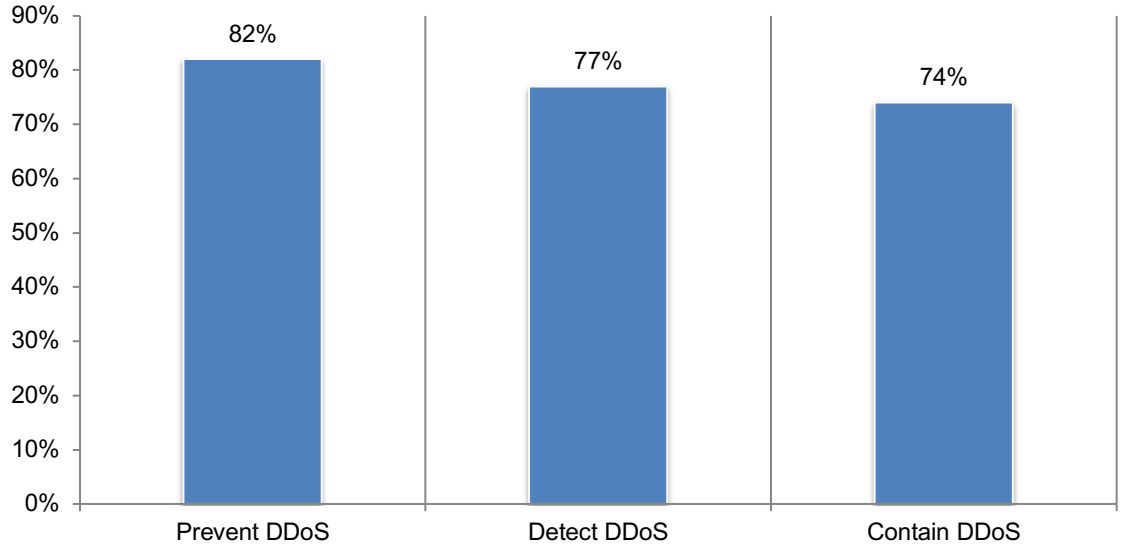
Figure 2. Wil DDoS attacks increase, decrease or stay the same in the next 12 to 24 months?



DDoS attacks are more difficult to prevent the impact, detect and contain than other cyberattacks. As shown in Figure 3, not only are DDoS attacks relentless, they are among the most difficult to prevent (82 percent of respondents), detect (77 percent of respondents) and contain (74 percent of respondents).

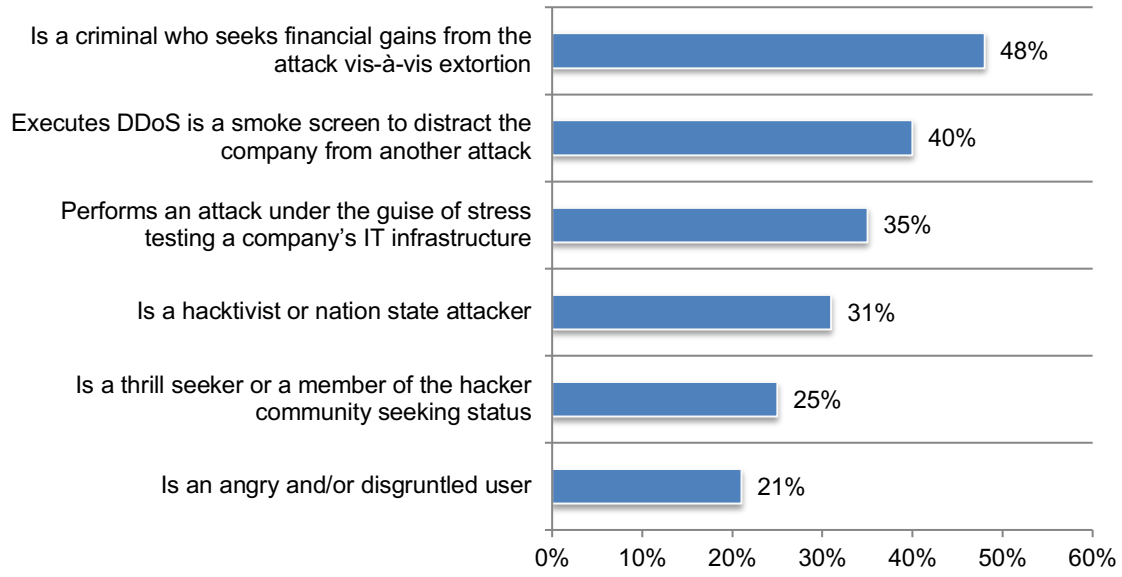
Figure 3. Relative to other cyberattacks, how difficult is DDoS to prevent the impact, detect and contain

Very difficult and Difficult responses combined



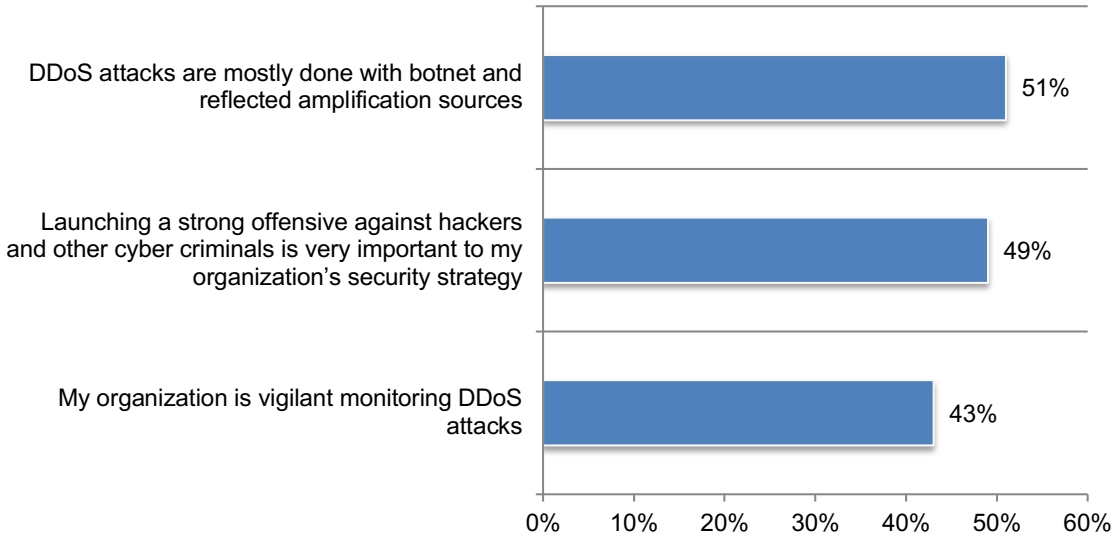
The most dangerous DDoS attackers are motivated by money. As shown in Figure 4, the DDoS attacker who uses extortion for financial gain represents the greatest cybersecurity risk to companies, according to 48 percent of respondents. These criminals make money offering their services to attack designated targets or to demand ransomware for not launching DDoS attacks. Forty percent of respondents fear the attacker who executes a DDoS attack to distract the company from another attack. Only 25 percent of respondents say a thrill seeker and 21 percent of respondents say an angry attacker pose the greatest cybersecurity risk.

Figure 4. DDoS attackers who present the greatest cybersecurity risk
Two responses permitted



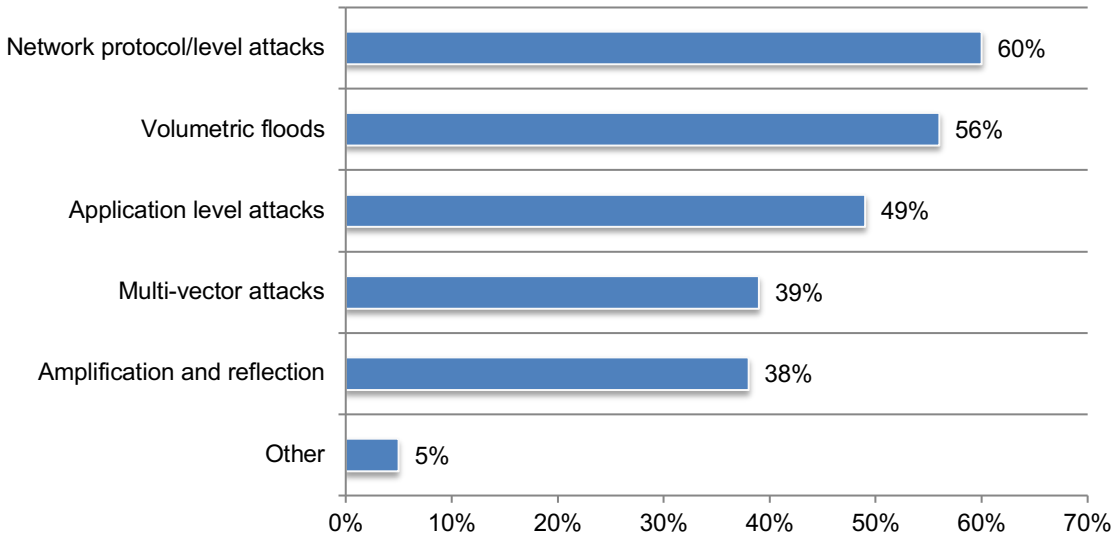
The majority of companies (51 percent of respondents) represented in this research say DDoS attacks are mostly done with botnet and reflected amplification sources, as shown in Figure 5. However, less than half of respondents (49 percent) say launching a strong offensive against hackers and other cyber criminals is very important to their organizations' security strategy.

Figure 5. Perceptions about DDoS attacks
Strongly agree and Agree responses combined



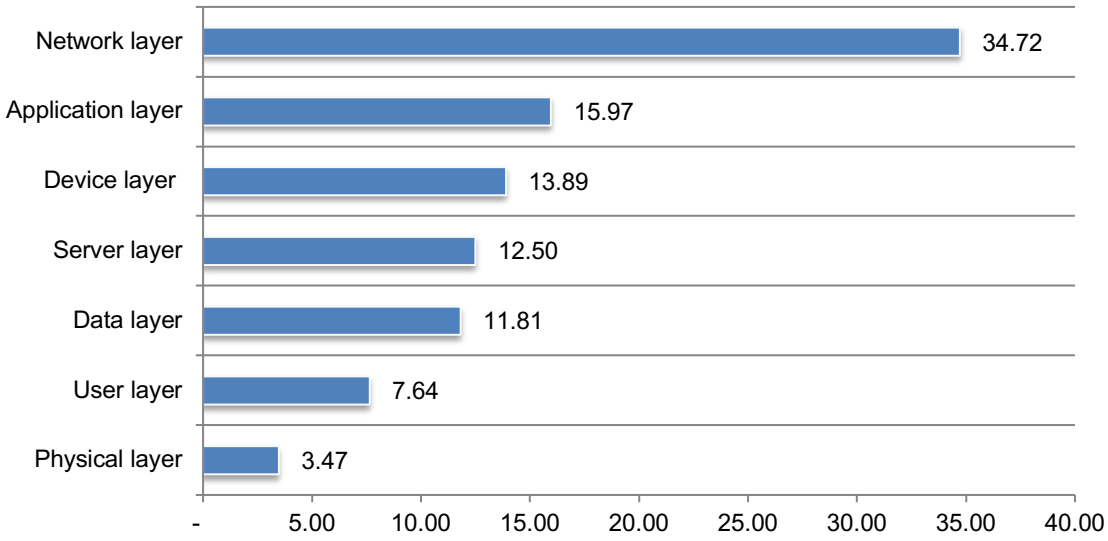
Attacks targeting the network protocol or volumetric floods are the most common attacks experienced. According to Figure 6, the most common types of DDoS attacks are network protocol/level attacks (60 percent of respondents) and volumetric floods (56 percent of respondents). In a volumetric flood, the attacker can simply flood the network with traffic to starve out the legitimate requests to the DNS or web server.

Figure 6. What types of DDoS attacks did your organization experience?
More than one response permitted



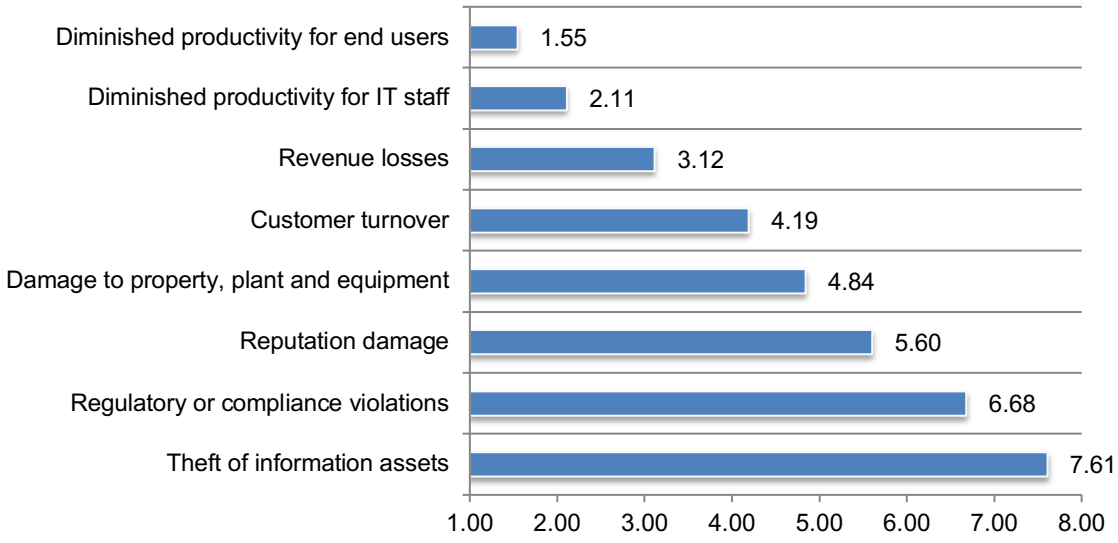
DDoS attacks pose the greatest threat at the network layer. Respondents were asked to allocate a total of 100 points to seven layers in the IT security stack. As shown in Figure 7, the layer most at risk for a DDoS attack is the network layer followed by the application layer. The findings suggest how organizations should allocate resources to prevent and detect DDoS attacks.

Figure 7. DDoS security risks in the IT security stack
Allocation of 100 points based on risk



DDoS attacks can have severe financial consequences because they cause a loss of productivity, customer turnover and damage to property, plant and equipment. Respondents were asked to rate 8 possible negative consequences of a DDoS attack from 1 = most severe consequence to 8 = least severe. All of these consequences affect the bottom line. However, as shown in Figure 8, the most severe consequences are diminished productivity for both end users and IT staff.

Figure 8. What were the consequences of the DDoS attacks?
From 1 = Most severe consequence to 8 = Least severe consequence

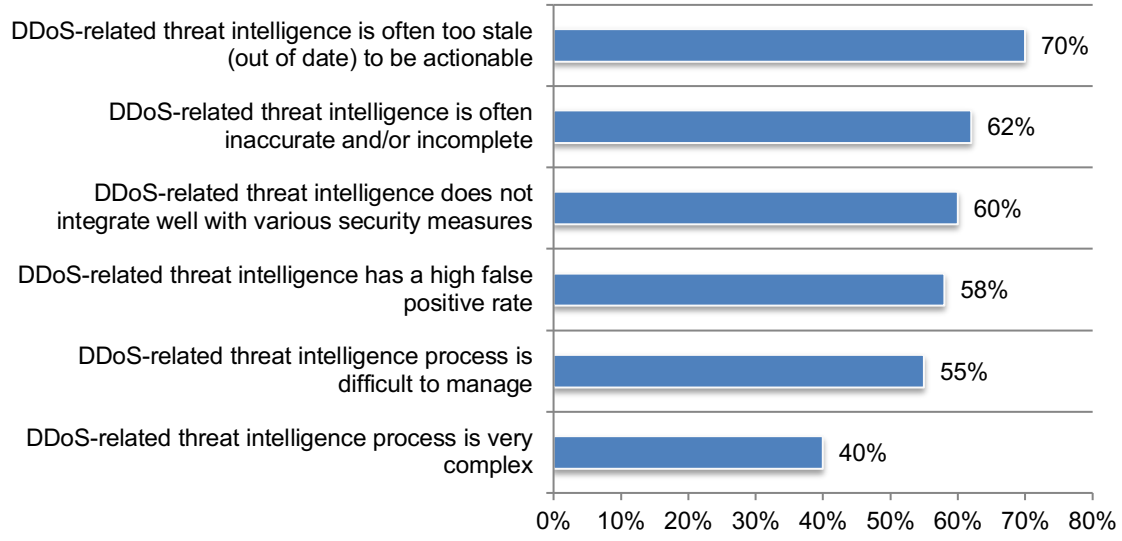


The value of scalability, automation, integration and precision in DDoS solutions

Threat intelligence currently used about DDoS attacks is stale, inaccurate, incomplete and does not integrate well with various security measures. According to Figure 9, most respondents in this study do not find their current DDoS-related threat intelligence helpful in protecting their organizations.

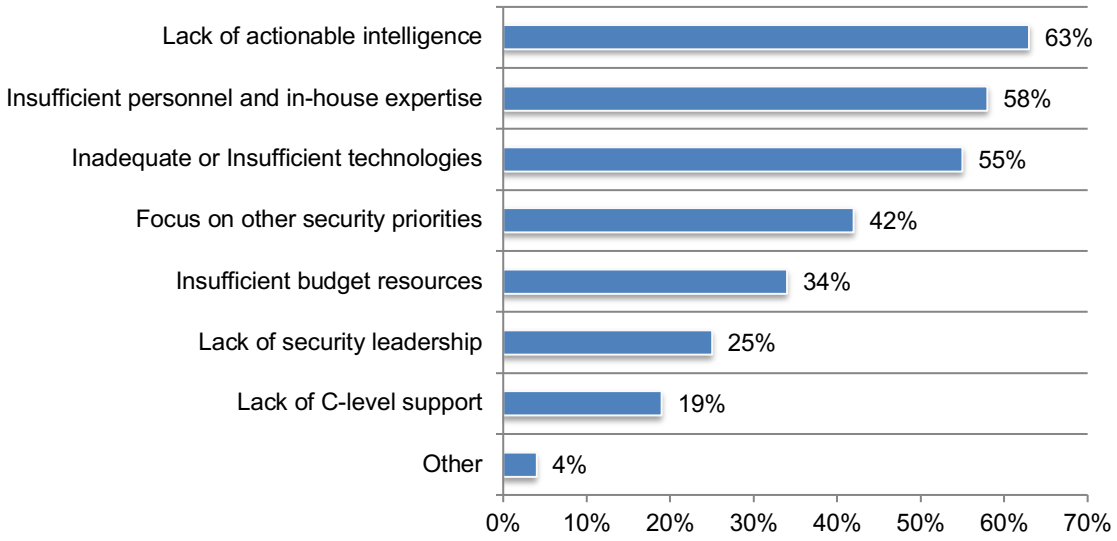
Seventy percent of respondents believe the threat intelligence is often too stale to be effective and 62 percent of respondents say it is often inaccurate and/or incomplete. Other issues include the difficulty in integrating DDoS threat intelligence with various security measures and the high false positive rate, 60 percent and 58 percent of respondents respectively.

Figure 9. The problems with threat intelligence currently used
Strongly agree and Agree responses combined



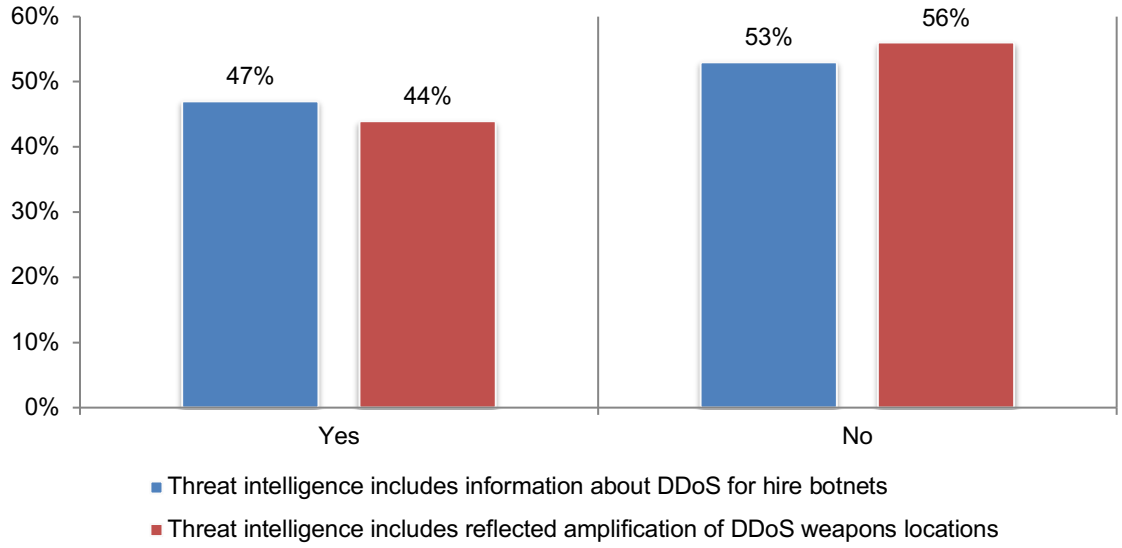
To improve prevention and detection of DDoS attacks, organizations need actionable threat intelligence, in-house expertise and sufficient technologies. As shown in Figure 10, the barriers to a stronger cybersecurity posture with respect to DDoS attacks are a lack of actionable intelligence, insufficient personnel and in-house expertise and inadequate technologies (63 percent, 58 percent and 55 percent of respondents respectively).

Figure 10. What are the most critical barriers to preventing DDoS attacks?
Three responses permitted



Reflected amplification attacks and attacks involving botnets are common. Despite the frequency of these types of attacks, most organizations' threat intelligence does not provide actionable information about DDoS for hire botnets (53 percent of respondents) or the reflected amplification of DDoS weapons locations (56 percent of respondents), as shown in Figure 11.

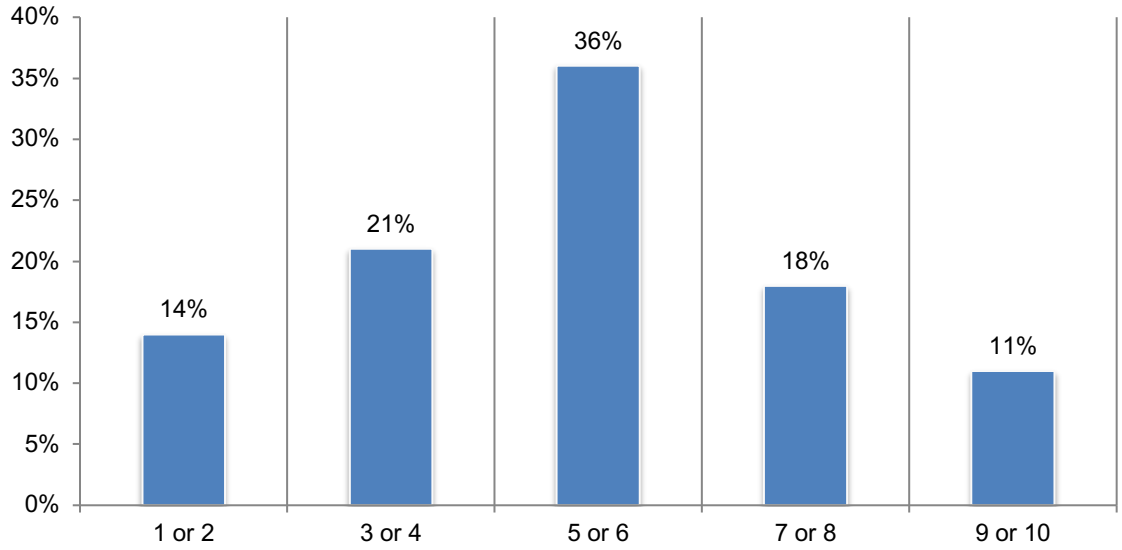
Figure 11. Features of organizations' threat intelligence operations



Most organizations are not capable of launching measures to moderate the impact of DDoS attacks. When asked to rate their organizations' capability in launching measures to reduce the impact of a DDoS attack on a scale of 1 = low capability to 10 = high capability, 71 percent of respondents rate their capability as low or moderate (1 to 6 responses on the 10-point scale), as shown in Figure 12.

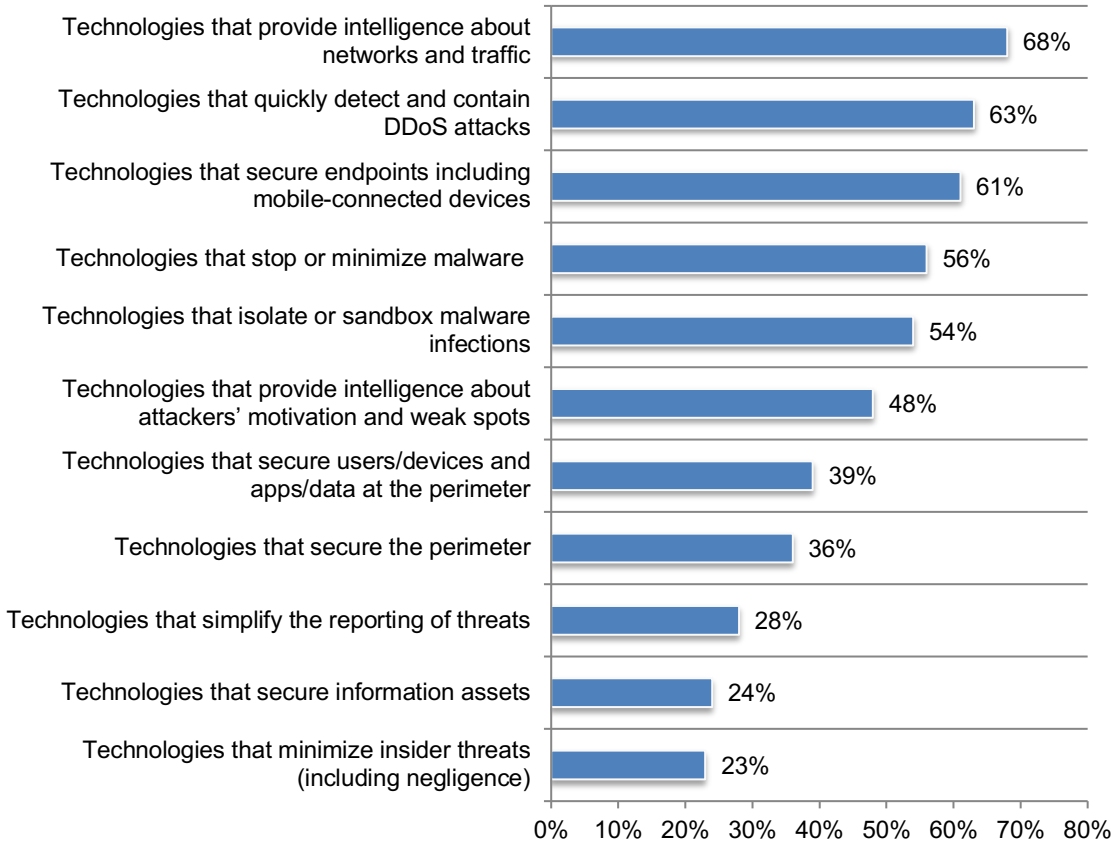
Figure 12. How capable is your organization in launching measures to moderate the impact of DDoS attacks?

Respondents rated their capability from 1 = low capability to 10 = high capability



Technologies that improve threat intelligence are considered the most effective. Respondents were asked to select the technologies that are most effective in improving the ability to moderate the impact of DDoS-related security risks. Because respondents believe their current threat intelligence technologies are failing to mitigate DDoS threats the most effective technology is one that provides intelligence about networks and traffic, as shown in Figure 13. Other technologies considered effective are ones that quickly detect and contain DDoS attacks and secure endpoints, including mobile-connected devices.

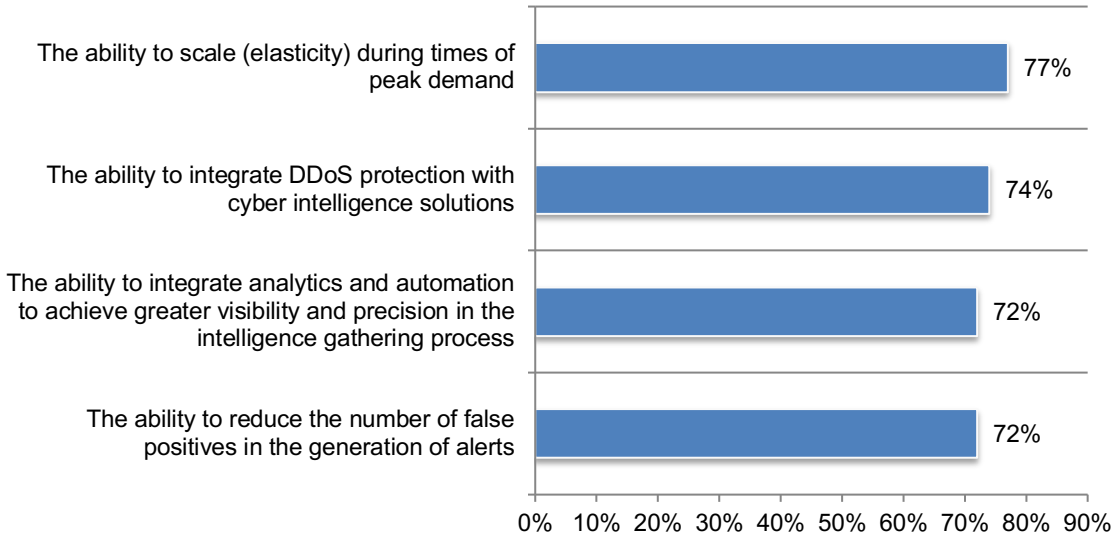
Figure 13. What are the most effective cybersecurity technologies for improving the ability to moderate the impact of DDoS-related security risks?
Five responses permitted



Scalability, integration and reduction of false positives are the most important features to defend against DDoS attacks. When asked to rate features that provide defensive capabilities on a scale of 1 = not important to 10 = very important, most respondents rate the features in Figure 14 as very important (7+ on the 10-point scale).

These include the ability to scale during times of peak demand, integrate DDoS protection with cyber intelligence solutions, integrate analytics and automation to achieve greater visibility and precision in the intelligence gathering process and reduce the number of false positives in the generation of alerts. Cyber intelligence solutions can include endpoint detection and response solutions (EDR), user and entity behavioral analysis, DevSecOps and automation and orchestration.

Figure 14. Importance of features that provide defensive capabilities against DDoS-based attacks
From 1 = not important to 10 = very important, 7+ responses presented

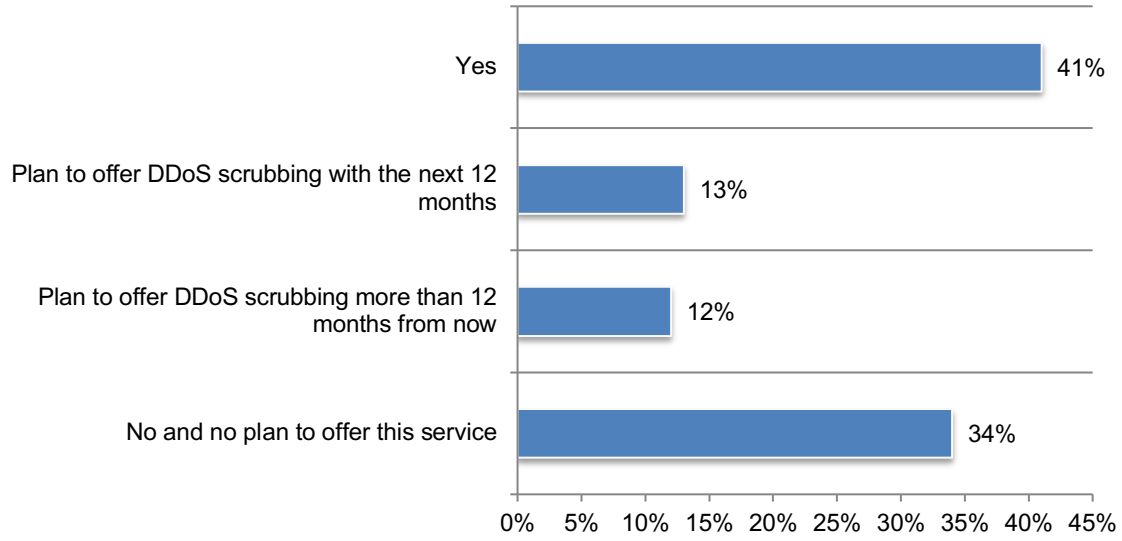


Scrubbing solutions are being offered to subscribers and address the threat of volumetric floods. In the context of this research, DDoS scrubbing solutions are used in large enterprises, ISPs and cloud providers, to off-ramp traffic to an out of path centralized data cleansing station.

When under a DDoS attack, traffic is redirected to the DDoS scrubbing center where anti-DDoS systems mitigate the DDoS attack traffic and passes clean traffic back to the network for delivery. The DDoS scrubbing center is equipped to sustain high volumetric floods at the network and application layers, low and slow DDoS attacks, RFC compliance checks, known vulnerabilities and zero day anomalies.

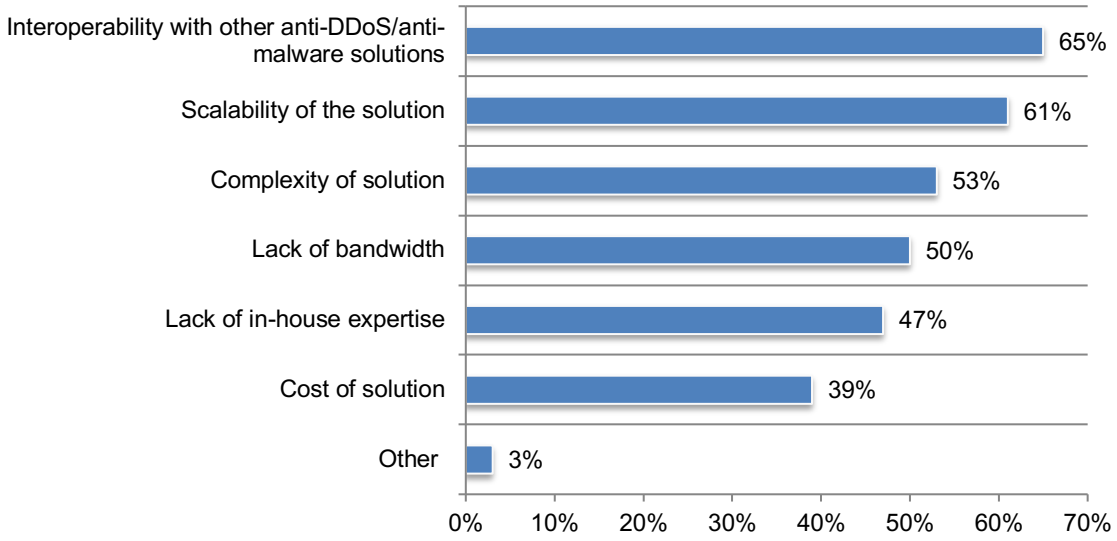
Most organizations plan to offer DDoS scrubbing services. According to Figure 15, 66 percent of respondents either have a DDoS scrubbing service (41 percent) or plan to in the future. Benefits to offering these services are revenue opportunities, enhanced customer loyalty and lower support tickets with subscribers.

Figure 15. Does your organization offer DDoS scrubbing services?



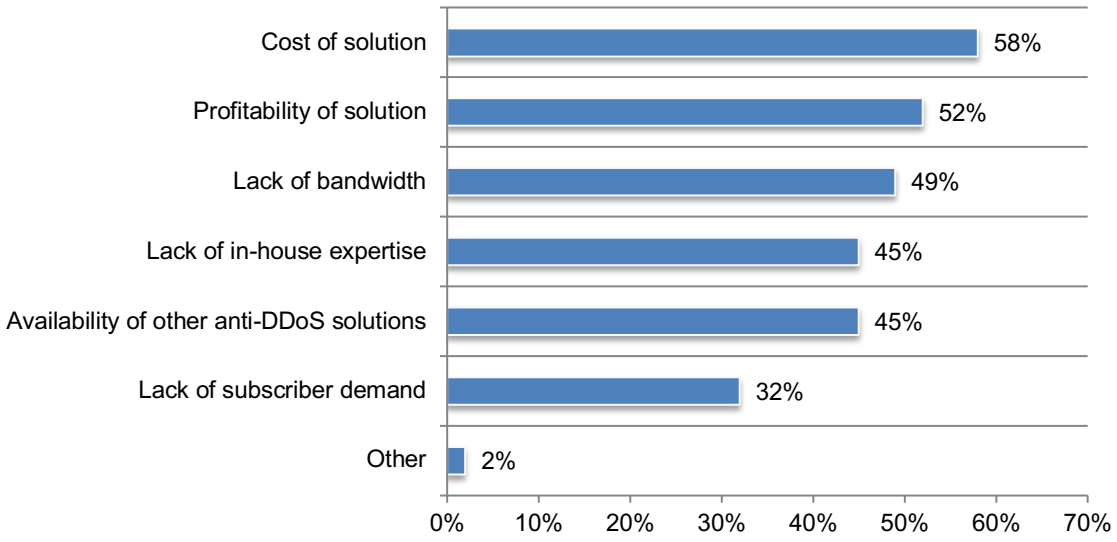
Despite the interest in DDoS scrubbing solutions, there are challenges to bringing it to market. As shown in Figure 16, 65 percent of respondents say interoperability with other anti-DDoS/anti-malware solutions is the main challenge followed by scalability of the solution (61 percent of respondents).

Figure 16. The main challenges for bringing a DDoS scrubbing solution to market
More than one response permitted



Cost and profitability are why 34 percent of respondents say they will not offer DDoS solutions. As shown in Figure 17, the decision not to use a DDoS solution is based on financial reasons. Fifty-eight percent of respondents say the solution costs too much and 52 percent of respondents say it is the lack of profitability. Only 32 percent of respondents say it is the lack of subscriber demand.

Figure 17. The main reasons for not offering DDoS scrubbing solutions
More than one response permitted



The importance of the Cyber Kill Chain in shaping DDoS threat mitigation tactics

The following describes the seven phases in the Cyber Kill Chain

Reconnaissance - Research, identification and selection of targets, often represented as crawling Internet websites such as conference proceedings and mailing lists for email addresses, social relationships or information on specific technologies.

Weaponization - Coupling a remote access Trojan with an exploit into a deliverable payload, typically by means of an automated tool (weaponizer). Increasingly, client application data files such as Adobe Portable Document Format (PDF) or Microsoft Office documents serve as the weaponized deliverables.

Delivery - Transmission of the weapon to the targeted environment. The three most prevalent delivery vectors for weaponized payloads by APT actors are email attachments, websites, and USB removable media.

Exploitation - After the weapon is delivered to the victim host, exploitation triggers intruders' code. Most often, exploitation targets an application or operating system vulnerability, but it could also more simply exploit the users themselves or leverage an operating system feature that auto-executes code.

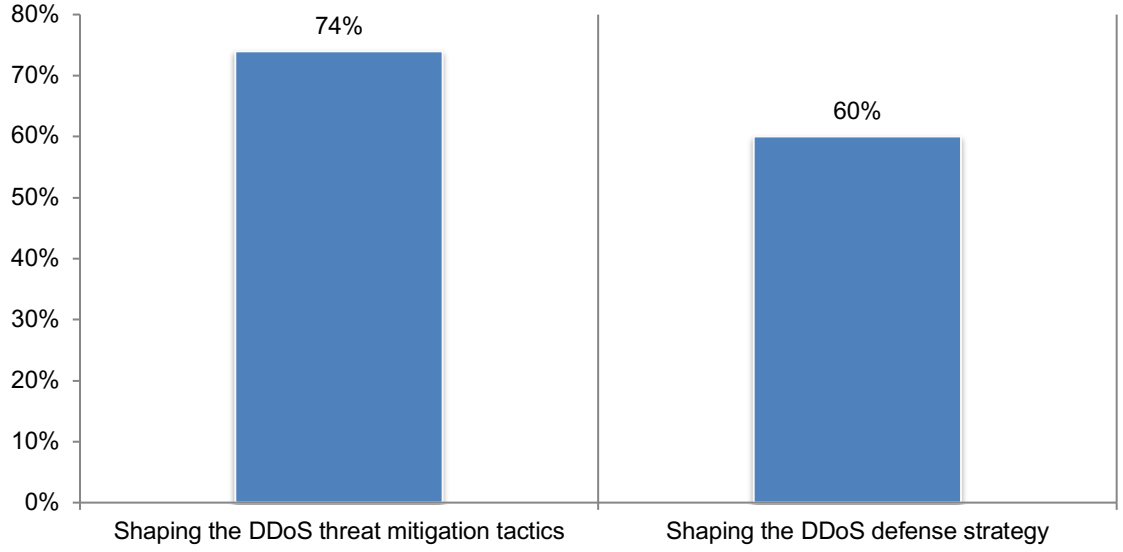
Installation - Installation of a remote access Trojan or backdoor on the victim system allows the adversary to maintain persistence inside the environment.

Command and Control (CnC) - Typically, compromised hosts must beacon outbound to an Internet controller server to establish a C2 channel. APT malware in particular requires manual interaction rather than conducting activity automatically. Once the C2 channel is established, intruders have "hands on the keyboard" access inside the target environment.

Actions on Objectives - Only now, after progressing through the first six phases, can intruders take actions to achieve their original objectives. Typically, this objective is data exfiltration, which involves collecting, encrypting and extracting information from the victim environment; violations of data integrity or availability are potential objectives as well. Alternatively, the intruders may only desire access to the initial victim box for use as a hop point to compromise additional systems and move laterally inside the network.

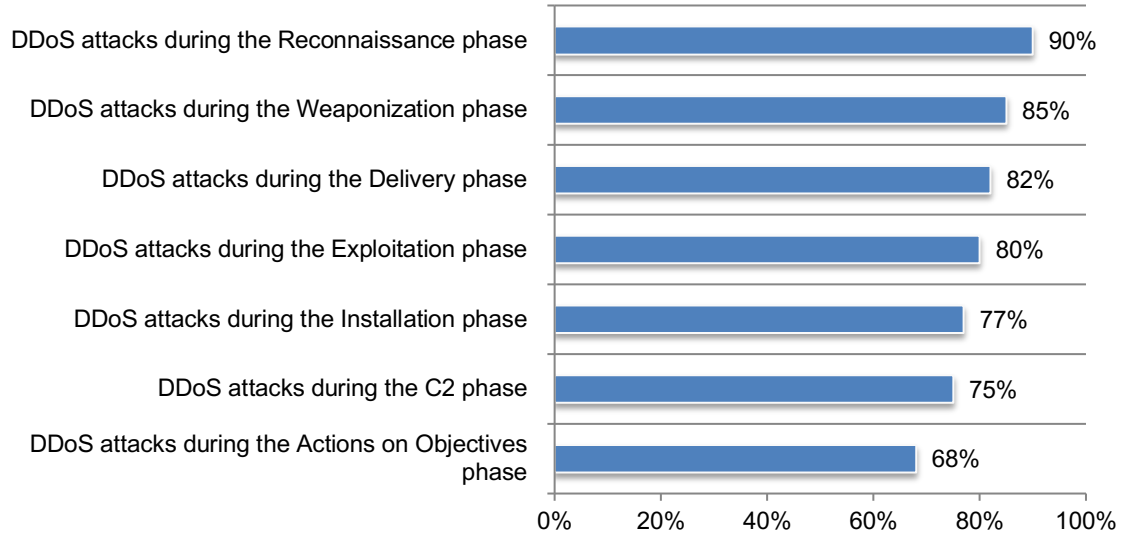
The Cyber Kill Chain is important to the tactics and defense strategies used to prevent DDoS attacks. When asked to rate the importance of the Cyber Kill Chain to reducing DDoS-related security risks on a scale of 1 = not important to 10 = very important, 74 percent of respondents say the Cyber Kill Chain is very important to shaping threat mitigation tactics and 60 percent say it is very important to the shaping of the DDoS defense strategy (7+ responses on the 10-point scale), as shown in Figure 18.

Figure 18. The importance of the Cyber Kill Chain
From 1 = not important to 10 = very important, 7+ responses presented



Stopping DDoS attacks in the Cyber Kill Chain is difficult. Respondents rate the importance of the Cyber Kill Chain in their approach to reducing DDoS security risks as very important. However, as shown in Figure 19, it is very difficult to stop DDoS attacks in the Cyber Kill Chain, especially during the reconnaissance phase.

Figure 19. Level of difficulty in stopping DDoS attacks in the Cyber Kill Chain
Very difficult and Difficult responses combined

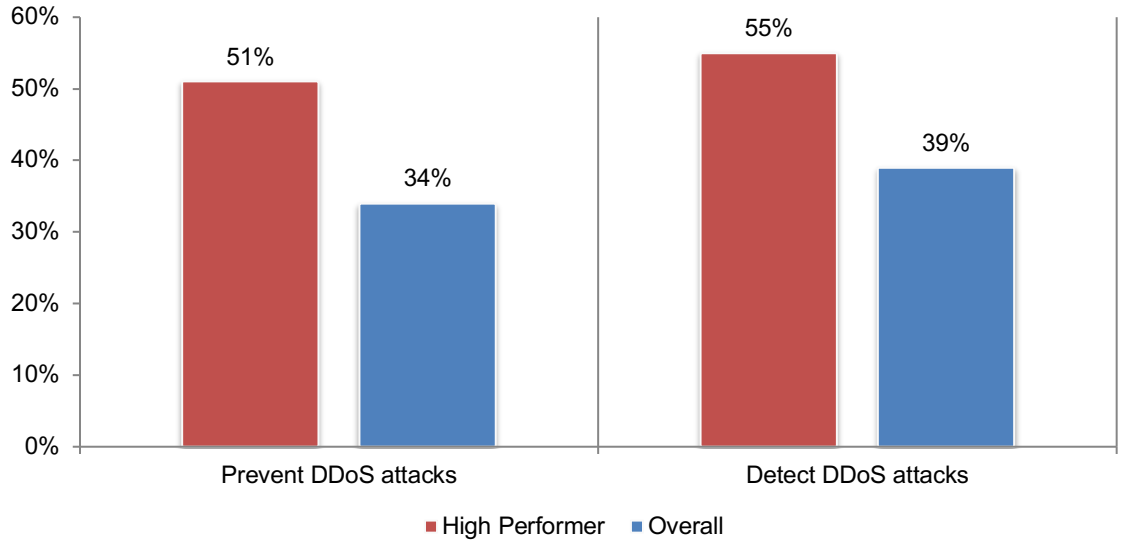


Best practices of communication service providers effective in moderating the impact of DDoS attacks

As part of this study, we conducted a special analysis of those organizations that are most capable of launching measures that moderate the impact of DDoS attacks. Twenty-nine percent of the total sample of respondents self-reported that their organizations have a high level of ability to accomplish this in order to reduce the impact and consequences of a DDoS attack. We refer to this sample as high performers and in this section, we compare the findings from this group to the overall sample.

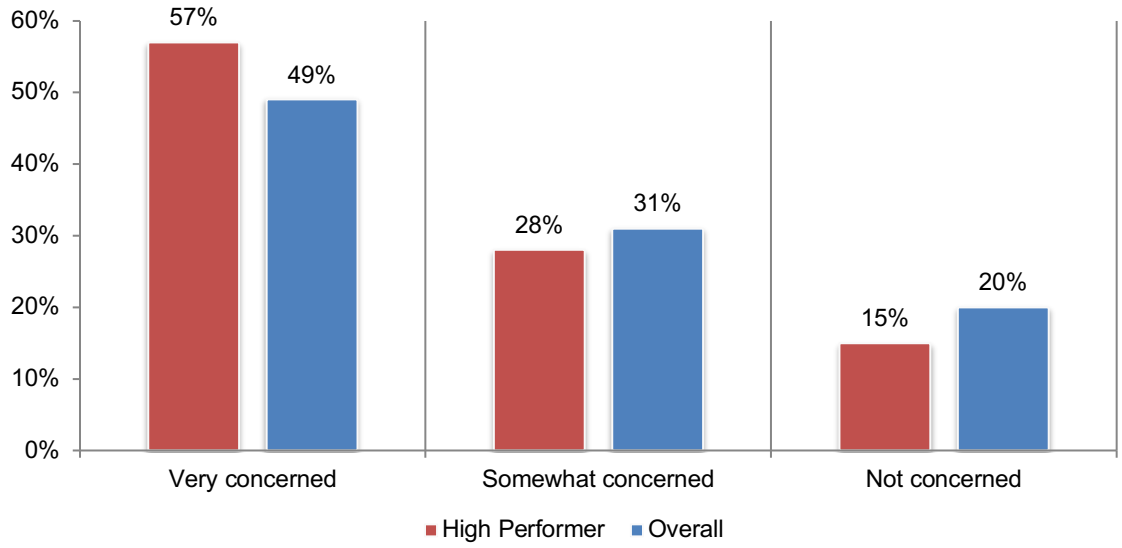
Organizations that are highly capable of launching measures that moderate the impact of DDoS attacks are more effective in preventing and detecting DDoS attacks. According to Figure 20, more than half of respondents (51 percent) say their organizations are very effective in preventing the impact of DDoS attacks and 55 percent say they are very effective in detecting these attacks. In contrast, only 34 percent and 39 percent of overall respondents say they are very effective in prevention and detection.

Figure 20. Effectiveness in preventing the impact of and detecting DDoS attacks
Very effective and Effective responses combined



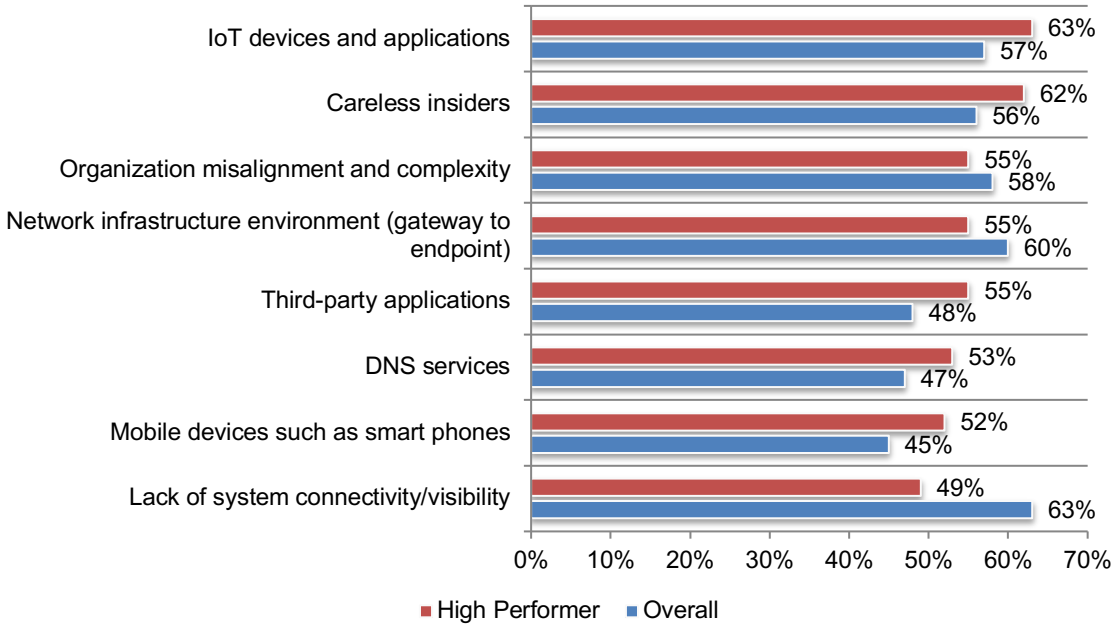
High performing organizations are more concerned than the overall sample about Mirai-type attacks. These attacks mobilize IoT devices to execute DDoS attacks and 57 percent of respondents in high performing organizations are very concerned about these attacks vs. 49 percent of respondents in the overall sample, as shown in Figure 21. The Mirai attack is a good example of IoT devices that are being used in DDoS attack.

Figure 21 How concerned is your organization about Mirai-type attacks that mobilize IoT devices to execute DDoS attacks?



High performing organizations are more likely to see the IoT, careless insiders and third-party applications as the most vulnerable to a DDoS-related security risk. As shown in Figure 22, 63 percent of respondents in high performing organizations are most likely to recognize that IoT devices and applications are areas at greatest security risk in the workplace. Careless insiders and third-party applications put their organizations at risk for a DDoS attack. In contrast, the overall sample of respondents are much more likely to be vulnerable to a DDoS attack because of lack of system connectivity/visibility.

Figure 22. Where are you seeing the greatest areas of potential DDoS-related security risk?
More than one response permitted



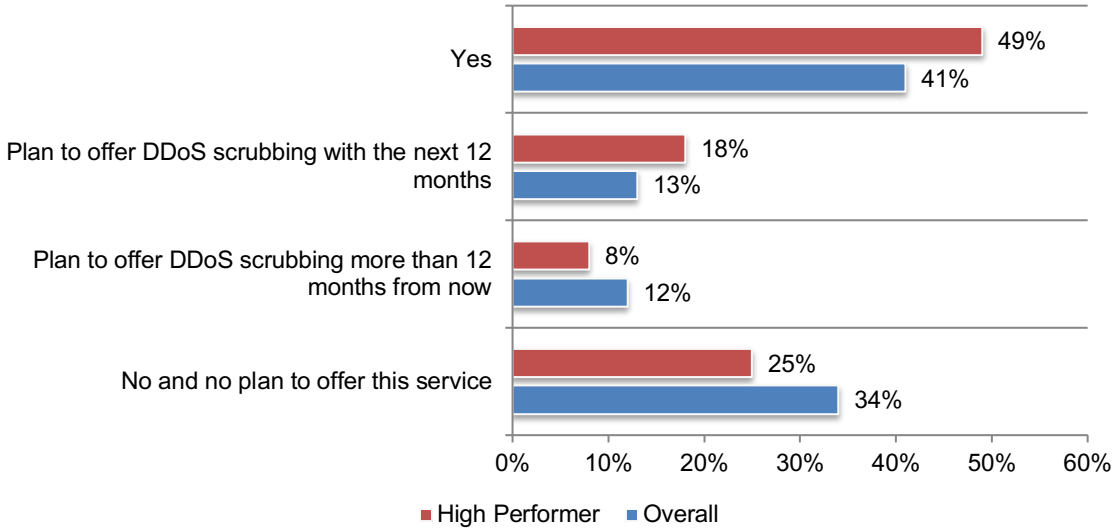
High performing organizations are more positive about their ability to respond to DDoS attacks. As shown in Figure 23, there is a significant gap between high performing organizations and the overall sample in perceptions about the difficulty in managing the threat intelligence process, integration with various security measures and a high false positive in DDoS-related threat intelligence.

Specifically, less than half of respondents (49 percent and 48 percent) in high performing organizations say the threat intelligence process is difficult to manage and DDoS-related intelligence does not integrate well with various security measures. Forty-five percent of respondents in high performing organizations vs. 58 percent of respondents in the overall sample say their DDoS-related intelligence has a high false positive rate.

Figure 23. Perceptions about the ability to respond to DDoS attacks
Strongly agree and Agree responses combined

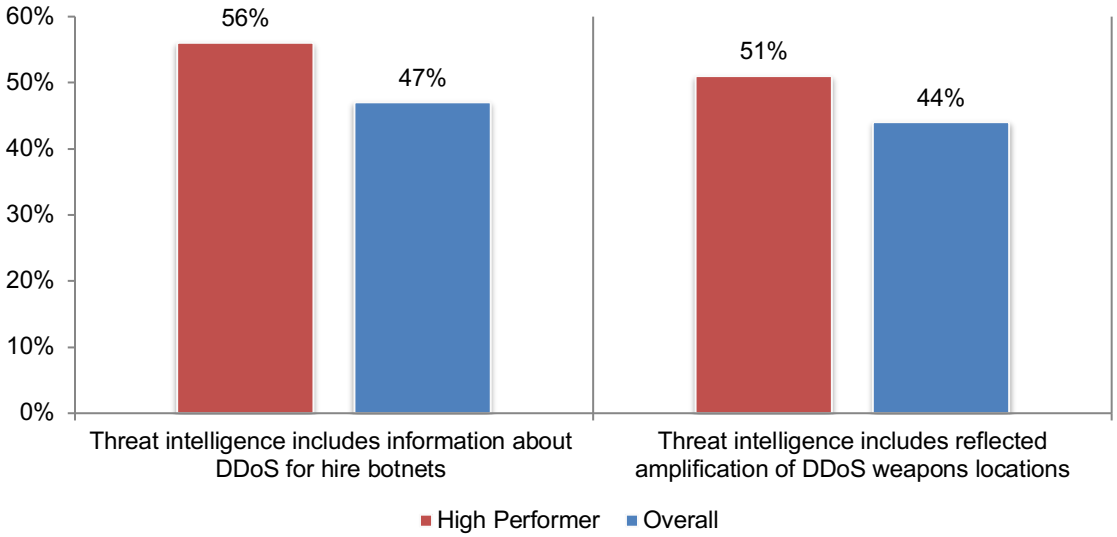
High performing organizations are more likely to offer DDoS scrubbing services. As shown in Figure 24, 75 percent of respondents in high performing organizations either offer DDoS scrubbing services today or plan to in the future. In contrast, 66 percent of respondents in the overall sample offer or plan to offer these services.

Figure 24. Does your organization offer DDoS scrubbing services to subscribers?



Reflected amplification attacks and attacks involving botnets are common. Despite the frequency of these types of attacks, most organizations' threat intelligence does not include actionable information about DDoS for hire botnets (56 percent of respondents) or the reflected amplification of DDoS weapons locations (51 percent of respondents), as shown in Figure 25.

Figure 25. Features of organizations' threat intelligence operations



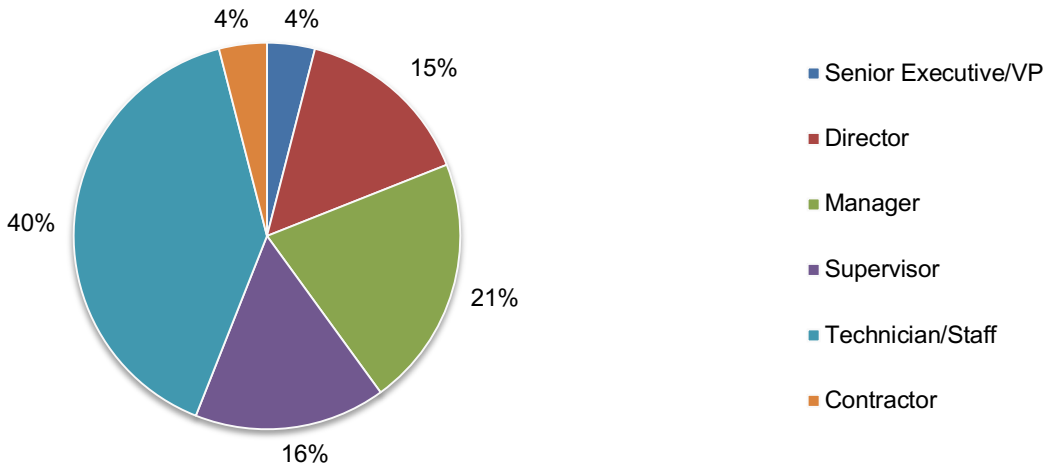
Part 3. Methods

A sampling frame of 7,086 IT and IT security practitioners in the United States who work in Internet Services Providers (ISPs), Mobile and/or Cloud Services Providers (CSPs) and are familiar with their organizations' defenses against DDoS were selected as participants in this survey. Table 1 shows 375 total returns. Screening and reliability checks required the removal of 50 surveys. Our final sample consisted of 325 surveys, or a 4.6 percent response rate.

Table 1. Sample response	FY2017	Pct%
Sampling frame	7,086	100.0%
Total returns	375	5.3%
Rejected or screened surveys	50	0.7%
Final sample	325	4.6%

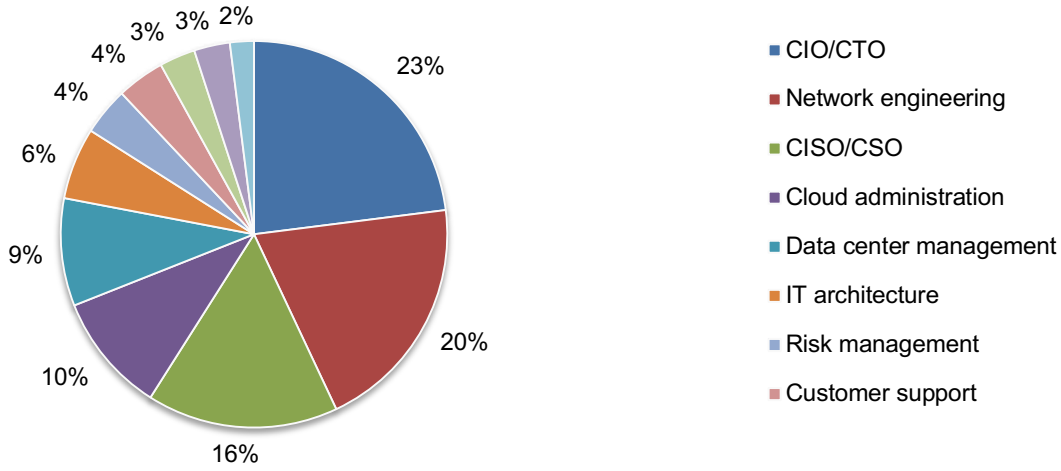
Pie Chart 1 reports the respondents' organizational levels within the participating organizations. By design, more than half of the respondents (56 percent) are at or above the supervisory levels and 40 percent of respondents described their position as technician/staff.

Pie Chart 1. Current position within the organization



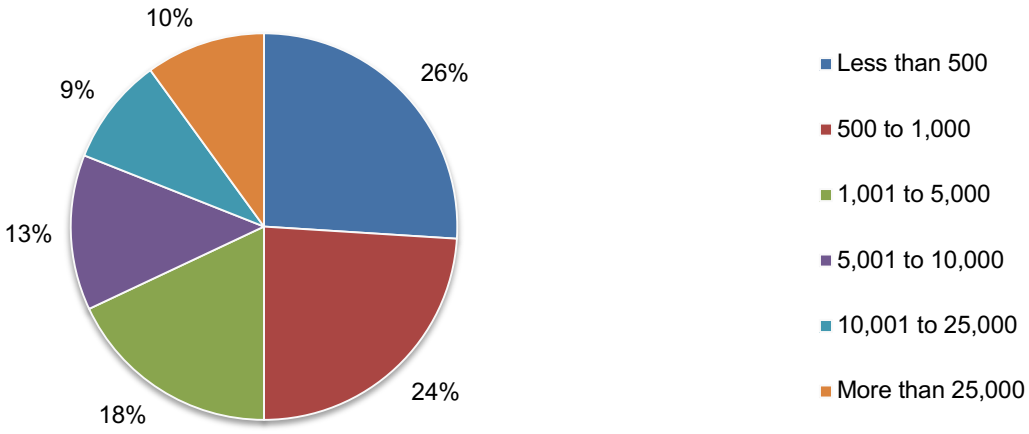
As shown in Pie Chart 2, 23 percent of respondents report to the CIO or CTO, 20 percent of respondents report to network engineering, 16 percent of respondents reports to the CISO or CSO and 10 percent of respondents report to the cloud administration.

Pie Chart 2. Respondents reporting channel or chain of command



Pie Chart 3 reports the head count of the respondents' global organizations. Half of respondents (50 percent) are from organizations with a worldwide head count greater than 1,000 employees.

Pie Chart 3. Head count of respondents' global organizations



Part 4. Caveats to this study

There are inherent limitations to survey research that need to be carefully considered before drawing inferences from findings. The following items are specific limitations that are germane to most Web-based surveys.

- Non-response bias: The current findings are based on a sample of survey returns. We sent surveys to a representative sample of individuals, resulting in a large number of usable returned responses. Despite non-response tests, it is always possible that individuals who did not participate are substantially different in terms of underlying beliefs from those who completed the instrument.

- Sampling-frame bias: The accuracy is based on contact information and the degree to which the list is representative of individuals who are IT or IT security practitioners who work in Internet Services Providers (ISPs) and/or Cloud Services Providers (CSPs) and are familiar with their organizations' defenses against DDoS. We also acknowledge that the results may be biased by external events such as media coverage. Finally, because we used a Web-based collection method, it is possible that non-Web responses by mailed survey or telephone call would result in a different pattern of findings.

- Self-reported results: The quality of survey research is based on the integrity of confidential responses received from subjects. While certain checks and balances can be incorporated into the survey process, the possibility remains that a subject did not provide accurate responses.

Appendix: Detailed Survey Results

The following tables provide the frequency or percentage frequency of responses to all survey questions contained in this study. All survey responses were captured between November 28, 2018 and December 18, 2018.

Survey response	Freq	Pct%
Total sampling frame	7,086	100.0%
Total returns	375	5.3%
Rejected surveys	50	0.7%
Final sample	325	4.6%

Part 1. Screening questions

S1. What best describes your organization's main focus?	Pct%
Internet Services Provider (ISP)	39%
Cloud Services Provider (CSP)	28%
Both an ISP and CSP	33%
None of the above (Stop)	0%
Total	100%

S2. How familiar are you with your organization's defense against DDoS?	
Very familiar	34%
Familiar	45%
Somewhat familiar	21%
No knowledge (Stop)	0%
Total	100%

S3. Do you have any responsibility in managing the IT security function within your organization?	Pct%
Yes, full responsibility	27%
Yes, some responsibility	55%
Yes, minimum responsibility	18%
No responsibility (Stop)	0%
Total	100%

Part 2. Background on DDoS

Q1a. How would you rate the effectiveness of your organization's effort **to prevent** DDoS attacks?	Pct%
Very effective	15%
Effective	19%
Somewhat effective	29%
Not effective	30%
Ineffective	7%
Total	100%

Q1b. How would you rate the effectiveness of your organization's efforts **to detect** DDoS attacks?	Pct%
Very effective	18%
Effective	21%
Somewhat effective	27%
Not effective	26%
Ineffective	8%
Total	100%

Q2. How many DDoS attacks did your organization experience in the past 12 months?	Pct%
Zero (skip to Q5)	31%
1 or 2	7%
3 or 4	14%
5 or 6	19%
7 or 8	15%
9 or 10	9%
More than 10	5%
Total	100%
Extrapolated value	4.22

Q3. What types of DDoS attacks did your organization experience? Please select all that apply.	Pct%
Volumetric floods	56%
Network protocol/level attacks	60%
Amplification and reflection	38%
Application level attacks	49%
Multi-vector attacks	39%
Other (please specify)	5%
Total	247%

Q4. What were the consequences of the DDoS attacks experienced by your organization in the past 12 months? Please rank from 1 = Most severe consequence to 8 = Least severe consequence	Average rank	Rank order
Revenue losses	3.12	3
Customer turnover	4.19	4
Diminished productivity for IT staff	2.11	2
Diminished productivity for end users	1.55	1
Theft of information assets	7.61	8
Damage to property, plant and equipment	4.84	5
Reputation damage	5.60	6
Regulatory or compliance violations	6.68	7

Q5. Please rank the following eight (8) security threats that your organization may face today (from 1 = the most severe to 8 = the least severe).	Average rank	Rank order
Distributed denial of services (DDoS)	4.27	4
Virus or malware infections	1.68	1
Web-based attacks	2.62	3
Stolen or hijacked computers	5.39	6
Malicious insider	6.60	8
SQL injection	4.51	5
Zero day attacks	5.52	7
Phishing & social engineering	2.13	2

Q6. In your opinion, what is the **most critical** barrier to preventing DDoS attacks? Please select only three top choices.	Pct%
Insufficient budget resources	34%
Lack of C-level support	19%
Lack of security leadership	25%
Lack of actionable intelligence	63%
Focus on other security priorities	42%
Insufficient personnel and in-house expertise	58%
Inadequate or Insufficient technologies	55%
Other (please specify)	4%
Total	300%

Q7. What security technologies do you use today to prevent, detect and contain DDoS attacks? Please select only three top choices.	Pct%
On-premises Anti-DDoS	47%
ISP or Cloud-based Anti-DDoS	61%
Anti-Virus	
Anti-DDoS	
Intrusion detection and prevention	50%
Firewalls/Next generation firewalls	44%
VPN and secure gateways	49%
Security incident and event management	45%
Other (please specify)	4%
Total	300%

Q8. Is your organization planning to purchase an Anti-DDoS technology in the next 6 to 12 months?	Pct%
Yes	45%
No	42%
Unsure	13%
Total	100%

Q9. In your opinion, are DDoS attacks going to increase, decrease or stay at the same level or frequency over the next 12 to 24 months? DDoS frequency is . . .	Pct%
Significantly increasing	21%
Increasing	33%
Not changing	31%
Decreasing	11%
Significantly decreasing	4%
Total	100%

Q10. Following are six (6) characteristics or persona of DDoS attackers. Please select the top two (2) DDoS attackers that present the greatest cybersecurity risk to your organization?	Pct%
Is a criminal who seeks financial gains from the attack vis-à-vis extortion.	48%
Performs an attack under the guise of stress testing a company's IT infrastructure	35%
Is a thrill seeker or a member of the hacker community seeking status	25%
Is an angry and/or disgruntled user	21%
Is a hacktivist or nation state attacker	31%
Executes DDoS is a smoke screen to distract the company from another attack.	40%
Total	200%

Q11. How concerned is your organization about Mirai-type attacks that mobilize IoT devices to execute DDoS attacks?	Pct%
Very concerned	49%
Somewhat concerned	31%
Not concerned	20%
Total	100%

Part 3. Current state of DDoS security

Q12. Please rate your organization's ability to launch measures that moderate the impact of DDoS attacks. Please use the following 10-point scale from 1 = unable to perform measures to 10 = fully capable of performing measures.	Pct%
1 or 2	14%
3 or 4	21%
5 or 6	36%
7 or 8	18%
9 or 10	11%
Total	100%
Extrapolated value	5.32

Attributions: Please rate the following statements about the security posture of your organization using the agreement scale provided below each item. **Strongly agree and agree response combined.**	Pct%
Q13a. My organization is vigilant monitoring DDoS attacks.	43%
Q13b. Launching a strong offensive against hackers and other cyber criminals is very important to my organization's security strategy.	49%
Q13c. In my organization, DDoS attacks are mostly done with botnet and reflected amplification sources.	51%
Q13d. My organization's DDoS-related threat intelligence is often too stale (out of date) to be actionable.	70%
Q13e. My organization's DDoS-related threat intelligence is often inaccurate and/or incomplete.	62%
Q13f. My organization's DDoS-related threat intelligence process is very complex.	40%
Q13g. My organization's DDoS-related threat intelligence process is difficult to manage.	55%
Q13h. My organization's DDoS-related threat intelligence has a high false positive rate.	58%
Q13i. My organization's DDoS-related threat intelligence does not integrate well with various security measures.	60%

Q14. The following table contains 7 (seven) layers in the typical IT security stack. Please allocate the **DDoS-related security risk** inherent in each one of the 7 (seven) layers experienced by your organization. Note that the sum of your allocation must equal 100 points.	Points
Physical layer	3.47
Network layer	34.72
Server layer	12.50
Application layer	15.97
Device layer	13.89
Data layer	11.81
User layer	7.64
Total must = 100	100.00

Q15. Where are you seeing the great areas of potential **DDoS-related security risk** within your IT environment today? Please choose only your top seven **(7)** choices.	Pct%
DNS services	47%
Data centers	39%
Operating systems	33%
Third-party applications	48%
Desktop or laptop computers	55%
Mobile devices such as smart phones	45%
IoT devices and applications	57%
Network infrastructure environment (gateway to endpoint)	60%
Malicious insiders	9%
Careless insiders	56%
Cloud computing infrastructure and services	38%
Virtual computing environments (servers, endpoints)	41%
Mobile/remote employees	46%
Lack of system connectivity/visibility	63%
Organization misalignment and complexity	58%
Other (please specify)	5%
Total	700%

Q16. What are the most effective cybersecurity technologies for improving your organization's ability to moderate the impact **DDoS-related security ri**sk? Please choose only your top five (5) choices.	Pct%
Technologies that secure the perimeter	36%
Technologies that secure users/devices and apps/data at the perimeter	39%
Technologies that stop or minimize malware	56%
Technologies that quickly detect and contain DDoS attacks	63%
Technologies that provide intelligence about networks and traffic	68%
Technologies that provide intelligence about attackers' motivation and weak spots	48%
Technologies that simplify the reporting of threats	28%
Technologies that secure endpoints including mobile-connected devices	61%
Technologies that minimize insider threats (including negligence)	23%
Technologies that secure information assets	24%
Technologies that isolate or sandbox malware infections	54%
Total	500%

Q17a. Relative to other cyber attacks, how difficult is DDoS to prevent?	Pct%
Very difficult	34%
Difficult	48%
Not difficult	18%
Total	100%

Q17b. Relative to other cyber attacks, how difficult is DDoS to detect?	Pct%
Very difficult	29%
Difficult	48%
Not difficult	23%
Total	100%

Q17c. Relative to other cybersecurity attacks, how difficult is DDoS to contain?	Pct%
Very difficult	27%
Difficult	47%
Not difficult	26%
Total	100%

Following are four (4) features of security technologies that provide defensive capabilities against DDoS-based attacks. Please rate the importance of each feature using the following 10-point scale from 1 – not important to 10 = very important.	
Q18a.The ability to integrate DDoS protection with cyber intelligence solutions	Pct%
1 or 2	6%
3 or 4	8%
5 or 6	12%
7 or 8	43%
9 or 10	31%
Total	100%
Extrapolated value	7.20

Q18b.The ability to scale (elasticity) during times of peak demand	Pct%
1 or 2	4%
3 or 4	10%
5 or 6	9%
7 or 8	35%
9 or 10	42%
Total	100%
Extrapolated value	7.52

Q18c. The ability to reduce the number of false positives in the generation of alerts	Pct%
1 or 2	5%
3 or 4	11%
5 or 6	12%
7 or 8	30%
9 or 10	42%
Total	100%
Extrapolated value	7.36

Q18d.The ability to integrate analytics and automation to achieve greater visibility and precision in the intelligence gathering process	Pct%
1 or 2	6%
3 or 4	8%
5 or 6	14%
7 or 8	33%
9 or 10	39%
Total	100%
Extrapolated value	7.32

Q19a.Does your organization offer DDoS scrubbing services to subscribers?	Pct%
Yes	41%
Plan to offer DDoS scrubbing with the next 12 months	13%
Plan to offer DDoS scrubbing more than 12 months from now	12%
No and no plan to offer this service	34%
Total	100%

Q19b. If yes, what are the top motivations for bringing a DDoS scrubbing solution to market? Please select two top choices.	Pct%
Source of new revenues	50%
Meeting subscriber demand	58%
Enhancing the security posture of subscriber	43%
Maintaining competitive edge	46%
Other (please specify)	3%
Total	200%

Q19c. If yes, what are the main challenges for bringing a DDoS scrubbing solution to market?	Pct%
Scalability of the solution	61%
Interoperability with other anti-DDoS/anti-malware solutions	65%
Cost of solution	39%
Complexity of solution	53%
Lack of in-house expertise	47%
Lack of bandwidth	50%
Other (please specify)	3%
Total	318%

Q19d. If no, what are the main reasons for not offering DDoS scrubbing to your subscribers?	Pct%
Lack of subscriber demand	32%
Cost of solution	58%
Profitability of solution	52%
Availability of other anti-DDoS solutions	45%
Lack of in-house expertise	45%
Lack of bandwidth	49%
Other (please specify)	2%
Total	283%

Q20. Does your organization threat intelligence operations include the minimization of DDoS for hire botnets?	Pct%
Yes	47%
No	53%
Total	100%

Q21. Does your organization's threat intelligence operations include the minimization of reflected amplification DDoS weapons?	Pct%
Yes	44%
No	56%
Total	100%

Part 4. Cyber Kill Chain

Q20. How familiar are you with the term Cyber Kill Chain?	Pct%
Very familiar	34%
Familiar	31%
Not familiar	14%
No knowledge (Skip to D1)	21%
Total	100%

Q21. How important is the Cyber Kill Chain framework for shaping your organization's DDoS defense strategy?	Pct%
1 or 2	8%
3 or 4	12%
5 or 6	20%
7 or 8	32%
9 or 10	28%
Total	100%
Extrapolated value	6.70

Q22. How important is the Cyber Kill Chain framework for shaping your organization's DDoS threat mitigation tactics?	Pct%
1 or 2	6%
3 or 4	7%
5 or 6	13%
7 or 8	33%
9 or 10	41%
Total	100%
Extrapolated value	7.42

Q23. In your opinion, how difficult is it to stop DDoS attacks during the Reconnaissance phase of the kill chain?	Pct%
Very difficult	51%
Difficult	39%
Not difficult	10%
Total	100%

Q24. In your opinion, how difficult is it to stop DDoS attacks during the Weaponization phase of the kill chain?	Pct%
Very difficult	49%
Difficult	36%
Not difficult	15%
Total	100%

Q25. In your opinion, how difficult is it to stop DDoS attacks during the Delivery phase of the kill chain?	Pct%
Very difficult	47%
Difficult	35%
Not difficult	18%
Total	100%

Q26. In your opinion, how difficult is it to stop DDoS attacks during the Exploitation phase of the kill chain?	Pct%
Very difficult	47%
Difficult	33%
Not difficult	20%
Total	100%

Q27. In your opinion, how difficult is it to stop DDoS attacks during the Installation phase of the kill chain?	Pct%
Very difficult	44%
Difficult	33%
Not difficult	23%
Total	100%

Q28. In your opinion, how difficult is it to stop DDoS attacks during the C2 phase of the kill chain?	Pct%
Very difficult	45%
Difficult	30%
Not difficult	25%
Total	100%

Q29. In your opinion, how difficult is it to stop DDoS attacks during the Actions on Objectives phase of the kill chain?	Pct%
Very difficult	36%
Difficult	32%
Not difficult	32%
Total	100%

Part 5. Your role and organization

D1. What organizational level best describes your current position?	Pct%
Senior Executive/VP	4%
Director	15%
Manager	21%
Supervisor	16%
Technician/Staff	40%
Contractor	4%
Total	100%

D2. Check the primary person you or your leader reports to within the organization.	Pct%
CEO/COO	3%
CIO/CTO	23%
CISO/CSO	16%
Risk management	4%
Cloud administration	10%
Data center management	9%
Compliance/audit	3%
Network engineering	20%
IT architecture	6%
Customer support	4%
Other business-related functions	2%
Total	100%

D3. What is the worldwide headcount of your organization?	Pct%
Less than 500	26%
500 to 1,000	24%
1,001 to 5,000	18%
5,001 to 10,000	13%
10,001 to 25,000	9%
More than 25,000	10%
Total	100%

For more information about this study, please contact Ponemon Institute by sending an email to research@ponemon.org or call at 1.800.887.3118.

Ponemon Institute

Advancing Responsible Information Management

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

We uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.