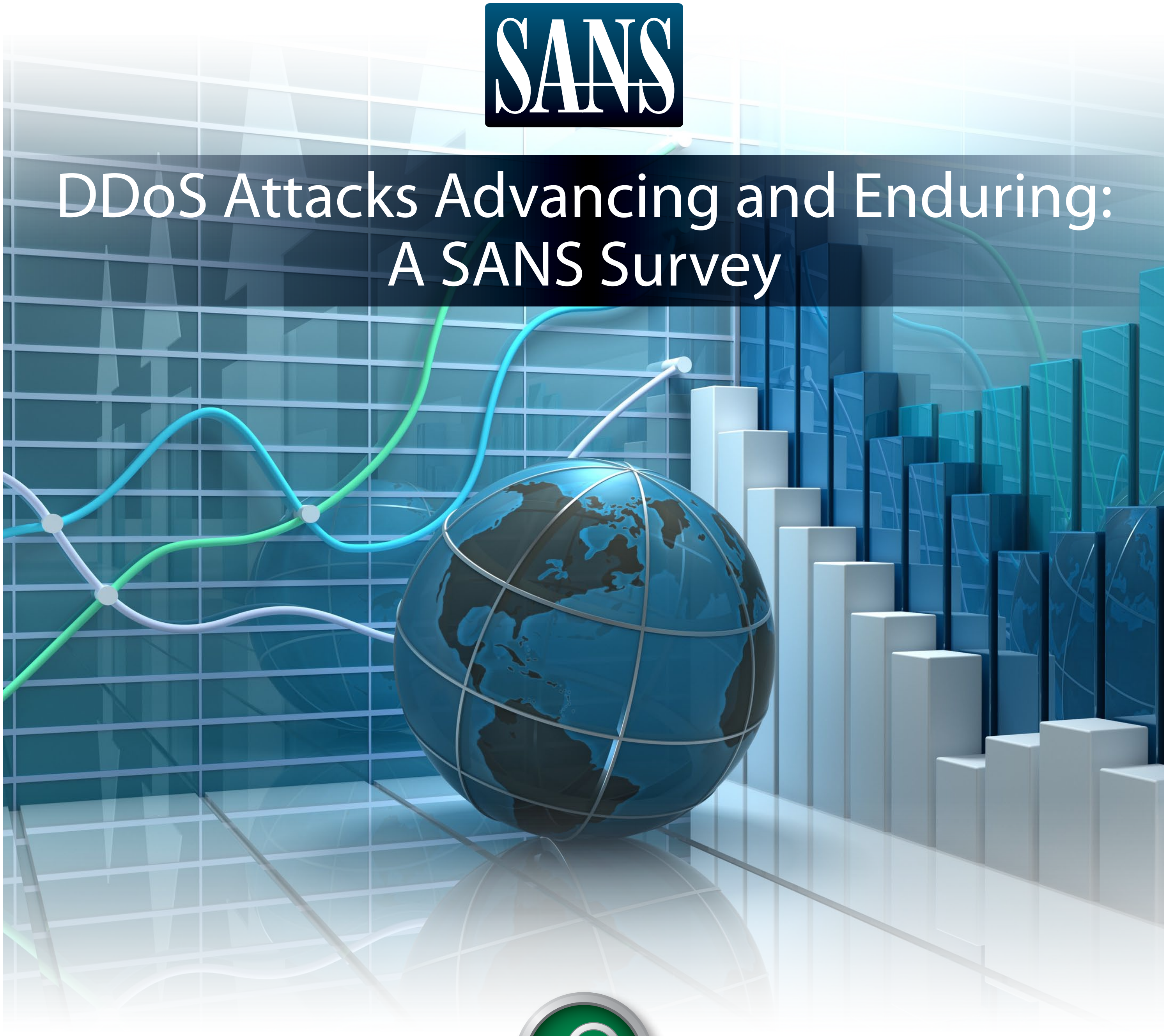
DDoS Attacks Advancing and Enduring: A SANS Survey

DDoS Attacks Advancing and Enduring: A SANS Survey



A SANS Analyst Survey

Written by John Pescatore

February 2014

Sponsored by
Corero Network Security

Executive Summary

Distributed denial of service (DDoS) attacks continue to grow in frequency, sophistication and bandwidth. There are numerous reasons for this. For example, DDoS tactics are increasingly targeting vulnerabilities in specific applications, such DNS servers or even Network Time Protocols (NTP) used for syncing date and time between machines on a network, according to Schneier on Security.[1]

Krebs on Security reports that these attacks are also increasing in volume, with a DDoS targeting NTP against his site sustaining 200 Gbps at its peak.[2] DDoS components are also becoming part of larger malware packages, such as DDoS bot installers on compromised servers.[3]

These trends are supported by a new SANS survey on the state of DDoS readiness. In the survey, 378 security and network managers reveal that they are experiencing more frequent and sophisticated DDoS attacks. The survey also reveals that many enterprises are indeed not prepared to deal with the problem.

These and other trends are discussed in the rest of this report.

Key Findings: SANS 2014 DDoS Survey

1. **Almost 40% of enterprises are completely or mostly unprepared for DDoS attacks.** Sadly, 23% of respondents indicated they did not have a plan for DDoS mitigation, and another 16% were unaware of any such plans. And, 50% have never tested their DDoS capabilities.
2. **Organizations are not upgrading their systems and tools to detect/mitigate DDoS attacks.** Respondents (26%, the most common response) still rely on their operational infrastructure to protect against denial of service attacks.
3. **Using weighted averages, respondents saw 4.5 DDoS attacks per year, with bandwidth averaging 1.7GBs per event.** The average attack duration was 8.7 hours, with service outages averaging 2.3 hours per event. At the extremes, some respondents experienced hundreds of attacks per year, and one suffered a two-day service outage.
4. **The most damaging DDoS attacks, which mix brute force (volumetric) attacks with targeted, application-specific attacks, have much the same frequency (39%) as targeted (42%) and volumetric (41%) alone.** DDoS attacks tend to use a small set of Internet ports, but a variety of techniques to cause damage.
5. **The most valued factor in a DDoS mitigation solution is preventing damage to specific applications, followed by preserving bandwidth and handling high-volume attacks.** These choices reflect the concern to protect against accidentally interrupting legitimate business sessions. Fully automated solutions that require little to no human intervention were not in demand.
6. **DDoS mitigation solutions integrating on-premise equipment and ISP and/or mitigation architectures are nearly four times more prevalent than on-premise or services-only solutions.** The growing sophistication of DDoS attacks and the sensitive nature of potential disruption to business services require both local and upstream protections that work in sync.
7. **DDoS mitigation is a shared responsibility between IT security and operations.** In the survey, 60% of respondents answered that responsibility is shared between security and operations, and the rest are equally split between security or operations. This indicates that DDoS mitigation is primarily seen and executed as a network operation.

[1] www.schneier.com/blog/archives/2014/01/ddos_attacks_us.html

[2] http://krebsonsecurity.com/2014/02/the-new-normal-200-400-gbps-ddos-attacks

[3] www.computerworld.com/s/article/9244878/New_DDoS_malware_targets_Linux_and_Windows_systems

Survey Participants

Participants responded to the electronic survey, which was available from late December 2013 through mid-February 2014.

Industry Representation

Survey respondents came from a broad range of industries, as illustrated in Figure 1.

What is your company's primary industry?

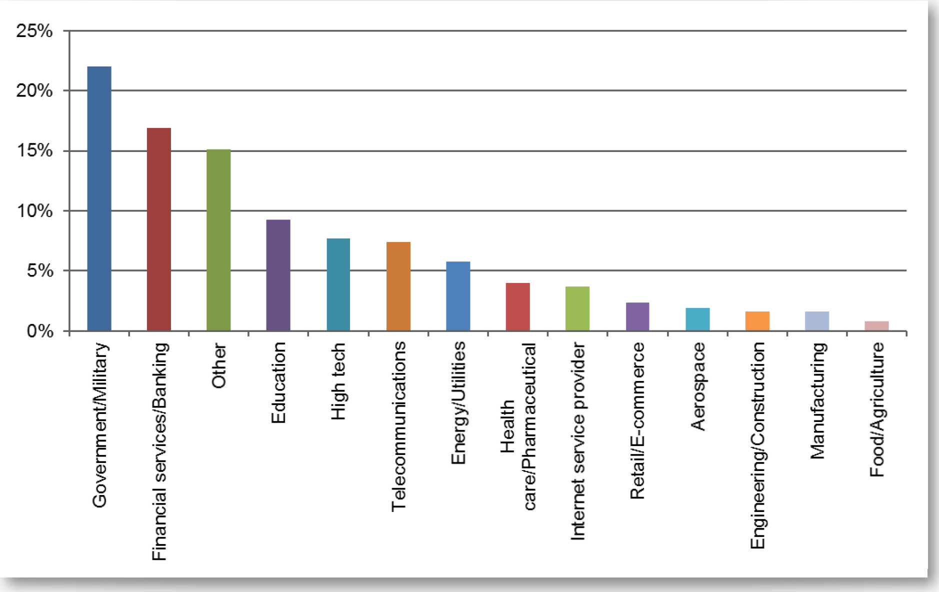
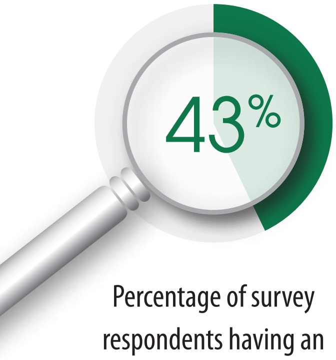


Figure 1. Respondent Industry Representation

This distribution generally mirrors the demographics of the SANS community, with significant participation from the government/military (22%) and financial services (17%) sectors. This sample has slightly higher representation from high tech (8%) and telecommunications (7%) and slightly lower participation from manufacturing (2%) than the SANS community. This aligns with the fact that the government, military and financial sectors are highly reliant on Internet connectivity for revenue, and manufacturing generally is not. The "Other" category, which was the third most selected option, was filled in with answers including "pharma," "online games," "insurance," and "entertainment." There were also many professional services and consulting firms written in under the "Other" category.



Percentage of survey respondents having an international workforce

Organizational Size

Respondents represented organizations of all sizes, from large to small. The largest companies (more than 15,000) were fairly evenly divided between domestic and international organizations; however, organizations of all sizes had some form of international reach, as shown in Figure 2.

What is the total size of the workforce at your organization?

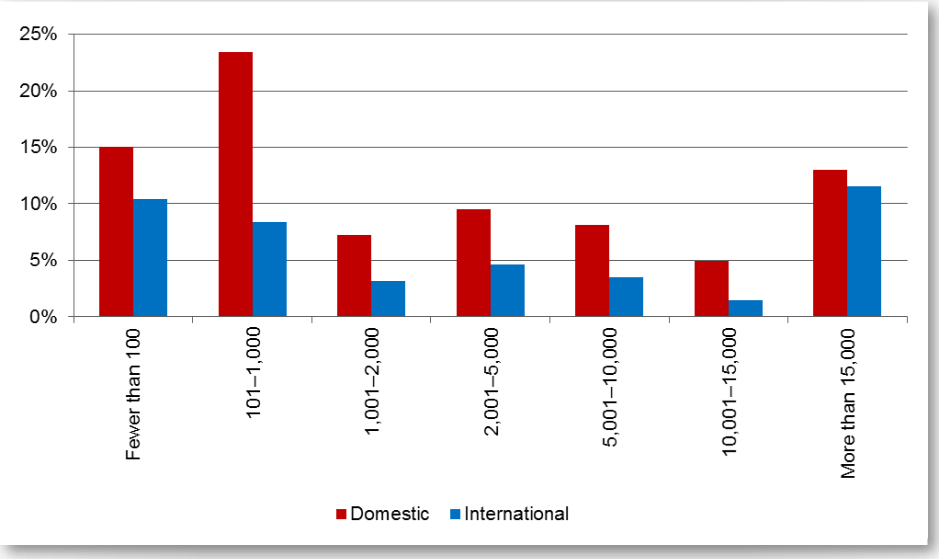


Figure 2. Domestic and International Workforce Size

This distribution also closely mirrors the demographics of the SANS community.

Respondent Roles

Security professionals represented the largest occupational group among the respondents, with security administrators or analysts being the largest occupational group selected (39%); 24% of respondents represent IT leadership positions when considering the combination of senior security professionals such as security managers, directors or CISOs (14%) and IT managers, IT directors or CIOs (10%). Figure 3 details the roles of survey participants.

20%

Percentage of survey respondents who were network or systems staff

What is your primary role in the organization?

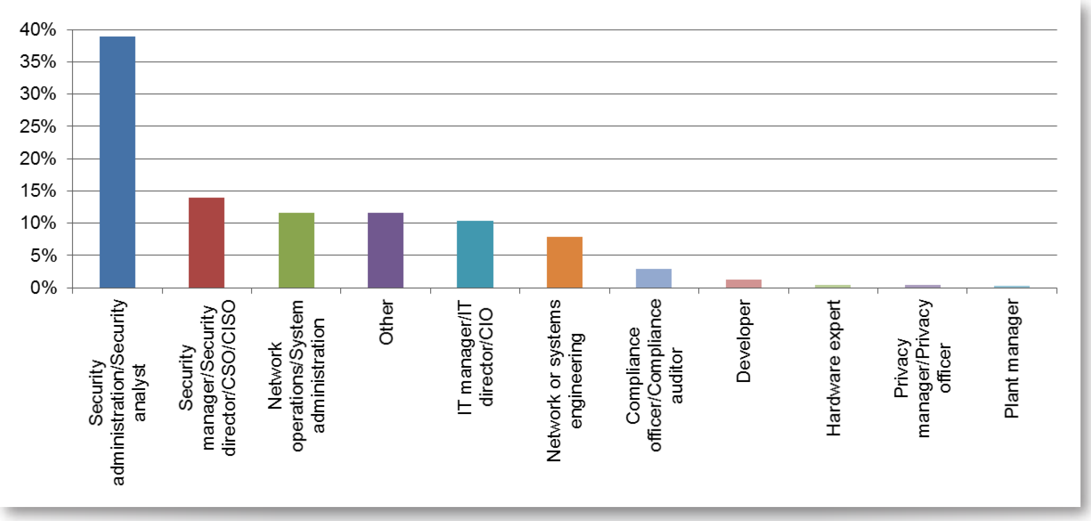


Figure 3. Respondent Roles

The relatively low levels of management participation in this survey indicates that DDoS is considered more of an operational issue than a governance issue. For the same reason, participation by privacy and compliance officers was also low.

Network operations, system administrators and network or systems engineers, who would be more responsible for operational security issues, comprised a combined 20%, slightly higher than in other SANS surveys, lending support to the idea that DDoS is of prime interest to those responsible for network operations. This is also supported in another question we report on in the next section, under which security and operations see DDoS mitigation as a shared responsibility.

Numerous respondents (12%) in the broadly distributed "Other" category indicated they were consultants or in the incident response group. One respondent noted, "I am the entire IT department!" (Note that respondents were allowed to choose more than one option, representing an overlap in responsibilities in some cases.)

Mitigation Plans

Understanding how your organization will respond if (when?) it suffers a DDoS attack is key to minimizing both vulnerabilities and damages. Often, however, establishing plans is hindered by conflicts over responsibility for the plan or budgetary concerns.

What's the Plan?

Enterprises should have DDoS plans in place, and those plans should be regularly tested. However, 39% of respondents did not have or did not know about a denial of service plan for their organization, as shown in Figure 4.

EXPERT ADVICE:

Enterprises should have DDoS plans in place, and those plans should be regularly tested. One way to achieve this is to include such planning as part of your organization's business continuity/ disaster recovery/ continuity of operations planning (COOP).

Does your organization have a plan for mitigation if it suffers a DDoS attack?

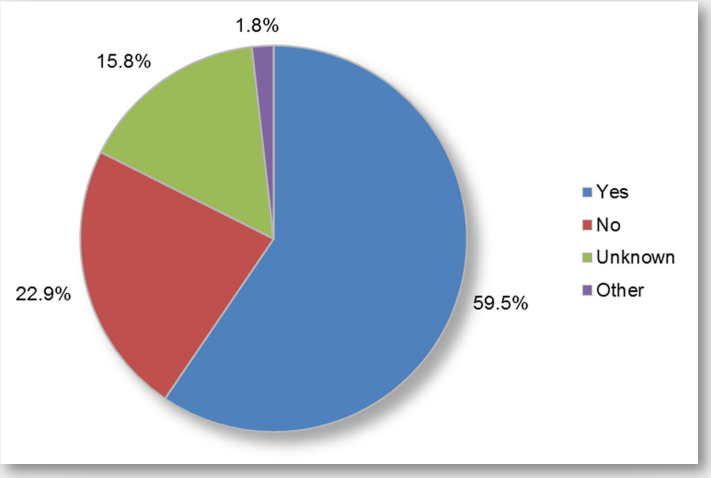


Figure 4. Organizational Plans for Mitigating DDoS Attacks

This percentage is slightly lower than the portion of respondents who reported they have not yet experienced a DDoS event (35%) or those that are unsure if they have (28%). This is the same problem noted years ago with respect to disaster recovery/ business continuity practices. Organizations often neglected developing a mitigation plan until a disaster occurred. Of course, that lack of planning was often determined to be a major reason why damage was so extensive.

Many security frameworks, such as NIST 800-34[4] and the Critical Security Controls (CSCs, Control 8),[5] have explicitly called for business continuity/contingency planning, which has increased the percentage of enterprises that do have such a plan.

[4] http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf

[5] www.sans.org/critical-security-controls/control/8

Who Drives the Plan?

Network security is often a shared responsibility between network operations and the security group. The same is true for responsibility for DDoS mitigation. The majority of organizations (62%) responded that denial of service is a shared responsibility between security and network operations. See Figure 5.

EXPERT ADVICE:

DDoS response plans should define roles and responsibilities of all groups involved in planning, response and mitigation.

Who within your organization has led DDoS mitiagation?

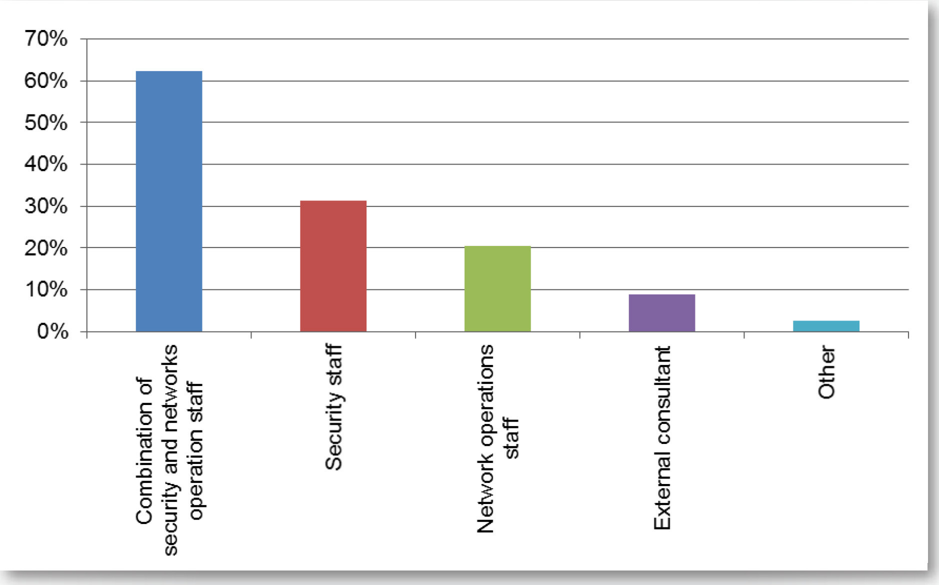


Figure 5. Responsibility for DDoS Mitigation

Shared responsibility is appropriate for organizations that do have a plan in place before a DDoS event. Network operations staff can handle many routine DDoS events, while more significant and more targeted attacks require direct involvement of the security staff.

However, this type of joint response requires advance planning, coordination and cooperation to be effective. The impact of a DDoS attack can actually be magnified if the wrong action, or a conflicting action, is taken. For example, one group disconnecting Internet connections or blocking apparent source IP addresses while the other group is applying mitigation strategies may actually disrupt legitimate business traffic, thus helping the attackers achieve their goal.

EXPERT ADVICE:

Enterprises should test their DDoS mitigation processes at least quarterly, or after any major network change, whichever comes first.

Ready, Set, Test?

Many organizations invested in backup generators and uninterruptible power systems, only to find that they didn't work when the power went out. It is now standard practice to test those systems at least quarterly to ensure continued business operations in case of an outage.

The DDoS mitigation world seems to be repeating that same pattern. Almost 50% don't test their systems at all, and only 26% test their capabilities yearly or more frequently, as shown in Figure 6.

Have you ever tested your DDoS mitigation capability?

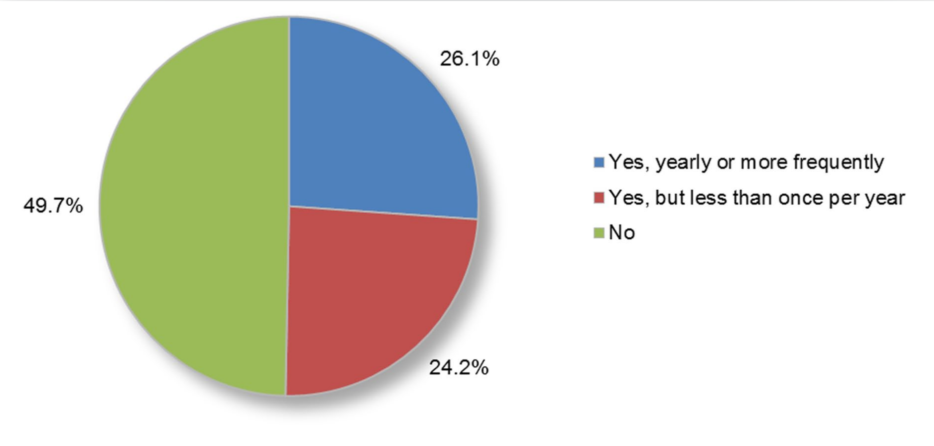


Figure 6. Testing of DDoS Mitigation Capabilities

Where's the Money?

Budgeting is always a concern when plans need to be created, security controls need to be procured and maintained and mitigation procedures are called into action.

Only 37% said that they carve out a percentage of the IT budget for DDoS security, as illustrated in Figure 7.

Do you carve out a percentage of IT budget for DDoS defense solutions/technology?

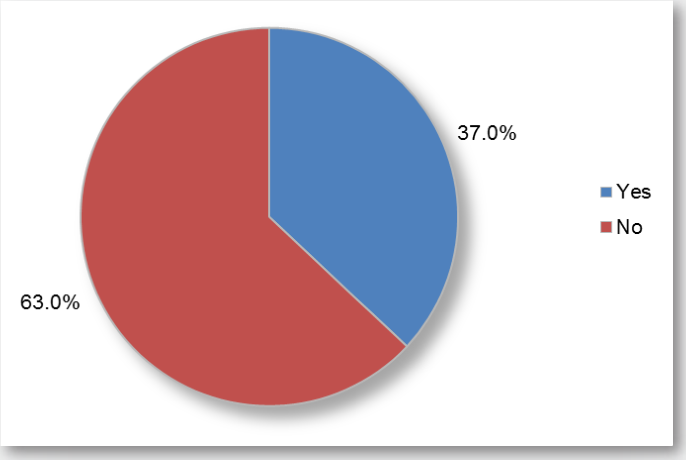


Figure 7. DDoS Defense Budgets

63%

Percentage of respondents who have not carved out a percentage of the IT budget for DDoS security

The percentage of organizations having a formal budget allocation for DDoS defense (37%) is very close to the percentage that have DDoS plans in place (39%). The minor difference likely indicates that many organizations rely on DDoS services from their ISPs, where the cost is included in the bandwidth costs with no separate procurement or budget line-item costs.

Typically, budget line items are needed whenever on-premise dedicated DDoS mitigation equipment is used. The percentage reporting that they do have a budget for DDoS is a bit lower than the percentage indicating that they have on-premises DDoS mitigation equipment in the mix (52%), likely indicating the on-premise equipment is part of a DDoS service offering, as opposed to being procured separately.

When asked about the history of DDoS attacks in their organization, the largest percentage (35%) said they had not yet experienced any DDoS attacks, followed by 28% who were unsure of whether they had experienced an attack. Given the previously cited statistics about growth in DDoS attacks, many of these organizations are likely to experience some level of denial of service attack in the near future.

How Frequent Are Attacks?

Of those that were attacked by some form of DDoS over the past year, 37% of respondents had experienced at least one DDoS attack in the past year. The most common response (18%) cited between one and three DDoS events. The weighted average across all individual enterprise respondents was just over 4.5 attacks per year. See Figure 8.

Has your organization ever experienced a DDoS attack?
If so, how many were you able to document within the last year?

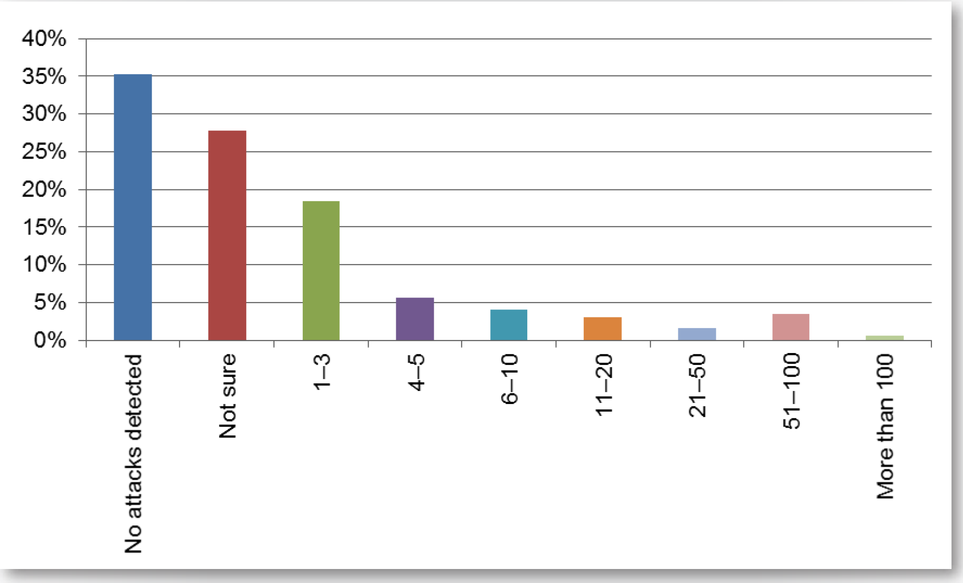


Figure 8. DDoS Attack Frequency

Another 4% of respondents experienced more than 50 DDoS attacks in the last year, two of whom experienced more than 100. One respondent commented that their organization experienced more than 300 attacks per month across their multitenant environment.

What Type of Attack?

The DDoS attack types experienced were evenly distributed across targeted (or application-specific, typically web app) attacks (42%), volumetric or brute force/flood events (41%) and attacks that combined both techniques (39%), as illustrated in Figure 9.

EXPERT ADVICE:

DDoS defenses must be able to mitigate both brute force (volumetric) attacks and targeted applications individually, while also providing the capacity to deal with blended attacks.

What type of attack(s) did you experience? Select all that apply.

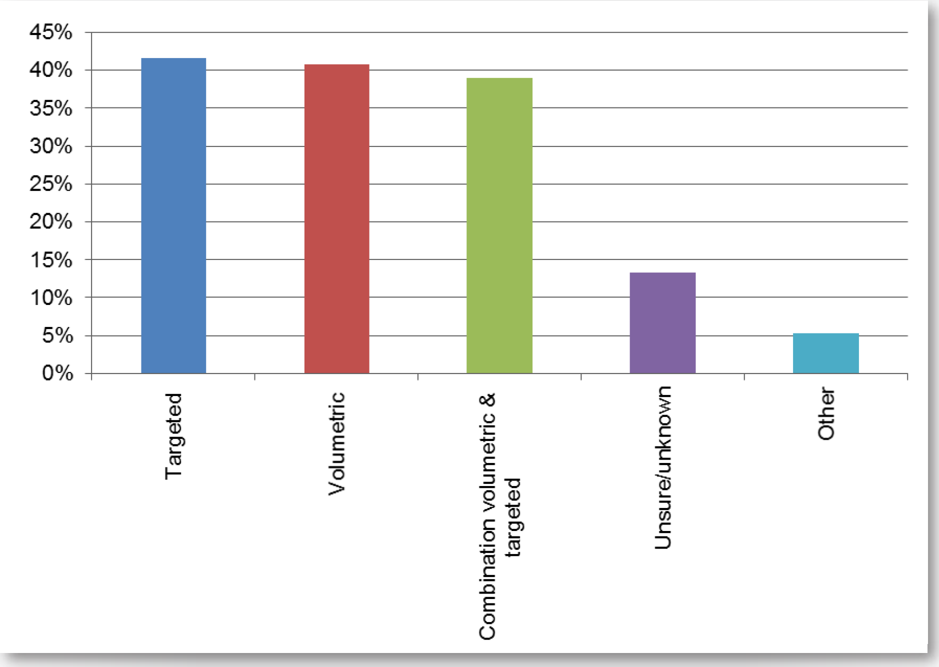


Figure 9. Types of Attacks

Discussions with security managers indicate that attacks commonly start with a single technique and escalate to combining multiple techniques when the attackers see that initial mitigation efforts are working. This is another reason why relying on infrastructure devices (as opposed to dedicated DDoS mitigation equipment and/or services) is a bad idea. Load balancers, firewalls and other such equipment are rarely effective against DDoS attacks using varying and combined techniques.

How Long Did It Last?

Time is money, and downtime is lost revenue. As a result, minimizing the time a detected attack lasts is an important task. The most common DDoS attacks lasted less than one hour (42%), although 14% experienced attacks that lasted for up to one day and 13% for more than a day (between one and three days). See Figure 10.

On average, how long did the detected attacks last?

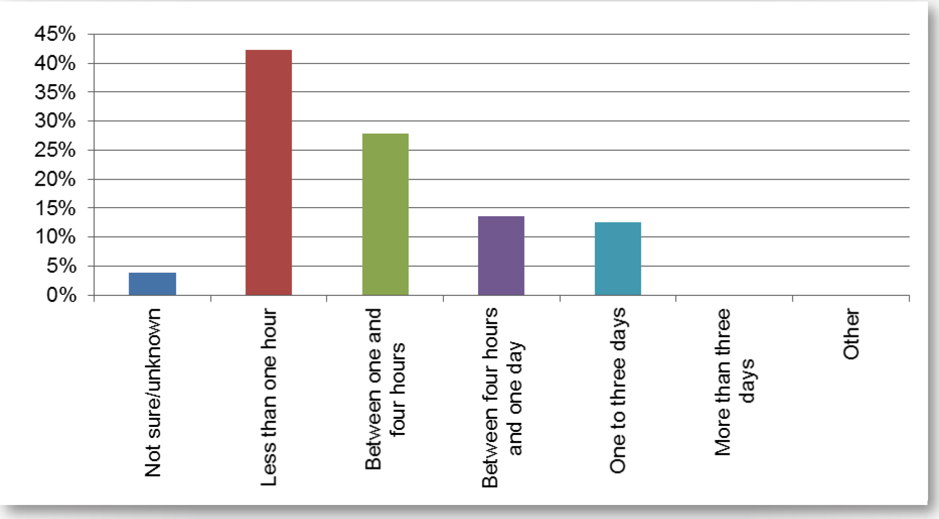


Figure 10. Average Length of DDoS Attacks

The weighted average for attack duration across all reported DDoS attacks is 8.7 hours, or an entire business day.

Percentage experiencing disruptions of one hour or less

To get an indication of how much damage DDoS attacks caused, we asked whether the attacks caused an outage that disrupted business, and if so, for how long. One hour or less was the most common duration, with 39% of respondents selecting this answer. However another 16% experienced outages for four hours, and 6% experienced outages for eight hours or more. See Figure 11.

Did the attacks cause an outage that disrupted your business and, if so, for how long was your business disrupted on average?

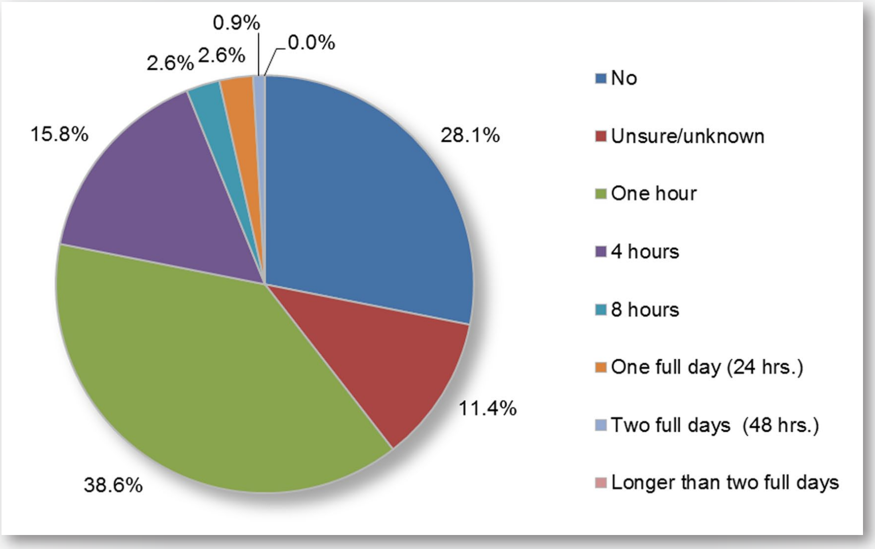


Figure 11. Time of Disruptions Caused by Outages

The weighted average disruption was 2.3 hours. For critical business systems, an average service disruption of two hours may not be acceptable. A recent Ponemon study[6] places the average disruption of service at 54 minutes, with an average cost of $22,000. It further suggests that costs can range from $1 to $100,000 per minute.

[6] http://security.radware.com/uploadedFiles/Resources_and_Content/Attack_Tools/CyberSecurityontheOffense.pdf

How Big Was It?

This survey points out that modern DDoS attacks are frequently combinations of high-bandwidth, brute force floods with equally damaging application-specific attacks. However, the press loves to quote claims of an attack being "the biggest DDoS attack ever," and management has often heard those claims. But just how big is a typical attack? According to our respondents, not nearly as large as those currently being reported in the media. Figure 12 illustrates the size of the attacks suffered by survey respondents.

On average, what was the bandwidth of the attacks?

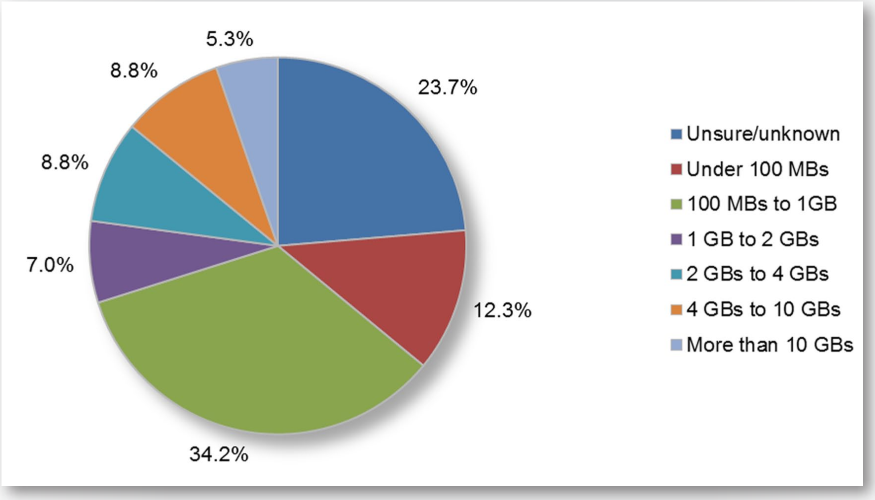


Figure 12. Bandwidth of Attacks

53%

Percentage of DDoS attacks reported to have bandwidths of less than 2 GBs

Overall, 53% of DDoS attacks were under 2 GBs in bandwidth, with those in the 100 MBs to 1 GB range (34%) the most frequently reported. However, 23% reported attacks averaged more than 2 GBs, with 13% averaging more than 4 GBs. A weighted average of all reported events is just under 1.7 GBs.

The rise in application-specific, targeted DDoS attacks makes bandwidth figures somewhat less important. Resource starvation and other sophisticated denial of service attacks can be just as damaging as brute force (volumetric) attacks. However, the finding that a mix of targeted and volumetric attacks is the norm shows that enterprises must be prepared to deal with high-bandwidth attacks.

Not surprisingly, respondents identified ports 80 (HTTP) and 443 (HTTPS) as being the vector for most attacks. Ports 53 (DNS), 445 (Microsoft Active Director and SMB) and 21 (FTP) are the only other ports receiving multiple mention. Write-in answers included DNS/NTP reflection attacks, described in the introduction of this paper, as well as ICMP attacks, port 80 UDP and random port attacks on high numbers above 20000.

Do You See What I See?

It is important that the business impact of DDoS become visible to people at all levels of the organization. Such visibility will remind administrators that DDoS attacks are real and pose a significant threat to the organization and may aid security and network staff in securing additional funding.

The most common level of visibility for DDoS attacks was to IT and security administrators (83%), which makes sense. However, only 67% of CISOs and CIOs had the same level of visibility, as shown in Figure 13.

What level of visibility did these attacks get in your organization? Please select all that apply.

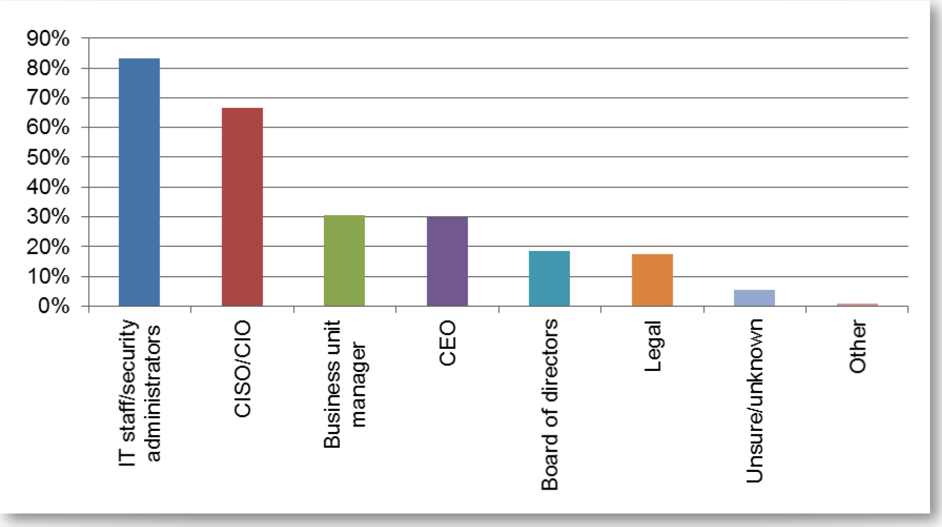


Figure 13. Visibility into DDoS Attacks

The relatively low level of visibility to CISOs and CIOs was surprising, especially because a high percentage of DDoS attacks resulted in service outages, as discussed earlier in this paper. Because 28% of respondents reported no business disruption due to DDoS attacks, it is likely that attacks that did not cause noticeable degradation of service were not reported to upper management.

Response Basics

Because denial of service often impacts critical business services, the response to a DDoS attack must take into account minimizing additional disruption to those (and other) services. This often requires dedicated local expertise with business knowledge. In the survey, the majority (87%) deployed their own personnel to respond, while 42% also involved their ISP or an outside service provider (see Figure 14).

Who usually responded to the attacks? Select all that apply.

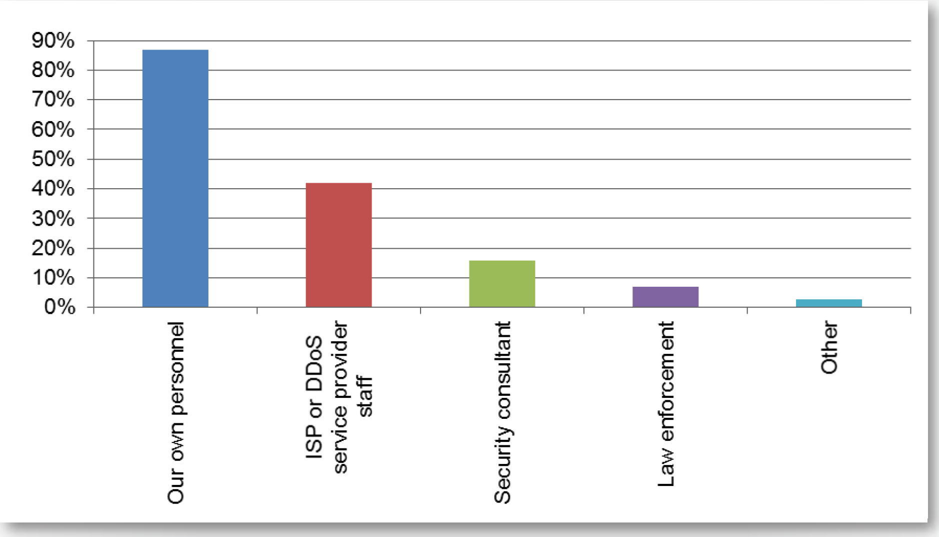


Figure 14. Attack Responders

Interestingly, although organizations may need to notify law enforcement after an event is under control to fulfill legal and regulatory obligations, only 7% involved law enforcement organizations in direct response efforts. Because DDoS events cause business disruption, response efforts focus on immediate mitigation and restoration of business services, whereas law enforcement focuses on determining who the attacker is, not how to quickly stop the attack.

EXPERT ADVICE:

Organizations should attempt to preserve logs and other information that may aid law enforcement investigative efforts after the attack.

How Are Mitigation Capabilities Deployed?

Although experience has generally shown that the least effective approach to mitigating a denial of service attack is relying on infrastructure elements (servers, gateways, routers, switches, firewalls and so on), this was the most frequently cited approach by respondents (26%). The respondents reporting this are very likely the same group that has yet to experience a major DDoS attack. It is common to see organizations procure DDoS products and services only after a DDoS attack has highlighted the failure of relying on existing infrastructure. See Figure 15 for more deployment statistics.

How are your denial of service mitigation capabilities deployed?

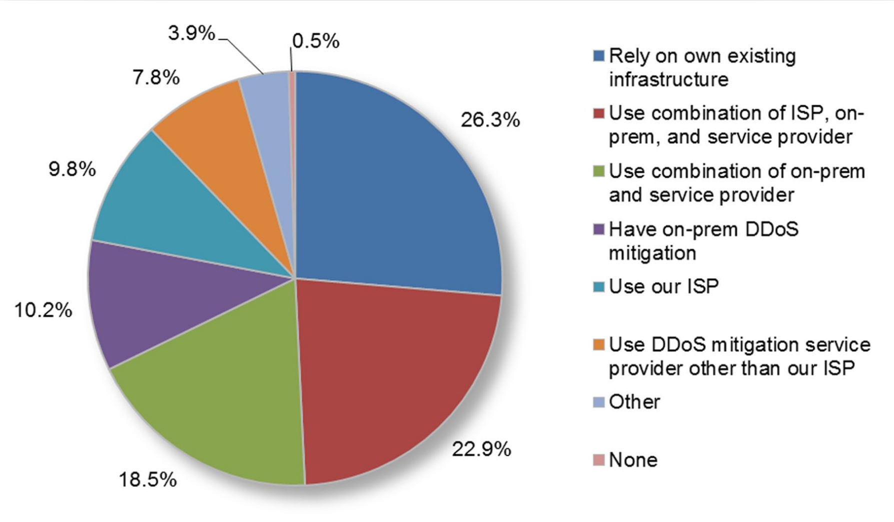


Figure 15. Deployment of Mitigation Capabilities

It is common to see organizations procure DDoS products and services only after a DDoS attack has highlighted the failure of relying on existing infrastructure.

The most effective DDoS mitigation architectures are normally a combination of on-premise DDoS mitigation and off-site ISP or service provider capabilities. This approach was cited as in use by more than 41% of respondents, with slightly more using ISPs (23%) over DDoS service providers (19%) in concert with on-premise capabilities. Just greater than 10% rely solely on on-premise DDoS mitigation hardware, whereas just fewer than 10% rely completely on ISPs. Only 8% rely exclusively on external DDoS mitigation service providers. Anecdotal evidence shows that larger enterprises are increasingly adopting combination approaches, whereas smaller enterprises that feel they are less likely to be the target of major attacks rely on pure services approaches.

What Solution Factors Are Important?

The DDoS mitigation feature that was most frequently cited as most important was maintaining bandwidth and throughput, as shown in Figure 16.

Please rank the following factors in order of importance in a DDoS mitigation solution. (1 = Most Important; 7 = Least Important)

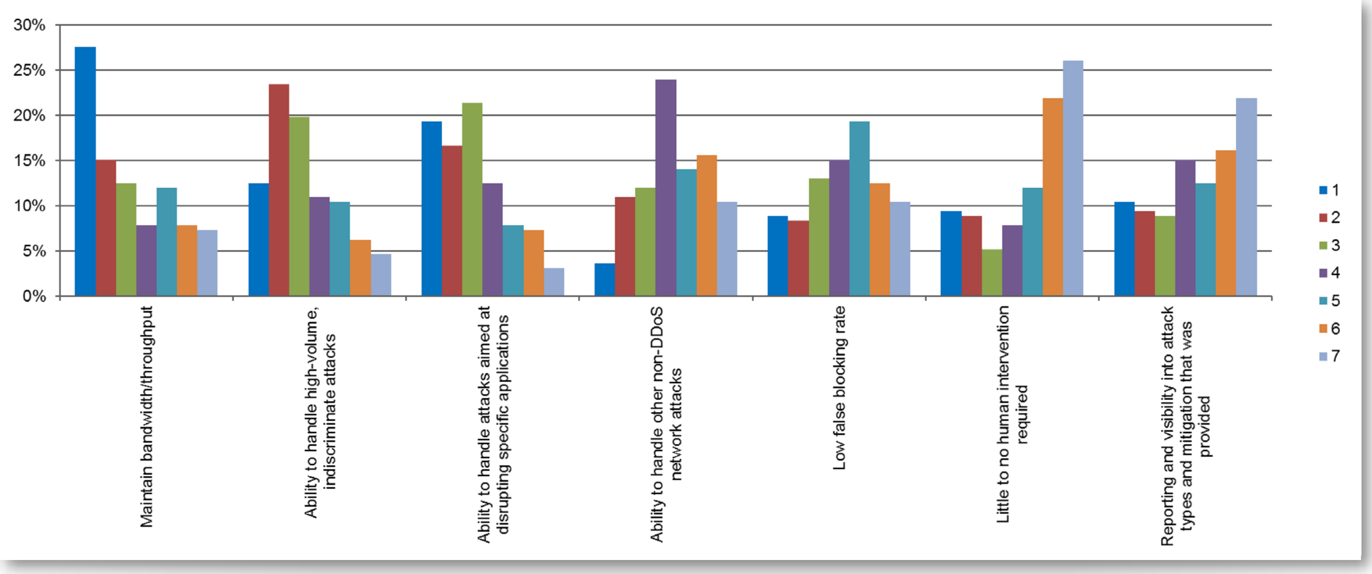


Figure 16. Factors Important in DDoS Mitigation Solutions

However, when all rankings were weighted, the ability to stop targeted/application-specific attacks emerged as the leading concern (see Table 1).

Table 1. Factors of Importance in DDoS Mitigation (1 = Most Important; 7 = Least Important)

Factor	Rating
Ability to handle attacks aimed at disrupting specific applications	3.08
Maintain bandwidth throughput	3.16
Ability to handle high-volume, indiscriminate attacks	3.24
Low false blocking rate	4.22
Ability to handle other non-DDoS network attacks	4.35
Reporting and visibility into attack types and mitigation	4.55
Little to no human intervention required	4.91

These responses reflect the pressures security and network operations managers face in avoiding disrupting legitimate customer application traffic while mitigating DDoS attacks. The least important feature was "Little to no human intervention required," which emphasizes the need for local human expertise to assure that DDoS mitigation doesn't lead to self-inflicted business disruption.

Anecdotal evidence shows that even enterprises that fully rely on external service providers for DDoS mitigation prefer to have an on-premises "human in the loop" to make the decision to turn on mitigation.

Conclusion

The results of this survey show that in the past year 37% of respondents have experienced a DDoS attack, with 61% of those attacks resulting in some level of business disruption. Those attacks came in many forms, with sophisticated combinations of volumetric and targeted, application-specific attacks becoming the norm. This survey, in agreement with others cited as references, shows that for most enterprises it is a question of *when*, not *if*, they will experience a DDoS attack.

The key to minimizing the business impact of a DDoS attack is preparation, processes and prevention. Here the results were mixed: Almost 60% of respondents have a DDoS mitigation plan in place, but fewer than 30% test their capabilities at least yearly, and half have never tested their capabilities at all. The dynamic nature of both threats and enterprise network configurations dictate that DDoS processes and mitigation systems should be tested at least as frequently as uninterruptible power, disaster recovery and other business continuity processes are tested.

On the prevention side, the bad news is that 26% of respondents are still relying on the operational infrastructure to protect itself, which is sort of like depending on drywall to withstand thunderstorms and hurricanes rather than having a roof on your building. The good news is that 41% of respondents are using combinations of on-premise dedicated DDoS mitigation controls and ISP or cloud provider-based DDoS scrubbing. This architecture has proven to be the most effective against attacks that blend brute force attacks with targeted application-level DDoS.

This survey also revealed valuable insight into how these organizations are protecting against DDoS and what they still need to be doing. For example, DDoS protection and mitigation is seen more as a combined security/operational IT function than solely a security function, which explains why the abilities to maintain bandwidth, handle high-volume attacks and ensure business application throughput are among the top three choices selected for features in a DDoS mitigation system. This shared responsibility also requires that plans and testing involve personnel from both security and IT/network operations.

The bottom line is that while DDoS attacks can't be predicted or avoided, they can be mitigated such that business disruption does not occur. The key elements to effective and efficient DDoS mitigation are flexible architectures that combine on-site and upstream detection and mitigation with regular testing of capabilities.

About the Author

John Pescatore joined SANS in January 2013, with 35 years of experience in computer, network and information security. He was Gartner's lead security analyst for more than 13 years, working with global 5000 corporations, government agencies and major technology and service providers. In 2008, he was named one of the top 15 most influential people in security and has testified before Congress on cybersecurity.

Prior to joining Gartner Inc. in 1999, John was senior consultant for Entrust Technologies and Trusted Information Systems, where he started, grew and managed security consulting groups focusing on firewalls, network security, encryption and public key infrastructures. Prior to that, he spent 11 years with GTE developing secure computing and telecommunications systems. In 1985 he won a GTE-wide Warner Technical Achievement award.

Mr. Pescatore began his career at the National Security Agency, where he designed secure voice systems, and the United States Secret Service, where he developed secure communications and surveillance systems—and the occasional ballistic armor installation. He holds a bachelor's degree in electrical engineering from the University of Connecticut and is an NSA-certified cryptologic engineer. He is an Extra class amateur radio operator, callsign K3TN.

Sponsor

SANS would like to thank this paper's sponsor:

corero
FIRST LINE OF DEFENSE

Last Updated: May 22nd, 2016

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANSFIRE 2016	Washington, DCUS	Jun 11, 2016 - Jun 18, 2016	Live Event
SANS Philippines 2016	Manila, PH	Jun 20, 2016 - Jun 25, 2016	Live Event
SANS Pen Test Berlin 2016	Berlin, DE	Jun 20, 2016 - Jun 25, 2016	Live Event
Digital Forensics & Incident Response Summit	Austin, TXUS	Jun 23, 2016 - Jun 30, 2016	Live Event
SANS Salt Lake City 2016	Salt Lake City, UTUS	Jun 27, 2016 - Jul 02, 2016	Live Event
SANS Cyber Defence Canberra 2016	Canberra, AU	Jun 27, 2016 - Jul 09, 2016	Live Event
MGT433 at SANS London Summer 2016	London, GB	Jul 07, 2016 - Jul 08, 2016	Live Event
SANS London Summer 2016	London, GB	Jul 09, 2016 - Jul 18, 2016	Live Event
SANS Rocky Mountain 2016	Denver, COUS	Jul 11, 2016 - Jul 16, 2016	Live Event
SANS San Antonio 2016	San Antonio, TXUS	Jul 18, 2016 - Jul 23, 2016	Live Event
SANS Delhi 2016	Delhi, IN	Jul 18, 2016 - Jul 30, 2016	Live Event
SANS Minneapolis 2016	Minneapolis, MNUS	Jul 18, 2016 - Jul 23, 2016	Live Event
SANS San Jose 2016	San Jose, CAUS	Jul 25, 2016 - Jul 30, 2016	Live Event
Industrial Control Systems Security Training	Houston, TXUS	Jul 25, 2016 - Jul 30, 2016	Live Event
Security Awareness Summit & Training	San Francisco, CAUS	Aug 01, 2016 - Aug 10, 2016	Live Event
SANS Boston 2016	Boston, MAUS	Aug 01, 2016 - Aug 06, 2016	Live Event
SANS Vienna	Vienna, AT	Aug 01, 2016 - Aug 06, 2016	Live Event
SANS Dallas 2016	Dallas, TXUS	Aug 08, 2016 - Aug 13, 2016	Live Event
SANS Portland 2016	Portland, ORUS	Aug 08, 2016 - Aug 13, 2016	Live Event
Data Breach Summit	Chicago, ILUS	Aug 18, 2016 - Aug 18, 2016	Live Event
SANS SEC401 Luxembourg en francais	OnlineLU	May 30, 2016 - Jun 04, 2016	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced