Denial of Service

Brighten Godfrey
CS 538 October 18 2012
DoS in the real world

Source: Arbor Networks

Disclaimers:

- Survey of 111 network operators, not direct measurement
- Arbor sells network security solutions :-)


DDoS is frequent and can be big

As shown in Figure 17, nearly 47 percent of respondents indicated that they experienced 1 to 10 DDoS attacks per month during the survey period, while over 44 percent experienced 10 to 500 or more DDoS attacks per month.

As illustrated in Figure 18, commercial flow-telemetry collection/analysis systems, such as Arbor’s Peakflow® SP solution (“Peakflow SP”), were the leading tools used to detect and classify the highest-bandwidth attacks experienced by respondents during the survey period. Custom in-house developed tools and various other mechanisms were the second- and third-most popular solutions in this category, respectively.

Figure 17 Source: Arbor Networks, Inc.
DDoS is frequent and can be big

During the survey period, respondents reported a significant increase in the prevalence of flood-based DDoS attacks in the 10 Gbps range. This represents the "mainstreaming" of large flood-based DDoS attacks, and indicates that network operators must be prepared to withstand and mitigate large flood attacks on a routine basis.

As illustrated in Figure 15, the highest-bandwidth attack observed by respondents during the survey period was a 60 Gbps DNS reflection/amplification attack. This represents a 40 percent decrease from the previous year in terms of sustained attack size for a single attack.

Based upon our experiences working with operators over the last year and data collected using Arbor’s ATLAS portal, we believe that this apparent decrease in attack magnitude at the high end does not represent a significant reduction of risk from flood-based DDoS attacks. Sixty Gbps is a very large attack, and the increased prominence of 10 Gbps and higher attacks reflected in survey responses indicates that the volume of traffic in large-scale flood attacks remains a significant risk.

Over 74 percent of respondents reported that the highest-bandwidth DDoS attack they experienced during this survey period was directed at their end customers, while nearly 13 percent reported that their own ancillary support services such as DNS and Web portals were targeted (Figure 16). Almost 11 percent indicated that their own network infrastructure was the target of the highest-bandwidth attack they experienced.

![Average Number of DDoS Attacks per Month](source: Arbor Networks, Inc.)

![Largest Bandwidth Attacks Reported](source: Arbor Networks, Inc.)
Many types of attacks

Largest Observed Attack Vectors

Figure 6: Largest Observed Attack Vectors
Source: Arbor Networks, Inc.
[2009 data]

Application-Layer DDoS Attacks

Figure 7 Source: Arbor Networks, Inc.
Therefore, the results in Figure 20—which indicate that ideology or "hacktivism" ranks as the single most commonly observed motivation for DDoS attacks, with online gaming-related attacks ranked second—were surprising, while at the same time confirming our subjective observations during the survey period.

We believe this finding may well comprise one of the single most important data points in this year's report, with major implications in terms of threat assessment, situational awareness and continuity of operations for network operators, governmental bodies, law enforcement agencies and end customers alike.

Some additional free-form comments in response to this question follow:

• “As a network operator, we see the traffic, but seldom are privy to the motivation behind the attack. I think that in many cases, our customers (colleges and universities) don’t know why the attack happened either—they just deal with it.”

• “[We see] attacks against online auction sites which are similar to attacks against online gaming sites and attacks intended to manipulate financial markets.”

• “We’ve experienced Quake 3/Source Engine-based exploit attacks. Attackers are abusing legitimate game servers to send specially-crafted attack packets directing them to attack others, similar to DNS reflection/amplification attacks.”

In this year’s survey, we asked respondents about the longest-duration DDoS attack they had observed during the survey period. Responses varied widely, ranging from “a few minutes” to “six months, with bursts and calm stages.”

Figure 20 Source: Arbor Networks, Inc.
As in previous reports, despite their functional and operational limitations, ACLs continue to be the single most widely used tool to mitigate DDoS attacks (Figure 27). Destination-based, remotely-triggered blackholes (D/RTBH) and intelligent DDoS mitigation systems (IDMS) such as the Peakflow® SP Threat Management System (“TMS”) and the now-discontinued Cisco Guard are the second and third most widely used mitigation mechanisms, respectively. Approximately 53 percent of respondents indicated that D/RTBH is still in common use—despite the fact that D/RTBH blocks all traffic to the target and essentially completes the DDoS attack for the attacker, penalizing the victim. Other techniques utilized by respondents include custom-coded application-layer classification tools, CDNs, DPI systems, load-balancers and GeoIP-based blocking of attack traffic purportedly emanating from specific geopolitical localities.

Once again this year, no respondents indicated that QoS is still in general use as an attack mitigation technique for inbound DDoS attacks. Rate-limiting inbound traffic to attack targets invariably has the unintended side effect of enabling attack traffic to “crowd out” traffic from legitimate sources.

Figure 27 Source: Arbor Networks, Inc.
DoS in context

Several questions were added based upon suggestions by respondents to a previous survey, or as a result of direct feedback from one of the many network security and operations forums from which survey review was expressly solicited.

Arbor Networks intends to continue conducting this survey annually and sharing the results with the global Internet security and operations communities. Our goals are:

1. To continually refine the questionnaire in order to provide more timely, detailed and relevant information in future editions.
2. To increase the scope of the survey respondent pool to provide greater representation of the global Internet network operations community.

Most Significant Operational Threats

More than 71 percent of respondents indicated that DDoS attacks toward end customers were a significant operational threat encountered during this 12-month survey period (Figure 6).

Over 62 percent also identified misconfigurations and/or equipment failures as contributing to outages during the survey period. Botnets and their unwanted effects (including DDoS attacks) were rated highly, as were DDoS attacks targeted at operators' network infrastructure and ancillary support services, such as DNS, Web portals and email servers. Spam and VoIP-related attacks were included in the “Other” category.

Figure 6 Source: Arbor Networks, Inc.
Announcements

Week after next: midterm project presentations

• Be ready by Tuesday of that week
• 5 minute presentation, 5 minute questions
  - What problem are you solving?
  - Why has past work not addressed the problem?
  - What is your approach for solving it?
  - What are your preliminary results & progress?