Navigating Today’s DDoS Landscape
# Table of Contents

Overview ............................................................................................................................................. 4
Step I. Understanding Today’s DDoS – Volumetric, Network, and Application Attacks…… 4
  So What Can Be Done About It? ........................................................................................................ 6
Step II. Defending in Kind .................................................................................................................... 6
Step III: Evolving Best Practices for Mitigating DDoS Attacks .......................................................... 7
  Ixia BreakingPoint: Keeping One Step Ahead.................................................................................... 8
Then What? ........................................................................................................................................... 10
Overview

Front-page headlines have increased awareness but network and application security remain moving targets. Threats continue to advance quickly in both number and complexity, causing enterprises to seek new, more advanced solutions for safeguarding customer data, intellectual property, financial assets, and their all-important reputation.

But even after investing heavily in systems and services, countless organizations fall prey each year to devastating outages, often prompted by catastrophic distributed denial of service (DDoS) attacks. And while it seems like DDoS has been around forever, attacks continue to scale and evolve.

Though countless individual attacks have come and gone, denial of service remains a perennial challenge. To date, defense strategies have been driven in large part by the need to comply with industry standards and regulations designed to ensure confidentiality and data integrity. That’s all well and good, but for many businesses, downtime — the lack of site or data availability — represents even greater risk.

Today’s sophisticated, highly orchestrated attacks are launched by multiple parties with the goal of compromising premium data, revenues, and corporate reputations, often using DDoS to create a diversion for more malicious activity. DDoS attacks are enjoying a revival of sorts, with hackers driven by different motives employing different tactics, and using new types of attacks in new and different ways.

While technology solutions abound, most enterprises don’t fully comprehend the extent of their vulnerability, and what’s needed to remedy it, until they come under attack.

Step I. Understanding Today’s DDoS – Volumetric, Network, and Application Attacks

Extortion. Political statements. Competition. Distraction. No matter what their ulterior motive, today’s DoS attacks have long since eclipsed early initiatives driven largely by the desire to make headlines.

Several distinct approaches to attack are now quite common:

- **Volumetric or network attacks** that center on flooding the target’s network pipes to the point where bandwidth becomes saturated or defenses overwhelmed. User access to resources may then be randomly- or universally-denied.

  Threats may involve protocol, SYN, or ICMP floods, or more sophisticated attacks adding IP spoofing to the mix to elicit responses that further saturate the network environment. Advanced DNS attacks also feature a small group of compromised servers, used to blast a site with as much as 200 megabytes of traffic.
While SYN floods are becoming less prolific, an attack launched from a single laptop can still be used to jam systems and rob users of high performance. Other volumetric attacks that impact availability can prove highly debilitating, not to mention extremely cost- and time-intensive to combat and overcome.

- **Application-oriented attacks**, such as Apache Killer and Slowloris, attack server infrastructures and web capabilities directly, overwhelming resources and commandeering legitimate functions such as search features and shopping carts. For example, multiple searches may be initiated on terms that will return millions of records to eventually bust web or application limits. Similarly, repeatedly filling and abandoning shopping carts from multiple locations will eventually knock down applications.

At the top of the OSI stack, the application layer is proving to be the most difficult to defend, especially with conventional security technology. Now heavily targeted by today’s attackers, application-layer attacks differ from network attacks in that they’re specific to the target application.

Where SYN floods may be launched against a particular IP address, an application attack will usually exploit properties specific to the victim, such as the repeated downloading of a single PDF file on the website. To lower-level security devices, application-layer attack connections are indistinguishable from normal traffic.

- **Economic attacks** introduce a new twist on classic denial-of-service attacks that preys on those with credit cards on file in the cloud. Along with the applications and services moved to public cloud services, attackers may now leverage the credit limits associated with the SLAs. DDoS attackers deplete bandwidth, storage, or computing credit limits to take down the service.

- **Smokescreen attacks** are becoming the real danger inherent within DDoS, as they are used to deflect attention. As it becomes obvious that web properties are under attack, internal and external resources commonly focus on shutting it down, scrubbing traffic, and staying up. These intensive efforts afford ample opportunity for additional attack troops to sneak in the back door and inject SQL tools. These injections typically involve large numbers of odd requests, which would ordinarily stand out, but may be lost in the chaos of a seemingly routine DDoS attack.

- **SQL tools** may be used to crash databases, compromise response times, or even steal data. Attacks by noted hactivist groups are rumored to have begun with simple phishing attempts and netted the perpetrators critical pieces of military information such as GPS coordinates.

- **The “Combo”** comes into play when many of today’s advanced DoS attacks combine some or all of the approaches described above into multifaceted initiatives, mandating multifaceted defenses.

On the whole, DoS attacks have morphed from scenarios where one attacker launches a one-dimensional attack from a single commanding control point, to highly distributed, phased attacks involving multiple domains and encrypted communications. Coordinated efforts are frequently launched by multiple groups acting in tandem from multiple locations – either deliberately or by virtue of hijacking and botnets.

Now heavily-targeted by hackers, the application layer is the most difficult to defend.
Today’s DDoS campaigns are run like military campaigns with extensive up-front planning, a high degree of coordination, and contingency plans that perpetrate or adjust attacks based on the success of the initial response effort. Extensive research done prior to attacks identifies multiple targets and their unique weaknesses. Feedback loops are used to monitor when a site goes down, indicating when a second round or next phase of attack should begin, and to chart progress until sites become unavailable or the ultimate goal is achieved.

Finally, attacks continue to increase in speed as well as complexity. As new vulnerabilities are introduced, new modules can be found within Metasploit and other frameworks by the next day. Internet repositories are updated overnight so that new attack types can be added by simply updating repositories online.

So What Can Be Done About It?

All companies – financial, retail, medical, and utility companies in particular – must account for how well they do or do not protect customer data, and how quickly and appropriately they respond to catastrophic events. Distinct, often compound defenses are required for each of the attacks described above, though some elements and “best practices” deliver essential value across the board.

Step II. Defending in Kind

The more attacks become complex and multi-dimensional, the more defenses must become strategic, proactive, and distributed. New and traditional approaches can be leveraged effectively in tandem:

- **Customer premises solutions** such as firewalls, web application firewalls, on-premises DDoS, and IPS/IDS help safeguard availability and combat volumetric attacks. Hybrid application firewalls feature built-in anti-denial-of-service capabilities that can also thwart application-based attacks such as Slowloris, Apache Killer, and attempts to take down search engines and shopping carts. Dedicated premises-based DDoS solutions also exist that can handle some filtering and cleaning.

  Web application firewalls may be compromised as traffic volumes impact their ability to process rules effectively. For example, as traffic from DDoS attacks clogs the pipes, defending devices may begin removing rules in order to maintain CPU, thus opening the door to SQL injections.

- **Content delivery and carrier services** can use proxies and content delivery networks (CDNs) to serve as front-ends to enterprise web properties. Traffic may further be diverted to “scrubbing centers” as volumetric attacks spiral out of control.
• **Cloud-hosted DDoS services** may prove crucial during high-bandwidth network attacks, distributing the workload to scrub and protect customer pipes very quickly.

• **Dedicated anti-DoS services** allow traffic to be routed to scrubbing centers where bad traffic is removed and legitimate traffic forwarded with minimal delay.

The bottom line: even more important than having multiple anti-DDoS options available, enterprises must increasingly have a strategic, proactive, proven security process in place, along with a dependable means of evolving it into the future.

Without the proper process and near-instant response, all the technology in the world won’t shut down an attack in time to save a business grief. The process must be broken down into three equally critical stages to address what happens before, during and following a successful attack:

- **Before:** The first steps, obviously, are being prepared with up-to-date threat databases and being able to detect and correctly identify attacks as soon as they happen. It must be determined—in advance—whether both in-house and external defenses are solid enough to withstand live attacks.

- **During:** While the war is on, it’s all about mobilizing highly skilled and well-prepared response teams that are able to maintain or restore availability as quickly as possible.

- **After:** In the wake of attack, efforts must be made to remediate the damage—financial loss, customer distrust, etc. From there, a forensic “audit” of failed systems and procedures must take place to identify and eliminate points of vulnerability going forward.

This lifecycle represents an ongoing process: a living, breathing thing that must constantly be evaluated and updated to keep pace with mounting threat complexity. Savvy IT teams need to consider everything from which people on which teams must be involved, to what and how to communicate with customers, and whether or not to involve law enforcement. They must work with ISP and other service providers to determine the optimal point at which to switch from on-premises DDoS solutions performing deep L7 inspection and basic DDoS at L4 to costly, high-volume, cloud-based scrubbing services that can quickly distribute the workload.

**Step III: Evolving Best Practices for Mitigating DDoS Attacks**

Practice makes perfect. The only way to know whether an enterprise or service provider’s strategies and procedures can meet the challenge of real-world threat environments is to put them to the test and use the results to refine security infrastructures and procedures. Of course, the ideal is to do this without compromising actual sites and systems and running the risk of bringing business to a halt.
Modern best practices call for the simulation of threats in a controlled manner, with precise measurement and the ability to pinpoint weak links in the chain. This process of testing and assessing internal mechanisms and third-party remediation services includes:

- **Generating sophisticated attacks**: Simply levying basic SYN flood attacks at a website won’t reveal its overall susceptibility to SQL injections. Volumetric attacks must be run then followed by subsequent, more sophisticated and targeted attacks to evaluate how well the infrastructure reacted.

- **Dynamically adding and removing filtering steps**: To anticipate high-orbit app cannon attacks, obtaining the configuration file called to see how the attack is run proves useful in building rules to defend against it.

- **Testing to scale**: A false positive rate of 1% may seem acceptable at a low volume, but might overwhelm an analysis team during a DDoS attack. Worst-case scenarios must be explored to ensure preparedness.

- **Testing logging functionality under attack conditions**: Attacks are inevitable and logging plays a crucial role that must be protected in advance.

- **Creating a staged network**: You need way to test without putting the performance of the production network at risk. Maintaining a test network also allows the quality and impact of new products, services, and releases to be evaluated prior to investment and deployment in live networks.

**Ixia BreakingPoint: Keeping One Step Ahead**

Ixia BreakingPoint security assessment solutions and professional services equip enterprises to create diverse security events that evaluate and help optimize their corporate defenses. BreakingPoint delivers the industry’s only means of creating real-world scenarios combining valid application traffic and batteries of volumetric and application-layer attack traffic. This ability to generate good and bad traffic from a highly efficient, integrated solution enables a new dimension and caliber of security assessment to be conducted on an ongoing basis.

Users can launch a wide range of multi-faceted attacks including layered DDoS and application-layer attacks, stateless, and remote exploits in a phased and controlled fashion.

Users can launch a wide range of multi-faceted attacks including layered DDoS and application-layer attacks, stateless, and remote exploits in a phased and controlled fashion. For example, after a certain amount of time following the launch of a network attack, application layer attacks may get going, followed by stateless and remote attacks. Attacks can be generated from subnets representing multiple locations to achieve coordinated attacks, and can scale to more than 600 gigabytes per second.

More importantly, the Ixia BreakingPoint solution allows those refining defense strategies to work in the same manner as those engineering new threats, trying lots of things all at once versus one at a time, and responding dynamically as each approach succeeds or fails. Users quickly see the entire landscape—how successful the DDoS attempt was, how successful real users continued to be, etc.—launching complex attacks from a simple-to-use GUI and netting actionable insight from easy-to-read reports.
With the pinpoint knowledge gained using Ixia BreakingPoint to assess network and application performance and workflow responses to DDoS attacks, IT departments can make meaningful adjustments and corrections to improve company defenses. But they can’t stop there...

### Comprehensive DDoS Testing

**Establish baseline background traffic**
- Enterprise APP profile
- Data center APP profile
- Mobile subscribers APP profile

**IP-based DoS attack types**
- ICMP flood test case
- ICMP fragmentation test case
- Ping flood test case

**UDP-based DoS attack types**
- UDP flood test case
- UDP fragmentation test case
- Non-spoofed UDP flood test case

**TCP-based DoS attack types**
- Syn flood test case
- Syn-ack flood test case
- Data ack and push flood test case
- Fragmented ack test case
- Session attack test case

**Application-layer attack types**
- DNS flood attack case
- Excessive verb attack case
- Recursive GET Floods
- Slow POSTs
Then What?

At some point, all attacks end. When they do, those responsible for security must conduct a detailed analysis of what actually took place – for example, did the system fail open or fail closed – where the infrastructure stands, and what steps must be taken to prevent a recurrence. These questions can only be answered by running the types of tests described above.

Critical risk management also includes having a process in place for modeling and quantifying the impact of future changes to the network on an ongoing basis. While evaluations can be commissioned or performed when evaluating new devices and services, the more powerful, “best practice” use of security testing actually places an enterprise in the safest, most-efficient and competitive position for the long haul.

Ixia BreakingPoint solutions help security strategists fine-tune defenses from product selection and infrastructure design to assessing upgrades and modeling potential threats to assess readiness. Evaluating DDoS responses and preparedness as security environments evolve minimizes risk over time and keeps organizations up to date and able to launch powerful, real-time responses to today’s ever more complex and powerful attacks.
This material is for informational purposes only and subject to change without notice. It describes Ixia’s present plans to develop and make available to its customers certain products, features, and functionality. Ixia is only obligated to provide those deliverables specifically included in a written agreement between Ixia and the customer.