**White Paper**

Mike Jack, Sr. Product Marketing Manager
Spirent Security Solutions

# Hardening Security Defenses Against Tomorrow's DDoS Attacks

## Executive Summary

Today, Distributed Denial of Service (DDoS) attacks are every network's problem. Powerful computing platforms, high bandwidth connections, low-cost hardware, global reach, and the easy availability of "how-to" toolkits for conducting DDoS attacks make wreaking havoc easy.

DDoS attacks are already more diverse than in the past—and they change constantly. For the enterprise, this knowledge is worrisome. But there are ways to preempt attacks and know in advance how your infrastructure will function in a DDoS attack.

This paper discusses current DDoS attack methodologies, providing examples, to give you insight into how your enterprise might be vulnerable, and describes steps you can take to harden defenses through preemptive security testing and measuring techniques.

## DDoS Attacks—An Inescapable Reality

In early 2019, DDoS attacks made headlines around the world with the largest ever recorded attack that peaked at over 80 million packets per second was recorded. Today DDoS attacks include more targets become larger, more diverse, potentially more dangerous, and significantly more costly.

Numerous types of cyber attacks, including phishing, use of spyware, hijacked accounts, and data leaks were initiated to influence elections in several countries. DDoS-style attacks occurred in the United Kingdom and Australia. In the United Kingdom, the voter registration website (Gov.uk/register-to-vote) experienced a service outage when it was flooded with requests just a few hours before the registration deadline. As a result, the government extended registration for another two days, which could have significantly shifted voter demographics through social manipulation.[1] In the USA, Hackers have launched distributed denial-of-service attacks against at least two municipal-level Democratic campaigns in 2018.[2]

Q1 of 2019 has seen a 967% increase in major DDoS attacks where over 77% of DDoS attacks sized 100Gbps and higher were targeting two or more vectors. While the largest DDoS attacks experienced the most growth, smaller attacks also increased exponentially. In the past, such attacks have limited access to or incapacitated multiple websites, including Twitter, Amazon, Spotify, Tumblr, Reddit, PayPal, Ticketmaster, HSBC, BankWest, and Netflix.[3]

As recently as late 2018, DDoS attacks have continued to target a myriad of different websites. A popular online code management service used by millions of developers, GitHub is used to high traffic and usage. What it wasn't prepared for was the record breaking 1.3 Tbps of traffic that flooded its servers with 126.9 million packets of data each second. The attack was the biggest recorded DDoS attack, but amazingly the onslaught only took GitHub's systems down for about 20 minutes. This was largely due to the fact that GitHub utilized a DDoS protection service that detected the attack and quickly took steps to minimize the impact. Later that year, politically motived attackers targeted a Portland, Oregon cloud computing company with DDoS attacks that crashed the French news websites Le Monde and Le Figaro.[4] June saw DDoS attacks on Qatar-based news network Al Jazeera's websites and internal systems.[5] And in the U.S., a botnet generated a DDoS attack against the Federal Communications Commission's website, temporarily disabling it.

## Costly Chaos

Early DDoS attacks were typically used to showcase the perpetrator's ability to disrupt service and create chaos. The attacks evolved into protest mechanisms and are now used to extort money, manipulate currency rates, and intimidate. For example, when Bitfinex, the world's largest Bitcoin exchange, began trading IOTA crypto currency tokens in June 2017, it was hit by a DDoS attack that many experts believe was motivated by a desire to manipulate exchange rates.[6]

As another example, in late June, a group calling itself the "Armada Collective" threatened seven South Korean banks with DDoS attacks if they did not each pay ransoms of $315,000. The Armada Collective apparently was emboldened by the $1 million ransom payment made by a South Korean web hosting company a week earlier to avoid DDoS attacks.[7]

[1] *"Cyber Attacks on French Election," Radware, April 21, 2017, www.radware.com.*

[2] *https://www.cyberscoop.com/ddos-democratic-campaigns-primary-dnc-dccc/*

[3] *https://www.techrepublic.com/article/major-ddos-attacks-increased-967-this-year/*

[4] *Nick Ismail, "Major French news sites victim of DDoS attack," Information Age, May 11, 2017, http://www.information-age.com/major-french-news-sites-victim-ddos-attack-123466206.*

[5] *John Leydon, "DDoS attack brings Qatar's Al Jazeera website to its knees," The Register, June 9, 2017, https://www.theregister.co.uk/2017/06/09/al_jazeera_battered_by_ddos_attack/.*

[6] *Phil Muncaster, "World's Largest Bitcoin Exchange Bitfinex Crippled by DDoS, InfoSecurity," June 15, 2017, https://www.infosecurity-magazine.com/news/worlds-largest-bitcoin-exchange.*

[7] *Catalan Cimpanu, "$1 Million Ransomware Payment Has Spurred New DDoS-for-Bitcoin Attacks," Bleeping Computer, June 26, 2017, https://www.bleepingcomputer.com/news/security/-1-million-ransomware-payment-has-spurred-new-ddos-for-bitcoin-attacks/.*

## Why DDoS Attacks Are Increasing

It's relatively easy and inexpensive for a bad actor to create chaos or extort money using DDoS attacks.[8]

### IoT Devices are Everywhere and Not Secured

All network-connected devices, such as video surveillance cameras, webcams, baby monitors, home routers—even TVs and refrigerators—have IP addresses and usually lack robust protection against security vulnerabilities and cyber attacks. By injecting code into a single webcam, an attacker can broadcast a highly distributed attack as the malicious code propagates to other vulnerable devices. The Mirai botnet included millions of IoT devices around the world. With more than 6.4 billion IoT devices currently connected and an additional 20 billion devices expected to be online by 2020, the IoT botnet business is booming.[9] Additionally, source code for the Mirai attack is opening available for anyone to study, analyze and potentially use for a future attack.

### Botnets Sold or Rented on the Dark Web

Want to launch a DDoS attack? Get out your bitcoin wallet—botnets are readily available. On the dark net, you can find a botnet vendor, decide how many you want to purchase or rent, determine how long you'll need them, and specify the country (or countries) in which you want them to reside. Prices range from 25¢ to $1 per host, with minimum orders of around 50-100.

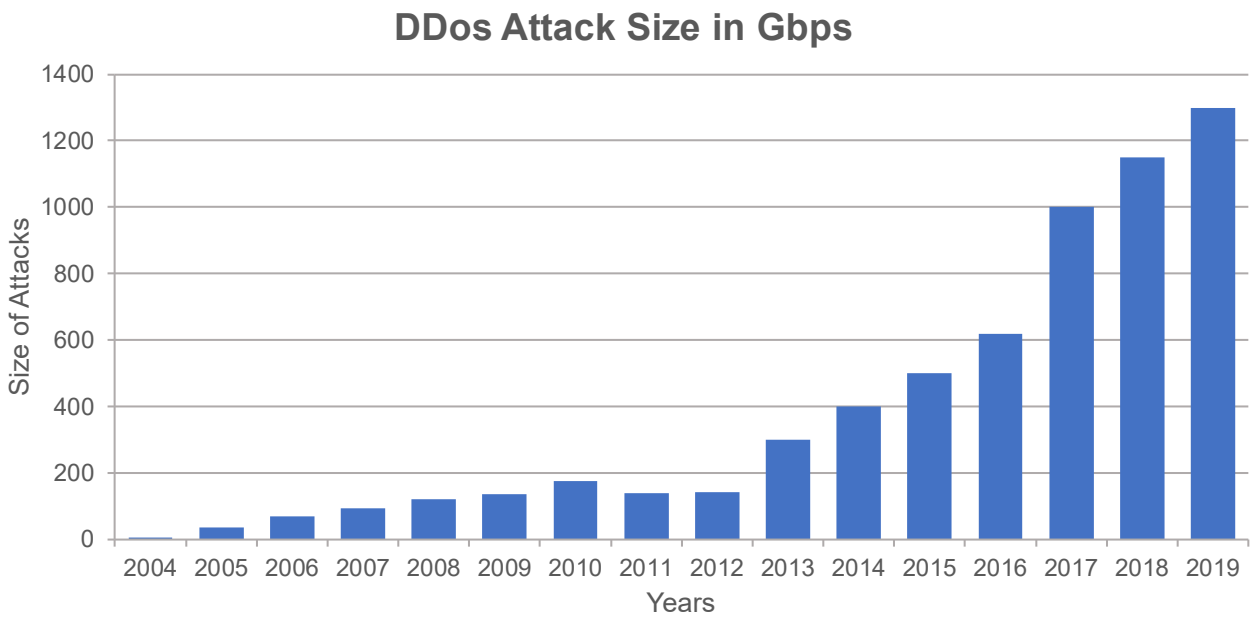
You can also buy IoT botnet stressers to use for service periods ranging from a day to several months. Stressers allow you to launch a limited number of attacks per day with a guaranteed minimum duration ranging from a few minutes to a few hours.

Botnet purveyors trade in crypto currency to evade payment trails. As long as crypto currency maintains value, the dark web economy will thrive.[10]

[8] *"The Cost of a DDoS Attack on the Darknet," Radware blog, March 15, 2017, https://blog.radware.com/security/2017/03/cost-of-ddos-attack-darknet.*

[9] *Ibid.*

[10] *Radware blog, March 15, 2017, op cit.*




## Preparedness: The Next Best Thing to Immunity

No enterprise is immune to DDoS attacks, but the next best step is preparedness. If your organization hasn't yet experienced a DDoS attack, it's only a matter of time. You can take three fundamental steps to harden defenses against DDoS attacks:

1. Become aware of the current DDoS landscape
2. Understand how DDoS attacks work
3. Recognize the challenges involved in creating a defense strategy

## Survey the DDoS Landscape

If you have experienced a DDoS attack, you're not alone. Even if you haven't, there's little comfort in findings indicating that you probably will. Web analytics firm Akamai surveyed 1,010 enterprises in early 2019 and issued their results in May. According to Neustar's Worldwide DDoS Attacks & Cyber Insights Research Report:

- A total of 849 organizations had experienced at least one DDoS attack in the previous 12 months, representing 84% of the organizations surveyed and an 11% increase (from 73%) in 2016.
- A total of 86% of the organizations surveyed had experienced multiple DDoS attacks.
- Of the organizations experiencing multiple attacks, 63% said that revenue losses at peak time could exceed $100,000 per hour, while 43% said financial losses per hour were actually closer to $250,000.
- Survey respondents had lost more than $2.2 billion collectively in the previous 12 months, a minimum of $2.5 million for each of the 849 organizations experiencing attacks.[11]

Neustar found that 45% of DDoS attacks were stronger than 10Gbps, and 15% reached at least 50Gbps—almost double the rates reported in 2016. In addition to using IoT devices to carry out attacks, attackers employed a variety of new techniques, such as Generic Routing Encapsulation (GRE)-based flooding and Connectionless Lightweight Directory Access Protocol (CLDAP) reflection.[12] These findings suggest that enterprises recognize the probability that one or more DDoS attacks on their organizations will occur and that DDoS attacks will continue to increase and diversify.

[11] *2019 State of the Internet/ Security: Credential Stuffing - Attacks and Economies, Apr, 2019*

[12] *Ibid.*

## Understand How DDoS Attacks Work

DDoS attacks are designed to make an online service unavailable by overwhelming it with traffic from multiple sources. Stopping DDoS attacks is more difficult than stopping other types of cyber attacks. There are different types of DDoS attacks, and each must be addressed in a different way. The three most common types are:[13]

- **Volumetric attacks.** These attacks saturate an organization's bandwidth with massive amounts of traffic. They are measured in bits per second and are commonly known as UDP Flood, TCP Flood, or Amplification attacks.
- **Protocol attacks.** These attacks exploit weaknesses in the Layer 3 or Layer 4 protocol stack. They consume all of the processing power of the target or of devices like firewalls. Syn Flood and Ping of Death are this type of attack.
- **Application attacks.** These are the most sophisticated types of DDoS attack and the hardest to identify and mitigate as they appear like legitimate user sessions. They establish a connection with a system and then monopolize processes and transactions, causing system crashes. In many cases application attacks do not require large volumes of traffic to cause system failures. HTTP Flood and DNS attacks are examples of application attacks.

Hackers stay ahead of the curve, continuously looking for new vulnerabilities and coming up with new techniques. They might use a DDoS attack as a smokescreen to divert attention and resources from a second location being compromised through other malicious methods. Not only can Botnets overwhelm networks, they can establish command-and-control presence for executing code, self propagation and exfiltrating data.

For these reasons, an enterprise can be affected by DDoS attacks through means that are completely unrelated to its business. One such example is a s a late 2019 DDoS attack on the Swedish Democratic Party's website at the end of August. Later that year, a mass attack targeting D-Link routers was launched when an attacker used Mirai malware to hijack routers, surveillance cameras, and baby monitors in a major DDoS attack.

## Recognizing the Challenges When Formulating a Defense Strategy

DDoS attacks create tremendous challenges for an enterprise. For example, you need to balance protection against DDoS attacks with enterprise network access and performance requirements. The ideal balance is different for different enterprises. In addition, enterprise IT and security teams already have their hands full. The ability to add new security measures and policies is often limited by available resources and budgets. Developing the most effective and achievable defense requires you to identify and prioritize the potential chokepoints that are the most vulnerable to a DDoS attack.

## Hardening Security Defenses

Since immunity from DDoS attacks is not an option, the best defense is to take a proactive, preemptive stance. Start to build protection into future products or services by incorporating security measures into your development processes. In the meantime, take the following steps to harden your defenses against DDoS attacks.

## Think Holistically and Be Proactive

First, think holistically and proactively. DDoS attacks typically affect multiple points in a network. Enterprises must decide which processes, paths, applications, and users are absolutely mission-critical for enterprise performance. Identifying mission-critical points will help determine the balance between optimal amounts of protection and access in order to simplify decision-making and prioritize actions.

[13] *Archana Kesavan, "Three Types of DDoS Attacks," Thousand Eyes blog, November 15, 2016, https://securelist.com/ddos-report-in-q3-2018/88617/.*

## Fix What You Can—Now

One of the most important measures for hardening defenses against DDoS attacks is to make certain that enterprise networks and systems are not running on manufacturers' default configurations or security measures. Use of default configurations is one of the most common—and preventable—vulnerabilities. Next, take advantage of next-generation firewall capabilities for DDoS mitigation. If firewalls or other security infrastructure components are due for a refresh, replace them with solutions that provide DDoS mitigation.

## Call the Experts

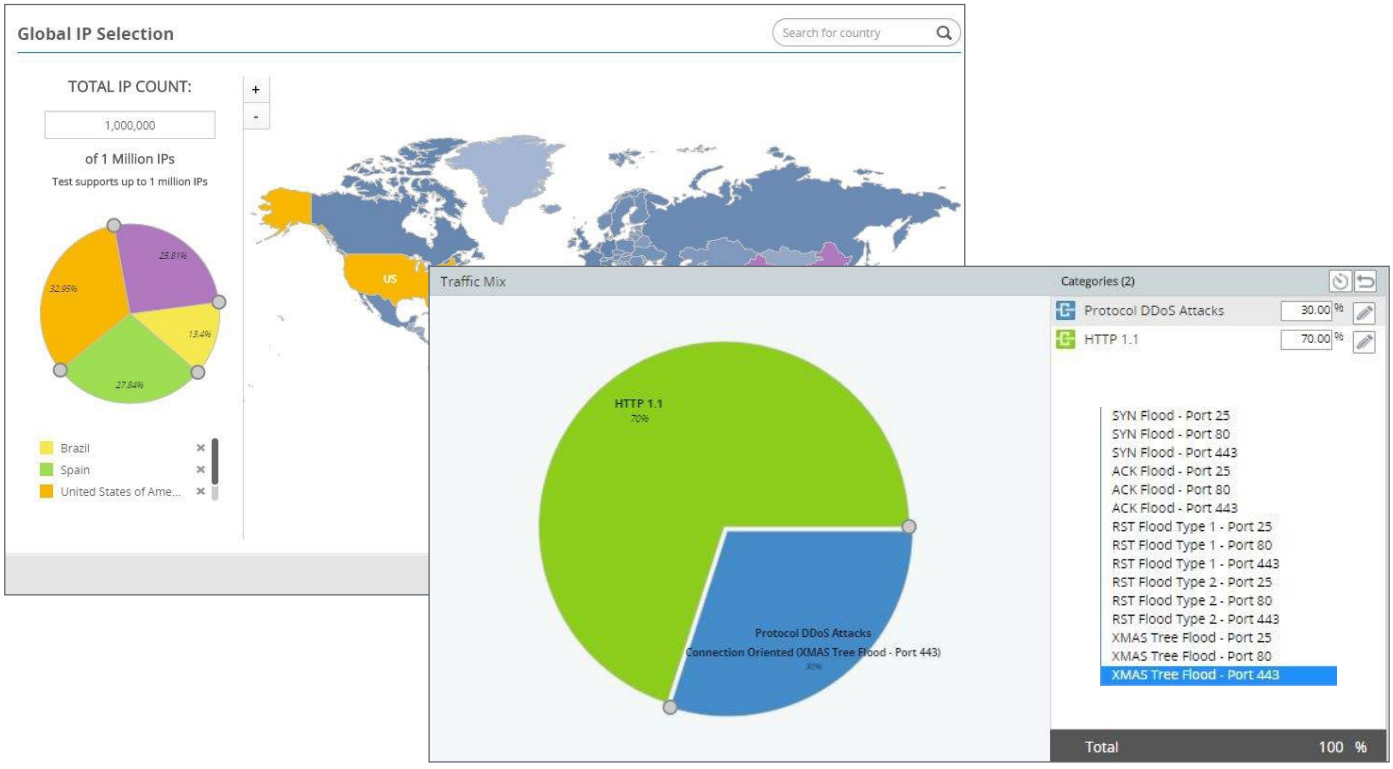
Consult DDoS protection experts for advice and resources. Look for experience in devising and validating DDoS mitigation strategies against volumetric, protocol, and application attack types. In addition, seek out testing expertise that delivers realistic results about the impact of a DDoS attack in your environment.

For example, Spirent uses its CyberFlood solution to combine legitimate and normal traffic with DDoS attack traffic in emulating a real-world DDoS attack on a test network. CyberFlood provides real-time statistics that enable you to measure user experience and security mitigation simultaneously, so that you know exactly how your security infrastructure is performing.

## Test, Test, Test

Test preemptively—and regularly. Preemptive testing helps ensure that your infrastructure performs as expected in case of a DDoS attack. Repeat preemptive testing every six months, or when major infrastructure changes occur, to continue to match defenses to current DDoS threats.

**Create Comprehensive tests with global IP sources, mixed attack and normal user traffic**



**About Spirent Communications**

Spirent Communications (LSE: SPT) is a global leader with deep expertise and decades of experience in testing, assurance, analytics and security, serving developers, service providers, and enterprise networks.

We help bring clarity to increasingly complex technological and business challenges.

Spirent's customers have made a promise to their customers to deliver superior performance. Spirent assures that those promises are fulfilled.

For more information, visit: www.spirent.com

## Begin Today

Understanding the current DDoS attack landscape and gaining insight into potential vulnerabilities can go a long way toward successfully mitigating a DDoS attack. Knowing that you're not alone—that experts in DDoS testing and mitigation are able to assist in hardening your defenses—is empowering. Let Spirent help you preempt DDoS attackers and minimize risk.

spirent™
Promise. Assured.

**Contact Us**

For more information, call your Spirent sales representative or visit us on the web at www.spirent.com/ContactSpirent.

**www.spirent.com**



Americas 1-800-SPIRENT
+1-800-774-7368 | sales@spirent.com

Europe and the Middle East
+44 (0) 1293 767979 | emeainfo@spirent.com

Asia and the Pacific
+86-10-8518-2539 | salesasia@spirent.com

Rev C | 05/19