10 Facts You Should Know About DDoS

DDoS (distributed denial of service) attacks pose some of the biggest cybersecurity threats to organizations today.

Due to their distributed nature, they are difficult to defend against, causing website and network disruption for organizations large and small. Here are 10 things you should know about DDoS attacks and how you can address them.

1. They're more common than you think

Cybercrimes are on the rise and DDoS attacks are among the most common. Almost half of all companies today have been victims of DDoS attacks, bringing business to a grinding halt—particularly organizations such as online retailers and banks that have a heavy web services component or depend on internal network services. DDoS attacks grew by 20% in 2020 to 10 million due to Covid and remote work.[1] And, it's continuing to grow in terms of scope, frequency, and complexity, making them harder and harder to fend off. If your company hasn't already been under attack, it could just be a matter of time.

2. Cybercriminals are everywhere

DDoS perpetrators are not a specialized breed. They can be university-educated or homegrown. They can reside overseas or in your own backyard. Hackers can come from anywhere. In terms of the cybercrime landscape, DDoS attacks are relatively simple to carry out and don't require specialized training. Anyone with malicious intent can purchase attack toolkits on the web for an affordable price. Whether the motivation is political, social, geographical, financial, competitive, or downright destructive, anyone, anywhere can coordinate an attack if he or she wants to. You need to be prepared.

3. They don't just target big companies

Although we tend to hear about large organizations that have been victims of DDoS attacks, smaller, lesser-known companies can be just as vulnerable. They may not have the enormous customer base that makes attractive target, but smaller companies tend to have less rigorous security. In fact, 43 percent of cyber-attacks target small business.[2] While major online industries such as financial services, online gaming, entertainment, news, and retail have typically been the most vulnerable, perpetrators will target any organization with a significant web presence.

[1] https://www.infosecurity-magazine.com/news/ddos-surge-202-covid/

[2] Verizon 2019 Data Breach Investigations Report link: https://enterprise.verizon.com/resources/reports/

4. Lightening can strike twice

Just because you've been hit once does not mean you won't be hit again. Like homes that are broken into multiple times, vulnerable organizations are not immune from multiple DDoS attacks. The bigger the potential damage, the more likely companies are susceptible to multiple attacks.

5. DDoS is not typically detected until it's too late

Because many companies fall short of deploying the correct DDoS tools, on average, DDoS attacks are not usually detected until 4.5 hours after they start. It takes another 4.9 hours before mitigation can begin. That means most companies under attack have already suffered irreparable damage, even before they realize it.

Because DDoS attacks can involve forging hundreds of thousands of IP sender addresses, it is not always easy to identify the location of attacking machines. To ward off attacks, you need a solution that can react within seconds, not minutes.

6. Bottom line impact

DDoS attacks are not just a nuisance; they can cripple your bottom line. According to Juniper Research, the average cost of a data breach will exceed $150 million by 2020. Attacks result in lost worker output, potential penalties for non-compliance, which can be costly, and revenue loss from customer defection. Sometimes attackers demand a ransom from site owners, which only adds to financial losses.

7. DDoS acts as "Smokescreen"

Most DDoS attacks do not attempt to breach a company's network, but rather overwhelm it with traffic so it comes to a halt. Increasingly, these attacks are used as "smokescreens" to distract from the real intent—data breaches—which is far more damaging than a website going down. DDoS attacks are extremely disruptive and distracting for the security operations teams, but more importantly, they allow other behavior such as reconnaissance and compromise attempts to fly under the radar. By launching a significant DDoS attack, a hacker stands a much better chance of breaking into your systems or exfiltrating sensitive data undetected.

8. Damage to customer trust

DDoS attacks do not only hurt brands financially, they damage your reputation and even more importantly, undermine customer trust. Customers realize that if you can't keep their personal data safe from hackers, they'll have to turn to someone who can. It takes less than a second to lose a customer, and bad press is viral. These days, a DDoS attack is more than just a public embarrassment—it can permanently damage your reputation and your customer relationships.

9. DDoS attack are always evolving

As organized attacks become more sophisticated and effective, companies need to become more savvy about how to protect themselves and their assets. Organizations are more vulnerable than they may realize with multiple entry points that are their achilles heels. Unsecure Internet of Things (IoT) devices—heating and cooling systems, printers, thermostats, video-conferencing, even vending machines—are some of the most vulnerable assets. Companies need to stay one-step ahead of cybercriminals as they continue to get smarter and more strategic.

10. You don't have to be defenseless

Organizations with significant web presences cannot sustain DDoS attacks without repercussions to their brand and bottom line. You need to determine the risk of a potential attack and identify what you need to protect. Ideally, you need a solution that will allow you to detect anomalies in network patterns in real time and alert on unusually high levels of incoming connections from one or more sources. To be secure, you need to provision your system for a one-terabit attack.

In addition to defending your own organization from a DDoS attack, it is also important that you behave like a "good Internet neighbor." By deploying a proper security visibility solution, you can detect whether your systems are being used to launch DDoS attacks against other victims and take responsibility by shutting down a DDoS attack at its source.

Riverbed Advance Security Module

Riverbed® NetProfiler with Advanced Security Module uses full-fidelity flow visibility to help you detect, investigate, and respond to threats that bypass your perimeter defenses. In one integrated solution, it delivers:

- **Active threat detection**: Leverage blacklists, anomaly detection, and threat feeds to actively detect and investigate cyber security attacks. Keep your networks and applications safe from internal and external threats

- **Stop DDoS in its tracks**: Fast, accurate DDoS identification and mitigation

- **Full-fidelity forensic recall**: Leverage Riverbed NPM's full-fidelity flow and packet data storage for threat hunting investigations into suspicious network behavior. Always have the data you need!

Learn More

To learn more about securing your network against DDoS and other cyber threats click here.

About Riverbed
Riverbed enables organizations to maximize performance and visibility for networks and applications, so they can overcome complexity and fully capitalize on their digital and cloud investments. The Riverbed Network and Application Performance Platform enables organizations to visualize, optimize, remediate and accelerate the performance of any network for any application. The platform addresses performance and visibility holistically with best-in-class WAN optimization, network performance management (NPM), application acceleration (including Office 365, SaaS, client and cloud acceleration), and enterprise-grade SD-WAN. Riverbed's 30,000+ customers include 99% of the *Fortune* 100. Learn more at riverbed.com.

riverbed®