How Does Your DDoS Protection Stack Up?

39%

of respondents indicated their existing firewalls, load-balancers were leveraged as part of a DDoS event

42%

of businesses surveyed in 2014 reported attack durations of over 6 hours (some as long as 4 weeks)

Source: *"Worldwide Infrastructure Security Report, Volume X,"* Arbor Networks, 2015

50%+

of respondents rank DDoS attacks as their number one concern for the coming year

Source: *"Worldwide Infrastructure Security Report, Volume X,"* Arbor Networks, 2015

Distributed Denial of Service (DDoS) attacks continue to grow in frequency, size, and sophistication. DDoS events are increasingly integrated components of advanced attack campaigns. New multi-vector DDoS campaigns combine volumetric, state-exhaustion and application layer techniques concurrently, aimed at the same target, to thwart mitigation and increase the attacker's chance of success.

And any business with Internet-facing applications is at risk. It no longer takes an expert, or even basic coding experience, to initiate significant DDoS attacks. The days of "it will never happen to me" are long gone.

Where do you stand in combatting DDoS? Best practices for DDoS protection cover far more than just technology. They include broader threat intelligence and awareness, incident response processes and enterprise-wide planning. You can find out how your DDoS protection stacks up with a simple self-assessment that will rate your security posture on 5 important aspects of DDoS protection:

1. BUSINESS CONTINUITY

What Role Does DDoS Protection Play in Planning?

Forty-two percent of businesses surveyed in 2014 reported attack durations of over 6 hours—some as long as 4 weeks.[1] If you were hit by a DDoS attack right now, do you have agreed upon processes in place across business functions? With your ISP? Or would you find yourself making hurried, under-the-gun decisions? Do you know what downtime would cost your organization? Not only in terms of revenue loss—but also indirect costs such as resources to mitigate, impact on other business initiatives, SLA credits, legal/regulatory fees, PR costs for brand repair, customer churn, etc. **Take the self-assessment ›**

2. ODDS OF BEING ATTACKED

How Much Do You Hedge Your Bets?

No other cyber threat is as easy to launch as DDoS—Low Orbit Ion Cannon (LOIC) is free open source code, and attack services can be hired for as little as $5 and an IP address. It's no surprise that nearly half of respondents surveyed in 2014 saw DDoS attacks. And significantly, over half rank DDoS as their number one concern for the coming year. And remember, you don't even have to be the direct target. If your services are hosted by a public service provider any attack that cripples that environment brings you down too. So you have to ask yourself, "Do I feel lucky?" **Take the self-assessment ›**

ARBOR® NETWORKS

50%

of businesses indicated they have experienced DDoS attacks targeting infrastrucutre such as firewalls, routers and load balancers

Source: *"Worldwide Infrastructure Security Report, Volume X,"* Arbor Networks, 2015

42%

of respondents saw multi-vector DDoS attacks (36 percent did not know)

3. MITIGATION SOLUTION

How Do You Stop DDoS Attacks?

Think your firewalls, Intrusion Protection Systems (IPS) or other on-premise solutions have you covered for DDoS? Think again. Nearly half of businesses surveyed in 2014 indicated they have experienced DDoS attacks actually targeting infrastructure such as firewalls, routers, and load balancers. And your Internet Service Provider? The proportion of respondents seeing attacks targeting cloud-based services has grown significantly, from 14 percent in 2012 to 29 percent in 2014. Where have you put your money? **Take the self-assessment ›**

4. DDOS & ADVANCED THREATS

Together or Apart?

Research has shown that DDoS has become more sophisticated, with multi-vector attack strategies, and can play an integral part of an advanced attack. In 2014, 42 percent of respondents reported seeing multi-vector DDoS attacks, and 36 percent did not know. More worrisome, DDoS is used as part of advanced attacks to test of your strengths (or weaknesses) during a reconnaissance stage; flooding logs and data files to obscure weaponization and malware delivery; and diverting attention during data exfiltration. Do you employ threat intelligence for DDoS protection? How proactively do you "hunt" for signs of compromise or breach before they impact your organization? **Take the self-assessment ›**

5. TEAM & PROCESS

Who's Responsible for What?

Only 18% of organizations surveyed in 2014 said they have an incident handling plan with a well-resourced team; 15% have neither a plan nor a team! Do you have an incident response procedure in place across business functions? Do you have a clear escalation and communication policy internally and with your ISP? 45% feel only somewhat prepared while an additional 10% feel completely unprepared. What about your organization—are you ready to rumble? **Take the self-assessment ›**

Essentially every business initiative in the modern enterprise, whether driven by sales, marketing, manufacturing, finance, R&D or HR, is dependent upon reliable network availability and continuity. Modern DDoS attacks can seriously impact not only revenue, but your ability to be productive and execute your business initiatives.

Sponsoring strong DDoS protection must be an enterprise-wide commitment—not just an IT problem. Taking this quick self-assessment will give you an idea of where you stand, and perhaps help clearly communicate to all stakeholders a real sense of urgency for prioritizing DDoS defense.

ARBOR NETWORKS

Corporate Headquarters
76 Blanchard Road
Burlington, MA 01803 USA
Toll Free USA +1 866 212 7267
T +1 781 362 4300

North America Sales
Toll Free +1 855 773 9200

Europe
T +44 207 127 8147

Asia Pacific
T +65 68096226

www.arbornetworks.com

SB/COMBATTINGDDoS/EN/0915-LETTER