Research Report | White Paper | neustar | CSO Strategic Marketing Services

DDoS Attacks No Longer Kids' Play

The eras of DDoS attacks being used by just prankers is over. Today, these are the most persistent cybersecurity threats.

When a large Domain Name System (DNS) services provider suffered a massive distributed denial-of-service (DDoS) attack last October, millions of people experienced internet service disruptions in North America and parts of Europe. The attack was also noteworthy because of its size: Peak traffic was clocked at 1.2 terabits per second—far larger than any previous DDoS attack on record. If that's not enough of a wake-up call, consider this: An attack of 10 gigabits per second can knock most organizations offline.

The era when DDoS attacks were used primarily by pranksters is over. DDoS attacks now rank among the most persistent cybersecurity threats. They are part of the arsenal regularly deployed by cyberattackers with criminal or political aims, as well as for extortion or competitive advantage. And the cadence of attacks is on the increase: Half of the respondents in a recent IDG survey of IT managers, for instance, report having suffered DDoS attacks on at least an occasional—or more frequent—basis.

Bad actors are not only able to launch increasingly potent DDoS attacks, but they also have unfettered access to tools of the trade—anyone can rent DDoS attack services from underground hacking forums for as little as $5. Conventional DDoS attacks involve the deployment of Transmission Control Protocol synchronize-based and DNS-based attacks. Other favored types of attack include User Datagram Protocol (UDP), Internet Control Message Protocol (ICMP), Simple Service Discovery Protocol (SSDP), and Network Time Protocol (NTP). DDoS attackers have also learned to marshal IoT botnets to exploit poorly secured devices to overwhelm networks with waves of traffic. What's more, cybercriminals have become increasingly savvy, carrying out DDoS attacks as distractions to keep incident response teams busy while they execute planned network infiltrations.

In the majority of incidents, victims of DDoS attacks also turn out to be victims of data theft or some other attack carried out simultaneously. Organizations must now contend with increasingly powerful and changing attack combinations. In fact, over 80% of the DDoS incidents that Neustar mitigated in the first quarter of 2017 involved multivector attacks.

IDG survey

50%

of the respondents of IT managers report having suffered DDoS attacks on at least an occasional—or more frequent—basis.

SOURCE: IDG

Attack mitigation

Despite the gathering threats, enterprises remain confident in their ability to mitigate the DDoS attacks that they manage to detect.

Only 4% of the respondents in the IDG survey report doing poorly at identifying DDoS attacks. About 39% characterize their success rate as very good, another 40% describe it as good, while 18% put it as fair. But at the same time, they still don't have a high level of confidence in any single solution or proverbial silver bullets. That's because there aren't any.

"The best approach relative to DDoS mitigation processes starts with assess, test, and plan."

– JOSEPH LOVELESS, NEUSTAR'S DIRECTOR OF SECURITY SOLUTIONS

DDoS detection remains difficult, and most organizations only investigate possible attacks after viewing spikes in activity levels, experiencing server performance slowdowns, or finding inconsistencies or anomalies in log data. Consider the fact that about 51% of the organizations surveyed globally by Neustar say they need at least three hours to detect an incident.

When Neustar studied the victims of DDoS attacks, regardless of who did the notifying, it went public very fast and detection by IT is slower than it should be to prevent customer impact. In a world where damage can occur in moments, that is an awful lot of risk to shoulder. Imagine what advantage that three-hour delay hands to attackers using DDoS as a distraction or a means of saturating a company's security management tools to carry out IP theft. Companies don't have much wiggle room because they are literally in a race against crime.

Multiple DDoS mitigation practices are in use, with companies reporting varying levels of success. Though organizations report the most success using IP filtering and analysis, no one approach stands out.

But security practitioners don't have the luxury of a silver bullet; there are literally hundreds of different kinds of attacks, plus new attacks and attack types surface constantly. When older attack types become ineffective, they get replaced quickly, putting added onus on organizations to stay on top of a continually shifting threat.

The idea that there's a single best approach to DDoS defense is misleading. All companies have individual requirements and investment capabilities and responses obviously will vary. But defending against DDoS attacks shouldn't come down to trial and error.

The mitigation processes involve a test, assess, and plan approach. A strong defense depends upon a thorough risk assessment that identifies an organization's relative vulnerabilities. Organizations should also view themselves as targets and perform tests to understand the tolerance of their infrastructure, particularly their hardware, to learn what it is capable of processing. Once they know their saturation points, they can determine their failover levels and decide whether or not they are structured adequately to handle the job by themselves.

Who handles the call?

Company size matters. The majority of organizations choose to handle the task of DDoS mitigation internally. But keep in mind that bigger organizations also have the resources to do things in-house, such as deep packet inspection or analyzing IP anomalies and rate limiting. That's a challenge for smaller and medium-size companies, and one reason why a sizable number—39% of survey respondents in the IDG survey—contract with a third party to take on one or more of these security-related jobs.

Outsourcing works: Organizations face a huge shortage finding qualified security professionals. The nonprofit information security advocacy group ISACA estimates a global shortage of 2 million cybersecurity professionals by 2019. Companies that use a third party for aspects of DDoS mitigation usually report better success rates, particularly when it comes to strategy creation, IP analysis, and rate limiting.

DDoS attack victims

40%

of the organizations found out about DDoS attacks only after being notified by service anomalies by their customers.

SOURCE: Neustar study

"If organizations are implementing defenses via trial and error, then they are doing something wrong and need to adjust."

– JOSEPH LOVELESS, NEUSTAR'S DIRECTOR OF SECURITY SOLUTIONS

Improvements Needed to Keep Pace with Modern DDoS Threats

SOURCE: IDG Research, 2017

Bridging strategic disconnects

When the character playing the infamous jail warden in the movie *Cool Hand Luke* noted a "failure to communicate," he could just as easily have been describing the gap separating IT from the business side when it comes to understanding DDoS and its implications for the enterprise.

DDoS is technical, complex subject matter. C-suite executives don't typically involve themselves with the intricacies of UDP floods and DNS amplification attacks. They care about risk, so DDoS is a topic that needs to get translated into the language of business without getting garbled by wading into deep technical waters.

Security managers need to better communicate to senior management how the attacks affect operations outside of IT, such as company call centers or customer service. For example, a five-hour DDoS attack translates into a two-week problem resolving customer issues. The impact of a successful DDoS attack carried out in conjunction with a malware infiltration can be devastating when you consider that estimated cost of the loss for a stolen customer record is now $158. Imagine an organization suddenly losing 20,000 customer records because a DDoS attack saturated its security management intrusion detection system.

ISACA estimates

a global shortage of

2 million

cybersecurity professionals by 2019

SOURCE: https://cybersecurity.isaca.org

Conclusion

Don't assume you won't get attacked. If you are online, you are a likely target and will not go unnoticed by attackers. Whether attackers want to target your infrastructure to disrupt, steal, or practice, dark days for the unprepared are coming. Underestimating the temptation that online organizations offer to attackers forfeits the protection initiative and reinforces vulnerabilities that can cost business big. Organizations should prepare for any contingencies by planning for DDoS mitigation with an approach of assess, test, and plan.

For more information on Neustar's solutions, **visit security.neustar**.