FLOWTRAQ

10 THINGS YOU MAY NOT KNOW ABOUT DDOS ATTACKS, BUT SHOULD

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 MAY THINK

Cybercrimes are on the rise and DDoS attacks are among the most common. Roughly 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. In 2014, DDoS attacks reached an average rate of 28 per hour[1] and continue 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. Basically, 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 or even a computer science degree. And for anyone with malicious intent, attack toolkits can be purchased 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. So you need to be prepared.

3. THEY DON'T JUST TARGET BIG COMPANIES

Though we tend to hear about the huge 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, which makes large organizations a desirable target, but smaller companies tend to have less rigorous security. 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] Preimesberger, Chris; "DDoS Attack Volume Escalates as New Methods Emerge." *eWeek*. May 28, 2014.

4. JUST BECAUSE YOU'VE BEEN HIT ONCE DOESN'T 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 to be susceptible to multiple attacks. In fact, more than 42% of the organizations monitored by one DDoS protection company were hit more than once, and 2.5% were attacked repeatedly over 10 times.[2]

5. THEY'RE NOT USUALLY DETECTED UNTIL IT'S TOO LATE

While most companies have invested in some type of cybersecurity solution, they often fall short of deploying the correct visibility tools to help them understand what's happening. Intrusion prevention systems like firewalls and routers cannot prevent DDoS attacks. Rather, they can actually exacerbate outages by causing traffic bottlenecks. On average, DDoS attacks aren't usually detected until 4.5 hours after they commence, and it takes another 4.9 hours before mitigation can begin.[3] 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, the location of attacking machines cannot be easily identified. To ward off attacks, you need a solution that can react within seconds, not minutes.

6. THEY HAVE A SIGNIFICANT IMPACT ON YOUR BOTTOM LINE

DDoS attacks are not just a nuisance, they can cripple your bottom line. 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. According to IDG, company downtime costs average $100,000 an hour which means DDoS attacks can cost you at least $1 million, even before you begin to mitigate the attack.[4]

7. THEY OFTEN SERVE AS "SMOKE SCREENS"

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 though, these attacks are being used as "smokescreens" to distract from the real intent — data breaches — which are far more damaging than the problems caused from 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. THEY CAN DAMAGE YOUR CUSTOMER TRUST

DDoS attacks don't 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.

---

[2] Kovacs, Eduard; "DDoS Attacks Shorter, Repeated Frequently in 1H 2014: Report." *Security Week*. Sept. 24, 2014.
[3] "A DDoS Attack Could Cost $1 Million Before Mitigation Even Starts." *Infosecurity*. Oct. 24, 2013.
[4] Ibid.

9. THEY'RE ALWAYS EVOLVING

As organized attacks become more sophisticated and effective, and networks and server capabilities grow, 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 — heating and cooling systems, printers, thermostats, videoconferencing, even vending machines. Companies need to stay one step ahead of these 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 be alerted to unusually high levels of incoming connections from one or more sources. And to be really secure, you need to provision your system for a one-terabit attack.

Besides defending your own organization from a DDoS attack, it's also important that you behave like a "good Internet neighbor." By deploying the proper visibility solutions that enable you to detect whether your systems are being used in a DDoS attack against another victim, you can take responsibility for helping to shut down a DDoS attack at its source.

These 10 tips provide a basic guideline for considering different security solutions for your organization. It's important to understand the potential threats first so you can make the right decision about how best to protect your employees, your company secrets and your valued customer relationships.

ABOUT FLOWTRAQ

FlowTraq provides software and services for high-performance network monitoring, analytics, security and forensics to detect a range of network behaviors, including distributed denial of service (DDoS), brute force attacks, botnets, worms, network scans and other network traffic anomalies. To request a free trial of FlowTraq, visit **www.flowtraq.com/trial**.

FLOWTRAQ

16 Cavendish Court, Lebanon, NH 03766
Phone +1 (603) 727-4477 | Email info@flowtraq.com