Distributed Denial of Service Attacks: What are They?

Distributed Denial of Service Attacks: What are They?

Distributed Denial of Service (DDoS) attacks occur when multiple systems flood the bandwidth of a company, typically through a web server. These types of attacks are more often than not a result of multiple compromised systems being used as botnets, that flood the target with traffic to overwhelm their environment. Imagine a town that only has one road as a way to reach it, if too many cars suddenly flood this road, the town has no way to receive visitors, and the town cannot operate effectively.

> “*Someone can bring companies to a crippling halt by DDoS attacks...*”

A Distributed Denial of Service attack is something that can affect every company these days even if their own procedures help guard against them. On February 28th, 2018, Github which is a popular platform for developers faced a sudden attack that clocked in at 1.35 terabits per second. This was record-breaking traffic with the last big attack being the Occupy Central Hong Kong Attack that reached 500 GBPS. This means that the Github DDoS attack caused more than double the traffic that the world had seen from any DDoS attack. While Github was prepared for DDoS attacks as many internet companies are these days, Github had no way of knowing an attack they would launch this massive against them.

What could these attacks cost?

Someone can bring companies to a crippling halt by DDoS attacks, while larger companies have the ability to bounce back with large reserves of cash flow, smaller businesses are not so lucky.

In 2017 the average DDoS attack cost for businesses rose to over 2.5 million dollars (a), these attacks, however, were small attacks compared to the Github attack with the average attack strength being only around 10 GBPS. In 2014 the internet firm Code Spaces when out of business because of a DDoS extortion attack. Code Spaces, which was a company that provided services akin to Github, discovered that this attack had occurred far too late.

What or who is to blame?

With millions of IoT devices accessing the network daily, from thermostats to smart outlets to refrigerators, it is critical that everyone keeps these devices secure so that they cannot be leveraged in a DDoS attack. These smart-devices rarely possess any security that keeps them from being breached, as they are designed for innovation and not safeguarding against malware.

This issue is compounded by the fact that many users never change their devices from having default user names and passwords for their admin consoles.

This makes these devices prime targets for hackers to leverage to use in these large DDoS attacks. This is where companies can use IoT security such as Fortinet, and Gemalto to help secure these devices and ensure that their systems are not only kept safe from compromise but not used in DDoS attacks against other companies.

IoT is not the only culprit here, as it has become quite easy for bad actors to build, or rent, the botnets needed for these attacks. Once upon a time creating a botnet required months if not years of planning and work, now there are bot-net for hire services that allow attackers to purchase time from other attackers to leverage in their attack. The more an attacker is willing to pay, the longer and more robust the attack launched against a company. What compounds this issue is that more often than not DDoS attacks are being used as a distraction in order for attackers to gain access to a system while security departments are scrambling to put out the DDoS "fire".

Guarding against DDoS

There are fortunately ways to guard against these DDoS attacks, both proactive and reactive ways to ensure that a company is not caught unawares. In a technical article written in 2018, Ahmad Nassiri points out 3 detection methods that you can use to help get ahead of DDoS attacks. (b)

Flow Sampling: In flow sampling, the router samples packets and then exports a datagram that contains information about those packets. Nearly all routers support this type of technology, plus it's highly scalable, making it a popular choice. However, this method only gives you a limited snapshot of your traffic and doesn't allow for detailed analysis.

Packet Analysis: When a high-performance DDoS mitigation device is deployed in-path, it can instantly detect and mitigate anomalies. This type of device continuously processing all incoming traffic and can also process all outgoing traffic—this is known as asymmetric and symmetric processing, respectively.

Mirrored Data Packets: Although mirrored data packets don't operate in the path of traffic, they provide the full detail for in-depth analysis, and can detect anomalies quickly. The only downside to this method is that it can be difficult to scale up.

The Future:

The development of faster and stronger DDoS attacks continues to loom over us all with more IoT devices being developed every day and the ease of hiring botnet services. The sharp increase of traffic being used in these attacks is even more terrifying. The next attack, should this trend continue, may end up being one that cripples a large company, or even the internet.

> *"The next attack, should this trend continue, may end up being one that cripples a large company, or even the internet."*

References

(a) Osborne, Charlie. "The Average DDoS Attack Cost for Businesses Rises to over $2.5 Million." ZDNet, ZDNet, 2 May 2017, www.zdnet.com/article/the-average-ddos-attack-cost-for-businesses-rises-to-over-2-5m/.

(b) NassiriAug, Ahmad, et al. "5 Most Famous DDoS Attacks." A10 Networks, www.a10networks.com/resources/articles/5-most-famous-ddos-attacks.