Mitigating Modern DDoS Attacks – The Missing Link

The world recently witnessed a massive improvement in the sophistication of the damaging DDoS attacks that hackers are launching. Hackers continuously study DDoS protection limitations, and they are increasingly aware of one major evident deficiency, that DDoS protection solutions are practically focused on responding to an attack only after an attack has been detected.

The market got used to this obvious deficiency since it was impractical to evaluate DDoS protection levels continuously in peaceful times. A customary defense strategy would naturally, on a continuous basis, gather detailed intelligence about existing weaknesses, and then continuously strengthen defenses against them, before becoming vulnerable to a damaging attack.

Unfortunately, this is not happening in the DDoS protection world.

Today's hackers are utilizing these known deficiencies in various ways:

1) **Low and Slow,** the attack focuses on loading the service, but does not trigger the mitigation system thresholds, creating a set of different attacks that together slow services down, take a long time to detect, and cause the response team's focus to be distracted.

2) **Multi-Vector Attacks,** use a complex mix of different attack vectors to a variety of targets, making it much more complex for mitigation systems and services to focus on what's going on, and what to block first. This strategy successfully achieves longer downtime before attack detection and mitigation.

3) **Time to Mitigation,** stems from the realization that in many cases, DDoS protection systems have an intrinsic minimum response time required to detect malicious DDoS traffic, and that mitigating the attack requires even more time. Hackers abuse this particular deficiency by changing attack tactics (vectors and target combinations) in a time frame shorter than the protection system's response time, avoiding triggering the mitigation system. A series of such short attacks will easily cause damage to the target network services.

A recent example of a complex attack that took down a major part of government services in Belgium is the attack on BelNet:
https://www.zdnet.com/article/this-massive-ddos-attack-took-large-sections-of-a-countrys-internet-offline/
where hackers successfully used complex and constantly changing attacks to create chaos that could not be addressed by the service provider on time.

Perhaps the most important quote from Belnet on this attack is:

"The fact that the perpetrators of the attack constantly changed tactics made it even more difficult to neutralize it," said Dirk Haex, technical director at Belnet.

The above discussion and example reinforce the fact that it is no longer relevant to rely on traditional DDoS protection systems responding to attacks, a major strategy improvement is required, and sooner would be better than later.

Detection and protection theories suggest a few very basic concepts to effectively block complex and intermittently changing threats, using two main concepts:

1. Continuously Validate and Remediate: your entire DDoS protection posture in peaceful times, fix known areas of weakness proactively, as you have no time to do so once an attack starts. Any DDoS attack that is not automatically blocked when an attack starts, means downtime!

2. Break Complex Attacks into Building Blocks: make sure you are protected against any known attack vector individually; complex attacks are essentially composed of many individual attack vectors, once you are protected against every attack building block, you will automatically block any mixed vectors attack (solve the problem by separation of variables).

This new technology allows you to address the two gaps discussed above through:

1. Vulnerability Identification across the complete attack surface, automatically discovering the attack surface, running thousands of non-disruptive smart attack simulations against protections in place to identify the entire vulnerability landscape.

2. Guided Remediation Process and Revalidation of specific network vulnerability intelligence collection throughout the process creates a prioritized remediation plan, guiding customers in closing vulnerabilities in the most accurate and effective manner

3. Finally, the system immediately revalidates the protection level, ensuring the highest level of protection is achieved.

Modern hybrid DDoS protection postures require pre and post-attack protection, cloud and on-prem solutions, to lower the chances for downtime to the minimum possible.

Essentially when before and after DDoS protection systems are employed, the chance for down time is practically eliminated.

About MazeBolt

MazeBolt is a leading innovative cyber security company, and part of the mitigation space. Offering full DDoS risk detection and elimination. Working with any mitigation system to provide end to end full coverage. Avoiding downtime and eliminating mitigation vulnerabilities before an attack happens.

For more information, please visit: www.mazebolt.com or
e-mail: info@mazebolt.com