neustar®

DDOS ATTACKS
A TASTE OF WHAT'S TO COME

The Neustar Security Operations Center (SOC) analyzes global client mitigation data. The full 2015 report will be released in March 2016; in the meantime, here are notable findings to whet your appetite. **Three key takeaways:**

1 Sometimes a single vector attack just won't do

Multi-vector attacks are a troubling sign of persistence. Rather than using one method to attack your infrastructure, attackers are increasingly using a multi-vector approach to wear out defenses and persist until they succeed. And with average monthly attacks of 66 Gbps, when attackers use multiple vectors, they hit hard.

57% of all multi-vector attacks involved reflection attacks

17% of all attacks involved multiple vectors with a peak size of 6.63 Gbps

TCP SYN accounted for nearly 20% of overall vector attacks; DNS was second at 13%

2 Death by a thousand cuts

Not every attack is intended to cause an outage. By using smaller, more pointed assaults, the attack can fly under the radar and avoid network level DDoS detection techniques. These "low and slow" attacks are capable of disrupting the network and set the stage for exfiltration opportunities.

57% of single-vector attacks were less than 1 Gbps

43% of multi-vector attacks were less than 1 Gbps

3 Note the time of attacks

It's no surprise that attacks ramped up in the fourth quarter of the year. Attackers took note of high volume transaction periods and responded with some of their most vicious attacks.

32% of cloud attacks occurred in Q4, just in time for Cyber Monday and the online holiday shopping period

Attack peak size crested in February at 245.76 Gbps, and also spiked in July and December. 47% of all multi-vector attacks occurred in the last four months of the year

GET AN ADVANCE COPY OF THE NEUSTAR SOC REPORT

Visit us in Booth #515, Moscone South to give us your business card at RSA. We'll send you an advance copy of the Neustar SOC report on DDoS trends, based on data from the Neustar DDoS mitigation network.

neustar

DDOS PROTECTION IN 2016: LET'S LOOK UNDER YOUR HOOD

A strong and well-defended network can be the driving force behind your company's success. With DDoS attacks and threats increasing, the right protection matters, and every second counts.

If Your CEO Asks: Three Questions You Should Answer in 2016

1. "Are we protected across the board?"

Your cloud services may not be protecting you. Every device connected to the network puts your digital infrastructure at risk.

What you need to know:

- Cloud services typically don't include tailored detection and prevention services, which can leave you vulnerable to DDoS attacks
- Load balancers and firewalls can be a point of failure; and horizontal scaling to absorb an attack can be costly and error inducing
- To defeat DDoS attackers, you need specialized protection managed by experienced professionals to augment your existing defenses

2. " What's the plan if we get a DDoS ransom note?"

The precedent is set; some companies have already paid hefty ransoms to restore service and "minimize losses." But, as the saying goes, the only real defense is an active defense.

What you need to know:

- Hope is not a strategy
- Rather than allocate funds for ransom, invest in the proper protection, technologies and expertise that will yield dividends
- Establish relationships with law enforcement to help identify trends and defeat DDoS attacks

3. " Are we agile enough to block constantly shifting attacks?"

With every DDoS assault, attackers are probing and learning about your defenses; and soon they'll be back with different tactics.

What you need to know – An example from the Neustar Security Operations Center:

- One client incident started as a DNS reflection attack to a certain port, which later expanded to every port
- Neustar SOC responded with applied filtering to affected ports eventually rate limiting all inbound DNS traffic
- The attacker responded by launching an NTP reflection attack
- Several moves and counter-moves later the attacker gave up, stymied by professionals who fight DDoS every day

As DDoS attacks and losses increase, the right protection can help you steer clear of pitfalls and avoid downtime. What's your top cybersecurity concern? Send us a tweet **@NeustarCTO** using **#NeustarFightsDDoS** for a **chance to win a drone!**

© 2016. Neustar. All Rights Reserved.