APRIL 2016
SECURITY OPERATIONS CENTER REPORT

DDOS ATTACKS ANALYSIS AND TRENDS

neustar®

CONTENTS

2015 ATTACK THEATER

In recent years, distributed denial of service (DDoS) attacks evolved from a novelty used to create a minor nuisance to a stealth weapon capable of crippling digital infrastructures. As security measures to defend against DDoS attacks improved, hackers continued to improvise and refine their techniques in an attempt to stay ahead of the curve.

The DDoS attacks of 2015 were persistent, and for organizations that didn't have adequate DDoS defenses in place, they were also costly. The attack vectors ranged from using DNS as a reflection source, one of the oldest types of UDP amplification attacks, to targeted strikes using DNSSEC – signed zones.

As you'll read in this report, hackers learned, altered and timed their tactics for maximum impact, to hit their targets where and when it hurts the most.

- 32% of attacks occurred in Q4, just in time for Cyber Monday and the online holiday shopping period
- 17% of all attacks involved multiple vectors
- Holiday season/end of year saw a decrease in popular SSDP attacks with marked increase in NTP attacks
- More intention appeared to be focused on activities besides pipe saturation and service disruption
- Neustar protected customers subjected to extortion attempts that reflected growth in attacker tactics and motivations
- Neustar saw an evolution of DNS reflection attacks that utilized DNSSEC for both increasing the complexity of and amplifying the attack. Neustar has also seen a resurgence in DNS reflections using hosts loaded up with misc. A records which had dramatically fallen off from two years ago

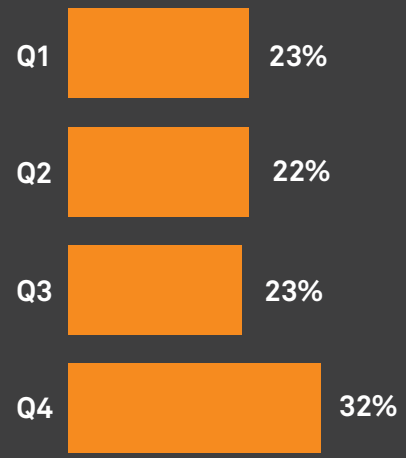
Multi-vector attacks were particularly complex and persistent

- Multi-vector attacks were significant in size and in intent, especially towards end of year
- It was common to fend off three or four vector attacks, necessitating interactive defenses against determined foes
- TCP SYN accounted for nearly 20% of overall vector attacks
- ICMP attacks, though not large in size and volume individually, were popular in multi-vector attacks, appearing in more than 1 out of every 4 strikes - especially late in the year
- NTP reflection + SSDP reflection was a particularly popular multi-vector attack sequence representing 1 of every 3 multi-vector attacks involving NTP reflection/amplification

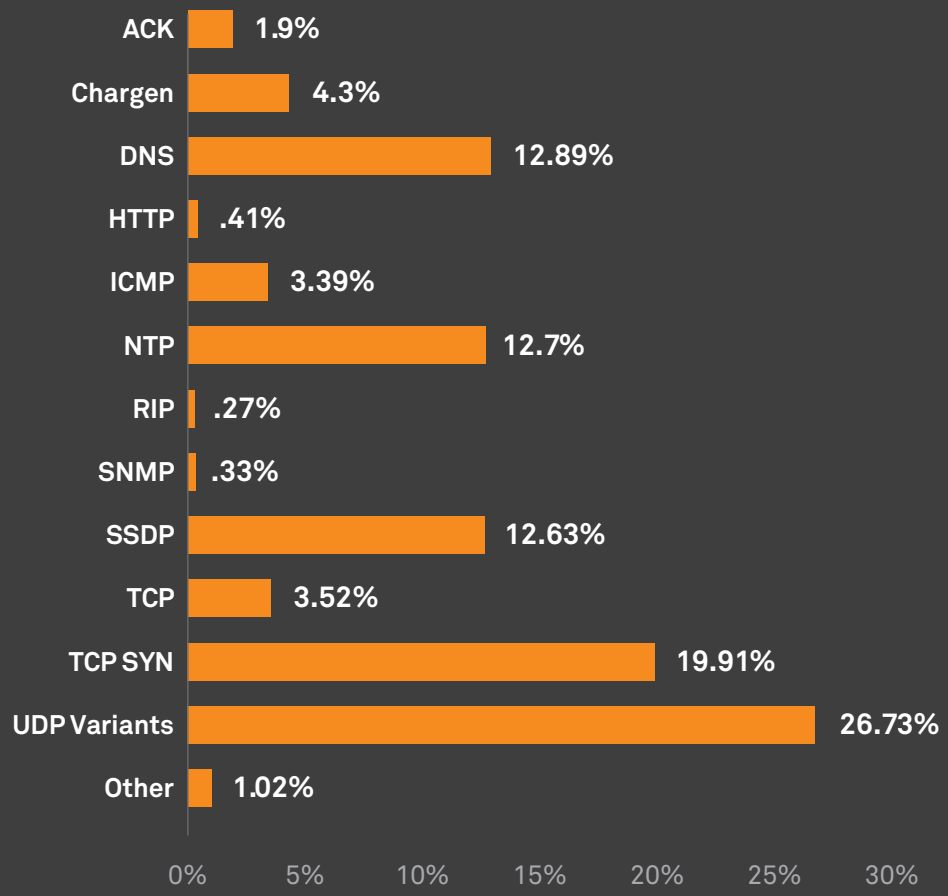
This report analyzes some of the major attack types seen in 2015 and discusses trends for 2016.

DDOS
ATTACKS VECTORS

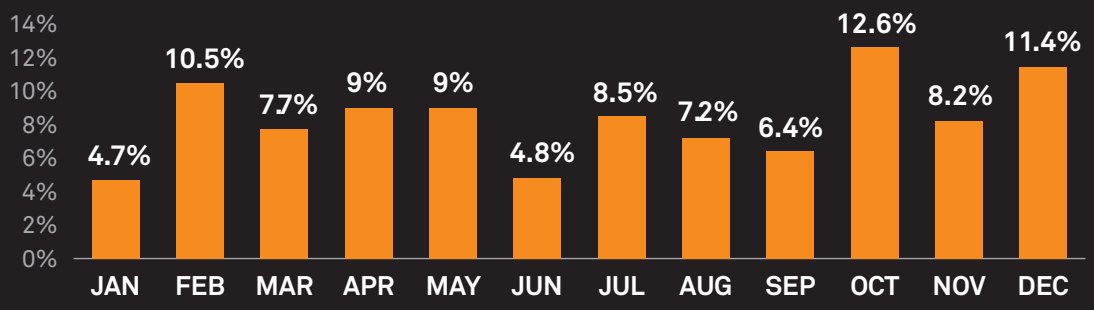
DDOS ATTACKS
By Quarter 2015



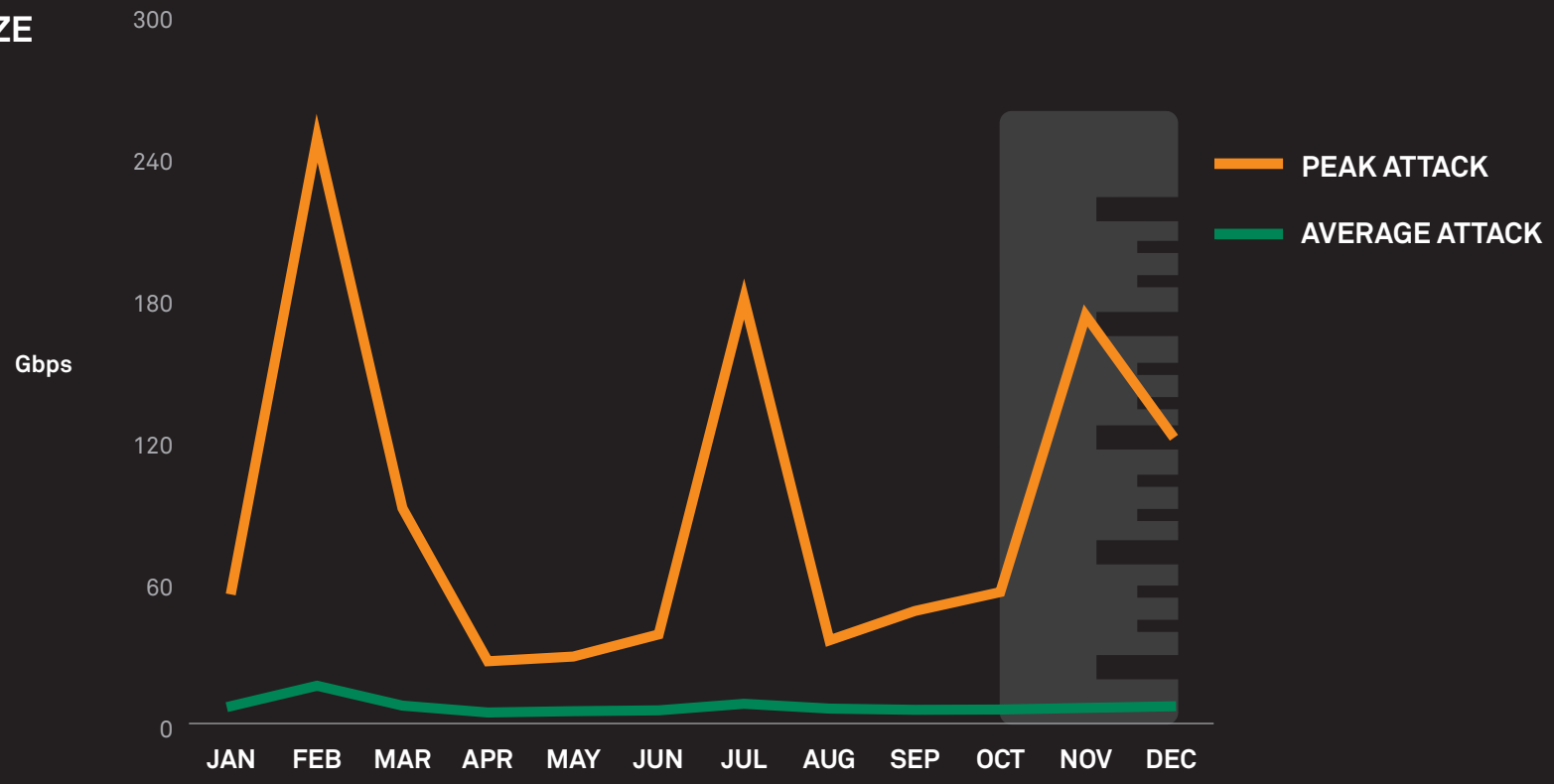
DDOS ATTACKS VECTORS
2015



DDOS ATTACKS 2015
By Month



PEAK ATTACK SIZE
By Month



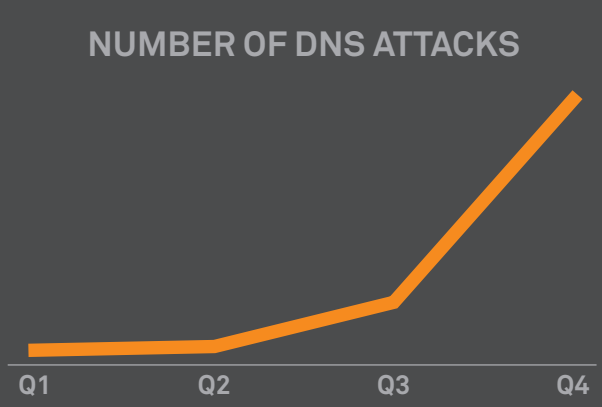
ATTACK ANALYSIS

When it comes to attacks, hackers know there's more than one way to achieve their goal. In this section, we'll examine some of the most popular attack vectors the SOC defended.

DNS

WHAT IT IS: Attacks that use Domain Name System (DNS) server resources to overwhelm targets using techniques including flooding, amplification, and reflection

WHAT NEUSTAR SAW:



11.4 Gbps Average peak size

122.9 Gbps Largest attack

22% Part of multi-vector attacks

WHAT MAKES THEM DANGEROUS:

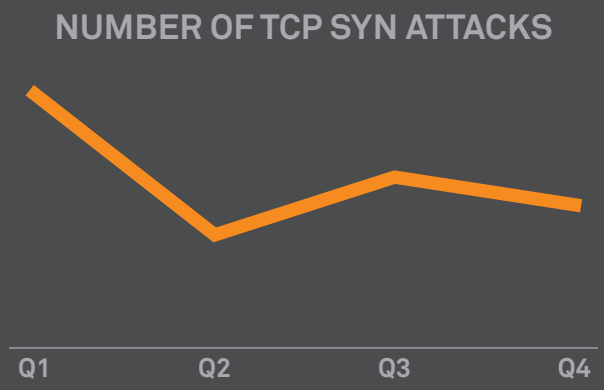
DNS attacks are easy to ramp up and complex to identify if the attacks are subtle. DNS is a popular option for multi-vector attacks since it's often mismanaged.

There are more than 25 million open recursive servers that can be used in amplification attacks.

TCP SYN

WHAT IT IS: Attack type that leverages legitimate protocol handshake conduct between hosts and clients to consume target resources

WHAT NEUSTAR SAW:



8.1 Gbps Average peak size

174.1 Gbps Largest attack

35% Part of multi-vector attacks

WHAT MAKES THEM DANGEROUS:

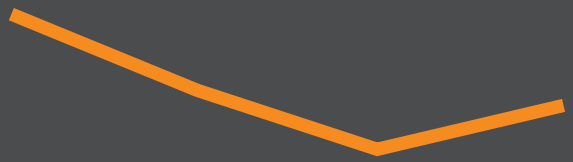
TCP SYN attacks can be very difficult to differentiate as there is an appearance of legitimate traffic, often seen in concert with other cyber activities such as network intrusion.

UDP

WHAT IT IS: Common attack that uses connectionless UDP protocol 17 as a non-amplification vector to easily build sizable attacks, particularly in multi-vector attack scenarios

WHAT NEUSTAR SAW:

NUMBER OF UDP ATTACKS



Q1 Q2 Q3 Q4

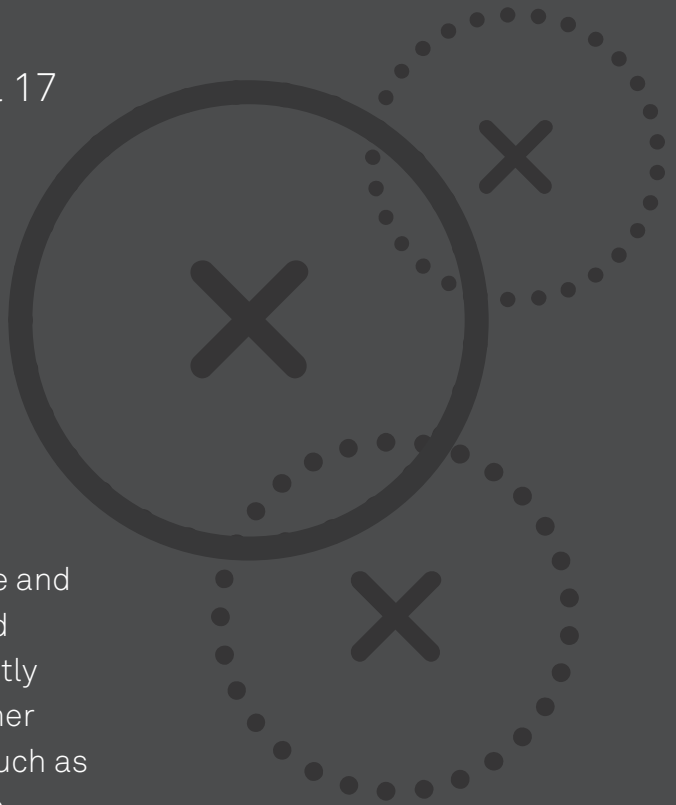
3.1 Gbps Average peak size

89.9 Gbps Largest attack

39% Part of multi-vector attacks

WHAT MAKES THEM DANGEROUS:

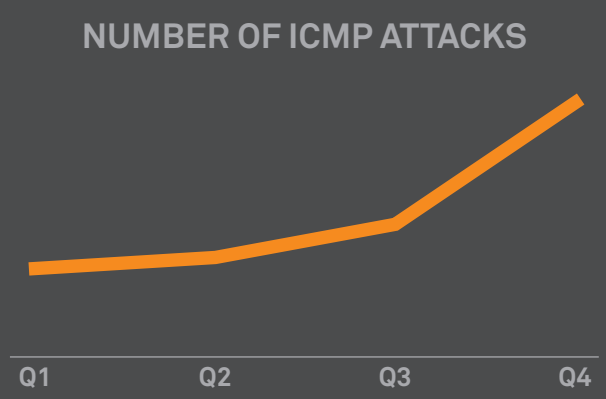
UDP attacks can quickly become large and challenge defenses if not properly and efficiently handled. Also, UDP frequently serves as a smokescreen to shield other simultaneous malicious activities – such as compromise of personally identifiable information, IP exfiltration, malware deployment and remote code execution.



ICMP

WHAT IT IS: Also referred to as Ping Flood, ICMP attacks are simplistic attacks that saturate target resources with voluminous ping requests

WHAT NEUSTAR SAW:



1.0 Gbps Average peak size

23.8 Gbps Largest attack

25% Part of multi-vector attacks

WHAT MAKES THEM DANGEROUS:

ICMP are easy to build and launch, but on their own, ICMP attacks can be easily thwarted. However, it's their presence in aggregated multi-vector attacks that often creates trouble.

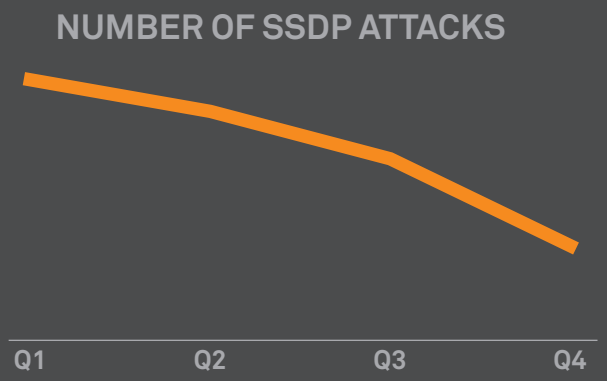
ICMP IS ONE OF THE OLDEST AND MORE EASILY DEFENSIBLE DDOS ATTACK VECTORS, BUT IT IS OFTEN USED TO CREATE ADDITIONAL ATTACK VOLUME.

Home Invasion? NTP and SSDP reflections are two of the largest amplifiers of DDoS attacks. In fact, many are launched from NTP servers and poorly configured home routers, enabling our homes to become launching pads for attacks.

SSDP

WHAT IT IS: Attacks initiated by botnets exploiting Universal Plug and Play devices, such as a home-based internet router

WHAT NEUSTAR SAW:



3.7 Gbps Average peak size

72.8 Gbps Largest attack

21% Part of multi-vector attacks

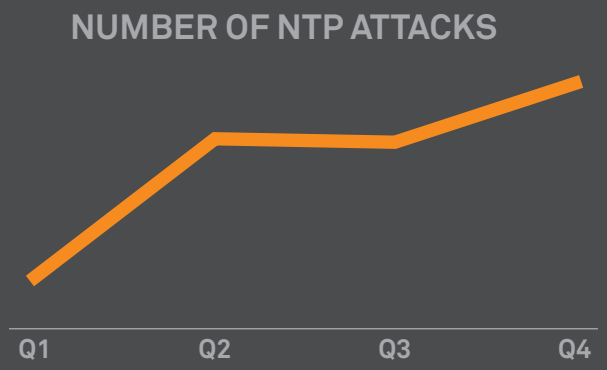
WHAT MAKES THEM DANGEROUS:

Easy-to-build large botnets can overwhelm network server resources.

NTP

WHAT IT IS: Attacks that exploit the Network Time Protocol commonly used to synchronize network device clocks

WHAT NEUSTAR SAW:



5.1 Gbps Average peak size

46.1 Gbps Largest attack

29% Part of multi-vector attacks

WHAT MAKES THEM DANGEROUS:

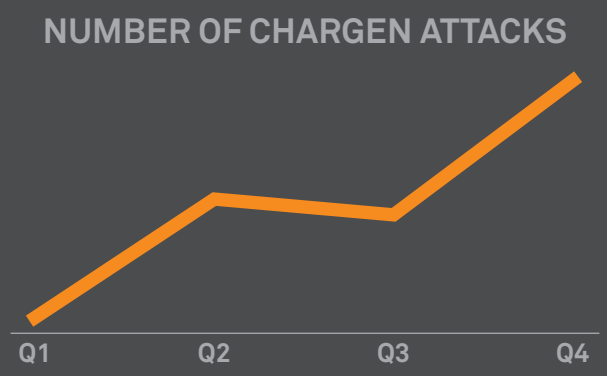
NTP can be used to build sizable, unrelenting attacks that, through amplification, can seriously impact network availability – especially in multi-vector attacks. The appearance of legitimate traffic can make the attack difficult to detect if used in smaller quantities to accompany intrusion activities.

NTP and SSDP are two of the largest possible amplifying multiples. They leverage open/unrestricted NTP servers – which can get up to 600 times the amplification factor – and can also leverage poorly configured or misconfigured home routers, which can have 30 times the amplification factor.

CHARGEN

WHAT IT IS: Short for character generator protocol, Chargen is an older printer protocol that generates alphanumeric characters, which is now being misused for flooding and reflection attacks

WHAT NEUSTAR SAW:



3.4 Gbps Average peak size

10.2 Gbps Largest attack

12% Part of multi-vector attacks

WHAT MAKES THEM DANGEROUS:

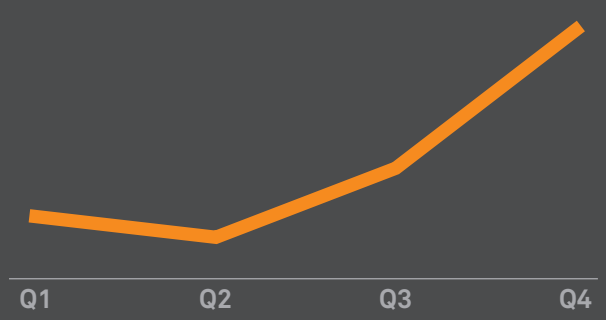
It's difficult to identify the source of a Chargen attack, and they can easily and rapidly scale to overwhelm server resources.

OTHER

WHAT IT IS: Attacks that included BitTorrent, SUNPRC, NetBIOS, and SNMP amplification, among others

WHAT NEUSTAR SAW:

NUMBER OF OTHER ATTACKS



1.1 Gbps Average peak size

17.2 Gbps Largest attack

7% Part of multi-vector attacks

WHAT MAKES THEM DANGEROUS:

These attacks have unique characteristics, making them difficult to detect without expertise.

The dozens of attack types and thousands of individual attacks spanned the spectrum of sophistication and intent. Neustar mitigated these attacks by leveraging experience and best practices to remain ahead of the variances and defeat the attackers.

MULTI-VECTOR ATTACK COMBAT

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 probe defenses and persist until they succeed. Multi-vector attacks often expose preconfigured, unmanaged solutions that are not adaptable enough to address threats.

The average largest monthly attack exceeded 66 Gbps in size. When attackers used multiple vectors, they struck with purpose.

57% 57% of all multi-vector attacks involved reflection attacks

17% 17% of all attacks involved multiple vectors

20% TCP SYN accounted for nearly 20% of overall vector attacks; DNS was second at 12.9%

1 in 5 1 in 5 multi-vector attacks involved DNS vector attacks including floods, amplification, and reflection

246 246 Gbps Largest aggregated multi-vector attack composed of SYN Flood and UDP Flood

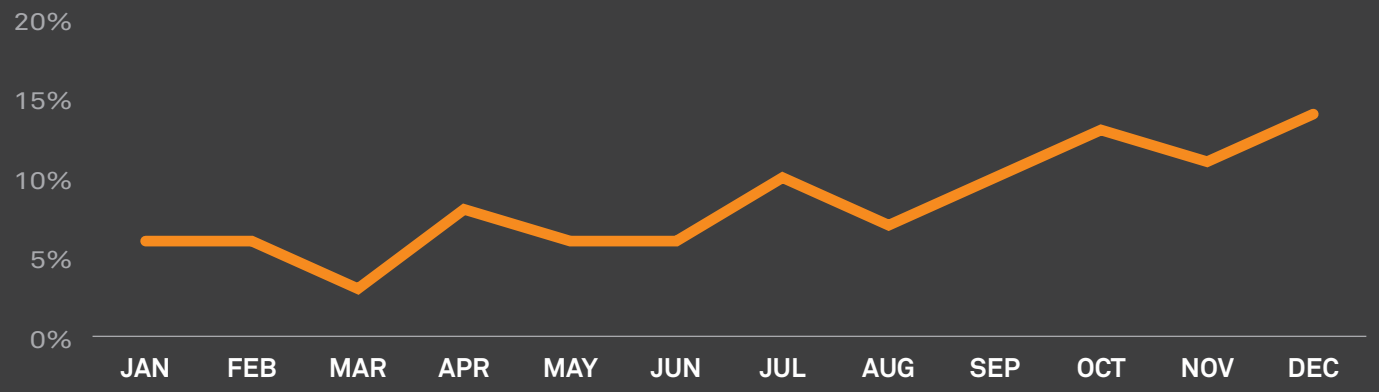
20% Attacks launched using NTP attack types as the first stage in multi-vector attacks accounted for 20% of all multi-vector attacks and had an average size of 7.0 Gbps

16% TCP SYN Floods when used as the initial attack vector accounted for only 16% of all multi-vector attacks, but averaged 6.9 Gbps in size with the largest attack exceeding 245 Gbps

40% UDP attacks were the greatest in quantity. They were involved in nearly 40% of all multi-vector attacks, but averaged 4.1 Gbps, little more than half the size of NTP and TCP SYN attacks

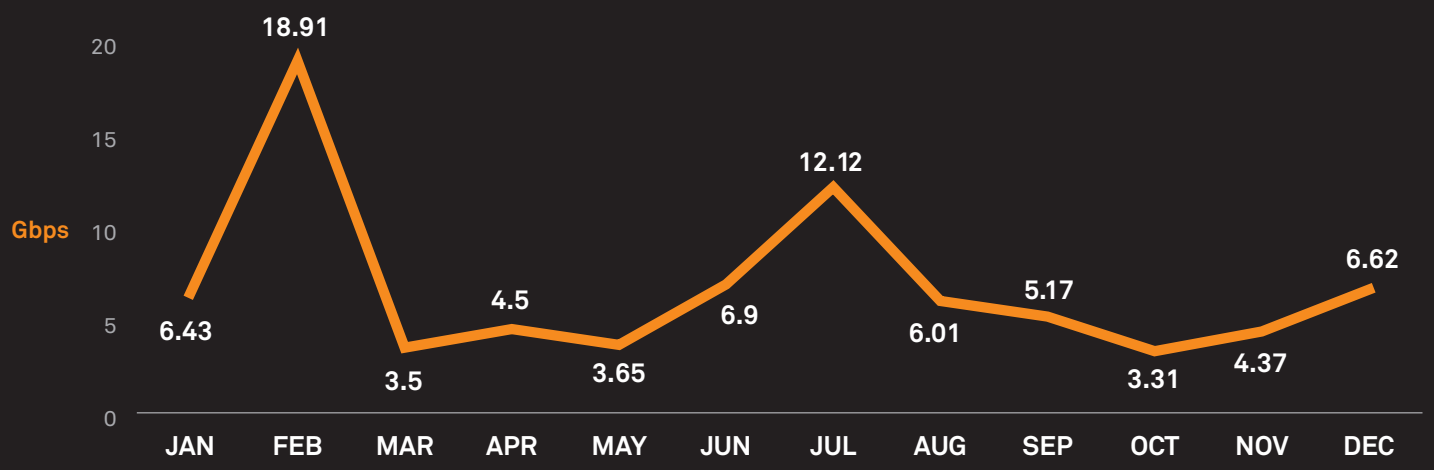
Multi-vector attacks and the persistence of the attackers in repetition against high-profile targets showed a determination of intent. As the holiday season opened, the attacks grew more creative and complex.

MULTI-VECTOR ATTACKS



Multi-vector attacks increased as the year wore on and their average size reflected potentially more deliberate activities to distract and intrude.

MULTI-VECTOR AVERAGE PEAK SIZE



A QUICK NOTE ON DNSSEC

The Neustar SOC is seeing and mitigating attacks using DNSSEC to amplify DNS reflection and amplification attacks. There are a number of variables that dramatically affect the amplification output of a DNSSEC reflection DDoS attack in terms of bytes/packet.

In the tests that Neustar ran using real world DNSSEC zones, the following points emerged:

- A normal DNS (non-DNSSEC) website A record query can have a 3:1 or larger ratio between the query and simulated response in terms of bytes/packet. However, using DNSSEC can create higher amplification
- A DNSSEC query for a DNSSEC signed website A record can bump that amplification factor up to 15X or greater (query to response in bytes/packet)
- Non-existent zones can also be exploited for response traffic
- Some obscure zones were registered just before the attacks occurred so they could pack maliciously queried records to ensure longer responses (which have more amplification), and some attacks targeted the DNSSEC-signed zones where the responses would be longer due to hashes
- IPv6 can also add to the amplification factor
- Tools such as NSLOOKUP can be exploited
- DNS has other commands that can result in additional records being requested, and further amplify reflection attacks

FROM THE SOC DDOS FORENSIC FILES: As is the case in any crime, you can tell the perpetrator's sophistication by their tactics and evidence. In the SOC, we've noticed some techniques and trends that help us identify the maturity of the attacker, and even stay a couple of steps ahead by anticipating their next moves.

Here are a few differentiating factors between the novice who rents a DDoS service and a seasoned vet:

	NOVICE	VETERAN
VOLUME	**Less volume** since it usually costs more	Knows how to access a larger network to **launch larger attacks**
COMPLEXITY	Standard attack types with **little variation**; tend to attack **one vector** at a time	Deploys **complex, multi-vector attacks** either in waves, or all at once
PREFERRED ATTACK VECTOR	**SSDP and NTP reflection Basic SYN flood**	**Intricate TCP floods, NETBIOS reflections, SIP floods**
VARIATION	**None**	Will **change vectors** if first attempts are stymied
CALLING CARD	**Tells roommates**	**Takes to social media** (mainly Twitter) to take credit for attacks

TRENDS FORECAST

After examining the patterns and trends that we saw in 2015, here are some forecasts for anticipated attacks in 2016:

TRENDS

- 2016 is shaping up to expand the use of DDoS attacks, whether for solo attacks or in conjunction with other sinister activity including extortion and intrusion
- DNS reflection attacks are going to keep growing, given that they are effective as well as being easy to mount, quick to scale, more difficult to detect
- DDoS attackers are determined with an increasingly powerful and easy-to-use array of tools
- NTP and most Layer 7 attacks will continue to increase
- TCP SYN Flood multi-vector combinations will continue their growth and effectiveness
- As IoT adoption increases, the use of non-human assets enrolled into botnets will exponentially increase, giving attackers even more options and opportunities to elude detection

SUMMARY

5 KEY TAKEAWAYS FROM THIS REPORT

1. **Sometimes a single vector attack just won't do.** If at first they don't succeed, attackers will try again. Motivated by money and aware that all it takes is one successful breach, attackers are continually working to penetrate defenses through different attack methods.

2. **Death by a thousand cuts.** Not every attack is intended to cause an outage. By using smaller, pointed assaults, attackers can fly under the radar and avoid network-level DDoS detection. These 'low and slow' attacks can disrupt the network and set the stage for exfiltration opportunities.

3. **They're the most dangerous times of the year.** Attackers chose high-volume transaction periods – such as the tax return period and Q4 for some of their most vicious strikes. Forty-seven percent of all multi-vector attacks occurred in the last four months of the year.

4. **Defend your DNS.** Attacks on DNS skyrocketed in Q4. As the layer of the Internet that's most responsible for your digital presence, DNS is often the first target of a DDoS attack, and the least protected. No DNS, no website.

5. **The combat continues.** DDoS attacks are inevitable. As too many companies, organizations and governments found out, it's no longer a matter of if or when, but how often the attacks will occur. As hackers continue to innovate ways to attack, the best defense remains an active, vigilant defense.

TO LEARN MORE ABOUT DDOS PROTECTION, VISIT Neustar.biz/services/ddos-protection

To mitigate DDoS attacks, Neustar blends expertise, proven responses, and diverse technologies. Neustar SiteProtect, our DDoS mitigation service, offers options to meet your level of risk, budget, and technical environment: cloud-based protection; on-premise, always-on hardware; or a hybrid of both, fully managed by us. SiteProtect is backed by the Neustar Security Operations Center, whose experts bring years of experience to blocking every attack.

ABOUT NEUSTAR

Neustar, Inc. (NYSE:NSR) is the first real-time provider of cloud-based information services and data analytics, enabling marketing and IT security professionals to promote and protect their businesses. With a commitment to privacy and neutrality, Neustar operates complex data registries and uses its expertise to deliver actionable, data-driven insights that help clients make high-value business decisions in real time, one customer interaction at a time. More information is available at **www.neustar.biz**.

neustar®

www.neustar.biz

RPRT-SEC-12806b 03302016