



VERISIGN®

VERISIGN DISTRIBUTED DENIAL OF SERVICE TRENDS REPORT

VOLUME 3, ISSUE 4 – 4TH QUARTER 2016

Complimentary report
supplied by

axians

CONTENTS

EXECUTIVE SUMMARY	3
VERISIGN-OBSERVED DDoS ATTACK TRENDS: Q4 2016	4
DDoS Attacks Remain Complex and Unpredictable	4
Multi-Vector DDoS Attacks Dominate	6
Highest Intensity Flood and Largest Volumetric Attack	8
DDoS Attacks Against Public Sector Increases	8
FEATURE ARTICLE	
Market Landscape: The Botnet Ecosystem	11

EXECUTIVE SUMMARY

This report contains the observations and insights derived from distributed denial of service (DDoS) attack mitigations enacted on behalf of, and in cooperation with, customers of **Verisign DDoS Protection Services** from Oct. 1, 2016 through Dec. 31, 2016 (“Q4 2016”) and the security research of **Verisign iDefense® Security Intelligence Services** conducted during that time. It represents a unique view into the attack trends unfolding online, including attack statistics and behavioral trends for Q4 2016.*

Verisign observed the following key trends in Q4 2016:

Number of Attacks

5%
decrease from Q3 2016

Peak Attack Size

Volume
127
Gigabits per second (Gbps)

Speed
50
Million packets per second (Mpps)

Most Common Attack Mitigated

52%
of attacks were User Datagram Protocol (UDP) floods

86%
of attacks employed multiple attack types

Average Peak Attack Size

11.2 Gbps
12% decrease compared with Q3 2016

22%
of attacks over 10 Gbps

52%
of attacks over 5 Gbps

Overall, 2016 saw a 167 percent increase in average attack peak size (16.1 Gbps) compared with 2015 (6.02 Gbps).



167%
INCREASE
in average attack peak size from 2015 to 2016.

VERISIGN-OBSERVED DDoS ATTACK TRENDS: Q4 2016

DDoS Attacks Remain Complex and Unpredictable

In Q4 2016, Verisign observed that DDoS attacks continued to be complex and unpredictable, frequently requiring human intervention and expertise in addition to technical safeguards to mitigate.

Attack Frequency

Attackers in Q4 2016 launched sustained and repeated attacks against their targets. Verisign observed that more than 50 percent of customers who experienced DDoS attacks in Q4 2016 were targeted multiple times during the quarter.



More than

50%

of customers who experienced DDoS attacks in Q4 2016 were targeted multiple times.

Attack Size



87% peaked over 1 Gbps

52% peaked over 5 Gbps

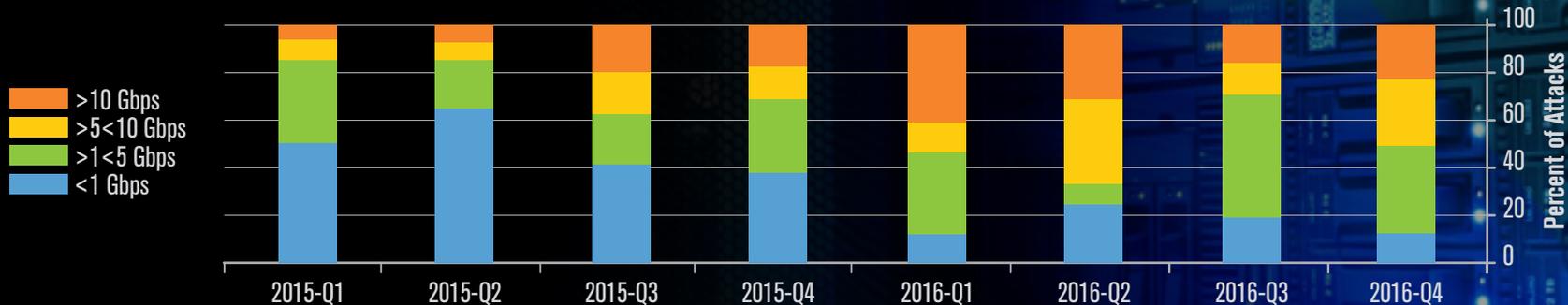


Figure 1: Mitigation Peaks by Quarter from Q1 2015 to Q4 2016

Average Attack Peak Size

11.2 Gbps

↑ **63%**

increase in average attack peak size since Q4 2015



With more than half of attacks in Q4 2016 peaking over

5 GBPS

a “do-it-yourself” approach to DDoS protection would be challenging for the in-house IT departments of most organizations.

Overall, average attack peak sizes in 2016 were larger than previous years. In fact, Verisign observed an average attack peak size of 16.1 Gbps in 2016, a 167 percent increase from 2015, in which the average attack peak size was 6.02 Gbps.

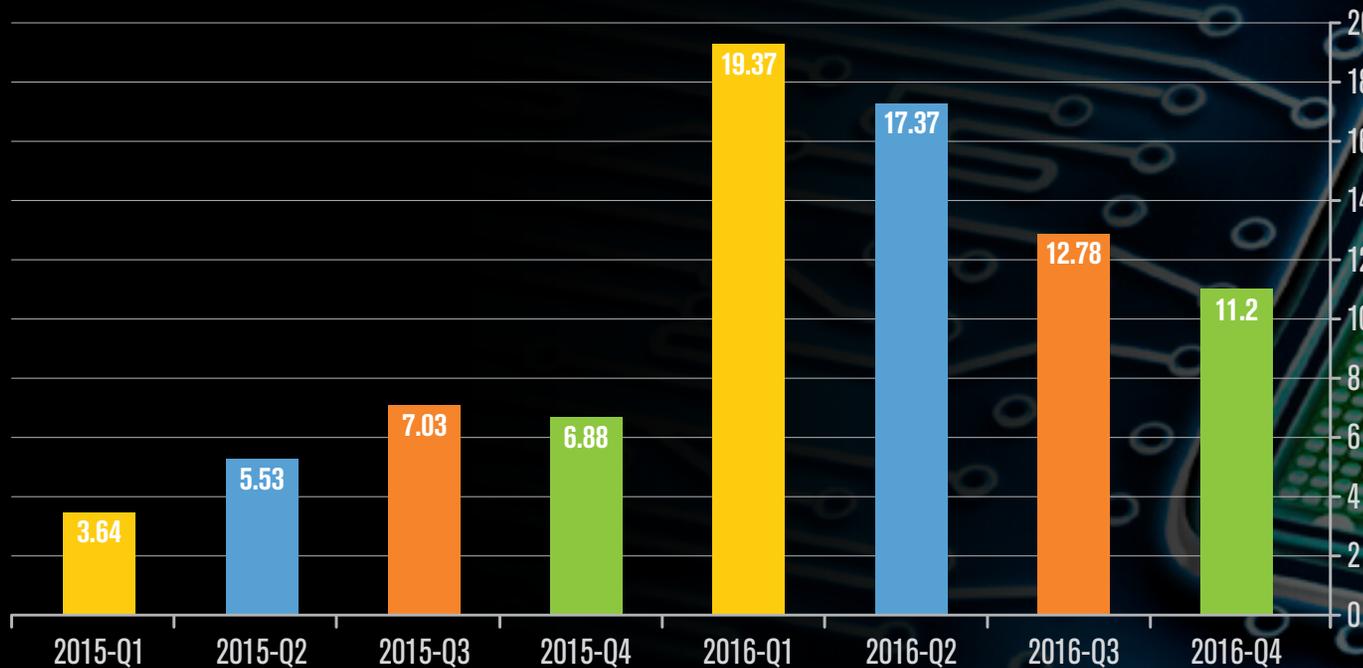


Figure 2: Average Attack Peak Size by Quarter from Q1 2015 to Q4 2016

Multi-Vector DDoS Attacks Dominate

Eighty-six percent of the DDoS attacks mitigated by Verisign in Q4 2016 employed multiple attack types indicating that DDoS attacks remain complex, and thus require continuous monitoring to optimize mitigation strategy.

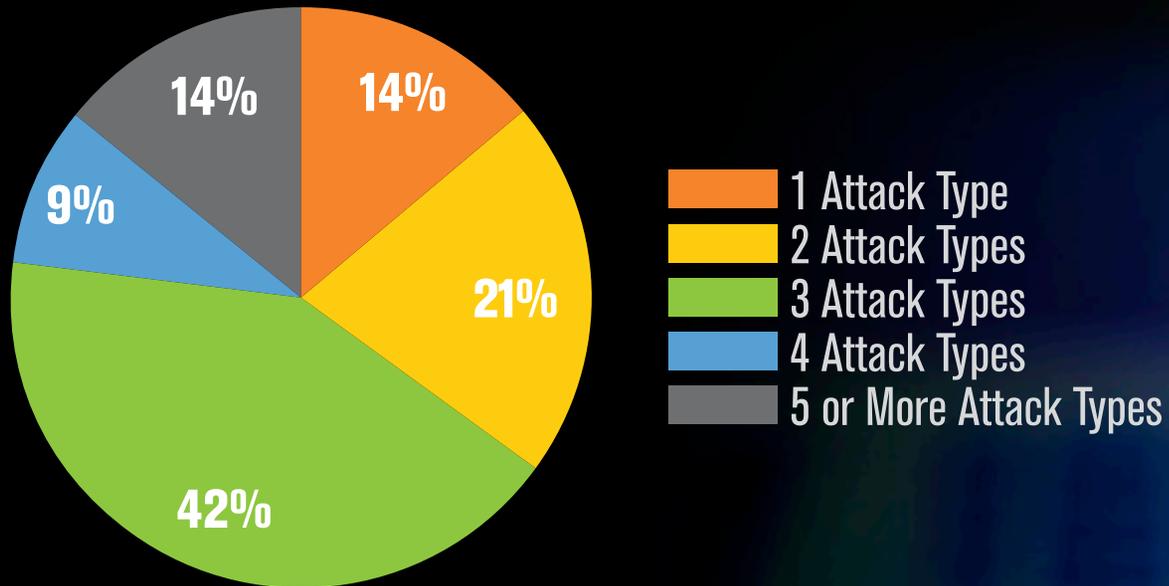


Figure 3: Number of Attack Types Per DDoS Event in Q4 2016



65%

of DDoS attacks in Q4 2016 utilized 3 or more different attack types.

Types of DDoS Attacks

UDP flood attacks continue to dominate in Q4 2016, making up 52 percent of total attacks in the quarter. The most common UDP floods mitigated were Domain Name System (DNS) reflection attacks, followed by Network Time Protocol (NTP) reflection attacks.

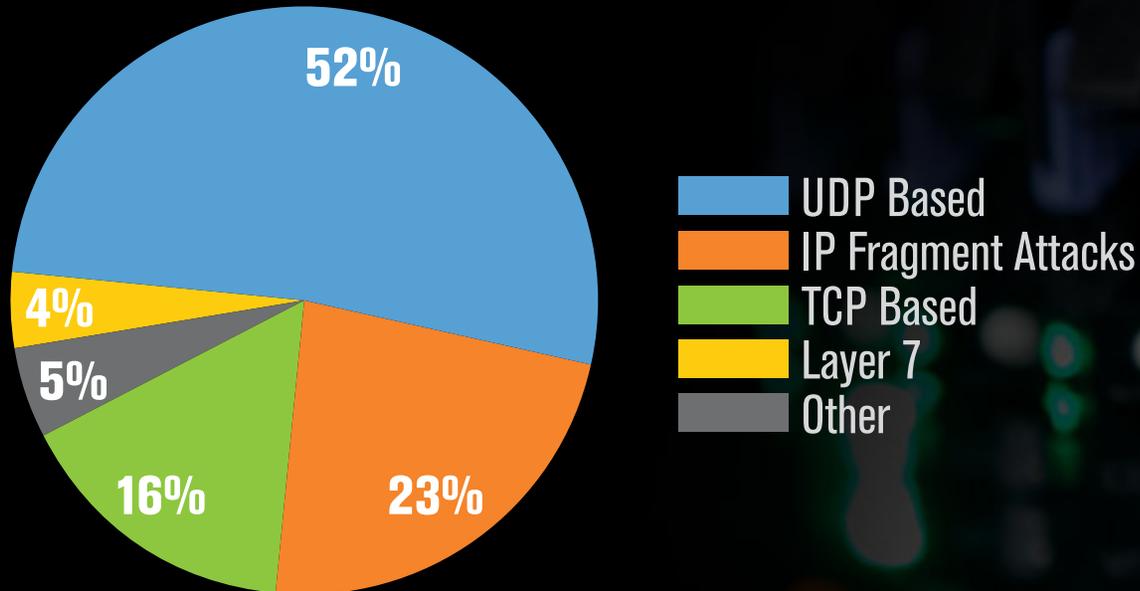


Figure 4: Types of DDoS Attacks in Q4 2016



52%
of attacks were
UDP FLOODS

Highest Intensity Flood and Largest Volumetric Attack

The largest and highest intensity DDoS attack observed by Verisign in Q4 2016 was a multi-vector attack that peaked at over 125 Gbps and around 50 Mpps. The attack was notable because attackers were persistent, sending attack traffic on a daily basis for almost an entire month. The attack consisted of DNS Reflection traffic and Internet Control Message Protocol (ICMP) traffic and the attackers switched periodically to TCP SYN and TCP Reset floods peaking at approximately 70 Gbps and 50 Mpps. The attack also included floods of IP fragments to increase the volume of the attack.

Mitigations on Behalf of Verisign Customers by Industry for Q4 2016¹

IT Services/ Cloud/SaaS

49%
of mitigations

Average
attack size:

16.3 Gbps

Public Sector

32%
of mitigations

Average
attack size:

6.9 Gbps

Financial

7%
of mitigations

Average
attack size:

10.4 Gbps

Media and Entertainment/ Content

6%
of mitigations

Average
attack size:

25.5 Gbps

Telecommunications and Other

4%
of mitigations

Average
attack size:

15.8 Gbps

E-Commerce and Online Advertising

2%
of mitigations

Average
attack size:

1.3 Gbps

DDoS Attacks Against Public Sector Increases

In Q4 2016, public sector customers experienced the second highest number of DDoS attacks among the Verisign DDoS Protection Services customer base (32 percent of total attacks). This is the highest percentage of DDoS attacks that Verisign has observed against Verisign public sector customers since the inception of the Verisign DDoS Trends Report in Q1 2014. Customers in the IT Services/Cloud/SaaS industry continue to have the largest number of DDoS attacks in Q4 2016.

¹ The attacks reported by industry in this document are solely a reflection of the Verisign DDoS Protection Services customer base.

Peak Attack Size by Industry (Q4 2016)

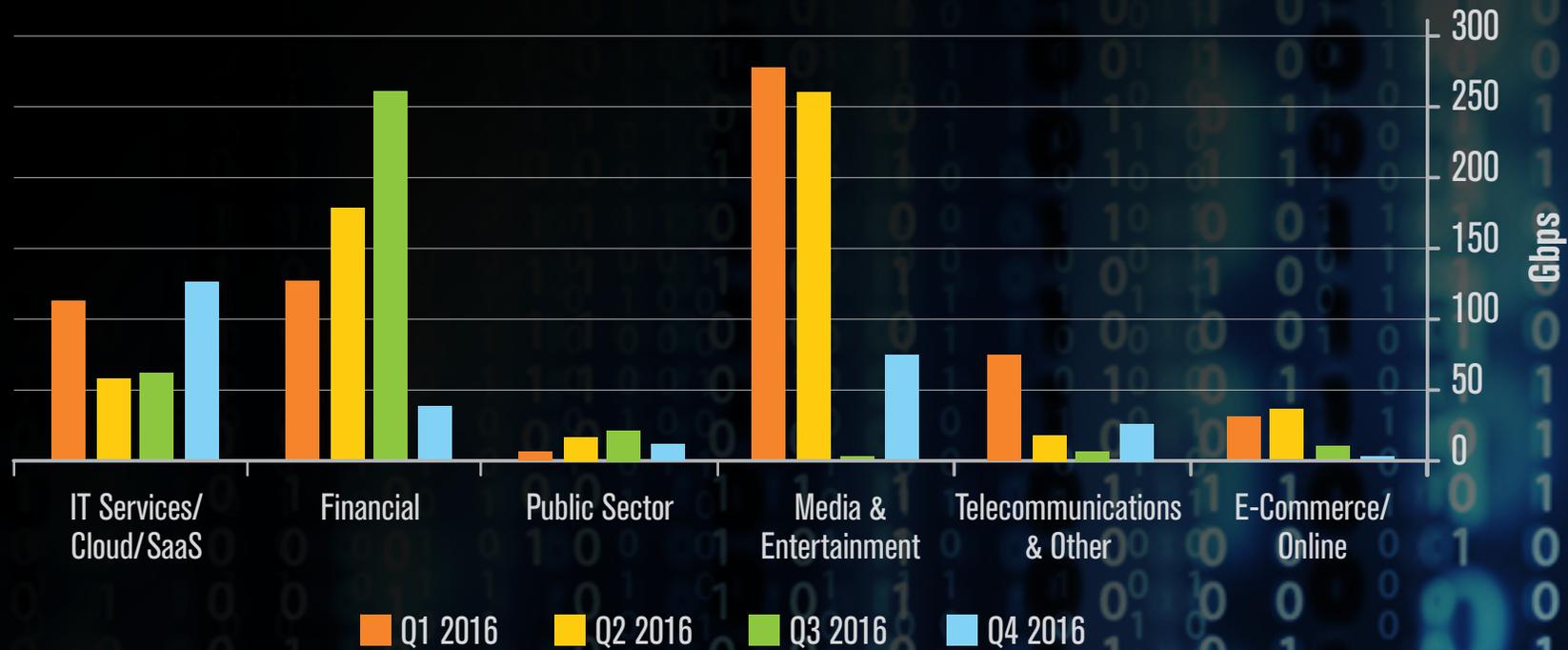


Figure 5: Peak DDoS Attack Size by Industry from Q1 2016 to Q4 2016

The IT Services/Cloud/SaaS, Financial, and Media & Entertainment industries saw peak attack sizes over 100 Gbps in 2016.

FEATURE ARTICLE

MARKET LANDSCAPE: THE BOTNET ECOSYSTEM

Launching a DDoS attack is much more accessible to attackers thanks to the rise of cloud computing, cheap hosting, readily available bandwidth and open-source attack tools. From low-skilled teenagers aiming to cheat while playing online games to cybercriminals looking to supplement their income by renting out their botnets for opportunistic attacks, the DDoS-for-hire market is booming.

The Botnet Ecosystem

Botnets utilized in DDoS attacks vary greatly in size and potency, from as small as a dozen compromised computers to as large as over one million devices. For example, a recent DNS-based DDoS attack that caused significant portions of the east coast of the United States to experience connectivity issues to certain websites involved a flood of malicious requests from up to 100,000 malicious endpoints.² Botnets are comprised of computers, smartphones, servers, routers, printers and even IoT devices like networked refrigerators. With more devices continuously connected to the internet, the available pool of devices that could be used as botnets has increased. Attackers can now rapidly identify and leverage thousands of compromised devices and harness their bandwidth to launch DDoS attacks that can overwhelm even the most prepared networks.

Mitigating DDoS Attacks by Botnets

Because most DDoS-for-hire services frequently share similar characteristics, identifying popular DDoS techniques can help companies mitigate and defend against a variety of DDoS attacks. However, there still is a human element involved. Since most DDoS attacks are concerted efforts by live attackers to bring down a network, many of the attacks start out as one type of attack, but then morph into something new or different. Consequently, organizations need to have access to a high level of expertise and experience in combatting these complex hybrid DDoS attacks. Having a solution that includes monitoring of traffic behavior, the ability to defend against not only network, but also application layer attacks, and the flexibility to transfer large attack traffic to a cloud-based DDoS provider can help to alleviate dangerous threats and costly attacks.

² Loshin, Peter. Details emerging on Dyn DDoS attack, Mirai IoT botnet. <http://searchsecurity.techtarget.com/news/450401962/Details-emerging-on-Dyn-DNS-DDoS-attack-Mirai-IoT-botnet>. Retrieved Jan. 25, 2016

**TO LEARN MORE ABOUT VERISIGN DDoS PROTECTION SERVICES,
VISIT [Verisign.com/DDoS](https://www.verisign.com/DDoS).**

About Verisign

Verisign, a global leader in domain names and internet security, enables internet navigation for many of the world's most recognized domain names and provides protection for websites and enterprises around the world. Verisign ensures the security, stability and resiliency of key internet infrastructure and services, including the .com and .net domains and two of the internet's root servers, as well as performs the root-zone maintainer function for the core of the internet's Domain Name System (DNS). Verisign's Security Services include intelligence-driven Distributed Denial of Service Protection, iDefense Security Intelligence and Managed DNS. To learn more about what it means to be Powered by Verisign, please visit [Verisign.com](https://www.verisign.com).

*The information in this Verisign Distributed Denial of Service Trends Report (this "Report") is believed by Verisign to be accurate at the time of publishing based on currently available information. Verisign provides this Report for your use in "AS IS" condition. Verisign does not make any and disclaims all representations and warranties of any kind with regard to this Report, including, but not limited to, any warranties of merchantability or fitness for a particular purpose.



VERISIGN®

Verisign.com

© 2017 VeriSign, Inc. All rights reserved. VERISIGN and other trademarks, service marks, and designs are registered or unregistered trademarks of VeriSign, Inc. and its subsidiaries in the United States and in foreign countries. All other trademarks are property of their respective owners.

Verisign Public

VRSN_DDoS_TR_Axians_Q4-16_201703