VERISIGN DISTRIBUTED DENIAL OF SERVICE TRENDS REPORT

VOLUME 3, ISSUE 2 – 2ND QUARTER 2016

CONTENTS

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 April 1, 2016 through June 30, 2016 ("Q2 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 Q2 2016.*

Verisign observed the following key trends in Q2 2016:

Number of Attacks

75%
increase year over year

Peak Attack Size

Volume
256 Gigabits per second (Gbps)

Speed
64 Million packets per second (Mpps)

Average Peak Attack Size

17.37 Gbps
Driven by multiple, persistent 100+ Gbps attacks

32%
of attacks over 10 Gbps

Most Common Attack Mitigated

56%
of attacks were User Datagram Protocol (UDP) floods

64%
of attacks employed multiple attack types

45%
of mitigation activity
IT Services/ Cloud/SaaS

VERISIGN-OBSERVED DDoS ATTACK TRENDS: Q2 2016

DDoS Attacks Become More Sophisticated and Persistent

DDoS attacks are a reality for today's web-reliant organizations. In Q2 2016, DDoS attacks continued to become more frequent, persistent and complex.

Attack Frequency

75% increase year over year

Attackers in Q2 2016 launched sustained attacks against targets with a few customers attacked repeatedly throughout the quarter.

Attack Size

75% peaked over 1 Gbps

32% peaked over 10 Gbps

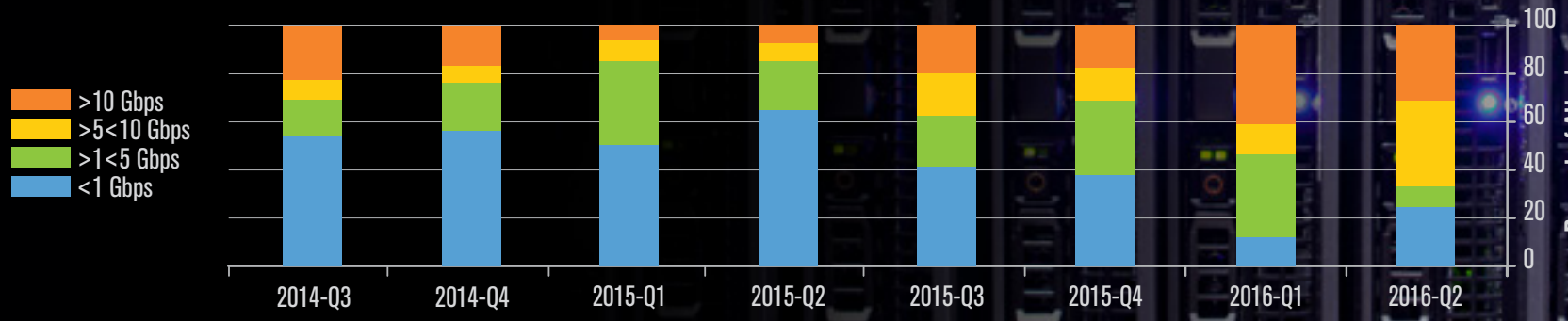


Figure 1: Mitigation Peaks by Quarter from Q3 2014 to Q2 2016

Average Peak Attack Size

17.37 Gbps

The second highest average peak since Q2 2014

214%

increase in average peak attack size compared to Q2 2015

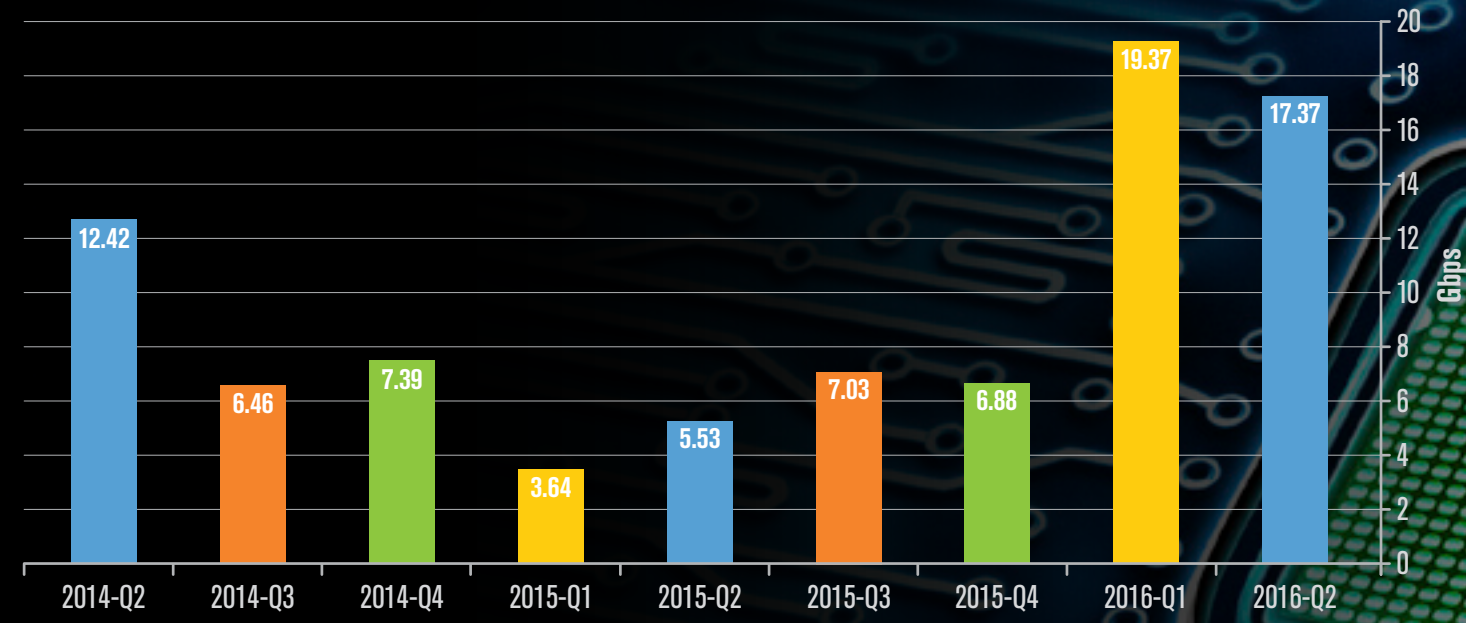


Figure 2: Average Peak Attack Size by Quarter from Q2 2014 to Q2 2016

Multi-Vector DDoS Attacks Dominate

Sixty-four percent of the DDoS attacks mitigated by Verisign in Q2 2016 employed multiple attack types indicating that DDoS attacks continue to increase in complexity, and as a result, require more time and effort to mitigate.

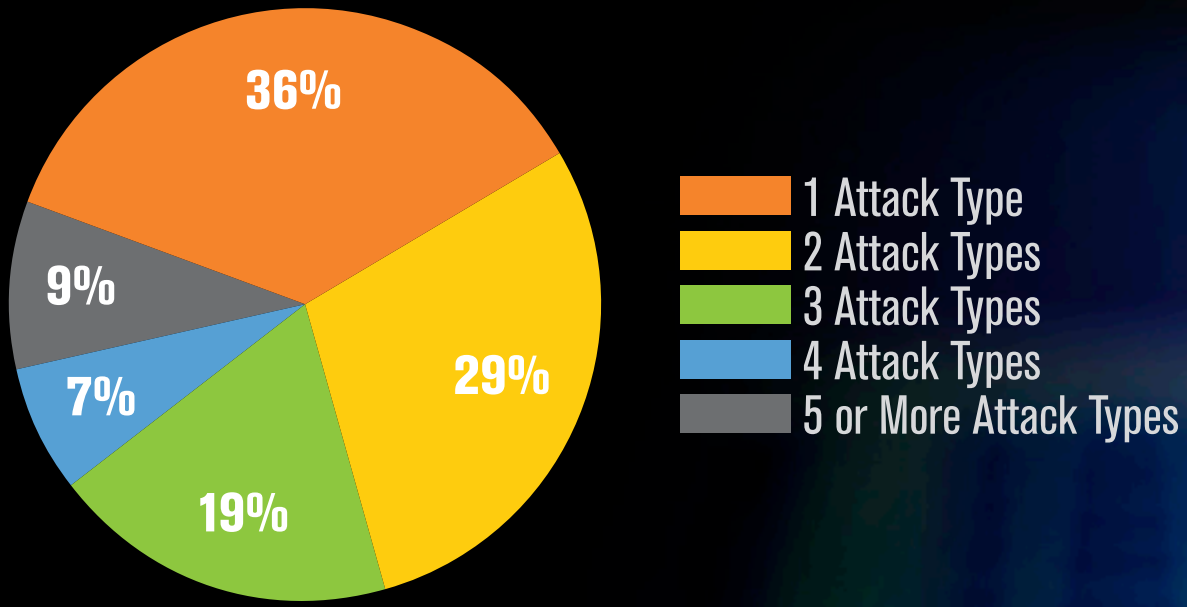


Figure 3: Number of Attack Types Per DDoS Event in Q2 2016

64%

of the DDoS attacks in Q2 2016 employed multiple attack types

Continuing the trend from Q1 2016, the most common DDoS attack types in Q2 2016 were **UDP floods** (including Domain Name System (DNS), Network Time Protocol (NTP), Simple Service Discovery Protocol (SSDP) and Chargen) - making up 56 percent of the total attacks in the quarter. The most common UDP floods mitigated were DNS reflection attacks, followed by NTP reflection attacks.

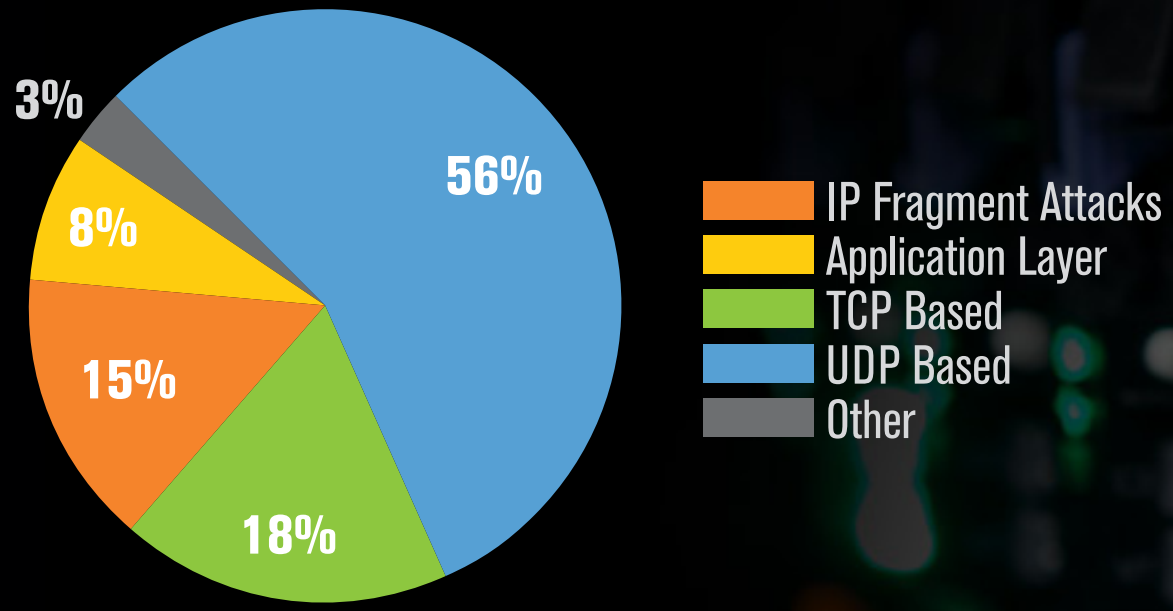


Figure 4: Types of DDoS Attacks in Q2 2016

56%
of attacks were
UDP FLOODS

DDoS ATTACKS REMAIN UNPREDICTABLE

An Increase in Application Layer Attacks

In Q2 2016, Verisign observed a growing trend of low-volume application layer, also known as Layer 7, attacks that probe for vulnerabilities in application code, employing various techniques to use HTTP/S field headers within request packets in order to disable the application. These attacks are frequently coupled with high-volume UDP flood attacks to distract the victim from the Layer 7 attack component.

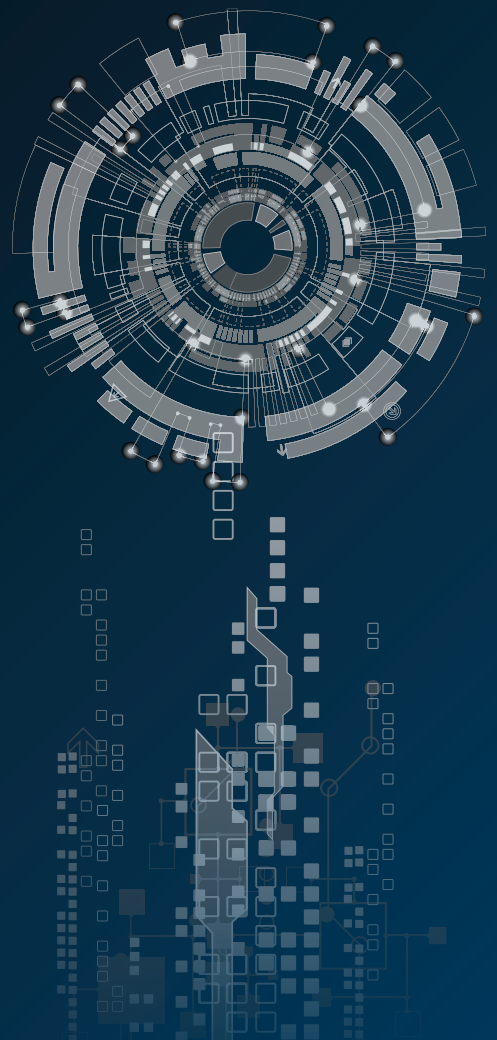
These types of sophisticated low-bandwidth DDoS attacks are a form of denial of service (DoS) attack that typically uses less traffic but increases its effectiveness by aiming at a weak point in the victim's system design. These attacks often utilize SQL injection, a code injection technique, to attack data-driven applications by inserting nefarious SQL statements into the request entry fields for execution. The malicious requests typically include long "Host:" values in the request.

Layer 7 attacks often require multiple and advanced filtering techniques, including adaptive origin response code and regex-based filtering, along with network protection techniques like SYN authentication, invalid IP fragments and UDP flood filtering.

Large Volumetric Attack and Fastest Flood

The largest and fastest DDoS attack in Q2 2016 peaked at 256 Gbps and exceeded 64 Mpps. The DNS reflection attack consisted of small packets, which helped to enable its growth and speed, and also included a flood of invalid packets peaking at over 16 Gbps.

Initially, the attack quickly ramped up to over 250 Gbps over a period of about 15 minutes before settling in at a 200+ Gbps flood for almost two hours before the flood subsided.



The largest volumetric attack in Q2 2016 peaked at

250+ Gbps

before settling in at

200+ Gbps

for almost 2 hours.

Every Organization is at Risk

DDoS attacks are not limited to any specific industry or vertical.

Mitigations on behalf of Verisign Customers by Industry for Q2 2016[1]

IT Services/ Cloud/SaaS

45%
of mitigations

Average attack size:
17.2 Gbps

Financial

23%
of mitigations

Average attack size:
29.1 Gbps

Public Sector

14%
of mitigations

Average attack size:
3.54 Gbps

E-Commerce and Online Advertising

11%
of mitigations
(up from 4% of mitigations in Q1)

Average attack size:
5.5 Gbps

Media and Entertainment/ Content

5%
of mitigations

Average attack size:
67.8 Gbps
(driven by several large events targeting this vertical)

Telecommunications and Other

2%
of mitigations

Average attack size:
9.7 Gbps

The Media & Entertainment and Financial industries continue to experience some of the largest average attack sizes in Q2 2016. The average attack size for the Media & Entertainment industry was 67.8 Gbps and 29.1 Gbps for the Financial industry.

1 The attacks reported by industry in this document are solely a reflection of the Verisign-protected customer base; however, this data may be helpful in understanding the evolution of attacks by industry and the importance of prioritizing security expenditures to ensure protection mechanisms are in place.

Peak Attack Size by Industry (Quarterly)

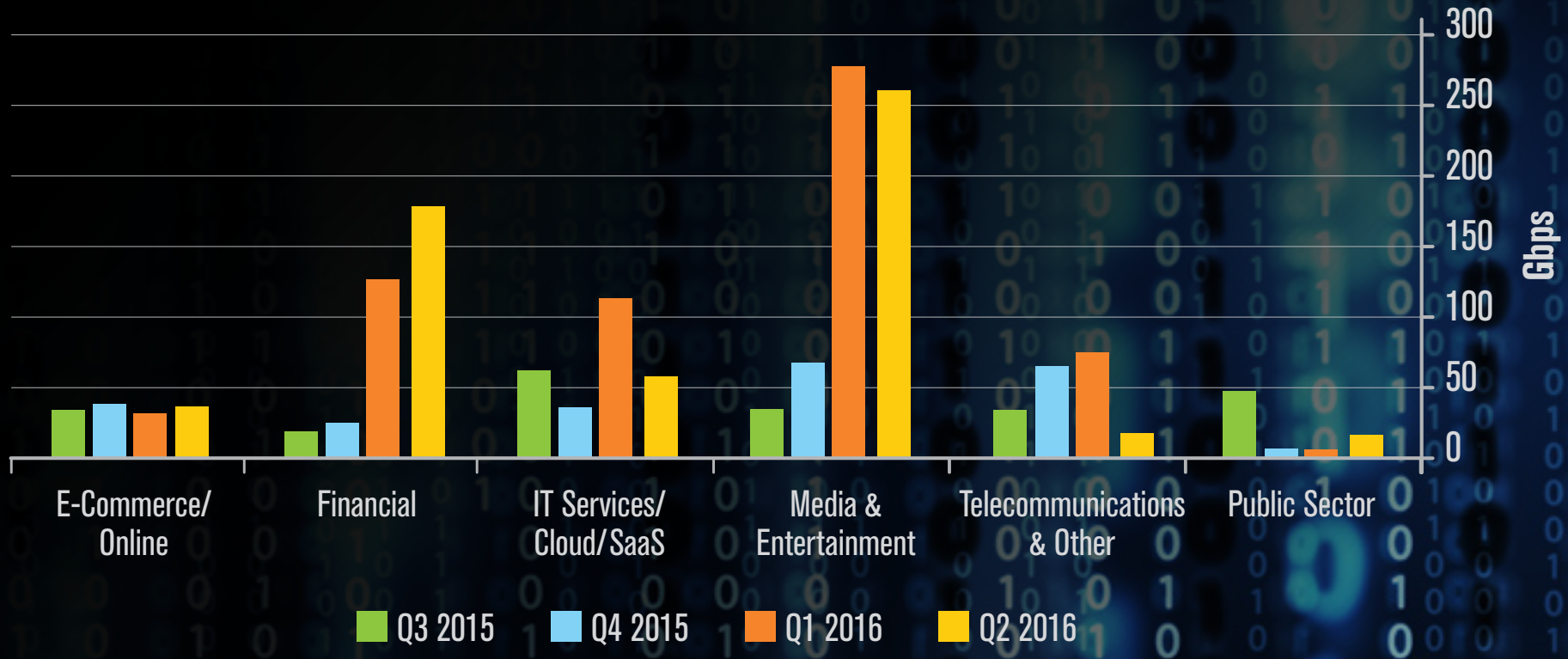


Figure 5: Peak Attack Size by Industry (Quarterly)

FEATURE

DEFENDING AGAINST LAYER 7 DDoS ATTACKS

Layer 7 attacks are some of the most difficult attacks to mitigate because they mimic normal user behavior and are harder to identify. The application layer (per the **Open Systems Interconnection model**) consists of protocols that focus on process-to-process communication across an IP network and is the only layer that directly interacts with the end user. A sophisticated Layer 7 attack may target specific areas of a website, making it even more difficult to separate from normal traffic. For example, a Layer 7 DDoS attack might target a website element (e.g., company logo or page graphic) to consume resources every time it is downloaded with the intent to exhaust the server. Additionally, some attackers may use Layer 7 DDoS attacks as diversionary tactics to steal information.

A Multi-Vector Approach

Verisign's recent trends show that DDoS attacks are becoming more sophisticated and complex, including an increase in application layer attacks. Verisign has observed that Layer 7 attacks are regularly mixed in with Layer 3 and Layer 4 DDoS flooding attacks. In fact, 35 percent of DDoS attacks mitigated in Q2 2016 utilized three or more attack types.

In a recent Layer 7 DDoS attack mitigated by Verisign, the attackers started out with NTP and SSDP reflection attacks that generated volumetric floods of UDP traffic peaking over 50 Gbps and over 5 Mpps designed to consume the target organization's bandwidth. Verisign's analysis shows that the attack was launched from a well-distributed botnet of more than 30,000 bots from across the globe with almost half of the attack traffic originating in the United States.

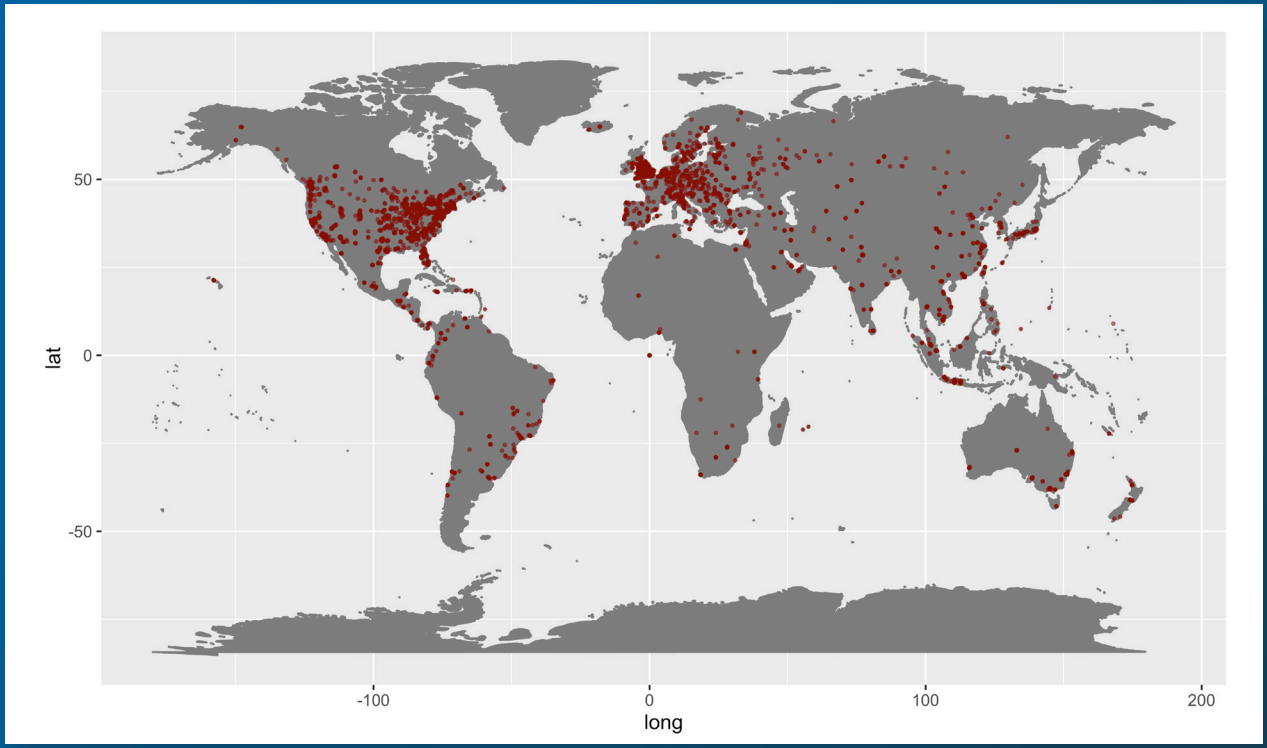


Figure 6: Map of Botnets From Recent Layer 7 Attack Mitigated by Verisign
(Note: The above geolocation is based on source IPs that may have been spoofed)

Once the attackers realized that the volumetric attack was mitigated, they progressed to Layer 7 **HTTP/HTTPS attacks**. Hoping to exhaust the server, the attackers flooded the target organization with a large number of HTTPS GET/POST requests using the following methods, amongst others:

- Basic HTTP Floods: Requests for URLs with an old version of HTTP no longer used by the latest browsers or proxies
- WordPress Floods: WordPress pingback attacks where the requests bypassed all caching by including a random number in the URL to make each request appear unique
- Randomized HTTP Floods: Requests for random URLs that do not exist – for example, if www.example.com is the valid URL, the attackers were abusing this by requesting pages like www.example.com/loc id=12345, etc.

Lessons Learned

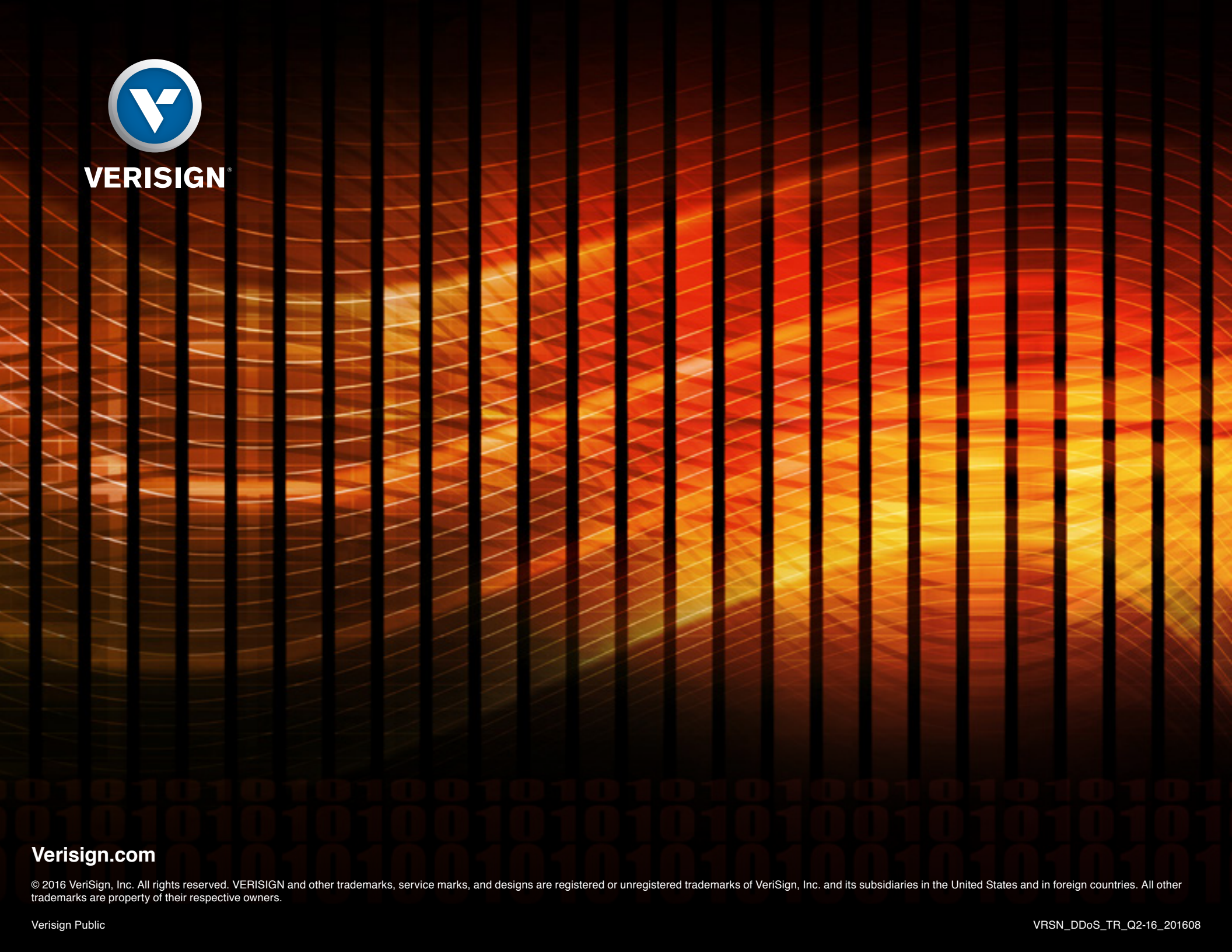
The challenge with a Layer 7 DDoS attack lies in the ability to distinguish human traffic from bot traffic, which can make it harder to defend against the volumetric attacks. As Layer 7 attacks continue to grow in complexity with ever-changing attack signatures and patterns, organizations and DDoS mitigation providers will need to have a dynamic mitigation strategy in place. Layer 7 visibility along with proactive monitoring and advanced alerting are critical to effectively defend against increasing Layer 7 threats.

As organizations develop their DDoS protection strategies, many may focus solely on solutions that can handle large network layer attacks. However, they should also consider whether the solution can detect and mitigate Layer 7 attacks, which require less bandwidth and fewer packets to achieve the same goal of bringing down a site.

TO LEARN MORE ABOUT VERISIGN DDoS PROTECTION SERVICES, VISIT 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**.



Verisign.com