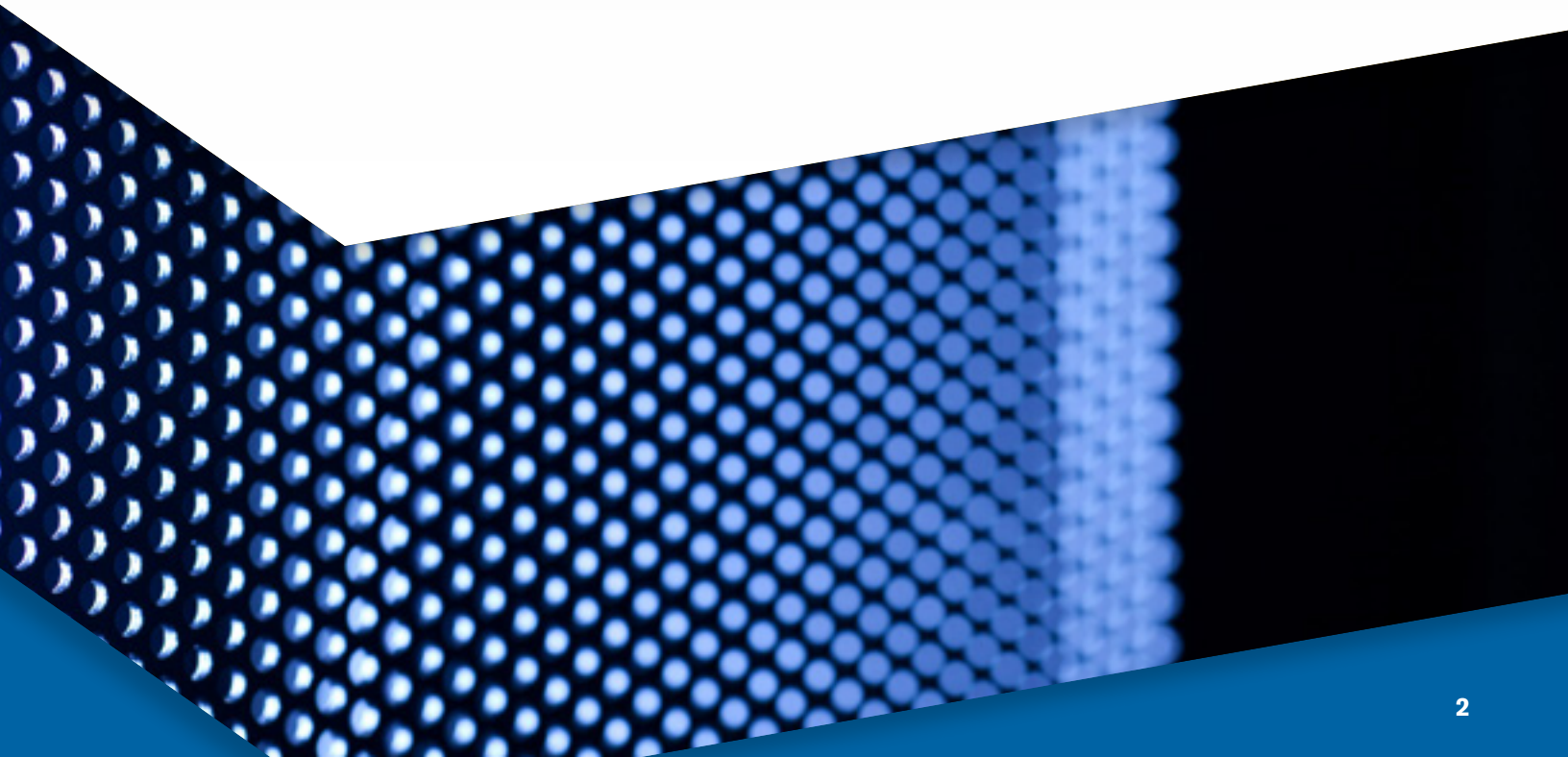
VERISIGN DISTRIBUTED DENIAL OF SERVICE TRENDS REPORT

ISSUE 2 – 2ND QUARTER 2015

VERISIGN®

VERISIGN

CONTENTS



VERISIGN

Verisign mitigated

34%

MORE ATTACKS

in the first half of 2015 than in the first half of 2014

Verisign saw the average attack size increase to

5.53 GBPS,

52%

higher than Q1 2015

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 and the security research of Verisign iDefense Security Intelligence Services. It represents a unique view into the attack trends unfolding online for the previous quarter, including attack statistics and behavioral trends.

For the period starting April 1, 2015 and ending June 30, 2015, Verisign observed the following key trends:

- Verisign's customer base saw increased activity from the DDoS For Bitcoin (DD4BC) attacker group in the form of ransom threats as well as some of those threats culminating into actual attacks. While most attacks ranged between one to five Gbps, Verisign mitigated attacks by this group peaking at 25 Gbps in July 2015 (outside of the Q2 period).
- Verisign mitigated 34 percent more attacks in the first half of 2015 than in the first half of 2014.
- The largest volumetric attack Verisign defended in Q2 was a User Datagram Protocol (UDP) flood with a mix of Network Time Protocol (NTP) and Simple Service Discovery Protocol (SSDP) traffic that targeted the Media and Entertainment industry and peaked at 82 Gbps and 22 Mpps.
- Verisign saw the average attack size increase to 5.53 Gbps, 52 percent higher than Q1 2015.
- Thirty-eight percent of attacks peaked at more than one Gbps and 20 percent of attacks were between one and five Gbps.
- For the third quarter in a row, the industry most frequently targeted by DDoS attacks in Q2 was IT Services/Cloud/SaaS, representing one-third of all mitigation activity.
- The Financial (and Payments) sector was the second most targeted industry, making up 22 percent of attacks mitigated by Verisign, up from 18 percent in Q1 2015 and largely driven by the DD4BC attacker group.
- The Media and Entertainment industry remains heavily targeted, representing 20 percent of all Verisign mitigations in Q2.
- The primary DDoS attack vector leveraged in Q2 was UDP floods consisting of NTP and SSDP traffic.

VERISIGN

DDoS attacks over

5

Gbps

made up

18%

of all attacks

VERISIGN-OBSERVED DDoS ATTACK TRENDS: Q2 2015

Mitigations by Attack Size

In Q2 2015, DDoS attacks over five Gbps made up 18 percent of all attacks, an increase of two percentage points over Q1 2015. Attack activity in the one to five Gbps category represented 20 percent of all attacks (Figure 1) mitigated by Verisign. Compared to previous quarters, Verisign saw an increased percentage of smaller attacks under the one Gbps range. Almost a third of these smaller attacks targeted the Financial industry and were driven in part by the DD4BC campaign (See Feature Article for more information) and low-level application layer attacks.

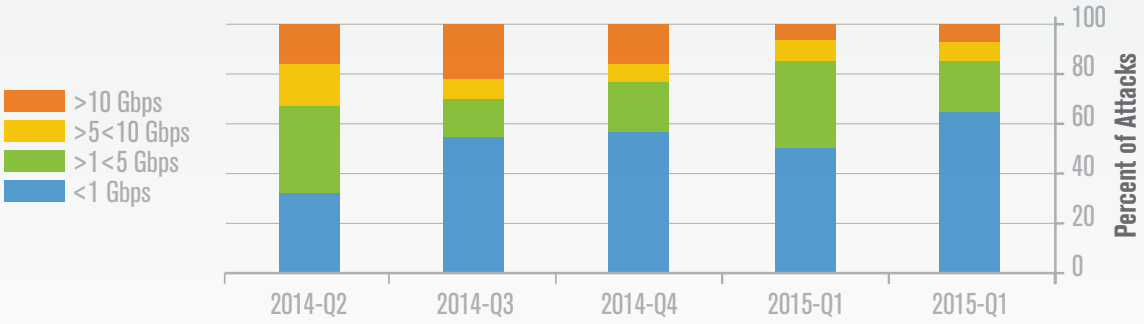


Figure 1: Mitigation Peaks by Quarter

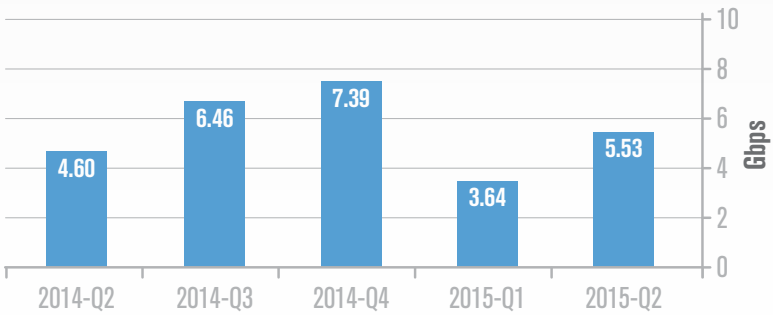


Figure 2: Mean Peak Attack Size by Quarter

Attacks mitigated by Verisign yielded an average peak size of

5

Gbps

Attacks mitigated by Verisign in the second quarter yielded an average peak size of 5.53 Gbps (Figure 2), which represents a 52 percent increase in average attack size compared to Q1 2015. The largest Q2 volumetric attack Verisign defended was a UDP flood with a mix of NTP and SSDP traffic that targeted the Media and Entertainment industry and peaked at 82 Gbps and 22 Mpps. This attack, aimed at disrupting critical online customer services, largely consisted of 10- to 15-minute spikes in traffic before the attack stopped.

VERISIGN

IT SERVICES/ CLOUD/SAAS

customers experienced the largest volume of attacks in Q2

Mitigations by Industry

DDoS attacks are a global threat and not limited to any specific industry or vertical, as illustrated in Figure 3. Verisign acknowledges that the attacks by industry reported 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.

IT Services / Cloud / SaaS customers experienced the largest volume of attacks in Q2, representing over one-third of all attacks. Attacks on this industry peaked at 80 Gbps and 11 Mpps. Financial Services was the second most frequently attacked industry, with 22 percent of all mitigations, up from 18 percent in Q1 2015. The Media and Entertainment industry remains heavily targeted, representing 20 percent of all Verisign mitigations in Q2, up from 12 percent in Q1 2015. Additionally, Verisign saw increased activity against the Telecom industry, including customers in the VoIP services segment, which was targeted by DDoS attacks that peaked at over 10 Gbps.

The ready availability of an increased number of DDoS toolkits and DDoS botnets for hire highlighted in Verisign's Q4 2014 DDoS Trends Report may be driving the increase in the overall number of DDoS attacks in the first half of 2015.

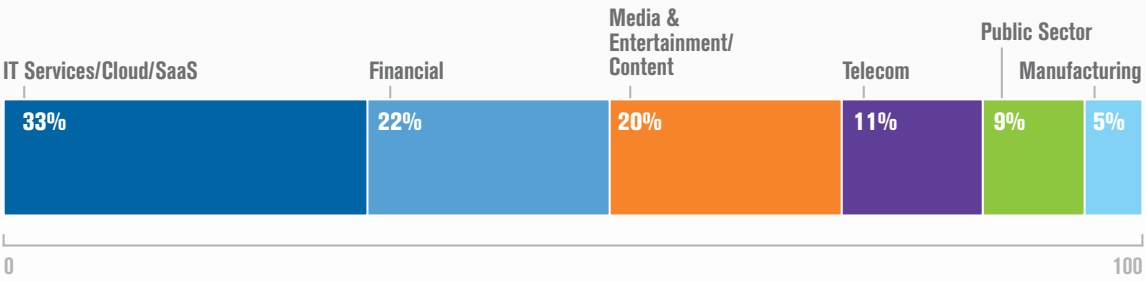


Figure 3: Mitigations by Industry

VERISIGN

Verisign mitigated

34%

more attacks in the first half of 2015 than in the first half of 2014

DDoS Attack Vector Observations

Verisign continued to see an upward trend in the number of attacks in Q2 and mitigated 34 percent more attacks in the first half of 2015 than in the first half of 2014. The most common attacks mitigated were NTP, DNS and SSDP UDP floods which accounted for approximately 70 percent of attacks in the quarter. The balance of attacks mitigated were TCP floods (20 percent) and application layer attacks (10 percent).

Application layer attacks require advanced filtering techniques and can be particularly difficult to detect since they can be effective in crippling an application without a large volumetric flood.

PROFILE: USING ADVANCED FILTERING TECHNIQUES TO COMBAT A LAYER 7 ATTACK

One of the more complex application-based DDoS events Verisign observed in Q2 involved a low-volume attack on a large financial institution. The attack was relatively small in size at less than 100 Mbps, but notable because it targeted the application layer with well-formed packets in an attempt to gain access to sensitive financial customer data. Cyber criminals targeted the application layer by hiding the attack payload within the SSL-encrypted packet. The attackers leveraged a well-distributed botnet that was timing the connections and attempting unauthorized dictionary-based credentials while flooding the customer network with a low volume SYN flood to mask the exploit attempts.

Verisign was able to block the attack traffic by employing a custom mitigation response using its proprietary mitigation platform, Athena, which has the ability to mitigate complex DDoS attacks with sophisticated dynamic traffic profiling and analysis - superior to simple flood-based attack mitigation. Verisign's Athena platform was used to mitigate this attack using a proprietary Dictionary Attack Mitigation (DAM) technique to identify appropriate filters. Once these filters were in place the attacks quickly ceased and the customer returned to normal operations. Verisign's advanced filtering technology was able to mitigate the attack without adversely affecting the legitimate traffic traversing the system.

VERISIGN

FEATURE: THE DD4BC THREAT CAMPAIGN

DD4BC sends extortion email to victim demanding Bitcoin payment to prevent DDoS attack

DD4BC sends small DDoS attack to victim to prove claim

Victim has 24 to 48 hours to pay ransom or risk a larger DDoS attack

Victim pays ransom or, if proper DDoS protection is in place, mitigates attack traffic

One of the most prolific cyber-attack stories from Q2 was that of DD4BC, a small group of people (determined by Verisign iDefense to likely be fewer than five) that has conducted extortion operations globally against at least three dozen known targets – and countless unknown – in industries including Banking, Exchanges (Bitcoin specifically) and Gaming.

DD4BC's threat campaigns usually commence with an extortion email claiming that a victim's website is vulnerable to DDoS attacks and that a one-time Bitcoin payment will ensure the victim's online operation. These extortion emails are private and accessible to only the victims. If the victims block the DD4BC email address, the group often generates a new email address within hours, resends the extortion email, and increases the Bitcoin payment requirement. What follows is usually a small DDoS attack (one to five Gbps) against the victim to prove the claim. DD4BC allows a victim 24 to 48 hours to pay the ransom before launching larger attacks, often in the range of 10 to 30 Gbps.

The Verisign DDoS Protection Services team has mitigated attacks on behalf of customers targeted by DD4BC in the form of small floods, typically TCP SYN or UDP (SSDP+NTP) floods, in the range of one to five Gbps that subsided in less than an hour. More recently, in July the group targeted e-commerce online travel organizations with attacks peaking at 25 Gbps. DD4BC has been recorded using NTP, UDP, SYN Flood and Wordpress XML-RPC reflection/amplification DDoS attacks. Additionally, DD4BC appears to use common UDP reflection DDoS attack techniques and SYN flood attacks that spoof Google crawler IP addresses to mask malicious traffic. Verisign iDefense found evidence that DD4BC carried out attacks that sent data at 20 Gbps against allcoin.com – suggesting the use of a functioning botnet – and suspects that the actors are renting DDoS-for-hire services often advertised in the underground.

Since the beginning of the year, DD4BC has increased the frequency of attacks and broadened its geographic targeting. In Q2, a report from the New Zealand Internet Task Force (NZITF) referenced extortion attempts on New Zealand and Australian companies that were threatened with DDoS attacks if a ransom was not paid. These emails contained statements with DDoS threats consistent with the format and linguistic content in extortion emails associated with DD4BC. According to NZITF, the networks of at least four New Zealand organizations, as well as a number of Australian organizations, have been affected.

Similarly, according to David Rebuck, director of the New Jersey Gaming Enforcement Division, on July 2, 2015, an unidentified malicious actor launched a DDoS attack against four New Jersey Internet gambling sites. The DDoS attack allegedly forced the sites offline for 30 minutes. According to Rebuck, "the attack was followed by the threat of a more powerful and sustained attack to be initiated 24 hours later unless a Bitcoin ransom was paid." The ransom was not paid, but the quick collaboration between

law enforcement and casino staff allowed for a mitigation of the threat and helped the online casinos avoid significant disruption. Although Rebuck did not identify the malicious actor behind this attack, according to Verisign iDefense sources, it appears that the attacks had the same modus operandi and tactics, techniques and procedures (TTPs) used by DD4BC.

While the DD4BC operation launched with a sporadic and exploratory phase, it has grown into a complex and targeted cyber crime campaign likely separated into persons conducting target reconnaissance and tool maintenance, while concurrently conducting other, separate criminal operations. The one commonality allowing DD4BC to be successful is the broad array of company networks vulnerable to DDoS attacks. A 2014 Survey on DDoS conducted by SANS Institute found that of 378 IT professionals surveyed, 39 percent either didn't have a DDoS mitigation plan or were unaware of one existing for their organization. This lack of preparedness is consistent with other similar industry research.

To combat the ever-evolving cyber threat landscape, Verisign Security Services recommends that organizations implement a strong security posture made up of an open hybrid approach to DDoS protection and an expert cyber threat intelligence service, such as Verisign iDefense, for timely and actionable cyber threat Intelligence to help identify vulnerabilities and threat actors before they affect their networks.

To learn more about how Verisign Security Services can help protect your network, visit Verisign.com/SecurityServices.

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 functions 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.