

# VERISIGN DISTRIBUTED DENIAL OF SERVICE TRENDS REPORT

ISSUE 1 – 1ST QUARTER 2014



**VERISIGN®**

## EXECUTIVE SUMMARY

This report contains the observations and insights derived from mitigations enacted on behalf of, and in cooperation with, customers of Verisign DDoS Protection Services. It represents a unique view into the attack trends unfolding online for the previous quarter, including attack statistics, behavioral trends and future outlook.

For the period starting Jan. 1, 2014 and ending March 31, Verisign observed the following key trends:

- Verisign saw an 83-percent increase in average attack size over previous quarter (Q4 2013) and an approximate 6-percent increase over the same quarter last year (Q1 2013).
- Attackers launched massive amplification attacks using NTP reflector and DNS amplification techniques against customer targets and infrastructure providers. The most common volumetric attack size ranged from 50-75 gigabits per second (Gbps).
- Approximately 30 percent of attacks against Verisign clients were targeted specifically at the application layer (the SSL layer in particular), requiring Verisign to employ advanced mitigation techniques.
- Attackers are targeting a much broader set of verticals than just the financial services sector. Media and entertainment represented the most frequently attacked vertical in Q1, followed by the IT Services/Cloud/SaaS sector.
- Verisign sees indications that attackers could further exploit other UDP protocols for large amplification attacks in the near future; this could be an attractive vector due to the simplicity and stateless nature of UDP.

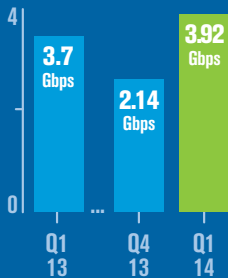


**83**  
PERCENT  
INCREASE

in average attack size  
over previous quarter







## ATTACK STATISTICS

Verisign mitigation data from the first quarter of 2014 reinforces that DDoS attacks against online businesses and Web applications continue to increase in size and complexity. During this period, Verisign saw a dramatic increase in the average peak size of DDoS attacks targeting customers. The average attack size – 3.92 Gbps – was up 83 percent over the previous quarter (Q4 2013 averaged 2.14 Gbps), and represented a 6-percent increase over the same quarter last year (Q1 2013 stood at 3.7Gbps).

In Q1 2014, NTP reflection attacks and DNS amplification attacks stood out as the two most common attack types observed by Verisign. The most common vector in Q1 2013 emanated from DNS amplification due to attacks using itsoknoprobembro, better known as Brobot, which compromised PHP and Joomla installations. The NTP attack type replaced the largest attack vectors seen last year. Verisign witnessed large NTP reflection attacks around December 2013, and the trend has continued through Q1 2014 to the time of this writing. Verisign mitigated multiple amplification attacks, ranging from 50-75 Gbps, on behalf of customers in Q1.

## BEHAVIORAL TRENDS

### Increased Adaptability

In Q1 2014, Verisign saw DDoS attackers continue to show increasingly adaptive behavior similar to that observed in 2013. On a number of occasions, attackers continuously monitored the effectiveness of their attacks while underway, and then changed attack techniques to work around applied mitigation strategies.

Attacker techniques also evolved to attack the infrastructure components of victim websites and any DDoS mitigation providers protecting those websites. Normally, attack traffic is destined for the IP address of a targeted website; using these new attack methods, attackers targeted the IP address of the various routers that sit along the network path to the target website, searching out the “weakest link.”



**50-75**  
GBPS

Average Size of Q1  
Amplification Attacks

## WHAT IS NTP?

### DESCRIPTION

Organizations use the Network-Time Protocol (NTP) to synchronize their network devices, routers, switches, firewalls, intrusion-detection systems, servers, workstations, VoIP systems and clients' devices that log onto those organizations' networks. NTP runs over the User Datagram Protocol (UDP) using port 123 as both the source and destination, which in turn runs over IP, as described in Request for Comments (RFC) 5905 for the current version of NTP, version 4. NTP provides a potential attacker with information about a system, including uptime, time since last reset, memory statistics and NTP peer listings.

### EXPLOITATION

An attacker using common tools like Metasploit and Nmap can determine open NTP servers that support monlist. The success of this attack relies on the exploitation of the monlist feature of NTP. This feature is enabled by default on older NTP-capable devices. This command sends a list of the last 600 IP addresses that connected to the NTP server to the victim. Due to the spoofed source address, when the NTP server sends the response, it is sent to the target instead of the spoofed address making the request. Because the size of the response is much larger than the request, the attacker is able to amplify the volume of traffic directed at the victim's network.

### MITIGATION

One way to decrease the effects of an ongoing NTP attack is to limit the amount of NTP traffic that is allowed to enter the network. One workaround is to disable monlist within the NTP server or to upgrade to the latest version of NTP (4.2.7), which disables the monlist functionality.



Verisign saw

**30**  
PERCENT

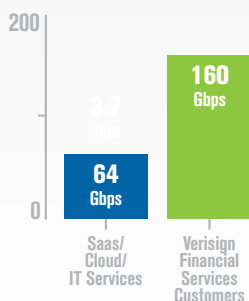
of attacks target the  
application layer

### APPLICATION-LAYER TARGETING

Of attacks mitigated by the DDoS Protection Services platform, Verisign saw approximately 30 percent targeting the application layers, and specifically the SSL layer. These attackers targeted specific Web applications, protocol headers and application parameters to impact the availability of the targeted victim. While these attacks were often smaller in overall volume, they represented more complex attacks, requiring Verisign to apply sophisticated mitigation techniques, often comprising a combination of real-time signature generation, packet inspection, and diverse client capability handling and resource management techniques. Verisign's proprietary Athena DDoS mitigation platform, supported by internally shared threat intelligence from Verisign iDefense Security Intelligence Services, proved highly effective in mitigating these complex attacks.

### EXPANDED TARGETING OF MULTIPLE INDUSTRIES

Also of note in Q1 2014, attackers increasingly targeted industries besides financial services. Verisign saw media and entertainment customers the most frequently attacked, followed by IT Services/Cloud/SaaS sector (see Figure 1). The number of Verisign mitigations on behalf of financial services customers decreased 34 percent in Q1 2014 compared to all of 2013. The percentage of mitigations performed for Media/Entertainment and e-commerce sectors increased 33 percent as compared to 2013. IT Services/Cloud/SaaS vertical saw the largest attacks, peaking at 64 Gbps, compared to the largest 2013 Verisign customer attack sizes, which peaked at more than 160 Gbps and were directed against financial services customers.



### WHEN FIGHTING DDOS, NETWORK SIZE MATTERS

Effective mitigation against volumetric attacks requires a sophisticated network footprint and expertise from service providers. DDoS attack traffic can originate from any region in the world and any given attack profile can inundate regional provider mitigation centers without the capabilities and flexibility of a globally interconnected backbone.

Verisign's DDoS mitigation network is strategically engineered to handle both nominal traffic loads in addition to large traffic spikes which occur under DDoS attack conditions. The flexible MPLS configuration allows Verisign's DDoS engineers to selectively engineer and route traffic flows in response to global DDoS attack dynamics so that no single component is overwhelmed.

### Q1 2014 MITIGATIONS BY VERTICAL

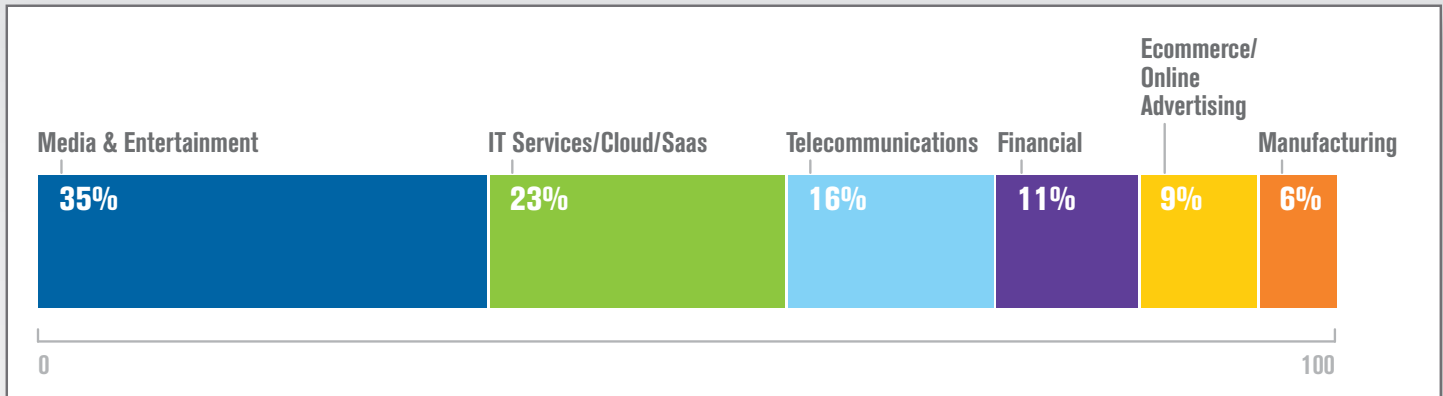


Figure 1: Verisign Mitigations by Customer Industry

### FUTURE OUTLOOK

The DDoS attack landscape is changing every day, and attackers are deploying new techniques, targeting a much wider set of organizations and becoming more sophisticated. Based on trend analysis, Verisign anticipates DDoS attacks to continue to evolve in size and complexity in subsequent quarters and throughout 2014.

While DNS amplification attacks are still common, and NTP reflection attacks have emerged, Verisign expects new amplification and reflection attack types to appear and proliferate. These attacks will likely exploit additional protocols and port types, and could potentially catch unprepared organizations and even DDoS mitigation providers by surprise in short order. Other UDP protocols that are potential targets are SNMP and IKE, which can be used to launch source-IP-spoofed attack types and have the potential to be amplified similar to DNS or NTP.

For more information about DDoS attacks, best practices for defense, and Verisign DDoS Protection services, visit [VerisignInc.com/DDoS](http://VerisignInc.com/DDoS).

“Verisign expects new amplification and reflection attack types to appear and proliferate.”