F5 Silverline DDoS Protection Mitigates 448 Gbps DDoS Attack

By **Ilan Meller**

Distributed Denial of Service (DDoS) is a common attack method used by hacker groups and individuals to severely hamper or shut down an organization's online services, causing both monetary and reputation losses. Whereas DDoS attacks have been common since the late 2000s, attack sizes have increased significantly in the past few years. New protocol exploits and amplification attacks have become too large for most organizations to combat without the support of a cloud-based DDoS scrubbing service. In 2013, it was reported that SpamHaus services were brought down "thanks" to a 300 Gbps attack, then in 2014, an attack peaking at 400 Gbps was recorded. However, the world's largest DDoS attack in history (with records to prove it) was captured in 2015 with a peak of 500 Gbps.

An interesting story was published in multiple media channels in January this year when a group calling itself New World Hacking said it initiated a successful 602 Gbps DDoS attack, targeting BBC websites. However, even while the group was marketing itself and its supposed largest DDoS attack in history, there was no real evidence of such attack. The group claimed it used Amazon's cloud service to conduct the attack and it "programmed a bypass linked to proxies" so monitoring firms "wouldn't detect it, anyway." A source with direct technical knowledge of Amazon's systems and internal processes, who did not want to be named as he or she was not authorized to speak on the record, dismissed the allegation, saying that it "doesn't line up" with how Amazon's cloud services work.

Around the same time that New World Hacking went public with its story, the F5 Security Operations Center (SOC) started seeing an increase in volumetric DDoS attacks. The F5 SOC has already mitigated ten ongoing attacks that peaked north of 100 Gbps in 2016, four over 200 Gbps, and two over 400 Gbps.

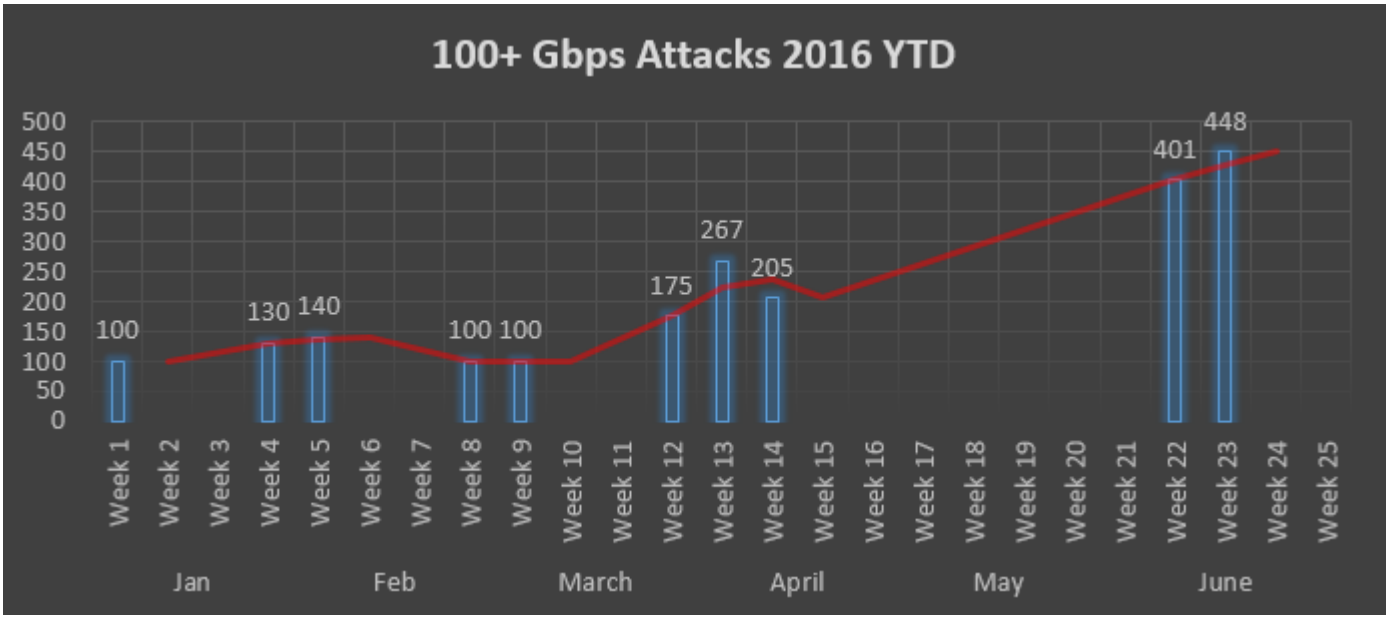
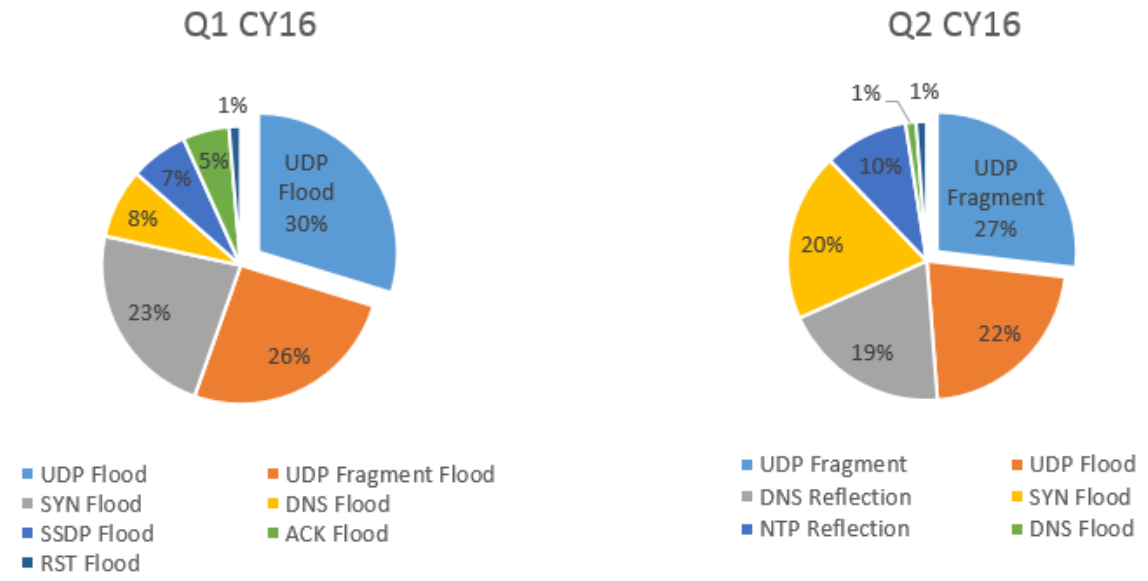


Figure 1: Peak attack bandwidth in Gbps, 2016 YTD, as mitigated by F5 Silverline DDoS Protection

Whereas the quantity of large volumetric attacks in Q1 was higher, the size of attacks grew exponentially in Q2, peaking at 448 Gbps in June. As expected, we are seeing flux in attack types quarter over quarter. UDP remains the most popular protocol for exploit whereas DNS and NTP exploits have been ramping up in Q2.



Figures 2 & 3: Q1 and Q2 attack types as detected by F5 Silverline DDoS Protection

“The F5 SOC observed a sizeable 448 Gbps UDP/ICMP fragmentation flood destined primarily towards one specific subnet,” said Nic Garmendia, the F5 SOC analyst who monitored the attack, making sure mitigation was in place. “It ramped up extremely quickly and dropped drastically back down over the length of about nine minutes. As is common in UDP floods, the attackers sent highly-spoofed UDP packets at a very high packet rate using a large distributed source IP range. In this specific attack, over 100,000 IP addresses were used. Human intervention in order to apply mitigation was unnecessary upon detection as UDP ACLs began dropping the attack at the border.”

Below is the breakdown of attack traffic per data center, peaking at a total of 447.7 Gbps.

	Bandwidth (Gbps)
Data Center 1	130.4
Data Center 2	154.3
Data Center 3	82.2
Data Center 4	80.8
TOTAL	447.7

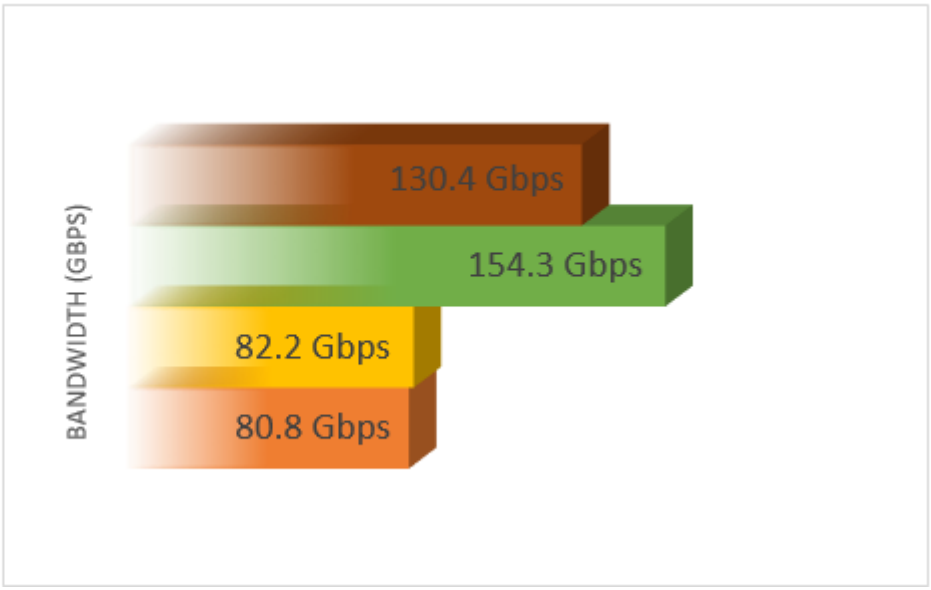


Figure 4: Pre-mitigated traffic summary by F5 Silverline DDoS Protection (in Gbps)

During the latest 448 Gbps attack, the F5 SOC revealed that the source countries and ASNs used for this attack spread worldwide, a common method used to decrease the likelihood of authorities catching the perpetrators.

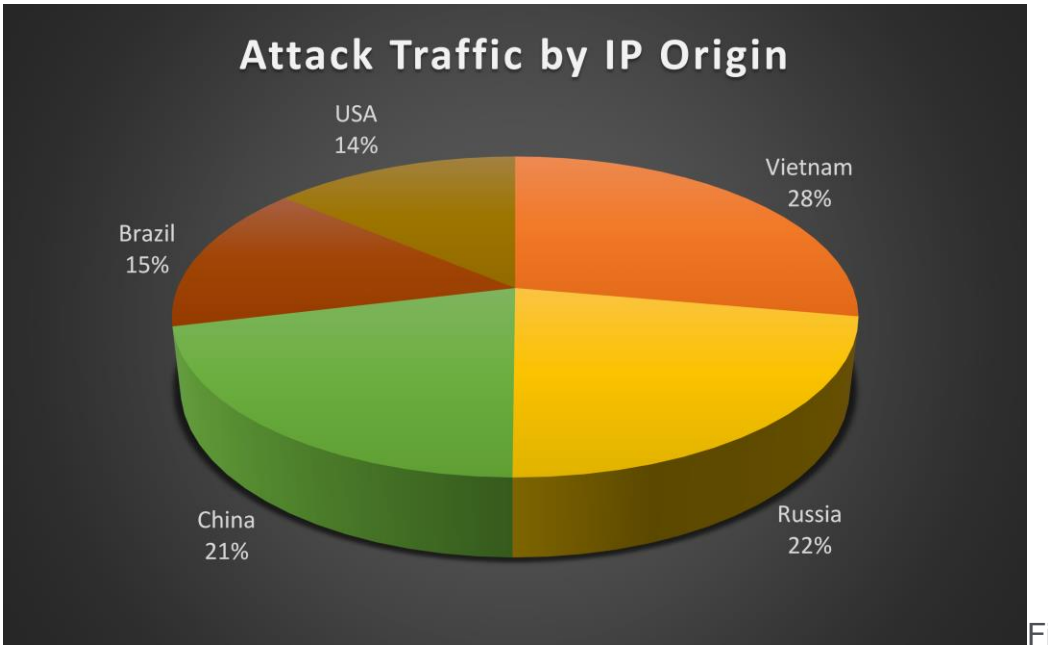


Figure 5: Botnets segmentation by source country

Who was Behind the Attack?

No one has claimed responsibility for this attack as of yet, and mitigation efforts are ongoing. What we can say is the attack destination is a U.S.-based financial institution that is routinely targeted. A quick Google search can lead to some assumptions regarding current campaigns that target financial institutions by a well-known hacker collective.

DDoS, like all other Internet-based attacks, show no signs of slowing down, only increasing in sophistication, attack volume, and frequency.

About F5 DDoS Protection Services

F5® Silverline™ DDoS Protection is a service delivered via the F5 Silverline cloud-based application services platform. It detects and mitigates DDoS attacks in real time, with industry-leading DDoS attack mitigation bandwidth to stop even the largest of volumetric DDoS attacks from ever reaching your network. F5 Security Operations Center experts deploy, manage, and support Silverline cloud-based application services 24x7.

Silverline DDoS Protection can be implemented independently or together with F5's on-premises DDoS solution for detecting and mitigating mid-volume, SSL, and application-targeted attacks. When implemented together, you get the most comprehensive L3–L7 DDoS protection. You can keep your business online when under DDoS attack with real-time DDoS mitigation response times, unparalleled visibility and reporting, cost efficiencies, and reduced risk of downtime. F5 is the first leading application services company to offer a hybrid solution for DDoS protection.