Prolexic Attack Report

Q4 2011

Prolexic believes the nature of DDoS attacks are changing: they are becoming more concentrated and damaging. Packet-per-second volume is increasing dramatically, while attack duration is declining.

PROLEXIC
DDoS Attacks End Here.

Emerging trends

At a Glance

Compared to Q410

- 7x increase in total mitigated DDoS traffic
- 18x increase in packet-per-second volume
- Shorter attack duration: 43 hours vs. 34 hours
- The total number of attacks increased 45%
- The number of Layer 7 attacks almost doubled

Other facts this quarter

- Country originating most attacks: Japan
- Average attack duration was 34 hours
- Average attack bandwidth was 5.2 Gbps

Increases in the frequency and intensity of DDoS attacks are not uncommon in the fourth quarter or "holiday shopping season" as attackers target e-Commerce providers and ancillary service partners. Even so, Q411 was characterized by an unexpectedly large and foreboding surge in the number of DDoS attacks in comparison to the same quarter one year ago. Of concern is the increase in attack size and packet-per-second volume that Prolexic has charted this quarter. Prolexic sees this sea change as a warning sign that 2012 will be an exceptionally challenging year for online businesses as they try to develop effective countermeasures to increasingly devastating DDoS attacks.

Prolexic logged a 7-fold increase in total bandwidth and a 45% rise in the number of DDoS attacks against its clients compared to Q410. In addition, we saw an unprecedented 18-fold increase in packet-per-second mitigated volume compared to the same quarter last year. Attack duration declined from 43 hours in Q410 to 34 hours this quarter.

Q411 was a very active quarter and compared to Q3, the total number of attacks against Prolexic clients increased by almost 50%. When comparing attack types, we saw a mild uptick in Layer 7 (application layer) attacks in Q411, rising from 17% in Q3 to 21% in Q4. Correspondingly, Layer 3 and Layer 4 (network/transport layer attacks) declined in Q4 to 79% from 83% in Q311. While average attack duration remained constant at approximately 34 hours, Prolexic logged a significant increase in average attack bandwidth, which increased from 2.1 Gbps in Q311 to 5.2 Gbps. November was the busiest month for attacks, while the week with the highest number of attacks was December 3-10.

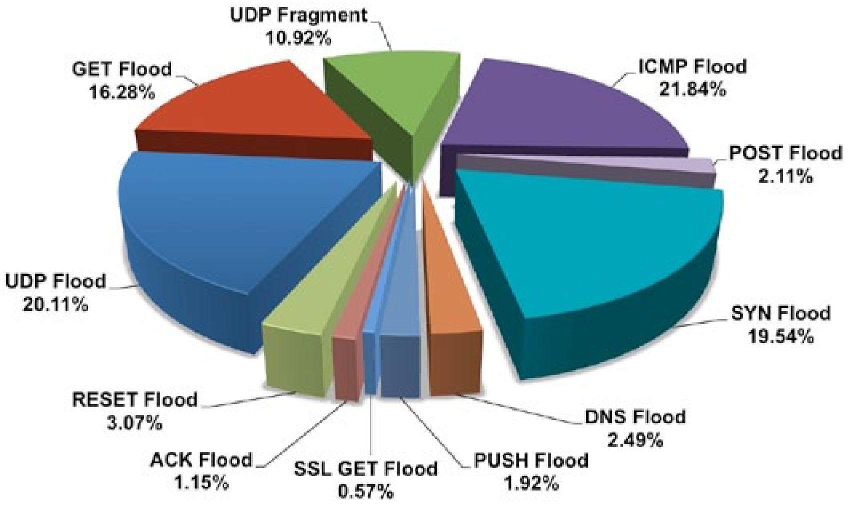
Comparing 2011 and 2010

As Q4 represents the end of the calendar year, it provides an opportunity to compare 2010 and 2011 as a whole. Some interesting data points emerged that can be useful in understanding the changing nature of DDoS attacks. The total number of attacks increased marginally in 2011 over 2010 – by just 2%. Attack types over the two years also remained surprisingly constant with only a slight difference. In 2010, Layer 7 and Layer 3 attacks totaled 26% and 74% respectively. In 2011, Layer 7 and Layer 3 attacks totaled 26.5% and 73.5% respectively. However, not everything is status quo. The average mitigated bandwidth increased by 236% in 2011 compared to 2010. Prolexic expects the number of Layer 7 attacks to increase in 2012 and packet-per-second volume to continue to ramp up. This trend increases the importance of effective traffic monitoring and analysis tools at Layers 3, 4 and especially 7. The faster a DDoS attack can be recognized and analyzed, the faster it can be mitigated, minimizing downtime and potential revenue loss.

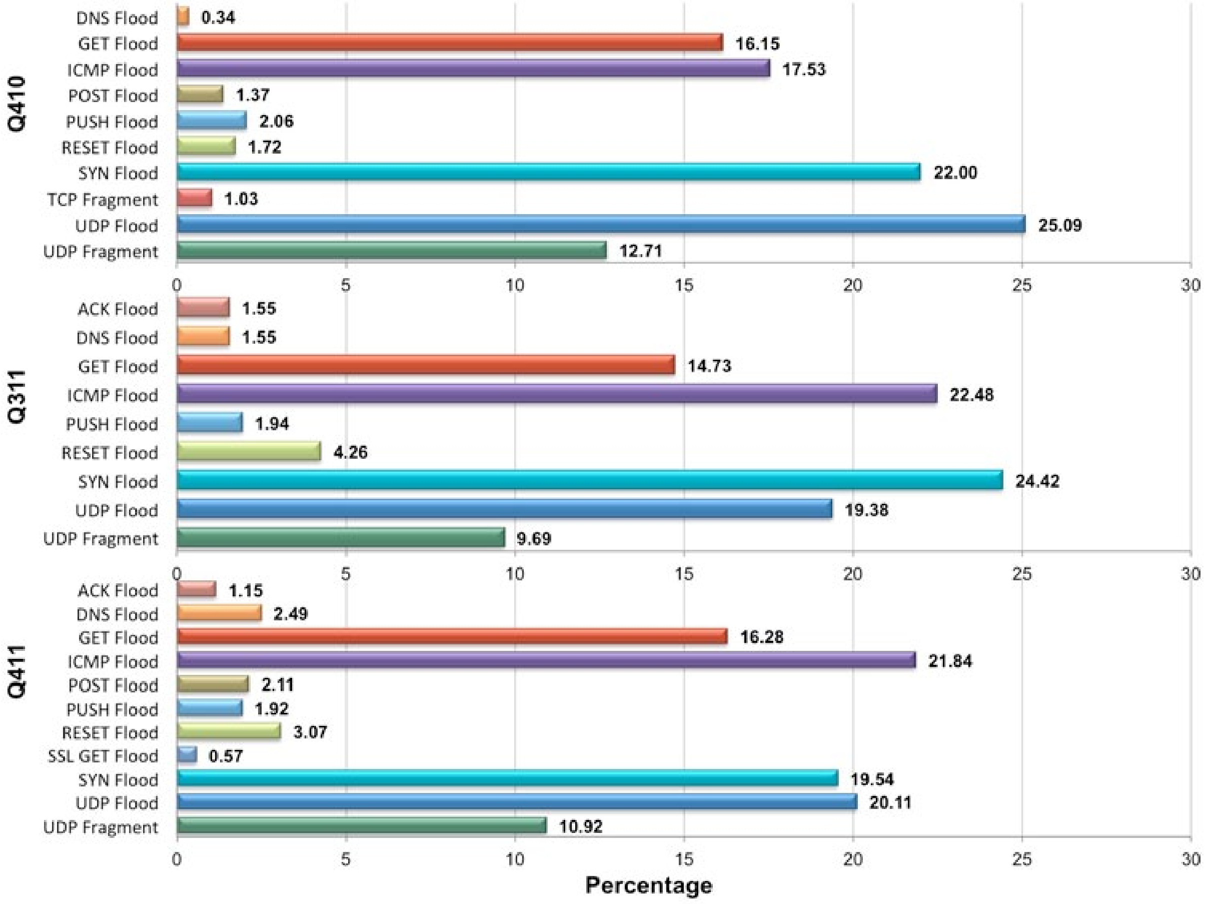
Report overview continues on page 10

Total Attack Types (Q411)

Prolexic mitigated a total of 45% more individual DDoS attacks in Q411 compared to Q410. When broken down by attack type, approximately 22% were ICMP floods, 20% were UDP Floods, 20% were SYN Floods and 16% were GET Floods this quarter. Compared to Q410, ICMP Floods have increased slightly in the last two quarters of 2011.



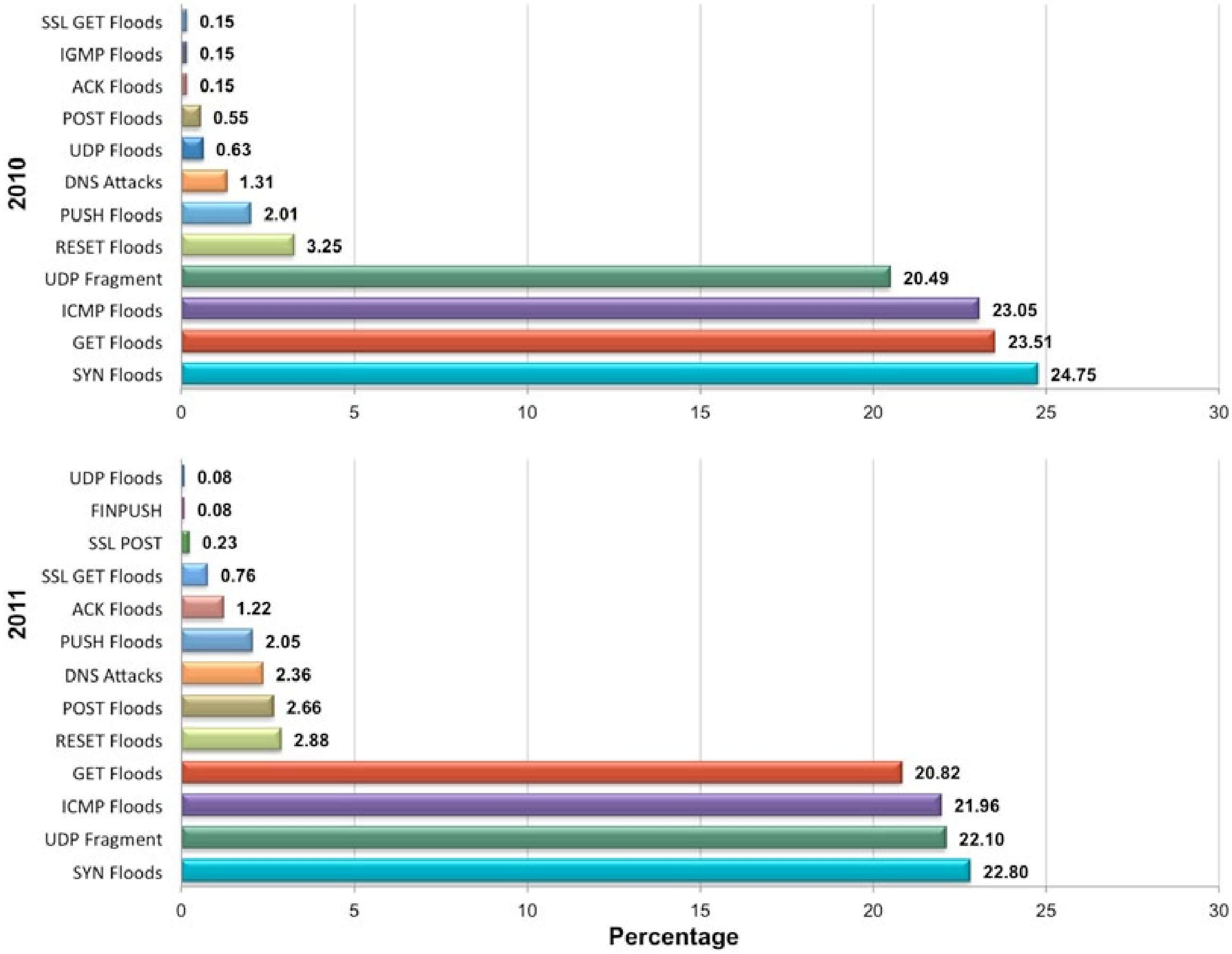
Comparison: Attack Types (Q410, Q311 and Q411)



Attack Types (2010 vs. 2011)

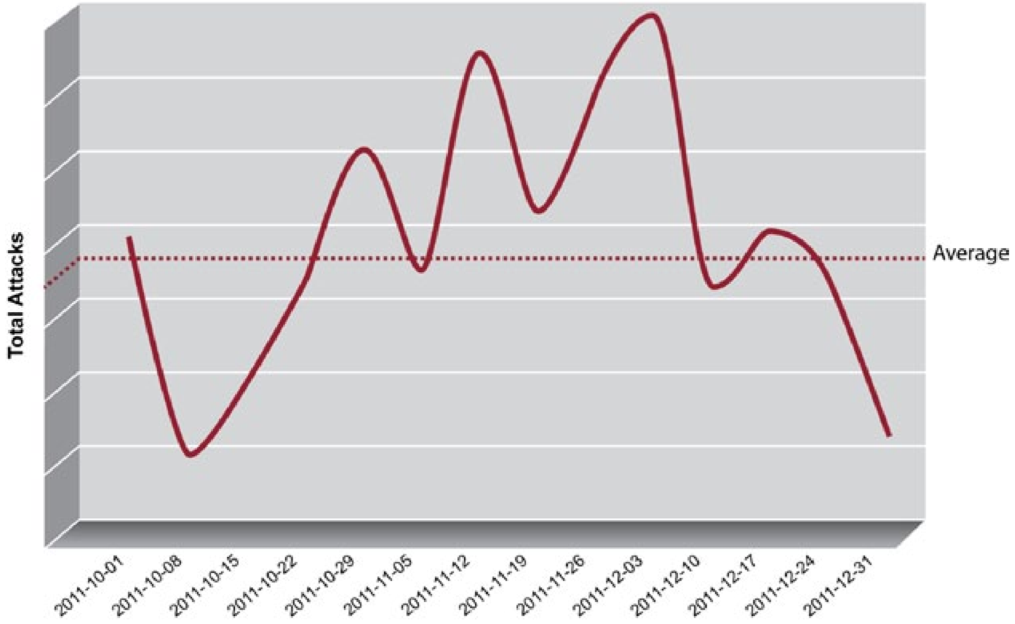
When comparing 2010 and 2011, certain attack types have maintained their popularity. Mitigated SYN floods were at 24.75 % in 2010 and 22.80 % in 2011. This attack type still remains as the most popular DDoS variant being used against Prolexic's protected customers. Following close behind is the application layer GET Flood, which has been consistently used by attackers, accounting for 23.51 % in 2010 and 20.82 % in 2011.

Several attack types have increased in when we look at 2011 vs. 2010. The highlighted campaigns include DNS, POST, and SSL GET floods. These are considered more difficult attacks to defend against and require sophisticated mitigation strategies to be implemented



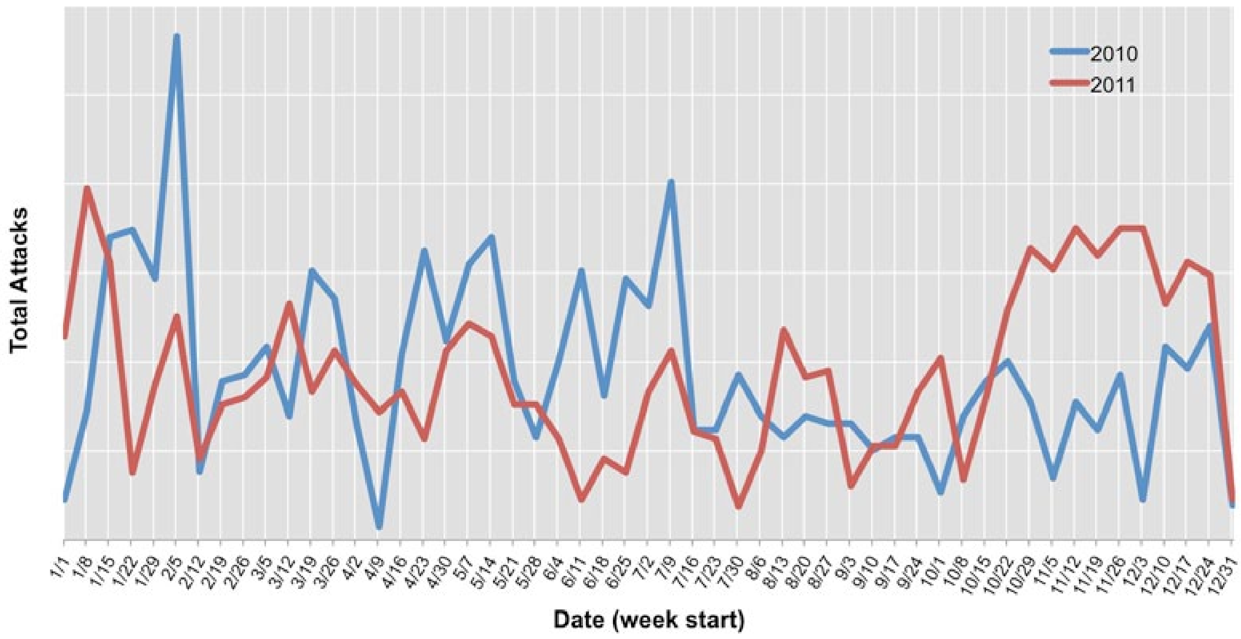
Total Attacks per Week - Q411

November was the busiest month for DDoS attacks against Prolexic customers this quarter, while the busiest week was December 3-10.



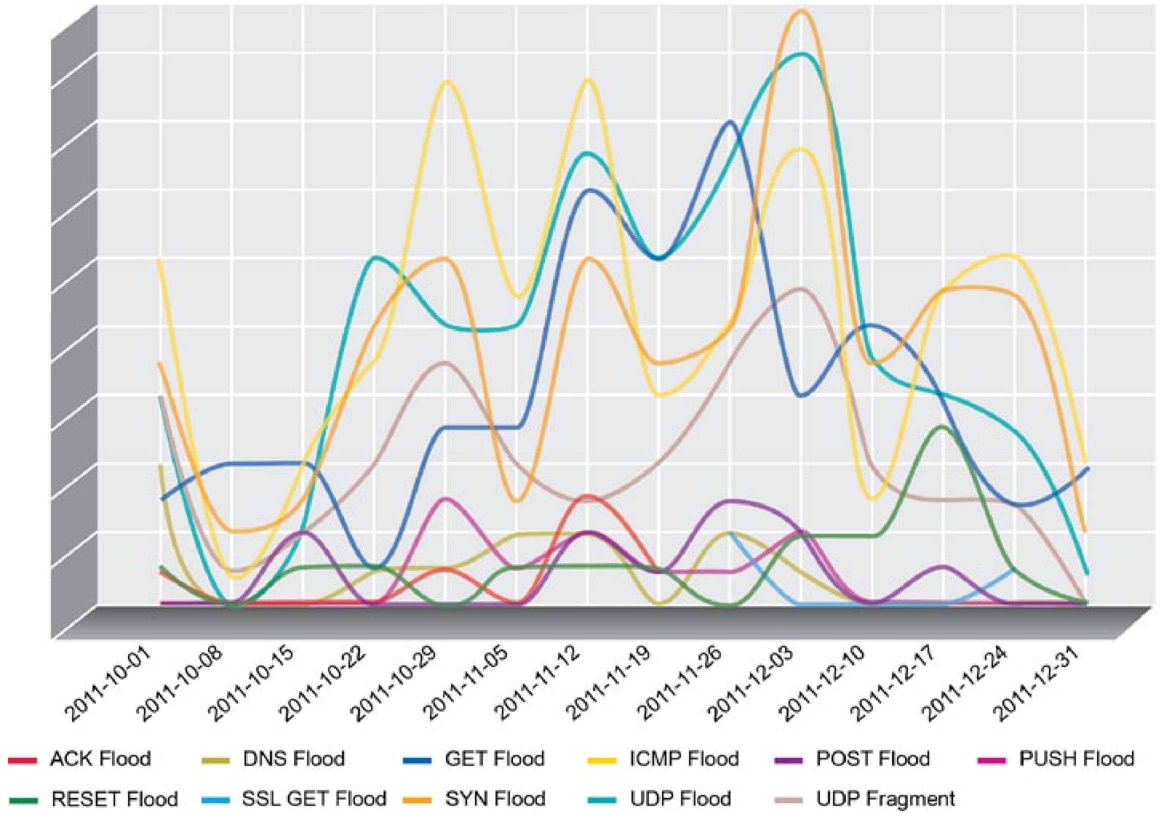
Total Attacks per Week (2010 vs. 2011)

This graph represents the number of attack campaigns launched against Prolexic Technologies customers within a full calendar year. The direct comparison between 2010 and 2011 depicts an interesting statistical metric. During the months of October through December, attackers have created a sustainable effort to launch campaigns – data shows an increase from last year. Increased strength in botnet frameworks utilized during these time frames affect multiple industries. However, based on PLXsert data analysis, the most popular targets were e-Commerce and ancillary service businesses.

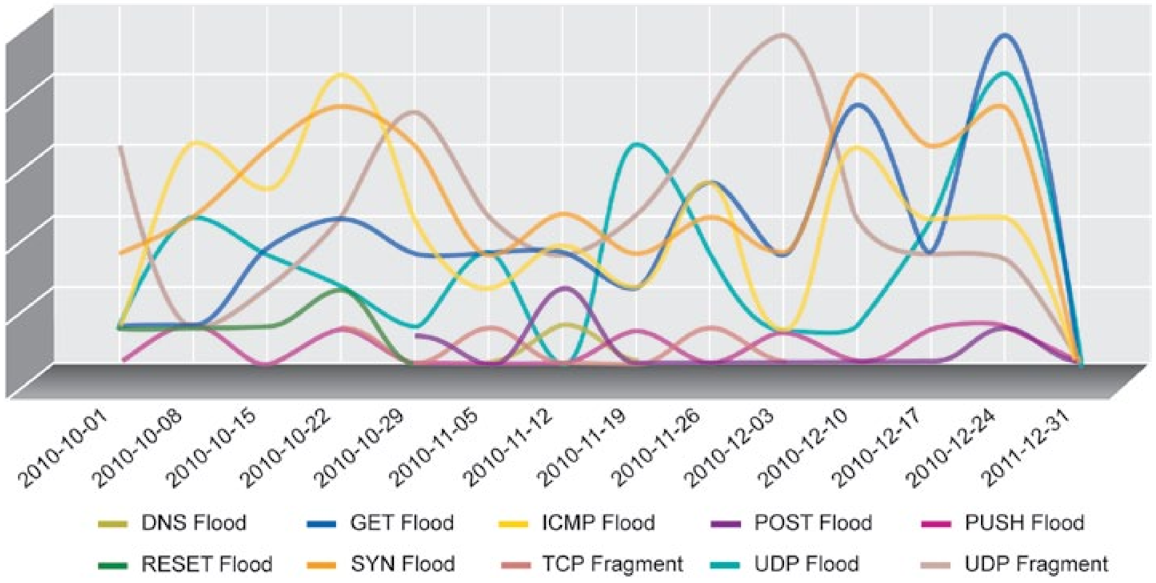


Total Attacks per Week by Types - Q411

This quarter, attackers chose to use more ICMP and SYN Floods, especially during the last few weeks of the year. In Q410, UDP Floods and GET Floods were more prevalent in the weeks before Christmas.

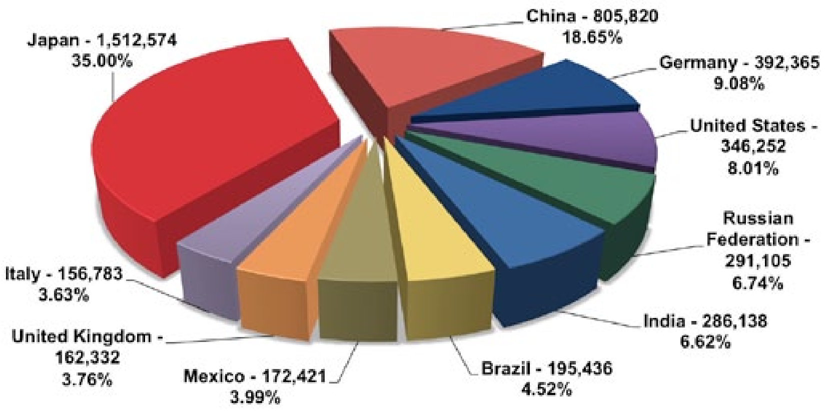


Total Attacks per Week by Types - Q410



Top Ten Source Countries (Q411)

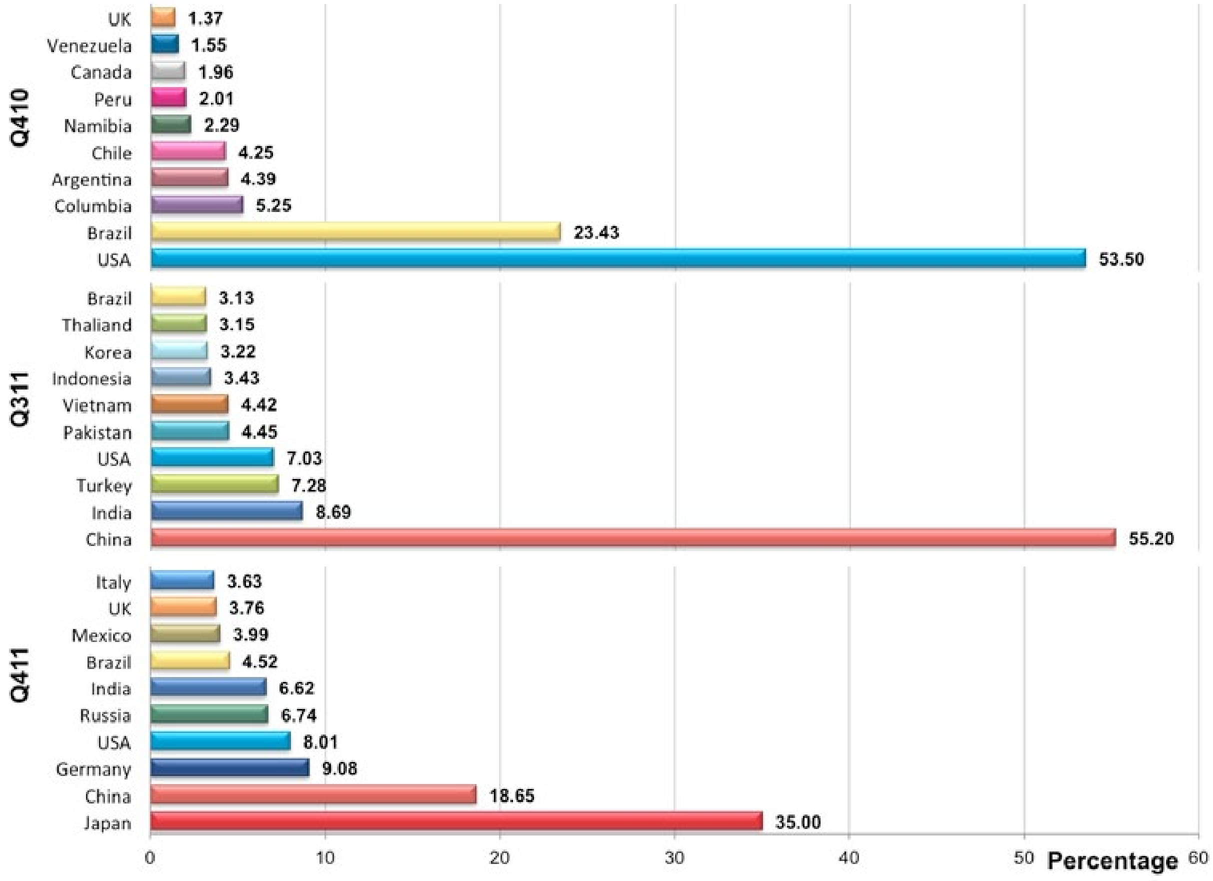
Japan (1st), China (2nd), and Germany (3rd) are currently the top three origins of DDoS attacks, according to Prolexic's accumulated DDoS statistics.



Comparison: Top Ten Source Countries (Q410, Q311, Q411)

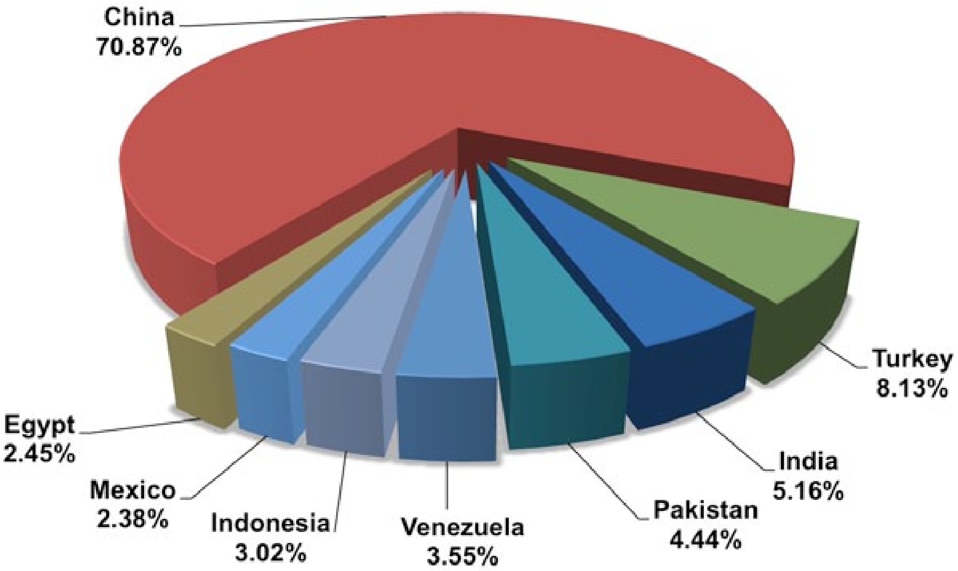
As of Q411, Japan is the leading source of new malicious hosts participating in DDoS attacks. While topping the list this quarter, Japan is typically not an originating source of DDoS attacks. In previous reports, China was the leading source of malicious DDoS hosts (Q311) and exactly one year ago (Q410) the USA was the leading source of new malicious DDoS hosts. In all, 234 geographic locations were sources of botnets.

There is no firm evidence why Japan has assumed a leadership position this quarter, but we can speculate that the disasters in that country have caused infrastructure changes that led to an increased infection rate of hosts and increased Japanese participation in globally controlled botnets.



Top Ten Source Countries (Overall)

This list represents the top ten overall ASNs that have sourced malicious traffic to Prolexic's infrastructure. This data does not represent IP addresses that did not pass our anti-spoof mechanisms.

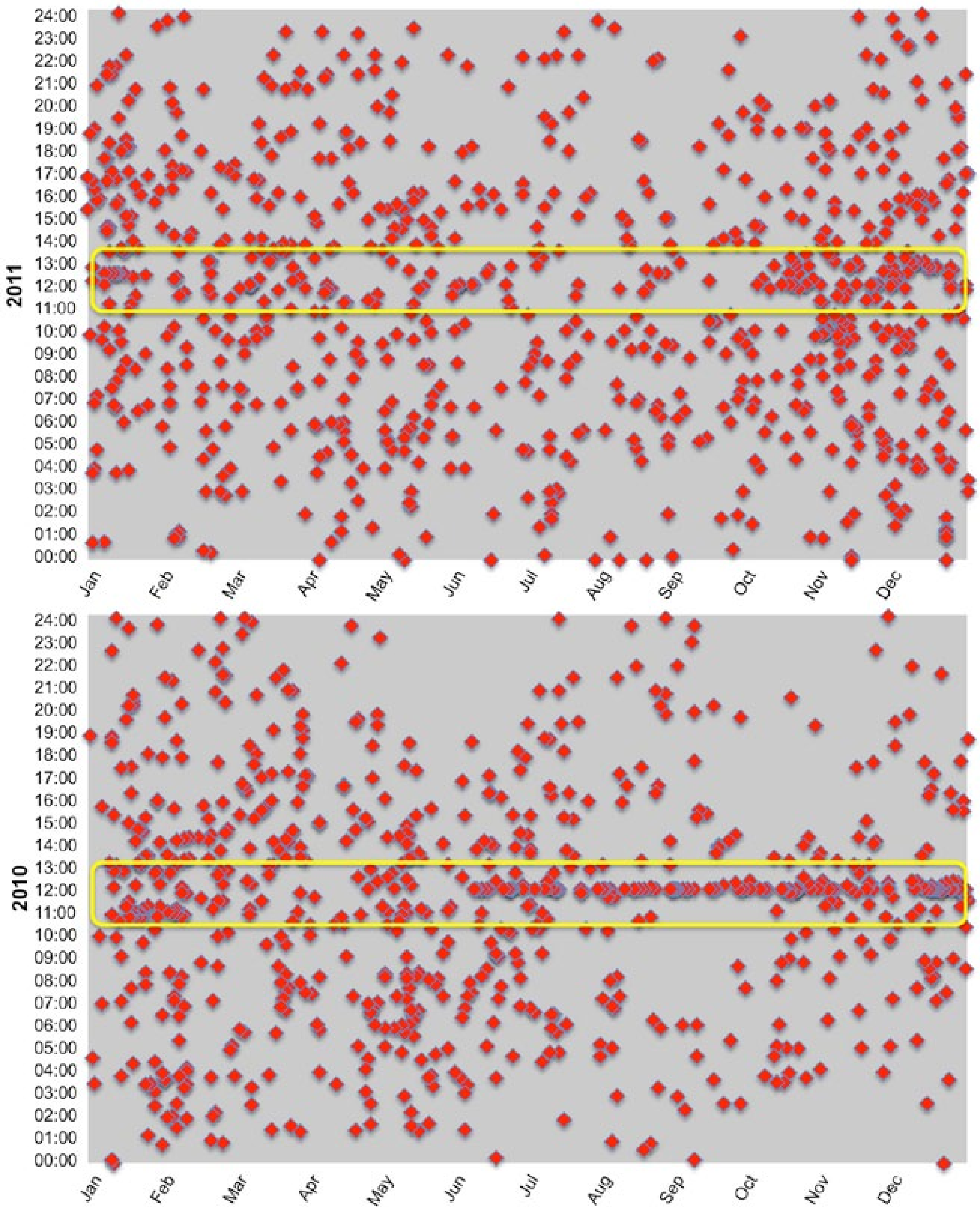


Country	Registry	ASN	ASN Count
China	apnic	4134	1933354
China	apnic	4837	909057
Turkey	ripencc	9121	336784
India	apnic	9829	213768
Pakistan	apnic	45595	183957
Venezuela	apnic	45899	147005
Indonesia	apnic	17974	125072
Egypt	afrinic	8452	101325
Mexico	lacnic	8151	98616
China	apnic	9394	94284

Attack Campaign Start Time per Day (2010 vs. 2011)

For the majority of 2011, attack start times have been well distributed. However, it is clear from the chart below that the most common attack campaign start time is 12:00 GMT. In Q411, start time moved closer to 11:00 GMT. It should be noted however, that DDoS attacks typically occur when the most impact can be made – for example, before or during a special promotion or similar event.

Being that Q4 was anomalous compared to other quarters, one could speculate that this has everything to do with the holiday season. Prolexic plotted e-Commerce statistics against other attack data. These graphs indicate that the highest concentration of attack start times is between 10:00 and 14:00 GMT.



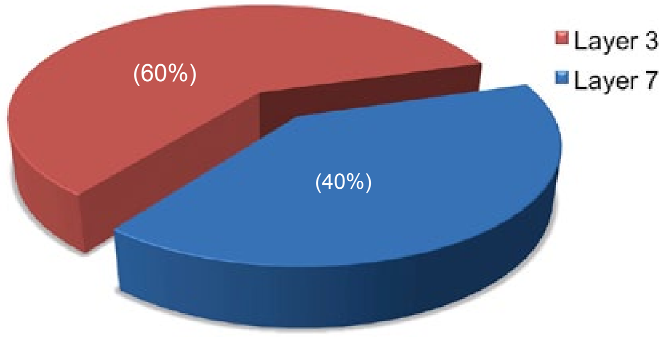
The fourth quarter was also characterized by a somewhat surprising surge in DDoS attacks from botnets with large concentrations of bots in Japan, a geographic location rarely in the top ten source countries and usually not known for large concentrations of botnets. Prolexic speculates that this activity may stem from infrastructure changes that led to an increased infection rate of hosts due to the setting up of impromptu communication networks after the 2011 tsunami and nuclear plant disaster. Prolexic speculates that this activity may stem from temporarily lax security practices when many global vendors set up impromptu communication networks after the tragedy in Japan.

Another interesting change in the top ten source list is that the United States has fallen to number 4 in Q411 in contrast to being at the top of the list a year ago. Prolexic believes that U.S. companies are getting better at locking down their infrastructures and therefore reducing their vulnerability to being an unsuspecting participant in botnet activity. It is clear individuals and organizations in the U.S. have become more educated about how computer technology works, how to recognize viruses and malware, and are improving the protection of their systems against malicious hackers.

Vertical Industry Analysis

This quarter, due to the holiday shopping season, Prolexic focused attack report observations on the e-Commerce sector. Attacks were primarily directed at the infrastructure (Layer 3 and 4) and applications (Layer 7). It is notable that this quarter, data showed this sector received a disproportionately high percentage of Layer 7 attacks (40%). Average attack duration for e-Commerce was 80 hours with an average attack bandwidth of 622 Mbps. Attack duration directed at this vertical was significantly higher than normal this quarter; attack duration against Prolexic clients in other industries averaged just 32 hours in comparison.

Mitigated Attacks on e-Commerce Industry (Q411)



Looking forward

As DDoS attackers begin to pull in more resources and unleash higher packet-per-second attacks, the Internet will be a far more dangerous place in 2012 for online companies – and mitigation providers – that do not have the infrastructure or bandwidth to defend against these attacks. To stay ahead of the curve, Prolexic continues to invest heavily in increasing network capacity, staffing, and research and development.

About Prolexic Security Engineering & Response Team (PLXsert)

PLXsert monitors malicious cyber threats globally and analyzes DDoS attacks using proprietary techniques and equipment. Through data forensics and post attack analysis, PLXsert is able to build a global view of DDoS attacks, which is shared with customers. By identifying the sources and associated attributes of individual attacks, the PLXsert team helps organizations adopt best practices and make more informed, proactive decisions about DDoS threats.

About Prolexic

Prolexic is the world's largest, most trusted Distributed Denial of Service (DDoS) mitigation provider. Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission critical Internet facing infrastructures for global enterprises and government agencies within minutes. Six of the world's ten largest banks and the leading companies in e-Commerce, SaaS, payment processing, travel/hospitality, gaming and other at risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world's first "in the cloud" DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida and has scrubbing centers located in the Americas, Europe and Asia. For more information, visit **www.prolexic.com**, email **sales@prolexic.com** or call **+1 (954) 620 6002**.