Prolexic Attack Report

Q1 2012

Financial services firms get hit by
DDoS attacks as malicious packet volume
increases 3,000% quarter over quarter.

PROLEXIC
DDoS Attacks End Here.

Analysis and emerging trends

At a Glance

Compared to Q1 2011

- 25% increase in total number of DDoS attacks
- 25% increase in Layer 7 (application layer) attacks
- Shorter attack duration: 28.5 hours vs. 65 hours
- Decline in use of UDP Floods

Compared to Q4 2011

- Total number of attacks was constant
- 6% rise in Layer 7 attacks
- Average attack duration declined to 28.5 hours from 34 hours
- China remains the top source country for attacks but the U.S. and Russia both move up in the rankings

The Prolexic Security Engineering and Response Team (PLXsert) logged a significant (25%) increase in the total number of attacks in Q1 2012 compared to the same quarter last year. However, the split between attack types remained virtually identical: 73% were infrastructure attacks (Layer 3 and 4) while 27% were aimed at the application layer (Layer 7). The most popular Layer 3 infrastructure attacks were SYN floods, ICMP floods, UDP floods and UDP fragment floods. The most popular Layer 7 application attacks were GET Floods and POST floods.

The choice of attack type has shifted significantly over the last 12 months. UDP floods are less common with SYN Floods emerging as the "go to" attack type. In fact, SYN Floods accounted for a quarter of all attacks in Q1 2012, in line with last quarter's observations. Compared to Q1 2011, average attack duration has declined (28.5 hours vs. 65 hours).

During the first quarter, January was by far the most active month for DDoS attacks, accounting for 41% of the quarter's total attacks. The number of attacks declined throughout the quarter with January being the most active and March being the least active. The most active week of the quarter was February 12-19, which accounted for 40% of the month's total attacks.

During the first quarter, PLXsert logged a significant increase in DDoS attacks against financial services organizations, both in quantity and intensity. The total number of attacks against the financial services sector almost tripled compared to Q1 2011. Among attacks within this sector, the PLXsert team charted considerable increases in both bandwidth and packet per second rates over the quarter. For more details on DDoS attacks against the financial services vertical market, please refer to the analysis on page 3.

Compared to Q4 2011

While the fourth quarter is often an active month for DDoS attacks due to the holiday season, Q1 2012 was equally busy with a slight decrease in the total number of attacks compared to Q4 2011. Interestingly, PLXsert logged a 6% increase in application layer (Layer 7) attacks compared to the previous quarter.

Average attack duration continued to edge down, dropping from 34 hours in Q4 to 28.5 hours this quarter. Of note, the average attack bandwidth increased to 6.1 Gbps, up from 5.2 Gbps in the previous quarter. Taken together, these two metrics indicate a continued trend toward more powerful, but shorter attacks. This is true both when comparing data quarterly (Q1 2012 to Q4 2011) as well as annually (Q1 2012 to Q1 2011).

As for the top countries originating DDoS attacks, rankings returned to a more traditional order this quarter. China (1st), United States (2nd), and Russian Federation (3rd) were the top three origins of DDoS attack campaigns. Japan, last quarter's leader, fell to 26th place, confirming Prolexic's assertion in last quarter's report that this was a one-time anomaly.

Vertical Industry Analysis - Financial Services

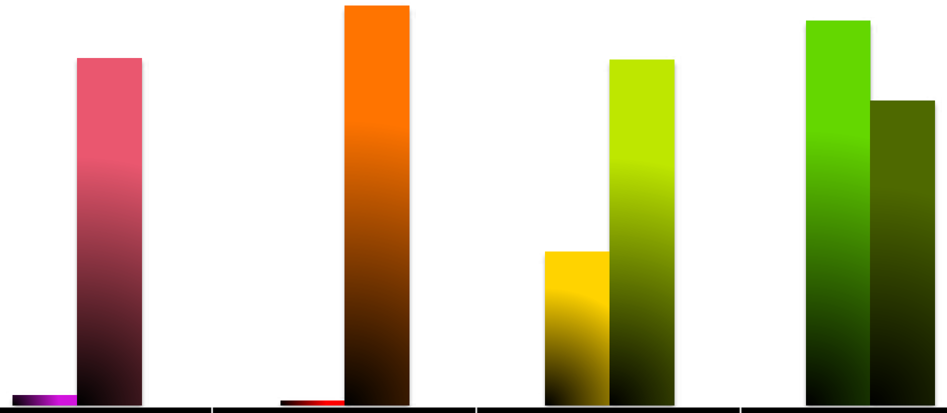
Comparisons between Q4 2011 and Q1 2012 statistics demonstrate a considerable increase in attacks targeted towards the financial service industry, in both quantity and intensity.

Mitigated Q4 2011 attack traffic targeting the financial services sector during Q4 2011 was approximately 19.1TB of data and 14 billion packets of malicious traffic. During Q1 2012, there was a significant increase in malicious traffic with 65TB of data and 1.1 trillion packets that were identified and mitigated. This represents an almost 80-fold increase in packets between Q4 2011 and Q1 2012.

For Prolexic's financial services clients, the average attack campaign duration this quarter showed a reduction from 50 hours in Q4 2011 to 40 hours in Q1 2012.

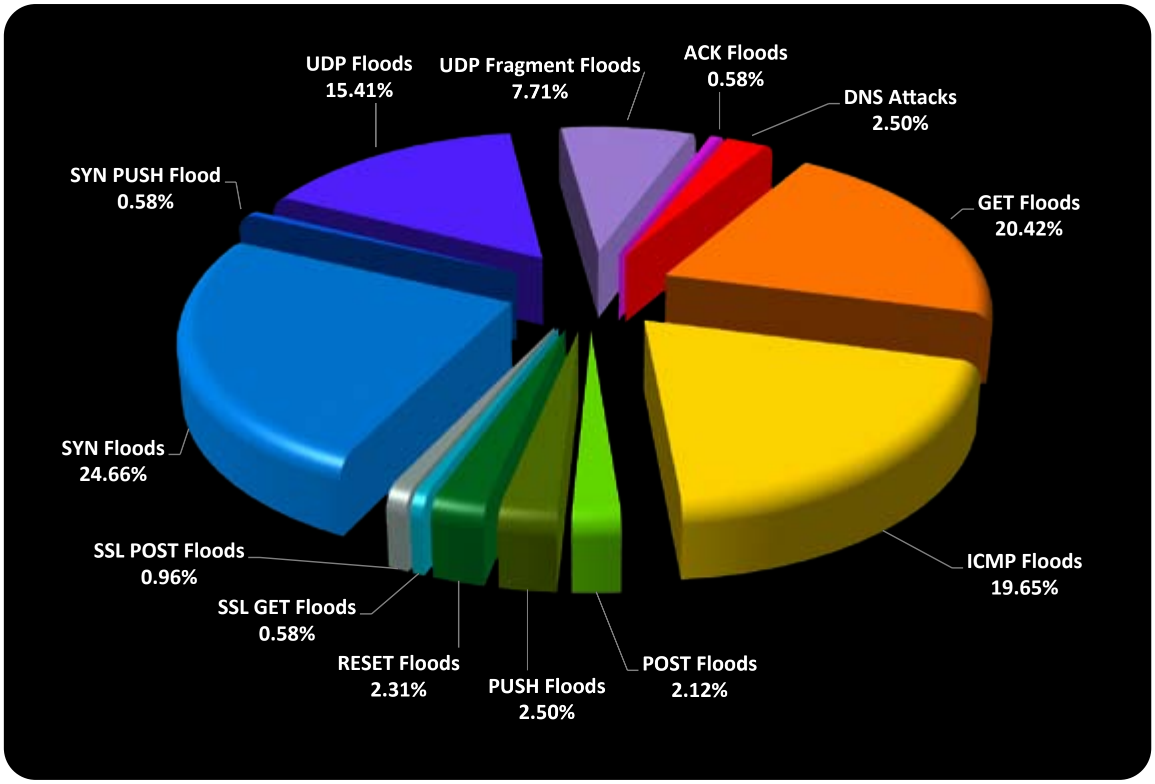
The reduction in attack campaign duration, combined with an increase in mitigated bytes and packets indicates that attackers are using shorter, stronger bursts of traffic to conduct DDoS campaigns. The considerable increase in attack intensity also indicates that attackers are evolving their strategies, increasing their firepower, and focusing on specific targets such as financial services.

Key Metrics Q1 2012: Financial Services



	Total bits mitigated	Total packets mitigated	Aggregate in sec.	Avg. attack length in sec.
Q411	168,090,664,850,000	14,101,420,520	2,199,699	183,308
Q112	5,793,175,030,861,800	1,142,235,586,498	4,937,363	145,216

Total Attack Types (Q1 2012)



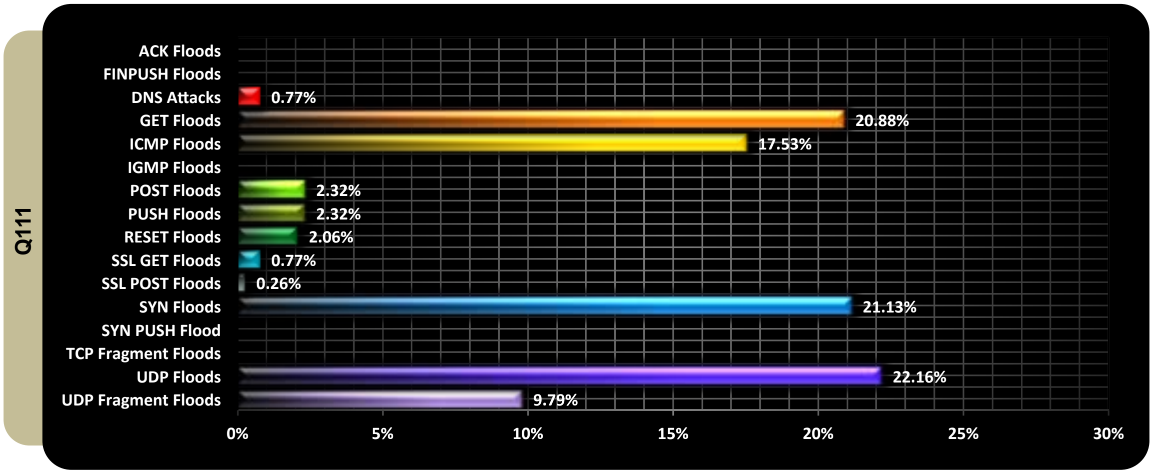
Throughout Q1 2012, PLXsert analysts were able to identify several trends within the attack types being leveraged by attackers. Overall during Q1 2012, attackers preferred infrastructure layer attacks (Layer 3) over application layer attacks (Layer 7). Of the attacks mitigated by Prolexic, 73.4% were infrastructure attacks and 26.6% were application layer attacks.

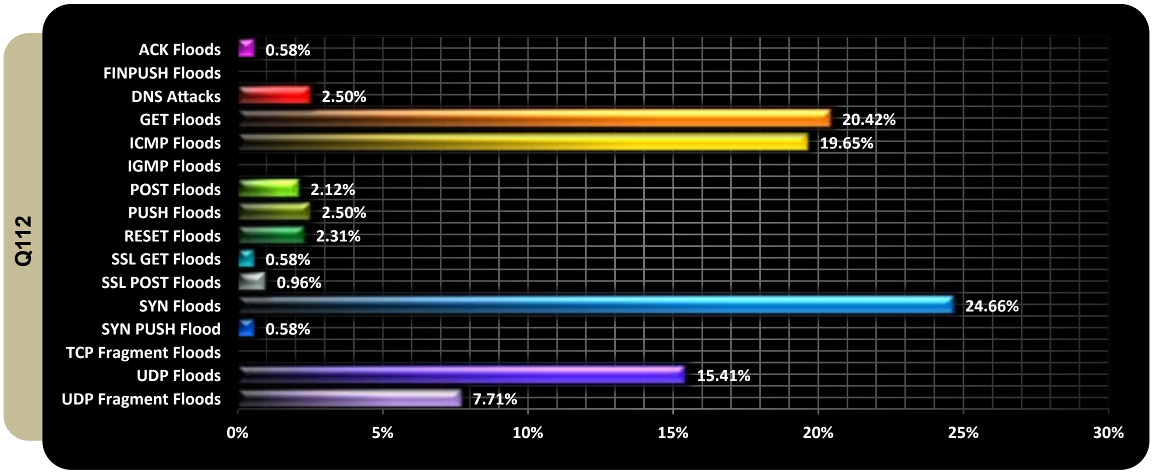
- Infrastructure (Layer 3 – 4) – When only looking at infrastructure attacks, the three most common within this attack classification were SYN floods (32%), ICMP floods (26%), and UDP floods (20%).
- Application (Layer 7) – When only looking at application layer attacks, GET Floods (77%) and POST Floods (8%) were the most common application based attacks mitigated within the quarter.

The above pie chart represents a complete breakdown of all DDoS attacks and associated percentages:

Attack Types (Q1 2011 vs. Q1 2012)

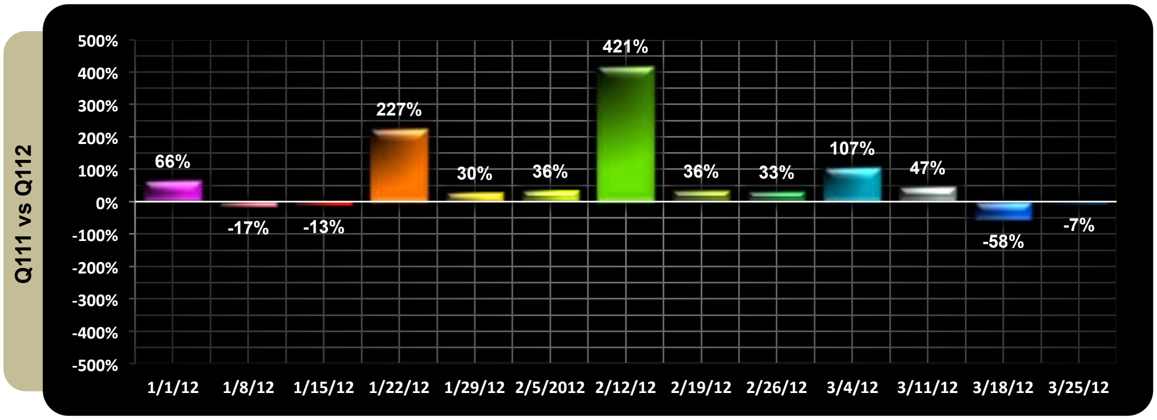
There was a dramatic shift in attack types in the first quarter of 2012 compared to the first quarter of 2011. UDP Floods fell to fourth place, losing their top position to SYN Floods, which accounted for a quarter of the attacks for Q1 2012. This continues the pattern previously observed.





Total Attacks per Week (Q1 2011 vs. Q1 2012)

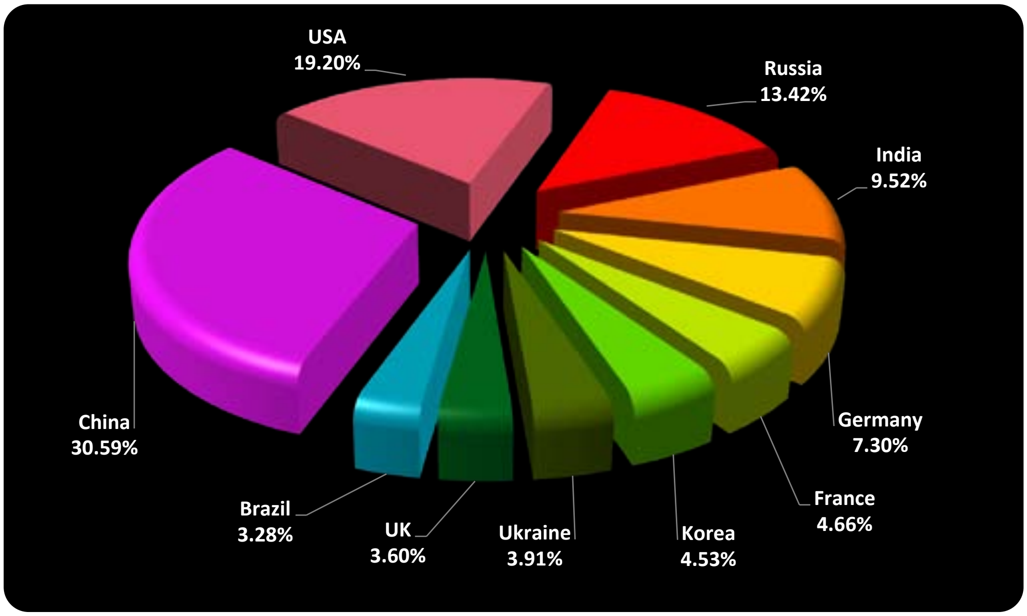
The following graph charts the percentage increases and decreases when comparing the total number of attacks between the first quarters of 2011 and 2012. Compared to 12 months ago, there was a noticeable increase in DDoS attacks from mid-January through mid-March. In Q1 2012, January was the busiest month for DDoS attacks, while the period of February 12-19 was the most active week.



Top Ten Source Countries (Q1 2012)

China (1st), United States (2nd), and Russian Federation (3rd) are currently the top three origins of DDoS attack campaigns for this quarter. Based on Prolexic's accumulated DDoS statistics, this reflects the more traditional geographical locations for botnet host origins.

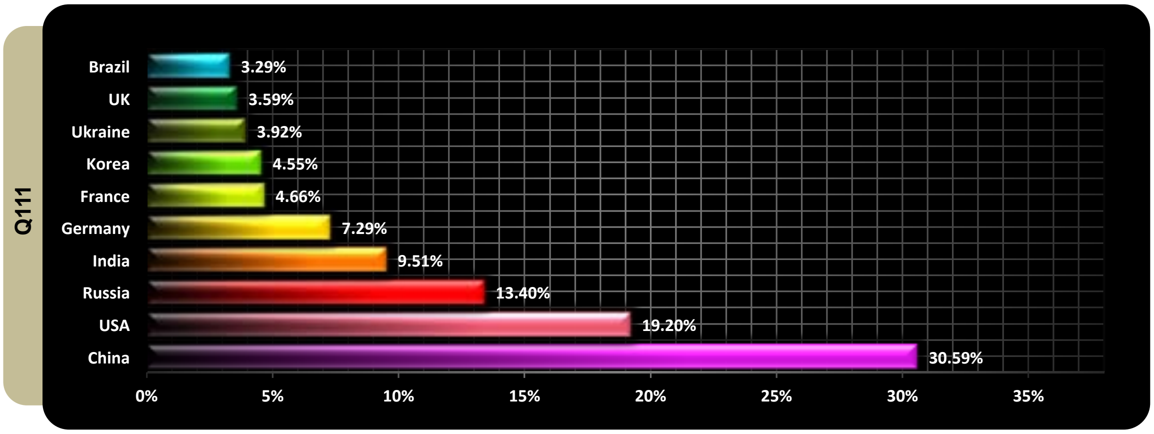
Prolexic has recorded over 2.9 million malicious source IP addresses during this quarter. The graph below highlights the top ten countries and associated percentages:

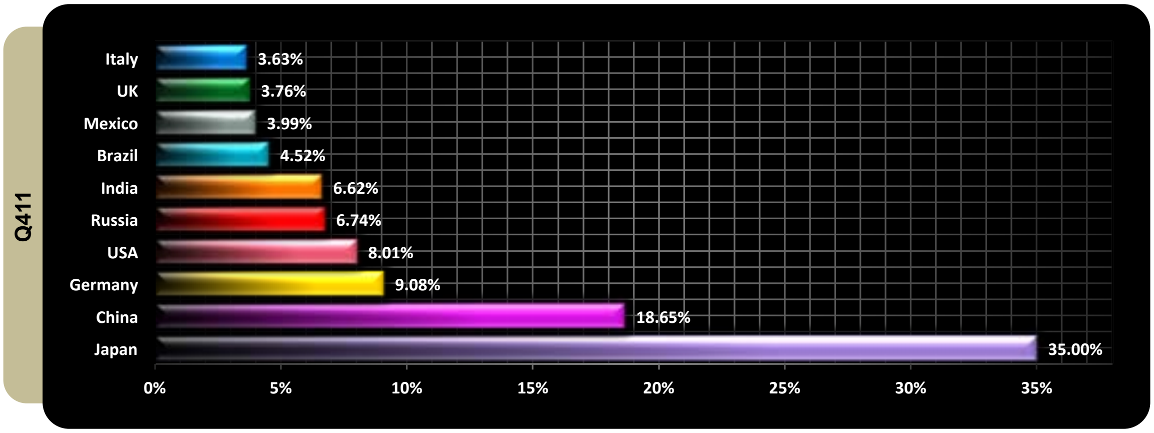


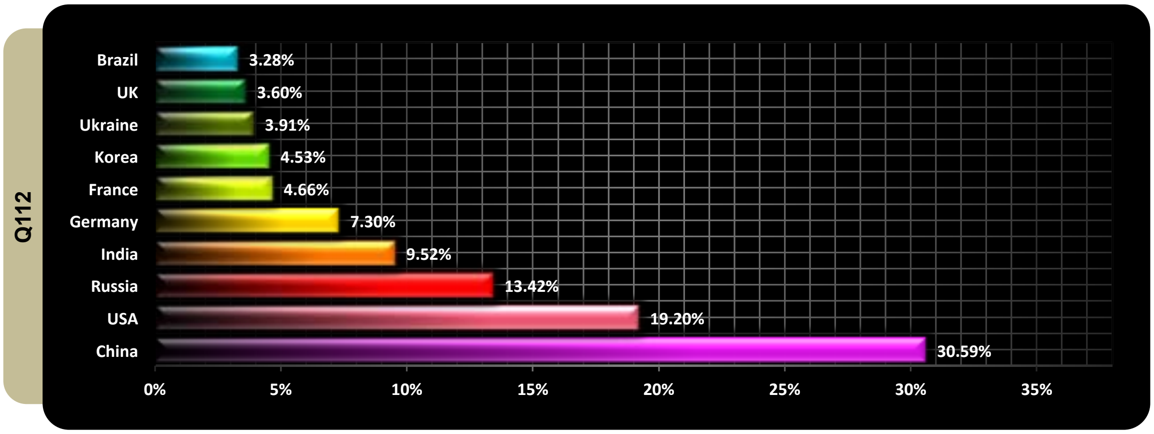
Comparison: Top Ten Source Countries (Q1 2011, Q4 2011, Q1 2012)

A shift in malicious traffic origin was identified this quarter. While Japan was the leading source of new malicious hosts participating in DDoS attacks in Q4 2011, it dropped down to 26th in Q1 2012. In 4th place, India has maintained consistency over the last year and its botnets have increased in size. Larger botnet infrastructures equate to more robust DDoS campaigns.

This quarter, a total of 230 countries were analyzed as source locations for infected hosts and now include locations such as Cook Islands, Somalia, and Holy See (Vatican City State).



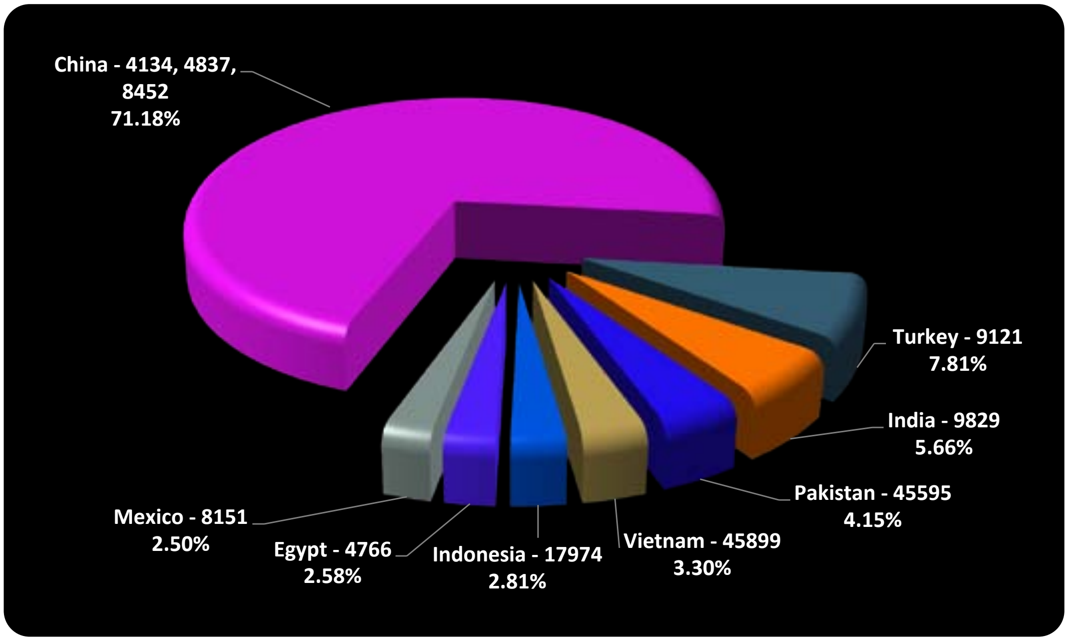




Top Ten ASNs

Analysis of the global DDoS attack threatscape shows the majority of malicious traffic is being sourced from ASNs that reside within Asia. The most likely explanation for this behavior is the fact that Asia continues to see increased penetration of high-speed Internet connectivity. At the same time, the use of unpatched and pirated copies of Microsoft Windows is known to be prevalent within the Asia Pacific region.

ASNs 4134 and 4837, both originating within China, take first and second place as the primary source of DDoS traffic. ASN 9121, originating within Turkey, ranks third, followed up by ASN 9829, originating within India, in fourth place.

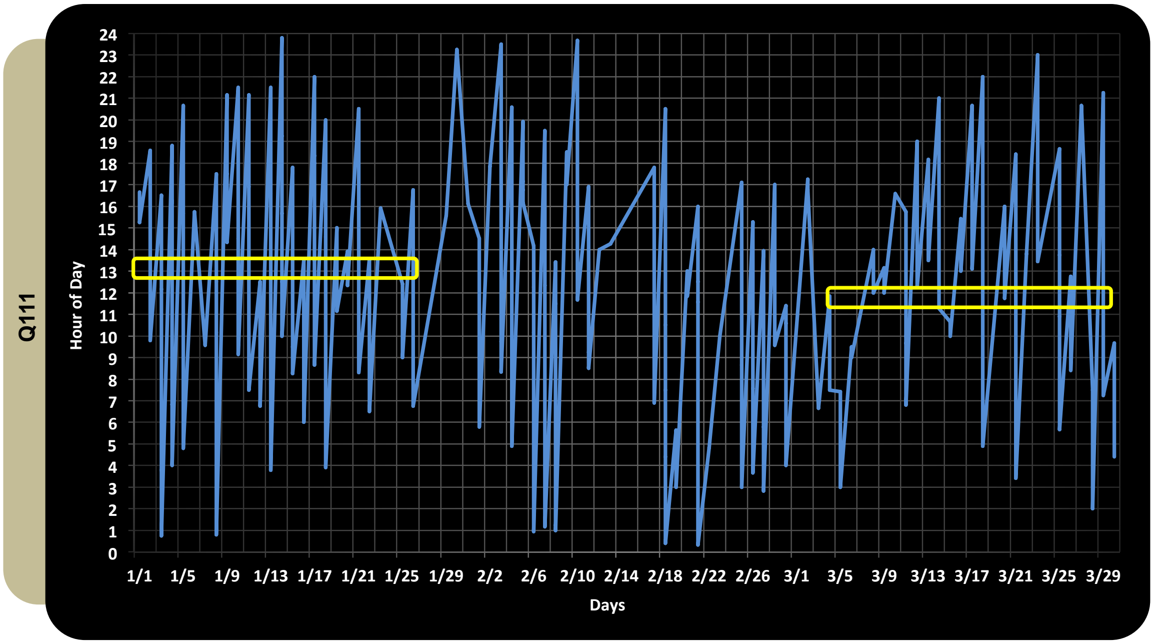


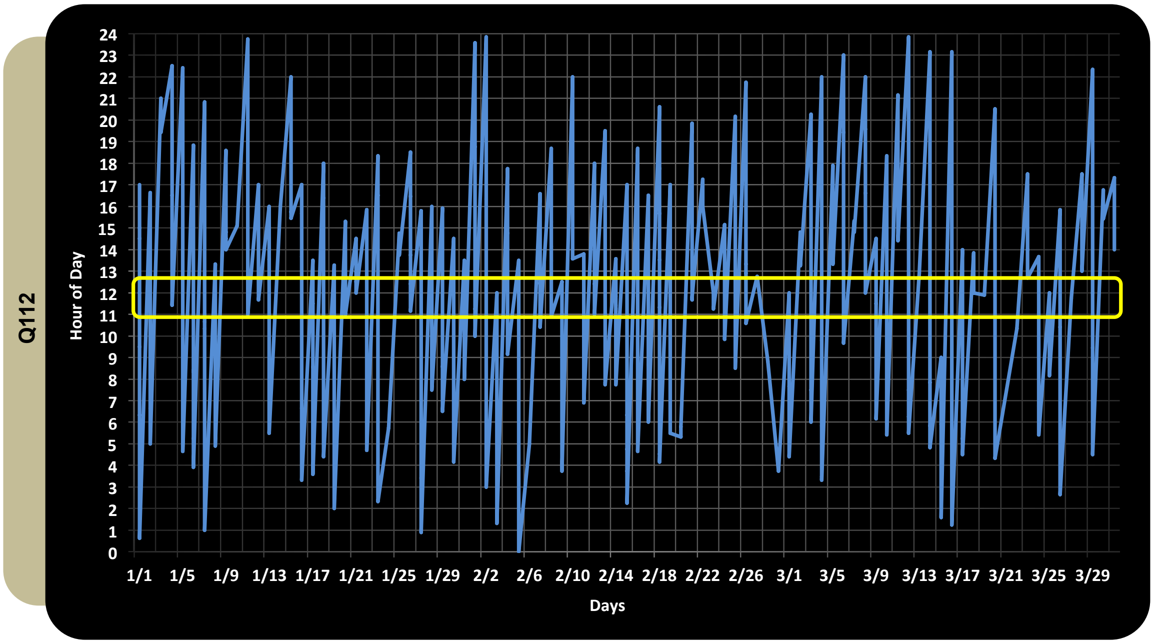
Country	Registry	ASN	ASN Count
China	apnic	4134	2138151
China	apnic	4837	983045
Turkey	ripencc	9121	353684
India	apnic	9829	256619
Pakistan	apnic	45595	188151
Vietnam	apnic	45899	149485
Indonesia	apnic	17974	127195
Egypt	apnic	4766	116837
Mexico	lacnic	8151	113459
China	afrinic	8452	103369

Attack Campaign Start Time per Day (Q1 2011 vs. Q1 2012)

At the beginning of Q1 2011, most attacks started near 13:00 GMT. Toward the end of Q1 2011, attacks started near 11:45 GMT.

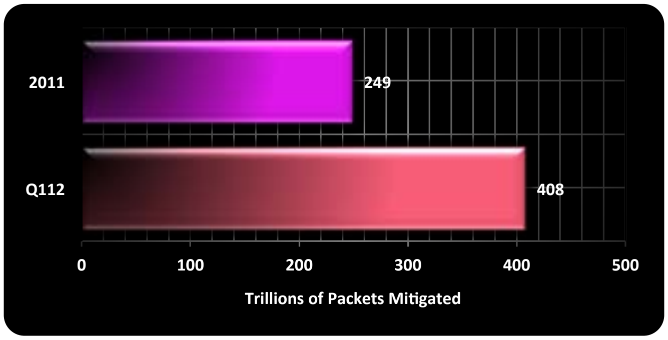
In Q1 2012, the start time was close to 12:00 GMT. The graph below shows an average of the start times for the observed DDoS attacks. The start/stop times of campaigns remain consistent among attackers.





Total Mitigated Traffic – Q1 2012 vs. 2011

In 2011, Prolexic mitigated a total of 9.5 Petabytes of data. In Q1 2012, Prolexic mitigated 9.5 petabytes of data. A Petabyte is a unit of information equal to one quadrillion bytes, or 1000 terabytes.



How big is a Petabyte?

- The BBC's iPlayer is reported to use 7 petabytes of bandwidth each month.[1]
- The Internet Archive contains about 5.8 petabytes of data as of December 2010.[2]
- The experiments in the Large Hadron Collider produce about 15 petabytes of data per year, which will be distributed over the LHC Computing Grid.[3]

Looking forward

Traditionally, malicious attackers have spent little time customizing their toolkits to target specific applications for a given target. In 2011, that changed and PLXsert observed a number of attacks that targeted specific applications. For example, one attack in particular was custom coded to emulate a flash application that the target used as part of its business. We see this trend continuing into 2012 and expect to see an increase in OS X botnets performing DDoS, now that the OS X platform has gained market share. Mobile phones and devices are also an emerging launch platform. While they are becoming increasingly capable of performing DDoS attacks, they are limited to carrier networks that usually proxy their connections due to limited IPv4 address space. PLXsert also expects to see a rise in browser-based attacks because of their ubiquity on the Internet.

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 our 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. Ten of the world's 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**.

1. CNET UK. http://crave.cnet.co.uk/software/iplayer-uncovered-what-powers-the-bbcs-epic-creation-49302215/. Retrieved 2010-01-11.
2. "Internet Archive: Petabox". Archive.org. http://www.archive.org/web/petabox.php. Retrieved 2011-07-16.
3. "3 October 2008 - CERN: Let the number-crunching begin: the Worldwide LHC Computing Grid celebrates first data". Interactions.org. http://www.interactions.org/cms/?pid=1027032. Retrieved 2009-08-16.