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

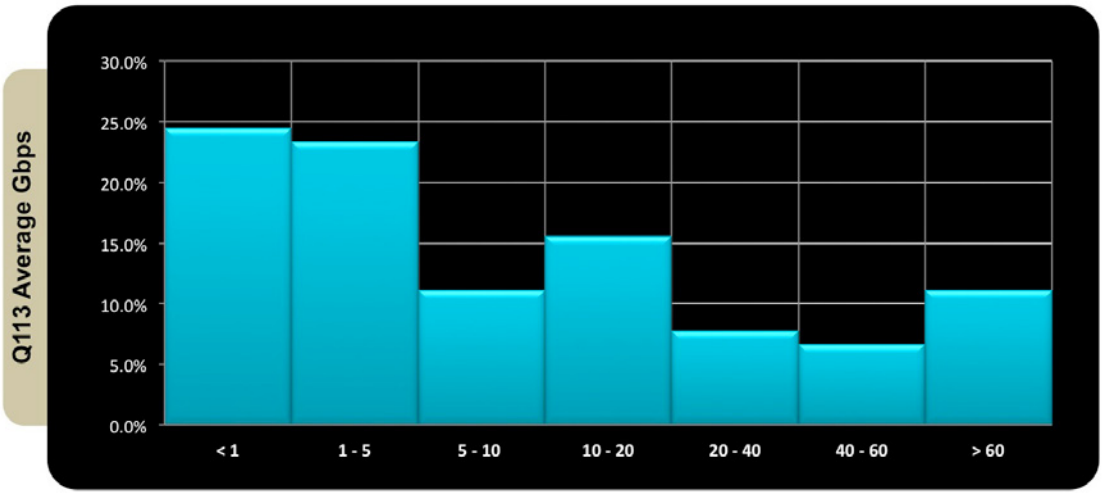
Compared to the same quarter one year ago, the total number of attacks increased 21 percent in Q1 2013. While the split between the total number of infrastructure attacks and application layer attacks was similar between the two quarters, both attack types increased when the two quarters are compared – 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.

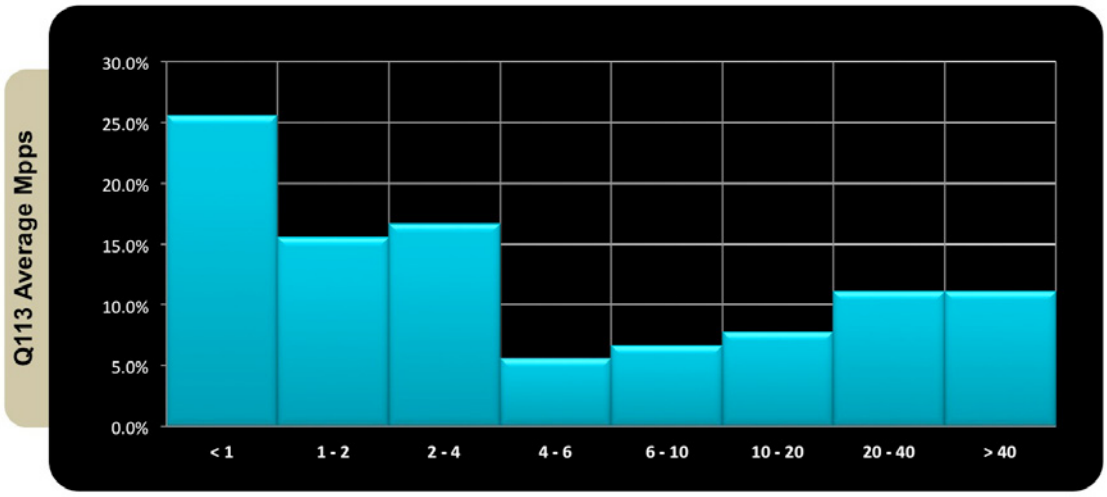


Q1 2013 Average Mpps

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).

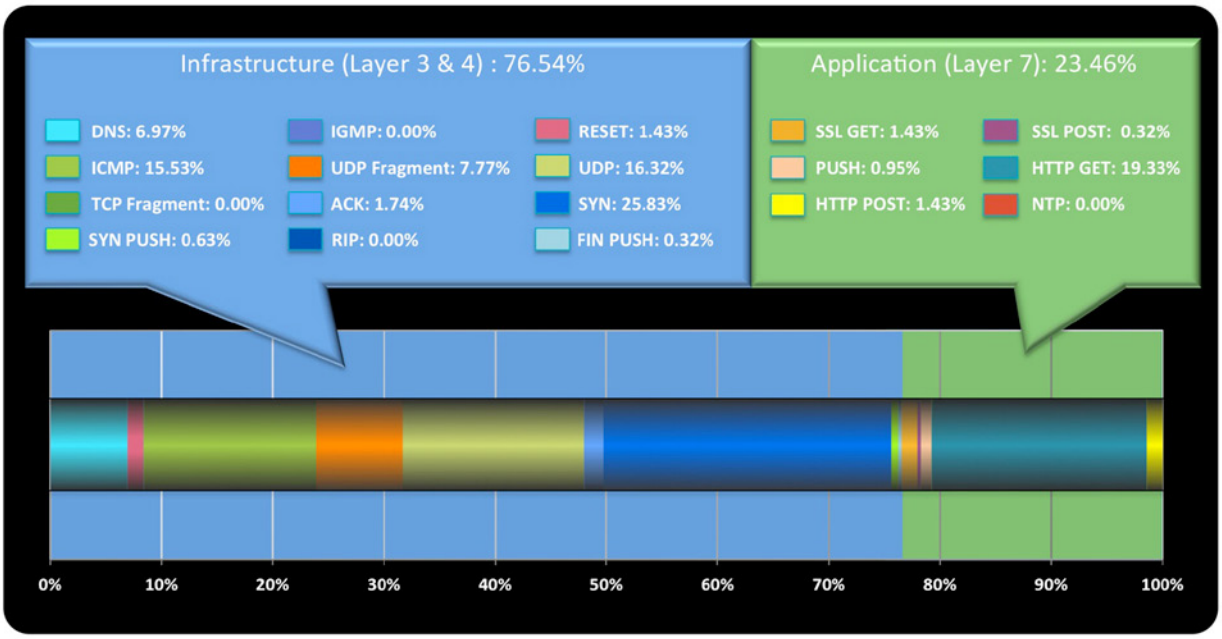
This section will examine the technical detail behind the protocols that were used in these attacks.

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.

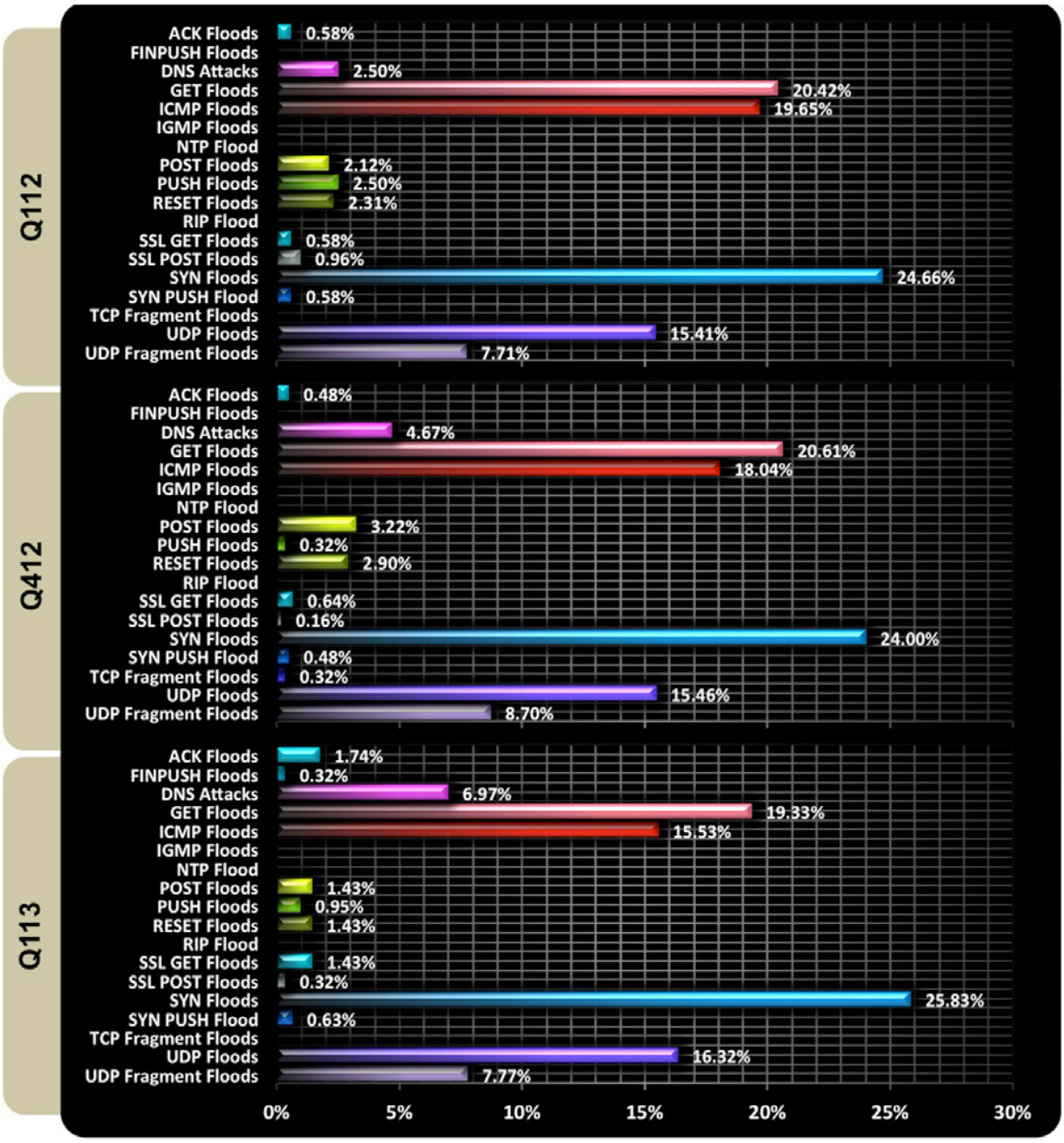
Based on collected data, an increasing trend can be seen by the percentages of SYN and UDP attacks rendered in the graphic. Data shows SYN floods in Q1 2012 (24.66 percent), Q4 2012 (24 percent), Q1 2013 (25.83 percent) respectively, and UDP floods with Q1 2012 (15.41 percent), Q4 2012 (15.46 percent), 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)

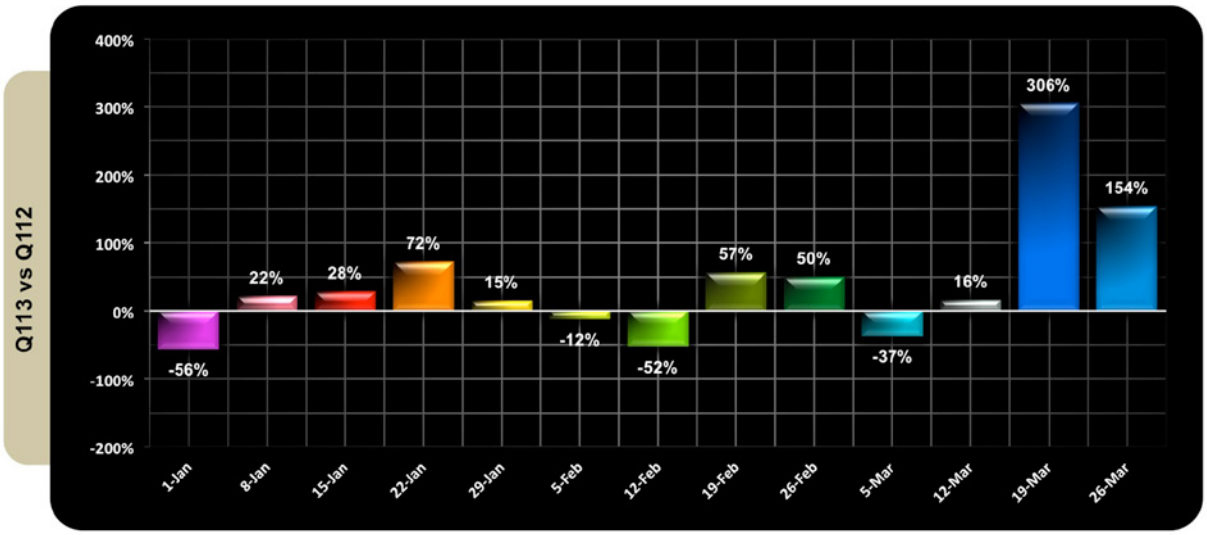
Comparison: Attack Types (Q1 2012, Q4 2012, Q1 2013) (continued)



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)

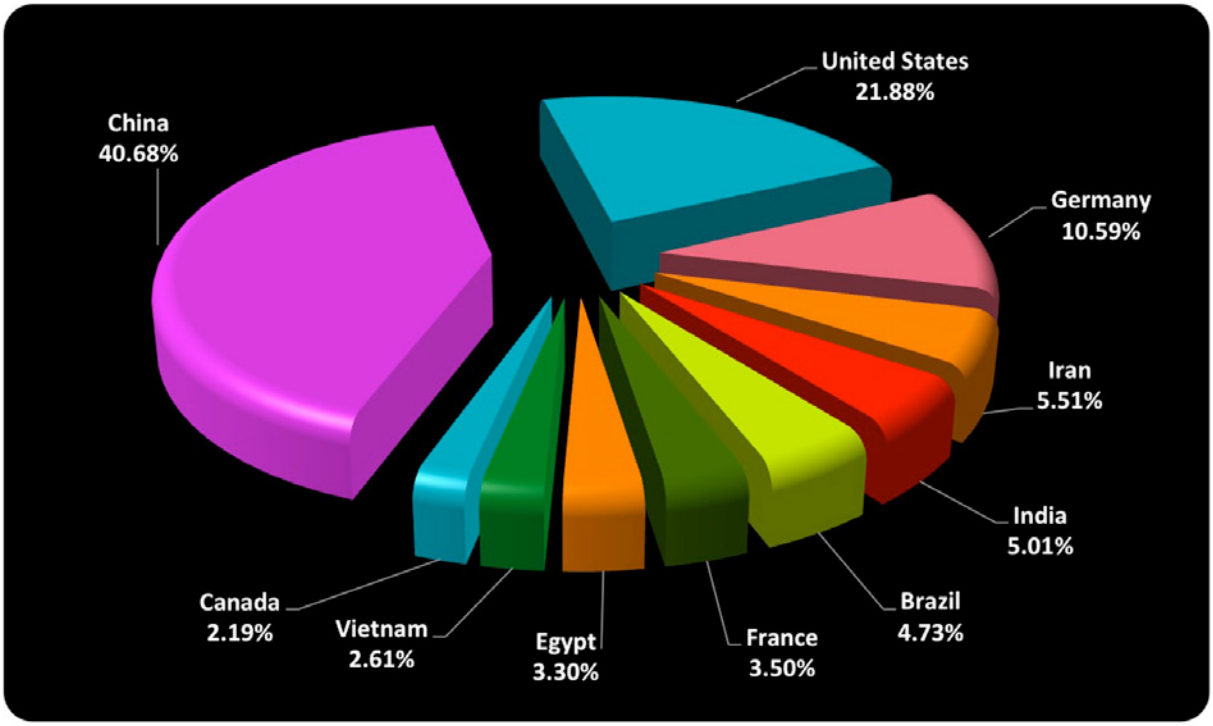
The first quarter shows China as the leader of botnet activity with 40.68 percent of sourced botnet activity. This was a significant drop from last quarter, where China represented over half (55.44 percent) of all maliciously sourced DDoS traffic. The United States was in second place with 21.88 percent, 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.



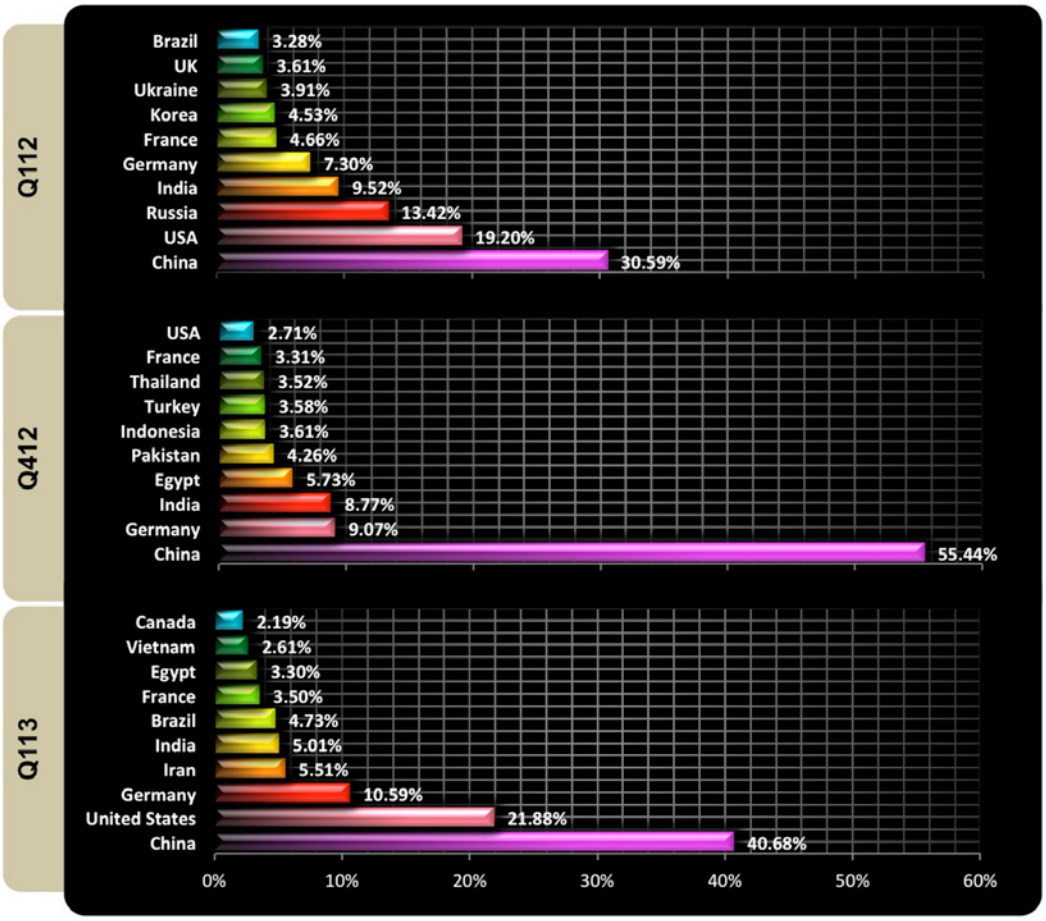
Comparison: Top Ten Source Countries (Q1 2012, Q4 2012, Q1 2013)

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.

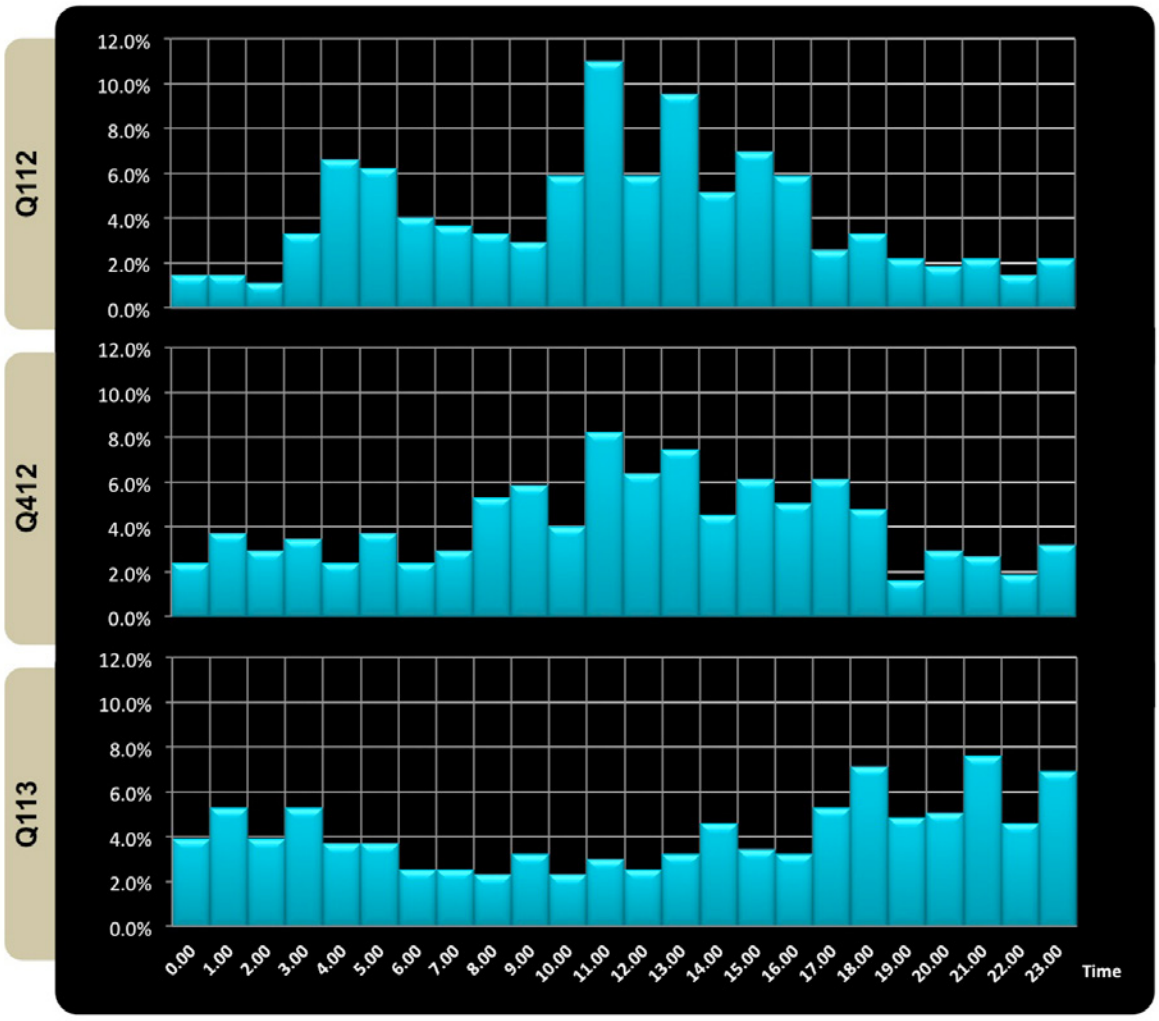


Comparison: Attack Campaign Start Time per Day (Q1 2012, Q4 2012, Q1 2013)

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

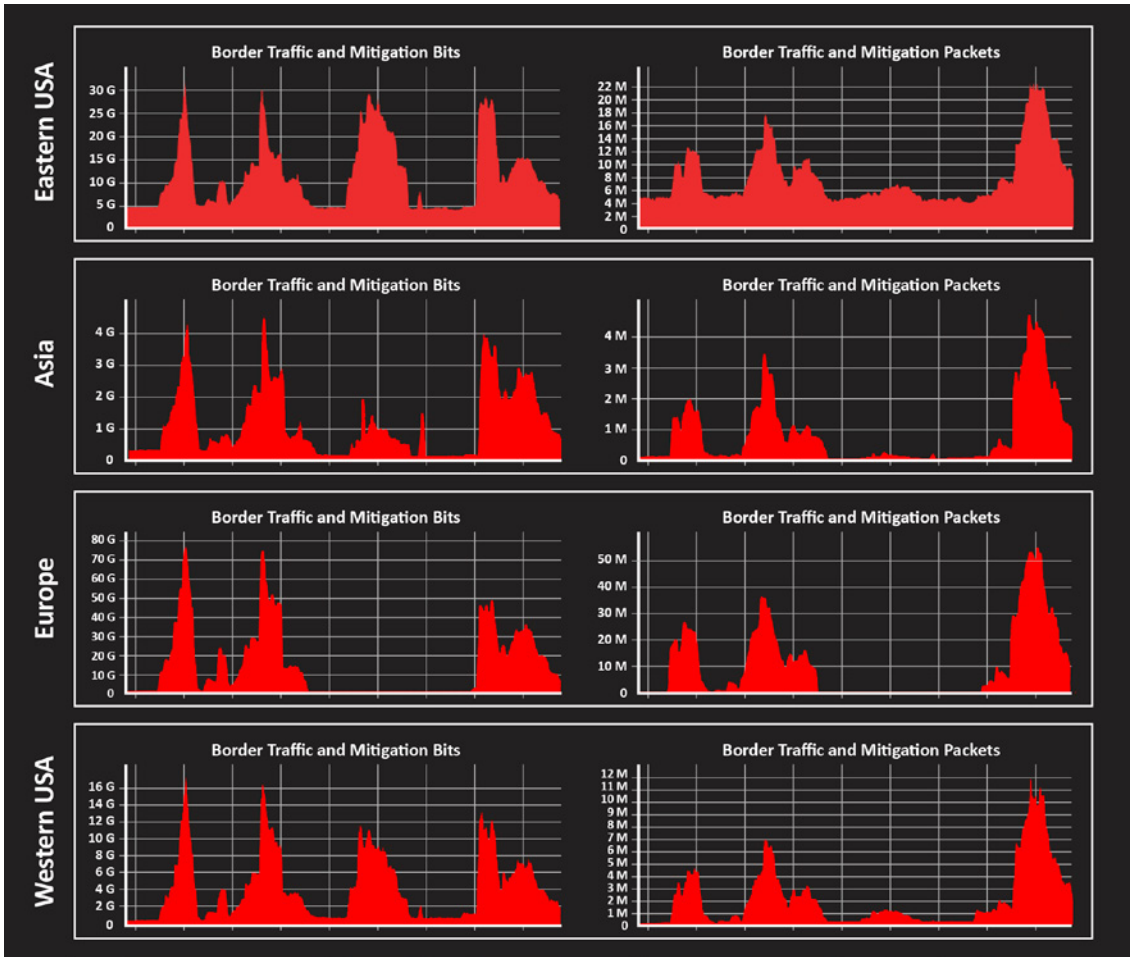
Prolexic is retained by an enterprise organization, which was targeted with a DDoS attack of significant proportions. Attack traffic peaked at 130 Gbps, which was routed through various global Prolexic data centers. The architecture of the attack consisted of thousands of compromised servers hosting 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.

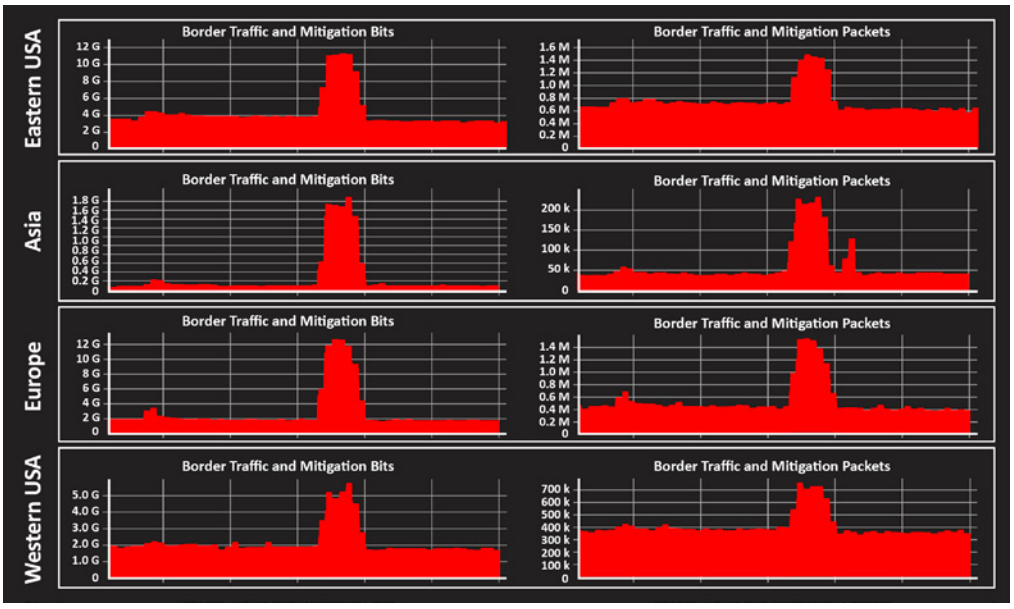
Attack Campaign Metrics

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

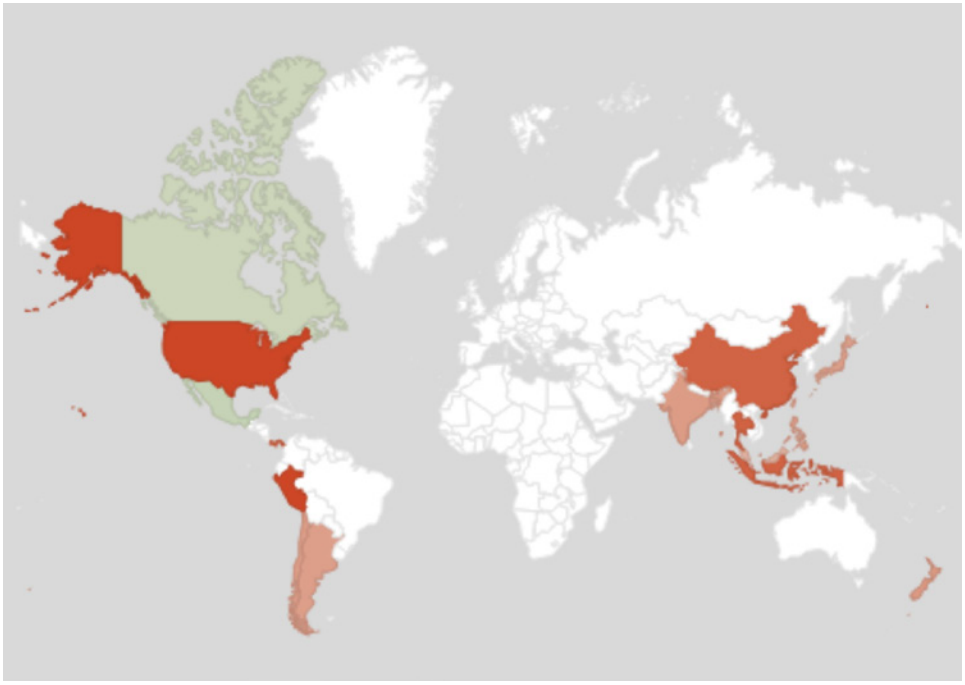
This attack event was short, but was of high volume. Attacks that reach 20+ Gbps attacks are quite easy to accomplish through the use of DNS Amplification attack techniques.

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

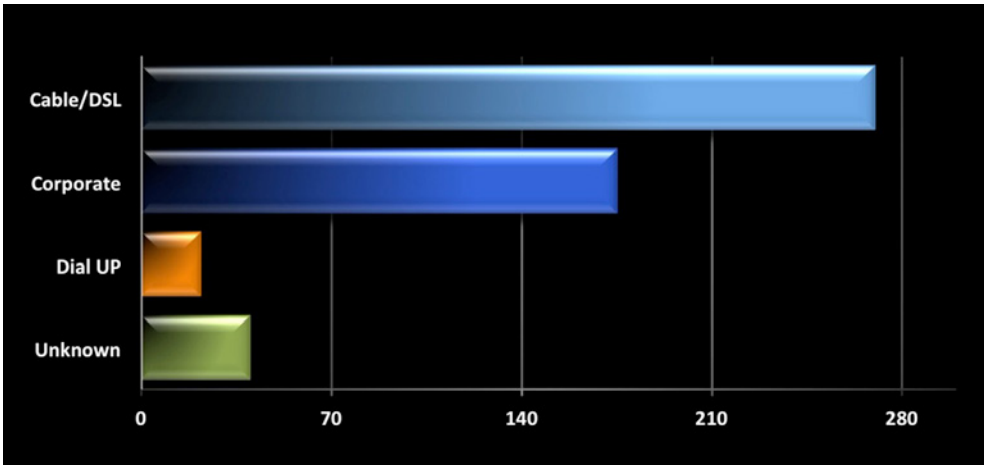


In this above graph, it can be noted that Prolexic observed a 25 Gbps increase in traffic for approximately 7 minutes.



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:

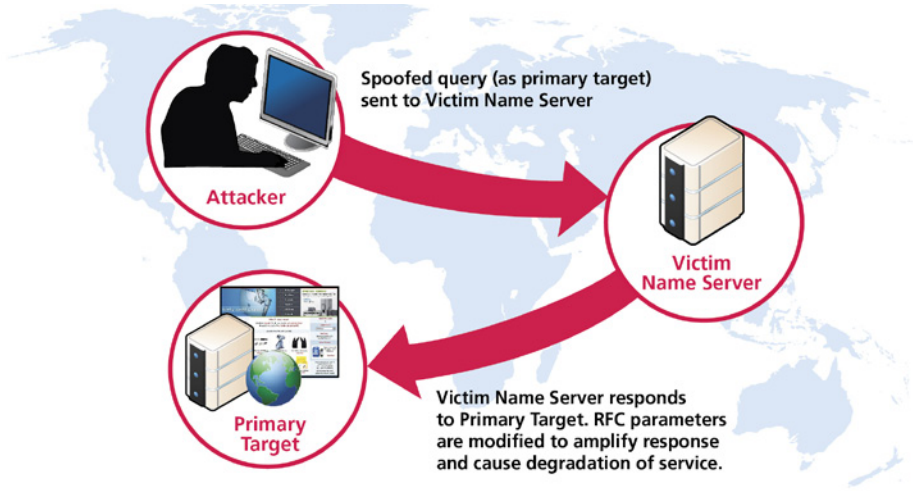
```
p=IP(dst="192.168.146.2")/UDP(sport=25345,dport=53)/DNS(rd=1L,qd=DNSQR(qtype=255,qclass="IN",qname="isc.org"),ar
=DNSOPTRR(edns_flags="DO",edns_bufsize=4096),id=57369)
```

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.