Prolexic Quarterly Global DDoS Attack Report

Q4 2013

Malicious actors begin using mobile applications
in well-orchestrated DDoS attacks

www.prolexic.com

PROLEXIC
DDoS Attacks End Here.

Table of Contents

At a Glance

Compared to Q4 2012

- 26.09% increase in total DDoS attacks
- 17.42% increase in application layer (Layer 7) attacks
- 28.97% increase in infrastructure layer (Layer 3 & 4) attacks
- 28.95% decrease in average attack duration: 22.88 vs. 32.21 hours

Compared to Q3 2013

- 1.56% increase in total DDoS attacks
- 0.55% increase in application layer (Layer 7) attacks
- 1.86% increase in infrastructure layer (Layer 3 & 4) attacks
- 7.25% increase in average attack duration: 22.88 vs. 21.33 hours
- 48.04% increase in average peak attack bandwidth from 3.06 Gbps to 4.53 Gbps
- 151.21% increase in average peak packets-per-second rate from 4.22 Mpps to 10.60 Mpps

Analysis and emerging trends

The consistently high level of distributed denial of service (DDoS) attacks worldwide in 2013 was maintained in the final quarter of the year. Data collected from attacks launched against Prolexic's global client base in Q4 showed increases across nearly all key metrics.

While the total number of attacks only increased 2 percent over the previous quarter, Prolexic once again mitigated more attacks this quarter than ever before. Prolexic mitigated extremely large bandwidth attacks and in some cases, highly sophisticated, multi-vector attacks. In Q4, several attacks over 100 Gbps were mitigated with the largest peaking at 179 Gbps. This is the largest attack to date that has traversed Prolexic's 1.8 Tbps cloud-based mitigation infrastructure.

As in previous quarters, malicious actors continued to favor launching Layer 3 and Layer 4 attacks targeting infrastructure elements. Infrastructure attacks accounted for 76.76 percent of total attacks during the quarter with application layer attacks making up the remaining 23.24 percent. UDP, UDP fragment, DNS, SYN and HTTP GET floods were the most common attack types directed against Prolexic clients. Use of the CHARGEN protocol in reflection attacks continued to increase significantly (reflection attacks were covered in detail in Prolexic's ***Q3 2013 Global DDoS Attack Report***). This quarter, average attack duration totaled 22.88 hours.

In Q4, the Prolexic Security Engineering and Response Team (PLXsert) uncovered evidence of the use of mobile applications launching DDoS attacks against enterprise clients, including one of the world's largest financial services firms. Attack signature analysis showed the use of AnDOSid, an Android operating system app that performs an HTTP POST flood attack. The use of mobile applications in DDoS attacks is an emerging trend that PLXsert expects to become more prevalent in 2014 as many of these opt-in apps can be downloaded from online app stores and no experience is required to use them.

Attack volume was remarkably consistent this period, showing only a 1 percent deviation between the three months of the quarter. October and November registered the same number of attacks and consequently tied as the months with the greatest number of individual attacks for the period. The week of 11/5-11/12 was the most active week of the quarter.

This quarter, the United States replaced China at the top of the top 10 source countries list for DDoS attacks. This is primarily a result of Prolexic improving its threat intelligence capabilities. Prolexic has deployed new technologies that broaden the sources of IP input by logging and validating more Layer 3, Layer 4, and Layer 7 non-spoofed IP addresses. This new model, while being more accurate and broader, has also changed the distribution of attack origination. However, a general trend can be seen where Asian countries are emerging as the main source of the world's DDoS attacks. This quarter, the United States was joined at the top of the list by China, Thailand, United Kingdom and Republic of Korea (South Korea).

Compared to Q4 2012

Compared to the same quarter one year ago, the total number of attacks increased 26 percent in Q4 2013. While the split between the total number of infrastructure attacks and application layer attacks was similar between the two quarters, both attack categories increased when the two quarters are compared year-over-year – by 28.97 percent and 17.42 percent respectively. In contrast, average attack duration fell 28.95 percent from 32.21 hours to 22.88 hours. These metrics illustrate that over the last year, there are not just more DDoS attacks, but more potent DDoS attacks that are more efficient and take less time to execute.

Compared to Q3 2013

Despite mitigating the highest volume of attacks to date in Q3 2013, the total number of attacks increased yet again in Q4 (up 1.56 percent), highlighting that a level once regarded as an anomalous peak is now the norm. Compared to the previous quarter, average peak attack bandwidth increased 48.04 percent to 4.53 Gbps and the peak packets-per-second rate increased 151.21 percent to 10.60 Mpps.

2013 vs. 2012 comparison

Prolexic noted a clear evolution in the strategies and tactics malicious actors embraced over the past 12 months. The construction of botnets utilized to carry out DDoS attacks grew in both size and sophistication in 2013. Consequently, Prolexic regularly mitigated attacks in excess of 60 Gbps directed against its global client base and attacks over 100 Gbps were not uncommon.

In addition to increasing size, DDoS attacks in 2013 also increased in frequency. Prolexic mitigated 32.43 percent more attacks in 2013 than in 2012. In 2013, both application and infrastructure layer attacks increased from last year. Application layer attacks rose approximately 42 percent and infrastructure layer attacks increased approximately 30 percent. As in 2012, infrastructure layer attacks still remained the most popular in 2013 accounting for roughly 76 percent of the total number of attacks for the entire year. In particular, 2013 saw increases in DNS, UDP and UDP fragmentation flood attacks (DNS 216 percent and combination UDP and UDP fragmentation up 29 percent). At the same time, there was a revival of the CHARGEN attack vector. All four of these attack types supported the uptick in reflected amplification DDoS attacks observed throughout 2013. While several infrastructure attack vectors increased, other more traditional attack methods such as ICMP floods declined this year (ICMP declined 6 percent).

There was also a geographical shift toward Asian countries as a growing source for DDoS attack origination in 2013. An Asian country has ranked as number one or two in Prolexic's list of top 10 source countries for DDoS attacks throughout 2013. And, at least six of the countries in the top 10 source countries list have been Asian countries for each quarter of 2013.

Total attack vectors Q4 2013

The split between application and infrastructure attacks remained similar during Q4 2013 as compared to the previous quarter. Application attacks totaled 23.24 percent, down a negligible .24 percent in comparison to the third quarter. This also represents a 1.71 percent reduction compared to Q4 2012 (24.95 percent).

Infrastructure attacks made up 76.76 percent of the total in Q4 2013, up from 76.52 percent in Q3. The split between infrastructure and application has remained consistent throughout 2013, however there have been changes in the attack vectors used for infrastructure attacks. Two changes in particular are worth noting.

A significant increase in the use of the CHARGEN protocol was observed during the previous quarter, rising to 3.37 percent. This trend continued in Q4 with the use of CHARGEN attack vectors rising to 6.39 percent, representing a 92.31 percent increase. The use of the Network Time Protocol (NTP), a protocol used to synchronize time in computers, is also increasing even though its current level is still very low. Due to the release of newly developed DDoS attack tools, old protocols can again become relevant attack vectors. There still remain a high number of unpatched and vulnerable servers worldwide that contribute to the cyclical return of these protocols in DDoS attack campaigns.

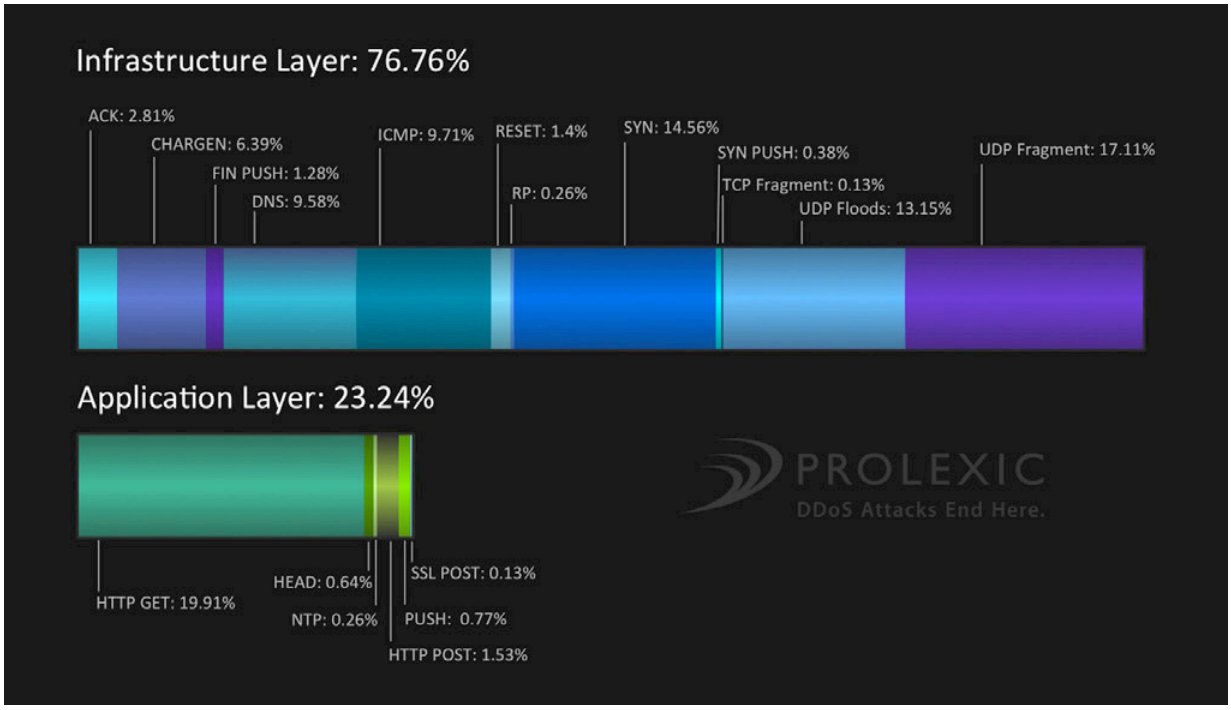

Figure 1: Types of DDoS attacks and their relative distribution in Q4 2013

Infrastructure layer attacks

Prolexic data shows the majority of DDoS attacks are directed against the infrastructure layer, accounting for 76.76 percent of attacks in Q4 2013. The UDP protocol was most commonly used with a combined 30.27 percent total in comparison with other protocols. SYN floods placed second as the preferred DDoS infrastructure attack vector with a total of 14.94 percent.

In third place was the ICMP protocol with 9.71 percent followed by DNS with 9.58 percent. PLXsert has previously noted the increase in the use of DNS reflection as an attack vector and this is likely to remain so with new tools being released and adapted by DDoS-for-hire-vendors. In the fifth place, the old but revived CHARGEN protocol continues its rise in popularity, accounting for 6.39 percent of the total infrastructure layer attacks this quarter. PLXsert has identified over 110,000 CHARGEN servers on the Internet, and to date most of these servers are still open and vulnerable, which is one factor contributing to a 92.31 percent increase of CHARGEN usage between Q3 2013 and Q4 2013.

Following CHARGEN, lesser used attack vectors in DDoS attacks against infrastructure were ACK Floods (2.81 percent), FIN PUSH (1.28 percent), TCP RST (1.4 percent), SYN PUSH (0.38 percent), RIP (0.26 percent), and TCP Fragment (0.13 percent).

Application attacks

Application layer attacks account for approximately one quarter of all campaigns launched against Prolexic's global client base. Application-based attacks require a higher level of knowledge and sophistication in order to be successful. Recently, there has been a noticeable increase in the adaptation of booter scripts by DDoS-for-hire vendors. This in turn makes it easier for malicious actors to purchase these services without having to build technical resources and spend considerable time creating a botnet powerful enough to perform significant attacks.

At 19.91 percent, HTTP GET was by far the most commonly used application layer attack vector in Q4 2013. This vector was followed by HTTP POST (1.53 percent), PUSH (0.77 percent), HEAD (0.64 percent), NTP (0.26 percent) and SSL POST with 0.13 percent.

PLXsert has observed an increase in the use of the Network Time Protocol (NTP) as an attack vector. Defined in RFC 958, the NTP protocol is widely used to synchronize multiple network clocks on the Internet using a set of distributed clients and servers. NTP is built on the User Datagram Protocol (UDP), which provides connectionless transport of data. NTP evolved from the Time Protocol and the ICMP Timestamp message; the NTP protocol acts as a suitable replacement for both.

The NTP protocol is implemented in all major operating systems, network infrastructure devices, and embedded devices. By using UDP, NTP is susceptible to spoofing. In addition, misconfiguration of network equipment can allow enterprise infrastructure to be used as unwilling participants in a DDoS attack. This can be achieved by responding to requests for NTP updates and directing the response to a victim host and overwhelming it with NTP traffic.

The use and reuse of certain protocols believed to be obsolete and decommissioned is usually driven by rediscovery and repurposing via the creation of new tools. These tools eventually get leaked in crimeware forums or obtained by compromising the original vendors. Once the tools are leaked, an increase of use in campaigns ensues and eventually gets adapted and implemented by DDoS-for-hire vendors.

Comparison: Attack vectors (Q4 2013, Q3 2013, Q4 2012)

Attack vectors increased en masse this quarter compared to total attacks from the previous quarter and from one year ago. The use of infrastructure layer attacks was significantly higher than application layer attacks. Fueled by ample supplies of PHP booter web shells, infrastructure UDP fragment flood attacks reached 17.11 percent. Because DNS and CHARGEN attacks are methods underpinning PHP booter frameworks, escalations in these two attack vectors (DNS 9.58 percent and CHARGEN 6.39 percent) were also observed this quarter.

Overall, the trend toward the use of reflected amplification style attacks over traditional attack methods continued as seen in the persistent decline in ICMP floods (9.71 percent) and the rise in DNS, CHARGEN, and UDP/UDP Fragment attacks.

Although SYN floods remain a mainstay of Layer 3 attacks, garnering 14.56 percent of total DDoS attacks observed this quarter, SYN flood activity continued to decline, decreasing from 18.16 percent last quarter and logging an even bigger decrease from Q4 2012, down from 24 percent. SYN PUSH flood attacks experienced a slight increase from 0.13 percent last quarter to 0.38 percent, but still followed the waning trend of SYN floods, decreasing .48 percent from one year ago.

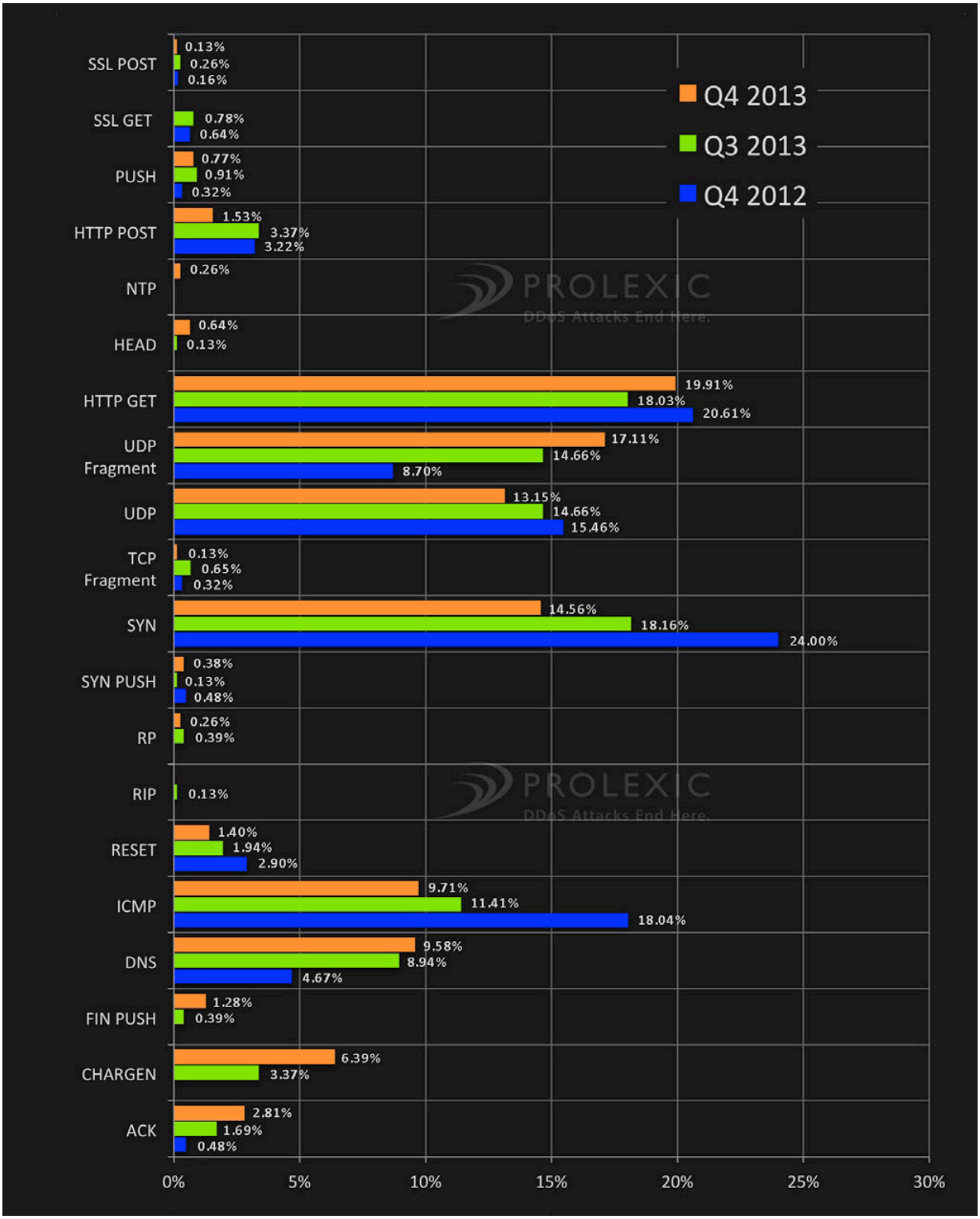

Figure 2: Attack vectors in Q4 2013, Q3 2013 and Q4 2012

Comparison: Attack vectors (2013 vs. 2012)

Q4 data clearly shows a strong increase in the adoption of UDP-based attack methodologies compared to last year. UDP fragmentation floods increased to 12.27 percent from 8.21 percent during 2012 and UDP floods for both years were one of the most utilized attack vectors.

Reflected amplification attacks remained popular in 2013 as demonstrated by the growth in DNS (3.54 percent to 8.37 percent) and CHARGEN (0 percent to 2.16 percent) attacks as well as the aforementioned UDP/UDP Fragmentation attacks.

While infrastructure layer attacks dominated both years with respect to total DDoS attacks, application layer attacks experienced gains, especially in Layer 7 HTTP protocol attacks, including HTTP GET (17.45 percent to 19.52 percent) and SSL GET (0.54 percent to 0.71 percent). These additions are consistent with the rise of DDoS-as-a-Service vendors, unaffiliated hacking groups, and the use of PHP web shell-based botnets.

Traditional attack methods such as ICMP floods (18.04 percent to 13.24 percent) and SYN floods (24.54 percent to 22.39 percent) declined this year. The movement away from ICMP and SYN floods is a direct consequence of the movement toward reflected amplification attacks because of the shift in attack offerings among DDoS-as-a-Service stressor services. While these attack types have declined, it is important to point out that overall, they both remain among the most popular of attack vector types (especially SYN floods) as validated by their percentage usage totals.

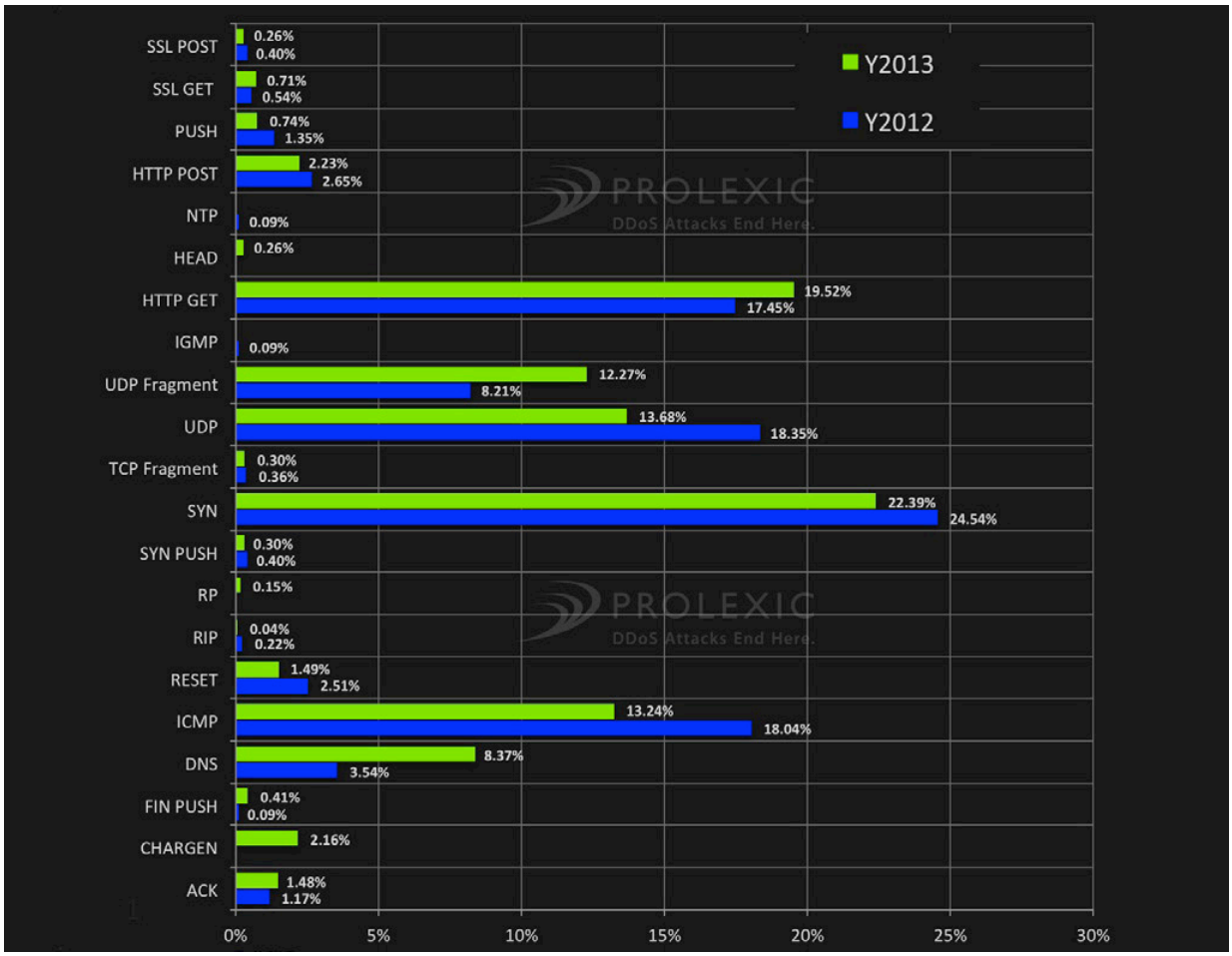

Figure 3: Attack vectors – 2013 vs. 2012

Total attacks per week (Q4 2013 vs. Q4 2012)

Figure 4 shows the percentage increase/decrease in the total number of weekly attacks against Prolexic's client base when Q4 2013 is compared to the same quarter one year ago. This quarter, the most active week for DDoS attacks was November 12th, which showed a 172 percent increase compared to Q4 2012. The majority of the DDoS campaigns launched during this active week primarily targeted gambling and gaming services organizations.

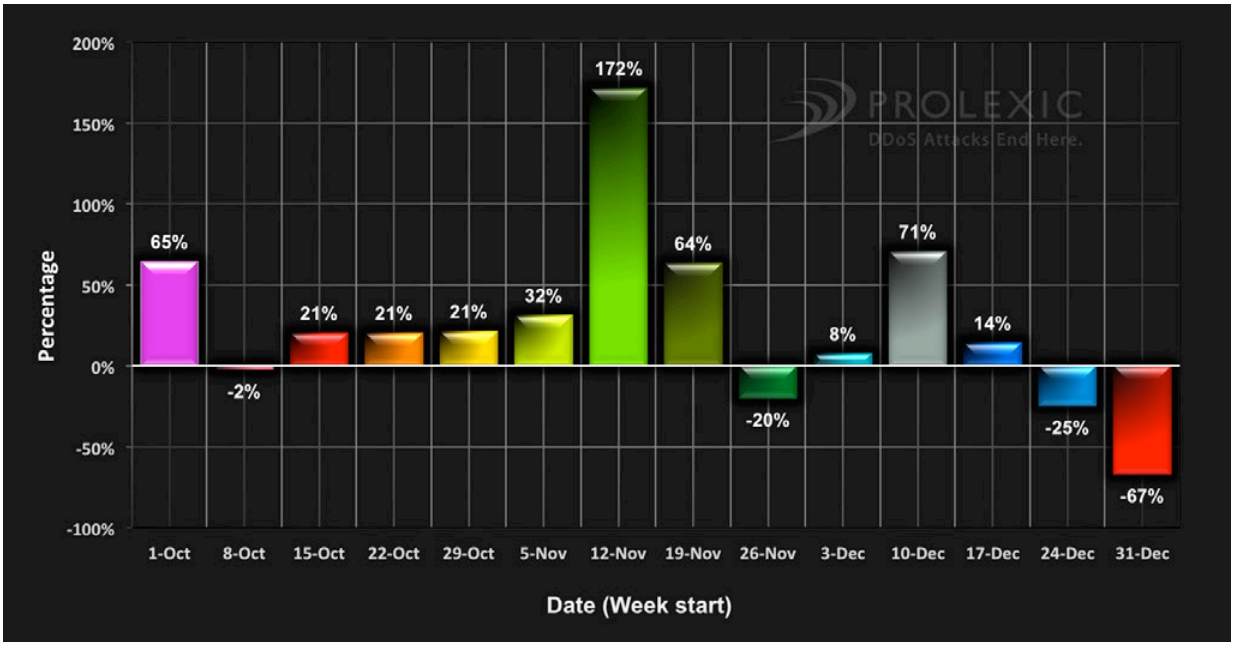

Figure 4: Changes in DDoS attacks per week – Q4 2013 vs. Q4 2012

Comparison: Attacks (2013 vs. 2012)

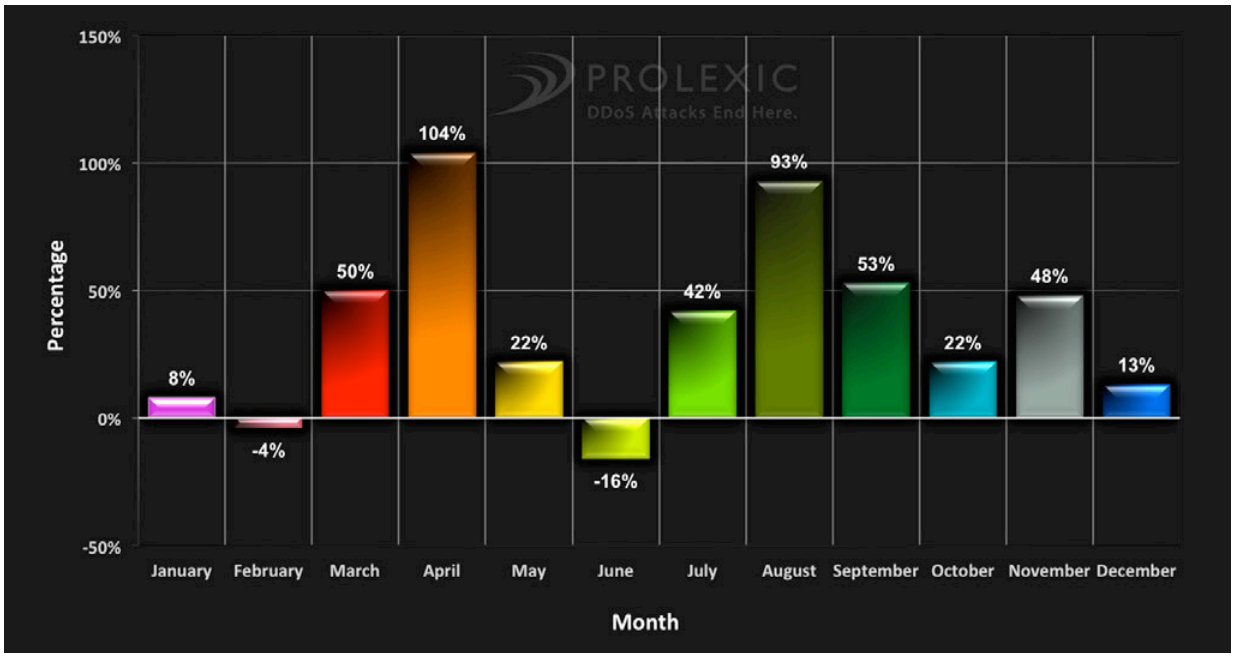

Figure 5: Changes in DDoS attacks per month – 2013 vs. 2012

Figure 5 represents the percentage increase/decrease comparison of attacks mitigated by Prolexic in 2013 versus 2012. As displayed, there has been a significant increase in DDoS activity over the course of the year. Except for February and June, 2013 has yielded an increase in DDoS attacks for every month of 2013. When the total number of attacks against Prolexic's client base in 2012 and 2013 are compared, there has been a 32.43 percent increase in attack volume in 2013. This has affected multiple industry verticals, including financial services, gaming, e-Commerce and energy.

Top 10 source countries (Q4 2013)

The United States was the main source of DDoS attacks during Q4 2013, accounting for 23.62 percent of attacks. China took second place this quarter at 19.09 percent relinquishing its spot as the number one source of DDoS attacks. In an interesting turn of events, Thailand not only rejoined the top 10 after several quarters of not appearing on the list, but also ranked third with 13.5 percent. The United Kingdom (8.49 percent) and the Republic of Korea (South Korea; 7.33 percent) round out the top five.

The remainder of the top 10 list includes India (6.57 percent), Turkey (5.84 percent), Italy (5.76 percent), Brazil (5.30 percent) and Saudi Arabia (4.43 percent).

This quarter, Prolexic improved its threat intelligence capabilities by adding new technologies that broaden the sources of IP input by logging and validating more Layer 3, Layer 4, and Layer 7 non-spoofed IP addresses. This new model, while being more accurate and broader, has also changed the distribution of attack origination, and this is the primary reason for the U.S. taking first place on the source country rankings.

There is a noticeable presence of Asian countries in the top 10 source countries. Growing economies and an expanding IT infrastructure, plus large online populations, are fueling DDoS attack campaigns. There are also indicators of an increasing number of hacktivist groups becoming active participants in DDoS campaigns from Asia.

During Q4 2013, Prolexic observed a significant and lengthy campaign against a financial institution in the Asia region, which is highlighted in this report. PLXsert also detected the incorporation of mobile devices in DDoS campaigns, and this is an emerging trend. Asia is poised to have the largest mobile user population in the upcoming years and the use of mobile devices in DDoS campaigns is only going to increase with time.

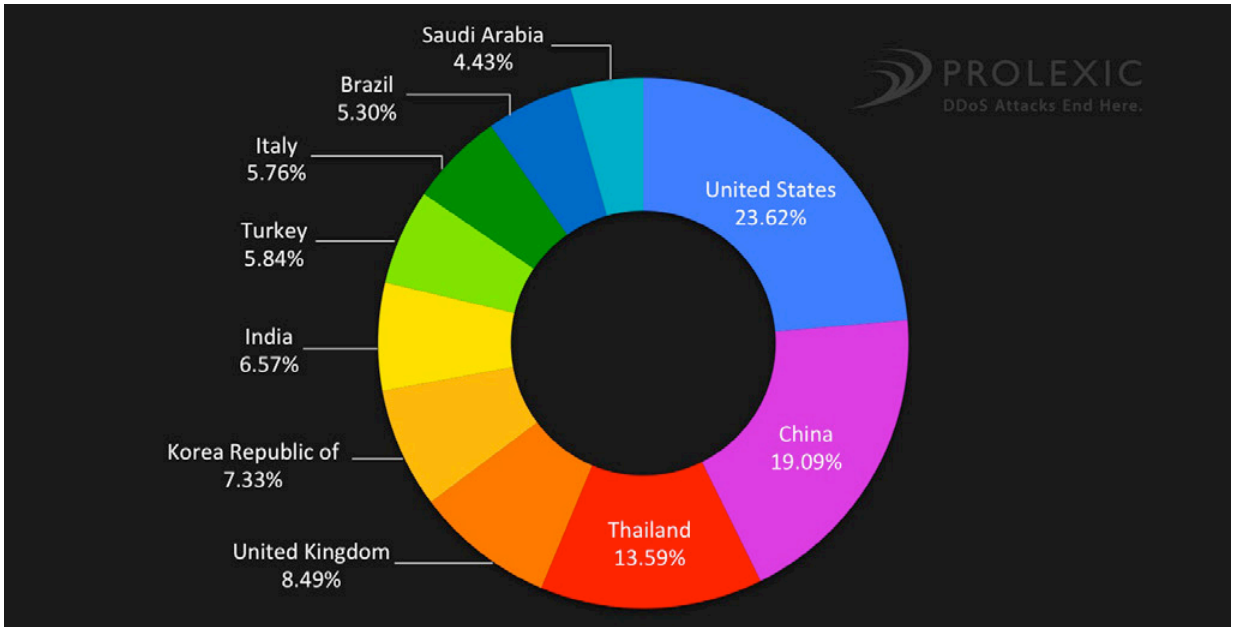

Figure 6: Top 10 source countries for DDoS attacks in Q4 2013

Comparison: Top 10 source countries (Q4 2013, Q3 2013, Q4 2012)

A look at the source countries from Q4 2013, Q3 2013, and Q4 2012 illustrates how country rankings in the top 10 continue to fluctuate as new vulnerabilities arise, attack agendas vary, malicious actors change, and existing attacks shift because of toolkit economics.

A notable observation from this quarter is the number of attacks originating from the United States (23.62 percent) increasing 14.56 percent compared to last quarter (9.06 percent) and increasing 20.91 percent compared to Q4 2012 (2.71 percent). The United States ousted China as the top supplier of DDoS attacks this quarter.

China (19.09 percent) fell to second place in Q4 2013, a drop of 43.17 percent from the previous quarter's 62.26 percent and a drop of 36.35 percent from Q4 2012 (55.44 percent).

Another significant occurrence was Thailand's rise. Thailand secured third place this quarter with 13.59 percent after not appearing on the top 10 list last quarter and ranking eighth with 3.52 percent in Q4 2012.

Looking at data from the three individual quarters reveals that Asian countries have continually dominated the top 10 list. In Q4 2013, Asian countries accounted for 56.85 percent of attacks from the top 10 countries, with six Asian countries making the list. In Q3 2013, Asian countries accounted for 82.31 percent of the attacks from top 10 countries with six Asian countries making the list. Finally, in Q4 2012, Asian countries accounted for 79.18 percent of attacks from the top 10 list with six Asian countries again making the rankings. While several of the Asian countries have changed their rankings from quarter-to-quarter and rotated on and off the list, in every quarter, an Asian country has ranked either number one or number two as the top producer of DDoS attacks.

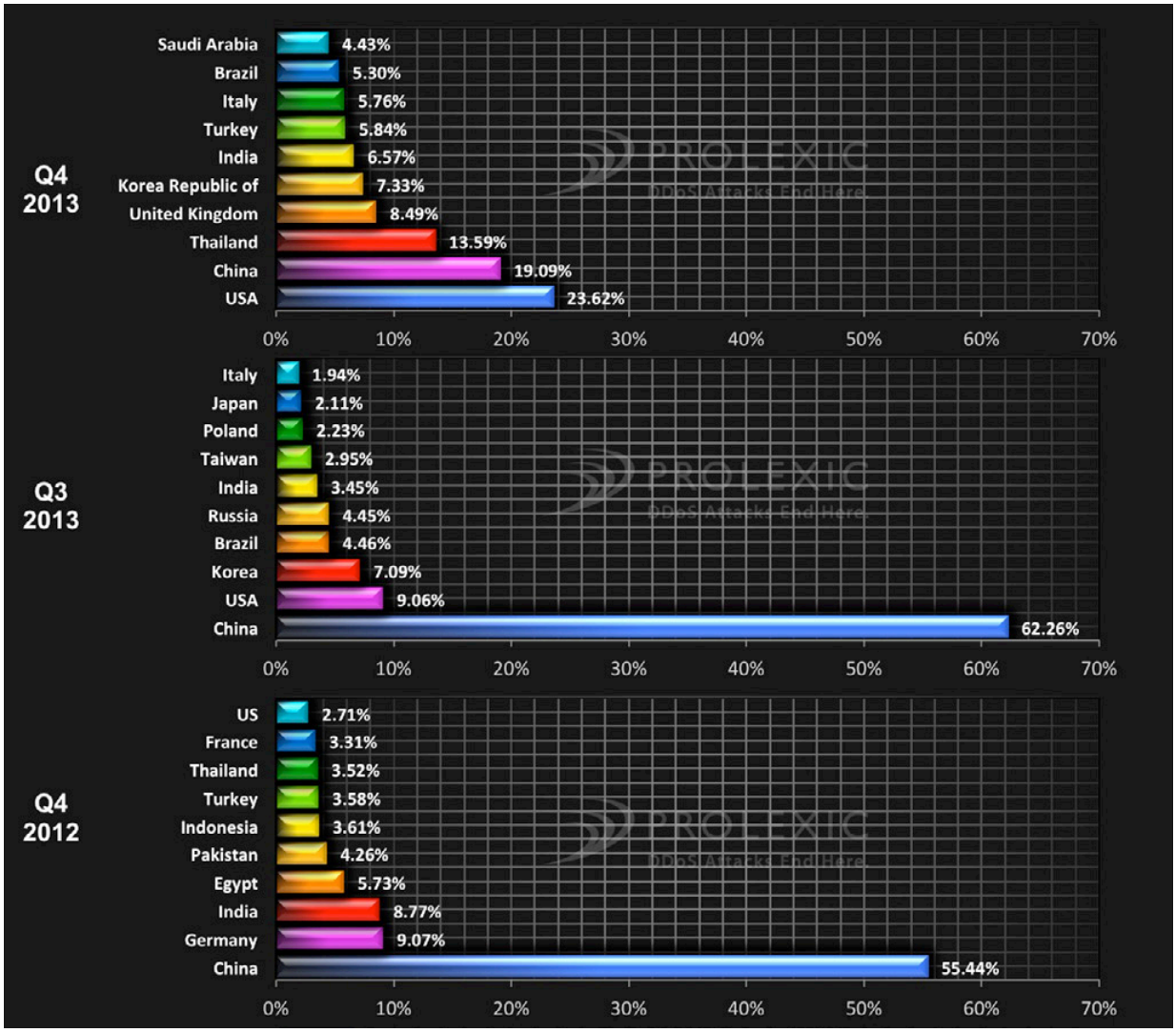

Figure 7: Top 10 source countries for DDoS attacks in Q4 2013, Q3 2013 and Q4 2012

Comparison: Attack campaign start time per day (Q4 2013, Q3 2013, Q4 2012)

In Q4 2013 there was a noticeable shift in the time of day that DDoS attacks took place. Q2 2013 and Q3 2012 saw the majority of attacks occurring around 12:00 GMT (4 a.m. PST and 7 a.m. EST) while attacks in Q4 2013 saw their highest peaks at 20:00 GMT (12 p.m. PST and 3 p.m. EST). The attacks would then fluctuate between 20:00 and 00:00. The second and third most popular attack times were 23:00 GMT (4 p.m. PST and 7 p.m. EST) and 0:00 GMT (3 p.m. PST and 6 p.m. EST). One possible conclusion that could be drawn from this sudden change in the time of attacks is the introduction of new attack campaigns, replacing the itsoknoproblembro campaign, which played a major role in the previous quarters' attack times.

Figure 8 outlines the distribution of attack start times. The graph also shows attack traffic during Q4 2012 and Q3 2013. The data indicates the shift in the time of day that the majority of attacks took place in Q4 2013 compared to Q3 2013 and Q4 2012.

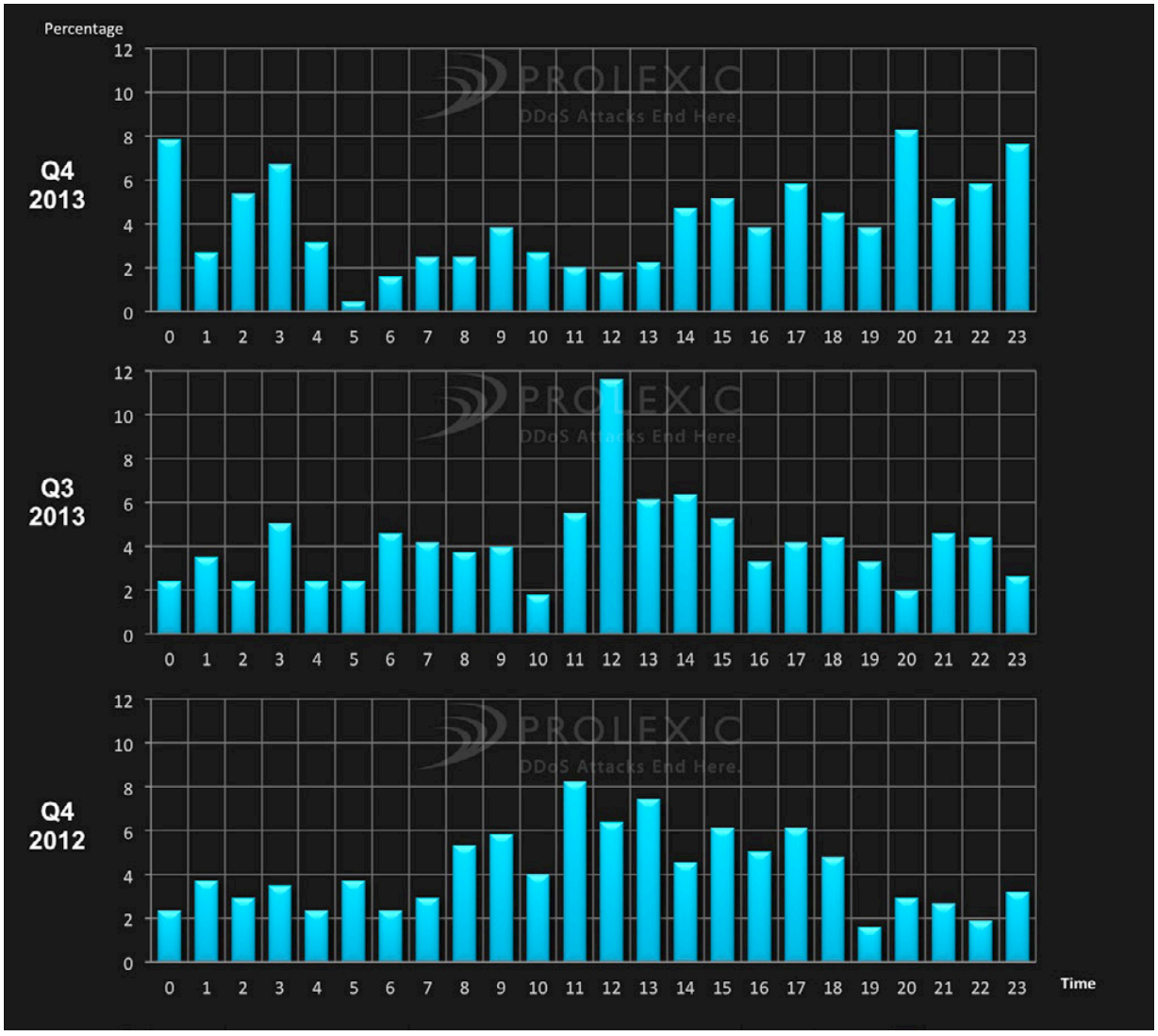

Figure 8: Attack campaign start time in Q4 2013, Q3 2013 and Q4 2012

Attack Spotlight: Multi-vector DDoS campaign

Overview

Multi-vector DDoS attack campaigns make mitigation more difficult, which is the attacker's intention. The addition of each new attack vector requires the DDoS mitigation team to track more details and fight the attack on multiple fronts simultaneously. In Q4 2013, Prolexic blocked the following multi-vector DDoS campaign against a global financial institution. The sophisticated attacks continued for four days, during which time, Prolexic continuously monitored and responded to changing attack signatures and attack methods day and night. Although this campaign was unsuccessful, it was well orchestrated and used multiple attack vectors and custom signatures. In an emerging trend seen in other recent DDoS attacks, mobile phones played a pivotal role in this campaign.

The attack campaign spanned the globe, with Asian botnets playing a large role. The malicious actors leveraged multiple botnets. The main source countries were Indonesia, China, the United States and Mexico.

The source of the botnets was hidden behind a *super proxy* – an IP address that acts as an intermediary for tens of thousands of other computer systems. Legitimate users may use a super proxy for privacy, and many of the computer systems using the same super proxy were not involved in the DDoS attack. To avoid blocking all traffic from the super proxy, the DDoS mitigation team at Prolexic used mitigation technologies employing advanced deep-packet inspection to isolate malicious traffic from legitimate traffic.

The campaign comprised at least twelve different attacks, some of which attempted to take down the target by overwhelming the network layer (Layer 3) while others struck via the application layer (Layer 7). A multi-pronged attack campaign such as this one is more likely to succeed, as it is likely to bypass DDoS mitigation devices. Prolexic combined advanced mitigation technology and skilled DDoS mitigation expertise of engineers to block the attack every time it changed.

This campaign is a good example of how sophisticated malicious actors use a multi-pronged approach, incorporating multiple attack vectors and using every device at their disposal, including mobile phones.

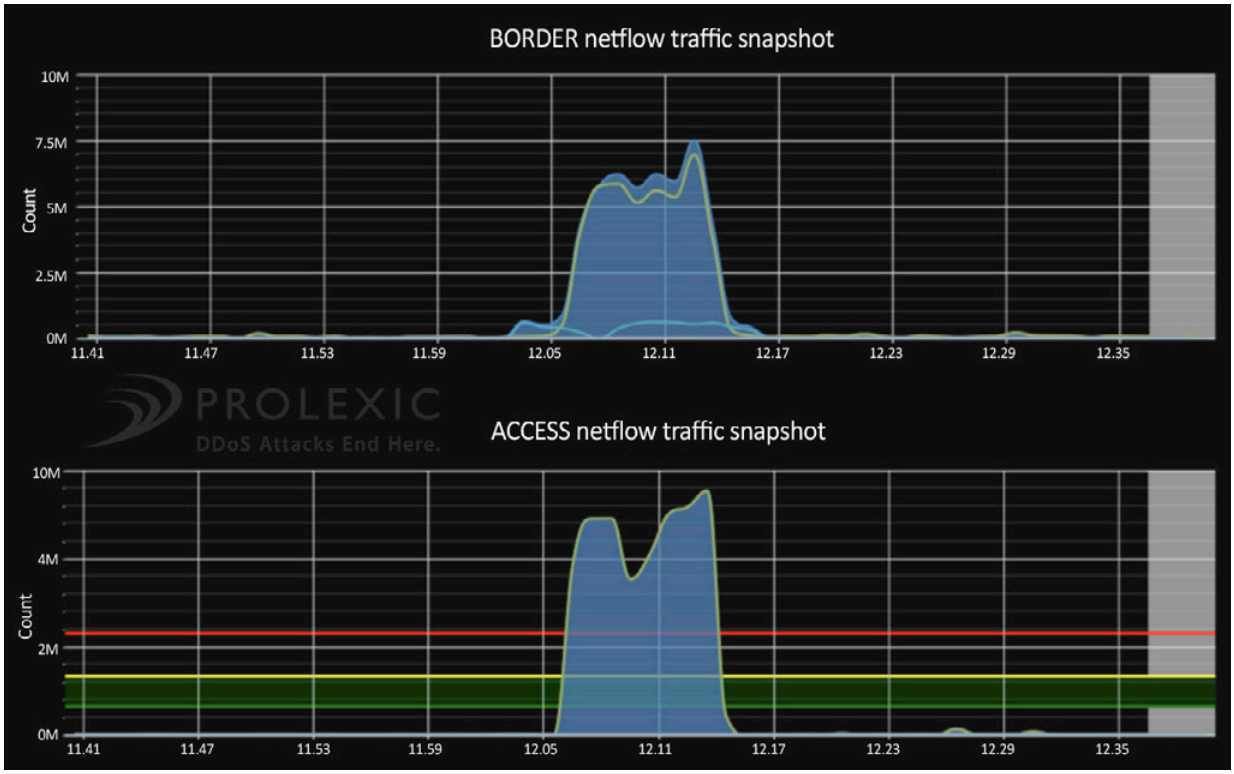

Figure 9: Border traffic and access traffic surged at times during the campaign, as shown in this half-hour timeframe. The attack campaign involved a dozen unique attacks.

Attack vectors in this campaign

Attackers in this campaign used at least 12 unique attacks, one of which included a hacktivist message. The attack signatures indicate the malicious actors recruited voluntary and involuntary participants into the botnet to create an army with which to launch distributed attacks. The mobile applications AnDOSid and mobile Low Orbit Ion Canon (LOIC) played a significant role. In addition, unwitting domain name servers were victimized via spoofing to launch distributed reflection denial of service (DrDoS) attacks.

Volunteers opted into the botnet with Low Orbit Ion Cannon (LOIC)

Botnets are usually formed when servers and personal computers are infected with a Trojan virus or other malware that cause them to become unwitting participants in a DDoS attack. LOIC (see figure 10) is a DDoS tool that takes a different approach as it enables supporters to lend their computing resources by opting into a campaign. To become part of the botnet, a participant simply downloads the tool and voluntarily connects to the command and control server. Once connected, the members of the Anonymous cooperative who lead the attack can control the participating devices remotely via Internet relay chat (IRC) or URL shortening services, such as Bit.ly.

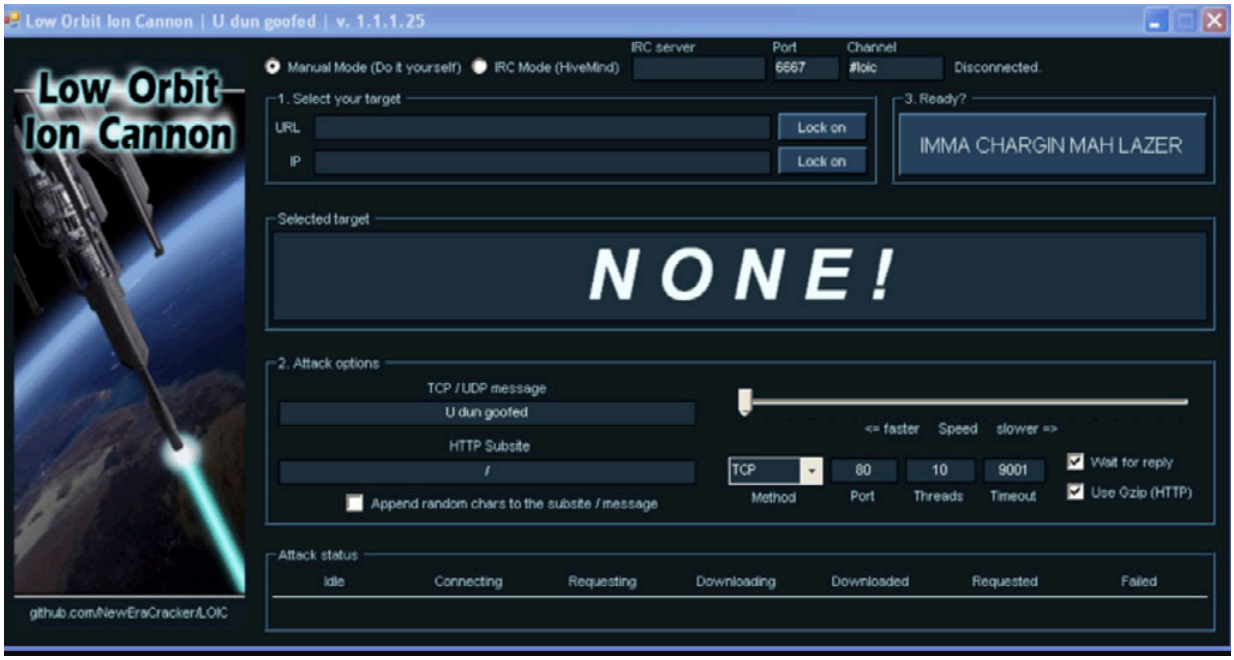

Figure 10: Volunteers can opt into an attack, leaving the attackers to specify the target.

Smartphone users participated using a mobile DoS application

As smartphones become more widespread worldwide, the use of mobile devices is also becoming a primary means of access to the Internet – and of spreading malware. There are an estimated 6.8 billion mobile subscriptions worldwide.[1] In fact, in some developed nations mobile penetration exceeds 100 percent, with some users having more than one mobile phone.

More than a half of the world's mobile subscribers are located in the Asia Pacific region. The fastest growing markets include some of the most populated areas, including China and India. In the Asia Pacific region there are an estimated 3.5 billion mobile subscriptions with mobile market penetration of around 89 percent.[2] China had 820 million mobile users as of July 2013.[3] Many of these devices are used to access the Internet.

Mobile devices are vulnerable to malware. Further, a larger number of devices increases the likelihood of the spread of malware and provides a vector for compromising personal and financial information. The Chinese National Computer Network Emergency Response Technical Team/Coordination Center of China (CNCERT/CC), reported 162,981 samples of mobile malware in 2012, and 82 percent of the malware discovered was targeting smartphones running the Android operating system, which now has the highest number of users worldwide.[4]

PLXsert, has observed an increasing use of mobile devices in DDoS campaigns. This trend is most notable in markets where the main means of access to the Internet is a mobile phone, including Asia.

1 http://mobithinking.com/mobile-marketing-tools/latest-mobile-stats/a#subscribers
2 http://mobithinking.com/mobile-marketing-tools/latest-mobile-stats/a#subscribers
3 http://www.chinainternetwatch.com/3666/china-mobile-internet-users-reached-820m/
4 http://www.zdnet.com/cn/mobile-malware-rises-more-than-25-times-in-china-7000017678/

AnDOSid

Signatures matching AnDOSid, a DDoS attack tool for Android devices, were observed during this campaign. Described as a penetration tester denial of service tool, the AnDOSid mobile application can also produce POST floods, a type of application layer (Layer 7) DDoS attack. Although the app, shown in Figures 11 and 12, states that it is only for use by professional security staff to test their own sites, other device owners used it in this DDoS attack campaign. The app's easy-to-use interface can be operated by inexperienced attackers.

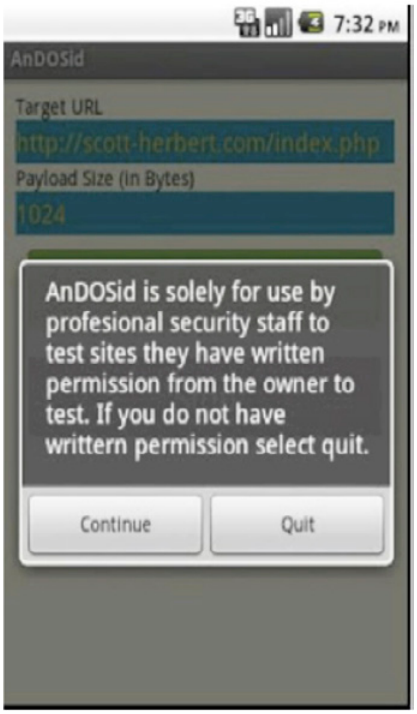

Figure 11: AnDOSid states that it is only intended for use by professional security staff, but DDoSers use it too

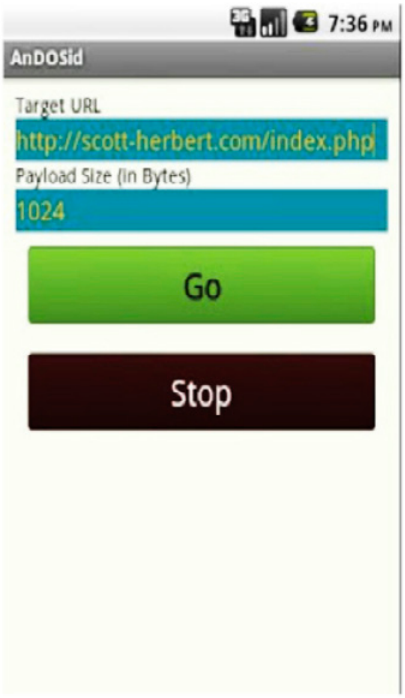

Figure 12: The AnDOSid app is easy to use for less-sophisticated users.

Mobile LOIC

PLXsert also observed the appearance of a new tool called mobile LOIC participating in the attack campaign. This new tool can be installed as an app on Android mobile phones and was available from the official Google Play appstore in December 2013, as shown in Figures 13 and 14.

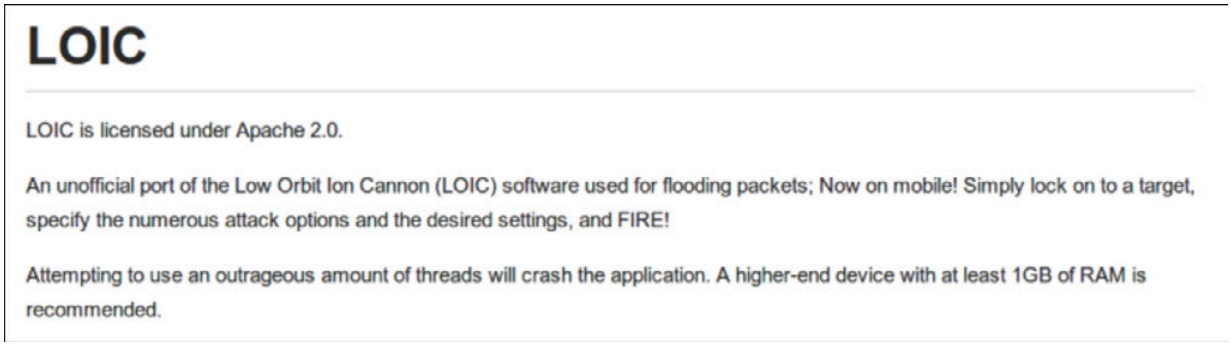

Figure 13: A Pastebin announcement for the capabilities of the mobile Low Orbit Ion Cannon (LOIC) app[5]

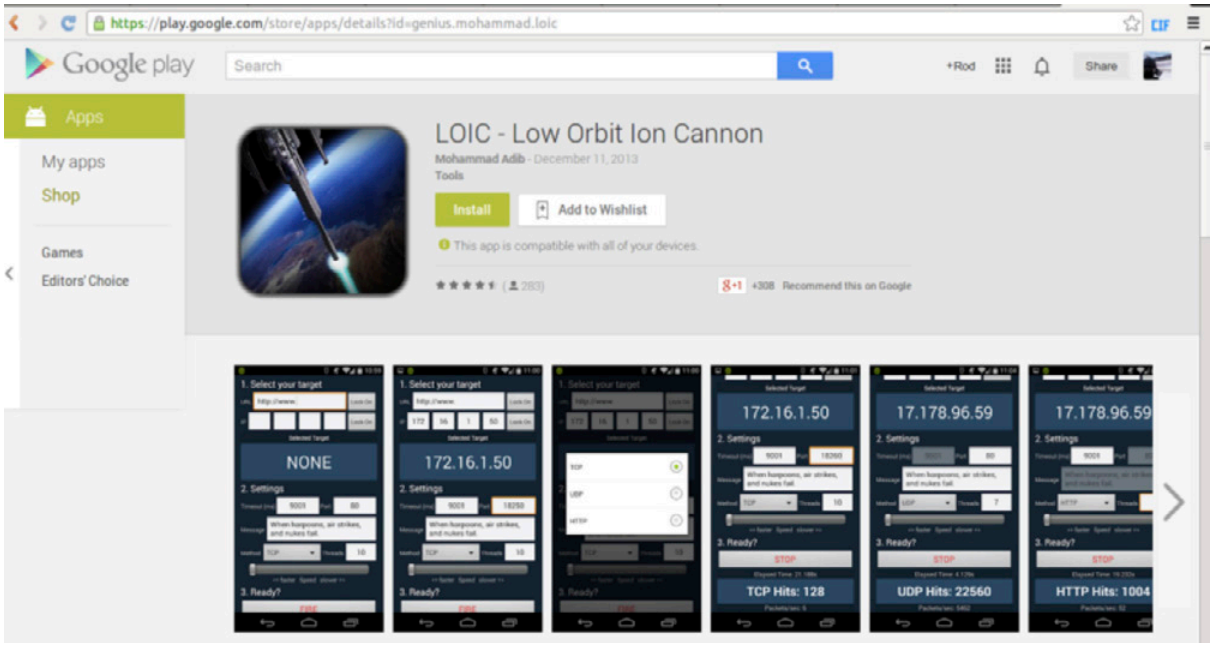

Figure 14: Mobile LOIC was available from the Google Play appstore in December 2013

The availability of these tools in mainstream application stores will rapidly increase user adoption. PLXsert expects a significant increase in the number of mobile devices participating in DDoS campaigns as the availability and adoption of these tools becomes widespread. Considering the rapid advance of mobile technology, especially as smartphone processing power increases, the inclusion of these devices in botnets and DDoS campaigns will certainly increase their use as attack vectors.

Attack signatures reveal more than 12 unique attack vectors

Multiple attack signatures were observed in this campaign, including HEAD floods, GET floods, a POST flood, a SYN flood, a Reset flood, a DNS flood, a UDP fragmentation flood and an ICMP flood, as shown in Figures 15-23. In addition, a POST flood from the AnDOSid app was also identified. Although some of the attacks are easily identified and attributed to commonly known DDoS tools such as LOIC, a combination of many different attack methods can be very powerful and difficult to mitigate.

5 http://pastebin.com/tjNPvdsk

This campaign also contained a political element, seen in one of the attack signatures, where attackers purposely left a message directed at the target. This messaging indicates the participation of hacktivists. PLXsert has observed a growing trend of hacktivist groups and possible state-sponsored participation in DDoS campaigns in the Asia Pacific region. This will be covered in more detail in future PLXsert publications.

```
HEAD /:80 HTTP/1.1
HOST: target domain
User-Agent: Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10_6_4; en-US) AppleWebKit/534.7 (KHTML, like Gecko)
Chrome/7.0.517.44 Safari/534.7
Connection: Keep-Alive



20:04:49.712239 IP x.x.x.x.48652 > x.x.x.x.80: Flags [P.], seq 986161390:986161642, ack 3197510149, win 32,
options [nop,nop,TS val 599702363 ecr 1912020279], length 252
.e..E..0..@.2...E.....P:.....”.... .....
#..[q..7GET /statistics/tables/xls/c06hist.xls?11/19/13 HTTP/1.1
Host: target domain
Accept: text/html;q=1.0, text/*;q=0.8, */*;q=0.5
Accept-encoding: gzip;q=1.0, *;q=0.5
From: webcontent@domain
User-Agent: BLP_bbot/0.1
Connection: Keep-Alive
```

Figure 15: Attack signatures for two different HEAD floods were used in the campaign

```
20:43:09.696305 IP x.x.x.x.15676 > x.x.x.x.80: P 3425550523:3425551602(1079) ack 727945313 win 65535
,....=<.P.-..+c.aP...M...GET /
dili3ezxku5dqv5yquihwsl4k0cyvg4ak4cbcteil8oic3f04he2cfm5zwfzylacqu9uocdgrfbo6dzkzipykvh4waacyg8qz2c
s6qpvlu8vmrnxg7op4dajofy7n641828g9xkbcx8shylhuyby8hllnqrjyv83g9yoz3ogblenj28r931pwzvywfwe9jn577yk
q1oq797rwvgbuon4cmqabmmw8et02hjljzkt2dbtsw9tg7w0rk8pgshe5rz69ey6vp4dv1q4nu8xzvirrz47c8k3vbjlqam
ssuxej6nhgh7b80ytz7qsbe4saenzne0njjdc1nm715kv33j9euel0flhh7ei4sgqjoafeslrctapqf7c9a4gneu114gg8rud6p
zzgxegvr99zwnmhghqcj49n3p3f8d5vpo8q7arkdlju66tkwvvk6q41lphqwmqhq975lovok3z66mwbq8fbo1m0i5o8swj
26aisvhh3711rjg5aaz7wcp5wxfb2481g60ecal9d05piejwpjgtvammlslp3qavddhwg5rquhirexp6b6vidvzkz9ecb06q3
hneo48oef44wqzf63935mdkih2zv93dnslhhc4gty3ab80y51cm3z356fda2h2h9zriiziqe1re7g1r3q6tg264ut38xxu1d
mmj0ffhvikt9o68l4qyvgyk4t93730abg4uugz2er3x4mqa0ws7xsr328aigq8kzvf14c9c9xfzhy67a5ge52c5lmxhtfdq49
5qblabirgcn2q70lqlcmtnuq44hc4sk7oneehhyruqe8y966ridp0tva7zh05v9sn22w0vpfdzz75u4d1r4q3q9owqgfb3du
7iqxc87wl1psrha6meiyj60h496637urm26vcecijutlinkdphujnuvkggwjtr9cygviihwl28ekwo1dmr838qw7zj1g0pad9z4
cj2v0ypds5bff1wt1m1qc9uqxxqhppeqzrkg8zkwe30kfffke0o4geh HTTP/1.1
Host: target domain: IP Address
20:04:51.592355 IP x.x.x.x.56954 > x.x.x.x.80: Flags [P.], seq 589579100:589579352, ack 1851326573, win 46,
options [nop,nop,TS val 1803880352 ecr 1912022157], length 252
.e..E..0E.@.5...E.....z.P#$C\nY.m.....
k...q.$.GET /statistics/tables/xls/f12hist.xls?11/19/13 HTTP/1.1
Host: target domain
Accept: text/html;q=1.0, text/*;q=0.8, */*;q=0.5
Accept-encoding: gzip;q=1.0, *;q=0.5
From: webcontent@domain
User-Agent: BLP_bbot/0.1
Connection: Keep-Alive
```

Continued on next page >

```
11:08:54.366397 IP x.x.x.x.12822 > x.x.x.x.80: P 1380:2760(1380) ack 1 win 4140
....E...W.@.u...n.......2..P'f.....OP..,.b..TOP SPYING INDONESIA ....!!!!!STOP SPYING INDONESIA ....!!!!!STOP
SPYING INDONESIA ....!!!!!STOP SPYING INDONESIA ....!!!!!STOP SPYING INDONESIA ....!!!!!STOP SPYING
INDONESIA ....!!!!!STOP SPYING INDONESIA ....!!!!!STOP SPYING INDONESIA ....!!!!!STOP SPYING
INDONESIA ....!!!!!STOP SPYING INDONESIA ....!!!!!STOP SPYING INDONESIA ....!!!!!STOP SPYING
INDONESIA ....!!!!!STOP SPYING INDONESIA ....!!!!!STOP SPYING INDONESIA ....!!!!!STOP SPYING
INDONESIA ....!!!!!STOP SPYING INDONESIA ....!!!!!STOP SPYING INDONESIA ....!!!!!STOP SPYING
INDONESIA ....!!!!!STOP SPYING INDONESIA ....!!!!!STOP SPYING INDONESIA ....!!!!!STOP SPYING
INDONESIA ....!!!!!STOP SPYING INDONESIA ....!!!!!STOP SPYING INDONESIA ....!!!!!STOP SPYING
INDONESIA ....!!!!!STOP SPYING INDONESIA ....!!!!!STOP SPYING INDONESIA ....!!!!!STOP SPYING
INDONESIA ....!!!!!STOP SPYING INDONESIA ....!!!!!STOP SPYING INDONESIA ....!!!!!STOP SPYING
INDONESIA ....!!!!!STOP SPYING INDONESIA ....!!!!!STOP SPYING INDONESIA ....!!!!!STOP SPYING
INDONESIA ....!!!!!STOP SPYING INDONESIA ....!!!!!STOP SPYING INDONESIA ....!!!!!STOP SPYING
INDONESIA ....!!!!!STOP SPYING INDONESIA ....!!!!!STOP SPYING INDONESIA ....!!!!!STOP SPYING
INDONESIA ....!!!!!STOP SPYING INDONESIA ....!!!!!STOP SPYING INDONESIA ....!!!!!STOP SPYING
INDONESIA ....!!!!!STOP SPYING INDONESIA ....!!!!!STOP SPYING INDONESIA ....!!!!!STOP SPYING
INDONESIA
```

Figure 16: Attack signatures for three GET floods used in the campaign, including a distinct signature to stating, STOP SPYING INDONESIA

```
21:16:47.915443 IP x.x.x.x.59793 > x.x.x.x.80: Flags [P.], seq 3380290312:3380290375, ack 286153051, win
16560, length 63
.e..E..g=.@.w.>...c........P.{#...Y[P.@. ...POST / HTTP/1.1
Host: target domain
Content-length: 5235
```

Figure 17: The attack signature for a POST flood used in the campaign

```
17:43:11.991204 IP x.x.x.x.22121 > x.x.x.x.80: Flags [S], seq 616169472, win 0, length 0
17:43:11.991210 IP x.x.x.x.38148 > x.x.x.x.80: Flags [S], seq 3972726784, win 0, length 0
17:43:11.991214 IP x.x.x.x.38124 > x.x.x.x.80: Flags [S], seq 808779776, win 0, length 0
```

Figure 18: The attack signature for a SYN flood used in the campaign

```
7:23:59.095026 IP x.x.x.x.57688 > x.x.x.x.80: Flags [R], seq 2525888513, win 0, length 0
.e..E..(....3..*BIK......X.P........P...C.........
17:23:59.096321 IP x.x.x.x.19180 > x.x.x.x.80: Flags [R], seq 435486721, win 0, length 0
.e..E..(_)....I9`89.....J..P........P...KB........
17:23:59.096887 IP x.x.x.x.11598 > x.x.x.x.80: Flags [R], seq 4078108673, win 0, length 0
.e..E..(.......5........-N.P........P...+7........
17:23:59.097918 IP x.x.x.x.42975 > x.x.x.x.80: Flags [R.], seq 26083329, ack 872278452, win 1400, options [mss
512], length 0
17:23:59.098729 IP x.x.x.x.31230 > x.x.x.x.80: Flags [R.], seq 3626762241, ack 872236948, win 1400, options
[mss 512], length 0
.e..E..,....#.(...p.....y..P.,..3.G.`..xY.........
```

Figure 19: The attack signature for a Reset flood used in the campaign

```
16:56:52.712955 IP x.x.x.x.53 > x.x.x.x.15389: 17694 2/2/4 NS[|domain]
16:56:52.713051 IP x.x.x.x.53 > x.x.x.x.39354: 26089 1/2/1 TXT[|domain]
16:56:52.713052 IP x.x.x.x.53 > x.x.x.x.6475: 15526 ServFail 0/0/1 (39)
16:56:52.713229 IP x.x.x.x.53 > x.x.x.x.22112: 15526 2/2/0 NS[|domain]
16:56:52.713230 IP x.x.x.x.53 > x.x.x.x.15899: 16379 1/2/3 TXT[|domain
```

Figure 20: The attack signature for a DNS flood used in the campaign

```
16:56:52.712796 IP x.x.x.x > x.x.x.x: udp
16:56:52.712856 IP x.x.x.x > x.x.x.x: udp
16:56:52.712902 IP x.x.x.x > x.x.x.x: udp
```

Figure 21: The attack signature of a UDP fragmentation flood used in the campaign

```
16:35:03.581805 IP x.x.x.x > x.x.x.x: ICMP source quench, length 36
16:35:03.582688 IP x.x.x.x > x.x.x.x: ICMP source quench, length 36
16:35:03.583684 IP x.x.x.x > x.x.x.x: ICMP source quench, length 36
```

Figure 22: The attack signature for an ICMP flood used in the campaign

```
..<.rD..POST / HTTP/1.1
User-Agent: AnDOSid - Android based Http post flooder, for help see http://scott-herbert.com/blog/andosid
Content-Length: 1080
Content-Type: application/x-www-form-urlencoded
Host: target domain
Connection: Keep-Alive

...+rK}.POST / HTTP/1.1
User-Agent: AnDOSid - Android based Http post flooder, for help see http://scott-herbert.com/blog/andosid
Content-Length: 1080
Content-Type: application/x-www-form-urlencoded
Host: target domain
Connection: Keep-Alive
```

Figure 23: The signature of the AnDOSid tool, which runs on the Android operating system and performs an HTTP POST flood attack

Conclusion

This multi-pronged attack from the fourth quarter of 2013 is a prime example of DDoS attacks today. No longer are they simple attacks but instead they take a scatter shot approach, seeking to find any weakness with which to take down a website in number of ways. Attacks of this caliber cannot be stopped by any automated DDoS mitigation device and can only be stopped with the skill and creativity of expert DDoS mitigation engineers.

Case Study: The Asian DDoS Threat

Overview

Recent years have marked a significant rise in distributed denial of service (DDoS) activity from Asia, with targets within the region and around the world. Prolexic has observed malicious actors compromising Chinese and other Asian infrastructure resources and using them as command and control (CnC, CC or C2) and zombies in DDoS botnets. In fact, six of the top 10 source countries for DDoS activity are in Asia: China, Thailand, Korea, Turkey, Saudi Arabia and India – as shown in Figure 24.

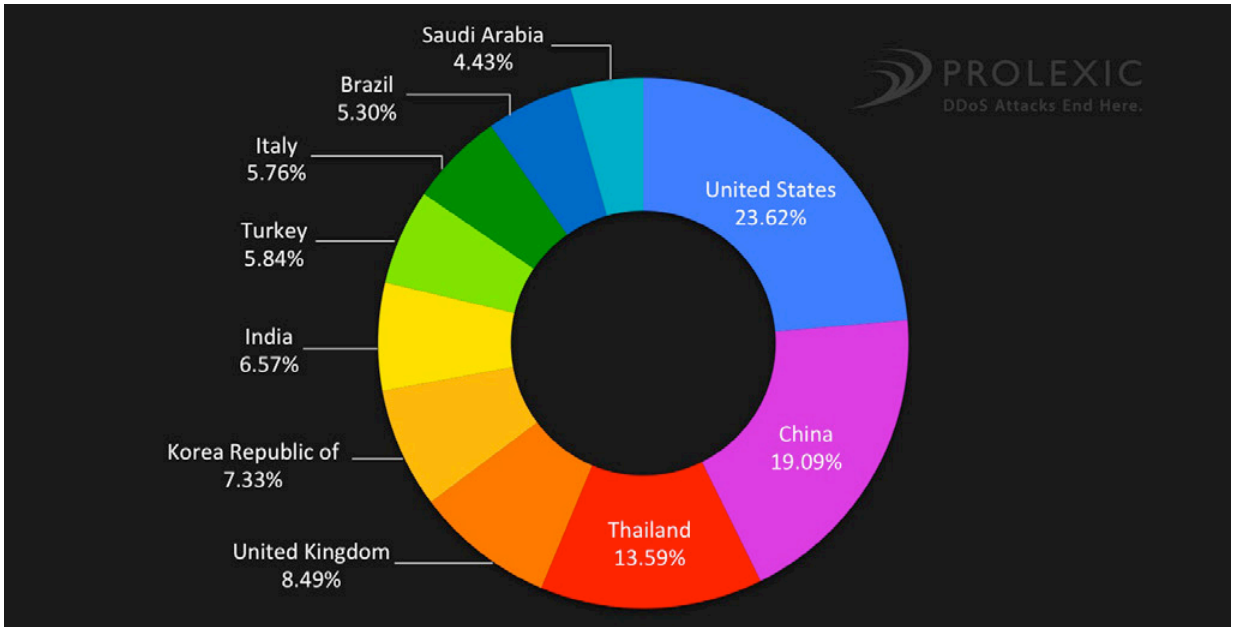

Figure 24: Five of the top 10 source countries for DDoS attacks in Q4 2013 were in Asia

China tops the list of Asian countries for DDoS attacks at 19.09 percent as observed by Prolexic in Q4 2013. The involvement of Asian countries in denial of service attacks is not new. As shown in Figure 25, the percentage of Asian countries participating in denial of service attack campaigns has increased continually since Q4 2012.

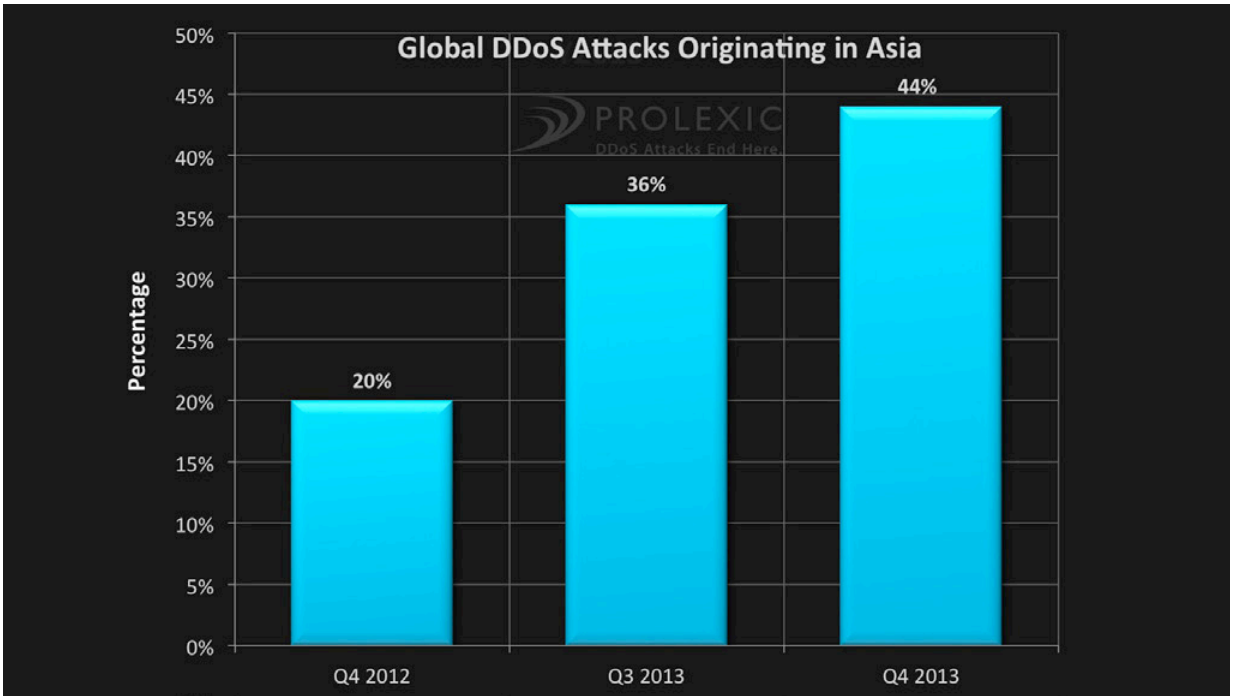

Figure 25: Percent of Global DDoS Attacks with Origins in Asia

With expanded use of the Internet and the addition of data centers in Asia, the region has become a hub for Internet crime and DDoS activity. Regions where technological growth is expanding rapidly are often susceptible to a lack of oversight and shortage of management for large server farms. Malicious actors have been observed taking advantage of these unprotected infrastructure resources.

As detailed in previous attack reports, China has had a persistent and solid position as a key source of DDoS traffic throughout 2013, with a two-fold increase in its role in Q3 2013.

As a result of this rapid expansion of Internet infrastructure and technology, there are significant vulnerabilities that can be exploited by malicious actors. According to a report released by the People's Public Security University of China, the annual economic loss from Internet crime reached 289 billion yuan ($46 billion) in 2012.[6]

Vulnerabilities in Chinese Internet infrastructure

Asia's economic growth has led to more Internet users, more Internet servers and more DDoS activity. China has the largest infrastructure and Internet population in Asia. By June 2012, China had 538 million Internet-connected users, as shown in Figure 26, and was projected to have more than 564 million users by December 2012.[7]

6 http://www.globaltimes.cn/content/758798.shtml
7 http://www1.cnnic.cn/IDR/ReportDownloads/201302/P020130221391269963814.pdf

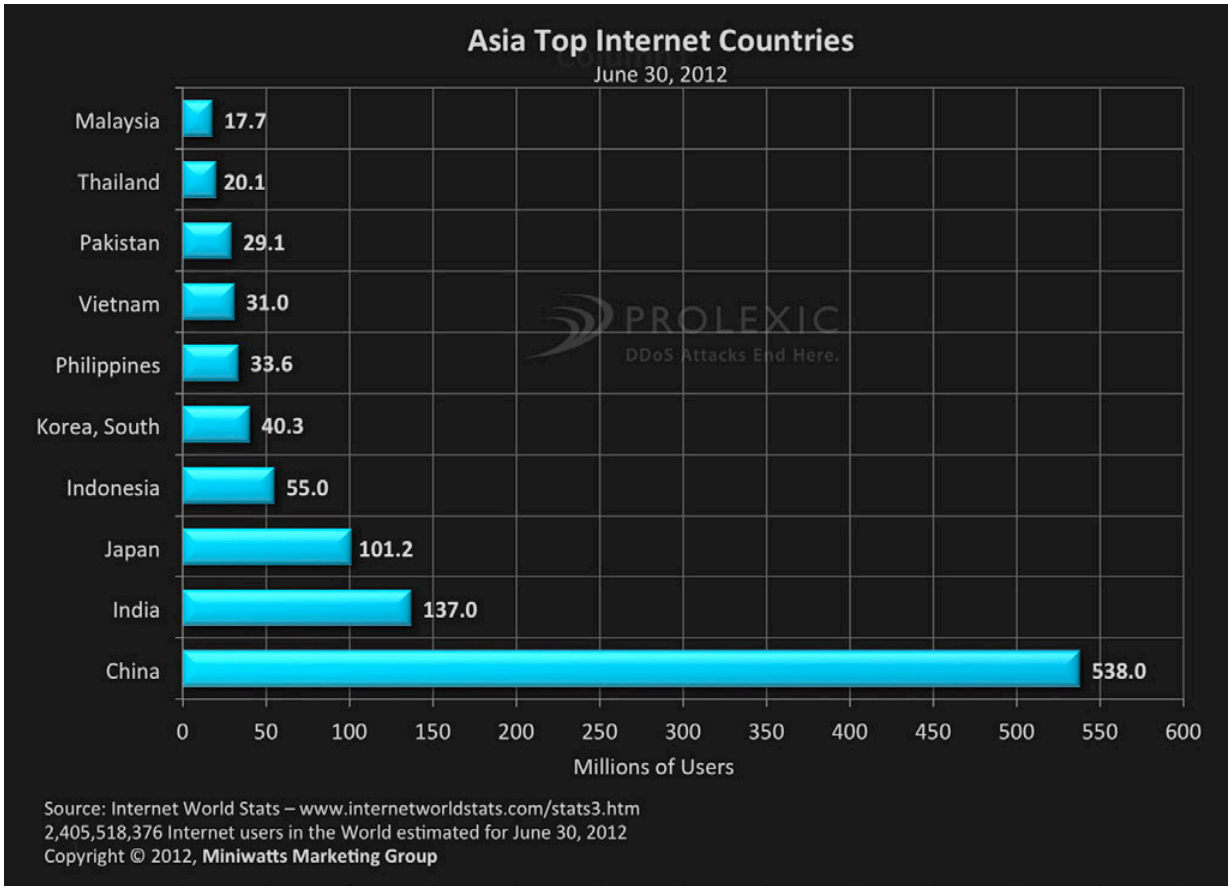

Figure 26: Top countries in Asia by millions of Internet users as of June 2012

The Chinese government has promoted Internet adoption as part of its geopolitical and economic growth strategy and has an aggressive government policy of building new IT infrastructure.[8] This infrastructure is mainly state-owned, though recent deregulation has allowed some foreign companies to partner with state-owned companies to reach the country's goals. The Chinese Internet infrastructure is intended to satisfy demand for a wide range of services including co-location, hosting, disaster recovery and backup, managed services, and Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS) capabilities.

The sheer number of devices in China's Internet-connected IT infrastructure combined with the country's tendency to run older, pirated and unpatched operating systems, creates a serious vulnerability:

- China had an estimated 8.73 million domain names and 2.5 million websites in June 2012[9], creating a huge source of opportunity for hackers.
- The dominant operating system is Windows XP with a prevalence of 60 percent[10], and Microsoft will stop supporting Windows XP on April 8, 2014.[11]
- In China, the software piracy rate was estimated at 80 percent in 2008.[12] Pirated software is rarely updated in order to avoid identification and subsequent suspension of services from software developers.

8 http://www.chinadaily.com.cn/bizchina/2010-07/23/content_11042851.htm
9 http://www1.cnnic.cn/IDR/ReportDownloads/201209/t20120928_36586.htm
10 http://www.chinaInternetwatch.com/3911/windows-os-market-share-august-2013/
11 http://windows.microsoft.com/en-us/windows/end-support-help
12 http://www.nytimes.com/2009/10/19/business/global/19iht-windows.html?_r=0

- China has 330 million IPv4 addresses[13], and is rapidly implementing IPv6 addresses.
- China is estimated to have the highest rate of computer infections of any country.[14]

China also has a huge number of mobile users, as many as 388 million in the first half of 2012. In fact, mobile Internet usage in the country is now believed to have surpassed Internet access via desktop.[15] There are strong indications that these devices also have a high infection rate. In 2012, there were an estimated 162,981 mobile malware programs in China.[16]

Trends in DDoS campaigns originated from China

The growing DDoS threat from China takes several forms, including an increase in DDoS reflection attacks using the CHARGEN protocol, the use of botnets built from Asian IT resources, DDoS attacks by hacktivist groups, and the presence of Chinese DDoS attack kits.

Increasing use of CHARGEN DDoS attacks

One of the factors causing the spike in DDoS traffic from China is the almost forgotten – but now increasingly common – reflection-based DDoS attacks that use the CHARGEN networking protocol. While most CHARGEN attacks come from the United States, China was the second most common source for this type of DDoS attack in Q4 2013, as shown in Figures 27 and 28. PLXsert has observed a growing number of CHARGEN-based DDoS attacks coming from China, and Q4 2013 confirmed the trend.

Q4 2013, as shown in Figures 27 and 28. PLXsert has observed a growing number of CHARGEN-based DDoS attacks coming from China, and Q4 2013 confirmed the trend.

Source Country	Number of CHARGEN DDoS Attacks
United States	273
China	173
Russian Federation	142
Ukraine	54
Republic of Korea	44
Turkey	43
France	32
Germany	30
Canada	22
Romania	21

Figure 27: Top 10 source countries of CHARGEN-based reflection attacks in Q4 2013 by number of attacks observed by Prolexic

13 http://www.bgpexpert.com/addressespercountry.php
14 http://www.switch.ch/export/sites/default/about/news/2013/files/PandaLabs-Quaterly-Report.pdf
15 http://www1.cnnic.cn/IDR/ReportDownloads/201209/t20120928_36586.htm
16 China with most mobile Internet malware spread through smartphone application stores, forums and sites offering other downloadable content. http://www.chinadaily.com.cn/china/2013-07/04/content_16727268.htm http://windows.microsoft.com/en-us/windows/end-support-help

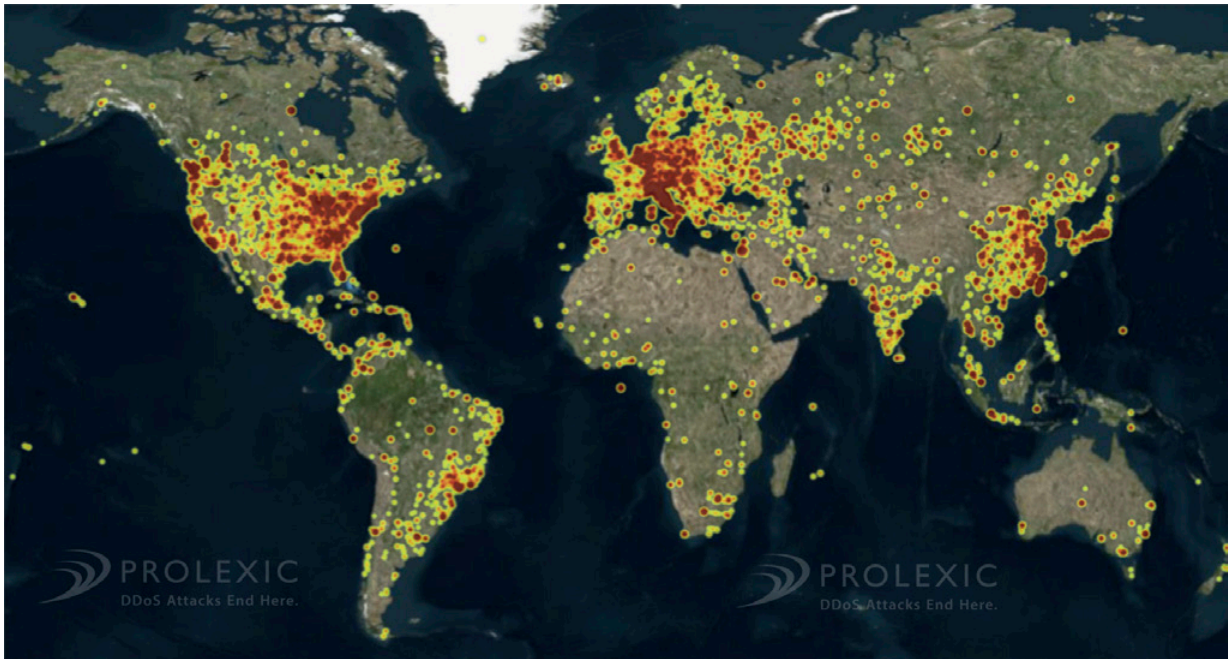

Figure 28: Global distribution of CHARGEN reflector IPs shows a significant cluster in Asia, including China.

PLXsert has identified at least 13,000 CHARGEN servers hosted in China. Factors contributing to a large number of CHARGEN attacks from China are the prevalence of unpatched legacy operating systems and rampant software piracy in the Chinese marketplace. There is a plethora of unpatched vulnerable hosts with the CHARGEN protocol activated by default. In addition, the default configuration of much of the pirated software includes the CHARGEN protocol.

An older protocol now being used in ways it was never intended, CHARGEN is a debugging and measurement tool and a character generator service. When triggered, it simply sends the same output of alphabetic letters and numbers without regard to the input, as shown in Figure 29. The CHARGEN service is susceptible to use in attacks where spoofing the source of transmissions is used by malicious actors as a reflection attack vector. The misuse of the testing features of the CHARGEN service may allow attackers to craft malicious network payloads and reflect them to the target.

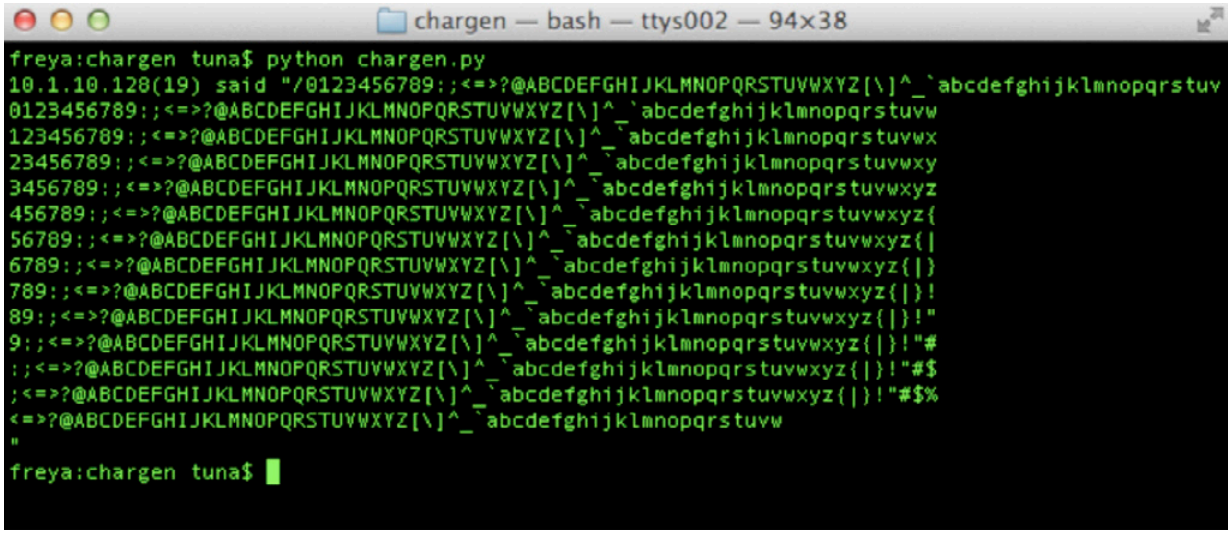

Figure 29: The CHARGEN response from the command line

It's easy enough to turn off the protocol on a server and remediate the risk, if the IT administrator knows how to do it. PLXsert has established a procedure for remediating the use of open CHARGEN services on Windows-based servers.

Botnets built from Asian IT resources

The Asia Pacific region has a diverse population of malicious actors who specialize in credit card fraud, pirating software, malware, botnets and DDoS attacks. Being located in the region with the largest Internet population is also a big driver of opportunity for malicious activity, especially in ransomware and botnets.

Botnets are powerful harvesters of resources, and these resources can be used for multiple attack vectors. The most successful botnet-building DDoS kits tend to be adaptable and have the ability to evade detection and install add-on software that allows the controlled device to be used in a number of ways. For example, toolkit add-on features may provide malware to enable a zombie to be used for tasks such as crypto currency mining and DDoS attack functions. Once the botnet is in place and achieves critical mass, a botmaster is likely to use it for new purposes. One of the interesting developments in the Asia Pacific DDoS threatscape is the use of mobile malware and DDoS kits to bring mobile devices into the botnet.

Hacktivism

The Asia Pacific region is witnessing an emergence of many hacktivist groups that use DDoS attacks as a means of protest. For example, hacktivist groups have launched DDoS attacks against the governments of Singapore and Australia. There are also allegations of state-sponsored DDoS campaigns coming from China, such as the DDoS campaigns against WordPress in 2011 and other Digital Freedom Advocate websites.[17, 18] China has also been the target of large DDoS campaigns, with a significant campaign reported in Q3 2013.[19] Motives and authors of this campaign have yet to be attributed.

17 http://www.prolexic.com/knowledge-center-white-paper-series-dns-reflection-amplification-drdos-attacks-ddos.html
18 http://dissenter.firedoglake.com/2011/09/09/the-idea-that-dos-attacks-against-wikileaks-are-war-crimes/
19 http://www.thewire.com/technology/2013/08/who-hacked-chinas-Internet-yesterday/68712/

Chinese DDoS kits & code snippets

China has a homegrown malicious software development industry that has authored several Chinese DDoS kits. Example attack kits and attack signatures are shown in Figures 30-35. These attack vectors have been responsible for the majority of DDoS attacks originating from China in Q4.

```
CString Msg=”欢迎使用暴风网络压力测试V6\r\n”
                                “\r\n”
                                “请VIP不要私自泄露VIP账号密码，否则将对其进行封号处理\r\n”
                                “\r\n”
                                “软件分为个人版与源码版，源码版除了可以无限期使用软件外，还可获得服务
端源码。\r\n”
                                “\r\n”
                                “综合特色:服务端纯SDK打造，无MFC类，体积小巧，方便免杀，采用Shell
Code特殊方式注入，无DLL穿越防火墙\r\n”
                                “自动探测系统是否支持raw发包 提升攻击效率30 percent，注册服务启动，安
全稳定\r\n”
                                “客户端使用IOCP完成端口上线，无上线限制，具有高效率，高发包率，不死
锁等特点。\r\n”
                                “\r\n”
                                “压力测试模式主要可分为四大类。\r\n”
                                “第一类：流量模式\r\n”
                                “包含TCP多连接攻击，UDP洪水攻击，ICMP洪水攻击，传奇sf专攻等，这些模
式可支持全部系统。\r\n”
                                “\r\n”
                                “第二类：网站压力测试模式\r\n”
                                “CC攻击：使用GET对网页进行请求，直到耗尽网页资源。\r\n”
                                “\r\n”
                                “无敌CC：快速的TCPGET请求，不仅对静态动态网站都有很好的效果，而且
可以对游戏端口进行攻击。\r\n”
                                “\r\n”
                                “模拟打开：模拟IE浏览器真实的访问，在肉鸡多的时候使用可发挥极强的效
果，否则威力较弱。\r\n”
                                “\r\n”
                                “轮回CC：针对带有参数的地址进行攻击，例如：论坛后缀地址等使用
percentd代替真实攻击地址，服务端将只能对网页进行攻击。\r\n”
                                “\r\n”
                                “地三类：综合模式\r\n”
                                “纯流量模式：主要用于对大型服务器，路由设计的攻击模式，可灵活选择应用
达到穿墙目的。\r\n”
                                “\r\n”
                                “纯连接模式：主要针对大型网络游戏，聊天室设计可智能穿越防火墙（攻击端
口必须为开放端口，否则攻击无效）\r\n”
                                “\r\n”
                                “第四类：自定义攻击模式\r\n”
                                “自定义UDP模式：可以自定义UDP数据测试防火墙，支持所有系统。\r\n”
                                “\r\n”
                                “自定义TCP模式：可以自定义TCP数据测试防火墙，支持所有系统。\r\n”
                                “\r\n”
                                “软件只可运行在Windows NT 5.0以上的系统平台，不支持Win 9X系列。\
r\n”
```

Continued on next page >

```
                                        “如果发现软件达不到上述效果可以反馈信息 请直接在VIP群内留言（多数情况是由于肉鸡不够造成的）。\r\n”；

CString Msg = “ Welcome to the Storm network stress testing V6 \ r \ n”
  “\ r \ n”
  “Please do not secretly leaked VIP VIP account password, otherwise the title will be processed \ r \ n”
  “\ r \ n”
  “Software is divided into Personal Edition with source version , in addition to the source code version of the software can be used indefinitely , but also access to server source code . \ R \ n”
  “\ r \ n”
  “Integrated Features : server SDK to create a pure , non- MFC class , compact , easy to avoid killing , using Shell Code injecting a special way , no DLL through the firewall \ r \ n”
  “Automatic detection system supports raw contracting efficiency by 30 percent Increased Attack registered service starts , security and stability \ r \ n”
  “ The client uses IOCP completion port on the line, the line limit supreme , with high efficiency, high contracting rates , no deadlock characteristics . \ R \ n”
  “\ r \ n”
  “Stress test mode can be divided into four categories . \ R \ n”
  “ First class: traffic patterns \ r \ n”
  “ Contains multiple TCP connections attack , UDP flood attacks , ICMP flood attacks, specializing legendary sf , these models can support the entire system . \ R \ n”
  “\ r \ n”
  “ The second category : Website stress test mode \ r \ n”
  “CC attacks: using a GET request to the web pages until exhausted web resources \ r \ n.”
  “\ r \ n”
  “Invincible CC: Fast TCPGET request , not only for static and dynamic websites have good results, but also for the game port to attack \ r \ n.”
  “\ r \ n”
  “Analog Open : Analog IE browser to access the real , when in use in many broiler can play a very strong effect, or the power of the weaker \ r \ n.”
  “\ r \ n”
  “ Reincarnation CC: address with parameters for the attack , such as : forums suffix address using percent d instead of attacking the real address of the web server will only attack \ r \ n.”
  “\ r \ n”
  “ In three categories: integrated mode \ r \ n”
  “Pure Flow mode: mainly used for large servers , routing design attack mode , the flexibility to choose the application through the wall to reach the purpose of \ r \ n.”
  “\ r \ n”
  “Pure Connection Mode : mainly for large-scale online games, chat rooms designed intelligently through the firewall ( port must be open port attack , attack otherwise invalid ) \ r \ n”
  “\ r \ n”
  “ The fourth category : Custom attack mode \ r \ n”
  “Custom UDP mode: You can customize the firewall UDP test data to support all system \ r \ n”
  “\ r \ n”
  “Custom TCP mode: You can customize the data to test the firewall TCP support all systems \ r \ n.”
  “\ r \ n”
  “ Software only runs on Windows NT 5.0 or more platform does not support Win 9X series . \ R \ n”
  “ If you find software can not meet the above effect feedback , please leave a message directly in the VIP group ( in most cases is due to the inadequacy of the broiler ) \ r \ n.” ;
```

Figure 30: The Chinese Storm Network stress testing toolkit, offering multiple DDoS attack vectors, was distributed through a private, paid forum

```
void CCcDlg::OnButton8()
{
// TODO: Add your control notification handler code here
UpdateData();
//here to set forbid list
//here is the exact site
if (m_Target2Add.Find (“xiakexing.com”,0)>0)
{
AfxMessageBox(“This Site is Forbid!”);
return;
}
if (m_Target2Add.Find (“itaq.ynpc.com”,0)>0)
{
AfxMessageBox(“This Site is Forbid!”);
return;
}
if (m_Target2Add.Find (“hacker.com.cn”,0)>0)
{
AfxMessageBox(“This Site is Forbid!”);
return;
}
//here is some site
if (m_Target2Add.Find (“.20cn.”,0)>0)
{
AfxMessageBox(“This Site is Forbid!”);
return;
}
if (m_Target2Add.Find (“.77169.”,0)>0)
{
AfxMessageBox(“This Site is Forbid!”);
return;
}
if (m_Target2Add.Find (“.xfocus.”,0)>0)
{
AfxMessageBox(“This Site is Forbid!”);
return;
}
if (m_Target2Add.Find (“.cnhonker.”,0)>0)
{
AfxMessageBox(“This Site is Forbid!”);
return;
}
//here is a wide site
if (m_Target2Add.Find (“gov.cn/”,0)>0)
{
AfxMessageBox(“This Site is Forbid!”);
return;
}
if (m_Target2Add.Find (“edu.cn/”,0)>0)
{
AfxMessageBox(“This Site is Forbid!”);
return;
}
m_Attack.AddString (m_Target2Add);
}
```

Figure 31: This Chinese DDoS code snippet, found on Chinese underground forums, was intended to protect several Chinese government, educational and other Chinese sites from attack

```
..<.rD..POST / HTTP/1.1
User-Agent: AnDOSid - Android based Http post flooder, for help see http://scott-herbert.com/blog/andosid
Content-Length: 1080
Content-Type: application/x-www-form-urlencoded
Host: www.targetvictim.com
Connection: Keep-Alive

...+rK}.POST / HTTP/1.1
User-Agent: AnDOSid - Android based Http post flooder, for help see http://scott-herbert.com/blog/andosid
Content-Length: 1080
Content-Type: application/x-www-form-urlencoded
Host: www.targetvictimcom
Connection: Keep-Alive
```

Figure 32: Mobile DDoS attack signature (AnDOSid) observed in a recent POST flood campaign in the Asia Pacific region

```
if (http.Left(1)=="G")
{
    //Get Mode,No Sorted Mode
    http=http.Right (http.GetLength ()-1);
    url="GET "+rsCS(jj)+" HTTP/1.1\r\n"
        +"Accept: */*\r\n"
        +"Referer:"+http
        +"\r\nAccept-Language: zh-cn\r\nAccept-Encoding: gzip, deflate\r\n"
        +"User-Agent:Mozilla/4.0 (compatible; MSIE 6.0; Windows 5.1)"
        +"\r\nHost:"+rhost
        +"\r\nProxy-Connection: Keep-Alive\r\nPragma: no-cache\r\n";
}
else
{
    //Post Mode,No Sorted Mode
    arg1=http.Right(http.GetLength ()-1);   //去掉GP
    mi=http.Find("?",0);if (http.Find("?",mi+1)>0) mi=http.Find("?",mi+1);  //找到参数的位置
    arg2=rsCS(arg1.Right(arg1.GetLength ()-mi));   //获得参数arg2并且做处理
    arg1=rsCS(arg1.Left(mi-1));      //获得要提交的URL
    larg.Format ("%d",arg2.GetLength());    //获得参数长度larg
    url="GET "+rsCS(jj)+" HTTP/1.1\r\n"
        +"Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, application/vnd.ms-excel,
        +"Accept-Language: zh-cn\r\n"
        +"Accept-Encoding: gzip, deflate"
        +"\r\nUser-Agent:Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)"
        +"\r\nHost:"+rhost
        +"\r\nConnection: Keep-Alive"
        +"\r\n\r\n";
}
    while (1)
```

Figure 33: Attack signature for a popular Layer 7 Chinese DDoS attack vector

```
========================================================================
      MICROSOFT FOUNDATION CLASS LIBRARY : DDOS
========================================================================


AppWizard has created this DDOS application for you.  This application
not only demonstrates the basics of using the Microsoft Foundation classes
but is also a starting point for writing your application.

This file contains a summary of what you will find in each of the files that
make up your DDOS application.

DDOS.dsp
    This file (the project file) contains information at the project level and
    is used to build a single project or subproject. Other users can share the
    project (.dsp) file, but they should export the makefiles locally.

DDOS.h
    This is the main header file for the application.  It includes other
    project specific headers (including Resource.h) and declares the
    CDDOSApp application class.

DDOS.cpp
    This is the main application source file that contains the application
    class CDDOSApp.

DDOS.rc
    This is a listing of all of the Microsoft Windows resources that the
    program uses.  It includes the icons, bitmaps, and cursors that are stored
    in the RES subdirectory.  This file can be directly edited in Microsoft
        Visual C++.

DDOS.clw
    This file contains information used by ClassWizard to edit existing
    classes or add new classes.  ClassWizard also uses this file to store
    information needed to create and edit message maps and dialog data
    maps and to create prototype member functions.

res\DDOS.ico
    This is an icon file, which is used as the application's icon.  This
    icon is included by the main resource file DDOS.rc.

res\DDOS.rc2
    This file contains resources that are not edited by Microsoft
        Visual C++.  You should place all resources not editable by
        the resource editor in this file.
```

Figure 34: ReadMe section from feilongyali, a Chinese DDoS kit for a low-level GET flood. This library is often packaged in other Chinese malware.

Figure 35: A website offering the feilongyali toolkit

Conclusion

Asia is an important contributor to the current and future DDoS threatscape. Internet adoption will continue to spread, data centers will expand, and growing economies will come to use the Internet as fundamental means of conducting day-to-day business functions, such as e-banking and e-commerce.

Given current trends, PLXsert expects the use of mobile devices in malicious acts to expand. Malicious actors will seek to target these devices because they have the ability to infect so many users. Attackers will deliver malware and malicious code to more mobile devices, increasing the role of these devices in DDoS attack campaigns.

PLXsert also anticipates an increase in DDoS activity from existing hacktivist groups and the appearance of new hacktivist groups. Many of these groups have emulated the Anonymous iconography, but their core values differ, as their missions are defined by nationalism and religion. These groups may join DDoS attack campaigns that involve regional rivalries within the Asia Pacific region as the regional powers compete in financial, geographical and political arenas.

China will become the epicenter of the DDoS threatscape by nature of having the largest Internet population and infrastructure, being a significant economic power, and having a foreign policy strategy that involves using the Internet to gain advantage over regional and world adversaries. Past experience leads PLXsert to anticipate that the Chinese government will participate in DDoS campaigns that involve vertical markets and types of business deemed illegal in Mainland China, such as online gambling.

Looking forward

Looking back over 2013, the most significant developments from the DDoS front lines have been Layer 7 DDoS toolkits, the use of reflection and amplification in attacks, and Best Common Practice 38 (BCP 38) adoptions.

Over the last quarter, PLXsert has examined the sourcing of malicious application layer traffic by Asian countries. We identified a high amount of code reuse and public DDoS attack source code, available on private forums and pay-to-use websites. A perfect example is *Storm network stress testing v.6*, a DDoS library written for .NET. Storm network stress testing attacks have plagued the Internet since 2007 as validated by archived mitigation rules used and associated signatures for these attack vectors.

The resurrection of amplified Distributed Reflection Denial of Service (DrDoS) has been an aggravation for those that are prepared and a nightmare for corporate infrastructures unprepared or without the resources to handle these attacks. With amplification ratios reaching 50:1, this approach has reduced the resources needed for malicious actors to perform devastating infrastructure attacks with as little as three servers. For example, in a DNS reflection scenario, an attacker created a resource record that had a maximum response size of 4176 bytes that could be retrieved with an 83 byte request. This, along with thousands of misconfigured DNS servers on the Internet, provides the attacker with 50 times the original attack bandwidth. In theory, if an attacker had access to two servers with 1 Gbps links, the attacker could potentially generate as much as 100 Gbps of amplified response traffic.

If the security community were to remediate all misconfigured CHARGEN and NTP servers, the Internet as a whole would benefit. Of course fixing just one server is better than not fixing any, even though attackers would just find another way to amplify traffic using other vulnerable protocols. This situation is why the Internet Engineering Task Force (IETF) spent time drafting Best Common Practice 38 (BCP38). This document proposes ingress filtering at the Internet service provider level to deny packets with forged addresses a route to the Internet. This is the most efficient way to solve the problem of amplification or reflection in general. Unfortunately, this comes at a cost for the ISPs and hosting providers that the attackers are using to launch these attacks. This difficulty is not true of all ISPs though. One of the major implementers of this in the United States has been Comcast, which has removed the ability for actors to utilize its services to participate in this style of attacks on their network. If more local and commercial carriers would follow in Comcast's footsteps this advantage could be removed from malicious actors.

So what will 2014 bring? We hope so to see researchers continuing their efforts on misconfigured host cleanup, thereby putting a dent in the attackers' amplification arsenal. We hope that security organizations continue to work with carriers to move on BCP38 deployment initiatives. And there are communities that will continue to keep the Internet usable for everyone. At the same time, we are aware that malicious actors will continue to abuse these services and will research more ways and protocols that can be abused above these 50:1 ratios.

Mobile DDoS attacks that have been researched in the past will start to become part of the attackers' arsenal as well. Most of these will likely be seen targeting specific web services or application programming interfaces (APIs). We also expect infrastructure attacks to become more of an issue for small- to medium-sized businesses without mitigation service providers because of the rise in inexpensive and easy-to-use DDoS-for-hire sites surfacing all over 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 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 Fort Lauderdale, 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.