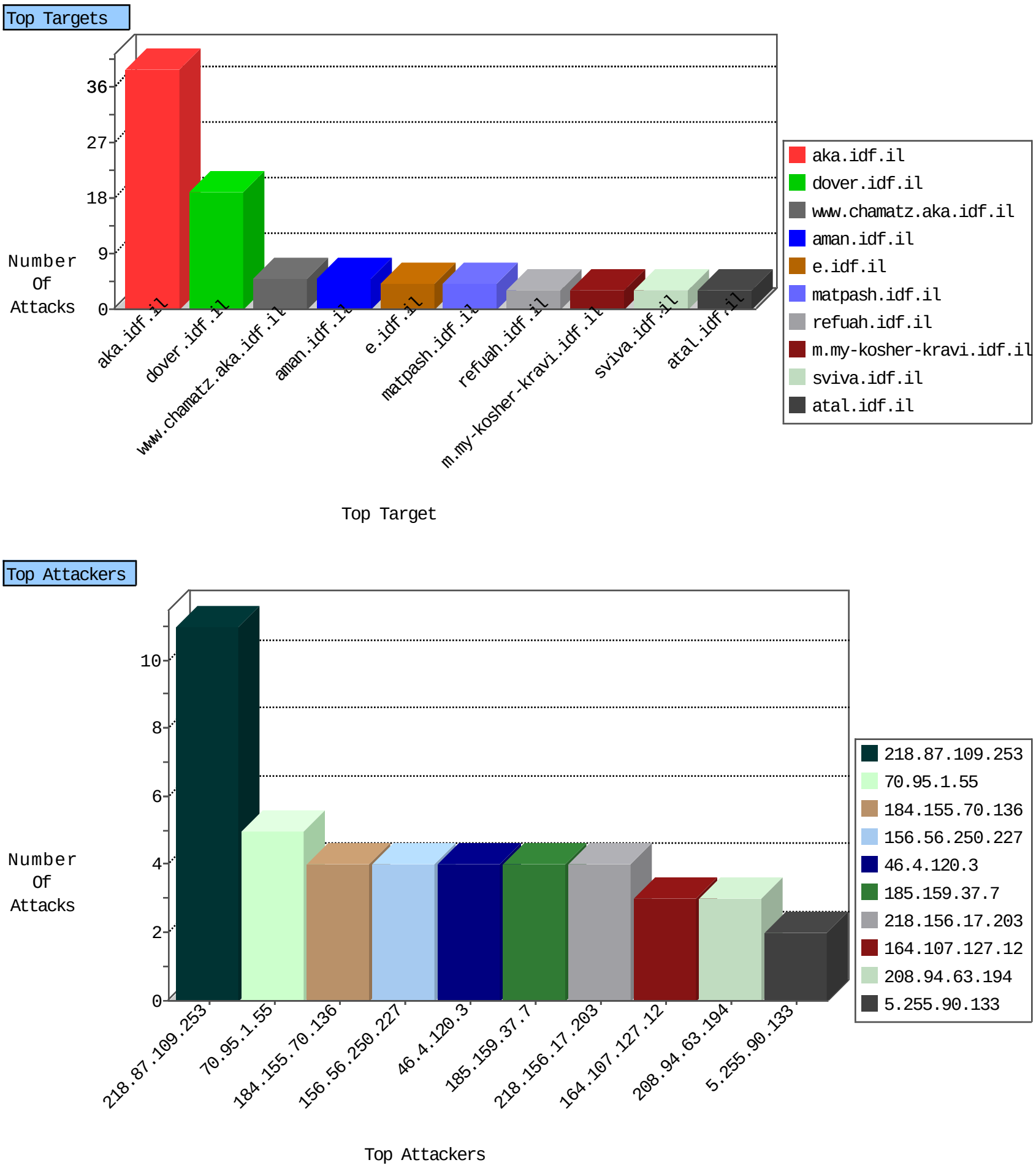
09-19-2016-04:04:04 to 09-19-2016-05:04:04

# IDF Under Attack Daily Report



09-19-2016-04:04:04 to 09-19-2016-05:04:04

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 156.56.250.227 | United States | 147.237.72.166 | aka.idf.il | network flood IPv4 ICMP | drop | 4 |
| 164.107.127.12 | United States | 147.237.72.166 | aka.idf.il | network flood IPv4 ICMP | drop | 3 |
| 208.94.63.194 | United States | 147.237.72.166 | aka.idf.il | network flood IPv4 ICMP | drop | 3 |
| 129.93.229.139 | United States | 147.237.72.166 | aka.idf.il | network flood IPv4 ICMP | drop | 2 |
| 204.85.191.11 | United States | 147.237.72.166 | aka.idf.il | network flood IPv4 ICMP | drop | 2 |
| 129.93.229.138 | United States | 147.237.72.166 | aka.idf.il | network flood IPv4 ICMP | drop | 1 |
| 200.19.159.34 | Brazil | 147.237.72.166 | aka.idf.il | network flood IPv4 ICMP | drop | 1 |
| 143.225.229.236 | Italy | 147.237.72.166 | aka.idf.il | network flood IPv4 ICMP | drop | 1 |
| 128.42.142.45 | United States | 147.237.72.166 | aka.idf.il | network flood IPv4 ICMP | drop | 1 |
| 195.113.161.84 | Czech Republic | 147.237.72.166 | aka.idf.il | network flood IPv4 ICMP | drop | 1 |
| 153.90.1.34 | United States | 147.237.72.166 | aka.idf.il | network flood IPv4 ICMP | drop | 1 |
| 128.223.8.112 | United States | 147.237.72.166 | aka.idf.il | network flood IPv4 ICMP | drop | 1 |
| 198.82.160.221 | United States | 147.237.72.166 | aka.idf.il | network flood IPv4 ICMP | drop | 1 |
| 130.195.4.69 | New Zealand | 147.237.72.166 | aka.idf.il | network flood IPv4 ICMP | drop | 1 |
| 128.10.18.52 | United States | 147.237.72.166 | aka.idf.il | network flood IPv4 ICMP | drop | 1 |
| 129.10.120.193 | United States | 147.237.72.166 | aka.idf.il | network flood IPv4 ICMP | drop | 1 |
| 198.133.224.147 | United States | 147.237.72.217 | e.idf.il | network flood IPv4 ICMP | drop | 1 |
| 134.197.113.3 | United States | 147.237.72.166 | aka.idf.il | network flood IPv4 ICMP | drop | 1 |
| 128.42.142.45 | United States | 147.237.72.156 | aman.idf.il | network flood IPv4 ICMP | drop | 1 |

09-19-2016-04:04:04 to 09-19-2016-05:04:04

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 46.4.120.3 | Germany | 147.237.72.166 | aka.idf.il | C1000074: HTTP: majestic bot | Permit | 2 |
| 46.4.120.3 | Germany | 147.237.76.42 | refuah.idf.il | C1000074: HTTP: majestic bot | Permit | 2 |

09-19-2016-04:04:04 to 09-19-2016-05:04:04

Top Attackers In IDS

| Attacker Address | Target Address | Attacker Country | Site | Signature | Count |
|---|---|---|---|---|---|
| 89.74.234.251 | 147.237.72.166 | Poland | aka.idf.il | Xenu Link Sleuth User Agent | 2 |
| 213.128.65.141 | 147.237.0.17 | Turkey | m.my-kosher-kravi.idf.il | ET SCAN Potential SSH Scan | 1 |
| 163.172.238.45 | 147.237.77.170 | United Kingdom | maarachot.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 117.21.248.87 | 147.237.0.34 | China | tikshuv.idf.il | ET SCAN Potential SSH Scan | 1 |
| 218.87.109.253 | 147.237.77.226 | China | www.chamatz.aka.idf.il | ET SCAN Potential SSH Scan | 1 |
| 113.240.250.154 | 147.237.77.179 | China | e.mazi.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 218.87.109.253 | 147.237.77.178 | China | e.matpash.idf.il | ET SCAN Potential SSH Scan | 1 |
| 83.56.9.24 | 147.237.76.44 | Spain | e.refuah.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 218.87.109.253 | 147.237.77.170 | China | maarachot.idf.il | ET SCAN Potential SSH Scan | 1 |
| 31.24.228.20 | 147.237.72.217 | United Kingdom | e.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 218.87.109.253 | 147.237.72.217 | China | e.idf.il | ET SCAN Potential SSH Scan | 1 |
| 5.255.90.133 | 147.237.72.156 | Netherlands | aman.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 218.87.109.253 | 147.237.72.166 | China | aka.idf.il | ET SCAN Potential SSH Scan | 1 |
| 213.128.65.141 | 147.237.77.216 | Turkey | dover.idf.il | ET SCAN Potential SSH Scan | 1 |
| 188.138.56.180 | 147.237.0.33 | Germany | idf.il | ET SCAN Potential SSH Scan | 1 |
| 117.21.248.87 | 147.237.77.216 | China | dover.idf.il | ET SCAN Potential SSH Scan | 1 |
| 218.87.109.253 | 147.237.77.235 | China | sviva.idf.il | ET SCAN Potential SSH Scan | 1 |
| 115.219.86.245 | 147.237.8.28 | China | e.mobile-ks.idf.il | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |
| 218.87.109.253 | 147.237.77.205 | China | prisha.idf.il | ET SCAN Potential SSH Scan | 1 |
| 218.87.109.253 | 147.237.77.176 | China | matpash.idf.il | ET SCAN Potential SSH Scan | 1 |
| 80.15.154.133 | 147.237.76.176 | France | test.ncore.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 218.87.109.253 | 147.237.76.34 | China | yohalan.idf.il | ET SCAN Potential SSH Scan | 1 |
| 5.255.90.133 | 147.237.72.217 | Netherlands | e.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 218.87.109.253 | 147.237.72.167 | China | ishurim.aka.idf.il | ET SCAN Potential SSH Scan | 1 |
| 218.87.109.253 | 147.237.0.17 | China | m.my-kosher-kravi.idf.il | ET SCAN Potential SSH Scan | 1 |

09-19-2016-04:04:04 to 09-19-2016-05:04:04

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 70.95.1.55 | United States | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 5 |
| 184.155.70.136 | United States | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 4 |
| 212.143.142.56 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 2 |
| 185.159.37.7 | | 147.237.77.235 | sviva.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 1 |
| 141.212.122.103 | United States | 147.237.72.156 | aman.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 1 |
| 71.6.167.142 | United States | 147.237.77.176 | matpash.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 1 |
| 218.156.17.203 | Korea, Republic of | 147.237.0.17 | m.my-kosher-kravi.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 1 |
| 176.13.245.176 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 1 |
| 138.246.253.19 | Germany | 147.237.76.202 | e.halag.idf.il | Geo-location enforcement | Geo-location inbound enforcement | drop | 1 |
| 195.62.53.168 | Russian Federation | 147.237.8.27 | e.madim.atal.idf.il | Geo-location enforcement | Geo-location inbound enforcement | drop | 1 |
| 141.212.122.108 | United States | 147.237.77.226 | www.chamatz.aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 1 |
| 74.82.47.20 | United States | 147.237.8.14 | e.orchot.idf.il | Geo-location enforcement | Geo-location inbound enforcement | drop | 1 |
| 218.156.17.203 | Korea, Republic of | 147.237.0.19 | madim.atal.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 1 |
| 141.212.122.67 | United States | 147.237.77.226 | www.chamatz.aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 1 |
| 195.62.53.168 | Russian Federation | 147.237.77.121 | e.navy.idf.il | Geo-location enforcement | Geo-location inbound enforcement | drop | 1 |
| 141.212.122.109 | United States | 147.237.77.226 | www.chamatz.aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 1 |
| 76.236.121.228 | United States | 147.237.77.176 | matpash.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 1 |
| 218.156.17.203 | Korea, Republic of | 147.237.0.200 | m4u.idf.il | Geo-location enforcement | Geo-location inbound enforcement | drop | 1 |
| 185.20.5.157 | United Kingdom | 147.237.72.166 | aka.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 1 |
| 141.212.122.68 | United States | 147.237.77.226 | www.chamatz.aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 1 |
| 5.102.242.169 | Israel | 147.237.72.156 | aman.idf.il | drop | First packet isn't SYN | drop | 1 |
| 141.212.122.109 | United States | 147.237.77.227 | e.hamaz.idf.il | Geo-location enforcement | Geo-location inbound enforcement | drop | 1 |
| 106.38.241.105 | China | 147.237.0.34 | tikshuv.idf.il | drop | SAM rule | drop | 1 |
| 185.159.37.7 | | 147.237.77.235 | sviva.idf.il | drop | First packet isn't SYN | drop | 1 |
| 141.212.122.102 | United States | 147.237.72.156 | aman.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 1 |
| 218.156.17.203 | Korea, Republic of | 147.237.0.15 | kosher-kravi.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 1 |
| 141.212.122.110 | United States | 147.237.77.227 | e.hamaz.idf.il | Geo-location enforcement | Geo-location inbound enforcement | drop | 1 |
| 106.38.241.105 | China | 147.237.72.166 | aka.idf.il | drop | SAM rule | drop | 1 |

09-19-2016-04:04:04 to 09-19-2016-05:04:04

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 207.46.13.162 | United States | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/robots.txt | Block | 1 |
| 79.177.162.94 | Israel | 147.237.76.31 | nakchal.idf.il | Unauthorized URL Access to www.nakhal.idf.il/xmlrpc.php | Block | 1 |
| 185.159.37.7 | | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to 147.237.77.233/ | Block | 1 |
| 66.249.76.106 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter gt; in www.aka.idf.il/iturim/asp/search.asp | None | 1 |
| 217.69.133.244 | Russian Federation | 147.237.77.216 | dover.idf.il | Illegal Byte Code Character in URL /mivtza>специальном сайте</a>, созд анном для этих целей.#012#012#012#012#012<p>#012ссылки  по теме: <hr size=1 noshade>#012<span class= | Block | 1 |
| 108.82.223.123 | United States | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 108.82.223.123 | Block | 1 |
| 189.217.241.19 | Mexico | 147.237.72.166 | aka.idf.il | Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx | Block | 1 |
| 66.249.76.115 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to 147.237.77.216/894-he/dover.aspx | Block | 1 |
| 108.82.223.123 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/spanish | Block | 1 |
| 66.249.64.180 | Israel | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to 147.237.77.233/1387-he/atal.aspx | Block | 1 |
| 204.79.180.157 | United States | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx | Block | 1 |
| 71.6.167.142 | United States | 147.237.77.176 | matpash.idf.il | Unauthorized URL Access to 147.237.77.176/robots.txt | Block | 1 |
| 181.215.123.111 | United States | 147.237.72.167 | ishurim.aka.idf.i | PHP Attempt | Block | 1 |
| 66.249.65.24 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to 147.237.77.216/1133-22525-he/idfgdover.aspx | Block | 1 |
| 204.79.180.209 | United States | 147.237.72.166 | aka.idf.il | Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/kapatz/default.aspx | Block | 1 |
| 79.177.162.94 | Israel | 147.237.76.31 | nakchal.idf.il | PHP Attempt | Block | 1 |
| 185.159.37.7 | | 147.237.77.233 | atal.idf.il | Multiple Unauthorized URL Access from 185.159.37.7 | Block | 1 |
| 66.249.76.77 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp | Block | 1 |

09-19-2016-04:04:04 to 09-19-2016-05:04:04