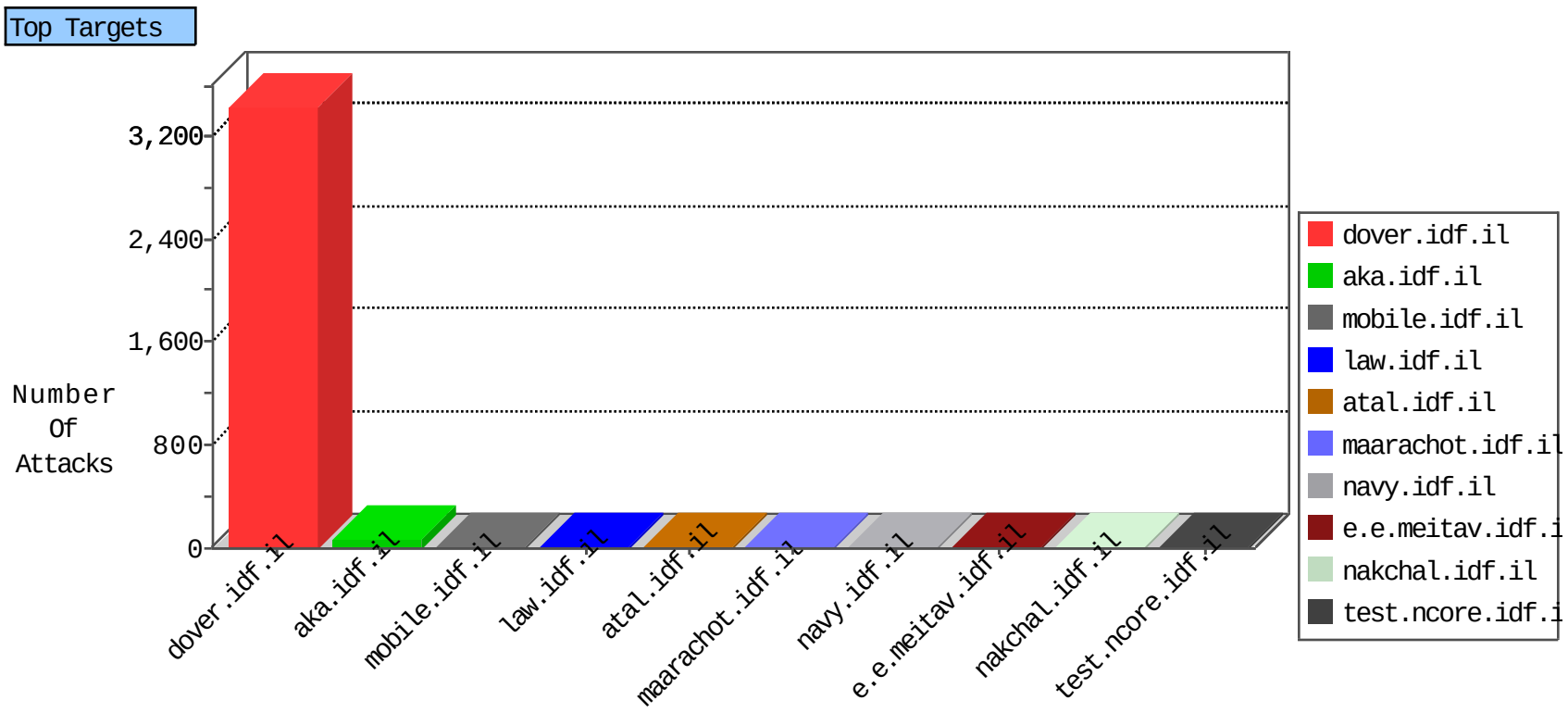
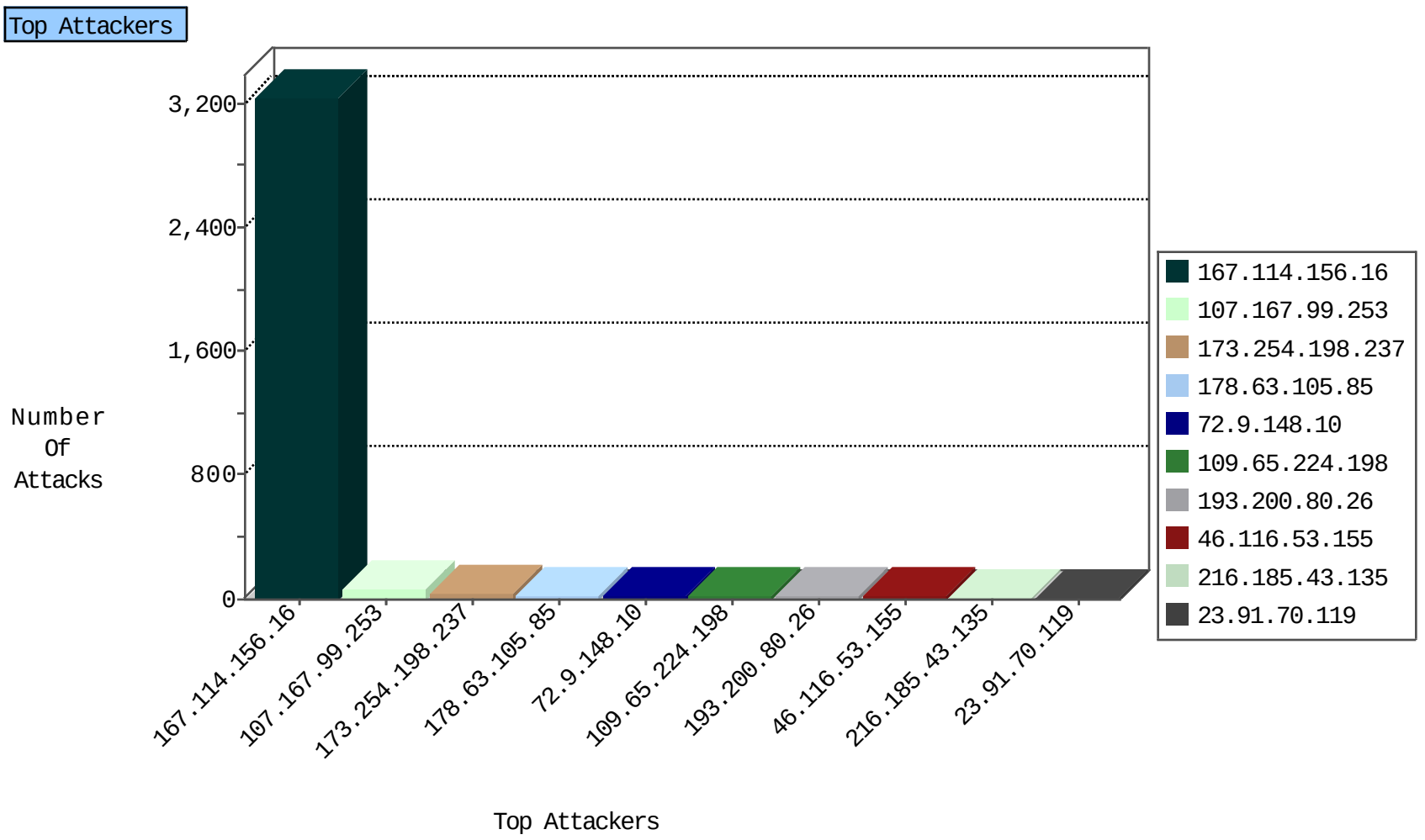
03-13-2016-01:04:27 to 03-13-2016-02:04:27

# IDF Under Attack
# Daily Report

Top Targets




Top Attackers



03-13-2016-01:04:27 to 03-13-2016-02:04:27

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 167.114.156.16 | Canada | 147.237.77.216 | dover.idf.il | DOS-Tool-SwitchbladG | dest-reset | 10129 |
| 81.218.65.210 | Israel | 147.237.77.216 | dover.idf.il | Block_Udp_All_Nets | drop | 6 |

03-13-2016-01:04:27 to 03-13-2016-02:04:27

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 173.254.198.237 | United States | 147.237.77.216 | dover.idf.il | 0854: HTTP: upload* Access | Block | 12 |
| 193.200.80.26 | United Kingdom | 147.237.72.166 | aka.idf.il | 5670: HTTP: SQL Injection (SELECT) | Block | 4 |
| 23.91.70.119 | United States | 147.237.77.74 | law.idf.il | 5670: HTTP: SQL Injection (SELECT) | Block | 4 |
| 216.185.43.135 | United States | 147.237.77.233 | atal.idf.il | 5670: HTTP: SQL Injection (SELECT) | Block | 3 |
| 216.185.43.135 | United States | 147.237.77.233 | atal.idf.il | 3808: HTTP: SQL Injection Variable Declaration Evasion | Block | 1 |
| 106.120.173.102 | China | 147.237.76.42 | refuah.idf.il | C1000071: HTTP: User Agent Sogou+web+spider | Block | 1 |
| 106.120.173.159 | China | 147.237.77.233 | atal.idf.il | C1000071: HTTP: User Agent Sogou+web+spider | Block | 1 |

03-13-2016-01:04:27 to 03-13-2016-02:04:27

## Top Attackers In IDS

| Attacker Address | Target Address | Attacker Country | Site | Signature | Count |
|---|---|---|---|---|---|
| 193.200.80.26 | 147.237.72.166 | United Kingdom | aka.idf.il | SQL Injection - Select From | 12 |
| 23.91.70.119 | 147.237.77.74 | United States | law.idf.il | SQL Injection - Select From | 6 |
| 216.185.43.135 | 147.237.77.233 | United States | atal.idf.il | SQL Injection - Select From | 6 |
| 195.34.150.18 | 147.237.77.216 | Austria | dover.idf.il | Tehila - Perl LWP with fake user agent | 4 |
| 66.249.64.102 | 147.237.77.170 | United States | maarachot.idf.il | ET SCAN NMAP -sA (2) | 2 |
| 198.64.143.244 | 147.237.77.170 | United States | maarachot.idf.il | ET SCAN Potential SSH Scan | 1 |
| 198.64.143.244 | 147.237.72.217 | United States | e.idf.il | ET SCAN Potential SSH Scan | 1 |
| 198.64.143.244 | 147.237.8.14 | United States | e.orchot.idf.il | ET SCAN Potential SSH Scan | 1 |
| 198.64.143.244 | 147.237.0.33 | United States | idf.il | ET SCAN Potential SSH Scan | 1 |
| 198.20.69.74 | 147.237.72.156 | United States | aman.idf.il | ET DROP Dshield Block Listed Source | 1 |
| 218.246.0.97 | 147.237.76.38 | China | e.e.meitav.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 212.83.140.6 | 147.237.77.74 | France | law.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 178.63.11.208 | 147.237.8.45 | Germany | e.eitan.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 199.101.186.238 | 147.237.77.61 | United States | e.cogat.idf.il | ET SCAN NMAP -sS window 3072 | 1 |
| 198.64.143.244 | 147.237.77.212 | United States | e.dover.idf.il | ET SCAN Potential SSH Scan | 1 |
| 198.64.143.244 | 147.237.76.198 | United States | e.yohalan.idf.il | ET SCAN Potential SSH Scan | 1 |
| 198.64.143.244 | 147.237.8.46 | United States | e.chinuch.idf.il | ET SCAN Potential SSH Scan | 1 |
| 198.64.143.244 | 147.237.0.34 | United States | tikshuv.idf.il | ET SCAN Potential SSH Scan | 1 |
| 198.64.143.244 | 147.237.0.17 | United States | m.my-kosher-kravi.idf.il | ET SCAN Potential SSH Scan | 1 |
| 178.63.11.208 | 147.237.76.86 | Germany | navy.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 199.101.186.238 | 147.237.77.61 | United States | e.cogat.idf.il | ET SCAN NMAP -sS window 4096 | 1 |
| 173.65.154.27 | 147.237.77.234 | United States | halag.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 198.64.143.244 | 147.237.77.235 | United States | sviva.idf.il | ET SCAN Potential SSH Scan | 1 |

03-13-2016-01:04:27 to 03-13-2016-02:04:27

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 167.114.156.16 | Canada | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 1109 |
| 107.167.99.253 | United States | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 68 |
| 167.114.156.16 | Canada | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 30 |
| 72.9.148.10 | United States | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 16 |
| 46.116.53.155 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 12 |
| 109.65.224.198 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 9 |
| 212.143.142.56 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 7 |
| 5.22.135.205 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 178.63.105.85 | Germany | 147.237.76.38 | e.e.meitav.idf.il | drop | SAM rule | drop | 6 |
| 178.63.105.85 | Germany | 147.237.76.176 | test.ncore.idf.il | drop | SAM rule | drop | 5 |
| 185.3.144.112 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 109.65.224.198 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 4 |
| 178.63.105.85 | Germany | 147.237.77.179 | e.mazi.idf.il | drop | SAM rule | drop | 4 |
| 72.9.148.10 | United States | 147.237.77.176 | matpash.idf.il | drop | SAM rule | drop | 4 |
| 178.63.105.85 | Germany | 147.237.8.45 | e.eitan.idf.il | drop | SAM rule | drop | 3 |
| 37.26.147.151 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 185.120.126.12 | | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 2.54.181.82 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 31.168.26.28 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 46.19.85.143 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 37.26.148.245 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 109.67.35.197 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 109.65.224.198 | Israel | 147.237.76.31 | nakchal.idf.il | drop | First packet isn't SYN | drop | 3 |
| 176.13.12.172 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 212.179.216.13 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 37.46.38.2 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 3 |
| 5.29.78.38 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 3 |
| 37.204.51.205 | Russian Federation | 147.237.76.86 | navy.idf.il | HTTP Format Sizes | 'Referer' header length exceeded maximum allowed length | monitor | 2 |
| 136.243.152.18 | Germany | 147.237.77.233 | atal.idf.il | drop | SAM rule | drop | 2 |
| 5.102.254.204 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 2 |
| 178.63.105.85 | Germany | 147.237.76.177 | ncore.idf.il | drop | SAM rule | drop | 2 |
| 66.249.69.93 | United States | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 2 |
| 41.141.84.52 | Morocco | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 2 |
| 178.63.105.85 | Germany | 147.237.77.61 | e.cogat.idf.il | drop | SAM rule | drop | 2 |
| 72.9.148.10 | United States | 147.237.77.74 | law.idf.il | drop | SAM rule | drop | 2 |
| 5.9.89.170 | Germany | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 2 |
| 167.114.156.16 | Canada | 147.237.77.216 | dover.idf.il | SYN Attack | | reject | 2 |
| 37.204.51.205 | Russian Federation | 147.237.76.86 | navy.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 2 |
| 31.168.149.92 | Israel | 147.237.0.34 | tikshuv.idf.il | Bad TCP sequence | Invalid sequence number | monitor | 2 |
| 91.200.12.7 | Ukraine | 147.237.77.74 | law.idf.il | drop | SAM rule | drop | 2 |
| 46.120.182.45 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Bad TCP sequence | Invalid ACK number | alert | 2 |
| 91.200.12.7 | Ukraine | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 2 |
| 46.120.182.45 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Bad TCP sequence | Invalid ACK number | monitor | 2 |
| 201.131.148.28 | Panama | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 2 |
| 37.26.147.151 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 1 |
| 84.108.129.0 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 1 |
| 46.19.85.218 | Israel | 147.237.76.31 | nakchal.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 1 |
| 157.55.39.11 | United States | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 1 |
| 195.62.53.168 | Russian Federation | 147.237.0.200 | m4u.idf.il | Geo-location enforcement | Geo-location inbound enforcement | drop | 1 |
| 94.230.93.119 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 1 |

03-13-2016-01:04:27 to 03-13-2016-02:04:27

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 173.254.198.237 | United States | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 173.254.198.237 | Block | 25 |
| 46.116.53.155 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 85.65.133.129 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 201.248.233.47 | Venezuela | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 2 |
| 66.249.64.53 | Israel | 147.237.77.170 | maarachot.idf.il | Unauthorized URL Access to 147.237.77.170/pdf/files/7/108577.pdf | Block | 1 |
| 207.46.13.18 | United States | 147.237.0.15 | kosher-kravi.idf.i | Unauthorized URL Access to kosher-kravi.idf.il/templates/shared/usercontrols/headerupper/ | Block | 1 |
| 66.249.75.44 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/portalmiluim/templates/inner.asp | Block | 1 |
| 31.44.142.96 | Israel | 147.237.72.166 | aka.idf.il | Illegal Byte Code Character in URL /main/kapatz//res#012 ources/images/innerpage/goback.gif | Block | 1 |
| 66.249.64.58 | Israel | 147.237.77.170 | maarachot.idf.il | Unauthorized URL Access to 147.237.77.170/pdf/files/6/107176.pdf | Block | 1 |
| 220.181.132.216 | China | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to 147.237.77.216/894-he/dover.aspx | Block | 1 |
| 66.249.75.61 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter amp;sOrderBy in aka.idf.il/iturim/asp/displayallsoldiers.asp | None | 1 |
| 31.44.142.96 | Israel | 147.237.72.166 | aka.idf.il | Multiple Illegal Byte Code Character in URL from 31.44.142.96 | Block | 1 |
| 173.254.198.237 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/fck/ | Block | 1 |
| 66.249.66.25 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/atal1/izkor/main.asp | Block | 1 |
| 198.20.69.74 | United States | 147.237.72.156 | aman.idf.il | Unauthorized URL Access to 147.237.72.156/modiin/default.aspx | Block | 1 |
| 66.249.66.188 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/robots.txt | Block | 1 |
| 152.200.195.177 | Colombia | 147.237.77.216 | dover.idf.il | SSL Untraceable Connection - Open Mode | None | 1 |
| 66.249.64.48 | Israel | 147.237.77.170 | maarachot.idf.il | Unauthorized URL Access to 147.237.77.170/pdf/files/7/112217.pdf | Block | 1 |
| 66.249.69.2 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/robots.txt | Block | 1 |
| 173.254.198.237 | United States | 147.237.77.216 | dover.idf.il | Multiple Admin Blocking from 173.254.198.237 | Block | 1 |

03-13-2016-01:04:27 to 03-13-2016-02:04:27