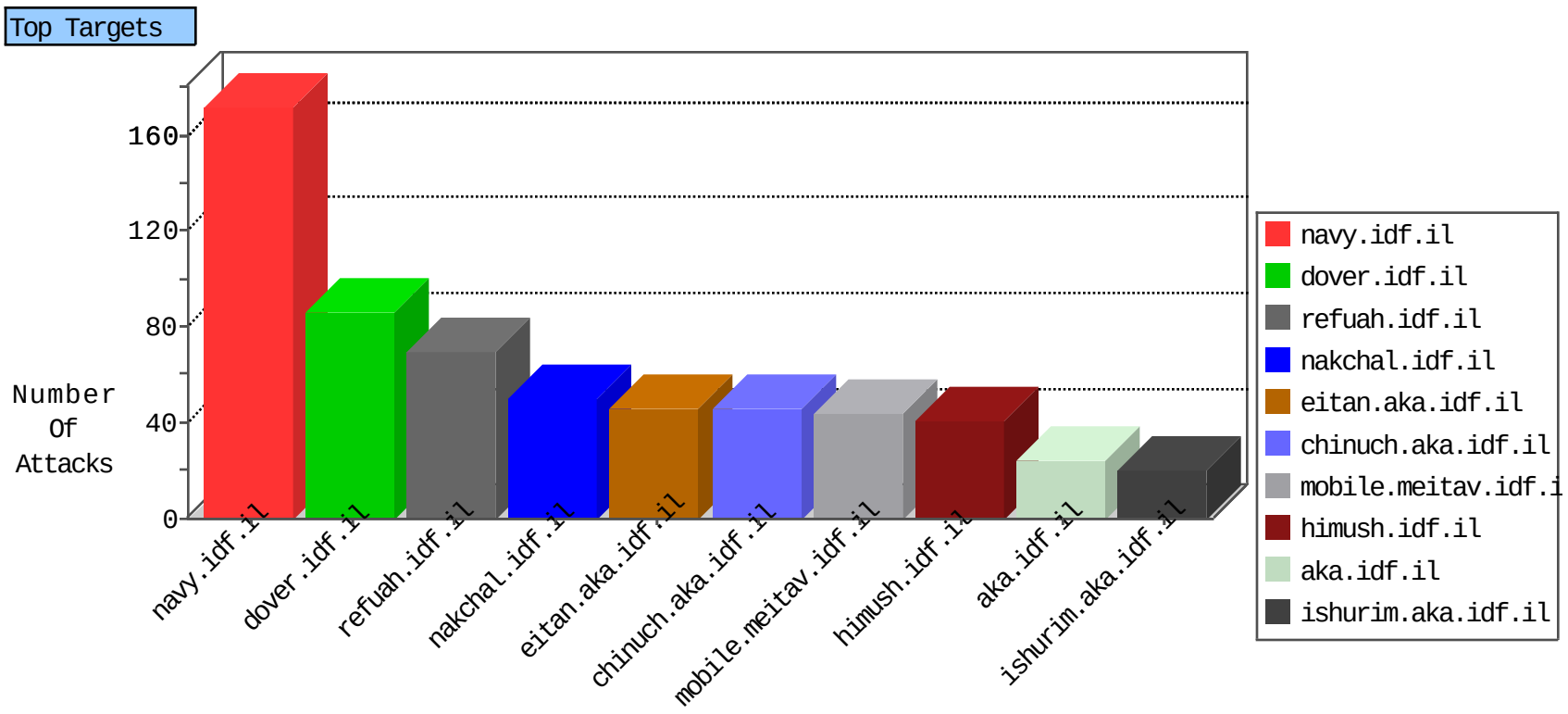
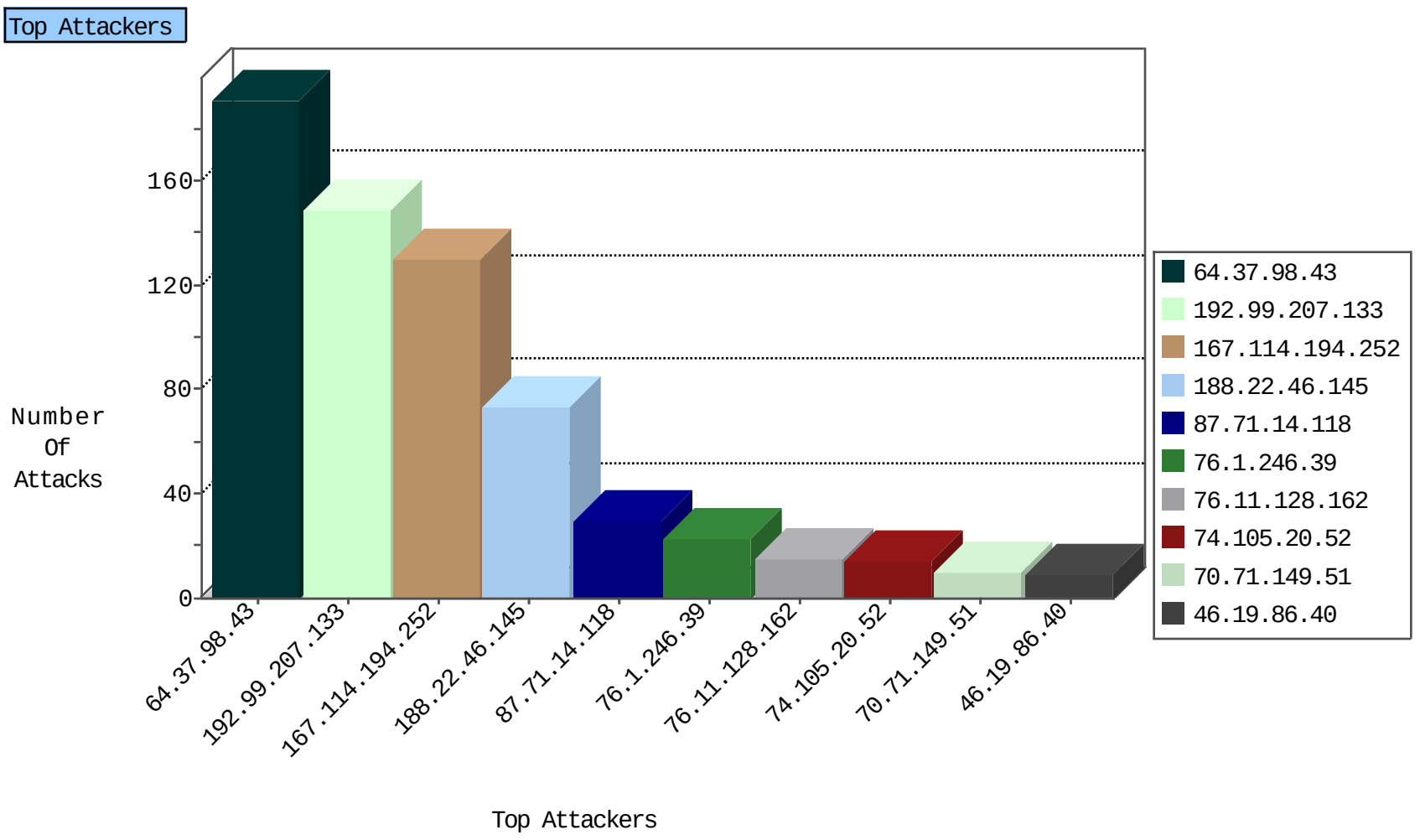
09-06-2016-04:04:07 to 09-06-2016-05:04:07

# IDF Under Attack Daily Report



09-06-2016-04:04:07 to 09-06-2016-05:04:07

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 204.42.253.130 | United States | 147.237.76.34 | yohalan.idf.il | Black List | drop | 2 |
| 80.82.65.168 | Netherlands | 147.237.76.196 | e.sviva.idf.il | Black List | drop | 1 |
| 173.252.115.12 | United States | 147.237.77.216 | dover.idf.il | HTTP-Misc-BadBlue-Dir-Trave-2 | dest-reset | 1 |
| 80.82.65.168 | Netherlands | 147.237.76.176 | test.ncore.idf.il | Black List | drop | 1 |

09-06-2016-04:04:07 to 09-06-2016-05:04:07

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 199.58.86.211 | United States | 147.237.77.216 | dover.idf.il | C1000074: HTTP: majestic bot | Permit | 5 |
| 62.138.2.243 | Germany | 147.237.77.216 | dover.idf.il | C1000074: HTTP: majestic bot | Permit | 2 |
| 91.219.236.136 | Hungary | 147.237.77.216 | dover.idf.il | 24910: HTTP: Python urllib User-Agent Header | Block | 1 |

09-06-2016-04:04:07 to 09-06-2016-05:04:07

Top Attackers In IDS

| Attacker Address | Target Address | Attacker Country | Site | Signature | Count |
|---|---|---|---|---|---|
| 45.79.71.122 | 147.237.72.167 | United States | ishurim.aka.idf.il | WEB-MISC Chunked-Encoding transfer attempt | 2 |
| 45.79.111.169 | 147.237.72.156 | United States | aman.idf.il | WEB-MISC Chunked-Encoding transfer attempt | 1 |
| 200.53.121.94 | 147.237.76.39 | Mexico | mobile.meitav.idf.il | ET SCAN Potential SSH Scan | 1 |
| 5.79.66.235 | 147.237.76.196 | Netherlands | e.sviva.idf.il | ET SCAN NMAP -sS window 4096 | 1 |
| 200.53.121.94 | 147.237.0.200 | Mexico | m4u.idf.il | ET SCAN Potential SSH Scan | 1 |
| 120.236.19.10 | 147.237.76.42 | China | refuah.idf.il | ET SCAN NMAP -sS window 2048 | 1 |
| 120.236.19.2 | 147.237.76.42 | China | refuah.idf.il | ET SCAN NMAP -sS window 2048 | 1 |
| 104.197.206.193 | 147.237.76.199 | United States | e.nakchal.idf.il | ET SCAN NMAP -sS window 3072 | 1 |
| 104.197.206.193 | 147.237.76.199 | United States | e.nakchal.idf.il | ET SCAN NMAP -f -sS | 1 |
| 208.100.26.228 | 147.237.77.176 | United States | matpash.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 91.201.236.50 | 147.237.8.24 | Ukraine | e.lifestyle.idf.il | ET SCAN NMAP -sS window 4096 | 1 |
| 208.67.1.220 | 147.237.8.46 | United States | e.chinuch.idf.il | ET SCAN Potential SSH Scan | 1 |
| 64.137.171.55 | 147.237.76.31 | Canada | nakchal.idf.il | ET SCAN Potential SSH Scan | 1 |
| 200.53.121.94 | 147.237.76.42 | Mexico | refuah.idf.il | ET SCAN Potential SSH Scan | 1 |
| 200.53.121.94 | 147.237.72.167 | Mexico | ishurim.aka.idf.il | ET SCAN Potential SSH Scan | 1 |
| 200.53.121.94 | 147.237.0.35 | Mexico | akaws.idf.il | ET SCAN Potential SSH Scan | 1 |
| 120.236.19.10 | 147.237.76.42 | China | refuah.idf.il | ET SCAN NMAP -f -sS | 1 |
| 120.236.19.2 | 147.237.76.42 | China | refuah.idf.il | ET SCAN NMAP -f -sS | 1 |
| 104.197.206.193 | 147.237.76.199 | United States | e.nakchal.idf.il | ET SCAN NMAP -sS window 2048 | 1 |
| 94.102.48.195 | 147.237.76.31 | Netherlands | nakchal.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 208.67.1.220 | 147.237.72.156 | United States | aman.idf.il | ET SCAN Potential SSH Scan | 1 |
| 91.201.236.50 | 147.237.8.24 | Ukraine | e.lifestyle.idf.il | ET SCAN NMAP -sS window 3072 | 1 |
| 200.53.121.94 | 147.237.76.44 | Mexico | e.refuah.idf.il | ET SCAN Potential SSH Scan | 1 |

09-06-2016-04:04:07 to 09-06-2016-05:04:07

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 188.22.46.145 | Austria | 147.237.76.86 | navy.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 73 |
| 87.71.14.118 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 20 |
| 167.114.194.252 | Canada | 147.237.76.86 | navy.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 19 |
| 167.114.194.252 | Canada | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 18 |
| 167.114.194.252 | Canada | 147.237.76.42 | refuah.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 18 |
| 167.114.194.252 | Canada | 147.237.76.200 | eitan.aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 16 |
| 76.11.128.162 | United States | 147.237.76.86 | navy.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 15 |
| 167.114.194.252 | Canada | 147.237.76.147 | chinuch.aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 15 |
| 167.114.194.252 | Canada | 147.237.76.31 | nakchal.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 15 |
| 167.114.194.252 | Canada | 147.237.76.39 | mobile.meitav.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 15 |
| 167.114.194.252 | Canada | 147.237.76.30 | himush.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 14 |
| 74.105.20.52 | United States | 147.237.76.86 | navy.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 14 |
| 192.99.207.133 | Canada | 147.237.76.147 | chinuch.aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 12 |
| 192.99.207.133 | Canada | 147.237.76.86 | navy.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 12 |
| 192.99.207.133 | Canada | 147.237.76.39 | mobile.meitav.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 12 |
| 192.99.207.133 | Canada | 147.237.76.31 | nakchal.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 11 |
| 192.99.207.133 | Canada | 147.237.76.30 | himush.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 11 |
| 192.99.207.133 | Canada | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 11 |
| 192.99.207.133 | Canada | 147.237.76.42 | refuah.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 10 |
| 64.37.98.43 | United States | 147.237.77.74 | law.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 10 |
| 87.71.14.118 | Israel | 147.237.76.42 | refuah.idf.il | drop | First packet isn't SYN | drop | 10 |
| 64.37.98.43 | United States | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 10 |
| 70.71.149.51 | Canada | 147.237.76.86 | navy.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 10 |
| 192.99.207.133 | Canada | 147.237.76.200 | eitan.aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 10 |
| 64.37.98.43 | United States | 147.237.76.86 | navy.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 10 |
| 64.37.98.43 | United States | 147.237.76.147 | chinuch.aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 10 |
| 64.37.98.43 | United States | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 10 |
| 64.37.98.43 | United States | 147.237.76.200 | eitan.aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 9 |
| 64.37.98.43 | United States | 147.237.72.156 | aman.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 9 |
| 64.37.98.43 | United States | 147.237.77.226 | www.chamatz.aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 9 |
| 64.37.98.43 | United States | 147.237.0.15 | kosher-kravi.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 9 |
| 64.37.98.43 | United States | 147.237.76.42 | refuah.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 9 |
| 64.37.98.43 | United States | 147.237.72.167 | ishurim.aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 9 |
| 64.37.98.43 | United States | 147.237.0.19 | madim.atal.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 9 |
| 64.37.98.43 | United States | 147.237.76.31 | nakchal.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 9 |
| 192.99.207.133 | Canada | 147.237.76.42 | refuah.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | alert | 8 |
| 192.99.207.133 | Canada | 147.237.76.31 | nakchal.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | alert | 8 |
| 192.99.207.133 | Canada | 147.237.76.200 | eitan.aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | alert | 8 |
| 64.37.98.43 | United States | 147.237.77.233 | atal.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 8 |
| 64.37.98.43 | United States | 147.237.0.17 | m.my-kosher-kravi.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 8 |
| 192.99.207.133 | Canada | 147.237.76.86 | navy.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | alert | 8 |
| 64.37.98.43 | United States | 147.237.77.170 | maarachot.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 8 |
| 64.37.98.43 | United States | 147.237.77.234 | halag.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 8 |
| 64.37.98.43 | United States | 147.237.76.30 | himush.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 8 |
| 192.99.207.133 | Canada | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | alert | 8 |
| 64.37.98.43 | United States | 147.237.77.235 | sviva.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 8 |
| 64.37.98.43 | United States | 147.237.0.34 | tikshuv.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 8 |
| 64.37.98.43 | United States | 147.237.76.39 | mobile.meitav.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 7 |
| 192.99.207.133 | Canada | 147.237.76.39 | mobile.meitav.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | alert | 7 |
| 192.99.207.133 | Canada | 147.237.76.147 | chinuch.aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | alert | 7 |

09-06-2016-04:04:07 to 09-06-2016-05:04:07

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 46.19.86.40 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 68.180.230.54 | United States | 147.237.0.34 | tikshuv.idf.il | Parameter Type Violation PageNum in www.tikshuv.idf.il/901-he/tikshuv.aspx | Block | 1 |
| 66.249.69.119 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/robots.txt | Block | 1 |
| 45.79.71.122 | United States | 147.237.72.167 | ishurim.aka.idf.il | Multiple Unknown HTTP Request Method from 45.79.71.122 | Block | 1 |
| 207.46.13.32 | United States | 147.237.72.166 | aka.idf.il | Multiple Unauthorized URL Access from 207.46.13.32 | Block | 1 |
| 66.249.76.116 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to 147.237.77.216/1380-21438-he/dover.aspx | Block | 1 |
| 45.79.71.122 | United States | 147.237.72.167 | ishurim.aka.idf.il | Malformed HTTP Header Line 2 | Block | 1 |
| 104.237.234.109 | United States | 147.237.77.226 | www.chamatz.aka.idf.il | Unauthorized URL Access to 147.237.77.226/ | Block | 1 |
| 66.249.76.75 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on 147.237.72.166/eitan/listpage/ | Block | 1 |
| 45.79.71.122 | United States | 147.237.72.167 | ishurim.aka.idf.il | Unknown HTTP Request Method 1 in URL | Block | 1 |
| 66.249.79.139 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/sip_storage/files/3/2363.jpg | Block | 1 |
| 66.249.64.137 | Israel | 147.237.0.17 | m.my-kosher-kravi.idf.il | Illegal Parameter Encoding rnd in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx | None | 1 |
| 45.79.71.122 | United States | 147.237.72.167 | ishurim.aka.idf.il | Malformed URL | Block | 1 |
| 104.237.234.109 | United States | 147.237.77.234 | halag.idf.il | Unauthorized URL Access to 147.237.77.234/ | Block | 1 |
| 66.249.76.77 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/yohalan/main/main.asp | Block | 1 |
| 45.79.111.169 | United States | 147.237.72.156 | aman.idf.il | Malformed HTTP Header Line 3 | Block | 1 |
| 66.249.79.143 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/sip_storage/files/1/2331.jpg | Block | 1 |
| 66.249.66.133 | Israel | 147.237.76.200 | eitan.aka.idf.il | Unauthorized URL Access to www.eitan.aka.idf.il/shared/usercontrols/headerupper/ | Block | 1 |
| 45.79.71.122 | United States | 147.237.72.167 | ishurim.aka.idf.il | Multiple Malformed HTTP Header Line from 45.79.71.122 | Block | 1 |
| 108.92.157.123 | United States | 147.237.72.166 | aka.idf.il | Illegal Byte Code Character in URL /main/kapatz//res#012 ources/images/innerpage/goback.gif | Block | 1 |
| 66.249.76.100 | Israel | 147.237.72.156 | aman.idf.il | Unauthorized URL Access to list.ips.gov.il/robots.txt | Block | 1 |
| 45.79.111.169 | United States | 147.237.72.156 | aman.idf.il | Malformed URL | Block | 1 |
| 68.180.228.167 | United States | 147.237.77.226 | www.chamatz.aka.idf.il | Unauthorized URL Access to www.chamatz.aka.idf.il/templates/shared/usercontrols/headerupper/ | Block | 1 |
| 66.249.69.83 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/eitan/pratim/pirteychayal/ | Block | 1 |
| 45.79.71.122 | United States | 147.237.72.167 | ishurim.aka.idf.il | Multiple Malformed URL from 45.79.71.122 | Block | 1 |
| 204.79.180.232 | United States | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for 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 147.237.77.216/1133-19883-he/idfgdover.aspx | Block | 1 |
| 45.79.111.169 | United States | 147.237.72.156 | aman.idf.il | Unknown HTTP Request Method 1 in URL | Block | 1 |

09-06-2016-04:04:07 to 09-06-2016-05:04:07