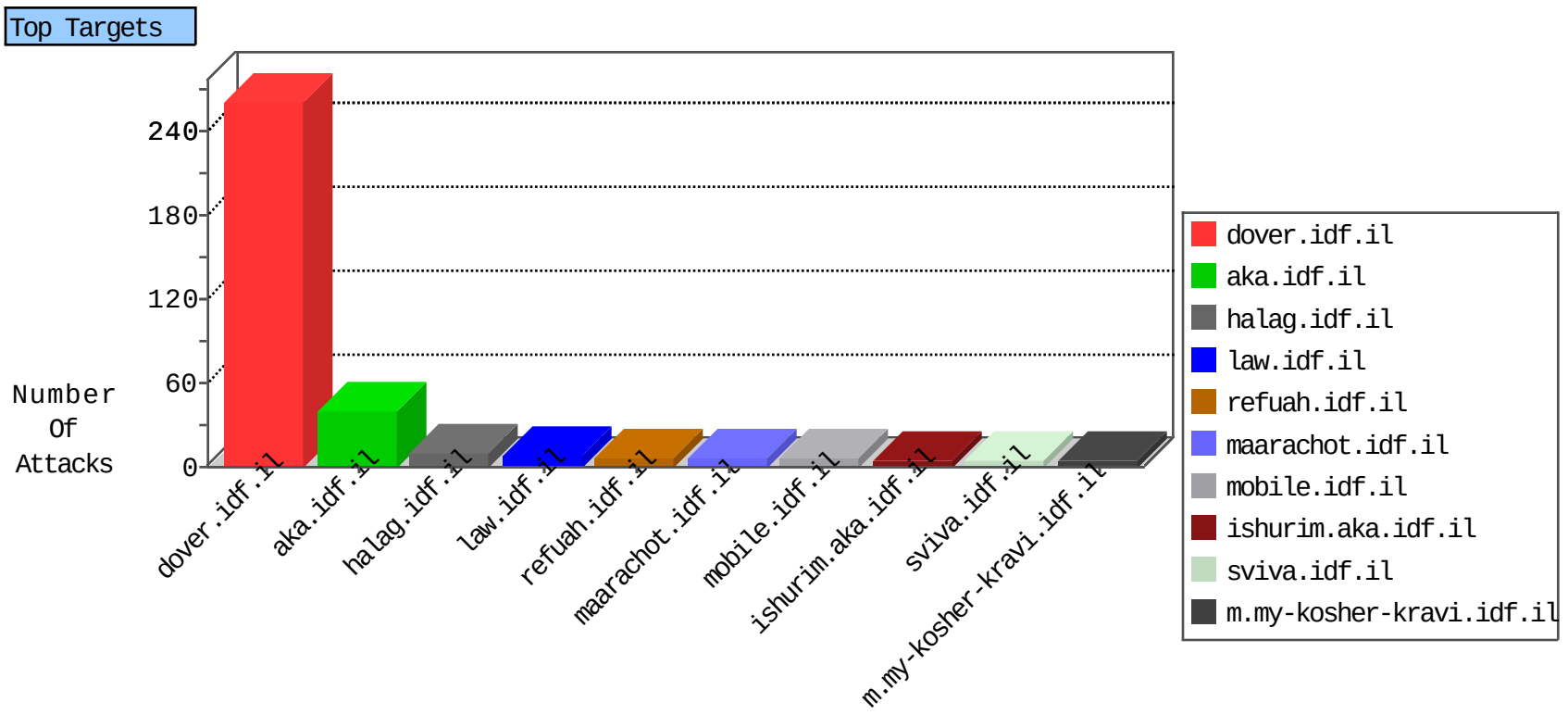
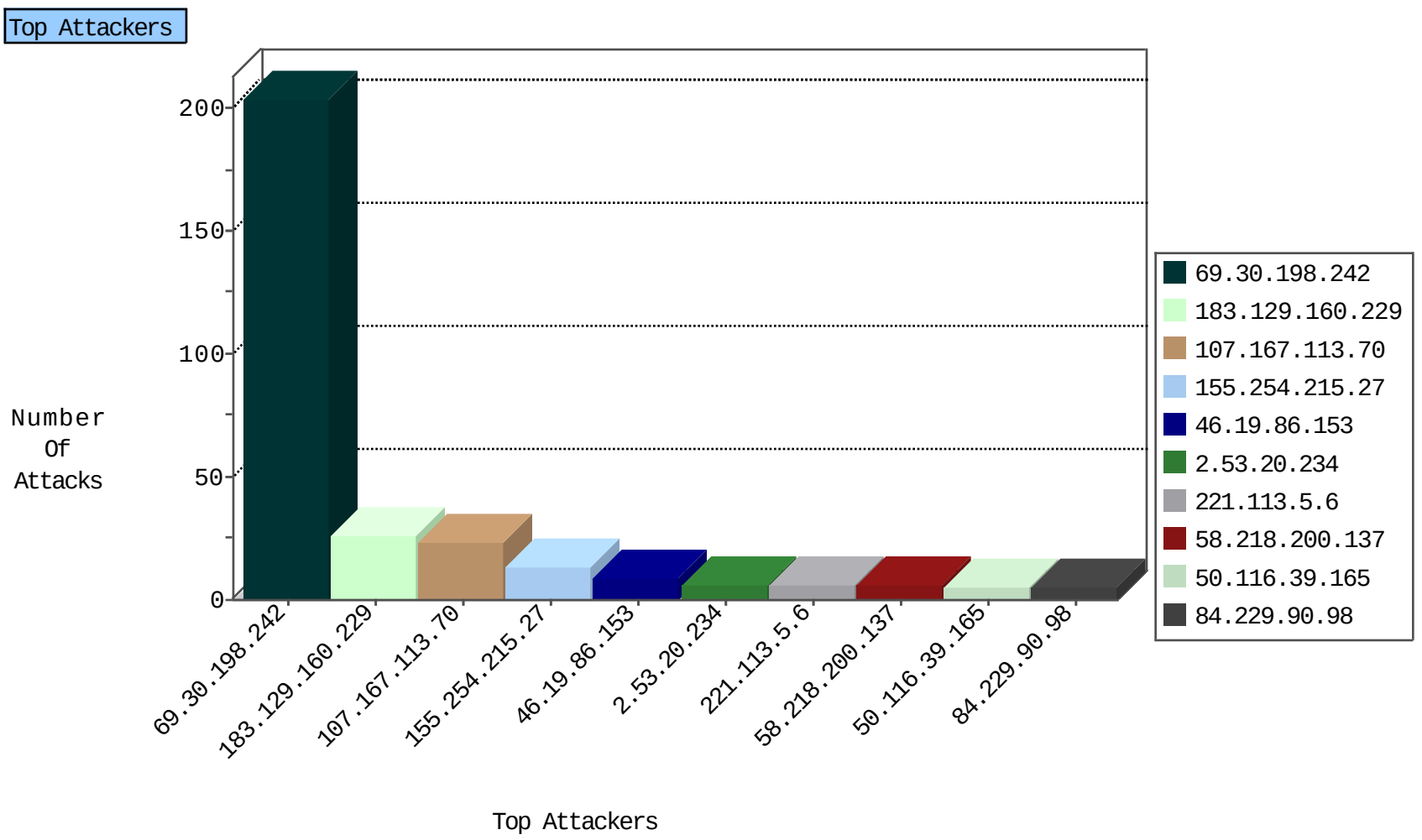
10-05-2016-02:04:09 to 10-05-2016-03:04:09

# IDF Under Attack Daily Report



10-05-2016-02:04:09 to 10-05-2016-03:04:09

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 77.127.16.111 | Israel | 147.237.76.86 | navy.idf.il | Black List | drop | 1 |
| 115.239.251.250 | China | 147.237.72.14 | dover.idf.il(old) | JLM_Purple_Con_Limit_Tcp | drop | 1 |
| 71.6.216.54 | United States | 147.237.76.147 | chinuch.aka.idf.il | Black List | drop | 1 |
| 71.6.216.56 | United States | 147.237.76.177 | ncore.idf.il | Black List | drop | 1 |

10-05-2016-02:04:09 to 10-05-2016-03:04:09

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 69.30.198.242 | United States | 147.237.77.216 | dover.idf.il | C1000074: HTTP: majestic bot | Permit | 182 |
| 69.30.198.242 | United States | 147.237.72.166 | aka.idf.il | C1000074: HTTP: majestic bot | Permit | 4 |
| 69.30.198.242 | United States | 147.237.77.74 | law.idf.il | C1000074: HTTP: majestic bot | Permit | 4 |
| 62.210.247.125 | France | 147.237.72.166 | aka.idf.il | C1000074: HTTP: majestic bot | Permit | 2 |
| 74.111.27.177 | United States | 147.237.77.216 | dover.idf.il | C1000074: HTTP: majestic bot | Permit | 2 |
| 69.30.198.242 | United States | 147.237.0.34 | tikshuv.idf.il | C1000074: HTTP: majestic bot | Permit | 2 |
| 51.254.32.82 | France | 147.237.77.216 | dover.idf.il | C1000074: HTTP: majestic bot | Permit | 2 |
| 51.254.32.82 | France | 147.237.77.176 | matpash.idf.il | C1000074: HTTP: majestic bot | Permit | 1 |

10-05-2016-02:04:09 to 10-05-2016-03:04:09

Top Attackers In IDS

| Attacker Address | Target Address | Attacker Country | Site | Signature | Count |
|---|---|---|---|---|---|
| 91.121.221.160 | 147.237.77.216 | France | dover.idf.il | ET WEB_SERVER Fake Googlebot UA 1 Inbound | 2 |
| 62.210.243.100 | 147.237.76.148 | France | gqcenter.aka.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 200.48.200.59 | 147.237.76.30 | Peru | himush.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 58.218.200.137 | 147.237.76.177 | China | ncore.idf.il | ET SCAN Potential SSH Scan | 1 |
| 180.150.177.188 | 147.237.8.14 | China | e.orchot.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 58.218.200.137 | 147.237.76.31 | China | nakchal.idf.il | ET SCAN Potential SSH Scan | 1 |
| 163.172.169.150 | 147.237.76.201 | United Kingdom | e.atal.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 58.218.200.137 | 147.237.0.17 | China | m.my-kosher-kravi.idf.il | ET SCAN Potential SSH Scan | 1 |
| 109.86.228.105 | 147.237.76.198 | Ukraine | e.yohalan.idf.il | ET SCAN Potential SSH Scan | 1 |
| 50.116.123.33 | 147.237.76.202 | United States | e.halag.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 109.86.228.105 | 147.237.0.34 | Ukraine | tikshuv.idf.il | ET SCAN Potential SSH Scan | 1 |
| 14.152.59.11 | 147.237.76.148 | China | gqcenter.aka.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 109.48.117.38 | 147.237.72.166 | Portugal | aka.idf.il | ET SCAN Potential SSH Scan | 1 |
| 12.139.34.20 | 147.237.72.217 | United States | e.idf.il | ET SCAN NMAP -sS window 3072 | 1 |
| 12.139.34.20 | 147.237.72.217 | United States | e.idf.il | ET SCAN NMAP -f -sS | 1 |
| 222.77.254.105 | 147.237.0.35 | China | akaws.idf.il | ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection | 1 |
| 62.210.243.100 | 147.237.76.196 | France | e.sviva.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 200.48.200.59 | 147.237.76.30 | Peru | himush.idf.il | ET SCAN NMAP -sS window 3072 | 1 |
| 58.218.200.137 | 147.237.76.196 | China | e.sviva.idf.il | ET SCAN Potential SSH Scan | 1 |
| 191.12.213.135 | 147.237.76.147 | Brazil | chinuch.aka.idf.il | ET SCAN Potential SSH Scan | 1 |
| 58.218.200.137 | 147.237.76.148 | China | gqcenter.aka.idf.il | ET SCAN Potential SSH Scan | 1 |
| 180.109.151.103 | 147.237.77.170 | China | maarachot.idf.il | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |
| 58.218.200.137 | 147.237.0.33 | China | idf.il | ET SCAN Potential SSH Scan | 1 |
| 109.236.86.32 | 147.237.0.17 | Netherlands | m.my-kosher-kravi.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 54.147.8.50 | 147.237.77.216 | United States | dover.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 109.86.228.105 | 147.237.76.42 | Ukraine | refuah.idf.il | ET SCAN Potential SSH Scan | 1 |
| 50.116.123.33 | 147.237.76.197 | United States | e.himush.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 109.86.228.105 | 147.237.0.19 | Ukraine | madim.atal.idf.il | ET SCAN Potential SSH Scan | 1 |
| 14.152.59.11 | 147.237.0.16 | China | my-kosher-kravi.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 93.193.5.16 | 147.237.76.86 | Germany | navy.idf.il | ET SCAN Potential SSH Scan | 1 |
| 12.139.34.20 | 147.237.72.217 | United States | e.idf.il | ET SCAN NMAP -sS window 2048 | 1 |
| 66.249.76.118 | 147.237.72.166 | United States | aka.idf.il | SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt | 1 |
| 208.100.26.228 | 147.237.76.176 | United States | test.ncore.idf.il | ET SCAN NMAP -sS window 1024 | 1 |

10-05-2016-02:04:09 to 10-05-2016-03:04:09

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 107.167.113.70 | United States | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 23 |
| 155.254.215.27 | Bahrain | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 13 |
| 69.30.198.242 | United States | 147.237.77.216 | dover.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 7 |
| 2.53.20.234 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 6 |
| 221.113.5.6 | Japan | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 6 |
| 84.229.90.98 | Israel | 147.237.76.42 | refuah.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 5 |
| 5.29.6.156 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 4 |
| 46.19.86.153 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 4 |
| 46.19.86.153 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 74.73.20.33 | United States | 147.237.72.167 | ishurim.aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 3 |
| 46.19.86.46 | Israel | 147.237.77.226 | www.chamatz.aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 3 |
| 46.19.85.115 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 212.143.142.56 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 3 |
| 46.19.85.241 | Israel | 147.237.76.31 | nakchal.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 2 |
| 50.116.39.165 | United States | 147.237.0.17 | m.my-kosher-kravi.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 2 |
| 131.253.27.25 | United States | 147.237.76.200 | eitan.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 2 |
| 77.138.46.133 | France | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 2 |
| 50.116.39.165 | United States | 147.237.76.39 | mobile.meitav.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 2 |
| 69.30.198.242 | United States | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 2 |
| 2.53.52.154 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 2 |
| 137.226.113.7 | Germany | 147.237.77.234 | halag.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 1 |
| 85.65.228.111 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | alert | 1 |
| 183.129.160.229 | China | 147.237.77.170 | maarachot.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 1 |
| 69.30.198.242 | United States | 147.237.72.166 | aka.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 1 |
| 180.97.106.162 | China | 147.237.0.15 | kosher-kravi.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 1 |
| 2.53.138.171 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 1 |
| 109.66.164.186 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 1 |
| 183.129.160.229 | China | 147.237.77.235 | sviva.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 1 |
| 183.129.160.229 | China | 147.237.76.176 | test.ncore.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 1 |
| 180.97.106.37 | China | 147.237.77.234 | halag.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 1 |
| 5.29.74.163 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 1 |
| 141.212.122.38 | United States | 147.237.76.197 | e.himush.idf.il | Geo-location enforcement | Geo-location inbound enforcement | drop | 1 |
| 85.65.228.111 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 1 |
| 183.129.160.229 | China | 147.237.77.212 | e.dover.idf.il | Geo-location enforcement | Geo-location inbound enforcement | drop | 1 |
| 69.30.198.242 | United States | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 1 |
| 180.97.106.162 | China | 147.237.8.24 | e.lifestyle.idf.il | Geo-location enforcement | Geo-location inbound enforcement | drop | 1 |
| 180.97.106.37 | China | 147.237.8.28 | e.mobile-ks.idf.il | Geo-location enforcement | Geo-location inbound enforcement | drop | 1 |
| 2.53.144.37 | Israel | 147.237.72.156 | aman.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 1 |
| 185.32.179.121 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 1 |
| 183.129.160.229 | China | 147.237.76.177 | ncore.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 1 |
| 180.97.106.161 | China | 147.237.8.50 | e.tikshuv.idf.il | Geo-location enforcement | Geo-location inbound enforcement | drop | 1 |
| 141.212.122.39 | United States | 147.237.76.197 | e.himush.idf.il | Geo-location enforcement | Geo-location inbound enforcement | drop | 1 |
| 85.210.138.250 | United Kingdom | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 1 |
| 183.129.160.229 | China | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 1 |
| 180.97.106.162 | China | 147.237.76.34 | yohalan.idf.il | drop | | drop | 1 |
| 180.97.106.37 | China | 147.237.76.30 | himush.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 1 |
| 2.53.184.168 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | alert | 1 |
| 137.116.71.170 | United States | 147.237.8.27 | e.madim.atal.idf.il | Geo-location enforcement | Geo-location inbound enforcement | drop | 1 |
| 79.180.203.40 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 1 |
| 183.129.160.229 | China | 147.237.77.74 | law.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 1 |

10-05-2016-02:04:09 to 10-05-2016-03:04:09

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 86.247.50.205 | France | 147.237.72.166 | aka.idf.il | Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx | Block | 2 |
| 46.19.86.77 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to www.refua.atal.idf.il/1325-he/refuah.aspx) | Block | 1 |
| 183.129.160.229 | China | 147.237.77.234 | halag.idf.il | Distributed Malformed URL | Block | 1 |
| 183.129.160.229 | China | 147.237.77.74 | law.idf.il | Distributed Malformed URL | Block | 1 |
| 66.249.76.77 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/edim/yoman/yoman.asp | Block | 1 |
| 183.129.160.229 | China | 147.237.77.235 | sviva.idf.il | Multiple Unknown HTTP Request Method from 183.129.160.229 | Block | 1 |
| 183.129.160.229 | China | 147.237.77.170 | maarachot.idf.il | Multiple Unknown HTTP Request Method from 183.129.160.229 | Block | 1 |
| 84.94.67.133 | Israel | 147.237.72.166 | aka.idf.il | SSL Untraceable Connection - Open Mode | None | 1 |
| 66.102.9.8 | United States | 147.237.72.166 | aka.idf.il | Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx | Block | 1 |
| 183.129.160.229 | China | 147.237.77.234 | halag.idf.il | Distributed Unknown HTTP Request Method | Block | 1 |
| 183.129.160.229 | China | 147.237.77.74 | law.idf.il | Distributed Unknown HTTP Request Method | Block | 1 |
| 66.249.93.69 | Israel | 147.237.77.234 | halag.idf.il | Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif | Block | 1 |
| 183.129.160.229 | China | 147.237.77.216 | dover.idf.il | Malformed HTTP Header Line 1 | Block | 1 |
| 66.249.64.124 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/sip_storage/files/2/שקופית10 | Block | 1 |
| 183.129.160.229 | China | 147.237.77.234 | halag.idf.il | Multiple Malformed HTTP Header Line from 183.129.160.229 | Block | 1 |
| 183.129.160.229 | China | 147.237.77.74 | law.idf.il | Malformed HTTP Header Line 1 | Block | 1 |
| 69.114.98.99 | United States | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for www.aka.idf.il/main/sachar | Block | 1 |
| 2.53.9.234 | Israel | 147.237.77.234 | halag.idf.il | Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif | Block | 1 |
| 183.129.160.229 | China | 147.237.77.216 | dover.idf.il | Malformed URL | Block | 1 |
| 106.38.241.106 | China | 147.237.76.86 | navy.idf.il | SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO) | None | 1 |
| 66.249.66.23 | Israel | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to 147.237.77.233/994-8517-he/atal.aspx | Block | 1 |
| 183.129.160.229 | China | 147.237.77.235 | sviva.idf.il | Multiple Malformed HTTP Header Line from 183.129.160.229 | Block | 1 |
| 183.129.160.229 | China | 147.237.77.170 | maarachot.idf.il | Multiple Malformed HTTP Header Line from 183.129.160.229 | Block | 1 |
| 77.139.207.13 | France | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for www.aka.idf.il/main/rabanut/faq.aspx | Block | 1 |
| 46.4.74.42 | Germany | 147.237.72.166 | aka.idf.il | Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp | Block | 1 |
| 183.129.160.229 | China | 147.237.77.216 | dover.idf.il | Unknown HTTP Request Method test in URL | Block | 1 |
| 176.195.108.25 | Russian Federation | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for www.aka.idf.il/main/giyus/pniotanswer.aspx | Block | 1 |
| 66.249.75.149 | Israel | 147.237.76.86 | navy.idf.il | Unauthorized URL Access to www.navy.idf.il/templates/shared/usercontrols/headerupper/ | Block | 1 |
| 183.129.160.229 | China | 147.237.77.235 | sviva.idf.il | Multiple Malformed URL from 183.129.160.229 | Block | 1 |
| 183.129.160.229 | China | 147.237.77.170 | maarachot.idf.il | Multiple Malformed URL from 183.129.160.229 | Block | 1 |
| 80.1.254.176 | United Kingdom | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx | Block | 1 |

10-05-2016-02:04:09 to 10-05-2016-03:04:09