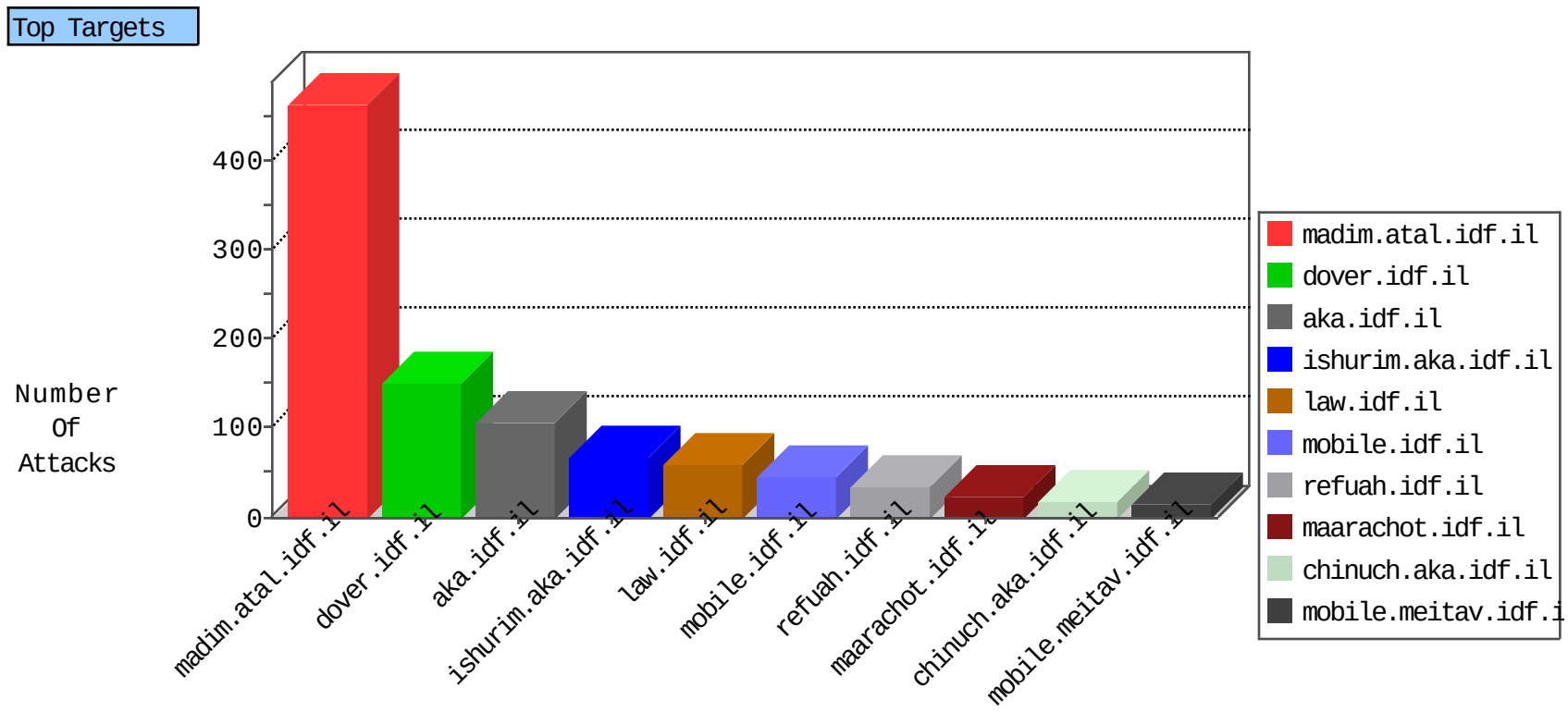
09-25-2016-14:04:03 to 09-25-2016-15:04:03

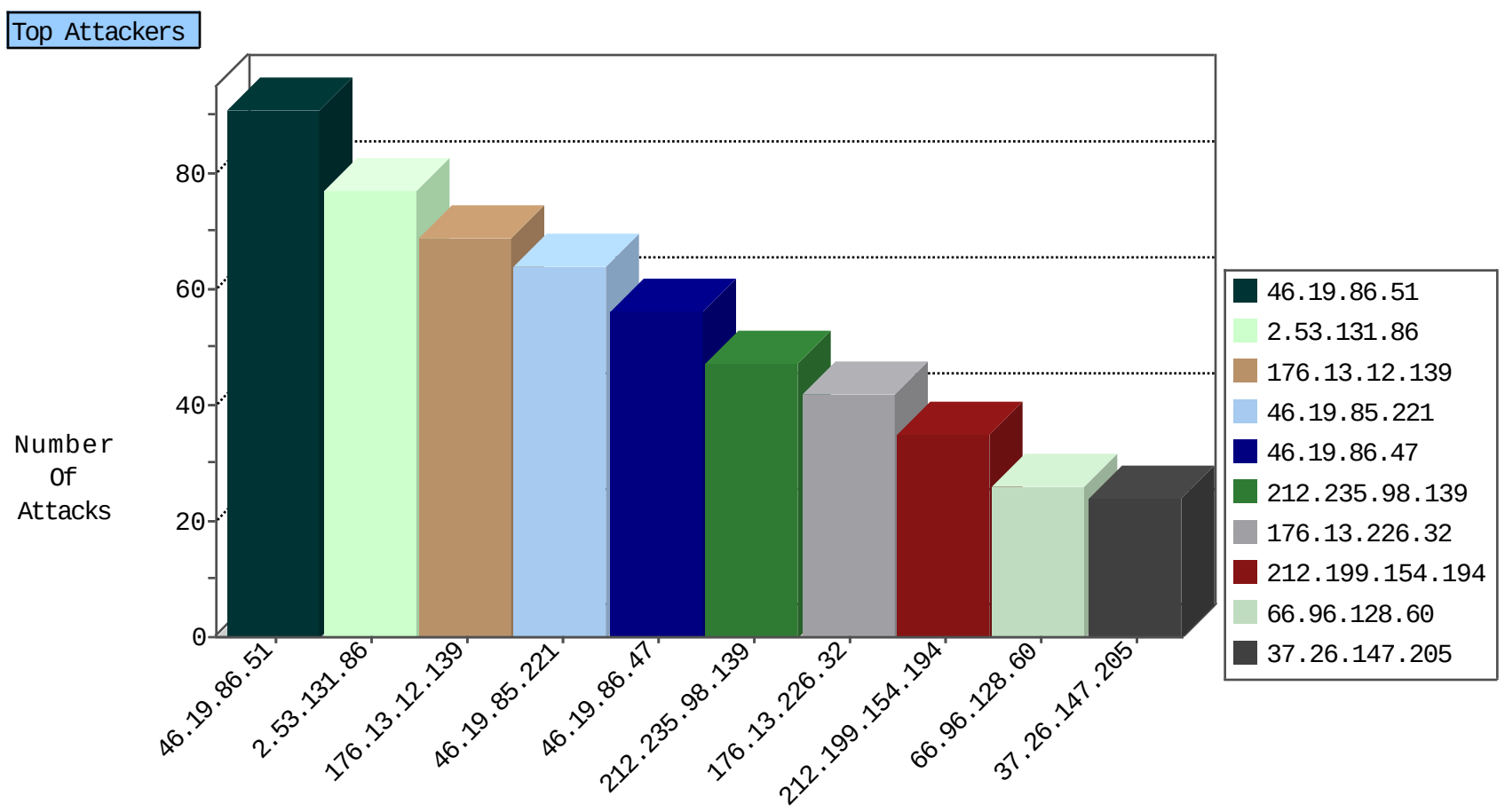
# IDF Under Attack Daily Report

Top Targets




Top Target

Top Attackers




Top Attackers

09-25-2016-14:04:03 to 09-25-2016-15:04:03

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 212.199.154.194 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Anomaly-TLS-renegotiation-Cli | dest-reset | 237 |
| 78.129.171.175 | United Kingdom | 147.237.76.34 | yohalan.idf.il | Black List | drop | 1 |
| 78.129.171.175 | United Kingdom | 147.237.76.39 | mobile.meitav.idf.il | Black List | drop | 1 |
| 78.129.171.175 | United Kingdom | 147.237.76.176 | test.ncore.idf.il | Black List | drop | 1 |
| 82.145.56.173 | United Kingdom | 147.237.76.200 | eitan.aka.idf.il | Black List | drop | 1 |

09-25-2016-14:04:03 to 09-25-2016-15:04:03

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 50.63.197.11 | United States | 147.237.77.74 | law.idf.il | 5670: HTTP: SQL Injection (SELECT) | Block | 6 |
| 66.96.128.60 | United States | 147.237.72.166 | aka.idf.il | 5670: HTTP: SQL Injection (SELECT) | Block | 6 |
| 163.172.49.61 | United Kingdom | 147.237.77.216 | dover.idf.il | C1000074: HTTP: majestic bot | Permit | 3 |
| 151.80.31.169 | France | 147.237.77.74 | law.idf.il | C1000146: HTTP:  AhrefBot crawler | Block | 1 |

09-25-2016-14:04:03 to 09-25-2016-15:04:03

Top Attackers In IDS

| Attacker Address | Target Address | Attacker Country | Site | Signature | Count |
|---|---|---|---|---|---|
| 66.96.128.60 | 147.237.72.166 | United States | aka.idf.il | SQL Injection - Select From | 17 |
| 50.63.197.11 | 147.237.77.74 | United States | law.idf.il | SQL Injection - Select From | 10 |
| 109.226.40.40 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 77.125.53.19 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 109.60.153.178 | 147.237.76.44 | Russian Federation | e.refuah.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 93.174.93.17 | 147.237.77.205 | Netherlands | prisha.idf.il | ET SCAN Potential SSH Scan | 1 |
| 46.19.85.30 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 93.174.93.17 | 147.237.76.42 | Netherlands | refuah.idf.il | ET SCAN Potential SSH Scan | 1 |
| 2.55.131.215 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 91.201.236.158 | 147.237.77.212 | Ukraine | e.dover.idf.il | ET DROP Spamhaus DROP Listed Traffic Inbound | 1 |
| 217.246.252.53 | 147.237.77.216 | Germany | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 84.94.75.134 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 209.20.68.190 | 147.237.77.216 | United States | dover.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 82.81.74.252 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 145.53.121.127 | 147.237.77.216 | Netherlands | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 79.180.220.248 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 141.226.161.232 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 77.126.95.152 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 109.65.186.171 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 66.249.66.242 | 147.237.77.74 | United States | law.idf.il | ET SCAN NMAP -sA (2) | 1 |
| 93.174.93.17 | 147.237.77.233 | Netherlands | atal.idf.il | ET SCAN Potential SSH Scan | 1 |
| 93.174.93.17 | 147.237.77.19 | Netherlands | law-forum.idf.il | ET SCAN Potential SSH Scan | 1 |
| 31.154.53.142 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 91.201.236.158 | 147.237.77.212 | Ukraine | e.dover.idf.il | ET SCAN NMAP -sS window 4096 | 1 |
| 2.53.22.66 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 85.64.218.198 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 212.179.41.221 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 84.94.1.47 | 147.237.72.166 | Israel | aka.idf.il | portscan: TCP Distributed Portscan | 1 |
| 192.116.105.60 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 79.181.230.103 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 141.226.162.58 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 77.127.14.74 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |

09-25-2016-14:04:03 to 09-25-2016-15:04:03

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | **Signature** | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 212.235.98.139 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 47 |
| 77.126.13.183 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 20 |
| 91.228.248.251 | Israel | 147.237.72.167 | ishurim.aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 16 |
| 212.199.154.194 | Israel | 147.237.72.167 | ishurim.aka.idf.il | drop | First packet isn't SYN | drop | 15 |
| 185.89.217.235 | Netherlands | 147.237.77.74 | law.idf.il | drop | First packet isn't SYN | drop | 8 |
| 82.166.2.56 | Israel | 147.237.77.170 | maarachot.idf.il | drop | First packet isn't SYN | drop | 8 |
| 46.19.85.30 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 6 |
| 37.26.146.240 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 185.89.217.226 | Netherlands | 147.237.77.74 | law.idf.il | drop | First packet isn't SYN | drop | 6 |
| 46.19.85.30 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 62.219.225.2 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid sequence number | monitor | 6 |
| 46.19.86.23 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 6 |
| 185.89.217.234 | Netherlands | 147.237.77.74 | law.idf.il | drop | First packet isn't SYN | drop | 6 |
| 109.253.216.177 | Israel | 147.237.0.15 | kosher-kravi.idf.i | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 6 |
| 89.139.107.4 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 5 |
| 46.19.85.23 | Israel | 147.237.76.86 | navy.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 5 |
| 82.166.2.56 | Israel | 147.237.77.170 | maarachot.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 5 |
| 46.19.85.112 | Israel | 147.237.76.31 | nakchal.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 5 |
| 88.202.218.240 | United Kingdom | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 4 |
| 2.55.151.35 | Israel | 147.237.72.167 | ishurim.aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 4 |
| 46.19.85.206 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 4 |
| 185.137.19.76 | | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 4 |
| 82.166.2.56 | Israel | 147.237.77.170 | maarachot.idf.il | Bad TCP sequence | Invalid ACK number | alert | 4 |
| 46.19.85.206 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 81.50.90.124 | France | 147.237.76.147 | chinuch.aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 4 |
| 66.96.128.60 | United States | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 3 |
| 77.138.52.97 | France | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 3 |
| 46.19.85.147 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 3 |
| 109.65.23.45 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 81.50.90.124 | France | 147.237.76.147 | chinuch.aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | alert | 3 |
| 176.106.44.120 | Palestinian Territory Occupied | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 3 |
| 46.19.86.226 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 3 |
| 185.89.217.232 | Netherlands | 147.237.77.74 | law.idf.il | drop | First packet isn't SYN | drop | 3 |
| 2.55.44.223 | Israel | 147.237.76.42 | refuah.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 3 |
| 46.19.85.112 | Israel | 147.237.76.31 | nakchal.idf.il | Bad TCP sequence | Invalid ACK number | alert | 3 |
| 185.89.217.228 | Netherlands | 147.237.77.74 | law.idf.il | drop | First packet isn't SYN | drop | 3 |
| 176.13.4.119 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 3 |
| 185.89.217.233 | Netherlands | 147.237.77.74 | law.idf.il | drop | First packet isn't SYN | drop | 3 |
| 2.55.161.18 | Israel | 147.237.72.156 | aman.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 3 |
| 2.55.146.240 | Israel | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 3 |
| 46.19.85.147 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 3 |
| 79.183.96.191 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 185.89.217.230 | Netherlands | 147.237.77.74 | law.idf.il | drop | First packet isn't SYN | drop | 2 |
| 5.22.134.93 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 2 |
| 176.13.10.99 | Israel | 147.237.76.42 | refuah.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 2 |
| 62.219.160.128 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 2 |
| 84.94.178.14 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 2 |
| 109.253.216.177 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | alert | 2 |
| 2.53.161.13 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 2 |
| 212.143.142.56 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 2 |

09-25-2016-14:04:03 to 09-25-2016-15:04:03

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 46.19.86.51 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 91 |
| 2.53.131.86 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 77 |
| 176.13.12.139 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 66 |
| 46.19.85.221 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 64 |
| 46.19.86.47 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 56 |
| 176.13.226.32 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 42 |
| 37.26.147.205 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 24 |
| 2.55.146.145 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 18 |
| 2.55.11.131 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 12 |
| 77.126.13.183 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 4 |
| 109.253.141.189 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 80.246.140.150 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 2.53.149.208 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 31.154.19.5 | Israel | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 31.154.19.5 | Block | 3 |
| 37.26.148.234 | Israel | 147.237.77.170 | maarachot.idf.il | Unauthorized URL Access to maarachot.idf.il/pdf/files/7/112277.pdf,23-2 | Block | 2 |
| 32.213.242.86 | United States | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for www.aka.idf.il/main/giyus/miyun/miyunlobby.aspx | Block | 2 |
| 66.249.66.113 | Israel | 147.237.0.17 | m.my-kosher-kravi.idf.il | Distributed Illegal Parameter Encoding | None | 2 |
| 46.19.86.14 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 160.83.42.137 | United Kingdom | 147.237.77.74 | law.idf.il | Unauthorized HTTP Method | Block | 2 |
| 79.178.107.242 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/kamlar/images/ | Block | 2 |
| 169.229.3.91 | United States | 147.237.77.235 | sviva.idf.il | Multiple Illegal Byte Code Character in Method from 169.229.3.91 | Block | 1 |
| 66.249.66.115 | Israel | 147.237.0.17 | m.my-kosher-kravi.idf.il | Distributed Illegal Parameter Encoding | None | 1 |
| 66.176.73.239 | United States | 147.237.76.42 | refuah.idf.il | Distributed Illegal Byte Code Character in Method | Block | 1 |
| 160.83.42.137 | United Kingdom | 147.237.77.74 | law.idf.il | Unauthorized URL Access to www.law.idf.il/sip_storage/files/7/ | Block | 1 |
| 79.180.194.120 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mas.aspx | None | 1 |
| 66.249.75.8 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/sip_storage/files/6/3426.jpg | Block | 1 |
| 212.117.143.250 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/login | Block | 1 |
| 169.229.3.91 | United States | 147.237.76.147 | chinuch.aka.idf.il | Illegal Byte Code Character in Method | Block | 1 |
| 66.176.73.239 | United States | 147.237.76.42 | refuah.idf.il | Illegal Byte Code Character in Parameter Name ₪[[†''#18[[]]#15ni ]] t…₪´¿„ˆnz3„g:ʊ6°,ÿʊɤ„ʊʔ=]]62#[[€¡e¨™•f¦ʊ<„[[61#]]ת ¶[[#25]]lÊ[[#17]]¸€ü | Block | 1 |
| 77.139.76.238 | France | 147.237.72.166 | aka.idf.il | Distributed Unauthorized Method for Known URL on www.aka.idf.il/ishurim/exampcert/ | Block | 1 |
| 169.229.3.91 | United States | 147.237.77.235 | sviva.idf.il | Multiple Unknown HTTP Request Method from 169.229.3.91 | Block | 1 |
| 66.249.66.117 | Israel | 147.237.0.17 | m.my-kosher-kravi.idf.il | Distributed Illegal Parameter Encoding | None | 1 |
| 66.176.73.239 | United States | 147.237.76.42 | refuah.idf.il | Distributed Illegal Byte Code Character in Query String | Block | 1 |
| 169.229.3.91 | United States | 147.237.72.167 | ishurim.aka.idf.il | Abnormally Long Request method | Block | 1 |
| 37.26.149.182 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 66.249.93.83 | Israel | 147.237.77.216 | dover.idf.il | Distributed URL is Above Root Directory | Block | 1 |
| 212.199.11.57 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 169.229.3.91 | United States | 147.237.77.235 | sviva.idf.il | Abnormally Long Request method | Block | 1 |
| 66.176.73.239 | United States | 147.237.76.42 | refuah.idf.il | NULL Character in Method ¬[[#0]][[#0]][[#0]]B¦#012•ÝÀbXdïMRìþn•Í¬£[[#27]]•{tÇ^Ý[[#5]]§*óõ ¦p±\ïÀœ"ó[[#14]]¸¿–[[#22]]′ôI¹@RƒñÄbEÖ…¸Õ | Block | 1 |
| 109.253.204.88 | Israel | 147.237.76.42 | refuah.idf.il | Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css | Block | 1 |
| 62.219.193.110 | Israel | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx | Block | 1 |
| 37.26.146.240 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 1 |
| 77.139.156.47 | France | 147.237.72.166 | aka.idf.il | Multiple Unauthorized Method for Known URL from 77.139.156.47 | Block | 1 |
| 66.249.69.224 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/atal1/izkor/print_text.asp | Block | 1 |
| 66.176.73.239 | United States | 147.237.76.42 | refuah.idf.il | Distributed Illegal Byte Code Character in URL | Block | 1 |
| 169.229.3.91 | United States | 147.237.72.167 | ishurim.aka.idf.il | Illegal Byte Code Character in URL | Block | 1 |
| 81.218.193.149 | Israel | 147.237.72.166 | aka.idf.il | Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/register.aspx | None | 1 |
| 169.229.3.91 | United States | 147.237.77.235 | sviva.idf.il | Illegal Byte Code Character in Query String on | Block | 1 |
| 160.83.42.137 | United Kingdom | 147.237.77.74 | law.idf.il | Multiple Unauthorized URL Access from 160.83.42.137 | Block | 1 |
| 66.102.9.24 | United States | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for aka.idf.il/main/home/default.aspx | Block | 1 |

09-25-2016-14:04:03 to 09-25-2016-15:04:03