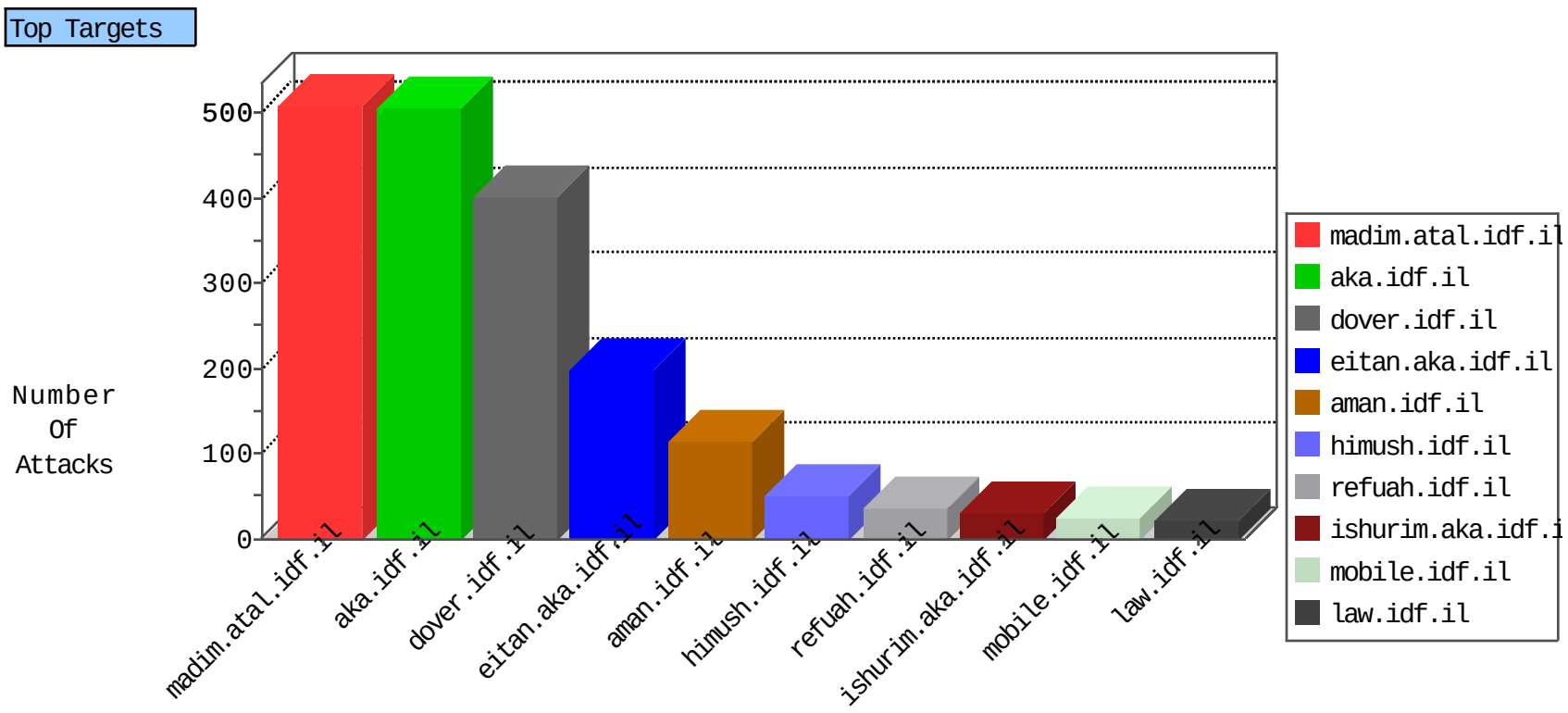
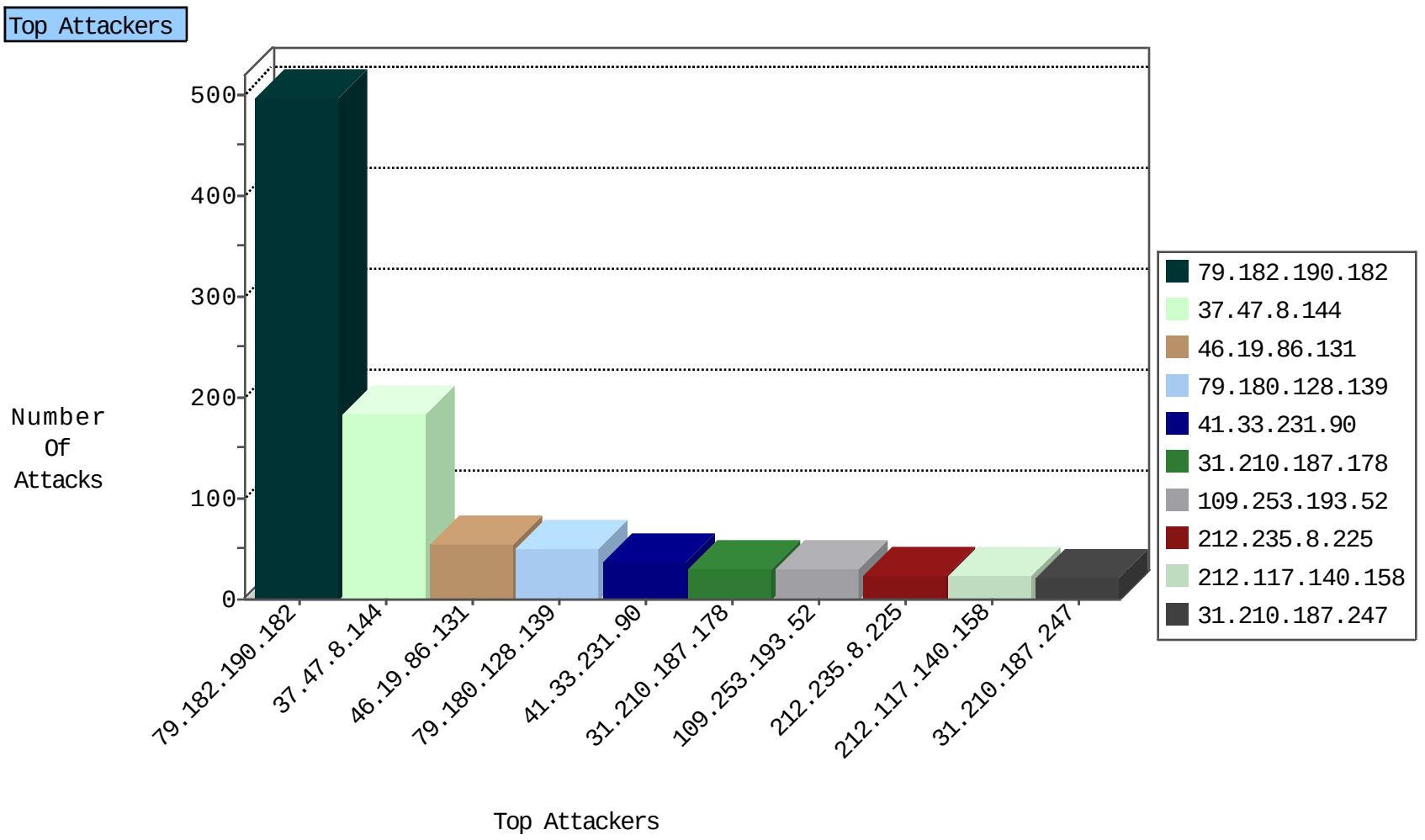
02-12-2016-17:04:09 to 02-12-2016-18:04:09

# IDF Under Attack Daily Report

Top Targets




Top Attackers



02-12-2016-17:04:09 to 02-12-2016-18:04:09

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 188.93.234.208 | Portugal | 147.237.76.176 | test.ncore.idf.il | Block_Ntp_All_Net | drop | 1 |
| 89.248.160.138 | Netherlands | 147.237.76.34 | yohalan.idf.il | Block_Ntp_All_Net | drop | 1 |
| 188.93.234.208 | Portugal | 147.237.76.200 | eitan.aka.idf.il | Block_Ntp_All_Net | drop | 1 |
| 158.130.6.191 | United States | 147.237.76.202 | e.halag.idf.il | Block_Udp_All_Nets | drop | 1 |
| 188.93.234.208 | Portugal | 147.237.76.201 | e.atal.idf.il | Block_Ntp_All_Net | drop | 1 |
| 185.130.5.224 | | 147.237.76.38 | e.e.meitav.idf.il | Block_Udp_All_Nets | drop | 1 |

02-12-2016-17:04:09 to 02-12-2016-18:04:09

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 195.39.211.247 | Ukraine | 147.237.77.176 | matpash.idf.il | C008: HTTP: Xenu UserAgent | Block | 1 |

02-12-2016-17:04:09 to 02-12-2016-18:04:09

## Top Attackers In IDS

| Attacker Address | Target Address | Attacker Country | Site | Signature | Count |
|---|---|---|---|---|---|
| 66.249.64.153 | 147.237.77.226 | United States | www.chamatz.aka.idf.il | ET SCAN NMAP -sA (2) | 2 |
| 195.34.150.18 | 147.237.77.216 | Austria | dover.idf.il | Tehila - Perl LWP with fake user agent | 2 |
| 95.156.251.10 | 147.237.76.199 | Germany | e.nakchal.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 183.61.109.189 | 147.237.0.15 | China | kosher-kravi.idf.il | ET SCAN NMAP -sS window 3072 | 1 |
| 183.61.109.189 | 147.237.0.15 | China | kosher-kravi.idf.il | ET SCAN NMAP -f -sS | 1 |
| 108.59.248.198 | 147.237.8.14 | United States | e.orchot.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 94.102.48.193 | 147.237.77.235 | Netherlands | sviva.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 218.246.0.97 | 147.237.8.14 | China | e.orchot.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 185.130.5.103 | 147.237.77.176 |  | matpash.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 183.61.109.189 | 147.237.0.15 | China | kosher-kravi.idf.il | ET SCAN NMAP -sS window 2048 | 1 |
| 130.211.100.171 | 147.237.0.35 | United States | akaws.idf.il | ET SCAN NMAP -sS window 1024 | 1 |

02-12-2016-17:04:09 to 02-12-2016-18:04:09

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 37.47.8.144 | Poland | 147.237.76.200 | eitan.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 183 |
| 46.19.86.131 | Israel | 147.237.76.30 | himush.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 44 |
| 41.33.231.90 | Egypt | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 35 |
| 109.253.193.52 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 29 |
| 79.180.128.139 | Israel | 147.237.72.156 | aman.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 24 |
| 79.180.128.139 | Israel | 147.237.72.156 | aman.idf.il | Bad TCP sequence | Invalid ACK number | alert | 24 |
| 149.78.154.69 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 16 |
| 52.33.66.29 | United States | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 16 |
| 31.210.187.247 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 15 |
| 31.168.240.21 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 15 |
| 31.210.187.178 | Israel | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 13 |
| 77.126.175.111 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 12 |
| 212.117.140.158 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 12 |
| 82.81.14.50 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 12 |
| 79.180.145.107 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 12 |
| 109.253.204.174 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 12 |
| 212.117.140.158 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | alert | 11 |
| 2.54.20.162 | Israel | 147.237.72.156 | aman.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 10 |
| 213.57.39.93 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 10 |
| 5.22.131.71 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 9 |
| 37.26.148.186 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 9 |
| 46.19.86.90 | Israel | 147.237.76.31 | nakchal.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 9 |
| 79.178.199.46 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 9 |
| 37.142.131.117 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | alert | 8 |
| 37.26.148.186 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | alert | 8 |
| 37.142.131.117 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 8 |
| 84.109.236.20 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 8 |
| 212.199.182.150 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 8 |
| 149.88.241.104 | Israel | 147.237.72.156 | aman.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 7 |
| 216.161.139.230 | United States | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 7 |
| 46.19.86.91 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 7 |
| 83.162.247.186 | Netherlands | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 7 |
| 157.55.39.31 | United States | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 7 |
| 83.162.247.186 | Netherlands | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 7 |
| 46.19.85.77 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 85.65.111.78 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 5.22.131.71 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid sequence number | monitor | 6 |
| 66.249.64.139 | United States | 147.237.77.234 | halag.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 85.65.111.78 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid sequence number | monitor | 6 |
| 79.183.0.41 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 109.66.8.131 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 216.161.139.230 | United States | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 6 |
| 85.65.202.79 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | alert | 6 |
| 79.180.7.244 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 6 |
| 213.57.39.93 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | alert | 6 |
| 31.210.187.178 | Israel | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | Invalid ACK number | alert | 6 |
| 5.29.233.51 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 66.249.65.14 | United States | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 77.125.121.8 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 85.65.202.79 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |

02-12-2016-17:04:09 to 02-12-2016-18:04:09

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 79.182.190.182 | Israel | 147.237.0.19 | madim.atal.idf.i | Too Many of the Same Response Code (404) in Session from 79.182.190.182 | Block | 293 |
| 79.182.190.182 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 147 |
| 79.182.190.182 | Israel | 147.237.0.19 | madim.atal.idf.i | Too Many of the Same Response Code (403) in Session from 79.182.190.182 | Block | 58 |
| 17.138.57.70 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 4 |
| 17.138.57.70 | United States | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 17.138.57.70 | Block | 4 |
| 31.154.235.163 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 3 |
| 212.235.8.225 | Israel | 147.237.72.166 | aka.idf.il | Multiple Abnormally Long Request from 212.235.8.225 | Block | 2 |
| 212.235.8.225 | Israel | 147.237.72.166 | aka.idf.il | Multiple Malformed HTTP Header Line from 212.235.8.225 | Block | 2 |
| 2.54.1.171 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 2 |
| 212.235.8.225 | Israel | 147.237.72.166 | aka.idf.il | Multiple Illegal Byte Code Character in Header Name from 212.235.8.225 | Block | 2 |
| 212.235.8.225 | Israel | 147.237.72.166 | aka.idf.il | Multiple Malformed URL from 212.235.8.225 | Block | 2 |
| 212.235.8.225 | Israel | 147.237.72.166 | aka.idf.il | Multiple Illegal Byte Code Character in Header Value from 212.235.8.225 | Block | 2 |
| 212.235.8.225 | Israel | 147.237.72.166 | aka.idf.il | Multiple NULL Character in Header Name from 212.235.8.225 | Block | 2 |
| 212.235.8.225 | Israel | 147.237.72.166 | aka.idf.il | Multiple Illegal Byte Code Character in Method from 212.235.8.225 | Block | 2 |
| 46.19.85.227 | Israel | 147.237.77.243 | mobile.idf.il | Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1465 | Block | 2 |
| 212.235.8.225 | Israel | 147.237.72.166 | aka.idf.il | Multiple Abnormally Long Header Line from 212.235.8.225 | Block | 2 |
| 88.198.48.46 | Germany | 147.237.0.34 | tikshuv.idf.il | Unauthorized URL Access to tikshuv.idf.il/shared/usercontrols/headerupper/ | Block | 2 |
| 212.235.8.225 | Israel | 147.237.72.166 | aka.idf.il | Multiple Unknown HTTP Request Method from 212.235.8.225 | Block | 2 |
| 72.9.148.10 | United States | 147.237.76.86 | navy.idf.il | Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx | Block | 1 |
| 66.249.65.224 | Israel | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 66.249.65.224 | Block | 1 |
| 149.78.253.93 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl38$ctl01$ctl03$cblQuestion$2 in www.aka.idf.il/main/giyus/questionnaire.aspx | None | 1 |
| 91.207.60.66 | Ukraine | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to 147.237.77.216/ | Block | 1 |
| 217.194.198.104 | Israel | 147.237.72.166 | aka.idf.il | Multiple Untraceable SSL Sessions from 217.194.198.104 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)) | None | 1 |
| 207.46.13.187 | United States | 147.237.77.170 | maarachot.idf.il | Unauthorized URL Access to maarachot.idf.il/pdf/files/5/109335.pdf×¦×'×?-×"×"×¦×œ×" | Block | 1 |
| 66.249.78.233 | Israel | 147.237.76.200 | eitan.aka.idf.il | Unknown Parameter PageNum in eitan.aka.idf.il/938-en/eitan.aspx | None | 1 |
| 93.172.155.192 | Israel | 147.237.77.216 | dover.idf.il | Distributed PHP Attempt | Block | 1 |
| 46.121.232.50 | Israel | 147.237.72.156 | aman.idf.il | Too Many Cookies in a Request - 101 cookies | Block | 1 |
| 212.235.8.225 | Israel | 147.237.72.166 | aka.idf.il | NULL Character in URL [[#29]]ÂŽÃŸ#×¢×ƒÃžâ€œÃœ Â§Â¿×¥Ö°taÂ½o×§[Ã·[[#27]]â€¦Â¢Â°×ƒÂ¬×™Ö¿[[#22]];Æ'Â³×' Ã?]7nwcÂ?.=Â¼"kÃ›3Â Â«v)@Ë†×§×ŸÂ±â€"×?zâ€˜â€¢"Âš×ƒÃž[[#18]]$ Â¨l,×£dl:Â±j[[#24]]×™Â·nâ€"sÂµxÂ¾Ö±;Â¹Â?Â¿[[#1]]ifÂ?×' Â»\Â¥Ö½lÖ¼Â dâ€™[[#26]]p}[[#22]]Ã»Â°7[[#21]][[#25]]j[[#29]]Â®Âž×¡â€š ×¡Ö´[[#15]]×ª8Ö¸Â?4Â¯â€¢o[[#30]]yuq[[#0]]Â¥×¥[[#28]]×§Ã¼k/"iÂŸ×¤×š â€˜%×ƒ Â¼Âµ×™>[[#18]]_Ã»Â¥"Ö½×€Ö»d^×©(â€"n×•Â³e×°â€°,×Ÿ Ö´[[#17]]u*×Ÿx×š×™oÖ»Â¯Â½[[#4]]Ã¿[[#21]]â,¬â€œÂš•Â¯tlÂ?Â¸[[#26]]×™ Ö·â€™[[#6]]rl0×™â€šy(×€Ö´ÂŽcy;×¢Ö¼Â¨â€ h×'Â | Block | 1 |
| 83.162.247.186 | Netherlands | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx | Block | 1 |
| 77.125.140.97 | Israel | 147.237.72.156 | aman.idf.il | Distributed Unauthorized URL Access on www.aman.idf.il/https:/www.aman.idf.il/ | Block | 1 |
| 66.249.65.231 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/fr.hamas | Block | 1 |
| 157.55.39.61 | United States | 147.237.76.42 | refuah.idf.il | Distributed Unauthorized URL Access on 147.237.76.42/robots.txt | Block | 1 |
| 93.172.155.192 | Israel | 147.237.76.42 | refuah.idf.il | Distributed PHP Attempt | Block | 1 |
| 37.142.164.72 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$42 in aka.idf.il/main/giyus/questionnaire.aspx | None | 1 |
| 212.235.8.225 | Israel | 147.237.72.166 | aka.idf.il | Distributed Illegal Byte Code Character in URL | Block | 1 |
| 66.249.78.233 | Israel | 147.237.76.200 | eitan.aka.idf.il | Unknown Parameter lang in eitan.aka.idf.il/938-en/eitan.aspx | None | 1 |
| 93.172.155.192 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/xmlrpc.php | Block | 1 |
| 66.249.64.239 | Israel | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to 147.237.77.233/1408-he/atal.aspx | Block | 1 |
| 8.37.70.126 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/1283-17305-en/dover.aspx&usg=alkjrhjnenwro66ftydx4i6inlnfh4qryq | Block | 1 |
| 212.235.8.225 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE) | None | 1 |
| 84.228.212.254 | Israel | 147.237.77.216 | dover.idf.il | SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE) | None | 1 |
| 79.179.118.118 | Israel | 147.237.72.166 | aka.idf.il | Illegal Byte Code Character in URL /main/kapatz//resources/images/innerpage/goback.gif | Block | 1 |
| 66.249.66.131 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/sip_storage/files/8/2828.jpg | Block | 1 |
| 157.55.39.209 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/1283-18058-en/dover.aspx <a href= | Block | 1 |
| 93.172.155.192 | Israel | 147.237.76.42 | refuah.idf.il | Distributed Unauthorized URL Access on www.refua.atal.idf.il/xmlrpc.php | Block | 1 |
| 40.77.167.17 | United States | 147.237.77.176 | matpash.idf.il | Unauthorized URL Access to 147.237.77.176/ | Block | 1 |
| 80.246.130.220 | Israel | 147.237.76.42 | refuah.idf.il | Distributed PHP Attempt | Block | 1 |
| 212.235.8.225 | Israel | 147.237.72.166 | aka.idf.il | Illegal URL Path Encoding [[#29]]ÂŽÃŸ#×¢×ƒÃžâ€œÃœ Â§Â¿×¥Ö°taÂ½o×§[Ã·[[#27]]â€¦Â¢Â°×ƒÂ¬×™Ö¿[[#22]];Æ'Â³×' Ã?]7nwcÂ?.=Â¼"kÃ›3Â Â«v)@Ë†×§×ŸÂ±â€"×?zâ€˜â€¢"Âš×ƒÃž[[#18]]$ Â¨l,×£dl:Â±j[[#24]]×™Â·nâ€"sÂµxÂ¾Ö±;Â¹Â?Â¿[[#1]]ifÂ?×' Â»\Â¥Ö½lÖ¼Â dâ€™[[#26]]p}[[#22]]Ã»Â°7[[#21]][[#25]]j[[#29]]Â®Âž×¡â€š ×¡Ö´[[#15]]×ª8Ö¸Â?4Â¯â€¢o[[#30]]yuq[[#0]]Â¥×¥[[#28]]×§Ã¼k/"iÂŸ×¤×š â€˜%×ƒ Â¼Âµ×™>[[#18]]_Ã»Â¥"Ö½×€Ö»d^×©(â€"n×•Â³e×°â€°,×Ÿ Ö´[[#17]]u*×Ÿx×š×™oÖ»Â¯Â½[[#4]]Ã¿[[#21]]â,¬â€œÂš•Â¯tlÂ?Â¸[[#26]]×™ Ö·â€™[[#6]]rl0×™â€šy(×€Ö´ÂŽcy;×¢Ö¼Â¨â€ | Block | 1 |
| 68.180.228.112 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/newsite/english/main.asp | Block | 1 |
| 66.249.65.14 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 1 |

02-12-2016-17:04:09 to 02-12-2016-18:04:09

02-12-2016-17:04:09 to 02-12-2016-18:04:09