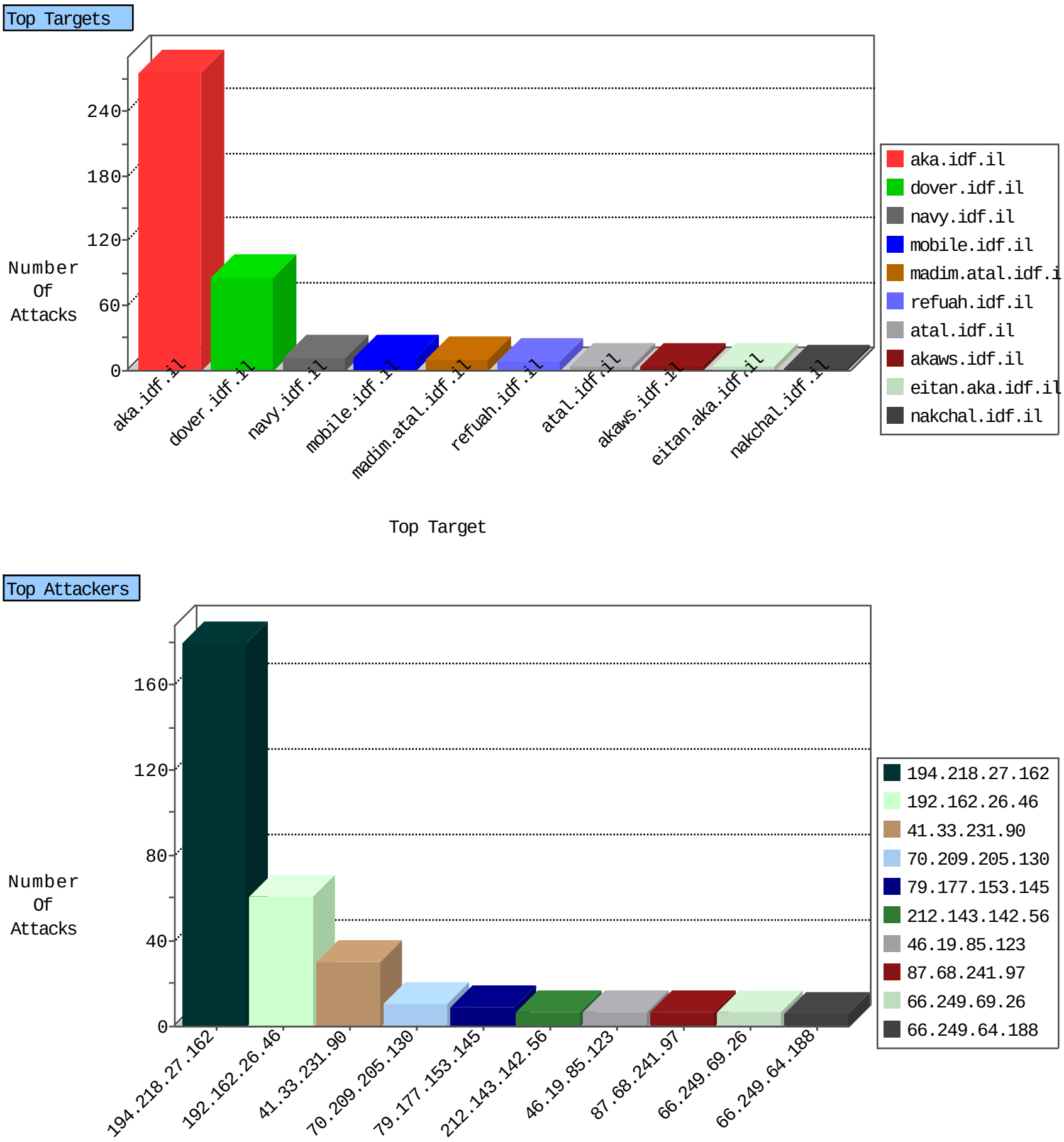
03-01-2016-04:04:02 to 03-01-2016-05:04:02

# IDF Under Attack
# Daily Report



03-01-2016-04:04:02 to 03-01-2016-05:04:02

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 89.248.172.207 | Netherlands | 147.237.76.31 | nakchal.idf.il | Block_Ntp_All_Net | drop | 1 |
| 185.130.5.246 | | 147.237.76.31 | nakchal.idf.il | Block_Ntp_All_Net | drop | 1 |
| 89.248.172.207 | Netherlands | 147.237.77.176 | matpash.idf.il | Block_Ntp_All_Net | drop | 1 |
| 185.130.5.246 | | 147.237.76.86 | navy.idf.il | Block_Ntp_All_Net | drop | 1 |
| 23.239.64.15 | United States | 147.237.76.42 | refuah.idf.il | Block_Ntp_All_Net | drop | 1 |
| 91.121.183.16 | France | 147.237.76.42 | refuah.idf.il | Block_Udp_All_Nets | drop | 1 |
| 85.25.43.94 | Germany | 147.237.77.233 | atal.idf.il | Block_Ntp_All_Net | drop | 1 |
| 185.130.5.246 | | 147.237.72.156 | aman.idf.il | Block_Ntp_All_Net | drop | 1 |

03-01-2016-04:04:02 to 03-01-2016-05:04:02

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 77.250.107.12 | Netherlands | 147.237.77.216 | dover.idf.il | C1000074: HTTP: majestic bot | Block | 3 |
| 83.149.126.98 | Netherlands | 147.237.72.166 | aka.idf.il | C1000074: HTTP: majestic bot | Block | 2 |
| 178.24.113.152 | Germany | 147.237.77.216 | dover.idf.il | C1000074: HTTP: majestic bot | Block | 2 |

03-01-2016-04:04:02 to 03-01-2016-05:04:02

## Top Attackers In IDS

| Attacker Address | Target Address | Attacker Country | Site | Signature | Count |
|---|---|---|---|---|---|
| 195.34.150.18 | 147.237.77.216 | Austria | dover.idf.il | Tehila - Perl LWP with fake user agent | 4 |
| 66.249.69.26 | 147.237.77.216 | United States | dover.idf.il | ET SCAN NMAP -sA (2) | 2 |
| 218.246.0.97 | 147.237.77.178 | China | e.matpash.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 188.191.21.221 | 147.237.0.34 | Ukraine | tikshuv.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 177.206.46.131 | 147.237.0.19 | Brazil | madim.atal.idf.i | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |
| 66.249.66.149 | 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 |
| 185.59.31.137 | 147.237.76.196 | Turkey | e.sviva.idf.il | ET SCAN Potential SSH Scan | 1 |

03-01-2016-04:04:02 to 03-01-2016-05:04:02

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 194.218.27.162 | Sweden | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 119 |
| 194.218.27.162 | Sweden | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | alert | 59 |
| 192.162.26.46 | Spain | 147.237.72.166 | aka.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 38 |
| 41.33.231.90 | Egypt | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 30 |
| 79.177.153.145 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 9 |
| 212.143.142.56 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 7 |
| 46.19.85.123 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 66.249.64.188 | United States | 147.237.0.19 | madim.atal.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 70.209.205.130 | United States | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 5 |
| 77.127.227.91 | Israel | 147.237.76.86 | navy.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 5 |
| 70.209.205.130 | United States | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 5 |
| 199.30.24.63 | United States | 147.237.76.200 | eitan.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 4 |
| 85.250.175.199 | Israel | 147.237.76.86 | navy.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 4 |
| 110.22.142.193 | Australia | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 4 |
| 109.253.150.153 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 109.253.202.251 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 77.125.76.24 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 2.54.8.29 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 79.178.101.2 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 106.38.241.106 | China | 147.237.72.166 | aka.idf.il | drop | SAM rule | drop | 2 |
| 77.247.181.163 | Netherlands | 147.237.77.216 | dover.idf.il | Directory Traversal | directory traversal overflow | monitor | 1 |
| 184.105.139.118 | United States | 147.237.8.50 | e.tikshuv.idf.il | Geo-location enforcement | Geo-location inbound enforcement | drop | 1 |
| 149.78.192.228 | Israel | 147.237.77.233 | atal.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 1 |
| 216.218.206.84 | United States | 147.237.77.205 | prisha.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 1 |
| 85.214.11.209 | Germany | 147.237.77.216 | dover.idf.il | Directory Traversal | directory traversal overflow | monitor | 1 |
| 185.38.14.215 | Netherlands | 147.237.77.216 | dover.idf.il | Directory Traversal | directory traversal overflow | monitor | 1 |
| 74.82.47.48 | United States | 147.237.77.234 | halag.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 1 |
| 184.105.139.86 | United States | 147.237.77.234 | halag.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 1 |
| 141.212.122.155 | United States | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 1 |
| 106.38.241.106 | China | 147.237.77.176 | matpash.idf.il | drop | SAM rule | drop | 1 |
| 77.247.181.165 | Netherlands | 147.237.77.216 | dover.idf.il | Directory Traversal | directory traversal overflow | monitor | 1 |
| 184.105.139.123 | United States | 147.237.0.35 | akaws.idf.il | drop | | drop | 1 |
| 70.209.205.130 | United States | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid sequence number | monitor | 1 |
| 158.58.188.211 | Iran, Islamic Republic of | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 1 |
| 184.105.139.86 | United States | 147.237.77.243 | mobile.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 1 |
| 46.166.170.6 | Lithuania | 147.237.77.216 | dover.idf.il | Directory Traversal | directory traversal overflow | monitor | 1 |
| 141.212.122.156 | United States | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 1 |
| 106.38.241.106 | China | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 1 |
| 199.87.154.251 | Canada | 147.237.77.216 | dover.idf.il | Directory Traversal | directory traversal overflow | monitor | 1 |
| 184.105.247.204 | United States | 147.237.8.14 | e.orchot.idf.il | Geo-location enforcement | Geo-location inbound enforcement | drop | 1 |
| 74.82.47.18 | United States | 147.237.8.24 | e.lifestyle.idf.il | Geo-location enforcement | Geo-location inbound enforcement | drop | 1 |
| 158.58.188.211 | Iran, Islamic Republic of | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 1 |
| 93.115.95.201 | Anonymous Proxy | 147.237.77.216 | dover.idf.il | Directory Traversal | directory traversal overflow | monitor | 1 |
| 193.90.12.90 | Norway | 147.237.77.216 | dover.idf.il | Directory Traversal | directory traversal overflow | monitor | 1 |
| 184.105.139.88 | United States | 147.237.8.27 | e.madim.atal.idf.i | Geo-location enforcement | Geo-location inbound enforcement | drop | 1 |
| 146.185.239.102 | Russian Federation | 147.237.76.44 | e.refuah.idf.il | Geo-location enforcement | Geo-location inbound enforcement | drop | 1 |
| 106.38.241.106 | China | 147.237.77.233 | atal.idf.il | drop | SAM rule | drop | 1 |
| 184.105.247.212 | United States | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 1 |
| 74.82.47.18 | United States | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 1 |
| 184.105.139.72 | United States | 147.237.77.74 | law.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 1 |

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 87.68.241.97 | Israel | 147.237.77.243 | mobile.idf.il | Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071 | Block | 4 |
| 66.249.69.26 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/error.htm | Block | 3 |
| 87.68.241.97 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 3 |
| 66.249.69.26 | United States | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 66.249.69.26 | Block | 2 |
| 115.79.90.235 | Vietnam | 147.237.76.42 | refuah.idf.il | Abnormally Long Request method | Block | 1 |
| 192.162.26.46 | Spain | 147.237.72.166 | aka.idf.il | Multiple NULL Character in Header Name from 192.162.26.46 | Block | 1 |
| 66.249.64.234 | United States | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to 147.237.77.233/1408-he/atal.aspx | Block | 1 |
| 192.162.26.46 | Spain | 147.237.72.166 | aka.idf.il | Malformed HTTP Header Line 1 | Block | 1 |
| 148.251.21.227 | Germany | 147.237.77.74 | law.idf.il | Multiple Unauthorized URL Access from 148.251.21.227 | Block | 1 |
| 74.82.47.2 | United States | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/ | Block | 1 |
| 192.162.26.46 | Spain | 147.237.72.166 | aka.idf.il | Too Many Headers per Request - 38 Headers | Block | 1 |
| 192.162.26.46 | Spain | 147.237.72.166 | aka.idf.il | Multiple Illegal Byte Code Character in Header Value from 192.162.26.46 | Block | 1 |
| 192.162.26.46 | Spain | 147.237.72.166 | aka.idf.il | Illegal Byte Code Character in Header Value | Block | 1 |
| 115.79.90.235 | Vietnam | 147.237.76.42 | refuah.idf.il | Illegal Byte Code Character in Method ¬[[#0]][[#0]][[#0]]p;[[#23]]Ü‘0W'[[#31]]D¹°úêmCvðžFš¸AµŸÿê²…/ašr_i¡[[#2]]bR˜Iåü[[#30]]›Khv×¥Ó[[#6]]•°÷}[[#11]]ð×ÄÐ± | Block | 1 |
| 192.162.26.46 | Spain | 147.237.72.166 | aka.idf.il | Multiple Unknown HTTP Request Method from 192.162.26.46 | Block | 1 |
| 66.249.66.149 | United States | 147.237.72.166 | aka.idf.il | SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO) | None | 1 |
| 192.162.26.46 | Spain | 147.237.72.166 | aka.idf.il | Malformed URL ¡[[#21]]Œ[[#1]][[#31]]¸cm¼~ | Block | 1 |
| 148.251.21.227 | Germany | 147.237.77.74 | law.idf.il | Unauthorized URL Access to www.mag.idf.il/320/patzar.aspx | Block | 1 |
| 77.75.76.171 | Czech Republic | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/newsite/english/documents.asp | Block | 1 |
| 192.162.26.46 | Spain | 147.237.72.166 | aka.idf.il | Unknown HTTP Request Method Aï[[#2]]~c[[#15]]y in URL ¡[[#21]]Œ[[#1]][[#31]]¸cm¼~ | Block | 1 |
| 27.55.78.42 | Thailand | 147.237.77.216 | dover.idf.il | SSL Untraceable Connection - Open Mode | None | 1 |
| 192.162.26.46 | Spain | 147.237.72.166 | aka.idf.il | Multiple Illegal Byte Code Character in Method from 192.162.26.46 | Block | 1 |
| 192.162.26.46 | Spain | 147.237.72.166 | aka.idf.il | Illegal Byte Code Character in Method Aï[[#2]]~c[[#15]]y | Block | 1 |
| 115.79.90.235 | Vietnam | 147.237.76.42 | refuah.idf.il | Illegal Byte Code Character in URL | Block | 1 |
| 192.162.26.46 | Spain | 147.237.72.166 | aka.idf.il | NULL Character in Header Name at \àl40-i[[#0]]º4˜]]yc[[#24]][[#16]]uöL¸Ñ<™G‘K4\@Ë®[[#0]]åÎ[[#20]]•[[#17]]nöW«[[#12]]¥>ÇLû ä•Ç[[#12]]<=UF[[#17]]œïÄ•-Ê½[[#2]]€ØD[[#21]] 2a[[#29]][[#29]]W“"hŒEVªSáˆ’-[[#15]]ÇB×‘j—ˆ Uh°[[#22]]µ`®¦jCòÍ–°+hlqiì¥#[[#16]]´[[#23]]•°sSUˆÃ*[[#26]]²[[#15]]ÌQ | Block | 1 |
| 192.162.26.46 | Spain | 147.237.72.166 | aka.idf.il | Multiple Abnormally Long Header Line from 192.162.26.46 | Block | 1 |
| 192.162.26.46 | Spain | 147.237.72.166 | aka.idf.il | Abnormally Long Header Line request header name | Block | 1 |
| 207.46.13.95 | United States | 147.237.72.166 | aka.idf.il | Unknown Parameter amp&amp in www.aka.idf.il/ | None | 1 |
| 46.19.85.123 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 1 |
| 192.162.26.46 | Spain | 147.237.72.166 | aka.idf.il | Multiple Malformed HTTP Header Line from 192.162.26.46 | Block | 1 |
| 192.162.26.46 | Spain | 147.237.72.166 | aka.idf.il | Illegal Byte Code Character in URL ¡[[#21]]Œ[[#1]][[#31]]¸cm¼~ | Block | 1 |
| 115.79.90.235 | Vietnam | 147.237.76.42 | refuah.idf.il | NULL Character in Method ¬[[#0]][[#0]][[#0]]p;[[#23]]Ü‘0W'[[#31]]D¹°úêmCvðžFš¸AµŸÿê²…/ašr_i¡[[#2]]bR˜Iåü[[#30]]›Khv×¥Ó[[#6]]•°÷}[[#11]]ð×ÄÐ± | Block | 1 |
| 192.162.26.46 | Spain | 147.237.72.166 | aka.idf.il | NULL Character in Method öÿYXf¦R-aÃ¹mMmËü[[#11]]™àÞBÈxÒtç€üöêeî¢§7w¸`Ñ2²8[[#18]]ž[[#24]][[#25]]ÿöñaZPÛ[[#23]]ßñeÆ¹LXebðRzàÓ•[[#3]]Å«'[[#19]][[#0]]þ¨”[[#16]]••<ÓÃ¼ýƒ»#§1nœ~’[[#0]][[#4]][[#23]]ø£o[[#2]]Y.úü(„ÈSlçKç[[#24]]Ãõ[[#30]]Sš[[#8]])p[[#20]]¶••®_•—vz•„õ©Á | Block | 1 |
| 192.162.26.46 | Spain | 147.237.72.166 | aka.idf.il | Multiple Abnormally Long Request from 192.162.26.46 | Block | 1 |
| 192.162.26.46 | Spain | 147.237.72.166 | aka.idf.il | Abnormally Long Request request version | Block | 1 |
| 210.87.255.225 | Hong Kong | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to www.refua.atal.idf.il/894-en/refuah.aspx | Block | 1 |
| 192.162.26.46 | Spain | 147.237.72.166 | aka.idf.il | Multiple Malformed URL from 192.162.26.46 | Block | 1 |
| 66.87.114.137 | United States | 147.237.77.216 | dover.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 192.162.26.46 | Spain | 147.237.72.166 | aka.idf.il | Illegal HTTP Version ª[[#6]]]ûc3ÐINah[[#3]]Î1Ä[[#7]][[#16]]©µM-öèZòµÐt;á,[[#19]]¥–1"ÿÌ[[#29]]-a | Block | 1 |
| 115.79.90.235 | Vietnam | 147.237.76.42 | refuah.idf.il | Unknown HTTP Request Method ¬[[#0]][[#0]][[#0]]p;[[#23]]Ü‘0W'[[#31]]D¹°úêmCvðžFš¸AµŸÿê²…/ašr_i¡[[#2]]bR˜Iåü[[#30]]›Khv×¥Ó[[#6]]•°÷}[[#11]]ð×ÄÐ± | Block | 1 |
| 192.162.26.46 | Spain | 147.237.72.166 | aka.idf.il | SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE) | None | 1 |
| 68.180.228.95 | United States | 147.237.76.31 | nakchal.idf.il | Parameter Type Violation PageNum in nakhal.idf.il/1110-he/nakhal.aspx | Block | 1 |
| 192.162.26.46 | Spain | 147.237.72.166 | aka.idf.il | Multiple Illegal Byte Code Character in Header Name from 192.162.26.46 | Block | 1 |
| 192.162.26.46 | Spain | 147.237.72.166 | aka.idf.il | Illegal Byte Code Character in Header Name \àl40-i[[#0]]º4˜]]yc[[#24]][[#16]]uöL¸Ñ<™G‘K4\@Ë®[[#0]]åÎ[[#20]]•[[#17]]nöW«[[#12]]¥>ÇLû ä•Ç[[#12]]<=UF[[#17]]œïÄ•-Ê½[[#2]]€ØD[[#21]] 2a[[#29]][[#29]]W“"hŒEVªSáˆ’-[[#15]]ÇB×‘j—ˆ Uh°[[#22]]µ`®¦jCòÍ–°+hlqiì¥#[[#16]]´[[#23]]•°sSUˆÃ*[[#26]]²[[#15]]ÌQ | Block | 1 |