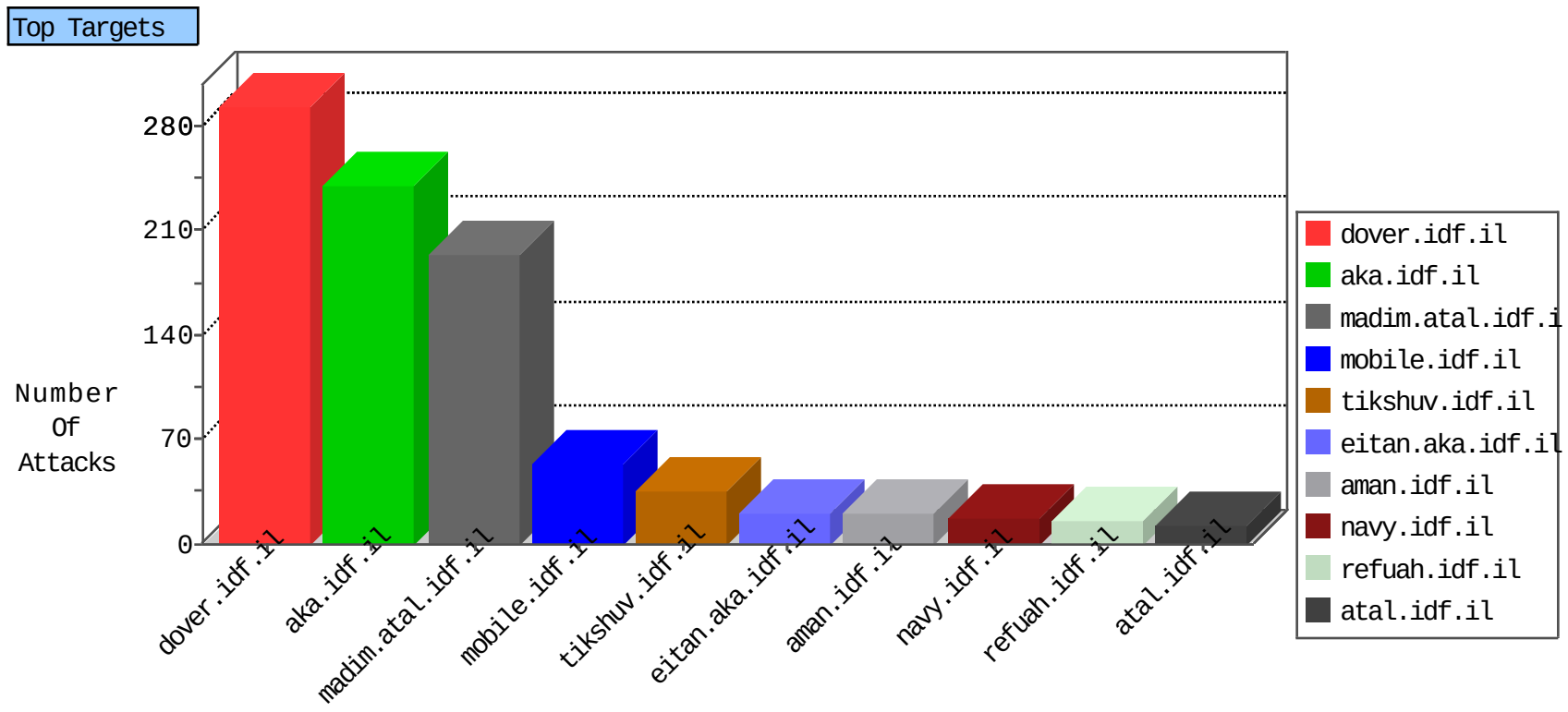
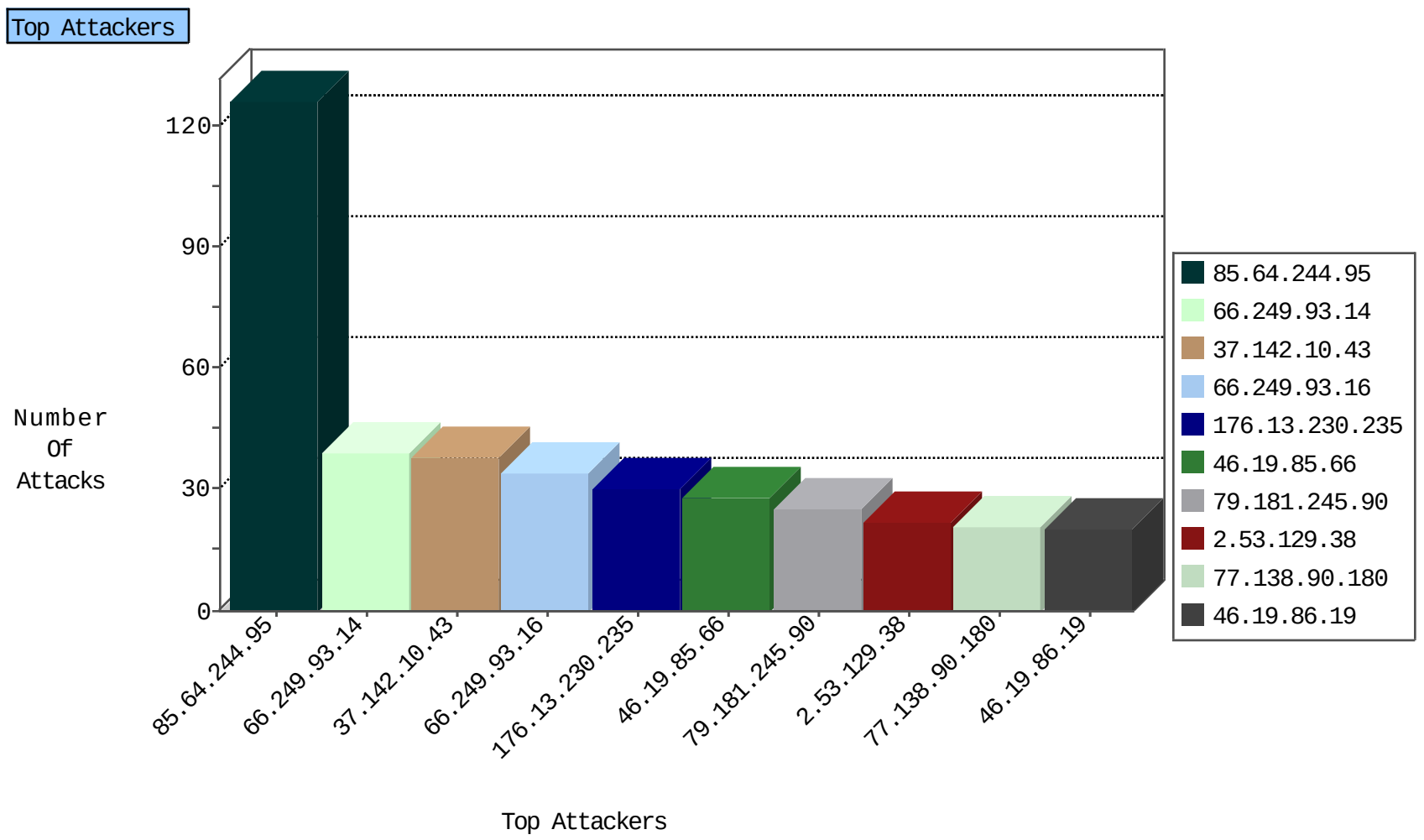
09-26-2016-21:04:00 to 09-26-2016-22:04:00

# IDF Under Attack
# Daily Report

Top Targets




Top Attackers



09-26-2016-21:04:00 to 09-26-2016-22:04:00

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 46.120.92.93 | Israel | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 7 |
| 195.228.168.121 | Hungary | 147.237.76.201 | e.atal.idf.il | L4 Source or Dest Port Zero | drop | 4 |
| 220.169.242.158 | China | 147.237.77.19 | law-forum.idf.il | JLM_Purple_Con_Limit_Tcp | drop | 1 |
| 54.72.73.168 | Ireland | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 1 |

09-26-2016-21:04:00 to 09-26-2016-22:04:00

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 91.200.12.47 | Ukraine | 147.237.77.74 | law.idf.il | C1000016: HTTP: administrator in URI | Permit | 8 |
| 106.38.241.106 | China | 147.237.77.216 | dover.idf.il | C1000071: HTTP: User Agent Sogou+web+spider | Permit | 8 |

09-26-2016-21:04:00 to 09-26-2016-22:04:00

Top Attackers In IDS

| Attacker Address | Target Address | Attacker Country | Site | Signature | Count |
|---|---|---|---|---|---|
| 46.219.66.30 | 147.237.77.178 | Ukraine | e.matpash.idf.il | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 3 |
| 163.172.129.15 | 147.237.76.199 | United Kingdom | e.nakchal.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 139.162.187.89 | 147.237.76.177 | United States | ncore.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 106.187.45.144 | 147.237.72.156 | Japan | aman.idf.il | ET SCAN Potential SSH Scan | 1 |
| 213.170.68.2 | 147.237.77.226 | Russian Federation | www.chamatz.aka.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 163.172.129.15 | 147.237.76.198 | United Kingdom | e.yohalan.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 106.187.45.144 | 147.237.76.42 | Japan | refuah.idf.il | ET SCAN Potential SSH Scan | 1 |
| 89.139.89.149 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 213.170.68.2 | 147.237.77.226 | Russian Federation | www.chamatz.aka.idf.il | ET SCAN NMAP -sS window 3072 | 1 |

09-26-2016-21:04:00 to 09-26-2016-22:04:00

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 37.142.10.43 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 38 |
| 46.19.85.66 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 24 |
| 77.138.90.180 | France | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 21 |
| 95.86.80.164 | Israel | 147.237.76.200 | eitan.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 16 |
| 79.181.245.90 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 14 |
| 79.179.96.132 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 12 |
| 79.181.245.90 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 11 |
| 46.19.86.19 | Israel | 147.237.0.34 | tikshuv.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 11 |
| 2.53.129.38 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 10 |
| 66.249.93.14 | Europe | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 9 |
| 66.249.93.14 | Europe | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 9 |
| 66.249.93.14 | Europe | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 9 |
| 212.143.142.56 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 9 |
| 66.249.93.14 | Europe | 147.237.77.216 | dover.idf.il | drop | Unexpected post SYN packet - RST or SYN expected | drop | 9 |
| 109.253.204.39 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 8 |
| 66.249.93.16 | Europe | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 8 |
| 66.249.93.16 | Europe | 147.237.77.216 | dover.idf.il | drop | Unexpected post SYN packet - RST or SYN expected | drop | 8 |
| 46.19.86.19 | Israel | 147.237.0.34 | tikshuv.idf.il | Bad TCP sequence | Invalid ACK number | alert | 8 |
| 66.249.93.16 | Europe | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 8 |
| 46.19.85.126 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 8 |
| 66.249.93.16 | Europe | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 8 |
| 46.19.85.210 | Israel | 147.237.77.233 | atal.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 7 |
| 62.219.144.118 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 7 |
| 217.132.140.15 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 7 |
| 46.19.86.231 | Israel | 147.237.0.34 | tikshuv.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 7 |
| 109.67.240.171 | Israel | 147.237.76.86 | navy.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 217.132.123.67 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 6 |
| 87.70.247.111 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 6 |
| 46.19.85.126 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 6 |
| 203.111.224.85 | Philippines | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 6 |
| 79.180.119.32 | Israel | 147.237.76.42 | refuah.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 6 |
| 87.68.45.177 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 69.62.177.74 | United States | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 6 |
| 2.53.144.8 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 5 |
| 66.249.93.15 | Europe | 147.237.77.216 | dover.idf.il | Directory Traversal | directory traversal overflow | monitor | 5 |
| 87.71.42.175 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 5 |
| 2.53.129.38 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 5 |
| 46.19.86.161 | Israel | 147.237.77.234 | halag.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 4 |
| 80.246.136.104 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 4 |
| 62.90.234.66 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 4 |
| 93.172.31.122 | Israel | 147.237.76.200 | eitan.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 4 |
| 109.253.204.39 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 4 |
| 46.19.86.71 | Israel | 147.237.76.147 | chinuch.aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 4 |
| 2.53.129.38 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | alert | 4 |
| 109.253.204.39 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 4 |
| 37.26.147.133 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 4 |
| 5.28.158.246 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 4 |
| 217.132.140.15 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 4 |
| 93.172.154.249 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 4 |
| 80.82.24.129 | Poland | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 4 |

09-26-2016-21:04:00 to 09-26-2016-22:04:00

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 85.64.244.95 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 126 |
| 176.13.230.235 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 30 |
| 77.139.106.82 | France | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 12 |
| 46.19.86.167 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 12 |
| 176.13.243.85 | Israel | 147.237.77.243 | mobile.idf.il | Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword | Block | 5 |
| 5.29.15.114 | Israel | 147.237.72.166 | aka.idf.il | Multiple Illegal Byte Code Character in URL from 5.29.15.114 | Block | 5 |
| 77.139.106.82 | France | 147.237.77.243 | mobile.idf.il | Distributed Parameter Type Violation on mobile.idf.il/sachar/changepassword parameter CurrentPassword | Block | 4 |
| 46.19.85.66 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 4 |
| 77.138.238.48 | France | 147.237.72.166 | aka.idf.il | Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/yahash2017/lobby.aspx | Block | 3 |
| 79.180.23.70 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 109.253.142.178 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 85.250.116.100 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 46.121.115.171 | Israel | 147.237.72.166 | aka.idf.il | Multiple Unauthorized Method for Known URL from 46.121.115.171 | Block | 2 |
| 46.19.86.197 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 46.120.115.177 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 176.13.13.11 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Parameter Type Violation on mobile.idf.il/sachar/changepassword parameter CurrentPassword | Block | 2 |
| 46.121.115.171 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/login.aspx | Block | 2 |
| 77.138.234.231 | France | 147.237.72.156 | aman.idf.il | Unauthorized URL Access to www.aman.idf.il/favicon.ico | Block | 1 |
| 109.190.129.127 | France | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for aka.idf.il/giyus/ | Block | 1 |
| 46.19.85.166 | Israel | 147.237.72.166 | aka.idf.il | Distributed Illegal Byte Code Character in URL | Block | 1 |
| 195.154.181.168 | France | 147.237.76.31 | nakchal.idf.il | Admin Blocking | Block | 1 |
| 85.65.232.167 | Israel | 147.237.72.156 | aman.idf.il | Illegal Parameter Encoding ctl00&2 in www.aman.idf.il/modiin/questionnaires.aspx | None | 1 |
| 77.139.236.27 | France | 147.237.72.166 | aka.idf.il | Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/miyun/miyunsummary.aspx | Block | 1 |
| 195.154.181.168 | France | 147.237.0.15 | kosher-kravi.idf.i | Unauthorized URL Access to kosher-kravi.idf.il/administrator/components/com_aceftp/quixplorer/index.php | Block | 1 |
| 169.229.3.91 | United States | 147.237.77.233 | atal.idf.il | Multiple Untraceable SSL Sessions from 169.229.3.91 (Protocol violation (SSL_CONN_CLIENT_HELLO)) | None | 1 |
| 66.249.93.14 | Israel | 147.237.77.216 | dover.idf.il | Distributed URL is Above Root Directory | Block | 1 |
| 91.200.12.47 | Ukraine | 147.237.77.74 | law.idf.il | Unauthorized URL Access to www.law.idf.il/wp-login.php | Block | 1 |
| 195.154.181.168 | France | 147.237.76.86 | navy.idf.il | PHP Attempt | Block | 1 |
| 24.38.9.130 | United States | 147.237.72.166 | aka.idf.il | Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/yahash2017/lobby.aspx | Block | 1 |
| 195.154.181.168 | France | 147.237.72.166 | aka.idf.il | PHP Attempt | Block | 1 |
| 84.108.87.238 | Israel | 147.237.77.176 | matpash.idf.il | Unauthorized URL Access to www.cogat.idf.il/wp-login.php | Block | 1 |
| 46.121.115.171 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized Method HEAD for www.aka.idf.il/main/giyus/kiosk/kiosk.aspx | Block | 1 |
| 109.253.129.103 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 46.19.86.149 | Israel | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to 147.237.77.233/1246-he/atal.aspx | Block | 1 |
| 195.154.181.168 | France | 147.237.76.31 | nakchal.idf.il | Distributed PHP Attempt | Block | 1 |
| 85.65.232.167 | Israel | 147.237.72.156 | aman.idf.il | SSL Untraceable Connection - Open Mode | None | 1 |
| 2.53.129.38 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 195.154.181.168 | France | 147.237.72.156 | aman.idf.il | Admin Blocking | Block | 1 |
| 169.229.3.91 | United States | 147.237.77.234 | halag.idf.il | SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO) | None | 1 |
| 68.180.231.57 | United States | 147.237.77.216 | dover.idf.il | Parameter Type Violation PageNum in www.idf.il/1779-he/dover.aspx | Block | 1 |
| 107.178.41.12 | United States | 147.237.72.166 | aka.idf.il | Distributed Illegal Byte Code Character in URL | Block | 1 |
| 45.33.130.244 | United States | 147.237.72.166 | aka.idf.il | Distributed Illegal Byte Code Character in URL | Block | 1 |
| 195.154.181.168 | France | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to aka.idf.il/administrator/components/com_aceftp/quixplorer/index.php | Block | 1 |
| 180.76.15.17 | China | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to www.atal.idf.il/templates/shared/usercontrols/headerupper/ | Block | 1 |
| 66.102.6.3 | United States | 147.237.72.166 | aka.idf.il | Distributed Unauthorized Method for Known URL on www.aka.idf.il/sachar | Block | 1 |
| 195.154.181.168 | France | 147.237.76.31 | nakchal.idf.il | Unauthorized URL Access to nakhal.idf.il/administrator/components/com_aceftp/quixplorer/index.php | Block | 1 |
| 80.82.24.129 | Poland | 147.237.72.166 | aka.idf.il | Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/yahash2017/lobby.aspx | Block | 1 |
| 5.29.15.114 | Israel | 147.237.72.166 | aka.idf.il | Distributed Illegal Byte Code Character in URL | Block | 1 |
| 195.154.181.168 | France | 147.237.72.156 | aman.idf.il | PHP Attempt | Block | 1 |
| 176.13.1.241 | Israel | 147.237.76.42 | refuah.idf.il | Parameter Type Violation ctl00$ContentPlaceHolder1$txtLastName in www.refua.atal.idf.il/1518-he/refuah.aspx | Block | 1 |

09-26-2016-21:04:00 to 09-26-2016-22:04:00