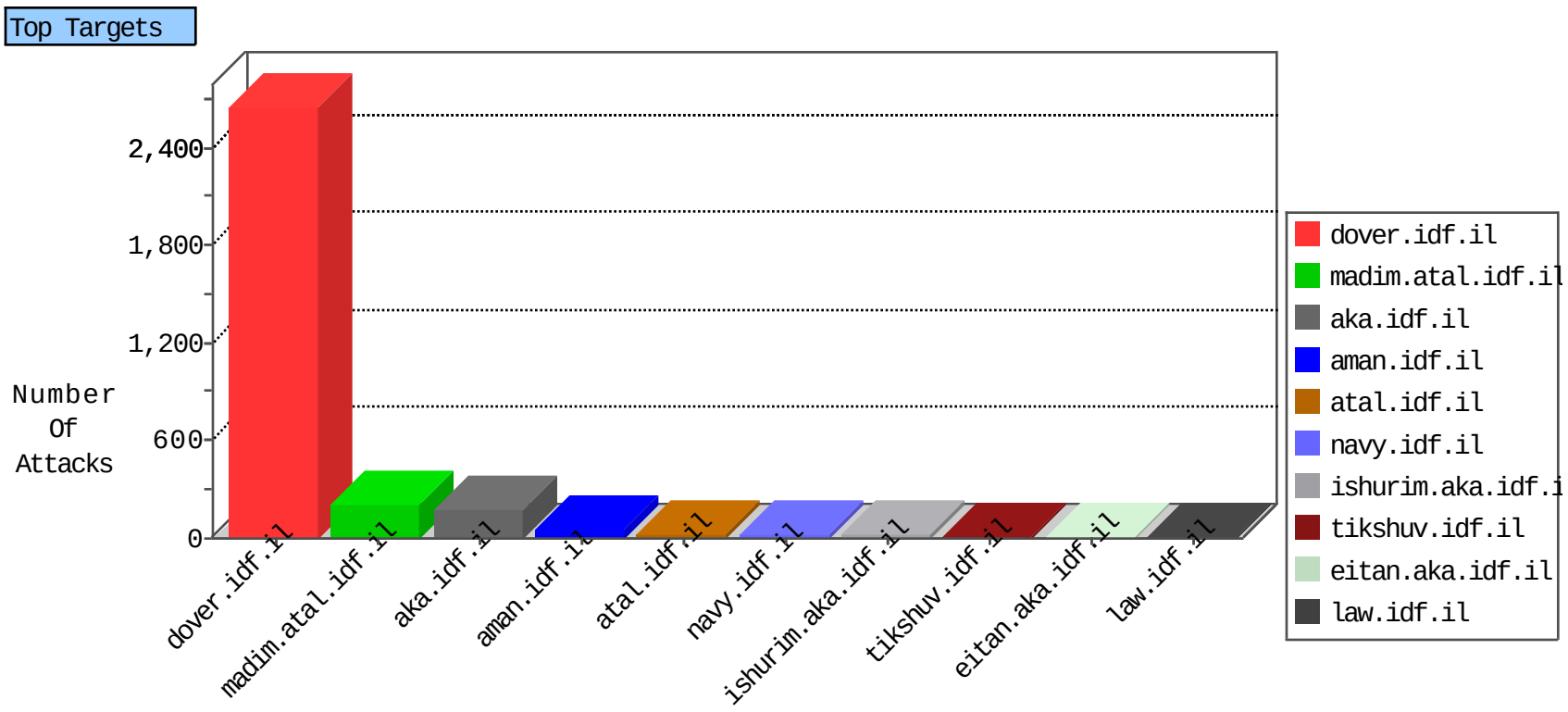
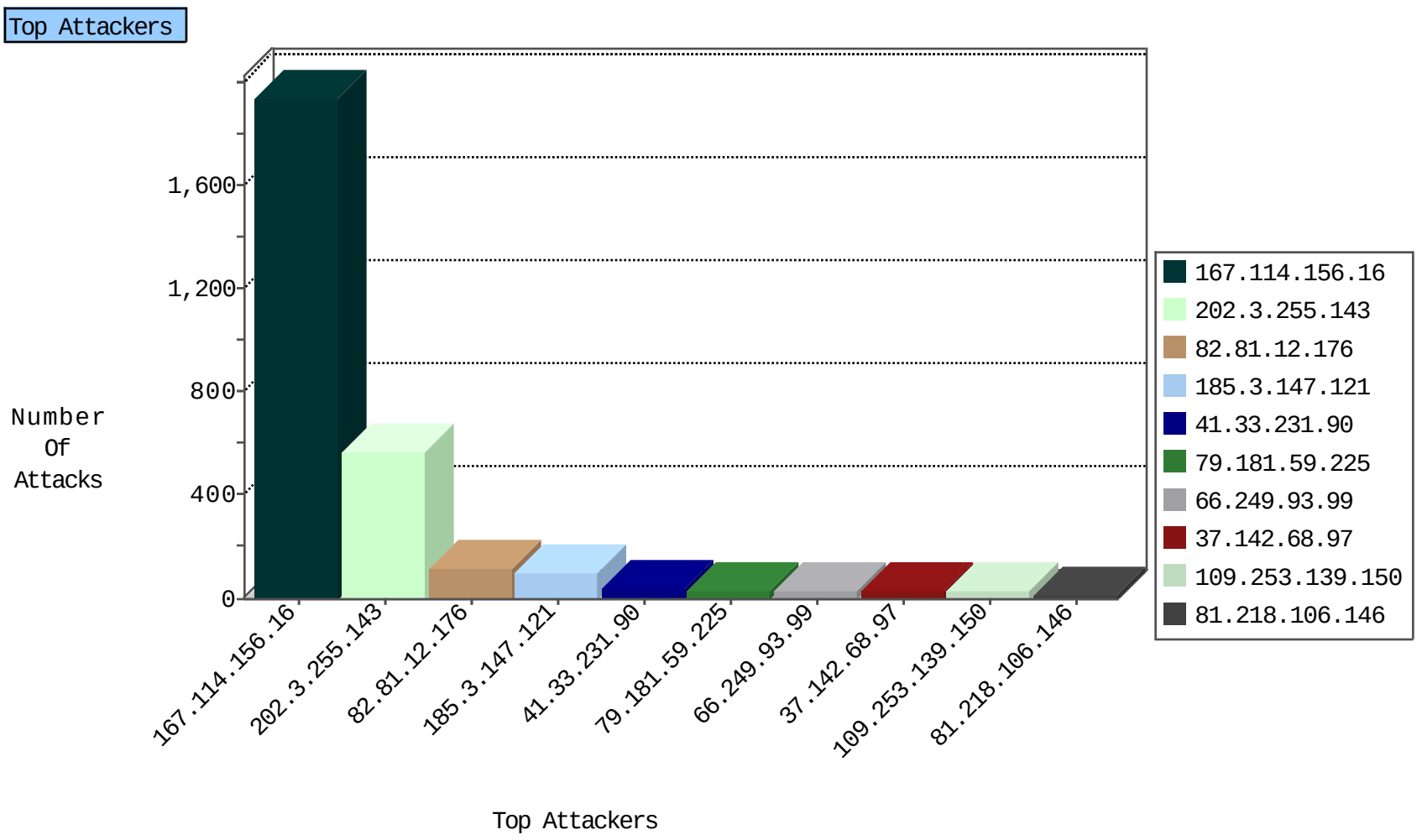
01-19-2016-06:04:07 to 01-19-2016-07:04:07

# IDF Under Attack
# Daily Report



01-19-2016-06:04:07 to 01-19-2016-07:04:07

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 167.114.156.16 | Canada | 147.237.77.216 | dover.idf.il | DOS-Tool-SwitchbladG | dest-reset | 3202 |
| 82.81.12.176 | Israel | 147.237.72.166 | aka.idf.il | Block_Udp_All_Nets | drop | 119 |
| 185.35.62.33 | Switzerland | 147.237.76.201 | e.atal.idf.il | Block_Udp_All_Nets | drop | 1 |
| 218.232.247.187 | Korea, Republic of | 147.237.76.31 | nakchal.idf.il | Block_Udp_All_Nets | drop | 1 |
| 218.232.247.187 | Korea, Republic of | 147.237.76.38 | e.e.meitav.idf.il | Block_Udp_All_Nets | drop | 1 |

01-19-2016-06:04:07 to 01-19-2016-07:04:07

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 123.126.113.154 | China | 147.237.77.216 | dover.idf.il | C103: HTTP: User Agent Sogou+web+spider | Block | 5 |
| 106.38.241.106 | China | 147.237.72.166 | aka.idf.il | C103: HTTP: User Agent Sogou+web+spider | Block | 1 |
| 106.38.241.106 | China | 147.237.77.216 | dover.idf.il | C103: HTTP: User Agent Sogou+web+spider | Block | 1 |

01-19-2016-06:04:07 to 01-19-2016-07:04:07

Top Attackers In IDS

| Attacker Address | Target Address | Attacker Country | Site | Signature | Count |
|---|---|---|---|---|---|
| 202.3.255.143 | 147.237.77.216 | French Polynesia | dover.idf.il | GPL SCAN nmap TCP | 530 |
| 66.249.93.99 | 147.237.77.216 | United States | dover.idf.il | ET SCAN NMAP -sA (2) | 30 |
| 192.35.222.17 | 147.237.77.216 | United States | dover.idf.il | ET DOS SSL Bomb DoS Attempt | 5 |
| 195.34.150.18 | 147.237.77.216 | Austria | dover.idf.il | Tehila - Perl LWP with fake user agent | 4 |
| 66.249.64.13 | 147.237.76.42 | United States | refuah.idf.il | ET SCAN NMAP -sA (2) | 2 |
| 41.33.231.90 | 147.237.77.216 | Egypt | dover.idf.il | Tehila - Perl LWP with fake user agent | 2 |
| 183.60.48.25 | 147.237.76.196 | China | e.sviva.idf.il | ET SCAN Potential SSH Scan | 1 |
| 183.60.48.25 | 147.237.0.200 | China | m4u.idf.il | ET SCAN Potential SSH Scan | 1 |
| 94.102.48.195 | 147.237.8.14 | Netherlands | e.orchot.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 183.60.48.25 | 147.237.76.200 | China | eitan.aka.idf.il | ET SCAN Potential SSH Scan | 1 |
| 183.60.48.25 | 147.237.76.86 | China | navy.idf.il | ET SCAN Potential SSH Scan | 1 |
| 108.61.228.100 | 147.237.76.196 | United States | e.sviva.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 60.209.5.30 | 147.237.8.45 | China | e.eitan.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |

01-19-2016-06:04:07 to 01-19-2016-07:04:07

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 202.3.255.143 | French Polynesia | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 37 |
| 41.33.231.90 | Egypt | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 28 |
| 81.218.106.146 | Israel | 147.237.77.233 | atal.idf.il | drop | First packet isn't SYN | drop | 10 |
| 213.55.111.38 | Ethiopia | 147.237.76.86 | navy.idf.il | drop | First packet isn't SYN | drop | 9 |
| 37.105.201.173 | Saudi Arabia | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 8 |
| 46.19.85.204 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 8 |
| 188.120.148.188 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 7 |
| 41.33.232.66 | Egypt | 147.237.77.216 | dover.idf.il | Block HTTP Non Compliant | Failed to handle connection data | monitor | 6 |
| 109.66.26.158 | Israel | 147.237.72.156 | aman.idf.il | drop | First packet isn't SYN | drop | 6 |
| 110.168.232.245 | Thailand | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 5 |
| 195.34.150.18 | Austria | 147.237.77.216 | dover.idf.il | Block HTTP Non Compliant | Failed to handle connection data | monitor | 4 |
| 46.19.86.206 | Israel | 147.237.76.86 | navy.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 46.19.85.249 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 3 |
| 141.8.132.112 | Russian Federation | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 147.236.38.162 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 109.66.6.140 | Israel | 147.237.72.166 | aka.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 |
| 79.176.153.68 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 167.114.156.16 | Canada | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 3 |
| 41.33.231.90 | Egypt | 147.237.77.216 | dover.idf.il | Block HTTP Non Compliant | Failed to handle connection data | monitor | 3 |
| 167.114.156.16 | Canada | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 3 |
| 192.35.222.17 | United States | 147.237.77.216 | dover.idf.il | SSL Enforcement Violation | TLS Servers Cipher Suites Vulnerability Scanning Tools | reject | 2 |
| 91.200.12.143 | Ukraine | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 2 |
| 81.169.237.146 | Germany | 147.237.8.46 | e.chinuch.idf.il | drop | SAM rule | drop | 2 |
| 66.249.78.144 | United States | 147.237.76.86 | navy.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 2 |
| 84.109.145.49 | Israel | 147.237.76.86 | navy.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 2 |
| 91.200.12.7 | Ukraine | 147.237.72.166 | aka.idf.il | drop | SAM rule | drop | 2 |
| 157.55.2.137 | United States | 147.237.76.200 | eitan.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 2 |
| 81.218.40.194 | Israel | 147.237.76.86 | navy.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 2 |
| 130.193.51.91 | Russian Federation | 147.237.76.200 | eitan.aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 2 |
| 91.200.12.7 | Ukraine | 147.237.77.226 | www.chamatz.aka.idf.il | drop | SAM rule | drop | 2 |
| 91.200.12.143 | Ukraine | 147.237.0.34 | tikshuv.idf.il | drop | SAM rule | drop | 2 |
| 54.241.198.78 | United States | 147.237.77.216 | dover.idf.il | Block HTTP Non Compliant | Failed to handle connection data | monitor | 2 |
| 41.33.231.90 | Egypt | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 2 |
| 5.22.135.194 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 1 |
| 74.82.47.50 | United States | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 1 |
| 184.105.139.114 | United States | 147.237.77.227 | e.hamaz.idf.il | Geo-location enforcement | Geo-location inbound enforcement | drop | 1 |
| 208.115.113.84 | United States | 147.237.77.74 | law.idf.il | drop | SAM rule | drop | 1 |
| 184.105.247.243 | United States | 147.237.76.176 | test.ncore.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 1 |
| 184.105.139.83 | United States | 147.237.72.156 | aman.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 1 |
| 216.218.206.90 | United States | 147.237.77.121 | e.navy.idf.il | Geo-location enforcement | Geo-location inbound enforcement | drop | 1 |
| 5.29.218.128 | Israel | 147.237.0.15 | kosher-kravi.idf.il | Bad TCP sequence | Invalid ACK number | alert | 1 |
| 192.249.66.247 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 1 |
| 74.82.47.52 | United States | 147.237.77.74 | law.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 1 |
| 184.105.247.208 | United States | 147.237.72.167 | ishurim.aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 1 |
| 46.19.86.12 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 1 |
| 37.142.64.56 | Israel | 147.237.0.34 | tikshuv.idf.il | Bad TCP sequence | Invalid ACK number | alert | 1 |
| 81.218.40.194 | Israel | 147.237.76.86 | navy.idf.il | Bad TCP sequence | Invalid ACK number | alert | 1 |
| 184.105.247.243 | United States | 147.237.77.235 | sviva.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 1 |
| 67.83.156.83 | United States | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 1 |

01-19-2016-06:04:07 to 01-19-2016-07:04:07

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 185.3.147.121 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 80 |
| 79.181.59.225 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 31 |
| 37.142.68.97 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 28 |
| 109.253.139.150 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 27 |
| 185.3.147.121 | Israel | 147.237.0.19 | madim.atal.idf.il | Too Many of the Same Response Code (404) in Session from 185.3.147.121 | Block | 16 |
| 23.96.208.27 | United States | 147.237.77.233 | atal.idf.il | Multiple Unauthorized URL Access from 23.96.208.27 | Block | 4 |
| 85.214.116.128 | Germany | 147.237.77.233 | atal.idf.il | Multiple Unauthorized URL Access from 85.214.116.128 | Block | 4 |
| 84.94.84.31 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 72.167.190.33 | United States | 147.237.72.156 | aman.idf.il | Distributed PHP Attempt | Block | 2 |
| 191.252.51.11 | Brazil | 147.237.72.167 | ishurim.aka.idf.i | Distributed PHP Attempt | Block | 2 |
| 72.167.190.33 | United States | 147.237.72.156 | aman.idf.il | Distributed Unauthorized URL Access on www.aman.idf.il/wp-login.php | Block | 2 |
| 109.253.141.202 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 2 |
| 2.54.140.19 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 2 |
| 208.184.112.74 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx. | Block | 2 |
| 66.249.69.32 | Israel | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on 147.237.77.216/ | Block | 1 |
| 186.202.127.34 | Brazil | 147.237.72.156 | aman.idf.il | Distributed PHP Attempt | Block | 1 |
| 89.218.26.108 | Kazakstan | 147.237.72.156 | aman.idf.il | Distributed PHP Attempt | Block | 1 |
| 217.160.130.162 | Germany | 147.237.72.156 | aman.idf.il | Distributed Unauthorized URL Access on www.aman.idf.il/wp-login.php | Block | 1 |
| 82.145.45.44 | United Kingdom | 147.237.0.19 | madim.atal.idf.il | Distributed Unauthorized URL Access on madim.atal.idf.il/old/wp-admin/ | Block | 1 |
| 207.46.13.167 | United States | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/robots.txt | Block | 1 |
| 61.135.190.71 | China | 147.237.0.34 | tikshuv.idf.il | Unauthorized URL Access to 147.237.0.34/style/shared/datepicker.css | Block | 1 |
| 176.28.17.231 | Germany | 147.237.0.19 | madim.atal.idf.il | Unauthorized URL Access to madim.atal.idf.il/test/wp-admin/ | Block | 1 |
| 159.253.147.4 | Netherlands | 147.237.72.156 | aman.idf.il | Distributed Unauthorized URL Access on www.aman.idf.il/wp-login.php | Block | 1 |
| 74.208.77.114 | United States | 147.237.72.156 | aman.idf.il | Distributed Unauthorized URL Access on www.aman.idf.il/wp-login.php | Block | 1 |
| 196.37.186.227 | South Africa | 147.237.72.167 | ishurim.aka.idf.i | Distributed PHP Attempt | Block | 1 |
| 23.96.208.191 | United States | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to atal.idf.il/wp-admin/ | Block | 1 |
| 5.9.60.113 | Germany | 147.237.72.156 | aman.idf.il | Distributed PHP Attempt | Block | 1 |
| 97.74.6.175 | United States | 147.237.0.19 | madim.atal.idf.il | Unauthorized URL Access to madim.atal.idf.il/wp/wp-admin/ | Block | 1 |
| 61.135.190.198 | China | 147.237.0.34 | tikshuv.idf.il | Unauthorized URL Access to 147.237.0.34/style/shared/reset.css | Block | 1 |
| 85.214.116.128 | Germany | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to atal.idf.il/test/wp-admin/ | Block | 1 |
| 212.85.108.202 | Poland | 147.237.72.167 | ishurim.aka.idf.i | Distributed PHP Attempt | Block | 1 |
| 50.62.208.71 | United States | 147.237.72.156 | aman.idf.il | Distributed PHP Attempt | Block | 1 |
| 174.136.25.169 | United States | 147.237.72.156 | aman.idf.il | Distributed Unauthorized URL Access on www.aman.idf.il/wp-login.php | Block | 1 |
| 79.170.44.85 | United Kingdom | 147.237.0.19 | madim.atal.idf.il | Unauthorized URL Access to madim.atal.idf.il/wordpress/wp-admin/ | Block | 1 |
| 201.172.52.37 | Mexico | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/mazi | Block | 1 |
| 74.82.47.2 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to 147.237.77.216/ | Block | 1 |
| 195.154.146.225 | France | 147.237.77.216 | dover.idf.il | Illegal HTTP Version HTTP/ | Block | 1 |
| 5.150.195.212 | Sweden | 147.237.72.156 | aman.idf.il | Distributed Unauthorized URL Access on www.aman.idf.il/wp-login.php | Block | 1 |
| 107.178.194.87 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx. | Block | 1 |
| 66.249.78.104 | Israel | 147.237.72.166 | aka.idf.il | Distributed Unauthorized URL Access on 147.237.72.166/ | Block | 1 |
| 186.202.127.34 | Brazil | 147.237.72.156 | aman.idf.il | Distributed Unauthorized URL Access on www.aman.idf.il/wp-login.php | Block | 1 |
| 89.218.26.108 | Kazakstan | 147.237.72.156 | aman.idf.il | Distributed Unauthorized URL Access on www.aman.idf.il/wp-login.php | Block | 1 |
| 208.109.207.221 | United States | 147.237.0.19 | madim.atal.idf.il | Distributed Unauthorized URL Access on madim.atal.idf.il/wp-admin/ | Block | 1 |
| 61.135.190.72 | China | 147.237.0.34 | tikshuv.idf.il | Distributed Unauthorized URL Access on 147.237.0.34/style/shared/960.css | Block | 1 |
| 179.188.17.23 | Brazil | 147.237.72.167 | ishurim.aka.idf.i | Distributed PHP Attempt | Block | 1 |
| 162.144.75.80 | United States | 147.237.72.156 | aman.idf.il | Distributed PHP Attempt | Block | 1 |
| 79.96.38.53 | Poland | 147.237.72.156 | aman.idf.il | Distributed PHP Attempt | Block | 1 |
| 198.1.70.245 | United States | 147.237.72.167 | ishurim.aka.idf.i | Distributed PHP Attempt | Block | 1 |
| 5.9.60.113 | Germany | 147.237.72.156 | aman.idf.il | Distributed Unauthorized URL Access on www.aman.idf.il/wp-login.php | Block | 1 |
| 97.74.215.78 | United States | 147.237.0.19 | madim.atal.idf.il | Distributed Unauthorized URL Access on madim.atal.idf.il/blog/wp-admin/ | Block | 1 |

01-19-2016-06:04:07 to 01-19-2016-07:04:07