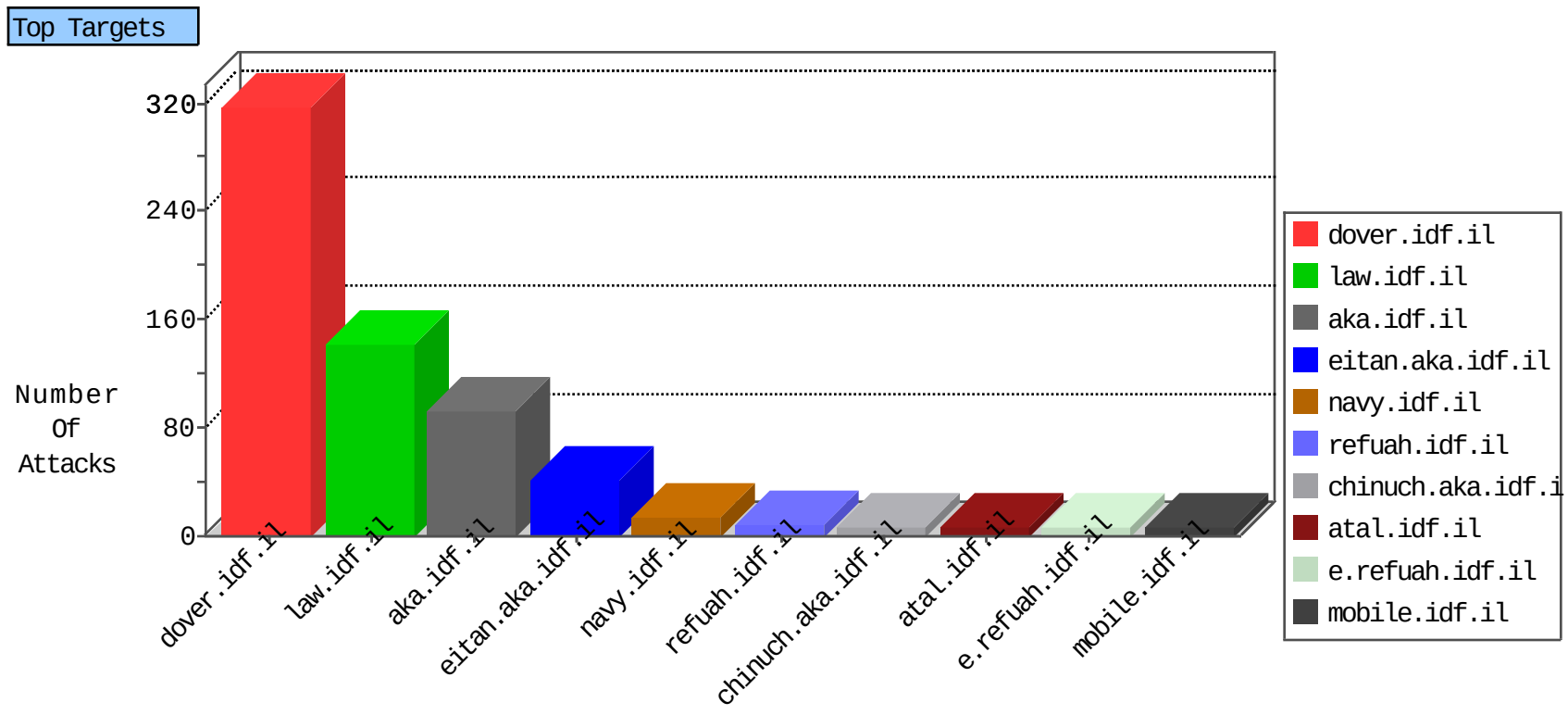
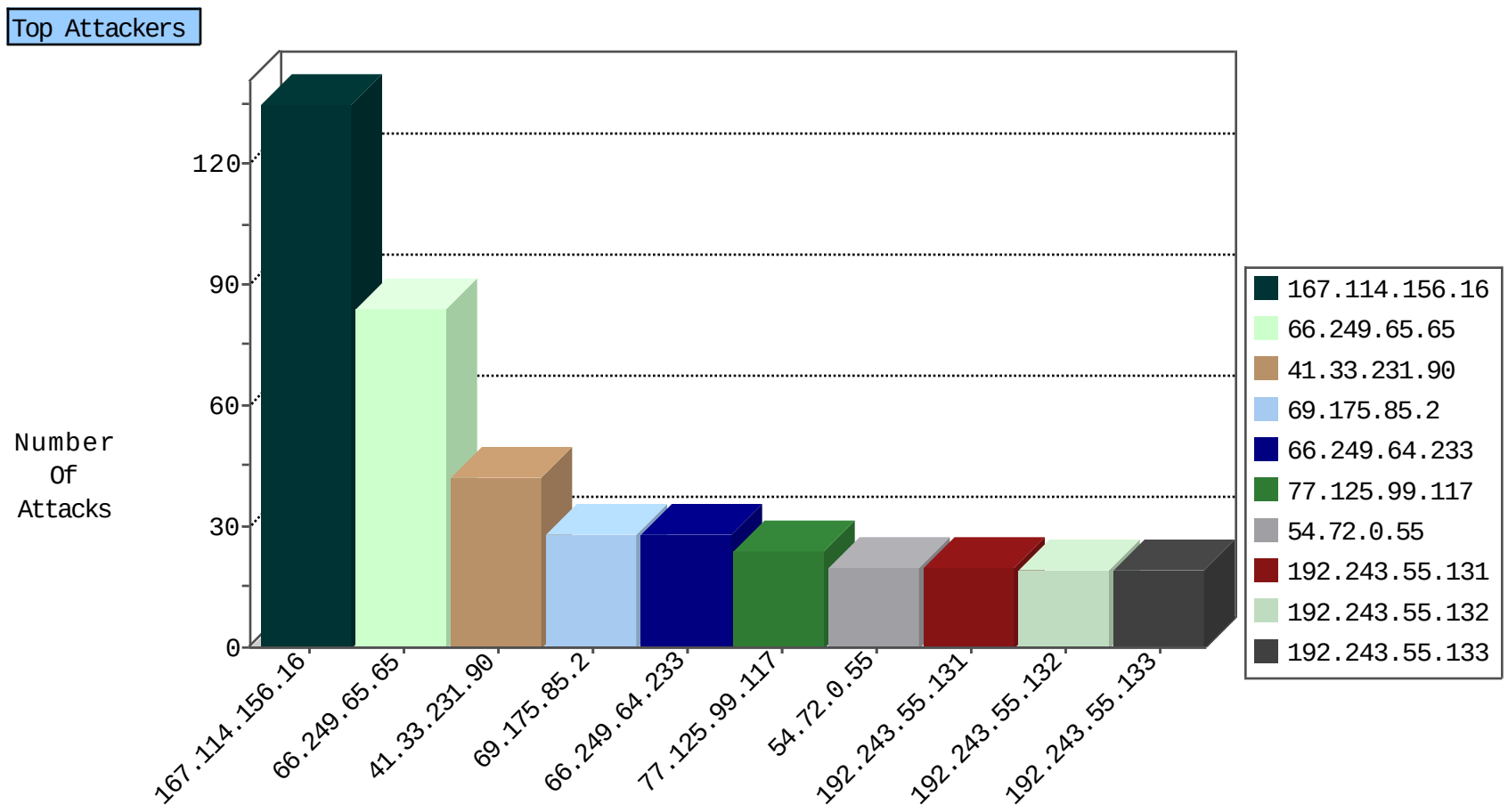
04-22-2016-05:04:04 to 04-22-2016-06:04:04

# IDF Under Attack Daily Report

Top Targets




Top Attackers



04-22-2016-05:04:04 to 04-22-2016-06:04:04

## 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 | HTTP-POST-Segmented-DoS | dest-reset | 9380 |
| 167.114.156.16 | Canada | 147.237.77.216 | dover.idf.il | DOS-Tool-SwitchbladG | dest-reset | 4 |
| 120.132.50.135 | China | 147.237.76.147 | chinuch.aka.idf.il | block-sp-traf1 | forward | 4 |
| 204.42.253.2 | United States | 147.237.76.42 | refuah.idf.il | Block_Ntp_All_Net | drop | 2 |
| 204.42.253.2 | United States | 147.237.76.44 | e.refuah.idf.il | Block_Ntp_All_Net | drop | 2 |
| 142.0.41.223 | United States | 147.237.76.199 | e.nakchal.idf.il | Block_Udp_All_Nets | drop | 1 |
| 185.94.111.1 | Russian Federation | 147.237.76.39 | mobile.meitav.idf.il | Block_Udp_All_Nets | drop | 1 |
| 142.0.41.223 | United States | 147.237.76.196 | e.sviva.idf.il | Block_Udp_All_Nets | drop | 1 |
| 85.25.43.94 | Germany | 147.237.76.199 | e.nakchal.idf.il | Block_Ntp_All_Net | drop | 1 |
| 192.243.55.136 | United States | 147.237.77.74 | law.idf.il | TCP handshake violation, first packet not syn | drop | 1 |
| 142.0.41.223 | United States | 147.237.76.197 | e.himush.idf.il | Block_Udp_All_Nets | drop | 1 |
| 91.217.164.102 | France | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 1 |
| 142.0.41.223 | United States | 147.237.76.198 | e.yohalan.idf.il | Block_Udp_All_Nets | drop | 1 |
| 185.94.111.1 | Russian Federation | 147.237.76.38 | e.e.meitav.idf.il | Block_Udp_All_Nets | drop | 1 |

04-22-2016-05:04:04 to 04-22-2016-06:04:04

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|

04-22-2016-05:04:04 to 04-22-2016-06:04:04

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 |
| 41.33.231.90 | 147.237.77.216 | Egypt | dover.idf.il | Tehila - Perl LWP with fake user agent | 2 |
| 69.175.85.2 | 147.237.76.31 | United States | nakchal.idf.il | ET SCAN Potential SSH Scan | 2 |
| 40.114.42.13 | 147.237.76.86 | United States | navy.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 104.43.14.234 | 147.237.0.19 | United States | madim.atal.idf.i | ET SCAN Potential SSH Scan | 1 |
| 81.169.171.4 | 147.237.76.42 | Germany | refuah.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 69.175.85.2 | 147.237.76.42 | United States | refuah.idf.il | ET SCAN Potential SSH Scan | 1 |
| 46.225.116.166 | 147.237.0.19 | Iran, Islamic Republic of | madim.atal.idf.i | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |
| 40.114.42.13 | 147.237.76.86 | United States | navy.idf.il | ET SCAN Potential SSH Scan | 1 |
| 212.129.15.245 | 147.237.72.217 | France | e.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 175.253.55.199 | 147.237.0.34 | Korea, Republic of | tikshuv.idf.il | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |
| 81.169.171.4 | 147.237.76.42 | Germany | refuah.idf.il | ET SCAN NMAP -sS window 3072 | 1 |
| 80.82.78.38 | 147.237.77.227 | Netherlands | e.hamaz.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 69.175.85.2 | 147.237.76.38 | United States | e.e.meitav.idf.i | ET SCAN NMAP -sS window 1024 | 1 |
| 69.175.85.2 | 147.237.76.30 | United States | himush.idf.il | ET SCAN Rapid POP3 Connections - Possible Brute Force Attack | 1 |

04-22-2016-05:04:04 to 04-22-2016-06:04:04

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 66.249.65.65 | United States | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 78 |
| 77.125.99.117 | Israel | 147.237.76.200 | eitan.aka.idf.i | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 24 |
| 41.33.231.90 | Egypt | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 22 |
| 54.72.0.55 | Ireland | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 20 |
| 41.33.231.90 | Egypt | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 18 |
| 2.53.129.191 | Israel | 147.237.76.200 | eitan.aka.idf.i | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 12 |
| 52.29.223.39 | Germany | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 12 |
| 192.243.55.138 | United States | 147.237.77.74 | law.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 7 |
| 68.180.231.43 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 7 |
| 192.243.55.131 | United States | 147.237.77.74 | law.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 50.87.144.145 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 6 |
| 54.72.73.168 | Ireland | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 6 |
| 50.116.30.23 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 6 |
| 213.151.32.163 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 192.243.55.137 | United States | 147.237.77.74 | law.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 6 |
| 66.249.64.233 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 5 |
| 192.243.55.135 | United States | 147.237.77.74 | law.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 5 |
| 209.37.96.5 | United States | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 5 |
| 192.243.55.133 | United States | 147.237.77.74 | law.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 5 |
| 212.143.142.56 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 5 |
| 192.243.55.132 | United States | 147.237.77.74 | law.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 5 |
| 192.243.55.136 | United States | 147.237.77.74 | law.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 5 |
| 192.243.55.129 | United States | 147.237.77.74 | law.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 4 |
| 192.243.55.132 | United States | 147.237.77.74 | law.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 192.243.55.129 | United States | 147.237.77.74 | law.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 4 |
| 192.243.55.137 | United States | 147.237.77.74 | law.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 192.243.55.132 | United States | 147.237.77.74 | law.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 4 |
| 192.243.55.130 | United States | 147.237.77.74 | law.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 4 |
| 192.243.55.129 | United States | 147.237.77.74 | law.idf.il | drop | First packet isn't SYN | drop | 4 |
| 91.217.164.102 | France | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 4 |
| 192.243.55.131 | United States | 147.237.77.74 | law.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 4 |
| 192.243.55.131 | United States | 147.237.77.74 | law.idf.il | drop | First packet isn't SYN | drop | 4 |
| 192.243.55.132 | United States | 147.237.77.74 | law.idf.il | drop | First packet isn't SYN | drop | 4 |
| 192.243.55.137 | United States | 147.237.77.74 | law.idf.il | drop | First packet isn't SYN | drop | 4 |
| 130.193.51.91 | Russian Federation | 147.237.76.200 | eitan.aka.idf.i | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 192.243.55.130 | United States | 147.237.77.74 | law.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 3 |
| 141.8.142.1 | Russian Federation | 147.237.76.200 | eitan.aka.idf.i | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 192.243.55.133 | United States | 147.237.77.74 | law.idf.il | Bad TCP sequence | Invalid ACK number | alert | 3 |
| 192.243.55.131 | United States | 147.237.77.74 | law.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 3 |
| 2.53.153.169 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 66.102.8.200 | United States | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 192.243.55.137 | United States | 147.237.77.74 | law.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 3 |
| 91.223.89.57 | Ukraine | 147.237.77.233 | atal.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 3 |
| 192.243.55.133 | United States | 147.237.77.74 | law.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 3 |
| 69.175.85.2 | United States | 147.237.76.44 | e.refuah.idf.il | Geo-location enforcement | Geo-location inbound enforcement | drop | 3 |
| 192.243.55.131 | United States | 147.237.77.74 | law.idf.il | Bad TCP sequence | Invalid ACK number | alert | 3 |
| 205.197.242.163 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 3 |
| 192.243.55.129 | United States | 147.237.77.74 | law.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 3 |
| 192.243.55.133 | United States | 147.237.77.74 | law.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 3 |
| 192.243.55.132 | United States | 147.237.77.74 | law.idf.il | Bad TCP sequence | Invalid ACK number | alert | 2 |

04-22-2016-05:04:04 to 04-22-2016-06:04:04

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 66.249.64.233 | Israel | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 66.249.64.233 | Block | 21 |
| 208.115.113.88 | United States | 147.237.76.86 | navy.idf.il | Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp | Block | 7 |
| 178.137.93.24 | Ukraine | 147.237.77.74 | law.idf.il | Multiple Unauthorized URL Access from 178.137.93.24 | Block | 3 |
| 208.115.113.88 | United States | 147.237.76.86 | navy.idf.il | Multiple Unauthorized URL Access from 208.115.113.88 | Block | 2 |
| 192.243.55.133 | United States | 147.237.77.74 | law.idf.il | Unauthorized URL Access to www.law.idf.il/templates/getfile/getfile.aspx?filename=xgf5b3nolwrvy3ncdghpa2fcdhphdmltxdewodcuzg9j&infocenteritem=true | Block | 1 |
| 120.132.50.135 | China | 147.237.76.147 | chinuch.aka.idf.il | Unauthorized URL Access to www.qunar.com/894-he/chinuch.aspx | Block | 1 |
| 31.13.109.122 | Ireland | 147.237.77.176 | matpash.idf.il | Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/5/2925.pdf&ved=0ahukewj71oi6mahmahxkirokhuwdbl8qfgggmaq&usg=afqjcnhwuwsjdnhthbcvmghjp8hlmvvxgq&sig2=5g2-ii-b2_k8ug7m4jx35g | Block | 1 |
| 178.137.93.24 | Ukraine | 147.237.77.74 | law.idf.il | PHP Attempt | Block | 1 |
| 91.223.89.57 | Ukraine | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to 147.237.77.233/ | Block | 1 |
| 203.219.157.44 | Australia | 147.237.72.166 | aka.idf.il | Illegal Byte Code Character in URL /main/giyus/[[#11]]general.aspx | Block | 1 |
| 145.255.1.48 | Russian Federation | 147.237.0.34 | tikshuv.idf.il | Parameter Type Violation catId in www.tikshuv.idf.il/site/faq.aspx | Block | 1 |
| 66.249.64.108 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to 147.237.77.216/ | Block | 1 |
| 178.137.93.24 | Ukraine | 147.237.77.74 | law.idf.il | Unauthorized URL Access to www.law.idf.il/xmlrpc.php | Block | 1 |
| 91.223.89.57 | Ukraine | 147.237.77.235 | sviva.idf.il | Unauthorized URL Access to www.hagnas.atal.idf.il/hnap1/ | Block | 1 |
| 207.46.13.144 | United States | 147.237.77.233 | atal.idf.il | Distributed Unauthorized URL Access on 147.237.77.233/ | Block | 1 |
| 157.55.39.77 | United States | 147.237.77.74 | law.idf.il | Unauthorized URL Access to www.law.idf.il/templates/templatecontrols/news/sip_storage/files/6/1446.pdf/ | Block | 1 |
| 66.249.64.159 | Israel | 147.237.77.74 | law.idf.il | Unauthorized URL Access to www.mag.idf.il/993/patzar.aspx | Block | 1 |
| 184.105.139.67 | United States | 147.237.0.17 | m.my-kosher-kravi.idf.il | Unauthorized URL Access to 147.237.0.17/ | Block | 1 |
| 93.160.60.22 | Denmark | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/newsite/english | Block | 1 |
| 157.55.39.194 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx | Block | 1 |
| 66.249.64.181 | Israel | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to www.atal.idf.il/1413-he/אגף הטכנולוגיה וה לוגיסטיקה.aspx | Block | 1 |
| 192.243.55.130 | United States | 147.237.77.74 | law.idf.il | Unauthorized URL Access to www.law.idf.il/templates/getfile/getfile.aspx?filename=xhllytaxltawms5kb2m=&infocenteritem=true | Block | 1 |
| 107.133.32.146 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx | Block | 1 |

04-22-2016-05:04:04 to 04-22-2016-06:04:04