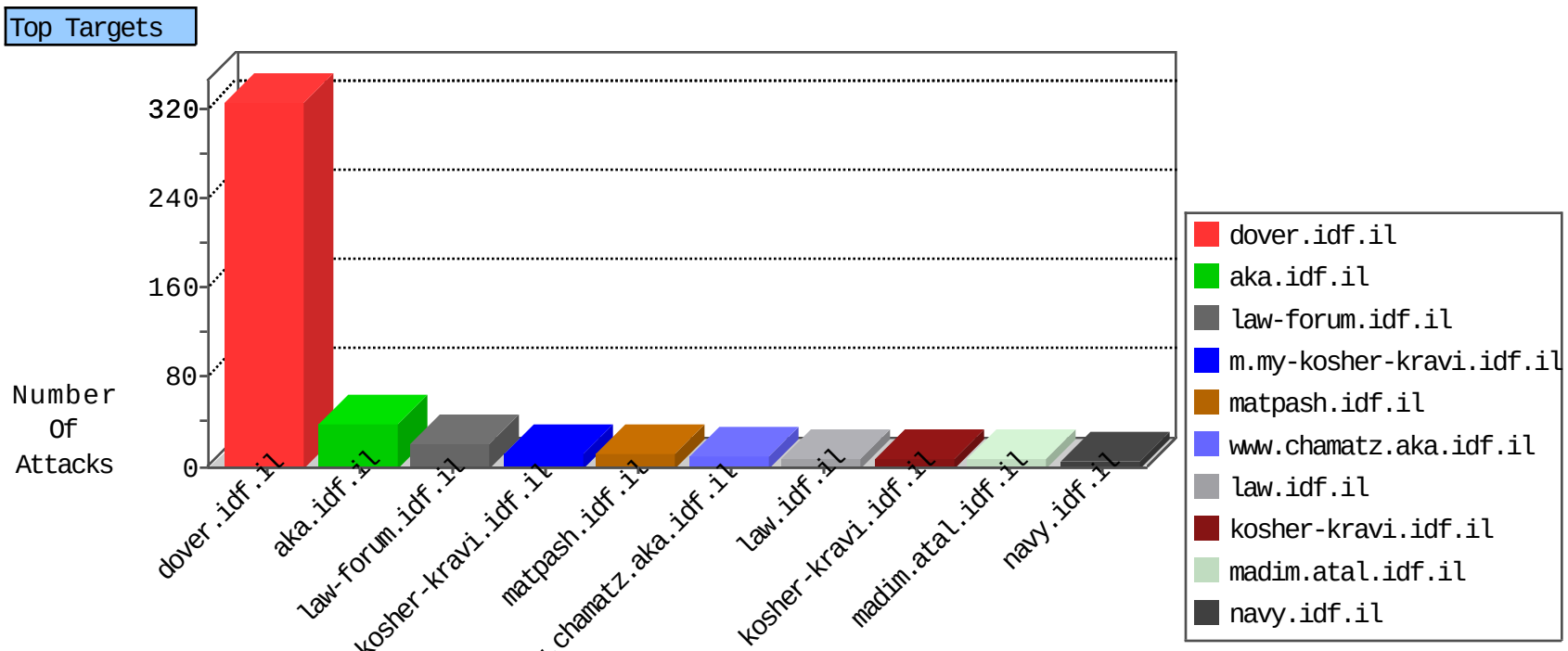
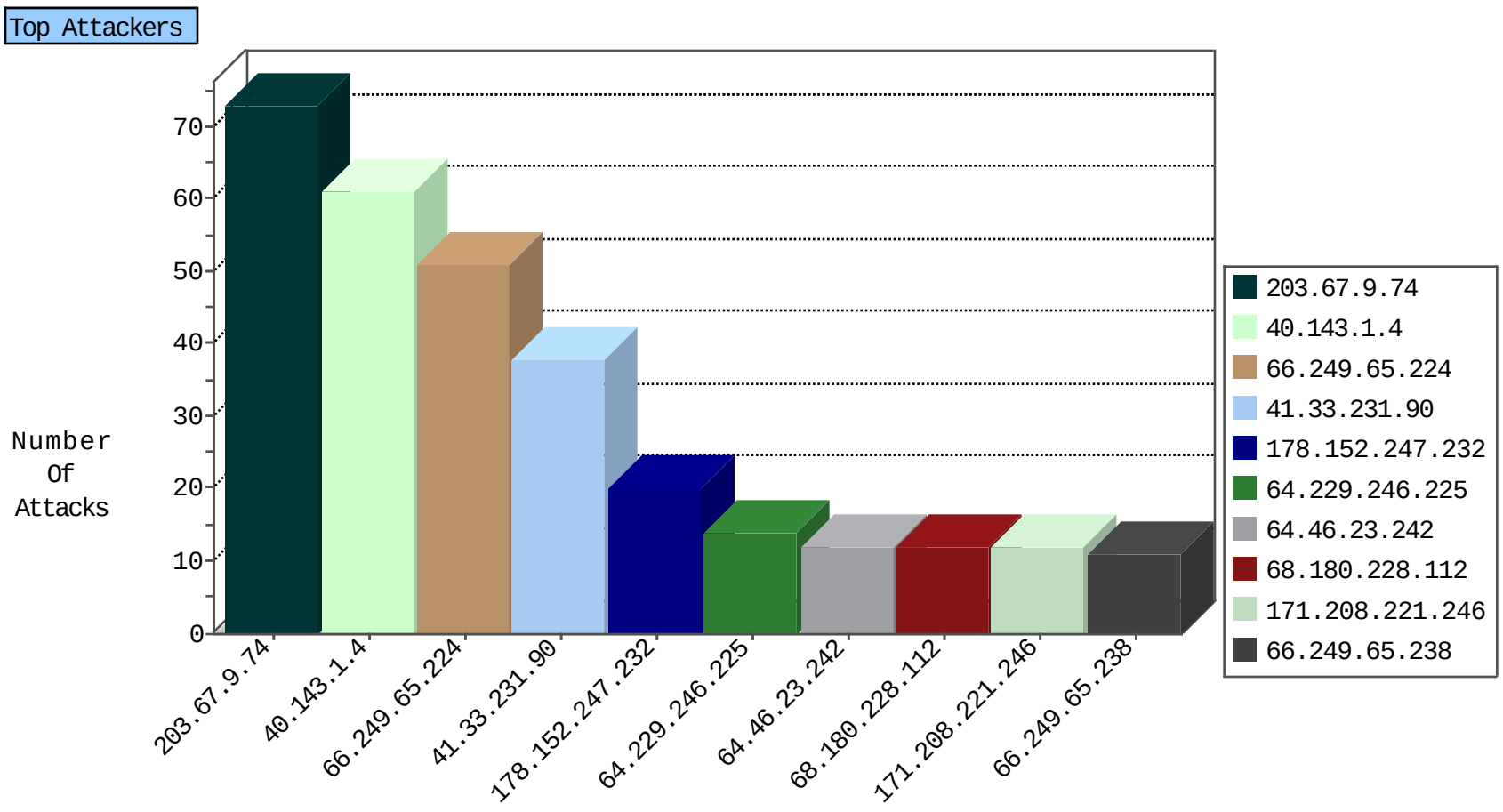
11-21-2015-06:04:03 to 11-21-2015-07:04:03

# IDF Under Attack Daily Report

Top Targets




Top Attackers



11-21-2015-06:04:03 to 11-21-2015-07:04:03

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 121.54.32.170 | Philippines | 147.237.77.216 | dover.idf.il | TCP handshake violation, first packet not syn | drop | 1 |
| 167.114.156.16 | Canada | 147.237.77.216 | dover.idf.il | DOS-Tool-SwitchbladG | dest-reset | 1 |
| 67.128.38.64 | United States | 147.237.76.86 | navy.idf.il | Block_Ntp_All_Net | drop | 1 |

11-21-2015-06:04:03 to 11-21-2015-07:04:03

## Top Attackers In IPS

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

11-21-2015-06:04:03 to 11-21-2015-07:04:03

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 |
| 185.106.94.66 | 147.237.76.197 | | e.himush.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 91.201.236.113 | 147.237.77.226 | Ukraine | www.chamatz.aka.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 185.106.94.66 | 147.237.76.147 | | chinuch.aka.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 65.255.43.24 | 147.237.0.35 | United States | akaws.idf.il | ET SCAN NMAP -sS window 4096 | 1 |
| 122.157.228.232 | 147.237.0.35 | China | akaws.idf.il | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |
| 122.114.17.100 | 147.237.0.34 | China | tikshuv.idf.il | ET SCAN Potential SSH Scan | 1 |
| 122.114.17.100 | 147.237.0.19 | China | madim.atal.idf.il | ET SCAN Potential SSH Scan | 1 |
| 122.114.17.100 | 147.237.0.16 | China | my-kosher-kravi.idf.il | ET SCAN Potential SSH Scan | 1 |
| 121.27.152.52 | 147.237.0.17 | China | m.my-kosher-kravi.idf.il | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |
| 222.218.64.161 | 147.237.0.17 | China | m.my-kosher-kravi.idf.il | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |
| 111.93.198.54 | 147.237.77.243 | India | mobile.idf.il | ET SCAN NMAP -f -sS | 1 |
| 91.201.236.114 | 147.237.76.147 | Ukraine | chinuch.aka.idf.il | ET DROP Spamhaus DROP Listed Traffic Inbound | 1 |
| 185.106.94.66 | 147.237.76.196 | | e.sviva.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 91.201.236.113 | 147.237.77.226 | Ukraine | www.chamatz.aka.idf.il | ET DROP Spamhaus DROP Listed Traffic Inbound | 1 |
| 185.106.94.66 | 147.237.0.15 | | kosher-kravi.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 5.39.222.253 | 147.237.76.42 | Netherlands | refuah.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 122.114.17.100 | 147.237.0.200 | China | m4u.idf.il | ET SCAN Potential SSH Scan | 1 |
| 122.114.17.100 | 147.237.0.33 | China | idf.il | ET SCAN Potential SSH Scan | 1 |
| 122.114.17.100 | 147.237.0.17 | China | m.my-kosher-kravi.idf.il | ET SCAN Potential SSH Scan | 1 |
| 122.114.17.100 | 147.237.0.15 | China | kosher-kravi.idf.il | ET SCAN Potential SSH Scan | 1 |
| 111.93.198.54 | 147.237.77.243 | India | mobile.idf.il | ET SCAN NMAP -sS window 2048 | 1 |
| 203.67.9.74 | 147.237.72.156 | Taiwan | aman.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 91.201.236.114 | 147.237.76.147 | Ukraine | chinuch.aka.idf.il | ET SCAN NMAP -sS window 1024 | 1 |

11-21-2015-06:04:03 to 11-21-2015-07:04:03

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 66.249.65.224 | United States | 147.237.77.216 | dover.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 34 |
| 41.33.231.90 | Egypt | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 33 |
| 64.229.246.225 | Canada | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 14 |
| 178.152.247.232 | Qatar | 147.237.77.19 | law-forum.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 13 |
| 64.46.23.242 | Canada | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 12 |
| 68.180.228.112 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 10 |
| 54.72.0.55 | Ireland | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 10 |
| 207.241.229.193 | United States | 147.237.72.166 | aka.idf.il | Web Server Enforcement Violation | Web Servers Slow HTTP Denial of Service | reject | 10 |
| 69.175.127.10 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 8 |
| 40.143.1.4 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 8 |
| 54.244.22.103 | United States | 147.237.77.176 | matpash.idf.il | drop | First packet isn't SYN | drop | 7 |
| 66.249.65.238 | United States | 147.237.77.216 | dover.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 207.46.13.160 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 6 |
| 5.22.134.76 | Israel | 147.237.77.216 | dover.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 52.16.5.197 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 6 |
| 209.133.111.211 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 5 |
| 67.186.14.201 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 5 |
| 66.249.65.224 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 4 |
| 109.67.130.253 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 4 |
| 66.249.67.13 | United States | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 4 |
| 65.19.138.34 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 4 |
| 98.113.149.163 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 4 |
| 188.120.148.238 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 3 |
| 208.115.113.89 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 3 |
| 37.8.24.10 | Palestinian Territory, Occupied | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 3 |
| 197.35.82.249 | Egypt | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 3 |
| 79.178.53.31 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 121.54.32.170 | Philippines | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 3 |
| 41.33.231.90 | Egypt | 147.237.77.216 | dover.idf.il | drop | | drop | 3 |
| 203.67.9.74 | Taiwan | 147.237.76.197 | e.himush.idf.il | Geo-location enforcement | Geo-location inbound enforcement | drop | 2 |
| 141.212.122.80 | United States | 147.237.0.15 | kosher-kravi.idf.il | drop | SAM rule | drop | 2 |
| 203.67.9.74 | Taiwan | 147.237.76.34 | yohalan.idf.il | drop | | drop | 2 |
| 41.33.231.90 | Egypt | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 2 |
| 82.192.68.46 | Netherlands | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 2 |
| 203.67.9.74 | Taiwan | 147.237.76.202 | e.halag.idf.il | Geo-location enforcement | Geo-location inbound enforcement | drop | 2 |
| 203.67.9.74 | Taiwan | 147.237.72.167 | ishurim.aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 2 |
| 157.55.39.168 | United States | 147.237.76.200 | eitan.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 2 |
| 66.249.67.6 | United States | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 2 |
| 203.67.9.74 | Taiwan | 147.237.76.198 | e.yohalan.idf.il | Geo-location enforcement | Geo-location inbound enforcement | drop | 2 |
| 203.67.9.74 | Taiwan | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 2 |
| 203.67.9.74 | Taiwan | 147.237.0.17 | m.my-kosher-kravi.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 2 |
| 188.138.17.205 | France | 147.237.76.176 | test.ncore.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 2 |
| 203.67.9.74 | Taiwan | 147.237.76.148 | gqcenter.aka.idf.il | drop | | drop | 2 |
| 54.72.73.168 | Ireland | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 2 |
| 115.31.176.2 | Thailand | 147.237.77.74 | law.idf.il | drop | First packet isn't SYN | drop | 2 |
| 203.67.9.74 | Taiwan | 147.237.0.200 | m4u.idf.il | Geo-location enforcement | Geo-location inbound enforcement | drop | 2 |
| 203.67.9.74 | Taiwan | 147.237.77.176 | matpash.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 2 |
| 199.16.156.126 | United States | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 2 |
| 46.19.85.90 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 2 |
| 72.9.148.10 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 2 |

11-21-2015-06:04:03 to 11-21-2015-07:04:03

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 40.143.1.4 | United States | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 40.143.1.4 | Block | 36 |
| 40.143.1.4 | United States | 147.237.77.216 | dover.idf.il | Distributed PHP Attempt | Block | 17 |
| 66.249.65.224 | Israel | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 66.249.65.224 | Block | 10 |
| 176.13.22.104 | Israel | 147.237.0.17 | m.my-kosher-kravi .idf.il | Multiple Illegal Parameter Encoding from 176.13.22.104 | None | 3 |
| 66.249.65.224 | Israel | 147.237.77.216 | dover.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 198.1.101.123 | United States | 147.237.77.216 | dover.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 66.249.65.238 | Israel | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 66.249.65.238 | Block | 2 |
| 46.19.86.169 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 68.180.228.112 | United States | 147.237.77.216 | dover.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 107.178.194.83 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx. | Block | 2 |
| 176.13.13.226 | Israel | 147.237.0.17 | m.my-kosher-kravi .idf.il | Distributed Illegal Parameter Encoding | None | 2 |
| 77.40.129.123 | Norway | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx. | Block | 1 |
| 66.249.67.122 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter pop in www.aka.idf.il/main/home/ | None | 1 |
| 208.115.113.89 | United States | 147.237.77.74 | law.idf.il | Unauthorized URL Access to www.mag.idf.il/templates/templatecontrols/news/sip_storage/files/6/1446.pdf/ | Block | 1 |
| 178.152.247.232 | Qatar | 147.237.77.19 | law-forum.idf.il | Illegal Byte Code Character in Method Â‹[[#0]][[#0]][[#0]]tmÃŠÂ' jU9w[[#0]]PÃ¢Â»Â¤1Ã"3RÃ£Ã?[[#17]]Â'[[#16]]vÂ?LG*[[#29]]Ã‹EÃ' Â¸;•#OÃŸÃ¦Âƒ+Â„Ã•9hÂ…ÃªÃ¼ÂªqQ,ÃŠhÃ¿QÂŸ N[[#31]]Ã¶Â¤[[#22]]}Â¬h[[#14]]Ãš[[#22]]@ÂºÂ' [[#18]]Âª[Ã¦IqÂ¨Â?Y[[#15]]Â'My/Â Â¨]v$Ã¼zÃˆ [[#22]]Â«Â¦[nUÃ¡SÃ¿[[#18]]#Ã¡)ÃŸ[[#7]]_2sÂ?^Z[[#31]]oÂˆÃ¿4[[#3]]Â—ÃŸnÃ€ÃŒG | 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 |
| 74.6.53.161 | United States | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to aka.idf.il/wp-admin/ | Block | 1 |
| 178.255.215.87 | France | 147.237.77.216 | dover.idf.il | Distributed Suspicious Response Code | Block | 1 |
| 66.249.65.238 | Israel | 147.237.77.216 | dover.idf.il | Distributed Suspicious Response Code | Block | 1 |
| 176.13.22.104 | Israel | 147.237.0.17 | m.my-kosher-kravi .idf.il | Illegal Parameter Encoding rnd in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx | None | 1 |
| 85.93.91.84 | Germany | 147.237.77.216 | dover.idf.il | Distributed Suspicious Response Code | Block | 1 |
| 66.249.67.234 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx | Block | 1 |
| 208.184.112.74 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx. | Block | 1 |
| 178.152.247.232 | Qatar | 147.237.77.19 | law-forum.idf.il | Malformed URL | Block | 1 |
| 66.249.65.230 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to 147.237.77.216/m/1361-10624-he/dover.aspx | Block | 1 |
| 141.212.122.160 | United States | 147.237.76.86 | navy.idf.il | Unauthorized URL Access to 147.237.76.86/ | Block | 1 |
| 74.6.53.162 | United States | 147.237.72.166 | aka.idf.il | Multiple Unauthorized URL Access from 74.6.53.162 | Block | 1 |
| 107.150.43.204 | United States | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to / | Block | 1 |
| 208.184.112.75 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx. | Block | 1 |
| 178.152.247.232 | Qatar | 147.237.77.19 | law-forum.idf.il | NULL Character in Method Â‹[[#0]][[#0]][[#0]]tmÃŠÂ' jU9w[[#0]]PÃ¢Â»Â¤1Ã"3RÃ£Ã?[[#17]]Â'[[#16]]vÂ?LG*[[#29]]Ã‹EÃ' Â¸;•#OÃŸÃ¦Âƒ+Â„Ã•9hÂ…ÃªÃ¼ÂªqQ,ÃŠhÃ¿QÂŸ N[[#31]]Ã¶Â¤[[#22]]}Â¬h[[#14]]Ãš[[#22]]@ÂºÂ' [[#18]]Âª[Ã¦IqÂ¨Â?Y[[#15]]Â'My/Â Â¨]v$Ã¼zÃˆ [[#22]]Â«Â¦[nUÃ¡SÃ¿[[#18]]#Ã¡)ÃŸ[[#7]]_2sÂ?^Z[[#31]]oÂˆÃ¿4[[#3]]Â—ÃŸnÃ€ÃŒG | Block | 1 |
| 66.249.65.231 | Israel | 147.237.77.216 | dover.idf.il | Distributed Suspicious Response Code | Block | 1 |
| 141.212.122.160 | United States | 147.237.77.74 | law.idf.il | Unauthorized URL Access to 147.237.77.74/ | Block | 1 |
| 74.6.53.162 | United States | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to aka.idf.il/blog/wp-admin/ | Block | 1 |
| 66.249.67.6 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 1 |
| 204.13.200.200 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx. | Block | 1 |
| 66.249.65.223 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to 147.237.77.216/1361-10635-he/dover.aspx | Block | 1 |
| 178.152.247.232 | Qatar | 147.237.77.19 | law-forum.idf.il | Abnormally Long Request method | Block | 1 |
| 74.6.53.160 | United States | 147.237.72.166 | aka.idf.il | Multiple Unauthorized URL Access from 74.6.53.160 | Block | 1 |
| 216.218.206.68 | United States | 147.237.76.39 | mobile.meitav.idf.i | Unauthorized URL Access to 147.237.76.39/ | Block | 1 |
| 178.152.247.232 | Qatar | 147.237.77.19 | law-forum.idf.il | Unauthorized URL Access to 147.237.77.19/ | Block | 1 |
| 66.249.65.231 | Israel | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 66.249.65.231 | Block | 1 |
| 24.67.204.247 | Canada | 147.237.77.216 | dover.idf.il | Parameter Type Violation SearchText in www.idf.il/1065-en/dover.aspx | Block | 1 |
| 141.212.122.160 | United States | 147.237.77.226 | www.chamatz.aka.idf.il | Unauthorized URL Access to 147.237.77.226/ | Block | 1 |
| 74.82.47.2 | United States | 147.237.0.19 | madim.atal.idf.il | Unauthorized URL Access to 147.237.0.19/ | Block | 1 |
| 66.249.67.13 | Israel | 147.237.72.166 | aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 1 |
| 204.13.200.200 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx. | Block | 1 |
| 178.152.247.232 | Qatar | 147.237.77.19 | law-forum.idf.il | Illegal Byte Code Character in Header Name | Block | 1 |
| 107.178.194.83 | United States | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx. | Block | 1 |

11-21-2015-06:04:03 to 11-21-2015-07:04:03

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 74.6.53.160 | United States | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to aka.idf.il/test/wp-admin/ | Block | 1 |
| 178.152.247.232 | Qatar | 147.237.77.19 | law-forum.idf.il | Unknown HTTP Request Method Â‹[[#0]][[#0]][[#0]]tmAÃšÂ‘ jU9w[[#0]]PÃ¢Â»Â¤1Ã“3RÃ£Ã?[[#17]]Â’[[#16]]vÂ?LG*[[#29]]Ã‹EÃ‘ Â¸;•#OÃŸÂ¦Âƒ+Â„Ã•9hÂ…ÃªÃ¼Âªq Q,ÃŠhÃ¿QÂŸ N[[#31]]Ã¶Â¤[[#22]]}Â¬h[[#14]]Ãš[[#22]]@Â°Â’ [[#18]]Âª[Ã¦IqÂ¨Â?Y[[#15]]Â’My/Â Â¨]v$Ã¼zÃˆ [[#22]]Â«Â¦[nUÃ¡SÃ¿[[#18]]#Ã¡)ÃŸ[[#7]]_2sÂ?^Z[[#31]]oÂˆÃ¿4[[#3]]Â—ÃŸnÃ€ÃŒG in URL | Block | 1 |

11-21-2015-06:04:03 to 11-21-2015-07:04:03