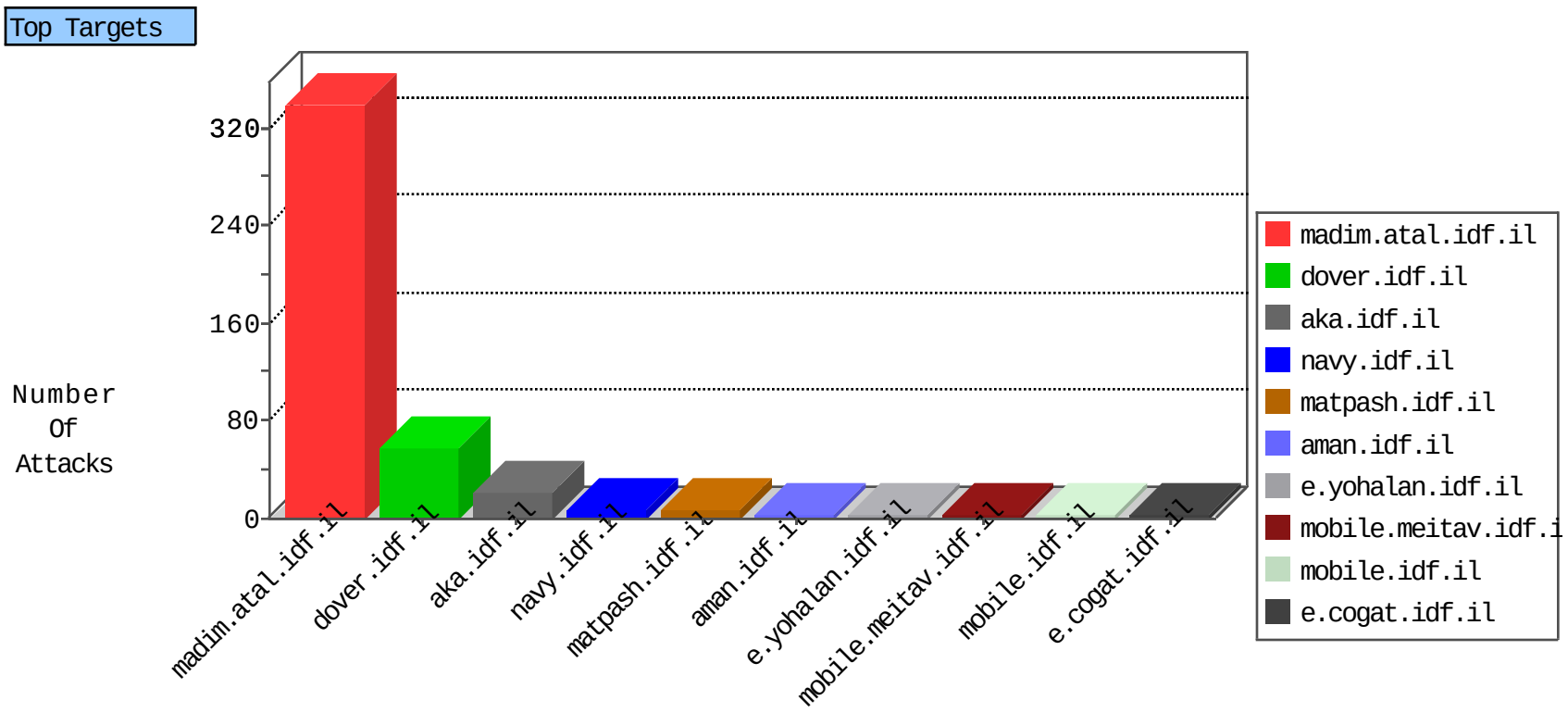
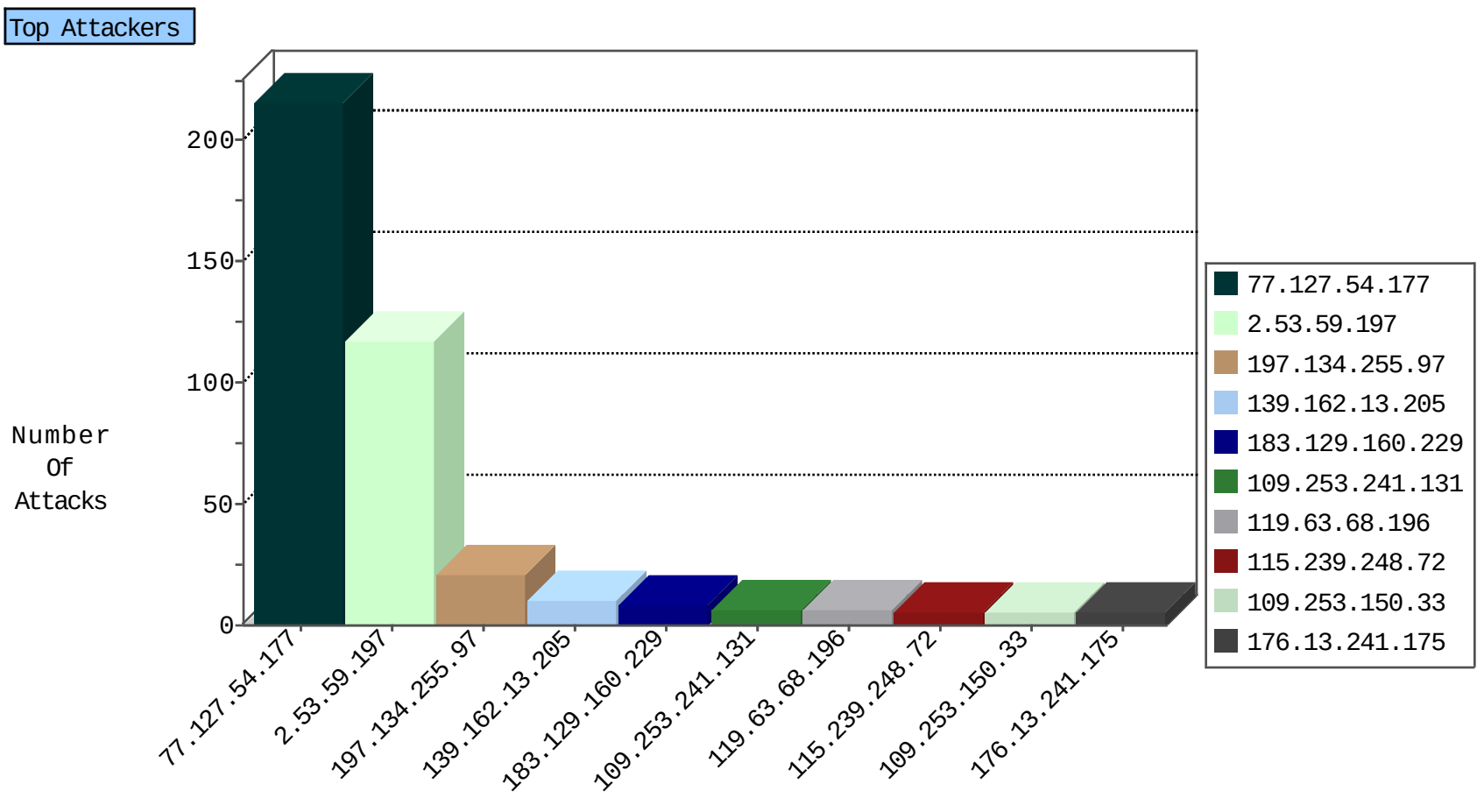
08-19-2016-19:04:02 to 08-19-2016-20:04:02

# IDF Under Attack Daily Report

Top Targets




Top Attackers



08-19-2016-19:04:02 to 08-19-2016-20:04:02

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 134.147.203.115 | Germany | 147.237.76.198 | e.yohalan.idf.il | Black List | drop | 2 |
| 134.147.203.115 | Germany | 147.237.76.200 | eitan.aka.idf.il | Black List | drop | 2 |
| 82.80.78.2 | Israel | 147.237.72.166 | aka.idf.il | Black List | drop | 2 |
| 198.20.70.114 | United States | 147.237.76.30 | himush.idf.il | Black List | drop | 1 |
| 82.80.78.2 | Israel | 147.237.77.176 | matpash.idf.il | Black List | drop | 1 |

08-19-2016-19:04:02 to 08-19-2016-20:04:02

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 68.135.8.175 | United States | 147.237.77.216 | dover.idf.il | C1000074: HTTP: majestic bot | Permit | 2 |
| 164.132.161.82 | Italy | 147.237.76.42 | refuah.idf.il | C1000146: HTTP:  AhrefBot crawler | Block | 1 |
| 66.240.219.146 | United States | 147.237.0.16 | my-kosher-kravi.idf.il | 13840: TLS: OpenSSL Heartbeat Packet | Block | 1 |

08-19-2016-19:04:02 to 08-19-2016-20:04:02

Top Attackers In IDS

| Attacker Address | Target Address | Attacker Country | Site | Signature | Count |
|---|---|---|---|---|---|
| 91.121.147.218 | 147.237.77.176 | France | matpash.idf.il | ET WEB_SERVER Fake Googlebot UA 1 Inbound | 2 |
| 91.201.236.155 | 147.237.76.39 | Ukraine | mobile.meitav.idf.il | ET SCAN NMAP -sS window 3072 | 1 |
| 183.129.160.229 | 147.237.77.233 | China | atal.idf.il | ET SCAN Potential SSH Scan | 1 |
| 91.201.236.155 | 147.237.76.39 | Ukraine | mobile.meitav.idf.il | ET DROP Spamhaus DROP Listed Traffic Inbound | 1 |
| 183.82.106.200 | 147.237.0.34 | India | tikshuv.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 90.127.61.170 | 147.237.77.227 | France | e.hamaz.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 173.208.249.35 | 147.237.76.198 | United States | e.yohalan.idf.il | ET SCAN NMAP -f -sS | 1 |
| 68.190.208.191 | 147.237.77.61 | United States | e.cogat.idf.il | ET SCAN NMAP -f -sS | 1 |
| 128.199.96.95 | 147.237.77.176 | Singapore | matpash.idf.il | ET DROP Spamhaus DROP Listed Traffic Inbound | 1 |
| 58.218.204.245 | 147.237.76.148 | China | gqcenter.aka.idf.il | ET SCAN Potential SSH Scan | 1 |
| 115.239.248.72 | 147.237.76.201 | China | e.atal.idf.il | ET SCAN Potential SSH Scan | 1 |
| 58.218.204.245 | 147.237.0.35 | China | akaws.idf.il | ET SCAN Potential SSH Scan | 1 |
| 115.239.248.72 | 147.237.76.34 | China | yohalan.idf.il | ET SCAN Potential SSH Scan | 1 |
| 46.172.71.251 | 147.237.76.42 | Ukraine | refuah.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 115.239.248.72 | 147.237.0.33 | China | idf.il | ET SCAN Potential SSH Scan | 1 |
| 2.55.131.115 | 147.237.77.216 | Israel | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 94.102.48.195 | 147.237.8.46 | Netherlands | e.chinuch.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 190.185.132.195 | 147.237.8.28 | Argentina | e.mobile-ks.idf.il | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |
| 91.201.236.155 | 147.237.76.39 | Ukraine | mobile.meitav.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 183.82.106.200 | 147.237.0.34 | India | tikshuv.idf.il | ET SCAN NMAP -sS window 4096 | 1 |
| 173.208.249.35 | 147.237.76.198 | United States | e.yohalan.idf.il | ET SCAN NMAP -sS window 2048 | 1 |
| 68.190.208.191 | 147.237.77.61 | United States | e.cogat.idf.il | ET SCAN NMAP -sS window 2048 | 1 |
| 128.199.239.94 | 147.237.77.176 | Singapore | matpash.idf.il | ET DROP Spamhaus DROP Listed Traffic Inbound | 1 |
| 66.249.64.183 | 147.237.77.216 | United States | dover.idf.il | ET SCAN NMAP -sA (2) | 1 |
| 120.26.213.39 | 147.237.76.38 | China | e.e.meitav.idf.il | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |
| 58.218.204.245 | 147.237.8.50 | China | e.tikshuv.idf.il | ET SCAN Potential SSH Scan | 1 |
| 115.239.248.72 | 147.237.76.86 | China | navy.idf.il | ET SCAN Potential SSH Scan | 1 |
| 46.227.67.169 | 147.237.0.17 | Sweden | m.my-kosher-kravi.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 115.239.248.72 | 147.237.0.200 | China | m4u.idf.il | ET SCAN Potential SSH Scan | 1 |
| 37.220.14.234 | 147.237.76.148 | United Kingdom | gqcenter.aka.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 94.102.48.195 | 147.237.8.50 | Netherlands | e.tikshuv.idf.il | ET SCAN NMAP -sS window 1024 | 1 |

08-19-2016-19:04:02 to 08-19-2016-20:04:02

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 197.134.255.97 | Egypt | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 21 |
| 119.63.68.196 | Thailand | 147.237.76.86 | navy.idf.il | drop | First packet isn't SYN | drop | 6 |
| 109.253.150.33 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 5 |
| 176.13.241.175 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 5 |
| 212.143.142.56 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 4 |
| 78.186.74.69 | Turkey | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 4 |
| 85.130.227.215 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 3 |
| 151.63.164.190 | Italy | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 3 |
| 141.0.13.253 | Norway | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 2 |
| 151.63.164.190 | Italy | 147.237.72.156 | aman.idf.il | drop | First packet isn't SYN | drop | 2 |
| 183.129.160.229 | China | 147.237.77.61 | e.cogat.idf.il | drop | SAM rule | drop | 1 |
| 183.129.160.229 | China | 147.237.77.226 | www.chamatz.aka.idf.il | drop | SAM rule | drop | 1 |
| 216.243.31.2 | United States | 147.237.0.33 | idf.il | drop | | drop | 1 |
| 183.129.160.229 | China | 147.237.77.170 | maarachot.idf.il | drop | SAM rule | drop | 1 |
| 183.129.160.229 | China | 147.237.77.227 | e.hamaz.idf.il | drop | SAM rule | drop | 1 |
| 216.243.31.2 | United States | 147.237.0.200 | m4u.idf.il | drop | | drop | 1 |
| 183.129.160.229 | China | 147.237.77.179 | e.mazi.idf.il | drop | SAM rule | drop | 1 |
| 109.253.196.95 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 1 |
| 184.105.139.107 | United States | 147.237.76.34 | yohalan.idf.il | drop | | drop | 1 |
| 45.63.126.189 | Japan | 147.237.76.148 | gqcenter.aka.idf.il | drop | | drop | 1 |
| 183.129.160.229 | China | 147.237.77.212 | e.dover.idf.il | drop | SAM rule | drop | 1 |
| 176.13.246.82 | Israel | 147.237.77.243 | mobile.idf.il | drop | First packet isn't SYN | drop | 1 |
| 183.129.160.229 | China | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 1 |

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 77.127.54.177 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 215 |
| 2.53.59.197 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 117 |
| 109.253.241.131 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 6 |
| 67.245.1.115 | United States | 147.237.77.216 | dover.idf.il | Unauthorized HTTP Method | Block | 2 |
| 204.79.180.106 | United States | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for aka.idf.il/miluim/templates/inner.asp | Block | 1 |
| 37.142.73.78 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 139.162.13.205 | Singapore | 147.237.77.216 | dover.idf.il | Malformed URL | Block | 1 |
| 84.95.208.20 | Israel | 147.237.77.74 | law.idf.il | Unauthorized URL Access to www.law.idf.il/templates/homepage/piwik.php | Block | 1 |
| 139.162.13.205 | Singapore | 147.237.77.216 | dover.idf.il | Unknown HTTP Request Method [[#0]œ[[#0]][[#1]][[#26]]+<M[[#0]][[#1]][[#0]][[#0]][[#1]][[#0]][[#0]][[#0]][[#0]][[#0]][[#0]][[#1]][[#0]][[#0]] in URL | Block | 1 |
| 139.162.13.205 | Singapore | 147.237.76.86 | navy.idf.il | SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO) | None | 1 |
| 77.138.96.199 | France | 147.237.77.233 | atal.idf.il | Unauthorized URL Access to 147.237.77.233/favicon.ico | Block | 1 |
| 207.46.13.9 | United States | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to 147.237.72.166/robots.txt | Block | 1 |
| 38.81.65.42 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to 147.237.77.216/robots.txt | Block | 1 |
| 139.162.13.205 | Singapore | 147.237.77.216 | dover.idf.il | Multiple Illegal Byte Code Character in Method from 139.162.13.205 | Block | 1 |
| 84.109.202.86 | Israel | 147.237.76.31 | nakchal.idf.il | Unauthorized URL Access to 147.237.76.31/894-he/nakhal.aspx | Block | 1 |
| 67.245.1.115 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/1133-22232-he/ | Block | 1 |
| 165.183.168.14 | Chile | 147.237.77.176 | matpash.idf.il | Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/4/ | Block | 1 |
| 139.162.13.205 | Singapore | 147.237.77.216 | dover.idf.il | Abnormally Long Request method | Block | 1 |
| 77.138.238.48 | France | 147.237.72.156 | aman.idf.il | Distributed Unauthorized URL Access on www.aman.idf.il/favicon.ico | Block | 1 |
| 208.115.111.73 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/atal1/izkor/main.asp | Block | 1 |
| 46.117.121.13 | Israel | 147.237.72.156 | aman.idf.il | SSL Untraceable Connection - Open Mode | None | 1 |
| 139.162.13.205 | Singapore | 147.237.77.216 | dover.idf.il | Multiple NULL Character in Method from 139.162.13.205 | Block | 1 |
| 87.68.58.248 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/templates/templatecontrols/generic/ | Block | 1 |
| 176.13.7.74 | Israel | 147.237.77.234 | halag.idf.il | Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif | Block | 1 |
| 139.162.13.205 | Singapore | 147.237.77.216 | dover.idf.il | Illegal Byte Code Character in Header Name | Block | 1 |
| 77.139.14.255 | France | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for www.aka.idf.il/main/giyus/booklets.aspx | Block | 1 |
| 208.115.113.89 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/894-he | Block | 1 |
| 66.249.79.141 | Israel | 147.237.77.243 | mobile.idf.il | Unauthorized URL Access to mobile.idf.il/.well-known/apple-app-site-association | Block | 1 |
| 139.162.13.205 | Singapore | 147.237.77.216 | dover.idf.il | NULL Character in Header Name at | Block | 1 |
| 77.127.54.177 | Israel | 147.237.77.243 | mobile.idf.il | Distributed Suspicious Response Code | Block | 1 |
| 37.46.41.121 | Israel | 147.237.0.19 | madim.atal.idf.i | Distributed Suspicious Response Code | Block | 1 |
| 199.30.17.51 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/error.htm | Block | 1 |
| 139.162.13.205 | Singapore | 147.237.77.216 | dover.idf.il | Illegal Byte Code Character in Method [[#0]œ[[#0]][[#1]][[#26]]+<M[[#0]][[#1]][[#0]][[#0]][[#1]][[#0]][[#0]][[#0]][[#0]][[#0]][[#0]][[#1]][[#0]][[#0]] | Block | 1 |
| 84.95.208.20 | Israel | 147.237.77.74 | law.idf.il | PHP Attempt | Block | 1 |
| 67.245.1.115 | United States | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 67.245.1.115 | Block | 1 |
| 139.162.13.205 | Singapore | 147.237.77.216 | dover.idf.il | NULL Character in Method [[#0]œ[[#0]][[#1]][[#26]]+<M[[#0]][[#1]][[#0]][[#0]][[#1]][[#0]][[#0]][[#0]][[#0]][[#0]][[#0]][[#1]][[#0]][[#0]] | Block | 1 |
| 128.199.96.95 | Singapore | 147.237.77.176 | matpash.idf.il | Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/4/#99 | Block | 1 |
| 77.138.69.112 | France | 147.237.72.166 | aka.idf.il | Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx | Block | 1 |