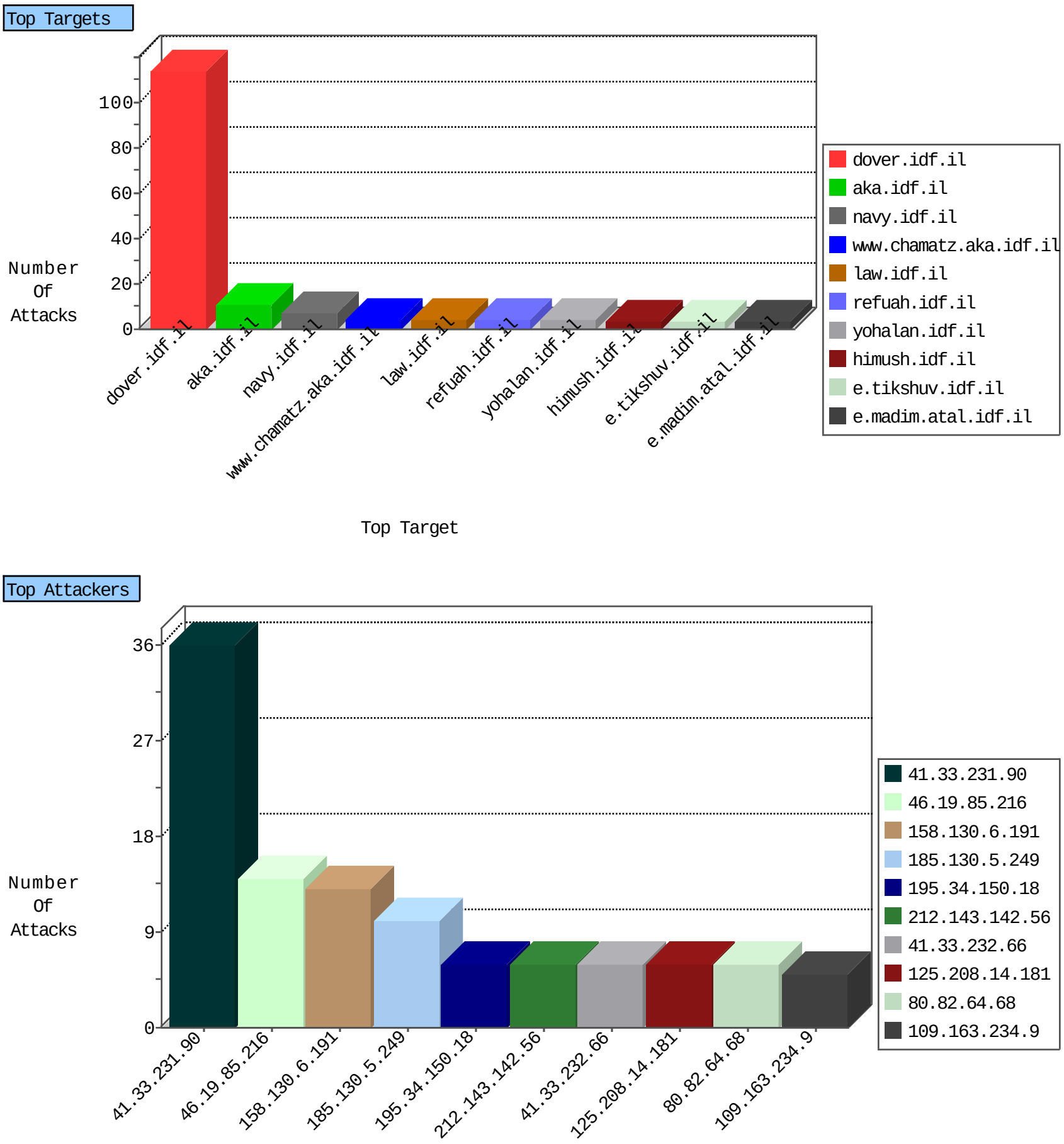
02-11-2016-03:04:09 to 02-11-2016-04:04:09

# IDF Under Attack Daily Report



02-11-2016-03:04:09 to 02-11-2016-04:04:09

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 151.80.230.228 | Italy | 147.237.76.201 | e.atal.idf.il | Block_Ntp_All_Net | drop | 1 |

02-11-2016-03:04:09 to 02-11-2016-04:04:09

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 188.165.15.132 | France | 147.237.72.166 | aka.idf.il | C228: HTTP:  AhrefBot crawler | Block | 1 |
| 195.10.212.190 | Netherlands | 147.237.77.216 | dover.idf.i | 16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability | Block | 1 |

02-11-2016-03:04:09 to 02-11-2016-04:04:09

## 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 | 2 |
| 185.130.5.249 | 147.237.76.176 | | test.ncore.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 149.210.216.68 | 147.237.8.46 | Netherlands | e.chinuch.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 125.208.14.181 | 147.237.8.46 | China | e.chinuch.idf.il | ET SCAN Potential SSH Scan | 1 |
| 125.208.14.181 | 147.237.8.27 | China | e.madim.atal.idf.il | ET SCAN Potential SSH Scan | 1 |
| 125.208.14.181 | 147.237.8.14 | China | e.orchot.idf.il | ET SCAN Potential SSH Scan | 1 |
| 185.130.5.249 | 147.237.76.177 | | ncore.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 185.130.5.249 | 147.237.8.50 | | e.tikshuv.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 125.208.14.181 | 147.237.8.50 | China | e.tikshuv.idf.il | ET SCAN Potential SSH Scan | 1 |
| 125.208.14.181 | 147.237.8.45 | China | e.eitan.idf.il | ET SCAN Potential SSH Scan | 1 |
| 125.208.14.181 | 147.237.8.24 | China | e.lifestyle.idf.il | ET SCAN Potential SSH Scan | 1 |
| 114.215.150.44 | 147.237.77.212 | China | e.dover.idf.il | ET SCAN NMAP -sS window 1024 | 1 |

02-11-2016-03:04:09 to 02-11-2016-04:04:09

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 41.33.231.90 | Egypt | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 36 |
| 46.19.85.216 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 6 |
| 41.33.232.66 | Egypt | 147.237.77.216 | dover.idf.il | Block HTTP Non Compliant | Failed to handle connection data | monitor | 6 |
| 212.143.142.56 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 6 |
| 46.19.85.216 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 6 |
| 141.0.14.19 | Europe | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 4 |
| 195.34.150.18 | Austria | 147.237.77.216 | dover.idf.il | Block HTTP Non Compliant | Failed to handle connection data | monitor | 4 |
| 80.82.64.68 | Netherlands | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Segment Limit Enforcement | TCP segment out of maximum allowed sequence. Packet dropped. | drop | 3 |
| 176.10.104.240 | Switzerland | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 2 |
| 84.108.116.200 | Israel | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 2 |
| 188.40.50.75 | Germany | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 2 |
| 142.4.213.25 | Canada | 147.237.77.216 | dover.idf.il | Directory Traversal | directory traversal overflow | monitor | 1 |
| 212.83.40.238 | Germany | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 1 |
| 141.212.122.194 | United States | 147.237.77.226 | www.chamatz.aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 1 |
| 185.130.5.249 | | 147.237.76.199 | e.nakchal.idf.il | drop | SAM rule | drop | 1 |
| 131.253.26.237 | United States | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 1 |
| 158.130.6.191 | United States | 147.237.77.227 | e.hamaz.idf.il | Geo-location enforcement | Geo-location inbound enforcement | drop | 1 |
| 5.79.68.161 | Netherlands | 147.237.77.216 | dover.idf.il | Directory Traversal | directory traversal overflow | monitor | 1 |
| 94.242.246.23 | Luxembourg | 147.237.77.216 | dover.idf.il | Directory Traversal | directory traversal overflow | monitor | 1 |
| 158.130.6.191 | United States | 147.237.76.30 | himush.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 1 |
| 74.82.47.38 | United States | 147.237.76.197 | e.himush.idf.il | Geo-location enforcement | Geo-location inbound enforcement | drop | 1 |
| 141.212.122.198 | United States | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 1 |
| 195.62.53.168 | Russian Federation | 147.237.77.226 | www.chamatz.aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 1 |
| 141.212.122.193 | United States | 147.237.0.33 | idf.il | drop | | drop | 1 |
| 185.130.5.249 | | 147.237.8.28 | e.mobile-ks.idf.il | drop | SAM rule | drop | 1 |
| 109.163.234.9 | Romania | 147.237.77.216 | dover.idf.il | drop | Unexpected post SYN packet - RST or SYN expected | drop | 1 |
| 158.130.6.191 | United States | 147.237.76.148 | gqcenter.aka.idf.il | drop | | drop | 1 |
| 84.108.116.200 | Israel | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | Invalid ACK number | alert | 1 |
| 149.78.154.69 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 1 |
| 141.212.122.195 | United States | 147.237.76.196 | e.sviva.idf.il | Geo-location enforcement | Geo-location inbound enforcement | drop | 1 |
| 185.130.5.249 | | 147.237.76.200 | eitan.aka.idf.il | drop | SAM rule | drop | 1 |
| 31.210.187.182 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 1 |
| 131.253.26.250 | United States | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 1 |
| 158.130.6.191 | United States | 147.237.76.34 | yohalan.idf.il | drop | | drop | 1 |
| 109.65.179.212 | Israel | 147.237.77.226 | www.chamatz.aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 1 |
| 77.247.181.162 | Netherlands | 147.237.77.216 | dover.idf.il | Directory Traversal | directory traversal overflow | monitor | 1 |
| 141.212.122.198 | United States | 147.237.76.198 | e.yohalan.idf.il | Geo-location enforcement | Geo-location inbound enforcement | drop | 1 |
| 197.231.221.211 | Liberia | 147.237.77.216 | dover.idf.il | Directory Traversal | directory traversal overflow | monitor | 1 |
| 41.82.126.138 | Senegal | 147.237.77.216 | dover.idf.il | Header Rejection | header rejection pattern found in request | monitor | 1 |
| 141.212.122.193 | United States | 147.237.76.34 | yohalan.idf.il | drop | | drop | 1 |
| 185.130.5.249 | | 147.237.8.50 | e.tikshuv.idf.il | drop | SAM rule | drop | 1 |
| 109.163.234.9 | Romania | 147.237.77.216 | dover.idf.il | Directory Traversal | directory traversal overflow | monitor | 1 |
| 158.130.6.191 | United States | 147.237.76.200 | eitan.aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 1 |
| 158.130.6.191 | United States | 147.237.0.19 | madim.atal.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 1 |
| 46.19.85.225 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 1 |
| 141.212.122.196 | United States | 147.237.76.196 | e.sviva.idf.il | Geo-location enforcement | Geo-location inbound enforcement | drop | 1 |
| 37.48.80.101 | Netherlands | 147.237.77.216 | dover.idf.il | Directory Traversal | directory traversal overflow | monitor | 1 |
| 137.151.175.32 | United States | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 1 |
| 176.126.252.11 | Romania | 147.237.77.216 | dover.idf.il | Directory Traversal | directory traversal overflow | monitor | 1 |
| 109.163.234.9 | Romania | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 1 |

02-11-2016-03:04:09 to 02-11-2016-04:04:09

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 79.181.53.55 | Israel | 147.237.76.31 | nakchal.idf.il | Unauthorized URL Access to www.nakhal.idf.il/xmlrpc.php | Block | 1 |
| 46.19.85.225 | Israel | 147.237.77.233 | atal.idf.il | Unknown HTTP Request Method .xml in URL | Block | 1 |
| 197.6.205.180 | Tunisia | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php | Block | 1 |
| 68.180.228.175 | United States | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/994-8906-he/refuah.aspx | Block | 1 |
| 40.77.167.73 | United States | 147.237.76.86 | navy.idf.il | Unauthorized URL Access to navy.idf.il/yohalan/forums/asp/showforum.asp | Block | 1 |
| 207.46.13.73 | United States | 147.237.76.86 | navy.idf.il | Unauthorized URL Access to navy.idf.il/navy/links.aspx | Block | 1 |
| 80.82.64.68 | Netherlands | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to iwannaknow.tk/index.php | Block | 1 |
| 50.7.178.100 | Netherlands | 147.237.77.216 | dover.idf.il | URL is Above Root Directory www.idf.il/../shared/clientscripts/jquery/jquery-1.4.2.min.js | Block | 1 |
| 202.142.106.22 | India | 147.237.77.74 | law.idf.il | PHP Attempt | Block | 1 |
| 68.180.229.239 | United States | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/doctor | Block | 1 |
| 41.82.126.138 | Senegal | 147.237.77.216 | dover.idf.il | E-mail collector robots 14 | Block | 1 |
| 207.46.13.79 | United States | 147.237.76.200 | eitan.aka.idf.i | Unauthorized URL Access to www.eitan.aka.idf.il/templates/opmissingperson/opmissingperson.aspx | Block | 1 |
| 130.83.167.219 | Germany | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/newsite/english/documents.asp | Block | 1 |
| 66.249.78.95 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to 147.237.77.216/ | Block | 1 |
| 202.142.106.22 | India | 147.237.77.74 | law.idf.il | Unauthorized URL Access to www.law.idf.il/xmlrpc.php | Block | 1 |
| 79.179.120.104 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/error.htm | Block | 1 |
| 41.82.126.138 | Senegal | 147.237.77.216 | dover.idf.il | eMail Hoarding | Block | 1 |
| 207.46.13.92 | United States | 147.237.76.86 | navy.idf.il | Distributed Unauthorized URL Access on navy.idf.il/yohalan/forums/asp/showforum.asp | Block | 1 |
| 157.55.39.113 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/international_training/services.asp | Block | 1 |
| 68.180.228.112 | United States | 147.237.77.216 | dover.idf.il | Parameter Type Violation PageNum in www.idf.il/1133-he/dover.aspx | Block | 1 |
| 207.46.13.6 | United States | 147.237.76.86 | navy.idf.il | Distributed Unauthorized URL Access on navy.idf.il/yohalan/forums/asp/showforum.asp | Block | 1 |
| 79.181.53.55 | Israel | 147.237.76.31 | nakchal.idf.il | Distributed PHP Attempt | Block | 1 |
| 46.19.85.225 | Israel | 147.237.77.233 | atal.idf.il | Malformed URL | Block | 1 |
| 207.46.13.92 | United States | 147.237.76.86 | navy.idf.il | Unauthorized URL Access to navy.idf.il/yohalan/contact/contact.asp | Block | 1 |
| 197.6.205.180 | Tunisia | 147.237.77.216 | dover.idf.il | Distributed PHP Attempt | Block | 1 |
| 68.180.228.112 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/english/announcements/2003/june10a.stm) | Block | 1 |
| 5.64.237.137 | United Kingdom | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx | Block | 1 |
| 207.46.13.73 | United States | 147.237.76.86 | navy.idf.il | Distributed Unauthorized URL Access on navy.idf.il/yohalan/forums/asp/showforum.asp | Block | 1 |

02-11-2016-03:04:09 to 02-11-2016-04:04:09