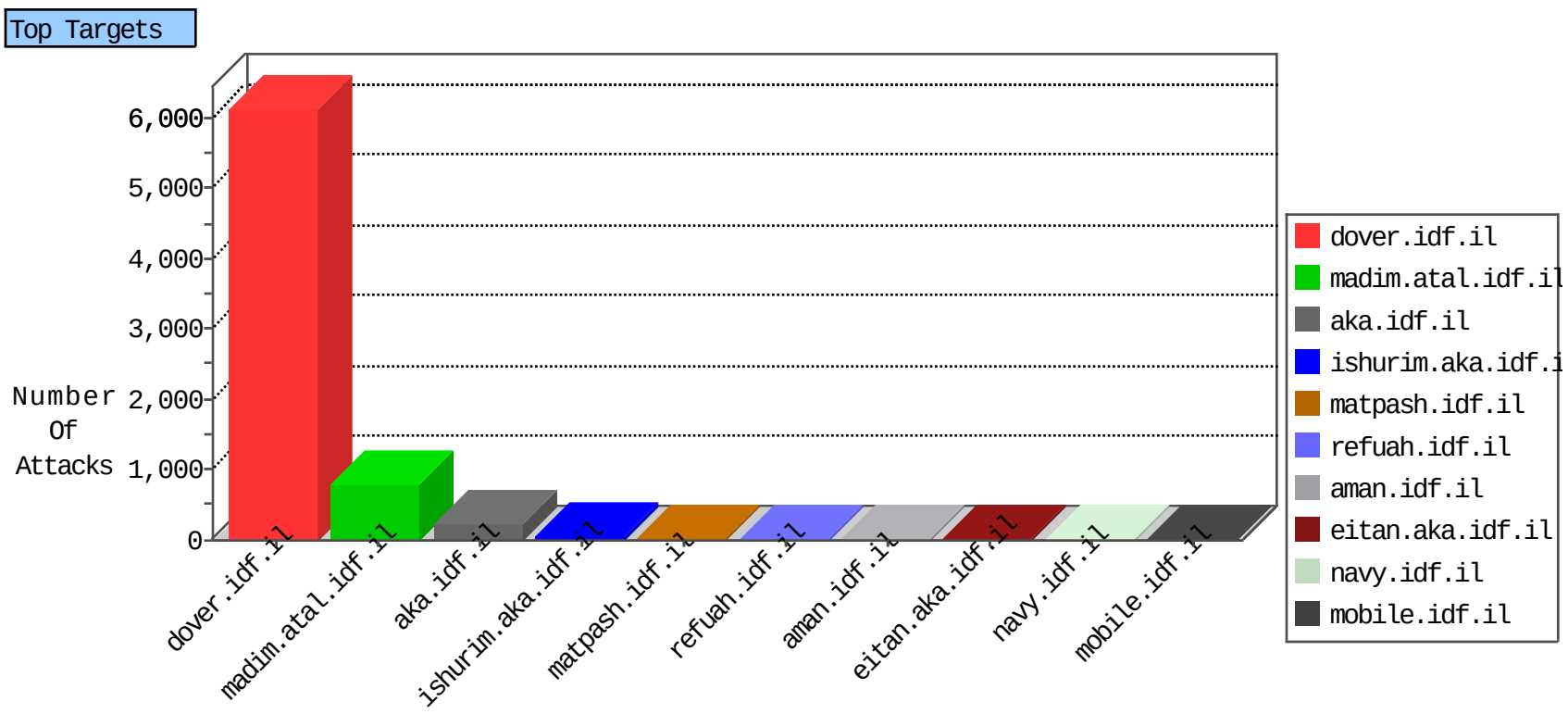
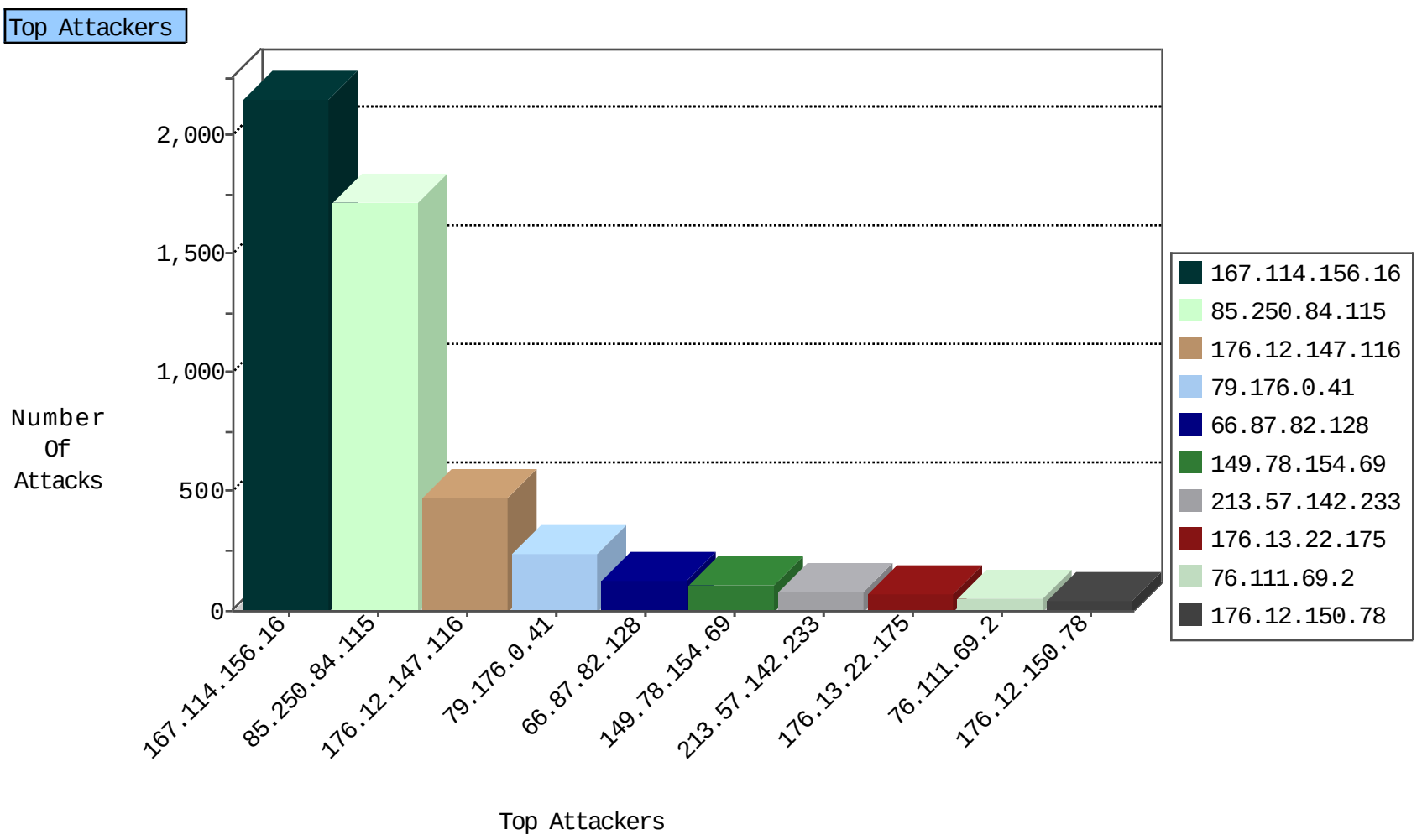
11-07-2015-23:04:04 to 11-08-2015-00:04:04

IDF Under Attack Daily Report

Top Targets



Top Attackers



11-07-2015-23:04:04 to 11-08-2015-00:04:04

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	DOS-Tool-SwitchbladG	dest-reset	3141
79.179.217.78	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2616
66.249.64.191	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	158
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	108
79.183.15.160	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	28
5.29.123.144	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	24
74.190.94.42	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	16
98.242.47.246	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	15
176.13.15.40	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	15
109.66.196.125	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	14
68.175.79.186	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	12
79.183.16.46	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	11
89.138.219.40	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
79.181.27.220	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
79.181.49.37	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
66.87.82.128	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
141.0.13.42	Norway	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
84.108.10.180	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
31.168.185.65	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
80.178.222.218	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
46.117.228.118	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
79.183.15.160	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
46.117.239.238	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
85.64.73.175	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
5.29.182.180	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
2.52.15.146	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
37.26.149.229	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
109.67.11.86	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
5.29.160.84	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
77.125.81.179	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
109.65.176.87	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	3
37.26.149.229	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
46.19.85.103	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
95.86.108.18	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
141.0.12.93	Norway	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
176.13.3.124	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
2.52.12.44	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
62.219.254.22	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	3
85.250.84.115	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
134.225.30.35	United Kingdom	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
219.145.119.190	China	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	2
109.67.29.64	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
109.66.193.152	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
46.19.85.103	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
107.213.83.79	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
79.180.118.200	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
46.19.85.68	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
180.213.93.135	China	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1
2.52.12.44	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1

11-07-2015-23:04:04 to 11-08-2015-00:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
31.154.158.231	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6

11-07-2015-23:04:04 to 11-08-2015-00:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	8
176.12.147.116	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	7
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.67.124	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	2
104.128.144.131	147.237.77.226	Canada	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 3072	1
101.81.134.22	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
103.232.35.46	147.237.72.166	Hong Kong	aka.idf.il	ET SCAN NMAP -sS window 3072	1
89.160.38.36	147.237.8.27	Sweden	e.madim.atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
101.81.134.22	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
101.81.134.22	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
101.81.134.22	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	1
222.186.21.196	147.237.0.35	China	akaws.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
101.81.134.22	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
202.96.25.62	147.237.72.166	China	aka.idf.il	ET SCAN Potential SSH Scan	1
101.81.134.22	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
101.81.134.22	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
101.81.134.22	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
103.232.35.46	147.237.72.166	Hong Kong	aka.idf.il	ET SCAN NMAP -sS window 4096	1
89.240.193.9	147.237.76.42	United Kingdom	refuah.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
101.81.134.22	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	1
77.45.156.216	147.237.76.30	Russian Federation	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
101.81.134.22	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
61.109.58.174	147.237.0.33	Korea, Republic of	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
101.81.134.22	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential SSH Scan	1
31.6.71.154	147.237.0.17	Poland	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
222.186.21.196	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
101.81.134.22	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
222.186.21.196	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
101.81.134.22	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
202.96.25.62	147.237.72.156	China	aman.idf.il	ET SCAN Potential SSH Scan	1
101.81.134.22	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1
188.138.9.51	147.237.0.17	Germany	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
101.81.134.22	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1

11-07-2015-23:04:04 to 11-08-2015-00:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
85.250.84.115	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1719
66.87.82.128	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	115
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	106
213.57.142.233	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	79
176.13.22.175	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	71
76.111.69.2	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	55
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
74.190.94.42	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
86.140.213.87	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
62.0.84.239	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
133.130.52.247	Japan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
66.249.65.231	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
79.178.212.222	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
66.249.93.196	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
46.120.206.135	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
37.46.174.171	Sweden	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
54.224.21.23	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
185.3.144.46	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
79.176.29.203	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
5.28.135.44	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
89.138.207.161	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
89.138.95.33	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
186.204.246.30	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
213.233.64.164	Romania	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
85.250.74.139	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
164.138.126.156	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
46.117.190.134	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
66.249.65.238	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
157.55.39.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
77.127.188.65	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
54.187.55.213	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	16
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
89.138.214.245	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
172.56.39.118	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
77.127.56.60	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
89.138.219.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
46.19.85.104	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
84.109.166.172	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	14
79.180.118.200	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
132.76.50.6	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
79.181.27.220	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
77.127.150.153	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
134.225.30.35	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
87.19.253.74	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13

11-07-2015-23:04:04 to 11-08-2015-00:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.12.147.116	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	297
79.176.0.41	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	107
176.12.147.116	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	104
79.176.0.41	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	96
176.12.147.116	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	71
176.12.150.78	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	46
79.176.0.41	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	40
89.139.4.147	Israel	147.237.72.167	ishurim.aka.idf.i	Too Many of the Same Response Code (404) in Session from 89.139.4.147	Block	39
176.12.149.216	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
208.115.111.72	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	4
62.219.144.222	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
185.32.179.254	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.15.40	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
5.102.192.212	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
185.3.144.46	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
80.246.136.34	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
5.102.254.213	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
66.249.67.122	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
2.52.12.44	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.117.63.247	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.179.18.94	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/nmain/giyus/kiosk/kiosk.aspx	Block	1
66.249.67.242	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
66.249.65.237	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/templates/sendtofriend/sendtofriend.aspx	Block	1
66.249.67.71	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/yohalan/main/main.asp	Block	1
95.86.70.127	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized Method POST for www.eitan.aka.idf.il/1105-he/contactus.aspx	None	1
212.117.151.42	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/templates/shared/usercontrols/trajector/	Block	1
66.249.67.250	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/giyus/general.aspx	Block	1
66.249.67.6	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
89.139.46.91	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
95.86.70.127	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter r in www.eitan.aka.idf.il/templates/opcontactus/govcaptchaimage.axd	None	1
62.219.144.222	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
84.109.166.172	Israel	147.237.72.166	aka.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 84.109.166.172	Block	1
213.57.160.27	Israel	147.237.72.156	aman.idf.il	Too Many Cookies in a Request - 111 cookies	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1038-ar/cogat.aspx	Block	1
66.249.67.13	Israel	147.237.72.166	aka.idf.il	Unknown Parameter pop in www.aka.idf.il/main/home/	None	1
37.26.146.202	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
93.223.183.56	Germany	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
79.177.32.83	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	1
66.249.67.147	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/list20041220a.htm	Block	1
188.165.15.14	France	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
109.65.176.87	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.65.223	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/webresource.axd	Block	1
85.250.74.139	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
68.180.230.57	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/templates/shared/usercontrols/headerupper/	Block	1
66.249.67.59	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
37.26.147.195	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
95.86.68.10	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 95.86.68.10	Block	1
79.178.216.61	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
208.115.111.72	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 208.115.111.72	Block	1
66.249.67.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1

11-07-2015-23:04:04 to 11-08-2015-00:04:04