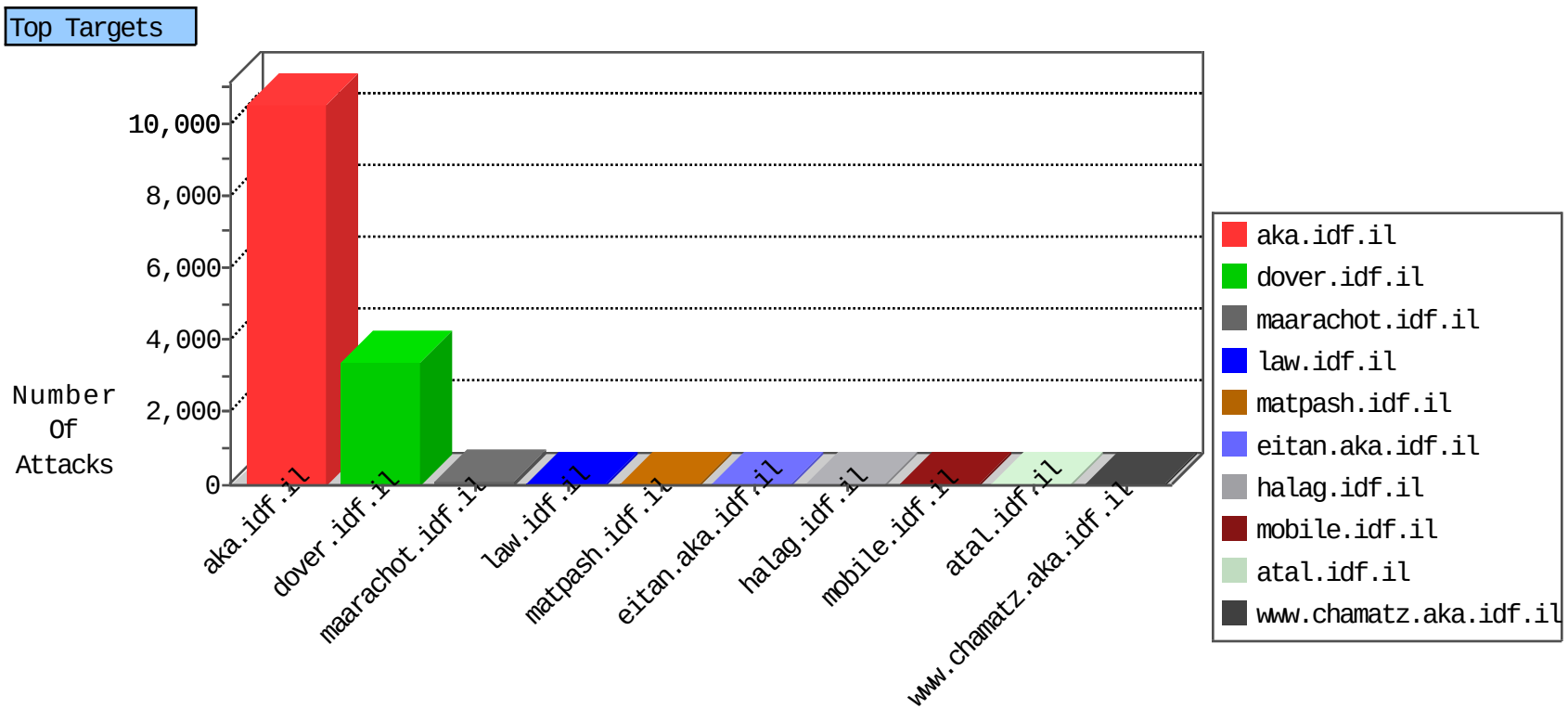
11-04-2015-00:04:02 to 11-04-2015-01:04:02

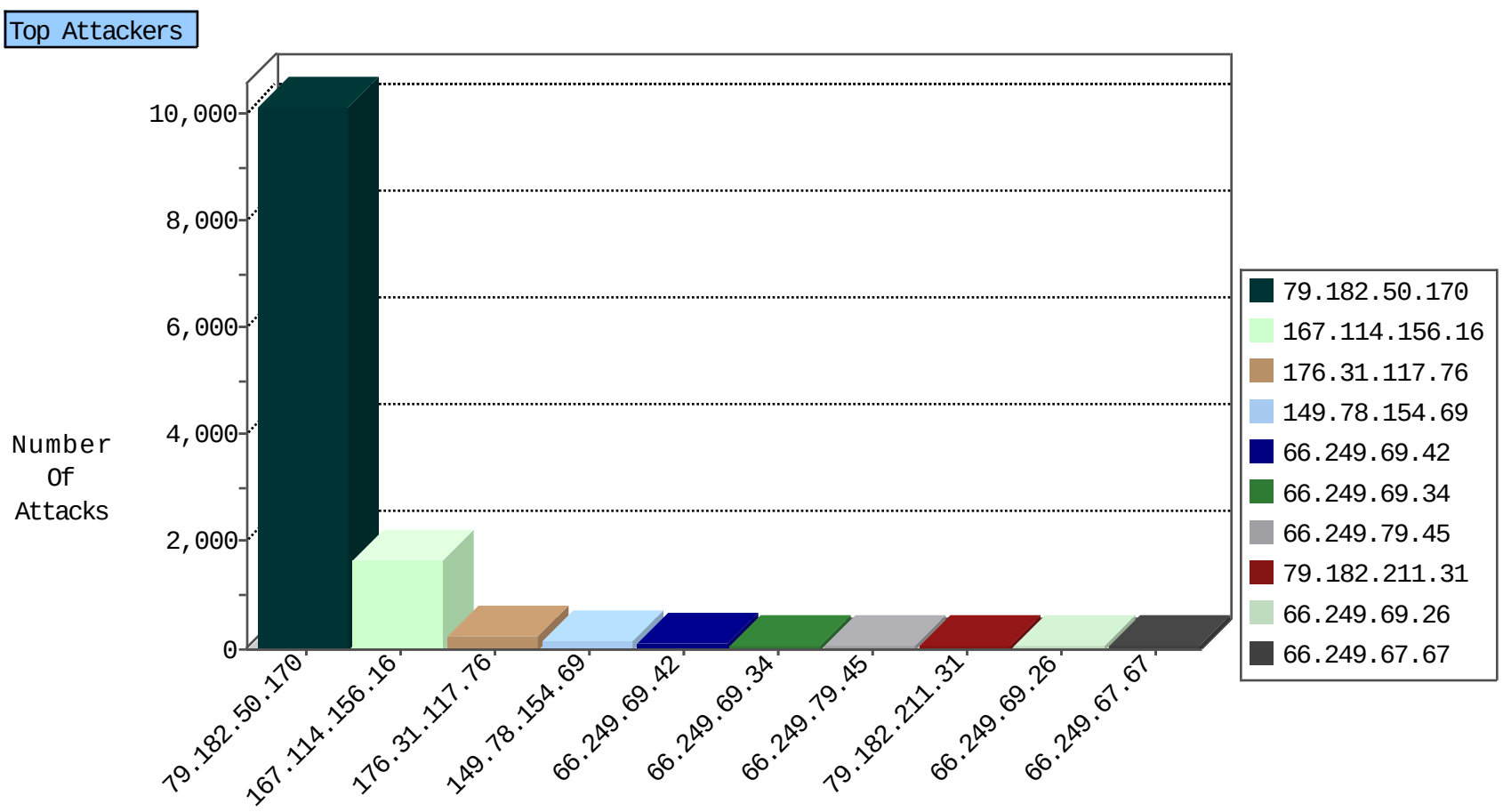
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

11-04-2015-00:04:02 to 11-04-2015-01:04:02

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	TCP handshake violation, first packet not syn	drop	20982
66.249.69.34	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5519
66.249.79.45	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	5212
66.249.69.42	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2490
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	2391
37.76.113.31	Hungary	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1873
66.249.79.78	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	1862
68.180.228.112	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1760
66.249.67.60	United States	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	1687
176.31.117.76	France	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1386
151.207.250.51	United States	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	1339
188.165.15.126	France	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1085
66.249.67.67	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	1053
50.87.144.145	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	984
66.249.67.219	United States	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	967
54.224.21.23	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	759
66.249.67.235	United States	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	685
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	600
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	475
66.249.79.41	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	362
66.249.67.79	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	192
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	134
52.16.5.197	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	72
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	49
132.70.66.13	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	25
109.67.139.118	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	24
77.127.238.241	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
212.76.102.184	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
84.228.229.113	Bulgaria	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
66.249.69.50	United States	147.237.77.226	www.chamatz.aka.idf.il	TCP handshake violation, first packet not syn	drop	6
46.116.136.93	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
149.78.251.241	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
37.142.68.57	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
66.249.69.34	United States	147.237.77.226	www.chamatz.aka.idf.il	TCP handshake violation, first packet not syn	drop	4
77.127.245.79	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
46.120.83.232	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
176.13.23.66	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
46.19.86.151	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
134.121.116.209	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
66.102.9.81	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
2.54.150.232	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
66.249.67.134	United States	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	2
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
83.244.54.142	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	2
52.23.156.32	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
65.55.210.0	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
46.166.188.68	Netherlands	147.237.76.34	yohalan.idf.il	Block_Ntp_All_Net	drop	1
188.247.72.83	Jordan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
108.59.253.71	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

11-04-2015-00:04:02 to 11-04-2015-01:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
63.237.114.10	United States	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
52.1.90.117	United States	147.237.77.216	dover.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

11-04-2015-00:04:02 to 11-04-2015-01:04:02

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	6
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
177.37.128.117	147.237.0.16	Brazil	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
177.37.128.117	147.237.76.197	Brazil	e.himush.idf.il	ET SCAN Potential SSH Scan	2
177.37.128.117	147.237.77.121	Brazil	e.navy.idf.il	ET SCAN Potential SSH Scan	1
177.37.128.117	147.237.76.200	Brazil	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
119.10.8.133	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
177.37.128.117	147.237.76.148	Brazil	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
14.117.132.33	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
177.37.128.117	147.237.76.86	Brazil	navy.idf.il	ET SCAN Potential SSH Scan	1
177.37.128.117	147.237.76.31	Brazil	nakchal.idf.il	ET SCAN Potential SSH Scan	1
177.37.128.117	147.237.72.167	Brazil	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
188.138.9.51	147.237.0.35	Germany	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
177.37.128.117	147.237.72.156	Brazil	aman.idf.il	ET SCAN Potential SSH Scan	1
177.37.128.117	147.237.77.227	Brazil	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
177.37.128.117	147.237.8.46	Brazil	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
177.37.128.117	147.237.77.176	Brazil	matpash.idf.il	ET SCAN Potential SSH Scan	1
177.37.128.117	147.237.0.19	Brazil	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
177.37.128.117	147.237.77.19	Brazil	law-forum.idf.il	ET SCAN Potential SSH Scan	1
173.1.121.85	147.237.0.35	United States	akaws.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
177.37.128.117	147.237.76.147	Brazil	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
5.39.222.253	147.237.72.217	Netherlands	e.idf.il	ET SCAN Potential SSH Scan	1
177.37.128.117	147.237.76.38	Brazil	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
177.37.128.117	147.237.72.217	Brazil	e.idf.il	ET SCAN Potential SSH Scan	1
177.37.128.117	147.237.72.166	Brazil	aka.idf.il	ET SCAN Potential SSH Scan	1
185.82.201.17	147.237.77.216		dover.idf.il	ET DOS SSL Bomb DoS Attempt	1
177.37.128.117	147.237.8.50	Brazil	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
177.37.128.117	147.237.77.226	Brazil	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
177.37.128.117	147.237.0.35	Brazil	akaws.idf.il	ET SCAN Potential SSH Scan	1

11-04-2015-00:04:02 to 11-04-2015-01:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.182.50.170	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2658
176.31.117.76	France	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	215
149.78.154.69	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	141
79.182.211.31	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	66
66.249.69.42	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
66.249.69.34	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	49
79.182.50.170	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	49
79.182.50.170	Israel	147.237.72.166	aka.idf.il	drop		drop	45
66.249.69.26	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
37.76.113.31	Hungary	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	40
54.72.73.168	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	35
5.22.134.234	Israel	147.237.77.234	halag.idf.i	Bad TCP sequence	Invalid ACK number	monitor	35
54.72.0.55	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	34
2.54.147.94	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	27
41.33.231.90	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	25
130.126.255.195	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	23
108.59.253.71	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	23
46.19.86.50	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	22
172.56.30.186	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	22
52.16.5.197	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	22
2.54.26.159	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	21
109.67.139.118	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	21
212.179.90.106	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	19
207.241.229.188	United States	147.237.72.166	aka.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	19
114.108.229.241	Philippines	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	19
46.19.86.120	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	18
50.87.144.145	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	17
212.199.182.150	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	17
41.33.232.66	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	15
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	15
157.55.39.32	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	13
104.131.195.214	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
185.87.156.235		147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
46.19.85.114	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
176.12.151.228	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
79.182.100.248	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
100.100.51.31		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
157.55.39.236	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	11
213.57.224.240	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	11
66.249.83.155	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	11
68.4.93.63	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	11
40.77.167.39	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	11
66.249.69.42	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	11
109.67.197.133	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	10
98.161.59.186	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	10
149.78.251.241	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	10
41.33.231.90	Egypt	147.237.77.216	dover.idf.i	drop		drop	10
66.249.69.26	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	10
185.58.201.11	Lebanon	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	10
66.249.69.34	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	10

11-04-2015-00:04:02 to 11-04-2015-01:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.182.50.170	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Request from 79.182.50.170	Block	4407
79.182.50.170	Israel	147.237.72.166	aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	1548
79.182.50.170	Israel	147.237.72.166	aka.idf.il	Automated Vulnerability Scanning	Block	1445
207.232.21.105	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 207.232.21.105	Block	42
109.64.19.30	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	2
46.116.190.74	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	2
66.249.67.13	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
185.32.179.183	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
109.65.104.220	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
138.134.192.10	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 138.134.192.10	Block	1
66.249.65.132	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/894-he	Block	1
31.168.86.225	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
80.246.136.146	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.125.80.8	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.67.71	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
207.46.13.58	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
66.249.67.250	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
176.13.18.239	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
36.250.182.168	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/shared/usercontrols/headerupper/	Block	1
80.246.136.146	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
78.54.90.150	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
66.249.67.122	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/1146-he/chinuch.aspx	Block	1
207.46.13.153	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/	Block	1
109.64.108.28	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/	Block	1
66.249.65.80	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/print_bottom.asp	Block	1
66.249.67.59	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
37.142.68.0	Israel	147.237.0.19	madim.atal.idf.il	Admin Blocking	Block	1
85.250.121.145	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar	Block	1
79.98.148.82	Poland	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.67.196	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/798-3157-he/patzar.aspx	Block	1
207.232.21.105	Israel	147.237.76.200	eitan.aka.idf.il	Too Many 404: Response Code per Session	Block	1
66.249.65.99	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.182.50.170	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.74.104	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/	Block	1
66.249.67.60	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
185.49.14.190	Poland	147.237.72.156	aman.idf.il	Unauthorized URL Access to testp5.mielno.lubin.pl/testproxy.php	Block	1
37.142.68.0	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/admin/	Block	1
105.105.7.111	Algeria	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 105.105.7.111	Block	1
79.179.128.139	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
66.249.67.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/giyus/general.aspx	Block	1
138.134.192.10	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//resources/images/innerpage/goback.gif	Block	1
66.249.65.115	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/2/2272.jpg	Block	1
5.22.134.234	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
79.183.207.106	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
68.180.229.239	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.67.65	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/smalim/showbig.aspx	Block	1
185.49.14.190	Poland	147.237.72.166	aka.idf.il	Unauthorized URL Access to testp2.czar.bielawa.pl/testproxy.php	Block	1
105.105.7.111	Algeria	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/console	Block	1
46.116.150.228	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/request.aspx	None	1

11-04-2015-00:04:02 to 11-04-2015-01:04:02