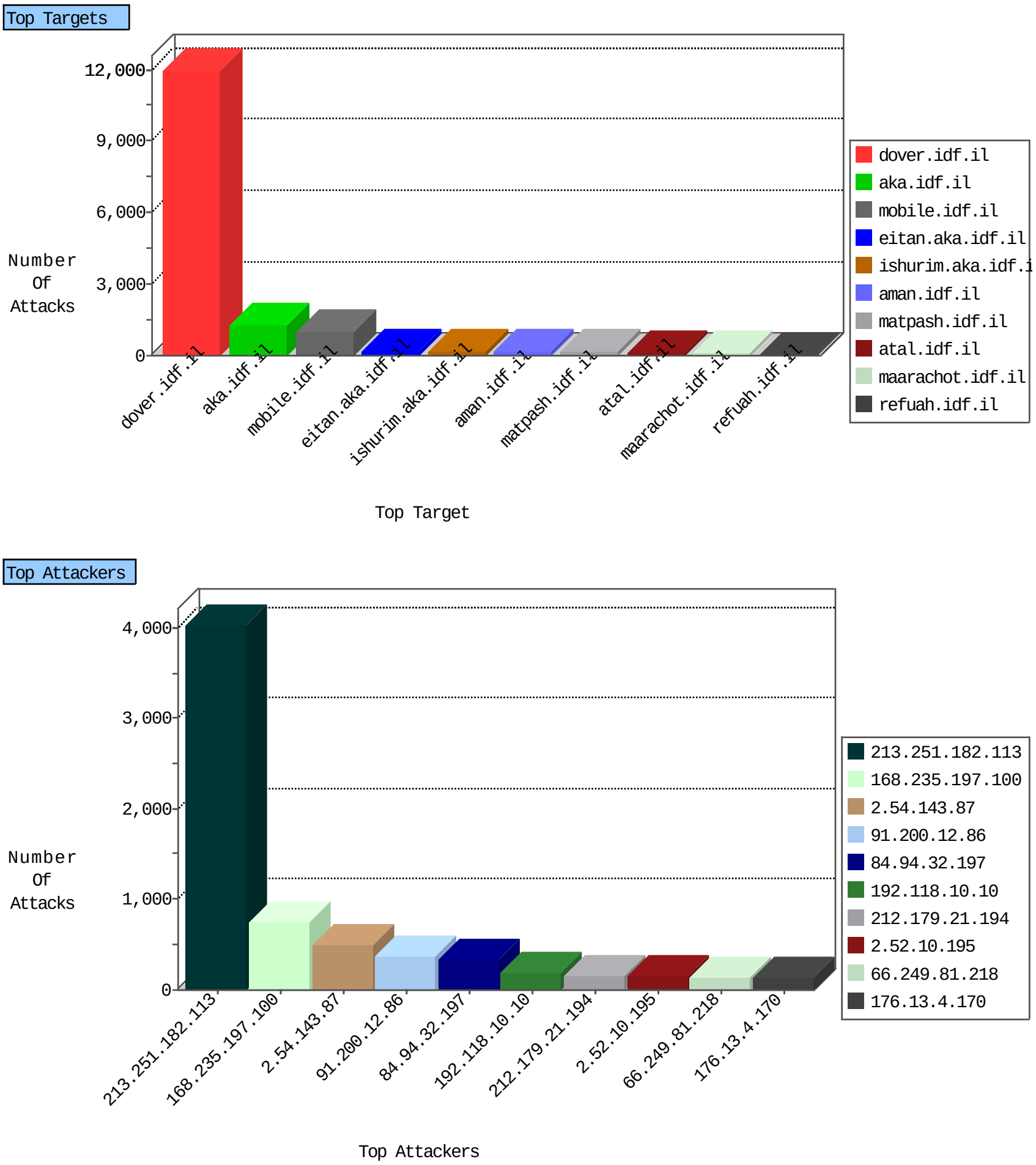
11-01-2015-14:04:03 to 11-01-2015-15:04:03

IDF Under Attack Daily Report



11-01-2015-14:04:03 to 11-01-2015-15:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
213.251.182.113	France	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5608
66.249.81.209	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	3947
167.114.156.16	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3289
192.114.177.190	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2592
87.68.26.182	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	529
66.249.81.218	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	455
66.249.78.159	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	421
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	327
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	182
149.78.148.114	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	153
192.116.167.41	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	107
79.179.170.135	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	100
66.249.81.212	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	92
46.120.248.245	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	80
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	75
66.102.9.91	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	39
212.117.143.250	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	31
212.179.21.194	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	31
62.128.42.106	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	24
87.68.30.194	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	18
176.13.18.149	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	15
37.26.146.154	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	14
212.179.46.16	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	13
176.13.18.149	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	12
84.228.198.96	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
46.19.86.207	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
2.54.13.138	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
84.108.49.172	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	8
2.54.38.94	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	8
192.118.10.10	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7
79.182.69.199	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
168.235.197.100	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6
66.102.9.101	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6
52.16.5.197	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6
79.180.181.131	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
80.246.136.37	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
46.19.86.4	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
178.130.40.48	Russian Federation	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
185.32.179.1	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
77.125.86.236	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
89.138.224.221	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
31.154.5.181	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
176.13.20.67	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
37.26.147.207	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
146.185.57.7	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	3
212.117.143.250	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
115.231.222.40	China	147.237.76.197	e.himush.idf.il	JLM_Purple_Con_Limit_Http	drop	3
95.35.184.1	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
212.179.210.163	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
50.118.196.232	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3

11-01-2015-14:04:03 to 11-01-2015-15:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
92.45.142.175	Turkey	147.237.72.166	aka.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1
81.218.33.77	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1

11-01-2015-14:04:03 to 11-01-2015-15:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.109.57.127	147.237.77.216	Algeria	dover.idf.il	SQL Injection - Select From	2
213.57.189.82	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	2
36.100.169.93	147.237.77.234	China	halag.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
109.66.190.223	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.9.76	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.64.146.111	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.179.21.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.192.68.46	147.237.77.216	Netherlands	dover.idf.il	portscan: TCP Distributed Portscan	1
200.142.182.24	147.237.77.19	Brazil	law-forum.idf.il	ET SCAN Potential SSH Scan	1
79.181.65.24	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
200.142.182.24	147.237.76.44	Brazil	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
77.126.93.73	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
176.13.14.199	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
62.90.35.105	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.12.142.61	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.117.249.167	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
149.78.63.11	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.67.134.227	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
31.154.91.157	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.66.58.69	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.108.147.76	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
200.142.182.24	147.237.77.170	Brazil	maarachot.idf.il	ET SCAN Potential SSH Scan	1
82.80.57.222	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
200.142.182.24	147.237.76.196	Brazil	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
79.181.53.113	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
75.67.134.195	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
176.13.6.213	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
50.118.196.232	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
176.12.139.244	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.90	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
149.78.1.25	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

11-01-2015-14:04:03 to 11-01-2015-15:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
213.251.182.113	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3985
168.235.197.100	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	749
84.94.32.197	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	321
2.52.10.195	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	154
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	133
217.132.38.183	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	124
66.249.81.218	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	115
213.244.65.90	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	100
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	94
197.144.4.58	Morocco	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	93
66.249.81.215	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	91
37.26.146.154	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	87
54.187.55.213	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	86
100.100.4.0		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	84
212.179.46.16	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	80
66.249.81.212	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	72
178.214.75.64	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	72
64.233.172.155	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	71
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	65
176.13.20.104	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	58
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	58
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	57
84.108.38.146	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	53
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	53
46.120.229.31	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	52
37.26.149.157	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	50
84.108.126.117	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
5.28.133.125	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
79.180.107.37	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	47
2.54.138.58	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	46
192.114.177.190	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	46
84.108.49.172	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
2.54.130.113	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
46.120.229.31	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
77.125.161.240	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
93.172.157.116	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
85.64.183.55	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
87.68.30.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
212.117.143.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
212.179.219.165	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
37.26.147.167	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
79.178.160.254	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
2.54.60.41	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
79.180.181.131	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
5.22.129.186	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
46.19.86.237	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
80.179.212.154	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
66.249.78.159	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	32
100.100.87.103		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	31

11-01-2015-14:04:03 to 11-01-2015-15:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.143.87	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	330
91.200.12.86	Ukraine	147.237.77.216	dover.idf.il	PHP Attempt	Block	180
2.54.143.87	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	173
91.200.12.86	Ukraine	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 91.200.12.86	Block	135
176.13.4.170	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	120
192.118.10.10	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 192.118.10.10	Block	120
212.179.155.129	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	93
46.19.86.87	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	83
2.54.174.198	Israel	147.237.72.167	ishurim.aka.idf.i	Distributed Too Many of the Same Response Code (404)	Block	83
212.199.185.228	Israel	147.237.72.166	aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	60
2.54.139.227	Israel	147.237.72.166	aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	60
149.88.152.242	Israel	147.237.72.156	aman.idf.il	PHP Attempt	Block	45
149.88.152.242	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/ajax/updatestatus.php	Block	45
185.32.179.37	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	45
171.107.25.58	China	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	45
91.200.12.86	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	45
46.19.86.116	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	30
5.22.129.188	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/aman	Block	30
176.13.12.255	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	30
80.246.136.7	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	30
2.54.155.214	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	30
192.118.10.10	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 192.118.10.10	Block	30
46.121.68.142	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	30
46.121.68.142	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php	Block	30
192.114.5.10	Israel	147.237.72.167	ishurim.aka.idf.i	Untraceable SSL Sessions: Open Mode	None	30
171.107.25.58	China	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 171.107.25.58	Block	30
109.66.112.34	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	30
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	30
149.78.216.248	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/aman	Block	24
46.117.30.165	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	15
85.65.192.207	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	15
37.26.146.195	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	15
151.80.31.112	Italy	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	15
79.180.141.116	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	15
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/newsflash/youtube.com/idfspox1	Block	15
109.67.18.233	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	15
66.249.67.6	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/family	Block	15
192.118.10.10	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/images/shared/home.png	Block	15
82.221.105.6	Iceland	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/	Block	15
176.12.147.11	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	15
77.125.151.118	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/giyus/talpiotquestionnaire.aspx	None	15
2.52.130.138	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	15
104.227.190.21		147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/documents.asp	Block	15
66.249.67.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/yohalan/main/main.asp	Block	15
46.120.229.31	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 46.120.229.31	Block	15
85.130.248.6	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	15
46.19.85.5	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	15
157.55.39.253	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/robots.txt	Block	15
66.249.81.218	Israel	147.237.77.216	dover.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 66.249.81.218	Block	15
66.249.67.65	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	15

11-01-2015-14:04:03 to 11-01-2015-15:04:03