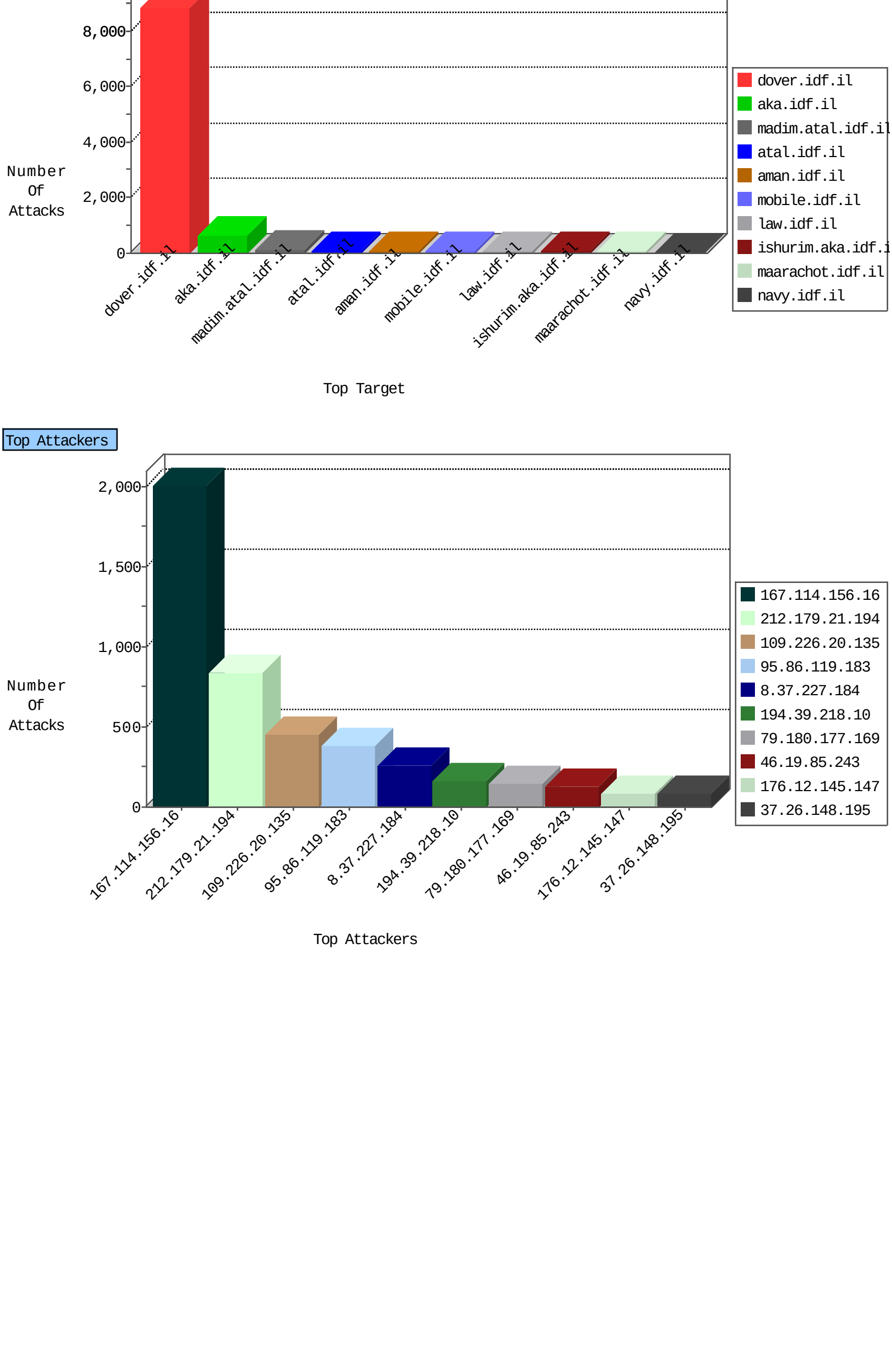
11-04-2015-14:04:05 to 11-04-2015-15:04:05

IDF Under Attack Daily Report



11-04-2015-14:04:05 to 11-04-2015-15:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
197.115.207.146	Algeria	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	18704
66.249.67.216	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	12009
66.249.67.13	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	6923
167.114.156.16	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6412
66.249.69.42	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6128
66.249.67.67	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	5780
66.249.67.194	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	4455
66.249.79.41	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	4129
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3461
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3205
66.249.79.43	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	2524
66.249.67.79	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	1922
50.87.144.145	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	340
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	209
66.249.79.45	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	180
0.0.0.0		147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	130
2.54.166.64	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	85
66.249.67.235	United States	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	70
37.26.147.241	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	39
197.115.207.146	Algeria	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	38
62.219.175.10	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	35
82.81.16.230	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	35
2.54.135.162	Israel	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	31
8.37.227.184	Anonymous Proxy	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	26
109.65.146.144	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	25
31.154.19.5	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	22
82.145.210.65	Europe	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	21
200.119.132.194	Guatemala	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
62.219.155.195	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
109.67.104.57	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
77.125.73.154	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
85.250.56.42	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
79.176.117.105	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
87.68.70.243	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
80.178.147.45	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
50.136.19.150	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5
79.183.21.218	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
194.39.218.10	Europe	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5
37.26.146.241	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
87.68.251.15	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
80.246.136.165	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
192.3.152.101	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
5.29.82.250	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
2.52.157.208	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
213.144.0.113	Germany	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
2.52.153.138	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
62.219.254.22	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	3
79.180.177.169	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
77.125.147.56	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
91.211.116.35	Ukraine	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	3

11-04-2015-14:04:05 to 11-04-2015-15:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
95.86.102.126	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2

11-04-2015-14:04:05 to 11-04-2015-15:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
80.246.137.76	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	2
149.78.251.252	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
85.250.197.136	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
31.154.91.250	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	1
149.78.58.10	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.109.152.101	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.85	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.13.97.100	147.237.72.166	Ireland	aka.idf.il	portscan: TCP Distributed Portscan	1
185.27.105.190	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

11-04-2015-14:04:05 to 11-04-2015-15:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	830
109.226.20.135	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	454
95.86.119.183	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	385
8.37.227.184	Anonymous Proxy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	259
194.39.218.10	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	158
46.19.85.243	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	125
79.180.177.169	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	92
37.26.148.195	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	82
54.187.55.213	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	80
192.114.91.247	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	70
81.218.251.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	68
217.132.32.223	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	66
185.27.105.190	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	63
62.128.42.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	60
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	60
46.19.86.10	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	59
212.235.28.30	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	53
5.29.251.225	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
31.154.19.5	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
31.168.245.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	50
79.178.154.79	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	50
185.120.126.30		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
5.255.253.157	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
79.180.177.169	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
104.53.248.183	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
79.182.35.111	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
79.178.123.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
37.26.146.241	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
85.250.135.252	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
66.249.69.26	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
213.57.188.35	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
50.136.19.150	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
46.19.85.142	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
64.233.172.155	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
85.250.56.42	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
5.29.6.130	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
2.54.8.249	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
71.32.162.204	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
2.54.57.20	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
46.19.85.115	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
95.86.78.50	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
109.67.104.57	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
62.219.155.195	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
46.210.233.88	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
66.249.69.42	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24

11-04-2015-14:04:05 to 11-04-2015-15:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.12.145.147	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	61
176.12.145.147	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.12.145.147	Block	24
46.19.86.34	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	21
2.54.37.59	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
149.78.251.252	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 149.78.251.252	Block	17
46.19.86.100	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
46.19.86.113	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	6
46.19.85.95	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
80.179.78.66	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	4
80.179.78.66	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/pages/fan_status.php	Block	4
66.249.65.83	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	3
93.172.172.220	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	3
93.172.172.220	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/pages/fan_status.php	Block	3
213.57.188.35	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
171.107.24.219	China	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	3
54.210.135.42	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/894-he/hamaz.aspx	Block	2
93.172.172.220	Israel	147.237.72.156	aman.idf.il	PHP Attempt	Block	2
37.26.149.179	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
171.107.24.219	China	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 171.107.24.219	Block	2
93.172.172.220	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/ajax/pages/fan_status.php	Block	2
37.26.149.227	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
149.78.251.252	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	2
2.54.134.5	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
149.78.251.252	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/pages/fan_status.php	Block	2
5.29.251.225	Israel	147.237.72.156	aman.idf.il	Unauthorized HTTP Method	Block	2
66.249.65.93	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
149.78.221.132	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giys	Block	1
207.46.13.150	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.181.120.49	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
2.52.44.195	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
149.78.251.252	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/kiosk/[object object]	Block	1
66.249.67.71	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
109.66.179.11	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 109.66.179.11	Block	1
66.249.65.80	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	1
216.218.206.66	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	1
46.19.85.133	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Double URL Encoding - parameter: ReturnUrl in m.my-kosher-kravi.idf.il/templates/login.aspx	Block	1
184.105.139.68	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/6/67906.pdf	Block	1
31.154.92.223	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/pages/fan_status.php	Block	1
68.180.230.224	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in www.nakhal.idf.il/1111-he/nakhal.aspx	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/7/2347.jpg	Block	1
149.78.221.132	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
54.210.135.42	United States	147.237.72.166	aka.idf.il	Unknown Parameter amp;list in www.aka.idf.il/chamatz/klali/default.asp	None	1
208.115.113.82	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-en	Block	1
176.13.7.170	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
149.78.255.165	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/webresource.axd	Block	1
66.249.67.122	Israel	147.237.72.166	aka.idf.il	Unknown Parameter gt; in www.aka.idf.il/main/rabanut/general.aspx	None	1
109.66.179.11	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/9/	Block	1
216.218.206.68	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1
195.3.144.124	Latvia	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1

11-04-2015-14:04:05 to 11-04-2015-15:04:05