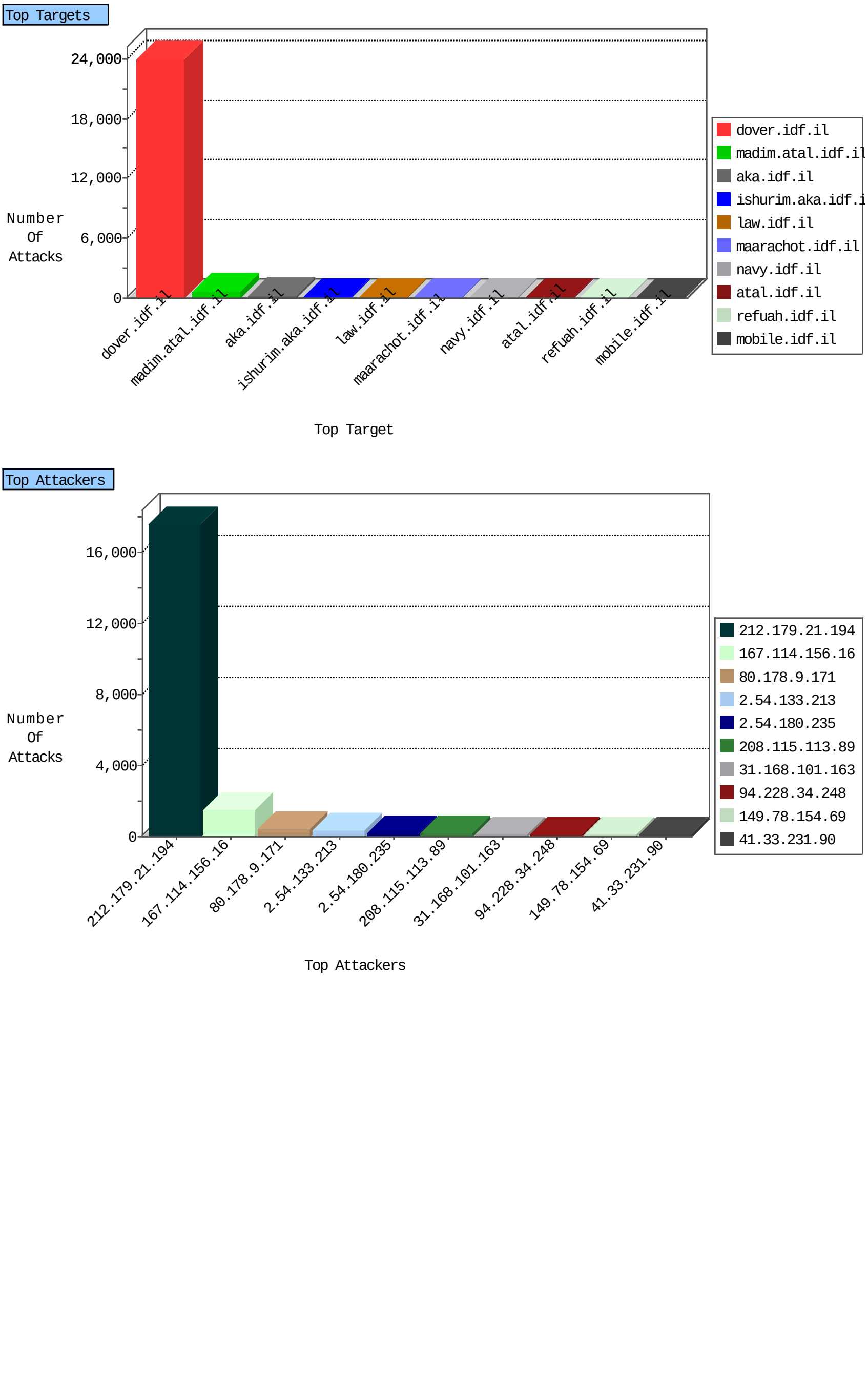
11-05-2015-08:04:06 to 11-05-2015-09:04:06

IDF Under Attack Daily Report



11-05-2015-08:04:06 to 11-05-2015-09:04:06

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	2539
66.249.65.224	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1260
167.114.156.16	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	903
66.249.79.16	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	887
66.249.67.79	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	551
85.159.214.126	United Kingdom	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	211
66.249.79.43	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	186
66.249.67.67	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	107
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	53
95.86.104.72	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	35
82.80.234.100	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	34
132.64.171.235	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	30
5.29.143.123	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	28
46.19.85.63	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	25
93.172.134.79	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	22
46.19.85.156	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	22
176.13.20.112	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	15
176.12.139.194	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	15
176.13.11.2	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	15
79.183.21.175	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	13
66.249.79.41	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	12
77.127.109.138	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	12
31.168.101.163	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
202.70.74.77	Nepal	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7
66.249.79.45	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	6
79.177.99.160	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
82.80.196.44	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
82.145.217.193	Europe	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	5
62.219.254.22	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	5
2.54.50.215	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
79.183.64.192	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
79.176.110.198	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
62.105.140.248	Russian Federation	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
31.186.228.60	United Kingdom	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
80.246.136.109	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
46.121.193.138	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
2.54.190.70	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
37.26.147.174	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
212.179.21.194	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
37.26.149.236	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
93.159.239.12	Russian Federation	147.237.77.170	maarachot.idf.il	Frk_Under_Attack_Con_Tcp	drop	2
2.52.41.17	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
71.198.94.170	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
183.60.48.25	China	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets_Con_Limit	drop	1
89.248.172.98	Netherlands	147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	1
212.199.195.61	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
176.13.4.102	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
95.172.79.244	United Kingdom	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
185.84.238.25		147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

11-05-2015-08:04:06 to 11-05-2015-09:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
31.168.136.9	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
194.114.146.227	Israel	147.237.72.166	aka.idf.il	C1000169: Block - dns poisoning (Clalit)	Permit	1

11-05-2015-08:04:06 to 11-05-2015-09:04:06

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	3
115.72.103.148	147.237.0.19	Vietnam	madim.atal.idf.il	ET SCAN Potential SSH Scan	2
94.102.49.122	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
89.248.174.106	147.237.8.24	Netherlands	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.64.37	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
112.175.228.13	147.237.76.176	Korea, Republic of	test.ncore.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	1
94.102.49.79	147.237.76.31	Netherlands	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
89.248.172.154	147.237.0.33	Netherlands	idf.il	ET SCAN NMAP -sS window 1024	1
46.19.85.65	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
5.22.134.253	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

11-05-2015-08:04:06 to 11-05-2015-09:04:06

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	17608
80.178.9.171	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	442
2.54.180.235	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	229
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	153
31.168.101.163	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	133
94.228.34.248	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	132
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	102
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	82
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	80
37.26.148.130	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	79
2.52.52.32	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	75
37.26.149.160	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	65
2.54.176.34	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	64
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	53
176.13.6.152	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	49
202.70.74.77	Nepal	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
198.251.52.101	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
80.179.40.62	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
79.183.21.175	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
95.86.104.72	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
85.130.141.152	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	37
2.54.144.106	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
37.26.147.197	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
66.249.93.200	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
85.250.118.17	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
85.130.141.152	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	alert	31
41.238.186.6	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
77.127.109.138	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
124.171.196.120	Australia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
207.46.13.177	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
80.178.157.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
81.218.251.252	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
62.219.110.138	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
46.19.86.213	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	23
81.218.170.239	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
37.60.41.164	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
66.249.65.231	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	22
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
66.249.65.238	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
199.203.215.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
46.121.220.117	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
77.125.84.221	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19

11-05-2015-08:04:06 to 11-05-2015-09:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.133.213	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	205
2.54.133.213	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	111
79.178.11.157	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	69
2.54.133.213	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	53
2.54.144.106	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	35
80.246.137.140	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
208.115.113.88	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	6
2.54.162.70	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
176.12.142.239	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
46.19.85.179	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
185.32.179.60	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
72.52.128.19	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 72.52.128.19	Block	3
87.69.166.175	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ajax/pages/fan_status.php	Block	2
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	2
109.186.160.116	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.178.178.166	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.18.54	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
149.88.118.227	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	2
31.154.8.98	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
54.244.22.103	United States	147.237.76.147	chinuch.aka.idf.i	Distributed Suspicious Response Code_Custom_Temporary	Block	2
66.249.79.10	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
37.26.148.219	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
87.69.166.175	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	2
66.249.79.16	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
157.55.39.103	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.79.232	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
216.223.27.30	United States	147.237.76.31	nakchal.idf.il	URL is Above Root Directory www.nakhal.idf.il/../images/shared/home.png	Block	1
185.3.144.234	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
66.249.65.80	Israel	147.237.76.147	chinuch.aka.idf.i	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	1
79.178.11.157	Israel	147.237.0.19	madim.atal.idf.il	Too Many 404: Response Code per Session	Block	1
208.115.113.89	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.79.16	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	1
46.121.116.116	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
82.145.211.188	Europe	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/www.navy.idf.il	Block	1
66.249.65.231	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
66.249.79.105	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/home/default.aspx	Block	1
212.179.21.194	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
46.121.193.138	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
87.69.166.175	Israel	147.237.72.156	aman.idf.il	PHP Attempt	Block	1
194.90.134.226	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
66.249.67.46	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1376-he/atal.aspx	Block	1
79.181.59.194	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/3/63903.pdf<o:p></o:p></p>	Block	1
66.249.79.107	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/home/default.aspx	Block	1
212.199.251.227	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
180.76.15.11	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/main.asp	Block	1
87.69.166.175	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/ajax/pages/fan_status.php	Block	1
2.54.133.213	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 2.54.133.213	Block	1
74.82.47.2	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to 147.237.72.156/	Block	1
194.114.146.227	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
151.80.31.116	Italy	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1

11-05-2015-08:04:06 to 11-05-2015-09:04:06