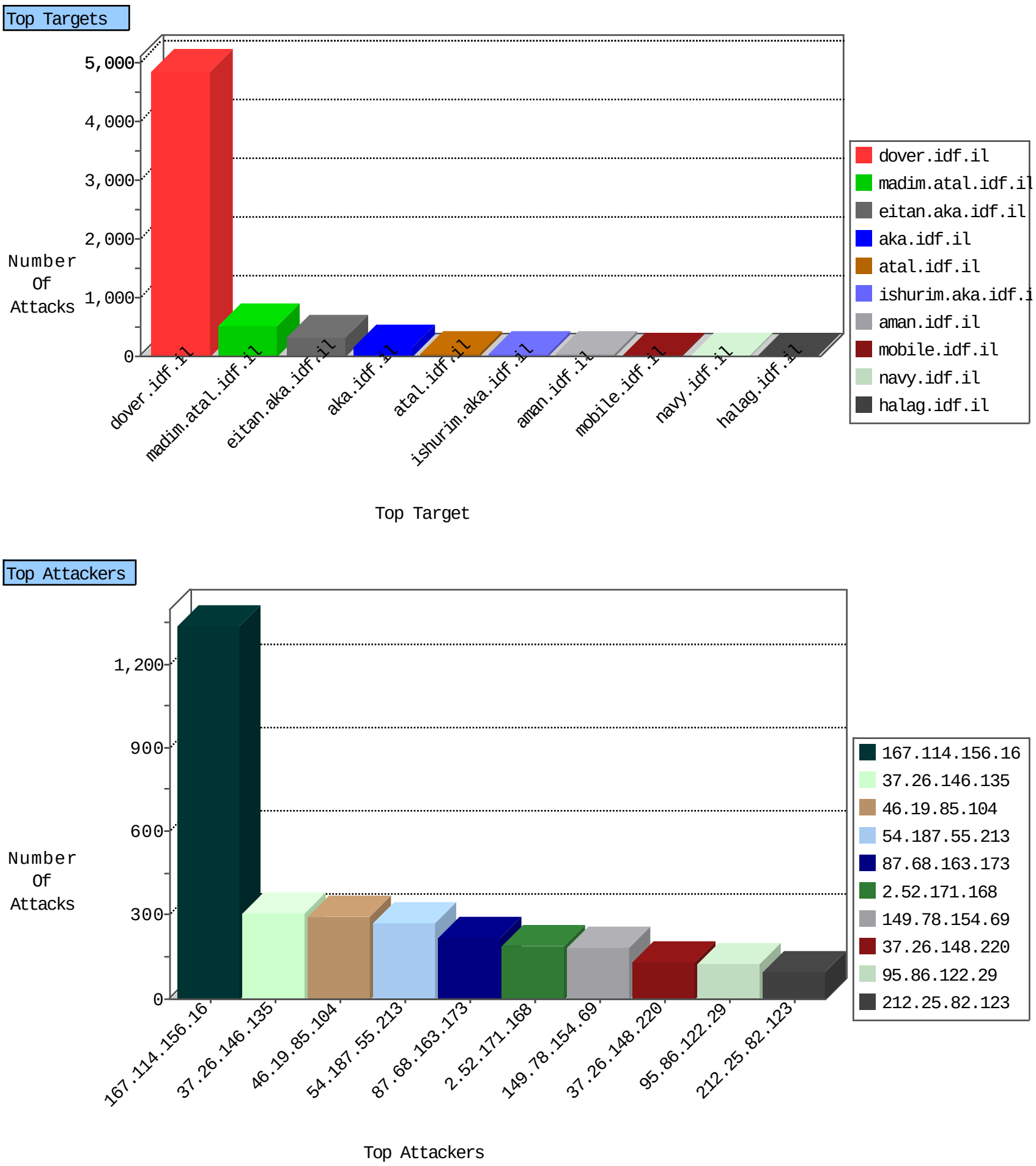
11-08-2015-07:04:05 to 11-08-2015-08:04:05

IDF Under Attack Daily Report



11-08-2015-07:04:05 to 11-08-2015-08:04:05

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	2315
66.249.67.6	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	475
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	155
81.218.241.25	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	94
5.102.227.122	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	17
46.117.106.75	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	13
212.117.143.29	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	12
176.12.145.225	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	11
46.19.86.71	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
99.238.51.128	Canada	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
24.206.250.76	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
2.52.60.251	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
147.236.138.212	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
80.246.137.216	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
212.179.224.96	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
176.12.149.219	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
185.27.105.65	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
79.176.2.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
176.13.7.234	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
51.36.103.181	United Kingdom	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
176.13.17.234	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
37.26.146.214	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
46.19.85.36	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
82.102.169.113	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
46.19.86.20	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
81.218.48.37	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
185.24.76.157	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
76.123.208.131	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
2.54.161.217	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
84.228.5.56	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1

11-08-2015-07:04:05 to 11-08-2015-08:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.65.4.204	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
5.9.89.170	Germany	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1

11-08-2015-07:04:05 to 11-08-2015-08:04:05

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	3
138.134.192.10	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
82.166.22.79	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
66.249.64.165	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	1
1.235.195.234	147.237.77.235	Korea, Republic of	sviva.idf.il	ET SCAN NMAP -sS window 4096	1
212.179.21.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
188.138.9.51	147.237.77.178	Germany	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
94.53.246.135	147.237.77.179	Romania	e.mazi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
66.249.73.212	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sA (2)	1

11-08-2015-07:04:05 to 11-08-2015-08:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
37.26.146.135	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	309
54.187.55.213	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	273
87.68.163.173	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	217
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	180
37.26.148.220	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	134
95.86.122.29	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	126
212.25.82.123	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	99
37.26.148.225	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	77
175.142.64.253	Malaysia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	75
37.26.148.201	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	69
2.54.141.160	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	59
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	59
46.19.86.71	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	50
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
210.46.79.1	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	46
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	45
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
84.229.157.7	Israel	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
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
74.141.163.215	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
66.102.8.238	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
46.19.85.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
107.223.140.164	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
85.65.244.190	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
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
66.249.93.216	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	27
46.19.85.42	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
131.253.35.149	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
46.19.86.4	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
37.26.146.207	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
2.52.60.251	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
76.123.208.131	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
157.55.39.31	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
66.102.8.233	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
212.235.98.139	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
66.102.8.243	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
66.249.65.231	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
2.54.131.158	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
66.249.65.224	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
157.55.39.175	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
185.24.76.157	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
24.206.250.76	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
162.157.68.29	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
79.182.20.114	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15

11-08-2015-07:04:05 to 11-08-2015-08:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.104	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	145
2.52.171.168	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	120
46.19.85.104	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	117
2.52.171.168	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.52.171.168	Block	73
46.19.85.104	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 46.19.85.104	Block	33
84.111.23.42	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	10
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	8
46.19.86.94	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	7
176.12.138.234	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
79.181.57.188	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	2
80.179.9.115	Israel	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
31.168.88.29	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	2
109.65.4.204	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 109.65.4.204	Block	2
199.16.156.125	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/sip_storage/files/9/size220x0/17479.jpg	Block	2
66.249.79.28	Israel	147.237.76.147	chinuch.aka.idf.i	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	1
176.13.9.150	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-he/dover.aspx	Block	1
66.249.67.13	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	1
207.46.13.20	United States	147.237.0.34	tikshuv.idf.il	Parameter Type Violation catId in www.tikshuv.idf.il/site/general.aspx	Block	1
109.67.66.207	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
62.0.34.177	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//resources/images/innerpage/goback.gif	Block	1
176.13.22.211	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
2.54.168.83	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
85.64.205.157	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/960.css	Block	1
66.249.67.13	Israel	147.237.72.166	aka.idf.il	Unknown Parameter 4d9c6f40 in www.aka.idf.il/main/kapatz/contactus.aspx	None	1
109.160.140.162	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
62.0.34.177	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 62.0.34.177	Block	1
184.105.247.195	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to 147.237.77.243/	Block	1
5.9.60.46	Germany	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
98.7.109.156	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to /tmunblock.cgi	Block	1
66.249.67.65	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
46.19.86.20	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	1
212.179.21.194	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
2.52.49.89	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	1
66.249.64.51	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8921-he/refuah.aspx	Block	1
185.24.76.157	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc	Block	1
66.249.67.71	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/mailbox.aspx	Block	1
46.19.86.71	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
220.181.108.141	China	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
176.12.145.79	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	1
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.65.231	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
109.65.4.204	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/1/	Block	1

11-08-2015-07:04:05 to 11-08-2015-08:04:05