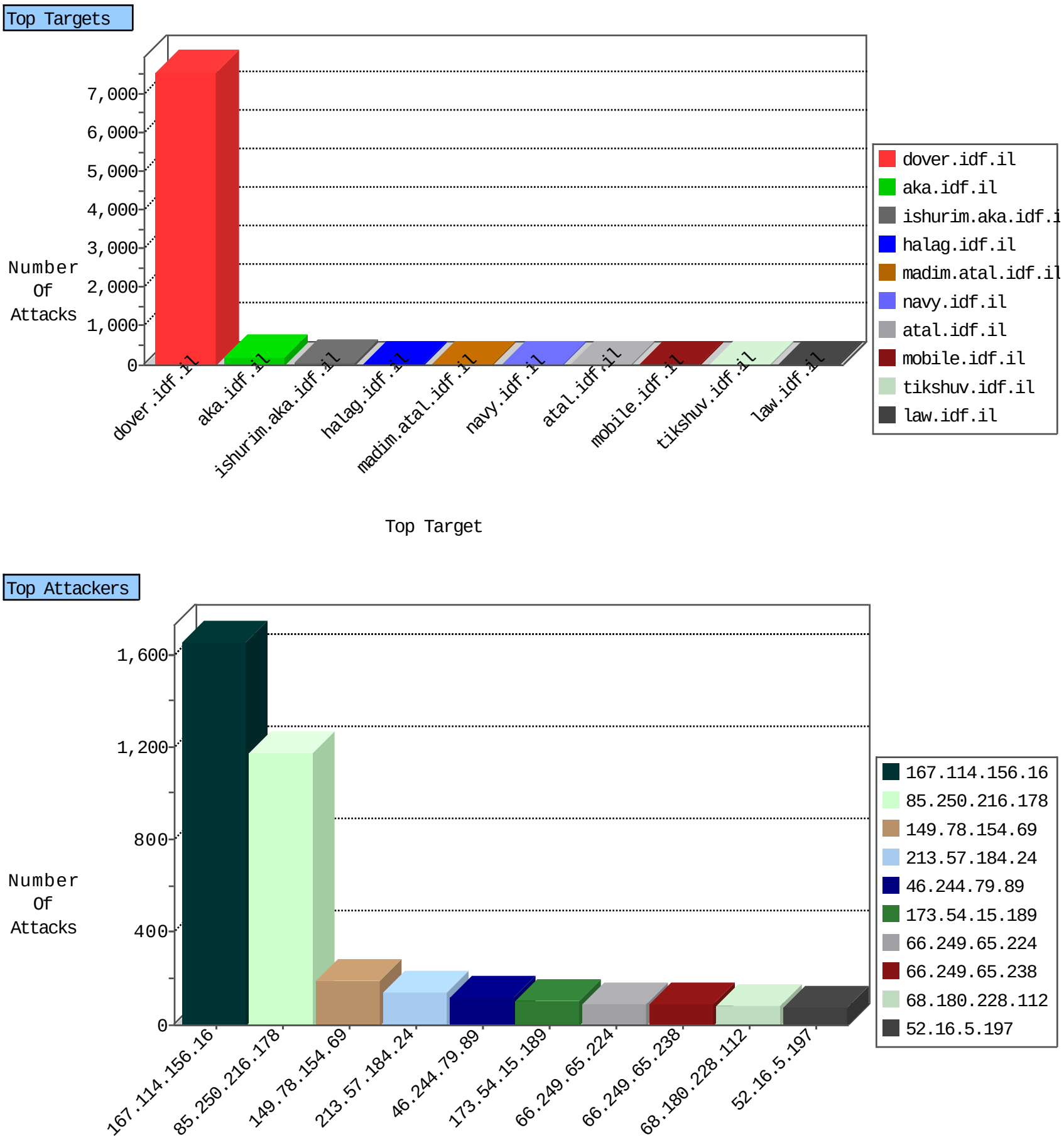
11-08-2015-23:04:09 to 11-09-2015-00:04:09

IDF Under Attack Daily Report



11-08-2015-23:04:09 to 11-09-2015-00:04:09

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	2712
220.181.108.101	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	60
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	54
5.102.246.108	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	30
46.121.254.205	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	23
109.186.61.112	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	20
46.19.85.107	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	20
2.52.53.26	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	15
185.32.179.125	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	12
176.106.227.244	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
100.38.183.54	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
84.110.192.196	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
77.125.15.174	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
78.190.117.249	Turkey	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
37.46.39.127	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
2.54.25.200	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
93.173.53.106	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
5.102.217.130	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
79.182.188.125	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
37.142.215.238	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
62.219.254.22	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
85.102.104.33	Turkey	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
5.29.77.226	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
109.66.106.147	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
14.192.205.176	Malaysia	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	2
46.19.86.168	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
146.185.239.100	Russian Federation	147.237.76.42	refuah.idf.il	block-sp-traf1	drop	1
2.54.173.245	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
2.54.175.120	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
192.168.2.103		147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	1
2.54.17.123	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
176.13.14.169	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1

11-08-2015-23:04:09 to 11-09-2015-00:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

11-08-2015-23:04:09 to 11-09-2015-00:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
77.125.118.187	147.237.72.166	Israel	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	22
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	8
213.151.32.163	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	8
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
66.249.67.13	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
66.249.64.186	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
66.249.64.191	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	1
122.114.17.100	147.237.77.178	China	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
122.114.17.100	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
122.114.17.100	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
199.101.186.134	147.237.76.198	United States	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
122.114.17.100	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
198.98.52.117	147.237.76.39	United States	mobile.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
116.58.237.195	147.237.8.28	Thailand	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
198.98.52.117	147.237.0.34	United States	tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
188.138.9.51	147.237.0.200	Germany	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
122.114.17.100	147.237.77.234	China	halag.idf.il	ET SCAN Potential SSH Scan	1
122.114.17.100	147.237.77.170	China	maarachot.idf.il	ET SCAN Potential SSH Scan	1
122.114.17.100	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1
199.101.186.134	147.237.76.198	United States	e.yohalan.idf.il	ET SCAN NMAP -sS window 2048	1
122.114.17.100	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
199.101.186.134	147.237.76.198	United States	e.yohalan.idf.il	ET SCAN NMAP -f -sS	1
119.55.73.40	147.237.0.33	China	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
198.98.52.117	147.237.76.31	United States	nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
198.98.52.117	147.237.0.19	United States	madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
188.138.9.51	147.237.72.166	Germany	aka.idf.il	ET SCAN NMAP -sS window 1024	1

11-08-2015-23:04:09 to 11-09-2015-00:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
85.250.216.178	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1177
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	189
213.57.184.24	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	140
46.244.79.89	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	118
173.54.15.189	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	104
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	83
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	77
79.182.56.91	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	76
89.35.91.68	Romania	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	75
79.182.211.31	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	70
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	70
66.249.93.200	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	66
66.249.93.196	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	65
79.180.59.27	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	59
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	57
46.19.85.17	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	56
187.64.235.206	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	50
202.62.119.130	Fiji	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	49
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
2.54.57.254	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	46
109.65.109.149	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	46
66.249.65.224	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	44
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
87.148.92.63	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
66.249.65.238	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	40
141.105.63.26	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
66.249.65.238	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
92.40.248.195	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
208.69.40.101	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
46.120.170.183	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
157.55.39.175	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
66.249.65.231	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
93.173.53.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
79.129.54.52	Greece	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
66.249.65.231	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
46.19.86.218	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
185.3.144.96	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
66.249.81.218	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
176.13.14.70	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
46.117.122.138	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
77.126.113.187	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	27
109.186.61.112	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
66.249.65.224	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
40.77.167.2	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
207.46.13.169	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
2.54.17.123	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
149.78.90.228	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.81	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	20
176.12.139.186	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
40.77.167.105	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	3
77.125.118.187	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
37.26.146.139	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 37.26.146.139	Block	2
109.66.13.200	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.120.46.55	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	2
37.26.146.139	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/eng	Block	1
114.98.237.246	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/1819-he/idfg.aspx/trackback/	Block	1
66.249.69.41	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/71538-he/maarachot.aspx	Block	1
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
213.188.52.57	Switzerland	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
46.19.85.121	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	1
2.54.63.89	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
87.68.61.66	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
66.249.67.13	Israel	147.237.72.166	aka.idf.il	Unknown Parameter pop in www.aka.idf.il/main/home/	None	1
46.244.79.89	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/894-ar	Block	1
37.142.172.191	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
149.78.25.104	Israel	147.237.72.167	ishurim.aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
66.249.65.231	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
46.19.85.147	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1135-he/atal.aspx	Block	1
2.54.63.231	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1136-he/atal.aspx	Block	1
107.150.43.206	United States	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on www.cloud.ph/	Block	1
66.249.67.48	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/894-he/nakhal.aspx	Block	1
61.135.190.71	China	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	1
40.77.167.42	United States	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
77.126.113.187	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
66.249.67.6	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.19.86.117	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/hinuch	Block	1
5.29.136.159	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
109.65.129.119	Israel	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/giyus/general.aspx	Block	1
61.135.190.200	China	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.15/	Block	1
183.79.222.1	Japan	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
79.180.55.33	Israel	147.237.0.34	tikshuv.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 79.180.55.33	Block	1
66.249.67.13	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.117.62.166	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.67.129	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/	Block	1
62.210.88.201	France	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.google.pl/search	Block	1
185.32.179.113	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
86.96.24.129	United Arab Emirates	147.237.77.216	dover.idf.il	Unknown HTTP Request Method COOK in URL www.idf.il/1133-20835-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/1151-he/chinuch.aspx	Block	1

11-08-2015-23:04:09 to 11-09-2015-00:04:09