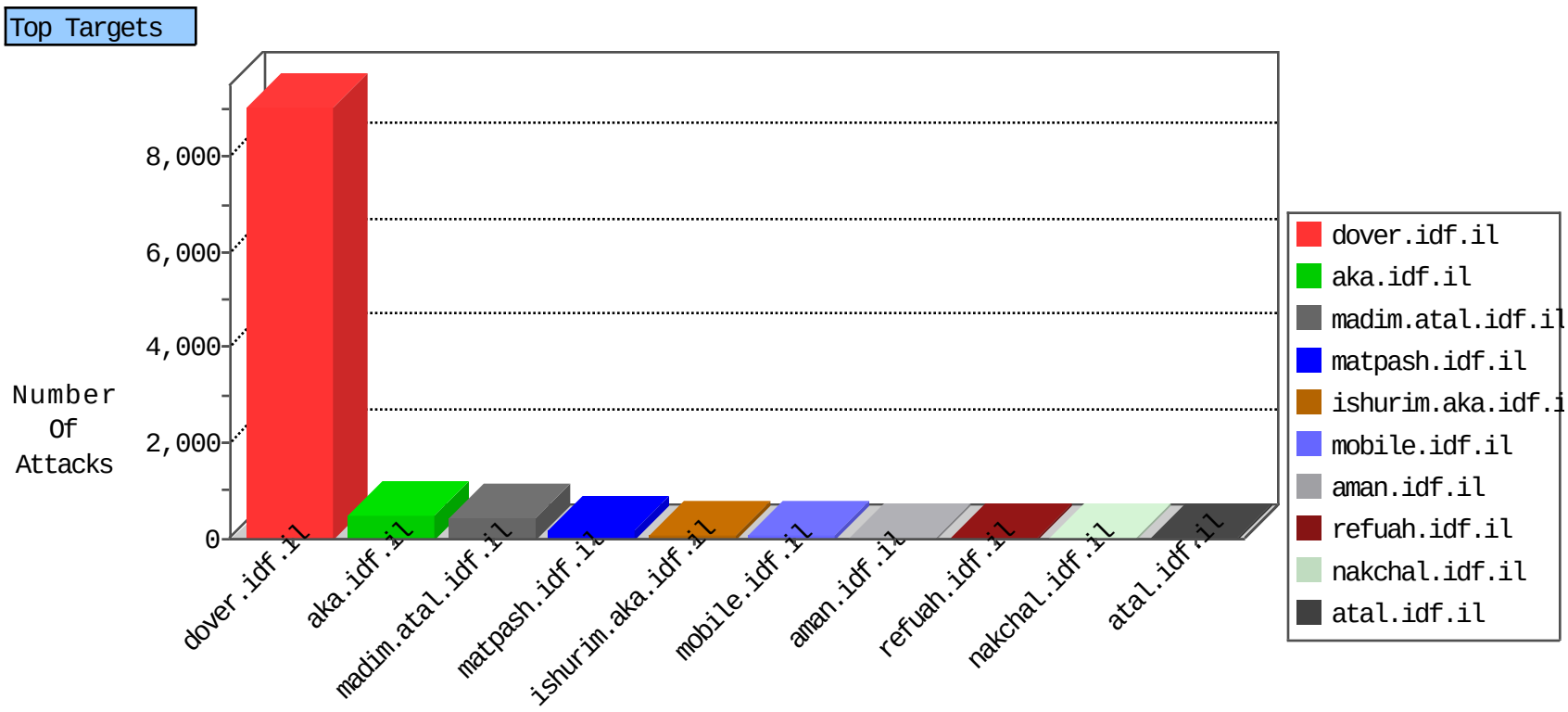
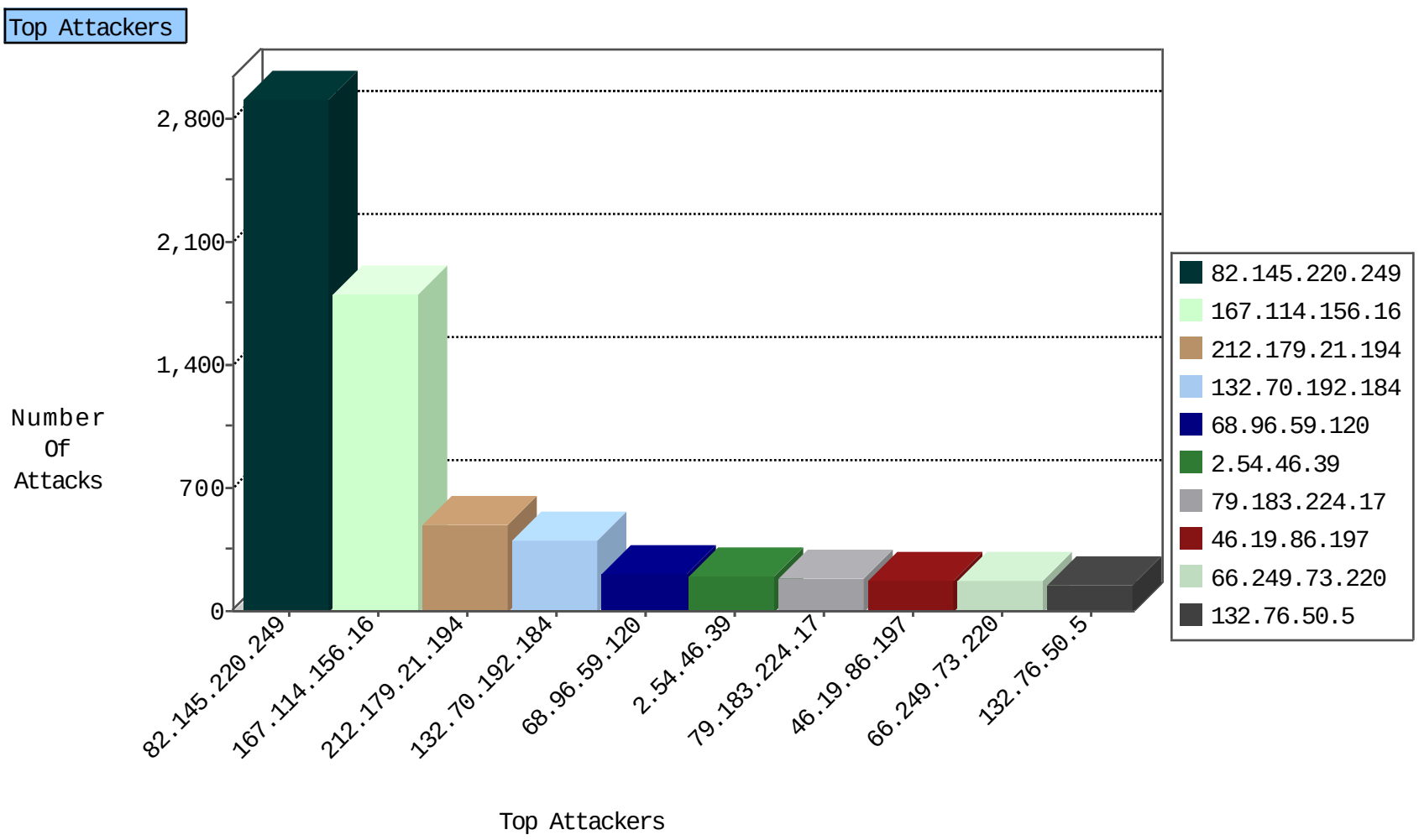
11-08-2015-16:04:01 to 11-08-2015-17:04:01

IDF Under Attack
Daily Report





11-08-2015-16:04:01 to 11-08-2015-17:04:01

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	2900
46.19.85.249	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	232
81.218.37.2	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	216
192.118.30.102	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	150
46.19.85.242	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	36
212.179.21.194	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	30
109.65.123.42	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	25
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	16
2.54.180.206	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
138.134.192.10	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
24.214.201.114	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
62.219.254.22	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	6
109.66.48.171	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
109.67.8.188	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
2.54.180.206	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
2.54.180.206	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
192.115.252.2	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
134.147.203.115	Germany	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	4
2.54.184.176	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
213.57.63.12	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
82.145.220.249	Europe	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
81.218.56.245	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	3
37.142.185.10	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
213.57.203.115	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
134.147.203.115	Germany	147.237.76.39	mobile.meitav.idf.il	Block_Ntp_All_Net	drop	2
112.133.243.202	India	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
212.179.21.194	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
149.78.151.8	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
82.145.220.249	Europe	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
138.134.192.10	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
132.70.192.184	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
85.64.21.229	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
146.185.239.100	Russian Federation	147.237.77.226	www.chamatz.aka.idf.il	block-sp-traf1	drop	1
176.12.150.107	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
66.249.65.231	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
132.64.208.164	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
71.6.167.142	United States	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1

11-08-2015-16:04:01 to 11-08-2015-17:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.186.27.195	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5

11-08-2015-16:04:01 to 11-08-2015-17:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.73.220	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sA (2)	166
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	5
79.182.168.108	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.64.191	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	1
31.6.71.154	147.237.77.61	Poland	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
176.13.15.162	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.246.140.243	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.121.135.120	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
31.168.9.50	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.152.119	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.179.28.34	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
176.13.1.251	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

11-08-2015-16:04:01 to 11-08-2015-17:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
82.145.220.249	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2911
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	474
132.70.192.184	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	403
68.96.59.120	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	214
79.183.224.17	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	189
46.19.86.197	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	176
132.76.50.5	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	139
95.86.118.224	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	98
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	80
31.168.153.31	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	75
77.127.150.111	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	69
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	58
37.26.148.149	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	53
73.199.19.220	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	47
157.55.39.175	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	45
41.101.118.155	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
46.19.85.249	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
40.77.167.2	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
100.100.102.140		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	37
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
46.19.85.244	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	35
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
79.180.181.137	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
149.78.151.8	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
108.72.13.144	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
40.77.167.9	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
212.179.155.129	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
97.100.149.238	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
155.56.68.217	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
23.27.248.173	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	27
79.181.97.189	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
100.100.109.74		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	26
40.77.167.82	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
84.228.11.8	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
2.54.42.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
24.214.201.114	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
184.145.57.110	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
66.249.65.231	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
66.249.65.238	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
81.218.37.2	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	20
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
157.55.39.147	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
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
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
5.22.131.239	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
46.19.86.225	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	17

11-08-2015-16:04:01 to 11-08-2015-17:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.46.39	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	130
37.142.132.133	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	75
2.54.139.193	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	67
2.54.46.39	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	56
132.72.138.1	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 132.72.138.1	Block	46
79.181.60.237	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	40
37.142.132.133	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 37.142.132.133	Block	14
109.65.123.42	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giys	Block	12
132.72.138.1	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/resources/images/	Block	8
46.19.86.144	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	7
96.239.94.196	United States	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	5
46.19.86.106	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
2.54.153.48	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
37.26.149.179	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.136	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.149.213	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.17.247	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
85.250.55.183	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.117.63.247	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.6.70	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.156	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
82.102.169.210	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
109.186.40.244	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/_blank	Block	2
46.19.86.250	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
213.57.203.115	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	2
66.249.79.28	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
46.19.86.137	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
62.0.103.156	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
80.246.136.240	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.67.122	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catid in www.aka.idf.il/main/rabanut/general.aspx	None	1
37.142.132.133	Israel	147.237.0.19	madim.atal.idf.il	Cookie Tampering on cookie _pk_ref.322.9cd2: Expected ["","",1446980945,"https://www.google.co.il/"], Observed ["","",1446992400,"https://www.google.co.il/"]	None	1
188.40.11.194	Germany	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 188.40.11.194	Block	1
62.219.193.62	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/	Block	1
87.69.0.204	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/https:/www.aman.idf.il/	Block	1
46.19.85.78	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method q34baw in URL	Block	1
79.176.98.173	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	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
5.29.250.70	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	1
62.210.88.201	France	147.237.77.234	halag.idf.il	Unauthorized URL Access to 51.254.206.142/httptest.php	Block	1
80.246.139.27	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
194.90.66.15	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	1
66.249.67.242	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
142.54.174.70	United States	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to www.cloud.ph/	Block	1
66.249.64.56	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9841-he/refuah.aspx	Block	1
46.120.56.59	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	1
93.173.247.216	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
66.249.67.59	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
176.13.7.74	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
62.210.88.201	France	147.237.77.235	sviva.idf.il	Unauthorized URL Access to 51.254.206.142/httptest.php	Block	1
109.67.105.132	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1

11-08-2015-16:04:01 to 11-08-2015-17:04:01