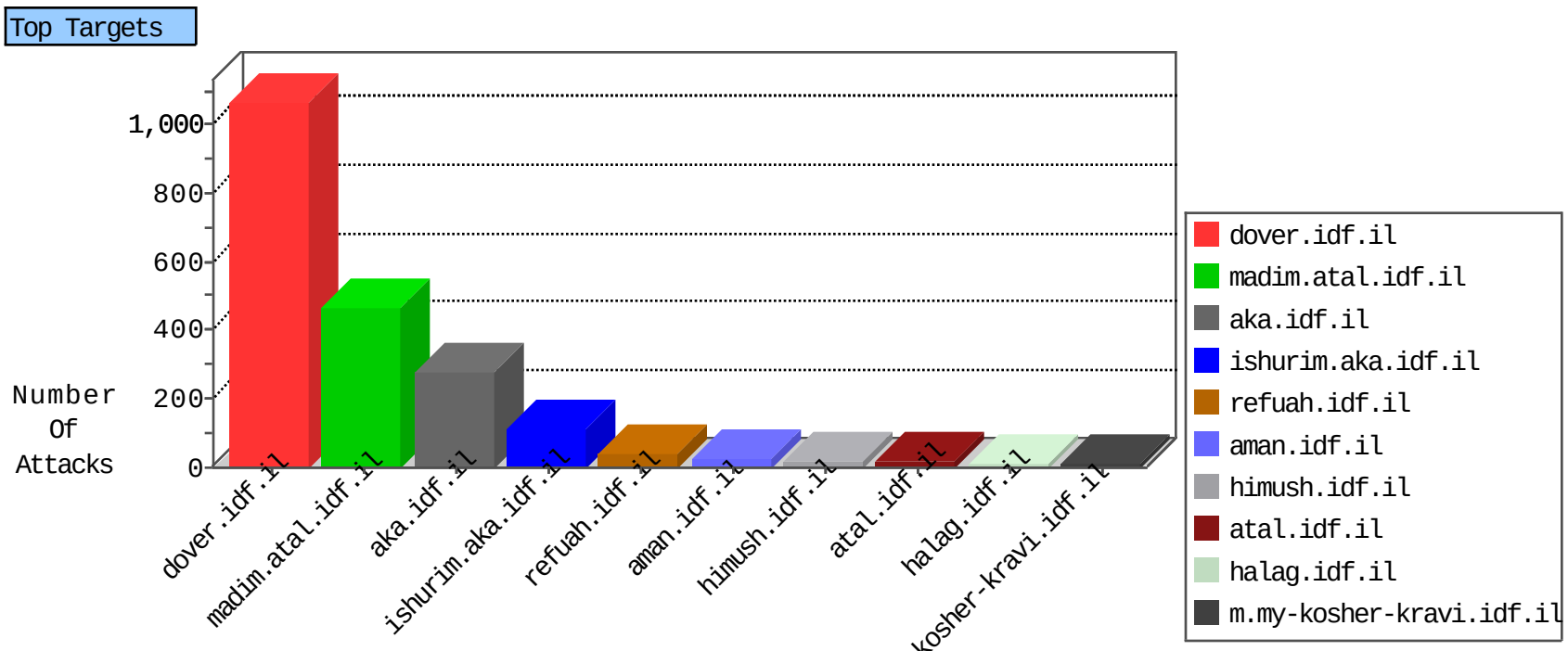
11-24-2015-08:04:00 to 11-24-2015-09:04:00

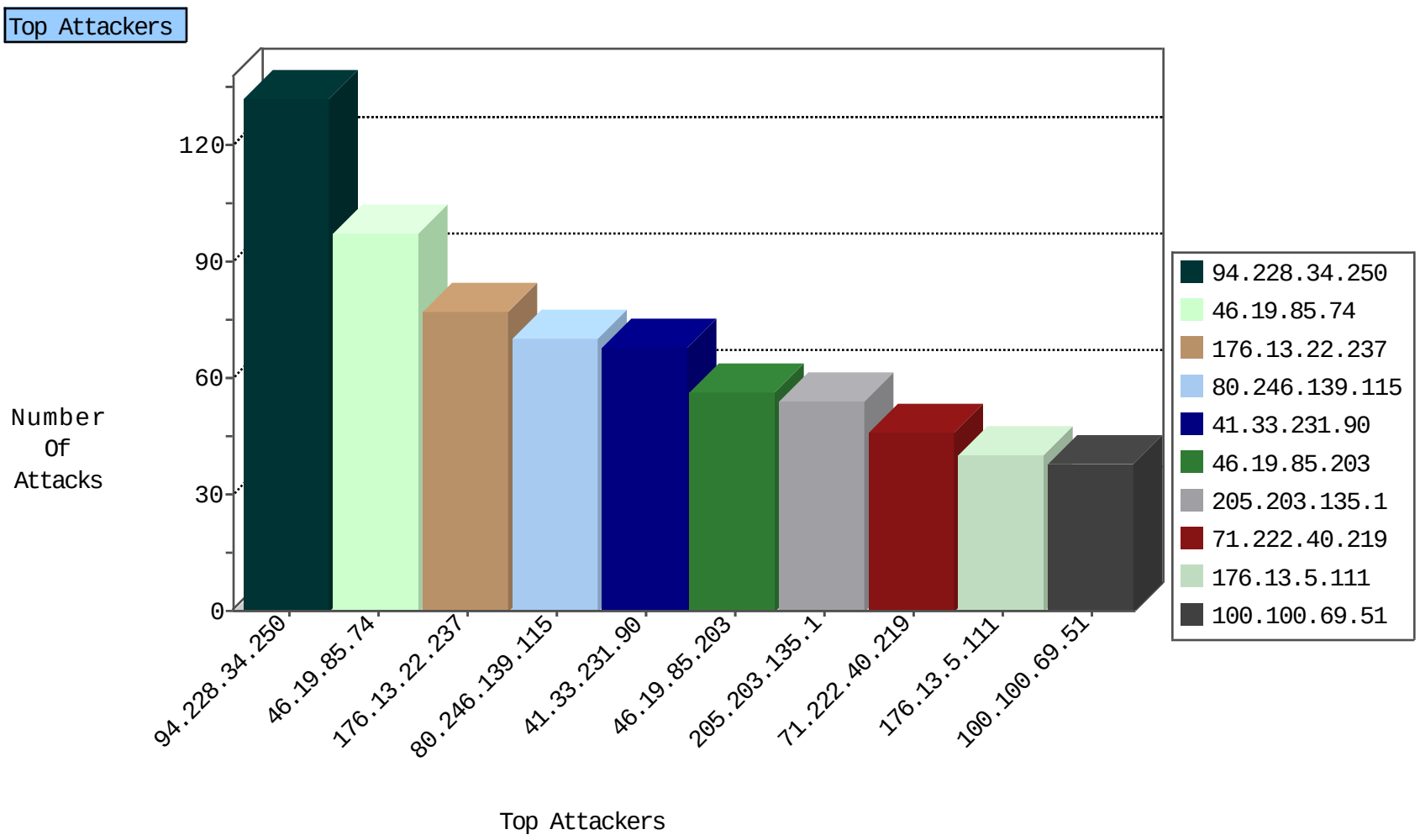
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

11-24-2015-08:04:00 to 11-24-2015-09:04:00

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	5
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
37.26.147.162	Israel	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	2
114.80.122.91	China	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	1
185.106.94.28		147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	1
47.88.56.170	Canada	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1

11-24-2015-08:04:00 to 11-24-2015-09:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
62.210.250.215	France	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
188.165.15.127	France	147.237.77.170	maarachot.idf.il	C228: HTTP: AhrefBot crawler	Block	1
195.154.187.115	France	147.237.77.74	law.idf.il	C1000106: HTTP: majestic bot	Block	1

11-24-2015-08:04:00 to 11-24-2015-09:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
66.249.66.109	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
109.67.107.6	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
94.230.86.129	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.117	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.72.156	China	aman.idf.il	ET SCAN Potential SSH Scan	1
31.154.92.164	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
208.115.111.73	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1
109.235.254.181	147.237.77.19	Turkey	law-forum.idf.il	ET SCAN NMAP -sS window 4096	1
104.192.0.226	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sS window 1024	1
79.181.111.204	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.117	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
58.249.25.15	147.237.77.176	China	matpash.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
31.6.71.154	147.237.72.14	Poland	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1

11-24-2015-08:04:00 to 11-24-2015-09:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
94.228.34.250	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	132
46.19.85.74	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	95
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	54
71.222.40.219	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	46
100.100.69.51		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	38
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
206.190.158.75	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
176.12.140.63	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	31
41.33.231.90	Egypt	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	SAM rule	drop	29
108.59.253.71	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
94.230.85.236	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
100.100.4.230		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
183.79.219.165	Japan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
66.249.79.75	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
114.23.235.61	New Zealand	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
179.43.141.241	Switzerland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
5.255.253.158	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
199.30.24.85	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
149.88.229.76	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
212.179.9.245	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
198.58.103.102	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
37.140.141.2	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
66.249.81.215	Russian Federation	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
95.108.158.171	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
5.255.253.168	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
5.255.253.150	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
80.178.208.185	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
87.203.98.130	Greece	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
66.249.81.212	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
79.182.171.188	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
157.55.39.227	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop		drop	10
220.255.98.33	Singapore	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
212.235.69.34	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
212.235.98.139	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	9
82.102.169.113	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
219.74.38.243	Singapore	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
37.26.148.147	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
128.242.249.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
81.218.198.236	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
46.19.85.96	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
173.252.122.117	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
37.26.146.208	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.86.73	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
176.13.5.111	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
5.255.253.157	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8

11-24-2015-08:04:00 to 11-24-2015-09:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.22.237	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	66
80.246.139.115	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	56
46.19.85.203	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	54
80.246.139.190	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	37
85.250.198.1	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	35
176.13.5.111	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	32
80.246.139.67	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	30
80.246.139.82	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	28
2.54.139.95	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	19
80.246.139.214	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	17
176.13.22.237	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 176.13.22.237	Block	10
82.166.137.19	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/$$$&?&?$$$	Block	8
80.246.139.115	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 80.246.139.115	Block	8
85.65.46.57	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	7
80.246.139.115	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
2.54.176.131	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
2.54.146.165	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
80.246.140.56	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
211.123.214.30	Japan	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 211.123.214.30	Block	4
185.32.179.66	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	4
80.246.140.204	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	4
80.246.140.204	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	3
176.13.9.136	Israel	147.237.76.31	nakchal.idf.il	Parameter Type Violation search in www.nakhal.idf.il/1072-he/nakhal.aspx	Block	3
80.246.140.236	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
176.13.9.204	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
176.13.1.252	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
84.108.237.95	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
80.246.140.136	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	3
80.246.136.217	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
46.19.85.203	Israel	147.237.0.19	madim.atal.idf.i	Parameter Type Violation ctl00$ContentPlaceHolder1$txtCity in madim.atal.idf.il/mobile/1088-he/meretz.aspx	Block	2
2.54.99.15	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.19.86.57	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
80.246.140.136	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
85.250.138.148	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
80.246.140.136	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	2
46.19.86.238	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.19.85.56	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
185.32.179.74	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
176.12.140.63	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
37.26.148.246	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.66.69	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/idkonim/pages/ayosh15092010.aspx	Block	1
2.52.170.181	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.85.243	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.19.85.199	Israel	147.237.76.42	refuah.idf.il	Abnormally Long Request method	Block	1
109.253.90.65	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/giyus/login.aspx	None	1
66.249.79.79	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/international_training	Block	1
199.16.156.126	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/1/size220x0/16641.jpg	Block	1

11-24-2015-08:04:00 to 11-24-2015-09:04:00