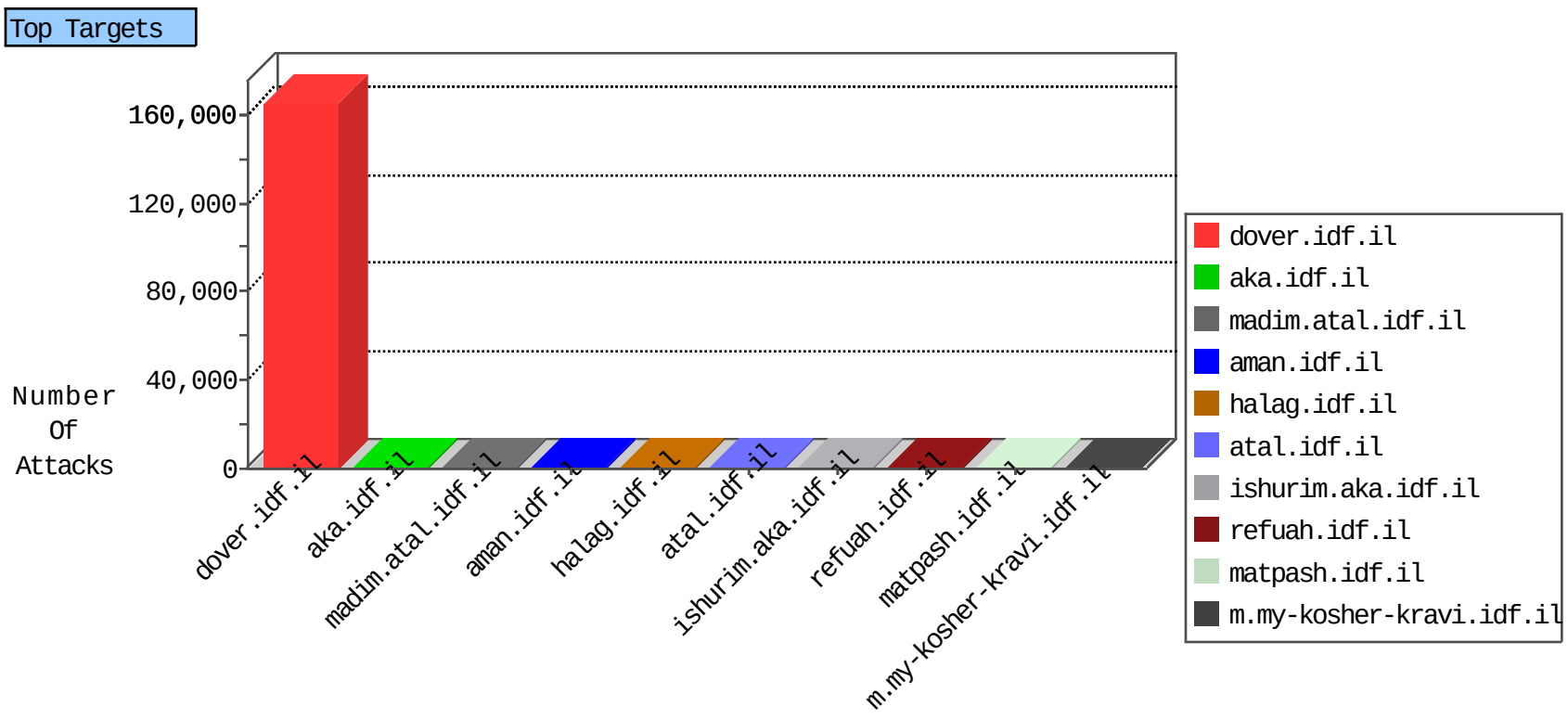
11-17-2015-19:04:06 to 11-17-2015-20:04:06

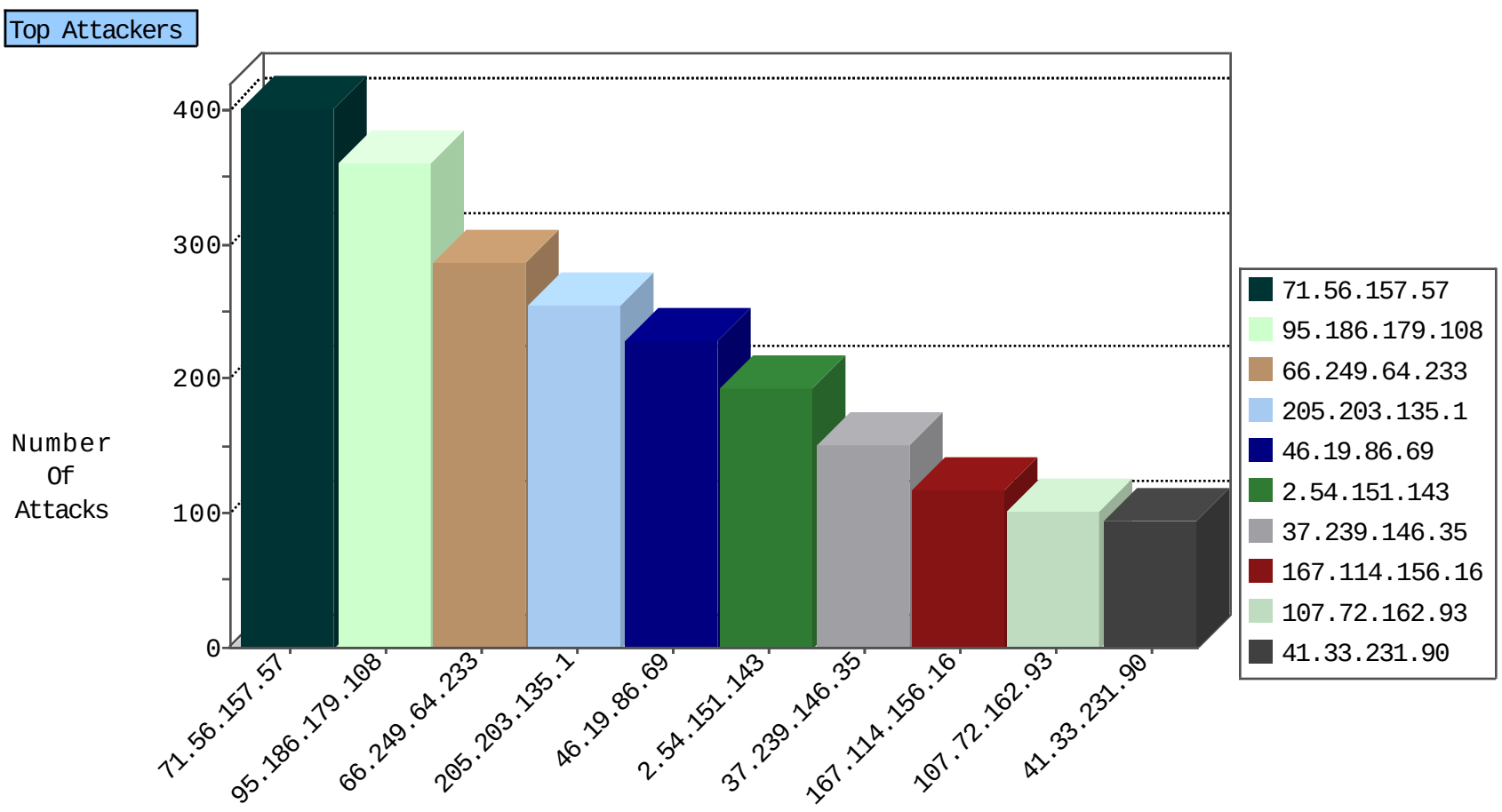
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

11-17-2015-19:04:06 to 11-17-2015-20:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	10086
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	1715
95.186.179.108	Saudi Arabia	147.237.77.216	dover.idf.il	DOS-LOIC-TCP-80-cat	dest-reset	421
204.93.154.216	United States	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	228
192.118.30.102	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	118
46.19.85.174	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	18
31.168.157.119	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
89.138.227.231	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
181.65.103.205	Peru	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6
93.172.1.134	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
77.127.128.142	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	4
95.186.179.108	Saudi Arabia	147.237.77.216	dover.idf.il	Frk_Purple_Con_Limit_Http	drop	3
46.117.100.110	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
95.186.179.108	Saudi Arabia	147.237.77.216	dover.idf.il	Frk_Under_Attack_Con_Http	drop	2
72.209.227.74	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
187.103.107.7	Brazil	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
31.208.81.44	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
94.135.207.121	Germany	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
5.22.129.98	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
89.233.198.3	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
69.6.134.89	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
174.95.7.56	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
64.68.241.37	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
146.6.31.53	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
86.48.101.42	Denmark	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
83.233.116.22	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
216.114.56.18	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
63.248.34.100	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
105.235.107.123	Cote D'Ivoire	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
46.9.172.16	Norway	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
94.255.219.124	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
74.115.59.96	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
201.209.228.106	Venezuela	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
69.168.186.41	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
185.3.108.26	Italy	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
94.47.129.118	Italy	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
66.129.57.88	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
172.97.247.10		147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
85.89.88.114	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
63.248.181.20	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
128.111.162.60	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
96.49.0.71	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
78.154.149.75	Latvia	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
209.40.158.96	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
73.55.88.44	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
188.113.122.66	Norway	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
37.130.38.116	Poland	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
94.245.37.99	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
5.144.0.37	Switzerland	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1

11-17-2015-19:04:06 to 11-17-2015-20:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.108.249.168	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
23.91.70.63	United States	147.237.77.233	atal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	1

11-17-2015-19:04:06 to 11-17-2015-20:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	**Signature**	**Count**

11-17-2015-19:04:06 to 11-17-2015-20:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
71.56.157.57	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	402
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	255
66.249.64.233	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	250
46.19.86.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	228
37.239.146.35	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	151
107.72.162.93	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	102
173.231.115.59	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	84
54.224.21.23	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	84
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	68
173.220.141.227	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	68
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	65
66.249.64.238	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	55
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	52
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	52
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
52.0.238.61	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
66.249.64.243	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
202.3.255.8	French Polynesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
109.186.186.211	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
213.57.138.140	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	36
86.176.229.80	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
213.57.140.40	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	31
213.57.140.40	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	29
66.249.64.233	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
83.183.218.48	Sweden	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
162.243.199.26	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
192.117.150.233	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	23
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
128.242.249.11	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
77.126.167.209	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	21
93.169.168.206	Romania	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop		drop	20
178.63.165.187	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
31.51.118.217	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
109.65.140.42	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
100.100.98.238		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	18
208.69.40.101	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
213.204.101.24	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
5.102.254.19	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
66.249.69.128	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
69.175.127.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
52.68.136.185	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
66.249.93.192	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
37.201.168.1	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
50.49.182.199	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	13
46.19.85.17	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	13
109.67.102.7	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
2.54.151.143	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
139.162.216.112	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12

11-17-2015-19:04:06 to 11-17-2015-20:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.151.143	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	103
176.12.150.248	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	83
2.54.151.143	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	78
176.13.5.184	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	77
185.32.179.241	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	57
176.106.226.53	Israel	147.237.72.166	aka.idf.il	Distributed Unknown HTTP Request Method	Block	35
185.32.179.241	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	13
37.26.149.128	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
5.28.170.119	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 5.28.170.119	Block	4
79.183.126.16	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	4
80.246.136.239	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
79.183.126.16	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/pages/fan_status.php	Block	4
37.26.147.168	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.67.102.7	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	3
176.12.137.138	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
89.138.84.59	Israel	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	3
89.138.84.59	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/ajax/pages/fan_status.php	Block	3
176.13.14.243	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.12.150.171	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
93.172.59.88	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/pages/fan_status.php	Block	2
176.12.146.230	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 176.12.146.230	None	2
46.19.85.63	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	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
79.183.126.16	Israel	147.237.77.234	halag.idf.il	PHP Attempt	Block	2
46.19.85.145	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.228.197.176	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
109.186.49.137	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.183.126.16	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/ajax/pages/fan_status.php	Block	2
93.172.59.88	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	2
31.154.150.3	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 31.154.150.3	Block	1
82.81.0.32	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	1
62.25.16.234	Netherlands	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to /	Block	1
149.88.90.240	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	1
46.121.140.55	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Header Name	Block	1
109.66.25.250	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
5.28.166.77	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl41 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
79.182.173.151	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.106.226.97	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.86.193	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
95.86.81.68	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/&sa=u&ved=0cacqfjaaahukewi7ol-phzjjahvfwbqkhswicbq&usg=afqjcngd2jl649buwom7nwtttq1ultb2da	Block	1
2.54.8.41	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
77.125.96.12	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.65.37	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/14-3182-he	Block	1
173.252.81.118	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
40.77.167.96	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/0/	Block	1
85.250.180.112	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
5.29.156.200	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	1
80.246.136.222	Israel	147.237.72.166	aka.idf.il	Too Many 403: Response Code per Session	Block	1
46.121.140.55	Israel	147.237.72.166	aka.idf.il	NULL Character in URL y[[#14]][[#17]]ÂŸ•>×›â€˜Â¦ÂŒ×″ 5Ö½`is2[[#23]][[#22]]×?:w-)Â£aâ€šxxÂ£×š[[#20]]Â¶Â?×¤mâ€ ¡Ö´Â¶Â¯"×′Ã™Ö¾â€˜[[#0]]â€¢<Ã?Â â€˜rm×²	Block	1
128.232.110.28	United Kingdom	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.15/	Block	1

11-17-2015-19:04:06 to 11-17-2015-20:04:06