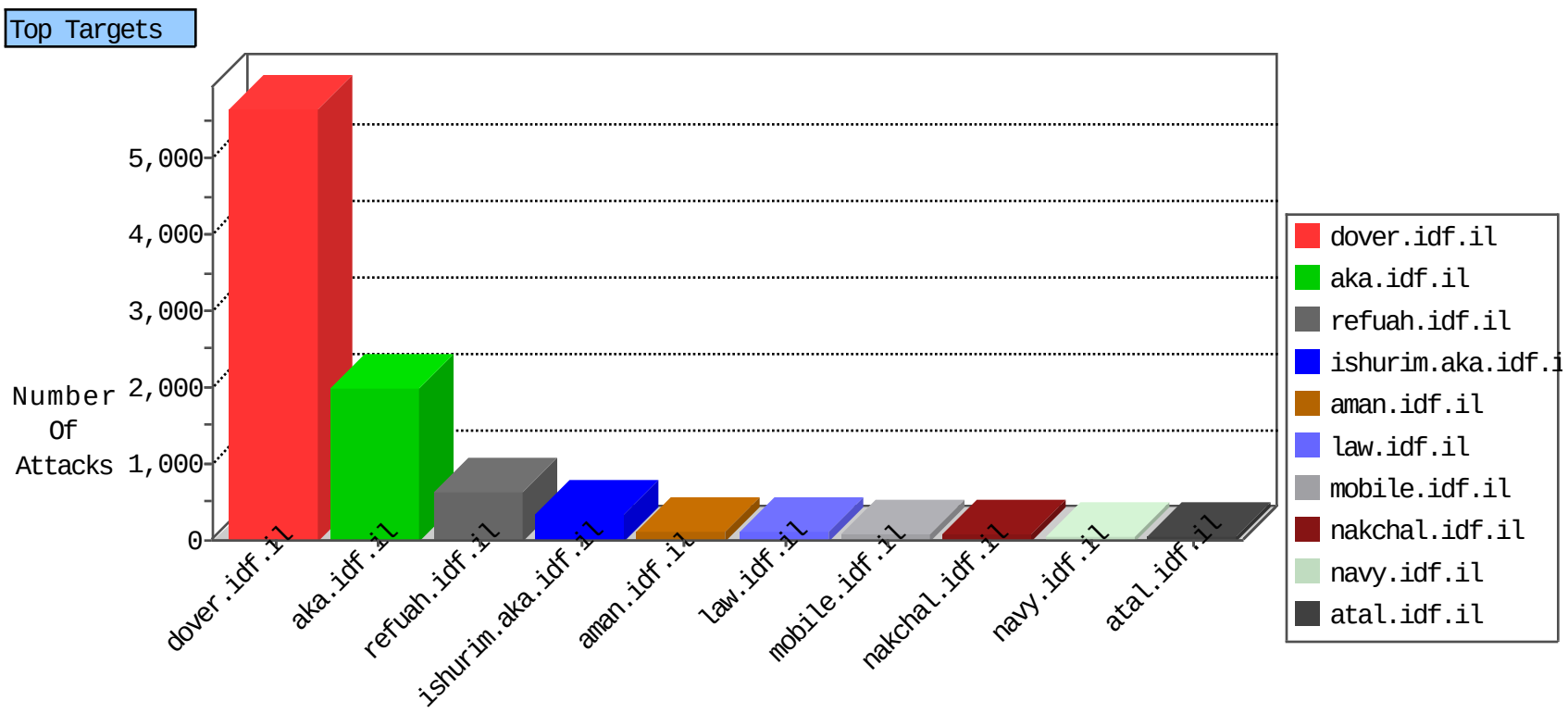
10-26-2015-13:04:09 to 10-26-2015-14:04:09

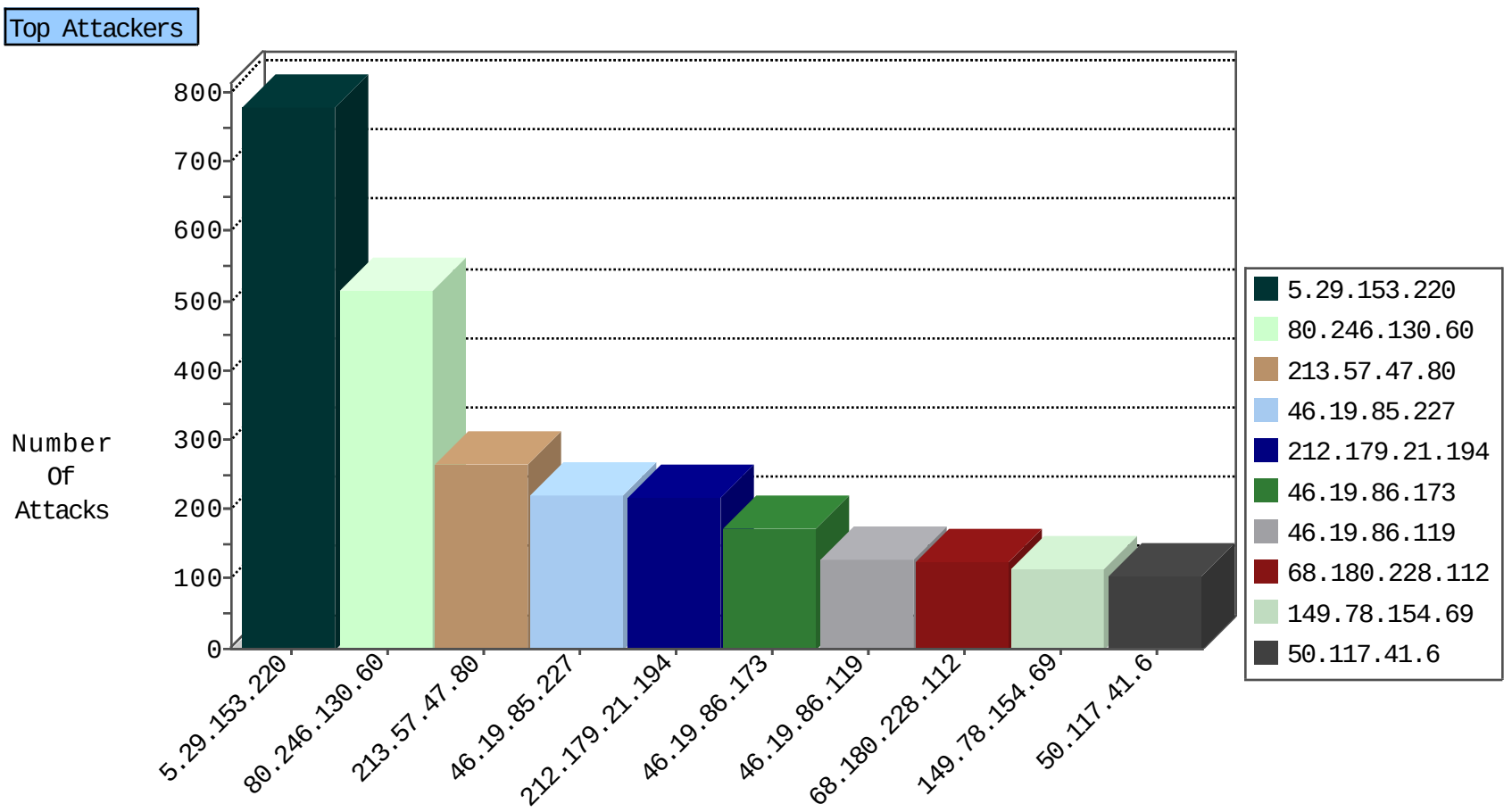
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

10-26-2015-13:04:09 to 10-26-2015-14:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.29.153.220	Israel	147.237.72.166	aka.idf.il	TCP Scan (vertical)	drop	3577
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	782
66.249.67.53	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	509
80.246.136.59	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	183
77.127.196.198	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	124
84.228.2.171	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	37
85.250.0.77	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	35
5.29.201.53	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	29
2.54.29.26	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	25
138.134.102.15	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	25
89.139.174.197	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	25
77.126.72.108	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	25
176.13.13.190	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	22
79.180.38.190	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	15
2.54.140.154	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	15
46.116.202.23	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	14
128.139.23.33	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	13
212.25.84.200	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	12
5.28.149.236	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	12
37.26.147.249	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	12
41.191.80.4	Egypt	147.237.77.216	dover.idf.il	SYN Flood full table	drop	11
79.177.207.109	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
212.179.166.210	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
176.13.19.146	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
81.218.116.230	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
212.150.249.184	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
2.54.43.194	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
80.246.139.10	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
84.94.199.6	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
46.19.86.151	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
192.116.236.181	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
46.120.210.187	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
213.57.235.254	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
82.166.148.88	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
81.218.20.161	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
84.94.198.64	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
212.179.239.194	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
212.76.105.29	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
2.54.179.81	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
212.179.46.16	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
85.64.110.176	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
46.19.86.86	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
89.138.94.36	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
62.219.233.89	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
46.19.85.187	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
85.64.207.51	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
46.19.85.227	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
37.26.149.163	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
109.67.13.137	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
109.160.217.22	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5

10-26-2015-13:04:09 to 10-26-2015-14:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

10-26-2015-13:04:09 to 10-26-2015-14:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
5.29.153.220	147.237.72.166	Israel	aka.idf.il	ET SCAN NMAP -sS window 1024	58
5.29.153.220	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	4
37.142.68.36	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
37.26.149.173	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
169.54.233.119	147.237.72.166	Netherlands	aka.idf.il	ET SCAN NMAP -sS window 1024	1
115.236.75.201	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
2.54.12.121	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
94.102.48.194	147.237.76.147	Netherlands	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
84.228.93.47	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
66.249.67.59	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
217.194.206.113	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
58.110.100.144	147.237.77.216	Australia	dover.idf.il	portscan: TCP Distributed Portscan	1
205.252.110.19	147.237.77.216	United Kingdom	dover.idf.il	portscan: TCP Distributed Portscan	1
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	1
199.101.186.159	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sS window 3072	1
37.142.64.35	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
192.146.6.2	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1
115.236.75.201	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
5.29.45.21	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
94.102.48.194	147.237.76.201	Netherlands	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
85.64.110.176	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.108.154.236	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
62.219.164.106	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
213.57.235.254	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.119	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
199.203.62.15	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

10-26-2015-13:04:09 to 10-26-2015-14:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
80.246.130.60	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	498
213.57.47.80	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	252
46.19.85.227	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	187
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	186
46.19.86.173	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	174
46.19.86.119	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	126
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	114
50.117.41.6	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	105
46.19.86.95	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	96
41.215.1.62	Kenya	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	79
46.19.86.249	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	72
84.111.217.248	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	67
95.86.76.62	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	66
185.58.201.28	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	62
85.65.154.212	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	61
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	58
81.218.20.161	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	57
109.65.104.229	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	56
46.19.86.7	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	54
84.228.61.231	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	53
212.235.53.206	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	53
212.235.37.72	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
46.19.86.132	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	47
5.156.216.47	Romania	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	47
41.218.184.141	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	47
213.8.130.204	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	46
213.151.48.80	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	45
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	45
37.26.147.249	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
212.150.249.184	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
84.228.42.13	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
46.19.85.230	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
212.143.3.44	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
212.25.84.200	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
41.191.80.4	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
93.173.233.91	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
166.137.8.23	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
213.14.96.122	Turkey	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
2.52.60.160	Israel	147.237.76.31	nakchal.idf.il	drop	First packet isn't SYN	drop	33
82.145.218.224	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
46.19.86.58	Israel	147.237.72.156	aman.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
212.179.46.16	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
132.70.66.11	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
46.19.86.151	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
46.19.86.178	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
176.106.227.141	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
132.70.66.14	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
46.19.86.66	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25

10-26-2015-13:04:09 to 10-26-2015-14:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
68.180.229.239	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	84
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	68
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	56
84.228.142.227	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.228.142.227	Block	28
87.69.87.39	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtAreaRemarks in m.my-kosher-kravi.idf.il/templates/training/training.aspx	Block	28
46.19.86.116	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	28
192.115.97.253	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.115.97.253	Block	28
194.90.83.233	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-he/	Block	26
188.165.15.205	France	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/163-5860-he/patzar.aspx	Block	14
66.249.67.142	Israel	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/	Block	14
132.70.66.11	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	14
64.41.200.102	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/	Block	14
46.19.86.12	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/	Block	14
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	14
193.106.54.36	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	14
66.249.67.65	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	14
176.12.140.141	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	14
62.90.162.75	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/scripts/css3pie.htc	Block	14
218.200.139.242	China	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/miluim/about.aspx	Block	14
80.246.130.60	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	14
37.26.149.175	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	14
188.165.15.241	France	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/reserve/	Block	14
66.249.69.35	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
66.249.67.53	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.53	Block	14
155.94.171.212	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	14
46.19.86.85	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	14
84.228.142.227	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/g	Block	14
2.54.7.30	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	14
66.249.67.65	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi	Block	14
178.62.209.185	United Kingdom	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/getfile/getfile.aspx?filename=xhllyta2ltawms5kb2m=&infocenteritem=true	Block	14
89.106.221.2	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	14
62.210.88.201	France	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to www.google.pl/search	Block	14
37.26.149.199	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	14
218.200.139.242	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	14
80.246.133.145	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc	Block	14
192.114.23.18	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	14
66.249.69.51	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
66.249.67.59	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/robots.txt	Block	14
175.44.9.222	China	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/brothers/skira/default.asp/trackback/	Block	14
84.228.216.185	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
31.168.25.193	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	14
207.46.13.144	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	14
185.32.179.136	Israel	147.237.0.19	madim.atal.idf.il	Untraceable SSL Sessions: Open Mode	None	14
66.249.67.77	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/shared/clientscripts/ui/ui.datepicker.js	Block	14
109.65.167.226	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	14
64.41.200.102	United States	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Unsupported Cipher	None	14
46.19.85.63	Israel	147.237.76.42	refuah.idf.il	Malformed URL	Block	14
81.218.40.59	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	14
66.249.78.20	Israel	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/robots.txt	Block	14
66.249.67.59	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.59	Block	14

10-26-2015-13:04:09 to 10-26-2015-14:04:09