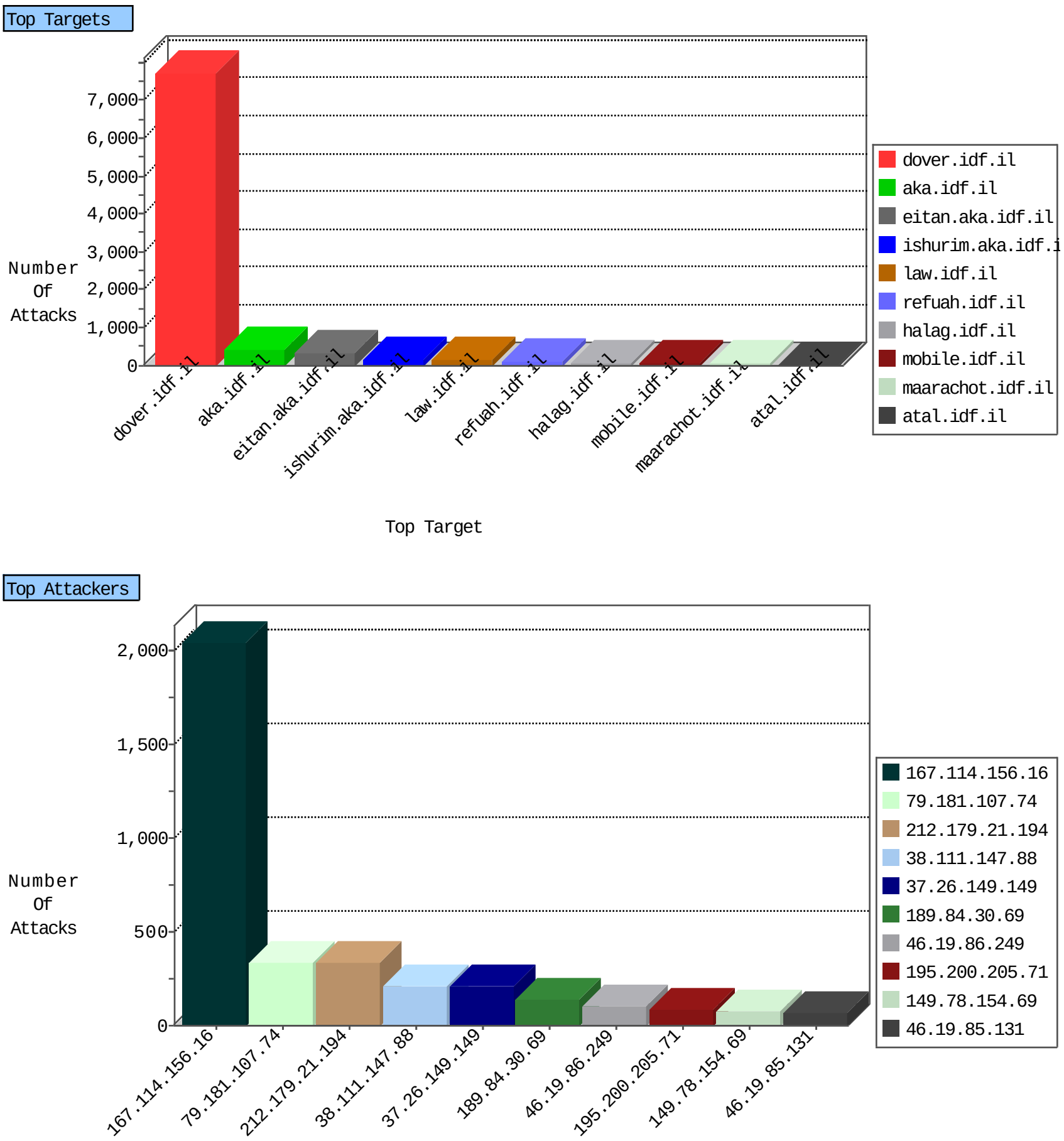
11-04-2015-11:04:03 to 11-04-2015-12:04:03

IDF Under Attack Daily Report



11-04-2015-11:04:03 to 11-04-2015-12:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.69.42	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	20996
167.114.156.16	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	14028
66.249.79.43	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	10481
189.84.30.69	Brazil	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	9764
66.249.67.194	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	6429
66.249.67.202	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	6156
66.249.69.26	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6013
37.26.146.189	Israel	147.237.72.167	ishurim.aka.idf.il	TCP handshake violation, first packet not syn	drop	5618
37.26.146.213	Israel	147.237.0.34	tikshuv.idf.il	TCP handshake violation, first packet not syn	drop	5541
66.249.67.67	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	5302
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5079
66.249.67.194	United States	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	4730
207.46.13.74	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4525
66.249.67.6	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	3456
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3187
66.249.69.34	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2988
86.108.12.107	Jordan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2776
66.249.81.209	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	2526
66.249.79.45	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	2487
66.249.67.122	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	2408
5.255.253.157	Russian Federation	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1644
66.249.79.41	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	1468
66.249.88.1	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1466
60.241.77.198	Australia	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	1402
108.59.253.71	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1003
94.119.1.1	Germany	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	970
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	662
37.25.120.178	Ukraine	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	605
37.26.148.221	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	433
66.249.67.227	United States	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	418
66.249.67.79	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	390
66.249.67.73	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	371
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	301
66.249.67.210	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	157
81.218.241.26	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	113
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	92
212.199.112.144	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	84
176.13.18.57	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	61
37.26.149.149	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	42
195.110.40.244	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	30
109.67.155.204	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	27
79.177.191.112	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	20
46.19.85.108	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	20
183.56.172.222	China	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	19
46.19.85.250	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	18
109.67.155.204	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	17
176.13.18.57	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	15
109.64.165.22	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	15
82.80.36.243	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	11
38.111.147.88	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	10

11-04-2015-11:04:03 to 11-04-2015-12:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
52.1.90.117	United States	147.237.72.166	aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
66.249.69.34	Israel	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	1
212.130.109.156	Denmark	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1

11-04-2015-11:04:03 to 11-04-2015-12:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
189.84.30.69	147.237.77.216	Brazil	dover.idf.il	portscan: TCP Distributed Portscan	1
84.228.71.236	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.67.224	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1
2.52.185.66	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.25.99.77	147.237.77.170	Israel	maarachot.idf.il	ET SCAN Potential SSH Scan	1
176.13.2.125	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.183.109.108	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
66.249.67.79	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	1

11-04-2015-11:04:03 to 11-04-2015-12:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.181.107.74	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	330
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	297
38.111.147.88	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	203
189.84.30.69	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	126
46.19.86.249	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	97
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	80
46.19.85.131	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	71
176.13.19.179	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	60
37.26.149.149	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	59
109.186.4.72	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	57
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	53
176.13.11.210	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	53
176.12.148.140	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	52
82.80.36.243	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	50
37.26.146.171	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	50
46.19.86.25	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
80.246.130.97	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	47
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	47
80.74.105.174	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	46
149.78.56.32	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	46
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
82.166.103.214	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
81.218.251.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
46.116.78.216	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
80.246.130.119	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	39
66.249.93.192	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
149.78.252.36	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
46.19.86.255	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	36
66.249.69.34	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
93.173.246.155	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
105.202.113.243	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
176.13.16.104	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
5.28.149.201	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
37.26.149.149	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	31
37.26.149.149	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	31
37.26.149.149	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	31
66.249.69.26	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
105.202.93.251	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
109.65.155.74	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
195.200.205.71	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
37.26.149.149	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	29
176.13.12.104	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
46.19.86.13	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
195.200.205.71	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	27
195.200.205.71	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	27
176.193.104.68	Russian Federation	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	27
85.64.191.182	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25

11-04-2015-11:04:03 to 11-04-2015-12:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.52.32.45	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
192.115.177.203	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	4
79.181.107.74	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 79.181.107.74	Block	4
176.12.140.183	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1465	Block	3
46.19.85.112	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
82.80.196.44	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/ajax/updatestatus.php	Block	2
46.19.86.182	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.54.54.85	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.52.164.64	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.69.42	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
82.80.196.44	Israel	147.237.72.156	aman.idf.il	PHP Attempt	Block	2
79.180.134.74	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
54.244.22.103	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
212.179.244.106	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
46.19.86.64	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
2.54.46.152	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	1
79.180.221.22	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/shchar	Block	1
66.249.67.196	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/templates/getfile/getfile.aspx	Block	1
176.13.3.118	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
61.135.190.71	China	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/	Block	1
91.231.193.150	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;t in www.aka.idf.il/main/kapatz/scriptresource.axd	None	1
80.246.136.91	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
37.26.149.149	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
212.199.112.144	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl108.x in www.aka.idf.il/main/sachar/payslips.aspx	None	1
176.13.14.102	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	1
68.180.228.109	United States	147.237.0.34	tikshuv.idf.il	Parameter Type Violation PageNum in www.tikshuv.idf.il/901-he/tikshuv.aspx	Block	1
66.249.67.6	Israel	147.237.72.166	aka.idf.il	Unknown Parameter pop in www.aka.idf.il/main/home/	None	1
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
195.200.205.71	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
79.181.39.154	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.67.234	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
176.13.11.210	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
121.16.52.107	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/shared/usercontrols/headerupper/	Block	1
61.135.190.198	China	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	1
80.246.139.129	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
213.151.32.163	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
2.52.52.47	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
176.13.19.213	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1927-he/cogat.aspx	Block	1
176.12.144.58	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.67.59	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
46.19.86.225	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1136-he/atal.aspx	Block	1
84.108.5.87	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	1
79.181.107.74	Israel	147.237.76.200	eitan.aka.idf.il	Too Many 404: Response Code per Session	Block	1
2.54.178.229	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
199.115.117.88	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/themes/elastixneo/ie.css	Block	1
66.249.67.251	Israel	147.237.72.166	aka.idf.il	Unauthorized Method GET for aka.idf.il/iturim/asp/searchresults.asp	Block	1
176.13.12.98	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
141.212.122.64	United States	147.237.0.19	madim.atal.idf.il	Malformed URL proxytest.zmap.io:80	Block	1
66.249.65.112	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/4/3384.jpg	Block	1

11-04-2015-11:04:03 to 11-04-2015-12:04:03