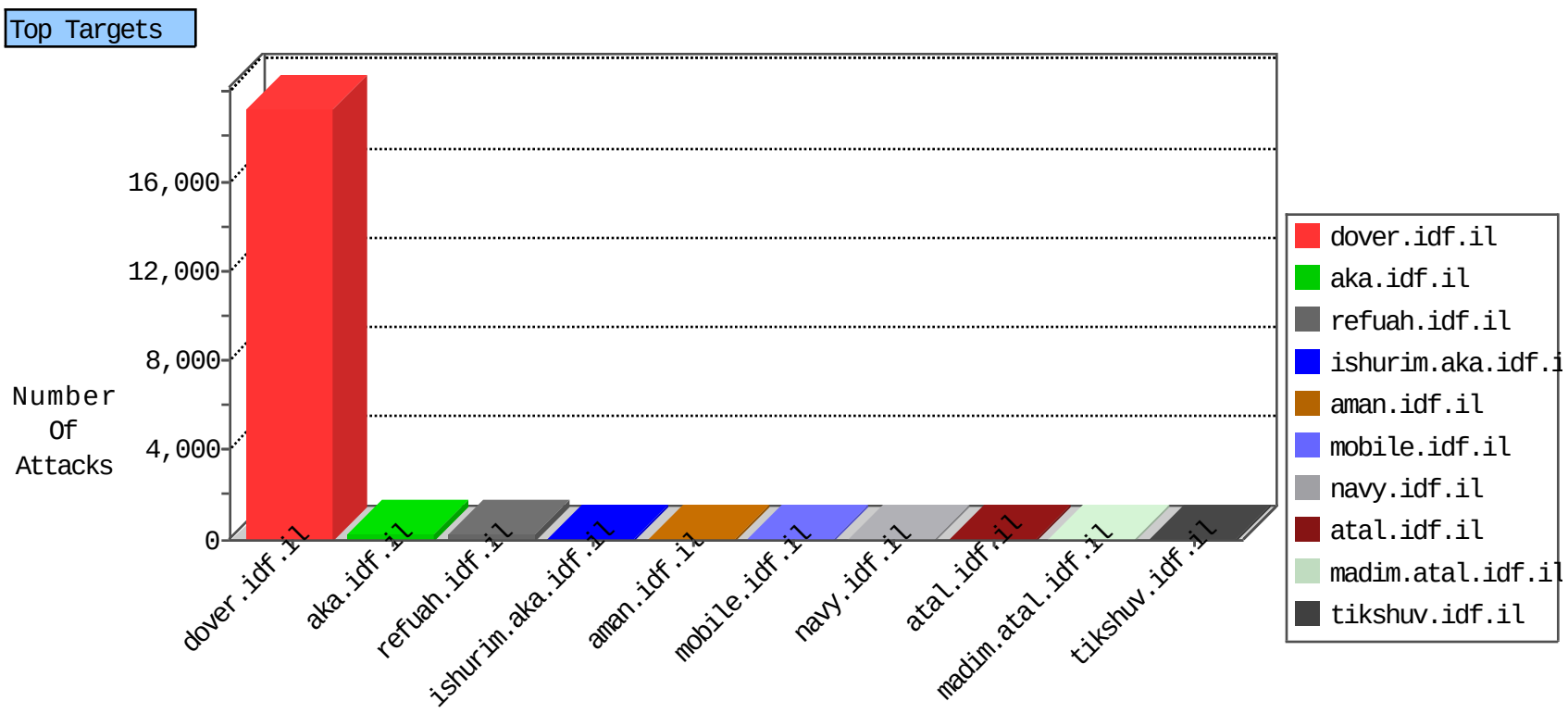
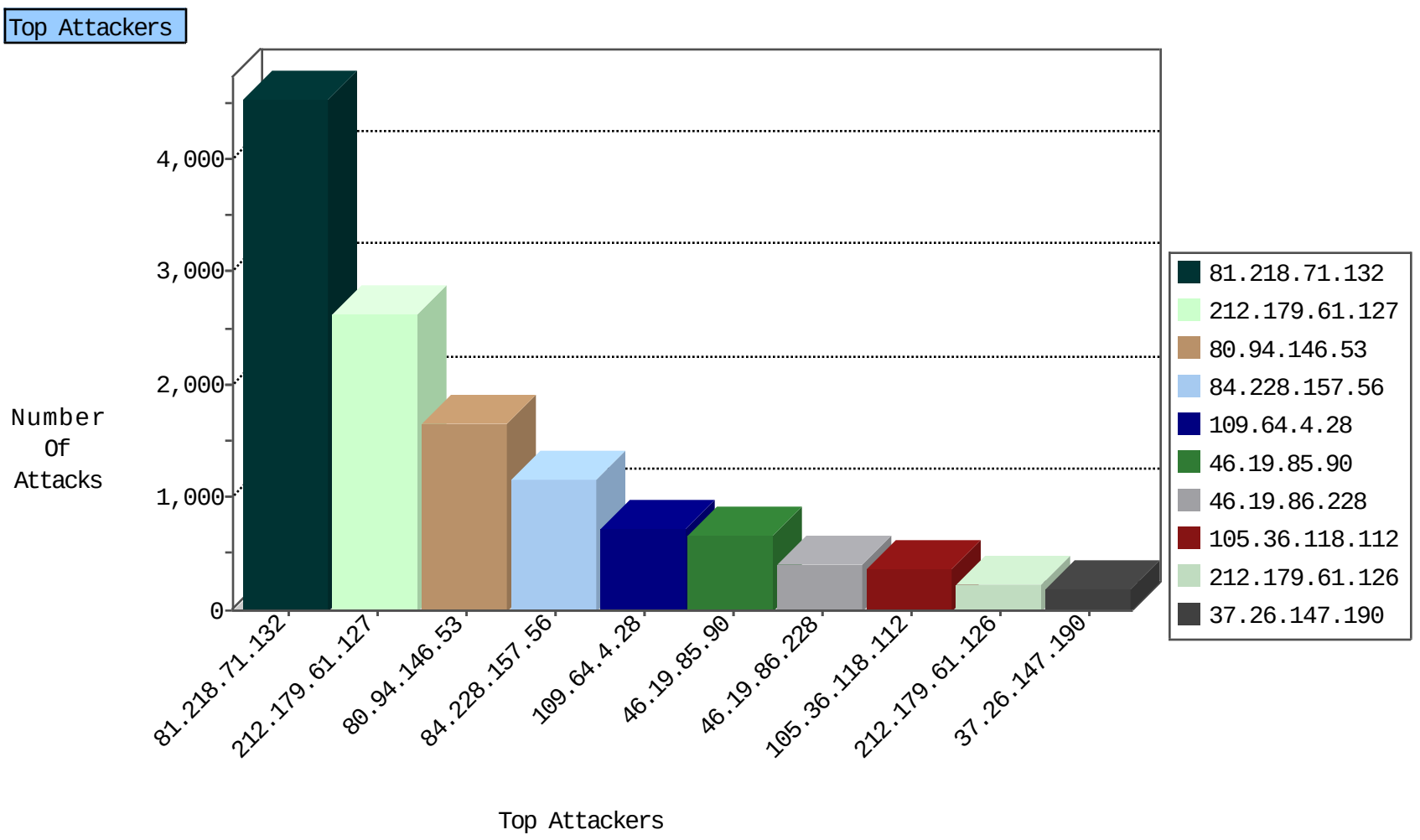
04-28-2015-13:03:10 to 04-28-2015-14:03:10

IDF Under Attack
04-28-2015-13:03:10

Top Targets



Top Attackers



04-28-2015-13:03:10 to 04-28-2015-14:03:10

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
85.250.228.56	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3385
109.253.133.15	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	466
81.218.37.2	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	180
220.181.108.152	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	30
37.26.147.199	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	13
123.218.153.6	Japan	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	5
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	4
192.118.27.253	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
37.26.148.181	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
212.117.136.7	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
176.12.136.207	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
79.183.110.53	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
95.86.105.60	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
82.80.69.90	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
2.52.151.145	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
212.179.61.126	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
109.253.132.59	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
84.108.122.109	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
2.54.15.146	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
199.203.215.1	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1

04-28-2015-13:03:10 to 04-28-2015-14:03:10

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
37.142.128.208	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	7
46.19.85.97	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
109.186.122.30	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
37.142.128.208	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
80.74.105.107	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
220.181.125.15	China	147.237.77.74	law.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
85.25.103.50	Germany	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.0.16	my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	1
46.19.85.113	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.25.103.50	Germany	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	1
2.52.40.52	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
185.32.178.74	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.167.142	United States	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.38	e.e.meitav.idf.il	7610: IP Reputation	Block	1
85.25.103.50	Germany	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.226	www.chamatz.aka.idf.il	7610: IP Reputation	Block	1
71.6.165.200	United States	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	1
212.25.102.57	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
84.109.212.169	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.165.200	United States	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	1

04-28-2015-13:03:10 to 04-28-2015-14:03:10

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
185.32.179.20	Israel	147.237.72.167	ishurim.aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	5
82.80.230.200	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
43.255.191.165	Japan	147.237.76.200	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
2.54.180.146	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	1
212.179.102.167	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
194.114.146.227	Israel	147.237.72.166	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
104.167.118.60		147.237.76.200	eitan.aka.idf.il	ET SCAN NMAP -sS window 3072	1
79.183.102.163	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
61.240.144.67	China	147.237.0.15	kosher-kravi.idf.i	ET SCAN NMAP -sS window 1024	1
46.116.107.243	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
43.255.191.165	Japan	147.237.76.202	e.halag.idf.il	ET SCAN Potential SSH Scan	1
37.142.77.189	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
212.235.103.203	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
194.114.146.227	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
66.249.78.95	United States	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
46.117.134.101	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
43.255.191.165	Japan	147.237.77.19	law-forum.idf.il	ET SCAN Potential SSH Scan	1

04-28-2015-13:03:10 to 04-28-2015-14:03:10

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
81.218.71.132	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4539
212.179.61.127	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2636
80.94.146.53	Switzerland	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1649
84.228.157.56	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1157
109.64.4.28	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	715
46.19.85.90	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	671
46.19.86.228	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	397
105.36.118.112		147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	367
212.179.61.126	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	233
37.26.147.190	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	194
109.64.173.202	Israel	147.237.76.42	refuah.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	141
192.116.232.69	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	137
94.230.95.76	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	135
31.168.78.243	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	109
62.90.255.56	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	87
46.116.211.238	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	85
37.26.148.138	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	82
109.186.24.71	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	81
82.145.210.164	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	78
66.249.78.102	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	76
46.19.86.2	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	74
41.33.232.65	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	71
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	69
66.249.78.95	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	67
46.19.86.182	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	63
173.13.243.61	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	61
108.50.210.59	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	61
66.249.78.109	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	60
46.19.86.170	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	55
79.183.105.247	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	51
109.64.173.202	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	50
213.8.52.149	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	46
95.86.112.147	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	46
66.249.78.166	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	45
149.78.14.9	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	45
70.192.64.32	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	45
46.19.86.250	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	42
212.117.136.8	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	42
66.249.78.173	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	42
5.28.167.170	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	41
176.12.138.253	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	40
176.12.148.255	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	39
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	39
84.95.205.88	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	34
109.64.26.146	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	34
2.54.134.4	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	32
212.179.221.78	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	32
176.12.147.168	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	32
79.176.104.28	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	31
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	31

04-28-2015-13:03:10 to 04-28-2015-14:03:10

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
192.114.163.27	Israel	147.237.76.42	refuah.idf.il	Too Many of the Same Response Code (404) in Session from 192.114.163.27	Block	63
109.253.140.79	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 109.253.140.79	Block	15
109.253.147.170	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	12
212.25.102.57	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/modiin/maslulim.aspx	Block	4
2.54.26.12	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	3
46.19.85.147	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	3
5.29.167.173	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	3
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
176.12.145.244	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	2
95.86.116.178	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	2
85.65.54.88	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
46.19.85.92	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	2
176.12.148.73	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
147.236.16.190	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
109.64.204.57	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	2
87.68.228.78	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	2
66.249.64.77	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il//console/core/doc_mgr/undefined	Block	1
93.172.169.104	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/console/core/doc_mgr/undefined	Block	1
46.19.86.57	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
5.29.221.145	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
178.120.244.167	Belarus	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
149.78.246.248	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/statistics/gens.stm	Block	1
66.249.78.102	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1065-he/dover.aspx	Block	1
66.249.64.26	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1129-he/dover.aspx	Block	1
212.179.61.126	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/163-7278-he/patzar.aspxtuytu8	Block	1
109.186.122.30	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42//1518-he/refuah.aspx	Block	1
84.108.96.120	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
37.142.171.168	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
193.106.54.21	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	1
66.249.78.236	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/938-he/refuah.aspx	Block	1
2.54.18.124	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
138.134.192.10	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/milnet	Block	1
66.249.67.66	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/1132-8000-he/navy.aspx	Block	1
212.76.117.120	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.121.110.69	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
5.255.253.16	Russian Federation	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 5.255.253.16	Block	1
180.76.4.64	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
79.179.209.82	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il//https:/www.aman.idf.il/	Block	1
66.249.78.109	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-16854-he/dover.aspx	Block	1
157.55.39.208	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/	Block	1
66.249.64.66	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/993/patzar.aspx	Block	1
109.253.137.141	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
194.114.146.227	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.78.242	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/	Block	1
141.212.122.26	United States	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/	Block	1
66.249.69.36	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/giyus/general.aspx	Block	1
61.91.144.102	Thailand	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
212.117.143.250	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 212.117.143.250 (Unknown SSL Session)	None	1
109.64.173.202	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42//1518-he/refuah.aspx	Block	1
31.168.101.163	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	1

04-28-2015-13:03:10 to 04-28-2015-14:03:10