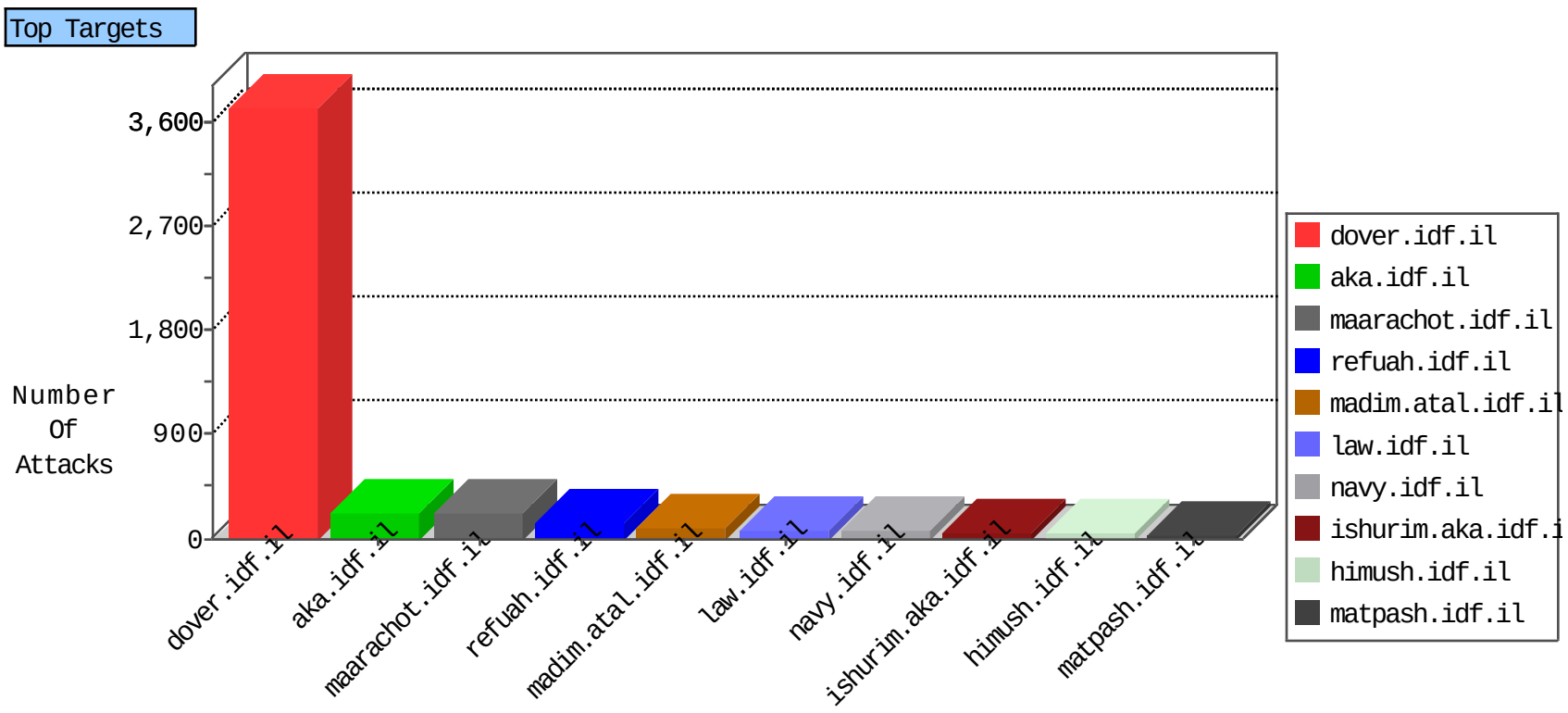
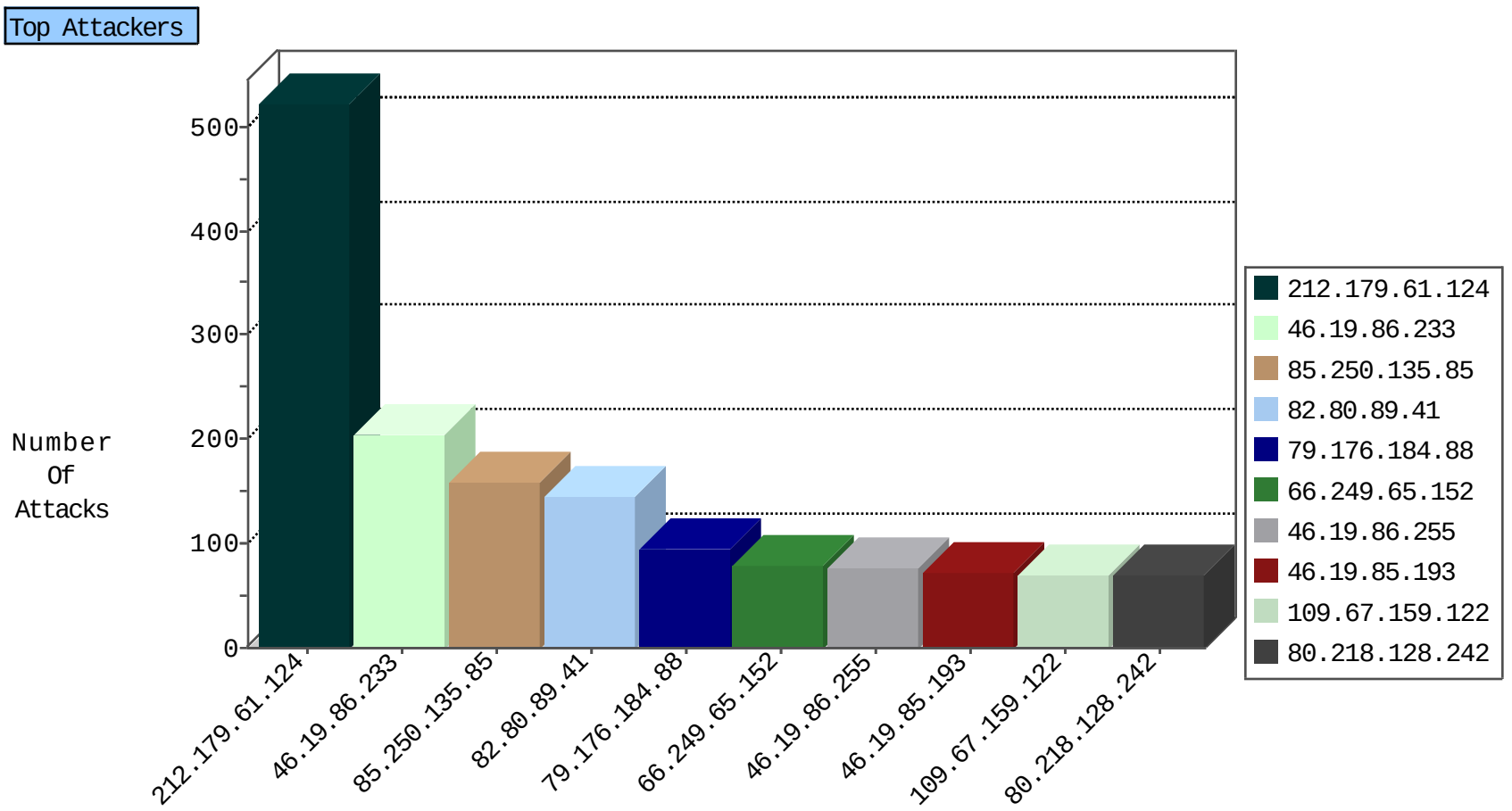
04-13-2015-09:03:03 to 04-13-2015-10:03:03

IDF Under Attack
04-13-2015-09:03:03

Top Targets



Top Attackers



04-13-2015-09:03:03 to 04-13-2015-10:03:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
220.181.108.119	China	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	1511
108.59.253.71	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	785
82.169.159.17	Netherlands	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	724
192.116.232.69	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	93
66.249.65.152	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	80
66.249.65.148	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	68
66.249.65.156	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	55
66.249.67.115	United States	147.237.76.30	himush.idf.il	Block_Ip_Web_In	drop	21
80.246.138.250	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	21
66.249.67.107	United States	147.237.76.30	himush.idf.il	Block_Ip_Web_In	drop	21
66.249.93.160	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	20
66.249.78.159	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	18
66.249.67.14	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	18
66.249.78.173	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	18
66.249.67.116	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	18
66.249.93.168	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	16
66.249.67.30	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	16
66.249.78.21	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	15
66.249.78.166	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	15
46.19.86.25	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	14
66.249.78.174	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	14
66.249.78.14	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	14
66.249.78.215	United States	147.237.72.167	ishurim.aka.idf.il	Block_Ip_Web_In	drop	14
66.249.73.132	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	13
192.118.30.102	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	12
66.249.78.160	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	12
66.249.67.22	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	12
66.249.67.92	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	11
66.249.93.168	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	11
66.249.93.176	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	11
66.249.78.190	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	10
66.249.67.108	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	10
66.249.78.167	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	10
66.249.67.100	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	10
66.249.93.245	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	10
66.249.78.242	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	10
66.249.67.84	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	10
66.249.93.172	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	9
66.249.67.76	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	9
66.249.93.171	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	9
66.249.78.236	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	8
66.249.78.208	United States	147.237.72.167	ishurim.aka.idf.il	Block_Ip_Web_In	drop	8
66.249.78.127	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	7
66.249.93.190	United States	147.237.0.19	madim.atal.idf.il	Block_Ip_Web_In	drop	7
66.249.93.242	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	7
66.249.73.209	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	7
66.249.73.244	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	7
66.249.78.28	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	7
66.249.93.164	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	6
66.249.89.101	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	6

04-13-2015-09:03:03 to 04-13-2015-10:03:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
213.8.52.149	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	9
213.8.52.146	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
212.235.98.139	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
37.26.147.236	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
79.176.60.3	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.25.43.94	Germany	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.16	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.25.43.94	Germany	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.217	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.65.36.250	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1

04-13-2015-09:03:03 to 04-13-2015-10:03:03

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	2
85.250.135.85	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
77.125.135.65	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
46.116.230.218	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
23.118.252.239	United States	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
200.107.233.92	Honduras	147.237.76.196	e.sviva.idf.il	ET SCAN NMAP -sS window 4096	1
200.107.233.92	Honduras	147.237.76.196	e.sviva.idf.il	ET SCAN NMAP -f -sS	1
125.5.16.195	Philippines	147.237.72.156	aman.idf.il	ET SCAN NMAP -sS window 1024	1
84.108.79.117	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
61.240.144.66	China	147.237.76.31	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
37.26.147.210	Israel	147.237.72.166	aka.idf.il	WEB-CGI redirect access	1
200.107.233.92	Honduras	147.237.76.196	e.sviva.idf.il	ET SCAN NMAP -sS window 2048	1

04-13-2015-09:03:03 to 04-13-2015-10:03:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
212.179.61.124	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	512
46.19.86.233	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	204
85.250.135.85	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	157
82.80.89.41	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	145
46.19.86.255	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	76
46.19.85.193	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	71
109.67.159.122	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	69
80.218.128.242	Switzerland	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	69
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	48
2.54.4.29	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	40
213.57.113.24	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	37
199.203.215.1	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	34
46.19.85.74	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	34
125.88.8.235	China	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	32
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	31
109.253.144.42	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	31
212.199.16.150	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	30
80.179.204.53	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	30
213.8.52.146	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	29
94.159.143.55	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	29
80.179.223.31	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	29
46.19.85.42	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	29
95.185.136.47	Romania	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	27
2.54.13.175	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	26
89.139.183.55	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	26
84.108.28.30	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	24
82.169.159.17	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	24
176.12.141.212	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	23
109.253.139.231	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	23
82.166.236.77	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	21
212.179.28.34	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
46.19.85.211	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
82.80.153.251	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
46.19.86.99	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
81.218.48.37	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
37.142.251.23	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
176.12.147.70	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
93.172.34.126	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
173.199.65.20	Canada	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
213.151.36.98	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
213.151.41.128	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
50.253.249.190	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
212.143.24.189	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
207.46.13.82	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
207.46.13.89	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
109.253.135.40	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
109.160.130.31	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15

04-13-2015-09:03:03 to 04-13-2015-10:03:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
79.176.184.88	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 79.176.184.88	Block	92
212.76.107.97	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
176.12.160.4	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
109.253.133.202	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
81.218.251.252	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	2
159.253.7.9	Netherlands	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	2
213.57.188.251	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	2
79.170.40.232	United Kingdom	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	2
213.151.36.98	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	2
67.20.76.104	United States	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	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
212.235.10.18	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
192.114.105.254	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	2
207.46.13.89	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.89	Block	2
46.19.85.42	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
213.57.113.24	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-13098-he/dover.aspx, accessed march 30, 2015.	Block	2
194.90.239.2	Israel	147.237.72.167	ishurim.aka.idf.il	Multiple Untraceable SSL Sessions from 194.90.239.2 (Unknown SSL Session)	None	1
107.170.46.176	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/228-he/faq.aspx	Block	1
176.12.140.160	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$txtMisparIshi in www.aka.idf.il/main/sachar/	None	1
79.181.186.215	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
62.219.239.81	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	1
109.253.147.236	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
209.88.198.1	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42//1518-he/refuah.aspx	Block	1
188.143.232.72	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/searchresults/searchresults.aspx/templates/sendtofriend/sendtofriend.aspx	Block	1
79.170.40.232	United Kingdom	147.237.77.176	matpash.idf.il	Distributed Admin Blocking	Block	1
109.253.140.124	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
62.128.45.194	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
194.90.239.2	Israel	147.237.72.167	ishurim.aka.idf.il	SSL Untraceable Connection - Unknown SSL Session	None	1
109.64.7.57	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/scripts/css3pie.htc	Block	1
80.179.188.50	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
176.12.145.154	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
67.20.76.104	United States	147.237.77.176	matpash.idf.il	Distributed Admin Blocking	Block	1
141.212.122.66	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/	Block	1
109.253.136.208	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
2.54.7.33	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	SSL Untraceable Connection - Unknown Server Certificate	None	1
82.166.146.18	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
192.99.39.235	Canada	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
167.114.64.100	United States	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
62.219.13.180	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.253.140.176	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
207.46.13.79	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/miluim/templates/www.behazdaa.org	Block	1
109.253.129.163	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
80.246.130.175	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	1
155.94.222.12		147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/	Block	1
109.253.137.19	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
2.54.14.230	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/scriptresource.axd	Block	1
212.143.3.44	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
192.111.146.34	United States	147.237.76.42	refuah.idf.il	PHP Attempt	Block	1
84.109.37.120	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
176.12.138.132	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1

04-13-2015-09:03:03 to 04-13-2015-10:03:03