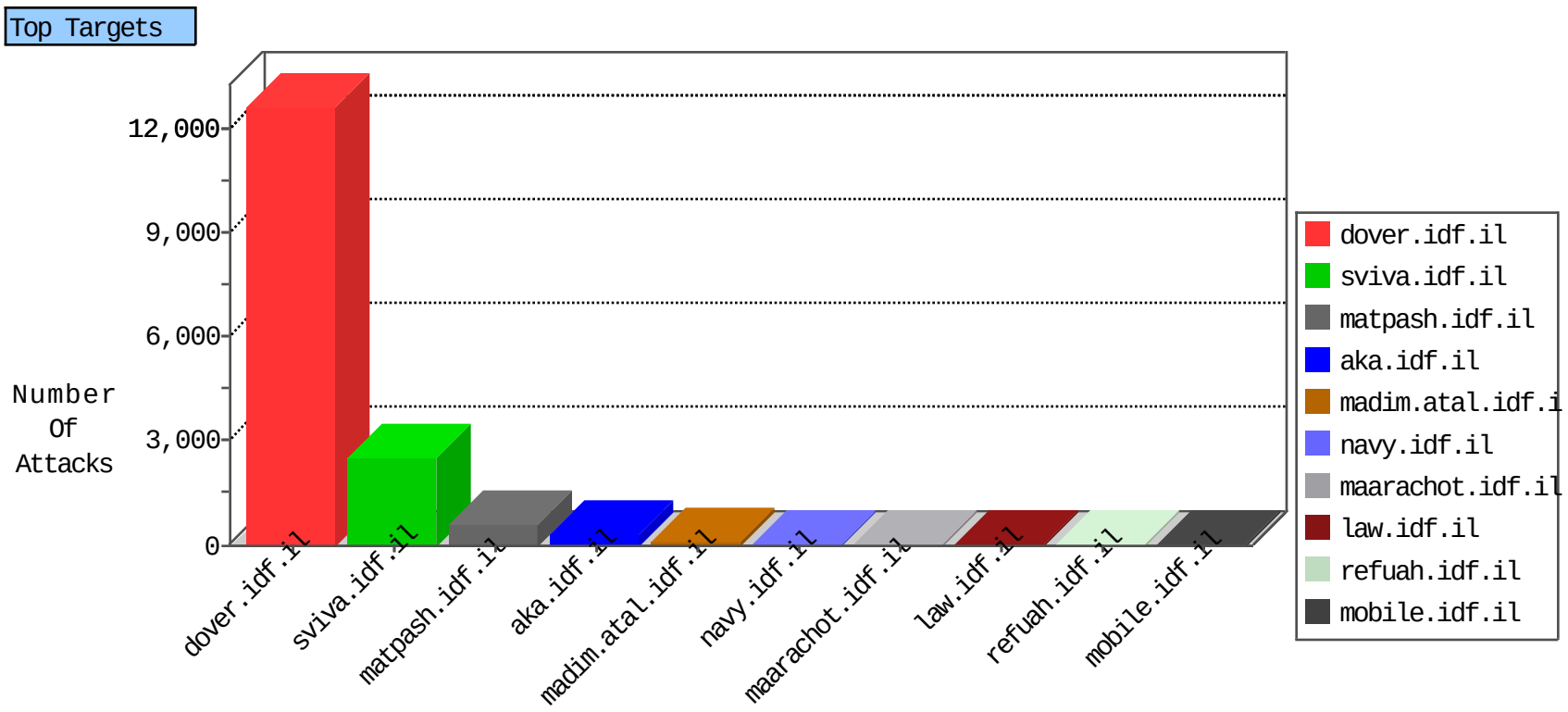
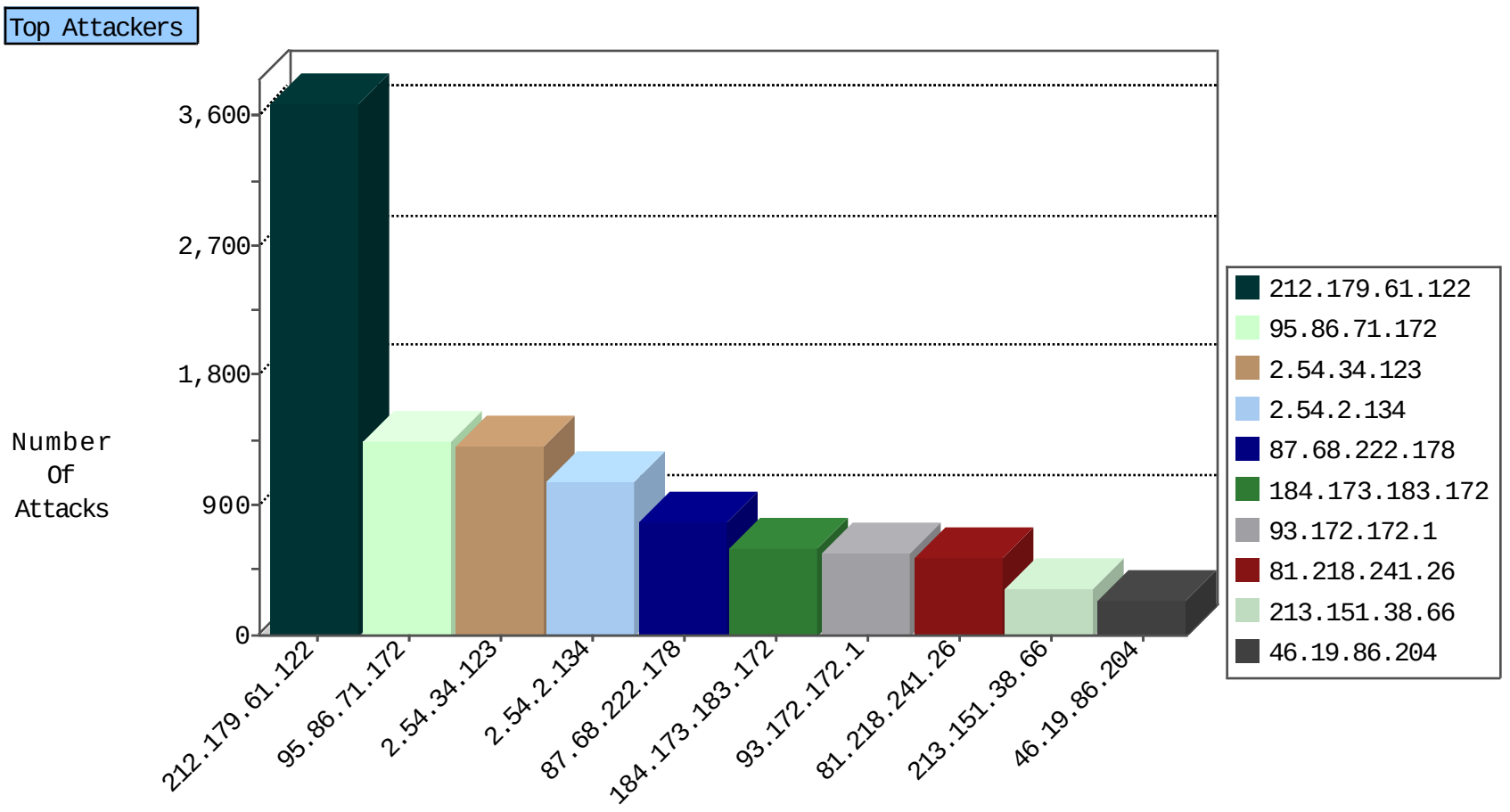
04-20-2015-17:03:07 to 04-20-2015-18:03:07

IDF Under Attack
04-20-2015-17:03:07

Top Targets



Top Attackers



04-20-2015-17:03:07 to 04-20-2015-18:03:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.67.24	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	7230
132.67.170.166	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2660
66.249.67.40	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	433
46.19.85.129	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	47
84.228.142.111	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	21
84.110.110.87	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	12
95.86.85.111	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
192.114.105.254	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
80.246.137.19	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
222.186.56.107	China	147.237.76.176	test.ncore.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
78.193.244.18	France	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
79.178.132.246	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
220.246.178.196	Hong Kong	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
31.168.133.226	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
104.50.141.32		147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1
58.176.168.169	Hong Kong	147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	1

04-20-2015-17:03:07 to 04-20-2015-18:03:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
184.173.183.172	United States	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	608
46.137.134.188	Ireland	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	10
85.64.240.67	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
85.25.43.94	Germany	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1
94.159.235.254	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.165.200	United States	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
98.240.93.71	United States	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
71.6.165.200	United States	147.237.76.148	gqcenter.aka.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.192	Israel	147.237.77.226	www.chamatz.aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
188.138.9.50	Germany	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	1
46.116.211.238	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
198.20.69.98	United States	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
79.178.196.252	Israel	147.237.72.167	ishurim.aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
46.137.134.188	Ireland	147.237.72.156	aman.idf.il	DVRep_P-N_40-59	Permit	1
198.20.69.98	United States	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	1

04-20-2015-17:03:07 to 04-20-2015-18:03:07

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
66.249.67.32	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.78.197	United States	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	2
66.249.78.204	United States	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	2
61.240.144.67	China	147.237.0.200	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
113.59.33.61	China	147.237.77.178	e.matpash.idf.il	ET SCAN NMAP -sS window 2048	1
61.240.144.64	China	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
109.186.16.115	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
46.121.248.208	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
104.167.96.44		147.237.76.148	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 3072	1
87.69.199.241	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
79.181.105.50	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
212.235.98.139	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
195.82.63.197	Germany	147.237.77.212	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
113.59.33.61	China	147.237.77.233	atal.idf.il	ET SCAN NMAP -sS window 4096	1
61.240.144.67	China	147.237.76.147	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
113.59.33.61	China	147.237.77.233	atal.idf.il	ET SCAN NMAP -f -sS	1
61.240.144.65	China	147.237.76.86	navy.idf.il	ET SCAN NMAP -sS window 1024	1
113.59.33.61	China	147.237.77.178	e.matpash.idf.il	ET SCAN NMAP -f -sS	1
50.243.183.193	United States	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
109.64.120.134	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
101.69.199.71	China	147.237.8.27	e.madim.atal.idf.il	ET SCAN NMAP -sS window 3072	1
82.214.114.5	Macedonia, the Former Yugoslav Republic of	147.237.77.61	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
218.6.132.45	China	147.237.77.121	e.navy.idf.il	ET SCAN NMAP -sS window 4096	1
212.179.21.195	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.78.134	United States	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	1
66.249.64.83	United States	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	1
113.59.33.61	China	147.237.77.233	atal.idf.il	ET SCAN NMAP -sS window 2048	1

04-20-2015-17:03:07 to 04-20-2015-18:03:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
212.179.61.122	Israel	147.237.77.235	sviva.idf.i	First packet isn't SYN	drop	drop	2559
95.86.71.172	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1342
2.54.34.123	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1306
212.179.61.122	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1131
2.54.2.134	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1068
87.68.222.178	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	781
93.172.172.1	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	569
81.218.241.26	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	530
213.151.38.66	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	314
46.19.86.204	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	237
5.22.130.225	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	208
212.179.42.241	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	186
2.54.33.146	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	174
212.179.21.195	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	164
2.52.153.24	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	159
82.102.136.65	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	111
171.33.193.149	United Kingdom	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	93
93.172.179.151	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	91
149.78.202.40	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	77
80.74.121.142	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	70
212.179.42.66	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	67
194.176.105.150	United Kingdom	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	64
132.70.66.11	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	57
5.28.175.162	Israel	147.237.72.166	aka.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	56
82.166.28.72	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	51
2.54.9.109	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	46
87.69.115.141	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	44
79.178.5.46	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	41
37.26.148.225	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	39
109.253.145.7	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	39
192.114.105.254	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	38
208.54.70.185	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	38
2.52.173.82	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	38
193.43.246.250	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	36
79.180.102.239	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	36
79.176.63.188	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	34
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	33
109.253.132.142	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	33
66.249.78.159	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	32
66.249.78.159	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	32
176.12.142.150	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	30
70.198.47.150	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	30
79.180.26.246	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	28
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	28
66.249.78.166	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	27
79.183.5.45	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	26
66.249.78.166	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	26
93.172.34.126	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	26
82.166.75.217	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	26
12.69.179.102	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	25

04-20-2015-17:03:07 to 04-20-2015-18:03:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
46.19.86.103	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	54
109.253.129.3	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	13
2.54.170.190	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	12
192.116.188.37	Israel	147.237.76.39	mobile.meitav.idf.il	Cookie Tampering on cookie .ASPNETAUTH: Expected 0102D063AA2B8B49D208FED0DBEBF68D49D20800093300330037003900320032003400320031000012F00FF, Observed 010226D0E07A0032D208FE264822460332D2080009330033003700390032003200340032003100000012F00FF	None	8
67.86.240.10	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	5
79.180.205.42	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 79.180.205.42	Block	4
37.26.147.210	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	4
109.253.141.73	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	4
80.246.130.119	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	3
79.180.150.57	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	3
109.66.138.223	Israel	147.237.72.166	aka.idf.il	Distributed Unknown HTTP Request Method	Block	2
176.12.144.86	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	2
95.86.106.73	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	2
77.126.39.135	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	2
54.235.160.85	United States	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	2
79.180.58.173	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
69.89.21.65	United States	147.237.77.176	matpash.idf.il	PHP Attempt	Block	2
109.64.20.129	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	2
109.253.138.123	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	2
87.69.194.149	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	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
81.218.140.248	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
109.160.225.147	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	2
46.19.86.39	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
109.253.144.194	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
77.125.127.230	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.66.138.223	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 109.66.138.223 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	1
66.249.78.109	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19748-he/idfgdover.aspx	Block	1
54.235.160.85	United States	147.237.72.166	aka.idf.il	Distributed Admin Blocking	Block	1
84.228.20.222	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/nagan_tizmoret_tzahal/	Block	1
5.29.0.4	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 5.29.0.4	Block	1
109.168.211.24	Russian Federation	147.237.77.176	matpash.idf.il	Distributed Unknown HTTP Request Method	Block	1
79.178.196.252	Israel	147.237.72.167	ishurim.aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_SERVER_HELLO)	None	1
69.89.21.65	United States	147.237.77.176	matpash.idf.il	Admin Blocking	Block	1
109.66.138.223	Israel	147.237.72.166	aka.idf.il	Malformed URL y[[#24]]	Block	1
66.249.64.84	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/giyus/general.aspx	Block	1
198.20.69.74	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
79.180.205.42	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/6_s3_	Block	1
149.88.149.80	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
2.52.1.2	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/authenticationservice.asmx/getuserdetails	Block	1
109.66.138.223	Israel	147.237.72.166	aka.idf.il	NULL Character in Header Name at	Block	1
109.66.138.223	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Header Name	Block	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	1
176.12.149.83	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	1
85.64.163.132	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/giyus/terms.aspx	None	1
5.29.0.4	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/templates/general/6_s3_	Block	1
109.66.138.223	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Request from 109.66.138.223	Block	1
66.249.64.88	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.181.153.202	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.116.240.105	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1

04-20-2015-17:03:07 to 04-20-2015-18:03:07