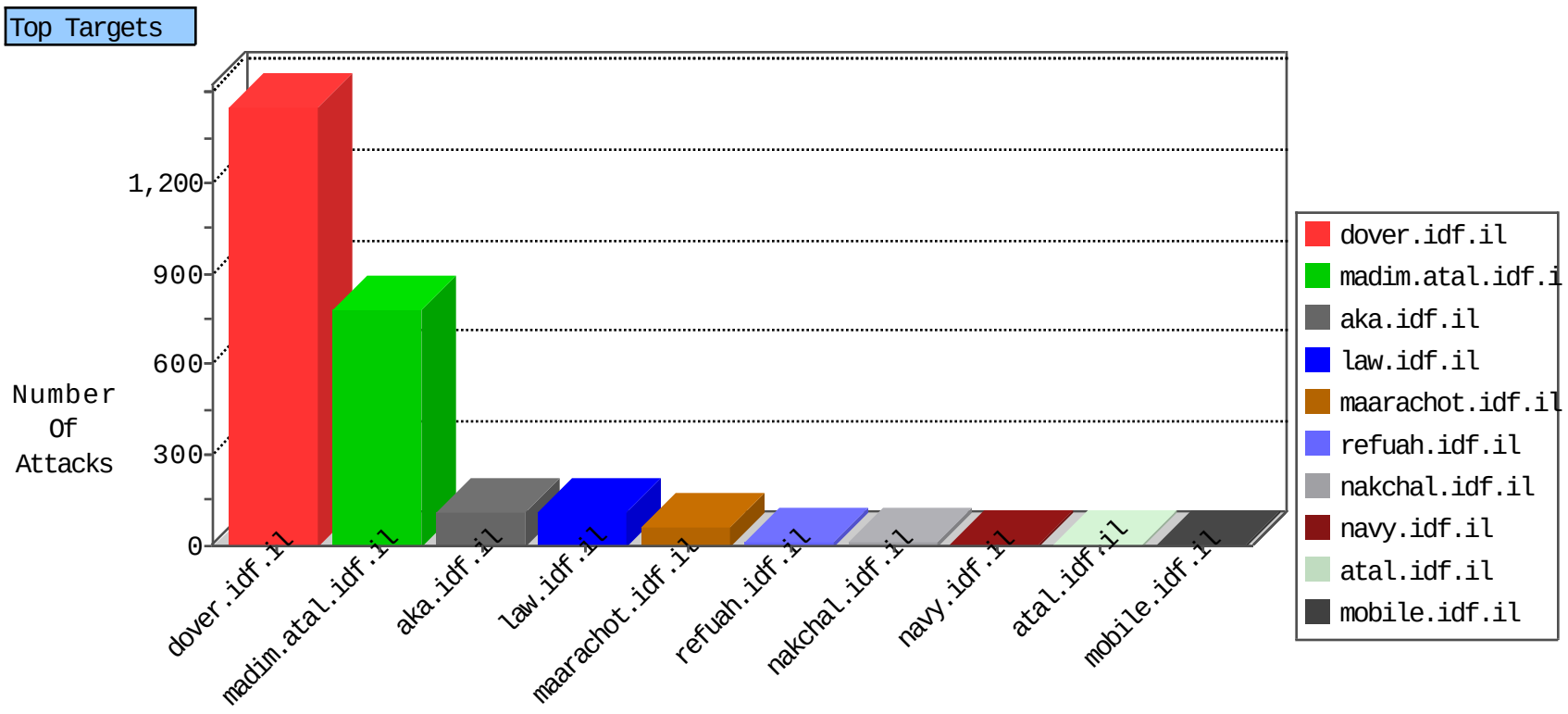
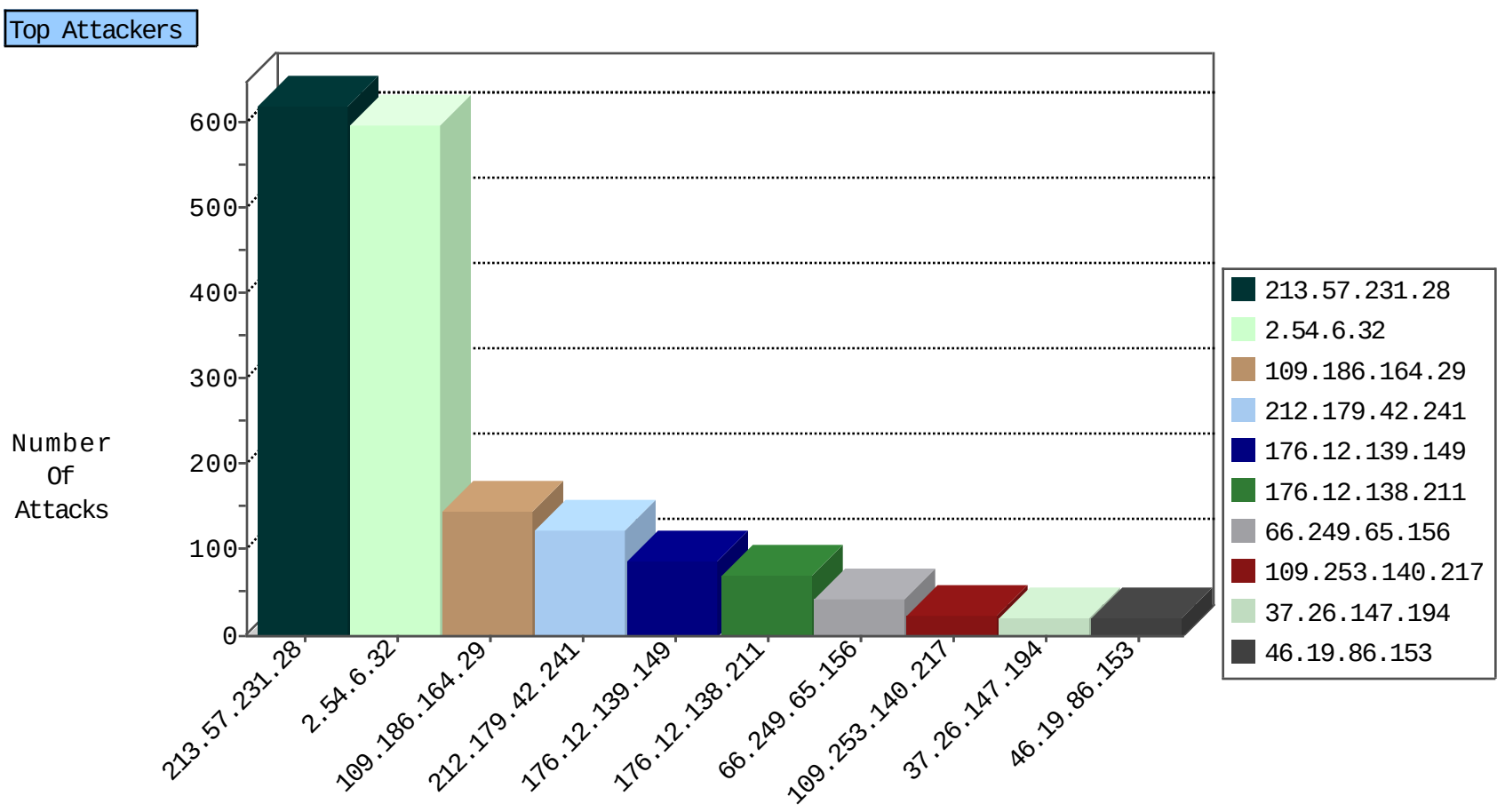
04-14-2015-22:03:02 to 04-14-2015-23:03:02

IDF Under Attack
04-14-2015-22:03:02

Top Targets



Top Attackers



04-14-2015-22:03:02 to 04-14-2015-23:03:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
204.13.200.28	United States	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	forward	277
220.181.108.112	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	47
46.19.86.153	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	12
149.78.172.18	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
95.86.65.98	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
46.19.86.157	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
124.244.12.180	Hong Kong	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
58.183.99.194	Japan	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1

04-14-2015-22:03:02 to 04-14-2015-23:03:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
79.177.151.148	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
109.67.63.126	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
85.250.135.85	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
31.154.248.55	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
84.228.194.243	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
71.6.165.200	United States	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	2
71.6.167.142	United States	147.237.76.148	gqcenter.aka.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
84.109.38.30	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	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
184.173.183.172	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	1
71.6.165.200	United States	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	1
2.54.54.56	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
213.57.231.28	Israel	147.237.0.19	madim.atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
93.120.27.62	Romania	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	1
98.118.10.246	United States	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
71.6.167.142	United States	147.237.77.205	prisha.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
198.20.69.98	United States	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.148	gqcenter.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.245	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
105.49.154.188	Kenya	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	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	1

04-14-2015-22:03:02 to 04-14-2015-23:03:02

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
66.249.65.156	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	42
66.249.65.152	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	6
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
66.249.65.187	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	4
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	4
66.249.65.50	United States	147.237.77.233	atal.idf.il	ET SCAN NMAP -sA (2)	2
52.4.127.156	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sS window 1024	1
109.253.145.108	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
104.167.117.197		147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
104.167.117.197		147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sS window 4096	1
94.100.31.179	Netherlands	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1

04-14-2015-22:03:02 to 04-14-2015-23:03:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
2.54.6.32	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	595
109.186.164.29	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	145
212.179.42.241	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	124
109.253.140.217	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
37.26.147.194	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	22
69.41.14.161	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
69.41.14.215	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
112.215.36.145	Indonesia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
112.215.36.142	Indonesia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
66.249.65.39	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
176.12.146.30	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
149.78.249.63	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
46.19.86.153	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
87.68.31.114	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
46.19.86.168	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
5.29.49.127	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
82.95.73.185	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
79.182.138.86	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
84.228.130.64	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
112.215.36.144	Indonesia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
192.117.8.10	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
213.57.231.28	Israel	147.237.0.19	madim.atal.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
31.186.228.62	United Kingdom	147.237.77.74	law.idf.il	First packet isn't SYN	drop	drop	8
149.78.172.18	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
176.12.147.139	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
31.186.228.92	United Kingdom	147.237.77.74	law.idf.il	First packet isn't SYN	drop	drop	7
31.186.228.170	United Kingdom	147.237.77.74	law.idf.il	First packet isn't SYN	drop	drop	7
31.186.228.57	United Kingdom	147.237.77.74	law.idf.il	First packet isn't SYN	drop	drop	7
109.253.156.32	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
109.253.136.220	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
109.253.138.250	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
212.76.127.212	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
112.215.36.143	Indonesia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
46.19.85.227	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
79.180.172.243	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
46.121.64.252	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
176.12.140.37	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
46.116.177.58	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
31.186.228.28	United Kingdom	147.237.77.74	law.idf.il	First packet isn't SYN	drop	drop	5
66.249.78.173	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
31.186.228.89	United Kingdom	147.237.77.74	law.idf.il	First packet isn't SYN	drop	drop	5
71.52.35.140	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
176.12.141.170	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
46.19.86.108	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
72.159.132.4	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
31.186.228.64	United Kingdom	147.237.77.74	law.idf.il	First packet isn't SYN	drop	drop	4
66.249.78.159	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
166.137.252.108	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
213.57.231.28	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	606
176.12.139.149	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	87
176.12.138.211	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	70
164.138.112.71	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	16
79.177.151.148	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	7
149.78.43.140	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	7
37.26.147.160	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	5
85.64.34.122	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	4
213.57.231.28	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/mobile/shared/ajax/updatemakatqauntity.aspx	Block	4
66.249.73.222	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/console/core/doc_mgr/undefined	Block	2
84.111.64.33	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
109.67.63.126	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 109.67.63.126	Block	2
79.177.151.148	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/sip_storage/files/8	Block	2
176.12.139.116	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	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
95.86.89.43	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
89.139.2.208	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.65.43	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/gen...px	Block	1
207.46.13.82	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-19725-ar/dover.aspx"	Block	1
84.109.38.30	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
77.237.138.202	Czech Republic	147.237.77.233	atal.idf.il	Unauthorized URL Access to /	Block	1
95.173.184.138	Turkey	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal HTTP Version	Block	1
85.65.149.189	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
46.19.86.104	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
180.76.4.172	China	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
79.181.201.33	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
109.253.147.105	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.166	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/bdtz/mivne_details/bet_so.stm	Block	1
66.249.65.72	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/938-he/refuah.aspx	Block	1
91.217.90.49	Ukraine	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.15/rom-0	Block	1
2.52.132.94	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
208.113.198.126	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/blog/wp-admin/	Block	1
66.249.73.230	United States	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il//console/core/doc_mgr/undefined	Block	1
85.250.57.226	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
46.117.83.50	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
188.138.17.205	France	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/	Block	1
80.230.77.141	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.93.245	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	1
66.249.65.153	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1239-he/atal.aspx	Block	1
93.173.243.227	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 93.173.243.227	Block	1
5.248.174.221	Ukraine	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
109.186.1.73	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.95	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/templates/sendtofriend/sendtofriend.aspx	Block	1
87.69.188.39	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
50.63.197.201	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp/wp-admin/	Block	1
196.38.40.110	South Africa	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp-admin/	Block	1
80.246.133.203	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
149.88.67.178	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.67.64	United States	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to www.kosher-kravi.idf.il/templates/shared/usercontrols/headerupper/	Block	1
93.173.243.227	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/9/	Block	1

04-14-2015-22:03:02 to 04-14-2015-23:03:02