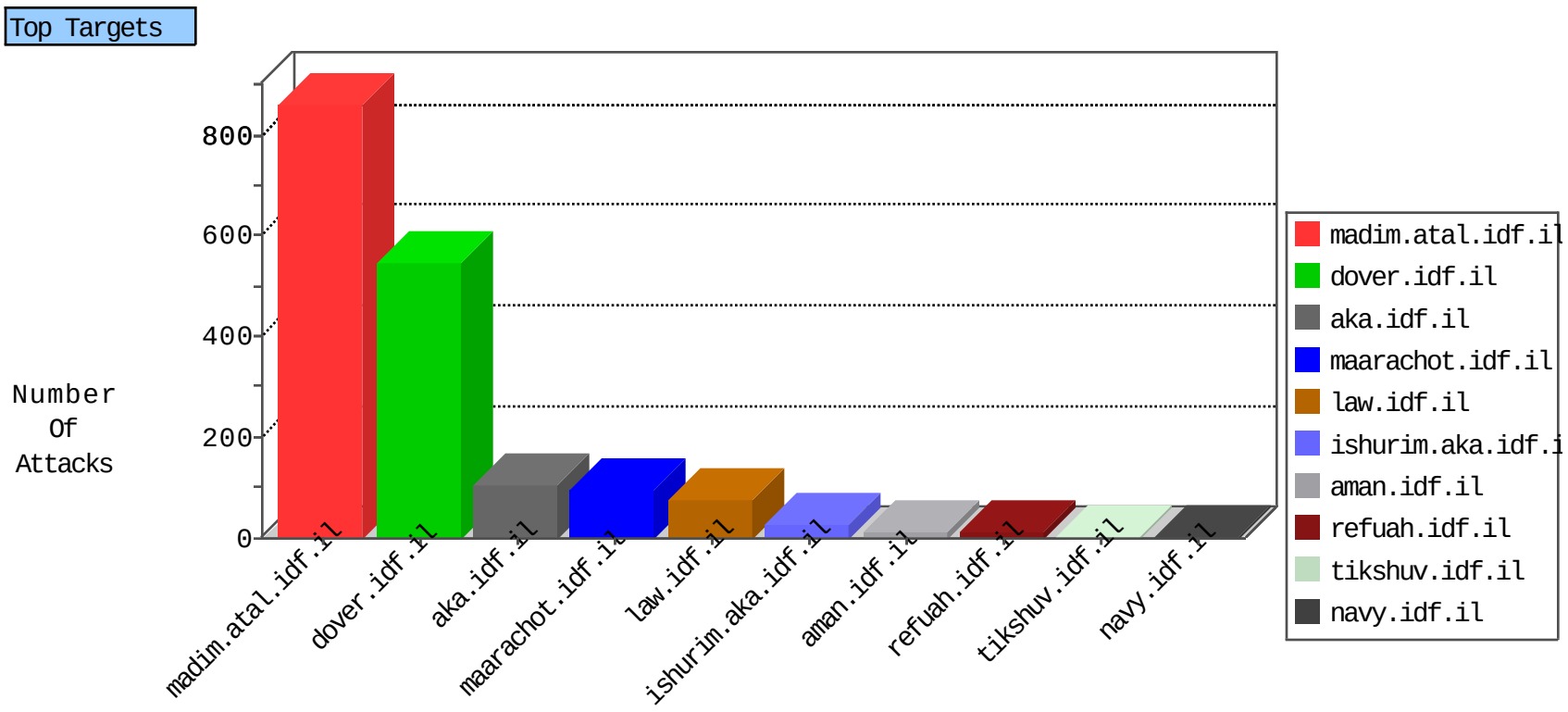
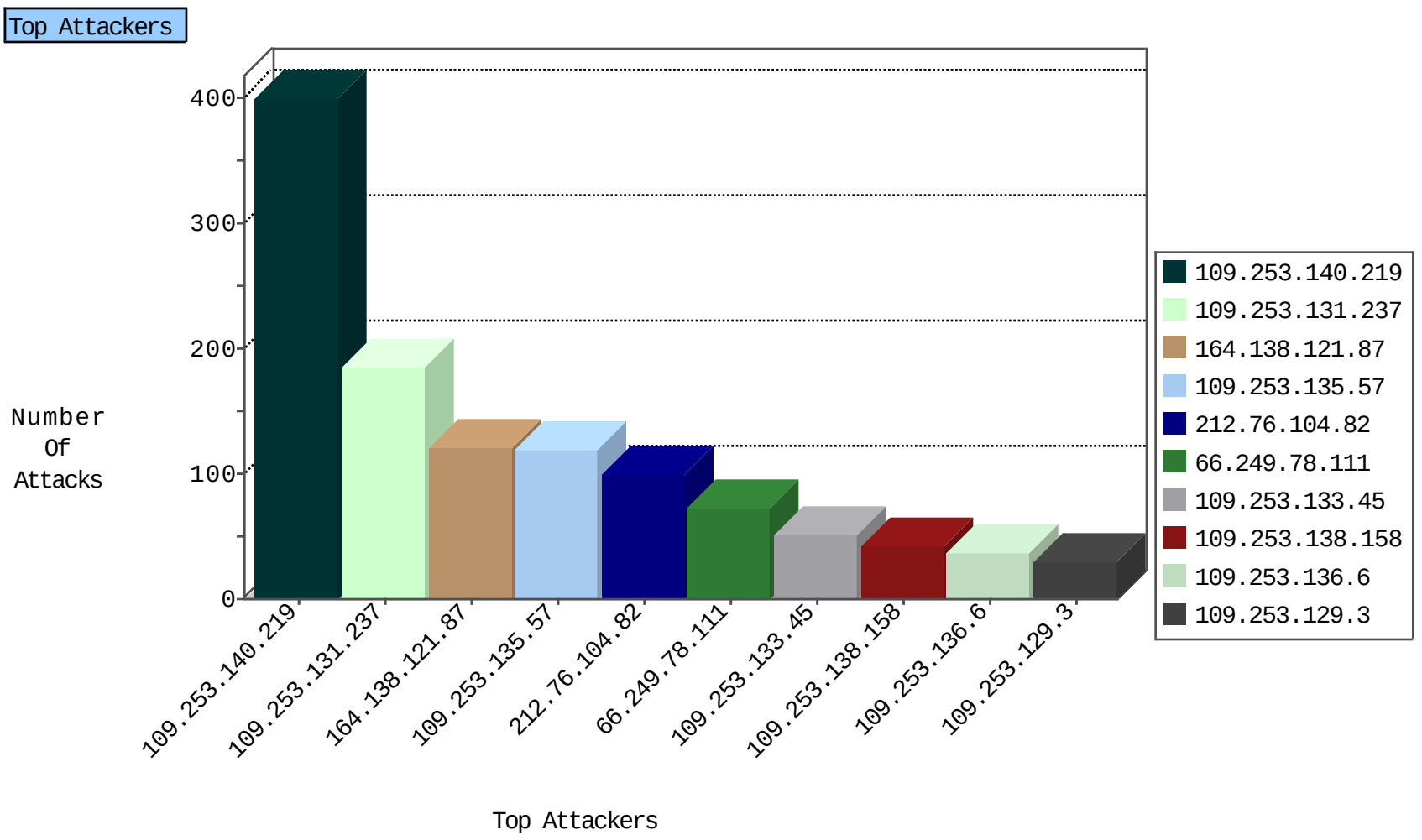
04-26-2015-18:03:07 to 04-26-2015-19:03:07

IDF Under Attack
04-26-2015-18:03:07

Top Targets



Top Attackers



04-26-2015-18:03:07 to 04-26-2015-19:03:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.78.9	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	6193
66.249.78.111	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	4186
66.249.78.96	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	2105
66.249.78.104	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	1568
77.126.175.247	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	983
66.249.78.82	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	806
66.249.78.97	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	676
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	648
66.249.78.89	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	287
66.249.75.58	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	248
212.143.110.33	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	235
66.249.78.2	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	229
37.26.148.151	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	218
207.46.13.1	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	192
213.57.137.150	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	130
79.181.241.78	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	25
212.143.40.37	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	19
109.66.147.118	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
24.135.229.97		147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
46.117.128.85	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
81.218.135.161	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
66.249.67.92	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	1
23.95.82.226	United States	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
82.80.54.167	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
66.249.78.31	Israel	147.237.77.226	www.chamatz.aka.idf.il	TCP handshake violation, first packet not syn	drop	1
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
176.12.136.201	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
109.65.151.121	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
66.249.78.254	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1
66.249.78.45	Israel	147.237.77.226	www.chamatz.aka.idf.il	TCP handshake violation, first packet not syn	drop	1
185.32.176.239	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
79.183.55.153	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
52.16.5.197	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
37.142.217.25	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
109.67.108.217	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
78.131.209.186	Poland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

04-26-2015-18:03:07 to 04-26-2015-19:03:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
71.6.165.200	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.159	Israel	147.237.76.86	navy.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.135.131	United States	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	1

04-26-2015-18:03:07 to 04-26-2015-19:03:07

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	4
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
91.224.132.118	Russian Federation	147.237.72.166	aka.idf.il	ET SCAN NMAP -sS window 1024	1
85.65.205.228	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	1
79.180.133.44	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
46.117.192.36	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.153	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
43.255.191.165	Japan	147.237.77.205	prisha.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.165	Japan	147.237.8.28	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
212.179.222.212	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
31.168.205.197	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
109.67.116.65	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
1.93.23.196	China	147.237.76.148	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
87.69.180.202	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
77.127.74.118	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
46.116.211.238	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
43.255.191.165	Japan	147.237.77.235	sviva.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.165	Japan	147.237.76.197	e.himush.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.165	Japan	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
1.93.24.229	China	147.237.72.217	e.idf.il	ET SCAN NMAP -sS window 1024	1

04-26-2015-18:03:07 to 04-26-2015-19:03:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
164.138.121.87	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	121
212.76.104.82	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	100
109.253.136.6	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	37
46.116.211.238	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	22
109.253.142.101	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	19
109.253.141.14	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
109.253.133.161	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
141.0.10.17	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
37.26.147.130	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
93.172.18.17	Israel	147.237.76.42	refuah.idf.i	SYN retransmit with different window scale	Bad TCP sequence	monitor	5
109.253.141.117	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
37.26.147.138	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
91.135.102.171	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
212.143.110.33	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
207.46.13.1	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
149.78.153.75	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
207.46.13.95	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
31.186.228.94	United Kingdom	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
89.139.184.98	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
109.253.129.92	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
81.218.55.253	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
109.253.131.95	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
2.54.35.12	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
185.26.180.143	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
46.116.224.208	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
192.115.98.200	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
157.55.39.3	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
188.120.148.134	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
77.125.119.104	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
149.78.97.192	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
31.154.10.196	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
79.179.99.198	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
188.165.15.13	France	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
77.127.160.181	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
213.57.225.88	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
31.168.65.82	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
109.253.159.143	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
46.19.86.249	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
212.179.46.22	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
77.127.183.192	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
109.253.139.202	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
93.172.34.126	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
80.246.130.194	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
212.179.61.124	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
87.69.231.239	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
109.253.140.219	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	401
109.253.131.237	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	186
109.253.135.57	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	120
109.253.133.45	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	51
109.253.138.158	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	42
109.253.129.3	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	29
109.253.133.59	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	26
5.29.127.37	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	8
79.177.114.31	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	6
79.180.237.210	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	6
79.182.39.170	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	5
157.55.39.3	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
109.253.143.110	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	4
213.251.182.103	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/0/size220x0/3410.jpg.src	Block	3
85.64.149.67	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
37.26.146.154	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	3
85.64.86.246	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/1/	Block	2
109.253.136.156	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	2
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	2
149.78.238.199	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
79.177.183.73	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
207.46.13.131	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
85.65.127.87	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
95.86.76.138	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/giyus/www.navy.idf.il	Block	2
84.94.46.196	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
87.68.57.175	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
93.172.18.17	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/webresource.axd	Block	1
66.249.69.32	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/938-he/refuah.aspx	Block	1
82.102.136.68	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
37.142.54.242	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
185.32.178.187	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
17.142.152.71	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/idf_in_pictures/2000/october/piguim.stm	Block	1
149.78.227.189	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
66.249.75.74	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_moreinfo.asp	Block	1
66.249.64.62	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to atal.idf.il/templates/shared/usercontrols/trajector/	Block	1
212.150.128.10	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/statistics/gens.stm	Block	1
79.182.150.232	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyusâ€”	Block	1
31.186.228.94	United Kingdom	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
157.55.39.8	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
69.125.226.201	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
66.249.69.32	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1065-he/dover.aspx	Block	1
192.185.83.222	United States	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
82.102.136.69	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
46.19.85.1	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
24.135.229.97		147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 24.135.229.97	Block	1
66.249.75.117	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sachar/forms/downloadform.asp	Block	1
66.249.64.91	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
212.179.42.227	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42//webresource.axd	Block	1
80.246.133.250	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1

04-26-2015-18:03:07 to 04-26-2015-19:03:07