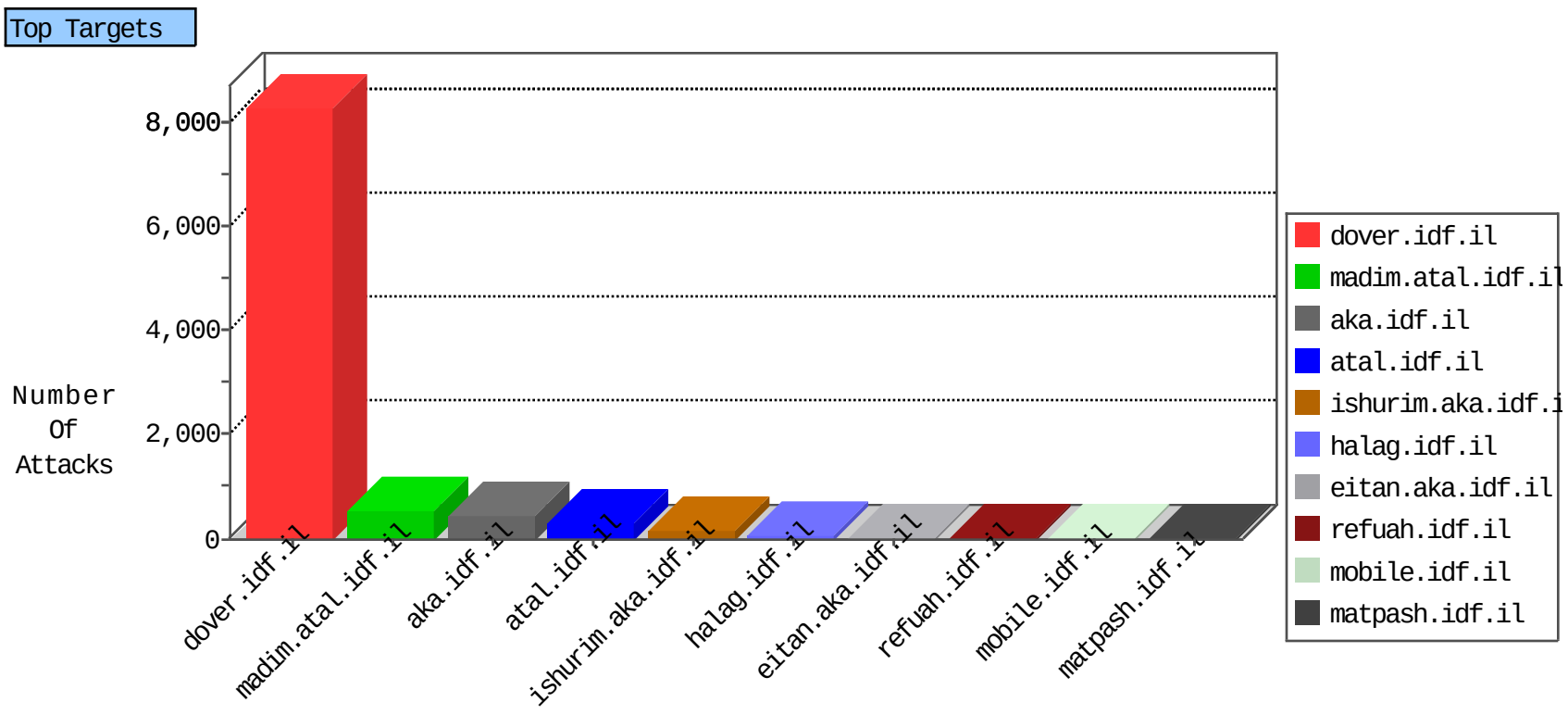
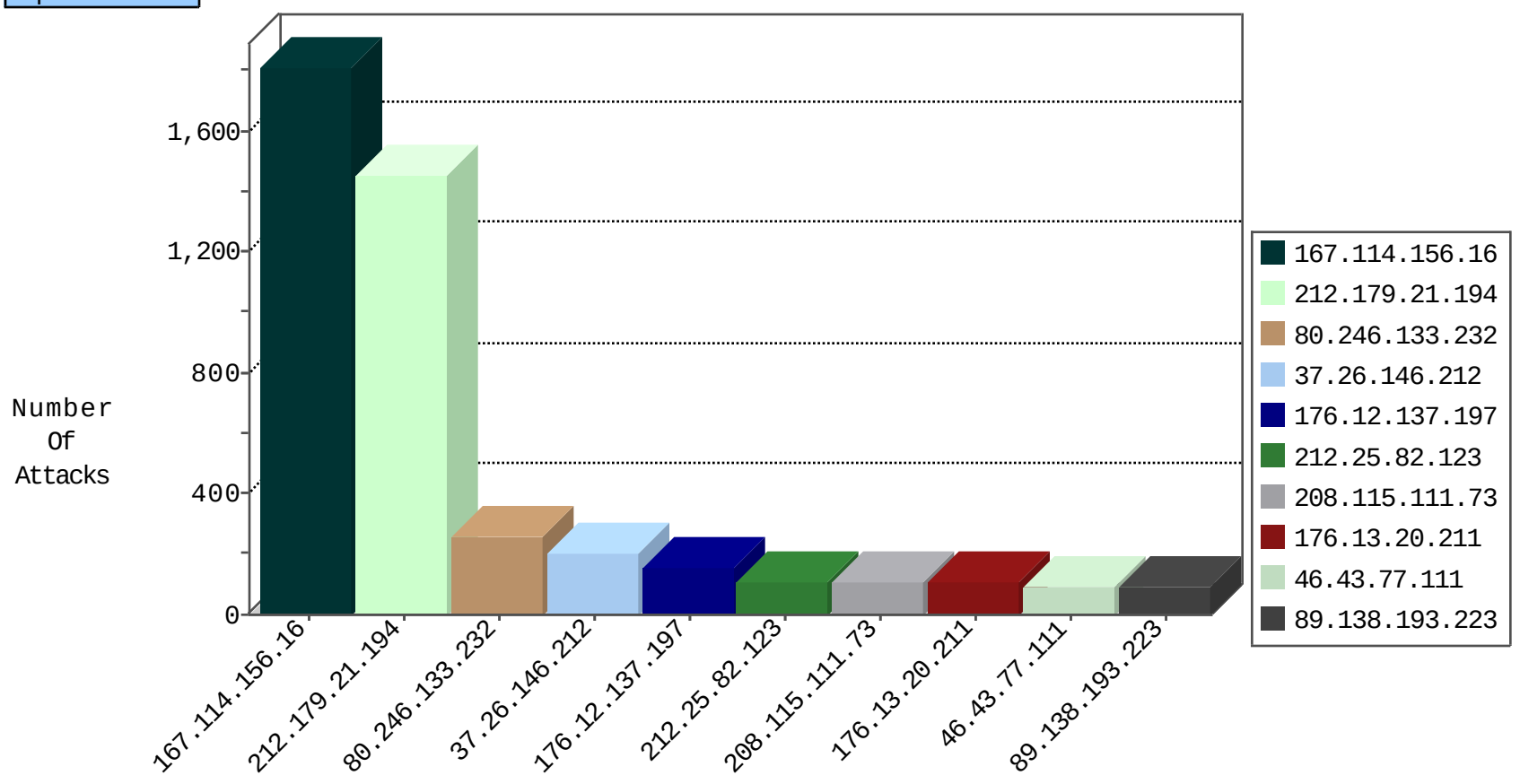
11-08-2015-10:04:05 to 11-08-2015-11:04:05

IDF Under Attack Daily Report

Top Targets



Top Attackers



11-08-2015-10:04:05 to 11-08-2015-11:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.i	DOS-Tool-SwitchbladG	dest-reset	2736
0.0.0.0		147.237.77.216	dover.idf.i	SYN Flood full table	drop	359
212.199.108.202	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	39
176.13.0.238	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	37
93.172.25.228	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	34
2.54.139.71	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	25
2.54.208.202	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	25
84.108.63.182	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	21
46.116.252.184	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	19
80.246.136.216	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	19
95.86.98.224	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	17
45.114.179.244		147.237.77.216	dover.idf.i	SYN Flood full table	drop	15
79.182.23.33	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	15
86.142.234.64	United Kingdom	147.237.77.216	dover.idf.i	SYN Flood full table	drop	11
84.108.138.1	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	10
212.179.21.194	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	10
212.199.108.202	Israel	147.237.77.216	dover.idf.i	SYN Flood out of context	drop	10
94.230.89.132	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	10
95.86.68.72	Israel	147.237.77.216	dover.idf.i	SYN Flood unverified cookie	drop	10
31.168.121.205	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	10
89.139.161.178	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	10
84.229.174.108	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	9
199.203.62.41	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	9
80.246.136.193	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	8
149.78.123.140	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	8
82.80.196.44	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	7
46.116.152.138	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	6
79.182.67.226	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	6
79.176.194.93	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	6
2.52.188.137	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	6
109.160.132.20	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	6
2.52.135.54	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	6
46.116.103.98	Israel	147.237.77.216	dover.idf.i	SYN Flood unverified cookie	drop	6
84.228.161.7	Israel	147.237.77.216	dover.idf.i	SYN Flood unverified cookie	drop	6
46.120.64.138	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	6
109.65.125.155	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	5
212.179.21.194	Israel	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	5
2.54.139.71	Israel	147.237.77.216	dover.idf.i	SYN Flood out of context	drop	5
80.246.138.131	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	5
2.54.59.12	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	4
37.8.93.249	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	SYN Flood full table	drop	4
37.26.149.244	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	4
2.52.161.178	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	4
2.54.174.218	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	4
79.183.55.161	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	4
212.199.108.202	Israel	147.237.77.216	dover.idf.i	SYN Flood unverified cookie	drop	4
194.90.25.90	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	4
5.102.254.43	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	3
2.52.140.21	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	3
81.218.48.37	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	3

11-08-2015-10:04:05 to 11-08-2015-11:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
134.191.232.69	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
134.191.232.72	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
195.160.240.11	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
80.230.24.46	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1

11-08-2015-10:04:05 to 11-08-2015-11:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.73.212	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sA (2)	20
176.13.6.105	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
111.93.198.54	147.237.76.86	India	navy.idf.il	ET SCAN NMAP -f -sS	1
79.177.9.235	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
59.2.36.33	147.237.76.86	Korea, Republic of	navy.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	1
204.13.204.139	147.237.0.35	United States	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
176.13.23.103	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
111.93.198.54	147.237.76.86	India	navy.idf.il	ET SCAN NMAP -sS window 2048	1
80.246.136.240	147.237.72.167	Israel	ishurim.aka.idf.i	portscan: TCP Distributed Portscan	1
46.151.52.8	147.237.8.14	Ukraine	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
212.29.192.150	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
198.20.69.98	147.237.77.74	United States	law.idf.il	ET DROP Dshield Block Listed Source	1

11-08-2015-10:04:05 to 11-08-2015-11:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.179.21.194	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	1444
80.246.133.232	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	232
212.25.82.123	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	107
208.115.111.73	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	105
46.43.77.111	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	91
89.138.193.223	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	89
85.65.60.23	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	87
82.173.140.195	Netherlands	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	75
46.19.86.242	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	71
2.52.136.113	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	66
212.143.110.33	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	58
82.192.68.46	Netherlands	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	56
192.116.167.41	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	56
168.63.139.43	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	55
149.78.154.69	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	52
5.29.154.237	Israel	147.237.77.234	halag.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	51
80.179.115.198	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	51
46.18.17.249	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	49
208.69.40.101	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	46
54.72.0.55	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	44
54.72.73.168	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	44
41.33.231.90	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	43
37.26.149.242	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	43
46.116.162.242	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	41
46.19.85.192	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	40
52.16.5.197	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	36
62.219.48.135	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	36
64.233.172.171	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	35
46.19.85.164	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	35
68.180.228.112	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	35
64.233.172.163	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	34
93.220.28.236	Germany	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	34
212.179.90.106	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	34
66.249.65.231	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	34
64.233.172.155	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	33
66.249.65.224	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	30
66.249.81.212	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	30
50.87.144.145	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	30
95.86.68.72	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	30
212.199.108.202	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	29
82.81.3.74	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	28
217.136.50.226	Belgium	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	28
45.114.179.244		147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	27
37.26.148.201	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	27
100.100.60.65		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	27
100.100.29.162		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	25
46.116.152.138	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	25
66.249.81.218	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	25
66.249.65.231	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
82.81.129.229	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	24

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.146.212	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	184
176.12.137.197	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	106
176.13.20.211	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	73
46.19.85.43	Israel	147.237.72.166	aka.idf.il	Distributed Unknown HTTP Request Method	Block	50
176.12.137.197	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.12.137.197	Block	48
176.13.5.97	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	40
176.13.20.211	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	31
46.19.86.44	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	23
37.26.146.212	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	18
81.218.118.126	Israel	147.237.72.166	aka.idf.il	Multiple Unknown HTTP Request Method from 81.218.118.126	Block	17
176.12.141.144	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	13
66.249.67.216	Israel	147.237.72.166	aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	8
37.26.147.224	Israel	147.237.72.167	ishurim.aka.idf.i	Distributed Too Many of the Same Response Code (404)	Block	6
176.12.140.108	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
178.150.15.158	Ukraine	147.237.72.166	aka.idf.il	PHP Attempt	Block	6
192.116.232.69	Israel	147.237.72.167	ishurim.aka.idf.i	Distributed Too Many of the Same Response Code (404)	Block	6
178.150.15.158	Ukraine	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 178.150.15.158	Block	5
199.203.100.145	Israel	147.237.72.167	ishurim.aka.idf.i	Distributed Too Many of the Same Response Code (404)	Block	4
80.246.136.240	Israel	147.237.72.167	ishurim.aka.idf.i	Distributed Too Many of the Same Response Code (404)	Block	4
37.26.148.201	Israel	147.237.72.167	ishurim.aka.idf.i	Distributed Too Many of the Same Response Code (404)	Block	4
176.12.136.78	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
194.90.255.226	Israel	147.237.72.167	ishurim.aka.idf.i	Distributed Too Many of the Same Response Code (404)	Block	3
66.249.67.224	Israel	147.237.72.166	aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	3
2.54.63.121	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.181.174.130	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/0/	Block	3
212.117.143.250	Israel	147.237.72.167	ishurim.aka.idf.i	Distributed Too Many of the Same Response Code (404)	Block	3
46.19.86.198	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
66.249.67.208	Israel	147.237.72.166	aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	3
94.230.92.190	Israel	147.237.72.166	aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	2
80.246.140.20	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
82.81.34.74	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ajax/pages/fan_status.php	Block	2
80.179.202.191	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
46.19.85.105	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
192.116.217.10	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
149.78.15.150	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	2
87.69.173.167	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.10.128	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
2.54.45.122	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
80.246.139.7	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
40.77.167.91	United States	147.237.76.147	chinuch.aka.idf.i	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	2
149.78.237.68	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 149.78.237.68	Block	2
82.81.34.74	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	2
66.249.69.49	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/0/105860.pdf	Block	1
212.143.3.44	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
2.54.46.143	Israel	147.237.72.167	ishurim.aka.idf.i	Distributed Too Many of the Same Response Code (404)	Block	1
85.65.60.23	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	1
66.249.67.65	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/smalim/showbig.aspx	Block	1
188.138.17.205	France	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to 147.237.76.147/	Block	1
46.210.139.199	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1

11-08-2015-10:04:05 to 11-08-2015-11:04:05