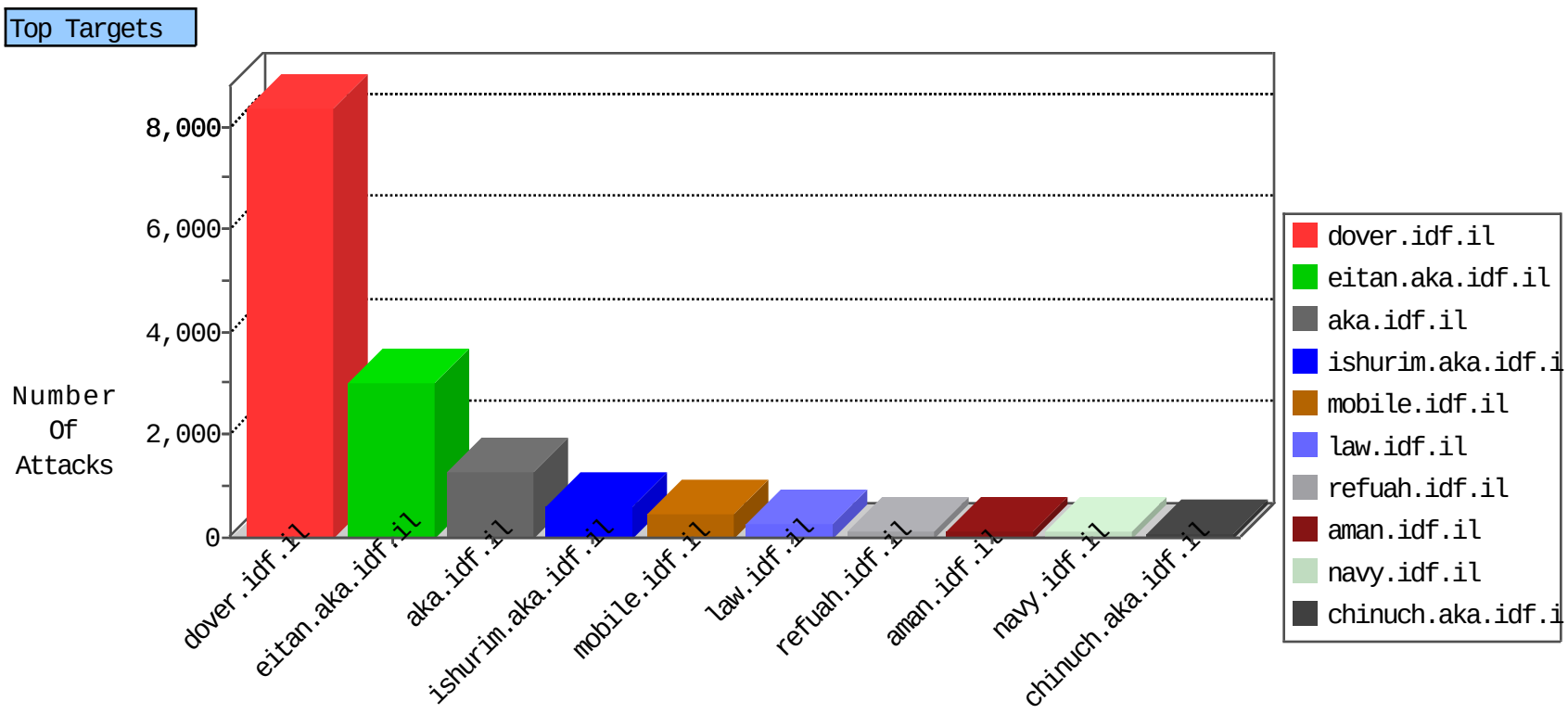
11-01-2015-13:04:09 to 11-01-2015-14:04:09

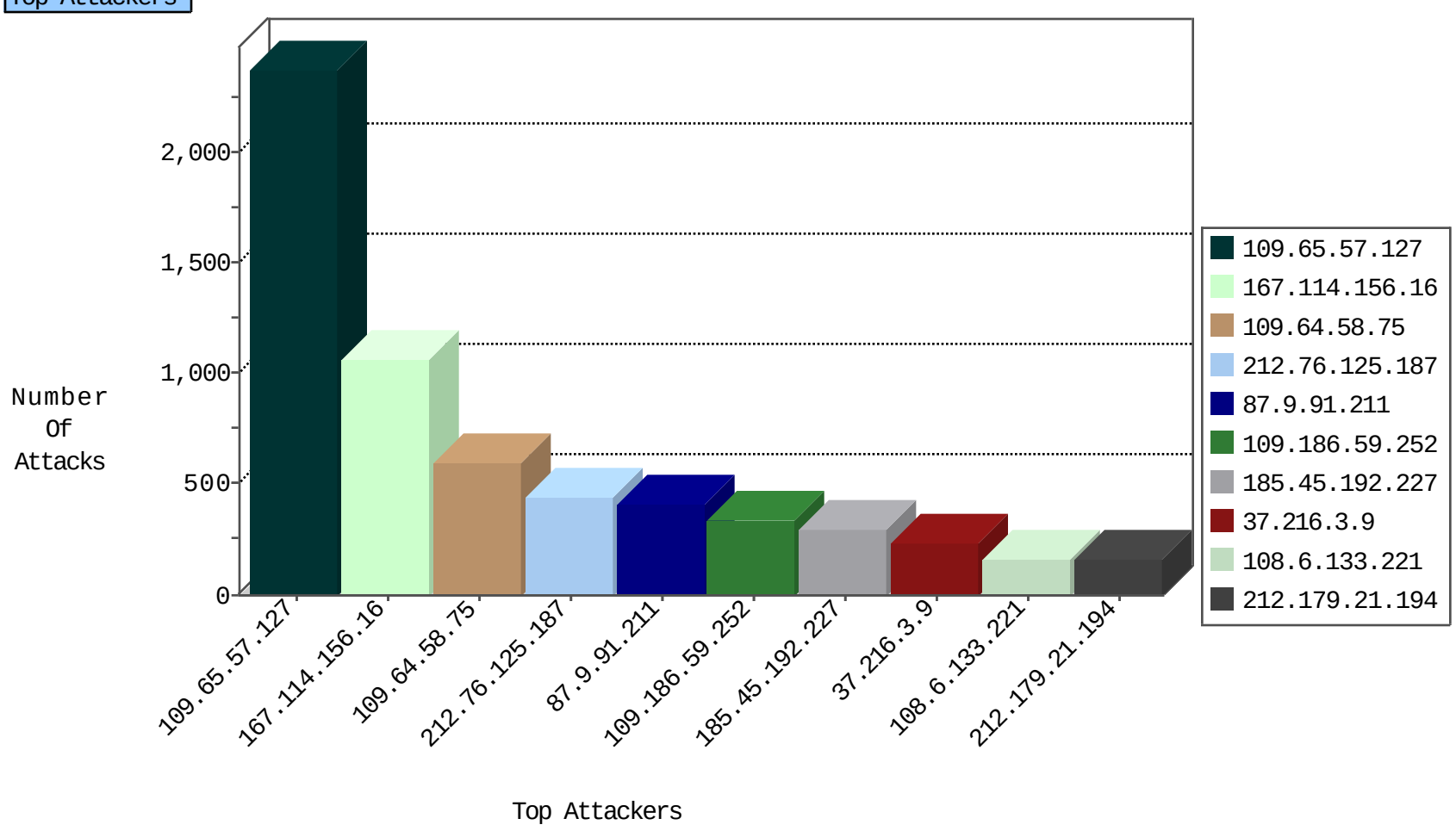
IDF Under Attack
Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

11-01-2015-13:04:09 to 11-01-2015-14:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.67.122	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	4477
79.182.223.94	Israel	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	1180
0.0.0.0		147.237.77.216	dover.idf.i	SYN Flood full table	drop	439
66.249.78.173	United States	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	332
46.19.86.183	Israel	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	286
108.6.133.221	United States	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	176
167.114.156.16	Canada	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	135
167.114.156.16	Canada	147.237.77.216	dover.idf.i	DOS-Tool-SwitchbladG	dest-reset	48
81.218.97.45	Israel	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	43
79.177.4.217	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	40
79.182.190.214	Israel	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	38
62.219.228.143	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	32
79.180.147.209	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	31
2.52.41.126	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	30
85.250.49.53	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	28
109.65.49.253	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	27
46.19.85.189	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	25
37.142.97.13	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	20
54.244.22.103	United States	147.237.77.216	dover.idf.i	SYN Flood full table	drop	18
2.52.163.236	Israel	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	17
108.6.133.221	United States	147.237.77.216	dover.idf.i	SYN Flood full table	drop	17
79.179.121.110	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	16
176.13.16.213	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	16
87.69.242.220	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	15
84.95.228.148	Israel	147.237.77.216	dover.idf.i	SYN Flood unverified cookie	drop	14
109.65.57.127	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	12
46.19.85.200	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	10
79.179.172.121	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	10
212.235.98.139	Israel	147.237.77.216	dover.idf.i	SYN Flood unverified cookie	drop	9
77.2.251.59	Germany	147.237.77.216	dover.idf.i	SYN Flood full table	drop	9
149.78.124.3	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	9
62.0.102.190	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	7
176.13.16.213	Israel	147.237.77.216	dover.idf.i	SYN Flood unverified cookie	drop	7
46.19.85.64	Israel	147.237.77.216	dover.idf.i	SYN Flood unverified cookie	drop	7
132.74.168.177	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	7
79.180.147.209	Israel	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	7
92.201.66.247	Germany	147.237.77.216	dover.idf.i	SYN Flood full table	drop	7
79.178.185.149	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	6
46.19.86.85	Israel	147.237.77.216	dover.idf.i	SYN Flood unverified cookie	drop	6
188.225.180.51	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	SYN Flood unverified cookie	drop	6
79.182.3.52	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	6
77.125.247.14	Israel	147.237.77.216	dover.idf.i	SYN Flood unverified cookie	drop	6
46.19.85.189	Israel	147.237.77.216	dover.idf.i	SYN Flood unverified cookie	drop	5
37.216.3.9	Saudi Arabia	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	5
93.172.53.242	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	5
2.54.3.56	Israel	147.237.77.216	dover.idf.i	SYN Flood unverified cookie	drop	5
81.218.97.45	Israel	147.237.77.216	dover.idf.i	SYN Flood unverified cookie	drop	5
188.225.180.51	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	SYN Flood full table	drop	5
149.78.229.51	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	5
0.0.0.0		147.237.77.216	dover.idf.i	SYN Flood unverified cookie	drop	5

11-01-2015-13:04:09 to 11-01-2015-14:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	8262: HTTP: Slowloris DoS Tool	Block	21
81.218.33.77	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1

11-01-2015-13:04:09 to 11-01-2015-14:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
31.168.68.3	147.237.77.216	Israel	dover.idf.i	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	20
195.34.150.18	147.237.77.216	Austria	dover.idf.i	Tehila - Perl LWP with fake user agent	2
2.54.7.77	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
176.13.4.190	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.64.50.218	147.237.77.216	Israel	dover.idf.i	portscan: TCP Distributed Portscan	1
82.166.22.6	147.237.77.216	Israel	dover.idf.i	portscan: TCP Distributed Portscan	1
81.218.46.66	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.180.121.113	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.120.206.11	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
41.33.231.90	147.237.77.216	Egypt	dover.idf.i	Tehila - Perl LWP with fake user agent	1
2.54.165.88	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
176.13.15.78	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
176.13.2.31	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.95.228.148	147.237.77.216	Israel	dover.idf.i	portscan: TCP Distributed Portscan	1
82.80.147.22	147.237.77.216	Israel	dover.idf.i	portscan: TCP Distributed Portscan	1
80.246.130.236	147.237.77.216	Israel	dover.idf.i	portscan: TCP Distributed Portscan	1
66.249.69.84	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	1
46.19.86.223	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.27.105.70	147.237.77.216	Israel	dover.idf.i	portscan: TCP Distributed Portscan	1

11-01-2015-13:04:09 to 11-01-2015-14:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1023
109.65.57.127	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	660
212.76.125.187	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	439
87.9.91.211	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	409
109.64.58.75	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	369
37.216.3.9	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	225
37.26.148.232	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	155
108.6.133.221	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	154
212.143.134.129	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	117
41.38.152.40	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	107
46.19.86.43	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	99
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	93
79.181.199.139	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	85
41.142.200.171	Morocco	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	81
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	75
46.120.229.31	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	70
65.49.68.199	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	69
213.151.62.149	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	65
62.219.228.143	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	61
81.218.251.251	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	61
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	59
79.182.223.94	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	59
212.235.98.139	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	57
109.66.168.109	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	56
85.64.188.185	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	54
37.142.122.193	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	54
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	54
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	52
54.244.22.103	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
107.222.34.206	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	50
46.19.85.37	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	50
132.66.237.166	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	49
46.116.98.44	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
54.187.55.213	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
46.19.86.96	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
31.96.215.118	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
79.180.147.209	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
80.246.133.11	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
62.150.17.6	Kuwait	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
176.12.140.201	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
87.69.193.201	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
31.154.34.130	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
66.249.78.159	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	32
195.160.240.11	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
46.19.86.189	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
77.2.251.59	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
2.54.187.74	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30

11-01-2015-13:04:09 to 11-01-2015-14:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.65.57.127	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	1680
109.186.59.252	Israel	147.237.72.167	ishurim.aka.idf.i	Distributed Too Many of the Same Response Code (404)	Block	330
109.64.58.75	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	227
185.45.192.227	Netherlands	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/__	Block	210
2.54.187.74	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	90
37.142.122.193	Israel	147.237.76.147	chinuch.aka.idf.i	Distributed Too Many of the Same Response Code (404)	Block	75
185.45.192.227	Netherlands	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/__	Block	75
46.19.86.148	Israel	147.237.72.166	aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	60
176.13.11.141	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	60
193.169.70.101	Israel	147.237.72.167	ishurim.aka.idf.i	Distributed Too Many of the Same Response Code (404)	Block	60
212.143.24.176	Israel	147.237.72.167	ishurim.aka.idf.i	Distributed Too Many of the Same Response Code (404)	Block	60
212.179.21.194	Israel	147.237.72.166	aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	60
212.25.102.57	Israel	147.237.72.167	ishurim.aka.idf.i	Distributed Too Many of the Same Response Code (404)	Block	30
46.120.229.31	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/size100x0/sip_storage	Block	30
85.250.74.139	Israel	147.237.77.233	atal.idf.il	Parameter Type Violation searchText in www.atal.idf.il/1620-he/atal.aspx	Block	30
2.54.188.84	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	30
109.66.112.34	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	30
185.27.105.138	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/default.aspx	Block	30
37.26.149.221	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/aman	Block	30
5.29.49.180	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	30
46.19.85.167	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	30
31.168.230.122	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	30
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	30
157.55.39.142	United States	147.237.72.166	aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	30
2.52.131.210	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	30
84.109.32.240	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for aka.idf.il/drushim	Block	30
66.249.67.122	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	30
109.67.179.191	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	30
2.54.47.136	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	15
85.65.80.220	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/aman	Block	15
66.249.65.139	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/navy/ajaxpage.aspx	Block	15
188.161.20.54	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	15
80.246.133.167	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	15
37.26.147.132	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/faq.aspx	Block	15
149.78.82.123	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	15
66.249.81.215	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/id=125	Block	15
220.181.108.115	China	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/sip_storage/files/3/size338x0/1613.jpg	Block	15
66.249.67.122	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.67.122	Block	15
176.13.23.139	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	15
2.52.10.104	Israel	147.237.72.166	aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	15
83.222.232.216	United Kingdom	147.237.72.166	aka.idf.il	Unauthorized URL Access to /	Block	15
79.178.124.203	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	15
46.19.85.7	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	15
176.12.136.163	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	15
31.168.103.115	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 31.168.103.115	Block	15
109.160.142.77	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 109.160.142.77	Block	15
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	15
212.199.57.197	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	15
2.54.133.29	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	15
66.249.65.251	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/navy/default.aspx×¦×•	Block	15

11-01-2015-13:04:09 to 11-01-2015-14:04:09