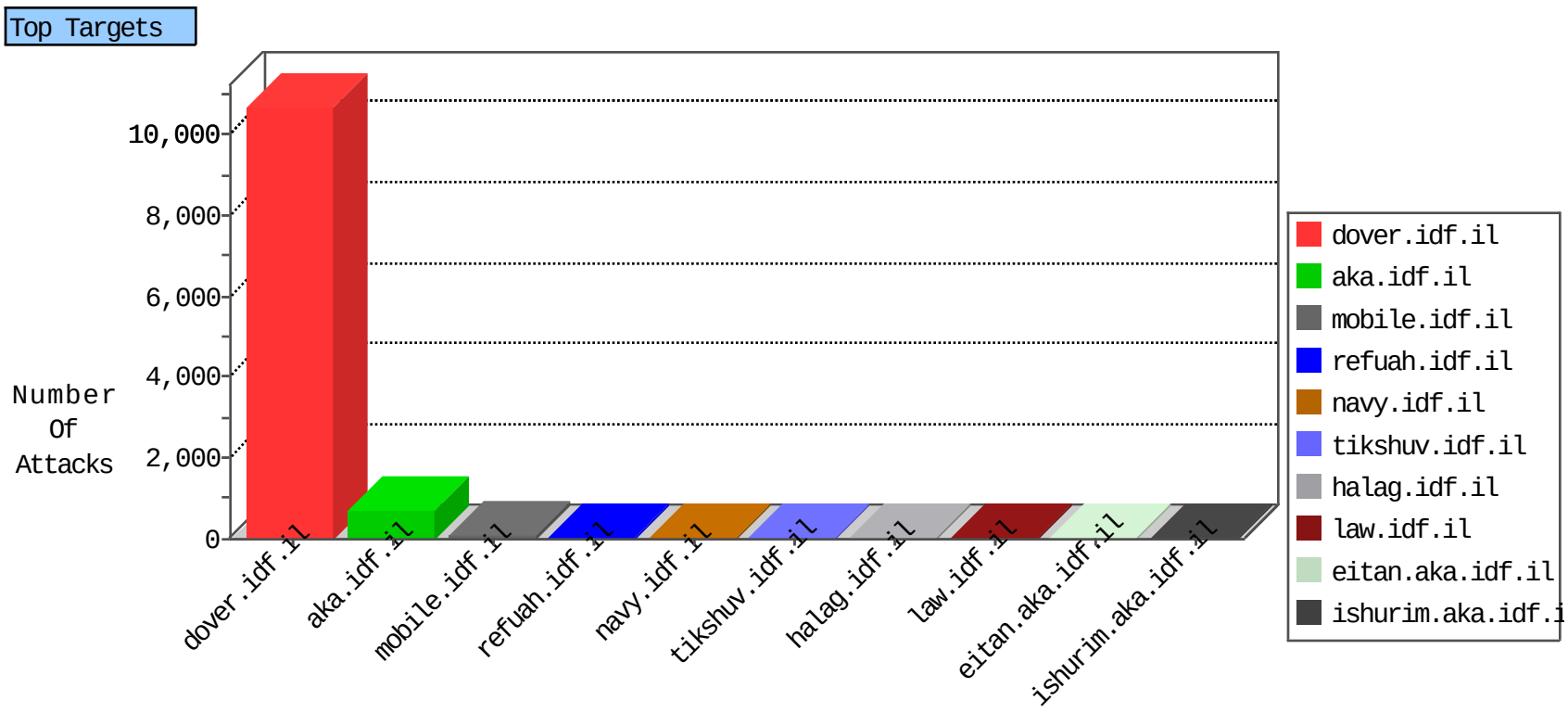
11-02-2015-21:04:01 to 11-02-2015-22:04:01

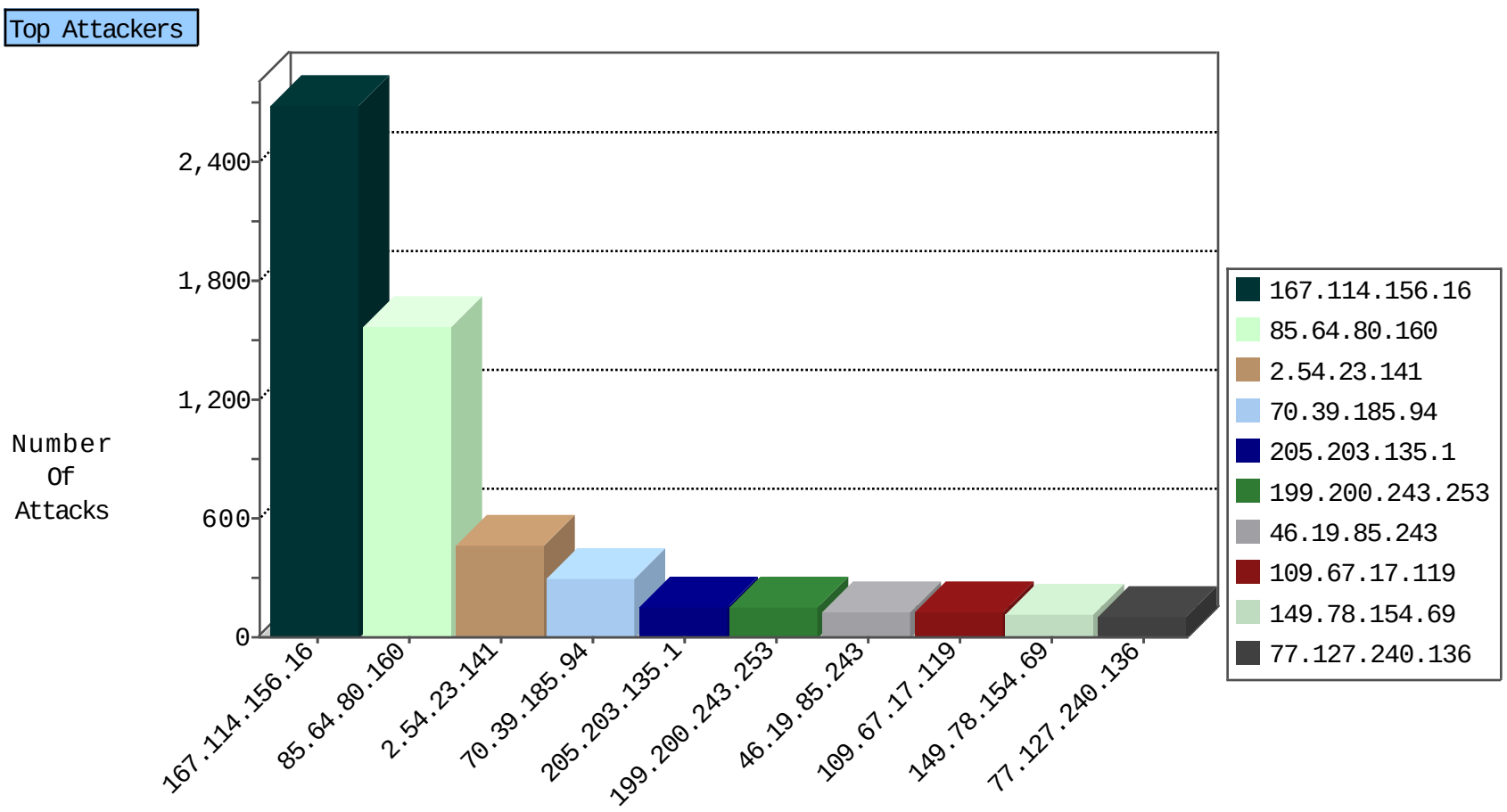
IDF Under Attack
Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

11-02-2015-21:04:01 to 11-02-2015-22:04:01

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.il	DOS-Tool-SwitchbladG	dest-reset	3074
167.114.156.16	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2567
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1847
66.249.88.81	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1409
50.58.193.130	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1255
66.249.64.186	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	769
66.249.67.6	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	465
66.249.67.27	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	244
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	198
220.181.108.80	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	152
66.249.67.224	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	104
109.186.146.109	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	75
79.183.145.120	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	36
37.142.153.214	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	33
2.54.136.199	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	33
66.249.75.114	United States	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	29
79.176.180.197	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	18
85.130.219.89	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	12
79.178.50.244	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	12
84.109.3.163	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	11
84.228.118.130	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
79.182.22.47	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
37.142.64.104	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
46.117.70.91	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
217.208.155.154	Sweden	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
109.66.52.249	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
2.52.147.152	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
93.173.22.121	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
89.139.183.248	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
66.249.64.181	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	6
66.249.67.122	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	6
46.121.61.195	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
213.57.194.137	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
46.116.104.199	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
213.233.84.234	Romania	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
176.13.6.0	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
85.65.6.17	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
79.176.154.15	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
149.88.228.138	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
79.182.23.86	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
109.65.42.144	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
87.68.157.161	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
79.178.148.117	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
212.179.155.129	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
90.177.100.129	Czech Republic	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
176.13.17.178	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
2.54.165.96	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
62.219.254.22	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
46.19.86.142	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
37.26.147.159	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3

11-02-2015-21:04:01 to 11-02-2015-22:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.180.14.147	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
94.159.157.9	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2

11-02-2015-21:04:01 to 11-02-2015-22:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	11
77.127.134.236	147.237.0.34	Israel	tikshuv.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	9
66.249.64.153	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
37.142.68.56	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
191.196.221.74	147.237.0.33	Brazil	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
140.232.211.8	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
117.21.174.87	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
109.67.138.142	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
93.173.165.244	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
201.249.199.91	147.237.77.243	Venezuela	mobile.idf.il	ET SCAN Potential SSH Scan	1
58.253.96.122	147.237.77.212	China	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
201.249.199.91	147.237.77.226	Venezuela	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
149.78.12.19	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
117.21.174.87	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
117.21.174.87	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
109.64.185.165	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
58.253.96.122	147.237.77.212	China	e.dover.idf.il	ET SCAN NMAP -sS window 4096	1
201.249.199.91	147.237.77.233	Venezuela	atal.idf.il	ET SCAN Potential SSH Scan	1
46.31.103.60	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
201.249.199.91	147.237.77.212	Venezuela	e.dover.idf.il	ET SCAN Potential SSH Scan	1

11-02-2015-21:04:01 to 11-02-2015-22:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
85.64.80.160	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1571
2.54.23.141	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	458
70.39.185.94	Satellite Provide	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	287
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	156
199.200.243.253	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	145
46.19.85.243	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	131
109.67.17.119	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	130
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	119
77.127.240.136	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	106
37.26.148.245	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	103
37.140.188.78	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	97
54.187.55.213	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	96
46.19.85.223	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	93
67.217.129.7	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	84
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	72
213.233.84.234	Romania	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	66
94.23.159.155	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	66
78.95.32.175	Romania	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	60
100.100.39.69		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	58
100.100.68.18		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	55
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	52
212.179.155.129	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
140.232.211.8	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	46
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
85.65.165.205	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
98.102.163.137	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
82.173.140.195	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
2.54.165.96	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
109.65.42.144	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
37.46.39.64	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
46.117.70.91	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
88.128.80.122	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
66.249.78.166	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
37.201.193.81	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
37.26.146.214	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
151.80.31.112	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
66.249.78.159	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
79.179.107.237	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
207.46.13.114	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
79.179.145.251	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
109.66.52.249	Israel	147.237.77.243	mobile.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
82.80.159.176	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
66.249.78.173	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
95.35.167.10	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
5.29.88.102	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
79.178.37.60	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21

11-02-2015-21:04:01 to 11-02-2015-22:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.180.228.100	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php	Block	8
79.180.228.100	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	8
79.180.228.100	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	8
5.29.66.98	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	6
89.138.55.7	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	6
5.29.66.98	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	6
5.29.66.98	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php	Block	6
84.109.92.50	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php	Block	5
84.109.92.50	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	5
79.177.208.198	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 79.177.208.198	Block	5
109.66.52.249	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
84.109.92.50	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	5
79.182.60.167	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	3
5.144.60.212	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	3
79.177.208.198	Israel	147.237.0.34	tikshuv.idf.il	PHP Attempt	Block	3
79.182.60.167	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	3
79.182.60.167	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php	Block	3
46.19.85.74	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	3
84.108.102.161	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php	Block	2
84.108.102.161	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	2
87.69.229.250	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	2
85.250.42.116	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	2
37.142.64.122	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
93.157.80.72	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
87.69.229.250	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php	Block	2
85.250.42.116	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php	Block	2
84.228.93.240	Israel	147.237.0.19	madim.atal.idf.i	Parameter Type Violation ctl00$ContentPlaceHolder1$txtStreet in madim.atal.idf.il/1088-he/meretz.aspx	Block	2
46.120.122.24	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	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
87.69.229.250	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	2
66.249.67.122	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
85.250.42.116	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	2
84.108.102.161	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	2
77.127.17.137	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/request.aspx	None	1
109.186.181.247	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.67.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/yohalan/forums/asp/showforum.asp	Block	1
88.238.230.171	Turkey	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
66.249.64.118	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/sip_storage/files/2/282.pdf	Block	1
87.69.41.177	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
79.180.52.223	Israel	147.237.72.166	aka.idf.il	Too Many Headers per Request - 42 Headers	Block	1
79.180.52.223	Israel	147.237.72.166	aka.idf.il	Abnormally Long Request method	Block	1
149.88.188.98	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush/site/he/himush.asp	Block	1
46.19.85.100	Israel	147.237.77.216	dover.idf.il	Malformed URL	Block	1
84.228.109.49	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	1
109.64.29.34	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/120203	Block	1
2.54.55.226	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.67.59	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/6/70006.doc	Block	1
87.69.205.215	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/ajax/updatestatus.php	Block	1
64.39.109.20	United States	147.237.72.156	aman.idf.il	Multiple Untraceable SSL Sessions from 64.39.109.20 (Protocol violation (SSL_CONN_CLIENT_KEY_EXCHANGE))	None	1

11-02-2015-21:04:01 to 11-02-2015-22:04:01