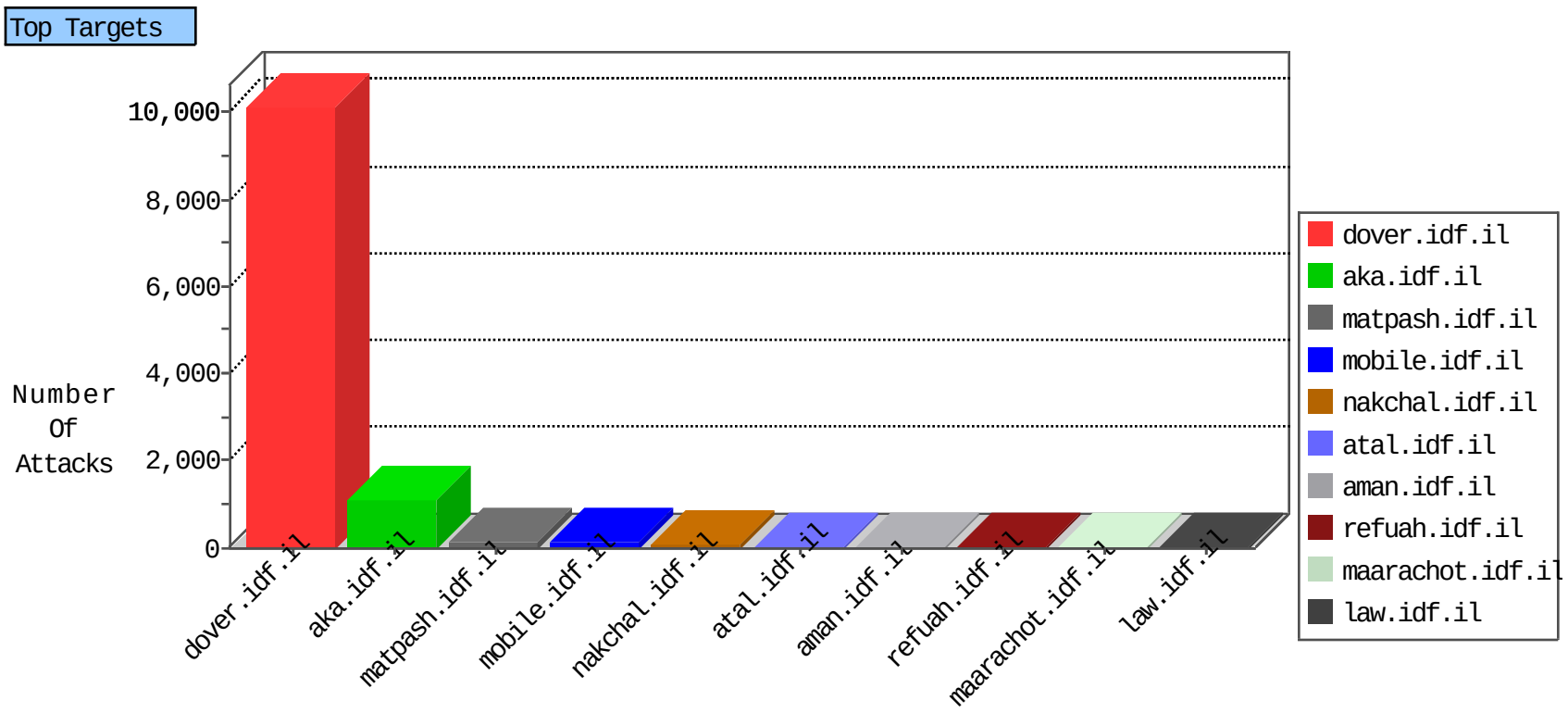
10-27-2015-23:04:08 to 10-28-2015-00:04:08

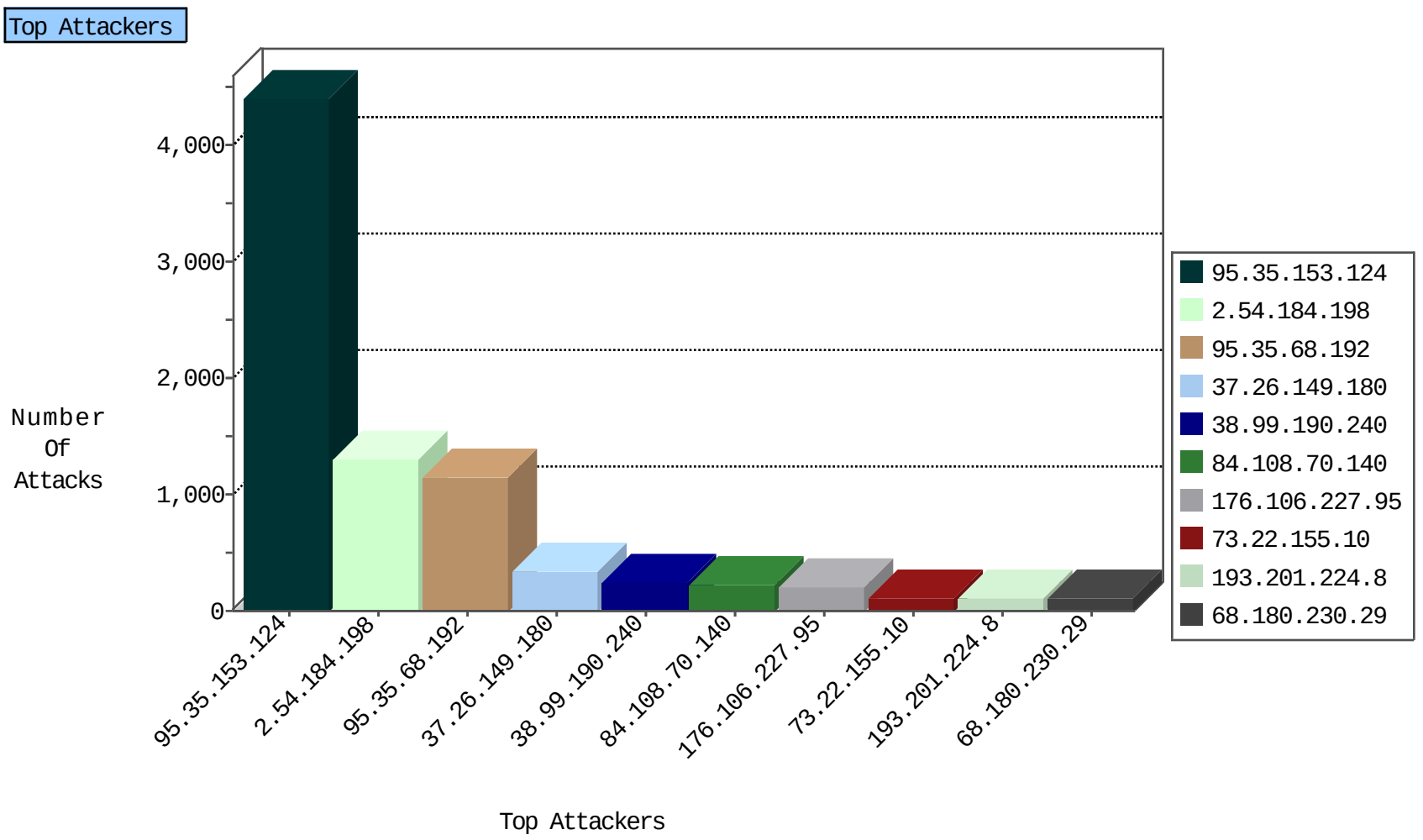
IDF Under Attack
Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

10-27-2015-23:04:08 to 10-28-2015-00:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	52
85.250.241.77	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	37
109.64.167.123	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	25
100.38.183.54	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	13
79.183.17.92	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	13
95.35.153.124	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
37.105.47.226	Saudi Arabia	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
46.120.190.80	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
95.86.76.152	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
62.219.254.22	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
95.86.65.53	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
37.26.149.130	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
115.239.248.245	China	147.237.76.42	refuah.idf.il	JLM_Under_Attack_Con_Http	drop	2
46.19.86.32	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
176.12.140.55	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
46.19.86.197	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
46.19.85.32	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
2.54.144.113	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
109.67.126.125	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
45.63.1.67		147.237.76.176	test.ncore.idf.il	Block_Ntp_All_Net	drop	1
46.19.86.201	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
5.8.66.70	Russian Federation	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
114.112.90.54	China	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1

10-27-2015-23:04:08 to 10-28-2015-00:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.121.228.158	Israel	147.237.77.216	dover.idf.il	C1000098: Block - dns poisoning	Block	3
173.48.141.204	United States	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1

10-27-2015-23:04:08 to 10-28-2015-00:04:08

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	8
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
41.140.253.9	147.237.8.14	Morocco	e.orchot.idf.il	ET SCAN NMAP -sS window 4096	1
193.107.17.72	147.237.76.38	Seychelles	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
119.90.139.50	147.237.77.121	China	e.navy.idf.il	ET SCAN NMAP -sS window 3072	1
119.90.139.50	147.237.77.121	China	e.navy.idf.il	ET SCAN NMAP -f -sS	1
115.182.17.13	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN NMAP -sS window 2048	1
89.248.171.19	147.237.76.198	Netherlands	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
65.79.240.148	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
217.219.67.177	147.237.77.61	Iran, Islamic Republic of	e.cogat.idf.il	ET SCAN NMAP -sS window 3072	1
58.63.239.135	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
217.219.67.177	147.237.77.61	Iran, Islamic Republic of	e.cogat.idf.il	ET SCAN NMAP -f -sS	1
58.63.239.135	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
193.201.224.8	147.237.72.166	Ukraine	aka.idf.il	SERVER-WEBAPP admin.php access	1
41.140.253.9	147.237.8.14	Morocco	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
169.54.233.120	147.237.76.202	Netherlands	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
119.90.139.50	147.237.77.121	China	e.navy.idf.il	ET SCAN NMAP -sS window 2048	1
115.182.17.13	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN NMAP -sS window 4096	1
115.182.17.13	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN NMAP -f -sS	1
89.44.207.205	147.237.8.28	Romania	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
58.63.239.135	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential SSH Scan	1
217.219.67.177	147.237.77.61	Iran, Islamic Republic of	e.cogat.idf.il	ET SCAN NMAP -sS window 2048	1
58.63.239.135	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1

10-27-2015-23:04:08 to 10-28-2015-00:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
95.35.153.124	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	4379
2.54.184.198	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	1304
95.35.68.192	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	1141
37.26.149.180	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	339
38.99.190.240	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	245
73.22.155.10	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	113
79.180.110.35	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	91
181.103.215.232	Argentina	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	69
149.78.154.69	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	57
68.180.228.112	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	57
84.228.198.17	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	53
82.192.68.46	Netherlands	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	51
54.187.55.213	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	43
109.67.185.129	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	42
65.13.19.193	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	39
41.33.232.66	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	37
2.54.11.19	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	36
37.142.140.250	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	33
79.182.200.102	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	32
66.249.78.173	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	32
66.249.78.166	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	31
212.179.90.106	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	29
84.228.150.175	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	28
66.249.78.159	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	28
41.33.231.90	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	28
54.72.73.168	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	27
187.105.21.152	Brazil	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	26
91.177.15.208	Belgium	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	26
50.87.144.145	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	26
31.154.160.170	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	25
79.182.186.216	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	24
54.72.0.55	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	24
46.19.86.204	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	23
100.100.58.175		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	23
46.19.86.191	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	22
151.80.31.112	Italy	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	22
92.241.36.127	Jordan	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	22
129.100.253.75	Canada	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	21
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	21
46.120.203.5	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	21
66.249.78.166	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
66.249.78.159	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	18
66.249.78.173	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	18
207.46.13.144	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	17
157.55.39.55	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	17
46.185.179.15	Jordan	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	15
66.249.64.173	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	15
100.100.51.107		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	15
100.38.183.54	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	14
52.16.5.197	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	13

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.108.70.140	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	112
84.108.70.140	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php	Block	112
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1934-he/cogat.aspx	Block	84
176.106.227.95	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	84
68.180.230.167	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in nakhal.idf.il/1111-he/nakhal.aspx	Block	84
68.180.229.239	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/general...067&docid=31516	Block	84
79.182.52.244	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152	Block	56
176.106.227.95	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php	Block	42
176.106.227.95	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ajax/updatestatus.php	Block	42
193.201.224.8	Ukraine	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	28
79.183.130.180	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	28
85.250.71.21	Israel	147.237.72.166	aka.idf.il	Distributed Parameter Read Only Violation www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx parameter	None	28
193.201.224.8	Ukraine	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 193.201.224.8	Block	28
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1380-he/dover.aspx	Block	28
176.58.78.108	Palestinian Territory Occupied	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to 147.237.0.15/	Block	14
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	14
93.173.248.129	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	14
46.116.179.206	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
212.76.99.253	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	14
84.110.144.2	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	14
184.173.183.172	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/14-en/patzar.aspx&usg=alkjrhhnk8ynchc3uf8fordeiy27zqiglq	Block	14
66.249.78.109	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-14396-he/dover.aspx	Block	14
109.186.23.155	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	14
85.113.106.124	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/en	Block	14
5.29.88.64	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	14
193.201.224.8	Ukraine	147.237.72.166	aka.idf.il	Multiple Admin Blocking from 193.201.224.8	Block	14
66.249.78.253	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/	Block	14
95.35.153.124	Israel	147.237.77.216	dover.idf.il	NULL Character in Method	Block	14
46.121.228.158	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	14
213.57.84.82	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
84.228.180.85	Israel	147.237.72.166	aka.idf.il	Distributed Parameter Read Only Violation www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx parameter	None	14
184.173.183.173	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/456-en/patzar.aspx&usg=alkjrhhh5npgyd2zcas-mm6h8kzietizfq	Block	14
149.88.244.60	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
31.154.167.230	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl13 in www.aka.idf.il/main/sachar/payslips.aspx	None	14
82.205.38.70	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-22777-ar/dover.aspx)	Block	14
66.249.64.235	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1361-10641-he/dover.aspx	Block	14
109.64.96.197	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/894-he/nakhal.aspx	Block	14
84.229.133.95	Israel	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 84.229.133.95	Block	14
77.126.22.61	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
185.120.126.63		147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/viewpniot.aspx	None	14
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	14
151.80.31.112	Italy	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
93.172.52.229	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	14
31.168.136.250	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	14
193.201.224.8	Ukraine	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-login.php	Block	14
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8867-he/refuah.aspx	Block	14
66.249.67.250	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	14
109.67.36.108	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	14
84.229.133.95	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/0/113730.pd	Block	14
79.176.161.215	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/request.aspx	None	14