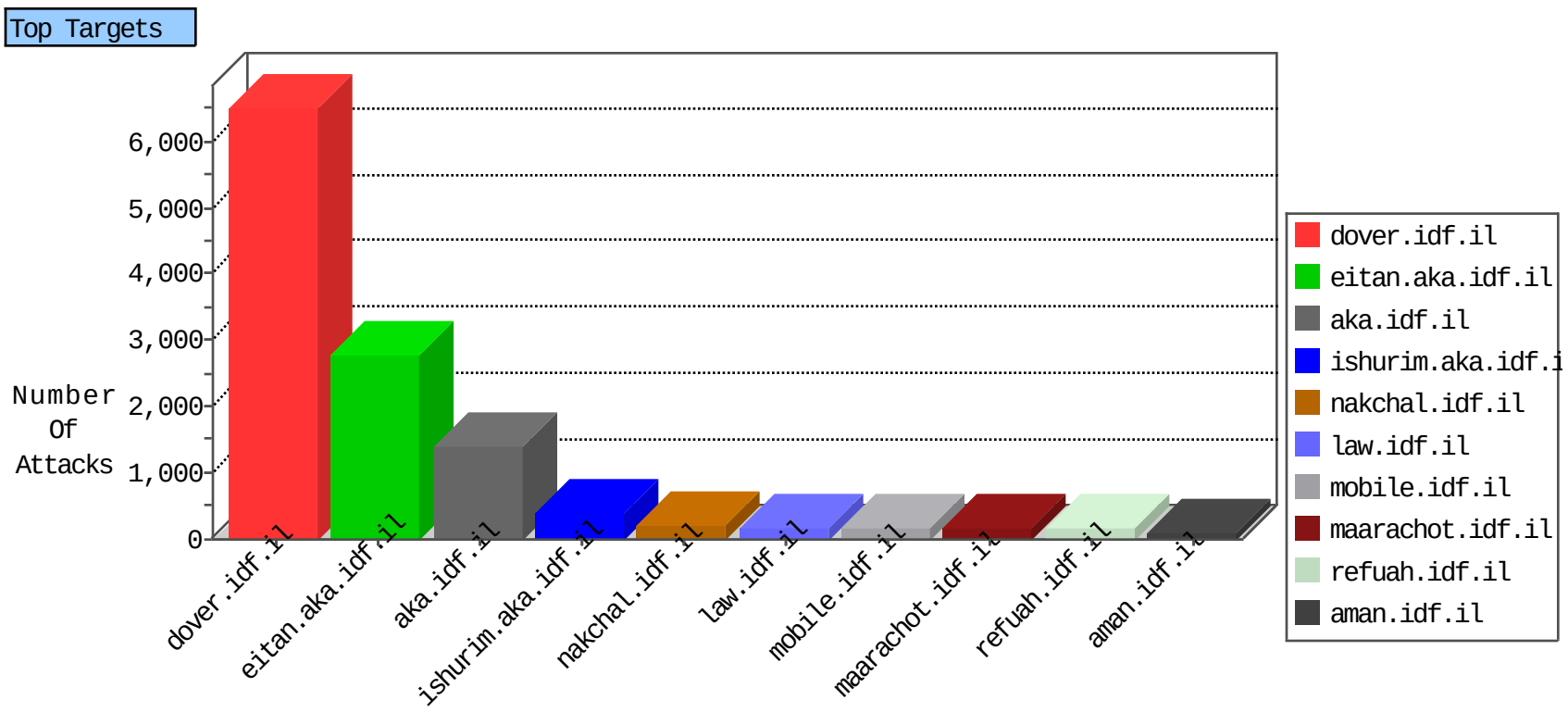
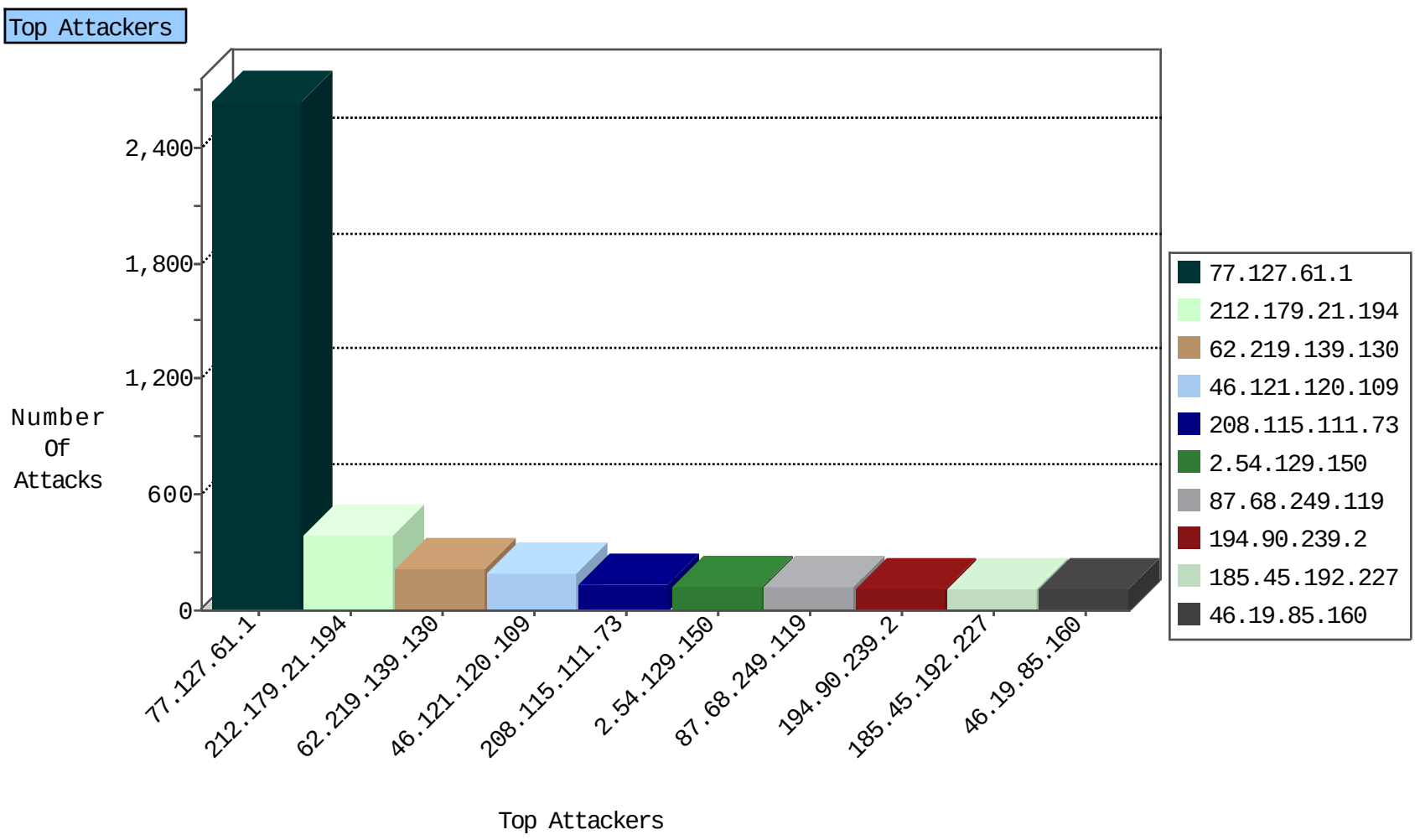
10-29-2015-11:04:08 to 10-29-2015-12:04:08

IDF Under Attack
Daily Report

Top Targets



Top Attackers



10-29-2015-11:04:08 to 10-29-2015-12:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.67.20	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	7628
66.249.67.34	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	6570
66.249.67.210	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	5947
66.249.67.194	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	3441
66.249.93.196	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1835
46.19.85.21	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1647
208.115.111.73	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1501
66.249.93.192	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1242
79.181.114.103	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	999
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	836
194.90.239.2	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	747
66.249.67.27	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	711
52.23.199.183	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	657
46.19.86.129	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	566
80.246.133.50	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	549
46.19.86.145	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	543
213.57.118.66	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	478
52.29.83.65	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	451
66.249.69.128	United States	147.237.77.234	halag.idf.il	TCP handshake violation, first packet not syn	drop	374
194.90.178.37	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	305
109.186.13.168	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	264
72.9.148.10	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	240
176.12.139.12	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	182
46.19.86.239	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	169
31.168.3.114	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	158
46.19.85.160	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	154
66.249.67.79	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	150
176.13.0.253	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	127
77.127.55.231	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	124
37.26.149.240	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	95
82.102.169.113	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	75
80.246.136.157	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	68
2.54.153.116	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	59
2.54.150.146	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	46
46.116.203.237	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	40
79.180.131.207	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	35
62.90.162.37	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	31
212.199.106.194	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	30
94.230.86.142	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	29
185.32.179.78	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	26
31.210.187.166	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	26
46.19.86.158	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	25
84.109.100.242	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	25
213.57.83.186	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	25
5.22.129.193	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	25
212.150.82.67	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	25
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	24
2.52.191.106	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	22
194.90.178.37	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	20
84.109.213.53	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	20

10-29-2015-11:04:08 to 10-29-2015-12:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.121.120.109	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
79.180.54.197	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
195.160.240.11	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1

10-29-2015-11:04:08 to 10-29-2015-12:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	1
2.54.164.108	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.66.18.56	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
85.64.191.13	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
81.218.116.129	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.162.116.98	147.237.77.170	Sweden	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.86.74	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
31.168.14.94	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
176.13.7.80	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
94.159.177.90	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.228.123.247	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
69.64.46.86	147.237.0.19	United States	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.86.169	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

10-29-2015-11:04:08 to 10-29-2015-12:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
77.127.61.1	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	699
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	360
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	133
2.54.129.150	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	123
194.90.239.2	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	103
84.109.100.242	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	76
46.19.86.230	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	73
109.64.17.212	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	66
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	60
37.26.146.198	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	58
176.228.198.126	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	57
61.16.189.178	India	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	56
220.238.32.14	Australia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	53
46.19.86.32	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	53
109.64.216.62	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
46.19.86.147	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	49
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	47
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	47
82.166.22.111	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	46
46.19.86.251	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
46.120.173.112	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
66.249.93.192	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
46.116.120.4	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
37.26.147.197	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
109.65.215.92	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
81.218.251.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
212.150.245.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
46.19.85.202	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
46.116.203.237	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
46.19.86.239	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
46.19.86.129	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
79.178.221.207	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	33
46.19.85.21	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
195.95.183.254	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
37.142.136.48	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	33
5.29.241.241	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
66.249.78.159	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
46.19.86.31	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
46.19.85.119	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
78.167.205.37	Turkey	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
2.54.150.146	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
64.233.172.171	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
192.115.67.2	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
65.49.14.164	Anonymous Proxy	147.237.72.166	aka.idf.il	drop		drop	26

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
77.127.61.1	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	1935
62.219.139.130	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	105
62.219.139.130	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php	Block	105
46.121.120.109	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	90
46.121.120.109	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 46.121.120.109	Block	75
87.68.249.119	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php	Block	60
185.45.192.227	Netherlands	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/__	Block	60
87.68.249.119	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	60
80.179.92.156	Israel	147.237.72.167	ishurim.aka.idf.i	Distributed PHP Attempt	Block	45
185.45.192.227	Netherlands	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/__	Block	45
2.52.36.142	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/	Block	30
62.219.161.81	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	30
46.120.18.45	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	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
46.120.18.45	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php	Block	30
85.250.106.172	Israel	147.237.72.167	ishurim.aka.idf.i	Distributed PHP Attempt	Block	30
79.181.205.239	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 79.181.205.239	Block	30
95.86.93.60	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 95.86.93.60	Block	30
79.181.205.239	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1403	Block	30
66.249.75.16	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/6/3176.pdf	Block	15
2.54.189.55	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	15
185.46.212.70	Switzerland	147.237.72.166	aka.idf.il	Unknown Parameter amp;utm_medium in www.aka.idf.il/main/home/default.aspx	None	15
95.86.93.60	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/&sa=u&ved=0cagqfjaaahukewicumv6sefiahwctxqkhcxgddi&usg=afqjcnhcvyyg7w1cq-yhd5_ammzoyodtwa	Block	15
66.249.64.137	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/5/71475.pdf	Block	15
84.111.114.52	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sacha	Block	15
46.121.120.109	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/sip_storage/files/8/	Block	15
46.19.85.206	Israel	147.237.76.42	refuah.idf.il	Distributed Malformed URL	Block	15
207.46.13.44	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/page.asp	Block	15
68.180.230.244	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	15
66.249.67.204	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/templates/getfile/getfile.aspx	Block	15
178.211.22.210	Russian Federation	147.237.77.216	dover.idf.il	Unknown HTTP Request Method COOK in URL www.idf.il/1527-en/dover.aspx	Block	15
79.183.97.55	Israel	147.237.72.167	ishurim.aka.idf.i	Distributed PHP Attempt	Block	15
66.249.75.120	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/4/2154.doc	Block	15
5.29.213.220	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar/faq.aspx	Block	15
188.165.15.162	France	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8956-he/refuah.aspx	Block	15
109.66.143.74	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	15
66.249.64.143	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	15
84.228.165.179	Israel	147.237.76.42	refuah.idf.il	PHP Attempt	Block	15
59.60.115.59	China	147.237.77.216	dover.idf.il	PHP Attempt	Block	15
46.19.85.206	Israel	147.237.76.42	refuah.idf.il	Distributed Unknown HTTP Request Method	Block	15
207.46.13.77	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/993/patzar.aspx	Block	15
66.249.69.8	Israel	147.237.76.147	chinuch.aka.idf.i	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	15
2.52.184.254	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	15
66.249.64.13	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	15
94.197.120.100	United Kingdom	147.237.72.156	aman.idf.il	Multiple Untraceable SSL Sessions from 94.197.120.100 (Open Mode)	None	15
192.115.67.2	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	15
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	15
37.26.146.153	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-he	Block	15
149.78.22.242	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	15
66.249.64.200	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	15