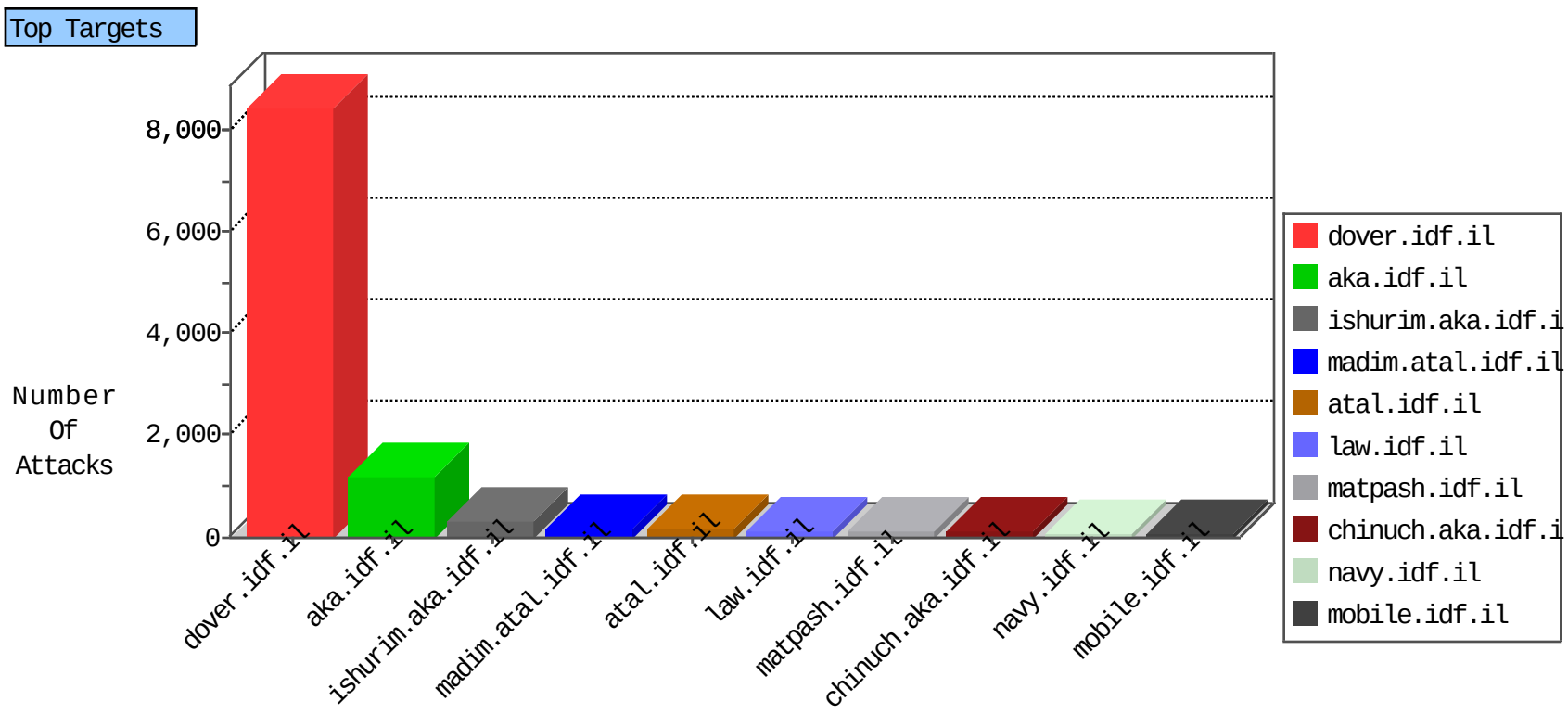
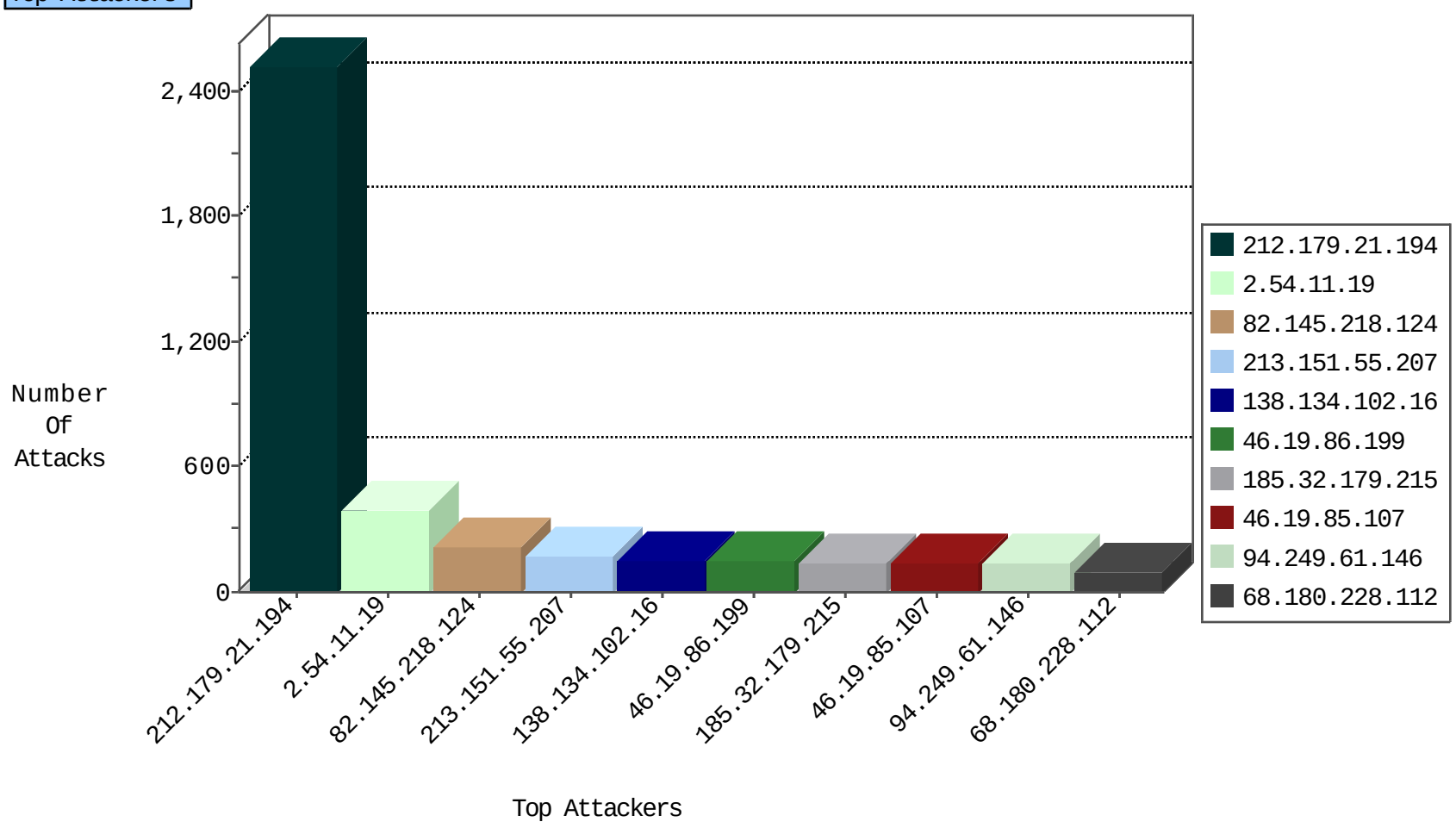
10-27-2015-12:04:09 to 10-27-2015-13:04:09

IDF Under Attack Daily Report

Top Targets



Top Attackers



10-27-2015-12:04:09 to 10-27-2015-13:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.179.21.194	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2987
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	290
185.32.179.215	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	193
217.41.11.42	United Kingdom	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	105
80.246.139.175	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	63
149.88.84.232	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	38
5.28.134.179	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	35
62.219.164.115	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	20
2.52.42.61	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	20
194.56.215.66	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	17
37.26.147.169	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	12
46.19.85.184	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	11
46.19.85.240	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
2.54.11.19	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	10
194.56.215.66	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
2.52.131.80	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	8
46.19.86.191	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
194.90.167.203	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
82.81.160.245	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
81.218.137.57	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
84.108.211.97	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
2.52.166.42	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	5
134.191.232.70	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
46.19.86.141	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
5.22.130.120	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
176.13.16.110	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
2.54.10.220	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
212.143.225.79	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
109.186.133.44	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
212.150.255.134	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
46.19.85.133	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
2.54.10.220	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
77.127.190.204	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
46.19.86.227	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
46.19.85.89	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
79.182.58.147	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
176.106.46.249	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
95.86.86.56	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
185.97.92.64		147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
80.246.137.38	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
87.68.57.17	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
82.81.7.95	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
192.115.200.9	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
176.12.141.248	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
91.231.193.150	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
46.19.85.56	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
134.191.232.70	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
31.154.3.222	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
199.203.172.65	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2

10-27-2015-12:04:09 to 10-27-2015-13:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.29.202.206	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	12
195.200.205.2	Israel	147.237.76.147	chinuch.aka.idf.il	C1000122: HTTP: Access to - .exe or .dll	Permit	3

10-27-2015-12:04:09 to 10-27-2015-13:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.200.205.2	147.237.76.147	Israel	chinuch.aka.idf.il	WEB-FRONTPAGE /_vti_bin/ access	2
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	2
31.168.21.81	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
176.13.13.7	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
94.230.80.180	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.80.196.44	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.178.13.212	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.185.244.204	147.237.77.216	Jordan	dover.idf.il	portscan: TCP Distributed Portscan	1
46.121.214.168	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.107	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.239.92.64	147.237.77.216	Iraq	dover.idf.il	portscan: TCP Distributed Portscan	1
109.65.1.109	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.166.224.133	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.180.230.51	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
66.102.8.173	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
46.151.52.8	147.237.77.170	Ukraine	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.85.239	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

10-27-2015-12:04:09 to 10-27-2015-13:04:09

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.il	drop	First packet isn't SYN	drop	2510
2.54.11.19	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	376
82.145.218.124	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	220
213.151.55.207	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	172
94.249.61.146	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	138
46.19.85.107	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	138
132.70.66.12	Israel	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	92
190.213.186.148	Trinidad and Tobago	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	89
46.19.86.113	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	86
91.231.193.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	75
138.134.102.16	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	71
46.19.86.248	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	69
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	66
176.106.46.249	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	61
37.26.149.170	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	57
37.140.188.78	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	55
93.34.184.143	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	54
2.54.10.220	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	53
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	52
185.32.179.215	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	51
212.179.64.162	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
212.150.145.153	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	50
46.19.86.104	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	50
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	49
195.160.240.11	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	46
46.210.212.129	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	45
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
149.88.234.25	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
46.19.85.21	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
100.100.24.53		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	40
213.57.83.22	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
62.0.112.189	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
62.168.89.182	Slovakia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
81.218.66.108	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
93.31.213.222	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
84.108.211.97	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
66.102.8.173	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
149.78.160.134	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
85.250.27.132	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
185.22.32.5	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
80.179.33.11	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
66.249.78.173	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
82.166.142.49	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
31.28.7.225	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
81.218.137.57	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
46.19.85.75	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.199	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.86.199	Block	140
195.200.205.2	Israel	147.237.76.147	chinuch.aka.idf.il	Multiple Unauthorized URL Access from 195.200.205.2	Block	84
138.134.102.16	Israel	147.237.77.233	atal.idf.il	Parameter Type Violation searchText in www.atal.idf.il/1620-he/atal.aspx	Block	80
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	56
2.52.164.84	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	42
46.117.171.165	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	42
46.117.171.165	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php	Block	42
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	42
37.239.92.64	Iraq	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/arr/	Block	28
192.117.12.65	Israel	147.237.77.233	atal.idf.il	Parameter Type Violation d in www.atal.idf.il/webresource.axd	Block	28
62.90.96.102	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/sip_storage/files/8/	Block	28
109.67.251.227	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php	Block	28
213.244.82.59	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Parameter Type Violation SearchText in www.cogat.idf.il/938-en/cogat.aspx	Block	28
212.199.57.198	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	28
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	28
37.238.21.220	Iraq	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	28
109.67.251.227	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	28
66.249.65.48	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/main/sachar/faq.aspx	Block	14
2.54.142.14	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
203.67.9.77	Taiwan	147.237.76.30	himush.idf.il	Multiple Untraceable SSL Sessions from 203.67.9.77 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	14
54.149.246.49	United States	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	14
84.109.242.66	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/1355-he=miluim/	Block	14
5.175.25.171	Germany	147.237.72.166	aka.idf.il	Unknown Parameter amp;docId in www.aka.idf.il/giyus/forms/	None	14
212.150.174.180	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/sip_storage/files/6/size338x0/1686.jpg	Block	14
74.52.129.242	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
2.52.140.224	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/www.navy.idf.il	Block	14
80.246.139.175	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	14
37.26.148.217	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	14
66.249.67.219	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 66.249.67.219	Block	14
2.54.164.240	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	14
203.67.9.77	Taiwan	147.237.76.42	refuah.idf.il	Multiple Untraceable SSL Sessions from 203.67.9.77 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	14
141.212.122.160	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/	Block	14
54.149.246.49	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/wp-login.php	Block	14
94.230.80.180	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-en/dover.aspx	Block	14
45.63.49.95		147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to 147.237.76.200/	Block	14
5.175.25.171	Germany	147.237.72.166	aka.idf.il	Unknown Parameter amp;moduletogoto in www.aka.idf.il/giyus/login/	None	14
79.181.178.162	Israel	147.237.72.167	ishurim.aka.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 79.181.178.162	Block	14
62.219.161.81	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	14
194.114.146.227	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/homas/site/	Block	14
113.99.255.215	China	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/miluim/about.aspx	Block	14
37.26.149.145	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	14
217.194.194.165	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	14
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-18481-he/dover	Block	14
2.54.188.74	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	14
203.67.9.77	Taiwan	147.237.76.200	eitan.aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	14
157.55.39.202	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
54.186.43.160	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	14
95.86.113.123	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	14
46.19.85.85	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	14
31.154.145.17	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14