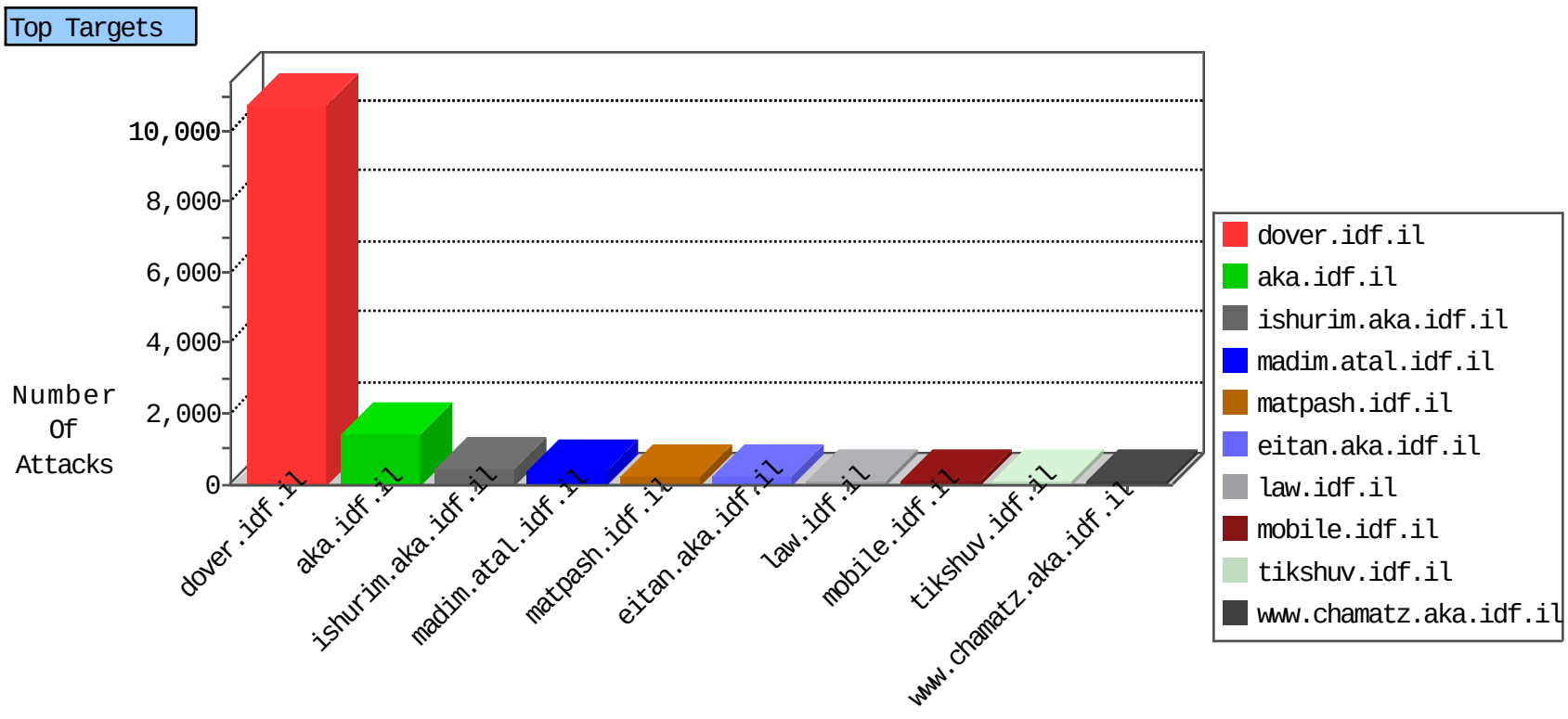
10-27-2015-11:04:04 to 10-27-2015-12:04:04

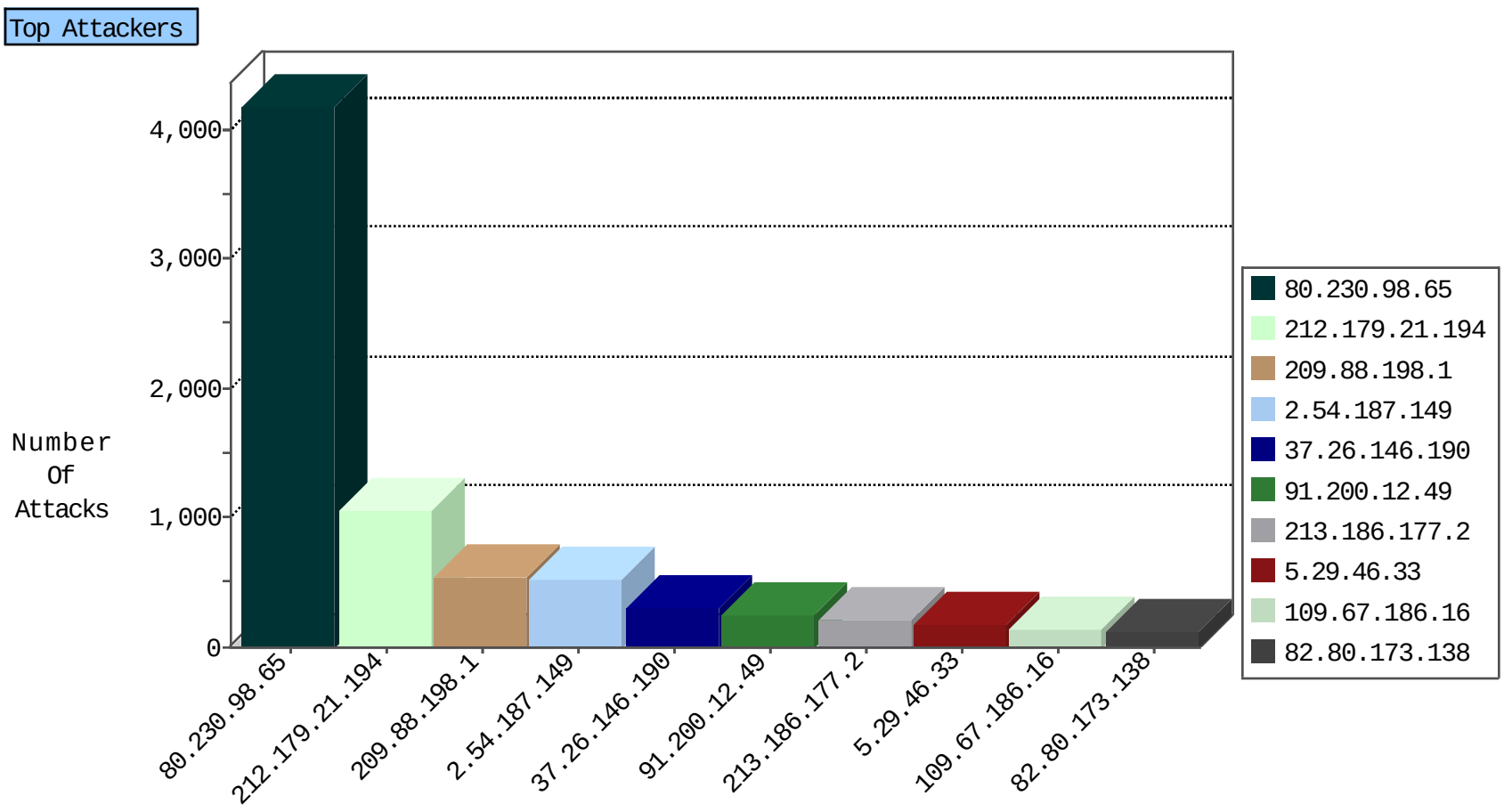
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

10-27-2015-11:04:04 to 10-27-2015-12:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
192.118.30.102	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	796
79.180.18.248	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	502
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	175
80.246.136.56	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	162
46.19.86.121	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	123
46.19.86.82	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	77
37.26.147.242	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	68
2.54.32.103	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	68
2.54.186.56	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	63
84.111.64.45	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	28
85.65.8.133	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	18
146.185.58.66	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	14
2.52.164.81	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	11
176.13.15.58	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	10
46.19.85.192	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
109.65.24.138	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
176.13.15.58	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
81.218.118.126	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
77.125.150.193	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	5
2.54.166.120	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
212.179.21.194	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
192.114.105.254	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
2.54.166.120	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
213.151.35.218	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
2.54.168.88	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
2.54.42.191	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
24.107.23.207	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
176.12.140.128	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
212.179.28.34	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
176.13.22.181	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
2.52.164.255	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
138.86.234.128	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
50.161.24.42	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
192.114.1.131	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
176.13.22.2	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
2.54.168.88	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
108.87.189.143	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
2.54.170.117	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
79.181.121.101	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
46.19.86.255	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
79.177.213.242	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
46.19.86.83	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
185.32.179.48	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
100.100.2.202		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
79.177.213.242	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
46.19.86.83	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
5.29.244.252	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
52.23.156.32	United States	147.237.72.166	aka.idf.il	SYN Flood unverified cookie	drop	1
212.179.28.34	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1

10-27-2015-11:04:04 to 10-27-2015-12:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
62.90.96.102	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
212.129.31.161	France	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1

10-27-2015-11:04:04 to 10-27-2015-12:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
176.12.136.15	147.237.76.42	Israel	refuah.idf.il	GPL SCAN myscan	2
176.12.136.15	147.237.76.42	Israel	refuah.idf.il	INDICATOR-SCAN myscan	2
82.81.15.115	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
5.29.91.3	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.54.137.197	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.199.182.150	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.143.125.195	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
149.88.185.178	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.192	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.187.149	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.35.21	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.179.21.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
151.11.201.3	147.237.72.167	Italy	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1

10-27-2015-11:04:04 to 10-27-2015-12:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
80.230.98.65	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4180
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1015
209.88.198.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	549
2.54.187.149	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	519
213.186.177.2	Jordan	147.237.76.200	eitan.aka.idf..	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	201
2.54.166.120	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	106
132.70.66.12	Israel	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	70
164.138.118.59	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	62
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	59
192.116.167.41	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	59
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	55
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	53
176.13.14.231	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	53
109.65.178.16	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	52
185.22.32.5	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	50
176.13.15.169	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
183.90.36.92	Singapore	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
31.168.246.85	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
37.142.190.2	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	47
198.103.104.11	Canada	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	47
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	45
100.100.23.58		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	44
31.168.19.211	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
80.178.249.73	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
109.65.24.138	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
46.19.86.222	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
173.84.92.52	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
206.213.43.100	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
2.54.154.224	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
37.140.188.78	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
81.218.251.252	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
110.92.98.1	Singapore	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
79.178.197.206	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
185.24.207.14	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
138.86.234.128	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
192.118.30.102	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
84.228.150.223	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
50.161.24.42	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
100.100.76.114		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	29
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
82.80.219.164	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
46.19.85.192	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
176.12.143.253	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
132.66.35.36	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
5.29.244.252	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
66.249.78.159	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
46.19.86.121	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22

10-27-2015-11:04:04 to 10-27-2015-12:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.146.190	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	308
91.200.12.49	Ukraine	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	126
91.200.12.49	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	126
5.29.46.33	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	84
37.8.53.255	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	84
5.29.46.33	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php	Block	84
109.67.186.16	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	84
192.115.177.203	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mivtza	Block	70
82.80.173.138	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	70
82.80.173.138	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/www.tikshuv.idf.il	Block	56
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
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	56
109.67.186.16	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/1/	Block	42
66.249.93.203	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	42
46.19.86.85	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	42
194.114.146.227	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/homas/site/	Block	42
2.52.63.177	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/www.tikshuv.idf.il	Block	37
176.13.18.47	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
82.166.77.241	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	28
85.64.244.51	Israel	147.237.0.19	madim.atal.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	28
46.19.85.125	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	28
79.178.209.239	Israel	147.237.0.34	tikshuv.idf.il	Distributed PHP Attempt	Block	28
66.249.93.207	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	28
79.178.209.239	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/ajax/updatestatus.php	Block	28
37.26.146.218	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	28
5.29.246.89	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php	Block	28
5.29.246.89	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	27
66.249.93.199	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
66.249.67.219	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/idkonim/pages/20032011yezu.aspx	Block	14
54.169.222.155	Singapore	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to 147.237.76.200/	Block	14
46.19.85.43	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	14
194.114.146.227	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/6/	Block	14
79.177.52.171	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/declarationofemployment.aspx	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
157.55.39.225	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/tizmoret/news/	None	14
54.215.187.95	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/wp-login.php	Block	14
95.35.174.241	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$passwordUpdate$txtPassword in www.aka.idf.il/main/giyus/faq.aspx	None	14
81.218.251.252	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc	Block	14
52.18.55.197	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/	Block	14
185.32.179.142	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	14
138.134.102.16	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/milnet	Block	14
66.249.67.227	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/idkonim/pages/081210tot.aspx	Block	14
54.186.43.160	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	14
195.250.33.251	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//resources/images/innerpage/goback.gif	Block	14
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
157.55.39.225	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in aka.idf.il/iturim/asp/displayonesoldier.asp	None	14
54.215.187.143	United States	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	14
95.211.174.70	Netherlands	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	Block	14
82.80.17.163	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	14
52.88.3.64	United States	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to 147.237.77.19/	Block	14

10-27-2015-11:04:04 to 10-27-2015-12:04:04