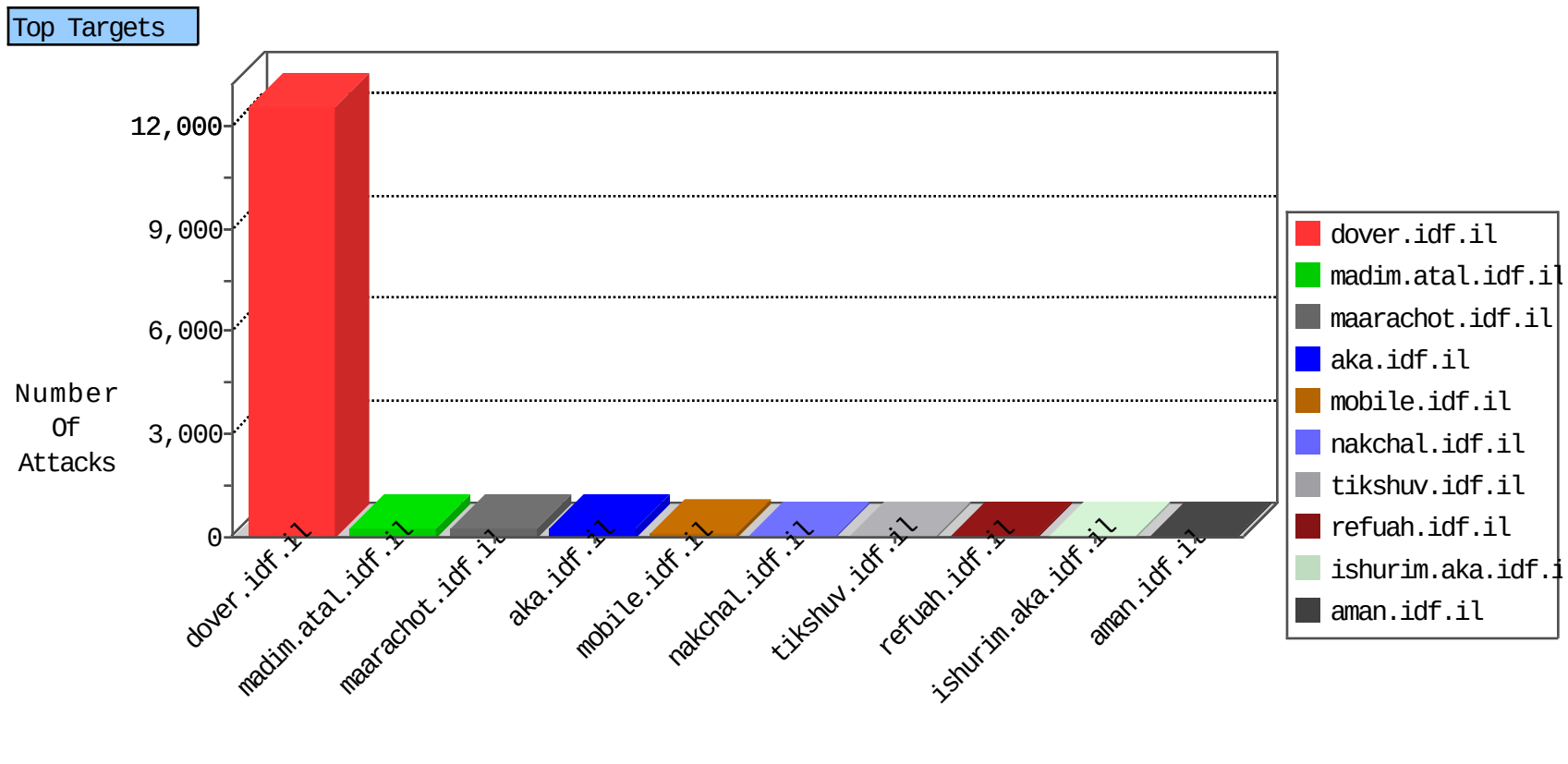
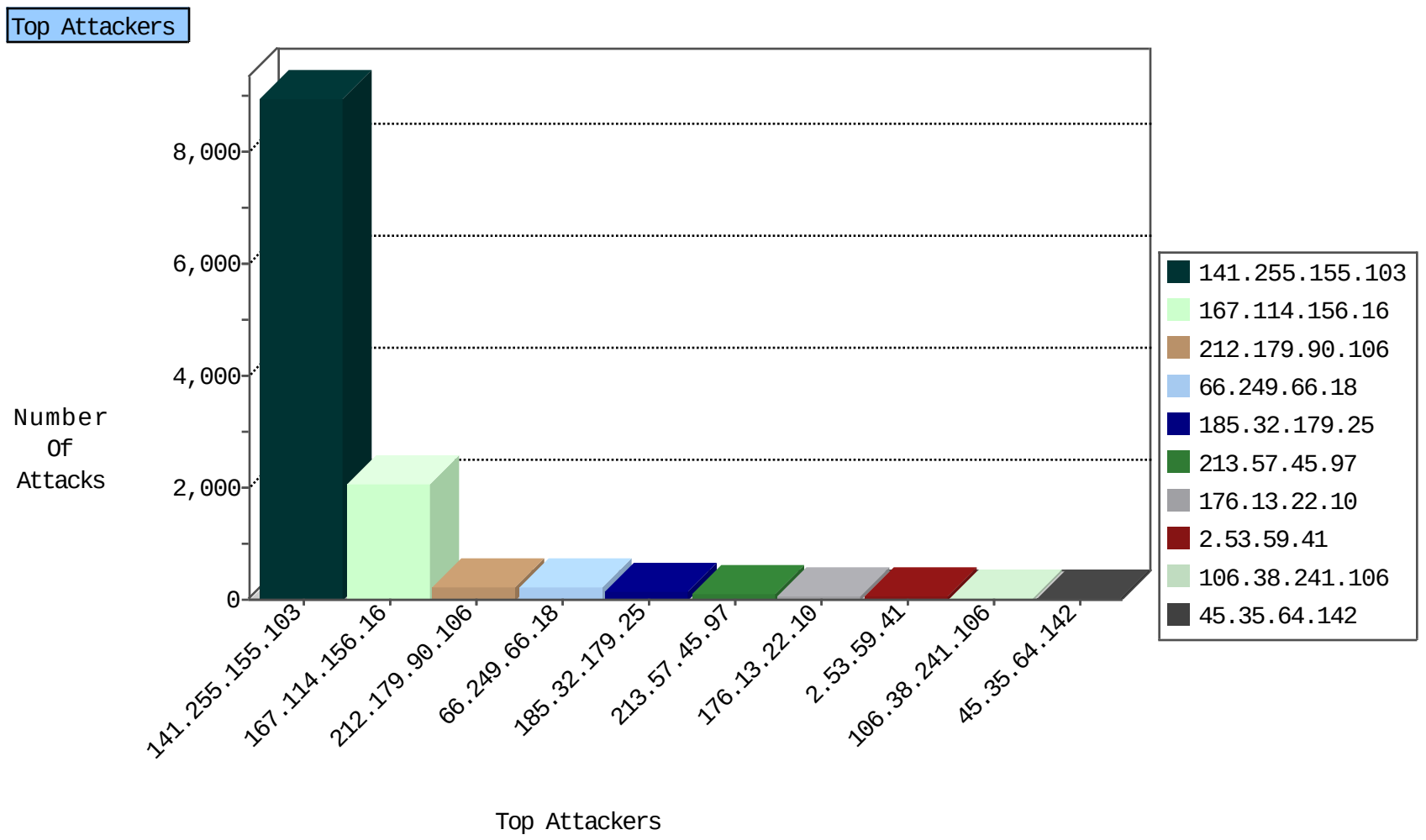
04-13-2016-16:04:08 to 04-13-2016-17:04:08

IDF Under Attack Daily Report

Top Targets



Top Attackers



04-13-2016-16:04:08 to 04-13-2016-17:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
141.255.155.103	Netherlands	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	191784
141.255.155.103	Netherlands	147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	13488
141.255.155.103	Netherlands	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6741
167.114.156.16	Canada	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	2053
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	1051
85.250.100.225	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	12
188.238.119.233	Finland	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	10
81.218.65.210	Israel	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	6
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
109.65.24.162	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2

04-13-2016-16:04:08 to 04-13-2016-17:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	5
109.64.247.68	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
62.219.160.95	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
31.168.180.232	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	3
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
166.62.85.222	United States	147.237.77.170	maarachot.idf.il	C1000016: HTTP: administrator in URI	Block	1

04-13-2016-16:04:08 to 04-13-2016-17:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.66.18	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	227
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	8
195.64.208.129	147.237.77.216	Russian Federation	dover.idf.il	portscan: TCP Distributed Portscan	1
109.67.54.4	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
85.65.155.208	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.178.154.32	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.82.78.38	147.237.0.200	Netherlands	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
213.151.32.163	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.53.59.41	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.143.219.222	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
163.172.140.23	147.237.8.28	United Kingdom	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
88.249.106.23	147.237.76.147	Turkey	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
80.178.157.101	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.82.78.38	147.237.77.227	Netherlands	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
75.127.167.98	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
58.218.205.69	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
2.55.50.15	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.179.229.187	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

04-13-2016-16:04:08 to 04-13-2016-17:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	230
213.57.45.97	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	84
2.53.59.41	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	61
171.159.64.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
125.215.235.181	Hong Kong	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
87.70.52.243	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
2.53.38.238	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
106.38.241.106	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
201.6.147.199	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
37.26.148.246	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
37.26.148.130	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
109.186.49.99	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
2.55.50.15	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
109.67.2.234	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
79.176.159.231	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	14
37.46.38.78	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
157.55.39.65	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
5.29.163.189	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
79.182.201.87	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
2.53.152.214	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
176.13.4.140	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.170	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
37.26.149.210	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.86.145	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.86.10	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
201.6.147.198	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
176.13.4.62	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
46.19.86.210	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
46.117.4.123	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
107.77.104.59	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
46.19.85.185	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
46.19.86.22	Israel	147.237.76.31	nakchal.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
184.153.75.12	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
79.180.172.46	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
216.143.42.57	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
2.53.1.120	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.53.178.172	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
157.55.39.54	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.209	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.59	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.173	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.32.179.25	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	139
176.13.22.10	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	78
109.253.218.81	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	27
87.71.46.74	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	5
87.71.46.74	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/sip_storage/files/2/	Block	4
77.125.85.5	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.179.9.7	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
201.6.147.198	Brazil	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
2.53.130.253	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.53.1.120	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
201.6.147.199	Brazil	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
2.53.133.11	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.183	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.246.137.227	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.53.38.238	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/authentication/index	Block	2
82.102.169.113	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
77.125.104.128	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
80.179.9.115	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
37.26.149.210	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
157.55.39.217	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
212.76.107.100	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
37.26.146.208	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
109.253.134.100	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
197.231.221.211	Liberia	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
62.0.100.86	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl47 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
2.53.129.115	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/960.css	Block	1
157.55.39.221	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
84.111.186.142	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
216.218.206.66	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
37.26.148.246	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
185.24.207.38	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/br><brothers/skira/default.asp	Block	1
166.62.85.222	United States	147.237.77.170	maarachot.idf.il	PHP Attempt	Block	1
87.71.46.74	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 87.71.46.74	Block	1
77.237.138.202	Czech Republic	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to /	Block	1
216.218.206.67	United States	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/	Block	1
157.55.39.30	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/forgotpassword.aspx	Block	1
80.179.115.198	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/payslips.aspx	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/smalim/showbig.aspx	Block	1
166.62.85.222	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/wp-login.php	Block	1
79.182.14.145	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	1
192.198.151.44	Europe	147.237.72.166	aka.idf.il	Unknown Parameter amp;t in www.aka.idf.il/main/rabanut/scriptresource.axd	None	1
157.55.39.65	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
2.53.38.238	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
201.6.147.202	Brazil	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
77.125.7.5	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
5.29.4.61	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
174.129.228.67	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
79.182.201.87	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
194.28.112.169	Netherlands	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1