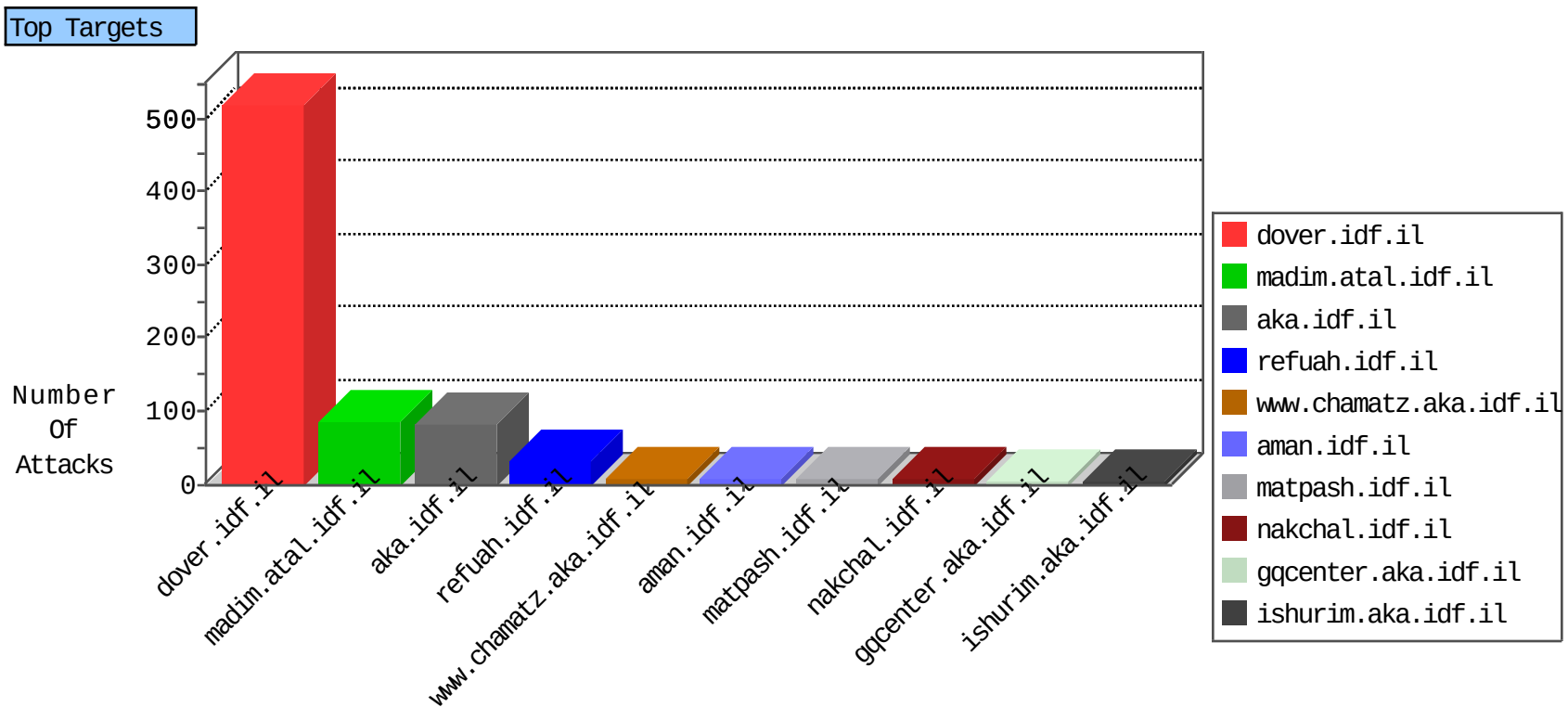
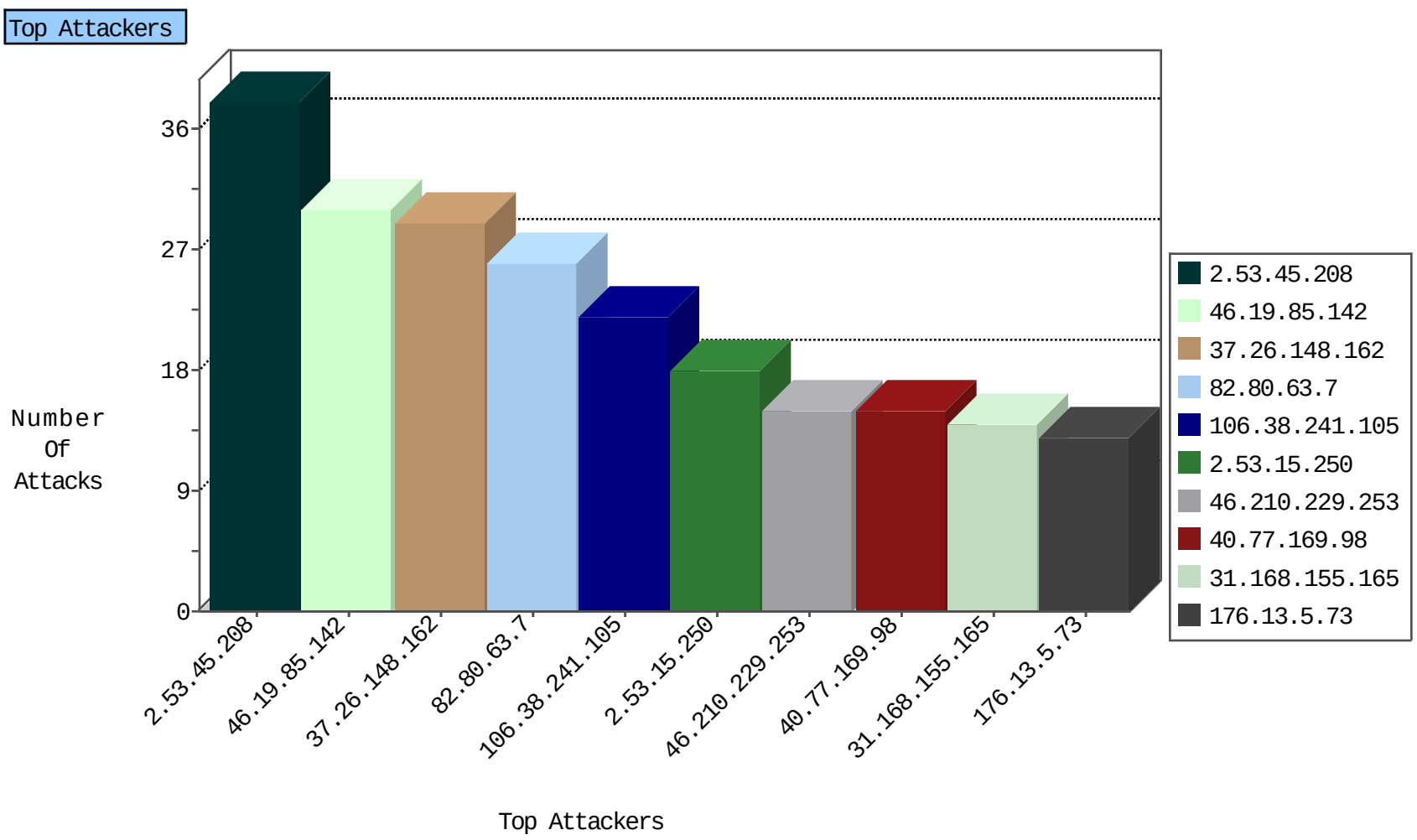
08-25-2016-11:04:05 to 08-25-2016-12:04:05

IDF Under Attack Daily Report





08-25-2016-11:04:05 to 08-25-2016-12:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.143.220	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	23
109.253.201.63	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	9
82.80.78.2	Israel	147.237.77.226	www.chamatz.aka.idf.il	Black List	drop	8
212.179.21.194	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6
45.35.64.142	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
168.235.196.169	United States	147.237.76.42	refuah.idf.il	JLM_Under_Attack_Con_Http	drop	1
185.128.40.162	Switzerland	147.237.76.44	e.refuah.idf.il	Black List	drop	1
2.53.165.229	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

08-25-2016-11:04:05 to 08-25-2016-12:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.105	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	18
5.9.63.149	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	3
5.9.63.149	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
106.38.241.105	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	2
163.172.211.135	United Kingdom	147.237.77.216	dover.idf.il	24910: HTTP: Python urllib User-Agent Header	Block	1
51.255.65.47	France	147.237.0.15	kosher-kravi.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
106.38.241.105	China	147.237.76.86	navy.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1

08-25-2016-11:04:05 to 08-25-2016-12:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
89.139.191.241	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.55.175.112	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.95.211.87	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
81.218.159.113	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
201.38.68.132	147.237.77.212	Brazil	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
79.177.252.19	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
188.0.236.165	147.237.72.156	Moldova, Republic of	aman.idf.il	ET SCAN Potential SSH Scan	1
62.0.6.226	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
133.242.4.52	147.237.76.30	Japan	himush.idf.il	ET SCAN NMAP -sS window 1024	1
46.172.71.251	147.237.8.24	Ukraine	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
123.206.85.139	147.237.72.166	China	aka.idf.il	ET SCAN NMAP -sS window 1024	1
45.55.8.238	147.237.77.19	United States	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
109.65.129.138	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.60.44.83	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
106.38.241.105	147.237.72.166	China	aka.idf.il	portscan: TCP Distributed Portscan	1
31.168.133.146	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.65.5.240	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.53.40.3	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
83.130.76.16	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
201.238.202.219	147.237.77.212	Chile	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
79.181.220.68	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
193.201.225.149	147.237.0.33	Ukraine	idf.il	ET SCAN NMAP -sS window 1024	1
62.90.163.180	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.13.16.251	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.227.67.172	147.237.72.167	Sweden	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
133.242.3.168	147.237.77.179	Japan	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.86.148	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.253.222.32	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.142.241.200	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.65.64.252	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.26.146.234	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

08-25-2016-11:04:05 to 08-25-2016-12:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
82.80.63.7	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
46.19.85.142	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	24
2.53.15.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
46.210.229.253	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	15
31.168.155.165	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
176.13.5.73	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
91.197.103.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.85.43	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.85.156	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
85.65.52.103	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
40.77.169.98	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	10
62.0.217.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
37.26.146.205	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
176.13.237.140	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
79.177.191.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
188.29.164.183	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
2.53.6.111	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
31.168.104.233	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
37.26.148.157	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
40.77.169.97	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	7
109.186.94.168	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
109.253.214.206	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
176.13.4.165	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
176.13.17.173	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
176.13.11.183	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
40.77.169.103	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	6
109.253.210.78	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.142	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
176.58.77.93	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
176.13.0.145	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
109.253.159.189	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
37.26.146.128	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.191	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.68	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.253	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
109.64.143.15	Israel	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	5
2.53.148.167	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
40.77.169.98	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
81.218.251.251	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
176.13.11.255	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
109.253.230.124	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
2.53.22.28	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
176.13.247.16	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.214	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.215	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
109.253.210.78	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	3
109.64.143.15	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
46.19.86.89	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3

08-25-2016-11:04:05 to 08-25-2016-12:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.45.208	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	36
37.26.148.162	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	29
2.55.149.37	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
209.88.198.1	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	4
2.55.145.159	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
209.88.198.1	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/sip_storage/files/4/	Block	3
46.19.86.51	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.86.249	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
82.166.158.215	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	2
212.179.159.253	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
94.69.106.17	Greece	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
77.139.192.18	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/giyus/forms/downloadform.asp	Block	2
2.53.185.201	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
185.32.179.187	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/rabanut/contactus.aspx	Block	2
89.139.222.254	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
5.102.195.81	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
77.139.179.249	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/miluim/templates/home.asp	Block	1
176.13.247.190	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.19.86.149	Israel	147.237.77.234	halag.idf.il	Illegal HTTP Version Safari/601.1	Block	1
37.26.148.239	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	1
2.53.45.208	Israel	147.237.0.19	madim.atal.idf.i	SSL Untraceable Connection - Open Mode	None	1
79.44.108.42	Italy	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl03$ct in www.aka.idf.il/main/giyus/talpiotquestionnaire.aspx	None	1
66.102.9.95	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
46.19.85.253	Israel	147.237.72.156	aman.idf.il	Multiple Untraceable SSL Sessions from 46.19.85.253 (Open Mode)	None	1
148.251.2.180	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1
84.95.208.20	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
10.100.35.59		147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/main/	Block	1
217.69.133.30	Russian Federation	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on list.ips.gov.il/robots.txt	Block	1
180.76.15.28	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	Block	1
46.19.86.149	Israel	147.237.77.234	halag.idf.il	Malformed URL mobile/13e238	Block	1
109.66.131.195	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
40.77.169.104	United States	147.237.77.216	dover.idf.il	Illegal Byte Code Character in URL /1361-10625-he/dover.aspx#011404	Block	1
79.176.140.200	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sahar	Block	1
66.249.64.134	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage/files/7/שקופית4	Block	1
209.88.198.1	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 209.88.198.1	Block	1
46.19.85.253	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
157.55.39.37	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_pictures.asp	Block	1
84.108.236.27	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
23.99.122.165	Hong Kong	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to 147.237.76.200/	Block	1
77.139.204.106	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/exampcert/	Block	1
46.19.86.149	Israel	147.237.77.234	halag.idf.il	Unknown HTTP Request Method .0 in URL mobile/13e238	Block	1
46.19.85.107	Israel	147.237.77.216	dover.idf.il	Illegal HTTP Version	Block	1
109.253.214.74	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	1
79.179.62.6	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/shurim	Block	1
66.249.69.224	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	1
169.229.3.91	United States	147.237.76.30	himush.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
85.65.146.78	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
37.26.147.129	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.139.248.120	France	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/0/112900.pdf	Block	1
207.46.13.166	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1

08-25-2016-11:04:05 to 08-25-2016-12:04:05