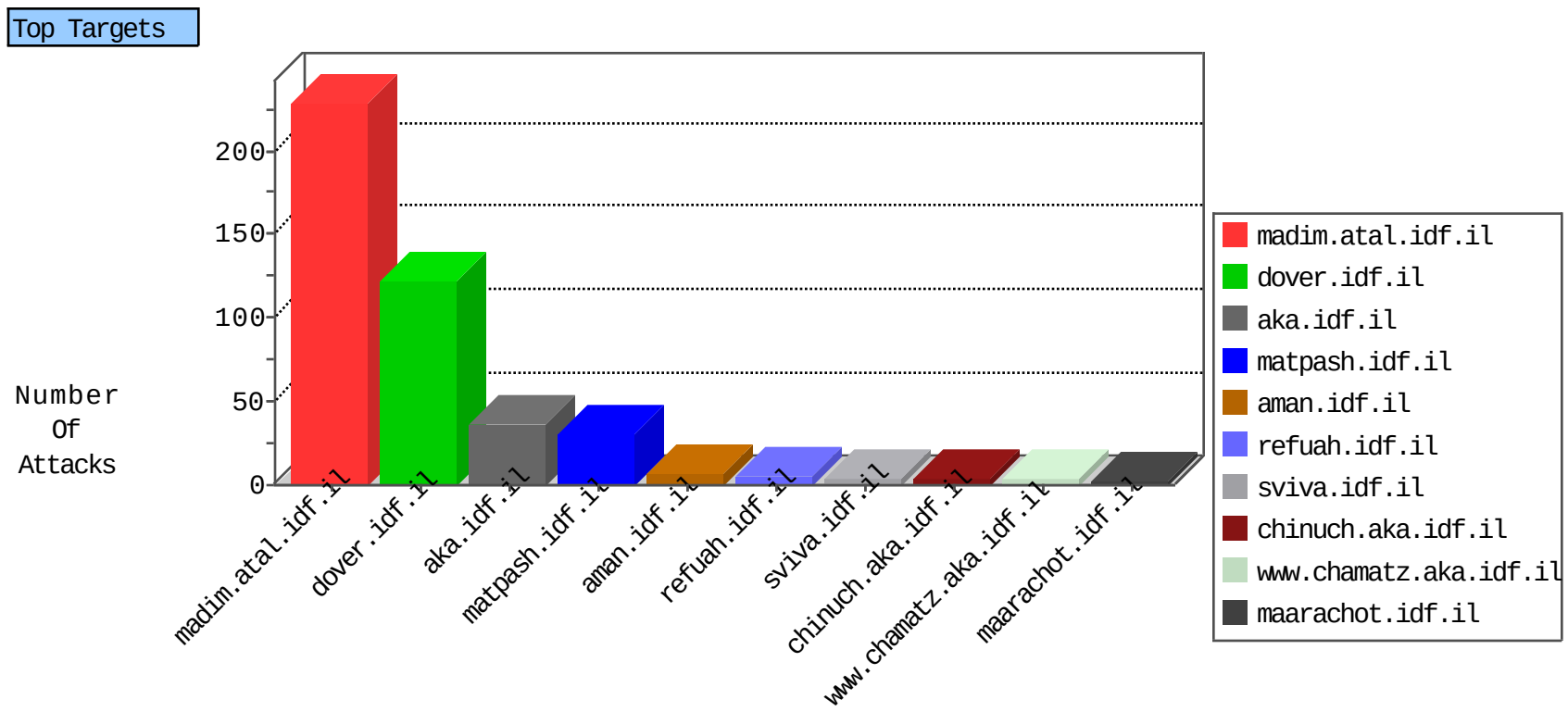
08-18-2016-13:04:08 to 08-18-2016-14:04:08

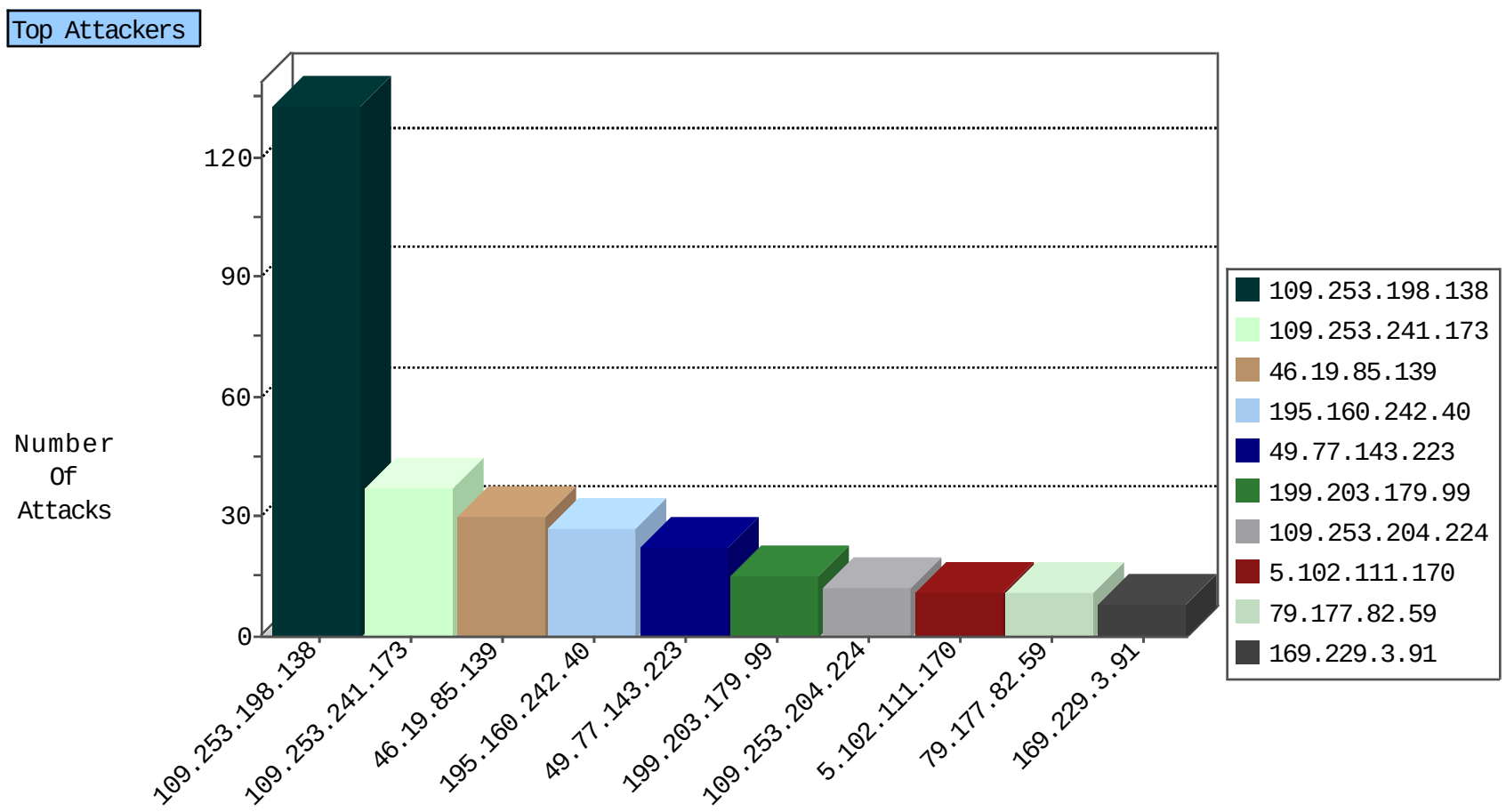
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

08-18-2016-13:04:08 to 08-18-2016-14:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.55.40.224	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7
62.219.229.77	Israel	147.237.72.166	aka.idf.il	Black List	drop	2
183.61.146.10	China	147.237.76.30	himush.idf.il	JLM_Under_Attack_Con_Tcp	drop	1
185.115.41.129	Turkey	147.237.8.27	e.madim.atal.idf.il	L4 Source or Dest Port Zero	drop	1
66.249.76.51	Israel	147.237.72.166	aka.idf.il	HTTP-Misc-BadBlue-Dir-Trave-2	dest-reset	1
37.26.146.131	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid TCP Flags	drop	1
93.158.200.105	Netherlands	147.237.76.42	refuah.idf.il	Black List	drop	1
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

08-18-2016-13:04:08 to 08-18-2016-14:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
52.1.90.117	United States	147.237.77.216	dover.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
71.6.167.142	United States	147.237.76.196	e.sviva.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
151.80.31.183	France	147.237.72.156	aman.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1

08-18-2016-13:04:08 to 08-18-2016-14:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
79.180.118.107	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
185.118.65.230	147.237.8.50	Russian Federation	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	2
2.55.180.231	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
158.85.182.203	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
2.53.38.197	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.125.184.101	147.237.77.176	United Kingdom	matpash.idf.il	Tehila - Perl LWP with fake user agent	1
80.246.138.30	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.25.102.63	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.176.16.228	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
77.125.54.86	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
158.85.182.203	147.237.77.227	United States	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
64.42.248.50	147.237.8.28	Canada	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 3072	1
158.85.182.203	147.237.77.178	United States	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
46.19.86.66	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
158.85.182.203	147.237.72.166	United States	aka.idf.il	ET SCAN Potential SSH Scan	1
2.53.180.147	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
158.85.182.203	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
87.236.194.161	147.237.77.226	Czech Republic	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
80.178.136.74	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.8.204.6	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.178.62.93	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
188.120.148.37	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
77.126.73.112	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.23.175.13	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
64.42.248.50	147.237.8.28	Canada	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 4096	1
158.85.182.203	147.237.77.212	United States	e.dover.idf.il	ET SCAN Potential SSH Scan	1
46.227.67.169	147.237.77.170	Sweden	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
158.85.182.203	147.237.77.170	United States	maarachot.idf.il	ET SCAN Potential SSH Scan	1

08-18-2016-13:04:08 to 08-18-2016-14:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
195.160.242.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
199.203.179.99	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
109.253.204.224	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
77.127.44.216	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
5.102.111.170	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
109.253.222.52	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
46.19.86.65	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
79.182.20.249	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
212.199.108.62	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
2.53.35.104	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
5.102.111.170	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	2
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
46.19.86.62	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	2
169.229.3.91	United States	147.237.0.33	idf.il	drop		drop	1
80.179.114.27	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
176.13.246.185	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
176.13.5.124	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
81.218.70.243	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
139.162.37.113	United States	147.237.0.200	m4u.idf.il	drop		drop	1
213.151.37.208	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
176.13.225.207	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
86.104.161.7	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.33	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
216.243.31.2	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
176.13.237.207	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.34	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
176.13.242.132	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	1
109.253.204.224	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.198.138	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	133
109.253.241.173	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	37
46.19.85.139	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	30
49.77.143.223	China	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 49.77.143.223	Block	15
79.177.82.59	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	11
109.253.217.116	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	7
49.77.143.223	China	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	6
17.78.148.64	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/haredim/general.aspx	Block	5
172.56.17.75	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	5
5.102.111.170	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/homepage/www.youtube.com/v/3g51ei5nuhg	Block	5
66.249.81.215	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
109.253.198.192	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
66.249.81.212	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
46.19.86.194	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.53.36.250	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
77.139.115.20	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/	Block	3
2.53.34.44	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.66.177	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.66.177	Block	2
157.55.39.131	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
185.110.110.37	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	1
68.180.228.185	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1589-en/dover.aspxthe	Block	1
49.77.143.223	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/index.asp	Block	1
169.229.3.91	United States	147.237.76.147	chinuch.aka.idf.il	Abnormally Long Request method	Block	1
80.246.138.30	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
213.151.35.218	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/klali.aspx	Block	1
169.229.3.91	United States	147.237.77.235	sviva.idf.il	Malformed URL ¯[ˬ¥p₪[[#18]]^·h•5¼¥»|˜uy[[#21]]´n[[*Ž′′#29‡]]¬gjdm r″sd–,ı½)	Block	1
66.249.76.58	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
139.162.13.205	Singapore	147.237.77.234	halag.idf.il	NULL Character in Method	Block	1
109.64.176.47	Israel	147.237.72.156	aman.idf.il	Multiple Untraceable SSL Sessions from 109.64.176.47 (Open Mode)	None	1
185.120.124.32	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
77.139.115.20	France	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012ources/images/innerpage/goback.gif	Block	1
66.249.64.181	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
169.229.3.91	United States	147.237.76.147	chinuch.aka.idf.il	Illegal Byte Code Character in Method â€²[[#1]][[#29]]•Mþ[[#1]]e[[#3]]Ä5(»ëI_$*š8Yåª[[#23]]B•‰é+kÖrsáÖÎ•€DkhAzùùa•U°†½¿O"Ù	Block	1
37.142.201.232	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
109.253.198.192	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	1
81.218.241.26	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 81.218.241.26	Block	1
169.229.3.91	United States	147.237.77.235	sviva.idf.il	Unknown HTTP Request Method 4 in URL ¯[ˬ¥p₪[[#18]]^·h•5¼¥»|˜uy[[#21]]´n[[*Ž′′#29ı½)‡]],–gjdm r″sd¬	Block	1
147.236.232.252	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
109.64.176.47	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
194.90.186.34	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1133-he/atal.aspx	Block	1
169.229.3.91	United States	147.237.76.147	chinuch.aka.idf.il	Unknown HTTP Request Method â€²[[#1]][[#29]]•Mþ[[#1]]e[[#3]]Ä5(»ëI_$*š8Yåª[[#23]]B•‰é+kÖrsáÖÎ•€DkhAzùùa•U°†½¿O"Ù in URL	Block	1
37.142.201.232	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
82.102.169.113	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
2.53.155.127	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc	Block	1
109.253.156.144	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
204.79.180.93	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/default.aspx	Block	1
66.249.69.8	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to atal.idf.il/templates/shared/usercontrols/navmenu/	Block	1
169.229.3.91	United States	147.237.77.235	sviva.idf.il	Abnormally Long Request request version	Block	1
40.77.167.37	United States	147.237.77.216	dover.idf.il	Distributed Abnormally Long Request	Block	1
87.70.247.126	Israel	147.237.77.226	www.chamatz.aka.idf.il	PHP Attempt	Block	1