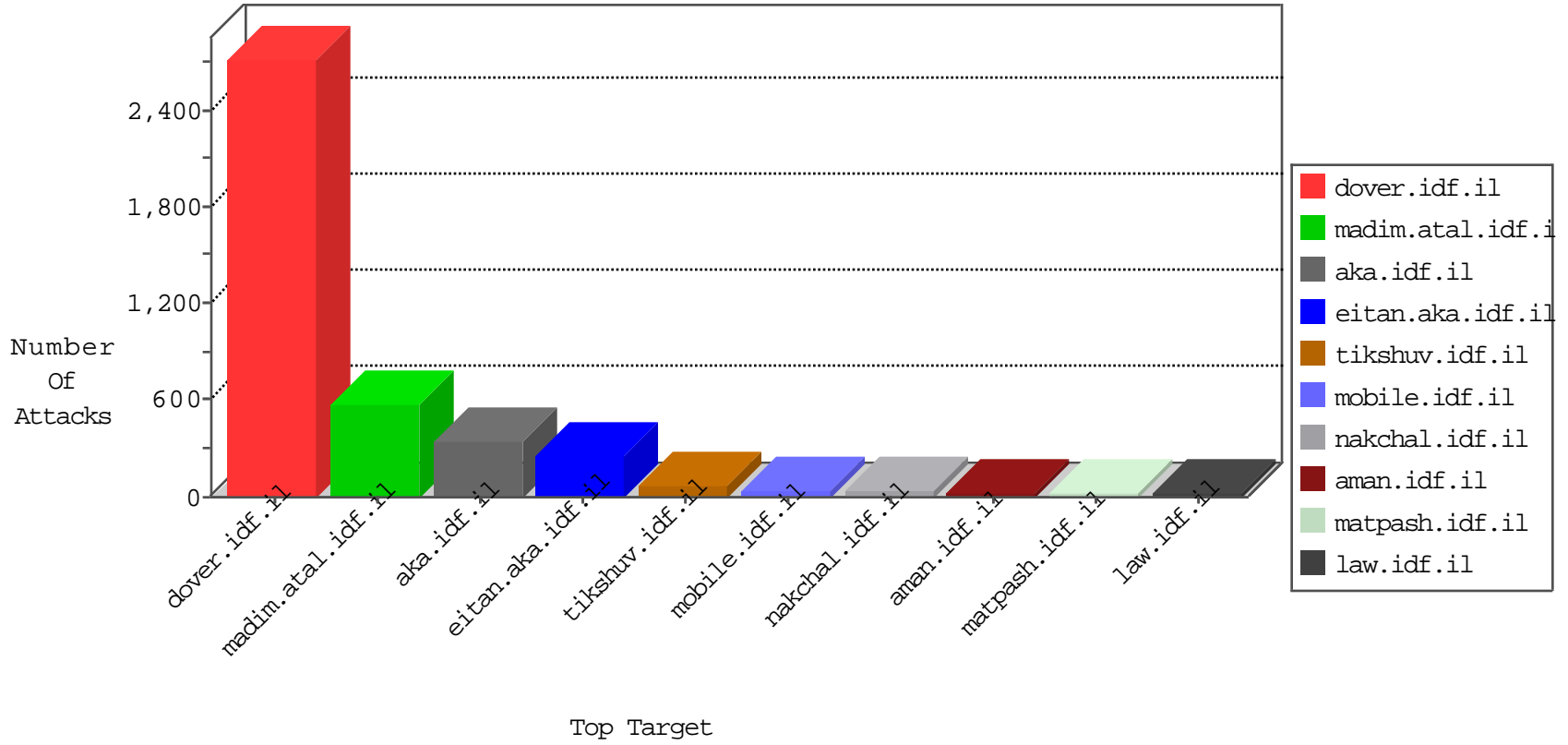


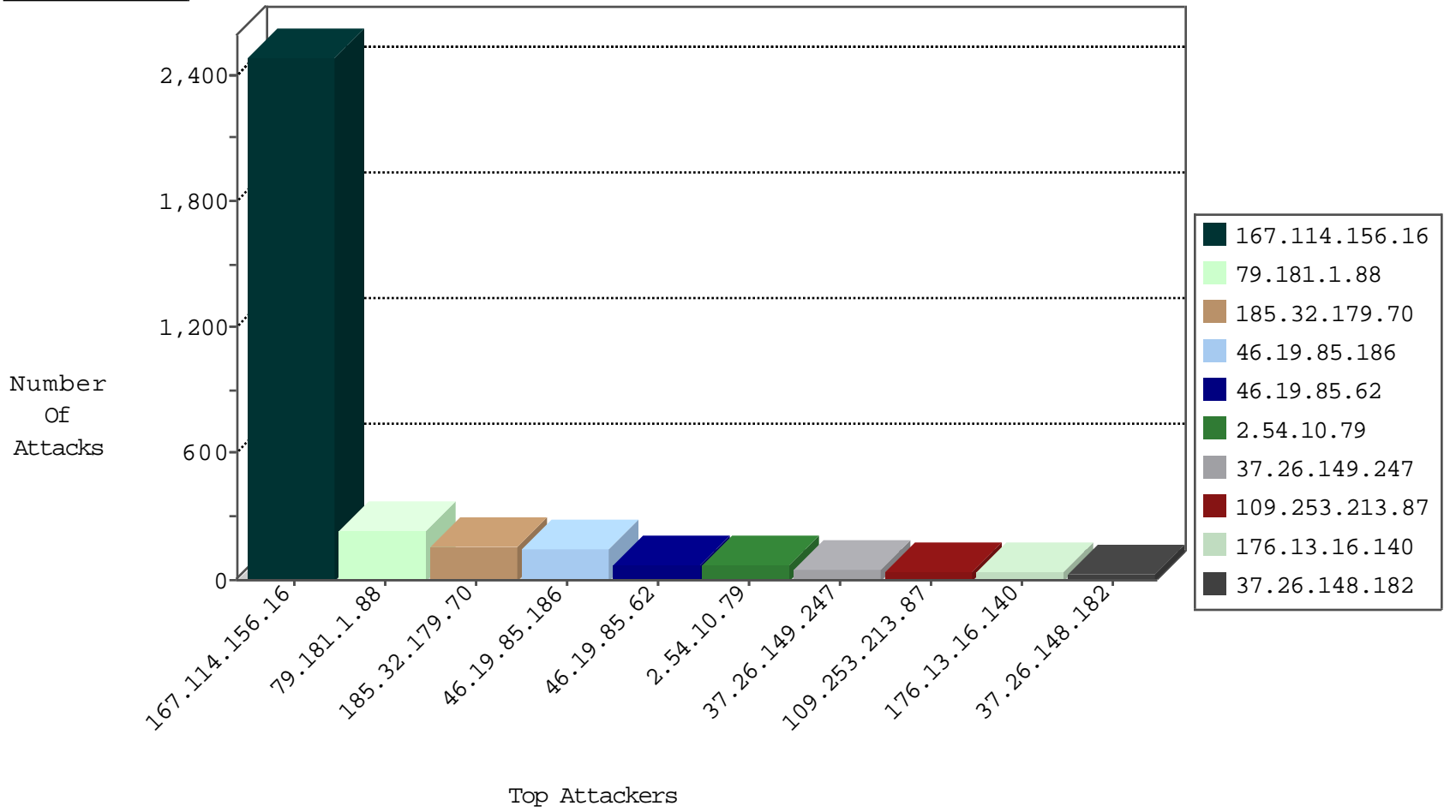
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3544
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	87
109.67.49.85	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
81.218.65.210	Israel	147.237.0.34	tikshuv.idf.il	Block_Udp_All_Nets	drop	3
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
83.130.108.116	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
80.246.133.106	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
2.54.38.103	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
85.130.207.167	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
89.138.83.19	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
162.219.4.147	United States	147.237.0.34	tikshuv.idf.il	C1000016: HTTP: administrator in URI	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

## Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
162.219.4.147	147.237.0.34	United States	tikshuv.idf.il	SERVER-WEBAPP admin.php access	1
149.50.84.56	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1
84.108.132.104	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.211	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.163.188	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	1
149.88.34.86	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
93.172.129.100	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.81.9.247	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
5.29.69.224	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.8.41.250	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
192.117.8.10	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.181.1.88	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	222
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	28
79.182.128.139	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
176.13.16.140	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
37.26.148.182	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
79.181.226.241	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
109.253.150.94	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
138.134.192.10	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	13
176.13.18.39	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
176.13.5.90	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
84.95.59.160	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	11
2.52.131.73	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
46.19.85.29	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
176.13.16.140	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
2.52.60.54	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
85.130.252.37	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
85.130.252.37	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
80.179.23.147	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.183.220.212	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.147.186	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.46.39.74	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
31.154.251.229	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.66	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
157.55.39.57	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
83.130.108.116	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.132	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.85.42	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.64.57.96	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
194.31.58.8	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.102.195.248	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.66	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
157.55.39.117	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.66	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
81.218.241.25	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
80.246.139.157	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	5
46.19.85.230	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.160	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
185.32.179.70	Israel	147.237.0.19	madim.atal.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.66	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
80.246.139.157	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
151.19.174.173	Italy	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
80.246.139.157	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
2.54.2.220	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
80.246.139.157	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.230	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
2.52.60.54	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
2.52.60.54	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
176.13.16.140	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
185.32.179.70	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.186	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	149
185.32.179.70	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	149
46.19.85.62	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	70
2.54.10.79	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	67
37.26.149.247	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	48
109.253.213.87	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	43
2.54.178.252	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
131.253.25.209	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	6
176.13.20.58	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
46.121.195.127	Israel	147.237.0.34	tikshuv.idf.il	Automated Vulnerability Scanning VI	Block	5
82.81.20.146	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	5
41.130.160.162	Egypt	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	4
41.130.160.162	Egypt	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	4
197.38.175.202	Egypt	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakchal.idf.il/xmlrpc.php	Block	3
195.227.81.66	Germany	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/templates/templatecontrols/generic/	Block	3
176.13.10.119	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.19.5	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
197.38.175.202	Egypt	147.237.76.31	nakchal.idf.il	Distributed PHP Attempt	Block	3
149.3.5.240	Georgia	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	2
162.219.4.147	United States	147.237.0.34	tikshuv.idf.il	Distributed PHP Attempt	Block	2
176.13.5.244	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
207.46.13.105	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
217.132.126.156	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
84.108.88.60	Israel	147.237.76.147	chinuch.aka.idf.il	PHP Attempt	Block	1
31.154.19.5	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 31.154.19.5	Block	1
66.249.69.48	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-14137-he/dover.aspx	Block	1
176.13.20.143	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Header Name ~[[#28]]ñuÖíY>RÙ[[#22]]Ë•v@è[[#2]]S[nÂÚê[[#28]]/[[[#27]]]jIÆ[šã-[[#2]]<X601&1[[#5]]	Block	1
37.26.146.175	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
207.46.13.160	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/templates/templatecontrols/generic/	Block	1
94.230.95.82	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/xmlrpc.php	Block	1
80.178.157.42	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/templatecontrols/generic/	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
157.55.39.66	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/163	Block	1
84.108.88.60	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/xmlrpc.php	Block	1
37.8.121.187	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
197.38.175.202	Egypt	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
176.13.20.143	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Header Value	Block	1
68.180.228.167	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1927-he/cogat.aspx	Block	1
162.219.4.147	United States	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 162.219.4.147	Block	1
62.210.252.207	France	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to 147.237.77.19/	Block	1
37.26.148.213	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
212.199.154.194	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 212.199.154.194	Block	1
109.253.150.94	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
196.221.144.203	Egypt	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
66.249.64.234	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
157.55.39.193	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/main.asp	Block	1
91.231.193.150	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;t in www.aka.idf.il/main/sachar/scriptresource.axd	None	1
37.26.146.136	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
197.38.175.202	Egypt	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	1
176.13.20.143	Israel	147.237.72.166	aka.idf.il	Malformed HTTP Header Line 6	Block	1