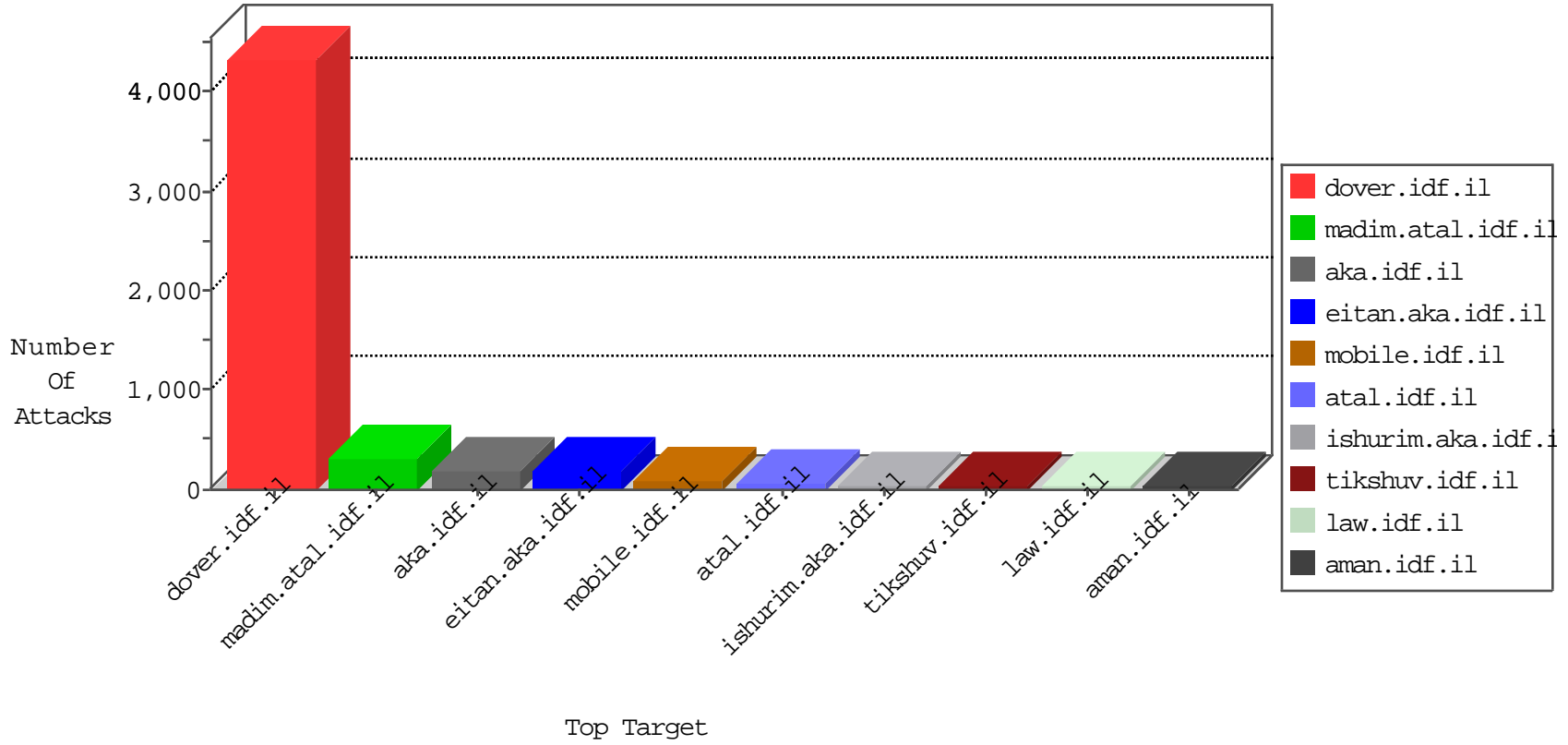


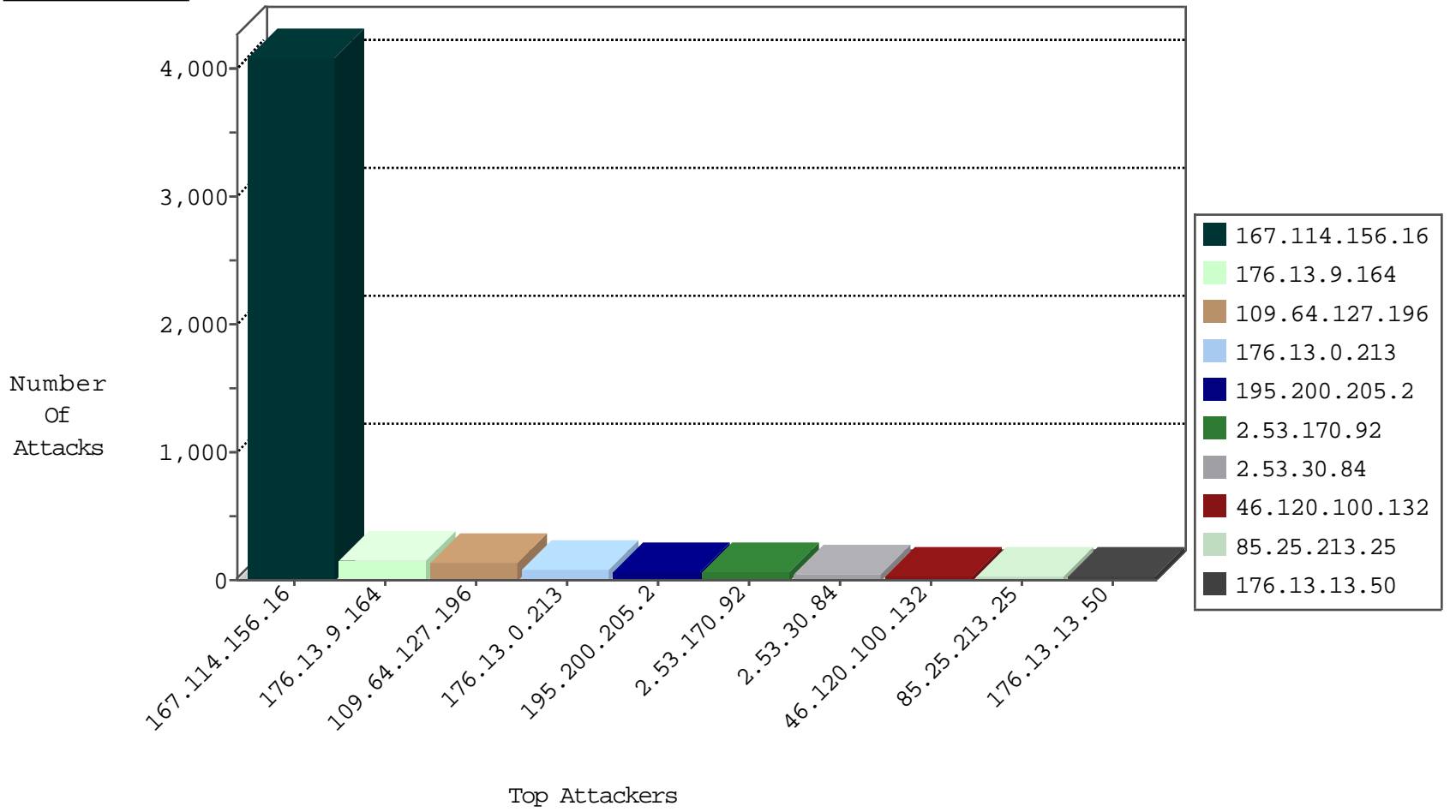
# IDF Under Attack Daily Report



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	Block_Ip_Web_In	drop	4096
79.177.128.141	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
74.91.23.108	United States	147.237.72.167	ishurim.aka.idf.il	block-sp-trafl	forward	2
107.150.46.34	United States	147.237.77.226	www.chamatz.aka.idf.il	block-sp-trafl	forward	2
69.30.202.227	United States	147.237.76.147	chinuch.aka.idf.il	block-sp-trafl	forward	2
173.208.197.252	United States	147.237.76.86	navy.idf.il	block-sp-trafl	forward	2
69.197.185.18	United States	147.237.77.216	dover.idf.il	block-sp-trafl	forward	2
89.46.102.242	Romania	147.237.77.212	e.dover.idf.il	Block_Udp_All_Nets	drop	1
159.122.220.135	United States	147.237.72.167	ishurim.aka.idf.il	Block_Ntp_All_Net	drop	1
114.33.223.210	Taiwan	147.237.77.233	atal.idf.il	Block_Udp_All_Nets	drop	1
82.145.222.69	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	1
159.122.220.135	United States	147.237.0.19	madim.atal.idf.il	Block_Ntp_All_Net	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
------------------	------------------	----------------	------	-----------	---------------	-------

## Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
209.173.241.141	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	4
209.173.241.141	147.237.77.74	United States	law.idf.il	ET WEB_SERVER Possible SQL Injection (varchar)	3
209.173.241.141	147.237.77.74	United States	law.idf.il	ET WEB_SERVER Possible SQL Injection Attempt SELECT FROM	3
209.173.241.141	147.237.77.74	United States	law.idf.il	ET WEB_SERVER Possible MySQL SQLi Attempt Information Schema Access	3
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
185.3.147.219	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
106.38.241.106	147.237.72.166	China	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
81.218.201.187	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.187	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
194.90.153.133	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.186.128.132	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
87.68.9.255	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
67.194.229.137	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
109.64.127.196	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	141
2.53.30.84	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
195.200.205.2	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	31
195.200.205.2	Israel	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	28
176.13.13.50	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
66.249.66.61	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
87.70.44.178	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
46.19.85.96	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
93.89.19.29	Turkey	147.237.0.34	tikshuv.idf.il	SQL Injection	SQL injection detected in URL: 'varchar'	monitor	12
80.178.204.97	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
24.114.223.254	Canada	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
87.71.130.197	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	12
85.25.213.25	Germany	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
46.120.100.132	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	9
2.53.176.144	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.120.100.132	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
194.90.153.133	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
185.18.206.194	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
85.25.213.25	Germany	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
85.130.248.28	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
85.130.248.28	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.178.27.249	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
188.120.148.142	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
195.62.160.60	Italy	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.117.223.237	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
79.179.112.153	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
213.57.88.66	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.45	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.117.62.14	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
66.102.9.60	United States	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	5
46.117.62.14	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
85.25.213.25	Germany	147.237.72.156	aman.idf.il	SYN Attack		reject	5
46.19.85.26	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
85.25.213.25	Germany	147.237.76.147	chinuch.aka.idf.il	SYN Attack		reject	5
46.19.85.45	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
2.53.181.120	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	4
177.185.192.77	Brazil	147.237.77.74	law.idf.il	SQL Injection	SQL injection detected in URL: 'varchar'	monitor	4
46.120.100.132	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
195.200.205.2	Israel	147.237.77.234	halag.idf.il	drop	First packet isn't SYN	drop	4
2.53.181.120	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
177.185.194.47	Brazil	147.237.77.216	dover.idf.il	SQL Injection	SQL injection detected in URL: 'varchar'	monitor	4
209.173.241.141	United States	147.237.77.74	law.idf.il	SQL Injection	SQL injection detected in URL: 'varchar'	monitor	4
46.120.100.132	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
213.8.145.99	Israel	147.237.72.166	aka.idf.il	SQL Injection	SQL injection detected in URL: 'varchar'	monitor	4
46.19.85.45	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
195.200.205.2	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
2.53.181.120	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
85.250.99.122	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.9.164	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	152
176.13.0.213	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	75
2.53.170.92	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	61
46.19.86.206	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	20
209.173.241.141	United States	147.237.77.74	law.idf.il	Parameter Type Violation InfoCenterItem in www.mag.idf.il/templates/getfile/getfile.aspx	Block	4
177.185.192.77	Brazil	147.237.77.74	law.idf.il	Parameter Type Violation pos in www.law.idf.il/164-4030-he/patzar.aspx	Block	4
93.89.19.29	Turkey	147.237.0.34	tikshuv.idf.il	Distributed Parameter Type Violation on www.tikshuv.idf.il/modules/forums/forum.aspx parameter FolderId	Block	4
177.185.194.47	Brazil	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1129-he/dover.aspx	Block	4
93.89.19.29	Turkey	147.237.0.34	tikshuv.idf.il	Distributed Parameter Type Violation on www.tikshuv.idf.il/modules/forums/forum.aspx parameter ForumId	Block	4
93.89.19.29	Turkey	147.237.0.34	tikshuv.idf.il	Distributed Parameter Type Violation on www.tikshuv.idf.il/modules/forums/forum.aspx parameter lang	Block	4
192.193.216.148	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
46.19.86.152	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.53.171.74	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
80.246.130.66	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
212.179.180.30	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/sip_storage/files/6/size338x0/1796.jpg	Block	2
87.71.136.171	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https://www.aman.idf.il/	Block	1
69.197.185.18	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.ps780.com/	Block	1
208.115.113.82	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/main/giyus/general.aspx	Block	1
66.249.66.121	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/9/size100x0/3249.jpg	Block	1
95.143.222.14	Russian Federation	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/changelog.txt	Block	1
213.151.35.213	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 213.151.35.213	Block	1
83.244.48.23	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19396-he/idfgdover.aspx	Block	1
193.200.80.26	United Kingdom	147.237.77.74	law.idf.il	Parameter Type Violation pos in www.law.idf.il/164-3857-he/patzar.aspx	Block	1
66.102.9.101	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-en/www.idf.il/english	Block	1
109.203.221.121	Russian Federation	147.237.0.34	tikshuv.idf.il	Parameter Type Violation lang in www.tikshuv.idf.il/modules/forums/forum.aspx	Block	1
91.79.240.239	Russian Federation	147.237.0.34	tikshuv.idf.il	Parameter Type Violation catId in www.tikshuv.idf.il/site/general.aspx	Block	1
2.55.45.251	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
79.178.27.249	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	1
66.249.66.123	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/2/size100x0/2412.jpg	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
213.254.241.7	France	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
84.94.71.165	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/https://mobile.idf.il/	Block	1
66.249.78.102	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19683-he/idfgdover.aspx	Block	1
195.154.114.37	France	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/arr/	Block	1
66.249.66.61	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/mobile/main/smalim/showbig.aspx	Block	1
149.50.30.39	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/home/d	Block	1
37.26.146.148	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
212.150.174.180	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
66.249.66.125	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/2/size100x0/3382.jpg	Block	1
46.117.199.124	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/sachar/	Block	1
107.150.46.34	United States	147.237.77.226	www.chamatz.aka.idf.il	Distributed Unauthorized URL Access on www.ps780.com/	Block	1
2.53.134.117	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
220.167.100.13	China	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/manager/html	Block	1
85.65.36.133	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/templatecontrols/generic/	Block	1
195.200.205.2	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	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
66.249.66.99	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
38.111.147.84	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1