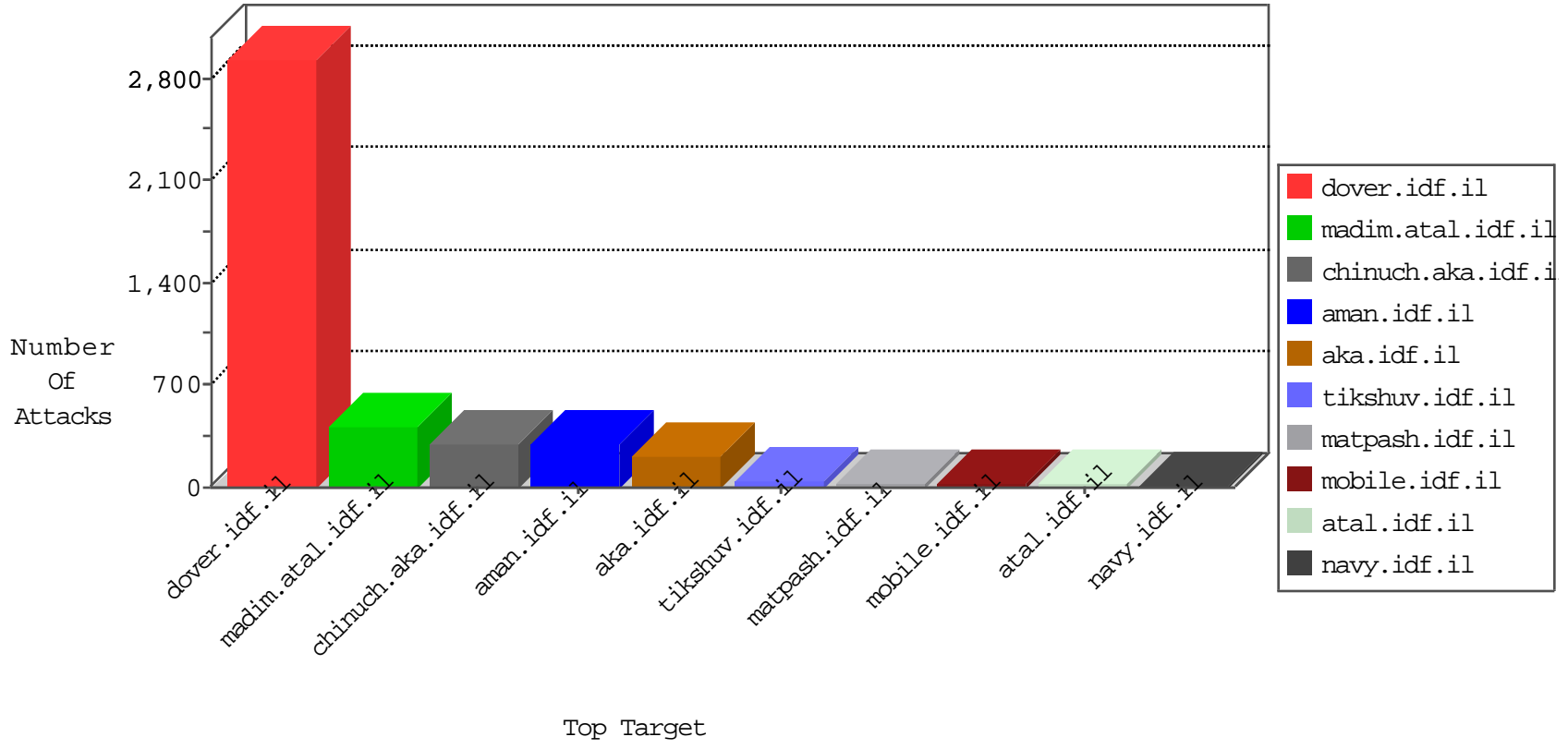


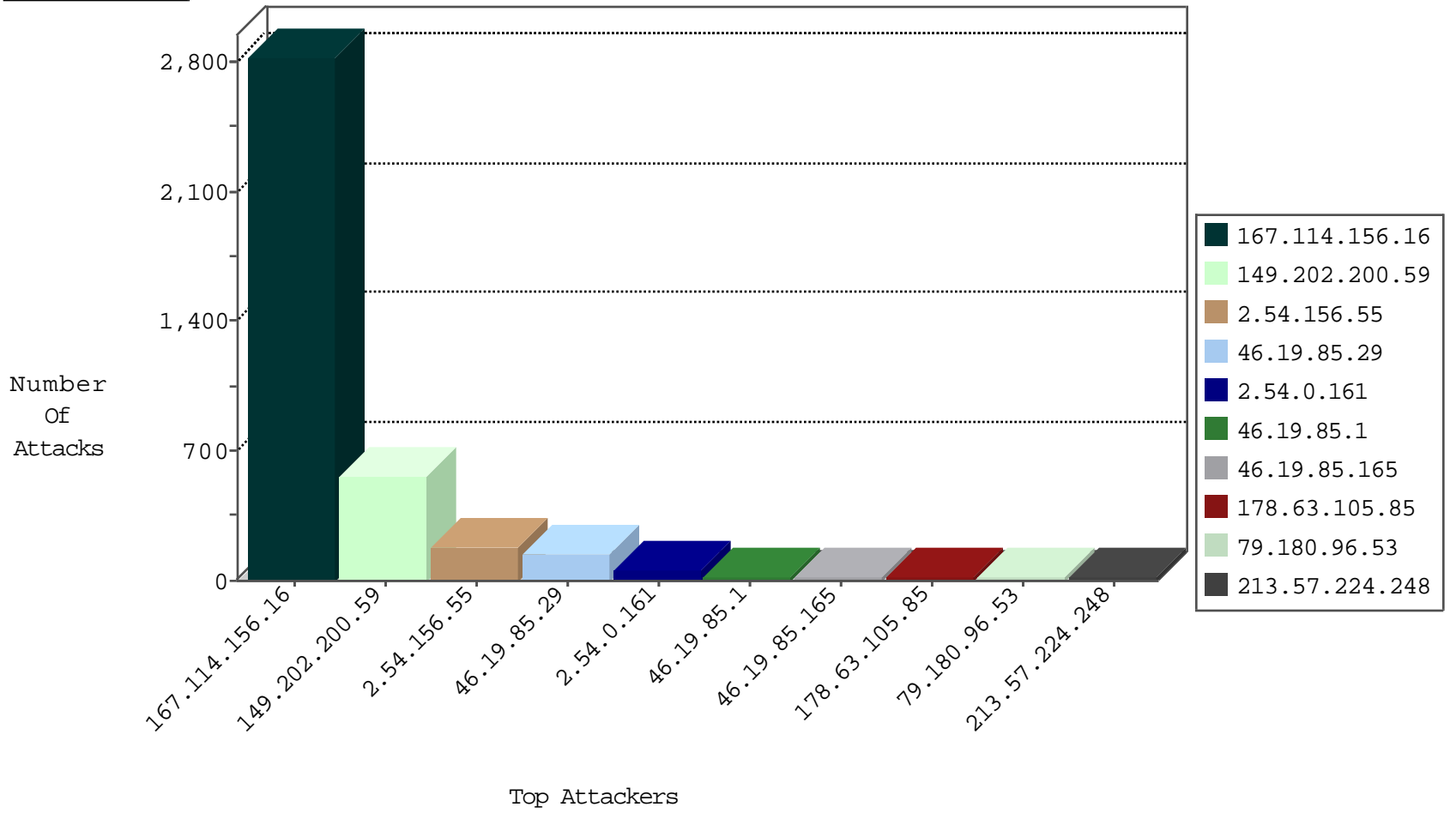
IDF Under Attack Daily Report



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	3836

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
213.57.224.248	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	18
217.132.114.35	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	12
46.117.230.191	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
79.178.169.225	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	5
106.38.241.149	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	4
87.70.74.164	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
174.34.135.242	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
46.116.11.31	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
151.80.31.135	Italy	147.237.77.226	www.chamatz.aka.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
80.246.130.252	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	4
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.240.213.93	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.77.19	China	law-forum.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.8.27	China	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
198.20.69.98	147.237.76.177	United States	ncore.idf.il	ET DROP Dshield Block Listed Source	1
193.105.134.220	147.237.77.121	Sweden	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
104.232.98.38	147.237.76.147		chinuch.aka.idf.il	ET SCAN NMAP -sS window 4096	1
66.240.213.93	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
66.240.213.93	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1
218.246.0.97	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
187.189.118.25	147.237.0.17	Mexico	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
149.202.200.59	Germany	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	178
149.202.200.59	Germany	147.237.76.147	chinuch.aka.idf.il	SYN Attack		reject	170
149.202.200.59	Germany	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	105
149.202.200.59	Germany	147.237.72.156	aman.idf.il	SYN Attack		reject	93
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	19
46.19.85.1	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
46.19.85.194	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
149.202.200.59	Germany	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
46.19.86.234	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
109.65.71.121	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.1	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.195	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.85.198	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
2.52.129.250	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
178.63.105.85	Germany	147.237.76.176	test.noore.idf.il	drop	SAM rule	drop	7
185.32.179.36	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.65.75.193	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.85.63	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
2.54.0.88	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.9.217	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.183.113.238	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
85.140.3.242	Russian Federation	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
185.32.179.214	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.180.96.53	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
79.180.96.53	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
149.202.200.59	Germany	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
37.142.64.80	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	5
79.179.205.96	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
178.63.105.85	Germany	147.237.8.45	e.eitan.idf.il	drop	SAM rule	drop	5
46.19.85.38	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.195	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
89.138.89.166	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
80.246.130.252	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
109.66.131.174	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
91.200.12.141	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
37.46.39.1	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
213.8.204.53	Israel	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
24.164.130.147	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.195	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.142.64.80	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
77.127.187.77	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.148.163	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.56.168	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
149.78.247.128	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.129.92	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.178.32.75	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.165	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.156.55	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	174
46.19.85.29	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	144
2.54.0.161	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	60
46.19.85.165	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	16
2.52.169.80	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
185.32.179.36	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.85.205	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
85.65.231.234	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
2.52.63.69	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/size220x0/sip_storage	Block	2
37.26.149.128	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
216.106.71.189	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
2.54.0.88	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
216.106.71.189	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	2
37.26.146.130	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
118.108.157.117	Japan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
84.111.165.15	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/giys	Block	1
66.249.78.247	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/list20050529.htm	Block	1
220.181.132.216	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/894-he/dover.aspx	Block	1
177.22.120.18	Brazil	147.237.72.166	aka.idf.il	Unknown Parameter amp;pagenum in www.aka.idf.il/iturim/asp/displayallsoldiers.asp	None	1
5.29.49.38	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/templatecontrols/generic/	Block	1
105.158.186.122	Morocco	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
77.75.79.11	Czech Republic	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/page/28/	Block	1
66.249.64.229	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1537-8810-he/atal.aspx	Block	1
197.250.195.243	Tanzania, United Republic of	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
37.26.148.189	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
141.212.122.145	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
2.54.5.206	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
68.180.230.189	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1781-he/dover.aspx	Block	1
179.55.68.192	Brazil	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.19.85.165	Israel	147.237.77.233	atal.idf.il	Parameter Type Violation search in atal.idf.il/1440-he/atal.aspx	Block	1
24.30.148.57	United States	147.237.77.74	law.idf.il	PHP Attempt	Block	1
109.65.23.129	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giys/authenticationsevice.aspx/getauthuser	Block	1
79.178.188.51	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman/	Block	1
199.30.16.167	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
149.88.71.234	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
86.133.52.182	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/2/4912.png	Block	1
2.54.38.234	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
69.121.153.40	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giys/authenticationsevice.aspx/getauthuser	Block	1
46.19.85.165	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
24.30.148.57	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	1
110.172.144.130	India	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-13490-en/dover.aspx'	Block	1
84.94.82.178	Israel	147.237.77.176	matpash.idf.il	Parameter Type Violation SearchText in www.cogat.idf.il/938-en/cogat.aspx	Block	1
66.249.78.236	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/6/size100x0/3426.jpg	Block	1
157.55.39.193	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
41.248.40.39	Morocco	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
87.70.86.88	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	1
71.166.87.2	United States	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
187.160.29.23	Mexico	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-9703-en/dover.aspx'	Block	1
31.13.112.121	Ireland	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1