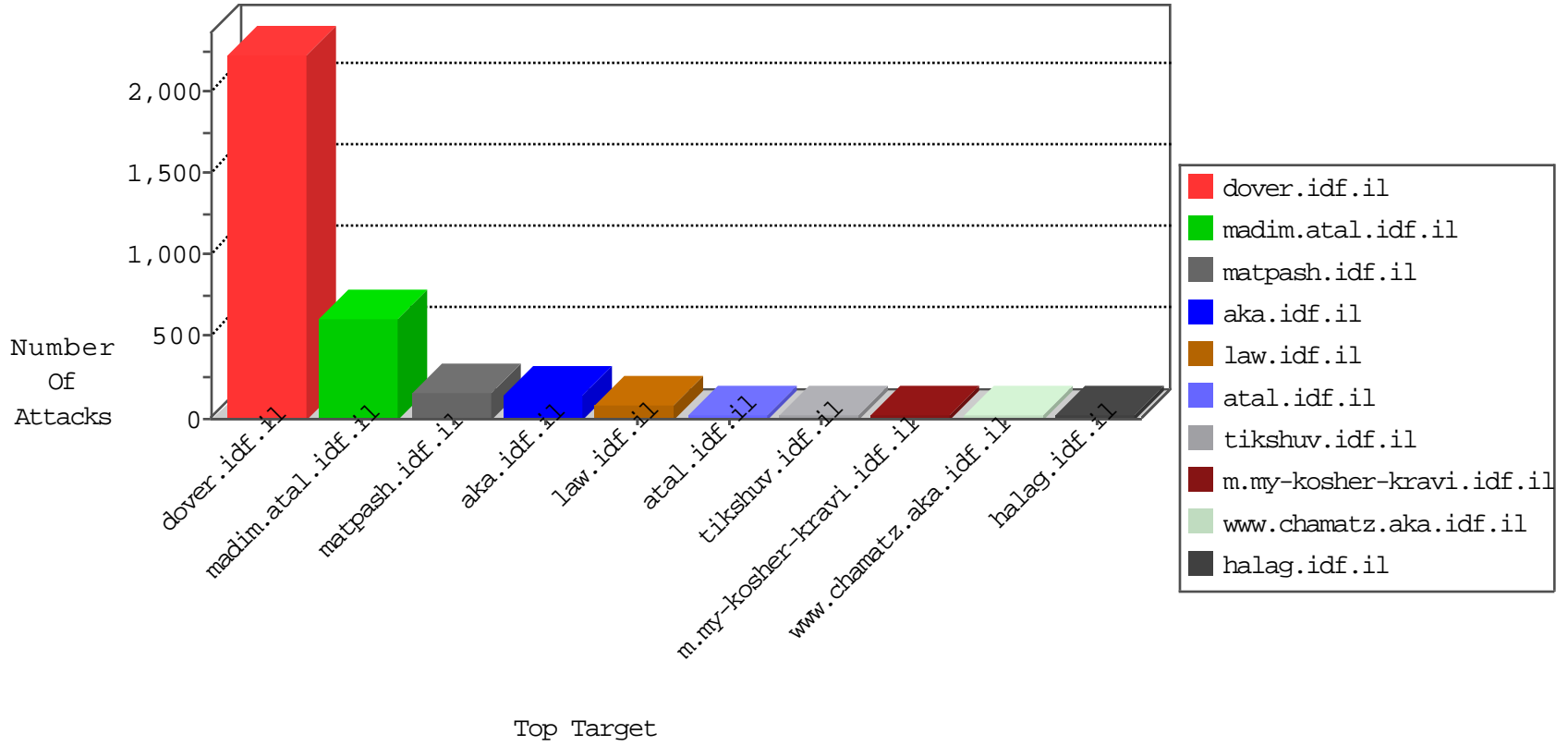


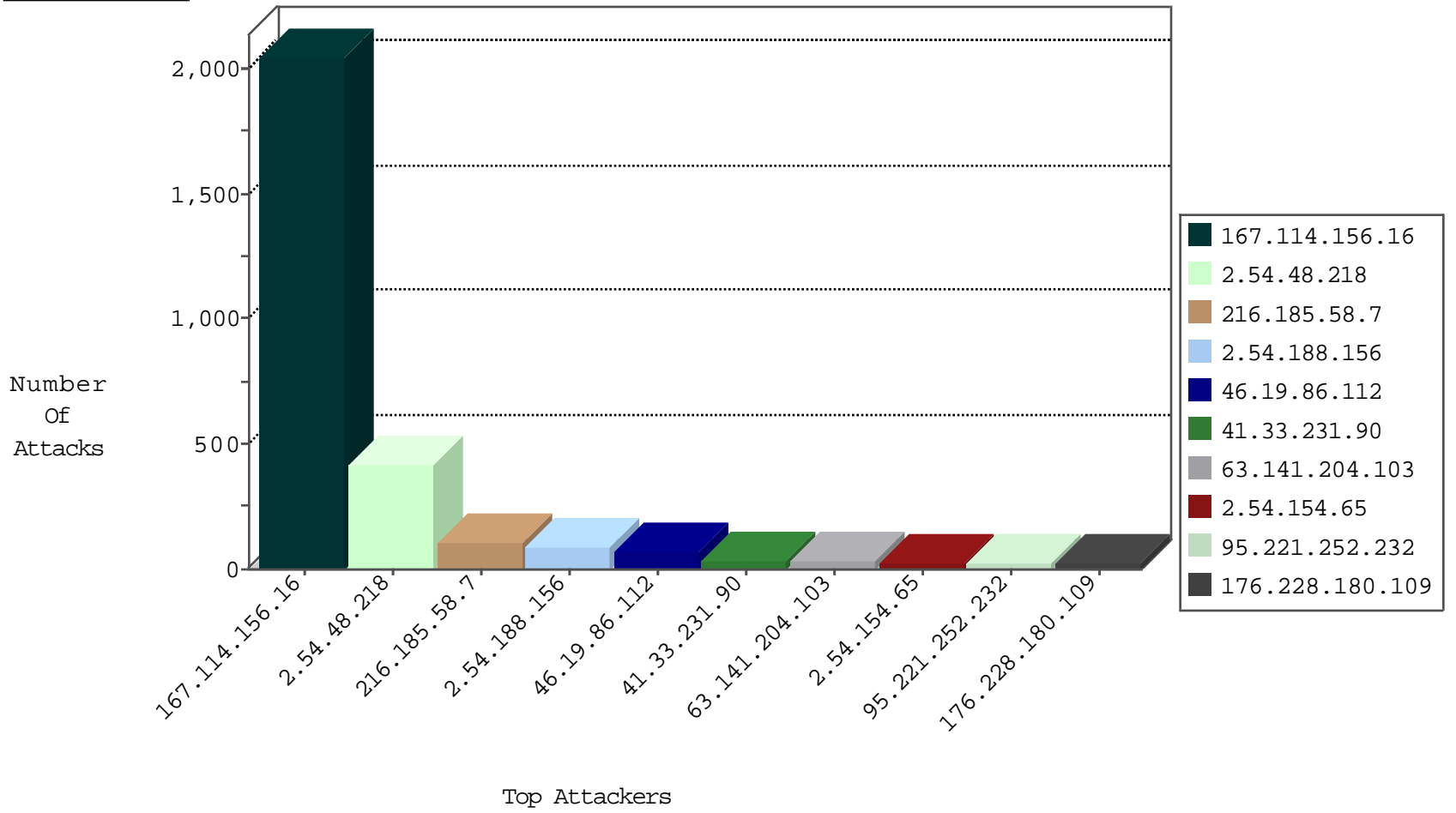
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.78.146	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	3314
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3203
198.58.103.92	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
52.16.5.197	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
107.170.42.128	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
82.145.229.7	Turkey	147.237.76.148	ggcenter.aka.idf.il	Block_Ip_Web_In	drop	1

12-25-2015-18:04:00 to 12-25-2015-19:04:00

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
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
209.66.70.253	147.237.77.176	United States	matpash.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.66.33	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sA (2)	2
109.235.254.181	147.237.76.176	Turkey	test.ncore.idf.il	ET SCAN NMAP -sS window 3072	1
109.235.254.181	147.237.76.176	Turkey	test.ncore.idf.il	ET SCAN NMAP -f -sS	1
82.117.208.243	147.237.72.217		e.idf.il	ET SCAN NMAP -sS window 1024	1
209.236.124.188	147.237.0.200	United States	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
78.193.2.8	147.237.76.86	France	navy.idf.il	ET SCAN NMAP -sS window 1024	1
187.253.111.157	147.237.77.74	Mexico	law.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
117.31.224.80	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
117.31.224.80	147.237.8.14	China	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
109.253.192.131	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
109.235.254.181	147.237.76.176	Turkey	test.ncore.idf.il	ET SCAN NMAP -sS window 2048	1
87.197.159.157	147.237.76.31	Slovakia	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
82.117.208.243	147.237.8.50		e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
189.214.42.18	147.237.72.14	Mexico	dover.idf.il(old)	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
117.31.224.80	147.237.8.46	China	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
117.31.224.80	147.237.8.24	China	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
114.215.111.222	147.237.76.86	China	navy.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
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	163
216.185.58.7	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	108
63.141.204.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	34
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	34
95.221.252.232	Russian Federation	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	24
95.108.132.178	Russian Federation	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	16
130.193.51.104	Russian Federation	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	14
141.8.142.43	Russian Federation	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	10
46.19.86.59	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
176.228.180.109	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
5.102.254.69	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
207.46.13.89	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
157.55.39.228	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
208.115.113.92	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.175	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
94.230.86.188	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.253.192.131	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.253.192.131	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.175	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
5.102.254.69	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.179	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
176.228.180.109	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	5
46.19.85.168	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
188.120.148.175	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.117.89.247	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
46.19.85.179	Israel	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
84.228.235.129	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.25	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
130.193.51.83	Russian Federation	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
31.168.247.135	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.108.214.72	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.65.182.20	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
188.139.250.137	Syrian Arab Republic	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
79.180.15.117	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.189.222	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.179	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
87.69.151.191	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.210.186.155	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
217.132.13.35	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.66.154.219	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.228.147.224	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.206.36	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.228.180.109	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.121.122.48	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
31.210.187.208	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
149.88.75.92	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.48.218	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	190
2.54.48.218	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	144
2.54.48.218	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 2.54.48.218	Block	79
2.54.188.156	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	70
46.19.86.112	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	65
2.54.154.65	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	26
2.54.188.156	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	21
85.250.193.37	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	9
46.120.75.230	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/templates/news/news.in.aspx	Block	6
46.19.86.219	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	4
84.228.9.221	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.67.31.246	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/main/sachar/default.aspx	Block	3
207.46.13.171	United States	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	3
212.199.112.144	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/8/	Block	3
46.120.206.95	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
87.69.215.29	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
41.107.38.86	Algeria	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/arr/	Block	2
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
79.183.104.14	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
188.143.232.19	Russian Federation	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/headerupper/	Block	2
217.132.95.238	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
46.120.142.235	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	2
85.250.230.240	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	2
176.228.128.6	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	2
79.181.14.210	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
61.135.190.198	China	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/style/shared/datepicker.css	Block	1
109.66.117.123	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.166.186.200	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
209.66.70.253	United States	147.237.77.176	matpash.idf.il	Directory Traversal (In URL)	Block	1
79.183.99.169	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
185.32.179.9	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/band	Block	1
68.180.231.40	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/templatecontrols/news/æx>x'x" x" xžæx?x"	Block	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
61.135.190.71	China	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/style/shared/reset.css	Block	1
213.57.108.248	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/	Block	1
173.254.33.42	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/xmlrpc.php	Block	1
79.116.25.197	Romania	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 79.116.25.197	Block	1
61.135.190.200	China	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/style/shared/text.css	Block	1
94.242.246.24	Luxembourg	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
50.87.43.17	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
209.66.70.253	United States	147.237.77.176	matpash.idf.il	Directory Traversal - 16	Block	1
46.19.85.210	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.48.218	Israel	147.237.0.19	madim.atal.idf.il	Too Many 403: Response Code per Session	Block	1
149.88.114.180	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
77.125.123.231	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/	Block	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
61.135.190.72	China	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	1
79.116.25.197	Romania	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/).html(	Block	1