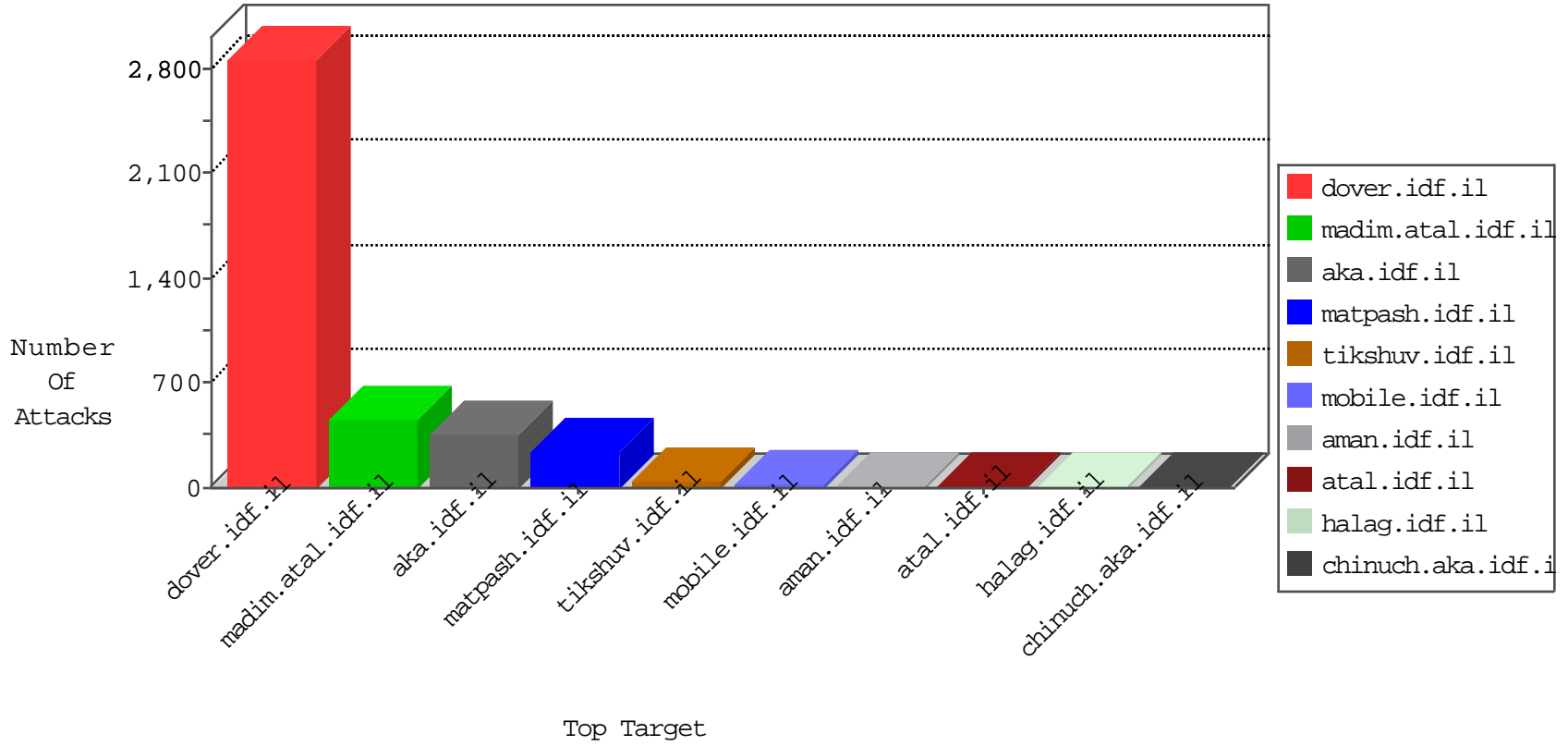


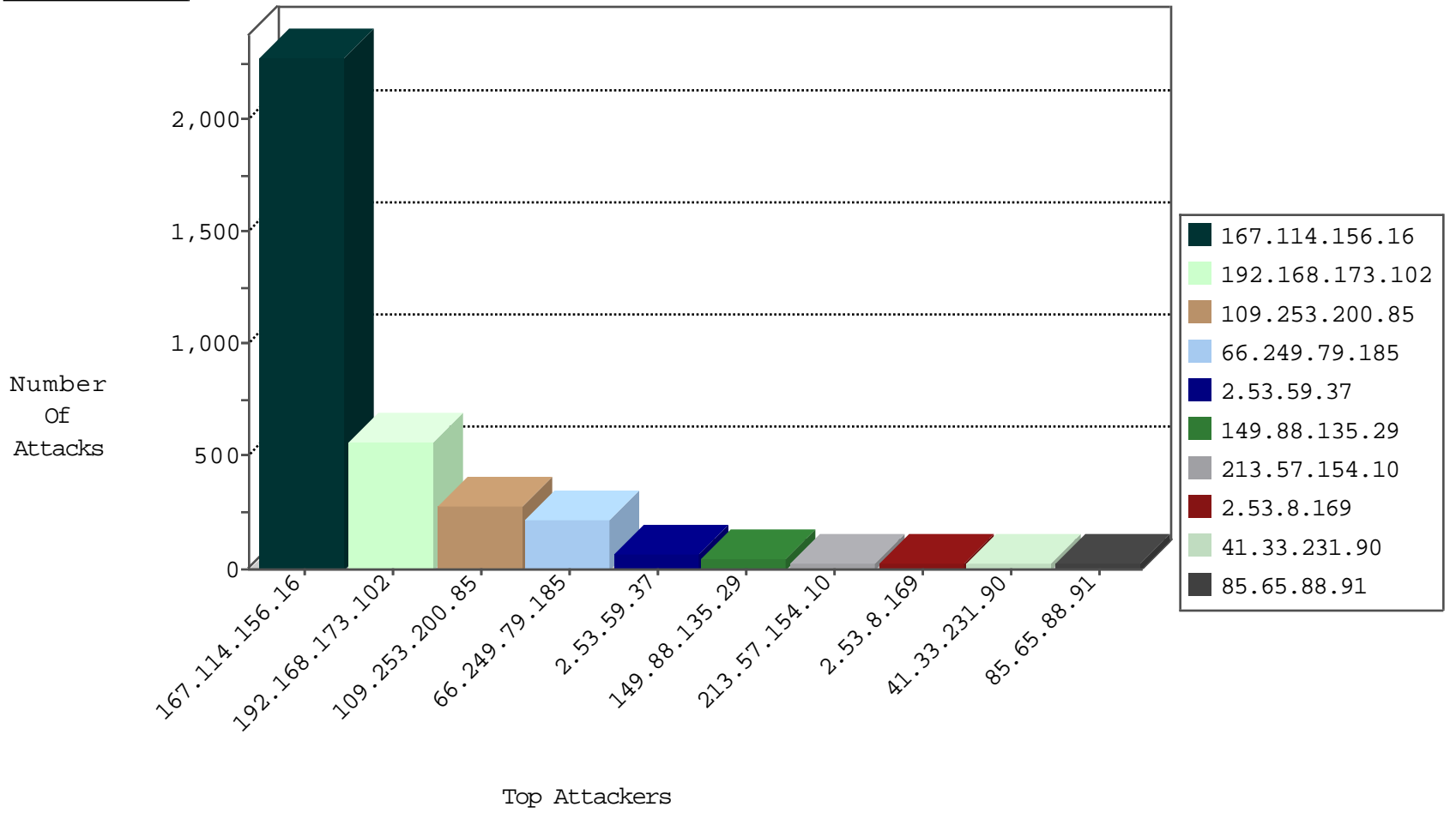
IDF Under Attack Daily Report



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	2279
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	615
37.26.146.234	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	264
213.57.251.102	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	248
85.65.88.91	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	93
105.225.188.189	South Africa	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	15
81.218.65.210	Israel	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	5
46.39.166.70	Czech Republic	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
105.101.74.132	Algeria	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
197.115.42.176	Algeria	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
74.91.20.196	United States	147.237.72.156	aman.idf.il	block-sp-traf1	forward	2
212.143.142.56	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
107.150.32.60	United States	147.237.76.147	chinuch.aka.idf.il	block-sp-traf1	forward	2
120.132.50.135	China	147.237.77.19	law-forum.idf.il	block-sp-traf1	forward	2
213.151.62.102	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
169.54.233.124	United States	147.237.77.233	atal.idf.il	JLM_Under_Attack_Con_Tcp	drop	1
93.201.95.195	Germany	147.237.0.35	akaws.idf.il	Block_Ntp_All_Net	drop	1
178.72.137.92	Armenia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
95.159.8.244	Syrian Arab Republic	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
185.70.184.164	Netherlands	147.237.77.178	e.matpash.idf.il	L4 Source or Dest Port Zero	drop	1
89.22.23.249	Russian Federation	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
5.170.128.187	Italy	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
213.57.154.10	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	28
85.64.109.180	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
87.69.130.210	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
89.238.143.70	United Kingdom	147.237.77.216	dover.idf.il	12026: HTTP: LOIC DDoS Tool (ONLY enable when under DoS attack)	Block	4
84.108.90.62	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	3
149.78.168.201	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	3
37.26.149.145	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.79.185	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sA (2)	224
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.64.181	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
185.114.157.12	147.237.77.74	Netherlands	law.idf.il	ET SCAN NMAP -f -sS	1
104.128.144.131	147.237.76.30	Canada	himush.idf.il	ET SCAN NMAP -sS window 4096	1
93.179.68.181	147.237.76.31	United Kingdom	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
70.33.31.101	147.237.8.28	United States	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
185.114.157.12	147.237.77.74	Netherlands	law.idf.il	ET SCAN NMAP -sS window 2048	1
113.190.20.120	147.237.0.16	Vietnam	my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
93.179.68.181	147.237.77.216	United Kingdom	dover.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.78.38	147.237.76.34	Netherlands	yochalan.idf.il	ET SCAN NMAP -sS window 1024	1
198.20.69.74	147.237.77.216	United States	dover.idf.il	ET DROP Dshield Block Listed Source	1
185.114.157.12	147.237.77.74	Netherlands	law.idf.il	ET SCAN NMAP -sS window 4096	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
192.168.173.102		147.237.77.216	dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	368
192.168.173.102		147.237.72.166	aka.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	195
109.253.200.85	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	19
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	18
85.65.88.91	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
46.19.85.165	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
109.65.75.222	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.182.162.168	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.27.105.73	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.203.64	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.116.124.41	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
185.32.179.31	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
109.253.200.85	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
185.89.217.231	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
185.3.144.34	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
149.78.59.158	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
46.116.232.21	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
85.65.88.91	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	4
46.120.54.215	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	4
185.89.217.229	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
5.22.131.112	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
149.78.238.81	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.125.93.253	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
94.230.86.13	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
87.71.10.233	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
2.54.152.95	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
85.65.88.91	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
79.181.200.195	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
149.78.59.158	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
109.65.105.253	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
62.90.35.177	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.71.27.126	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.55.39.106	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.67.27.152	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
157.55.39.194	United States	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.178.188.81	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
188.120.142.74	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.71.63.57	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.100.129	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.70.89.54	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.67.118.108	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
160.177.66.66	Morocco	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
87.71.90.35	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.0.38	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.131.33	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.86.203	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.120.88	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

04-07-2016-22:04:01 to 04-07-2016-23:04:01

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
109.64.82.231	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.71.10.233	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.200.85	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	258
2.53.59.37	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	67
149.88.135.29	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	44
2.53.8.169	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	26
80.246.133.178	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	15
84.109.226.220	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 84.109.226.220	Block	7
46.19.85.107	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	7
46.120.165.206	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
46.19.85.186	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
37.26.149.143	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
149.202.239.135	France	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1283-en/dover.aspx	Block	4
79.183.39.12	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
54.208.209.209	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 54.208.209.209	Block	3
194.114.146.227	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 194.114.146.227	Block	3
217.132.52.138	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.109.16.247	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
54.210.33.62	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 54.210.33.62	Block	2
46.120.186.153	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00\$ContentPlaceHolder1\$txtCaptcha in madim.atal.idf.il/login.aspx	Block	2
54.84.118.203	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 54.84.118.203	Block	2
54.164.146.184	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/894-he/-	Block	1
82.81.45.120	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/www.navy.idf.il	Block	1
79.180.193.64	Israel	147.237.76.42	refuah.idf.il	Unauthorized HTTP Method	Block	1
2.53.45.107	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
66.249.69.93	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/qanda/newsservice.aspx/js	Block	1
207.46.13.71	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
54.210.32.19	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 54.210.32.19	Block	1
79.182.162.168	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
46.116.124.41	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
68.180.229.89	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/undefined/	Block	1
54.210.117.241	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 54.210.117.241	Block	1
149.202.239.135	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
54.164.146.184	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 54.164.146.184	Block	1
79.181.29.16	Israel	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
66.249.75.44	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/7/63577.doc	Block	1
209.33.155.210	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-en/idfgdover.aspx	Block	1
109.253.203.64	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
78.41.115.145	Austria	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/./shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.224	Block	1
185.23.164.81	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/	Block	1
79.181.29.16	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
212.179.21.194	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc	Block	1
66.249.79.178	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/1392-en/cogat.asp	Block	1
120.132.50.135	China	147.237.77.19	law-forum.idf.il	Suspicious Response Code	Block	1
54.210.33.62	United States	147.237.77.226	www.chamatz.aka.idf.il	URL is Above Root Directory www.chamatz.aka.idf.il/./images/shared/home.png	Block	1
78.154.170.2	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi'a=0	Block	1
66.249.69.2	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/yoman/enlarge.asp	Block	1
87.71.63.57	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/faq.aspx	Block	1
54.210.18.124	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
79.181.29.16	Israel	147.237.77.226	www.chamatz.aka.idf.il	PHP Attempt	Block	1
213.254.241.4	France	147.237.72.166	aka.idf.il	Unknown Parameter ctl00\$ctl00\$btnSearch in www.aka.idf.il/main/sachar/default.aspx	None	1