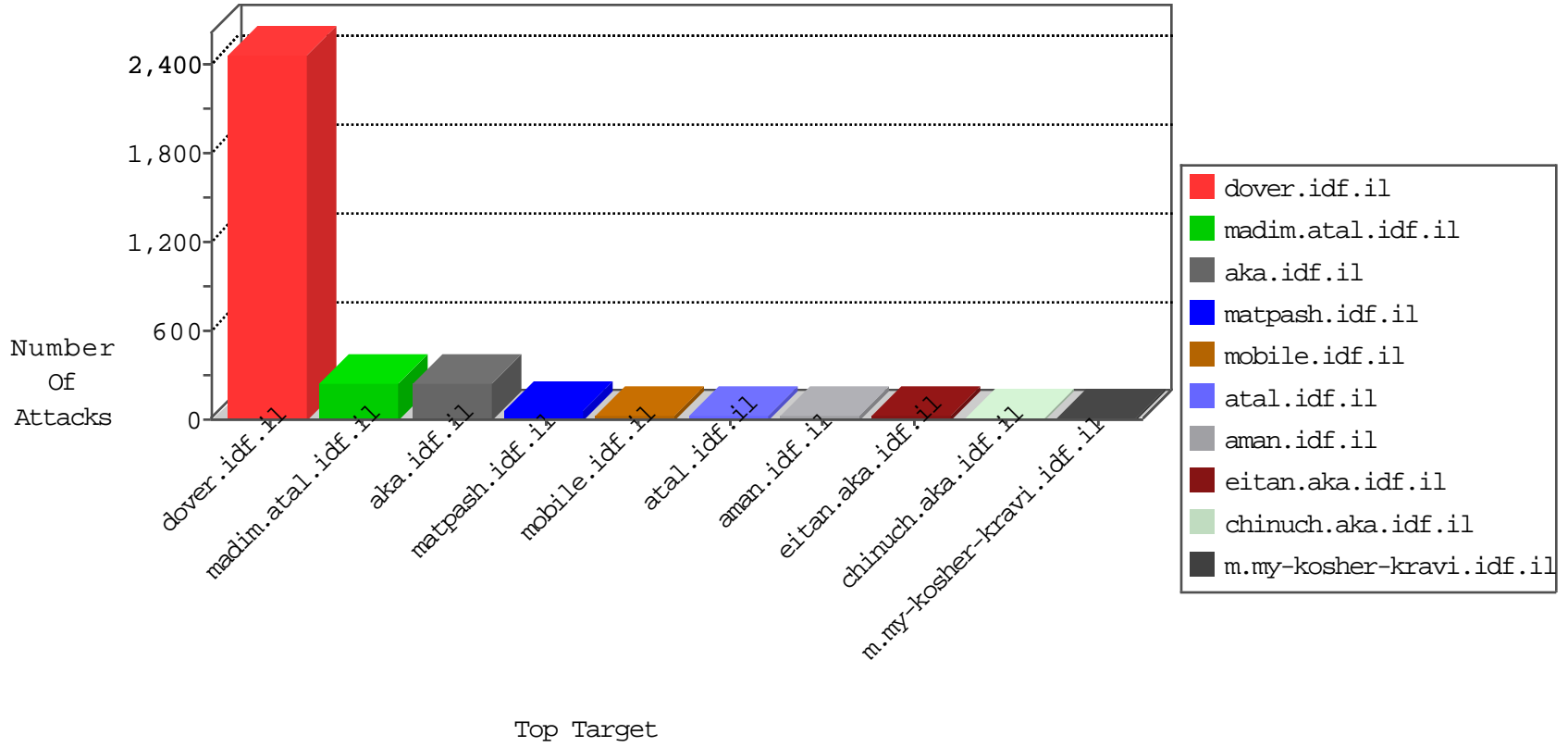


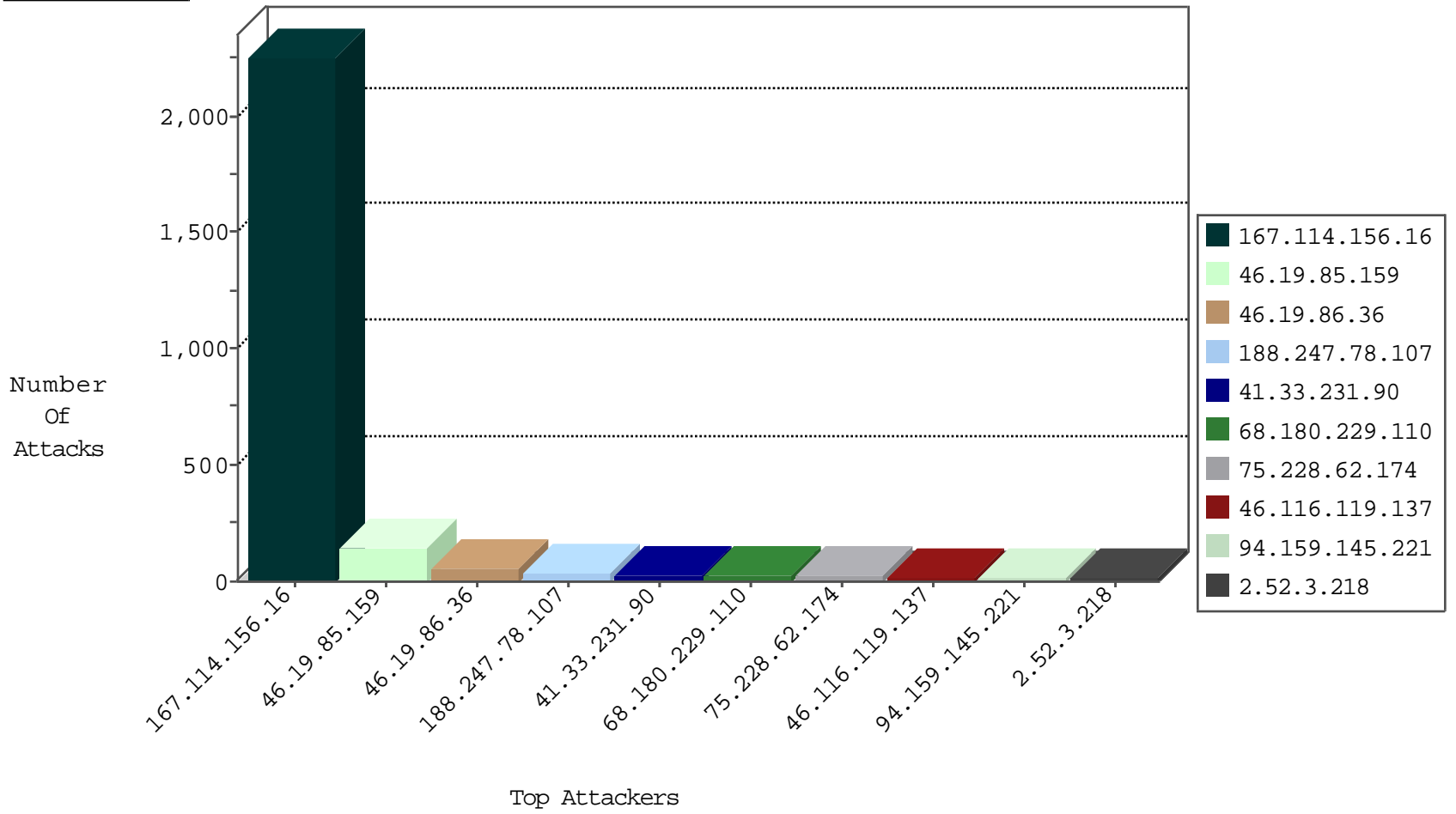
IDF Under Attack Daily Report



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	3131
105.107.183.209	Algeria	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
180.175.85.137	China	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
27.145.224.136	Thailand	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
62.210.85.77	France	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
123.126.113.154	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	10
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
58.253.96.122	147.237.0.33	China	idf.il	ET SCAN NMAP -f -sS	1
46.120.128.52	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
40.115.58.160	147.237.77.61	United States	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
40.115.58.160	147.237.76.148	United States	ggcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
178.20.72.19	147.237.72.14	Italy	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
168.62.238.153	147.237.8.45	United States	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
115.47.52.157	147.237.77.74	China	law.idf.il	ET SCAN NMAP -f -sS	1
58.253.96.122	147.237.0.33	China	idf.il	ET SCAN NMAP -sS window 2048	1
51.254.44.137	147.237.76.196	United Kingdom	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
40.115.58.160	147.237.76.199	United States	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
218.108.132.58	147.237.72.14	China	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
195.22.126.20	147.237.8.28	Poland	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
168.62.238.153	147.237.8.45	United States	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
115.47.52.157	147.237.77.74	China	law.idf.il	ET SCAN NMAP -sS window 2048	1
58.253.96.122	147.237.0.33	China	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
188.247.78.107	Jordan	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	33
94.159.145.221	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
68.68.96.204	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	12
94.230.86.216	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
109.67.182.105	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	10
5.102.254.13	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
130.193.51.91	Russian Federation	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
79.176.16.141	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.200	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.114	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
5.22.129.92	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.67.124.89	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.90	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.90	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.65.169.129	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	6
75.228.62.174	United States	147.237.77.216	dover.idf.il	Bad TCP sequence		alert	5
109.67.17.77	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
75.228.62.174	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
89.138.78.230	Israel	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	5
75.228.62.174	United States	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	5
109.67.17.77	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
188.120.148.168	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
185.3.144.72	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.160	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.22	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
5.102.254.221	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
85.64.44.252	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
65.55.210.63	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
2.52.3.218	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.248	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
2.52.3.218	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	4
94.230.86.219	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
199.30.24.39	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
149.88.140.99	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
79.180.134.54	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.228.197.24	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
188.120.148.220	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
185.3.146.213	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.3.218	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
79.182.191.254	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.0.186	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.177.52.21	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.102.254.58	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.86.108	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.69.50.244	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
77.125.92.84	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.27.105.155	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
46.19.85.159	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	77
46.19.85.159	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	61
46.19.86.36	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	59
68.180.229.110	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	24
46.116.119.137	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	19
66.249.65.93	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	12
176.13.5.81	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	11
2.54.150.104	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 2.54.150.104	Block	9
84.111.4.162	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation RepeatPassword in mobile.idf.il/sachar/changepassword	Block	6
68.180.229.239	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	6
88.208.252.195	United Kingdom	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 88.208.252.195	Block	5
84.228.144.192	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	4
5.102.254.165	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
95.86.82.10	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
85.64.25.115	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
79.180.134.54	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
62.219.137.5	Israel	147.237.72.156	aman.idf.il	Multiple Untraceable SSL Sessions from 62.219.137.5 (Unknown SSL Session)	None	2
79.183.131.11	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	2
37.238.83.58	Iraq	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	2
46.19.86.115	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
93.160.60.22	Denmark	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english	Block	1
62.128.48.166	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-20162-he/kkkkkkk=0ff22d83kkkkkkk_0ff22d83	Block	1
2.54.150.104	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-23032-he/dover.asp	Block	1
109.186.156.139	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/faq.aspx	Block	1
66.249.66.61	Israel	147.237.72.166	aka.idf.il	Unknown Parameter pop in www.aka.idf.il/main/home/	None	1
104.131.193.233	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
199.115.117.117	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to 147.237.72.156/_asterisk	Block	1
87.69.9.143	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf	Block	1
81.101.107.163	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
162.205.92.239	United States	147.237.77.216	dover.idf.il	Parameter Type Violation ct100\$ContentPlaceHolder1\$txtEmail in www.idf.il/1038-en/dover.aspx	Block	1
2.54.19.235	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
109.65.99.31	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
93.173.145.144	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
183.206.167.34	China	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/fckeditor/editor/	Block	1
85.65.17.228	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.161.185	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1462-he/atal.aspx	Block	1
109.201.154.217	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
79.182.172.12	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-22638-he/dover.aspx.	Block	1
46.120.255.9	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
199.115.117.117	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/_asterisk	Block	1
83.166.234.6	Russian Federation	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Unauthorized URL Access on 147.237.0.17/	Block	1
24.173.182.186	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
176.13.0.186	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
2.54.25.242	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.67.17.77	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1