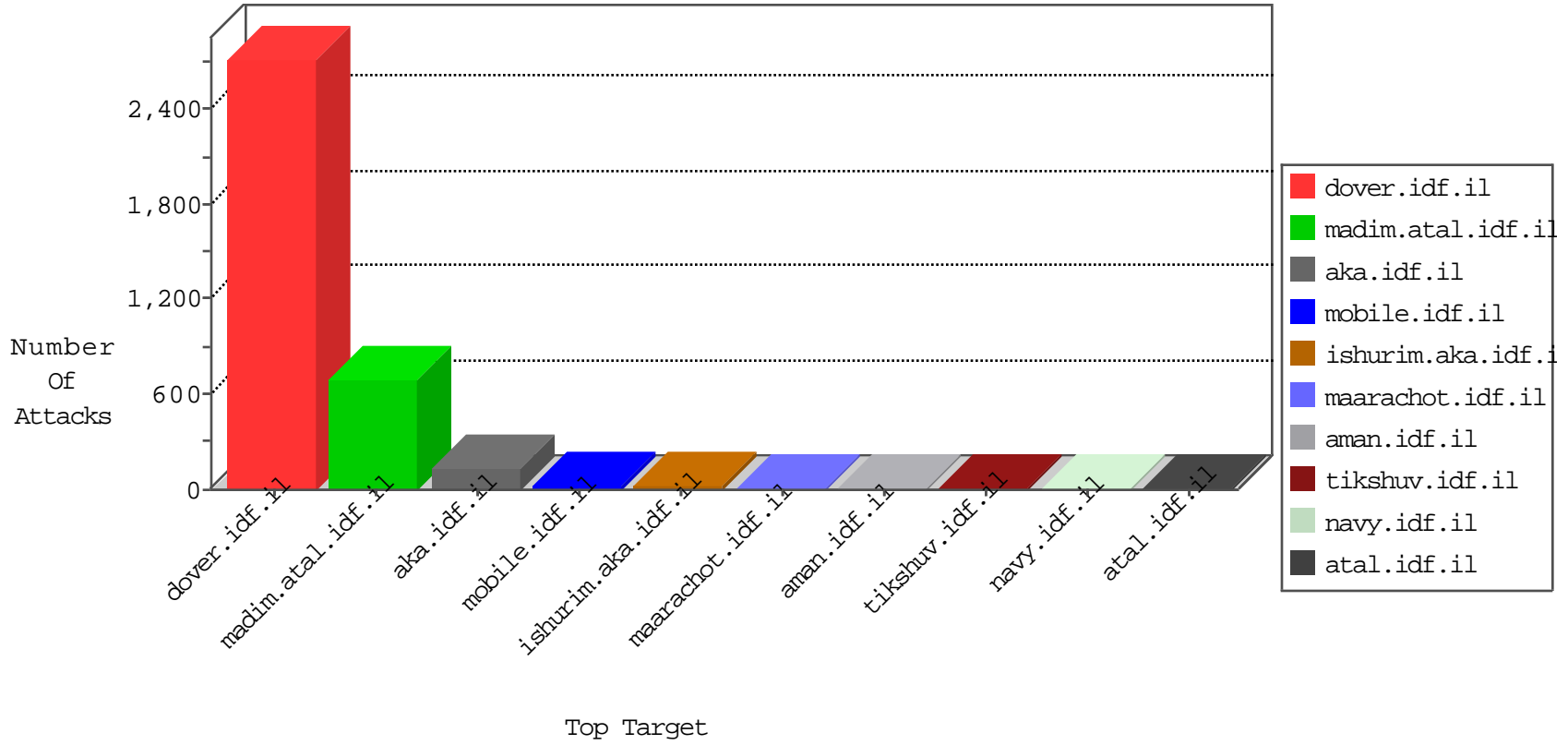


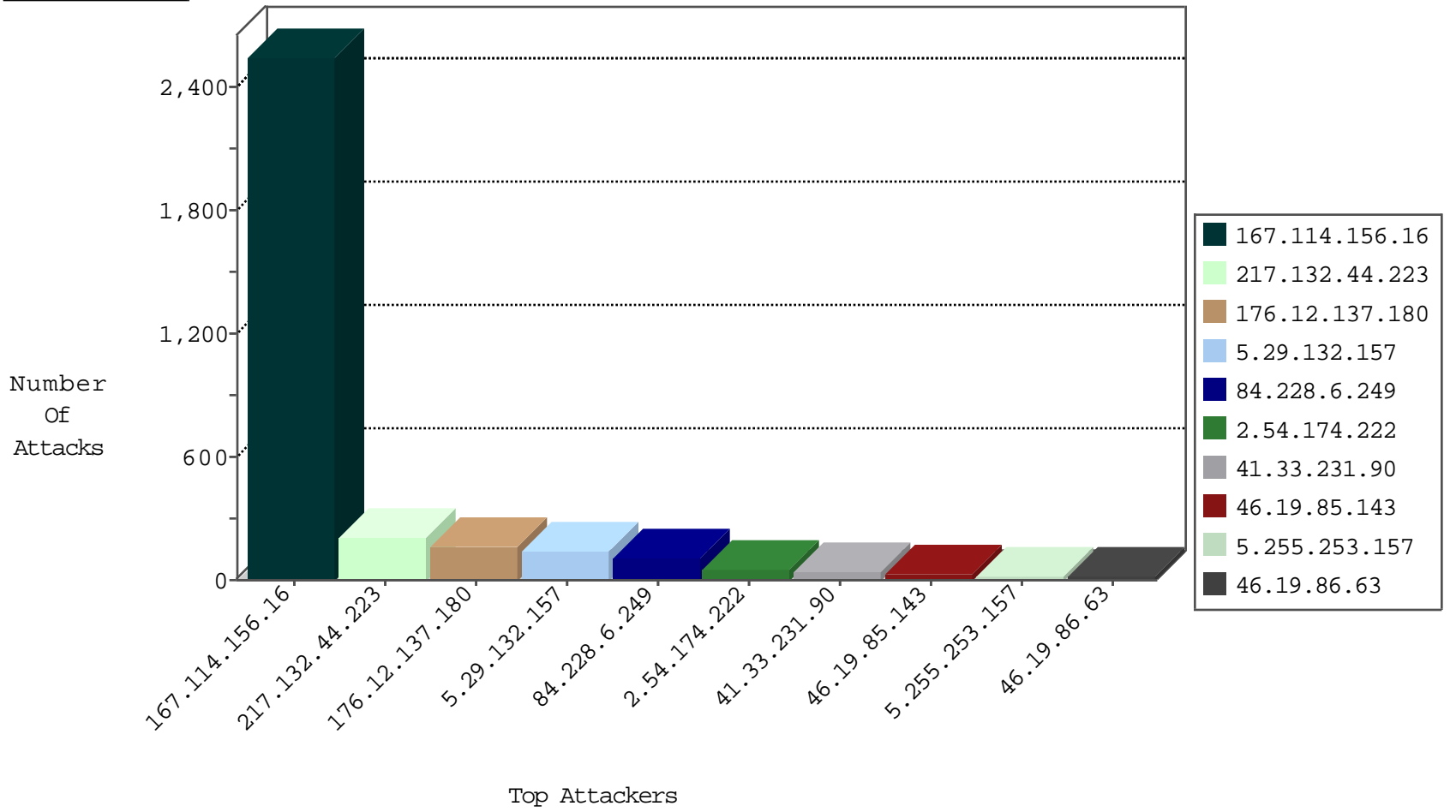
# IDF Under Attack Daily Report



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	3418
41.107.58.176	Algeria	147.237.77.216	dover.idf.il	HTTP-MISC-Acunetix-product3	dest-reset	9
41.107.58.176	Algeria	147.237.77.216	dover.idf.il	HTTP-MISC-Acunetix-Url	dest-reset	4
176.31.165.76	Germany	147.237.76.176	test.ncore.idf.il	Block_Ntp_All_Net	drop	1
107.150.55.51	United States	147.237.0.34	tikshuv.idf.il	block-sp-trafl	drop	1
176.31.165.76	Germany	147.237.76.177	ncore.idf.il	Block_Ntp_All_Net	drop	1
107.150.55.52	United States	147.237.76.39	mobile.meitav.idf.il	block-sp-trafl	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
52.35.180.112	United States	147.237.77.170	maarachot.idf.il	C1000107: DDOS-Spoofed HTTP Packets	Block	1
106.38.241.147	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
123.125.125.77	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
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.66.61	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
46.151.209.157	147.237.77.216	Saudi Arabia	dover.idf.il	ET WEB_SERVER PyCurl Suspicious User Agent Inbound	2
27.214.150.93	147.237.76.30	China	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
109.169.48.140	147.237.76.176	United Kingdom	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
109.169.48.140	147.237.0.17	United Kingdom	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
91.230.110.6	147.237.77.74	Russian Federation	law.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
201.172.124.181	147.237.72.14	Mexico	dover.idf.il(old)	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
113.59.33.61	147.237.0.33	China	idf.il	ET SCAN NMAP -sS window 3072	1
109.169.48.140	147.237.0.34	United Kingdom	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
91.236.120.166	147.237.77.74	Russian Federation	law.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	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	67
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
46.19.86.63	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	19
46.19.85.143	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
5.255.253.157	Russian Federation	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	12
46.151.209.157	Saudi Arabia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
66.249.66.61	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
5.255.253.157	Russian Federation	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
157.55.39.173	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
46.19.85.143	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
213.57.42.136	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
85.64.45.241	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
85.64.45.241	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.143	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.86.176	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
85.64.22.53	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	4
176.13.14.189	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
37.142.68.57	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
149.78.207.202	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
46.19.86.176	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.120	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
94.230.86.219	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
2.54.22.189	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.179.174.234	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.22.191	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.108.13	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.179.241.69	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.102.254.116	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.64.101.49	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
31.168.241.236	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.137.15	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.102.254.44	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.85.186	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.179.148.213	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.67.31.189	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.102.254.79	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
5.144.131.170	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
85.64.81.23	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.86.22	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
5.102.254.79	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
87.69.26.224	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
213.57.128.185	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
192.116.162.182	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
128.232.110.28	United Kingdom	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
213.57.128.185	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
5.29.247.44	Israel	147.237.76.30	himush.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
46.117.128.154	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
213.57.42.136	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	2

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.12.137.180	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	112
217.132.44.223	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	107
84.228.6.249	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	104
5.29.132.157	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	101
217.132.44.223	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	79
2.54.174.222	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	55
176.12.137.180	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 176.12.137.180	Block	43
5.29.132.157	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	36
217.132.44.223	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	24
37.142.64.19	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 37.142.64.19	Block	11
109.67.185.173	Israel	147.237.0.19	madim.atal.idf.i	Parameter Type Violation ctl00\$ContentPlaceHolder1\$txtLastName in madim.atal.idf.il/1088-he/meretz.aspx	Block	8
2.54.48.88	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
41.107.58.176	Algeria	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 41.107.58.176	Block	3
37.142.64.19	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1431	Block	3
176.12.140.167	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
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	2
85.64.45.241	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
176.12.149.233	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	2
157.55.39.173	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
46.19.85.196	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
77.125.240.93	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
176.12.144.31	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
52.35.180.112	United States	147.237.77.170	maarachot.idf.il	NULL Character in Header Name at	Block	1
194.90.15.61	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/9/109129.pdf	Block	1
176.12.137.180	Israel	147.237.0.19	madim.atal.idf.i	Too Many 404: Response Code per Session	Block	1
79.180.206.215	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.67.185.173	Israel	147.237.0.19	madim.atal.idf.i	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatenakatgauntity.aspx	Block	1
66.249.66.61	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	1
52.35.180.112	United States	147.237.77.170	maarachot.idf.il	Illegal Byte Code Character in Method	Block	1
103.30.90.134	Indonesia	147.237.77.216	dover.idf.il	eMail Hoarding	Block	1
84.109.81.170	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.26.147.196	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/aman	Block	1
176.12.148.134	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.81.149	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/templates/shared/usercontrols/trajector/	Block	1
129.64.152.64	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
109.65.3.71	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
52.35.180.112	United States	147.237.77.170	maarachot.idf.il	NULL Character in Method	Block	1
41.107.58.176	Algeria	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/cgi-bin/le_check_v3.exe	Block	1
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	1
176.12.137.180	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 176.12.137.180	Block	1
79.183.65.42	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https://www.idf.il/	Block	1
66.249.66.61	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catID in www.aka.idf.il/yohalan/home/home.asp	None	1
109.186.16.4	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/hinuch	Block	1
52.35.180.112	United States	147.237.77.170	maarachot.idf.il	Malformed HTTP Header Line 1	Block	1
208.184.112.75	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	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
84.109.242.29	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
68.180.230.224	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in www.nakchal.idf.il/1073-he/nakchal.aspx	Block	1
149.78.254.59	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1