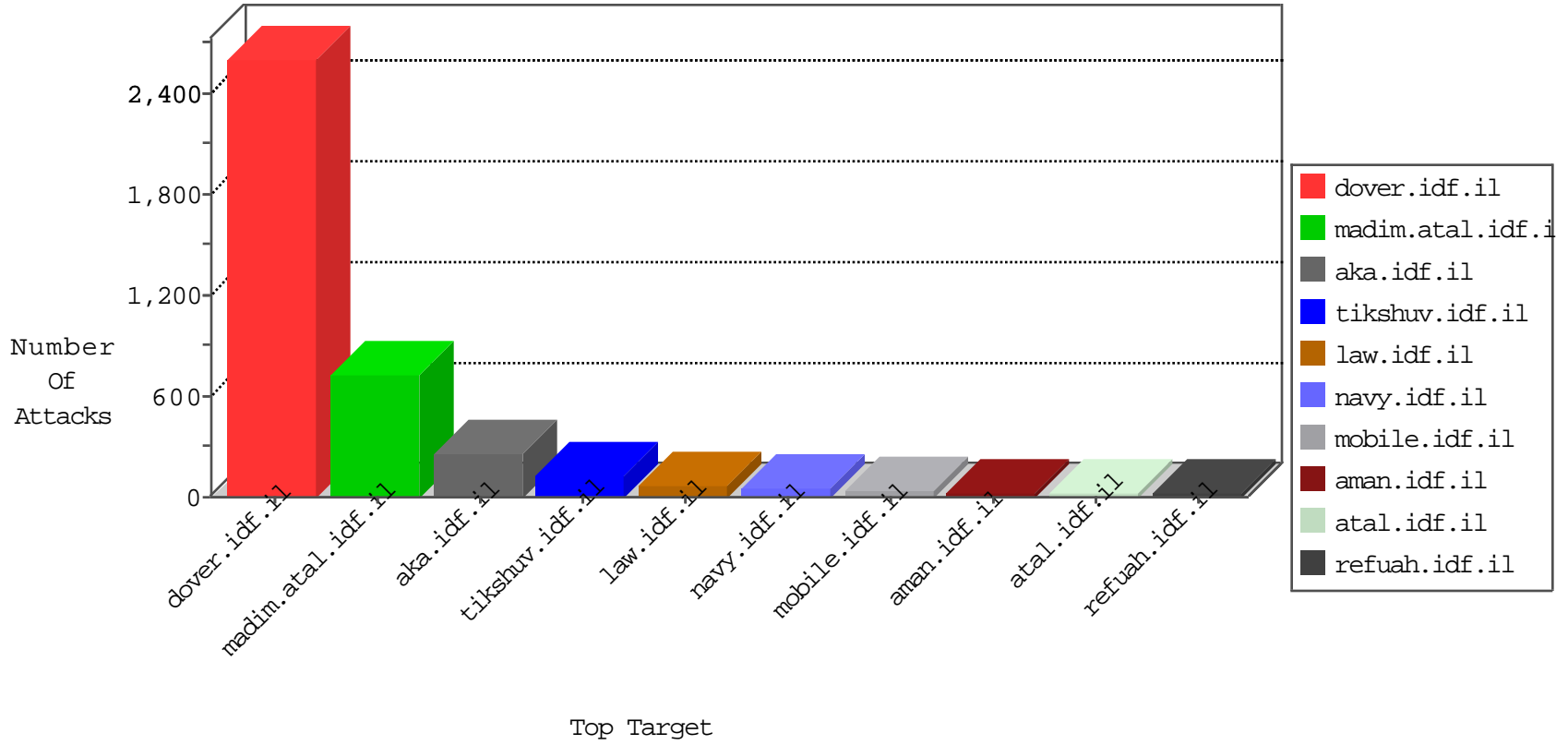


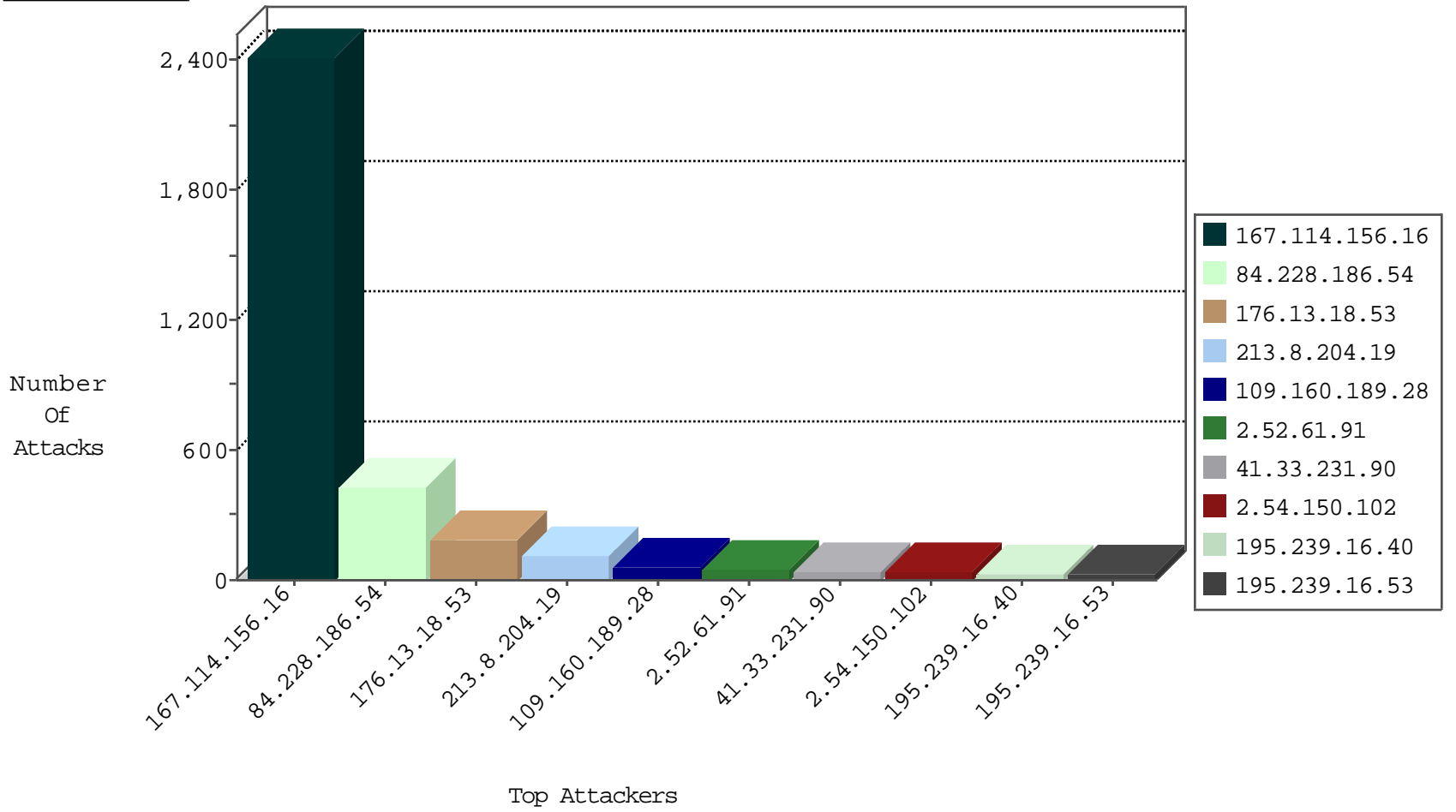
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.78.111	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	5076
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3058
79.181.167.157	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
212.179.54.237	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
217.23.5.212	Netherlands	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
151.80.31.152	Italy	147.237.76.42	refuah.idf.il	C228: HTTP: AhrefBot crawler	Block	3
151.80.31.151	Italy	147.237.76.42	refuah.idf.il	C228: HTTP: AhrefBot crawler	Block	2
151.80.31.154	Italy	147.237.76.42	refuah.idf.il	C228: HTTP: AhrefBot crawler	Block	2
188.165.15.204	France	147.237.76.30	himush.idf.il	C228: HTTP: AhrefBot crawler	Block	1
188.165.225.121	France	147.237.76.86	navy.idf.il	0543: HTTP: php.cgi Access	Block	1
151.80.31.153	Italy	147.237.76.42	refuah.idf.il	C228: HTTP: AhrefBot crawler	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
66.249.78.111	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
46.228.207.18	147.237.76.201	Germany	e.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
185.130.5.247	147.237.72.167		ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
112.196.49.101	147.237.77.216	India	dover.idf.il	ET SCAN NMAP -sS window 4096	1
84.117.113.152	147.237.77.216	Romania	dover.idf.il	ET SCAN NMAP -sS window 1024	1
50.204.188.142	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sS window 2048	1
50.204.188.142	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -f -sS	1
163.172.13.173	147.237.72.166	United Kingdom	aka.idf.il	ET SCAN NMAP -sS window 1024	1
112.196.49.101	147.237.77.216	India	dover.idf.il	ET SCAN NMAP -sS window 1024	1
50.204.188.142	147.237.77.176	United States	matpash.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
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	34
109.160.189.28	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	26
195.239.16.40	Russian Federation	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	26
109.160.189.28	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	26
195.239.16.53	Russian Federation	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	26
147.235.236.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
85.65.57.201	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
85.130.136.8	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
85.65.86.3	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
66.102.9.81	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	12
109.253.208.158	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.54.136.164	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
84.229.32.117	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
85.130.254.75	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
85.130.254.75	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
46.19.85.82	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.236	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
70.209.49.249	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
188.120.148.178	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
157.55.39.168	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.22.164	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.46	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.236	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
89.139.254.211	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
85.130.254.75	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
77.126.164.124	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.236	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.236	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
64.246.161.42	United States	147.237.0.34	tikshuv.idf.il	Header Rejection	header rejection pattern found in request	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
87.69.2.116	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
46.19.85.63	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
109.160.189.28	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
109.253.207.17	Israel	147.237.76.42	refuah.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
188.120.148.202	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.160.189.28	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
178.154.189.201	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.168.189.73	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
124.219.193.229	Japan	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
46.19.86.163	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.2.208	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.175	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.179.208.41	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.120.66.96	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
188.146.137.26	Poland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
2.54.36.89	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.108.249.65	Israel	147.237.77.216	dover.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
84.228.186.54	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	208
213.8.204.19	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 213.8.204.19	Block	115
84.228.186.54	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 84.228.186.54	Block	111
84.228.186.54	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	110
176.13.18.53	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	104
176.13.18.53	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	60
2.52.61.91	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	49
2.54.150.102	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	33
176.13.18.53	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	14
46.19.86.40	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
89.138.168.63	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
79.181.57.214	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
149.88.72.127	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.178.138.160	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/controls/atuda/Å	Block	3
176.13.0.149	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
217.132.118.163	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
195.154.146.225	France	147.237.77.216	dover.idf.il	Multiple Illegal HTTP Version from 195.154.146.225	Block	2
46.19.86.17	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	2
95.35.165.100	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
85.250.84.248	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
188.165.225.121	France	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 188.165.225.121	Block	2
79.179.167.175	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
91.200.12.5	Ukraine	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
87.69.209.199	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
31.13.97.123	Ireland	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
188.165.225.121	France	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/cgi-bin/php5	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
68.180.229.62	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/robots.txt	Block	1
66.102.9.81	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-en/www.idf.il/english	Block	1
204.13.201.137	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
91.200.12.5	Ukraine	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
183.79.223.169	Japan	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on list.ips.gov.il/robots.txt	Block	1
77.126.237.42	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
149.78.148.80	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	1
104.194.26.205	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/wp-login.php	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atall/izkor/view_imgtop.asp	Block	1
89.138.82.181	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.142.189.56	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.183.38.164	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
69.171.228.116	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
108.18.45.218	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
66.249.64.13	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/giyus/general.aspx	Block	1
212.76.103.3	Israel	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to kosher-kravi.idf.il/1137-he/orchot.aspx&sa=u&ved=0ahukewirrii38sdkahw h8ywkhc09b2cqqoubcbmwaw&sig2=nhjforzyv_dl8p36c9sjoq&usg=afqjcnhy 8j1hal_maedfg0lc5phcg8kbbq	Block	1
91.200.12.5	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
85.250.81.36	Israel	147.237.0.15	kosher-kravi.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 85.250.81.36	Block	1
184.168.200.236	United States	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
79.170.40.167	United Kingdom	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refuah.atal.idf.il/old/wp-admin/	Block	1
107.150.45.106	United States	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
200.21.240.135	Colombia	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1