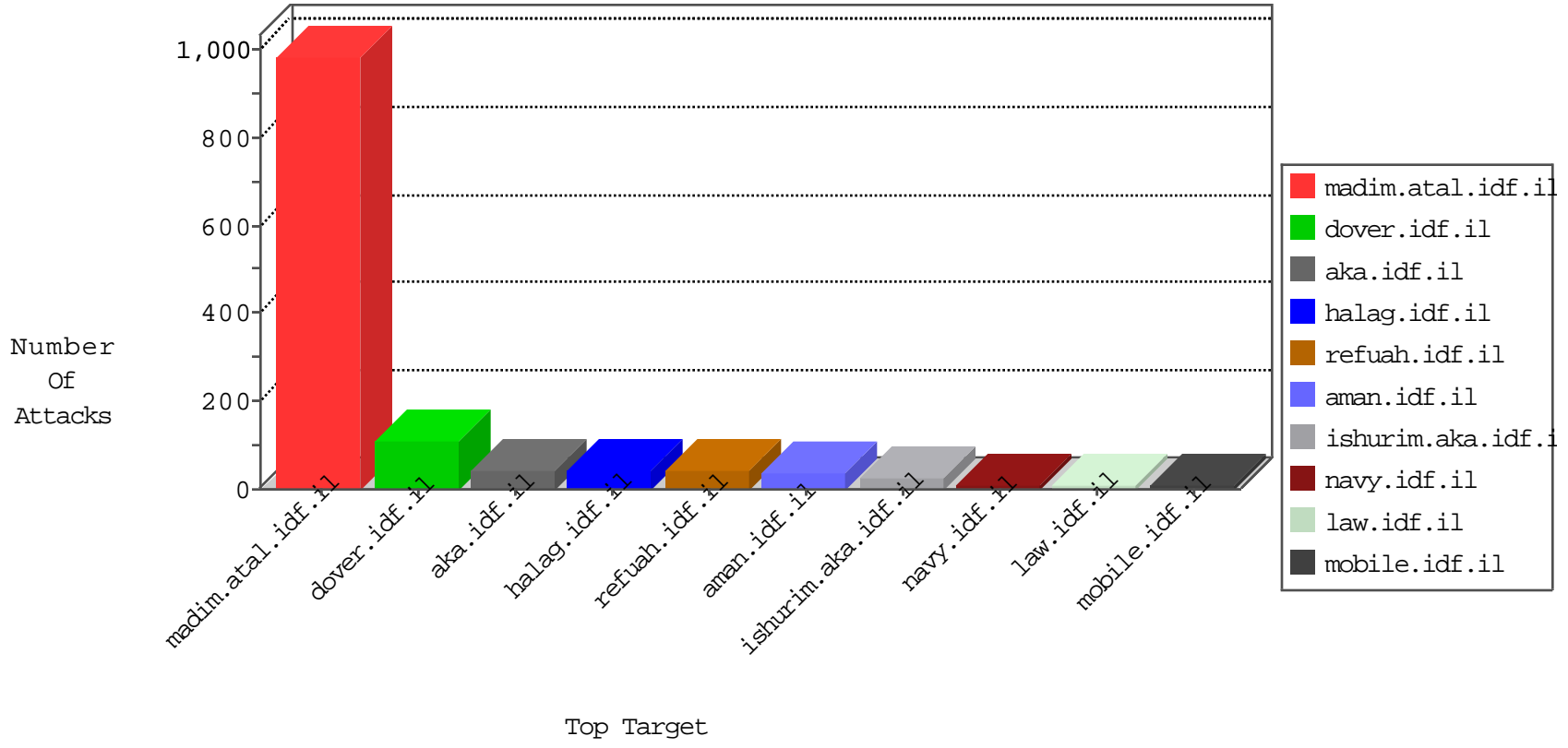


# IDF Under Attack

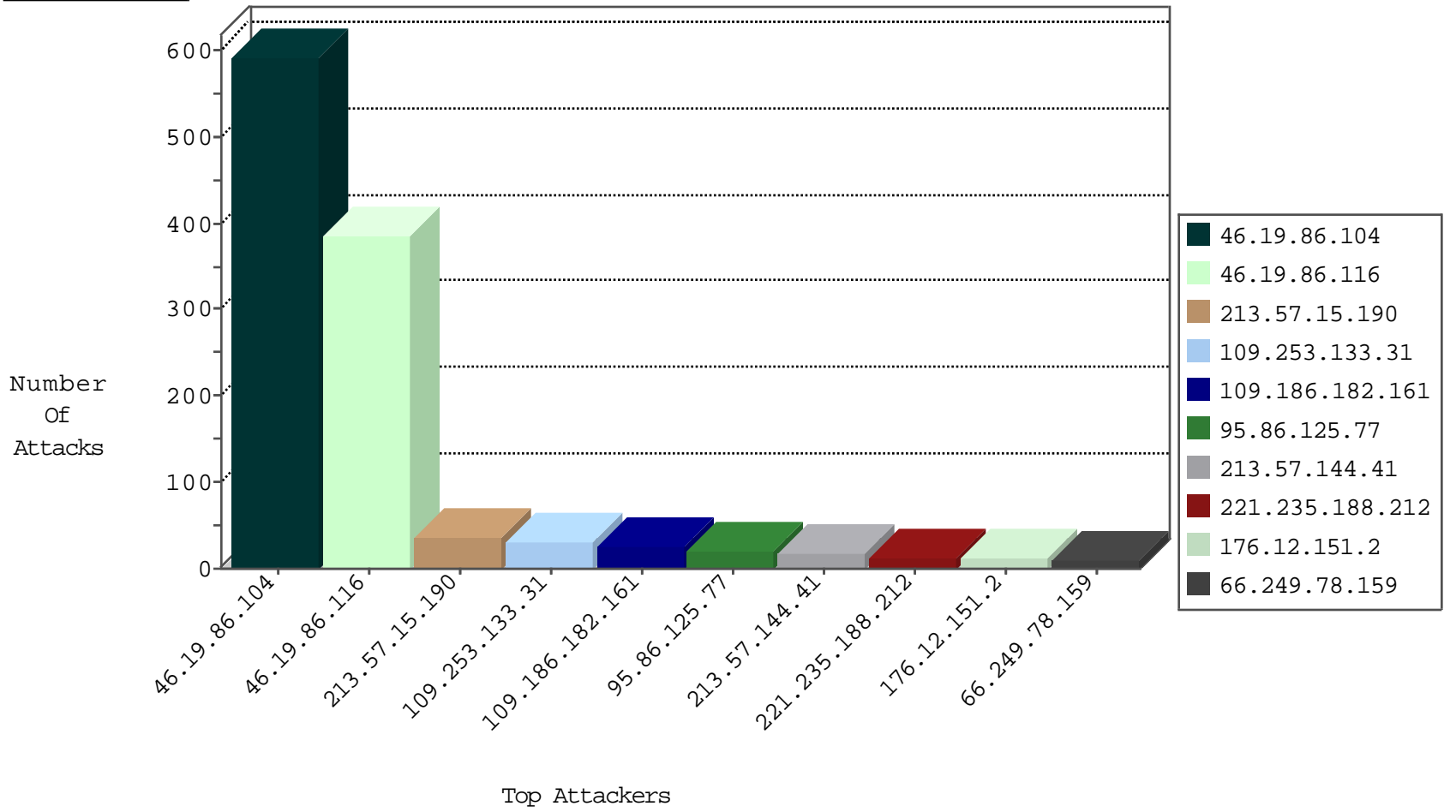
03-31-2015-00:03:05



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
95.86.125.77	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	320
109.186.182.161	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	258
213.57.144.41	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	174
66.249.78.204	United States	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	161
121.229.220.117	China	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
85.250.146.221	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
77.127.132.2	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
212.34.12.126	Jordan	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
71.6.135.131	United States	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	2
188.138.9.50	Germany	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	2
66.240.236.119	United States	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	2
71.6.165.200	United States	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	2
71.6.167.142	United States	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	2
71.6.135.131	United States	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	2
213.57.15.190	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
85.25.103.50	Germany	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.0.16	my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	1
175.44.5.185	China	147.237.77.74	law.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	1
71.6.165.200	United States	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.76.148	ggcenter.aka.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
83.244.51.227	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
66.240.236.119	United States	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1

## Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	8
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
149.78.123.178	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
43.255.191.166	Japan	147.237.77.233	atal.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.212	China	147.237.8.50	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.166	Japan	147.237.76.44	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.212	China	147.237.8.14	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.166	Japan	147.237.72.217	e.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.166	Japan	147.237.0.33	idf.il	ET SCAN Potential SSH Scan	1
222.69.94.13	China	147.237.76.147	chinuch.aka.idf.il	ET SCAN NMAP -sS window 2048	1
128.61.240.66	United States	147.237.77.235	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.188.212	China	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
104.155.230.225		147.237.0.200	m4u.idf.il	ET SCAN NMAP -sS window 3072	1
221.235.188.212	China	147.237.77.74	law.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.188.212	China	147.237.76.201	e.atal.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	China	147.237.77.243	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.188.212	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.166	Japan	147.237.77.234	halag.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.212	China	147.237.72.156	aman.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.166	Japan	147.237.76.201	e.atal.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.212	China	147.237.8.24	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.166	Japan	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.166	Japan	147.237.8.28	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
222.69.94.13	China	147.237.76.147	chinuch.aka.idf.il	ET SCAN NMAP -sS window 3072	1
142.204.145.248	Canada	147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
222.69.94.13	China	147.237.76.147	chinuch.aka.idf.il	ET SCAN NMAP -f -sS	1
104.155.230.225		147.237.0.200	m4u.idf.il	ET SCAN NMAP -sS window 4096	1
221.235.188.212	China	147.237.77.216	dover.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.212	China	147.237.77.61	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.188.212	China	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	China	147.237.0.33	idf.il	ET SCAN NMAP -sS window 1024	1
221.235.188.212	China	147.237.72.167	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
213.57.15.190	Israel	147.237.76.42	refuah.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	32
109.253.133.31	Israel	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
176.12.151.2	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	10
66.249.78.37	United States	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
109.253.159.242	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
46.19.86.39	Israel	147.237.77.243	mobile.idf.il	Invalid ACK number	Bad TCP sequence	monitor	6
2.52.187.190	Israel	147.237.76.86	navy.idf.il	Invalid ACK number	Bad TCP sequence	monitor	5
157.55.39.6	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
2.52.187.190	Israel	147.237.76.86	navy.idf.il	Invalid ACK number	Bad TCP sequence	alert	4
198.162.52.99	Canada	147.237.76.34	yohalan.idf.il		drop	drop	4
212.179.218.246	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	4
46.19.85.198	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	3
77.52.89.144	Ukraine	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
188.239.90.135	Ukraine	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
157.55.39.41	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
46.19.85.247	Israel	147.237.76.31	nakchal.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
157.55.39.42	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
207.46.13.16	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
68.180.228.117	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
207.46.13.112	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
141.212.122.13	United States	147.237.76.148	ggcenter.aka.idf.il		drop	drop	1
46.117.105.219	Israel	147.237.77.74	law.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
2.54.40.56	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
99.252.128.179	Canada	147.237.77.233	atal.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
46.19.85.190	Israel	147.237.76.42	refuah.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
212.179.23.22	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
77.237.138.202	Czech Republic	147.237.77.234	halag.idf.il	Response out of state	Block HTTP Non Compliant	monitor	1
46.117.105.219	Israel	147.237.77.74	law.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
37.46.39.217	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
99.252.128.179	Canada	147.237.77.233	atal.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
212.179.23.22	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
80.178.208.92	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	1
46.117.105.219	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
46.19.85.80	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
66.249.81.229	United States	147.237.76.31	nakchal.idf.il	directory traversal overflow	Directory Traversal	monitor	1
80.246.133.116	Israel	147.237.77.170	maarachot.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
46.19.85.161	Israel	147.237.77.233	atal.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
213.57.15.190	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
2.54.9.0	Israel	147.237.72.166	aka.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	1
157.55.39.121	United States	147.237.77.74	law.idf.il	Failed to handle connection data	Block HTTP Non Compliant	monitor	1
81.17.25.130	Switzerland	147.237.76.34	yohalan.idf.il		drop	drop	1
46.19.85.161	Israel	147.237.77.233	atal.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
46.19.86.104	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	594
46.19.86.116	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	387
109.66.132.66	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/webresource.axd	Block	4
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 5.255.253.124	Block	3
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	2
46.117.27.221	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
188.165.15.196	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.165.15.196	Block	2
213.251.182.10	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/0/size220x0/3410.jpg.src	Block	2
79.179.127.214	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to ww.idf.il/english/history/degania.stm	Block	1
188.2.175.245	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
109.253.158.49	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
80.246.133.226	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	1
188.239.90.135	Ukraine	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
79.177.3.225	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.64.137	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/	Block	1
178.120.231.39	Belarus	147.237.77.74	law.idf.il	Unknown HTTP Request Method COOK in URL www.law.idf.il/14-en/patzar.aspx	Block	1
37.142.113.188	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	1
109.65.99.75	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https://www.aka.idf.il/	Block	1
79.181.131.75	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	1
188.165.15.176	France	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9736-he/refuah.aspx	Block	1
157.55.39.207	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19748-he/idfgdover.aspx	Block	1
2.52.19.15	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	1
85.65.195.24	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https://www.aka.idf.il/	Block	1
207.46.13.72	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1392-he/refuah.aspx	Block	1
79.177.11.27	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to ww.idf.il/https://www.idf.il/	Block	1
66.249.78.89	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/templatecontrols/news/sip_storage/files/7/1437.pdf /	Block	1
178.137.93.140	Ukraine	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/+	Block	1
37.142.144.203	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00\$ctl00\$cpMain\$cpMain\$cpMain\$ctl121 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
79.183.155.248	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on ww.idf.il/https://www.idf.il/	Block	1
188.165.15.196	France	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
77.52.89.144	Ukraine	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
176.12.136.57	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	1
46.117.87.50	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
5.28.164.251	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
91.206.110.69	Ukraine	147.237.77.74	law.idf.il	Distributed Unknown HTTP Request Method	Block	1
213.57.15.190	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/webresource.axd	Block	1
79.177.159.125	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.97	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166//	Block	1
181.65.222.2	Peru	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
109.253.129.211	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	1
37.142.205.2	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/tfasim.aspx	None	1
80.246.133.20	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
77.127.112.91	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	1
176.12.136.224	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.117.192.77	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
94.231.178.30	Ukraine	147.237.77.216	dover.idf.il	Unknown HTTP Request Method COOK in URL www.idf.il/1116-en/dover.aspx	Block	1
79.178.204.73	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	1
66.249.78.166	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	1
187.137.51.169	Mexico	147.237.77.74	law.idf.il	Distributed Unknown HTTP Request Method	Block	1