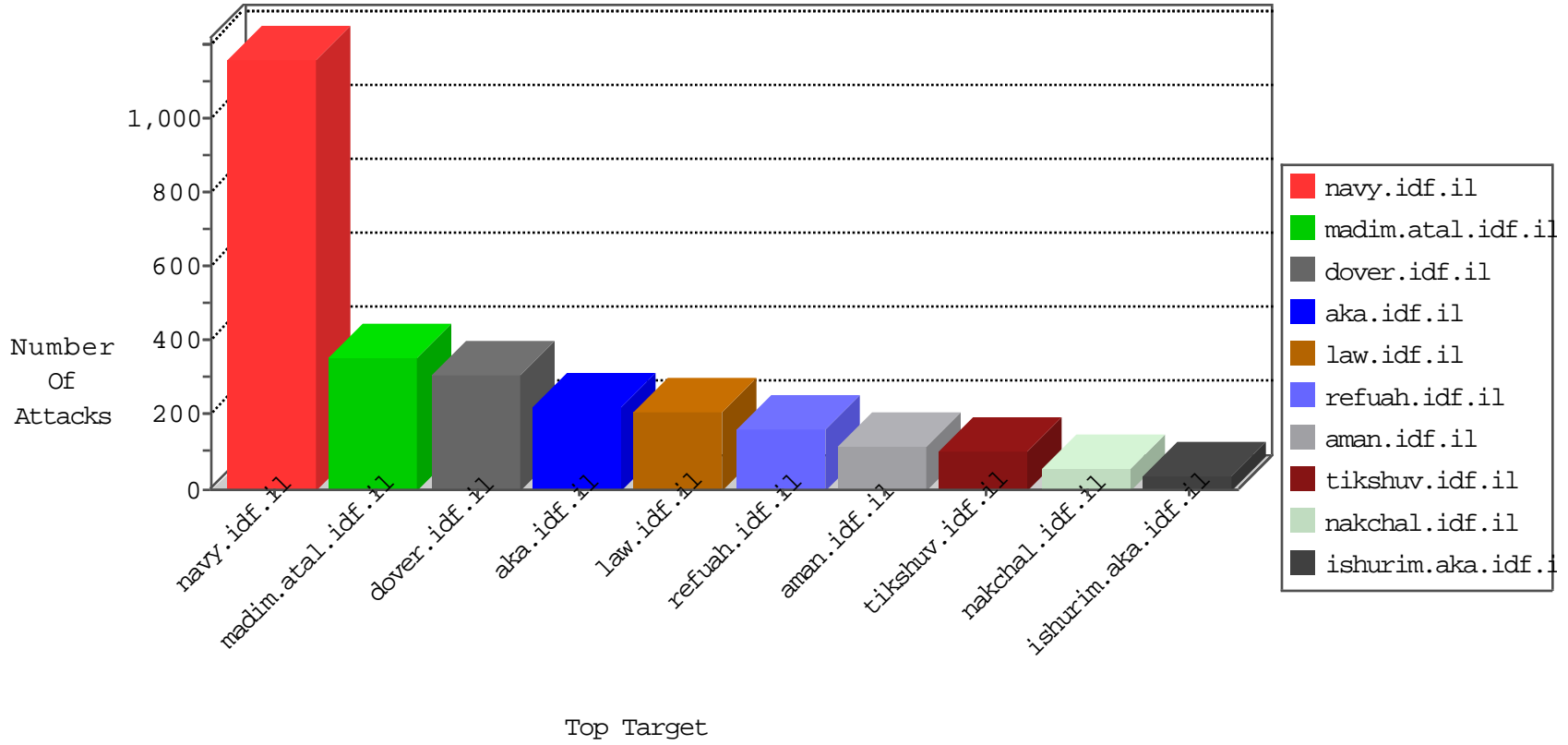


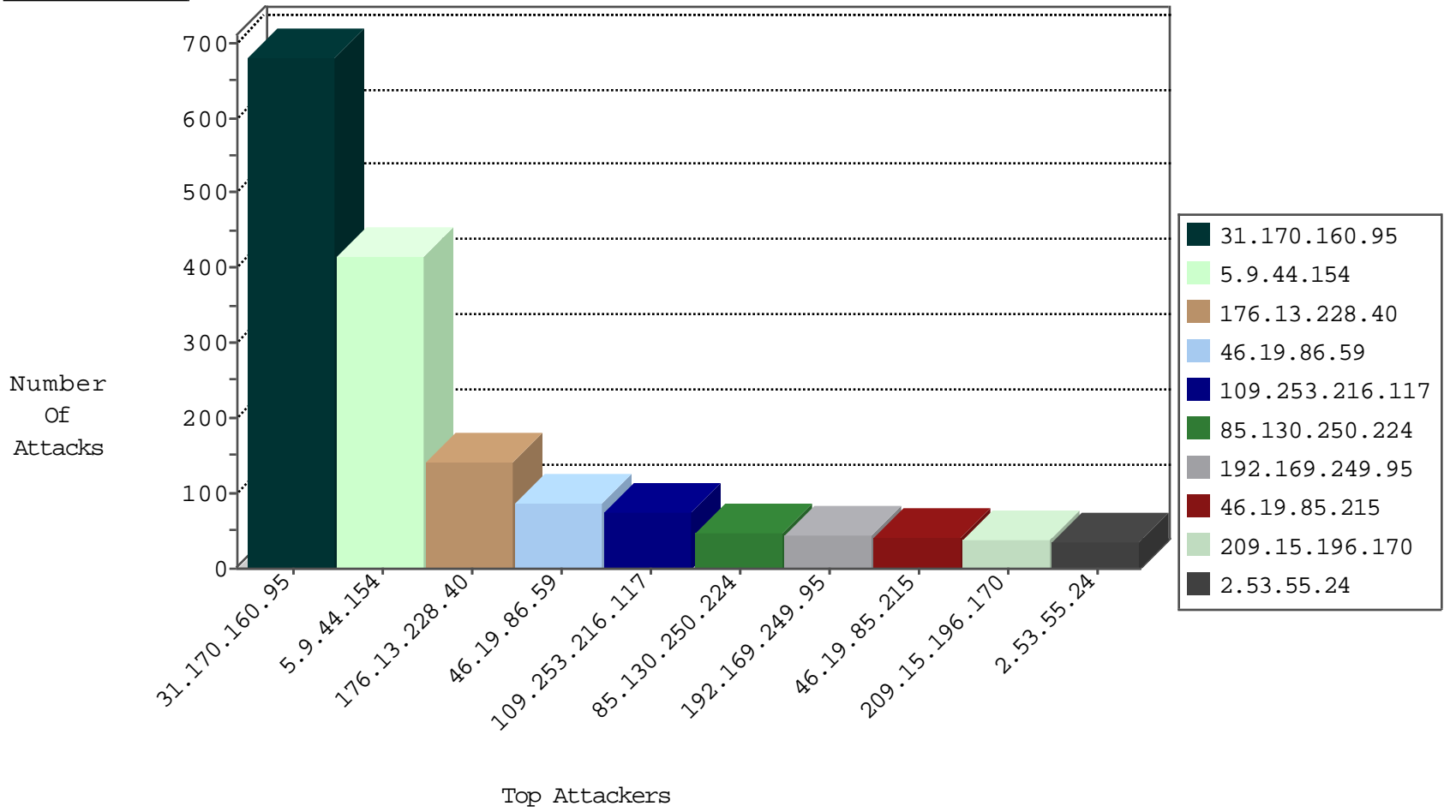
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
129.93.229.139	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
0.0.0.0		147.237.77.216	doover.idf.il	HTTP Page Flood Attack	forward	2
128.10.18.52	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
129.97.74.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
164.107.127.12	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
200.19.159.35	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
165.242.90.128	Japan	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
130.195.4.69	New Zealand	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
198.82.160.221	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
153.90.1.34	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
204.85.191.11	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
192.168.14.107		147.237.72.156	aman.idf.il	Invalid TCP Flags	drop	1
130.206.158.138	Spain	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
198.133.224.147	United States	147.237.72.217	e.idf.il	network flood IPv4 ICMP	drop	1
156.56.250.227	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
216.48.80.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
193.166.167.4	Finland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
134.197.113.3	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.223.8.112	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
200.19.159.34	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
129.97.74.14	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
195.113.161.83	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
147.83.29.234	Spain	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
129.93.229.138	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
209.15.196.170	Canada	147.237.0.34	tikshuv.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
195.74.38.15	Sweden	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	12
184.168.46.74	United States	147.237.0.34	tikshuv.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
37.228.93.70	Russian Federation	147.237.76.42	refuah.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
178.18.194.186	Turkey	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
23.91.70.51	United States	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
192.169.249.95	United States	147.237.76.42	refuah.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	6
50.63.197.208	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
209.222.4.188	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
184.168.46.74	United States	147.237.0.34	tikshuv.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
83.168.250.50	Sweden	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
37.228.93.70	Russian Federation	147.237.76.42	refuah.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	6
94.73.145.50	Turkey	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
50.63.197.208	United States	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	6
87.106.184.160	Germany	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
37.228.93.70	Russian Federation	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
97.74.215.165	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
69.10.156.44	Canada	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
217.37.125.121	United Kingdom	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
192.169.249.95	United States	147.237.76.42	refuah.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	6
87.242.112.35	Russian Federation	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
209.15.196.170	Canada	147.237.0.34	tikshuv.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
173.198.251.2	United States	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
74.208.230.195	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
192.169.249.95	United States	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
195.76.149.15	Spain	147.237.77.216	dover.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	5
87.242.112.35	Russian Federation	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	5
83.149.126.98	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	4
216.119.125.159	United States	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
50.63.197.204	United States	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
87.242.112.35	Russian Federation	147.237.77.74	law.idf.il	9785: HTTP: SQL Injection (Referer Header)	Block	1

## Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
192.169.249.95	147.237.76.42	United States	refuah.idf.il	SQL Injection - Select From	25
50.63.197.208	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	20
209.15.196.170	147.237.0.34	Canada	tikshuv.idf.il	SQL Injection - Select From	20
195.74.38.15	147.237.77.74	Sweden	law.idf.il	SQL Injection - Select From	14
87.242.112.35	147.237.77.74	Russian Federation	law.idf.il	SQL Injection - Select From	14
69.10.156.44	147.237.77.74	Canada	law.idf.il	SQL Injection - Select From	8
23.91.70.51	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	8
209.222.4.188	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	8
74.208.230.195	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	8
178.18.194.186	147.237.72.166	Turkey	aka.idf.il	SQL Injection - Select From	8
83.168.250.50	147.237.77.74	Sweden	law.idf.il	SQL Injection - Select From	8
217.37.125.121	147.237.77.74	United Kingdom	law.idf.il	SQL Injection - Select From	8
87.106.184.160	147.237.77.74	Germany	law.idf.il	SQL Injection - Select From	7
173.198.251.2	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	6
97.74.215.165	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	6
184.168.46.74	147.237.0.34	United States	tikshuv.idf.il	SQL Injection - Select From	3
79.182.32.127	147.237.76.200	Israel	eitan.aka.idf.il	Xenu Link Sleuth User Agent	2
79.182.32.127	147.237.72.166	Israel	aka.idf.il	Xenu Link Sleuth User Agent	2
58.218.200.137	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	1
50.63.197.204	147.237.76.42	United States	refuah.idf.il	SQL Injection - Select From	1
116.12.175.233	147.237.76.44	Singapore	e.refuah.idf.il	ET SCAN NMAP -sS window 2048	1
202.131.97.219	147.237.0.35	India	akaws.idf.il	ET SCAN Potential SSH Scan	1
66.249.73.163	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	1
37.228.93.70	147.237.76.42	Russian Federation	refuah.idf.il	SQL Injection - Select From	1
116.12.175.233	147.237.76.44	Singapore	e.refuah.idf.il	ET SCAN NMAP -sS window 4096	1
116.12.175.233	147.237.76.44	Singapore	e.refuah.idf.il	ET SCAN NMAP -f -sS	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
31.170.160.95	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	682
5.9.44.154	Germany	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	228
5.9.44.154	Germany	147.237.76.86	navy.idf.il	SYN Attack		monitor	135
5.9.44.154	Germany	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	52
46.19.85.215	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
50.63.197.204	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	17
46.19.85.67	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
46.19.85.67	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	14
85.130.250.224	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	13
46.19.85.65	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	13
46.19.85.215	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
37.26.146.175	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	12
37.26.146.175	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
37.26.149.134	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
37.26.146.175	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
46.19.85.215	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
46.19.86.157	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
85.130.250.224	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
85.130.250.224	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	9
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
37.221.160.114	Romania	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
46.19.86.67	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
176.13.18.212	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
46.19.86.91	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.65	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.86.91	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
2.53.13.32	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	7
156.204.212.202	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
5.22.134.207	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
85.130.250.224	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
2.53.13.32	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
2.53.173.183	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
50.63.196.35	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	6
50.63.197.145	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
80.178.126.47	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.213.198.101	Finland	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
46.19.85.67	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
77.125.84.241	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.221.160.114	Romania	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
79.180.213.17	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.69	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
24.8.42.50	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.123	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
24.8.42.50	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	5
46.19.86.3	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
24.8.42.50	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	5
24.8.42.50	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
101.184.78.24	Australia	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
92.208.248.162	Germany	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.228.40	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	140
46.19.86.59	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	88
109.253.216.117	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	76
2.53.55.24	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	36
213.8.115.122	Israel	147.237.77.216	dover.idf.il	Unauthorized HTTP Method	Block	6
213.8.115.122	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 213.8.115.122	Block	5
77.138.121.97	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar	Block	4
82.81.10.32	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	3
31.154.81.14	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	3
109.253.139.131	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.189	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.149.239	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.55.18.101	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
79.181.180.102	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	2
77.138.28.163	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/giyus/	Block	2
213.57.63.81	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/console/core/doc_mgr/undefined	Block	2
79.180.130.214	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/homepage/homepage.aspx	Block	2
80.246.138.58	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
79.176.90.140	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
62.101.184.125	Spain	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/2/4912.png	Block	1
5.22.134.60	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/wp-login.php	Block	1
148.251.95.16	Germany	147.237.77.216	dover.idf.il	Illegal Byte Code Character in URL /1283-16421-en/dover.aspx#012	Block	1
37.60.46.61	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
2.55.26.192	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
82.81.43.139	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.179.117.235	Israel	147.237.72.156	aman.idf.il	Multiple Untraceable SSL Sessions from 79.179.117.235 (Protocol violation (SSL_CONN_CLIENT_KEY_EXCHANGE))	None	1
66.102.9.5	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
5.22.134.207	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/apple-touch-icon-precomposed.png	Block	1
79.182.32.127	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/eitan/main/	Block	1
2.53.151.178	Israel	147.237.72.156	aman.idf.il	Illegal Parameter Encoding ctl00\$ctl00\$cpMain\$CPHMainContent7 in www.aman.idf.il/modiin/questionnaires.aspx	None	1
77.138.70.126	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
213.8.115.122	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/4/	Block	1
46.19.86.3	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
5.22.134.60	Israel	147.237.76.42	refuah.idf.il	PHP Attempt	Block	1
94.100.224.145	Georgia	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar/registrationwizard/step4.aspx	Block	1
79.179.117.235	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_KEY_EXCHANGE)	None	1
66.249.66.174	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
185.32.179.149	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
79.182.32.127	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized Method HEAD for www.eitan.aka.idf.il/	None	1
2.53.171.91	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
5.22.134.60	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/wp-login.php	Block	1
66.249.66.176	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
192.115.189.20	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip storage/files	Block	1
37.26.146.175	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
2.53.173.183	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
77.139.11.12	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/favicon.ico	Block	1
5.22.134.60	Israel	147.237.77.170	maarachot.idf.il	PHP Attempt	Block	1
79.180.213.17	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
69.171.230.110	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/9/1919.jpg	Block	1