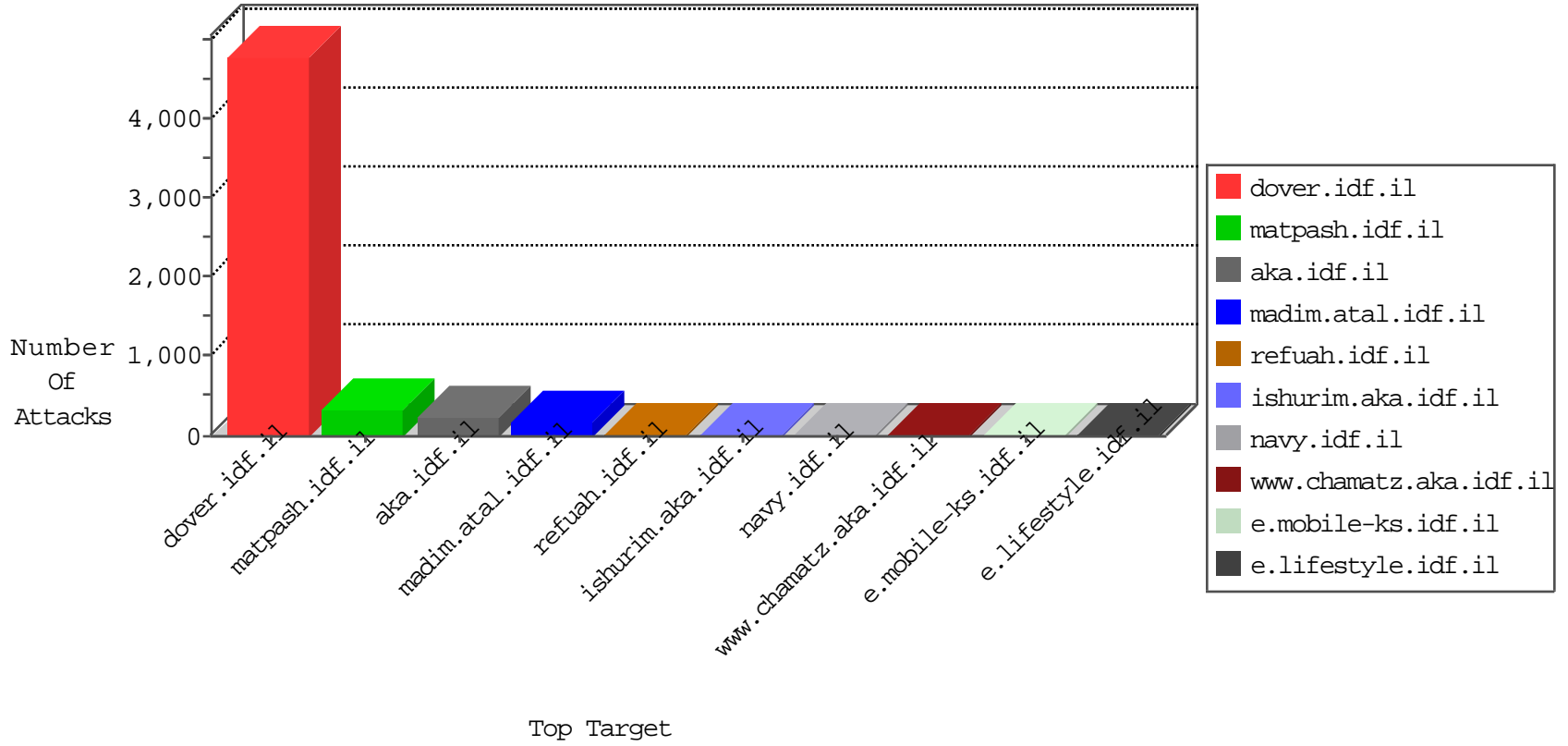
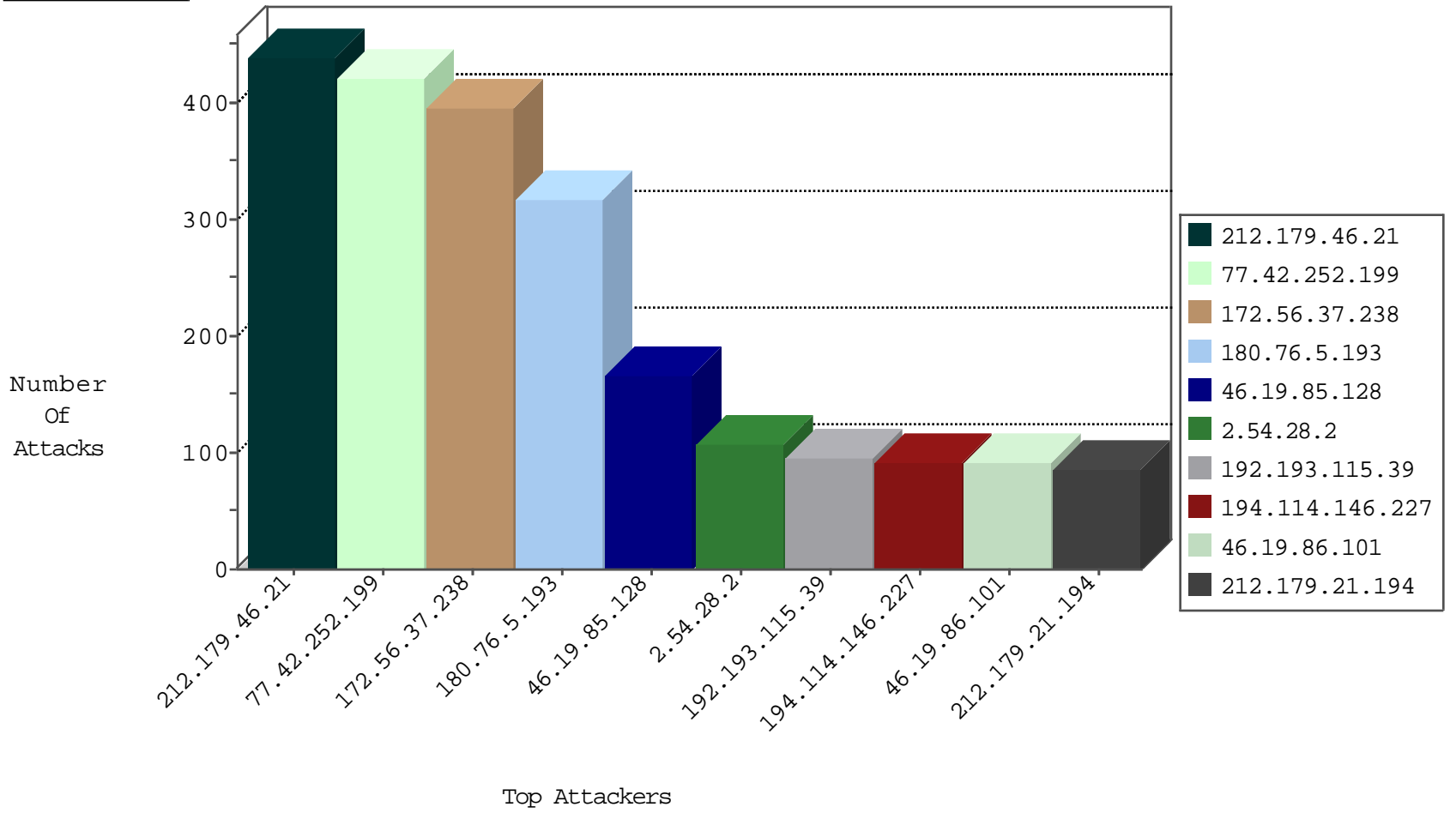


Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.67.152	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	883
46.19.85.128	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	74
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	5
94.188.161.145	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	5
212.235.80.238	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
46.116.252.6	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
2.54.15.217	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
81.218.208.46	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
194.177.16.3	Israel	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
124.232.142.220	China	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
180.76.5.193	China	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	317
81.218.251.251	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
212.179.55.126	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
194.90.178.37	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
66.240.192.138	United States	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	2
79.183.129.75	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.135.131	United States	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.25	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
93.120.27.62	Romania	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.0.16	my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.147	chimuch.aka.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.125	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
198.20.69.98	United States	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	1
94.188.161.145	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
71.6.167.142	United States	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.204	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
198.20.69.98	United States	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	1
176.106.46.74	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.167.142	United States	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.228	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
198.20.69.98	United States	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	1
184.168.139.128	United States	147.237.77.243	mobile.idf.il	EgovRep_B-N_70-99	Block	1

## Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
41.74.167.2	Rwanda	147.237.72.166	aka.idf.il	ET SCAN Potential SSH Scan	2
31.44.135.38	Israel	147.237.77.216	dover.idf.il	http_inspect: MULTIPLE HOST HEADERS DETECTED	2
66.249.73.193	United States	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
199.101.186.200	United States	147.237.77.178	e.matpash.idf.il	ET SCAN NMAP -sS window 3072	1
61.240.144.65	China	147.237.76.148	ggcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
198.20.69.98	United States	147.237.76.147	chinuch.aka.idf.il	ET DROP Dshield Block Listed Source	1
46.19.85.55	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
185.45.192.252	Seychelles	147.237.76.38	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
176.12.137.17	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
2.54.57.3	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
89.248.174.46	Netherlands	147.237.76.44	e.refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
1.241.229.116	Korea, Republic of	147.237.77.243	mobile.idf.il	ET SCAN Potential SSH Scan	1
89.248.174.46	Netherlands	147.237.0.33	idf.il	ET SCAN Potential VNC Scan 5900-5920	1
87.229.10.80	Hungary	147.237.8.28	e.mobile-ks.idf.il	ET SCAN NMAP -f -sS	1
80.179.225.42	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
212.25.85.234	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
61.240.144.67	China	147.237.0.33	idf.il	ET SCAN NMAP -sS window 1024	1
199.101.186.200	United States	147.237.77.178	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.86.17	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
192.117.113.18	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
43.229.52.201	Japan	147.237.0.200	m4u.idf.il	ET SCAN Potential SSH Scan	1
185.32.178.32	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
149.88.100.29	United States	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
2.52.162.75	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
89.248.174.46	Netherlands	147.237.76.34	yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
87.229.10.80	Hungary	147.237.8.28	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 2048	1
81.218.182.85	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
222.69.94.13	China	147.237.77.205	prisha.idf.il	ET SCAN NMAP -sS window 3072	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
212.179.46.21	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	439
77.42.252.199	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	421
172.56.37.238	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	388
2.54.28.2	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	106
192.193.115.39	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	95
46.19.86.101	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	90
212.179.21.194	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	84
192.115.29.157	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	77
46.19.86.92	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	76
46.19.85.27	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	71
46.19.85.58	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	68
146.234.100.106	Germany	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	67
79.178.136.69	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	53
194.114.146.227	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	52
176.12.146.71	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	36
46.19.86.80	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	36
81.218.40.194	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	34
37.26.147.201	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	32
46.19.86.63	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	30
82.166.252.77	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	30
84.228.40.166	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	28
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	28
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	28
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	27
46.19.86.157	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	26
46.116.133.234	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	25
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	23
2.54.15.217	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	22
207.232.29.213	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	22
80.74.97.148	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	22
31.186.228.68	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	22
87.68.152.31	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	22
213.8.44.227	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	22
46.19.86.149	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	21
80.178.214.27	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
109.253.141.22	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	19
46.19.86.234	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	19
2.52.52.11	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	19
185.24.79.57	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	19
37.26.147.222	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
38.111.147.86	United States	147.237.72.166	aka.idf.il		drop	drop	18
2.54.169.239	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
185.32.177.130	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
109.64.134.38	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
79.176.113.117	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
85.64.189.95	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
46.19.86.17	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
41.33.232.65	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
94.159.150.106	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	15

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
46.19.85.128	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.85.128	Block	155
80.246.138.94	Israel	147.237.72.166	aka.idf.il	Multiple Unknown HTTP Request Method from 80.246.138.94	Block	38
185.32.176.54	Israel	147.237.72.166	aka.idf.il	Distributed Unknown HTTP Request Method	Block	18
109.253.156.158	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	14
80.246.138.94	Israel	147.237.72.166	aka.idf.il	Distributed Unknown HTTP Request Method	Block	4
157.55.39.62	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 157.55.39.62	Block	3
213.151.52.249	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	3
212.117.137.146	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
157.55.39.32	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 157.55.39.32	Block	2
2.54.130.172	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
212.150.215.238	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	2
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
157.55.39.137	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 157.55.39.137	Block	2
212.150.215.238	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	2
66.249.78.87	Israel	147.237.77.226	www.chamatz.aka.idf.il	Distributed Unauthorized URL Access on 147.237.77.226//938-he/hamaz.aspx	Block	1
66.249.64.225	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip.storage/files/4/	Block	1
37.60.45.189	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
104.149.77.194		147.237.72.166	aka.idf.il	PHP Attempt	Block	1
208.80.192.33	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166//	Block	1
66.249.65.237	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-18775-he/dover.aspx	Block	1
157.55.39.161	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/www.tikshuv.idf.il	Block	1
46.19.86.203	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
157.55.39.32	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
84.228.153.12	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/forgotpassword.aspx	None	1
2.52.130.161	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
185.32.176.111	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.242	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1364-he/refuah.aspx	Block	1
157.55.39.62	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage/files/1/24	Block	1
66.249.64.247	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/edim/yoman/enlarge.asp	Block	1
37.142.163.120	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.66.112.66	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
81.218.193.19	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman/site/spotting/spotting.asp	Block	1
66.249.67.79	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 66.249.67.79	Block	1
157.55.39.162	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 157.55.39.162	Block	1
46.116.252.6	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https://www.idf.il/	Block	1
84.228.234.207	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
217.69.133.190	Russian Federation	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/brothers/skira/default.asp	None	1
185.32.177.130	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.81.233	Israel	147.237.77.176	matpash.idf.il	URL is Above Root Directory www.cogat.idf.il/./favicon.ico	Block	1
157.55.39.136	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/brothers/sitemap	Block	1
66.249.64.252	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/manilot/login	Block	1
109.67.172.103	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
81.218.251.250	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
66.249.73.136	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/71902-he/maarachot.aspx	Block	1
157.55.39.162	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/brothers/skira/default.asp-catid=57478&docid	Block	1
157.55.39.32	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/yohalan/main/asp	Block	1
54.245.64.111	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 54.245.64.111	Block	1
93.173.155.63	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
2.54.152.26	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/webresource.axd	Block	1
185.32.178.109	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1