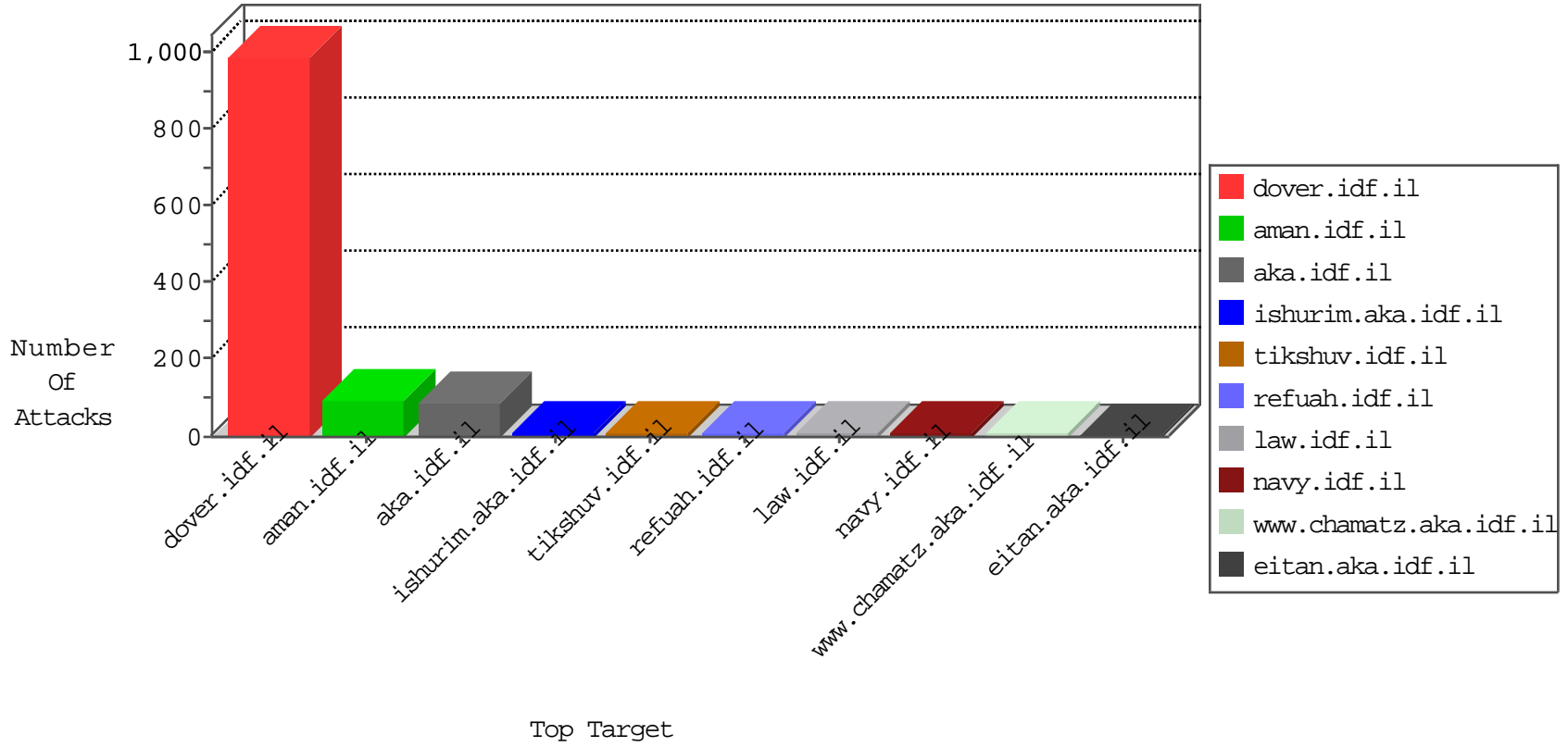
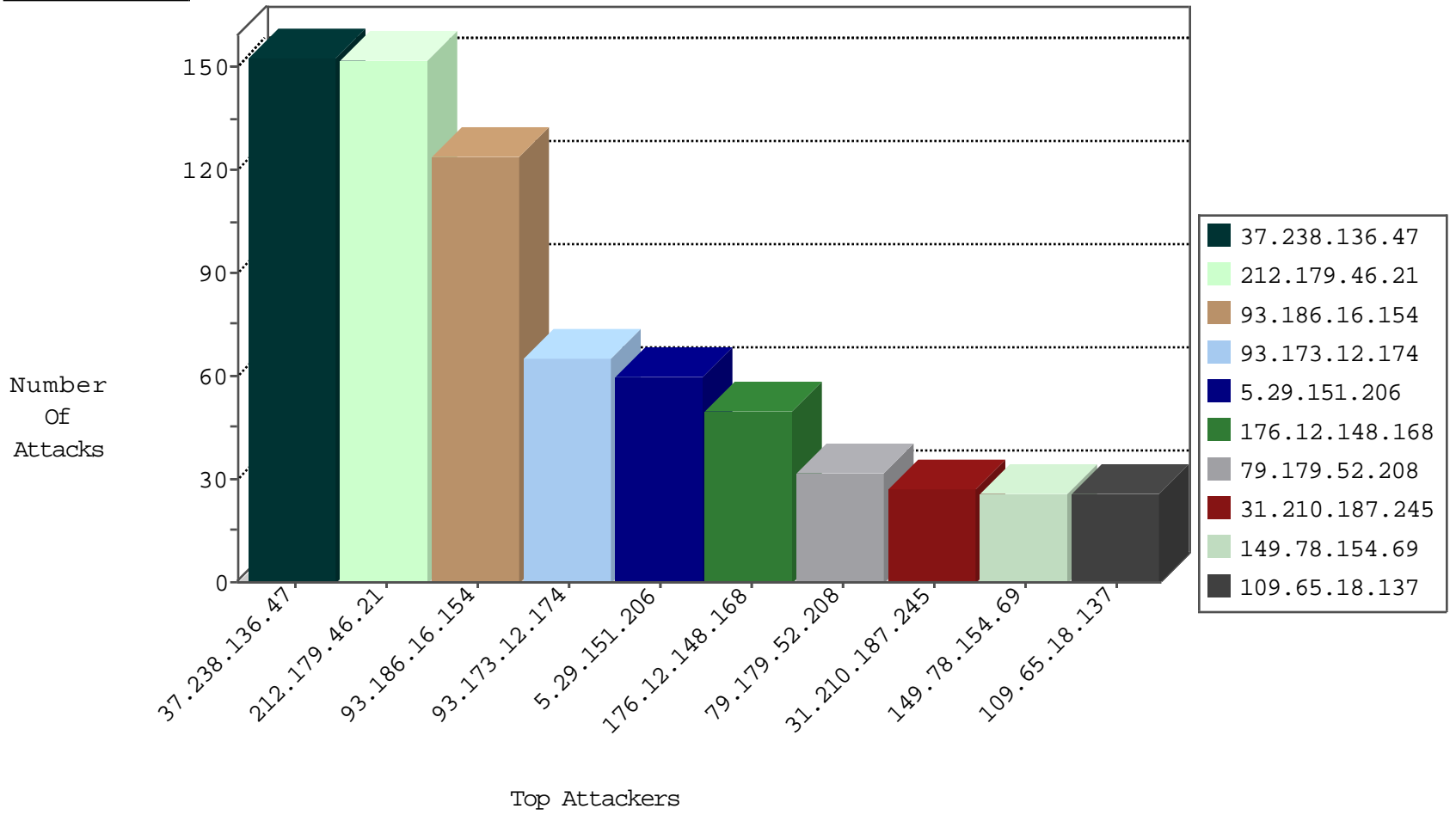


Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.78.89	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	1040
5.29.151.206	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	830
31.210.187.245	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	311
149.88.93.170	United States	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	107
109.67.177.176	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
41.105.39.66	Algeria	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
163.177.99.219	China	147.237.76.198	e.yohalan.idf.il	JIM_Purple_Con_Limit_Top	drop	1
71.6.216.35	United States	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
80.82.78.186	Netherlands	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1
163.177.99.219	China	147.237.76.86	navy.idf.il	JIM_Purple_Con_Limit_Top	drop	1
66.240.236.119	United States	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
93.186.16.154	South Africa	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	124
46.19.85.51	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
46.19.85.167	Israel	147.237.76.86	navy.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
77.126.144.88	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
79.179.190.125	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
149.88.171.82	United States	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
66.240.236.119	United States	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.179	e.mazi.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
66.240.236.119	United States	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.65	Israel	147.237.0.34	tikshuv.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.165.200	United States	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.76.196	e.sviva.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
66.240.192.138	United States	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.76.34	yochanan.idf.il	DVRep_B-N_60_100	Block	1
95.90.194.99	Germany	147.237.72.166	aka.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1
46.19.85.81	Israel	147.237.76.31	nakchal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.165.200	United States	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	1
89.138.63.125	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
66.240.236.119	United States	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.0.16	my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	1
98.139.135.199	United States	147.237.76.31	nakchal.idf.il	EgovRep_B-N_70-99	Block	1
84.108.42.214	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
71.6.165.200	United States	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	1
109.66.26.155	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.25.43.94	Germany	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	1

## Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	4
93.173.29.114	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
125.73.143.245	China	147.237.76.200	eitan.aka.idf.il	GPL SCAN nmap TCP	2
89.139.43.244	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	2
80.246.133.31	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
37.46.39.121	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
117.141.4.232	China	147.237.76.200	eitan.aka.idf.il	GPL SCAN nmap TCP	2
110.139.164.106	Indonesia	147.237.8.27	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
110.139.164.106	Indonesia	147.237.8.14	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
104.155.211.71		147.237.77.178	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
218.6.132.45	China	147.237.72.14	dover.idf.il(old)	ET SCAN NMAP -sS window 2048	1
218.6.132.45	China	147.237.72.14	dover.idf.il(old)	ET SCAN NMAP -f -sS	1
84.109.7.86	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
62.225.2.2	Germany	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
58.20.54.249	China	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
117.212.186.163	India	147.237.8.27	e.madim.atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
110.139.164.106	Indonesia	147.237.8.45	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
110.139.164.106	Indonesia	147.237.8.24	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
104.155.211.71		147.237.77.178	e.matpash.idf.il	ET SCAN NMAP -sS window 3072	1
221.7.135.55	China	147.237.76.200	eitan.aka.idf.il	GPL SCAN nmap TCP	1
94.230.86.163	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
218.6.132.45	China	147.237.72.14	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
201.239.118.143	Chile	147.237.76.200	eitan.aka.idf.il	ET SCAN NMAP -sS window 4096	1
174.48.143.155	United States	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
61.240.144.64	China	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
121.88.5.177	Korea, Republic of	147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
37.238.136.47	Iraq	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	153
212.179.46.21	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	151
93.173.12.174	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	65
176.12.148.168	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	50
79.179.52.208	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	32
149.78.154.69	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	26
109.65.18.137	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	26
66.87.116.44	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	21
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	20
79.178.39.77	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	18
39.58.200.235	Pakistan	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	14
176.228.169.158	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
66.249.78.159	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
79.179.211.250	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
79.183.99.68	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
109.253.130.109	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
54.72.73.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
80.246.140.111	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
186.158.141.252	Argentina	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5
65.55.210.151	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5
157.55.39.191	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5
132.3.29.78	United States	147.237.77.74	law.idf.il	First packet isn't SYN	drop	drop	5
109.64.202.212	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5
195.64.77.107	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5
41.33.231.86	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5
37.46.39.121	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5
80.179.118.131	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
46.19.85.243	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
109.66.150.217	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
62.225.2.2	Germany	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	4
95.86.89.130	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
39.58.200.235	Pakistan	147.237.77.216	dover.idf.i	Invalid ACK number	Bad TCP sequence	monitor	3
176.12.145.253	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3
212.179.46.19	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3
37.142.77.105	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3
157.55.39.136	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3
39.58.200.235	Pakistan	147.237.77.216	dover.idf.i	Invalid sequence number	Bad TCP sequence	monitor	3
79.177.33.46	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3
37.142.160.171	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3
31.168.126.158	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3
50.156.135.247	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3
188.234.36.62	Russian Federation	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3
157.55.39.204	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3
31.168.172.139	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3
146.115.71.149	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3
46.19.86.88	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3
84.26.33.126	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3
87.69.119.88	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
31.210.186.136	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
149.78.178.120	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	5
207.46.13.101	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	5
84.95.2.27	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	5
2.54.39.223	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
5.255.253.93	Russian Federation	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/mod	Block	4
157.55.39.107	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
2.52.33.207	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
157.55.39.137	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 157.55.39.137	Block	2
149.78.178.120	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/gyus	Block	2
87.68.8.204	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
157.55.39.137	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
62.225.2.2	Germany	147.237.72.166	aka.idf.il	Unknown Parameter ScriptManager1_HiddenField in www.aka.idf.il/main/kapatz/relativecontact.aspx	None	1
82.80.42.175	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/gyus/authenticationservice.aspx/getuserdetails	Block	1
37.26.148.182	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	1
188.138.17.205	France	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/	Block	1
157.55.39.191	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.191	Block	1
68.180.228.99	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/templates/shared/usercontrols/headerupper/	Block	1
157.55.39.81	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/captcha.ashx	Block	1
66.249.64.178	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
46.116.250.115	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
199.255.137.70	United States	147.237.77.176	matpash.idf.il	eMail Hoarding	Block	1
93.172.151.116	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https://www.aka.idf.il/	Block	1
79.178.50.140	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https://www.aka.idf.il/	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-17333-he/mmmmmmm=0b972cd6mmmmmm_0b972cd6	Block	1
66.249.73.229	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/938-he/hamaz.aspx	Block	1
149.78.178.120	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 149.78.178.120	Block	1
66.249.64.66	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/gyus/general.aspx	Block	1
84.94.70.203	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
37.142.86.140	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
195.242.218.133	Ukraine	147.237.72.156	anan.idf.il	Unauthorized URL Access to list.ips.gov.il/	Block	1
157.55.39.191	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-13387-en/dover.aspx forcerecrawl: 0	Block	1
68.180.229.51	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.229.51	Block	1
66.249.64.183	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1375-he/refuah.aspx	Block	1
46.120.66.63	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https://www.aka.idf.il/	Block	1
95.90.194.99	Germany	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
79.178.162.102	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https://www.aka.idf.il/	Block	1
180.76.6.16	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/idf_in_pictures/2003/november/15.stm	Block	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	1
157.55.39.137	United States	147.237.72.166	aka.idf.il	Unknown Parameter docId in www.aka.idf.il/shalishut/site/news.aspx	None	1
66.249.64.76	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.76	Block	1
199.255.137.70	United States	147.237.77.74	law.idf.il	E-mail collector robots 14	Block	1
42.3.203.219	Hong Kong	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 42.3.203.219	Block	1
157.55.39.192	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/history/darom.stm	Block	1
68.180.229.51	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/golani/gdudim.stm	Block	1
66.249.67.70	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/320-6277-he/patzar.aspx	Block	1
157.55.39.107	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 157.55.39.107	Block	1
50.156.135.247	United States	147.237.77.216	dover.idf.il	NULL Character in Method	Block	1
207.46.13.101	United States	147.237.72.166	aka.idf.il	Unknown Parameter 98160f90 in aka.idf.il/gyus/	None	1
109.253.156.194	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
79.179.31.218	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docId in www.aka.idf.il/main/sachar/faq.aspx	None	1