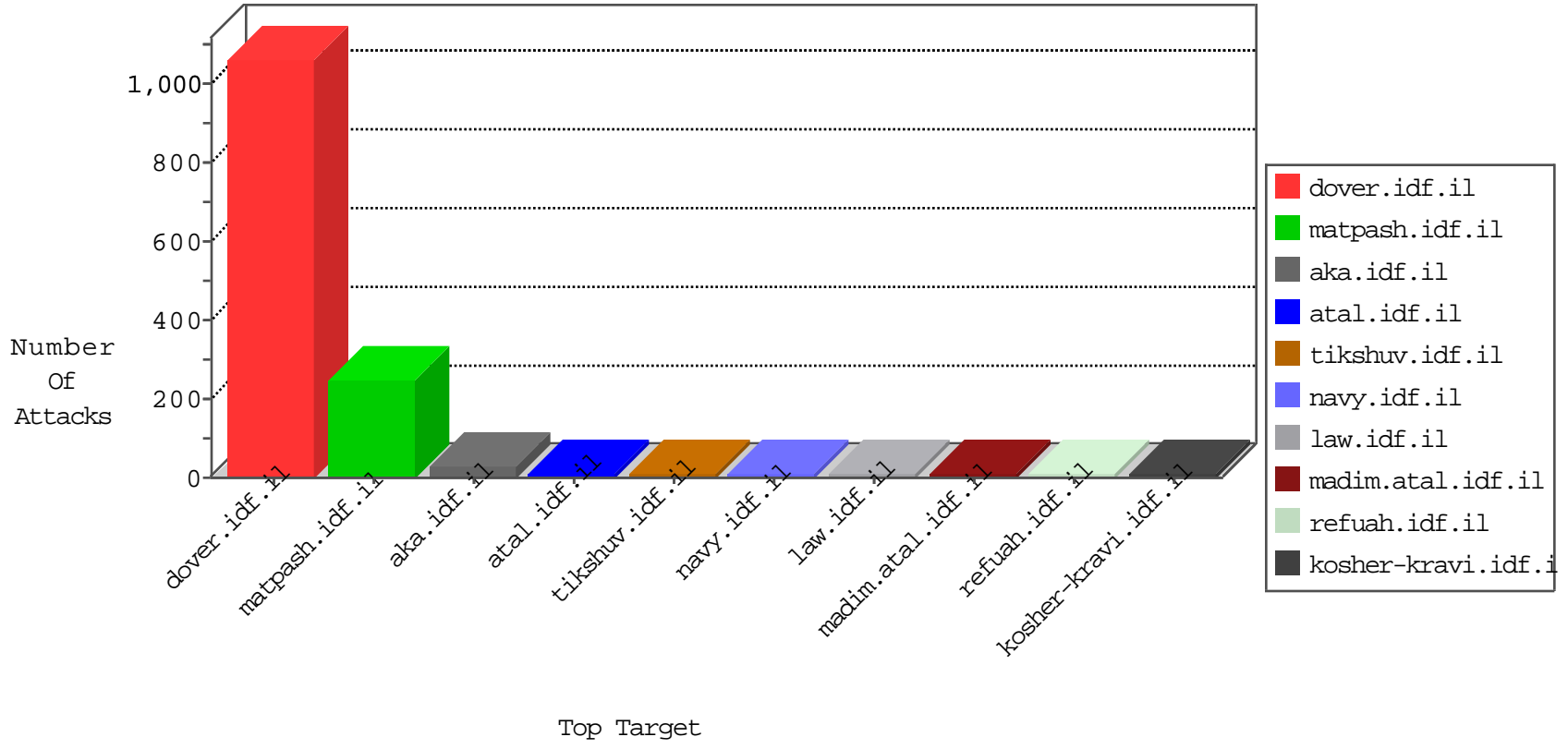
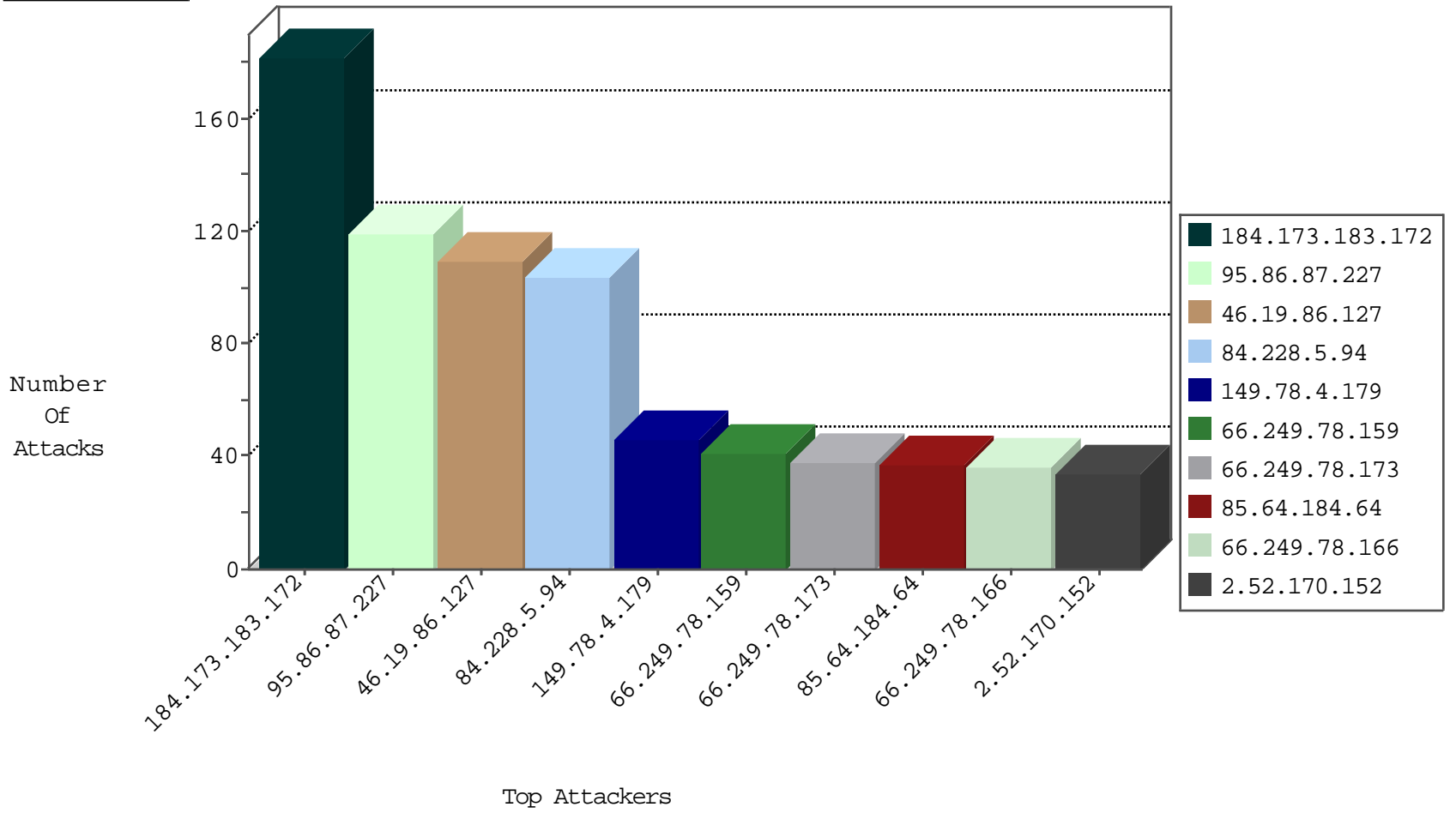




Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
220.181.108.186	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	196
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	8
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
71.6.167.142	United States	147.237.76.42	refuah.idf.il	Block_Ntp_All_Net	drop	1
146.185.239.100	Russian Federation	147.237.76.86	navy.idf.il	block-sp-trafl	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
184.173.183.172	United States	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	182
24.209.241.78	United States	147.237.0.15	kosher-kravi.idf.il	12348: HTTP: PHP-CGI Query String Parameter Command Injection Vulnerability	Block	4
24.209.241.78	United States	147.237.0.17	m.my-kosher-kravi.idf.il	12348: HTTP: PHP-CGI Query String Parameter Command Injection Vulnerability	Block	4
24.209.241.78	United States	147.237.0.19	madim.atal.idf.il	12348: HTTP: PHP-CGI Query String Parameter Command Injection Vulnerability	Block	4
71.6.167.142	United States	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.0.200	m4u.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
66.240.192.138	United States	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	1
24.209.241.78	United States	147.237.0.17	m.my-kosher-kravi.idf.il	0543: HTTP: php.cgi Access	Block	1
71.6.167.142	United States	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.0.16	my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.8.46	e.chimuch.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.76.39	mobile.meitav.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
66.240.236.119	United States	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	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	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	1
24.209.241.78	United States	147.237.0.19	madim.atal.idf.il	0543: HTTP: php.cgi Access	Block	1
71.6.167.142	United States	147.237.77.74	law.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
66.240.192.138	United States	147.237.77.227	e.haraz.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	1
24.209.241.78	United States	147.237.0.15	kosher-kravi.idf.il	0543: HTTP: php.cgi Access	Block	1
71.6.165.200	United States	147.237.77.227	e.haraz.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
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
66.249.78.133	United States	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sA (2)	2
66.249.67.81	United States	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sA (2)	2
91.224.132.118	Russian Federation	147.237.77.61	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.165	Japan	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
36.72.228.72	Indonesia	147.237.77.205	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.65	China	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.165	Japan	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
193.107.16.206	Russian Federation	147.237.72.166	aka.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
43.255.191.165	Japan	147.237.77.74	law.idf.il	ET SCAN Potential SSH Scan	1
193.0.200.132	Russian Federation	147.237.0.15	kosher-kravi.idf.il	ET WEB_SERVER Muieblackcat scanner	1
43.255.191.165	Japan	147.237.76.198	e.yochalan.idf.il	ET SCAN Potential SSH Scan	1
187.11.121.110	Brazil	147.237.8.50	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.165	Japan	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
125.39.116.219	China	147.237.76.176	test.ncore.idf.il	ET SCAN NMAP -sS window 4096	1
43.255.191.165	Japan	147.237.72.156	aman.idf.il	ET SCAN Potential SSH Scan	1
125.39.116.219	China	147.237.76.176	test.ncore.idf.il	ET SCAN NMAP -f -sS	1
43.255.191.165	Japan	147.237.0.200	m4u.idf.il	ET SCAN Potential SSH Scan	1
88.249.106.23	Turkey	147.237.8.24	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
36.72.228.72	Indonesia	147.237.77.205	prisha.idf.il	ET SCAN NMAP -sS window 2048	1
36.72.228.72	Indonesia	147.237.77.205	prisha.idf.il	ET SCAN NMAP -f -sS	1
61.240.144.65	China	147.237.8.45	e.eitan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
193.107.16.206	Russian Federation	147.237.72.166	aka.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.165	Japan	147.237.77.121	e.navy.idf.il	ET SCAN Potential SSH Scan	1
193.0.200.132	Russian Federation	147.237.0.19	madim.atal.idf.il	ET WEB_SERVER Muieblackcat scanner	1
43.255.191.165	Japan	147.237.77.19	law-forum.idf.il	ET SCAN Potential SSH Scan	1
187.11.121.110	Brazil	147.237.8.50	e.tikshuv.idf.il	ET SCAN NMAP -sS window 3072	1
43.255.191.165	Japan	147.237.76.44	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
176.103.49.29	Ukraine	147.237.77.243	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.165	Japan	147.237.76.31	nakchal.idf.il	ET SCAN Potential SSH Scan	1
125.39.116.219	China	147.237.76.176	test.ncore.idf.il	ET SCAN NMAP -sS window 2048	1
43.255.191.165	Japan	147.237.8.27	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
95.86.87.227	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	119
46.19.86.127	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	109
84.228.5.94	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	104
149.78.4.179	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	46
85.64.184.64	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	37
2.52.170.152	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	34
31.44.139.23	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	31
207.107.138.54	Canada	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	21
69.199.224.222	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	19
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	16
129.81.209.229	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	16
93.173.140.229	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	15
66.249.78.166	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	14
66.249.78.173	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	14
134.191.232.70	Israel	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	14
134.191.232.71	Israel	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
46.19.85.215	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	12
107.77.83.115	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11
66.249.78.166	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11
195.34.150.18	Austria	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
41.33.232.65	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
46.19.86.19	Israel	147.237.77.233	atal.idf.il	Invalid ACK number	Bad TCP sequence	monitor	7
66.249.78.159	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
66.249.78.173	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
199.30.25.204	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
91.66.162.63	Germany	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
37.140.141.39	Russian Federation	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
134.191.232.68	Israel	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
132.64.43.214	Israel	147.237.77.216	dover.idf.i	Invalid ACK number	Bad TCP sequence	monitor	6
134.191.232.69	Israel	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
132.64.43.214	Israel	147.237.77.216	dover.idf.i	Invalid sequence number	Bad TCP sequence	monitor	6
93.173.40.158	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5
84.109.113.161	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5
66.249.78.109	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5
66.249.78.95	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5
66.249.78.109	Israel	147.237.77.216	dover.idf.i	Invalid ACK number	Bad TCP sequence	alert	5
70.192.70.199	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5
66.249.78.109	Israel	147.237.77.216	dover.idf.i	Invalid ACK number	Bad TCP sequence	monitor	5
157.55.39.176	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5
52.16.5.197	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
46.19.85.7	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
199.76.66.200	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
66.249.78.159	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
199.168.151.86	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
46.19.85.3	Israel	147.237.77.216	dover.idf.i	Invalid ACK number	Bad TCP sequence	alert	4
79.161.92.176	Norway	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
66.249.78.109	Israel	147.237.77.216	dover.idf.i	Unexpected post SYN packet - RST or SYN expected	drop	drop	4
93.172.34.126	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
66.249.78.204	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 66.249.78.204	Block	22
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	17
66.249.78.197	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 66.249.78.197	Block	17
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	17
66.249.78.190	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 66.249.78.190	Block	16
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	11
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	6
157.55.39.92	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
157.55.39.178	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
93.173.153.125	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	3
66.249.78.140	Israel	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized URL Access on tikshuv.idf.il/main/giyus/general.aspx	Block	2
38.121.100.67	United States	147.237.77.176	matpash.idf.il	PHP Attempt	Block	2
66.249.78.147	Israel	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized URL Access on tikshuv.idf.il/main/giyus/general.aspx	Block	2
66.249.75.5	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
66.249.75.5	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docI.. in www.aka.idf.il/main/giyus/general.aspx	None	1
66.249.64.240	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-8579-he/dover.aspx	Block	1
66.249.64.10	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/320-6353-he/patzar.aspx	Block	1
193.0.200.132	Russian Federation	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/muieblackcat	Block	1
66.249.75.117	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/misrot.aspx	Block	1
66.249.69.28	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
66.249.64.130	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/idkonim/pages/30012011masaiyot.aspx	Block	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-he/dover.aspx	Block	1
185.56.11.190		147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/+@web.de&as_gdr=all&filter=0&num=100&complete=0&cr=countrysl&gws_rd=ssl&hl=iw&&ct=clnk	Block	1
157.55.39.137	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.75.34	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/eitan/pratim/pirteychayal/	Block	1
66.249.67.65	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1014-he/atal.aspx	Block	1
66.249.64.12	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/163-5247-he/patzar.aspx	Block	1
199.30.25.248	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.140	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/main/drushim/general.aspx	Block	1
157.55.39.182	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/320/patzar.aspx	Block	1
66.249.78.20	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/	Block	1
66.249.69.78	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
103.245.44.14	India	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	Block	1
66.249.64.224	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 66.249.64.224	Block	1
66.249.78.102	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19009-he/dover.aspx	Block	1
54.186.248.49	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-he/www.idf.il	Block	1
188.165.15.195	France	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
157.55.39.158	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
66.249.75.42	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/miluum/	Block	1
77.237.138.202	Czech Republic	147.237.77.235	sviva.idf.il	Unauthorized URL Access to /	Block	1
66.249.67.81	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/m/	Block	1
66.249.64.66	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/993/patzar.aspx	Block	1
207.46.13.19	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/captcha.ashx	Block	1
66.249.78.73	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
157.55.39.191	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.191	Block	1
109.253.129.177	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
66.249.64.224	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/idkonim/pages/jhgjg.aspx	Block	1
66.249.78.109	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1153-he/dover.aspx	Block	1
66.199.231.242	United States	147.237.72.166	aka.idf.il	Unknown Parameter pop in www.aka.idf.il/main/home/	None	1
188.234.0.32	Russian Federation	147.237.77.170	maarachot.idf.il	Unknown HTTP Request Method COOK in URL maarachot.idf.il/71828-he/maarachot.aspx	Block	1