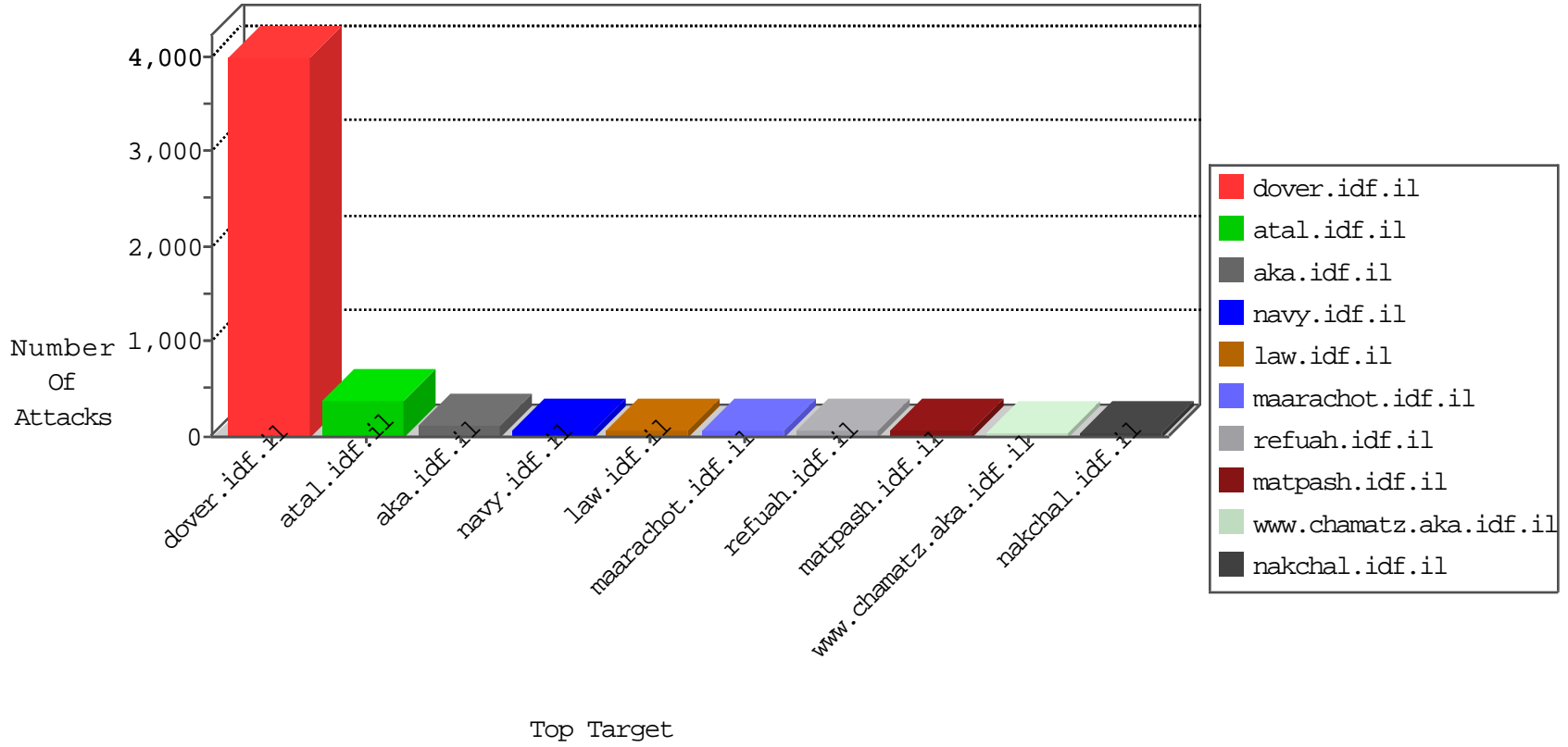
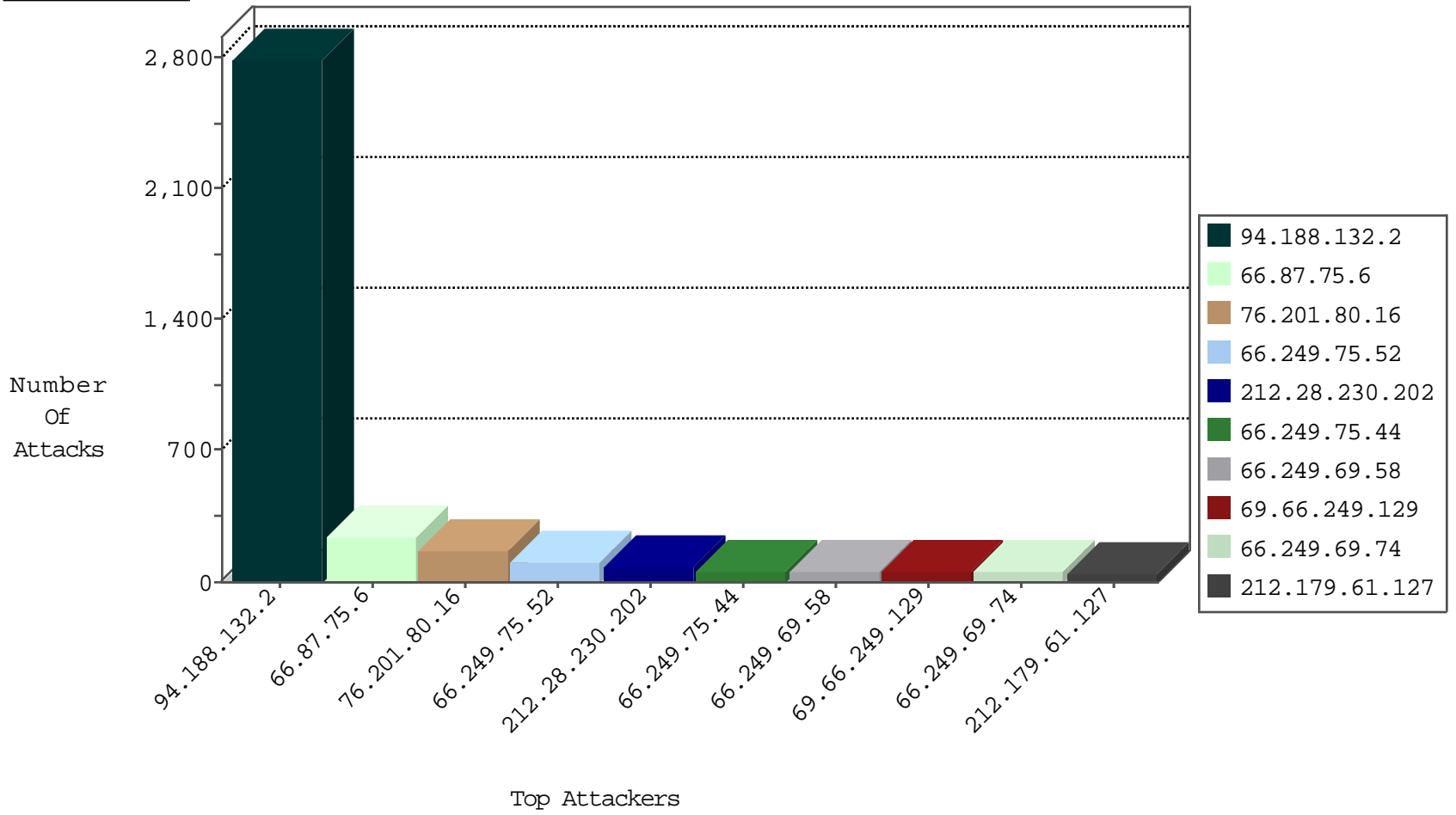


Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
2.54.130.188	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	228
120.60.12.211	India	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	192
66.249.75.52	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	103
76.201.80.16	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	103
66.249.75.44	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	61
66.249.69.58	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	60
66.249.69.74	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	53
66.249.69.66	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	47
66.249.75.60	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	42
66.249.67.14	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	32
66.249.78.159	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	28
66.249.78.166	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	23
66.249.67.22	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	23
66.249.64.121	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	23
66.249.64.129	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	22
66.249.78.97	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	22
66.249.78.111	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	21
66.249.78.254	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	20
66.249.67.84	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	19
66.249.64.146	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ip_Web_In	drop	19
66.249.67.13	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	18
66.249.78.104	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	17
66.249.67.21	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	17
66.249.78.173	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	15
66.249.67.92	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	14
66.249.78.2	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	14
66.249.78.153	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	12
66.249.67.76	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	12
66.249.67.5	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	11
66.249.64.154	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ip_Web_In	drop	11
66.249.64.125	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	10
66.249.67.108	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	9
5.102.254.148	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	9
66.249.64.150	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ip_Web_In	drop	9
66.249.67.30	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	9
66.249.78.160	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	9
66.249.78.9	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	8
66.249.78.146	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	8
66.249.67.116	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	8
66.249.78.148	United States	147.237.72.156	aman.idf.il	Block_Ip_Web_In	drop	7
66.249.78.61	United States	147.237.0.15	kosher-kravi.idf.il	Block_Ip_Web_In	drop	6
66.249.64.169	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	5
66.249.67.100	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	5
66.249.64.46	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	4
66.249.64.150	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	4
66.249.83.182	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	4
66.249.67.131	United States	147.237.76.31	nakchal.idf.il	Block_Ip_Web_In	drop	4
66.249.78.76	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	4
66.249.67.51	United States	147.237.76.31	nakchal.idf.il	Block_Ip_Web_In	drop	4
66.249.78.141	United States	147.237.72.156	aman.idf.il	Block_Ip_Web_In	drop	4

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	24
89.138.57.123	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	7
37.236.41.169	Iraq	147.237.77.176	matpash.idf.il	14170: HTTP: Blank User-Agent (descriptor but no string)	Block	3
89.139.185.104	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
212.28.230.202	Lebanon	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
91.200.12.28	Ukraine	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	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
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
198.13.107.107	United States	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.161	Japan	147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	China	147.237.76.177	ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
43.255.191.161	Japan	147.237.72.166	aka.idf.il	ET SCAN Potential SSH Scan	1
198.13.107.107	United States	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	China	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
43.255.191.161	Japan	147.237.0.200	m4u.idf.il	ET SCAN Potential SSH Scan	1
193.107.17.72	Russian Federation	147.237.8.24	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	China	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
171.111.158.210	China	147.237.76.200	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	China	147.237.0.35	akaws.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
171.111.158.210	China	147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
58.20.54.249	China	147.237.77.61	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
104.128.144.130		147.237.76.202	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.161	Japan	147.237.77.233	atal.idf.il	ET SCAN Potential SSH Scan	1
198.13.107.107	United States	147.237.76.200	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.67	China	147.237.76.200	eitan.aka.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
198.13.107.107	United States	147.237.76.176	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.161	Japan	147.237.76.201	e.atal.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	China	147.237.77.235	sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
198.13.107.107	United States	147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.161	Japan	147.237.76.86	navy.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	China	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
198.13.107.107	United States	147.237.76.31	nakchal.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.161	Japan	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	China	147.237.76.176	test.ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
43.255.191.161	Japan	147.237.8.46	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	China	147.237.76.86	navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
183.136.216.7	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	China	147.237.8.46	e.chinuch.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
171.111.158.210	China	147.237.76.86	navy.idf.il	ET SCAN Potential SSH Scan	1
58.20.54.249	China	147.237.77.74	law.idf.il	ET SCAN NMAP -sS window 1024	1
171.111.158.210	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
58.20.54.249	China	147.237.76.198	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
211.155.16.154	China	147.237.0.19	madim.atal.idf.il	GPL SCAN nmap TCP	1
198.13.107.107	United States	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.161	Japan	147.237.77.121	e.navy.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.67	China	147.237.8.28	e.mobile-ks.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
198.13.107.107	United States	147.237.76.148	ggcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.161	Japan	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	China	147.237.77.234	halag.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
94.188.132.2	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2791
66.87.75.6	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	244
76.201.80.16	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	157
212.28.230.202	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	80
212.179.61.127	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	48
69.66.249.129	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	48
50.100.251.66	Canada	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	40
212.76.127.111	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	29
96.20.176.223	Canada	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	23
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	21
212.179.23.22	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
89.138.67.88	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
108.59.253.71	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
85.65.20.15	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
87.68.81.17	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
213.57.229.70	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
37.26.147.213	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
45.64.237.12		147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
70.199.76.32	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
82.80.25.221	Israel	147.237.77.216	dover.idf.il	SAM rule	drop	drop	7
94.159.158.110	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
91.200.12.28	Ukraine	147.237.77.216	dover.idf.il	SAM rule	drop	drop	6
194.90.119.162	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
62.90.255.10	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
82.102.141.253	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
190.181.201.93	Honduras	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
46.19.86.237	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
93.168.248.246	Romania	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
176.12.140.152	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
162.205.78.141	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
176.12.149.142	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
66.61.7.196	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
192.249.64.249	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
46.19.86.142	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
71.59.249.54	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
68.180.228.117	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
79.179.139.167	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
85.72.40.4	Greece	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
79.183.5.45	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
46.19.85.40	Israel	147.237.76.31	nakchal.idf.i	SAM rule	drop	drop	4
77.125.163.240	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
212.76.127.44	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
82.80.25.221	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
46.121.65.142	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
46.19.85.40	Israel	147.237.77.216	dover.idf.il	SAM rule	drop	drop	3

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
207.46.13.79	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/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
46.19.85.134	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	2
207.46.13.5	United States	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	1
68.180.228.232	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/miluum/templates/http://www.aka.idf.il/sip_storage/files/6/66556.pdf	Block	1
37.142.224.61	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/forgotpassword.aspx	None	1
157.55.39.136	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/iturim/asp/list.asp	Block	1
62.90.10.14	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00\$ctl100\$cphMain\$cphSachar\$btnSubmit.x in www.aka.idf.il/main/sachar/	None	1
193.47.165.251	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/scripts/css3pie.htc	Block	1
62.210.114.129	France	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/sip_storage/files/8/3198.pdf/trackback/	Block	1
31.44.134.167	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	1
79.178.155.71	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/payslips.aspx	None	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
193.201.224.176	Ukraine	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 193.201.224.176	Block	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.117	Block	1
31.184.195.166	Russian Federation	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
157.55.39.67	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
54.245.64.111	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-he	Block	1
193.201.224.176	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.stm	Block	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/jenin/site/english/main_index.stm	Block	1
31.193.51.84	France	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
157.55.39.136	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
62.90.10.14	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/home.aspx	None	1