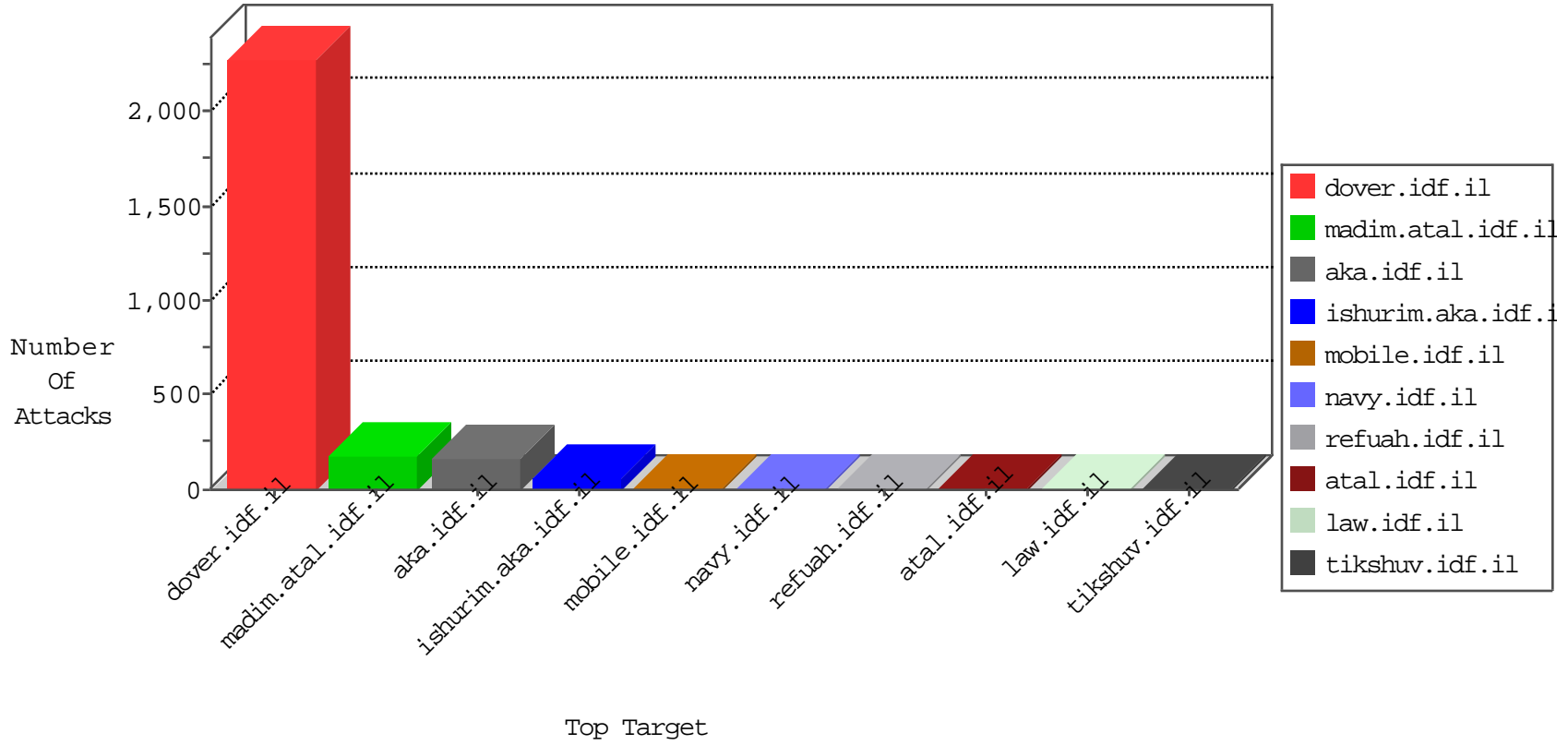
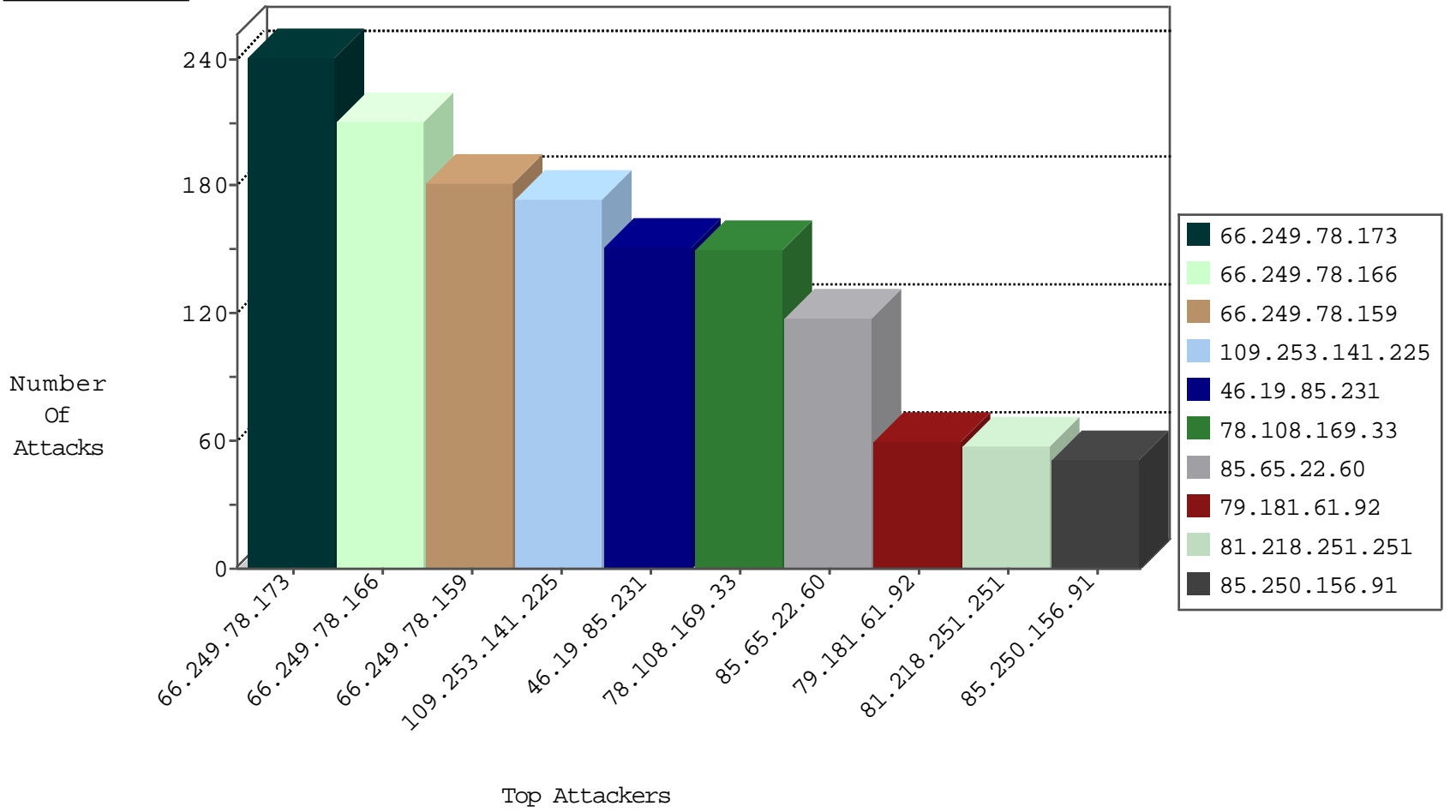


Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.64.68	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	692
46.117.232.243	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	466
2.52.174.28	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	65
83.130.115.213	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
93.173.242.136	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
79.179.184.188	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	4
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	4
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	4
139.228.174.38	Indonesia	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
124.244.155.187	Hong Kong	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	2
157.55.39.92	United States	147.237.72.166	aka.idf.il	HTTP-Misc-BadBlue-Dir-Trave-2	dest-reset	1
109.66.135.198	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
79.178.134.145	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
177.67.137.205	Brazil	147.237.8.14	e.orchot.idf.il	JIM_Purple_Con_Limit_Http	drop	1
124.78.233.157	China	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1
139.228.174.38	Indonesia	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
98.116.241.10	United States	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
58.62.118.101	China	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1
146.185.239.100	Russian Federation	147.237.72.166	aka.idf.il	block-sp-trafl	drop	1
107.154.64.10	United States	147.237.77.170	maarachot.idf.il	I4 Source or Dest Port Zero	drop	1
132.70.66.14	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
85.25.103.50	Germany	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	2
71.6.167.142	United States	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	1
82.102.169.113	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.165.200	United States	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	1
31.7.57.198	Switzerland	147.237.72.156	aran.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	1
84.228.14.235	Israel	147.237.77.170	maarachot.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.165.200	United States	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	1
31.7.57.198	Switzerland	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	1
31.7.57.198	Switzerland	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	1
31.7.57.198	Switzerland	147.237.0.17	m.ny-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.0.17	m.ny-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
95.86.124.155	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
71.6.167.142	United States	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	1
31.7.57.198	Switzerland	147.237.0.33	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
66.249.67.132	United States	147.237.77.233	atal.idf.il	ET SCAN NMAP -sA (2)	2
79.183.177.107	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.78.147	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	2
81.218.251.252	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
79.181.203.126	Israel	147.237.72.156	aman.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	1
66.249.78.134	United States	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	1
213.210.205.2	Saudi Arabia	147.237.76.201	e.atal.idf.il	ET SCAN NMAP -sS window 4096	1
199.231.185.135	United States	147.237.8.50	e.tikshuv.idf.il	ET SCAN NMAP -sS window 2048	1
61.240.144.65	China	147.237.77.212	e.dover.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.168	Japan	147.237.77.233	atal.idf.il	ET SCAN Potential SSH Scan	1
177.67.137.205	Brazil	147.237.0.17	m.my-kosher-kravi.idf.il	SERVER-APACHE Apache Tomcat Web Application Manager access	1
43.255.191.168	Japan	147.237.77.179	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
111.161.71.206	China	147.237.77.216	dover.idf.il	ET SCAN NMAP -sS window 4096	1
43.255.191.168	Japan	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
82.117.208.243		147.237.0.200	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.168	Japan	147.237.0.33	idf.il	ET SCAN Potential SSH Scan	1
31.7.57.198	Switzerland	147.237.0.33	idf.il	ET SCAN NMAP -sS window 1024	1
218.77.79.43	China	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
66.249.78.127	United States	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	1
199.231.185.135	United States	147.237.8.50	e.tikshuv.idf.il	ET SCAN NMAP -sS window 3072	1
64.76.71.18	Peru	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 3072	1
199.231.185.135	United States	147.237.8.50	e.tikshuv.idf.il	ET SCAN NMAP -f -sS	1
61.240.144.65	China	147.237.77.179	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
177.67.137.205	Brazil	147.237.0.19	madim.atal.idf.il	SERVER-APACHE Apache Tomcat Web Application Manager access	1
43.255.191.168	Japan	147.237.77.205	prisha.idf.il	ET SCAN Potential SSH Scan	1
128.136.227.196	United States	147.237.77.234	halag.idf.il	ET SCAN NMAP -sS window 4096	1
43.255.191.168	Japan	147.237.76.201	e.atal.idf.il	ET SCAN Potential SSH Scan	1
92.47.29.12	Kazakistan	147.237.0.33	idf.il	ET SCAN Potential SSH Scan	1
43.255.191.168	Japan	147.237.8.24	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
31.7.57.198	Switzerland	147.237.72.167	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
46.19.85.231	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	150
78.108.169.33	Lebanon	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	150
85.65.22.60	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	118
66.249.78.173	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	83
66.249.78.166	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	62
66.249.78.159	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	61
79.181.61.92	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	60
81.218.251.251	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	58
85.250.156.91	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	51
66.249.78.173	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	40
66.249.78.173	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	39
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	36
66.249.78.166	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	34
157.55.39.26	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	31
79.177.62.48	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	28
93.172.163.187	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	28
157.55.39.191	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	27
83.130.115.213	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	24
85.65.244.190	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	24
66.249.78.159	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	23
46.116.158.90	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	22
5.102.254.0	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	22
66.249.78.166	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	22
109.253.135.245	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	21
84.228.6.86	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	21
220.233.116.246	Australia	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	20
66.249.78.159	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	20
66.249.64.76	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	17
84.228.128.226	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	16
66.249.64.72	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	15
185.32.178.152	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	15
66.249.64.74	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	15
46.19.85.161	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	14
157.55.39.13	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
46.19.85.183	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
54.72.73.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
37.26.148.253	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
157.55.39.176	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
212.199.182.150	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11
180.191.224.245	Philippines	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11
52.16.5.197	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11
41.33.231.86	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
149.78.154.69	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
213.57.202.111	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	10
46.116.87.94	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	10
46.19.86.38	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
93.172.34.126	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
93.173.242.136	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
54.72.0.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
109.253.141.225	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	164
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	77
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	71
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	62
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal/izkor/view_imgtop.asp	Block	27
157.55.39.92	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	12
66.249.64.74	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.74	Block	9
66.249.64.72	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.72	Block	8
178.137.19.143	Ukraine	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/901-11442-en/	Block	5
157.55.39.106	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	5
66.249.64.76	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.76	Block	5
66.249.64.4	Israel	147.237.77.74	law.idf.il	Distributed Illegal Parameter Encoding	None	4
157.55.39.178	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
74.4.183.17	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	3
66.249.64.76	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal/izkor/view_imgtop.asp	Block	3
77.127.126.199	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	3
46.19.85.31	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
157.55.39.92	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/sachar/forms/downloadform.asp	Block	3
66.249.64.74	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal/izkor/view_imgtop.asp	Block	3
5.28.166.246	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	2
188.143.232.14	Russian Federation	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 188.143.232.14	Block	2
157.55.39.91	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
157.55.39.138	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
66.249.64.72	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal/izkor/view_imgtop.asp	Block	2
66.249.64.2	Israel	147.237.77.74	law.idf.il	Distributed Illegal Parameter Encoding	None	2
176.12.150.183	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/webresource.axd	Block	2
142.54.161.131	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-17055-en/dover.aspx/trackback/	Block	1
66.249.67.57	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1000-he/atal.aspx	Block	1
185.53.44.95		147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/kamlar/eurl.axd/928b5cf9a6471a47995ba48bd1ecf317/	Block	1
82.80.79.50	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
66.249.64.12	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/531-he/patzar.aspx	Block	1
185.32.178.152	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
157.55.39.178	United States	147.237.72.166	aka.idf.il	Unknown Parameter docId in www.aka.idf.il/shalishut/site/faq.aspx	None	1
66.249.69.42	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
185.53.44.90		147.237.72.166	aka.idf.il	Unknown Parameter catId in www.aka.idf.il/patzar/klali/	None	1
87.230.26.123	Germany	147.237.0.34	tikshuv.idf.il	PHP Attempt	Block	1
52.16.20.161	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
177.67.137.205	Brazil	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/manager/html	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
207.46.13.108	United States	147.237.77.226	www.chamatz.aka.idf.il	Distributed Unauthorized URL Access on 147.237.77.226//	Block	1
149.78.154.69	United States	147.237.77.216	dover.idf.il	Illegal Byte Code Character in URL /1153-21973-he/dover.aspx[[#15]][[#3]]5	Block	1
66.249.67.65	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
185.53.44.96		147.237.72.166	aka.idf.il	Unknown Parameter docId in www.aka.idf.il/chinuch/home/	None	1
185.53.44.61		147.237.72.166	aka.idf.il	Unknown Parameter docId in www.aka.idf.il/chinuch/klali/	None	1
84.228.1.221	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.19.85.27	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233//1134-he/atal.aspx	Block	1
157.55.39.179	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
66.249.75.13	Israel	147.237.72.166	aka.idf.il	Unknown Parameter c... in www.aka.idf.il/miluum/templates/inner.asp	None	1
188.143.232.14	Russian Federation	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/900-he/	Block	1