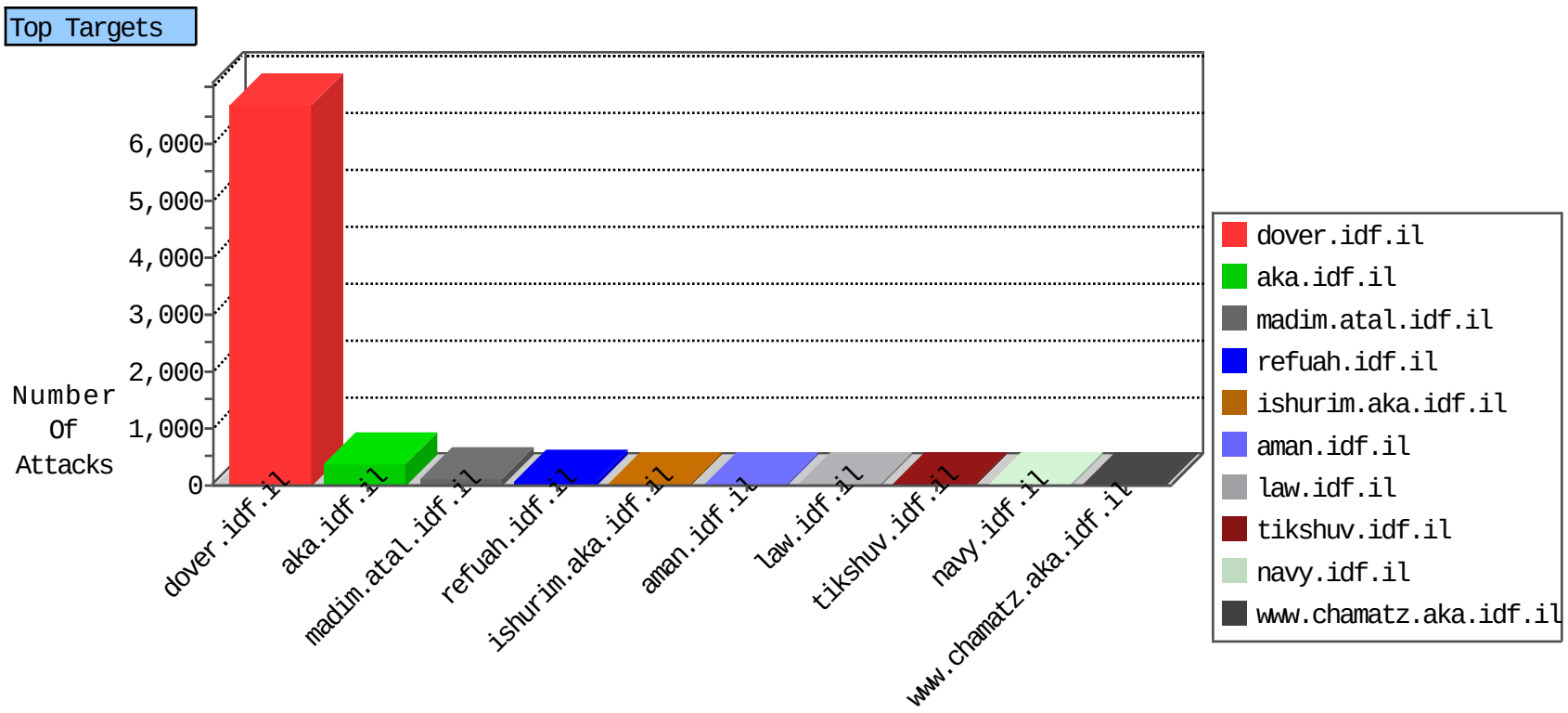
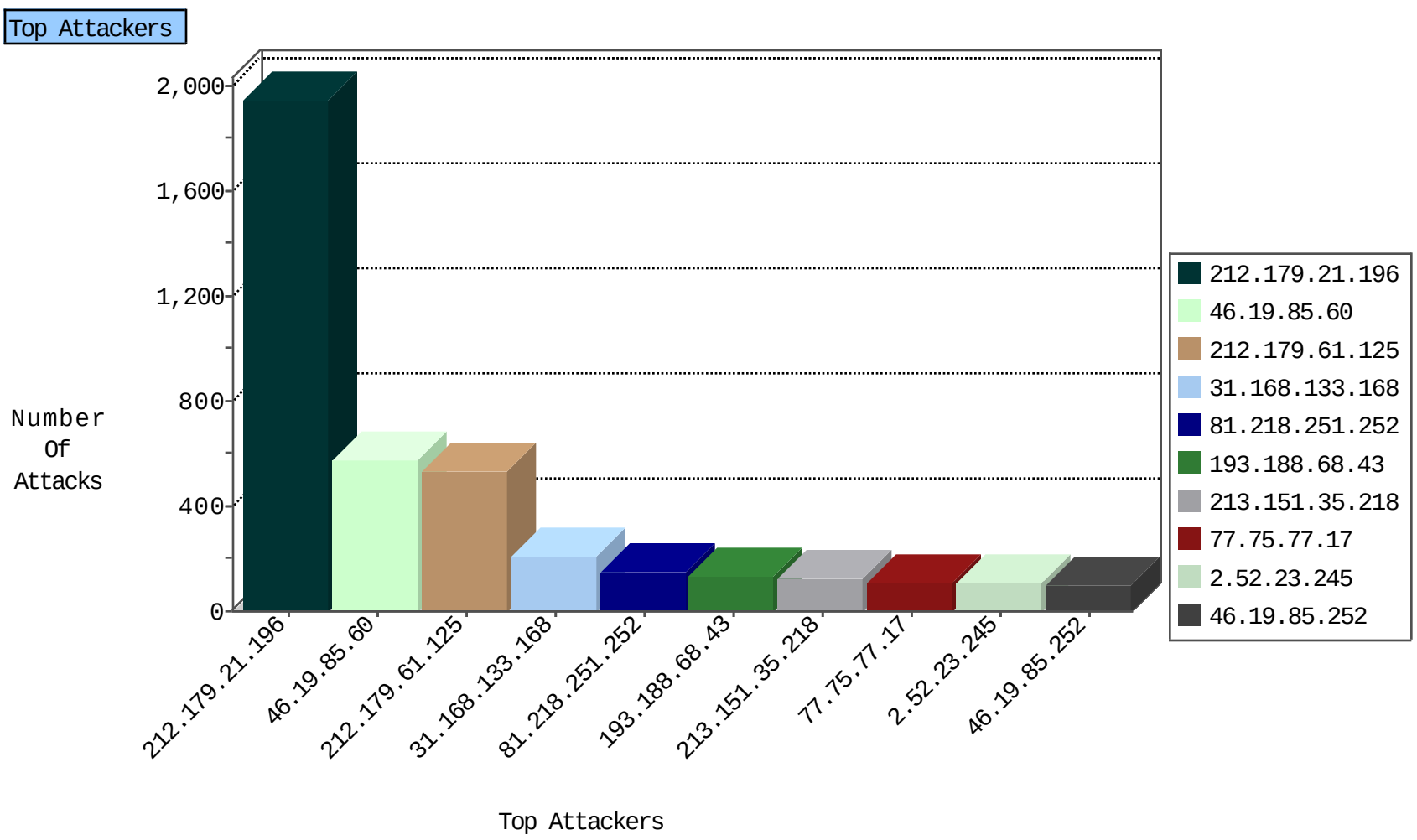
04-27-2015-12:03:00 to 04-27-2015-13:03:00

IDF Under Attack
04-27-2015-12:03:00





04-27-2015-12:03:00 to 04-27-2015-13:03:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
31.168.103.115	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	298
192.115.116.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	218
89.138.2.187	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	116
91.231.193.150	Israel	147.237.76.42	refuah.idf.il	JLM_Purple_Con_Limit_Http	drop	82
91.231.193.150	Israel	147.237.76.42	refuah.idf.il	JLM_Purple_Con_Limit_Tcp	drop	32
192.114.2.38	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	24
91.199.69.254	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	14
46.19.85.52	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	7
109.64.112.208	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
46.116.241.192	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
84.94.197.241	Israel	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
62.90.159.206	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
66.249.69.43	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
132.68.1.231	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
147.236.238.250	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
31.168.242.117	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
109.186.17.125	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
84.108.111.66	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
87.68.58.65	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
46.19.86.199	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
195.37.190.86	Germany	147.237.76.38	e.e.meitav.idf.il	Block_Ntp_All_Net	drop	1

04-27-2015-12:03:00 to 04-27-2015-13:03:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
94.230.86.214	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	7
37.46.41.84	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
46.19.85.79	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
46.116.211.238	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
66.240.192.138	United States	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	2
213.57.55.230	Israel	147.237.77.74	law.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
62.219.141.71	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
66.240.236.119	United States	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	2
79.182.25.111	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
66.240.192.138	United States	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	1
2.52.28.7	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	147.237.77.212	e.dover.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
85.25.103.50	Germany	147.237.0.16	my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
37.205.9.131	Slovakia	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	1
80.178.11.217	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
66.240.192.138	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
62.90.8.145	Israel	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	147.237.72.156	aman.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
31.7.57.198	Switzerland	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
37.205.9.131	Slovakia	147.237.72.166	aka.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
66.240.236.119	United States	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	1
84.109.160.91	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.167.142	United States	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	1
31.7.57.198	Switzerland	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	1
85.64.123.101	Israel	147.237.77.74	law.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.167.142	United States	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
220.181.125.15	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
71.6.165.200	United States	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	1
193.164.156.110	France	147.237.77.170	maarachot.idf.il	12348: HTTP: PHP-CGI Query String Parameter Command Injection Vulnerability	Block	1

04-27-2015-12:03:00 to 04-27-2015-13:03:00

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	2
149.78.137.30	United States	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
87.68.84.56	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
79.177.11.41	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
59.41.39.125	China	147.237.8.28	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 2048	1
46.120.23.43	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
218.6.132.45	China	147.237.77.227	e.hamaz.idf.il	ET SCAN NMAP -sS window 3072	1
185.32.178.228	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
91.199.69.254	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
84.228.135.133	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	1
61.160.224.130	China	147.237.72.166	aka.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
59.41.39.125	China	147.237.8.28	e.mobile-ks.idf.il	ET SCAN NMAP -f -sS	1
37.46.41.84	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1

04-27-2015-12:03:00 to 04-27-2015-13:03:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
212.179.21.196	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1945
46.19.85.60	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	574
212.179.61.125	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	534
31.168.133.168	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	210
81.218.251.252	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	147
193.188.68.43	Jordan	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	132
213.151.35.218	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	127
77.75.77.17	Czech Republic	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	106
46.19.85.252	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	99
130.226.237.4	Denmark	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	74
79.177.171.142	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	73
66.249.69.40	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	64
37.231.167.148	Kuwait	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	55
46.19.86.2	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	51
66.249.69.48	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	48
128.177.108.218	United States	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	48
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	41
176.12.151.70	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	41
66.249.69.32	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	40
109.64.97.230	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	35
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	32
66.249.69.48	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	31
84.94.197.241	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	31
212.199.10.60	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	28
81.218.131.82	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	27
95.86.91.139	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	25
80.246.133.233	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	25
138.134.192.10	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	25
192.114.105.254	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	22
46.19.85.79	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	22
168.63.139.43	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	22
207.46.13.52	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	22
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	22
41.33.232.65	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	22
192.114.105.254	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	21
194.56.215.66	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	21
147.236.238.75	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
46.116.211.238	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
207.46.13.1	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
2.54.146.222	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
176.12.140.112	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	19
66.249.69.40	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	19
46.19.85.96	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
84.94.119.22	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
66.249.75.66	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
80.178.147.220	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
66.249.69.32	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
176.12.150.110	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
2.52.23.245	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	105
79.183.58.9	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	9
46.116.65.24	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//www.tikshuv.idf.il	Block	7
213.8.52.149	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	4
109.253.136.66	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	4
212.179.102.167	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/9/	Block	3
77.127.190.156	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
212.235.98.139	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	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
79.180.133.238	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/gius	Block	2
212.179.132.204	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	2
81.218.76.25	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
77.127.241.234	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
79.181.141.51	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
81.218.118.124	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.117.25.198	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
192.88.162.1	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
79.178.168.36	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
31.13.100.114	Ireland	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage/files/6	Block	1
157.55.39.178	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 157.55.39.178	Block	1
109.64.202.212	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.78.80	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/	Block	1
202.112.50.77	China	147.237.77.216	dover.idf.il	Unknown HTTP Request Method quit in URL	Block	1
84.111.216.173	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
66.249.64.68	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
46.19.85.53	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
176.12.149.128	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
66.249.78.125	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/261-5611-he/patzar.aspx	Block	1
2.54.3.241	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/kamlar/styles/import/bottomnavigaton.asp	Block	1
157.55.39.5	United States	147.237.72.166	aka.idf.il	Unknown Parameter docId in www.aka.idf.il/shalishut/site/gallery.aspx	None	1
66.249.69.69	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/search/results.aspx	Block	1
212.150.209.205	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/login.aspx?moduletogoto=0	Block	1
94.230.84.152	Israel	147.237.72.166	aka.idf.il	Redundant HTTP Headers Referer	Block	1
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Unknown Parameter wb48617274 in www.aka.idf.il/chinuch/faq/default.asp	None	1
46.117.161.91	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
195.160.240.11	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
173.252.115.88	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage/files/8	Block	1
79.180.133.238	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
31.186.228.62	United Kingdom	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.65.7.185	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/scripts/css3pie.htc	Block	1
66.249.78.82	Israel	147.237.77.74	law.idf.il	Illegal Parameter Encoding searchText in www.law.idf.il/275-he/patzar.aspx	None	1
213.8.52.148	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.69.2	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
207.46.13.1	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-he/×¦×″	Block	1
91.200.12.74	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-11845-en/dover.aspx/trackback/	Block	1
46.19.85.253	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
178.134.237.19	Georgia	147.237.77.74	law.idf.il	Unknown HTTP Request Method COOK in URL www.law.idf.il/14-en/patzar.aspx	Block	1
80.178.169.176	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
2.54.35.75	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
157.55.39.6	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1