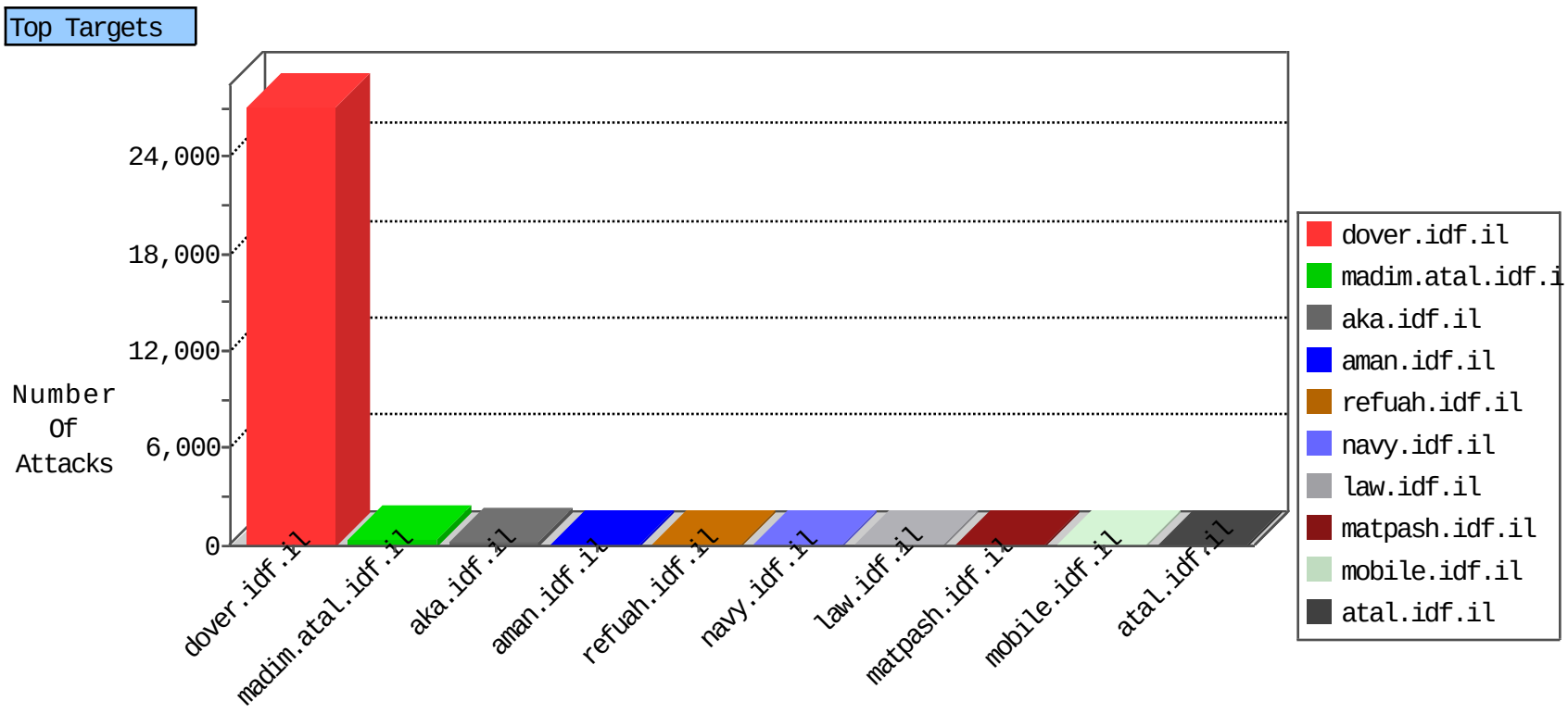
04-16-2015-16:03:08 to 04-16-2015-17:03:08

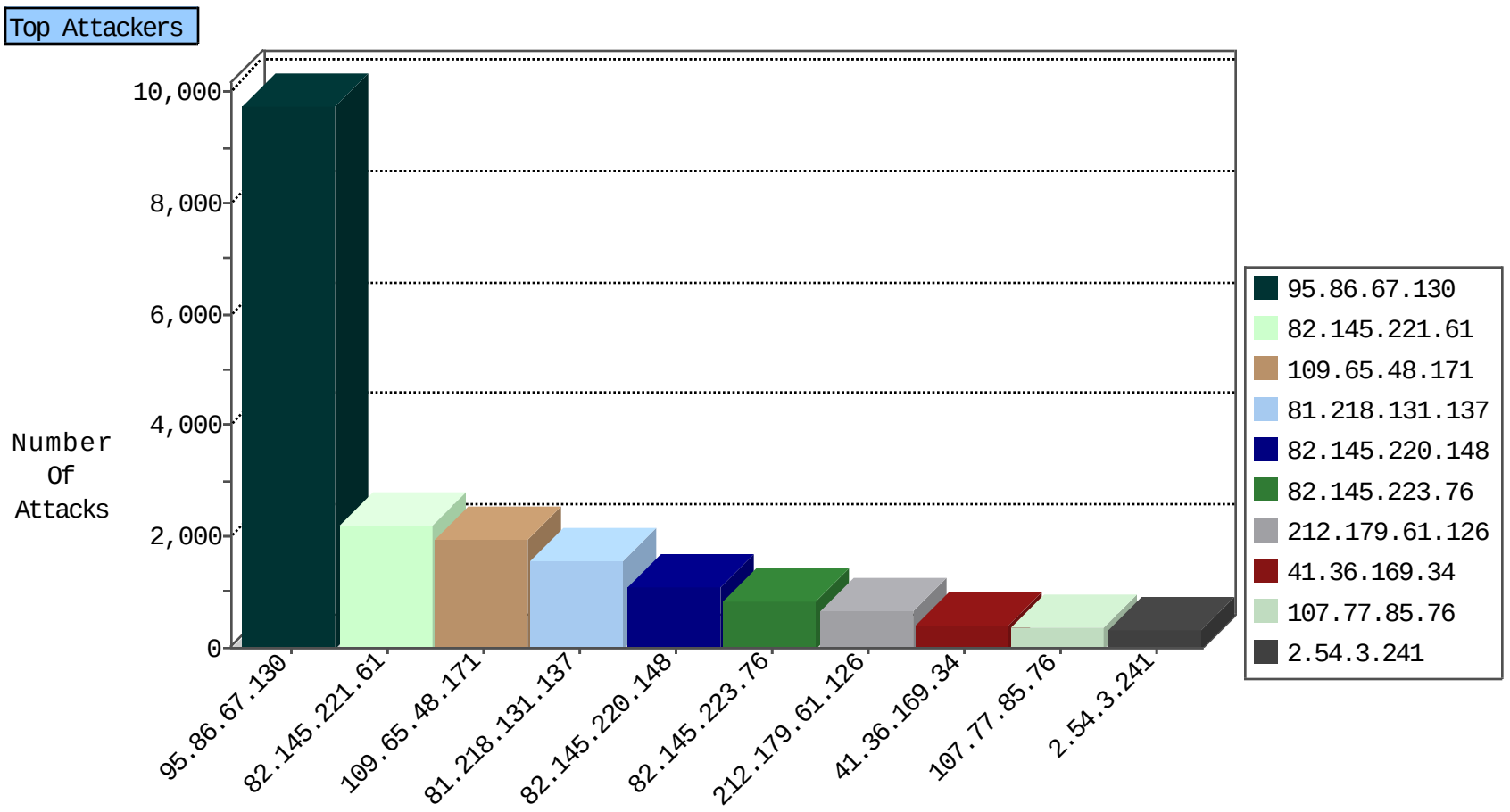
IDF Under Attack
04-16-2015-16:03:08

Top Targets



Top Target

Top Attackers



Top Attackers

04-16-2015-16:03:08 to 04-16-2015-17:03:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
84.229.30.43	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	255
89.139.52.13	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	241
77.127.2.103	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	153
46.116.170.154	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	106
79.183.116.179	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	92
197.130.207.132	Morocco	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	62
54.72.0.55	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	62
82.145.221.61	Europe	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	10
196.204.80.120	Egypt	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7
176.106.46.79	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
24.16.43.47	United States	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	3
41.69.143.7	Egypt	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
207.46.13.1	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
124.232.142.220	China	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1
41.36.169.34	Egypt	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
197.163.38.11	Egypt	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
94.96.0.234	Saudi Arabia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
72.18.133.66	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
84.94.149.46	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
197.202.220.219	Algeria	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
109.66.174.248	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
206.223.175.232	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
121.54.44.88	Philippines	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1

04-16-2015-16:03:08 to 04-16-2015-17:03:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
85.250.117.50	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
109.66.99.98	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
5.29.132.157	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
46.117.8.125	Israel	147.237.76.30	himush.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
77.56.26.69	Switzerland	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
188.138.9.50	Germany	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	2
79.180.164.246	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
71.6.165.200	United States	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	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	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	1
185.32.179.243	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
27.84.201.161	Japan	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	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.0.19	madim.atal.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
31.154.7.4	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.135.131	United States	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	1
89.139.24.250	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	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	1
37.26.147.198	Israel	147.237.77.216	dover.idf.il	14170: HTTP: Blank User-Agent (descriptor but no string)	Block	1
71.6.135.131	United States	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.76.44	e.refuah.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
71.6.135.131	United States	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	1
79.181.113.224	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.135.131	United States	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	1

04-16-2015-16:03:08 to 04-16-2015-17:03:08

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	3
43.255.191.168	Japan	147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
41.159.136.58	Gabon	147.237.76.44	e.refuah.idf.il	ET SCAN NMAP -f -sS	1
132.71.84.45	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	1
2.54.175.10	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
82.80.55.172	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.73.211	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	1
58.20.54.249	China	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.168	Japan	147.237.76.86	navy.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.168	Japan	147.237.72.217	e.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.168	Japan	147.237.0.33	idf.il	ET SCAN Potential SSH Scan	1
198.20.69.74	United States	147.237.77.226	www.chamatz.aka.idf.il	ET DROP Dshield Block Listed Source	1
41.159.136.58	Gabon	147.237.76.44	e.refuah.idf.il	ET SCAN NMAP -sS window 2048	1
176.12.147.108	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	1
5.28.164.94	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
101.71.71.167	China	147.237.8.45	e.eitan.idf.il	ET SCAN NMAP -sS window 3072	1
77.126.220.51	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
61.240.144.66	China	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.168	Japan	147.237.77.121	e.navy.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.168	Japan	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.168	Japan	147.237.72.14	dover.idf.il(old)	ET SCAN Potential SSH Scan	1

04-16-2015-16:03:08 to 04-16-2015-17:03:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
95.86.67.130	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9764
82.145.221.61	Europe	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2198
109.65.48.171	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1971
81.218.131.137	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1582
82.145.220.148	Europe	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1107
82.145.223.76	Europe	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	850
212.179.61.126	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	686
41.36.169.34	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	402
107.77.85.76	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	375
2.54.3.241	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	339
66.249.78.166	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	149
37.26.147.236	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	148
66.249.78.173	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	143
66.249.78.159	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	137
212.200.247.165		147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	135
80.179.223.31	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	108
84.229.30.43	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	107
94.159.162.67	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	95
196.221.144.201	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	81
162.243.210.161	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	80
66.249.78.159	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	71
172.56.34.199	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	67
2.54.163.13	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	67
66.249.78.173	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	65
66.249.78.166	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	65
84.108.149.161	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	64
66.87.65.9	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	63
31.44.132.69	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	62
105.201.86.191	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	62
93.172.182.122	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	59
207.46.13.31	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	56
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	55
157.55.39.33	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	54
82.102.136.65	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	54
62.215.132.82	Kuwait	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	54
149.88.69.97	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	54
197.247.216.224	Morocco	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	54
207.46.13.77	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	53
92.99.237.128	United Arab Emirates	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	52
5.108.42.108	Saudi Arabia	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	51
188.247.78.81	Jordan	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	51
195.34.150.18	Austria	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	51
66.249.78.159	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	50
109.110.116.112	Lebanon	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	49
41.235.241.33	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	48
176.12.145.186	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	48
207.46.13.1	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	47
85.250.122.13	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	46
37.143.220.117	Bulgaria	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	46
197.163.38.11	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	44

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
37.26.147.215	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	335
109.253.134.55	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	51
109.253.139.58	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	48
109.67.169.153	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	5
173.192.238.44	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 173.192.238.44	Block	4
109.253.141.41	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	4
167.220.196.85	United Kingdom	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	3
84.228.115.125	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
5.102.254.124	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	3
83.130.103.98	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	3
31.154.7.4	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
85.250.14.122	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
120.149.184.62	Australia	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	2
157.55.39.206	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
62.90.179.94	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	2
109.66.144.54	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
31.168.84.255	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/8/	Block	1
87.69.172.74	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.181.98.62	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/authenticationservice.asmx/getuserdetails	Block	1
66.249.73.219	Israel	147.237.77.74	law.idf.il	Distributed Illegal Parameter Encoding	None	1
92.253.34.226	Jordan	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/984-en/	Block	1
46.19.86.56	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
185.32.176.106	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
5.29.207.9	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
157.55.39.14	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/general...067&docid=31516	Block	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/coni/english/main_index.stm	Block	1
62.219.99.130	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
37.8.109.75	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ar'	Block	1
89.138.44.95	Israel	147.237.77.170	maarachot.idf.il	CVE-2011-3192:Apache_httpd_Remote_Denial_of_Service_ME	Block	1
79.182.150.37	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
5.29.42.151	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
66.249.79.13	Israel	147.237.72.166	aka.idf.il	Unknown Parameter doc.. in www.aka.idf.il/main/drushim/misrot.aspx	None	1
95.86.105.144	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.117.8.125	Israel	147.237.76.30	himush.idf.il	Unauthorized URL Access to www.himush.atal.idf.il/scriptresource.axd	Block	1
188.37.226.128	Portugal	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/	Block	1
157.55.39.15	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
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	1
66.249.65.186	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/templates/getfile/getfile.aspx	Block	1
91.217.90.49	Ukraine	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to 147.237.77.19/rom-0	Block	1
5.29.97.172	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
173.192.238.44	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/feed/atom/	Block	1
66.249.79.42	Israel	147.237.72.166	aka.idf.il	Unknown Parameter 4d9c6f40 in www.aka.idf.il/main/giyus/faq.aspx	None	1
95.173.171.236	Turkey	147.237.0.34	tikshuv.idf.il	Illegal HTTP Version	Block	1
46.121.76.167	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyua	Block	1
194.60.77.207	Ukraine	147.237.72.166	aka.idf.il	Unknown Parameter sorderby in www.aka.idf.il/iturim/asp/displayallsoldiers.asp	None	1
85.250.108.78	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/0/	Block	1
79.178.140.189	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
66.249.73.203	Israel	147.237.77.74	law.idf.il	Distributed Illegal Parameter Encoding	None	1
109.253.134.193	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
91.217.90.49	Ukraine	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/rom-0	Block	1

04-16-2015-16:03:08 to 04-16-2015-17:03:08