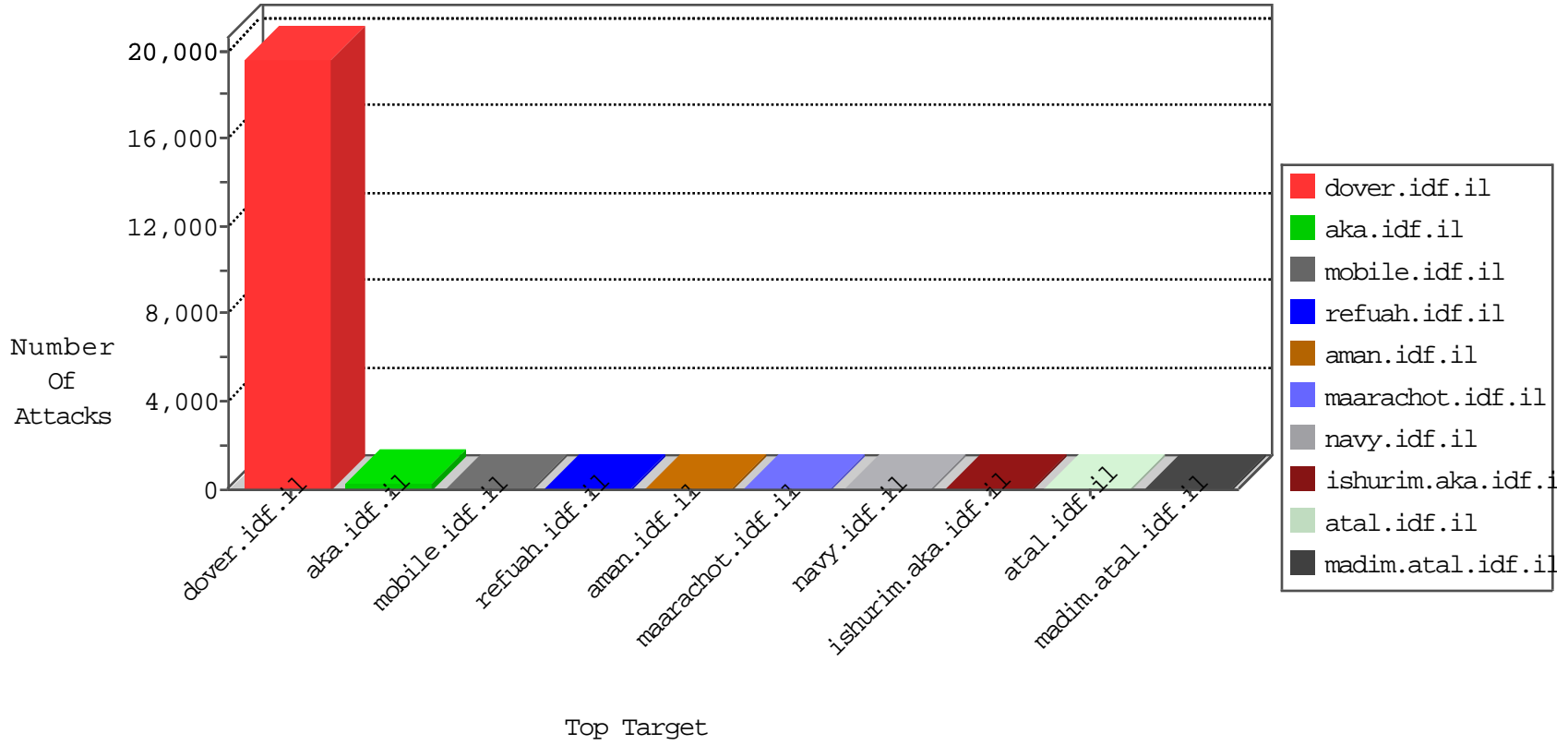


IDF Under Attack

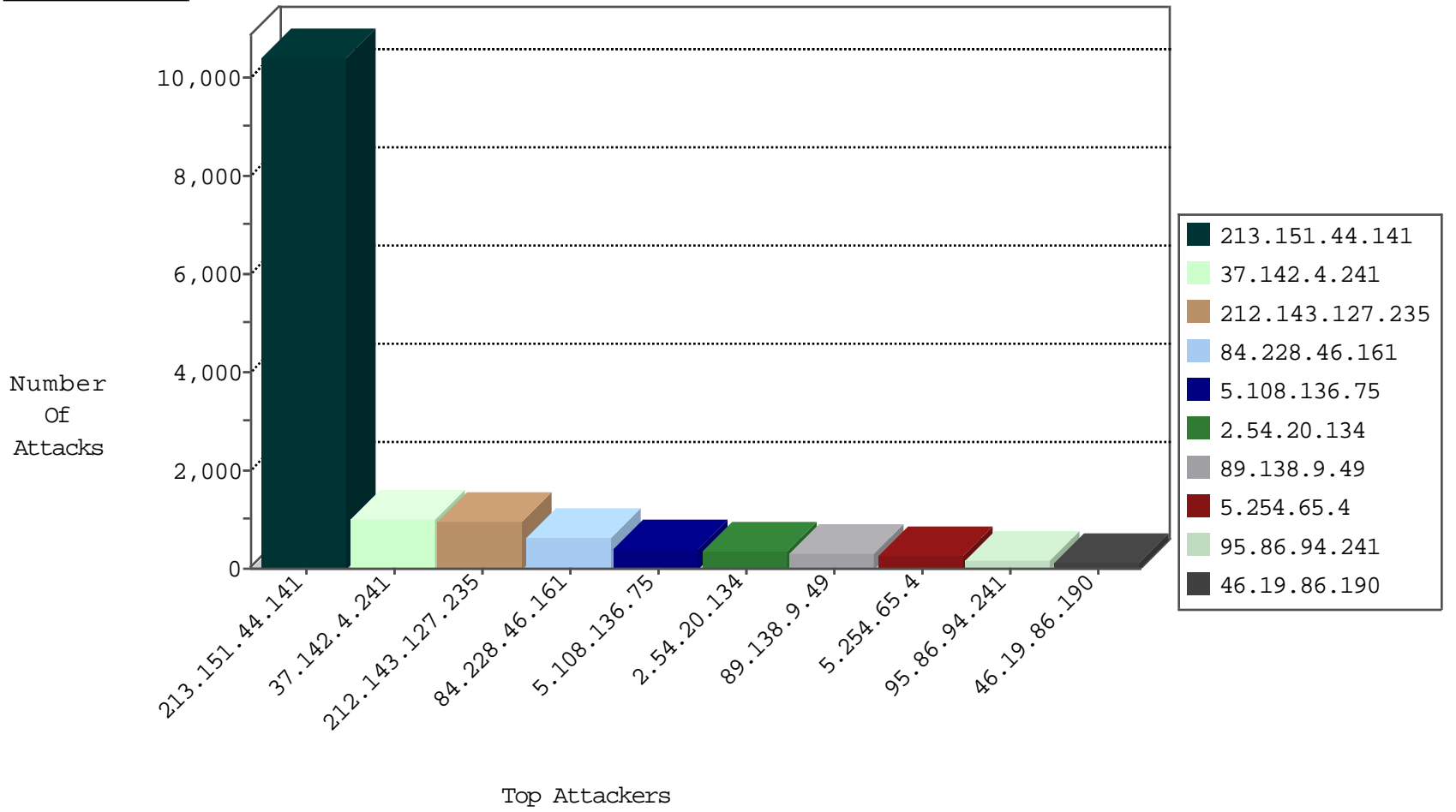
05-10-2015-16:03:09



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
82.166.145.239	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	128
109.67.147.248	Israel	147.237.72.156	anan.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	98
82.102.141.255	Israel	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	35
82.145.219.134	Europe	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	10
31.168.64.134	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	5
5.22.129.255	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
183.136.216.4	China	147.237.76.200	eitan.aka.idf.il	JLM_Under_Attack_Con_Top	drop	2
37.26.147.129	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
80.246.138.213	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
37.9.62.22	United Kingdom	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1
212.179.61.127	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
46.121.243.68	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
2.54.156.9	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
37.9.62.22	United Kingdom	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1
66.240.192.138	United States	147.237.76.39	mobile.meitav.idf.il	Block_Ntp_All_Net	drop	1
188.120.148.253	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
82.102.141.249	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid TCP Flags	drop	1
79.182.63.124	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
207.46.13.26	United States	147.237.72.166	aka.idf.il	HTTP-Misc-BadBlue-Dir-Trave-2	dest-reset	1
46.19.85.235	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
140.242.64.131	United States	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
184.173.183.172	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	21
85.250.93.88	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
149.78.180.148	United States	147.237.72.167	ishurim.aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
213.57.29.128	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
198.20.69.98	United States	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	1
80.179.223.31	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
71.6.135.131	United States	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	1
2.52.156.162	Israel	147.237.77.234	halag.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.25.43.94	Germany	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.201	e.atal.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
198.20.70.114	United States	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	1
31.168.180.89	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
185.32.178.20	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.25.43.94	Germany	147.237.8.46	e.chimuch.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	1
77.127.158.138	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	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
54.215.74.228	United States	147.237.0.17	m.my-kosher-kravi.idf.il	12348: HTTP: PHP-CGI Query String Parameter Command Injection Vulnerability	Block	1
188.138.9.50	Germany	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	1
79.181.28.118	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	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.38	e.e.meitav.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
85.25.103.50	Germany	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	1

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
84.108.193.192	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
87.69.87.164	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
78.129.148.77	United Kingdom	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
46.116.160.61	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
196.47.173.21	Cote D'Ivoire	147.237.76.196	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
5.29.68.122	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	1
183.136.216.4	China	147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	1
128.199.254.26	Singapore	147.237.72.156	aman.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
119.61.7.7	China	147.237.77.233	atal.idf.il	ET SCAN Potential SSH Scan	1
85.64.86.85	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
79.182.63.124	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	1
61.240.144.67	China	147.237.72.166	aka.idf.il	ET SCAN NMAP -sS window 1024	1
196.47.173.21	Cote D'Ivoire	147.237.76.196	e.sviva.idf.il	ET SCAN NMAP -sS window 2048	1
46.19.85.54	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	1
196.47.173.21	Cote D'Ivoire	147.237.76.196	e.sviva.idf.il	ET SCAN NMAP -f -sS	1
193.33.16.2	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
177.189.208.184	Brazil	147.237.8.14	e.orchot.idf.il	ET SCAN NMAP -sS window 4096	1
119.61.7.7	China	147.237.77.243	mobile.idf.il	ET SCAN Potential SSH Scan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
213.151.44.141	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10386
37.142.4.241	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1004
212.143.127.235	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	942
84.228.46.161	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	612
2.54.20.134	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	328
89.138.9.49	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	292
5.254.65.4	Romania	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	245
95.86.94.241	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	183
46.19.86.190	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	125
212.179.46.22	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	122
2.52.182.244	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	110
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	109
66.87.116.236	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	99
31.154.9.162	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	96
2.54.150.189	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	93
213.151.32.163	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	81
85.115.248.141	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	71
66.249.81.212	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	68
213.57.134.73	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	65
66.249.81.215	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	54
84.228.202.1	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	53
66.249.81.218	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	46
195.160.240.11	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	44
66.249.75.58	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	41
84.228.132.6	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	40
80.246.130.110	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	39
46.19.85.4	Israel	147.237.77.243	mobile.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	39
95.86.99.91	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	36
166.137.118.75	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	35
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	34
66.249.93.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	33
212.179.61.127	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	32
85.250.124.206	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	29
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	29
77.126.29.2	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	29
46.19.85.123	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	29
81.218.108.134	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	28
46.19.86.108	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	28
37.140.141.39	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	28
69.248.82.82	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	28
66.249.75.74	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	27
45.56.15.113		147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	27
212.150.192.180	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	26
79.180.125.220	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	26
2.52.44.25	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	26
92.61.225.10	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	25
62.90.5.209	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	25
84.228.165.105	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	24
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	24
192.117.12.65	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	24

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
5.108.136.75	Saudi Arabia	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 5.108.136.75	Block	358
192.117.12.65	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	24
212.179.50.230	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/scripts/css3pie.htc	Block	7
5.108.136.75	Saudi Arabia	147.237.77.216	dover.idf.il	PHP Attempt	Block	7
84.108.4.137	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	6
77.127.202.152	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	5
93.172.136.89	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	5
176.12.138.209	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.12.138.209	Block	5
109.253.137.205	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
2.52.44.54	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	4
157.55.39.137	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	3
209.88.198.1	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	3
157.55.39.162	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
109.160.156.220	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
37.26.147.186	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	3
176.12.136.37	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
178.137.19.143	Ukraine	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/901-11442-en/	Block	3
46.19.86.153	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
79.176.4.153	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
188.120.148.240	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
93.173.168.65	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	2
66.249.78.148	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/mobile/	Block	2
207.46.13.26	United States	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
207.46.13.26	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 207.46.13.26	Block	2
109.64.142.90	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
46.19.85.3	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
66.249.69.41	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/71878-he/maarachot.aspx	Block	1
188.93.144.88	Netherlands	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/old/wp-admin/	Block	1
66.249.64.145	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
176.12.138.209	Israel	147.237.0.19	madim.atal.idf.il	Too Many 404: Response Code per Session	Block	1
85.64.158.194	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
81.218.56.171	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
5.108.136.75	Saudi Arabia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/	Block	1
149.88.3.154	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.75.74	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-16189-en/dover.aspx-title=idf	Block	1
192.117.12.65	Israel	147.237.72.167	ishurim.aka.idf.il	SSL Untraceable Connection - Unknown SSL Session	None	1
109.67.115.90	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
87.69.249.43	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https://www.idf.il/	Block	1
66.249.67.79	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/templates/getfile/getfile.aspx	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
84.108.213.30	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.253.138.37	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
66.249.73.197	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 66.249.73.197	Block	1
93.173.16.3	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https://www.idf.il/	Block	1
66.249.64.150	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/gyus/forum/asp/showforum.asp	Block	1
87.68.216.29	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/gyus/authenticationservice.aspx/getuserdetails	Block	1
81.218.70.243	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
23.20.154.145	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
157.55.39.7	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1