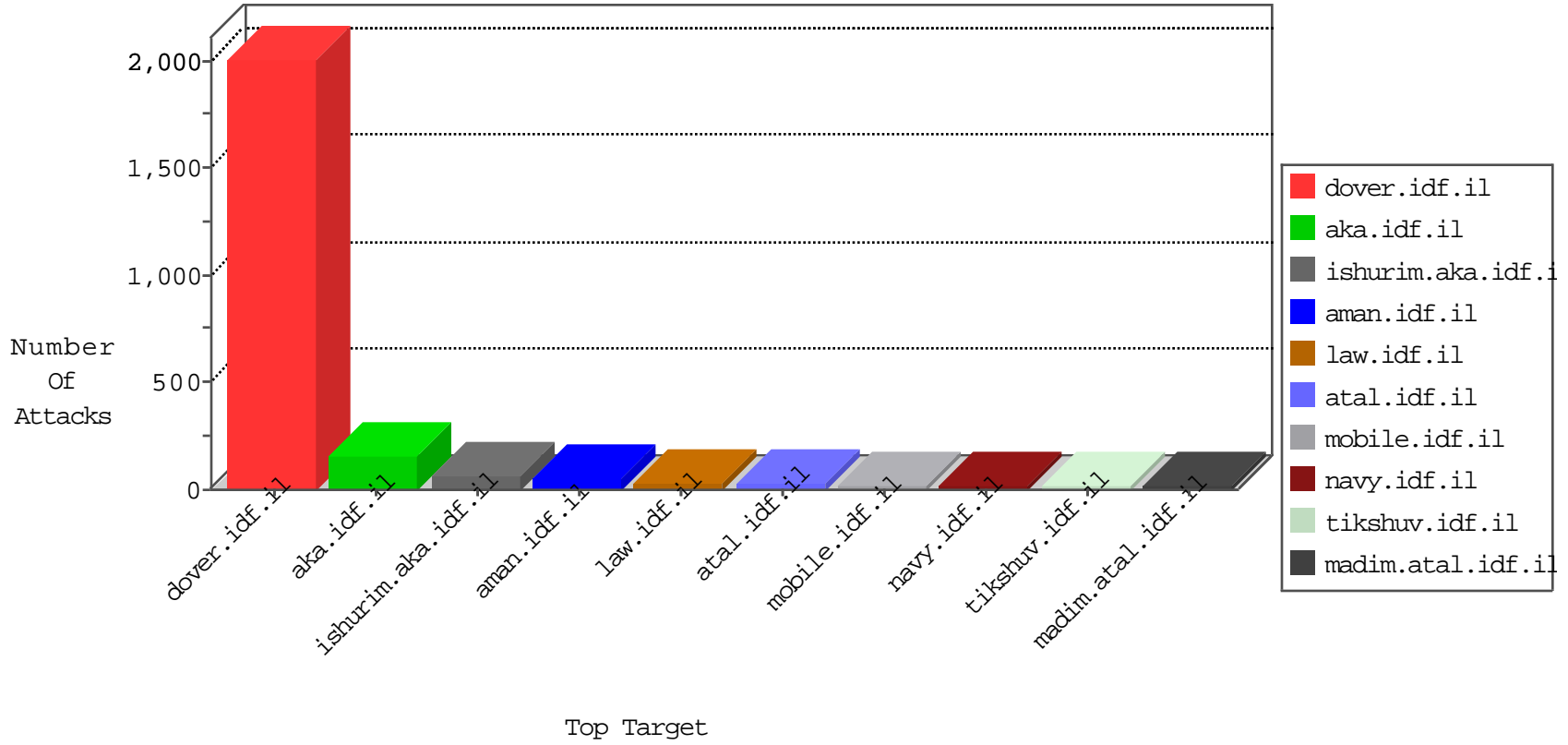
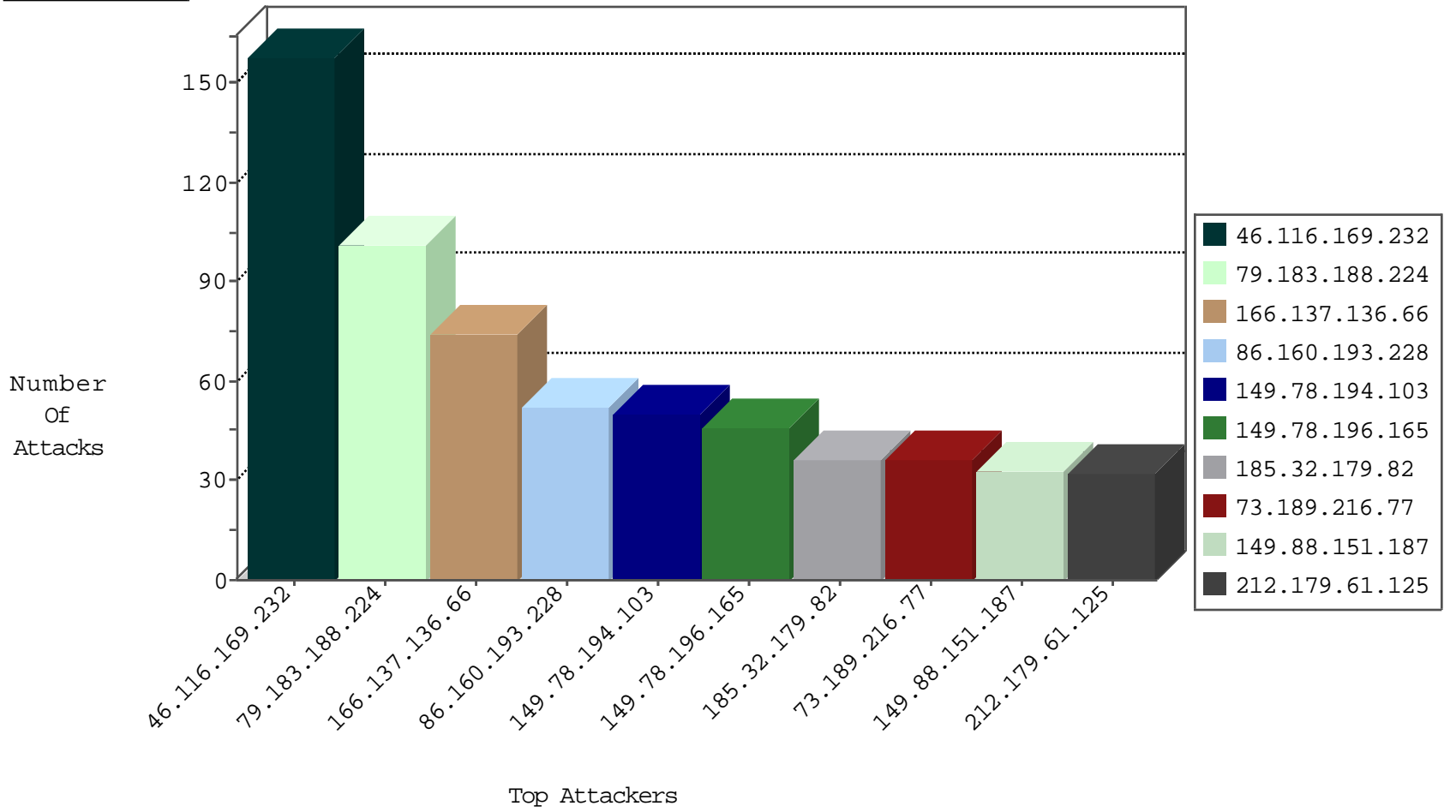




Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.64.2	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	989
204.13.200.28	United States	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	forward	366
66.249.78.166	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	200
66.249.64.64	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	101
46.19.85.35	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	25
46.19.85.35	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	25
109.184.24.226	Russian Federation	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
5.102.254.220	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
176.12.160.5	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
176.12.160.5	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
73.189.216.77	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
79.183.37.102	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
176.12.143.190	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
71.6.216.47	United States	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1
14.198.176.81	Hong Kong	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
213.57.245.68	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
109.67.110.214	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
66.249.78.18	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	1
2.54.182.132	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
195.37.190.86	Germany	147.237.76.201	e.atal.idf.il	Block_Ntp_All_Net	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
5.29.109.51	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	9
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	8
84.109.180.46	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
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	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	1
93.172.211.88	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
46.19.85.148	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.165.200	United States	147.237.76.34	yohalan.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
85.25.103.50	Germany	147.237.77.19	law-forum.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	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	1
46.116.160.236	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
84.109.209.33	Israel	147.237.76.86	navy.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	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	1
79.176.14.243	Israel	147.237.76.42	refuah.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
192.116.98.196	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
66.240.236.119	United States	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.42	refuah.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
93.120.27.62	Romania	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
81.218.104.85	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.135.131	United States	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.176	test.ncore.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
93.120.27.62	Romania	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	1
84.108.174.212	Israel	147.237.0.34	tikshuv.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.135.131	United States	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.77.216	dover.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
85.64.32.30	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
212.33.127.200	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	2
192.117.10.227	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
147.236.31.182	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
87.68.47.104	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
82.166.114.245	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.64.98	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
41.159.136.195	Gabon	147.237.76.39	mobile.meitav.idf.il	ET SCAN NMAP -sS window 2048	1
212.179.28.34	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
41.159.136.58	Gabon	147.237.76.39	mobile.meitav.idf.il	ET SCAN NMAP -sS window 3072	1
183.136.216.3	China	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	1
91.224.132.118	Russian Federation	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
79.176.131.23	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
61.240.144.65	China	147.237.77.233	atal.idf.il	ET SCAN NMAP -sS window 1024	1
61.183.128.6	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
41.159.136.195	Gabon	147.237.76.39	mobile.meitav.idf.il	ET SCAN NMAP -f -sS	1
5.196.147.122	Germany	147.237.76.30	himush.idf.il	ET SCAN NMAP -sS window 1024	1
61.183.128.6	China	147.237.77.234	halag.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
46.116.169.232	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	158
79.183.188.224	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	101
166.137.136.66	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	74
86.160.193.228	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	52
149.78.194.103	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	50
149.78.196.165	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	46
73.189.216.77	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	34
149.88.151.187	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	33
109.65.51.98	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	32
212.179.61.125	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	32
109.65.66.66	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	27
93.173.189.34	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	27
86.46.117.186	Ireland	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	24
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
46.19.85.131	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
192.117.10.227	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	19
77.127.184.38	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	19
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	19
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
213.55.108.94	Ethiopia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
46.19.85.80	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
79.179.146.112	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
2.54.36.188	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
31.210.186.152	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
94.153.222.138	Ukraine	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
12.230.217.7	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
109.253.145.59	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
5.29.120.181	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
195.64.77.107	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
12.69.179.102	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
185.32.179.82	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid sequence number	Bad TCP sequence	monitor	12
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
109.64.9.14	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
212.25.83.133	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
5.102.254.220	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
65.55.210.79	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
185.32.179.82	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid ACK number	Bad TCP sequence	alert	12
109.253.143.53	Israel	147.237.77.243	mobile.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
46.19.85.121	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
185.32.179.82	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid ACK number	Bad TCP sequence	monitor	12
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
109.253.140.91	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	10
77.126.29.77	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
66.249.64.76	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
79.183.136.9	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
213.151.48.226	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
109.160.245.110	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
37.26.146.150	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
157.55.39.10	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
176.12.139.0	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	14
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	7
185.13.195.17	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/modiin/default.aspx.co.il	Block	6
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	5
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	3
79.183.145.5	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom Temporary	Block	2
157.55.39.3	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/rabanut/webresource.axd	Block	2
79.142.66.15	Netherlands	147.237.72.166	aka.idf.il	PHP Attempt	Block	2
109.65.66.66	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	2
149.78.15.196	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom Temporary	Block	2
77.126.42.147	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	2
68.180.228.117	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/homefront/hebrew/ie-welcome.stm	Block	1
149.88.148.206	United States	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1136-he/atal.aspx	Block	1
109.65.35.112	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https://www.aka.idf.il/	Block	1
66.249.75.34	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/terms.aspx	Block	1
62.219.144.212	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom Temporary	Block	1
192.116.98.196	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https://www.aman.idf.il/	Block	1
84.109.180.46	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
157.55.39.176	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.176	Block	1
77.237.138.202	Czech Republic	147.237.77.233	atal.idf.il	Unauthorized URL Access to /	Block	1
109.66.111.20	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/giyus/terms.aspx	None	1
66.249.67.57	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1273-he/atal.aspx	Block	1
89.138.20.232	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https://www.idf.il/	Block	1
46.4.68.142	Germany	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 46.4.68.142	Block	1
176.12.143.215	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/homefront/tele.stm	Block	1
109.65.37.201	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https://www.aka.idf.il/	Block	1
66.249.75.42	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/home/pniot.aspx	Block	1
66.249.64.12	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/219-he/patzar.aspx	Block	1
212.76.99.24	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	1
84.228.110.99	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https://www.aka.idf.il/	Block	1
157.55.39.178	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/main/snalim/faq.aspx	None	1
109.253.147.38	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	SSL Untraceable Connection - Unknown Server Certificate	None	1
89.138.44.103	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/	Block	1
66.249.67.65	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1246-he/atal.aspx	Block	1
80.230.1.23	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/authentication-service.aspx/getuserdetails	Block	1
46.120.154.228	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https://www.aka.idf.il/	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/sendtofriend/kkkkkkkk=6084b0bckkkkkkkk_6084b0bc	Block	1
157.55.39.5	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	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
66.249.78.58	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/71918-he/maarachot.aspx	Block	1
66.249.64.219	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/	Block	1
217.132.65.124	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https://www.aka.idf.il/	Block	1
85.65.229.218	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https://www.aka.idf.il/	Block	1
157.55.39.182	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/320/patzar.aspx	Block	1
79.176.101.194	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https://www.idf.il/	Block	1
109.64.101.58	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	1
66.249.69.86	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/1172-he/hamaz.aspx	Block	1
84.108.25.150	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
61.135.190.68	China	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.15/	Block	1