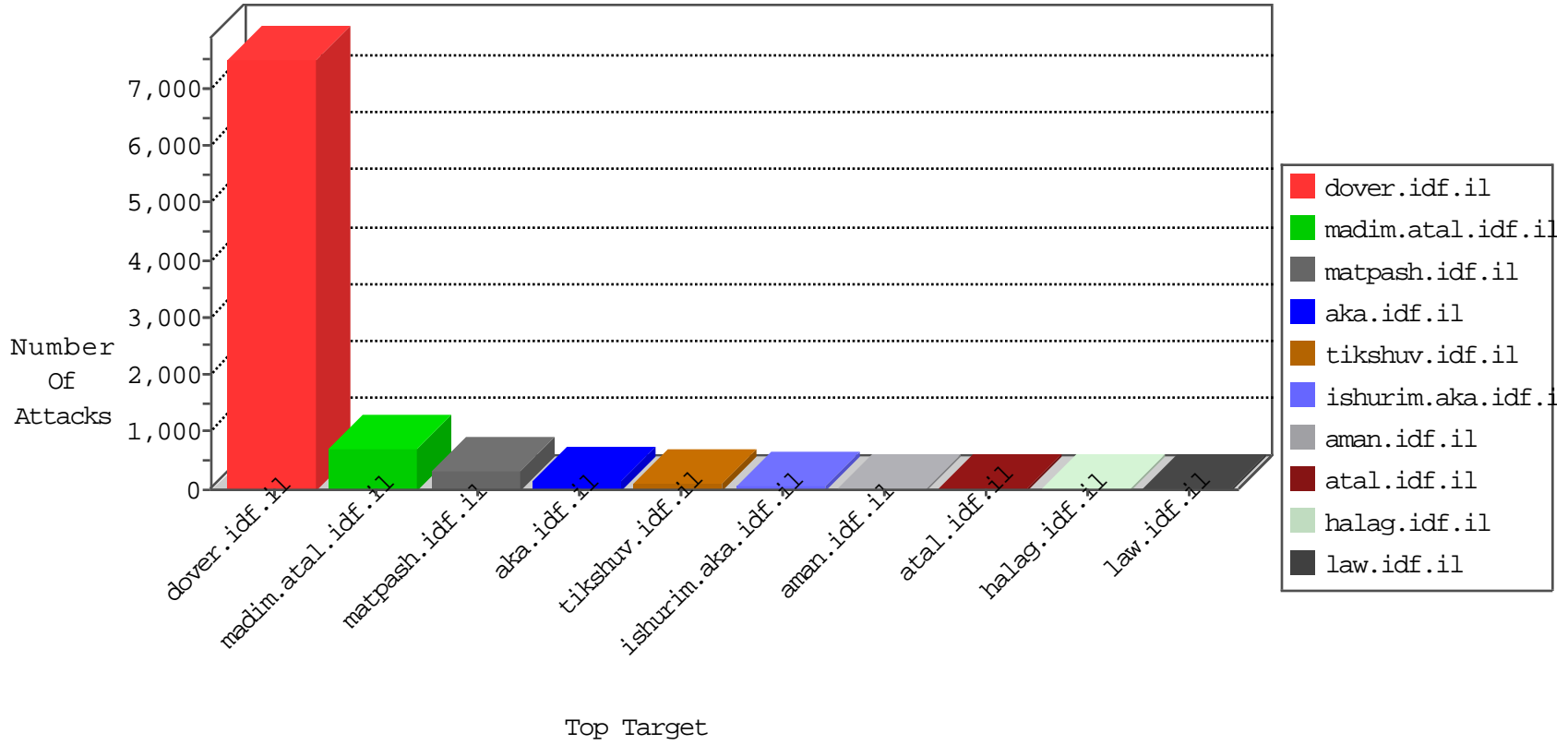
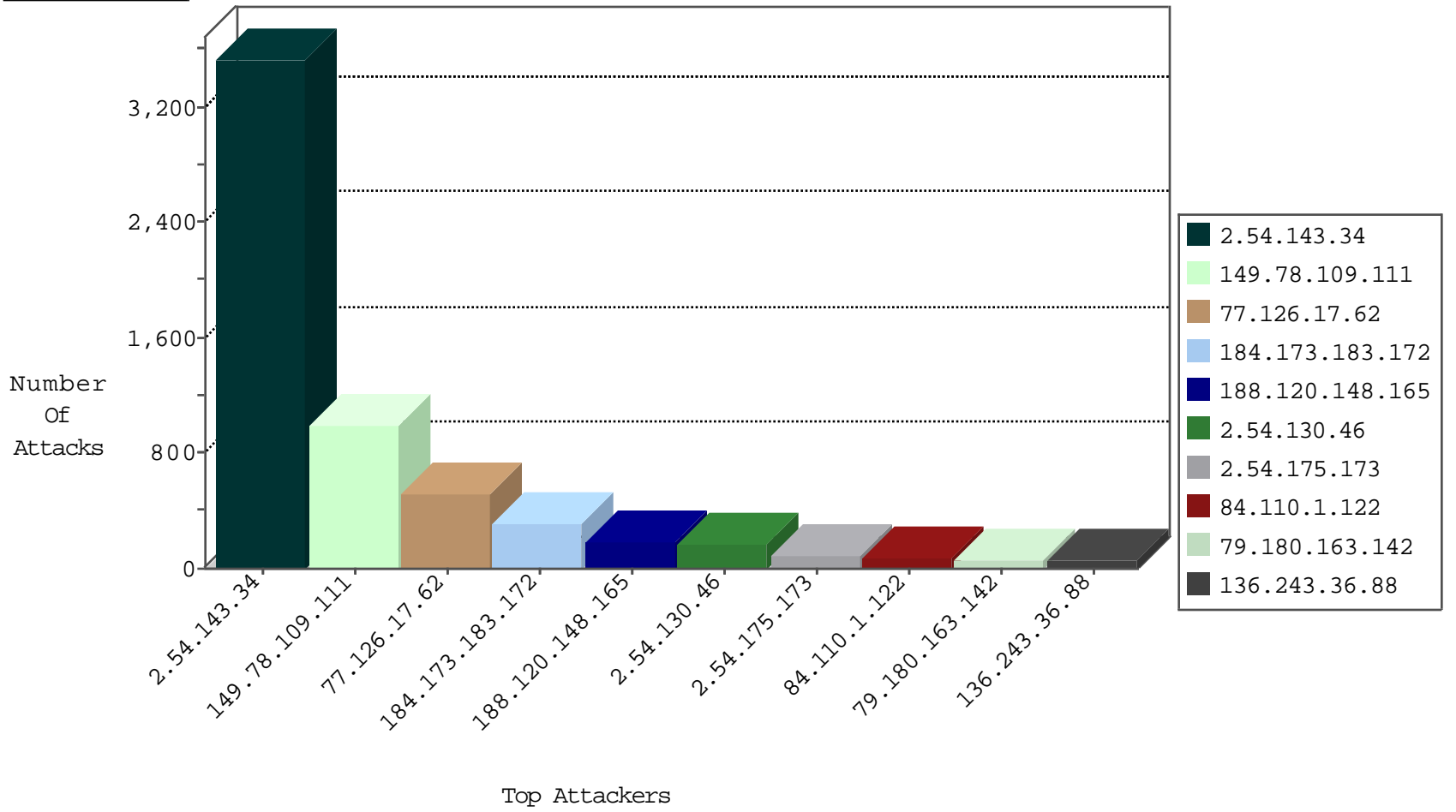


Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
79.179.139.123	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	261
46.116.154.43	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	117
84.228.86.155	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	74
66.249.67.40	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	26
82.102.141.252	Israel	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	6
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
124.232.142.220	China	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
107.154.64.10	United States	147.237.0.19	madim.atal.idf.il	I4 Source or Dest Port Zero	drop	1
2.54.173.71	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
80.141.203.28	Germany	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
184.173.183.172	United States	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	310
46.137.134.188	Ireland	147.237.72.156	aman.idf.il	DVRep_P-N_40-59	Permit	10
46.137.134.188	Ireland	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	10
46.19.85.203	Israel	147.237.76.31	nakchal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
188.120.148.165	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
213.57.104.125	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
66.240.192.138	United States	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	2
46.121.214.109	Israel	147.237.76.31	nakchal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
198.20.70.114	United States	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	1
79.180.141.99	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
66.240.192.138	United States	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	1
85.250.150.78	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.165.200	United States	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	1
95.139.206.189	Russian Federation	147.237.72.166	aka.idf.il	3617: HTTP: Paros Proxy HTTP Request	Block	1
71.6.167.142	United States	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	1
109.65.71.84	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.167.142	United States	147.237.8.24	e.lifestyle.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
198.20.69.98	United States	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	1
46.117.29.99	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
198.20.70.114	United States	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.8.46	e.chimch.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.8.24	e.lifestyle.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	4
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	4
66.249.78.197	United States	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	2
66.249.67.40	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
66.249.73.203	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
66.249.65.28	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
89.248.171.167	Netherlands	147.237.77.74	law.idf.il	ET SCAN NMAP -sS window 1024	1
78.93.225.18	Saudi Arabia	147.237.76.197	e.himush.idf.il	ET SCAN NMAP -sS window 3072	1
202.71.25.29	India	147.237.76.44	e.refuah.idf.il	ET SCAN NMAP -sS window 4096	1
61.240.144.65	China	147.237.76.30	himush.idf.il	ET SCAN NMAP -sS window 1024	1
46.116.237.236	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
119.97.231.102	China	147.237.0.200	m4u.idf.il	ET SCAN NMAP -sS window 3072	1
117.74.137.59	China	147.237.77.227	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
117.74.137.59	China	147.237.76.31	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
78.93.225.18	Saudi Arabia	147.237.76.197	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
202.71.25.29	India	147.237.76.44	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	China	147.237.76.198	e.yohalan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
119.97.231.102	China	147.237.0.200	m4u.idf.il	ET SCAN NMAP -sS window 4096	1
117.74.137.59	China	147.237.77.227	e.hamaz.idf.il	ET SCAN NMAP -sS window 2048	1
117.74.137.59	China	147.237.77.227	e.hamaz.idf.il	ET SCAN NMAP -f -sS	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
2.54.143.34	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3532
149.78.109.111	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	983
188.120.148.165	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	169
2.54.130.46	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	166
79.180.163.142	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	63
87.69.42.233	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	61
46.117.62.194	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	58
136.243.36.88	Germany	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	56
37.26.147.199	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	50
176.12.151.46	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	50
46.120.240.207	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	47
176.12.146.62	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	42
2.52.40.86	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	42
85.65.221.90	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	41
109.64.102.107	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	35
197.242.114.33	Nigeria	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	34
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	34
109.253.128.130	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	33
109.253.131.2	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	32
176.12.137.61	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	32
46.19.86.241	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	29
2.54.130.34	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	28
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	27
176.12.151.217	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	27
52.16.5.197	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	27
89.139.184.131	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	27
85.64.98.30	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	26
54.72.0.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	25
66.249.78.173	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	25
82.102.141.252	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	25
176.12.143.6	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	24
109.253.134.165	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	24
77.125.245.52	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	23
192.178.5.65	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	23
84.229.130.149	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	21
77.127.233.17	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	20
207.46.13.1	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	20
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	20
46.19.85.75	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	20
85.250.150.78	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	20
46.19.86.178	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	19
70.192.66.8	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	19
66.249.78.166	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	18
93.172.34.126	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	18
66.249.78.159	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	18
84.110.60.59	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	18
207.46.13.52	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	18
176.12.149.17	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	17
109.253.145.37	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	17
79.183.0.90	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	16

