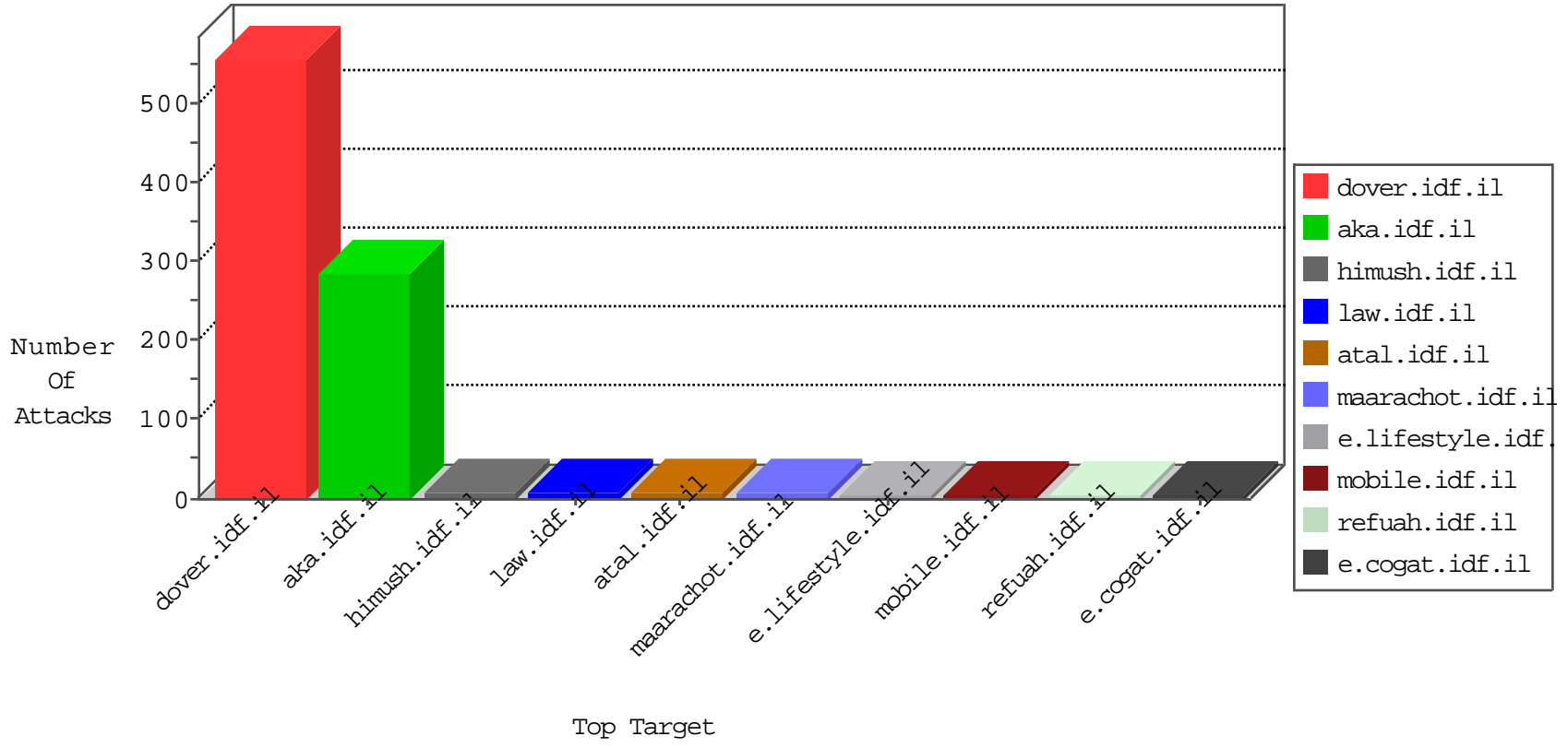
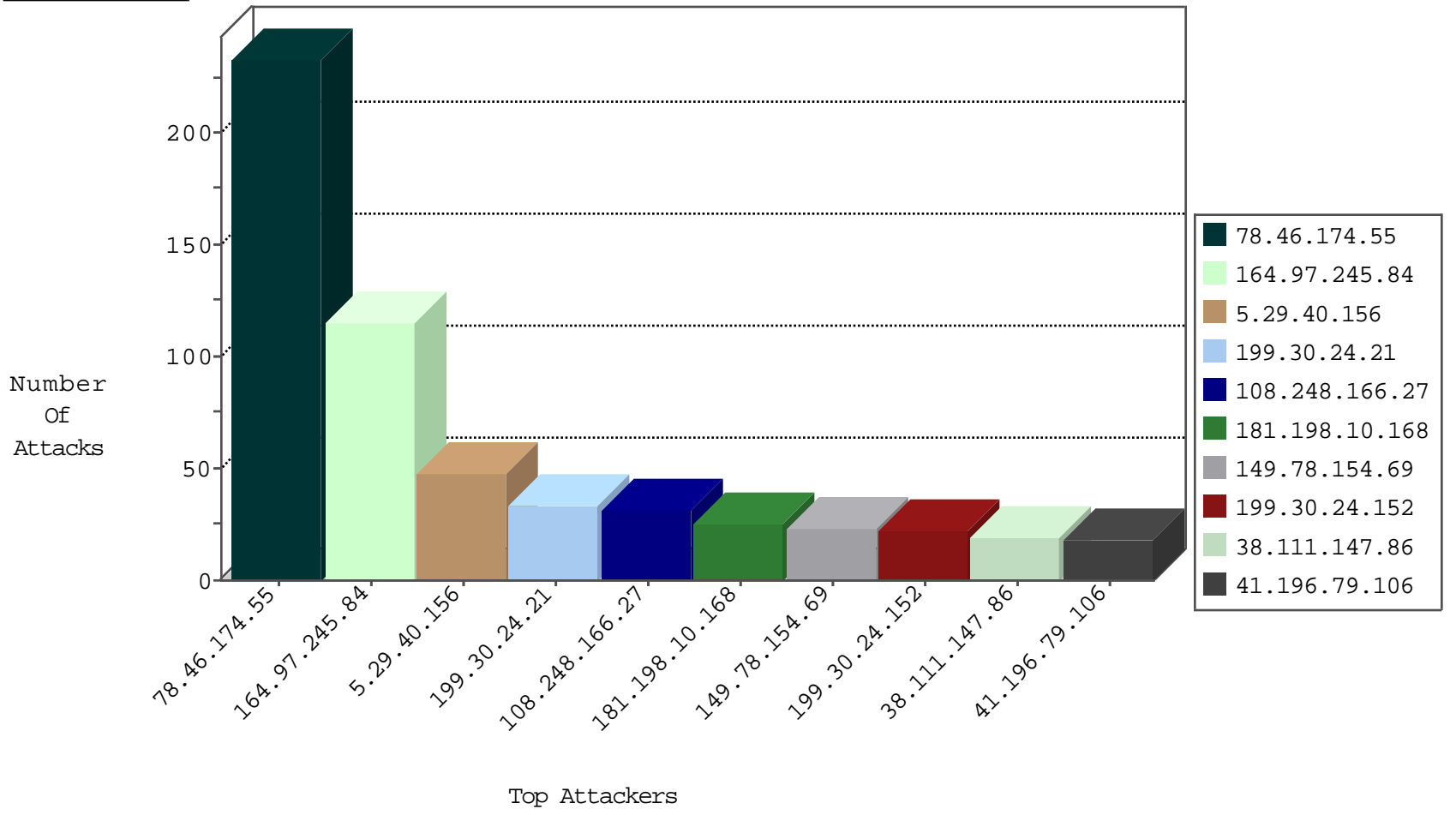




Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.67.190	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	121
220.181.108.86	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	53
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	4

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
198.20.69.98	United States	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	2
85.25.103.50	Germany	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	2
71.6.167.142	United States	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	1
129.98.212.68	United States	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	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	1
89.216.115.8		147.237.77.216	dover.idf.il	17272: HTTP: Suspicious User-Agent (WindowsNT) With No Separating Space	Block	1
71.6.135.131	United States	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.8.27	e.madim.atal.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
71.6.167.142	United States	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.0.19	madim.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
66.240.192.138	United States	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.0.16	my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.227	e.hamaz.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
93.120.27.62	Romania	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.148	ggcenter.aka.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.8.50	e.tikshuv.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
71.6.135.131	United States	147.237.0.19	madim.atal.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
94.23.19.178	France	147.237.72.166	aka.idf.il	C1000106: HTTP: majestic bot	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	5
66.249.64.146	United States	147.237.77.233	atal.idf.il	ET SCAN NMAP -sA (2)	2
66.249.67.172	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
61.240.144.64	China	147.237.76.202	e.halag.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
171.107.83.229	China	147.237.77.243	mobile.idf.il	ET SCAN NMAP -sS window 3072	1
23.24.131.164	United States	147.237.8.50	e.tikshuv.idf.il	ET SCAN NMAP -sS window 3072	1
171.107.83.229	China	147.237.77.243	mobile.idf.il	ET SCAN NMAP -f -sS	1
162.248.10.134	Canada	147.237.77.233	atal.idf.il	ET SCAN NMAP -sS window 4096	1
110.55.118.159	Philippines	147.237.8.24	e.lifestyle.idf.il	ET SCAN NMAP -sS window 2048	1
110.55.118.159	Philippines	147.237.8.24	e.lifestyle.idf.il	ET SCAN NMAP -f -sS	1
78.129.148.77	United Kingdom	147.237.77.121	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.66	China	147.237.76.86	navy.idf.il	ET SCAN NMAP -sS window 1024	1
178.19.107.114	Poland	147.237.76.196	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
23.24.131.164	United States	147.237.8.50	e.tikshuv.idf.il	ET SCAN NMAP -sS window 4096	1
171.107.83.229	China	147.237.77.243	mobile.idf.il	ET SCAN NMAP -sS window 2048	1
162.248.10.134	Canada	147.237.77.233	atal.idf.il	ET SCAN Potential SSH Scan	1
162.248.10.134	Canada	147.237.77.233	atal.idf.il	ET SCAN NMAP -sS window 1024	1
110.55.118.159	Philippines	147.237.8.24	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
94.23.210.101	France	147.237.77.170	maarachot.idf.il	SERVER-WEBAPP admin.php access	1
78.129.148.77	United Kingdom	147.237.77.61	e.cogat.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
164.97.245.84	Australia	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	115
5.29.40.156	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	48
199.30.24.21	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	32
181.198.10.168	Ecuador	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	25
149.78.154.69	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	23
199.30.24.152	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	22
38.111.147.86	United States	147.237.72.166	aka.idf.il		drop	drop	19
41.196.79.106	Egypt	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
24.168.9.138	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	18
108.248.166.27	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	16
66.249.73.201	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	14
66.249.73.185	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	14
199.30.25.68	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	14
109.253.132.7	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
46.19.85.247	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
199.30.24.126	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
66.249.73.193	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
174.239.194.102	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
71.195.229.42	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
64.149.142.67	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
50.171.178.221	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
157.55.39.191	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
119.206.17.14	Korea, Republic of	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
188.165.15.14	France	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
99.59.38.233	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
157.55.39.136	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5
108.248.166.27	United States	147.237.77.216	dover.idf.i	Invalid ACK number	Bad TCP sequence	alert	5
46.19.85.139	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	5
108.248.166.27	United States	147.237.77.216	dover.idf.i	Invalid ACK number	Bad TCP sequence	monitor	5
108.248.166.27	United States	147.237.77.216	dover.idf.i	Unexpected post SYN packet - RST or SYN expected	drop	drop	5
157.55.39.191	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
108.59.253.71	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
41.33.232.65	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
212.199.182.150	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3
72.178.98.27	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
61.135.190.70	China	147.237.0.200	m4u.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	2
93.33.129.234	Italy	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
2.54.171.174	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
79.176.159.36	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
54.72.0.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
66.249.73.193	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
195.34.150.18	Austria	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
157.55.39.66	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
54.72.73.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
109.65.185.23	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
157.55.39.204	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
46.19.86.179	Israel	147.237.77.216	dover.idf.i	Invalid ACK number	Bad TCP sequence	monitor	1
199.30.24.21	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1
8.37.227.68	Anonymous Proxy	147.237.77.216	dover.idf.i	Response out of state	Block HTTP Non Compliant	monitor	1

