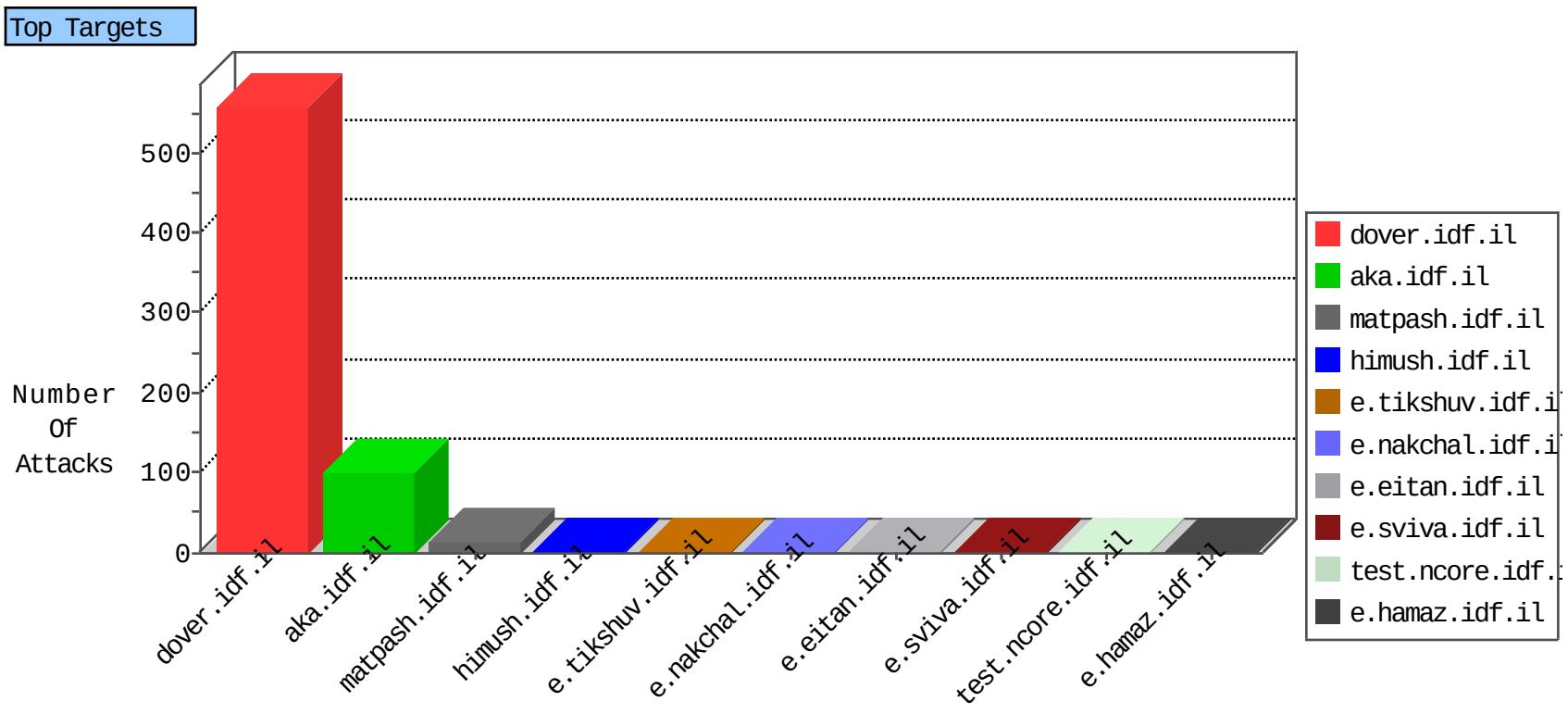
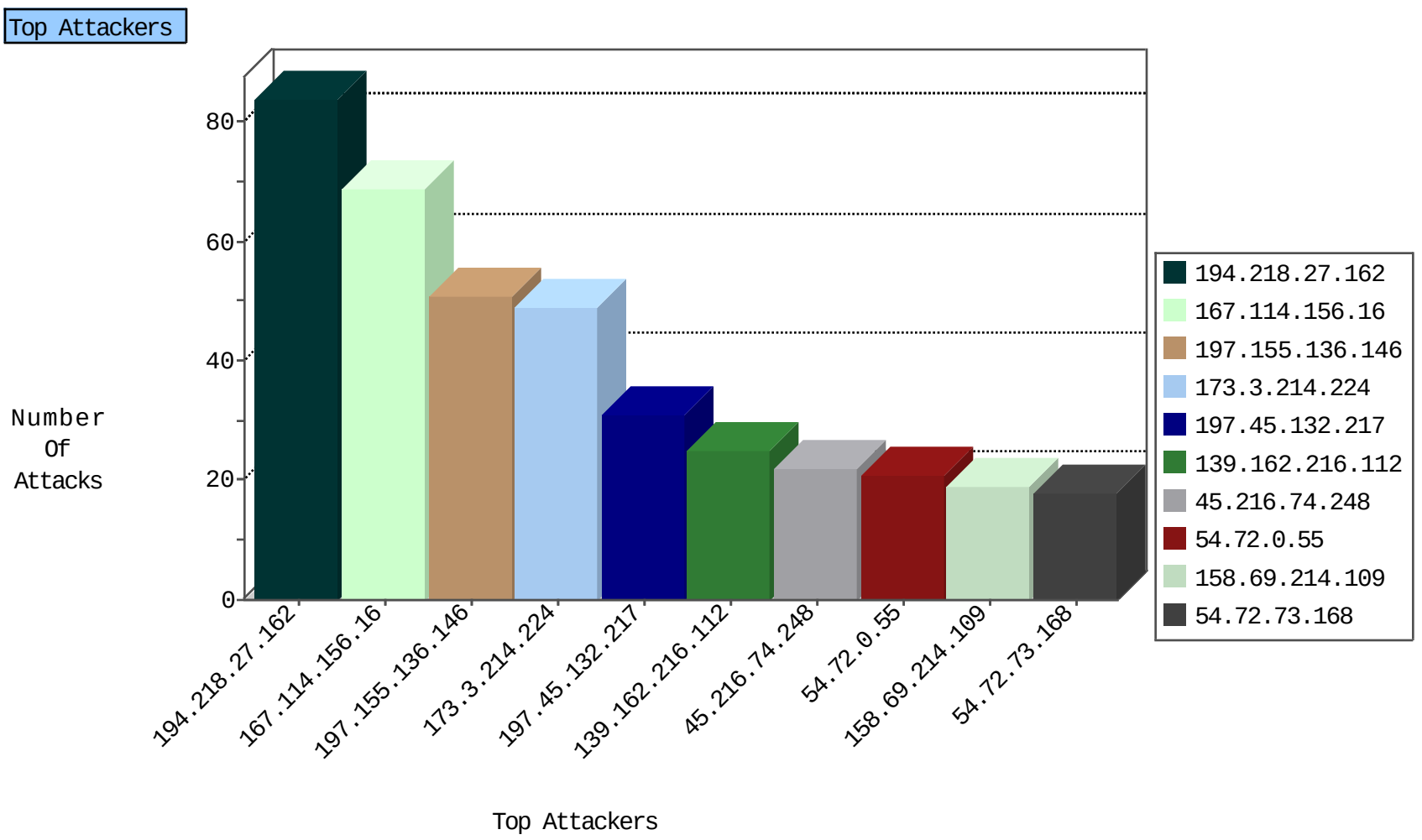
05-02-2016-03:04:09 to 05-02-2016-04:04:09

IDF Under Attack Daily Report

Top Targets



Top Attackers



05-02-2016-03:04:09 to 05-02-2016-04:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	10557
139.162.216.112	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	646
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	24
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	9
192.55.54.40	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
66.240.192.138	United States	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
185.103.252.110	Russian Federation	147.237.76.200	eitan.aka.idf.i	Block_Ntp_All_Net	drop	1
141.212.122.194	United States	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1

05-02-2016-03:04:09 to 05-02-2016-04:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

05-02-2016-03:04:09 to 05-02-2016-04:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
173.193.130.50	147.237.77.121	United States	e.navy.idf.il	ET SCAN NMAP -sS window 4096	1
104.171.122.176	147.237.76.148	United States	gqcenter.aka.idf.il	ET SCAN NMAP -f -sS	1
42.55.136.243	147.237.77.233	China	atal.idf.il	ET SCAN Potential SSH Scan	1
42.55.136.243	147.237.77.176	China	matpash.idf.il	ET SCAN Potential SSH Scan	1
42.55.136.243	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1
42.55.136.243	147.237.8.46	China	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
208.100.26.228	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
104.171.122.176	147.237.76.148	United States	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 2048	1
42.55.136.243	147.237.77.235	China	sviva.idf.il	ET SCAN Potential SSH Scan	1
42.55.136.243	147.237.77.227	China	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
42.55.136.243	147.237.77.19	China	law-forum.idf.il	ET SCAN Potential SSH Scan	1
42.55.136.243	147.237.72.217	China	e.idf.il	ET SCAN Potential SSH Scan	1
13.94.46.116	147.237.76.196	United States	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
208.100.26.228	147.237.0.33	United States	idf.il	ET SCAN NMAP -sS window 1024	1
203.86.29.220	147.237.76.197	China	e.himush.idf.il	ET SCAN NMAP -sS window 3072	1

05-02-2016-03:04:09 to 05-02-2016-04:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	56
197.155.136.146	Mali	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
173.3.214.224	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	49
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	28
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
158.69.214.109	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
157.55.39.106	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
157.55.39.53	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
203.133.169.205	Korea, Republic of	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.102.96	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
45.216.74.248	Morocco	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
54.185.148.8	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
45.216.74.248	Morocco	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
173.21.91.0	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
104.14.42.46	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
192.249.66.247	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
192.55.54.40	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
185.22.32.16	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
97.32.200.253	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
73.171.202.86	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
66.102.8.238	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
209.133.111.211	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
213.205.251.248	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
186.9.134.215	Chile	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
107.77.106.59	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
173.72.240.163	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
207.46.13.178	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
24.156.203.250	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
35.0.127.52	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
66.249.93.119	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
207.46.13.22	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
84.108.169.85	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
141.212.122.113	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
128.242.249.13	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
173.218.193.74	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
69.166.47.131	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
192.55.54.44	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
97.32.200.253	United States	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid sequence number	monitor	2

05-02-2016-03:04:09 to 05-02-2016-04:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

05-02-2016-03:04:09 to 05-02-2016-04:04:09