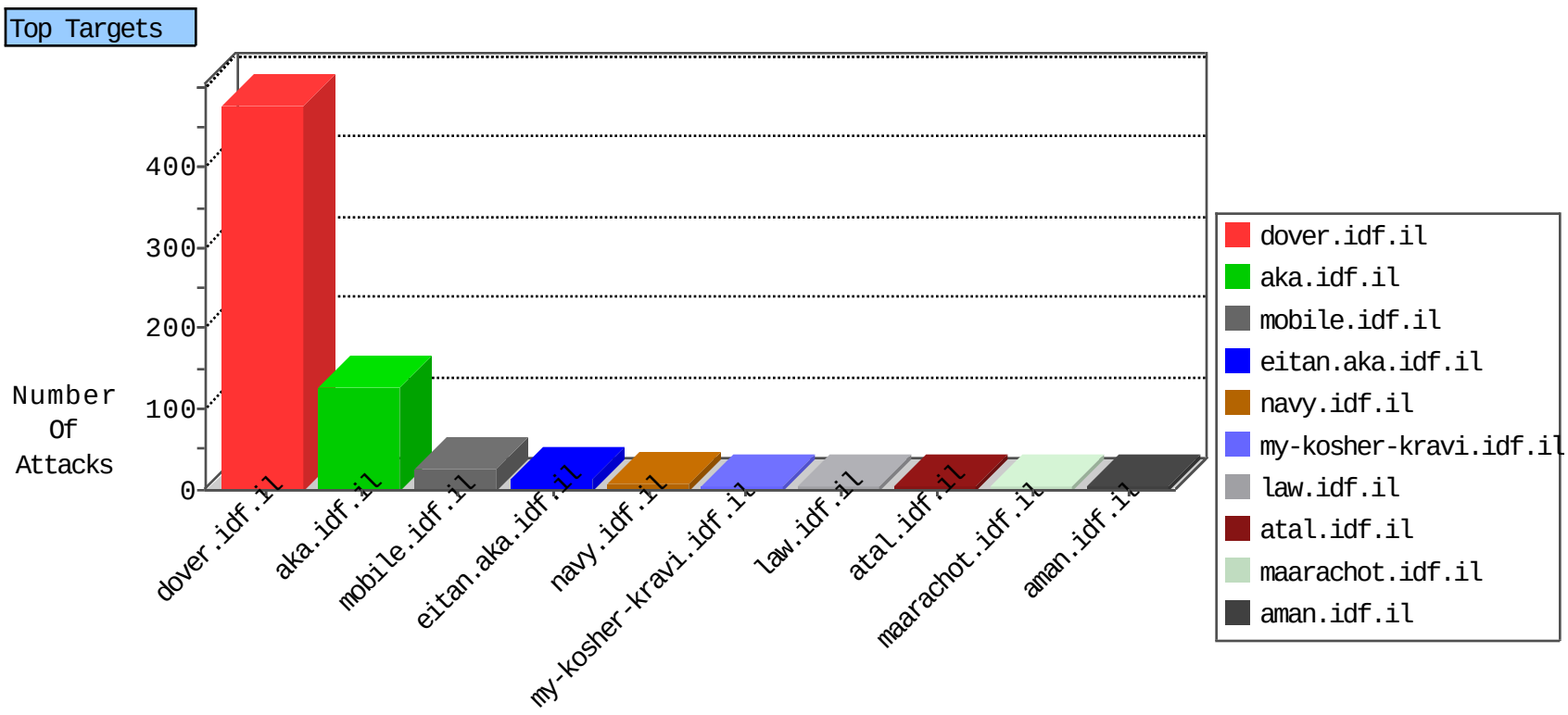
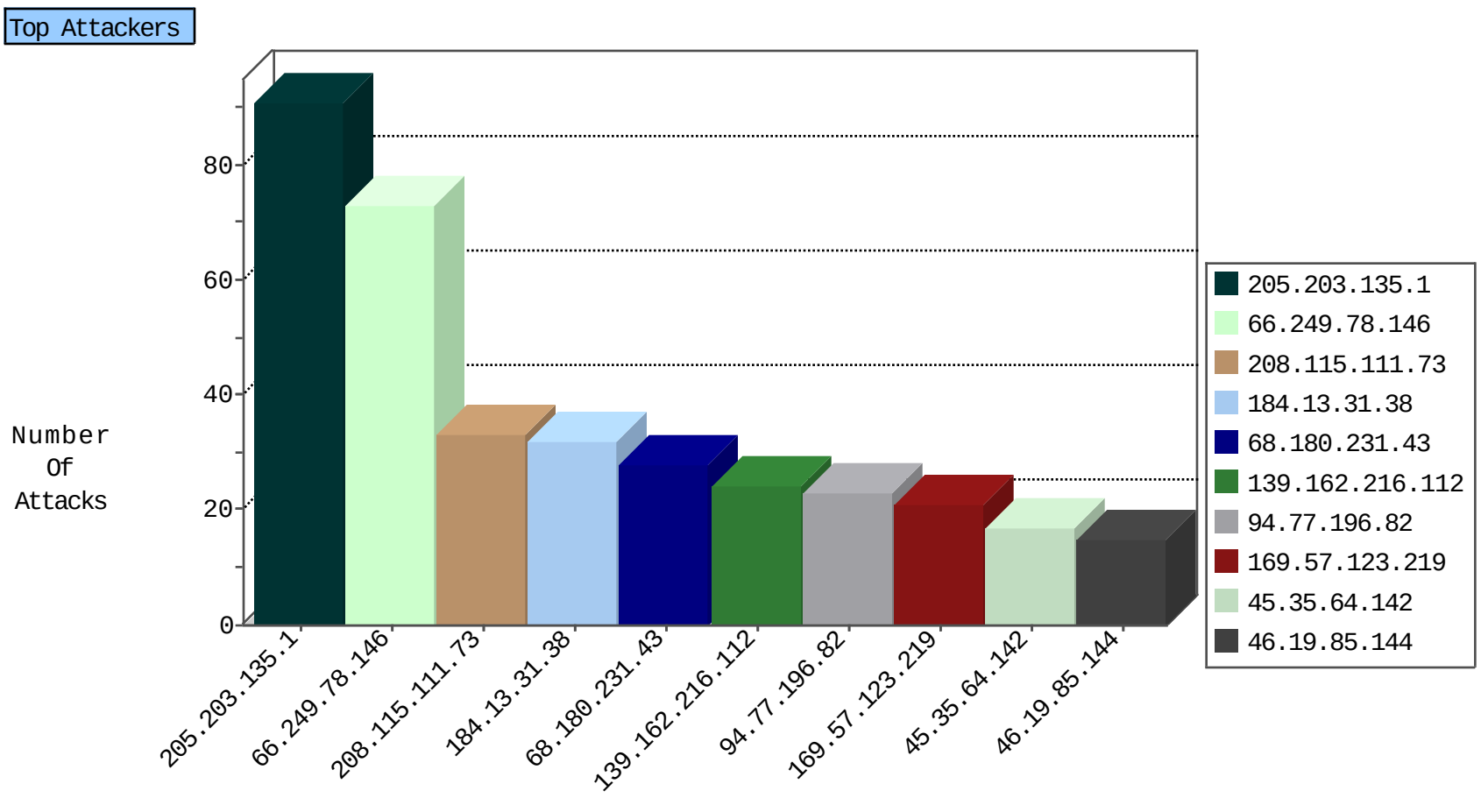
05-03-2016-04:04:05 to 05-03-2016-05:04:05

IDF Under Attack Daily Report

Top Targets



Top Attackers



05-03-2016-04:04:05 to 05-03-2016-05:04:05

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	213
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	1
71.6.216.52	United States	147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	1
71.6.216.55	United States	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
71.6.216.46	United States	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1

05-03-2016-04:04:05 to 05-03-2016-05:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

05-03-2016-04:04:05 to 05-03-2016-05:04:05

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
66.249.66.15	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
106.184.2.29	147.237.77.235	Japan	sviva.idf.il	ET SCAN Potential SSH Scan	1
208.100.26.228	147.237.76.197	United States	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
208.100.26.228	147.237.0.35	United States	akaws.idf.il	ET SCAN Potential SSH Scan	1
183.26.218.211	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
183.26.218.211	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
120.199.111.137	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN NMAP -f -sS	1
106.184.2.29	147.237.8.46	Japan	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
66.240.213.93	147.237.76.200	United States	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
208.100.26.228	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sS window 1024	1
183.26.218.211	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
120.199.111.137	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 2048	1

05-03-2016-04:04:05 to 05-03-2016-05:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	91
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	72
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
169.57.123.219	Mexico	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.85.144	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
14.17.44.216	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
184.13.31.38	United States	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	8
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
198.58.103.115	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
207.46.13.22	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
207.46.13.178	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
184.13.31.38	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
95.221.232.67	Russian Federation	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
87.71.14.83	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.146.235	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
128.69.167.173	Russian Federation	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
184.13.31.38	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
37.26.146.163	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
184.13.31.38	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
157.55.39.106	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
190.102.56.98	Panama	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
5.102.254.44	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
66.249.64.233	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
213.6.8.86	Palestinian Territory, Occupied	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	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
87.71.24.126	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
106.38.241.106	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
184.13.31.38	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
37.26.146.198	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
66.249.78.254	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
187.171.147.252	Mexico	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
176.13.7.200	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.79.102	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.69.23	United States	147.237.72.156	aman.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
75.62.42.52	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
27.227.168.164	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
128.242.249.13	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
46.19.85.144	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.78.213	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

05-03-2016-04:04:05 to 05-03-2016-05:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
91.198.106.180	Netherlands	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 91.198.106.180	Block	5
192.206.203.100	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/mobile	Block	4
46.118.116.239	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1556-en/	Block	2
164.132.161.20	Italy	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/history/history/stm	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/yoman/enlarge.asp	Block	1
194.28.112.51	Netherlands	147.237.77.235	sviva.idf.il	Unauthorized URL Access to www.hagnas.atal.idf.il/hnap1/	Block	1
66.249.64.3	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/civiladministration/minhalnews/pages/default.aspx	Block	1
176.13.7.200	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.79.72	Israel	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/templates/login/login.aspx	Block	1
199.30.24.13	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
109.67.109.146	Israel	147.237.77.170	maarachot.idf.il	Unauthorized HTTP Method	Block	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1380-21254-he/dover.aspx	Block	1
184.105.247.196	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	1
68.180.229.170	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/shared/usercontrols/navmenu/	Block	1
207.46.13.55	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in www.aka.idf.il/chamatz/miktzoa/default.asp	None	1
109.67.109.146	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/5/	Block	1
66.249.78.102	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1362-15556-he/dover.aspx	Block	1
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
216.218.206.66	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to 147.237.77.243/	Block	1
148.251.176.212	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/iturim/asp/displayonesoldier.asp	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	1
194.28.112.51	Netherlands	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
87.71.14.83	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
51.255.65.52	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/iraq/english/	Block	1

05-03-2016-04:04:05 to 05-03-2016-05:04:05