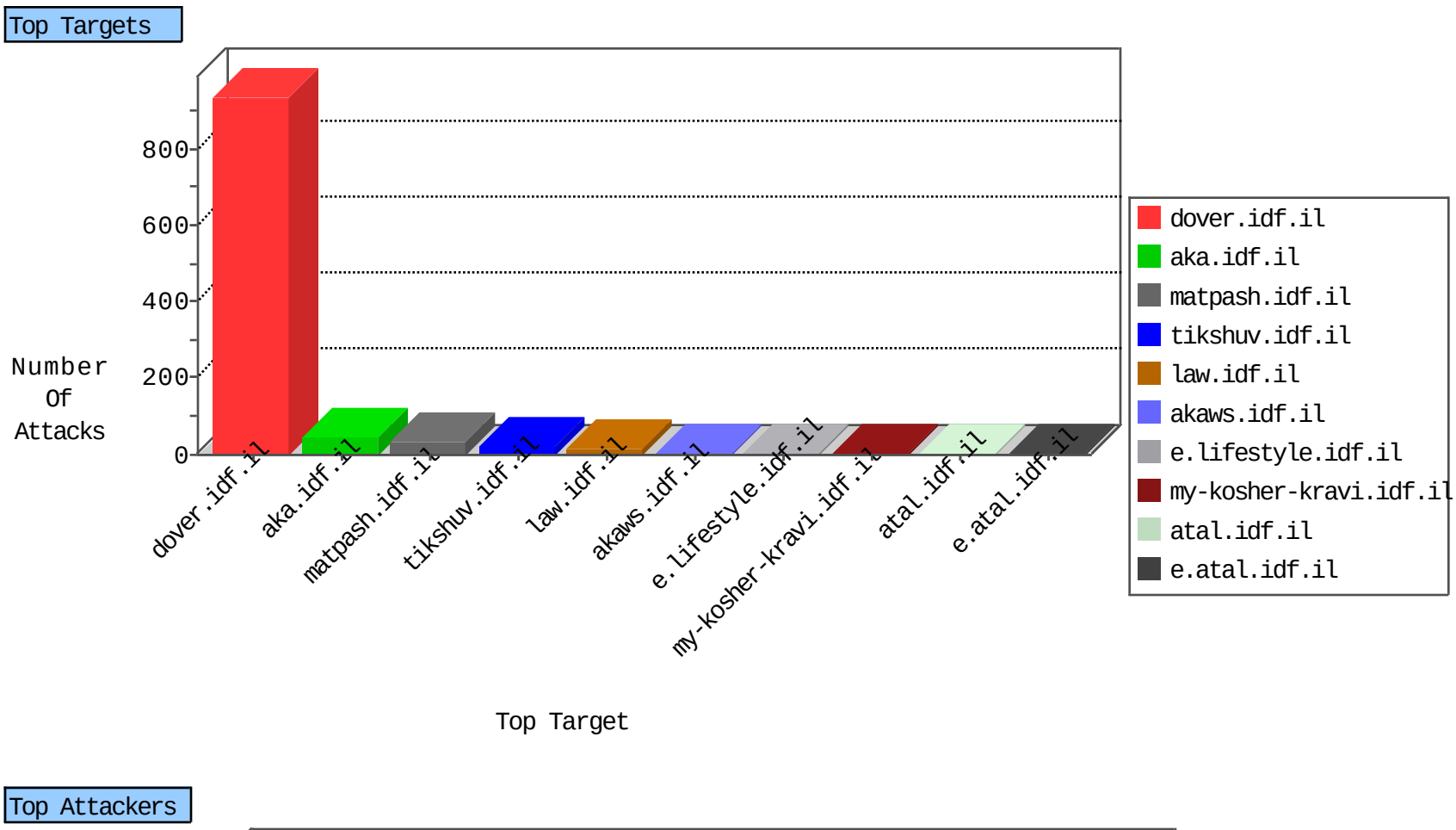
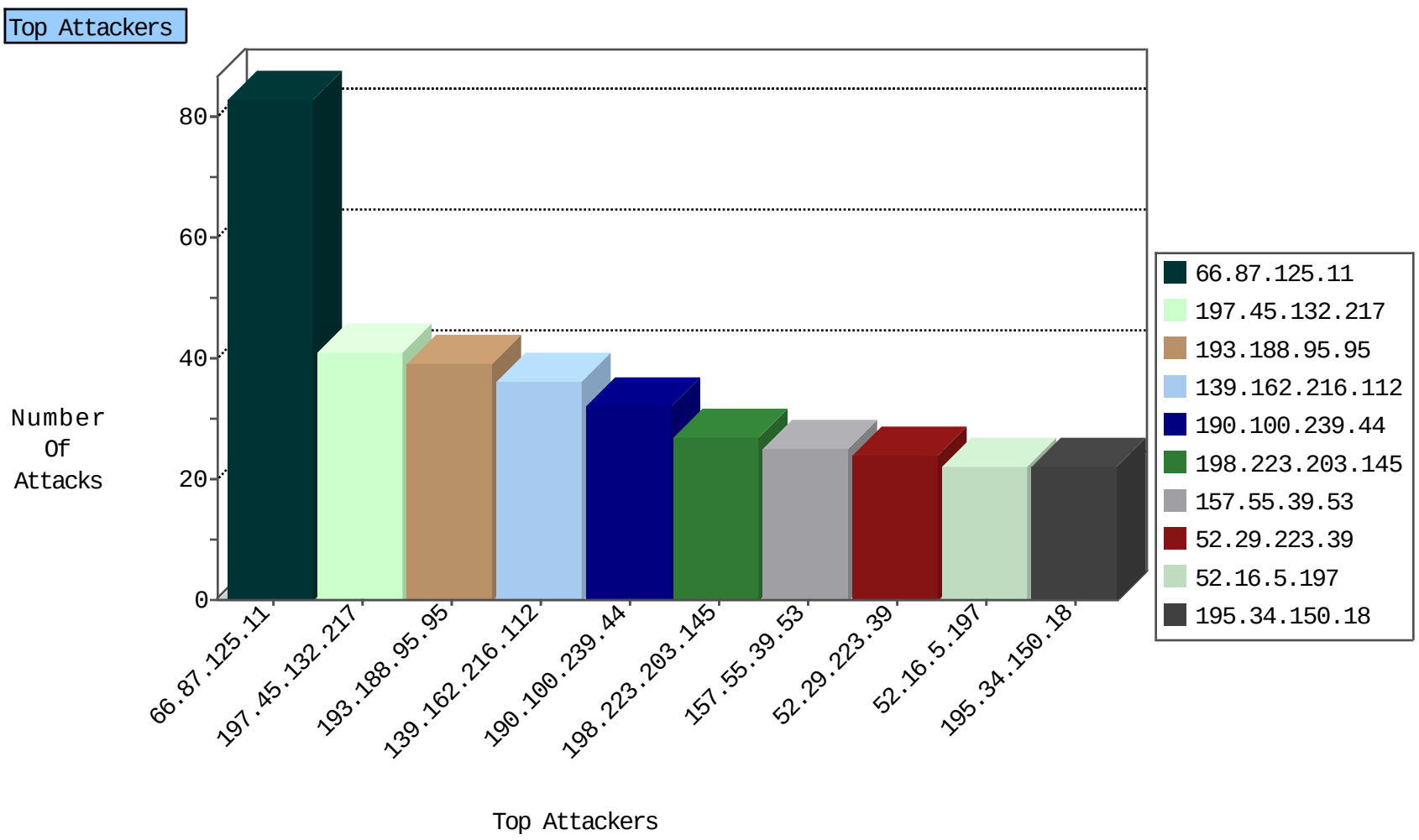
05-01-2016-04:04:01 to 05-01-2016-05:04:01

IDF Under Attack Daily Report





05-01-2016-04:04:01 to 05-01-2016-05:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	9
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3
204.42.253.2	United States	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1
185.94.111.1	Russian Federation	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1
185.94.111.1	Russian Federation	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1

05-01-2016-04:04:01 to 05-01-2016-05:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
52.1.90.117	United States	147.237.77.216	dover.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

05-01-2016-04:04:01 to 05-01-2016-05:04:01

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
91.227.164.5	147.237.77.216	Israel	dover.idf.il	GPL SCAN myscan	2
14.161.38.245	147.237.76.198	Vietnam	e.yohalan.idf.il	ET SCAN Potential SSH Scan	2
91.227.164.5	147.237.77.216	Israel	dover.idf.il	INDICATOR-SCAN myscan	2
220.249.194.151	147.237.76.86	China	navy.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.78.38	147.237.0.16	Netherlands	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
220.231.195.122	147.237.0.35	China	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
66.240.213.93	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sS window 1024	1
14.161.38.245	147.237.76.202	Vietnam	e.halag.idf.il	ET SCAN Potential SSH Scan	1
104.197.72.206	147.237.76.177	United States	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
14.161.38.245	147.237.76.148	Vietnam	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
104.171.122.176	147.237.77.227	United States	e.hamaz.idf.il	ET SCAN NMAP -sS window 3072	1
104.171.122.176	147.237.8.24	United States	e.lifestyle.idf.il	ET SCAN NMAP -sS window 2048	1
93.189.26.18	147.237.77.61	Austria	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.78.38	147.237.76.44	Netherlands	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
220.231.195.122	147.237.0.35	China	akaws.idf.il	ET SCAN NMAP -sS window 3072	1
78.63.82.209	147.237.77.216	Lithuania	dover.idf.il	Xenu Link Sleuth User Agent	1
208.100.26.228	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
66.240.213.93	147.237.77.121	United States	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
104.197.72.206	147.237.76.199	United States	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
104.171.122.176	147.237.77.227	United States	e.hamaz.idf.il	ET SCAN NMAP -sS window 4096	1
14.161.38.245	147.237.0.16	Vietnam	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
104.171.122.176	147.237.8.24	United States	e.lifestyle.idf.il	ET SCAN NMAP -sS window 3072	1
104.171.122.176	147.237.8.24	United States	e.lifestyle.idf.il	ET SCAN NMAP -f -sS	1
89.248.167.131	147.237.77.233	Netherlands	atal.idf.il	ET SCAN Potential SSH Scan	1

05-01-2016-04:04:01 to 05-01-2016-05:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.87.125.11	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	83
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
193.188.95.95	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
157.55.39.53	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
198.223.203.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
136.243.5.203	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
66.249.66.184	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
157.55.39.106	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
198.58.103.115	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
162.243.99.146	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
162.243.126.57	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
175.136.91.80	Malaysia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
190.100.239.44	Chile	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
207.46.13.22	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
190.100.239.44	Chile	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
130.203.136.75	United States	147.237.77.74	law.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	8
190.100.239.44	Chile	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	8
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
204.79.180.8	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
92.247.181.29	Bulgaria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
185.3.147.246	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.130.227.133	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
204.79.180.163	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
204.79.180.86	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
204.79.180.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
54.162.224.26	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
37.26.148.191	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
204.79.180.33	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
192.249.66.247	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
130.211.130.218	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
24.236.84.108	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
204.79.180.223	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
204.79.180.5	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
204.79.180.171	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
204.79.180.114	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
204.79.180.236	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
204.79.180.104	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3

05-01-2016-04:04:01 to 05-01-2016-05:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
157.55.39.106	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/india/	Block	1
5.39.222.159	Netherlands	147.237.0.19	madim.atal.idf.il	Distributed Unauthorized URL Access on 147.237.0.19/	Block	1
208.115.113.82	United States	147.237.0.34	tikshuv.idf.il	Parameter Type Violation docId in tikshuv.idf.il/site/story.aspx	Block	1
80.246.136.10	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	1
157.55.39.122	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/templates/journalview/journalview.aspx	Block	1
54.184.28.94	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1397-en/dover.aspx	Block	1
157.55.2.142	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
207.46.13.104	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/935-4489-	Block	1
66.249.78.246	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/smalim/showbig.aspx	Block	1
157.55.39.43	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/templates/oprolescategory/oprolescategory.in.aspx	Block	1
207.46.13.143	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/templates/general/general.aspx	Block	1
68.180.229.241	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1038-ar/cogat.aspx	Block	1
157.55.39.85	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/modules/shared/usercontrols/navmenu/mazi.idf.il	Block	1
2.53.53.155	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/templates/news/mobile	Block	1
207.241.237.229	United States	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to kosher-kravi.idf.il/templates/homepage/homepage.aspx	Block	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1399-en/dover.aspx	Block	1

05-01-2016-04:04:01 to 05-01-2016-05:04:01