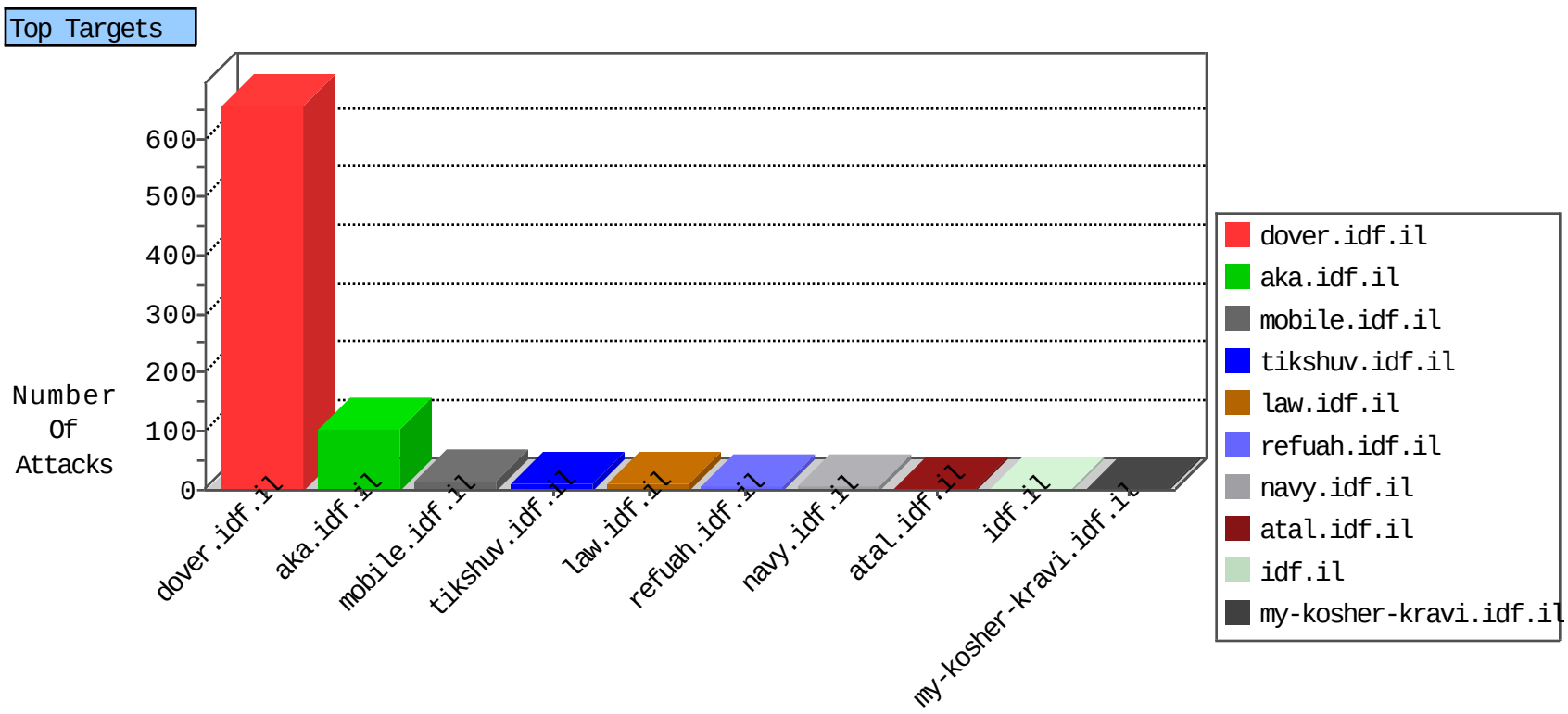
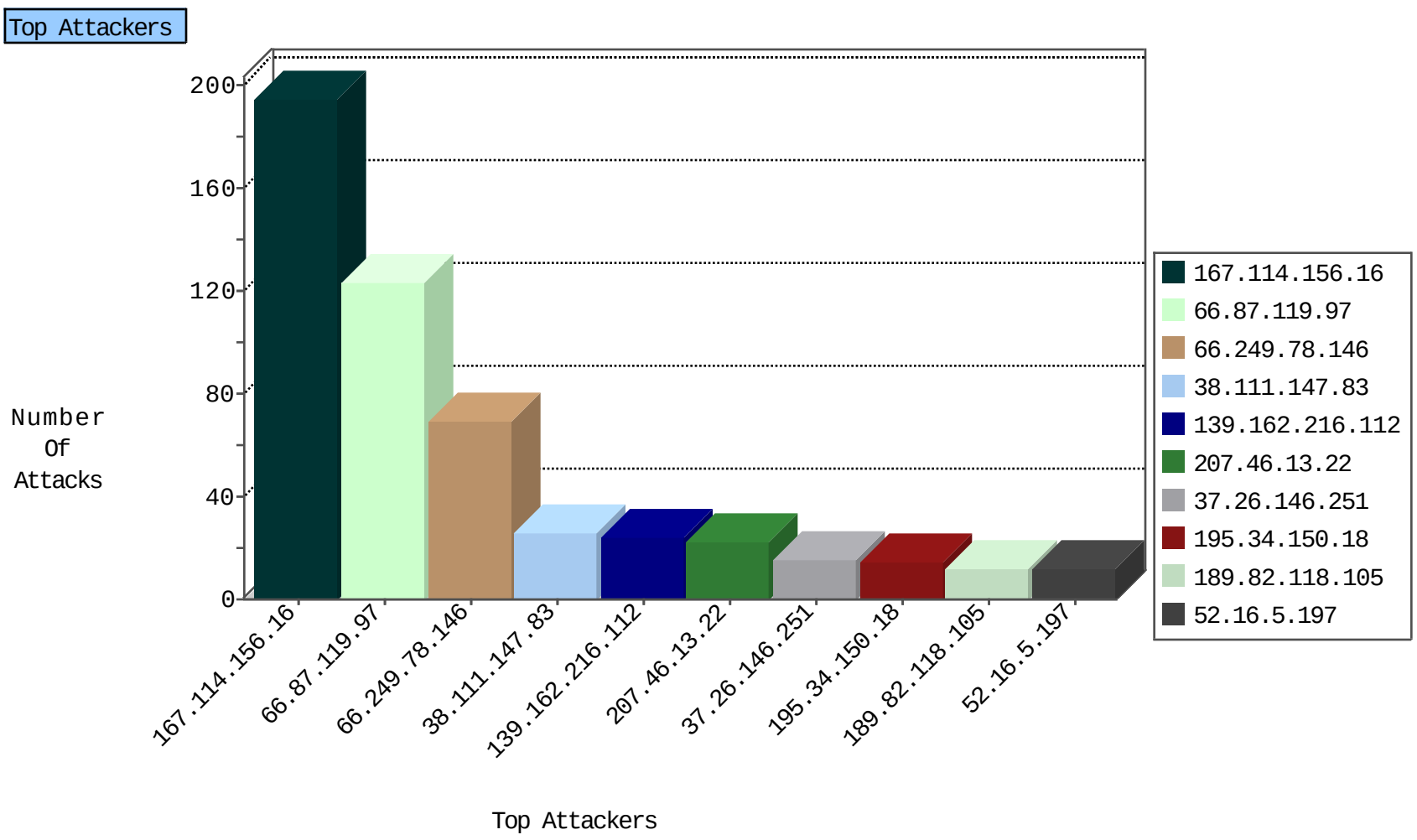
05-01-2016-03:04:01 to 05-01-2016-04:04:01

IDF Under Attack Daily Report





05-01-2016-03:04:01 to 05-01-2016-04:04:01

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	HTTP-POST-Segmented-DoS	dest-reset	8077
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	1086
79.181.149.214	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	1
66.240.192.138	United States	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1
204.42.253.2	United States	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
123.59.59.52	China	147.237.77.170	maarachot.idf.il	block-sp-traf1	drop	1

05-01-2016-03:04:01 to 05-01-2016-04:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

05-01-2016-03:04:01 to 05-01-2016-04:04:01

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
85.189.179.48	147.237.0.35	United Kingdom	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
13.92.103.193	147.237.0.33	United States	idf.il	ET SCAN NMAP -sS window 3072	1
13.92.103.193	147.237.0.33	United States	idf.il	ET SCAN NMAP -f -sS	1
113.240.250.154	147.237.77.233	China	atal.idf.il	ET SCAN NMAP -sS window 1024	1
13.92.100.128	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sS window 1024	1
113.240.250.154	147.237.77.205	China	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
111.68.104.195	147.237.76.86	Pakistan	navy.idf.il	ET SCAN NMAP -sS window 2048	1
107.158.255.194	147.237.77.234	United States	halag.idf.il	ET SCAN NMAP -sS window 2048	1
107.158.255.194	147.237.77.234	United States	halag.idf.il	ET SCAN NMAP -f -sS	1
93.189.26.18	147.237.77.74	Austria	law.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
13.92.103.193	147.237.0.33	United States	idf.il	ET SCAN NMAP -sS window 2048	1
130.211.77.81	147.237.8.27	United States	e.madim.atal.idf.i	ET SCAN Potential VNC Scan 5900-5920	1
13.92.100.128	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sS window 4096	1
113.240.250.154	147.237.77.227	China	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
111.68.104.195	147.237.76.86	Pakistan	navy.idf.il	ET SCAN NMAP -sS window 4096	1
111.68.104.195	147.237.76.86	Pakistan	navy.idf.il	ET SCAN NMAP -f -sS	1
107.158.255.194	147.237.77.234	United States	halag.idf.il	ET SCAN NMAP -sS window 1024	1
104.197.72.206	147.237.8.28	United States	e.mobile-ks.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

05-01-2016-03:04:01 to 05-01-2016-04:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.87.119.97	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	123
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	69
38.111.147.83	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
207.46.13.22	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
37.26.146.251	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.103.114	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
66.249.66.184	United States	147.237.0.34	tikshuv.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
189.82.118.105	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.103.158	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
87.203.102.200	Greece	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
157.55.39.53	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
84.132.35.90	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	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
54.72.0.55	Ireland	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	6
45.35.64.142	United States	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
38.108.87.20	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
89.138.201.2	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
70.198.203.121	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
109.65.186.97	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
96.224.0.54	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
38.111.147.88	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
176.13.6.177	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
66.44.112.104	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
95.186.89.221	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
185.44.151.206	Germany	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
109.253.150.23	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
88.191.204.49	France	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
109.253.225.50	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.165	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
93.13.36.93	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
185.18.206.194	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
46.19.86.46	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.163.117.90	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
217.132.87.189	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
185.3.144.82	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
185.18.206.194	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
86.25.51.239	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
192.249.66.247	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
79.179.13.155	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2

05-01-2016-03:04:01 to 05-01-2016-04:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.120.125.130	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	2
159.255.164.55	Iraq	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.15/	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
216.218.206.66	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	1
109.92.189.61		147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/	Block	1
38.111.147.83	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
159.255.164.55	Iraq	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
5.39.222.159	Netherlands	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to 147.237.76.147/	Block	1
220.255.97.209	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
109.253.145.21	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-he/dover.aspx	Block	1
49.177.22.136	Australia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/mobile	Block	1
176.13.6.177	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
68.180.229.241	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/2065-he/cogat.aspx	Block	1
36.250.175.18	China	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/miluim/about.aspx	Block	1
131.253.25.182	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
54.86.145.194	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/&lt	Block	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1133-ar/dover.aspx	Block	1
36.250.175.18	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 36.250.175.18	Block	1
131.253.25.205	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
66.249.64.72	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/0/61340.jpg	Block	1
207.46.13.178	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-19405-he/dover.aspx)	Block	1
89.138.201.2	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
36.250.175.18	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	1

05-01-2016-03:04:01 to 05-01-2016-04:04:01