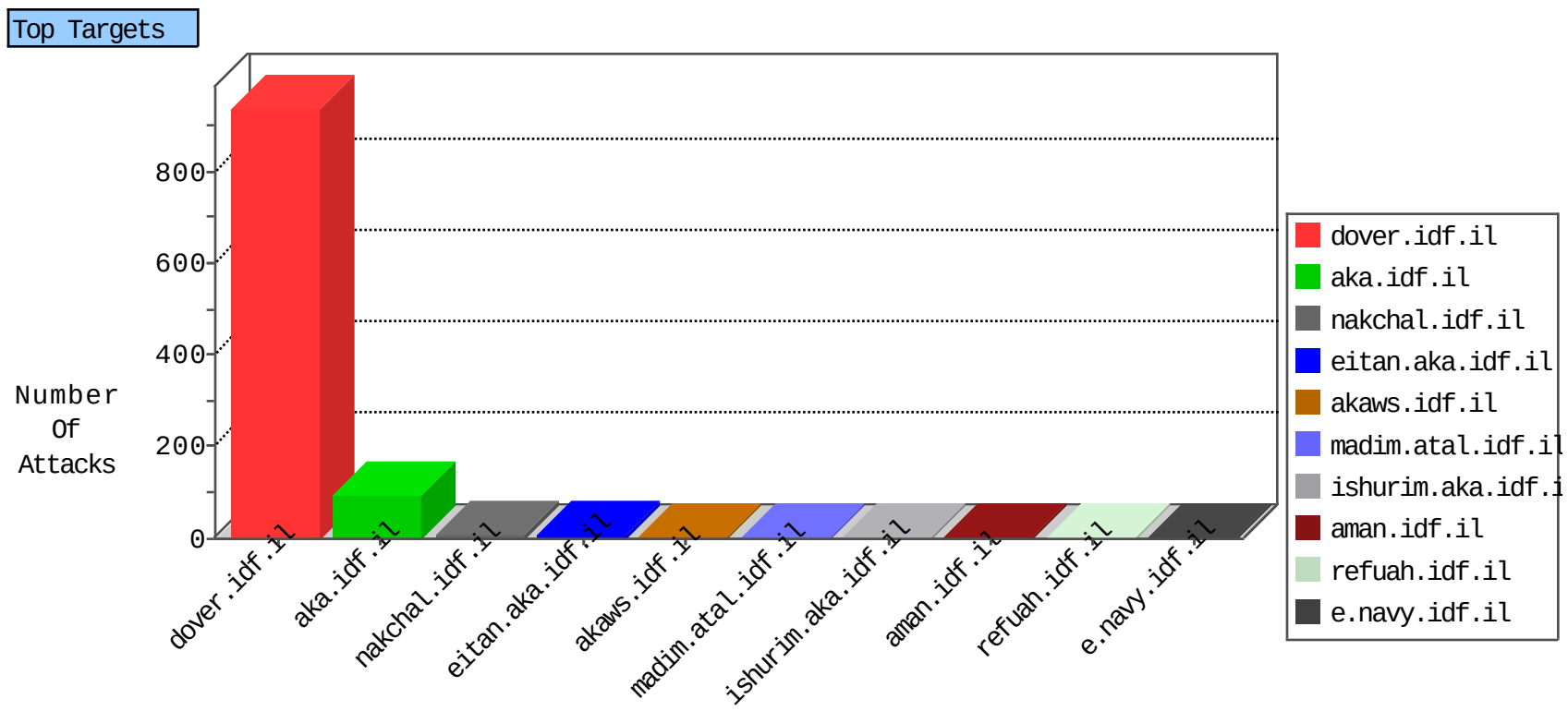
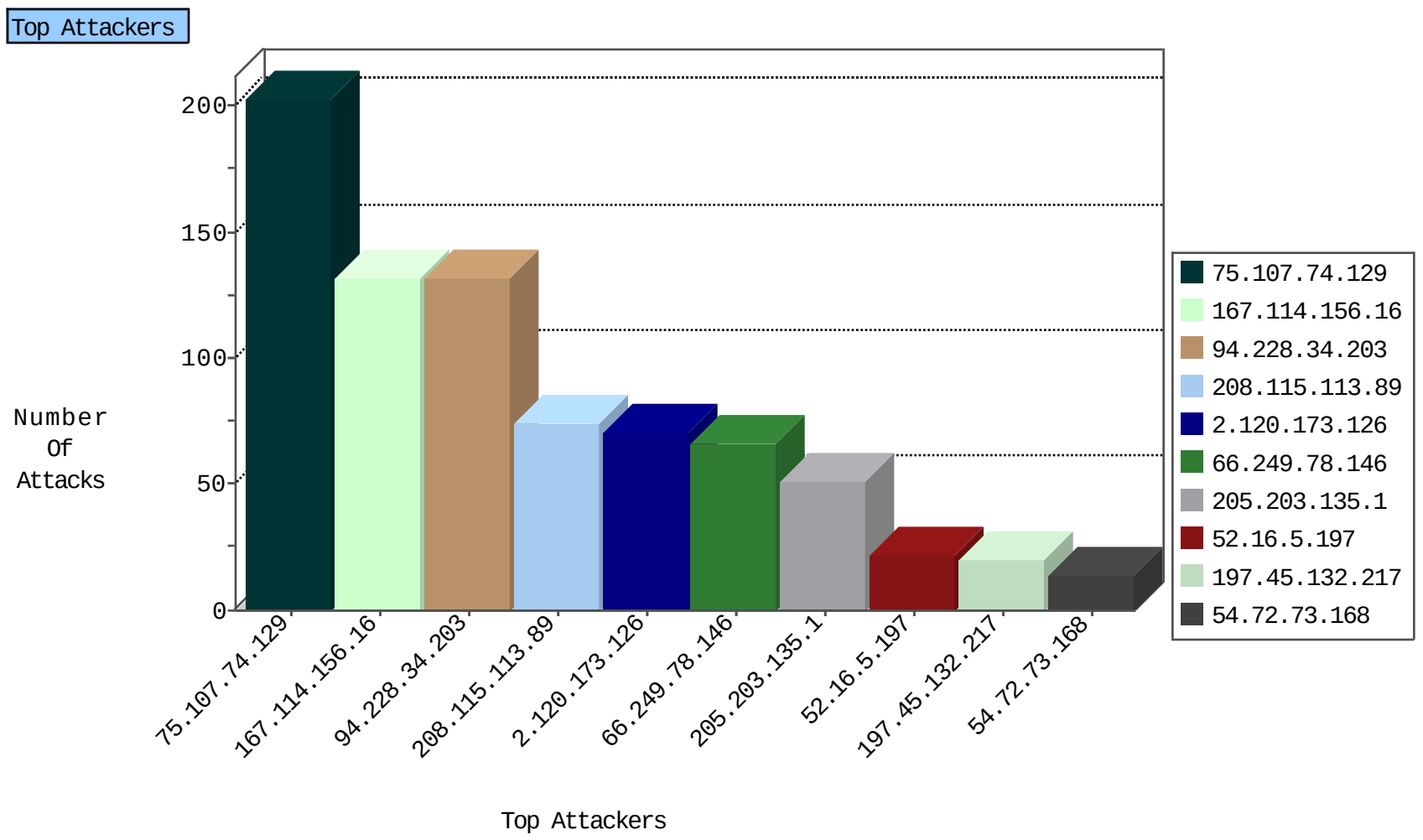
04-28-2016-05:04:06 to 04-28-2016-06:04:06

IDF Under Attack Daily Report

Top Targets



Top Attackers



04-28-2016-05:04:06 to 04-28-2016-06:04:06

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	6409
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	1589
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	2
52.90.101.121	United States	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	1
212.143.254.66	Israel	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
52.90.101.121	United States	147.237.76.34	yohalan.idf.il	Block_Ntp_All_Net	drop	1

04-28-2016-05:04:06 to 04-28-2016-06:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

04-28-2016-05:04:06 to 04-28-2016-06:04:06

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
163.172.140.23	147.237.72.167	United Kingdom	ishurim.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
89.216.119.94	147.237.72.217		e.idf.il	ET SCAN NMAP -sS window 1024	1
58.218.204.211	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1
58.218.204.211	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
42.114.176.102	147.237.8.24	Vietnam	e.lifestyle.idf.il	ET SCAN NMAP -sS window 2048	1
198.20.69.74	147.237.76.147	United States	chinuch.aka.idf.il	ET DROP Dshield Block Listed Source	1
40.76.60.52	147.237.72.156	United States	aman.idf.il	ET SCAN NMAP -sS window 4096	1
195.216.176.244	147.237.8.50	Latvia	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
40.76.60.52	147.237.72.156	United States	aman.idf.il	ET SCAN NMAP -f -sS	1
173.193.130.50	147.237.0.35	United States	akaws.idf.il	ET SCAN NMAP -sS window 3072	1
163.172.140.23	147.237.76.198	United Kingdom	e.yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
163.172.140.23	147.237.72.167	United Kingdom	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.78.38	147.237.76.34	Netherlands	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
58.218.204.211	147.237.76.39	China	mobile.meitav.idf.i	ET SCAN Potential SSH Scan	1
58.218.204.211	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
221.9.166.42	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
42.114.176.102	147.237.8.24	Vietnam	e.lifestyle.idf.il	ET SCAN NMAP -f -sS	1
195.216.176.244	147.237.76.86	Latvia	navy.idf.il	ET SCAN NMAP -sS window 1024	1
40.76.60.52	147.237.72.156	United States	aman.idf.il	ET SCAN NMAP -sS window 2048	1
173.193.130.50	147.237.0.35	United States	akaws.idf.il	ET SCAN NMAP -sS window 1024	1

04-28-2016-05:04:06 to 04-28-2016-06:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
75.107.74.129	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	183
94.228.34.203	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	132
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	74
2.120.173.126	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	71
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	66
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
75.107.74.129	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	18
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
139.162.216.112	United States	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
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
162.243.104.237	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
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
157.55.39.106	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
207.46.13.137	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
157.55.39.204	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
104.13.249.81	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
62.16.67.30	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
192.249.66.247	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
62.16.72.138	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
207.46.13.2	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
92.247.181.31	Bulgaria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
70.51.3.219	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
199.30.25.184	United States	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
104.13.249.81	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
37.26.148.208	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
174.37.194.144	United States	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
46.19.85.7	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
70.82.118.4	Canada	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	3
177.193.23.152	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
141.8.183.16	Russian Federation	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	2
95.186.198.81	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
141.8.184.13	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
88.191.108.74	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
64.12.253.130	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
123.254.121.195	Australia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
51.255.65.75	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
130.193.37.10	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
199.30.25.3	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
54.221.158.153	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
184.105.247.239	United States	147.237.8.24	e.lifestyle.idf	Geo-location enforcement	Geo-location inbound enforcement	drop	1
52.29.21.27	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1

04-28-2016-05:04:06 to 04-28-2016-06:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
186.202.95.56	Brazil	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 186.202.95.56	Block	5
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	2
46.117.223.120	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
66.249.66.125	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8871-he/refuah.aspx	Block	1
141.212.122.161	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
66.249.64.143	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/news.aspx	Block	1
186.202.95.56	Brazil	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-admin/	Block	1
66.249.69.124	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
157.55.39.106	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-17615-en/dover.asp	Block	1
198.58.103.92	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-he/www.idf.il	Block	1
74.6.254.127	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/0/size220x0/16770.jpg	Block	1
37.26.148.208	Israel	147.237.0.19	madim.atal.idf.i	Suspicious Response Code	Block	1
157.55.39.135	United States	147.237.72.166	aka.idf.il	Unknown Parameter catId in www.aka.idf.il/kamlar/	None	1
66.249.66.121	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/3/2363.jpg	Block	1
199.30.24.157	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/scripts.asmx/getjs	Block	1
74.82.47.4	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
157.55.39.204	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.66.123	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/6/size100x0/2796.jpg	Block	1
207.46.13.2	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
130.193.51.91	Russian Federation	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to eitan.aka.idf.il/1105-en/contactus.aspx	Block	1
51.255.65.76	France	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/smalim/html/6.asp	Block	1

04-28-2016-05:04:06 to 04-28-2016-06:04:06