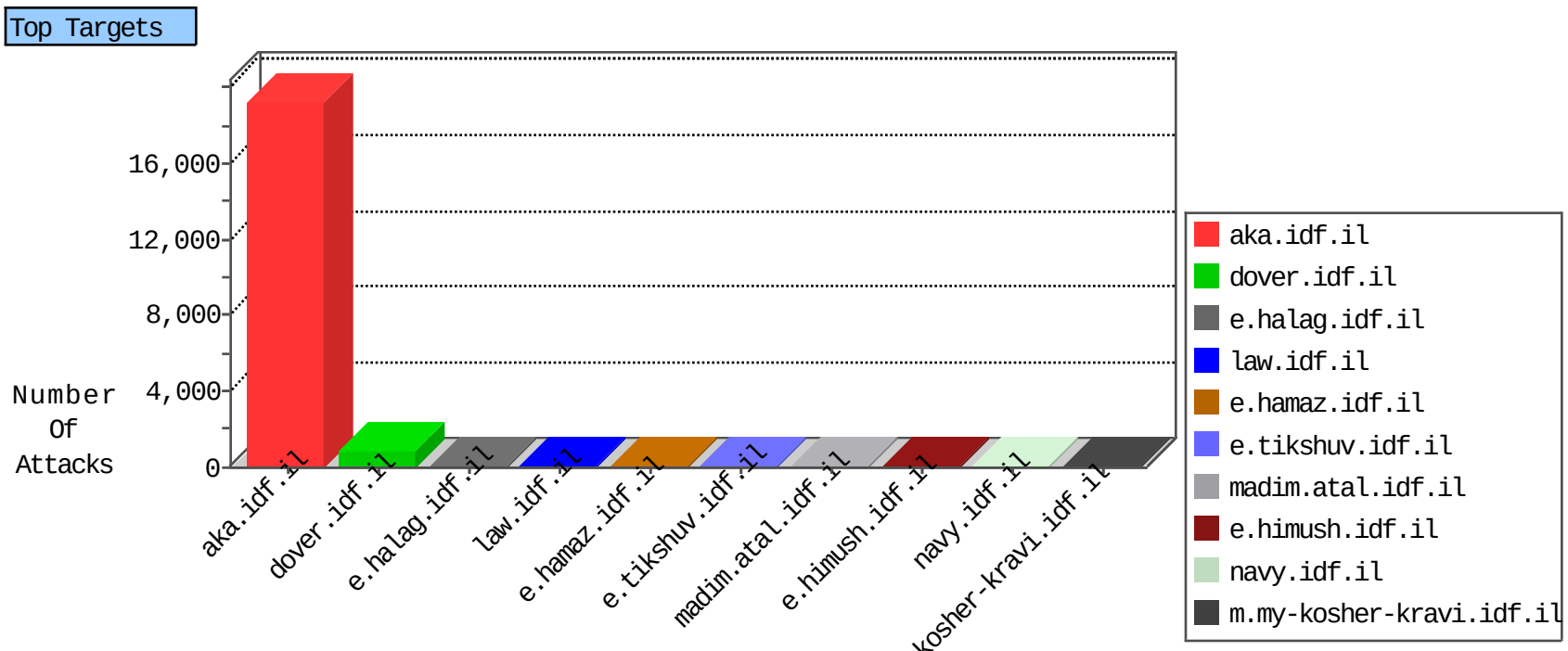
04-20-2016-05:04:08 to 04-20-2016-06:04:08

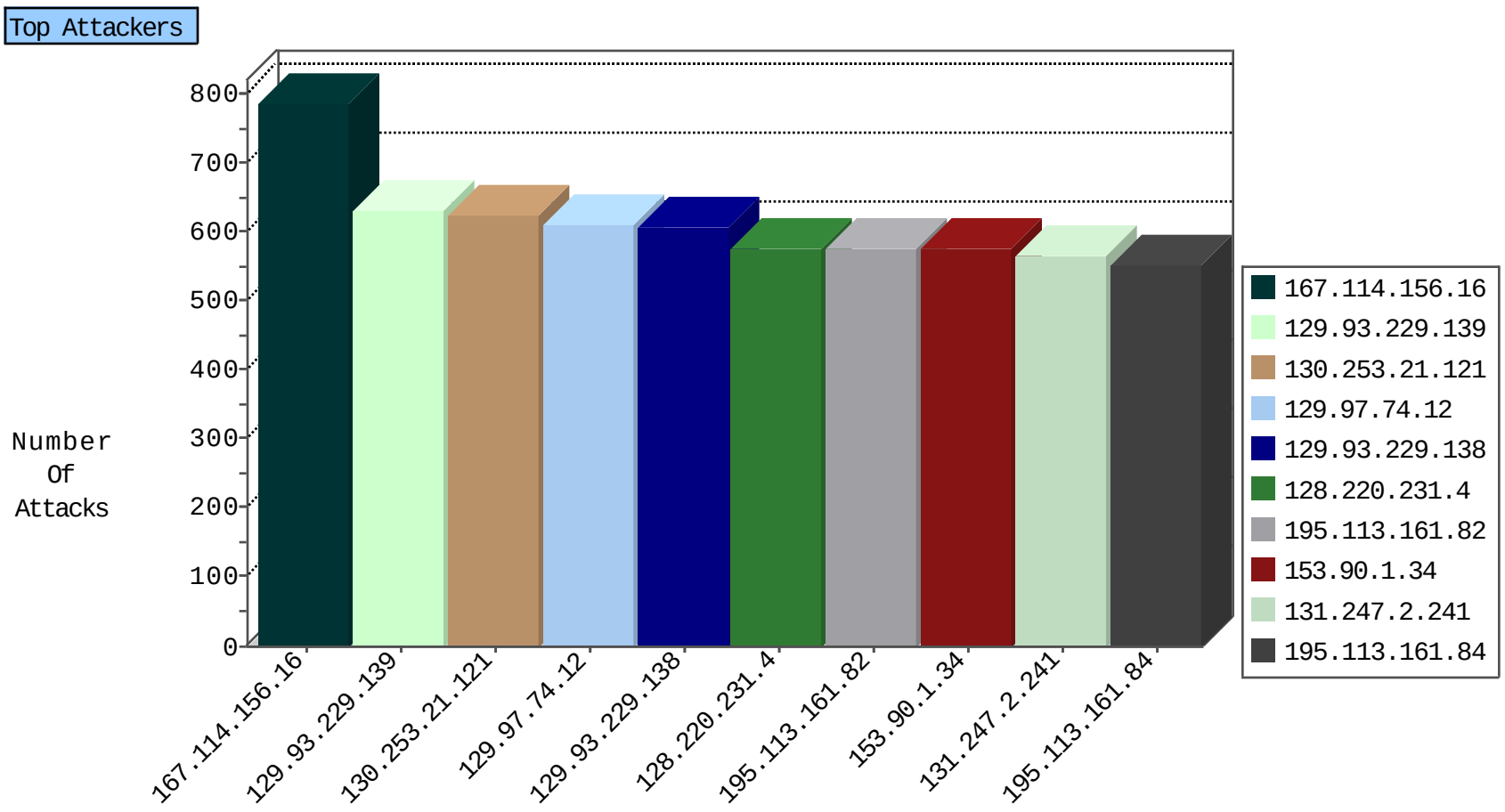
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

04-20-2016-05:04:08 to 04-20-2016-06:04:08

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	Block_Ip_Web_In	drop	788
206.207.248.35	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
74.82.47.2	United States	147.237.77.235	sviva.idf.il	Block_Udp_All_Nets	drop	1
74.82.47.50	United States	147.237.77.233	atal.idf.il	Block_Udp_All_Nets	drop	1
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1

04-20-2016-05:04:08 to 04-20-2016-06:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

04-20-2016-05:04:08 to 04-20-2016-06:04:08

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
66.249.78.254	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
104.207.142.91	147.237.77.179	United States	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
80.82.78.38	147.237.77.235	Netherlands	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
104.207.142.91	147.237.77.61	United States	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
104.207.142.91	147.237.76.176	United States	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
14.161.36.92	147.237.76.199	Vietnam	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
104.207.142.91	147.237.76.34	United States	yohalan.idf.il	ET SCAN Potential SSH Scan	1
104.207.142.91	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
104.207.142.91	147.237.8.50	United States	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
104.207.142.91	147.237.8.14	United States	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
107.158.255.194	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -sS window 4096	1
104.207.142.91	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
104.207.142.91	147.237.77.205	United States	prisha.idf.il	ET SCAN Potential SSH Scan	1
101.200.82.129	147.237.76.30	China	himush.idf.il	ET SCAN NMAP -sS window 1024	1
104.207.142.91	147.237.77.170	United States	maarachot.idf.il	ET SCAN Potential SSH Scan	1
80.82.78.38	147.237.77.234	Netherlands	halag.idf.il	ET SCAN NMAP -sS window 1024	1
104.207.142.91	147.237.76.177	United States	ncore.idf.il	ET SCAN Potential SSH Scan	1
66.249.64.253	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
104.207.142.91	147.237.76.42	United States	refuah.idf.il	ET SCAN Potential SSH Scan	1
14.161.36.92	147.237.72.166	Vietnam	aka.idf.il	ET SCAN NMAP -sS window 1024	1
104.207.142.91	147.237.76.31	United States	nakchal.idf.il	ET SCAN Potential SSH Scan	1
104.207.142.91	147.237.72.166	United States	aka.idf.il	ET SCAN Potential SSH Scan	1
197.89.117.144	147.237.72.14	South Africa	dover.idf.il(old)	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
104.207.142.91	147.237.8.28	United States	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
185.34.0.141	147.237.72.14	Germany	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
104.207.142.91	147.237.0.200	United States	m4u.idf.il	ET SCAN Potential SSH Scan	1
107.158.255.194	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -sS window 3072	1
104.207.142.91	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1

04-20-2016-05:04:08 to 04-20-2016-06:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
129.93.229.139	United States	147.237.72.166	aka.idf.il	drop	Echo Request	drop	632
130.253.21.121	United States	147.237.72.166	aka.idf.il	drop	Echo Request	drop	624
129.97.74.12	Canada	147.237.72.166	aka.idf.il	drop	Echo Request	drop	612
129.93.229.138	United States	147.237.72.166	aka.idf.il	drop	Echo Request	drop	608
153.90.1.34	United States	147.237.72.166	aka.idf.il	drop	Echo Request	drop	576
128.220.231.4	United States	147.237.72.166	aka.idf.il	drop	Echo Request	drop	576
195.113.161.82	Czech Republic	147.237.72.166	aka.idf.il	drop	Echo Request	drop	576
131.247.2.241	United States	147.237.72.166	aka.idf.il	drop	Echo Request	drop	568
195.113.161.84	Czech Republic	147.237.72.166	aka.idf.il	drop	Echo Request	drop	552
128.42.142.45	United States	147.237.72.166	aka.idf.il	drop	Echo Request	drop	544
130.194.252.8	Australia	147.237.72.166	aka.idf.il	drop	Echo Request	drop	540
128.227.150.12	United States	147.237.72.166	aka.idf.il	drop	Echo Request	drop	516
200.19.159.34	Brazil	147.237.72.166	aka.idf.il	drop	Echo Request	drop	510
193.1.13.14	Ireland	147.237.72.166	aka.idf.il	drop	Echo Request	drop	508
165.230.49.115	United States	147.237.72.166	aka.idf.il	drop	Echo Request	drop	504
195.113.161.83	Czech Republic	147.237.72.166	aka.idf.il	drop	Echo Request	drop	488
129.97.74.14	Canada	147.237.72.166	aka.idf.il	drop	Echo Request	drop	488
200.19.159.35	Brazil	147.237.72.166	aka.idf.il	drop	Echo Request	drop	484
132.66.194.80	Israel	147.237.72.166	aka.idf.il	drop	Echo Request	drop	480
216.48.80.12	Canada	147.237.72.166	aka.idf.il	drop	Echo Request	drop	480
206.207.248.38	United States	147.237.72.166	aka.idf.il	drop	Echo Request	drop	476
198.82.160.221	United States	147.237.72.166	aka.idf.il	drop	Echo Request	drop	460
139.78.141.243	United States	147.237.72.166	aka.idf.il	drop	Echo Request	drop	460
194.254.215.12	France	147.237.72.166	aka.idf.il	drop	Echo Request	drop	460
129.63.159.102	United States	147.237.72.166	aka.idf.il	drop	Echo Request	drop	460
129.32.84.160	United States	147.237.72.166	aka.idf.il	drop	Echo Request	drop	448
198.82.160.238	United States	147.237.72.166	aka.idf.il	drop	Echo Request	drop	440
128.223.8.112	United States	147.237.72.166	aka.idf.il	drop	Echo Request	drop	432
130.195.4.69	New Zealand	147.237.72.166	aka.idf.il	drop	Echo Request	drop	420
130.217.77.2	New Zealand	147.237.72.166	aka.idf.il	drop	Echo Request	drop	416
194.199.68.166	France	147.237.72.166	aka.idf.il	drop	Echo Request	drop	413
156.56.250.227	United States	147.237.72.166	aka.idf.il	drop	Echo Request	drop	378
198.83.85.46	United States	147.237.72.166	aka.idf.il	drop	Echo Request	drop	372
206.207.248.35	United States	147.237.72.166	aka.idf.il	drop	Echo Request	drop	364
194.29.178.14	Poland	147.237.72.166	aka.idf.il	drop	Echo Request	drop	352
133.9.81.164	Japan	147.237.72.166	aka.idf.il	drop	Echo Request	drop	316
129.69.210.97	Germany	147.237.72.166	aka.idf.il	drop	Echo Request	drop	300
198.133.224.147	United States	147.237.72.166	aka.idf.il	drop	Echo Request	drop	288
141.22.213.34	Germany	147.237.72.166	aka.idf.il	drop	Echo Request	drop	264
134.197.113.3	United States	147.237.72.166	aka.idf.il	drop	Echo Request	drop	204
143.225.229.236	Italy	147.237.72.166	aka.idf.il	drop	Echo Request	drop	204
204.85.191.11	United States	147.237.72.166	aka.idf.il	drop	Echo Request	drop	188
165.242.90.128	Japan	147.237.72.166	aka.idf.il	drop	Echo Request	drop	156
204.85.191.10	United States	147.237.72.166	aka.idf.il	drop	Echo Request	drop	80
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
82.80.168.133	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid sequence number	monitor	11
116.48.145.55	Hong Kong	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	6
74.62.159.211	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
112.5.77.239	China	147.237.76.198	e.yohalan.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	6

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 141.8.132.78	Block	3
66.102.6.191	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
80.246.130.8	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/mobile	Block	2
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
46.19.85.173	Israel	147.237.77.216	dover.idf.il	Illegal HTTP Version _pk_ses.20.8afc=*	Block	1
212.227.221.39	Germany	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/test/wp-admin/	Block	1
130.185.155.10	Sweden	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
74.208.16.87	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/old/wp-admin/	Block	1
66.249.64.13	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
199.30.24.153	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
84.95.208.20	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/templates/news/piwik.php	Block	1
66.249.78.153	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/mobile/main/smalim/showbig.aspx	Block	1
216.218.206.66	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.16/	Block	1
46.19.85.173	Israel	147.237.77.216	dover.idf.il	Malformed URL _pk_id.20.8afc=2ab1ae947776970f.1440438120.3.1461120884.1461120884.;	Block	1
77.75.79.109	Czech Republic	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/page/29/	Block	1
66.249.64.50	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/redirects/ssl-redirect.html	Block	1
207.46.13.116	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
93.160.60.22	Denmark	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english	Block	1
66.249.78.254	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/m/	Block	1
46.19.85.173	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method 2C%22https%3A%2F%2Fhe.m.wikipedia.org%2F%22%5D; in URL _pk_id.20.8afc=2ab1ae947776970f.1440438120.3.1461120884.1461120884.	Block	1
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-11677-	Block	1
80.246.130.8	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/templates/general/mobile	Block	1
66.249.64.253	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
207.46.13.116	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/promotioncube/	Block	1
108.59.8.70	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/8/4148.pdf&gt	Block	1
68.180.230.108	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in www.nakhal.idf.il/1117-he/nakhal.aspx	Block	1
50.62.161.212	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp/wp-admin/	Block	1
141.8.183.16	Russian Federation	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/901-9903-	Block	1
66.249.69.89	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1437-he/atal.aspx	Block	1
46.19.85.173	Israel	147.237.77.216	dover.idf.il	Abnormally Long Request request version	Block	1
208.80.155.255	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/iturim/asp/displayonesoldier.asp	Block	1
130.185.155.10	Sweden	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
74.82.47.3	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
180.76.15.143	China	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9724-he/refuah.aspx	Block	1
84.95.208.20	Israel	147.237.77.74	law.idf.il	PHP Attempt	Block	1