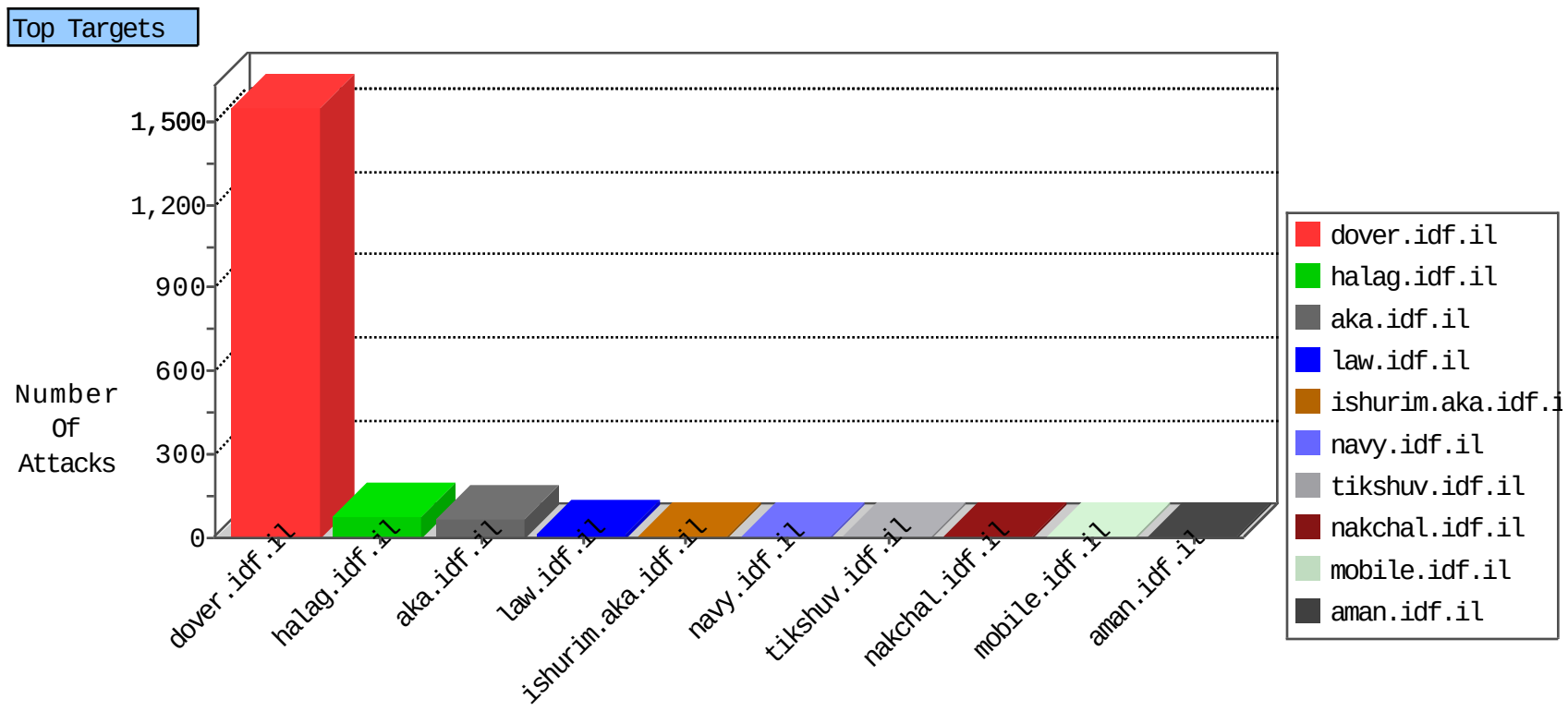
04-27-2016-06:04:05 to 04-27-2016-07:04:05

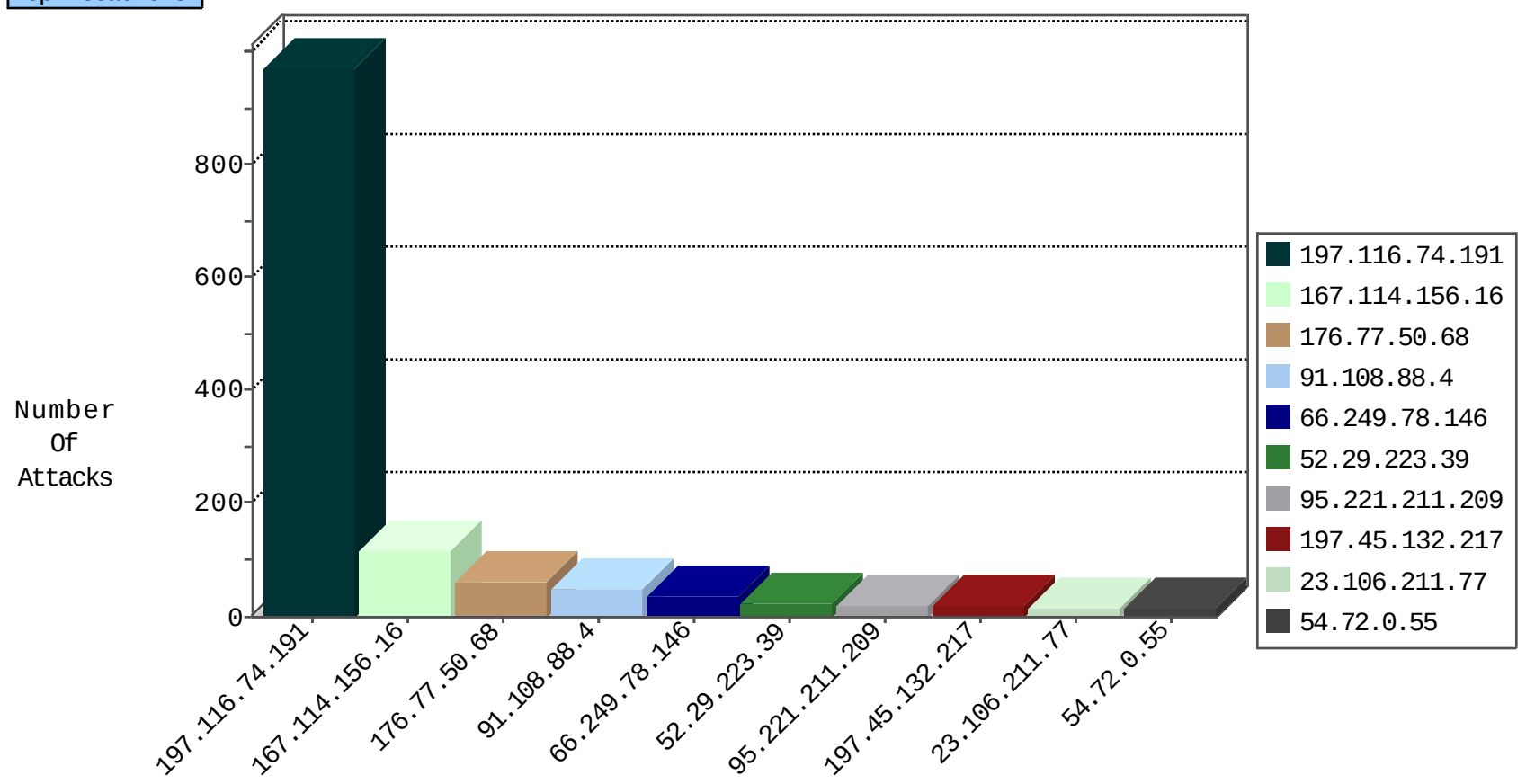
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

04-27-2016-06:04:05 to 04-27-2016-07:04:05

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	HTTP-POST-Segmented-DoS	dest-reset	6652
197.116.74.191	Algeria	147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	31
42.112.10.92	Vietnam	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
42.112.10.66	Vietnam	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
197.116.52.55	Algeria	147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	1
42.112.10.87	Vietnam	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
42.112.10.93	Vietnam	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
42.112.10.83	Vietnam	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
42.112.10.88	Vietnam	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	1
42.112.10.84	Vietnam	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
42.112.10.89	Vietnam	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
42.112.10.65	Vietnam	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
42.112.10.85	Vietnam	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1

04-27-2016-06:04:05 to 04-27-2016-07:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

04-27-2016-06:04:05 to 04-27-2016-07:04:05

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
104.219.238.10	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
202.115.30.83	147.237.72.156	China	aman.idf.il	ET SCAN NMAP -sS window 1024	1
195.216.176.244	147.237.76.176	Latvia	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
193.36.35.241	147.237.77.205	Russian Federation	prisha.idf.il	ET SCAN Potential SSH Scan	1
125.27.55.160	147.237.76.38	Thailand	e.e.meitav.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
106.184.2.29	147.237.8.28	Japan	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
82.117.208.243	147.237.0.200		m4u.idf.il	ET SCAN NMAP -sS window 1024	1
202.115.30.83	147.237.72.156	China	aman.idf.il	ET SCAN NMAP -sS window 3072	1
202.67.237.220	147.237.8.50	Hong Kong	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
178.17.42.103	147.237.76.200	United Kingdom	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
124.120.53.252	147.237.0.33	Thailand	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

04-27-2016-06:04:05 to 04-27-2016-07:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
197.116.74.191	Algeria	147.237.77.216	dover.idf.i	drop		drop	508
197.116.74.191	Algeria	147.237.77.216	dover.idf.i	Bad TCP sequence	Invalid ACK number	monitor	237
197.116.74.191	Algeria	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	182
176.77.50.68	Russian Federation	147.237.77.234	halag.idf.i	drop	First packet isn't SYN	drop	58
91.108.88.4	Germany	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	51
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
52.29.223.39	Germany	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	24
197.45.132.217	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	20
23.106.211.77	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	17
95.221.211.209	Russian Federation	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	17
54.72.0.55	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	16
50.87.144.145	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	14
52.16.5.197	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	14
54.72.73.168	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	13
108.173.185.55	Canada	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
203.133.169.231	Korea, Republic of	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
207.46.13.49	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
139.162.216.112	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
162.243.99.146	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
197.116.74.191	Algeria	147.237.77.216	dover.idf.i	drop	Unexpected post SYN packet - RST or SYN expected	drop	12
195.34.150.18	Austria	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	11
68.180.231.43	United States	147.237.77.216	dover.idf.i	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
45.35.64.142	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	9
91.78.4.50	Russian Federation	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	8
41.33.232.66	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	8
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	8
89.178.141.94	Russian Federation	147.237.77.234	halag.idf.i	drop	First packet isn't SYN	drop	8
199.30.25.81	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	7
169.234.88.240	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	6
72.10.240.17	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	6
37.26.146.186	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
54.89.54.3	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	6
166.137.8.118	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	5
212.143.142.56	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	5
207.46.13.89	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	5
98.243.38.41	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	4
207.119.114.12	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	4
95.221.211.209	Russian Federation	147.237.77.234	halag.idf.i	drop	First packet isn't SYN	drop	4
95.221.254.13	Russian Federation	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	4
46.42.174.45	Russian Federation	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	4
95.221.254.13	Russian Federation	147.237.77.234	halag.idf.i	drop	First packet isn't SYN	drop	4
89.178.141.94	Russian Federation	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	4
37.26.148.190	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	4
66.251.26.184	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	4
40.77.167.31	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	4
176.77.50.68	Russian Federation	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	4
62.90.153.168	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.81.234	Europe	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.46.39.67	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3

04-27-2016-06:04:05 to 04-27-2016-07:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
131.253.25.193	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	5
64.79.85.205	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	4
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
68.180.231.43	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/page/2/	Block	1
203.133.169.231	Korea, Republic of	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
84.95.208.20	Israel	147.237.77.74	law.idf.il	PHP Attempt	Block	1
141.212.122.161	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
73.25.158.80	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/mobile	Block	1
203.133.171.39	Korea, Republic of	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/modiin/default.aspx	Block	1
84.95.208.20	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/news/piwik.php	Block	1
66.249.66.121	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/8/3288.jpg	Block	1
174.37.194.144	United States	147.237.77.176	matpash.idf.il	Multiple Untraceable SSL Sessions from 174.37.194.144 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
74.82.47.4	United States	147.237.72.167	ishurim.aka.idf.i	Unauthorized URL Access to 147.237.72.167/	Block	1
109.64.106.80	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/images/1.he/infocenteritem/	Block	1
66.249.78.246	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/yoman/yoman.asp	Block	1
197.116.52.55	Algeria	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
79.176.30.228	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
51.255.65.82	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-16648-en/dover.asp	Block	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.231.43	Block	1
203.133.169.210	Korea, Republic of	147.237.76.147	chinuch.aka.idf.i	Unknown Parameter l in www.chinuch.aka.idf.il/templates/sendtofriend/sendtofriend.aspx	None	1
79.182.101.22	Israel	147.237.72.167	ishurim.aka.idf.i	SSL Untraceable Connection - Open Mode	None	1
131.253.25.237	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1

04-27-2016-06:04:05 to 04-27-2016-07:04:05