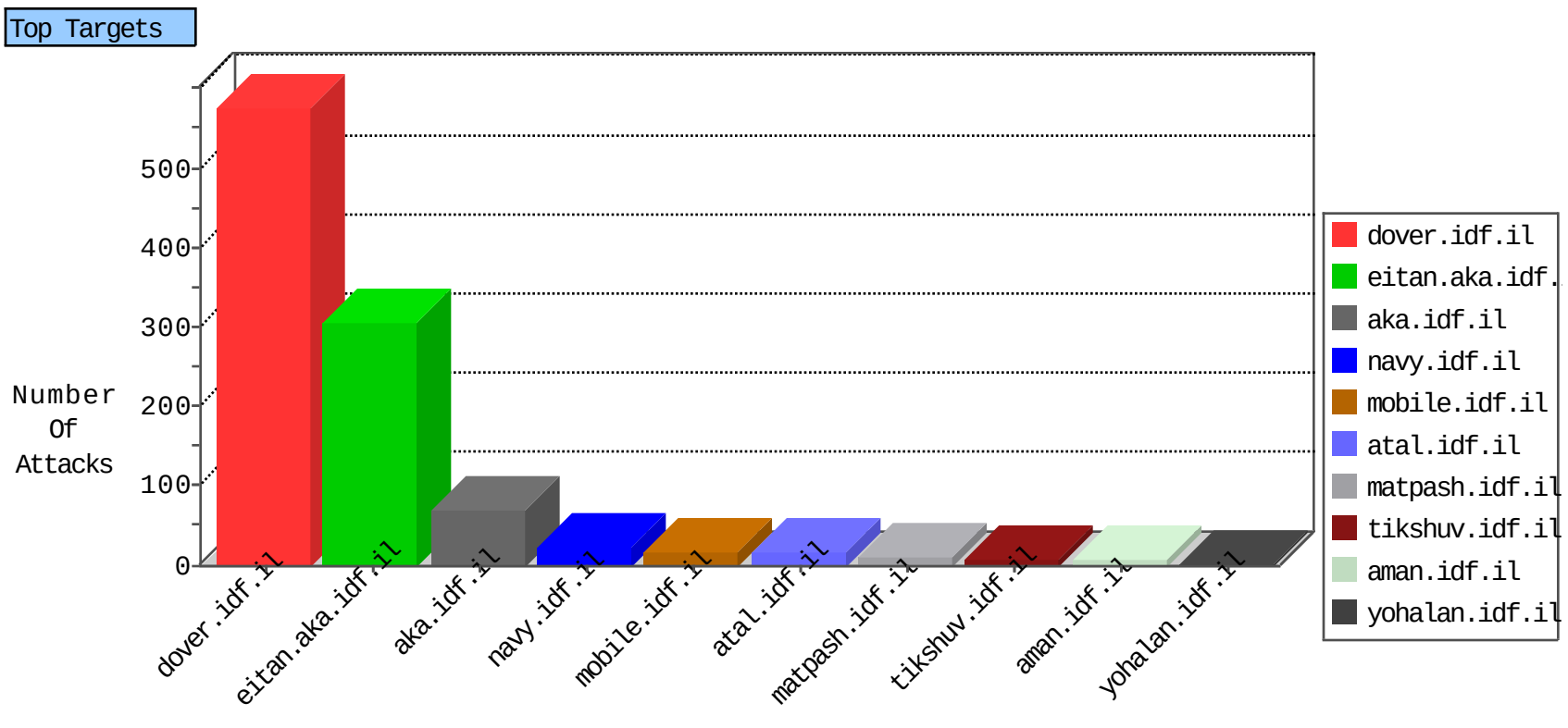
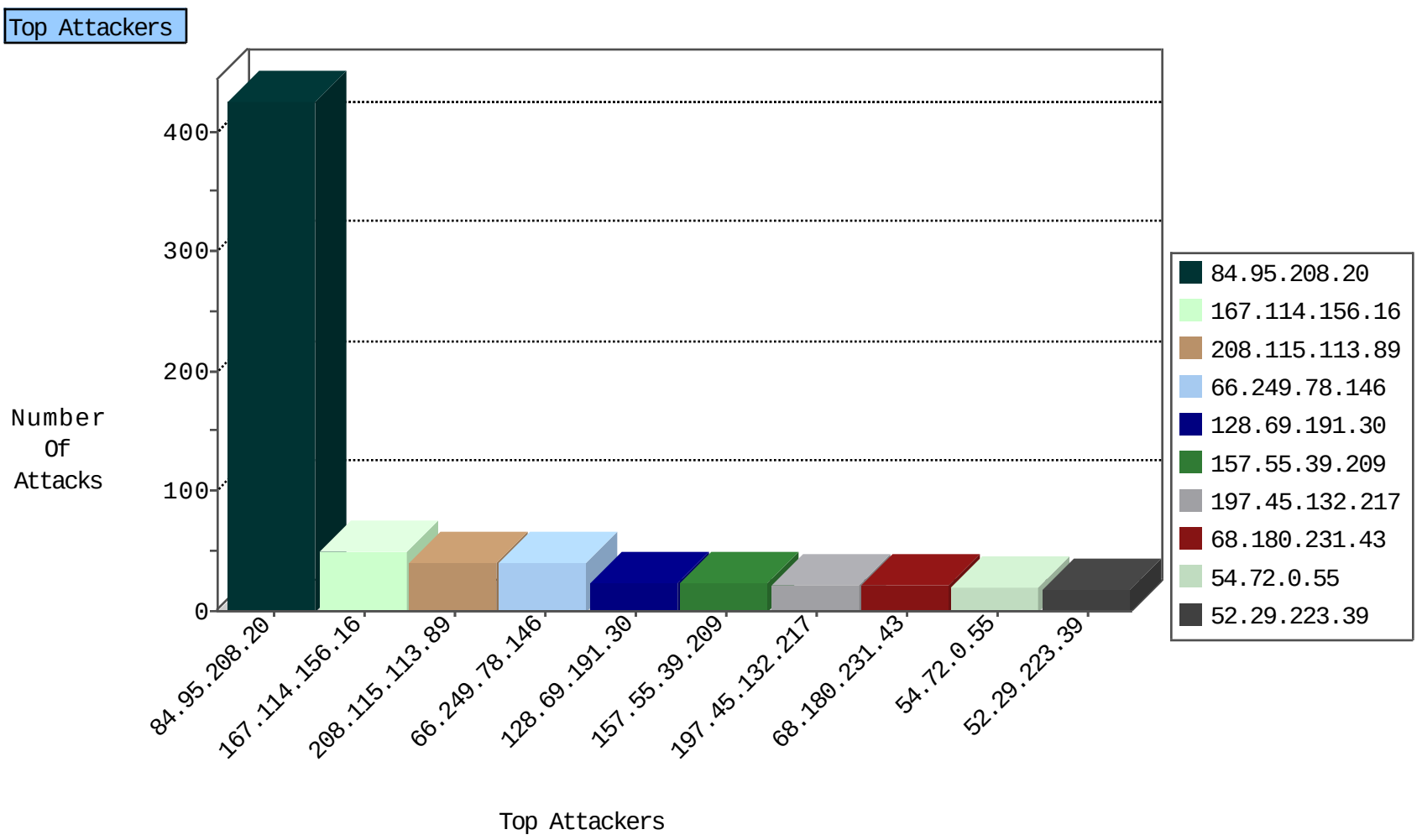
04-29-2016-03:04:07 to 04-29-2016-04:04:07

IDF Under Attack Daily Report





04-29-2016-03:04:07 to 04-29-2016-04:04:07

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	TCP handshake violation, first packet not syn	drop	12722
208.115.113.89	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	8335
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	10
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	8
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
128.69.191.30	Russian Federation	147.237.76.86	navy.idf.il	JLM_Purple_Con_Limit_Http	drop	3
128.69.191.30	Russian Federation	147.237.76.86	navy.idf.il	JLM_Under_Attack_Con_Http	drop	1
94.102.49.116	Netherlands	147.237.76.176	test.ncore.idf.i	Block_Ntp_All_Net	drop	1
141.212.122.219	United States	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
100.4.201.148	United States	147.237.76.176	test.ncore.idf.i	Block_Udp_All_Nets	drop	1

04-29-2016-03:04:07 to 04-29-2016-04:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
104.221.183.130	United States	147.237.0.34	tikshuv.idf.i	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	1

04-29-2016-03:04:07 to 04-29-2016-04:04:07

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
78.56.201.63	147.237.72.166	Lithuania	aka.idf.il	Xenu Link Sleuth User Agent	2
112.196.49.101	147.237.76.39	India	mobile.meitav.idf.i	ET SCAN NMAP -sS window 2048	1
83.110.221.42	147.237.0.19	United Arab Emirates	madim.atal.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
76.181.249.213	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sS window 2048	1
66.240.213.93	147.237.76.177	United States	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
187.28.151.178	147.237.0.34	Brazil	tikshuv.idf.il	ET SCAN NMAP -sS window 2048	1
112.196.49.101	147.237.76.39	India	mobile.meitav.idf.i	ET SCAN NMAP -sS window 3072	1
112.196.49.101	147.237.76.39	India	mobile.meitav.idf.i	ET SCAN NMAP -f -sS	1
76.181.249.213	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -f -sS	1
61.182.170.38	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
187.28.151.178	147.237.0.34	Brazil	tikshuv.idf.il	ET SCAN NMAP -sS window 3072	1
187.28.151.178	147.237.0.34	Brazil	tikshuv.idf.il	ET SCAN NMAP -f -sS	1

04-29-2016-03:04:07 to 04-29-2016-04:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	222
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	39
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
157.55.39.209	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
54.72.0.55	Ireland	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
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
207.46.13.137	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
181.49.177.171	Colombia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
87.70.25.121	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
198.58.96.215	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.103.102	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.103.160	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
157.55.39.106	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
105.107.174.121	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
54.188.241.114	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	11
128.69.191.30	Russian Federation	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	10
220.76.203.73	Korea, Republic of	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
128.69.191.30	Russian Federation	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
87.203.102.200	Greece	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
209.133.111.211	United States	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	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
203.133.169.234	Korea, Republic of	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
66.249.79.89	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
204.237.2.151	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
52.23.170.193	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
17.142.156.109	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
152.23.197.203	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
2.53.15.143	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
66.249.66.44	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.83.147	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
207.46.13.74	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
216.135.125.138	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
66.249.93.180	Europe	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
164.153.209.242	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
217.21.13.88	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
66.249.79.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
207.46.13.22	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
52.91.40.35	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
37.9.122.203	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2

04-29-2016-03:04:07 to 04-29-2016-04:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	100
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	84
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	8
149.202.239.134	France	147.237.77.216	dover.idf.il	Distributed Parameter Type Violation on www.idf.il/1283-en/dover.aspx parameter PageNum	Block	6
84.95.208.20	Israel	147.237.77.233	atal.idf.il	PHP Attempt	Block	6
149.202.239.135	France	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1283-en/dover.aspx	Block	6
65.55.210.248	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
66.102.8.238	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
87.70.25.121	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
178.137.87.242	Ukraine	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
66.249.79.89	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
220.255.148.8	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
5.29.196.252	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/bamahane	Block	1
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter tab in www.eitan.aka.idf.il/938-he/eitan.aspx	None	1
178.137.87.242	Ukraine	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 178.137.87.242	Block	1
68.180.230.45	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
17.142.156.109	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/apple-app-site-association	Block	1
149.202.239.134	France	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
184.105.139.68	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to 147.237.77.243/	Block	1
78.56.201.63	Lithuania	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/home/default.aspx	Block	1
51.255.65.6	France	147.237.72.166	aka.idf.il	Unauthorized Method GET for www.aka.idf.il/kamlar/contact/default.asp	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
203.127.58.235	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
141.212.122.161	United States	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to 147.237.0.15/	Block	1
79.177.17.79	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-he/dover.aspx	Block	1
52.12.99.95	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1379-he/dover.aspx	Block	1
149.202.239.135	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
207.46.13.137	United States	147.237.77.216	dover.idf.il	Abnormally Long Request URL	Block	1
2.55.138.243	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/templates/general/mobile	Block	1
149.88.128.202	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
54.184.244.254	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	Block	1

04-29-2016-03:04:07 to 04-29-2016-04:04:07