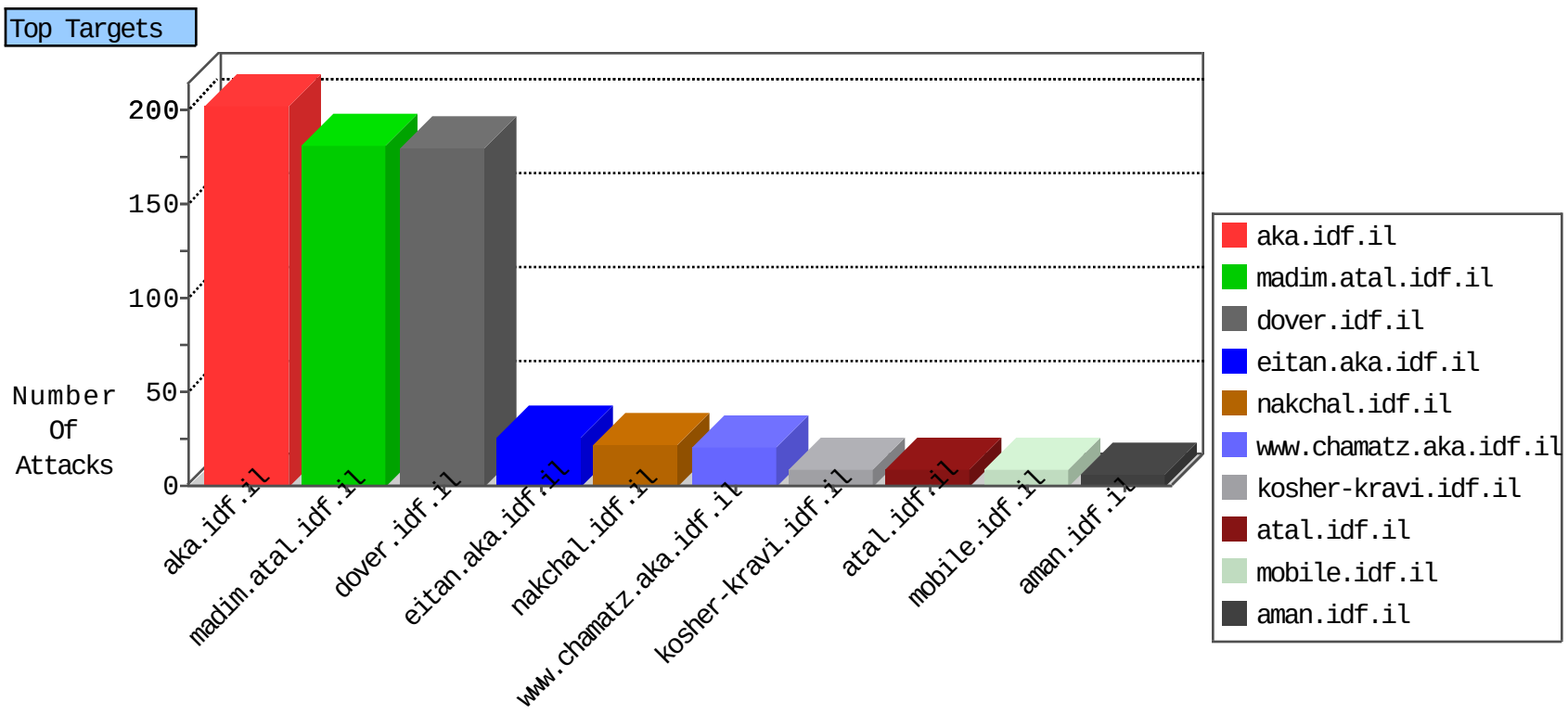
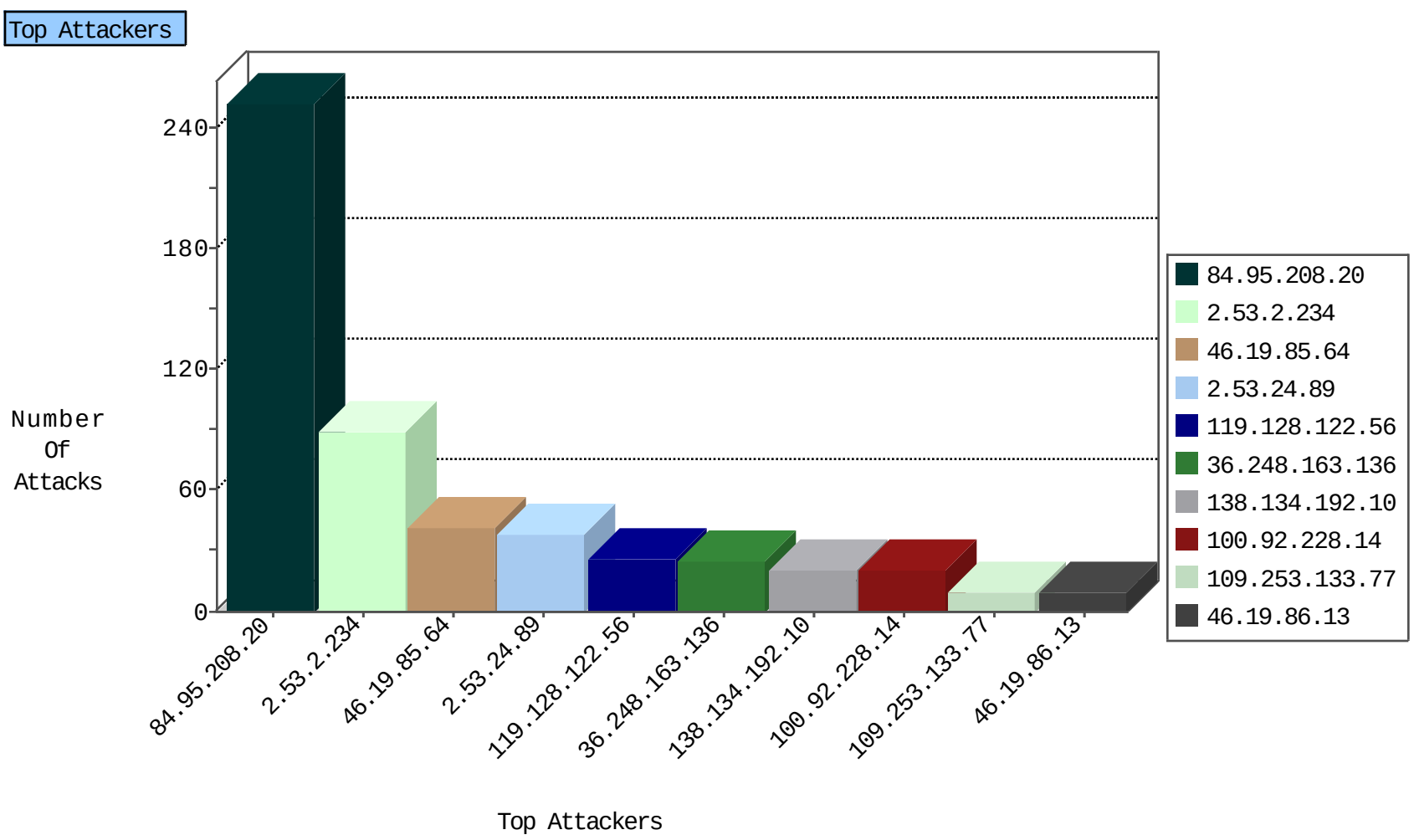
08-31-2016-11:04:04 to 08-31-2016-12:04:04

IDF Under Attack
Daily Report

Top Targets



Top Attackers



08-31-2016-11:04:04 to 08-31-2016-12:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.28.230.14	Russian Federation	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	10
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
82.221.105.7	Iceland	147.237.76.44	e.refuah.idf.il	Black List	drop	1

08-31-2016-11:04:04 to 08-31-2016-12:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
213.61.149.100	Germany	147.237.77.216	dover.idf.il	24910: HTTP: Python urllib User-Agent Header	Block	1

08-31-2016-11:04:04 to 08-31-2016-12:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.120.122.219	147.237.77.216	Israel	dover.idf.il	Xenu Link Sleuth User Agent	1
95.86.71.181	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.119	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
89.237.87.220	147.237.72.166	France	aka.idf.il	portscan: TCP Distributed Portscan	1
31.168.96.254	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.94.172.166	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.53.52.145	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.246.130.33	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.183.83.36	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
217.132.103.115	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.180.186.220	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
193.201.225.149	147.237.0.16	Ukraine	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
62.90.162.163	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
124.205.115.114	147.237.77.216	China	dover.idf.il	portscan: TCP Distributed Portscan	1
46.121.88.184	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.65.22.248	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.120.122.219	147.237.77.74	Israel	law.idf.il	Xenu Link Sleuth User Agent	1
94.103.150.195	147.237.76.202	Netherlands	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
37.46.41.66	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.111.208.52	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
31.168.13.78	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
82.81.12.232	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.178.116.193	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.181.30.171	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
193.201.225.149	147.237.0.16	Ukraine	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
79.176.107.251	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
132.72.11.90	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
58.218.204.245	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
114.34.212.68	147.237.8.28	Taiwan	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

08-31-2016-11:04:04 to 08-31-2016-12:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
100.92.228.14		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	20
109.253.133.77	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	9
46.19.86.13	Israel	147.237.0.15	kosher-kravi.idf.il	drop	First packet isn't SYN	drop	9
199.203.179.99	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
212.116.182.86	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
176.13.229.134	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	4
176.13.229.134	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
212.150.128.10	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
109.253.150.187	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	3
192.169.7.223	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	2
46.28.230.14	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
117.195.73.72	India	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	2
100.92.114.156		147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	2
79.178.92.62	Israel	147.237.76.31	nakchal.idf.il	drop	First packet isn't SYN	drop	2
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
109.253.205.128	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
79.180.177.230	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.43	United States	147.237.0.35	akaws.idf.il	drop		drop	1
115.230.125.146	China	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
94.103.150.195	Netherlands	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
141.212.122.86	United States	147.237.0.35	akaws.idf.il	drop		drop	1
109.253.140.210	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
176.13.245.162	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
212.34.72.92	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.87	United States	147.237.0.35	akaws.idf.il	drop		drop	1
109.253.143.10	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
77.126.24.150	Israel	147.237.72.166	aka.idf.il	drop	Virtual defragmentation error: Timeout	drop	1
176.13.246.106	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
137.116.71.170	United States	147.237.0.33	idf.il	drop		drop	1
176.13.23.187	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
192.168.173.102		147.237.77.216	dover.idf.il	drop		drop	1
141.212.122.42	United States	147.237.0.35	akaws.idf.il	drop		drop	1
109.253.129.101	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	131
2.53.2.234	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	89
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	85
46.19.85.64	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	41
2.53.24.89	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	38
119.128.122.56	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 119.128.122.56	Block	18
36.248.163.136	China	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 36.248.163.136	Block	17
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	17
138.134.192.10	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	12
138.134.192.10	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 138.134.192.10	Block	7
119.128.122.56	China	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	7
36.248.163.136	China	147.237.76.200	eitan.aka.idf.il	Distributed PHP Attempt	Block	6
66.249.64.22	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.22	Block	6
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	5
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	4
109.253.216.63	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Distributed PHP Attempt	Block	3
77.138.125.180	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/atudalane.aspx	Block	3
109.67.192.71	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	3
84.95.208.20	Israel	147.237.77.233	atal.idf.il	PHP Attempt	Block	3
77.139.6.178	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar	Block	2
192.115.64.250	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/home/default.aspx	Block	2
79.181.191.140	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.124	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	2
80.246.133.60	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
207.46.13.64	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
83.69.171.107	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	2
176.13.5.145	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.55.129.91	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
207.46.13.109	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
109.253.211.120	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
37.26.149.226	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
192.115.64.250	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/general.aspx	Block	1
66.249.64.12	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/apple-app-site-association	Block	1
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to atal.idf.il/templates/homepage/piwik.php	Block	1
84.95.208.20	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
209.132.178.17	United States	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 209.132.178.17 (Unsupported Cipher)	None	1
68.180.230.47	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1115-ar/dover.aspx	Block	1
119.128.122.56	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/index.asp	Block	1
89.248.172.16	Netherlands	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/robots.txt	Block	1
84.95.208.20	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
212.199.224.24	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/images/trans.gif	Block	1
138.134.192.10	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/sip_storage/files/2/	Block	1
68.180.230.47	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1133-ar/dover.aspx	Block	1
117.241.146.193	India	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
194.90.119.123	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/6/67906	Block	1
66.249.64.33	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
132.74.7.46	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
109.65.108.176	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/https:/www.aman.idf.il/	Block	1
36.248.163.136	China	147.237.76.200	eitan.aka.idf.il	Unauthorized Method HEAD for www.eitan.aka.idf.il/	None	1