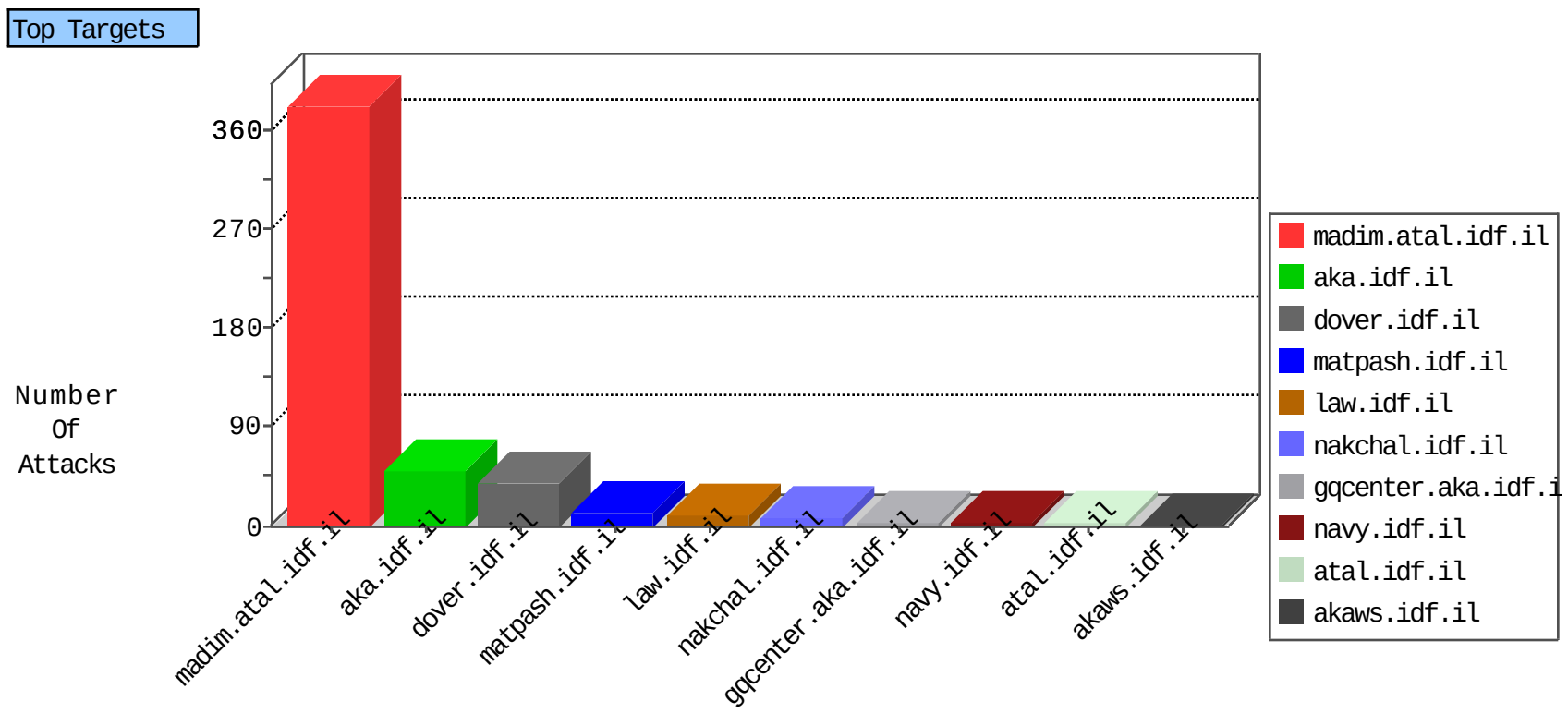
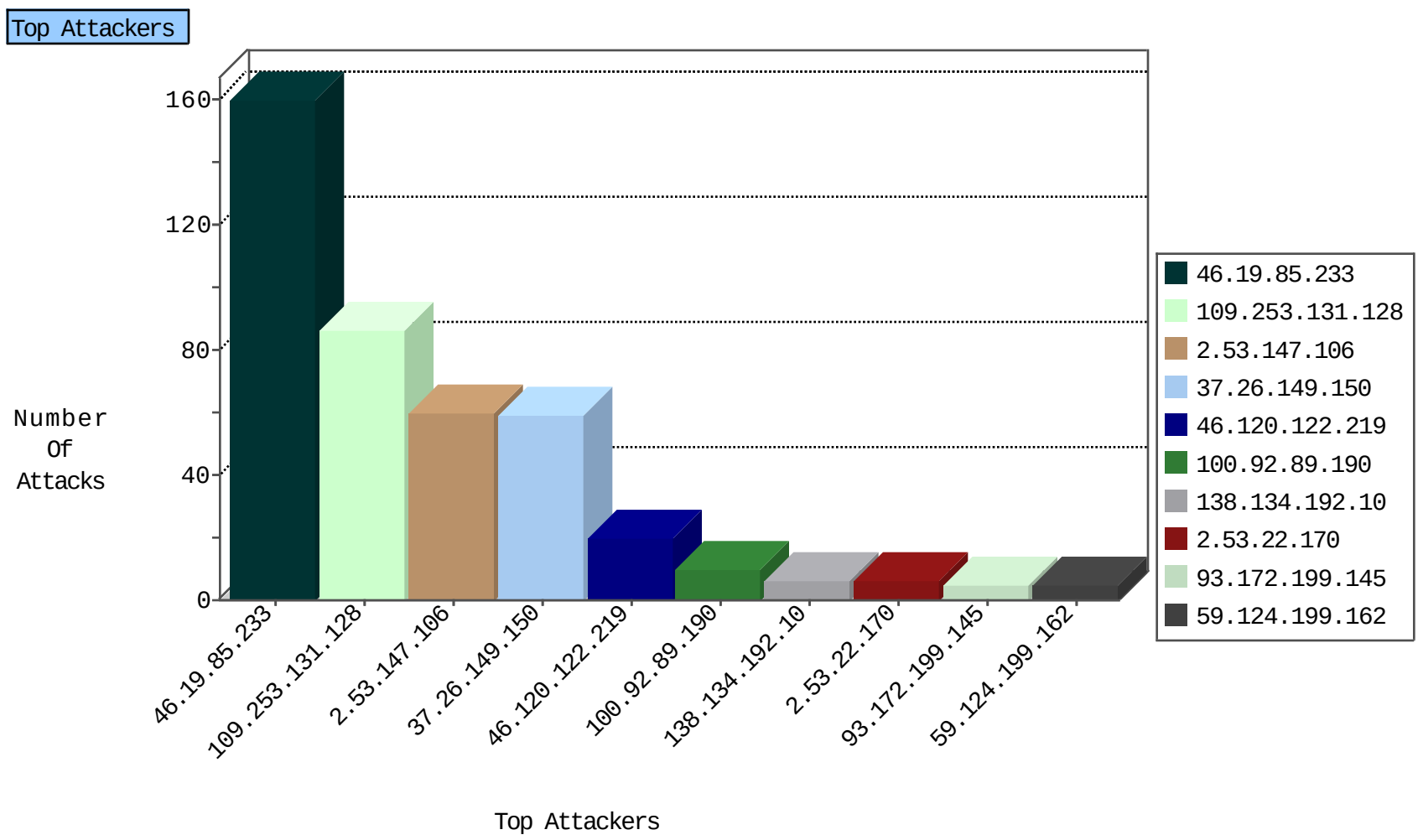
08-31-2016-08:04:03 to 08-31-2016-09:04:03

IDF Under Attack Daily Report

Top Targets



Top Attackers



08-31-2016-08:04:03 to 08-31-2016-09:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.64.82.99	Israel	147.237.77.216	dover.idf.il	Black List	drop	2
163.172.216.36	United Kingdom	147.237.76.31	nakchal.idf.il	Black List	drop	1

08-31-2016-08:04:03 to 08-31-2016-09:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.105	China	147.237.77.74	law.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	2
162.210.196.98	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2

08-31-2016-08:04:03 to 08-31-2016-09:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.120.122.219	147.237.77.176	Israel	matpash.idf.il	Xenu Link Sleuth User Agent	10
46.120.122.219	147.237.77.74	Israel	law.idf.il	Xenu Link Sleuth User Agent	6
46.120.122.219	147.237.77.216	Israel	dover.idf.il	Xenu Link Sleuth User Agent	4
199.203.126.110	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.168.61.111	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
162.243.119.221	147.237.77.234	United States	halag.idf.il	ET SCAN Potential SSH Scan	1
5.255.90.133	147.237.76.39	Netherlands	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
104.232.98.38	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN NMAP -sS window 3072	1
2.53.131.196	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
103.207.36.84	147.237.0.35	Vietnam	akaws.idf.il	ET SCAN NMAP -f -sS	1
80.246.139.209	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.82.78.184	147.237.77.233	Netherlands	atal.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.79.103	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	1
219.87.191.219	147.237.0.19	Taiwan	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
37.26.149.139	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
198.167.223.33	147.237.76.34	Saint Kitts and Nevis	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
5.255.90.133	147.237.76.86	Netherlands	navy.idf.il	ET SCAN NMAP -sS window 1024	1
147.236.238.75	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.255.90.133	147.237.76.38	Netherlands	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
103.207.36.84	147.237.0.35	Vietnam	akaws.idf.il	ET SCAN NMAP -sS window 2048	1
2.53.50.145	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.135.102.171	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.179.196.19	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.82.78.184	147.237.72.156	Netherlands	aman.idf.il	ET SCAN Potential SSH Scan	1

08-31-2016-08:04:03 to 08-31-2016-09:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
100.92.89.190		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	10
93.172.199.145	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
192.169.7.223	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	3
62.90.210.131	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
100.92.228.14		147.237.72.166	aka.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
109.253.219.214	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
80.178.138.115	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
82.102.173.79	Israel	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
109.253.213.169	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
62.90.210.131	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
94.103.150.195	Netherlands	147.237.0.200	m4u.idf.il	drop		drop	1
176.13.16.227	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
77.124.15.123	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
176.13.234.98	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
46.19.85.233	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	160
109.253.131.128	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	84
2.53.147.106	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	60
37.26.149.150	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	59
2.53.22.170	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
59.124.199.162	Taiwan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	5
138.134.192.10	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	5
124.219.66.130	Taiwan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
217.132.99.107	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
77.139.6.178	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar	Block	3
66.249.64.22	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.22	Block	3
80.246.139.24	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.149.222	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.55.29.75	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	3
10.111.80.54		147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/main/	Block	2
176.13.233.194	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
79.177.82.127	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
66.249.66.251	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
216.244.66.233	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/האתר	Block	1
148.251.2.180	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1
37.26.149.222	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/894-he/atal.aspx	Block	1
85.64.144.223	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il./favicon.ico	Block	1
77.138.255.126	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	1
66.147.244.101	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	1
192.116.232.69	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 192.116.232.69	Block	1
2.55.44.40	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
79.177.163.86	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/mailn/sachar	Block	1
66.249.79.102	Israel	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on navy.idf.il/giyus/forum/asp/showforum.asp	Block	1
157.55.39.37	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/	Block	1
85.65.23.14	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
207.46.13.59	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/320/patzar.aspx	Block	1
79.181.111.202	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/sachar/undefined	Block	1
66.249.79.110	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	1
157.55.39.133	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
59.124.134.130	Taiwan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
2.53.52.145	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/homepage/homepage.aspx	Block	1
87.69.54.82	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
79.176.86.63	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl09 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
66.249.64.116	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 66.249.64.116	Block	1
207.46.13.64	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
138.134.192.10	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 138.134.192.10	Block	1
68.180.230.47	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
87.69.220.99	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/faq.aspx	Block	1
79.176.86.63	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl13 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
66.249.64.116	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/about/memorial/pages/netanelpitusi.aspx	Block	1
216.244.66.232	United States	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on navy.idf.il/giyus/forum/asp/showforum.asp	Block	1
84.95.208.20	Israel	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to www.kosher-kravi.idf.il/default.aspx	Block	1
77.138.47.89	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/popups/markivsachar.aspx	Block	1
180.76.15.149	China	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/templates/shared/usercontrols/headerupper/	Block	1
66.102.6.4	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim	Block	1