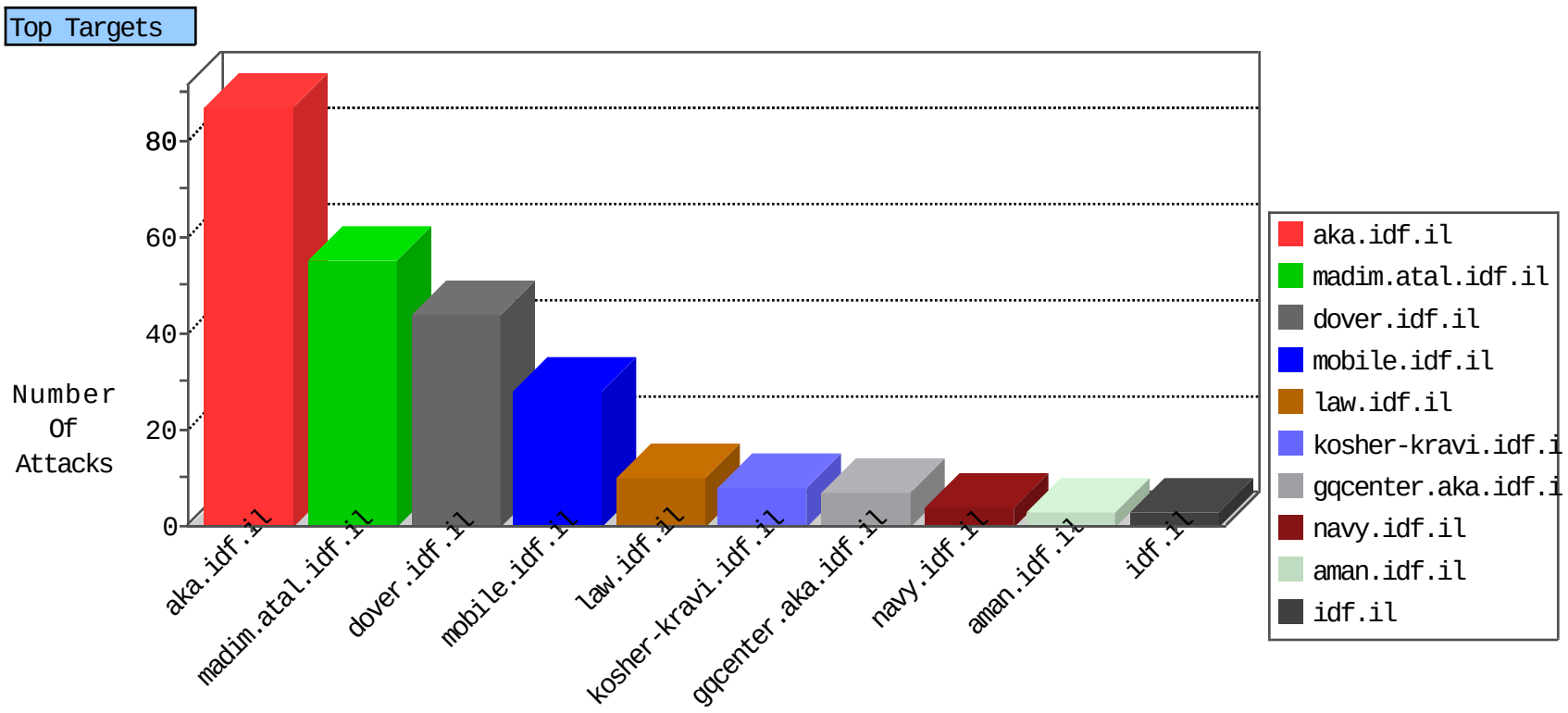
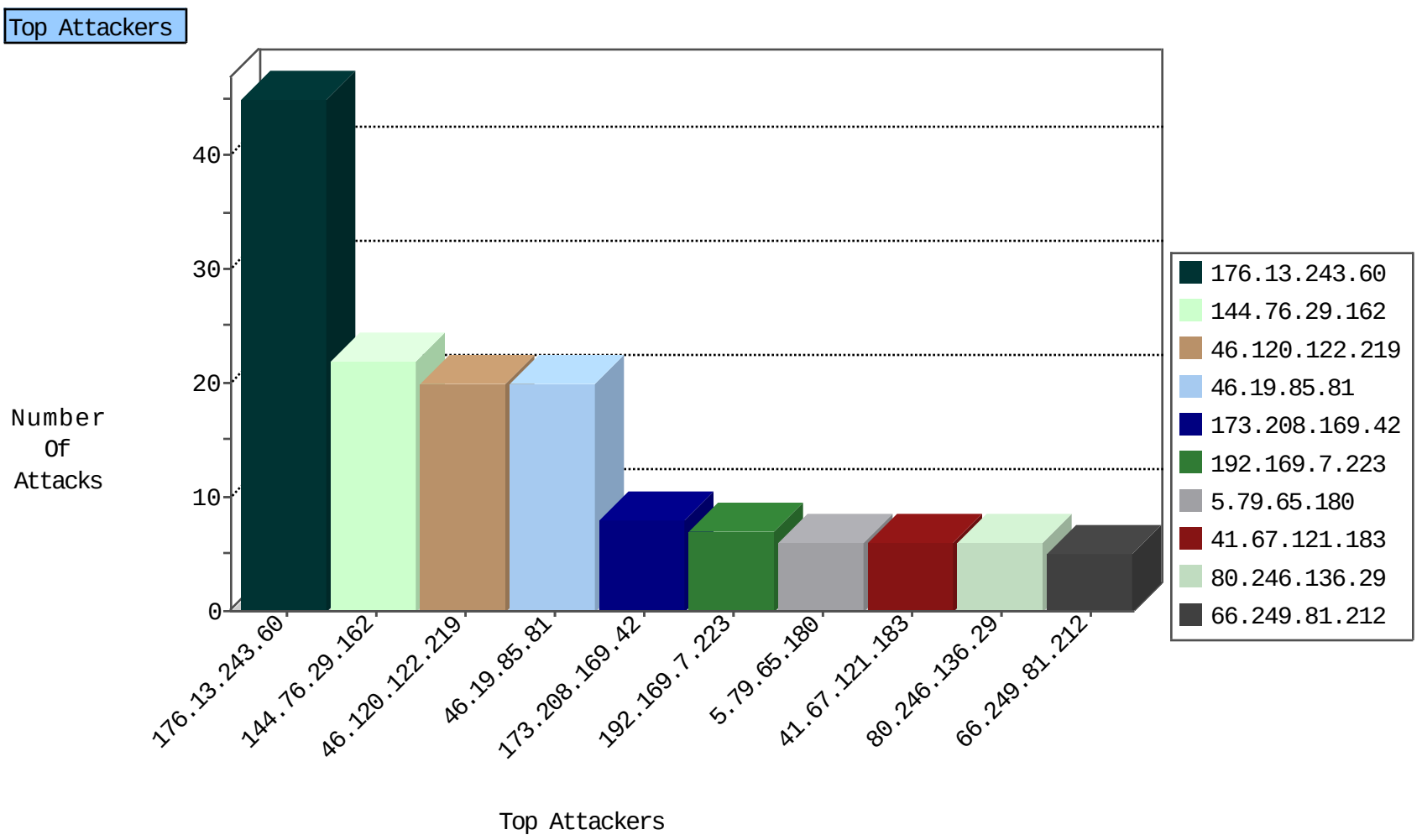
08-30-2016-00:04:05 to 08-30-2016-01:04:05

IDF Under Attack Daily Report

Top Targets



Top Attackers



08-30-2016-00:04:05 to 08-30-2016-01:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
41.67.121.183	Egypt	147.237.77.216	dover.idf.il	HTTP-MISC-Acunetix-Url	dest-reset	5
93.158.200.97	Netherlands	147.237.76.196	e.sviva.idf.il	Black List	drop	1
37.112.229.255	Russian Federation	147.237.72.167	ishurim.aka.idf.il	TCP handshake violation, first packet not syn	drop	1

08-30-2016-00:04:05 to 08-30-2016-01:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
144.76.29.162	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	13
173.208.169.42	United States	147.237.0.15	kosher-kravi.idf.il	C1000125: HTTP: Block admin login to gov.il sites ?q=user	Permit	8
144.76.29.162	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	7
144.76.29.162	Germany	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Permit	2
41.67.121.183	Egypt	147.237.77.216	dover.idf.il	10767: HTTP: Acunetix Security Scanner	Block	1

08-30-2016-00:04:05 to 08-30-2016-01:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.120.122.219	147.237.72.166	Israel	aka.idf.il	Xenu Link Sleuth User Agent	8
46.120.122.219	147.237.76.86	Israel	navy.idf.il	Xenu Link Sleuth User Agent	4
46.120.122.219	147.237.77.216	Israel	dover.idf.il	Xenu Link Sleuth User Agent	2
198.167.223.33	147.237.0.33	Saint Kitts and Nevis	idf.il	ET SCAN NMAP -sS window 1024	1
183.222.97.82	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
139.162.13.205	147.237.76.196	Singapore	e.sviva.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
85.65.48.28	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
50.116.123.135	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
46.120.122.219	147.237.77.176	Israel	matpash.idf.il	Xenu Link Sleuth User Agent	1
212.224.109.175	147.237.77.216	Germany	dover.idf.il	ET SCAN Potential SSH Scan	1
198.167.223.33	147.237.0.19	Saint Kitts and Nevis	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.169.150	147.237.0.34	United Kingdom	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
85.250.255.121	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
50.116.123.135	147.237.77.234	United States	halag.idf.il	ET SCAN NMAP -sS window 1024	1

08-30-2016-00:04:05 to 08-30-2016-01:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.19.85.81	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	20
192.169.7.223	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	6
195.239.16.40	Russian Federation	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
195.239.16.53	Russian Federation	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
176.13.20.49	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
176.13.2.191	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
93.173.240.71	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	2
104.173.243.178	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
176.13.20.171	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	2
109.253.159.62	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
66.249.76.83	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
109.253.132.127	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
5.79.65.180	Netherlands	147.237.76.197	e.himush.idf.il	drop	SAM rule	drop	1
176.13.21.22	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
163.172.169.150	United Kingdom	147.237.0.33	idf.il	drop		drop	1
79.181.254.3	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
5.79.65.180	Netherlands	147.237.76.38	e.e.meitav.idf.il	drop	SAM rule	drop	1
176.13.10.185	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
109.253.134.184	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	1
176.13.23.61	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	1
163.172.169.150	United Kingdom	147.237.0.35	akaws.idf.il	drop		drop	1
5.79.65.180	Netherlands	147.237.76.148	gqcenter.aka.idf.il	drop	SAM rule	drop	1
109.253.143.5	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
54.169.197.38	Singapore	147.237.0.33	idf.il	drop		drop	1
176.13.237.105	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.76.31	nakchal.idf.il	drop	First packet isn't SYN	drop	1
94.61.182.255	Portugal	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
5.79.65.180	Netherlands	147.237.76.176	test.ncore.idf.il	drop	SAM rule	drop	1
176.13.20.56	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
109.253.157.134	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
54.169.197.38	Singapore	147.237.0.35	akaws.idf.il	drop		drop	1
2.53.167.35	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
176.13.243.98	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.76.34	yohalan.idf.il	drop	First packet isn't SYN	drop	1
5.79.65.180	Netherlands	147.237.76.177	ncore.idf.il	drop	SAM rule	drop	1
218.22.211.69	China	147.237.76.34	yohalan.idf.il	drop		drop	1
5.79.65.180	Netherlands	147.237.76.30	himush.idf.il	drop	SAM rule	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.243.60	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	45
46.120.122.219	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 46.120.122.219	Block	5
79.181.118.59	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
66.249.81.212	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	5
213.57.43.106	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
80.246.136.29	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
66.249.81.215	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
66.249.81.218	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
46.116.124.223	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
37.142.225.59	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/categorytemplates/listchilddocuments/1152	Block	3
37.26.148.139	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
207.46.13.109	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/print_bottom.asp	Block	2
80.246.136.29	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
93.173.33.249	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
71.196.123.129	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	2
176.13.21.175	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
77.138.49.129	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/miyun/miyunasmachta.aspx	Block	2
217.19.208.110	Moldova, Republic of	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	2
77.138.80.112	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
66.249.64.126	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/tizmoret/news/default.asp	Block	1
37.26.148.139	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
105.155.3.10	Morocco	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 105.155.3.10	Block	1
217.19.208.110	Moldova, Republic of	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
46.116.4.243	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012 ources/images/innerpage/goback.gif	Block	1
178.63.101.134	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/home/default.aspx	Block	1
89.138.254.32	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar/	Block	1
77.138.210.140	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
207.46.13.149	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/daily_statistics/english	Block	1
66.249.65.51	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
37.26.148.157	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
109.253.134.53	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
84.108.250.23	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
185.32.179.176	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
77.139.79.23	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	1
207.46.13.171	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
66.249.76.70	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/apple-app-site-association	Block	1
37.142.110.54	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/watch	Block	1
176.13.7.182	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/	Block	1
84.169.245.38	Germany	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/contactus.aspx	Block	1
192.169.7.223	United States	147.237.76.42	refuah.idf.il	Unauthorized Method HEAD for 147.237.76.42/	Block	1
104.173.243.178	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
2.53.145.217	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __PREVIOUSPAGE in www.aka.idf.il/main/sachar/default.aspx	None	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
85.64.255.47	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
195.167.10.2	Greece	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	1
62.0.119.135	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/	Block	1
105.155.3.10	Morocco	147.237.77.216	dover.idf.il	Multiple Admin Blocking from 105.155.3.10	Block	1
46.19.85.235	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
87.68.33.93	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	1