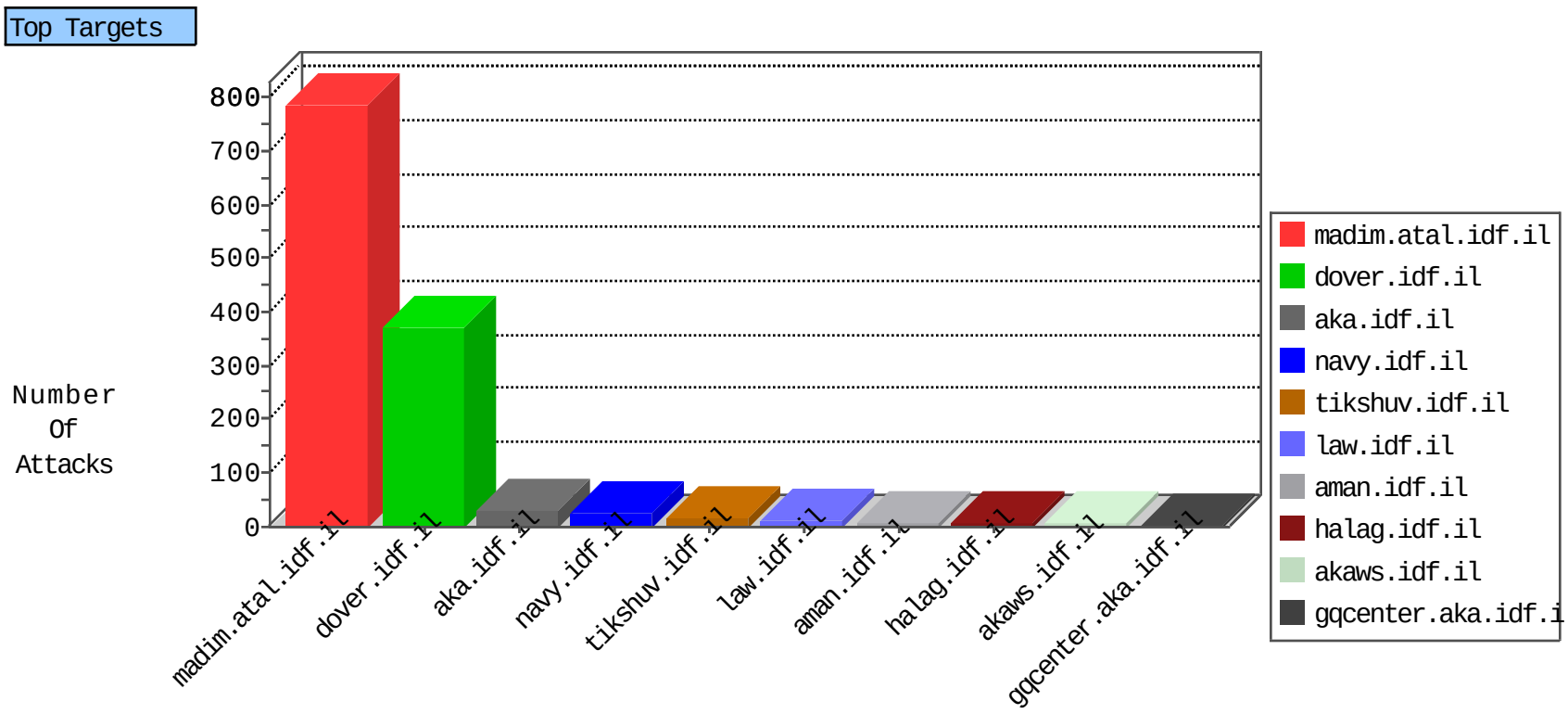
08-19-2016-17:04:05 to 08-19-2016-18:04:05

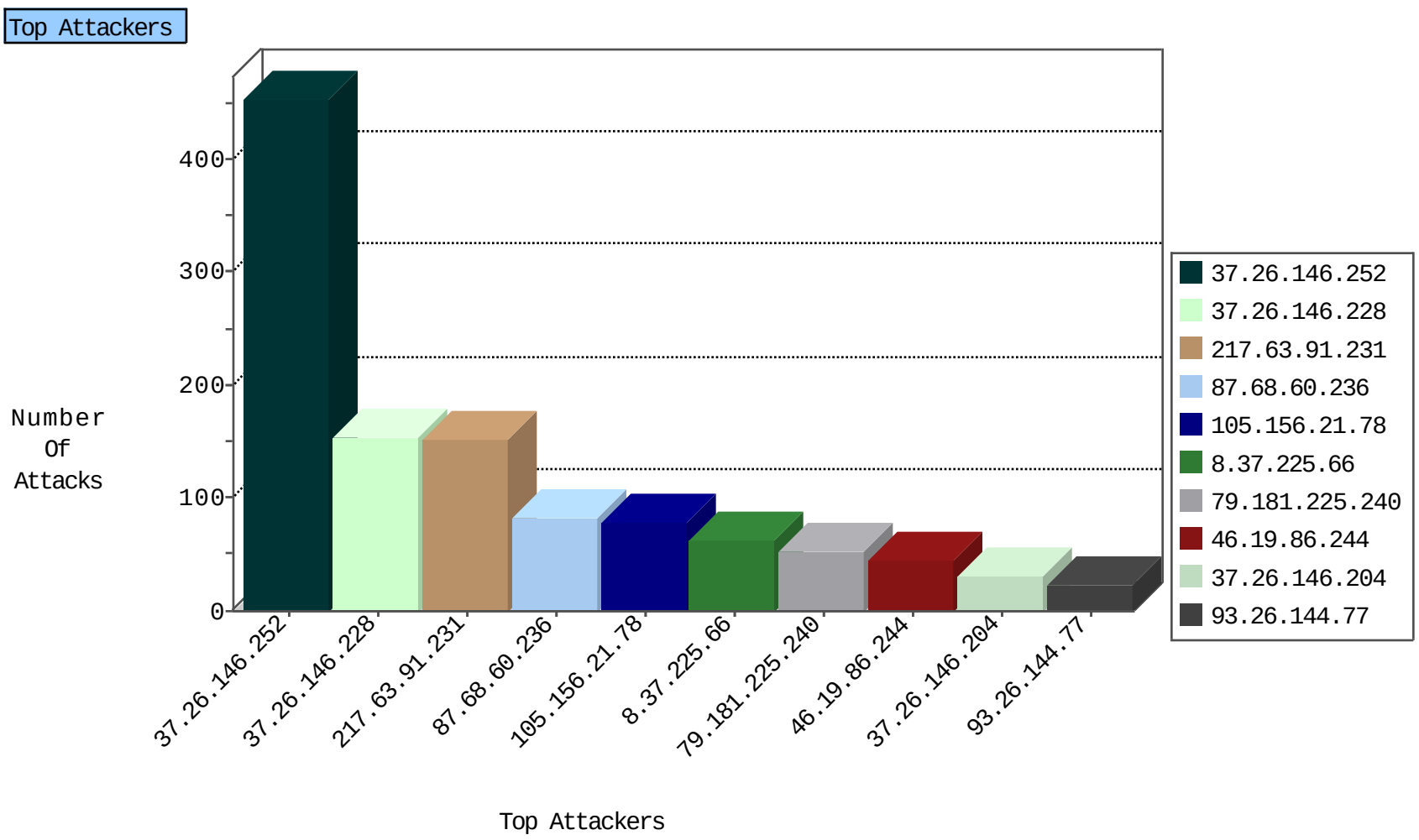
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

08-19-2016-17:04:05 to 08-19-2016-18:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
8.37.225.66	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
58.176.202.65	Hong Kong	147.237.76.148	gqcenter.aka.idf.il	Black List	drop	3
8.37.225.66	United States	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	3
82.80.78.2	Israel	147.237.72.166	aka.idf.il	Black List	drop	2
94.177.160.214	Romania	147.237.76.39	mobile.meitav.idf.il	Black List	drop	1
2.53.33.205	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
94.177.160.214	Romania	147.237.76.196	e.sviva.idf.il	Black List	drop	1
77.138.52.97	France	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
199.203.152.235	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1

08-19-2016-17:04:05 to 08-19-2016-18:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
205.144.171.34	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
5.9.142.226	Germany	147.237.0.34	tikshuv.idf.il	C1000074: HTTP: majestic bot	Permit	2
5.9.142.226	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
69.30.198.186	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
197.251.164.64	Ghana	147.237.77.216	dover.idf.il	12580: HTTP: SQL Injection (Cookie Header)	Block	1

08-19-2016-17:04:05 to 08-19-2016-18:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
109.65.127.72	147.237.0.34	Israel	tikshuv.idf.il	ET SCAN NMAP -sA (2)	11
205.144.171.34	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	4
93.26.144.77	147.237.77.61	France	e.cogat.idf.il	ET SCAN Potential SSH Scan	2
93.26.144.77	147.237.77.234	France	halag.idf.il	ET SCAN Potential SSH Scan	1
93.26.144.77	147.237.76.39	France	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
93.26.144.77	147.237.77.226	France	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
93.26.144.77	147.237.76.34	France	yohalan.idf.il	ET SCAN Potential SSH Scan	1
93.26.144.77	147.237.77.205	France	prisha.idf.il	ET SCAN Potential SSH Scan	1
93.26.144.77	147.237.76.30	France	himush.idf.il	ET SCAN Potential SSH Scan	1
93.26.144.77	147.237.77.178	France	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
66.249.66.185	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	1
212.224.109.179	147.237.77.176	Germany	matpash.idf.il	ET SCAN Potential SSH Scan	1
5.255.90.133	147.237.0.35	Netherlands	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
93.26.144.77	147.237.76.202	France	e.halag.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.0.35	China	akaws.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
93.26.144.77	147.237.76.200	France	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
125.212.233.35	147.237.76.38	Vietnam	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
93.26.144.77	147.237.76.176	France	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
93.26.144.77	147.237.76.44	France	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
93.26.144.77	147.237.77.233	France	atal.idf.il	ET SCAN Potential SSH Scan	1
93.26.144.77	147.237.76.38	France	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
93.26.144.77	147.237.77.212	France	e.dover.idf.il	ET SCAN Potential SSH Scan	1
93.26.144.77	147.237.76.31	France	nakchal.idf.il	ET SCAN Potential SSH Scan	1
93.26.144.77	147.237.77.179	France	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
79.182.28.24	147.237.76.42	Israel	refuah.idf.il	ET SCAN NMAP -sA (2)	1
93.26.144.77	147.237.77.74	France	law.idf.il	ET SCAN Potential SSH Scan	1
23.31.28.157	147.237.76.31	United States	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
93.26.144.77	147.237.77.19	France	law-forum.idf.il	ET SCAN Potential SSH Scan	1
2.180.17.102	147.237.76.30	Iran, Islamic Republic of	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
93.26.144.77	147.237.76.201	France	e.atal.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
93.26.144.77	147.237.76.197	France	e.himush.idf.il	ET SCAN Potential SSH Scan	1
125.212.233.35	147.237.76.31	Vietnam	nakchal.idf.il	ET SCAN Potential SSH Scan	1
93.26.144.77	147.237.76.148	France	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1

08-19-2016-17:04:05 to 08-19-2016-18:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
217.63.91.231	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	152
105.156.21.78	Morocco	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	79
8.37.225.66	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	54
79.181.225.240	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
79.181.225.240	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	18
176.13.228.93	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
93.214.241.101	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.151.209.155	Saudi Arabia	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	3
77.138.52.97	France	147.237.77.216	dover.idf.il	drop		drop	3
177.22.251.2	Brazil	147.237.0.35	akaws.idf.il	drop		drop	3
85.130.201.44	Israel	147.237.77.234	halag.idf.il	drop	First packet isn't SYN	drop	3
5.9.111.70	Germany	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
85.64.205.81	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	2
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
85.64.254.132	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	2
41.238.110.25	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
158.169.40.5	Belgium	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	1
2.53.33.205	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
66.249.81.212	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
176.13.16.121	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	1
84.229.62.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
109.253.139.243	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
176.13.251.99	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
109.253.199.24	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1

08-19-2016-17:04:05 to 08-19-2016-18:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.146.252	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	454
37.26.146.228	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	154
87.68.60.236	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	82
46.19.86.244	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	45
37.26.146.204	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	30
46.19.85.103	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
46.19.86.10	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
5.28.170.40	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.229.31.81	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.120.199.195	Israel	147.237.72.167	ishurim.aka.idf.i	Untraceable SSL Sessions: Open Mode	None	2
85.64.242.184	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush	Block	2
79.181.223.196	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.64.128	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/1/70001.jpg	Block	1
217.132.60.250	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/authenticationservice.asmx	Block	1
87.69.17.6	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
67.245.1.115	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/5/	Block	1
173.252.102.113	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.66.185	Israel	147.237.77.74	law.idf.il	Illegal URL Path Encoding www.law.idf.il/templates/getfile/getfile.aspx?filenamem	Block	1
89.138.183.88	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
77.138.107.29	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/klali.aspx	Block	1
180.76.15.19	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/news/jeninkilled/stn	Block	1
37.8.7.153	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
84.229.32.9	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl51 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
66.249.76.33	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/4/71594.gif	Block	1
37.26.148.229	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/gius	Block	1
109.253.222.60	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
77.138.140.102	France	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/favicon.ico	Block	1
185.120.125.118	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	1
37.8.7.153	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	1
66.249.76.40	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/apple-app-site-association	Block	1
37.26.148.242	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
149.3.93.83	Georgia	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/yahash2016/lobby.aspx	Block	1
66.102.9.85	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
213.57.181.145	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
67.245.1.115	United States	147.237.77.170	maarachot.idf.il	Unauthorized HTTP Method	Block	1
157.55.39.110	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
2.55.25.8	Israel	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
84.111.233.138	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1

08-19-2016-17:04:05 to 08-19-2016-18:04:05