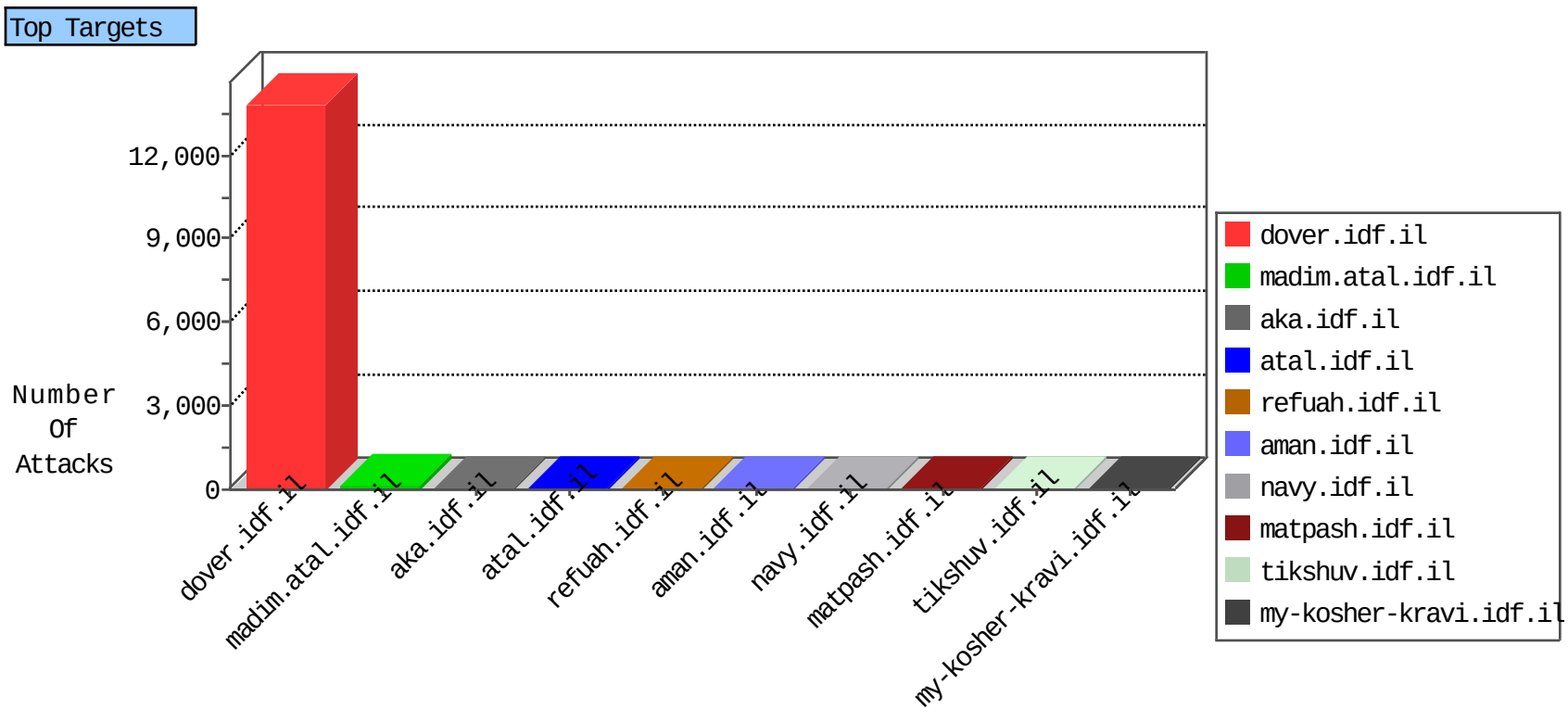
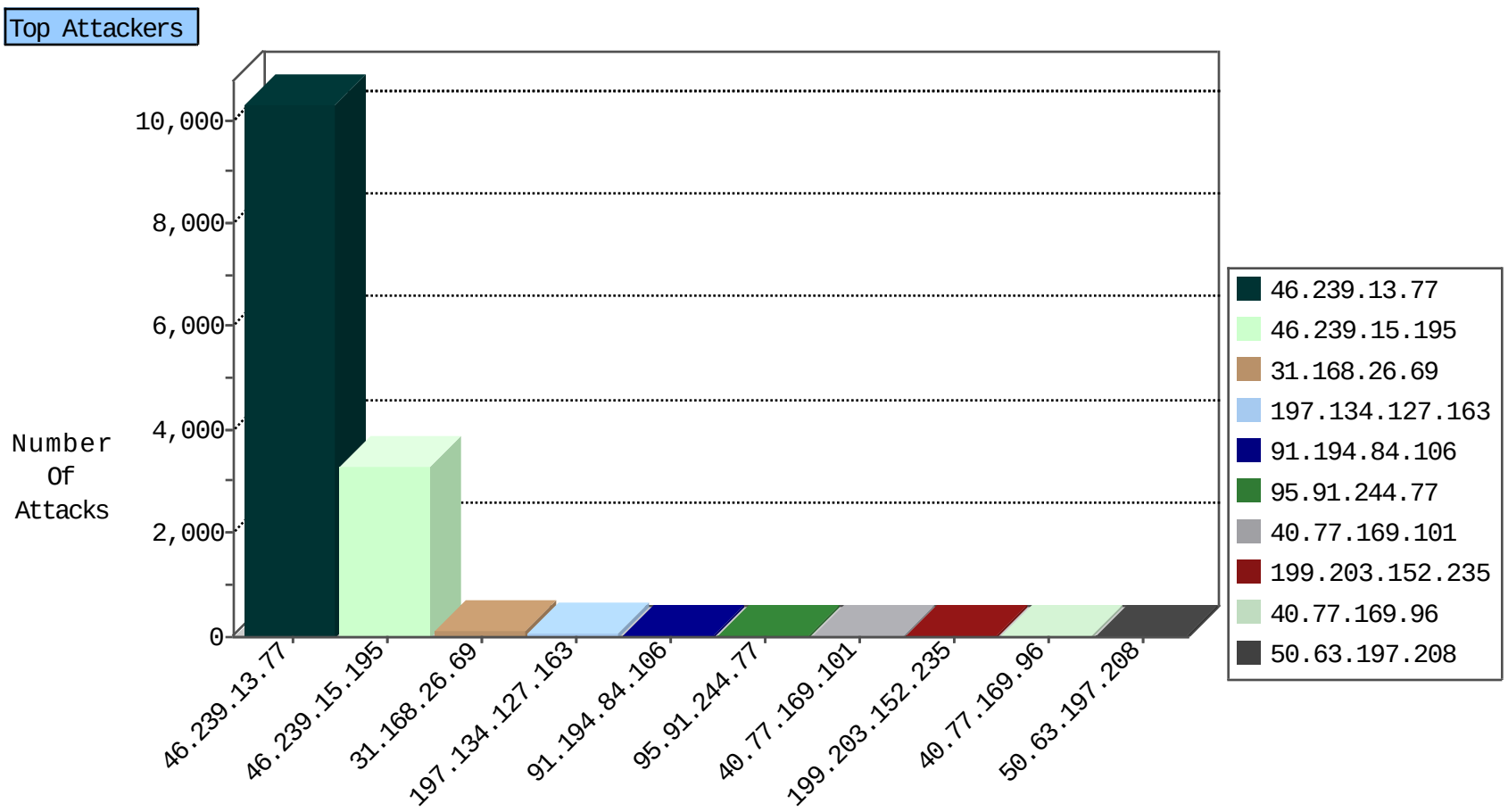
08-27-2016-11:04:04 to 08-27-2016-12:04:04

IDF Under Attack Daily Report

Top Targets



Top Attackers



08-27-2016-11:04:04 to 08-27-2016-12:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
222.186.34.73	China	147.237.76.196	e.sviva.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
114.91.45.77	China	147.237.76.197	e.himush.idf.il	Black List	drop	2
185.94.111.1	Russian Federation	147.237.76.42	refuah.idf.il	Black List	drop	1
115.28.7.221	China	147.237.76.199	e.nakchal.idf.il	JLM_Purple_Con_Limit_Http	drop	1
185.94.111.1	Russian Federation	147.237.76.44	e.refuah.idf.il	Black List	drop	1
115.28.7.221	China	147.237.76.199	e.nakchal.idf.il	JLM_Under_Attack_Con_Http	drop	1
46.239.15.195	Bosnia and Herzegovina	147.237.77.216	dover.idf.il	Frk_Under_Attack_Con_Http	drop	1
134.147.203.115	Germany	147.237.76.34	yohalan.idf.il	Black List	drop	1

08-27-2016-11:04:04 to 08-27-2016-12:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
91.194.84.106	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	18
91.194.84.106	Germany	147.237.76.42	refuah.idf.il	C1000074: HTTP: majestic bot	Permit	12
50.63.197.208	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
91.194.84.106	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
91.194.84.106	Germany	147.237.77.233	atal.idf.il	C1000074: HTTP: majestic bot	Permit	2
197.231.221.211	Liberia	147.237.77.216	dover.idf.il	24910: HTTP: Python urllib User-Agent Header	Block	1
51.255.65.58	France	147.237.0.15	kosher-kravi.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
123.126.68.99	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1

08-27-2016-11:04:04 to 08-27-2016-12:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
50.63.197.208	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	8
79.183.34.168	147.237.72.166	Israel	aka.idf.il	ET SCAN NMAP -sA (2)	6
91.121.30.197	147.237.72.166	France	aka.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	4
91.224.160.106	147.237.76.86	Netherlands	navy.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.158	147.237.72.156	Ukraine	aman.idf.il	ET SCAN NMAP -sS window 4096	1
91.201.236.158	147.237.72.156	Ukraine	aman.idf.il	ET SCAN NMAP -f -sS	1
66.249.83.245	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	1
222.186.34.73	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
46.227.67.172	147.237.76.31	Sweden	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
191.255.242.116	147.237.0.16	Brazil	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
91.224.160.106	147.237.76.148	Netherlands	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.76.39	Netherlands	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.158	147.237.72.156	Ukraine	aman.idf.il	ET SCAN NMAP -sS window 2048	1
66.249.93.103	147.237.77.216	Europe	dover.idf.il	portscan: TCP Distributed Portscan	1
216.81.230.167	147.237.77.178	United States	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
109.65.129.84	147.237.0.34	Israel	tikshuv.idf.il	ET SCAN NMAP -sA (2)	1

08-27-2016-11:04:04 to 08-27-2016-12:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.239.13.77	Bosnia and Herzegovina	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10216
46.239.15.195	Bosnia and Herzegovina	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3193
46.239.13.77	Bosnia and Herzegovina	147.237.77.216	dover.idf.il	drop		drop	100
46.239.15.195	Bosnia and Herzegovina	147.237.77.216	dover.idf.il	drop		drop	100
197.134.127.163	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	63
95.91.244.77	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
40.77.169.101	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	20
40.77.169.96	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	15
199.203.152.235	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
40.77.169.103	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	10
94.230.84.180	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
199.203.152.235	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	6
40.77.169.99	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	5
85.64.94.87	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
77.138.52.97	France	147.237.77.216	dover.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
37.46.41.48	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
165.231.96.221	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
191.255.242.116	Brazil	147.237.0.16	my-kosher-kravi.idf.il	drop	First packet isn't SYN	drop	2
213.57.54.189	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
40.77.169.96	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
106.38.241.105	China	147.237.72.167	ishurim.aka.idf.il	drop	SAM rule	drop	1
106.38.241.105	China	147.237.76.86	navy.idf.il	drop	SAM rule	drop	1
80.178.190.33	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
184.105.247.236	United States	147.237.0.35	akaws.idf.il	drop		drop	1
106.38.241.105	China	147.237.77.170	maarachot.idf.il	drop	SAM rule	drop	1
81.218.134.213	Israel	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	1
106.38.241.105	China	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	1
106.38.241.105	China	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
84.95.50.182	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
106.38.241.105	China	147.237.72.156	aman.idf.il	drop	SAM rule	drop	1
213.57.87.62	Israel	147.237.0.19	madim.atal.idf.il	drop	First packet isn't SYN	drop	1
109.253.214.69	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1

08-27-2016-11:04:04 to 08-27-2016-12:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
31.168.26.69	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	101
2.53.13.35	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	14
84.108.180.114	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 84.108.180.114	Block	6
40.77.169.102	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	4
131.253.25.175	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
77.138.65.160	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/smalim.aspx	Block	3
176.13.11.34	Israel	147.237.0.19	madim.atal.idf.i	Suspicious Response Code	Block	3
40.77.169.100	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	3
46.210.154.12	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
5.102.206.114	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
79.178.173.113	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/resources/images/payslips/	Block	2
46.19.85.242	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
84.108.180.114	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/	Block	2
66.249.83.248	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
84.108.180.114	Israel	147.237.77.233	atal.idf.il	Parameter Type Violation search in atal.idf.il/1440-he/atal.aspx	Block	2
64.62.219.155	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
109.186.90.255	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	2
40.77.169.98	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
77.138.46.180	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar	Block	2
64.62.219.165	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
40.77.169.100	United States	147.237.77.176	matpash.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	1
87.69.107.151	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
37.142.199.199	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
66.102.9.118	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
66.249.83.245	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
91.194.84.106	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/tikshuv/index.htm-אתר	Block	1
40.77.169.97	United States	147.237.77.176	matpash.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
77.139.107.209	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/megurim/	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage/files/6/ תשקופי15	Block	1
213.57.87.62	Israel	147.237.0.19	madim.atal.idf.i	SSL Untraceable Connection - Open Mode	None	1
62.128.45.204	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
109.67.179.13	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
40.77.169.98	United States	147.237.77.176	matpash.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
79.176.75.133	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.76.35	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage/files/7/ תשקופי5	Block	1
40.77.169.102	United States	147.237.77.234	halag.idf.il	Illegal Byte Code Character in URL /1090-he/halag.aspx#011404	Block	1
213.57.203.3	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
77.124.9.62	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
79.178.44.134	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/text.css	Block	1
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.76.83	Block	1
41.177.50.198	South Africa	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/accepted.aspx	Block	1
87.68.21.57	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage	Block	1

08-27-2016-11:04:04 to 08-27-2016-12:04:04