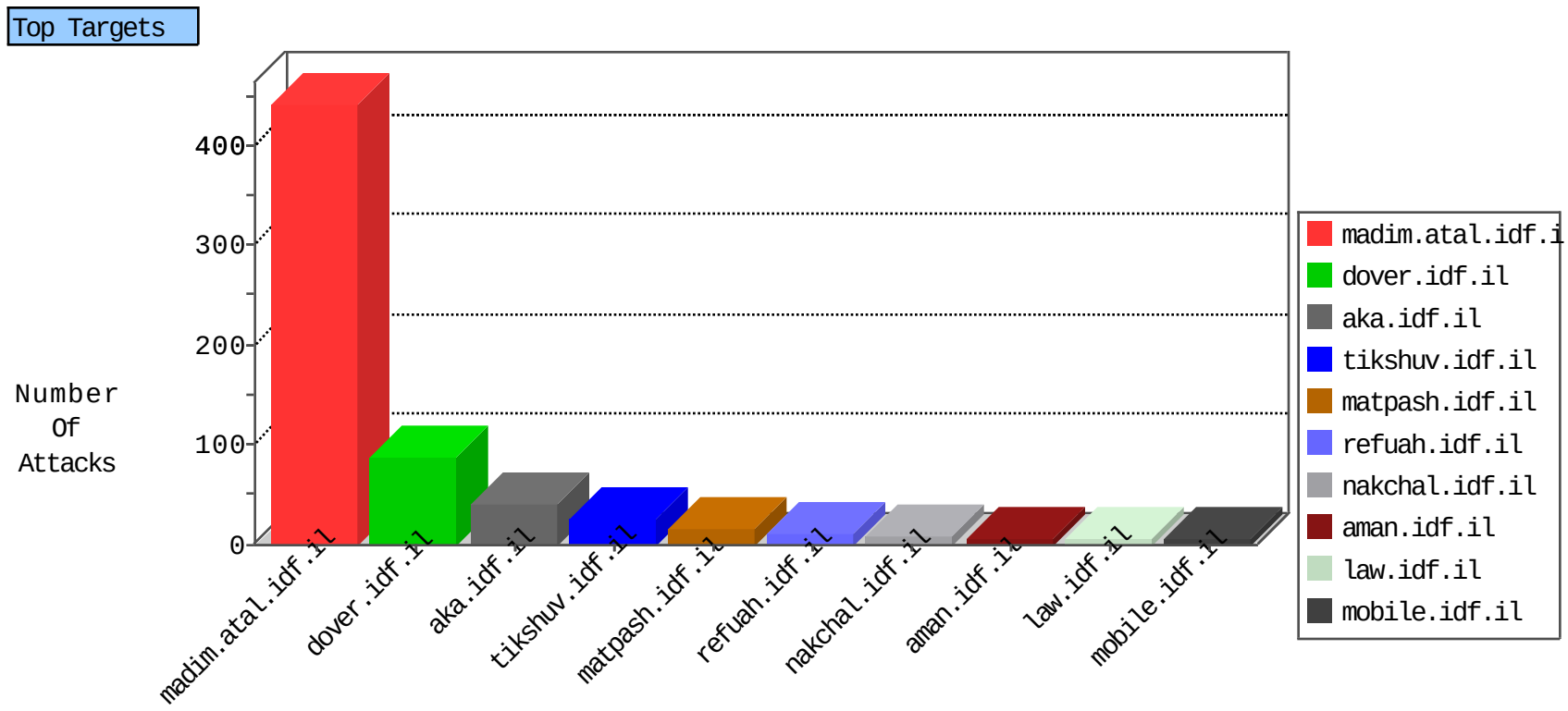
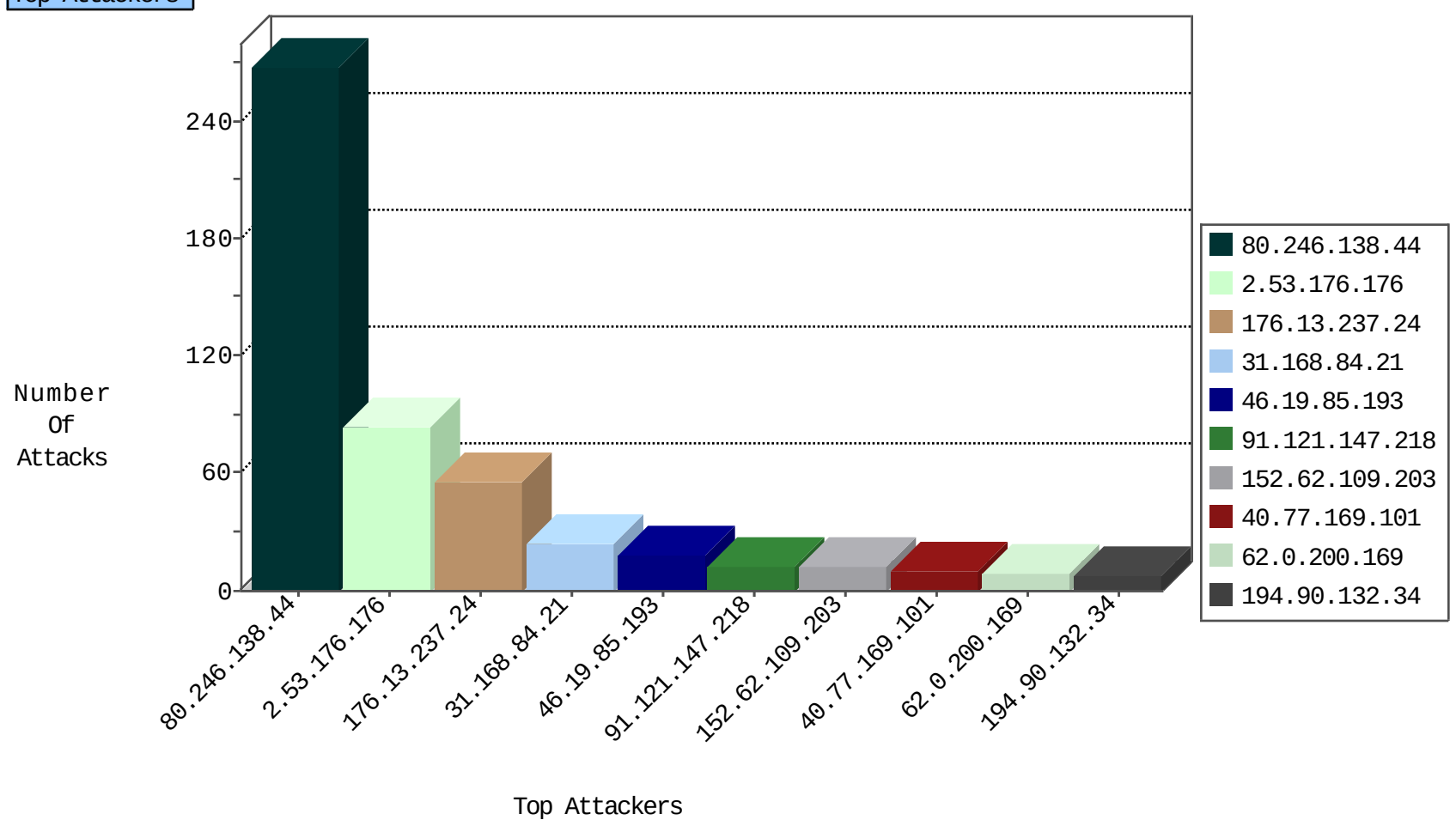
08-25-2016-09:04:04 to 08-25-2016-10:04:04

IDF Under Attack Daily Report

Top Targets



Top Attackers



08-25-2016-09:04:04 to 08-25-2016-10:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
50.206.89.77	United States	147.237.76.30	himush.idf.il	Black List	drop	1
123.59.59.52	China	147.237.72.166	aka.idf.il	block-sp-traf1	forward	1
71.6.165.200	United States	147.237.76.38	e.e.meitav.idf.il	Black List	drop	1
185.128.40.162	Switzerland	147.237.76.30	himush.idf.il	Black List	drop	1
93.158.200.166	Netherlands	147.237.76.44	e.refuah.idf.il	Black List	drop	1
5.22.132.51	Israel	147.237.77.216	dover.idf.il	Black List	drop	1
104.148.35.34	United States	147.237.76.38	e.e.meitav.idf.il	Black List	drop	1

08-25-2016-09:04:04 to 08-25-2016-10:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
195.154.233.177	France	147.237.77.176	matpash.idf.il	19791: HTTP: WordPress N-Media PHP File Upload	Block	1

08-25-2016-09:04:04 to 08-25-2016-10:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
180.97.75.130	147.237.0.33	China	idf.il	ET SCAN NMAP -sS window 1024	1
178.220.165.231	147.237.77.212		e.dover.idf.il	ET SCAN NMAP -sS window 2048	1
133.208.21.66	147.237.77.176	Japan	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
123.206.85.139	147.237.77.212	China	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
109.253.157.28	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
82.80.41.70	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.149.149	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
12.68.215.78	147.237.76.177	United States	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
185.27.105.81	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.53.167.243	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
178.220.165.231	147.237.77.212		e.dover.idf.il	ET SCAN NMAP -sS window 4096	1
178.220.165.231	147.237.77.212		e.dover.idf.il	ET SCAN NMAP -f -sS	1
133.208.21.66	147.237.0.34	Japan	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
123.206.85.139	147.237.77.170	China	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
89.138.182.64	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.246.137.95	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.149.130	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.57.72.251	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.55.151.141	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

08-25-2016-09:04:04 to 08-25-2016-10:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
31.168.84.21	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	24
91.121.147.218	France	147.237.72.166	aka.idf.il	drop	SAM rule	drop	12
152.62.109.203	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
62.0.200.169	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	9
46.19.85.108	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
5.29.168.53	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
40.77.169.101	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
79.181.121.114	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.181	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	5
40.77.169.98	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	5
40.77.169.100	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	5
40.77.169.101	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	4
40.77.169.96	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
176.106.46.74	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
81.218.66.211	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
40.77.169.102	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
193.56.243.6	France	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	3
37.46.41.102	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	3
46.19.85.247	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
46.19.86.110	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	2
151.68.157.63	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
80.246.133.11	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
40.77.169.102	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	2
128.232.110.28	United Kingdom	147.237.76.34	yohalan.idf.il	drop		drop	1
89.139.181.63	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
40.77.169.103	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
139.162.13.205	Singapore	147.237.0.16	my-kosher-kravi.idf.il	drop	SAM rule	drop	1
40.77.169.102	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	1
212.179.210.185	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
109.253.219.203	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	1
128.232.110.28	United Kingdom	147.237.0.200	m4u.idf.il	drop		drop	1

08-25-2016-09:04:04 to 08-25-2016-10:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.246.138.44	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	268
2.53.176.176	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	84
176.13.237.24	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	56
46.19.85.193	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	18
46.210.136.165	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	7
46.19.85.214	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
194.90.132.34	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	4
132.68.43.107	Israel	147.237.77.74	law.idf.il	Distributed Unauthorized HTTP Method	Block	4
77.138.26.134	France	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	3
194.90.132.34	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/sip_storage/files/4/	Block	3
37.26.147.230	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
66.249.69.224	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.224	Block	2
80.246.130.64	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
66.249.76.99	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/sip_storage/files/9/1209.pdftextgreater	Block	1
203.127.96.218	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
46.229.164.99	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
40.77.169.104	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
176.13.248.148	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	1
80.246.130.153	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.64.106	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/eitan/listpage/	Block	1
220.181.108.171	China	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/sip_storage/files/3/size338x0/1613.jpg	Block	1
195.154.233.177	France	147.237.77.176	matpash.idf.il	Distributed Admin Blocking	Block	1
132.68.43.107	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 132.68.43.107	Block	1
66.249.76.106	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/megurim/_blank	Block	1
66.102.9.43	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/drushim/	Block	1
207.46.13.155	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
46.4.15.197	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/rights/asp/info.asp	Block	1
194.90.132.34	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 194.90.132.34	Block	1
66.249.69.194	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 66.249.69.194	Block	1
195.154.233.177	France	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
132.68.43.107	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/sip_storage/files/4/	Block	1
66.102.9.54	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
209.88.198.1	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl56.y in www.aka.idf.il/main/sachar/payslips.aspx	None	1
46.19.85.65	Israel	147.237.76.42	refuah.idf.il	Illegal HTTP Version	Block	1
81.218.89.58	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
195.154.233.177	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/wp-admin/admin-ajax.php	Block	1
46.121.193.127	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 46.121.193.127	Block	1
80.179.118.96	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.64.56	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1244-he/atal.aspx	Block	1
212.179.21.194	Israel	147.237.77.234	halag.idf.il	Multiple Unauthorized URL Access from 212.179.21.194	Block	1
46.19.85.65	Israel	147.237.76.42	refuah.idf.il	Malformed URL he-il,he;q=0.8,en-us;q=0.6,en;q=0.4	Block	1
84.110.108.120	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.76.72	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/.well-known/apple-app-site-association	Block	1
195.200.205.2	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1406-he/atal.aspx	Block	1
176.13.237.101	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
66.249.64.60	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1241-he/atal.aspx	Block	1
212.179.21.194	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/size100x0/sip_storage	Block	1
194.114.146.227	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
46.19.85.65	Israel	147.237.76.42	refuah.idf.il	Unknown HTTP Request Method Language: in URL he-il,he	Block	1

08-25-2016-09:04:04 to 08-25-2016-10:04:04