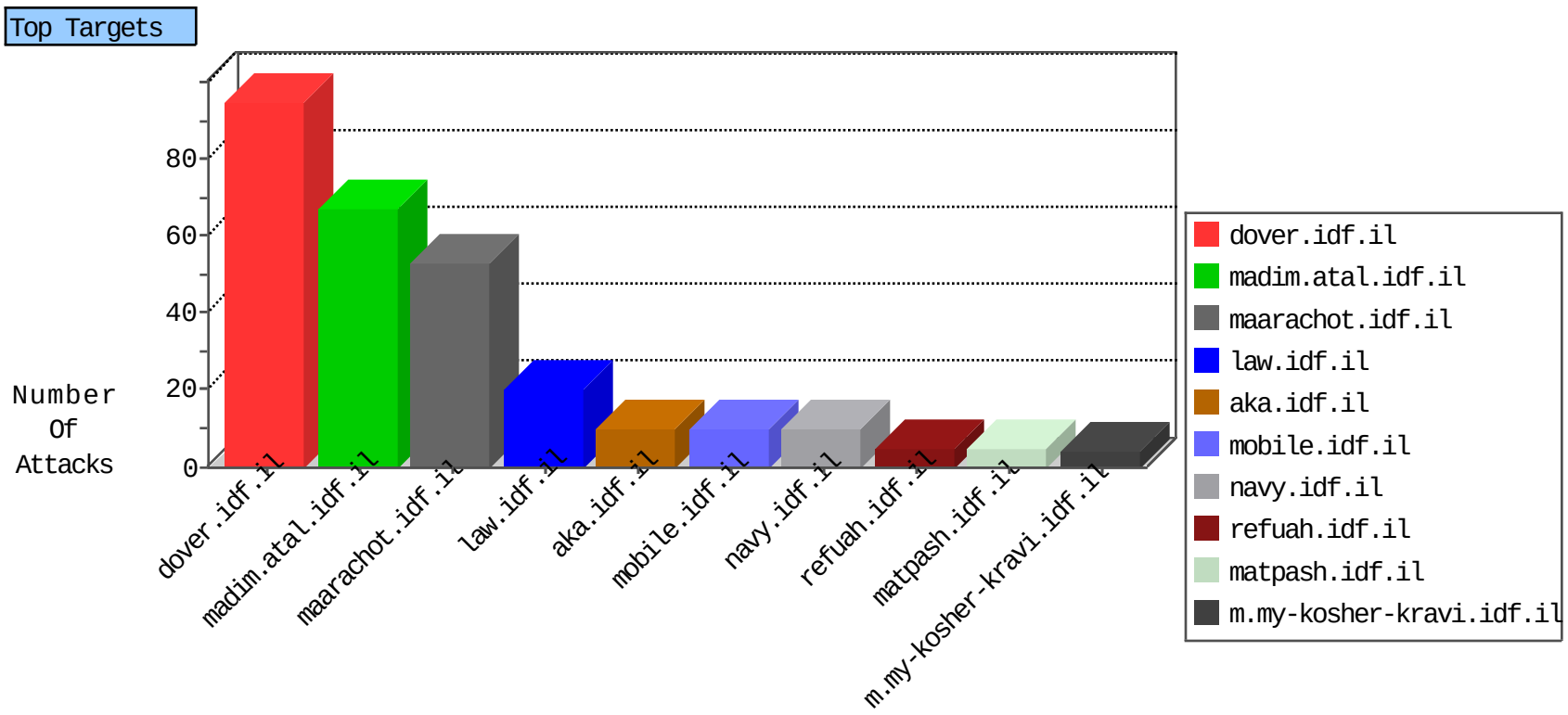
08-24-2016-06:04:03 to 08-24-2016-07:04:03

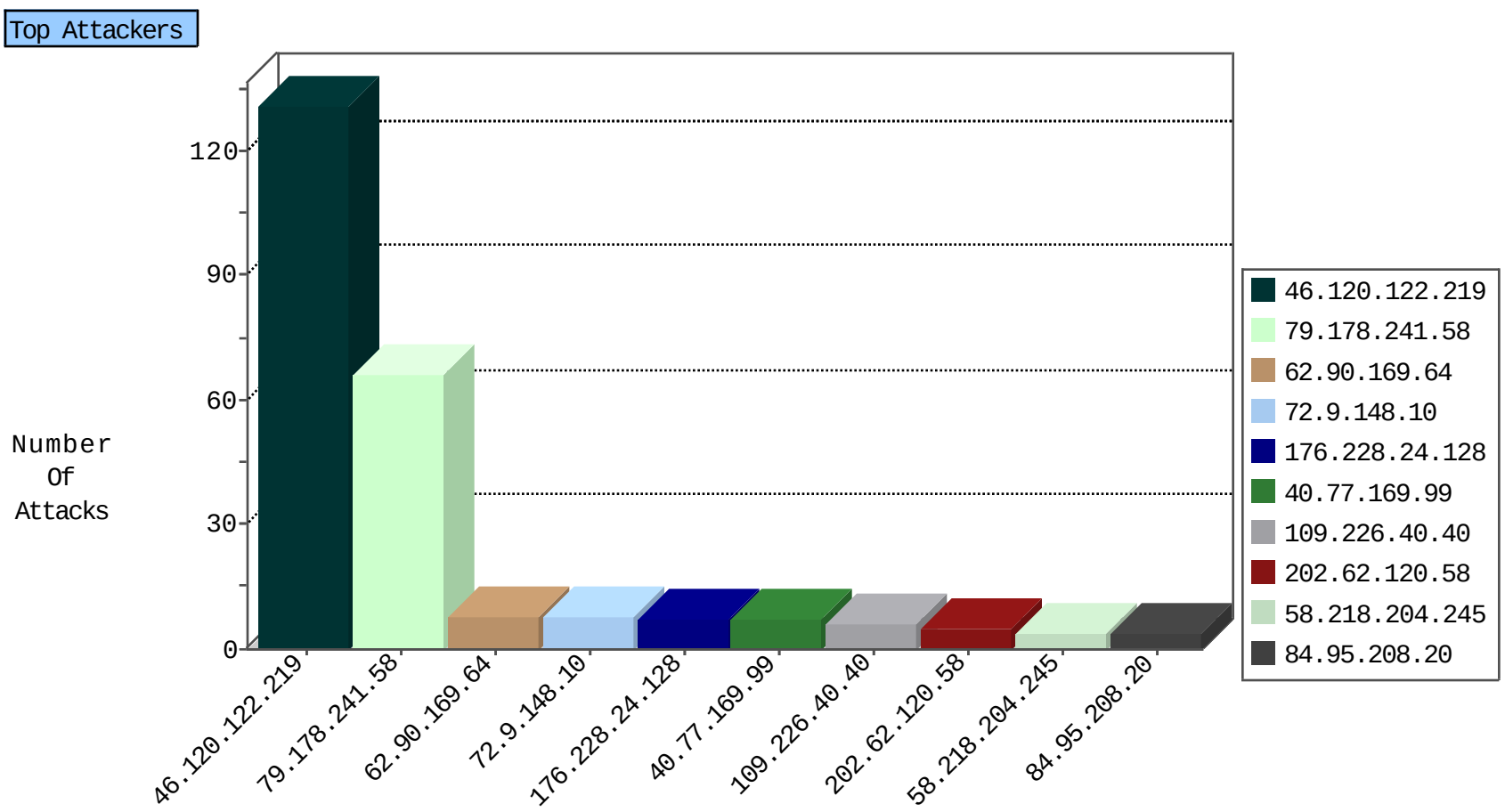
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

08-24-2016-06:04:03 to 08-24-2016-07:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
72.9.148.10	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	8
62.90.169.64	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	8
109.226.40.40	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
202.62.120.58	Fiji	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
213.57.218.213	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
82.80.78.2	Israel	147.237.77.216	dover.idf.il	Black List	drop	2
115.230.125.146	China	147.237.77.61	e.cogat.idf.il	JLM_Purple_Con_Limit_Http	drop	1
94.177.160.214	Romania	147.237.76.38	e.e.meitav.idf.il	Black List	drop	1
77.138.52.97	France	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
104.148.117.90	United States	147.237.76.147	chinuch.aka.idf.il	Black List	drop	1
69.162.116.83	United States	147.237.76.201	e.atal.idf.il	Black List	drop	1
93.158.200.166	Netherlands	147.237.76.39	mobile.meitav.idf.il	Black List	drop	1

08-24-2016-06:04:03 to 08-24-2016-07:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.9.151.22	Germany	147.237.76.86	navy.idf.il	C1000074: HTTP: majestic bot	Permit	2
5.9.151.22	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
36.110.147.67	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	2

08-24-2016-06:04:03 to 08-24-2016-07:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.120.122.219	147.237.77.170	Israel	maarachot.idf.il	Xenu Link Sleuth User Agent	52
46.120.122.219	147.237.77.216	Israel	dover.idf.il	Xenu Link Sleuth User Agent	42
46.120.122.219	147.237.77.74	Israel	law.idf.il	Xenu Link Sleuth User Agent	12
46.120.122.219	147.237.76.86	Israel	navy.idf.il	Xenu Link Sleuth User Agent	8
46.120.122.219	147.237.72.166	Israel	aka.idf.il	Xenu Link Sleuth User Agent	4
46.120.122.219	147.237.77.176	Israel	matpash.idf.il	Xenu Link Sleuth User Agent	4
66.249.66.131	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	3
46.120.122.219	147.237.77.234	Israel	halag.idf.il	Xenu Link Sleuth User Agent	2
46.120.122.219	147.237.76.42	Israel	refuah.idf.il	Xenu Link Sleuth User Agent	2
46.120.122.219	147.237.0.34	Israel	tikshuv.idf.il	Xenu Link Sleuth User Agent	2
133.208.21.66	147.237.77.216	Japan	dover.idf.il	ET SCAN NMAP -sS window 1024	1
116.31.116.12	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.195	147.237.8.45	Netherlands	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.50	147.237.0.17	Ukraine	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 2048	1
8.26.94.207	147.237.0.17	Canada	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.50	147.237.0.17	Ukraine	m.my-kosher-kravi.idf.il	ET SCAN NMAP -f -sS	1
58.218.204.245	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
58.218.204.245	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
176.47.24.205	147.237.77.176	Saudi Arabia	matpash.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
133.242.4.52	147.237.76.197	Japan	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
133.208.21.66	147.237.0.16	Japan	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
116.31.116.12	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
93.174.91.29	147.237.77.74	Netherlands	law.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.50	147.237.0.17	Ukraine	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
58.218.204.245	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
58.218.204.245	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
133.242.4.52	147.237.76.201	Japan	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1

08-24-2016-06:04:03 to 08-24-2016-07:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
40.77.169.99	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
169.229.3.91	United States	147.237.8.46	e.chinuch.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.77.170	maarachot.idf.il	drop	First packet isn't SYN	drop	1
184.105.139.67	United States	147.237.8.28	e.mobile-ks.idf.il	drop	SAM rule	drop	1
46.166.190.205	Netherlands	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
184.105.247.199	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
115.230.125.146	China	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1

08-24-2016-06:04:03 to 08-24-2016-07:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.178.241.58	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	66
176.228.24.128	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	4
176.228.24.128	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 176.228.24.128	Block	3
84.95.208.20	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
66.249.76.30	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1746	Block	2
84.95.208.20	Israel	147.237.77.74	law.idf.il	PHP Attempt	Block	2
66.249.69.224	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	2
46.120.122.219	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 46.120.122.219	Block	2
66.249.66.182	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/4/3384.jpg	Block	1
66.249.76.2	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1682	Block	1
66.249.66.185	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/2/2312.jpg	Block	1
207.46.13.18	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
37.144.80.204	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
66.249.66.188	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/7/2827.jpg	Block	1
68.180.230.171	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1393-en/dover.aspx	Block	1
46.120.122.219	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/smalim/smalim.aspx	Block	1
176.13.249.139	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
77.138.129.44	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
66.249.69.228	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_img.asp	Block	1

08-24-2016-06:04:03 to 08-24-2016-07:04:03