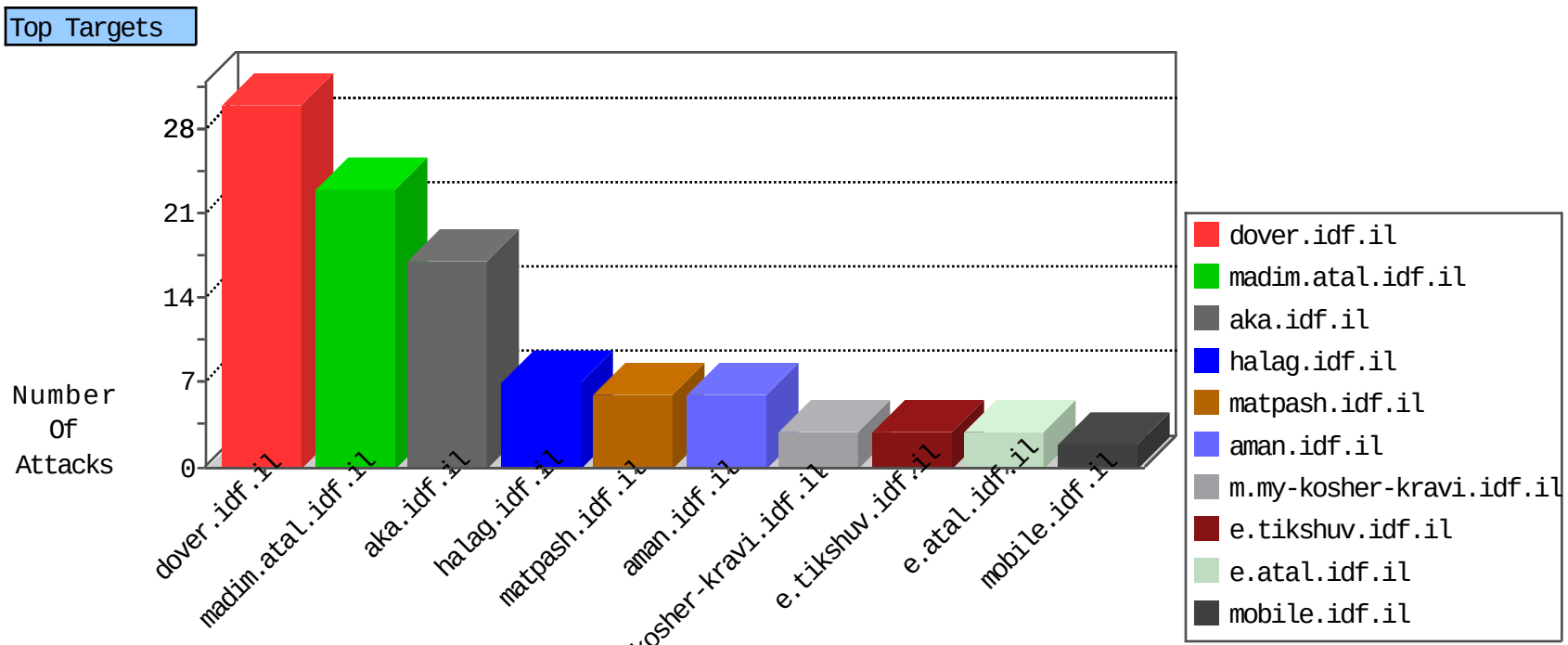
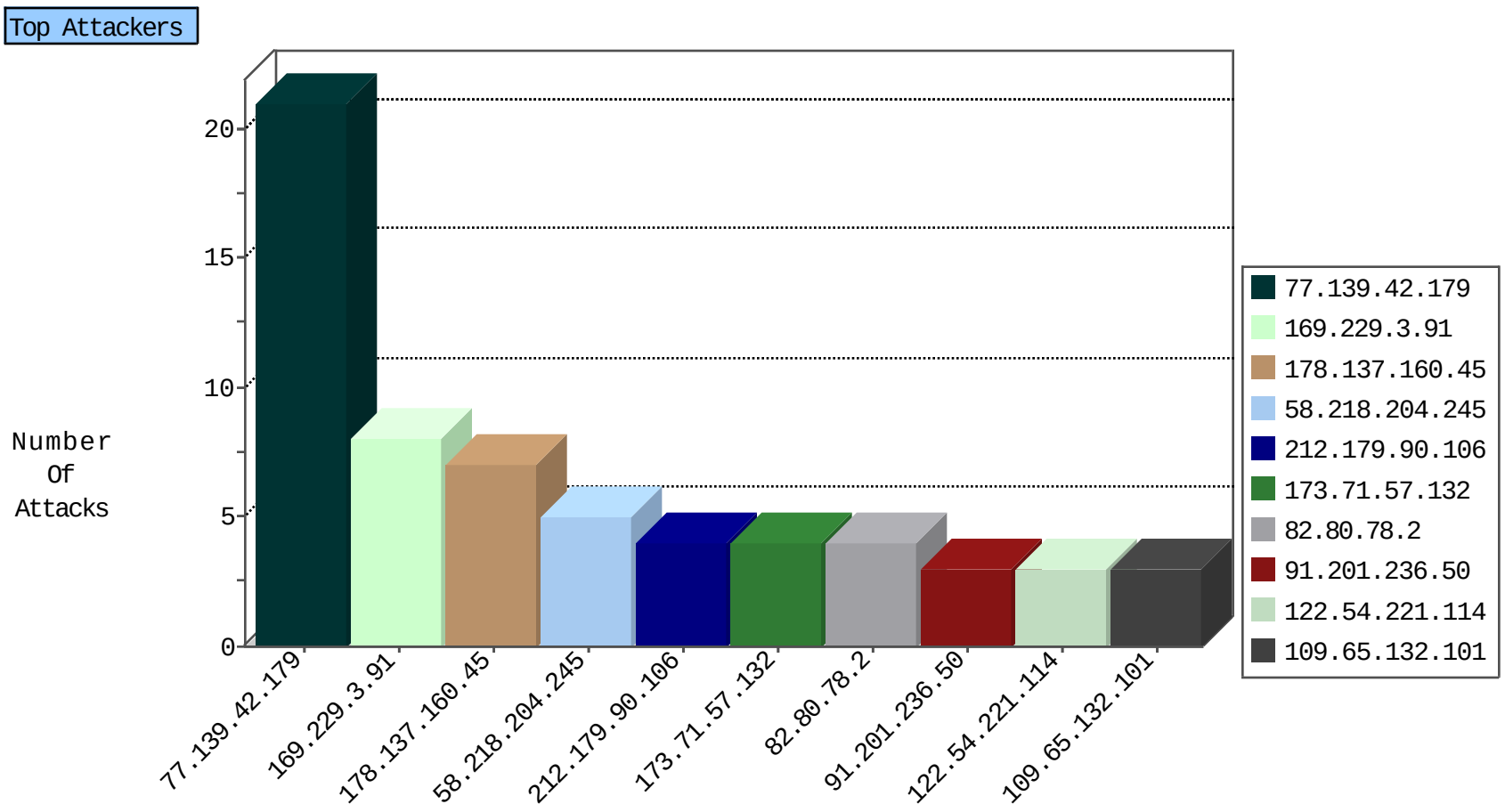
08-18-2016-23:04:08 to 08-19-2016-00:04:08

IDF Under Attack Daily Report

Top Targets



Top Attackers



08-18-2016-23:04:08 to 08-19-2016-00:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
173.71.57.132	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5
82.80.78.2	Israel	147.237.72.166	aka.idf.il	Black List	drop	2
82.80.78.2	Israel	147.237.77.176	matpash.idf.il	Black List	drop	2
120.132.50.135	China	147.237.77.234	halag.idf.il	block-sp-traf1	forward	2
186.170.204.184	Colombia	147.237.76.201	e.atal.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
123.59.59.52	China	147.237.77.234	halag.idf.il	block-sp-traf1	forward	2
186.112.103.75	Colombia	147.237.77.243	mobile.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1

08-18-2016-23:04:08 to 08-19-2016-00:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
178.137.160.45	Ukraine	147.237.72.166	aka.idf.il	C1000016: HTTP: administrator in URI	Permit	7

08-18-2016-23:04:08 to 08-19-2016-00:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
180.97.106.162	147.237.77.234	China	halag.idf.il	ET SCAN Potential SSH Scan	1
118.69.62.83	147.237.0.35	Vietnam	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.155	147.237.8.24	Ukraine	e.lifestyle.idf.il	ET SCAN NMAP -sS window 3072	1
91.201.236.50	147.237.8.50	Ukraine	e.tikshuv.idf.il	ET SCAN NMAP -sS window 2048	1
82.221.128.31	147.237.0.17	Iceland	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
58.218.204.245	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	1
58.218.204.245	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
58.218.204.245	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
183.129.160.229	147.237.8.24	China	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
46.19.86.214	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
180.97.106.37	147.237.77.121	China	e.navy.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.195	147.237.76.201	Netherlands	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.50	147.237.8.50	Ukraine	e.tikshuv.idf.il	ET SCAN NMAP -sS window 4096	1
91.201.236.50	147.237.8.50	Ukraine	e.tikshuv.idf.il	ET SCAN NMAP -f -sS	1
66.249.65.176	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sA (2)	1
58.218.204.245	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
58.218.204.245	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
186.170.204.184	147.237.0.33	Colombia	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
46.227.67.169	147.237.77.61	Sweden	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1

08-18-2016-23:04:08 to 08-19-2016-00:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
109.65.132.101	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	3
122.54.221.114	Philippines	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
79.181.102.81	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
79.254.30.96	Germany	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	2
173.71.57.132	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
100.92.106.175		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
169.229.3.91	United States	147.237.77.121	e.navy.idf.il	drop	SAM rule	drop	1
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.0.200	m4u.idf.il	drop	SAM rule	drop	1
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.77.179	e.mazi.idf.il	drop	SAM rule	drop	1
109.253.211.153	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.8.28	e.mobile-ks.idf.il	drop	SAM rule	drop	1
169.229.3.91	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
115.239.248.35	China	147.237.0.35	akaws.idf.il	drop		drop	1
169.229.3.91	United States	147.237.76.30	himush.idf.il	drop	SAM rule	drop	1
49.145.139.252	Philippines	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.76.86	navy.idf.il	drop	SAM rule	drop	1
191.96.249.18	Chile	147.237.0.33	idf.il	drop		drop	1
169.229.3.91	United States	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	1

08-18-2016-23:04:08 to 08-19-2016-00:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
77.139.42.179	France	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	21
77.43.56.128	Italy	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	2
2.53.33.160	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
80.230.229.100	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
37.142.189.223	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
131.253.25.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
79.181.136.127	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
66.249.66.177	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-22206-he/idfgdover.aspx	Block	1
80.230.229.102	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
46.120.199.195	Israel	147.237.72.167	ishurim.aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
157.55.39.238	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/templates/links/e.navy.idf.il/library/manage/resource/getfilecontent.hh.asp	Block	1
79.182.148.194	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
66.249.66.183	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
85.25.43.151	Germany	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
79.177.58.101	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
66.102.9.85	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	1
80.230.228.9	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.76.46	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/894-ar	Block	1
104.128.144.131	Canada	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/redirect.php	Block	1
79.180.202.1	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 79.180.202.1	Block	1
66.249.65.182	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
80.230.228.244	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
68.180.228.185	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1381-he/dover.aspx	Block	1
37.26.149.143	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
109.64.42.110	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_	Block	1
79.180.202.1	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
66.249.66.153	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/apple-app-site-association	Block	1

08-18-2016-23:04:08 to 08-19-2016-00:04:08