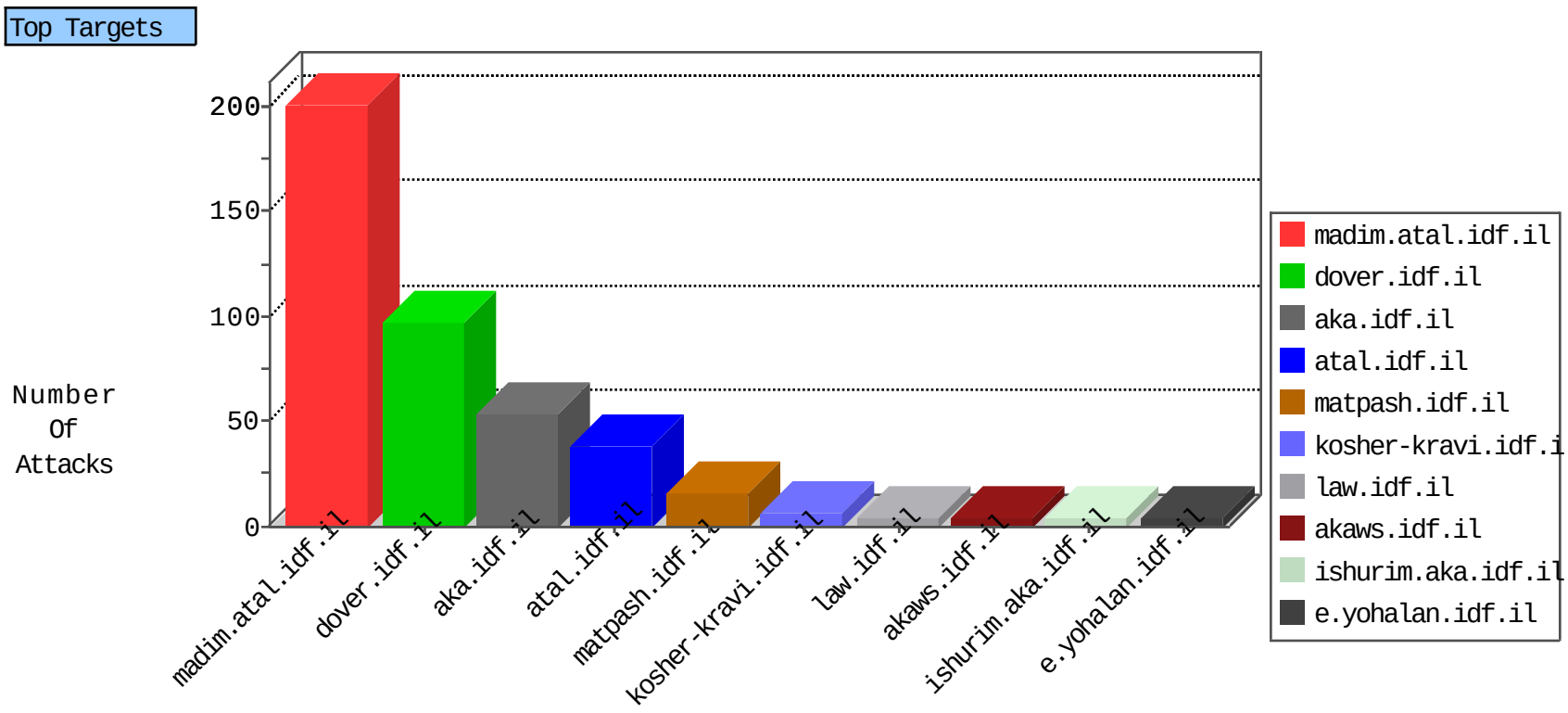
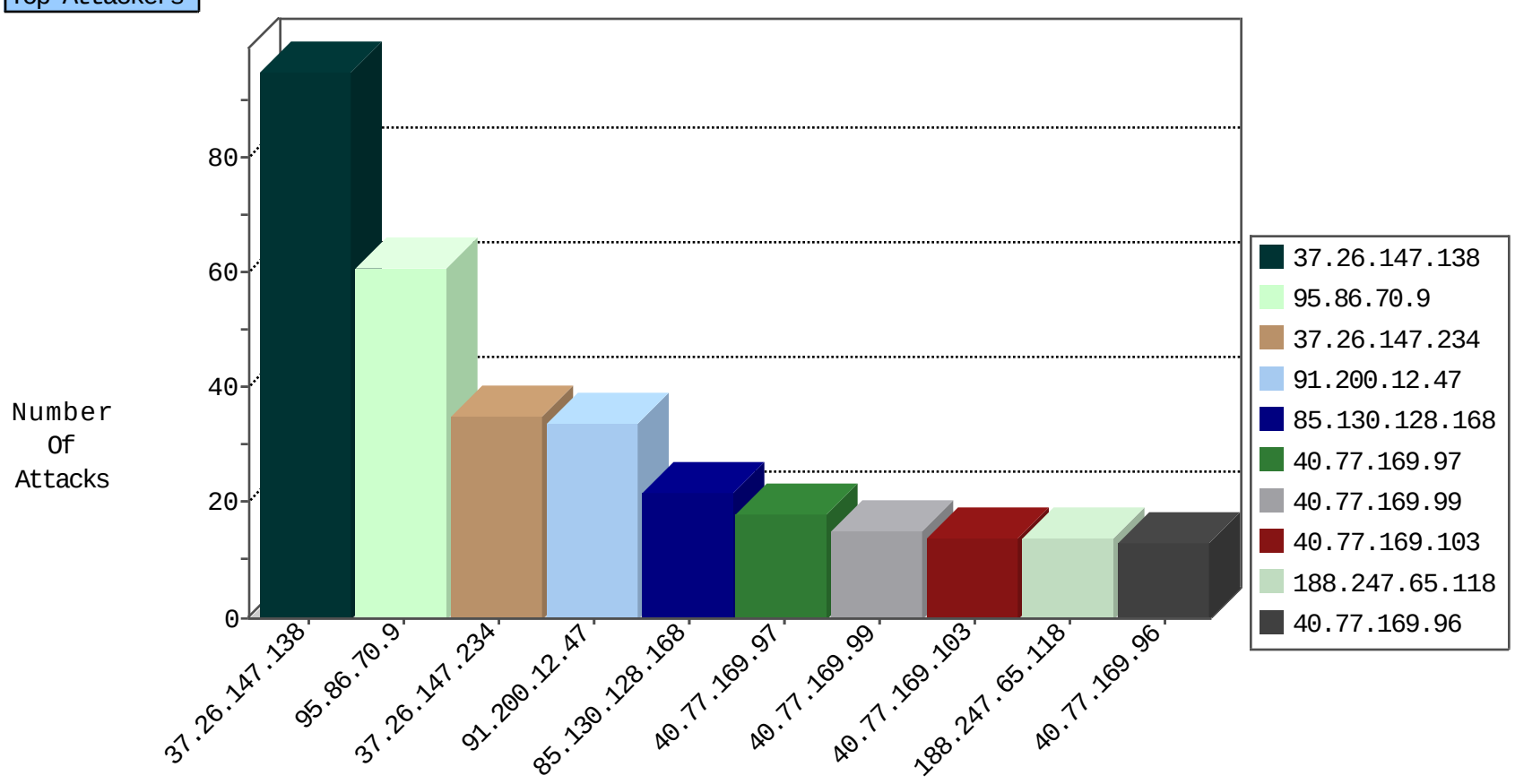
08-25-2016-21:04:08 to 08-25-2016-22:04:08

IDF Under Attack Daily Report

Top Targets



Top Attackers



08-25-2016-21:04:08 to 08-25-2016-22:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.80.78.2	Israel	147.237.72.166	aka.idf.il	Black List	drop	4
71.6.135.131	United States	147.237.76.177	ncore.idf.il	Black List	drop	1
185.94.111.1	Russian Federation	147.237.76.200	eitan.aka.idf.il	Black List	drop	1
79.179.116.228	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
185.94.111.1	Russian Federation	147.237.76.197	e.himush.idf.il	Black List	drop	1

08-25-2016-21:04:08 to 08-25-2016-22:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
91.200.12.47	Ukraine	147.237.77.233	atal.idf.il	C1000016: HTTP: administrator in URI	Permit	6
199.58.86.209	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
123.125.125.83	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1

08-25-2016-21:04:08 to 08-25-2016-22:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
138.128.221.194	147.237.8.50	United States	e.tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
138.128.221.194	147.237.8.45	United States	e.eitan.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
138.128.221.194	147.237.8.27	United States	e.madim.atal.idf.i	ET SCAN Potential VNC Scan 5900-5920	2
138.128.221.194	147.237.8.46	United States	e.chinuch.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
138.128.221.194	147.237.8.28	United States	e.mobile-ks.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
138.128.221.194	147.237.0.33	United States	idf.il	ET SCAN Potential VNC Scan 5900-5920	1
138.128.221.194	147.237.0.15	United States	kosher-kravi.idf.i	ET SCAN Potential VNC Scan 5900-5920	1
198.20.69.74	147.237.76.198	United States	e.yohalan.idf.il	ET DROP Dshield Block Listed Source	1
133.242.3.168	147.237.76.148	Japan	gqcenter.aka.idf.i	ET SCAN NMAP -sS window 1024	1
183.129.160.229	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
133.208.21.66	147.237.76.34	Japan	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
180.97.81.71	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
109.253.199.198	147.237.77.216	Israel	dover.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
180.97.75.130	147.237.72.166	China	aka.idf.il	ET SCAN NMAP -sS window 1024	1
50.116.123.135	147.237.0.33	United States	idf.il	ET SCAN Potential SSH Scan	1
2.53.32.141	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
138.128.221.194	147.237.0.19	United States	madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
133.242.3.168	147.237.77.227	Japan	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
191.96.249.189	147.237.76.30	Chile	himush.idf.il	ET SCAN NMAP -sS window 1024	1
133.208.21.66	147.237.77.212	Japan	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
180.97.106.161	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
109.253.199.198	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
180.97.75.130	147.237.76.198	China	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.195	147.237.76.198	Netherlands	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
169.54.233.118	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sS window 1024	1
2.53.52.177	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

08-25-2016-21:04:08 to 08-25-2016-22:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
85.130.128.168	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
40.77.169.97	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	15
40.77.169.103	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	14
188.247.65.118	Jordan	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	14
40.77.169.96	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	13
40.77.169.101	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	9
40.77.169.99	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	8
40.77.169.99	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	7
185.130.6.49	Lithuania	147.237.0.15	kosher-kravi.idf.il	drop	SAM rule	drop	6
178.134.206.160	Georgia	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.83	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
62.72.193.112	Netherlands	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
82.194.131.128	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
40.77.169.97	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	3
109.253.205.63	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	2
89.139.122.99	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
46.165.197.141	Germany	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
182.72.249.229	India	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
169.229.3.91	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	1
109.253.197.86	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	1
176.13.1.30	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.171	United States	147.237.0.200	m4u.idf.il	drop		drop	1
169.229.3.91	United States	147.237.76.34	yohalan.idf.il	drop	SAM rule	drop	1
45.244.74.52	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
216.243.31.2	United States	147.237.0.35	akaws.idf.il	drop		drop	1
176.13.14.111	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.0.17	m.my-kosher-kravi.idf.il	drop	SAM rule	drop	1
169.229.3.91	United States	147.237.76.196	e.sviva.idf.il	drop	SAM rule	drop	1
141.212.122.101	United States	147.237.0.35	akaws.idf.il	drop		drop	1
216.243.31.2	United States	147.237.0.200	m4u.idf.il	drop		drop	1
176.13.229.13	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.0.35	akaws.idf.il	drop	SAM rule	drop	1
191.96.249.189	Chile	147.237.76.34	yohalan.idf.il	drop		drop	1
169.229.3.91	United States	147.237.76.198	e.yohalan.idf.il	drop	SAM rule	drop	1
141.212.122.102	United States	147.237.0.35	akaws.idf.il	drop		drop	1
169.229.3.91	United States	147.237.8.14	e.orchot.idf.il	drop	SAM rule	drop	1
109.253.134.230	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
191.96.249.189	Chile	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
169.229.3.91	United States	147.237.76.199	e.nakchal.idf.il	drop	SAM rule	drop	1
141.212.122.170	United States	147.237.0.200	m4u.idf.il	drop		drop	1

08-25-2016-21:04:08 to 08-25-2016-22:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.147.138	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	95
95.86.70.9	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	61
37.26.147.234	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	35
91.200.12.47	Ukraine	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 91.200.12.47	Block	26
109.253.199.198	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
176.13.241.60	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.178.104.236	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	3
40.77.169.100	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	3
45.244.75.134	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
40.77.169.98	United States	147.237.77.176	matpash.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
212.199.133.77	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 212.199.133.77	Block	2
80.230.230.184	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/favicon.ico	Block	1
66.249.75.64	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19546-he/idfgdover.aspx	Block	1
157.55.39.229	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in aka.idf.il/chinuch/miktzoa/default.asp	None	1
91.200.12.47	Ukraine	147.237.77.233	atal.idf.il	PHP Attempt	Block	1
77.138.31.160	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/	Block	1
212.199.133.77	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/1319-en/refuah.aspx	Block	1
109.67.98.184	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
85.65.81.5	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/gius	Block	1
66.249.76.72	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/mobile/modiin/general.aspx	Block	1
77.139.247.145	France	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/favicon.ico	Block	1
46.19.86.238	Israel	147.237.76.86	navy.idf.il	Malformed URL	Block	1
85.219.143.163	Poland	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/favicon.ico	Block	1
68.180.228.87	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/1105-en/contactus.aspx	Block	1
178.255.87.242	United Kingdom	147.237.72.167	ishurim.aka.idf.i	Unauthorized URL Access to 147.237.72.167/robots.txt	Block	1
40.77.169.98	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
107.72.162.89	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
46.19.86.238	Israel	147.237.76.86	navy.idf.il	Unknown HTTP Request Method 5pgmkbn45 in URL	Block	1
5.28.160.172	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
148.251.2.180	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/iturim/asp/displayonesoldier.asp	Block	1
91.200.12.47	Ukraine	147.237.77.233	atal.idf.il	Multiple Admin Blocking from 91.200.12.47	Block	1
77.138.31.160	France	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012 ources/images/innerpage/goback.gif	Block	1
203.127.96.233	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
109.64.159.209	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
80.230.230.174	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1250-he/atal.aspx	Block	1
66.240.192.138	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/robots.txt	Block	1
157.55.39.181	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/navmenu/mazi.idf.il	Block	1
77.138.31.160	France	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 77.138.31.160	Block	1
45.244.68.78	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
109.67.98.184	Israel	147.237.77.216	dover.idf.il	PHP Attempt	Block	1

08-25-2016-21:04:08 to 08-25-2016-22:04:08