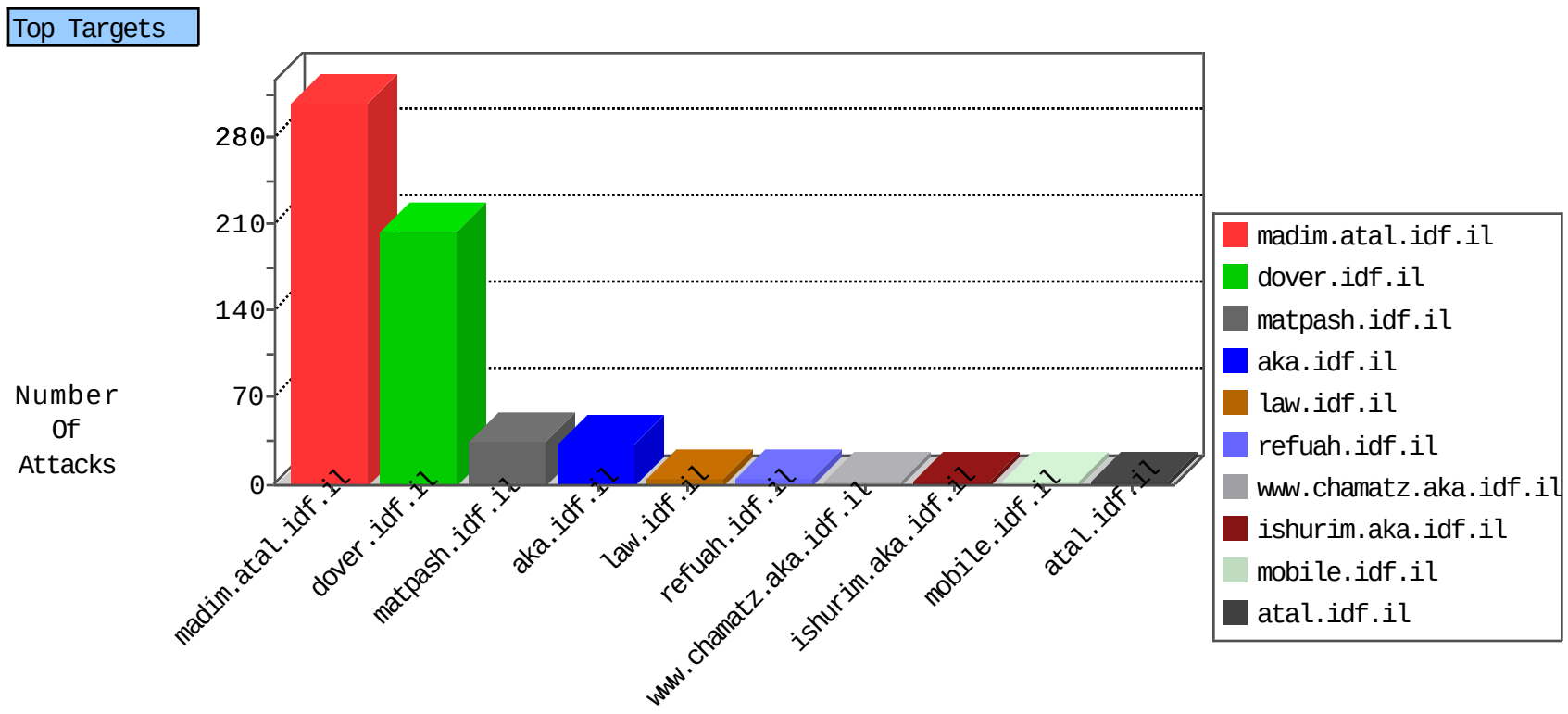
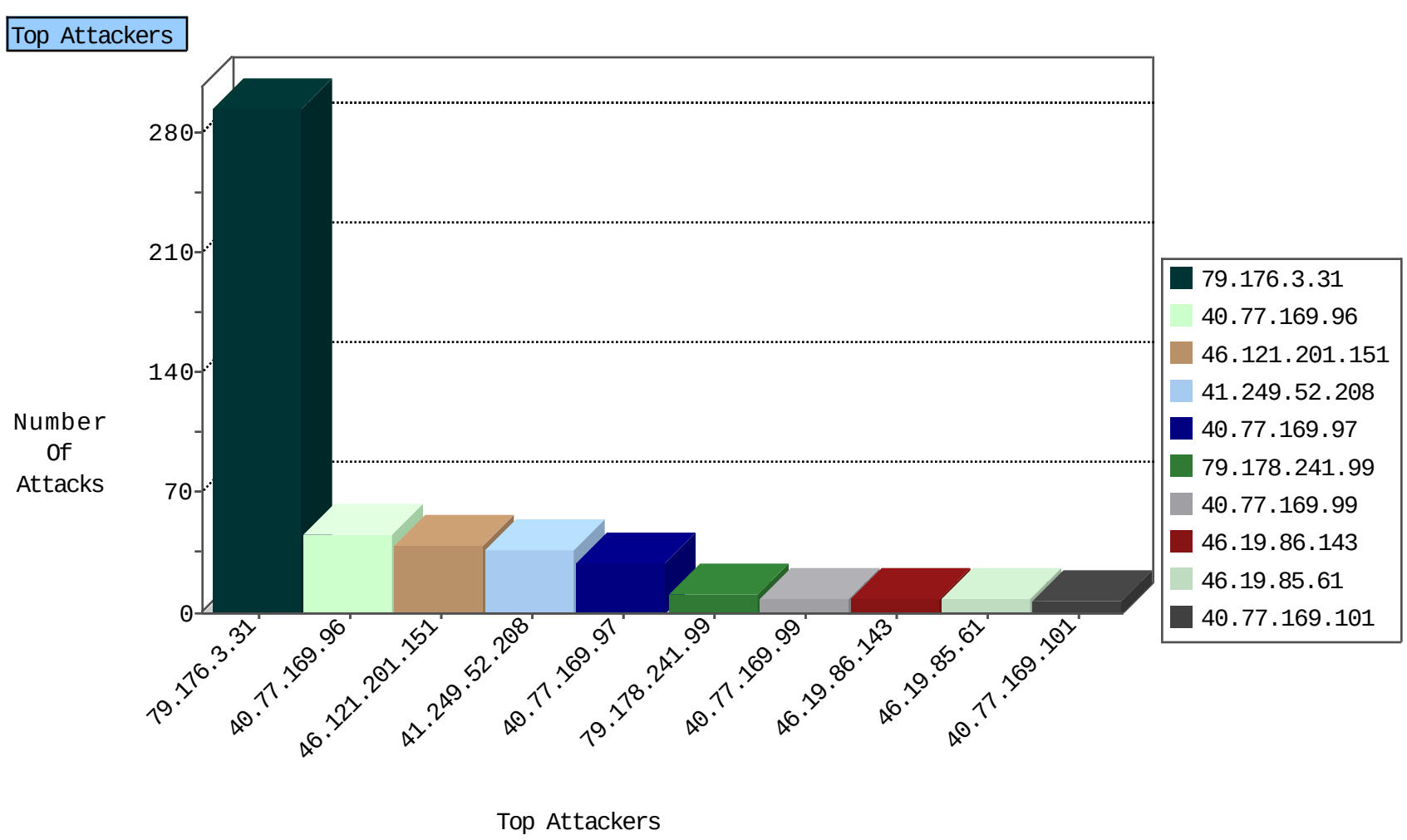
08-25-2016-18:04:01 to 08-25-2016-19:04:01

IDF Under Attack Daily Report

Top Targets



Top Attackers



08-25-2016-18:04:01 to 08-25-2016-19:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
89.237.116.220	France	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	10
46.19.86.143	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
82.80.78.2	Israel	147.237.77.226	www.chamatz.aka.idf.il	Black List	drop	3
120.132.50.135	China	147.237.72.167	ishurim.aka.idf.il	block-sp-traf1	forward	2
79.180.219.23	Israel	147.237.77.216	dover.idf.il	Black List	drop	2
123.59.59.52	China	147.237.72.167	ishurim.aka.idf.il	block-sp-traf1	forward	1

08-25-2016-18:04:01 to 08-25-2016-19:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
199.58.86.206	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	4
108.59.8.80	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
52.32.3.126	United States	147.237.0.34	tikshuv.idf.	12348: HTTP: PHP-CGI Query String Parameter Command Injection Vulnerability	Block	1

08-25-2016-18:04:01 to 08-25-2016-19:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.227.67.172	147.237.76.147	Sweden	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
36.231.232.98	147.237.8.28	Taiwan	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
141.8.132.78	147.237.77.216	Russian Federation	dover.idf.il	portscan: TCP Distributed Portscan	1
95.215.156.30	147.237.76.199	Ukraine	e.nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
95.215.156.30	147.237.0.33	Ukraine	idf.il	ET SCAN Potential VNC Scan 5900-5920	1
95.215.156.30	147.237.0.16	Ukraine	my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
94.102.48.195	147.237.76.199	Netherlands	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.195	147.237.76.147	Netherlands	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
46.227.67.172	147.237.76.198	Sweden	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.85.199	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
198.20.69.98	147.237.72.217	United States	e.idf.il	ET DROP Dshield Block Listed Source	1
123.206.73.185	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
95.215.156.30	147.237.76.38	Ukraine	e.e.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
95.215.156.30	147.237.0.19	Ukraine	madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
94.102.48.195	147.237.77.74	Netherlands	law.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.195	147.237.76.148	Netherlands	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.64.108	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sA (2)	1

08-25-2016-18:04:01 to 08-25-2016-19:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.121.201.151	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
41.249.52.208	Morocco	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
40.77.169.96	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	33
40.77.169.97	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	21
40.77.169.96	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	11
79.178.241.99	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
46.19.85.61	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
40.77.169.101	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	7
40.77.169.99	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	6
46.19.86.143	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
40.77.169.97	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	5
176.13.3.67	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
109.253.144.49	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
2.53.153.124	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
40.77.169.99	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	3
85.64.235.175	Israel	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	2
79.181.23.206	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	SAM rule	drop	2
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
59.96.26.161	India	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	2
157.55.39.37	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
40.77.169.97	United States	147.237.77.216	dover.idf.il	drop		drop	2
192.249.66.247	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
40.77.169.103	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
216.243.31.2	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
62.16.79.25	Russian Federation	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	1
2.55.0.45	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
109.226.40.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
109.253.136.19	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
46.119.127.129	Ukraine	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	1
40.77.169.97	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1

08-25-2016-18:04:01 to 08-25-2016-19:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.176.3.31	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	294
2.53.128.55	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
2.53.160.221	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	2
40.77.169.102	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
87.71.6.189	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.19.86.87	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
77.138.154.4	France	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 77.138.154.4	Block	2
91.197.103.1	Israel	147.237.77.74	law.idf.il	Unauthorized HTTP Method	Block	2
79.176.3.31	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	1
66.249.76.75	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1
91.197.103.1	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/sip_storage/files/4/	Block	1
77.138.216.183	France	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
66.102.9.105	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
176.14.64.87	Russian Federation	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/kapatz/	Block	1
85.113.96.180	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/favicon.ico	Block	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
104.172.166.88	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/miluim/te	Block	1
77.138.216.183	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/kapatz/	Block	1
66.249.64.60	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1437-he/atal.aspx	Block	1
2.53.153.124	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	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
66.249.76.102	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
109.67.211.187	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
77.139.2.223	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
66.249.69.224	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/french/nahal.stm.	Block	1
212.143.66.3	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
91.197.103.1	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 91.197.103.1	Block	1
62.219.160.130	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
157.55.39.37	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_pictures.asp	Block	1
66.249.69.236	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1755	Block	1
37.142.10.94	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
77.138.154.4	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/popups/markivsachar.aspx	Block	1
66.102.9.43	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
157.55.39.132	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1

08-25-2016-18:04:01 to 08-25-2016-19:04:01