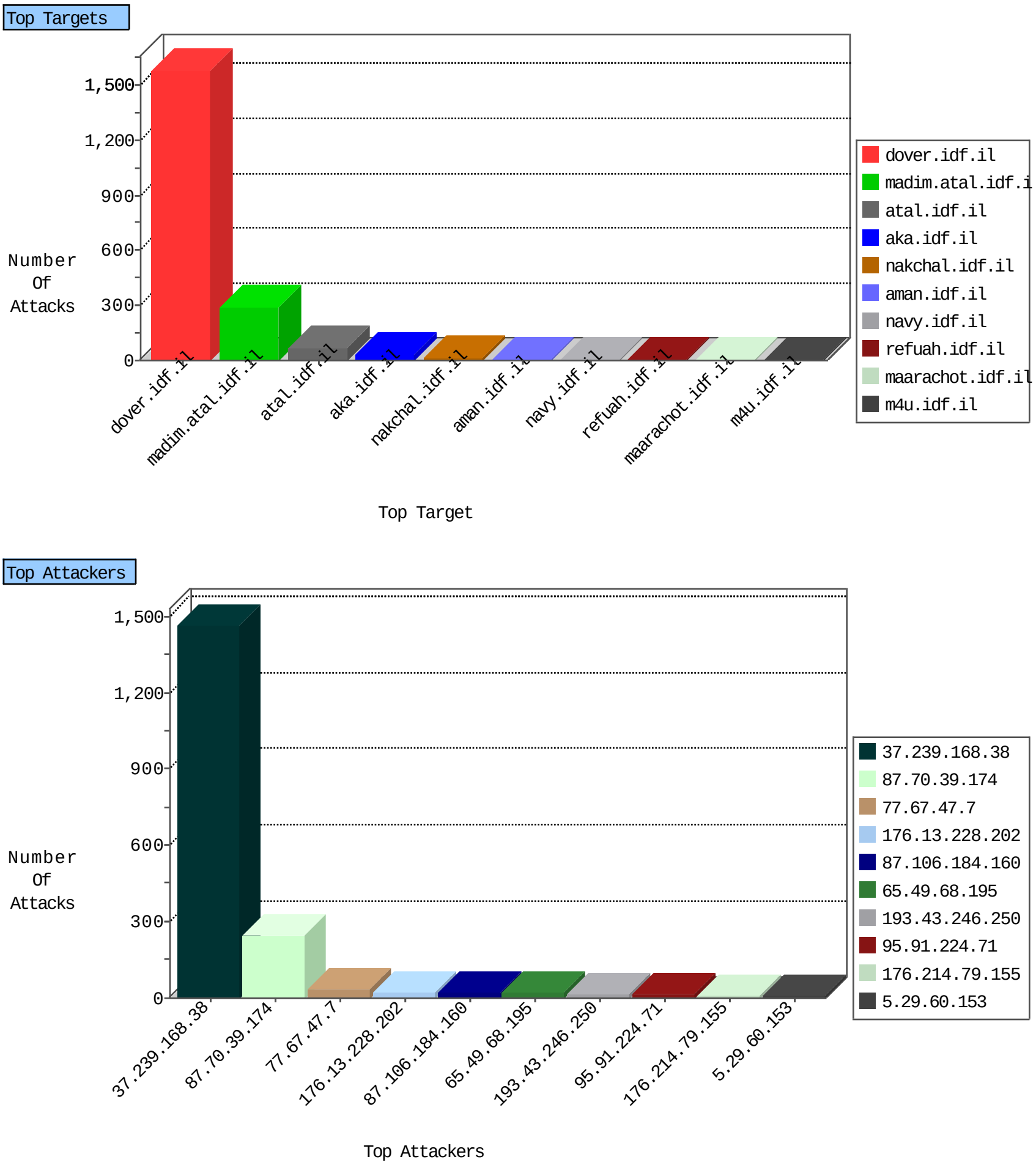
08-16-2016-18:04:09 to 08-16-2016-19:04:09

IDF Under Attack Daily Report



08-16-2016-18:04:09 to 08-16-2016-19:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.80.78.2	Israel	147.237.76.86	navy.idf.il	Black List	drop	3
82.80.78.2	Israel	147.237.72.166	aka.idf.il	Black List	drop	1
82.80.78.2	Israel	147.237.77.216	dover.idf.il	Black List	drop	1

08-16-2016-18:04:09 to 08-16-2016-19:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
77.67.47.7	France	147.237.77.233	atal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	6
77.67.47.7	France	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
77.67.47.7	France	147.237.77.233	atal.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	6
87.106.184.160	Germany	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6

08-16-2016-18:04:09 to 08-16-2016-19:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
77.67.47.7	147.237.77.233	France	atal.idf.il	SQL Injection - Select From	20
87.106.184.160	147.237.77.233	Germany	atal.idf.il	SQL Injection - Select From	17
79.181.154.41	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
94.102.48.195	147.237.0.35	Netherlands	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
89.248.168.29	147.237.77.233	Netherlands	atal.idf.il	ET SCAN NMAP -sS window 1024	1
213.57.173.76	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
72.252.249.125	147.237.76.199	Jamaica	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
193.192.59.61	147.237.76.177	Germany	ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
193.192.59.61	147.237.0.19	Germany	madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
189.62.18.66	147.237.8.28	Brazil	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
113.75.183.188	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
93.158.215.183	147.237.77.212	Netherlands	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
89.248.168.29	147.237.72.166	Netherlands	aka.idf.il	ET SCAN NMAP -sS window 1024	1
84.21.228.166	147.237.0.200	Russian Federation	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
213.57.221.231	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
198.167.223.33	147.237.76.38	Saint Kitts and Nevis	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.76.50	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	1
193.192.59.61	147.237.76.34	Germany	yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
191.96.249.42	147.237.77.170	Chile	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
113.108.10.31	147.237.0.200	China	m4u.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

08-16-2016-18:04:09 to 08-16-2016-19:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
37.239.168.38	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1466
176.13.228.202	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
65.49.68.195	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
176.214.79.155	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
192.118.78.199	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
100.92.22.34		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
37.76.204.25	Palestinian Territory, Occupied	147.237.77.216	dover.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	4
109.64.164.145	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.165	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	3
2.53.164.152	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
182.65.232.140	India	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
93.140.39.224	Croatia	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	2
176.13.13.124	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
66.249.81.212	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
100.92.142.169		147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	2
46.19.86.223	Israel	147.237.76.31	nakchal.idf.il	drop	First packet isn't SYN	drop	2
82.102.169.113	Israel	147.237.72.166	aka.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
46.35.84.197	Yemen	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
216.243.31.2	United States	147.237.0.200	m4u.idf.il	drop		drop	1
180.97.106.161	China	147.237.0.35	akaws.idf.il	drop		drop	1
109.253.136.21	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
180.97.106.162	China	147.237.0.16	my-kosher-kravi.idf.il	drop	SAM rule	drop	1
180.97.106.162	China	147.237.76.31	nakchal.idf.il	drop	SAM rule	drop	1
66.249.81.215	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
180.97.106.162	China	147.237.77.205	prisha.idf.il	drop	SAM rule	drop	1
216.243.31.2	United States	147.237.0.35	akaws.idf.il	drop		drop	1

08-16-2016-18:04:09 to 08-16-2016-19:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
87.70.39.174	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	233
95.91.224.71	Germany	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	13
5.29.60.153	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	6
85.250.177.16	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	5
87.69.37.33	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	4
80.246.133.240	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
5.29.71.189	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.78.146	Block	3
37.26.146.171	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.55.171.122	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
87.69.37.33	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/sip_storage/files/2/	Block	3
37.142.1.204	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
185.32.179.179	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.239.168.38	Iraq	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	3
87.70.39.174	Israel	147.237.0.19	madim.atal.idf.il	Untraceable SSL Sessions: Open Mode	None	3
2.53.152.191	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
5.29.60.153	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
80.246.133.43	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
46.19.86.6	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	2
62.107.66.237	Denmark	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/2/4912.png	Block	1
176.13.19.32	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
87.69.37.33	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 87.69.37.33	Block	1
42.118.243.201	Vietnam	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/miyun/miyunselectquestionnaire.aspx	Block	1
194.90.128.185	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/1.he/trigger.png	Block	1
95.35.51.149	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
2.53.158.130	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
84.111.18.152	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.102.9.105	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
176.228.56.14	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 176.228.56.14	Block	1
77.127.16.157	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
46.19.85.128	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
202.155.252.3	Hong Kong	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/miyun/miyunselectquestionnaire.aspx	Block	1
95.35.188.194	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
85.64.68.213	Israel	147.237.77.74	law.idf.il	PHP Attempt	Block	1
66.240.236.119	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/robots.txt	Block	1
37.26.148.205	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/www.navy.idf.il	Block	1
176.228.56.14	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
77.138.102.146	France	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl12$ctl01$ctl03$radQuestion in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
46.19.85.144	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
213.151.35.214	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 213.151.35.214	Block	1
85.64.68.213	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/wp-login.php	Block	1
66.249.64.160	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to eitan.aka.idf.il/templates/shared/usercontrols/headerupper/	Block	1
213.151.35.214	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/rabanut/contactus.aspx	Block	1
173.76.32.120	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
66.249.76.122	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding rnd in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	1
194.90.128.185	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 194.90.128.185	Block	1

08-16-2016-18:04:09 to 08-16-2016-19:04:09