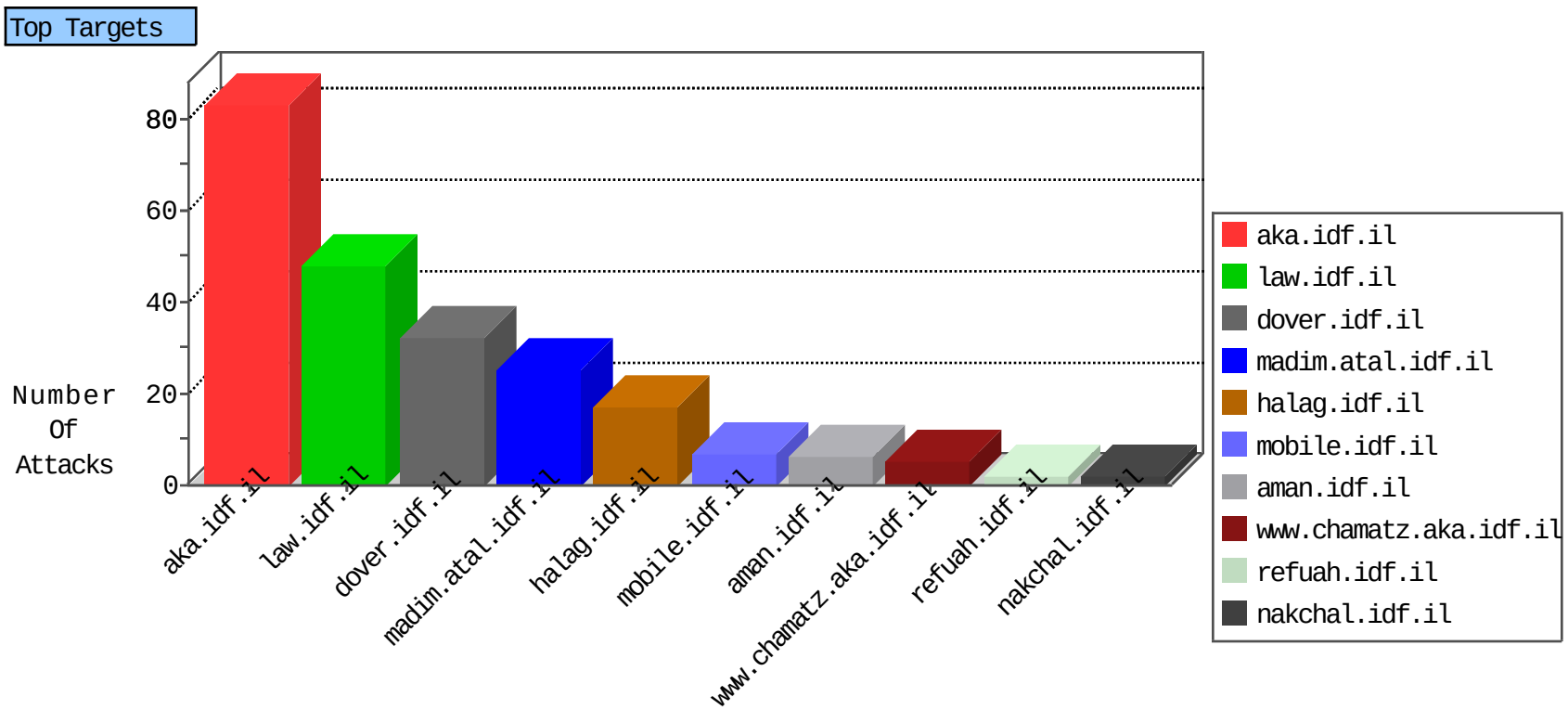
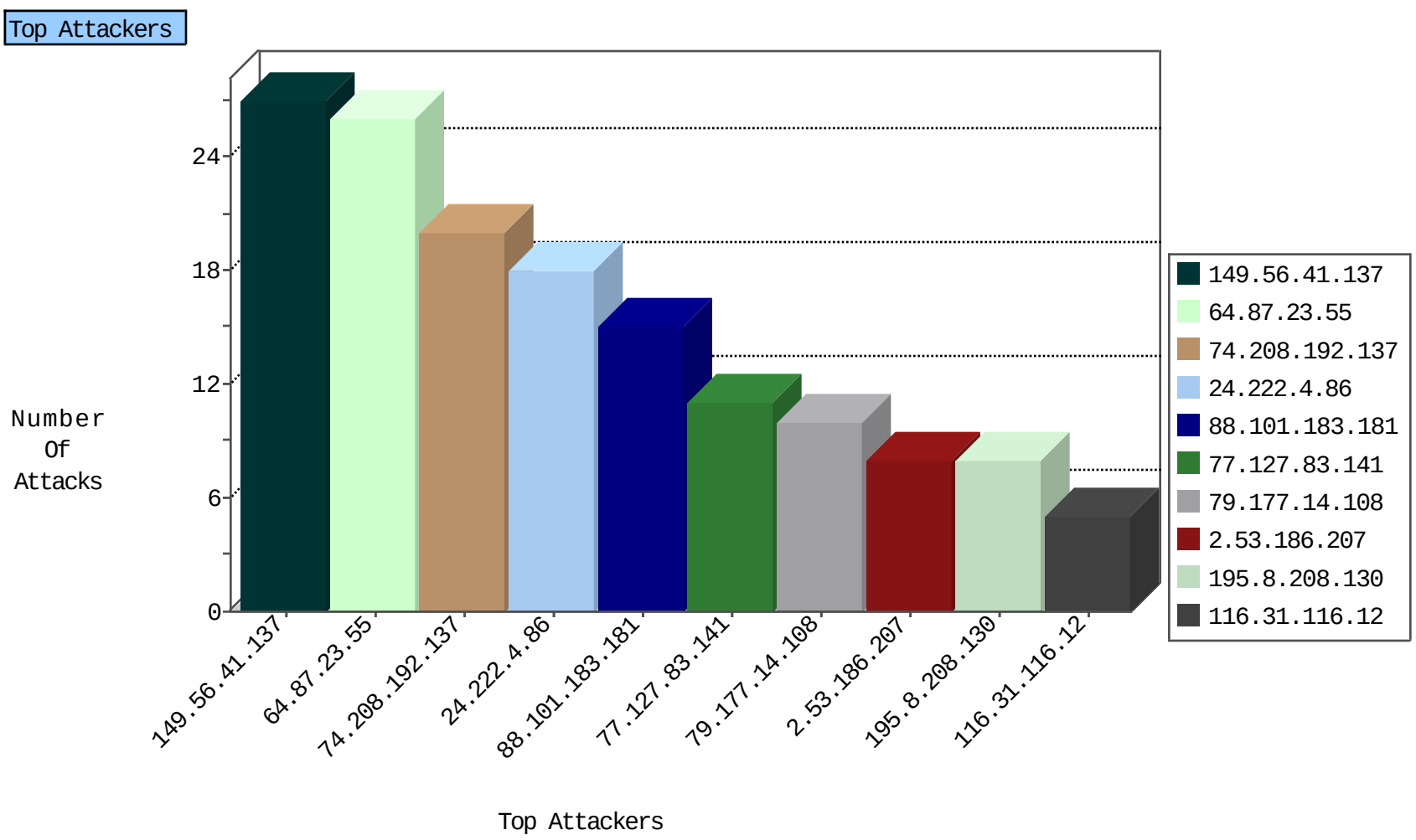
09-03-2016-19:04:05 to 09-03-2016-20:04:05

IDF Under Attack Daily Report





Top Target

Top Attackers

09-03-2016-19:04:05 to 09-03-2016-20:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.180.55.64	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
149.56.41.137	United States	147.237.77.74	law.idf.il	HTTP-Misc-BadBlue-Dir-Trave-2	dest-reset	3
134.147.203.115	Germany	147.237.76.199	e.nakchal.idf.il	Black List	drop	2
17.142.156.109	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
217.23.9.123	Netherlands	147.237.76.176	test.ncore.idf.il	Black List	drop	1

09-03-2016-19:04:05 to 09-03-2016-20:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

09-03-2016-19:04:05 to 09-03-2016-20:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
64.87.23.55	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	26
74.208.192.137	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	20
149.56.41.137	147.237.77.74	United States	law.idf.il	Tehila - Perl LWP with fake user agent	19
24.222.4.86	147.237.77.74	Canada	law.idf.il	SQL Injection - Select From	18
195.8.208.130	147.237.72.166	Netherlands	aka.idf.il	SQL Injection - Select From	8
46.120.122.219	147.237.72.166	Israel	aka.idf.il	Xenu Link Sleuth User Agent	2
116.31.116.12	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
116.31.116.12	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1
87.236.194.161	147.237.77.227	Czech Republic	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
208.100.26.228	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
54.72.73.168	147.237.77.216	Ireland	dover.idf.il	portscan: TCP Distributed Portscan	1
177.200.192.50	147.237.8.45	Brazil	e.eitan.idf.il	ET SCAN NMAP -sS window 2048	1
45.79.111.169	147.237.72.166	United States	aka.idf.il	WEB-MISC Chunked-Encoding transfer attempt	1
139.162.225.219	147.237.77.212	United States	e.dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
116.31.116.12	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	1
116.31.116.12	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
116.31.116.12	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
63.142.161.5	147.237.77.121	Canada	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
177.200.192.50	147.237.8.45	Brazil	e.eitan.idf.il	ET SCAN NMAP -f -sS	1
149.56.41.137	147.237.77.74	United States	law.idf.il	ET WEB_SERVER Exploit Suspected PHP Injection Attack (cmd=)	1
117.135.131.60	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1

09-03-2016-19:04:05 to 09-03-2016-20:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
88.101.183.181	Czech Republic	147.237.77.234	halag.idf.il	drop	First packet isn't SYN	drop	15
77.127.83.141	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
79.177.14.108	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	10
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
109.253.205.20	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	3
79.180.55.64	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
31.154.81.4	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
213.8.204.49	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
178.134.206.160	Georgia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
86.253.10.198	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
46.121.112.160	Israel	147.237.77.233	atal.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

09-03-2016-19:04:05 to 09-03-2016-20:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.186.207	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
84.108.249.206	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
84.111.102.219	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
149.56.41.137	United States	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 149.56.41.137	Block	4
2.53.156.6	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.178.166.22	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
5.29.150.68	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
87.69.184.148	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.68	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.136	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
77.138.167.221	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	2
68.180.228.29	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/האתר	Block	1
62.219.46.86	Israel	147.237.72.156	aman.idf.il	Multiple Untraceable SSL Sessions from 62.219.46.86 (Open Mode)	None	1
45.79.111.169	United States	147.237.72.166	aka.idf.il	Malformed HTTP Header Line 1	Block	1
93.172.239.120	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.64.147	Israel	147.237.77.226	www.chamatz.aka.idf.il	Distributed Unauthorized URL Access on www.chamatz.aka.idf.il/1119-he/idfg.aspxאם	Block	1
198.57.247.239	United States	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 198.57.247.239	Block	1
46.19.86.174	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
68.180.230.47	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/en	Block	1
62.219.46.86	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
45.79.111.169	United States	147.237.72.166	aka.idf.il	Malformed URL	Block	1
109.65.43.177	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
79.178.194.232	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
66.249.66.187	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/602-2265-he/patzar.aspx - paragraph_12	Block	1
207.46.13.90	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
46.116.103.9	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/matash	Block	1
85.250.222.198	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
66.102.9.24	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
45.79.111.169	United States	147.237.72.166	aka.idf.il	Unknown HTTP Request Method 1 in URL	Block	1
79.182.32.108	Israel	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
66.249.66.213	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/templates/shared/usercontrols/navmenu/	Block	1
207.46.13.134	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/print_bottom.asp	Block	1
46.120.160.252	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
5.102.242.210	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/1119-he/idfg.aspxDX	Block	1
79.177.217.226	Israel	147.237.77.226	www.chamatz.aka.idf.il	Distributed Unauthorized URL Access on www.chamatz.aka.idf.il/1119-he/idfg.aspxDX	Block	1
66.249.64.66	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/giyus/general/	Block	1
185.159.36.10		147.237.77.234	halag.idf.il	Multiple Unauthorized URL Access from 185.159.36.10	Block	1
79.182.32.108	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/wp-login.php	Block	1
66.249.76.73	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/robots.txt	Block	1
46.121.195.145	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
5.197.92.33	Azerbaijan	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar	Block	1
89.139.170.120	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
79.178.52.24	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/homepage/homepage.aspx	Block	1
66.249.64.126	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/main/sachar/klali.aspx	Block	1
198.57.247.239	United States	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1

09-03-2016-19:04:05 to 09-03-2016-20:04:05