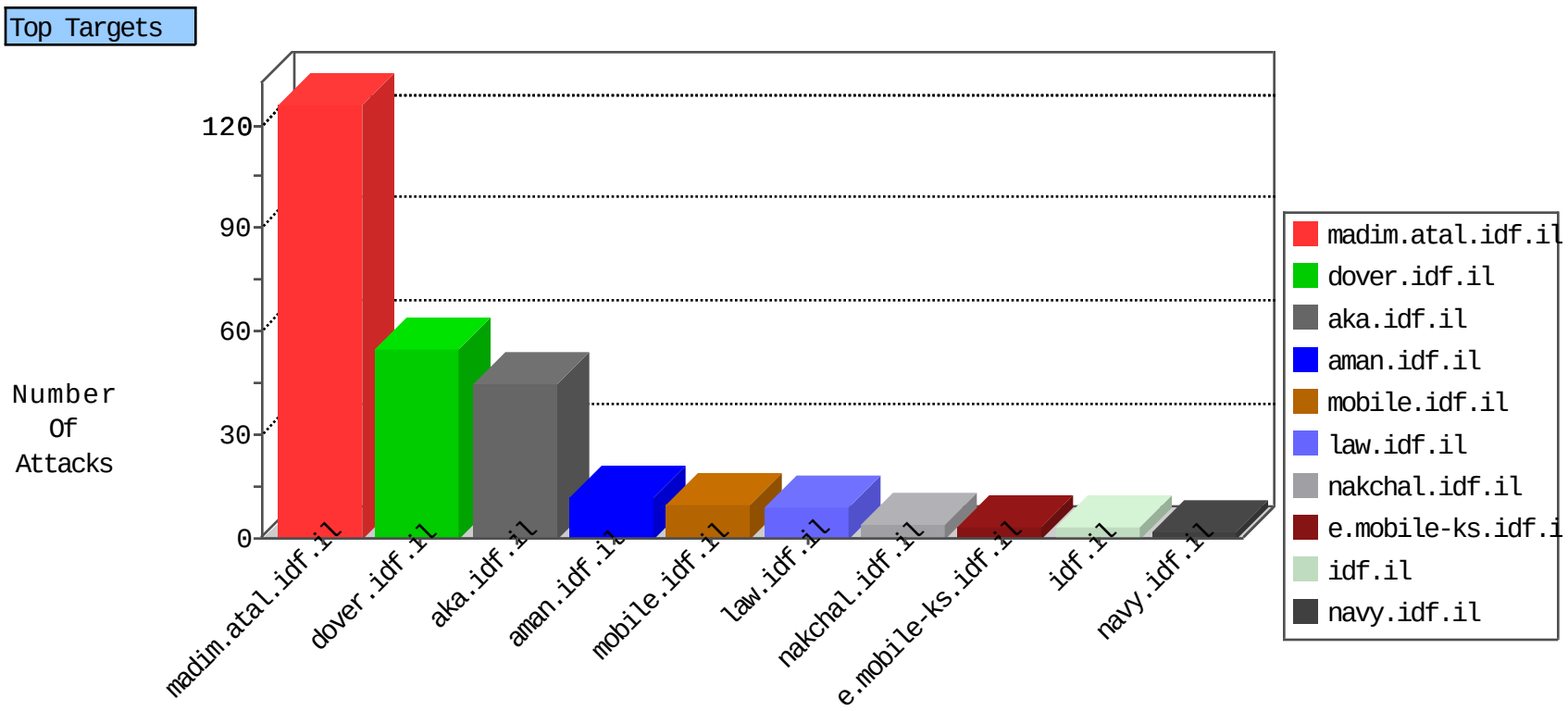
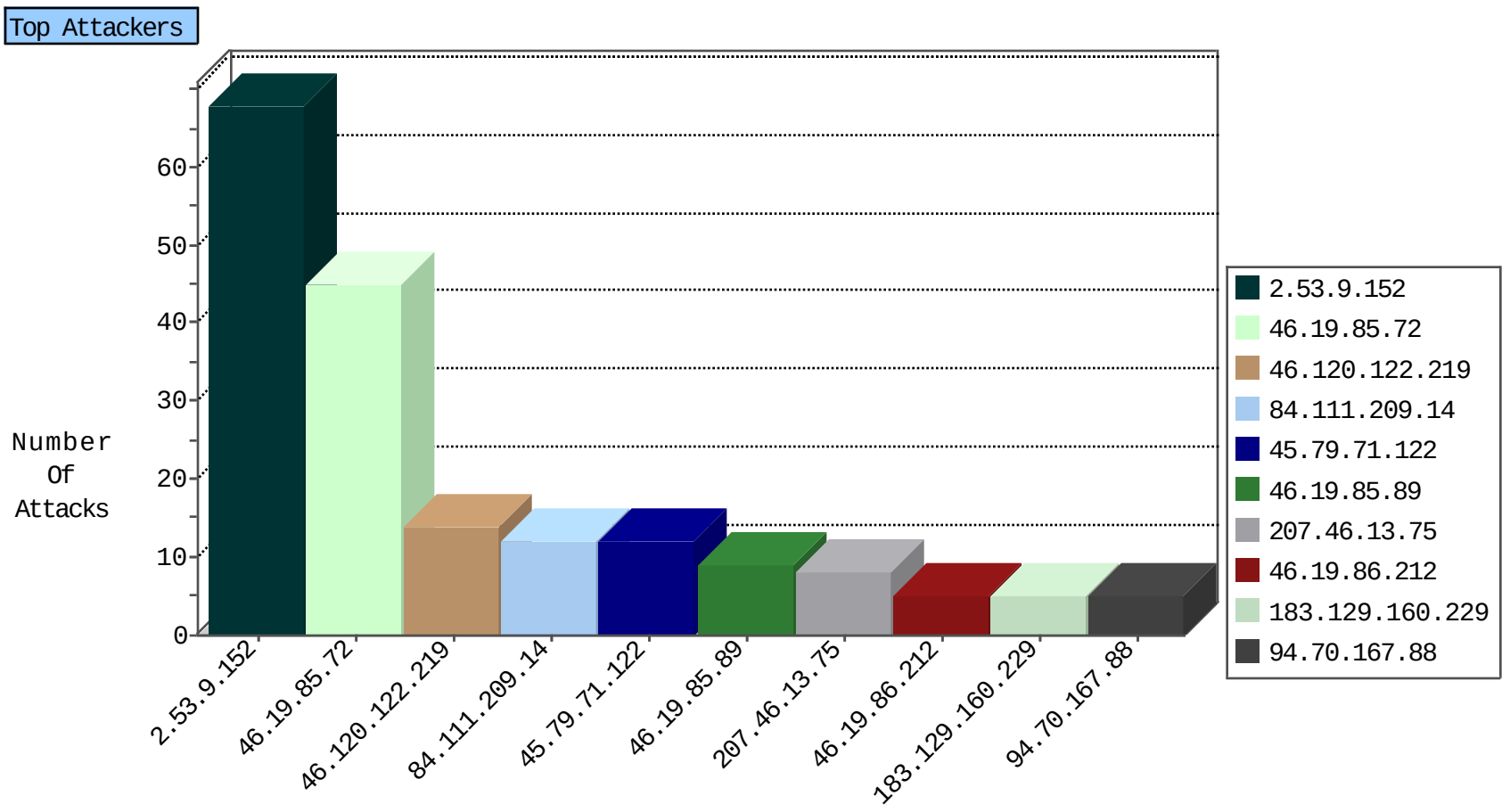
09-04-2016-00:04:07 to 09-04-2016-01:04:07

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-04-2016-00:04:07 to 09-04-2016-01:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
117.21.191.10	China	147.237.0.33	idf.il	Frk_Under_Attack_Con_Tcp	drop	2
114.112.153.187	China	147.237.76.197	e.himush.idf.il	JLM_Under_Attack_Con_Tcp	drop	1

09-04-2016-00:04:07 to 09-04-2016-01:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

09-04-2016-00:04:07 to 09-04-2016-01:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.120.122.219	147.237.77.216	Israel	dover.idf.il	Xenu Link Sleuth User Agent	10
46.120.122.219	147.237.77.74	Israel	law.idf.il	Xenu Link Sleuth User Agent	4
45.79.71.122	147.237.72.156	United States	aman.idf.il	WEB-MISC Chunked-Encoding transfer attempt	2
217.165.67.151	147.237.72.166	United Arab Emirates	aka.idf.il	ET SCAN NMAP -f -sS	1
190.196.178.78	147.237.8.28	Chile	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 3072	1
190.196.178.78	147.237.8.28	Chile	e.mobile-ks.idf.il	ET SCAN NMAP -f -sS	1
163.172.238.37	147.237.77.179	United Kingdom	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
109.226.40.40	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.180.110.141	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.9	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
217.165.67.151	147.237.72.166	United Arab Emirates	aka.idf.il	ET SCAN NMAP -sS window 2048	1
208.100.26.228	147.237.76.177	United States	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
190.196.178.78	147.237.8.28	Chile	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 2048	1
163.172.238.40	147.237.72.14	United Kingdom	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
122.178.17.197	147.237.76.31	India	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
79.182.164.108	147.237.72.156	Israel	aman.idf.il	ET SCAN NMAP -sA (2)	1
64.137.171.55	147.237.76.38	Canada	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
217.165.67.151	147.237.72.166	United Arab Emirates	aka.idf.il	ET SCAN NMAP -sS window 4096	1
45.79.71.122	147.237.72.166	United States	aka.idf.il	WEB-MISC Chunked-Encoding transfer attempt	1

09-04-2016-00:04:07 to 09-04-2016-01:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
84.111.209.14	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	12
207.46.13.75	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	8
46.19.85.89	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	6
46.19.85.89	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	3
2.54.197.163	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
195.239.16.53	Russian Federation	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	2
81.218.106.146	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
151.27.125.217	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
195.239.16.40	Russian Federation	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	2
112.204.203.154	Philippines	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
109.67.109.31	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	2
138.68.17.158	United States	147.237.0.200	m4u.idf.il	drop		drop	1
183.129.160.229	China	147.237.77.61	e.cogat.idf.il	drop	SAM rule	drop	1
109.160.200.213	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
183.129.160.229	China	147.237.77.121	e.navy.idf.il	drop	SAM rule	drop	1
109.253.144.121	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
209.141.39.34	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
176.13.251.197	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
85.65.164.165	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
183.129.160.229	China	147.237.77.235	sviva.idf.il	drop	SAM rule	drop	1
109.253.156.7	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
46.19.86.3	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
183.129.160.229	China	147.237.76.200	eitan.aka.idf.il	drop	SAM rule	drop	1
109.64.161.236	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	1
66.249.69.2	Israel	147.237.0.33	idf.il	drop		drop	1
183.129.160.229	China	147.237.77.19	law-forum.idf.il	drop	SAM rule	drop	1
31.146.14.189	Georgia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1

09-04-2016-00:04:07 to 09-04-2016-01:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.9.152	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	68
46.19.85.72	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	45
46.19.86.212	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
94.70.167.88	Greece	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	5
79.178.136.133	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
176.13.12.27	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
85.130.241.137	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
66.249.81.218	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
46.19.85.35	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
194.242.163.116	France	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 194.242.163.116	Block	2
213.151.35.212	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/rabanut/general.aspx	Block	2
109.253.135.20	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
80.246.139.229	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
217.132.32.120	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/templatecontrols/generic/	Block	2
190.246.194.13	Argentina	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	2
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	2
66.249.81.215	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
192.187.101.170	United States	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 192.187.101.170	Block	1
95.86.112.117	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/gyus	Block	1
45.79.71.122	United States	147.237.72.156	aman.idf.il	Malformed HTTP Header Line 3	Block	1
79.180.122.241	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	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
66.249.76.75	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
45.79.71.122	United States	147.237.72.156	aman.idf.il	Unknown HTTP Request Method 1 in URL	Block	1
107.77.225.82	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/	Block	1
45.79.71.122	United States	147.237.72.156	aman.idf.il	Malformed URL	Block	1
79.180.211.240	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/7/70187.doc	Block	1
45.79.71.122	United States	147.237.72.166	aka.idf.il	Malformed HTTP Header Line 4	Block	1
185.32.179.109	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
93.77.205.19	Ukraine	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/giyus/general/default.asp	Block	1
68.180.228.29	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/default.asp	Block	1
194.242.163.116	France	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/sip_storage	Block	1
45.79.71.122	United States	147.237.72.156	aman.idf.il	Multiple Malformed HTTP Header Line from 45.79.71.122	Block	1
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.76.83	Block	1
45.79.71.122	United States	147.237.72.166	aka.idf.il	Malformed URL	Block	1
68.180.229.230	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/templatecontrols/news/לכתבה המלאה	Block	1
204.79.180.106	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/miluim/templates/inner.asp	Block	1
46.116.172.133	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
45.79.71.122	United States	147.237.72.156	aman.idf.il	Multiple Malformed URL from 45.79.71.122	Block	1
157.55.39.221	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_moreinfo.asp	Block	1
83.235.170.248	Greece	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl41 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
45.79.71.122	United States	147.237.72.166	aka.idf.il	Unknown HTTP Request Method 1 in URL	Block	1
192.169.7.223	United States	147.237.77.170	maarachot.idf.il	Unauthorized Method HEAD for 147.237.77.170/	Block	1
95.24.34.82	Russian Federation	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
2.53.172.80	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
207.46.13.73	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
46.117.5.9	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
45.79.71.122	United States	147.237.72.156	aman.idf.il	Multiple Unknown HTTP Request Method from 45.79.71.122	Block	1
157.55.39.246	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/robots.txt	Block	1

09-04-2016-00:04:07 to 09-04-2016-01:04:07