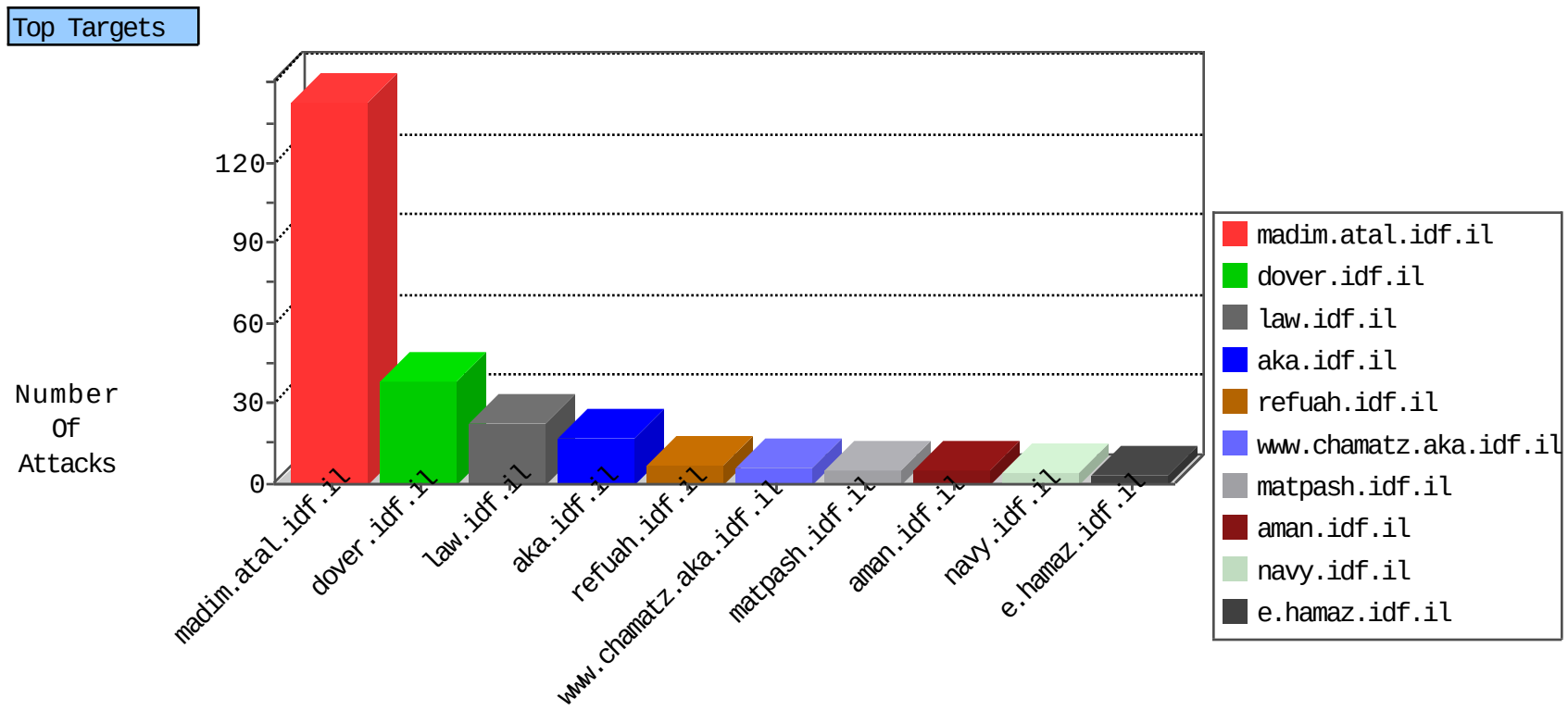
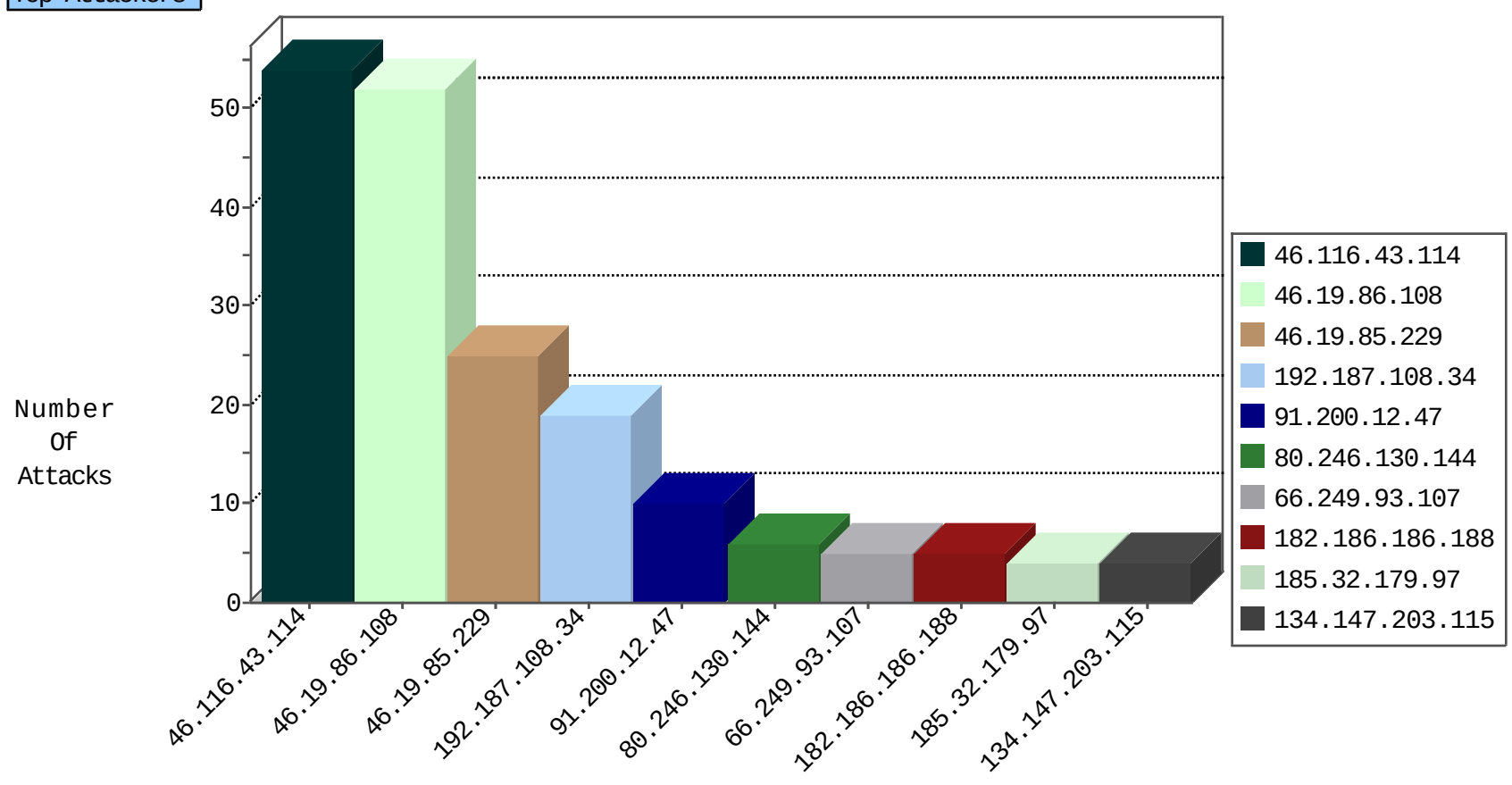
08-20-2016-18:04:08 to 08-20-2016-19:04:08

IDF Under Attack Daily Report

Top Targets



Top Attackers



08-20-2016-18:04:08 to 08-20-2016-19:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
134.147.203.115	Germany	147.237.76.42	refuah.idf.il	Black List	drop	2
134.147.203.115	Germany	147.237.76.86	navy.idf.il	Black List	drop	2
115.28.7.221	China	147.237.76.86	navy.idf.il	JLM_Purple_Con_Limit_Http	drop	1
82.80.78.2	Israel	147.237.77.176	matpash.idf.il	Black List	drop	1
115.199.169.70	China	147.237.76.177	ncore.idf.il	Black List	drop	1
104.148.55.162	United States	147.237.76.148	gqcenter.aka.idf.il	Black List	drop	1
123.151.42.61	China	147.237.76.34	yohalan.idf.il	JLM_Under_Attack_Con_Udp	drop	1
104.148.55.162	United States	147.237.76.202	e.halag.idf.il	Black List	drop	1

08-20-2016-18:04:08 to 08-20-2016-19:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
192.187.108.34	United States	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Permit	11
91.200.12.47	Ukraine	147.237.77.74	law.idf.il	C1000016: HTTP: administrator in URI	Permit	8
192.187.108.34	United States	147.237.77.226	www.chamatz.aka.idf.il	C1000074: HTTP: majestic bot	Permit	6
192.187.108.34	United States	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Permit	2

08-20-2016-18:04:08 to 08-20-2016-19:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
162.213.1.246	147.237.77.216	United States	dover.idf.il	Tehila - Perl LWP with fake user agent	3
63.221.141.195	147.237.76.31	United States	nakchal.idf.il	ET SCAN Potential SSH Scan	1
58.218.204.245	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential SSH Scan	1
173.208.249.37	147.237.77.227	United States	e.hamaz.idf.il	ET SCAN NMAP -sS window 4096	1
173.208.249.37	147.237.77.227	United States	e.hamaz.idf.il	ET SCAN NMAP -f -sS	1
122.100.64.251	147.237.8.14	Taiwan	e.orchot.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
66.249.76.120	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sA (2)	1
58.218.204.245	147.237.76.198	China	e.yohalan.idf.i	ET SCAN Potential SSH Scan	1
194.58.37.43	147.237.77.176	Russian Federation	matpash.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	1
173.208.249.37	147.237.77.227	United States	e.hamaz.idf.il	ET SCAN NMAP -sS window 2048	1
120.237.232.6	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	1

08-20-2016-18:04:08 to 08-20-2016-19:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.93.107	Europe	147.237.77.216	dover.idf.il	drop	SAM rule	drop	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
122.167.163.108	India	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
89.138.121.108	Israel	147.237.72.156	aman.idf.il	drop	Virtual defragmentation error: Timeout	drop	2
91.63.240.60	Germany	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
66.102.9.20	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
109.253.128.23	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
109.253.219.89	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
74.82.47.42	United States	147.237.0.200	m4u.idf.il	drop		drop	1

08-20-2016-18:04:08 to 08-20-2016-19:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.116.43.114	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	54
46.19.86.108	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	52
46.19.85.229	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	25
185.32.179.97	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
109.64.8.91	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
80.246.130.144	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
77.139.23.198	France	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
65.55.210.99	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
5.102.254.181	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
2.53.48.141	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
199.30.24.23	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
66.249.65.177	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.177	Block	2
199.30.24.144	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
5.102.253.158	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 5.102.253.158	Block	2
157.55.12.65	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
77.126.31.130	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
79.180.44.64	Israel	147.237.72.156	aman.idf.il	Too Many Cookies in a Request - 101 cookies	Block	1
66.220.156.106	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
46.19.85.36	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 46.19.85.36	Block	1
182.186.186.188	Pakistan	147.237.76.42	refuah.idf.il	Illegal Byte Code Character in Method ¬[[#0]][[#0]][[#0]]p;[[#23]]Ü‘0W'[[#31]]D¹°úêmCvðžFš¸AµŸÿê²…/äšr_i¡[[#2]]bR˜Iåü[[#30]]›Khv×¥Ó[[#6]]•°÷}[[#11]]ð×ÄÐ±	Block	1
90.182.178.182	Czech Republic	147.237.72.166	aka.idf.il	Unknown Parameter catID in www.aka.idf.il/yohalan/home/home.asp	None	1
77.127.52.173	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/watch	Block	1
66.102.9.20	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
109.253.240.111	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
41.79.187.106	Tanzania, United Republic of	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
182.186.186.188	Pakistan	147.237.76.42	refuah.idf.il	Illegal Byte Code Character in URL	Block	1
91.200.12.47	Ukraine	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
5.29.164.179	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/giyus/faq.aspx	None	1
66.102.9.31	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
109.253.240.133	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
42.200.34.83	Hong Kong	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
84.95.208.20	Israel	147.237.77.74	law.idf.il	PHP Attempt	Block	1
66.249.65.177	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_pictures.asp	Block	1
182.186.186.188	Pakistan	147.237.76.42	refuah.idf.il	NULL Character in Method ¬[[#0]][[#0]][[#0]]p;[[#23]]Ü‘0W'[[#31]]D¹°úêmCvðžFš¸AµŸÿê²…/äšr_i¡[[#2]]bR˜Iåü[[#30]]›Khv×¥Ó[[#6]]•°÷}[[#11]]ð×ÄÐ±	Block	1
91.200.12.47	Ukraine	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/wp-login.php	Block	1
77.139.247.213	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim	Block	1
204.79.180.76	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/main/	Block	1
66.102.9.76	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
42.200.34.83	Hong Kong	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
84.95.208.20	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/homepage/piwik.php	Block	1
66.249.76.42	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	1
182.186.186.188	Pakistan	147.237.76.42	refuah.idf.il	Unknown HTTP Request Method ¬[[#0]][[#0]][[#0]]p;[[#23]]Ü‘0W'[[#31]]D¹°úêmCvðžFš¸AµŸÿê²…/äšr_i¡[[#2]]bR˜Iåü[[#30]]›Khv×¥Ó[[#6]]•°÷}[[#11]]ð×ÄÐ±	Block	1
92.247.35.58	Bulgaria	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
5.102.253.158	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/1/	Block	1
79.176.29.94	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
66.102.9.85	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
46.19.85.36	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012 ources/images/innerpage/goback.gif	Block	1
182.186.186.188	Pakistan	147.237.76.42	refuah.idf.il	Abnormally Long Request method	Block	1
84.229.9.75	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1

08-20-2016-18:04:08 to 08-20-2016-19:04:08