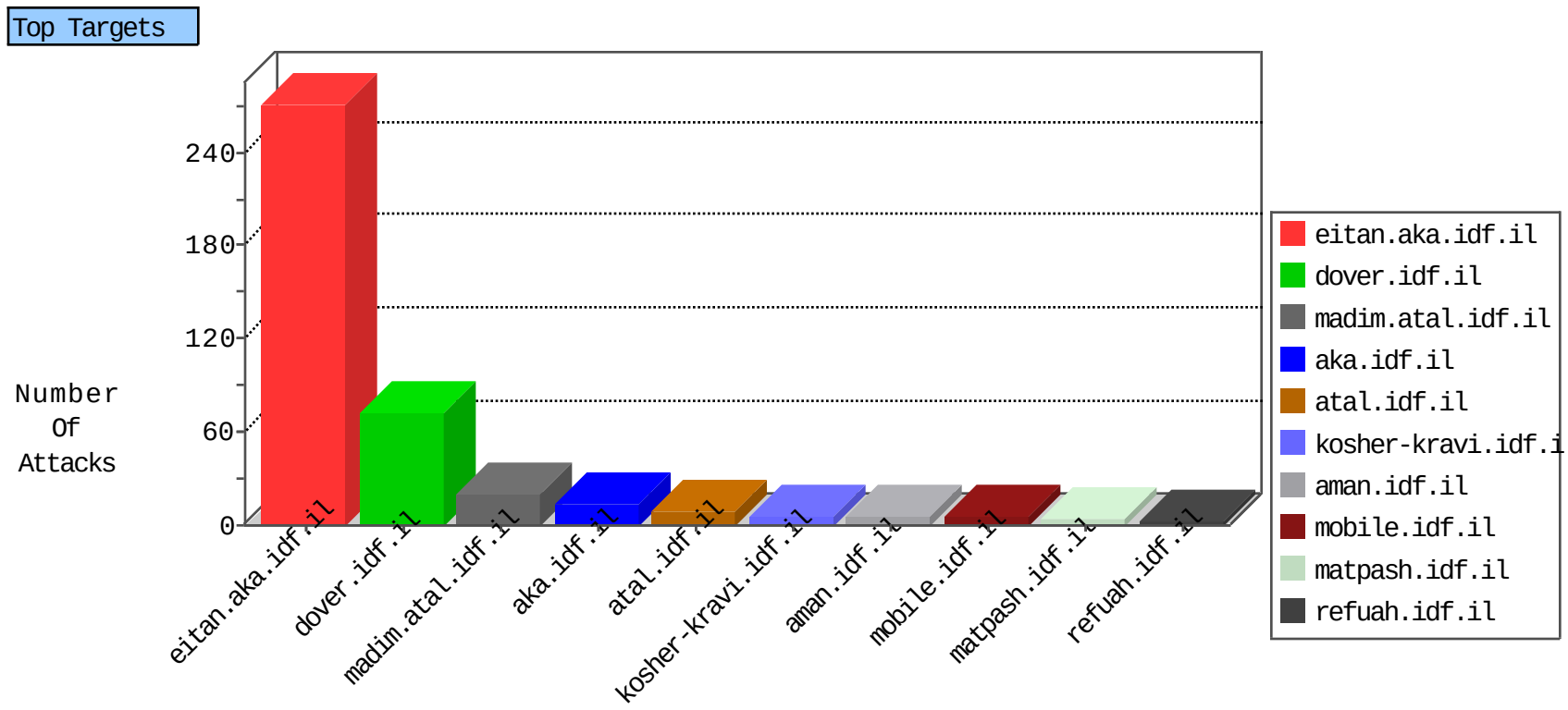
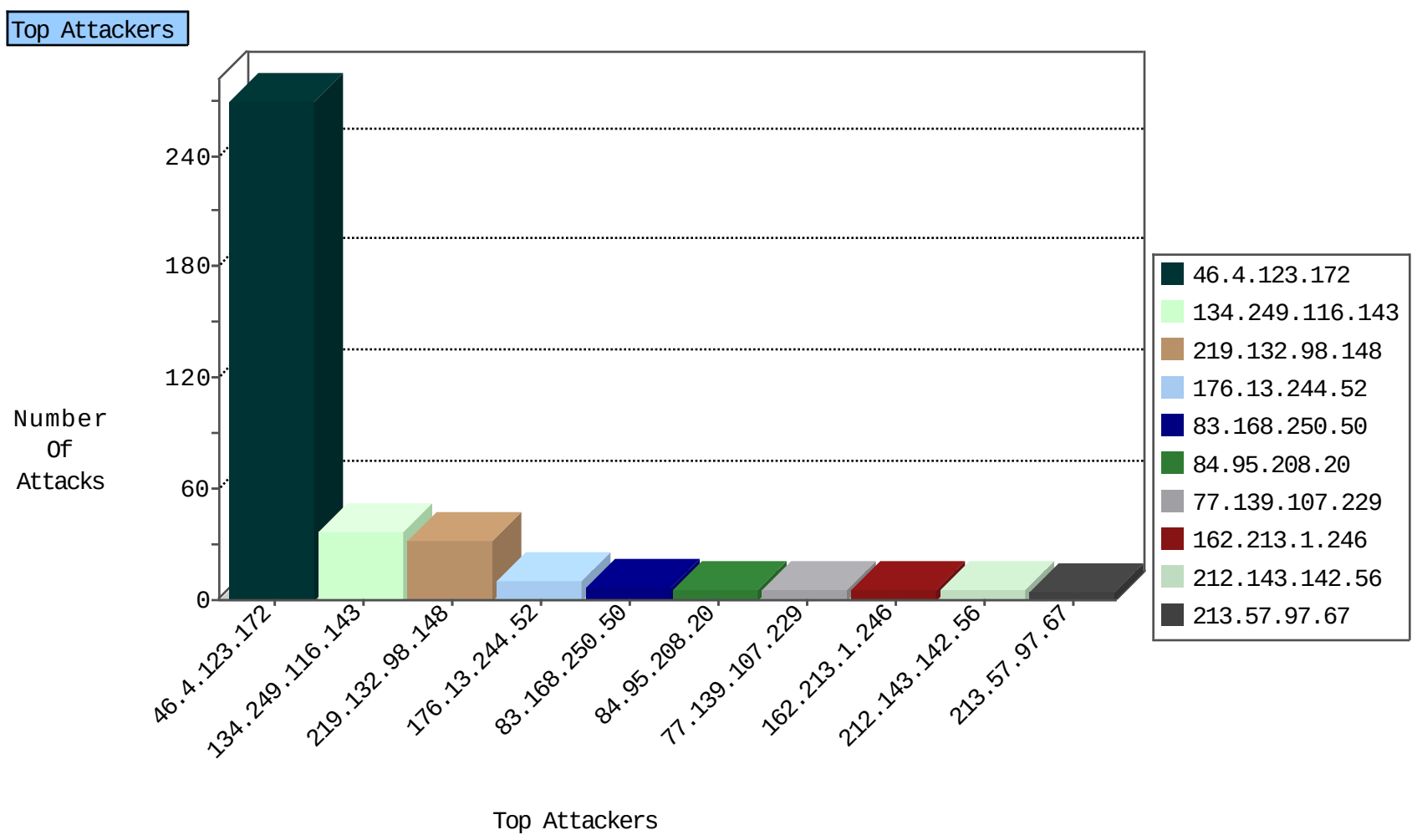
08-23-2016-01:07:55 to 08-23-2016-02:07:55

IDF Under Attack Daily Report

Top Targets



Top Attackers



08-23-2016-01:07:55 to 08-23-2016-02:07:55

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
111.40.226.248	China	147.237.76.199	e.nakchal.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
185.94.111.1	Russian Federation	147.237.76.200	eitan.aka.idf.il	Black List	drop	1
185.94.111.1	Russian Federation	147.237.76.42	refuah.idf.il	Black List	drop	1
185.94.111.1	Russian Federation	147.237.76.148	gqcenter.aka.idf.il	Black List	drop	1

08-23-2016-01:07:55 to 08-23-2016-02:07:55

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.4.123.172	Germany	147.237.76.200	eitan.aka.idf.il	C1000074: HTTP: majestic bot	Permit	266
134.249.116.143	Ukraine	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	37
83.168.250.50	Sweden	147.237.77.233	atal.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	5
162.210.196.129	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
83.168.250.50	Sweden	147.237.77.233	atal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	1
83.168.250.50	Sweden	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1

08-23-2016-01:07:55 to 08-23-2016-02:07:55

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	5
219.132.98.148	147.237.8.24	China	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	2
219.132.98.148	147.237.77.74	China	law.idf.il	ET SCAN Potential SSH Scan	2
219.132.98.148	147.237.77.178	China	e.matpash.idf.il	ET SCAN Potential SSH Scan	2
219.132.98.148	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential SSH Scan	2
219.132.98.148	147.237.77.227	China	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
70.63.217.190	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN NMAP -sS window 3072	1
219.132.98.148	147.237.72.166	China	aka.idf.il	ET SCAN Potential SSH Scan	1
219.132.98.148	147.237.77.179	China	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
70.63.217.190	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN NMAP -f -sS	1
219.132.98.148	147.237.8.45	China	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
219.132.98.148	147.237.77.170	China	maarachot.idf.il	ET SCAN Potential SSH Scan	1
46.172.71.251	147.237.8.28	Ukraine	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
219.132.98.148	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
219.132.98.148	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	1
219.132.98.148	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
219.132.98.148	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
176.47.70.66	147.237.77.216	Saudi Arabia	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
219.132.98.148	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1
128.199.70.132	147.237.72.166	Singapore	aka.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
219.132.98.148	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
87.236.194.161	147.237.77.212	Czech Republic	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
219.132.98.148	147.237.77.233	China	atal.idf.il	ET SCAN Potential SSH Scan	1
219.132.98.148	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
219.132.98.148	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	1
70.63.217.190	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN NMAP -sS window 2048	1
219.132.98.148	147.237.8.46	China	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
66.249.66.12	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	1
219.132.98.148	147.237.8.27	China	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
219.132.98.148	147.237.77.121	China	e.navy.idf.il	ET SCAN Potential SSH Scan	1
219.132.98.148	147.237.8.14	China	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
219.132.98.148	147.237.77.19	China	law-forum.idf.il	ET SCAN Potential SSH Scan	1
219.132.98.148	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
195.88.208.193	147.237.0.19	Russian Federation	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
219.132.98.148	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
219.132.98.148	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
91.125.184.101	147.237.77.216	United Kingdom	dover.idf.il	Tehila - Perl LWP with fake user agent	1
219.132.98.148	147.237.77.235	China	sviva.idf.il	ET SCAN Potential SSH Scan	1
219.132.98.148	147.237.72.217	China	e.idf.il	ET SCAN Potential SSH Scan	1

08-23-2016-01:07:55 to 08-23-2016-02:07:55

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.4.123.172	Germany	147.237.76.200	eitan.aka.idf.il	drop	SAM rule	drop	4
176.13.5.73	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	2
77.160.193.76	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
84.78.17.96	Spain	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	2
66.102.9.20	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
106.38.241.105	China	147.237.72.166	aka.idf.il	drop	SAM rule	drop	1
66.102.9.31	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.0.35	akaws.idf.il	drop		drop	1
66.102.9.42	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
46.117.216.39	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
176.13.244.52	Israel	147.237.0.19	madim.atal.idf.il	drop	First packet isn't SYN	drop	1
62.90.215.246	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1

08-23-2016-01:07:55 to 08-23-2016-02:07:55

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.244.52	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
77.139.107.229	France	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 77.139.107.229	Block	4
2.53.135.160	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
213.57.97.67	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
66.102.9.20	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
66.102.9.31	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
2.55.131.196	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
89.139.221.152	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	2
66.102.9.42	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
37.218.223.84	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/homepage/www.youtube.com/v/3g51ei5nuhg	Block	2
84.95.208.20	Israel	147.237.0.15	kosher-kravi.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
77.138.91.130	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/sachar	Block	1
46.19.85.169	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
84.95.208.20	Israel	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to www.kosher-kravi.idf.il/default.aspx	Block	1
2.55.150.0	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
138.219.167.151	Brazil	147.237.77.216	dover.idf.il	Parameter Type Violation lang in www.idf.il/1393-en/dover.aspx	Block	1
66.7.245.226	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
199.30.24.57	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
2.53.149.99	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
84.95.208.20	Israel	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
66.249.76.31	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/.well-known/apple-app-site-association	Block	1
2.55.167.186	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
157.55.39.139	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
77.139.107.229	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim	Block	1
66.102.6.25	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
2.53.165.207	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
84.95.208.20	Israel	147.237.72.156	aman.idf.il	PHP Attempt	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
169.229.3.91	United States	147.237.76.31	nakchal.idf.il	Multiple Untraceable SSL Sessions from 169.229.3.91 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
79.179.188.9	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
213.57.97.67	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
2.53.179.150	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
85.64.198.156	Israel	147.237.72.156	aman.idf.il	Distributed 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/	Block	1
46.19.85.59	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
169.229.3.91	United States	147.237.76.39	mobile.meitav.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1

08-23-2016-01:07:55 to 08-23-2016-02:07:55