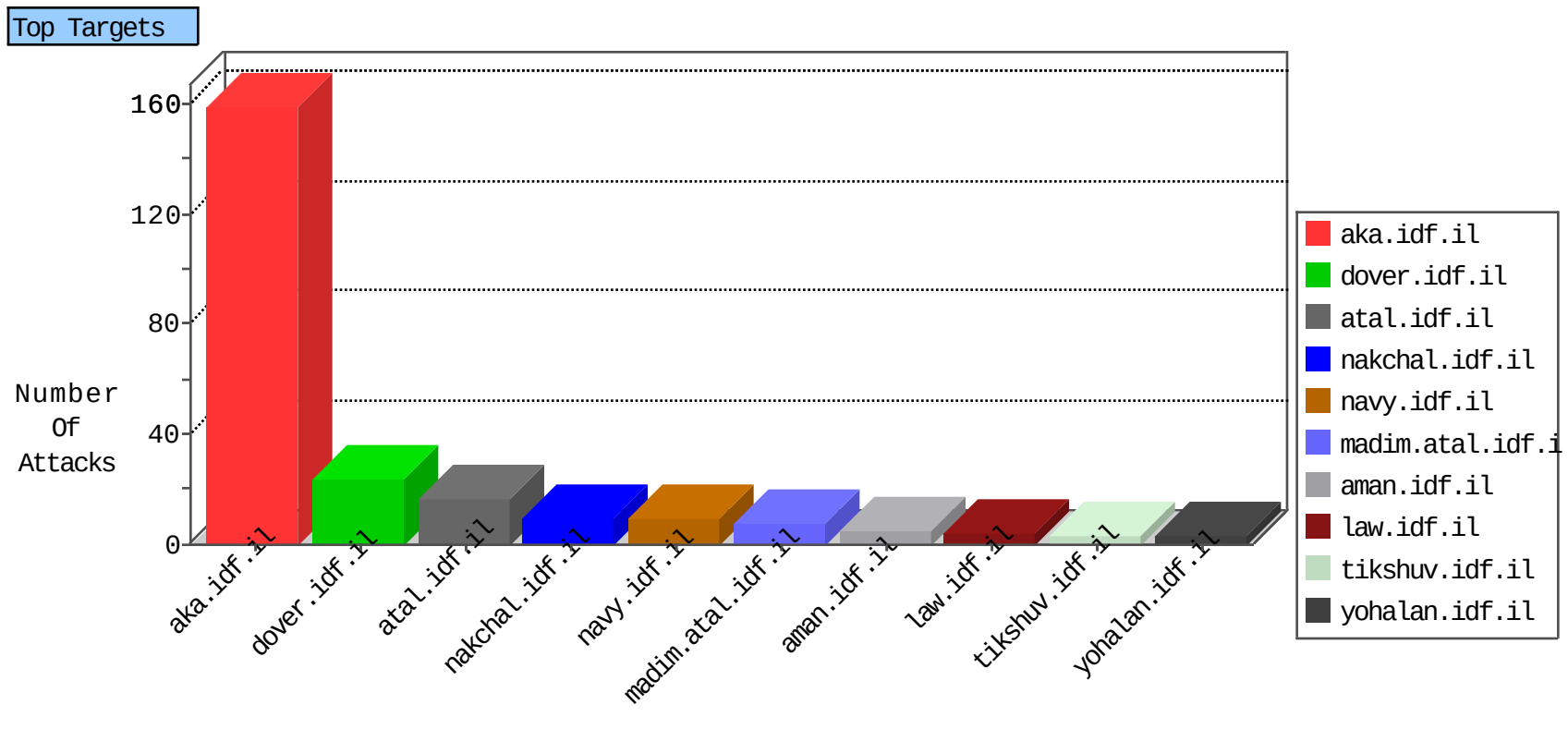
08-30-2016-01:07:28 to 08-30-2016-02:07:28

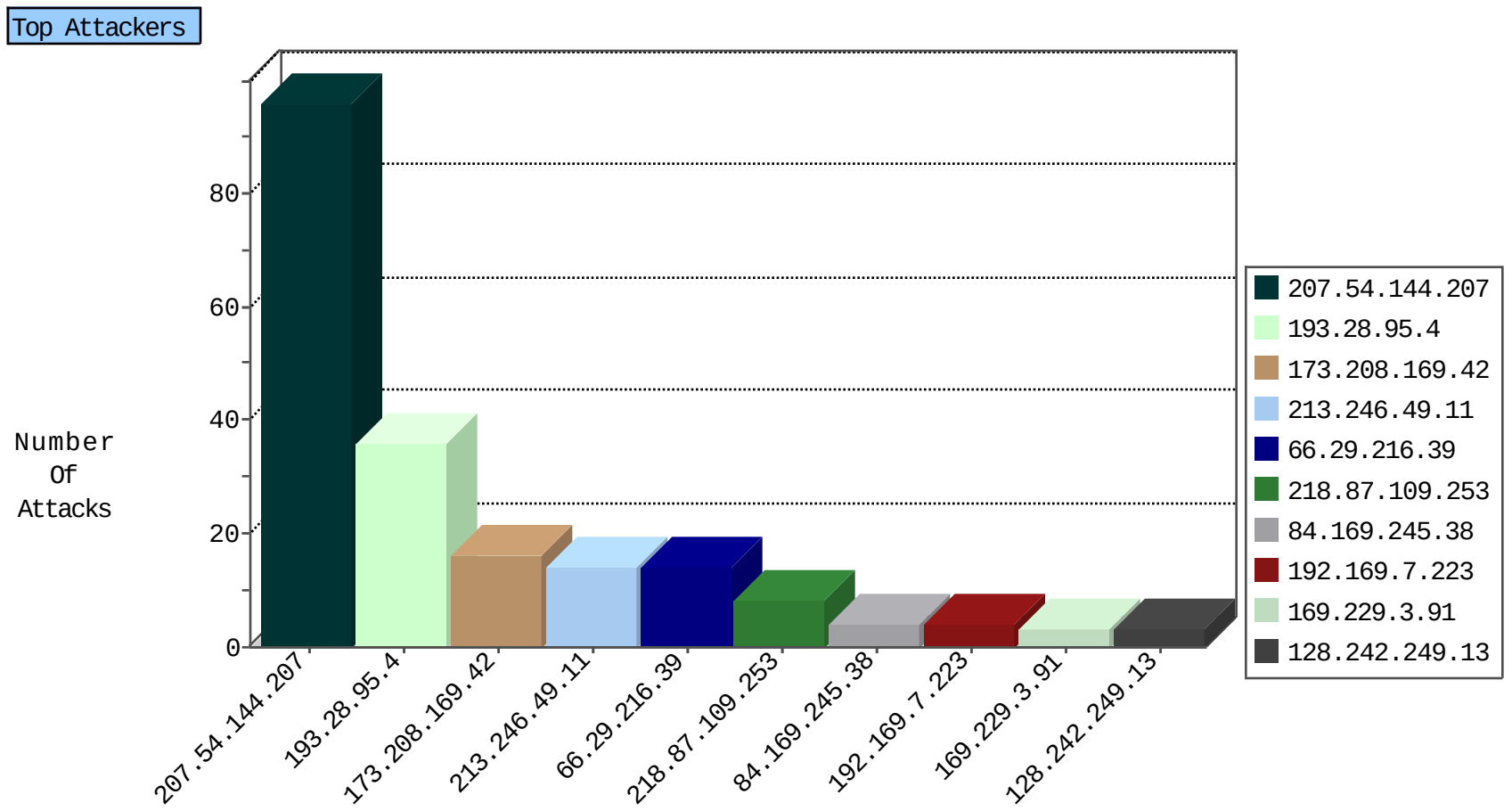
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

08-30-2016-01:07:28 to 08-30-2016-02:07:28

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
94.102.49.193	Netherlands	147.237.76.34	yohalan.idf.il	Black List	drop	1
178.239.62.141	Netherlands	147.237.76.31	nakchal.idf.il	Black List	drop	1
93.158.200.97	Netherlands	147.237.76.30	himush.idf.il	Black List	drop	1
178.239.62.201	Netherlands	147.237.76.200	eitan.aka.idf.il	Black List	drop	1
93.158.200.97	Netherlands	147.237.76.201	e.atal.idf.il	Black List	drop	1
192.162.101.50	Russian Federation	147.237.76.38	e.e.meitav.idf.il	Black List	drop	1

08-30-2016-01:07:28 to 08-30-2016-02:07:28

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
207.54.144.207	United States	147.237.72.166	aka.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	18
173.208.169.42	United States	147.237.76.31	nakchal.idf.il	C1000125: HTTP: Block admin login to gov.il sites ?q=user	Permit	8
173.208.169.42	United States	147.237.76.86	navy.idf.il	C1000125: HTTP: Block admin login to gov.il sites ?q=user	Permit	8
213.246.49.11	France	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
207.54.144.207	United States	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
66.29.216.39	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
61.135.189.120	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1
89.248.172.16	Netherlands	147.237.77.121	e.navy.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

08-30-2016-01:07:28 to 08-30-2016-02:07:28

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
207.54.144.207	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	72
66.29.216.39	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	8
213.246.49.11	147.237.72.166	France	aka.idf.il	SQL Injection - Select From	8
183.222.97.82	147.237.72.156	China	aman.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
175.253.55.199	147.237.76.30	Korea, Republic of	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
104.232.98.38	147.237.0.19	United States	madim.atal.idf.il	ET SCAN NMAP -sS window 2048	1
94.102.48.195	147.237.77.233	Netherlands	atal.idf.il	ET SCAN NMAP -sS window 1024	1
218.87.109.253	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential SSH Scan	1
218.87.109.253	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
218.87.109.253	147.237.72.14	China	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
218.87.109.253	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
179.33.85.57	147.237.0.33	Colombia	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
104.232.98.38	147.237.0.19	United States	madim.atal.idf.il	ET SCAN NMAP -sS window 4096	1
104.232.98.38	147.237.0.19	United States	madim.atal.idf.il	ET SCAN NMAP -f -sS	1
218.87.109.253	147.237.77.19	China	law-forum.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.195	147.237.77.216	Netherlands	dover.idf.il	ET SCAN NMAP -sS window 1024	1
218.87.109.253	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
218.87.109.253	147.237.72.217	China	e.idf.il	ET SCAN Potential SSH Scan	1
218.87.109.253	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1

08-30-2016-01:07:28 to 08-30-2016-02:07:28

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
193.28.95.4	Italy	147.237.72.166	aka.idf.il	drop	SAM rule	drop	36
84.169.245.38	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
92.24.47.104	United Kingdom	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	3
192.169.7.223	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	3
128.242.249.13	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
173.185.47.10	United States	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
46.19.86.113	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	2
109.253.210.251	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	2
141.212.122.123	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
141.212.122.124	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
176.13.241.97	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	1
109.253.158.191	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.0.200	m4u.idf.il	drop	First packet isn't SYN	drop	1
188.120.154.114	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.76.30	himush.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	1
85.250.126.150	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1

08-30-2016-01:07:28 to 08-30-2016-02:07:28

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.23.229	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
77.138.249.43	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/favicon.ico	Block	2
46.19.85.12	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
83.146.225.237	Finland	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	2
81.218.229.198	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/templates/news/news.aspx	Block	1
66.249.76.70	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.76.70	Block	1
207.46.13.109	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
109.253.138.136	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
77.138.162.143	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/main/sachar/popups/markivsachar.aspx	Block	1
192.116.177.194	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/popups/markivsachar.aspx	None	1
81.218.229.198	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 81.218.229.198	Block	1
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/print_text.asp	Block	1
207.46.13.109	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.109	Block	1
148.251.2.180	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1
192.169.7.223	United States	147.237.76.42	refuah.idf.il	Unauthorized Method HEAD for 147.237.76.42/	Block	1
68.180.230.47	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/kesher	Block	1
207.46.13.149	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
157.55.39.97	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
80.246.139.58	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
61.135.189.120	China	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
199.30.24.98	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
105.225.92.220	South Africa	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
77.138.105.125	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/rights/asp/info.asp	Block	1
207.46.13.149	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/print_bottom.asp	Block	1
81.218.229.198	Israel	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to www.kosher-kravi.idf.il/templates/homepage/homepage.aspx	Block	1
66.249.64.41	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
207.46.13.64	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
105.225.92.220	South Africa	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
77.138.115.17	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	1
178.63.101.134	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/home/default.aspx	Block	1

08-30-2016-01:07:28 to 08-30-2016-02:07:28