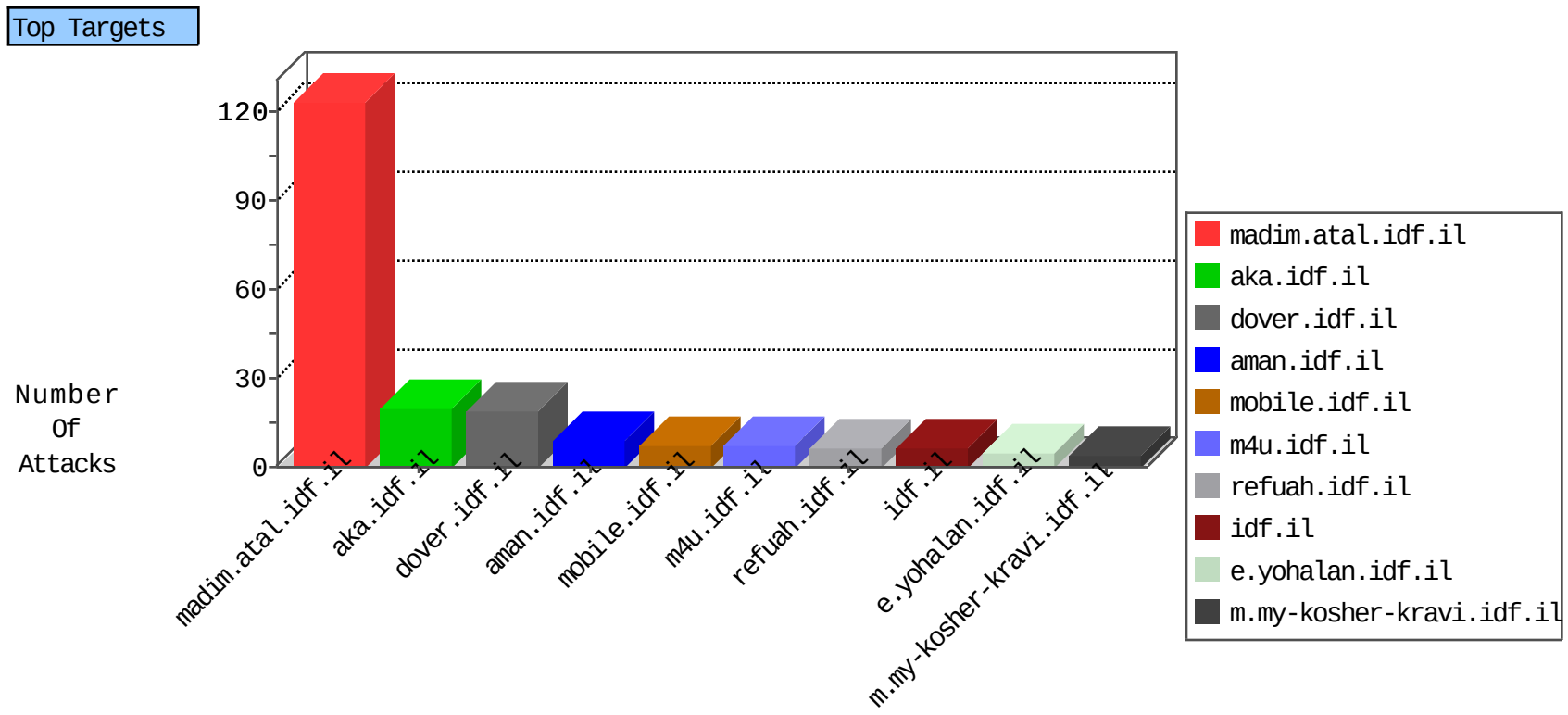
08-31-2016-00:04:00 to 08-31-2016-01:04:00

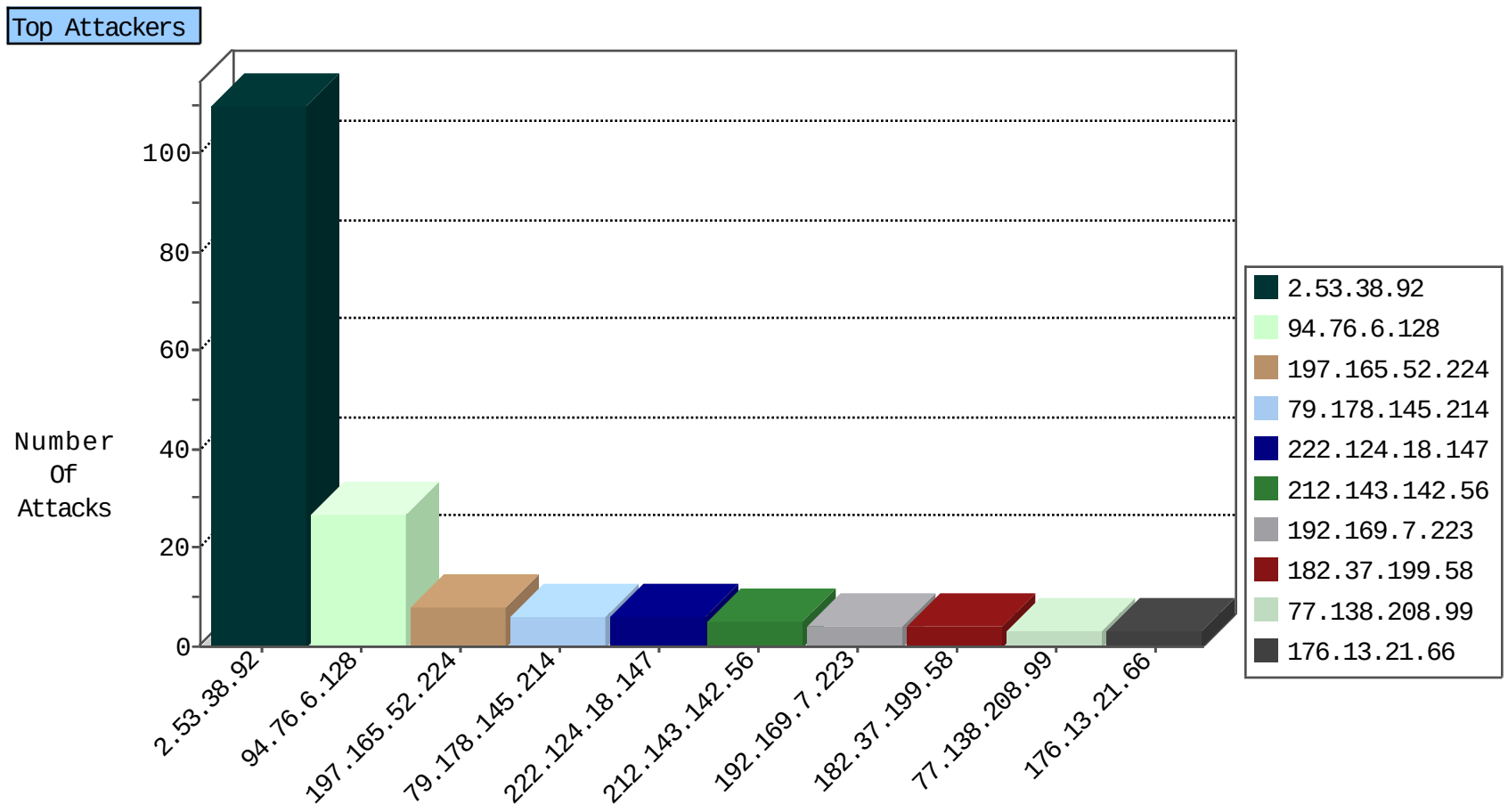
IDF Under Attack
Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

08-31-2016-00:04:00 to 08-31-2016-01:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
182.37.199.58	China	147.237.76.198	e.yohalan.idf.il	Black List	drop	4
5.189.181.23	Germany	147.237.76.177	ncore.idf.il	Black List	drop	1

08-31-2016-00:04:00 to 08-31-2016-01:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
94.102.49.193	Netherlands	147.237.76.44	e.refuah.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

08-31-2016-00:04:00 to 08-31-2016-01:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.120.122.219	147.237.76.200	Israel	eitan.aka.idf.il	Xenu Link Sleuth User Agent	2
87.115.230.45	147.237.77.216	United Kingdom	dover.idf.il	Tehila - Perl LWP with fake user agent	2
87.236.194.161	147.237.77.61	Czech Republic	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
222.124.18.147	147.237.0.19	Indonesia	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
46.227.67.172	147.237.0.19	Sweden	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
222.67.133.98	147.237.0.35	China	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
46.172.71.251	147.237.0.34	Ukraine	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
218.205.151.197	147.237.76.42	China	refuah.idf.il	ET SCAN NMAP -f -sS	1
183.60.175.108	147.237.8.45	China	e.eitan.idf.il	ET SCAN NMAP -f -sS	1
109.226.40.40	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
106.120.209.152	147.237.76.42	China	refuah.idf.il	ET SCAN NMAP -sS window 2048	1
94.76.6.128	147.237.0.200	Bahrain	m4u.idf.il	ET SCAN Potential SSH Scan	1
222.124.18.147	147.237.76.198	Indonesia	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
94.76.6.128	147.237.0.200	Bahrain	m4u.idf.il	ET SCAN NMAP -f -sS	1
222.124.18.147	147.237.0.200	Indonesia	m4u.idf.il	ET SCAN Potential SSH Scan	1
222.124.18.147	147.237.0.17	Indonesia	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
46.172.71.251	147.237.0.35	Ukraine	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
218.205.151.197	147.237.76.42	China	refuah.idf.il	ET SCAN NMAP -sS window 2048	1
46.172.71.251	147.237.0.19	Ukraine	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
212.224.109.175	147.237.77.233	Germany	atal.idf.il	ET SCAN Potential SSH Scan	1
121.138.48.203	147.237.0.19	Korea, Republic of	madim.atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
106.186.20.183	147.237.76.86	Japan	navy.idf.il	ET SCAN Potential SSH Scan	1
106.120.209.152	147.237.76.42	China	refuah.idf.il	ET SCAN NMAP -f -sS	1
222.124.18.147	147.237.77.226	Indonesia	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
94.76.6.128	147.237.0.200	Bahrain	m4u.idf.il	ET SCAN NMAP -sS window 2048	1
222.124.18.147	147.237.72.166	Indonesia	aka.idf.il	ET SCAN Potential SSH Scan	1

08-31-2016-00:04:00 to 08-31-2016-01:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
197.165.52.224	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
94.76.6.128	Bahrain	147.237.0.19	madim.atal.idf.il	drop	SAM rule	drop	4
94.76.6.128	Bahrain	147.237.0.33	idf.il	drop	SAM rule	drop	4
94.76.6.128	Bahrain	147.237.0.17	m.my-kosher-kravi.idf.il	drop	SAM rule	drop	3
192.169.7.223	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	3
94.76.6.128	Bahrain	147.237.0.15	kosher-kravi.idf.il	drop	SAM rule	drop	3
176.13.21.66	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	3
109.66.61.61	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	2
176.13.248.190	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	2
94.76.6.128	Bahrain	147.237.0.200	m4u.idf.il	drop	SAM rule	drop	2
94.76.6.128	Bahrain	147.237.0.16	my-kosher-kravi.idf.il	drop	SAM rule	drop	2
94.76.6.128	Bahrain	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	2
94.76.6.128	Bahrain	147.237.0.35	akaws.idf.il	drop		drop	1
176.13.1.10	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
180.97.106.162	China	147.237.0.33	idf.il	drop		drop	1
94.76.6.128	Bahrain	147.237.0.35	akaws.idf.il	drop	SAM rule	drop	1
79.177.25.32	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	1
176.13.10.160	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	1
94.76.6.128	Bahrain	147.237.0.33	idf.il	drop		drop	1
94.76.6.128	Bahrain	147.237.0.200	m4u.idf.il	drop		drop	1
176.13.11.28	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	1

08-31-2016-00:04:00 to 08-31-2016-01:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.38.92	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	110
79.178.145.214	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	5
77.138.208.99	France	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.247	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	3
5.29.225.75	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.229.90.13	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/sip_storage/files/2/2792.jpg	Block	2
213.151.35.213	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/rabanut/	Block	2
87.71.63.154	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
194.219.99.138	Greece	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/about.aspx	Block	1
79.178.145.214	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/4/	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
109.66.177.128	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
66.249.66.174	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
2.53.156.23	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
213.151.35.212	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	1
84.229.90.13	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.229.90.13	Block	1
46.120.122.219	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized Method HEAD for www.eitan.aka.idf.il/	None	1
2.53.7.17	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-he/dover.aspx	Block	1
148.251.13.51	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1
213.151.35.213	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 213.151.35.213	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
157.55.39.150	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/robots.txt	Block	1
79.176.140.56	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
37.46.39.157	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
85.65.126.156	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/markiveysachar.aspx	None	1
66.249.64.22	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	1
2.53.141.85	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/newsarchive.aspx	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
66.249.64.55	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_text.asp	Block	1
2.53.141.138	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1

08-31-2016-00:04:00 to 08-31-2016-01:04:00