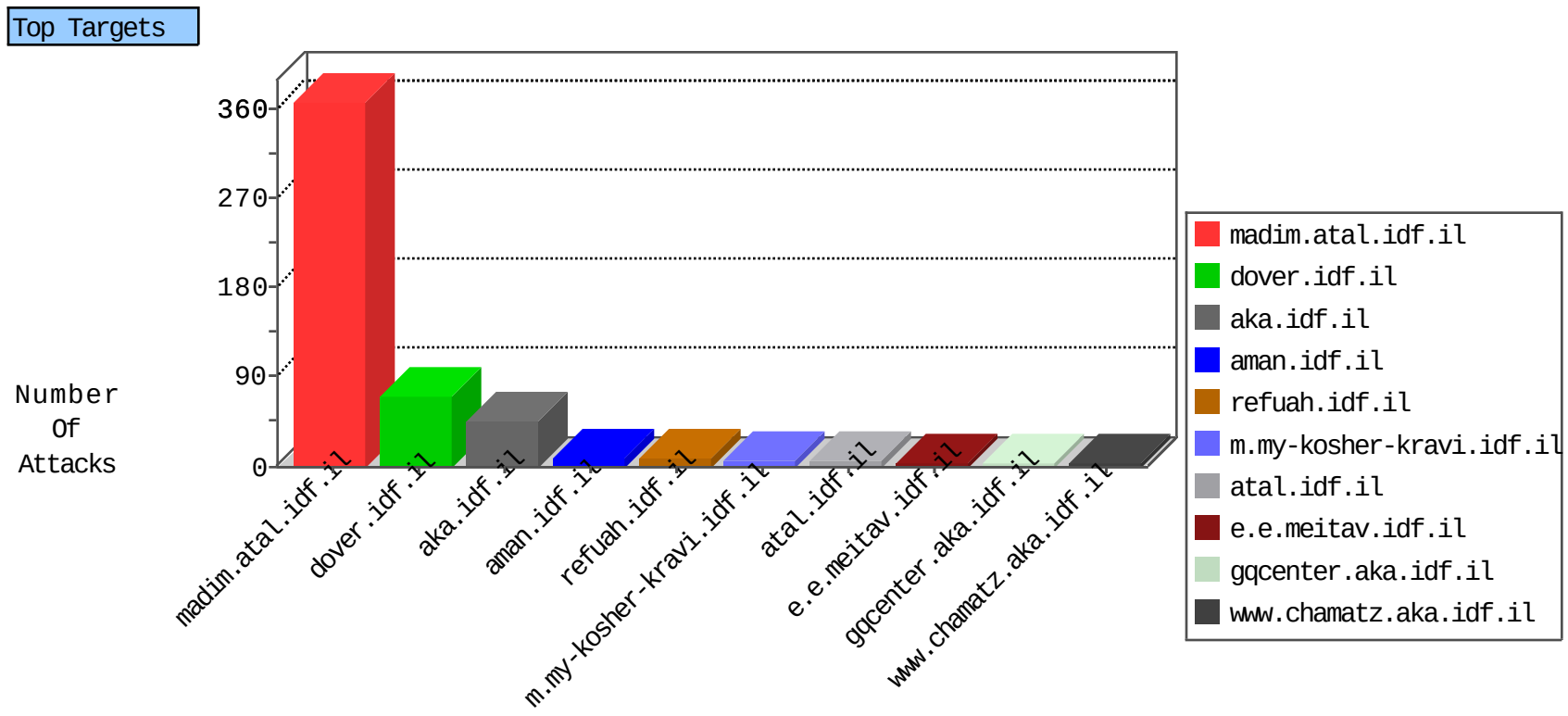
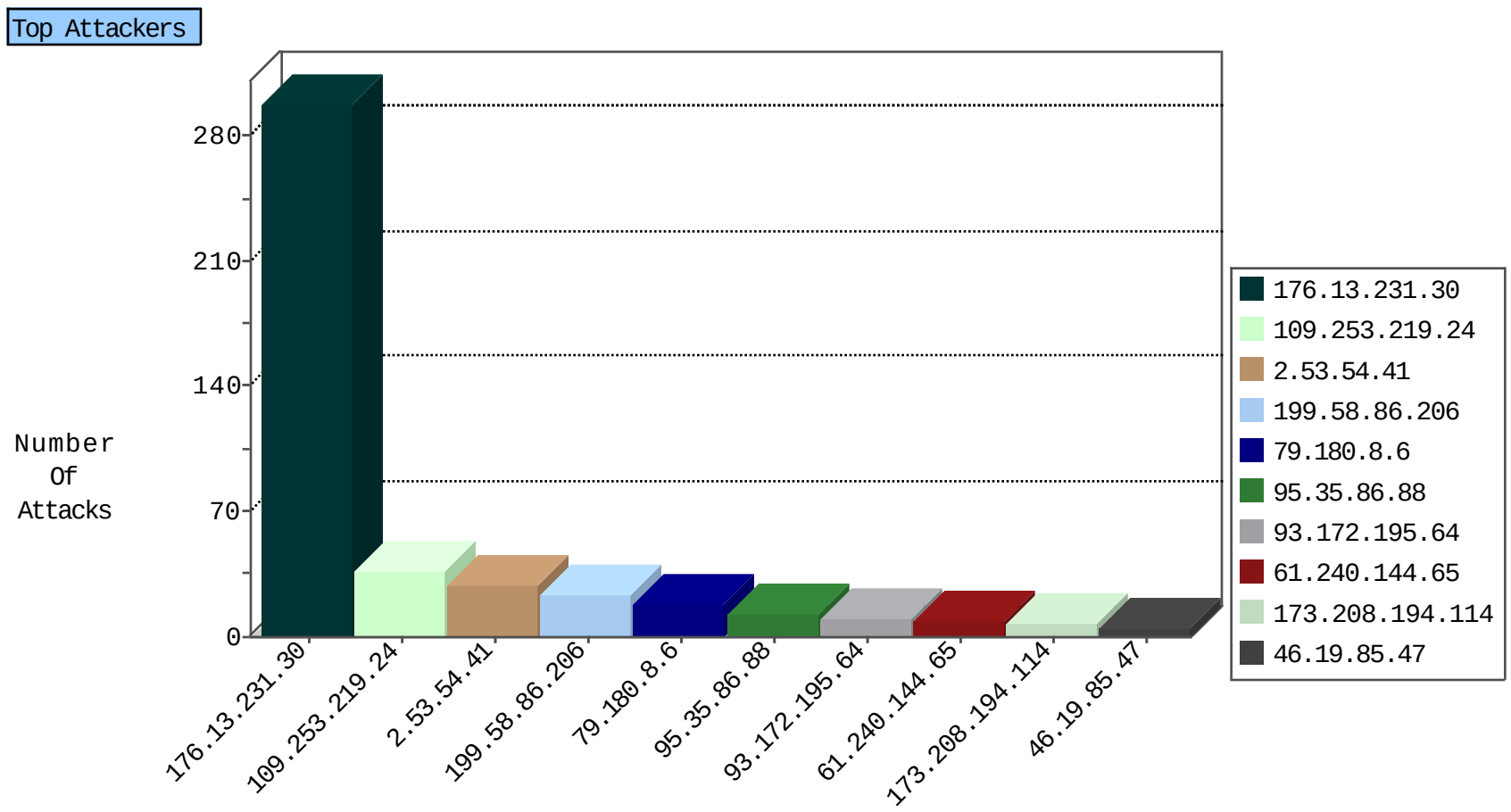
08-30-2016-22:04:00 to 08-30-2016-23:04:00

IDF Under Attack Daily Report

Top Targets



Top Attackers



08-30-2016-22:04:00 to 08-30-2016-23:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.180.8.6	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	18
95.35.86.88	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	12
185.3.146.246	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	10
134.191.232.70	Israel	147.237.76.42	refuah.idf.il	JLM_Under_Attack_Con_Http	drop	5
2.55.12.138	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
141.226.218.59	Israel	147.237.77.216	dover.idf.il	Black List	drop	1

08-30-2016-22:04:00 to 08-30-2016-23:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
199.58.86.206	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	18
173.208.194.114	United States	147.237.0.17	m.my-kosher-kravi.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	5
199.58.86.206	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	3
199.58.86.206	United States	147.237.76.30	himush.idf.il	C1000074: HTTP: majestic bot	Permit	2
173.208.194.114	United States	147.237.0.17	m.my-kosher-kravi.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	1

08-30-2016-22:04:00 to 08-30-2016-23:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
183.136.196.146	147.237.76.38	China	e.e.meitav.idf.il	GPL SCAN nmap TCP	2
220.181.167.182	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential SSH Scan	1
104.232.98.38	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -f -sS	1
220.181.167.182	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	147.237.77.19	China	law-forum.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
183.136.196.150	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN NMAP -f -sS	1
61.240.144.65	147.237.8.27	China	e.madim.atal.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
183.129.160.229	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
173.208.194.114	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET WEB_SERVER Muieblackcat scanner	1
5.255.90.133	147.237.76.176	Netherlands	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
115.47.12.162	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
115.47.12.162	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
109.60.153.178	147.237.0.200	Russian Federation	m4u.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
104.232.98.38	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sS window 2048	1
220.181.167.182	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
66.249.93.71	147.237.76.42	Europe	refuah.idf.il	ET SCAN NMAP -sA (2)	1
183.136.196.150	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN NMAP -sS window 2048	1
61.240.144.65	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
61.240.144.65	147.237.0.35	China	akaws.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
178.153.186.240	147.237.76.44	Qatar	e.refuah.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
61.240.144.65	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
115.47.12.162	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
5.255.90.133	147.237.76.86	Netherlands	navy.idf.il	ET SCAN NMAP -sS window 1024	1
115.47.12.162	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1
115.47.12.162	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
104.232.98.38	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sS window 3072	1

08-30-2016-22:04:00 to 08-30-2016-23:04:00

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
85.130.249.178	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
192.169.7.223	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	3
46.19.85.47	Israel	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	3
66.102.9.191	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	3
109.253.196.107	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
46.117.112.217	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
176.13.241.110	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	2
109.64.29.143	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	1
176.13.13.253	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	1
109.253.158.149	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	1
46.19.86.67	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	1
176.13.227.204	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
82.102.173.76	Israel	147.237.76.34	yohalan.idf.il	drop		drop	1
176.13.236.124	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
109.253.202.90	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
61.240.144.65	China	147.237.72.167	ishurim.aka.idf.il	drop	SAM rule	drop	1
100.92.117.144		147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	1
109.253.213.117	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
61.240.144.65	China	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.231.30	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	298
109.253.219.24	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	37
2.53.54.41	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
93.172.195.64	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 93.172.195.64	Block	8
77.138.16.221	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim	Block	3
79.180.94.67	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
77.139.170.208	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar	Block	2
77.125.15.80	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	2
93.172.195.64	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/	Block	2
77.139.192.198	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/	Block	2
66.249.64.22	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/print_text.asp	Block	1
46.19.85.149	Israel	147.237.72.156	aman.idf.il	Illegal Parameter Encoding ctl00$ctl00$cphMain$CPHMainContent$ctl72$ctl03$ctl03$txtField in www.aman.idf.il/modiin/questionnaires.aspx	None	1
176.13.234.38	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
84.229.34.138	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
213.8.204.31	Israel	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
46.116.2.66	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
5.102.195.123	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
109.64.91.109	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/4/	Block	1
79.179.131.54	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/faq.aspx	Block	1
66.249.66.174	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
185.3.146.246	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
46.19.85.149	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
85.64.8.185	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/declarationexplanation.aspx	None	1
77.138.242.185	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/favicon.ico	Block	1
46.116.193.129	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/	Block	1
37.26.146.232	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
69.171.230.113	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/9/1919.jpg	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
46.19.85.205	Israel	147.237.77.233	atal.idf.il	Illegal HTTP Version	Block	1
54.235.164.217	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/894-he/shared/usercontrols/headerupper/	Block	1
46.19.85.47	Israel	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 46.19.85.47 (Open Mode)	None	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
84.94.160.64	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
204.15.110.21	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/main/	Block	1
46.19.85.205	Israel	147.237.77.233	atal.idf.il	Malformed URL http/1.1	Block	1
66.102.9.2	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
46.19.85.47	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
84.109.231.212	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
77.138.12.211	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar	Block	1
212.249.10.98	Switzerland	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/favicon.ico	Block	1
46.19.85.205	Israel	147.237.77.233	atal.idf.il	Unknown HTTP Request Method /960.css in URL www.atal.idf.ilhttp/1.1	Block	1
109.64.91.109	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 109.64.91.109	Block	1
79.176.135.106	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1

08-30-2016-22:04:00 to 08-30-2016-23:04:00