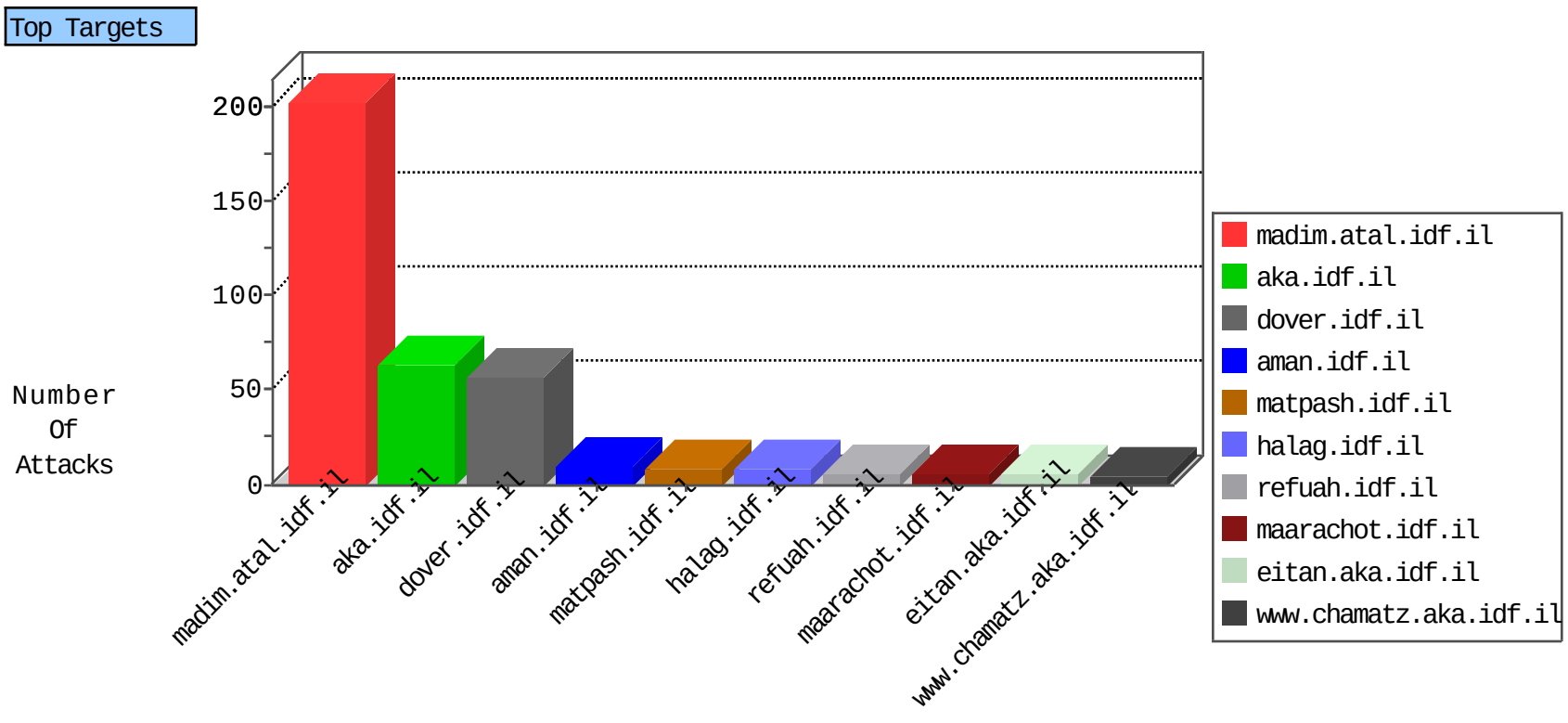
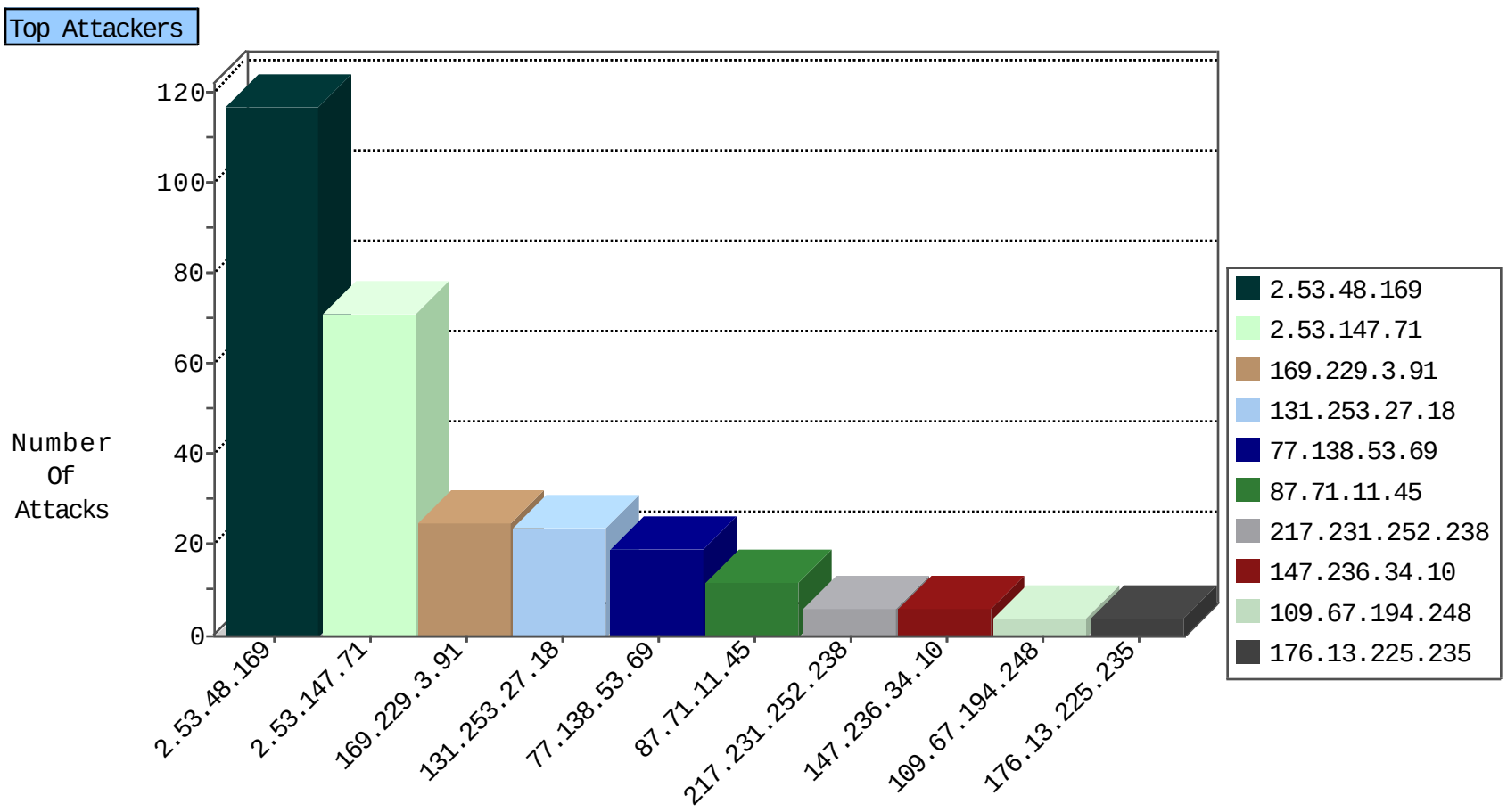
08-17-2016-16:04:09 to 08-17-2016-17:04:09

IDF Under Attack Daily Report

Top Targets



Top Attackers



08-17-2016-16:04:09 to 08-17-2016-17:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.80.217.70	Israel	147.237.72.167	ishurim.aka.idf.il	Black List	drop	2
82.80.78.2	Israel	147.237.77.216	dover.idf.il	Black List	drop	2
2.55.29.13	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
93.158.200.96	Netherlands	147.237.76.39	mobile.meitav.idf.il	Black List	drop	1
82.80.78.2	Israel	147.237.77.176	matpash.idf.il	Black List	drop	1
93.158.200.97	Netherlands	147.237.76.86	navy.idf.il	Black List	drop	1

08-17-2016-16:04:09 to 08-17-2016-17:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
144.76.12.75	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
144.76.12.75	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
162.210.196.100	United States	147.237.77.234	halag.idf.il	C1000074: HTTP: majestic bot	Permit	2

08-17-2016-16:04:09 to 08-17-2016-17:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
209.88.198.94	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.246.133.58	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
52.16.5.197	147.237.77.216	Ireland	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.50	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.255.90.133	147.237.76.199	Netherlands	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
5.29.147.58	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
117.218.181.207	147.237.76.31	India	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
79.178.122.108	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.190	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
5.255.90.133	147.237.77.19	Netherlands	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
5.255.90.133	147.237.76.147	Netherlands	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
5.28.158.233	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

08-17-2016-16:04:09 to 08-17-2016-17:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
87.71.11.45	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
147.236.34.10	Israel	147.237.77.170	maarachot.idf.il	drop	First packet isn't SYN	drop	6
217.231.252.238	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
109.253.130.178	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	2
217.231.252.238	Germany	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	2
176.13.246.15	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
109.253.138.178	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
184.105.139.67	United States	147.237.77.234	halag.idf.il	drop	SAM rule	drop	1
109.253.150.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
176.13.8.248	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
109.253.216.105	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
176.13.232.19	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
212.199.10.242	Israel	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	1
176.13.235.168	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
109.253.132.151	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		drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.48.169	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	117
2.53.147.71	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	71
131.253.27.18	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	24
77.138.53.69	France	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 77.138.53.69	Block	16
176.13.225.235	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
109.67.194.248	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 109.67.194.248	Block	3
46.19.85.129	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
77.126.71.253	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/smalim/undefined	Block	3
2.55.147.111	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
131.253.25.223	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
66.249.78.217	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.217	Block	2
2.53.151.102	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
80.246.133.182	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
176.13.11.5	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.129	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
80.246.136.28	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
77.138.53.69	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/miyun/miyunselectquestionnaire.aspx	Block	2
169.229.3.91	United States	147.237.76.200	eitan.aka.idf.il	Illegal Byte Code Character in Method c…Â2•]ï²]óËËœz=Í•W[[#30]][[#23]]Ç!»„$×#012äÈôî¼	Block	1
46.116.40.10	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 46.116.40.10	Block	1
193.172.37.106	Netherlands	147.237.77.176	matpash.idf.il	Unauthorized HTTP Method	Block	1
81.218.101.66	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/960.css	Block	1
169.229.3.91	United States	147.237.77.234	halag.idf.il	Illegal Byte Code Character in Method ¸áf[[#14]][[#1]]•‡â[[#7]]ƒ¶ßG[[#30]]™R°„Ë/ü[[#3]]_5ú)£[[#20]]g[[#7]]®pÃÍ@6'$iÐ÷ÀÂD÷r[[#25]]	Block	1
169.229.3.91	United States	147.237.77.176	matpash.idf.il	Illegal Byte Code Character in URL škt[[#26]](•0®[['ꞃ#31ן]]vס…Ÿ–#012x)ה\¯בתd[[„ג#1צ¸,®]]»q	Block	1
169.229.3.91	United States	147.237.72.156	aman.idf.il	Multiple Illegal Byte Code Character in URL from 169.229.3.91	Block	1
66.102.9.85	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/pniotanswer.aspx	Block	1
37.26.146.222	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.67.41.73	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
169.229.3.91	United States	147.237.77.226	www.chamatz.aka.idf.il	Multiple Abnormally Long Request from 169.229.3.91	Block	1
79.182.99.20	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
66.249.78.217	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/.well-known/apple-app-site-association	Block	1
169.229.3.91	United States	147.237.76.200	eitan.aka.idf.il	Malformed HTTP Header Line 1	Block	1
141.226.162.245	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
46.116.40.10	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/	Block	1
193.172.37.106	Netherlands	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-en/	Block	1
85.65.201.34	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
169.229.3.91	United States	147.237.77.234	halag.idf.il	Illegal Byte Code Character in URL	Block	1
169.229.3.91	United States	147.237.77.176	matpash.idf.il	Malformed URL škt[[#26]](•0®[['ꞃ#31ן]]v–Ÿ…ס#012)xבת¯\הdג„ ꝕ»צ¸,®]]#1[[	Block	1
77.138.53.69	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/miyun/miyunderugshikulim.aspx	Block	1
169.229.3.91	United States	147.237.72.156	aman.idf.il	Multiple Unknown HTTP Request Method from 169.229.3.91	Block	1
66.249.78.130	Israel	147.237.76.30	himush.idf.il	Unauthorized URL Access to www.tech.atal.idf.il/templates/shared/usercontrols/headerupper/	Block	1
37.142.5.107	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
176.13.245.169	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
80.246.133.99	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
169.229.3.91	United States	147.237.77.226	www.chamatz.aka.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
77.126.23.158	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012ources/images/innerpage/goback.gif	Block	1
169.229.3.91	United States	147.237.76.200	eitan.aka.idf.il	Malformed URL	Block	1
144.76.175.75	Germany	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/giyus	Block	1
46.121.89.28	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/	Block	1
208.115.111.73	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
85.65.202.146	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/	Block	1