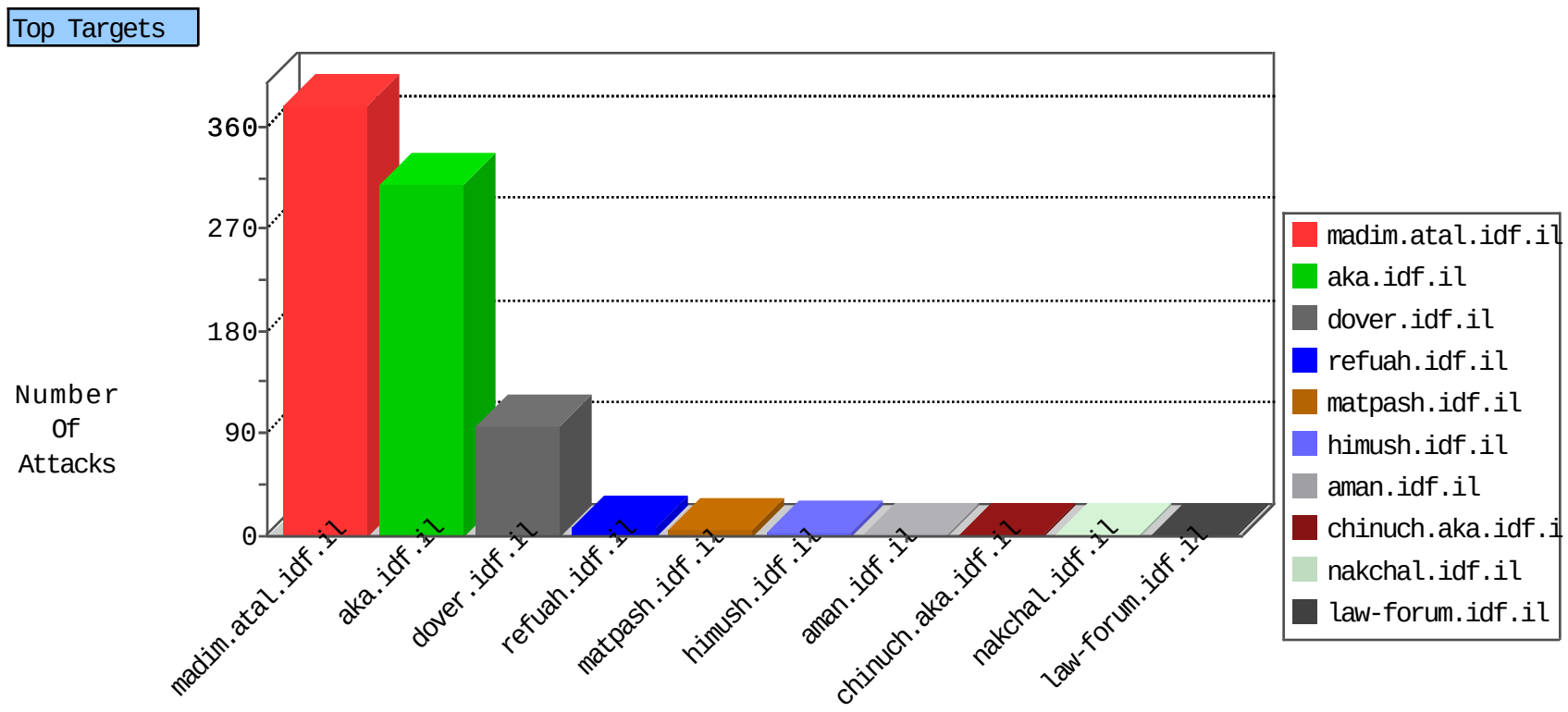
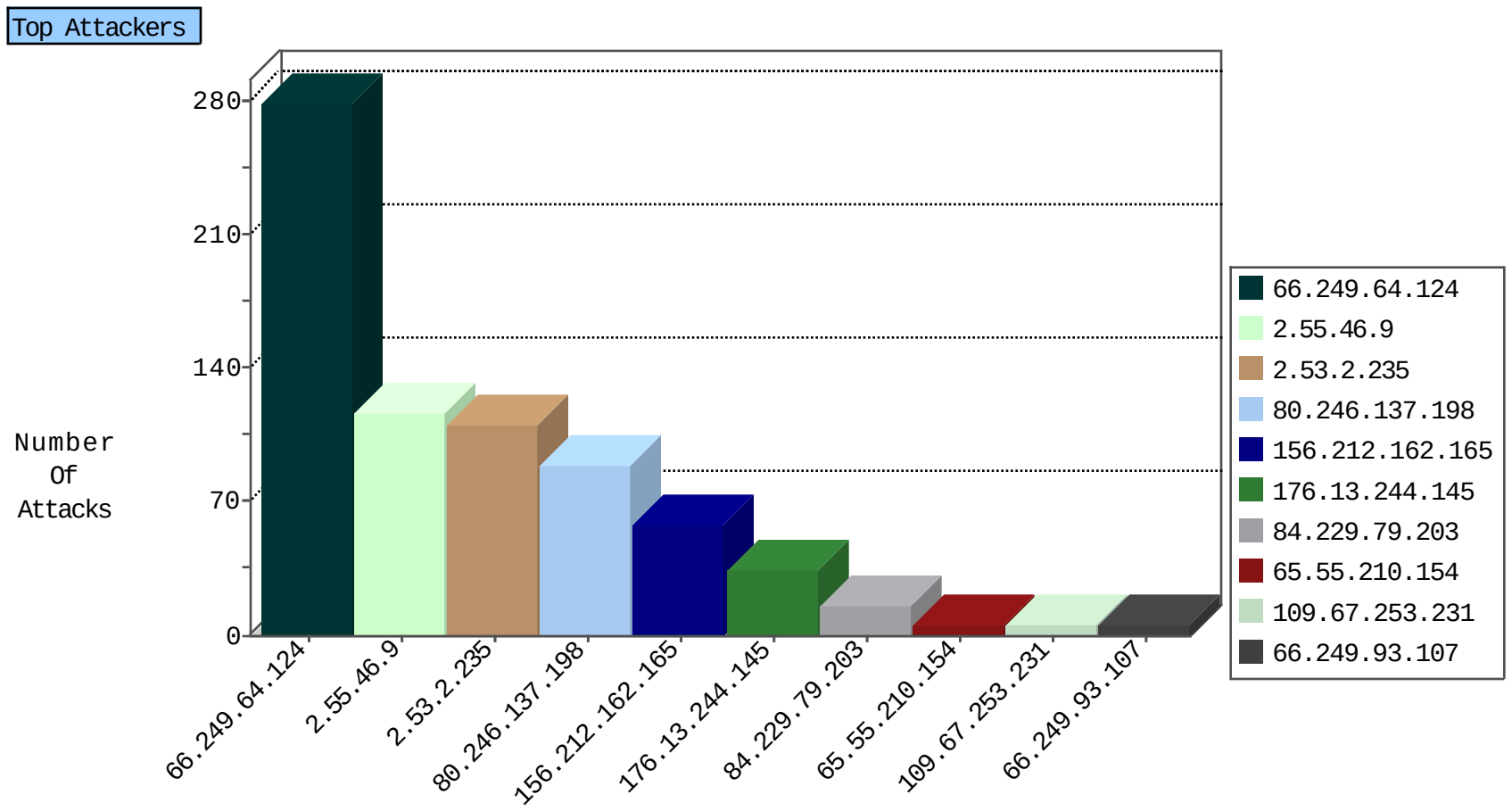
08-20-2016-20:04:05 to 08-20-2016-21:04:05

IDF Under Attack
Daily Report

Top Targets



Top Attackers



08-20-2016-20:04:05 to 08-20-2016-21:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.27.105.72	Israel	147.237.77.216	dover.idf.il	Invalid L4 Header Length	drop	2
185.27.105.72	Israel	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
94.177.160.214	Romania	147.237.76.42	refuah.idf.il	Black List	drop	1
222.187.223.120	China	147.237.76.31	nakchal.idf.il	JLM_Under_Attack_Con_Tcp	drop	1
82.80.78.2	Israel	147.237.77.176	matpash.idf.il	Black List	drop	1
94.177.160.214	Romania	147.237.76.34	yohalan.idf.il	Black List	drop	1
221.4.197.134	China	147.237.76.86	navy.idf.il	JLM_Purple_Con_Limit_Http	drop	1

08-20-2016-20:04:05 to 08-20-2016-21:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
156.212.162.165	Egypt	147.237.77.216	dover.idf.il	24910: HTTP: Python urllib User-Agent Header	Block	4
136.243.152.18	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	3
136.243.152.18	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
106.38.241.105	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1

08-20-2016-20:04:05 to 08-20-2016-21:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.64.124	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	279
156.212.162.165	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	45
162.213.1.246	147.237.77.216	United States	dover.idf.il	Tehila - Perl LWP with fake user agent	4
91.224.160.106	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
87.236.194.161	147.237.76.30	Czech Republic	himush.idf.il	ET SCAN NMAP -sS window 1024	1
179.43.141.228	147.237.8.14	Switzerland	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
71.86.124.86	147.237.77.19	United States	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
173.255.233.124	147.237.77.216	United States	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	1
66.249.64.112	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sA (2)	1
159.253.40.43	147.237.76.147	Turkey	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
46.172.71.251	147.237.77.235	Ukraine	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
159.253.40.43	147.237.76.30	Turkey	himush.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.76.39	Netherlands	mobile.meitav.idf.i	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
89.138.194.126	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
87.236.194.161	147.237.72.217	Czech Republic	e.idf.il	ET SCAN NMAP -sS window 1024	1
173.255.233.124	147.237.77.216	United States	dover.idf.il	SERVER-WEBAPP TRACE attempt	1
59.127.30.133	147.237.76.31	Taiwan	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
159.253.40.43	147.237.76.42	Turkey	refuah.idf.il	ET SCAN Potential SSH Scan	1
159.253.40.43	147.237.0.19	Turkey	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
120.237.232.6	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.76.30	Netherlands	himush.idf.il	ET SCAN Potential SSH Scan	1

08-20-2016-20:04:05 to 08-20-2016-21:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
109.67.253.231	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
66.249.93.107	Europe	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
117.203.166.114	India	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
176.13.243.164	Israel	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	1
109.253.134.145	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
176.13.5.153	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
66.249.93.107	Israel	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
2.55.46.9	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	117
2.53.2.235	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	110
80.246.137.198	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	89
176.13.244.145	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	34
84.229.79.203	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	16
156.212.162.165	Egypt	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 156.212.162.165	Block	6
65.55.210.154	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	6
199.30.24.220	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
46.19.85.95	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
85.64.155.96	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.94.66.20	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	3
84.108.246.184	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.67.194.248	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for aka.idf.il/main/home/default.aspx	Block	2
46.19.86.197	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
94.64.107.127	Greece	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
66.249.76.121	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/idkonim/pages/tutimprahim11012011.aspx	Block	1
157.55.39.110	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
37.26.149.217	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
109.67.194.248	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 109.67.194.248	Block	1
221.199.215.231	Australia	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/	Block	1
66.249.81.218	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
156.212.162.165	Egypt	147.237.77.216	dover.idf.il	Admin Blocking	Block	1
66.249.64.41	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.64.41	Block	1
109.65.145.97	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012ources/images/innerpage/goback.gif	Block	1
66.249.79.143	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8853-he/refuah.aspx	Block	1
176.13.13.195	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
68.180.228.231	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1038-he/cogat.aspx	Block	1
156.212.162.165	Egypt	147.237.77.216	dover.idf.il	Multiple Admin Blocking from 156.212.162.165	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
109.65.169.22	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	1
66.249.79.147	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
109.67.204.187	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.19.86.157	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
87.69.87.15	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
77.138.243.23	France	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/favicon.ico	Block	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/8/17708.pdf	Block	1
2.55.11.34	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
109.66.59.69	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/yohalan/main.asp	Block	1
84.108.47.121	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
66.249.81.212	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
131.253.27.15	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
79.177.125.213	Israel	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
66.249.76.120	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 66.249.76.120	Block	1
156.212.162.165	Egypt	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/admin/	Block	1
109.67.179.146	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
66.249.81.215	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
204.79.180.37	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/portalmiluim/templates/inner.asp	Block	1
148.251.2.180	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/iturim/asp/displayonesoldier.asp	Block	1
107.178.42.105	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
79.182.89.43	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1