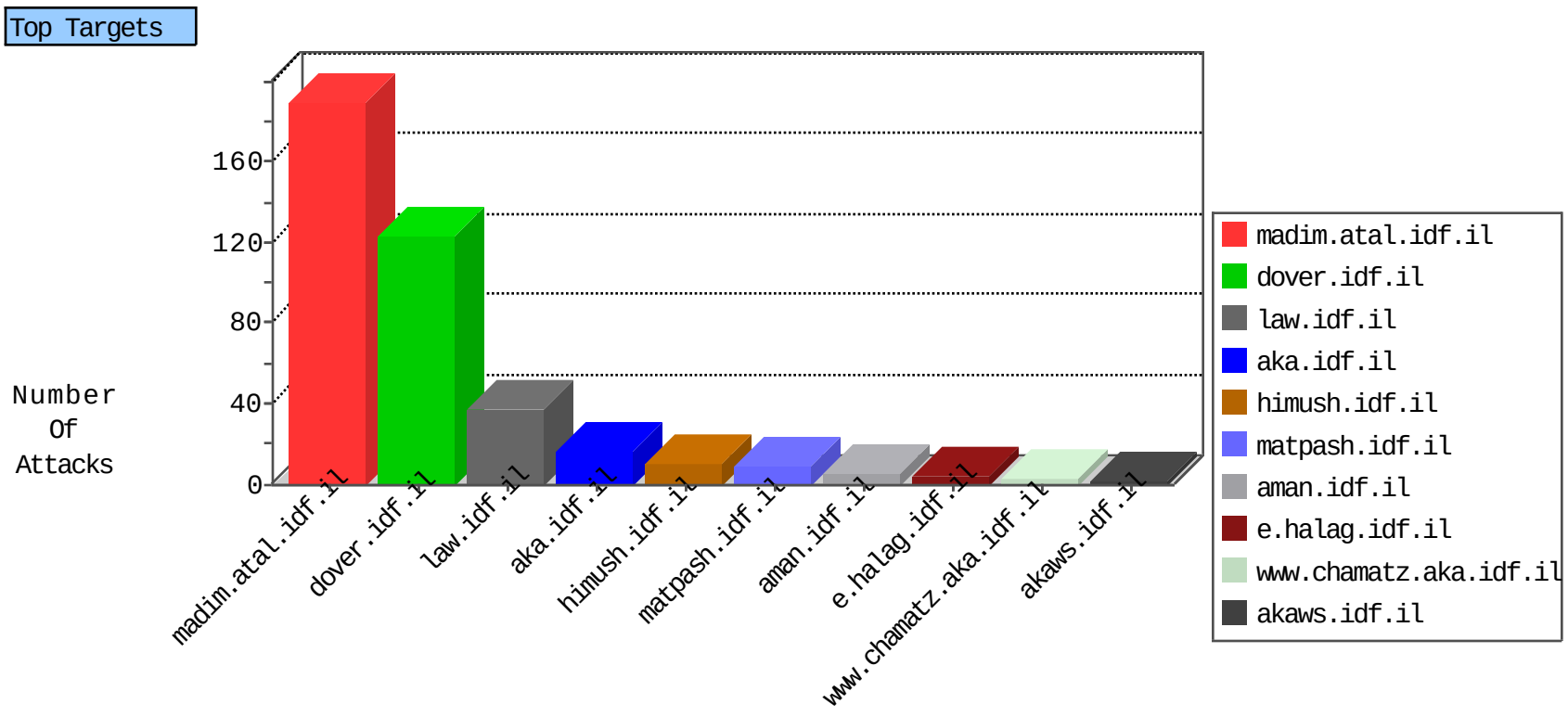
08-20-2016-16:04:01 to 08-20-2016-17:04:01

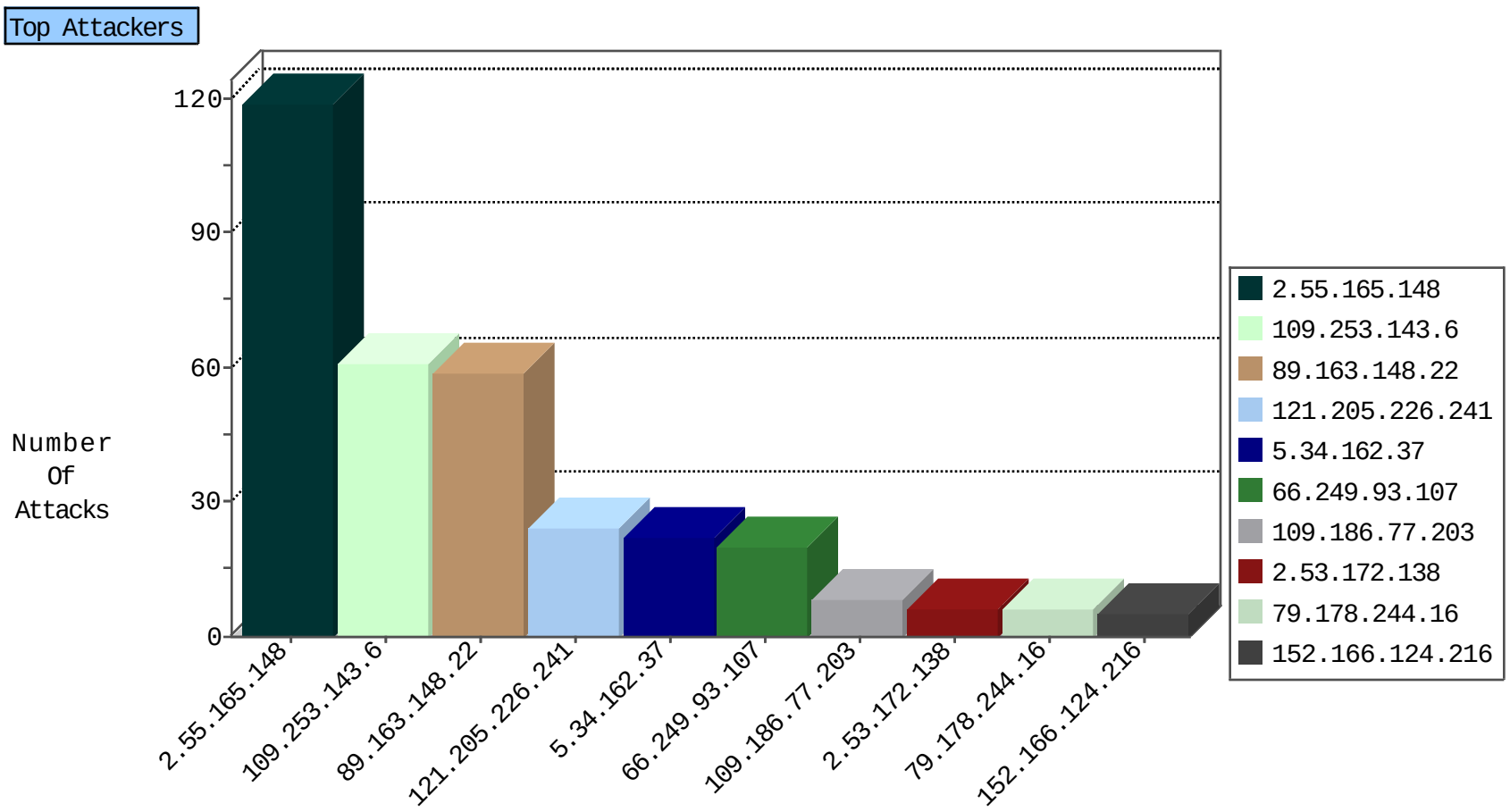
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

08-20-2016-16:04:01 to 08-20-2016-17:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.220.87	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6
58.11.155.3	Thailand	147.237.76.202	e.halag.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
115.230.125.146	China	147.237.76.202	e.halag.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
14.169.109.87	Vietnam	147.237.76.30	himush.idf.il	Black List	drop	1
115.230.125.146	China	147.237.77.61	e.cogat.idf.il	JLM_Purple_Con_Limit_Http	drop	1
192.69.91.134	United States	147.237.76.30	himush.idf.il	Black List	drop	1
115.230.125.146	China	147.237.77.121	e.navy.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
195.154.172.204	France	147.237.0.200	m4u.idf.il	JLM_Purple_Con_Limit_Http	drop	1
185.94.111.1	Russian Federation	147.237.76.176	test.ncore.idf.i	Black List	drop	1
185.94.111.1	Russian Federation	147.237.76.199	e.nakchal.idf.il	Black List	drop	1

08-20-2016-16:04:01 to 08-20-2016-17:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
89.163.148.22	Germany	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Permit	37
89.163.148.22	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	12
89.163.148.22	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	3
89.163.148.22	Germany	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Permit	3
89.163.148.22	Germany	147.237.0.34	tikshuv.idf.il	C1000074: HTTP: majestic bot	Permit	2
89.163.148.22	Germany	147.237.77.226	www.chamatz.aka.idf.il	C1000074: HTTP: majestic bot	Permit	2

08-20-2016-16:04:01 to 08-20-2016-17:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
109.186.77.203	147.237.76.30	Israel	himush.idf.il	ET SCAN NMAP -sA (2)	6
162.213.1.246	147.237.77.216	United States	dover.idf.il	Tehila - Perl LWP with fake user agent	4
91.125.184.101	147.237.77.216	United Kingdom	dover.idf.il	Tehila - Perl LWP with fake user agent	2
109.186.77.203	147.237.76.30	Israel	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
94.102.48.195	147.237.8.27	Netherlands	e.madim.atal.idf.i	ET SCAN NMAP -sS window 1024	1
92.29.66.222	147.237.76.196	United Kingdom	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.195	147.237.8.14	Netherlands	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.155	147.237.76.44	Ukraine	e.refuah.idf.il	ET SCAN NMAP -sS window 4096	1
58.11.155.3	147.237.76.31	Thailand	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
188.161.91.27	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	ET SCAN NMAP -sA (2)	1

08-20-2016-16:04:01 to 08-20-2016-17:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
5.34.162.37	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
66.249.93.107	Europe	147.237.77.216	dover.idf.il	drop	SAM rule	drop	13
5.34.162.37	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
79.178.244.16	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
152.166.124.216	Dominican Republic	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
66.249.93.107	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
66.249.93.107	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	3
210.213.146.164	Philippines	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
69.30.221.242	United States	147.237.72.156	aman.idf.il	drop	SAM rule	drop	2
5.28.175.190	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
129.56.2.38	Nigeria	147.237.0.35	akaws.idf.il	drop		drop	1
176.13.23.11	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
84.111.140.99	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
129.56.2.38	Nigeria	147.237.76.34	yohalan.idf.il	drop		drop	1
184.105.139.110	United States	147.237.0.33	idf.il	drop		drop	1
109.253.144.49	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
115.230.125.146	China	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
41.105.50.236	Algeria	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
157.55.39.110	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
129.56.2.38	Nigeria	147.237.0.33	idf.il	drop		drop	1
176.13.16.89	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
82.221.105.7	Iceland	147.237.0.35	akaws.idf.il	drop		drop	1

08-20-2016-16:04:01 to 08-20-2016-17:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.55.165.148	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	119
109.253.143.6	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	61
121.205.226.241	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 121.205.226.241	Block	17
121.205.226.241	China	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	6
2.53.172.138	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
46.117.106.108	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
66.249.83.245	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.76.83	Block	3
109.226.22.161	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
66.249.83.242	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
65.49.68.197	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/iturim/	Block	2
80.246.136.244	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
109.253.142.123	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
77.237.146.28	Czech Republic	147.237.77.74	law.idf.il	Unauthorized URL Access to /	Block	1
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
144.76.236.183	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1
84.109.126.219	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.102.9.76	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
5.29.208.47	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/4/	Block	1
79.177.124.204	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$rbSearchSit in www.aka.idf.il/main/sachar/	None	1
180.76.15.27	China	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/1.he/960.css	Block	1
46.121.96.74	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
87.68.32.127	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	1
66.249.83.248	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.102.9.105	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
37.26.149.254	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
79.180.2.59	Israel	147.237.77.216	dover.idf.il	PHP Attempt	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
54.81.168.187	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
89.138.14.102	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
68.180.228.185	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1379-he/dover.aspx	Block	1
66.249.64.244	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/templates/shared/usercontrols/headerupper/	Block	1
37.142.247.140	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
79.180.2.59	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
66.249.76.98	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
65.49.68.197	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 65.49.68.197	Block	1
77.138.140.176	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/favicon.ico	Block	1
66.249.66.177	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_pictures.asp	Block	1
121.205.226.241	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/index.asp	Block	1
46.19.85.126	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

08-20-2016-16:04:01 to 08-20-2016-17:04:01