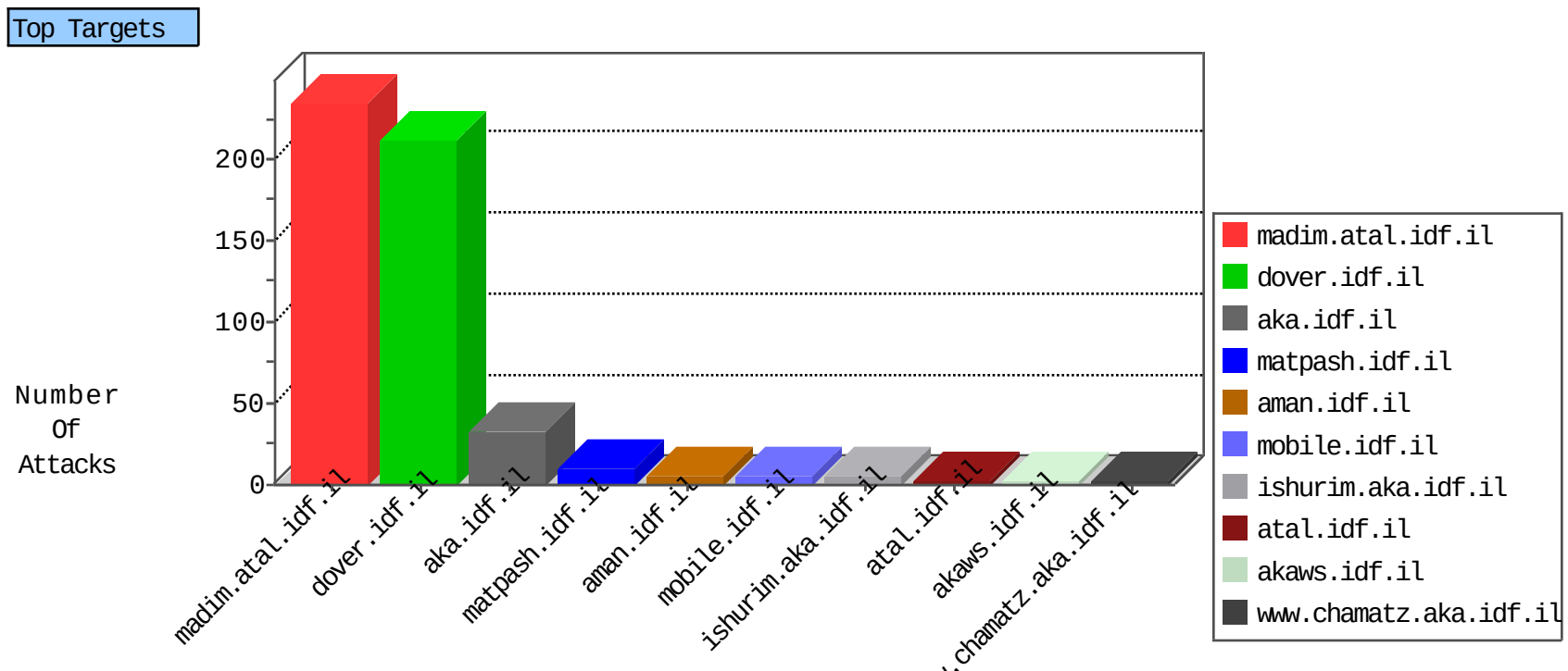
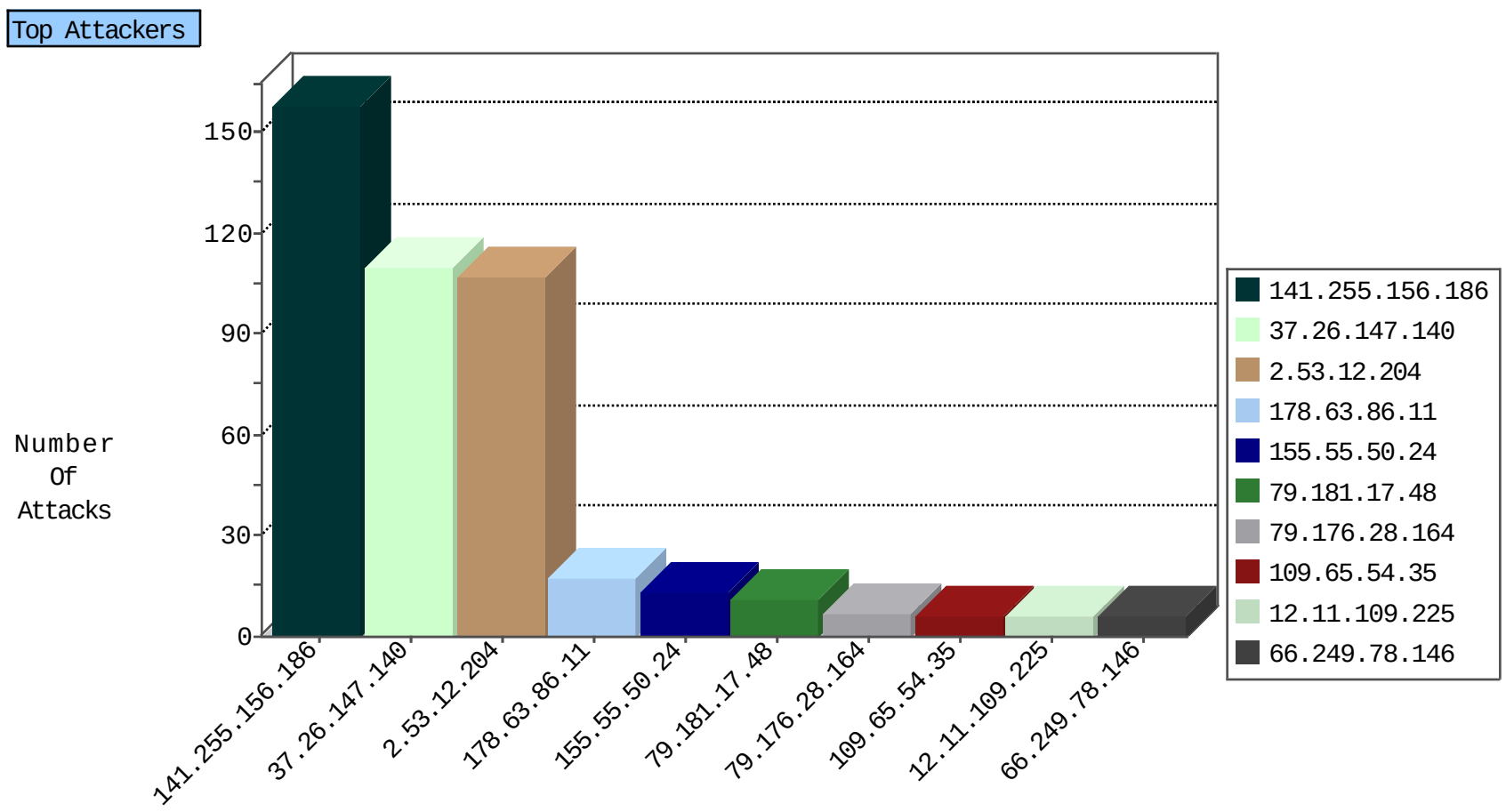
08-16-2016-23:04:01 to 08-17-2016-00:04:01

IDF Under Attack Daily Report

Top Targets



Top Attackers



08-16-2016-23:04:01 to 08-17-2016-00:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
141.255.156.186	Netherlands	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	2340
82.80.78.2	Israel	147.237.77.216	dover.idf.il	Black List	drop	2
149.202.223.177	France	147.237.76.34	yohalan.idf.il	Black List	drop	1
93.158.200.118	Netherlands	147.237.76.147	chinuch.aka.idf.il	Black List	drop	1
89.248.171.2	Netherlands	147.237.76.31	nakchal.idf.il	Black List	drop	1
123.59.59.52	China	147.237.77.233	atal.idf.il	block-sp-traf1	forward	1
89.248.174.4	Netherlands	147.237.76.199	e.nakchal.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	147.237.76.199	e.nakchal.idf.il	Black List	drop	1

08-16-2016-23:04:01 to 08-17-2016-00:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
178.63.86.11	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	17
69.30.198.178	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
79.182.130.132	Israel	147.237.72.156	aman.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
93.174.95.106	Netherlands	147.237.72.166	aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
141.255.156.186	Netherlands	147.237.77.216	dover.idf.il	4212: HTTP: PHP File Include Vulnerability	Block	1
178.17.174.99	Moldova, Republic of	147.237.77.216	dover.idf.il	24910: HTTP: Python urllib User-Agent Header	Block	1

08-16-2016-23:04:01 to 08-17-2016-00:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.120.122.219	147.237.77.216	Israel	dover.idf.il	Xenu Link Sleuth User Agent	3
123.241.251.40	147.237.76.42	Taiwan	refuah.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
113.108.10.31	147.237.77.61	China	e.cogat.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
112.196.49.101	147.237.77.226	India	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 4096	1
112.196.49.101	147.237.77.226	India	www.chamatz.aka.idf.il	ET SCAN NMAP -f -sS	1
94.102.48.195	147.237.76.200	Netherlands	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
93.158.215.183	147.237.77.234	Netherlands	halag.idf.il	ET SCAN NMAP -sS window 1024	1
82.91.20.184	147.237.0.200	Italy	m4u.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
204.245.56.245	147.237.8.46	United States	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
58.218.204.245	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
141.255.156.186	147.237.77.216	Netherlands	dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
58.218.204.245	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
113.199.6.58	147.237.76.177	Korea, Republic of	ncore.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
46.120.122.219	147.237.72.166	Israel	aka.idf.il	Xenu Link Sleuth User Agent	1
113.108.10.31	147.237.72.14	China	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
112.196.49.101	147.237.77.226	India	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 2048	1
94.102.48.195	147.237.77.19	Netherlands	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.195	147.237.76.197	Netherlands	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
93.158.215.183	147.237.77.227	Netherlands	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
80.246.130.208	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
177.141.223.124	147.237.8.46	Brazil	e.chinuch.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
58.218.204.245	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1

08-16-2016-23:04:01 to 08-17-2016-00:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.181.17.48	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
155.55.50.24	Norway	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	9
12.11.109.225	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
109.253.147.197	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	5
155.55.50.24	Norway	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
141.255.156.186	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
79.183.14.83	Israel	147.237.77.243	mobile.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	2
175.44.13.4	China	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
141.212.122.27	United States	147.237.0.33	idf.il	drop		drop	1
141.212.122.28	United States	147.237.0.35	akaws.idf.il	drop		drop	1
66.249.64.134	Israel	147.237.0.33	idf.il	drop		drop	1
141.212.122.29	United States	147.237.0.35	akaws.idf.il	drop		drop	1
74.88.66.25	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
176.13.6.209	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
109.253.207.191	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
79.177.223.69	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	1
195.138.201.60	Slovenia	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.26	United States	147.237.0.33	idf.il	drop		drop	1
5.102.242.137	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
202.28.10.20	Thailand	147.237.77.74	law.idf.il	drop	SAM rule	drop	1

08-16-2016-23:04:01 to 08-17-2016-00:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.147.140	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	110
2.53.12.204	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	107
79.176.28.164	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	7
109.65.54.35	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.78.146	Block	3
176.13.20.12	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.53.52.72	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
79.178.186.82	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
24.24.221.165	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/main/	Block	2
66.249.81.215	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
46.19.86.41	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
109.253.130.105	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
77.139.146.60	France	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
46.121.136.43	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
123.126.68.113	China	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
2.55.131.190	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
84.108.84.131	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	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
46.121.136.43	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/wp-login.php	Block	1
157.55.39.190	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/main/smalim/smalim.aspx	None	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sachar/forms/downloadform.asp	Block	1
84.108.84.131	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/wp-login.php	Block	1
66.249.64.136	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 66.249.64.136	Block	1
176.13.18.230	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
79.181.161.93	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1136-he/atal.aspx	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docId in www.aka.idf.il/chinuch/klali/	None	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
66.249.76.42	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/apple-app-site-association	Block	1
80.246.130.49	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docId in www.aka.idf.il/sites/skira/default.asp	None	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
83.215.180.139	Austria	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	1

08-16-2016-23:04:01 to 08-17-2016-00:04:01