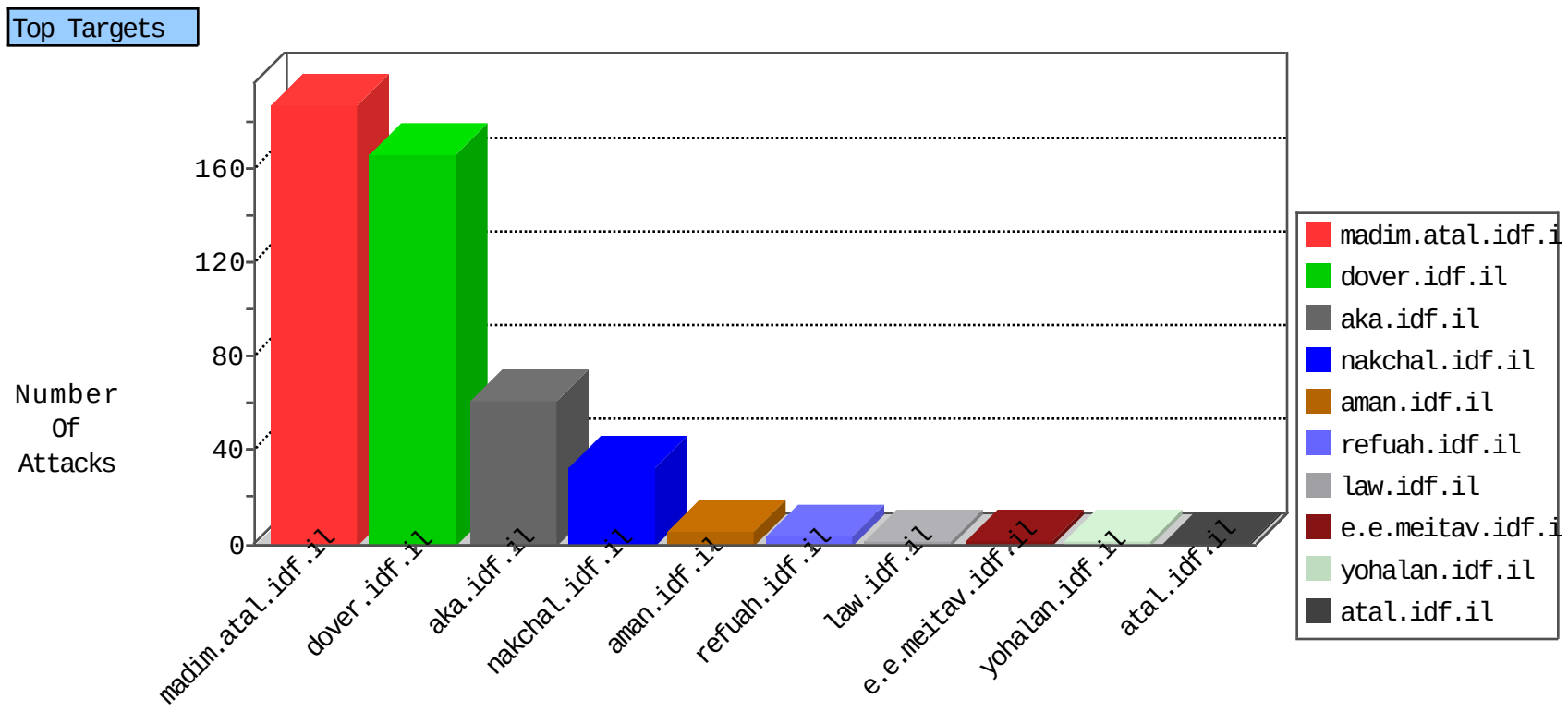
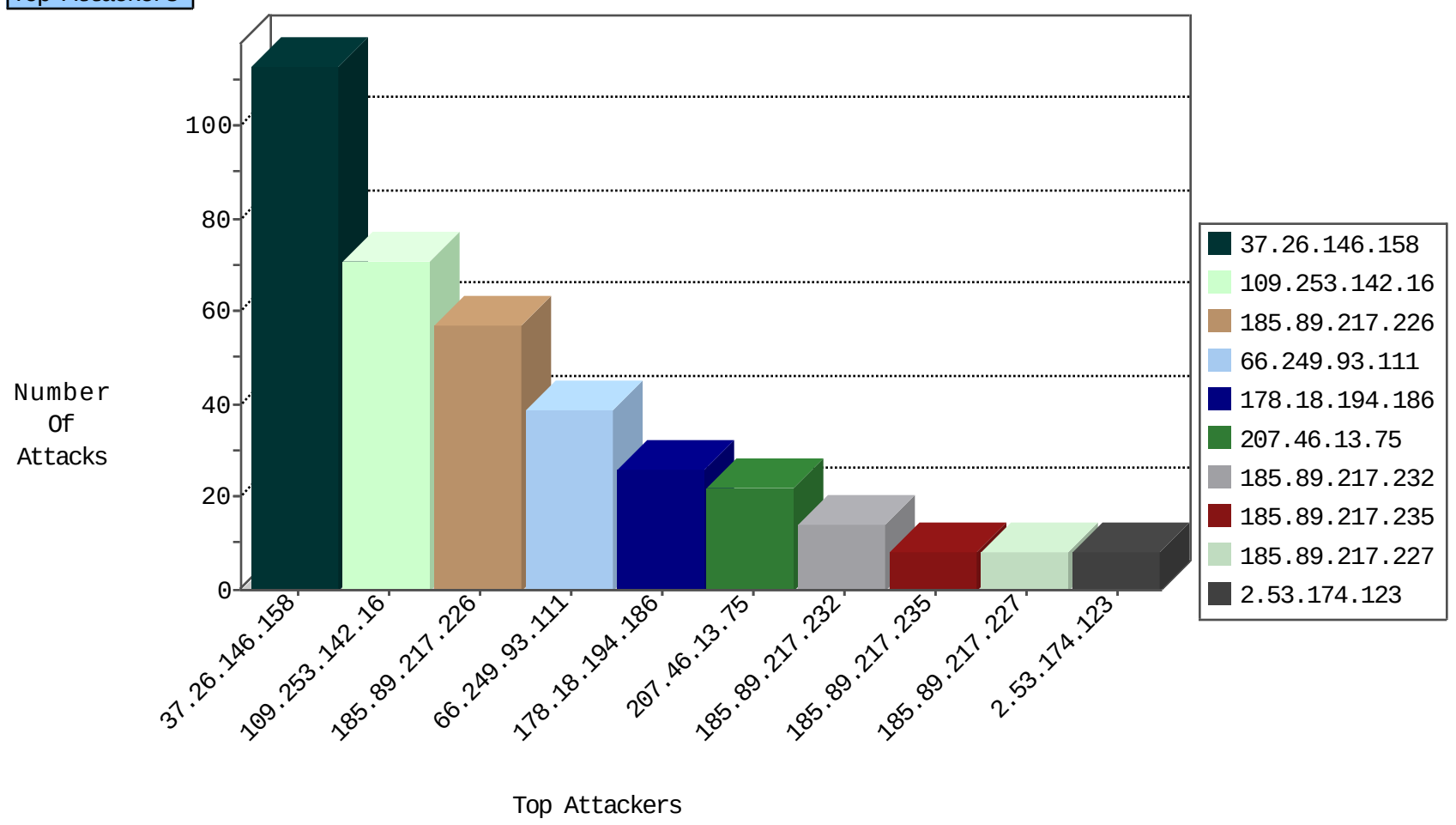
09-04-2016-06:04:01 to 09-04-2016-07:04:01

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-04-2016-06:04:01 to 09-04-2016-07:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.89.217.231	Netherlands	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
185.94.111.1	Russian Federation	147.237.76.38	e.e.meitav.idf.i	Black List	drop	1

09-04-2016-06:04:01 to 09-04-2016-07:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

09-04-2016-06:04:01 to 09-04-2016-07:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
178.18.194.186	147.237.72.166	Turkey	aka.idf.il	SQL Injection - Select From	26
62.149.132.252	147.237.72.166	Italy	aka.idf.il	SQL Injection - Select From	8
81.176.226.68	147.237.72.166	Russian Federation	aka.idf.il	SQL Injection - Select From	8
87.115.137.146	147.237.77.74	United Kingdom	law.idf.il	Tehila - Perl LWP with fake user agent	2
185.72.177.20	147.237.76.197	Romania	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
183.129.160.229	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
94.102.52.71	147.237.76.34	Netherlands	yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
66.249.76.117	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
183.129.160.229	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
183.129.160.229	147.237.0.15	China	kosher-kravi.idf.i	ET SCAN Potential SSH Scan	1
94.102.52.71	147.237.76.44	Netherlands	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
87.236.194.161	147.237.76.34	Czech Republic	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.65.46	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	1

09-04-2016-06:04:01 to 09-04-2016-07:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.93.111	Europe	147.237.77.216	dover.idf.il	drop	SAM rule	drop	38
185.89.217.226	Netherlands	147.237.76.31	nakchal.idf.il	drop	SAM rule	drop	33
207.46.13.75	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	22
185.89.217.232	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
185.89.217.226	Netherlands	147.237.77.216	dover.idf.il	drop	SAM rule	drop	13
185.89.217.226	Netherlands	147.237.77.216	dover.idf.il	drop		drop	11
185.89.217.235	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
185.89.217.227	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.86.107	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	6
185.89.217.230	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
185.89.217.233	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
185.89.217.225	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
185.89.217.228	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
109.253.200.95	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
185.89.217.229	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
134.174.21.23	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
185.89.217.231	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
185.89.217.234	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
2.55.34.167	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
134.174.21.190	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
176.13.249.254	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
66.249.93.111	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
46.19.85.239	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	1
216.218.206.94	United States	147.237.0.200	m4u.idf.il	drop		drop	1

09-04-2016-06:04:01 to 09-04-2016-07:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.146.158	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	113
109.253.142.16	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	71
2.53.174.123	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	8
109.253.157.176	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
87.69.224.165	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
157.55.39.221	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	1
31.154.49.17	Israel	147.237.72.156	aman.idf.il	Multiple Malformed URL from 31.154.49.17	Block	1
66.249.64.30	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/text.css	Block	1
180.76.15.158	China	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/datepicker.css	Block	1
66.249.76.117	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
31.154.49.17	Israel	147.237.72.156	aman.idf.il	Multiple Unknown HTTP Request Method from 31.154.49.17	Block	1
66.249.64.36	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
197.35.90.182	Egypt	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he/dover.aspx'	Block	1
79.181.248.160	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
31.154.49.17	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to /example	Block	1
115.28.154.44	China	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
66.249.64.227	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/994-9070-he/atal.aspx	Block	1
31.154.49.17	Israel	147.237.72.156	aman.idf.il	Illegal HTTP Version you	Block	1
84.229.3.29	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/favicon.ico	Block	1
31.154.49.17	Israel	147.237.72.156	aman.idf.il	Unknown HTTP Request Method send in URL	Block	1
115.28.154.44	China	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/wp-login.php	Block	1
66.249.76.46	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/default.asp	Block	1
31.154.49.17	Israel	147.237.72.156	aman.idf.il	Malformed URL	Block	1

09-04-2016-06:04:01 to 09-04-2016-07:04:01