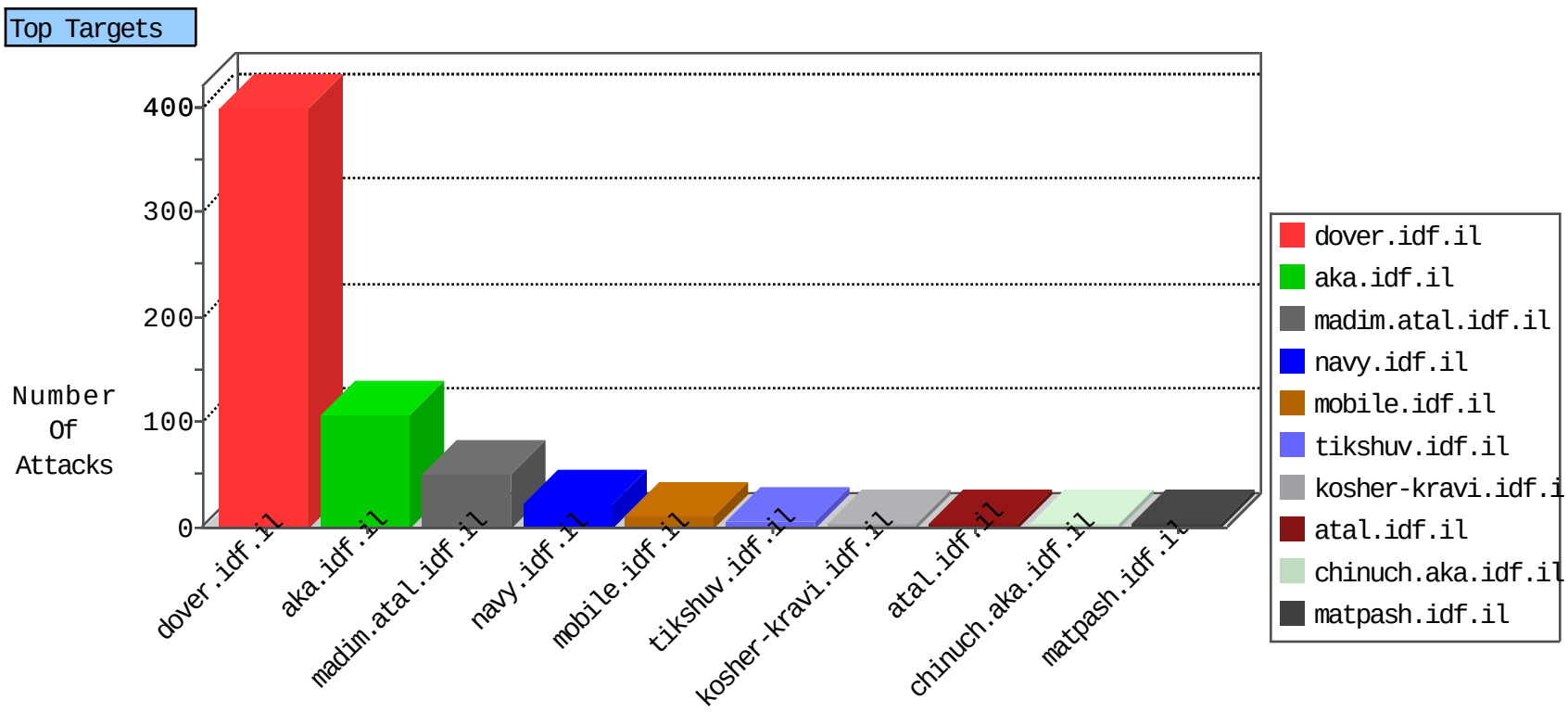
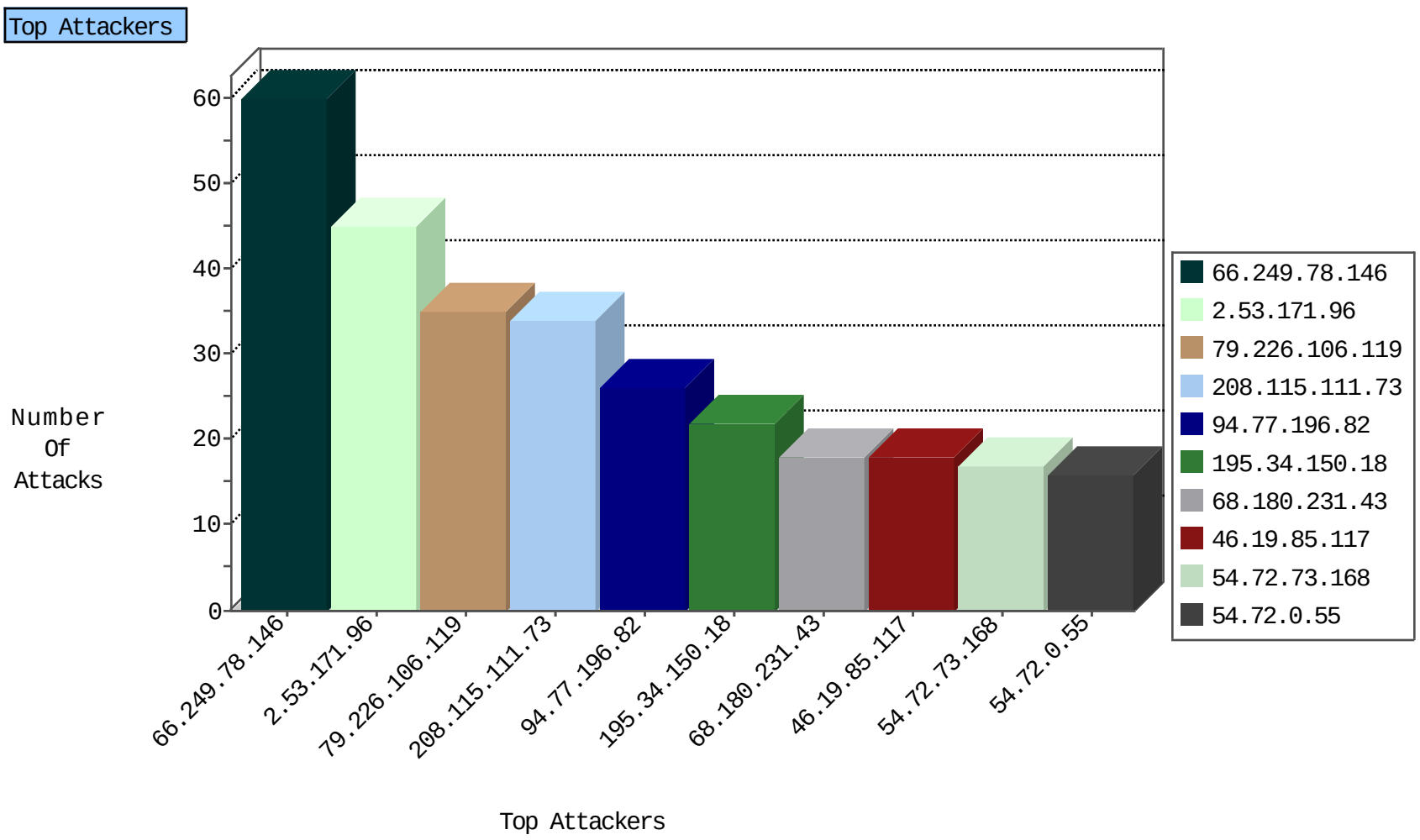
05-03-2016-06:04:01 to 05-03-2016-07:04:01

IDF Under Attack Daily Report

Top Targets



Top Attackers



05-03-2016-06:04:01 to 05-03-2016-07:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.142.68.22	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	18
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	2
52.28.32.164	Germany	147.237.76.197	e.himush.idf.il	JLM_Purple_Con_Limit_Https	drop	1
71.6.216.38	United States	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1

05-03-2016-06:04:01 to 05-03-2016-07:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

05-03-2016-06:04:01 to 05-03-2016-07:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
193.201.227.120	147.237.0.34	Ukraine	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
128.127.0.45	147.237.8.14	Italy	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
104.171.122.176	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sS window 1024	1
193.36.35.241	147.237.8.14	Russian Federation	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
104.171.122.176	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sS window 2048	1
104.171.122.176	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -f -sS	1

05-03-2016-06:04:01 to 05-03-2016-07:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	57
79.226.106.119	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
198.58.103.160	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
154.5.173.70	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.103.102	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.103.115	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
207.46.13.22	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
66.249.64.169	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
165.225.72.65	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
157.55.39.53	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
37.26.146.211	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
203.47.85.194	Australia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.117	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
192.249.66.247	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.20	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.117	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.20	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
174.93.118.195	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.117	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.85.117	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
66.249.78.95	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
66.249.64.230	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
66.249.93.245	Europe	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.160.178.97	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
194.187.168.223	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
87.71.78.69	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.66.190	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.64.187	United States	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.18.251	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.59	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.93.180	Europe	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
66.249.64.98	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.93.184	Europe	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
157.55.39.106	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.171.96	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	45
104.34.76.253	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 104.34.76.253	Block	5
46.19.85.128	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.55.34.242	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.78.254	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.78.254	Block	2
37.26.147.185	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/modiin/resources/images/favicon/favicon.png	Block	2
217.69.133.245	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/home/default.aspx 29/01/2012	Block	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1384-12681-he/dover.aspx	Block	1
104.236.18.208	United States	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to kosher-kravi.idf.il/templates/shared/usercontrols/headerupper/	Block	1
109.160.178.97	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012 ources/images/innerpage/goback.gif	Block	1
68.180.230.45	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
194.187.168.223	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
208.115.113.82	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/site/unselecatble.aspx	Block	1
66.249.64.230	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1362-14440-he/dover.aspx	Block	1
104.236.18.208	United States	147.237.0.15	kosher-kravi.idf.i	Multiple Unauthorized URL Access from 104.236.18.208	Block	1