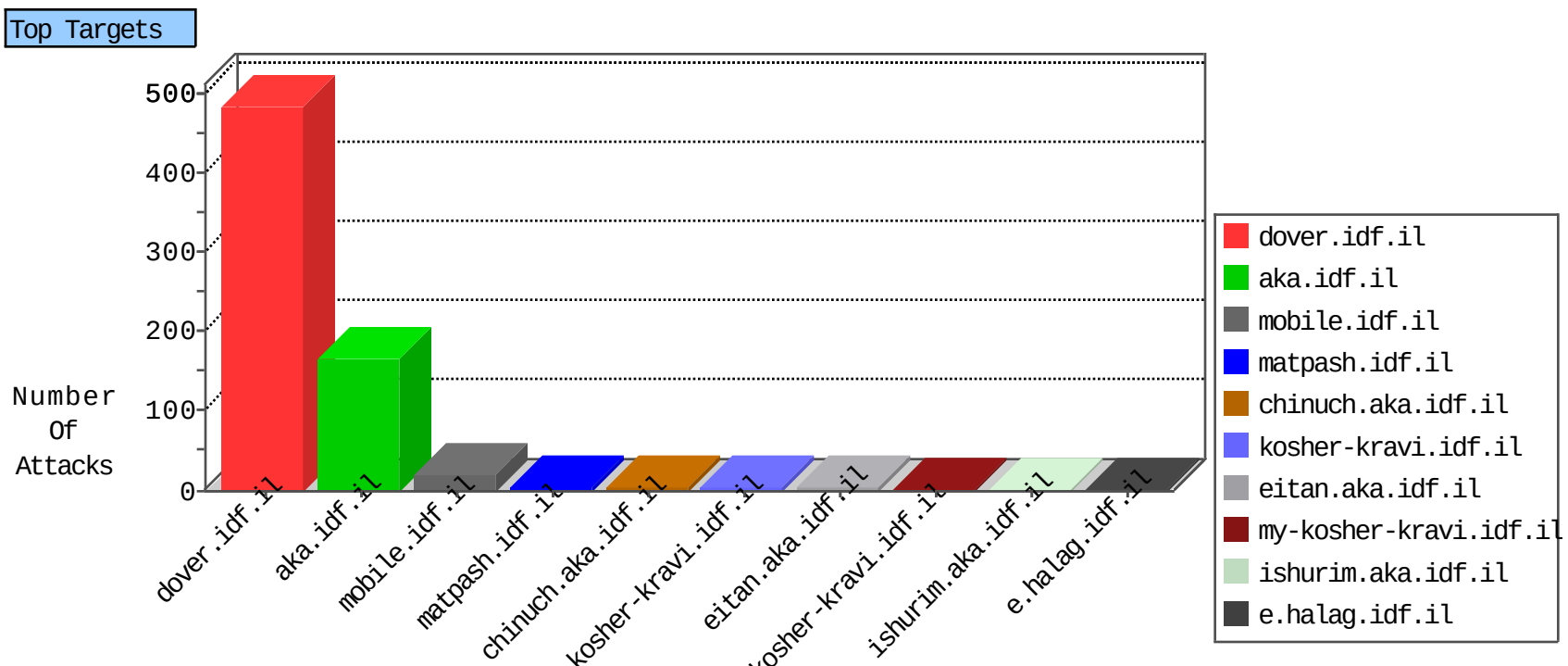
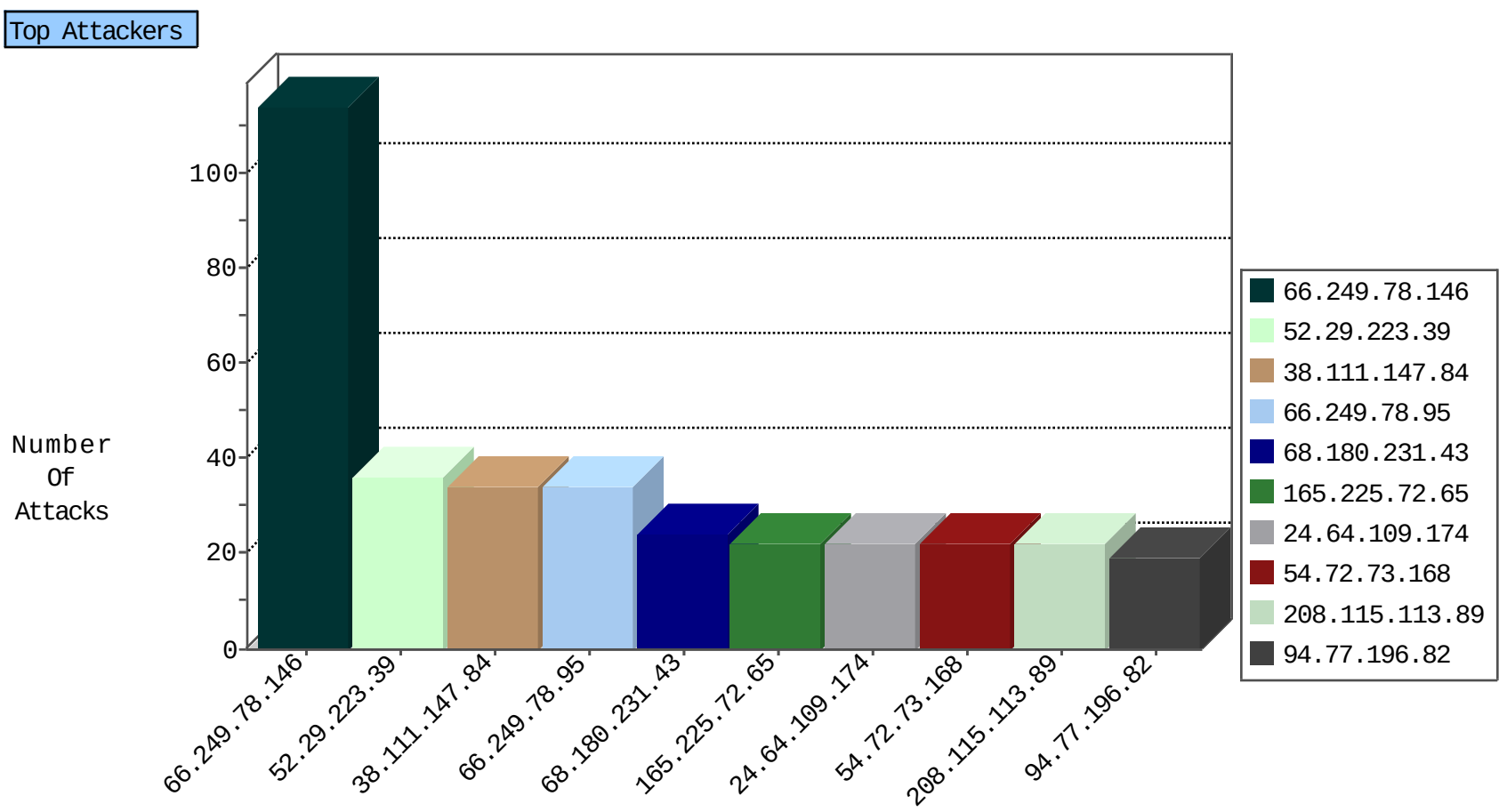
05-03-2016-05:04:08 to 05-03-2016-06:04:08

IDF Under Attack Daily Report

Top Targets



Top Attackers



05-03-2016-05:04:08 to 05-03-2016-06:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
121.42.55.132	China	147.237.72.14	dover.idf.il(old)	L4 Source or Dest Port Zero	drop	2
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	2

05-03-2016-05:04:08 to 05-03-2016-06:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

05-03-2016-05:04:08 to 05-03-2016-06:04:08

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
66.249.78.159	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
112.217.150.112	147.237.0.15	Korea, Republic of	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
62.38.220.113	147.237.76.147	Greece	chinuch.aka.idf.il	ET SCAN NMAP -sS window 4096	1
46.151.52.231	147.237.8.14	Ukraine	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
202.57.162.132	147.237.0.16	Thailand	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
189.202.1.40	147.237.77.234	Mexico	halag.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
183.60.252.84	147.237.76.202	China	e.halag.idf.il	ET SCAN NMAP -sS window 2048	1
183.60.252.84	147.237.76.202	China	e.halag.idf.il	ET SCAN NMAP -f -sS	1
62.38.220.113	147.237.76.147	Greece	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
208.100.26.228	147.237.77.179	United States	e.mazi.idf.il	ET SCAN Rapid POP3 Connections - Possible Brute Force Attack	1
189.202.1.40	147.237.77.74	Mexico	law.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
183.60.252.84	147.237.76.202	China	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1

05-03-2016-05:04:08 to 05-03-2016-06:04:08

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	114
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
38.111.147.84	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
24.64.109.174	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
165.225.72.65	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
66.249.78.95	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
66.87.117.118	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
73.153.29.153	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.102.95	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.103.28	United States	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
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
162.243.118.199	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
84.108.65.121	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
159.45.22.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
66.249.78.95	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
192.249.66.247	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
79.177.142.32	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
79.177.142.32	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
98.116.52.63	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
68.61.54.74	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
188.120.154.49	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
157.55.39.106	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
112.133.229.22	India	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
69.119.112.243	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
198.58.103.115	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
188.120.154.49	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
188.247.81.158	Jordan	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
37.26.146.187	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.78.206	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.126.235.112	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
207.46.13.178	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
141.8.142.1	Russian Federation	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	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
66.249.93.247	Europe	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
188.120.154.49	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
67.82.191.148	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3

05-03-2016-05:04:08 to 05-03-2016-06:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.32.179.229	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	3
73.22.155.10	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/	Block	2
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
66.249.64.143	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
104.34.76.253	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/	Block	1
66.249.78.236	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8833-he/refuah.aspx	Block	1
24.218.80.94	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/templates/homepage/mobile	Block	1
195.154.199.235	France	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
76.9.197.2	Canada	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	1
66.249.64.230	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1806-21853-he/dover.aspx	Block	1
118.138.38.42	Australia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/home/default.aspx	Block	1
38.111.147.84	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
195.154.199.235	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/wp-login.php	Block	1
84.111.13.58	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
164.132.161.85	Italy	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1139-he/atal.aspx	Block	1
66.249.78.254	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/m/	Block	1
66.249.64.3	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/yohalan/forums/forums.asp	Block	1
217.69.133.243	Russian Federation	147.237.72.166	aka.idf.il	Unknown Parameter sidescroll in aka.idf.il/giyus/leshakot/	None	1
85.111.44.238	Turkey	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/index.php	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	1
184.105.139.68	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.16/	Block	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-14402-he/do	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/5/71475.pdf	Block	1
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	1

05-03-2016-05:04:08 to 05-03-2016-06:04:08