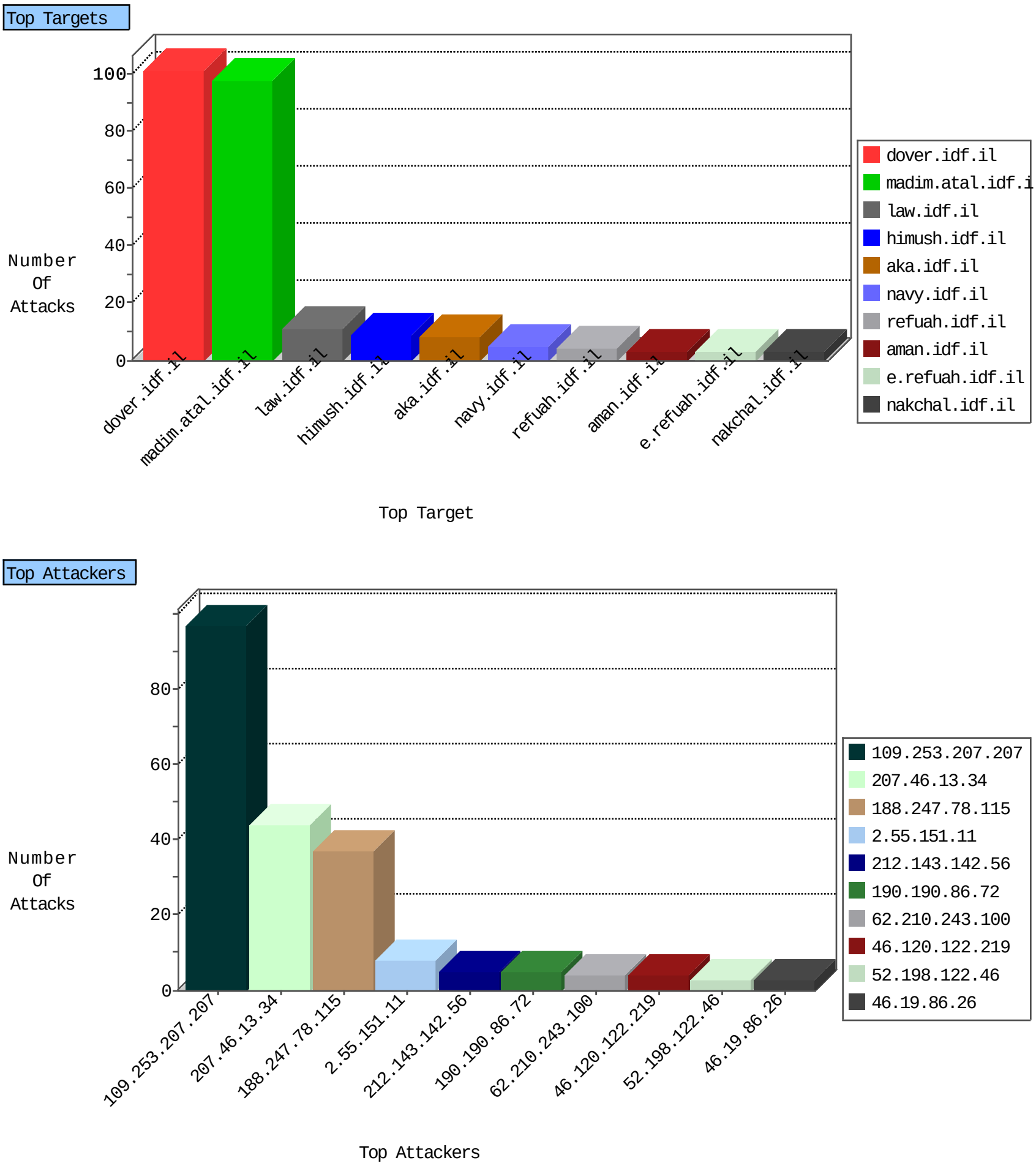
10-03-2016-05:04:01 to 10-03-2016-06:04:01

IDF Under Attack Daily Report



10-03-2016-05:04:01 to 10-03-2016-06:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.94.111.1	Russian Federation	147.237.76.197	e.himush.idf.il	Black List	drop	1
209.126.136.2	United States	147.237.76.44	e.refuah.idf.il	Black List	drop	1
93.174.94.235	Netherlands	147.237.76.30	himush.idf.il	Black List	drop	1
185.94.111.1	Russian Federation	147.237.76.42	refuah.idf.il	Black List	drop	1

10-03-2016-05:04:01 to 10-03-2016-06:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

10-03-2016-05:04:01 to 10-03-2016-06:04:01

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
123.59.173.17	147.237.77.74	China	law.idf.il	ET SCAN NMAP -sS window 1024	1
115.239.251.250	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	1
66.249.75.48	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	1
45.33.124.223	147.237.8.28	United States	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
31.220.3.180	147.237.76.39	Belize	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
31.45.132.4	147.237.77.178	Croatia	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
14.152.59.11	147.237.76.86	China	navy.idf.il	ET SCAN NMAP -sS window 1024	1
139.162.160.132	147.237.77.74	United States	law.idf.il	ET SCAN Potential SSH Scan	1
121.223.248.67	147.237.77.19	Australia	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
115.239.251.250	147.237.76.176	China	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
61.221.69.222	147.237.76.31	Taiwan	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
45.33.124.223	147.237.76.201	United States	e.atal.idf.il	ET SCAN Potential SSH Scan	1
31.220.3.180	147.237.76.44	Belize	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
31.220.3.180	147.237.76.34	Belize	yohalan.idf.il	ET SCAN Potential SSH Scan	1
31.45.132.4	147.237.76.34	Croatia	yohalan.idf.il	ET SCAN Potential SSH Scan	1

10-03-2016-05:04:01 to 10-03-2016-06:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
207.46.13.34	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	44
188.247.78.115	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
190.190.86.72	Argentina	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
37.77.51.136	Iraq	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
177.159.154.34	Brazil	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
46.19.86.26	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
5.9.88.103	Germany	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
190.190.86.72	Argentina	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	2
24.15.66.106	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
46.19.86.216	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
184.105.139.104	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
109.67.104.115	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
62.210.243.100	France	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
216.218.206.78	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
186.237.73.31	Brazil	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	1
176.13.21.209	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
71.6.146.130	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
52.3.105.23	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
190.190.86.72	Argentina	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	1
184.105.139.116	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
109.253.158.79	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
62.210.243.100	France	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
216.218.206.86	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
46.19.86.26	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
99.113.117.5	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
52.198.122.46	Japan	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
202.226.145.18	Japan	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
184.105.247.198	United States	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
138.246.253.19	Germany	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
62.210.243.100	France	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
216.218.206.86	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
188.247.78.115	Jordan	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
184.66.2.230	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
104.162.99.64	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
52.198.122.46	Japan	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
186.237.73.31	Brazil	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
141.212.122.25	United States	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
62.210.243.100	France	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.19.86.216	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
184.105.139.86	United States	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
104.162.99.64	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
52.198.122.46	Japan	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
186.237.73.31	Brazil	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	1
141.212.122.26	United States	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
70.119.94.185	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1

10-03-2016-05:04:01 to 10-03-2016-06:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.207.207	Israel	147.237.0.19	madim.atal.idf.i	Suspicious Response Code	Block	97
2.55.151.11	Israel	147.237.77.74	law.idf.il	Unauthorized HTTP Method	Block	4
2.55.151.11	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 2.55.151.11	Block	3
2.55.151.11	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/sip_storage/files/4/	Block	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/eitan/pratim/pirteychayal/	Block	1
46.120.122.219	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 46.120.122.219	Block	1
66.249.64.99	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf	Block	1
157.55.39.196	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/valtam	Block	1
66.249.65.59	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8898-he/refuah.aspx	Block	1
180.76.15.163	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/	Block	1
66.249.65.60	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1

10-03-2016-05:04:01 to 10-03-2016-06:04:01