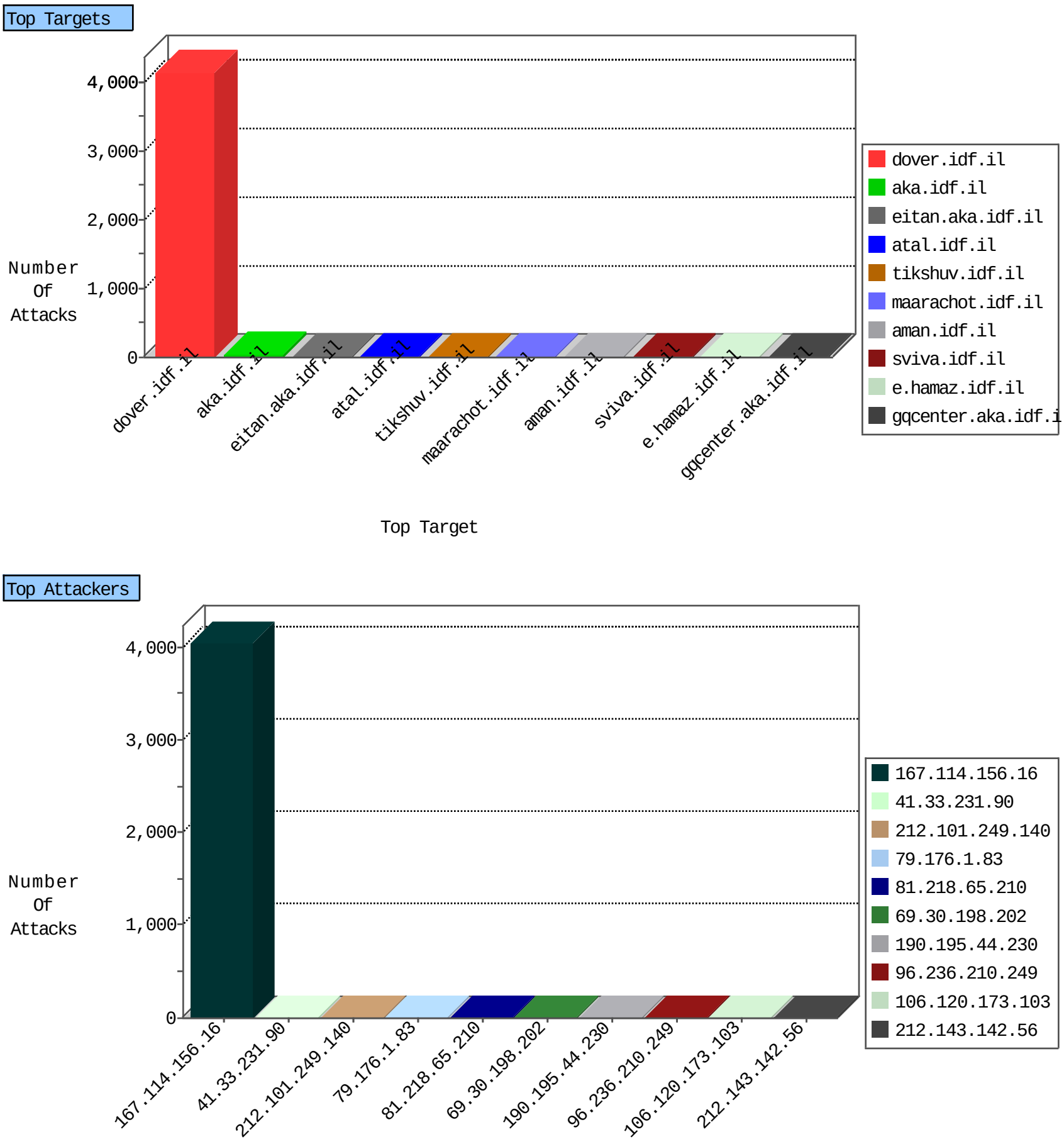
04-18-2016-03:04:07 to 04-18-2016-04:04:07

IDF Under Attack Daily Report



04-18-2016-03:04:07 to 04-18-2016-04:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	4045
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	9
184.105.139.126	United States	147.237.77.235	sviva.idf.il	Block_Udp_All_Nets	drop	1
159.122.220.135	United States	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	1
185.94.111.1	Russian Federation	147.237.8.28	e.mobile-ks.idf.il	Block_Udp_All_Nets	drop	1
159.122.220.135	United States	147.237.77.235	sviva.idf.il	Block_Ntp_All_Net	drop	1
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1

04-18-2016-03:04:07 to 04-18-2016-04:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.120.173.103	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	5
66.249.66.184	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	3
69.30.198.202	United States	147.237.76.86	navy.idf.il	C1000074: HTTP: majestic bot	Block	2
69.30.198.202	United States	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Block	2
69.30.198.202	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
69.30.198.202	United States	147.237.0.34	tikshuv.idf.il	C1000074: HTTP: majestic bot	Block	2

04-18-2016-03:04:07 to 04-18-2016-04:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	6
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.66.39	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
66.249.64.92	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
200.92.90.62	147.237.0.34	Mexico	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
185.112.248.50	147.237.76.30	United Kingdom	himush.idf.il	ET SCAN Potential SSH Scan	1
185.103.252.8	147.237.0.34	Russian Federation	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
104.232.98.38	147.237.76.177	United States	ncore.idf.il	ET SCAN NMAP -sS window 4096	1
91.201.236.155	147.237.72.156	Ukraine	aman.idf.il	ET SCAN NMAP -sS window 1024	1
204.152.218.49	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
185.103.252.8	147.237.0.35	Russian Federation	akaws.idf.il	ET SCAN Potential SSH Scan	1
185.103.252.8	147.237.0.15	Russian Federation	kosher-kravi.idf.i	ET SCAN Potential SSH Scan	1
104.219.238.10	147.237.72.14	United States	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
91.201.236.155	147.237.72.156	Ukraine	aman.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1

04-18-2016-03:04:07 to 04-18-2016-04:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.176.1.83	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	12
212.101.249.140	Lebanon	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
190.195.44.230	Argentina	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
212.101.249.140	Lebanon	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
109.64.245.234	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
73.8.28.14	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
79.178.162.95	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
89.219.32.195	Kazakstan	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
96.236.210.249	United States	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.86.6	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
178.255.215.87	France	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.228.71.191	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
141.212.122.94	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
71.6.167.142	United States	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
159.226.95.66	China	147.237.76.148	gqcenter.aka.idf.i	drop		drop	1
141.212.122.85	United States	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.82.47.51	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
185.130.5.209	Lithuania	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.197	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
168.1.6.35	Australia	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.85	United States	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.198	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
125.24.220.147	Thailand	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
74.82.47.12	United States	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
212.179.227.232	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
176.228.71.191	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.122.86	United States	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
207.5.120.21	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.206	United States	147.237.76.148	gqcenter.aka.idf.i	drop		drop	1
125.24.220.147	Thailand	147.237.77.216	dover.idf.il	Header Rejection	header rejection pattern found in request	monitor	1
74.82.47.36	United States	147.237.0.35	akaws.idf.il	drop		drop	1
212.179.227.232	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
141.212.122.93	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
141.212.122.207	United States	147.237.76.148	gqcenter.aka.idf.i	drop		drop	1
141.212.122.84	United States	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.82.47.39	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
222.73.18.162	China	147.237.0.15	kosher-kravi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

04-18-2016-03:04:07 to 04-18-2016-04:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
85.214.116.128	Germany	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 85.214.116.128	Block	3
73.153.7.140	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 73.153.7.140	Block	2
105.98.83.225	Algeria	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ar/wp-admin	Block	1
66.249.78.236	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8879-he/refuah.aspx	Block	1
220.255.148.148	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.64.234	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1236-he/atal.aspx	Block	1
141.212.122.81	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to /x	Block	1
66.249.79.105	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/3/71663.pdf	Block	1
73.153.7.140	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/mobile	Block	1
66.249.64.239	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1240-he/atal.aspx	Block	1
157.55.2.164	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
67.19.79.218	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to /robots.txt	Block	1
37.201.4.132	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/mobile	Block	1
66.249.66.121	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/4/size100x0/3044.jpg	Block	1
157.55.39.1	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	1
67.19.79.218	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to /robots.txt	Block	1
40.77.167.25	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/news/main/stm	Block	1
85.214.116.128	Germany	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-admin/	Block	1
66.249.66.125	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/6/size100x0/3426.jpg	Block	1
220.255.148.135	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
68.180.229.241	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1043-ar/cogat.aspx	Block	1
66.249.64.229	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1239-he/atal.aspx	Block	1

04-18-2016-03:04:07 to 04-18-2016-04:04:07