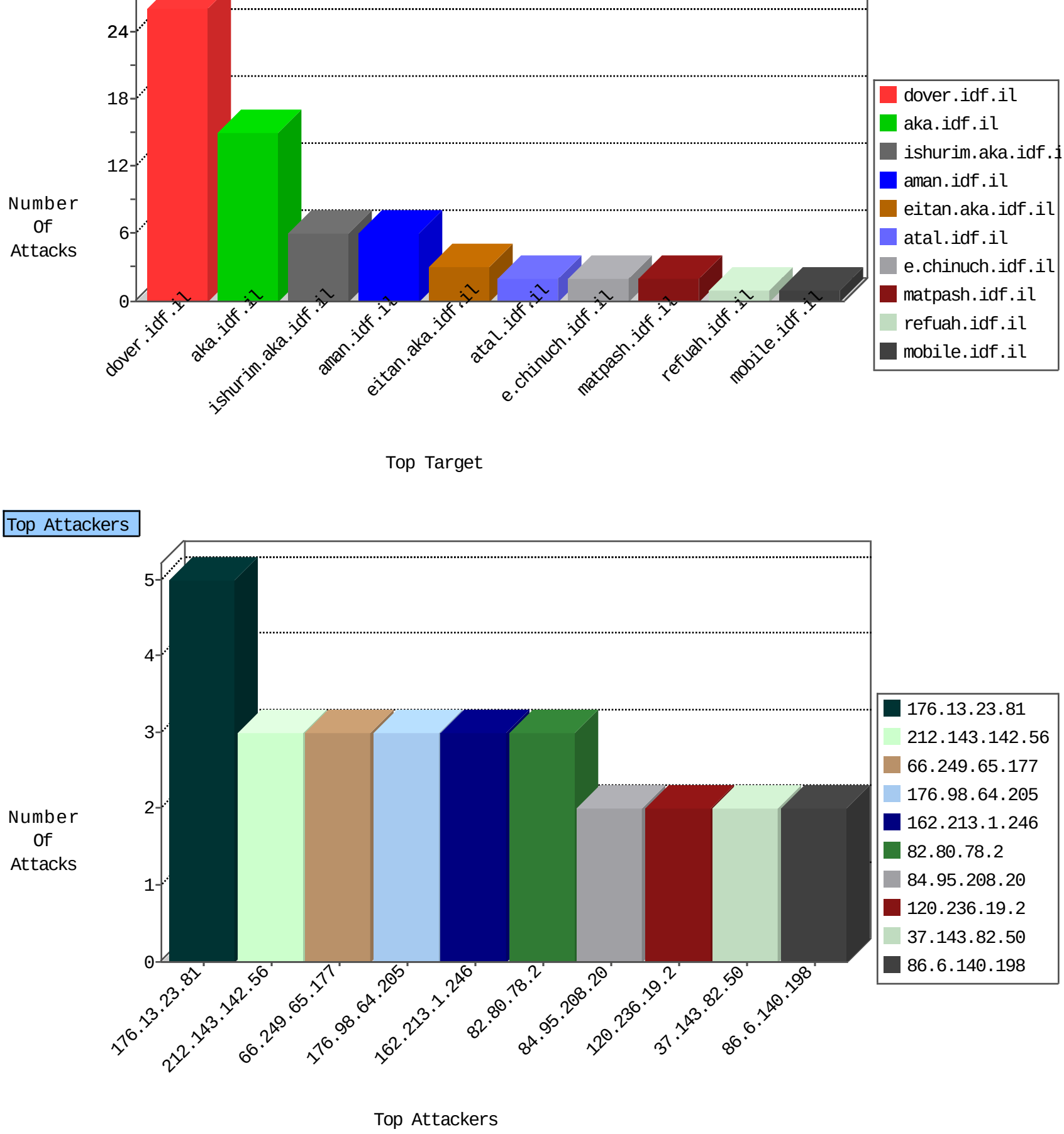
08-21-2016-04:04:05 to 08-21-2016-05:04:05

IDF Under Attack Daily Report



08-21-2016-04:04:05 to 08-21-2016-05:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.80.78.2	Israel	147.237.72.166	aka.idf.il	Black List	drop	2
93.93.101.150	Norway	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
205.132.55.27	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
93.93.101.145	Norway	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
93.93.101.152	Norway	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
205.132.55.28	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
93.93.101.148	Norway	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
93.93.101.153	Norway	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
219.106.109.190	Japan	147.237.76.147	chinuch.aka.idf.il	Black List	drop	1
93.93.101.149	Norway	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
205.132.55.25	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
82.80.78.2	Israel	147.237.77.176	matpash.idf.il	Black List	drop	1

08-21-2016-04:04:05 to 08-21-2016-05:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
164.132.161.72	Italy	147.237.76.200	eitan.aka.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
193.90.12.88	Norway	147.237.77.216	dover.idf.il	24910: HTTP: Python urllib User-Agent Header	Block	1
51.255.65.77	France	147.237.76.42	refuah.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
164.132.161.38	Italy	147.237.76.200	eitan.aka.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1

08-21-2016-04:04:05 to 08-21-2016-05:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
176.13.23.81	147.237.72.156	Israel	aman.idf.il	GPL SCAN nmap TCP	5
162.213.1.246	147.237.77.216	United States	dover.idf.il	Tehila - Perl LWP with fake user agent	3
176.98.64.205	147.237.0.34	Ukraine	tikshuv.idf.il	Xenu Link Sleuth User Agent	1
120.236.19.10	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN NMAP -f -sS	1
120.236.19.2	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN NMAP -f -sS	1
104.232.98.3	147.237.8.46	United States	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
46.228.207.18	147.237.76.201	Germany	e.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
37.143.82.50	147.237.72.167	Netherlands	ishurim.aka.idf.il	ET SCAN NMAP -f -sS	1
176.98.64.205	147.237.72.166	Ukraine	aka.idf.il	Xenu Link Sleuth User Agent	1
120.236.19.10	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN NMAP -sS window 2048	1
120.236.19.2	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN NMAP -sS window 2048	1
104.232.98.3	147.237.8.46	United States	e.chinuch.idf.il	ET SCAN NMAP -sS window 3072	1
46.228.207.18	147.237.77.19	Germany	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
37.143.82.50	147.237.72.167	Netherlands	ishurim.aka.idf.il	ET SCAN NMAP -sS window 2048	1
176.98.64.205	147.237.76.86	Ukraine	navy.idf.il	Xenu Link Sleuth User Agent	1

08-21-2016-04:04:05 to 08-21-2016-05:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
189.24.171.160	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
86.6.140.198	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
109.253.212.160	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1

08-21-2016-04:04:05 to 08-21-2016-05:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.65.177	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	3
77.138.207.46	France	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 77.138.207.46	Block	2
185.27.105.64	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
66.249.76.112	Israel	147.237.72.166	aka.idf.il	Unknown Parameter SearchParam in www.aka.idf.il/main/sachar/	None	1
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.i	Unknown Parameter tab in www.eitan.aka.idf.il/938-he/eitan.aspx	None	1
66.249.76.2	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/.well-known/apple-app-site-association	Block	1
188.120.148.235	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/	Block	1
68.180.228.231	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1934-he/cogat.aspx	Block	1
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
66.249.76.47	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/miluim1/main35cc.html	Block	1
208.115.111.71	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
66.249.64.41	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/0/17710.pdf	Block	1
87.69.66.235	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
66.249.76.48	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/miluim1/main02f1.html	Block	1
217.20.185.34	Ukraine	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
77.139.143.26	France	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 77.139.143.26	Block	1
185.27.105.64	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.76.77	Block	1
77.139.143.26	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/exampcert/	Block	1
66.249.73.137	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1

08-21-2016-04:04:05 to 08-21-2016-05:04:05