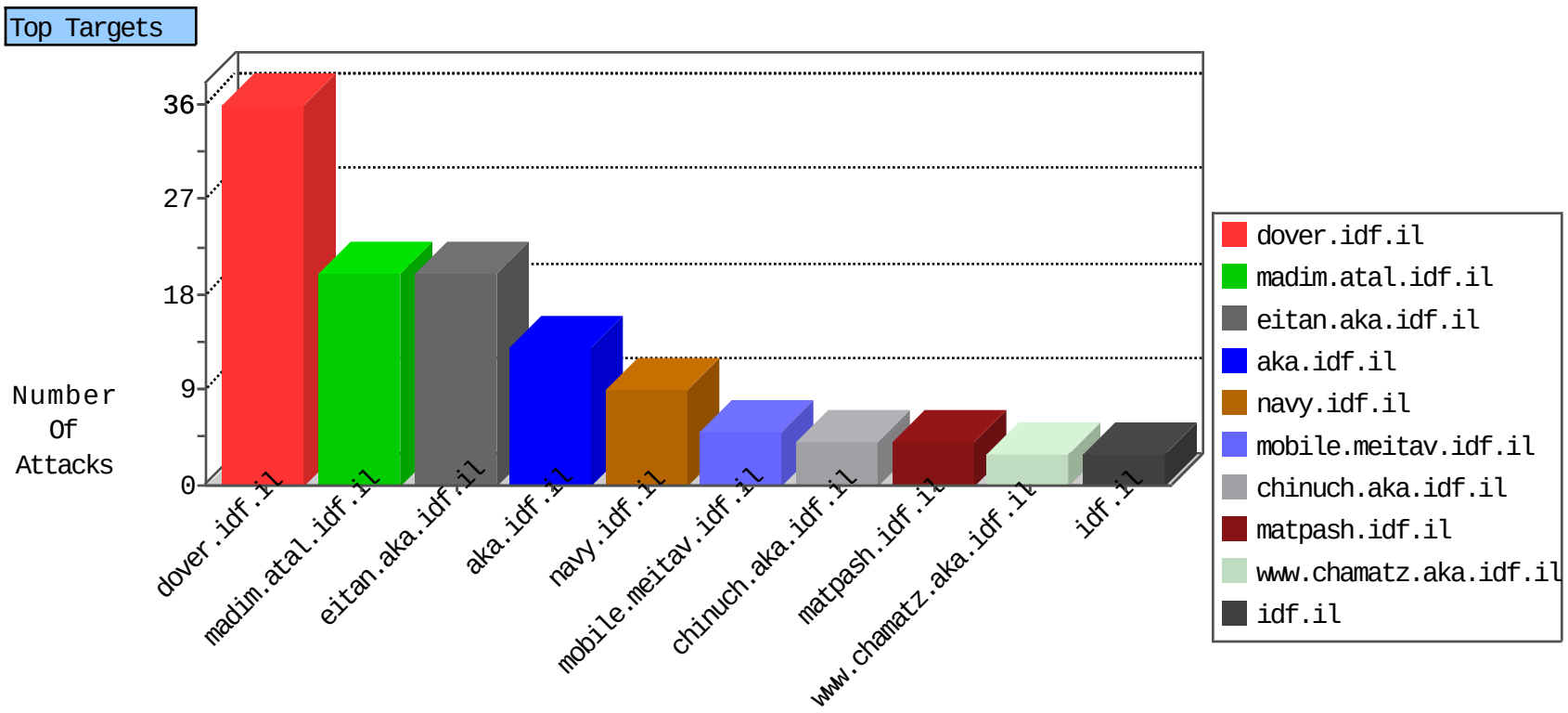
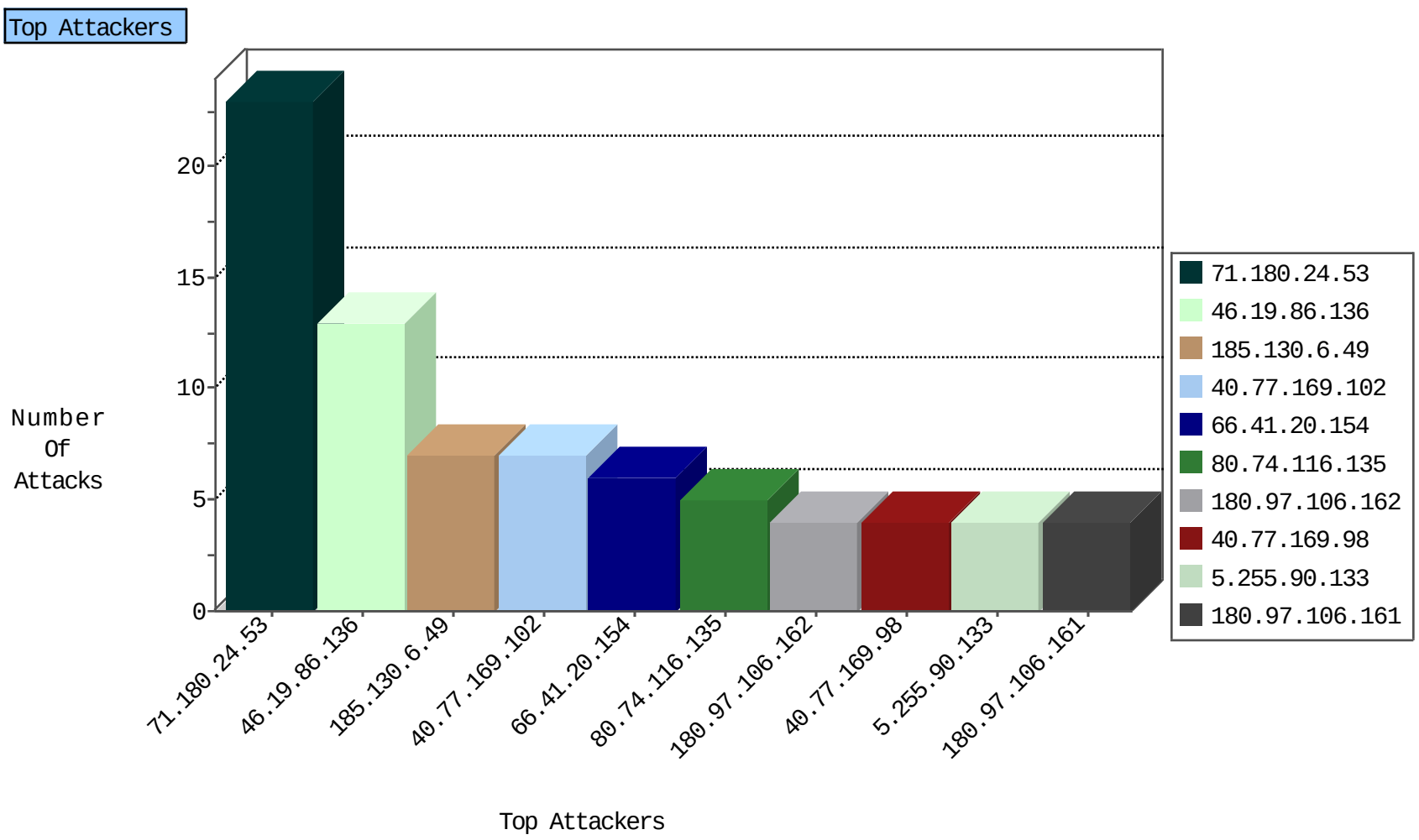
08-25-2016-06:04:01 to 08-25-2016-07:04:01

IDF Under Attack
Daily Report





08-25-2016-06:04:01 to 08-25-2016-07:04:01

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	3
104.148.55.162	United States	147.237.76.198	e.yohalan.idf.il	Black List	drop	1
93.158.200.166	Netherlands	147.237.76.34	yohalan.idf.il	Black List	drop	1
104.148.55.162	United States	147.237.76.38	e.e.meitav.idf.il	Black List	drop	1

08-25-2016-06:04:01 to 08-25-2016-07:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
71.180.24.53	United States	147.237.76.200	eitan.aka.idf.il	C1000074: HTTP: majestic bot	Permit	20
185.130.6.49	Lithuania	147.237.0.19	madim.atal.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	5
71.180.24.53	United States	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Permit	2
93.174.95.106	Netherlands	147.237.0.17	m.my-kosher-kravi.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
54.83.133.210	United States	147.237.72.156	aman.idf.il	12348: HTTP: PHP-CGI Query String Parameter Command Injection Vulnerability	Block	1
185.130.6.49	Lithuania	147.237.0.19	madim.atal.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	1
71.180.24.53	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	1

08-25-2016-06:04:01 to 08-25-2016-07:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
92.251.97.204	147.237.77.216	Malta	dover.idf.il	Xenu Link Sleuth User Agent	2
59.67.64.13	147.237.77.212	China	e.dover.idf.il	GPL SCAN nmap TCP	2
66.249.64.108	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sA (2)	1
58.218.204.245	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
203.4.240.101	147.237.0.33	Australia	idf.il	ET SCAN NMAP -sS window 1024	1
5.255.90.133	147.237.77.212	Netherlands	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
179.223.142.160	147.237.8.28	Brazil	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
5.255.90.133	147.237.77.170	Netherlands	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
133.242.3.168	147.237.76.39	Japan	mobile.meitav.idf.i	ET SCAN NMAP -sS window 1024	1
93.115.96.31	147.237.76.39	France	mobile.meitav.idf.i	ET SCAN NMAP -sS window 1024	1
91.201.236.158	147.237.72.166	Ukraine	aka.idf.il	ET SCAN NMAP -sS window 3072	1
66.249.64.124	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	1
5.255.90.133	147.237.77.233	Netherlands	atal.idf.il	ET SCAN NMAP -sS window 1024	1
185.130.6.49	147.237.0.19	Lithuania	madim.atal.idf.il	ET WEB_SERVER Muieblackcat scanner	1
5.255.90.133	147.237.77.178	Netherlands	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
133.242.4.52	147.237.76.177	Japan	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
93.115.96.31	147.237.76.39	France	mobile.meitav.idf.i	ET SCAN NMAP -sS window 2048	1
93.115.96.31	147.237.76.39	France	mobile.meitav.idf.i	ET SCAN NMAP -f -sS	1
91.201.236.158	147.237.72.166	Ukraine	aka.idf.il	ET SCAN NMAP -sS window 4096	1
91.201.236.158	147.237.0.35	Ukraine	akaws.idf.il	ET SCAN NMAP -sS window 4096	1

08-25-2016-06:04:01 to 08-25-2016-07:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
40.77.169.102	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	7
40.77.169.98	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
176.77.118.203	Russian Federation	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	3
176.9.131.69	Germany	147.237.76.147	chinuch.aka.idf.il	drop	SAM rule	drop	2
40.77.169.100	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	2
178.134.206.160	Georgia	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
180.97.106.161	China	147.237.0.17	m.my-kosher-kravi.idf.il	drop	SAM rule	drop	1
180.97.106.162	China	147.237.77.170	maarachot.idf.il	drop	SAM rule	drop	1
129.56.2.38	Nigeria	147.237.0.200	m4u.idf.il	drop		drop	1
180.97.106.161	China	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	1
74.82.47.31	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
212.143.142.44	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
180.97.106.162	China	147.237.72.166	aka.idf.il	drop	SAM rule	drop	1
89.248.174.4	Netherlands	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
180.97.106.162	China	147.237.76.39	mobile.meitav.idf.il	drop	SAM rule	drop	1
118.173.205.42	Thailand	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
40.77.169.100	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
180.97.106.162	China	147.237.77.74	law.idf.il	drop	SAM rule	drop	1
128.232.110.28	United Kingdom	147.237.0.33	idf.il	drop		drop	1

08-25-2016-06:04:01 to 08-25-2016-07:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.136	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	13
80.74.116.135	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	5
131.253.25.191	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
66.41.20.154	United States	147.237.76.86	navy.idf.il	Distributed Illegal Byte Code Character in Method	Block	1
157.55.39.198	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/robots.txt	Block	1
66.249.69.228	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.228	Block	1
40.77.169.101	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
180.97.106.161	China	147.237.76.86	navy.idf.il	Distributed NULL Character in Method	Block	1
66.41.20.154	United States	147.237.76.86	navy.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
2.53.131.35	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
178.134.206.160	Georgia	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/giyus/	Block	1
66.249.69.228	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/.well-known/apple-app-site-association	Block	1
40.77.169.103	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
208.115.111.73	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 208.115.111.73	Block	1
81.218.46.131	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.41.20.154	United States	147.237.76.86	navy.idf.il	Distributed NULL Character in Method	Block	1
40.77.167.8	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
180.97.106.37	China	147.237.76.147	chinuch.aka.idf.i	Distributed Illegal Byte Code Character in Method	Block	1
66.249.69.232	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 66.249.69.232	Block	1
208.115.111.73	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/halochamim	Block	1
66.41.20.154	United States	147.237.76.86	navy.idf.il	Illegal Byte Code Character in Header Name	Block	1
40.77.169.99	United States	147.237.77.176	matpash.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
180.97.106.37	China	147.237.76.147	chinuch.aka.idf.i	Distributed NULL Character in Method	Block	1
66.249.69.232	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/.well-known/assetlinks.json	Block	1
66.41.20.154	United States	147.237.76.86	navy.idf.il	Abnormally Long Request method	Block	1
157.55.39.37	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/print_bottom.asp	Block	1
66.41.20.154	United States	147.237.76.86	navy.idf.il	Illegal HTTP Version	Block	1
40.77.169.99	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
180.97.106.161	China	147.237.76.86	navy.idf.il	Distributed Illegal Byte Code Character in Method	Block	1
66.249.75.64	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19369-he/idfgdover.aspx	Block	1

08-25-2016-06:04:01 to 08-25-2016-07:04:01