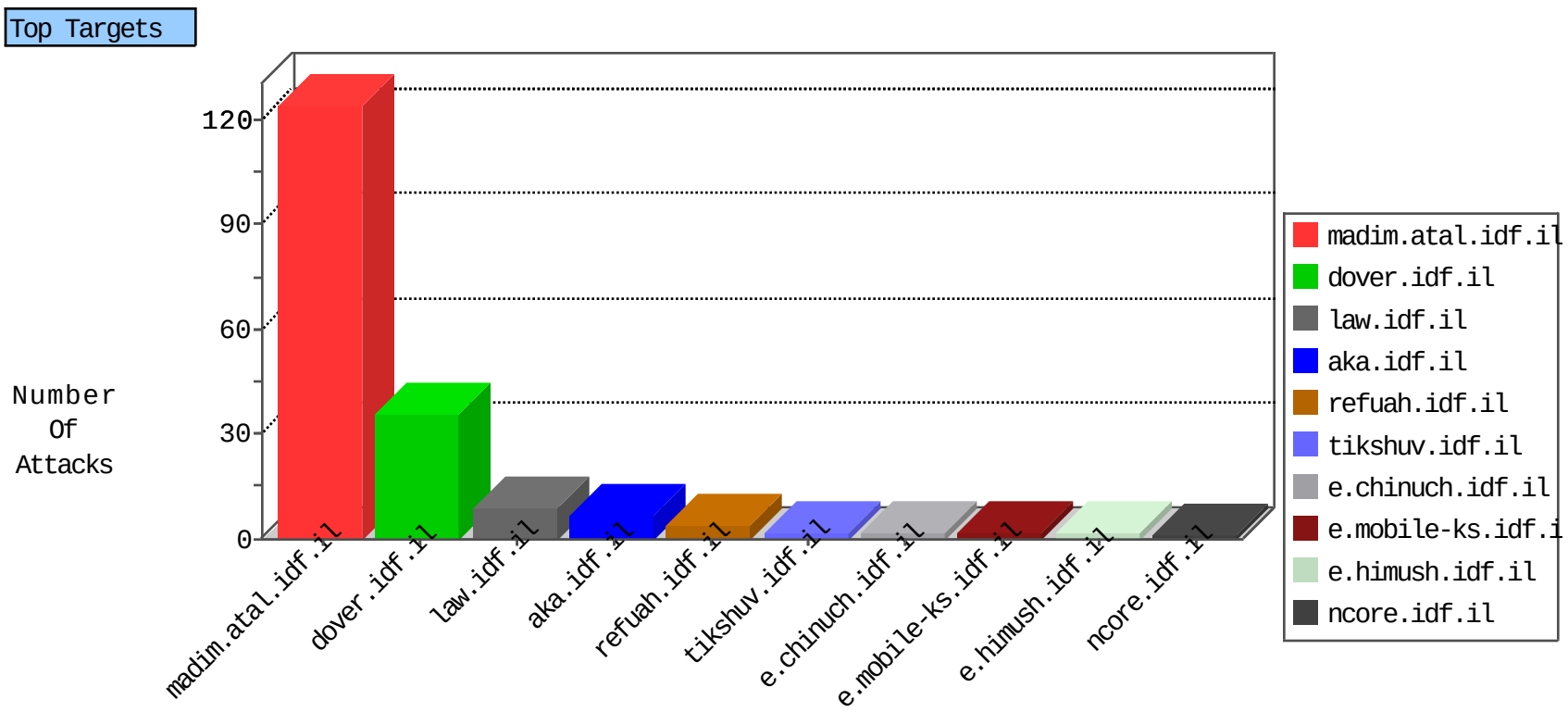
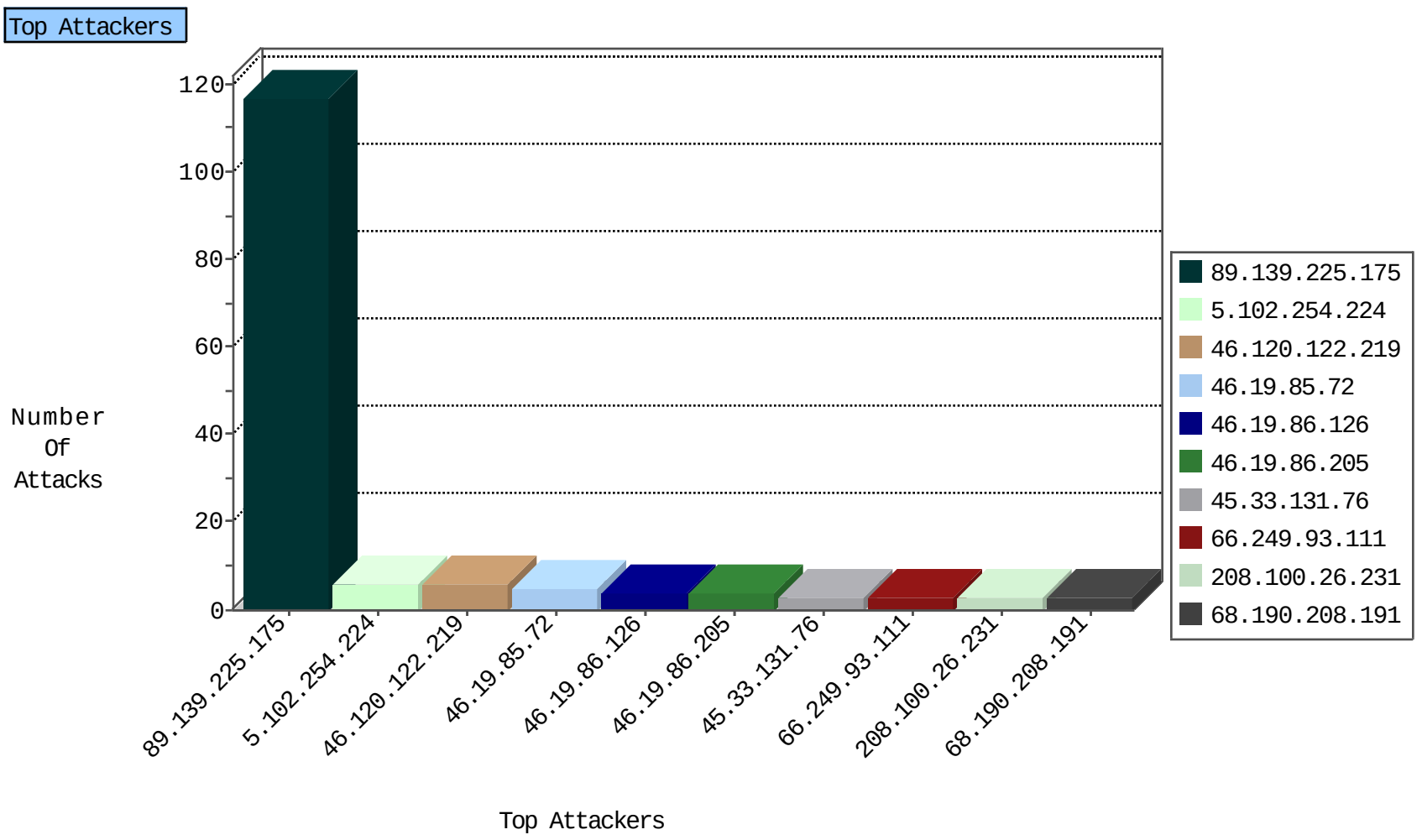
09-04-2016-01:05:54 to 09-04-2016-02:05:54

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-04-2016-01:05:54 to 09-04-2016-02:05:54

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.240.236.119	United States	147.237.76.199	e.nakchal.idf.il	Black List	drop	1
115.230.125.146	China	147.237.77.216	dover.idf.il	block-sp-traf1	forward	1

09-04-2016-01:05:54 to 09-04-2016-02:05:54

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

09-04-2016-01:05:54 to 09-04-2016-02:05:54

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.120.122.219	147.237.77.74	Israel	law.idf.il	Xenu Link Sleuth User Agent	6
5.102.254.224	147.237.77.216	Israel	dover.idf.il	GPL SCAN myscan	3
5.102.254.224	147.237.77.216	Israel	dover.idf.il	INDICATOR-SCAN myscan	3
68.190.208.191	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sS window 4096	1
208.100.26.231	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
68.190.208.191	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -f -sS	1
196.47.173.21	147.237.8.46	Cote D'Ivoire	e.chinuch.idf.il	ET SCAN NMAP -sS window 4096	1
5.255.90.133	147.237.76.177	Netherlands	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
193.36.35.241	147.237.77.176	Russian Federation	matpash.idf.il	ET SCAN Potential SSH Scan	1
157.157.107.4	147.237.77.216	Iceland	dover.idf.il	ET SCAN NMAP -sS window 4096	1
116.12.175.233	147.237.76.197	Singapore	e.himush.idf.il	ET SCAN NMAP -sS window 3072	1
94.102.48.195	147.237.76.86	Netherlands	navy.idf.il	ET SCAN NMAP -sS window 1024	1
79.177.209.208	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
71.86.124.86	147.237.8.28	United States	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 3072	1
68.190.208.191	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sS window 2048	1
208.100.26.228	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
196.47.173.21	147.237.8.46	Cote D'Ivoire	e.chinuch.idf.il	ET SCAN NMAP -sS window 3072	1
181.55.122.110	147.237.76.34	Colombia	yohalan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
116.12.175.233	147.237.76.197	Singapore	e.himush.idf.il	ET SCAN NMAP -sS window 4096	1
95.42.13.239	147.237.8.28	Bulgaria	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
87.236.194.161	147.237.8.14	Czech Republic	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
77.138.52.97	147.237.77.216	France	dover.idf.il	portscan: TCP Distributed Portscan	1

09-04-2016-01:05:54 to 09-04-2016-02:05:54

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.19.86.205	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
66.249.93.111	Europe	147.237.77.216	dover.idf.il	drop	SAM rule	drop	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
37.26.148.199	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
46.19.85.239	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
84.108.71.42	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	1
46.19.86.56	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
109.253.136.108	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
46.19.86.107	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1

09-04-2016-01:05:54 to 09-04-2016-02:05:54

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
89.139.225.175	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	117
46.19.85.72	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
45.33.131.76	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	3
2.53.152.38	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
157.55.39.221	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.76.83	Block	2
31.210.187.1	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/templates/oprolescategory/oprolescategory.in.aspx	Block	2
77.138.14.140	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar	Block	2
208.100.26.231	United States	147.237.76.42	refuah.idf.il	Unauthorized Method OPTIONS for /	Block	1
66.249.66.177	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
46.19.86.126	Israel	147.237.77.216	dover.idf.il	Abnormally Long Request method	Block	1
213.151.35.212	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/rabanut/general.aspx	Block	1
66.249.66.241	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/templates/shared/usercontrols/navmenu/undefined	Block	1
23.92.21.19	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/eitan/pratim/pirteyerua/	Block	1
207.46.13.90	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
46.19.86.126	Israel	147.237.77.216	dover.idf.il	Illegal HTTP Version	Block	1
217.132.25.211	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
207.46.13.134	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.134	Block	1
46.19.86.126	Israel	147.237.77.216	dover.idf.il	Malformed URL http/1.1	Block	1
208.100.26.231	United States	147.237.76.42	refuah.idf.il	Unauthorized HTTP Method	Block	1
46.19.86.126	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method /Shared/datepicker.css in URL www.idf.ilhttp/1.1	Block	1

09-04-2016-01:05:54 to 09-04-2016-02:05:54