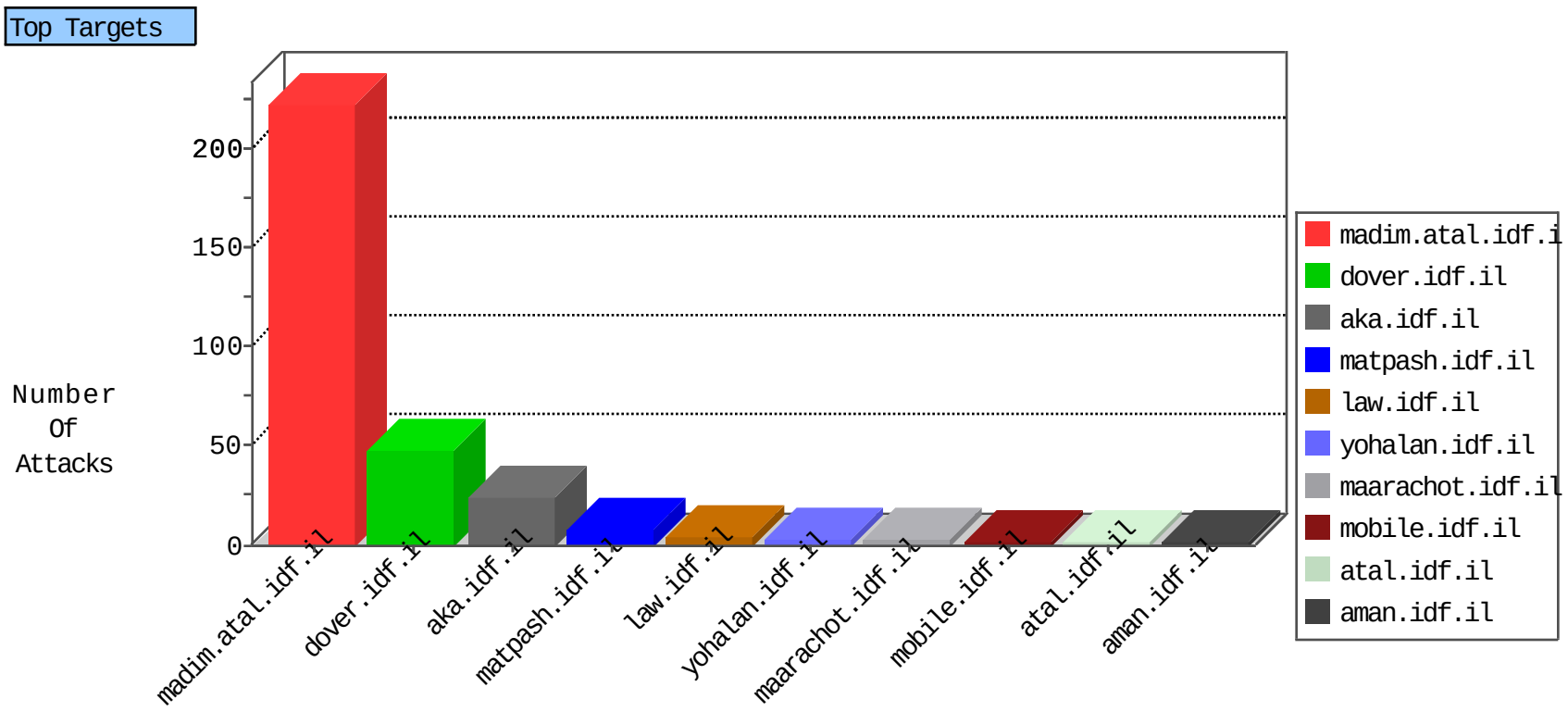
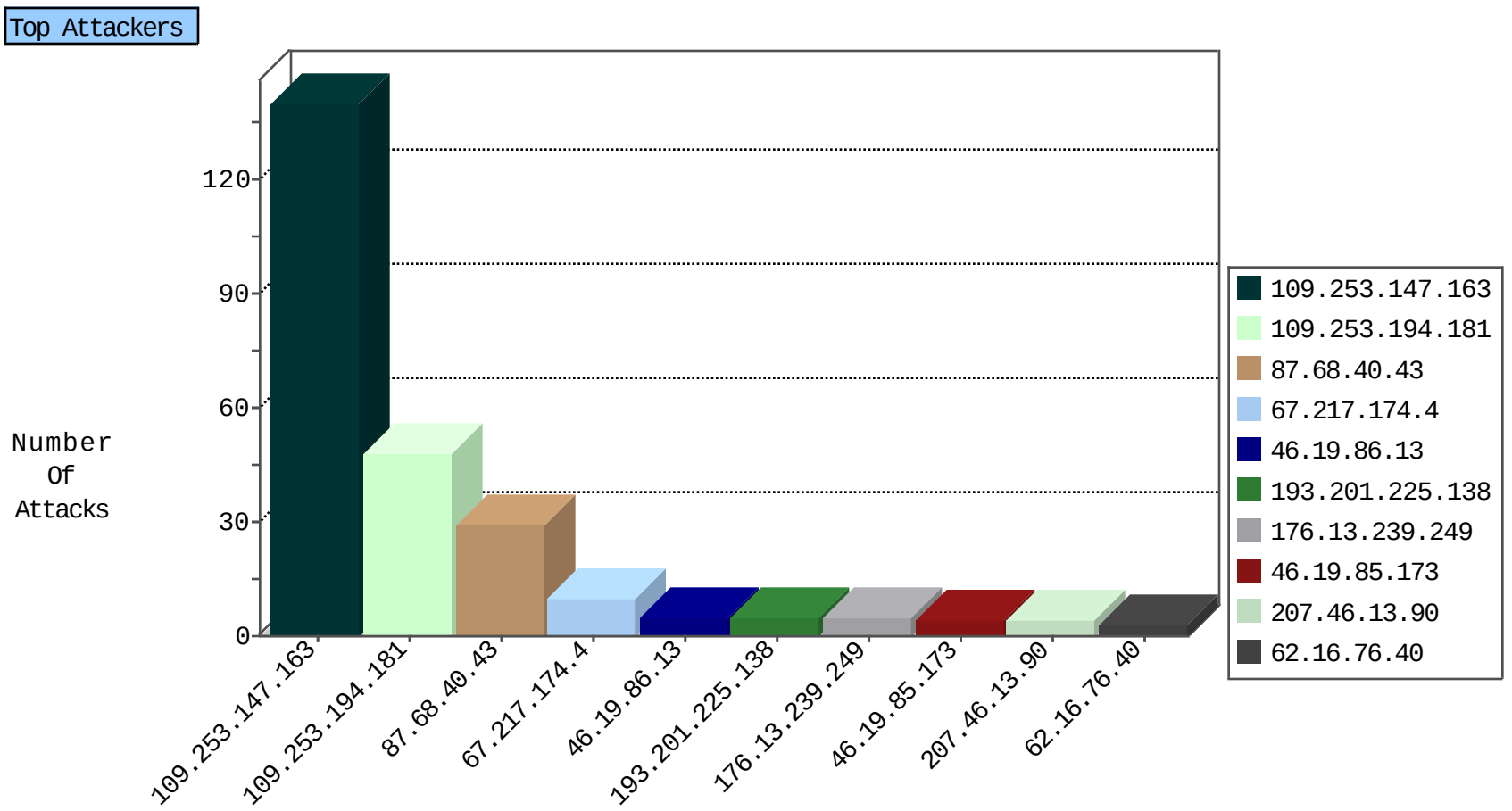
09-02-2016-20:04:00 to 09-02-2016-21:04:00

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-02-2016-20:04:00 to 09-02-2016-21:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
8.37.225.230	United States	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	3
193.111.60.251	Ukraine	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
203.166.137.12	Singapore	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
203.166.137.11	Singapore	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2

09-02-2016-20:04:00 to 09-02-2016-21:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

09-02-2016-20:04:00 to 09-02-2016-21:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
193.201.225.138	147.237.77.178	Ukraine	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
193.201.225.138	147.237.76.197	Ukraine	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
176.13.235.136	147.237.76.86	Israel	navy.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
104.197.206.193	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sS window 2048	1
103.207.37.81	147.237.77.74	Vietnam	law.idf.il	ET SCAN NMAP -sS window 1024	1
46.227.67.172	147.237.77.234	Sweden	halag.idf.il	ET SCAN NMAP -sS window 1024	1
46.227.67.172	147.237.77.179	Sweden	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
198.52.97.94	147.237.77.74	United States	law.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	1
193.201.225.138	147.237.77.216	Ukraine	dover.idf.il	ET SCAN NMAP -sS window 1024	1
193.201.225.138	147.237.77.176	Ukraine	matpash.idf.il	ET SCAN Potential SSH Scan	1
179.104.210.96	147.237.76.31	Brazil	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
104.197.206.193	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sS window 3072	1
104.197.206.193	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -f -sS	1
66.249.76.119	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
46.227.67.172	147.237.77.233	Sweden	atal.idf.il	ET SCAN NMAP -sS window 1024	1
208.100.26.228	147.237.72.167	United States	ishurim.aka.idf.i	ET SCAN NMAP -sS window 1024	1
5.255.90.133	147.237.72.156	Netherlands	aman.idf.il	ET SCAN NMAP -sS window 1024	1
193.201.225.138	147.237.77.227	Ukraine	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1

09-02-2016-20:04:00 to 09-02-2016-21:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
67.217.174.4	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
176.13.239.249	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
46.19.86.13	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.173	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
66.249.81.230	Europe	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	3
62.16.76.40	Russian Federation	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
91.121.116.113	France	147.237.77.74	law.idf.il	drop	SAM rule	drop	2
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
109.253.201.139	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
66.249.76.115	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
79.177.163.79	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
216.243.31.2	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
109.253.219.126	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	1
66.249.81.227	Israel	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	1
183.129.160.229	China	147.237.76.198	e.yohalan.idf.il	drop	SAM rule	drop	1
216.243.31.2	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
141.212.122.16	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
183.129.160.229	China	147.237.76.199	e.nakchal.idf.il	drop	SAM rule	drop	1
109.253.139.102	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.31	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
207.46.13.90	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
109.253.157.224	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
64.95.102.36	United States	147.237.0.35	akaws.idf.il	drop		drop	1
176.13.236.224	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1

09-02-2016-20:04:00 to 09-02-2016-21:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.147.163	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	139
109.253.194.181	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	48
87.68.40.43	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	29
77.127.82.114	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
207.46.13.90	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
37.26.149.132	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
54.240.196.171	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
66.249.81.212	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
77.139.241.56	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/rabanut/general.aspx	Block	1
66.249.76.75	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.76.75	Block	1
24.64.110.244	Canada	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/navmenu/mazi.idf.il	Block	1
109.253.132.72	Israel	147.237.77.233	atal.idf.il	Parameter Type Violation search in atal.idf.il/1440-he/atal.aspx	Block	1
66.249.81.215	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
54.240.196.186	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
136.179.21.76	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	1
80.11.241.108	France	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	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
66.249.81.218	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.64.9	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/miluim/templates/inner.asp	Block	1
207.46.13.77	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-18630-he/dover.aspx„'ƒ„'„,¬¯„ƒλ€Š„,¬¿„ƒ„'©'½„,¬Š€λƒ„'„,¬¯„ƒλ€Š„,¬¿„ƒ„'™½„,¬Š€λƒ„'„,¬¯„ƒλ€Š„,¬¿„ƒλ€Š„,¬½,	Block	1
80.14.201.115	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/favicon.ico	Block	1
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/daily_	Block	1
109.253.147.163	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	1
66.249.69.72	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1394-he/refuah.aspx	Block	1
84.109.72.253	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/registrationwizard/step4.aspx	Block	1
66.249.76.119	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
54.240.196.185	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
109.253.158.99	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-he/dover.aspx	Block	1
77.138.133.62	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/news.aspx	Block	1
66.249.76.71	Israel	147.237.0.19	madim.atal.idf.i	Unauthorized URL Access to madim.atal.idf.il/robots.txt	Block	1
54.240.196.185	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1

09-02-2016-20:04:00 to 09-02-2016-21:04:00