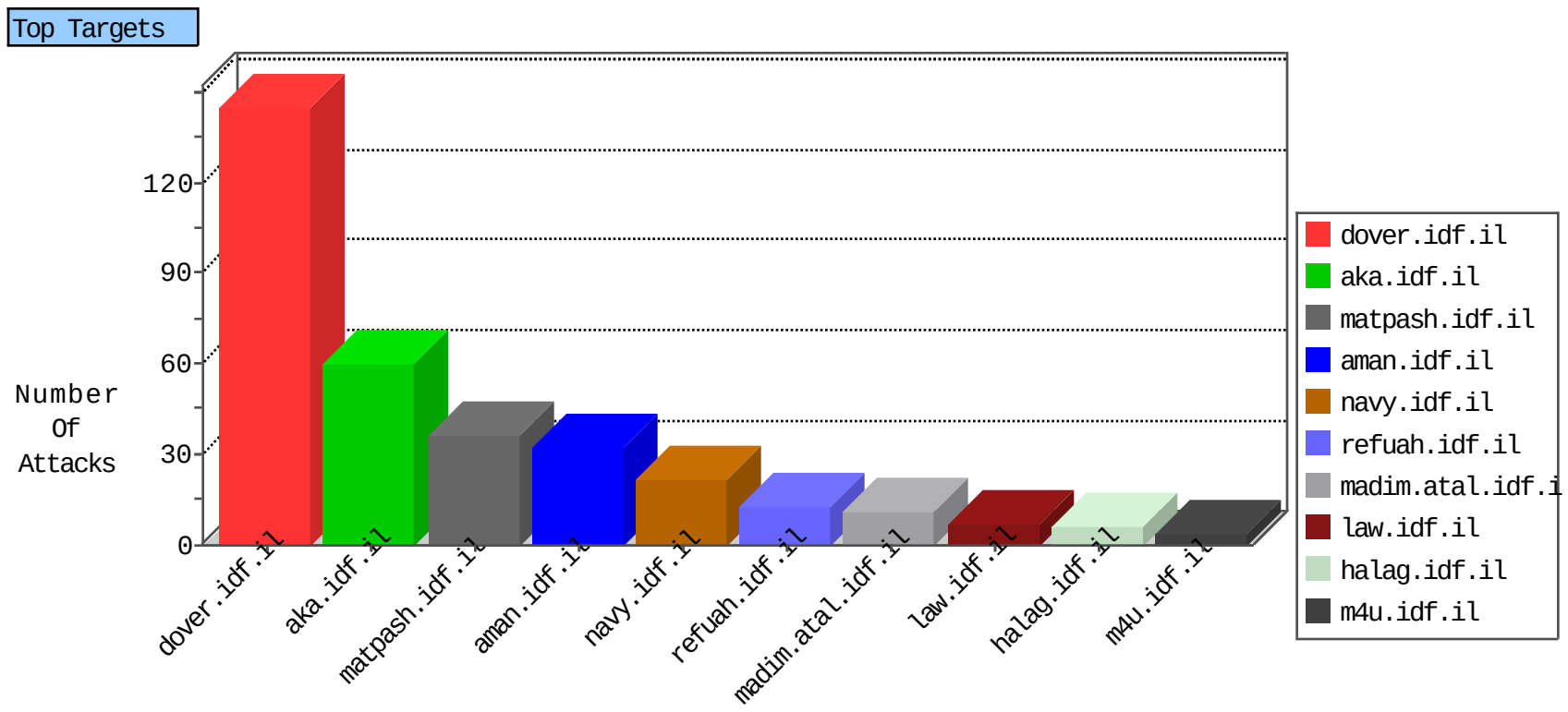
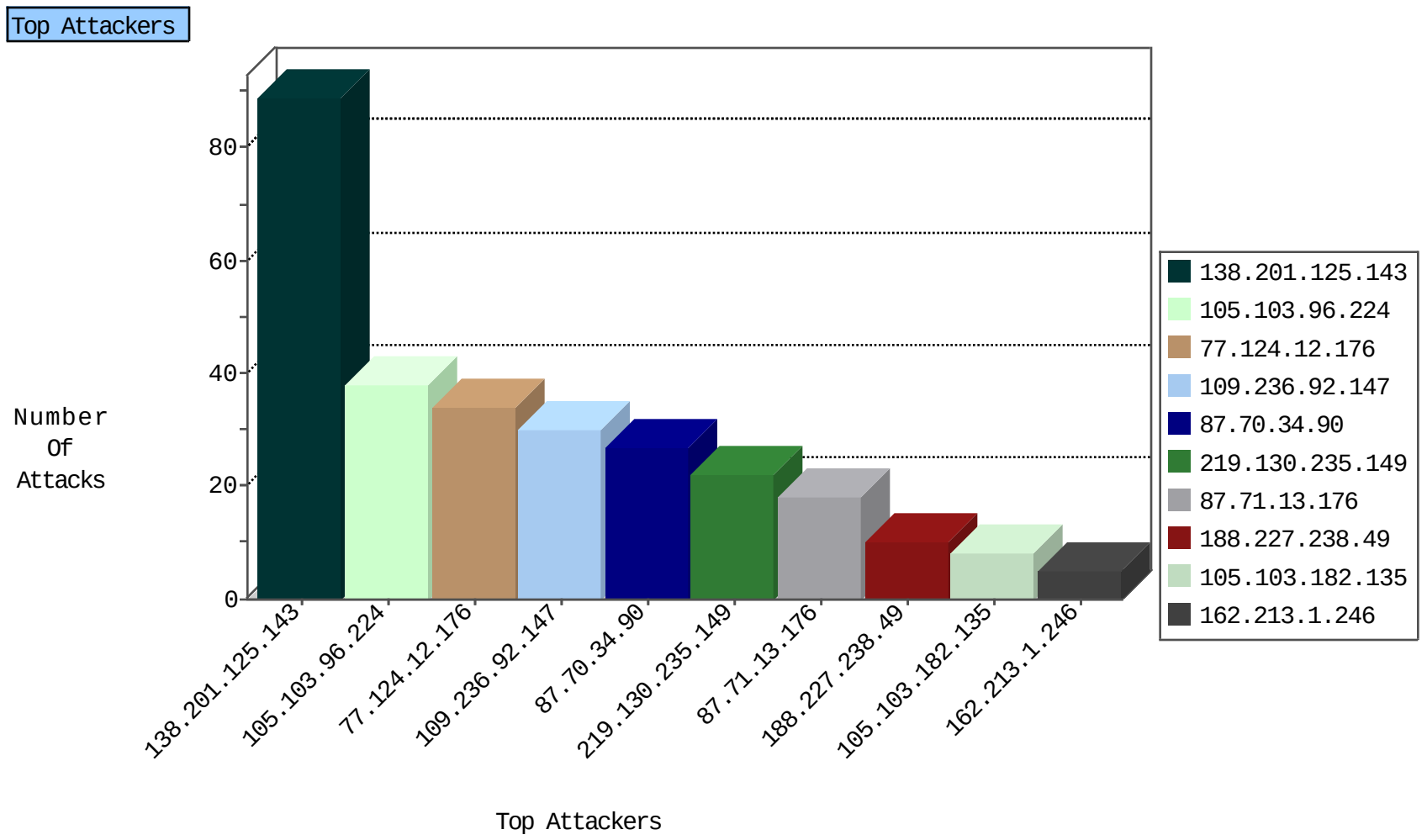
08-20-2016-12:04:08 to 08-20-2016-13:04:08

IDF Under Attack Daily Report

Top Targets



Top Attackers



08-20-2016-12:04:08 to 08-20-2016-13:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.80.78.2	Israel	147.237.77.176	matpash.idf.il	Black List	drop	1
93.174.93.156	Netherlands	147.237.76.148	gqcenter.aka.idf.il	Black List	drop	1
185.94.111.1	Russian Federation	147.237.76.38	e.e.meitav.idf.il	Black List	drop	1

08-20-2016-12:04:08 to 08-20-2016-13:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
138.201.125.143	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	34
138.201.125.143	Germany	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Permit	31
138.201.125.143	Germany	147.237.76.42	refuah.idf.il	C1000074: HTTP: majestic bot	Permit	12
138.201.125.143	Germany	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Permit	7
105.103.96.224	Algeria	147.237.77.216	dover.idf.il	3886: HTTP: Cross Site Scripting in POST Request	Block	4
138.201.125.143	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	3
138.201.125.143	Germany	147.237.76.31	nakchal.idf.il	C1000074: HTTP: majestic bot	Permit	2
105.103.182.135	Algeria	147.237.77.216	dover.idf.il	0361: HTTP: Protected File Access (/etc/passwd)	Block	1
62.212.73.211	Netherlands	147.237.76.42	refuah.idf.il	C1000074: HTTP: majestic bot	Permit	1
105.103.182.135	Algeria	147.237.77.216	dover.idf.il	19690: HTTP: Microsoft IIS Integer Overflow Vulnerability	Block	1
62.212.73.211	Netherlands	147.237.77.233	atal.idf.il	C1000074: HTTP: majestic bot	Permit	1
105.103.182.135	Algeria	147.237.77.216	dover.idf.il	2809: HTTP: IIS TRACK Method	Block	1
62.212.73.211	Netherlands	147.237.77.234	halag.idf.il	C1000074: HTTP: majestic bot	Permit	1

08-20-2016-12:04:08 to 08-20-2016-13:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
162.213.1.246	147.237.77.216	United States	dover.idf.il	Tehila - Perl LWP with fake user agent	5
5.135.165.89	147.237.77.176	France	matpash.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
105.103.96.224	147.237.77.216	Algeria	dover.idf.il	ET WEB_SERVER IIS 8.3 Filename With Wildcard (Possible File/Dir Bruteforce)	2
46.60.106.224	147.237.77.176	Palestinian Territory, Occupied	matpash.idf.il	ET SCAN NMAP -sA (2)	1
120.237.232.6	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	1
120.237.232.6	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
105.103.182.135	147.237.77.216	Algeria	dover.idf.il	SERVER-WEBAPP TRACE attempt	1
105.103.182.135	147.237.77.216	Algeria	dover.idf.il	ET DOS SSL Bomb DoS Attempt	1
104.232.98.3	147.237.77.121	United States	e.navy.idf.il	ET SCAN NMAP -sS window 3072	1
190.196.178.78	147.237.77.233	Chile	atal.idf.il	ET SCAN NMAP -sS window 3072	1
104.232.98.3	147.237.77.121	United States	e.navy.idf.il	ET SCAN NMAP -f -sS	1
177.200.192.50	147.237.0.200	Brazil	m4u.idf.il	ET SCAN NMAP -sS window 2048	1
91.201.236.50	147.237.0.200	Ukraine	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.64.249	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sA (2)	1
148.245.192.248	147.237.0.15	Mexico	kosher-kravi.idf.i	ET SCAN NMAP -sS window 1024	1
24.105.159.242	147.237.76.148	United States	gqcenter.aka.idf.i	ET SCAN NMAP -sS window 1024	1
120.237.232.6	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
120.237.232.6	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
105.103.182.135	147.237.77.216	Algeria	dover.idf.il	GPL WEB_SERVER /etc/passwd	1
190.196.178.78	147.237.77.233	Chile	atal.idf.il	ET SCAN NMAP -sS window 4096	1
104.232.98.3	147.237.77.121	United States	e.navy.idf.il	ET SCAN NMAP -sS window 2048	1
179.43.141.228	147.237.77.235	Switzerland	sviva.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.50	147.237.0.200	Ukraine	m4u.idf.il	ET SCAN NMAP -sS window 3072	1
177.200.192.50	147.237.0.200	Brazil	m4u.idf.il	ET SCAN NMAP -f -sS	1
82.81.90.6	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
152.169.248.125	147.237.8.27	Argentina	e.madim.atal.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

08-20-2016-12:04:08 to 08-20-2016-13:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
109.236.92.147	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
77.124.12.176	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	18
87.70.34.90	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	18
77.124.12.176	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	16
105.103.96.224	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
87.71.13.176	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
188.227.238.49	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
87.70.34.90	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	9
87.71.13.176	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	6
66.249.93.107	Europe	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
38.111.147.86	United States	147.237.77.216	dover.idf.il	drop		drop	2
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
109.253.157.122	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	2
182.64.197.173	India	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
216.243.31.2	United States	147.237.0.35	akaws.idf.il	drop		drop	1
216.243.31.2	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
192.168.173.102		147.237.77.216	dover.idf.il	drop		drop	1
66.249.81.230	Israel	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	1
216.243.31.2	United States	147.237.0.33	idf.il	drop		drop	1

08-20-2016-12:04:08 to 08-20-2016-13:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
219.130.235.149	China	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 219.130.235.149	Block	15
105.103.96.224	Algeria	147.237.77.216	dover.idf.il	Unauthorized HTTP Method	Block	8
105.103.96.224	Algeria	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 105.103.96.224	Block	7
219.130.235.149	China	147.237.76.86	navy.idf.il	PHP Attempt	Block	6
46.19.85.35	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
176.13.236.97	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
31.154.9.46	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
105.103.182.135	Algeria	147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	2
77.139.73.244	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/main/	Block	2
79.177.247.238	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/size100x0/sip_storage	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
74.91.23.166	United States	147.237.72.167	ishurim.aka.idf.i	Unauthorized URL Access to 147.237.72.167/	Block	1
46.19.86.3	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
84.111.138.183	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
66.249.76.70	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/.well-known/apple-app-site-association	Block	1
105.103.96.224	Algeria	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ar/*~1*\a.aspx	Block	1
74.91.23.166	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
66.102.9.85	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/pniotanswer.aspx	Block	1
185.120.125.21	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
105.103.96.224	Algeria	147.237.77.216	dover.idf.il	Illegal Byte Code Character in URL /ar/#012ns:netsparker056650=vuln	Block	1
66.249.76.75	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
37.142.10.244	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
219.130.235.149	China	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/index.asp	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/9/71769.doc	Block	1
207.46.13.9	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
105.103.96.224	Algeria	147.237.77.216	dover.idf.il	Multiple Illegal Byte Code Character in URL from 105.103.96.224	Block	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/1/69681.pdf	Block	1
37.142.217.160	Israel	147.237.72.156	aman.idf.il	Unauthorized HTTP Method	Block	1
109.253.158.204	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
66.249.66.177	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.66.177	Block	1
217.132.146.204	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
109.253.202.156	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
82.145.218.251	Europe	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/main/home/default.aspx	Block	1
66.249.76.70	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.76.70	Block	1

08-20-2016-12:04:08 to 08-20-2016-13:04:08