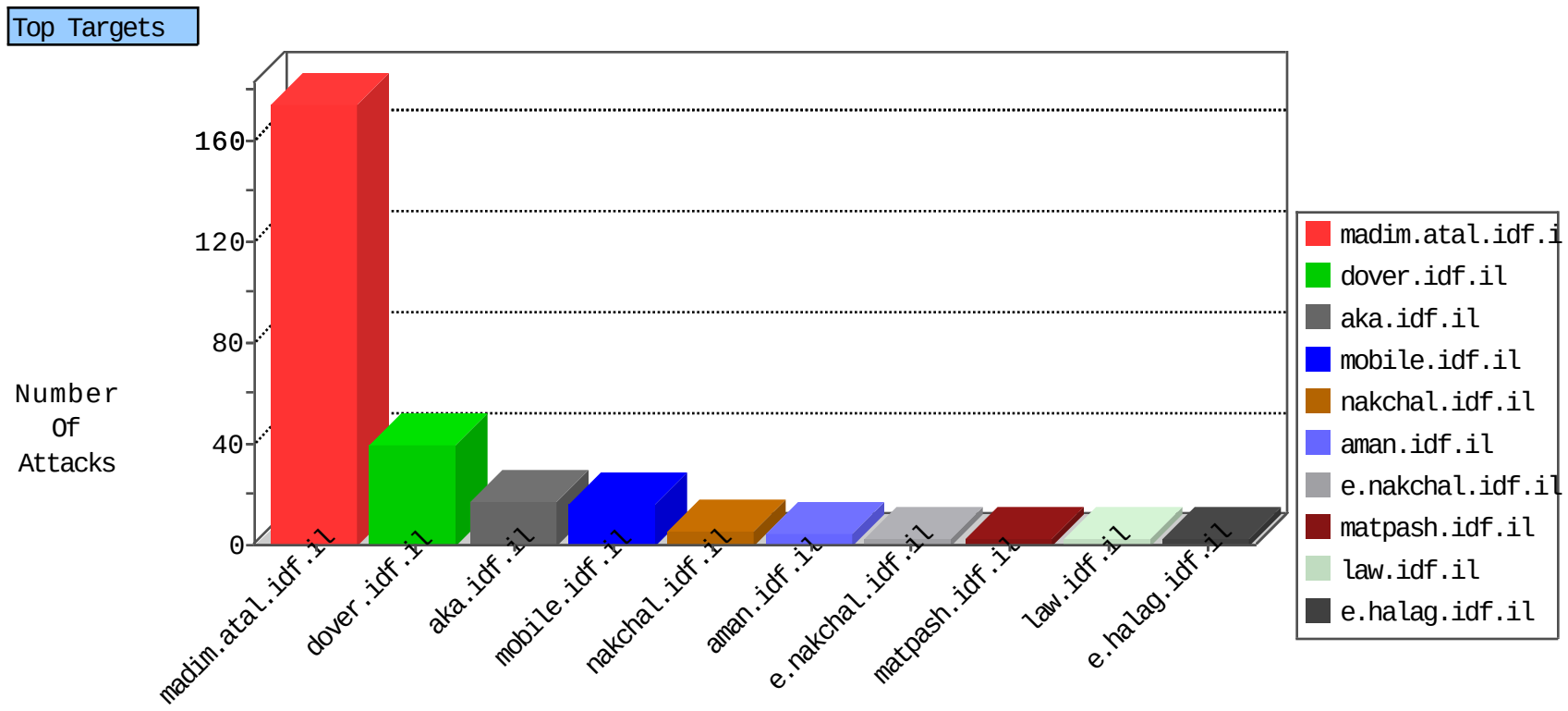
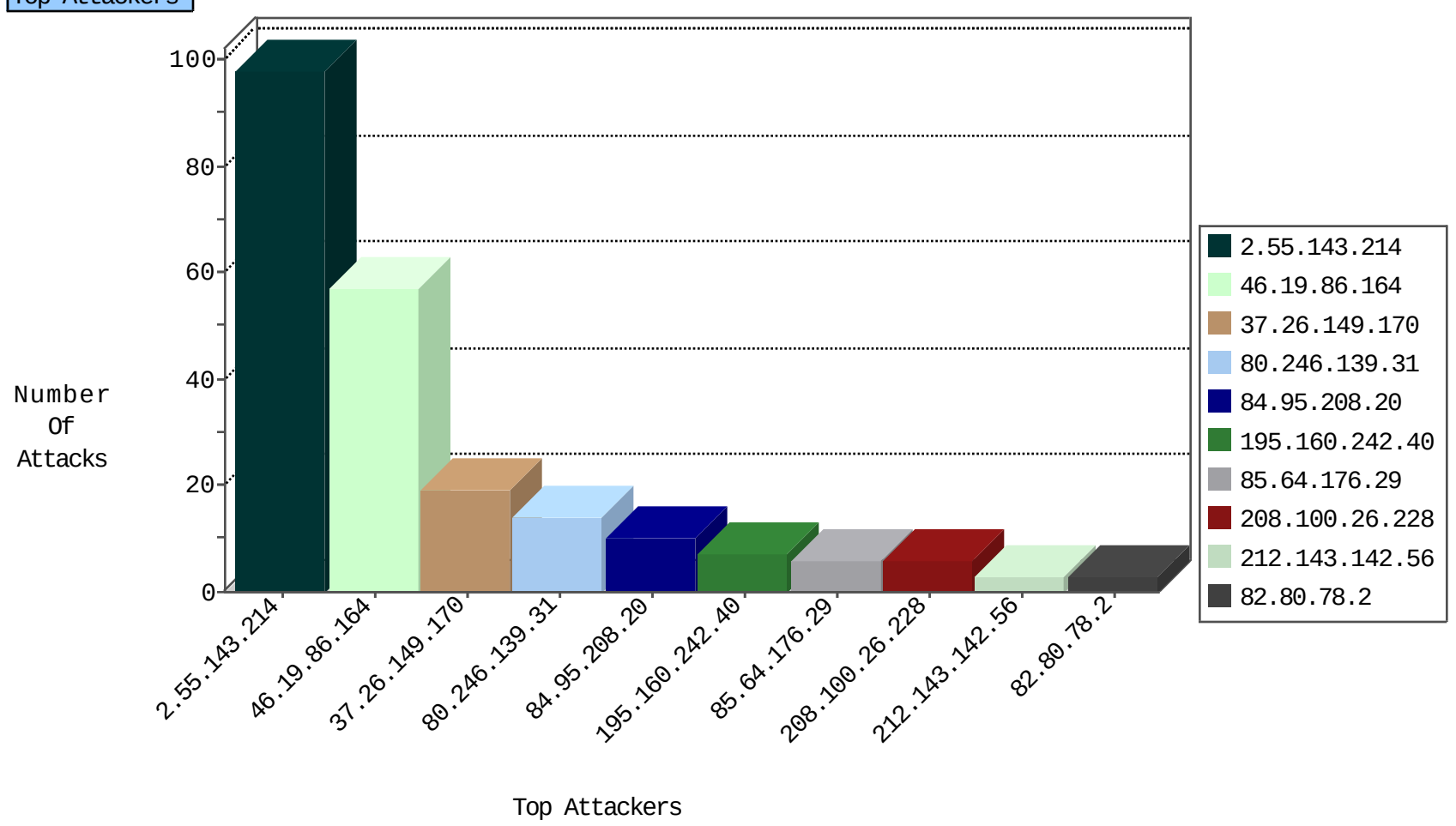
08-18-2016-08:04:06 to 08-18-2016-09:04:06

IDF Under Attack Daily Report

Top Targets



Top Attackers



08-18-2016-08:04:06 to 08-18-2016-09:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.80.78.2	Israel	147.237.77.216	dover.idf.il	Black List	drop	2
208.100.26.228	United States	147.237.76.199	e.nakchal.idf.il	Black List	drop	1
208.100.26.228	United States	147.237.76.177	ncore.idf.il	Black List	drop	1
208.100.26.228	United States	147.237.76.200	eitan.aka.idf.il	Black List	drop	1
85.173.79.57	Russian Federation	147.237.76.31	nakchal.idf.il	Black List	drop	1
208.100.26.228	United States	147.237.76.196	e.sviva.idf.il	Black List	drop	1
208.100.26.228	United States	147.237.76.202	e.halag.idf.il	Black List	drop	1
85.173.79.57	Russian Federation	147.237.76.34	yohalan.idf.il	Black List	drop	1
208.100.26.228	United States	147.237.76.197	e.himush.idf.il	Black List	drop	1
82.80.78.2	Israel	147.237.72.166	aka.idf.il	Black List	drop	1
91.92.120.134	Bulgaria	147.237.76.202	e.halag.idf.il	Black List	drop	1

08-18-2016-08:04:06 to 08-18-2016-09:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
162.210.196.129	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
93.174.95.106	Netherlands	147.237.72.156	aman.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
36.110.147.74	China	147.237.77.74	law.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1
89.248.172.16	Netherlands	147.237.77.179	e.mazi.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

08-18-2016-08:04:06 to 08-18-2016-09:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
219.68.160.114	147.237.76.39	Taiwan	mobile.meitav.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
194.90.239.2	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.118.65.230	147.237.0.16	Russian Federation	my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
173.208.249.37	147.237.76.31	United States	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.195	147.237.77.178	Netherlands	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
80.178.190.33	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.86	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.76.98.38	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
191.17.7.101	147.237.76.201	Brazil	e.atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
179.192.5.177	147.237.76.199	Brazil	e.nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
113.108.10.31	147.237.8.27	China	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
86.126.162.98	147.237.0.33	Romania	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
62.90.219.142	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

08-18-2016-08:04:06 to 08-18-2016-09:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
195.160.242.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
93.173.57.62	Israel	147.237.72.166	aka.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	3
37.26.146.233	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
176.13.241.133	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	1
176.13.249.43	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	1
176.13.4.121	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	1
180.97.106.162	China	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	1
176.13.8.50	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	1
180.97.106.162	China	147.237.76.176	test.ncore.idf.il	drop	SAM rule	drop	1
176.13.230.233	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
185.130.6.49	Lithuania	147.237.0.200	m4u.idf.il	drop		drop	1
62.219.137.27	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	1

08-18-2016-08:04:06 to 08-18-2016-09:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.55.143.214	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	98
46.19.86.164	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	57
37.26.149.170	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	19
80.246.139.31	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 80.246.139.31	Block	14
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	10
85.64.176.29	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	6
169.253.194.1	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 169.253.194.1	Block	1
204.79.180.165	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
87.71.39.90	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/newsarchive.aspx	Block	1
66.249.66.183	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1384-11005-he/dover.aspx	Block	1
169.253.194.1	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/9/4629.jpg	Block	1
212.150.125.195	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/994-7237-he/atal.aspx	Block	1
104.173.254.180	United States	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
77.138.22.177	France	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
176.13.231.127	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/894-he/nakhal.aspx	Block	1
212.150.178.32	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
109.253.136.176	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
77.138.22.177	France	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/kapatz/relativecontact.aspx	Block	1
2.55.7.219	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catId in www.aka.idf.il/main/giyus/main/giyus/resources/images/master/favicon.gif	None	1
185.32.179.12	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
87.70.247.126	Israel	147.237.76.31	nakchal.idf.il	Distributed PHP Attempt	Block	1
66.102.9.95	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/0218-	Block	1
77.139.125.122	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/default.aspx	Block	1
2.55.35.8	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
192.243.55.129	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/228-he/faq.aspx	Block	1
87.70.247.126	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/wp-login.php	Block	1
66.249.66.177	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1

08-18-2016-08:04:06 to 08-18-2016-09:04:06