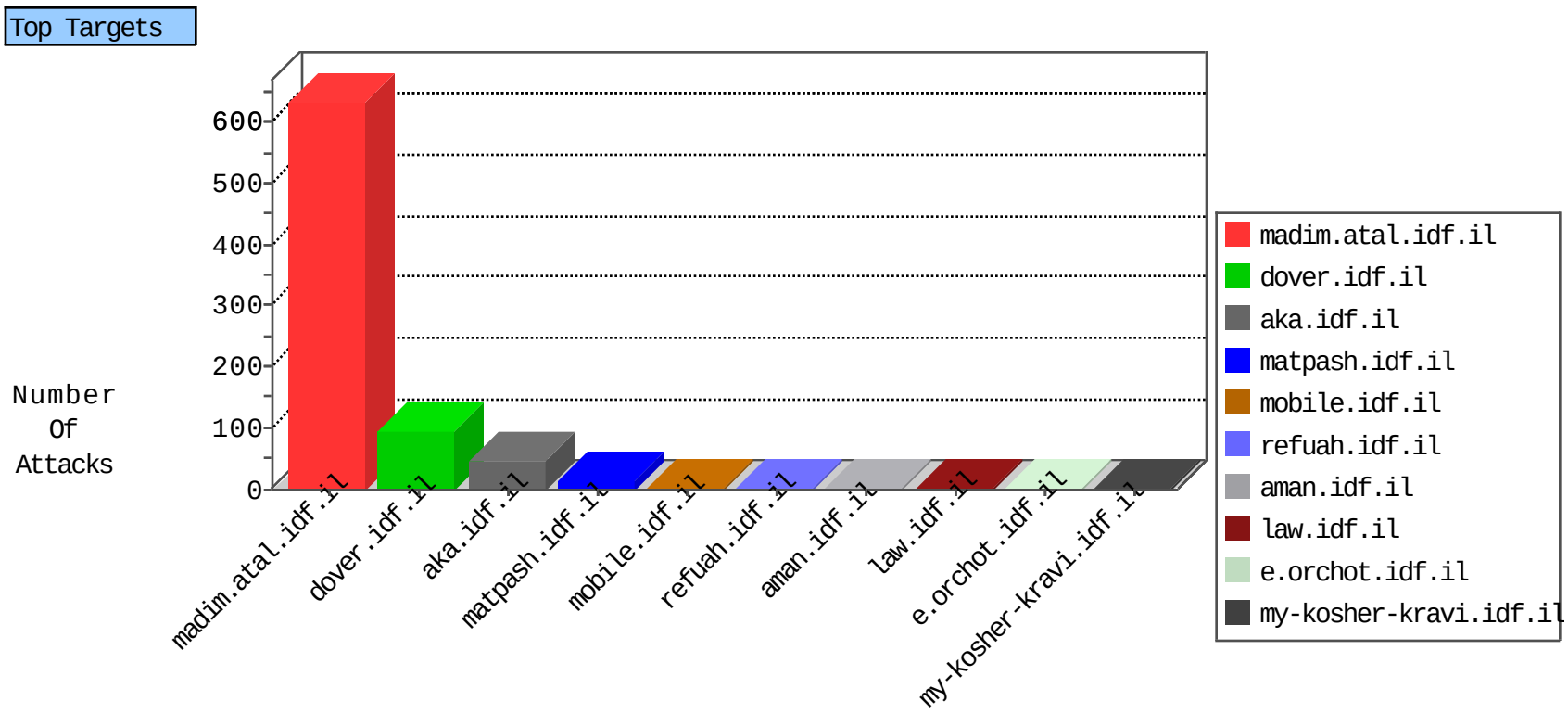
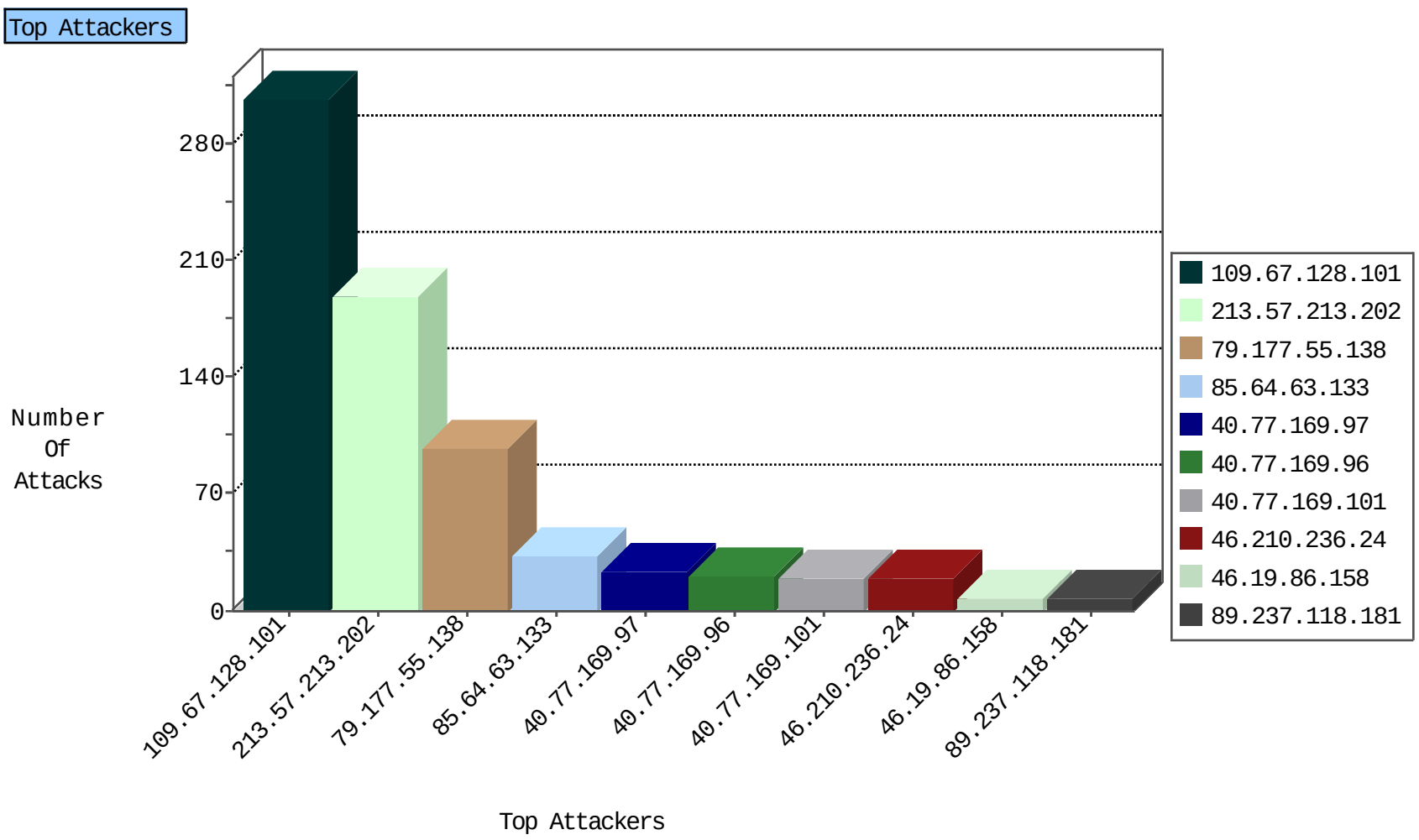
08-25-2016-23:04:08 to 08-26-2016-00:04:08

IDF Under Attack Daily Report

Top Targets



Top Attackers



08-25-2016-23:04:08 to 08-26-2016-00:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	4
109.226.40.40	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
120.132.50.135	China	147.237.72.166	aka.idf.il	block-sp-traf1	forward	2

08-25-2016-23:04:08 to 08-26-2016-00:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
83.149.126.98	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
83.149.126.98	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2

08-25-2016-23:04:08 to 08-26-2016-00:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
203.4.240.101	147.237.77.205	Australia	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
201.238.202.219	147.237.76.39	Chile	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
180.97.106.37	147.237.77.234	China	halag.idf.il	ET SCAN Potential SSH Scan	1
180.97.75.130	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
133.208.21.66	147.237.77.74	Japan	law.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.50	147.237.8.14	Ukraine	e.orchot.idf.il	ET SCAN NMAP -sS window 3072	1
91.201.236.50	147.237.8.14	Ukraine	e.orchot.idf.il	ET SCAN NMAP -f -sS	1
2.53.48.136	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
203.4.240.101	147.237.77.179	Australia	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
191.109.137.126	147.237.76.31	Colombia	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
180.97.106.37	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
163.172.169.150	147.237.76.31	United Kingdom	nakchal.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
109.186.87.188	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.201.236.50	147.237.8.14	Ukraine	e.orchot.idf.il	ET SCAN NMAP -sS window 2048	1
54.79.2.19	147.237.76.42	Australia	refuah.idf.il	ET SCAN NMAP -sS window 1024	1

08-25-2016-23:04:08 to 08-26-2016-00:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
40.77.169.97	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	24
40.77.169.96	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	20
46.210.236.24	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
40.77.169.101	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	13
89.237.118.181	France	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
109.253.204.3	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
40.77.169.101	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	4
40.77.169.101	United States	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
92.40.248.106	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
40.77.169.103	United States	147.237.76.86	navy.idf.il	drop	SAM rule	drop	2
216.243.31.2	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
169.229.3.91	United States	147.237.8.46	e.chinuch.idf.il	drop	SAM rule	drop	1
183.129.160.229	China	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	1
109.253.210.204	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.76.147	chinuch.aka.idf.il	drop	SAM rule	drop	1
80.178.208.214	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
183.129.160.229	China	147.237.77.234	halag.idf.il	drop	SAM rule	drop	1
133.208.21.66	Japan	147.237.76.34	yohalan.idf.il	drop		drop	1
169.229.3.91	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	1
192.116.111.159	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.0.16	my-kosher-kravi.idf.il	drop	SAM rule	drop	1
169.229.3.91	United States	147.237.77.233	atal.idf.il	drop	SAM rule	drop	1
169.229.3.91	United States	147.237.8.28	e.mobile-ks.idf.il	drop	SAM rule	drop	1
176.13.232.189	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.67.128.101	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	300
213.57.213.202	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	189
79.177.55.138	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	97
85.64.63.133	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	33
46.19.86.158	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1674	Block	3
2.55.0.195	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.158	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
213.57.57.27	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
131.253.27.148	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
84.108.235.7	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
178.165.130.24	Austria	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
40.77.169.100	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
79.177.228.222	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
109.253.131.79	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
2.53.21.12	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
77.139.123.165	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/haredim/general.aspx	Block	2
178.165.128.17	Austria	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
178.165.128.17	Austria	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/kapatz/	Block	2
79.179.149.53	Israel	147.237.77.170	maarachot.idf.il	PHP Attempt	Block	1
66.102.9.85	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
40.77.169.98	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
46.19.86.158	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 46.19.86.158	Block	1
79.179.149.53	Israel	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
66.249.69.14	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/doctrine/doctrine.stm"	Block	1
141.226.242.160	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$employmentStatus in www.aka.idf.il/main/sachar/payslips.aspx	None	1
84.169.244.100	Germany	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
178.165.130.24	Austria	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012 ources/images/innerpage/goback.gif	Block	1
109.67.144.252	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
79.179.149.53	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
77.125.14.149	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
40.77.169.104	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
157.55.39.93	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_pictures.asp	Block	1
79.178.44.134	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/images/shared/mailthis.gif	Block	1
178.165.130.24	Austria	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/	Block	1
61.141.94.157	China	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
80.178.208.214	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.19.86.92	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
109.64.170.173	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
79.179.149.53	Israel	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 79.179.149.53	Block	1
207.46.13.89	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/robots.txt	Block	1
61.141.94.157	China	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 61.141.94.157	Block	1
109.253.201.184	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
81.18.218.190	Poland	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/favicon.ico	Block	1
77.139.225.127	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/cityofficers	Block	1
109.65.78.123	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1

08-25-2016-23:04:08 to 08-26-2016-00:04:08