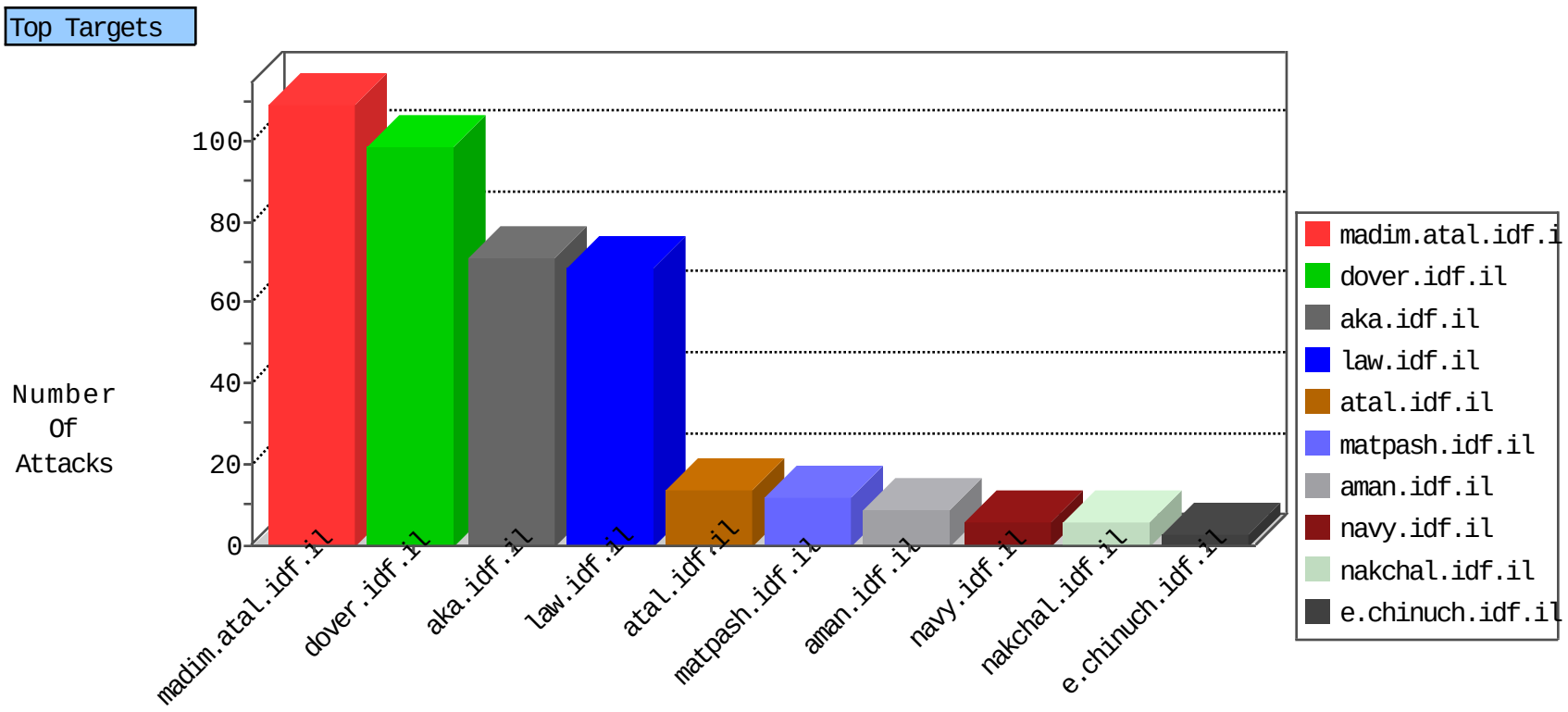
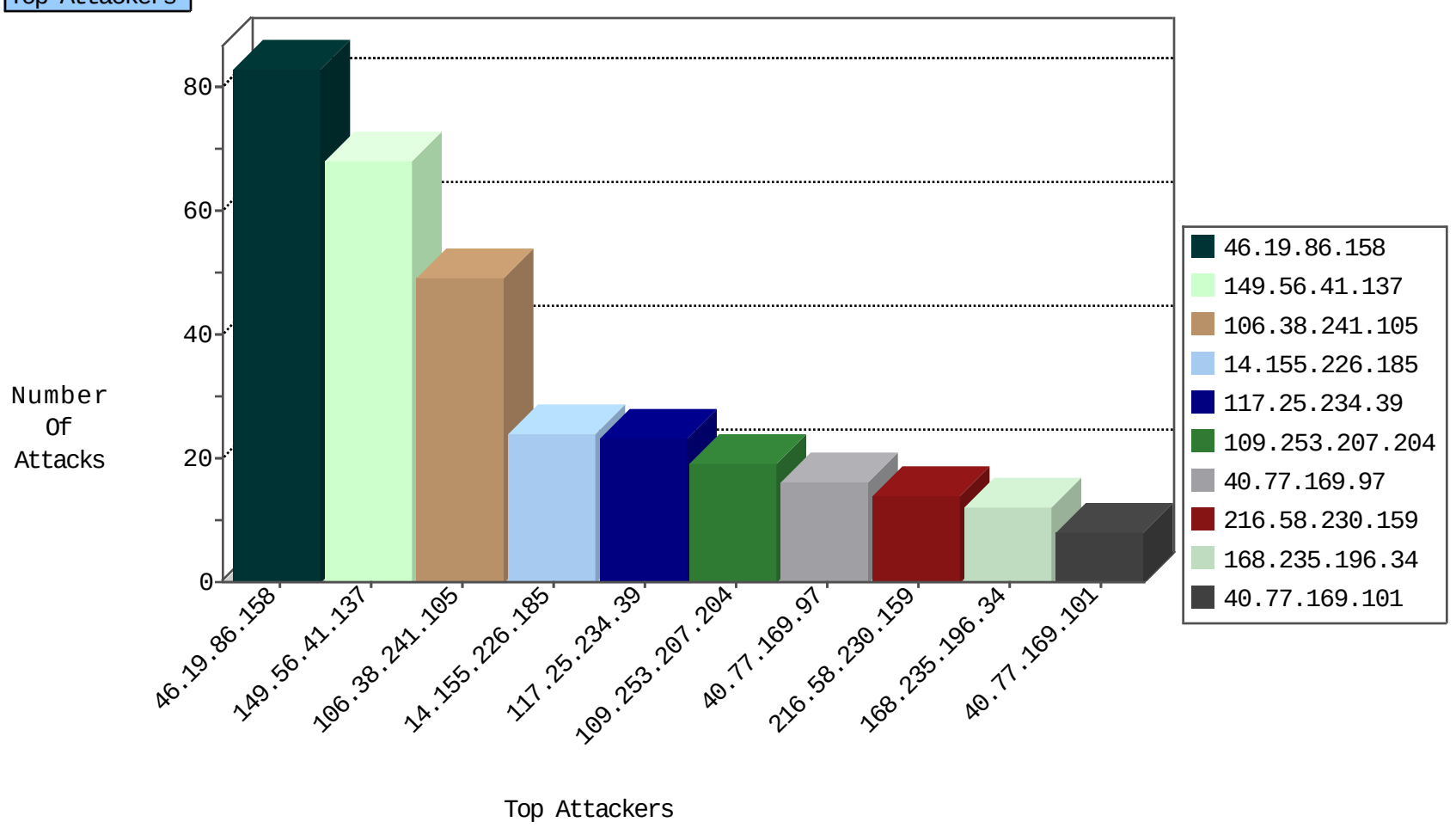
08-23-2016-07:04:04 to 08-23-2016-08:04:04

IDF Under Attack Daily Report

Top Targets



Top Attackers



08-23-2016-07:04:04 to 08-23-2016-08:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
168.235.196.34	United States	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	83
149.56.41.137	United States	147.237.77.74	law.idf.il	HTTP-Misc-BadBlue-Dir-Trave-2	dest-reset	3
110.82.201.182	China	147.237.77.226	www.chamatz.aka.idf.il	Frk_Under_Attack_Con_Tcp	drop	2
115.230.125.146	China	147.237.77.216	dover.idf.il	block-sp-traf1	forward	1
52.28.32.164	Germany	147.237.76.198	e.yohalan.idf.il	JLM_Purple_Con_Limit_Https	drop	1
52.28.32.164	Germany	147.237.76.202	e.halag.idf.il	JLM_Purple_Con_Limit_Https	drop	1

08-23-2016-07:04:04 to 08-23-2016-08:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.105	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	30
106.38.241.105	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	19
216.58.230.159	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
164.132.161.63	Italy	147.237.77.74	law.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1

08-23-2016-07:04:04 to 08-23-2016-08:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
149.56.41.137	147.237.77.74	United States	law.idf.il	Tehila - Perl LWP with fake user agent	54
216.58.230.159	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	8
162.213.1.246	147.237.77.216	United States	dover.idf.il	Tehila - Perl LWP with fake user agent	5
84.109.180.213	147.237.77.170	Israel	maarachot.idf.il	Xenu Link Sleuth User Agent	2
149.56.41.137	147.237.77.74	United States	law.idf.il	ET WEB_SERVER Exploit Suspected PHP Injection Attack (cmd=)	2
91.201.236.158	147.237.8.46	Ukraine	e.chinuch.idf.il	ET SCAN NMAP -f -sS	1
87.236.194.161	147.237.72.14	Czech Republic	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
65.156.199.242	147.237.77.178	United States	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
58.218.204.245	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
97.79.244.122	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sS window 1024	1
91.224.160.131	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.158	147.237.8.46	Ukraine	e.chinuch.idf.il	ET SCAN NMAP -sS window 2048	1
91.201.236.155	147.237.77.227	Ukraine	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
58.218.204.245	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.195	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.158	147.237.8.46	Ukraine	e.chinuch.idf.il	ET SCAN NMAP -sS window 4096	1

08-23-2016-07:04:04 to 08-23-2016-08:04:04

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	11
197.25.106.154	Tunisia	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
85.130.191.104	Israel	147.237.76.31	nakchal.idf.il	drop	First packet isn't SYN	drop	6
40.77.169.97	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	5
40.77.169.101	United States	147.237.76.86	navy.idf.il	drop	SAM rule	drop	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
40.77.169.102	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	5
193.43.246.250	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
40.77.169.98	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	4
40.77.169.101	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	3
79.181.29.180	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	3
40.77.169.102	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	3
176.13.6.134	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
131.108.75.254	Brazil	147.237.76.34	yohalan.idf.il	drop		drop	1
40.77.169.100	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	1
52.28.32.164	Germany	147.237.76.34	yohalan.idf.il	drop		drop	1
52.28.32.164	Germany	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
176.13.227.88	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
176.13.229.197	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
185.103.12.66	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1

08-23-2016-07:04:04 to 08-23-2016-08:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.158	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	83
109.253.207.204	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	19
14.155.226.185	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 14.155.226.185	Block	17
117.25.234.39	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 117.25.234.39	Block	16
14.155.226.185	China	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	6
117.25.234.39	China	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	5
149.56.41.137	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/sip_storage/files/4/304.pdf&amp	Block	5
5.29.25.5	Israel	147.237.72.156	aman.idf.il	Unauthorized HTTP Method	Block	4
80.246.136.47	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
95.35.173.136	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
66.249.76.35	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.76.35	Block	2
66.249.76.31	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/.well-known/assetlinks.json	Block	1
199.30.17.48	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
117.25.234.39	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/index.asp	Block	1
69.169.43.8	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
40.77.169.103	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
180.76.15.144	China	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/list5.htm	Block	1
208.115.111.73	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/kamlar/news/סטודנ על אף שאינו נחשב ט על פי קובץ הוראות הקריאה לשמ"פ, רשאי להגיש בקשה למדור ולת"ם.	Block	1
149.56.41.137	United States	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 149.56.41.137	Block	1
80.246.133.249	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sahar	Block	1
46.19.86.19	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtLastName in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	1
185.103.12.53	Lebanon	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.76.35	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/.well-known/apple-app-site-association	Block	1
212.179.28.34	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	1
149.56.41.137	United States	147.237.77.74	law.idf.il	PHP Attempt	Block	1
188.120.148.32	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	1
117.25.234.39	China	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/default.aspx	Block	1
66.249.79.58	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/.well-known/assetlinks.json	Block	1
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/default.aspx	Block	1
46.229.164.99	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
197.119.245.58	Algeria	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
68.180.230.171	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1362-he/dover.aspx	Block	1
14.155.226.185	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/index.asp	Block	1
176.13.2.154	Israel	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1

08-23-2016-07:04:04 to 08-23-2016-08:04:04