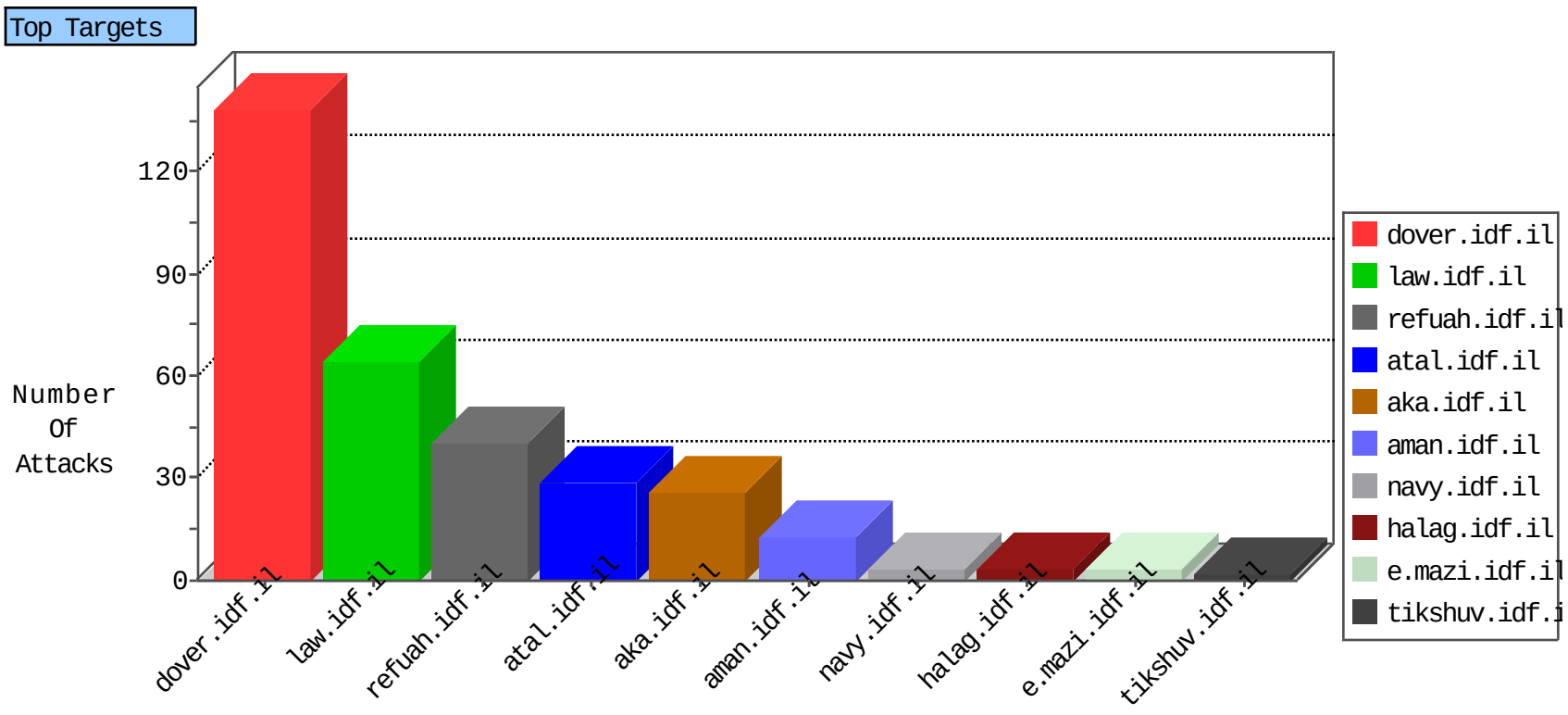
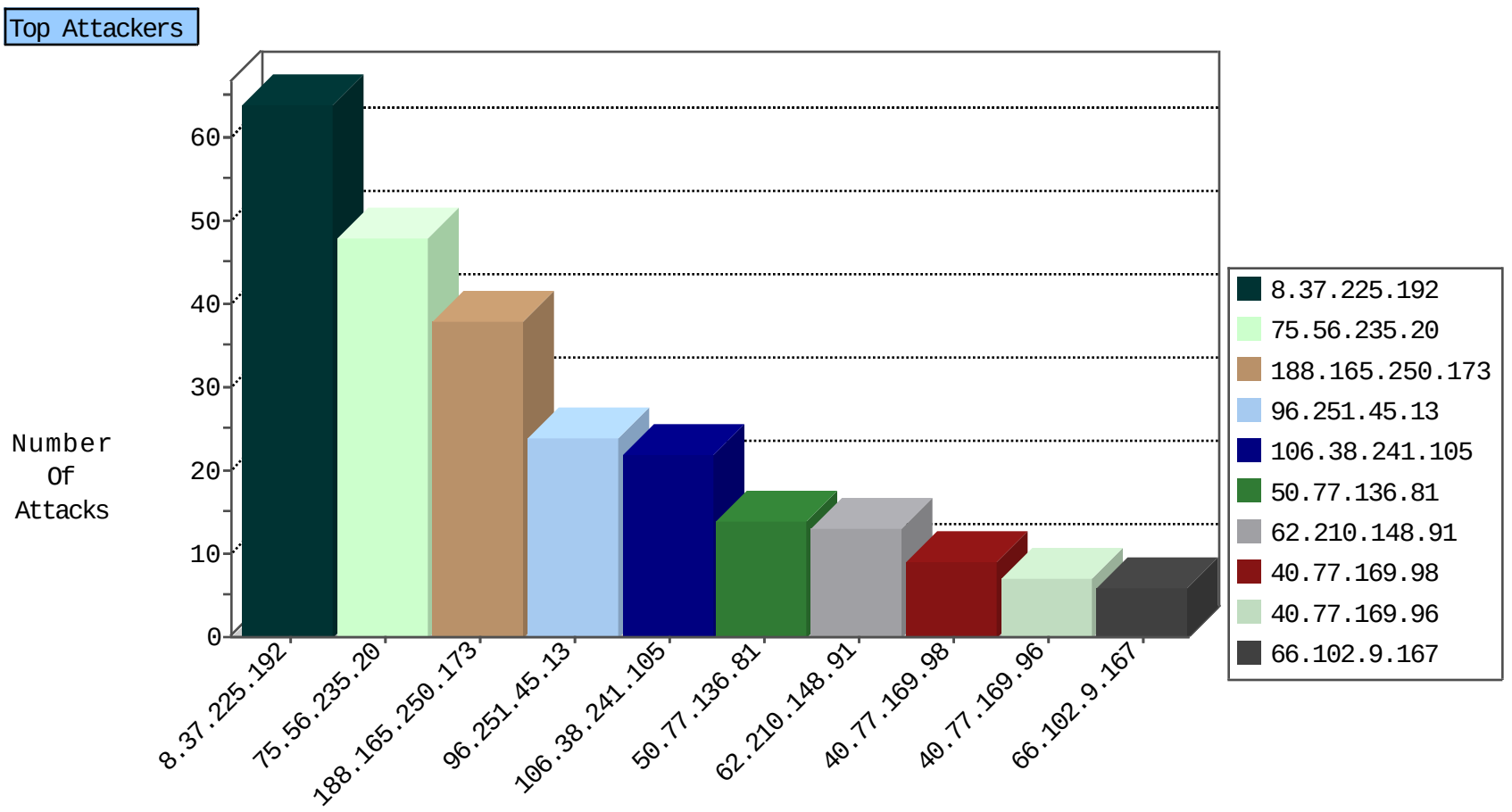
08-24-2016-23:04:02 to 08-25-2016-00:04:02

IDF Under Attack Daily Report





08-24-2016-23:04:02 to 08-25-2016-00:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
50.87.144.145	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
77.138.52.97	France	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
8.37.225.192	United States	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	3
66.249.93.111	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
195.154.172.204	France	147.237.72.217	e.idf.il	JLM_Purple_Con_Limit_Http	drop	1
104.148.55.162	United States	147.237.76.30	himush.idf.il	Black List	drop	1
185.94.111.1	Russian Federation	147.237.76.34	yohalan.idf.il	Black List	drop	1

08-24-2016-23:04:02 to 08-25-2016-00:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.105	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	20
75.56.235.20	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	12
188.165.250.173	France	147.237.76.42	refuah.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
50.77.136.81	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
188.165.250.173	France	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
96.251.45.13	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
185.29.8.211	Sweden	147.237.77.216	dover.idf.il	24910: HTTP: Python urllib User-Agent Header	Block	1

08-24-2016-23:04:02 to 08-25-2016-00:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
75.56.235.20	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	36
188.165.250.173	147.237.76.42	France	refuah.idf.il	SQL Injection - Select From	20
96.251.45.13	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	18
50.77.136.81	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	8
62.210.148.91	147.237.72.166	France	aka.idf.il	ET WEB_SERVER Tilde in URI, potential .php source disclosure vulnerability	1
133.208.21.66	147.237.76.30	Japan	himush.idf.il	ET SCAN NMAP -sS window 1024	1
62.210.148.91	147.237.0.15	France	kosher-kravi.idf.il	ET WEB_SERVER Tilde in URI, potential .php source disclosure vulnerability	1
50.84.213.146	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -sS window 2048	1
94.102.60.173	147.237.76.44	Netherlands	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
50.84.213.146	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -f -sS	1
85.65.245.248	147.237.72.166	Israel	aka.idf.il	ET SCAN NMAP -sA (2)	1
2.53.0.7	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
62.210.148.91	147.237.77.233	France	atal.idf.il	ET WEB_SERVER Tilde in URI, potential .php source disclosure vulnerability	1
62.210.148.91	147.237.76.86	France	navy.idf.il	ET WEB_SERVER Tilde in URI, potential .php source disclosure vulnerability	1
133.242.3.168	147.237.8.24	Japan	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
62.210.148.91	147.237.76.31	France	nakchal.idf.il	ET WEB_SERVER Tilde in URI, potential .php source disclosure vulnerability	1
133.208.21.66	147.237.76.202	Japan	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
62.210.148.91	147.237.0.34	France	tikshuv.idf.il	ET WEB_SERVER Tilde in URI, potential .php source disclosure vulnerability	1
106.38.241.105	147.237.72.156	China	aman.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
61.240.144.66	147.237.76.200	China	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.60.173	147.237.76.86	Netherlands	navy.idf.il	ET SCAN Potential SSH Scan	1
50.84.213.146	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.60.173	147.237.76.31	Netherlands	nakchal.idf.il	ET SCAN Potential SSH Scan	1
80.246.137.78	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
62.210.148.91	147.237.77.234	France	halag.idf.il	ET WEB_SERVER Tilde in URI, potential .php source disclosure vulnerability	1
62.210.148.91	147.237.77.226	France	www.chamatz.aka.idf.il	ET WEB_SERVER Tilde in URI, potential .php source disclosure vulnerability	1
133.242.4.52	147.237.0.34	Japan	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
62.210.148.91	147.237.76.42	France	refuah.idf.il	ET WEB_SERVER Tilde in URI, potential .php source disclosure vulnerability	1
133.242.3.168	147.237.0.33	Japan	idf.il	ET SCAN NMAP -sS window 1024	1

08-24-2016-23:04:02 to 08-25-2016-00:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
8.37.225.192	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	61
40.77.169.98	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	9
40.77.169.96	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	7
66.102.9.167	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
46.120.56.149	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
109.253.205.77	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
216.243.31.2	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
85.130.234.154	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	1
176.13.18.158	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	1
89.139.119.230	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	1
176.13.249.126	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
176.67.123.212	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
131.161.176.110	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
84.109.119.166	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
157.55.39.37	United States	147.237.77.216	dover.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
172.1.149.62	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	5
213.57.59.50	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	4
77.138.145.208	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/exampcert/	Block	3
85.250.150.134	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/www.navy.idf.il	Block	2
46.19.86.92	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
66.102.9.105	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
40.77.169.99	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
66.249.69.224	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.224	Block	1
180.97.106.162	China	147.237.77.235	sviva.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
62.210.148.91	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/configuration.php~	Block	1
144.76.236.183	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1
80.178.83.12	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
66.249.64.58	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
213.57.96.227	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
40.77.169.101	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
176.13.15.183	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchildsubcategories/1423	Block	1
106.38.241.105	China	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
207.46.13.34	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1589-en/dover.aspxthe	Block	1
62.210.148.91	France	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/configuration.php~	Block	1
2.55.8.181	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1275-he/atal.aspx	Block	1
157.55.39.37	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
82.166.121.114	Israel	147.237.77.74	law.idf.il	PHP Attempt	Block	1
66.249.64.60	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1409-he/atal.aspx	Block	1
180.97.106.37	China	147.237.77.234	halag.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
109.206.58.12	Ukraine	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
79.179.57.71	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
207.46.13.176	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/list20050529.htm	Block	1
62.210.148.91	France	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 62.210.148.91	Block	1
37.26.148.164	Israel	147.237.77.233	atal.idf.il	Parameter Type Violation search in atal.idf.il/1440-he/atal.aspx	Block	1
157.55.39.110	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
82.166.121.114	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/wp-login.php	Block	1
66.249.64.108	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 66.249.64.108	Block	1
180.97.106.161	China	147.237.0.19	madim.atal.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
46.117.152.71	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/default.aspxnrg	Block	1
109.253.205.77	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.180.44.64	Israel	147.237.72.156	aman.idf.il	Too Many Cookies in a Request - 101 cookies	Block	1
213.55.184.243	Switzerland	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/chamatz	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
37.112.226.215	Russian Federation	147.237.76.42	refuah.idf.il	Unauthorized Method POST for 147.237.76.42/	Block	1
157.55.39.173	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/	Block	1
85.64.38.190	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/homepage/homepage.aspx	Block	1
66.249.64.153	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage/files/5/שקופית3	Block	1
180.97.106.161	China	147.237.76.200	eitan.aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
62.210.148.91	France	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to kosher-kravi.idf.il/configuration.php~	Block	1
123.125.71.80	China	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/robots.txt	Block	1
79.182.58.31	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx	Block	1