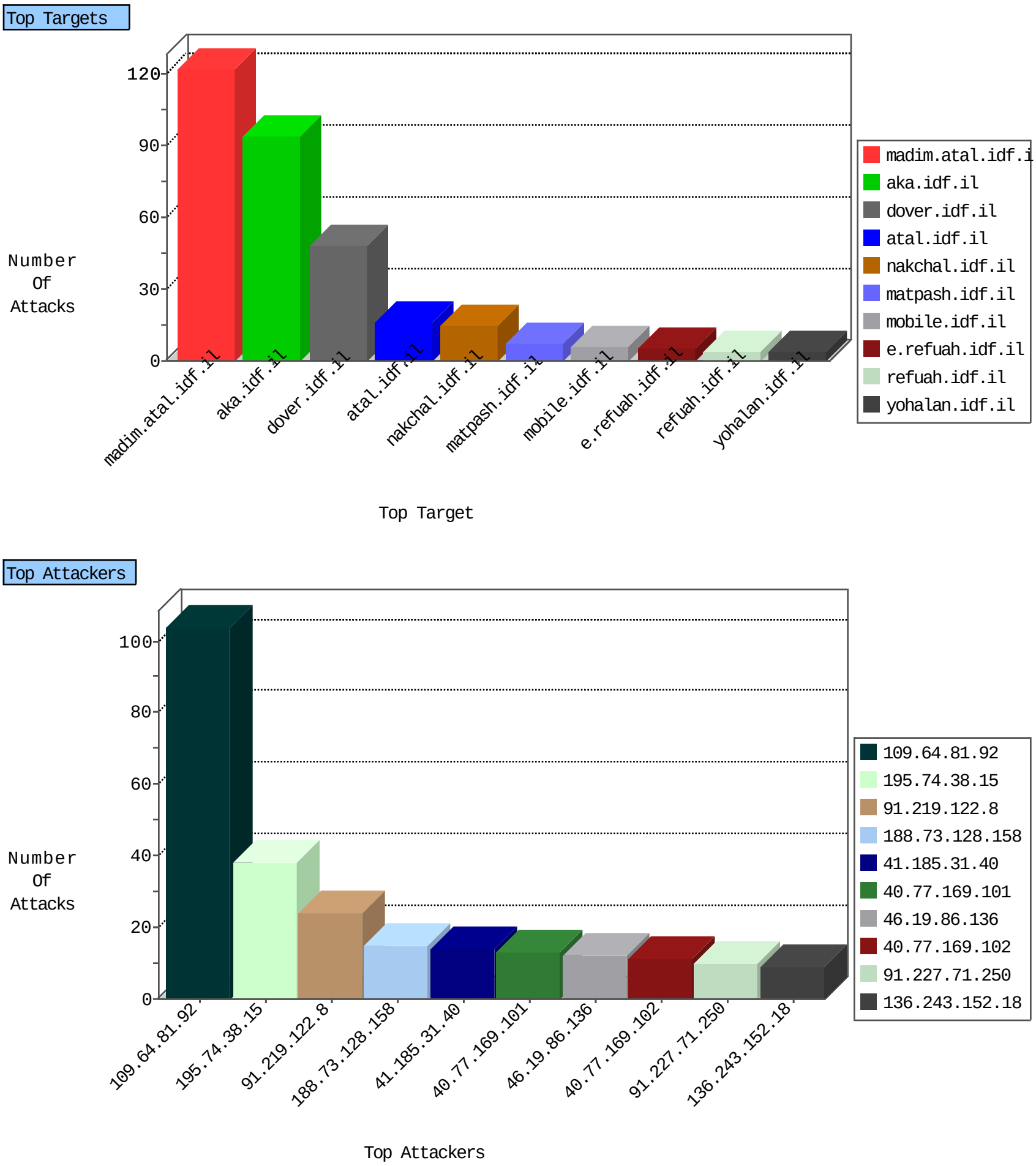
08-25-2016-07:04:02 to 08-25-2016-08:04:02

IDF Under Attack Daily Report



08-25-2016-07:04:02 to 08-25-2016-08:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
120.132.50.135	China	147.237.76.31	nakchal.idf.il	block-sp-traf1	forward	2
42.114.92.135	Vietnam	147.237.76.202	e.halag.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
104.148.55.162	United States	147.237.76.44	e.refuah.idf.il	Black List	drop	1

08-25-2016-07:04:02 to 08-25-2016-08:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
195.74.38.15	Sweden	147.237.72.166	aka.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
136.243.152.18	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	7
41.185.31.40	South Africa	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
91.219.122.8	Poland	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	5
195.74.38.15	Sweden	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	5
136.243.152.18	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
195.74.38.15	Sweden	147.237.72.166	aka.idf.il	9785: HTTP: SQL Injection (Referer Header)	Block	1
91.219.122.8	Poland	147.237.72.166	aka.idf.il	9785: HTTP: SQL Injection (Referer Header)	Block	1
94.102.49.190	Netherlands	147.237.76.197	e.himush.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

08-25-2016-07:04:02 to 08-25-2016-08:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.74.38.15	147.237.72.166	Sweden	aka.idf.il	SQL Injection - Select From	20
91.219.122.8	147.237.72.166	Poland	aka.idf.il	SQL Injection - Select From	18
41.185.31.40	147.237.72.166	South Africa	aka.idf.il	SQL Injection - Select From	8
91.227.71.250	147.237.76.31	Israel	nakchal.idf.il	LOCAL_RULES - HTTP Request with OPTIONS method to a .doc file	2
91.227.71.250	147.237.76.31	Israel	nakchal.idf.il	WEB-FRONTPAGE /_vti_bin/ access	2
59.100.214.202	147.237.77.19	Australia	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
186.113.224.103	147.237.0.34	Colombia	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
5.255.90.133	147.237.76.31	Netherlands	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
133.242.4.52	147.237.8.24	Japan	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
117.27.240.24	147.237.77.226	China	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
93.115.96.31	147.237.76.34	France	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.158	147.237.76.44	Ukraine	e.refuah.idf.il	ET SCAN NMAP -sS window 4096	1
91.201.236.158	147.237.76.44	Ukraine	e.refuah.idf.il	ET SCAN NMAP -f -sS	1
59.100.214.202	147.237.77.19	Australia	law-forum.idf.il	ET SCAN NMAP -sS window 4096	1
190.66.210.212	147.237.76.39	Colombia	mobile.meitav.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
161.18.13.228	147.237.76.34	Colombia	yohalan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
124.107.75.14	147.237.0.33	Philippines	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
93.115.96.31	147.237.76.34	France	yohalan.idf.il	ET SCAN NMAP -sS window 3072	1
91.201.236.158	147.237.76.44	Ukraine	e.refuah.idf.il	ET SCAN NMAP -sS window 2048	1
91.201.236.158	147.237.76.44	Ukraine	e.refuah.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
193.201.225.149	147.237.72.167	Ukraine	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1

08-25-2016-07:04:02 to 08-25-2016-08:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
188.73.128.158	Russian Federation	147.237.77.233	atal.idf.il	drop	Unexpected post SYN packet - RST or SYN expected	drop	13
40.77.169.101	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	13
40.77.169.102	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	7
40.77.169.96	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	7
40.77.169.97	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	6
40.77.169.102	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
109.253.206.220	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
176.9.131.69	Germany	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
180.97.106.161	China	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	1
5.102.195.91	Israel	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	1
188.73.128.158	Russian Federation	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	1
176.13.14.109	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
89.248.174.4	Netherlands	147.237.76.34	yohalan.idf.il	drop		drop	1
180.97.106.37	China	147.237.0.15	kosher-kravi.idf.il	drop	SAM rule	drop	1
109.253.156.155	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
180.97.106.37	China	147.237.72.156	aman.idf.il	drop	SAM rule	drop	1

08-25-2016-07:04:02 to 08-25-2016-08:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.64.81.92	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	104
46.19.86.136	Israel	147.237.0.19	madim.atal.idf.i	Suspicious Response Code	Block	12
176.13.7.113	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword	Block	5
91.227.71.250	Israel	147.237.76.31	nakchal.idf.il	Multiple signatures from 91.227.71.250	Block	3
37.26.147.251	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.85.22	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
91.227.71.250	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 91.227.71.250	Block	2
157.55.39.110	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
80.230.220.134	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
46.19.85.215	Israel	147.237.76.42	refuah.idf.il	Abnormally Long Request method	Block	1
46.121.61.194	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/3/1723.pdf	Block	1
5.22.132.112	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
212.235.53.129	Israel	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
157.55.39.194	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
80.230.220.135	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
46.19.85.215	Israel	147.237.76.42	refuah.idf.il	Illegal HTTP Version __atuvs=57be78e52d55c916000; _pk_id.118.fd1c=1475e8c913910977.1472100583.1.1472100583.1472100583.; _pk_ses.118.fd1c=*	Block	1
188.73.128.158	Russian Federation	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/favicon.ico	Block	1
91.227.71.250	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	1
66.249.64.118	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/robots.txt	Block	1
212.235.53.129	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
157.55.39.194	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/international_training/about_our_courses.asp	Block	1
80.230.221.208	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
46.19.85.215	Israel	147.237.76.42	refuah.idf.il	Malformed URL __atuvc=1	Block	1
192.118.10.10	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 192.118.10.10	Block	1
66.249.69.236	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/apple-app-site-association	Block	1
40.77.169.99	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
173.180.204.245	Canada	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 173.180.204.245 (Open Mode)	None	1
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/default.aspx	Block	1
46.19.85.215	Israel	147.237.76.42	refuah.idf.il	Unknown HTTP Request Method 45akynqvjc1inj3a45; in URL __atuvc=1	Block	1
204.79.180.251	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/miluim/templates/inner.asp	Block	1
138.134.192.10	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012 ources/images/innerpage/goback.gif	Block	1
66.249.76.106	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/900-he/chinuch.aspx	Block	1
173.180.204.245	Canada	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
212.129.62.79	France	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1

08-25-2016-07:04:02 to 08-25-2016-08:04:02