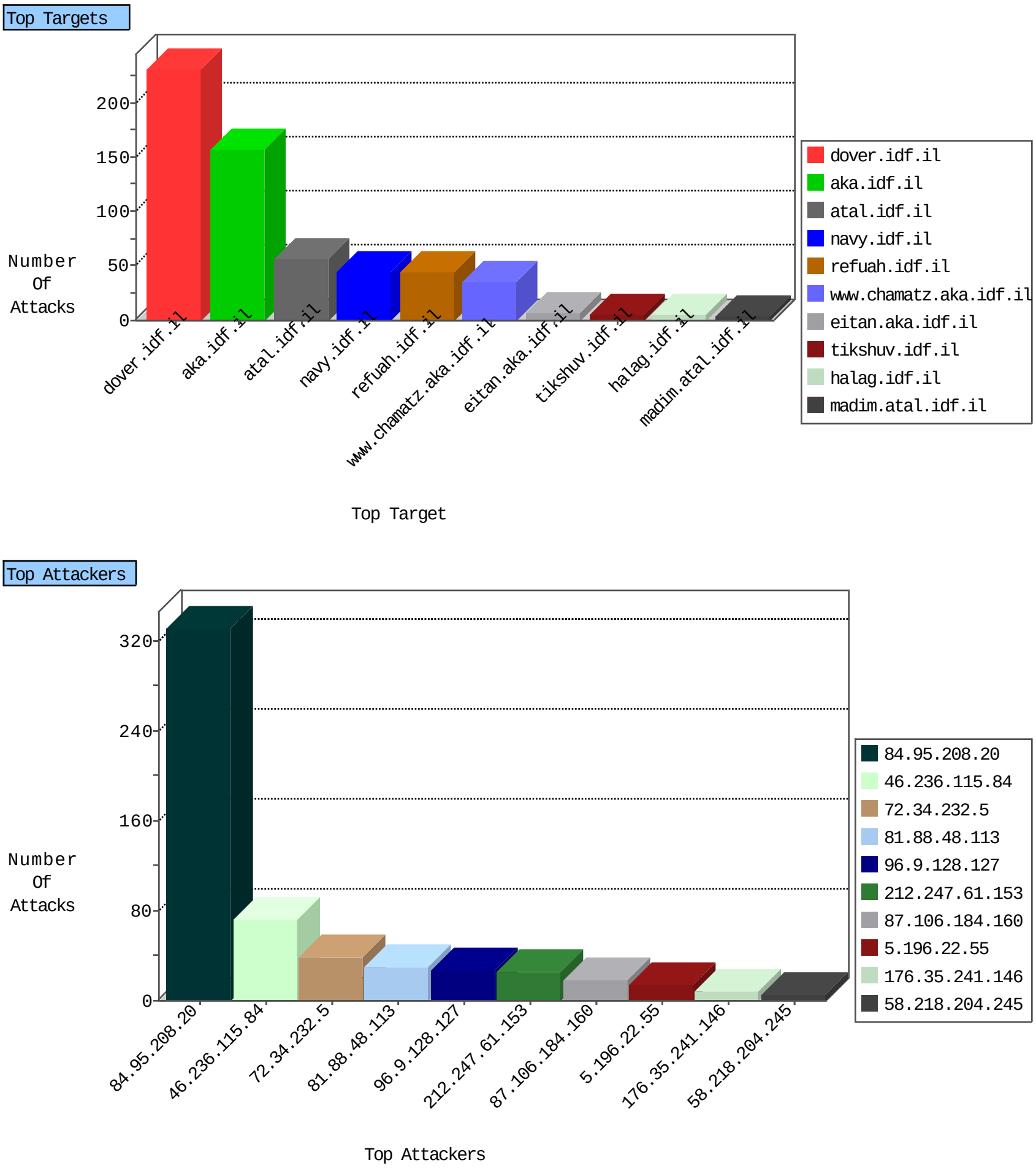
08-21-2016-02:04:03 to 08-21-2016-03:04:03

IDF Under Attack Daily Report



08-21-2016-02:04:03 to 08-21-2016-03:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
93.174.93.156	Netherlands	147.237.76.147	chinuch.aka.idf.il	Black List	drop	1
51.254.51.2	France	147.237.76.200	eitan.aka.idf.il	Black List	drop	1
79.176.19.113	Israel	147.237.72.166	aka.idf.il	Black List	drop	1
93.174.93.156	Netherlands	147.237.76.31	nakchal.idf.il	Black List	drop	1

08-21-2016-02:04:03 to 08-21-2016-03:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.236.115.84	Sweden	147.237.77.216	dover.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	13
72.34.232.5	United States	147.237.76.86	navy.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	12
81.88.48.113	Italy	147.237.77.233	atal.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	11
212.247.61.153	Sweden	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
5.196.22.55	France	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
81.88.48.113	Italy	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
212.247.61.153	Sweden	147.237.76.42	refuah.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	6
72.34.232.5	United States	147.237.76.86	navy.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	6
46.236.115.84	Sweden	147.237.77.216	dover.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	5
162.210.196.130	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
81.88.48.113	Italy	147.237.77.233	atal.idf.il	9785: HTTP: SQL Injection (Referer Header)	Block	1

08-21-2016-02:04:03 to 08-21-2016-03:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.236.115.84	147.237.77.216	Sweden	dover.idf.il	SQL Injection - Select From	54
72.34.232.5	147.237.76.86	United States	navy.idf.il	SQL Injection - Select From	20
212.247.61.153	147.237.76.42	Sweden	refuah.idf.il	SQL Injection - Select From	14
81.88.48.113	147.237.77.233	Italy	atal.idf.il	SQL Injection - Select From	12
5.196.22.55	147.237.77.233	France	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	4
58.218.204.245	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
58.218.204.245	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
129.56.2.38	147.237.8.50	Nigeria	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.195	147.237.8.24	Netherlands	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
58.218.204.245	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
58.218.204.245	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	1
58.218.204.245	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
123.206.73.185	147.237.8.27	China	e.madim.atal.idf.i	ET SCAN NMAP -sS window 1024	1
91.125.184.101	147.237.77.216	United Kingdom	dover.idf.il	Tehila - Perl LWP with fake user agent	1
72.89.107.124	147.237.8.28	United States	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
65.98.59.26	147.237.72.156	United States	aman.idf.il	ET SCAN Potential SSH Scan	1

08-21-2016-02:04:03 to 08-21-2016-03:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
96.9.128.127	Singapore	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
87.106.184.160	Germany	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	18
176.35.241.146	United Kingdom	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
168.1.128.34	United States	147.237.0.19	madim.atal.idf.il	drop	First packet isn't SYN	drop	1
168.1.128.34	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
109.253.197.29	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
185.125.4.222	Poland	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	1
129.56.2.38	Nigeria	147.237.0.200	m4u.idf.il	drop		drop	1

08-21-2016-02:04:03 to 08-21-2016-03:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	133
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	104
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	25
84.95.208.20	Israel	147.237.77.216	dover.idf.il	PHP Attempt	Block	13
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	PHP Attempt	Block	10
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	8
84.95.208.20	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	5
84.95.208.20	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	5
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	5
84.95.208.20	Israel	147.237.77.234	halag.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	4
84.95.208.20	Israel	147.237.77.233	atal.idf.il	PHP Attempt	Block	3
84.95.208.20	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	3
84.95.208.20	Israel	147.237.0.15	kosher-kravi.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	3
37.26.149.142	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.95.208.20	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
84.95.208.20	Israel	147.237.0.15	kosher-kravi.idf.il	PHP Attempt	Block	1
85.65.145.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/kapatz/undefined	Block	1
41.85.67.152	South Africa	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtLastName in www.idf.il/1038-en/dover.aspx	Block	1
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/piwik.php	Block	1
79.177.120.210	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
136.243.16.208	Germany	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/brothers/skira/default.asp	Block	1
66.249.66.131	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to atal.idf.il/templates/shared/usercontrols/navmenu/	Block	1
79.182.129.78	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 79.182.129.78	Block	1
84.95.208.20	Israel	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
84.95.208.20	Israel	147.237.0.34	tikshuv.idf.il	PHP Attempt	Block	1
157.55.39.190	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/main/smalim/smalim.aspx	None	1
66.249.79.114	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/apple-app-site-association	Block	1
79.182.129.78	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/patzar	Block	1
84.95.208.20	Israel	147.237.77.234	halag.idf.il	PHP Attempt	Block	1
84.95.208.20	Israel	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
77.139.175.85	France	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/favicon.ico	Block	1
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/homepage/div.item	Block	1
84.95.208.20	Israel	147.237.76.86	navy.idf.il	PHP Attempt	Block	1
85.65.145.131	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 85.65.145.131	Block	1
84.95.208.20	Israel	147.237.72.156	aman.idf.il	PHP Attempt	Block	1
79.177.120.210	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 79.177.120.210 (Open Mode)	None	1

08-21-2016-02:04:03 to 08-21-2016-03:04:03