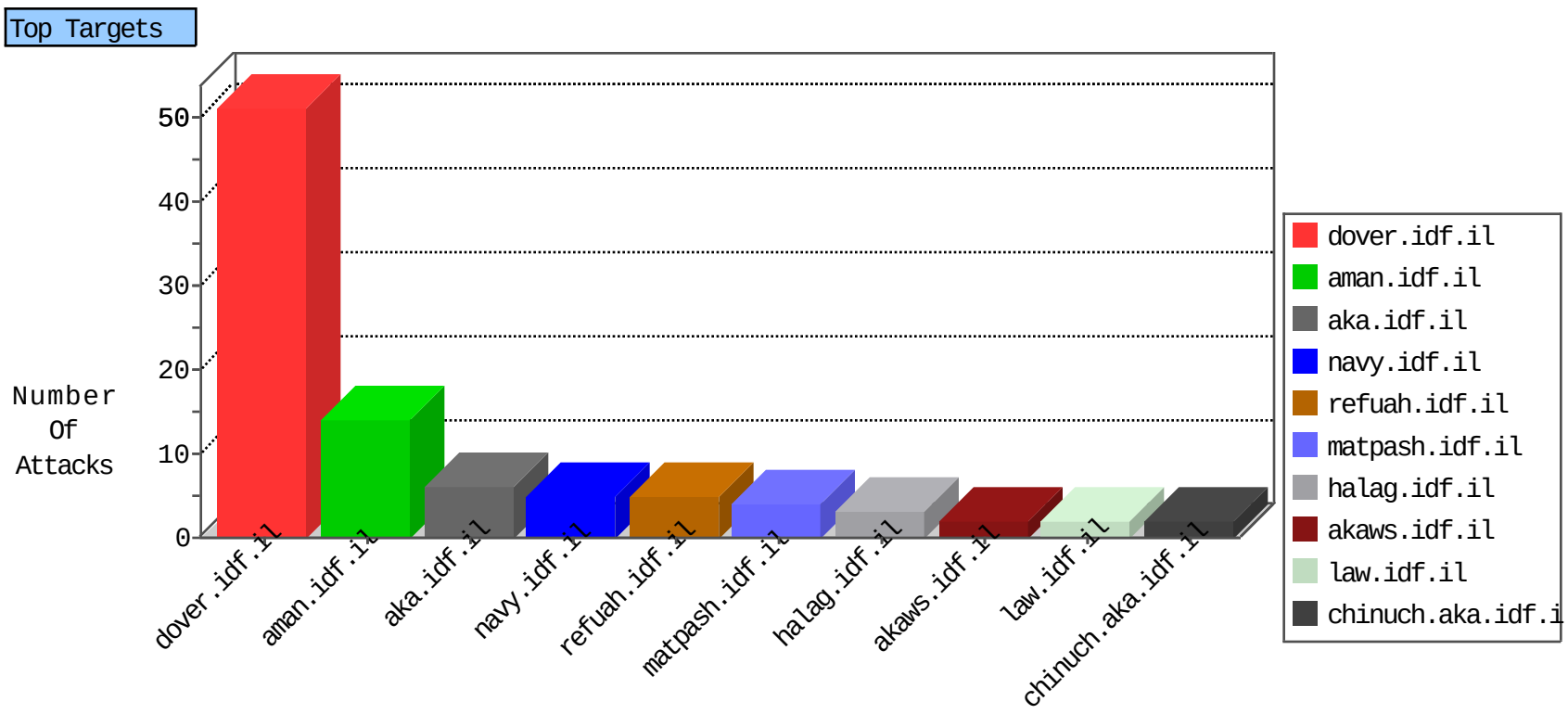
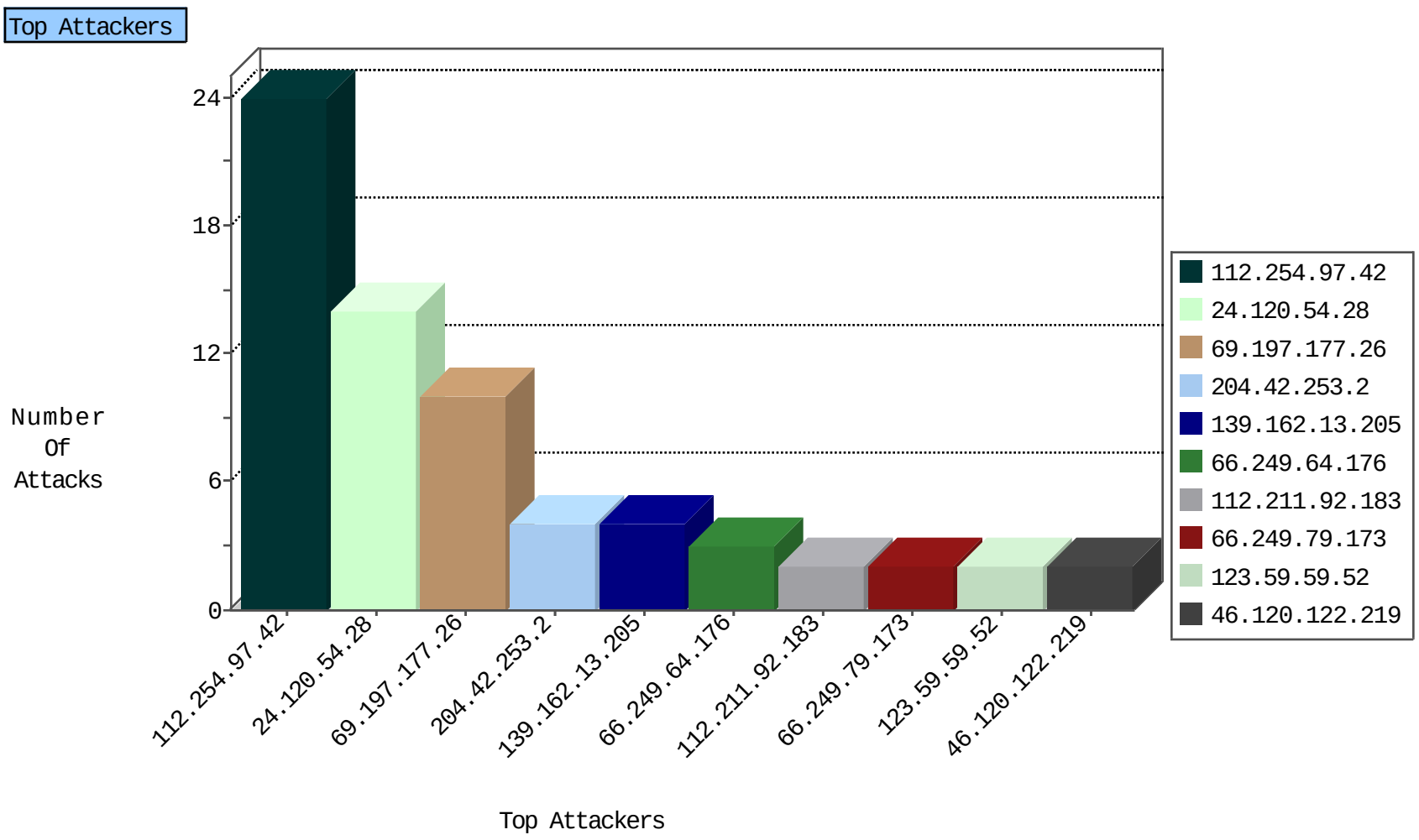
08-19-2016-05:04:03 to 08-19-2016-06:04:03

IDF Under Attack Daily Report

Top Targets



Top Attackers



08-19-2016-05:04:03 to 08-19-2016-06:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
123.59.59.52	China	147.237.76.86	navy.idf.il	block-sp-traf1	forward	2
204.42.253.2	United States	147.237.76.42	refuah.idf.il	Black List	drop	2
204.42.253.2	United States	147.237.76.44	e.refuah.idf.il	Black List	drop	2
82.80.78.2	Israel	147.237.77.176	matpash.idf.il	Black List	drop	1
198.20.69.74	United States	147.237.76.147	chinuch.aka.idf.il	Black List	drop	1
93.158.200.93	Netherlands	147.237.76.147	chinuch.aka.idf.il	Black List	drop	1
104.148.55.162	United States	147.237.76.86	navy.idf.il	Black List	drop	1

08-19-2016-05:04:03 to 08-19-2016-06:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
69.197.177.26	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	9
108.59.8.70	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
199.58.86.206	United States	147.237.77.234	halag.idf.il	C1000074: HTTP: majestic bot	Permit	2
71.6.135.131	United States	147.237.0.17	m.my-kosher-kravi.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

08-19-2016-05:04:03 to 08-19-2016-06:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
191.111.184.186	147.237.0.35	Colombia	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
139.162.13.205	147.237.76.42	Singapore	refuah.idf.i	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
93.174.91.29	147.237.8.45	Netherlands	e.eitan.idf.	ET SCAN NMAP -sS window 1024	1
46.120.122.219	147.237.72.166	Israel	aka.idf.il	Xenu Link Sleuth User Agent	1
171.232.239.160	147.237.0.35	Vietnam	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
139.162.13.205	147.237.8.45	Singapore	e.eitan.idf.	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
91.201.236.50	147.237.0.200	Ukraine	m4u.idf.il	ET SCAN Potential SSH Scan	1

08-19-2016-05:04:03 to 08-19-2016-06:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
24.120.54.28	United States	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	14
212.47.231.31	France	147.237.77.74	law.idf.il	drop	SAM rule	drop	2
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
112.206.148.127	Philippines	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
112.211.92.183	Philippines	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
124.106.41.60	Philippines	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1

08-19-2016-05:04:03 to 08-19-2016-06:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
112.254.97.42	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 112.254.97.42	Block	17
112.254.97.42	China	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	6
66.249.64.176	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 66.249.64.176	Block	3
66.249.64.183	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.183	Block	2
207.46.13.73	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
104.174.36.37	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/favicon.ico	Block	1
66.249.69.249	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/main/giyus/general.aspx	Block	1
139.162.13.205	Singapore	147.237.76.42	refuah.idf.il	Multiple Untraceable SSL Sessions from 139.162.13.205 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
84.95.208.20	Israel	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
40.77.167.8	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
208.115.113.89	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/console/core/doc_mgr/iaf.org.il	Block	1
104.236.242.195	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/patzar	Block	1
66.249.79.173	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 66.249.79.173	Block	1
139.162.13.205	Singapore	147.237.76.42	refuah.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
94.178.150.195	Ukraine	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
46.120.122.219	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/miluim/horaot/templates/main.asp	Block	1
66.249.79.173	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	1
157.55.39.24	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/giyus/..aspx	Block	1
104.128.144.131	Canada	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/redirect.php	Block	1
69.197.177.26	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english	Block	1
180.76.15.135	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	Block	1
104.128.144.131	Canada	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/redirect.php	Block	1
112.254.97.42	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/index.asp	Block	1
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1

08-19-2016-05:04:03 to 08-19-2016-06:04:03