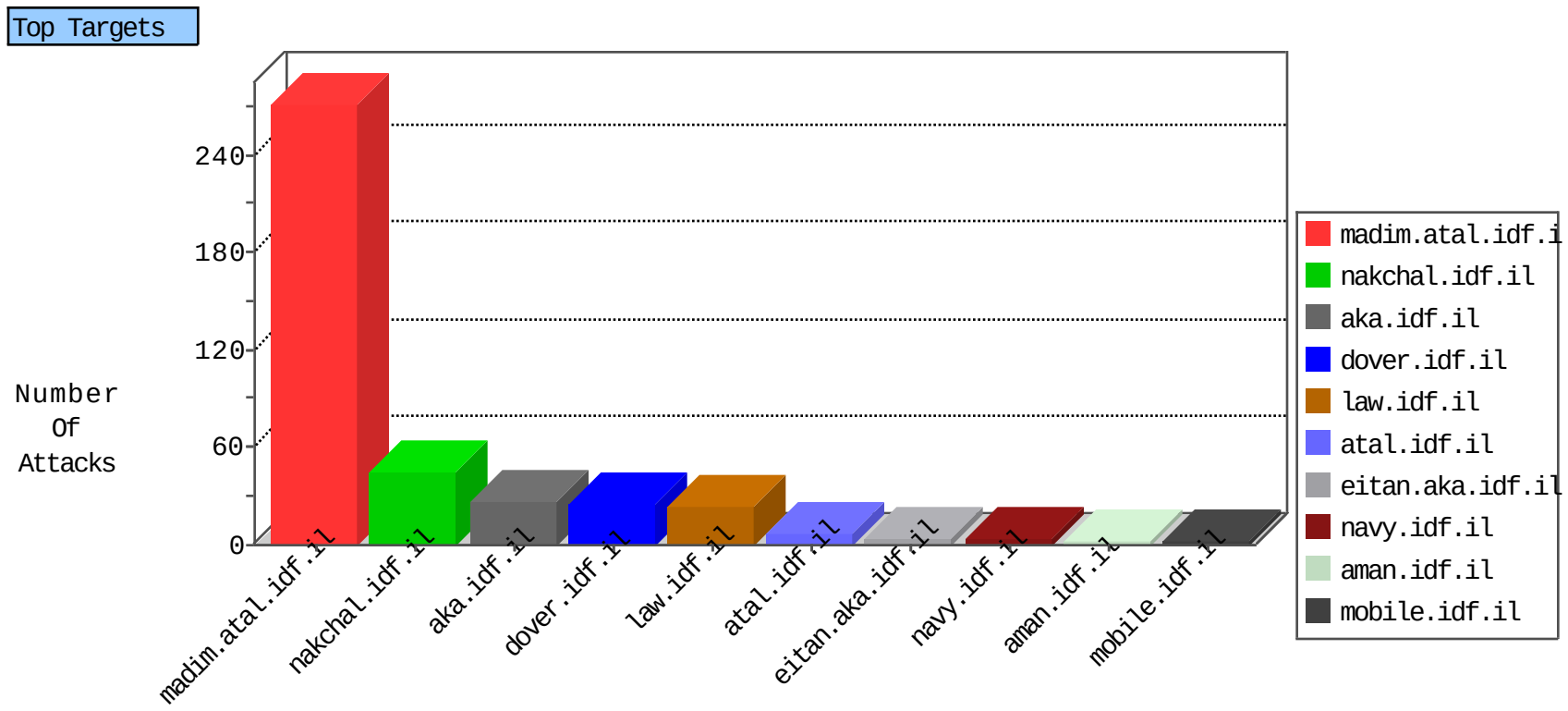
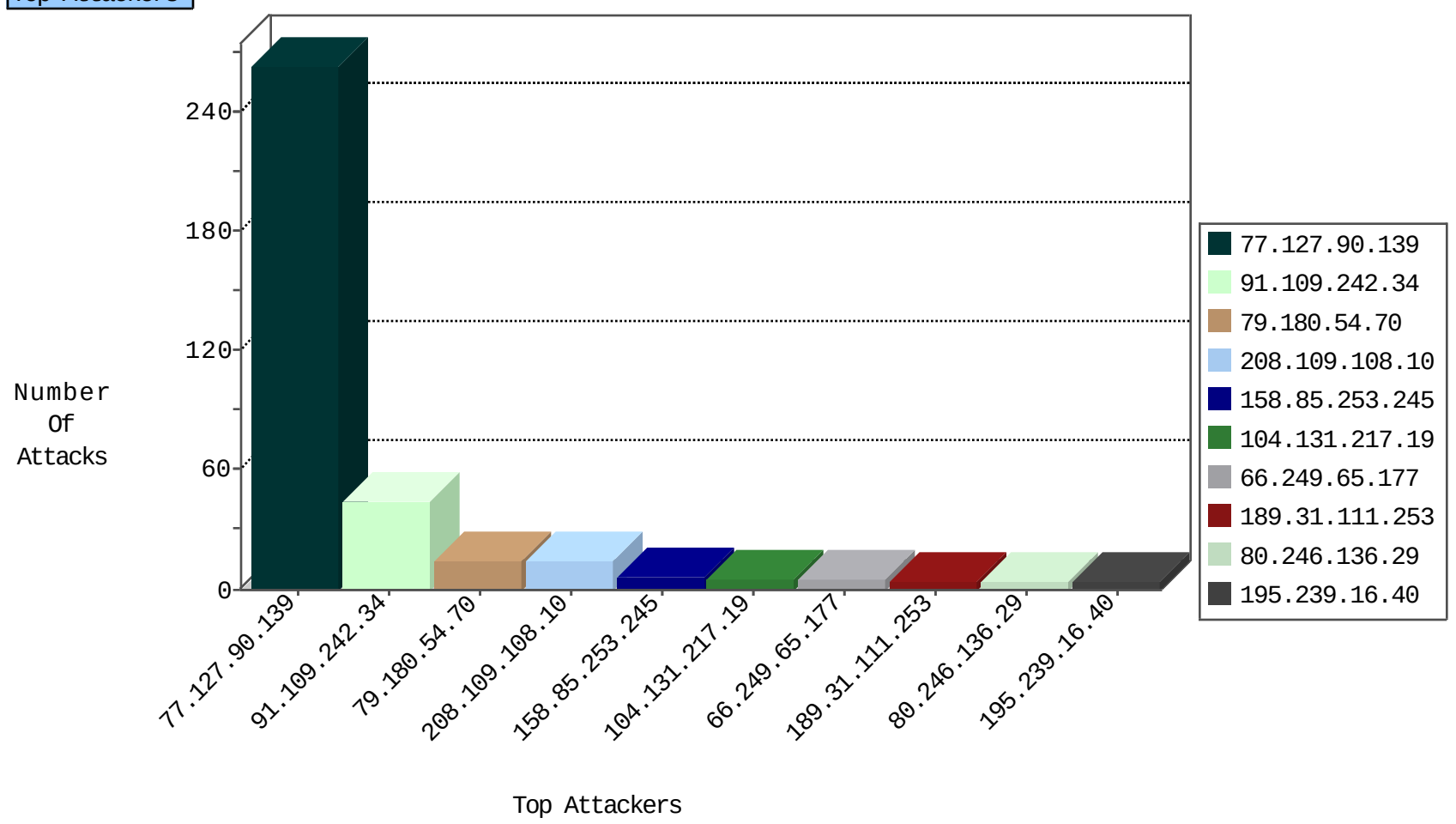
08-21-2016-00:04:04 to 08-21-2016-01:04:04

IDF Under Attack Daily Report

Top Targets



Top Attackers



08-21-2016-00:04:04 to 08-21-2016-01:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
189.31.111.253	Brazil	147.237.76.86	navy.idf.il	Black List	drop	4
2.53.41.187	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
82.80.78.2	Israel	147.237.77.216	dover.idf.il	Black List	drop	1
109.65.4.192	Israel	147.237.72.166	aka.idf.il	Black List	drop	1
91.230.121.156	Ukraine	147.237.76.198	e.yohalan.idf.il	Black List	drop	1
93.158.200.86	Netherlands	147.237.76.42	refuah.idf.il	Black List	drop	1
93.174.93.156	Netherlands	147.237.76.202	e.halag.idf.il	Black List	drop	1

08-21-2016-00:04:04 to 08-21-2016-01:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
91.109.242.34	United Kingdom	147.237.76.31	nakchal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	6
91.109.242.34	United Kingdom	147.237.76.31	nakchal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
91.109.242.34	United Kingdom	147.237.76.31	nakchal.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	6
208.109.108.10	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
108.59.8.80	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
164.132.161.40	Italy	147.237.76.200	eitan.aka.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
164.132.161.49	Italy	147.237.76.200	eitan.aka.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
164.132.161.59	Italy	147.237.76.200	eitan.aka.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
51.255.65.97	France	147.237.76.200	eitan.aka.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
151.80.31.155	France	147.237.77.234	halag.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1

08-21-2016-00:04:04 to 08-21-2016-01:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
91.109.242.34	147.237.76.31	United Kingdom	nakchal.idf.il	SQL Injection - Select From	26
208.109.108.10	147.237.77.74	United States	law.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	3
37.26.148.171	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
193.201.225.138	147.237.72.167	Ukraine	ishurim.aka.idf.i	ET SCAN NMAP -sS window 1024	1
104.131.217.19	147.237.76.31	United States	nakchal.idf.il	ET SCAN Potential SSH Scan	1
104.131.217.19	147.237.0.35	United States	akaws.idf.il	ET SCAN Potential SSH Scan	1
103.207.39.11	147.237.77.235	Vietnam	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.76.117	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
14.104.138.27	147.237.0.34	China	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
182.209.162.182	147.237.76.38	Korea, Republic of	e.e.meitav.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
104.131.217.19	147.237.76.176	United States	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
104.131.217.19	147.237.76.30	United States	himush.idf.il	ET SCAN Potential SSH Scan	1
104.131.217.19	147.237.0.33	United States	idf.il	ET SCAN Potential SSH Scan	1
91.125.184.101	147.237.77.74	United Kingdom	law.idf.il	Tehila - Perl LWP with fake user agent	1
66.249.79.104	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sA (2)	1

08-21-2016-00:04:04 to 08-21-2016-01:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.180.54.70	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	14
158.85.253.245	United States	147.237.77.233	atal.idf.il	drop	SAM rule	drop	6
195.239.16.40	Russian Federation	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
195.239.16.53	Russian Federation	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
62.210.113.73	France	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	2
202.207.240.35	China	147.237.76.34	yohalan.idf.il	drop		drop	1
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
66.249.93.107	Israel	147.237.77.170	maarachot.idf.il	drop	SAM rule	drop	1
176.13.9.91	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
66.249.93.107	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
31.168.172.143	Israel	147.237.0.200	m4u.idf.il	drop		drop	1
115.230.125.146	China	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1

08-21-2016-00:04:04 to 08-21-2016-01:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
77.127.90.139	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	263
66.249.65.177	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.177	Block	5
80.246.136.29	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
46.10.208.83	Bulgaria	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
89.139.100.134	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
109.67.151.28	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
176.13.22.125	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152	Block	2
66.102.9.43	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
85.65.54.95	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1136-he/atal.aspx	Block	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/5/71545.pdf	Block	1
37.142.92.232	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
180.76.15.149	China	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/robots.txt	Block	1
77.126.27.22	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/aman	Block	1
66.249.76.117	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
37.142.183.4	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
207.46.13.9	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
66.249.73.137	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-20706-he/idfgdover.aspx	Block	1
66.249.81.212	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
213.151.35.220	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/registrationwizard/step4.aspx	Block	1
79.180.44.64	Israel	147.237.72.156	aman.idf.il	Too Many Cookies in a Request - 101 cookies	Block	1
66.249.73.155	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19412-he/dover.aspx	Block	1
2.55.159.112	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
132.74.95.19	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/0/113010.pdf	Block	1
66.249.81.215	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
46.19.86.183	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.76.2	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1680	Block	1
5.22.135.174	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/apple-touch-icon-precomposed.png	Block	1
66.249.88.40	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1

08-21-2016-00:04:04 to 08-21-2016-01:04:04