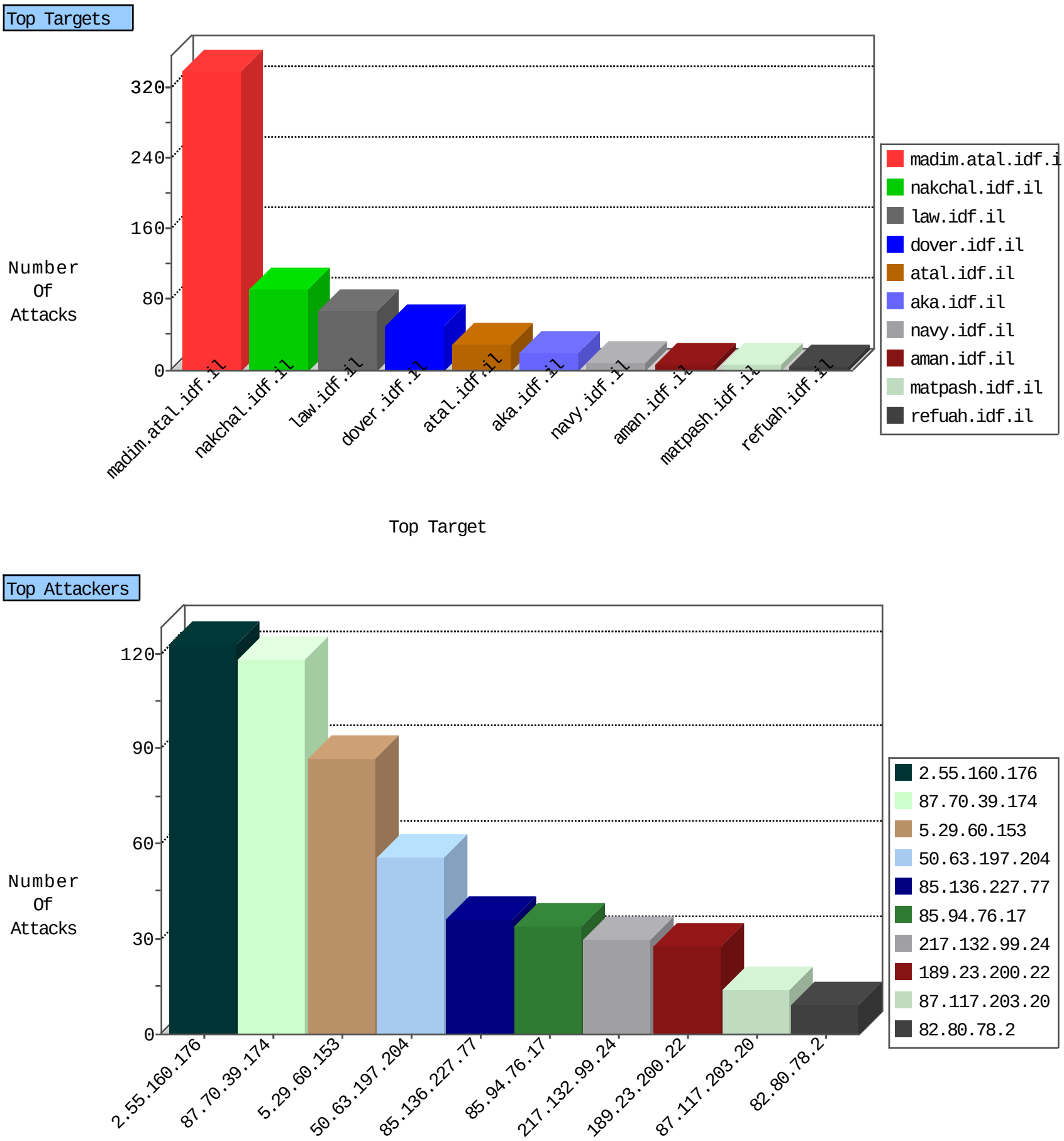
08-16-2016-19:04:06 to 08-16-2016-20:04:06

IDF Under Attack Daily Report



08-16-2016-19:04:06 to 08-16-2016-20:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.80.78.2	Israel	147.237.76.86	navy.idf.il	Black List	drop	9
91.92.120.134	Bulgaria	147.237.76.148	gqcenter.aka.idf.il	Black List	drop	1
93.158.200.118	Netherlands	147.237.76.201	e.atal.idf.il	Black List	drop	1
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
115.230.125.146	China	147.237.77.74	law.idf.il	JLM_Purple_Con_Limit_Http	drop	1

08-16-2016-19:04:06 to 08-16-2016-20:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
50.63.197.204	United States	147.237.76.31	nakchal.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
85.136.227.77	Spain	147.237.76.31	nakchal.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	11
87.117.203.20	United Kingdom	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
85.94.76.17	Croatia	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	6
189.23.200.22	Brazil	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	6
50.63.197.204	United States	147.237.76.31	nakchal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	6
50.63.197.204	United States	147.237.76.31	nakchal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
85.94.76.17	Croatia	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	5
85.136.227.77	Spain	147.237.76.31	nakchal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	5
189.23.200.22	Brazil	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	2

08-16-2016-19:04:06 to 08-16-2016-20:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
50.63.197.204	147.237.76.31	United States	nakchal.idf.il	SQL Injection - Select From	32
85.94.76.17	147.237.77.74	Croatia	law.idf.il	SQL Injection - Select From	21
85.136.227.77	147.237.76.31	Spain	nakchal.idf.il	SQL Injection - Select From	20
189.23.200.22	147.237.77.74	Brazil	law.idf.il	SQL Injection - Select From	19
87.117.203.20	147.237.77.233	United Kingdom	atal.idf.il	SQL Injection - Select From	8
132.74.95.19	147.237.77.170	Israel	maarachot.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
113.108.10.31	147.237.77.121	China	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
113.108.10.31	147.237.76.42	China	refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
95.86.124.12	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.109.152.144	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
62.210.88.186	147.237.77.74	France	law.idf.il	SERVER-WEBAPP backup access	1
24.153.127.135	147.237.72.156	United States	aman.idf.il	ET SCAN NMAP -sS window 1024	1
113.108.10.31	147.237.77.170	China	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
113.108.10.31	147.237.76.199	China	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
113.108.10.31	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
69.30.204.5	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
175.144.206.193	147.237.76.30	Malaysia	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
113.108.10.31	147.237.77.179	China	e.mazi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

08-16-2016-19:04:06 to 08-16-2016-20:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
217.132.99.24	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
46.19.86.195	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
217.132.99.24	Israel	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	6
87.106.184.160	Germany	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	6
194.114.146.227	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	6
46.19.86.165	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	4
109.253.198.221	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
149.56.223.104	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	3
85.130.223.95	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
176.13.241.61	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
191.96.249.18	Chile	147.237.0.200	m4u.idf.il	drop		drop	1
169.229.3.90	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
180.97.106.162	China	147.237.0.19	madim.atal.idf.il	drop	SAM rule	drop	1
176.13.3.41	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
180.97.106.162	China	147.237.76.30	himush.idf.il	drop	SAM rule	drop	1
176.13.23.151	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
180.97.106.162	China	147.237.76.38	e.e.meitav.idf.il	drop	SAM rule	drop	1
109.253.212.203	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
176.13.229.130	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
180.97.106.162	China	147.237.76.197	e.himush.idf.il	drop	SAM rule	drop	1

08-16-2016-19:04:06 to 08-16-2016-20:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.55.160.176	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	123
87.70.39.174	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	117
5.29.60.153	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	86
46.19.86.215	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
80.179.22.146	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 80.179.22.146	Block	3
46.19.85.6	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
213.87.145.130	Russian Federation	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 213.87.145.130	Block	3
82.81.4.131	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	3
176.13.3.70	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
217.132.42.251	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	2
2.53.51.81	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	2
46.116.25.124	Israel	147.237.77.176	matpash.idf.il	Parameter Type Violation searchText in www.cogat.idf.il/1043-he/cogat.aspx	Block	2
80.179.22.146	Israel	147.237.77.74	law.idf.il	Parameter Type Violation Master$Header1$ucHeaderSearch$txtSearch in www.mag.idf.il/602-4730-he/patzar.aspx	Block	2
74.91.23.166	United States	147.237.72.167	ishurim.aka.idf.i	Unauthorized URL Access to 147.237.72.167/	Block	1
31.184.234.145		147.237.77.233	atal.idf.il	PHP Attempt	Block	1
46.19.86.99	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
5.29.60.153	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtCaptcha in madim.atal.idf.il/login.aspx	Block	1
213.151.35.214	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 213.151.35.214	Block	1
87.70.39.174	Israel	147.237.0.19	madim.atal.idf.il	Untraceable SSL Sessions: Open Mode	None	1
74.91.23.166	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
31.184.234.145		147.237.77.233	atal.idf.il	Unauthorized URL Access to atal.idf.il/xmlrpc.php	Block	1
181.28.35.17	Argentina	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
80.179.22.146	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files	Block	1
5.29.78.184	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	1
87.71.5.166	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.139.1.16	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/faq.aspx	Block	1
37.142.207.141	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
192.114.105.254	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	1
80.246.130.226	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
5.29.123.202	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
157.55.39.24	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/rabanut/ general.aspx	Block	1
79.177.83.131	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
66.249.79.172	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
5.29.169.254	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
157.55.39.125	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
46.19.86.6	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
213.87.145.130	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/miluim/about.aspx	Block	1

08-16-2016-19:04:06 to 08-16-2016-20:04:06