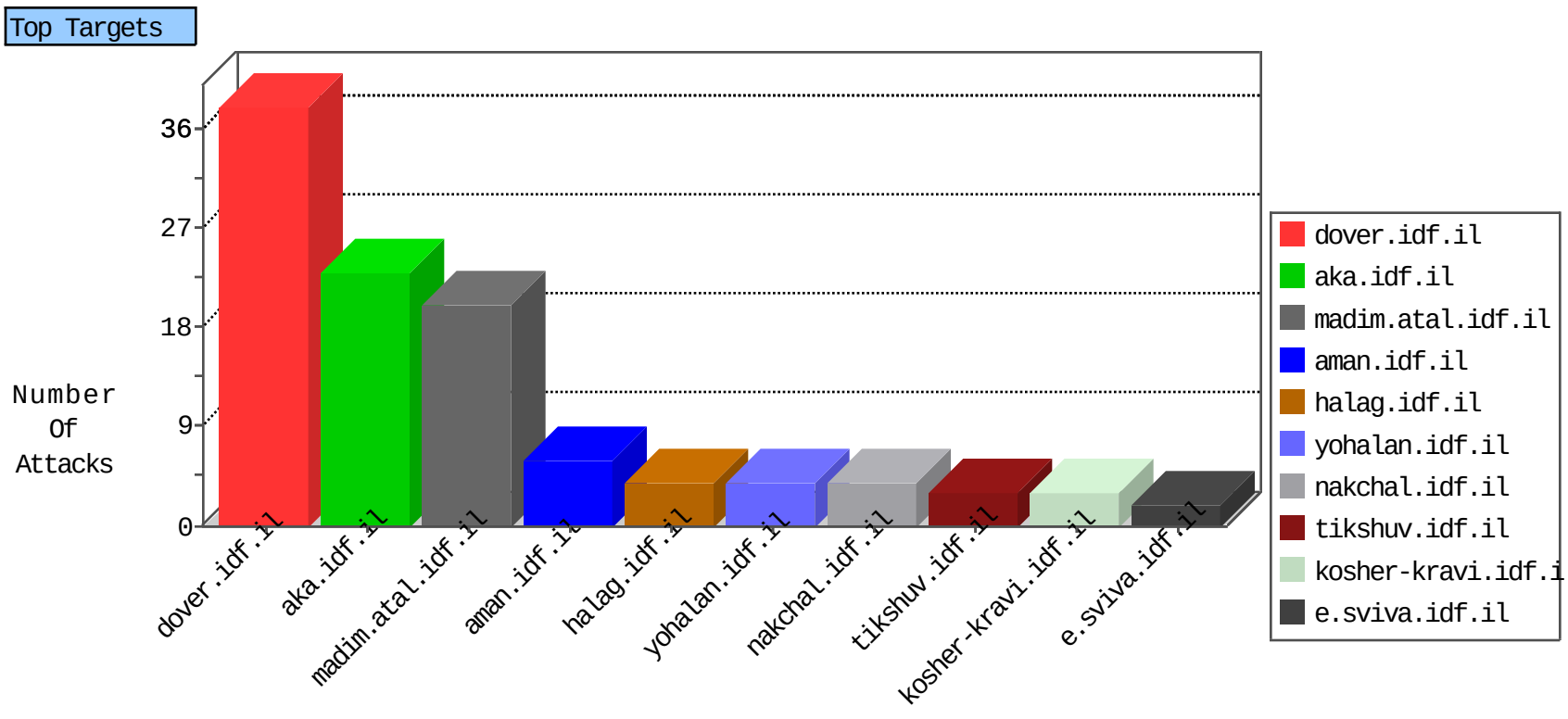
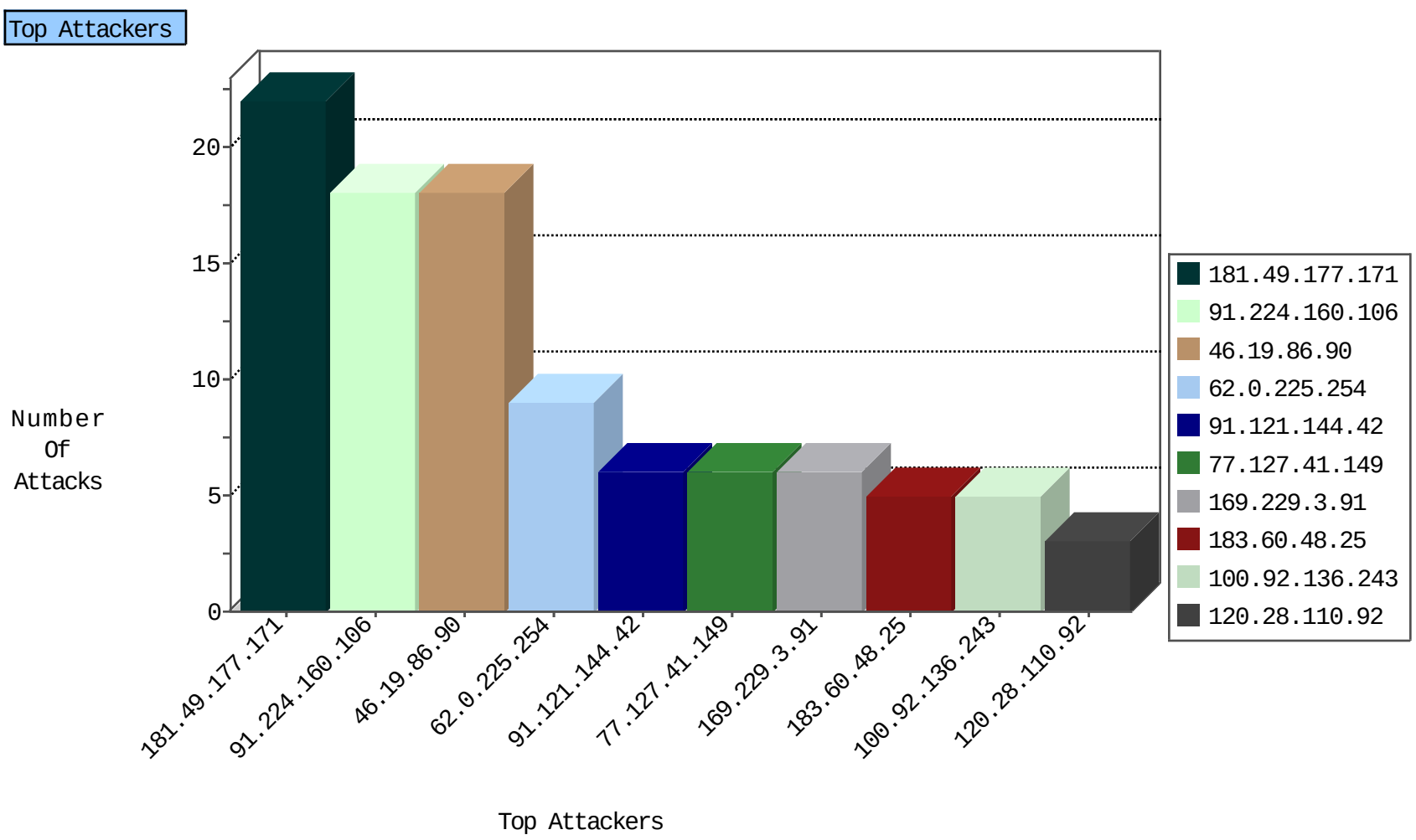
09-02-2016-08:04:08 to 09-02-2016-09:04:08

IDF Under Attack
Daily Report





09-02-2016-08:04:08 to 09-02-2016-09:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.164.170	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
185.94.111.1	Russian Federation	147.237.76.197	e.himush.idf.il	Black List	drop	1
185.94.111.1	Russian Federation	147.237.76.198	e.yohalan.idf.il	Black List	drop	1
181.49.177.171	Colombia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

09-02-2016-08:04:08 to 09-02-2016-09:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

09-02-2016-08:04:08 to 09-02-2016-09:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
91.121.144.42	147.237.72.166	France	aka.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	6
91.224.160.106	147.237.76.196	Netherlands	e.sviva.idf.il	ET SCAN Potential SSH Scan	2
91.224.160.106	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN Potential SSH Scan	2
91.224.160.106	147.237.76.148	Netherlands	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	2
91.224.160.106	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN Potential SSH Scan	2
183.60.48.25	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.195	147.237.8.46	Netherlands	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
37.26.148.247	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.224.160.106	147.237.76.199	Netherlands	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.76.176	Netherlands	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
208.100.26.228	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sS window 1024	1
91.224.160.106	147.237.76.86	Netherlands	navy.idf.il	ET SCAN Potential SSH Scan	1
192.223.90.236	147.237.76.176	Bolivia	test.ncore.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
91.224.160.106	147.237.76.42	Netherlands	refuah.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.76.31	Netherlands	nakchal.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1
146.185.146.112	147.237.77.226	Netherlands	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.76.99	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	1
91.224.160.106	147.237.76.201	Netherlands	e.atal.idf.il	ET SCAN Potential SSH Scan	1
2.55.146.220	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.224.160.106	147.237.76.198	Netherlands	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.76.177	Netherlands	ncore.idf.il	ET SCAN Potential SSH Scan	1
208.100.26.228	147.237.77.61	United States	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
91.224.160.106	147.237.76.44	Netherlands	e.refuah.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
91.224.160.106	147.237.76.34	Netherlands	yohalan.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	1

09-02-2016-08:04:08 to 09-02-2016-09:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
181.49.177.171	Colombia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
62.0.225.254	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	9
77.127.41.149	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
100.92.136.243		147.237.77.234	halag.idf.il	drop	First packet isn't SYN	drop	3
156.205.199.204	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
176.13.4.213	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
100.92.136.243		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
176.13.15.74	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.159	United States	147.237.0.200	m4u.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
169.229.3.91	United States	147.237.77.178	e.matpash.idf.il	drop	First packet isn't SYN	drop	1
87.153.88.132	Germany	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.77.205	prisha.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.44	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
183.129.160.229	China	147.237.77.19	law-forum.idf.il	drop	SAM rule	drop	1
169.229.3.91	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	1
93.174.93.99	Netherlands	147.237.0.33	idf.il	drop		drop	1
169.229.3.91	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.45	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
62.0.197.85	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
184.105.139.84	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
169.229.3.91	United States	147.237.76.31	nakchal.idf.il	drop	First packet isn't SYN	drop	1
93.174.93.99	Netherlands	147.237.0.35	akaws.idf.il	drop		drop	1
141.212.122.144	United States	147.237.0.200	m4u.idf.il	drop		drop	1
197.48.157.2	Egypt	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.77.121	e.navy.idf.il	drop	First packet isn't SYN	drop	1

09-02-2016-08:04:08 to 09-02-2016-09:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.90	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
120.28.110.92	Philippines	147.237.72.156	aman.idf.il	Illegal Byte Code Character in Method	Block	1
46.19.85.141	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1462-he/atal.aspx	Block	1
68.180.229.39	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in www.nakhal.idf.il/1109-he/nakhal.aspx	Block	1
120.28.110.92	Philippines	147.237.72.156	aman.idf.il	NULL Character in Method	Block	1
77.126.17.182	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
120.28.110.92	Philippines	147.237.72.156	aman.idf.il	Unauthorized Method POST for 147.237.72.156/	Block	1
66.102.8.232	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	1
80.246.133.126	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
37.26.146.232	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	1
180.76.15.144	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	Block	1
66.249.66.100	Israel	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to kosher-kravi.idf.il/templates/homepage/homepage.aspx	Block	1
109.65.88.14	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl55 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
37.142.202.25	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
185.24.207.100	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
66.249.66.203	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/templates/shared/usercontrols/navmenu/undefined	Block	1

09-02-2016-08:04:08 to 09-02-2016-09:04:08