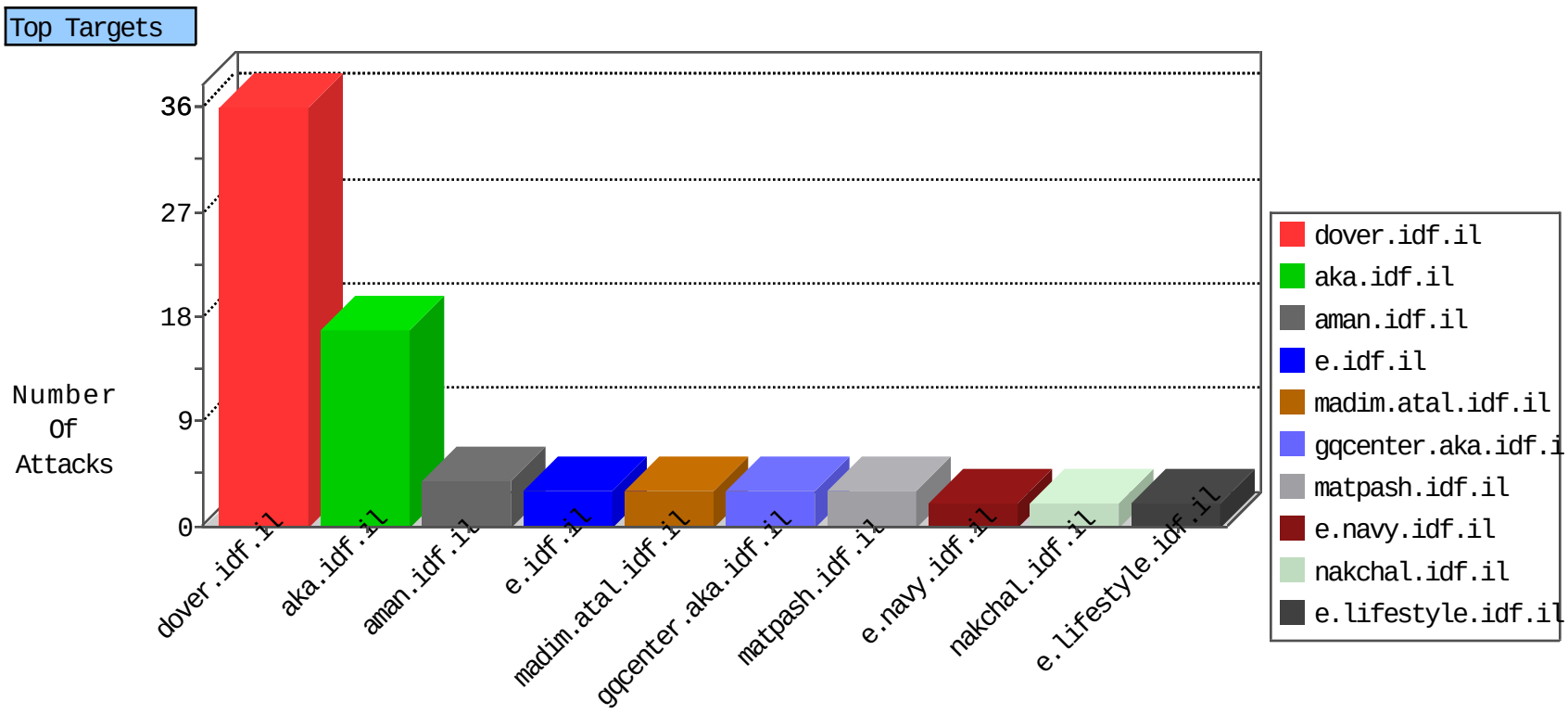
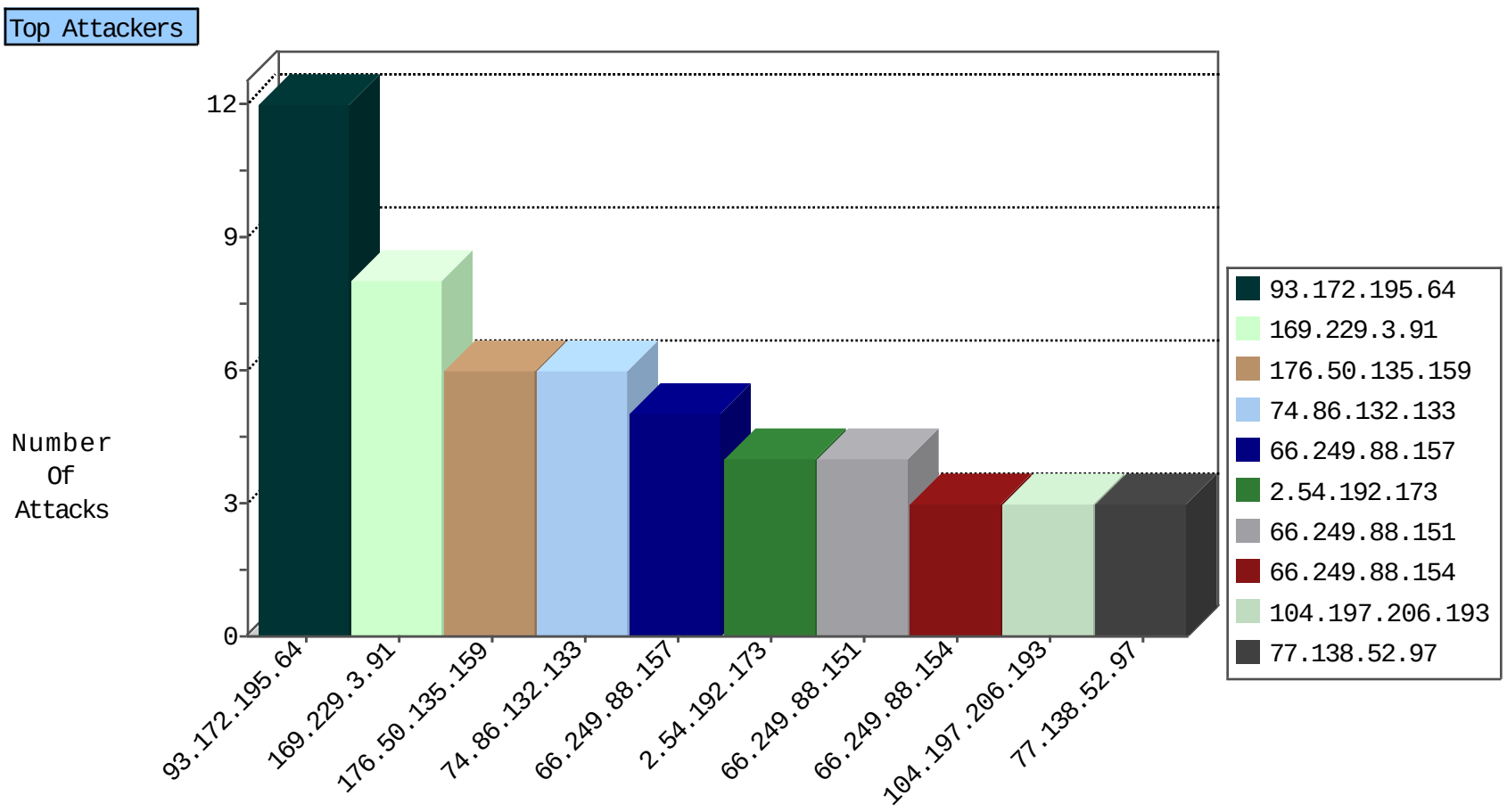
09-02-2016-06:04:01 to 09-02-2016-07:04:01

IDF Under Attack Daily Report





09-02-2016-06:04:01 to 09-02-2016-07:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
91.230.107.174	Russian Federation	147.237.76.196	e.sviva.idf.il	Black List	drop	1

09-02-2016-06:04:01 to 09-02-2016-07:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

09-02-2016-06:04:01 to 09-02-2016-07:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
201.238.202.219	147.237.8.45	Chile	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
88.249.106.23	147.237.76.177	Turkey	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
176.50.135.159	147.237.77.176	Russian Federation	matpash.idf.il	ET SCAN Potential SSH Scan	1
74.86.132.133	147.237.76.86	United States	navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
176.50.135.159	147.237.76.197	Russian Federation	e.himush.idf.il	ET SCAN Potential SSH Scan	1
74.86.132.133	147.237.72.217	United States	e.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
176.50.135.159	147.237.72.156	Russian Federation	aman.idf.il	ET SCAN Potential SSH Scan	1
74.86.132.133	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
122.72.53.188	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
45.56.98.154	147.237.76.202	United States	e.halag.idf.il	ET SCAN Potential SSH Scan	1
122.72.53.188	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
104.197.206.193	147.237.77.121	United States	e.navy.idf.il	ET SCAN NMAP -sS window 2048	1
104.197.206.193	147.237.8.46	United States	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
208.73.143.36	147.237.8.24	United States	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
104.128.144.131	147.237.72.217	Canada	e.idf.il	ET SCAN NMAP -f -sS	1
176.50.135.159	147.237.77.226	Russian Federation	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
74.86.132.133	147.237.77.216	United States	dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
176.50.135.159	147.237.76.201	Russian Federation	e.atal.idf.il	ET SCAN Potential SSH Scan	1
74.86.132.133	147.237.76.39	United States	mobile.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
176.50.135.159	147.237.76.148	Russian Federation	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
74.86.132.133	147.237.72.156	United States	aman.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
163.172.169.150	147.237.72.167	United Kingdom	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.83.242	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	1
122.72.53.188	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
45.33.116.208	147.237.8.28	United States	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
116.55.226.30	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
104.197.206.193	147.237.77.121	United States	e.navy.idf.il	ET SCAN NMAP -f -sS	1
219.87.191.219	147.237.76.42	Taiwan	refuah.idf.il	ET SCAN Potential SSH Scan	1
104.128.144.131	147.237.72.217	Canada	e.idf.il	ET SCAN NMAP -sS window 2048	1

09-02-2016-06:04:01 to 09-02-2016-07:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
2.54.192.173	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
66.249.88.157	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
213.57.181.237	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
66.249.88.151	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
183.129.160.229	China	147.237.0.35	akaws.idf.il	drop	SAM rule	drop	1
141.212.122.156	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
169.229.3.91	United States	147.237.8.50	e.tikshuv.idf.il	drop	First packet isn't SYN	drop	1
183.129.160.229	China	147.237.0.200	m4u.idf.il	drop	SAM rule	drop	1
169.229.3.91	United States	147.237.8.24	e.lifestyle.idf.il	drop	First packet isn't SYN	drop	1
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.72.14	dover.idf.il(old)	drop	First packet isn't SYN	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	147.237.8.27	e.madim.atal.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.76.176	test.ncore.idf.il	drop	First packet isn't SYN	drop	1
112.210.121.226	Philippines	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.8.45	e.eitan.idf.il	drop	First packet isn't SYN	drop	1
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.155	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
169.229.3.91	United States	147.237.8.46	e.chinuch.idf.il	drop	First packet isn't SYN	drop	1

09-02-2016-06:04:01 to 09-02-2016-07:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
93.172.195.64	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 93.172.195.64	Block	11
79.180.17.1	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	3
66.249.88.154	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
66.249.88.157	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
46.118.157.136	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1519-en/	Block	2
66.249.88.151	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
66.249.66.19	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/1130-he/אגף הטכנולוגיה והלוגיסטיקה.aspx	Block	1
207.46.13.176	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
87.71.29.74	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	1
66.249.76.116	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/main/sachar/tfasim.aspx	Block	1
24.68.6.134	Canada	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
157.55.39.150	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
70.72.138.204	Canada	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/favicon.ico	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/	Block	1
66.249.83.248	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
157.55.39.175	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/homepage/	Block	1
66.249.69.72	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/1/3251.pdf	Block	1
93.172.195.64	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	1
66.249.64.112	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/idkonim/pages/24112010usaid.aspx	Block	1
204.79.180.0	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/main/	Block	1
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
66.249.76.70	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/.well-known/apple-app-site-association	Block	1
128.232.110.28	United Kingdom	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	1
66.249.64.150	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/kamlar/news/על אף שאינו נחשב סטודנט על פי קובץ הוראות הקריאה לשמ"פ, רשאי להגיש בקשה למדור זל ת"ם.	Block	1
204.79.180.233	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/default.aspx	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
66.249.76.115	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 66.249.76.115	Block	1
5.164.77.229	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/kiosk/printablekiosk.aspx	Block	1
128.232.110.28	United Kingdom	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1

09-02-2016-06:04:01 to 09-02-2016-07:04:01