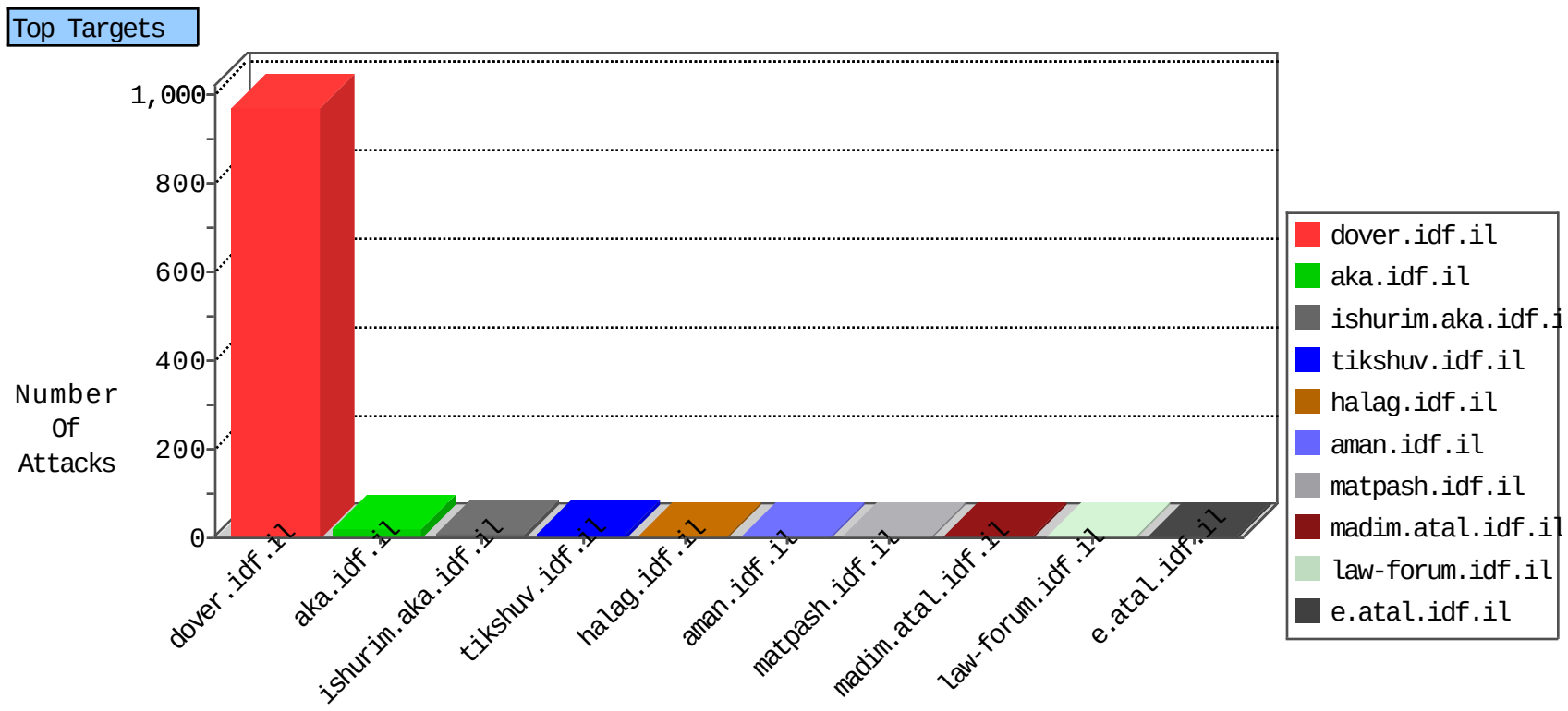
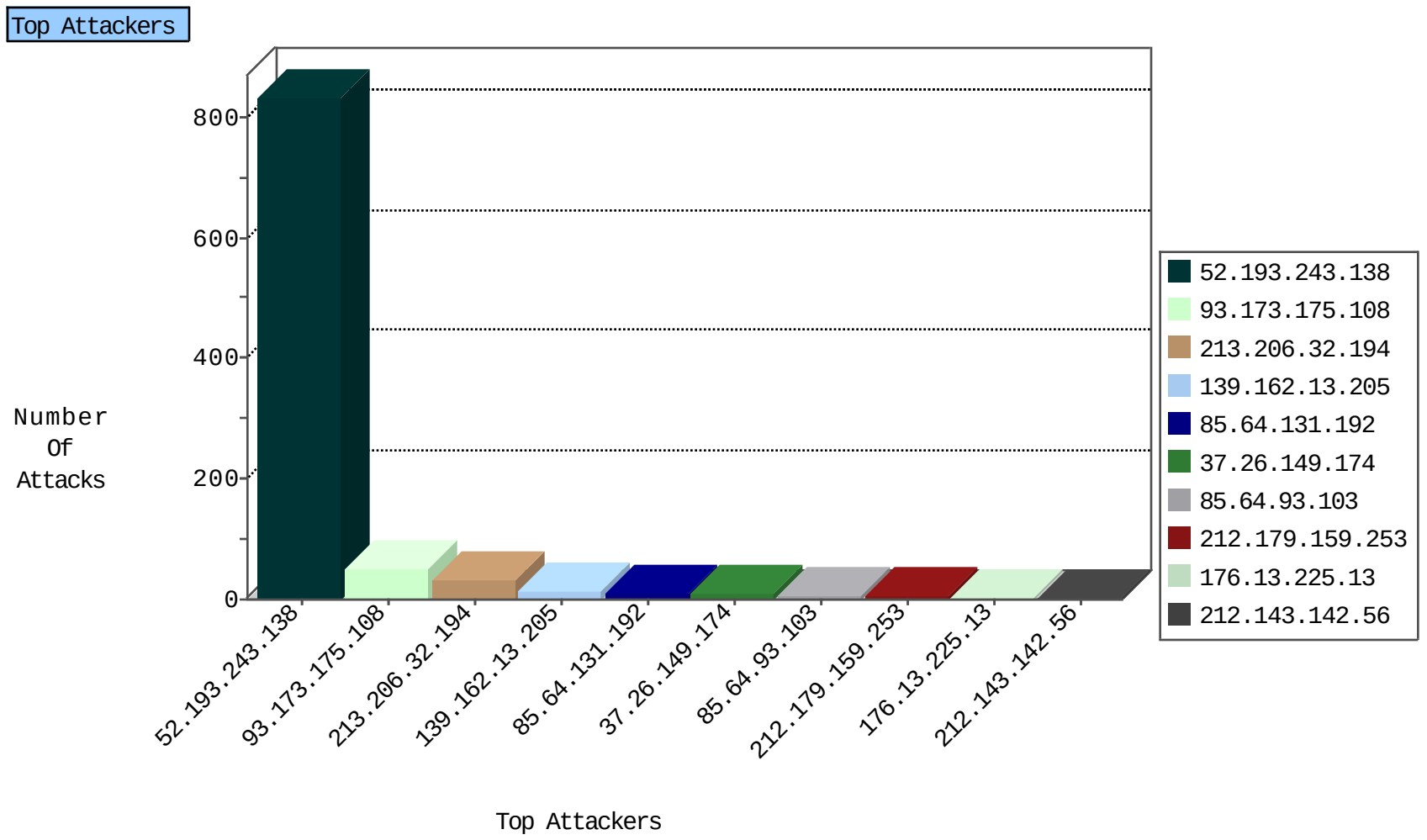
08-24-2016-08:04:09 to 08-24-2016-09:04:09

IDF Under Attack Daily Report

Top Targets



Top Attackers



08-24-2016-08:04:09 to 08-24-2016-09:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
93.173.175.108	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	52
85.64.131.192	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	10
2.53.50.64	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
2.55.139.52	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
104.156.245.113	United States	147.237.76.201	e.atal.idf.il	Black List	drop	1
185.94.111.1	Russian Federation	147.237.76.44	e.refuah.idf.i	Black List	drop	1
93.158.200.166	Netherlands	147.237.76.201	e.atal.idf.il	Black List	drop	1
46.19.86.80	Israel	147.237.77.216	dover.idf.il	Black List	drop	1

08-24-2016-08:04:09 to 08-24-2016-09:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
195.154.209.110	France	147.237.77.176	matpash.idf.il	C1000016: HTTP: administrator in URI	Permit	2
89.248.172.16	Netherlands	147.237.76.176	test.ncore.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
151.80.41.169	France	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Permit	1

08-24-2016-08:04:09 to 08-24-2016-09:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
91.201.236.158	147.237.77.19	Ukraine	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
80.246.136.43	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
66.249.66.238	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	1
8.26.94.207	147.237.0.16	Canada	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
193.201.225.138	147.237.76.196	Ukraine	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
133.242.4.52	147.237.76.202	Japan	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
91.236.246.40	147.237.76.31	Russian Federation	nakchal.idf.il	ET DROP Dshield Block Listed Source	1
91.224.160.106	147.237.0.17	Netherlands	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.158	147.237.77.19	Ukraine	law-forum.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
80.246.130.206	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
12.68.215.78	147.237.76.198	United States	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
199.203.68.10	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
193.201.225.138	147.237.72.217	Ukraine	e.idf.il	ET SCAN NMAP -sS window 1024	1
117.135.131.60	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.76.30	Netherlands	himush.idf.il	ET SCAN Potential SSH Scan	1

08-24-2016-08:04:09 to 08-24-2016-09:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
52.193.243.138	Japan	147.237.77.216	dover.idf.il	drop	SAM rule	drop	831
213.206.32.194	Uzbekistan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
37.26.149.174	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
139.162.13.205	Singapore	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	7
139.162.13.205	Singapore	147.237.72.167	ishurim.aka.idf.il	drop	SAM rule	drop	7
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
176.13.225.13	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
144.139.140.64	Australia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
109.253.213.81	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	1
82.102.168.38	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
137.116.71.170	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
8.26.94.207	Canada	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
185.125.4.222	Poland	147.237.77.234	halag.idf.il	drop	SAM rule	drop	1
82.102.168.38	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	1
192.168.173.102		147.237.77.216	dover.idf.il	drop		drop	1
109.201.154.145	Netherlands	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
216.218.206.74	United States	147.237.0.33	idf.il	drop		drop	1
201.238.202.219	Chile	147.237.8.14	e.orchot.idf.il	drop	SAM rule	drop	1
109.253.209.194	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1

08-24-2016-08:04:09 to 08-24-2016-09:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
85.64.93.103	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
212.179.159.253	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 212.179.159.253	Block	3
2.53.23.85	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
66.249.69.224	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.224	Block	3
66.249.76.112	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.76.112	Block	2
64.137.244.235	Canada	147.237.72.166	aka.idf.il	Admin Blocking	Block	1
85.64.68.213	Israel	147.237.77.170	maarachot.idf.il	PHP Attempt	Block	1
66.249.76.106	Israel	147.237.72.166	aka.idf.il	Unknown Parameter itemid in www.aka.idf.il/kamlar/gallery/showpicture.asp	None	1
37.142.104.207	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl77 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
157.55.39.37	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
80.246.136.188	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
64.137.244.235	Canada	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/admin/cms_wysiwyg/directive/index/	Block	1
212.179.159.253	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/8/	Block	1
85.64.68.213	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/wp-login.php	Block	1
40.77.169.100	United States	147.237.77.216	dover.idf.il	Illegal Byte Code Character in URL /1500-en/dover.aspx#011200	Block	1
182.73.13.118	India	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
84.95.208.20	Israel	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to www.kosher-kravi.idf.il/default.aspx	Block	1
66.102.9.54	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
2.53.129.237	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.76.112	Israel	147.237.72.166	aka.idf.il	Unknown Parameter SearchParam in www.aka.idf.il/main/sachar/	None	1
46.19.85.171	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
207.46.13.18	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
84.95.208.20	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
66.249.64.24	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/templates/shared/usercontrols/headerupper/	Block	1
37.46.38.42	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
87.69.17.105	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	1
75.82.117.252	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/giyus/	Block	1
46.19.85.187	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012 ources/images/innerpage/goback.gif	Block	1
207.46.13.118	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/modiin/sip_storage/files/4/68624	Block	1
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/piwik.php	Block	1
37.46.38.42	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
147.236.238.22	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
80.246.130.148	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtLastName in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	1

08-24-2016-08:04:09 to 08-24-2016-09:04:09