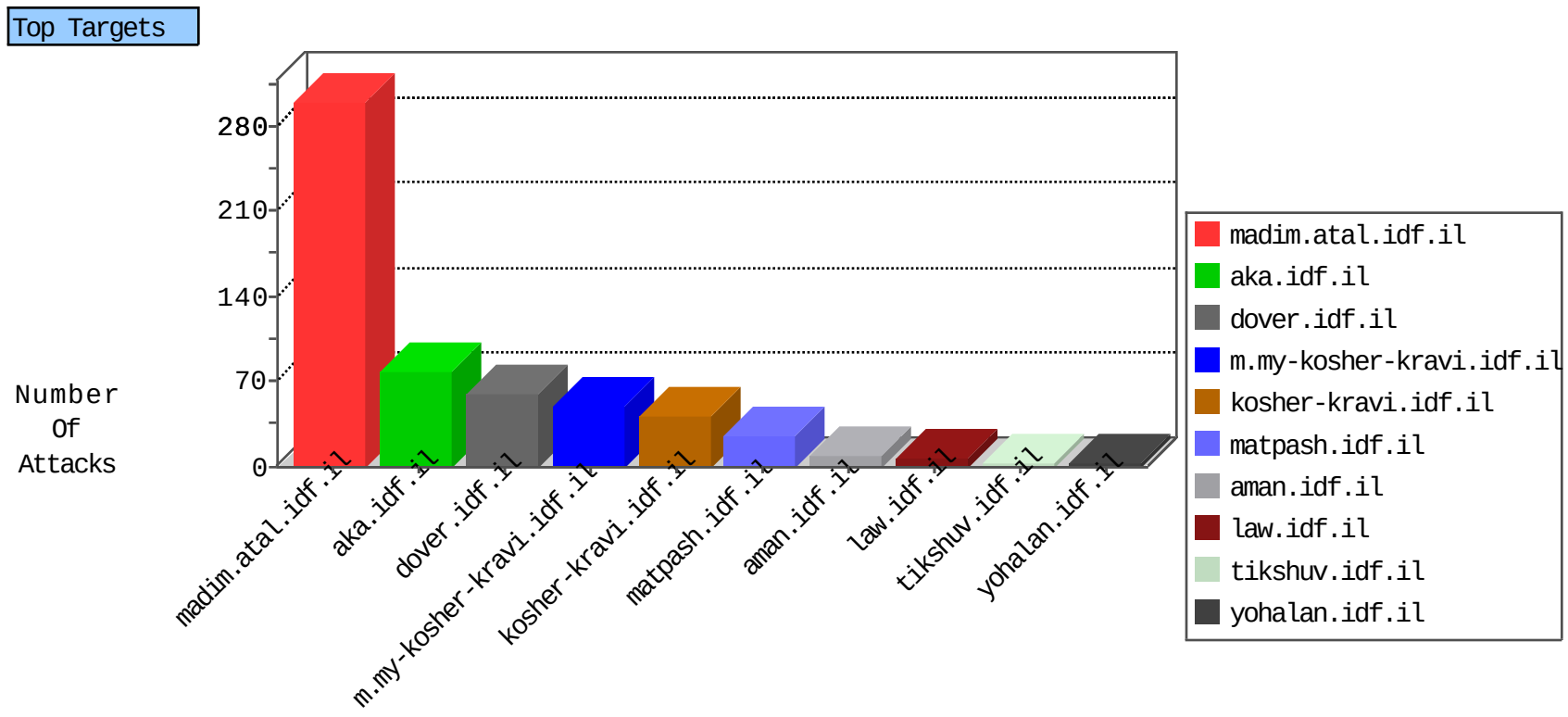
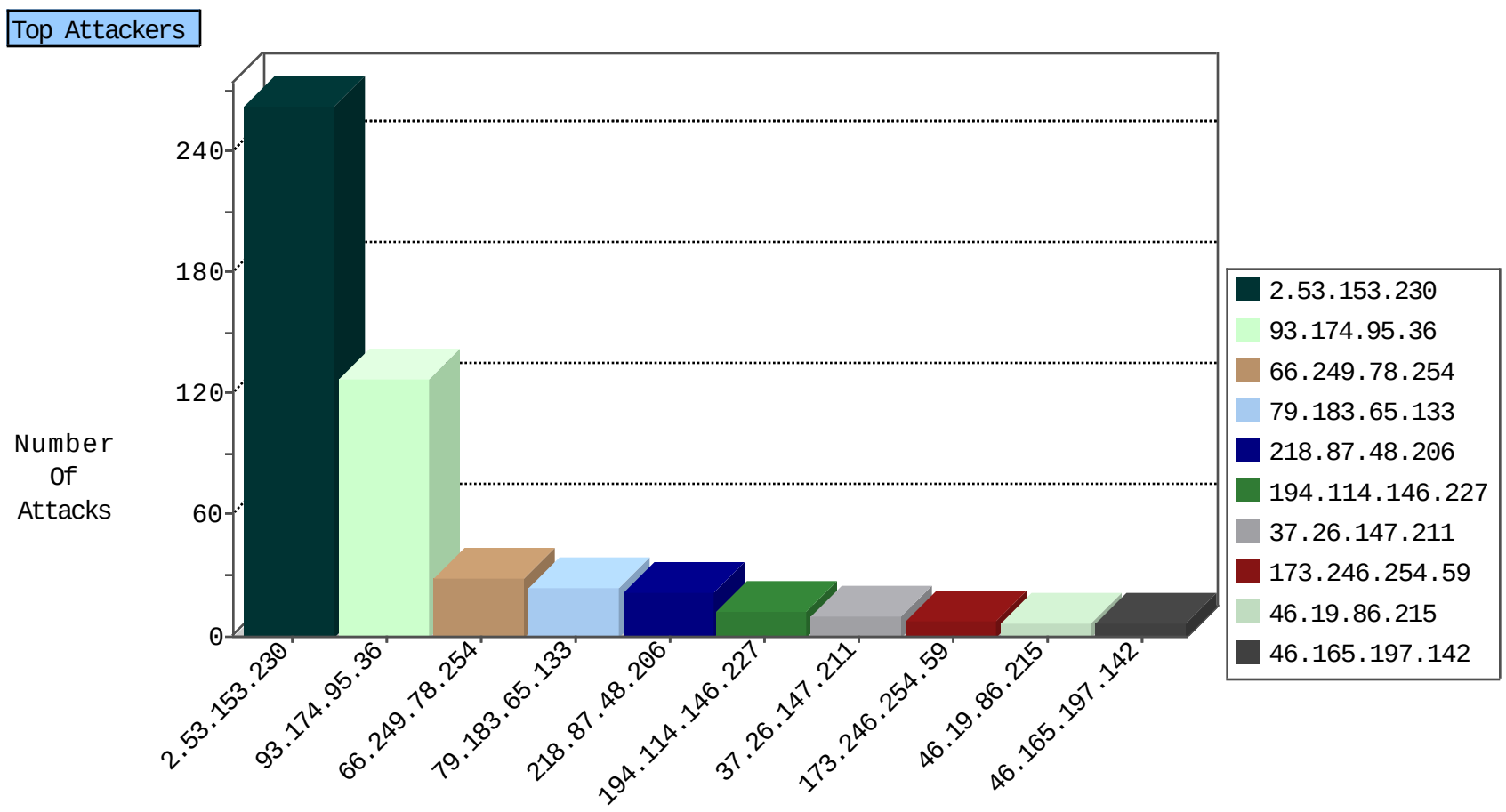
08-17-2016-00:04:09 to 08-17-2016-01:04:09

IDF Under Attack Daily Report

Top Targets



Top Attackers



08-17-2016-00:04:09 to 08-17-2016-01:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.78.254	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	6549
82.80.78.2	Israel	147.237.77.176	matpash.idf.il	Black List	drop	4
66.249.78.252	Israel	147.237.0.19	madim.atal.idf.il	TCP handshake violation, first packet not syn	drop	2
93.158.200.96	Netherlands	147.237.76.34	yohalan.idf.il	Black List	drop	1
89.248.171.2	Netherlands	147.237.76.44	e.refuah.idf.il	Black List	drop	1
89.248.171.2	Netherlands	147.237.76.197	e.himush.idf.il	Black List	drop	1
27.105.237.142	Taiwan	147.237.76.30	himush.idf.il	Black List	drop	1
89.248.174.4	Netherlands	147.237.76.202	e.halag.idf.il	Black List	drop	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	HTTP-Misc-BadBlue-Dir-Trave-2	dest-reset	1
82.80.217.70	Israel	147.237.72.156	aman.idf.il	Black List	drop	1

08-17-2016-00:04:09 to 08-17-2016-01:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
93.174.95.36	Netherlands	147.237.0.17	m.my-kosher-kravi.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	47
93.174.95.36	Netherlands	147.237.0.15	kosher-kravi.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	42
93.174.95.36	Netherlands	147.237.77.216	dover.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	24
93.174.95.36	Netherlands	147.237.0.19	madim.atal.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	13
46.165.197.142	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	4
46.165.197.142	Germany	147.237.76.147	chinuch.aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
93.174.95.36	Netherlands	147.237.0.17	m.my-kosher-kravi.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	1

08-17-2016-00:04:09 to 08-17-2016-01:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.120.122.219	147.237.77.216	Israel	dover.idf.il	Xenu Link Sleuth User Agent	2
93.174.95.36	147.237.0.17	Netherlands	m.my-kosher-kravi.idf.il	ET WEB_SERVER Muieblackcat scanner	1
91.201.236.158	147.237.0.34	Ukraine	tikshuv.idf.il	ET SCAN NMAP -sS window 2048	1
85.99.242.253	147.237.0.33	Turkey	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
66.249.78.254	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	1
202.65.138.2	147.237.76.147	India	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
180.97.75.130	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
115.77.205.224	147.237.0.33	Vietnam	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
91.201.236.158	147.237.0.34	Ukraine	tikshuv.idf.il	ET SCAN NMAP -sS window 3072	1
91.201.236.158	147.237.0.34	Ukraine	tikshuv.idf.il	ET SCAN NMAP -f -sS	1
85.93.5.66	147.237.77.178	United Arab Emirates	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
66.249.76.51	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	1
219.159.88.94	147.237.0.35	China	akaws.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
185.29.11.182	147.237.76.39	Latvia	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
180.97.75.130	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

08-17-2016-00:04:09 to 08-17-2016-01:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.183.65.133	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
194.114.146.227	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	12
173.246.254.59	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
213.57.112.56	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	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
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
89.139.188.90	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	2
87.135.246.197	Germany	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
180.97.106.162	China	147.237.77.234	halag.idf.il	drop	SAM rule	drop	1
141.212.122.27	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
177.67.92.12	Brazil	147.237.0.35	akaws.idf.il	drop		drop	1
192.168.173.102		147.237.77.216	dover.idf.il	drop		drop	1
141.212.122.28	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
180.97.106.161	China	147.237.76.31	nakchal.idf.il	drop	SAM rule	drop	1
109.253.222.229	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
31.13.110.107	Ireland	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	1
180.97.106.162	China	147.237.8.14	e.orchot.idf.il	drop	SAM rule	drop	1
141.212.122.17	United States	147.237.0.200	m4u.idf.il	drop		drop	1
176.13.243.172	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	1
180.97.106.162	China	147.237.77.19	law-forum.idf.il	drop	SAM rule	drop	1
141.212.122.18	United States	147.237.0.200	m4u.idf.il	drop		drop	1
176.13.248.24	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1

08-17-2016-00:04:09 to 08-17-2016-01:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.153.230	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	263
218.87.48.206	China	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 218.87.48.206	Block	15
37.26.147.211	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	9
46.19.86.215	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	7
218.87.48.206	China	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	6
31.154.81.34	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
189.177.54.131	Mexico	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/giyus/general/	Block	2
46.19.86.41	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
176.119.89.93	Ukraine	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	2
109.64.21.114	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
46.116.32.19	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
66.147.244.101	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	1
192.243.55.135	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/giyus/kadatz	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/megurim/_blank	Block	1
192.243.55.137	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/faq.asp?catid=38227	Block	1
192.243.55.131	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/templates/shared/usercontrols/headerupper	Block	1
176.13.0.169	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.64.142	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/edim/yoman/enlarge.asp	Block	1
218.87.48.206	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/index.asp	Block	1
192.243.55.135	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ishurim/exampcert	Block	1
37.26.147.211	Israel	147.237.0.19	madim.atal.idf.i	Parameter Type Violation ctl00$ContentPlaceHolder1$txtCaptcha in madim.atal.idf.il/mobile/login.aspx	Block	1
192.243.55.129	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/1181-he/navy.aspx?pagenum=2&lang=he&sortdir=asc	Block	1
77.138.155.102	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/forms.aspx	Block	1
192.243.55.138	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/giyus/kadatz	Block	1
2.53.27.246	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
192.243.55.132	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/general.aspx?catid=59269&docid=59488	Block	1
66.249.64.182	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/page.asp	Block	1
192.243.55.135	United States	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/templates/shared/usercontrols/headerupper	Block	1
37.26.149.178	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
192.243.55.130	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/kadatz	Block	1
192.243.55.138	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/templates/shared/usercontrols/headerupper/	Block	1
192.243.55.133	United States	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/templates/shared/usercontrols/headerupper/	Block	1
180.76.15.136	China	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to eitan.aka.idf.il/templates/shared/usercontrols/headerupper/	Block	1
66.249.78.69	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage/files/6/שקופית13/	Block	1
192.243.55.136	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in www.aka.idf.il/kamlar/klali/default.asp	None	1
37.142.238.47	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
192.243.55.130	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/general.aspx?catid=59331&docid=64447	Block	1
141.226.162.183	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$tfasimSignAll in www.aka.idf.il/main/sachar/payslips.aspx	None	1
46.116.38.30	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
192.243.55.134	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/shared/usercontrols/headerupper	Block	1
186.90.233.26	Venezuela	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
66.249.78.130	Israel	147.237.76.30	himush.idf.il	Unauthorized URL Access to www.tech.atal.idf.il/templates/shared/usercontrols/navmenu/	Block	1
192.243.55.137	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/giyus/kadatz	Block	1
46.19.85.77	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1256-he/refuah.aspx	Block	1
192.243.55.131	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/tizmoret/gallery	Block	1
172.56.17.124	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/ishurim/main/	Block	1

08-17-2016-00:04:09 to 08-17-2016-01:04:09