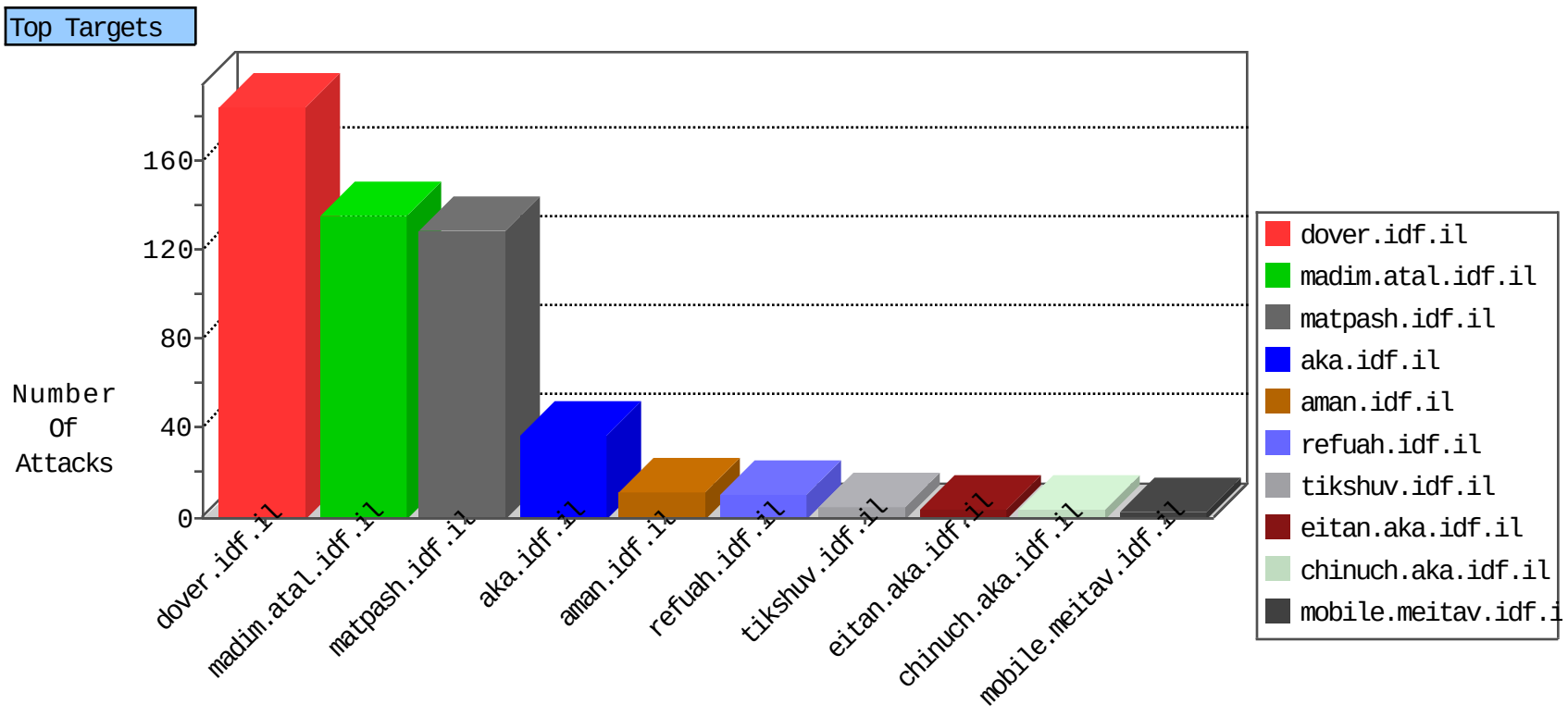
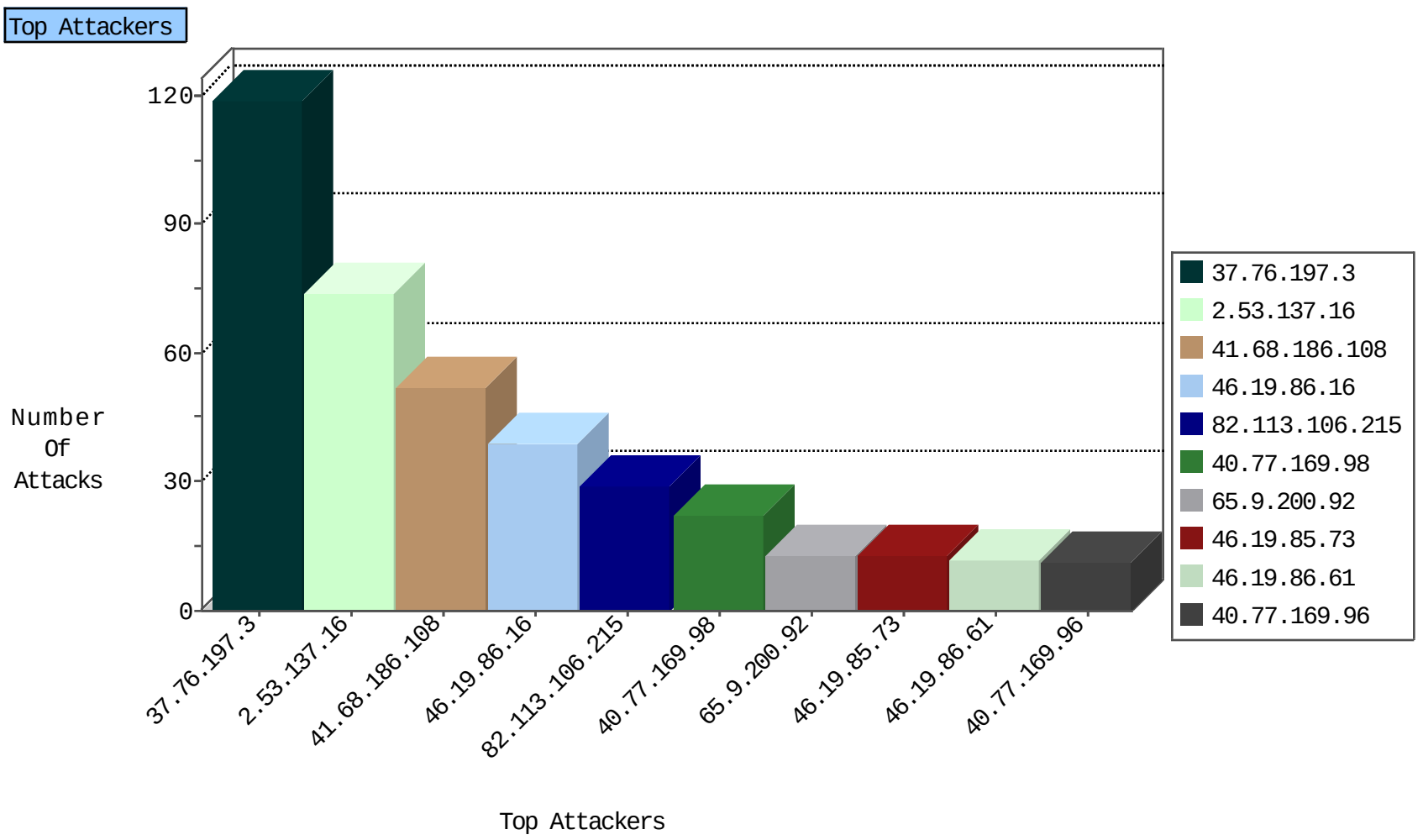
08-24-2016-18:04:02 to 08-24-2016-19:04:02

IDF Under Attack Daily Report





08-24-2016-18:04:02 to 08-24-2016-19:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.72	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	69
109.253.223.193	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6
109.67.183.248	Israel	147.237.72.166	aka.idf.il	Invalid L4 Header Length	drop	4
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
95.90.230.71	Germany	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
116.227.66.166	China	147.237.76.200	eitan.aka.idf.il	Black List	drop	2
31.168.133.226	Israel	147.237.77.216	dover.idf.il	Black List	drop	2
185.94.111.1	Russian Federation	147.237.76.147	chinuch.aka.idf.il	Black List	drop	1
63.135.128.2	United States	147.237.76.147	chinuch.aka.idf.il	Black List	drop	1
185.94.111.1	Russian Federation	147.237.76.196	e.sviva.idf.il	Black List	drop	1
206.40.102.223	United States	147.237.76.147	chinuch.aka.idf.il	Black List	drop	1
124.173.113.45	China	147.237.77.176	matpash.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
221.131.64.85	China	147.237.76.200	eitan.aka.idf.il	Black List	drop	1
109.67.183.248	Israel	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	1

08-24-2016-18:04:02 to 08-24-2016-19:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
178.137.160.45	Ukraine	147.237.76.42	refuah.idf.il	C1000016: HTTP: administrator in URI	Permit	8
144.76.8.132	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2

08-24-2016-18:04:02 to 08-24-2016-19:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
91.125.184.101	147.237.77.176	United Kingdom	matpash.idf.il	Tehila - Perl LWP with fake user agent	3
91.125.184.101	147.237.77.216	United Kingdom	dover.idf.il	Tehila - Perl LWP with fake user agent	2
91.125.184.101	147.237.77.74	United Kingdom	law.idf.il	Tehila - Perl LWP with fake user agent	2
5.255.90.133	147.237.76.30	Netherlands	himush.idf.il	ET SCAN NMAP -sS window 1024	1
139.162.13.205	147.237.8.45	Singapore	e.eitan.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
119.93.87.90	147.237.0.33	Philippines	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
104.193.252.231	147.237.76.44	United States	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
93.172.25.68	147.237.77.233	Israel	atal.idf.il	ET SCAN NMAP -sA (2)	1
58.218.204.245	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
5.255.90.133	147.237.76.86	Netherlands	navy.idf.il	ET SCAN NMAP -sS window 1024	1
5.255.90.133	147.237.76.39	Netherlands	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
186.114.248.160	147.237.0.33	Colombia	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
119.93.87.90	147.237.77.235	Philippines	sviva.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
117.27.240.24	147.237.8.45	China	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.195	147.237.76.39	Netherlands	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
58.218.204.245	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
5.255.90.133	147.237.76.44	Netherlands	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
199.168.138.170	147.237.76.34	United States	yohalan.idf.il	ET SCAN Potential SSH Scan	1

08-24-2016-18:04:02 to 08-24-2016-19:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
37.76.197.3	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	119
41.68.186.108	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	52
82.113.106.215	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
40.77.169.98	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	14
46.19.85.73	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
65.9.200.92	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
46.19.86.61	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
40.77.169.96	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	11
40.77.169.98	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	8
40.77.169.102	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	6
176.13.0.55	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
2.54.192.16	Israel	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
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
109.253.130.78	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	2
31.13.102.109	Ireland	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	2
31.13.102.119	Ireland	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	2
109.253.142.51	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
176.13.233.226	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	1
92.124.239.7	Russian Federation	147.237.0.200	m4u.idf.il	drop		drop	1
77.40.0.13	Russian Federation	147.237.0.33	idf.il	drop		drop	1
109.253.158.3	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	1
85.130.190.227	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	1
176.13.237.157	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
95.90.230.71	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
85.130.190.227	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
31.13.100.112	Ireland	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	1
176.13.243.245	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
85.143.143.235	Russian Federation	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
183.129.160.229	China	147.237.77.227	e.hamaz.idf.il	drop	SAM rule	drop	1
109.253.135.199	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	1
85.130.137.229	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
176.13.4.19	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
92.124.239.7	Russian Federation	147.237.0.35	akaws.idf.il	drop		drop	1
85.130.190.227	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.137.16	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	74
46.19.86.16	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	39
46.19.85.163	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
46.19.86.219	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
66.249.69.224	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.224	Block	3
46.19.85.236	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
87.71.45.42	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.25	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
40.77.169.101	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
176.13.241.193	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
189.26.155.49	Brazil	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
40.77.167.8	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
66.249.64.163	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1721	Block	1
131.253.25.241	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
80.246.130.236	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
46.121.86.209	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
192.198.151.43	Europe	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/miluim/templates/home.asp	Block	1
40.77.169.97	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
93.172.25.68	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush	Block	1
66.249.69.14	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	1
157.55.39.194	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
5.102.242.67	Israel	147.237.77.226	www.chamatz.aka.idf.il	Distributed Unauthorized URL Access on www.chamatz.aka.idf.il/templates/homepage/homepage.aspx	Block	1
84.110.145.111	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl75 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
62.219.142.11	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/דשבישר	Block	1
195.154.41.132	France	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to 147.237.76.200/	Block	1
109.65.28.180	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
46.19.86.72	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
159.220.74.2	United Kingdom	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 159.220.74.2	Block	1
31.223.176.126	Palestinian Territory, Occupied	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/	Block	1
85.130.137.229	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/	Block	1
66.102.9.105	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 66.102.9.105	Block	1
212.129.62.79	France	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/	Block	1
109.65.41.45	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1517-he/atal.aspx	Block	1
66.249.76.106	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;docId in www.aka.idf.il/navy/navy/general.aspx	None	1
37.26.149.220	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/text.css	Block	1
87.71.44.249	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/watch	Block	1
66.102.9.105	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/pniotanswer.aspx	Block	1
109.253.156.12	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.139.129.178	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
46.120.159.103	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyusעירונירעננה	Block	1

08-24-2016-18:04:02 to 08-24-2016-19:04:02