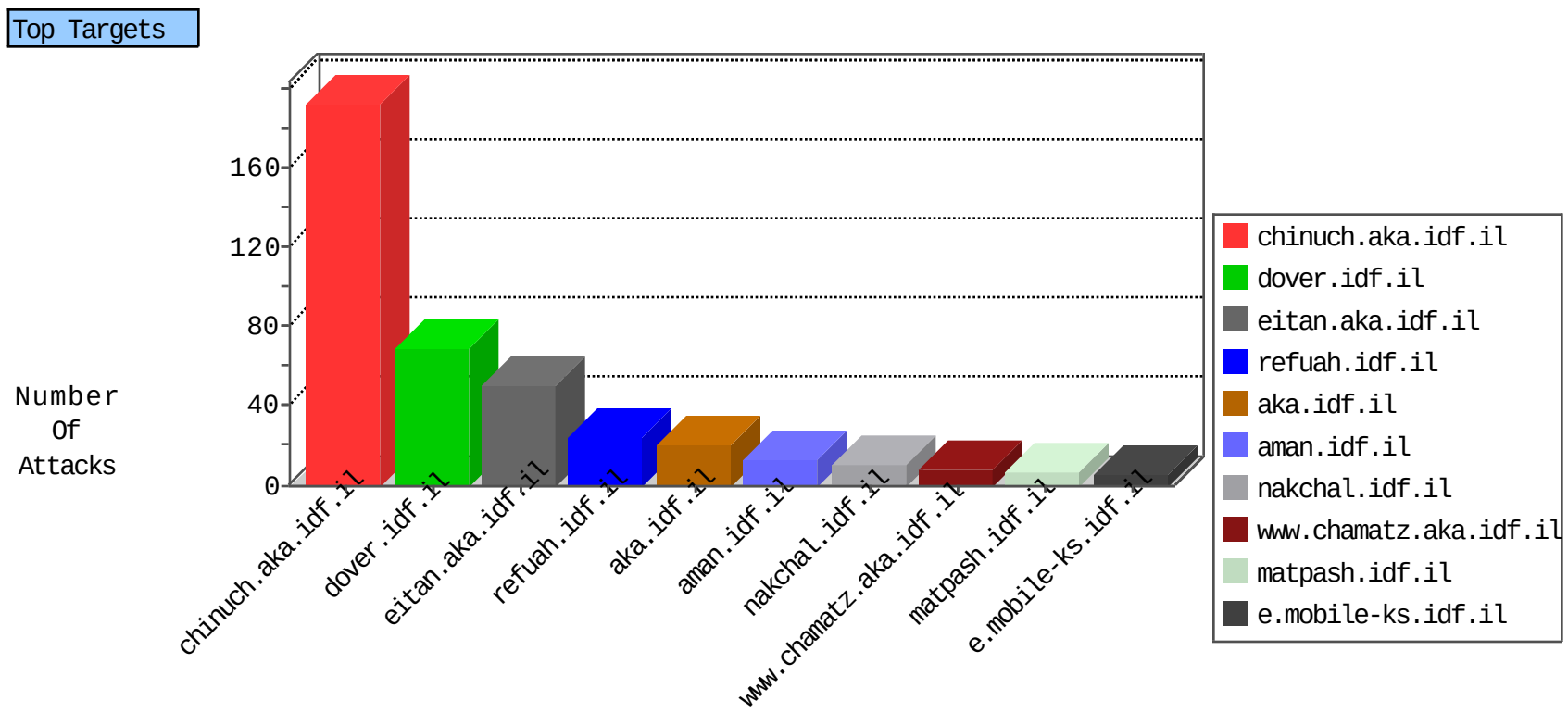
09-27-2016-01:33:21 to 09-27-2016-02:33:21

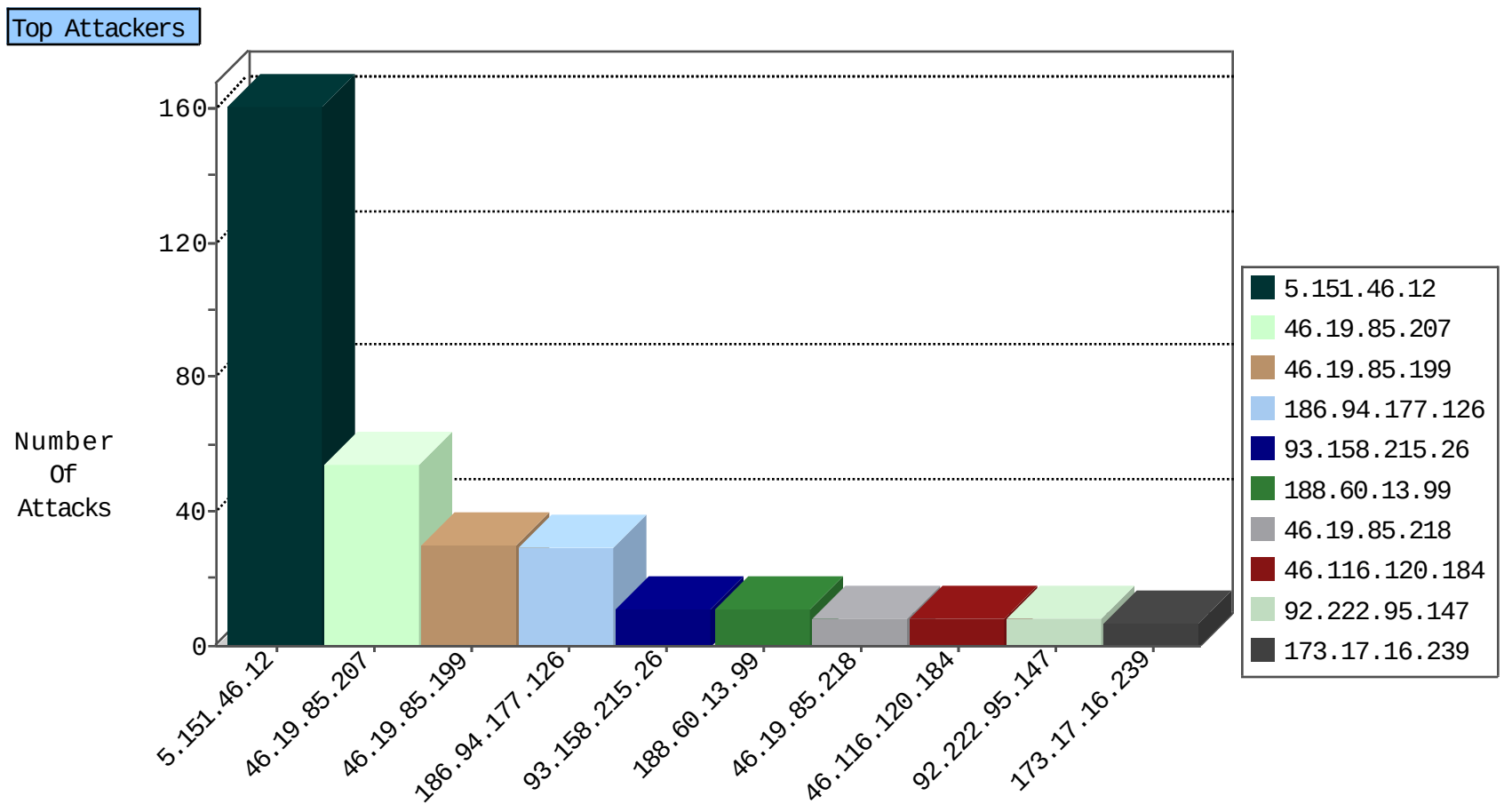
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

09-27-2016-01:33:21 to 09-27-2016-02:33:21

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
93.174.94.235	Netherlands	147.237.76.148	gqcenter.aka.idf.il	Black List	drop	1
195.93.222.124	Poland	147.237.77.212	e.dover.idf.il	L4 Source or Dest Port Zero	drop	1
93.174.94.235	Netherlands	147.237.76.201	e.atal.idf.il	Black List	drop	1
104.238.147.65	United States	147.237.76.39	mobile.meitav.idf.il	Black List	drop	1
104.238.147.65	United States	147.237.76.86	navy.idf.il	Black List	drop	1

09-27-2016-01:33:21 to 09-27-2016-02:33:21

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

09-27-2016-01:33:21 to 09-27-2016-02:33:21

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
109.75.43.41	147.237.72.14	Armenia	dover.idf.il(old)	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	3
108.250.76.145	147.237.76.199	United States	e.nakchal.idf.il	ET SCAN NMAP -sS window 4096	1
103.207.36.31	147.237.72.167	Vietnam	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
218.24.113.2	147.237.0.35	China	akaws.idf.il	ET SCAN NMAP -sS window 3072	1
66.249.64.105	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	1
188.136.237.251	147.237.76.196	Iran, Islamic Republic of	e.sviva.idf.il	ET SCAN NMAP -sS window 3072	1
36.72.228.72	147.237.77.19	Indonesia	law-forum.idf.il	ET SCAN NMAP -sS window 2048	1
188.136.237.251	147.237.76.196	Iran, Islamic Republic of	e.sviva.idf.il	ET SCAN NMAP -f -sS	1
161.106.88.6	147.237.76.196	France	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
161.106.88.6	147.237.0.15	France	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
139.162.187.89	147.237.77.121	United States	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
103.207.37.81	147.237.77.226	Vietnam	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
218.24.113.2	147.237.0.35	China	akaws.idf.il	ET SCAN NMAP -sS window 4096	1
78.129.171.173	147.237.76.197	United Kingdom	e.himush.idf.il	ET SCAN Potential SSH Scan	1
201.73.83.242	147.237.8.46	Brazil	e.chinuch.idf.il	ET SCAN NMAP -sS window 3072	1
36.72.228.72	147.237.77.19	Indonesia	law-forum.idf.il	ET SCAN NMAP -sS window 3072	1
188.136.237.251	147.237.76.196	Iran, Islamic Republic of	e.sviva.idf.il	ET SCAN NMAP -sS window 2048	1
36.72.228.72	147.237.77.19	Indonesia	law-forum.idf.il	ET SCAN NMAP -f -sS	1
179.43.144.18	147.237.77.176	Switzerland	matpash.idf.il	ET SCAN Potential SSH Scan	1
161.106.88.6	147.237.0.16	France	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
149.255.108.192	147.237.0.17	United Kingdom	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
139.162.187.89	147.237.76.196	United States	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1

09-27-2016-01:33:21 to 09-27-2016-02:33:21

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
5.151.46.12	United Kingdom	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	127
46.19.85.207	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	39
5.151.46.12	United Kingdom	147.237.76.147	chinuch.aka.idf.il	SYN Attack		monitor	28
186.94.177.126	Venezuela	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.85.199	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
46.19.85.199	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
173.17.16.239	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.207	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.166.186.249	Netherlands	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	6
5.151.46.12	United Kingdom	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
186.94.177.126	Venezuela	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
46.19.85.207	Israel	147.237.76.200	eitan.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.199	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.199	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
186.94.177.126	Venezuela	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
93.158.215.26	Netherlands	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
93.158.215.26	Netherlands	147.237.76.147	chinuch.aka.idf.il	SYN Attack		monitor	4
186.94.177.126	Venezuela	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
46.19.85.207	Israel	147.237.76.200	eitan.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
93.158.215.26	Netherlands	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
176.13.245.194	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
186.94.177.126	Venezuela	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
185.32.179.241	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
188.60.13.99	Switzerland	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	3
207.46.13.56	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
176.13.230.129	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
188.60.13.99	Switzerland	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	2
188.60.13.99	Switzerland	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
82.209.144.110	Sweden	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
216.244.66.243	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
92.222.95.147	France	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	2
188.60.13.99	Switzerland	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	2
46.19.86.78	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
92.222.95.147	France	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	2
188.60.13.99	Switzerland	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
46.120.25.138	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
92.222.95.147	France	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
2.53.151.38	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
46.19.85.218	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
169.229.3.91	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
46.19.85.126	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
109.253.135.32	Israel	147.237.0.19	madim.atal.idf.il	drop	First packet isn't SYN	drop	1
92.222.95.147	France	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	1
46.19.86.78	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.169	United States	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
24.4.50.221	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	1
2.53.175.175	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
72.9.148.10	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
46.19.86.3	Israel	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1

09-27-2016-01:33:21 to 09-27-2016-02:33:21

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.218	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	7
46.116.120.184	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	4
46.116.120.184	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 46.116.120.184	Block	3
66.108.189.205	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en	Block	3
183.232.175.2	China	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/rabanut/	Block	2
66.249.76.62	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 66.249.76.62	Block	1
66.249.66.182	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8944-he/refuah.aspx	Block	1
66.249.69.232	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_img.asp	Block	1
46.120.25.138	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.76.62	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1778	Block	1
66.249.66.235	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 66.249.66.235	Block	1
204.79.180.146	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/miluim/templates/home.asp	Block	1
66.249.75.4	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 66.249.75.4	Block	1
66.102.9.5	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
66.249.79.114	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/sip_storage/files/3/68633...	Block	1
66.249.66.235	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/idkonim/pages/25012011masaiyot.aspx	Block	1
220.181.108.170	China	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/sip_storage/files/3/size338x0/1613.jpg	Block	1
66.249.75.12	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 66.249.75.12	Block	1
66.249.79.118	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/apple-app-site-association	Block	1
66.249.69.224	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_img.asp	Block	1
46.116.120.184	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/sip_storage/files/2/	Block	1
66.249.75.32	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-20405-he/idfgdover.aspx	Block	1
66.249.64.169	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1779	Block	1
24.251.42.207	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
89.138.98.163	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/size100x0/sip_storage	Block	1
66.249.69.224	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_text.asp	Block	1
46.120.25.138	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 46.120.25.138 (Open Mode)	None	1

09-27-2016-01:33:21 to 09-27-2016-02:33:21