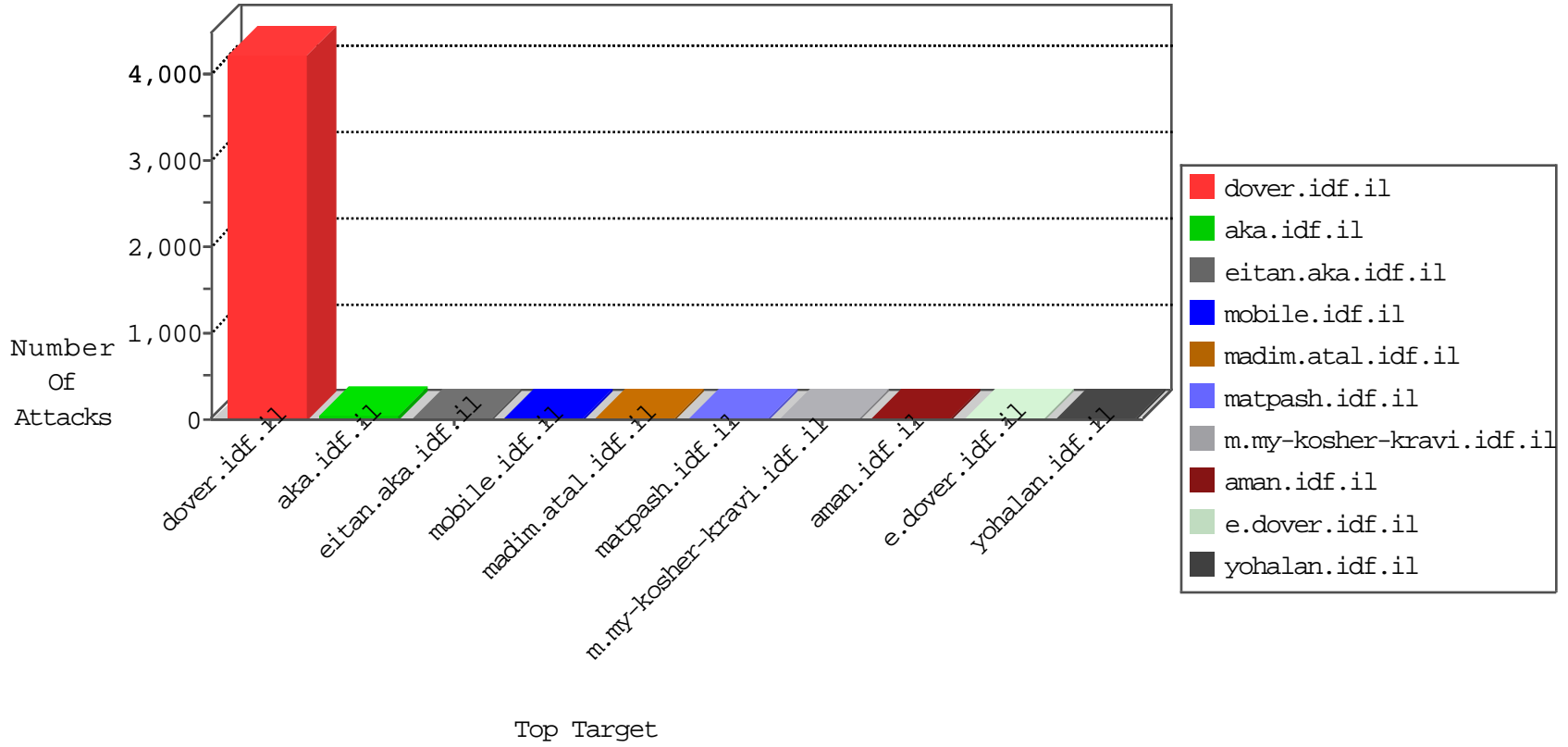




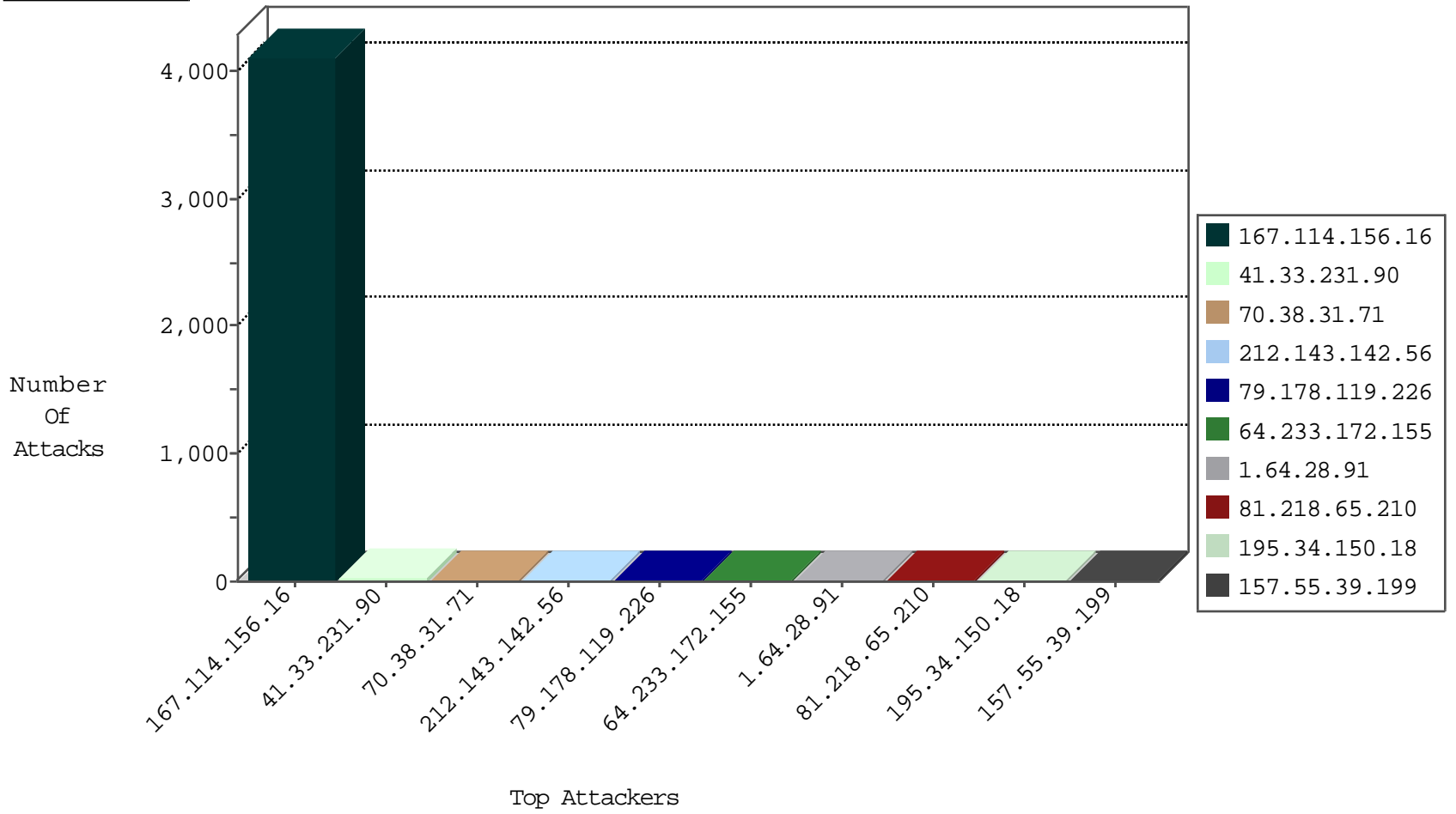
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	Block_Tp_Web_In	drop	4116
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
81.218.65.210	Israel	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	3
184.105.139.124	United States	147.237.77.170	maarachot.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.104	United States	147.237.0.19	madim.atal.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.72	United States	147.237.77.61	e.cogat.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.116	United States	147.237.77.205	prisha.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.92	United States	147.237.8.50	e.tikshuv.idf.il	Block_Ntp_All_Net	drop	1
184.164.195.29	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
184.105.139.104	United States	147.237.0.33	idf.il	Block_Ntp_All_Net	drop	1
184.105.139.76	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.120	United States	147.237.77.243	mobile.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.92	United States	147.237.77.227	e.hamaz.idf.il	Block_Ntp_All_Net	drop	1
184.164.195.68	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
184.105.139.116	United States	147.237.0.35	akaws.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.84	United States	147.237.77.233	atal.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.124	United States	147.237.72.156	aman.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.96	United States	147.237.77.176	matpash.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.68	United States	147.237.72.167	ishurim.aka.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.116	United States	147.237.77.121	e.navy.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.92	United States	147.237.0.16	ny-kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
------------------	------------------	----------------	------	-----------	---------------	-------

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
122.141.236.69	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
106.186.113.67	147.237.77.233	Japan	atal.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.158	147.237.0.17	Ukraine	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 3072	1
122.141.236.69	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.158	147.237.0.17	Ukraine	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 4096	1
61.178.42.242	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	34
70.38.31.71	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	15
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
79.178.119.226	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
64.233.172.155	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
1.64.28.91	Hong Kong	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
157.55.39.199	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
130.193.51.91	Russian Federation	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.65.18	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
216.218.206.71	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.205	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
106.186.113.132	Japan	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.247.240	United States	147.237.0.33	idf.il	drop		drop	1
141.212.122.200	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
5.22.135.230	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
216.218.206.111	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.206	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.116.9.112	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
189.188.233.84	Mexico	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.201	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
74.82.47.31	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
5.39.222.159	Netherlands	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
189.188.233.84	Mexico	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
141.212.122.202	United States	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.82.47.42	United States	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
5.39.222.159	Netherlands	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.139.84	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
141.212.122.197	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.203	United States	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
37.142.244.228	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.103	United States	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.198	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.224.21	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	3
149.78.87.36	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	2
194.187.168.202	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
65.55.213.24	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
184.105.139.67	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to 147.237.77.243/	Block	1
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/smalim/webresource.axd	Block	1
207.46.13.32	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/coordinatingaza/terminalsnap/pages/karny.aspx	Block	1
66.249.64.137	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/smalim/resources/scripts/mootools.ext.js	Block	1
185.77.91.113	Turkey	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/index.php	Block	1
66.249.78.246	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/smalim/resources/styles/masterstyle.css	Block	1
207.46.13.72	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/watch	Block	1
157.55.39.42	United States	147.237.72.166	aka.idf.il	Unknown Parameter 4f9c0c80 in www.aka.idf.il/main/home/default.aspx	None	1
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
194.114.146.227	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 194.114.146.227	Block	1
68.180.230.45	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9682-he/refuah.aspx	Block	1
157.55.39.234	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/templates/homepage/homepage.aspx	Block	1
194.114.146.227	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage/files/4/	Block	1
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	1
5.39.222.159	Netherlands	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	1
180.76.15.17	China	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/smalim/resources/scripts/generalfunctions.js	Block	1