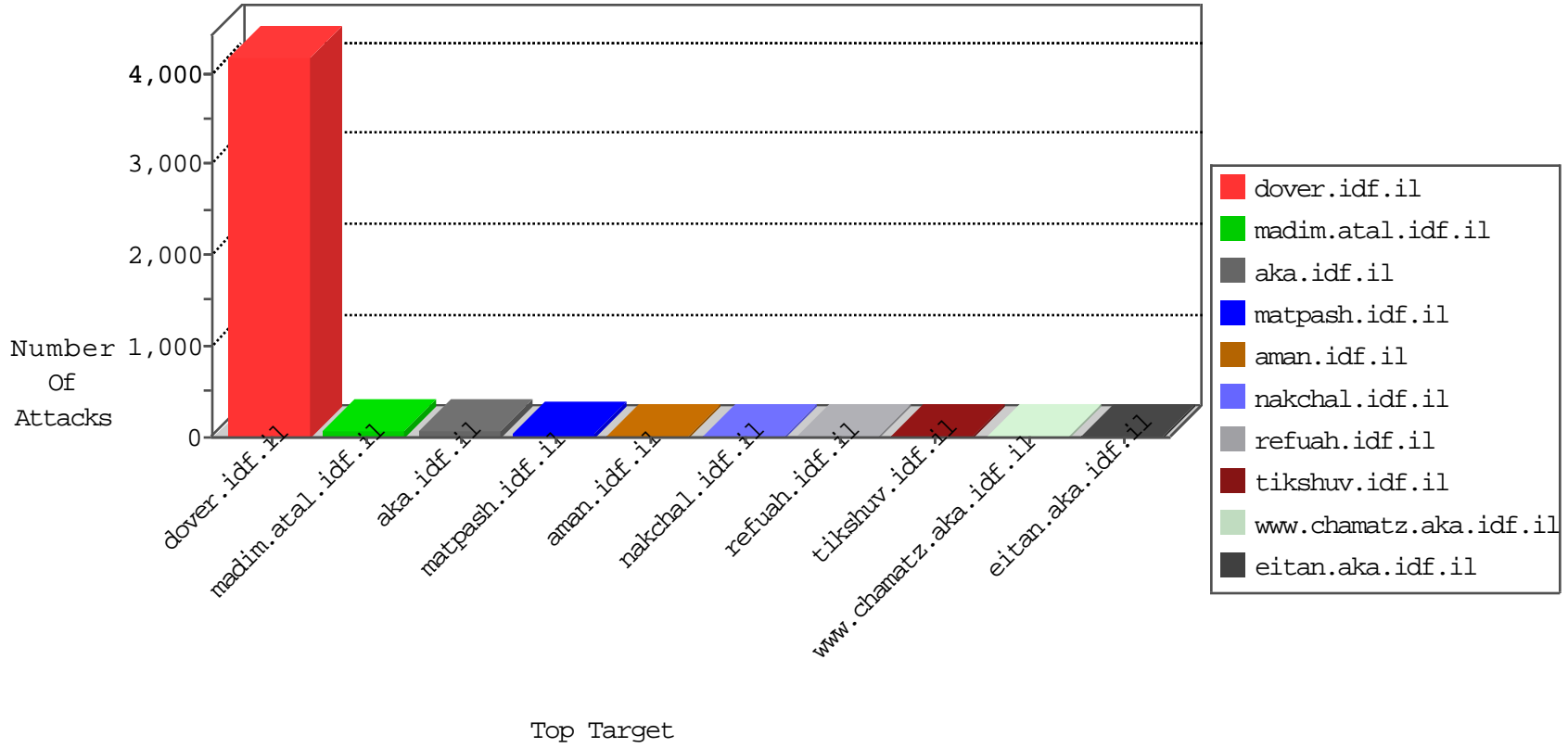


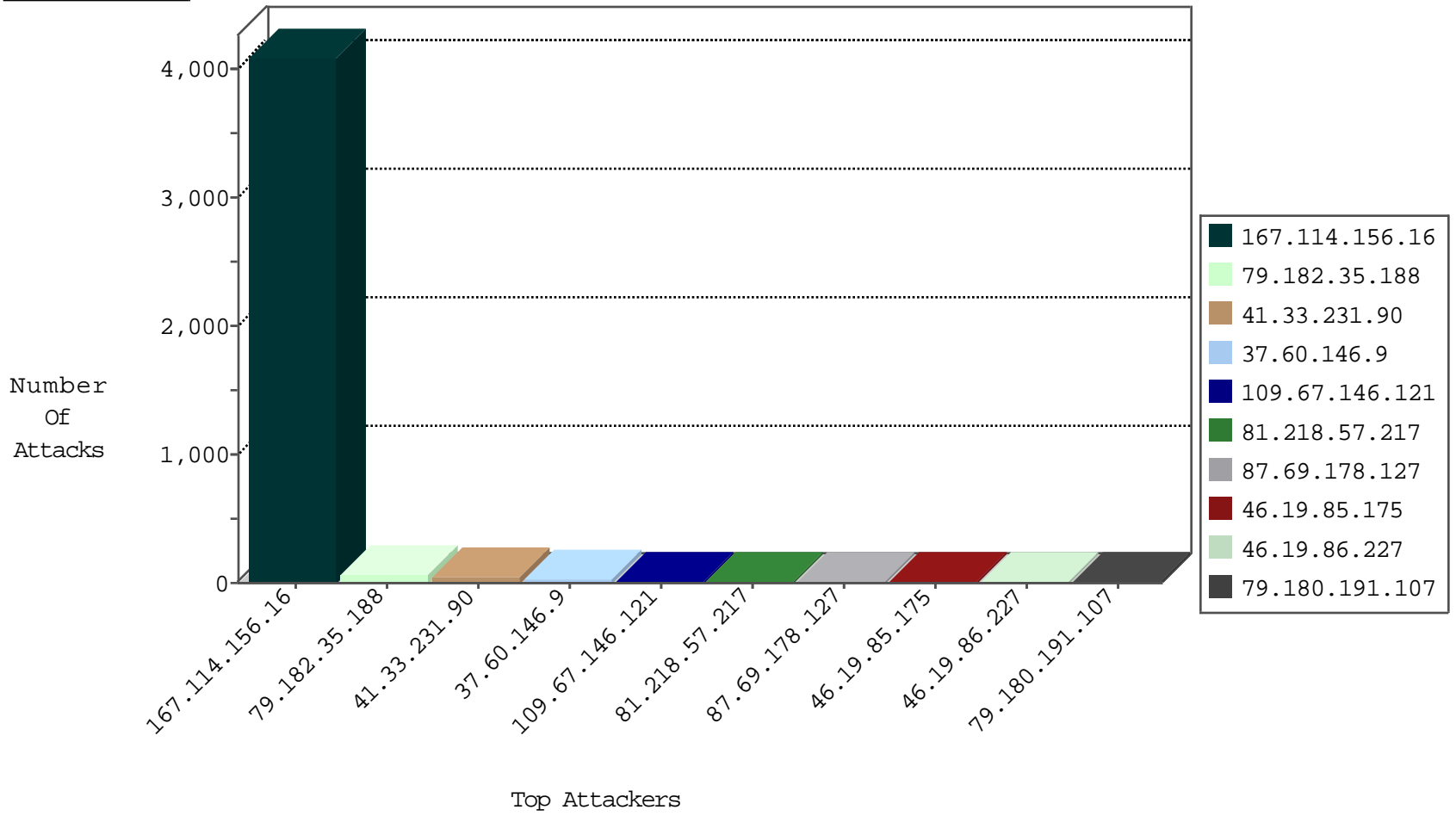
# IDF Under Attack Daily Report



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_Ip_Web_In	drop	4092
81.218.65.210	Israel	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	3
134.147.203.115	Germany	147.237.77.19	law-forum.idf.il	Block_Ntp_All_Net	drop	2
184.105.139.102	United States	147.237.0.35	akaws.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.118	United States	147.237.8.24	e.lifestyle.idf.il	Block_Ntp_All_Net	drop	1
104.255.70.247	United States	147.237.0.16	my-kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.70	United States	147.237.8.27	e.madim.atal.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.122	United States	147.237.77.205	prisha.idf.il	Block_Ntp_All_Net	drop	1
104.255.70.247	United States	147.237.0.200	m4u.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.82	United States	147.237.8.28	e.mobile-ks.idf.il	Block_Ntp_All_Net	drop	1
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.144	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	5
144.76.12.75	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
144.76.12.75	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
66.249.66.184	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1

## 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
91.201.236.155	147.237.72.217	Ukraine	e.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
218.107.34.5	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
195.216.176.244	147.237.77.121	Latvia	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.155	147.237.72.217	Ukraine	e.idf.il	ET SCAN NMAP -sS window 1024	1
82.166.184.187	147.237.77.121	Israel	e.navy.idf.il	ET SCAN NMAP -sS window 3072	1
218.107.34.5	147.237.0.16	China	ny-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
195.216.176.244	147.237.77.233	Latvia	atal.idf.il	ET SCAN NMAP -sS window 1024	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	36
37.60.146.9	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	26
109.67.146.121	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
46.19.85.175	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.86.227	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	9
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
87.69.178.127	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
37.60.146.9	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
79.179.36.182	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
84.95.208.20	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	6
87.69.178.127	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
81.218.57.217	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence		monitor	4
185.3.144.26	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
85.250.14.59	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
2.53.10.109	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.70.5.5	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
2.53.190.76	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.179.56.131	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
178.255.215.87	France	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.148.141	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.109.30.137	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
79.180.5.1	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.135.244	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
81.218.57.217	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.182.34.104	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.107.102.131	Hungary	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	3
106.184.3.122	Japan	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
46.117.19.15	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
79.180.191.107	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
79.177.193.60	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
81.218.57.217	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	2
79.180.191.107	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
81.218.57.217	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
92.111.43.134	Netherlands	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
79.180.191.107	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
207.46.13.136	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
81.218.57.217	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
87.69.141.248	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
159.226.95.66	China	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.205	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
176.13.16.8	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
5.102.254.174	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
144.168.45.117	United States	147.237.72.156	aman.idf.il	drop	SAM rule	drop	1
141.212.122.192	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.112	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
104.148.44.145	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
184.105.247.216	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
87.69.141.248	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
162.144.41.122	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.206	United States	147.237.76.200	eitan.aka.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
79.182.35.188	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	67
176.13.20.238	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
92.111.43.134	Netherlands	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
190.58.253.35	Trinidad and Tobago	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/wp-login.php	Block	1
104.236.55.186	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/	Block	1
66.249.64.230	Israel	147.237.77.216	doover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-14463-he/doover.aspx	Block	1
174.129.228.67	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
82.81.31.84	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
198.20.70.114	United States	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to 147.237.77.19/	Block	1
106.184.3.122	Japan	147.237.76.39	mobile.meitav.idf.il	Illegal Byte Code Character in Method	Block	1
66.249.64.235	Israel	147.237.77.216	doover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-17858-he/doover.aspx	Block	1
82.114.76.77	Albania	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
199.30.16.181	United States	147.237.77.216	doover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
106.184.3.122	Japan	147.237.76.39	mobile.meitav.idf.il	NULL Character in Method	Block	1
66.249.66.121	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/938-he/refuah.aspx	Block	1
176.13.21.162	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/tfasim.aspx	Block	1
82.114.76.77	Albania	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/wp-login.php	Block	1
2.53.48.204	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
207.46.13.93	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
128.232.110.28	United Kingdom	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to 147.237.76.200/	Block	1
66.249.78.246	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
190.58.253.35	Trinidad and Tobago	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
5.29.82.66	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
208.115.113.82	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/main/giyus/general.aspx	Block	1
157.55.39.236	United States	147.237.72.166	aka.idf.il	Unknown Parameter pageNum in aka.idf.il/patzar/klali/default.asp	None	1