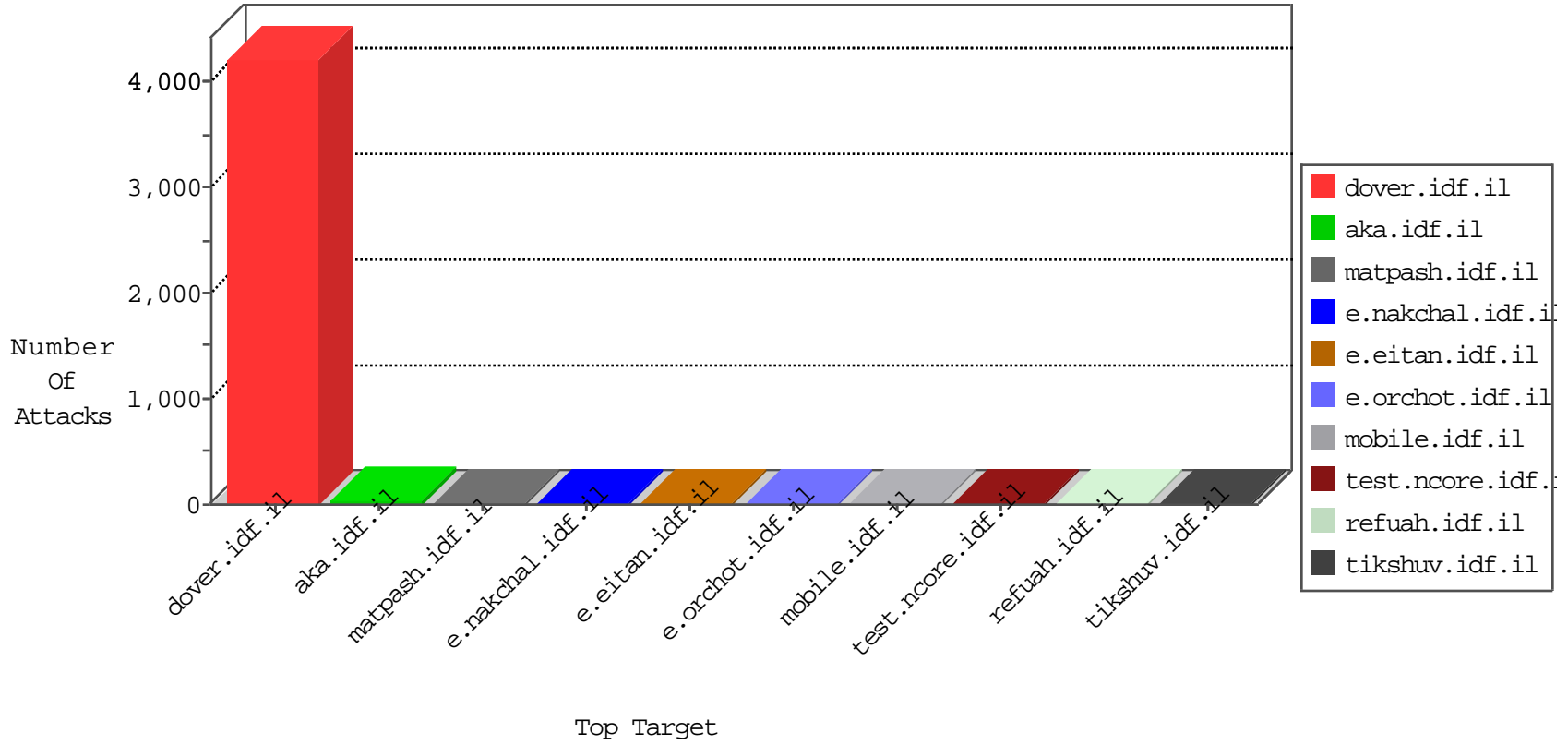




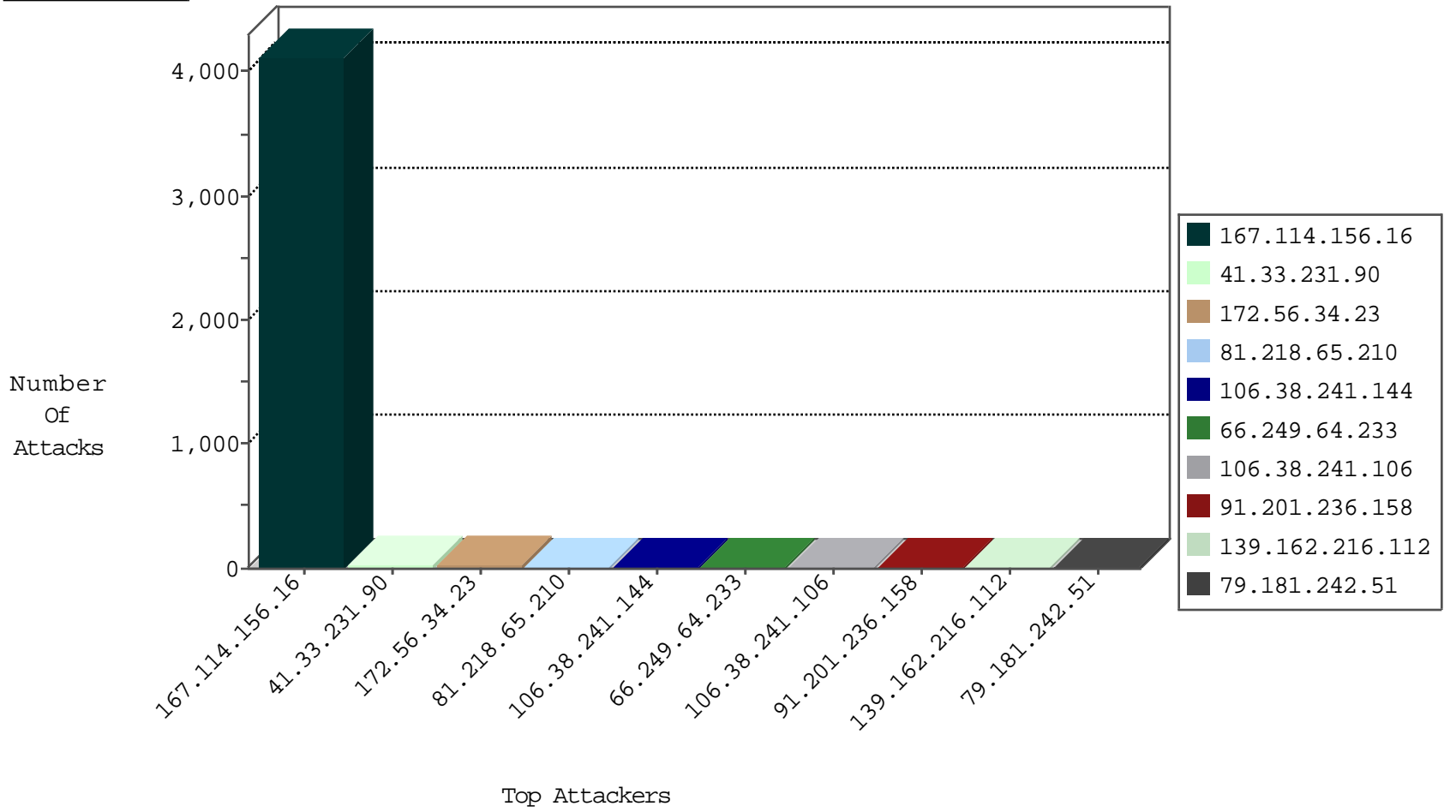
# IDF Under Attack Daily Report



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	4112
81.218.65.210	Israel	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	9
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
184.105.139.68	United States	147.237.77.212	e.dover.idf.il	Block_Ntp_All_Net	drop	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	HTTP-Misc-BadBlue-Dir-Trave-2	dest-reset	1
121.127.88.47	Korea, Republic of	147.237.76.176	test.noore.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.92	United States	147.237.77.216	dover.idf.il	Block_Ntp_All_Net	drop	1
184.105.247.212	United States	147.237.8.45	e.eitan.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.68	United States	147.237.77.121	e.navy.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
185.94.111.1	Russian Federation	147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	1
93.120.133.157	Russian Federation	147.237.76.176	test.noore.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	7
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
66.249.66.190	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	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
95.45.254.123	147.237.72.166	Ireland	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	3
66.249.64.233	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
85.65.15.215	147.237.72.166	Israel	aka.idf.il	ET SCAN NMAP -sA (2)	2
66.249.78.146	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
113.240.250.154	147.237.8.27	China	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
109.235.254.181	147.237.8.45	Turkey	e.eitan.idf.il	ET SCAN NMAP -sS window 2048	1
104.238.82.190	147.237.77.178	United States	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.158	147.237.76.199	Ukraine	e.nakchal.idf.il	ET SCAN NMAP -sS window 2048	1
217.133.53.77	147.237.77.176	Italy	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.158	147.237.76.199	Ukraine	e.nakchal.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
185.112.248.50	147.237.77.74	United Kingdom	law.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.78.38	147.237.77.205	Netherlands	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
185.72.179.130	147.237.76.39	Romania	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
115.29.138.97	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
23.88.236.73	147.237.0.19	United States	madim.atal.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
109.235.254.181	147.237.8.45	Turkey	e.eitan.idf.il	ET SCAN NMAP -sS window 3072	1
109.235.254.181	147.237.8.45	Turkey	e.eitan.idf.il	ET SCAN NMAP -f -sS	1
104.238.82.190	147.237.0.200	United States	m4u.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.158	147.237.76.199	Ukraine	e.nakchal.idf.il	ET SCAN NMAP -sS window 3072	1
217.133.53.77	147.237.77.176	Italy	matpash.idf.il	ET SCAN NMAP -sS window 4096	1
91.201.236.158	147.237.76.199	Ukraine	e.nakchal.idf.il	ET SCAN NMAP -f -sS	1
185.72.179.130	147.237.76.177	Romania	noore.idf.il	ET SCAN NMAP -sS window 1024	1
118.193.20.114	147.237.76.148	Hong Kong	ggcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
46.4.79.76	147.237.76.38	Germany	e.e.meitav.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	24
172.56.34.23	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	21
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
178.154.189.201	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.78.216	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
172.56.14.167	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
79.181.242.51	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
195.220.95.105	France	147.237.76.34	yohalan.idf.il	drop		drop	1
141.212.122.221	United States	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.82.47.54	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.84	United States	147.237.0.35	akaws.idf.il	drop		drop	1
108.90.158.146	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
198.20.69.74	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
144.168.45.117	United States	147.237.76.31	nakchal.idf.il	drop	SAM rule	drop	1
74.82.47.55	United States	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
216.218.206.87	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
109.186.49.99	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
216.218.206.104	United States	147.237.0.33	idf.il	drop		drop	1
184.105.139.126	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.8	United States	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
159.226.95.66	China	147.237.0.33	idf.il	drop		drop	1
79.181.242.51	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
24.42.165.85	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
184.105.247.230	United States	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.220	United States	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.82.47.20	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
216.218.206.71	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
104.148.44.145	United States	147.237.77.19	law-forum.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
37.28.152.58	Poland	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
131.253.25.163	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
68.180.231.43	United States	147.237.77.216	dover.idf.il	Parameter Type Violation pageNum in www.idf.il/1115-ar/dover.aspx	Block	2
24.42.165.85	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	2
136.243.16.208	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
46.161.9.6	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 46.161.9.6	Block	1
79.181.242.51	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/templatecontrols/generic/	Block	1
198.20.69.74	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
68.180.229.241	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation pageNum in www.cogat.idf.il/1038-ar/cogat.aspx	Block	1
46.161.9.6	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/general/general.aspx/templates/sendtofriend/sendtofriend.aspx	Block	1
95.45.254.123	Ireland	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.66.123	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/9/3049.jpg	Block	1
66.249.64.137	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/smalim/showbig.aspx	Block	1
109.253.134.135	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/tfasim.aspx	Block	1
66.249.78.82	Israel	147.237.77.74	law.idf.il	Illegal Parameter Encoding searchText in www.law.idf.il/275-he/patzar.aspx	None	1
70.24.154.49	Canada	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
66.249.64.230	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-20752-he/idfgdover.aspx	Block	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
46.161.9.6	Russian Federation	147.237.0.34	tikshuv.idf.il	Parameter Type Violation FolderId in www.tikshuv.idf.il/modules/forums/forum.aspx	Block	1
70.24.154.49	Canada	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/wp-login.php	Block	1