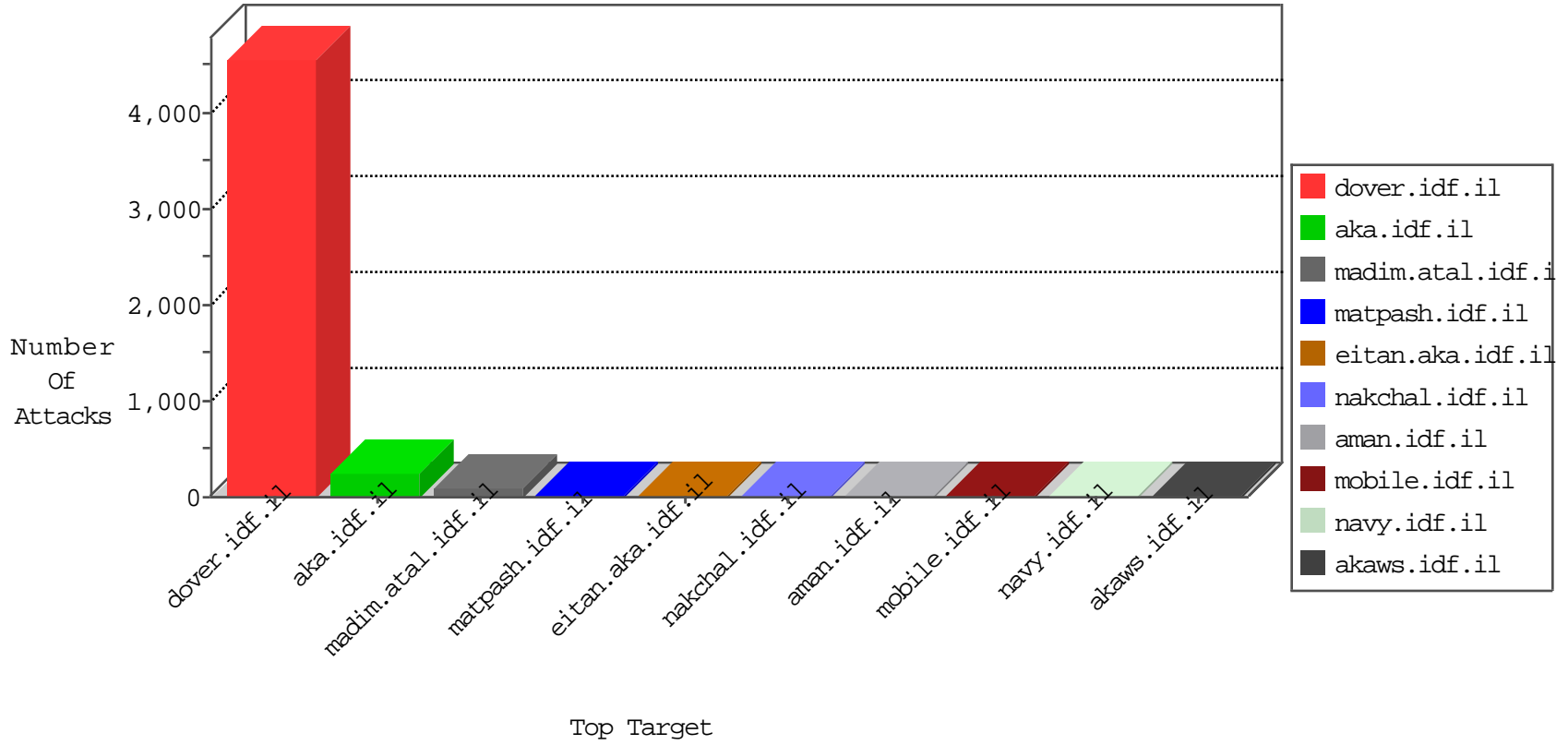




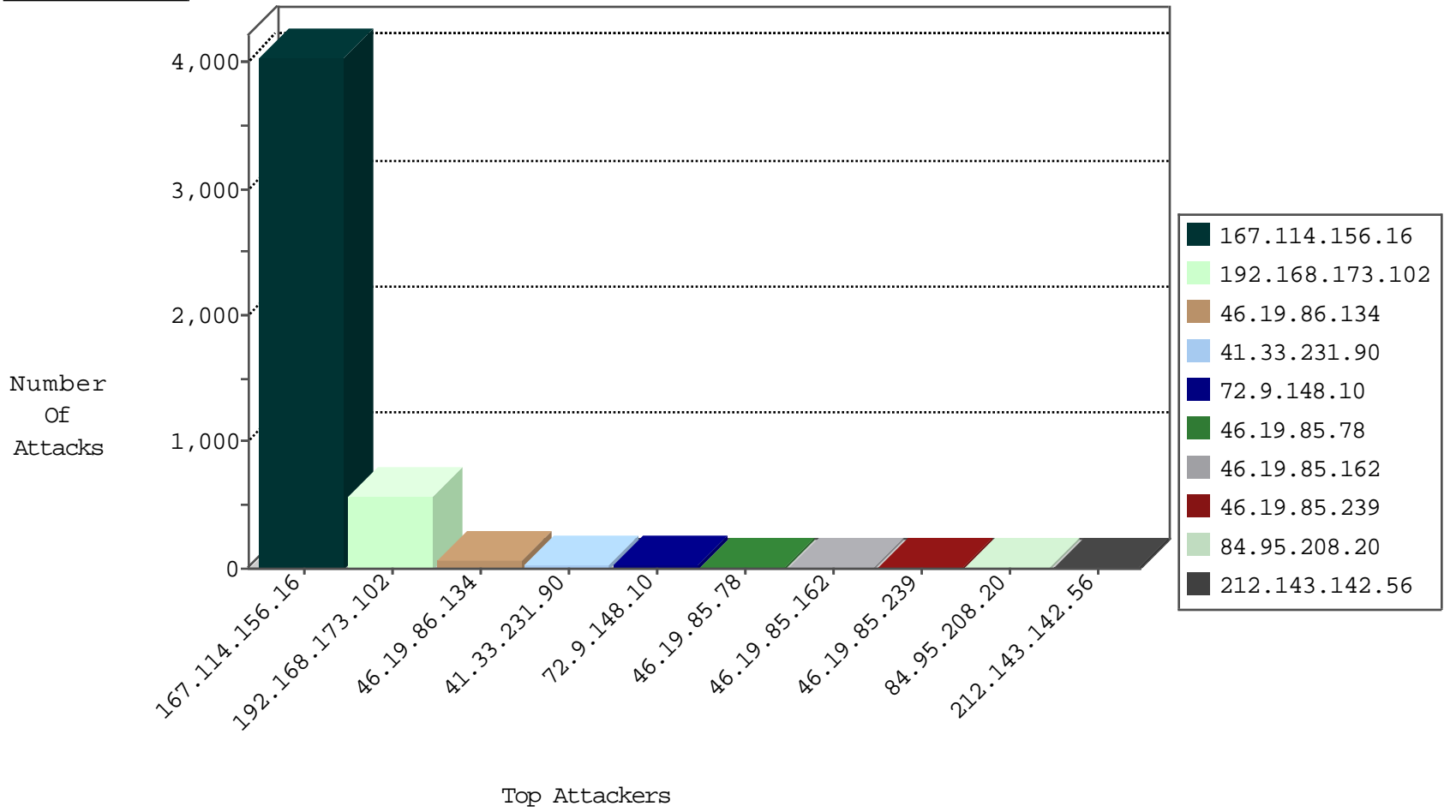
# IDF Under Attack Daily Report



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	4046
81.218.65.210	Israel	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	6
79.182.7.136	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
192.3.220.210	United States	147.237.0.35	akaws.idf.il	Block_Udp_All_Nets	drop	1
222.186.52.95	China	147.237.0.35	akaws.idf.il	JLM_Purple_Con_Limit_Http	drop	1
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
222.186.52.95	China	147.237.0.35	akaws.idf.il	JLM_Under_Attack_Con_Http	drop	1
66.249.69.93	Israel	147.237.72.166	aka.idf.il	HTTP-Misc-BadBlue-Dir-Trave-2	dest-reset	1

04-08-2016-08:04:01 to 04-08-2016-09:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.78.120	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
123.126.113.80	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	3
120.26.115.52	147.237.0.35	China	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
114.199.230.194	147.237.77.234	Korea, Republic of	halag.idf.il	ET SCAN NMAP -sS window 3072	1
92.46.215.94	147.237.76.31	Kazakstan	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
91.201.236.114	147.237.76.176	Ukraine	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
82.117.208.243	147.237.76.38		e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
212.252.132.107	147.237.0.33	Turkey	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
183.60.48.25	147.237.0.200	China	m4u.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
176.223.1.38	147.237.0.15	Romania	kosher-kravi.idf.i	ET SCAN NMAP -sS window 1024	1
118.37.34.34	147.237.8.28	Korea, Republic of	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
114.199.230.194	147.237.77.234	Korea, Republic of	halag.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.114	147.237.77.176	Ukraine	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.114	147.237.76.176	Ukraine	test.ncore.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
183.60.48.25	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
192.168.173.102		147.237.77.216	dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	372
192.168.173.102		147.237.72.166	aka.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	197
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
46.19.85.78	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	14
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
109.253.140.75	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.162	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.239	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.239	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.52.174.120	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
84.95.208.20	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	6
84.95.208.20	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	6
46.19.85.162	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
37.60.144.175	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	5
66.102.9.91	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
72.9.148.10	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	4
46.19.85.80	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
85.71.168.122	Czech Republic	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.85.71	Israel	147.237.72.156	aman.idf.il	drop	SAM rule	drop	4
109.253.196.71	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.148.236	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.142.249	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
81.218.150.58	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.53.53.130	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.108.147.42	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	2
46.19.85.152	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
2.54.191.227	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
46.19.85.162	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
46.19.85.152	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
72.9.148.10	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	2
46.19.85.162	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.86.48	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
199.203.125.80	Israel	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	1
184.105.247.224	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
93.173.181.227	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
2.54.191.227	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
74.82.47.58	United States	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
216.218.206.100	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.117.212.211	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
185.106.92.47	Russian Federation	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
149.88.213.43	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
37.28.152.58	Poland	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
84.108.175.151	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
184.105.247.236	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
2.54.191.227	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	1
216.218.206.102	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.120.200.77	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
188.120.148.163	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.85.162	Israel	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
46.19.86.134	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	70
37.26.149.190	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
208.115.111.72	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	4
2.53.53.130	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
27.255.90.167	Korea, Republic of	147.237.77.216	dover.idf.il	PHP Attempt	Block	2
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.224	Block	1
27.255.90.167	Korea, Republic of	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 27.255.90.167	Block	1
150.183.45.253	Korea, Republic of	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-en/dover.aspx	Block	1
66.249.75.44	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
37.28.152.58	Poland	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
87.71.11.169	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi/site/templates/controller.asp	Block	1
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atall/izkor/print_bottom.asp	Block	1
150.183.45.253	Korea, Republic of	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
66.249.75.45	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/kamlar/news/www.israelbar.org.il	Block	1
40.77.167.42	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
91.108.88.168	Germany	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
66.249.66.121	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/8/2808.jpg	Block	1
27.255.90.167	Korea, Republic of	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
157.55.39.241	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/61998	Block	1
68.180.229.226	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/general/youtu.be/dsh2chqpxt0	Block	1
5.157.56.149	Sweden	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	1
91.121.161.167	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
66.249.69.2	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.69.2	Block	1
37.26.148.230	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
184.105.247.196	United States	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/	Block	1
74.82.47.2	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to 147.237.77.243/	Block	1
66.102.9.91	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-en/www.idf.il/english	Block	1
23.106.244.76	United States	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/shared/usercontrols/headerupper/	Block	1
91.227.165.5	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.69.93	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/1164-he/chinuch.aspx	Block	1
87.70.19.227	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1