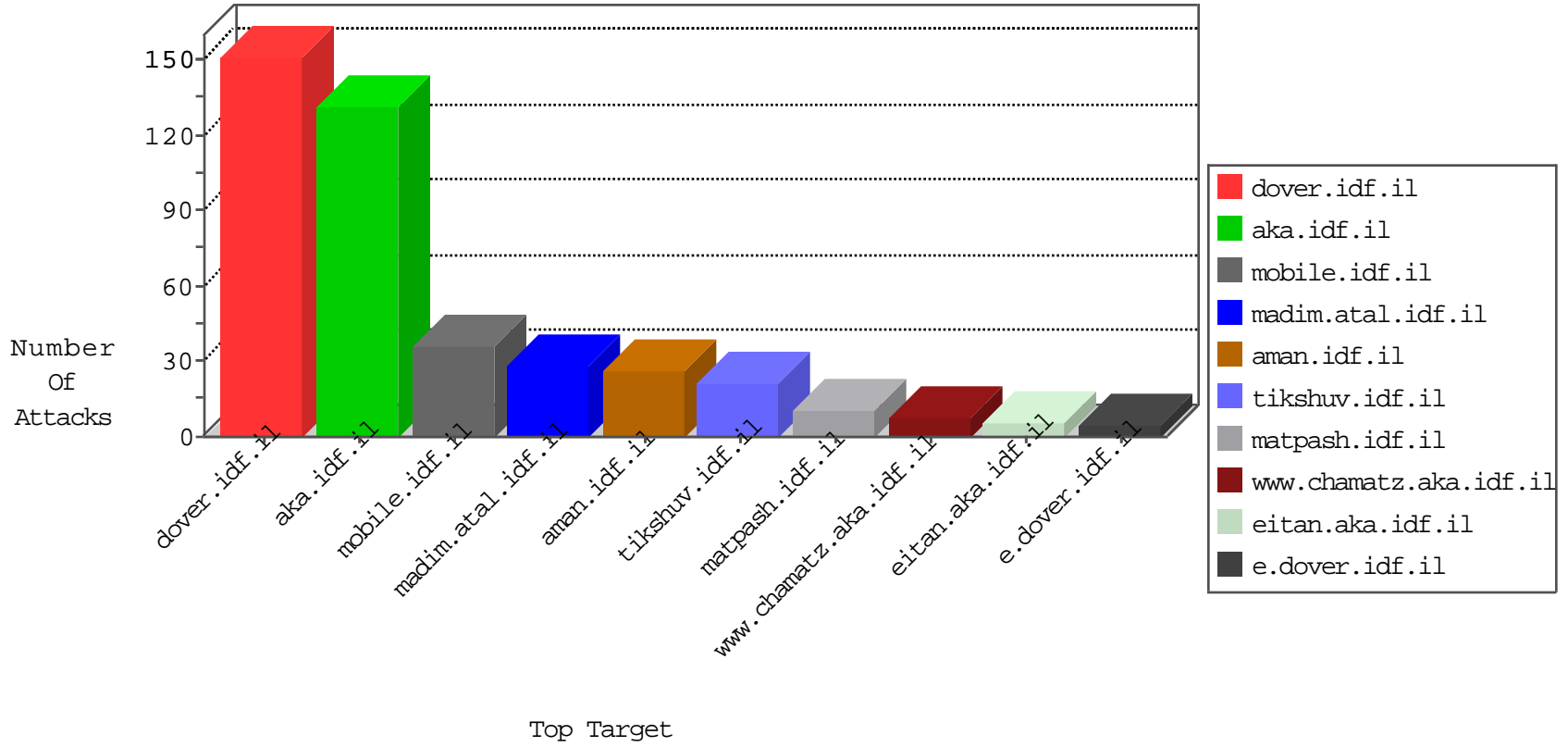


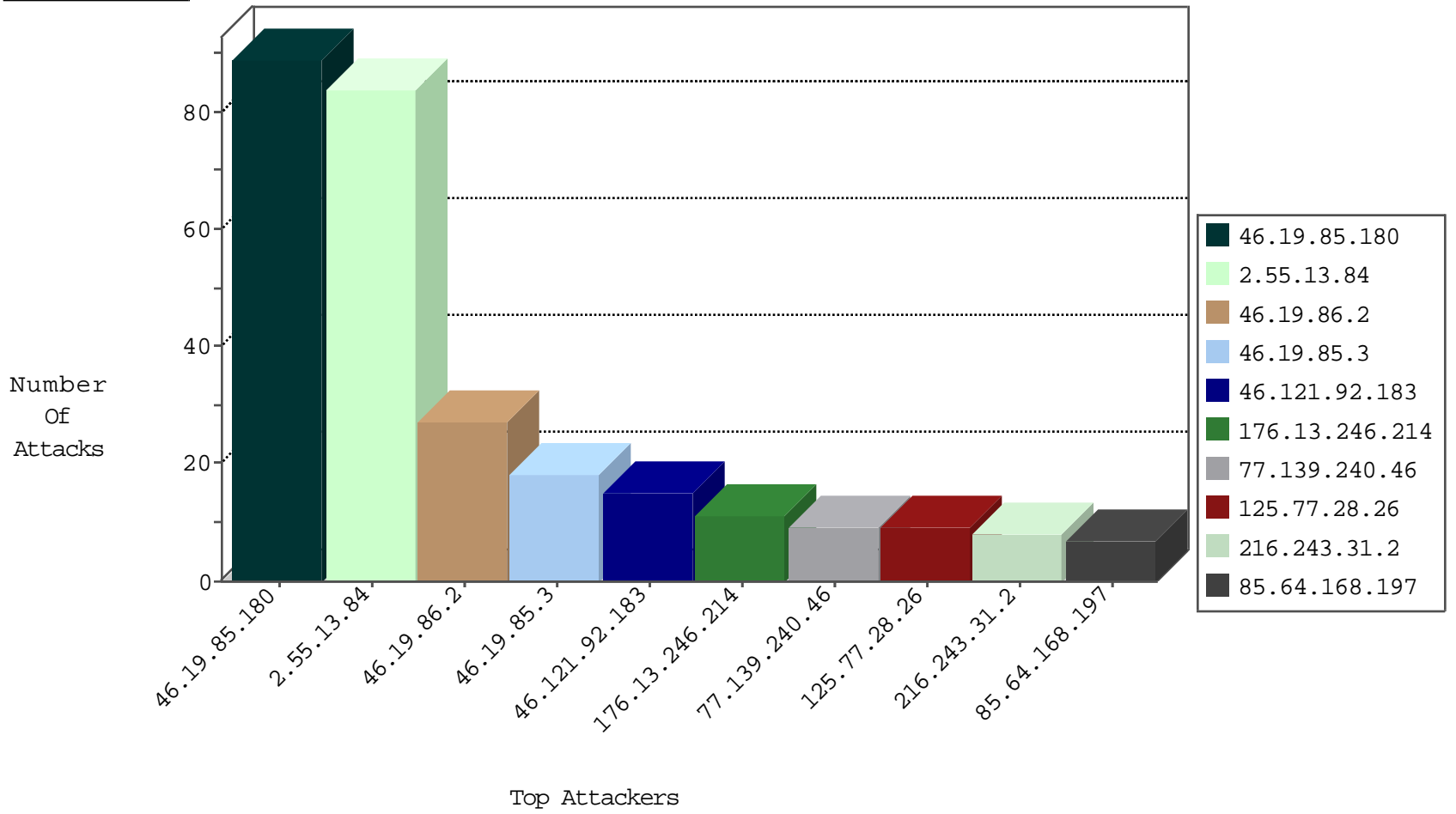
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
45.63.53.164	United States	147.237.76.31	nakchal.idf.il	Black List	drop	1
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	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
59.67.64.13	147.237.77.227	China	e.hamaz.idf.il	GPL SCAN nmap TCP	2
196.47.173.21	147.237.77.176	Cote D'Ivoire	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
185.93.185.10	147.237.77.61	Ukraine	e.cogat.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
82.200.142.180	147.237.76.177	Kazakstan	ncore.idf.il	ET SCAN NMAP -sS window 4096	1
79.177.14.166	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN NMAP -sA (2)	1
61.240.144.65	147.237.77.179	China	e.mazi.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
46.183.223.228	147.237.76.38	Latvia	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
46.161.40.17	147.237.0.16	Russian Federation	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
196.47.173.21	147.237.77.176	Cote D'Ivoire	matpash.idf.il	ET SCAN NMAP -sS window 3072	1
185.129.148.230	147.237.72.217	Latvia	e.idf.il	ET SCAN NMAP -sS window 1024	1
113.117.143.130	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
82.200.142.180	147.237.76.177	Kazakstan	ncore.idf.il	ET SCAN NMAP -sS window 3072	1
61.240.144.65	147.237.77.212	China	e.dover.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
46.161.40.17	147.237.77.216	Russian Federation	dover.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
46.19.85.180	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	39
46.19.85.180	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	35
2.55.13.84	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	24
2.55.13.84	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	24
2.55.13.84	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	24
46.19.85.3	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
46.19.86.2	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
2.55.13.84	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
46.19.85.180	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
176.13.246.214	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
79.180.33.184	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.149.200	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.146.253	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.3.147.244	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.2	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.86.2	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.180	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
46.19.86.2	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
89.139.218.22	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.121.92.183	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
176.228.158.118	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
85.64.168.197	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
5.29.163.209	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
193.124.251.193	Russian Federation	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	3
176.13.232.166	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
37.26.149.248	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.27.243	Israel	147.237.0.19	madim.atal.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
176.228.158.118	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
193.124.251.193	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
87.69.103.206	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
46.19.85.152	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
2.53.39.67	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
85.64.168.197	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	2
46.19.85.3	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
87.69.214.254	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
176.13.246.214	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	2
176.13.0.96	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.85.3	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.116.106.77	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
176.13.246.214	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
84.108.236.191	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
172.247.83.216	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
37.142.206.132	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
139.162.37.147	United States	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
216.243.31.2	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
23.248.234.28	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
125.77.28.26	China	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
2.53.180.211	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
85.64.168.197	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
77.139.240.46	France	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	9
46.121.92.183	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 46.121.92.183	Block	6
46.121.92.183	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
79.177.213.3	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
213.57.164.72	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
176.13.241.112	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.121.52.169	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
24.5.58.234	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/edim/library/generaldoc.asp	Block	2
79.179.28.249	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.121.92.183	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1431	Block	2
46.120.46.228	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/dover/site/mainpage.asp	Block	1
185.93.182.138	Spain	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 185.93.182.138	Block	1
66.249.64.116	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/idkonim/pages/150302011yezu.aspx	Block	1
95.185.234.66	Saudi Arabia	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/brothers/skira/default.asp	Block	1
68.180.231.57	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1380-he/dover.aspx	Block	1
185.93.182.138	Spain	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/shared/	Block	1
77.237.146.28	Czech Republic	147.237.77.216	dover.idf.il	Unauthorized Method HEAD for /	Block	1
66.249.66.75	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/iturim/asp/displayallsoldiers.asp	Block	1
109.253.202.113	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012ources/images/innerpage/goback.gif	Block	1
68.180.231.60	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1927-he/cogat.aspx	Block	1
199.17.232.4	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
66.249.75.8	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/4/2414.jpg	Block	1
109.253.202.113	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 109.253.202.113	Block	1
77.138.21.110	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/gyus/information.aspx	Block	1
66.249.75.32	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19072-he/dover.aspx	Block	1
37.26.146.253	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
77.138.224.65	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/drushim/	Block	1
79.180.27.243	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	1
68.180.230.186	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1