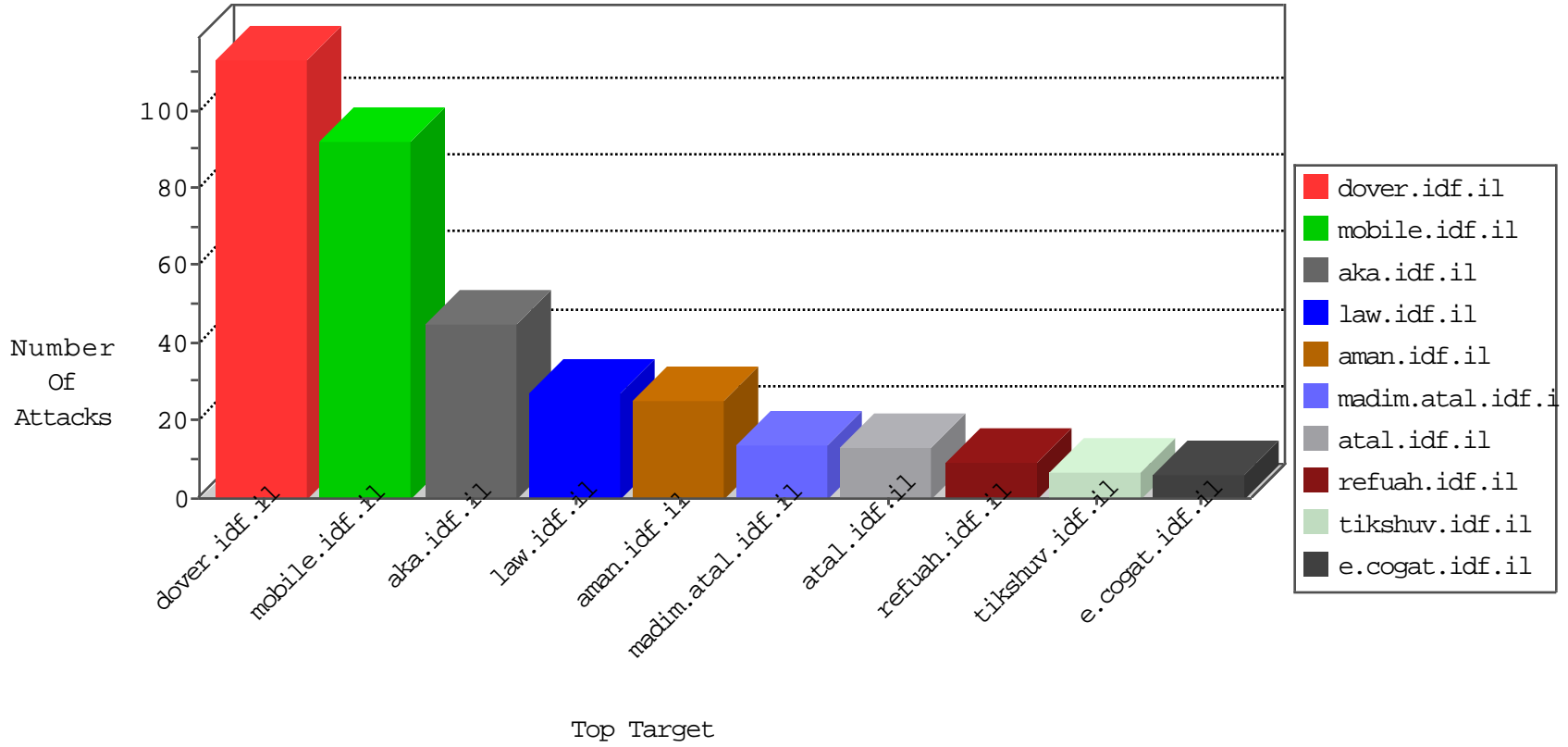


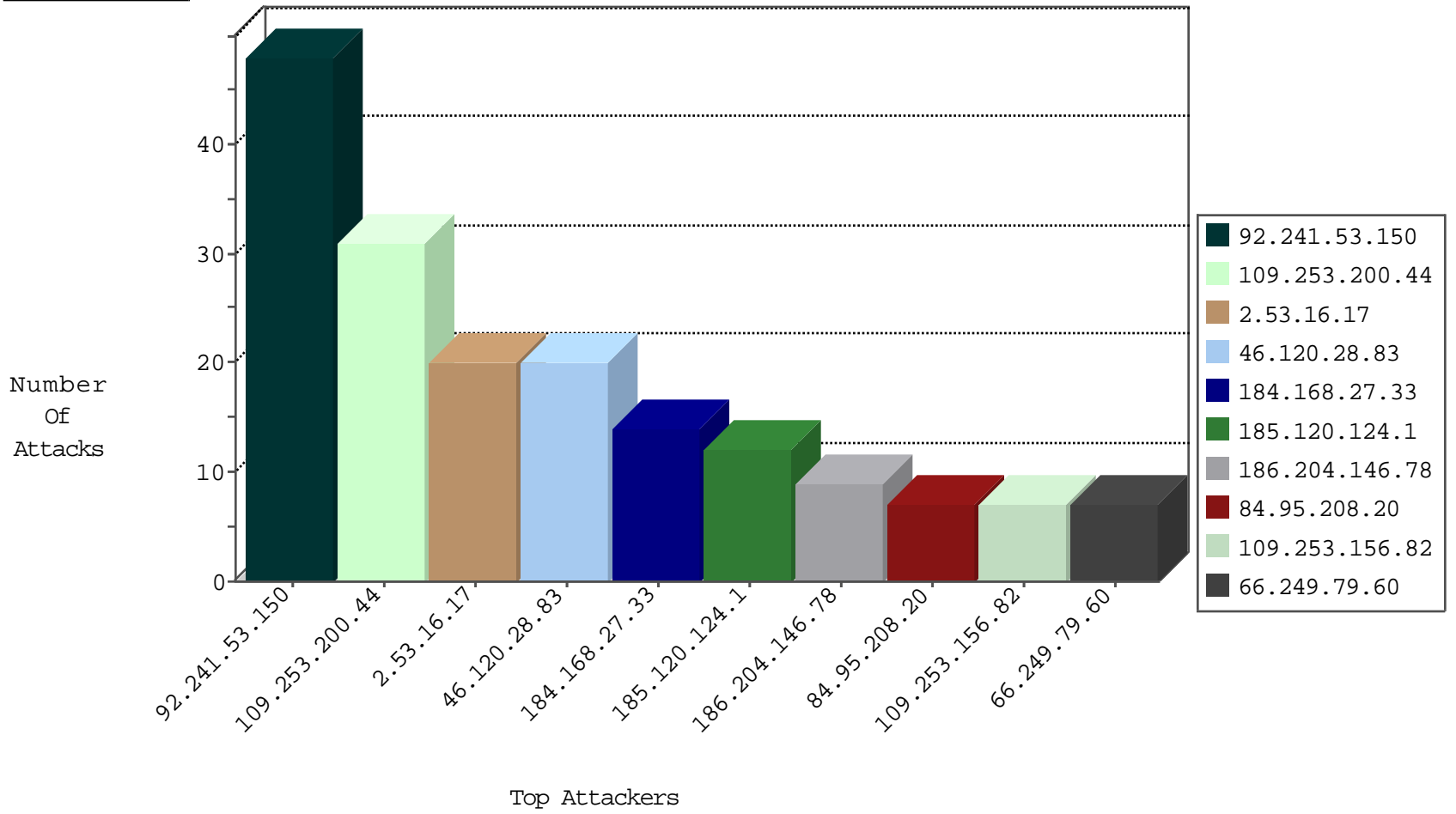
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
134.147.203.115	Germany	147.237.76.34	yohalan.idf.il	Black List	drop	2
42.60.112.73	Singapore	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
184.168.27.33	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6

## Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
184.168.27.33	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	8
185.120.124.1	147.237.76.30	Israel	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	4
91.224.118.2	147.237.77.61	Poland	e.cogat.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	2
104.152.188.86	147.237.77.61	United States	e.cogat.idf.il	ET SCAN NMAP -sS window 2048	1
78.129.171.173	147.237.77.233	United Kingdom	atal.idf.il	ET SCAN Potential SSH Scan	1
73.176.200.52	147.237.76.201	United States	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
198.20.69.98	147.237.76.44	United States	e.refuah.idf.il	ET DROP Dshield Block Listed Source	1
46.161.40.17	147.237.77.61	Russian Federation	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
45.63.28.189	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sS window 1024	1
183.60.48.25	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
45.63.28.189	147.237.77.178	United States	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
107.191.55.97	147.237.77.234	United States	halag.idf.il	ET SCAN NMAP -sS window 1024	1
104.152.188.86	147.237.77.61	United States	e.cogat.idf.il	ET SCAN NMAP -sS window 3072	1
104.152.188.86	147.237.77.61	United States	e.cogat.idf.il	ET SCAN NMAP -f -sS	1
84.108.236.198	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
78.129.171.173	147.237.8.14	United Kingdom	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
218.92.251.243	147.237.77.233	China	atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
58.218.200.137	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	1
46.161.40.17	147.237.72.166	Russian Federation	aka.idf.il	ET SCAN NMAP -sS window 1024	1
183.60.48.25	147.237.76.177	China	ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
45.63.28.189	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sS window 1024	1
122.238.83.146	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
107.191.55.97	147.237.76.200	United States	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
92.241.53.150	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
109.253.200.44	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
2.53.16.17	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
185.120.124.1	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
109.253.156.82	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.142.9.10	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
66.249.79.60	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
186.204.146.78	Brazil	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
84.95.208.20	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
66.249.93.194	Europe	147.237.77.74	law.idf.il	Directory Traversal	directory traversal overflow	monitor	5
46.120.28.83	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
87.69.205.175	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
5.29.243.241	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.120.28.83	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
46.120.28.83	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	4
2.53.17.204	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
79.178.187.25	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
109.253.157.19	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
186.204.146.78	Brazil	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
46.19.85.131	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.186	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
77.139.122.174	France	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
46.121.232.133	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
2.53.1.152	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
82.81.196.68	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.79.61	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.134.168	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.67.48.83	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.69.127.169	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	3
46.121.232.133	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
5.22.134.201	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.120.28.83	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
79.177.185.193	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.182.8.2	Ireland	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
43.251.173.145	India	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
37.26.149.172	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
49.231.201.66	Thailand	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
46.120.28.83	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
2.55.151.69	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
46.120.28.83	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.86.187	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
141.226.161.175	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
66.249.93.192	Europe	147.237.77.74	law.idf.il	Directory Traversal	directory traversal overflow	monitor	2
37.142.221.148	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
68.12.85.27	United States	147.237.77.243	mobile.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	1
216.243.31.2	United States	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
37.26.149.172	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
87.69.127.169	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.16.17	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
141.226.162.21	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.177.103.51	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.53.147.111	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.55.37.76	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.108.74.66	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	2
68.12.85.27	United States	147.237.76.86	navy.idf.il	Distributed PHP Attempt	Block	1
46.19.85.177	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/1217-he/refuah.aspx0404	Block	1
212.34.11.93	Jordan	147.237.77.176	matpash.idf.il	Unknown HTTP Request Method .8 in URL	Block	1
77.139.31.204	France	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/favicon.ico	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/2/2312.jpg	Block	1
31.154.81.5	Israel	147.237.76.42	refuah.idf.il	Distributed PHP Attempt	Block	1
68.12.85.27	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/license.php	Block	1
46.19.86.192	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
66.249.76.81	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catid in 147.237.72.166/main/giyus/general.aspx	Block	1
31.154.81.5	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on www.refua.atal.idf.il/xmlrpc.php	Block	1
157.55.39.58	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/894-he/dover.aspx	Block	1
74.91.23.166	United States	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/	Block	1
66.102.9.5	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
66.249.79.60	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
31.154.81.33	Israel	147.237.76.42	refuah.idf.il	Distributed PHP Attempt	Block	1
188.48.128.131	Saudi Arabia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ar/=1-	Block	1
74.91.23.166	United States	147.237.77.216	dover.idf.il	Unauthorized Method HEAD for 147.237.77.216/	Block	1
66.249.64.62	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/iturim/asp/displayallsoldiers.asp	Block	1
66.249.93.194	Israel	147.237.77.74	law.idf.il	Distributed URL is Above Root Directory	Block	1
31.154.81.33	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/xmlrpc.php	Block	1
212.34.11.93	Jordan	147.237.77.176	matpash.idf.il	Malformed URL	Block	1
77.138.32.64	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
66.249.75.4	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
109.253.156.82	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1