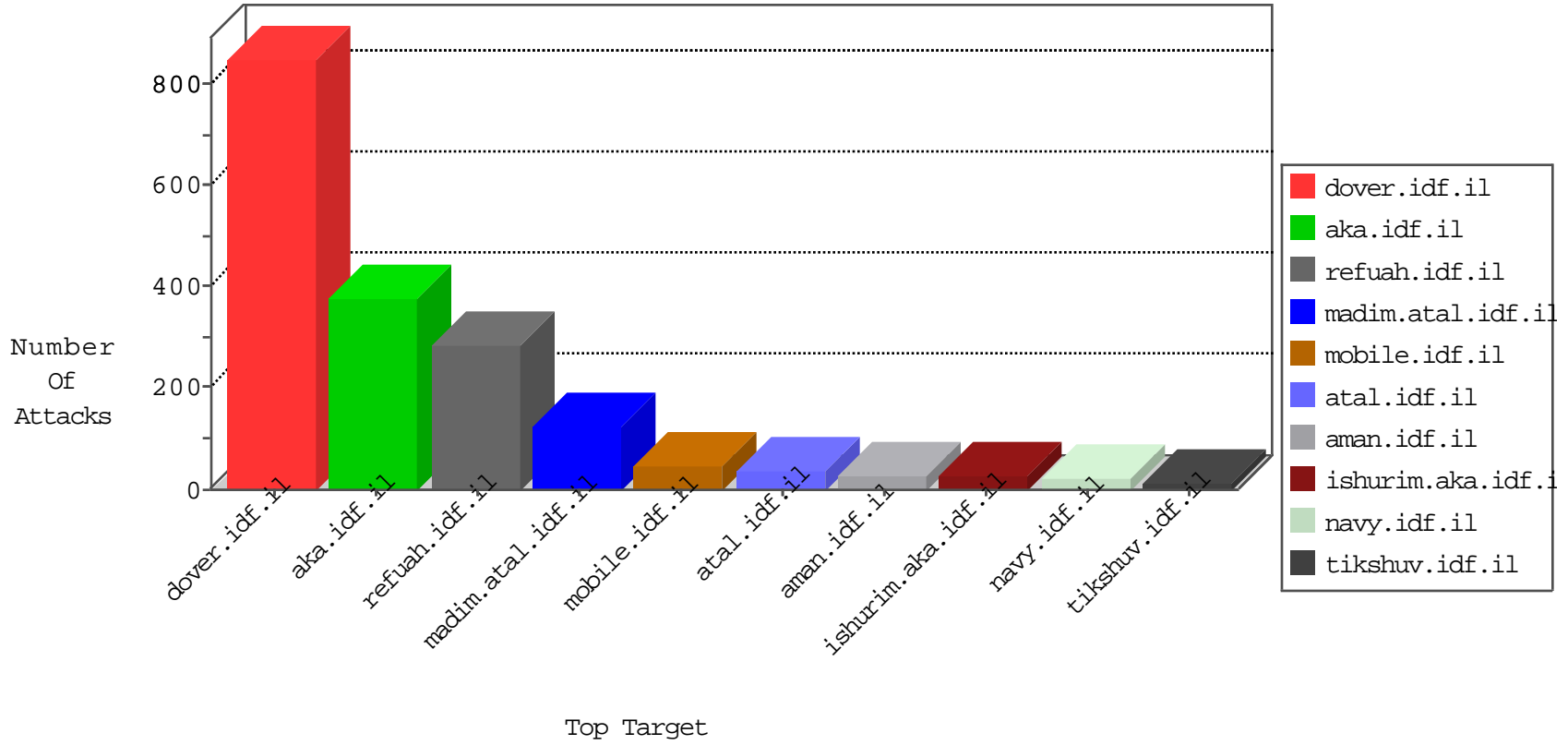


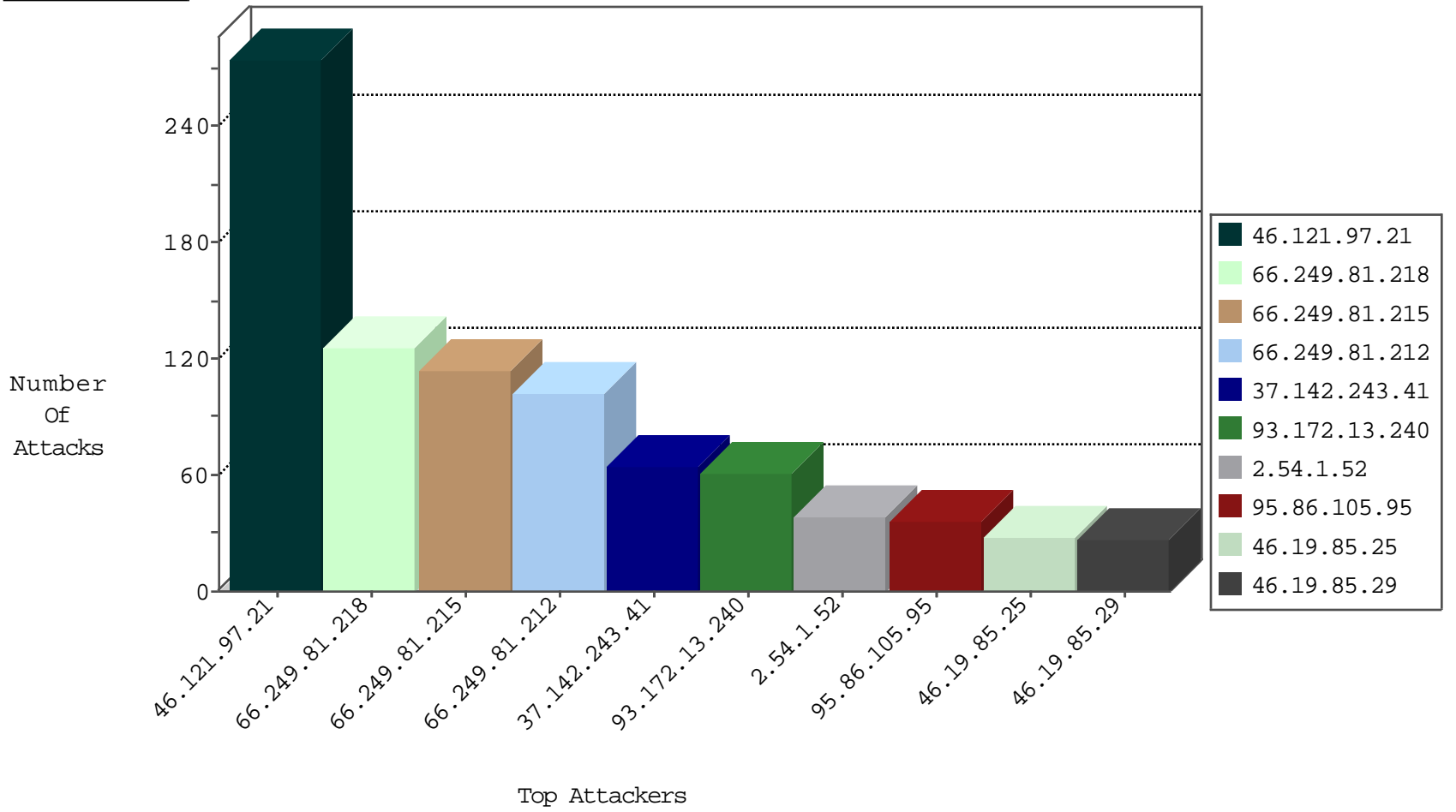
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.78.127	Israel	147.237.0.34	tikshuv.idf.il	TCP handshake violation, first packet not syn	drop	549
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	38
66.249.81.218	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
115.236.75.201	China	147.237.76.44	e.refuah.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
66.249.81.215	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
142.54.169.166	United States	147.237.77.19	law-forum.idf.il	block-sp-trafl	drop	1
74.91.28.62	United States	147.237.72.166	aka.idf.il	block-sp-trafl	drop	1
66.249.81.212	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
142.54.169.166	United States	147.237.0.15	kosher-kravi.idf.il	block-sp-trafl	forward	1

02-03-2016-22:04:00 to 02-03-2016-23:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
172.86.83.64		147.237.76.86	navy.idf.i	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	1

## Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	10
80.246.133.67	147.237.77.216	Israel	dover.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	5
176.13.11.98	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
213.151.52.91	147.237.77.216	Israel	dover.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
50.204.188.142	147.237.76.148	United States	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 4096	1
193.201.227.70	147.237.0.34	Ukraine	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
151.11.201.3	147.237.76.34	Italy	yohalan.idf.il	ET SCAN NMAP -sS window 3072	1
115.236.75.201	147.237.0.200	China	m4u.idf.il	ET SCAN Potential SSH Scan	1
112.33.3.175	147.237.0.200	China	m4u.idf.il	ET SCAN Potential SSH Scan	1
109.64.43.241	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.110.108.233	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
218.246.0.97	147.237.77.243	China	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
79.176.10.42	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
50.204.188.142	147.237.76.148	United States	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
193.201.227.70	147.237.0.15	Ukraine	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
5.29.93.76	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
151.11.201.3	147.237.76.34	Italy	yohalan.idf.il	ET SCAN NMAP -sS window 4096	1
149.78.24.196	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
114.112.90.54	147.237.77.121	China	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
109.160.198.29	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
89.139.239.205	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.121.97.21	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	274
66.249.81.218	United States	147.237.77.216	dover.idf.il	drop	Unexpected post SYN packet - RST or SYN expected	drop	35
66.249.81.215	Russian Federation	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	32
66.249.81.215	Russian Federation	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	32
66.249.81.215	Russian Federation	147.237.77.216	dover.idf.il	drop	Unexpected post SYN packet - RST or SYN expected	drop	32
46.19.85.25	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	28
66.249.81.212	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	27
66.249.81.212	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	27
66.249.81.218	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	25
66.249.81.218	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	25
46.19.85.29	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
66.249.81.212	United States	147.237.77.216	dover.idf.il	drop	Unexpected post SYN packet - RST or SYN expected	drop	24
79.183.55.9	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
2.54.1.52	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	13
66.249.81.218	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	13
66.249.81.218	United States	147.237.77.216	dover.idf.il	Bad TCP sequence		alert	11
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	11
66.249.81.218	United States	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	11
46.19.85.184	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
37.26.147.213	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
185.32.179.140	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
66.249.81.212	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	9
79.179.38.130	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
109.253.204.2	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
66.249.81.212	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	9
84.109.216.123	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
37.238.144.46	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
31.210.187.36	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
91.200.12.136	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
2.54.1.52	Israel	147.237.77.216	dover.idf.il	SYN Attack		reject	7
46.19.85.123	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
66.249.81.215	Russian Federation	147.237.77.216	dover.idf.il	Bad TCP sequence		alert	6
109.253.201.29	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.194	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.176.97.97	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.127	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
85.64.36.91	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.109	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.44	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.225	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.177.61.219	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.8	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.158	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.123	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.253	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
66.249.81.215	Russian Federation	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	6
79.179.111.172	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.201.29	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.109	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6

