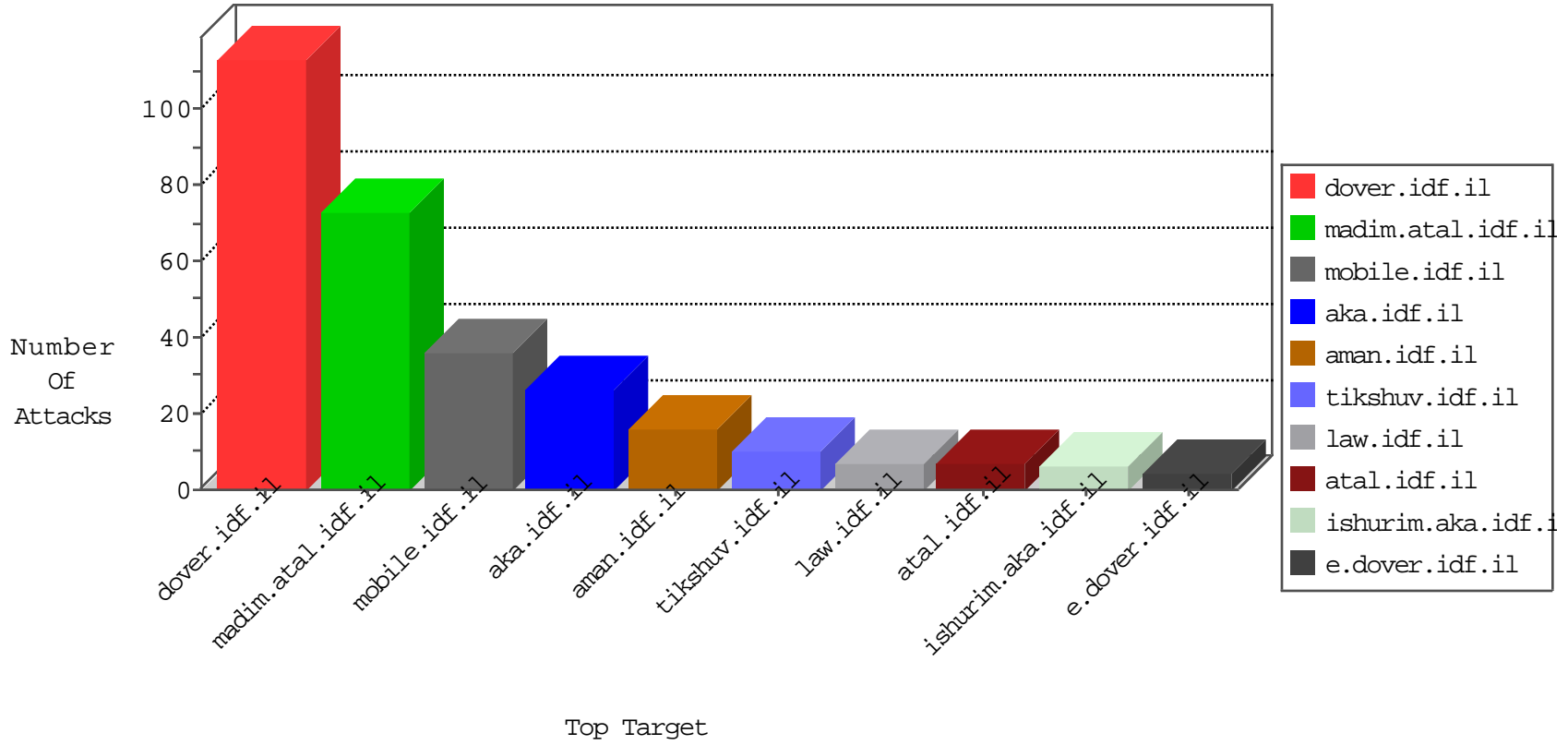


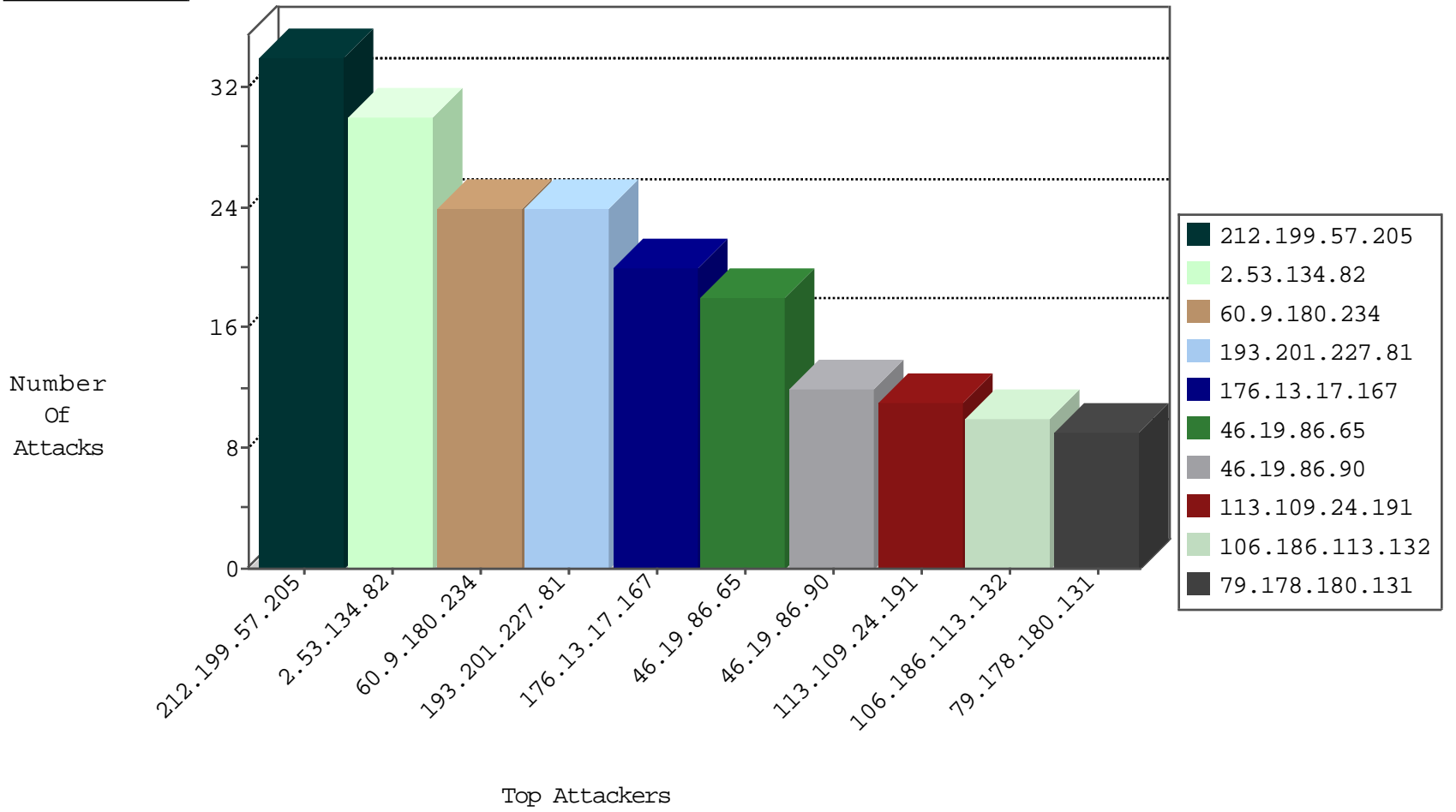
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
194.29.178.14	Poland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
106.186.113.132	Japan	147.237.0.34	tikshuv.idf.il	block-sp-traffic	forward	2
129.93.229.138	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
128.223.8.114	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
204.85.191.10	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
141.22.213.34	Germany	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
198.133.224.147	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
129.32.84.160	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
208.94.63.194	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
153.90.1.34	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.42.142.41	United States	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 ICMP	drop	1
200.19.159.34	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
156.56.250.226	United States	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 ICMP	drop	1
128.42.142.45	United States	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 ICMP	drop	1
200.19.159.35	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
129.110.125.52	United States	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
108.59.8.70	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
108.59.8.70	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2

## Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
193.201.227.81	147.237.8.28	Ukraine	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	2
193.201.227.81	147.237.76.199	Ukraine	e.nakchal.idf.il	ET SCAN Potential SSH Scan	2
46.4.120.149	147.237.77.212	Germany	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
193.201.227.81	147.237.8.46	Ukraine	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
46.4.85.112	147.237.77.212	Germany	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
193.201.227.81	147.237.77.226	Ukraine	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
193.201.227.81	147.237.8.14	Ukraine	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
193.201.227.81	147.237.77.176	Ukraine	matpash.idf.il	ET SCAN Potential SSH Scan	1
193.201.227.81	147.237.0.33	Ukraine	idf.il	ET SCAN Potential SSH Scan	1
193.201.227.81	147.237.0.16	Ukraine	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
193.201.227.81	147.237.76.148	Ukraine	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
163.172.238.45	147.237.72.167	United Kingdom	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
193.201.227.81	147.237.76.44	Ukraine	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
82.118.236.156	147.237.77.226	Bulgaria	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
193.201.227.81	147.237.72.167	Ukraine	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
69.162.69.222	147.237.76.176	United States	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
193.201.227.81	147.237.8.50	Ukraine	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
46.4.85.112	147.237.77.233	Germany	atal.idf.il	ET SCAN NMAP -sS window 1024	1
193.201.227.81	147.237.8.45	Ukraine	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
193.201.227.81	147.237.8.24	Ukraine	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
193.201.227.81	147.237.77.216	Ukraine	dover.idf.il	ET SCAN Potential SSH Scan	1
193.201.227.81	147.237.0.35	Ukraine	akaws.idf.il	ET SCAN Potential SSH Scan	1
193.201.227.81	147.237.77.61	Ukraine	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
193.201.227.81	147.237.0.17	Ukraine	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
193.201.227.81	147.237.76.196	Ukraine	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
163.172.238.45	147.237.77.235	United Kingdom	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
193.201.227.81	147.237.76.147	Ukraine	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
89.248.160.155	147.237.8.45	Netherlands	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
193.201.227.81	147.237.76.39	Ukraine	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
78.46.36.168	147.237.77.170	Germany	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
193.201.227.81	147.237.72.14	Ukraine	dover.idf.il(old)	ET SCAN Potential SSH Scan	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
2.53.134.82	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
79.178.180.131	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.90	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.90	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.226.26.171	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
37.26.147.210	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
109.66.116.89	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
84.109.14.223	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
46.19.86.216	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
109.253.243.109	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.216	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
80.246.136.250	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.111.122.96	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
157.55.39.142	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
109.253.221.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
109.253.221.69	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
108.180.145.49	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
109.253.215.213	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
31.13.110.99	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
109.64.168.57	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
74.63.246.42	United States	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
185.20.5.157	United Kingdom	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	1
46.4.120.149	Germany	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
109.253.215.213	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
104.156.240.158	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
218.22.211.69	China	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
66.249.69.224	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.60	United States	147.237.77.179	e.mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
46.4.120.149	Germany	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
185.20.5.157	United Kingdom	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
74.63.246.42	United States	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.4.85.112	Germany	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
106.186.113.132	Japan	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
79.178.180.131	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
69.162.69.222	United States	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.61	United States	147.237.77.179	e.mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
46.4.120.149	Germany	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
109.67.97.51	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
2.53.156.236	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
74.63.246.42	United States	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
185.20.5.157	United Kingdom	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
46.4.85.112	Germany	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
106.186.113.169	Japan	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
79.178.180.131	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
74.63.237.154	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.226.217.65	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
46.4.120.149	Germany	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
2.55.49.154	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
78.46.36.168	Germany	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1

