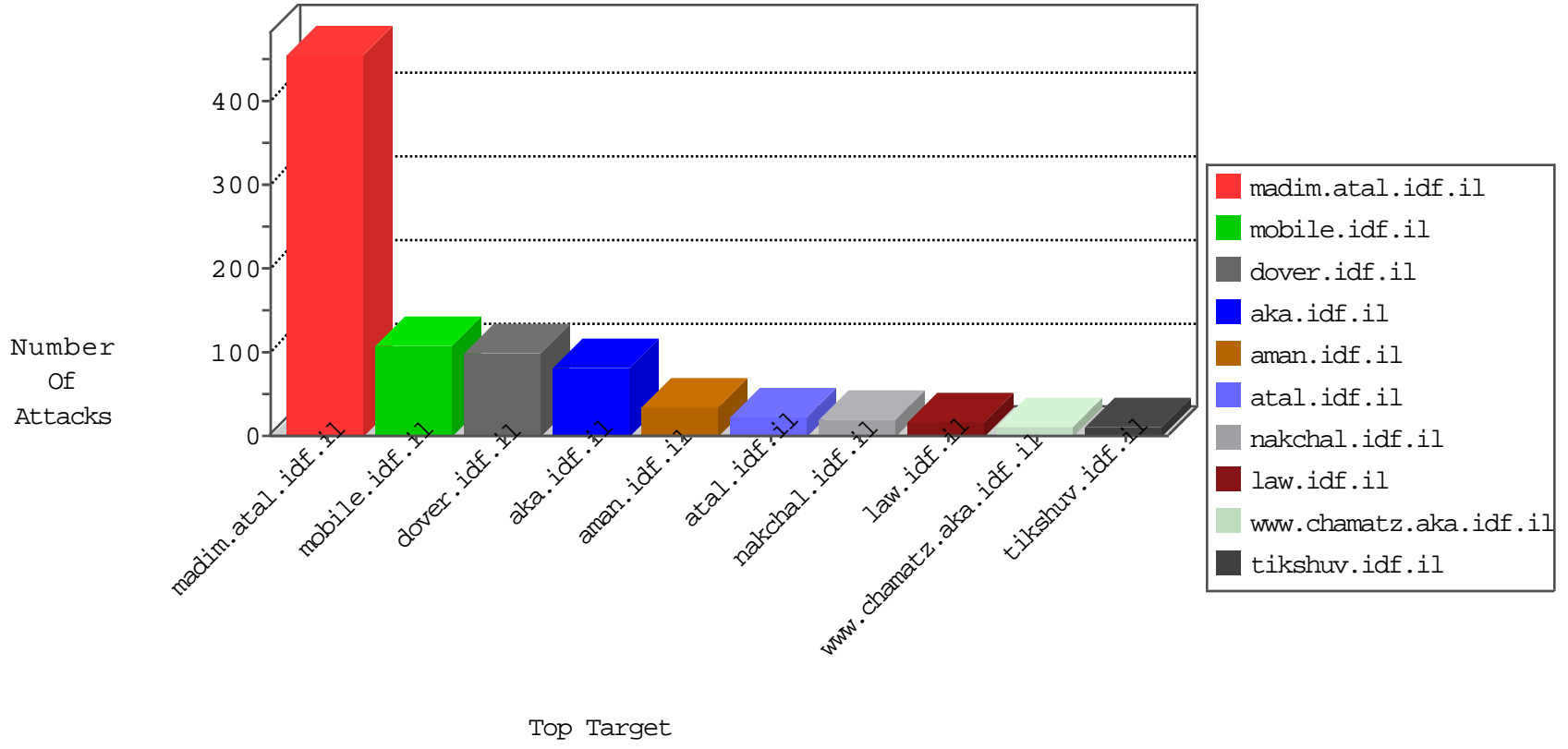


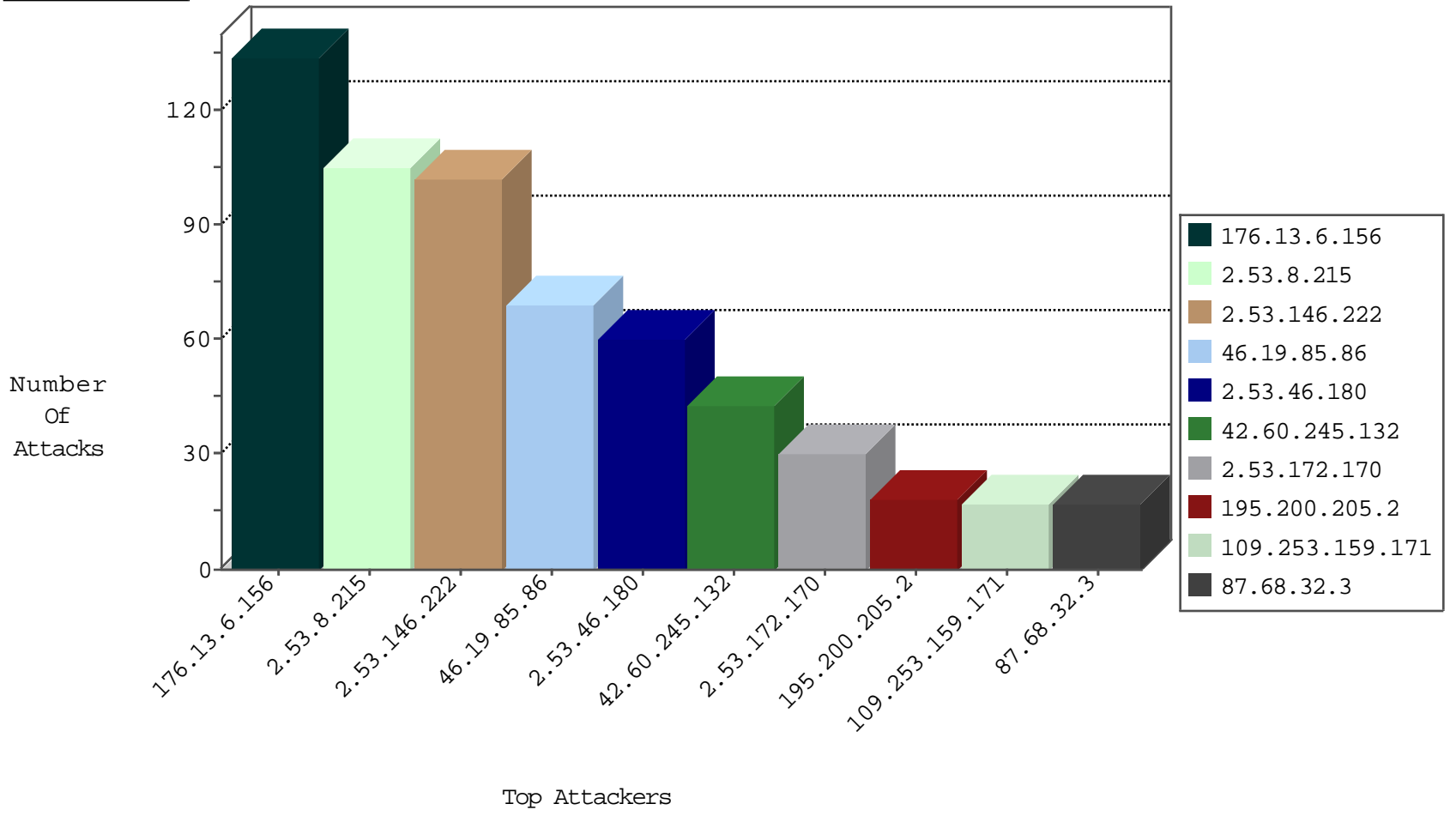
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
131.247.2.241	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	4
198.82.160.238	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
109.67.136.175	Israel	147.237.77.216	dover.idf.il	Black List	drop	3
198.133.224.147	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
141.22.213.34	Germany	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
129.32.84.160	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
156.56.250.227	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
173.208.150.116	United States	147.237.77.235	sviva.idf.il	block-sp-trafl	forward	1
131.179.150.72	United States	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 ICMP	drop	1
128.10.18.52	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
153.90.1.35	United States	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1
130.217.77.2	New Zealand	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
69.30.226.219	United States	147.237.0.34	tikshuv.idf.il	block-sp-trafl	forward	1
204.85.191.11	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
173.208.197.205	United States	147.237.72.156	aman.idf.il	block-sp-trafl	forward	1
128.223.8.112	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
42.60.245.132	Singapore	147.237.8.45	e.eitan.idf.il	JLM_Purple_Con_Limit_Https	drop	1
198.133.224.147	United States	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1
156.56.250.227	United States	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1
130.217.77.4	New Zealand	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1
216.48.80.12	Canada	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1
173.208.197.205	United States	147.237.77.234	halag.idf.il	block-sp-trafl	forward	1
63.141.242.195	United States	147.237.77.170	maarachot.idf.il	block-sp-trafl	forward	1
130.217.77.4	New Zealand	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 ICMP	drop	1
128.8.126.111	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
195.113.161.84	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
143.225.229.236	Italy	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
130.195.4.69	New Zealand	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
69.30.193.252	United States	147.237.76.42	refuah.idf.il	block-sp-trafl	forward	1
200.19.159.34	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
74.63.228.226	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
91.219.122.2	Poland	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
162.210.196.97	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	3
240.0.10.13		147.237.72.166	aka.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
91.219.122.2	147.237.77.74	Poland	law.idf.il	SQL Injection - Select From	8
74.63.228.226	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	8
42.112.239.171	147.237.77.226	Vietnam	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 3072	1
42.60.245.132	147.237.0.33	Singapore	idf.il	ET SCAN Potential SSH Scan	1
41.180.9.40	147.237.76.199	South Africa	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
188.138.56.180	147.237.72.167	Germany	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
5.255.90.133	147.237.72.156	Netherlands	aman.idf.il	ET SCAN NMAP -sS window 1024	1
123.157.123.214	147.237.76.34	China	yochalan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
77.252.26.51	147.237.76.39	Poland	mobile.meitav.idf.il	ET SCAN NMAP -sS window 2048	1
58.218.200.137	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
42.60.245.132	147.237.0.200	Singapore	m4u.idf.il	ET SCAN Potential SSH Scan	1
41.180.9.40	147.237.76.200	South Africa	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
222.254.34.165	147.237.77.212	Vietnam	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
41.180.9.40	147.237.76.86	South Africa	navy.idf.il	ET SCAN Potential SSH Scan	1
183.252.40.202	147.237.77.233	China	atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
116.71.128.85	147.237.8.24	Pakistan	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
77.252.26.51	147.237.76.39	Poland	mobile.meitav.idf.il	ET SCAN NMAP -sS window 3072	1
77.252.26.51	147.237.76.39	Poland	mobile.meitav.idf.il	ET SCAN NMAP -f -sS	1
66.249.66.234	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
2.53.46.180	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
2.53.172.170	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
46.19.85.41	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
87.68.32.3	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
80.179.9.7	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.86.62	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
109.67.190.20	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
46.19.86.62	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.185	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
87.68.32.3	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
37.26.146.254	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
62.90.181.44	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.24	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
46.19.85.117	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
42.60.245.132	Singapore	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	5
46.19.85.19	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.19	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.117	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
42.60.245.132	Singapore	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
42.60.245.132	Singapore	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
42.60.245.132	Singapore	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
42.60.245.132	Singapore	147.237.0.33	idf.il	drop		drop	4
42.60.245.132	Singapore	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
2.53.161.178	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
5.22.134.94	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
37.26.147.225	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
176.13.251.191	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.253.229.45	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.177.84.59	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
2.53.185.6	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
46.19.85.97	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
42.60.245.132	Singapore	147.237.0.35	akaws.idf.il	drop		drop	3
109.253.203.33	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
84.108.93.107	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
42.60.245.132	Singapore	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
213.8.204.6	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
79.176.131.218	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
2.53.42.80	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
42.60.245.132	Singapore	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
176.13.13.78	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
46.19.85.7	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.85.90	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
37.26.149.134	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		alert	2
42.60.245.132	Singapore	147.237.8.27	e.madim.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
80.246.136.224	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
37.26.149.134	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	2
2.55.41.180	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
212.227.136.232	Germany	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
188.169.146.152	Georgia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1

