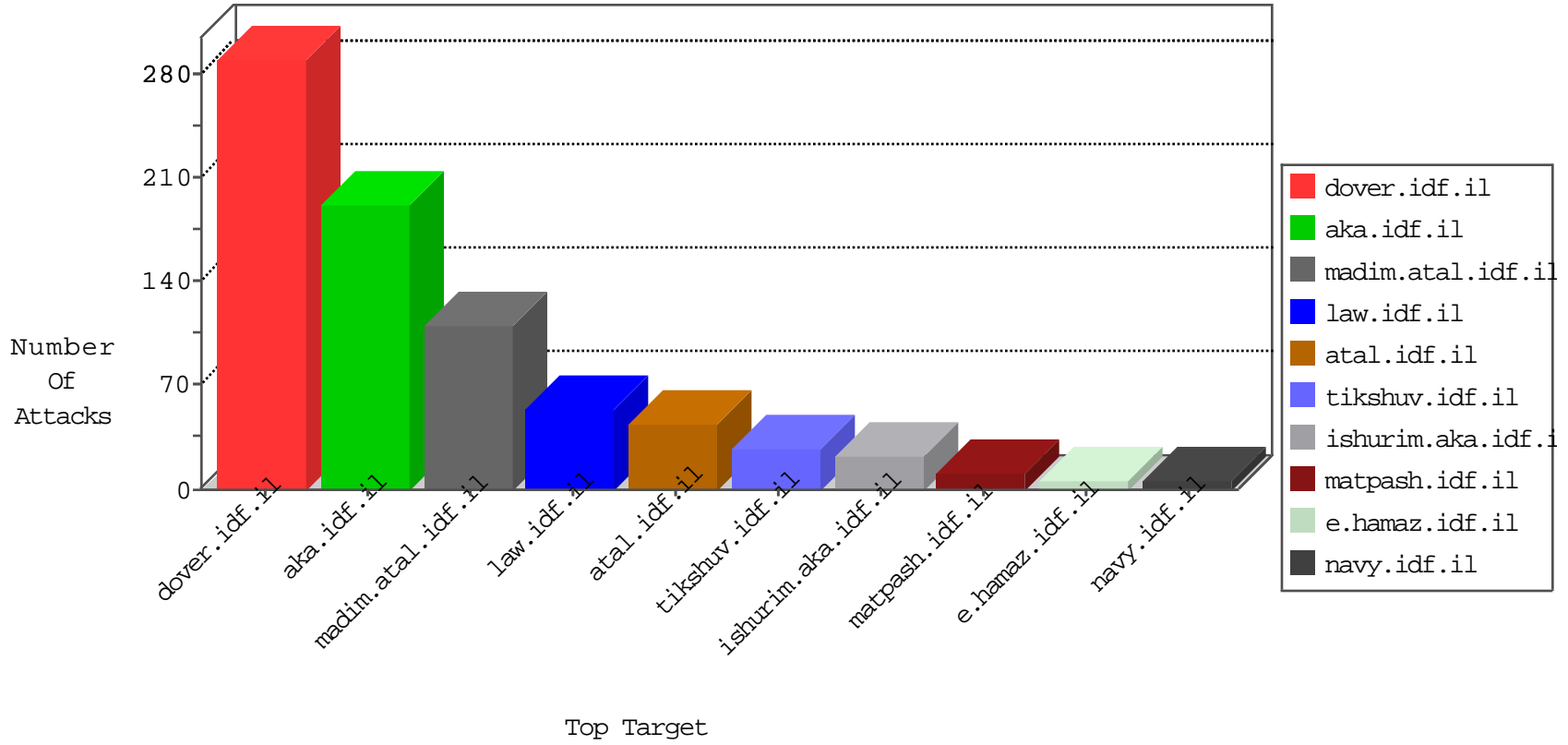


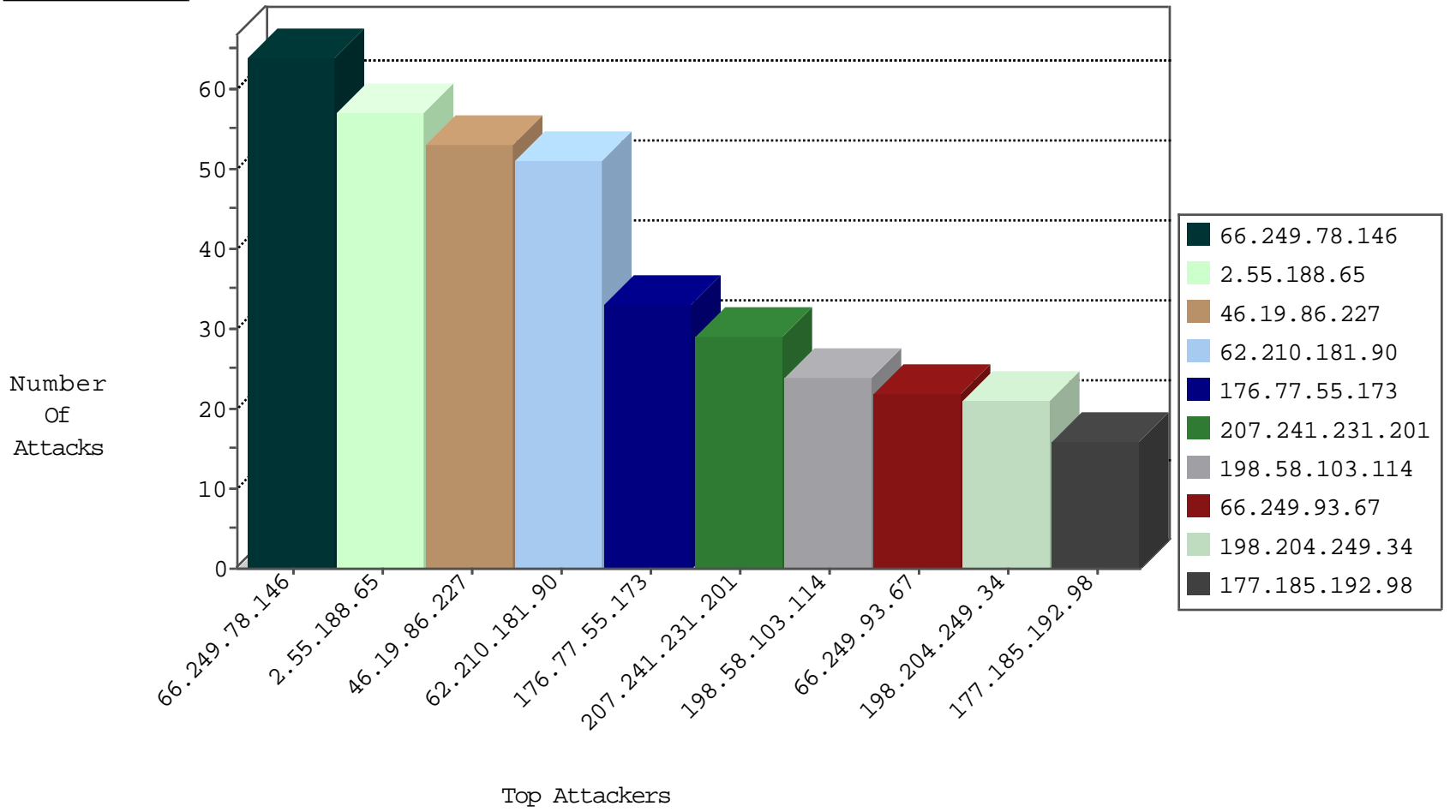
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.93.82	Israel	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	12629
167.114.156.16	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5537
66.249.93.67	Israel	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	4087
66.249.93.77	Israel	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	4
109.67.203.188	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
122.52.149.188	Philippines	147.237.77.176	matpash.idf.il	Frk_Purple_Con_Limit_Http	drop	3
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
122.52.149.188	Philippines	147.237.77.176	matpash.idf.il	Frk_Under_Attack_Con_Http	drop	2
188.138.1.218	Germany	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
85.25.43.94	Germany	147.237.76.176	test.ncore.idf.i	Block_Udp_All_Nets	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
177.185.192.98	Brazil	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
216.249.107.200	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
177.185.192.98	147.237.77.74	Brazil	law.idf.il	SQL Injection - Select From	12
109.253.139.245	147.237.72.166	Israel	aka.idf.il	GPL SCAN myscan	2
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
109.253.139.245	147.237.72.166	Israel	aka.idf.il	INDICATOR-SCAN myscan	2
66.240.213.93	147.237.76.31	United States	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
173.193.130.54	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 2048	1
66.240.213.93	147.237.76.39	United States	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
173.193.130.54	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -f -sS	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	63
62.210.181.90	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
176.77.55.173	Russian Federation	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	33
198.58.103.114	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
198.204.249.34	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
207.241.231.201	United States	147.237.72.166	aka.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	19
81.218.134.102	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
91.109.30.103	Germany	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	12
198.58.102.117	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
207.241.231.201	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	10
176.106.46.74	Palestinian Territory, Occupied	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	10
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
173.60.112.13	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
207.46.13.32	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
66.249.93.249	Europe	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
108.171.128.189	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
2.54.97.198	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
73.25.158.80	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
54.151.42.39	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
2.53.139.55	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
85.130.184.55	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
50.23.254.154	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
92.222.23.240	France	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
85.130.184.55	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
66.249.93.77	Europe	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	4
188.120.154.207	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
81.218.126.226	Israel	147.237.0.35	akaws.idf.il	drop		drop	3
212.143.214.165	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
130.193.51.73	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.55.26.132	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.78.206	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.29	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.53.21.143	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
157.55.39.167	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.88.98	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
81.218.241.26	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
109.253.139.245	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.70.79.196	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.50.113	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.102.242.21	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.55.188.65	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	57
46.19.86.227	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	53
109.253.225.240	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
109.253.225.251	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
68.180.230.45	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8878-he/refuah.aspx	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	1
194.28.115.231	Netherlands	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
85.130.222.103	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https://www.idf.il/	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
2.53.9.209	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
109.253.225.248	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/templatecontrols/generic/	Block	1
87.70.57.164	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
66.249.93.98	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1501-he/atal.aspx	Block	1
73.25.158.80	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/mobile	Block	1
66.249.66.121	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/6/2826.jpg	Block	1
106.38.241.100	China	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.93.102	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/favicon.ico	Block	1
149.202.75.239	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/tikshuv/index.htm-	Block	1
79.176.20.127	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https://www.idf.il/	Block	1
66.249.66.123	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/8/2978.jpg	Block	1
106.120.173.142	China	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.93.110	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1501-he/atal.aspx	Block	1
66.249.64.137	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
157.55.39.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
81.223.254.34	Austria	147.237.77.74	law.idf.il	Unauthorized URL Access to /robots.txt	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/mqm	Block	1