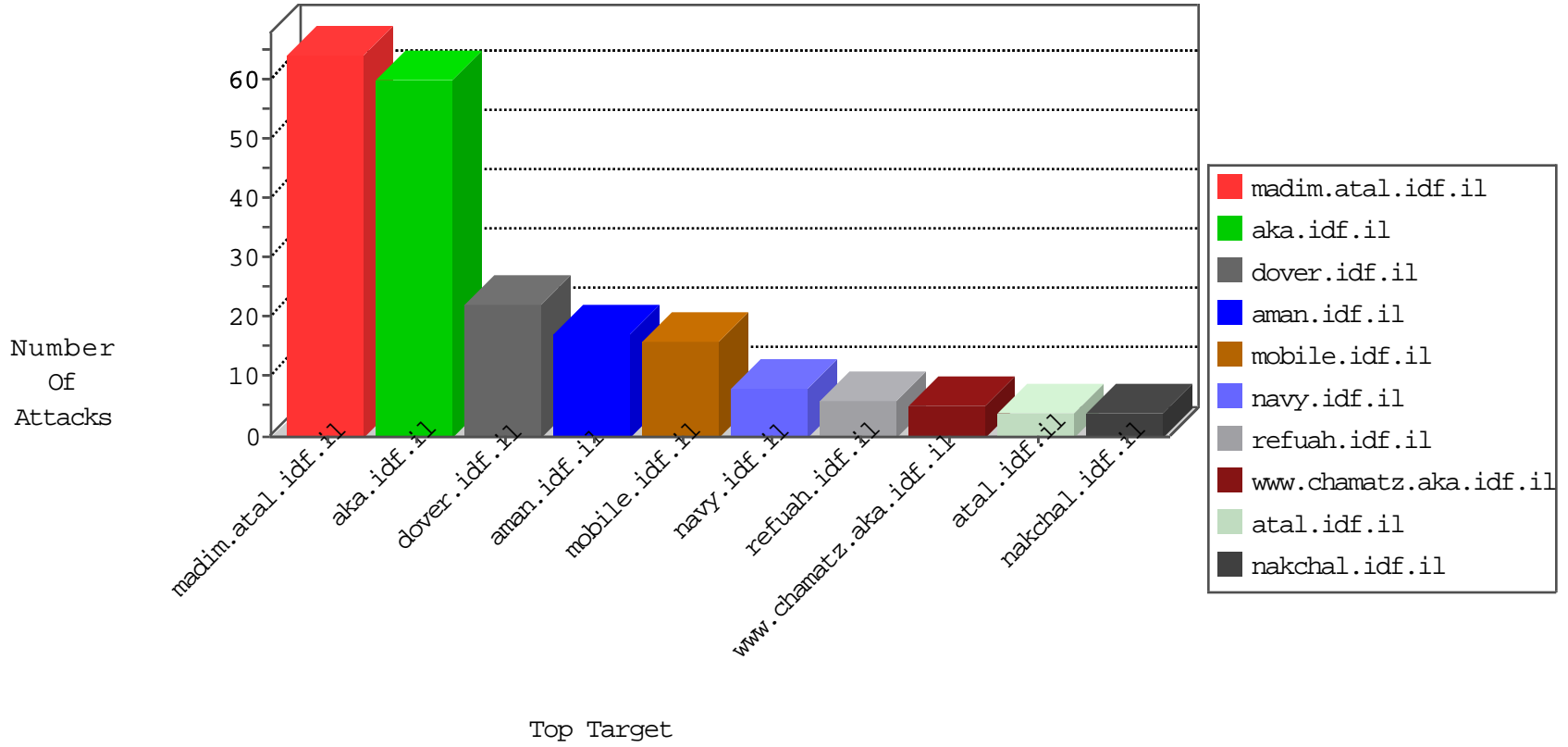


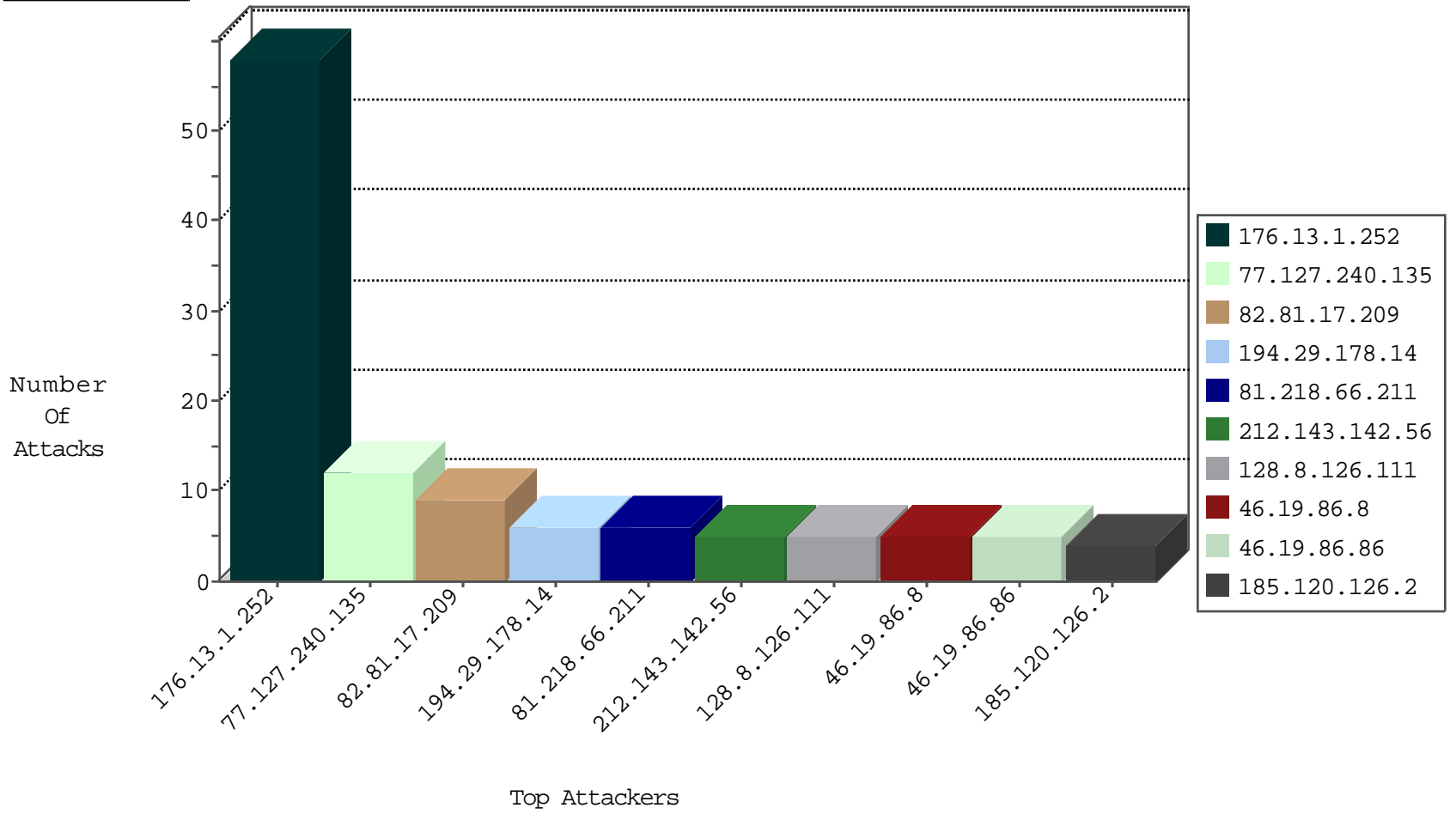
IDF Under Attack Daily Report



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	6
128.8.126.111	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	5
128.42.142.45	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
198.133.224.147	United States	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
134.197.113.3	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
128.223.8.112	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
139.78.141.243	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
129.97.74.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
195.113.161.82	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
130.194.252.8	Australia	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
131.247.2.241	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
123.59.59.52	China	147.237.76.39	mobile.meitav.idf.il	block-sp-traf1	forward	1
160.80.221.37	Italy	147.237.72.167	ishurim.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
128.208.4.99	United States	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1
200.19.159.34	Brazil	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1
129.93.229.139	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
130.217.77.2	New Zealand	147.237.72.217	e.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
131.247.2.241	United States	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1
129.10.120.193	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
46.19.86.8	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
156.56.250.226	United States	147.237.72.217	e.idf.il	network flood IPv4 ICMP	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
144.76.30.236	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
178.63.86.11	Germany	147.237.76.86	navy.idf.il	C1000074: HTTP: majestic bot	Permit	2
62.210.90.118	France	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Permit	2
151.80.31.159	France	147.237.77.233	atal.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
91.201.236.50	147.237.8.50	Ukraine	e.tikshuv.idf.il	ET SCAN NMAP -sS window 4096	1
220.231.195.122	147.237.77.226	China	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 4096	1
220.225.2.174	147.237.77.74	India	law.idf.il	ET SCAN NMAP -sS window 3072	1
212.227.55.94	147.237.0.16	Germany	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
208.73.143.36	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
106.38.241.105	147.237.76.86	China	navy.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
91.201.236.50	147.237.8.50	Ukraine	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
220.231.195.122	147.237.77.226	China	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 3072	1
220.225.2.174	147.237.77.74	India	law.idf.il	ET SCAN NMAP -sS window 1024	1
212.227.55.94	147.237.0.15	Germany	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
201.38.68.132	147.237.0.35	Brazil	akaws.idf.il	ET SCAN NMAP -sS window 1024	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
81.218.66.211	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
77.127.240.135	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
193.106.206.10	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
77.127.240.135	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	4
87.69.49.231	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
185.120.126.2	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	3
66.249.64.163	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
157.55.39.30	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.8	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
2.55.166.124	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
77.127.240.135	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
80.246.137.159	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
46.19.86.86	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
88.135.189.1	Poland	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
46.19.86.86	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
201.38.68.132	Brazil	147.237.0.35	akaws.idf.il	drop		drop	2
77.127.240.135	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
46.19.86.8	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.122.172	United States	147.237.76.176	test.ncore.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
2.54.193.31	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.118	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
185.20.5.157	United Kingdom	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
46.19.86.86	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
176.221.173.9	Georgia	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
23.95.31.63	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.168	United States	147.237.8.45	e.eitan.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
137.116.71.170	United States	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
207.46.13.162	United States	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
180.97.106.161	China	147.237.72.167	ishurim.aka.idf.il	drop	SAM rule	drop	1
141.212.122.173	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.123	United States	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
84.111.190.218	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
185.20.5.157	United Kingdom	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
46.19.86.220	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
180.97.106.37	China	147.237.72.156	aman.idf.il	drop	SAM rule	drop	1
37.26.148.196	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.169	United States	147.237.8.45	e.eitan.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
137.116.71.170	United States	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
180.97.106.161	China	147.237.77.226	www.chamatz.aka.idf.il	drop	SAM rule	drop	1
46.19.86.8	Israel	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	illegal header format detected: Illegal start line in request	monitor	1
141.226.217.92	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
5.29.81.31	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
141.212.122.124	United States	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
180.97.106.37	China	147.237.76.39	mobile.meitav.idf.il	drop	SAM rule	drop	1
46.19.85.61	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.171	United States	147.237.76.176	test.ncore.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
137.116.71.170	United States	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
180.97.106.162	China	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
5.29.81.31	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.1.252	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	58
82.81.17.209	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Email in mobile.idf.il/sachar/createaccount	Block	9
216.9.110.13	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/yahash2016/lobby.aspx	Block	2
46.19.86.179	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.253.131.23	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.76.31	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
212.179.21.194	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1
82.205.1.154	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1141-ar/dover.aspx'	Block	1
66.249.64.113	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/m/main/giyus/general.aspx	Block	1
124.73.11.123	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/1172-he/idfg.aspx/trackback/	Block	1
68.180.229.41	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/404.aspx	Block	1
85.65.17.111	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.64.183	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1086-he/dover.aspx	Block	1
68.180.229.105	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/templates/shared/usercontrols/headerupper/	Block	1
106.38.241.105	China	147.237.76.86	navy.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.65.131	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/mobile/templates/getfile/getfile.aspx	Block	1
185.120.126.2	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc	Block	1
77.138.157.248	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https://www.aman.idf.il/	Block	1
66.249.75.171	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/ozxeziezpgbeidy.html	Block	1
212.126.108.52	Iraq	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 212.126.108.52 (Open Mode)	None	1
66.249.64.9	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1
124.73.11.123	China	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 124.73.11.123	Block	1