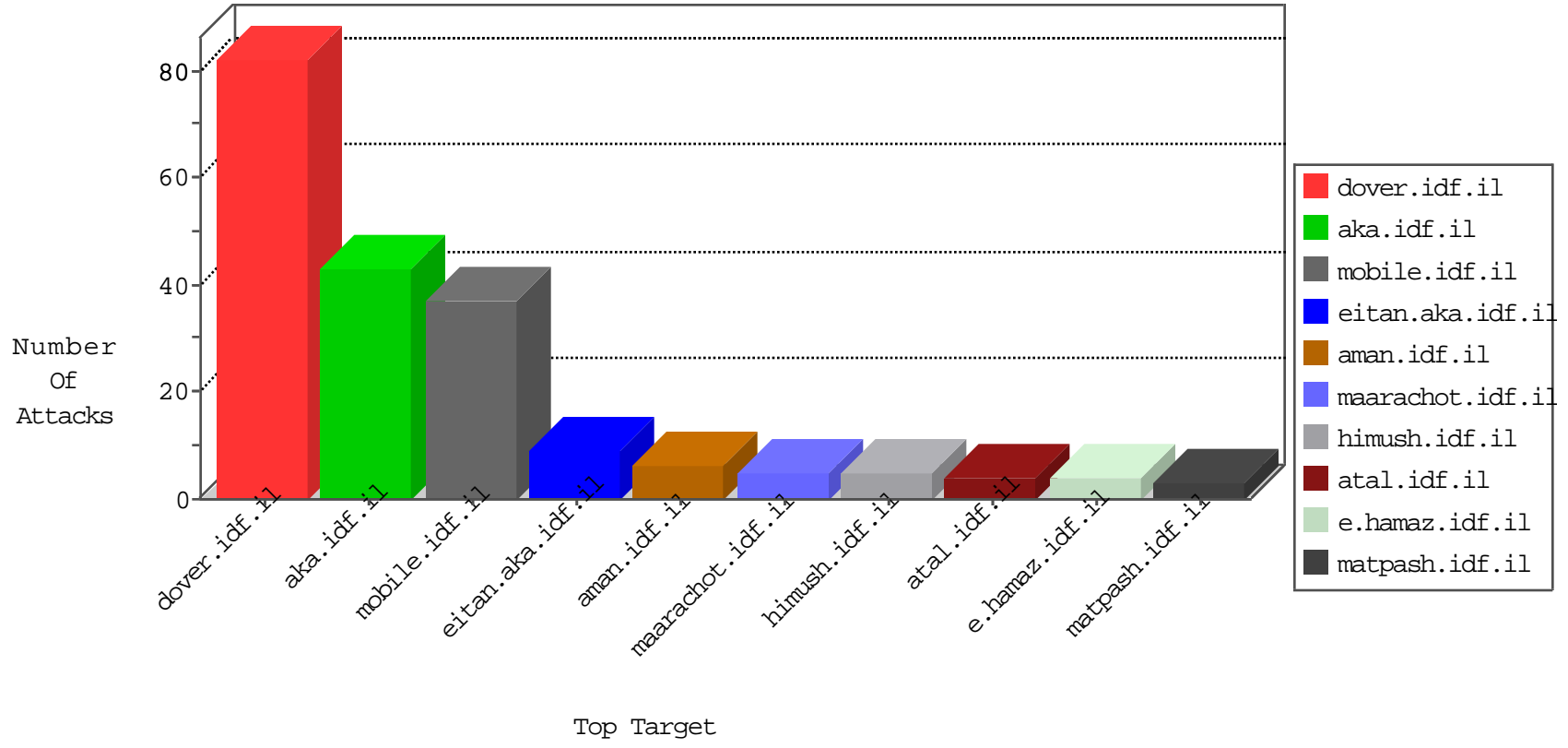


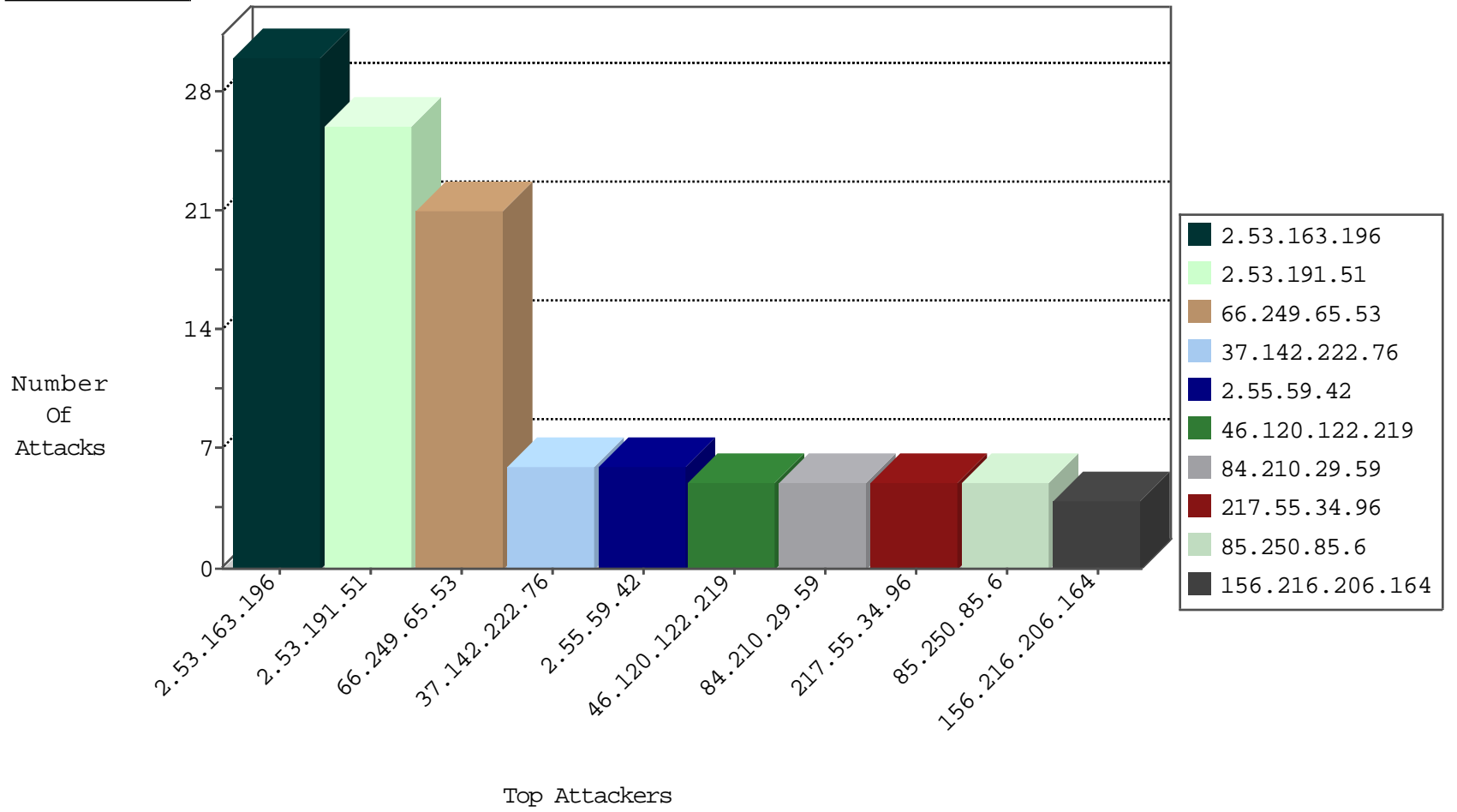
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
93.174.94.235	Netherlands	147.237.76.148	gqcenter.aka.idf.il	Black List	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
62.210.247.125	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
162.210.196.129	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
46.120.122.219	147.237.77.216	Israel	dover.idf.il	Xenu Link Sleuth User Agent	4
59.67.64.13	147.237.77.179	China	e.mazi.idf.il	GPL SCAN nmap TCP	2
156.202.29.57	147.237.77.216	Egypt	dover.idf.il	ET WEB_SERVER Poison Null Byte	2
84.210.29.59	147.237.8.50	Norway	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
208.100.26.228	147.237.76.177	United States	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
84.210.29.59	147.237.8.28	Norway	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
196.47.173.21	147.237.76.30	Cote D'Ivoire	himush.idf.il	ET SCAN NMAP -sS window 1024	1
84.210.29.59	147.237.8.14	Norway	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
180.213.5.205	147.237.76.196	China	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
109.236.86.32	147.237.77.233	Netherlands	atal.idf.il	ET SCAN NMAP -sS window 1024	1
5.255.90.133	147.237.72.14	Netherlands	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
94.102.48.194	147.237.76.44	Netherlands	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.194	147.237.76.38	Netherlands	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
89.163.224.115	147.237.76.42	Germany	refuah.idf.il	ET SCAN Potential SSH Scan	1
211.149.222.5	147.237.77.19	China	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
84.210.29.59	147.237.8.46	Norway	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
196.47.173.21	147.237.76.30	Cote D'Ivoire	himush.idf.il	ET SCAN NMAP -sS window 2048	1
84.210.29.59	147.237.8.24	Norway	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
196.47.173.21	147.237.76.30	Cote D'Ivoire	himush.idf.il	ET SCAN NMAP -f -sS	1
66.249.76.117	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
180.213.5.205	147.237.72.14	China	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
54.147.50.220	147.237.76.202	United States	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
109.236.86.32	147.237.77.243	Netherlands	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
14.152.59.11	147.237.0.200	China	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
109.236.86.32	147.237.76.177	Netherlands	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
5.206.231.131	147.237.8.50	Portugal	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.194	147.237.76.39	Netherlands	mobile.meitav.idf.i	ET SCAN NMAP -sS window 1024	1
89.163.224.115	147.237.76.44	Germany	e.refuah.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
2.53.163.196	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
66.249.65.53	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	21
2.55.59.42	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.53.191.51	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
2.53.191.51	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	5
2.53.191.51	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
2.53.191.51	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
85.250.85.6	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
2.53.191.51	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
109.65.153.186	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
217.55.34.96	Egypt	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	3
66.249.65.10	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
207.46.13.138	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.110.110.95	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
5.102.242.14	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
156.216.206.164	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
109.253.147.185	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
207.46.13.58	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
157.25.166.66	Poland	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
46.117.18.61	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
177.74.154.97	Brazil	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
217.55.34.96	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
176.13.225.142	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
93.172.98.105	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
185.27.105.76	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
156.216.206.164	Egypt	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
207.46.13.149	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
147.235.8.64	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
66.249.64.105	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
141.212.122.103	United States	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
2.53.5.12	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
72.204.67.171	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
46.19.86.126	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
176.13.237.215	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
156.198.3.81	Egypt	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	1
66.249.64.107	Israel	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
40.77.169.102	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.104	United States	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
84.109.80.65	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
156.198.3.81	Egypt	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
138.246.253.19	Germany	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
66.249.64.107	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
207.46.13.72	United States	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
46.19.85.130	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
176.13.11.12	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
147.235.8.64	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	1
46.121.111.103	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
185.20.5.157	United Kingdom	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	1
2.53.191.51	Israel	147.237.77.216	dover.idf.il	drop	Unexpected post SYN packet - RST or SYN expected	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.142.222.76	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/2/	Block	5
151.228.132.172	United Kingdom	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/	Block	4
190.247.154.215	Argentina	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/	Block	2
2.55.173.177	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
157.55.39.12	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/	Block	1
46.121.89.28	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
79.75.35.152	United Kingdom	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
37.26.149.196	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
176.13.237.215	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1501-he/atal.aspx	Block	1
66.249.65.52	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.52	Block	1
89.139.223.186	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/dover/site/mainpage.asp	Block	1
37.142.222.76	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 37.142.222.76	Block	1
176.14.37.75	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/gyus/yahash2017/lobby.aspx	Block	1
66.249.65.52	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atall/izkor/view_img.asp	Block	1
109.253.134.47	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
66.249.76.75	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
46.120.122.219	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/milum/templates/inner.asp	Block	1
77.138.45.57	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/favicon.ico	Block	1