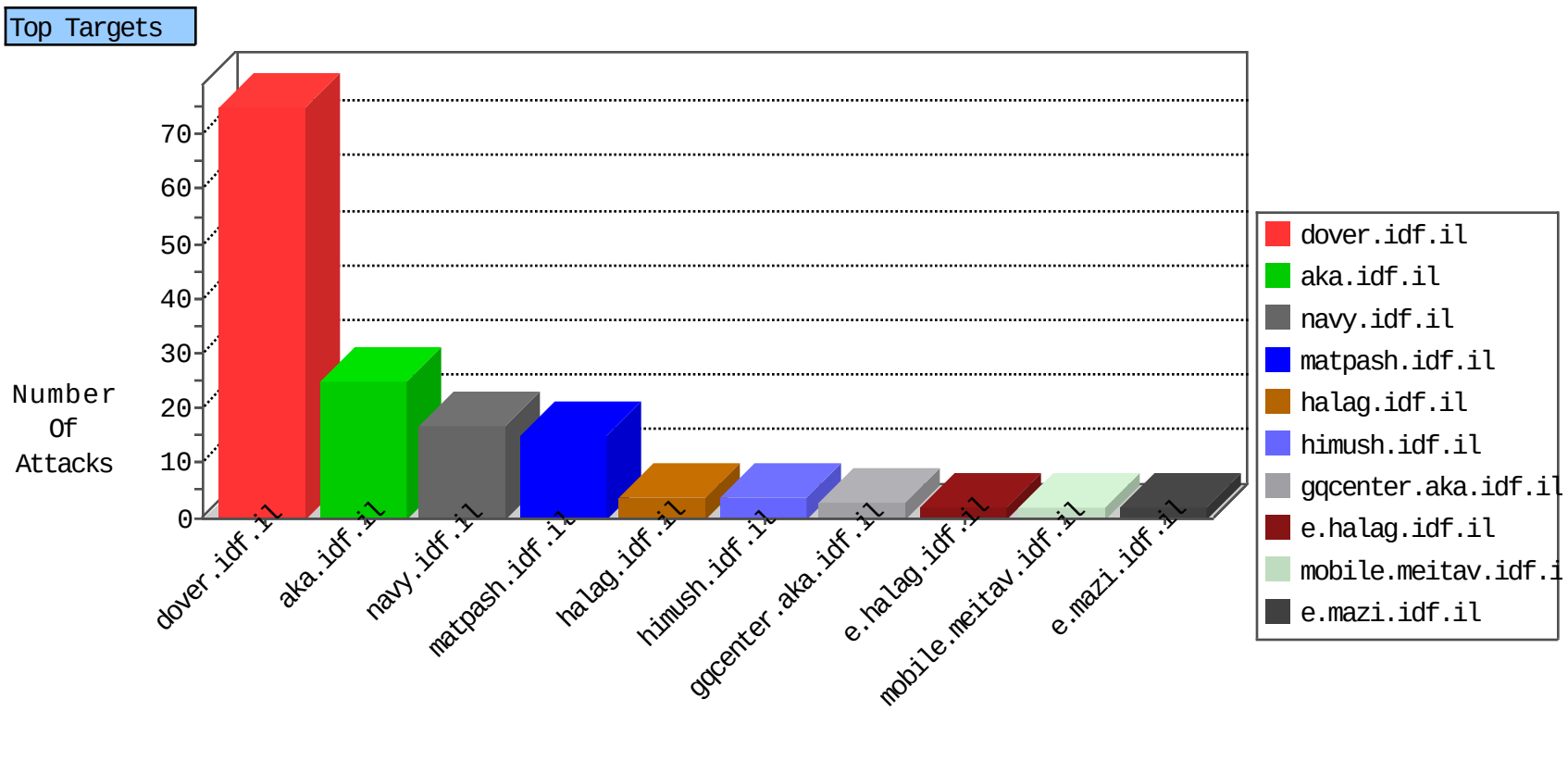
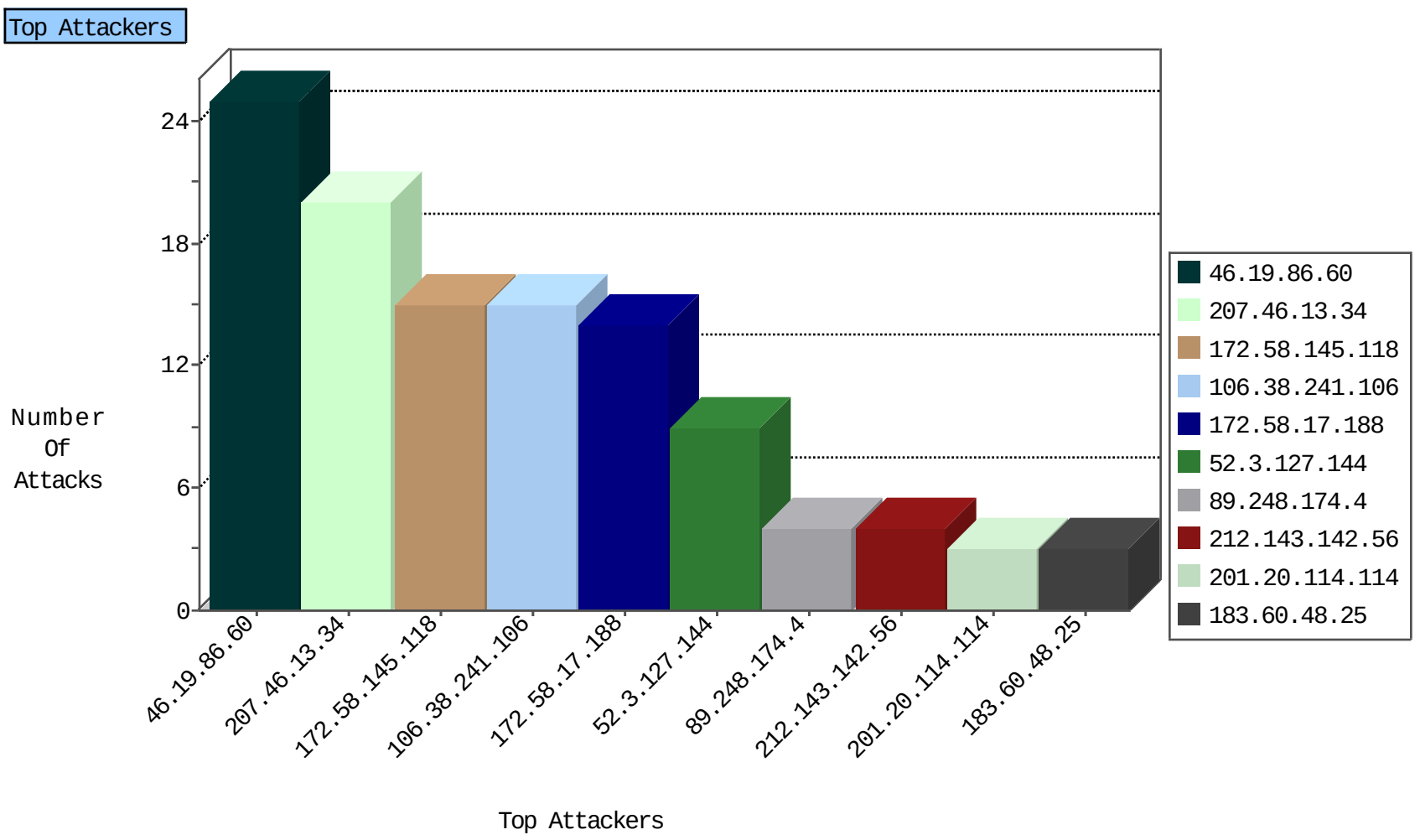
10-03-2016-04:04:01 to 10-03-2016-05:04:01

IDF Under Attack
Daily Report





10-03-2016-04:04:01 to 10-03-2016-05:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

10-03-2016-04:04:01 to 10-03-2016-05:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	15
178.151.143.163	Ukraine	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2

10-03-2016-04:04:01 to 10-03-2016-05:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
201.20.114.114	147.237.0.35	Brazil	akaws.idf.il	ET SCAN Potential SSH Scan	1
198.58.110.199	147.237.8.45	United States	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
183.129.160.229	147.237.76.176	China	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
123.59.173.17	147.237.77.235	China	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
61.221.69.222	147.237.8.46	Taiwan	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
58.220.2.5	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
208.100.26.228	147.237.76.148	United States	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
46.120.122.219	147.237.72.166	Israel	aka.idf.il	Xenu Link Sleuth User Agent	1
201.20.114.114	147.237.76.202	Brazil	e.halag.idf.il	ET SCAN Potential SSH Scan	1
201.20.114.114	147.237.0.33	Brazil	idf.il	ET SCAN Potential SSH Scan	1
183.129.160.229	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
183.60.48.25	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
85.120.95.250	147.237.76.39	Romania	mobile.meitav.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
61.221.69.222	147.237.8.28	Taiwan	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
58.220.2.5	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
202.106.38.21	147.237.77.216	China	dover.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1

10-03-2016-04:04:01 to 10-03-2016-05:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
207.46.13.34	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	19
172.58.145.118	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	15
172.58.17.188	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	11
46.19.86.60	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.86.60	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
52.3.127.144	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	6
46.19.86.60	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.60	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
172.58.17.188	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
66.249.76.109	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
108.41.45.37	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
52.3.127.144	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
141.212.122.98	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
52.198.122.46	Japan	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.139.116	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.20	United States	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
89.248.174.4	Netherlands	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.19.86.176	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
109.67.104.115	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
62.210.243.100	France	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.30	United States	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
89.248.174.4	Netherlands	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
109.201.154.143	Netherlands	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
212.143.142.44	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.31	United States	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
89.248.174.4	Netherlands	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
52.3.127.144	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	1
138.246.253.19	Germany	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
88.145.183.63	United Kingdom	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
141.212.122.97	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
89.248.174.4	Netherlands	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
184.105.139.99	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.19	United States	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
88.145.183.63	United Kingdom	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	1
216.218.206.94	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1

10-03-2016-04:04:01 to 10-03-2016-05:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.76.112	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.76.112	Block	1
46.101.138.168	Germany	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
77.138.126.79	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/pniotanswer.aspx	Block	1
66.249.76.61	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/.well-known/assetlinks.json	Block	1
2.92.39.174	Russian Federation	147.237.72.156	aman.idf.il	Unauthorized Method POST for list.ips.gov.il/	Block	1
66.249.76.112	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/apple-app-site-association	Block	1
46.120.122.219	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	1
204.79.180.36	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/miluim/templates/inner.asp	Block	1
66.249.76.62	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.76.62	Block	1
36.88.60.160	Indonesia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	1
66.249.76.113	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/.well-known/apple-app-site-association	Block	1
54.193.212.129	United States	147.237.77.216	dover.idf.il	Distributed Parameter Type Violation on www.idf.il/1065-he/dover.aspx parameter SearchText	Block	1
204.79.180.134	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/main/	Block	1
66.249.76.62	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/apple-app-site-association	Block	1
46.4.74.42	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1
66.249.79.44	Israel	147.237.76.31	nakchal.idf.i	Unauthorized URL Access to www.nakhal.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
66.102.6.4	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/sachar	Block	1
66.249.76.75	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
46.101.138.168	Germany	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 46.101.138.168 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
71.233.104.216	United States	147.237.72.166	aka.idf.il	Unknown Parameter docId in www.aka.idf.il/main/giyus/yahash2017/lobby.aspx	None	1
66.249.64.60	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1

10-03-2016-04:04:01 to 10-03-2016-05:04:01