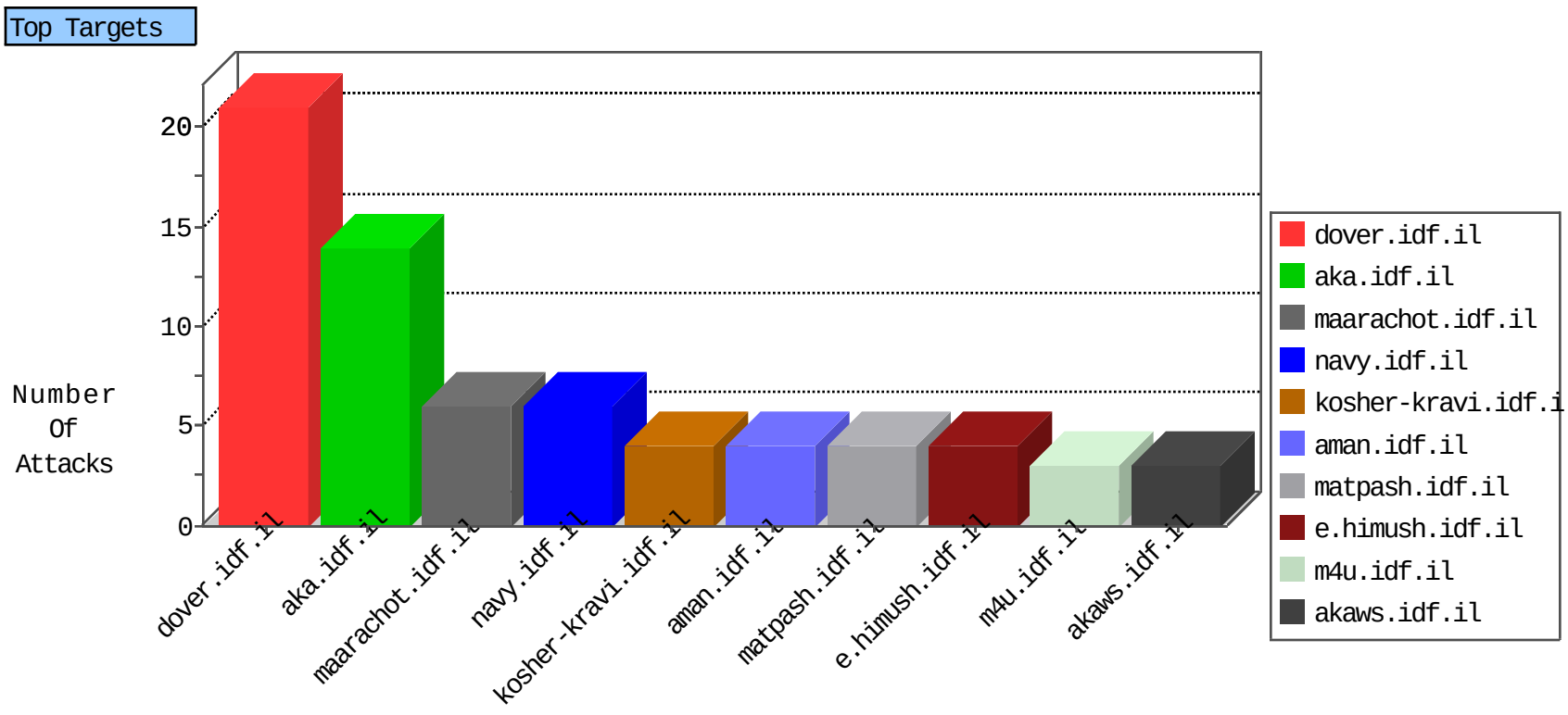
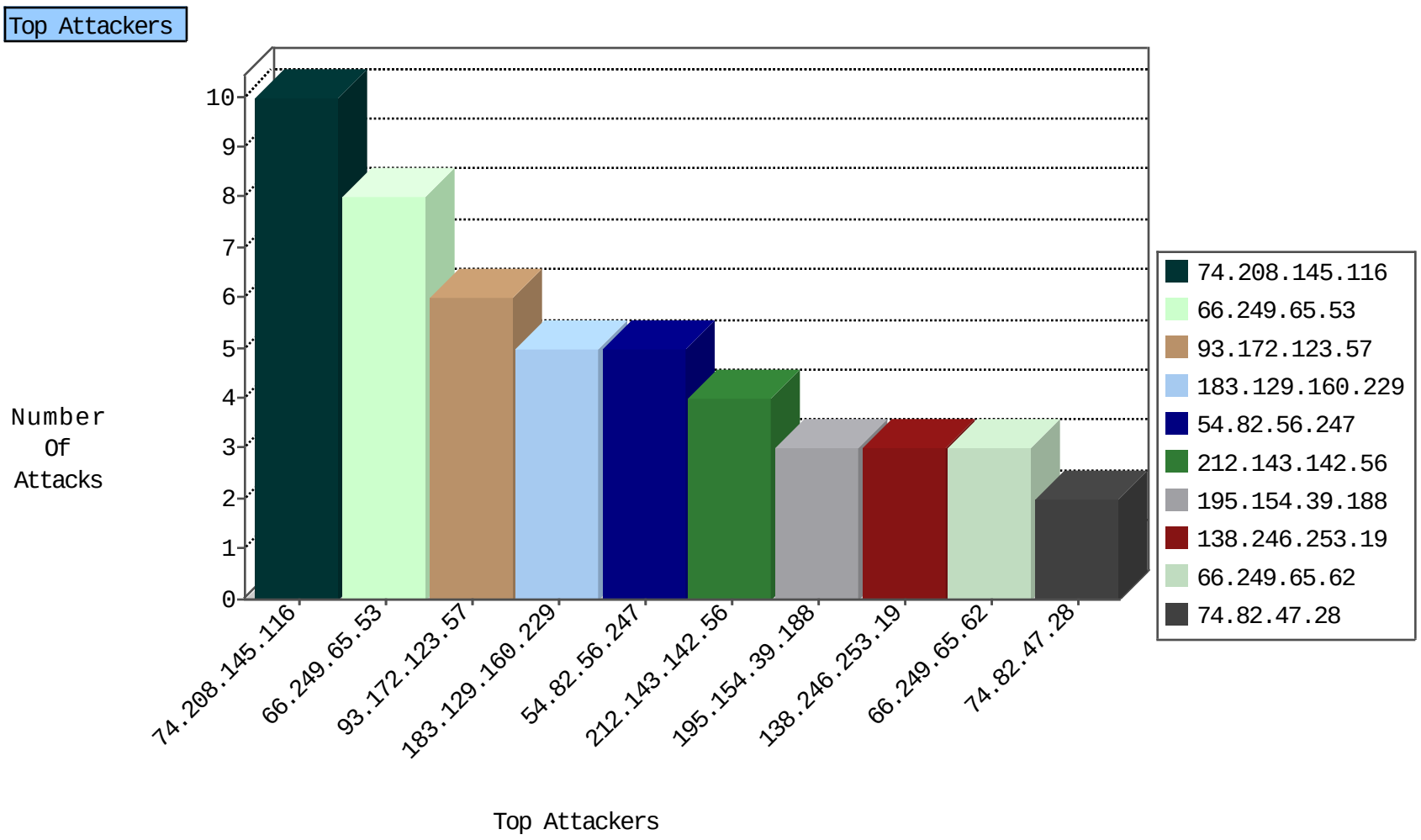
10-04-2016-04:04:05 to 10-04-2016-05:04:05

IDF Under Attack Daily Report

Top Targets



Top Attackers



10-04-2016-04:04:05 to 10-04-2016-05:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
93.174.94.235	Netherlands	147.237.76.197	e.himush.idf.il	Black List	drop	1

10-04-2016-04:04:05 to 10-04-2016-05:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.106	China	147.237.72.156	aman.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	2

10-04-2016-04:04:05 to 10-04-2016-05:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
117.5.148.240	147.237.77.216	Vietnam	dover.idf.il	Xenu Link Sleuth User Agent	2
195.154.39.188	147.237.0.200	France	m4u.idf.il	ET SCAN Potential SSH Scan	1
62.210.243.100	147.237.76.197	France	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
62.150.255.205	147.237.76.197	Kuwait	e.himush.idf.il	ET SCAN NMAP -sS window 4096	1
45.32.194.53	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
12.139.34.20	147.237.77.121	United States	e.navy.idf.il	ET SCAN NMAP -sS window 2048	1
222.186.56.242	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
195.154.39.188	147.237.76.30	France	himush.idf.il	ET SCAN Potential SSH Scan	1
195.154.39.188	147.237.0.15	France	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.194	147.237.76.177	Netherlands	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
62.210.243.100	147.237.76.147	France	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
62.150.255.205	147.237.76.197	Kuwait	e.himush.idf.il	ET SCAN NMAP -sS window 3072	1
14.152.59.11	147.237.76.201	China	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
12.139.34.20	147.237.77.121	United States	e.navy.idf.il	ET SCAN NMAP -f -sS	1
208.100.26.228	147.237.76.148	United States	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1

10-04-2016-04:04:05 to 10-04-2016-05:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.65.53	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	8
93.172.123.57	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
66.249.65.62	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
54.82.56.247	United States	147.237.77.170	maarachot.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	3
23.248.237.25	United States	147.237.0.200	m4u.idf.il	drop		drop	2
172.247.84.209	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
23.224.124.23	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
74.208.145.116	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
172.247.84.214	United States	147.237.0.35	akaws.idf.il	drop		drop	2
23.248.234.22	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
172.58.175.32	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
172.247.84.219	United States	147.237.0.33	idf.il	drop		drop	2
172.247.82.206	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
172.247.84.195	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
109.253.199.194	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
74.208.145.116	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
188.44.55.20	Russian Federation	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
183.129.160.229	China	147.237.77.179	e.mazi.idf.il	drop	SAM rule	drop	1
2.53.4.255	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.104	United States	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.208.145.116	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.82.47.31	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
184.105.247.220	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
31.210.188.85	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
118.173.172.244	Thailand	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
74.208.145.116	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
74.82.47.15	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
183.129.160.229	China	147.237.77.205	prisha.idf.il	drop	SAM rule	drop	1
141.212.122.105	United States	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.82.47.59	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
184.105.247.244	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
46.19.86.76	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
138.246.253.19	Germany	147.237.0.35	akaws.idf.il	drop		drop	1
74.208.145.116	United States	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.82.47.28	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
183.129.160.229	China	147.237.77.233	atal.idf.il	drop	SAM rule	drop	1
184.105.247.244	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
74.208.145.116	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
138.246.253.19	Germany	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.208.145.116	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
74.82.47.28	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
183.129.160.229	China	147.237.77.243	mobile.idf.il	drop	SAM rule	drop	1
23.248.237.5	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
93.174.93.218	Netherlands	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
74.208.145.116	United States	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
188.44.55.20	Russian Federation	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	1
183.129.160.229	China	147.237.77.170	maarachot.idf.il	drop	SAM rule	drop	1
138.246.253.19	Germany	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
74.208.145.116	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.8.91.141	Palestinian Territory, Occupied	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/	Block	1
66.249.64.45	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/5/69215.jpg	Block	1
68.180.229.178	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
54.82.56.247	United States	147.237.77.170	maarachot.idf.il	Malformed URL 54.90.189.128:80	Block	1
66.249.66.18	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/apple-app-site-association	Block	1
89.138.246.248	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/yahash2018/lobby.aspx	Block	1
54.82.56.247	United States	147.237.77.170	maarachot.idf.il	NULL Character in Method	Block	1
66.249.69.239	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/1294-en/cogat	Block	1
178.255.215.87	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/robots.txt	Block	1
66.147.244.101	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	1
66.249.76.75	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
207.46.13.172	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
66.249.64.12	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
66.249.76.81	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/apple-app-site-association	Block	1