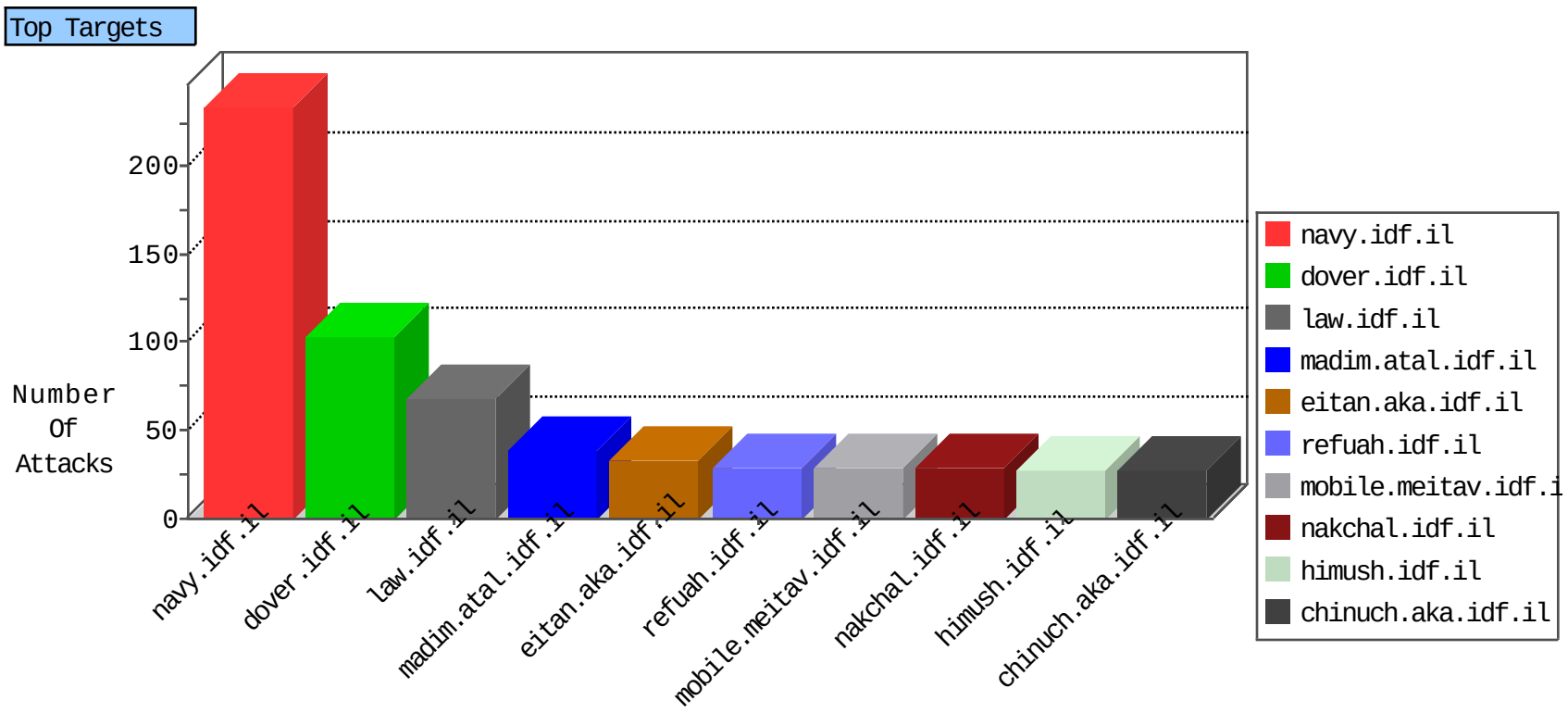
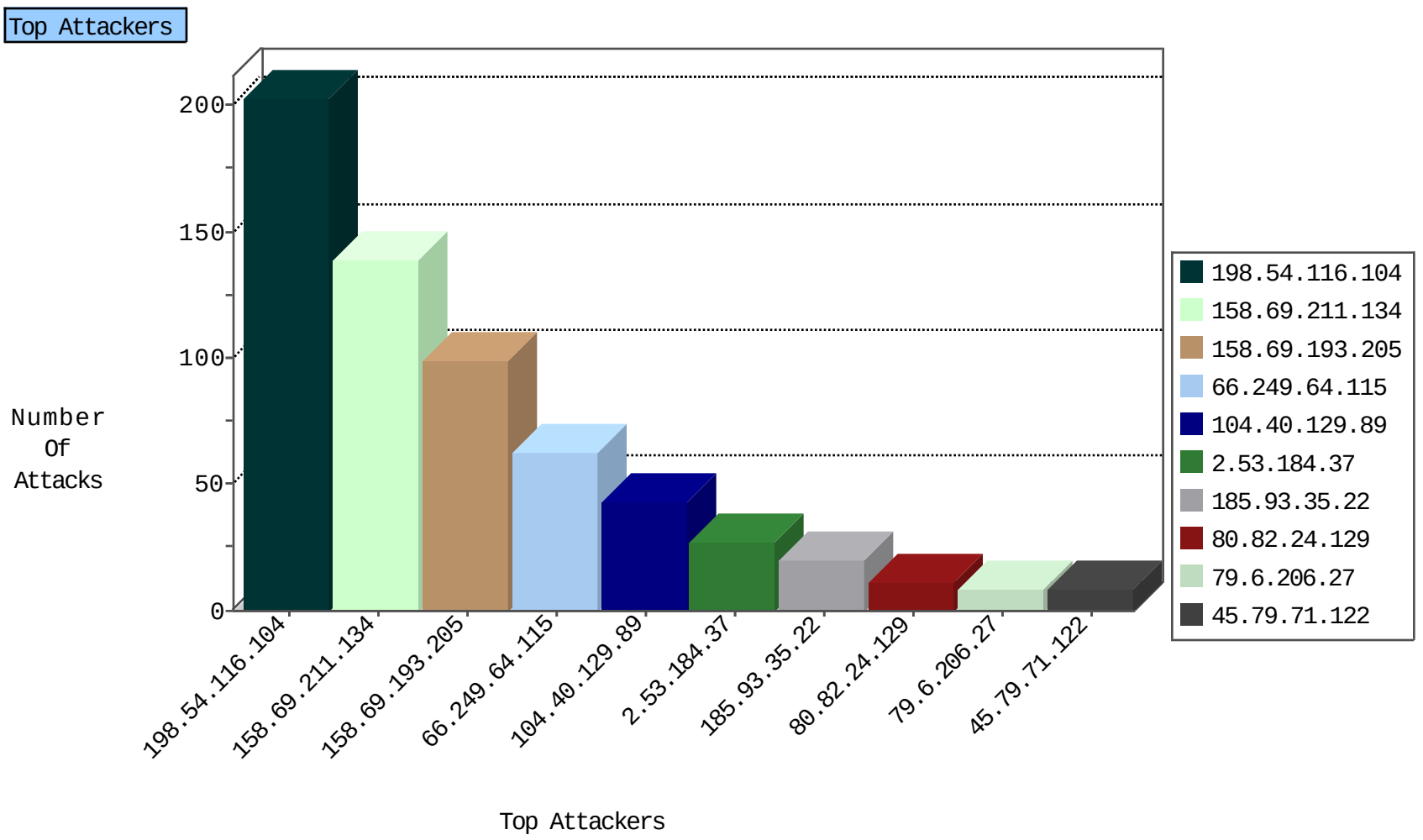
09-07-2016-02:04:00 to 09-07-2016-03:04:00

IDF Under Attack Daily Report





09-07-2016-02:04:00 to 09-07-2016-03:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	4
66.249.69.251	Israel	147.237.72.166	aka.idf.il	HTTP-Misc-BadBlue-Dir-Trave-2	dest-reset	1

09-07-2016-02:04:00 to 09-07-2016-03:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
199.58.86.211	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	3

09-07-2016-02:04:00 to 09-07-2016-03:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.64.115	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	63
45.79.71.122	147.237.77.216	United States	dover.idf.il	WEB-MISC Chunked-Encoding transfer attempt	2
50.116.123.135	147.237.8.27	United States	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
221.204.249.157	147.237.72.217	China	e.idf.il	ET SCAN NMAP -sS window 1024	1
202.65.138.2	147.237.76.44	India	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
143.0.115.31	147.237.76.44	Brazil	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
64.137.171.55	147.237.77.61	Canada	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
208.100.26.228	147.237.76.39	United States	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
143.0.115.31	147.237.76.44	Brazil	e.refuah.idf.il	ET SCAN NMAP -sS window 4096	1

09-07-2016-02:04:00 to 09-07-2016-03:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
198.54.116.104	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	203
185.93.35.22	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
158.69.211.134	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	16
158.69.211.134	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
158.69.211.134	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
158.69.211.134	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
158.69.211.134	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
158.69.211.134	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
158.69.211.134	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
158.69.211.134	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
158.69.193.205	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
158.69.193.205	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
158.69.193.205	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
158.69.193.205	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
158.69.193.205	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
158.69.193.205	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
158.69.193.205	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
158.69.193.205	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
79.6.206.27	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
80.82.24.129	Poland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
2.55.155.67	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.46.41.105	Israel	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	6
158.69.211.134	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
158.69.211.134	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
2.53.184.37	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
158.69.193.205	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
158.69.211.134	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	3
80.82.24.129	Poland	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
158.69.211.134	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	3
75.39.97.119	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
84.229.24.140	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
104.40.129.89	Netherlands	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
158.69.193.205	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
104.40.129.89	Netherlands	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
104.40.129.89	Netherlands	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
104.40.129.89	Netherlands	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
104.40.129.89	Netherlands	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
158.69.193.205	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
158.69.211.134	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	2
158.69.211.134	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	2
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
104.40.129.89	Netherlands	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
158.69.193.205	United States	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
104.40.129.89	Netherlands	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
158.69.193.205	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
104.40.129.89	Netherlands	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
104.40.129.89	Netherlands	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
158.69.193.205	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
158.69.193.205	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
104.40.129.89	Netherlands	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2

09-07-2016-02:04:00 to 09-07-2016-03:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.184.37	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	24
2.53.129.198	Israel	147.237.0.19	madim.atal.idf.i	Suspicious Response Code	Block	6
157.55.39.115	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
148.251.2.180	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1
66.249.69.232	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/apple-app-site-association	Block	1
45.79.71.122	United States	147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method from 45.79.71.122	Block	1
207.46.13.10	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/templates/sitemap/	Block	1
68.180.229.101	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/templates/general/eitan.aspx	Block	1
66.249.65.24	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
45.79.71.122	United States	147.237.77.216	dover.idf.il	Malformed HTTP Header Line 2	Block	1
66.249.76.75	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/yoman/yoman.asp	Block	1
45.79.71.122	United States	147.237.77.216	dover.idf.il	Unknown HTTP Request Method 1 in URL	Block	1
207.46.13.142	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/modiin/sip_storage/files/5/68625	Block	1
68.180.230.47	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1399-en/dover.aspx	Block	1
66.249.65.51	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.51	Block	1
45.79.71.122	United States	147.237.77.216	dover.idf.il	Malformed URL	Block	1
173.230.174.123	Canada	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 173.230.174.123	Block	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/eitan/pratim/pirteychayal/	Block	1
46.19.85.41	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
71.86.197.31	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
66.249.65.51	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1153-17287-	Block	1
45.79.71.122	United States	147.237.77.216	dover.idf.il	Multiple Malformed HTTP Header Line from 45.79.71.122	Block	1
173.230.174.123	Canada	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/default.aspx	Block	1
66.249.76.112	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.76.112	Block	1
66.249.64.108	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/idkonim/pages/xasdfaf.aspx	Block	1
80.82.24.129	Poland	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/edim/theproj/theproj.asp	Block	1
66.249.69.208	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/library/generaldoc.asp	Block	1
45.79.71.122	United States	147.237.77.216	dover.idf.il	Multiple Malformed URL from 45.79.71.122	Block	1
185.32.179.30	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.76.112	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/.well-known/apple-app-site-association	Block	1
66.249.64.224	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/sip_storage/files/4/444.doc	Block	1

09-07-2016-02:04:00 to 09-07-2016-03:04:00