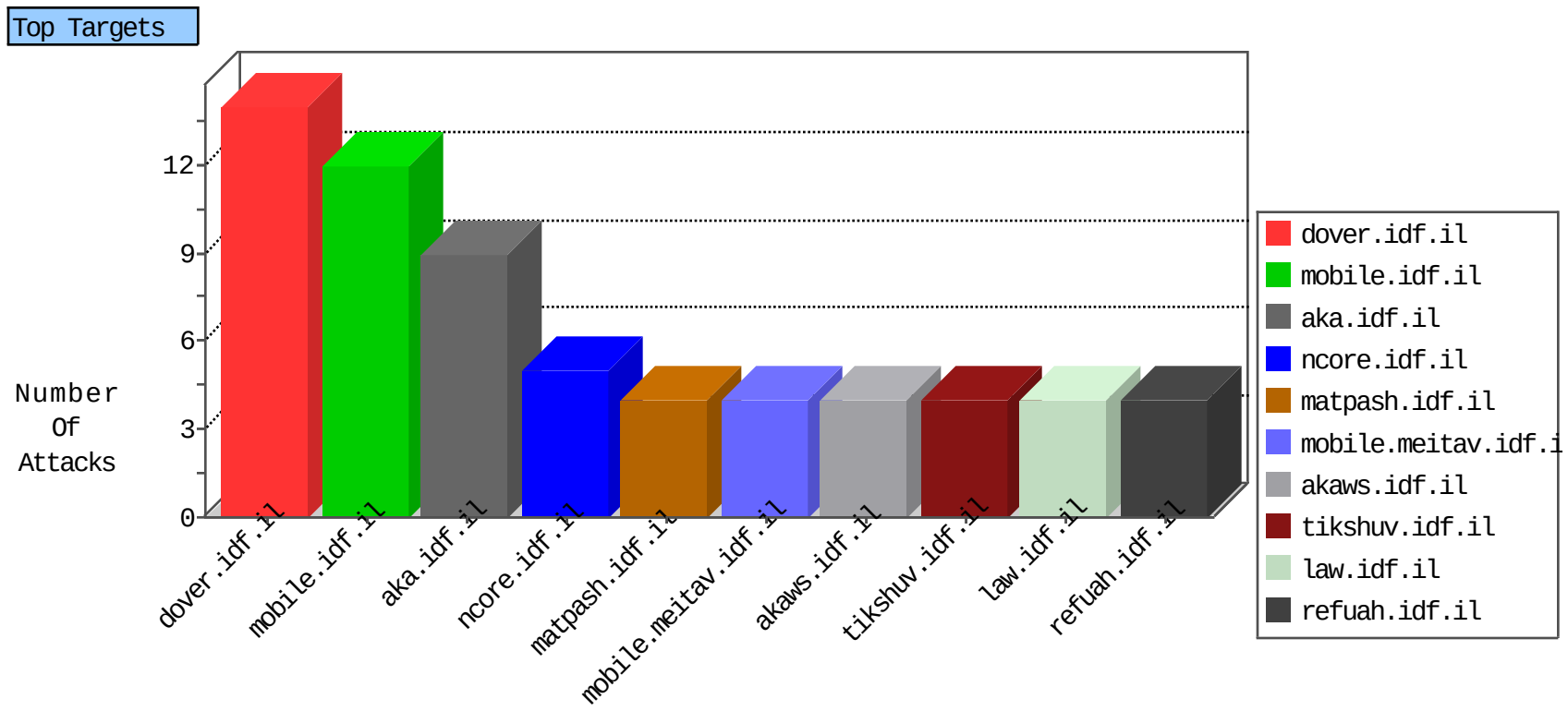
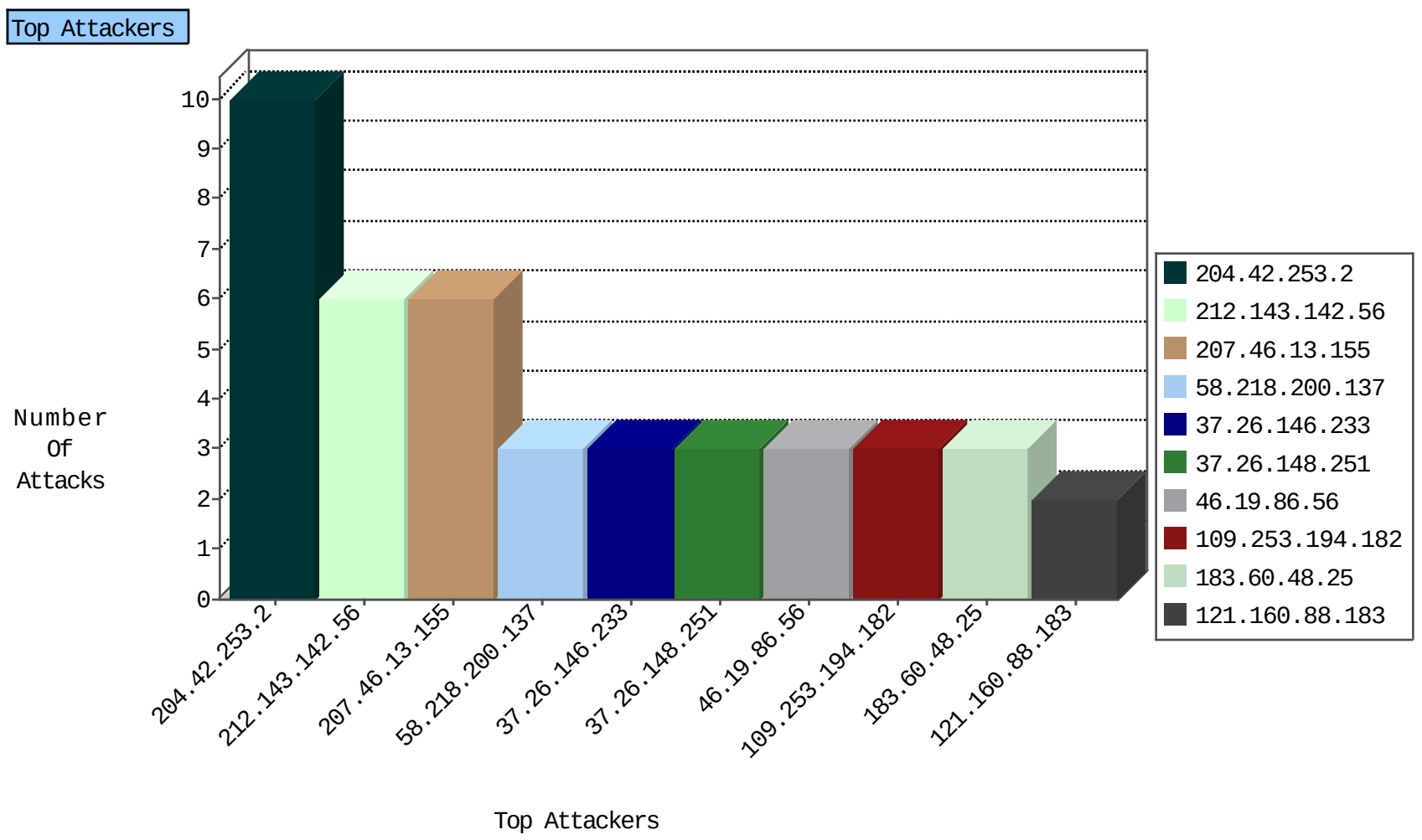
09-23-2016-04:04:04 to 09-23-2016-05:04:04

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-23-2016-04:04:04 to 09-23-2016-05:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
204.42.253.2	United States	147.237.76.30	himush.idf.il	Black List	drop	2
204.42.253.2	United States	147.237.76.39	mobile.meitav.idf.il	Black List	drop	2
204.42.253.2	United States	147.237.76.31	nakchal.idf.il	Black List	drop	2
204.42.253.2	United States	147.237.76.34	yohalan.idf.il	Black List	drop	2
204.42.253.2	United States	147.237.76.38	e.e.meitav.idf.il	Black List	drop	2
179.99.200.39	Brazil	147.237.0.34	tikshuv.idf.il	block-sp-traf1	forward	1
187.108.192.90	Brazil	147.237.76.177	ncore.idf.il	Black List	drop	1

09-23-2016-04:04:04 to 09-23-2016-05:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.4.120.3	Germany	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Permit	2
83.149.126.98	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
151.80.31.182	France	147.237.72.166	aka.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1

09-23-2016-04:04:04 to 09-23-2016-05:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
121.160.88.183	147.237.76.200	Korea, Republic of	eitan.aka.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	2
117.135.131.60	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
66.249.79.52	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	1
58.218.200.137	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
46.183.223.228	147.237.8.46	Latvia	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
220.242.82.131	147.237.77.74	China	law.idf.il	ET SCAN NMAP -f -sS	1
31.24.228.20	147.237.77.234	United Kingdom	halag.idf.il	ET SCAN NMAP -sS window 1024	1
183.60.156.140	147.237.77.74	China	law.idf.il	ET SCAN NMAP -sS window 1024	1
183.60.48.25	147.237.76.176	China	test.ncore.idf.i	ET SCAN Potential VNC Scan 5900-5920	1
125.213.243.10	147.237.76.177	Thailand	ncore.idf.il	ET SCAN Potential SSH Scan	1
106.110.106.46	147.237.8.46	China	e.chinuch.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
58.218.200.137	147.237.76.176	China	test.ncore.idf.i	ET SCAN Potential SSH Scan	1
58.218.200.137	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
220.242.82.131	147.237.77.74	China	law.idf.il	ET SCAN NMAP -sS window 2048	1
46.183.223.228	147.237.0.35	Latvia	akaws.idf.il	ET SCAN Potential SSH Scan	1
210.212.207.80	147.237.77.19	India	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
183.60.48.25	147.237.77.216	China	dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
183.60.48.25	147.237.0.19	China	madim.atal.idf.i	ET SCAN Potential VNC Scan 5900-5920	1
125.213.243.10	147.237.76.177	Thailand	ncore.idf.il	ET SCAN NMAP -sS window 1024	1

09-23-2016-04:04:04 to 09-23-2016-05:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
207.46.13.155	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
109.253.194.182	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
37.26.146.233	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.148.251	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
46.19.86.56	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
93.238.200.226	Germany	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
141.212.122.80	United States	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.133	United States	147.237.8.45	e.eitan.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.60	United States	147.237.0.35	akaws.idf.il	drop		drop	1
74.82.47.15	United States	147.237.8.27	e.madim.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.93	United States	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
104.200.151.95	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
141.212.122.136	United States	147.237.76.177	ncore.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.61	United States	147.237.0.35	akaws.idf.il	drop		drop	1
74.82.47.28	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.94	United States	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.137	United States	147.237.76.177	ncore.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.62	United States	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.82.47.53	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
216.218.206.86	United States	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.95	United States	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.48	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
157.55.39.25	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
141.212.122.63	United States	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
77.138.46.226	France	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
216.218.206.108	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.132	United States	147.237.8.45	e.eitan.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.49	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
172.56.27.171	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1

09-23-2016-04:04:04 to 09-23-2016-05:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.64.105	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/manilot/login/	Block	1
77.138.45.12	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/miluim/	Block	1
2.55.151.127	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/miluim/	Block	1
157.55.39.228	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/robots.txt	Block	1
63.238.236.71	United States	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
207.46.13.108	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
66.102.9.2	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
207.46.13.191	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/recruitinformation/faq/pages/default.aspx	Block	1

09-23-2016-04:04:04 to 09-23-2016-05:04:04