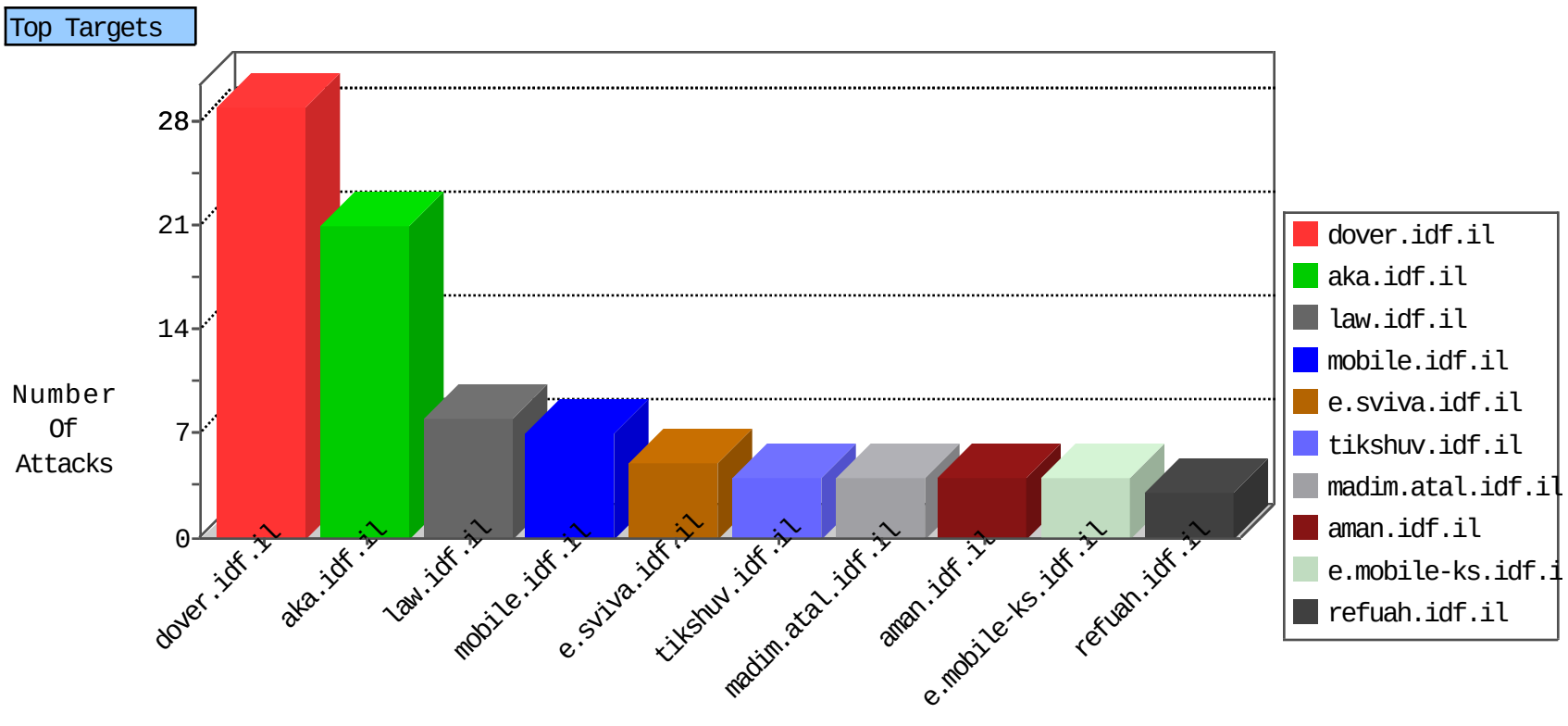
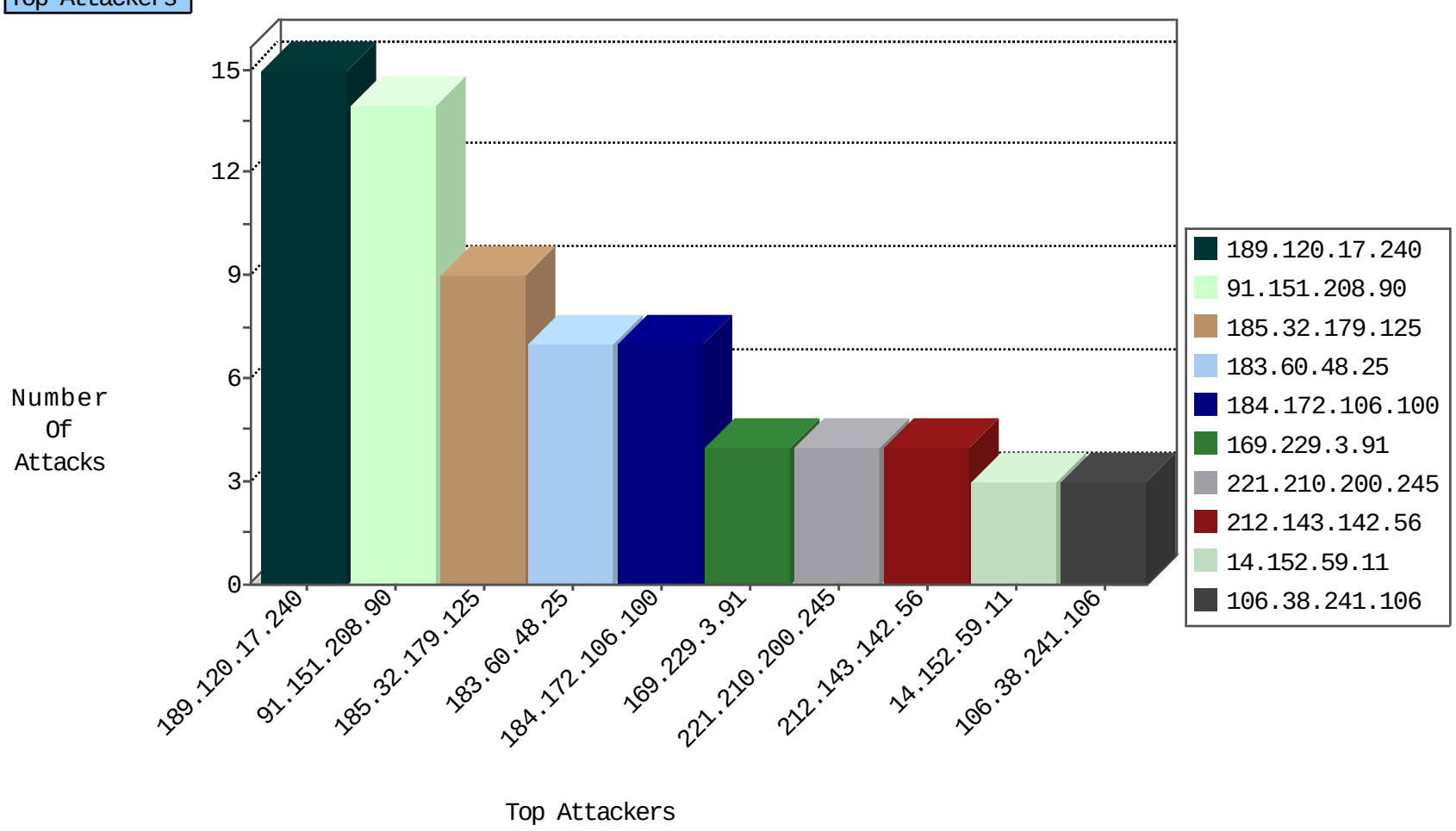
10-01-2016-03:04:09 to 10-01-2016-04:04:09

IDF Under Attack Daily Report

Top Targets



Top Attackers



10-01-2016-03:04:09 to 10-01-2016-04:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
134.147.203.115	Germany	147.237.76.196	e.sviva.idf.il	Black List	drop	2
14.119.155.13	China	147.237.77.212	e.dover.idf.il	L4 Source or Dest Port Zero	drop	2
93.158.200.66	Netherlands	147.237.76.198	e.yohalan.idf.il	Black List	drop	1
183.60.48.25	China	147.237.76.30	himush.idf.il	JLM_Under_Attack_Con_Tcp	drop	1
191.96.249.116	Chile	147.237.76.196	e.sviva.idf.il	Black List	drop	1

10-01-2016-03:04:09 to 10-01-2016-04:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
91.151.208.90	United Kingdom	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6

10-01-2016-03:04:09 to 10-01-2016-04:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
91.151.208.90	147.237.72.166	United Kingdom	aka.idf.il	SQL Injection - Select From	8
184.172.106.100	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	6
218.24.171.223	147.237.8.28	China	e.mobile-ks.idf.il	GPL SCAN nmap TCP	2
59.46.193.114	147.237.8.28	China	e.mobile-ks.idf.il	GPL SCAN nmap TCP	2
183.60.48.25	147.237.76.39	China	mobile.meitav.idf.i	ET SCAN Potential VNC Scan 5900-5920	1
183.60.48.25	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
173.220.218.14	147.237.76.198	United States	e.yohalan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
94.102.48.194	147.237.0.35	Netherlands	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
221.210.200.245	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
66.102.8.155	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	1
221.210.200.245	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
58.220.2.5	147.237.77.205	China	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
46.172.91.21	147.237.77.234	Ukraine	halag.idf.il	ET SCAN NMAP -sS window 1024	1
40.114.15.49	147.237.8.50	United States	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
183.60.48.25	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
14.176.170.36	147.237.76.39	Vietnam	mobile.meitav.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
183.60.48.25	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
183.60.48.25	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
117.158.160.211	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
221.210.200.245	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
221.210.200.245	147.237.76.39	China	mobile.meitav.idf.i	ET SCAN Potential SSH Scan	1
58.220.2.5	147.237.77.170	China	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
211.149.222.5	147.237.0.200	China	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
46.172.91.21	147.237.0.34	Ukraine	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
183.60.48.25	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
14.191.225.254	147.237.76.199	Vietnam	e.nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

10-01-2016-03:04:09 to 10-01-2016-04:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
189.120.17.240	Brazil	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
185.32.179.125	Israel	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	4
65.55.210.225	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
38.111.147.86	United States	147.237.77.216	dover.idf.il	drop		drop	2
169.229.3.91	United States	147.237.8.46	e.chinuch.idf.il	drop	SAM rule	drop	1
85.130.189.208	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
188.120.148.12	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
106.38.241.106	China	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	1
79.181.99.166	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
14.152.59.11	China	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
169.229.3.91	United States	147.237.76.38	e.e.meitav.idf.il	drop	SAM rule	drop	1
89.248.174.60	Netherlands	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
73.205.93.82	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
141.212.122.19	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
79.181.99.166	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
14.152.59.11	China	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
169.229.3.91	United States	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
93.174.93.17	Netherlands	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
74.82.47.22	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
189.120.17.240	Brazil	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
141.212.122.20	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
81.199.120.6	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
176.13.226.116	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
106.38.241.106	China	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	1
74.82.47.33	United States	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
5.22.134.69	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
169.229.3.91	United States	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	1
85.130.189.208	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
52.198.196.15	Japan	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
106.38.241.106	China	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	1
74.82.47.45	United States	147.237.77.61	e.cogat.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
14.152.59.11	China	147.237.8.27	e.madim.atal.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	1

10-01-2016-03:04:09 to 10-01-2016-04:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.32.179.125	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	3
157.55.39.128	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/robots.txt	Block	1
66.249.65.12	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 66.249.65.12	Block	1
68.180.231.57	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/main.asp	Block	1
162.247.97.162	Virgin Islands, British	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
66.249.65.182	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9724-he/refuah.aspx	Block	1
77.139.161.124	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/information.aspx	Block	1
162.247.97.162	Virgin Islands, British	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
66.249.66.146	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/apple-app-site-association	Block	1
84.95.208.20	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
66.249.64.9	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/piwik.php	Block	1
66.249.64.56	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1098-7637-he/atal.aspx	Block	1
68.180.229.103	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/228-he/faq.aspx	Block	1

10-01-2016-03:04:09 to 10-01-2016-04:04:09