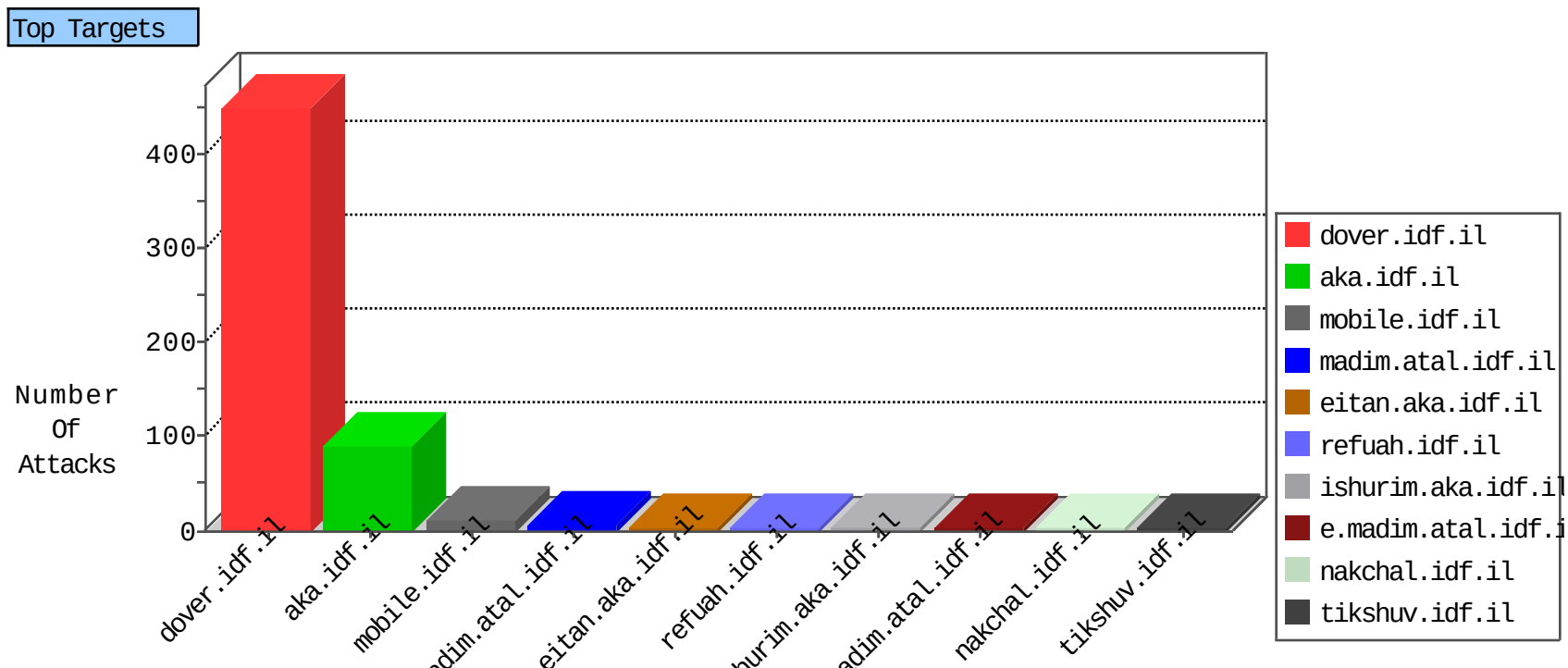
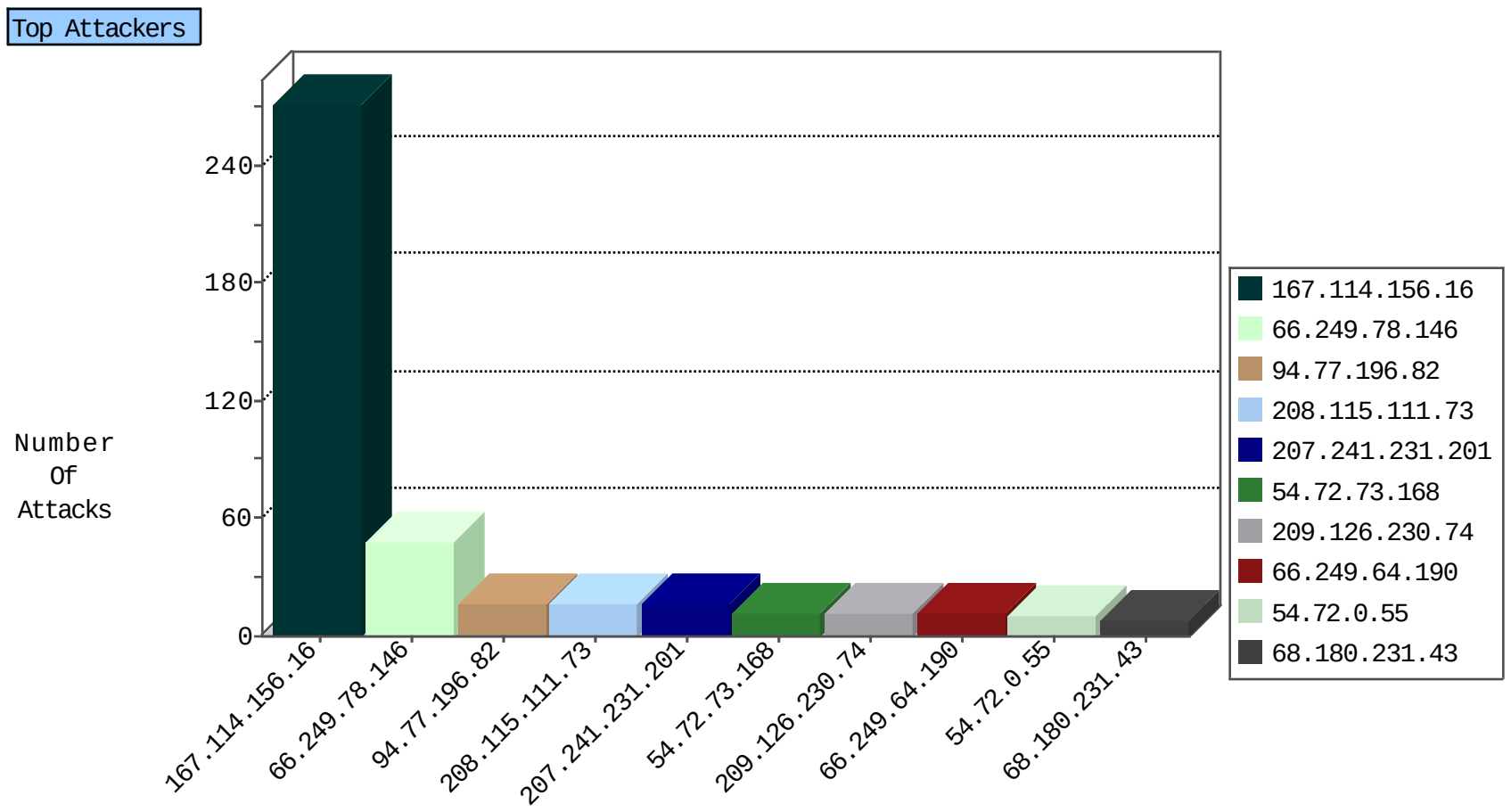
04-26-2016-06:04:03 to 04-26-2016-07:04:03

IDF Under Attack Daily Report

Top Targets



Top Attackers



04-26-2016-06:04:03 to 04-26-2016-07:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	15613
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	1823
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	5
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
45.63.20.231	United States	147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	1
45.63.20.231	United States	147.237.76.202	e.halag.idf.il	Block_Ntp_All_Net	drop	1
183.60.48.25	China	147.237.76.38	e.e.meitav.idf.il	JLM_Under_Attack_Con_Tcp	drop	1
195.88.209.6	Russian Federation	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1

04-26-2016-06:04:03 to 04-26-2016-07:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

04-26-2016-06:04:03 to 04-26-2016-07:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
80.82.78.38	147.237.76.176	Netherlands	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.78.38	147.237.0.17	Netherlands	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
23.91.1.34	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
13.82.25.17	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sS window 4096	1
185.130.5.48	147.237.8.50	Lithuania	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
117.20.41.62	147.237.8.50	Singapore	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
106.184.2.29	147.237.8.50	Japan	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
80.82.78.38	147.237.76.31	Netherlands	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
23.91.1.34	147.237.0.33	United States	idf.il	ET SCAN Potential SSH Scan	1
14.161.29.233	147.237.8.27	Vietnam	e.madim.atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
13.82.25.17	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
202.29.86.129	147.237.76.34	Thailand	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
185.130.5.48	147.237.77.19	Lithuania	law-forum.idf.il	ET SCAN Potential SSH Scan	1
139.217.27.204	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1
117.20.41.62	147.237.0.19	Singapore	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1

04-26-2016-06:04:03 to 04-26-2016-07:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
207.241.231.201	United States	147.237.72.166	aka.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	16
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
157.55.39.150	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
157.55.39.194	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
156.210.114.40	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
197.252.4.15	Sudan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
207.46.13.165	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.66.64	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.35	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
207.46.13.32	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
65.55.210.169	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
209.126.230.74	United States	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
46.19.86.83	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
209.126.230.74	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
188.138.1.217	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
209.126.230.74	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
199.30.25.29	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
190.210.38.17	Argentina	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
64.12.253.130	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
46.19.85.171	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
130.185.155.10	Sweden	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
93.115.95.216	Anonymous Proxy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
64.247.79.236	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
81.7.17.171	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
8.37.227.69	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	1
194.90.83.233	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
74.82.47.56	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.139.75	United States	147.237.8.45	e.eitan.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
222.73.18.162	China	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.219	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
120.132.84.137	China	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
207.46.13.147	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
84.94.45.168	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
184.105.247.248	United States	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
66.249.89.119	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
37.9.122.203	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1

04-26-2016-06:04:03 to 04-26-2016-07:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.177.193.231	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	3
46.19.86.227	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	3
79.177.193.231	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 79.177.193.231	Block	2
207.46.13.32	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
81.223.254.34	Austria	147.237.77.234	halag.idf.il	Unauthorized URL Access to /robots.txt	Block	1
66.249.64.230	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/robots.txt	Block	1
138.207.152.150	United States	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
85.65.86.200	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 85.65.86.200 (Open Mode)	None	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
192.95.29.116	Canada	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
74.82.47.3	United States	147.237.72.167	ishurim.aka.idf.i	Unauthorized URL Access to 147.237.72.167/	Block	1
85.65.86.200	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.66.70	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/templates/shared/usercontrols/navmenu/undefined	Block	1
198.24.162.179	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/sitefinity/usercontrols/dialogs/documenteditordialog.aspx	Block	1
131.253.25.249	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.66.121	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 66.249.66.121	Block	1
198.24.162.179	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sitefinity/usercontrols/dialogs/documenteditordialog.aspx	Block	1
136.243.11.18	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1
66.249.66.125	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/7/2827.jpg	Block	1

04-26-2016-06:04:03 to 04-26-2016-07:04:03