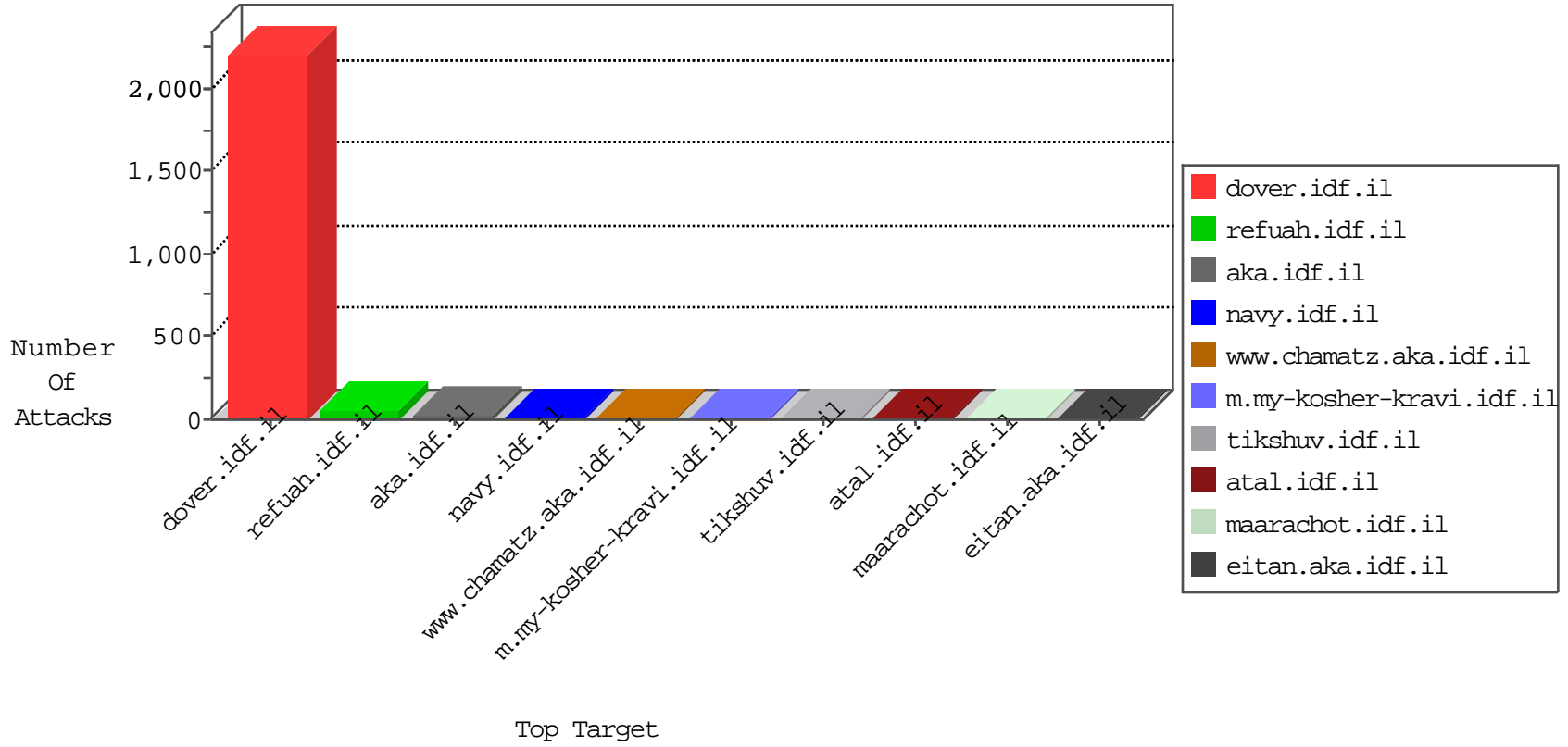




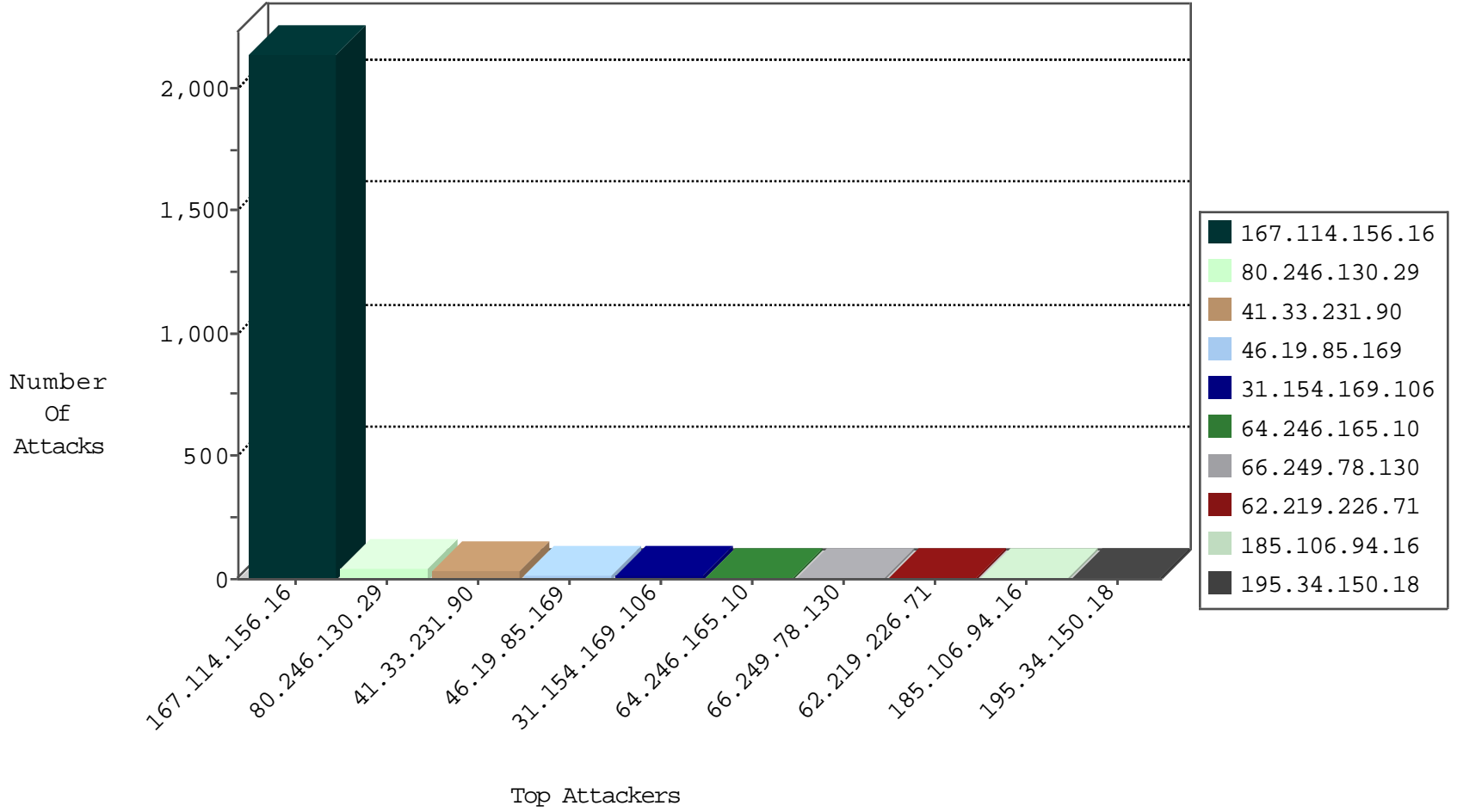
# IDF Under Attack Daily Report



Top Targets



Top Attackers



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	DOS-Tool-SwitchbladG	dest-reset	3327
141.212.122.171	United States	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1

12-07-2015-05:04:03 to 12-07-2015-06:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
62.212.73.211	Netherlands	147.237.72.166	aka.idf.il	C1000106: HTTP: majestic bot	Block	1

## 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	3
66.249.78.130	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	2
201.132.222.21	147.237.8.14	Mexico	e.orchot.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
80.246.130.29	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	44
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
31.154.169.106	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	10
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.169	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.169	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.85.169	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
64.246.165.10	United States	147.237.76.86	navy.idf.il	Header Rejection	header rejection pattern found in request	monitor	4
46.19.85.169	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
66.249.67.164	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
66.249.78.130	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
66.249.78.137	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
198.20.87.98	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
68.80.138.46	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
185.106.94.16		147.237.76.201	e.atal.idf.il	drop	SAM rule	drop	1
141.212.121.190	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
84.109.3.6	Israel	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
216.218.206.112	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.123	United States	147.237.0.33	idf.il	drop		drop	1
141.212.121.178	United States	147.237.77.61	e.cogat.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
185.106.94.16		147.237.76.202	e.halag.idf.il	drop	SAM rule	drop	1
141.212.121.191	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
98.209.58.41	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
46.19.85.175	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
216.218.206.112	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.247.211	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.121.179	United States	147.237.77.61	e.cogat.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
98.209.58.41	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
52.21.176.42	United States	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
216.218.206.114	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.247.227	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
141.212.121.185	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
109.186.129.58	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
5.255.253.157	Russian Federation	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
185.106.94.16		147.237.76.198	e.yohalan.idf.il	drop	SAM rule	drop	1
141.212.121.186	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
216.218.206.98	United States	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
176.12.149.230	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	1
115.230.124.164	China	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
62.219.226.71	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 62.219.226.71	None	3
213.57.215.159	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
2.54.19.206	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	2
46.166.190.161	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
176.13.5.23	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Parameter Type Violation ct100\$ContentPlaceholder1\$txtAreaRemarks in m.my-kosher-kravi.idf.il/templates/training/training.aspx	Block	1
80.246.130.29	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
66.249.64.55	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docI.. in www.aka.idf.il/main/giyus/general.aspx	None	1
8.37.70.126	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/&usg=alkjrhjzvwrfocqy9qb2sv8c97q_el-exq	Block	1
142.54.185.250	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/test/wp-admin/	Block	1
66.249.66.126	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/5/109415.pdf	Block	1
46.166.190.171	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
176.13.9.162	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
81.95.96.160	Czech Republic	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/blog/wp-admin/	Block	1
66.249.64.190	Israel	147.237.72.166	aka.idf.il	Unknown Parameter 4d9c6f40 in www.aka.idf.il/main/kapatz/contactus.aspx	None	1
31.184.238.200	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage/files/9/61589.pdf/filesman	Block	1
157.55.39.149	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-10770-en	Block	1
66.249.79.242	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8929-he/refuah.aspx	Block	1
50.63.197.22	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/wp-admin/	Block	1
195.62.53.168	Russian Federation	147.237.77.234	halag.idf.il	Unauthorized URL Access to /css/css	Block	1
89.161.202.147	Poland	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/wordpress/wp-admin/	Block	1
66.249.64.235	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19754-he/dover.aspx	Block	1
40.77.167.8	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/miluum/templates/www.behazdaa.org.il	Block	1
157.55.39.196	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/x'x™xœx™ x•x x•xª	Block	1
68.180.231.40	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/shared/usercontrols/lobbyinfocenteritem/	Block	1
62.219.226.71	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding md in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
107.178.195.167	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.64.238	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/weeblylink_new_window	Block	1
40.77.167.8	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/megurim/skira/default.asp	None	1
176.12.149.230	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1250-he/atal.aspx	Block	1
74.82.47.4	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
8.37.70.36	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1116-en/dover.aspx&usg=alkjrhgc6j1scvcchuk_agbeqny2hkemyw	Block	1
208.184.112.75	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
107.178.195.167	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.66.16	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1