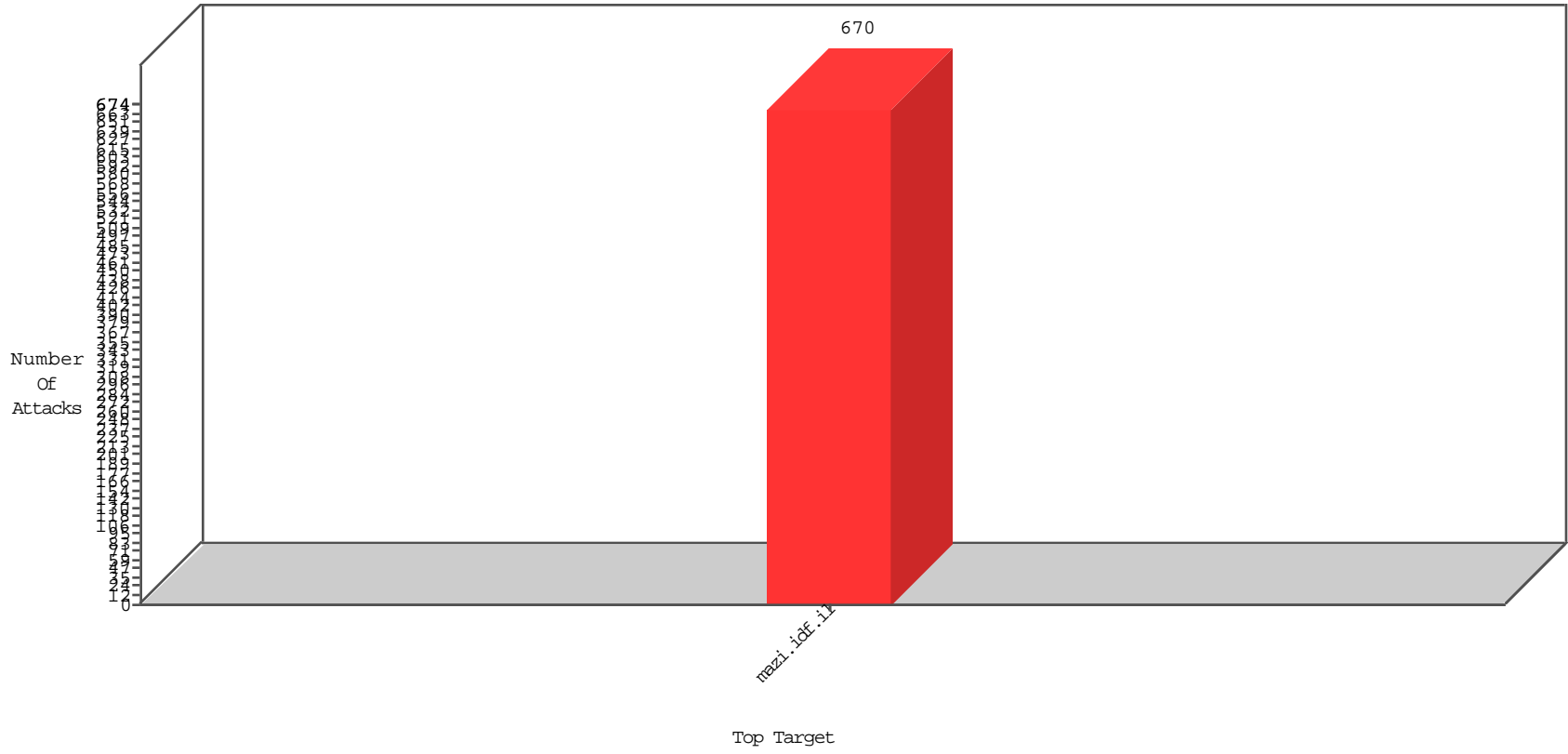


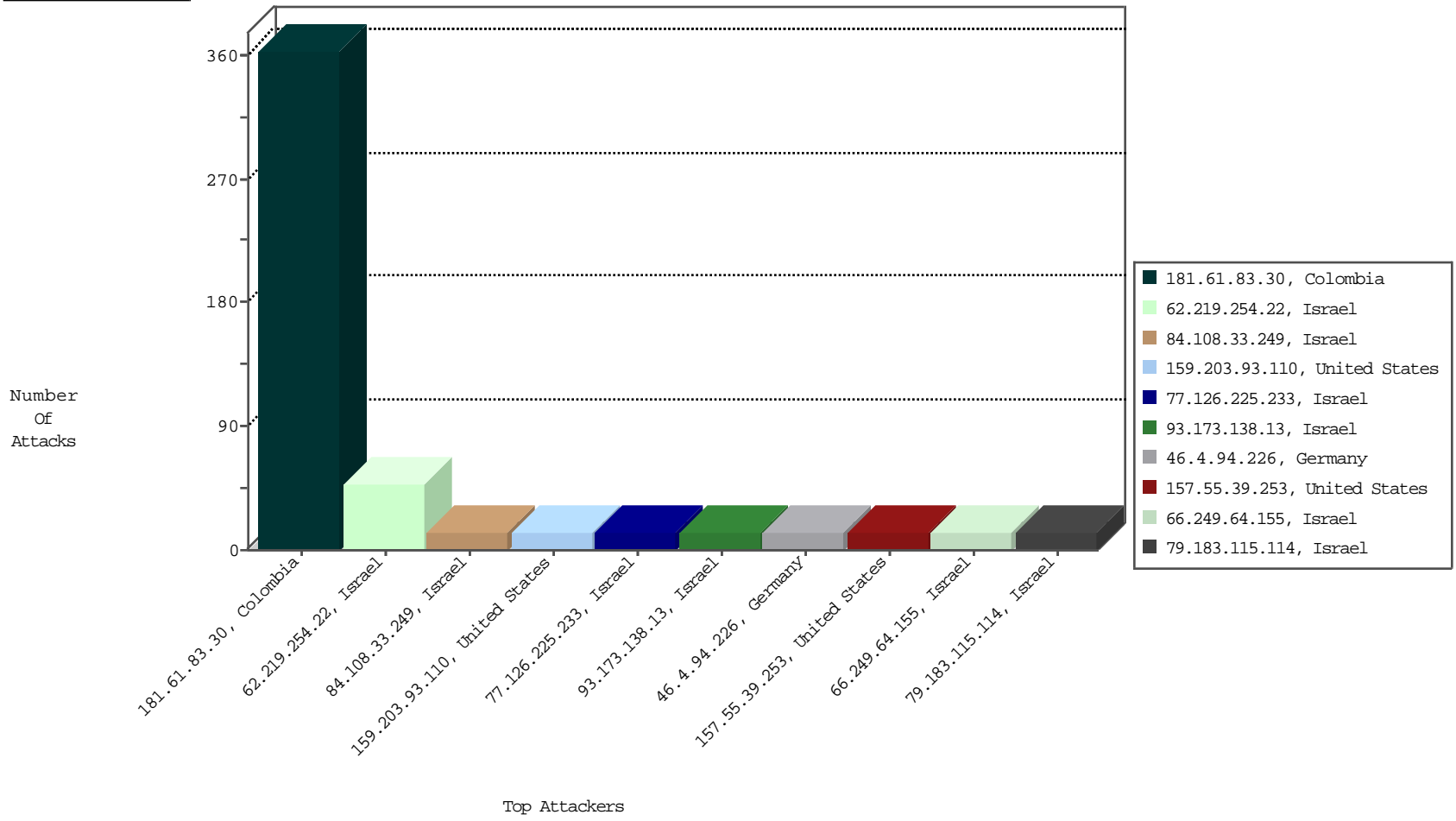
# Focused IP Under Attack Daily Report



## Top Targets



## Top Attackers



10-15-2015 to 10-16-2015

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
62.219.254.22	Israel	147.237.77.17	mazi.idf.il	Block_Udp_All_Nets	drop	BBL-Isreal	48
81.218.143.178	Israel	147.237.77.17	mazi.idf.il	Block_Udp_All_Nets	drop	BBL-Isreal	3

10-15-2015 to 10-16-2015

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
199.203.62.54	Israel	147.237.77.17	mazi.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1

10-15-2015 to 10-16-2015

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
87.81.208.80	United Kingdom	147.237.77.17	mazi.idf.il	Tehila - Perl LWP with fake user agent	4
193.105.134.220	Sweden	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 1024	1
103.226.89.45	India	147.237.77.17	mazi.idf.il	ET SCAN Potential SSH Scan	1
210.195.95.21	Malaysia	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 3072	1

## Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
85.130.176.190	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17
208.115.113.91	United States	147.237.77.17	mazi.idf.il	drop	SAM rule	drop	8
62.128.48.130	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
5.22.129.242	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
94.230.86.203	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
80.246.133.175	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
5.22.130.231	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
2.54.134.137	Israel	147.237.77.17	mazi.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	2
85.65.126.136	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
52.16.5.197	United States	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
5.29.179.78	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
216.223.27.61	United States	147.237.77.17	mazi.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
80.246.130.122	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.85.19	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
5.22.129.224	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
212.199.52.194	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
5.29.179.78	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
216.223.27.61	United States	147.237.77.17	mazi.idf.il	Directory Traversal	directory traversal overflow	monitor	1
149.78.134.6	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.85.94	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
216.223.27.59	United States	147.237.77.17	mazi.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
85.130.223.17	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
62.219.99.154	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
5.102.254.77	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
159.203.93.110	United States	147.237.77.17	mazi.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
85.65.126.136	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
46.19.85.129	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
216.223.27.59	United States	147.237.77.17	mazi.idf.il	Directory Traversal	directory traversal overflow	monitor	1
91.199.69.254	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
79.100.249.205	Bulgaria	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.85.19	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	1

## Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
181.61.83.30	Colombia	147.237.77.17	mazi.idf.i	Multiple Unknown HTTP Request Method from 181.61.83.30	Block	39
181.61.83.30	Colombia	147.237.77.17	mazi.idf.i	Multiple Illegal HTTP Version from 181.61.83.30	Block	39
181.61.83.30	Colombia	147.237.77.17	mazi.idf.i	Multiple Abnormally Long Header Line from 181.61.83.30	Block	39
181.61.83.30	Colombia	147.237.77.17	mazi.idf.i	Multiple Malformed HTTP Header Line from 181.61.83.30	Block	39
181.61.83.30	Colombia	147.237.77.17	mazi.idf.i	Multiple Abnormally Long Request from 181.61.83.30	Block	39
181.61.83.30	Colombia	147.237.77.17	mazi.idf.i	Multiple Malformed URL from 181.61.83.30	Block	39
181.61.83.30	Colombia	147.237.77.17	mazi.idf.i	Multiple Illegal Byte Code Character in Header Name from 181.61.83.30	Block	39
181.61.83.30	Colombia	147.237.77.17	mazi.idf.i	Malformed URL moved</title></head><body>	Block	13
157.55.39.253	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to igf.idf.il/templates/newslist/undefined	Block	13
79.183.115.114	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/sip_storage/files/1/1351.jpg	Block	13
216.223.27.61	United States	147.237.77.17	mazi.idf.i	URL is Above Root Directory mazi.idf.il/./images/1.he/navigation/navigation_arrow.gif	Block	13
46.4.94.226	Germany	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/vodchannel/vodchannel.aspx	Block	13
181.61.83.30	Colombia	147.237.77.17	mazi.idf.i	Illegal Byte Code Character in Header Name </body></html>	Block	13
93.173.138.13	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3849-5035-he/igf.aspx	Block	13
77.126.225.233	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/4944-he/igf.aspx	Block	13
181.61.83.30	Colombia	147.237.77.17	mazi.idf.i	Unknown HTTP Request Method <html><head><title>Object in URL moved</title></head><body>	Block	13
159.203.93.110	United States	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on /	Block	13
84.108.33.249	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3849-5035-he/igf.aspx	Block	13
62.128.48.130	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/4637-5227-he/igf.aspx	Block	13
181.61.83.30	Colombia	147.237.77.17	mazi.idf.i	Illegal HTTP Version	Block	13
141.212.122.160	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/	Block	13
79.177.49.56	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/571-he/igf.aspx	Block	13
188.165.15.99	France	147.237.77.17	mazi.idf.i	Unauthorized URL Access to www.mazi.idf.il/14-8347-he	Block	13
181.61.83.30	Colombia	147.237.77.17	mazi.idf.i	Abnormally Long Header Line request header name	Block	13
84.228.198.238	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/sip_storage/files/7/1087.jpg	Block	13
66.249.64.150	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	13
181.61.83.30	Colombia	147.237.77.17	mazi.idf.i	Malformed HTTP Header Line 2	Block	13
157.55.39.29	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	13
79.177.178.21	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/sip_storage/files/7/1087.jpg	Block	13
207.46.13.26	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to www.mazi.idf.il/5013-he/	Block	13
181.61.83.30	Colombia	147.237.77.17	mazi.idf.i	Abnormally Long Request method	Block	13
85.65.46.147	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/sip_storage/files/7/1087.jpg	Block	13
66.249.64.155	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	13