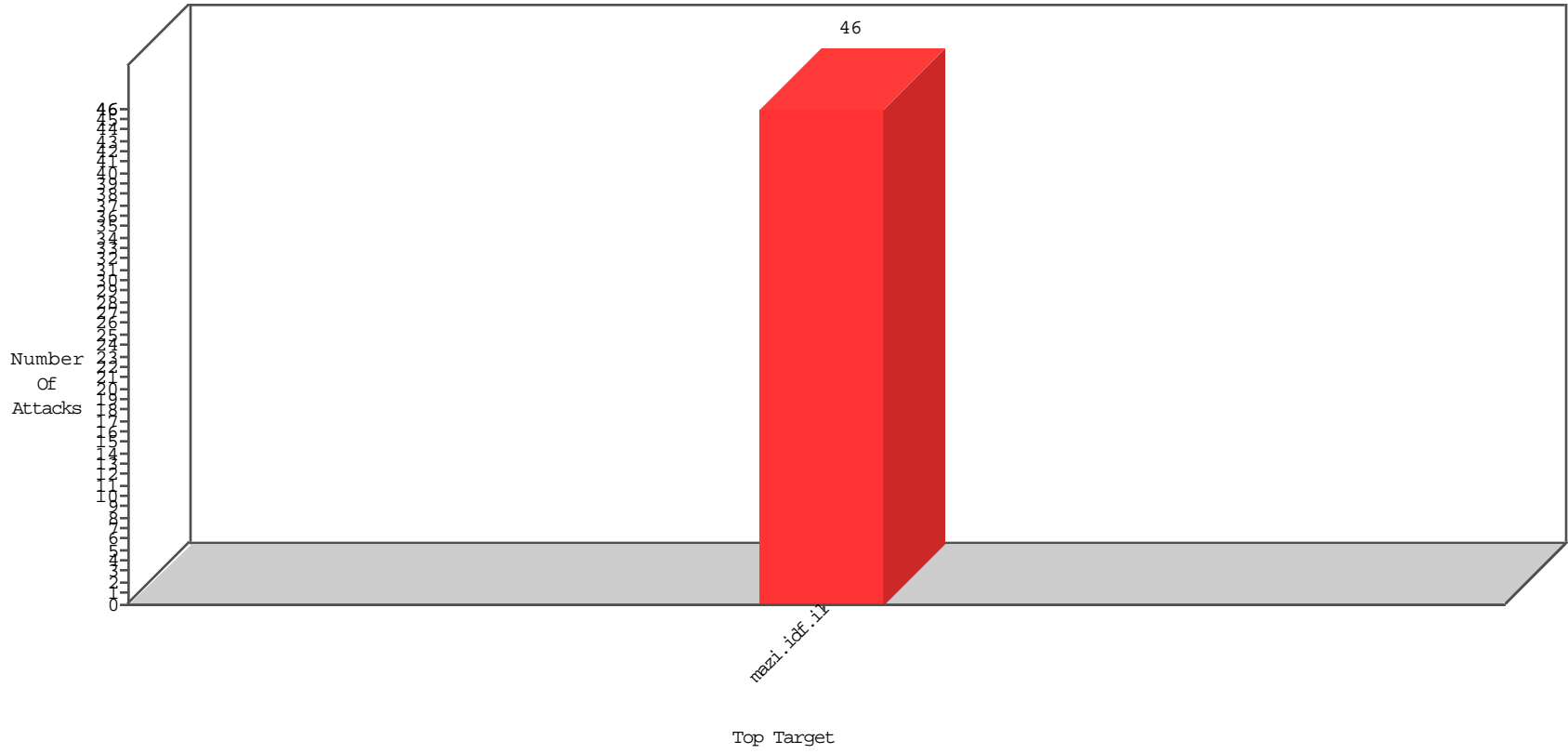


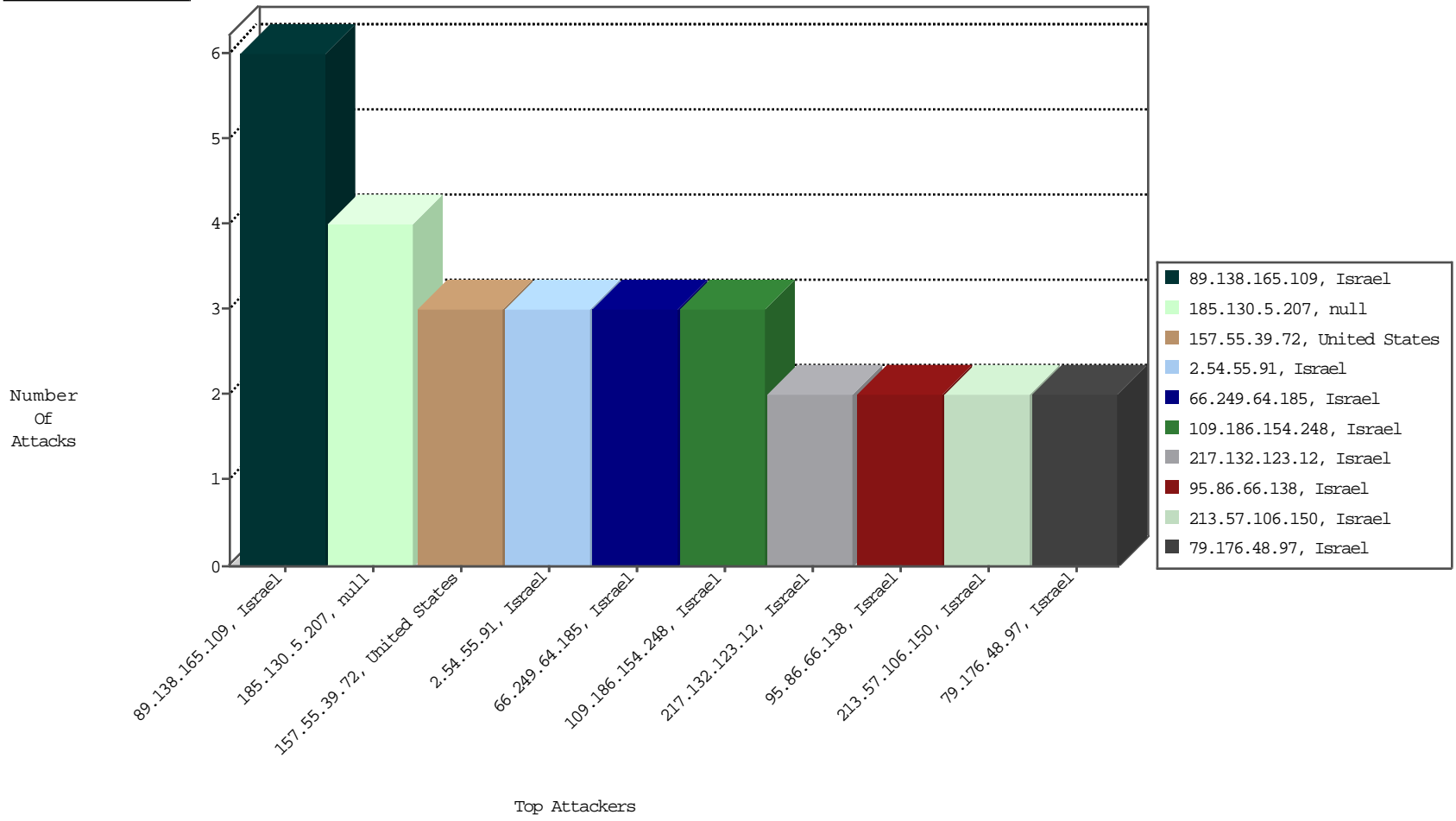
# Focused IP Under Attack Daily Report



## Top Targets



## Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
74.91.28.62	United States	147.237.77.17	mazi.idf.il	block-sp-trafl	drop	BBL-Frankfurt	1
202.112.51.96	China	147.237.77.17	mazi.idf.il	block-sp-trafl	drop	BBL-Frankfurt	1

01-16-2016 to 01-17-2016

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
185.130.5.207		147.237.77.17	mazi.idf.il	20085: HTTP: Mnieblackcat Security Scanner Initial Request	Block	1

01-16-2016 to 01-17-2016

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
185.130.5.207		147.237.77.17	mazi.idf.il	ET WEB_SERVER Muieblackcat scanner	1
185.130.5.207		147.237.77.17	mazi.idf.il	SERVER-WEBAPP Setup.php access	1

## Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
109.66.166.114	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence		monitor	64
85.130.240.235	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	64
85.130.240.235	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	64
46.19.85.200	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	36
37.26.147.226	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	25
77.126.169.139	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	21
37.26.146.206	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	19
46.19.85.207	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	16
109.66.166.114	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	16
109.66.166.114	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	16
109.66.166.114	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	16
46.117.140.254	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	12
79.176.222.53	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
195.239.16.40	Russian Federation	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	9
46.19.85.44	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	9
195.239.16.53	Russian Federation	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	9
80.249.92.17	Belarus	147.237.77.17	mazi.idf.i	drop		drop	8
5.102.254.81	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	6
94.230.86.167	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	6
93.172.240.136	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
188.120.148.242	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	5
84.108.46.60	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
2.54.9.24	Israel	147.237.77.17	mazi.idf.i	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	4
69.125.160.106	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
46.121.12.76	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
131.253.24.9	United States	147.237.77.17	mazi.idf.i	Bad TCP sequence		monitor	4
46.19.85.44	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
84.108.46.60	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	4
31.154.151.152	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
188.142.190.36	Hungary	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.85.30	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.85.14	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
2.54.134.190	Israel	147.237.77.17	mazi.idf.i	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	2
37.142.171.176	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
207.46.13.114	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
5.39.93.143	France	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
184.164.166.154	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.120.184.88	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1
141.212.122.188	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
213.8.204.33	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
84.94.80.52	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1
169.229.3.91	United States	147.237.77.17	mazi.idf.i	drop	SAM rule	drop	1
131.253.24.9	United States	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.85.159	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
109.65.111.251	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
213.57.189.33	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
42.156.138.104	China	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
85.71.7.209	Czech Republic	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
207.46.13.147	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
80.246.133.134	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1

01-16-2016 to 01-17-2016

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
89.138.165.109	Israel	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on mazi.idf.il/templates/newslist/undefined	Block	6
2.54.55.91	Israel	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on mazi.idf.il/images/transvideocounter.gif	Block	3
109.186.154.248	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/transvideocounter.gif	Block	3
213.57.106.150	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/sip_storage	Block	2
95.86.66.138	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/transvideocounter.gif	Block	2
79.176.48.97	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/newslist/undefined	Block	2
217.132.123.12	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/shared/usercontrols/vodchannel/	Block	1
157.55.39.72	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-8338-he	Block	1
87.69.202.21	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3850-5216-he/igf.aspx	Block	1
66.249.64.175	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/4223-he/igf.aspx	Block	1
207.46.13.193	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1
131.253.26.232	United States	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on mazi.idf.il/templates/newslist/undefined	Block	1
66.249.64.185	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1
54.167.183.116	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/4637-5227-he/igf.aspx	Block	1
157.55.39.72	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/newslist/undefined	Block	1
66.249.64.180	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3697-8411-he/igf.aspx	Block	1
37.142.64.49	Israel	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on mazi.idf.il/images/transvideocounter.gif	Block	1
131.253.26.238	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/newslist/undefined	Block	1
77.237.138.202	Czech Republic	147.237.77.17	mazi.idf.i	Unauthorized Method HEAD for /	Block	1
62.219.133.21	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/sip_storage/files/1/1351.jpg	Block	1
157.55.39.72	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to www.mazi.idf.il/14-8338-he	Block	1
66.249.64.185	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/457-he/igf.aspx	Block	1
40.77.167.20	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to www.mazi.idf.il/120-he/	Block	1
217.132.123.12	Israel	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on mazi.idf.il/images/transvideocounter.gif	Block	1
141.212.122.177	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/14-he/igf.aspx	Block	1
66.249.64.175	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/14-he/igf.aspx	Block	1
185.130.5.207		147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/scripts/setup.php	Block	1
66.249.64.185	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/5392-7074-he/igf.aspx	Block	1
46.117.140.254	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3848-5183-he/igf.aspx	Block	1

01-16-2016 to 01-17-2016