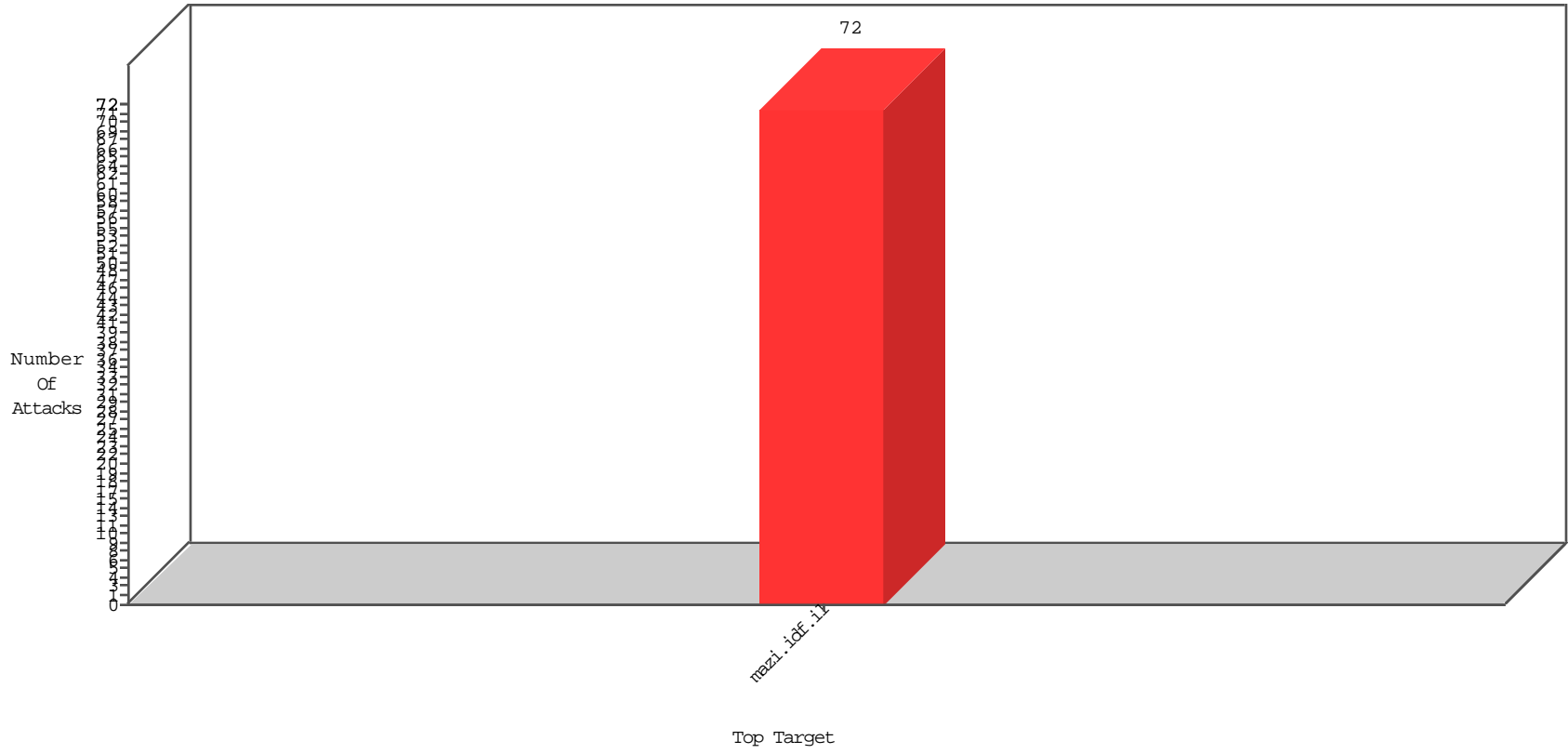


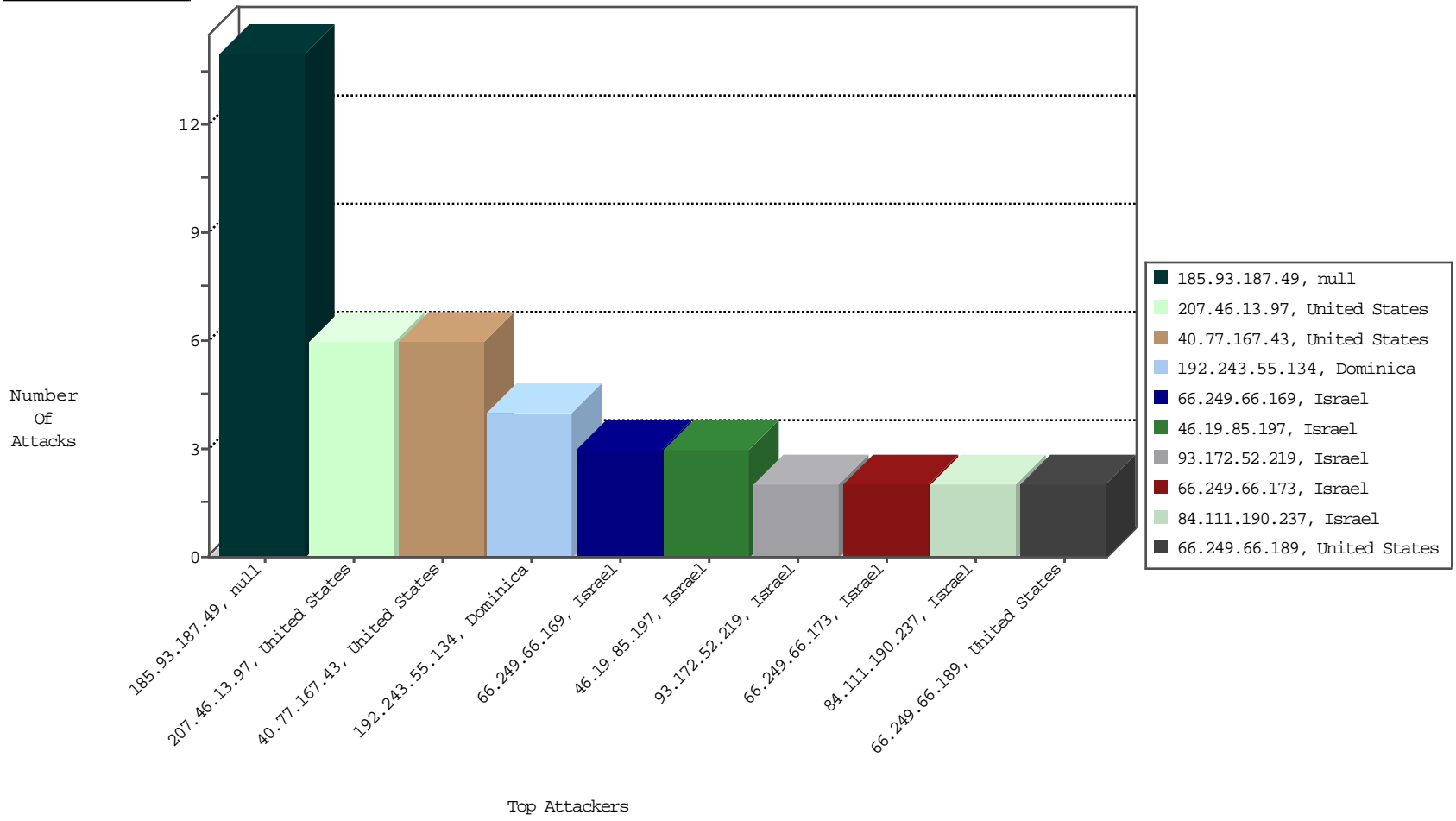
# Focused IP Under Attack Daily Report



Top Targets



Top Attackers



01-11-2016 to 01-12-2016

Top Attackers In DDoS-Defence

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

01-11-2016 to 01-12-2016

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
188.165.15.43	France	147.237.77.17	mazi.idf.il	C228: HTTP: AhrefBot crawler	Block	1

## Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
66.249.66.189	United States	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sA (2)	2
66.249.66.43	United States	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sA (2)	1
146.0.78.156	Netherlands	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 1024	1
164.39.11.198	United Kingdom	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 1024	1

## Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
40.77.167.43	United States	147.237.77.17	mazi.idf.i	drop	SAM rule	drop	662
91.228.248.251	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	49
46.19.85.197	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	26
149.78.198.160	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	16
149.78.198.160	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	16
46.19.85.197	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	16
2.52.16.55	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	13
31.154.167.72	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
46.19.86.239	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
2.52.16.55	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	9
185.89.217.225		147.237.77.17	mazi.idf.i	drop		drop	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
46.117.116.208	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	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
46.19.85.99	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.23	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.159	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
149.78.228.117	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.85.68	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.92	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
130.193.51.60	Russian Federation	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
185.89.217.225		147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
169.229.3.91	United States	147.237.77.17	mazi.idf.i	drop	SAM rule	drop	2
46.19.85.0	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
5.28.186.53	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.15	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
185.89.217.225		147.237.77.17	mazi.idf.i	Directory Traversal	directory traversal overflow	monitor	1
46.19.86.199	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.108	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.85.170	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.85.2	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
109.253.205.205	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1
213.57.188.103	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
81.218.251.252	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1
192.243.55.136	Dominica	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
46.117.214.253	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1
185.89.217.225		147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1
46.19.86.132	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
169.229.3.90	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
130.193.51.60	Russian Federation	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
85.64.228.210	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
208.115.111.75	United States	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
5.39.93.143	France	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
79.176.57.87	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1
185.89.217.227		147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
184.168.152.7	United States	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
46.19.85.183	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
109.253.205.205	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
216.243.31.2	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
31.168.11.194	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1

## Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
185.93.187.49		147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 185.93.187.49	Block	6
40.77.167.43	United States	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on mazi.idf.il/oic/scriptresource.axd	Block	5
185.93.187.49		147.237.77.17	mazi.idf.i	Multiple Admin Blocking from 185.93.187.49	Block	4
207.46.13.97	United States	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on mazi.idf.il/oic/scriptresource.axd	Block	4
185.93.187.49		147.237.77.17	mazi.idf.i	PHP Attempt	Block	4
84.111.190.237	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/newslist/undefined	Block	2
93.172.52.219	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/transvideocounter.gif	Block	2
192.243.55.134	Dominica	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 192.243.55.134	Block	2
66.249.66.169	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	2
213.57.54.169	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/transvideocounter.gif	Block	1
66.249.66.134	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-8333-he	Block	1
40.77.167.43	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/oic/webresource.axd	Block	1
207.46.13.18	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/oic/scriptresource.axd	Block	1
192.118.10.10	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/sip_storage/files/9/5839.jpg	Block	1
131.253.24.151	United States	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on mazi.idf.il/templates/newslist/undefined	Block	1
66.249.66.173	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/4944-he/igf.aspx	Block	1
207.46.13.97	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/general/x"	Block	1
46.121.158.222	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3849-5035-he/igf.aspx	Block	1
5.28.186.53	Israel	147.237.77.17	mazi.idf.i	Parameter Type Violation Master\$ucHeader\$ucSearchControl\$txtSearch in www.mazi.idf.il/14-he/igf.aspx	Block	1
192.243.55.134	Dominica	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/5551-11516-he/xžx@xex'x™x? x§x"x™xœx".aspx	Block	1
66.249.66.165	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/14-he/igf.aspx	Block	1
46.19.85.197	Israel	147.237.77.17	mazi.idf.i	Abnormally Long Request method	Block	1
207.46.13.86	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/templatecontrols/pictureinfo/pictureinfo.aspx	Block	1
192.243.55.130	Dominica	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/113-11581-he/xœxœx? x'x'x•xœx•xª.aspx	Block	1
131.253.36.196	United States	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on mazi.idf.il/templates/newslist/undefined	Block	1
66.249.66.173	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/6578-9989-he/igf.aspx	Block	1
212.179.9.140	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/transvideocounter.gif	Block	1
66.249.66.40	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to igf.idf.il/templates/shared/usercontrols/newsgallery/	Block	1
5.102.217.217	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/sip_storage/files/1/2061.jpg	Block	1
192.243.55.135	Dominica	147.237.77.17	mazi.idf.i	Unauthorized URL Access to igf.idf.il/14-4980-he	Block	1
66.249.66.169	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/571-he/igf.aspx	Block	1
46.19.85.197	Israel	147.237.77.17	mazi.idf.i	Malformed URL	Block	1
141.212.122.81	United States	147.237.77.17	mazi.idf.i	Malformed URL proxytest.zmap.io:80	Block	1
66.249.66.189	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/shared/usercontrols/newsgallery/	Block	1
212.199.52.66	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/transvideocounter.gif	Block	1
66.249.66.46	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to www.mazi.idf.il/14-he	Block	1
192.243.55.137	Dominica	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/sip_storage/files	Block	1
104.131.147.112	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3850-5216-he/igf.aspx	Block	1
207.46.13.97	United States	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on mazi.idf.il/oic/webresource.axd	Block	1
46.19.85.197	Israel	147.237.77.17	mazi.idf.i	Unknown HTTP Request Method =0.9,image/webp,*/*;q=0.8 in URL	Block	1
192.243.55.134	Dominica	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/3697-9630-he/igf.aspx 10 x'x x•x'xžx'x" 2010	Block	1
185.89.217.225		147.237.77.17	mazi.idf.i	URL is Above Root Directory mazi.idf.il/./images/1.he/navigation/navigation_arrow.gif	Block	1
77.75.77.72	Czech Republic	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/sip_storage/files/9/8699.jpg	Block	1