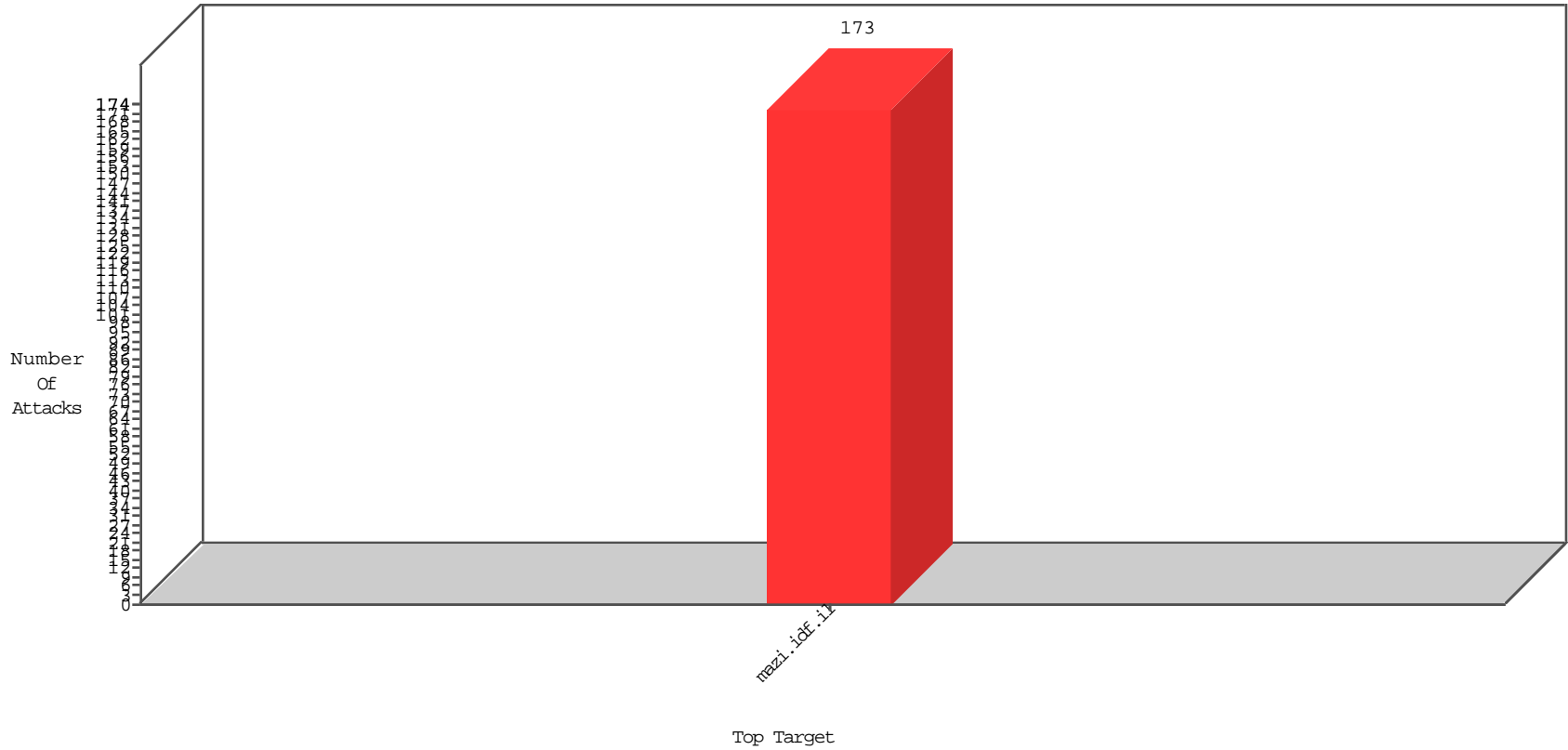


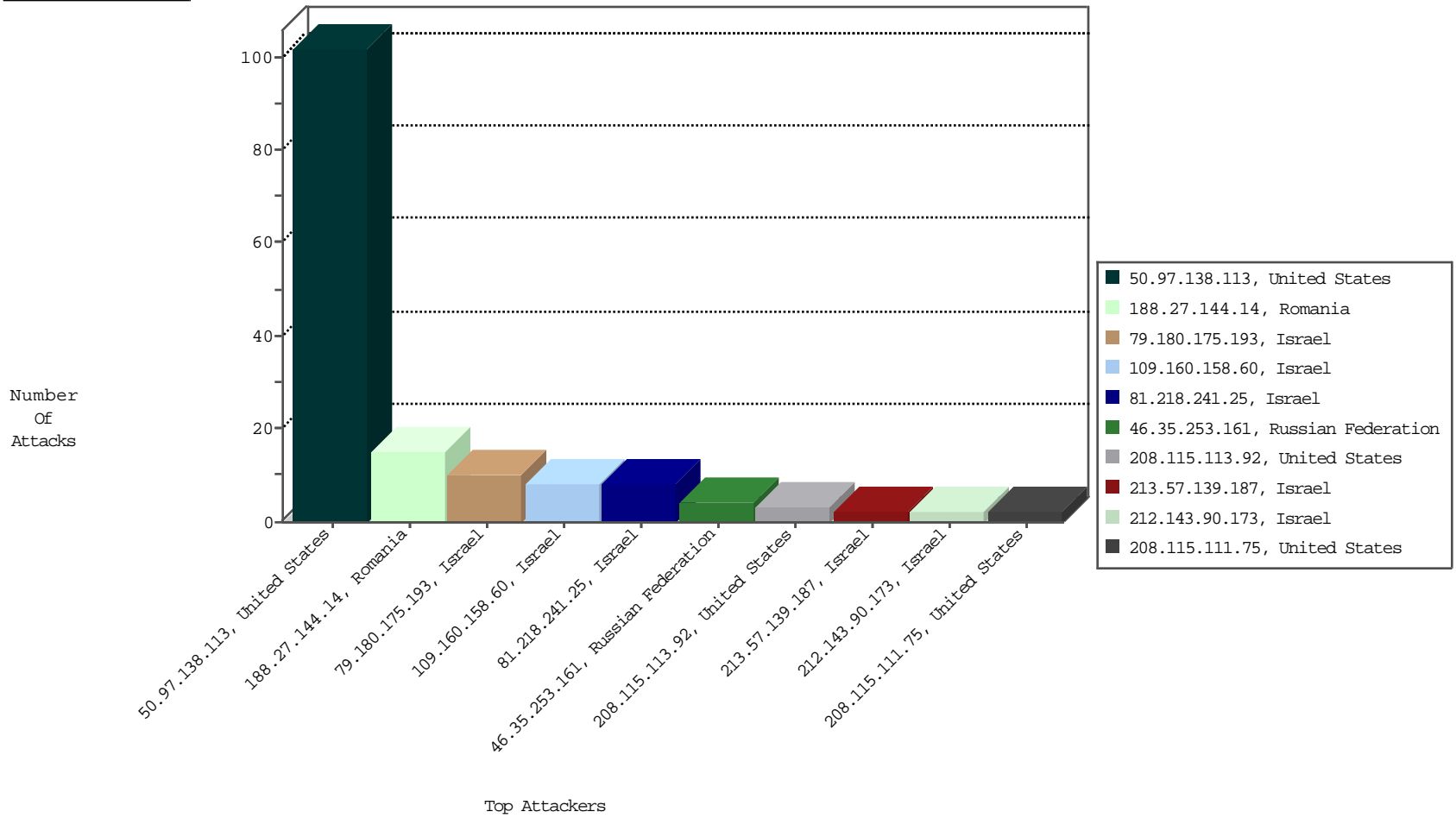
# Focused IP Under Attack Daily Report



## Top Targets



## Top Attackers



02-15-2016 to 02-16-2016

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
------------------	--------------	----------------	------	-----------	---------------	----------------------	-------

## Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
50.97.138.113	United States	147.237.77.17	mazi.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	74
50.97.138.113	United States	147.237.77.17	mazi.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	10
85.17.112.142	Netherlands	147.237.77.17	mazi.idf.il	C106: HTTP: majestic bot	Block	1
220.156.187.4	India	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
50.97.138.113	United States	147.237.77.17	mazi.idf.il	SQL Injection - Select From	18
66.249.66.189	United States	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sA (2)	2
123.157.146.108	China	147.237.77.17	mazi.idf.il	ET SCAN Potential SSH Scan	1
218.246.0.97	China	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 1024	1
93.23.130.198	France	147.237.77.17	mazi.idf.il	ET SCAN Potential SSH Scan	1
194.63.140.74	Russian Federation	147.237.77.17	mazi.idf.il	ET SCAN Potential SSH Scan	1

## Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
130.203.136.75	United States	147.237.77.17	mazi.idf.i	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	55
109.64.39.60	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	33
195.160.242.40	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	24
46.19.85.6	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	19
46.19.86.13	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	17
70.197.128.111	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
195.160.242.40	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	14
46.19.85.6	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
5.29.139.194	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	10
46.19.86.13	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	9
46.121.243.52	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
195.239.16.53	Russian Federation	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	9
149.78.169.140	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	6
149.78.169.140	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	5
83.144.17.2	France	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.85.116	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.114	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.117	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
94.228.34.248	United Kingdom	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
62.219.137.24	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid sequence number	monitor	4
5.102.195.50	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
84.111.108.40	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	4
46.19.85.6	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
62.219.137.24	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	4
84.111.108.40	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
94.228.34.248	United Kingdom	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	4
62.219.137.24	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.228	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.116	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	2
5.29.139.194	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	2
46.19.85.160	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
37.26.146.153	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
84.228.75.135	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN retransmit with different window scale	alert	1
212.150.214.90	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
5.29.77.143	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1
66.249.93.22	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
46.121.112.214	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
185.3.147.103	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
216.218.206.118	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
5.29.180.239	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
208.115.113.82	United States	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
5.22.135.195	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
192.115.85.15	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid sequence number	monitor	1
46.19.86.249	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1
172.56.26.95	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.85.6	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
84.228.75.135	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	1
212.179.172.219	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
5.29.77.143	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1

## Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
79.180.175.193	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/newslst/undefined	Block	10
109.160.158.60	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/newslst/undefined	Block	8
81.218.241.25	Israel	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 81.218.241.25	Block	7
188.27.144.14	Romania	147.237.77.17	mazi.idf.i	PHP Attempt	Block	7
188.27.144.14	Romania	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 188.27.144.14	Block	6
188.27.144.14	Romania	147.237.77.17	mazi.idf.i	Admin Blocking	Block	1
46.35.253.161	Russian Federation	147.237.77.17	mazi.idf.i	Parameter Type Violation folderid in mazi.idf.il/templatecontrols/pictureinfo/pictureinfo.aspx	Block	1
212.143.90.173	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/1.he/logo.gif	Block	1
207.46.13.124	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/113-10504-he/igf.aspx	Block	1
95.213.182.43	Russian Federation	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/6216-he/igf.aspx'	Block	1
66.249.66.173	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3850-5187-he/igf.aspx	Block	1
208.115.113.92	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to igf.idf.il/3728-11581-he/xæxæx? x'x'x*xæx*xæx".aspx	Block	1
81.218.241.25	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/1.he/logo.gif	Block	1
46.35.253.161	Russian Federation	147.237.77.17	mazi.idf.i	Parameter Type Violation lang in mazi.idf.il/templatecontrols/pictureinfo/pictureinfo.aspx	Block	1
213.57.139.187	Israel	147.237.77.17	mazi.idf.i	Distributed PHP Attempt	Block	1
208.115.111.75	United States	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 208.115.111.75	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
46.35.253.161	Russian Federation	147.237.77.17	mazi.idf.i	Parameter Type Violation DocID in mazi.idf.il/templatecontrols/pictureinfo/pictureinfo.aspx	Block	1
208.115.113.92	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to igf.idf.il/5551-11516-he/xžxæx'x™x? x§x"x™xæx".aspx	Block	1
89.138.224.80	Israel	147.237.77.17	mazi.idf.i	Distributed Too Many of the Same Response Code (404)	Block	1
62.219.160.202	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/newslst/undefined	Block	1
213.57.139.187	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to m.mazi.idf.il/xmlrpc.php	Block	1
208.115.111.75	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/450-he.aspx	Block	1
157.55.39.119	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1
46.35.253.161	Russian Federation	147.237.77.17	mazi.idf.i	Parameter Type Violation FileID in mazi.idf.il/templatecontrols/pictureinfo/pictureinfo.aspx	Block	1
212.143.90.173	Israel	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 212.143.90.173	Block	1
188.27.144.14	Romania	147.237.77.17	mazi.idf.i	Unauthorized URL Access to www.mazi.idf.il/phpmoadmin/moadmin.php	Block	1
91.200.12.138	Ukraine	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/forums/templates/forums/forum.aspx/trackback/	Block	1
66.249.66.165	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3848-5183-he/igf.aspx	Block	1
208.115.113.92	United States	147.237.77.17	mazi.idf.i	Distributed Too Many of the Same Response Code (404)	Block	1