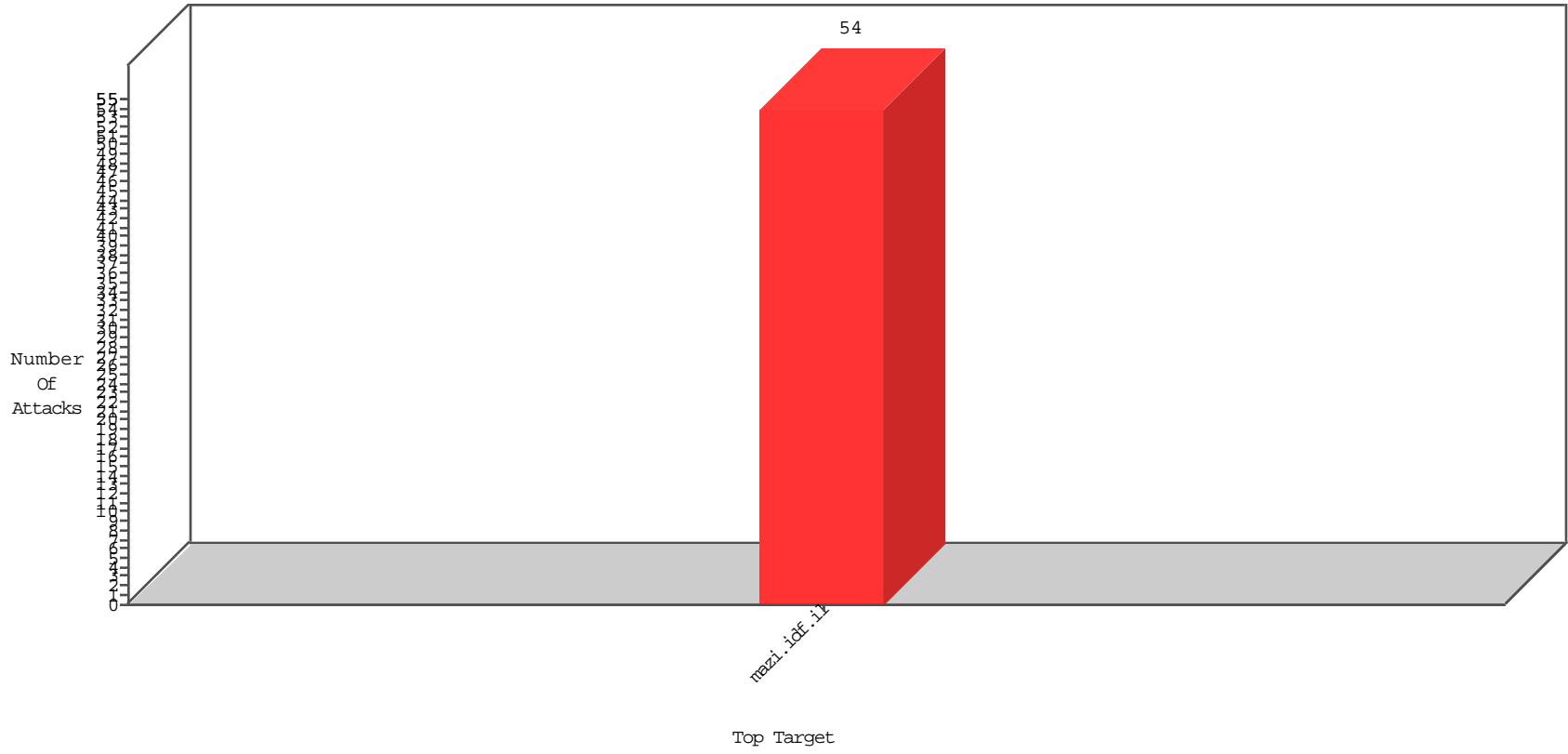


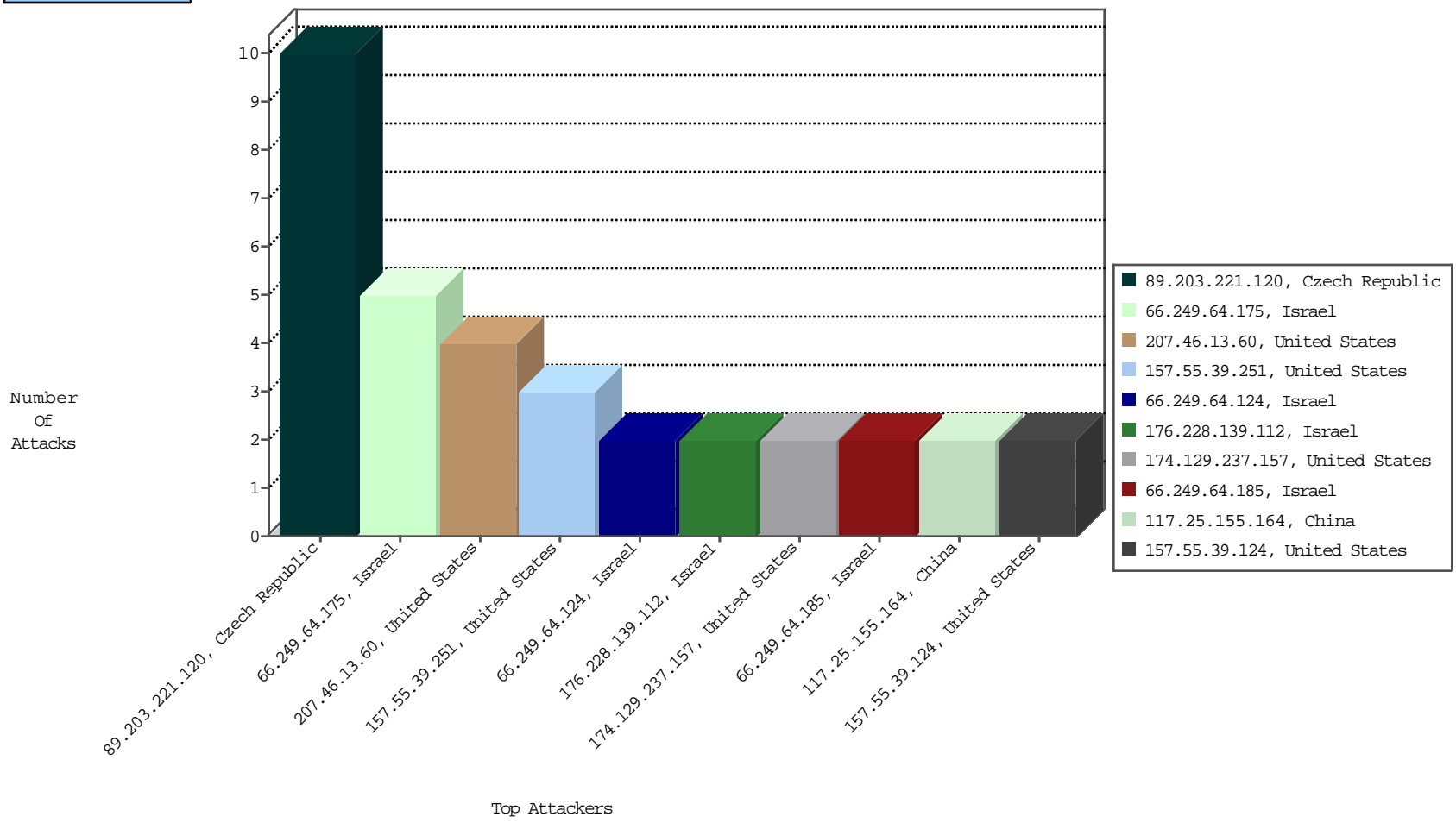
# Focused IP Under Attack Daily Report



## Top Targets



## Top Attackers



12-19-2015 to 12-20-2015

Top Attackers In DDoS-Defence

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

12-19-2015 to 12-20-2015

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
89.203.221.120	Czech Republic	147.237.77.17	mazi.idf.il	1633: HTTP: WebDAV Protocol PROPFIND Method	Block	10
188.165.15.181	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
117.25.155.164	China	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 1024	1
202.131.114.196	India	147.237.77.17	mazi.idf.il	ET SCAN Potential SSH Scan	1
94.102.60.89	Netherlands	147.237.77.17	mazi.idf.il	ET SCAN Potential SSH Scan	1
117.25.155.164	China	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 4096	1

## Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
109.65.73.234	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	46
46.19.85.160	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	16
89.138.82.132	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
37.26.149.162	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	14
85.65.102.28	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	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
188.120.148.130	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	9
85.65.102.28	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	9
84.111.102.110	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	9
149.88.92.166	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
37.26.149.162	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	9
85.65.245.56	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	9
5.22.131.156	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	9
185.3.146.185	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	9
213.57.136.7	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	8
213.57.136.7	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
37.26.149.240	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
213.57.136.7	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
149.88.138.169	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
46.19.85.26	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	5
37.26.149.162	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
46.19.86.88	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.41	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	5
92.96.74.124	United Arab Emirates	147.237.77.17	mazi.idf.i	drop	SAM rule	drop	5
2.54.164.112	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
130.193.51.60	Russian Federation	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
213.57.135.234	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
46.19.86.18	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
84.111.102.110	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	4
79.177.157.76	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
85.64.206.22	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	4
46.121.247.195	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
185.3.146.182	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
79.178.220.180	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
37.142.235.80	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
85.64.206.22	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
213.57.135.234	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
46.19.85.250	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
37.26.149.240	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
89.203.221.120	Czech Republic	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
46.19.86.88	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
46.19.86.41	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
46.19.86.150	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
46.19.86.96	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
2.54.185.155	Israel	147.237.77.17	mazi.idf.i	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	2
2.54.153.35	Israel	147.237.77.17	mazi.idf.i	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	2
37.26.149.240	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	2
31.154.34.190	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
169.229.3.90	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

12-19-2015 to 12-20-2015

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
176.228.139.112	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/transvideocounter.gif	Block	2
157.55.39.251	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	2
68.180.228.160	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/shared/usercontrols/newsgallery/	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
207.46.13.60	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-4983-he	Block	1
37.142.64.15	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to igf.idf.il/xmlrpc.php	Block	1
157.55.39.251	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/5010-9094-he/igf.aspx	Block	1
107.150.42.186	United States	147.237.77.17	mazi.idf.i	PHP Attempt	Block	1
66.249.64.180	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/5392-7074-he/igf.aspx	Block	1
66.249.64.124	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-8335-he	Block	1
149.88.138.169	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3849-5035-he/igf.aspx	Block	1
77.75.78.167	Czech Republic	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/sip_storage/files/9/8699.jpg	Block	1
66.249.64.175	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3697-he/igf.aspx	Block	1
37.142.239.153	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/4944-he/igf.aspx	Block	1
207.46.13.60	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-8330-he	Block	1
107.150.42.186	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/wp-login.php	Block	1
66.249.64.185	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/5010-he/igf.aspx	Block	1
66.249.64.124	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/shared/usercontrols/newsgallery/	Block	1
207.46.13.60	United States	147.237.77.17	mazi.idf.i	Distributed PHP Attempt	Block	1
2.54.63.46	Israel	147.237.77.17	mazi.idf.i	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 2.54.63.46	Block	1
157.55.39.124	United States	147.237.77.17	mazi.idf.i	Distributed PHP Attempt	Block	1
79.178.220.180	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3850-5187-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
46.19.86.13	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/4637-5227-he/igf.aspx	Block	1
208.90.57.196	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to ww.mazi.idf.il/joinmailinglist.aspx	Block	1
174.129.237.157	United States	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 174.129.237.157	Block	1
109.65.73.234	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3849-5035-he/igf.aspx	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
66.249.64.175	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/113-10962-he/igf.aspx	Block	1
207.46.13.60	United States	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on mazi.idf.il/w/load.php	Block	1
37.142.64.15	Israel	147.237.77.17	mazi.idf.i	PHP Attempt	Block	1
157.55.39.124	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/w/load.php	Block	1
87.69.204.239	Israel	147.237.77.17	mazi.idf.i	Parameter Type Violation Master\$ucHeader\$ucSearchControl\$txtSearch in mazi.idf.il/6547-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/robots.txt	Block	1
46.120.130.46	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
174.129.237.157	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/date(-62135596800000)/	Block	1
149.88.67.66	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3849-5035-he/igf.aspx	Block	1

12-19-2015 to 12-20-2015