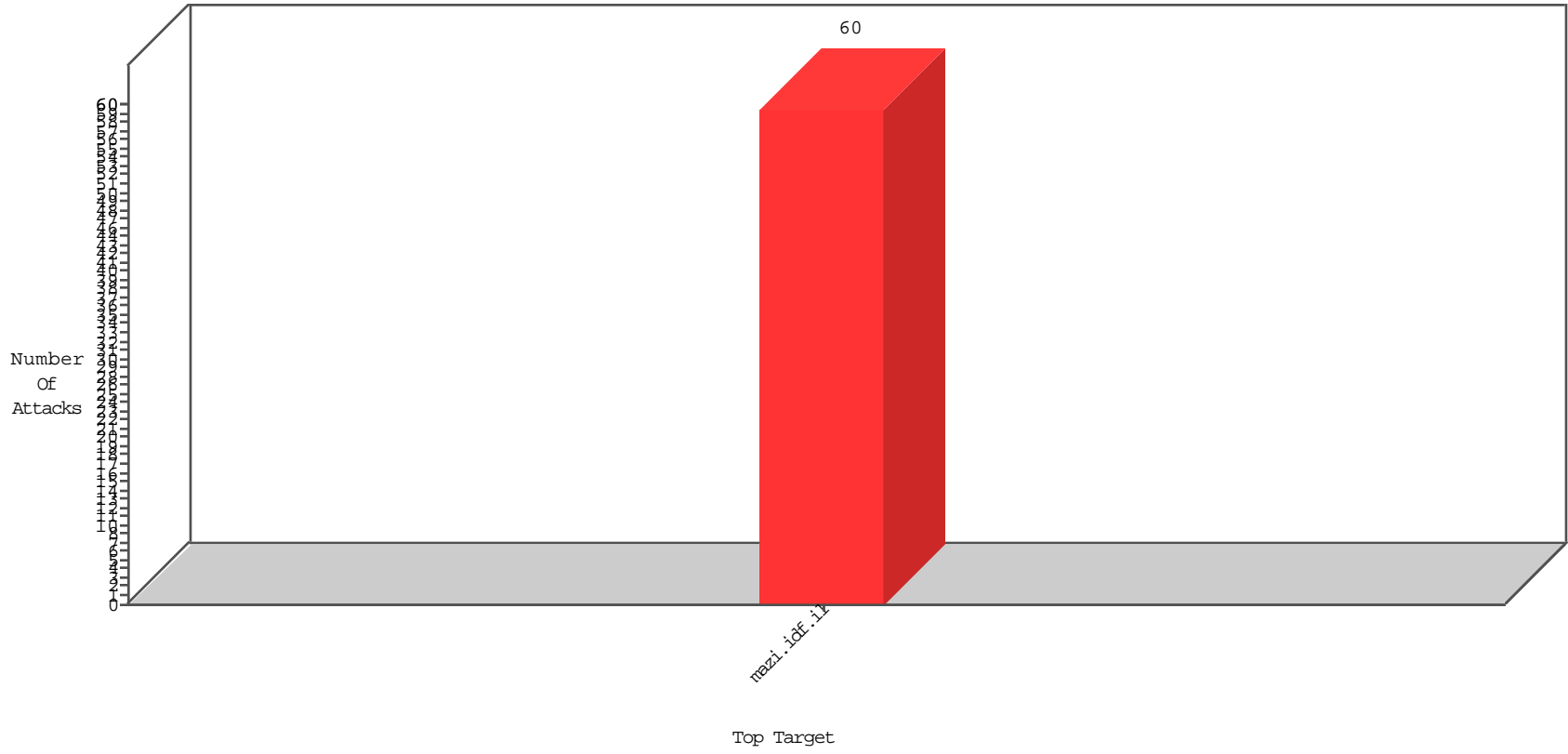


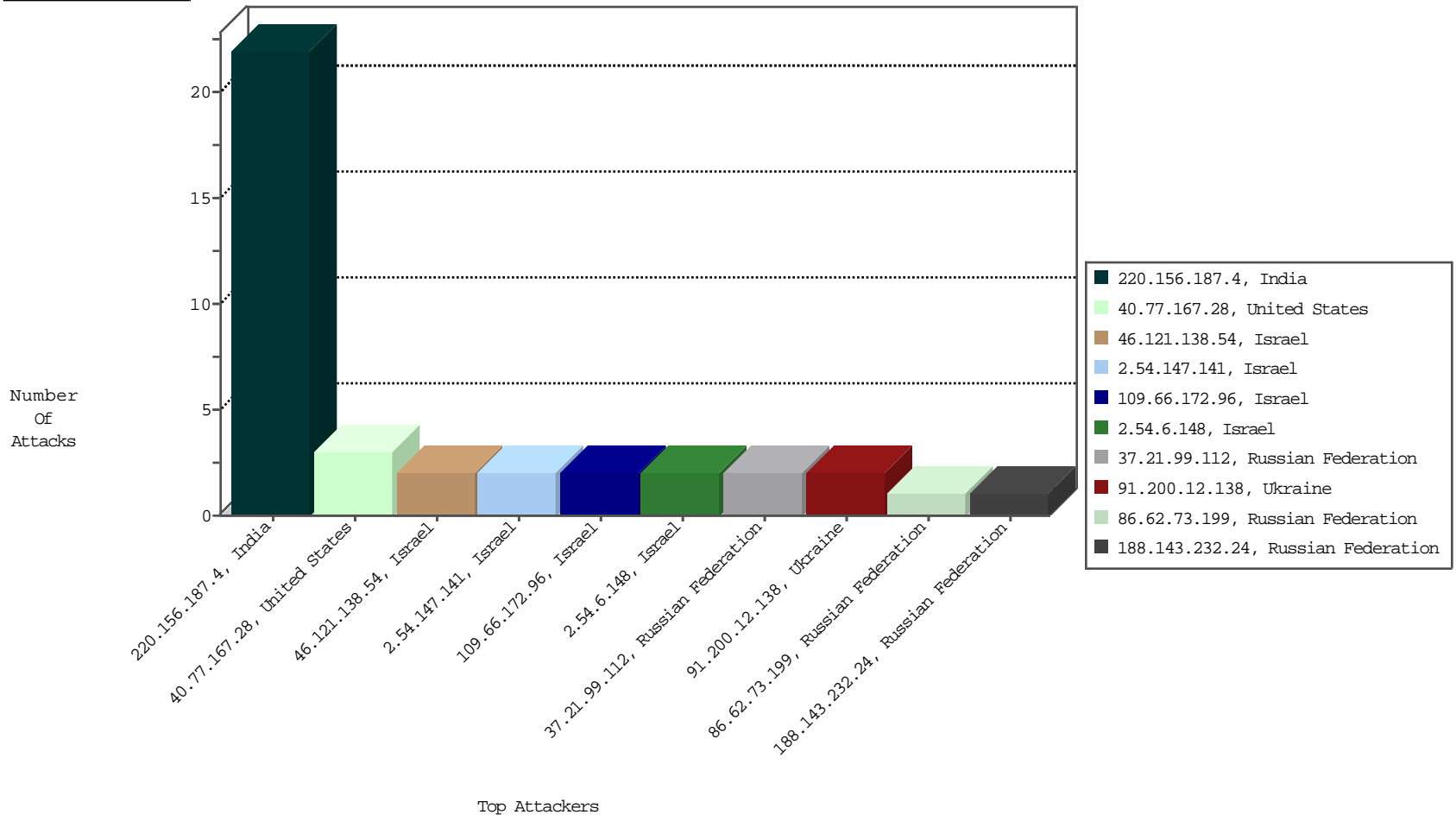
# Focused IP Under Attack Daily Report



## Top Targets



## Top Attackers



01-29-2016 to 01-30-2016

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
220.156.187.4	India	147.237.77.17	mazi.idf.il	C228: HTTP: AhrefBot crawler	Block	22
188.165.15.121	France	147.237.77.17	mazi.idf.il	C228: HTTP: AhrefBot crawler	Block	1
79.181.9.205	Israel	147.237.77.17	mazi.idf.il	C008: HTTP: Xenu UserAgent	Block	1
188.165.15.233	France	147.237.77.17	mazi.idf.il	C228: HTTP: AhrefBot crawler	Block	1
86.62.73.199	Russian Federation	147.237.77.17	mazi.idf.il	C008: HTTP: Xenu UserAgent	Block	1
188.165.15.61	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
37.21.99.112	Russian Federation	147.237.77.17	mazi.idf.il	ET SCAN Potential SSH Scan	2
113.207.36.253	China	147.237.77.17	mazi.idf.il	ET SCAN Potential SSH Scan	1
46.148.22.26	Lithuania	147.237.77.17	mazi.idf.il	ET SCAN Potential SSH Scan	1
168.62.238.153	United States	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
212.76.127.10	Israel	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	81
87.68.162.2	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	81
2.52.6.59	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	36
37.26.148.186	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	32
195.239.16.40	Russian Federation	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	9
212.76.127.219	Israel	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	9
185.120.125.5		147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	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
94.230.86.130	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	8
130.193.51.60	Russian Federation	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
37.46.39.60	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.199	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.246	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
212.76.127.111	Israel	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
79.181.191.86	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.85.119	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
5.22.131.64	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
109.67.30.174	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.85.17	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	3
80.246.133.42	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	3
130.193.51.60	Russian Federation	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
85.250.86.244	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
79.127.43.235	Iran, Islamic Republic of	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1
46.19.86.254	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1
216.243.31.2	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
188.120.148.191	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
84.109.83.203	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.121.44.217	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
31.154.94.79	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
184.105.139.92	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
79.127.43.235	Iran, Islamic Republic of	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.86.254	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
195.60.232.57	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
84.228.26.80	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
64.125.239.121	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
184.105.247.236	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
109.67.25.153	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.117.240.229	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
169.229.3.91	United States	147.237.77.17	mazi.idf.i	drop	SAM rule	drop	1
74.82.47.52	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.86.145	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
37.46.38.135	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
46.121.44.217	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1
46.19.85.183	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
5.22.134.207	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
173.208.176.2	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

01-29-2016 to 01-30-2016

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
46.121.138.54	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/shared/usercontrols/vodchannel/	Block	2
2.54.6.148	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	2
40.77.167.28	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/113-11516-he/~Å¼Ã-Ã@Ã-Ã"Ã-â€"Ã-â„¿Ã-Â? Ã-Â§Ã-â€?Ã-â„¿Ã-Ã"Ã-â€?.aspx	Block	2
2.54.147.141	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/sip_storage	Block	2
157.55.39.172	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to www.mazi.idf.il/6216-he/igf.aspx),\h	Block	1
91.200.12.138	Ukraine	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 91.200.12.138	Block	1
109.66.172.96	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to igf.idf.il/xmlrpc.php	Block	1
68.180.228.160	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-4983-he	Block	1
188.143.232.24	Russian Federation	147.237.77.17	mazi.idf.i	Parameter Type Violation __EVENTVALIDATION in mazi.idf.il/700-he/igf.aspx	Block	1
91.200.12.138	Ukraine	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/5479-he/igf.aspx/trackback/	Block	1
66.249.78.168	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to www.mazi.idf.il/113-11581-he/œœœ? x'x'xœ x*x*.aspx	Block	1
146.185.234.48	Russian Federation	147.237.77.17	mazi.idf.i	Unauthorized URL Access to www.mazi.idf.il/templates/newslist/newslist.in.aspxundefined	Block	1
85.65.244.66	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/5676-7827-he/ifg.aspx	Block	1
40.77.167.28	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/4262-he/	Block	1
194.176.105.138	United Kingdom	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/sip_storage	Block	1
109.65.155.159	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/sip_storage	Block	1
66.249.78.242	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/14-he/igf.aspx	Block	1
5.29.82.218	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3849-5035-he/igf.aspx	Block	1
149.78.41.173	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/newslist/undefined	Block	1
85.93.91.84	Germany	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/sip_storage/files	Block	1
46.19.86.68	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3849-5035-he/igf.aspx	Block	1
109.66.172.96	Israel	147.237.77.17	mazi.idf.i	Distributed PHP Attempt	Block	1
66.249.78.248	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1
31.154.94.55	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3850-5216-he/igf.aspx	Block	1

01-29-2016 to 01-30-2016