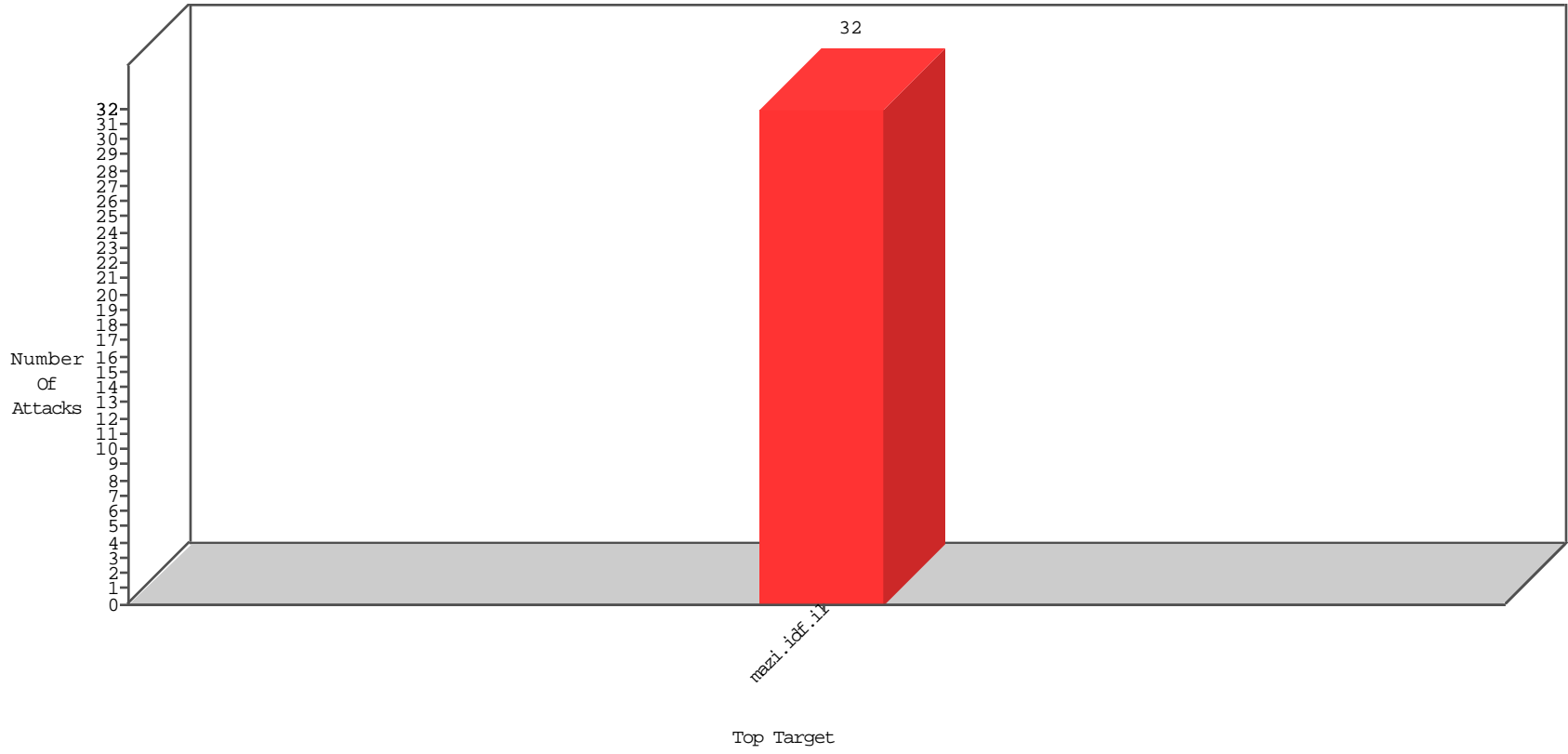


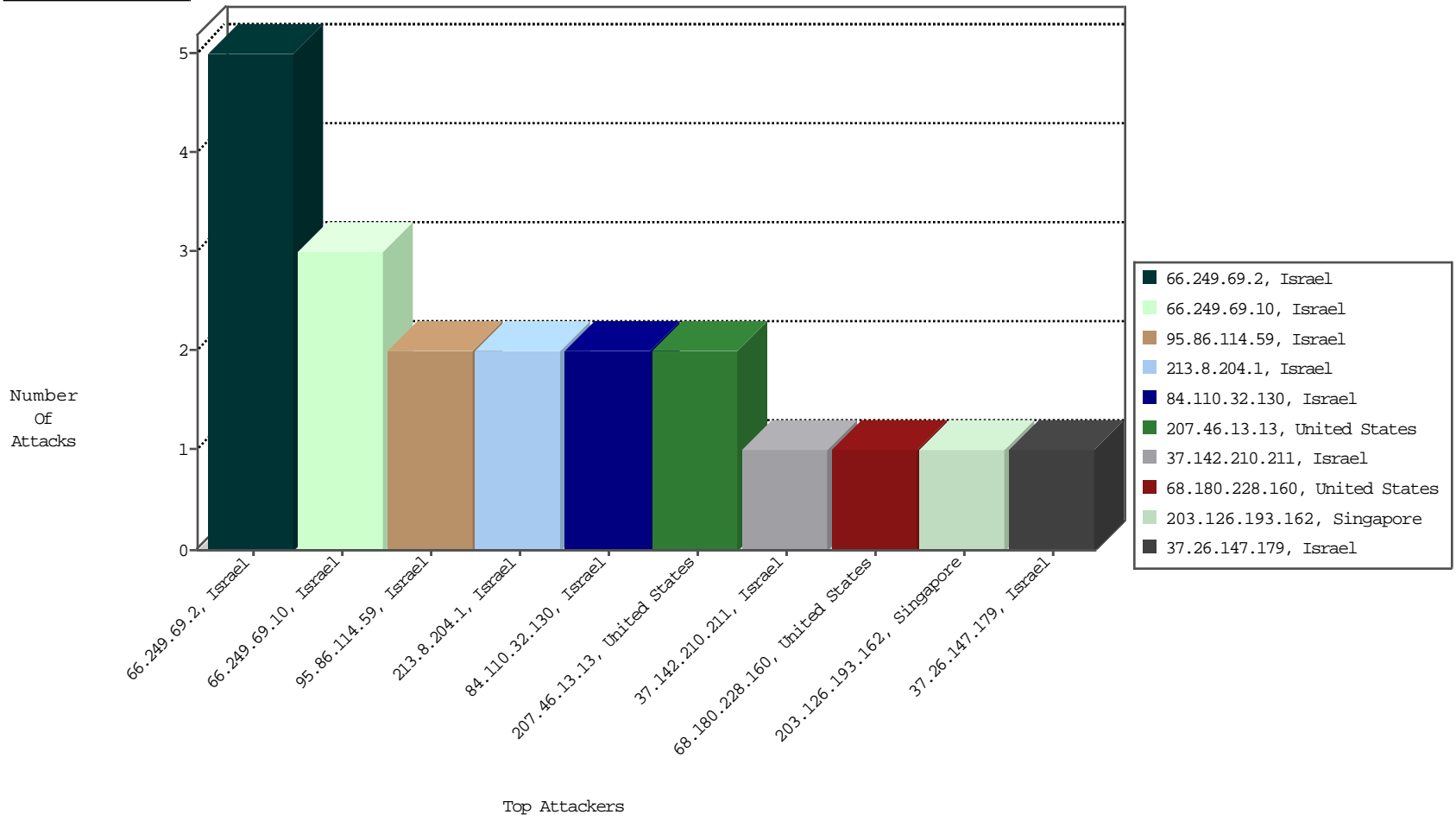
# Focused IP Under Attack Daily Report



Top Targets



Top Attackers



01-06-2016 to 01-07-2016

Top Attackers In DDoS-Defence

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

01-06-2016 to 01-07-2016

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
------------------	--------------	----------------	------	-----------	---------------	-------

## Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
89.248.162.131	Netherlands	147.237.77.17	mazi.idf.il	ET SCAN Potential SSH Scan	1
111.85.219.12	China	147.237.77.17	mazi.idf.il	ET SCAN Potential SSH Scan	1
49.75.129.202	China	147.237.77.17	mazi.idf.il	ET SCAN Potential SSH Scan	1
104.128.144.131	Canada	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 1024	1
185.130.5.231		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
212.76.127.10	Israel	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	104
46.19.85.210	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	100
46.19.85.210	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	100
46.19.85.150	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	36
46.19.85.150	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	36
46.19.85.237	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	26
46.19.85.237	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	25
89.138.125.165	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	25
84.228.229.107	Bulgaria	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
208.115.111.75	United States	147.237.77.17	mazi.idf.i	drop	SAM rule	drop	11
146.135.27.25	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
195.239.16.53	Russian Federation	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	9
149.78.198.160	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	9
212.76.127.111	Israel	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	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
46.19.85.195	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.85.195	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	5
128.127.107.108	Netherlands	147.237.77.17	mazi.idf.i	drop	SAM rule	drop	5
149.78.198.160	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.101	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.86.240	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.126	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
5.22.130.133	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.240	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
31.210.188.51	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
2.54.9.112	Israel	147.237.77.17	mazi.idf.i	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	2
94.230.86.133	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
2.54.131.221	Israel	147.237.77.17	mazi.idf.i	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	2
2.54.183.151	Israel	147.237.77.17	mazi.idf.i	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	2
93.174.93.203	Netherlands	147.237.77.17	mazi.idf.i	Web Server Enforcement Violation	Masscan Port Scanner	reject	1
5.22.130.101	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
84.228.11.174	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1
212.29.210.131	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
71.6.216.40	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.86.77	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
157.55.39.196	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
46.19.85.158	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.154	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
37.26.146.187	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
85.64.207.155	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
79.182.213.112	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1
207.46.13.141	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
185.35.62.196	Switzerland	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
84.228.11.174	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
74.82.47.50	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
203.133.168.9	Korea, Republic of	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.86.140	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	alert	1
141.212.122.155	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

01-06-2016 to 01-07-2016

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
213.8.204.1	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/transvideocounter.gif	Block	2
84.110.32.130	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/transvideocounter.gif	Block	2
95.86.114.59	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/transvideocounter.gif	Block	2
141.212.122.145	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/14-he/igf.aspx	Block	1
66.249.69.18	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/4260-he/igf.aspx	Block	1
66.249.69.2	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3849-5035-he/igf.aspx	Block	1
66.249.69.10	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3697-7116-he/igf.aspx	Block	1
40.77.167.49	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1
203.126.193.162	Singapore	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on mazi.idf.il/images/transvideocounter.gif	Block	1
66.249.69.106	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-10104-he	Block	1
66.249.69.2	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/4943-8365-he/igf.aspx	Block	1
85.17.73.12	Netherlands	147.237.77.17	mazi.idf.i	Parameter Type Violation lang in mazi.idf.il/forums/templates/forums/forumslist.aspx	Block	1
66.249.69.10	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3834-10288-he/igf.aspx	Block	1
46.19.85.213	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3849-5035-he/igf.aspx	Block	1
207.46.13.13	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/4085-he/	Block	1
66.249.69.114	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-10105-he	Block	1
66.249.69.2	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/5551-6171-he/igf.aspx	Block	1
37.26.147.179	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3850-5187-he/igf.aspx	Block	1
66.249.69.10	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1
66.249.69.2	Israel	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on 147.237.77.17/14-he/igf.aspx	Block	1
207.46.13.13	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/page/2	Block	1
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
66.249.69.2	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1
37.142.210.211	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/4637-5227-he/igf.aspx	Block	1

01-06-2016 to 01-07-2016