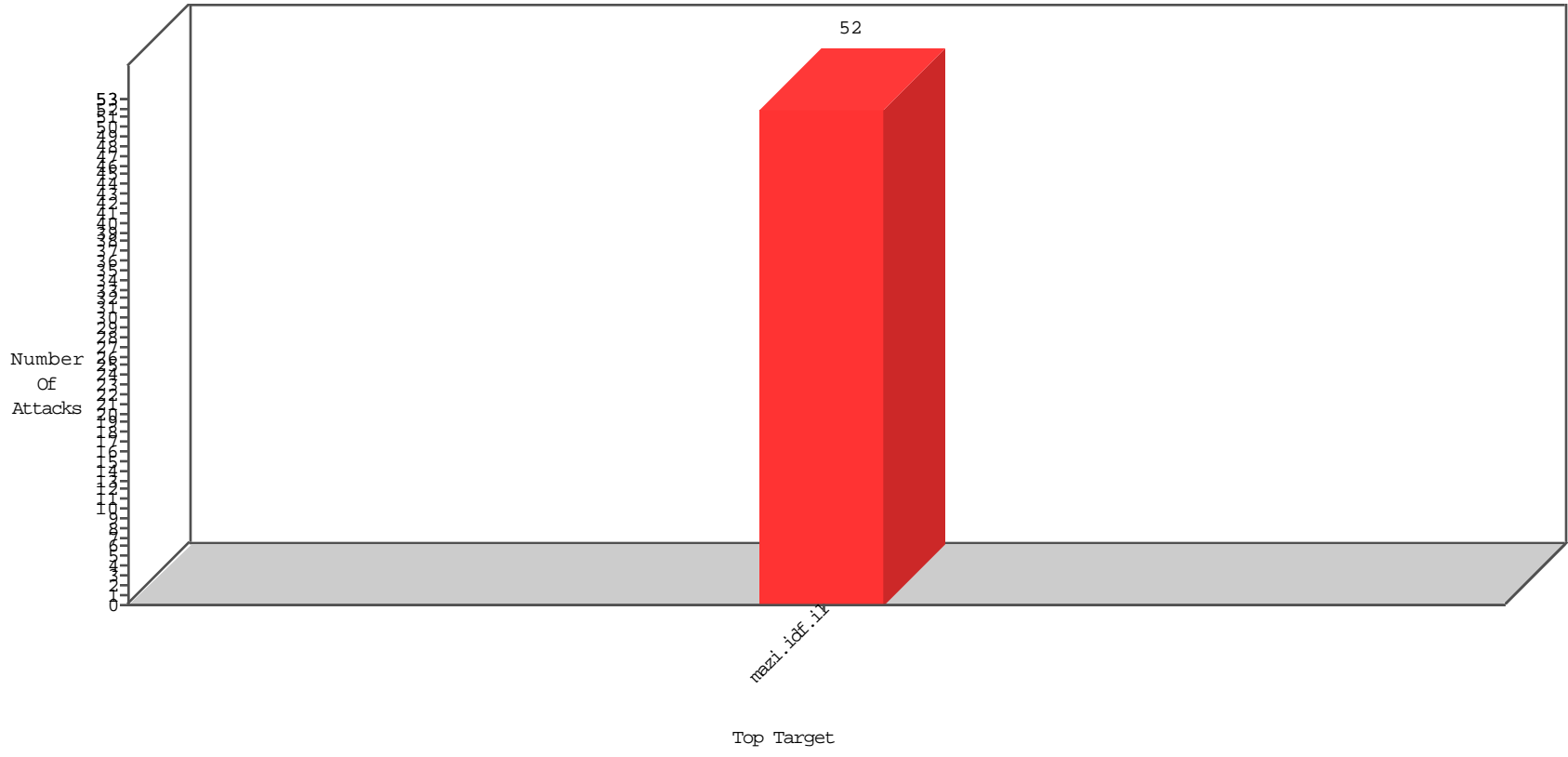


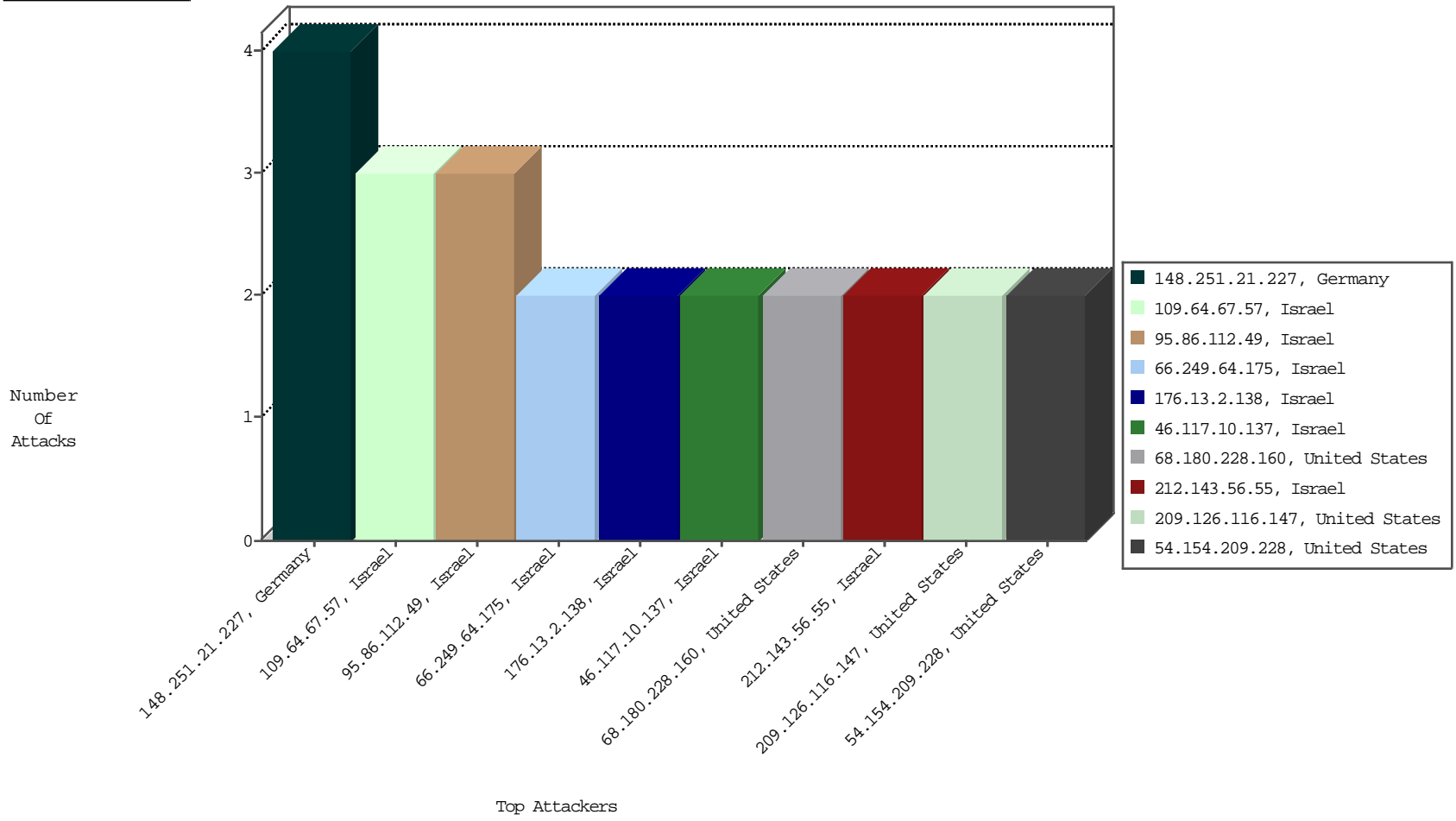
# Focused IP Under Attack Daily Report



Top Targets



Top Attackers



01-04-2016 to 01-05-2016

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
109.64.67.57	Israel	147.237.77.17	mazi.idf.il	Block_Udp_All_Nets	drop	BEL-Isreal	3

01-04-2016 to 01-05-2016

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
106.38.241.106	China	147.237.77.17	mazi.idf.il	C103: HTTP: User Agent Sogou+web+spider	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
180.150.177.188	China	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 1024	1
209.126.116.147	United States	147.237.77.17	mazi.idf.il	ET SCAN Potential SSH Scan	1
31.184.195.115	Russian Federation	147.237.77.17	mazi.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	China	147.237.77.17	mazi.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.224		147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 1024	1
209.126.116.147	United States	147.237.77.17	mazi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
46.172.71.251	Ukraine	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
71.63.209.148	United States	147.237.77.17	mazi.idf.i	drop		drop	289
71.63.209.148	United States	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	144
71.63.209.148	United States	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	144
71.63.209.148	United States	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	84
195.95.183.254	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	61
46.19.85.155	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	53
46.19.85.155	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	49
212.76.127.44	Israel	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	36
144.76.101.243	Germany	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	25
46.19.85.40	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	25
162.144.211.223	United States	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	25
187.45.193.166	Brazil	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	25
142.4.7.164	United States	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	17
79.178.176.78	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
212.76.127.111	Israel	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	9
78.55.29.177	Germany	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
79.182.32.171	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
78.25.121.31	Russian Federation	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.19.86.60	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.60	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
78.25.121.31	Russian Federation	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
185.89.217.225		147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
80.246.130.215	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	3
46.19.85.23	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
80.246.133.68	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
84.108.185.15	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
81.218.153.201	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	2
185.89.217.235		147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
46.19.85.121	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
74.82.47.60	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
185.89.217.233		147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
46.120.17.104	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1
185.3.144.97	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.85.132	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
37.26.147.201	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
83.167.248.160	Czech Republic	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
195.60.232.57	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
185.89.217.227		147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
169.229.3.90	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
87.68.40.29	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
5.39.93.143	France	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
216.243.31.2	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
77.125.245.128	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
185.89.217.233		147.237.77.17	mazi.idf.i	Directory Traversal	directory traversal overflow	monitor	1
46.120.17.104	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
185.24.76.154	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
37.46.39.72	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
185.89.217.228		147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
184.105.139.76	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
93.169.205.76	Romania	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

## Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
95.86.112.49	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/transvideocounter.gif	Block	3
46.117.10.137	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to igf.idf.il/images/transvideocounter.gif	Block	2
176.13.2.138	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to igf.idf.il/hil	Block	2
207.46.13.51	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	2
212.143.56.55	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/sip_storage	Block	2
68.180.230.40	United States	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 147.237.77.17/14-he/igf.aspx	Block	1
148.251.21.227	Germany	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/4070-11595-he/x%Zx-xæx\$xa x^axx x*xÿ x•x'x\$xx".aspx	Block	1
81.218.153.201	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/4637-5227-he/igf.aspx	Block	1
66.249.69.114	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/newslst/undefined	Block	1
54.154.209.228	United States	147.237.77.17	mazi.idf.i	PHP Attempt	Block	1
185.89.217.233		147.237.77.17	mazi.idf.i	URL is Above Root Directory mazi.idf.il/./images/l.he/navigation/navigation_arrow.gif	Block	1
148.251.21.227	Germany	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 148.251.21.227	Block	1
71.63.209.148	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/sip_storage/files/1/2061.jpg	Block	1
66.249.64.175	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/templatecontrols/pictureinfo/pictureinfo.aspx	Block	1
5.28.180.240	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to igf.idf.il/hi	Block	1
157.55.39.83	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/templatecontrols/pictureinfo/pictureinfo.aspx	Block	1
82.166.247.138	Israel	147.237.77.17	mazi.idf.i	Parameter Type Violation Master\$ucHeader\$ucSearchControl\$txtSearch in mazi.idf.il/319-he/igf.aspx	Block	1
68.180.228.160	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/5676-7827-he/ifg.aspx	Block	1
54.154.209.228	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/components/comSexyContactForm/fileupload/index.php	Block	1
185.89.217.233		147.237.77.17	mazi.idf.i	URL is Above Root Directory www.mazi.idf.il/./images/trans.gif	Block	1
148.251.21.227	Germany	147.237.77.17	mazi.idf.i	Unauthorized URL Access to igf.idf.il/templates/shared/usercontrols/newsgallery/	Block	1
77.126.253.68	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/sip_storage/files/1/1351.jpg	Block	1
66.249.64.185	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/571-he/igf.aspx	Block	1
213.151.59.220	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/5010-9153-he/igf.aspx&sa=u&ved=0ahukewjvrbbh2y7kahubgrqkhqf2bag4kbcqhqeiuzas&usg=afqjcnebyfjb6ahfwedj6lql3mqpkb3j1w	Block	1
5.29.223.241	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/sip_storage/files/1/2061.jpg	Block	1
176.12.147.207	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/shared/usercontrols/newsgallery/	Block	1
95.86.69.172	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3850-5216-he/igf.aspx	Block	1
68.180.228.160	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/general/x"	Block	1
66.249.64.26	Israel	147.237.77.17	mazi.idf.i	Parameter Type Violation Back in igf.idf.il/6053-he/igf.aspx	Block	1
206.253.226.22	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1
148.251.21.227	Germany	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-4980-he	Block	1
80.246.130.190	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/sip_storage	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