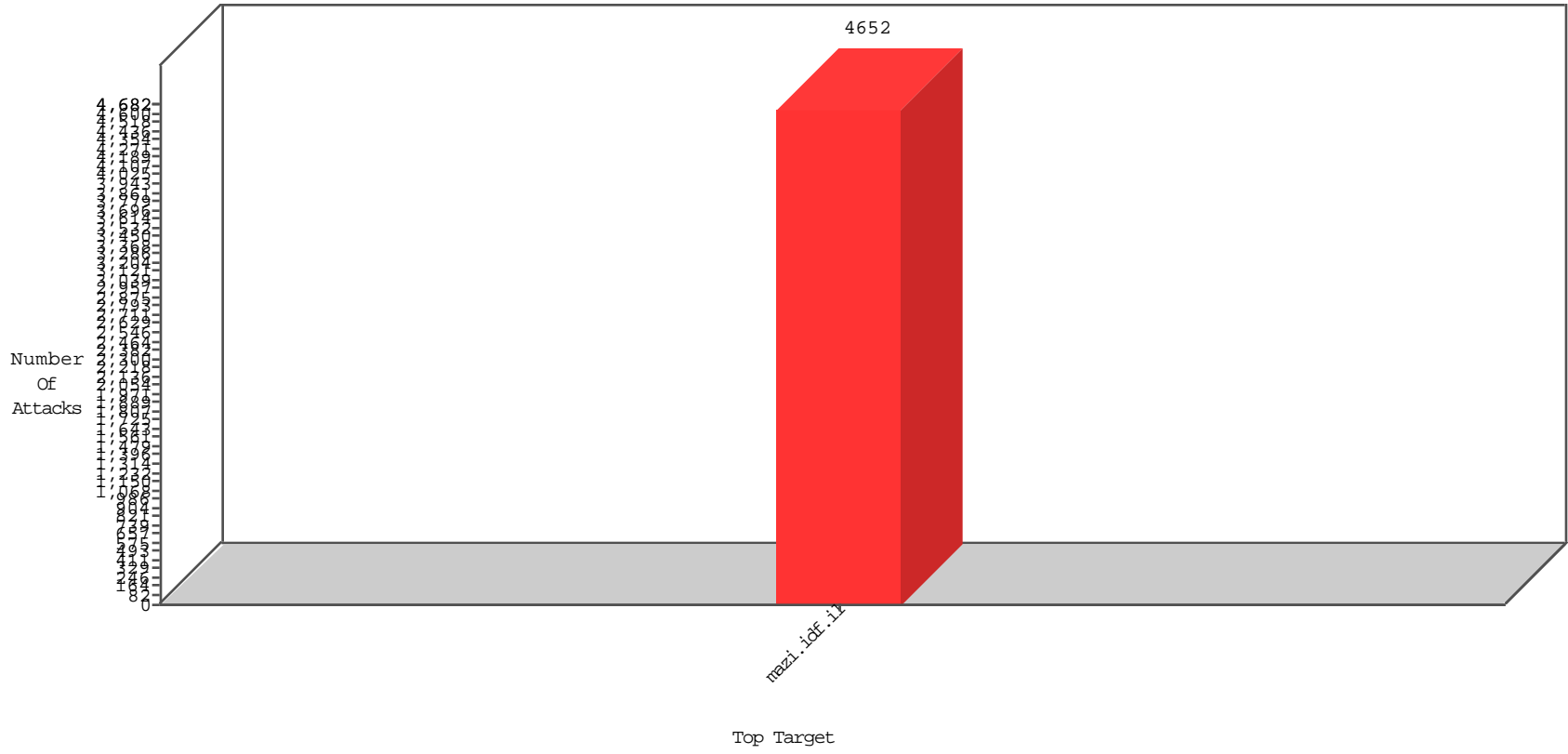


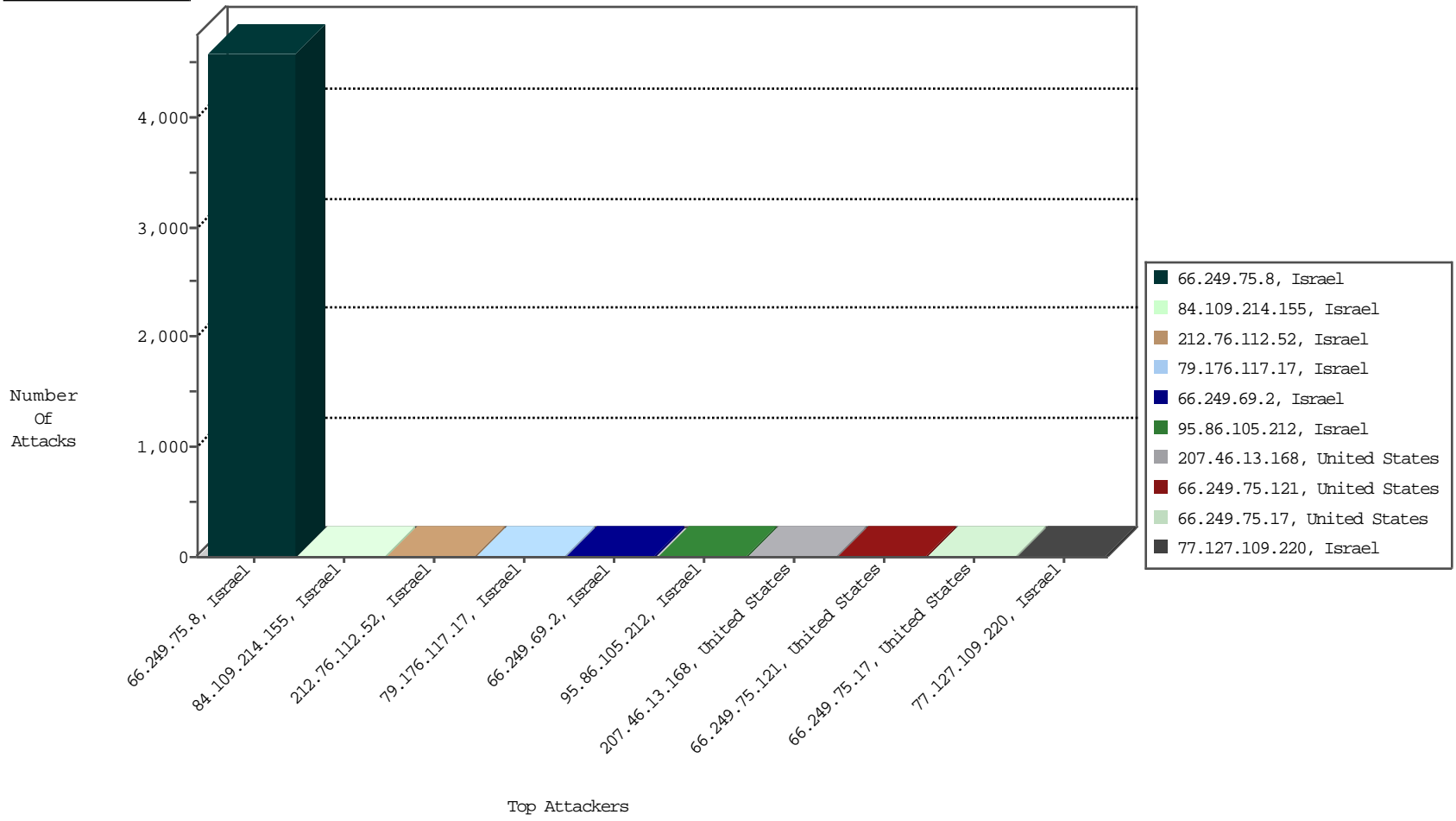
# Focused IP Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
66.249.75.8	Israel	147.237.77.17	mazi.idf.il	TCP handshake violation, first packet not syn	drop	BBL-Frankfurt	4596
79.176.117.17	Israel	147.237.77.17	mazi.idf.il	Block_Udp_All_Nets	drop	BBL-Israel	6

12-24-2015 to 12-25-2015

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	1
106.38.241.106	China	147.237.77.17	mazi.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1

## Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
66.249.75.121	United States	147.237.77.17	mazi.idf.i	ET SCAN NMAP -sA (2)	2
66.249.75.17	United States	147.237.77.17	mazi.idf.i	ET SCAN NMAP -sA (2)	2
87.197.159.157	Slovakia	147.237.77.17	mazi.idf.i	ET SCAN NMAP -sS window 1024	1
46.19.119.74	Russian Federation	147.237.77.17	mazi.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	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	117
37.26.146.226	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	36
109.186.185.133	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	34
212.143.166.113	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid sequence number	monitor	26
46.19.85.6	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	16
46.19.86.44	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	16
82.166.140.117	Israel	147.237.77.17	mazi.idf.i	drop	SAM rule	drop	16
85.130.189.107	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	13
2.52.159.57	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	10
5.29.54.24	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
212.76.127.44	Israel	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	9
46.19.86.233	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
195.239.16.53	Russian Federation	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	9
94.230.86.243	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	5
149.78.173.201	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
5.29.48.218	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
5.29.52.200	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
2.54.8.206	Israel	147.237.77.17	mazi.idf.i	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	4
149.78.126.191	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
37.26.146.139	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence		monitor	4
46.19.86.49	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
5.22.134.96	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
2.54.36.29	Israel	147.237.77.17	mazi.idf.i	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	2
207.241.237.211	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
46.19.85.210	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
85.65.5.181	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
2.54.10.39	Israel	147.237.77.17	mazi.idf.i	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	2
2.54.22.127	Israel	147.237.77.17	mazi.idf.i	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	2
2.52.26.59	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1
46.19.86.94	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.85.142	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
84.111.139.65	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
37.26.146.139	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
80.246.133.222	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1
188.120.148.158	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.86.35	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.131	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
85.65.5.181	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
23.101.61.176	Ireland	147.237.77.17	mazi.idf.i	Instant Messengers	instant messenger pattern found, application: Skype	monitor	1
84.94.32.197	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
79.179.29.147	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
199.203.215.1	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
2.52.26.59	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.86.125	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
176.228.192.18	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.85.196	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
85.65.5.181	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1
80.246.133.222	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1

12-24-2015 to 12-25-2015

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
84.109.214.155	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/newslist/undefined	Block	9
212.76.112.52	Israel	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on mazi.idf.il/images/transvideocounter.gif	Block	8
95.86.105.212	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/transvideocounter.gif	Block	3
77.127.109.220	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/transvideocounter.gif	Block	2
207.46.13.168	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	2
157.55.39.149	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to igf.idf.il/14-7713-he	Block	1
66.249.69.2	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/165-7902-he/igf.aspx	Block	1
95.86.100.229	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/4936-9463-he/igf.aspx&sa=u&ved=0ahukewja4jtv9_tjahvfchokherwdc8qqo ubccywaw&sig2=ru04w4pvw0wngugbwamvaa&usg=afqjcneywgyfk69f_cv7uxfpx916mt66ha	Block	1
66.249.69.62	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to www.mazi.idf.il/templates/shared/usercontrols/newsgallery/	Block	1
46.121.59.197	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/sip_storage	Block	1
157.55.39.155	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/watch_fragments_ajax	Block	1
79.178.34.43	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/sip_storage/files/1/1351.jpg	Block	1
66.249.69.2	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/6300-9396-he/igf.aspx	Block	1
66.249.75.121	Israel	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 147.237.77.17/14-he/igf.aspx	Block	1
157.55.39.203	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/watch_fragments_ajax	Block	1
81.218.182.134	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to igf.idf.il/hi	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
141.212.122.129	United States	147.237.77.17	mazi.idf.i	Malformed URL proxytest.zmap.io:80	Block	1
66.249.75.155	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to igf.idf.il/templates/newslist/undefined	Block	1
66.249.69.2	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/165-7456-he/igf.aspx	Block	1
66.249.69.18	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3728-6976-he/igf.aspx	Block	1
31.184.132.23	Iran, Islamic Republic of	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3850-5187-he/igf.aspx	Block	1

12-24-2015 to 12-25-2015