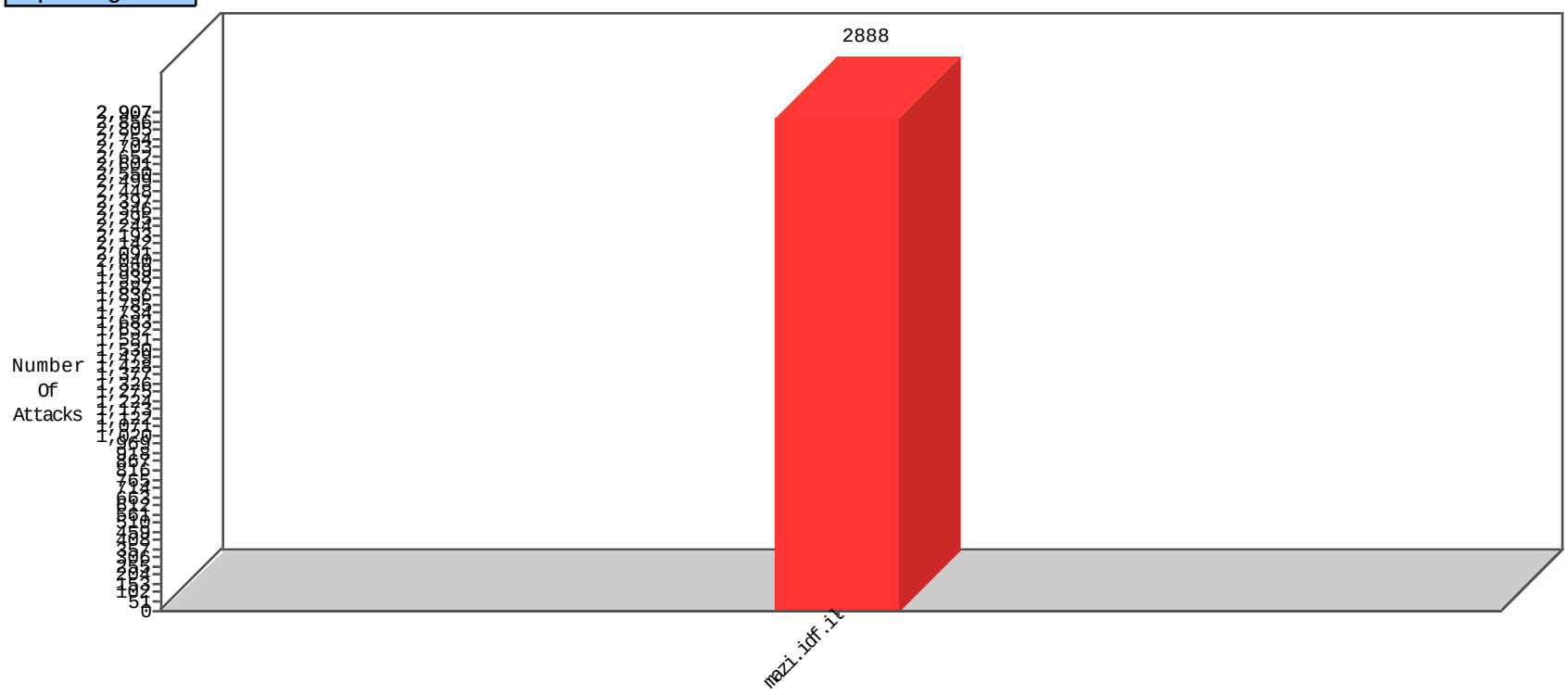
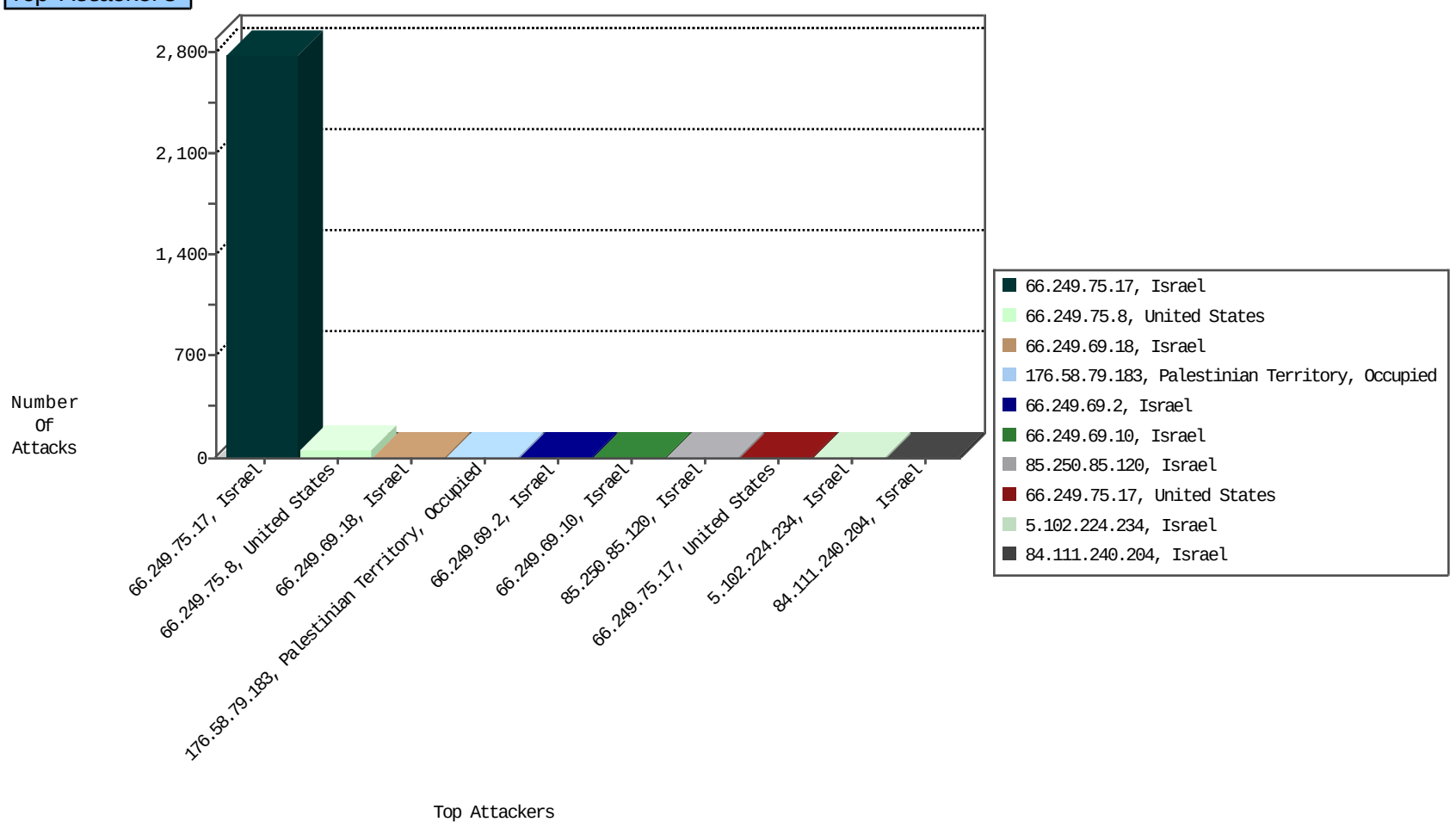
12-25-2015 to 12-26-2015

Focused IP Under Attack Daily Report

Top Targets



Top Attackers



12-25-2015 to 12-26-2015

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
66.249.75.17	Israel	147.237.77.17	mazi.idf.il	TCP handshake violation, first packet not syn	drop	BBL-Frankfurt	2776

12-25-2015 to 12-26-2015

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count

12-25-2015 to 12-26-2015

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
66.249.75.8	United States	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sA (2)	62
66.249.75.17	United States	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sA (2)	2
31.19.116.8	Germany	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 1024	1
88.249.106.23	Turkey	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 1024	1
218.104.49.211	China	147.237.77.17	mazi.idf.il	ET SCAN Potential SSH Scan	1
61.244.49.137	Hong Kong	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 1024	1
125.88.181.94	China	147.237.77.17	mazi.idf.il	ET SCAN Potential SSH Scan	1

12-25-2015 to 12-26-2015

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
46.19.85.74	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	36
46.19.85.74	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	26
46.19.86.56	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	25
84.111.240.204	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	16
84.111.240.204	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	16
195.239.16.40	Russian Federation	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	9
89.178.102.207	Russian Federation	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	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
2.52.185.165	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
89.178.102.207	Russian Federation	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	9
46.19.86.2	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
89.178.102.207	Russian Federation	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	9
203.133.169.154	Korea, Republic of	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
89.178.102.207	Russian Federation	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid sequence number	monitor	9
213.57.128.215	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
46.117.227.101	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.114	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
5.29.0.13	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
213.57.139.114	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
46.19.86.56	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
130.193.51.60	Russian Federation	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
130.193.51.60	Russian Federation	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
46.19.85.95	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
128.232.110.28	United Kingdom	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
2.54.59.179	Israel	147.237.77.17	mazi.idf.i	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	2
23.101.61.176	Ireland	147.237.77.17	mazi.idf.i	Instant Messengers	instant messenger pattern found, application: Skype	monitor	1
80.246.133.169	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
66.249.75.146	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
46.19.86.199	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1
46.19.86.50	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
94.230.86.147	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
213.57.165.236	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
85.64.24.193	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
207.241.237.211	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
5.22.131.161	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
77.125.162.124	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1
184.105.247.231	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.117.227.101	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1
149.88.86.183	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.86.78	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
109.67.36.216	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.86.2	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
84.111.82.42	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
66.249.93.19	Israel	147.237.77.17	mazi.idf.i	Directory Traversal	directory traversal overflow	monitor	1
180.76.15.154	China	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
46.19.86.199	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
141.0.15.160	Norway	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.86.52	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
103.237.36.230	Bangladesh	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	1

12-25-2015 to 12-26-2015

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
176.58.79.183	Palestinian Territory, Occupied	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/newslist/undefined	Block	4
85.250.85.120	Israel	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on mazi.idf.il/templates/newslist/undefined	Block	2
66.249.69.10	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	2
84.108.100.222	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to igf.idf.il/113-7894-he/undefined	Block	2
84.111.240.204	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/newslist/undefined	Block	2
66.249.75.121	Israel	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on mazi.idf.il/templates/newslist/undefined	Block	1
66.249.69.2	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/6578-9989-he/igf.aspx	Block	1
5.102.224.234	Israel	147.237.77.17	mazi.idf.i	PHP Attempt	Block	1
207.46.13.32	United States	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on 147.237.77.17/robots.txt	Block	1
103.237.36.230	Bangladesh	147.237.77.17	mazi.idf.i	Suspicious Response Code	Block	1
77.75.79.72	Czech Republic	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/sip_storage/files/9/8699.jpg	Block	1
66.249.69.18	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3697-he/igf.aspx	Block	1
66.249.69.2	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3697-10520-he/igf.aspx	Block	1
157.55.39.226	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/common/logininfo.aspx	Block	1
85.65.228.130	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/sip_storage/files/7/1087.jpg	Block	1
66.249.93.19	Israel	147.237.77.17	mazi.idf.i	URL is Above Root Directory m.mazi.idf.il/../images/body.jpg	Block	1
66.249.69.10	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/4940-8409-he/igf.aspx	Block	1
5.102.224.234	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to www.mazi.idf.il/xmlrpc.php	Block	1
207.46.13.32	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/6107-he/igf.aspx	Block	1
141.212.121.176	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/14-he/igf.aspx	Block	1
77.237.138.202	Czech Republic	147.237.77.17	mazi.idf.i	Unauthorized Method HEAD for /	Block	1
66.249.69.18	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/6222-9239-he/igf.aspx	Block	1
66.249.69.2	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3850-5187-he/igf.aspx	Block	1
77.75.77.17	Czech Republic	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/sip_storage/files/9/8699.jpg	Block	1
37.142.147.252	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3848-5183-he/igf.aspx	Block	1
207.46.13.44	United States	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on 147.237.77.17/robots.txt	Block	1
157.55.39.36	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1
66.249.69.18	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/6752-10492-he/igf.aspx	Block	1
66.249.69.2	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/5010-he/igf.aspx	Block	1
198.20.69.74	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1
87.68.63.127	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/sip_storage/files/1/1351.jpg	Block	1
77.75.78.171	Czech Republic	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/sip_storage/files/9/8699.jpg	Block	1
66.249.69.18	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/113-8759-he/igf.aspx	Block	1
46.117.18.170	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/14-he/igf.aspx	Block	1
207.46.13.168	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1
157.55.39.197	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1

12-25-2015 to 12-26-2015