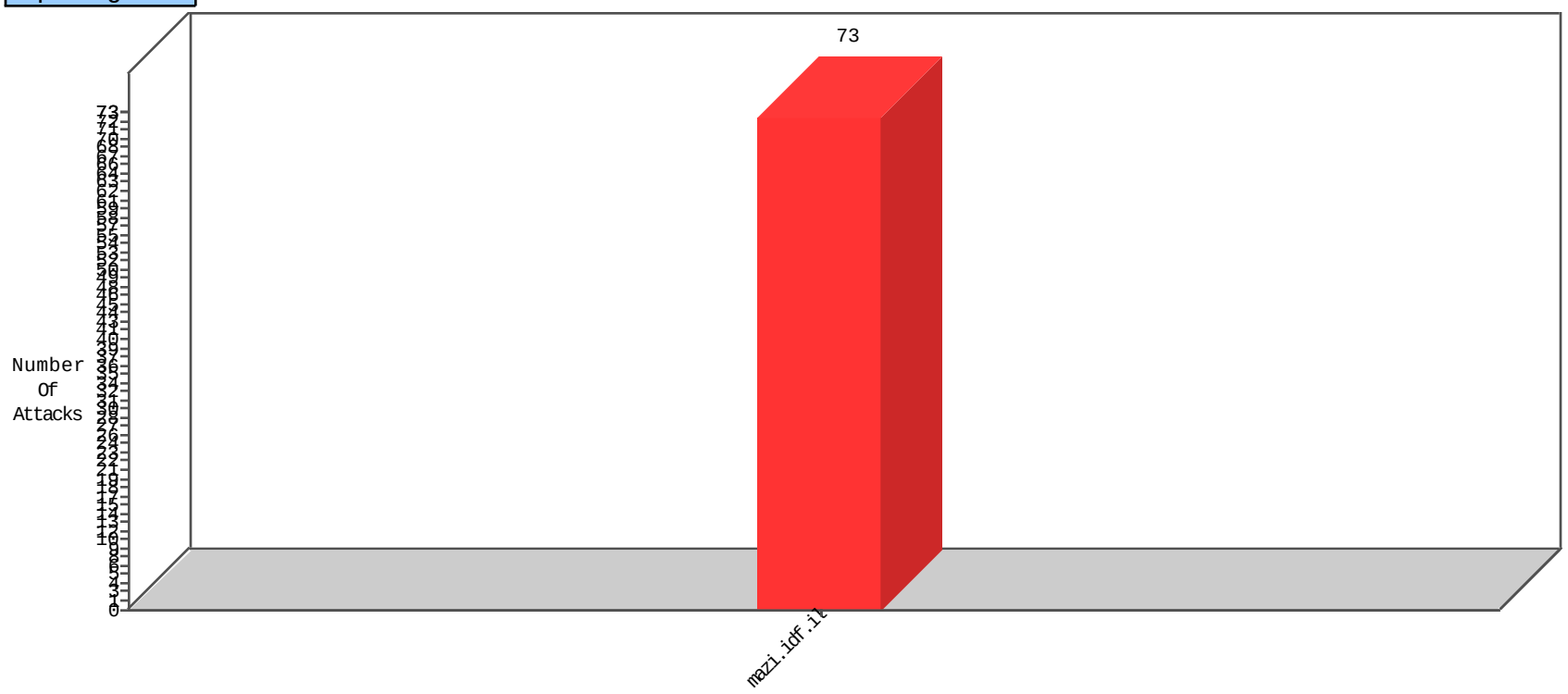
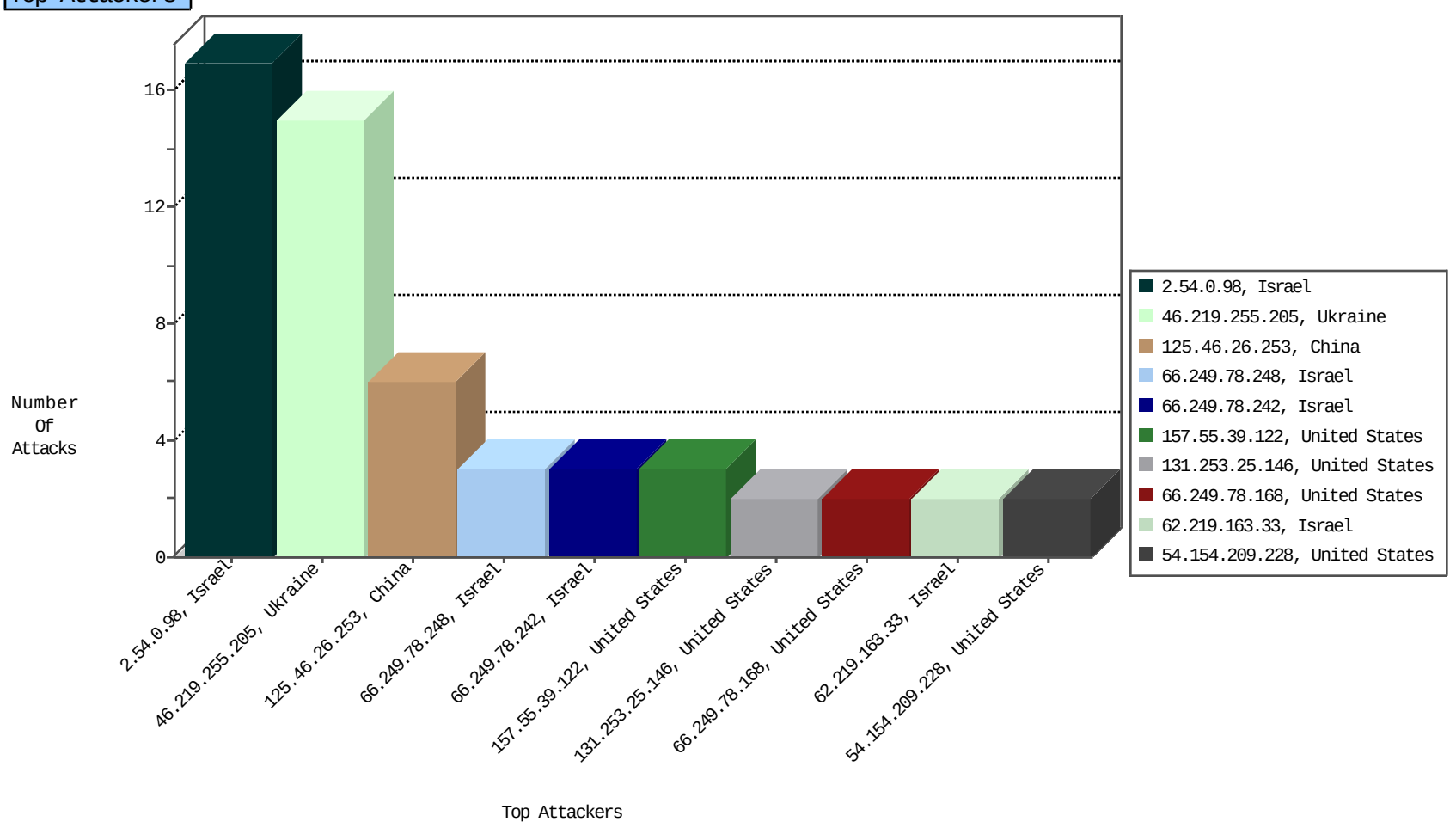
12-31-2015 to 01-01-2016

Focused IP Under Attack Daily Report

Top Targets



Top Attackers



12-31-2015 to 01-01-2016

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
180.97.106.36	China	147.237.77.17	mazi.idf.il	block-sp-traf1	drop	BBL-Frankfurt	1

12-31-2015 to 01-01-2016

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count

12-31-2015 to 01-01-2016

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
46.219.255.205	Ukraine	147.237.77.17	mazi.idf.il	SERVER-WEBAPP admin.php access	2
66.249.78.168	United States	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sA (2)	2
50.204.188.142	United States	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 1024	1

12-31-2015 to 01-01-2016

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
46.19.85.162	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	38
46.19.85.162	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	18
87.69.33.168	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	17
84.109.73.80	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	16
87.69.33.168	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	16
46.19.85.232	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	13
212.76.127.10	Israel	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	10
31.210.188.80	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	10
37.26.147.143	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	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
37.26.147.143	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	9
46.19.85.65	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	9
46.19.86.14	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	9
46.19.85.211	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	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
46.19.86.48	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	9
213.57.137.150	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
213.57.137.150	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
91.200.12.143	Ukraine	147.237.77.17	mazi.idf.i	drop	SAM rule	drop	8
46.19.86.172	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	5
31.210.188.65	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.232	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
91.200.12.7	Ukraine	147.237.77.17	mazi.idf.i	drop	SAM rule	drop	4
46.19.86.172	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
5.22.129.70	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.211	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
213.57.42.200	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
37.26.147.151	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	4
84.109.5.66	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	4
176.13.22.111	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	4
172.56.13.157	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
213.57.128.241	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
84.109.5.66	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
176.13.22.111	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
91.200.12.136	Ukraine	147.237.77.17	mazi.idf.i	drop	SAM rule	drop	3
37.26.147.151	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	3
5.29.116.237	Israel	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
37.26.147.223	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	2
2.54.173.70	Israel	147.237.77.17	mazi.idf.i	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	2
85.64.73.160	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	2
37.26.147.223	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
85.64.73.160	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
46.121.228.240	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
79.182.226.205	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
176.13.20.191	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1
109.162.158.204	Iran, Islamic Republic of	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.85.130	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
85.130.222.39	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
84.109.8.137	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1
176.228.186.39	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1

12-31-2015 to 01-01-2016

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
2.54.0.98	Israel	147.237.77.17	mazi.idf.i	Suspicious Response Code	Block	17
46.219.255.205	Ukraine	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 46.219.255.205	Block	5
46.219.255.205	Ukraine	147.237.77.17	mazi.idf.i	Distributed Admin Blocking	Block	4
46.219.255.205	Ukraine	147.237.77.17	mazi.idf.i	Distributed PHP Attempt	Block	4
62.219.163.33	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to igf.idf.il/templates/newslist/undefined	Block	2
125.46.26.253	China	147.237.77.17	mazi.idf.i	PHP Attempt	Block	2
125.46.26.253	China	147.237.77.17	mazi.idf.i	Unauthorized URL Access to igf.idf.il/wp-admin/admin-ajax.php	Block	2
207.46.13.16	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to www.mazi.idf.il/weather.html	Block	1
157.55.39.122	United States	147.237.77.17	mazi.idf.i	Distributed PHP Attempt	Block	1
125.46.26.253	China	147.237.77.17	mazi.idf.i	Admin Blocking	Block	1
66.249.78.242	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3849-5034-he/igf.aspx	Block	1
54.154.209.228	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/wp-includes/simplepie/theme-options.php	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
157.55.39.205	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1
131.253.25.146	United States	147.237.77.17	mazi.idf.i	PHP Attempt	Block	1
66.249.78.248	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/sip_storage/files/7/1087.jpg	Block	1
66.249.69.18	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1
207.46.13.104	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1
157.55.39.122	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/5551-7559-he/'+src+'	Block	1
125.46.26.253	China	147.237.77.17	mazi.idf.i	Multiple Admin Blocking from 125.46.26.253	Block	1
66.249.78.242	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/5010-7591-he/igf.aspx	Block	1
31.184.133.21	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
176.12.140.194	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/sip_storage/files/1/2061.jpg	Block	1
131.253.25.146	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/member/ajax_loginsta.php	Block	1
68.180.228.160	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-he	Block	1
66.249.78.10	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to igf.idf.il/templates/newslist/undefined	Block	1
157.55.39.122	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/index.php	Block	1
66.249.78.248	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/120-he/mazi.aspx	Block	1
66.249.69.2	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/6368-9575-he/igf.aspx	Block	1
46.19.86.154	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/sip_storage/files/1/1351.jpg	Block	1
182.118.55.191	China	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/14-he/igf.aspx	Block	1
133.130.48.124	Japan	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/4637-5227-he/igf.aspx	Block	1
77.237.138.202	Czech Republic	147.237.77.17	mazi.idf.i	Unauthorized Method HEAD for /	Block	1
66.249.78.242	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/14-he/igf.aspx	Block	1
54.154.209.228	United States	147.237.77.17	mazi.idf.i	Distributed PHP Attempt	Block	1
157.55.39.190	United States	147.237.77.17	mazi.idf.i	Parameter Type Violation t in www.mazi.idf.il/scriptresource.axd	Block	1
66.249.78.248	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/4943-8376-he/igf.aspx	Block	1
66.249.69.10	Israel	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on 147.237.77.17/robots.txt	Block	1

12-31-2015 to 01-01-2016