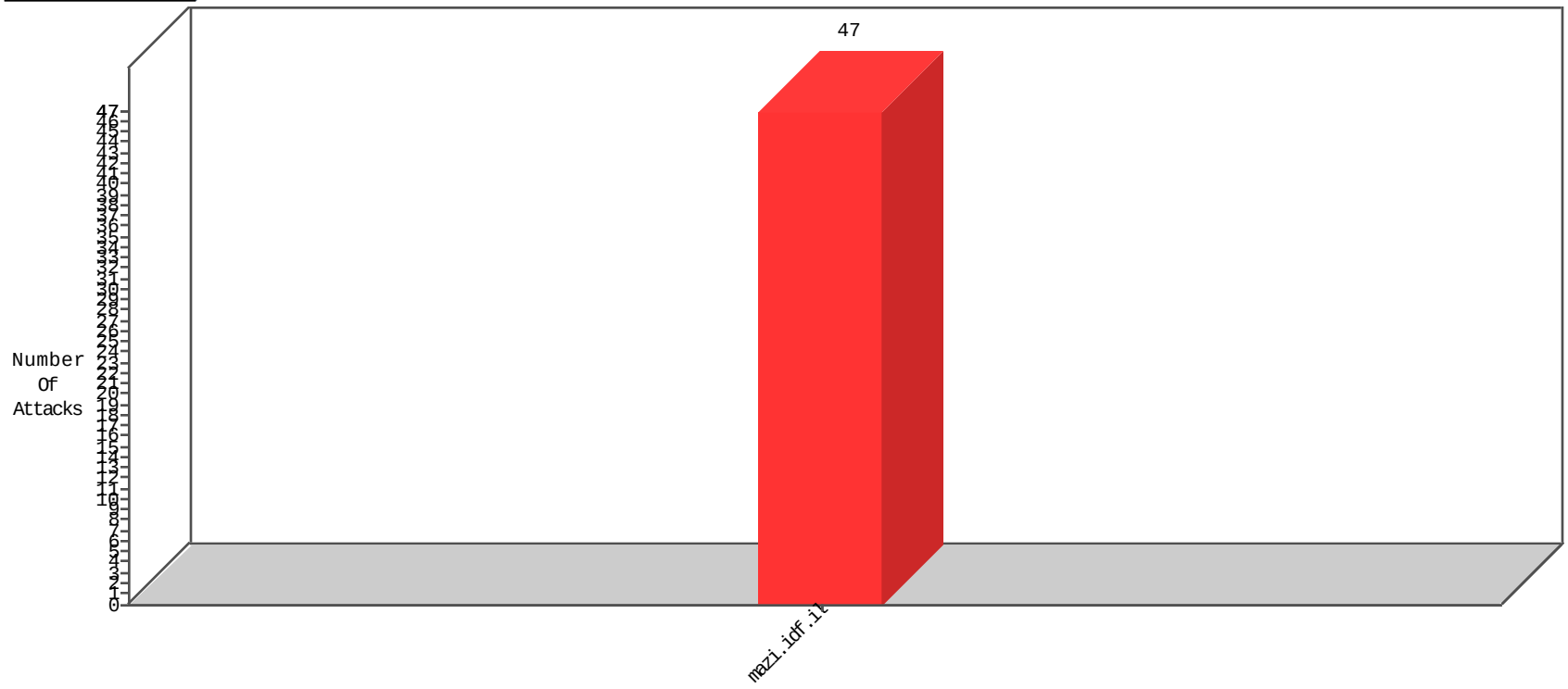
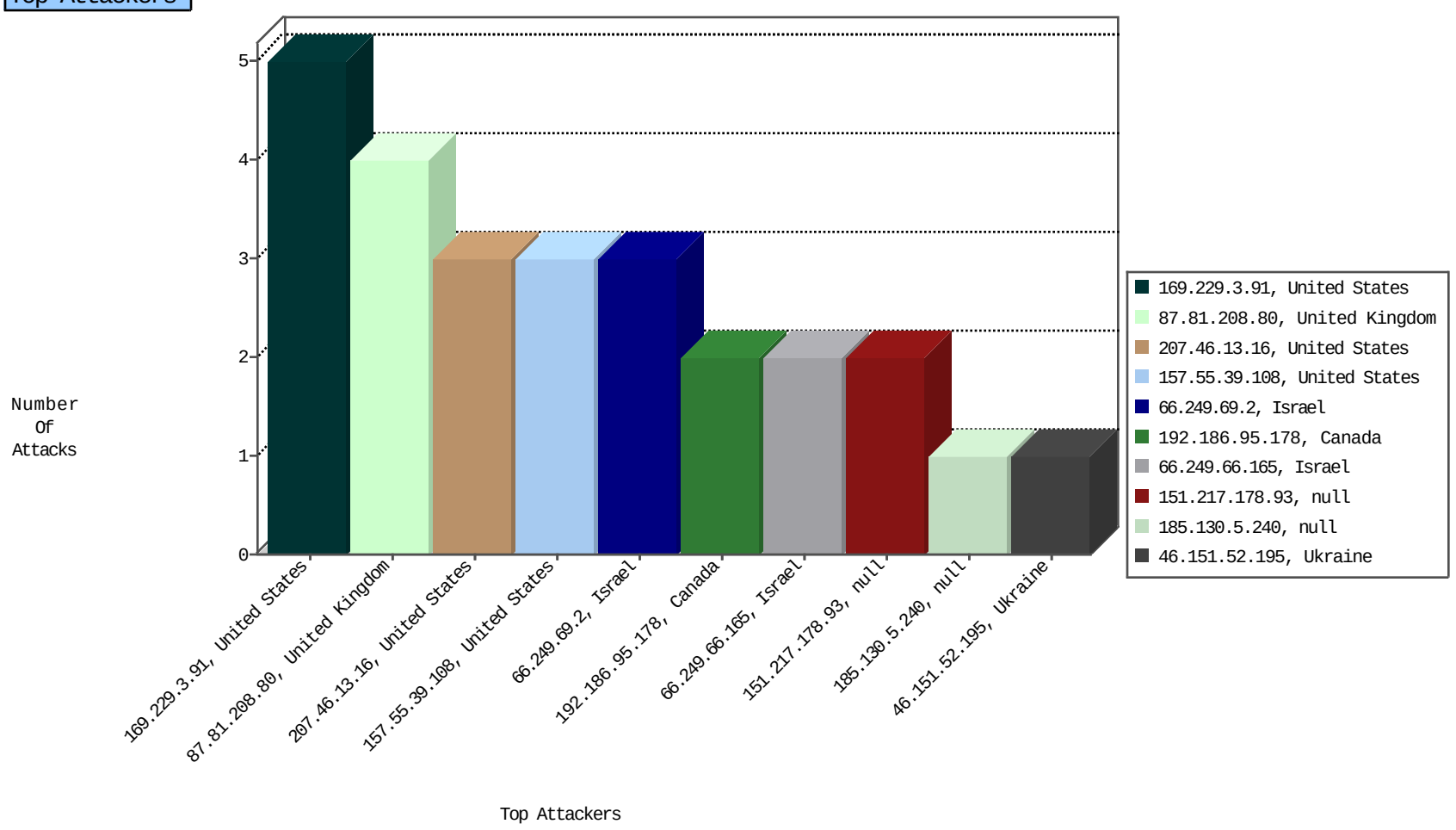
12-30-2015 to 12-31-2015

Focused IP Under Attack Daily Report

Top Targets



Top Attackers



12-30-2015 to 12-31-2015

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
66.249.78.181	Israel	147.237.77.17	mazi.idf.il	TCP handshake violation, first packet not syn	drop	BBL-Frankfurt	1

12-30-2015 to 12-31-2015

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

12-30-2015 to 12-31-2015

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
87.81.208.80	United Kingdom	147.237.77.17	mazi.idf.il	Tehila - Perl LWP with fake user agent	4
151.217.178.93		147.237.77.17	mazi.idf.il	ET SCAN Potential SSH Scan	2
46.151.52.195	Ukraine	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 1024	1
151.217.146.30		147.237.77.17	mazi.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.240		147.237.77.17	mazi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
192.186.95.178	Canada	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 2048	1
192.186.95.178	Canada	147.237.77.17	mazi.idf.il	ET SCAN NMAP -f -sS	1

12-30-2015 to 12-31-2015

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
2.54.148.174	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	144
31.168.24.58	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid sequence number	monitor	81
130.203.136.75	United States	147.237.77.17	mazi.idf.i	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	46
46.19.85.114	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	36
46.19.85.114	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	36
84.228.233.89	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	29
79.179.179.121	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	25
84.228.236.184	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	25
85.130.184.55	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	21
213.57.164.201	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	16
46.120.46.12	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	16
85.130.184.55	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	15
2.52.165.207	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
46.120.46.12	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	9
212.76.127.10	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
37.142.250.23	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
109.160.244.152	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	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
46.245.54.231	Iran, Islamic Republic of	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	9
213.57.164.201	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	9
213.57.135.234	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
178.62.48.159	United States	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	8
207.46.13.152	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.245.54.231	Iran, Islamic Republic of	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	5
213.57.135.234	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
31.210.188.123	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.185	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	4
2.52.11.30	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.85.231	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	4
82.81.46.21	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
46.19.85.231	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.119	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
84.108.123.92	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.117.104.184	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
109.253.140.147	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
2.54.182.22	Israel	147.237.77.17	mazi.idf.i	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	2
37.26.146.155	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
2.54.191.20	Israel	147.237.77.17	mazi.idf.i	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	2
5.102.254.29	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
109.65.96.238	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
2.54.3.0	Israel	147.237.77.17	mazi.idf.i	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	2
5.102.254.101	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
2.54.168.185	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.121.178	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.85.211	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
109.65.123.56	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
188.161.66.134	Palestinian Territory, Occupied	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1

12-30-2015 to 12-31-2015

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
84.228.233.89	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3849-5035-he/igf.aspx	Block	1
66.249.69.2	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/5198-he/igf.aspx	Block	1
207.46.13.44	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to www.mazi.idf.il/14-8671-he	Block	1
46.19.86.193	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3850-5187-he/igf.aspx	Block	1
169.229.3.91	United States	147.237.77.17	mazi.idf.i	Malformed URL	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
79.179.9.178	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to igf.idf.il/templates/newslist/undefined	Block	1
66.249.66.169	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1
207.46.13.16	United States	147.237.77.17	mazi.idf.i	PHP Attempt	Block	1
157.55.39.190	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/rendermap.ashx	Block	1
91.193.51.38	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3848-5183-he/igf.aspx	Block	1
66.249.69.2	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/6072-8876-he/igf.aspx	Block	1
213.57.57.215	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/sip_storage/files/1/1351.jpg	Block	1
46.200.25.112	Ukraine	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/sip_storage/files/5/8895.jpg	Block	1
169.229.3.91	United States	147.237.77.17	mazi.idf.i	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
157.55.39.108	United States	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 157.55.39.108	Block	1
79.182.116.223	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/transvideocounter.gif	Block	1
66.249.66.173	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/5477-he/igf.aspx	Block	1
207.46.13.16	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/4384-he/	Block	1
169.229.3.91	United States	147.237.77.17	mazi.idf.i	Abnormally Long Request method	Block	1
95.86.122.207	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to m.mazi.idf.il/7322-11795-he/mazi.aspx&sa=u&ved=0ahukewiatu6ykypkahwiphqkhuebbn0qfggpmai&sig2=ch0pgs7oabdsdyqn7c99fq&usg=afqjcngb9i08tw3fbb4lqxjmi_tdvhcb7w	Block	1
66.249.78.248	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/4943-8361-he/igf.aspx	Block	1
66.249.66.165	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/113-9067-he/igf.aspx	Block	1
169.229.3.91	United States	147.237.77.17	mazi.idf.i	Multiple Unknown HTTP Request Method from 169.229.3.91	Block	1
157.55.39.108	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/!file/!id9721	Block	1
80.246.133.243	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 147.237.77.17/14-he/igf.aspx	Block	1
207.46.13.16	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/buxus/project_includes/captcha/captcha_image.php	Block	1
169.229.3.91	United States	147.237.77.17	mazi.idf.i	Illegal Byte Code Character in Header Name	Block	1
104.254.235.13		147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/5580-7562-he/igf.asp	Block	1
68.180.228.160	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-4980-he	Block	1
66.249.66.165	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1
187.161.116.239	Mexico	147.237.77.17	mazi.idf.i	Unauthorized URL Access to /tmunblock.cgi	Block	1
157.55.39.108	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/bundles/company2	Block	1

12-30-2015 to 12-31-2015