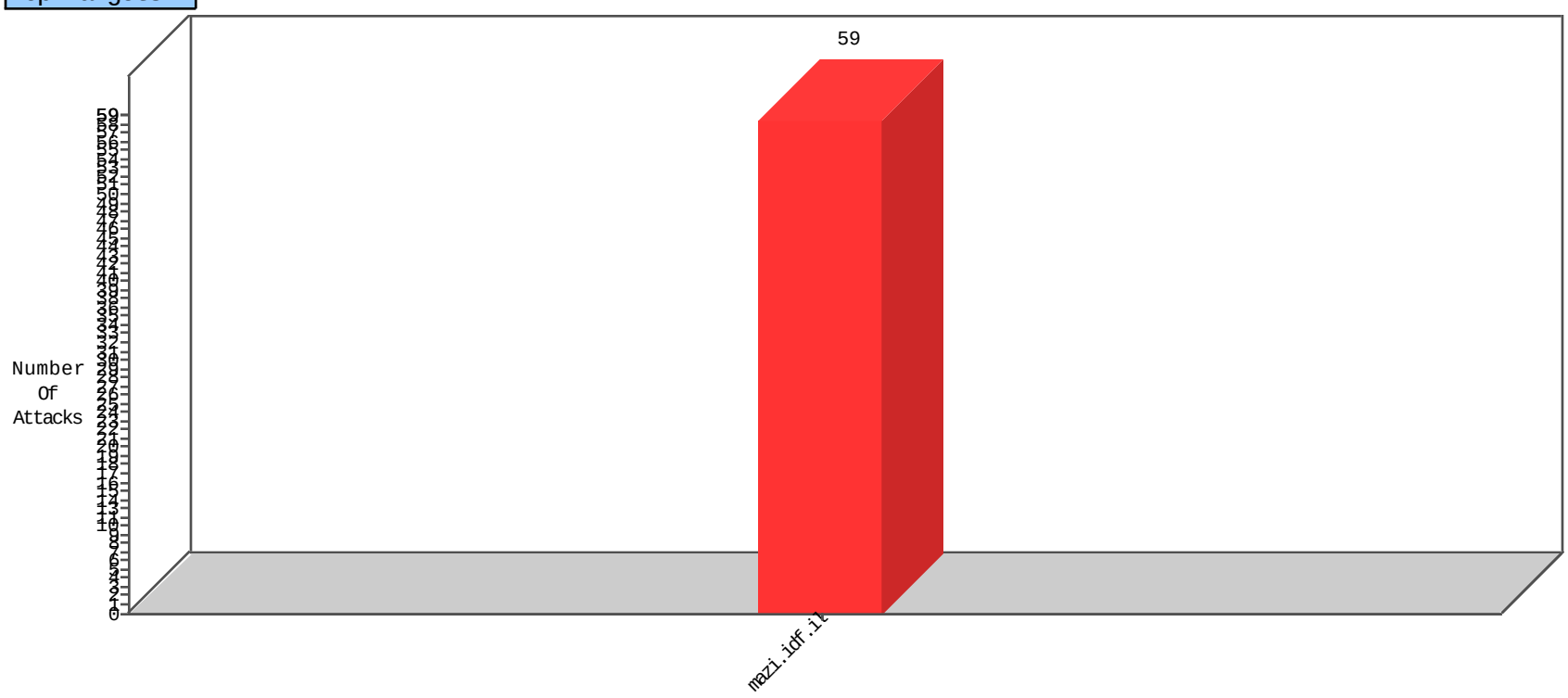
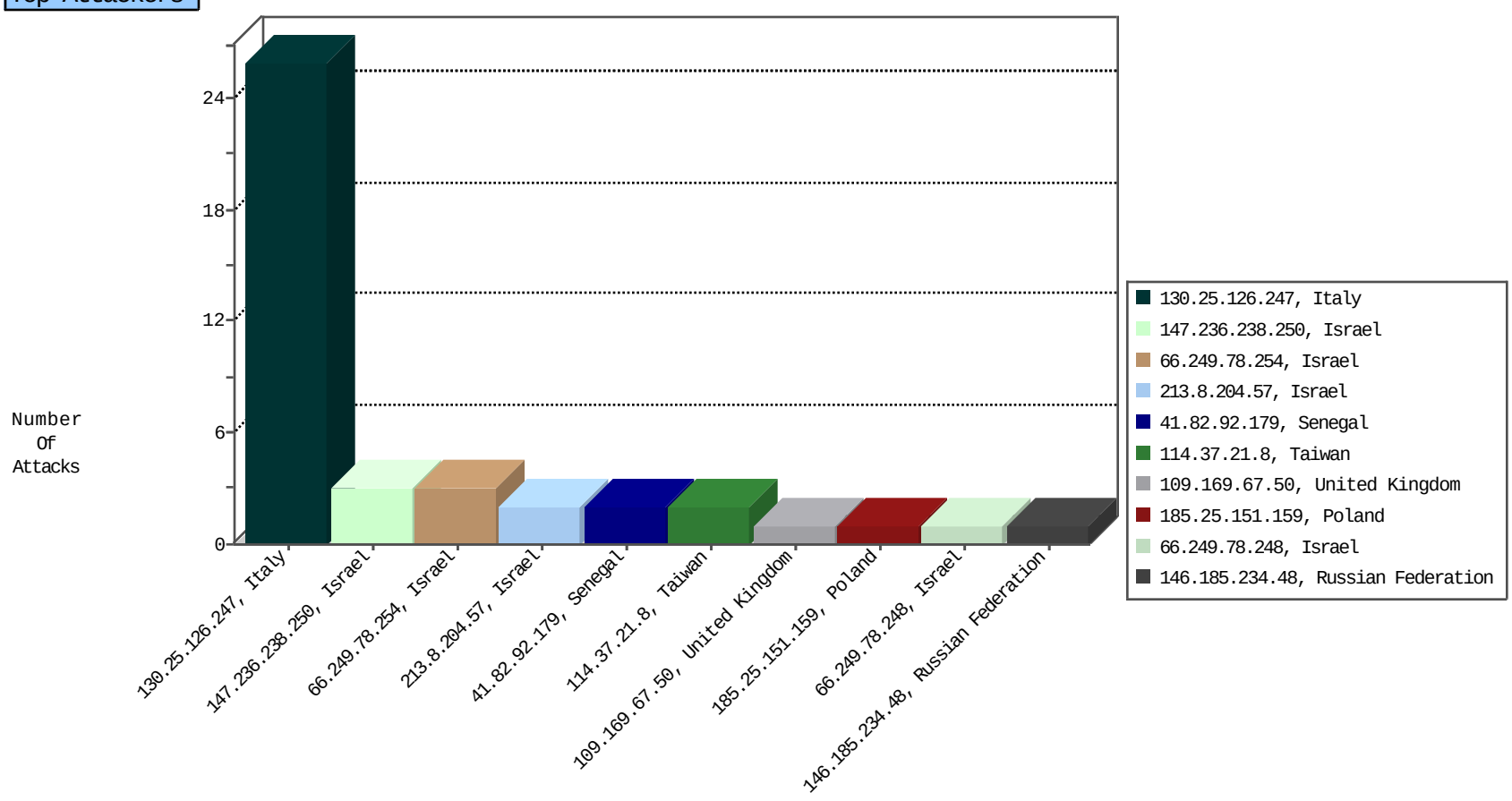
02-08-2016 to 02-09-2016

Focused IP Under Attack Daily Report

Top Targets



Top Attackers



02-08-2016 to 02-09-2016

Top Attackers In DDoS-Defence

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

02-08-2016 to 02-09-2016

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
151.80.31.131	Italy	147.237.77.17	mazi.idf.il	C228: HTTP: AhrefBot crawler	Block	1
220.156.187.4	India	147.237.77.17	mazi.idf.il	C228: HTTP: AhrefBot crawler	Block	1

02-08-2016 to 02-09-2016

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
130.25.126.247	Italy	147.237.77.17	mazi.idf.il	Tehila - Perl LWP with fake user agent	6
130.25.126.247	Italy	147.237.77.17	mazi.idf.il	LOCAL_RULES access attempt to file_manager.php	2
46.45.137.67	Turkey	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 1024	1
114.37.21.8	Taiwan	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 2048	1
218.246.0.97	China	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 1024	1
114.37.21.8	Taiwan	147.237.77.17	mazi.idf.il	ET SCAN NMAP -f -sS	1
185.130.5.165		147.237.77.17	mazi.idf.il	ET SCAN Potential SSH Scan	1

02-08-2016 to 02-09-2016

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
212.76.127.219	Israel	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	90
46.19.85.232	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	81
80.178.157.42	Israel	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	72
46.19.85.232	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	65
46.19.85.213	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	38
212.76.127.10	Israel	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	36
79.183.106.164	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	36
31.168.165.230	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	36
46.19.85.59	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	36
212.76.127.111	Israel	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	36
46.19.85.199	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	26
46.19.86.210	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	25
2.52.14.20	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	22
46.19.85.130	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	16
46.19.85.130	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	16
2.52.14.20	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	9
37.26.149.191	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
2.52.14.20	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	9
217.132.255.91	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	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
2.52.14.20	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid sequence number	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
46.19.86.188	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	9
37.46.38.63	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.213	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	5
41.82.92.179	Senegal	147.237.77.17	mazi.idf.i	Header Rejection	header rejection pattern found in request	monitor	4
212.76.127.44	Israel	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
89.138.111.76	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
46.19.85.178	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.227	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
176.13.4.97	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	3
185.3.147.10	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	3
78.95.111.61	Romania	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
37.130.227.133	United Kingdom	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
185.89.217.227		147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
157.55.39.105	United States	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
94.230.86.157	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
89.138.111.76	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
157.55.39.105	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
213.204.101.24	Lebanon	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
104.131.107.95	United States	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
5.102.254.11	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
85.130.128.143	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
193.105.134.220	Sweden	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
185.89.217.228		147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
184.105.139.104	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
155.94.254.143	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
212.179.219.26	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
37.26.147.191	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
91.207.60.64	Ukraine	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1

02-08-2016 to 02-09-2016

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
130.25.126.247	Italy	147.237.77.17	mazi.idf.i	PHP Attempt	Block	6
130.25.126.247	Italy	147.237.77.17	mazi.idf.i	Multiple Admin Blocking from 130.25.126.247	Block	5
130.25.126.247	Italy	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 130.25.126.247	Block	5
66.249.78.254	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	2
41.82.92.179	Senegal	147.237.77.17	mazi.idf.i	E-mail collector robots 14	Block	1
213.8.204.57	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to m.mazi.idf.il/xmlrpc.php	Block	1
166.137.252.32	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/transvideocounter.gif	Block	1
117.78.13.54	China	147.237.77.17	mazi.idf.i	Unauthorized URL Access to igf.idf.il/14-he	Block	1
66.249.78.248	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/4944-he/igf.aspx	Block	1
192.118.12.102	Israel	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on 147.237.77.17/3849-5035-he/igf.aspx	Block	1
91.207.60.64	Ukraine	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/14-he/igf.aspx	Block	1
41.82.92.179	Senegal	147.237.77.17	mazi.idf.i	eMail Hoarding	Block	1
216.72.40.186	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3850-5187-he/igf.aspx	Block	1
176.13.4.97	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/571-he/igf.aspx	Block	1
130.25.126.247	Italy	147.237.77.17	mazi.idf.i	Admin Blocking	Block	1
66.249.78.254	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3848-5183-he/igf.aspx	Block	1
194.90.117.51	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/transvideocounter.gif	Block	1
130.25.126.247	Italy	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/admin/categories.php/login.php	Block	1
104.131.107.95	United States	147.237.77.17	mazi.idf.i	Unauthorized Method HEAD for 147.237.77.17/	Block	1
46.121.229.40	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3849-5035-he/igf.aspx	Block	1
185.25.151.159	Poland	147.237.77.17	mazi.idf.i	Unauthorized URL Access to testp4.pospr.waw.pl/testproxy.php	Block	1
213.8.204.57	Israel	147.237.77.17	mazi.idf.i	PHP Attempt	Block	1
146.185.234.48	Russian Federation	147.237.77.17	mazi.idf.i	Unauthorized URL Access to www.mazi.idf.il/templates/newslist/newslist.in.aspxundefined	Block	1
109.169.67.50	United Kingdom	147.237.77.17	mazi.idf.i	Multiple Malformed URL from 109.169.67.50	Block	1
54.167.183.116	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3848-5222-he/igf.aspx	Block	1
185.89.217.234		147.237.77.17	mazi.idf.i	URL is Above Root Directory mazi.idf.il/../images/1.he/navigation/navigation_arrow.gif	Block	1
79.183.106.164	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3849-5035-he/igf.aspx	Block	1

02-08-2016 to 02-09-2016