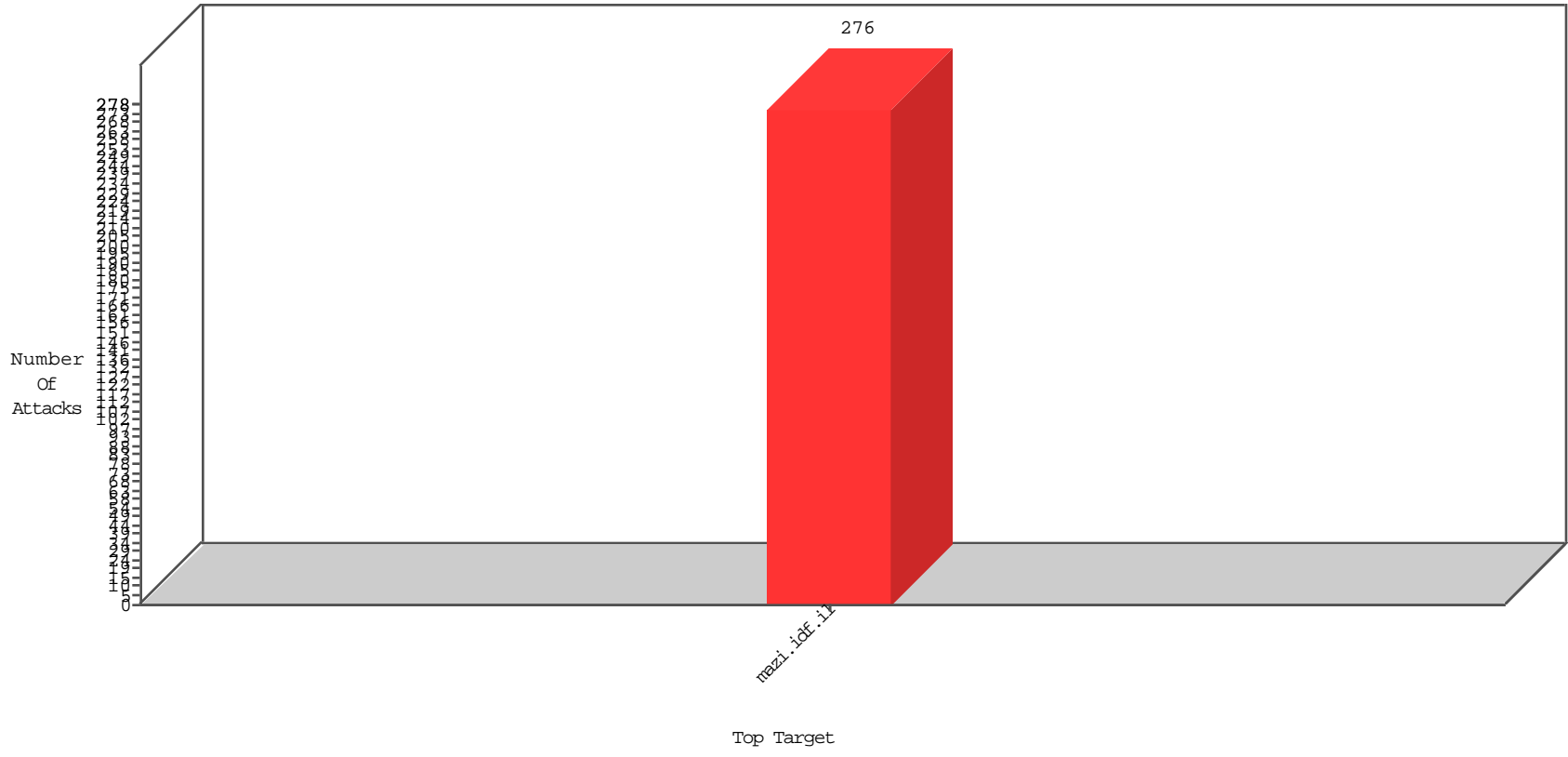


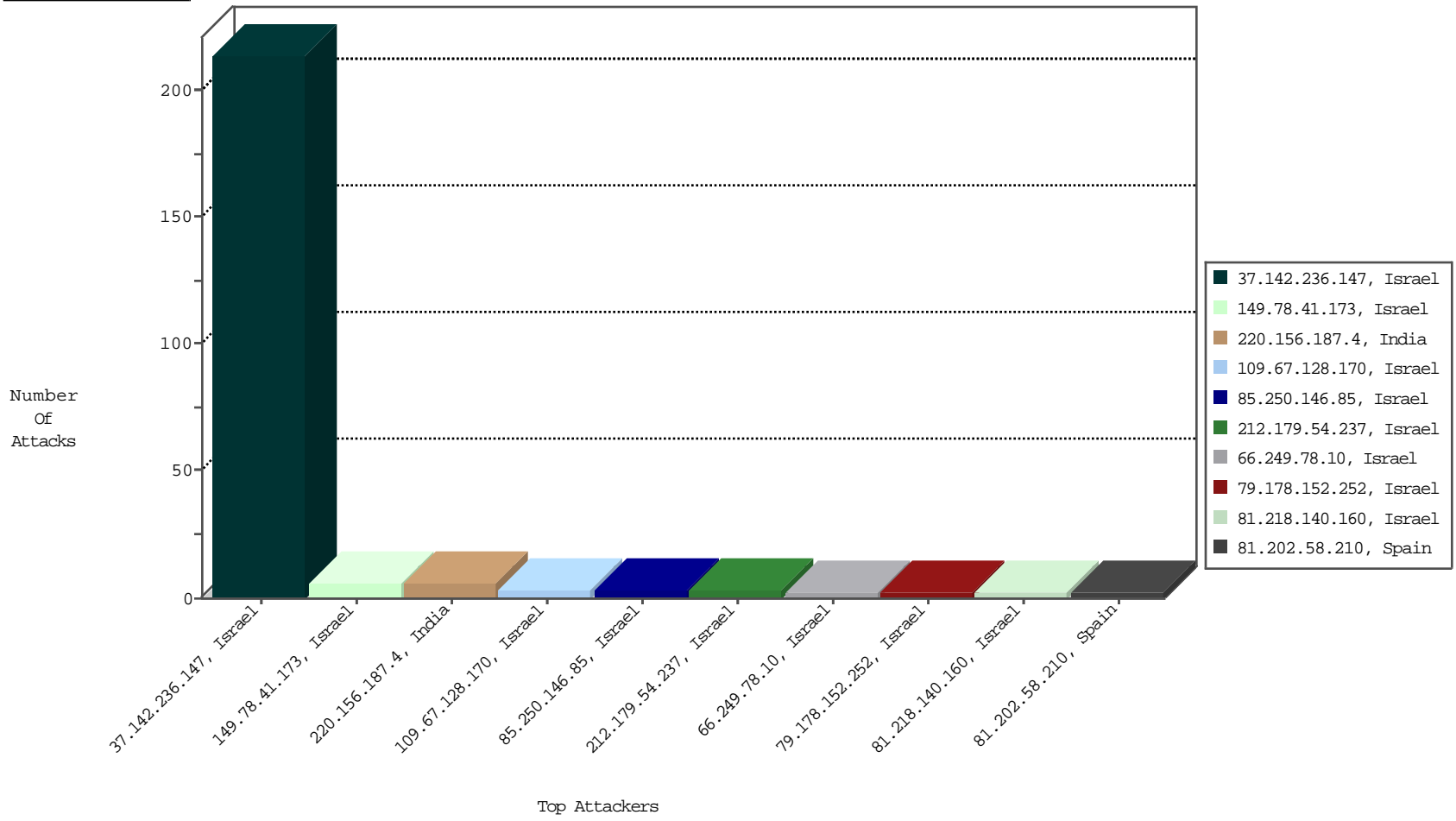
Focused IP Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
37.142.236.147	Israel	147.237.77.17	mazi.idf.il	HTTP-POST-Segmented-DoS	dest-reset	BEL-Israel	214
109.67.128.170	Israel	147.237.77.17	mazi.idf.il	Block_Udp_All_Nets	drop	BEL-Israel	3
212.179.54.237	Israel	147.237.77.17	mazi.idf.il	Block_Udp_All_Nets	drop	BEL-Israel	3
142.54.169.165	United States	147.237.77.17	mazi.idf.il	block-sp-traf1	drop	BEL-Frankfurt	1

01-26-2016 to 01-27-2016

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	6

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
81.202.58.210	Spain	147.237.77.17	mazi.idf.il	ET SCAN Potential SSH Scan	2
59.45.79.117	China	147.237.77.17	mazi.idf.il	ET SCAN Potential SSH Scan	1
82.117.208.243		147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 1024	1
193.104.41.141	Moldova, Republic of	147.237.77.17	mazi.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
185.130.5.235		147.237.77.17	mazi.idf.il	ET SCAN Potential SSH Scan	1
218.246.0.97	China	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 1024	1

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
2.52.52.28	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	36
2.52.128.211	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	36
46.19.85.15	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	26
37.19.121.244	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid sequence number	monitor	16
46.19.85.15	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	13
31.210.187.166	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	12
185.3.147.151	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	10
79.181.49.145	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
212.76.127.111	Israel	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	9
5.29.241.82	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	9
46.19.85.33	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	9
37.142.168.35	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	9
37.26.147.209	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
5.22.130.84	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	9
84.229.32.46	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
109.186.154.182	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
80.82.64.68	Netherlands	147.237.77.17	mazi.idf.i	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	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
37.142.236.147	Israel	147.237.77.17	mazi.idf.i	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	6
46.19.85.219	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.86.113	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	6
37.142.168.35	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	5
213.57.241.199	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.85.242	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.86.43	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.86.159	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.85.180	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.138	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
5.29.241.82	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	4
46.19.86.43	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
51.255.38.230	United Kingdom	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
94.230.86.206	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
123.57.175.207	China	147.237.77.17	mazi.idf.i	drop	SAM rule	drop	2
2.54.156.159	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
46.19.85.219	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
203.133.169.12	Korea, Republic of	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
130.193.51.60	Russian Federation	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
109.186.21.82	Israel	147.237.77.17	mazi.idf.i	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	2
207.46.13.156	United States	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
208.115.111.75	United States	147.237.77.17	mazi.idf.i	drop	SAM rule	drop	2
5.29.21.178	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
184.105.247.211	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.85.150	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
66.249.69.106	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
151.236.221.126	United Kingdom	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.120.103.233	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
37.26.147.209	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.86.138	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
85.130.226.205	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

01-26-2016 to 01-27-2016

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
149.78.41.173	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/newslst/undefined	Block	6
85.250.146.85	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/transvideocounter.gif	Block	3
66.249.79.245	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1
54.173.75.145	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/wp-login.php	Block	1
2.54.12.238	Israel	147.237.77.17	mazi.idf.i	Parameter Type Violation Master\$ucHeader\$ucSearchControl\$txtSearch in www.mazi.idf.il/14-he/igf.aspx	Block	1
164.138.123.181	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/7109-11196-he/igf.aspx&sa=u&ved=0ahukewio1irvnsfkahxl83ikhy01dn0qfggmmai&usg=afqjcnfvehbazc7nq2vi0cfwzqedbzj85w	Block	1
79.178.152.252	Israel	147.237.77.17	mazi.idf.i	Parameter Type Violation pageNumber in mazi.idf.il/forums/templates/forums/forum.aspx	Block	1
66.249.78.168	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to www.mazi.idf.il/templates/general/x"	Block	1
41.33.216.162	Egypt	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/xmlrpc.php	Block	1
146.185.234.48	Russian Federation	147.237.77.17	mazi.idf.i	Unauthorized URL Access to igf.idf.il/templates/newslst/newslst.in.aspxundefined	Block	1
80.82.64.68	Netherlands	147.237.77.17	mazi.idf.i	Unauthorized URL Access to alqassam.ps/arabic/0şÛ„Û?ÛŞÛ`ÛŞÛ^	Block	1
68.180.230.40	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1
66.249.78.10	Israel	147.237.77.17	mazi.idf.i	Parameter Type Violation Back in igf.idf.il/6053-he/igf.aspx	Block	1
2.54.12.238	Israel	147.237.77.17	mazi.idf.i	Parameter Type Violation Master\$ucHeader\$ucSearchControl\$txtSearch in www.mazi.idf.il/6547-he/igf.aspx	Block	1
169.229.3.91	United States	147.237.77.17	mazi.idf.i	Illegal Byte Code Character in Method	Block	1
95.86.103.171	Israel	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 95.86.103.171	Block	1
79.178.152.252	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/ admin	Block	1
66.249.79.231	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3850-5187-he/igf.aspx	Block	1
46.19.85.89	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/4944-he/igf.aspx	Block	1
81.218.140.160	Israel	147.237.77.17	mazi.idf.i	PHP Attempt	Block	1
77.126.62.217	Israel	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on mazi.idf.il/images/transvideocounter.gif	Block	1
66.249.78.10	Israel	147.237.77.17	mazi.idf.i	Parameter Type Violation TabNum in igf.idf.il/3793-he/igf.aspx	Block	1
40.77.167.92	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/sip_storage/files/7/1087.jpg	Block	1
207.46.13.172	United States	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on 147.237.77.17/robots.txt	Block	1
95.86.103.171	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/6368-9571-he/igf.aspx&sa=u&ved=0ahukewjsrtjwnsjkahxgwa4khehzb6uqfggomai&usg=afqjcnfvehbazc7nq2vi0cfwzqedbzj85w	Block	1
79.182.96.48	Israel	147.237.77.17	mazi.idf.i	PHP Attempt	Block	1
66.249.79.239	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/shared/usercontrols/newsgallery/	Block	1
54.173.75.145	United States	147.237.77.17	mazi.idf.i	PHP Attempt	Block	1
157.55.39.13	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/4316-he/	Block	1
81.218.140.160	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to igf.idf.il/xmlrpc.php	Block	1
77.237.138.202	Czech Republic	147.237.77.17	mazi.idf.i	Unauthorized Method HEAD for /	Block	1
66.249.78.17	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to igf.idf.il/templates/shared/usercontrols/newsgallery/	Block	1
41.33.216.162	Egypt	147.237.77.17	mazi.idf.i	PHP Attempt	Block	1
141.212.122.160	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/14-he/igf.aspx	Block	1
79.182.96.48	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to m.mazi.idf.il/xmlrpc.php	Block	1

01-26-2016 to 01-27-2016