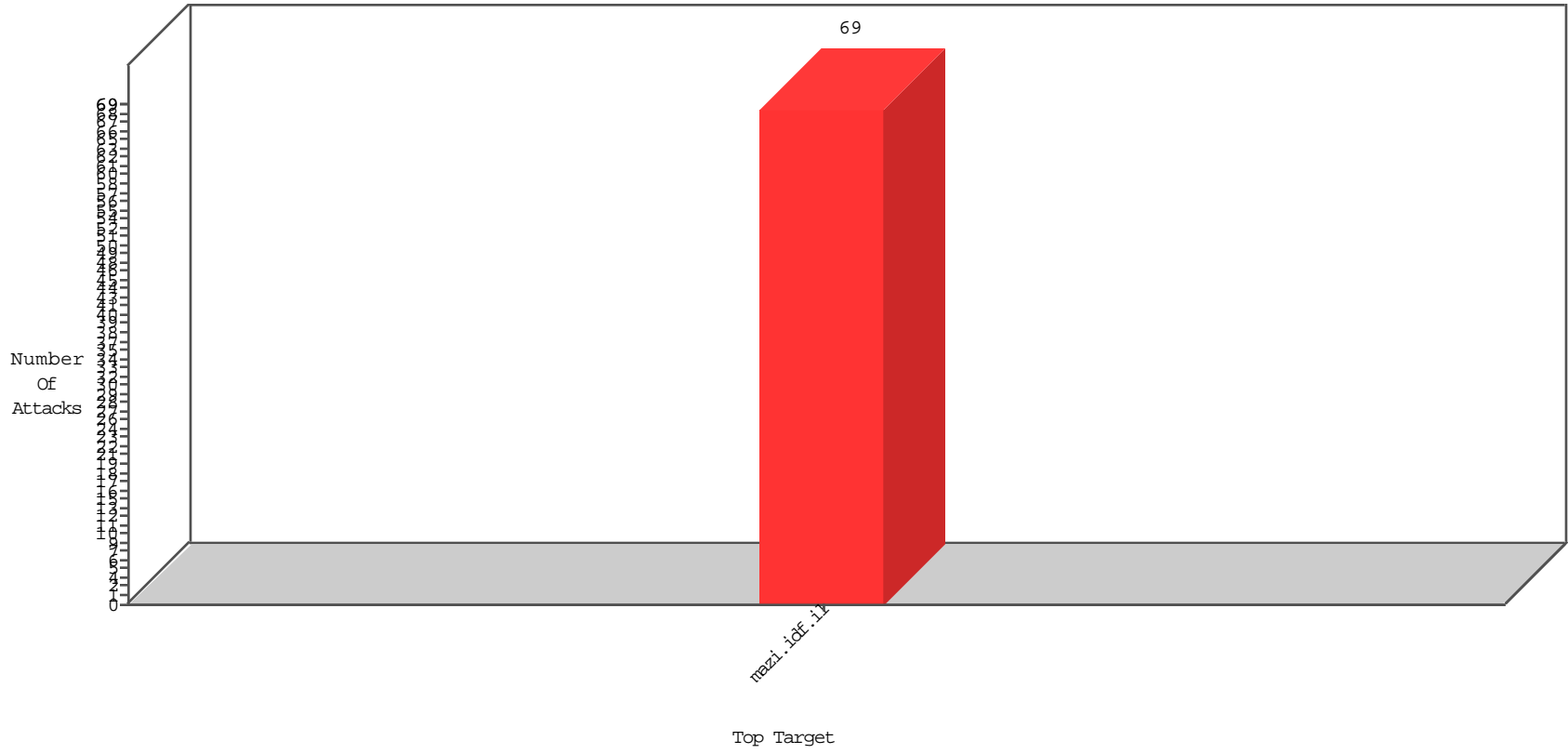


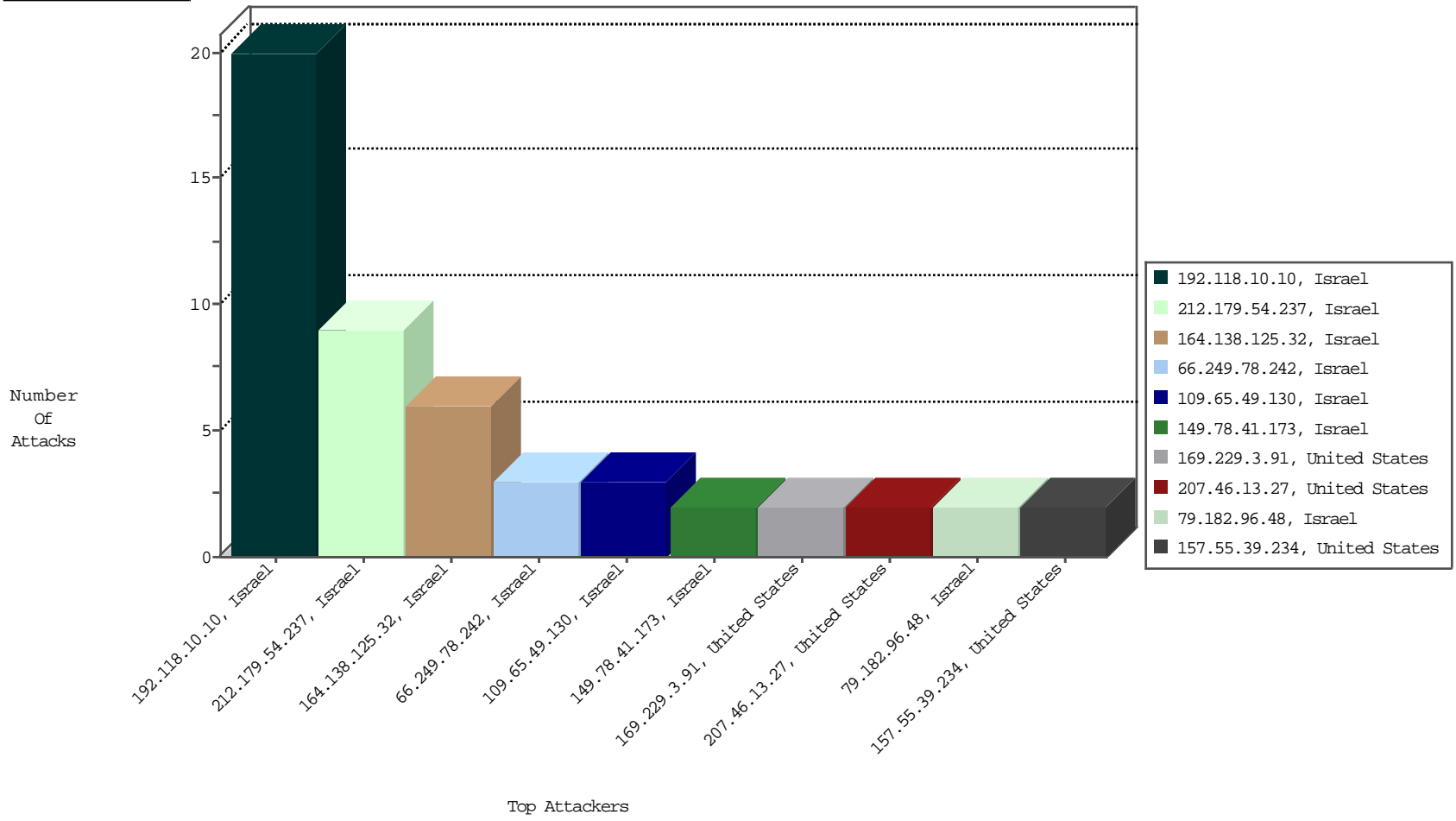
Focused IP Under Attack Daily Report



Top Targets



Top Attackers



01-24-2016 to 01-25-2016

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
212.179.54.237	Israel	147.237.77.17	mazi.idf.il	Block_Udp_All_Nets	drop	BBL-Isreal	9
109.65.49.130	Israel	147.237.77.17	mazi.idf.il	I4 Source or Dest Port Zero	drop	BBL-Isreal	3

01-24-2016 to 01-25-2016

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
------------------	--------------	----------------	------	-----------	---------------	-------

01-24-2016 to 01-25-2016

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
89.248.174.81	Netherlands	147.237.77.17	mazi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
93.174.93.181	Netherlands	147.237.77.17	mazi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
176.195.72.11	Russian Federation	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	225
212.76.127.219	Israel	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	81
188.161.48.7	Palestinian Territory, Occupied	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	62
188.161.48.7	Palestinian Territory, Occupied	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	62
79.180.58.171	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	53
46.19.85.171	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	27
81.218.48.37	Israel	147.237.77.17	mazi.idf.i	drop	SAM rule	drop	22
188.143.232.22	Russian Federation	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	17
37.46.39.124	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	17
84.109.0.29	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	16
176.77.96.48	Russian Federation	147.237.77.17	mazi.idf.i	SYN Attack		reject	16
46.120.206.131	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	16
94.230.86.89	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	16
46.19.85.133	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	14
46.19.85.171	Israel	147.237.77.17	mazi.idf.i	SYN Attack		reject	13
46.19.85.84	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	9
37.46.39.192	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	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
46.117.82.100	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK 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
46.120.206.131	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	9
46.19.85.78	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
213.8.204.28	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
46.19.85.171	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	6
37.26.148.238	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
188.143.232.22	Russian Federation	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
46.19.85.29	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	5
37.46.39.18	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.206	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	4
207.241.237.211	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
37.26.149.145	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence		monitor	4
62.219.153.194	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.117.82.100	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	4
46.19.85.73	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.94	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
85.250.95.204	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
197.214.99.35	Nigeria	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
37.26.149.145	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence		alert	4
46.19.86.138	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.120.103.43	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
37.26.148.238	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
2.52.157.198	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
31.210.187.215	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	3
146.185.234.48	Russian Federation	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
2.54.139.208	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1
141.212.121.192	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.85.19	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
79.179.197.110	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid sequence number	monitor	1
5.29.37.107	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1
169.229.3.91	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
192.118.10.10	Israel	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 192.118.10.10	Block	19
164.138.125.32	Israel	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 164.138.125.32	Block	4
62.219.160.20	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/sip_storage	Block	2
164.138.125.32	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/sip_storage/files	Block	2
157.55.39.234	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	2
149.78.41.173	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/newslist/undefined	Block	2
68.180.228.160	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-8331-he	Block	1
207.46.13.27	United States	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on 147.237.77.17/robots.txt	Block	1
80.246.130.121	Israel	147.237.77.17	mazi.idf.i	Parameter Type Violation phrase in mazi.idf.il/forums/templates/forums/searchresults.aspx	Block	1
66.249.78.242	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3728-6976-he/igf.aspx	Block	1
2.54.184.39	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to igf.idf.il/hi	Block	1
192.117.138.210	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
157.55.39.171	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/599-he/igf.aspx&sa=u&ei=thgitootlm_goikmqslsf&ved=0cbqqfjad&usg=afqjcne_k0jl7d6l9f-7frdrpk8wb6topw	Block	1
79.180.58.171	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3849-5035-he/igf.aspx	Block	1
66.249.65.231	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/14-he/igf.aspx	Block	1
207.46.13.27	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1
85.250.95.204	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3850-5187-he/igf.aspx	Block	1
66.249.78.242	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1
46.35.253.161	Russian Federation	147.237.77.17	mazi.idf.i	Parameter Type Violation TabNum in mazi.idf.il/3793-he/igf.aspx	Block	1
157.55.39.171	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to www.mazi.idf.il/4054-he/igf.aspx&f&A'Ã¢ÄÃ¢ÄÃ¢Ä, -Ã¢ÄÃ¢ÄÃ¢ÄÃ¢ÄÃ¢Ä?	Block	1
79.182.96.48	Israel	147.237.77.17	mazi.idf.i	PHP Attempt	Block	1
66.249.65.231	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/templatecontrols/pictureinfo/pictureinfo.aspx	Block	1
169.229.3.91	United States	147.237.77.17	mazi.idf.i	Abnormally Long Request method	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
66.249.78.254	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3728-9371-he/igf.aspx	Block	1
46.116.202.137	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3850-5216-he/igf.aspx	Block	1
192.118.10.10	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/1.he/lines/menurightcorner.gif	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
66.249.78.242	Israel	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on 147.237.77.17/robots.txt	Block	1
169.229.3.91	United States	147.237.77.17	mazi.idf.i	Illegal Byte Code Character in Method	Block	1