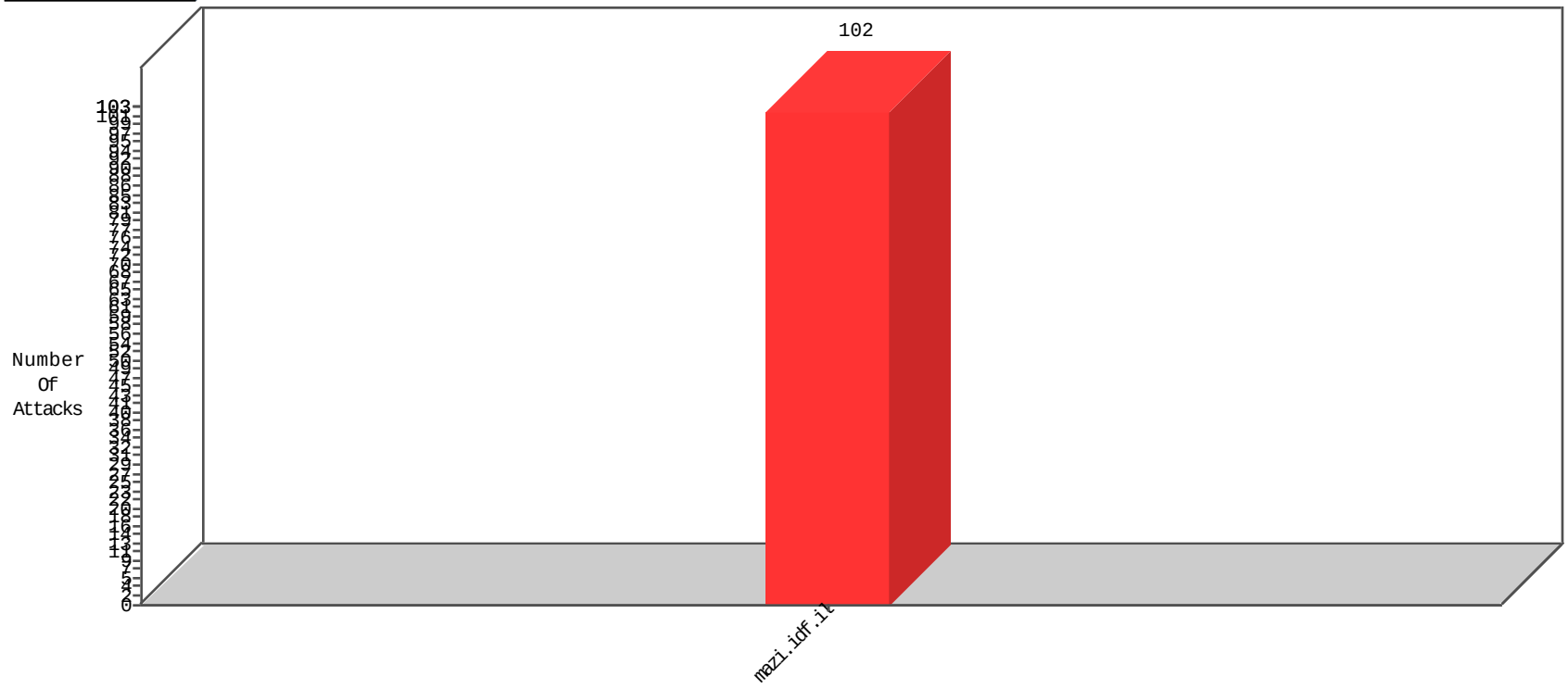
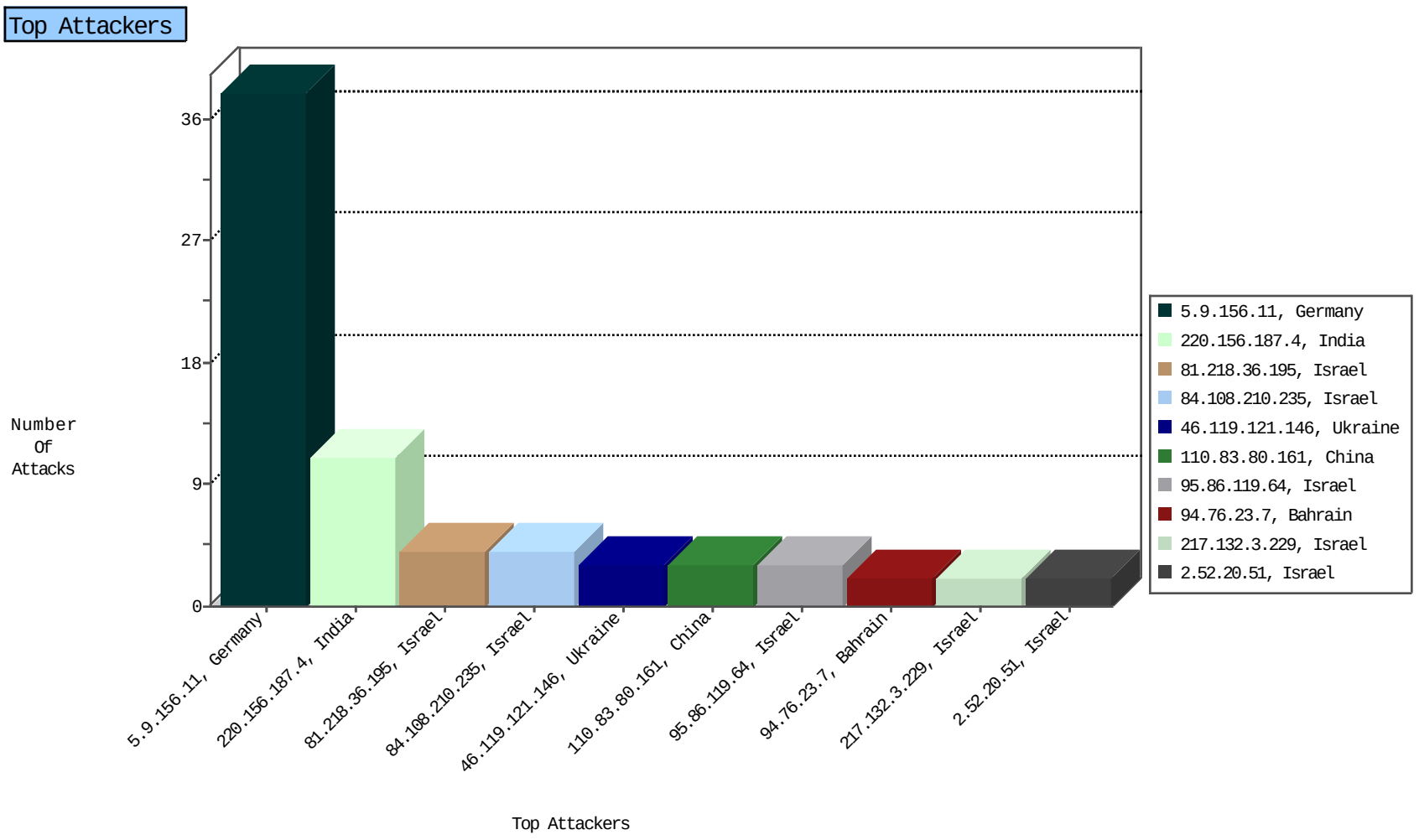
01-28-2016 to 01-29-2016

Focused IP Under Attack Daily Report

Top Targets



Top Attackers



01-28-2016 to 01-29-2016

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count

01-28-2016 to 01-29-2016

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	11
46.119.121.146	Ukraine	147.237.77.17	mazi.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1

01-28-2016 to 01-29-2016

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
94.76.23.7	Bahrain	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 1024	2
94.76.14.46	Bahrain	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 1024	1
119.112.73.226	China	147.237.77.17	mazi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
219.146.12.120	China	147.237.77.17	mazi.idf.il	ET SCAN Potential SSH Scan	1
94.76.11.99	Bahrain	147.237.77.17	mazi.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
172.98.200.238		147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 1024	1

01-28-2016 to 01-29-2016

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	45
37.26.149.209	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	34
208.115.111.75	United States	147.237.77.17	mazi.idf.i	drop	SAM rule	drop	32
208.115.113.91	United States	147.237.77.17	mazi.idf.i	drop	SAM rule	drop	26
79.176.14.69	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	26
46.19.85.90	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	26
46.19.85.90	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	25
85.130.255.129	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	25
217.132.17.247	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	20
5.29.238.42	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	16
130.193.51.60	Russian Federation	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	12
79.127.43.244	Iran, Islamic Republic of	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	10
79.127.43.244	Iran, Islamic Republic of	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	10
149.78.97.135	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	9
149.78.97.135	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	9
213.8.204.9	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
31.210.186.136	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
5.102.254.146	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
212.76.127.111	Israel	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	9
130.193.51.60	Russian Federation	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
5.29.238.42	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	5
85.130.255.129	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	5
2.52.190.227	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	4
85.65.71.175	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
37.26.147.154	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence		monitor	4
79.176.117.225	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
46.19.85.151	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
2.52.190.227	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
85.65.71.175	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	4
79.127.119.140	Iran, Islamic Republic of	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	3
79.127.119.140	Iran, Islamic Republic of	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	3
2.54.143.1	Israel	147.237.77.17	mazi.idf.i	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	2
31.210.186.117	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
2.54.188.172	Israel	147.237.77.17	mazi.idf.i	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	2
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
5.9.156.11	Germany	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
2.54.164.17	Israel	147.237.77.17	mazi.idf.i	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	2
37.142.68.40	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
216.218.206.103	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
82.80.161.65	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
207.46.13.86	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
31.154.94.52	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
180.76.15.149	China	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
5.22.134.225	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
79.127.43.235	Iran, Islamic Republic of	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1
87.68.55.196	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
84.110.208.35	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1
80.74.103.31	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1

01-28-2016 to 01-29-2016

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
5.9.156.11	Germany	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 5.9.156.11	Block	35
84.108.210.235	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/newslist/undefined	Block	4
95.86.119.64	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to m.mazi.idf.il/7322-11795-he/mazi.aspx&sa=u&ved=0ahukewism9hok8zkahwdwhqkhdsibxaqfggdmak&usg=afqjcngb9i08tw3fbb4lqxjmi_tdvhcb7w	Block	2
217.132.3.229	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/sip_storage	Block	2
5.22.131.76	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/newslist/undefined	Block	2
81.218.36.195	Israel	147.237.77.17	mazi.idf.i	Unauthorized HTTP Method	Block	2
2.52.20.51	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/sip_storage	Block	2
110.83.80.161	China	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 110.83.80.161	Block	2
46.119.121.146	Ukraine	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/wp-login.php	Block	1
2.54.166.81	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/sip_storage/files/1/1351.jpg	Block	1
149.78.31.181	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3850-5187-he/igf.aspx	Block	1
79.182.192.75	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to igf.idf.il/xmlrpc.php	Block	1
66.249.78.181	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-4980-he	Block	1
5.9.156.11	Germany	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/7247-11477-he/404.aspx	Block	1
207.46.13.86	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/5013-he/	Block	1
122.152.167.14	Japan	147.237.77.17	mazi.idf.i	Distributed PHP Attempt	Block	1
79.176.114.48	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to www.mazi.idf.il/images/transvideocounter.gif	Block	1
66.249.78.3	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to igf.idf.il/14-8333-he	Block	1
157.55.39.149	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1
109.253.193.178	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/sip_storage	Block	1
81.218.36.195	Israel	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 81.218.36.195	Block	1
66.249.78.181	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/newslist/undefined	Block	1
122.152.167.14	Japan	147.237.77.17	mazi.idf.i	Unauthorized URL Access to igf.idf.il/index.php	Block	1
89.139.0.4	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/571-he/igf.aspx	Block	1
79.176.117.225	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3849-5035-he/igf.aspx	Block	1
66.249.78.131	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/14-he/igf.aspx	Block	1
5.9.156.11	Germany	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-7707-he	Block	1
157.55.39.225	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/700-he/igf.aspx?pagenum=17	Block	1
110.83.80.161	China	147.237.77.17	mazi.idf.i	Multiple Admin Blocking from 110.83.80.161	Block	1
66.249.78.242	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3848-5183-he/igf.aspx	Block	1
217.132.17.247	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3848-5183-he/igf.aspx	Block	1
46.119.121.146	Ukraine	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 igf.idf.il/templates/newslist/newslist.in.aspxundefined	Block	1
95.86.119.64	Israel	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 95.86.119.64	Block	1
79.182.192.75	Israel	147.237.77.17	mazi.idf.i	PHP Attempt	Block	1
66.249.78.167	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/newslist/undefined	Block	1
5.9.156.11	Germany	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-8330-he	Block	1
194.9.253.237	United Kingdom	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3849-5039-he/igf.aspx	Block	1
81.218.36.195	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/sip_storage/files/5/	Block	1
66.249.78.254	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1

01-28-2016 to 01-29-2016