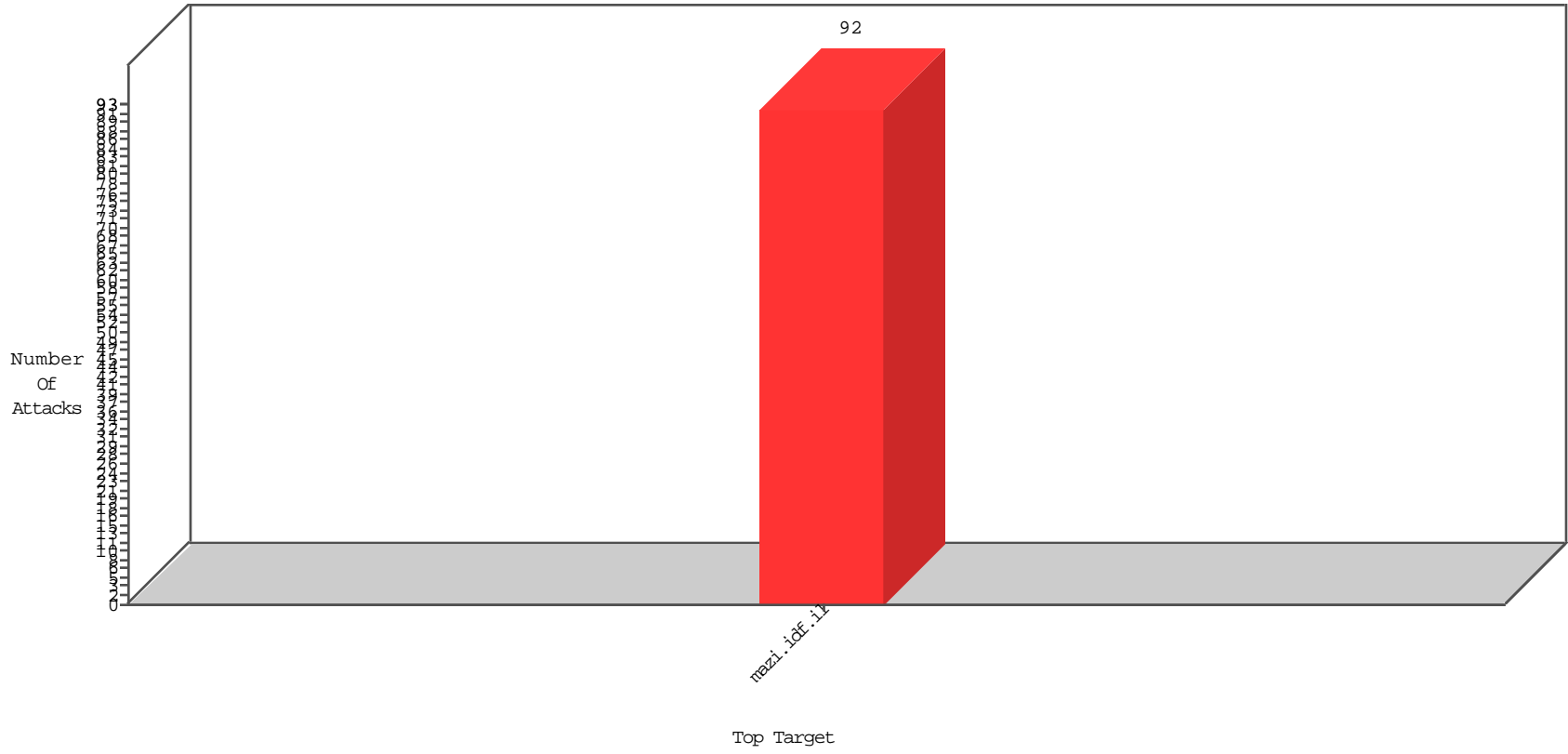


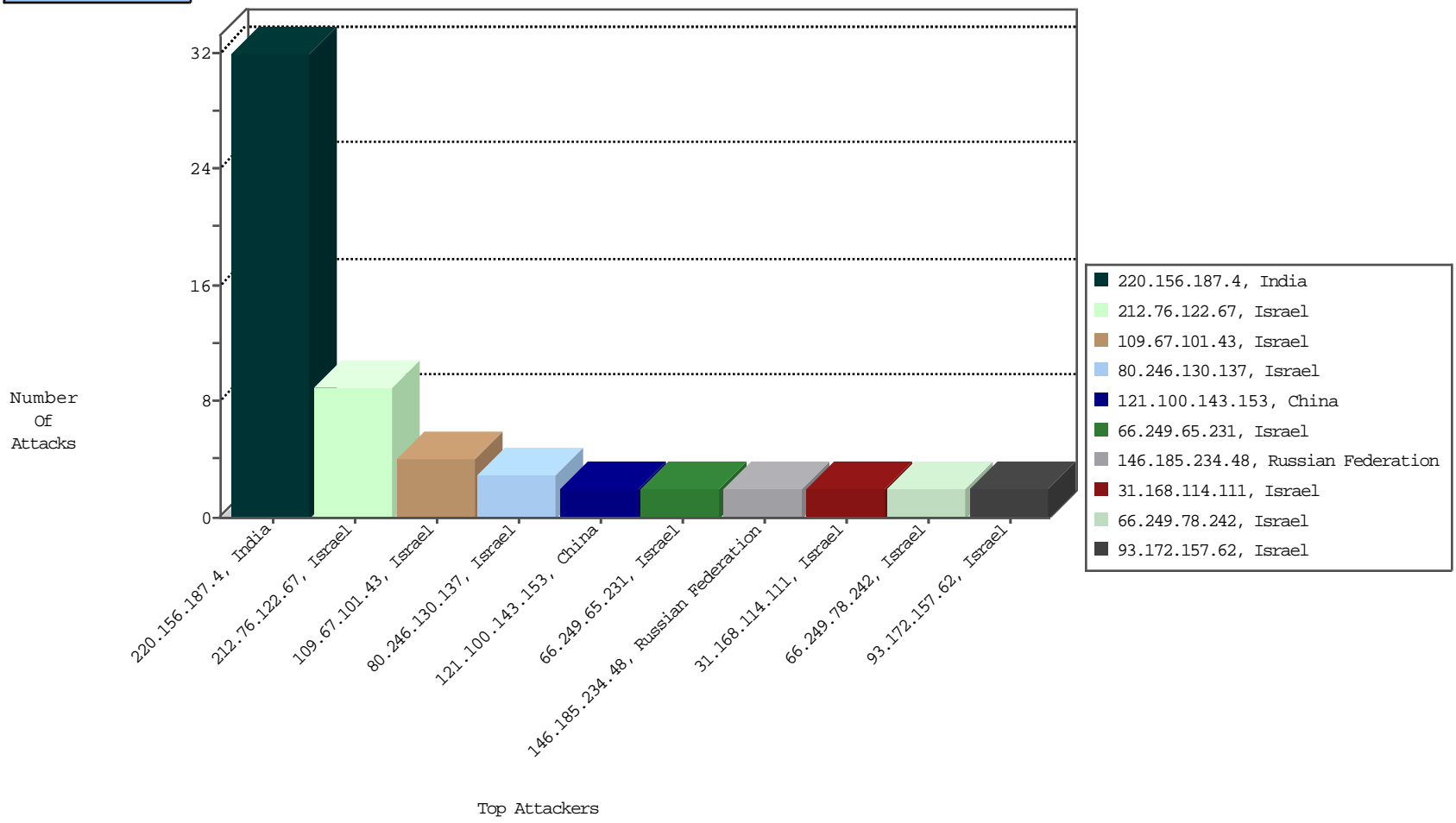
Focused IP Under Attack Daily Report



Top Targets



Top Attackers



02-04-2016 to 02-05-2016

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
54.67.38.74	United States	147.237.77.17	mazi.idf.il	DOS-httpd-hrequest-FS	dest-reset	BBL-Frankfurt	1
142.54.160.213	United States	147.237.77.17	mazi.idf.il	block-sp-trafl	drop	BBL-Frankfurt	1

02-04-2016 to 02-05-2016

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	32
121.100.143.153	China	147.237.77.17	mazi.idf.il	22280: HTTP: Joomla Object Injection Vulnerability	Block	2

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
61.240.144.67	China	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 1024	1
180.97.106.161	China	147.237.77.17	mazi.idf.il	ET SCAN Potential SSH Scan	1
194.44.19.210	Ukraine	147.237.77.17	mazi.idf.il	ET SCAN Potential SSH Scan	1
128.199.58.141	Singapore	147.237.77.17	mazi.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
185.112.81.67		147.237.77.17	mazi.idf.il	ET SCAN Potential SSH Scan	1
209.126.116.147	United States	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
5.29.68.221	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	96
2.52.133.2	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	81
212.76.127.10	Israel	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	59
212.76.127.219	Israel	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	45
46.19.85.103	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	36
46.19.85.103	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	36
46.19.85.209	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	25
176.228.76.25	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	18
84.94.74.185	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	16
109.186.163.111	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	16
5.102.254.99	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	14
37.46.39.167	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	12
46.117.80.182	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	10
84.94.74.185	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	9
84.108.83.27	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
109.186.163.111	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	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
5.102.254.134	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	9
46.19.85.14	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
77.127.32.63	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
5.102.254.60	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	5
93.172.157.62	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
31.210.187.172	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	5
46.117.80.182	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	5
94.230.86.174	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	5
79.179.52.248	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
37.26.147.148	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.61	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
149.78.219.19	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.85.72	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	4
37.46.39.209	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
31.210.188.25	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
87.69.123.41	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
46.19.85.22	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.212	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.72	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
192.243.55.133	Dominica	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
79.179.52.248	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
37.26.147.148	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	4
89.138.120.7	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
217.132.98.28	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
192.243.55.135	Dominica	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
2.54.3.7	Israel	147.237.77.17	mazi.idf.i	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	2
2.54.11.34	Israel	147.237.77.17	mazi.idf.i	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	2
79.181.213.106	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	2
2.52.9.191	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
79.179.52.248	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
2.54.38.47	Israel	147.237.77.17	mazi.idf.i	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	2
213.57.133.213	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	2

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
212.76.122.67	Israel	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on mazi.idf.il/images/transvideocounter.gif	Block	9
109.67.101.43	Israel	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on mazi.idf.il/images/transvideocounter.gif	Block	4
80.246.130.137	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to m.mazi.idf.il/7343-11581-he/xæxæx? x'x'x*xæx*x^a.aspx	Block	3
46.120.116.55	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/newslit/undefined	Block	2
87.68.77.242	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/transvideocounter.gif	Block	2
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
37.26.148.186	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/sip_storage/files/1/2061.jpg	Block	1
192.243.55.135	Dominica	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-8330-he	Block	1
93.172.157.62	Israel	147.237.77.17	mazi.idf.i	Parameter Type Violation Master\$ucHeader\$ucSearchControl\$txtSearch in mazi.idf.il/683-he/igf.aspx	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
66.249.65.238	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/5013-he/igf.aspx	Block	1
2.52.40.155	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/resource/userfollowresource/create/	Block	1
149.78.105.168	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3849-5035-he/igf.aspx	Block	1
66.249.78.242	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/591-he/igf.aspx	Block	1
192.243.55.136	Dominica	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-5475-he	Block	1
77.127.32.63	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3849-5035-he/igf.aspx	Block	1
66.249.65.245	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/692-he/igf.aspx	Block	1
213.8.204.78	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/transvideocounter.gif	Block	1
31.168.114.111	Israel	147.237.77.17	mazi.idf.i	PHP Attempt	Block	1
176.228.76.25	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3850-5187-he/igf.aspx	Block	1
66.249.78.248	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/113-he/igf.aspx	Block	1
66.249.65.231	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/41-he/igf.aspx	Block	1
192.243.55.137	Dominica	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/shared/usercontrols/vodchannel/	Block	1
146.185.234.48	Russian Federation	147.237.77.17	mazi.idf.i	Unauthorized URL Access to igf.idf.il/templates/newslit/newslit.in.aspxundefined	Block	1
79.178.175.1	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/4146-he/igf.aspx	Block	1
66.249.78.167	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/shared/usercontrols/vodchannel/	Block	1
217.132.51.233	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/4944-he/igf.aspx	Block	1
31.168.114.111	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to m.mazi.idf.il/xmlrpc.php	Block	1
192.243.55.131	Dominica	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-8331-he	Block	1
93.172.157.62	Israel	147.237.77.17	mazi.idf.i	Parameter Type Violation Master\$ucHeader\$ucSearchControl\$txtSearch in mazi.idf.il/4150-he/igf.aspx	Block	1
66.249.78.254	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/671-he/igf.aspx	Block	1
66.249.65.231	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/675-he/igf.aspx	Block	1
199.203.215.1	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/sip_storage/files/1/1351.jpg	Block	1
146.185.234.48	Russian Federation	147.237.77.17	mazi.idf.i	Unauthorized URL Access to www.mazi.idf.il/templates/newslit/newslit.in.aspxundefined	Block	1
79.181.213.106	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/sip_storage/files/1/1351.jpg	Block	1