\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\* \*

\* | |\_| |\_\_ \_\_\_ /\ /\\_\_ \_ \_ \_\_\_\_ \_\_\_\_\_ \_\_\_| |\_ \_\_\_ \_ \_\_ \*

\* | \_\_| '\_ \ / \_ \ / /\_/ / \_` | '\_\_\ \ / / \_ \/ \_\_| \_\_/ \_ \ '\_\_| \*

\* | |\_| | | | \_\_/ / \_\_ / (\_| | | \ V / \_\_/\\_\_ \ || \_\_/ | \*

\* \\_\_|\_| |\_|\\_\_\_| \/ /\_/ \\_\_,\_|\_| \\_/ \\_\_\_||\_\_\_/\\_\_\\_\_\_|\_| \*

\* \*

\* TheHarvester Ver. 2.7 \*

\*编码由Christian Martorella 提供 \*

\* Edge-Security Research \*

\* cmartorella@edge-security.com \*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

用法: theharvester 选项

-d: 查找域名，和公司名称

-b: 数据源: google, googleCSE, bing, bingapi, pgp, linkedin,

google-profiles, jigsaw, twitter, googleplus, all

-s: 在结果号为X中开始 (默认是 ：0)

-v: 验证通过DNS解析主机名和虚拟主机搜索

-f: 结果保存为HTML和XML文件（都）

-n: 执行DNS反向查询所有范围的发现

-c: 执行一个域名DNS的蛮力

-t: 执行DNS TLD扩展发现

-e: 使用此DNS服务器

-l: 限制与工作结果的数量(bing goes from 50 to 50 results,

google 100 to 100, and pgp doesn't use this option)

-h: 使用SHODAN 数据库来访问 发现的主机

例如:

theharvester -d microsoft.com -l 500 -b google -h myresults.html

theharvester -d microsoft.com -b pgp

theharvester -d microsoft -l 200 -b linkedin

theharvester -d apple.com -b googleCSE -l 500 -s 300