

什么是拖库和撞库？

如题

- 关注问题
- 写回答
- 邀请回答
- 添加评论
- 分享
-

4 个回答

默认排序

知道创宇 云安全
已认证的官方帐号

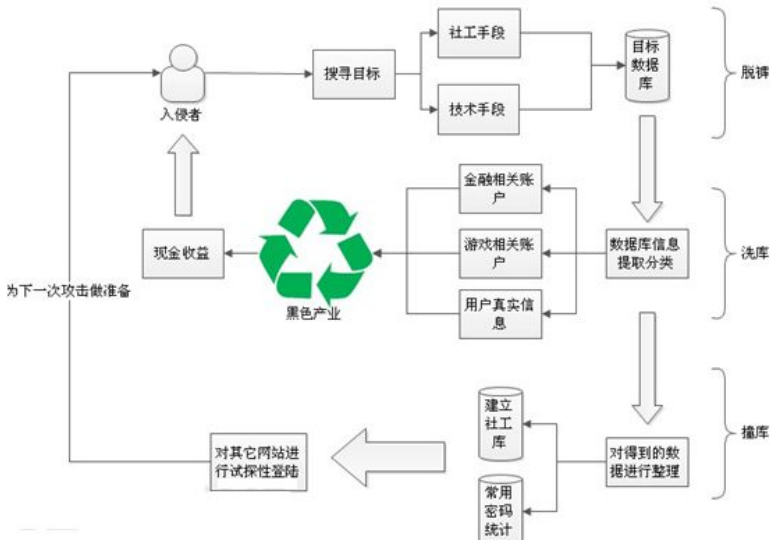
28 人赞同了该回答

先让我们先来看一下相关的名词~

- **拖库**：本来是数据库领域的专用语，指从数据库中导出数据。而现在它被用来指网站遭到入侵后，黑客窃取数据库的行为。
- **撞库**：使用大量的一个网站的账号密码，去另一个网站尝试登陆。
- **洗库**：黑客入侵网站在取得大量的用户数据之后，通过一系列的技术手段和黑色产业链将有价值的用户数据变现。
- **社工库**：黑客将获取的各种数据库关联起来，对用户进行全方位画像。

而这些“库”再联合撞库就可以形成一个黑色产业链：

黑客入侵A网站后对网站拖库，拿到的数据可以存到自己的社工库里，也可以直接洗库变现。拿到的这部分数据再去B网站尝试登陆，而这就可以称之为是撞库。撞库后的数据可以继续存入社工库，或是洗库变现，以此循环...



但通常用来撞库的数据非常庞大，这些数据怎么来？

- 黑市上购买
- 同行之间的交换
- 网站被黑客攻击后泄漏
- ...

那么如何避免撞库？

选择创宇盾为网站进行防护~创宇盾每天为90万个网站提供服务，强大的防御能力，帮助企业轻松应对撞库等安全问题。





我是网络安全公司知道创宇~如果你想获取**创宇盾**或**相关产品的白皮书**，欢迎添加微信好友kcsc818。

欢迎访问我们：

创宇盾

知道创宇云安全

编辑于 2019-05-22



遛弯的虫子
可能性！

6 人赞同了该回答

泻药

拖库，是把一个网站的数据库拖回来，就是把数据导出保存

撞库，是用拖回来的用户数据去尝试登陆别的网站，撞上就撞上了，撞不上拉倒

一般都是先从小规模漏洞大的网站拖，然后用拿到的数据去大网站比如支付宝腾讯这种网站撞最后，这些做法都不是传统最早定义的黑客们干的事情。

发布于 2016-02-02

▲ 赞同 6 ▼ ● 2 条评论 ➦ 分享 ★ 收藏 ♥ 感谢



腾讯安全联合实验室 ✓
已认证的官方帐号

6 人赞同了该回答

拖库这个行为现在已经被黑产黑化了，说到拖库，马上就能联想到黑产。谁能想到，人家原来可是正经操作。



这就是骄傲吧

拖库本来是数据库领域的术语，指从数据库中导出数据。原本这么单纯的事，在不法黑客多次攻击事件之后，被用来指不法黑客入侵有价值的网络站点，把注册用户的资料数据库全部盗走的行为。



骄傲过头

▲ 赞同 28 ▼ ● 1 条评论 ➦ 分享 ★ 收藏 ♥ 感谢 收起 ^





第一，不法黑客对目标网站进行扫描，查找其存在的漏洞，常见漏洞包括SQL注入、文件上传漏洞等；

第二，通过该漏洞在网站服务器上建立“后门(webshell)”，通过该后门获取服务器操作系统的权限；

第三，利用系统权限直接下载备份数据库，或查找数据库链接，将其导出到本地。

不法黑客完成拖库后，通常下一步就是撞库。

撞库是不法黑客通过收集互联网已泄露的用户和密码信息，生成对应的字典表，尝试批量登陆其他网站后，得到一系列可以登录的用户账号和密码。很多用户在不同网站使用的是相同的帐号密码，因此，不法黑客可以通过获取用户在A网站的账户从而尝试登录B网址，这就可以理解为撞库攻击。

部分网民习惯为邮箱、网上支付、购物等帐号设置相同密码，一旦数据泄露，任何人都可以拿着密码去各个网站尝试登录，对一些敏感的金融行业是致命的危害，对普通用户可能造成财产损失及个人隐私泄露，后果不堪设想。



喝几瓶风油精冷静下。

如何防止拖库？

第一，分级管理密码，重要帐号（如常用邮箱、网上支付、聊天帐号等）单独设置密码；

第二，定期修改密码，可有效避免网站数据库泄露影响到自身帐号；

第三，工作邮箱不用于注册网络帐号，以免密码泄露后危及企业信息安全；

第四，不让电脑“自动保存密码”，不随意在第三方网站输入帐号和密码。即便是个人电脑，也要定期在所有已登录站点手动强制注销进行安全退出；

第五，商家对网站数据库进行加密保护，并进行网站漏洞检测、网站挂马实时监控、网站篡改实时监控。






了解了拖库和撞库之后，你是不是想马上修改密码？记得密码里不要包含姓名、生日、手机号和身份证号哦。

更多腾讯安全联合实验室官方精品回答：

- 1、[黑客可以厉害到什么程度？](#)
- 2、[外界对于黑客都存在哪些误解？](#)
- 3、[身边有个黑客朋友是怎样的体验？](#)
- 4、[黑客黑产里的五件套都是什么？](#)
- 5、[有哪些有趣的电脑病毒？](#)
- 6、[个人信息的泄露在今天已经严重到了什么地步？对普通人的生活有多大的影响？](#)
- 7、[你平时如何维护电脑，保证电脑使用安全和安全上网？](#)
- 8、[电脑病毒能破坏硬件吗？](#)

编辑于 2018-06-27

▲ 赞同 6 ▼ ● 添加评论 ➦ 分享 ★ 收藏 ♥ 感谢 收起 ^

 **ZhetaoL**
努力不一定会成功，但是，不努力就一定很舒服。

撞库是黑客最常用的窃取个人信息的手法

近年来，大规模的个人身份泄漏已经发生多起

个人信息安全问题已经刻不容缓

那什么是撞库呢？

weixin.qq.com/r/Lki0rOP... (二维码自动识别)

编辑于 2018-08-15

▲ 赞同 ▼ ● 添加评论 ➦ 分享 ★ 收藏 ♥ 感谢 收起 ^

 写回答

▲ 赞同 28 ▼ ● 1 条评论 ➦ 分享 ★ 收藏 ♥ 感谢 收起 ^

