Windows 8 stores logon passwords in plain-text

Passcape Software

内容

1 Windows 8 stores logon passwords in plain-text

在我们之前的一篇文章中，你可以了解到在 Windows中恢复文本密码的方法 ，而不需要对其进行暴力攻击，以及系统中可能存在的文本密码的位置和用于恢复的工具。事实证明，Windows 8的发布也不是没有另一个苍蝇在里面。我们的专家在两种新的登录系统的方式中发现了一个严重的缺陷。我们正在谈论 图片密码 和PIN码。.

问题是，这两种认证方法是基于普通用户账户的。换句话说，用户必须先用普通密码创建一个账户，然后再选择性地切换到PIN或图片密码认证。值得注意的是，账户的原始纯文本（！）密码也保留在系统中。

一旦用户切换到新的认证方式，他的文本密码将使用AES算法进行加密，并保存在以下文件夹中受保护的Vault存储中：

%SYSTEM_DIR%/config/systemprofile/AppData/Local/Microsoft/Vault/4BF4C442-9B8A-41A0-B380-DD4A704DDB28

这个系统文件夹包含了带有SID的Vault记录和所有激活PIN或图片密码认证的用户的文字密码。文本密码不与PIN或图片密码绑定；因此，任何具有管理员权限的个人电脑用户都可以轻松恢复它（加密密钥由系统 DPAPI 保护）。

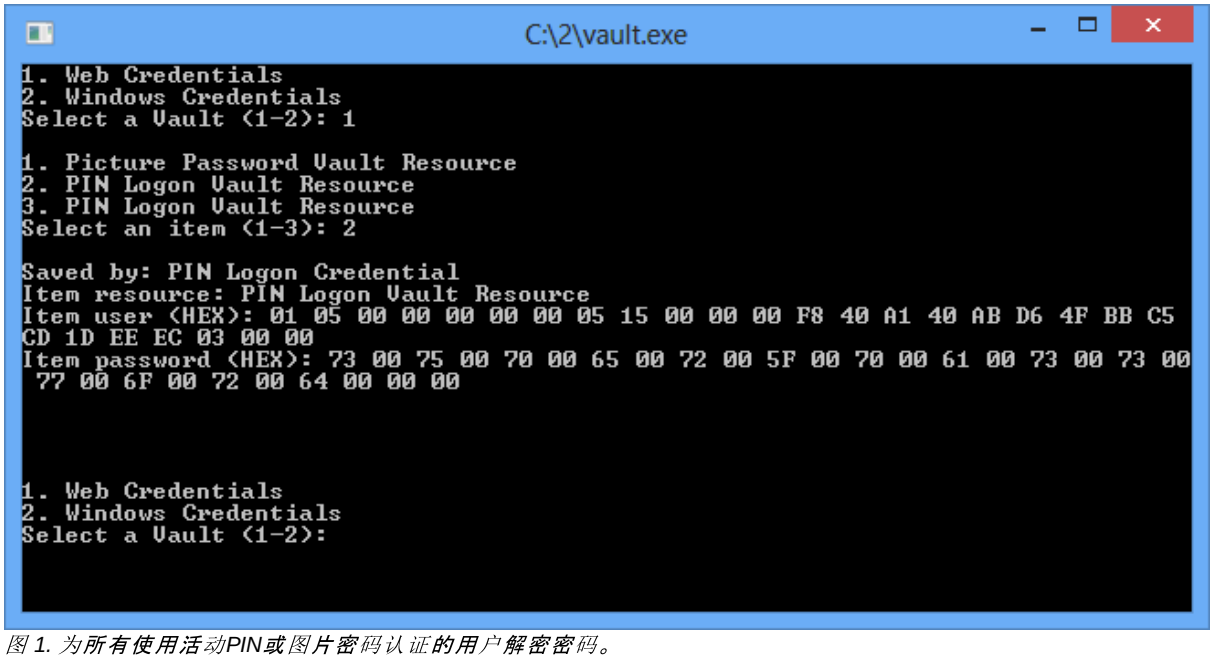

图 1. 为所有使用活动PIN或图片密码认证的用户解密密码。

简而言之，Vault可以被描述为用户私人数据的保护性存储。Windows Vault是随着Windows 7的发布而出现的，可以存储各种网络密码。在Windows 8中，Vault扩展了它的功能；它已成为一个更通用的存储，但同时也失去了与以前版本的兼容性。因此，"老 "Vault实现了自定义密码保护。而在Windows 8中，似乎这个功能被冻结了，它只使用基于DPAPI的保护。Windows Vault也被其他应用程序所使用。例如，Internet Explorer 10使用它来存储网站的密码。

我们的一些 密码恢复工具 已经实现了Windows 8纯文本密码解密。即将发布的Windows密码恢复工具预计将有一个成熟的金库分析器和离线解码器。

图片密码和PIN码是Windows 8中全新的认证方法，是摆脱密码记忆地狱的尝试。然而，使用它们时要小心谨慎。如果一个账户被配置为使用图片密码或PIN进行认证，你的原始纯文本密码就会被存储在系统中，任何具有管理员权限的用户都可以获得它。