Internet Explorer 10中的密码加密

Passcape Software

内容

1 Internet Explorer 10中的密码加密

关于即将发布的Windows 8和Internet Explorer 10，我们开始收到更多关于在新版本的Internet Explorer中存储密码的安全问题。因此，我们决定在我们的博客中对这一问题给予关注。

我们曾多次表示，新版IE浏览器的密码保护会更糟糕，因为存储密码的机制已经改变。为什么新的保护算法会变得更加脆弱？让我们来弄清楚。

Internet Explorer 7-9中的网站密码被存储在注册表中 并用用户的 DPAPI 进行加密。但这种保护是以一种非常巧妙的方式实现的；加密密钥是由源URL地址组成的。之后，该网站的URL就从系统中被抹去了。

让我们考虑一个例子，使之更清楚一些。例如，你打开了某个网站，在上面注册，输入了你的密码并保存了它（或启用了自动保存密码的设置）。对于加密密钥，它使用网页的原始URL。然后，加密的密码被写入注册表，而访问该URL的记录则从系统中删除。

因此，注册表存储了加密的密码，但它并没有解密的密钥！ 只有当我们知道原始网站的URL时，即再次访问该资源时，我们才能得到加密密钥。如果一个潜在的入侵者从注册表中窃取了加密的密码，他将无法解密（有所有其他限制），直到他得到记录所属的原始网站的URL。

相当聪明和狡猾，但这种算法并没有被微软申请专利，因此，一定有其他人已经使用过了 :) 无论如何，这已经不重要了，因为IE 10使用了不同的机制。所有IE 10的密码现在都存储在Windows Vault中，用常规的DPAPI保护，并且可以很容易地恢复。至少，比前三个版本更容易。Windows Vault 是一种新的私人数据存储机制，这在Windows中是非常缺乏的。

不幸的是，与Windows 7中使用的前一个版本相比，Windows 8中的Vault的功能有所减少。一个Vault用户的所有私人条目都可以在他的个人资料中找到。默认情况下，这就是文件夹

C:\Users\<USER_NAME>\AppData\Local\Microsoft\Vault\<VAULT_UID>
where **<USER_NAME>** - the user name
<VAULT_UID> - Vault identifier. By default, **4BF4C442-9B8A-41A0-B380-DD4A704DDB28**.

每个IE10密码条目都由一个扩展名为.vcrd（Vault Credential）的文件呈现；加密密钥则存储在同一文件夹中。

新版本的 Internet Explorer Password Recovery 可以在在线和离线模式下解密Internet Explorer 10的密码。也就是说，即使在无法启动的电脑上，你也能恢复IE密码。IE 10的当前登录用户的密码被立即解密，没有任何限制或约束。

因此，Internet Explorer 10的密码保护只是另一块蛋糕。密码大约可以像谷歌浏览器的密码一样容易被解密。完美是优秀的敌人