

## Android恶意软件偷取Uber凭证

 [secist](#)

2018-01-11 共82637人围观，发现 1 个不明物体

数据安全

系统安全

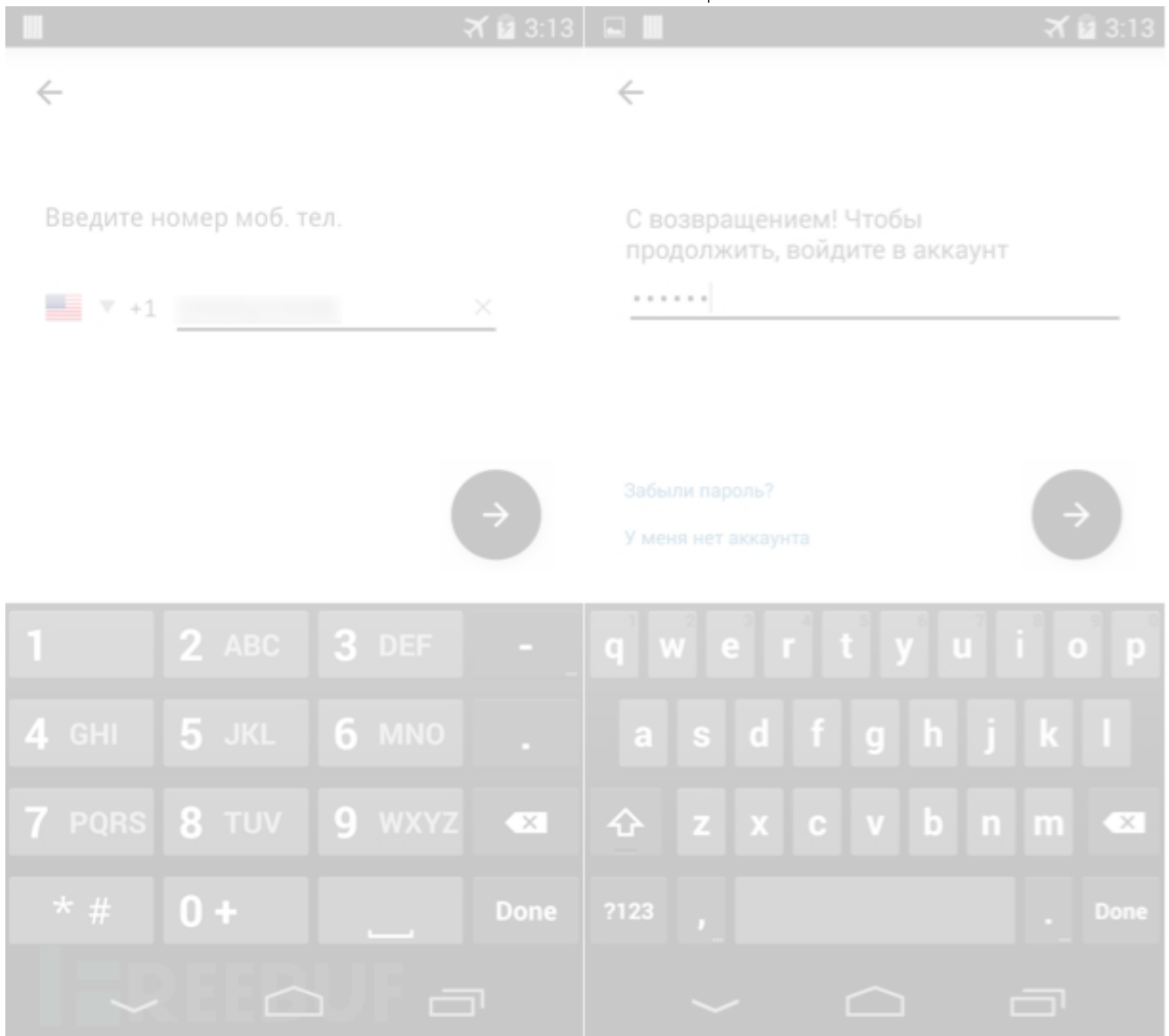
近期，一种新的Android恶意软件变种Android.Fakeapp被研究人员所披露。据了解该Android恶意软件主要目标是取Uber用户的凭证信息，然后使用合法的Uber app的深层链接来隐瞒真相。

在分析最新的Android.Fakeapp恶意软件变种时，一个样本引起了我们的关注。该样本使用了一种相当新颖和不同的技术手段，要求用户输入他们的信用卡详细信息。要知道Android用户数量在全球数以百万计，这对于使用Uber的安卓手机用户来说尤其值得关注！

此外经过我们进一步的分析发现，该Fakeapp变体有一个欺骗性的Uber app用户界面（UI），它会定期的在用户的设备上弹出，直到用户被诱骗输入其Uber ID（通常是注册的电话号码）和密码。

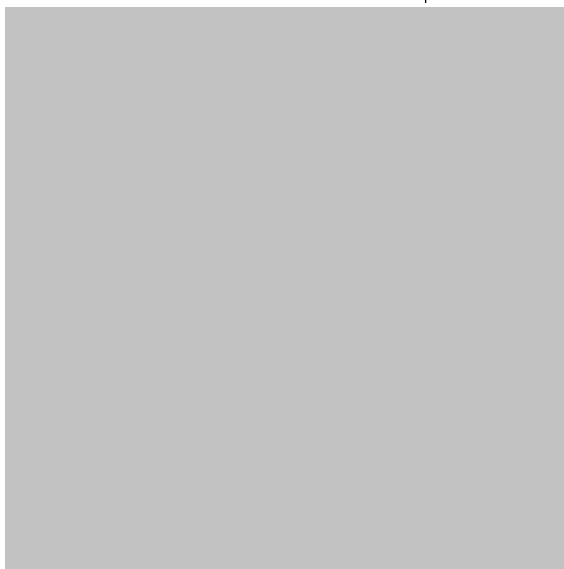
图1为该恶意软件弹出的假Uber app UI，用于欺骗用户输入其详细信息。一旦用户根据提示输入相关内容并点击“下一步”按钮（->），恶意软件则会将用户ID和密码发送到其远程服务器上。





接着，为了避免引起用户的注意，恶意软件会跳转回应用程序的合法界面并显示用户的当前位置，这么做通常不会起用户的怀疑。

这也是该Fakeapp变体非常具有创造性的地方。为了显示所述界面，恶意软件使用合法app的深层链接发起app的Rid Request，将受害者的当前位置作为预加载点。



深层链接是将用户直接带到应用中特定内容的网址。Android中的深层链接是识别应用程序内部特定内容或功能的一种方式。

但对于应用程序来说，这像是一个web URL。例如，Uber app的Ride Request活动具有以下深层链接URI：

```
uber://?action=setPickup&pickup=my_location
```

图3展示了恶意软件的部分代码片段，这个恶意软件在将Uber凭证发送给其远程服务器之后，会使用Ride Request深层链接URI来触发VIEW intent。





这个案例再次表明了恶意软件作者，正不断的创新和改进其欺骗和窃取技术，也为我们普通用户的移动应用安全问题再次敲响了警钟！‘

## 安全建议

赛门铁克建议用户遵循以下最佳安全实践，以防止移动安全威胁：

第一时间更新或升级应用程序的最新版本

避免从不熟悉的网站下载应用程序，只安装来自可信来源的应用程序

密切关注应用程序的相关请求权限

安装一个合适的移动安全应用程序，如[Norton](#)，以保护您的设备和数据安全

定时对重要的数据进行备份



上一篇：[从一道CTF题目看Gopher攻击MySQL](#)

下一篇：[开源安全情报引擎Critical Stack使用入门](#)

已有 1 条评论

死宅10086 (7级) 这家伙太懒了，还未填写个人描述！ 2018-01-11 1楼 [回](#)

666 🍷

亮了

选择文件

未选择任何文件

昵称

必须 您当前尚未登录。[登陆?](#) [注册](#)

请输入昵称

邮箱

必须 (保密)

请输入邮箱地址

表情

插图

提交评论(Ctrl+Enter) [取消](#) ☒ 有人回复时邮件通知我



[secist](#)

每个人的心中都有一个梦。。

105

文章数

42

评论数

最近文章

针对NFS的渗透测试

- [Android恶意软件偷取Uber凭证](#)

2018.01.11

- [用Golang写的域名信息搜集工具](#)

2018.01.08

[浏览更多](#)

## 相关阅读

[Uber修复三个漏洞，白帽子获数千美...](#)[年度盘点 | 2017年最严重的七大数据泄...](#)[挖洞经验 | 看我如何通过子域名接管绕...](#)[Uber平台现身份认证漏洞，利用漏洞...](#)[Android恶意软件又出新招：伪装Googl...](#)


## 特别推荐



<a href="#">willhuang</a>	2017-10-21	<a href="#">毒舌评论砖家</a>	2015-06-03
<a href="#">【已结束】第三届中国(北京)军民融合技术装备博览会现场实况</a>		<a href="#">Windows 10新变化：系统自动更新将“强制化”，用户不再可选</a>	
<a href="#">Elaine_z</a>	2017-07-03	<a href="#">dawner</a>	2015-07-20



Copyright © 2018 WWW.FREEBUF.COM All Rights Reserved [沪ICP备13033796号](#)

 阿里云 提供计算与安全服务