Netflix 网络钓鱼活动窃取用户凭证和信用卡数据

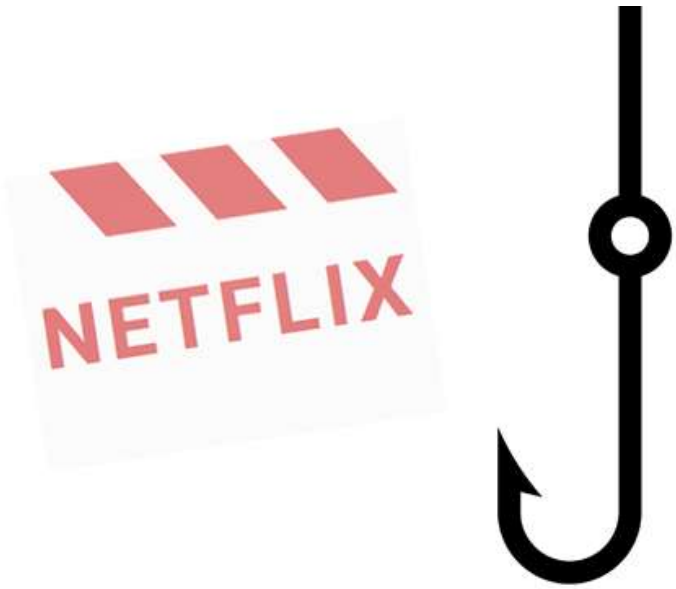
非官方中文译文·安天技术公益翻译组 译注

文档信息			
原文名称	Netflix Phishing Campaign Targeted User Information, Credit Card Data		
原文作者	Chris Brook	**原文发布日期**	2017 年 1 月 10 日
作者简介	Chris Brook 是卡巴斯基实验室《安全周报》（Threatpost）的副编辑。 https://www.linkedin.com/in/chris-brook-91223712		
原文发布单位	Threatpost		
原文出处	https://threatpost.com/netflix-phishing-campaign-targeted-user-information-credit-card-data/122988/		
译者	安天技术公益翻译组	**校对者**	安天技术公益翻译组
免责声明	• 本译文译者为安天实验室工程师，本文系出自个人兴趣在业余时间所译，本文原文来自互联网的公共方式，译者力图忠于所获得之电子版本进行翻译，但受翻译水平和技术水平所限，不能完全保证译文完全与原文含义一致，同时对所获得原文是否存在臆造、或者是否与其原始版本一致未进行可靠性验证和评价。 • 本译文对应原文所有观点亦不受本译文中任何打字、排版、印刷或翻译错误的影响。译者与安天实验室不对译文及原文中包含或引用的信息的真实性、准确性、可靠性、或完整性提供任何明示或暗示的保证。译者与安天实验室亦对原文和译文的任何内容不承担任何责任。翻译本文的行为不代表译者和安天实验室对原文立场持有任何立场和态度。 • 译者与安天实验室均与原作者与原始发布者没有联系，亦未获得相关的版权授权，鉴于译者及安天实验室出于学习参考之目的翻译本文，而无出版、发售译文等任何商业利益意图，因此亦不对任何可能因此导致的版权问题承担责任。 • 本文为安天内部参考文献，主要用于安天实验室内部进行外语和技术学习使用，亦向中国大陆境内的网络安全领域的研究人士进行有限分享。望尊重译者的劳动和意愿，不得以任何方式修改本译文。译者和安天实验室并未授权任何人士和第三方二次分享本译文，因此第三方对本译文的全部或者部分所做的分享、传播、报道、张贴行为，及所带来的后果与译者和安天实验室无关。本译文亦不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天实验室一律不予承担。		

Netflix 网络钓鱼活动窃取用户凭证和信用卡数据

Chris Brook

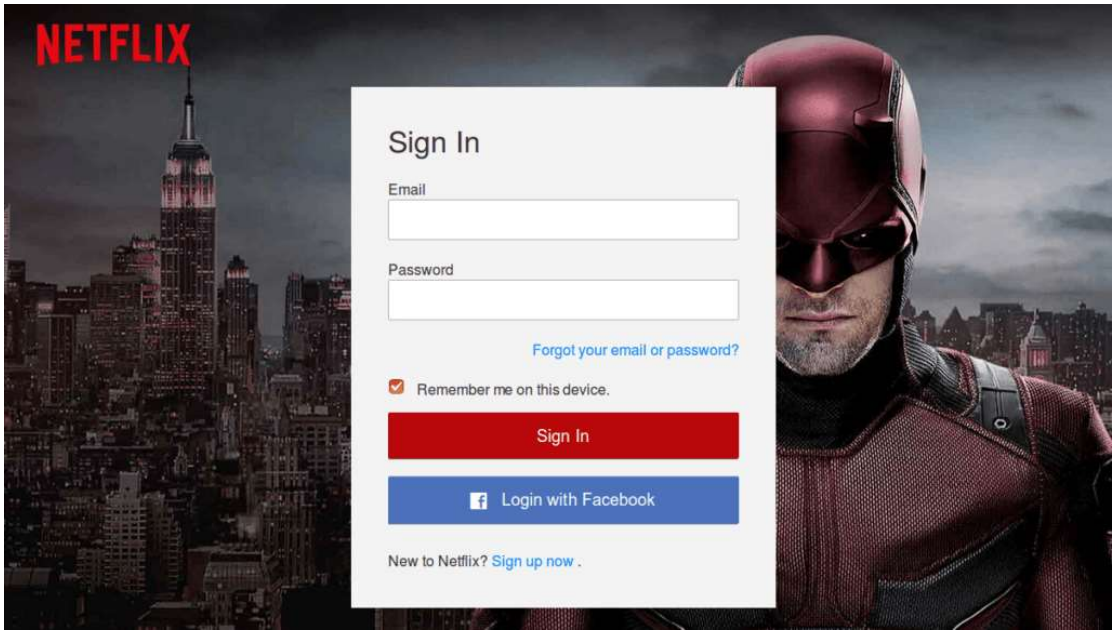
2017 年 1 月 10 日



最近，研究人员发现了一起网络钓鱼活动，该活动旨在诱使不知情的 Netflix 用户提供凭证和信用卡数据。

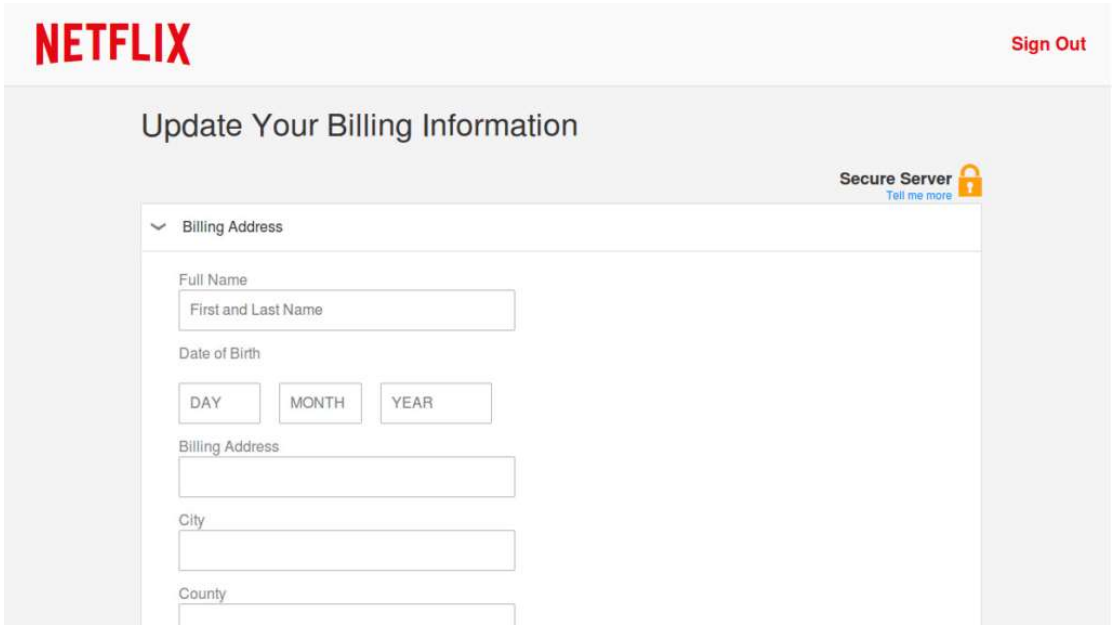
该活动（目前已经终止）首先向用户发送电子邮件，通知他们更新账户信息。

只要受害者点击邮件中的链接，就会被引向一个貌似合法的 Netflix 登录页面，并被要求输入电子邮件地址和 Netflix 密码。攻击者不满足于只获取用户的登录凭证，他们还将受害者引向另一个表格，要求他们更新支付信息（输入姓名、出生日期、地址和信用卡信息）。



攻击者也可能会做得过头，要求用户提供社保号（Netfli 从未有过这种要求）和 VBV 3D 安全代码（这是 Visa 在欧洲和印度使用的一个相当新的服务，尚未在美国部署）。

虽然钓鱼页面模仿真实的 Netflix 页面，甚至设置了一个黄色的“安全服务器”锁，但它们完全是伪造的。该活动通过 PHP 邮件实用程序将所有信息发送给攻击者，这样一来，攻击者就能够在多个网站部署网络钓鱼工具。



发现该钓鱼活动的是火眼公司威胁研究团队的研究员穆罕默德·莫辛·达拉（Mohamed Mohsin Dalla）。他指出，攻击者擅长绕过网络钓鱼过滤器，他们使用 AES 加密方法来加密提供的内容，能够更容易地规避检测。

达拉写到：“攻击者通过模糊网页来欺骗文本分类器，防止它们检查网页内容。该技术使用两个具有加密和解密功能的文件（一个 PHP 文件和一个 JavaScript 文件），用以加密和解密输入的字符串。PHP 文件在服务器端加密网页，JavaScript 文件则在客户端解密被加密的内容。”

此次针对 Netflix 客户的网络钓鱼活动并没有多么了不起，但是其规避检测和提供钓鱼页面的方式却有特殊之处。这些钓鱼页面托管在合法但被感染的服务器上，如果用户的 DNS 链接到 Google 或 PhishTank（一个反网络钓鱼服务），则不会向用户显示这些页面。

火眼公司指出，如果 Google，Phishtank 或其他网站（例如 Calyx Institute 或 Netflix）的用户访问了该伪造的网站，将会显示“404 Not Found error”消息，降低该钓鱼活动被发现的可能性。

Netflix 网络钓鱼活动的覆盖范围不断扩展。2016 年夏天，英国出现了一些假账单电子邮件，诱骗用户以为自己订阅了 Netflix 服务，要求他们提供信用卡信息。7 月发生的另一个骗局则通知 Netflix 用户他们需要更新信用卡数据。在受害者输入信息后，就会被告知其账户已停用，需要下载“Netflix 支持软件”。商业改进局（Better Business Bureau）指出，该软件是一款“远程登录软件”，会将受害者计算机的密钥发送给攻击者。