
# 趋势科技警告：“不留痕迹”的恶意程序已从欧洲蔓延至亚洲，专门锁定移动银行用户

**[趋势科技中国]– [2014 年 8 月 25 日]**网络银行帐号的防护很可能就像瑞士埃曼塔奶酪一样千疮百孔、充满漏洞。近日，全球服务器安全、虚拟化安全及云安全领导厂商趋势科技发现了一个名为“Operation Emmental”（埃曼塔行动）的全新网络犯罪行动，专门攻击利用手机短信(SMS) 进行双重认证的网络银行，拦截短信窃取银行客户的登录账号和密码，进而对账户实现完全掌控。这项在奥地利、瑞典和瑞士相当盛行的犯罪行动目前已现身日本，因而使得亚太地区遭受类似攻击的风险升高。

在这项攻击行动当中，不法分子会先以知名银行的名义散发假冒垃圾邮件给用户，然后引诱缺乏戒心的用户点击一个恶意的链接或附件，让用户的电脑感染一个特殊的恶意程序。该恶意程序有别于一般的网络银行恶意程序，此恶意程序会修改受感染电脑的域名系统(DNS)设置，让 DNS 指向一个不法分子所掌控的国外服务器，然后再将自己移除，因此很难被侦查到。这虽然只是一个小小的修改，但对受害者的影响却非常深远。

趋势科技（中国区）业务发展总监童宁指出：“多年来，银行一直试图通过各种安全机制来防止网络犯罪者入侵客户的账户，包括：密码、PIN 码、座标卡、交易认证代码（TANS)、会话令牌等等。另一方面，网络犯罪者的攻击却也日益精进。在 Operation Emmantel 行动当中，不法分子结合了多种不同技巧，包括：本地化的垃圾邮件、目的完成即消失的恶意程序、修改 DNS 设置、网络钓鱼页面、Android 恶意程序、幕后操作服务器，以及真正的后台服务器来达成目标。这使得银行必须建立更完整且涵盖不同层面和入侵点的防御机制，来保护客户免于网络威胁。”


【双重认证流程：未受感染与已感染 Operation Emmental 的电脑比较】

恶意程序会在受感染的电脑上安装一个流氓 SSL 证书，让电脑在默认情况下信任恶意 HTTPS 服务器。经过这番修改之后，当用户要开启自己的网络银行网站时，就会被自动引导至一个几可乱真的假银行网站，接着会要求用户输入账号和密码。最后，这个网络钓鱼网站指示用户在智能手机上安装一个恶意的 Android 应用程序。

这个伪装成银行会话令牌产生器的恶意 App 程序，事实上会拦截银行送出的认证短信，将它转发到不法分子的存储(C&C) 服务器或不法分子的手机号。也就是说，不法分子不仅通过网络钓鱼网站取得了用户的帐号密码，还取得了交易所需的会话令牌，因此便能完全掌控受害者的银行账户。

针对今日猖獗的移动网络犯罪，童宁进一步表示：“金钱依然是网络犯罪者最大的动机。根据《趋势科技 2014 年第一季信息安全总评季报》显示，网络银行恶意程序侦测数量在第一季度达到 116,000 个左右，较 2013 年同期稳定成长。更严重的是，Android 恶意程序数量在该季度已突破 210 万，较一年前成长了四倍以上。因此，银行必须监控多重入侵点的潜在攻击，并妥善加以防范，才能为客户提供安全的银行交易环境。”

针对该项攻击，趋势科技已发表一份新的白皮书：“Finding Holes: Operation Emmental”(寻找漏洞：Emmental 行动) 来深入讨论攻击细节。

**寻找漏洞：Emmental 行动白皮书下载地址，请点击：**

http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-finding-holes-operation-emmental.pdf

**如需有关 Operation Emmental 的最新信息，请点击：**

http://blog.trendmicro.com/trendlabs-security-intelligence/finding-holes-operation-emmental

###

**关于趋势科技（Trend Micro）**

趋势科技是全球虚拟化及云计算安全的领导厂商，致力于保障企业及消费者交换数字信息环境的安全。趋势科技始终秉持技术革新的理念，基于业内领先的云计算安全技术(Smart Protection Network)核心技术架构，为全世界各地用户提供领先的整合式信息安全威胁管理技术能防御恶意软件、垃圾邮件、数据外泄以及最新的 Web 信息安全，保障信息与财产的安全。同时，遍布全球各地的 1,500 余名趋势科技安全专家可为各国家和地区的企业级个人用户提供 7×24 的全天候响应及技术支持服务。更多关于趋势科技公司及最新产品信息，请访问：www.trendmicro.com.cn。请访问 Trend Watch：www.trendmicro.com/go/trendwatch 查询最新的信息安全威胁的详细资讯。