趋势科技新闻稿

[即时发布]

世界杯相关恶意 App 已超过 375 种！

趋势科技建议采取“读、不、安”三大法宝　保护球迷“百毒不侵”！

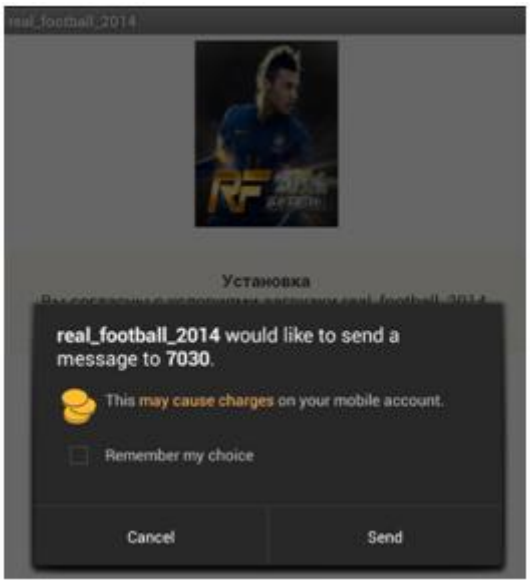
[趋势科技中国]– [2014 年 6 月 19 日]随著世界杯足球赛赛程推进，世界杯相关恶意程序也大量涌出！根据趋势科技最新统计，目前全球已出现超过 375 种移动恶意 App，正潜伏在未经授权/第三方应用程序下载商店，等待用户安装到移动设备上。趋势科技呼吁球迷可采取“读、不、安”三大防御法宝，让自己“百毒不侵”！

趋势科技（中国区）业务发展总监童宁表示：“除了最近充斥在网络上的网络钓鱼诈骗和黑客主义者外，网络犯罪分子也将目标瞄准移动设备的用户。趋势科技发现以世界杯为主题的移动恶意 App 已经高达 375 种，经过分析发现大部分有问题的恶意 App 都是目前普及的移动恶意软件家族变种，例如伪造热门应用程序的 ANDROIDOS_OPFAKE.CTD 家族、私下过滤短信和窃取信息的 ANDROIDOS_SMSSTEALER.HBT 家族、吃角子老虎诈骗程序 ANDROIDOS_MASNU.HNT、和木马程序 ANDROIDOS_OPFAKE.HTG 的变种等。”

伪造应用程序

趋势科技侦测到其中一个恶意软件家族是 ANDROIDOS_OPFAKE.CTD 家族，其最早出现在 2013 年 5 月，通过伪造热门应用程序的形式出现。它的恶意行为包括：替用户订阅增值服务，泄露用户的重要信息（如通讯录/短信），以及在移动设备主画面上安装恶意链接和快捷方式。

在短短一年间，被侦测到的 ANDROIDOS_OPFAKE.CTD 变种数量达到 10 万次，伪造了 14,707 种应用程序；并且该程序所连接的远程服务器有 66 个不同网域，每个网域都假装成著名的网站。



【假冒的世界杯游戏，会自动替用户订阅增值服务、恶意吸费】

短信过滤和信息窃取程序

趋势科技所侦测到的另一个利用世界杯热潮的恶意软件家族是 ANDROIDOS_SMSSTEALER.HBT 家族。这个家族变种有着和 OPFAKE 相似的诈骗和伪造方式，不过有一点不同的是：它们可以连接到远程 C&C 服务器接收并执行命令，其中一些会加入信息过滤程序（封锁/隐藏某些传入的信息），发送短信和安装新恶意软件。

分析其 C&C 服务器，发现有 76 个网域，它们都注册到 TanasovHennadiy。我们还发现这些有问题的 C&C 服务器也被用来代管第三方应用程序下载网站，其中大多数应用程序都用广告和信息窃取程序重新打包。

增值服务滥用

被侦测为 ANDROIDOS_OPFAKE.HTG 新变种的恶意程序也成为网络犯罪世界杯的一员，这是一个典型的增值服务滥用程序，受感染的用户会发现自己要支付从未注册过的昂贵服务费用。

吃角子老虎诈骗

趋势科技发现名为 ANDROIDOS_MASNU.HNT 的世界杯吃角子老虎恶意 App。它的恶意行为包括：过滤用户的付费确认信息，让用户不会注意到玩此游戏所花费的实际金额，因而可能会毫无节制地支出更多费用。

【世界杯吃角子老虎恶意 App】

有些足球博弈应用程序，也被发现会在用户不知情的状况下外泄用户信息，同时，在小额付费过程中，也会出现风险。我们建议移动用户使用这些应用程式时，要特别小心自己的财务和个人信息，或干脆避免使用。

趋势科技建议，球迷可采取“读、不、安”三个自我保护法宝，避免遭受恶意程序侵害：

- **读**：随时利用趋势科技整理的“FIFA 相关威胁信息”，来了解最新威胁信息与防御之道。
- **不**：只从有信誉的平台下载 App，不从未知的第三方平台下载程序，以降低风险。
- **安**：尽快安装移动安全解决方案，如趋势科技移动安全软件个人版免费 App，软件依托趋势科技 26 年的信息安全专业积累，能够在云端就能主动侦测通过 APP、网页、短信等传播的恶意程序，防堵其进行个人信息的搜集，保护自己不受恶意程序侵害！

世界杯相关威胁信息，请见：

http://about-threats.trendmicro.com/race-to-security/apac/

###

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。

更多媒体垂询，敬请联络：

趋势科技（中国）有限公司
刘婷婷
电话：010-85252277
电子邮件：angela_liu@trendmicro.com.cn

谋信传媒
那罡
电话：010-67047822
电子邮件：nagang@ctocio.com