趋势科技新闻稿

[即时发布]

隐藏的威胁浮上台面　趋势科技发布 2015 年及未来安全八大预测

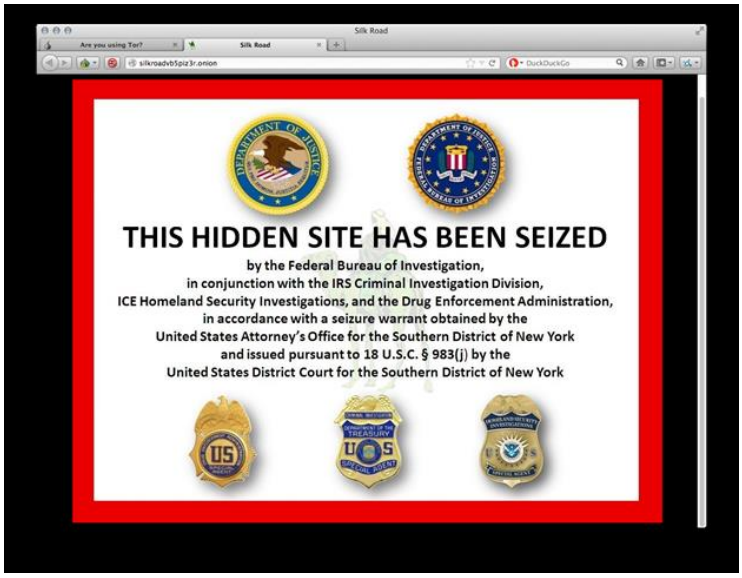
APT 攻击遍布全球 移动支付将带来全新威胁

[趋势科技中国]– [2014 年 11 月 21 日] “高级持续性威胁(Advanced Persistent Threat，APT) 会同最普通的网络攻击一样在全球泛滥；Apple Pay、Google Wallet 以及各类‘微’支付的流行将会带来移动应用的新风险。”这些极具写实性、前瞻性的消息来自《趋势科技 2015 年暨未来预测：隐藏的威胁浮上台面》报告。

趋势科技(中国区)业务发展总监童宁表示：“2014 年发生了多起由 APT 攻击导致的大型数据外泄事件，随着黑客攻击技能的泛化，攻击工具的商品化，这一威胁将更会更加猖獗，并波及更多国家。其次，针对 Android 移动设备的恶意软件正在以惊人速度的不断增长，2015 年这一数字将再创新高，突破至 800 万。此外，包括开放原始码应用程序漏洞、网络银行金融威胁及万物联网数据外泄等，都将成为 2015 新年度网络安全博弈的焦点区。”

网络威胁演进的速度超乎想象，形态也更为多元。作为全球服务器安全、虚拟化及云计算安全领导厂商，趋势科技不但通过已经发现的大量实际案例和云端海量数据分析，更借以年度《预测报告》的形式，发出了 2015 年网络安全领域即将出现的危险信号。以下是趋势科技对 2015 新安全威胁的八大预测：

1．更多的网络犯罪集团将利用 Darknet(黑暗网络)和专门的地下论坛来分享和贩卖犯罪软件。



【除了恶意软件，黑暗网络中还包含手枪、大麻商品，甚至是“买凶杀人”的服务】

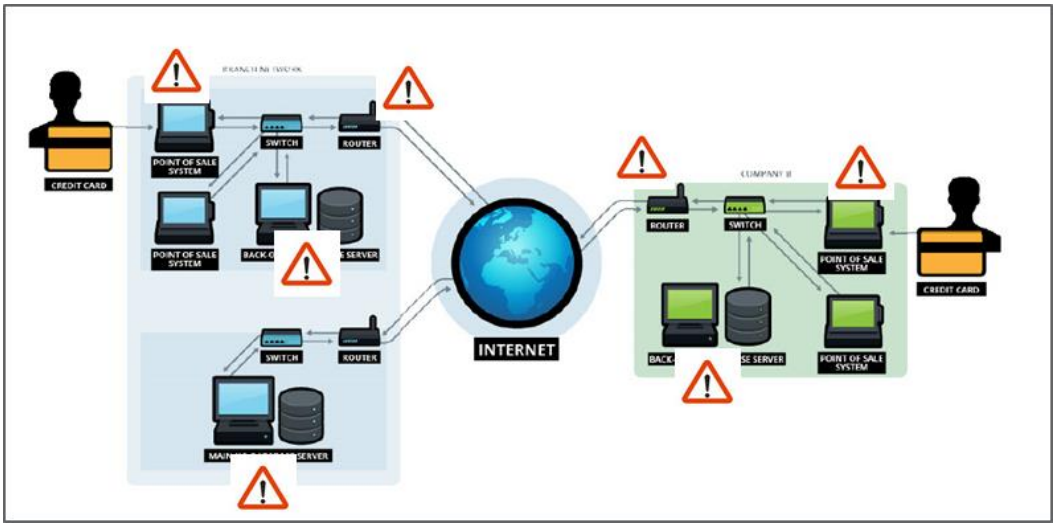
美剧《纸牌屋》中提及的 DeepWeb（深层网络）、Darknet（黑暗网络）是真实存在的。在这些搜索引擎无法找到的，或是需要加密客户端才能访问的站点上，网络攻击服务以及犯罪软件的价格正在逐年下滑，出现这一现象的原因在于恶意软件在地下市场供应量的增加。

不仅美国失窃信用卡资料、Facebook 和 Gmail 账号密码的价格大幅下跌，中国地下网络市场上的犯罪工具和服务也非常“琳琅满目”，而且采用了“明码标价”、“打包优惠”等促销模式。

2．网络犯罪活动加剧，将催生出功能更强、规模更大、效果更好的黑客工具及攻击手法。

【截至 2014 年 10 月大型数据泄露事件的统计数字】

2014 年的网络犯罪攻击愈演愈烈 ,美国 Target 超市 7000 万笔客户资料、美国 Home Depot 16 家饰建材连锁卖场的 6000 万笔客户资料、eBay 遭到神秘黑客的攻击、iCloud 泄露出大量好莱坞影星私密照片。

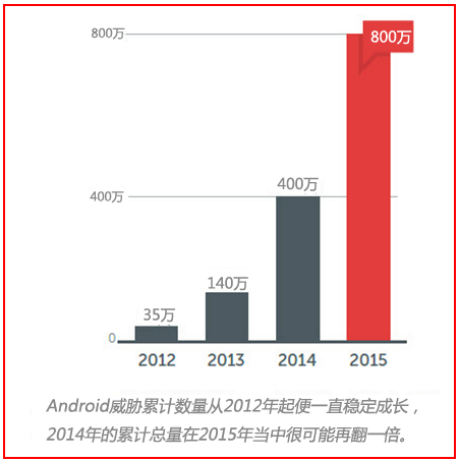


【入侵 POS 系统,网络及数据库等重要主机】

通过攻击频率数据的发展态势判断，趋势科技预计未来每个月都将见到两起或更多起大型资料外泄事件，而这些事件背后，正是那些神秘而强大的黑客工具。例如：发展迅速的 POS 病毒家族，犯罪集团所采用的恶意软件可以轻松入侵那些安装了 POS 软件的商家计算机，从而截获每笔付款的信息。这种恶意软件被用来取代以前在“ATM 上安装摄像头”等物理方式来进行的数据窃取。

3．移动设备漏洞逐渐成为重要的感染途径，漏洞攻击套件将开始锁定 Android 平台。

新型数据窃取恶意软件将会出现，网上银行恶意软件将继续发展，这让移动恶意软件和高风险应用程序的数量持续增长。趋势科技预计 2015 年 Android 威胁累积数量将达到目前的二倍，800 万将是人们不愿正视的数字纪录。



【Android 威胁累积数量将达到 800 万】

另外，移动设备、平台及 App 程序的漏洞数量将会增加，这将带来更严重的网络风险。未来，攻击移动设备的黑客将使用类似 Blackhole 漏洞的攻击套件，对 Android 设备释放出越来越多的网银病毒及勒索病毒。趋势科技还发现，不但第一个针对移动设备勒索程序 REVETON 已经现身，“OperationEmmental”(埃曼塔行动)全新网络犯罪行动背后的网络犯罪集团，他们不仅诱骗欧洲银行的客户安装恶意的 Android App 程序来骗取其账号密码，其威胁也已经蔓延到亚洲。

4．APT 攻击将变得与一般网络犯罪一样普遍。

尽管 2014 年很多政府机构和全球化企业在安全控管上都投入了巨大的人力和物力，但是 APT 攻击仍然渗透进这些组织，黑客将锁定高度机密的政府数据、金融信息、数字资产、工业设计资料等等。今年，网络犯罪集团成功利用 APT 攻击，在美国和加拿大制造多起大型数据外泄事件。趋势科技威胁防御专家预测，在 2015 年，越南、英国和印度等国黑客也将跟进，更多 APT 攻击来源和目标国家的名字，将会出现在 2015 年的盘点列表上。

另外，“电子邮件”成为了黑客最易取得 APT 攻击成效的入口。在某些案例中，攻击者会利用受害者的电子邮件账号来增加他们鱼叉式网络钓鱼攻击邮件的可信度。而经过足够多的研究分析后，网络犯罪份子可以制造出社交工程诱饵，骗取足够多的员工点击网络链接或者打开邮件附件。

5．新的移动交易支付方法将带来全新威胁。

预计 2017 年全球移动支付市场规模将高达 900 亿美元，移动支付服务这种新的支付形态很可能成为黑客攻击的新目标！当下，国外移动支付将因 Apple Pay、Google Wallet 催化而逐渐迈入主流，而国内“双 11” 支付宝移动支付交易笔数达到 1.97 亿笔，同比增长 336%。那么，移动支付的新风险又在哪里呢？

趋势科技认为，随着“心脏出血”、“Shellshock”等更多漏洞被发现，未来将可预见专门针对移动支付平台的威胁。例如 Android 的 FakeID 漏洞可能引发的风险，这可以让恶意应用程序冒用合法程序、存取设备上的敏感数据、访问 NFC 安全芯片上的内容。

所以，用户需要在未来重点观察和防止利用近场通信（NFC） 科技的犯罪行为，不要执行破解程序、在不使用 NFC 功能时将其关闭、定期检查软件是否有更新，开启屏幕

密码锁并为移动设备安装防护程序。而在国内，用户更应减少 Apple 设备“越狱”，提高安卓第三方应用商店的安全管理，因为这里都为移动支付威胁提供了滋生的沃土。

6．将会出现更多针对利用开源应用程序漏洞的攻击。

由于微软 Windows 和其他知名操作系统在安全方面的改进，将使得漏洞逐渐减少。所以，黑客将被迫转移目标到开源系统平台及应用程序的漏洞。一些存在多年的开放原始代码程序漏洞，今年都遭到了大量的攻击并造成了严重的灾情。这包 OpenSSL 软件的 Heartbleed 和命令行接口程序 Bash 中的 Shellshock 漏洞。

【黑客利用 Shellshock 漏洞可以盗取数据并发起大规模攻击】

未来几年之内，黑客仍将继续挖掘一些像 Heartbleed 和 Shellshock 这类潜藏已久的漏洞，这些可能比 25 年前就存在的漏洞更古老，但却对 Android 等其他终端系统造成

了更大的风险。这些漏洞可以入侵 Linux 桌面终端和服务器，控制 Android 系统及 APP 连接的内容，盗取数据或利用这些移动设备发动分布式拒绝服务（DDoS）等攻击。

7．万物联网（IOE）时代的设备多样性，将使其免于遭受大规模广泛性攻击，但设备中所处理与储存的数据将会成为黑客的新目标。

IoE、IoT 是近年最盛行的科技流行语，不仅手机、电脑、电视机等传统信息设备将连入网络，日常生活物品都将实现数字化、网络化、智能化。任何新科技产品在设计时都会考虑到网络的连接性，这可能包括：汽车、智能型烤面包机、计步器、婴儿监视器和电器设备。

设备的网络连接和运算能力，让它们变的“更聪明”，但也会带来安全风险。IoE、IoT 设备对黑客来说，充满了无限的可能性，黑客会想尽办法找到可攻击的目标。借助设备中所处理能力与储存的数据，他们可以执行更复杂、更严重的破坏任务，例如非法控制电灯、门窗等设备，甚至破坏一个国家的基础民生设施，威胁人身安全。

8．未来将出现更严重的网络银行及其他金融相关威胁。

网络银行恶意软件数量在 2014 上半年持续稳定增加，趋势科技监测结果显示，截至到第三季度，这些恶意程序的数量已经达到了 13.7 万个。Emmental 行动这样的复杂攻击手法，证明了即使是银行的双重认证机制也可能出现漏洞，而未来几年之内，跨平台的网银攻击会更加频繁。

网络是一个自由的空间，它给每个人自由选择的权利，但现在这个环境越来越难恶劣。对此，童宁表示：“如果隐藏的威胁已经浮上台面，仅仅做到关注是不够的，在这场黑与白的较量中获胜，需要主动的行动和全球用户的合力。当众多厂商在市场竞争压力下，不断推出更多缺乏安全机制的设备以满足日渐扩大的市场需求时，黑客也将发现更多可利用的漏洞，智能型设备制造商必须考虑如何协助用户保护这些设备当中的数据，而非仅是保护设备本身。”

完整的《趋势科技 2015 年暨未来预测：隐藏的威胁浮上台面》报告请参考：

http://www.trendmicro.tw/cloud-content/tw/pdfs/security-intelligence/reports/2015_prediction_tw.pdf

>> 点击阅读完整《2014年第3季度中国地区威胁报告》

###

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。