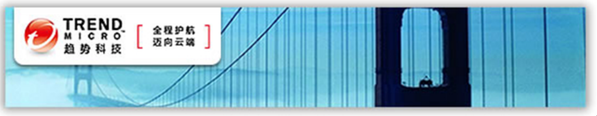


[趋势科技技术综述]

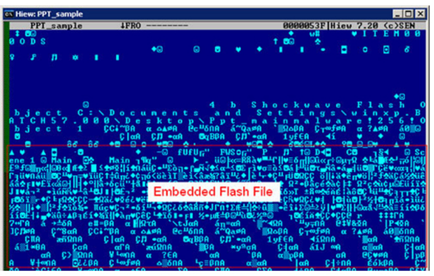
趋势科技提醒：APT 攻击已经瞄准白领办公环境 可实施“精准打击”

[趋势科技中国]– [2012 年 8 月 22 日]相信任何一个具有时代特征的企业都会减少或者拒绝纸质化的工作流程，取而代之的是各种版本的电子邮件与电子文档。由于这些电子邮件及电子文档包含了敏感的商业机密，因此相应的办公终端和程序极易成为黑客利用高级可持续威胁即 APT (Advanced Persistent Threat，也称为定向威胁) 攻入企业内部，对客户进行定向攻击从而窃取数据。

APT 为白领设下层层圈套

在最近的一段时期，全球服务器安全、虚拟化及云计算安全领导厂商趋势科技监测到了数起针对办公软件和平台漏洞的 APT 攻击案例，这使被攻击者承受了严重的经济和名誉损失。其中，多起 APT 攻击非常类似，它们都利用了 Office 办公软件或 Flash Player 的漏洞、后门程序，将带有恶意代码的附件植入到 PDF、DOC、PPT 或 XLS 档案中，进而实现窃取数据的目的。

不久前，趋势科技发现一个 PowerPoint 恶意文件，它会以邮件附件的形式攻击使用者。该 PPT 文档中内嵌了一个 Flash 动画，它会利用存在漏洞的 Flash Player 版本将后门程序植入到用户的计算机内。随后，它会连到远程的控制端跟攻击者进行握手通讯。攻击者利用它也可以下载并执行其他恶意软件，让受感染系统面临更可怕的威胁，甚至进行数据窃取等操作。



【趋势科技捕获到的恶意 PPT 文件，会以邮件附件的形式攻击使用者】

在日常的办公环境中，邮件和各种 Office 文档的使用率超过 90%，这给利用以办公软件为目标的 APT 攻击提供了广阔的充足的攻击对象；另外，在紧张、高效的办公环境中，很多白领们无闲顾忌和分析这些带有公司标识的邮件是否具有威胁，而轻易的点击和下载则有可能使企业陷入 APT 攻击者的圈套。

防范隐匿的社交工程陷阱

根据最新流行的 APT 攻击方式的分析，很多恶意邮件中的附件皆会以“热点事件、简报、报表、意见调查”的形式呈现出来。而此类社交工程陷阱(Social Engineering)诱饵又极具隐蔽性和自我防御性，在打开恶意附件的文件后，它们会停掉特定的防病毒程序，让其更难被侦测和清除。同时，这个后门程序也会下载并执行其它恶意文件，以进一步窃取内部网络中的其它数据。

趋势科技（中国区）高级产品经理林义轩表示：“APT 具有高隐蔽性、低能见度的特性。另外，APT 攻击者很聪明，它会千方百计躲避各类安全监测，并且只会去窃取高附加值的数据。而从趋势科技调查的状况来看，一次成功的感染可能会导致大量客户个人资料被窃取，而由于 Office 软件具有非常广大的用户群，所以现在的攻击很可能只是潜伏阶段，为了以后更大更广泛攻击做准备。有些用户是幸运的，因为他们很快就执行了适当的清除措施。但也有用户可能已经成为了 APT 攻击的俘虏，却并不知晓。所以，我们也必须保持警觉，尽快找到防范攻击的方法，因为这不会是我们最后一次看到这类威胁。”

从这些针对白领办公环境的 APT 攻击案例来看，网络犯罪份子通常会利用常见软件（如 Office 或在线办公平台等）的漏洞作为攻击点。由于 APT 类型的攻击具有“不让你看到”的特点，并且十分“低调”。针对 APT 攻击的防范，趋势科技提出三点建议：

第一，及时修补系统漏洞：企业将所有用户的系统更新到最新的安全修补程序，将有效地防范已知的 APT 攻击。

第二，云安全拦截恶意邮件：趋势科技的用户可以通过趋势科技云安全 Smart Protection Network 主动式云端拦截技术来侦测和删除相关的恶意文件，它可以在恶意邮件抵达使用者邮箱前就加以封锁。

第三，追踪隐匿的异常流量：如果企业用户怀疑已经遭遇了 APT 攻击，用户也可以通过网络流量的细微发现 APT 的破绽。这是因为，攻击者为了在受攻击目标内部建立更多的立足点。APT 攻击为了搜寻到高附加值的数据，需要不停进行跳板式攻击，当其通过交换机时就很容易被趋势科技的威胁发现设备 TDA 所发现。而及时修补网络安全防护漏洞，以及利用趋势科技的云安全技术及产品是可以有效的发现和抵御此类攻击的。

###

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 1,200 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。