# 网络钓鱼攻击的幕后

诸葛建伟

据专家预测，在未来几年中，网络钓鱼攻击的技术很可能进一步向前发展，并且网络钓鱼攻击的数量也将进一步增长。了解网络钓鱼的真实幕后，是信息安全“未雨绸缪”的最好法则。

网络钓鱼是指在互联网上，通过大量发送声称来自于银行或其他知名机构的欺骗性垃圾邮件，意图引诱收信人给出敏感信息（例如用户名、口令、账号ID、ATM PIN码或信用卡详细信息）的一种攻击方式。

最典型的网络钓鱼攻击将收信人引诱到一个通过精心设计与目标组织的网站非常相似的钓鱼网站上，并获取收信人在此网站上输入的个人敏感信息，通常这个攻击过程不会让受害者警觉。

二十一世纪，个人信息对黑客们具有越来越大的吸引力，因为这些信息使得他们可以假冒受害者进行欺诈性金融交易，从而获得经济利益。受害者经常遭受显著的经济损失或全部个人信息被窃取并用于犯罪的目的。

## 你被“钓”了吗？

欺骗别人给出口令或其他敏感信息的方法在黑客界已经有一个悠久的历史。传

PKCS#11等标准，提供用户基于外挂硬件模块方式的Windows下的安全应用。例如，基于Microsoft Office和Adobe Acrobat文档数字签名和工作流安全加强、基于Outlook和Outlook Express的安全邮件、支持CISCO和NORTEL的VPN客户端证书认证、文件加密、基于Web的SSL远程连接等。

然而，基于硬件TPM方案的安全终端，侧重信息保护和信任链的建立，但移动性和灵活性不高，还需要实现TSS等标准的应用支持，目前2～3年内难以推广应用。

基于软件方案的安全终端管理，侧重访问控制，可用性、可信度和安全性不高，升级困难，维护成本高。而且大都由边界安全产品厂商提供，通用性也存在问题。最主要的是不解决信息泄露的问题；

基于安全应用的安全终端采用外挂USB设备，使用隔离可信加密计算，很好的保护了信息隐秘问题，但其他与访问控制相关的安全应用都是直接在非专用的Windows平台上添加，这样一方面某些不需要的功能会造成系统负担，缺乏灵活性；同时工作特定的环境与其他安全应用环境无法分开，形成特定环境不安全的隐患。

## 未来的曙光

可信计算以及相似概念受到推崇的根本源自于日益复杂的计算环境中层出不穷的安全威胁，传统的安全保护方法无论从构架还是从强度上，人们都已经感觉到其后续发展的“力不从心”。

当前，业内的安全解决方案往往侧重于先防外后防内、先防服务设施后防终端设施，而可信计算则反其道而行之，首先保证所有终端的安全性，即透过确保安全的组件来组建更大的安全系统。

可信计算提供的安全功能有：终端设备认证、数据完整性校验、用户身份认证、用户权限合法性、端口控制和管理、数据的加密存储、重要信息的硬件保护。这些安全功能保证了使用者、软硬件的配置、应用程序等的可信，进一步保证了终端的可信，最终构建出可信任的计算机网络。

当前全球安全事件不断发生，蠕虫病毒肆虐、隐性黑客攻击，越来越多的网络面对内外夹击的尴尬处境，用户为不断发生的安全事故，疲于奔波，刚修复好崩溃的网络，病毒又开始在网络的某个角落密谋下一次的罪行。在这种情况下，极具安全性、便携性、灵活性和可扩展性的Secure Virtual（虚拟可信）外挂便携式可信终端模块提出了很好的解决方案，非常适合企业、金融、政府、军队、家庭等不同应用层次的安全需要，具有极强的产业前景。

另外，Secure Virtual外挂便携式可信终端模块让交换机、路由器、IDS、防火墙、用户管理系统、网元管理系统等拥有统一的沟通机制，从而让这些五花八门的设备实现联动。而且它们之间的通信数据采用TPM加密，避免被侦听识别而引发不安全动作。有了这样的联动管理机制，无论是来自于网络外部还是内部的影响稳定应用的干扰因素，网络都能够识别，并自动监控，如果问题严重，网络将自动强迫干扰源下线或者屏蔽这一干扰源。软


统上,这种行为一般以社交工程的方式进行。在二十世纪九十年代,随着互联网所连接的主机系统和用户量的飞速增长,攻击者开始将这个过程自动化,从而攻击数量巨大的互联网用户群体。

早期的网络钓鱼攻击主要目的是获得受害者的AOL账号的访问权,偶尔也期望获取信用卡数据以用于欺诈目的(如非法买卖这些信息)。这些钓鱼的信件通常包含一个简单的诡计从而哄骗一些“菜鸟”用户。

现在,钓鱼者所首选的策略是通过大量散发诱骗邮件,冒充成一个可信的组织机构(通常是那些钓鱼者所期望的已经被受害者所信任的机构),去引诱尽可能多的终端用户。被钓鱼者所青睐的目标机构已经包括很多著名的银行,信用卡公司和涉及日常性支付行为的知名互联网商务网站(如eBay和Paypal等)。大量针对互联网用户的钓鱼邮件的实例可以在反网络钓鱼工作组(Anti-Phishing Working Group)的网站上的钓鱼邮件归档中可以获得,其中许多邮件都显示了钓鱼者可以欺骗无知的用户。

## 真实的“网络钓鱼”

互联网用户经常在他们自己收到欺骗性邮件发觉网络钓鱼攻击,也常常在钓鱼网站所临时架设的主机被关闭很长时间后在技术新闻站点上看到这些恶意网站的记录副本,但这些事件只能被孤立从受害者的角度去观察,于是,就有了全新的“蜜网技术”。

目前,蜜网技术能够提供的一个最大的优势就在于其能够从攻击者角度捕获全部行为的能力,使得安全分析员能够对网络钓鱼攻击的整个生命周期建立起一个完整的理解体系。这种体系把钓鱼攻击分作几类。

通过攻陷的网站服务器钓鱼

大部分人们观察到真实世界中的网络钓鱼攻击涉及到攻击者攻入有漏洞的服务器,并安装恶意的网页内容。

通常情况下,网站钓鱼攻击的生命周期从钓鱼网站发布到互联网上后只有几个小时或几天的时间,因此人们的研究也发现网络钓鱼攻击在多台服务器上针对多个组织机构在同时并行进行。一个典型的网络钓鱼攻击的实际案例所捕获的数据可以阐述这些原理,该德国蜜网项目组观察到。在案例中,蜜网研究联盟的成员们部署了有漏洞的Linux蜜罐,而对蜜罐的攻陷过程显示了一种典型的攻击模式:蜜罐的被扫描和被攻陷具有非常强的连续性,并包括预先创建的钓鱼网站和群发垃圾邮件工具的上传和使用。

通过端口重定向钓鱼

2004年11日,德国蜜网项目组部署了包含一个Redhat Linux 7.3蜜罐的经典第二代蜜网。虽然安装的是相当旧的操作系统版本,攻击者也能够非常容易就能攻破,但它令人惊讶地经过了两个半月后才被首次成功攻陷——这和以上提及案例中讨论的蜜罐快速被攻陷的情况形成显著的反差。

2005年1月11日,一个攻击者却成功地攻陷了这台蜜罐,经调查发现,他使用了针对Redhat Linux 7.3缺省安装存在的OpenSSL SSLv2 Malformed Client Key Remote Buffer Overflow Vulnerability的攻击脚本。当攻击者获得被攻陷主机的访问权后,他并没有直接上传钓鱼网站内容。取而代之的是,攻击者在蜜罐上安装并配置了一个端口重定向服务。

这个端口重定向服务被设计成将发往该蜜罐网站服务器的HTTP请求以透明的方式重新路由到另外一个远程的网站服务器,这种方式潜在地使得对钓鱼网站内容更难追踪。

此外,攻击者下载并在蜜罐上安装了一个称为redir的工具,此工具是一个能够透明地将连入的TCP连接转发到一个远程的目标主机的端口重定向器。在此次案例中,攻击者配置该工具将所有到蜜罐TCP 80端口(HTTP)的流量重定向到一个位于 中国 的远程网站服务器的TCP 80端口。有意思的是,攻击者并没有在蜜罐上安装Rootkit以隐藏他的存在,这也说明攻击者并没有把被攻陷的主机的价值看的很重,同时并不担心被检测到。

“魔高一尺,道高一丈”。虽然上述钓鱼攻击的手段不断趋于复杂化,但信息安全业界的防范也从来没有停止过。可以预见的是,随着钓鱼攻击的技术门槛进一步增高及潜在的回报进一步增加,在未来几年中网络钓鱼攻击的技术很可能进一步地发展,并且网络钓鱼攻击的数量也将进一步增长。

减少可被僵尸网络控制的有漏洞的PC机,抑制数量不断增多的垃圾邮件,防止有组织性的犯罪活动,并且教育互联网用户关注来自社交工程的潜在安全风险,所有这些都还充满了挑战。软

责任编辑:蒋小瑜 E-mail:xiaoyu@swm.com.cn 美术编辑:赵庆琨 E-mail:zhaoqingkun@swm.com.cn