安全威胁每周警讯

2011/11/13～2011/11/19

本周威胁指数

***TrendMicro* 中国区网络安全监控中心**

前十大病毒警讯

排名	病毒名称	威胁类型	风险等级	趋势	病毒行为描述
1	TROJ_DOWNAD.INF	木马	★★★	→	DOWNAD 蠕虫关联木马
2	WORM_DOWNAD	蠕虫	★★★★	↑	该病毒会攻击未安装微软 IE 漏洞 MS08-067 的电脑，并且会在受感染电脑产生五万个恶意程序网址并试图在同一时间内随机连结其中 500 个恶意网站下载病毒
3	WORM_DOWNAD.AD	蠕虫	★★★★	↓	该病毒会攻击未安装微软 IE 漏洞 MS08-067 的电脑，并且会在受感染电脑产生五万个恶意程序网址并试图在同一时间内随机连结其中 500 个恶意网站下载病毒
4	TROJ_IFRAME.CP	木马	★★★	→	GIF、jpg 和 SWF 文件中被插入一个恶意的 iframe 标记时，趋势科技会将其判断为 TROJ_IFRAME.CP 病毒。当这些文件被执行时，会重定向到这些 URL，并下载恶意程序
5	Cryp_Xed-12	木马	★★	↑	木马病毒，通过访问恶意站点下载感染或由其他恶意程序下载感染
6	TROJ_SPNR.08JR11	木马	★★	↑	木马病毒，通过访问恶意站点下载感染或由其他恶意程序下载感染
7	HTML_IFRAME.AZ	网页病毒	★★	→	网页病毒,通常在网页在插入一个恶意 iframe,用户在访问该网页时会下载恶意文件或重定向到恶意网站
8	WORM_ECODE.E-CN	蠕虫	★★★★	↓	E 语言病毒,产生与当前文件夹同名 exe 文件
9	TROJ_SPNR.08KG11	木马	★★	↑	通过可执行文件传播的木马病毒
10	CRCK_KEYGEN	破解程序	★★	↓	非法破解程序

系统漏洞信息

MS11-085：Windows Mail 和 Windows 会议室中的漏洞可能允许远程执行代码 (2620704)

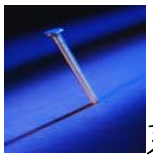
Windows Vista

Windows Server 2008

Windows 7

Windows Server 2008 R2

描述：http://technet.microsoft.com/zh-cn/security/bulletin/MS11-085



系统安全技巧

目前网络中存在着一些文件同步软件，这些软件能够极大程度的简化我们的数字生活，同时也适用于广大网民。这也是本文要和大家重点讨论的问题，因为一些专家认为这些文件同步程序可能存在安全风险。这意味着，要么我们在享受程序带来便利性的同时忍受潜在的数据风险，要么为了数据安全而停止使用这些软件，放弃这种方便的工具。但是我还希望有其他的选择。

其实安全性和便利性间的矛盾，并不是什么新的话题。早在远古时期，穴居的人类为了安全而将洞口设计的难于进出，这就是选择牺牲掉便利性。而我希望能有一个中间地带，既保留有安全性，又兼顾便利性。比如现在办公大楼门口常用的自动门。

安全性与便利性二者兼得

也许我们能做到二者兼得。曾经有人对此做过一些研究，认为在数字领域能够做到安全性与便利性兼得。这个人就是卡内基梅隆大学的 Bryan Parno 博士，他在安全方面的博士论文曾经获得过美国计算机协会颁发的 2010 年安全领域最佳博士论文奖。Parno 博士的这篇论文题目为：商业电脑上用于代码安全执行的信任扩展机制。论文的摘要如下：“我认为我们可以将某一商业设备上的信任用户迁移到其它设备上，并在不牺牲性能的前提下安全使用该设备的全部功能和服务，从而解决安全性和便利性之间长期存在的矛盾。”从论文的标题和摘要我们不难看出，这正是大家所关注的数字领域的“自动门”的问题。

就广大网友所关注的这些问题，我们采访了 Parno 博士。下面是本次采访的记录。

记者：我喜欢您对于用户信任的解释：“用户对于 X 对象掌握自己的私人数据的信任，意味着用户相信在未来任何时点，都不会因为将私人数据交给 X 对象保管而感到后悔。”这篇论文的本质是说我们可能实现既享受程序带给我们的功能性和便利性，又能确保我们的私人信息能够安全保存。您能概括的说一下，您为什么会认为这是可能实现的呢?

Parno 博士：通过我的大量研究工作，我发现通过提供按需分配的安全能力，可以满足用户对于安全性和产品性能功能方面的双重需求。比如，当你在打游戏或看视频的时候，对于安全性的需求一般会低于你在处理网上交易或税务报表时的安全需求。在使用同一个程序的时候，对于安全性的需求也会有所不同，比如在你访问网上银行页面，和访问新闻网站页面时，对于安全性的需求肯定不一样。如果安全系统能够实现按需提供安全防范能力，我们就可以在用户进行某些必要操作时提供足够的安全防护能力，而不影响用户在电脑上进行的其它操作，而不是提供一个一直都采用最高安全防范级别的系统来防护用户的所有日常操作。

记者：您的论文分为以下主题：

- 商用电脑的启动过程信任 Bootstrapping Trust in a Commodity Computer
- 商用电脑的按需安全代码执行 On-Demand Secure Code Execution on Commodity Computers
- 在网络上使用值得信任的基于主机的信息 Using Trustworthy Host-Based Information in the Network
- 可校验的计算：在不信任的软件或硬件环境实现安全代码执行 Verifiable Computing: Secure Code Execution Despite Un-trusted Software and Hardware

我想一项一项的跟您讨教。首先，我理解“商用电脑的启动过程信任”可以应用于个人电脑：“我们需要一套系统，让谨慎的用户对于本地的可信平台模块(TPM)实现引导过程信任，这样用户就能建立起对整个平台信任的基础了。”您打算如何实现这个功能?

Parno 博士：要信任一台计算机，你需要同时信任计算机的硬件设备和它所运行的全部软件。如果这台计算机是你自己的，那么你可以通过一系列标准步骤来确保硬件受信，比如你可以从大品牌的厂商那里购买硬件，当你离开屋子的时候锁好门窗，只让你所信任的人使用该电脑等等方法。

幸运的是，大部分人对于保护他们自己的物理资产都非常上心。不过，我们还需要一种方法将对电脑硬件设备的信任延伸到该电脑所运行的软件上。一些安全装置，比如刚才你说到的可信平台模块(TPM)，就是将硬件信任与软件信任相连接的纽带。

不幸的是，这个设备所使用的语言是二进制，所提供的保护功能是通过密码实现的，这两方面都是普通用户不够熟悉的。因此，我们打算采用一个用户信任的设备，比如你的手机或特制的 USB 密钥设备来与 TPM 进行对话，并将对话结果，也就是安全报告发送给用户，告知用户该计算机是否安全可用。

在论文里我介绍了几种安全的方法，可以将你自己的可靠设备(比如手机)与计算机中的安全模块联系起来。包括较复杂的采用特殊设备接口连接这两种设备，还有最简单的在电脑机箱接缝处贴易损条码，并通过手机软件来识别条码。每种方法都有自身的优势和不足。

记者：接下来，“商用电脑的按需安全代码执行”是指安全的使用未知计算机。您建议使用一种叫做Flicker的新方法。这个 Flicker 到底是什么，它有什么作用呢?

Parno 博士：Flicker 可是说是一种安全架构，它利用了 AMD 和 Intel 在 CPU 中新增添的安全功能，可以根据需要提供安全的代码执行环境。该架构的目的就是在你的电脑里建立一个完全独立于其它软件(甚至硬件)的环境来执行小段的敏感代码，这样就算电脑中感染了恶意软件，这部分敏感代码的执行也不会受到影响。

比如，假设你使用公司提供的 VPN 网络从远程访问网络，首先要做的就是在 VPN 客户端输入用户名和密码。如果这个客户端软件存在 bug，或者你的操作系统存在漏洞，或者电脑中任何设备驱动程序存在漏洞，任何以管理员权限运行的软件存在漏洞，都可以被黑客利用获取你的 VPN 用户名和密码。

通过 Flicker，我们可以将 VPN 软件中有关用户名和密码的代码提取出来，并在一个独立的环境中执行，这样就算其它软件(甚至操作系统)存在漏洞，也不会影响在独立环境中运行的密码处理代码的安全性。

Flicker 还可以显示出目前隔离环境中正在执行哪个程序，以及某个程序是否处于受保护环境。换句话说，通过 Flicker，你可以看到弹出的密码对话框确实是处在 Flicker 保护下的，同时你的公司也会知道你在使用正确的 VPN 客户端软件输入正确的密码，而不是在使用某个恶意代码。

记者：“在网络上使用值得信任的基于主机的信息”是你对于保护网络数据流安全的信条。你提到这个过程必须具有以下特性：

- 注释完整：恶意主机或网络元素无法改变或混淆注释信息中的数据。

- 网络处理无状态：为了确保那些依赖主机信息的网络元素的可扩展性，避免这些设备上保持 per-host 或 per-flow 状态。

- 隐私保护：我们的目标是防止任何用户信息泄露，而不是像目前系统这样漏洞百出。换句话说，我们的目标不仅仅是当用户访问某个网站键入个人信息时才提供保护。

- 增强的可部署能力：尽管我们都相信值得信任的主机信息对于未来的网络会有很大的帮助，但是我们目前应该努力让部属该系统的用户立即体会到其优势所在。

- 效率：在部署后，该架构必须不会明显降低客户端到服务器的网络性能。

您能简要的解释一下上述各点都是如何实现的吗?

Parno 博士：很多网络协议，尤其是与安全相关的协议，都会花费大量资源试图改变信息的结构，而这些信息对于信息源来说是已知的。

举个例子，研究表明，如果你知道电脑将要发送多少封电子邮件，以及这些邮件的目的地，你就能明确的知道这些邮件是否是垃圾邮件。任何一个邮件接收者都很难完成上述统计，但是对于邮件发送者来说，这种统计很容易。

通过诸如 Flicker 这样的架构，我们可以在隔离区域里进行这种统计运算，并将其通过加密的方式附加在每一封发出的邮件或网络数据包中。邮件服务器在接收到这些邮件后就会知道邮件发送源主机在最近一个小时内发送过多少封邮件，比如发现在过去一小时内，这台主机只发送出了两封邮件，那么这封邮件是垃圾邮件的可能性就很小了。

类似的方法还可以用于其它协议，比如帮助缓解拒绝服务攻击或者网络蠕虫的泛滥。当然，我们使用这种方法的同时也要注意保护用户隐私，比如通过组合的匿名技术，仔细选择作为标记的状态参数，以及使用小型的，独立的可校验的代码模块。

记者：最后，“可校验的计算：在不信任的软件或硬件环境实现安全代码执行”。据我的理解，这方面主要是针对外包计算和网络方面的安全规范。您认为应该使用 Yao 教授的乱码电路方案和同态加密方案。我了解同态加密，但是 Yao 教授的乱码电路方案是什么意思?

Parno 博士：乱码电路(Garbled circuits)是 Andrew Yao 教授在上世纪 80 年代发明的一种很聪明的技术。它可以让两个人针对某个算式来计算答案，而不需要知道他们在计算式所输入的数字。

举个例子说，假如你和我都想知道咱们两个到底谁更年长一些，但是我们两个都比较谨慎，不想直接告诉对方自己的年龄。使用乱码电路方案，我们可以通过交换一些信息的方法来让彼此知道答案(比如我说我比你年轻)，但是这种信息交换并不会让我知道你的确切年龄，你也同样不会知道我的确切年龄。

通过我的论文工作，我发现如果修改一下 Yao 教授的电路结构，我就可以创建一种新的协议，让你可以将某个计算功能外包给第三方，同时还能校验他们的计算工作是否正确。

比如我可以付费给你帮助我进行一些数据的傅里叶变换的计算工作 ，当你将结果反馈给我后，我需要确保你反馈回的数据是确实进行傅里叶变换后得到的数据，而不是随便给了我一个凭空捏造的数据。

经过修改后的 Yao 教授的协议可以让我对你的计算工作进行约束，从而在你完成计算工作后有效的对计算答案进行校验。相反，完全同态加密本身只能保证我所提供的数据安全，而不能告诉我第三方到底对我的数据进行了什么类型的计算。

不幸的是，只是修改 Yao 教授的协议还不够。因为建立一个乱码电路需要很多工作，而每次计算，都需要重新建立电路。现在我们通过在协议上增加一个加密层的方法来解决这一问题，这样我们就能多次重复利用同一个电路，从而在多次运算中平摊电路的设计成本。

总结

便利性与安全性兼得的方案看上去有些复杂，不过这确实是未来的发展方向。另外我们还要感谢 Parno 博士的研究，以及他抽出时间接受我们这次采访。

来源：ZDNet 安全管理