安全威胁每周警讯

2011/07/17～2011/07/23

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

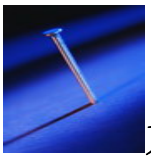
排名	病毒名称	威胁类型	风险等级	趋势	病毒行为描述
1	TROJ_DOWNAD.INF	木马	★★★	→	DOWNAD 蠕虫关联木马
2	WORM_DOWNAD.AD	蠕虫	★★★★	→	该病毒会攻击未安装微软 IE 漏洞 MS08-067 的电脑，并且会在受感染电脑产生五万个恶意程序网址并试图在同一时间内随机连结其中 500 个恶意网站下载病毒
3	WORM_DOWNAD	蠕虫	★★★★	→	该病毒会攻击未安装微软 IE 漏洞 MS08-067 的电脑，并且会在受感染电脑产生五万个恶意程序网址并试图在同一时间内随机连结其中 500 个恶意网站下载病毒
4	TROJ_IFRAME.CP	木马	★★★	→	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	Expl_ShellCodeSM	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	WORM_ECODE.E-CN	蠕虫	★★★★	↑	E 语言病毒,产生与当前文件夹同名 exe 文件
8	TROJ_DLOADER.UVD	木马	★★★	↑	木马病毒
9	CRCK_KEYGEN	破解程序	★★	→	非法破解程
10	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

系统漏洞信息

MS11-056：**Windows 客户端 / 服务器运行时子系统中的漏洞可能允许特权提升**

Windows XP
Windows Vista
Windows Server 2008
Windows 7

描述： http://www.microsoft.com/china/technet/security/bulletin/MS11-056.mspx



系统安全技巧

当今世界，信息化已经是大势所趋，计算机不仅成为人们生活工作不可或缺的工具，也是众多企业日常开展工作须臾不可离的工具，随着而来的，就是电子化办公，数字化信息存储带来的信息安全压力。越来越多的中国企业开始具有核心的知识产权与不可外泄的商业秘密，因而众多的企业也开始重视信息安全体系的建设。但是，更多的企业把自己的注意力放在了防止外部入侵即网络边界安全，而恰恰忽略了身边的威胁——内部泄密。据 FBI 和 CSI 曾对 484 家公司进行的网络安全调查结果显示：超过 85%的安全威胁来自公司内部，由于内部人员泄密所导致的资产损失高达 6000 多万美元，它是黑客所造成损失的 16 倍、病毒所造成损失的 12 倍。企业若是忽略了其内网安全防范措施，将损失许多宝贵的核心数据、专利技术信息，多年累积的技术资产和研发投入成为他人的嫁衣，甚至可能因此导致企业失去竞争力。企业还可能丧失的是其声誉，以及员工、合作伙伴与客户的信赖。

面对日渐严重的内部泄密事件，我们如何守护企业的核心信息，如何防止内部泄密也就成了摆在各个企业领导面前的一大问题。其实，针对内网安全，防止内部信息泄漏早已有了比较成熟的体系。这得益于一个还不为广大企业所知的行业——信息防泄漏行业。信息防泄漏从这个行业诞生时刻开始就致力于保护国家秘密，维护国家涉密内网安全，防止涉密信息泄漏。随着企业保护核心信息的需求日益增长，信息防泄漏行业也开始逐渐为广大企业提供信息安全服务。面对企业的内网安全问题，信息防泄漏行业凭借多年来服务于国家政府机关积累的经验，提出六项措施，有效防止内部泄密，守护企业核心机密。

措施一：严控计算机外设端口，监控、审计所有计算机的操作行为，封锁信息外泄途径。

在企业当中，有一种非常普遍的情况，就是对于计算机外设完全没有任何监控。每台计算机可以任意使用各种 USB 设备，可以随意读取光盘，可以连接打印机，能够随时的打印文件。这也就极大地方便了内部人员将核心信息，商业机密带离公司，从而导致信息泄漏。也有一部分公司，感觉都到了内部泄漏的风险，采取了一些手段，例如拆掉光驱，塑封 USB 口一些简单的方式，希望能够控制内部人员随意使用外设端口，但是这些控制方式都能够很轻易的破解，并没有带来真正意义上的效果。更有一些公司，感觉到简单的控制手段无法保证效果，就采用了一些技术手段，例如利用修改注册表或者设置组策略等形式，达到禁止外设端口的效果。这样在一定程度上，起到了一定效果，然而，针对那些真正企图泄漏内部机密的幕后黑手而言，这些手段能够很轻易地被破解。要达到彻底封锁信息外泄途径，就需要应用专门技术，例如鼎普科技的“内网安全综合管理系统”综合利用中间层驱动、驱动拦截、线程注入等驱动级技术，对操作系统底层驱动进行拦截，保证对接口、设备的监控准确有效，并在此基础上实现设备监控、文件监控、打印监控等。可准确识别打印机、硬盘、活动硬盘、MODEM 等设备，并可对设备的使用进行控制。通过严格控制计算机外设端口，有效监控审计所有的计算机操作行为，做到封锁信息外泄途径，起到让核心信息“看得见、用得了、拿不走”的效果。同时建立及时有效的报警审计功能，将内部信息泄漏的一切可能扼杀在萌芽状态，内部人员一旦出现可疑操作、违规操作及时阻断、发现并报警，防患于未然。

措施二：所有重要信息集中存储，终端不留密，信息使用权限细分。

随着信息化程度的不断提高和自动化办公的不断普及，公司文件由传统的纸质文件越来越多的向电子化文档转换，而这些公司文件零散的存储在各计算机中，然而大多数的公司在进行防护系统建设的时候，更多的是把目光放到了网络边界安全，也更多的偏向于监控计算机设备以及计算机使用者的操作，对于真正重要的核心信息本身的防护却有限。同时由于许多的公司业务流程已不再是狭窄孤立的，而是非常具有动态性、协作性和广泛性的合作过程。例如：在日常办公过程中，可能需要公司内外的人员通过演示文稿、电子表格或文档的形式来复制、共享、打印输出等信息。这也带来一个问题就是没有一个行之有效、更加细分化的策略权限控制手段，帮助管理者限定核心信息针对个人具体的使用权限。这是一个很有效地手段，就是将核心信息集中存储，保证终端不保存机密信息，在利用驱动级文件权限控制技术、剪贴板防护技术、数据消除技术、进程数字签名技术等技术，强制终端用户只能通过系统提供的安全虚拟平台访问文档集中管理服务器上的资源。这样就既解决了核心信息分散不易管理的难题，又可以针对核心信息进行详细的权限控制，针对不同的内部人员执行不用的读、写、复制、删除等等操作策略。保证公司能够对接触使用核心信息的内部人员进行控制，全面了解核心文件“谁能看、谁能改、谁能用、谁能带”。有效的降低了内部人员泄密的可能。

措施三：通过移动介质泄密往往是信息泄漏的主要方式。需要严格控制移动介质使用，划分介质使用范围与责任人。

目前广泛应用于企业单位中的信息交互工具就是移动介质，作为最有效的信息移动的手段之一，移动存储介质具有使用方便，存储空间大等众多的优点。然而移动存储介质的容量越做越大，体积却越做越做小，非常容易丢失。而移动存储设备本身在设计上由于考虑较多的是易用性，所以往往没有任何防护措施。一旦移动存储设备丢失或被盗，就会造成存储其中的信息外泄。并且大多数企业在日常使用的过程中，并不限定移动介质的使用范围，使得员工无论是在公司内的电脑，还是个人电脑，或者网吧等等其他地方的电脑上任意使用，使得文件可被轻易复制或者被病毒、木马侵害，造成信息泄密。由此可见不被管控的移动存储设备成为了最为危险的信息泄漏途径与工具。这也就需要我们严格控制移动介质的使用，划分介质使用范围与责任人。即对介质使用状态、配置信息全面的掌控；严格监控介质从购买后的注册发放、使用、统一台帐监控、状态查询到收集注销的运行周期，以及介质从插入、进行各种操作、到拔除全程进行跟踪记录和实时报警的运行周期。通过对公司内移动介质的注册，实现移动存储介质管理可信化、全程监控；防止移动存储介质使用导致的信息泄漏及木马病毒传染。因为经过公司对移动介质的统一注册管理，做到了公司内部移动介质无法被外部电脑识别，这样一旦出现介质丢失事件，也可以最大程度避免存储其中的核心数据外泄。

措施四：监控本地上网行为，监控员工的上网行为，避免信息从本地被转移。

随着网络的不断发展与进步，每个公司都会因为工作的需要，连接互联网。水能载舟亦能覆舟！互联网一方面能够帮助企业提高生产力、促进企业发展；另一方面也在企业管理、工作效率、信息安全、法律遵从、IT 投资等方面给企业提出了严峻的问题与挑战。日益发达的互联网让员工有了更多的选择，员工很难不受众多网络娱乐的诱惑，大家在或多或少地利用工作时间进行非业务操作。同时，由于某些公司员工信息安全意识比较薄弱，很多时候将客户信息、内部敏感信息等在公网上随便传播，并没有加密，这样的信息数据很容易被窃取修改。由此产生的泄密事件，也会给公司带来巨大损失。为此，某些公司高层反对开通网络，也曾经实施过惩罚制度，但效果不理想，因为如果不开通网络工作，会给工作带来不便。事实上并不是所有的员工都需要网络的，销售、采购外部协作、生产管理等部门的员工可能需要上网，但是像人事、工程设计等部门上班时间用网络的很少。这就是说，我们需要找到一个合适的手段例如网络信息监测系统，控制本地上网，监控员工上网行为。结合内核数据截收和预处理技术、深度内容检测技术、智能识别阻断等专利技术，为客户解决网页过滤、封堵与工作无关的网络应用需求。让企业可以根据行业特征、业务需要和企业文化来制定个性化的网页访问策略，过滤非工作相关的网页。同时制定精细的带宽管理策略，对不同岗位的员工、不同网络应用划分带宽通道，并设定优先级，合理利用有限的带宽资源，节省投入成本。并且可以制定全面的信息收发监控策略，有效控制关键信息的传播范围，以及避免可能引起的信息泄漏风险。

措施五：建立基于硬件级别的防护体系，避免众多安全防护产品基于操作系统的脆弱性。

在企业的日常工作中，计算机终端是信息存储、传输、应用处理的基础设施,它可以称为信息的源头，其自身安全性涉及到系统安全、数据安全等各个方面, 这就要求企业及时调整安全防护策略,重视计算机终端安全。目前多数计算机终端的防护思路是在既有操作系统上加载软件。这种方式就像建立在沙丘之上的堡垒，存在致命的弱点。例如，操作系统本身不安全;重装系统会使软件的功能全部失效，非法卸载安全软件，使敏感信息系统主机失去保护;硬盘丢失，所有重要信息数据将全部暴露等等。针对这些问题，目前就有一些产品，以 PCI 适配卡为硬件载体、基于 BIOS 级别的设计，实现了重要敏感信息终端的安全“硬”保护，从信息的源头保证了硬件级安全。因为 PCI 总线已成为当今计算机终端使用的事实总线标准，具有丰富的硬件资源，不易受资源环境限制。同时，PCI 设备配置空间采用自动方式，反跟踪能力强。且从 BIOS 级别上对计算机终端进行防护，是较高层次的技术实现途径，可行并有效。这种安全性不依赖于任何操作系统或软件，实现了强制终端从硬盘启动，杜绝从光盘启动，防止随意重装操作系统;用户可指定主机必须安装的软件，开机后该产品会自动对其进行检测，如果系统中不存在指定软件(可能被卸载)则主机不能启动和使用。同时实现了基于 BIOS 的硬件级登录认证，以及芯片级的数据全盘保护，但保护对用户完全透明，即使硬盘丢失数据也不可能被恢复。另外，这种可对硬盘实施整盘加密，对包括操作系统文件在内的所有硬盘数据实施全盘保护。即使硬盘丢失，其中的数据也无法被数据恢复技术破解而遭到窃取。部署这种基于硬件设备的防护产品，可以进一步阻止恶意破坏导致的信息泄漏，保护企业核心信息。

措施六：制定合适的制度，对违反企业规定的行为进行奖惩。对员工进行教育并严格执行制度，从头脑中杜绝信息泄漏。

我们知道有一句老话，"三分技术，七分管理"，这里切实反映出了制度规范在信息防泄漏的中重要性。内网安全系统是重要的安全系统，但也因为涉及到很多应用和便携设备，多少会对普通用户的使用习惯造成影响。这个时候，就要求企业能够利用成文规章来合理的约束用户的行为，加强用户教育，为系统的实施创造制度依据，才能让安全更加深入人心。“技术服务于管理，管理依托于技术”，管理和技术相结合，技术限制配合制度管理，对违反企业规定的行为进行奖惩，对员工进行教育并严格执行制度，这样企业信息安全不再内忧外患。

当今世界，信息化已经是大势所趋，计算机不仅成为人们生活工作不可或缺的工具，也是众多企业日常开展工作须臾不可离的工具，随着而来的，就是电子化办公，数字化信息存储带来的信息安全压力。越来越多的中国企业开始具有核心的知识产权与不可外泄的商业秘密，因而众多的企业也开始重视信息安全体系的建设。但是，更多的企业把自己的注意力放在了防止外部入侵即网络边界安全，而恰恰忽略了身边的威胁——

内部泄密。据 FBI 和 CSI 曾对 484 家公司进行的网络安全调查结果显示：超过 85%的安全威胁来自公司内部，由于内部人员泄密所导致的资产损失高达 6000 多万美元，它是黑客所造成损失的 16 倍、病毒所造成损失的 12 倍。企业若是忽略了其内网安全防范措施，将损失许多宝贵的核心数据、专利技术信息，多年累积的技术资产和研发投入成为他人的嫁衣，甚至可能因此导致企业失去竞争力。企业还可能丧失的是其声誉，以及员工、合作伙伴与客户的信赖。

面对日渐严重的内部泄密事件，我们如何守护企业的核心信息，如何防止内部泄密也就成了摆在各个企业领导面前的一大问题。其实，针对内网安全，防止内部信息泄漏早已有了比较成熟的体系。这得益于一个还不为广大企业所知的行业——信息防泄漏行业。信息防泄漏从这个行业诞生时刻开始就致力于保护国家秘密，维护国家涉密内网安全，防止涉密信息泄漏。随着企业保护核心信息的需求日益增长，信息防泄漏行业也开始逐渐为广大企业提供信息安全服务。面对企业的内网安全问题，信息防泄漏行业凭借多年来服务于国家政府机关积累的经验，提出六项措施，有效防止内部泄密，守护企业核心机密。

来源：51CTO