公司计算机病毒的分析与防范

目录

【摘 要】计算机病毒是一个程序或一段可执行代码。具有破坏性、隐蔽性、潜伏性、传染性的特点。随着网络技术的飞速发展，计算机病毒制造技术也日新月异。计算机病毒可以渗透到信息社会的各个领域，给计算机系统带来了巨大的破坏和潜在的威胁，严重地干扰了人们正常的工作与生活。公司信息网的安全与畅通已经不是某一个或者几个人重视就能解决的问题了，普及计算机病毒的防范措施已迫在眉睫，我们每个人都需要对新形势下的计算机病毒有一个对的的结识。本手册列举了计算机病毒的定义与传播特点、病毒爆发的案例、如何对的防止和查杀病毒等内容，希望每个人都能学习并掌握对的的病毒防止查杀办法，为公司信息网的安全运营奉献自己的一份力量。

【关键字】计算机病毒　病毒感染 破坏 传播 木马　杀毒　安全

一、概述

（一）病毒的定义

计算机病毒是指编制或者在计算机程序中插入的，破坏计算机功能或数据、影响计算机使用，并能自我复制的一组计算机指令或者程序代码。它只是一串二进制代码，但由于计算机病毒与生物医学上的“病毒”同样具有传染性、破坏性、隐敝性和潜伏性，因此人们从生物医学上引申了“病毒”这个名词。

（二）产生的因素

计算机病毒的产生是计算机技术和以计算机为核心的社会信息化进程发展到一定阶段的必然产物。特别是互联网的迅速发展，病毒的传播从通过软盘拷贝发展到网络传播。病毒的成因，归纳起来重要有以下四个方面的因素：

1.破坏心理

某些程序员编制一个病毒进行炫耀、报复或者发泄，这些源代码发送到互联网上以后，通过别有专心的程序员改编，制作成病毒，病毒不断的进行复制与传播，最终才导致大量计算机中毒瘫痪。

这类病毒往往扩散性、破坏性特别高。需要大家时刻警惕。

2.利益驱动

网络黑客们通过技术手段将公司或个人的机密数据加密、删除，然后鼓吹只有黑客自己才干解密、恢复数据。黑客们通过向受害者索要高额数据恢复费用的方式进行非法牟利。

这种病毒的危险限度最高。由于黑客们由于利益驱动，都会使用最新的技术漏洞来编写他们的恶意代码。由于杀毒软件病毒码总是慢一步，在各种防病毒软件杀毒码能辨认这些病毒、木马之前，这些黑客已经得手了。

3．恶作剧

某些精通计算机技术的人为了炫耀自己的高超技术和智慧，凭借对软硬件的进一步了解，编制一些特殊的程序，大多表现为播放一段音乐，显示一些动画，或在 WORD 文档打开时提一些智力问题等。

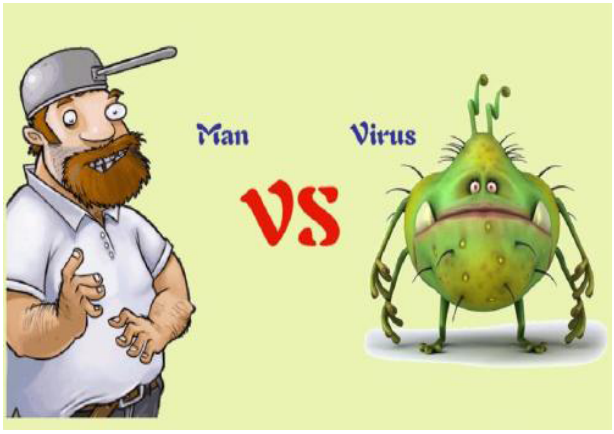
这类病毒传染性、破坏性都不高，但是也比较影响计算机正常的运营状态，假如源代码被别有专心的人运用，也会导致比较坏的影响。

4．用于特殊目的

某组织或个人为达成特殊目的，对政府机构、单位的特殊系统进行暗中破坏，窃取机密文献或数据。

二、病毒的分类

计算机病毒按破坏限度的大小可分为良性病毒和恶性病毒；按传染的对象可分为引导型病毒、文献型病毒、复合型病毒和宏病毒；按病毒所依赖的操作系统，可分为DOS 病毒、Windows 病毒、UNIX 病毒和 Linux 病毒等；按病毒的传媒可分为引导区病毒和网络病毒。然而，目前最常用的一种分类方式是按病毒的感染传播特性划分为系统病毒、蠕虫病毒、木马病毒、黑客病毒、破坏性程序和网页脚本病毒等。



（一）系统病毒

这种病毒会用它自己的程序加入操作系统或者取代部分操作系统进行工作，通常重要感染 Windows 操作系统的*.exe 和*.dll 文献，并通过这些文献进行传播。由于感染了操作系统，病毒在运营时，会用自己的程序片断取代操作系统的合法程序模块，并根据病毒自身的特点和被替代的操作系统中合法程序模块在操作系统中运营的地位与作用，以及病毒取代操作系统的取代方式等，对操作系统进行破坏，甚至导致整个系统瘫痪。CIH 病毒就属于此类病毒。

（二）蠕虫病毒

这种病毒是一种通过网络或系统漏洞传播的恶性病毒，它除了具有一般病毒的一些共性外，同时具有自己的一些特性，如不运用文献寄生(只存在于内存中)，对网络导致拒绝服务，并与黑客技术相结合等。蠕虫病毒重要的破坏方式是大量的复制自身，然后在网络中传播，严重的占用有限的网络资源，使用户不能通过网络进行正常的工作。有一些蠕虫病毒还具有更改用户文献、将用户文献自动当附件转发的功能，并且这类的病毒往往会频繁大量的出现变种，一旦中毒往往会导致数据丢失、个人信息失窃、网络或系统运营异常等。目前该类病毒重要的传播途径有电子邮件、系统漏洞、聊天软件等。如“尼姆达”病毒、“冲击波”、“震荡波”等都属于蠕虫病毒。

（三）特洛伊木马

特洛伊木马通常也被认为是通过网络传播的一种病毒。其特性重要是通过网络或者系统漏洞进入用户的系统并隐藏，然后向外界泄露用户的信息，它一般具有一个可视化的用户界面，能对用户的电脑进行远程控制。木马和黑客病毒往往是成对出现的，通常木马病毒负责侵入用户的电脑，而黑客病毒则通过该木马病毒来进行控制，以窃取用户的游戏账户、银行账户和信用卡、股票账户、个人通信及各种密码等方面信息。如“QQ 狩猎者”、“传奇窃贼”、“网游大盗”、“网银大盗”、“网络枭雄”、“黄金甲”等。

（四）破坏性程序病毒

这类病毒往往寄生于可执行程序之中，通过诱惑用户点击的方式来触发病毒代码的运营，这类病毒的运营会直接对用户计算机产生较大的破坏。如格式化 C 盘、熊猫烧香等病毒都属于此类病毒。

（五）网页脚本病毒

脚本病毒依赖一种特殊的脚本语言(如 VBScript、JavaScript 等)起作用，同时需要主软件或应用环境可以对的辨认和翻译这种脚本语言中嵌套的命令。脚本病毒在某方面与宏病毒类似，但脚本病毒可以在多个产品环境中进行，还能在其他所有可以辨认和翻译它的产品中运营，它是重要通过网页进行传播的病毒。脚本语言比宏语言更具有开放终端的趋势，这样使得病毒制造者对感染脚本病毒的机器可以有更多的控制力。如红色代码(Script.Redlof)、欢乐时光(VBS.Happytime)、十四日(Js.Fortnight.c.s)等。

三、技术分析

（一）病毒的特点

1．感染性

感染性是病毒的主线属性，病毒具有把自身复制到其它程序中的特性。在适当的条件下，计算机病毒可通过各种也许的渠道，如软盘、计算机网络去传染其他未被感染的计算机，在某些情况下导致被感染的计算机工作失常甚至瘫痪。 病

毒一旦进入计算机并执行，它就会搜寻其他符合其传染条件的程序或存储介质，拟定目的后再将自身代码插入其中，达成自我繁殖的目的。

只要一台计算机染毒，如不及时解决，那么病毒就会在这台机器上迅速扩散，计算机中的大量文献会被感染、破坏甚至删除，与此同时，被感染的文献又成了新的传染源，在与其他机器进行通信或网络接触时，病毒再继续进行传染，感染并破坏它所能接触到的所有机器、这样的感染最终会形成一个恶性循环，并导致极坏的影响。

2．潜伏性

潜伏性是指病毒具有依附于其他媒体的寄生能力。病毒通过修改其他程序而把自身的复制品嵌入到其他程序或磁盘的引导区寄生。大多数病毒都采用特殊的隐藏技术，进入系统之后一般不会立即发作，而是等待特定的时间或者指令才发作。

例如有些病毒感染程序时会将原程序压缩，并嵌入病毒程序。它可以在几周或者几个月内甚至几年内隐藏在合法文献中，一旦时机成熟，得到运营机会，就可以四处繁殖、扩散，继续为害，对其他系统进行传染，而不被人发现。潜伏性愈好，其在系统中的存在时间就会愈长，病毒的传染范围就会愈大。

3．可触发性

病毒因某个事件或数值的出现，诱使病毒实行感染或进行袭击的特性称为可触发性。病毒既要隐蔽又要维持杀伤力，它必须具有可触发性。病毒的触发机制就是用来控制感染和破坏动作的频率的。病毒具有预定的触发条件，这些条件也许是时间、日期、文献类型或某些特定数据等。病毒运营时，触发机制检查预定条件是否满足，假如满足，启动感染或破坏动作，使病毒进行感染或袭击；假如不满足，使病毒继续潜伏。

4．破坏性

所有的计算机病毒都是一种存在破坏威胁的可执行程序。对系统来说，所有的计算机病毒都存在一个共同的危害，即减少计算机系统的工作效率，占用系统资源，其具体情况取决于入侵系统的病毒程序。

假如病毒设计的目的在于彻底破坏系统的正常运营的话，那么这种病毒对计算机系统进行袭击导致的后果是难以设想的，它可以毁掉系统的部分数据，也可以破坏所有数据并使之无法恢复。在特定的情况下，病毒甚至可以产生极其恶劣的破坏作用，它可以直接破坏你的硬件，让设备彻底报废，计算机所有的数据也会荡然无存。

5．衍生性

分析计算机病毒的结构可知，传染的破坏部分反映了设计者的目的。但是，这可以被其他掌握原理的人以其个人的企图进行任意改动，从而又衍生出一种不同于原版本的新的计算机病毒（又称为变种），这就是计算机病毒的衍生性。这种特性为一些好事者提供了一种发明新病毒的捷径。

（二）计算机的易感文献

1．用户浏览器

根据国家计算机病毒应急解决中心每年发布的《全国信息网络安全状况与计算机和移动终端病毒疫情调查》来看，每年感染病毒的计算机设备中 67%是由于浏览器访问网页时感染的，浏览器仍然是病毒、木马袭击计算机的最重要入口。