

# 浅谈计算机病毒及其防范措施

商红伟

(兴城市职业教育中心 辽宁 兴城 125100)

**[摘要]**随着计算机技术的迅速发展,给我们的工作和生活提供了便利,并大大的提高了效率,所以计算机在社会生活以及各个领域广泛使用,但同时也渗透了计算机病毒到社会的各个领域。病毒给计算机系统造成巨大的破坏,还有我们想象不到的威胁,严重的干扰我们的正常生活和工作,而且通过互联网的传播,病毒的危害不断扩大,也会带来巨大的经济损失。

**[关键词]**计算机;病毒;防范;处理

**[DOI]** 10.12252/j.issn.2096-6288.2021.04.1263

## 一. 计算机病毒的含义

计算机病毒,英文名为Computer Virus。计算机病毒是一个程序,一段可执行码,但与别的计算机程序不同,是编制者在计算机程序中插入的破坏计算机功能或者数据的代码,能影响计算机的使用。和我们所熟知的生物病毒类似,它自己独特的复制能力。计算机病毒与人体生理病毒类似,也具有自己独特的特点:传播性,隐蔽性,感染性,潜伏性,可激发性,表现性,破坏性。

## 二. 计算机病毒的传播和危害

早期网络不发达的时候,只是通过单机的计算机软件的安装感染计算机病毒,随着网络的发展和时代的进步,用户更喜欢直接网上下载软件,音乐,视频,游戏,这样也大大提高了把病毒下载下来的概率,病毒就会感染计算机。

1. 网站上的下载资源传播和感染。
2. U盘“闪存”技术也会传染计算机病毒。
3. 网络木马程序。
4. “钓鱼”网站。

## 三. 计算机病毒的引导过程机制

计算机病毒实际上是一种特殊的程序,存储在磁盘上的,磁盘也就是病毒的寄生对象。病毒的寄生对象有两种:一种是寄生在磁盘引导扇区;另一种是寄生在可执行文件中。计算机病毒程序寄生在寄生对象上,获得执行权后,就会进入计算机系统,然后破坏操作系统,损坏等破坏活动。

计算机病毒的引导过程包括以下三方面:一是驻留内存;二是窃取系统控制权;三是恢复系统功能。病毒驻留内存以便于其发挥破坏作用,为此需要开辟内存空间或者占用部分内存空间。在病毒程序驻留内存后,必须使有关部分代替或扩大系统原有功能,并窃取系统的控制权。然后病毒程序依据设计思想,隐蔽自己,等待时机,在触发条件触发时,达到对计算机进行破坏的目的。病毒还具有隐蔽性,隐藏自己,驻留内存后,对系统进行恢复,系统正常运行,这样就可以悄悄的静待时机来临,达到攻击系统并破坏系统的目的。

## 四. 计算机病毒的触发机制

感染,潜伏,可触发,破坏是计算机病毒的基本特性。计算机病毒一般都有一个或几个触发条件,满足其触发条件或者激活病毒的传染机制,使之进行感染。触发其实就是一种条件的控制,设计者设计一个程序让病毒在一定的条件下实施攻击。目前病毒采用的触发条件主要有以下几种:日期触发,时间触发,键盘触发,感染触发,启动触发,访问磁盘次数触发,调用中断功能触发,其他触发机制。比如说输入某个特定的字符,某个特定的日期或者时刻,击某个键的次数,组合键,热启动键,机器的启动次数,病毒对磁盘的访问次数,或者是病毒内置的计数器达到一个一定的次数等等。病毒的重要部分是有关触发机制的编码。分析病毒时,如果搞清楚病毒的触发机制,可以修改此部分代码,这样病毒就没有攻击性,可以成为研究的案例。

## 五. 计算机病毒的破坏机制

根据现有的计算机病毒资料,可以把计算机病毒的破坏目标和攻击部位归纳如下:一是攻击系统数据区。二是攻击文

件。三是攻击内存。四是干扰系统运行。五是速度下降。六是攻击磁盘。七是扰乱屏幕显示。八是键盘输入紊乱。

## 六. 计算机病毒的预防

加强计算机网络病毒的防治,想十分有效地杜绝和防止计算机病毒的蔓延,光靠技术手段是不可能的,只有把技术手段和管理机制紧密结合起来,并让人们提高安全防范意识,所以计算机病毒防治的基本方法是预防为主,杀毒为辅,必须备份,及时升级。防治病毒的侵入要比病毒入侵后再去发现和消除它更重要。

那么如何防范计算机病毒呢,大致归纳如下几点:

1. 尽量使用正版的杀毒软件,并及时升级,定时对计算机进行病毒检查。不要轻易下载小网站的软件与程序。计算机病毒日益增多,安装杀毒软件对计算机进行杀毒是最经济的选择。安装杀毒软件的同时安装病毒防火墙,这样才能及时发现和阻止病毒对计算机的攻击和感染。
2. 对硬盘做DOS和FORMAT格式化以防止硬盘有隐藏的病毒。
3. 用户为了方便和价格便宜在网络上下载的软件或者盗版软件,这样的软件在使用之前,要先进行检查。因为这样的软件里往往可能藏着病毒。
4. 及时对使用的软件和杀毒软件进行补丁修补与升级,这样才能保证识别与查杀新病毒,保证计算机系统不被病毒所破坏。
5. 注意网址的正确性,不误入假的山寨网站。养成良好的上网安全习惯。陌生人发来的来历不明的文件网址不随意打开,这些习惯会让计算机更安全。不要光顾那些很诱人的不良小网站,很可能存在风险或者就是网络陷阱。

6. 经常注意计算机系统的工作状况,留心计算机有无异常。出现异常,进行分析,及时处理,将病毒杀死,避免传给整个计算机系统或整个磁盘。

- 7) 用软盘或者光盘的时候,不要先随便打开程序或安装,先复制到我们计算机的硬盘上,杀毒一下,确保安全后再去打开程序或者安装。

除了以上这些防范措施,还要尽量使用复杂的密码,对提高计算机的安全系数也是一个重要保证。而且我们应该提高对计算机病毒的认识,掌握更多的知识,预防与避免计算机感染病毒。

## 参考文献

- [1] 王恒青. 新时期计算机病毒的动态分析与防范[J]. 科技信息(学术研究), 2007.
- [2] 徐东亮. 关威. 计算机病毒的防范[J]. 黑龙江气象. 2002.
- [3] 张智勇. 浅析计算机病毒及防范的措施[J]. 黑龙江科技信息, 2007.
- [4] 刘孝国. 浅析计算机病毒与防范措施[J]. 实验室科学, 2007.
- [5] 王雨. 计算机病毒及防范措施[J]. 科技信息(科学·教研), 2008, (13)
- [6] 马国富, 李春雨. 浅谈计算机病毒及防范措施[J]. 电脑知识与技术(学术交流), 2007, (14)
- [7] 李志国. 论计算机病毒[J]. 科技信息(科学·教研) 2007, (29).