计算机病毒的危害

作者：小六 来源：网友投稿

本文原地址：https://xiaorob.com/fanwen/cankao/15396.html

计算机病毒的危害

阅读精选（1）：

计算机病毒的危害

计算机病毒的危害，正是由于计算机病毒的危害作用强大，才有这么多的杀毒软件、计算机保护方式。计算机病毒的的危害主要有哪些，我们如何防治计算机病毒的危害，在这样计算机病毒的危害泛滥的状况下我们还敢不敢使用远程控制软件，远程控制软件安全性能到达几何才能让人放心使用。

网络人远程控制软件安全级别远高于同行业，且不论它透过了国内各大安全厂商的安全检测认证，更是在2011年12月获得国家公安部安全监测认证以及销售许可证双重认证，并且是国内唯一一款使用U盾银行安全级别的远程控制软件。在这个计算机病毒的危害不断爆出来的时代，网络人远程控制软件无异于给慌张的人们一剂镇心剂。

下方网络人远程控制软件跟大家探讨一些计算机病毒的危害：

1计算机病毒的危害之一：电脑运行缓慢。当你的电脑出现打开网页很慢、操作其他也都很慢的状况，一般会首先清理系统垃圾，之后处理些该处理的插件，完之后再全面扫描查杀病毒，如果不行再重装系统。计算机病毒的危害会导致电脑运行缓慢，病毒运行时不仅仅要占用内存，还会抢占中断，干扰系统运行，这必然会使系统运行缓慢。

2计算机病毒的危害之二：消耗内存以及磁盘空间。当你发现自我的电脑并没有运行多少程序而系统内存已经被超多占用了，那么你的电脑可能已经收到了计算机病毒的危害。因为很多病毒在活动状态下都是常驻电脑内存的，尤其是文件感染类型的病毒，会不断超多感染违背计算机病毒危害过的文件，计算机病毒的危害会造成磁盘空间严重冗积。

3计算机病毒的危害之三：破坏硬盘以及电脑数据

4计算机病毒的危害之四：狂发垃圾邮件或其他信息，造成网络堵塞或瘫痪

5计算机病毒的危害之五：计算机病毒给用户造成严重的心理压力

6计算机病毒的危害之六：窃取用户保密、机密文件、账号信息等。这就是大部分木马病毒计算机病毒的危害的目的。大部分都是以窃取用户信息，以获取经济利益为目的，如窃取用户资料，网银账号密码，网游账号密码等。一旦这些信息失窃，将给用户带来不少经济损失。因此我们在这样的计算机病毒的危害环境之下不能说用户在使用远程控制软件的过程当中会有很多的顾虑，顾虑太多。正规的远程控制软件并不是木马病毒，就像网络人远程控制软件，需要双方电脑都安装软件方可进行远程控制、远程办公使用。

阅读精选（2）：

计算机病毒的危害以及症状

在计算机病毒出现的初期，说到计算机病毒的危害，往往注重于病毒对信息系统的直)接破坏作用，比如格式化硬盘、删除文件数据等，并以此来区分恶性病毒和良性病毒。其实这些只是病毒劣迹的一部分，随着计算机应用的发展，人们深刻地认识到凡是病毒都可能对计算机信息系统造成严重的破坏。

计算机病毒的主要危害

计算机病毒的主要危害有：

1。病毒激发对计算机数据信息的直接破坏作用

大部分病毒在激发的时候直接破坏计算机的重要信息数据，所利用的手段有格式化磁盘、改写文件分配表和目录区、删除重要文件或者用无好处的“垃圾”数据改写文件、破坏CMO5设置等。磁盘杀手病毒(D1SKKILLER)，内含计数器，在硬盘染毒后累计开机时光48小时内激发，激发的时候屏幕上显示“Warning!!Don'tturnoffpowerorremovediskettewhileDiskKillerisProsessing!”(警告!D1SKKILLERll1在工作，不要关掉电源或取出磁盘)，改写硬盘数据。被D1SKKILLER破坏的硬盘能够用杀毒软件修复，不要轻易放下。

2。占用磁盘空间和对信息的破坏

寄生在磁盘上的病毒总要非法占用一部分磁盘空间。引导型病毒的一般侵占方式是由病毒本身占据磁盘引导扇区，而把原先的引导区转移到其他扇区，也就是引导型病毒要覆盖一个磁盘扇区。被覆盖的扇区数据永久性丢失，无法恢复。文件型病毒利用一些DOS功能进行传染，这些DOS功能能够检测出磁盘的未用空间，把病毒的传染部分写到磁盘的未用部位去。所以在传染过程中一般不破坏磁盘上的原有数据，但非法侵占了磁盘空间。一些文件型病毒传染速度很快，在短时光内感染超多文件，每个文件都不一样程度地加长了，就造成磁盘空间的严重浪费。

3。抢占系统资源

除VIENNA、CASPER等少数病毒外，其他大多数病毒在动态下都是常驻内存的，这就必然抢占一部分系统资源。病毒所占用的基本内存长度大致与病毒本身长度相当。病毒抢占内存，导致内存减少，一部分软件不能运行。除占用内存外，病毒还抢占中断，干扰系统运行。计算机操作系统的很多功能是透过中断调用技术来实现的。病毒为了传染激发，总是修改一些有关的中断地址，在正常中断过程中加入病毒的“私货”，从而干扰了系统的正常运行。

4。影响计算机运行速度

病毒进驻内存后不但干扰系统运行，还影响计算机速度，主要表此刻：

(1)病毒为了决定传染激发条件，总要对计算机的工作状态进行监视，这相对于计算机的正常运行状态既剩余又有害。

(2)有些病毒为了保护自我，不但对磁盘上的静态病毒加密，而且进驻内存后的动态病毒也处在加密状态，CPU每次寻址到病毒处时要运行一段解密程序把加密的病毒解密成合法的CPU指令再执行;而病毒运行结束时再用一段程序对病毒重新加密。这样CPU额外执行数千条以至上万条指令。

(3)病毒在进行传染时同样要插入非法的额外操作，个性是传染软盘时不但计算机速度明显变慢，而且软盘正常的读写顺序被打乱，发出刺耳的噪声。

5。计算机病毒错误与不可预见的危害

计算机病毒与其他计算机软件的一大差别是病毒的无职责性。编制一个完善的计算机软件需要耗费超多的人力、物力，经过长时光调试完善，软件才能推出。但在病毒编制者看来既没有必要这样做，也不可能这样做。很多计算机病毒都是个别人在一台计算机上匆匆编制调试后就向外抛出。反病毒专家在分析超多病毒后发现绝大部分病毒都存在不一样程度的错误。

错误病毒的另一个主要来源是变种病毒。有些初学计算机者尚不具备独立编制软件的潜力，出于好奇或其他原因修改别人的病毒，造成错误。

计算机病毒错误所产生的后果往往是不可预见的，反病毒工作者以前详细指出黑色星期五病毒存在9处错误，乒乓病毒有5处错误等。但是人们不可能花费超多时光去分析数万种病毒的错误所在。超多内含未知错误的病毒扩散传播，其后果是难以预料的。

6。计算机病毒的兼容性对系统运行的影响

兼容性是计算机软件的一项重要指标，兼容性好的软件能够在各种计算机环境下运行，反之兼容性差的软件则对运行条件“挑肥拣瘦”，要求机型和操作系统版本等。病毒的编制者一般不会在各种计算机环境下对病毒进行测试，因此病毒的兼容性较差，常常导致死机。

7。计算机病毒给用户造成严重的心理压力

据有关计算机销售部门统计，计算机售后用户怀疑“计算机有病毒”而提出咨询约占售后服务工作量的60%以上。经检测确实存在病毒的约占70%，另有30%状况只是用户怀疑，而实际上计算机并没有病毒。那么用户怀疑病毒的理由是什么呢?多半是出现诸如计算机死机、软件运行异常等现象。这些现象确实很有可能是计算机病毒造成的。但又不全是，实际上在计算机工作“异常”的时候很难要求一位普通用户去准确决定是否是病毒所为。

大多数用户对病毒采取宁可信其有的态度，这对于保护计算机安全无疑是十分必要的，然而往往要付出时光、金钱等方面的代价。仅仅怀疑病毒而冒然格式化磁盘所带来的损失更是难以弥补。不仅仅是个人单机用户，在一些大型网络系统中也难免为甄别病毒而停机。总之计算机病毒像“

幽灵”一样笼罩在广大计算机用户心头，给人们造成巨大的心理压力，极大地影响了现代计算机的使用效率，由此带来的无形损失是难以估量的。

阅读精选（3）：

在计算机病毒出现的初期，说到计算机病毒的危害，往往注重于病毒对信息系统的`直）接破坏作用，比如格式化硬盘、删除文件数据等，并以此来区分恶性病毒和良性病毒。其实这些只是病毒劣迹的一部分，随着计算机应用的发展，人们深刻地认识到凡是病毒都可能对计算机信息系统造成严重的破坏。

计算机病毒的主要危害有：

1．病毒激发对计算机数据信息的直接破坏作用

大部分病毒在激发的时候直接破坏计算机的重要信息数据，所利用的手段有格式化磁盘、改写文件分配表和目录区、删除重要文件或者用无好处的“垃圾”数据改写文件、破坏CMO5设置等。磁盘杀手病毒（D1SKKILLER），内含计数器，在硬盘染毒后累计开机时光48小时内激发，激发的时候屏幕上显示“Warning!!Don'tturnoffpowerorremovediskettewhileDiskKillerisProsessing！”（警告！D1SKKILLERll1在工作，不要关掉电源或取出磁盘），改写硬盘数据。被D1SKKILLER破坏的硬盘能够用杀毒软件修复，不要轻易放下。

从广义上定义，凡能够引起计算机故障，破坏计算机数据的程序统称为计算机病毒。依据此定义，诸如逻辑炸弹，蠕虫等均可称为计算机病毒。1994年2月18日，我国正式颁布实施了《中华人民共和国计算机信息系统安全保护条例》，在《条例》第二十八条中明确指出：“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者毁坏数据，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。”此定义具有法律性、权威性。

2抢占系统资源

除VIENNA、CASPER等少数病毒外，其他大多数病毒在动态下都是常驻内存的，这就必然抢占一部分系统资源。病毒所占用的基本内存长度大致与病毒本身长度相当。病毒抢占内存，导致内存减少，一部分软件不能运行。除占用内存外，病毒还抢占中断，干扰系统运行。计算机操作系统的很多功能是透过中断调用技术来实现的。病毒为了传染激发，总是修改一些有关的中断地址，在正常中断过程中加入病毒的“私货”，从而干扰了系统的正常运行。

3．影响计算机运行速度

病毒进驻内存后不但干扰系统运行，还影响计算机速度，主要表此刻：

（1）病毒为了决定传染激发条件，总要对计算机的工作状态进行监视，这相对于计算机的正常运行状态既剩余又有害。

（2）有些病毒为了保护自我，不但对磁盘上的静态病毒加密，而且进驻内存后的动态病毒也处在加密状态，CPU每次寻址到病毒处时要运行一段解密程序把加密的病毒解密成合法的CPU指令再执行；而病毒运行结束时再用一段程序对病毒重新加密。这样CPU额外执行数千条以至上万条指令。

（3）病毒在进行传染时同样要插入非法的额外操作，个性是传染软盘时不但计算机速度明显变慢，而且软盘正常的读写顺序被打乱，发出刺耳的噪声。

4．计算机病毒错误与不可预见的危害

计算机病毒与其他计算机软件的一大差别是病毒的无职责性。编制一个完善的计算机软件需要耗费超多的人力、物力，经过长时光调试完善，软件才能推出。但在病毒编制者看来既没有必要这样做，也不可能这样做。很多计算机病毒都是个别人在一台计算机上匆匆编制调试后就向外抛出。反病毒专家在分析超多病毒后发现绝大部分病毒都存在不一样程度的错误。错误病毒的另一个主要来源是变种病毒。有些初学计算机者尚不具备独立编制软件的潜力，出于好奇或其他原因

修改别人的病毒，造成错误。计算机病毒错误所产生的后果往往是不可预见的，反病毒工作者以前详细指出黑色星期五病毒存在9处错误，乒乓病毒有5处错误等。但是人们不可能花费超多时光去分析数万种病毒的错误所在。超多内含未知错误的病毒扩散传播，其后果是难以预料的。

5．计算机病毒的兼容性对系统运行的影响

兼容性是计算机软件的一项重要指标，兼容性好的软件能够在各种计算机环境下运行，反之兼容性差的软件则对运行条件“挑肥拣瘦”，要求机型和操作系统版本等。病毒的编制者一般不会在各种计算机环境下对病毒进行测试，因此病毒的兼容性较差，常常导致死机。

6．计算机病毒给用户造成严重的心理压力

据有关计算机销售部门统计，计算机售后用户怀疑“计算机有病毒”而提出咨询约占售后服务工作量的60%以上。经检测确实存在病毒的约占70%，另有30%状况只是用户怀疑，而实际上计算机并没有病毒。那么用户怀疑病毒的理由是什么呢？多半是出现诸如计算机死机、软件运行异常等现象。这些现象确实很有可能是计算机病毒造成的。但又不全是，实际上在计算机工作“异常”的时候很难要求一位普通用户去准确决定是否是病毒所为。大多数用户对病毒采取宁可信其有的态度，这对于保护计算机安全无疑是十分必要的，然而往往要付出时光、金钱等方面的代价。仅仅怀疑病毒而冒然格式化磁盘所带来的损失更是难以弥补。不仅仅是个人单机用户，在一些大型网络系统中也难免为甄别病毒而停机。总之计算机病毒像“幽灵”一样笼罩在广大计算机用户心头，给人们造成巨大的心理压力，极大地影响了现代计算机的使用效率，由此带来的无形损失是难以估量的。

电脑病毒对电脑系统能够造成很大的影响。大部份的病毒都是把电脑程式及数据破坏。下方描述了病毒制造的不一样破坏及影响。

有些电脑病毒例如FormatC(macrovirus)及StonedDaniela，当它们被触发时，会无条件地把硬磁碟格式化及删除磁碟上所有系统档案。

以AOL4FreeTrojanHorse为例子，它附在电子邮件讯息上并以AOL4FREE。COM为档案名。其实它是用DOS的公用程式(utility)--BATEXEC1。5版本由成批文件(batchfile)转换过来的〔这个公用程式是用来转换一些很大的成批文件去更快的速度〕。

这个TrojanHorse首先会在DOS裏的不一样目录找寻DELTREE。EXE这个档案，然后用这个档案把硬磁碟裏的所有档案删除。当档案被删除后，它会显示一个DOS错误讯息:”BadCommandorfilena

me〃以及一个猥亵的讯息(obscenemessage)。如果这病毒找不到DELTREE。EXE的话，它就不能把档案删除，但猥亵的讯息(obscenemessage)仍会出现。

有些病毒，如Monkey(Stoned。Empire。Monkey)及AntiEXE，会感染主启动记录(MasterBootRecordMBR)及DOS启动磁区(DosBootSector)，之后它会降低记忆体及硬磁碟的效能，直至当我们的用电脑时萤光幕上显示一些讯息或有其他损坏。

以AntiEXE为例子，在启动过程时载入的主启动记录(MBR)，该病毒会把这个没有被感染的MBR贮存在硬磁碟中柱(Cylinder)O，边(Side)O，磁区(Sector)13的位置。

然后病毒会把它的病毒编码放在MBR裏，并且把已感染的MBR写在硬磁碟中柱(Cylinder)O，边(Side)O，扇区(Sector)1的位置。

当AntiEXE病毒在记忆体活跃时，它就会把由任何磁碟读取得来的有毒

MBR及\或DBS重新传入一个清洁相同的地区(cleancounterpart)。

随著在磁碟读取过程时把MBR及\或DBS安放，病毒会找寻一特定的*。EXE档案(它的身份到此刻还没有明白)，然后把档案破坏。