

# 电力系统 U 盘病毒防护浅析

周海峰

(南通供电公司, 江苏 南通 226006)

**摘 要:**随着计算机技术的普及和发展,计算机在人们的工作、生活中起到了越来越重要的作用,计算机病毒也随着计算机的发展而日益猖獗,U 盘因其使用的灵活性,在电力系统中作为存储、交换数据的重要工具得到了广泛的应用,同时也成了病毒常见的攻击目标,给电力系统数据信息带来了严重的安全隐患。正确的使用 U 盘,合理有效的预防和防治 U 盘病毒是我们必须面对和处理的问题。

**关键词:**U 盘病毒; 防护; 安全; autorun

## 0 引言

随着计算机技术的普及和发展,计算机在各行各业中已经得到了广泛的应用,同时计算机病毒也成了困扰计算机系统安全的一个重要问题,其中因 U 盘、移动硬盘、存储卡等移动存储设备的广泛使用,U 盘已成为病毒和恶意木马程序传播的主要途径。企业员工掌握一定的 U 盘病毒传播的原理以及防护方法,对于企业信息安全工作非常重要。

本文通过对计算机病毒的介绍,针对 U 盘病毒的传播方式、危害,分析了 U 盘病毒的特征,提出一些防范和处理 U 盘病毒的方法,以及企业工作人员正确使用 U 盘的注意事项。减少病毒对工作、生活带来的危害,给企业信息安全创造良好的计算机环境。

## 1 计算机病毒

计算机病毒(Computer Virus)在《中华人民共和国计算机信息系统安全保护条例》中被明确定义,病毒指“编制者在计算机程序中插入的破坏计算机功能或者破坏数据,影响计算机使用并且能够自我复制的一组计算机指令或者程序代码”。计算机病毒是某些人利用计算机软件 and 硬件所固有的脆弱性编制的一组指令集或程序代码。它通过某种途径潜伏在计算机的存储介质(或程序)里,当达到某种条件时即被激活,通过修改其他程序的方法将自己的精确拷贝或者可能演化的形式放入其他程序中,从而感染其他程序,对计算机资源进行破坏。

## 2 计算机病毒的特征

归纳起来,计算机病毒有如下特点:

一是攻击隐蔽性强,病毒在攻击计算机后不易被用户发现。

二是繁殖能力强,病毒可以通过自身复制程序复制到与其连接的计算机、存储设备上。

三是传染途径广。病毒可以通过移动存储设备、网络、硬件设备、即时通信系统(如 msn, QQ)等多渠道自动侵入计算机中,并不断蔓延。

四是潜伏性。病毒可以潜伏在计算机系统而不造成破坏,等满足一定条件后,就启动病毒破坏程序。

五是破坏力大。计算机病毒一旦发作,轻则影响计算机的正常运行,重则破坏磁盘数据、删除、篡改数据文件,使文件丢失,甚至泄露重要的企业用户机密数据,使个人或公司损失惨重,造成严重的信息安全事故。

六是针对性强。计算机病毒的设计是为了某种特殊的需要,在不同环境和时机的要求下实施攻击。

根据江民病毒疫情监测预警中心 2011 年全年统计数据,发现病毒种类:126164 种。病毒发现数量:11102226 个。病毒感染计算机数量:3743721 台。新病毒种类:66686 种。新病毒发现数量:2908451 个。新病毒感染计算机数量:1267503 台。其中排名前 5 的病毒感染情况如见表 1。

表 1 2011 年江民病毒疫情监测预警中心病毒排名前五名数据

排名	英文名称	中文名称	所占百分比/%	感染计算机数量
1	Checker/Autorun	“U盘寄生虫”	3.06	114708
2	Worm/Kido.aeb	“刻毒虫”变种aeb	2.42	90566
3	Checker/HideFolder	“文件夹寄生虫”变种	0.91	34116
4	Trojan/Generic.rmn	暂无	0.56	20938
5	AutoCAD/Virus.b	暂无	0.53	19928

由表 1 可见,“U 盘寄生虫病毒”在计算机系统感染情况最为严重。如何防范 U 盘病毒成为我们必须重视的工作。

### 3 U 盘病毒

U 盘病毒并不是具体某一个病毒,也不是只通过 U 盘来传播的病毒,而是指所有可以通过 U 盘来进行传播的病毒。因为 U 盘作为一种被广泛使用的数据存储、交换工具,U 盘病毒的数量与日俱增,国家计算机病毒处理中心发布公告称 U 盘已成为病毒和恶意木马程序传播的主要途径。U 盘病毒主要通过自动播放功能以及 Autorun 文件实现打开 U 盘时自动运行病毒程序,并将病毒程序复制到计算机系统中从而使计算机中毒,同时中毒的计算机又会感染接入该计算机的 U 盘。

### 4 U 盘病毒的特征

U 盘病毒又称 Autorun 病毒,是通过 AutoRun.inf 文件使用户所有的硬盘完全共享或中木马的病毒;能通过产生 AutoRun.inf 进行传播的病毒,都可以称为 U 盘病毒。随着 U 盘、移动硬盘、存储卡等移动存储设备的普及,U 盘病毒也开始泛滥。病毒首先向 U 盘写入病毒程序,然后更改 autorun.inf 文件。autorun.inf 文件记录用户选择何种程序来打开 U 盘。如果 autorun.inf 文件指向了病毒程序,那么 Window 就会运行这个程序,引发病毒。一般病毒还会检测插入的 U 盘,并对其实行上述操作,导致一个新的病毒 U 盘的诞生。当用户把 U 盘接入受感染的计算机或者拷贝了带有 U 盘病毒的文件都有可能感染 U 盘病毒。当用户使用受感染的 U 盘时,通过计算机系统自动播放或者用户的双击运行,U 盘中的指向病毒程序的 autorun.inf 文件就会启动而造成破坏。

### 5 使用安全 U 盘

国家电网公司推广实施的安全移动存储介质系统是通过专用注册工具对普通的 U 盘或者移动硬盘内数据经过高强度算法加密,根据需要对 U 盘进行数据区划分(一般划分为交换区和保密区),使其具有较高安全性能的安全 U 盘。

用户在授权计算机使用安全 U 盘时,输入安全密码可以读取和写入安全 U 盘中交换区和保密区内

的数据,而当安全 U 盘接入到非授权计算机时,只有交换区在输入密码后能登录,保密区则不能被打开。这种方式杜绝了用户双击 U 盘时计算机感染病毒的风险,降低了 U 盘和计算机之间相互复制传播病毒的几率,维护了公司计算机网络系统的安全,预防和控制了计算机病毒的感染、传播和扩散的途径,保证了公司信息系统的正常运行。

### 6 U 盘病毒的防护措施

除了使用 U 盘加密的方法降低病毒感染几率,针对 U 盘的特点和传播方式,我们还可以使用以下防护措施来防止 U 盘病毒的入侵:

#### (1) 关闭自动播放功能

一般情况下,计算机系统会默认打开接入 U 盘自动运行播放的功能,这时病毒就容易传播到计算机系统中。当用户接入 U 盘后,有的计算机系统会直接运行里面的 autorun.inf 文件,有的计算机弹出自动播放对话框,这种情况下计算机用户就要选择“不执行任何操作”选项。关闭了计算机自动播放功能后这种情况就不会出现。

关闭自动播放功能方法:在 Windows 下单击“开始”菜单—“运行”,输入“gpedit.msc”命令,进入“组策略”窗口,打开“本地计算机策略—用户配置—管理模板—系统”项,然后在窗口右边“设置”标题下,双击“关闭自动播放”关闭当前用户的自动播放功能;或者在“本地计算机策略—计算机配置—管理模板—系统”项,在窗口右边“设置”标题下,双击“关闭自动播放”关闭所有用户的自动播放功能。

#### (2) 修改注册表键值

在关闭 U 盘自动播放功能后,用户双击盘符后 U 盘病毒依然会自动运行感染系统,可以通过修改注册表来阻止双击自动运行 U 盘程序:打开注册表编辑器,找到如下注册项: HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2 右键单击“MountPoints2”设置该键值的权限,将 Administrators 组和 SYSTEM 组的完全控制项都设为拒绝。其中禁止 MountPoints2 的写入是为了阻止 Windows 读取 Autorun.inf 后添加新的右键菜单,阻止病毒菜单的出现,从而使病毒程序无法运行。

#### (3) 为每一个磁盘创建 Autorun.inf 文件夹

因为 U 盘病毒是利用 Autorun.inf 文件来进行传

播的,我们可以为每一个磁盘创建一个名为“Autorun.inf”的文件夹,如果有病毒要侵入时,这样病毒就无法再创建同名的 autorun.inf 文件,这时双击盘符也病毒程序也不会运行。

#### (4) 使用鼠标右键打开 U 盘

在接入 U 盘后,使用鼠标右键单击 U 盘盘符选择“打开”或者通过“资源管理器”窗口进入,因为双击 U 盘就是运行 U 盘程序,这样做可以避免运行 U 盘中的病毒程序。也可以在插入 U 盘前,按住“Shift”键,再插入 U 盘,过几秒后松开,这样也可以阻止 U 盘在插入计算机后自动运行 U 盘内的程序。

#### (5) 清除 U 盘病毒

如果计算机中了 U 盘病毒,可以进入安全模式,打开注册表编辑器,找到如下注册项:\HKEY\_CLASS\_ROOT\Drive\Shell,把所有的 Autorun 键值都删除。如果中毒比较严重,就需要下载 U 盘病毒专杀工具:例如 USBCleaner、USBKiller 等工具来清除,同时还需要检查计算机是否及时安装系统补丁,杀毒软件是否升级最新的病毒定义码等等。

## 7 结束语

为了维护公司计算机网络系统的安全,预防和控制计算机病毒的产生、感染、传播和扩散,保证公司各项应用系统的正常运行,国家电网公司推广实施的安全移动存储介质制作系统较好的解决了 U

盘病毒传播的问题,计算机使用人员要保证计算机安装防病毒工具,定期查杀病毒、木马、升级系统补丁程序,使用安全 U 盘并设置足够安全的密码,在使用外来 U 盘接入内网计算机进行数据交换前先查杀病毒、木马等恶意代码;在有涉密信息计算机上必须使用安全 U 盘并要专盘专用,确保数据单项传输;涉密 U 盘严禁在非涉密信息系统中使用以防感染病毒造成数据泄露。同时计算机用户要养成良好的移动存储设备使用习惯,安全 U 盘的正确、广泛使用和病毒防范意识提高,也是降低系统感染病毒、保护信息安全不可或缺的条件。

#### 参考文献:

- [1] 科教工作室. 玩转 BIOS 与注册表 [M]. 北京: 清华大学出版社, 2010.
- [2] 赖荣旭, 钟玮. 计算机病毒与防范技术 [M]. 北京: 清华大学出版社, 2011.
- [3] 周苏, 黄林国, 王文. 信息安全技术 [M]. 北京: 中国铁道工业出版社, 2009.
- [4] 民病毒疫情监测预警中心. 江民病毒疫情监测预警中心数据 [Z].

#### 作者简介:

周海峰 (1980—), 男, 江苏南通人, 本科, 助理工程师, 从事电力系统信息运维工作。