病毒的黑、灰、白理论

国际电脑安全协会主席
大卫.史坦博士(Dr.David Stang)

当电脑病毒、电脑安全等问题逐渐成为话题之际,事实上,安全之防范更重要的是"电脑使用伦理道德",因为基本上,电脑病毒的蔓延是一个"无解方程式",唯有不断宣传与教育使用者正确的电脑使用伦理,才能使病毒稍收炽旗。

然而"谈论病毒问题的结果是什么?"却有不同的意见。一派看法是只有通过对这问题的全面讨论,才能使人准备好采取适当的对付措施;另外一派看法则认为公开讨论,只会吸引对这个问题的注意及更多麻烦制造者的兴趣。

1.不同的声音

NSA NCSC FBI CIA*等对电脑安全关心的组织,并不喜欢谈论他们对此已知道什么,因为可能会因此暴露出已知的安全漏洞,而使系统容易受到破坏,但是相对地,安全专家则提出不同的看法,他们表示:如果这些机构不提供一些资料帮助的话,他们就无法从这些机构如何使其系统更安全的知识中获益。

许多厂商在他们的防毒产品中加入了隐藏的扫瞄串,致使病毒程式的作者必须要修改已存在的病毒,而不让扫瞄系统侦测到其病毒;但是使用者又常抱怨他们的扫瞄系统并不接受从其它资源之隐藏或非隐藏的扫瞄串。

此外,专门强调安全性的BBS*站,则常因为他们传布信息时,只要通过地下秘密的方式便可轻易获取,而备受评击。例如,在旧金山的COMSEC BBS站中是否该于其出版品"40HEX中发表有关病毒分解的文章。有些人认为应该,因为这些信息可能对安全性从业人员有所价值,有些人认为不应该,因为安全专家并不需要看病毒分解,而且其它人也不需要看。

我们常听到使用者说,他们觉的处理病毒问题的最好方法就是帮助人们发展对付病毒的第一手经验,而使任何有兴趣或确实想解决此问题的人能获得病毒。但为防有心人士趁机而入,故必须为其规格定下规范,如这些人之中,有些已经是防毒厂商,有些则明显地对某些病毒研究有兴趣,因而可通过此而成为"研究者的地位,并且酌收些许处理费用来提供病毒。

2.黑和白的世界

基本上,我们是居住在一个灰色的世界里,因此,我们不禁要问:给予病毒和收取处理费之间的差别是什么?将病毒给陌生人和给朋友之间的差别又是什么?

在多数办公室里,人们均试着与其用黑和白的绝对观点来看世界,不如用灰色的角度来看。先姑且不论其好坏,只是我们想强调:没有人应该有任何理由给任何人病毒,但我们也想说:好的病毒研究者应该去接近病毒。但问题是好人并没有戴上白帽,在一大群表面上灰色个人的病毒研究者之中,他们明显地曾做过好的和恶的,他们似乎是好人但却未获得我们的信任,甚至他们在取得我们的信任后似乎又要背判我们。

灰色论点在使用者身上更是清楚。我问班上同学是否有人相信防毒厂商?没有人举手。我又问是否有人相信:"防毒产品"包装盒后的说明?也没有人举手,相反的,我却几乎每周都被问到:"是否有厂商自行写病毒?"

当然,这论点已较两年前改善很多,当时,同学们均坚决相信病毒是厂商以某种秘密行动所投资,用来吓唬客户进而购买其产品,去年三月许多大众看到米开朗基罗病毒因厂商的鼓吹所引发的疯狂,葛瑞克尤特利在哥伦比亚广播公司晚间新闻中即访问我,是否认为这个米开朗基罗事件是个获取暴利的结果?我回答说我相信是有很多利益输送,因为厂商一般会表现很好,然后再表现真象。

然而这个说法却引起很多的异议,我想我可能欺骗了电视观众。在美国最大的防毒厂商们,在那个月每个厂商都多赚了一百万美元。

就 NCSA*的立场而言,不禁要问:若改为黑色论点,我们会做出什么呢?在任何地方我们都有立场吗?我想,不论何时我们都会强烈地感觉 NCSA 应该如此;我认为如果我们能够开始在某些有关病毒的道德问题表示立场,则某些灰色论点将会减少,而其它问题也会变得更清楚。

我相信写病毒程序是错的,特别是不容易被侦测到的或其中包括任何破坏码的病毒,但我并不确定所有的病毒是不是一样地"坏"。例如,提供其发病时间明显症状的病毒(像是 FLIP 或是 DEVILS DANCE)或是会不心地避开使用者资料的病毒(是 BRAIN 或是 FORM),虽然比起得用秘密技巧针对防毒产品或使用者档案,以及包括破坏码的病毒来说要好多了,但是换个角度来思索,我相信没有"好"病毒,因而所有的病毒都是坏的,虽然坏的程度不一,所以写病毒程式就是件坏事,这是无庸置疑的。

如果那是真的,那么你便能了解我对那些教人如何写病毒程序者的感觉是什么了,教人如何写病毒可能要比直接写还糟糕,因为每位老师能够使数十或数千位学生忙于撰写病毒程序;而有关如何撰写病毒的书籍不管写的好或者差,都和其主题一样坏,而且作者也和他们的书一样坏。

如果病毒是坏的,那么散布它们也是一样,因此散布病毒的 BBS 站和潜在客户分享它们的厂商,或者是提供它们给朋友或陌生人的青少年,不管是免费或收费,都是坏的。

3.病毒世界的道德观念

在我的黑色和白色世界中,你不是我组织中的一部份就是我的组织要有你。如果你经营一个病毒 BBS 站的话,我们会把你关机;如果你不写本有关如何撰写病毒的书,我们会将你列入黑名单而且还会杯葛你;如果你是提供客户病毒的厂商,我们希望设法让你为此恶行付出代价。

但是任何注意道德问题的人都会发现,他们自己经常用一个道德规范去妨害另一个;例如考虑我们有多重视言论自由,然后再想想写一本关于如何撰写病毒的书的问题。

我最近有个机会和马克卢德威辨论,他是一本解释如何撰写电脑病毒书籍的作者,我不确定谁赢了,因为观众早就站在我这边,卢德威先生几乎不反驳而且并位提出任何有关写这类书的强迫性理由。

我曾经看过这本书,就象你也可能会看,甚至我认为它写的不错,而且对任何想要写病毒的人有些帮助。

在辩论之中,卢德威先生提出这本书可以帮助那些想要了解病毒的人。我并不确定是否真是如此,因为它并未谈论那些现今在世界上漫游的病毒,卢德威病毒利用很多有趣的技巧,不是创新,也不是被一般病毒所必需使用的,而且尽管了解书中的每件事,你仍然一点也不知道 Jerusalen (耶路撒冷,黑色星期五) 或 STONED。

卢德威先生还坚信这本书对需要对抗病毒的经理会有所帮助,但从书中来看,这几乎不可能,因为书中并没有对搞病毒的解释,而且他建议用低阶格式化硬碟机的方法去除出现的档案病毒。

对我们来说,卢德威先生的动机仿佛是有革命性的,他提出了是否可以合法创造出售电脑病毒的问题,针对此,我们认为不行。

因为,言论自由不应该会危及到我们的资料,远超过我们的资料会危及到你自由的言论。类似卢德威先生般的病毒就如焚书般的在破坏电脑,那么,当他的病毒焚烧到我们的电子资料时,我们也不应该感到仁慈。

我希望卢德威先生会停止提供他目前的书,不再写他曾答应过其它有关病毒的书,其中之一是"刺探军事战略和现实生活的抨击以及挖掘武器系统的发展,破坏防毒防护等",我希望他会加入我们这一边,写一本关于如何击败病毒之有用的书,我希望卢德威先生会贡献一些从他第一本书的收入作为使用者防护基金,那将可以用于帮助防毒产品。

如果我的愿望没有通通实现,那么我们还可以再做些事情;我必须大声疾呼我们已经有够多的问题在我们的电脑上,实在没有必要教人们如何去创造更多问题。

注:

NSA　:美国安全协会
NCSC:　美国电脑安全委员会
FBI:　美国联邦调查局
CIA:　美国电讯情报局
BBS:　公共数据库服务网
NCSA:　美国电脑安全协会