感染病毒事件应急处置

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 感染病毒事件应急处置 | | | | |
| 一、人员及安排 | | | | |
| 姓名 | 职位 | 角色 | 职责 | 备注 |
| 姜兴振 | 副局长 | 总指挥 | 指导全局 |  |
| 赵烨 | 信息中心主任 | 副总指挥 | 现在人员安排，调度，工作安排。 |  |
| 王亚飞 |  | 现场指挥 | 协调现场工作 |  |
| 二、设备及软件 | | | | |
| 电脑，优盘，杀毒软件等设备 | | | | |
| 三、病毒种类、名称及危害 | | | | |
| 病毒 | 名称 | 危害 | | 备注 |
| 蠕虫病毒 | Worm | 蠕虫病毒是无须计算机使用者干预即可运行的独立程序，它通过不停的获得网络中存在漏洞的计算机上的部分或全部控制权来进行传播。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破坏数据和恶意篡改系统．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 | |  |
| 脚本病毒 | Script | 脚本病毒是主要采用脚本语言设计的计算机病毒。现在流行的脚本病毒大都是利用JavaScript和VBScript脚本语言编写。实际上在早期的系统中，病毒就己经开始利用脚本进行传播和破坏，不过专门的脚本型病毒并不常见。但是在脚本应用无所不在的今天，脚本病毒却成为危害最大、最为广泛的病毒，特别是当它们和一些传统的进行恶性破坏的病毒如CIH相结合时其危害就更为严重了。随着计算机系统软件技术的发展，新的病毒技术也应运而生，特别是结合脚本技术的病毒更让人防不胜防，由于脚本语言的易用性，并且脚本在现在的应用系统中特别是Internet应用中占据了重要地位，脚本病毒也成为互联网病毒中最为流行的网络病毒 | |  |
| 宏病毒 | Macro | 宏病毒是一种寄存在文档或模板的宏中的计算机病毒。一旦打开这样的文档，其中的宏就会被执行，于是宏病毒就会被激活，转移到计算机上，并驻留在Normal模板上。从此以后，所有自动保存的文档都会“感染”上这种宏病毒，而且其他用户打开了感染病毒的文档，又会转移到他的计算机上 | |  |
| 后门病毒 | Backdoor | 后门病毒的特性是通过网络传播，给系统开后门，给用户电脑带来安全隐患。2004年年初，IRC后门病毒开始在全球网络大规模出现。一方面有潜在的泄漏本地信息的危险，另一方面病毒出现在局域网中使网络阻塞，影响正常工作，从而造成损失。由于病毒的源代码是公开的，任何人拿到源码后稍加修改就可编译生成一个全新的病毒，再加上不同的壳，造成IRC后门病毒变种大量涌现。还有一些病毒每次运行后都会进行变形，给病毒查杀带来很大困难。 | |  |
| 种植程序病毒 | Dropper.BingHe2.2C | 病毒种植程序病毒这类病毒的公有特性是运行时会从体内释放出一个或几个新的病毒到系统目录下，由释放出来的新病毒产生破坏。 | |  |
| 破坏性程序病毒 | Harm | 破坏性程序病毒的特性是本身具有好看的图标来诱惑用户点击，当用户点击病毒时，病毒便会直接对用户计算机产生破坏。如格式化C盘（Harm.formatC.f）、杀手命令（Harm.Command.Killer）等 | |  |
| 玩笑病毒 | Joke | 玩笑病毒的也称恶作剧病毒。这类病毒的特性是本身具有好看的图标来诱惑用户点击，当用户点击这类病毒时，病毒会做出各种破坏操作来吓唬用户，其实病毒并没有对用户电脑进行任何破坏。 | |  |
| 捆绑机病毒 | Binder | 是一种和正常软件捆绑在一起的病毒，当用户运行这些捆绑病毒时，会表面上运行这些应用程序，然后隐藏运行捆绑在一起的病毒。 | |  |