网络上的病毒与防御

计算机连网,是九十年代的趋势。以往象孤岛的微机,由网络使彼此分享资料、数据及设备,形成一种迅速,功能强大的工作群(Work Group),使电脑使用更进一步提高。但是,随之而来的却是网络上数据资料的保密性及安全性问题。尤其是现在横行的电脑病毒,一旦经网络传播,对整个工作环境造成的干扰、损失比没有连网的情况更甚千倍。

病毒入侵网络的途径

电脑病毒入侵网络,一定是经由网络上的微机/工作站,再感染网络服务器的文件,然后再从文件的共享而传染其它微机/工作站。根据统计,在网络上病毒的感染是比未连网快 20 倍。网络上病毒的传播情况,可以用以下假设例子说明:

1.小石在早上 9 点上班后 Login 到网络上。

2.小石在它的微机/工作站上执行一个染上 Jer-b 病毒的 D-base 程序。

3.这种记忆体(内存)长驻型病毒于是感染了小石的 Memory(内存)。

4.小石又去执行网络服务器的文字处理软件(例如:Wordstar),他打的指令是 F:/WS。

5.于是 F:盘(即网络服务器的盘)上的文字处理软件(例如:Wordstar)的 W.EXC 程式便中了 Jer-B 病毒。

6.由于公司(单位)每个人都用文字处理。到上午九点四十五分,办公室(单位)内每部上网的(工作站)内存记忆体(Memory)中都有了 Jer-Bf 病毒。

7.最后,在当天每个被执行过的程序(无论在网络服务器上的或在各微机/工作站的)都感染了 Jer-B 病毒。

那些病毒可以传染网络系统

由于大多数网络系统都有自己 Security 结构,例如甲不能 Access 乙的文件,或文件可设只读(Read Only)。而且,DOS 一些中断向量(Interrupt)也为网络操作系统所取代;所以很多用户以为 DOS 病毒是不会感染网络。这是不正确的观念。其实,已有超过 500 种病毒可在网络上活跃。例如 JeruSalem 系列 Dark Avenger, Wolfman 等都可感染网络。

专门攻击网络系统的病毒

以上谈的病毒,都是一般的微机病毒,但现在欧美各地已出现一类专门来攻击网络系统的病毒,其中有一名为 GPE(GET Pase Word 1)的网络病毒最广泛的被人讨论。GPI 病毒据研究是耶路撒冷病毒的变种,但它被改写成为专门去破 Novevll 的安全结构。即使执行 GPI 病毒感染文件的用户是被 Netware(Novell)定义为使用权限最低者,GP1 病毒仍可以'往上'感染而达到如 Supervisor 只可以使用的文件。

GP1 病毒被用户执行后,便停留在微机工作站的随机记忆体中(Memory/RAM)。但是,它不象一般病毒使用 DOS 的中断向量(Interrupt)进行感染,而是一直等到 Novell 操作系统的长驻程序(即 IPX 和 NETX)被启动后,再去利用 21h 中断向量(Interrupt)的 OE3h 功能去进行传染的动作(Int21h 的 OE3h 是由 Novell Netware 的核心程序所控制的)。

一旦 Novell 的 IPX 及 NETX 程式启动后,GPI 病毒便会将目前使用者的使用权限改为最高权限,因而使 GPI 毫不受限制地在 Novell 网上横行。

在网络系统上防毒,可说是一件极困难的工作,因为网络基本的概念是共享资源。而防病毒的措施,就是要避免任何人使用资源。

一般防毒最有效的方法,就是以常驻式的监控程序,在每个程序被执行时,立即检查该程序是否被病毒感染,以便及时防止病毒扩散。但在网络系统上,由于网络服务器上并没有程序被执行,(所有程序都被调到工作站上执行)因此,这种防毒方法只能在工作站上使用。

美国 Trend Micro Device Inc 公司,在 1991 年 10 月和电脑巨人 Intel 公司签订合约,共同在 Novell 3.11 上,以 NLM(Netware Loadable Module)方式常驻在网络服务器开发了一套叫 LANPROTECT 的 NOVELL 网络防病毒技术。

LANPROTECT 已于 92 年 6 月正式面世,并已由美国电脑安全协会(National Computer Security Asso- ciation)及 Novell 公司担保,Novell 公司本身也在全球各办事处采用。Lanprotect 也为 92 美国唯一最畅销的网络防毒产品。

(美国电脑配件公司供稿)