南京大学
NANJING UNIVERSITY

？？

报告人：余锋根
于润 尹震

走近病毒

- the d

- 《中

统安全
保护
者在计
算机
或者
破坏
够自
我复
代码”。

走近病毒

- the origin of virus **The first hardware virus**

陈盈豪

走近病毒

- the development of virus

原始病毒阶段　混合型病毒阶段　多态性病毒阶段

攻击目标较单一；主要通过截获系统中断向量（硬件产生的终端信号）的方式监视系统的运行状态，并在一定的条件下对目标进行传染；病毒程序不具有自我保护的措施，容易被人们截获、分析和解剖。

攻击目标趋于混合型；采取更为隐蔽的方法驻留内存和文件；病毒传染目标后没有明显的特征；病毒程序往往采取了自我保护措施；出现许多病毒的变种等。

多态性病毒在每次传染时，嵌入宿主程序中的病毒程序大部分都是可变的。因此采用特征码检测非常困难。

走近病毒

- the development of virus

网络病毒阶段　　主动攻击型病毒阶段　　手机病毒阶段

随着国际互联网的发展……

依赖互联网络传播……

这些病毒利用操作系统的漏洞进行进攻型的扩散，并不需要任何媒介或操作，用户只要接入互联网络就有可能被感染。

……和多媒体信息服务方式传……利用手机发送短信、彩信……浏览网站，甚至会损毁SIM卡、芯片等硬件，导致使用者无法正常使用手机

走近病毒

- 1.破坏显示器
- 病毒可以通过篡改显示发电机参数来破坏显示器(分辨率、场频)。

- 2.超外频、加电压破坏CPU、显卡、内存等
- 通过改BIOS参数，加高CPU电压，或提高CPU的外频，使CPU和显卡、内存等外设超负荷工作而过热烧坏。

走近病毒

- 3.超“显频”破坏显卡
- 在Windows 注册表里改显频，显卡也就容易超负荷工作而烧坏。

- 4.破坏光驱
- 让光头走到盘片边缘无信号区域不停的读盘，光头读不到信号便加大发射功率不停地读，导致损坏。

走近病毒

- 5.破坏主板、显卡的FlashBIOS
- 这就是现在的CIH病毒破坏主板的方式。病毒用乱码冲掉了BIOS中的内容，使机器不能启动。

- 6.破坏硬盘
- 低级格式化对硬盘的寿命有较大的影响。 若病毒不停的对硬盘磁道做低级格式化，硬盘容量就会一点一点地被蚕食，磁道坏了，要再低级格式化。

7.浪费喷墨打印机的墨水

喷墨打印机的喷头易堵塞，为此特别发明了专门浪费墨水的“清洗喷头”功能，病毒不停调用该功能，导致墨水浪费

南京大学
NANJING UNIVERSITY

CIH病毒

```
VirusGame SEGMENT

ASSUME CS:VirusGame, DS:VirusGame, SS:VirusGame
ASSUME ES:VirusGame, FS:VirusGame, GS:VirusGame

; ******************************************************
; * Ring3 Virus Game Initial Program *
; ******************************************************

MyVirusStart:
push ebp

; ***********************************
; * Let's Modify Structured Exception *
; * Handing, Prevent Exception Error *
; * Occurrence, Especially in NT. *
; ***********************************

lea eax, [esp-04h*2]

xor ebx, ebx
xchg eax, fs:[ebx]

call @0
@0:
pop ebx

lea ecx, StopToRunVirusCode-@0[ebx]
push ecx
```

CIH病毒是一种能够破坏计算机系统硬件的恶性病毒。据目前掌握的材料来看，这个病毒产自台湾，最早随国际两大盗版集团贩卖的盗版光盘在欧美等地广泛传播，随后进一步通过Internet传播到全世界各个角落。

CIH病毒现已被认定是首例能够破坏计计算机系统硬件的病毒，同时也是最具杀伤力的恶性病毒。从破坏力看，CIH病毒对数据和硬件的破坏作用都是不可逆的。

从技术角度来看，CIH病毒实现了与操作系统的完美结合。

- 计算机病毒虽然主要作用在软件层面，不过，仍有部分病毒对硬件会造成一定损坏，能够：
- 1、破坏显示器；
- 2、超外频、加电压破坏CPU、内存；
- 3、超显屏破坏显卡等；

4、破坏光驱。

……

所以做好计算机病毒的预防与防治工作至关重要。

具体预防措施

- 1）注意对系统文件、重要可执行文件和数据进行写保护；
- 2）不使用来历不明的程序或数据；
- 3）尽量不用软盘进行系统引导；
- 4）不轻易打开来历不明的电子邮件；
- 5）使用新的计算机系统或软件时，要先杀毒后使用；
- 6）备份系统和参数，建立系统的应急计划等。
- 7）专机专用。
- 8）利用写保护。
- 9）安装杀毒软件。
- 10）分类管理数据。

计算机感染病毒的症状

- 1)操作系统无法正常启动,关闭计算机后自动重启。操作系统报告缺少必要的启动文件,或启动文件被破坏;
  2)经常无缘无故地死机:
  3)运行速度明显变慢;
  4)能正常运行的软件,运行时却提示内存不足;
  5)打印机的通讯发生异常,无法进行打印操作,或打印出来的是乱码;
  6)未使用软件,但自动出现读写操作

使用正版高效的杀毒软件

RISING
瑞星杀毒软件

360杀毒
快速轻巧・永久免费

McAfee

KASPERSKY
ANTI-VIRUS

金山毒霸

JIANGMIN
江民科技

AVIRA

360杀毒


360安全卫士 9.2
电脑体检
木马查杀
系统修复
电脑清理
优化加速
电脑救援
手机助手
软件管家
360安全卫士
已帮您修复了部分问题，还有一些问题需要手动修复！
100
修复这些项目可以强化您的电脑，提高安全和电脑性能
重新体检
登录我的360帐号
开启炫动卫士图标，10秒免费注册
专享特权：
体检发现的 3 项问题已修复 1 项，还有 2 项问题需要您手动处理
[系统强化] 发现长期不使用的软件，清理可以提高速度
查看
[系统强化] 发现有软件需要更新
查看
360手机助手安卓版 (14.1 MB 可升级至2.3.0.1025)
腾讯QQ (57.2 MB 可升级至1.99.8820.0)
快播5 (25.7 MB 可升级至5.17.154.0)
PPS影音 (17.9 MB 可升级至3.2.0.1021)
QQ游戏 (26.4 MB 可升级至3.1.107.51)
更多...
如果您还怀疑电脑存在故障无法自行解决，可以使用360专家免费提供人工服务
找专家帮忙
以下 59 项没有问题
系统强化（检测系统是否可以强化）
共 2 项
木马防火墙
360保镖
网购先赔
功能大全
更多
隐私保镖
手机助手
360网盾
开机加速
宽带测速器
断网急救箱
系统急救箱
文件粉碎机
默认软件设置
成功连接至云安全中心
9.2.0.2001

瑞星杀毒

全国最大木马库

更新及时

技术成熟-----“云技术”

Mcafee杀毒


McAfee
An Intel Company
防病毒+防火墙组合装
您的计算机面临风险
主页
订购
帮助
购买订购
您的试用版订购已过期。切勿使您的 PC 无法抵御最新威胁，请立即购买一个订购以持续受到保护。
购买
检查更新
在上次扫描期间检查的文件:
1

- Thank you