简介计算机病毒分析与处理（第一期）

by 2511-今天校对V了吗

首先，计算机病毒是什么呢?

定义：计算机病毒（Computer Virus）在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。

广义：因计算机中病毒后，轻则影响机器运行速度，重则死机系统破坏，所以，病毒给用户带来很大的损失，通常在这种情况下，我们称这种具有破坏作用的程序为计算机病毒，也可就是任何以某种方式对用户、计算机网络造成破坏的恶意程序，例如：木马、蠕虫、Rootkit、广告软件、捆绑软件、间谍软件、勒索病毒等等。

总结：可以带来危害的程序。

那些著名的计算机病毒案例……

“CIH病毒” 爆发年限：1998年6月

损失估计：全球约5亿美元

“梅利莎（Melissa）” 爆发年限：1999年3月

损失估计：全球约3亿——6亿美元

“爱虫（Iloveyou）” 爆发年限：2000年

损失估计：全球超过100亿美元

“红色代码（CodeRed）” 爆发年限：2001年7月

损失估计：全球约26亿美元

“冲击波（Blaster）” 爆发年限：2003年夏季

损失估计：数百亿美元

“巨无霸（Sobig）” 爆发年限：2003年8月

损失估计：50亿——100亿美元

“MyDoom” 爆发年限：2004年1月

损失估计：百亿美元

“震荡波（Sasser）” 爆发年限：2004年4月

损失估计：5亿——10亿美元

“熊猫烧香（Nimaya）” 爆发年限：2006年

损失估计：上亿美元

“网游大盗” 爆发年限：2007年

损失估计：千万美元

“想哭”勒索病毒爆发年限：2017年

损失估计：暂时无法估价。但它袭击全球150多个国家和地区，影响领域包括政府部门、医疗服务、公共交通、邮政、通信和汽车制造业。

那么计算机病毒如何分类呢?

为了更好的了解计算机病毒，我们常从以下几点进行分类。

媒介分类

引导型病毒：指寄生在磁盘引导区或主引导区的计算机病毒。此种病毒利用系统引导时，不对主引导区的内容正确与否进行判别的缺点，在引导型系统的过程中侵入系统，驻留内存，监视系统运行，待机传染和破坏。

文件型病毒：主要通过感染计算机中的可执行文件（`.exe`）和命令文件（`.com`）。文件型病毒是对计算机的源文件进行修改，使其成为新的带毒文件。一旦计算机运行该文件就会被感染，从而达到传播的目的。

混合型病毒：指具有引导型病毒和文件型病毒寄生方式的计算机病毒

链接方式

源码型病毒：攻击高级语言编写的程序，病毒在高级语言编写的程序编译之前插入到源程序中，经编译成功后成为合法程序的一部分。

嵌入型病毒：指病毒是将自身嵌入到现有程序中，把计算机病毒的主体程序与其攻击的对象以插入的方式链接。

操作系统型病毒：用它自己的程序加入操作系统或者取代部分操作系统进行工作，具有很强的破坏力，会导致整个系统瘫痪。而且由于感染了操作系统，这种病毒在运行时，会用自己的程序片断取代操作系统的合法程序模块

攻击的系统

DOS病毒：只能在DOS环境下运行（引导型病毒不局限于DOS操作系统而存在，早期的某些单纯占用引导记录来作为病毒体的病毒，至今仍可破坏计算机硬盘引导记录），传染的计算机病毒，是最早出现的计算机病毒。

Windows病毒：指能感染Windows可执行程序并可在Windows下运行的一类病毒。

UNIX、Linux病毒：只感染Unix、Linux操作系统的病毒。

物联网病毒：针对硬件进行感染。

APP病毒：对移动APP进行感染。

功能分类

蠕虫：可以自我复制并感染其它计算机病毒。

后门：攻击者可以绕过安全认证，远程控制受感染的计算机

僵尸网络：由大量被感染的计算机组成的网络，可以发起大规模的网络攻击，例如DDOS攻击。

木马：通过特定的程序木马程序来控制另一台计算机。木马通常有两个可执行程序，一个是控制端，另一个是被控制端，与一般的病毒不同，它不会自我繁殖，也并不刻意地去感染其他文件，它通过将自身伪装吸引用户下载执行，向施种木马者提供打开被种主机的门户，使施种者可以任意毁坏、窃取被种者的文件，甚至远程操控被种主机。

下载器、启动器：用来下载和执行其它病毒的恶意代码

间谍软件：从受害者计算机上收集信息并发送给攻击者的恶意代码

广告软件：附带广告的电脑程序，以广告作为盈利来源的软件。此类软件往往会强制安装并无法卸载；在后台收集用户信息牟利，危及用户隐私；频繁弹出广告，消耗系统资源，使其运行变慢等。

捆绑软件：捆绑软件是指用户安装一个软件时，该软件会自动安装单个或多个软件。安装时静默安装，并没有告诉用户是否要安装这个软件。

Rootkit：获得计算机root权限的工具，可以用来隐藏其它计算机病毒。

勒索软件：通过加密受感染用户的文件或硬盘，索要赎金的病毒。

垃圾邮件发送病毒：感染用户计算机之后，使用系统与网络资源来发送大量的垃圾邮件，例如广告邮件、钓鱼邮件等。

攻击目标

大众型的计算机病毒：比如勒索软件，采用的是一种撒网捞鱼的方法，设计目标是感染尽可能多的机器。这类恶意代码比较普遍，恶意行为比较明显，容易被检测和防御

针对型的计算机病毒：比如特质的后门病毒，是针对特定组织而研制的。不是广泛传播的，样本收集难度大。代码非常复杂，病毒分析往往要借助于一些高分析技巧。例如震网病毒，定向攻击工业系统。

那什么是计算机病毒分析呢?

计算机病毒分析，通常是为一起计算机病毒事件的应急响应提供所需信息，包括以下的分析内容：

（系统到底发生了什么？）

定位被感染的计算机和可疑的程序；

对可疑文件进行分析；

提取出可以在系统和网络上检测病毒的特征码；

衡量并消除计算机病毒所带来的损害。

那计算机病毒分析的目标是什么?

- 分析出是如何感染的
- 分析出病毒运行流程

- 分析出病毒运行危害
- 分析出如何识别此病毒
- 分析出如何消除此病毒

那如何第一时间找到计算机病毒呢?

可以从计算机病毒特征码入手，可用于查杀病毒文件、阻止病毒传播，可以按照一下分类进行细分。

主机特征码

主机特征码关注的是病毒对系统做了什么，而不是病毒本身的文件特征，它对比反病毒软件特征码（备注：可通过技术手段修改文件信息，导致特征码失效，例如：程序加壳、使用花指令等）反而更加有效。

例如:

特定的文件创建、读取、修改行为;

特定的注册表创建、读取、修改行为;

特定的开机启动项创建、读取、修改行为;

特殊的行为，如自删除。

网络特征码

通过分析计算机病毒的网络通信数据提取出的特征码，其包括恶意的IP地址、URL、邮件、攻击数据包、计算机病毒间的通信协议等，也可以和主机特征码想结合，提供更高的检测率和更少的误报。

例如:

与公布出的钓鱼网站、放马平台进行数据交互。

说了这么多，那常见的计算机病毒分析技术都有哪些呢?

为了更好的了解，我们从以下方面进行分类讲解:

静态分析：静态分析方法是在没有计算机病毒时，对其进行分析的相关技术，其包括分析病毒可执行文件，但不查看具体CPU指令的分析技术。

常见的分析工具有CoBOT、Coverity、Klocwork、Checkmarx、Fortify、Testbed、PinPoint、C++test、VirusTotal、strings、PC-Lint、QAC、IDA pro、cutter、GDA等等。

优点：非常快速、简单、可深入分析计算机病毒。

缺点：难以分析复杂的计算机病毒，而且可能会漏掉一些重要的行为，并易受代码混淆技术的干扰，例如加壳、花指令等。

动态分析：动态分析方法则需要运行计算机病毒，使用调试器来分析一个病毒运行时刻的内部状态，动态执行每一条指令验证静态高级分析的结果。

常见的分析工具有RegShot、Process Mointor、ApateDNS、Netcat、Wireshark、INetSim、OllyDbg、x64dbg、dnspy、Sysinternals工具集等等。

优点：简单、可以缓解代码混淆的干扰。

缺点：可能会漏洞一些重要病毒功能，并只能覆盖一条计算机病毒的执行轨迹。

那有什么分析经验可以分享吗？

首先，先做好分析前的防护工作，避免病毒使用某些途径进行扩散传播在进行静态分析、在进行动态分析，互相弥补，多方面思考，也不要过于陷入细节，关注其主要的危害、在后期深入分析之前做好有一个概要性的理解。

其次，可以尝试从不同角度、不同工具、不同方法来分析计算机病毒，不要被局限。

最后，计算机实在与时俱进的，分析也要与时俱进，不要停止前行的步伐，也要走在病毒发布者的前沿，先发现危害，着手进行防御以及分析。

在上面我们了解了计算机病毒的实质、分类和一些分析病毒的方法。但是在实际的应用中，同样重要的是解决问题。当我们在计算机中发现了病毒文件或代码时，该怎样处理呢？下面展示了一些更实用的——

常见病毒处理办法！

一、感染型病毒、蠕虫病毒/X KB 快捷方式病毒 /X KB EXE病毒

清空信任区，进入带网络的安全模式使用安全软件进行全盘查杀。

在全盘查杀之前记得进入设置开启选项“发生所有类型操作都扫描”。

二、勒索病毒

（一）加密文件型勒索

通常暂时无法解密，请附上被加密文件的后缀和勒索信图片交给安全厂商以确认勒索病毒家族。

安全厂商解密的条件只有两个：

1. 病毒作者公开了密钥；
2. 病毒加密模块存在逻辑缺陷可以逻辑漏洞进行破解。

数据恢复公司可以恢复部分机械硬盘和数据库的数据。

部分数据恢复公司会联系黑客赚取差价帮你进行解密。

（二）MBRLock型勒索

请提供病毒文件以供破解。

若无法破解，你需要：

1. 另一台电脑
2. 一个空U盘

制作U盘Windows PE后，打开DiskGenius，同意用户协议，右击你的整块硬盘，选择“重建主引导记录”，选择“是”按钮。

若发现硬盘分区全没了，整块硬盘变为“未分配”状态，你还需要点击DiskGenius上面的“查找丢失分区”，弹出的窗口全部选择“保留”，随后右上角“保存”，然后“确认执行操作”。

随后，你还需要在Windows PE内修复系统引导BCD等。

（三）敲竹杠型勒索（用户锁勒索）

请提供病毒文件给安全厂商以供破解。

若无法破解，你需要：

1. 另一台电脑
2. 一个空U盘

制作U盘Windows PE后，双击桌面上面的“Windows密码破解工具”（NTPWEdit），

单机右上角的“打开”按钮，选择被锁的用户名，点击“解锁”，随后单机“保存更改”，然后重启计算机。

三、广告程序（ADWare/PUP/PUA）

用杀毒软件全盘扫描一遍（此处推荐火绒、Kaspersky Virus Remove Tool、Norton Power Eraser）

用分析工具打开以下目录：

```
C:\Users\(UserID)\Appdata\local

C:\Users\(UserID)\Appdata\Roming

C:\Users\(UserID)\Appdata\locallow
```

寻找随机英文文件夹，尤其是带有“Path”“Host”“Svc”“PDF”“Note”字样的，全部删除。

最后，再使用CnSoftKiller工具扫描处理一下即可。

四、驱动病毒（内核后门病毒/RootKit）

请尝试使用火绒恶性木马专杀工具、360急救箱强力模式扫描2遍（360急救箱请去360官网下载最新版本，是一个压缩包形式的，使用前请解压全部的文件，不建议使用360所属的产品内自带的360急救箱）。

如无法解决，请咨询对应的安全厂商安全员，并留下你的QQ，可为远程操作安全员准备好以下工具：

360急救箱

火绒剑

PCHunter/PYArk/PDArk

AutoRun

必要时可能需要Windows PE（由空U盘制作）。

如使用360急救箱尝试扫描过，请提供360急救箱同目录下的`SysRepair.log`，强制进行内核驱动对抗存在一定的风险，可能会存在有容易蓝屏的问题，请知悉。

五、U盘文件乱码问题等

多数非病毒所致。

请以管理员权限打开Cmd/Powershell/终端，

键入以下命令后回车：`Chkdsk:/ /F`

六、系统更新升级失败问题

多数非病毒所致。

请打开记事本，

内容填写：

```
Sfc /scannow

Dism /Online /Cleanup-Image /ScanHealth

Dism /Online /Cleanup-Image /CheckHealth

Dism /Online /Cleanup-image /RestoreHealth

SC config wuauserv start=auto

SC config bits start=auto

SC config cryptSvc start=auto

SC config trustedinstaller start=auto

SC config wuauserv type=share

net stop wuauserv

net stop cryptSvc

net stop bits

net stop msiserver

ren C:\Windows\SoftwareDistribution SoftwareDistribution.old

ren C:\Windows\System32\catroot2 catroot2.old
```

```
net start wuauserv

net start cryptSvc

net start bits

net start msiserver

netsh winsock reset
```

随后另存为到桌面，“文件类型”选择“全部”，文件名称后缀修改为“`.bat`”

联网状态下，右击该文件，选择“以管理员权限运行”。等待执行完成后，请重启电脑后再次尝试。

七、蓝屏问题

请找到

```
%SystemRoot%\Minidump

%SystemRoot%\Memory.dmp
```

（`%SystemRoot%`是系统当中的一个环境变量，实质`C:\Windows`（若C盘为系统盘））

随后，将这几份文件交给你的安全软件厂商或者微软社区进行分析。

如蓝屏代码为英文的Memory Management，且无法成功生成Dump文件，请优先考虑是否为内存条出现了硬件故障的问题。

八、其他系统问题

多数非病毒所致。

请以管理员权限打开Cmd或Powershell

联网状态下，依次键入以下命令后回车：

```
Sfc /scannow
Dism /Online /Cleanup-Image /ScanHealth
Dism /Online /Cleanup-Image /CheckHealth
Dism /Online /Cleanup-Image /RestoreHealth
```

执行完毕后，重启电脑。