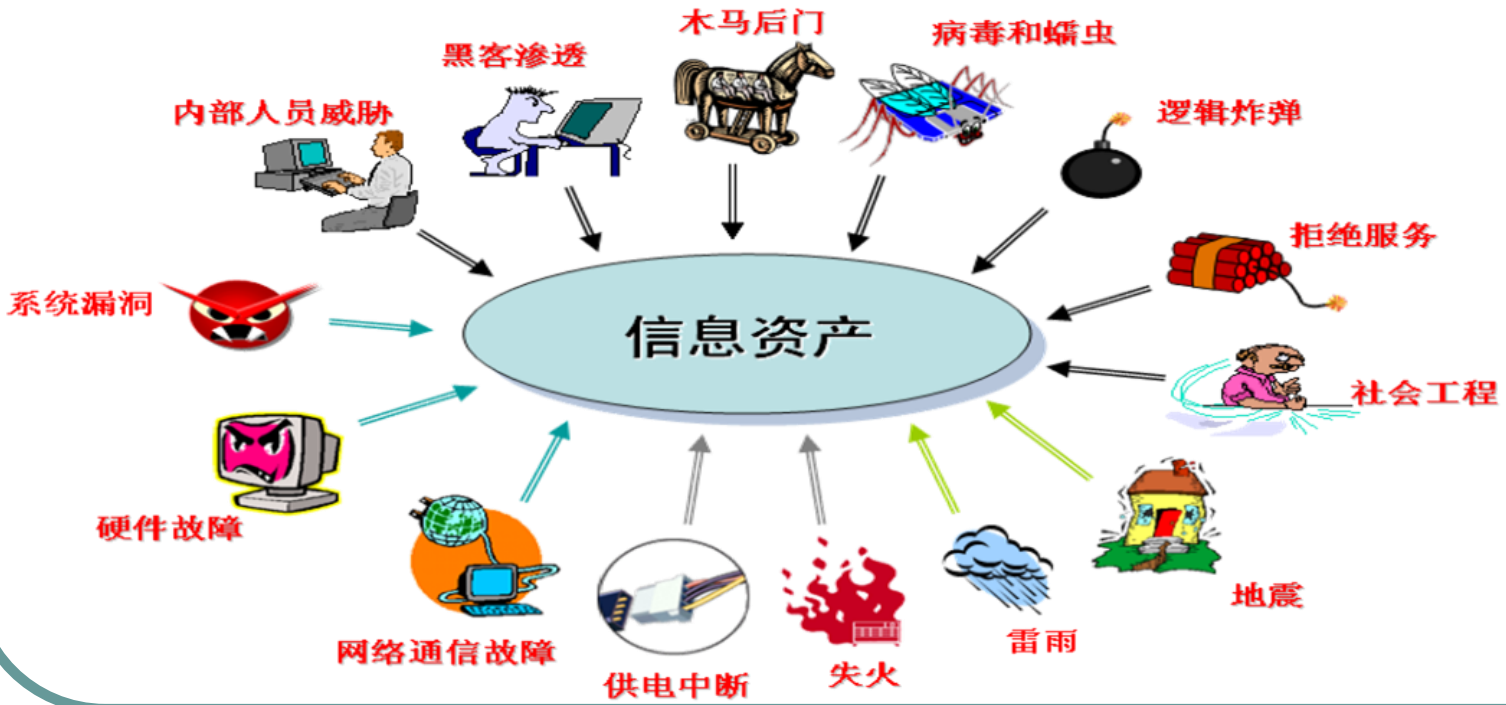
C3 恶意代码及其分类

刘铭

liuming@hust.edu.cn

威胁无处不在


木马后门
病毒和蠕虫
黑客渗透
内部人员威胁
逻辑炸弹
拒绝服务
系统漏洞
信息资产
社会工程
硬件故障
地震
网络通信故障
雷雨
供电中断
失火

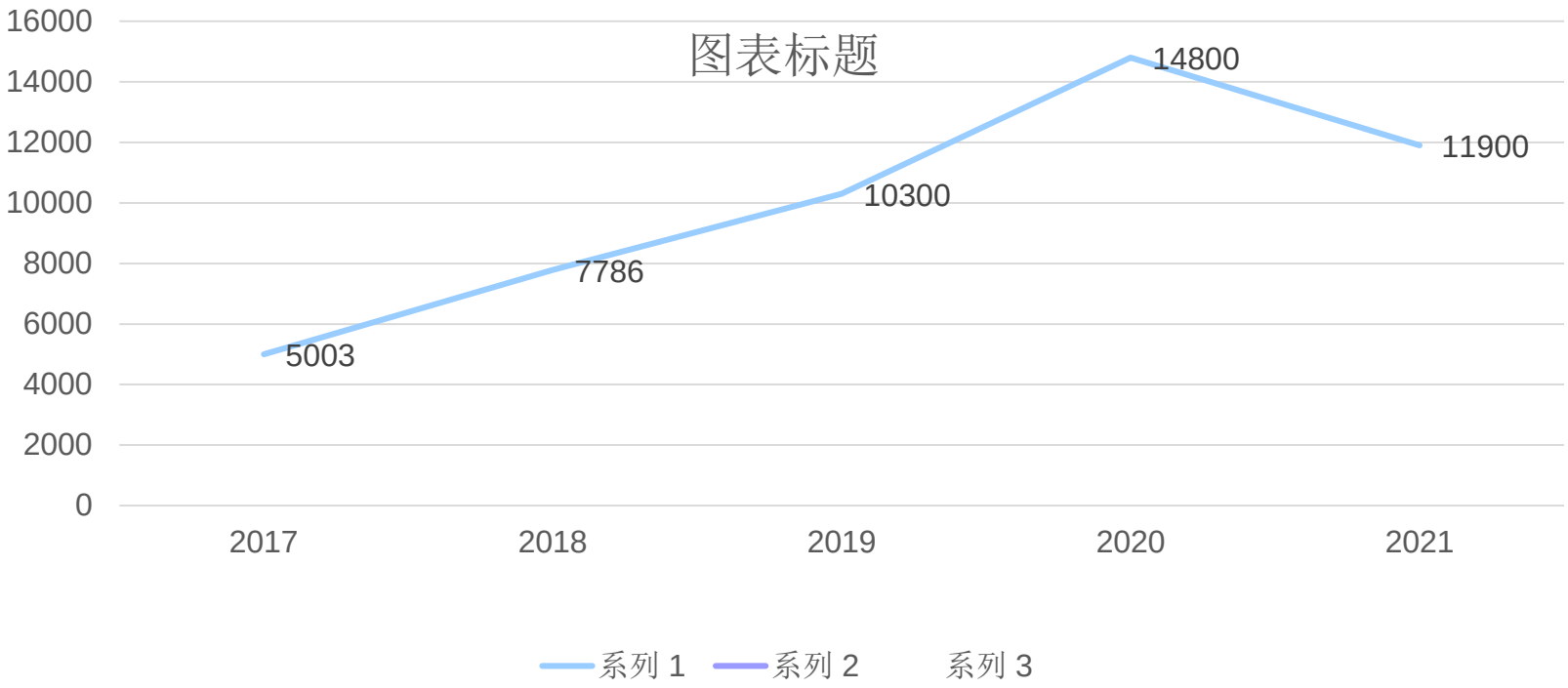
本讲提纲

- 3.1恶意代码的定义与发作情况
- 3.2恶意代码的功能
- 3.3恶意代码的分类
- 3.4恶意代码与网络犯罪

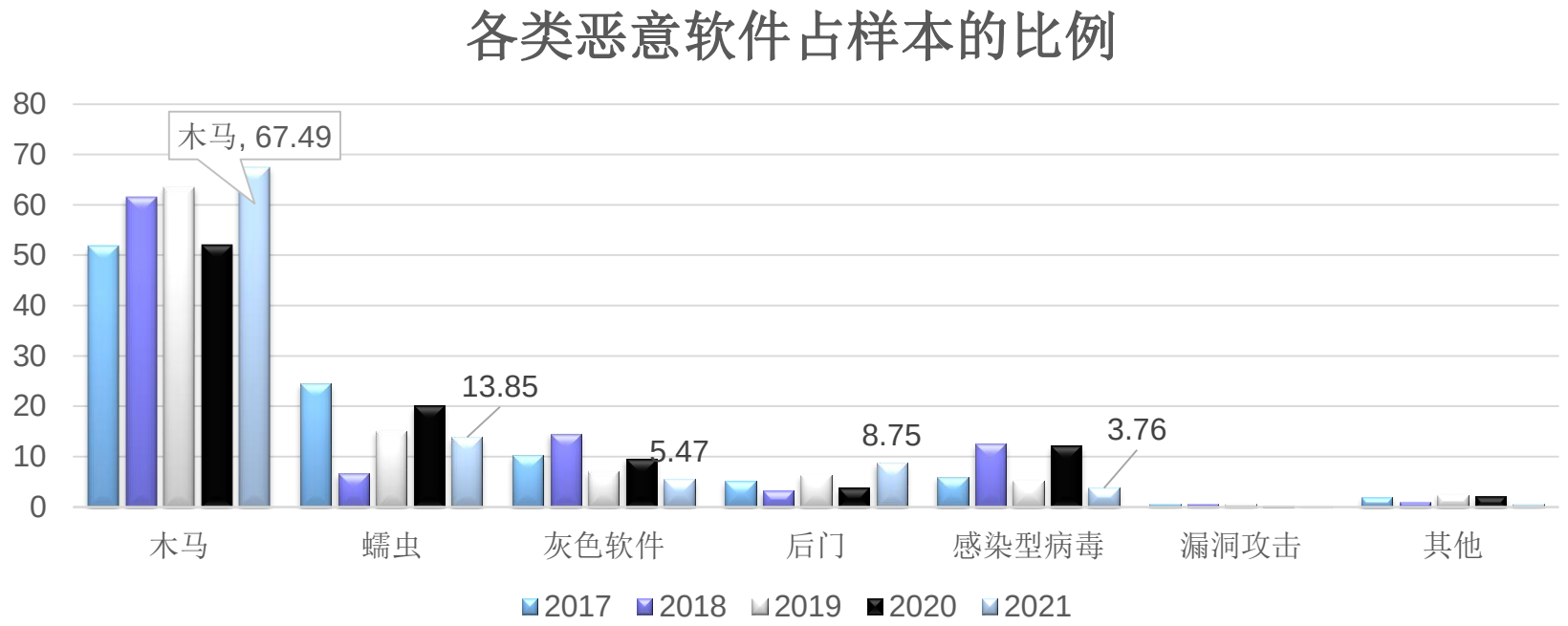
3.1 恶意代码的定义及发作情况

- 恶意代码（**Malicious Code、MalCode、MalWare**）。
  - 设计目的是用来实现恶意功能的代码或程序；
  - 正常软件也会引发安全问题，但绝大多数情况下并非作者有意。

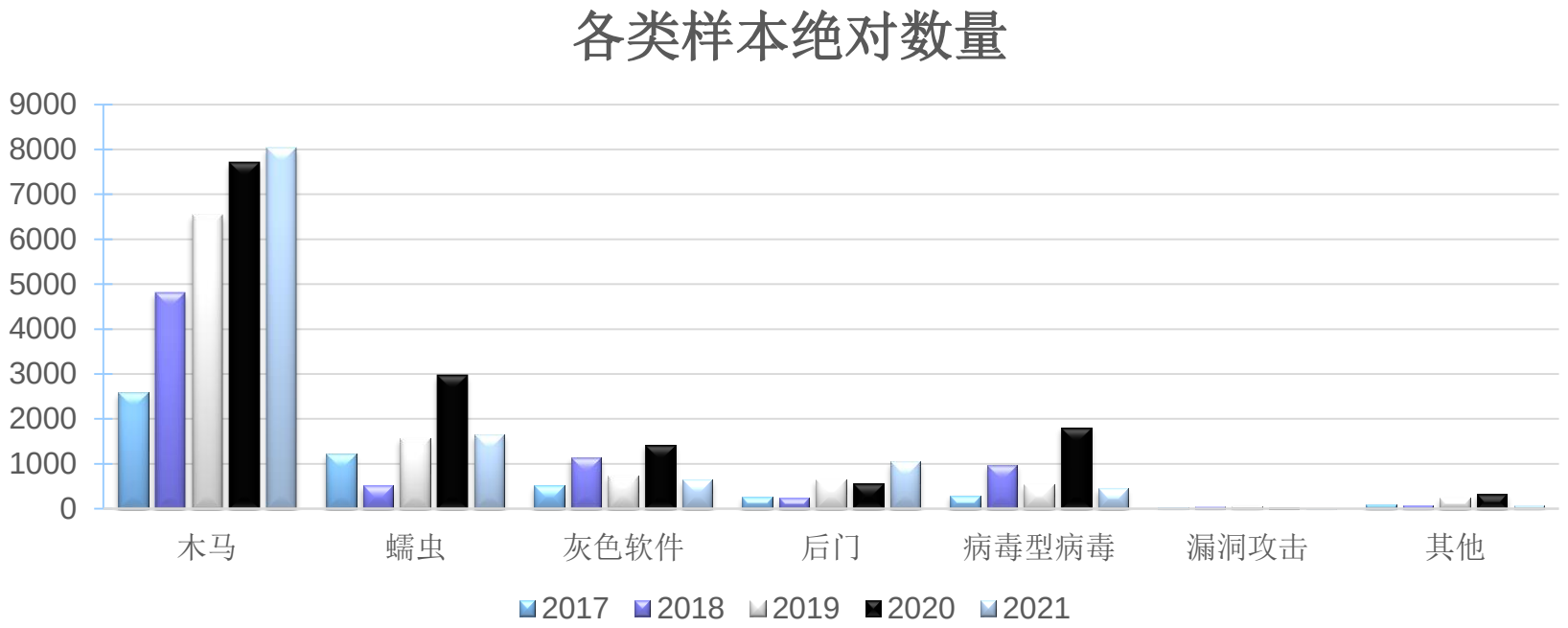
2017-2021恶意代码数量（瑞星）



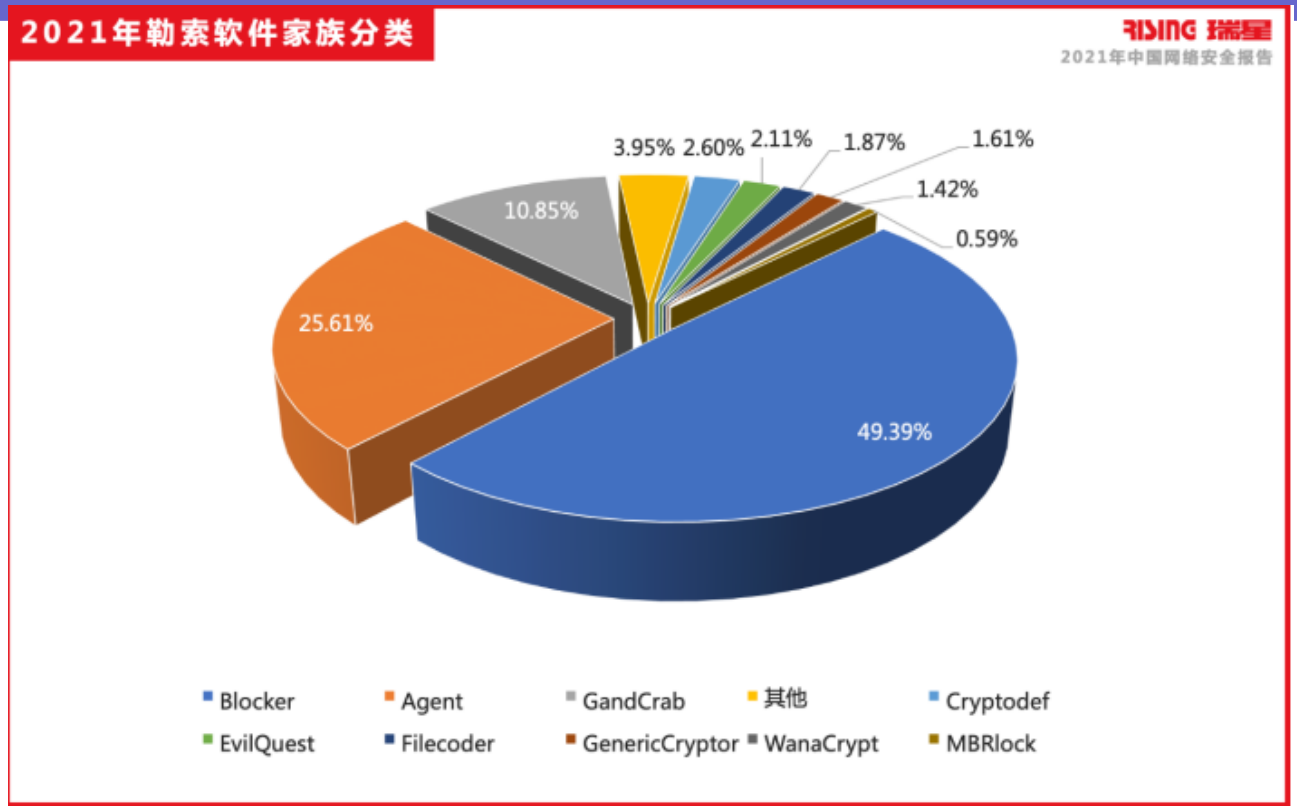
瑞星安全报告（2017-2021）



瑞星安全报告（2017-2021）



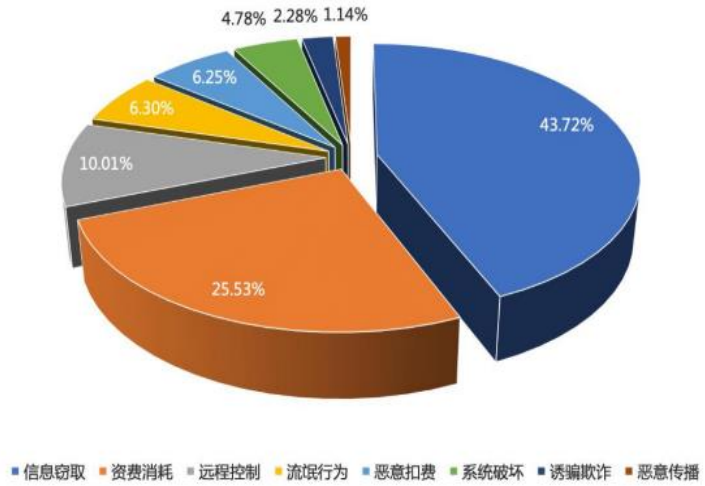
勒索软件（瑞星 2021）


2021年勒索软件家族分类
RISING 瑞星
2021年中国网络安全报告
3.95%
2.60%
2.11%
1.87%
1.61%
1.42%
0.59%
10.85%
25.61%
49.39%
Blocker
Agent
GandCrab
其他
Cryptodef
EvilQuest
Filecoder
GenericCryptor
WanaCrypt
MBRlock

智能终端恶意软件样本（瑞星 2021）

2021年手机病毒类型比例

RISING 瑞星 2021年中国网络安全报告



2021年手机病毒Top5

RISING 瑞星 2021年中国网络安全报告

排名	名称	描述
1	Trojan.SMSreg!8.2DFC	运行后无明显扣费提示，用户若不慎点击会发送扣费短信，造成用户资费损失，主要通过免费软件、下载站、共享软件等方式进行传播。
2	Adware.Mobby/Android!8.A0FC	广告软件，包含Mobby广告SDK的软件，该软件主要通过Web下载、共享软件等方式进行传播。
3	Dropper.Agent/Android!8.37E	释放型木马病毒，该病毒会释放其他木马并运行，主要通过下载站、共享软件等方式进行传播。
4	Trojan.Obfus/Android!8.3F7	带混淆的木马病毒，该病毒常使用混淆工具规避安全软件检测，主要通过免费软件、Web下载等方式进行传播。
5	Trojan.Agent/Android!8.358	安卓木马病毒，目的通常为破坏系统、窃取用户隐私、下载其他木马，主要通过免费软件、下载站、共享软件等方式进行传播。

3.2 恶意代码的功能

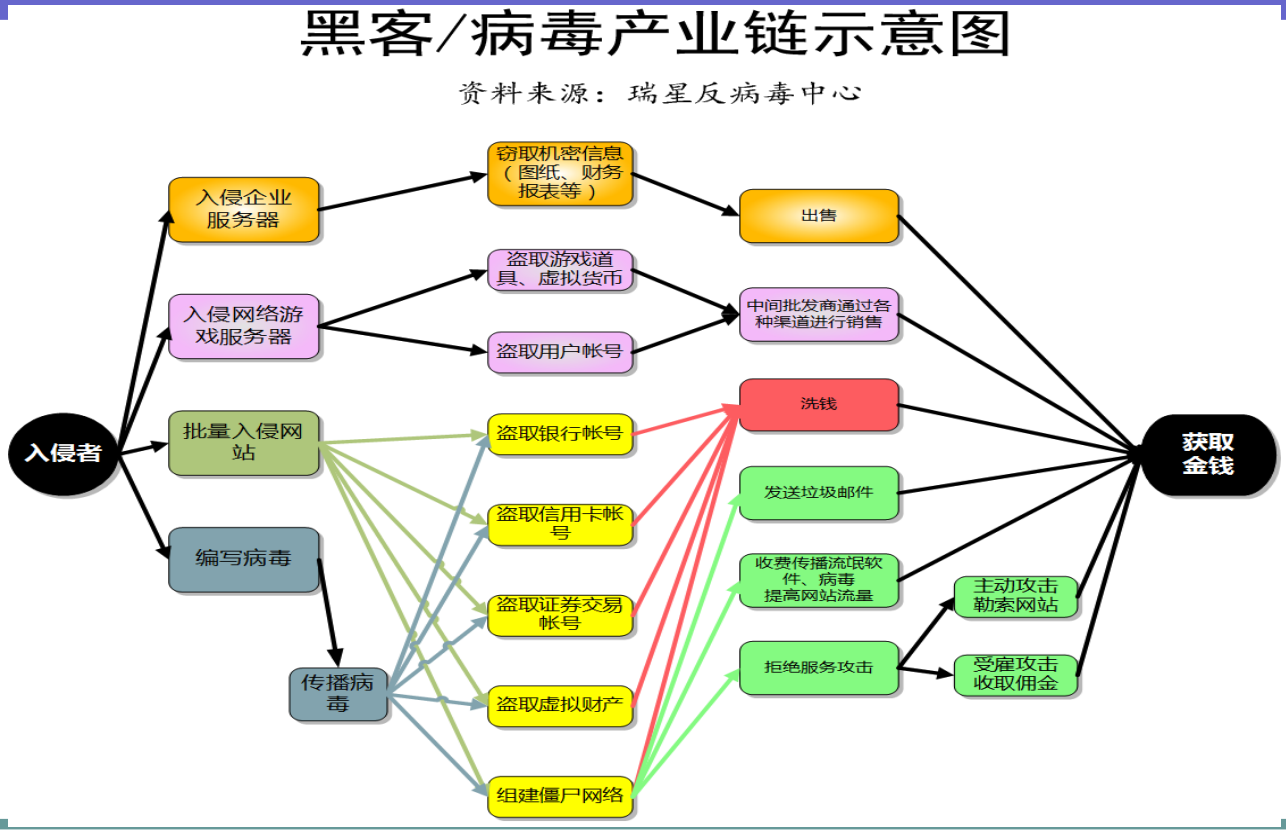
- 攻击目的是什么？
- 攻击目标有哪些？

3.2.1 攻击目的

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

图：暴雪官方公告

黑色产业链一示意图


黑客/病毒产业链示意图
资料来源：瑞星反病毒中心
入侵者
入侵企业服务器
入侵网络游戏服务器
批量入侵网站
编写病毒
传播病毒
窃取机密信息（图纸、财务报表等）
盗取游戏道具、虚拟货币
盗取用户帐号
盗取银行帐号
盗取信用卡帐号
盗取证券交易帐号
盗取虚拟财产
组建僵尸网络
出售
中间批发商通过各种渠道进行销售
洗钱
发送垃圾邮件
收费传播流氓软件、病毒提高网站流量
拒绝服务攻击
主动攻击勒索网站
受雇攻击收取佣金
获取金钱

黑色产业链—运转模式


资金流向:
入侵活动:
解密黑色产业链
6. 地下交易
-数百万肉鸡控制权
漏洞挖掘者
僵尸网络集团
病毒
1. 漏洞信息
5. 肉鸡控制权
病毒制造者
2. 病毒
牧马人(黑客)
肉鸡控制权
肉鸡中间商
攻击者
游戏玩家
虚拟装备中间商
信用卡盗刷
信用卡受害人
信用卡犯罪团伙
勒索
商业机密泄露公司
竞争对手
广告商/钓鱼集团/其他黑客集团
4. 弱鸡控制权
3. 后门/僵尸病毒
7. 盗号木马
控制命令
商业机密/隐私
帐号密码
计算能力
隐私资料
被盗窃后在黑市交易
被在黑市标价出租
被盗窃-勒索或泄漏
更多受害者
->商业机密被盗
->隐私活动被盗摄
->发送垃圾邮件
->DDOS攻击
->网站挂马
->建钓鱼网站

3.2.2 攻击目标

- 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

3.2.3 恶意代码的功能

- 获取数据
  - 静态数据：
    - 文件、数据库等；
  - 动态数据：
    - 口令、内存、计算机网络流量、通信网络数据、可移动存储介质、隔离电脑等
- 动态控制与渗透拓展攻击路径等
  - 中间系统
  - 相关人员
- 破坏系统
  - 数据：删除、修改数据；
  - 系统服务：通用Web服务系统，数据库系统，特定行业服务系统（如工控）等。
  - 支撑设备：网络设备、线路等。

3.3 恶意代码的分类

- 恶意代码，即广义上的计算机病毒。其可分为：
  1. 计算机病毒
  2. 蠕虫
  3. 木马
  4. 后门
  5. **Rootkit**
  6. 僵尸**(bot)**、流氓软件、间谍软件、广告软件、**Exploit**、黑客工具等。

网络恶意代码的分类

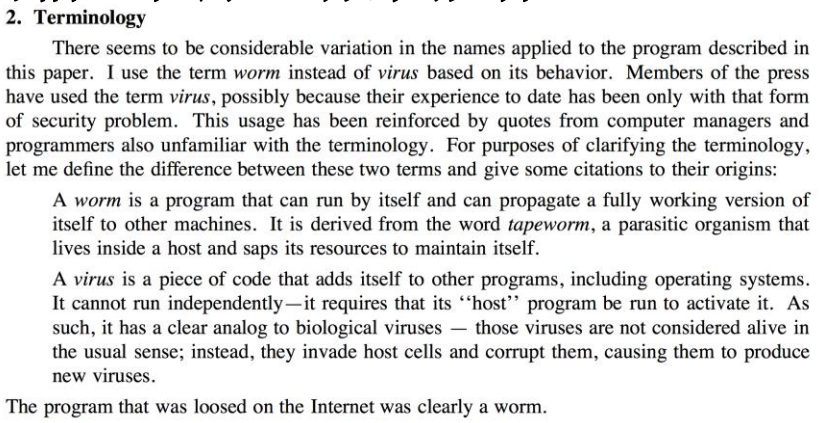
1. 计算机病毒：一组能够进行自我传播、需要用户干预来触发执行的破坏性程序或代码。
   - 如CIH、爱虫、美丽莎、新欢乐时光、求职信、恶鹰、rose、威金、熊猫烧香、小浩、机器狗、磁碟机、AV终结者、Flame…
2. 网络蠕虫:一组能够进行自我传播、不需要用户干预即可触发执行的破坏性程序或代码。
   - 其通过不断搜索和侵入具有漏洞的主机来自动传播。
   - 如红色代码、SQL蠕虫王、冲击波、震荡波、极速波、魔波、震网…

另一个被广泛采用的定义

- **1988年Morris莫里斯蠕虫爆发后，Eugene H. Spafford 为了区分蠕虫和病毒，给出蠕虫和计算机病毒的定义：**
  - “计算机蠕虫可以独立运行，并能把自身的一个包含所有功能的版本传播到另外的计算机上”
  - “计算机病毒是一段代码，能把自身加到其他程序包括操作系统上；它不能独立运行，需要由它的宿主程序运行来激活它”

Fred Cohen(1984)“计算机病毒是一种程序，它可以感染其它程序，感染的方式为在被感染程序中加入计算机病毒的一个副本，这个副本可能是在原病毒基础上演变过来的”。

阅读链接：
http://spaf.cerias.purdue.edu/tech-reps/823.pdf



2. Terminology

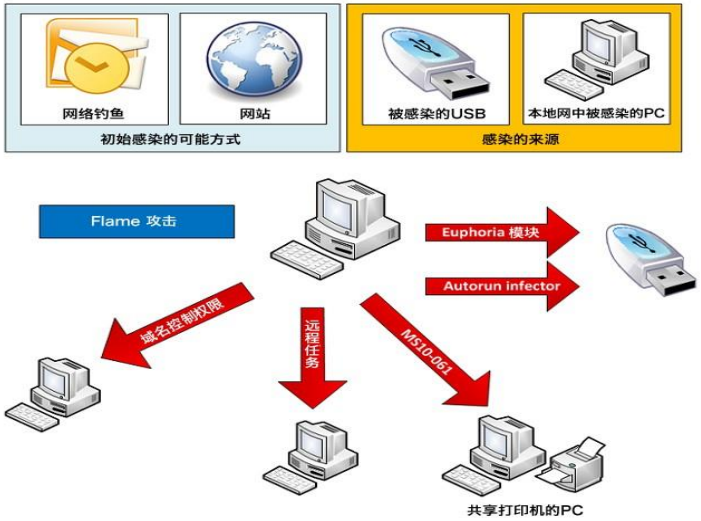
There seems to be considerable variation in the names applied to the program described in this paper. I use the term *worm* instead of *virus* based on its behavior. Members of the press have used the term *virus*, possibly because their experience to date has been only with that form of security problem. This usage has been reinforced by quotes from computer managers and programmers also unfamiliar with the terminology. For purposes of clarifying the terminology, let me define the difference between these two terms and give some citations to their origins:

A *worm* is a program that can run by itself and can propagate a fully working version of itself to other machines. It is derived from the word *tapeworm*, a parasitic organism that lives inside a host and saps its resources to maintain itself.

A *virus* is a piece of code that adds itself to other programs, including operating systems. It cannot run independently—it requires that its ‘‘host’’ program be run to activate it. As such, it has a clear analog to biological viruses — those viruses are not considered alive in the usual sense; instead, they invade host cells and corrupt them, causing them to produce new viruses.

The program that was loosed on the Internet was clearly a worm.

Flame（火焰）-超乎你的想象



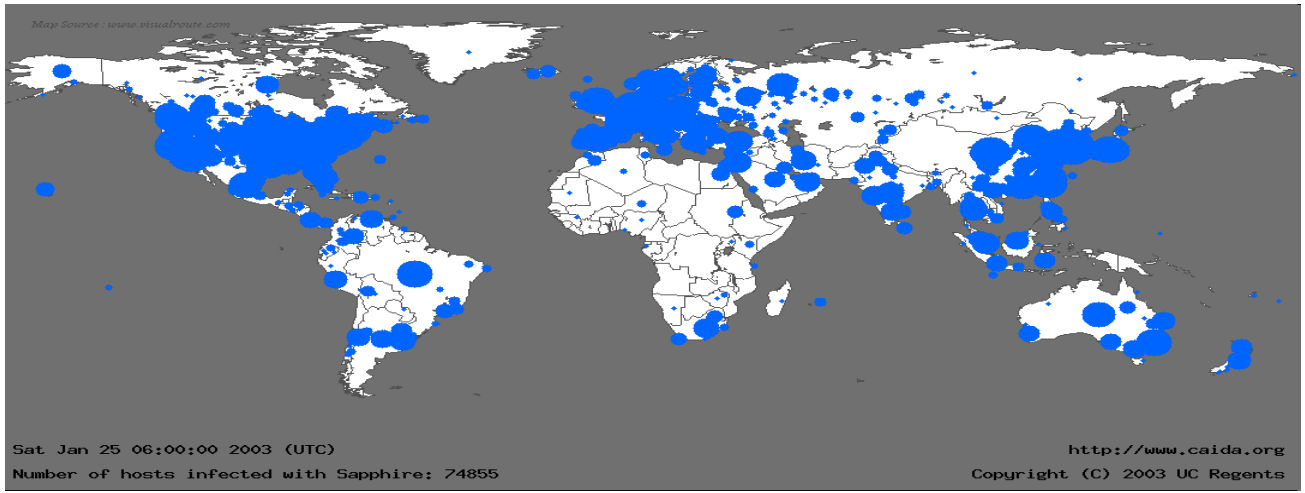
- 5 种加密算法
- 3 种压缩技术
- 至少 5 种文件格式
- 65万行代码

卡巴斯基CEO“Stuxnet、DuQu病毒属于一系列攻击的组成部分,...Flame病毒的发现，意味着互联网安全大战进入到新阶段”

2003年以来的部分典型重大蠕虫事件

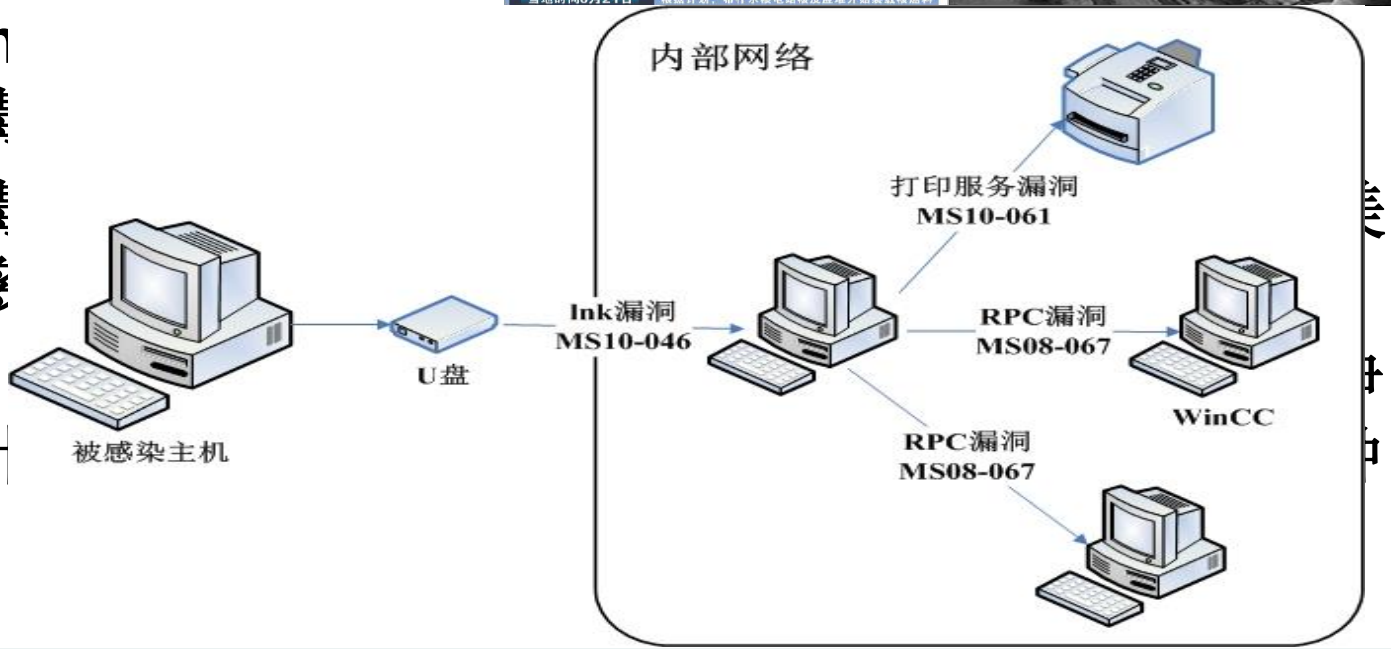
- 蠕虫王-slammer（2003年1月25日）
  - MS02-039
- 冲击波-msblast（2003年8月11日）
  - MS03-026
- 震荡波-sasser（2004年5月1日）
  - MS04-011
- 极速波-Zotob（2005年8月14日）
  - MS05-039
- 魔波-MocBot（2006年8月13日 ）
  - MS06-040
- 扫荡波-saodangbo（2008年11月7日）
  - MS08-067
- 飞客-Conficker(2008年11月-2012)
  - MS08-067
- Stuxnet（2010年7月被普遍捕获）
  - MS10-046(lnk) , MS08-067 , MS10-061等5个操作系统漏洞及2个西门子wincc系统漏洞
- Incaseformat 蠕虫（2010-2021）
- Jboss网站蠕虫（CNVD-2010-00821）
- The moon蠕虫(CNVD-2014-01260)

SQL蠕虫王（Slammer）—半小时感染全球90%易感染主机
—376个字节带来的网络世界灾难



Stuxnet(超级工厂蠕虫)—内网摆渡

- 2010年7月大面积爆发。
- Stuxn
  厂病毒
- 该病毒
  国等多
- 其中，
  朗布什
  病毒。



“飞客”蠕虫感染主机IP地址2011-2018

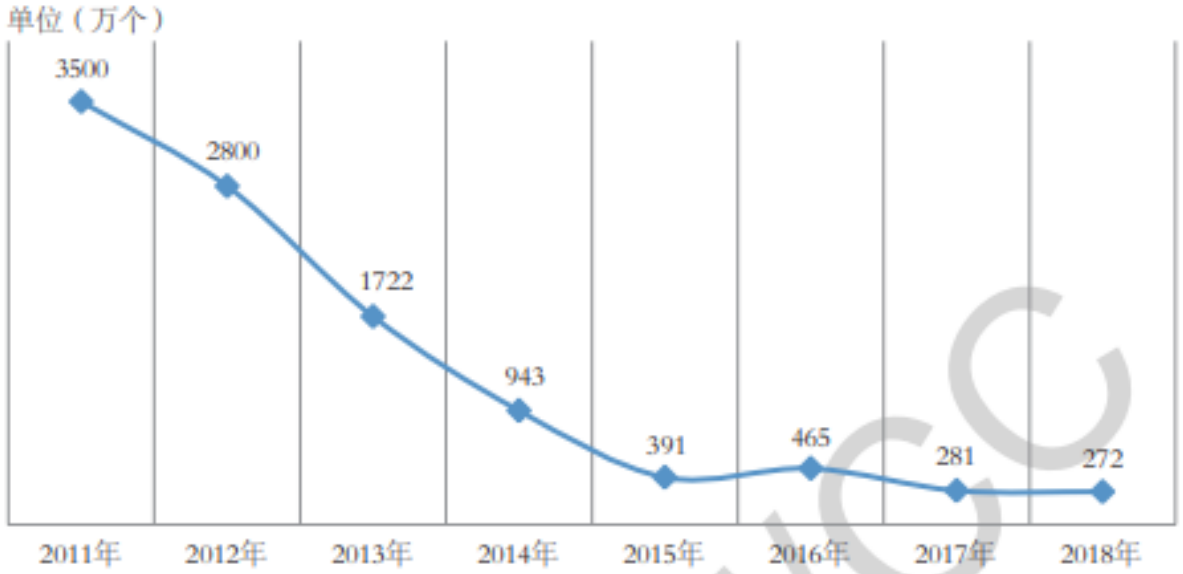
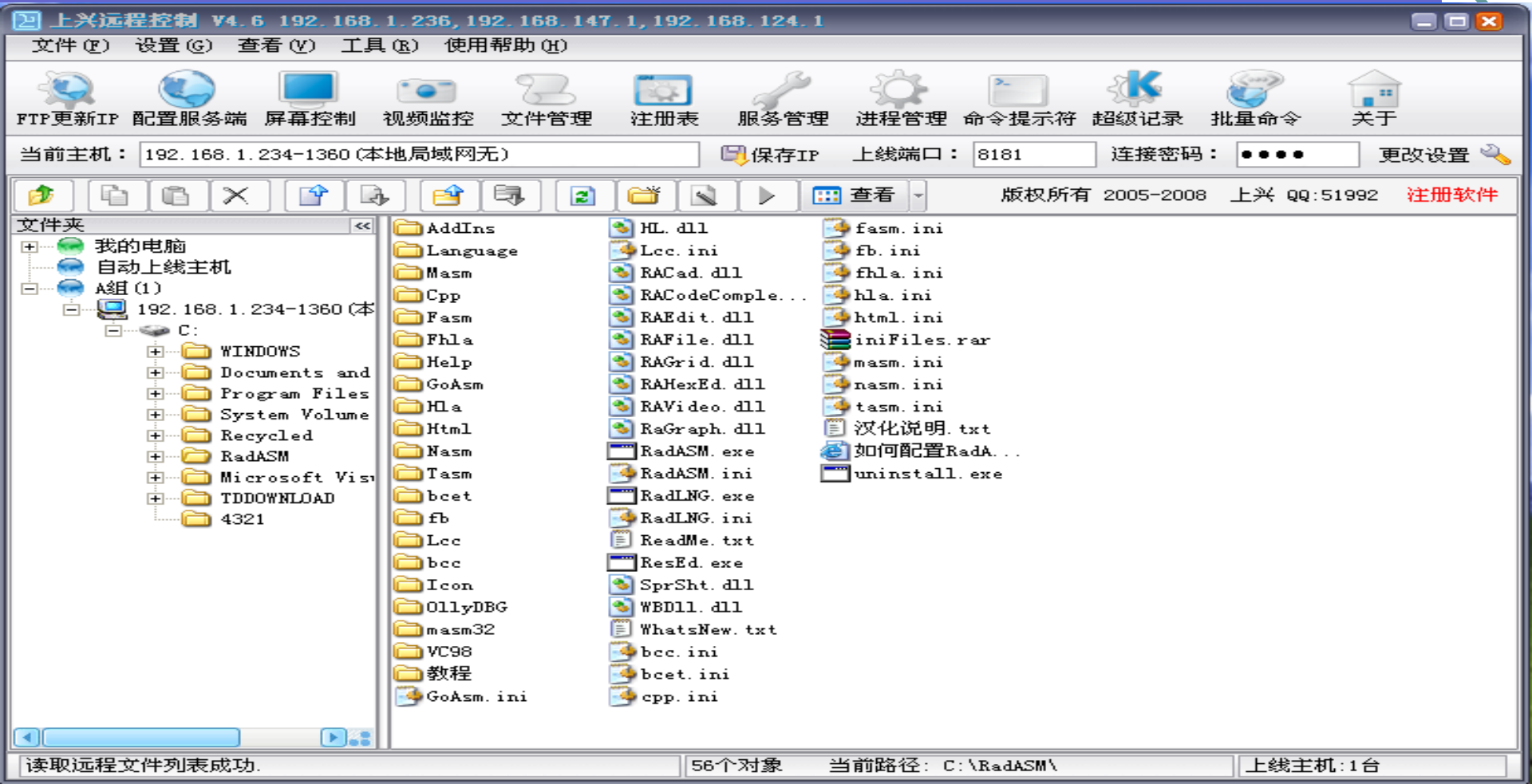


图 3-10　2011-2018 年全球互联网感染“飞客”蠕虫的主机 IP 地址月均数量
（来源：CNCERT/CC）

网络恶意代码的分类（续）

3. 特洛伊木马：是指一类看起来具有正常功能，但实际上隐藏着很多用户不希望功能的程序。通常由控制端和被控制端两端组成。
   - 如冰河、网络神偷、灰鸽子、Gh0st、上兴……

4. 后门：使得攻击者可以对系统进行非授权访问的一类程序。
   - 如Bits、WinEggDrop、Tini…
   - 阅读链接：2020 Annual Report.pdf 瑞星2021baogao.pdf


上兴远程控制 V4.6 192.168.1.236,192.168.147.1,192.168.124.1
文件(F) 设置(G) 查看(V) 工具(R) 使用帮助(H)
FTP更新IP
配置服务端
屏幕控制
视频监控
文件管理
注册表
服务管理
进程管理
命令提示符
超级记录
批量命令
关于
当前主机： 192.168.1.234-1360(本地局域网无)
保存IP
上线端口： 8181
连接密码： ••••
更改设置
查看
版权所有 2005-2008 上兴 QQ:51992 注册软件
文件夹
我的电脑
自动上线主机
A组(1)
192.168.1.234-1360(本
C:
WINDOWS
Documents and
Program Files
System Volume
Recycled
RadASM
Microsoft Visu
TDDOWNLOAD
4321
AddIns
Language
Masm
Cpp
Fasm
Fhla
Help
GoAsm
Hla
Html
Nasm
Tasm
bcet
fb
Lcc
bcc
Icon
OllyDBG
masm32
VC98
教程
GoAsm.ini
HL.dll
Lcc.ini
RACad.dll
RACodeComple...
RAEdit.dll
RAFile.dll
RAGrid.dll
RAHexEd.dll
RAVideo.dll
RaGraph.dll
RadASM.exe
RadASM.ini
RadLNG.exe
RadLNG.ini
ReadMe.txt
ResEd.exe
SprSht.dll
WBDll.dll
WhatsNew.txt
bcc.ini
bcet.ini
cpp.ini
fasm.ini
fb.ini
fhla.ini
hla.ini
html.ini
iniFiles.rar
masm.ini
nasm.ini
tasm.ini
汉化说明.txt
如何配置RadA...
uninstall.exe
读取远程文件列表成功.
56个对象
当前路径： C:\RadASM\
上线主机:1台

2019-2020恶意程序数量比较

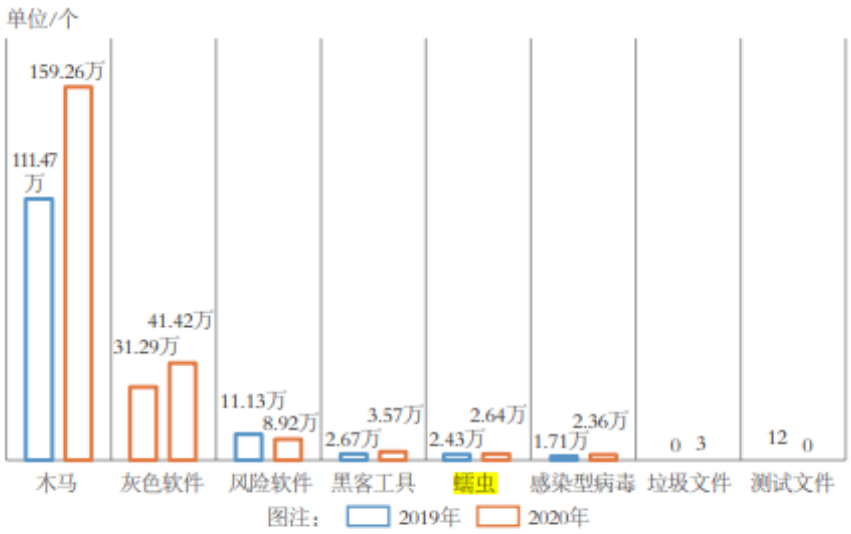
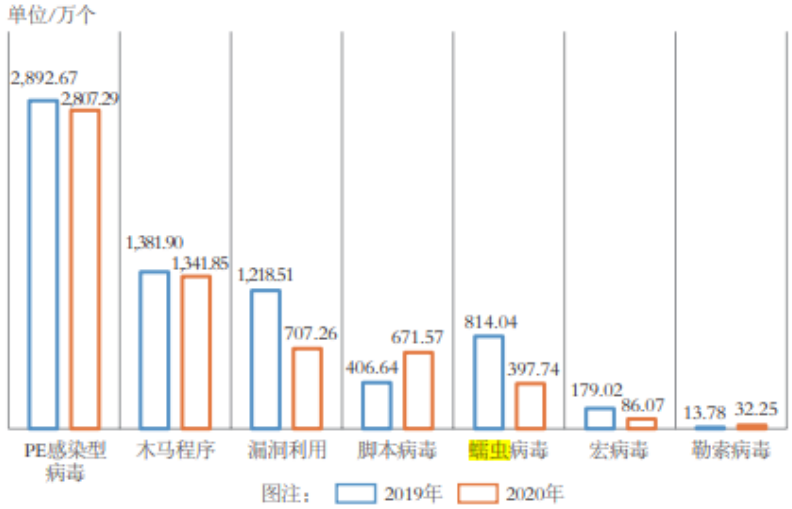
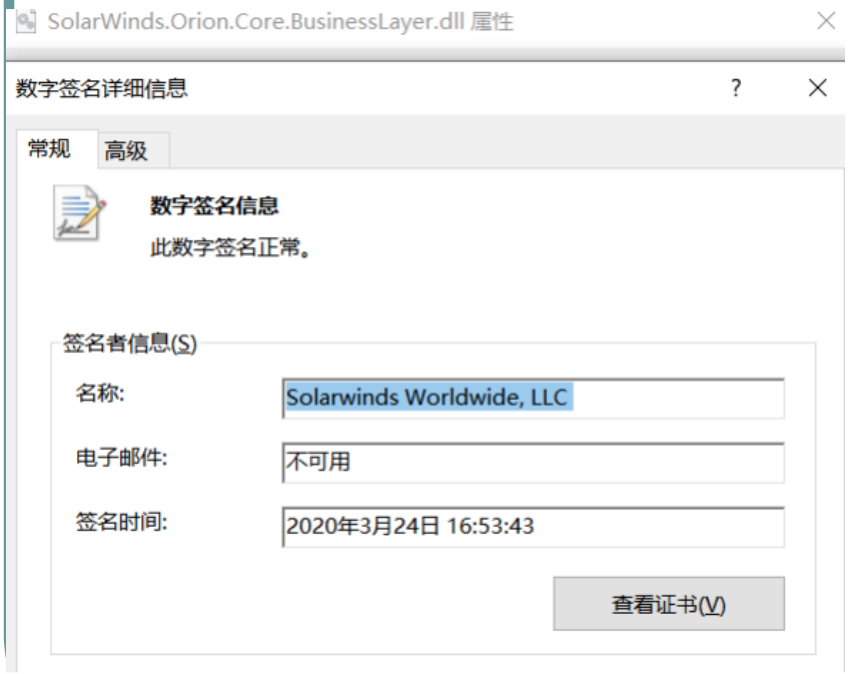


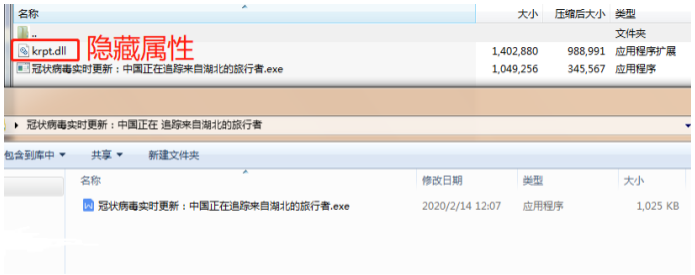
图 3-26　2019 年与 2020 年捕获的恶意程序数量分类比较
（来源：北京安天网络安全技术有限公司）



2019 年与 2020 年捕获的恶意程序数量分类比较（来源：亚信科技（成都）有限公司）



图：Sunburst数字签名



图：中国正在追踪来自湖北的旅行者.exe

图：诱饵文档

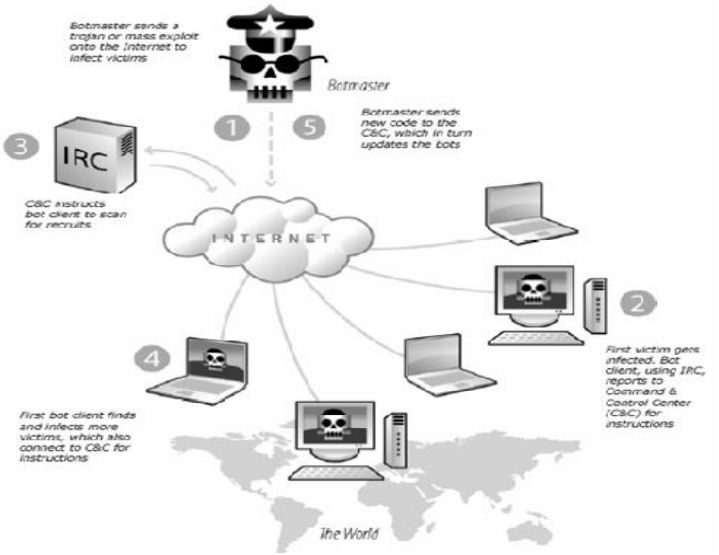
网络恶意代码的分类（续）

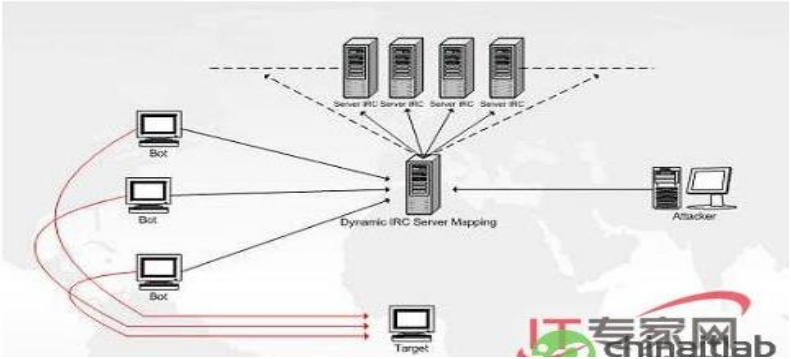
5. **RootKit：**通过修改现有的操作系统软件，使攻击者获得访问权并隐藏在计算机中的程序。
    5. 如**RootKit、Hkdef、ByShell…**

6. 僵尸程序，恶意网页，拒绝服务程序，黑客工具，广告软件，间谍软件……

僵尸程序

- 是指恶意控制功能的程序代码，能够自动执行预定义的功能、可以被预定义的命令控制





间谍软件

- 以主动收集用户个人信息、相关机密文件或隐私数据为主，搜集到的数据会主动传送到指定服务器。

广告软件

- 未经用户允许，下载并安装或与其他软件捆绑通过弹出式广告或以其他形式进行商业广告宣传的程序。

央视315曝光恶意捆绑软件,福昕PDF编辑器莫名躺枪

2022-03-16 14:31

2022年3月15日晚，315晚会上"ZOL中关村在线"等网站因下载站强制安装、弹窗广告等问题被点名。同时被点名的还有PC6下载网站、桔梗下载站、腾牛网等平台，以及马鞍山百助网络科技有限公司，均涉及强制弹窗下载等问题。

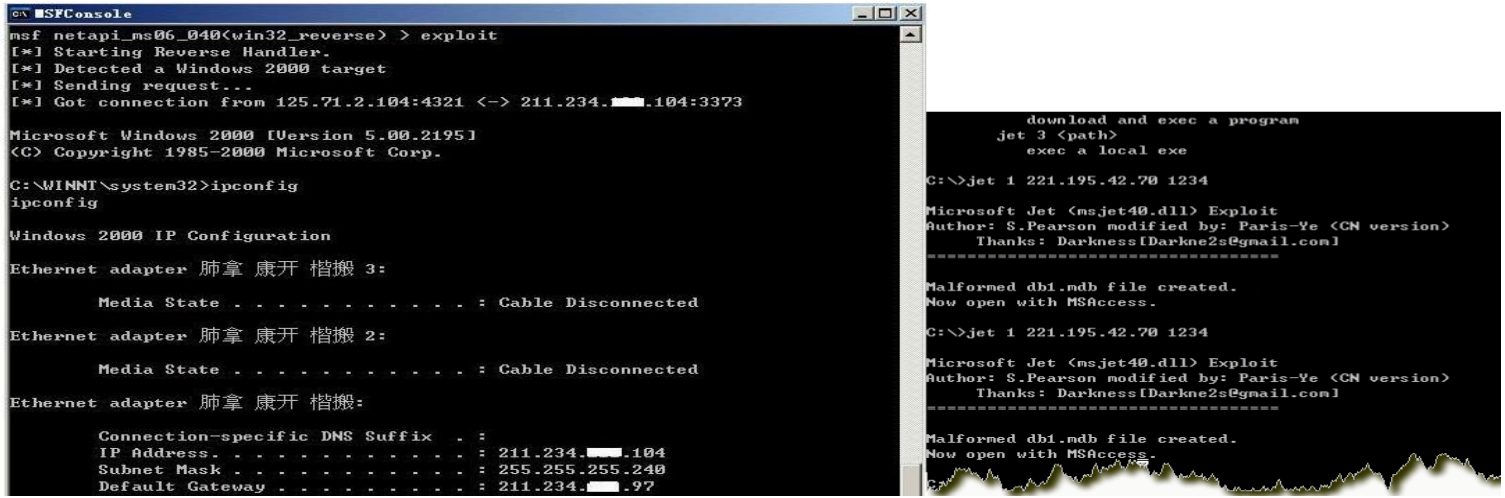
根据晚会视频画面，记者在PC6下载站中尝试下载软件，选择了福昕PDF进行操作演示，记者点击高速下载，很快下载好了安装包，点击安装包显示正在加速模式下载，接着出现一个醒目的"福昕PDF编辑器"，下面还有一行小字写着"热门推荐"以及好几个软件图标，还没来得及看清楚这个页面就消失了，紧接着跳出一个提示框"是否同意用户协议及隐私政策并完成软件安装"，只有一个"是的"选择，点击之后我们所需要的福昕PDF软件开始安装了，电脑变得有些卡顿，右下角还出现一个游戏的弹窗广告，但意外的是安装还没有结束，桌面上就多出了浏览器图标、ABC看图、打印机大师三款软件。

流氓软件

- 具有一定的实用价值但具备电脑病毒和黑客软件的部分特征的软件（特别是难以卸载）；
- 它处在合法软件和电脑病毒之间的灰色地带，同样极大地侵害着电脑用户的权益。也称为灰色软件。

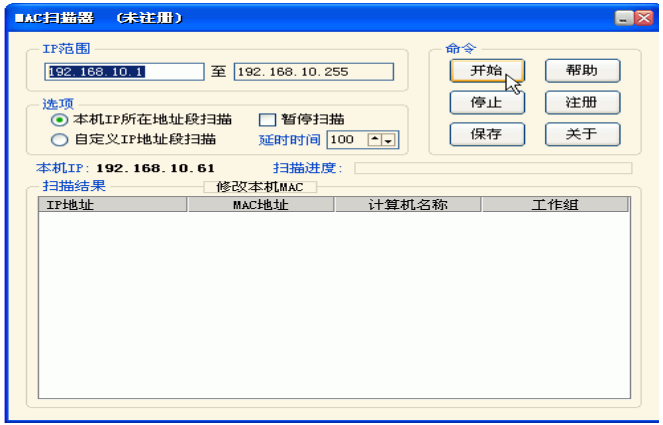
Exploit

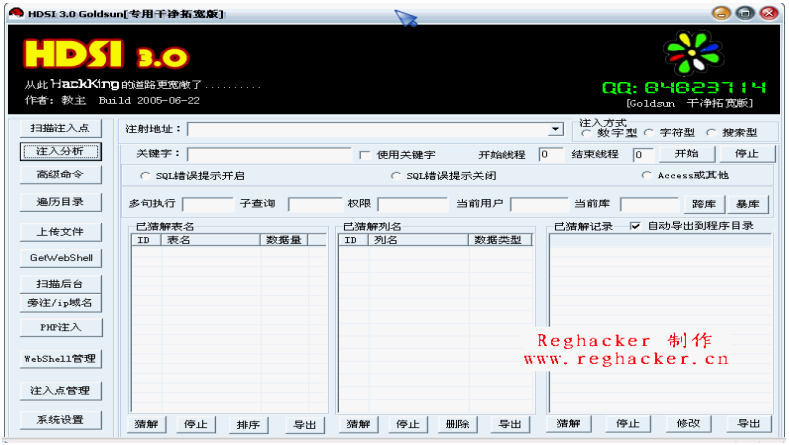
- 精心设计的用于利用特定漏洞以对目标系统进行控制的程序。



黑客工具等

- 黑客工具：各类直接或间接用于网络和主机渗透的软件，如各类扫描器、后门植入工具、密码嗅探器、权限提升工具…





3.4 恶意代码与网络犯罪

- 关于危害计算机信息系统安全的法律条款及司法解释：
- 刑法285、286：
  - http://www.jining.gov.cn/art/2007/8/7/art_325_36.html
- 《中华人民共和国刑法修正案（七）》2009年
  - 阅读链接：http://www.gov.cn/flfg/2009-02/28/content_1246438.htm
- 最高人民法院、最高人民检察院关于办理危害计算机信息系统安全刑事案件应用法律若干问题的解释2011年
  - 阅读链接：https://www.court.gov.cn/fabu-xiangqing-3085.html

中华人民共和国刑法

第二百八十五条 违反国家规定，侵入国家事务、国防建设、尖端科学技术领域的计算机信息系统的，处三年以下有期徒刑或者拘役。

修正案(七)：在刑法第二百八十五条中增加两款作为第二款、第三款：

“违反国家规定，侵入前款规定以外的计算机信息系统或者采用其他技术手段，获取该计算机信息系统中存储、处理或者传输的数据，或者对该计算机信息系统实施非法控制，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金；情节特别严重的，处三年以上七年以下有期徒刑，并处罚金。非法获取计算机信息系统数据、非法控制计算机信息系统罪

“提供专门用于侵入、非法控制计算机信息系统的程序、工具，或者明知他人实施侵入、非法控制计算机信息系统的违法犯罪行为而为其提供程序、工具，情节严重的，依照前款的规定处罚。” 提供侵入、非法控制计算机信息系统程序、工具罪

第二百八十六条 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。 →故意制作、传播计算机病毒等破坏性程序罪

最高人民法院、最高人民检察院关于办理危害计算机信息系统安全刑事案件应用法律若干问题的解释

- 285：
  - 10组
  - 500组
  - 20台
  - 5k/10k
  - 5倍以上

为依法惩治危害计算机信息系统安全的犯罪活动，根据《中华人民共和国刑法》、《全国人民代表大会常务委员会关于维护互联网安全的决定》的规定，现就办理这类刑事案件应用法律的若干问题解释如下：

第一条 非法获取计算机信息系统数据或者非法控制计算机信息系统，具有下列情形之一的，应当认定为刑法第二百八十五条第二款规定的“情节严重”：

（一）获取支付结算、证券交易、期货交易等网络金融服务的身份认证信息十组以上的；

（二）获取第（一）项以外的身份认证信息五百组以上的；

（三）非法控制计算机信息系统二十台以上的；

（四）违法所得五千元以上或者造成经济损失一万元以上的；

（五）其他情节严重的情形。

实施前款规定行为，具有下列情形之一的，应当认定为刑法第二百八十五条第二款规定的“情节特别严重”：

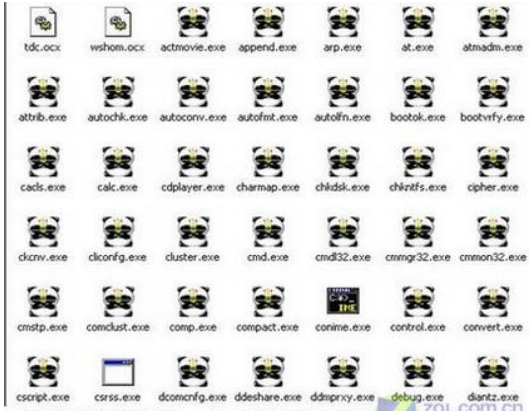
（一）数量或者数额达到前款第（一）项至第（四）项规定标准五倍以上的；

（二）其他情节特别严重的情形。

明知是他人非法控制的计算机信息系统，而对该计算机信息系统的控制权加以利用的，依照前两款的规定定罪处罚。

熊猫烧香

- 努力学习编程技术，赚得人生第一桶金！2006-2007
- 10万
- 学艺不精，将自己直接投入大牢！



XX神器－19岁大一学生的暑期爱好！2014年

动机：

- 展现能力
- 觉得很酷

安全专业
不懂法，太危险！
最高人民法院指导案例

课后思考

1. 计算机病毒与蠕虫的本质区别是什么？
2. 木马与后门程序功能比较类似，他们的本质区别是什么？
3. 统计数据看，近年来木马程序比例增高，传统感染病毒比例降低，原因是什么？
4. 震网stuxnet、DuQu、flam，查阅资料，属于什么类型的恶意软件，为什么？
5. “XX神器”，结合刑法和司法解释，其作者是否触及了相关条款，给出理由。
6. 阅读：823.pdf、2019-2020中国互联网网络安全报告、计算机犯罪相关内容