软件安全—恶意代码机理与防护

C5 恶意代码分类

武汉大学国家网络安全学院 彭国军

guojpeng@whu.edu.cn

本讲提纲

- 2.1恶意代码的定义与发作趋势
- 2.2恶意代码的功能
- 2.3恶意代码的分类
- 2.4恶意代码与法律

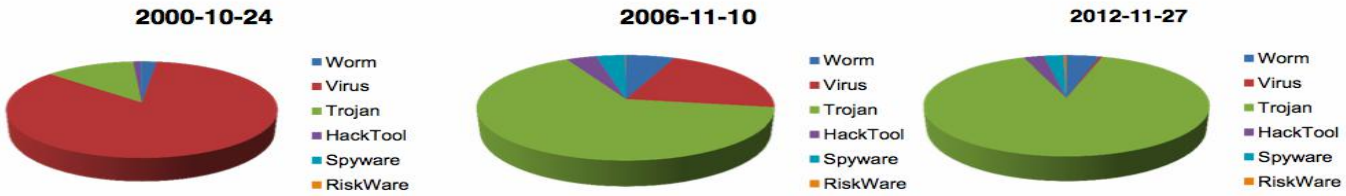
2.1 恶意代码的定义与发作趋势

- 恶意代码（Malicious Code，或MalCode），也称恶意软件（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。

恶意代码发作趋势

2000～2012数据回朔

对话·交流·合作



日期/分类	2000/10/24	2006/11/10	2012/11/27
Worm	512	8109	354049
Virus	21006	27760	29940
Trojan	3066	84811	7262094
HackTool	260	4968	217502
Spyware	37	4899	214570
RiskWare	0	88	25800

来源： Kapersky对应日期病毒名列表

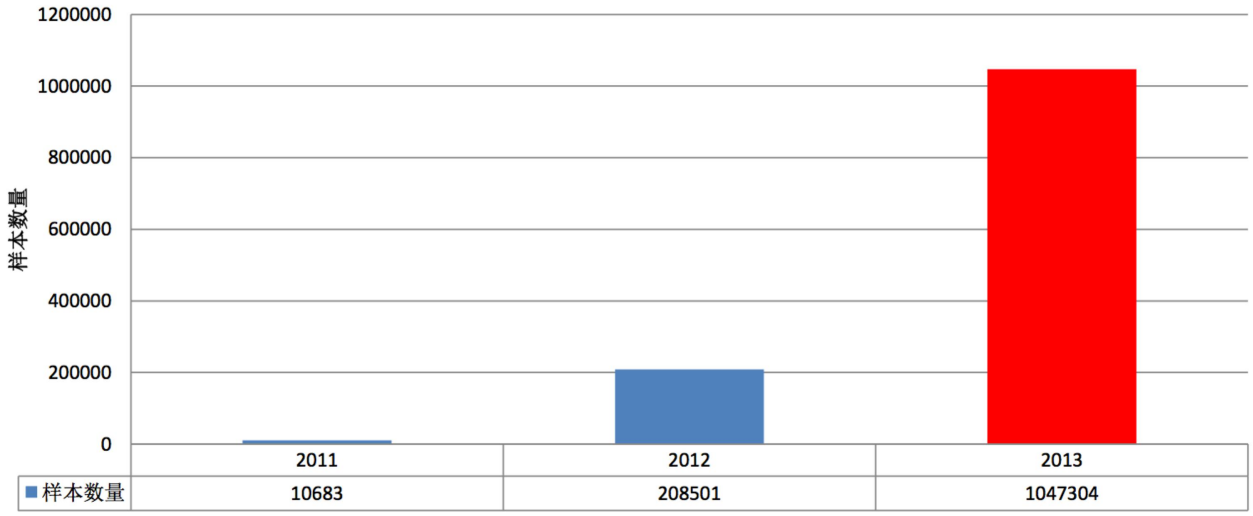
2010年金山数据


病毒感染台次统计（2010年、2009年）
76500000
76000000
75500000
75000000
74500000
74000000
73500000
73000000
72500000
72000000
2009年
2010年
金山网络


2003年以来的新增病毒数量
25000000
20000000
15000000
10000000
5000000
0
13568
20059
50745
240156
283084
13899717
20684223
17988452
2003
2004
2005
2006
2007
2008
2009
2010

移动智能终端恶意软件增长迅猛

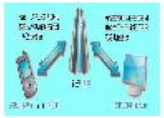
2011－2013年移动恶意软件累计增长数量情况



2011－2013年安天实验室历年移动恶意软件累计数量统计图

X卧底 - 移动智能终端威胁的始作俑者

产 品 展 示



产品名称： 手机x卧底软件
产品售价： 800元
产品规格： 每套
产品备注： 有手机监控卫士（商务卧底软件）让您的手机变成监听器！
产品类别： 手机x卧底软件 >> 手机x卧底软件

产品详细信息

有手机监控卫士（商务卧底软件）让您的手机变成监听器！

商务卧底软件实现了对手机通讯的实时监听监控，使您即便身在千里之外也能对手机进行远程监控。手机超强卫士（商务卧底）允许您指定一个号码（固话，手机，小灵通都可以），通过此号码您可以打往被监控手机（手机超强卫士（商务卧底）的手机）但被监控手机不会响铃、震动，也没有来电显示，只是被激活了其手机内的麦克风设置。此时，被监控手机相当于您的“监听器”，因此不管孩子在哪里，在做什么，您都可以监听到他的谈话和行动，以及所处的场所环境

它最主要的几大功能是：

1. 短信内容记录（发送/接收）手机监控卫士（商务卧底软件）可以使您查阅所有接收、发出的短信内容。）
2. 通话记录（打出/接听）（如果您忘记了前天谁给您打的电话，只要上网查看就知道了） 手机定位功能，拥有全国1500多个城市的电子地图，通过GPS定位达到精确15米的范围。
3. 短信收发时间、通话时间（记录所有拨出、接入的通话记录，包括通话开始、持续时间、联系人等。）
4. 短信/电话的联系人（账户中自动显示与电话号码相对应的通信录里的机主名称）

NSA－ANT工具箱

－APT攻击成为关注重点

间谍设备花样繁多

《明镜》周刊２０１３年１２月３０日报道，美国国安局这个下设团队内部代号为ＡＮＴ，是英文“高级网络技术”的简称，研发的设备主要用于网络设备渗透、手机和计算机监控等。

这家周刊获得一份近５０页的内部名录，详细罗列ＡＮＴ研发的产品、用途及价格。

比如，名录介绍一条经过技术处理的显示器连接线，称可以帮助国安局黑客团队“看到目标显示器上所展示的东西”，每条售价３３美元；

一个特制“短信基站”售价４万美元，可以帮助情报人员模拟目标网络手机信号塔，进而监听目标手机；

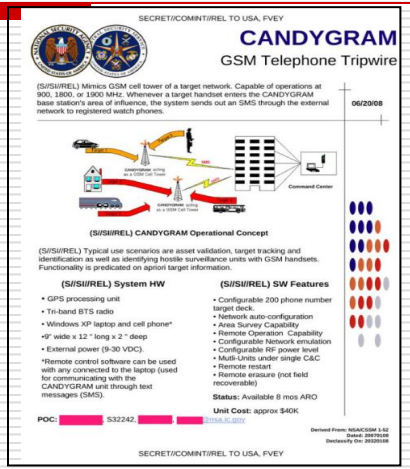
名录中有一种看似普通移动存储装置的计算机监视设备，可以利用无线电信号发送或接收目标计算机的数据，售价为每个２万美元。

《明镜》周刊报道，这份名录的时间为２００８年，其中不少设备可以应用的服务器系统或手机已经退市，因而可以推断名录并不完全。结合当年情况，外界仍可以据此看出美国国安局手中掌握的丰富“谍战”资源。

根据知名企业产品量身定制

这份名录还显示，美国国安局将不少知名信息技术企业为对象，量身打造监视设备，以确保情报获取范围扩展到尽可能广的用户群。这些企业包括美国思科、戴尔、惠普和中国华为等，ＡＮＴ团队研发的部分产品针对前者生产的服务器、计算器或者手机设备。

《明镜》周刊提到，尽管名录对应的２００８年还没有迎来智能手机的全球普及潮，但美国国安局针对手机的间谍设备已经出现。其中，名录还介绍一款研发中的木马病毒，目标就是美国苹果公司的智能手机ｉＰｈｏｎｅ。


SECRET//COMINT//REL TO USA, FVEY

CANDYGRAM

GSM Telephone Tripwire

(S//SI//REL) Mimics GSM cell tower of a target network. Capable of operations at 900, 1800, or 1900 MHz. Whenever a target handset enters the CANDYGRAM base station's area of influence, the system sends out an SMS through the external network to registered watch phones.

06/20/08

Command Center

(S//SI//REL) CANDYGRAM Operational Concept

(S//SI//REL) Typical use scenarios are asset validation, target tracking and identification as well as identifying hostile surveillance units with GSM handsets. Functionality is predicated on apriori target information.

(S//SI//REL) System HW

- GPS processing unit
- Tri-band BTS radio
- Windows XP laptop and cell phone*
- 9" wide x 12 " long x 2 " deep
- External power (9-30 VDC).

*Remote control software can be used with any connected to the laptop (used for communicating with the CANDYGRAM unit through text messages (SMS).

(S//SI//REL) SW Features

- Configurable 200 phone number target deck.
- Network auto-configuration
- Area Survey Capability
- Remote Operation Capability
- Configurable Network emulation
- Configurable RF power level
- Multi-Units under single C&C
- Remote restart
- Remote erasure (not field recoverable)

Status: Available 8 mos ARO

Unit Cost: approx $40K

POC: [redacted], S32242, [redacted], [redacted]@nsa.ic.gov

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

SECRET//COMINT//REL TO USA, FVEY

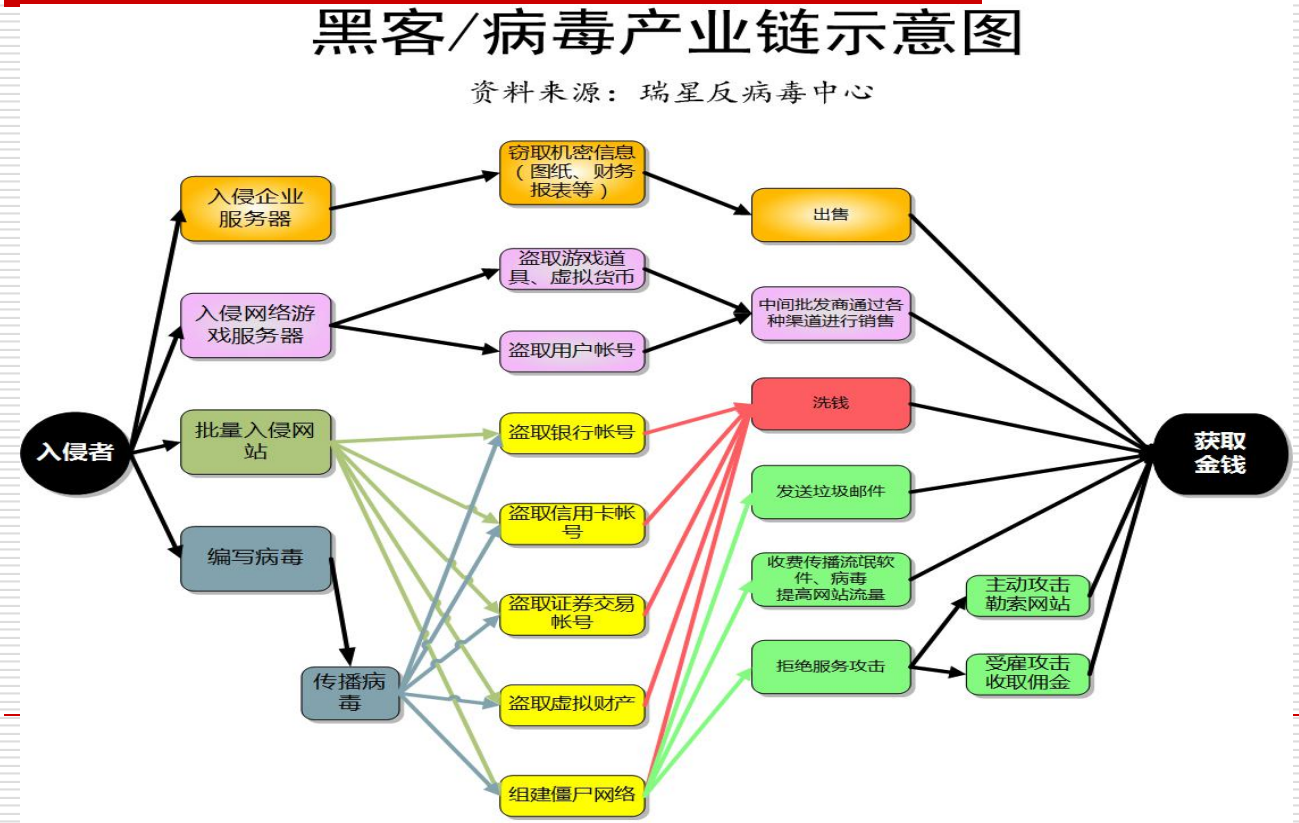
2.2 恶意代码的功能

- 攻击目的是什么？
- 攻击目标有哪些？
- 攻击手段有哪些？

2.2.1 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

黑色产业链 - 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
病毒制造者
牧马人(黑客)
1.漏洞信息
2.病毒
5.肉鸡控制权
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
->商业机密被盗
->隐私活动被盗摄
更多受害者
->发送垃圾邮件
->DDOS攻击
->网站挂马
->建钓鱼网站

2.2.2 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

2.2.3 攻击手段—如何达到攻击目的？

- 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；

- 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。

- 动态控制与渗透拓展攻击路径等
  - 中间系统
  - 相关人员

2.3 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：
  - 计算机病毒、蠕虫
  - 木马、后门
  - Rootkit
  - 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…

- 2003年，Kienzle 和 Elder 从破坏性、网络传播、主动攻击和独立性4 个方面对网络蠕虫进行了定义：网络蠕虫是通过网络传播，无须用户干预能够独立地或者依赖文件共享主动攻击的恶意代码。
  - 根据传播策略,他们把网络蠕虫分为 3 类:Email 蠕虫、文件共享蠕虫和传统蠕虫.

Kienzle DM, Elder MC . Recent worms: A survey and trends. In: Staniford S, ed. Proc. of the ACM CCS Workshop on Rapid Malcode (WORM 2003). Washington, 2003.

- 南开大学郑辉博士认为，蠕虫具有主动攻击、行踪隐蔽、利用漏洞、造成网络拥塞、降低系统性能、产生安全隐患、反复性和破坏性等特征，并给出相应的定义：“网络蠕虫是无须计算机使用者干预即可运行的独立程序，它通过不停地获得网络中存在漏洞的计算机上的部分或全部控制权来进行传播”。
  - 该定义包含了 Kienzle 和 Elder 定义的后两类蠕虫,不包括 E-mail 蠕虫.

郑辉. Internet蠕虫研究[博士学位论文].天津:南开大学信息技术科学学院,2003.

- 中科院文伟平博士等认为，“网络蠕虫是一种智能化、自动化，综合网络攻击、密码学和计算机病毒技术，不需要计算机使用者干预即可运行的攻击程序或代码。它会扫描和攻击网络上存在系统漏洞的节点主机，通过局域网或者国际互联网从一个节点传播到另外一个节点。
  - 该定义体现了新一代网络蠕虫智能化、自动化和高技术化的特征，是对郑辉网络蠕虫定义的扩展。

文伟平 等:网络蠕虫研究与进展. 软件学报，2004,15(8)：1208-1219 。

另外一种被业界广泛采用的分类方法

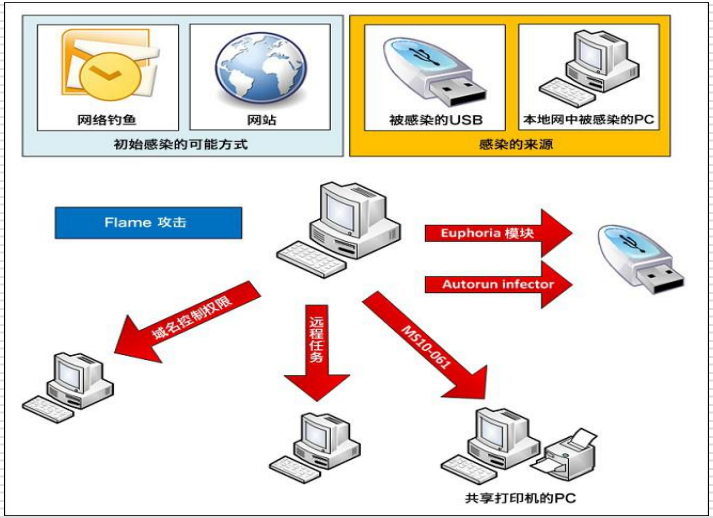
- 1988年Morris蠕虫爆发后，Eugene H. Spafford 为了区分蠕虫和病毒，给出蠕虫和计算机病毒的定义：

  - “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”。

Flame（火焰）



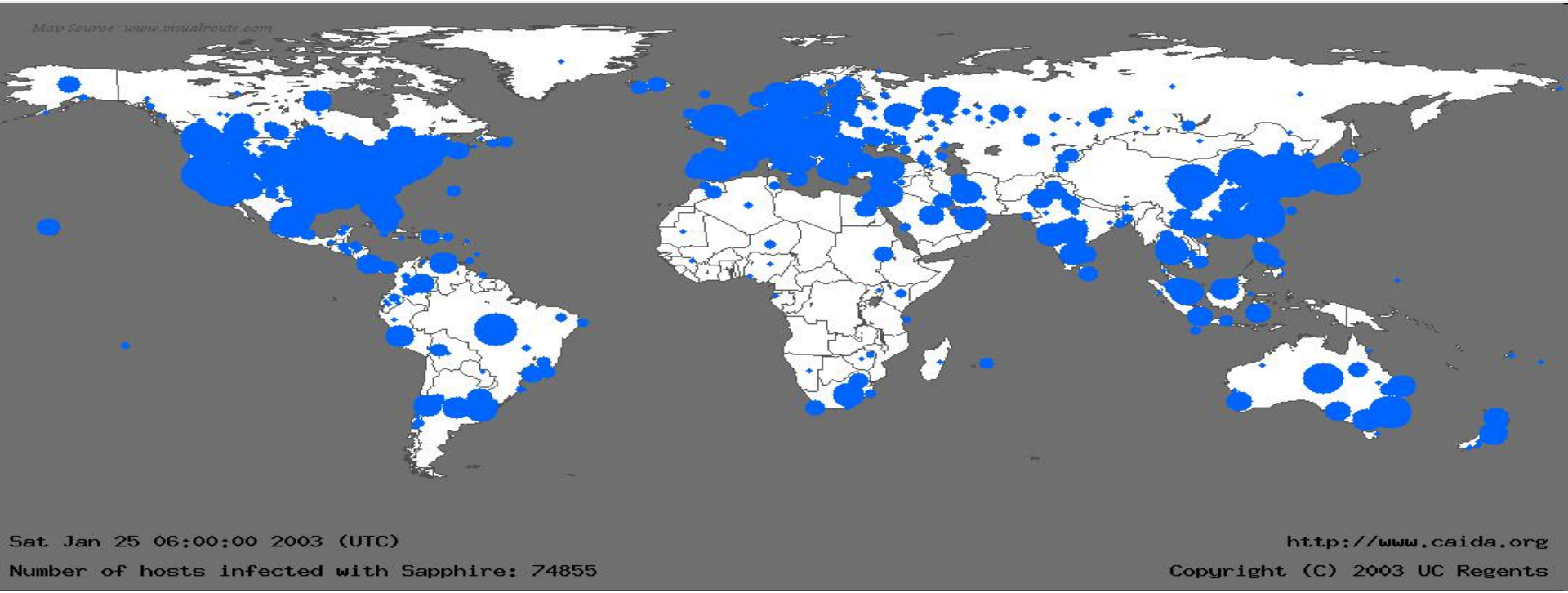
5 种加密算法，3 种压缩技术，至少 5 种文件格式，65万行代码，编写复杂。卡巴斯基实验室表示，要全面了解Flame病毒，可能得花上10年时间。

卡巴斯基联合创始人兼CEO尤金·卡巴斯基(Eugene Kaspersky)在一份声明中表示：“Stuxnet和DuQu病毒属于一系列攻击的组成部分，并引起了全球安全人士的警惕。Flame病毒的发现，意味着互联网安全大战进入到新阶段。我们必须明白，诸如Flame等病毒，能够被轻松用来攻击任何国家。”

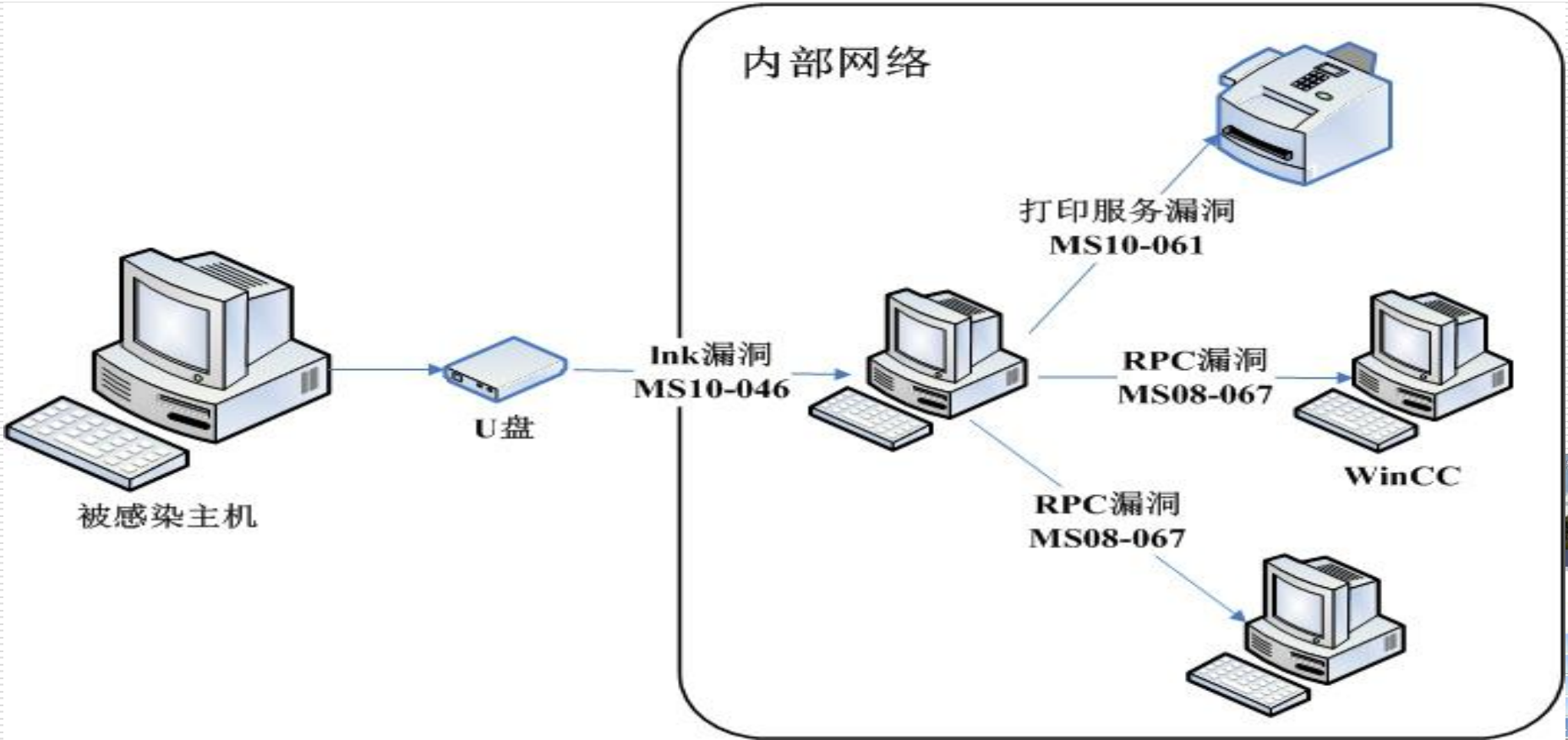
2003年以来的部分典型重大蠕虫事件

- 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)
  - 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

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

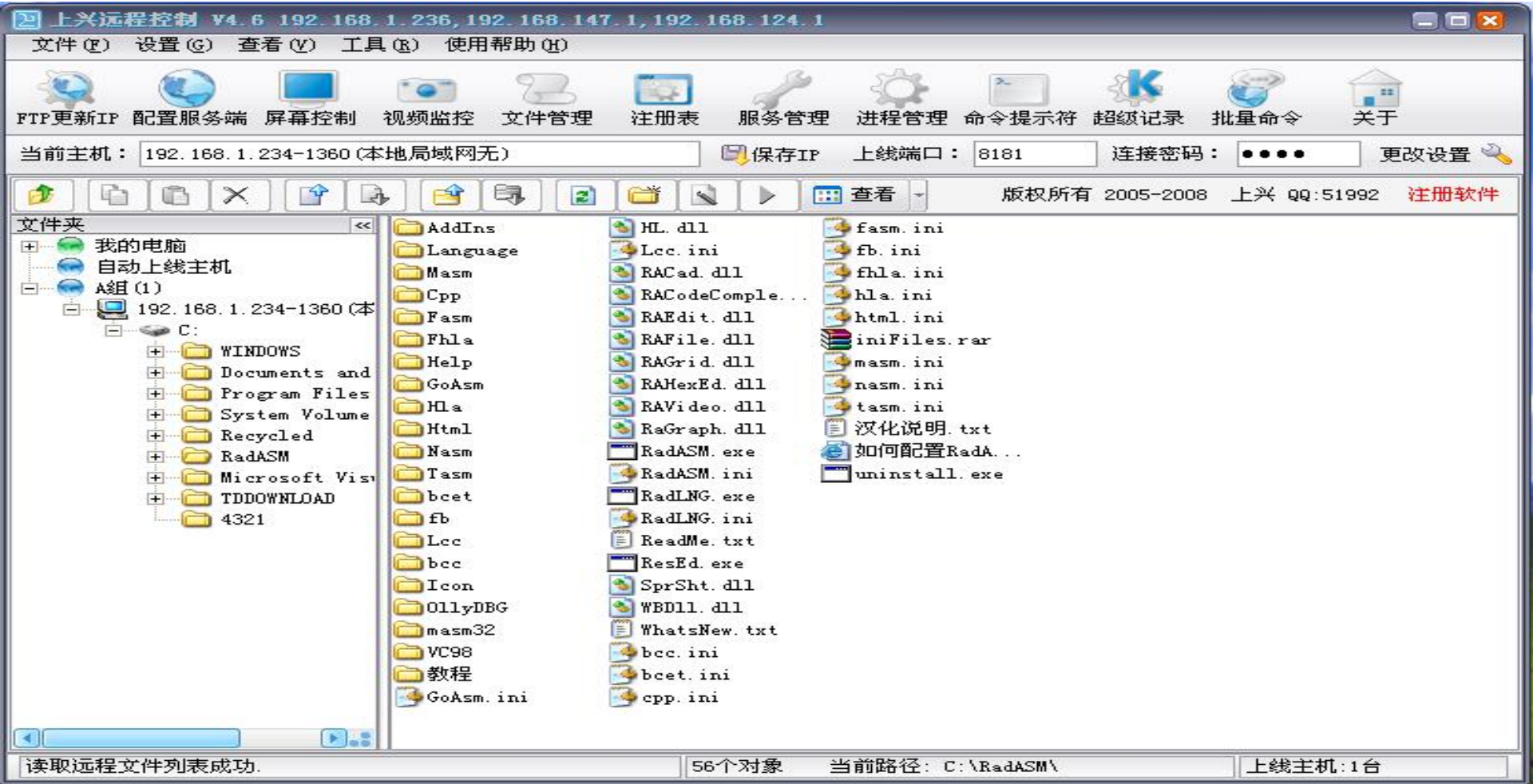


Stuxnet(超级工厂病毒)
—内网摆渡



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、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…

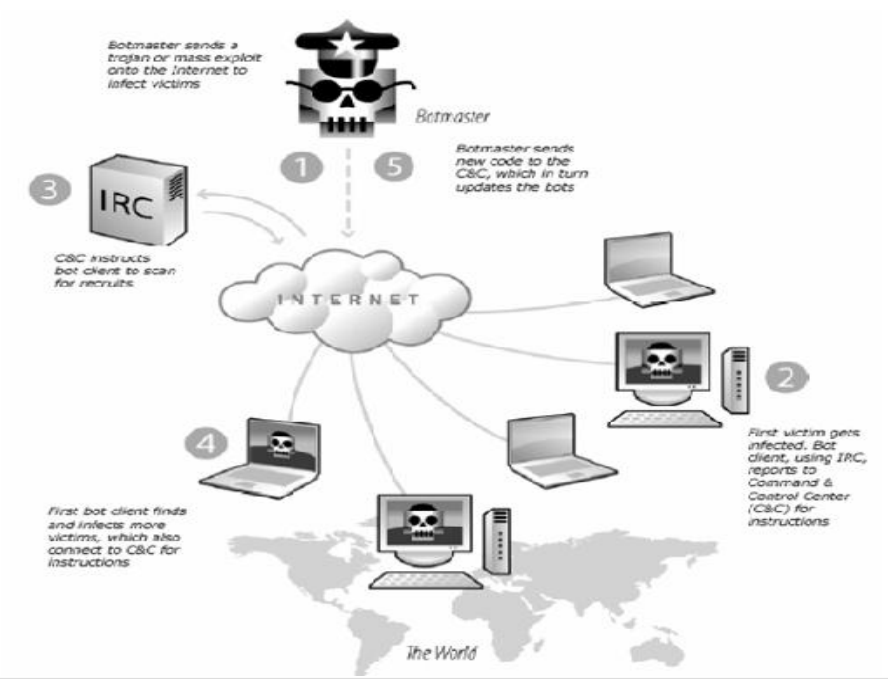

上兴远程控制 V4.6 192.168.1.236,192.168.147.1,192.168.124.1
文件(F) 设置(G) 查看(V) 工具(R) 使用帮助(H)
FTP更新IP
配置服务端
屏幕控制
视频监控
文件管理
注册表
服务管理
进程管理
命令提示符
超级记录
批量命令
关于
当前主机： 192.168.1.234-1360(本地局域网无)
保存IP
上线端口： 8181
连接密码： ••••
更改设置
查看
版权所有 2005-2008 上兴 QQ:51992
注册软件
文件夹
我的电脑
自动上线主机
A组(1)
192.168.1.234-1360(本
C:
WINDOWS
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

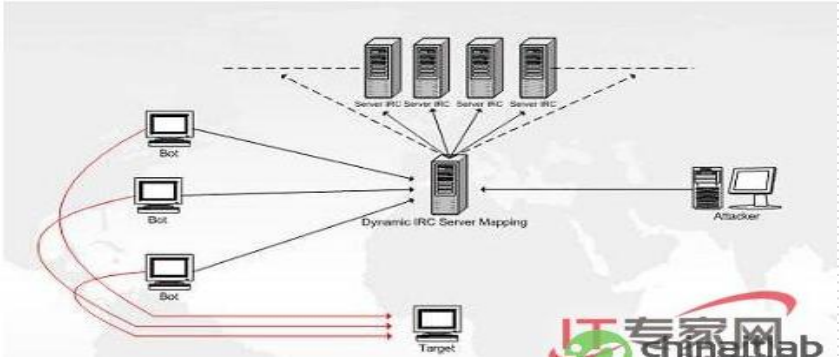
网络恶意代码的分类（续）

4. **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。**
   - **如RootKit、Hkdef、ByShell…**

5. **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


Botmaster sends a trojan or mass exploit onto the Internet to infect victims
Botmaster
1
5
Botmaster sends new code to the C&C, which in turn updates the bots
3
IRC
C&C instructs bot client to scan for recruits
INTERNET
2
First victim gets infected. Bot client, using IRC, reports to Command & Control Center (C&C) for instructions
4
First bot client finds and infects more victims, which also connect to C&C for instructions
The World


Server IRC
Server IRC
Server IRC
Server IRC
Bot
Bot
Bot
Dynamic IRC Server Mapping
Attacker
Target

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。

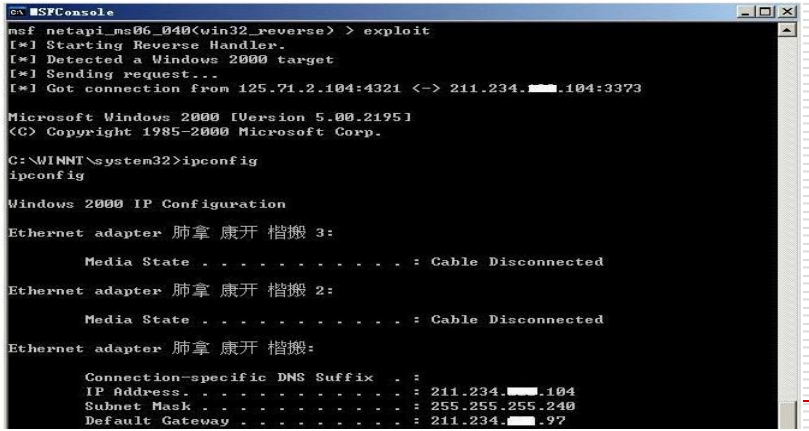
流氓软件

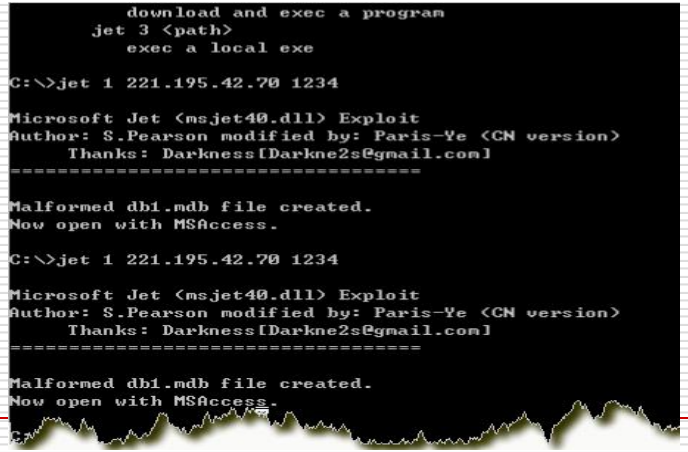
- 具有一定的实用价值但具备电脑病毒和黑客软件的部分特征的软件（特别是难以卸载）；

- 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

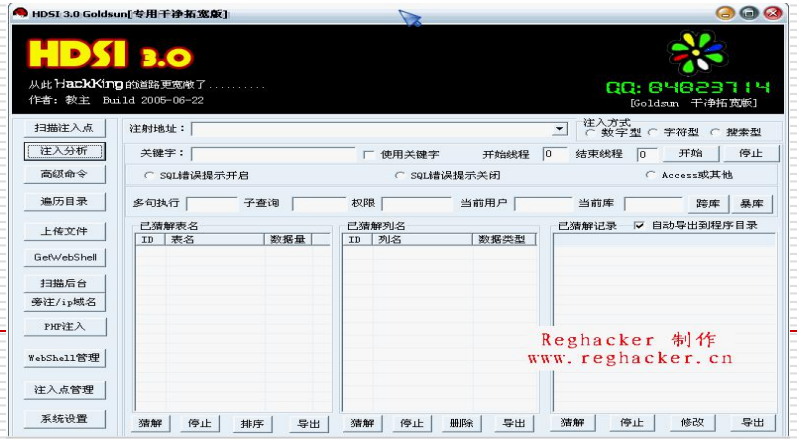
- 精心设计的用于利用特定漏洞以对目标系统进行控制的程序。





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...



5.4 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）》
  - 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
  - http://www.chinacourt.org/law/detail/2011/08/id/145416.shtml

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。”→非法获取计算机数据罪、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。”→为侵入、非法控制计算机信息系统非法提供程序、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

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—科技改变命运！？

- 努力学习编程技术，赚得人生第一桶金！（1个万）
- 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！

动机：

- 展现能力
- 觉得很酷

信息安全专业
不懂法，太危险！！！

拓展视频学习


云课堂
首页
全部课程
计算机专业体系
微专业
我的云课堂
客户端
播放视频简介
信息安全专业-大学生专业学习引导专场
信息安全专业-大学生专业学习引导专场
讲师：张焕国 肖新光 李建华 杨翼龙 潘柱廷 魏强 彭国军 等
发布者：XDef安全峰会
分类：IT/互联网 网络技术 职场技能 自我管理


XDef 2014
第三届全国网络与信息安全防护峰会
信息安全专业 —— 大学生专业学习引导专场
2014年11月20日—23日 湖北 · 武汉


云课堂
首页
全部课程
计算机专业体系
章节 1 走出迷茫-大学生专业学习引导计划
课时1 彭国军：走出迷茫- 大学生专业学习引导计划（字幕版）
章节 2 信息安全学科概论
课时2 张焕国：信息安全学科概论（字幕版）
章节 3 全球信息安全的企业创新与产业景观
课时3 肖新光：全球信息安全的企业创新与产业景观（字幕版）
章节 4 从安全思维谈到心思的修炼
课时4 潘柱廷：从安全思维谈到心思的修炼（字幕版）
章节 5 内容安全与专业学习引导
课时5 李建华：内容安全与专业学习引导（字幕版）
章节 6 Web安全与专业学习引导
课时6 杨翼龙：Web安全实战（字幕版）
章节 7 软件漏洞分析与专业学习引导
课时7 魏强：软件漏洞分析与专业学习引导（字幕版）
章节 8 恶意代码与专业学习引导
课时8 彭国军：恶意代码与专业学习引导（字幕版）

信息安全专业-大学生专业学习引导专场

大学生引导专场现场

武汉大学教授 张焕国

知道创宇创始人兼CTO 杨冀龙

启明星辰公司首席战略官 潘柱廷

安天实验室首席技术架构师 肖新光

上海交通大学信息安全工程学院教授 李建华

解放军信息工程大学四院副教授 魏强

武汉大学计算机学院副教授 彭国军

课后思考

- 计算机病毒和网络蠕虫都可以进行自我传播，那他们的本质区别是什么？
- 特洛伊木马和后门的功能类似，那他们的本质区别是什么？
- 为何计算机病毒的比例越来越低，而木马程序的比例越来越高？
- 请查阅Stuxnet、Duqu以及Flame的功能和传播方式，他们各自应该属于哪一类恶意软件？为什么？
- 请进一步了解“XX神器”事件的相关资料，请结合我国刑法及相关司法解释分析，该事件是否触犯了我国刑法相关条款？并给出你的理由。