

2021-2022学年春季学期

网络攻防基础
Network Attack and Defense

授课团队：张玉清、龚晓锐、吴槟
助 教：杨毅宇

第三部分：网络攻击高级技术与前沿技术

- 第一次课：病毒与各类恶意软件
- 第二次课：网络战与信息战
- 第三次课：隐蔽回传技术、基于脚本的恶意代码、网安行业分析

第三部分：网络攻击高级技术与前沿技术

○提醒：加分实验题目（10分）：

- 如何让Win10不在后台偷偷下载更新，占用网络带宽？（所有版本的Win10）
- 如何在Win7、Win8、Win10上彻底删除PowerShell？
- 以上两个题目最先提交报告且完美解答的3位同学得10分。如部分解答正确得3分，如解答完全错误或文不对题则扣10分，且机会顺延给下一个同学
- 报告发送至2109343050@qq.com，如有代码或可执行程序，务必用zip加密压缩，“北京雁栖湖大学”

内容概要

- 一、网络战
- 二、APT攻击的相关概念
- 三、APT攻击实例分析
- 四、信息战

中美撞机事件

- 2001 年 4 月 1 日早晨，美国一架 EP-3 侦察机进入中国南海上空，中国派出两架军用飞机对其进行监视（其中一架就是王伟驾驶的 编号81192 的歼-8 II 战斗机）。
- 不料美机突然转向，向中方飞机直冲过来，导致其机头和左翼与王伟的飞机相撞坠毁。

可能愚人节过傻了，也可能本就想这样，美国士兵驾驶 EP-3 侦察机突然冲向王伟的战机，据同行的赵宇回忆：王伟战机的尾部被 EP-3 侦察机的螺旋桨刮得“像纸片一样”飞散开了，飞机开始失控，翻滚下坠。起初，王伟不顾性命，试图挽救战机，最后，在赵宇的大声命令下，王伟才选择了跳伞。王伟失踪后，中国军方立即派出大量中国军民，进行了长达 14 天的搜救，可惜，还是没能找回王伟。



中美撞机事件

● 美国人的挑衅：

●4月4日，美国黑客组织 PoizonB0x”，对域名为 “.cn” 的网站
 进行攻击。据不完全统计，其一共进行了 283 次攻击。



中美撞机事件

○美国人的挑衅：

○4月4日，美国黑客组织 PoizonB0x ”，对域名为 “.cn ” 的网站

进

○该客密

○还吧

○美国

○文

○大

○复



黑在

起来

红客的反击

- 4月30日，Lion 在红客联盟平台上，召开“攻击美国网络动员大会”，商议五一期间怎么对美国网站进行攻



红客的反击

○ 5月4日，青年节特别行动：8万多中国红客，集中攻击美国白宫网站

○ 大闹白宫网站，提供信息。

○ 是



红客的反击

- 一直持续到5月8日，正好纪念了1999年5月8日，北约轰炸南联盟大使馆时，死去的三名中国烈士。



此次网络战的结果

- 单看结果：没有输赢，因为中美双方的网站都有沦陷，而且彼此谁也不服谁
- 收获：告诉世界，中国人是不可欺负的，保证了后来的几年内网络相对太平
- 代价：爱国举动给美国人声称的“制裁中国”留下口实和把柄：
 - 当美国一家独大时，自己可以做任何事，此时网络可以没有游戏规则
 - 当美国认为其他国家将要达到和自己相近的量级时，就开始设定游戏规则（网络主权、侵犯知识产权）
 - 当美国认为其他国家已经和自己相近时，就开始更改自己定的游戏规则
- 中国接招后，美国进一步将网络战与贸易、汇率、TW等“筹码”进行结合，将中国推向不利的地位
 - 此时为何不提“网络民主”、“网络无国界”？

美国的网络战政策



国家立法
保护边界

2009年初，经过60天的网络空间安全评估，美国正式成立网络战司令部，网络安全力量进入统一协调发展的“快车道”

美国政府2011.5.16率先提出了“网络空间行动策略”，奥巴马称：这是“美国第一次针对网络空间制定的全盘计划”

2013年，美热炒“中国涉军黑客”事件，借机扩编网络空间司令部由900人到4900人，宣布3年内扩建40支网络战部队

2014年，美国防部发布《四年防务评估报告》，明确提出“投资新扩展的网络能力，建设133支网络任务部队”



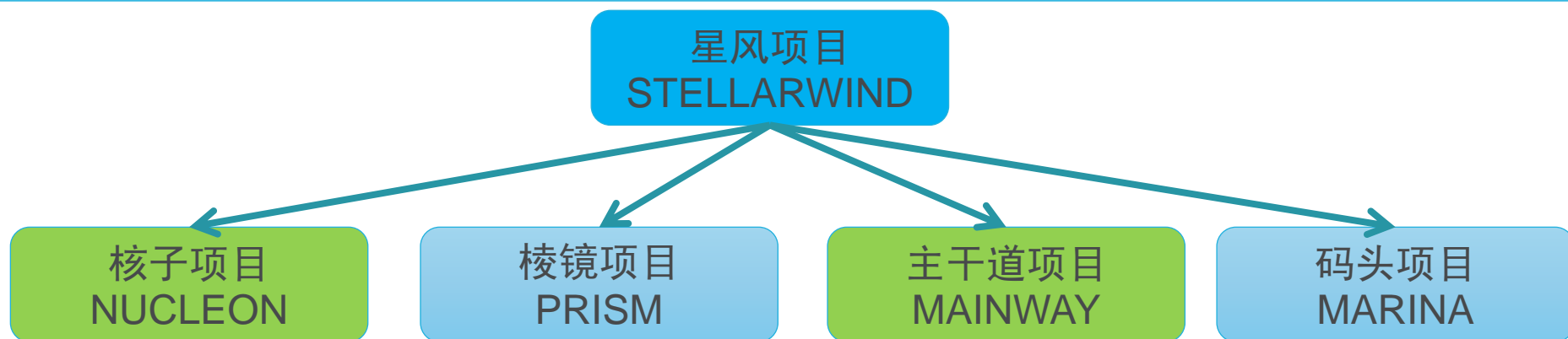
美国网络部队

| 序号 | 国家 | 部队名称 | 规模 |
|----|-----|--------------------|--------|
| 1 | 美国 | JFCCNW部队 (140部队) | 约10万人 |
| 2 | 俄罗斯 | 科技连 | 约1.2万人 |
| 3 | 以色列 | 8200部队 | 约5000人 |
| 4 | 法国 | CALID网络防御部队 | 约400人 |
| 5 | 英国 | 第77旅 | 约1500人 |
| 6 | 德国 | 信息和计算机网络操作部 | 约6000人 |
| 7 | 日本 | 网络空间防卫队 (CDU) | 约5000人 |
| 8 | 韩国 | 反黑客部队 | 约1000人 |
| 9 | 伊朗 | 伊朗网络军团 | 未知 |
| 10 | 印度 | 陆海空三军联合计算机应急分队 | 约50万人 |
| 11 | 朝鲜 | 121部队 | 约3000人 |

○主要战绩

- 2011年，通过监听通信数据成功发现本拉登藏身点
- 2014年，对朝鲜攻击索尼事件进行报复，攻击造成朝鲜全网瘫痪

NSA四大监视项目



- “棱镜”和“核子”负责截取内容
- “核子”负责截获电话通话者对话内容及关键词
- “棱镜”负责监视互联网，从包括微软、谷歌、雅虎、Facebook、PalTalk、AOL、Skype、YouTube以及苹果等美国IT巨头的公司服务器上收集个人信息
- “主干道”和“码头”对通信和互联网的“元数据”进行存储和分析
- “主干道”负责秘密监视电话信息，包括通话或通信的时间、地点、使用设备、参与者，但不会窃听通话内容
- “码头”负责监控电子邮件、网上聊天系统以及其他借助互联网交流的媒介

NSA武器库曝光

- 2016年8月13日，一个名叫“影子中间人”的黑客组织通过社交平台称，已攻入NSA的网络“武器库”——“方程式组织”，并在Github和Tumblr等网络平台上泄露了其中部分黑客工具和数据。
- 8月19日，通过对比证实，泄露出的“武器”中的MSGID追踪代码与斯诺登提供的NSA绝密文件中记载的相同

| Name | | Size |
|-----------------|-------------------------------------------------------------------------------------|----------|
| ▶ BANANAGLEE |  | 6 items |
| ▶ BARGLEE | | 1 item |
| ▶ BLATSTING | | 7 items |
| ▶ BUZZDIRECTION | | 2 items |
| ▶ EXPLOITS | | 8 items |
| ▶ OPS | | 6 items |
| ▶ SCRIPTS | | 33 items |
| ▶ TOOLS | | 15 items |
| ▶ TURBO | | 2 items |
| | | |

NSA武器库曝光

- 2017年1月12日，“影子经纪人”放出Equation Group 组件中的61个文件
- 2017年4月，为了抗议美国袭击叙利亚空军基地，影子经纪人曝光了Equation Group武器库的解密密钥
CrDj”(;Va.*NdlnzB9M?@K2)#>deB7mN, 让世界上所有人都可以查看美国的网络战武器
- 这里面就包含了著名了“永恒之蓝”，被不明黑客组织利用改良作为 SMB远程命令执行工具实施感染

内容概要

- 一、网络战
- 二、APT攻击的相关概念
- 三、APT攻击实例分析
- 四、信息战

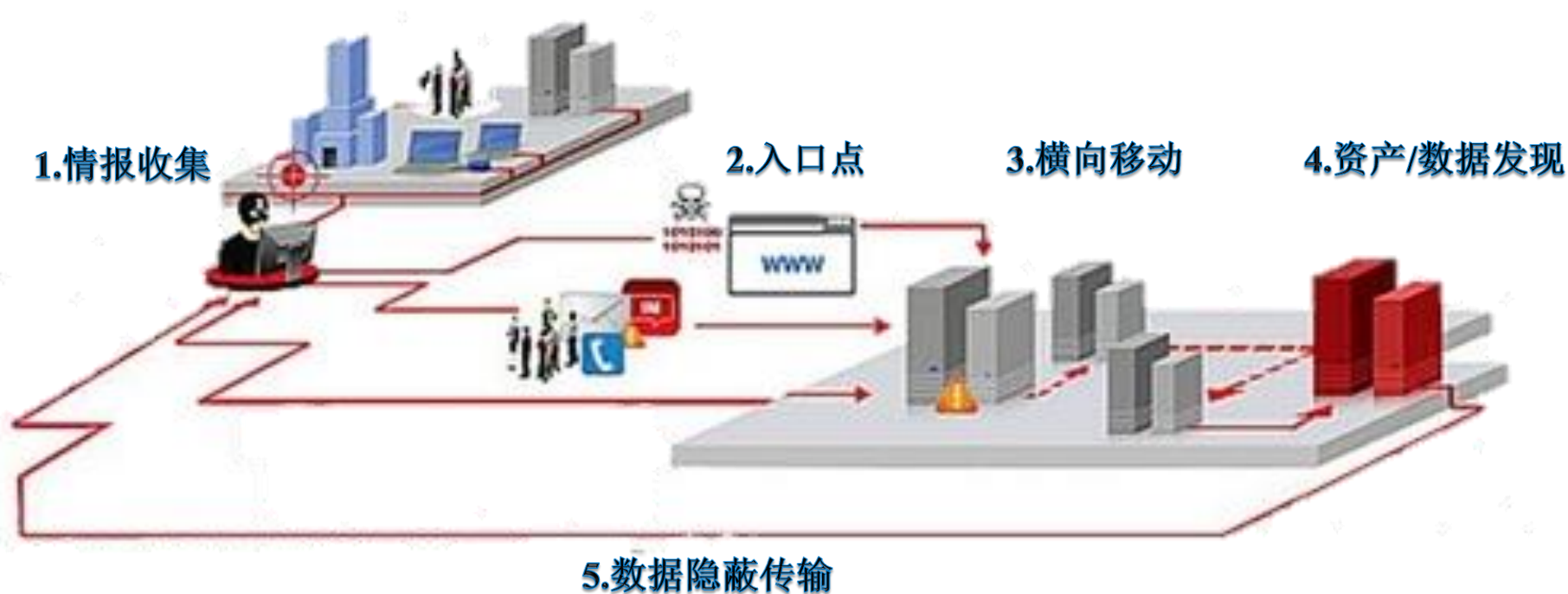
APT定义与要素

- APT : **A**dvanced **P**ersistent **T**hreat (高级持续性威胁)
 - **A**dvanced : (攻击水平) 高超
 - **P**ersistent : 威胁持续存在
 - **T**hreat : 可窃取严密保护下的信息 , 破坏物理隔离系统
- APT是一种网络战(Cyberwar)的重要表现形式
- 网络战的定义是 : 一个民族国家为渗透另一个国家的计算机或网络进行破坏和刺探的行为
- APT两大目标
 - 破坏系统
 - 窃取情报

APT定义与要素

○APT主要攻击环节：

1. 情报收集
2. 入口点渗透
3. 横向移动
4. 资产发现
5. 隐蔽回传



APT攻击的常用名词

- 0day
- 1day
- RAT
- 特马
- C&C , CC , C2
- DGA
- 白加黑
- Keylogger
- 社工
- 后门
- 鱼叉
- 水坑

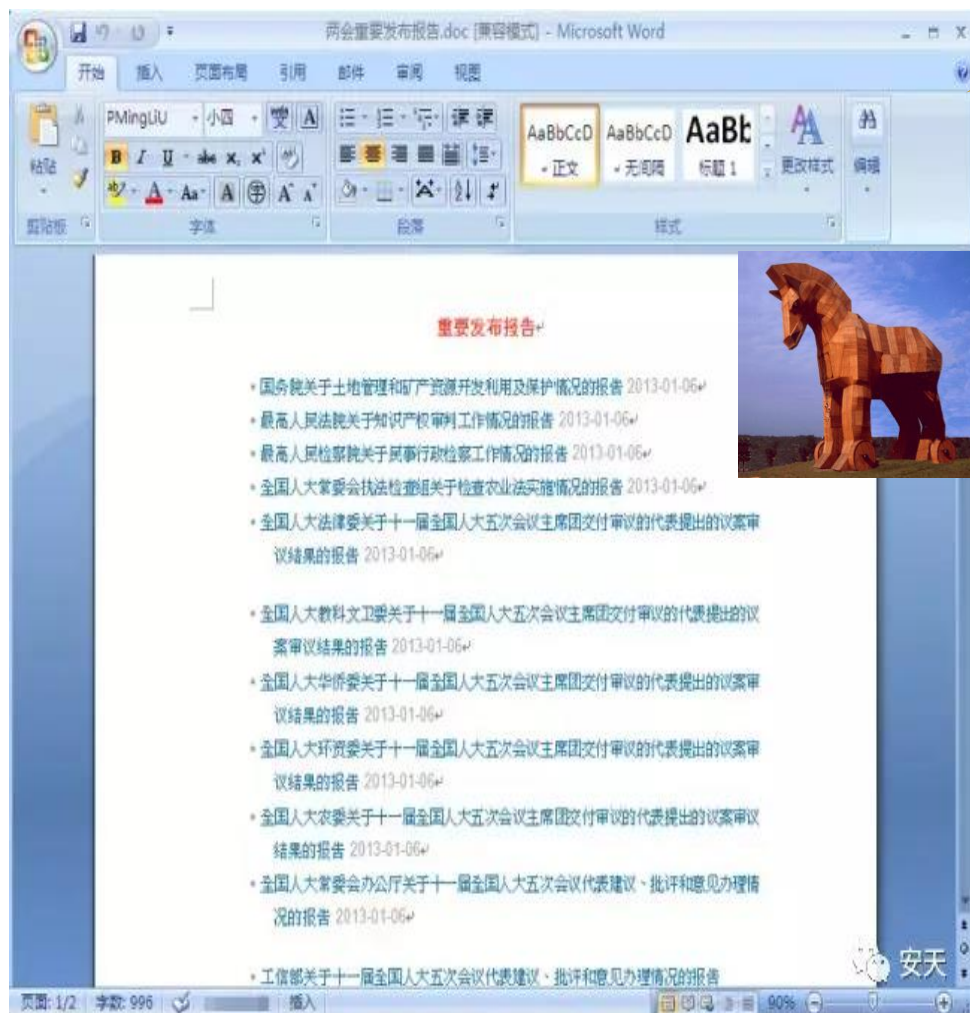
- 0day：危害极大的未公开漏洞
- 0day可怕之处：
 - 未公开：看不见的才是最可怕的
 - 可交易：越来越多的破解者们，已经把目光从率先发布漏洞信息的荣誉感转变到利用这些漏洞得到经济利益上
- 在国外，一个操作系统或数据库的远程溢出源码可以卖到数千美元甚至更高



- 1day：刚刚被公布的，还没有来得及被全面修补的漏洞
- Nday：早已披露的，但用户未及时修复陈旧漏洞
- 1day的用处：
 - 已公开，价格较低
 - 使用自动化利用工具，抢占先机
- Nday的用处：
 - 大规模利用，收益率确定（多份《安全事件观察报告》指出，由历史漏洞造成的安全事件占比高达 34%）
 - 增强隐蔽性、潜伏性
 - 充分挖掘安全意识缺乏者的价值（Botnet忠实群体）

○RAT : Remote Access Tool

Dropper



RAT&特马

- RAT : Remote Access Tool
- 特马：为了某次攻击行为特别定制的，针对某个人、某个系统或某个场景的RAT
- 最大特别：不是砒霜，不是鹤顶红，也不是WMD（按需生产）

在投放前就针对性的使用各种杀毒软件进行了测试，能够和杀毒软件“和平共处”

免杀能力

精心准备的毒药

穿透能力

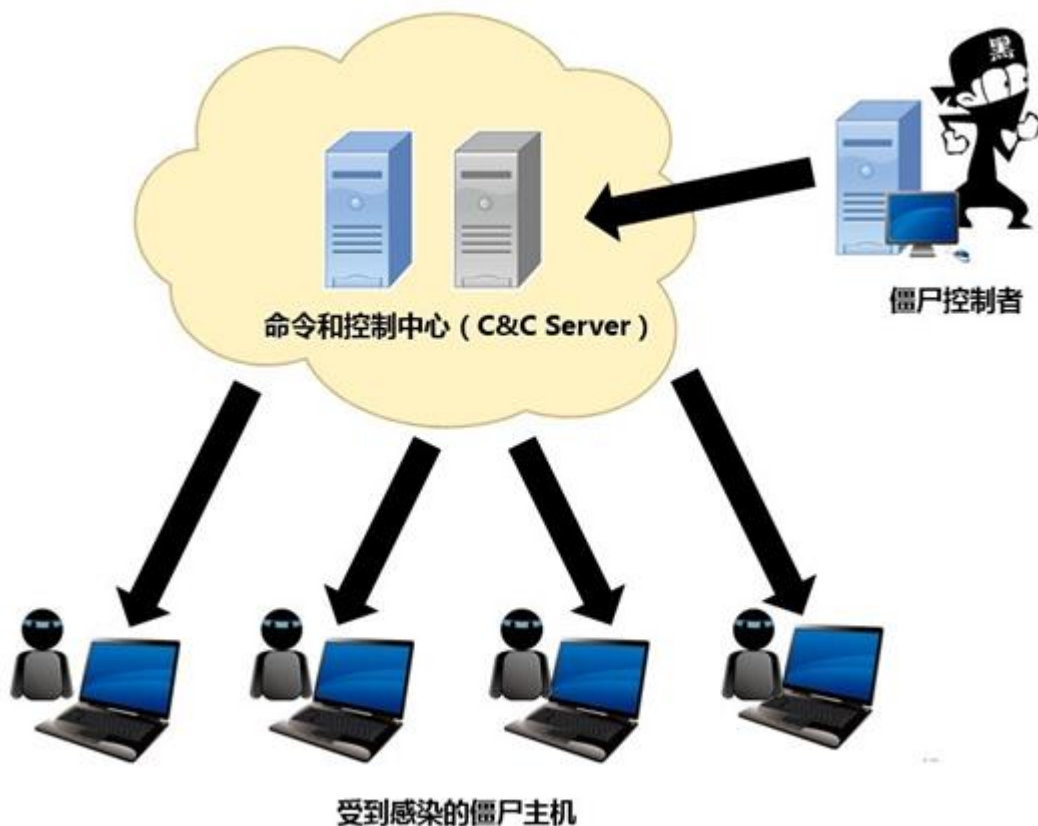
能够在使用了包过滤、应用网关、状态检测、复合型、ISA代理等防火网的网络环境保证数据回传

隐蔽能力

能够躲避一般管理员常用的检测工具，使之能够在系统中隐身

- 特马分类：怎么分都有理
- 按通信方式：不通信、直连、端口复用、反弹端口、反弹代理
- 按场景用途：破坏类、控守类、下载类、驻留类、窃密类、渗透类
- 按寄宿方式：操作系统、应用程序、硬件平台
- 特马怎么做？
- 从采集到的样本可以看出，绝大部分是针对某个漏洞与开源木马的结合：
 - QuasXX、Dark CoXXX、GhXXX、PoisXXXX , ZXXX、babyfXXX

- C&C : Command and Control , 命令与控制 , 原来主要指应用于僵尸网络的CC服务器 , 是建立在控制者与被控节点之间的通道
- 产生的原因 : 被控节点上的恶意软件 , 往往不能自动进行活动 , 通常需要通过网络与攻击者进行交互。所以需要需要一个CC服务器为恶意软件与攻击者进行交互服务
- 久而久之 , CC服务器成为很多攻击者操纵大部分入侵、攻击手段的“基础设施”

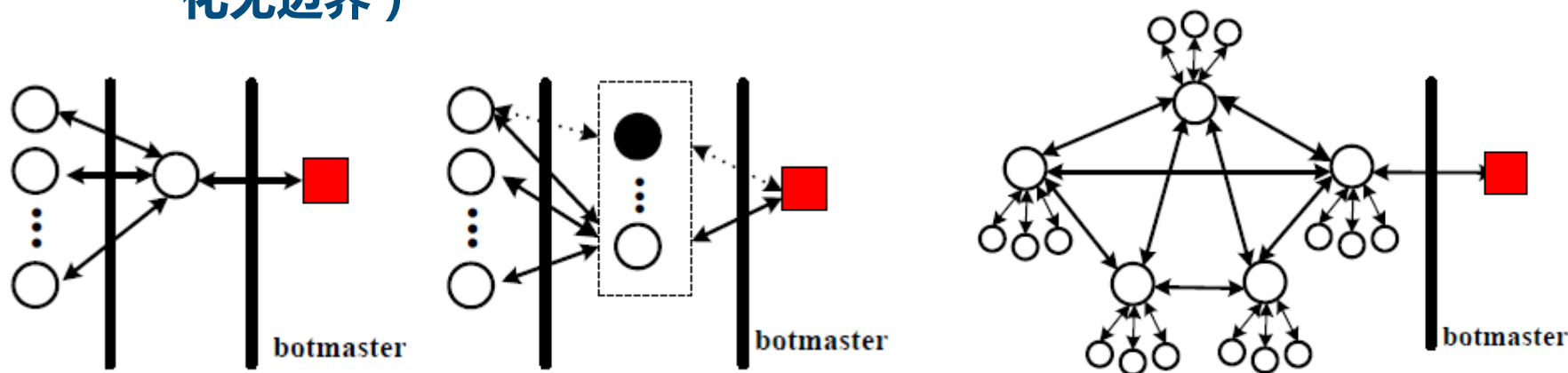


○C2在APT中的作用：

- 指令下发：通过C2通道进行远控指令的交互
- 资源下发：初次投递的载荷不会太大，通常要拉取二段exp进行驻留
- 数据上传：回传一些文件或者数据

○APT中使用C2的特点：

- 侧重与其它“武器”组合运用
- 追求隐秘的CC信道
- 建立过程中目标“聚焦”，区分内外边界（Botnet目标宽广扁平化无边界）



- 大致分类：（网际数据传输，必须要传输层以上协议）
 - 传输协议层：TCP、UDP
 - 应用协议层：HTTP、DNS
 - 应用服务层：twitter、云盘
- HTTP优势：
 - 应用层网络协议，简单易用、成熟稳定
 - Domain-IP模式，方便基础设施的迁移
 - 允许传输任何类型数据对象，配合GET、POST、HEAD满足大多数命令交互需求
 - 基于HTTP的web应用开发成熟，可在短时间开发、部署
 - 最常见的流量类型，不会引起防火墙和IDS注意
- 以HTTP为基础的CC占APT事件的近90%
- 缺陷：IP或者域名容易被拉入黑名单

- 为了应对IP或者域名会被拉入黑名单的问题，攻击者可以用DGA算法生成用作域名的伪随机字符串
- 攻击者和被控节点上的恶意软件根据同一算法，可以确定正在请求的域名，进行注册、解析
- 主要原理：（全部或部分）域名根据时间或者其他种子因素的变化而变化
 - fryjntzfvti.biz , asdfg.info , B007wedcf.com和B007bjgkre.com
- 这种动态变化的域名可以很好规避黑名单安全策略。加大发现攻击的难度
- 此外，还有其他的技术实例将在“隐蔽回传技术”章节中进行介绍

○免杀技术的一种

- 传统的恶意程序都是由单一文件构成的，因此为了避免被发现，可以由多个程序协作组合
- 结构：Exe(白) ---load---> dll (黑) ---load---> 恶意代码 (shellcode)

○白exe的选择：

- 带有正规厂商的签名
- 依赖最小，不同的windows版本下都可以运行
- Exe调用了自己的dll
- 尽可能的小

○黑dll的编写：

- 按照原dll的输出表构造编写一个伪造的dll, 在dll中的合适位置编写加载shellcode的代码，于是exe+dll共同组成了一个shellcode加载器

白加黑实例

○KuGou.exe+kugou.dll

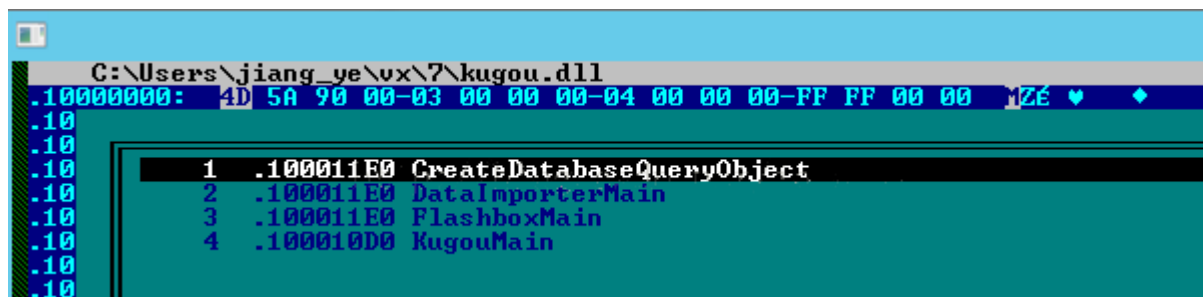
○首先用Sysinternals的sigcheck检查一下KuGou.exe签名

```
Verified: Signed
Signing date: 6:04 AM 9/12/2016
Publisher: GuangZhou KuGou Computer Technology Co.
Description: KuGou
Product: KuGou
Prod version: 8.1.00.19303
File version: 8.1.00.19303
MachineType: 32-bit
Binary Version: 8.1.0.19303
Original Name: KuGou.exe
Internal Name: KuGou
Copyright: Copyright 2016 KuGou-Inc.All Rights Reserved
Comments: n/a
Entropy: 6.206
```

○检查一下kugou.dll签名：

○分析一下导出函数

```
Verified: Unsigned
Link date: 8:52 AM 2/2/2017
Publisher: n/a
Description: n/a
Product: n/a
Prod version: n/a
File version: n/a
```

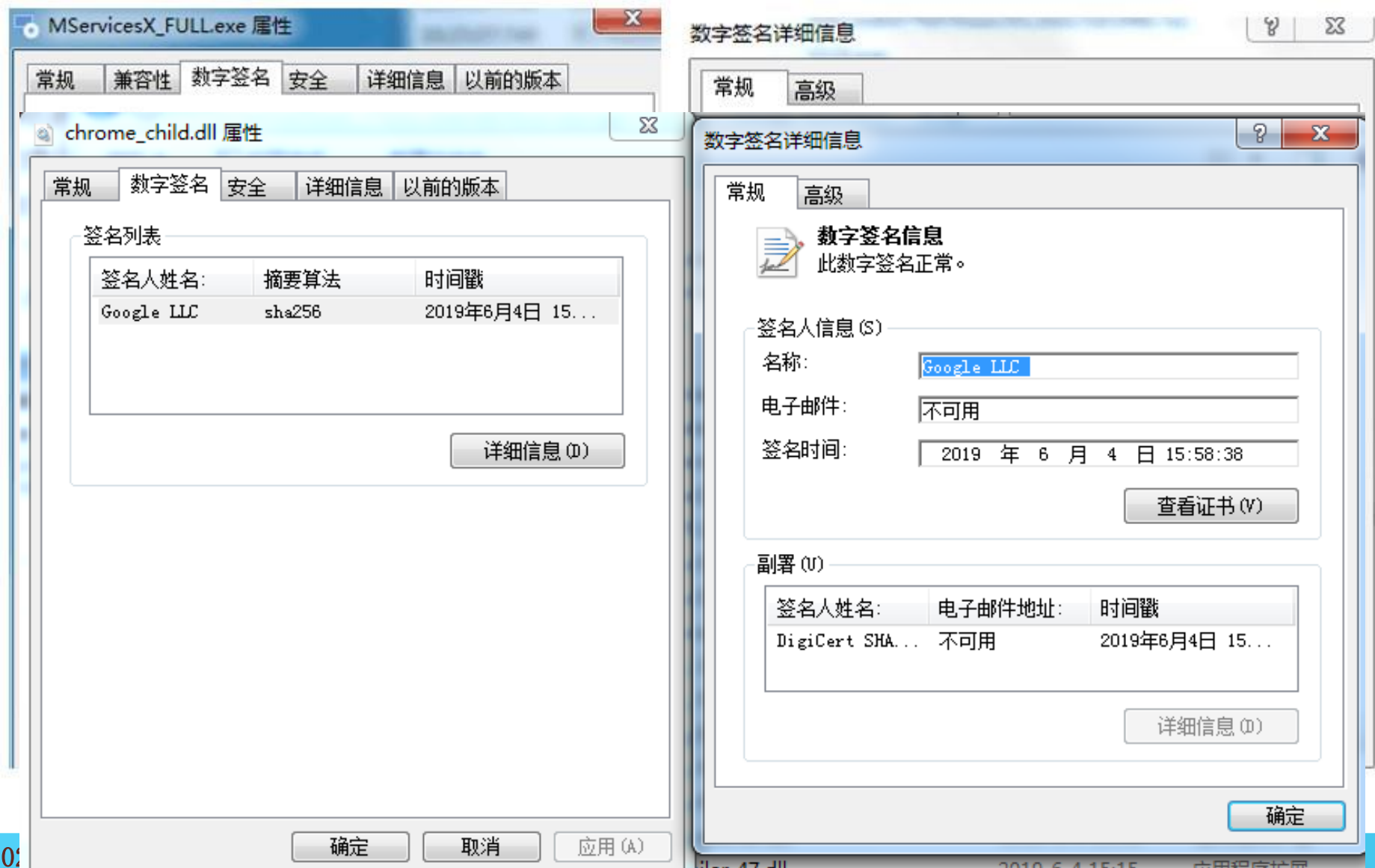


```
C:\Users\jiang_ye\vx\7\kugou.dll
.10000000: 4D 5A 90 00-03 00 00 00-04 00 00 00-FF FF 00 00 12E ♥ ♦
.10
.10
.10
.10 1 .100011E0 CreateDatabaseQueryObject
.10 2 .100011E0 DataImporterMain
.10 3 .100011E0 FlashboxMain
.10 4 .100010D0 KugouMain
.10
.10
```

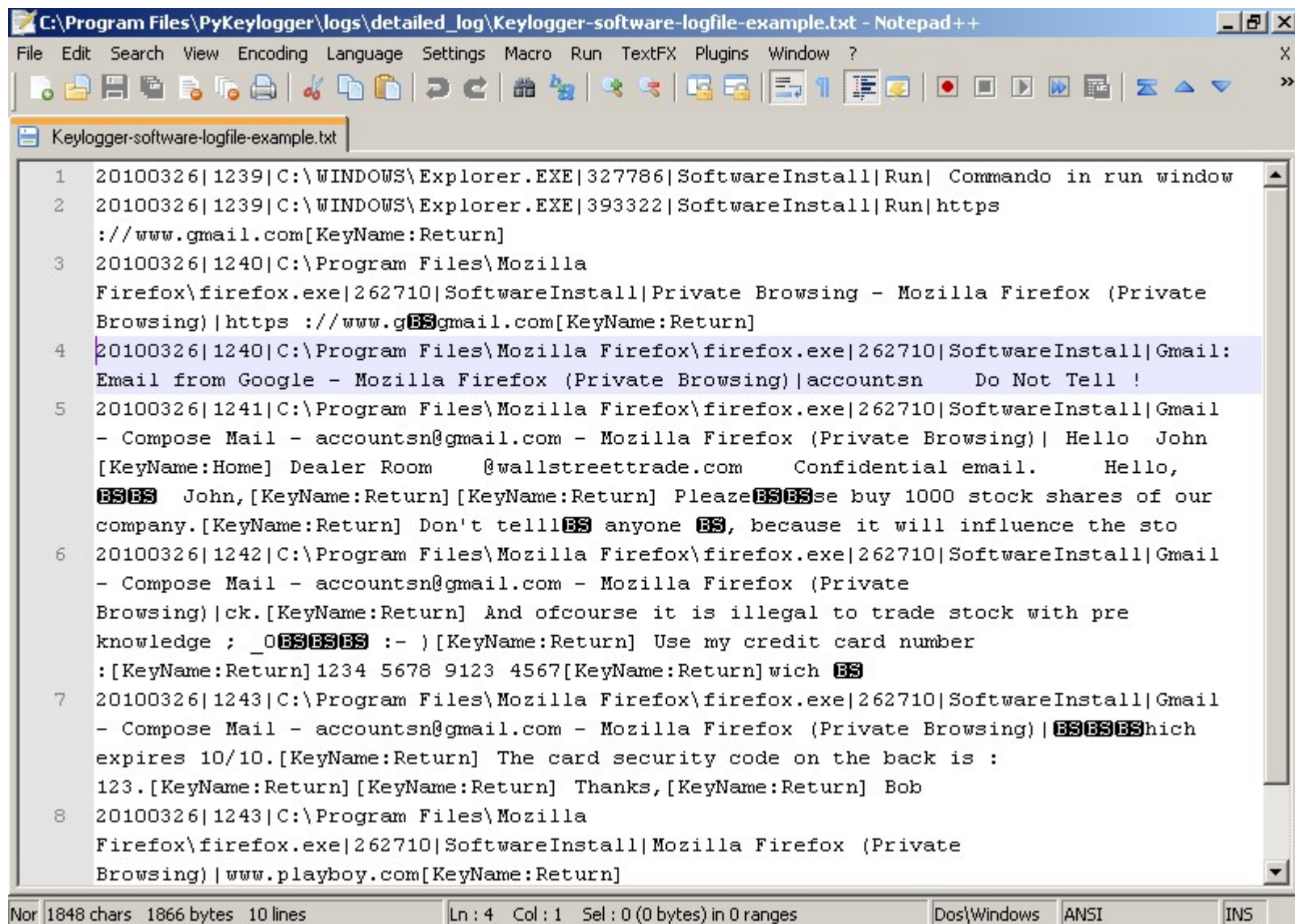
○结论：仅用LoadLibrary()函数+GetProcAddress()函数是不安全的

白加黑实例

以后只看应用程序的签名也是不够的



Keylogger



```
C:\Program Files\PyKeylogger\logs\detailed_log\Keylogger-software-logfile-example.txt - Notepad++
File Edit Search View Encoding Language Settings Macro Run TextFX Plugins Window ?
Keylogger-software-logfile-example.txt
1 20100326|1239|C:\WINDOWS\Explorer.EXE|327786|SoftwareInstall|Run| Commando in run window
2 20100326|1239|C:\WINDOWS\Explorer.EXE|393322|SoftwareInstall|Run|https
  ://www.gmail.com[KeyName:Return]
3 20100326|1240|C:\Program Files\Mozilla
  Firefox\firefox.exe|262710|SoftwareInstall|Private Browsing - Mozilla Firefox (Private
  Browsing)|https ://www.gBSgmail.com[KeyName:Return]
4 20100326|1240|C:\Program Files\Mozilla Firefox\firefox.exe|262710|SoftwareInstall|Gmail:
  Email from Google - Mozilla Firefox (Private Browsing)|accounts Do Not Tell !
5 20100326|1241|C:\Program Files\Mozilla Firefox\firefox.exe|262710|SoftwareInstall|Gmail
  - Compose Mail - accounts@gmail.com - Mozilla Firefox (Private Browsing)| Hello John
  [KeyName:Home] Dealer Room @wallstreettrade.com Confidential email. Hello,
  BSBS John,[KeyName:Return][KeyName:Return] PleaseBSBSse buy 1000 stock shares of our
  company.[KeyName:Return] Don't telllBS anyone BS, because it will influence the sto
6 20100326|1242|C:\Program Files\Mozilla Firefox\firefox.exe|262710|SoftwareInstall|Gmail
  - Compose Mail - accounts@gmail.com - Mozilla Firefox (Private
  Browsing)|ck.[KeyName:Return] And ofcourse it is illegal to trade stock with pre
  knowledge ; _0BSBSBS :- )[KeyName:Return] Use my credit card number
  :[KeyName:Return] 1234 5678 9123 4567[KeyName:Return] wich BS
7 20100326|1243|C:\Program Files\Mozilla Firefox\firefox.exe|262710|SoftwareInstall|Gmail
  - Compose Mail - accounts@gmail.com - Mozilla Firefox (Private Browsing)| BSBSBSwhich
  expires 10/10.[KeyName:Return] The card security code on the back is :
  123.[KeyName:Return][KeyName:Return] Thanks,[KeyName:Return] Bob
8 20100326|1243|C:\Program Files\Mozilla
  Firefox\firefox.exe|262710|SoftwareInstall|Mozilla Firefox (Private
  Browsing)| www.playboy.com[KeyName:Return]
```

Nor 1848 chars 1866 bytes 10 lines Ln: 4 Col: 1 Sel: 0 (0 bytes) in 0 ranges Dos\Windows ANSI INS

- social engineering
- 社交 工程
 - 社交的目的：获取信息、信用、熟悉度等
 - 工程的目的：不断的、可重复的进行
- 常见形式：
 - 钓鱼、假托、下饵、等价交换等等
- 以下不是社工的例子是：
 - 电子发票摇中奖品，请填写姓名、地址、电话
 - 某男子当街推销《如来神掌》、《易筋经》等，并请你安装“武功秘籍APP”学习更多NB武功
 - 1、男孩大献殷勤，确定男女关系→2、男孩告诉女孩现在两个人收入太少了，钱不够将来结婚用→3、诱导女孩去做沐足小姐；女孩想，沐足比较正规同意→4、男孩抱怨钱来得太慢，建议女孩做桑拿小姐→5、女孩成了桑拿小姐，把钱交给男孩保管→6、男孩甩掉该女孩，再去找下一个
 - 小明去找单位网管申请一个新邮箱，突然来了一批新服务器需要网管去验收。网管让小明在自己的机器上继续填信息，小明填完以后发现桌面上有一个pwd.xls文件，打开一看是全单位里各个重要系统的登录口令

- 后门：一种绕过产品，计算机系统，密码系统或算法等中的正常身份验证的方法，通常是秘密的
- 与前门相对，通常是一些隐蔽的、少数人知道的
- 与漏洞不一样，后门可以确定是故意留下的
 - 汉化版puTTY、WinSCP、SSH Secure等工具中发现后门，可以获取用户名、密码、地址，发送到指定网站
 - JavaScript公共库event-stream被发现植入恶意的后门代码

```
(node:27294) [DEP0106] DeprecationWarning: crypto.createDecipher is deprecated.  
  at [redacted]/node_modules/flatmap-stream/index.min.js:1:1264  
  at Object.<anonymous> ([redacted]/node_modules/flatmap-stream/index.min.js:1:1423)  
  at Module._compile (internal/modules/cjs/loader.js:707:30)  
  at Object.Module._extensions..js (internal/modules/cjs/loader.js:718:10)  
  at Module.load (internal/modules/cjs/loader.js:605:32)  
  at tryModuleLoad (internal/modules/cjs/loader.js:544:12)  
  at Function.Module._load (internal/modules/cjs/loader.js:536:3)  
  at Module.require (internal/modules/cjs/loader.js:643:17)  
  at require (internal/modules/cjs/helpers.js:22:18)  
  at Object.<anonymous> ([redacted]/node_modules/event-stream/index.js:11:15)
```


○鱼叉攻击：针对特定个人或群体的高度针对性的网络钓鱼

○最常见的是，发送包含恶意附件的邮件，并起上一个**对目标极具诱惑力**的标题，诱使受害者打开附件，



○外贸订单的邮件发给各位同学会怎么样？

○必须用社工手段获得对方的职业、爱好、联系方式等

- 鱼叉攻击：针对特定个人或群体的高度针对性的网络钓鱼
- 最常见的是，将木马程序作为电子邮件的附件，并起上一个**对目标极具诱惑力**的名称，发送给目标电脑，诱使受害者打开附件，从而感染木马。

吴槟老师，您好！

近日自然科学基金委信息中心发现有人冒用科学基金网络信息系统的名义给部分评审专家发送邮件，如下图所示。
现已确定这是一封钓鱼邮件。特此提醒各位专家：收该到邮件后，请仔细察看发件人与内容，以免受骗。

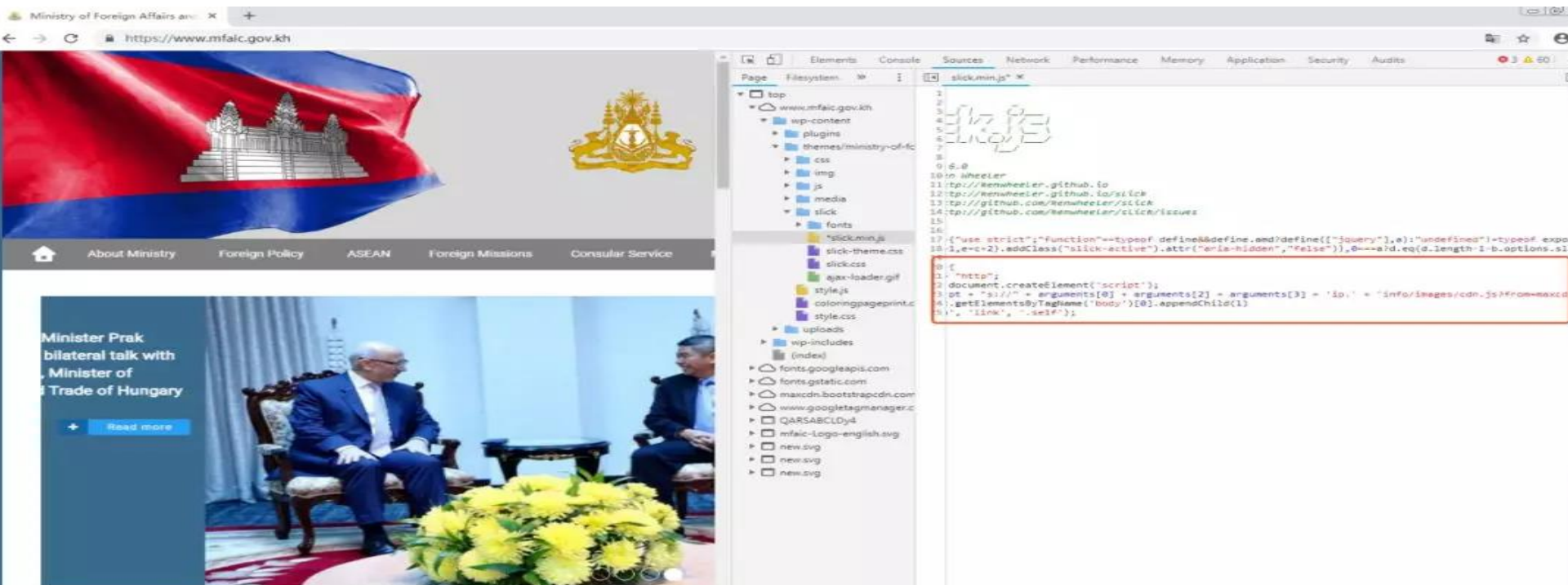
如果您已经通过这个链接提交了邮箱地址和口令，请立即更换邮箱口令。

如果您点击过仿冒邮件中的链接，请先把浏览器缓存(包括cookie)清理掉，然后关闭浏览器，使用杀毒软件在本机内进行全盘查杀。
谢谢您的配合！



水坑

- 水坑攻击：在受害者必经之路设置了一个“水坑(陷阱)”
- 最典型的做法是，黑客分析攻击目标的上网活动规律，猜测、寻找攻击目标经常访问的网站的弱点，先将此网站“攻破”并植入攻击代码，一旦攻击目标访问该网站就会“中招”
- 此种攻击借助了目标所信任的网站，攻击成功率极高



- 水坑攻击：在受害者必经之路设置了一个“水坑(陷阱)”
- 最典型的做法是，黑客分析攻击目标的上网活动规律，猜测、寻找攻击目标经常访问的网站的弱点，先将此网站“攻破”并植入攻击代码，一旦攻击目标访问该网站就会“中招”

The screenshot displays the NSFC website interface. At the top, there are logos for the NSFC and the ISIS (Internet-based Science Information System) network information system. A navigation bar includes links for 'NSFC首页', '关于ISIS', '常见问题', and '相关软件下载'. Below this, there are buttons for '单位查询', '项目公布', and '意见与建议'. The main banner features a satellite and the text '新时代科学基金资助导向' (New Era Science Fund Funding Guidance), along with the slogan '鼓励探索、突出原创；聚焦前沿、独辟蹊径；需求牵引、突破瓶颈；共性导向、交叉融通' (Encourage exploration, highlight originality; focus on the frontier, break new ground; demand-driven, break bottlenecks; commonality-oriented, cross-fertilization). On the right, a '系统登录' (System Login) form is visible, with fields for '用户名' (Username/Email), '密码' (Password), and '验证码' (Captcha), and a '登录' (Login) button. Below the login form, there are links for 'Application for Research Fund of International Young Scientists', '咨询方式' (Consultation Methods), and '友情链接' (Friendly Links). The left sidebar contains a '重要提示' (Important Notice) section with links to '优秀青年科学基金项目(海外)依托单位系统', '关于填报《国家自然科学基金资助项目结题报告/成果报告》的说明', 'ISIS系统添加申请人操作手册', '申请功能培训: 申请培训(申请人) 申请培训(依托单位)', '项目预算表编制说明(2020年8月)', '项目决算表编制说明(2020年8月)', '重点国际(地区)合作研究项目英文申请书', and '管理工作报告填报说明'.

国家自然科学基金委员会
National Natural Science Foundation of China

ISIS 科学基金网络信息系统
Internet-based Science Information System

NSFC首页 | 关于ISIS | 常见问题 | 相关软件下载

单位查询 | 项目公布 | 意见与建议

系统登录

用户名:

密码:

验证码: fgg?

登录 找回用户名/密码?

Application for Research Fund of International Young Scientists

咨询方式 (支持邮箱: support@nsfc.gov.cn)

常见问题 | 帮助中心 | 培训系统

友情链接

重要提示

- 优秀青年科学基金项目(海外)依托单位系统
- 关于填报《国家自然科学基金资助项目结题报告/成果报告》的说明 操作说明
- ISIS系统添加申请人操作手册
- 申请功能培训: 申请培训(申请人) 申请培训(依托单位)
- 项目预算表编制说明(2020年8月) 项目决算表编制说明(2020年8月)
- 重点国际(地区)合作研究项目英文申请书
- 管理工作报告填报说明

- 依然在广泛使用的简单有效的破解方式
- 勒索软件、挖矿软件寻找SSH弱口令

```
nmap -p 22 --script=ssh-brute --script-args userdb=2.txt,passdb=1.txt 192.168.229.129
```

- 此种攻击利用了疏于防范的心理，成功率非常高

| 登录查询 | 发信查询 | 收信查询 | 删信查询 | 中转站下载查询 | | |
|------------------|------|------|-----------------|---------|------|------------------------------------|
| 2021-05-13 09:30 | | | 183.142.99.108 | | SMTP | 登录失败 (密码错误) 0 次, 系统已为您拦截密码攻击 4 次 |
| 2021-05-13 09:33 | | | 115.208.123.39 | | SMTP | 登录失败 (密码错误了 13 次, 系统已为您拦截密码攻击 9 次) |
| 2021-05-13 09:13 | | | 60.167.20.233 | | SMTP | 登录失败 (密码错误了 8 次, 系统已为您拦截密码攻击 4 次) |
| 2021-05-13 06:30 | | | 180.110.151.240 | | SMTP | 登录失败 (密码错误了 5 次, 系统已为您拦截密码攻击 1 次) |
| 2021-05-13 05:29 | | | 222.93.180.176 | | SMTP | 登录失败 (密码错误了 2 次) |
| 2021-05-13 05:23 | | | 121.227.24.21 | | SMTP | 登录失败 |
| 2021-05-13 05:22 | | | 121.238.231.69 | | SMTP | 登录失败 (密码错误了 2 次) |
| 2021-05-13 05:20 | | | 121.239.51.36 | | SMTP | 登录失败 (密码错误了 2 次) |
| 2021-05-13 05:18 | | | 180.103.175.164 | | SMTP | 登录失败 (密码错误了 2 次) |
| 2021-05-13 05:17 | | | 117.83.16.137 | | SMTP | 登录失败 (密码错误了 3 次) |
| 2021-05-13 05:15 | | | 117.81.39.82 | | SMTP | 登录失败 (密码错误了 3 次) |
| 2021-05-13 05:12 | | | 117.80.57.249 | | SMTP | 登录失败 (密码错误了 7 次, 系统已为您拦截密码攻击 3 次) |
| 2021-05-13 05:11 | | | 117.80.59.68 | | SMTP | 登录失败 (密码错误了 5 次, 系统已为您拦截密码攻击 1 次) |
| 2021-05-13 05:10 | | | 117.80.57.105 | | SMTP | 登录失败 (密码错误了 3 次) |
| 2021-05-13 05:08 | | | 49.72.56.114 | | SMTP | 登录失败 (密码错误了 5 次, 系统已为您拦截密码攻击 1 次) |
| 2021-05-13 05:07 | | | 121.227.203.201 | | SMTP | 登录失败 (密码错误了 2 次) |

邮箱的真实查询记录