# 软件安全—恶意代码机理与防护

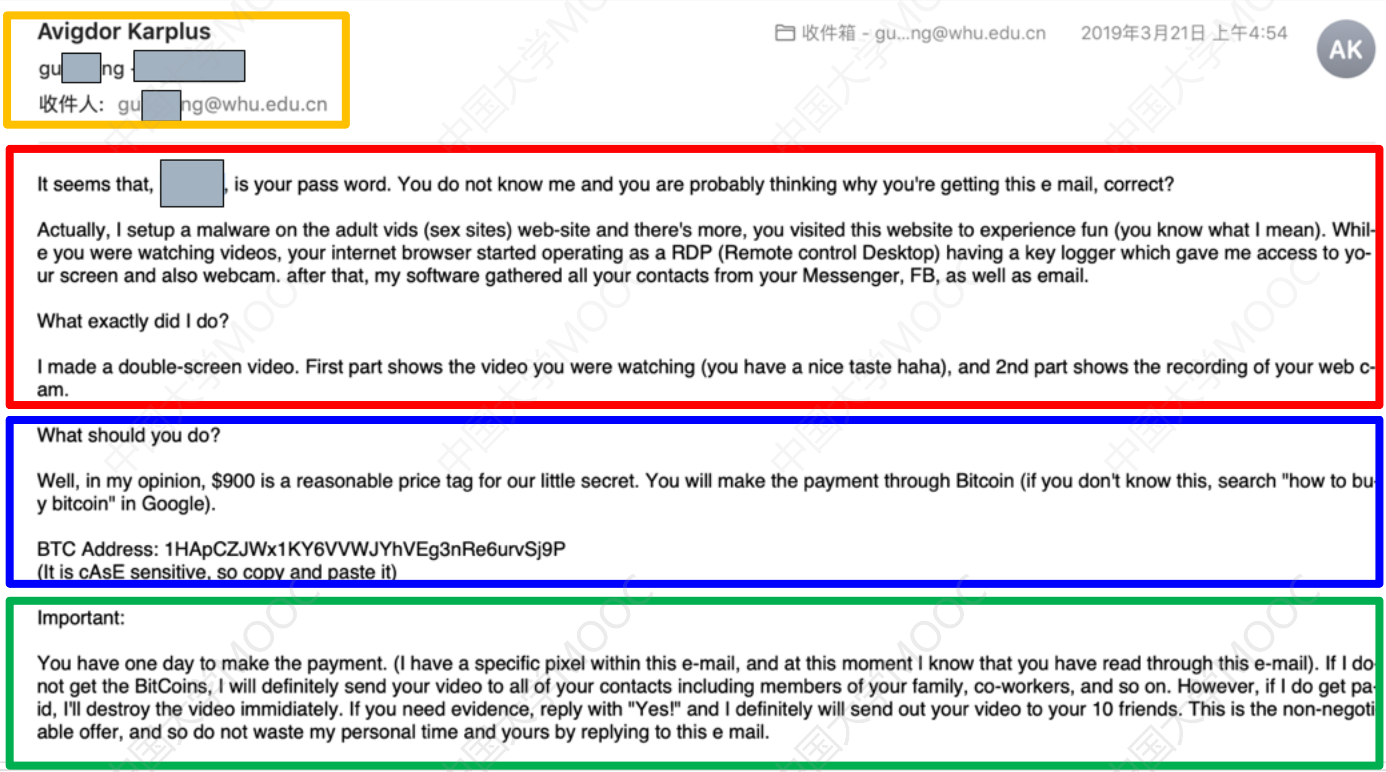
## 课程介绍

彭国军

武汉大学国家网络安全学院

guojpeng@whu.edu.cn

# 一封勒索邮件



Avigdor Karplus

gu[redacted]ng [redacted]

收件人：gu[redacted]ng@whu.edu.cn

收件箱 - gu...ng@whu.edu.cn 2019年3月21日 上午4:54

AK

It seems that, [redacted], is your pass word. You do not know me and you are probably thinking why you're getting this e mail, correct?

Actually, I setup a malware on the adult vids (sex sites) web-site and there's more, you visited this website to experience fun (you know what I mean). While you were watching videos, your internet browser started operating as a RDP (Remote control Desktop) having a key logger which gave me access to your screen and also webcam. after that, my software gathered all your contacts from your Messenger, FB, as well as email.

What exactly did I do?

I made a double-screen video. First part shows the video you were watching (you have a nice taste haha), and 2nd part shows the recording of your web cam.

What should you do?

Well, in my opinion, $900 is a reasonable price tag for our little secret. You will make the payment through Bitcoin (if you don't know this, search "how to buy bitcoin" in Google).

BTC Address: 1HApCZJWx1KY6VVWJYhVEg3nRe6urvSj9P
(It is cAsE sensitive, so copy and paste it)

Important:

You have one day to make the payment. (I have a specific pixel within this e-mail, and at this moment I know that you have read through this e-mail). If I do not get the BitCoins, I will definitely send your video to all of your contacts including members of your family, co-workers, and so on. However, if I do get paid, I'll destroy the video immidiately. If you need evidence, reply with "Yes!" and I definitely will send out your video to your 10 friends. This is the non-negotiable offer, and so do not waste my personal time and yours by replying to this e mail.

←用户名
+口令

←解释
攻击原理

←敲诈

←恐吓

# 邮件解读！

告知口令，引起恐慌！
解读原理，消除疑虑！

**邮件标题：guXXXng-xxxxxxxxx**

←用户名
+口令

邮件正文：

- □ It seems that, xxxxxxxxx, is your password.
- □ You do not know me and you are probably thinking why you‘re getting this email, correct?
  - ■ Actually, I setup a malware on the adult vids (sex sites) website and there's more, you visited this website to experience fun (you know what I mean).
  - ■ While you were watching videos, your internet browser started operating as a RDP (Remote control Desktop) having a **key logger** which gave me access to your screen and also webcam. after that, my software gathered all your contacts from your Messenger, FB, as well as email.

←解释
攻击原理

# What exactly did I do?

←告知
攻击结果

- □ I made a double-screen video.
  - First part shows the video you were watching (you have a nice taste haha),
  - and 2nd part shows the recording of your web cam.

屏幕录像+摄像头录像

# What should you do?

←敲诈

- □ Well, in my opinion, $900 is a reasonable price tag for our little secret.

- □ You will make the payment through Bitcoin (if you don't know this, **search "how to buy bitcoin" in Google**).

  **BTC Address:** 1HApCZJWx1KY6VVWJYhVEg3nRe6urvSj9P
  (It is cAsE sensitive, so copy and paste it)

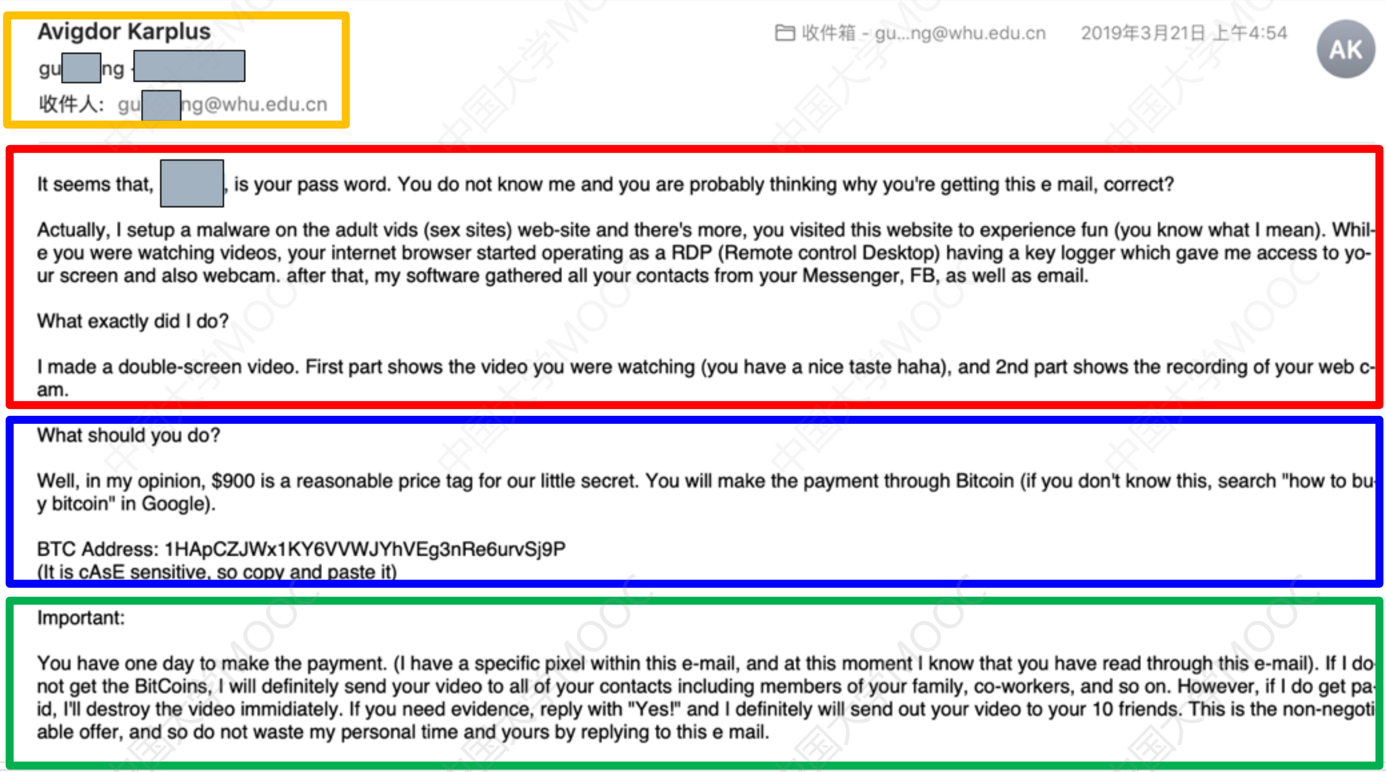
900美金，通过比特币支付！
不知道如何支付？请自行Google！

# Important: ←恐吓

- □ You have one day to make the payment. (I have a specific pixel within this e-mail, and at this moment I know that you have read through this e-mail).
- □ If I do not get the BitCoins, I will definitely send your video to all of your contacts including members of your family, co-workers, and so on.
- □ However, if I do get paid, I'll destroy the video immidiately. If you need evidence, reply with "Yes!" and I definitely will send out your video to your 10 friends. This is the non-negotiable offer, and so do not waste my personal time and yours by replying to this email.

24小时，不要挣扎，不要反抗！

# 一封勒索邮件



**Avigdor Karplus**

gu[redacted]ng [redacted]

收件人: gu[redacted]ng@whu.edu.cn

收件箱 - gu...ng@whu.edu.cn 2019年3月21日 上午4:54

←用户名
+口令

It seems that, [redacted], is your pass word. You do not know me and you are probably thinking why you're getting this e mail, correct?

Actually, I setup a malware on the adult vids (sex sites) web-site and there's more, you visited this website to experience fun (you know what I mean). While you were watching videos, your internet browser started operating as a RDP (Remote control Desktop) having a key logger which gave me access to your screen and also webcam. after that, my software gathered all your contacts from your Messenger, FB, as well as email.

What exactly did I do?

I made a double-screen video. First part shows the video you were watching (you have a nice taste haha), and 2nd part shows the recording of your web cam.

←解释
攻击原理

What should you do?

Well, in my opinion, $900 is a reasonable price tag for our little secret. You will make the payment through Bitcoin (if you don't know this, search "how to buy bitcoin" in Google).

BTC Address: 1HApCZJWx1KY6VVWJYhVEg3nRe6urvSj9P
(It is cAsE sensitive, so copy and paste it)

←敲诈

Important:

You have one day to make the payment. (I have a specific pixel within this e-mail, and at this moment I know that you have read through this e-mail). If I do not get the BitCoins, I will definitely send your video to all of your contacts including members of your family, co-workers, and so on. However, if I do get paid, I'll destroy the video immidiately. If you need evidence, reply with "Yes!" and I definitely will send out your video to your 10 friends. This is the non-negotiable offer, and so do not waste my personal time and yours by replying to this e mail.

←恐吓

# 技术分析

- 对方已获得和声称已获得的信息
  - **对方已获得的：**收件人的用户名和口令【事实】
  - **对方声称已获得的：**
    - 浏览网站视频的屏幕录像
    - 网络摄像头的录像
    - 收件人的联系人列表（Messenger、FB、email等）
  - 知道你已经阅读了该邮件

- 获取以上信息在技术上是否可行?
  - 攻击者如何进入电脑？攻击者又如何获取隐私信息?
    - 软件漏洞（非授权获得设备的控制权）
    - 恶意软件（Malware：Virus、RCS、Keylogger等）

“恶意代码”和“软件漏洞”正是软件安全课程的学习内容：机理分析

# 如何决断？

- 攻击者是否真正拥有所声称的信息？
  - **用户名+口令：**如何拿到的？什么时间的口令？在哪里用过？
    - 是自己的系统还是第三方服务器？）
      - 自己的系统是否存在漏洞？
    - 另外一种勒索邮件：发件地址是自己邮箱
  - **两部分录像（屏幕+摄像头）**
    - 是否存在？
  - **好友、联系人？**
    - Messenger、FB、Email等

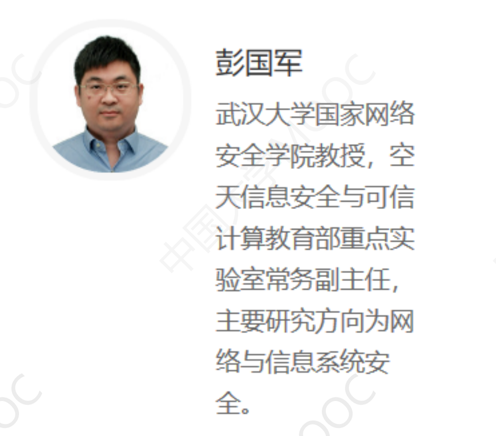
**←电脑中是否存在恶意软件？**

如何及时发现和阻止攻击？

软件安全课程的另外一个重要内容：分析、检测与防护

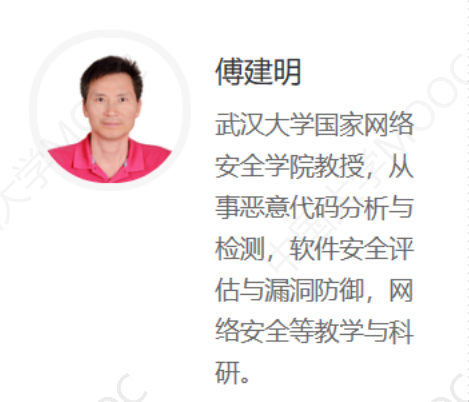
# 课程团队及教学安排

- □ 武汉大学国家网络安全学院3位老师共同主讲，3位研究生担任助教。



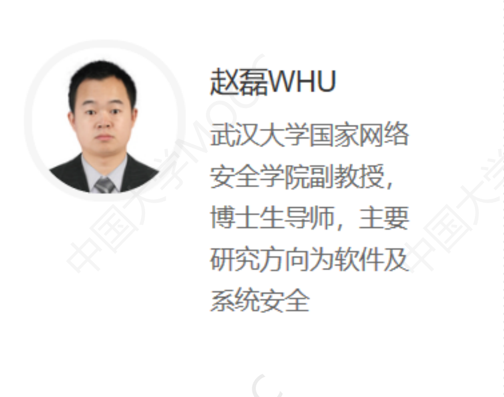
彭国军

武汉大学国家网络安全学院教授，空天信息安全与可信计算教育部重点实验室常务副主任，主要研究方向为网络与信息系统安全。



傅建明

武汉大学国家网络安全学院教授，从事恶意代码分析与检测，软件安全评估与漏洞防御，网络安全等教学与科研。



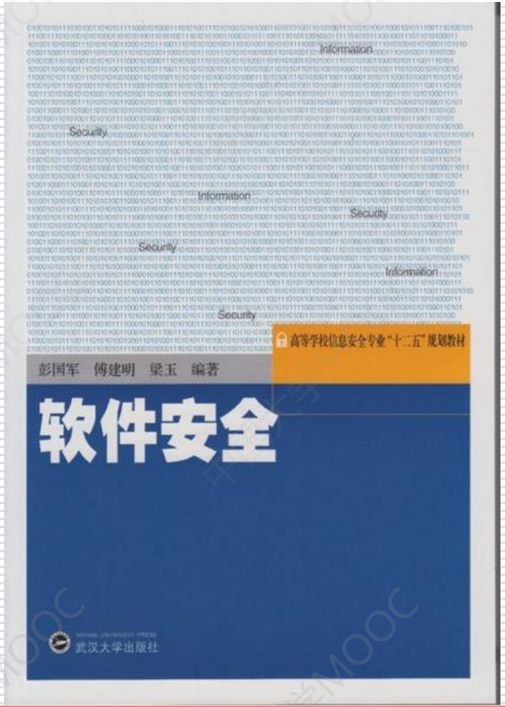
赵磊WHU

武汉大学国家网络安全学院副教授，博士生导师，主要研究方向为软件及系统安全

拟邀请讲师：“安天实验室”相关技术专家

# 教材

1. 彭国军、傅建明、梁玉，《软件安全》，武汉大学出版社，2015年9月。



# 课程内容安排

## 第1周 软件安全概述

1.1 信息与信息安全

1.2 软件安全威胁及其来源

1.3 典型的软件安全防护手段

## 第2周 计算机引导与磁盘管理

2.1 系统引导与控制权

2.2 80X86处理器的工作模式

2.3 Windows内存结构与管理

2.4 磁盘的物理与逻辑结构

2.5 FAT32文件系统及数据恢复

2.6 NTFS文件系统

# 课程内容安排

**第3周 PE文件格式**

3.1 PE文件及其表现形式

3.2 PE文件格式与Win32病毒的关系

3.3 PE文件格式总体结构概述

3.4 节与节表解析

3.5 引入函数节：PE文件的引入函数机制

3.6 引出函数节：PE文件函数引出机制

3.7 资源节：文件资源索引、定位与修改

3.8 重定位节：镜像地址改变后的地址自动修正

3.9 PE文件的数字签名与验证机制

**第4周 PE文件格式实践**

4.1手工构建引入函数表

4.2手工替换程序的已有图标

4.3手工提取程序图标资源

4.4手工为程序新增图标

4.5手工汉化

4.6挑战自己：手工打造最小PE文件

4.7CVE-2020-0601文件签名漏洞重现

# 课程内容安排

**第5周 恶意代码及其分类**

5.1 恶意代码定义

5.2 恶意代码的发展

5.3 恶意代码分类

5.4 恶意代码与网络犯罪

**第6周 Windows PE病毒**

6.1 PE病毒的基本概念

6.2 PE病毒的分类

6.3 传统文件寄生感染方式

6.4 捆绑释放型

6.5 系统感染型

6.6 典型案例

# 课程内容安排

## 第7周 脚本病毒与宏病毒

7.1 宏的基本概念与使用

7.2 宏病毒的传播方法

7.3 宏病毒的自我保护与对抗措施

7.4 VBS脚本的概念及使用

7.5 VBS脚本病毒的感染技术

7.6 VBS脚本病毒的变形技术

7.7 Powershell与无文件型恶意代码

## 第8周 网络蠕虫

8.1 网络蠕虫的定义

8.2 计算机病毒与蠕虫的异同

8.3 网络蠕虫的结构

8.4 网络蠕虫攻击的关键技术

8.5 网络蠕虫的检测与防治

8.6 经典蠕虫案例技术分析（Slammer与wannacry）

# 课程内容安排

**第9周 网络木马**

9.1木马的基本概念

9.2 木马的分类

9.3 木马的植入方式

9.4 远程控制型木马的通信方式

9.5 远程控制型木马的典型功能及意图

9.6 远程控制型木马的典型功能实现机理

9.7 APT攻击与远控木马[安天李柏松主讲]

9.8 木马检测思路探讨

**第10周 恶意代码检测与溯源**

10.1 特征值检测技术

10.2 校验和检测技术

10.3 虚拟机检测技术

10.4 启发式扫描技术

10.5 主动防御技术

10.6 云查杀技术

10.7 机器学习与恶意代码检测

10.8 安全软件测评方法与机构

10.9 APT攻击与恶意代码溯源

# 课程内容安排

**第11周 恶意软件样本捕获与分析【梁玉博士主讲】**

11.1 恶意软件样本捕获方法

11.2 恶意软件载体

11.3 恶意软件样本分析方法

11.4 典型恶意软件样本分析工具

11.5 恶意软件样本分析实例

11.6 恶意软件之威胁情报

11.7 恶意软件分析课后实战

# 课程内容安排

## 第12周  恶意代码与APT网络军火库

【特邀：安天首席技术架构师肖新光老师主讲】

12.1从恶意代码的发展看APT攻击

12.2 高级恶意代码工程体系--A2PT的攻击武器

12.3高级APT组织的自研恶意代码

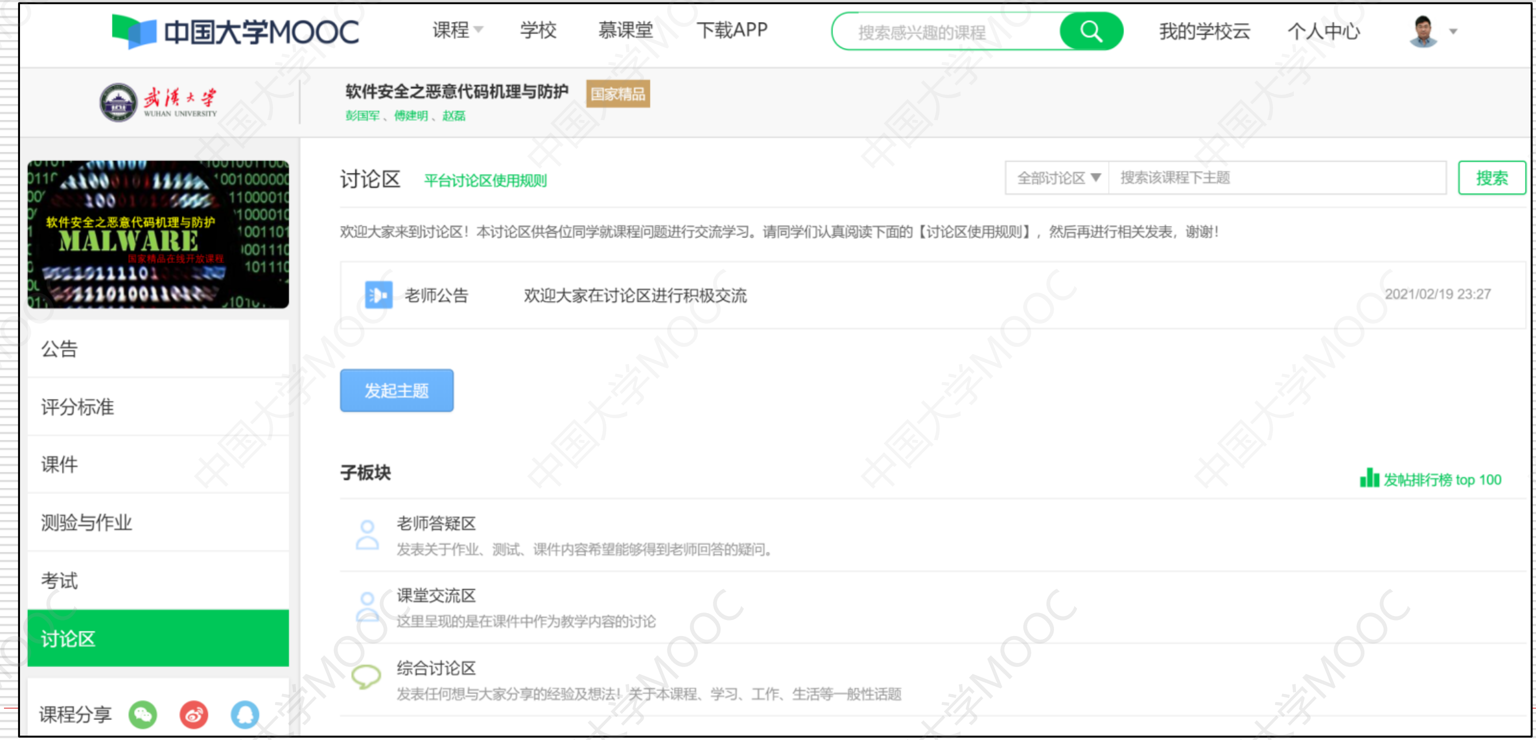
12.4商用恶意代码

12.5无恶意代码作业、开源和免费工具

12.6总结与思考

（以上为拟定教学计划，在课程录制过程中可能根据需要进行调整）

# 课程讨论区



软件安全之恶意代码机理与防护 国家精品

彭国军、傅建明、赵磊

讨论区 平台讨论区使用规则

欢迎大家来到讨论区！本讨论区供各位同学就课程问题进行交流学习。请同学们认真阅读下面的【讨论区使用规则】，然后再进行相关发表，谢谢！

老师公告 欢迎大家在讨论区进行积极交流 2021/02/19 23:27

子板块

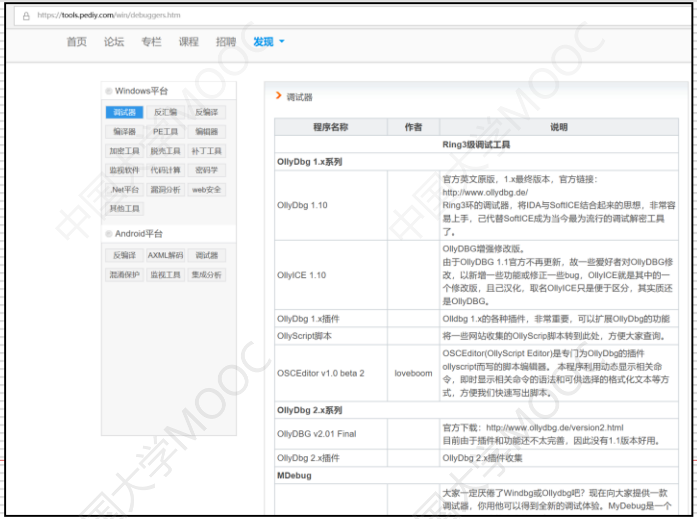
老师答疑区
发表关于作业、测试、课件内容希望能够得到老师回答的疑问。

课堂交流区
这里呈现的是在课件中作为教学内容的讨论

综合讨论区
发表任何想与大家分享的经验及想法！关于本课程、学习、工作、生活等一般性话题

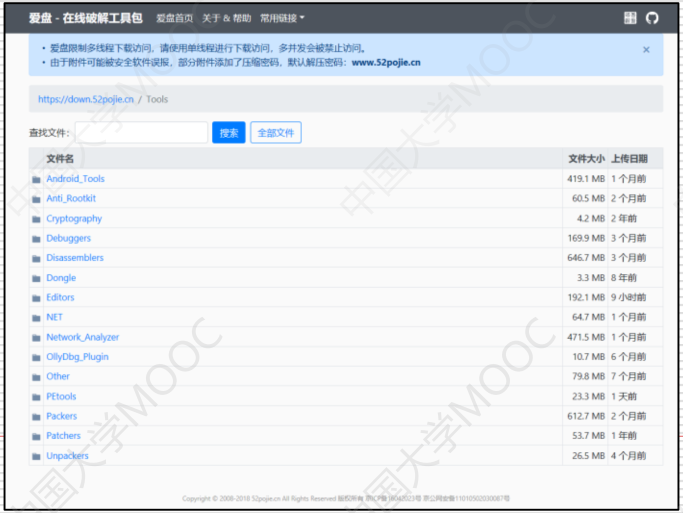
# 工具下载

- □ 看雪论坛：https://tools.pediy.com/
- □ 吾爱破解：https://down.52pojie.cn/Tools/



调试器

| 程序名称 | 作者 | 说明 |
|---|---|---|
| | | Ring3级调试工具 |
| OllyDbg 1.x系列 | | |
| OllyDbg 1.10 | | 官方英文原版，1.x最终版本，官方链接：<br>http://www.ollydbg.de/<br>Ring3环的调试器，将IDA与SoftICE结合起来的思想，非常容易上手，己代替SoftICE成为当今最为流行的调试解密工具了。 |
| OllyICE 1.10 | | OllyDBG增强修改版。<br>由于OllyDBG 1.1官方不再更新，故一些爱好者对OllyDBG修改，以新增一些功能或修正一些bug，OllyICE就是其中的一个修改版，且己汉化，取名OllyICE只是便于区分，其实质还是OllyDBG。 |
| OllyDbg 1.x插件 | | Olldbg 1.x的各种插件，非常重要，可以扩展OllyDbg的功能 |
| OllyScript脚本 | | 将一些网站收集的OllyScrip脚本转到此处，方便大家查询。 |
| OSCEditor v1.0 beta 2 | loveboom | OSCEditor(OllyScript Editor)是专门为OllyDbg的插件ollyscript而写的脚本编辑器。 本程序利用动态显示相关命令，即时显示相关命令的语法和可供选择的格式化文本等方式，方便我们快速写出脚本。 |
| OllyDbg 2.x系列 | | |
| OllyDBG v2.01 Final | | 官方下载：http://www.ollydbg.de/version2.html<br>目前由于插件和功能还不太完善，因此没有1.1版本好用。 |
| OllyDbg 2.x插件 | | OllyDbg 2.x插件收集 |
| MDebug | | |
| | | 大家一定厌倦了Windbg或Ollydbg吧？现在向大家提供一款调试器，你用他可以得到全新的调试体验。MyDebug是一个 |



- 爱盘限制多线程下载访问，请使用单线程进行下载访问，多并发会被禁止访问。
- 由于附件可能被安全软件误报，部分附件添加了压缩密码，默认解压密码：**www.52pojie.cn**

https://down.52pojie.cn / Tools

| 文件名 | 文件大小 | 上传日期 |
|---|---|---|
| Android_Tools | 419.1 MB | 1 个月前 |
| Anti_Rootkit | 60.5 MB | 2 个月前 |
| Cryptography | 4.2 MB | 2 年前 |
| Debuggers | 169.9 MB | 3 个月前 |
| Disassemblers | 646.7 MB | 3 个月前 |
| Dongle | 3.3 MB | 8 年前 |
| Editors | 192.1 MB | 9 小时前 |
| NET | 64.7 MB | 1 个月前 |
| Network_Analyzer | 471.5 MB | 1 个月前 |
| OllyDbg_Plugin | 10.7 MB | 6 个月前 |
| Other | 79.8 MB | 7 个月前 |
| PEtools | 23.3 MB | 1 天前 |
| Packers | 612.7 MB | 2 个月前 |
| Patchers | 53.7 MB | 1 年前 |
| Unpackers | 26.5 MB | 4 个月前 |