360 漏洞响应平台

渔夫与鱼儿

红队下的钓鱼行动

演讲人：李木

演讲时间：2021年5月xx日

目录
CONTENT

360 漏洞响应平台

CONTENTS

01 添加标题

02 添加标题

03 添加标题

04 添加标题

星火计划
360白帽校园行

前言

什么是红队？

红队泛指在网络安全攻防演练中的攻击方

有些公司也称为蓝军，例如腾讯蓝军等等

是进攻性安全的主要推手！

什么是网络攻防演练？

国内的网络安全演练俗称为HW(护网)

国家级目前是每年一次，省级的为每年一次以上。

由公安部门或网信部门举办，目的是在类似真实网络、

中黑客攻击的演练中发现漏洞加强防御等等

什么是网络攻防演练？

按照攻击规则：红队可以进行WEB攻击，鱼叉攻击，近源攻击，内网横向移动等等攻击方法。

HW中的攻击链

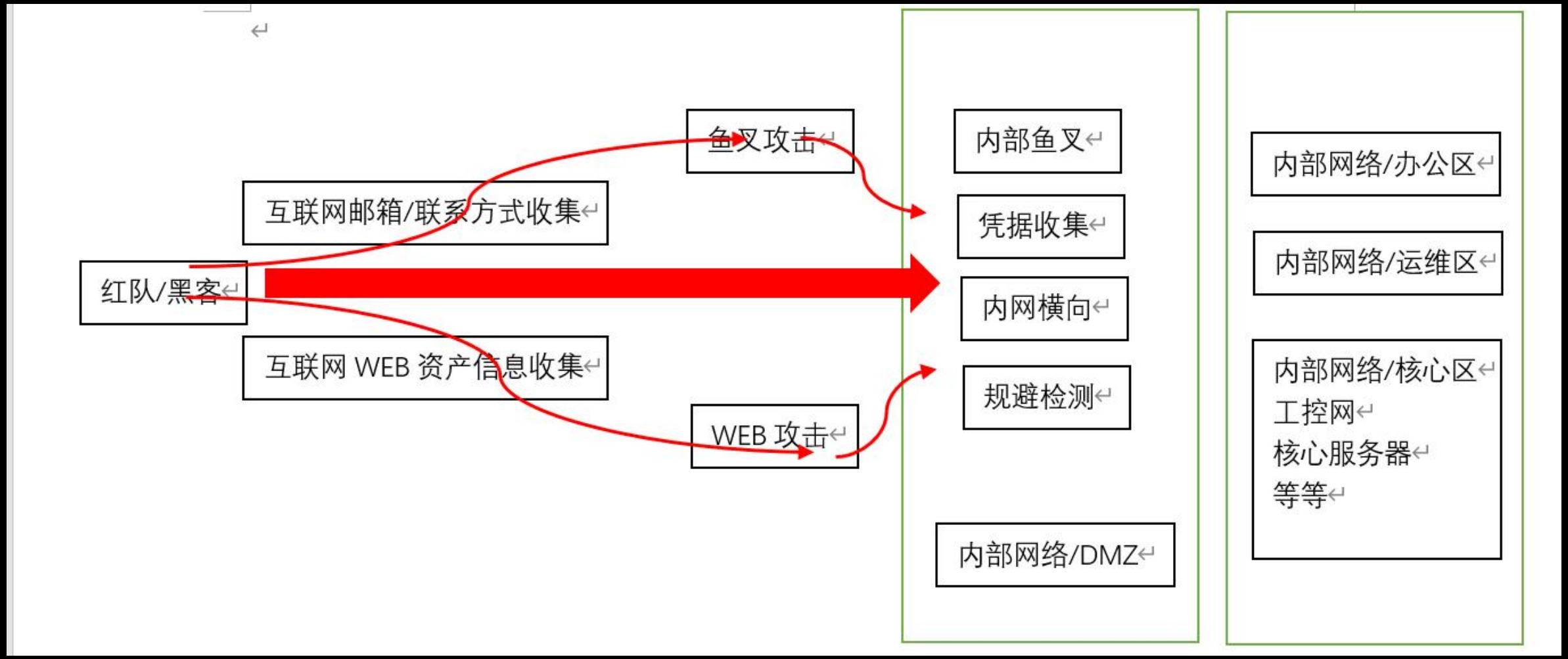
360 漏洞响应平台

HW中的攻击链

WEB打点/钓鱼/近源 》》边界突破 》内网横向

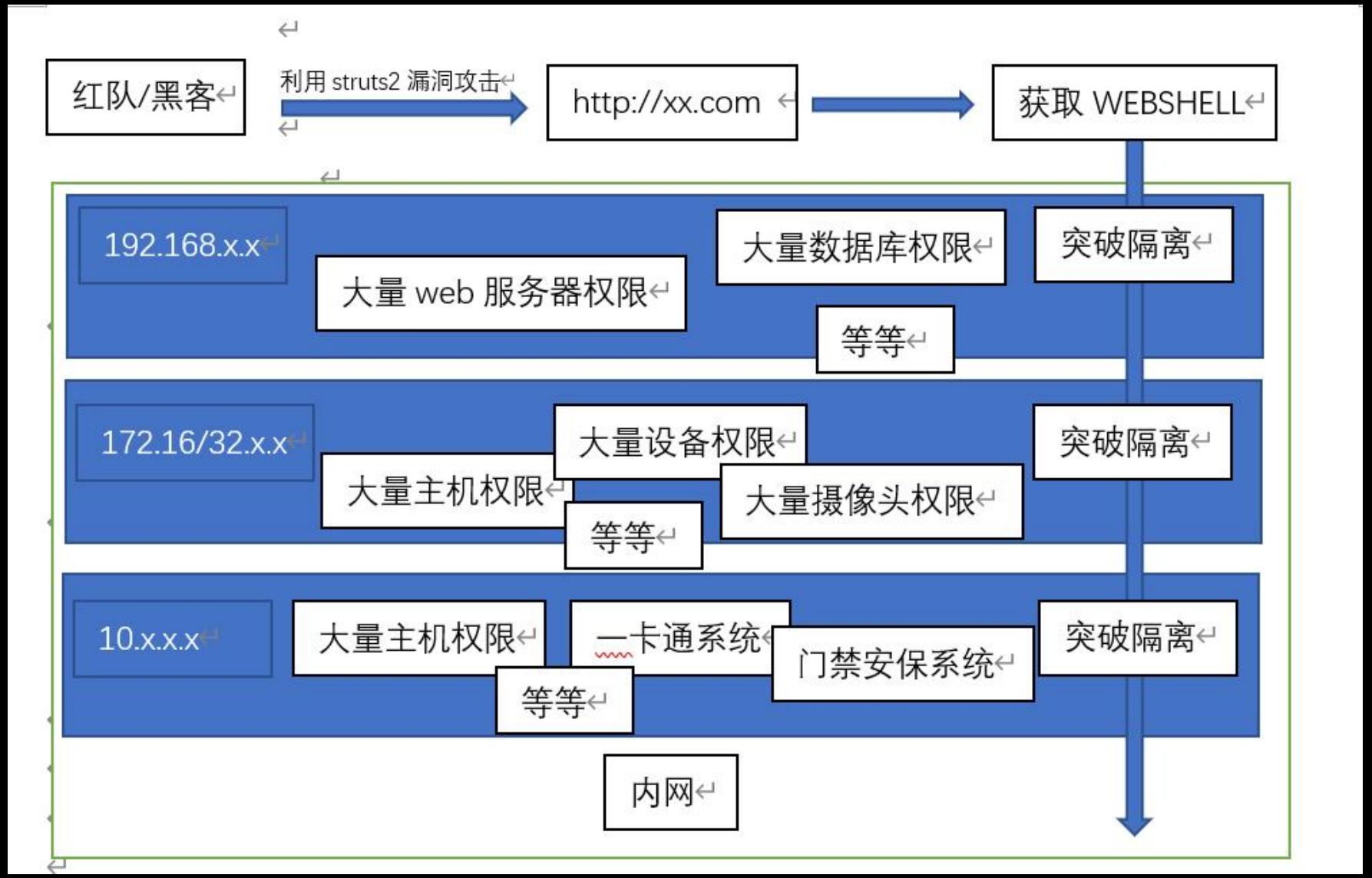
星火计划

360白帽校园行


鱼叉攻击
互联网邮箱/联系方式收集
红队/黑客
互联网 WEB 资产信息收集
WEB 攻击
内部鱼叉
凭据收集
内网横向
规避检测
内部网络/DMZ
内部网络/办公区
内部网络/运维区
内部网络/核心区
工控网
核心服务器
等等

HW中的攻击链/案例

某省网络安全演练中的某个xx大学完整攻击路径



常见鱼叉攻击手法

什么鱼叉攻击？

鱼叉攻击泛指利用社会工程学使目标执行木马或盗取账号密码的攻击手法。

常见的鱼叉攻击链/案例

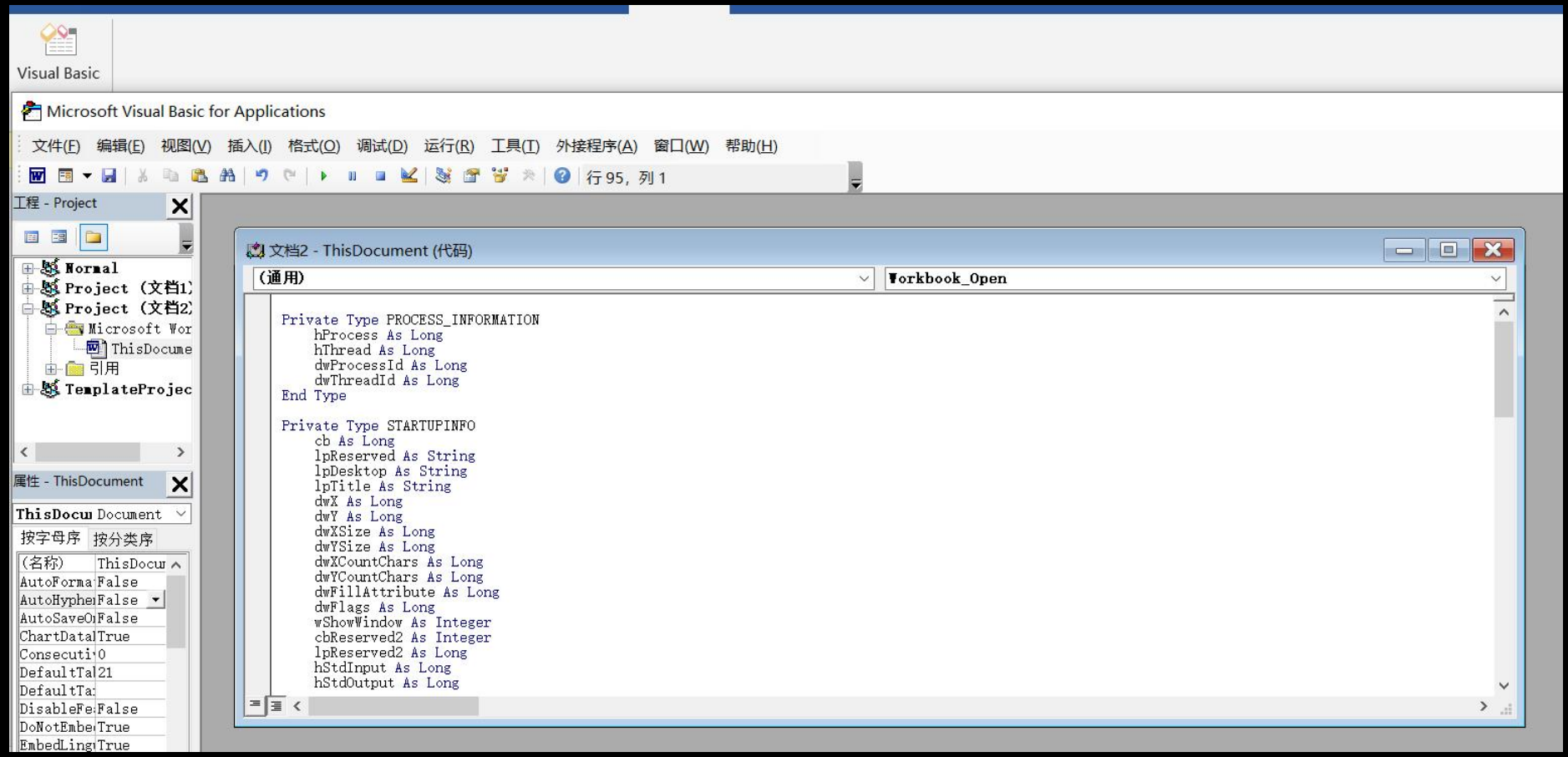
Office钓鱼攻击:

Word宏钓鱼攻击:

宏是Office自带的一种高级脚本特性，通过VBA代码，可以在Office中去完成某项特定的任务，而不必再重复相同的动作，目的是让用户文档中的一些任务自动化。。

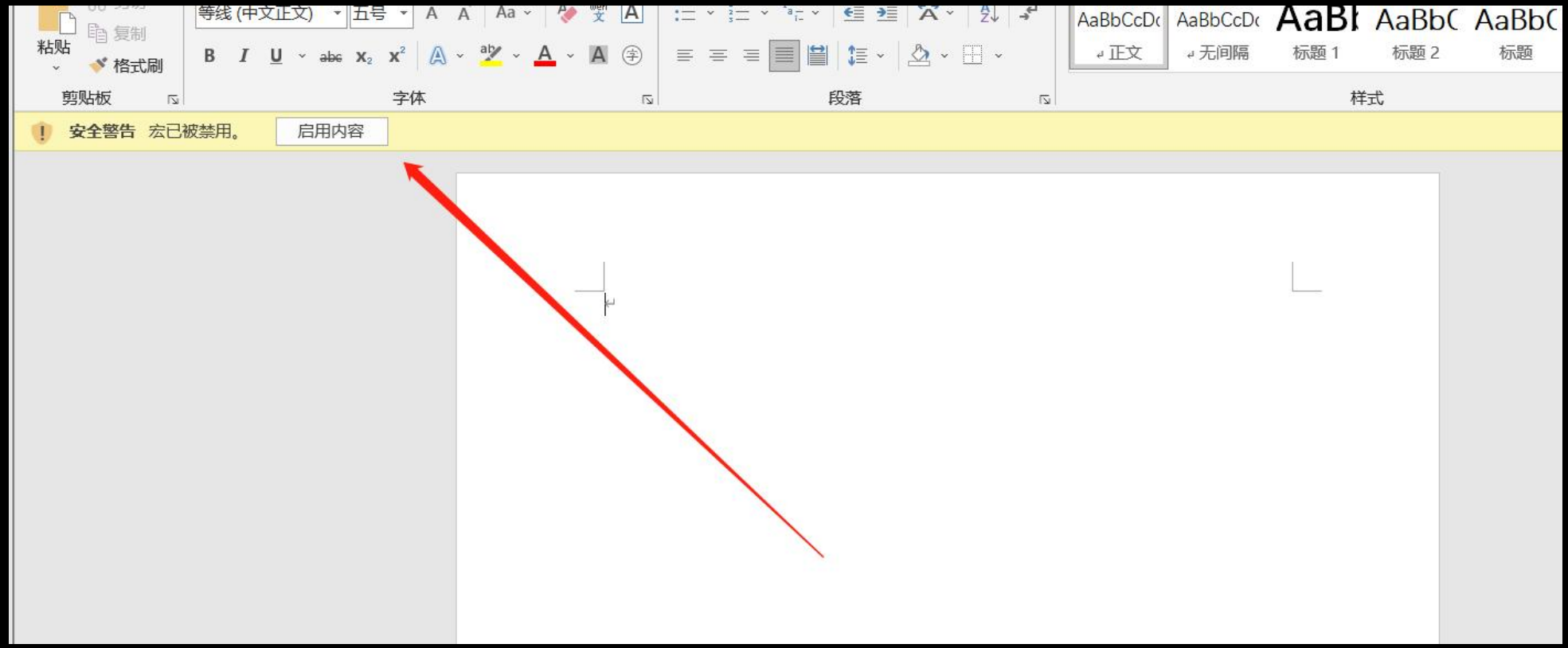
Word宏钓鱼攻击:

我们把宏木马通过VB隐藏在Word文档中



Word宏钓鱼攻击:

我们把宏木马通过VB隐藏在Word文档中



Word宏钓鱼攻击:

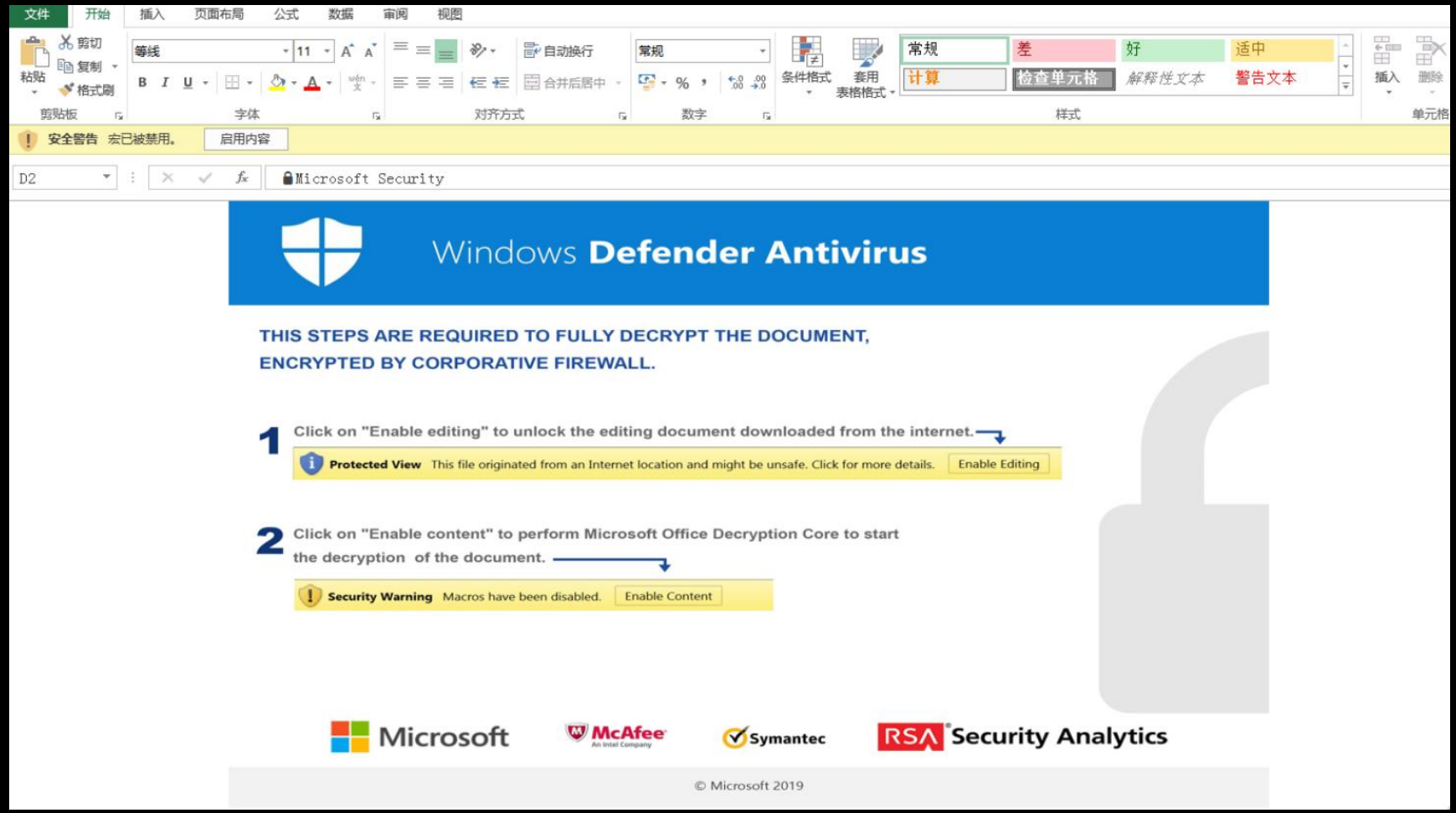
常见的诱导内容:

- 文档是被保护状态，需要启用宏才能查看
- 添加一张模糊的图片，提示需要启用宏才能查看高清图片
- 提示要查看文档，按给出的一系列步骤操作
- 贴一张某杀毒软件的Logo图片，暗示文档被安全软件保护

360 漏洞响应平台

Word宏钓鱼攻击:

伪造Windows Defender防病毒主题文档:



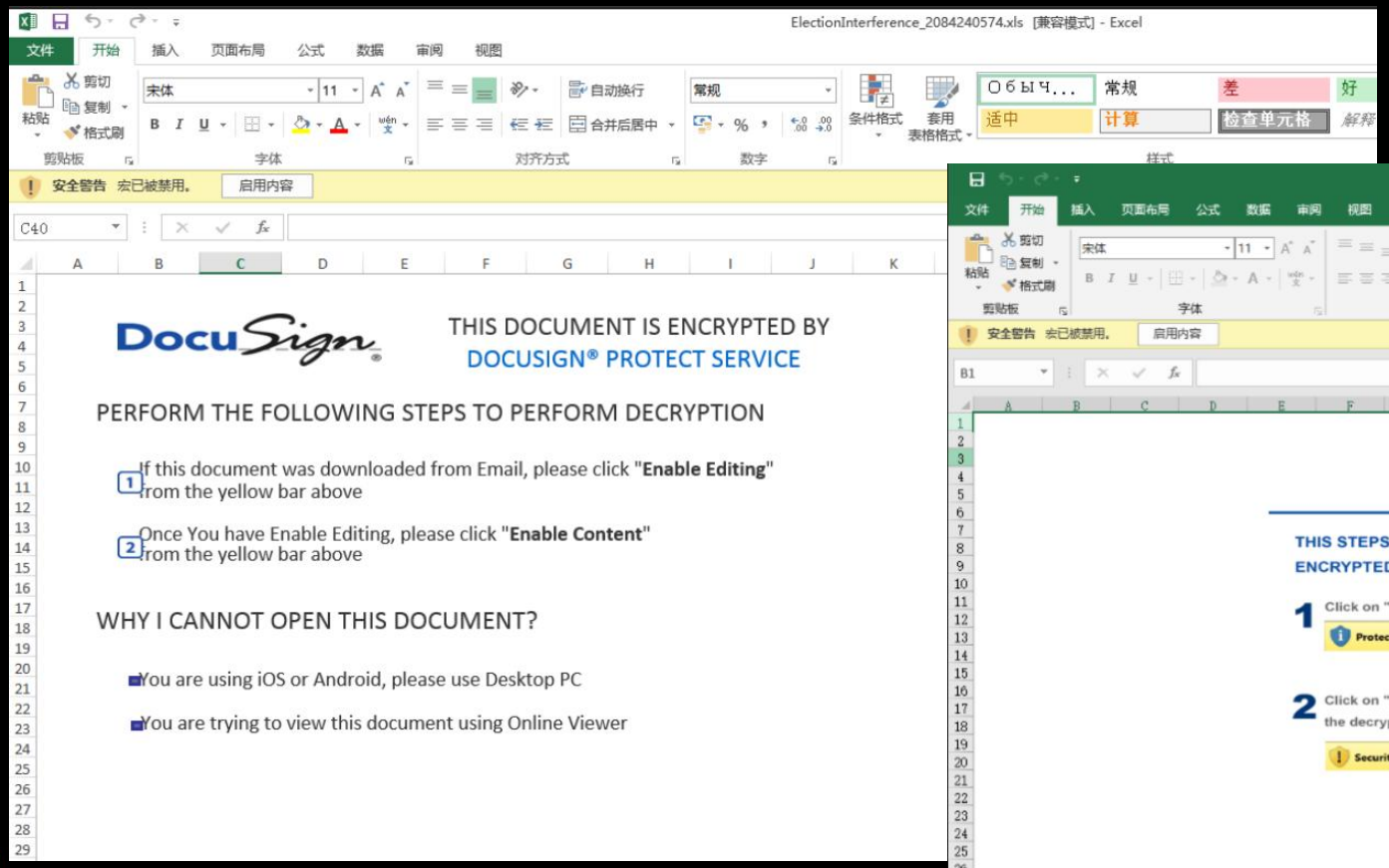
星火计划

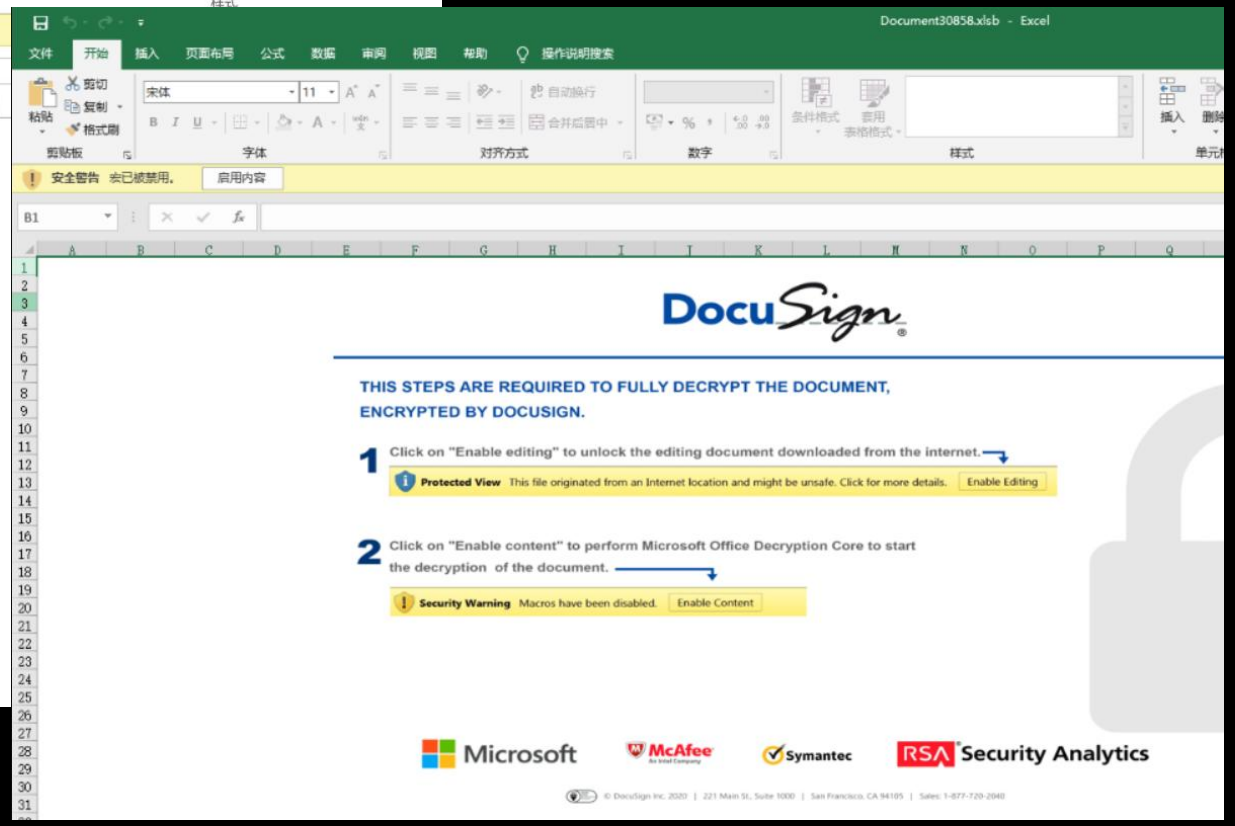
360白帽校园行

360 漏洞响应平台

Word宏钓鱼攻击:

伪造DocuSign加密文档:





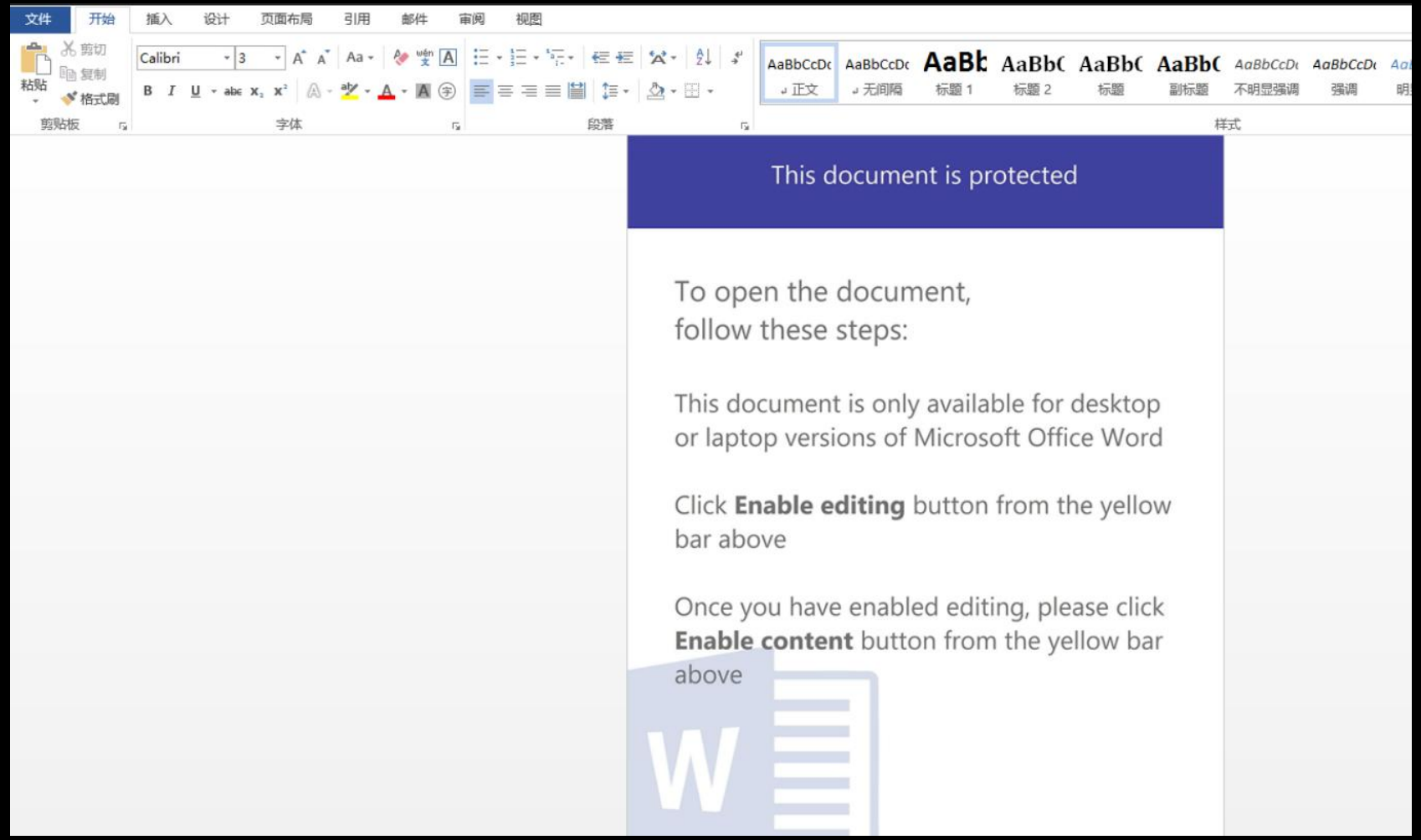
星火计划

360白帽校园行

360 漏洞响应平台

Word宏钓鱼攻击:

伪造受保护的Word文档:

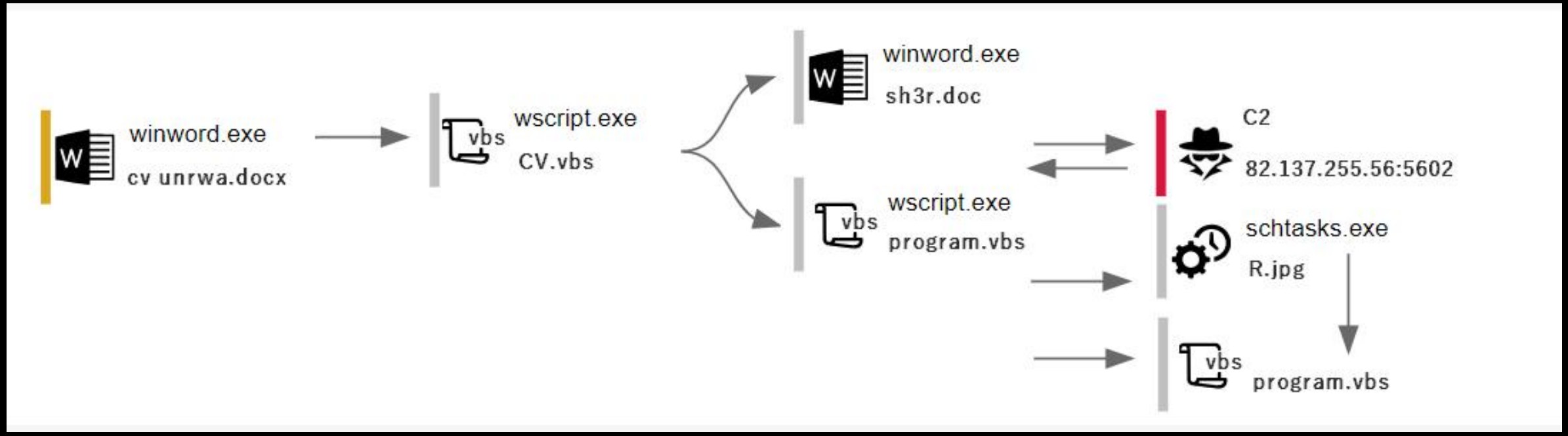


星火计划

360白帽校园行

Word宏钓鱼攻击:

当用户点击“启用内容”后:



Word宏钓鱼攻击:

简单来说：就是你的电脑不光是你的电脑

黑客可以做：


360 漏洞响应平台
星火计划
360白帽校园行
360白帽校园行
360白帽校园行
360白帽校园行
THANKS!