内网入口防护–钓鱼邮件检测与治理

背景：

2018 年 1 月到 12 月期间，微软报告的网络钓鱼事件数量增加了 250%；
钓鱼邮件攻击路径短，可以承载恶意软件、勒索木马等一系列高危攻击手段，
直接投递进企业内网，是最流行有效的网络攻击方式。

诉求：

即使员工毫无戒心，也要将钓鱼邮件对内网的威胁无限减小为0。

成果：

系统钓鱼邮件检出率达到邮件网关的200%以上；
自动化运营流程，大大节约了人力成本。

邮件威胁检测原则

- 邮件不落地
  - 数据拖库
  - 人为泄密
- 保证送达

最初的邮件系统

邮件网关主要解决的问题

- 威胁情报
  - 来源IP
  - 发件地址
  - MD5
- SPF
- 信誉
  - 历史发件数
  - 发件频率

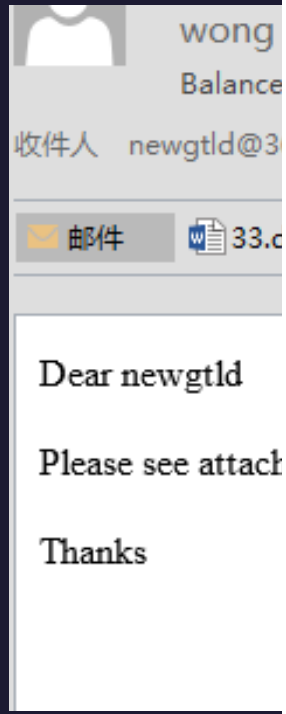
用户终端

邮件服务器

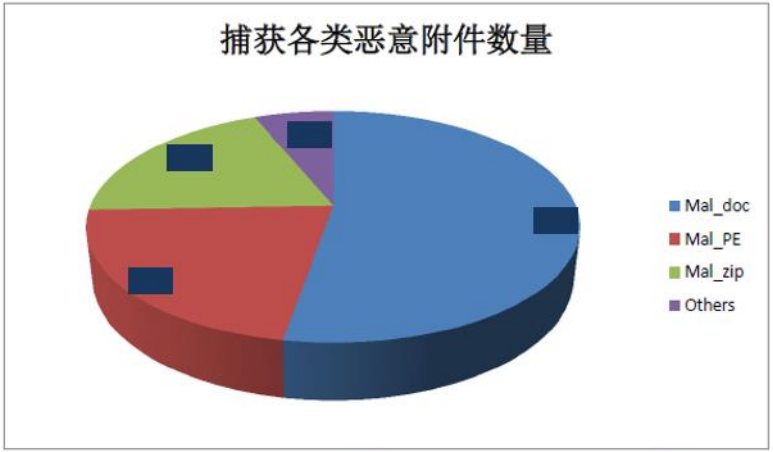
邮件网关

攻击收件人主机

- 特点：
  - 具有恶意行为（附件或链接）
- 安全检测上的对抗：
  - 静态检测
  - 沙箱检测



对上文中收集到的邮件附件进行滤重，得到[redacted]个恶意附件。在些附件中，有恶意文档型邮件[redacted]个，恶意 PE 文件[redacted]个，各类需要解压的恶意文件[redacted]个，无法解压的垃圾邮件附件[redacted]。



需要说明的是，在文档型附件中，有[redacted]个附件是启用宏功能的附件，其余[redacted]个为利用 Office，pdf 漏洞的格式溢出文档。

[redacted] 邮件网关对不同类型恶意附件的识别

在发现的[redacted]个恶意附件中，[redacted]邮件网关成功检出[redacted]个邮件附件，检出率 56.5%。有[redacted]个附件成功绕过[redacted]网关并完成投递。

目标一：增强文件检测能力

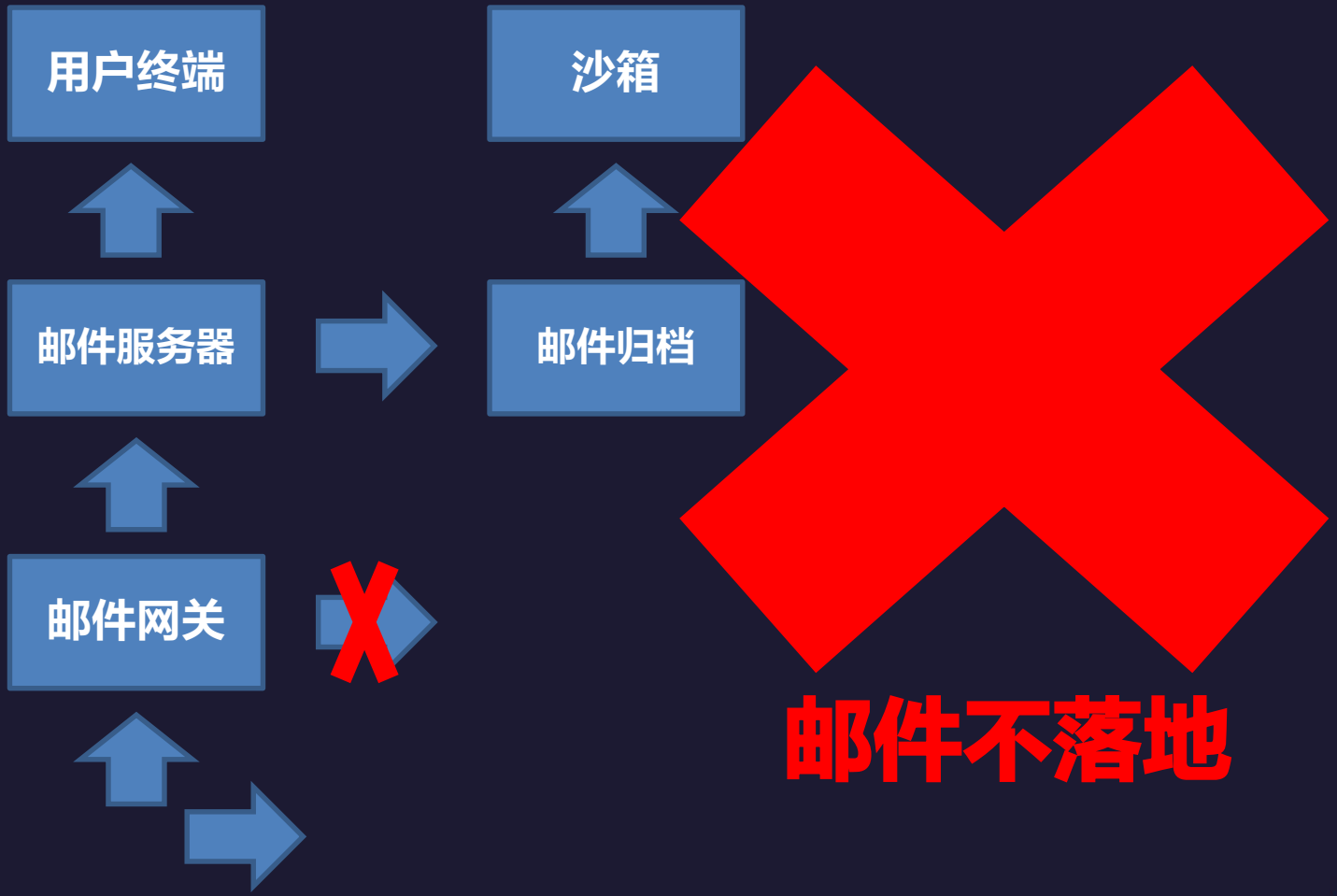
静态检测器

- 文件（网页）检测
  - API、特征字符串……
- URL检测（除情报外准确率低，一般不需要）
  - 情报检测
  - URI字符串格式
  - 域名信息
- 一般方案
  - 邮件网关
  - 静态特征库
- 替代方案
  - Yara

动态检测器

- 文件检测
  - 沙箱行为检测

- 一般方案
  - 沙箱
- 替代方案
  - cuckoo + 评分（分类）器


用户终端
沙箱
邮件服务器
邮件归档
邮件网关
邮件不落地

邮件还原

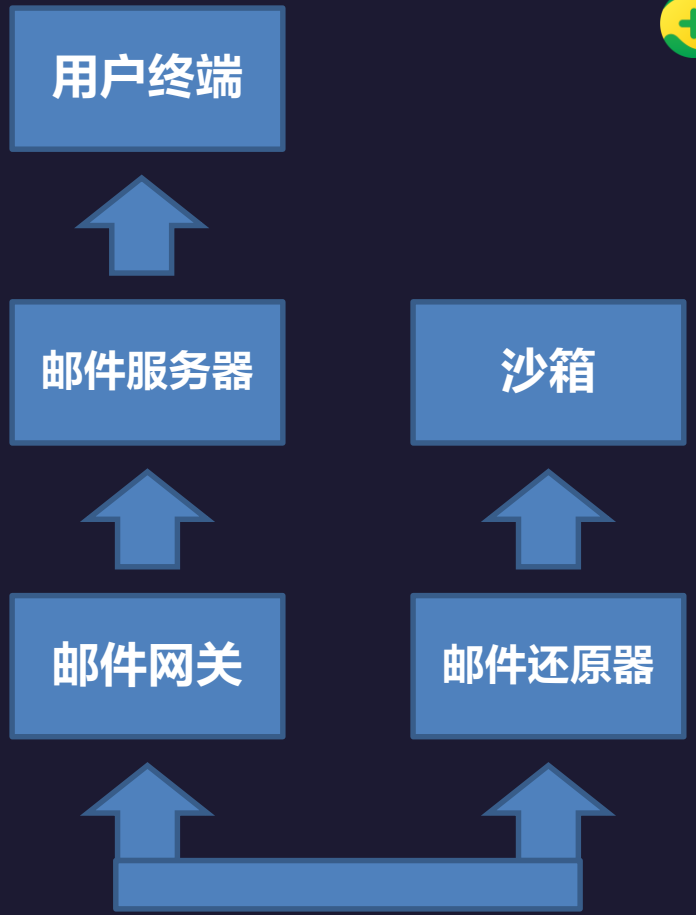
Suricata： SMTP、文件还原

↓

Redis：缓存

↓

代码模块：关联打包


用户终端
邮件服务器
沙箱
邮件网关
邮件还原器

骗取收件人凭证

- 特点：
  - 具有诱导的情感倾向
  - 凭证输入环节
- 邮件内容上的对抗：
  - 自然语言识别方法（意图分析）
  - 图片识别方法（文本识别）
  - 输入环节检查

欺骗收件人“感情”

- 特点：
  - 邮件本身不含有害内容
  - 形式复杂多变
- 安全意识/服务上的对抗：
  - 自然语言识别方法（情感程度分析）
  - 安全意识培训
  - 完善流程/安全制度/监控

发件人: [redacted]@360.cn <[redacted]@360.cn>
发送时间: 2018年12月9日 0:23
收件人: [redacted]@360.cn>
主题: [redacted]

Hello,

I am a spyware software developer. Your account has been hacked by me in the summer of 2018.

I understand that it is hard to believe, but here is my evidence (I sent you this email from your account).

The hacking was carried out using a hardware vulnerability through which you went online (Cisco router, vulnerability CVE-2018-0296).

I went around the security system in the router, installed an exploit there. When you went online, my exploit downloaded my malicious code (rootkit) to your device. This is driver software, I constantly updated it, so your antivirus is silent all time.

Since then I have been following you (I can connect to your device via the VNC protocol). That is, I can see absolutely everything that you do, view and download your files and any data to yourself. I also have access to the camera on your device, and I periodically take photos and videos with you.

At the moment, I have harvested a solid dirt... on you... I saved all your email and chats from your messangers. I also saved the entire history of the sites you visit.

I note that it is useless to change the passwords. My malware update passwords from your accounts every times.

I know what you like hard funs (adult sites). Oh, yes .. I'm know your secret life, which you are hiding from everyone. Oh my God, what are your like... I saw THIS ... Oh, you dirty naughty person ... :)

I took photos and videos of your most passionate funs with adult content, and synchronized them in real time with the image of your camera. Believe it turned out very high quality!

So, to the business! I'm sure you don't want to show these files and visiting history to all your contacts.

Transfer $982 to my Bitcoin cryptocurrency wallet: 1122NYbAT2KkZDZ5TFvGy4D2Ut7eYfx4en Just copy and paste the wallet number when transferring. If you do not know how to do this - ask Google.

My system automatically recognizes the translation. As soon as the specified amount is received, all your data will be destroyed from my server, and the rootkit will be automatically removed from your system. Do not worry, I really will delete everything, since I am 'working' with many people who have fallen into your position. You will only have to inform your provider about the vulnerabilities in the router so that other hackers will not use it.

Since opening this letter you have 48 hours. If funds not will be received, after the specified time has elapsed, the disk of your device will be formatted, and from my server will automatically send email and sms to all your contacts with compromising material.

I advise you to remain prudent and not engage in nonsense (all files on my server).

Good luck!

目标二：增加语义检测能力

语义检测

- 1. 图片识别（文本识别）
- 2. 密码自提（附件密码）
- 3. 情感分析
- 4. 意图分析

- 图片文本识别
  - API
- 密码自提
  - 关键词regex
- 情感分析
  - 情感词典+分类模型
- 意图识别
  - Topic模型+敏感信息关键词

用户终端

邮件服务器

沙箱

语义检测

邮件网关

邮件还原器

目标三：告警关联分析

邮件威胁检测模块

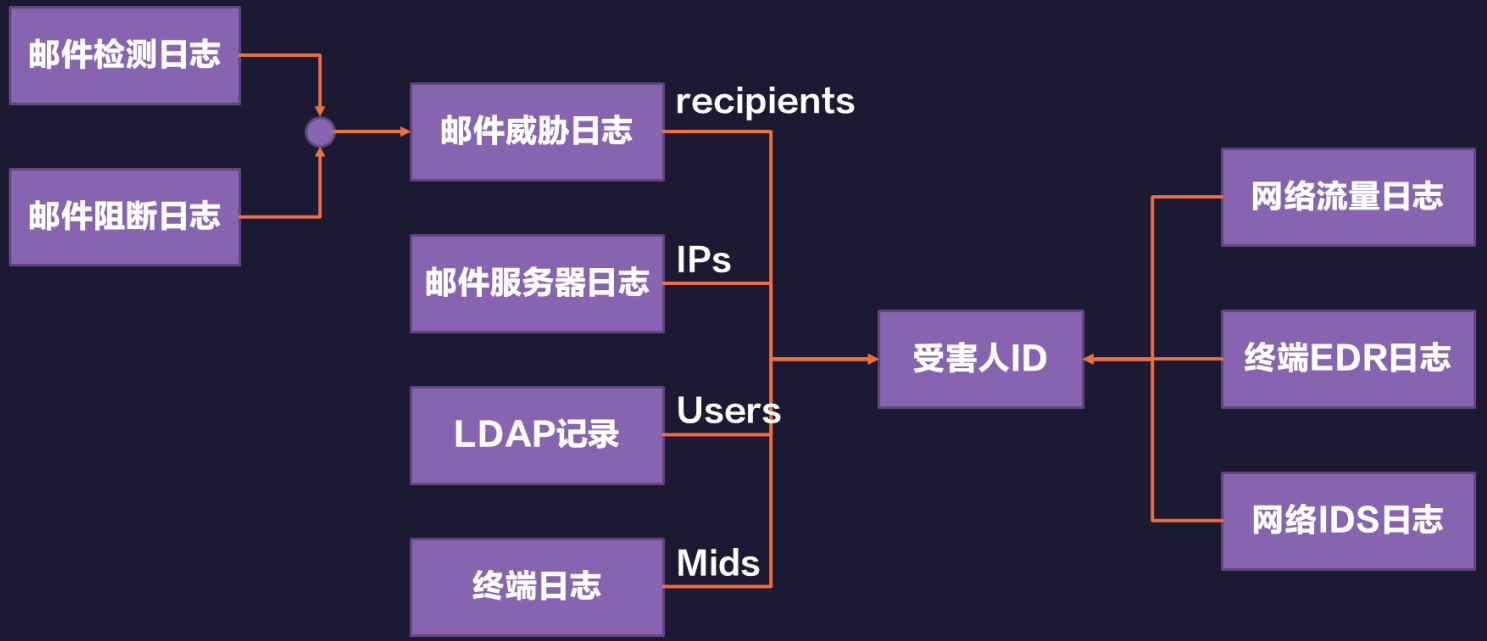
检测模块	静态检测模块	沙箱检测模块	语义检测模块
准确率	高	高	中
查全率	低	高	中
实时性	高	低	高

静态检测器威胁检测流程


邮件还原
邮件检测
告警分析
运营闭环

目标四：自动化运营闭环

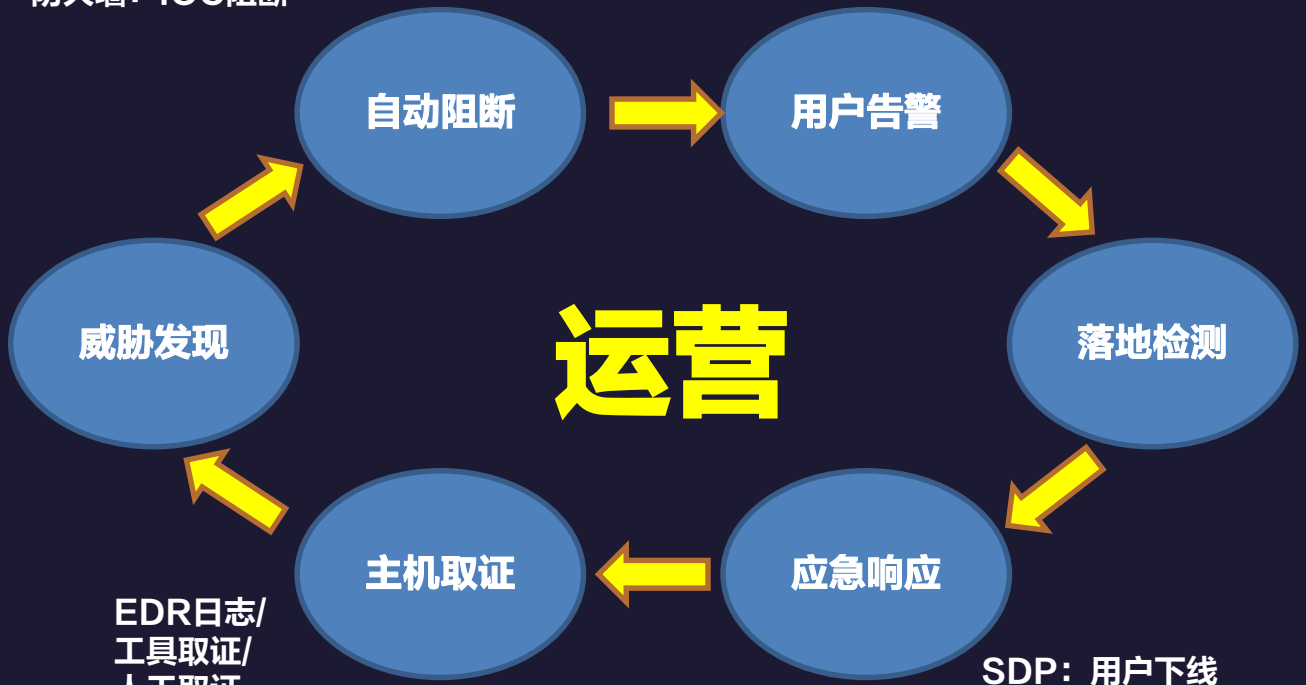
邮件威胁关联分析（ 威胁发现 → 确认落地 ）



邮件威胁运营流程

邮件网关：加黑发件人、IP、主题
防火墙：IOC阻断

对接告警工单平台



EDR日志/
工具取证/
人工取证

SDP：用户下线
筛查其它威胁检测告警，确认横向扩散威胁

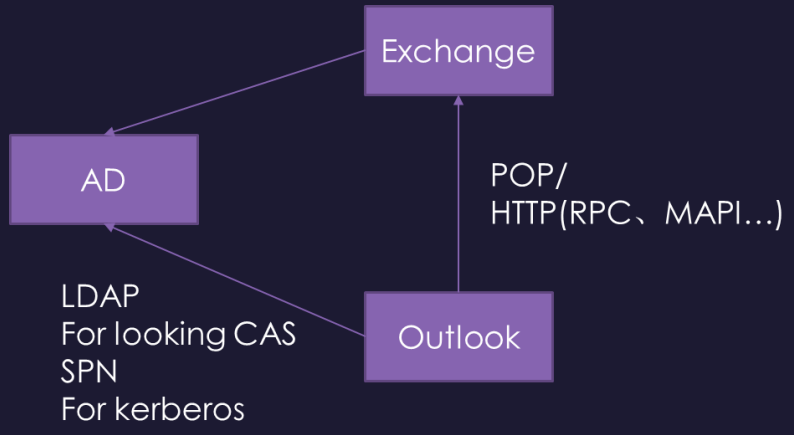
流量采集器	静态检测	语义检测	关联	阻断
	网络侧检测	沙箱检测		
邮件网关		邮件服务器	用户终端	

Lots of things to do

一. 邮箱安全
1. 漏洞防护
1.1 邮箱 APP 漏洞
1.2 Web 漏洞
1.3 认证漏洞
1.4 安全终端
2. 账号安全
2.1 账号登陆异常检测
2.2 账号异常锁定
2.3 认证溯源
3. 配置安全
3.1 安全域配置
3.2 网络架构设置
3.3 认证逻辑配置
二. 邮件安全检测
1. 主机威胁
1.1 静态检测
1.2 沙箱检测
2. 凭证威胁
2.1 语义检测
2.2 网页检测
2.3 快照对比检测
3. 能动性威胁
3.1 语义（敏感测）检测
4. 情报（信誉）检测
5. SPF 检测
三. 安全意识培训
1. 高危人群
1.1 高危人群客服人员
1.2 销售人员
1.3 高权限运维人员
1.4 有价值高管
2. 反馈渠道
2.1 反馈邮箱
2.2 邮箱反馈插件
四. 其它
1. 落地应急流程
2. 渗透信息收集
3. 数据防泄漏布置
4. 威胁溯源
5. 样本积累和情报共享

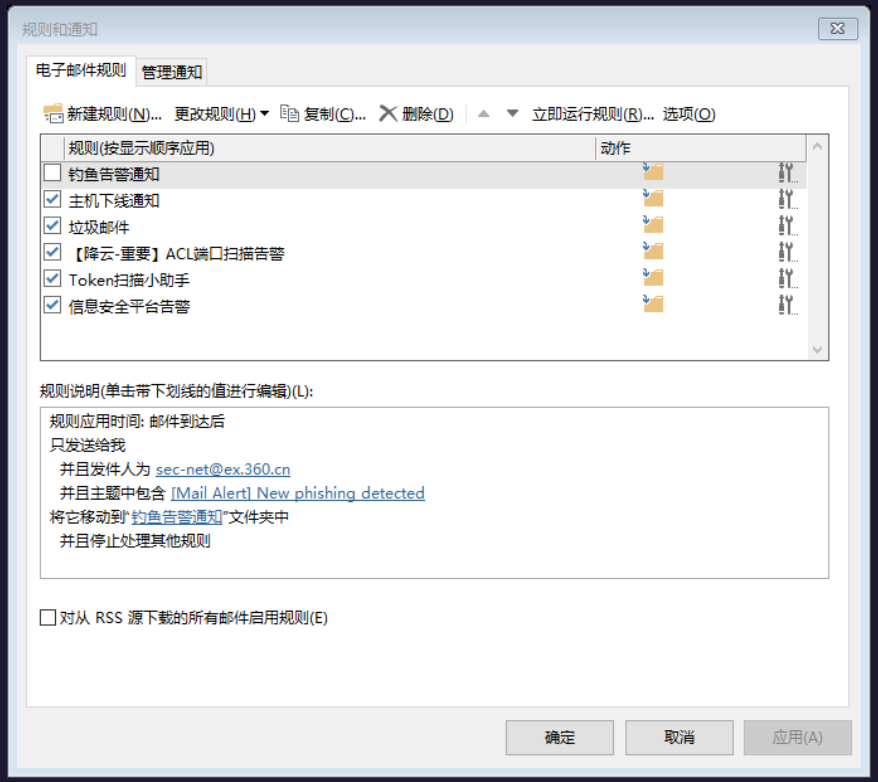
邮箱（账户系统）的安全

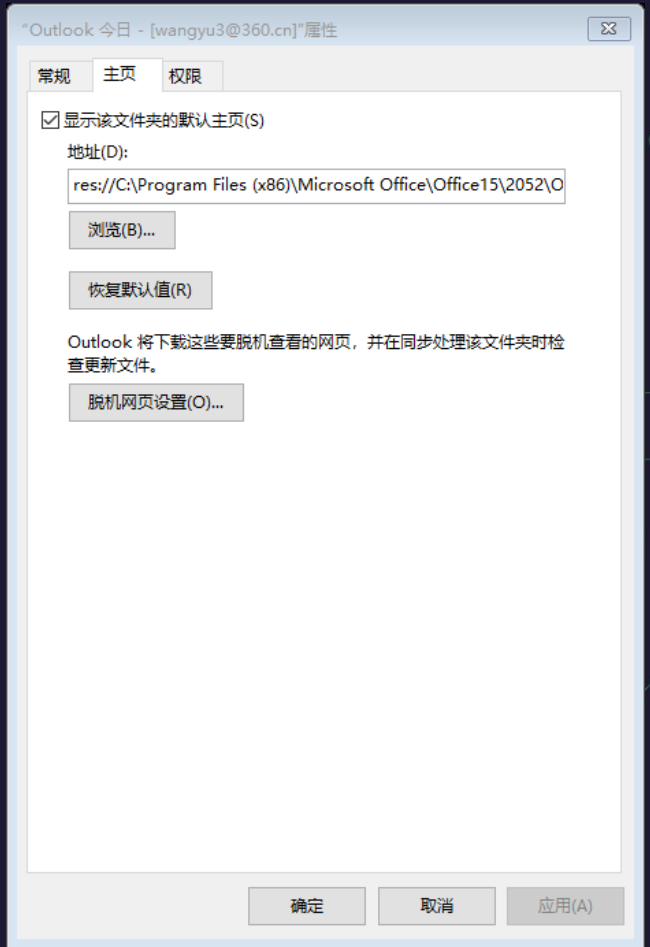
- 爆破
  - 限制密码强度
  - 账号的异常锁定
  - 双因素认证
- Password spray
  - 封IP
- NTLM中继



邮箱（账户系统）的安全

- 设定规则
- 设置主页





THANKS

打个广告

360信息安全运营中心

宙合SaaS：https://zhouhe.360.cn