



钓鱼邮件导论



主讲人：查鲁特

时间：2023.07

前言

1.一方面是随着安全的发展，DMZ区域的安全设备越来越多，而且有价值的目标往往都不缺钱，安全能力疯狂上，经常会出现一个单引号封一天的情况，这大大增加我们的入侵的难度和成本

2.另一方面，一些企业和机构也开始重视安全了，开始做安全治理，之前开放在公网的边界设备和服务纷纷移入内网，可以打的资产变少了，难度自然增加

综上两点，钓鱼就成了一个可以一发入魂并且异常快捷高效的攻击方式。

邮件钓鱼是钓鱼的一种方式，虽然随着IM工具的兴起，钓鱼的主要方式也从邮件向微信，脉脉，TG等即时社交工具偏移，但是邮件钓鱼作为一种经典方式还是值得讲一讲。



目录 / CONTENTS

01

钓鱼邮件种类

02

钓鱼邮件手法

03

如何成功制作一封钓鱼邮件

01

•钓鱼邮件种类

钓鱼邮件种类

- 1 钓账号密码
- 2 钓权限
- 3 其他（如金融诈骗等）



钓账号密码

形态:

往往邮件正文会存在一个超链接，超链接往往指向伪造页面/反向代理

目的:

以密码过期，权限失效等理由，威逼利诱引导受害者填写账号密码。

← admin@tsnighua.cn



收件人:

添加至群组

异常行为登录警告

今天 21:17

清华大学用户:

网盾系统监测发现，你的账号存在境外可疑地区多次登录的异常情况，可能已经泄露个人重要信息！

请遵照以下操作指南尽快更新账号密码，以免给个人和学校造成损失！

[专用链接](#)

IT技术部门

2021年12月1日


钓权限

关于2019年年终绩效考核制定 ☆ 已读

发件人: a <c...@m>

时间: 2019年12月18日(星期三) 中午1:03

收件人: j... <pub...@cn>

附件: 1 个 ( 2019年终绩效考核标准1.docm)

为了营造绿色健康的邮箱环境,我们想了解一下,这是否您订阅的邮件? [是我订阅的](#) [不是我订阅的](#) [我不确定](#) [自动归档](#)

各分中心:

根据《2019年人事考核方案》,总部已完成19年年终绩效考核制定,请全体员工于**2019年12月23日**之前完成年终绩效考核,以便您的考核人能及时完成反馈。

温馨提示:

- 1.请根据最新制定的《2019年年终绩效考核标准制定》进行制定,如果逾期可能会影响到**年终的排名及年终奖发放**。
- 2.总结逾期提交处罚方式(最终以集团后期发文为准):逾期1次,口头批评;逾期2次,书面批评;逾期3次,通报批评;逾期4次及以上,警告;以上所有处罚录入系统,不扣薪,应用于评优及晋级。
- 3.评分标准如附件,如果文档显示空白或者格式有错,请点击启用内容。

另请各分中心务必高度重视,持续改善人事基础工作的准确性、合规性。我们将持续通报检查情况,如有任何问题及建议,请随时沟通。

形态:

往往都会存在一个附件,可以是office文件,加密压缩的EXE,或者其他的可执行文件,内容一般是木马回连。也可以基于目的不通执行不通的操作。(比如说可以过UAC并提权的勒索软件),当然可执行文件需要能过杀软和邮件网关,不然都是白搭。

目的:

让用户执行附件,为了确保点击率,在话术上同样需要我们上一些手段,或威逼或者利诱,当然色诱也是一种方式。

钓权限

保存

2019年终绩效考核标准1.docm - 已保存到这台电脑

搜索

开始插入设计布局引用邮件审阅视图帮助

剪切复制格式刷

字体

段落

样式

编辑

全警告 宏已被禁用。 启用内容

2019 年终绩效考核标准

2019 年度检查考核标准--薪酬福利

主: 如果图表显示空白或者格式有错, 请点击启用内容。

检查频次	检查项目	检查目的	检
年度			

■ 钓权限



目标环境:

邮件网关: 本地EXChange

操作系统: Windows

杀软: 赛门铁克

中心:

为什么是docm:

因为在测试能否过邮件网关的时候发现, exchange邮件网关的拦截规则有点迷:

拦截: doc + 宏, 可执行程序(exe, lnk等)

进垃圾箱: 加密压缩包

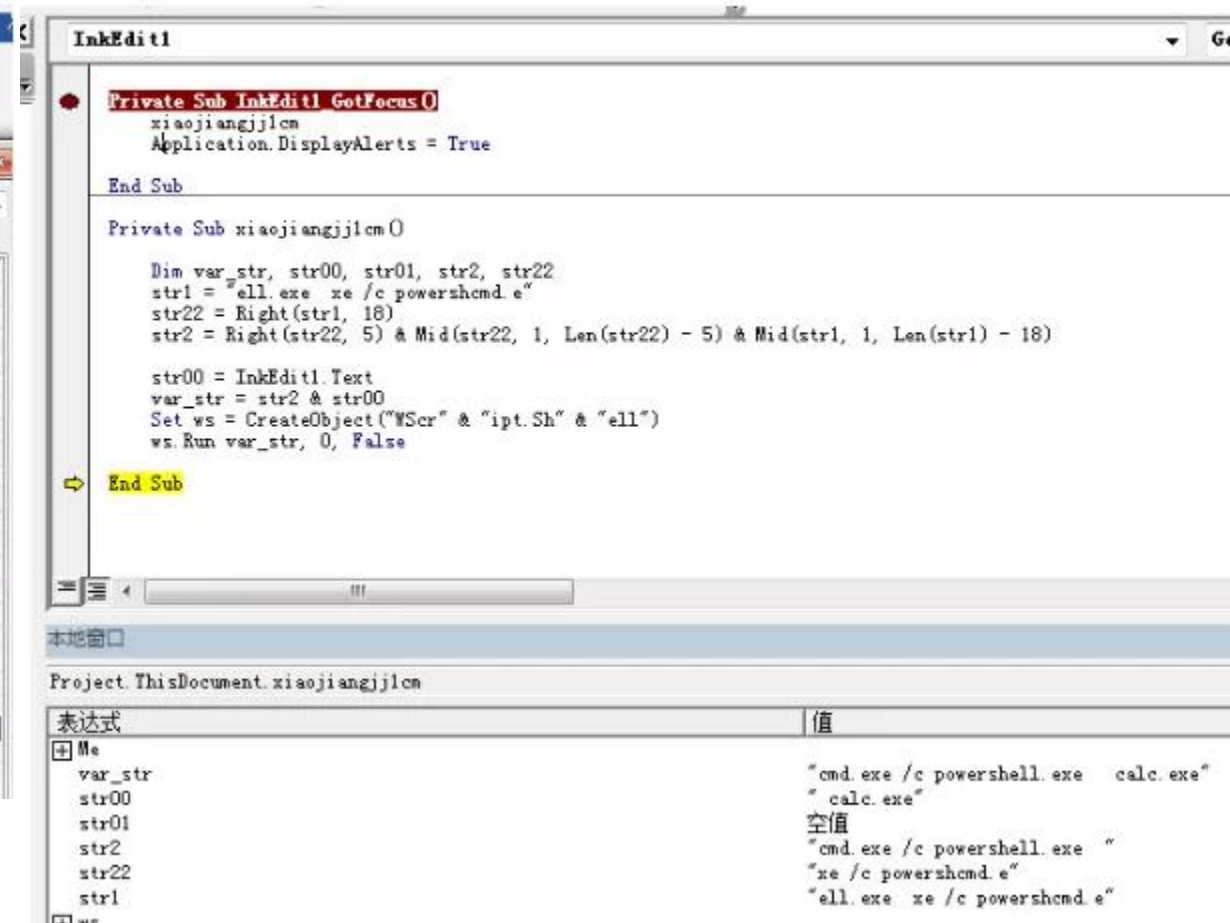
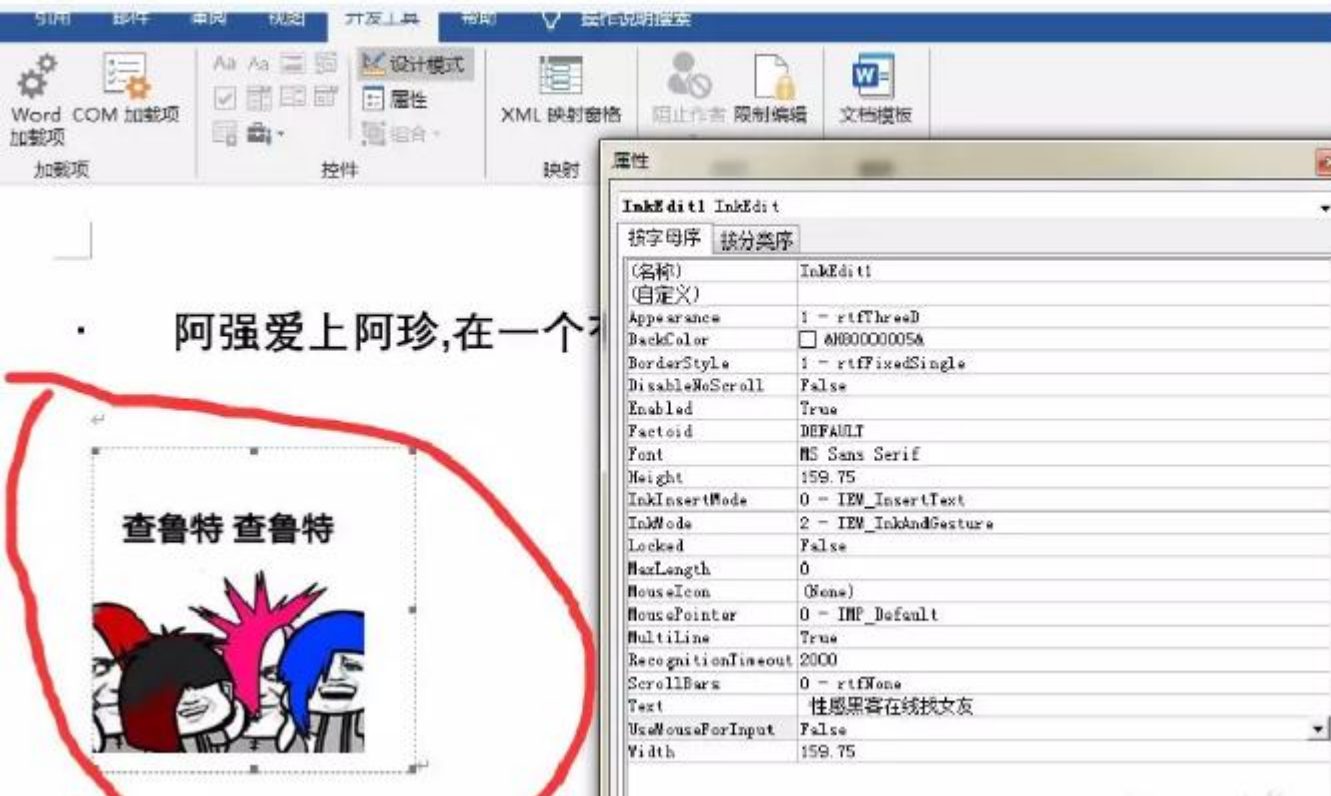
进收件箱: docm + 宏(非恶意)

所以最终采用DOCM+宏的方式作为钓鱼附件, 但是邮件和杀软拦截恶意特征的宏文件, 所以需要进行一定的绕过, 这次的文档采用了宏拼接进行绕过特征值。

钓权限

这里我们采用宏**拼接**的方法。这是一个过静态免杀的姿势，目的是为了过关键字特征，**拼接部分**的取值可以是文档任意部分，如左图就把代码插在了控件的属性变量中，在宏代码就可以直接取值

鼠标滚轮缩放图片

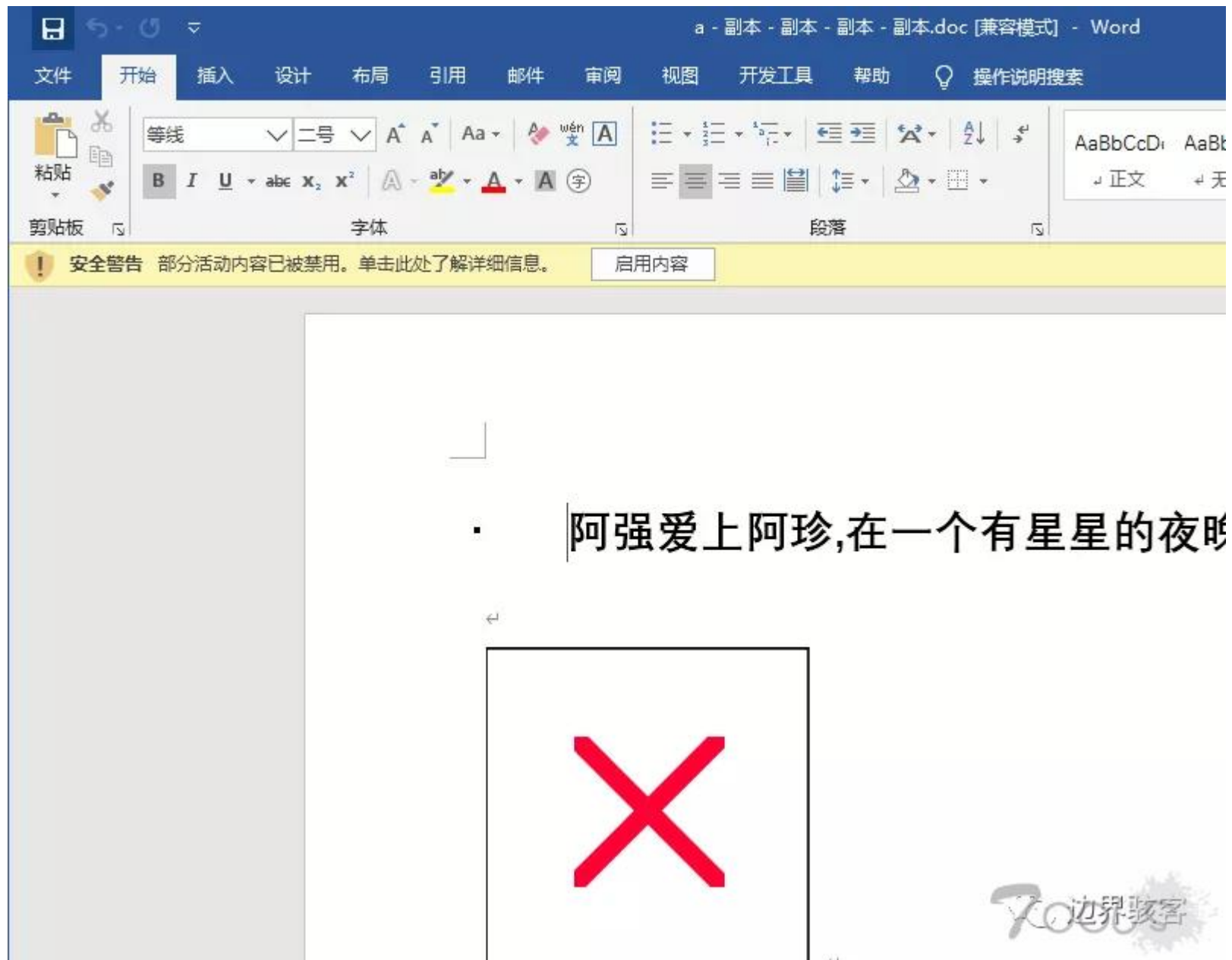


右边这张图是效果图和代码，为了方便大家理解，可以看下方拼接后的结果

钓权限

最后到受害者展现的效果图可以如右图一样，把样式改成不可见或者图裂的方法，诱导受害者启用宏。

具体的内容细节可以看土司论坛我的文章和微信公众号



其他类型钓鱼

形态:

二维码钓鱼，往往正文或者附件有一张二维码的图片，可以是APP木马诱骗安装，可以是钓账号密码，也可以是金融诈骗。二维码诈骗是一个比较与时俱进的手法，毕竟二维码才出来多少年。

目的:

诱骗受害者扫描，一般分金融诈骗和手机权限钓鱼

金融诈骗：普遍是伪造银行页面，骗取银行卡号，转账密码和短信验证码。

手机权限：装APK，获取通讯录权限，最经典的就是裸聊了。



02

钓鱼邮件手法

钓鱼邮件手法



01

伪造页面

02

伪造发件人

03

附件型钓鱼

04

链接，超链，二维码

05

反向代理

06

软件漏洞及系统特性

■ 页面伪造



登录

电子邮件、电话或 Skype

没有帐户? [创建一个!](#)

[无法访问您的帐户?](#)

后退

下一步



登录选项

■ 页面伪造

不管是页面伪造还是反向代理，我们在真实场景钓鱼的时候需要注意，当邮件正文中有链接的时候，当邮件经过邮件网关和用户点击链接的时候，邮件厂商，特别是当目标使用**在线邮箱**的时候（如上图的微软在线邮箱），用户每次点击厂商会有爬虫去爬取这个链接，来判断这个链接是否是钓鱼邮件。如果判定为钓鱼页面的话，会把信息报给**APWG**这个组织，几乎是在5分钟内，我们的域名会如下图一样，被标红并弹窗警告。

所以我们在实战中，在搭建钓鱼页面的时候，要把反爬虫考虑进去



Deceptive site ahead

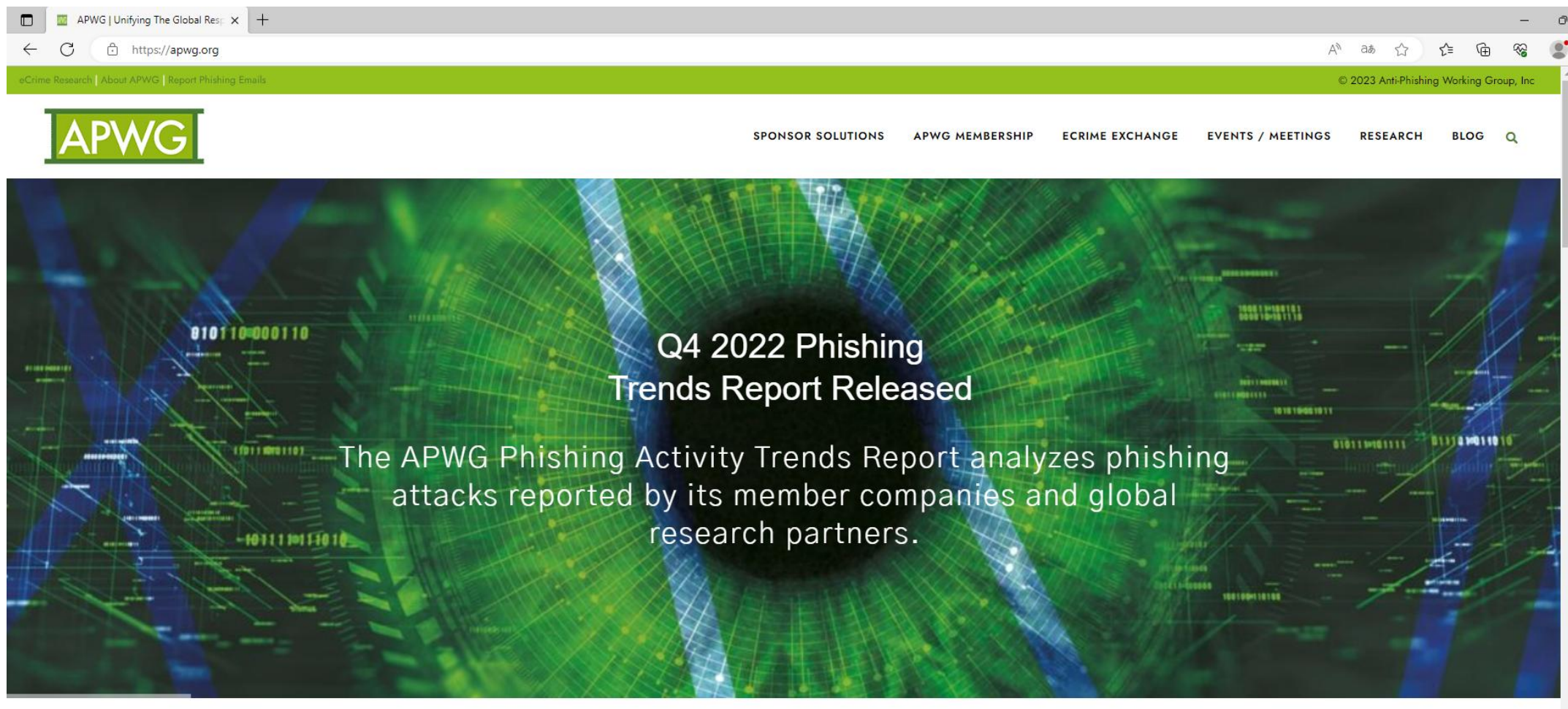
Attackers on **kat.cr** may trick you into doing something dangerous like installing software or revealing your personal information (for example, passwords, phone numbers, or credit cards).

[Details](#)

[Back to safety](#)

反网络钓鱼工作组(**APWG**) 是一个国际[联盟](#)，致力于消除[网络钓鱼](#)及相关事件引起的[欺诈](#)和[身份盗窃](#)。它汇集了受网络钓鱼攻击影响的企业：安全产品和服务公司、执法部门机构、政府机构、[行业协会](#)、区域性国际条约组织和通信公司。

APWG由[David Jevans](#)于 2003 年创立，拥有来自全球 1700 多家公司和机构的 3200 多名成员。成员包括[卡巴斯基实验室](#)、[BitDefender](#)、[赛门铁克](#)、[McAfee](#)、[VeriSign](#)、[IronKey](#)和[Internet Identity](#)等领先的安全公司。金融业成员包括[ING 集团](#)、[VISA](#)、[万事达卡](#)和[美国银行家协会](#)。



伪造发件人

1. 昵称伪造
2. 相近字符（罗马字符/相近的域名）
3. 发件人伪造（SPF）

（重要）汇通达邮箱升级通告！ ☆

发件人：邮件管理通知 <mail@servrce.pw>

时 间：2014年9月12日(星期五) 上午10:07

收件人：葛一枫 <yf.ge@htd.cn>

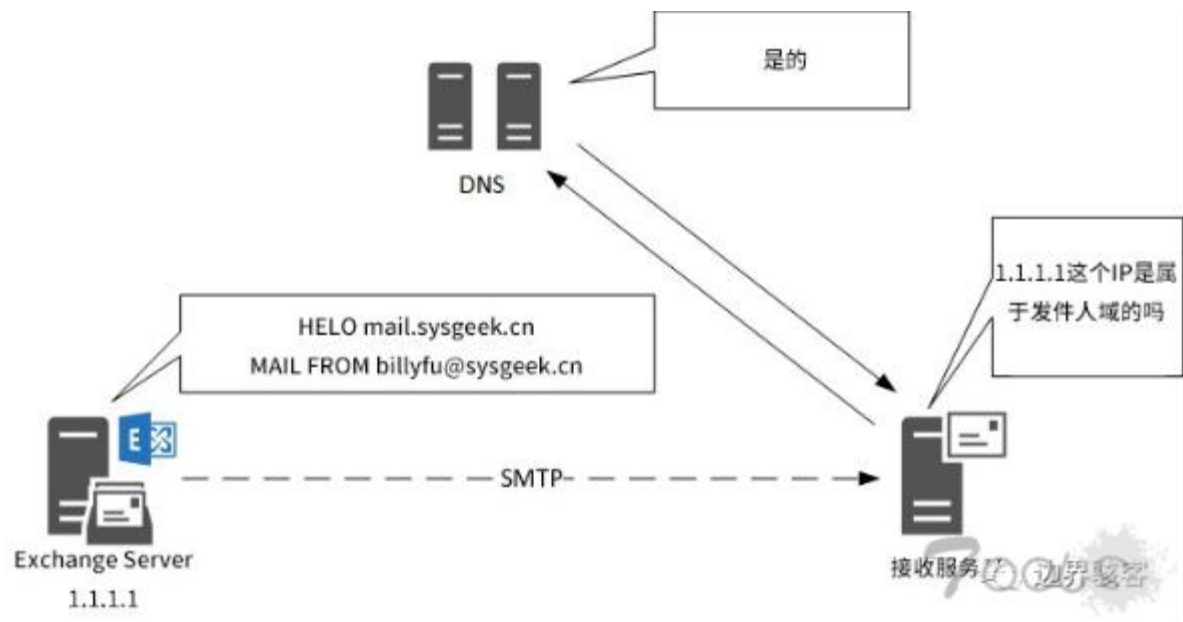
伪造发件人



发件人伪造

要了解什么是发件人伪造，就得先知道**SPF**是啥。

SPF记录的用途是阻止垃圾邮件发件人发送假冒您的域中的“发件人”地址的电子邮件。收件人可以参考SPF记录来确定号称来自您的域的邮件是否来自授权邮件服务器。对于大多主流的邮件服务商，鉴别发送者的SPF记录有助于抵御垃圾邮件给接收者带来的骚扰。



伪造发件人

```
C:\Users>nslookup -q=txt t001s.net
服务器: UnKnown
Address: 10.9.255.1

非权威应答:
t001s.net text =
"ca3-1268c7d3ec3949e689389f4d86818dce"
t001s.net text =
"v=spf1 include:spf.mail.qq.com ~all"

C:\Users>nslookup -q=txt spf.mail.qq.com
服务器: UnKnown
Address: 10.9.255.1

非权威应答:
spf.mail.qq.com text =
"v=spf1 include:qq-a.mail.qq.com include:qq-b.mail.qq.com include:qq-c.mail.qq.com include:biz-a.mail.qq.com include:biz-b.mail.qq.com include:biz-c.mail.qq.com include:biz-d.mail.qq.com -all"

C:\Users>nslookup -q=txt qq-a.mail.qq.com
服务器: UnKnown
Address: 10.9.255.1

非权威应答:
qq-a.mail.qq.com text =
"v=spf1 ip4:101.226.139.0/25 ip4:101.91.43.0/25 ip4:101.91.44.128/25 ip4:112.64.237.128/25 ip4:116.128.173.0/25 ip4:121.51.40.128/25 ip4:121.51.6.0/25 ip4:162.62.52.214 ip4:162.62.55.67 ip4:162.62.57.0/24 ip4:162.62.58.211 ip4:162.62.58.216 -all"

C:\Users>
```

v=spf1 SPF 的版本。如果使用 Sender ID 的话，这个字段就应该是 v=spf2 定义匹配时的返回值。

可能的返回值包括：

pre

返回值

描述

+

缺省值。在测试完成的时候表示通过。

-

表示测试失败。这个值通常是 -all，表示没有其他任何匹配发生。

~

表示软失败，通常表示测试没有完成。

?

表示不置可否。这个值也通常在测试没有完成的时候使用。

定义使用的确认测试的类型。

v=spf1 ip4:101.226.139.0/25 -all

解读：

允许 101.226.139.0/25这个网段的IP使用t00ls.net的发件人进行发现，策略为软拒绝（宽松策略）

附件型钓鱼


1. 可执行文件, exe, bat, lnk, 安装包等通常以加密压缩包的形式存在
2. 漏洞/ Office day (CVE-2021-40444)
3. JS 通常配合漏洞使用 (内部互相发送邮件默认加载JS)

关于2019年年终绩效考核制定 ☆ 印

发件人: a <6...jm>

时间: 2019年12月18日(星期三) 中午1:03

收件人: | <pub...cn>

附件: 1 个 ( 2019年年终绩效考核标准1.docm)

为了营造绿色健康的邮箱环境,我们想了解一下,这是否您订阅的邮件? [是我订阅的](#) [不是我订阅的](#) [我不确定](#) [自动归档](#)

各分中心:

根据《2019年人事考核方案》,总部已完成19年年终绩效考核制定,请全体员工于**2019年12月23日**之前完成年终绩效考核,以便您的考核人能及时完成反馈。

温馨提示:

1. 请根据最新制定的《2019年年终绩效考核标准制定》进行制定,如果逾期可能会影响到**年终的排名及年终奖发放**。
2. 总结逾期提交处罚方式(最终以集团后期发文为准):逾期1次,口头批评;逾期2次,书面批评;逾期3次,通报批评;逾期4次及以上,警告;以上所有处罚录入系统,不扣薪,应用于评优及晋级。
3. 评分标准如附件,如果文档显示空白或者格式有错,请点击启用内容。

另请各分中心务必高度重视,持续改善人事基础工作的准确性、合规性。我们将持续通报检查情况,如有任何问题及建议,请随时沟通。

超级链接

电子邮件暂停提醒 ★

dlut.edu.cn

发给 张巍

发件人: dlut.edu.cn <info@mieuxltech.com>

收件人: 张巍 <zhangwei@dlut.edu.cn>

时间: 2020年4月14日 (周二) 13:50 🕒

大小: 12 KB

这是通知您，我们正在验证活动帐户。请点击下面的验证链接确认您的电子邮件仍处于活动状态并正在使用中：

[验证电子邮件帐户](#)

此致

IT帮助台
信息技术办公室

■ 二维码钓鱼

出现位置：二维码经常出现的位置有正文，超链，图片附件

特性：难以防御，基于上面几个出现位置，当前主流的邮件网关和邮件沙箱等安全设备很难检测出来

邮件网关：正文是图片一般不拦截

邮件沙箱：附件是张图片，邮件沙箱一般不去跑，即使跑了也无法解析内容

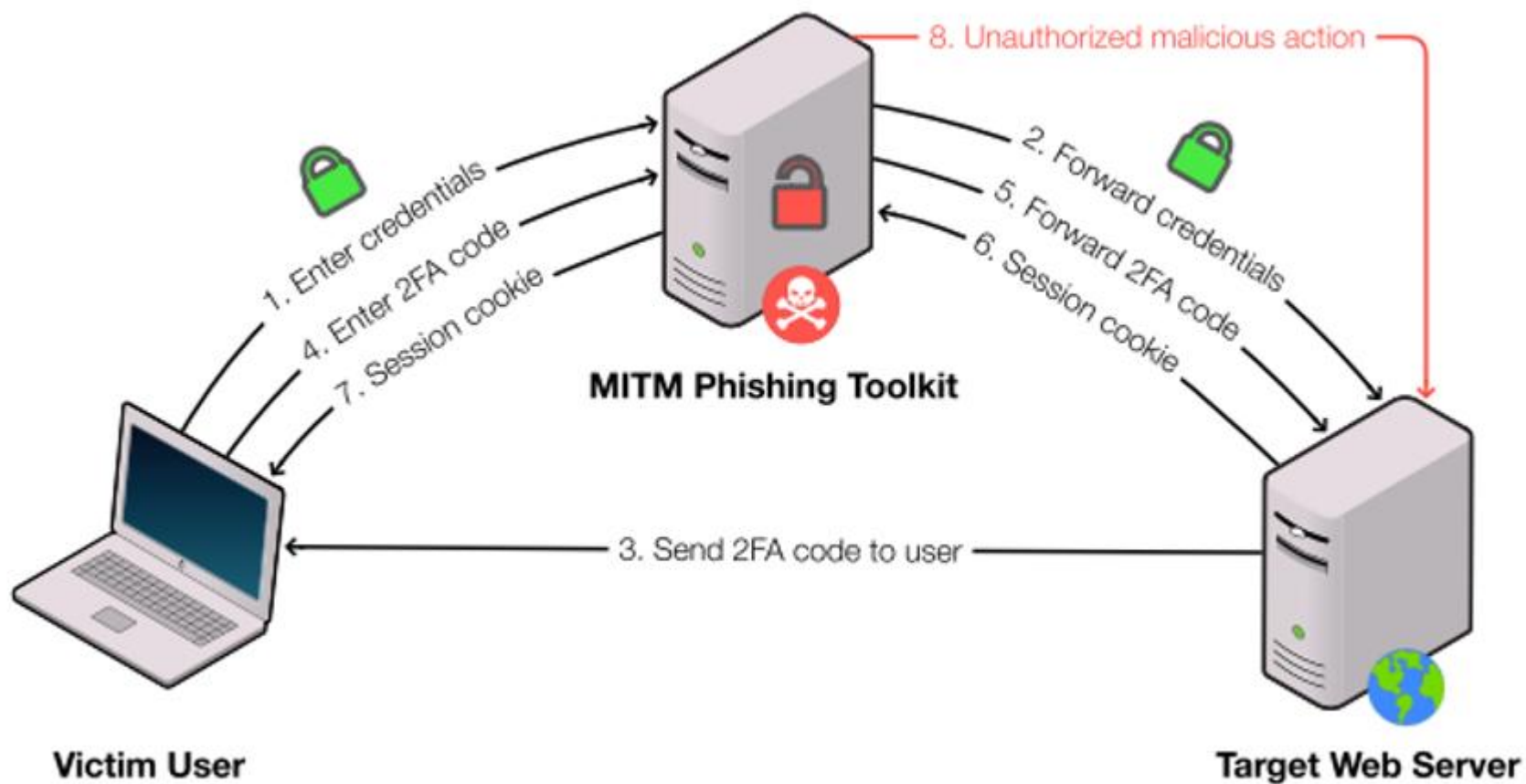
超链：把二维码上传到白域名的文件服务，头像或者论坛安全设备一看白域名，又是图片直接放行

难以止损：受害人是公司/组织的话，防火墙即使拉黑二维码解析的域名，但是二维码普遍是手机端扫描，大部分连的是4G/5G网络。即使发现是钓鱼邮件也很难止损



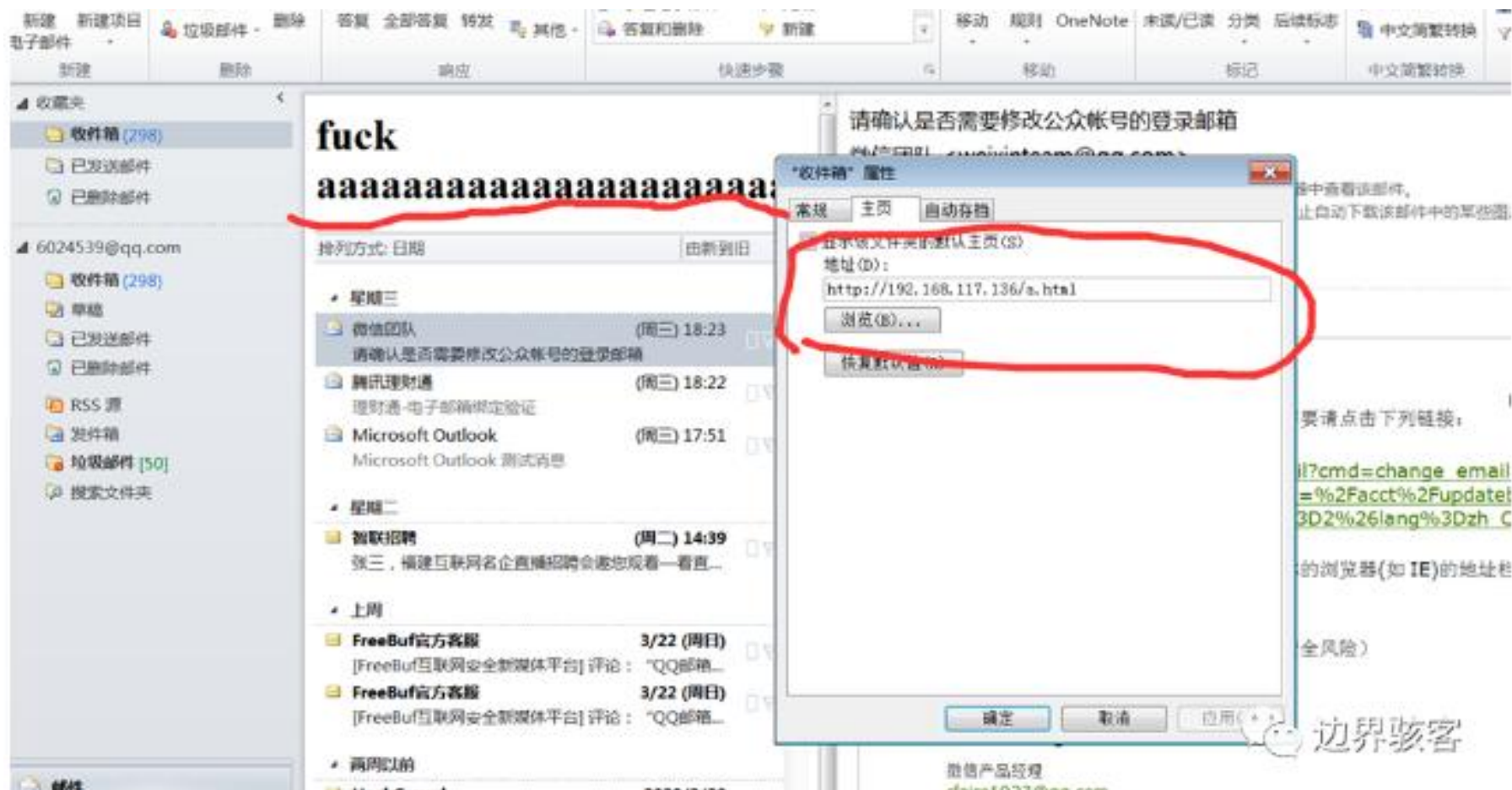
反向代理

常用于钓账号密码，可以过二次认证和异地登陆，缺点是存在一定技术难度，特别是在线邮箱，需要指定绕过

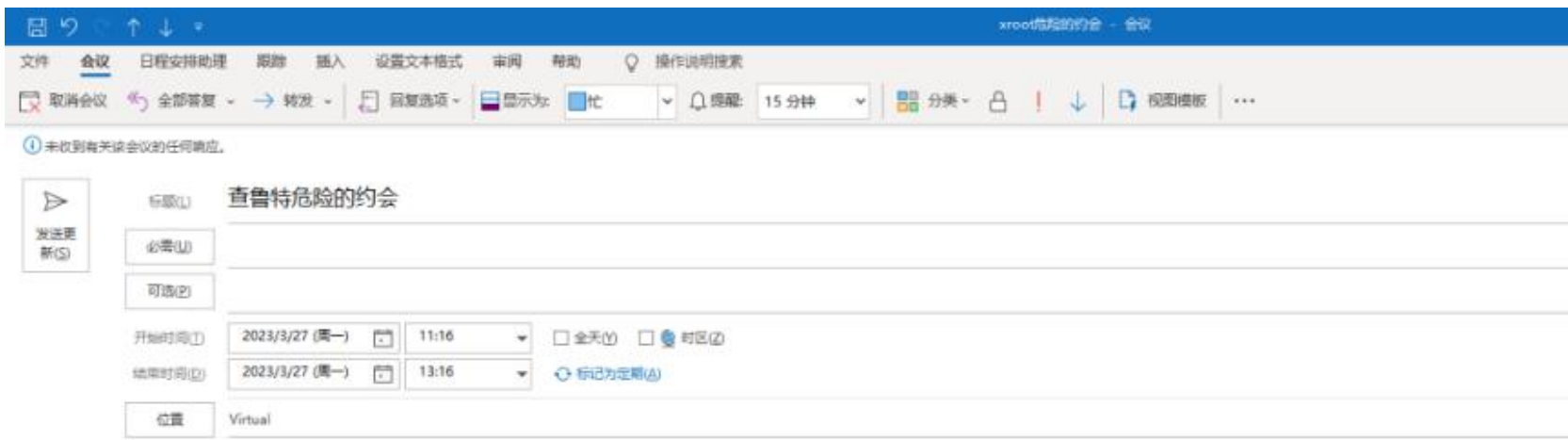


软件漏洞

运用了软件的漏洞，如下图的outlook主页滥用，因为内置低版本的IE，可以通过JS调用ACTIVEX执行命令



操作系统特性



运用了Windows两个特性

1.Windows资源管理器支持UNC-PATH
会把 **** 当成文件共享去解析

2.当访问文件共享的时候会带着当前
用户的HASH去认证

危险的约会



03

· 如何成功制作一封钓鱼邮件

如何成功制作一封钓鱼邮件

信息收集

系统的信息：

1. 目标用什么邮箱/邮件网关
2. 目标的邮箱登陆点在内网/外网
3. 目标用什么操作系统/软件
4. 目标用了什么杀毒软件/防护措施
5. 目标邮箱的配置（SPF/DMARC）
6.

有条件的建议自己搭建一套环境，
采用变量法慢慢调试

人的信息：

1. 目标可以发送的邮箱地址
2. 目标的组织架构
3. 目标的上下游/合作厂商信息
4. 目标的近况/爱好/泄露的内部文档/代码
5. 社工库是否有目标的邮箱账密/个人信息
6.

搜集一切可以收集的信息，甚至做到比目标更了解他自己

如何成功制作一封钓鱼邮件

信息收集

目标用什么邮箱/邮件网关:

域名解析查询(A/Txt/Cname/Mx/Srv/Aaaa...)

t00ls.net

Mx

立即查询

输入须知:

仅输入域名部分(可二级域名),部分查询类型比如DNS需输入顶部域名。

域名Mx记录查询结果

host	t00ls.net
class	IN
ttl	300
type	MX
pri	5
target	mxbiz1.qq.com

host	t00ls.net
class	IN
ttl	300
type	MX
pri	10
target	mxbiz2.qq.com

目标的邮箱登陆点在内网/外网:

1.在外网我们能做啥

1.1找泄露密码, 直接登陆

1.2伪造页面, 钓账号密码

1.3存在漏洞, 直接GETSHELL

1.4.....case by case

2.在内网我们能做啥

2.1.....

如何成功制作一封钓鱼邮件

信息收集

目标用什么操作系统/软件:

目标用了什么杀毒软件/防护措施:

1. Googlehacking
2. 邮件探测 (JS探测), 邮件头信息
3. 招标公告, 上下游供应商信息
4. 社工套近乎直接问
5.

谨防出现, 辛辛苦苦做了office免杀, 饶了邮件网关, 进了收件箱, 结果别人用的是WPS

```
Received: from out21-34.dm.aliyun.com (unknown [115.124.21.34])
  by bizmx41.qq.com (NewMx) with SMTP id
  for <chalute@t00ls.net>; Fri, 25 Mar 2022 16:27:38 +0800
X-QQ-SPAM: none
X-QQ-HITDIVERSE: none
X-QQ-FEAT: 6WLXEB60CfVWmtvct36lg6ldGIugnNwN/ATWaPRGGAsIpBnQsdr5ZLO/AG8uz
  Edqn9YttjX2pgv4zKpc09kReUP5LgK7uRKGJf7UmhrBhc1dtddnM2T2I8QYrGdrbzRpcy7r
  BAHhA/Ykyp8u9sLgLAk+dZuz+1B2auxZKM0QqlQneDXwiIIbYQngMlbzry/q6CWskDkVlln
  jHiQ97fs9eeuU9f5ylE3hgYoS12srZ5uqlkgoMmm1WZ1x7lrIpIGUqbKOCa+OReHuNqPz9G
  JOH/g/gqfnW6GQy09axStaua328cQQor1xux8tMT9qT2XCXiVlbqyZ/VFVz6wGin7Dppz5+
  BtGuTJ5NqQg/lyKtKIxxytvdZgkOrsDpuYTgZK4913vyqGLaGqKsRwn/jt0di3sYSOKjWjs
  xUSaB+HrSkHPpXHQ25kiIeiAtwqaD0zOavoNaSssN4=
X-QQ-MAILINFO: MRKS5XFSI5GR9FZGsH1ohv3JF/OzjIQUpOqAeK3AbYVw8e7xa0lgEcAPY
  YFCE7vNfYQ+1zBg++hnbwZkNpQmH9dXB+Rgwd35KlmpYmrYOS+gTdailBQI40+jcXfGQnEW
  jawULk2WypRRe6edmzh81gg6CNPUGyV17tI3vreNXSECz5xtghIBxGQO4cgx+CgrRKDIqrv
  ryllk
X-QQ-mid: bizmx41t1648196859tdm78fzyb
X-QQ-ORGSender: people@mail.xxxxxx
X-AltDM-RcptTo: Y2hhbHV0ZUB0MDBscY5uZXQ=
Feedback-ID: default:people@mail.xxxxxx:trigger:77434
DKIM-Signature:v=1; a=rsa-sha256; c=relaxed/relaxed;
  d=mail.xxxxxx; s=default;
  t=1648196858; h=Date:From:To:Message-ID:Subject:MIME-Version:Content-Type;
  bh=5a6AMwInruqSlEHcdJv1k+cdBQm9M/hVyTqozShVHLs;

  b=DR0o02KtPSi7gBYasAdFmDTiSSPSFbz/P2roSSXQYiJzTYSQw45CrZia2vc7reIV53WRZWB8+/valHjsf/1IiHARzFDKVwsYySbcHmUDj
  HWOJZiZrUOyNyfyOsPe3hQ6Cy6YtcSq/mOow5YE=
Received: from localhost (mailfrom:people@mail.xxxxxx fp:SMTPD_----1Iu5Lde)
  by smtpdm.aliyun.com (127.0.0.1);
  Fri, 25 Mar 2022 16:27:38 +0800
Date: Fri, 25 Mar 2022 16:27:38 +0800
From: "=?UTF-8?B?5a2X6IqC6Lez5YqoIEJ5dGVEYW5jZQ==?" <people@mail.xxxxxx>
Return-Path: "=?UTF-8?B?5a2X6IqC6Lez5YqoIEJ5dGVEYW5jZQ==?" <people@mail.xxxxxx>
To: <chalute@t00ls.net>
Reply-To: <people@mail.xxxxxx>
Message-ID: <b992b341-45a2-4ade-988c-2aec3e1319b6.people@mail.xxxxxx>
```



如何成功制作一封钓鱼邮件

信息收集

目标邮箱的配置 (SPF/DMARC)

前面也说了SPF的配置不严谨或者没配置可能导致发件人伪造的问题，DMARC也是一样。SPF是规则，DMARC是策略。

简单解释一下就是：当不满足SPF规则的时候，这封邮件是进垃圾箱还是拒收是DMARC配置的

```
C:\Users>
C:\Users>nslookup -q=txt t001s.net
服务器:  UnKnown
Address:  10.9.255.1
```

```
非权威应答:
t001s.net      text =

      "ca3-1268c7d3ec3949e689389f4d86818dce"
t001s.net      text =

      "v=spf1 include:spf.mail.qq.com ~all"
```

```
C:\Users>nslookup -q=txt spf.mail.qq.com
服务器:  UnKnown
Address:  10.9.255.1
```

```
非权威应答:
spf.mail.qq.com text =

      "v=spf1 include:qq-a.mail.qq.com include:qq-b.mail.qq.com include:qq-c.mail.qq.com include:biz-a.mail.qq.com include:biz-b.mail.qq.com include:biz-c.mail.qq.com include:biz-d.mail.qq.com -all"
```

```
C:\Users>nslookup -q=txt qq-a.mail.qq.com
服务器:  UnKnown
Address:  10.9.255.1
```

```
非权威应答:
qq-a.mail.qq.com      text =

      "v=spf1 ip4:101.226.139.0/25 ip4:101.91.43.0/25 ip4:101.91.44.128/25 ip4:112.64.237.128/25 ip4:116.128.173.0/25 ip4:121.51.40.128/25 ip4:121.51.6.0/25 ip4:162.62.52.214 ip4:162.62.55.67 ip4:162.62.57.0/24 ip4:162.62.58.211 ip4:162.62.58.216 -all"
```

```
C:\Users>
```

■ 如何成功制作一封钓鱼邮件

话术/手法定制

各分中心：

根据《2019年人事考核方案》，总部已完成19年年终绩效考核制定，请全体员工于**2019年12月23日**之前完成年终绩效考核，以便您的考核人能及时完成反馈。

温馨提示：

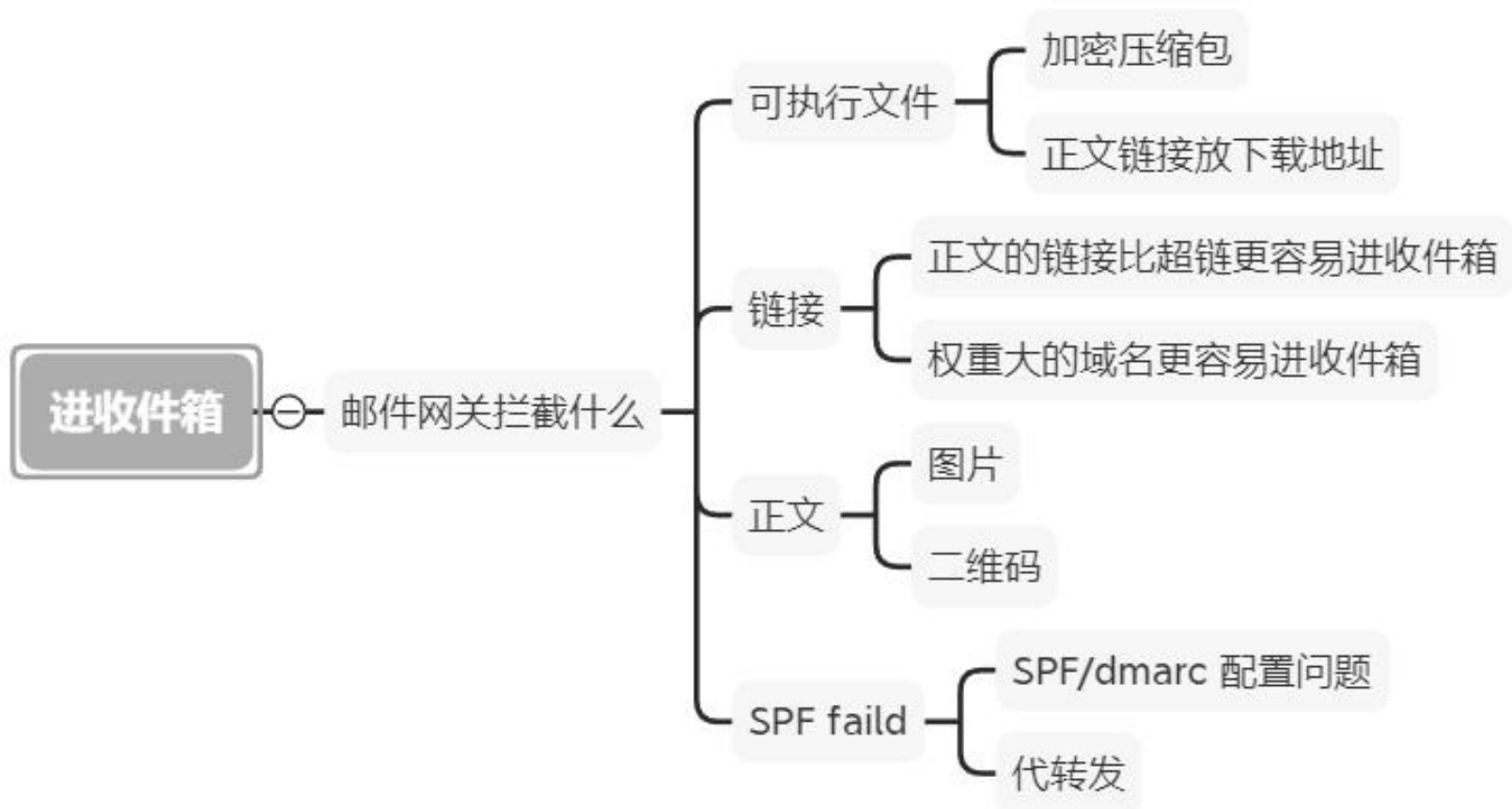
- 1.请根据最新制定的《2019年年终绩效考核标准制定》进行制定，如果逾期可能会影响到**年终的排名及年终奖发放**。
- 2.总结逾期提交处罚方式（最终以集团后期发文为准）：逾期1次，口头批评；逾期2次，书面批评；逾期3次，通报批评；逾期4次及以上，警告；以上所有处罚录入系统，不扣薪，应用于评优及晋级。
- 3.评分标准如附件，如果文档显示空白或者格式有错，请点击启用内容。

另请各分中心务必高度重视，持续改善人事基础工作的准确性、合规性。我们将持续通报检查情况，如有任何问题及建议，请随时沟通。

 如何成功制作一封钓鱼邮件

话术/手法定制

防御措施的绕过



如何成功制作一封钓鱼邮件

链接

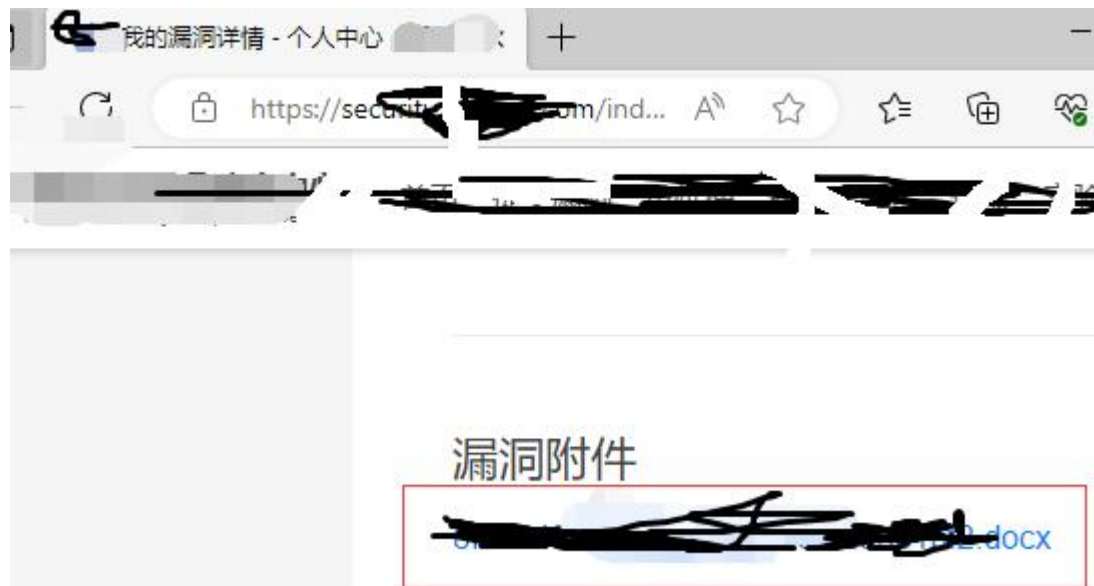
正文链接比超级链接更容易进收件箱



权重大的域名更容易进收件箱

常见利用姿势:

- 1.302跳转
- 2.文件附件



钓鱼邮件积分制

积分制是我自己定义的一个概念，灵感来自于杀软。当我们写的木马/可执行文件触发哪些会导致杀软告警，如自启动，写注册表，发起网络连接，连接的地址是否是恶意地址等。

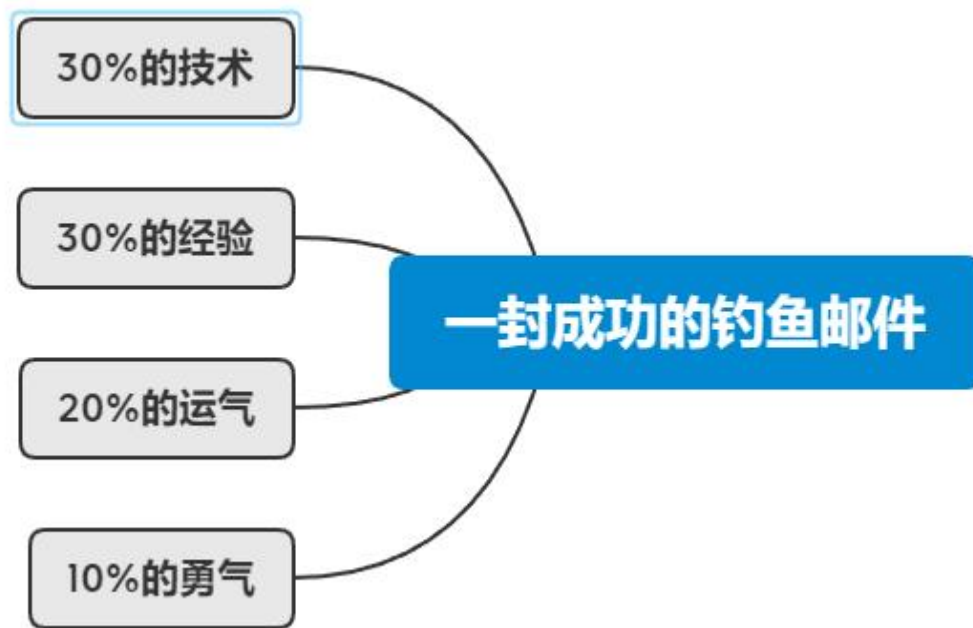
钓鱼邮件同理：比如SPF failed，附件是未压缩的可执行文件这种就很难进收件箱，甚至垃圾箱都进不去。

邮件积分制可以见：
<https://mp.weixin.qq.com/s/7NuJQMGOrq2EnB-7yOmkig>

邮件内容	举例	分值
是否过SPF	不过SPF会根据策略直接拒收或者进垃圾箱	10
是否带DKIM	同SPF但是因为DKIM有缺陷，强策略配置的不多	5
发件人是否可信IP	看具体配置跟白名单一样	5
是否代转发	代转发来自不可信域直接垃圾箱	5
发件人的邮箱域名	可信度:tencent.com>qq.com>自建域名	3
邮件正文内容	正文内容是否合法，一般为了防垃圾邮件	3
是否带可疑附件	正常附件>加密附件>恶意附件	3
邮件是否带可疑链接	链接可信度:google.com>ba idu.com>恶意链接	3
收发件域是否相似	发件人:baidu.com 收件人:ba1du.com 这样会被拦截	3
发件频率	发件频率快会被拉黑	2
是否使用别名	如把别名设置为admin	1



■ 写在最后



一次真实的案例：

经过信息收集，目标具有以下特性：

- 1.外网没有任何网站，连静态页面都没
- 2.有强劲的杀软和安全措施
- 3.定期做安全培训，有较强的安全意识
- 4.外网只有一个泄露的邮箱，是个财务
- 5.泄露邮箱的主人查不出任何信息，甚至不知道性别
- 6.尝试给对方发信（图片探测），拿到IP发现对方的物理位置在XXX局，XXX局是搞安全的

经过详细的信息收集发现目标太强了，这时候就有些纠结了，要不要给对方发钓鱼邮件，毕竟成功率太低了，如果失败，不仅会引起目标的警觉，而且自己的免杀马就是送样本。背后思虑半天最终还是选择付诸行动，当然这次运气比较好，结果是可喜的，同时也是戏剧性的。

■ 写在最后

第一天:财务上线,因为杀软原因没做自启动, 财务上线2分钟后掉线

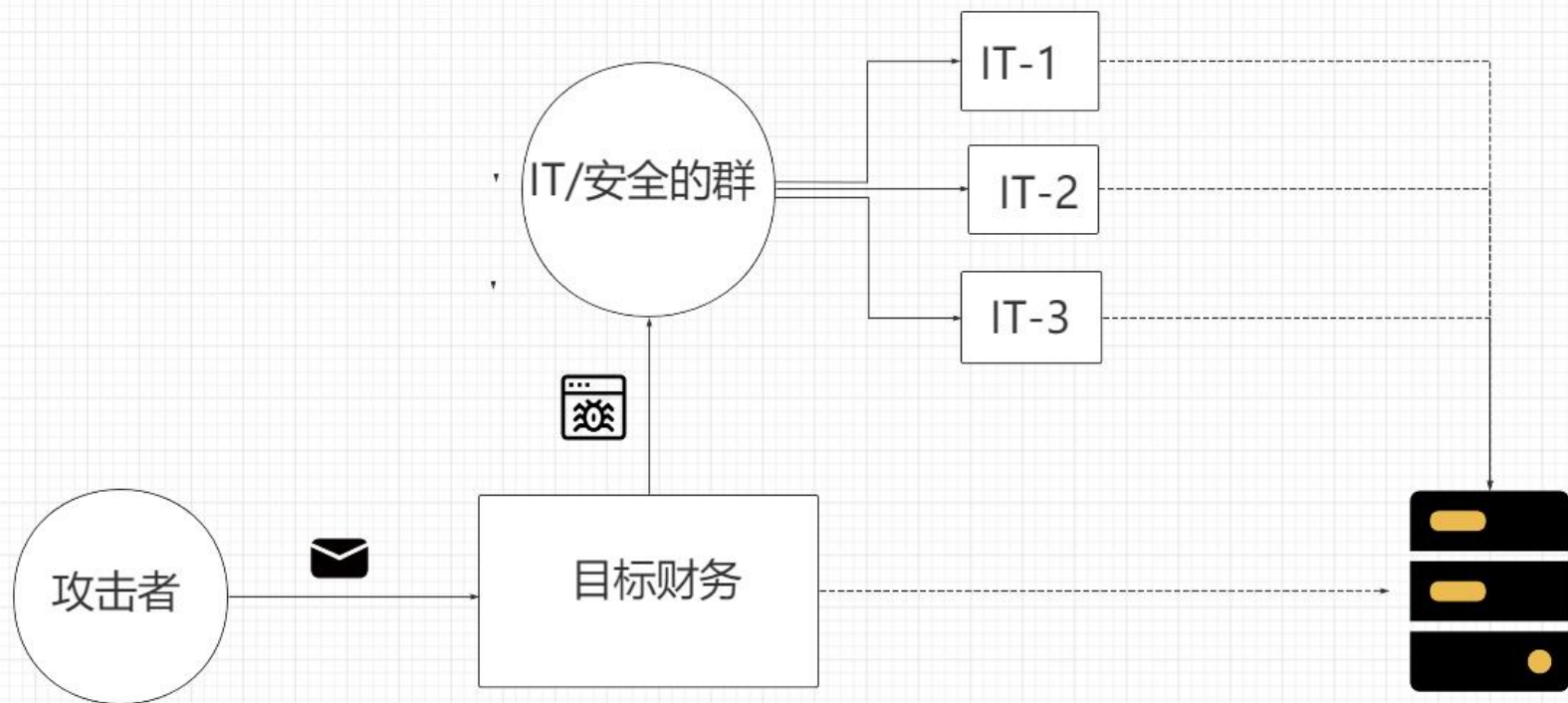
第二天:上线三台机器, 以为是沙箱, 过了一会发现心跳包是持续的, 确认为真人上线

第N天:打穿内网, 拿下IM的权限
发现聊天记录, 还原了上线的过程

1.财务收到邮件并运行, 觉得不妥
关闭后发送给IT排查

2.IT把样本扔到IT和安全的群里,
安全把样本扔virustotal, 发现几乎没有报红, 给出无威胁的判定

3.然后应该好奇心驱使下, 三个IT都
点击了该样本, 背后财务接着上线





感谢您的观看

主讲人：查鲁特

时间：2023.07