钓鱼邮件攻击防范应对指南

国家计算机网络应急技术处理协调中心

2022 年 9 月

目录

一、 编写目的

为防范和应对钓鱼邮件攻击事件，保护关键信息基础设施的网络和信息系统安全，指导相关单位科学开展事前防范、事中处置和事后恢复，特制定本指南。

二、 基本概念

“网络钓鱼”是上世纪 90 年代中期兴起的一种网络诈欺行为，其中最主要的攻击手段就是“钓鱼邮件”。1996 年首先在美国发现，后迅速扩散到其他国家和地区。近几年，“钓鱼邮件”攻击在我国呈现逐年上升，最常见的一种方式是：攻击者预先制作一个以假乱真的钓鱼网站，然后通过在电子邮件中植入钓鱼网站链接，引诱人们点击进入以假乱真的网站，骗取用户名、密码、个人信息等重要数据，或植入木马等恶意程序，从而导致遭受重大损失。该攻击方式往往包含社会工程学信息，欺骗性很强，人们很容易上当受骗。那么，什么是钓鱼邮件?如何识别钓鱼邮件?中招了怎么办?

（一）什么是钓鱼邮件

钓鱼邮件是指攻击者伪装成同事、合作伙伴、朋友、家人等用户信任的人，通过发送电子邮件的方式，诱使用户点击嵌入邮件正文的恶意链接或者打开邮件附件的恶意程序，进而窃取用户敏感数据、个人银行账户、邮箱账户和密码等信息，或者在设备上执行恶意代码以实施进一步的网络攻击活动。

（二）钓鱼邮件的危害

钓鱼邮件通过隐含的恶意链接或附带的恶意程序，窃取用户重要个人信息或政府企业敏感信息，可能造成直接或间接经济损失，甚至危害国家安全。

三、钓鱼邮件主要攻击方式

攻击者通过钓鱼邮件达成攻击目的主要有两种方式，第一种通过冒充权威机构或者与收件人有关联系人发送邮件，降低收件人戒心，提高打开钓鱼邮件可能性；第二种通过利用社会工程学或者暴力破解方式直接获得目标收件人邮箱账号凭据，之后收集目标收件人邮箱信息。

从攻击手法来看，钓鱼邮件前期需要对目标收件人进行信息收集，通过社会工程学引导，利用人性弱点，提高收件人对钓鱼邮件的信任度，诱导收件人点击钓鱼邮件中的恶意附件或恶意链接。

（一）通过社会工程学提高信任度

钓鱼邮件常常通过伪装身份发送电子邮件的方式进行，其伪装的身份包括但不限于：上级领导或上级单位、组织的信息网络管理人员、同事、有工作往来的其他组织的人员、银行、社保服务等外部服务，其目的主要是为了骗取收件人的信任，使其相信邮件内容的真实性，并按照邮件内容进行操作，从而达到其目的。如下图所示，其伪装成系统管理员骗取收件人的信任：

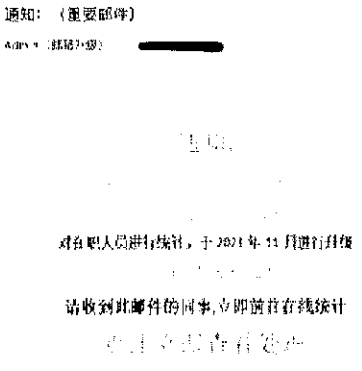


图 1 伪装成系统管理员的钓鱼邮件

钓鱼邮件会通过话术，进一步引导收件人填写内容。如下方钓鱼邮件，主题为“纪检委：通知”，邮件附件打开后显示一个表格，但是内容非常模糊无法识别，文档下方提示“如看不清图片内容请复制链接到浏览器登录查看详情”，进一步引导用户复制钓鱼链接打开恶意网站，从而达到收集用户账户密码的目的。

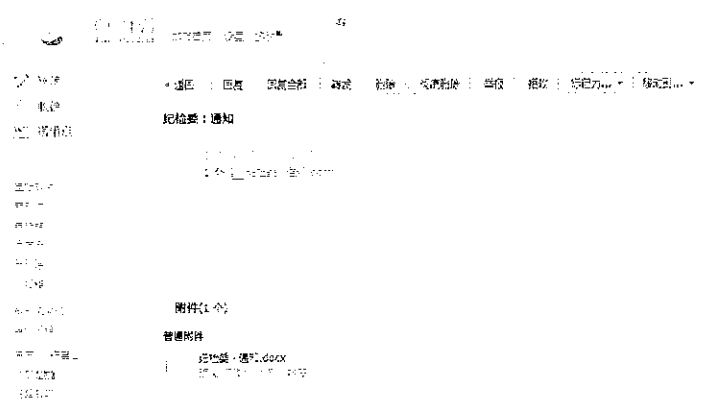


图 2 冒充纪检委通知的钓鱼邮件

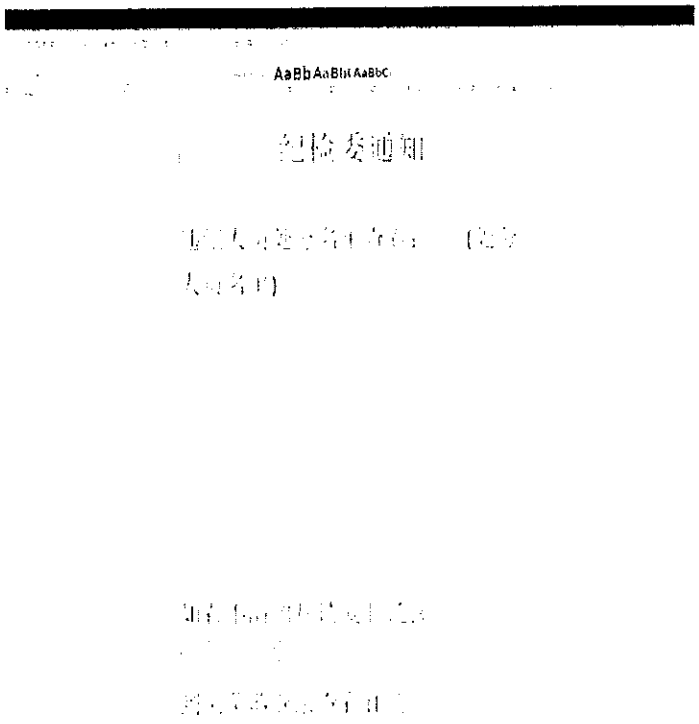


图 3 某钓鱼邮件正文

攻击者还可能利用普通人对个人信息保护观念的缺失和人性弱点进行诱导。如给老年人发打折促销返券链接，给信用卡用户发提升额度或兑奖链接等。如图是主题为“【财政部】关于发布年终最新工资补贴通知”的钓鱼邮件（如图3），通过使用具有吸引力的“补贴”为主题，利用用户对金钱的重视，达到攻击目的。

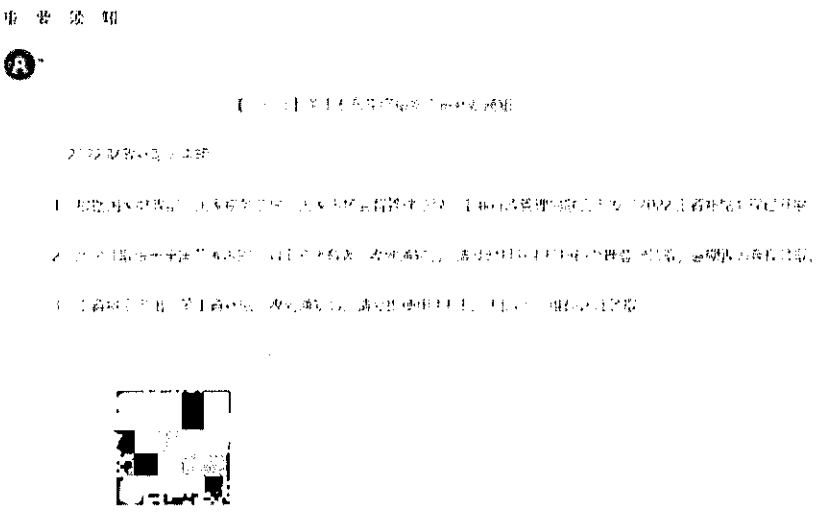


图 4 利用二维码掩饰钓鱼链接

收件人扫码后，就会跳转到钓鱼页面，诱导用户填写银行卡号、身份证号、手机号等敏感信息，攻击者之后会利用这些信息发起转账请求，通过受害者输入银行发来的验证码，攻击者就可以完成相关的转账操作，成功实施诈骗。

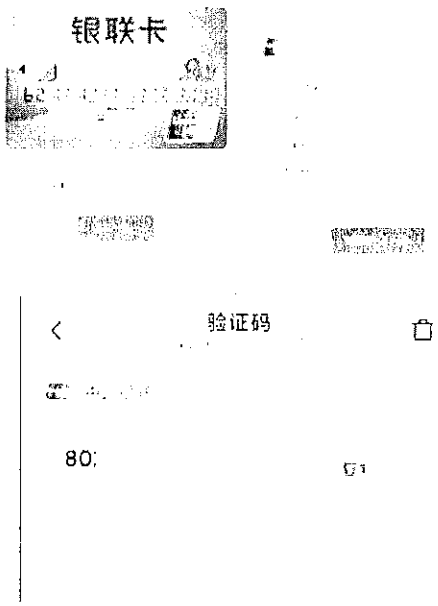


图 5 钓鱼页面收集受害人银行卡验证码

钓鱼邮件主题和内容还会限定事件时间、数量，从而制造紧迫感，引导收件人回复或参与活动，如“紧急通知”、“前100名3折先到先得”、“报名时间截止XX，过时不候”、“在X点前完成密码重置”等等。

图5钓鱼邮件以“紧急通知”为主题，并警告用户如果不按要求进行操作账号将不能使用，制造事件的紧迫感，压榨收件人谨慎思考的时间，促使收件人迅速采取行动。如果收件人点击钓鱼邮件正文中的“升级审核”，将会跳转至攻击者特制的钓鱼页面，从而收集用户的相关账号凭据，对用户造成损失。

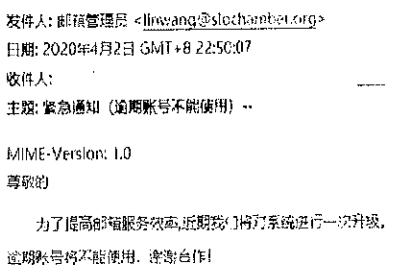

发件人: 邮箱管理员 <linwang@slechamber.org>
日期: 2020年4月2日 GMT+8 22:50:07
收件人:
主题: 紧急通知（逾期账号不能使用）
MIME-Version: 1.0
尊敬的
为了提高邮箱服务效率,近期我们将对系统进行一次升级，请在收到通知的第一时间，进行升级审核(一个工作日内完成)
逾期账号将不能使用，谢谢合作!

图6钓鱼邮件利用话术引导受害者点击

（二）利用第三方信誉降低受害者戒心

钓鱼邮件通常会伪装成具有公信力的第三方机构，以此降低用户戒心。例如冒充国家机构、公信机构（公安、公积金中心、社保中心、银行、购物网站等）；冒充官方机构的机构（如大学生对考研、公务员培训、资格认证、简历求职等方向有需求）；冒充管理方（如企业内邮箱管理员、邮箱

服务商等）。钓鱼邮件还会通过伪装或爆破某个人邮箱给熟人发钓鱼邮件，例如伪装成目标用户的领导、朋友、亲人、客户等等。或者通过直接获取目标收件人有关联系人的邮箱账号，借此发钓鱼邮件，降低收件人的戒心，从而达到攻击目的。

图 6 的钓鱼邮件伪装为具有公信力的机构，并在正文内容使用“最后”、“终止”等字眼，试图通过制造紧迫感来促使收件人采取行动，如果点击钓鱼邮件正文内容中的选项，将跳转至恶意网页，攻击者将对用户信息进行收集。

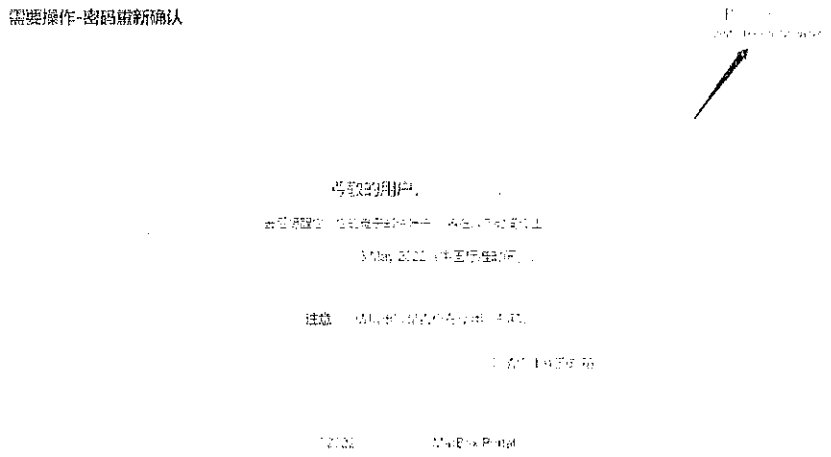


图 7 钓鱼链接利用话术引导受害者点击

图 7 钓鱼邮件首先使用“电邮安全警报”标题，提高收件人阅读的紧迫感，其次冒充电子邮件服务商，降低用户防备心。在邮件中要求用户在 24 小时内回复，如果未经验证，将关闭收件人电子邮件账户，制造事件紧迫感，促使收件人迅速对邮件做出回应。如果点击钓鱼邮件正文链接，则会跳

转至钓鱼网页，并被要求输入账号密码，从而达到窃取目标用户账号目的。

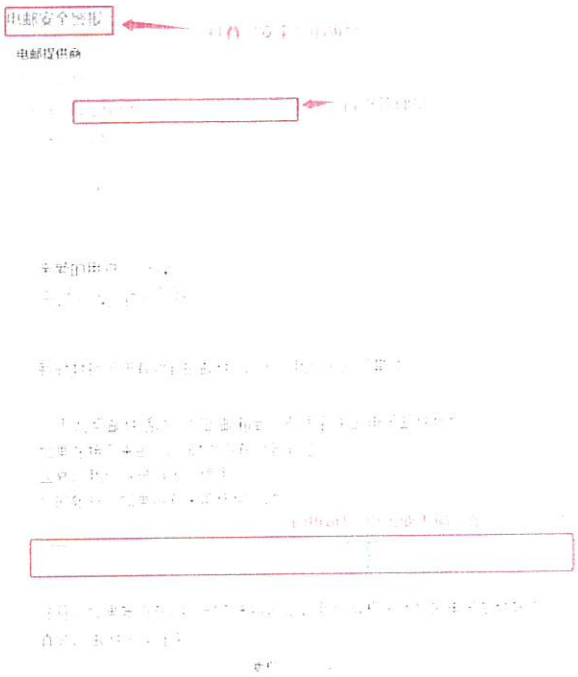


图 8 钓鱼邮件冒充电邮提供商

（三）攻击者攻陷上游管理方

上游管理机构一般都有安全方案和安全措施，但由于其特殊性，也有成为攻击者目标的可能性，虽然目前这种案例数量并不多，但造成的危害更大。如果目标账户上游管理方被攻击沦陷，也可能被利用来发送钓鱼邮件，例如：公司邮件服务器沦陷，邮箱服务商沦陷，DNS 解析服务器沦陷等，攻击者直接利用沦陷账号发送钓鱼邮件，就能更加容易达到其攻击目的。

四、主要攻击技术和目的

（一）邮件正文插入恶意链接

攻击者会在邮件中插入恶意链接，等待收件人点击恶意链接。恶意链接可能是一个简单的恶意程序下载入口，或者是伪造的网页（比如与已知网站类似、但拼写略有差别的超链接）等。有些攻击者会对邮件内容进行精心构造，在邮件正文中混杂官方合法的资源链接和恶意的虚假链接，从而避开垃圾邮件过滤器的筛选，骗取收件人的信任。如下图所示：

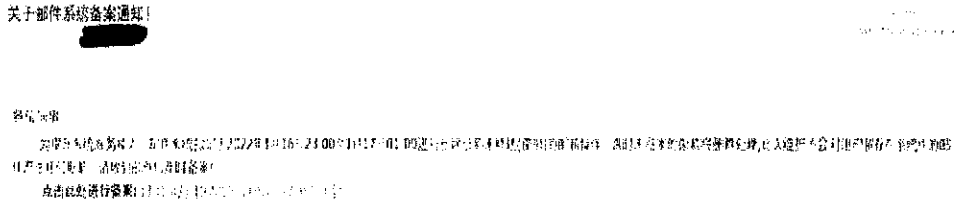

关于邮件系统备案通知[redacted]

图 9 邮件正文中插入链接

（二）邮件附件隐藏恶意程序

这是一种比较常见的钓鱼邮件攻击方式，尤其如今垃圾邮件过滤不断升级，攻击者更多地会选择在邮件附件中隐藏木马，从而实现非法目的。攻击者将木马程序隐藏在邮件附件中，一旦收件人出于无意或者好奇打开附件就会运行木马，导致数据泄露或者其他后果。攻击者常用的附件类型有文档（word、ppt、excel 等）、图片（gif、png 等）、压缩包（zip、rar 等）、脚本程序（vbs、bat 等）等，而且一般都会使用超长文件名隐藏后缀，从而规避邮箱安全机制的过滤。其中，

利用 word 文档宏代码调用 PowerShell 执行恶意程序安装进程比较常见，而 zip 等压缩包通常用来对恶意软件进行隐藏，从而避开邮件沙箱或者杀毒软件的直接查杀。

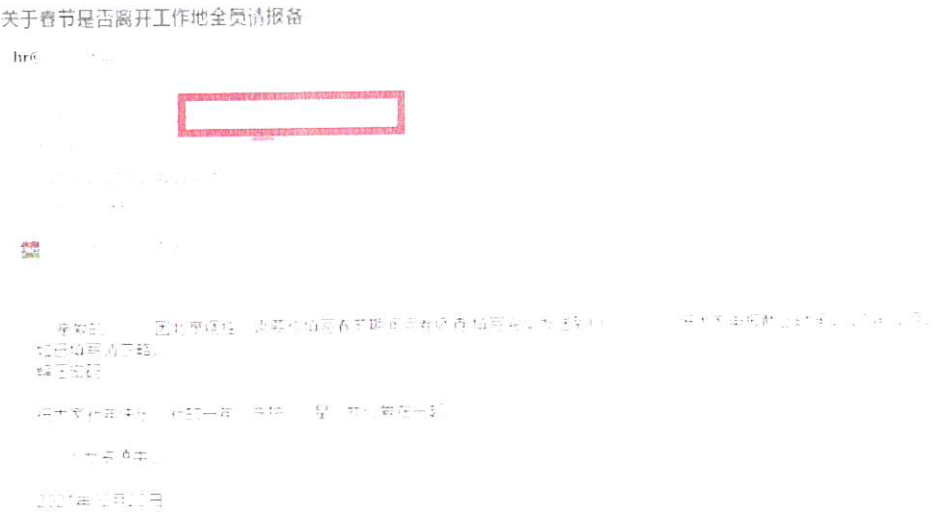


图 10zip 压缩包类型恶意邮件附件

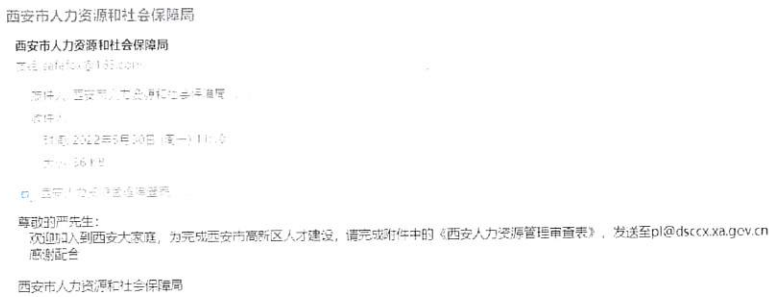


图 11 含有 word 宏病毒的钓鱼邮件

（三）利用软件漏洞攻击

钓鱼邮件攻击中比较常见的一种攻击方式，常用的漏洞包括浏览器漏洞、Office 漏洞以及系统漏洞。攻击者在邮件正文中嵌入包含漏洞利用代码的链接地址，或者邮件附件中隐藏漏洞利用代码，用户一旦点击漏洞利用链接地址或漏洞利用附件，则可能触发漏洞利用代码执行，后续下载僵尸木

马、窃密木马等恶意程序。

例如，Gamaredon 组织针对于乌克兰政府人员发起的钓鱼邮件攻击，样本名称为 Сводка 20.06.2021 роз.docx，攻击方式为 word 文档模板注入，在打开 word 文档时就会回连控制命令服务器下载恶意代码。

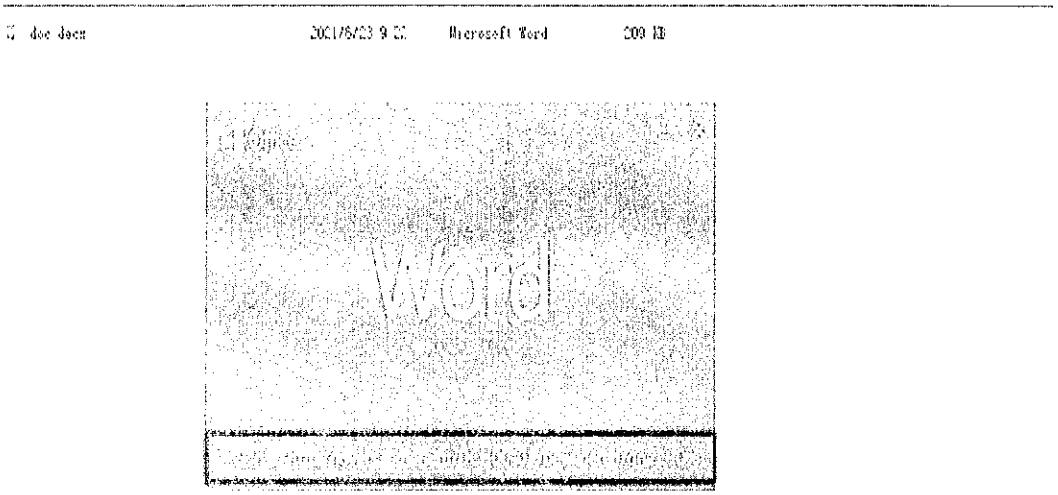


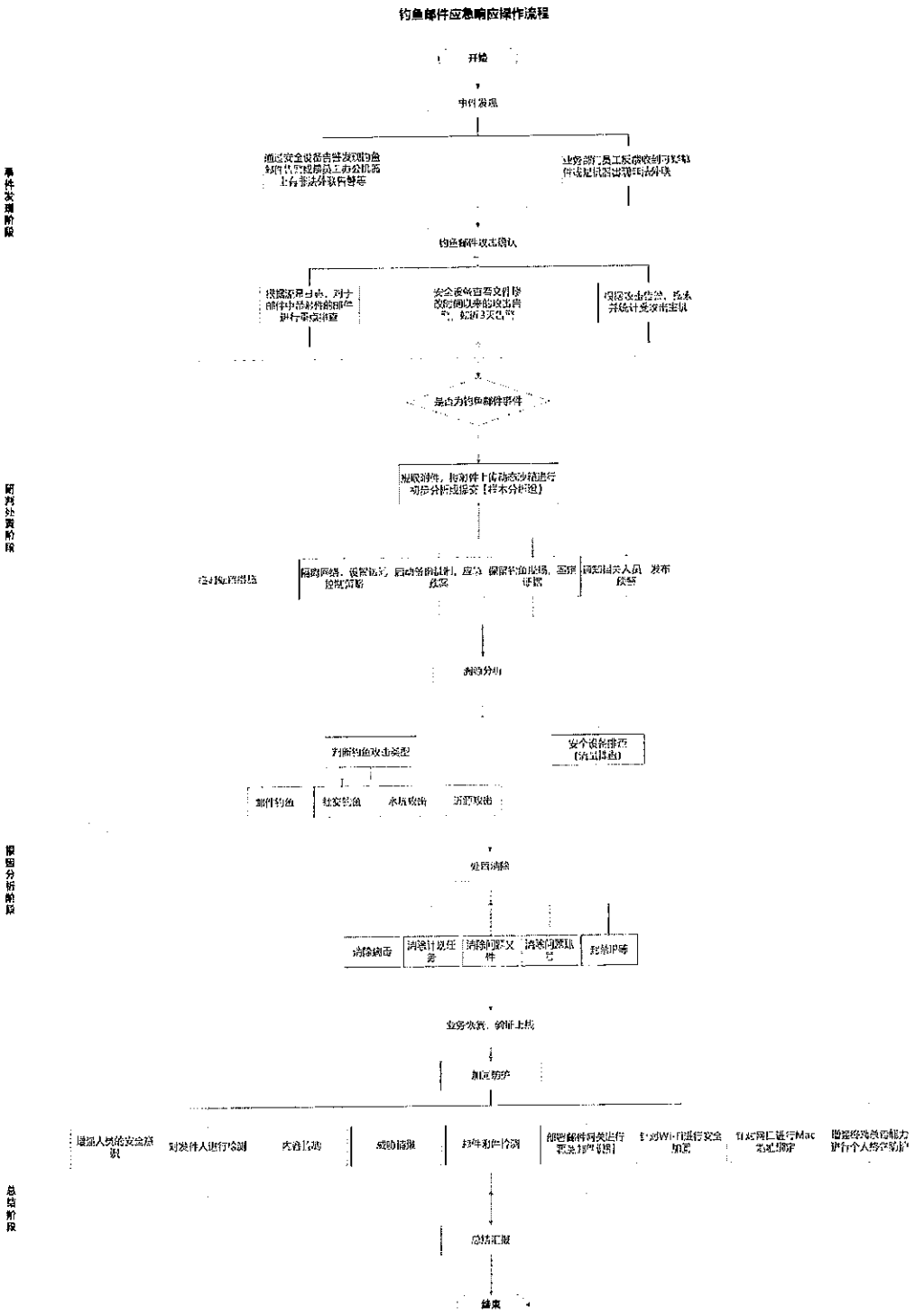
图 12 含有浏览器漏洞链接的钓鱼邮件

（四）寻找高价值目标发送钓鱼邮件

攻击者一旦获得邮箱的访问权限，就会获取邮箱内的通讯录，向其中特定单位的邮件地址或者向全部邮件地址发送钓鱼邮件，利用已攻陷的邮箱作为跳板发送钓鱼邮件更具有欺骗性和诱导性。例如某公司人事部门邮箱沦陷后，通过这个邮箱向全公司发送钓鱼邮件，或针对性地发送钓鱼邮件给管理层或投资人等，其成功率大大增加。

五、钓鱼邮件攻击应急响应流程

钓鱼邮件攻击的应急响应主要流程如下图所示：



（一）确认受到钓鱼邮件攻击

可采用以下方式初步研判是否受到钓鱼邮件攻击：

1. 对邮件中的跳转链接进行研判，是否为仿冒网页，诱

骗受害者点击。例如，在邮件页面按 F12，通过网页元素判断链接地址是否是正确链接，通过和官方发布的地址进行对比即可判断是否是仿冒钓鱼页面。对于可疑的网站可以在威胁情报平台(国内主流威胁情报平台见**错误!未找到引用源。**)查询。

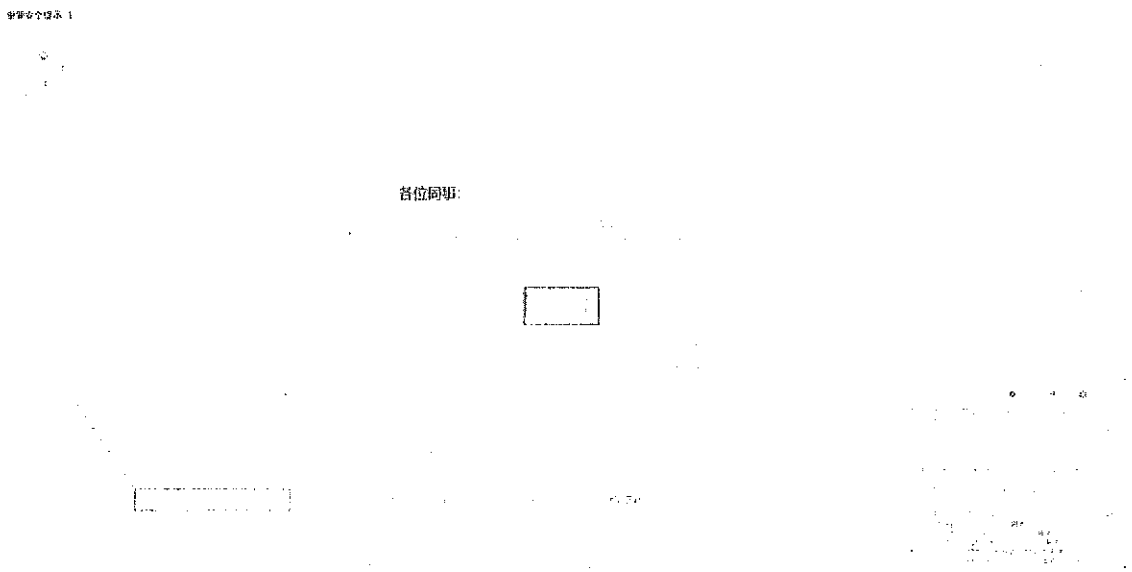


图 13 查看邮件页面链接地址

2. 将钓鱼邮件附件或是邮件中下载链接中的文件，上传到动态分析沙箱进行初步分析。常见的动态分析沙箱列表如下：

表 1 常见动态分析沙箱列表

名称	地址	公司
奇安信威胁情报中心	[redacted]	奇安信
微步在线云沙箱	[redacted]	微步
安恒威胁分析平台	[redacted]	安恒

钓鱼邮件的目的是为了帮助攻击者获取钓鱼目标的个

人隐私信息，包含用户敏感数据、个人银行账户、信息系统的账户、密码等信息，或者在目标设备上执行恶意载荷实施进一步的网络攻击活动，如果个人邮箱或者目标主机等信息设备出现了以下特征，则可能受到了钓鱼邮件的攻击。

1.索要隐私信息或诱导访问陌生站点

钓鱼邮件会通过社会工程学等手段，了解目标邮件的基本情况，通过伪造目标的领导，上级，同事，或者伪装为某些机构的官方人员，利用一定的社工话术诱导目标发送隐私信息或诱导访问黑客构造的非官方网站获取目标的信息。

如收到标题为某银行信用卡中心提示用卡异常，在邮件正文中出现需要回复个人信用卡信息，身份信息等，或诱导客户点击链接填写个人信用卡账号，手机号，身份证等信息。

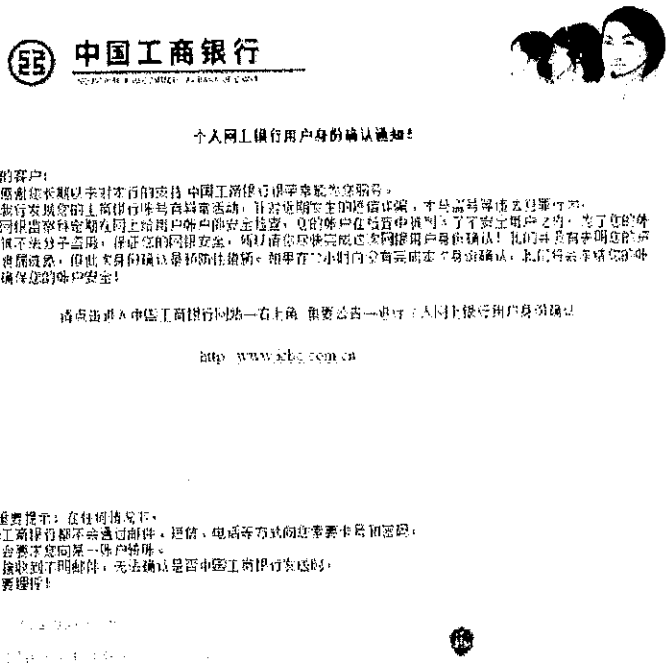
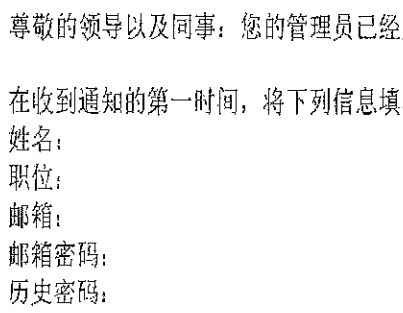


图 14 信用卡异常钓鱼短信

如收到了署名为某网站发送标题为系统升级，系统维护，安全信息设置等名义的邮件，并在邮件内容中要求目标回复个人隐私信息或诱导点击填写个人隐私信息。


尊敬的领导以及同事：您的管理员已经启动"邮箱搬家"，这将助于邮箱升级。

在收到通知的第一时间，将下列信息填写完毕回复本邮箱!
姓名：
职位：
邮箱：
邮箱密码：
历史密码：

图 15 伪装成系统升级的钓鱼邮件

有如上情况的可以基本确认，目标收到了钓鱼邮件，诱导目标泄露个人的隐私信息。

2. 下载邮件附件或点击链接后出现异常

钓鱼邮件攻击会通过邮件附件或者恶意链接伪装成合法信息，通过一定的话术诱导目标进行点击，下载，从而造成目标的信息丢失或系统故障，攻击者还可以利用客户端或者操作系统的漏洞直接植入远程控制或窃密木马。出现以下情况的，需警惕用户或者组织遭受到钓鱼邮件攻击。

（1）下载邮件附件或点击邮件中链接后，系统出现故障，如 CPU 突然占用过高，文档类资源无法打开等异常情况。

（2）目标向组织内投递了非目标本人意愿发送的邮件，或者目标所在组织内出现了一定范围的系统、网络故障等异常情况。

（二）隔离设备，保留证据

1. 网络隔离

切断受感染设备的网络连接（拔掉网线或者禁用网络），避免网络内其他设备被感染渗透，使安全事件范围得到控制，防止敏感文件被窃取，降低安全事件带来的损失。

2. 修改密码

邮箱的登录密码可能已经泄露，应在另外的机器上及时修改密码，防止攻击者获取邮箱中的邮件、联系人等敏感信息，遏制黑客进一步的攻击渗透。同时建议修改与邮箱相关联的用户名，密码，以免造成其他信息泄露或财产的损失。

3. 通知相关人员、发布预警

联系到可能受到影响的人员，避免受到类似的钓鱼邮件侵扰。安全管理员向单位发布全员预警通知。

4. 保留钓鱼现场

隔离相关设备和网络后，执行保留现场的操作，提取目标邮件的信息，包含邮件的内容、标题、发件人、发送时间、附件、链接、发送钓鱼邮件的 IP 等信息，获取可能的钓鱼链接源码或者数据，留存当前设备的内存镜像，不要进行任何的修改操作，以免造成后续分析的误差。**建议直接将钓鱼邮件导出为 eml 格式的存档文件。**

5. 设置访问控制策略

在防火墙等网络设备上封禁钓鱼攻击中使用的恶意链

接或 IP，关闭 3445、139、135 等不必要的端口。详细方法请见附件 1。

（三）钓鱼邮件事件分析

1.分析钓鱼方式、目的

根据前面确认的信息与提取的数据，分析黑客钓鱼的方式是利用仿冒网站或话术诱导目标进行信息的填写，造成数据泄露，还是利用 office,客户端，操作系统漏洞进行漏洞攻击，或者利用下载附件然后点击文件，释放恶意载荷导致受到恶意攻击。

在确定黑客钓鱼攻击的方式后，进一步分析钓鱼网站源码，恶意载荷附件，目标系统环境，通过提取的信息，查找可能已经泄露的数据，通过威胁情报平台关联相关域名，文件等 IoC 信息。

表 2 国内部分威胁情报平台

序号	威胁情报平台地址	名称
1	https://ti.360.cn/	360 威胁情报平台
2	https://ti.dbappsecurity.com.cn/	安恒威胁情报中心
3	https://ti.qianxin.com/	奇安信威胁情报中心
4	https://www.venuseye.com.cn/	启明星辰 VenusEye 威胁情报中心
5	https://ti.nsfocus.com/	绿盟 NTI 威胁情报中心

6	https://www.asiainfo-sec.com/product/detail-14.html	亚信安全运营与态势感知平台中的威胁情报中心

查找可疑文件，判断其是否恶意同时判断恶意载荷生成的时间，将提取的文件通过在线沙箱进行动态分析，最后通过上述信息，分析黑客是为了窃取隐私数据，还是为了其它目的，抑或是网络攻击，是否针对特定地区或目标进行钓鱼。

2.上报机构内部网络安全部门

发现钓鱼邮件攻击后，收集相关信息（主要为 eml 格式的钓鱼邮件），上报机构内部网络安全部门。同时，建议联系专业应急响应团队或者专业安全机构团队进行处置。

3.检查系统，分析攻击路径

针对收集的线索进行具体的溯源分析，确认攻击者行为路径，主要将从以下几个方面排查，该部分工作需要较为专业的知识，建议联系专业应急响应团队或者专业安全机构团队寻求技术协助与支持。

（1）邮件头信息分析

很多钓鱼邮件事件会伪造邮件发件人地址，让受害者放松警惕，通过对邮件头信息的查看，可以获取邮件发送的真实 IP、邮件网关等信息。

对邮件头中的信息进行分析提取，提取信息头中的 IP、网关、邮箱地址等信息，可以利用威胁情报平台对相关的信

息进行查询甄别。

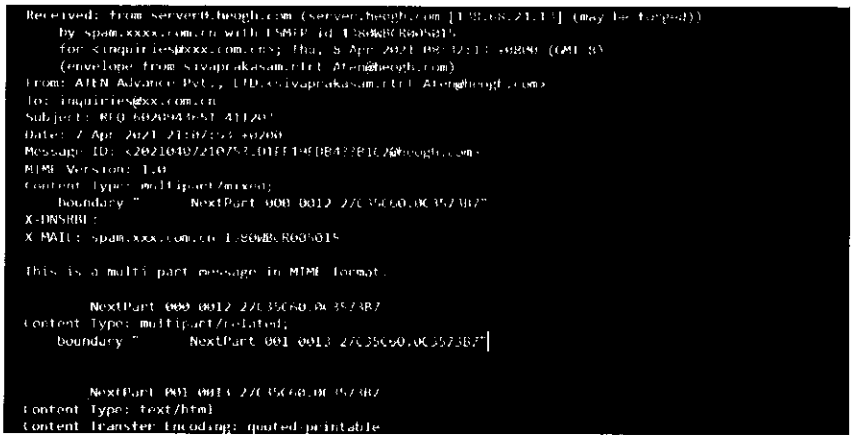


图 16 钓鱼邮件头源码

（2）邮件内容分析

对邮件的内容进行分析，判断邮件中是否包含诱骗点击的链接、下载地址或是邮件中包含附件的解压密码等信息。排查正文中的跳转链接是否为仿冒网站的诱骗链接。

对邮件中包含的点击链接，在虚拟机中使用无痕浏览模式进行访问，对跳转的链接的域名、IP 及页面源码进行甄别，是否存在被仿冒。

对邮件中存在的下载地址，在虚拟机中进行下载，并对下载的地址及附件进行分析，IP 和附件的哈希值（MD5、SHA1 或 SHA256）可以在公开的威胁情报平台进行威胁查询，进一步溯源攻击者信息。

（3）邮件附件分析

对邮件中的附件进行分析，分析样本的关键动作，记录样本的回连 URL、域名、IP 地址。

可以使用公开的威胁情报平台（见**错误!未找到引用源。**）中的文件分析功能进行样本快速分析研判工作。

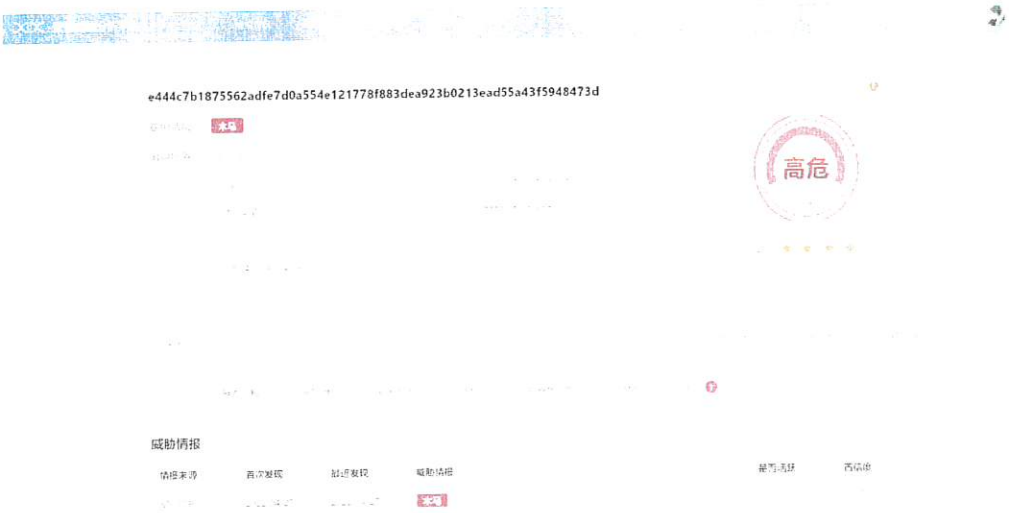


图 17 威胁情报平台中的文件分析功能

如果样本自动化分析功能的分析结果信息未能达到要求，可以反馈专业样本分析团队对样本进行人工分析。

（4）社交钓鱼分析

攻击者通常伪装成求职者、人力资源、客户等角色，从互联网招聘平台筛选薄弱目标，获取具体联系方式后引流至微信、钉钉等社交工具，诱导对方上线，向其发送包含带木马的文件，或以短链接、网盘地址等形式发送包含恶意程序的链接，诱导对方点击。有的攻击者还可能伪装成目标甲方技术服务人员，实施电话诈骗，骗取 VPN 或系统账号密码、验证码等信息。

通过分析平台（包含流量类设备、主机防护等）排查针对被攻陷目标主机的告警信息，并搜索存在同样告警的其它主机，以此作为推断条件判断可能被攻陷的主机。

（5）日志分析

对于已经被钓鱼邮件攻陷的主机可以使用应急采集工具对主机日志进行采集，自动收集分析所需数据，提高工作效率；发现攻击者留下的其他痕迹，利用公开或专业的分析平台快速定位异常，生成攻击链。

常见的日志采集工具：

工具名称	工具描述
Logstash	一个数据收集器，将各种格式各种渠道的数据收集解析之后格式化输出到 Elasticsearch
Filebeat	一个轻量级的日志传输工具
Fluentd	Fluentd 是一个免费，而且完全开源的日志管理工具，简化了日志的收集、处理、和存储
Logagent	Logagent 是 Sematext 提供的传输工具，它用来将日志传输到 Logsene(一个基于 SaaS 平台的 Elasticsearch API)
rsyslog	绝大多数 Linux 发布版本默认的 syslog 守护进程，rsyslog 可以将日志从 syslog socket 读取并写入 /var/log/messages 。它可以提取文件、解析、缓冲(磁盘和内存)以及将它们传输到

	多个目的地，包括 Elasticsearch 。
Autoruns	用于显示在 Windows 启动或登录时自动运行的程序。
Everything	一款文件搜索工具。
PCHunter	一款功能强大的 Windows 系统信息查看软件。
ProcessExplorer	Windows 系统和应用程序监视工具。
ProcessMonitor	一款系统进程监视软件。
Sysmon	微软团队出品的一款日志搜集工具。
TCPView	查看端口和线程的小工具。

（6）攻击链梳理

针对如上的排查分析得到的线索进行梳理，按时间排序，将攻击路径进行还原，形成溯源分析报告，为业务恢复和安全加固提交依据。

4.寻求外部技术支持

被攻击单位可联系专业应急响应团队或者专业安全机构团队寻求技术协助与支持。

单位	网站	电话	电子邮件
国家互联网应急中心（CNCERT）	www.cert.org.cn	010-82990999	cncert@cert.org.cn
北京鸿腾智能科技有限公司	https://lesuobingdu.360.cn/		
北京安天网络安全技术有限公司	https://vs.antiy.cn/	400-840-9234	support@antiy.cn
杭州安恒信息技术股份有限公司	bbs.dbappsecurity.com.cn	4006059110-3	4006059110@dbappsecurity.com.cn

深信服科技股份有限公司	bbs.sangfor.com.cn	400-630-6430 转 6	
奇安信科技集团股份有限公司	https://www.qianxin.com/	95015	
北京神州绿盟科技有限公司	https://user.nsfocus.com/hm_wechat/hm_Robot/webchatNsfocus.html	400-818-6868 转 4	irs@nsfocus.com
北京天融信网络安全技术有限公司	http://www.topsec.com.cn/	400 777 0777	cssc@topsec.com.cn
恒安嘉新（北京）科技股份公司		010-59437722	
亚信安全	https://www.asiainfo-sec.com/	010-82166688	

（四）风险处置和安全加固

1.风险处置

可以通过手动或使用杀毒工具清除病毒，但由于很多恶意载荷可能会在系统多个位置释放样本，并通过多种方式设置自启动，手动杀毒很可能处理不完全，建议优先使用杀毒工具清除，手动清除病毒仅供了解和参考。

2.安全加固

分析掌握攻击方式之后，待恢复系统后，需要对设备进行安全加固，防止类似的网络攻击再次发生。

（1）部署邮件安全监测和检测技术手段

对发件人进行检测，加强对伪造发件人攻击的检测能力，可以设置 SPF、DKIM、DMARC，具体设置方法见附件 2。

部署邮件网关进行恶意邮件识别；邮件附件检测，对邮

件中的附件进行沙箱等安全分析检测。邮件内容检测，基于邮件的内容进行检测，检测内容中是否包含常用的钓鱼邮件关键字及恶意链接；使用威胁情报，基于威胁情报，对钓鱼邮件的 IP 及域名进行检测。

产品名称	公司名称	官网地址	联系方式
奇安信网神邮件威胁检测系统	奇安信科技集团股份有限公司	https://www.qianxin.com/product/detail/pid/406	95015
信桅深度威胁邮件网关	亚信安全	https://www.asiainfo-sec.com/product/detail-24.html	

（2）个人终端加固

增强个人终端防护水平，安装杀毒软件，并将病毒库更新进最新，有条件的单位可以部署终端检测与响应平台（EDR）、端点防护平台（EPP）、下一代终端安全保护平台（NGEP）等专业防护产品。

（3）检查系统漏洞

检查操作系统存在的漏洞情况有两种方式：一是使用漏洞扫描设备，对设备进行扫描获取系统的漏洞情况；二是在系统中手动检测，使用 cmd 输入命令 systeminfo 查询系

统补丁安装情况，已打的补丁序号是 KB 开头的。

图 18systeminfo 查询系统补丁安装情况

表 3 漏洞扫描工具列表

名称	下载地址	备注
AWVS	https://www.acunetix.com/	收费、免费两个版本
APPScan	https://www.hcltechsw.com/products/appscan	收费、免费
Nikto	https://github.com/sullo/nikto	免费
OpenVAS	https://www.openvas.org/	免费
Xray	https://xray.cool/	免费

Nessus	https://www.tenable.com/products/nessus	个人免费 商用收费

（五）上报主管部门

发生重要钓鱼邮件攻击事件后，涉事单位应按照国家相关规定向行业主管部门以及网信部门、公安部门及时、如实报告事件有关信息，不得瞒报、谎报或缓报。上报事项包括但不限于：单位名称、报告人、联系方式，事件定级、事件发生时间、事件发生地点、事件简要描述、事件影响范围、事件造成的危害、事件发生的原因、已采取的措施和效果、需要有关部门和单位协助的相关事宜等。

六、防范措施和方法

钓鱼是一种基于社会工程学的体系化攻击方式，通常以钓鱼邮件、钓鱼页面（或钓鱼网站）的形式进行部署。与之相对，防范策略也应该是体系化的应对策略。

（一）钓鱼邮件防范建议

1. 区分工作和生活邮件，分别设置高强度密码

将工作和生活邮箱分开，邮箱密码分别设置，采用中、高强度的密码。按照不同使用目的，有效控制邮箱的使用范围。防止邮箱地址大范围泄漏。

2. 安装并开启终端防护软件。

安装并开启相应的终端防护软件，对每一封邮件及其附

件进行安全查杀。定期更新终端防护软件病毒库。

表 4 部分终端防护软件列表

序号	终端防护软件	官方地址
1	360 安全卫士个人版 v13.0	https://weishi.360.cn
2	360 安全卫士中小企业版	https://ent.online.360.cn
3	金山毒霸	https://www.ijinshan.com/
4	天融信终端威胁防御系统	http://edr.topsec.com.cn/
5	亚信安全防毒墙网络版 v16	https://www.asiainfo-sec.com/download/

3. 谨慎打开邮件，关闭客户端自动下载附件功能。

打开邮件之前对邮件标题进行判断，涉及敏感关键词的邮件主题，打开之前利用安全防护软件进行邮件查杀。对于所使用的邮件客户端，关闭自动下载附件功能。

邮件主题敏感关键词包括：OA 通知、管理员通知、人力（或人事）通知、重要提醒、代办事项、Post Master 邮件退信、邮件异常、新冠疫苗接种注意事项、工资补贴、参会名单、历届会议回顾、通知、采购单、订单、会议日程、升级安装包、系统管理员、紧急通知、账户异常、密码过期、账户重置、信用卡账单、XX 系统紧急通知、工作补贴、退税补贴、高温补贴、紧急备案、立即执行等。

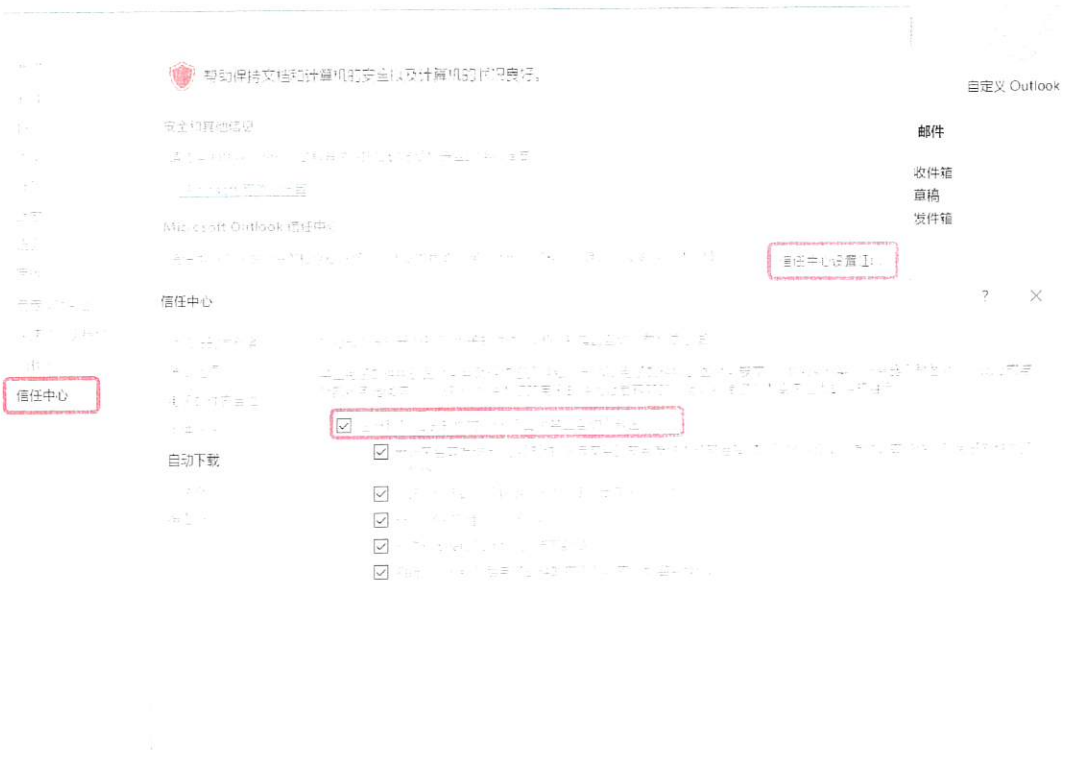
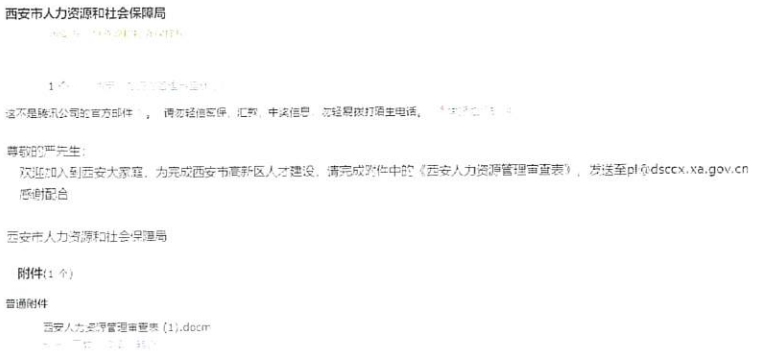


图 19 关闭 Outlook 自动下载功能

4. 仔细核对发件人地址，不轻信“显示名”。

收信时对发件人地址进行检查，遇到陌生发件人或显示为某国家机关、部门等地址时，不轻信“显示名”。对显示某某地址代发的邮件，通过“查看邮件源代码”功能，查看实际发件人地址。对未知发件人的邮件不查看、不点击文中链接，不下载邮件附件。


西安市人力资源和社会保障局

这不是腾讯公司的官方邮件。请勿轻信密保、汇款、中奖信息，勿轻易拨打陌生电话。

尊敬的严先生：

欢迎加入到西安大家庭，为完成西安市高新区人才建设，请完成附件中的《西安人力资源管理审查表》，发送至pl@dsccx.xa.gov.cn

感谢配合

西安市人力资源和社会保障局

附件(1 个)

普通附件

西安人力资源管理审查表 (1).docm

图 20 伪装成政府机构“显示名”的钓鱼邮件

5. 理性判断邮件正文内容，不轻易点击其中的链接。

对邮件的正文内容进行理性判断，不轻信其内容；对于制造紧张气氛、索要密码或个人隐私信息等内容的邮件，通过公开搜索引擎或电话进行事件二次确认。对于正文内存在的链接，切勿轻易点击。

（二）钓鱼网站防范建议

1. 对来源不明的链接和附件不点击不打开

对于任何邮件、短信、即时消息中来源不明的链接和附件不点击不打开。

2. 输入重要信息前确认网站安全性

凡是要求输密码登录的页面，必须确认页面地址（URL）尤其是主域名的安全，查看其网站证书是否合法有效。

正常页面，可以通过浏览器查看证书文件，且证书文件状态为“该证书没有问题”。

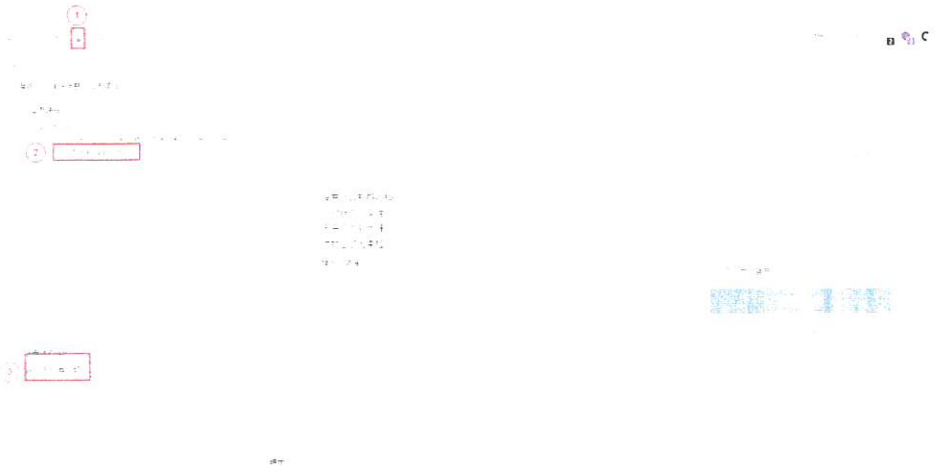


图 21 正常页面证书查看方式

钓鱼页面由于没有 CA 颁布的证书文件所以浏览器会提

示不安全。

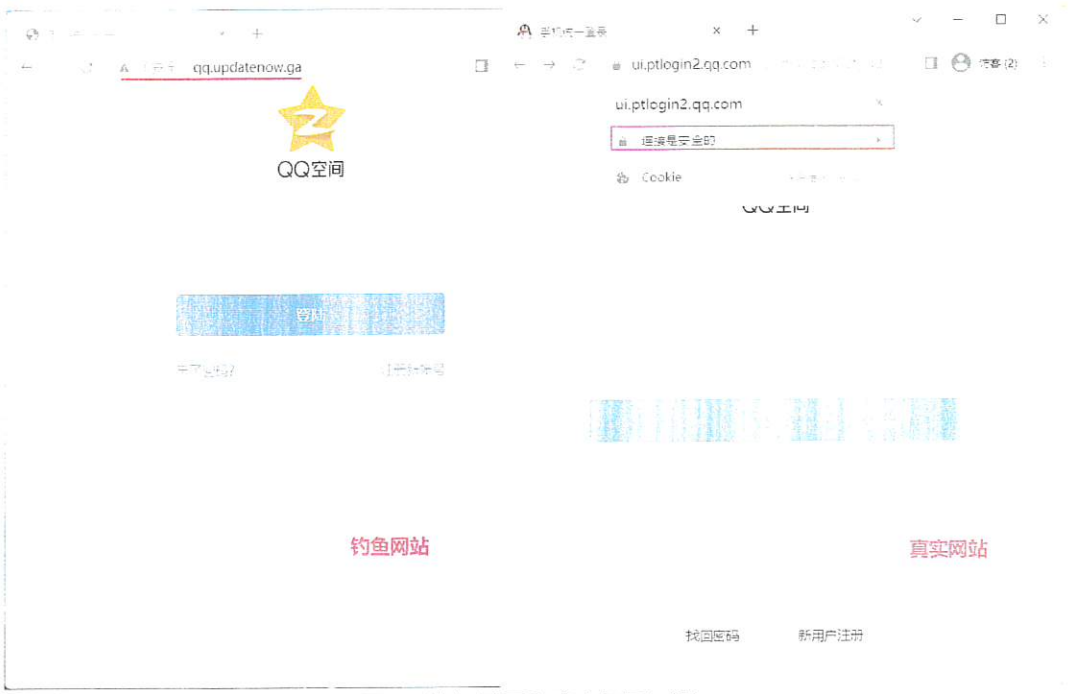


图 22 钓鱼页面和真实页面对比

3. 安装终端安全防护软件

安装或开启终端防护软件，对浏览器的访问地址进行实时安全过滤。

4. 定期检查本机 HOSTS 文件

定期检查本机 hosts 文件，确保文件内容不被篡改，对文件中的 IP 和对应域名进行安全确认，删除所有可疑条目。

表 5hosts 文件位置

系统类型	host 文件位置
Windows	C:\Windows\System32\drivers\etc\hosts
Linux	/etc/hosts

5. 配置可信的 DNS 服务器

接入任何网络后，首先对 DNS 服务器地址配置进行确认，

手动配置可信的 DNS 服务器地址（如：223.5.5.5）不使用来源不明的DNS服务器地址。国内部分公开可用的DNS服务器列表如下：

表6 国内部分公共DNS服务器列表

序号	DNS服务器地址	单位
1	114.114.114.114	114DNS
2	114.114.115.115	114DNS
3	123.125.81.6	DNS 派
4	101.226.4.6	DNS 派
5	218.30.118.6	DNS 派
6	223.5.5.5	阿里
7	223.6.6.6	阿里
8	180.76.76.76	百度
9	119.29.29.29	DNSPod
10	1.2.4.8	中国互联网网络信息中心
11	202.38.64.1	中国科技大学

6. 访问可疑页面或链接时进行手动检查

访问可疑页面或来源不明的链接时，可通过浏览器调试功能（F12 可快捷打开当前浏览器的调试工具，对于笔记本电脑，按 Fn+F12 可快捷打开调试工具），对页面元素进行手动检查。通过搜索官方页面，进行页面元素对比，识别钓鱼页面。

例如：在钓鱼页面中，按 F12 通过页面元素发现页面登录账号标签为 id="username"：

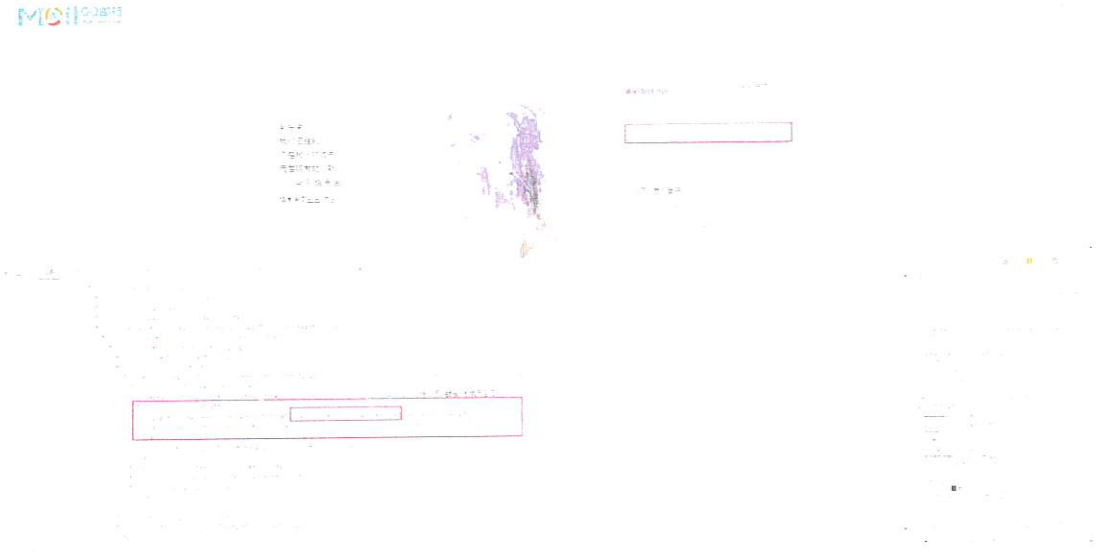


图 23 钓鱼页面元素查看

而在官方页面中，按 F12 通过页面元素发现页面登录账号标签为 id="u"：

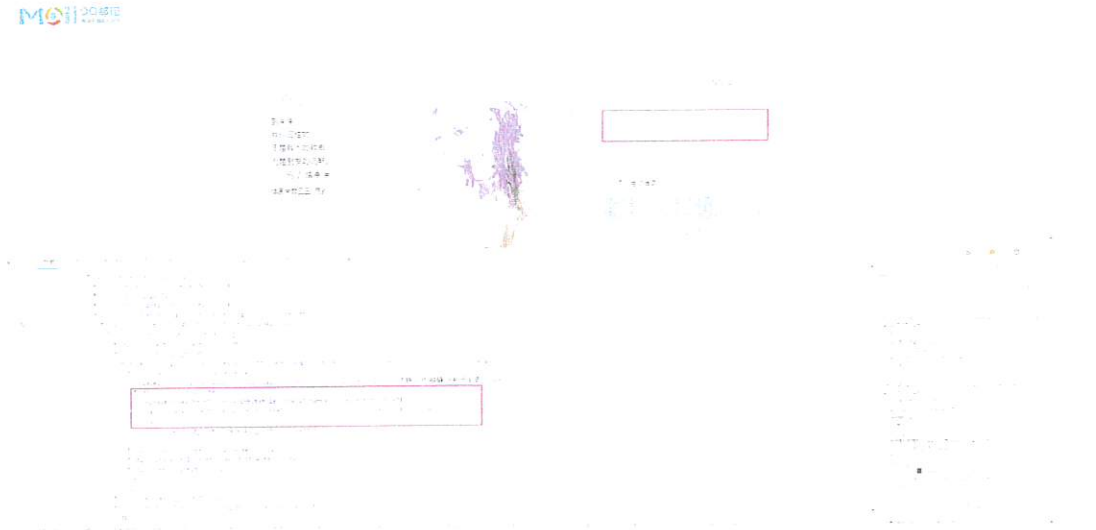


图 24 官方页面元素查看

7. 登录网站出错或失败后及时联系官方客服

在登录出现错误或多次输入密码并登陆失败后及时搜索官方页面修改账号密码或拨打官方客服电话冻结账号，防

止密码泄露账户被控。

（三）安全意识教育培训

1.安全意识测评

通过模拟真实的网络钓鱼、社工攻击等，对单位员工进行网络安全意识特别是对网络钓鱼防范意识的测试，对人员安全意识整体情况、安全意识薄弱环节进行摸底。

2.安全意识培训

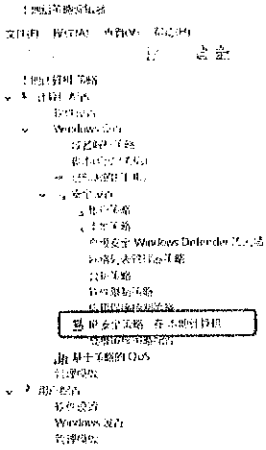
通过攻击原理和过程演示、防范措施和注意事项讲解等方式，开展对员工的安全意识培训，促使员工建立对钓鱼邮件等社工攻击的防范意识。

附件 1 Windows 主机上关闭 135、139 等端口

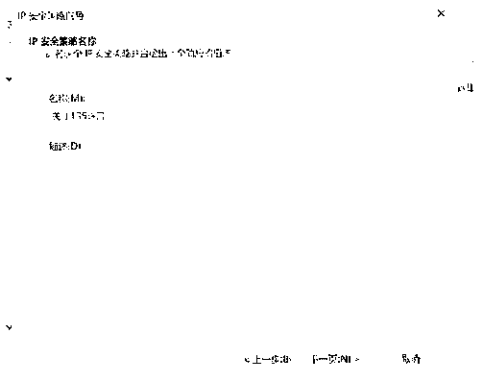
Windows 主机上关闭 135、139 等端口

方式一：通过 IP 安全策略（以关闭 135 端口为例）

(1) 在“开始”菜单选择“运行”，输入“gpedit.msc”后回车，打开本地组策略编辑器。依次展开“计算机配置—windows 设置—安全设置—ip 安全策略，在 本地计算机”



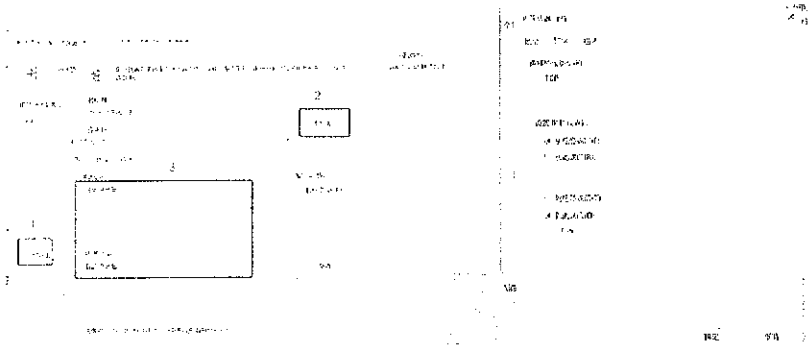
(2) 右键单击鼠标，选择“创建 IP 安全策略”，弹出 IP 安全策略向导对话框，单击下一步；在出现的对话框中的名称处写“关闭端口”（可随意填写），点击下一步；对话框中的“激活默认响应规则”选项不要勾选，然后单击下一步；勾选“编辑属性”，单击完成。



(3) 在出现的“关闭 135 端口 属性”对话框中，选择“规则”选项卡，去掉“使用添加向导”前边的勾后，单击“添加”按钮.

(4) 在弹出的“新规则 属性”对话框中，选择“IP 筛选器列表”选项卡，单击左下角的“添加”

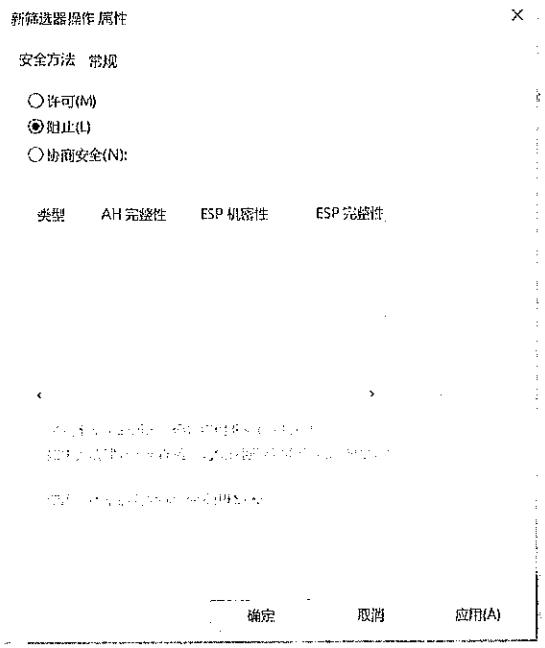
(5) 在出现的“IP 筛选器 属性”对话框中，选择“地址”选项卡，“源地址”选择“任何”，“目标地址”选择“我的 IP 地址”； 选择“协议”选项卡，各项设置如图片中所示。设置好后点击“确定”。



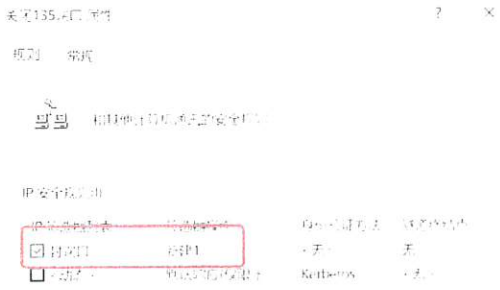
(6) 返回到“ip 筛选器列表”，点击“确定”。返回到“新规则 属性”对话框

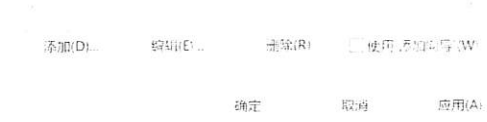
(7) 在 ip 筛选器列表中选择刚才添加的“封端口”，然后选择“筛选器操作”选项卡，，去掉“使用 添加向导”前面的勾，单击“添加”按钮

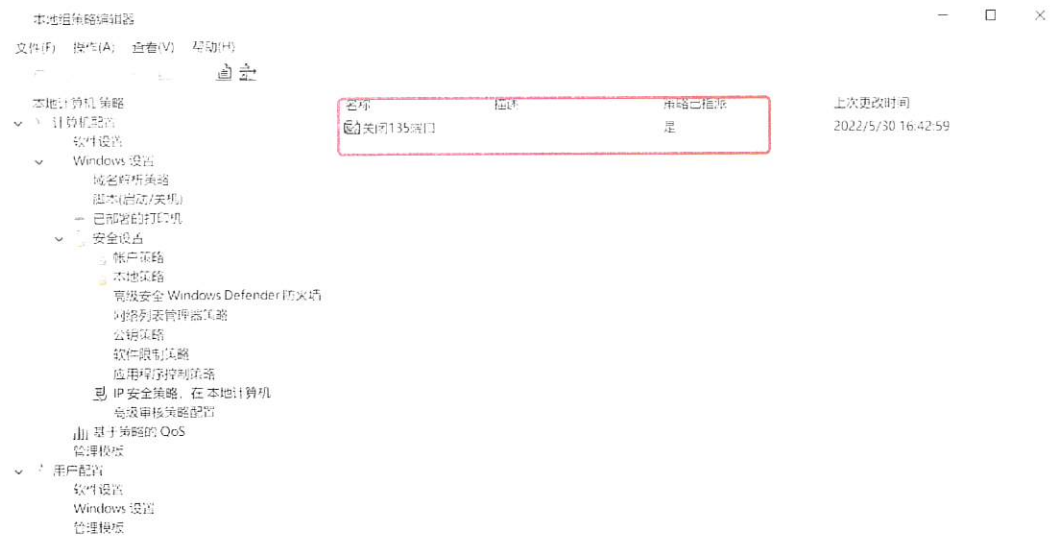
(8) 在“筛选器操作 属性”中，选择“安全方法”选项卡，选择“阻止”选项；在“常规”选项卡中，对该操作命名，点确定



(9) 在组策略编辑器中，可以看到刚才新建的“关闭 135 端口”规则，选中它并单击鼠标右键，选择“分配”选项，使该规则开始应用！到此完成。






本地组策略编辑器
文件(F) 操作(A) 查看(V) 帮助(H)
本地计算机 策略
计算机配置
软件设置
Windows 设置
域名解析策略
脚本(启动/关机)
已部署的打印机
安全设置
帐户策略
本地策略
高级安全 Windows Defender 防火墙
对等列表管理器策略
公钥策略
软件限制策略
应用程序控制策略
IP 安全策略，在 本地计算机
高级审核策略配置
基于策略的 QoS
管理模板
用户配置
软件设置
Windows 设置
管理模板
名称
描述
策略已指派
上次更改时间
关闭135端口
是
2022/5/30 16:42:59

附件 2 SPF、DKIM、DMARC 设置方法

SPF、DKIM、DMARC 设置方法

1. SPF 设置

SPF, 全称 Sender Policy Framework, 即发件人策略框架。SPF 是为了防范伪造发件人地址发送垃圾邮件而提出的一种开放式标准, 是一种以 IP 地址认证电子邮件发件人身份的技术。

为您的域配置 SPF 很容易。前往您域的控制面板，找到设置 DNS 记录的部分，然后添加新 TXT 记录。写入一个有效的 SPF 字符串作为值并保存您的记录。

SPF 记录支持多种白名单令牌:

- ip4: 123.123.123.123 – 允许指定的 IPv4 地址。
- ip6: abcd: 1234: 90ab: cdef: 5678: 90de: fabc – 允许指定的 IPv6 地址。
- a: example.com– 允许 DNSA 记录给出的 IP 地址 example.com。
- mx: example.com– 允许由 DNSMX 记录之一给出的 IP 地址 example.com。
- include: example.com– 查询该域的 SPF 记录，除直接定义外，还使用其白名单。简化流行的第三方电子邮件服务的集成。

- redirect:example.com– 忽略其他令牌并使用 example.com.

您可以通过向标头添加多个令牌来组合多个来源:

v=spf1 ip4:123.123.123.123 include:example.com ¯al

2.设置 DKIM

DKIM 使用加密来启用服务器身份验证。设置 DKIM 需要生成公钥和私钥对。公钥会添加到您域的 DNS 记录中。

私钥保密并成为邮件服务器配置的一部分。该软件将使用此密钥对其发送的每封电子邮件进行签名。当接收服务器收到新邮件时，它会查询域的 DKIM DNS 记录并使用公钥来检查电子邮件是否被篡改。

设置 DKIM 的确切步骤将因您使用的邮件传输代理而异。这是一个如何让它与 Postfix 一起工作的例子:

Install OpenDKIMimplementationsudo apt install opendkimopendkim-tools# Add the Postfix user to the OpenDKIMgroupsudogpasswd -a postfix opendkim

打开/etc/opendkim.conf 并取消注释或添加以下行:

Canonicalization relaxed/simpleModesvAutoRestartyesAutoRestartRate 5/1HSignatureAlgorithm rsa-sha256UserID opendkim

这将 OpenDKIM 配置为用作传出邮件的签名者和传入消息的验证者。这是您要设置的内容:

- Canonicalization– 定义 OpenDKIM 在验证传入电子邮件是否已被篡改时的严格程度。默认是 simple 不允许修改。这通常会导致合法电子邮件丢失，因为中间邮件服务器稍微修改过的消息(例如通过调整空格或行长度)将被丢弃。relaxed/simple 允许更多非关键差异。
- Mode– 启用签名 （s） 和验证 （v） 模式。
- AutoRestart 以及 AutoRestartRate– 失败时重新启动，前提是一小时内重新启动次数不超过五次。
- SignatureAlgorithm – 对传出消息进行签名时使用的加密算法。

接下来将以下额外行添加到文件中:

```
# Maps domains to the keys used to sign emailsKeyTable
refile:/etc/opendkim/key.tableSigningTable
refile:/etc/opendkim/signing.table# Ignore these
hosts when verifying incoming
signaturesExternalIgnoreList
/etc/opendkim/trusted.hosts# Internal hosts to enable
outgoing mail signing forInternalHosts
/etc/opendkim/trusted.hosts
```

保存并关闭配置文件。接下来创建上面引用的映射文件:

sudomkdir /etc/opendkimsudomkdir

/etc/opendkim/keyssudochown -R opendkim:opendkim

/etc/opendkimsudochmod go-rw /etc/opendkim/keys

/etc/opendkim/trusted.hosts

先创建:

127.0.0.1localhost*.example.com

这指定来自本地地址或您的域的电子邮件已经受信任。

打开/etc/opendkim/signing.table 并添加以下内容:

*@example.com default._domainkey.example.com

这会指示 OpenDKIM 从任何 example.com 地址发送的消息都应使用 default._domainkey.example.com 密钥进行签名。

现在打开/etc/opendkim/key.table 并添加以下内容:

default._domainkey.example.com

example.com:default:/etc/opendkim/keys/example.com/default.private

default._domainkey.example.com 上面定义的选择器被配置为使用在的私钥 /etc/opendkim/keys/example.com/default.private。

接下来我们将生成这个密钥。

sudoopendkim-genkey -d example.com -D

/etc/opendkim/keys/example.com -s default

-vsudochownopendkim:opendkim

/etc/opendkim/keys/example.com/default.privatesudoc

hmod 600

/etc/opendkim/keys/example.com/default.private

密钥生成命令将生成您的公钥和私钥。

接下来，您需要将公钥添加为域上的 DNS 记录。打开 /etc/opendkim/keys/example.com/default.txt。复制之后的所有内容 TXT 并将其粘贴为您的 DNS 记录的值。使用 default._domainkey，因为这是在整个上面的命令中使用的选择器的名称作为 DNS 主机名。

最后一步是将 OpenDKIM 连接到 Postfix。再次打开您的 OpenDKIM 配置文件并添加以下行（如果尚不存在）:

Socket inet:8891@localhost

这将创建一个 TCP 套接字，Postfix 将使用该套接字将电子邮件传递给 OpenDKIM 以进行签名和验证。

接下来打开你的 Postfix 配置文件，

/etc/postfix/main.cf:

milter_protocol = 2milter_default_action =

acceptsmtpd_milters =

inet:localhost:8891non_smtpd_milters =

inet:localhost:8891

如果最后两行已经存在以逗号分隔的值，那么您已经使用了一些 Postfix 过滤器。将 OpenDKIM 过滤器添加到现有列表的末尾，而不是创建一个新行。这将确保 OpenDKIM 除了您现有的过滤器外也适用。

现在您可以重新启动 Postfix（service postfix restart）并从 DKIM 签名的消息中受益。您可以使用以下 opendkim-testkey 命令检查您的密钥配置是否正确：

sudoopendkim-testkey -d example.com -s default -vvv opendkim-testkey: using default configfile /etc/opendkim.confopendkim-testkey: checking key 'default._domainkey.example.com'opendkim-testkey: key secureopendkim-testkey: key OK

要测试实际的电子邮件，请将消息发送到 check-auth@verifier.port25.com。DKIM check: pass 在结果中寻找。如果指示失败，请检查 Postfix 日志 /etc/var/mail.log 以查找签名错误。

==========

=======Summary of Results==========

==========SPF check: passDomainKeys check: neutralDKIM check: pass

3. DMARC 设置

DMARC 是"基于域的消息身份验证、报告和一致性"。它是另一种通过发送电子邮件服务器来防止未经授权使用域名的协议。

与 SPF 和 DKIM 不同，DMARC 为域所有者提供了一种方法来指定当电子邮件服务器收到未经适当身份验证的消息时会发生什么。支持三种操作:

- none – 服务器可以继续传递消息。
- quarantine – 将邮件发送到垃圾邮件或垃圾邮件。
- reject – 拒绝并退回邮件。

DMARC 还提供报告机制。您可以指定接收邮件服务器在收到声称来自您的域的电子邮件时调用的服务器端点。这为您提供了作为您的域发送的服务器的跨 Internet 视图。

这是一个示例 DMARC DNS 记录。它应该添加为针对 _dmarc.example.com 主机名的 TXT 记录。

v=DMARC1; p=none; rua=mailto:user@example.com

- p=none–p 标签告诉邮件服务器在未经身份验证的邮件到达时要做什么。它的值必须是上面指定的操作之一。
- rua=mailto...–rua 标签指示服务器将报告数据发送到何处。在这种情况下，它会通过电子邮件发送给您。报告通常每天发送一次，让您可以监控未经授权的发送活动。

还有其他受支持的 DMARC 标签。这些使您可以为子域定义单独的策略操作，改变 SPF 和 DKIM 检查的执行严格性，并配置 DMARC 将应用于的电子邮件的百分比。