钓鱼攻击案例分享与总结

前言

每年HVV总有一批日夜坚守的小伙伴们，他们一定还记得HVV期间发生的一起起钓鱼攻击案例，总是让人心有余悸。作为“HVV利剑”，钓鱼邮件攻击已经成了一种常用的手法，它是一个绝佳的打开内网通道的入口点，邮件可以携带文字、图片、网址、附件等多种信息媒介，结合社工手段可以对未经训练的人群进行“降维打击”，而且钓鱼邮件还可以做到很强的针对性，对于运维部门、企业高管等较高价值目标还可以做到精准打击。

本文我们就通过站在蓝队视角下针对于HVV期间发生的一些钓鱼邮件案例谈一谈我们对钓鱼邮件的一些体会和关于邮件安全防范的一些思考。

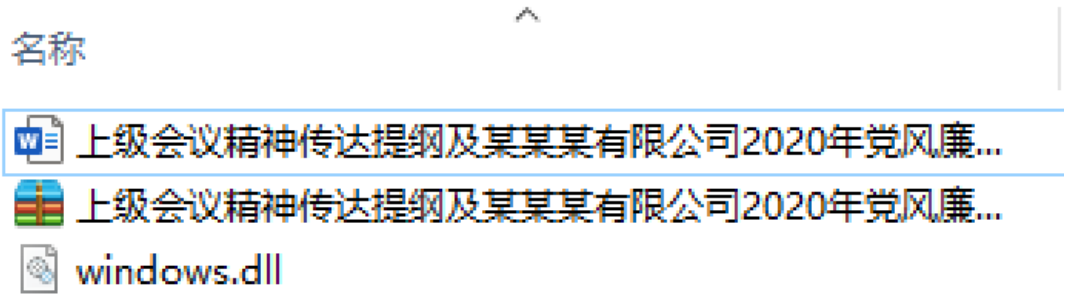
02

钓鱼攻击案例分享

本篇的第一部分，我们先来看一个护网期间真实的案例，一起感受一下“HVV利剑”的锋利。

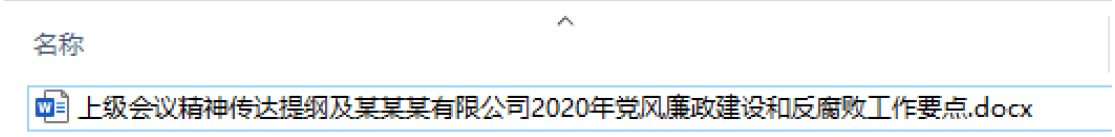
某日，客户反馈他们单位大量人员都收到了一份邮件主题为：上级会议精神传达提纲及xxxx2020年党风廉政建设和反腐败工作要点（xxxx为客单位名称），发件人也确实是集团总部党办工作组的成员，但是此人并不负责他们单位的党政工作。通过电话联系发件人后，确认不是该员工本人发送的，因此我们立即敏锐的进入应急状态。　　我们拿到邮件后正常打开如下，正文仅有一个压缩包没有其他内容。

我们打开压缩包后发现了压缩包里面是一个使用了超长文件名伪装成word文档的exe，里面还有dll库文件。不过在windows环境下显示如下，由于使用了超长文件名，即便开了显示文件拓展名也无法正常显示后缀。：



当我们在沙箱里面点击这个 exe 程序后，竟然真的直接就打开了 word 并且显示了一篇正常的文章。

等我们关闭 word 回到目录的时候发现，exe 和 dll 文件都没有，只留下了一个真正的 docx 文档，而此时我们的沙箱主机应该已经在攻击者的服务器上线了：



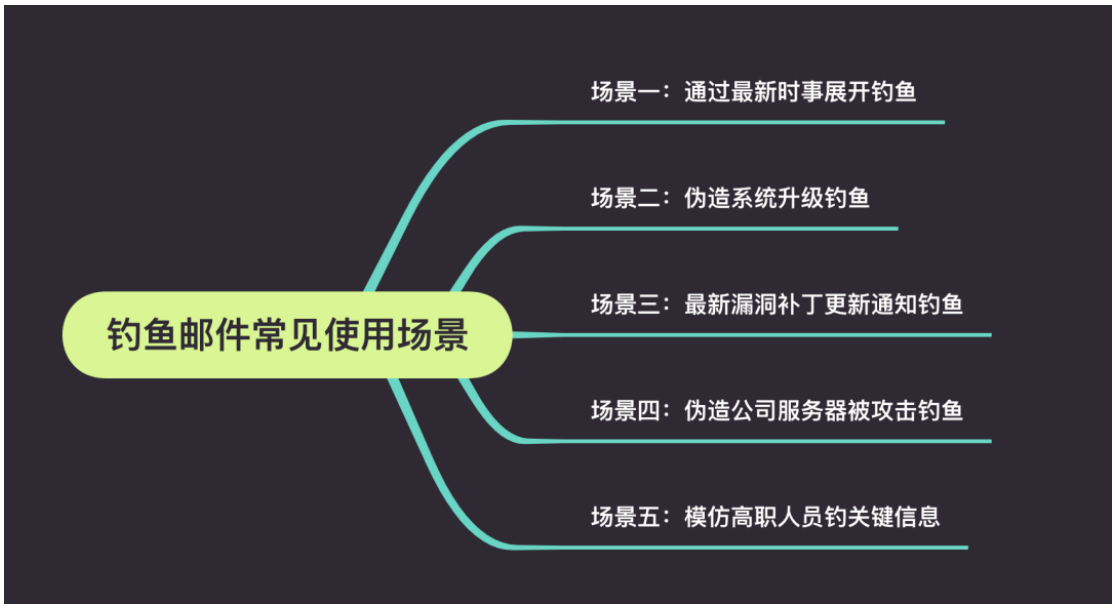
此案例中攻击者通过前期钓鱼邮件获得了一个可信度较高的员工邮箱，然后利用该单位一份真实的文件做毒饵，向该单位人员邮箱进行精准投放，且恶意软件执行过程和 word 文档打开过程中没有任何异常提示，真正的无感，对于一些安全意识比较低的员工，根本不会意识到自己被攻击了。

03

钓鱼邮件常见使用场景

上面我们分享了一个在护网中真实的钓鱼攻击案例，通过这个案例我们对钓鱼攻击应该有了一个简单的认识。但是我们知道，实际的钓鱼场景肯定远远不止

我们上面这个案例所列举的场景。所以下面我们对钓鱼邮件常见的使用场景做了一个梳理：



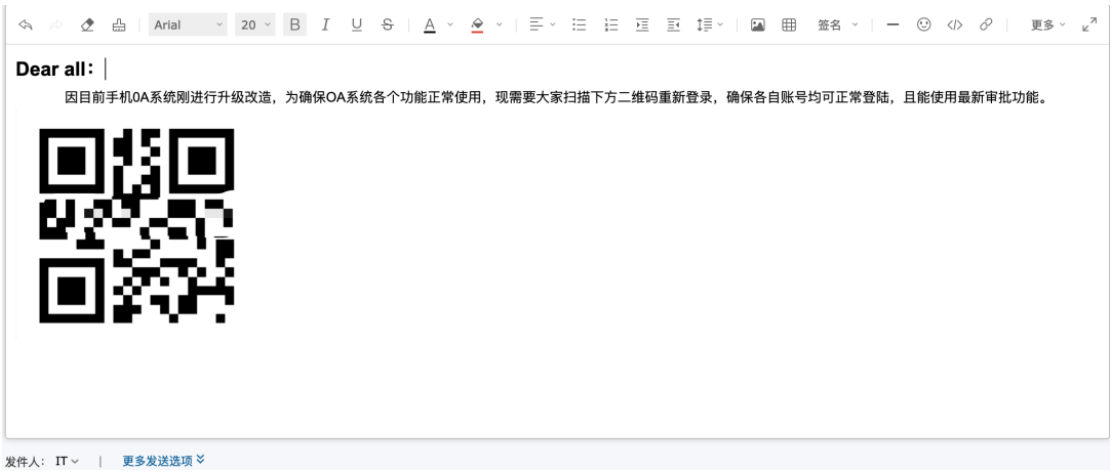
场景一

以最近某段时间的最新时事展开钓鱼，比如：2020 年广为人知的新冠肺炎疫情，以它为一个钓鱼点，发送相关的钓鱼邮件，获取员工相关账号和密码，或者员工的个人敏感信息，如姓名、电话、身份证号、家庭住址、家庭情况等敏感信息。

构造如下的这样一封钓鱼邮件，通过利用大家对新冠肺炎疫情的实时关注，在邮件中放入钓鱼链接，可轻松获取大量人员敏感信息：

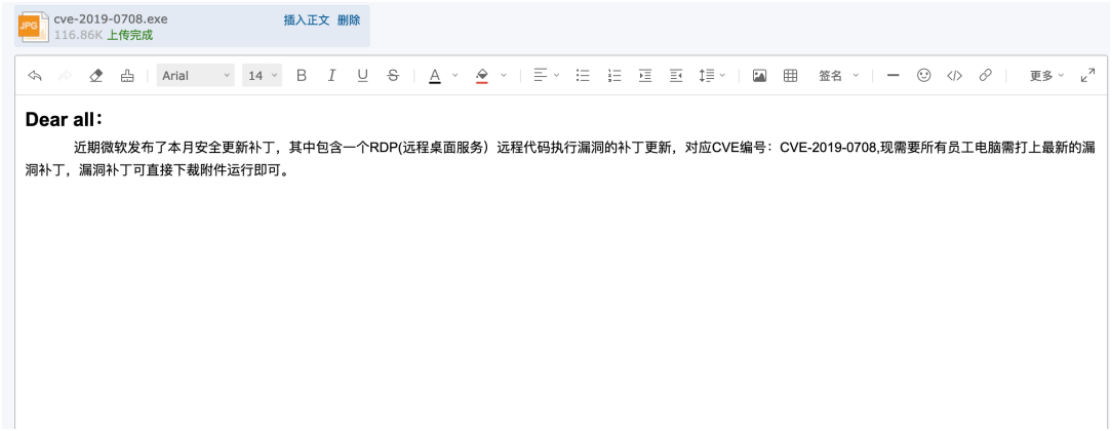
场景二

邮件通知公司全员：公司常用系统升级，需要通过新的系统进行相关操作。比如构造如下的一封钓鱼邮件，通知公司全员，手机 OA 系统升级，需要通过扫描二维码重新进入，从而诱导员工扫描钓鱼二维码，钓取员工相关的账号和密码等敏感信息：



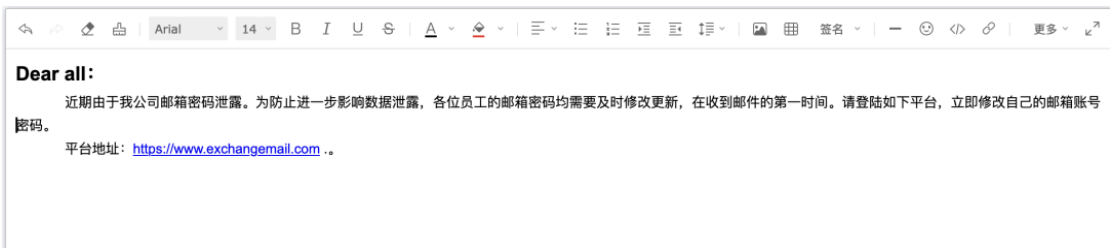
场景三

通过信息收集获取到公司安全或运维部门的邮箱时，可根据最新爆发的漏洞给全体员工发送补丁更新通知，可将最新漏洞的补丁（exe 为免杀的远控木马等）作为邮件附件，并提示大家下载后运行进行补丁修复，比如这样的一封钓鱼邮件：



场景四

通过伪造公司服务器被攻击，账号密码泄露等理由进行邮件钓鱼攻击。比如下面这封钓鱼邮件：



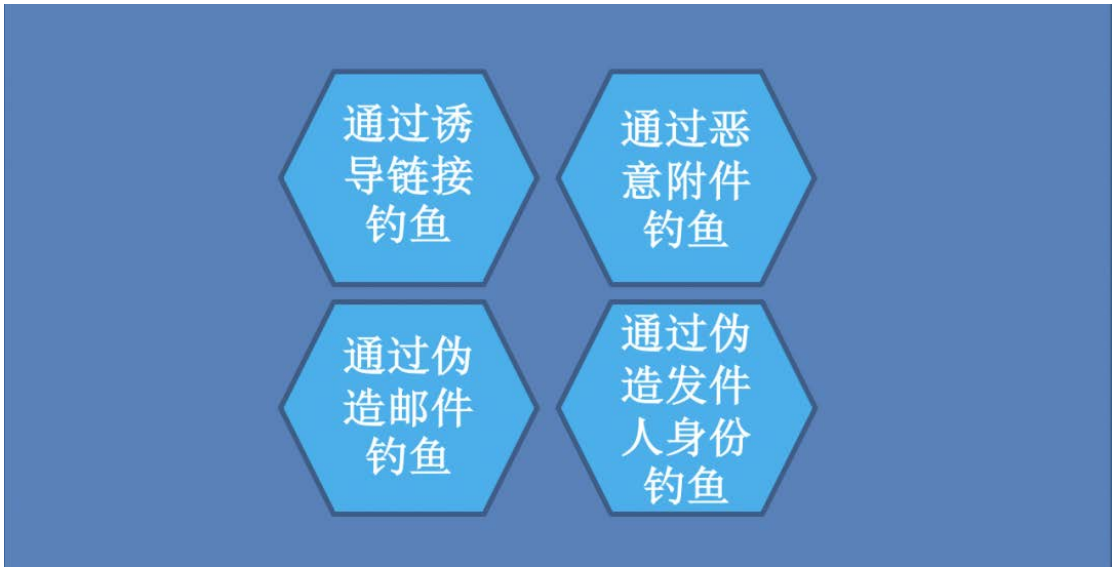
场景五

由于公司高职人员相关信息往往在互联网上都有披露，在拿到公司高职人员的相关信息后可通过模仿高职人员向下属部门或人员发送邮件，比如通过模仿公司领导去钓运维人员，从而获取到领导个人的相关账号密码等信息：

04

钓鱼邮件主流攻击方式

在了解了钓鱼邮件常见的使用场景后，我们再来看一下钓鱼邮件当前的一些主流攻击方式：



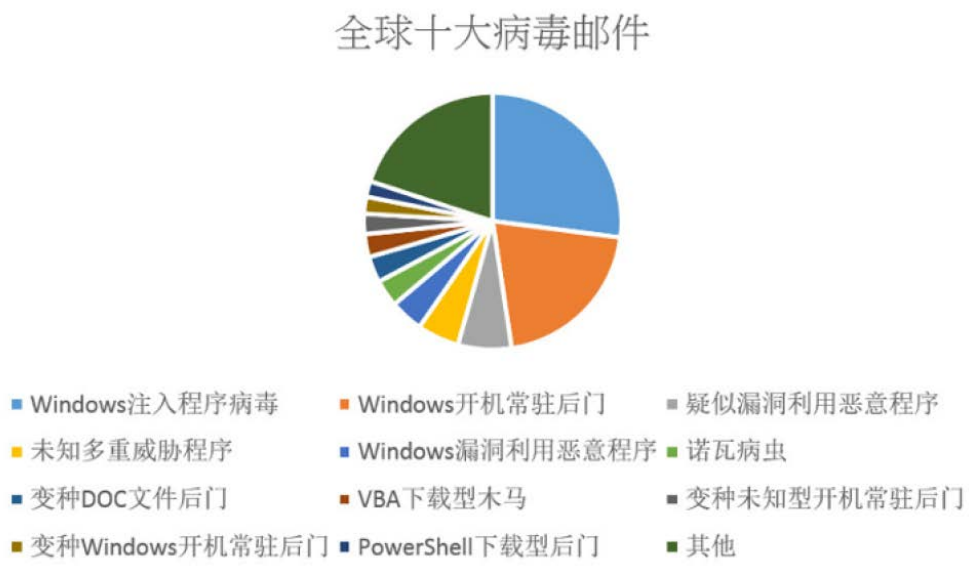
通过诱导链接钓鱼

通过诱导链接钓鱼是一种最常见也最基础的攻击方式，通常就是在邮件正文中通过一些诱导性的文字诱导用户点击攻击者精心构造的钓鱼链接，点击后将会进入一个伪造的网站或者一个恶意程序下载页面等。当然，在实际的攻击实施过程中，攻击者往往会结合一些上面叙述的诸如一些近期热点事件、公司内部系统升级等场景，以提高内容可信度，诱导用户点击链接，同时恶意链接部分也常会进行一系列伪装，这里我们以 http://www.taobao.com 为例：

伪装手法	示例
1.近似 URL	http://www.taoba0.com/
2.仿冒子域名	http://secure-taobao.com/
3.利用链接的显示与实际不同进行欺骗	点击此处跳转淘宝（真实地址为钓鱼链接：www.diaoyu.com）
4.短链接	http://dwz.date/dr6m（实际为 http://www.diaoyu.com）
5.利用 URL 特性	http://www.taobao.com@baidu.com(实际访问的是 www.baidu.com)

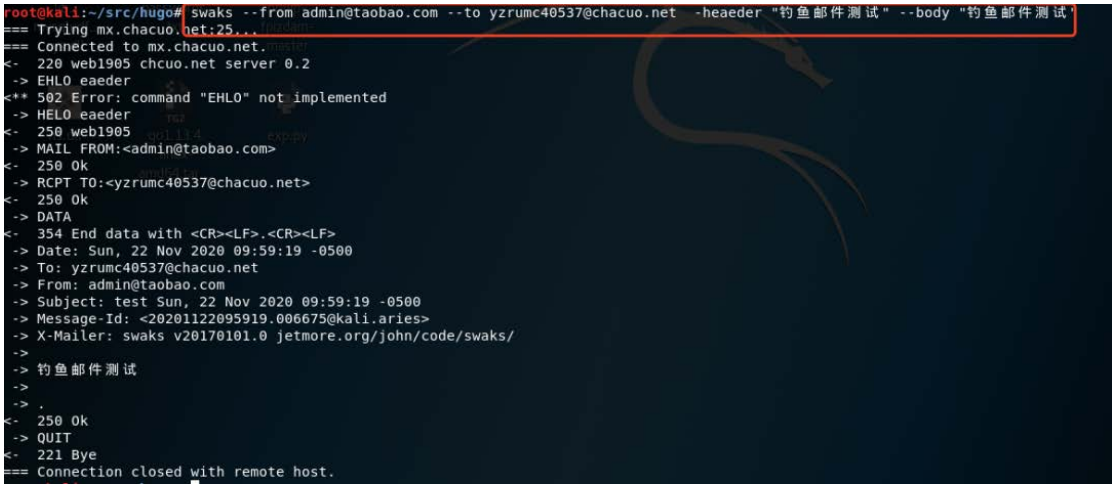
通过恶意附件钓鱼

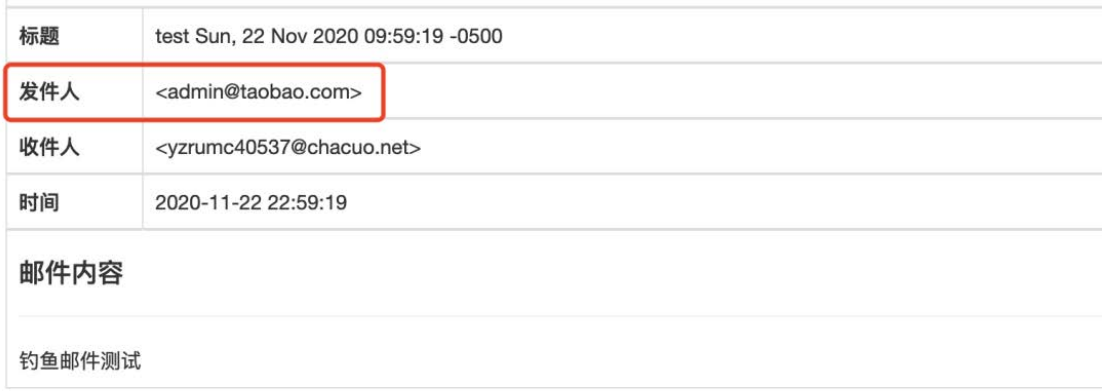
通过恶意附件钓鱼可以算是另一类最为常见的钓鱼手法了。攻击者通过在邮件附件中添加木马、后门或软件漏洞的利用 EXP 等攻击程序，再辅以诱导性的文字诱导用户下载运行，从而达到窃取敏感信息，甚至是控制上钩者电脑的目的。常见的木马、后门程序的载体有直接的文档、图片、压缩包、脚本程序（exe、vbs、bat）等。



通过伪造邮件钓鱼

我们现在邮件系统的实现大多是使用 SMTP 协议，SMTP 邮件服务器在进行邮件中转的时候不需要认证，利用这个特点攻击者可以轻易进行邮件伪造从而实施钓鱼攻击。此处我们使用 swaks 伪造 admin@taobao.com 向目标投送伪造的钓鱼邮件如下：

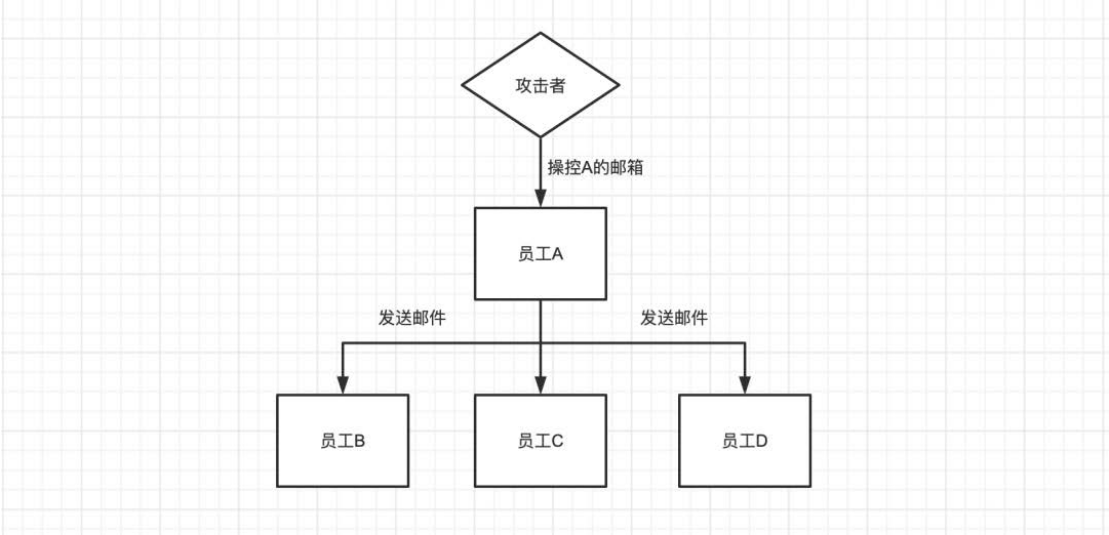




swaks 常见参数说明：--from<要显示的发件人邮箱>--to<目标邮箱地址>--header<邮件头信息，subject 为邮件标题>--body<邮件正文>

通过伪造发件人身份钓鱼

最后一种较为主流的手法就是通过伪造发件人身份来实施钓鱼攻击。这里的伪造不同于我们上面所说的通过技术手段进行邮件伪造，而是在经过前期大量的信息收集以后，窃取目标公司内某员工的真实邮箱，然后以这个员工的名义向公司内的其他人员发送邮件，也就是说，这里的邮箱是真实邮箱，而发件人的身份却是由攻击者伪装的，这样利用大家对发件人本身的信任来实施钓鱼攻击，可以达到事半功倍的效果。

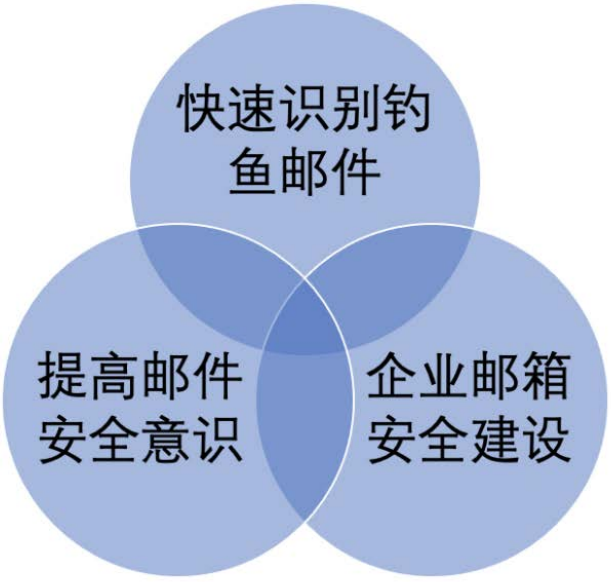


在实战过程中还有一些类似的手法，比如通过邮箱直接攻击 A 单位人员无法成功，那么攻击 A 单位的上级单位或者有较强业务往来的 B 单位人员邮箱，然后利用 A 对 B 的信任，伪造邮件向其索要一些敏感信息或者要求安装一些攻击程序等。

05

钓鱼邮件防范手段

知攻善防，上面我们一直在说如何通过钓鱼邮件进行攻击的相关知识，也可以清晰的感受到钓鱼邮件是高级网络攻击重灾区，那么面对钓鱼邮件，作为蓝队该如何进行一些有效的防范呢？下面我们就通过“快速识别钓鱼邮件”、“提高邮件安全意识”、“企业邮箱安全建设”三个维度来看一下：



快速识别钓鱼邮件：

- 看发件人地址。如果是公务邮件，发件人多数会使用工作邮箱，如果发现对方使用的是个人邮箱帐号或者邮箱账号拼写很奇怪，那么就需要提高警惕。钓鱼邮件的发件人地址经常会进行伪造，比如伪造成本单位域名的邮箱账号或者系统管理员账号。

- 看邮件标题。大量钓鱼邮件主题关键字涉及“系统管理员”、“通知”、“订单”、“采购单”、“发票”、“会议日程”、“参会名单”、“历届会议回顾”等，收到此类关键词的邮件，需提高警惕。

- 看正文措辞。对使用“亲爱的用户”、“亲爱的同事”等一些泛化问候的邮件应保持警惕。同时也要对任何制造紧急气氛的邮件提高警惕，如要求“请务必今日下班前完成”，这是让人慌忙中犯错的手段之一。

- 看正文目的。当心对方索要登录密码，一般正规的发件人所发送的邮件是不会索要收件人的邮箱登录账号和密码的，所以在收到邮件后要留意此类要求避免上当。

- 看正文内容。当心邮件内容中需要点击的链接地址，若包含“&redirect”字段，很可能就是钓鱼链接；当心垃圾邮件的“退订”功能，有些垃圾邮件正文中的“退订”按钮可能是虚假的。点击之后可能会收到更多的垃圾邮件，或者被植入恶意代码。可以直接将发件人拉进黑名单，拒收后续邮件。

提高邮件安全意识：

- 不轻信发件人地址中显示的“显示名”。因为显示名实际上是可以随便设置的，要注意阅读发件邮箱全称。
- 不轻易点开陌生邮件中的链接。正文中如果有链接地址，切忌直接打开，大量的钓鱼邮件使用短链接（例如 http://t.cn/zWU7f71）或带链接的文字来迷惑用户。如果接到的邮件是邮箱升级、邮箱停用等办公信息通知类邮件，在点开链接时，还应认真比对链接中的网址是否为单位网址，如果不是，则可能为钓鱼邮件。
- 不放松对“熟人”邮件的警惕。攻击者常常会利用攻陷的组织内成员邮箱发送钓鱼邮件，如果收到了来自信任的朋友或者同事的邮件，你对邮件内容表示怀疑，可直接拨打电话向其核实。
- 不使用公共场所的网络设备执行敏感操作。不要使用公共场所的电脑登入电子信箱、使用即时通讯软件、网上银行或进行其它涉及敏感资料的

操作。在无法确定其安全性的前提下，请不要在连接 Wi-Fi 后进行登录和收发邮件，慎防免费无线网络因疏于管理被别有用心人士使用数据截留监侦手段获取用户信息。

- 不将敏感信息发布到互联网上。用户发布到互联网上的信息和数据会被攻击者收集。攻击者可以通过分析这些信息和数据，有针对性的向用户发送钓鱼邮件。

企业邮箱安全建设：

邮件服务器如同企业内其他业务服务器一样，也需要纳入企业本身的安全防护体系，使用 IPS、WAF 等安全防护设备保证邮件服务器的基础环境安全。除此之外，还需要通过 SPF、DKIM、DMARC 等邮件防伪造协议来防止别人伪造自己公司的邮箱域名来发邮件。而对于邮件正文中的钓鱼链接、恶意脚本等，还可以通过采购邮件安全网关，来达到反垃圾邮件、防病毒、防钓鱼等效果。

除了技术上的建设，对于邮箱的安全管理，我们可以结合公司现状尝试以下几点：

- 安排专职的邮件管理员对企业邮件进行管理，发现异常邮件时能够进行批量撤回，并且能追踪恶意邮件的阅读状态，对已阅读查看的账户发送提醒邮件或应急排查手册。
- 尽可能减少邮箱各类访问登录接口，如 web 登录接口，OWA 接口，邮件服务端口，移动端接口、移动办公 app 接口等，暴露出来的接口做好监测防护。
- 内部定期进行钓鱼邮件测试，尤其是非技术部门，对于中招的员工进行安全意识培训，甚至是内部通报，以时刻给大家敲响警钟。

企业邮箱建设是个长远且复杂的路程，需要结合自身企业现状进行合适的规划落地，三言两语也无法尽述其中细节，还需要大家去持续探索实践，在此不再赘述。

06

总 结

当前互联网技术快速发展，网络安全防护能力升级的同时，网络攻击手段和网络安全威胁却是越发高级和复杂。邮件钓鱼是高级网络攻击和网络犯罪发生的重灾区，同时也是我们在护网行动中见到的最为频繁，防御最为困难的一种攻击手法，更是蓝队视角下的“护网利剑”。本文简单介绍了钓鱼邮件常见的场景，主流攻击方式、以及防范手段，希望给各位安全人员提供一些攻击和防御的灵感和思路，同时也给用户提供一些防范此类攻击的想法。