以练代防--增强钓鱼邮件防护

中国xxx集团有限公司 张三 182xxxxxxxx

# 一、背景与目标

网络安全防护是一项系统性工作，从技术体系建设和管理体系建设两大层面覆盖多项要素。从攻击角度，采用社会工程学方法，利用人的弱点进行攻击，已经成为了普适性的攻击手段。电子邮件作为日常办公的主要工具，是攻击者利用的重要目标，已沦为诈骗、勒索软件攻击的重灾区。在近几年的演习活动中，采用钓鱼邮件获取访问口令或控制系统权限也已经成为了主流的攻击方式。

在【客户名称】日常的网络安全运营管理中，监测到的钓鱼邮件攻击行为众多。在【客户名称】业务广泛、队伍庞大的现状下，防护和管理态势十分严峻。因此，为有效地加强日常钓鱼邮件防护，并为本次演习做好准备，【客户名称】决定，从本质上进行治理，提升员工的防护意识。采用钓鱼邮件模拟攻击的形式，让员工真正意识到钓鱼邮件防护必要性，能够自主的识别潜在的危险。

# 二、制定钓鱼策略及思路

为检验员工对钓鱼邮件识别和防护的安全意识，工作组决定使用Cobalt Strike在互联网搭建服务端，通过Cobalt Strike客户端克隆【客户名称】OA系统，并开启键盘记录功能。

在发送者构造和内容选择上，工作组清晰地知道，钓鱼邮件主要是利用人性中的弱点。一方面是信任关系，另一方面是和自己利益相关的诱导内容。所以选择伪造关键岗位（信息化部门管理者）的相似邮箱名称和邮件签名。并将大家已经知道消息的，演习工作启动会相关配合要求，作为钓鱼邮件内容，诱骗业务部门系统管理员和普通员工点击登录伪造的OA系统，达到获取员工用户名/密码的目的。

# 三、钓鱼邮件实施

1、通过在互联网上对相关新闻，招投标信息等公开资料的查询，获取了邮箱为XXX@xx.com（XXX为信息化部门关键人物）的内部邮件用户名称。

2、通过163邮箱注册XXX\_xx@163.com邮箱，达到模仿关键人物邮箱地址的目的。从人性角度分析，163虽然很明显为伪造邮箱，但极易被忽略。

3、伪造钓鱼邮件正文

根据XXXX年XX月XX日，将召开的【客户名称】网络安全专题会要求，并添加了为了防止重保演习期间协同办公系统（OA）账号锁定，需x月x日前登录此地址http://XXX.XXX.XXX.XXX/使用谷歌浏览器/IE浏览器认证OA账号，如未认证登录，可能导致重保期间OA账号锁定，请各位务必进行账号认证的相关诱骗信息。

4、使用公网IP地址搭建Cobalt Strike服务器端，通过客户端进行联通测试。

5、获取中国【客户名称】OA系统登陆界面URL地址，通过Cobalt Strike客户端钓鱼网站克隆功能，伪造OA系统登陆界面，并开启键盘记录功能。

6、获取xx余个【客户名称】内部邮件地址，通过伪造的163邮箱发送。

# 四、钓鱼邮件成果

经过2天的守株待兔，共30人点击钓鱼邮件中伪造的股份OA系统。其中，2名员工在伪造的股份OA系统中输入了用户/密码。

捕获用户名/密码后，进一步深入测试，首先通过捕获的用户名/密码成功登录OA系统，又使用同一密码尝试登录邮件系统、统一认证系统、劳务管理等系统均登录成功。从此成果可以得出，钓鱼邮件攻击成本简单，危害性极强。

# 五、培训宣贯

根据本次模拟的成果，通过【客户名称】全员推送、公众号和即时通广播三渠道发布了钓鱼邮件防范宣贯图文。针对网络安全意识，在公众号推送了包括“安全上网十二条”、“手机网络办公安全知识”、“如何查找网络安全漏洞信息”等专题文章。同时，发布钓鱼邮件、修改密码、近期漏洞报送等专题通知，确保网络安全意识宣贯工作落实到位。

# 六、收获和后续工作

通过本次模拟的开展，信息化部门管理人员、业务部门系统使用人员和员工均认识到了钓鱼邮件攻击的危害，并具备了主动识别的谨慎意识。在后续的网络安全管理工作中，信息化部门将定期通过攻防演练平台，组织钓鱼邮件的相关模拟，以练代防，不断地加强关键岗人员和广大员工的网络安全意识，最大程度的减少因人为因素带来的安全风险隐患。

# 七、钓鱼邮件预防

通过本次模拟，工作组总结了钓鱼邮件预防的几项措施，后续将在【客户名称】内部进行重复宣贯。

1. 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。

1. 看收件人地址

如果发现所接收的邮件被群发给公司内大量人员，而这些人员并不是工作常用联系人或同一工作组织内人员，那么就需要警惕，有可能是钓鱼邮件。

1. 看发件日期

公务邮件通常接收邮件的时间在工作时间内，如果收到邮件是非工作时间，需要提高警惕。比如，凌晨3点钟。

1. 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。

1. 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”，这是让人在慌忙中犯错的手段之一。

1. 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。

1. 看正文内容

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。

1. 看附件内容

当心邮件中的附件信息，不要随便点击下载。诸如word、pdf、excel、PPT、rar等文件都可能植入木马或间谍程序，尤其是附件中直接带有后缀为.exe、.bat的可执行文件，千万不要点击。