2024 守内安信息科技 & ASRC
第三季度邮件安全观察

ASRC

Spam Mail
Virus Mail
Malicious Mail

Oct 2024 released.

第三季，电子邮件安全的整体基调仍以泛滥的钓鱼邮件为主。利用二维码将钓鱼链接编码的攻击已渐渐常态化，成为钓鱼邮件流行的一种类型。比较值得注意的是，本季发现试图利用 CVE-2014-4114 的恶意邮件的趋势明显升高，附件文件多为.ppt。建议避免使用盗版的 Office 软件并确保适时进行安全更新，才能有效避开这个历时十年不衰的漏洞影响。

Quishing 常态化，锁定移动设备攻击

通过二维码隐藏钓鱼地址的钓鱼行动，称为 Quishing（QR code phishing），本质上是一种网络钓鱼攻击，与传统网络钓鱼攻击有许多相同的概念与技术。区别在于利用二维码隐藏钓鱼地址以防安全机制的侦测，且受攻击者多半以手机来译码二维码，因此将钓鱼攻击目标由受保护的个人计算机，转移至较不受保护的个人电子设备。

Quishing 已逐渐成为常态。在第三季，我们观察到国内的大规模 Quishing 攻击，多半是假冒政府或企业发放福利，并附上一个以二维码编码过的钓鱼链接。

观察到的大规模 Quishing，多半是假冒政府或企业发放福利

较特别的是，这些钓鱼网站的目标锁定为个人移动设备，必须使用移动设备访问才能正确地显示诈骗页面。

```
<!DOCTYPE html>
<html>
    <head>
        <meta charset="utf-8">
        <title></title>
    </head>
<script>
    if((navigator.userAgent.match(/(iPhone|iPod|Android|ios|iOS|iPad|Backerry|WebOS|Symbian|Windows Phone|Phone)/i))) {

     window.location.href="https://aa2.32884aaka.cn/1/xm.php?rukou=https://aa2.3il8g.cn";


    }else{

     window.location.href="https://aa2.32884aaka.cn/diannao.php?rukou=https://aa2.3il8g.cn";
    }

            </script>
    <body>


    </body>
</html>
```

使用移动设备访问才能正确地显示出诈骗页面

钓鱼网站还精心布置了许多干扰的文字，用来干扰信息安全设备爬虫的自动检测。

用来扰乱威胁爬虫自动检测的干扰文字

这个钓鱼页面最主要的目的为获取受害者的信用卡数据，以假借社保局自助申请系统的名义，先骗取受害者的敏感真实数据。再以核对资产的名义，实时确认提供的敏感信息与信用卡是否可以盗刷。

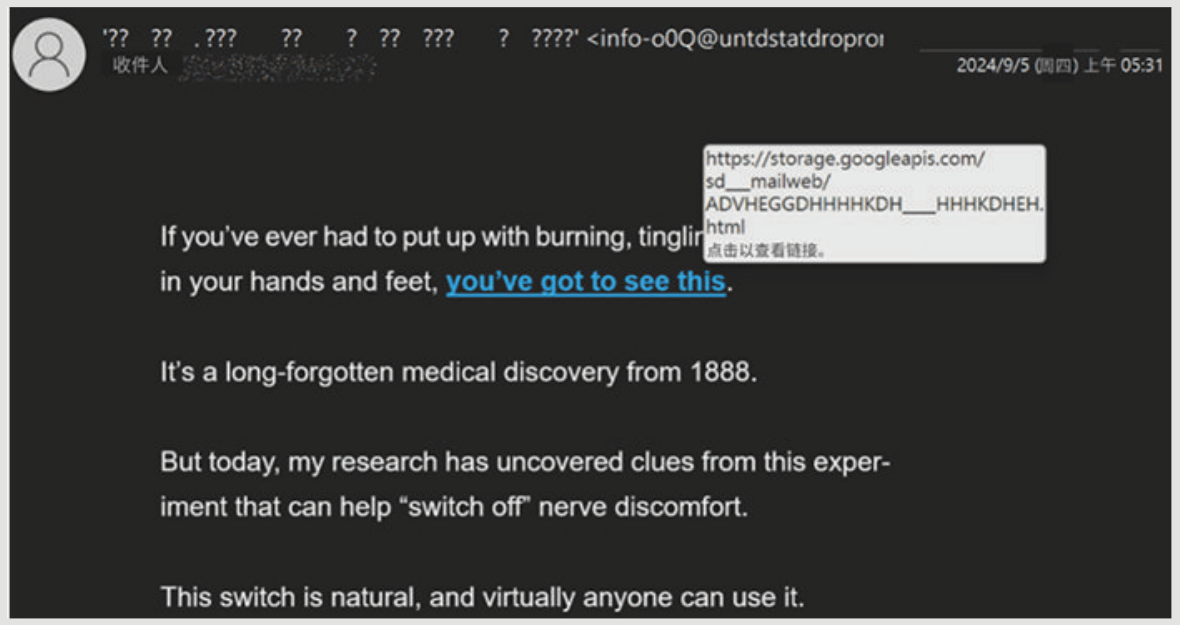
假借社保自助申请系统名义，先骗取受害者的敏感真实数据

实时确认提供的敏感信息与信用卡是否可以盗刷

利用公有服务转址，增加钓鱼隐蔽性并进行前置过滤

将钓鱼链接直接发送给攻击的对象是过去网络钓鱼攻击很直观的做法。但在 ISP 与网安组织等的联防、情报交换下，钓鱼网站可能在很短的时间内便遭到封禁或被网安公司搜集做成黑名单，缩短钓鱼链接的使用寿命。

因此，越来越多的钓鱼邮件，携带的钓鱼链接并不是直接指向恶意网站，而是知名的合法服务地址：比方由 Google 或其他信誉良好的公司所提供的档案、静态网页的网址。



钓鱼邮件携带的钓鱼链接指向知名的合法服务地址

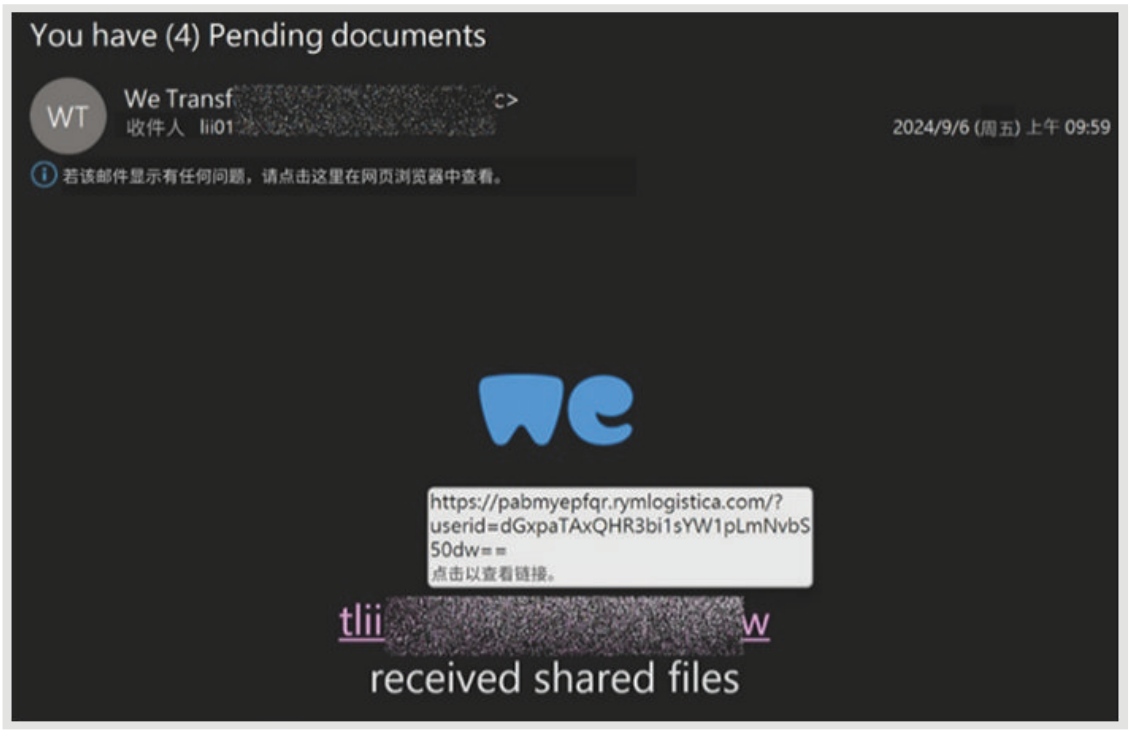
这个网站不会做复杂的事，只做转址的动作，将受害者带往真正的钓鱼网站。这样做的好处除了可以通过信誉良好的网址，掩护恶意的钓鱼网站之外，还可以针对被导向的受害者做一些前置的过滤动作，比方锁定来源、锁定某些浏览器，或是锁定某些组织的域名后，再进行真正的攻击动作。

```
<meta http-equiv="refresh"content="0; url=https://www.govwlfeloony.com/2FRNJG5BQ/HTDG86K/
```

转址将受害者带往真正的钓鱼网站

设计多重圈套提高网络钓鱼有效性

攻击者为了提高网络钓鱼的有效性，并提高钓鱼网站的存活率，会同时使用许多方法来达成这个目标。我们观察到一种钓鱼邮件，使用的社交工程的手段是诱导受害者连接到外部网页去下载文件数据。



钓鱼邮件以社交工程手段诱导受害者链接外部网页下载文件数据

当受害者点击该链接时，会先以 Captcha 人机验证。只有通过 Captcha 验证，才会导向真正的钓鱼页面。

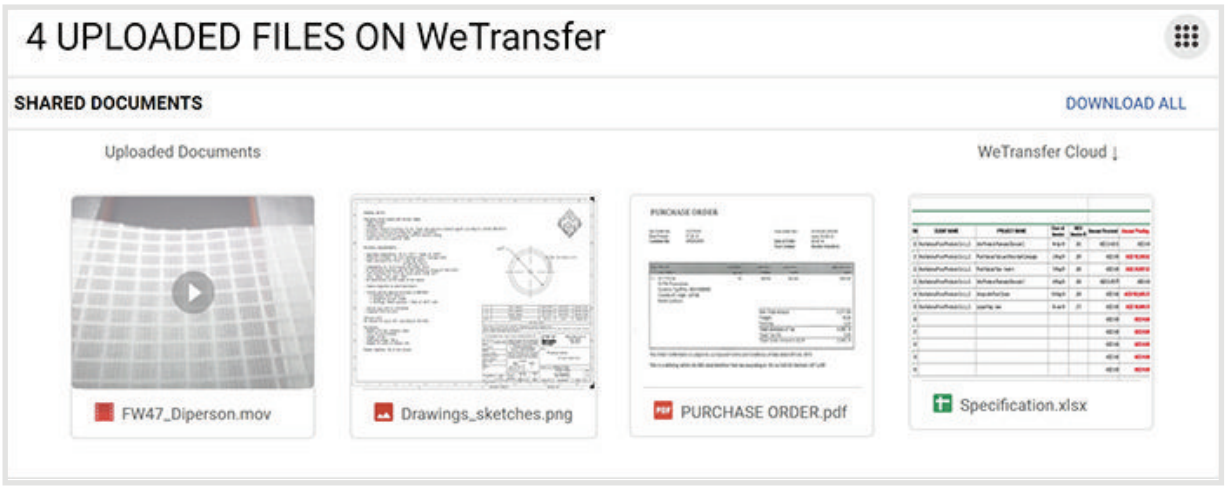
```
// Function to check if a string is base64 encoded
function isBase64(input) {
    try {
        return btoa(atob(input)) == input;
    } catch (e) {
        return false;
    }
}

// Function to decode the email and redirect
function decode(email) {
    if (isBase64(email)) {
        email = atob(email);
    }
    // Append the decoded email to the URL and redirect
    window.location.href = 'https://ipfs.io/ipfs/bafkreiahkhijpw7trmjelm4mc76kdd7hh2e42usnxom7xuoi144q2wr36q/#' + email;
}

// Function to handle reCAPTCHA callback
function recaptcha_callback() {
    // Check if 'userid' is in the URL and not empty
    const urlParams = new URLSearchParams(window.location.search);
    const userId = urlParams.get('userid');
    if (userId) {
        decode(userId);
    }
}
```

只有通过 Captcha 验证，才会导向真正的钓鱼页面

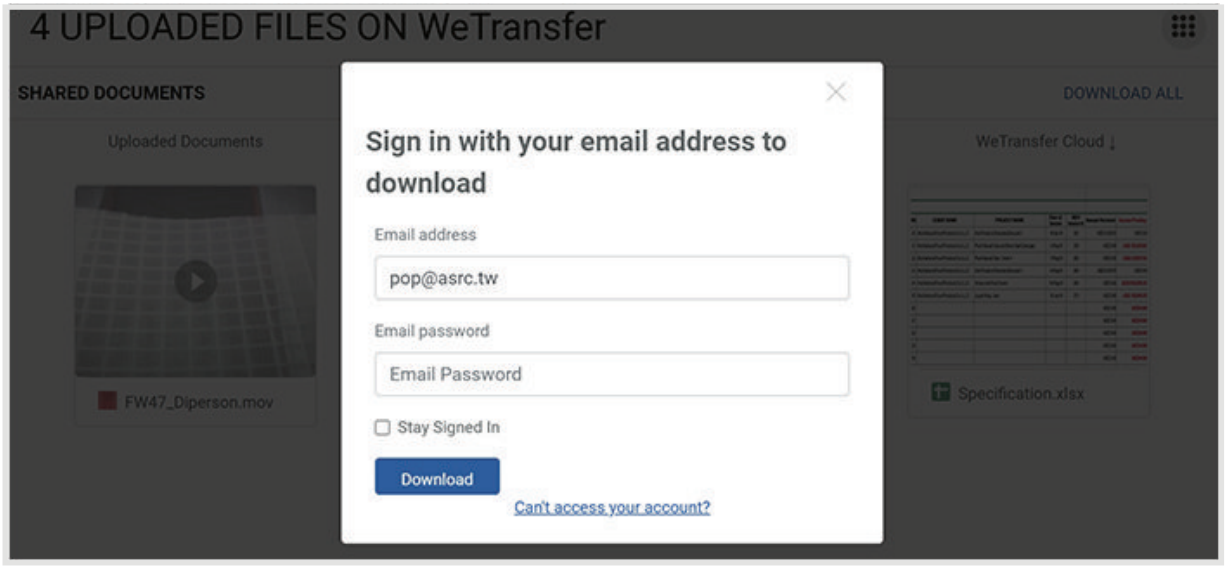
钓鱼页面被伪装成 WeTransfer 的服务，煞有其事的以多个重要的商务文件缩略图营造出这些文件需要下载并仔细查看的错觉。



多个重要的商务文件缩略图营造文件应该下载来仔细查看的错觉

下载时，要求受害者输入电子邮件信箱账号密码作为验证，通过验证后才能下载文件。但事实上，这就是钓走受害者电子邮件信箱账号密码的关键环节。受害者第一次输入密码后，系统一定会显示错误，要求再次输入；第二次则不论输入内容为何，都会导向受害者电子邮件地址的来源域名。攻击者利用这样的方式，提高收集密码的正确性！

攻击者甚至可以在最后步骤稍加变化，让受害者下载一个恶意文件或档案作为后续的利用，进一步增加攻击的深度。



要求受害者输入电子邮件账号密码作为验证，就是钓取数据的关键环节

如何防范网络钓鱼?

在科技的手段上,重点在于及早或事后识别出钓鱼网站的链接,及时阻止受害者连接;或在事态未扩大前主动发现可能被钓走的敏感信息,并遏止进一步的利用。在培训安全意识上,则是通过识别钓鱼邮件的大致样式,做到不点击、不转发,并主动通报网络安全部门以达到防御的效果。不过,攻击者正试图以多种方式,让钓鱼网站依附在合法的网站、转址等功能之下,让钓鱼链接的识别更加困难;受到攻击的人,可能无法完全记得曾受过的安全培训中的识别细节,这个时候,不妨使用安全的浏览器,它可以帮你阻挡一些恶意网站的链接;当对于要访问的页面有所怀疑的时候,也可利用浏览器内建的AI,询问这个页面是否安全。虽然未必能直接得到答案,但一定可以获取有用的提醒建议或是识别方法的参考信息。

关于 ASRC 威胁邮件研究中心

ASRC 威胁邮件研究中心 (AsiaSpam-message ResearchCenter),与守内安长期合作,致力于全球垃圾邮件、威胁邮件、钓鱼邮件、网络攻击等相关研究,运用相关数据统计、调查、趋势分析、学术研究、跨界交流、研讨活动等方式,与学术,行业及政府共同推动净化电子邮件使用环境。