2024 守内安信息科技 & ASRC
第二季度邮件安全观察

ASRC

Spam Mail
Virus Mail
Malicious Mail

July 2024 released.

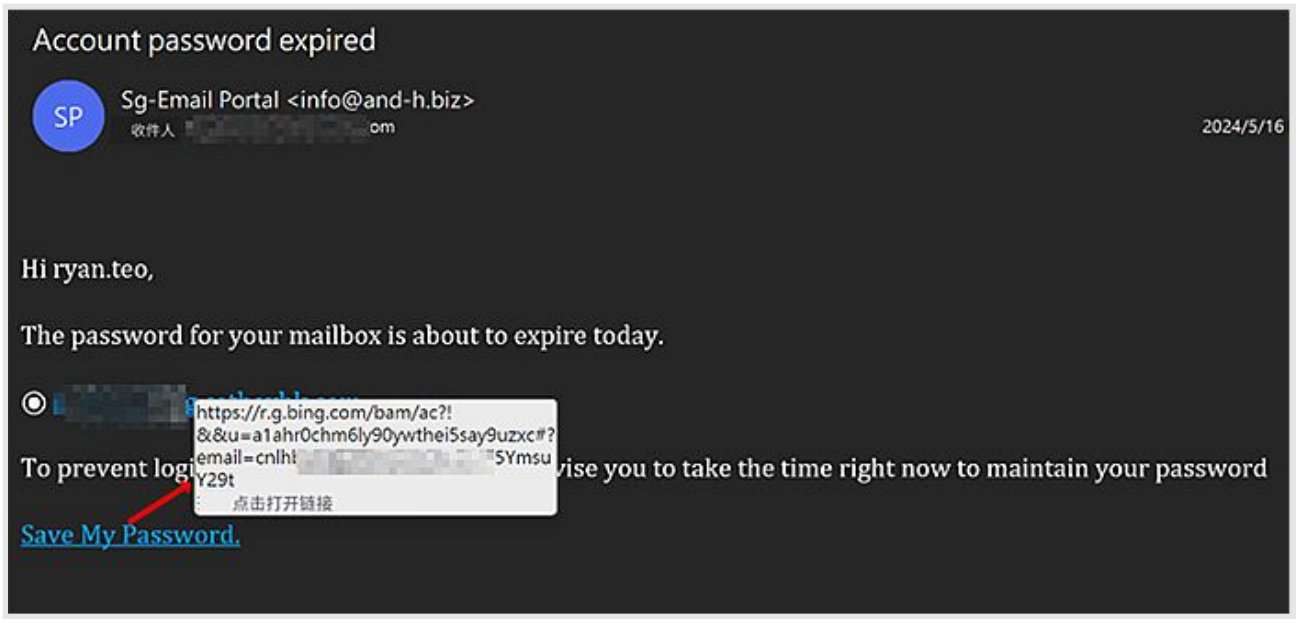
如今网络攻击的分工越来越细致，通过近期攻击趋势分析，明显分为初始入侵和后续的横向移动或深入攻击两大阶段。

初始入侵，即通过漏洞利用或泄露凭证两大手段进行；其中，泄露凭证的重要获取途径之一就是钓鱼邮件。**而本季度，需要特别警惕的就是钓鱼邮件。**年中时，许多单位会集中进行社交工程演练，导致信息安全或IT部门的负担加重，因此应特别留意防护！**上一季度主流的二维码钓鱼邮件攻击仍在持续，未来大概率将演变成常态化的攻击方式。**

以下是本季度特殊的攻击样本介绍：

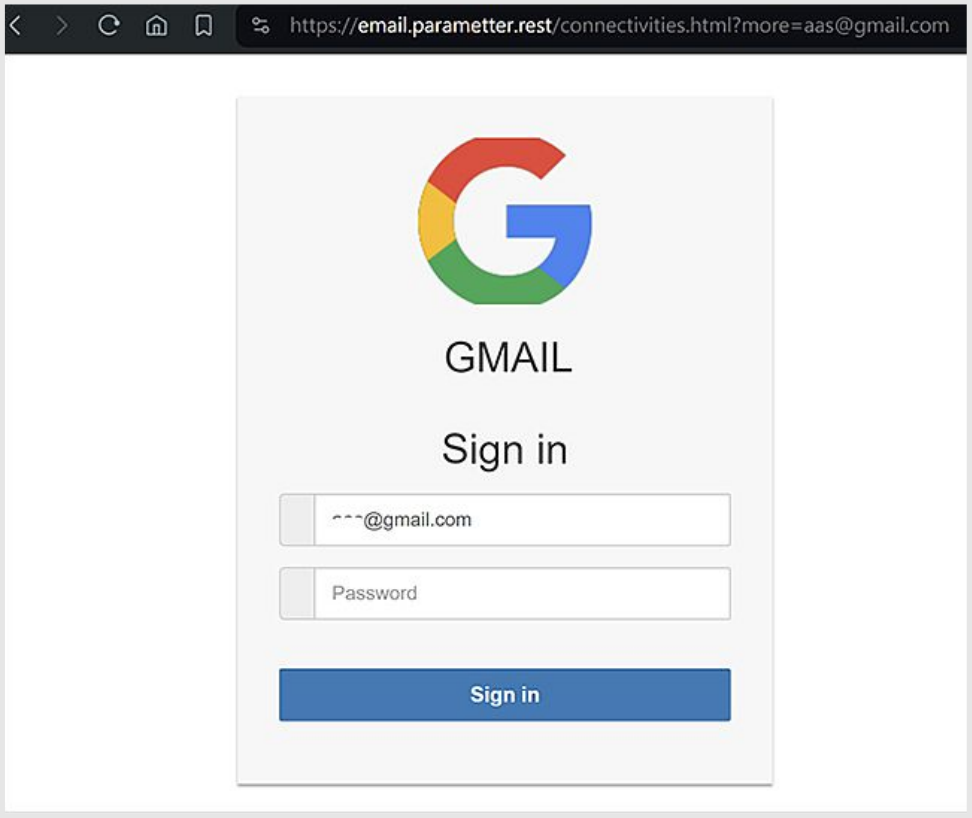
Bing 服务被用于钓鱼邮件

合法服务一直是钓鱼邮件的目标，因为钓鱼邮件中的超链接是其最关键、也是最容易被识别的部分。最近，**我们发现 Bing 的服务被用于钓鱼邮件的超链接置换。**



Bing 的服务被利用于钓鱼邮件的超链接置换

通过 Bing 的链接，受害者首先会被引导至恶意网站中继，然后再被重定向到真正的恶意页面。这个恶意页面会直接显示受害人的电子邮箱，并模仿 Gmail 的登录页面，主要目的是骗取邮件登录的账号及密码！更有趣的是，**输入第一次密码后，页面会更新一次，让受害者误以为没有输入成功；第二次输入时则会直接跳转到 Gmail 的登录页面，**这个手法可能是为了提高密码获取的正确性。



页面直接显示受害人的电子邮箱，并仿造登入页

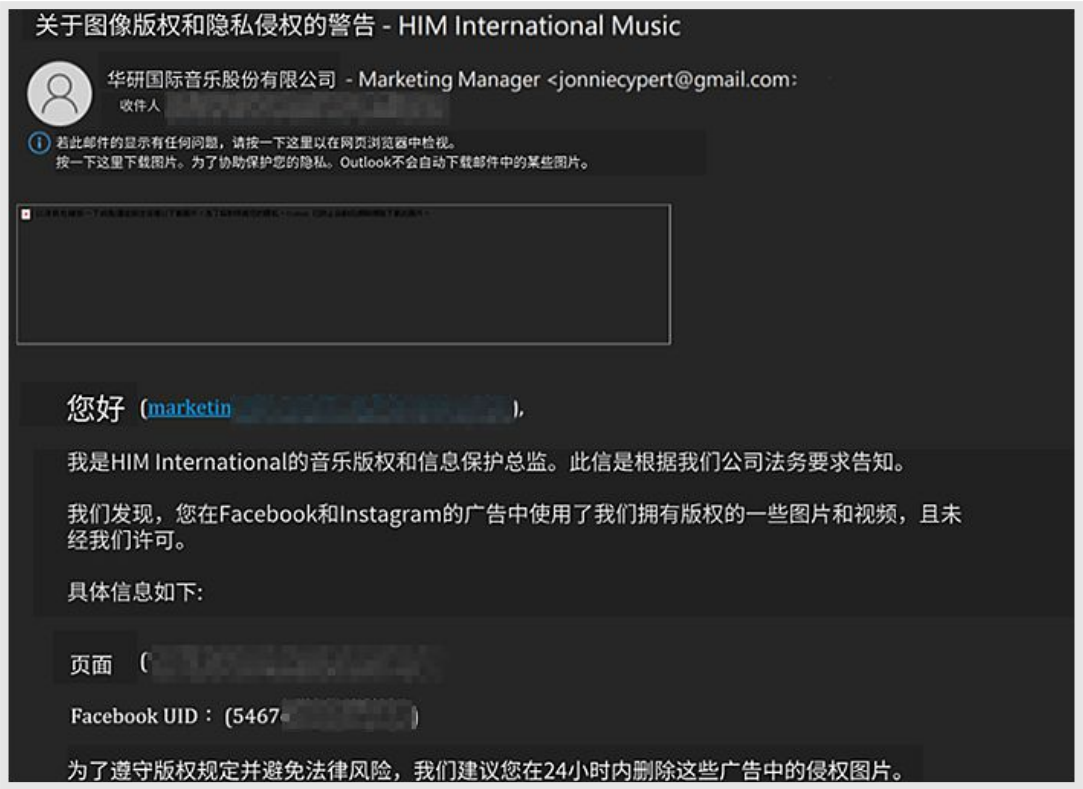
真假难辨的钓鱼邮件

有些钓鱼邮件会利用真实的通知邮件进行改造，甚至包含防范诈骗的提示链接，整封邮件的大部分超链接都指向正常的网站；**但只有一个关键的超链接，会被导向真正的钓鱼网站！这对受害者或扫描机制来说，都具有一定的欺骗性。**

以假乱真的钓鱼邮件

假冒侵权警告的攻击邮件

本季度，我们还观察到假冒侵权警告的攻击邮件。这些邮件制作得十分精细，对侵权内容的举证也看似确凿，极具欺骗性！但这些邮件来自Gmail，**通常正式的商业交流或重要通知不会通过免费邮箱发送。收到此类邮件时，只要冷静判断，便能发现其中的异常。**涉及金钱、法律等重大事件的邮件，一定要通过官方公布的合法渠道进行核实；绝对不能因为一时心急，就顺着邮件中的联系方式或超链接与对方接触，或轻率地下载相关文件。



钓鱼邮件制作十分精细

这封邮件主要诱使受害人下载他们整理的“侵权证据文件”，但**黑客并不希望自动扫描机制介入检查文件内容，因此在正式下载文件之前需要先进行“人机验证”，验证成功后才会开始下载压缩文件。**

确定为人类后，就会自动下载压缩文件案

在这份压缩文件中，包含三个文件，**最主要的是可执行的 PE 文件，其图标被替换为 PDF 图标，用以诱骗受害者打开 PDF 文件；.dll 文件则是 Remcos 后门；而另一个 .inf 文件在解压后会变得非常大，可能用于干扰扫描和检查机制。Remcos 的常见部署方式是被嵌入在伪装成 PDF 的恶意 ZIP 文件中，**声称包含发票或订单；其后门功能包括躲避防病毒检查、提升权限以及数据收集。

Remcos 以前常见的部署方式为嵌入在伪装成 PDF 的恶意 ZIP 文件中，声称包含发票或订单

结论

有调查显示，发送试探性的社交工程演练邮件可能会让员工感到紧张和压力，但这对于识别真正的钓鱼或攻击邮件可能并没有太大帮助；相反，通过样本示例进行的教育性质训练能更好的提升员工的安全意识和识别能力！钓鱼或诈骗邮件都是以社交工程为基础的攻击手段，因此，这类攻击很容易利用受害者的好奇心、恐惧、时间紧迫或其他压力的心理，使受害者疏忽大意。

面对千变万化的钓鱼邮件，仅仅通过邮件的外观来识别，有时真的很难分辨真假！但钓鱼或诈骗邮件的通常手段，都是希望受害者按照邮件提供的“渠道”进行确认或执行某个操作。如果遇到邮件要求这样的操作，请务必通过官方网站，或自行查询官方电话进行确认或联系，不要直接通过邮件提供的“渠道”进行确认，这样可以避免许多钓鱼风险！

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。