2023 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 2024 released.

2023 年**整体的电子邮件数量增长了 20%;能在第一时间被防病毒软件识别的病毒邮件虽然减少了 16%**,但这并不代表攻击趋势有所减缓; 在全局威胁的邮件数量中,**恶意链接的邮件数量增加了35%,夹带恶意文件的邮件数量则大幅增加了96%;其中利用压缩打包附件的攻击行为中, .rar 为主流,其次是 .zip ;而 419 诈骗邮件的数量相较前一年则增加了 116%。更有大量隐藏钓鱼链接的二维码邮件开始流行。**新变种,新挑战无不考验着邮件安全企业的专业功底。为企业提供优质可靠的邮件安全防护始终是守内安第一目标。

在漏洞利用方面,2023 年 3 月份披露的 **Outlook 零日漏洞 CVE-2023-23397** ,除了 2022 年底被用于攻击乌克兰国家移民局及一家经营军舰与国防科技的土耳其公司外,在 2023 年12月也被俄罗斯黑客 APT28 利用用于访问 Exchange 服务器上的电子邮箱账号,攻击目标为美国、欧洲、中东的政府机构、运输业与非政府组织等。其他数量较多的漏洞利用还有 : **利用 Zip 文件内的只读属性绕过 MotW 的 CVE-2022-41049 (MotW,Mark of the Web,为 Windows 安全功能);以及透过 Office 文件触发 OLE Package Manager 的漏洞 CVE-2014-4114。**

在钓鱼邮件方面,我们观察到以下的变化:

钓鱼链接隐藏于二维码中

将钓鱼链接隐藏在二维码中的邮件,在 2023 年第一季度末开始大量出现。这种攻击方式让钓鱼链接无法直观地被安全设备监测或人员识别,需要借助手机或其他二维码的解码软件才能解析出恶意链接。**值得特别注意的是,习惯用手机扫描二维码内容的受害者,暴露的设备由计算机转向了手机,由于企业大多数安全措施的保护对象是工作用计算机,**因此个人的手机便成了新的风险突破口。

直至 2023 年底,在邮件内附上藏有钓鱼链接的二维码变成了常见手段。**从第四季陆续开始出现将钓鱼用的二维码内嵌于 Word 附件中的加密案例,**进一步增加了信息安全工程的识别与解码难度;而这样特殊的手法与一般正常邮件的发送方式却形成了明显的区别,建议适当的网络安全宣传或教育训练,提高员工对加密邮件的认知,有效避免员工落入社交工程的圈套而点击钓鱼邮件的风险。当然,管理者也可以在邮件过滤系统中设置一些条件进行预防拦截或观察:如,检查邮件同时存在密码与加密文件,又无压缩文件,则需要提高警惕,进行进一步审核。

二维码钓鱼绑定图片

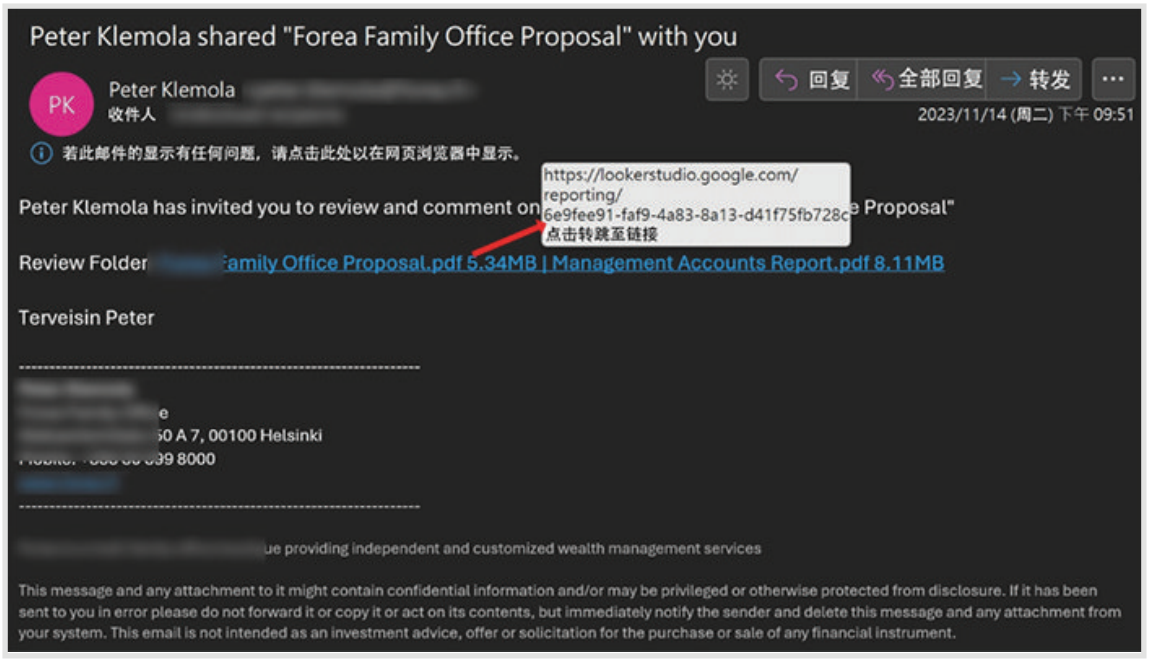
或利用邮件过滤机制中二维码的监测功能,对这些邮件进行审核。

建议开启二维码监测

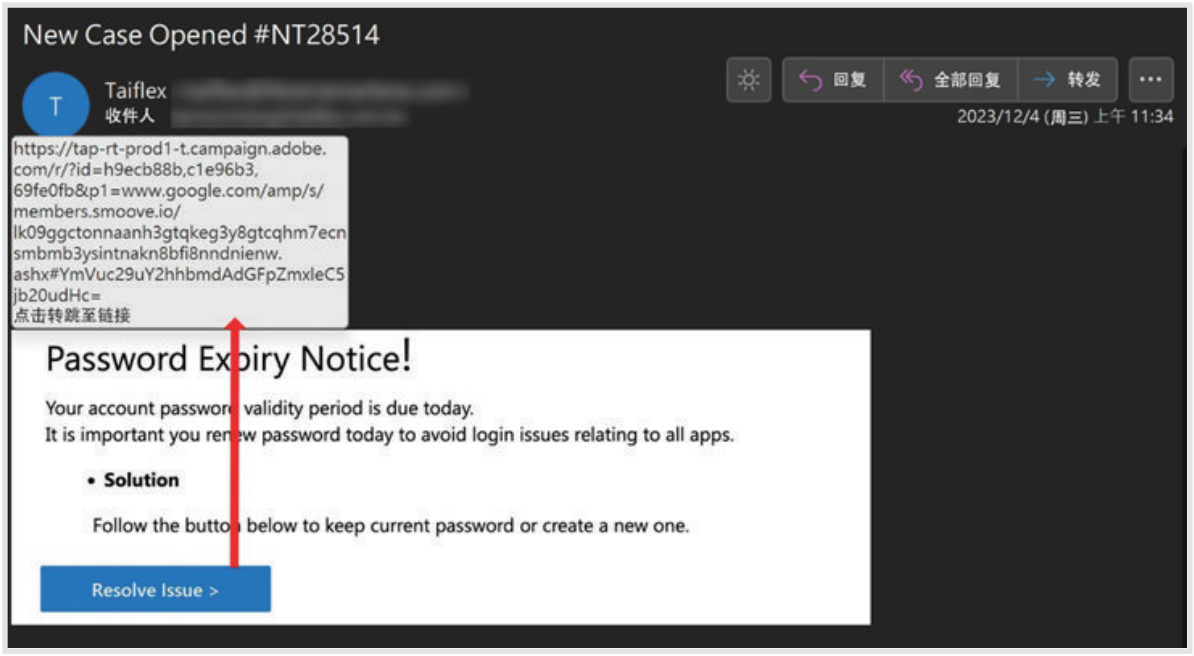
恶意链接的变化

钓鱼邮件链接为了避免被安全设备发现,同时又要能对目标发动攻击,有很多不同的做法,例如,网址跳转、滥用公开服务等。然而,大多数跳转服务的域名并不那么值得信赖,因此,若能使用值得信赖的厂商所提供的服务,不仅能躲避监测,还能使被攻击的对象信以为真。

在 2023 年第四季度,我们发现谷歌和 Adobe 的服务被用来导向钓鱼网站的案例。



Google Looker Studio 服务被利用



Adobe 服务被利用

此外,也有攻击使用 Unicode 字符替换域名中的部分字符。攻击者能对邮件内恶意链接中的域名做一些细微的改变,例如:**将小写字母切换为大写字母,或插入不可见字符等,借此绕过数据库的比对判断,而这种域名含有特殊字符的恶意网址对于浏览器和邮箱系统来说,仍能将其解析为可被收件人点击的网址。**

星际文件系统(InterPlanetary File System,缩写为IPFS)的利用

三年前,由网络服务提供商、域名管理公司、云服务商及其他基础设施管理单位与安全公司通力合作,大约 1/3 的钓鱼网站出现不到一天,便会遭到举报、关闭。而自 2022 年开始,越来越多的钓鱼邮件开始搭配使用星际文件系统 (InterPlanetary File System,缩写为 IPFS) 的钓鱼网站。**IPFS 是一个对等的分布式文件系统,舍弃了传统的集中式架构,改用遍布全球的点对点 (P2P) 数据网络,无需第三方或中央机构管理,因此,IPFS网络钓鱼内容可以很容易地分发、更难以检测、具有持久性,且钓鱼网站只能由建立者自行删除。**

鉴于星际文件系统的发展之初有其合理的应用范围,因此,利用 IPFS 产生寿命更长的钓鱼网站将会形成一种新的趋势。

2024年可能带来的变化与防御对策

2023 年 3 月微软发布的Microsoft Security Copilot 可显著提高企业安全团队的覆盖范围、速度和效率;但道高一尺,魔高一丈,**生成式 AI 带来的效益若被用于攻击,则可以预见,也能提高攻击者的效率。尽管目前尚未看到较具体的攻击应用,但生成式AI确实能在短时间内产生较以往更令人信服的文字、流畅的翻译和以假乱真的图像。加上 2023 年许多研究都指出,利用 AI 识别 AI 生成内容的准确性过低。**因此,社会工程攻击将会是未来的一大隐忧,而跨语言的社会工程攻击因为 AI 的关系将变得更加流畅!

由于攻击的升级,防御对策的部署或信息安全概念也必须跟着升级。面对来自电子邮件的威胁,人是最大的目标,运用防御设备使人避免接触威胁邮件是最基本的措施。更进一步,应该利用设备的记录、分析、调查等能力,找出企业较易遭受攻击的恶意邮件类型与人员,并通过动态调整,才能更及时地应对多变的攻击手段。

在人员教育训练方面,应本着“零信任”的态度,教育内部员工在发现可疑邮件时,不点击、不回应、不转发、并及时通报内部安全人员,以便早期发现攻击征兆,提升整体信息安全防护,应对不断演进的威胁。

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。