2023 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 2023 released.

2023 第二季，整体垃圾邮件、钓鱼邮件数量小幅上升，常见病毒附文件邮件有些许减少，来自新申请域名的垃圾邮件约较上季增加 60%。不确定是否因为生成式 AI 的出现，让语言在邮件的隔阂明显被打破：这些过去常用英语书写的诈骗邮件，转成中文内容时，变得比过去更加流利了；同样的情况也发生在过去出现在非英语语系流行的诈骗邮件，英文的诈骗内容文法变得流利，更不容易看出破绽。另一个较特别的威胁邮件是简体中文的钓鱼邮件，数量较上一季飙升许多，滥发时间落在三月底四月初。

本季特殊邮件攻击样本解析：

钓鱼邮件搭配 QRcode 进行攻击，手机成为新突破口

第二季，我们观察到大量持续且携带二维码的钓鱼邮件爆发，攻击时间持续了一整季。这波钓鱼邮件的主要特色为冒用政府或公司公告邮件，假借补助、退款或其他名义，进行钓鱼诈骗，并且不带有任何文字内文；一般钓鱼邮件常见的钓鱼连结及诱骗受害者点击的社交工程文字内文，则被攻击者分别以 QRcode 及图片格式的方式隐蔽，藉以躲开传统的超链接及文字扫描。

以 QRcode 及图片格式的方式隐蔽钓鱼链接及社交工程文字

我们观察了许多样本，发现攻击者除了试图以 QRcode 及图片格式妨碍扫描外，也试图挑战邮件扫描机制对图片的解析功能，例如同一类型的攻击，图片夹带的方式就有一般图片附件、非图片附件及通过 HTML 的 <img> tag 将图片内嵌于内文三种方式。


```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">=0D=0A<HTML><=
HEAD>=0D=0A<META content=3D"text/html; charset=3Dutf-8" http-equiv=3DConten=
t-Type>=0D=0A<META name=3DGENERATOR content=3D"MSHTML 11.00.9600.18315"></H=
EAD>=0D=0A<BODY>=0D=0A<P><img src=3D"cid:_Foxmail.1@a6387981-3c20-49fa-ac38=
-b8738b385aba" style=3D"width:518px;height:703px; "id=3D"img_insert_9303830=
3505887912752860510530"></P></BODY></HTML>=0D=0A
--------=_002_NextPart451744533084_=----
Content-Type: application/octet-stream;
  name="MRUL9PZcXMus.yh02A"
Content-Transfer-Encoding: base64
Content-Disposition: inline
Content-ID: <_Foxmail.1@a6387981-3c20-49fa-ac38-b8738b385aba>

/9j/4AAQSkZJRgABAQEAYABgAAD/2wBDAA8KCw0LCQ8NDA0REA8RFiUYFhQUFi0gIhslNS84NzQv
NDM7QlVIOz9QPzM0SmRLUFdaX2BfOUdob2dcblVdX1v/2wBDARARERYTFisYGCtbPTQ9W1tbW1tb
W1tbW1tbW1tbW1tbW1tbW1tbW1tbW1tbW1tbW1tbW1tbW1tbW1tbW1v/wAARCAK/AgYDASIA
AhEBAxEB/8QAHwAAAQUBAQEBAQEAAAAAAAAAAAECAwQFBgcICQoL/8QAtRAAAgEDAwIEAwUFBAQA
AAF9AQIDAAQRBRIhMUEGE1FhByJxFDKBkaEII0KxwRVS0fAkM2JyggkKFhcYGRolJicoKSo0NTY3
ODk6Q0RFRkdISUpTVFVWV1hZWmNkZWZnaGlqc3R1dnd4eXqDhIWGh4iJipKTlJWWl5iZmqKjpKWm
p6ipqrKztLW2t7i5usLDxMXGx8jJytLT1NXW19jZ2uHi4+Tl5ufo6erx8vP09fb3+Pn6/8QAHwEA
AwEBAQEBAQEBAQAAAAAAAAECAwQFBgcICQoL/8QAtREAAgECBAQDBAcFBAQAAQJ3AAECAxEEBSEx
BhJBUQdhcRMiMoEIFEKRobHBCSMzUvAVYnLRChYkNOEl8RcYGRomJygpKjU2Nzg5OkNERUZHSElK
U1RVVldYWVpjZGVmZ2hpanN0dXZ3eHl6goOEhYaHiImKkpOUlZaXmJmaoqOkpaanqKmqsrO0tba3
uLm6wsPExcbHyMnK0tPU1dbX2Nna4uPk5ebn6Onq8vP09fb3+Pn6/9oADAMBAAIRAxEAPwD0Siii
gAooooAKKKKACiiigBG6U2nN0ptABRRRQAUUjMFUk9BWZfaisURdm8tB+ZrGrWjSWu5cIObsjReV
E+8wFM+1Q/3v0rjbnW55Mm3j2oP42GTTLa+uJQWmvGUDjAAHPauV4mpukdywMl1G8jtRdRH+MCpVZ
WGVINcCdTvY5NgmMmOzIK0tP1v8AeiO4BhfpkHimsVNaywWgp4GUVdHW0VVt7reQj9exq1XXTqRqK
8ThlFxdmFEFH16VoSFFZMmqhdRXac2agrLKANoc9Ofzz9adfXlyt5bO2hibzWvecnYBvTxwPer5G
```


非图片附件方式夹带


```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<HTML><HEAD>
<META content="text/html; charset=utf-8" http-equiv=Content-Type>
<META name=GENERATOR content="MSHTML 11.00.9600.18315"></HEAD>
<BODY>
<P><img src="
ZoPMUYHynFaFqt2C32p4mGPl2AilOSaQRWrOfneOSRZJr0yEdpYW259hS3EiXCrvnjXH3WW3YEfjWjLosstx5z3jEg5XcgOKdPpMtygWe
MQxFVDJLeQubaFHtVukkMkUTrubqxwScAUAben6zLqUO6GO1VypKxm5y+R6jb0qKfxDLZxW5uraKKSTh0eYhkPrtCk7eOtZ2jNJe3CTPJ
kk3BgAcDoM569qtKiQ6hYW63zTvExBiJT5AEPOAAfzoQM26KKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigA
qk2lzJJIkVtF+8iMW63hSJBkjJPzknGPSuhooArCSZbwxNFmFlyki9iOoP9KnclVyFLewp1FAGVqD3V1biNNOuARIj/M0fQMD/f8AarDT
LqMMs7+WfKZkEbswQqASe2evtQBo/2xpu8p9ut8gZz5gx+fSrCXETymNXBbaGx6g9x61yYukDmf7U2WUDibJxn2uN3fpV6K4ni1dU23CK
IVQMkk4Aqs2p2CMVe9tlYdQZVB/nQA0abCNhYu7IhLyFFkV1y2SMEEDPpxTv7QswUH2uDnkKDzB8309amEqG
RxIiMfmQY54I/TFNgar6jbosTEyN5kCROx145wBkdR1p0F7BOJCjMPPK+/5iMhXjPRgO1c1CrRwkky2r5MMkjBXWDcPkyQYh09jzVy3Y
70YPy57kDsajGlwYiG+ceVEIl2ysmQNf3cslmKK/xkAnnH86jmv703F49PFP12vIFP60AV49Jihufv/ujr
2VkmXpL22icpJcRIw6hnANBvYPs8kySLLjxVyiUBQCMkEDrlufripLUm5tpIljV0R1LLGFy/c5yx9PXNLm6FexSip
WnR6fK0TxTBArkEtk0eBjgbQBwK1aKKXXi/ayM46BiZUI0IbLFHzY6c09rrWb1F2Fb1QnUk92Z0lvcrA6+X
Cb3/n5t//AB7/AAoA6D/hKdG/4Qm9/wCfm3/8e/8AAoo4Qm9/wCfm3/8e/woA6D/AISnRv8Anp/8e/8AAoA6D/AISnRv8An
AkYrX/gf/AKA1ABrGgTaRDHL+NHIHbaAoNa/gL/s1bWu6P/bNvF+k7G3Z2bs8fUgz+DZCiFbv7UoJGzbtz7nn1oA2dX8R
B/wB/U/xr0GaRYYXlf7qKWKo7K5F5ZxXKqVEqhqEqhgD2p11EZ7WaIb1kgIHBkRlz9RigdmdbdbSaffaVcW0JkLuBjKYHUGuNroNR8Kz6fZ3
AMjxZ/wAi7df8A/8AQ1rn/Av/rj/wCzugAP/AENa5/wL/AHK4//ACAp/3sP+AAh5/KP+Pf+rq/h2pAKP+f+y1yFdf49/5cP8AgPz2Pr
qtHExRmlM7x4LNt+7830QSTgqWdcgKUC/Ilw6SzYUpL5wbODAp16Yz90H1FZdgl5I4/fyhY48lEV+VWBOSGUgnj2pP
D/aiCORpIJ42jVW8tgu5SbTgyuCeTjPJ4/E1P5Ulx1CxLJcXFizJ5QjiGFIFhijF+ck9cfrQBYe+McStbIxIc
```

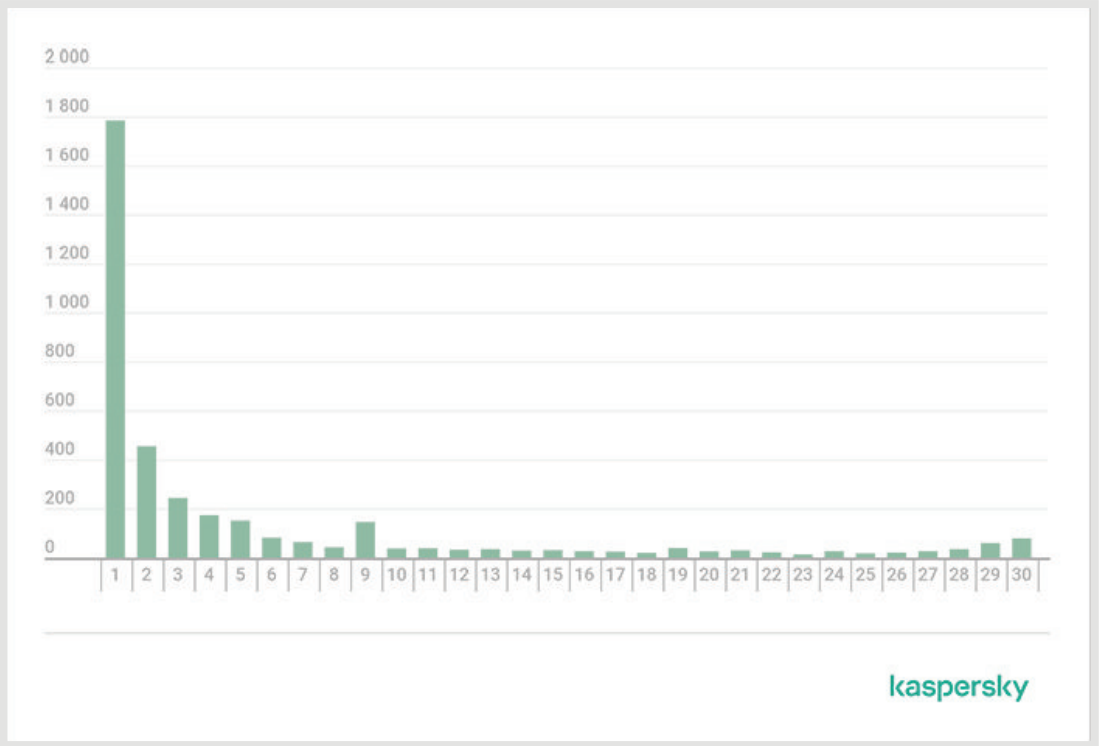

通过 HTML 的 <img> tag 将图片内嵌于内文

这样的手段除了可以尝试突破邮件扫描机制外，攻击者也可能藉由这些攻击穿透成功的统计，推测邮件扫描机制对夹带图片的处理方式或实作上的弱点，用以改良后续的攻击手段。

此外，由于恶意连结藏在 QRcode 中，所以惯于用手机扫描 QRcode 内容的受害者，曝险的对象由计算机转向了手机，企业较多保护措施的终端对象通常是工作用计算机，而个人用的手机就成了新的风险突破口。

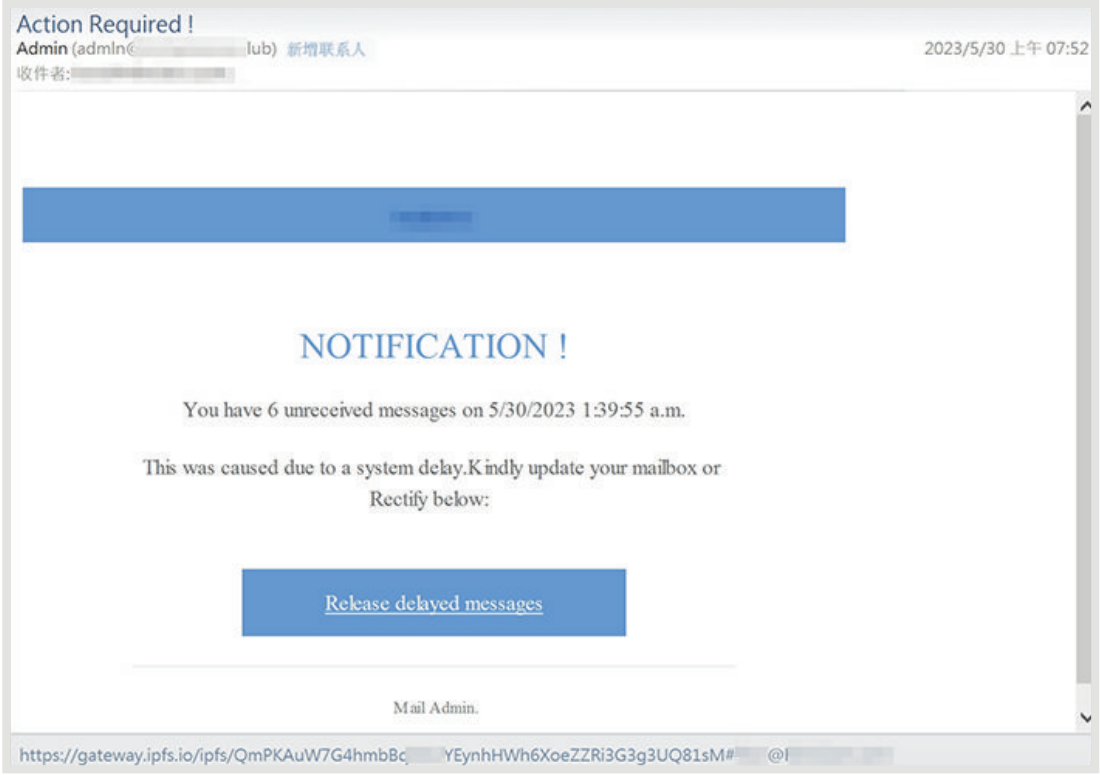
存活时间长，难以封控的钓鱼网站

在过去，钓鱼网站的生命周期都不长，尤其是寄宿在有管理的服务主机或域名上的钓鱼网站。根据卡巴斯基公司在 2021 年揭露的钓鱼网站活动统计，多数的钓鱼网站在一天后，甚至是出现的数小时之后，就已经处于非活动 (inactive) 状态。



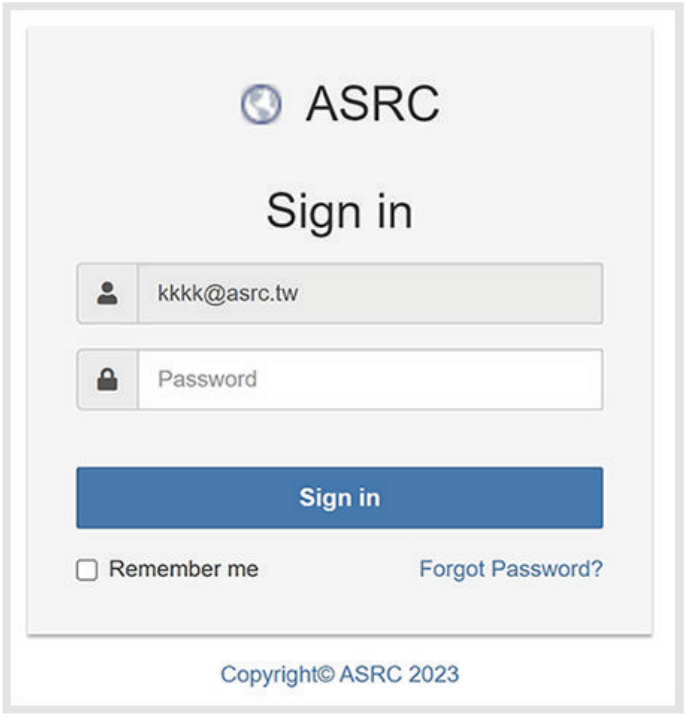
钓鱼网站生命周期统计 引用来源：https://securelist.com/phishing-page-life-cycle/105171/

第二季开始，我们明显观察到有许多的钓鱼邮件开始搭配星际文件系统（InterPlanetary File System，缩写为 IPFS）作为钓鱼网站。IPFS 是一个对等的分布式文件系统，没有采用传统的集中式架构，而是使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，并且具有持久性，这样的钓鱼网站只能由建立者自行删除。



利用 IPFS 的钓鱼邮件

以 IPFS 建构的钓鱼网站，存活时间非常久，直至截稿前，这些恶意的钓鱼网站仍在正常运行。并且这个钓鱼网站会根据攻击目标 E-Mail 账号的域名进行页面的标题变化，藉此降低戒心；当受害者第一次输入密码时，系统会响应密码错误，再输入第二次窃取密码后，将页面重新导向至目标 E-Mail 账号的域名。



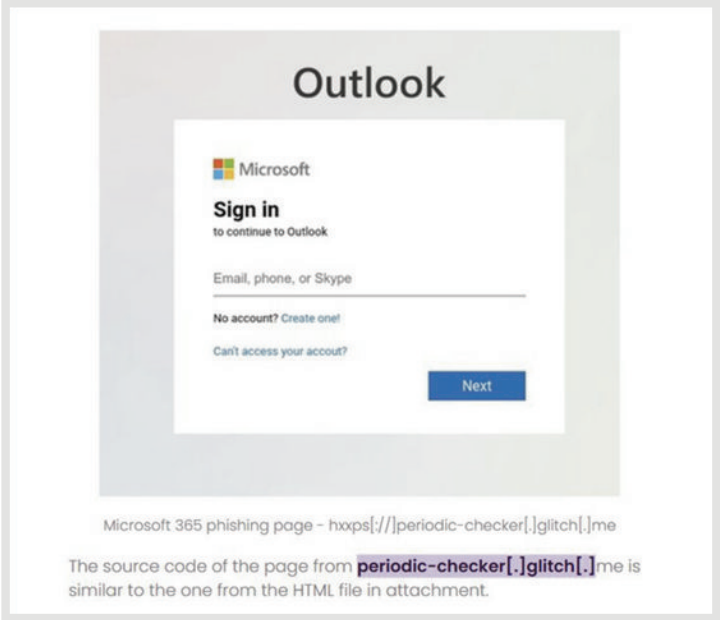
该钓鱼网站会根据攻击目标 E-Mail 账号的域名进行页面的标题变化

黑客滥用 Glitch 平台散布钓鱼邮件，骗取 Microsoft 365 账号

同样，网络上关于最新邮件安全的内容也屡见不鲜，就在昨日，具 IT 之家 7 月 12 日消息，网络安全分析公司 Vade 日前揭露有黑客利用 Glitch（网站代管服务平台），平台上部署钓鱼邮件服务器，并针对 Microsoft 365 用户进行钓鱼邮件攻击。

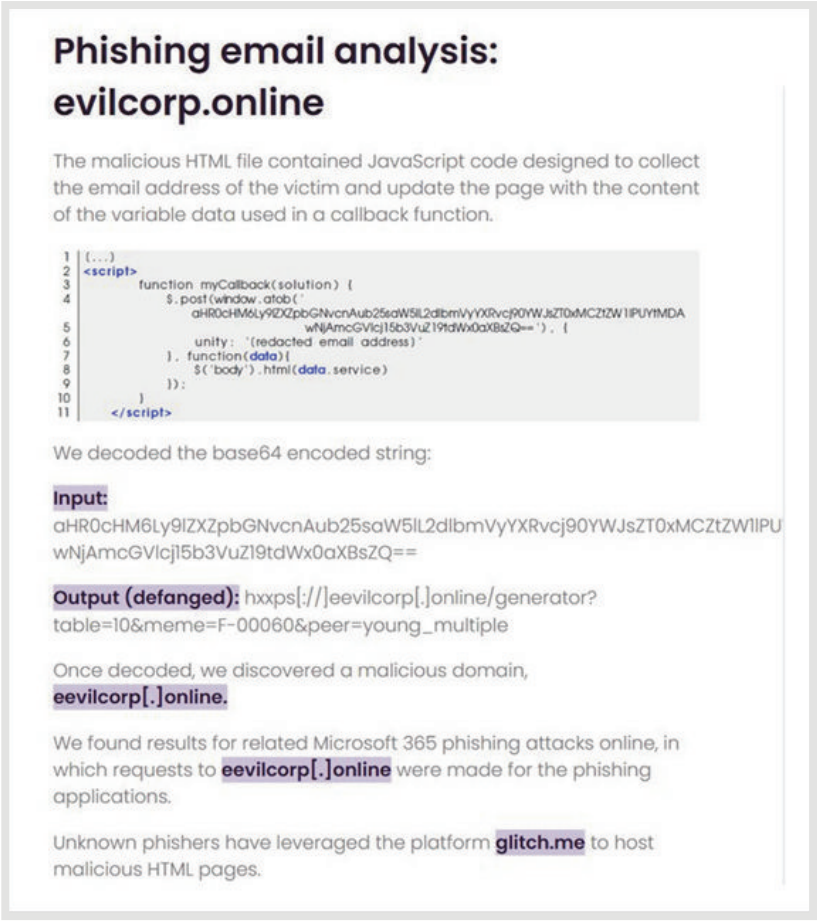
图片来自 Vade

据悉，黑客在钓鱼邮件中夹带含有 JavaScript 程序代码的 HTML 附件，一旦收件人按照邮件中的指示打开附件，就会看到伪装成 Microsoft 365 登录页面的钓鱼网页，在这一步，一些没有那么仔细的用户就会在其中输入账号密码，将自己的信息主动交给黑客。



图片来自 Vade

研究人员分析 HTML 代码后，发现黑客的钓鱼邮件是从名为 eevilcorp [.] online 处发出，该钓鱼网站实际上是部署在网站代管服务 Glitch 上，黑客滥用了其托管服务，并绕过了相关网络安全系统，得以分发传播此类钓鱼文件。



图片来自 Vade

除了 Microsoft 365 用户外，研究人员同时注意到，黑客也假借登录 Adobe Document Cloud 的名义发送相关钓鱼邮件，要求收件人登录伪装的网站，输入 Office 365、Outlook、AOL 或 Yahoo! 账号密码信息进行身份验证。

- 本公众号最后有关Vade的案例文章转载自互联网，文末已注明出处，其内容和图片版权归原网站或作者本人所有，若有无意侵权或转载不当之处请联系我们处理！

结语

利用 IPFS 建设的钓鱼网站，由于其分散系统的特性，没有中央机构可以对它稽查或管理，再加上 IPFS 还可搭配缩址、转址等功能进行更复杂的蒙骗或躲避稽查，未来可能会变成钓鱼网站存在的主流趋势。

企业防御最直接的方式是避免接触这类的钓鱼邮件，采用有效的邮件扫描机制是一个好方法；此外，在无必要使用 IPFS 的前提下，直接隔离 IPFS 网址，也可让此类风险大幅度降低。

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。