2022 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 2022 released.

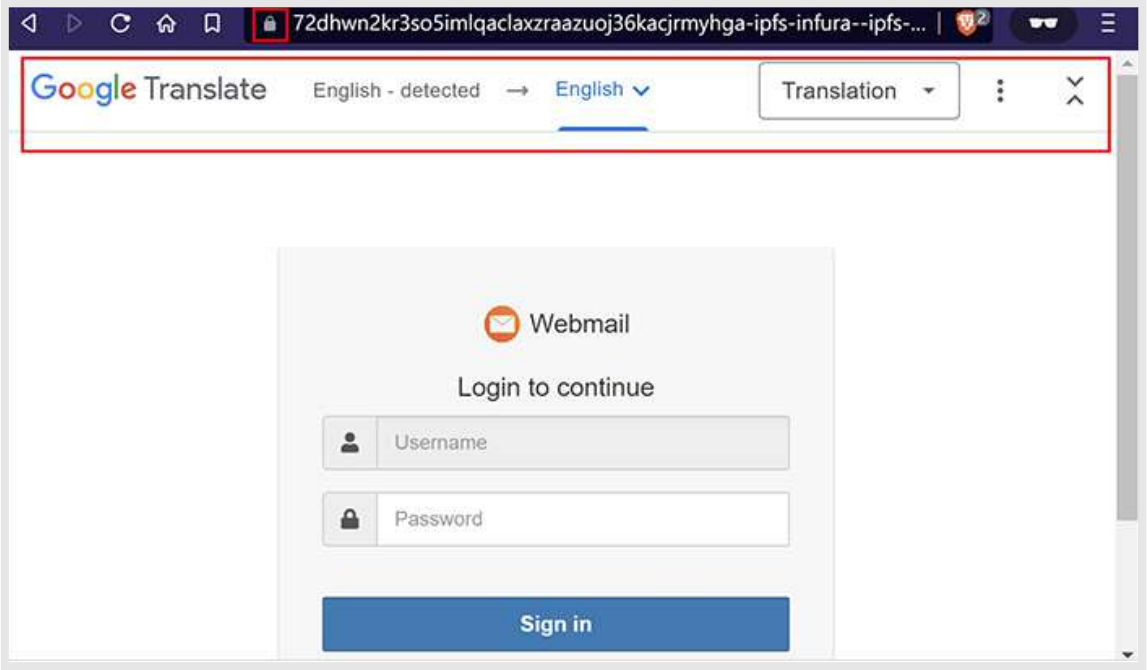
时间来到了今年第三季度，随着国际局势紧张，带有恶意链接的攻击邮件较上一季爆增了4倍、带有HTML的钓鱼邮件则翻了3倍；且诈骗及APT攻击、漏洞的利用都比上季度略有上升，但整体垃圾邮件、常见病毒邮件的数量都有所下降。值得注意的是利用恶意PDF文件格式进行的攻击有明显增加的趋势。以下为本季值得特别留意的特殊攻击手段：

被利用的 Google 翻译

Google翻译本身支持了翻译整个网站的功能，并且可将翻译结果页以链接传送给他人，让他人也可直接看到翻译后的结果，翻译结果的网址是Google翻译的合法网址，所以若是将钓鱼网站交给Google翻译后，取得这个网址，再放入钓鱼邮件中传播，便可利用合法掩护躲过众多安全检测。

钓鱼网站由 Google 翻译后，穿上了白马甲

收件人万一点击链接则会直接跳转至钓鱼网站且大部分浏览器的钓鱼保护功能不会提醒。不过，如果我们仔细观察，还是能发现异常：我们可以看到Google翻译列的控制选项，正常的登入网站并不会出现。



识别的秘诀是，会看到 Google 的翻译列

除此之外，网站本身的原码也做了一些特定的编码保护，这有助于网络爬虫不易识别出这是一个钓鱼网站，也让这类钓鱼网站可以存活的更久。

网站本身的原码也做了一些特定的编码保护以躲避爬虫检查

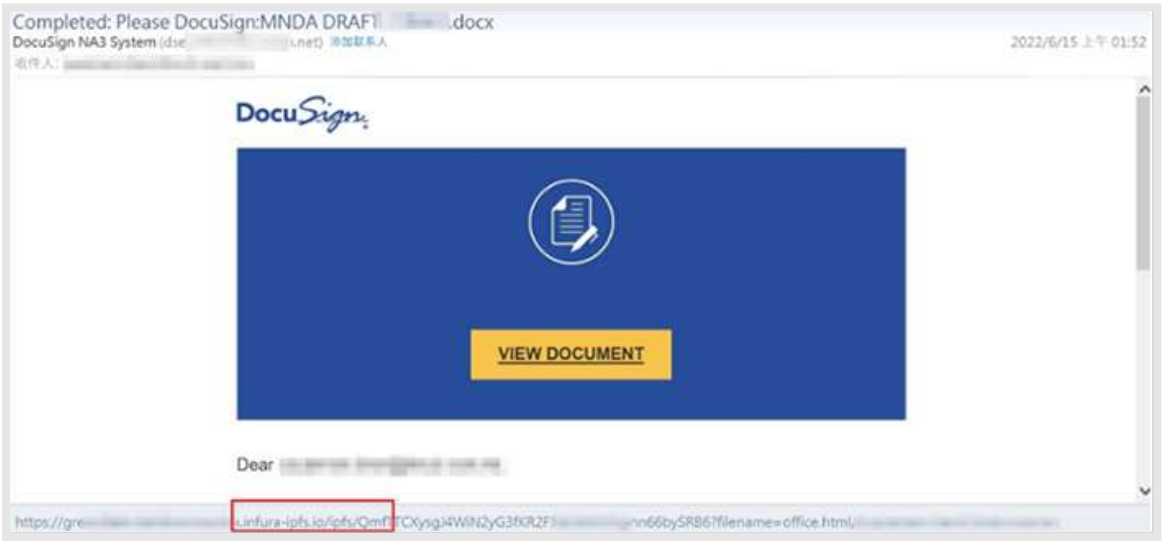
通过 IPFS 协议续命

在上述 Google 翻译被利用的例子，实际上钓鱼邮件的网址是：

hxxps://72dhwn2kr3so5imlqaclaxzraazuoj36kacjrmyhga.ipf[redacted]'ab.html

而在经过了 Google 翻译之后，网址会跟着改变。不过，目前中国地区 Google 翻译服务已于今年10月1日正式关闭。目前也算是从物理端解决了该问题，不过可能很快就能在其它平台看见利用此手段的钓鱼邮件。

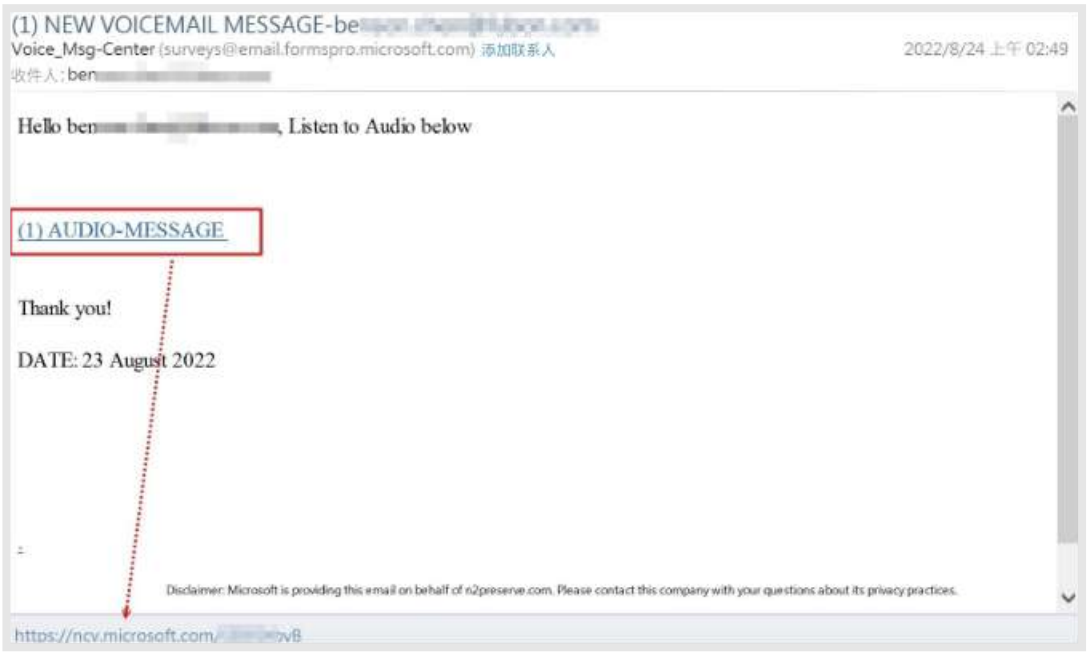
我们可以看见原始的网址主域为infura-ipfs.io，这是利用了星际文件系统所实现的分布式储存。星际文件系统（InterPlanetary File System，缩写为IPFS）是一个旨在实现文件的分布式储存、共享和持久化的网络传输协议。它是一种内容可追溯的对等超媒体分发协议。在IPFS网络中的节点构成一个分布式文件系统。传统的恶意文件寄存于单一网站，一旦服务器宕机或联机断线，恶意文件或是钓鱼页面就无法使用。但在IPFS上，文件可利用多个网络节点传送，确保内容长久保留，大幅度提高了恶意网站的生命周期，对于恶意流量的侦测也变得更加困难。



恶意页面或文件开始利用 IPFS 协议躲避封锁

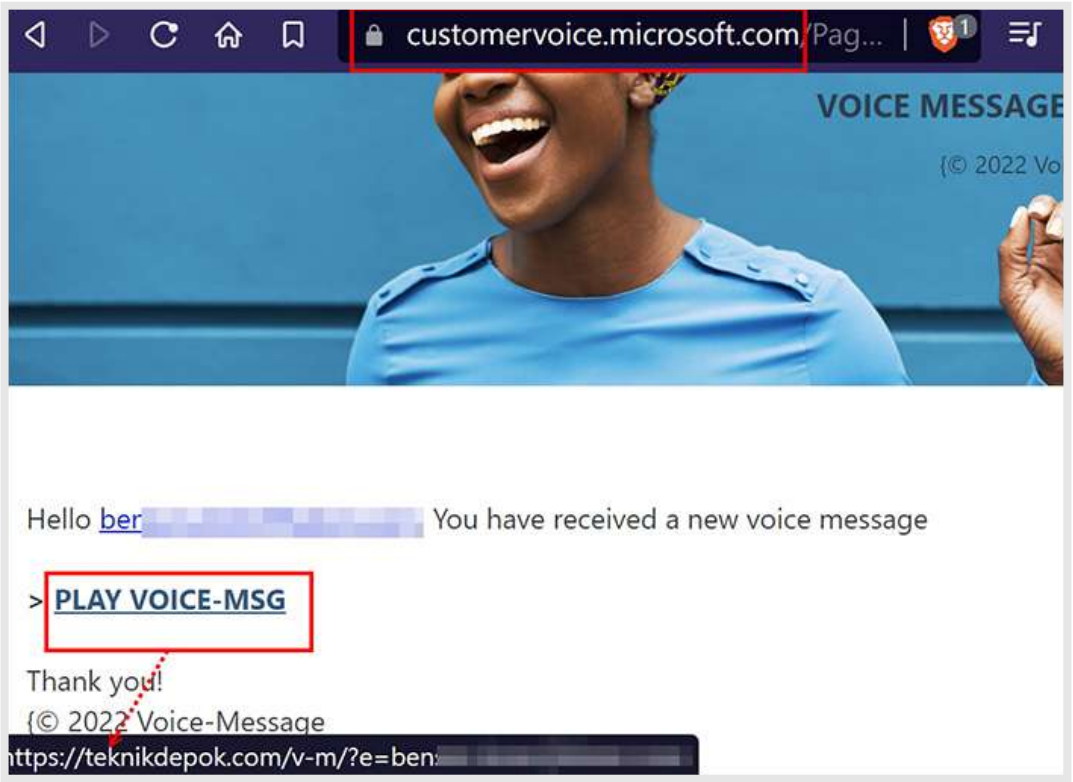
被利用的在线问卷

钓鱼邮件内容简洁，主要以邀请聆听语音信息作为社交工程的诱骗手段，而语音信息的链接，则寄宿于微软 ncv.microsoft.com。



携带了位于 ncv.microsoft.com 的钓鱼链接

点击该链接时，会连到一个钓鱼的中介页面，这个页面是存放在微软服务器上真实合法的网址与网页。但这个页面却附带有一个恶意的钓鱼链接，并利用了微软 Dynamics 365 Customer Voice 问卷调查功能，为了避免受害者发现，中间被嵌入了大量的空白，让受害者不会直接看到微软 Dynamics 365 Customer Voice 问卷调查功能页的页尾。由于是以合法网域掩护的钓鱼网页，浏览器不会弹出任何警告。

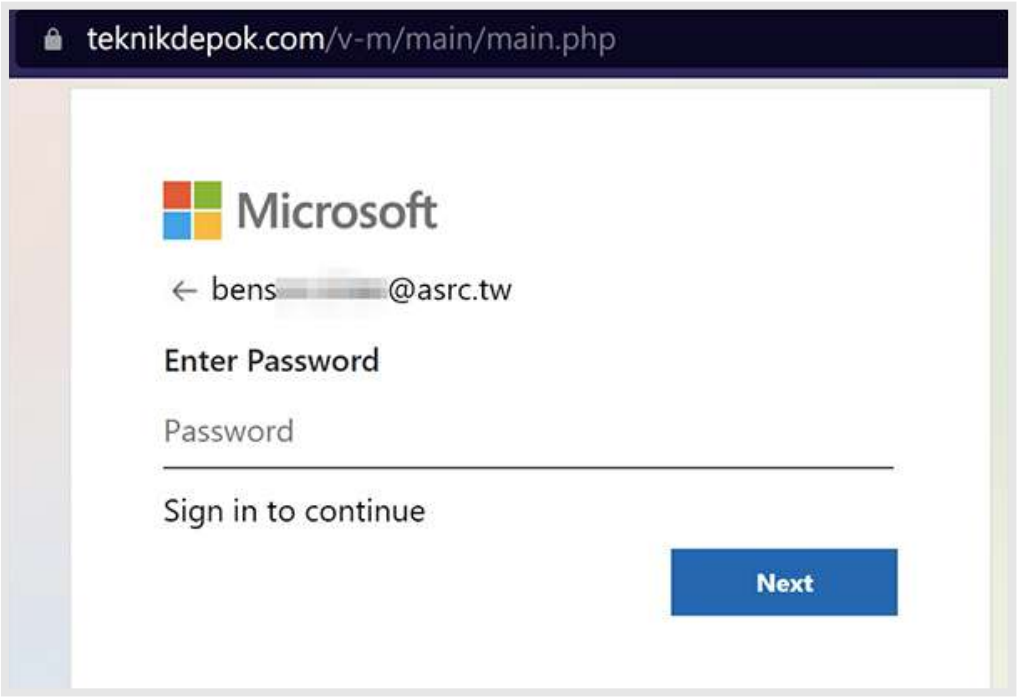


钓鱼攻击滥用了微软的在线问卷调查机制

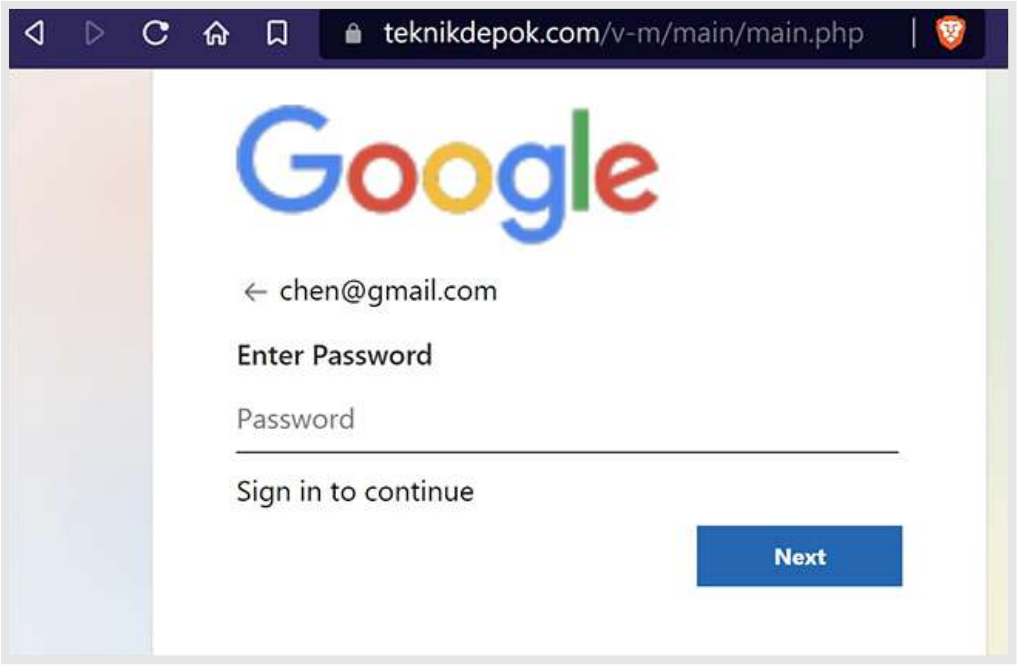
当受害者不慎点击真正的钓鱼链接页面时，并不会马上开始进行钓鱼动作，会先进行人机身份验证（CAPTCHA）筛除自动爬虫检测，让真正的钓鱼网站继续潜藏在暗处。

人机验证（CAPTCHA），用以筛除自动爬虫检测

通过人机验证 CAPTCHA 测试后，来到真正钓鱼的阶段，其目标是为了骗取某些网络服务的密码。攻击者可能考虑到后续会大量运用发送钓鱼邮件，并为了增加可信度的需求，钓鱼网页会根据要骗取的电子邮件域名的不同，页面的Logo图案会有一些不同的变化。



目的是为了骗取某些网络服务密码



logo 随页面变化

在这个例子中，可以看见钓鱼邮件用了众多方式，让人相信它的真实性，并且确认被钓鱼的对象是真实的人类。

总结

通过本季的几个案例可以观察到，配合攻击邮件的钓鱼网站除了大量地使用合法公用机制来掩护非法行动外，也会试图躲避安全人员的自动扫描检查，并且利用各种先进的技术设法提高钓鱼网站、恶意文件的存活时间。攻击邮件中若不直接携带攻击程序或文件，多半都将其真正的攻击武器藏于外部的网站上，触发方式多数需要透过浏览器及社交工程手段。因此，着重邮件安全的同时也需要留意浏览器的安全，并需要养成及时更新的好习惯。

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。

更多信息请参考 www.asrc-global.cn