2022 守内安信息科技 & ASRC
第二季度邮件安全观察

ASRC

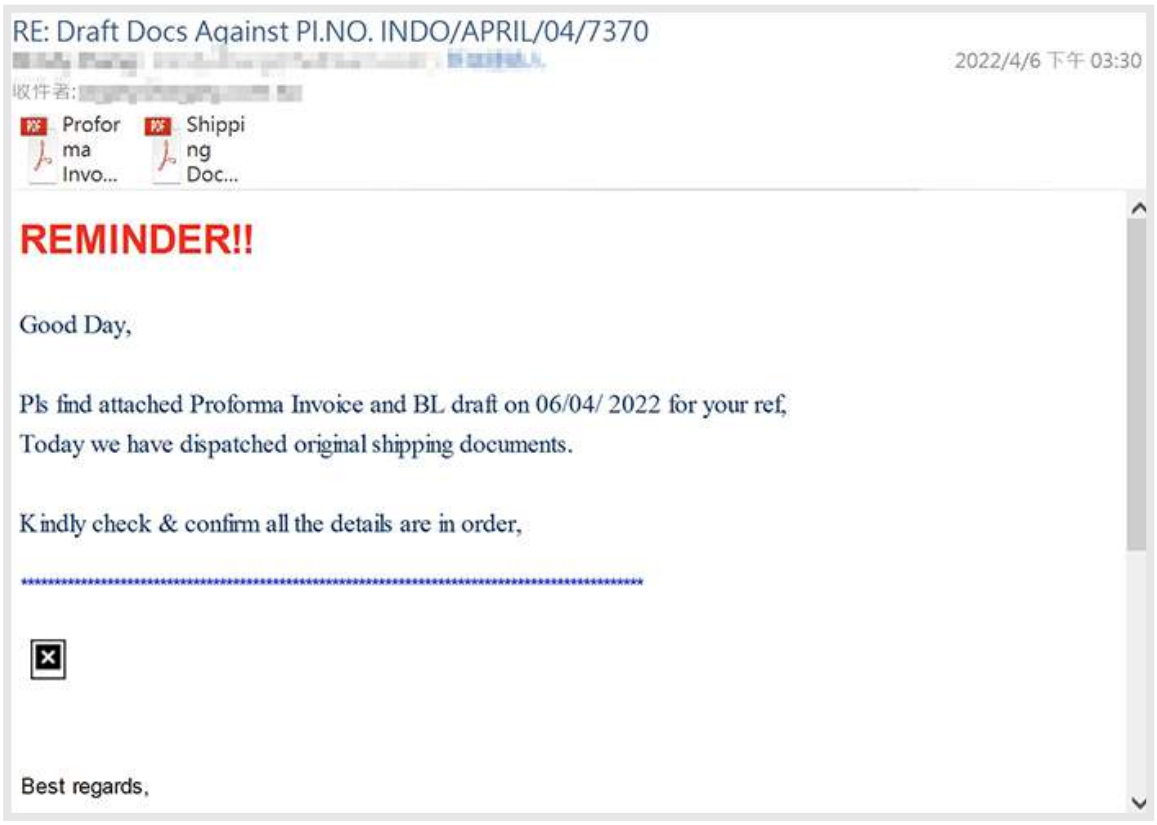
Spam Mail
Virus Mail
Malicious Mail

July 2022 released.

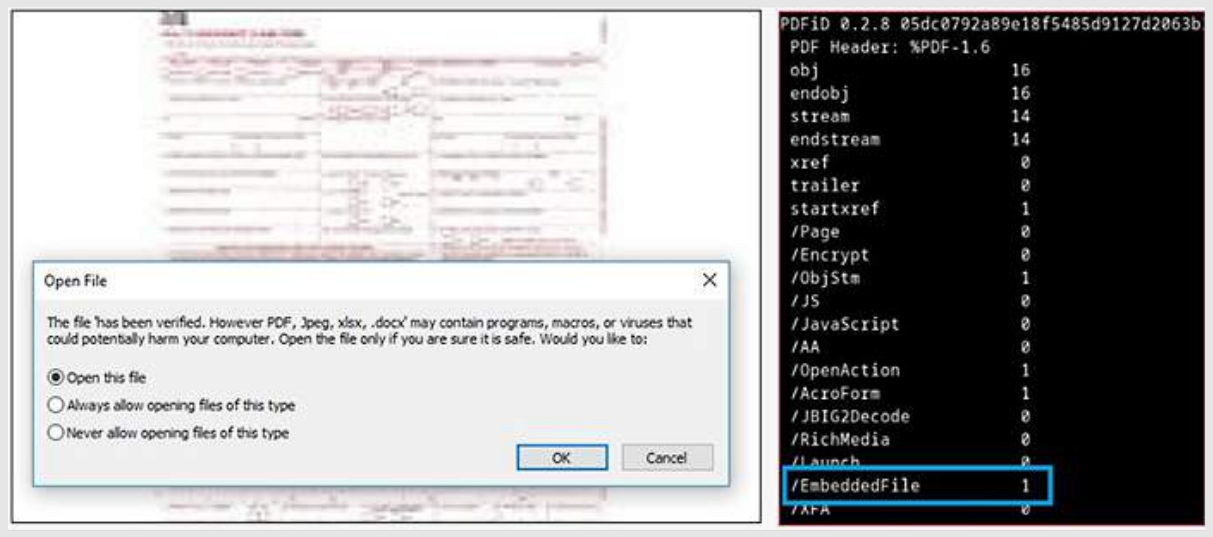
根据 ASRC 研究中心与守内安联合报告，本季来自电子邮件的攻击，仍以钓鱼邮件为主；其次是带有加密病毒附件的邮件，其数量较上个季度约增长 4 倍。通过大量联机攻击的次数约为上季度的两倍。同时本季度也有新的攻击手法及漏洞被发现，需对后续漏洞利用情况提高警惕。

通过 PDF 掩护夹带恶意 Office 文件

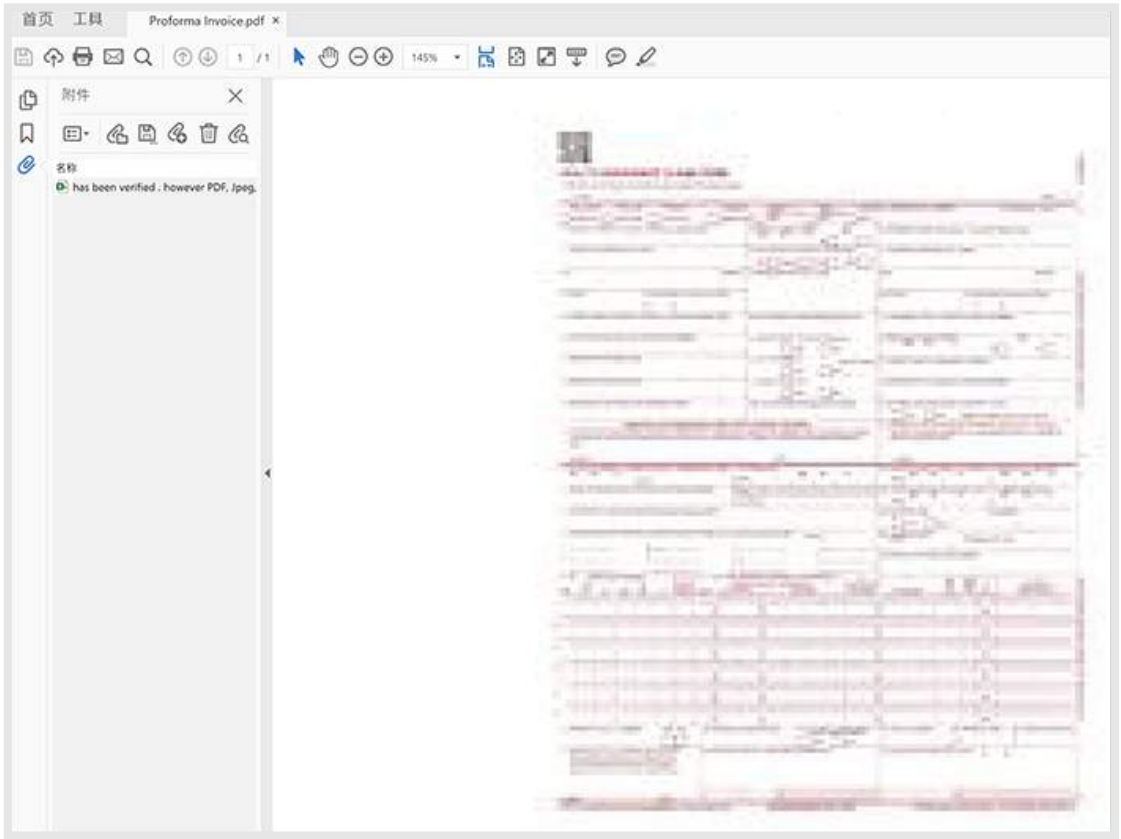
本季我们发现有夹带恶意 Office PDF 的格式文件。这种恶意文件本体，是一个利用了 Excel 默认密码加密过的恶意 xls 文件，所利用的漏洞为 CVE-2017-11882，内嵌于 PDF 的附件内，利用 PDF 编码作为掩护，使得防毒或网络安全检测软件极难发现。当受害者不慎通过 Adobe Acrobat Reader 等 PDF 阅读工具开启了这个恶意的 PDF 文件时，会自动询问是否要开启其中的恶意附件，若受害者不慎同意开启，则恶意文件会立即在受害者的计算机上安装后门程序。要防范此类攻击，除了采用较好的网安查毒检测机制外，在打开文件时的任何软件警示最好都不要轻易忽视！



夹带恶意软件的 PDF 文件



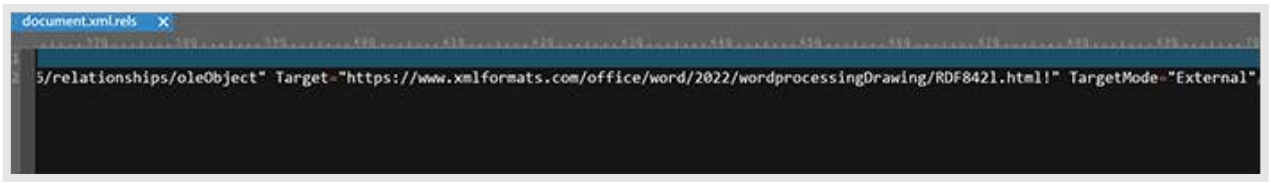
Adobe Acrobat Reader 等 PDF 阅读工具开启了这个恶意的 PDF 文件时，会自动询问是否要开启其中的恶意附件，若不同意则不会触发后续的恶意程序；若通过 Chrome 等功能较单一的 PDF 阅读工具，打开时则不会显示该 PDF 内嵌有附件



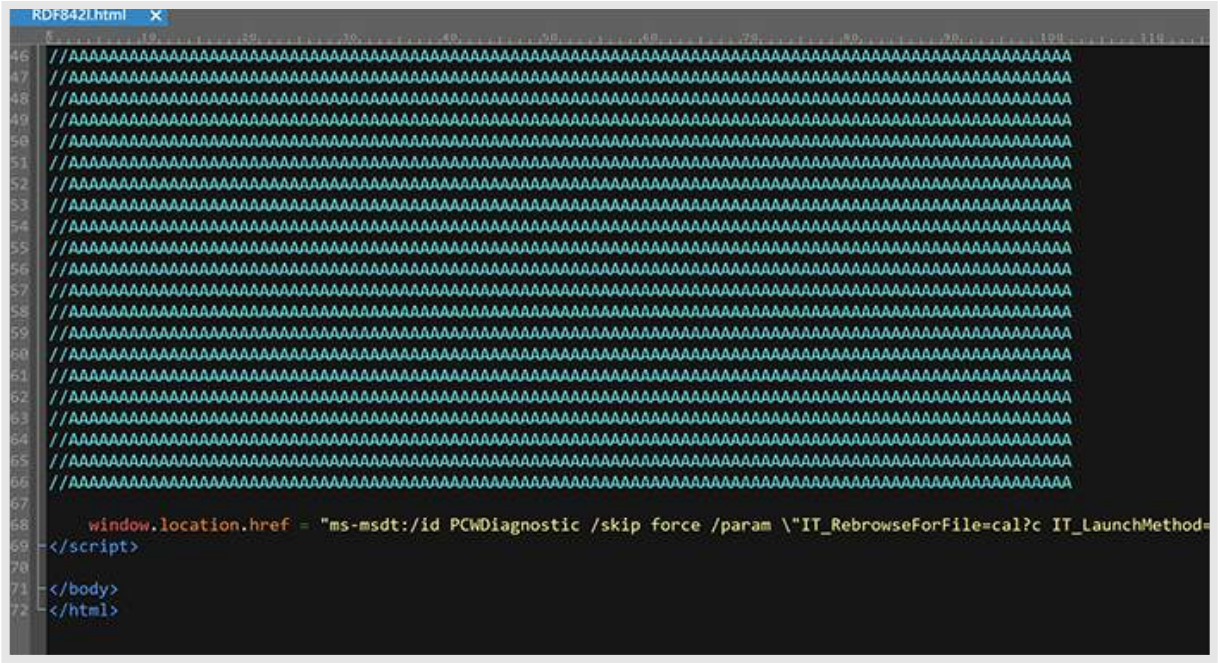
恶意代码内嵌于附件的 PDF 中，利用 PDF 编码作为掩护，使得防毒或网安检测软件极难辨识

Follina 攻击，通过电子邮件触发

微软于 5 月 30 日公布位于 MSDT (MS Support Diagnostic Tool) 的 Windows 漏洞 CVE-2022-30190，这个漏洞被命名为 Follina，因为一开始发现的攻击文件名有着 0438 这个数字 (05-2022-0438.rar)，0438 是意大利 Follina 的区号，因而得名。这个漏洞是 Windows 本身的漏洞，但触发方式可通过电子邮件来进行：在电子邮件中以附件文件夹带一个恶意的 Office 文件或是 RTF 格式文件，并利用 Office 程序向外抓取一个恶意的 HTML，再借此恶意 HTML 使用「ms-msdt」MSProtocol URI scheme 以加载一段程序代码，触发 PowerShell 执行。



透过 WORD 的 XML 向外请求恶意的 HTML ole 对象



恶意的 HTML 通过 Office 程序的权限执行后，使用「ms-msdt」MSProtocol URI scheme 以加载一段程序代码，触发 PowerShell 执行

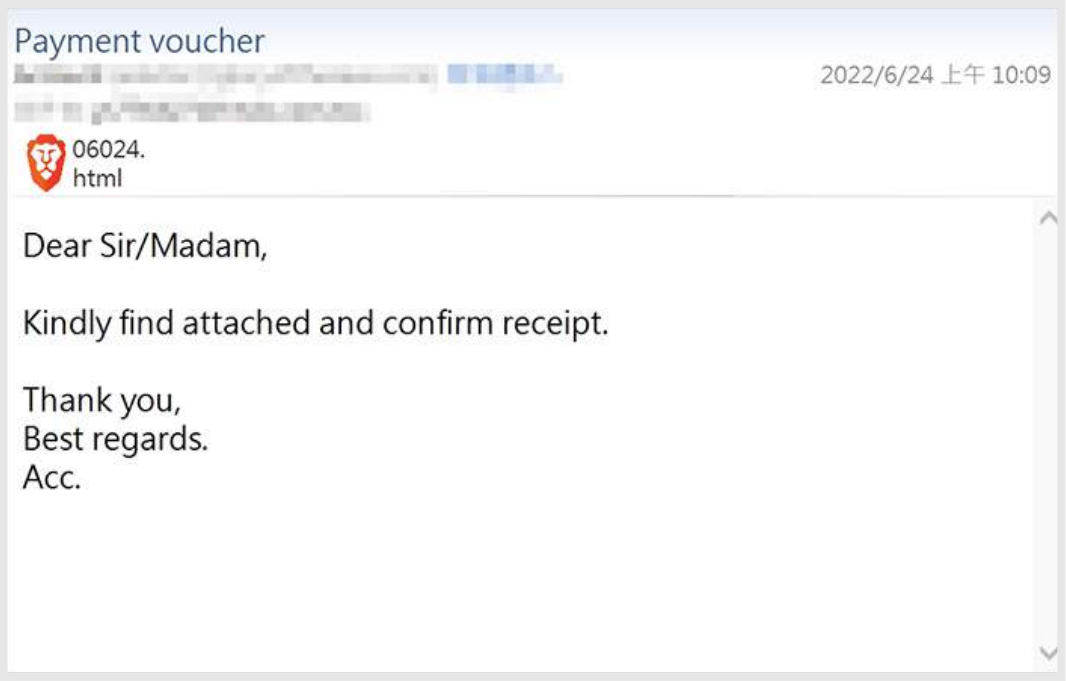
微软 MSDT 延伸漏洞 - DogWalk

与 Follina 同样是 MSDT 通过电子邮件的利用，另一种攻击方式，是通过电子邮件寄送恶意超链接的方式，令受害者下载一个恶意的 diagcab 文件，并以社交工程的方式诱骗受害者点击才能触发。触发后利用路径/目录穿越（Path Traversal），允许攻击者将任何文件，存在文件系统任何地方，比如 Windows 的「启动」文件夹中，进行长期的潜伏，并且这个过程完全是静默的。这种攻击方式有另一个昵称为 DogWalk。

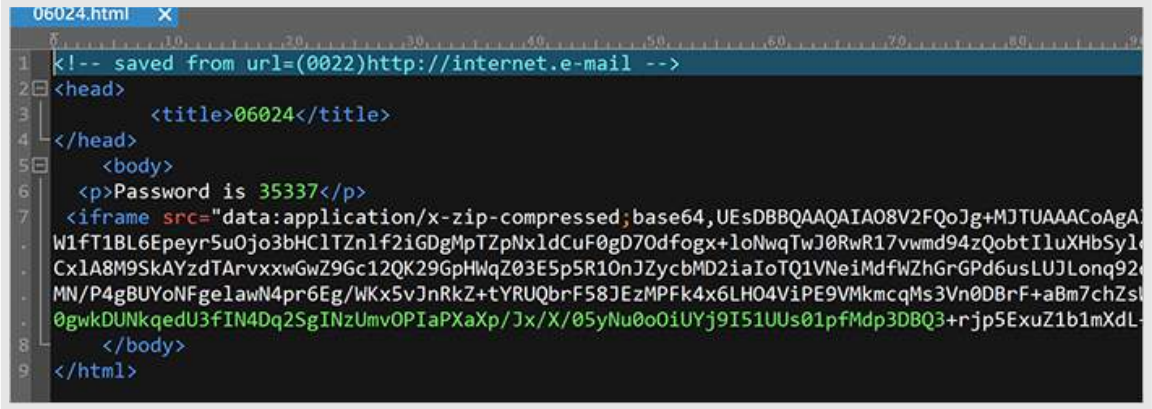
通过后台调用浏览器，解码藏在 HTML 文件中的压缩文件

在过去，将各种威胁文件隐藏在压缩文件里，是很常见的行为。因为压缩文件给了恶意软件一个外壳，需要进行解压缩才能分析，但这对于多数的杀毒分析机制都不是什么大问题。于是，攻击者在压缩文件加上密码，并于邮件中告知受害者密码，这就给了病毒附件机会躲过杀毒检测并执行后续的后门安装。我们在本季看到了一个有别于传统攻击手段的利用。

这个特别的利用方式是，在电子邮件的附件中放入一个 HTML 文件，当这个 HTML 被受害者点击后，便会“下载”一个加密的恶意文件。事实上，这并非真的从网络上“下载”一个恶意文件，而是通过浏览器，解码出内嵌于 HTML 内的一个加密恶意文件，由于这个文件不是从外部而来，因此浏览器的文件下载保护，及 Windows 内建的「网络标记」(Mark of the Web) 保护也会因此失效。根据我们分析的恶意样本，加密的 zip 里是一个 PE 文件的后门程序。



电子邮件的附件文件中放入一个 HTML 文件，再藉由这个 HTML 被受害者点击后，下载一个加密的恶意文件



通过浏览器，解码出内嵌于 HTML 内的一个加密恶意文件，文件并非从外部而来

结论

在电子邮件安全在早期还不受重视时，多数的收信软件或是 Webmail，几乎都能像浏览器一样完整的执行各种网页程序。随着时间推移，大家慢慢意识到电子邮件这个通道若不进行管控或限制，会是一个很容易被主动攻击的突破口。因此，现在的收信软件或是 Webmail 都不再能直接执行各种网页程序。攻击者在演化的过程中留意到了电子邮件可夹带各种附件的可能性，开始通过夹带各种恶意文件以利用这些文件开启软件的漏洞。HTML 可以调用本地浏览器开启，在过去经常被用来做脱机钓鱼，这次我们看到了脱机下载文件攻击样本，未来在呼叫浏览器的利用方面恐怕将更加深化及普及化。

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