# 2019 守内安信息科技 & ASRC
# 邮件安全趋势回顾报告

ASRC

Spam Mail
Virus Mail
Malicious Mail

Feb 2020 released.

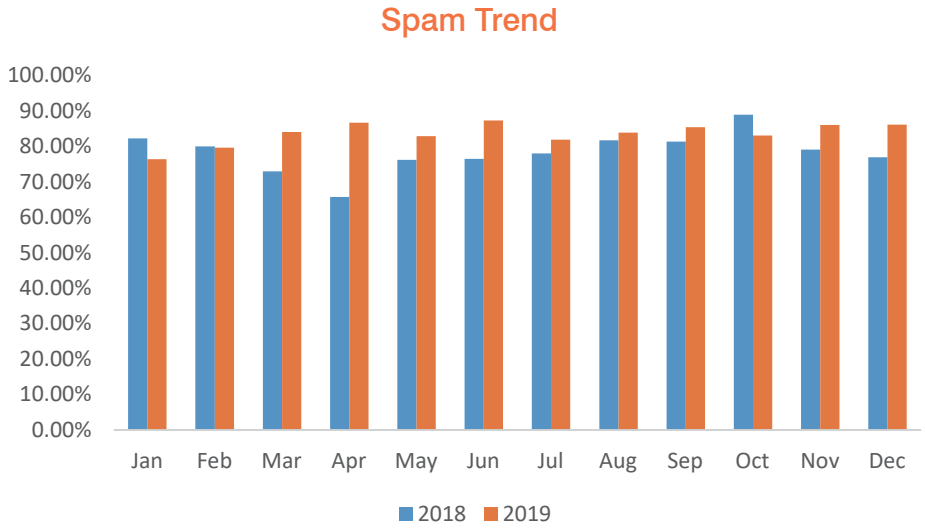
# 概观

根据ASRC 研究中心 (Asia Spam-message Research Center) 与守内安的观察，2019 年总体来说，垃圾邮件与病毒邮件的数量呈现均匀分布，没有哪个月份特别爆量，但是相较于2018年，数量稍有增长。邮件量爆发、诈骗邮件与钓鱼攻击在2019年第四季度达到全年高峰；BEC 诈骗邮件的数量虽然降低，但是BEC事件并未因此缓和。CVE-2014-4114、CVE-2018-0802、CVE-2017-11882这三个 Microsoft Office 文件漏洞利用全年可见；2019 年第一季度被揭露的 WinRAR 漏洞 (包含 CVE-2018-20250、CVE-2018-20251、CVE-2018-20252与CVE-2018-20253)，皆被用于 APT攻击或是渗透测试、红队演练。

# 统计

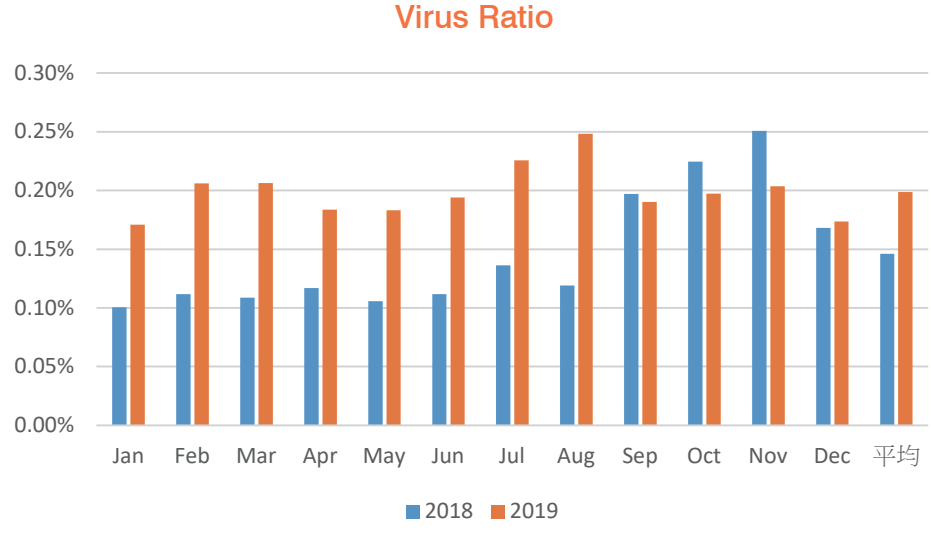
## 垃圾邮件占比趋势统计

2019年垃圾邮件平均约占总体邮件的83.67%，相较于2018年的占比增加了6%左右；2019年每个月的垃圾邮件占比几乎都在80%以上，月份之间的波动很平均，且多数月份垃圾邮件占比都较 2018 年来得高。



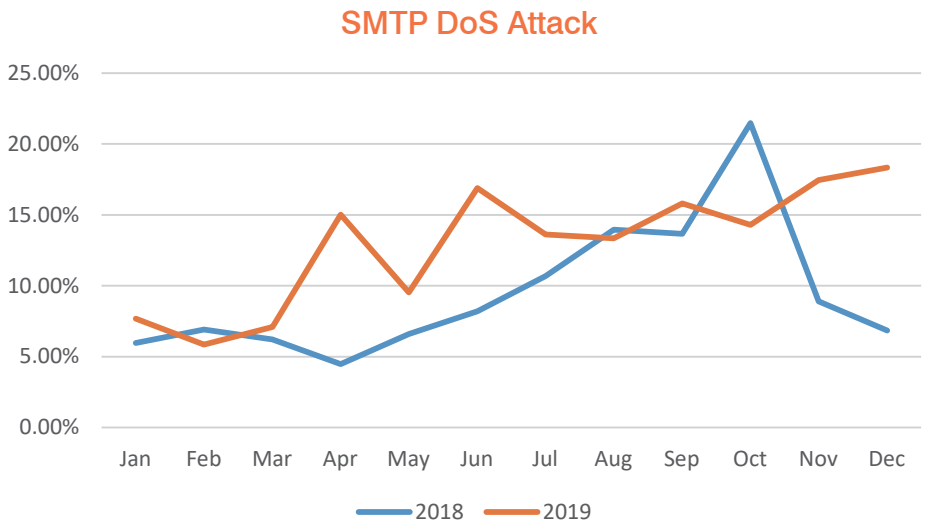

## 垃圾邮件中的病毒邮件

垃圾邮件中，一般病毒的占比大约在0.1~0.2%之间。2018年在第四季的波动幅度较大，2019年则平均占比都维持在0.15%之上。



## SMTP DoS攻击

同一个 IP 集中发送大量邮件，并可能造成SMTP服务阻塞或中断的攻击，多半发生在第四季，可能因为第四季为消费旺季，双十一、双十二、圣诞节与跨年接踵而来，搭配EDM与Phishing一起出现。但是2019除了第四季度外，在四月及六月类型的攻击也都有明显上升的迹象。




## 邮件附件类型

电子邮件中，常用的附件类型，可能被用以攻击的机率大概有多少呢?我们统计了2018、2019年的数据，最常用来攻击的办公文件为Word文件(注：凡含有不当目的的Word文件皆从严认定)，其次为Excel文件；多数操作系统都可以直接支持ZIP解压缩，因此ZIP压缩格式较常被用来夹带恶意文件。

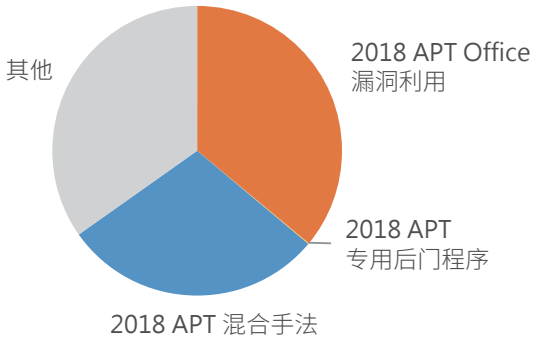
| | 2018 | 2019 |
|---|---|---|
| **办公文件类型** | | |
| Word | 28.65% | 24.90% |
| Excel | 5.86% | 3.33% |
| PDF | 2.69% | 3.12% |
| PowerPoint | 0.82% | 1.40% |
| **压缩文件类型** | | |
| ZIP | 14.03% | 9.98% |
| RAR | 4.99% | 9.51% |

## APT 攻击邮件

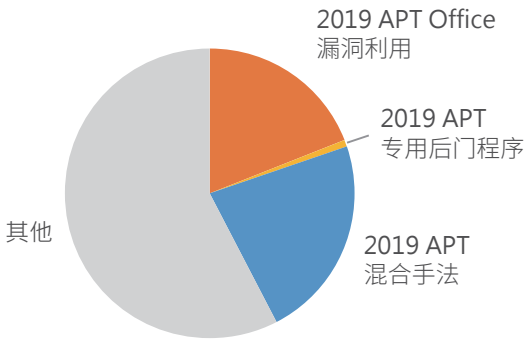
2018 年 APT 攻击邮件最常见的是 Office 漏洞利用的手法，较常被利用的漏洞编号分别是 OLE 漏洞 (CVE-2014-4114) 与方程式漏洞 (CVE-2017-11882)。

2019 年 APT 攻击邮件最常见利用的 Office 漏洞编号为 CVE-2014-4114、CVE-2018-0802、CVE-2017-11882，大致上承继了 2018 年的利用情况。

2018




2019

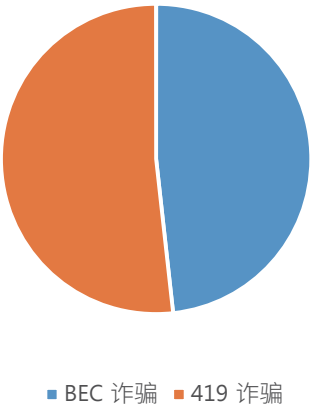



## 诈骗邮件

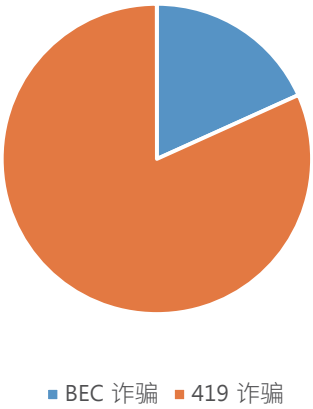
2018年的 BEC 与 419 诈骗占比大约各占一半。2019 年 BEC 与 419 诈骗占比发生了不一样的变化，BEC 诈骗与 419 诈骗邮件总量相较 2018 年的总量下降；虽然 BEC 诈骗邮件下降的幅度高于 419 诈骗，并不表示 BEC 诈骗的风险跟着下降了。

相反，BEC 诈骗邮件显得更有策略性，不会过早介入商谈中的交易，也减少接触不必要收到 BEC 邮件的人员，大幅提高 BEC 诈骗的成功机率。

2018




2019



# 重要趋势

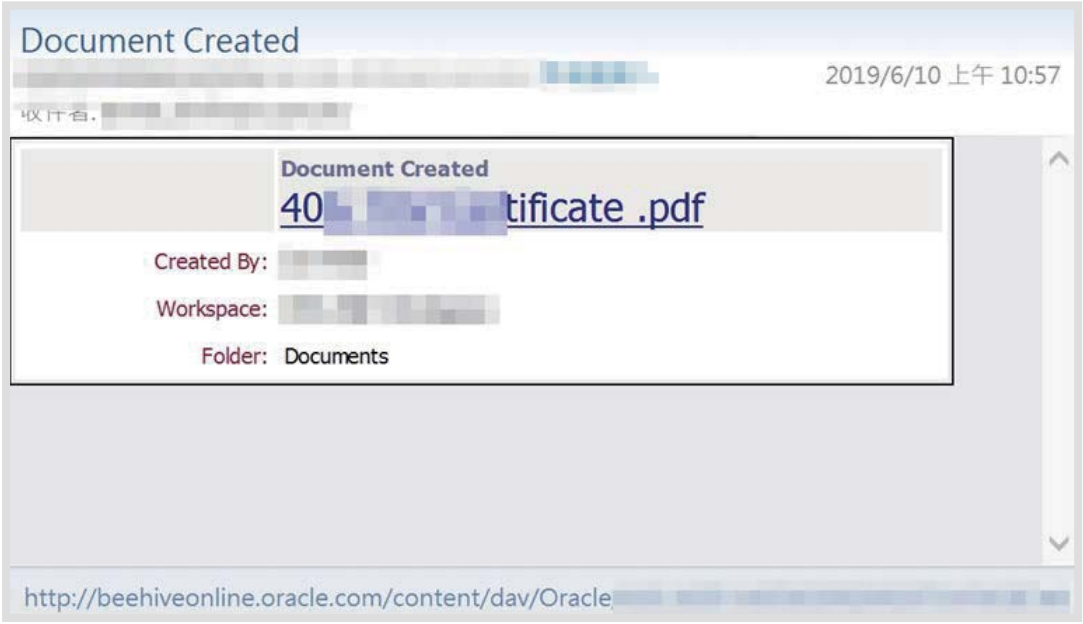
## 信任来源饱受挑战

电子邮件的可信度，在近年来不停地受到挑战，尤其BEC事件高发的情况下，对于邮件中提及异常的变更事项，都需要特别留意，尤其是汇款账号的变更，一定要通过电子邮件以外的渠道再次进行确认。

其次需要特别注意的是在电子邮件内的超链接。并不是超链接带有可信赖的域名，就表示这样的超链接不带有威胁！也不是所有恶意的超链接都必然会下载恶意软件，或需要被攻击者配合输入账号密码相关数据，毕竟，并非所有人使用网络服务都会随手注销。在2017年开始出现钓鱼邮件结合 Google OAuth，就是企图蒙骗收件人通过点击一个共享文件的链接，授与攻击者存取Google App的权限，如今类似的手法也开始出现在 Office 365。

最后，白名单一定要慎用，看似来自熟悉的同事、供应商的邮件，也有可能隐藏恶意攻击！

供应链攻击是国家级资助的APT攻击常用的手段。攻击者的主要目标可能具备了很高的警戒意识与防护能力，因此攻击者可从主要目标的合作对象下手，之后再通过主要目标对合作对象的信任，直接穿过各种防护措施进行攻击。




合法域名空间遭到滥用的实例

# 钓鱼邮件与诈骗邮件泛滥

2019 年电子邮件中，带有恶意链接的数量，大约是 2018 年的 2.8 倍。钓鱼邮件为了取信收件人点击，多半会使用一些当地化用语及社交工程的手法。由于钓鱼邮件主要目的是骗取网络服务的账号密码或其他机密数据，因此多半在点击之后，会通过浏览器连往一个收集这些机密资料的钓鱼网站或钓鱼窗体，再诱骗受害者输入其机密数据。浏览器的开发商也注意到类似的问题，于是纷纷在网址列加入了检查与提醒的功能，希望能藉此保护使用者。

攻击者也开始改变做法，在电子邮件中直接夹入一个恶意的静态 HTML 页面，诱骗收件人填入机密数据，但是这个页面通过浏览器打开时，网址列显示的是本地端的储存地址而非远程的钓鱼网站。当收件人填完数据按下发送后，浏览器即以 POST 搭配加密联机的方式，将机密数据送往钓鱼网站，这样的钓鱼手段能略过多数的浏览器保护措施。这类型的攻击邮件，在 2019 年第四季度大量出现。


恶意的静态HTML钓鱼邮件

# Office 文件漏洞充满威胁

屡试不爽的 Office 文件漏洞，一直是攻击者爱用的武器之一。除了作业人员、防病毒软件对文档的警觉性较低外，许多人所使用的 Office 不会经常性更新。除了公司预算的问题外，原本就使用了非正版 Windows，或担心兼容性、使用上的适应性，以及缺乏漏洞修补的概念，都是使用者不愿更新的原因。根据 ASRC 的统计，2018 年最常见的邮件漏洞利用攻击为 OLE 漏洞 (CVE-2014-4114) 与方程式漏洞 (CVE-2017-11882)。

2019 年，CVE-2014-4114 仍持续被利用，且在第三季度爆发大量的攻击样本，主要目标产业为电子、食品、医疗相关产业；CVE-2018-0802 则做为 CVE-2017-11882 其后续的衍生变形攻击持续存在。2020 年初刚刚被披露的 CVE-2020-0674 及其后续影响力，我们也将持续关注。

# 结论

2020年是5G基础建设部署、成熟加速的一年，随着整体网速的加快，移动应用服务将更趋复杂化，因此，个人信息遭到刺探、外泄的速度与规模、攻击的速度及频率，都会跟着大幅提高；而恶意软件也可以不必再拘泥文件大小的限制，更可朝向功能完备的方向发展；加上量子计算机、云计算的推波助澜，信息安全事故的发生与危害程度可能是过去难以想象的。电子邮件仍会是网络攻击重要的入侵渠道，单纯的账号密码防护力渐趋薄弱，多因素验证已是势在必行。

## 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。