

2019 守内安信息科技 & ASRC

第二季度电子邮件安全趋势



ASRC
Asia Spam-message
Research Center

根据 ASRC 研究中心 (Asia Spam-message Research Center) 与守内安的观察, 2019 年第二季度, 电子邮件安全趋势基本为第一季度情况的延续。有更多的合法域名遭到滥用; 诈骗邮件的数量比第一季度上升了 250% 以上, 其中以无差别攻击的尼日利亚诈骗邮件占比最高; 针对型的商务电子邮件诈骗虽然占比低, 背后隐藏的信息安全问题却不容忽视; 而 Office 的漏洞, 仍是稳定、易触发、全版本都可用, 最被攻击者青睐。以下是本季主要的趋势观察:

诈骗邮件总数比上季度上升 250% 以上

诈骗邮件可以分为商务电子邮件诈骗 (BEC, Business Email Compromise) 与尼日利亚诈骗 (419scam) 两大类。商务电子邮件诈骗主要是针对正与外部供应链从事商务洽谈或执行电汇时, 介入的复杂诈骗攻击。而尼日利亚诈骗则是对全球不特定目标发送各种诈骗信息, 内容涵盖了灾难、遗产或巨额资金转移、网络交友、募款等主题, 对收件人进行诈骗。不论是商务电子邮件诈骗或尼日利亚诈骗, 主要采用的都是社交工程手法, 需与收件人互动。

由于商务电子邮件诈骗发动前, 需要先能入侵目标对象的电子邮箱, 并进行一段时间的监测, 才会在交易时, 发动商务电子邮件诈骗。因此曾遭受商务电子邮件诈骗的企业单位, 多半已存在信息安全问题; 而尼日利亚诈骗只需要捏造故事, 并将这些故事发送给曾外泄的、暴露在外的电子邮件地址, 接着等防备较弱的人上钩, 就可以开始进行诈骗。两者的攻击难度差异甚大, 因此在 2019 年上半年, 这两种诈骗的比率很稳定, 商务电子邮件诈骗约占 2%, 而尼日利亚诈骗高达 98%; 而整体的诈骗数量, 第二季度较第一季度上升了约 250% 以上。



通过 Google 翻译后, 发送至华语地区国家的尼日利亚诈骗

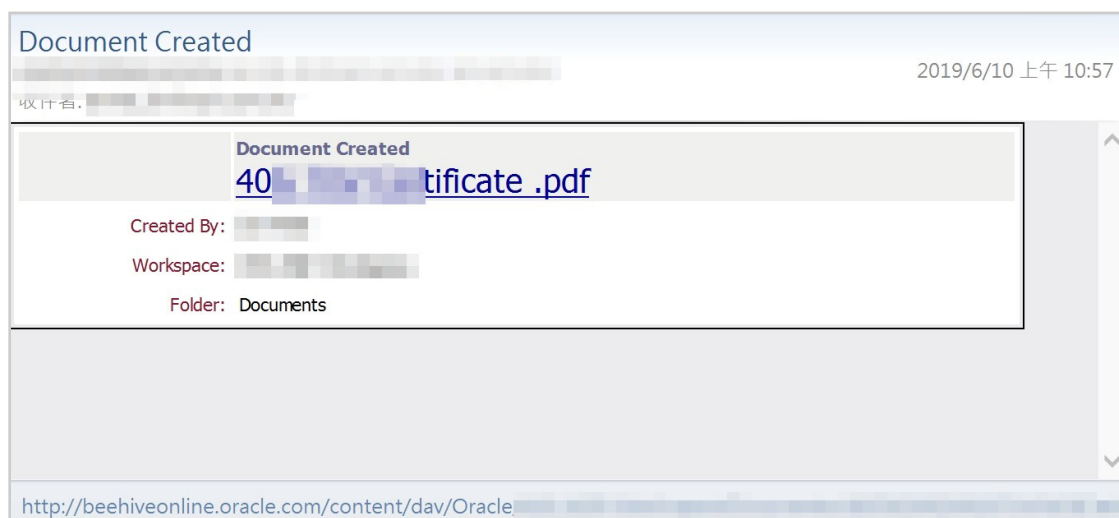
越来越多的合法空间遭到利用,藉以掩护攻击目的

ASRC 在第二季度持续观察到新的合法空间被用来放置恶意文档或文件。这类攻击邮件多半以很简单的内容附上一个合法域名的超链接,希望收件人可以前往该链接以下载或开启文档。

经常遭到滥用的知名合法域名:

- .web.core.windows.net
- 1drv.ms
- .github.io
- .oracle.com
- drive.google.com
- .appspot.com
- .dropbox.com

这些域名的拥有者都是跨国的大型企业,并为知名的网络服务提供商,因此,当收件人点击这些链接时,可逃过多数上网保护或管理机制的检测,进而接触存在风险的恶意文档。



越来越多的合法空间,遭到利用

●● 电子邮件的漏洞利用，Office 漏洞运用最广，WinRAR 漏洞多用于针对型攻击

2019 年上半年来自电子邮件的漏洞利用，前三名分别为 CVE20144114、CVE20180802、CVE201711882。这三个都是 Microsoft Office 漏洞，它们稳定、易触发、全版本都可用，只要能够引起使用者好奇，一旦附件被开启，不需要使用者再配合执行其他动作，漏洞便会触发执行恶意软件，接着攻击者便能取得计算机掌控权。

除此之外，值得特别留意的是第一季度被揭露的 WinRAR 漏洞 CVE201820250 系列，在第二季度的攻击范围与数量都有明显增加的趋势，攻击普遍出现于金融、制造、医疗、石油等相关产业。这个漏洞几乎都为针对型 APT 攻击所利用，不同前述利用目的较为多元的 Office 漏洞。

●● 无文档式攻击，让防御更加艰巨

我们也从许多电子邮件的攻击中观察到无文档式 (Fileless) 的攻击，也称为「离地攻击」(living off the land)。这类攻击不必下载专用工具，因此无从发现恶意软件！攻击的初始可能从一份有害的恶意文件开始，在漏洞被触发或以社交工程的方式成功促使收件人执行 VBA 后，开始使用受害者操作系统中种种合法工具，开始进行一连串的攻击，尤其是 Windows 上的 PowerShell，更是攻击者的最爱。这让以侦测恶意软件存在发现的防卫手段，面临艰巨的考验。

结语

90% 的网络攻击皆由电子邮件拉开序幕，因此，将电子邮件的防守做得牢靠，就能防住大多数的网络攻击。攻击者似乎也明白这一点，因此，越来越多来自电子邮件的攻击者利用超链接、短网址、合法空间存放恶意软件等手法，试图将战场从电子邮件过滤的网关口延伸至收件人的终端计算机、浏览器等，并且试图制造出防守方的各种逻辑漏洞或矛盾，例如，为了解决恶意超链接所带来的风险，而针对电子邮件内的每一个超链接进行检测，这就可能带来许多未经授权的点击，造成各种身分认证、稽核、确认订阅或退订混乱的情况，这可能是许多开发者或方案采用者不会直接意识到的风险。

关于 ASRC 垃圾信息研究中心

ASRC 垃圾信息研究中心 (Asia Spam-message Research Center), 长期与 Softnext 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, 促成产政学界共同致力于净化网络之电子邮件使用环境。

关于守内安

守内安信息科技(上海)有限公司(以下简称“守内安”), 是上海市政府及国家奖励支持的自主研发高科技创新的“双软认定企业”和“高新技术企业”, 钻研邮件风险管理和信息安全内控管理。以电子邮件安全管理为核心, 研发了一系列“电邮安全与合规”为中心的核心产品线, 衍生到威胁防御与联合防御体系。守内安十几年来秉承“以客为尊”的服务理念, 树立了“服务·品质·值得信赖”的品牌理念, 目前已拥有 7000+ 家全球性企业级用户, 终端用户达 80,000,000+ 人次。

守内安受到广大客户认可的端口 25 邮件安全生态防御明星产品:

- SPAM SQR: 防垃圾邮件过滤系统-提供勒索、APT 及商业邮件诈骗等恶意邮件的防御。
- MSE: 电子邮件过滤审批系统-邮件事先过滤审批策略, 防止数据通过邮件外泄 (DLP)。
- MAE: 电子邮件归档审计系统-事后快速调阅, 审计举证与合规性。
- Mail SOC: 提供邮件巡航与 RBL 等侦测服务。
- SMRS: 外发邮件不通转发安全中继平台服务。

服务咨询: +86-021-51036007

官网: www.softnext.com.cn



Softnext 守内安 | 微信公众平台

您的邮箱安全管家, 专业的企业级邮件安全服务提供商。
欢迎扫描二维码关注取得第一手安全消息

