2019 守内安信息科技 & ASRC
第一季度电子邮件安全趋势

ASRC
Asia Spam-message
Research Center

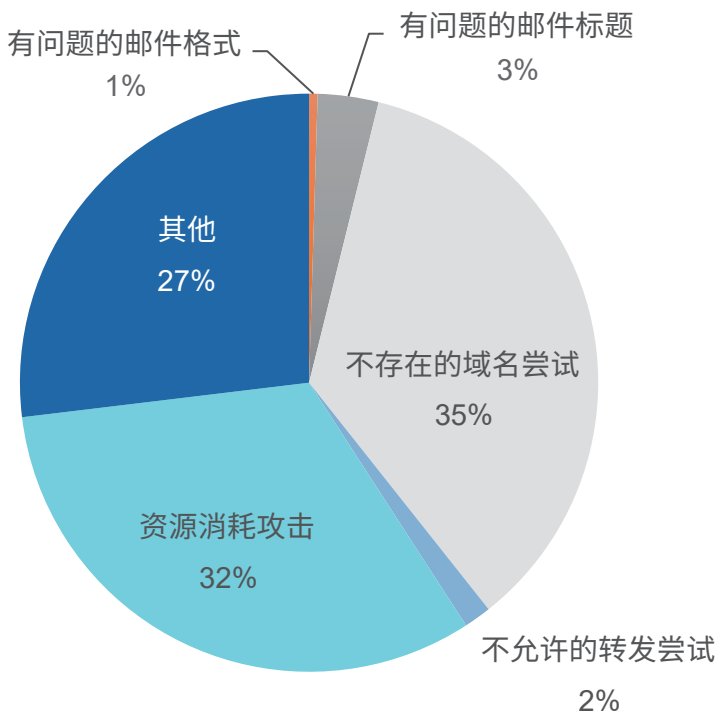
May 2019 released.

2019 年第一季度，邮件服务器攻击活动统计显示，占比最高的是“以不存在的域名任意尝试发送邮件”；其次是“消耗性攻击：多个联机到邮件主机，不进行动作或是以十分缓慢的方式响应以便能保持联机，使邮件主机的资源消耗”。病毒邮件方面，占比最高的仍是“由遭到蠕虫感染主机所发出的扩散感染邮件”，其中以“诺瓦病虫 (MyDoom) ”活动最为活跃。在第一季度中，WinRAR 漏洞 APT 攻击、GandCrab 勒索程序，以及合法空间掩护攻击目的邮件需要特别当心！

邮件系统攻击尝试

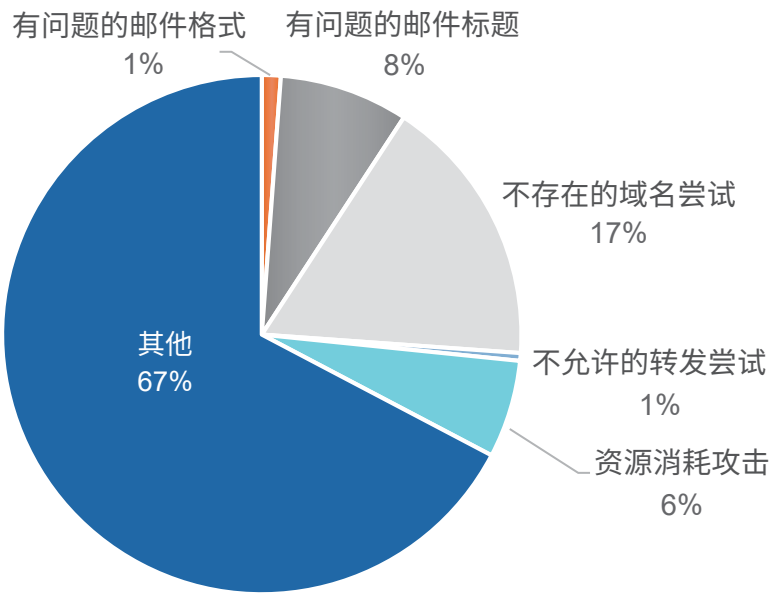
第一季度中，全球邮件攻击尝试统计显示，占比最高的是“发送机以任意不存在的域名尝试对邮件主机发送邮件”；其次是“试图消耗邮件主机运算资源的无用联机”。需要特别留意的是，世界上仍有许多漫无目的尝试测试邮件主机是否有设定不当，而可任意被用来转发的“开放转发 (OpenRelay) ”的试探。

全球邮件服务器攻击尝试统计



中国的邮件服务器尝试，较为多样化，对比全球趋势来看，集中性较不明确。

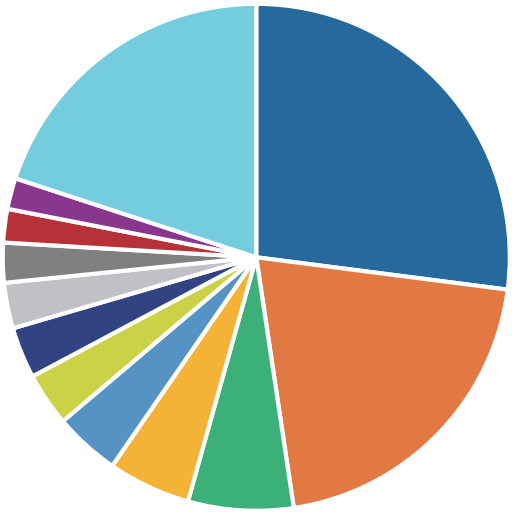
中国邮件服务器攻击尝试统计



收件人攻击尝试

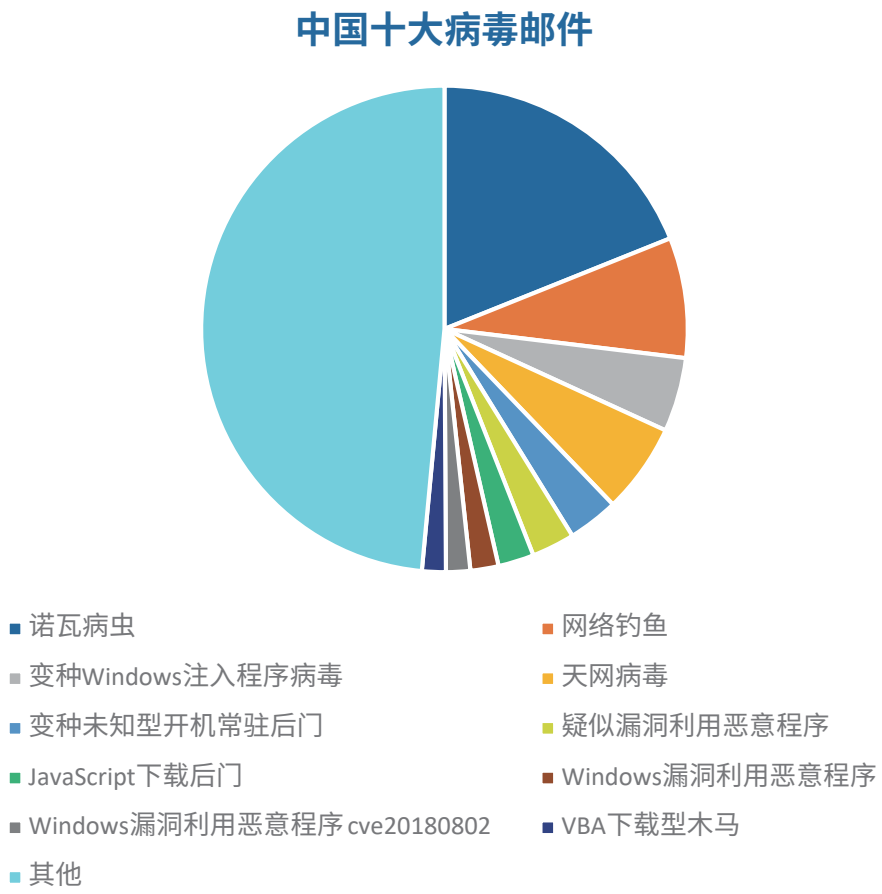
病毒邮件主要以遭到蠕虫感染的主机所发出的扩散感染邮件为主。从全球趋势来看，“诺瓦病虫(MyDoom)”是最大的蠕虫邮件扩散源；其次为各种具备 Windows 感染能力，并在开机后会尝试执行并常驻的病毒藉由邮件扩散。

全球十大病毒邮件



- Windows注入程序病毒
- Windows开机常驻后门
- 疑似漏洞利用恶意程序
- 未知多重威胁程序
- Windows漏洞利用恶意程序
- 诺瓦病虫
- 变种DOC文件后门
- VBA下载型木马
- 变种未知型开机常驻后门
- 变种Windows开机常驻后门
- PowerShell下载型后门
- 其他

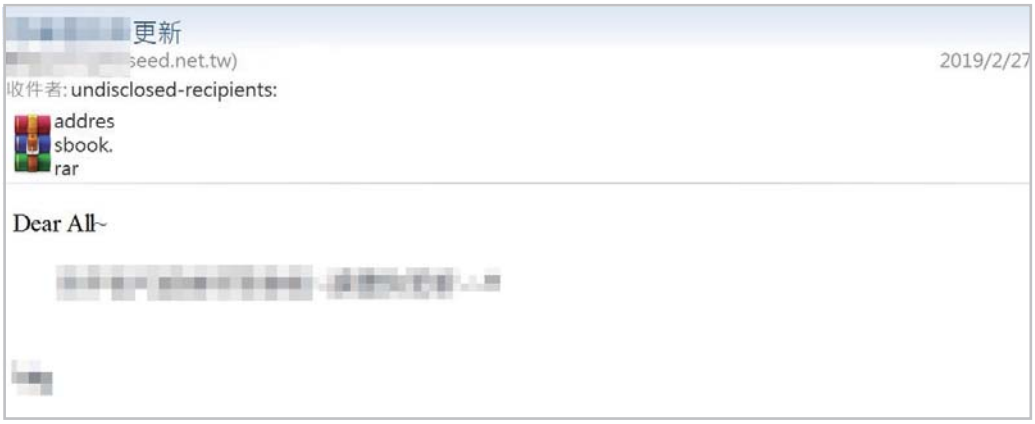
中国的病毒邮件也呈现较多样而分散的趋势。与全球趋势类似，以蠕虫扩散型的病毒邮件为主，分别是“诺瓦病虫 (MyDoom)”与“天网病毒 (Netsky)”。



在2019年第一季度中，除了常见的病毒邮件、钓鱼链接外，以收件人为目标，并诱使收件人配合执行恶意程序的攻击，我们特别举出下列几个值得注意的例子，请您谨慎提防：

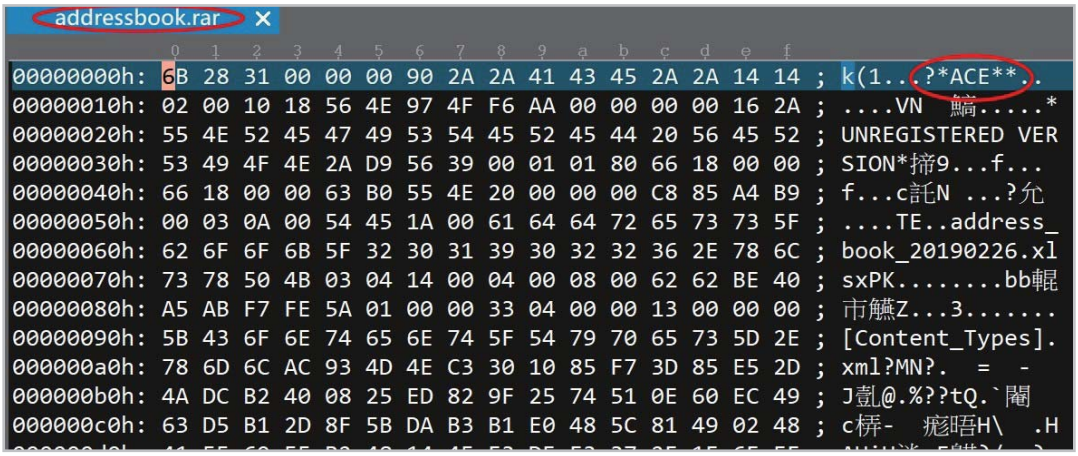
WinRAR漏洞APT攻击

大约在 2019 年 2 月 20 日披露了一个 WinRAR 长年潜在的漏洞。这个漏洞的肇因于 WinRAR 引用第三方函式库 UNACEV2.DLL，用于支持 ACE 这种压缩格式。UNACEV2.DLL 存在一个解压缩时可写入及执行任意文档的漏洞，且这个函式库自 2005 年以来便没有更新，造成了十多年以来 WinRAR 的各种版本皆受此漏洞的影响。由于WinRAR的开发团队不握有 UNACEV2.DLL 的原始码，因此在近期 WinRAR 5.7 版，以取消对 ACE 压缩格式的支持的方式解决这个漏洞。



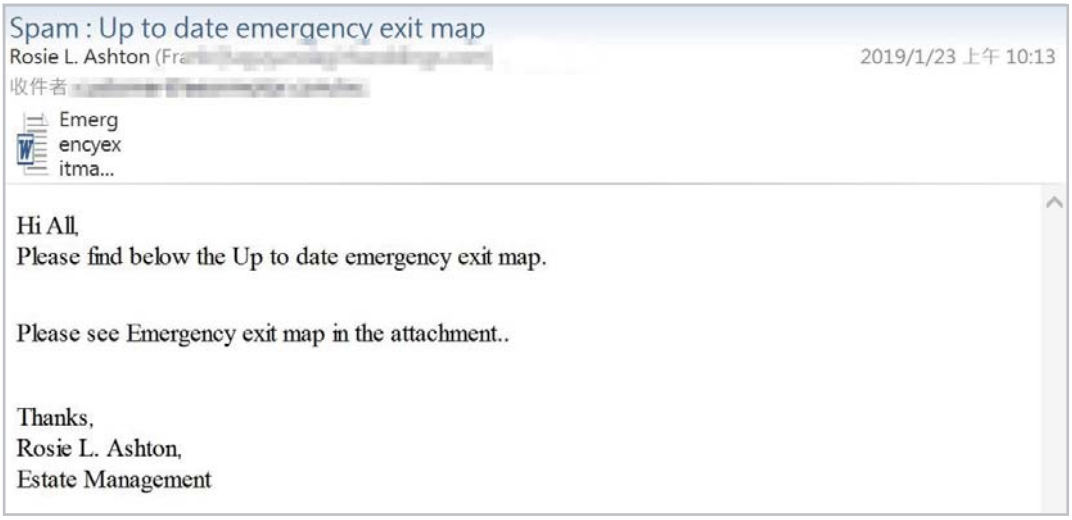
在该漏洞被披露的两天内，ASRC 与守内安团队就侦测到了利用此漏洞的 APT 攻击

虽然这个漏洞发生于解压缩ACE格式的压缩文件时才会触发，很多个人或企业单位根本不使用或没听过ACE这种压缩格式，因此可能会疏忽此漏洞的危险性。实际的攻击，只要能呼叫出UNACEV2.DLL，不一定需要扩展名看来是 .ace 的压缩文件。我们观测到的攻击来自遭到入侵的非公务邮箱，针对特定的高科技企业与政府单位发送含有漏洞利用的恶意文档进行攻击，这个文档的扩展名是 .rar。当收件人试图使用WinRAR解压缩文件案查看其中内容时，便会遭到夹带于恶意文档中的恶意软件攻击，并在每次开机都会执行特定的恶意软件。这个恶意软件搜集加密受攻击者的计算机机密信息，加密后，利用 Dropbox 免费空间进行恶意工具的下载与机密数据的上传。



GandCrab 勒索程序

GandCrab 第一次被大众关注是在 2018 年的 1 月，由罗马尼亚的安全公司 Bitdefender、罗马尼亚警政署、欧洲刑警组织连手揭露了这个恶意勒索软件。这个勒索病毒的开发者十分积极，很快地在同年的3月5日，5月3日先后释出 GandCrab2.0 与 3.0 版本。GandCrab 最新版是 2019 年 2 月 19 日左右所推出的 5.2 版。



通过电子邮件发送 GandCrab v5.1 版的前导攻击恶意文件

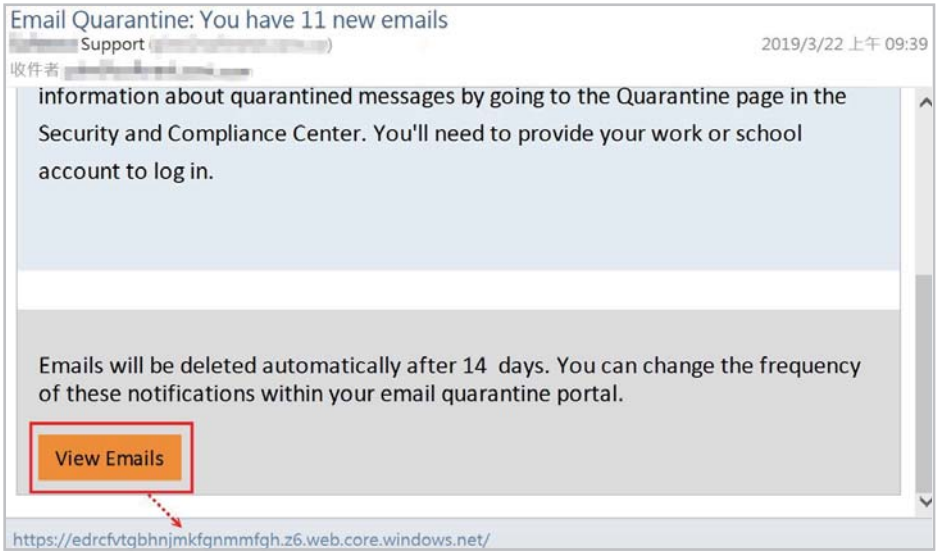
当GandCrab被触发后，它会尝试向外联机至内建的上千个独立主机列表，联机成功后，它会开始进行感染主机的加密。遭到加密的文档，文档的扩展名为 5-10 码随机字母。GandCrab 主要勒索的目标是 Bitcoin、DASH 或其他虚拟货币。虽说GandCrab在全球都有其踪迹，但在亚洲地区最大的受害国是南韩，其次为中国。值得庆幸的是守内安的用户均没有受到该勒索邮件的影响。

合法空间掩护攻击目的

越来越多的免费文档储存、程序存储空间、免费的网页生成，被用来寄放恶意攻击程序，或一页式的网络钓鱼页面，攻击者再将这些恶意链接，通过钓鱼邮件的方式进行发送以进行攻击。由于这些网站本体都是合法的，只是某一页、某个文档不怀好意，因此，并不能直接将这些网站封锁；而特定的某个恶意页面或某个恶意文档的存活时间也不长，但新的恶意页面与文档却不停地快速生成。

Github.io 被用来建构钓鱼网页，通过钓鱼邮件发送

钓鱼页面，主要目标是钓取电子邮件的密码



寄宿在 windows.net 的网络钓鱼链接

结语

来自电子邮件的攻击，不论是附件文档或是超链接，要收件人直接辨别是否带有恶意，是十分不容易的事。部分收件人为了进一步确认这些链接或文档是否和自己工作内容相关，在危险的情况下直接开启、预览文档，而造成入侵、感染事件时常发生。因此，以适当的安全作业流程搭配设备，尽量让人员不要接触问题邮件才能有效避免攻击事件的发生。

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