2018 守内安信息科技 & ASRC
邮件安全年度分析報告

ASRC
Asia Spam-message
Research Center

January 2019 released.

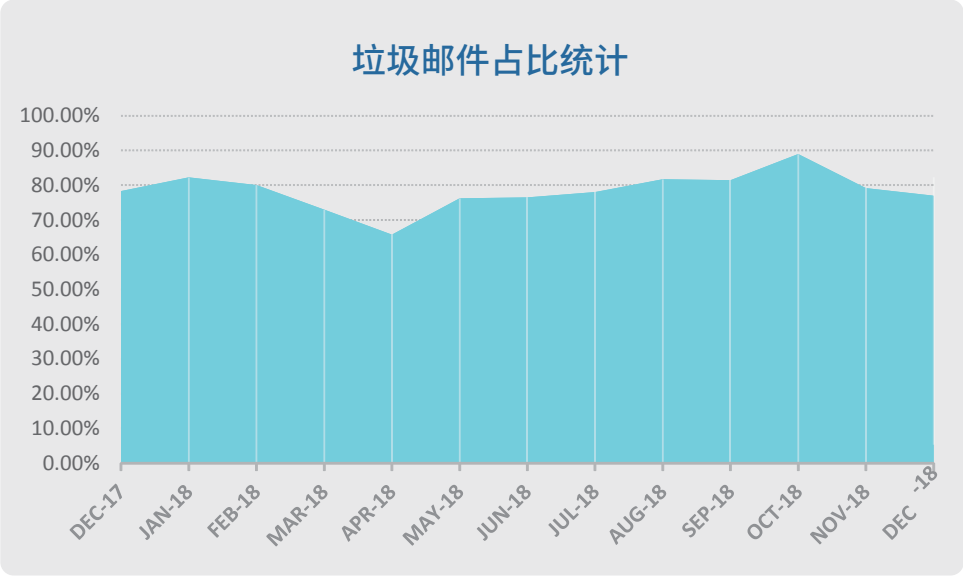
概要

2017年最令人印象深刻的信息安全议题，大概是勒索病毒。2018年，值得注意的信息安全议题有哪些呢？CPU的缓存安全漏洞、挖矿以及虚拟货币窃案、脸书泄密与剑桥分析事件，这一些的确是2018年十分重大的信息安全议题，然而，每一年的信息安全议题出现，总少不了利用这些议题所进行的电子邮件攻击：在CPU安全漏洞公布后，2018年一月份即出现重大漏洞更新的网钓邮件，该邮件佯称可下载并安装修补程序，但实际上为木马程序Smoke　Loader。虚拟货币交易平台Binance，以及日本虚拟货币交易所Coincheck都曾遭受过钓鱼邮件的攻击，后者还因此蒙受了巨大的损失；最后，以脸书、Apple等知名公司名义发送的钓鱼邮件更是经常可见，受害用户并无法直接分辨这些钓鱼邮件的可信度，当自己有使用相关服务，多半都很容易成为上钩的对象。

邮件安全已成为各种信息安全措施中，最基础且无法忽视的重要环节，以下，我们将针对2018年邮件安全相关事件与统计，进行重点回顾。

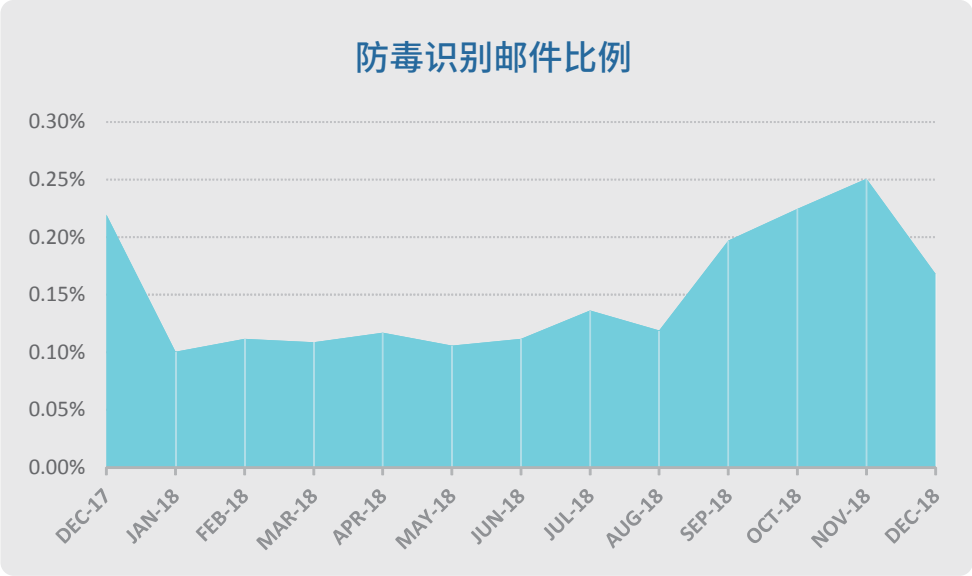
统计

2018年的垃圾邮件活动统计图如下。全年垃圾邮件占比大约落在78%左右，相较于往年，并没有太大差异；全年最多垃圾邮件爆发的月份落在十月，最少的月份则是四月，这两个月份的垃圾邮件落差约20%。大致上而言，垃圾邮件并没有消灭或趋缓的迹象。



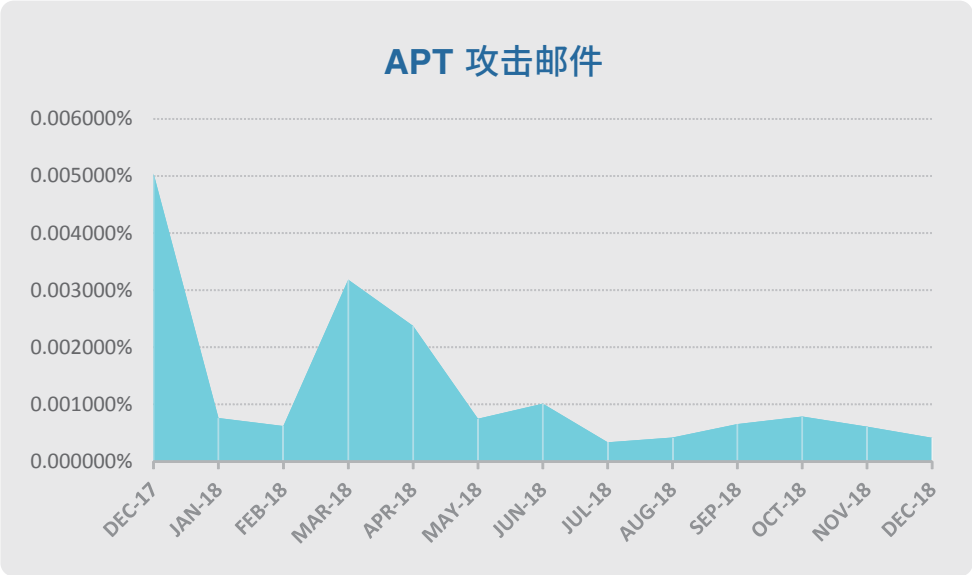
2018 垃圾邮件活动统计图

在垃圾邮件中，于第一时间即可被防毒软件侦测出的病毒邮件统计如下。2018年第四季的病毒邮件占比居全年之冠。病毒邮件，大约占全体总邮件量的0.15%。



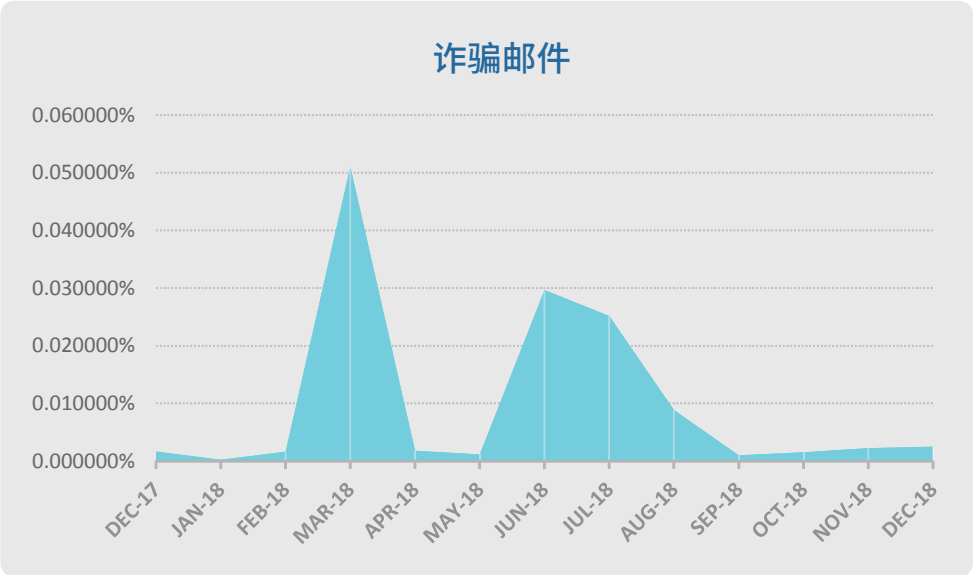
第一时间可被防毒软件侦测出的病毒邮件比例

而在其中比例更少，却不容忽视的APT攻击，占比虽少风险却十分巨大；2018年三月至五月为全年APT攻击邮件最活跃的月份。



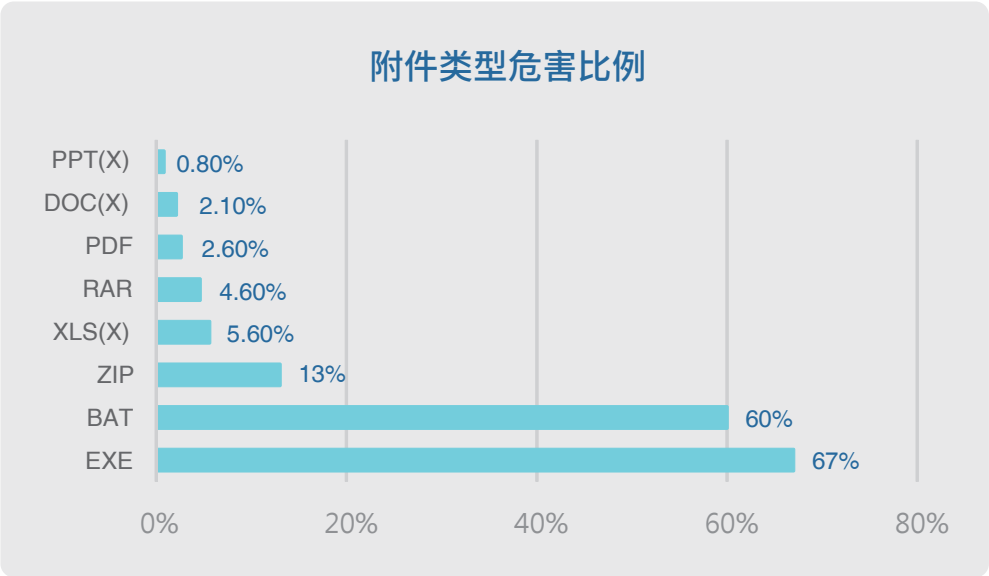
APT 邮件攻击，在2018年三至五月最为活跃

而诈骗邮件则在2018年的三月份，以及六、七月份有明显增多的情况。



诈骗邮件，在2018年三月以及六、七月份明显增多

针对电子邮件附件，ASRC也做了一些统计。一封邮件中，若带有附件，则文件类型的档案，收件者应特别小心EXCEL类的附件，因其相较于其他文件型的附件，更常被用于攻击；而压缩档方面，常见的两种压缩档ZIP、RAR，以ZIP压缩档格式夹带恶意程序较为常见。若邮件中直接夹带EXE或BAT等可执行档类型，则超过一半以上的比例，可能是有害的。



邮件中直接夹带EXE或BAT等可执行档类型，危害比例超过一半

重要事记

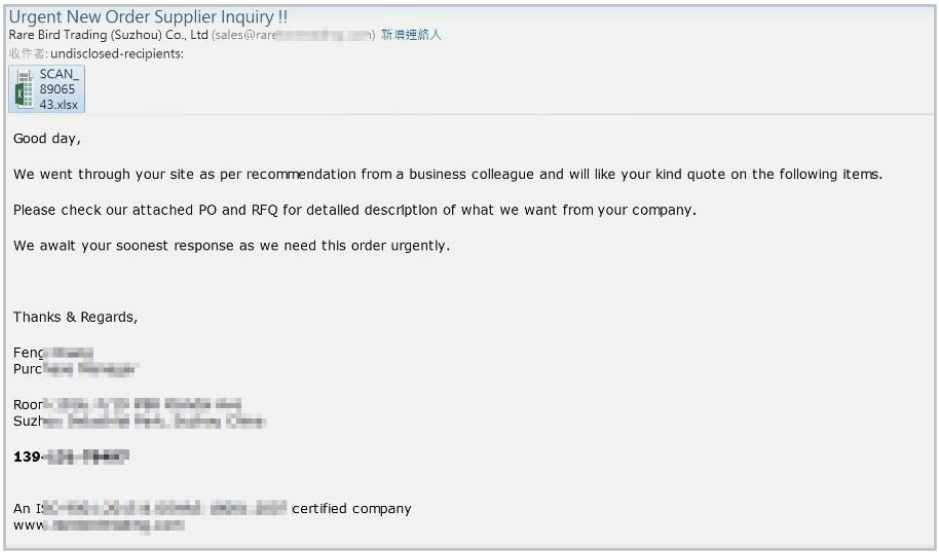
根据2018年，ASRC与Softnext守内安所观察的邮件趋势，大约可归结漏洞利用攻击、钓鱼邮件，以及诈骗或恐吓四种主要型态。这四种邮件攻击难度与目的整理如下表，越偏向技术取向的攻击难度越高，越偏向社交工程取向的攻击技术难度较低。

2018四种常见邮件攻击型态与攻击目的

透过邮件所采取的漏洞攻击

根据ASRC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），这两个漏洞都是利用寄送恶意的Office文件附件，诱使收件者以未修补的Office程序开启后触发漏洞，接着进行进一步的攻击。而在2018年一月份揭露的CVE-2018-0802漏洞，为方程式漏洞（CVE-2017-11882）的变形，主要是利用漏洞修补后仍不完善部分进行攻击。这些经典稳定的漏洞，仍可能会被沿用多年，原因是许多人所使用的Office并不经常性的更新，理由可能为非正版Windows、担心兼容性或使用上的适应性，以及缺乏漏洞修补的概念。

漏洞的利用，通常是复杂的APT攻击行动的前奏，漏洞本身的直接危害性，主要是造成触发该漏洞的电脑控制权被有心人士夺取。透过鱼叉式钓鱼邮件的手法，将带有触发这些漏洞的恶意邮件寄送予特定对象，诱使特定对象开启邮件，由于漏洞已触发，因此可进一步下载并执行更具危险性的攻击程序。CVE-2014-4114的漏洞就曾被用以下载及触发BlackEnergy木马程序，造成乌克兰大停电的事件。


Urgent New Order Supplier Inquiry !!
Rare Bird Trading (Suzhou) Co., Ltd (sales@rare) 新增連絡人
收件者: undisclosed-recipients:
SCAN_ 89065 43.xlsx
Good day,
We went through your site as per recommendation from a business colleague and will like your kind quote on the following items.
Please check our attached PO and RFQ for detailed description of what we want from your company.
We await your soonest response as we need this order urgently.
Thanks & Regards,
Fenc
Purc
Roor
Suzh
139
An I certified company
www

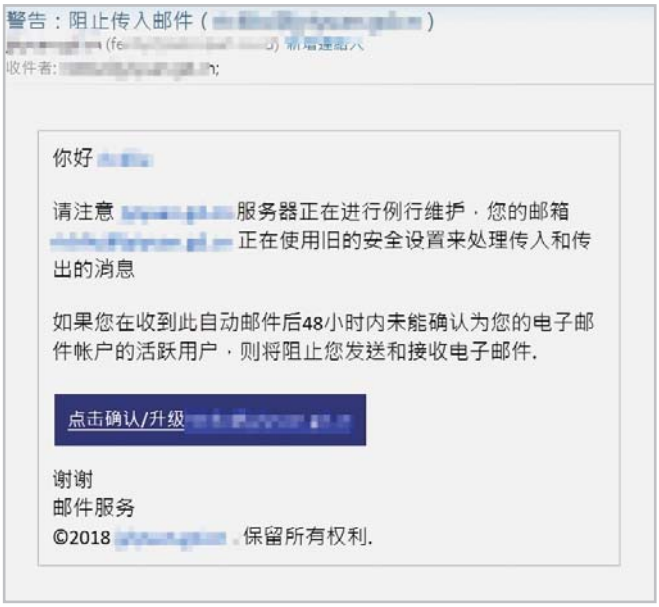
CVE-2017-11882电子邮件攻击样本

除了漏洞攻击外，2018年的四月至九月间，我们也发现了利用Office特殊档案格式所进行的攻击—扩展名为IQY的档案。IQY为Microsoft Excel所使用的 Web 查询设定档，Excel 读取该档后会连向指定的网址取得数据，这种攻击是利用了比较不常被注意到的软件特性进行攻击。由于IQY为纯文字格式，预设的档案开启程序又是Excel，攻击者便利用这个特性，将恶意的网址写入IQY档，欺骗使用者开启档案后连外取得恶意程序回来执行。由于，IQY的纯文字内容并不含有恶意行为，因此也能有效规避防毒软件的检查。

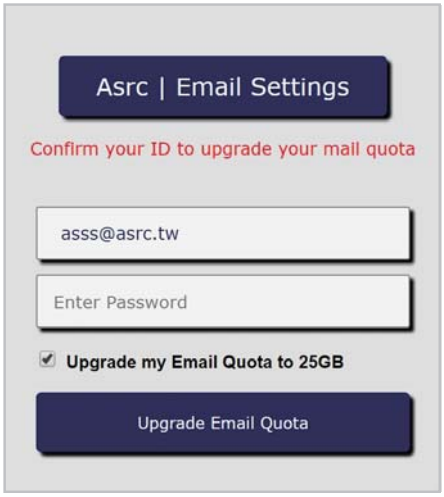
不曾停止的钓鱼邮件

钓鱼邮件已经不是一个新的名词，但恶意攻击者仍乐此不疲，原因是这种攻击行动几乎不需要复杂的技术，但只要能钓到几个有用的帐号密码，投资报酬率相当高。

2018年钓鱼邮件出现的高峰期是在第四季度。钓鱼邮件的内容多半是一个关于你邮箱被停用、升级、非法登录的理由，并附上一个超链接。钓鱼邮件本身并不能钓到帐号密码，他需要搭配一个钓鱼网站，而钓鱼邮件的最大目的就是诱骗收件者拜访钓鱼网站并填入收件者的帐号密码。大约有 7% 的钓鱼邮件，其所配合的钓鱼网站是免费的网站或表单生成器；约有80％以上的钓鱼网站是遭到入侵的 Wordpresss 内容管理系统。



典型的钓鱼邮件，佯称须以个人帐号密码登录进行邮件邮箱的升级



钓鱼网站的登录页面，页面相关资讯的形成是动态的，依据受害者点击链接中所带的参数而有变化

输入帐号密码后，虽然看到一个失败的画面，但实际上帐号密码已遭到收集

除了传统的直接骗取帐号密码外，2018年三月我们也观察到一波不寻常的攻击邮件，这种邮件附带了一个藏在压缩档内的.url档案。当收件人在Windows下解开附件，并点击.url档时会询问是否透过SMB通信协议取得并执行远端作为Downloader的.wsf档案；但.url档有个特殊之处：使用者光是「提取」.url档案，Windows就会主动向.url要求的位址以SMB通信协议要求信息.，此时已对远端恶意主机泄漏收件人使用的IP与其电脑名称。若url内指向的为远端恶意主机的Samba路径，且恶意主机上的Samba服务器启用了NTLMv2验证机制，当Windows自动拜访该主机时，就会将使用者的密码进行哈希运算后送至恶意主机进行验证。虽然无法从哈希码反推回实际的密码，但若是密码的强度不足，只要对密码字典表进行哈希编码后再做比对，就有很高的机会还原密码，并进一步攻击企业外部服务，以此密码尝试登录。这算是钓鱼邮件中一个很特别的例子！

隐而不显的BEC诈骗事件

在2018年，BEC商业电子邮件诈骗事件发生频率并没有趋缓，根据ASRC研究中心与Softnext守内安的观察，2018年的BEC邮件出现的高峰期为第三季。最常遭受BEC诈骗邮件攻击的产业以金融业、高科技制造业、制造业的比例最高。某些特定企业每一到两个月就会遭到1~2次的BEC邮件攻击，且这样的攻击会持续3个月以上。在遭遇BEC诈骗事件后，仅8.23%的企业会寻求专业安全厂商的协助，清查鉴识事件背后的信息安全问题。

美国联邦调查局（FBI）网际网络犯罪申诉中心在2018年7月发布的一则消息中指出，自2013年10月起至2018年5月，全球已曝光的BEC诈骗案件计有78,617件，损失金额超过125亿美元；从2016年12月到2018年5月，已曝光的BEC诈骗损失金额成长了136%。

BEC诈骗与APT攻击间有着相同的特性，黑客在事前经过长时间监控观察以及缜密计划后发动攻击，一旦被盯上，攻击就有可能重复发生。若只把事后补救重点放在「款项追回」，未正视处理事件背后隐藏的信息安全问题，就算企业幸运追回款项，难保黑客不会再度发动攻击。因此若不幸被诈骗，除了立即采取行动与警方、金融单位联系外，也应寻求专业鉴识伙伴协助，协助清查鉴识受害电脑与关联网络，改善企业信息安全问题避免再度受黑。

全球

已曝光的BEC案件数

78,617

损失总额

125 亿美元

资料来源：美国联邦调查局（FBI）
统计期间：2013年10月~2018年5月

BEC诈骗事件统计

最常遭受攻击的产业
金融业
高科技制造业
制造业

某些特定企业
每个月 遭到 1~2次
BEC邮件攻击。且这样的
攻击 持续3个月 以上

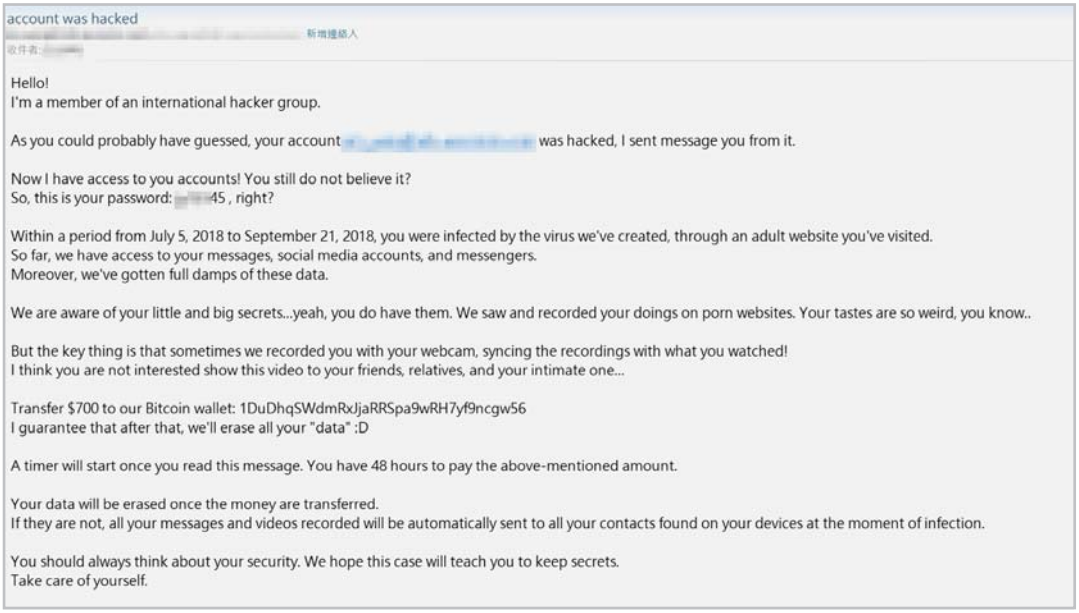
遭遇BEC 诈骗事件后
仅8.23%
的企业寻求专业厂商协助
厘清背后的资安问题

资料来源：ASRC 研究中心

比勒索更简单的「恐吓邮件」

恐吓邮件，并没有夹带任何的恶意档案或攻击代码，纯粹是透过在心理上的恐吓，迫使收到此类邮件的受害者因害怕而依照邮件的指示言听计从。这些恐吓信的收信人名单有不少是从过去社群网站或是大规模泄漏事件中取得的，因此在其内容会提供该收件者过去遭到泄漏的密码，用以取信收件者相信自己的帐号确实遭到入侵。除了以密码恫吓收信者外，也有部分是用诓称收信人电脑已被植入病毒，并透过收件者电脑的网路摄影机拍下一些敏感画面，或收信者有机敏数据在入侵者手上的说词来达到恐吓的目的。

这类邮件最初皆由英文写成，但在2018下半年后观察到有语言变形的趋向，但不见得是直接攻击使用该语言最多的地区；再者，这类恐吓信通常要求使用比特币来进行支付，对于使用比特币较不方便或禁止使用的地区，其恐吓取财成功的机率应不会太高。


account was hacked

Hello!
I'm a member of an international hacker group.

As you could probably have guessed, your account was hacked, I sent message you from it.

Now I have access to you accounts! You still do not believe it?
So, this is your password: 45 , right?

Within a period from July 5, 2018 to September 21, 2018, you were infected by the virus we've created, through an adult website you've visited.
So far, we have access to your messages, social media accounts, and messengers.
Moreover, we've gotten full damps of these data.

We are aware of your little and big secrets...yeah, you do have them. We saw and recorded your doings on porn websites. Your tastes are so weird, you know..

But the key thing is that sometimes we recorded you with your webcam, syncing the recordings with what you watched!
I think you are not interested show this video to your friends, relatives, and your intimate one...

Transfer $700 to our Bitcoin wallet: 1DuDhqSWdmRxJjaRRSpa9wRH7yf9ncgw56
I guarantee that after that, we'll erase all your "data" :D

A timer will start once you read this message. You have 48 hours to pay the above-mentioned amount.

Your data will be erased once the money are transferred.
If they are not, all your messages and videos recorded will be automatically sent to all your contacts found on your devices at the moment of infection.

You should always think about your security. We hope this case will teach you to keep secrets.
Take care of yourself.

恐吓邮件，并没有夹带任何的恶意档案或攻击代码，纯粹是透过在心理上的恐吓

2019趋势与结语

2018年曾出现的攻击手法，2019年可能多半都还能沿用，来自电子邮件的攻击从来不会绝迹，只会变形。2019年出现的攻击邮件夹带附件的比例可能会略为下降，以超链接配合遭到入侵的网站进行恶意程序下载攻击，或骗取帐号密码为主要攻击方法。然而要特别留意的是，随着多国语言自动翻译技术的进步，未来的邮件攻击的内文会更加流畅的以本地化语言进行社交工程攻击。

因此，教育使用者提高信息安全意识固然重要，但若光是要求使用者提升安全意识，来防御多变的邮件攻击恐怕已不足矣，企业更应提供使用者相较安全的电子邮件使用环境，如导入SPAM SQR ADM进阶防御机制，以降低遭受攻击的风险。

关于SPAM SQR与ADM进阶防御机制

Softnext守内安SPAM SQR内置多种引擎（恶意档案分析引擎、威胁感知引擎、智能诈骗引擎）及恶意网址信誉评价机制，可整合防毒与动态沙箱等机制。以多层式的运行过滤方式，深度剖析邮件中恶意档案、恶意链接的行为与特征，有效对抗钓鱼邮件、恶意威胁邮件的入侵。研究团队经过长时间追踪黑客攻击行为，模拟产出静态特征，其挂载的ADM（Advanced Defense Module）进阶防御机制，可防御鱼叉式攻击、APT攻击、BEC诈骗、文件漏洞攻击附件…等新型进阶攻击手法邮件。

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。
更多资讯请参考 www.asrc-global.cn