2019 守内安信息科技 & ASRC
第三季度电子邮件安全趋势

ASRC
Asia Spam-message
Research Center

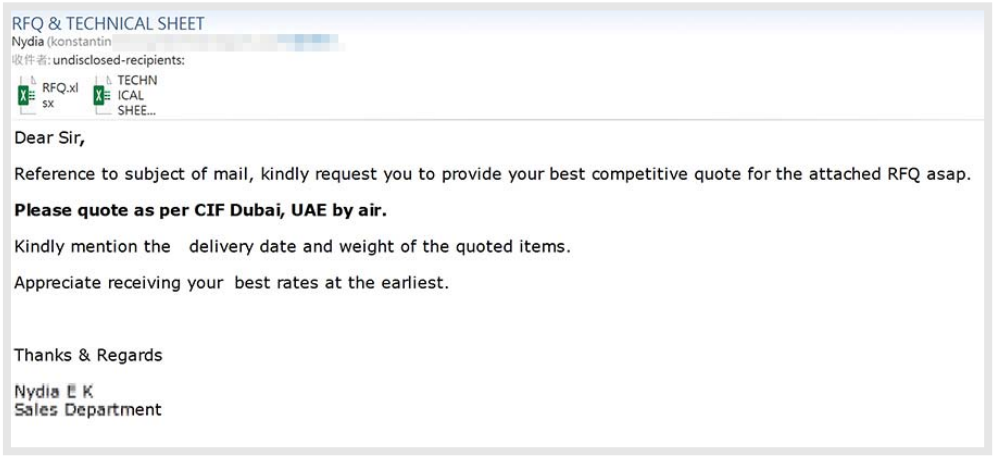
Nov 2019 released.

根据 ASRC 研究中心 (Asia Spam-message Research Center) 与守内安的观察，2019 年第三季不论是垃圾邮件或攻击邮件，在数量上都有明显上升。钓鱼邮件以及经过变化后的附件文件钓鱼邮件，是所有攻击邮件中最引人注目的；其次是漏洞利用的攻击，今年于电子邮件附件中最常见的漏洞利用当属 CVE20144114、CVE20180802 及其后续的衍生变形攻击。CVE20144114 数量在第三季度大幅增加，主要被攻击的目标有电子、食品、医疗相关产业；最后则是镜像文件病毒以及域名诈骗，这类威胁虽不直接，但也是信息安全防御工程上需要特别留意的地方。

漏洞利用频率创新高，较今年一月成长超过30倍

CVE20144114 漏洞利用频率，一季比一季高，9 月达到了高峰，较于今年一月的频率成长了 30 倍以上，且并非平均分布，而是集中在某些企业单位才出现大量攻击，被攻击目标企业包括电子、食品、医疗相关产业。其次是 CVE20180802 漏洞利用，虽然没有明显的突发性成长，每月都有稳定的攻击数量。

以第三季度的样本为例，最常见的就是夹带 .xlsx 的附件，少量为 .doc 的附件，附件文件名多半带有 Swiftt Copy、Scan、RFQ、Request、Remittance、Quotation、Purchase、Invoice、PO、Payment、Order等关键词。


RFQ & TECHNICAL SHEET
Nydia (konstantin
收件者: undisclosed-recipients:
RFQ.xlsx
TECHNICAL SHEE...
Dear Sir,
Reference to subject of mail, kindly request you to provide your best competitive quote for the attached RFQ asap.
Please quote as per CIF Dubai, UAE by air.
Kindly mention the delivery date and weight of the quoted items.
Appreciate receiving your best rates at the earliest.
Thanks & Regards
Nydia E K
Sales Department

CVE20180802 漏洞利用攻击样本

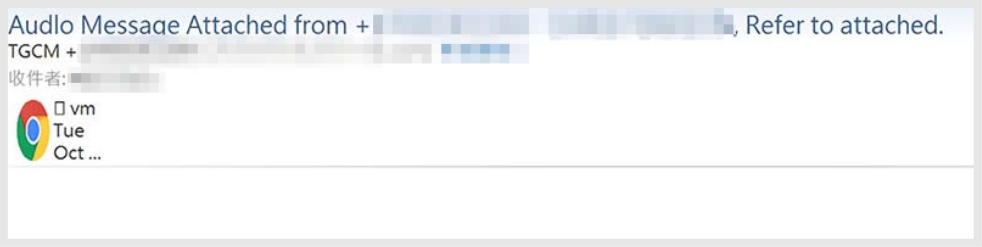
漏洞利用攻击防御建议

建议企业单位除了采用合适的邮件过滤软件外，也应进行内部软件信息安全盘点，将已知的漏洞修补，防范后续的 N Day 攻击。

附件文件钓鱼邮件利用浏览器与收信软件特性，发展更多更复杂的攻击组合

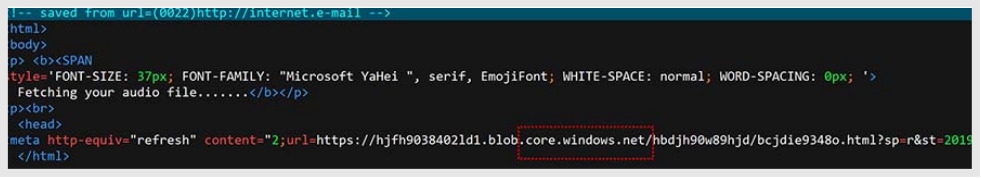
附件文件钓鱼邮件近几年的数量持续占有一定比例，主要是在一封钓鱼邮件中，不直接放入钓鱼网站的链接，取而代之的是放入一个带有钓鱼网站链接及其他网页程序代码的 HTML 附件。与一般钓鱼邮件目的相同，是为了骗取收件者的个人信息，但附件文件钓鱼邮件会利用浏览器与收信软件的某些特性，做出更多复杂的攻击组合。

比如某些收信软件会将 .html 的附件文件内容直接展开在邮件内；.html 由浏览器打开后，可以不再受到收信软件的限制，而能执行 Javascript、页面跳转等复杂与高风险的操作。钓鱼网址，可以躲过邮件扫描；通过合法网站的寄宿，还可绕过浏览器钓鱼黑名单的封锁。



附件文件钓鱼邮件样本

附件文件钓鱼邮件其中的.html展开后，会从本机的html页面，跳转至真实的钓鱼网站



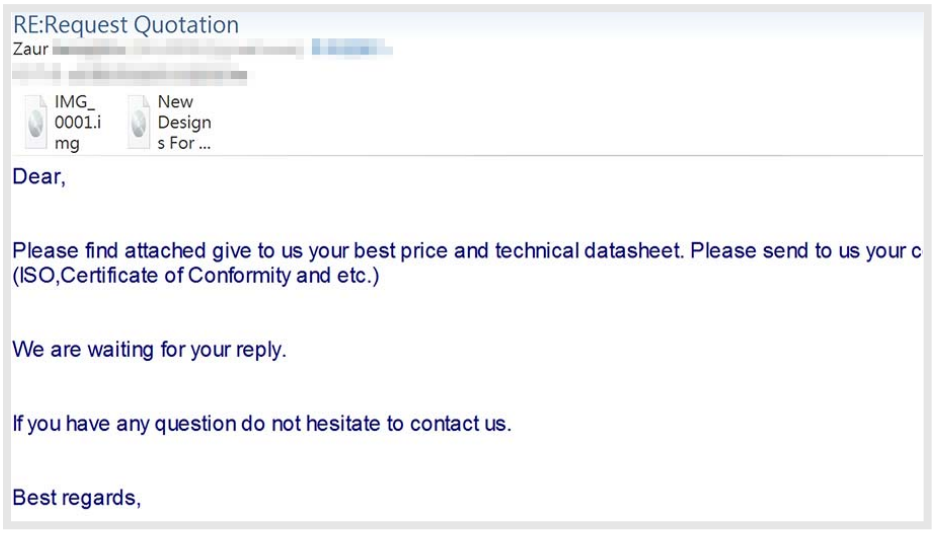
附件文件钓鱼邮件其中的.html，带有寄宿于合法网站的钓鱼页面

附件文件钓鱼邮件防御建议

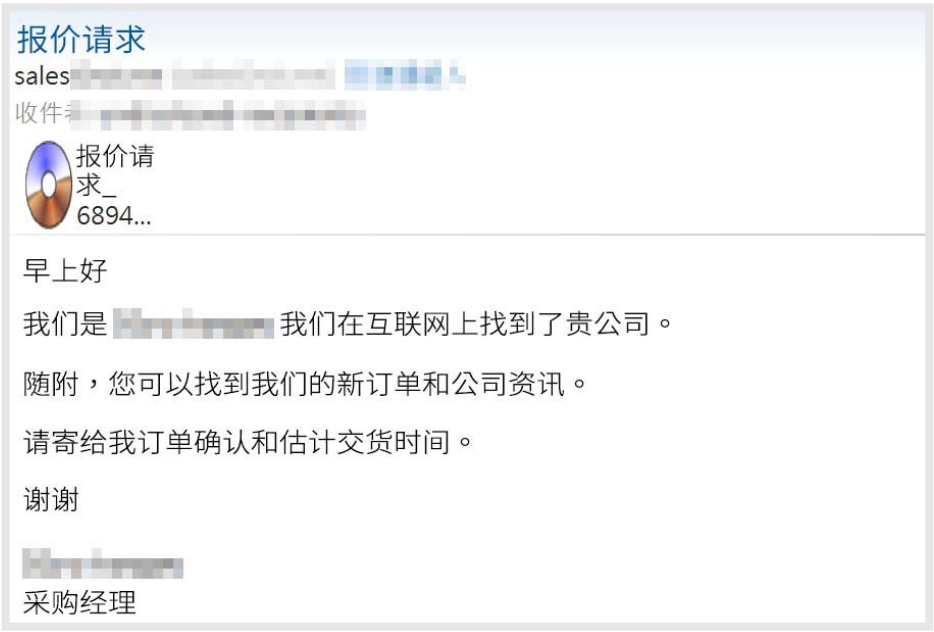
面对钓鱼威胁，最好从人的认知着手！在任何地方，要求输入个人信息时，特别不是由**主动获取服务而进行认证**；当**被动要求认证**时，一定要与原需求认证的单位通过其他渠道作确认。

镜像文件有其特定用途，多数因防御机制忽略检查，而沦为攻击者的工具

第三季度出现了不少夹带藏有病毒的 UDF 镜像文件附件。UDF 镜像文件原是用于光盘备份、刻录前暂存、准备或大量复制光盘之用，其扩展名多为.iso、.img等。由于这类镜像文件有其特定用途，部分的防病毒网关、防火墙、杀毒软件会忽略这类格式文件的大小限制或其内容的检查，因此攻击者就利用此缺口，将病毒嵌在标准合法的 UDF 镜像文件格式内，以躲过各种检查关卡。

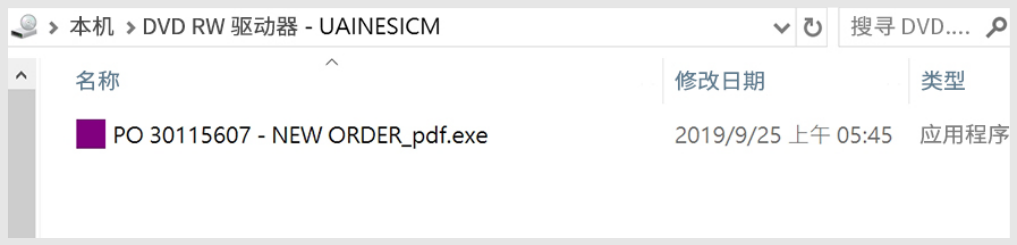


带有 .img 附件的镜像文件病毒邮件



带有 .iso 附件的中文内容镜像文件病毒邮件

病毒被嵌在标准的 UDF 镜像文件格式内，这个镜像文件其实是可以被挂载于虚拟光驱的；也能够被一般的解压缩软件打开而执行内容，且 Microsoft Windows 预设以档案总管作为此类镜像文件的开启关联程序，十分容易因为收件者误执行而中毒。



标准的 UDF 镜像文件可以被挂载于虚拟光驱，挂载后，里面的可执行文件就是病毒的本体

镜像文件病毒防御建议

设定显示被隐藏的扩展名；而管理者也要意识到镜像文件也可以被运用于攻击，并作为信息安全策略。

域名诈骗再进化，提供在线购买续费，窃取个人信息运用于后续攻击

域名诈骗邮件由来已久，过去常见的域名诈骗，多半利用纯社交工程的手段，以域名已过期、将遭占用，诱骗收件者回复后，进一步进行互动与诈骗。这类诈骗邮件提及的域名，有时是受害单位没注册过但非常相似的域名，因此若受害者思虑不周，直接查询邮件中提及的域名，可能信以为真落入攻击者的圈套。


BRAND & DOMAIN NAME REGISTRATION

Tim [redacted] 2018/7/23 下午 06

(Please forward this letter to your President or CEO. Thank you)

Dear Sir or Madam,

We are the Department of Asian Domain & Brand Registration Service in China. We have a formal affair to confirm with you. Our Registration Department received an application from PRCV GROUP who applies to register [redacted] as their Brand Name and some top-level domain names through our organization. We found the main body of domain names they apply to register is same as your company. We inform you of this matter because it involves your intellectual property.

Now we are handling this registration. Please let me know whether or not you authorized them to register these names. If you authorize them, I will formally pass through their registration; if not, please let us know as soon as possible in order to handle this issue better. Looking forward to your reply. Have a nice day!

Best Regards

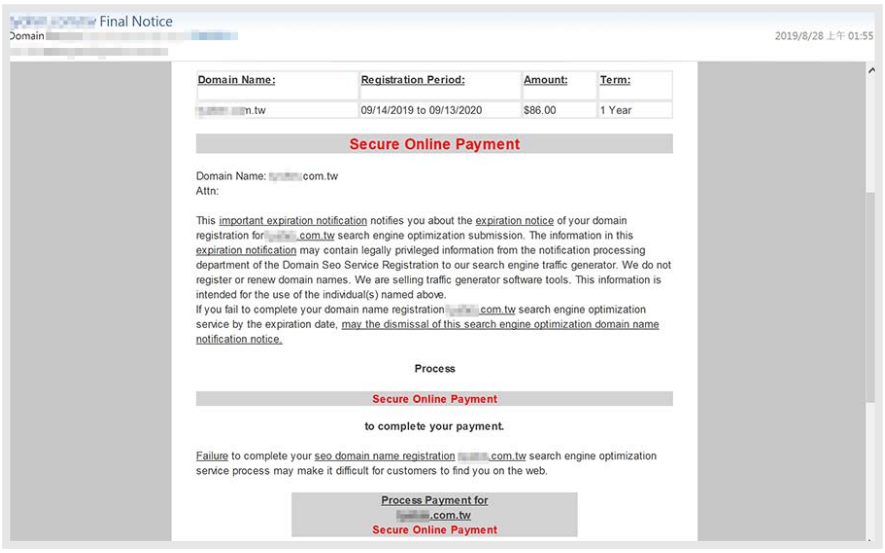
Tim Huang
Head [redacted]
Tel: [redacted] 6512-0084
No. [redacted], Hefei , China

过去常见的域名诈骗样本

在第三季度出现不少进化版的域名诈骗。大致与过去的域名诈骗内容差不多，但是多了可以在线购买或续用域名的链接，供受害人点击。当受害人信以为真并点击后，则会连到钓鱼网站，并要受害人填写详细的个人资料，攻击者得手后便可做后续的身分冒用或入侵受害者所使用的各种网络服务。

域名诈骗防御建议

域名的注册、管理，应有固定的管理人员与监控流程；若真的需要购买、续用域名，应主动寻访合适的合作厂商协助，而非照着可疑邮件的指示进行。


Final Notice

2019/8/28 上午 01:55

Domain Name:	Registration Period:	Amount:	Term:
[redacted]n.tw	09/14/2019 to 09/13/2020	$86.00	1 Year

Secure Online Payment

Domain Name: [redacted].com.tw
Attn:

This important expiration notification notifies you about the expiration notice of your domain registration for [redacted].com.tw search engine optimization submission. The information in this expiration notification may contain legally privileged information from the notification processing department of the Domain Seo Service Registration to our search engine traffic generator. We do not register or renew domain names. We are selling traffic generator software tools. This information is intended for the use of the individual(s) named above.
If you fail to complete your domain name registration [redacted].com.tw search engine optimization service by the expiration date, may the dismissal of this search engine optimization domain name notification notice.

Process

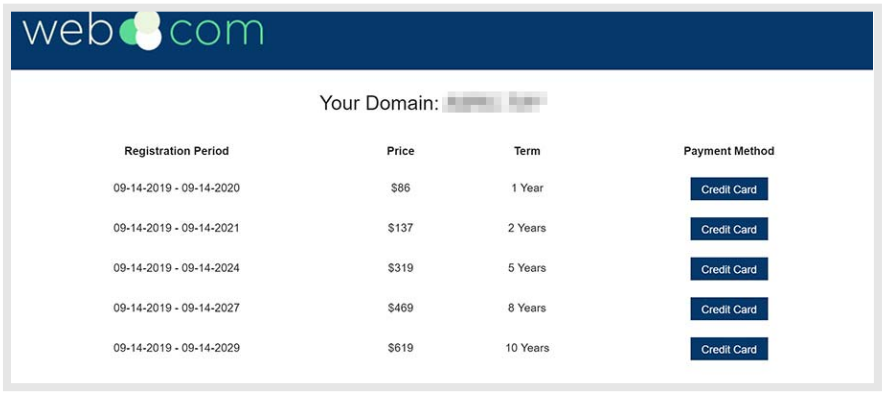
Secure Online Payment

to complete your payment.

Failure to complete your seo domain name registration [redacted].com.tw search engine optimization service process may make it difficult for customers to find you on the web.

Process Payment for [redacted].com.tw
Secure Online Payment

域名诈骗邮件多了可以在线购买或续用域名的链接


web.com

Your Domain: [redacted]

Registration Period	Price	Term	Payment Method
09-14-2019 - 09-14-2020	$86	1 Year	Credit Card
09-14-2019 - 09-14-2021	$137	2 Years	Credit Card
09-14-2019 - 09-14-2024	$319	5 Years	Credit Card
09-14-2019 - 09-14-2027	$469	8 Years	Credit Card
09-14-2019 - 09-14-2029	$619	10 Years	Credit Card

看似真的域名购买的钓鱼网站


Secure Transaction

Billing Information	
First Name:	
Last Name:	
Company Name:	
Country:	United States
Address:	
City:	
State/Province:	- Select State -
Zip/Postal Code:	
Phone Number:	
Fax Number:	
Email Address:	
Website Address:	

Continue

主要用以骗取受害者个人信息，以进行后续身分冒用等攻击

总结

曾经暴露在外的电子邮箱，经网络爬虫收录之后，天天都收到许多广告与攻击邮件，几乎难以有洗白的一天，这种情况持续了多年，虽然大家对于邮件地址不随意暴露在公开的网页开始有了认知，但暴露在外的文件内带有电子邮箱的情况仍然不少，这值得注意。

此外，各种信息安全事件，慢慢地都不是独立存在了，只要曾经发生过入侵，或是个人、企业单位的数据曾经被外泄，接踵而来的就是一次又一次BEC攻击，或是收不完的网络钓鱼邮件。电子邮件的攻击手段不断推陈出新，虽然少有横空出世新的攻击手法，但通过“利用”、“链接”、“交错”将旧的攻击手段缓慢持续演进，却是从未停止过的！

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。