# 文档型漏洞攻击研究报告

360互联网安全中心

2017 年 7 月 3 日

# 摘　　要


- 本文研究的漏洞文档是指利用漏洞进行网络攻击的恶意文档，且此报告中统计的数据是2017 年一月到六月的漏洞文档。
- 通过对 360 互联网安全中心截获的漏洞文档抽样分析统计显示，攻击者最喜欢利用的载体为 Office 文档，占比高达 52.3%，其次为 RTF（Rich Text Format）文档占比达到了31.5%。
- 漏洞文档直接下载恶意程序是攻击者使用的主要方式，占据 68.5%，直接释放恶意程序比例达到了 24.1%。
- 在含有伪装内容的文档中，跟经济相关的文档占据比例最大，达到了 15.7%，其次为教育科研机构，占比达到 9.6%。
- 抽样统计显示，2017 上半年中 CVE-2017-0199 漏洞被利用的次数最多，相关的漏洞文档占比高达 35.5%，其次是 CVE-2012-0158 占据 17.5%。
- 在 2017 上半年被利用的主要漏洞中，变化最为明显的是 CVE-2017-0199，该漏洞在 2017 年前三个月未被公开，其占比为 0，但是被公开后其占比一路走高，在四月份集中爆发，占比超过了所统计漏洞文档的 60%。
- 通过统计漏洞文档载荷下载或释放的恶意程序功能，发现远控木马和信息盗取木马依然是主流，分别达到了 36.6%和 29.3%。
- 统计的恶意程序中，EXE 和 DLL 文件依然占据主导地位，分别占 70%和 16%。
- 恶意程序开发语言中 C/C++占比最高，达 47.8%，其次为 C#语言，占 31.1%。
- 漏洞文档载荷下载或释放的恶意程序中，攻击者最喜欢使用的程序名为 svchost.exe，占比高达 48.3%，其次为 winlogin.exe 占 13.7%。
- 通过统计漏洞文档载荷直接访问或通过域名解析访问的两类 C&C 服务器，发现恶意程序作者所使用的 C&C 服务器地理位置主要集中在美国、俄罗斯以及德国，占比分别为43.9%、15.2%和 7.0%。
- 通过统计载荷直接使用域名访问 C&C 服务器的漏洞文档，发现攻击者更喜欢.com 的顶级域名作为C&C服务器，其占比高达61.1%，尼日利亚国家的顶级域名.ng，占比为10.4%。
- 通过统计载荷直接使用 IP 地址访问 C&C 服务器的漏洞文档，发现攻击者偏向于使用443、80 与 8080 端口，占比分别为 32.8%、25.4%和 18.3%。


**关键词：** 漏洞文档、载荷、恶意程序、变化趋势、C&C 服务器、顶级域名、端口

# 目　　录

# 研究背景

由于反病毒技术快速发展及免费安全软件在全球的高度普及，恶意程序的传播变得越来越困难。自 2013 年以来，中国一直是全球个人电脑恶意程序感染率最低的国家。

但是随着漏洞挖掘及利用技术越来越公开化，导致越来越多的黑客更加倾向于利用常见办公软件的文档漏洞进行恶意攻击，特别是在一些 APT（Advanced Persistent Threat）攻击中，更是体现得淋漓尽致。针对特定目标投递含有恶意代码的文档，安全意识薄弱的用户只要打开文档就会中招。

对于漏洞文档（本文所说的漏洞文档是指利用漏洞进行网络攻击的恶意文档），为何用户容易中招呢？2017 年 6 月，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研究。总结了两部分原因，一、漏洞文档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文档名，结合鱼叉或水坑等攻击方式进行传播，并配有诱饵内容，极具欺骗性，导致很多用户中招；二、部分用户安全意识只停留在可执行的恶意程序上，对漏洞文档危害的防范意识较弱。

鉴于此种情况，360 安全专家对 2017 上半年 PC 平台上漏洞文档进行深入的抽样分析研究，形成此报告，希望能够借此帮助更多的用户提高安全意识，对漏洞文档有个直观感受，有效防范此类恶意攻击。

# 第一章　漏洞文档综述

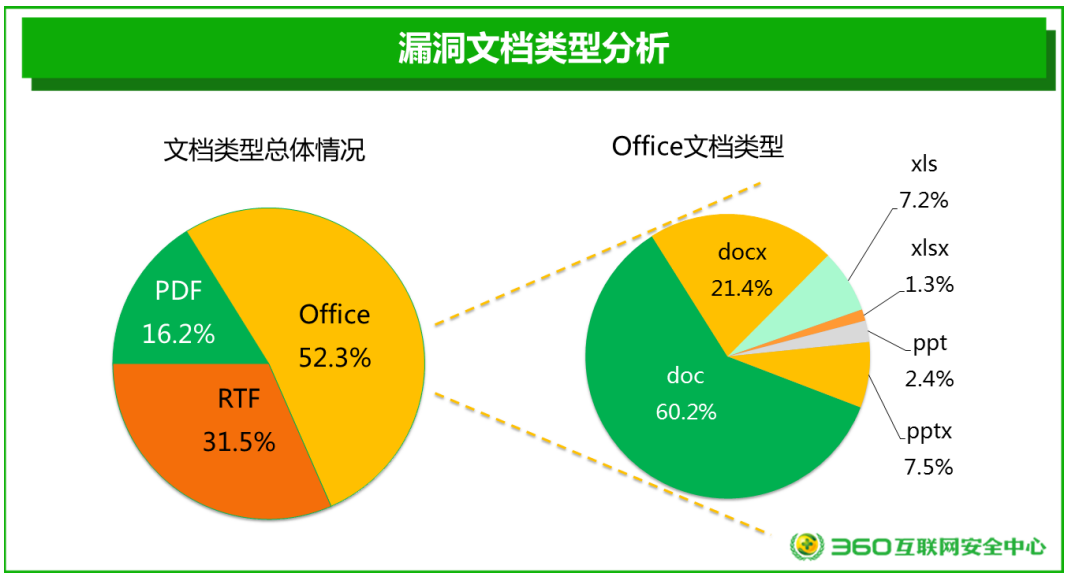
## 一、　漏洞文档类型分析

通过对 360 互联网安全中心截获的漏洞文档抽样分析统计显示，攻击者最喜欢利用的载体为 Office 文档，占比高达 52.3%。由于 Office 文档类型众多，包括 doc、docx、xls、xlsx、ppt、pptx 等类型，攻击者选择的载体类型较多，并且 Office 用户群体庞大，因此此类漏洞文档占比最高。其中在 Office 系列中 Word 文档类型尤为突出，占据了 Office 文档的 81.6%，其次是 PowerPoint 文档，占据了近 10%。

除了 Office 文档之外，攻击者也喜欢利用 RTF（Rich Text Format）文档作为载体进行攻击，其占比也达到了 31.5%。很多 Office 漏洞需要成功运行恶意程序，会嵌入一些 OLE 对象进行堆喷射或用于绕过 ASLR（Address Space Layout Randomization）安全机制，而 Rich Text Format 文档很容易嵌入 OLE 对象，并且默认情况下 RTF 类型的文件系统会调用 Word 程序来解析，因此很多攻击者会使用 RTF 文档来制作漏洞利用样本，以便更好的触发漏洞运行恶意代码。

此外，PDF 文档也在文档漏洞类型中占据 16.2%，该类文档中通常包含一些恶意的 JavaScript 脚本，这些脚本会连接云端下载恶意程序。

另外，研究过程中，我们观察到大量包含了漏洞文档的电子邮件，这是由于攻击者经常会通过电子邮件来进行传播，并且会精心构造邮件内容，以便诱导用户点击，提高中招比例。在此提醒用户，请不要轻易打开陌生人发来的文档，该文档很可能携带恶意载荷，导致自己蒙受损失。




## 二、　漏洞文档载荷类型分析

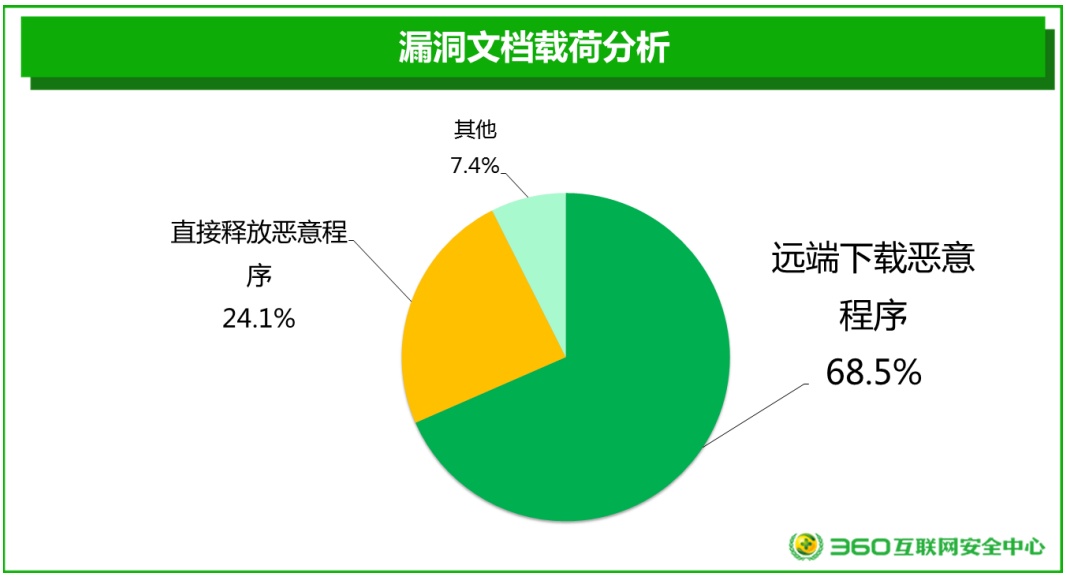
这些经过攻击者精心伪装的漏洞文档一旦运行后，是怎么样运行恶意程序或代码呢？

抽样统计显示，漏洞文档直接下载恶意程序是攻击者使用的主要方式，占据 68.5%，该方式是指攻击者在精心构造的样本中嵌入恶意链接，用户打开文档中招后就会连接远端下载

恶意程序，从而导致用户计算机中毒。攻击者使用这种载荷的好处是可以随时在云端替换下载文件，以达到自己想要的目的。

此外，漏洞文档直接释放恶意程序比例也较大，达到了 24.1%，该类方式主要是指攻击者直接将恶意程序捆绑在漏洞文档中，用户打开文档触发漏洞的同时，载荷会将捆绑的恶意程序运行起来，导致用户中招。这两类方式是现今漏洞文档中出现的主流方式。

另外，下图中所列出的其他类型的载荷主要包括两部分，一、漏洞文档中的载荷主动连接远端特定 IP 和端口等待命令，以便进行不同操作；二、漏洞文档中的载荷选择在本地开放特定端口，等待攻击者主动连接，这种方式可能会因为防火墙不允许外边的计算机主动连接该计算机而失效。因此在实际的漏洞文档中，载荷一般是主动连接远端地址，而不是等待远端来连接。这两类载荷跟上面所说的漏洞文档下载恶意程序载荷和漏洞文档释放恶意程序载荷有着较大区别，它是一段 shellcode，直接与远端服务器交互，不存在特定的恶意程序，此两种载荷经常出现在 PDF 漏洞文档中。



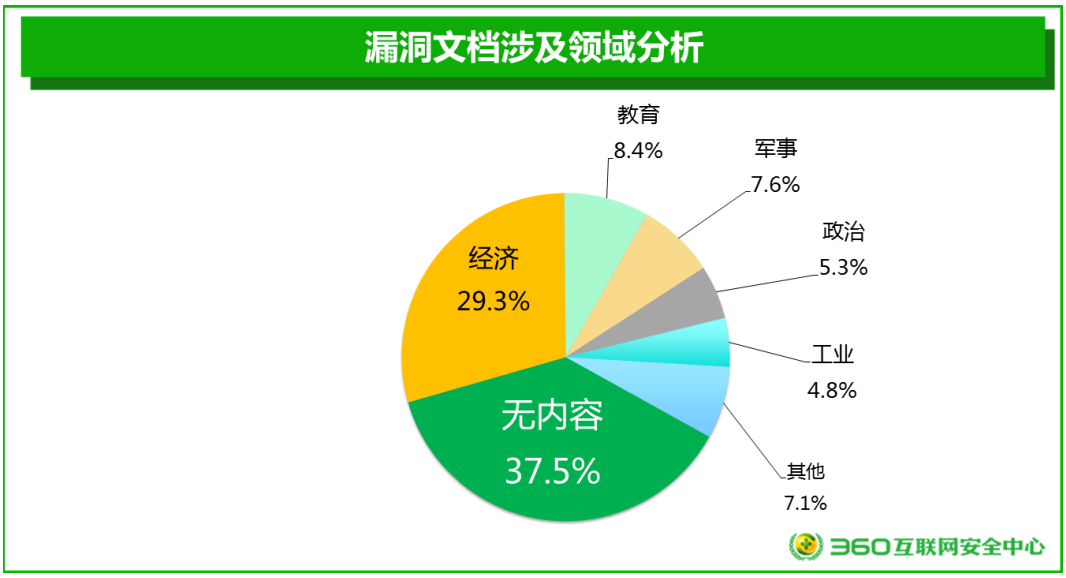

## 三、 漏洞文档涉及领域分析

抽样分析统计显示，37.5%样本为空白内容，没有进行伪装，其中主要原因有两点：1、为了节约攻击成本及缩短漏洞文档制作时间，比如攻击者通过邮件传播，他们只需要在邮件内容中诱导用户打开文档附件就能达到攻击效果，不需要添加文档伪装内容；2、很多真实的漏洞利用样本是基于已有版本改进的，如原模版没有内容，那么部分攻击者不会再主动添加文档伪装内容，因为贸然添加了伪装内容，容易破坏漏洞文档的结构，导致漏洞利用失败。

在含有伪装内容的样本中，跟经济相关的文档占据比例最大，达到了 29.3%，这类漏洞文档通常是用于攻击企业、公司，内容一般是涉及订单信息、材料价格等。其次是教育科研机构，占比达到 8.4%，这些文档内容通常涉及到高等学府的研究成果、高考成绩等。需要特别注意的是与政治相关的文档也占据了 5.3%，这部分文档内容涉及一些会议概要以及向政府部门提出的建议等，该类文档通常出现在 APT 攻击中。上面提到的这些漏洞文档通常会使用邮件传播，并且邮件内容与文档名相符合，很多安全意识薄弱的用户很容易中招。

另外需要说明的是，“其他”类别占据了 7.1%，这部分内容涉及到成人、诱导执行、农业等方面。其中诱导执行相关的文档通常涉及到朋友之间聚会照片、个人信息等，此类对于敏

感性不强或好奇心比较重的用户，很容易去点击这些文档导致自己蒙受损失。因此在这里也提醒用户对于不知来历的文档，应特别小心，否则很容易中招。



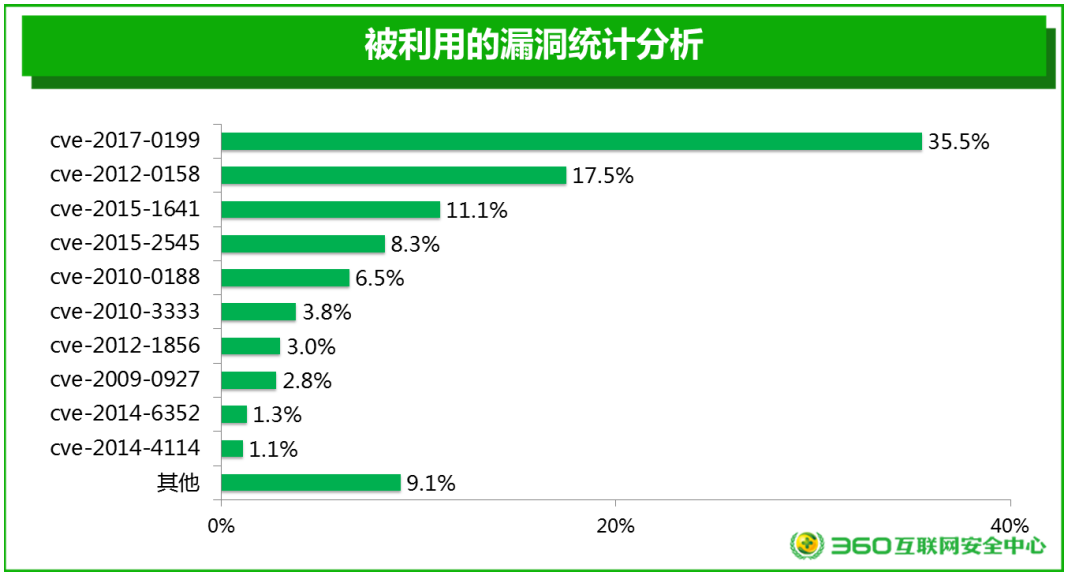

## 四、 被利用的漏洞统计分析

通过对 360 互联网安全中心截获的漏洞文档抽样分析统计显示， CVE-2017-0199 漏洞被利用的次数最多，相关的漏洞文档占比高达 35.5%，这是由于该漏洞为 2017 年 3 月爆出的新漏洞，很多用户未能及时打补丁，并且漏洞利用方法简单，漏洞影响范围广，Windows 操作系统之上的所有 Office 版本，包括在 Windows 10 上运行的最新 Office 2016 均受影响，危害程度极高。当用户打开包含该漏洞的文档（Microsoft Office RTF 格式）时，此漏洞会下载并执行包含 PowerShell 命令的 Visual Basic 脚本，往往攻击者只需要在 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，由于攻击成本低且容易量产恶意文档，所以该漏洞深受攻击者喜爱。

除了 CVE-2017-0199 之外，漏洞受欢迎程序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 17.5%和 11.1%。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，因此也很受攻击者青睐。

此外，CVE-2015-2545 漏洞占比也较高，达到了 8.3%。其中比较特别的是 CVE-2010-0188 漏洞，该漏洞为 PDF 漏洞，它在 PDF 漏洞中占比最高，在总的漏洞样本占比也达到了 6.5%，在该漏洞文档中载荷通常为上述所说的直接连接服务端等待命令或者本地开放端口等待攻击者主动连接。由于可利用的漏洞众多，因此“其他”漏洞文档占比达到了 9.1%，其中包括了如 CVE-2016-7193、CVE-2013-3906、CVE-2008-2992 等漏洞。

据下图统计显示，攻击者更偏向于使用影响版本广且利用稳定的漏洞来进行攻击，这样有助于提高用户中招概率，并且此类漏洞利用方法通常比较成熟，也能减少攻击者前期准备时间和攻击利用成本。

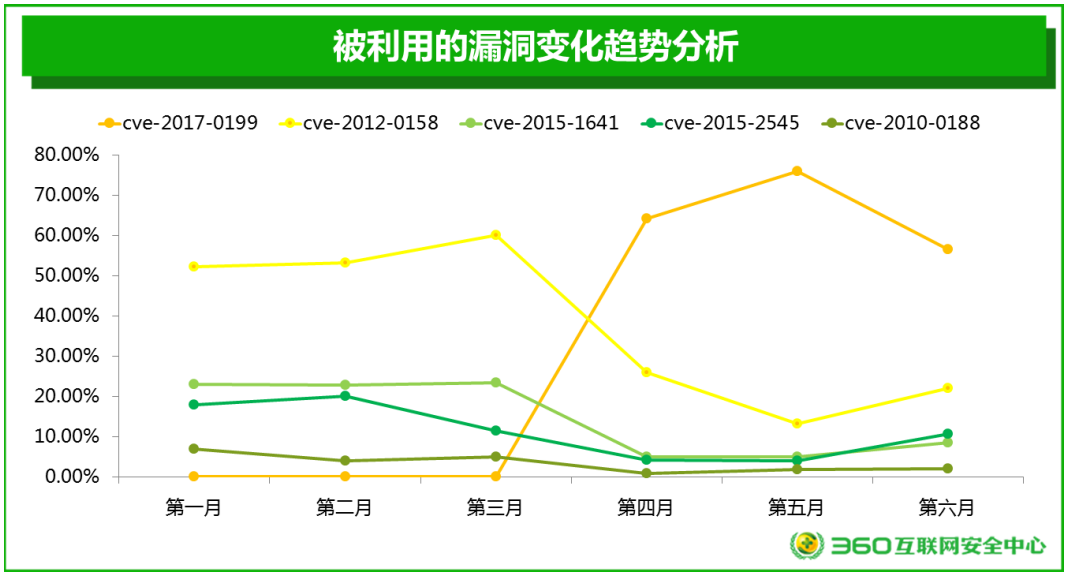



## 五、 被利用的漏洞变化趋势分析

下图给出了 2017 上半年被利用漏洞占比前五的变化趋势，变化趋势最为明显的是 CVE-2017-0199，该漏洞在 2017 年前三个月未被公开，其占比为 0，但是被公开后其占比一路走高，在四月集中爆发，占比超过了所统计五类漏洞文档的 60%，说明该漏洞公开披露后被攻击者广泛利用，并且第五月继续呈现出上升趋势，但是在第六月逐渐下降，这跟漏洞补丁出现时间相关，虽然微软在漏洞披露后快速发布了漏洞补丁，但是部分用户并未意识到该漏洞的危害，打补丁存在延迟，这也是六月份漏洞文档才逐渐下降的原因。

其次，在 360 互联网安全中心 2017 上半年截获的所有漏洞文档中，CVE-2012-0158 占据比例一直偏高，在第三月超过了总量的百分之六十，说明了 CVE-2012-0158 漏洞很受攻击者欢迎，被利用的次数居高不下，并且该漏洞也经常出现在 APT 攻击中。与此对应的还有 CVE-2015-1641 漏洞，该漏洞在前三个月一直处于缓慢上升阶段，但是在四月份下降比较明显，这是由于攻击者将目标瞄准了其他高危漏洞，如 CVE-2017-0199 漏洞。另外，CVE-2015-2545 漏洞被利用的次数一直趋于稳定，并且此类漏洞文档一般是通过现有模版配置生成。

另外需要注意的是 CVE-2010-0188 漏洞，该漏洞属于 Adobe Reader 漏洞，该漏洞在统计的漏洞中一直处在最低位置，由于 Adobe Reader 更新很频繁，打补丁的速度很快，很多攻击者通过此漏洞攻击容易失败，这直接导致了该漏洞利用率较低。

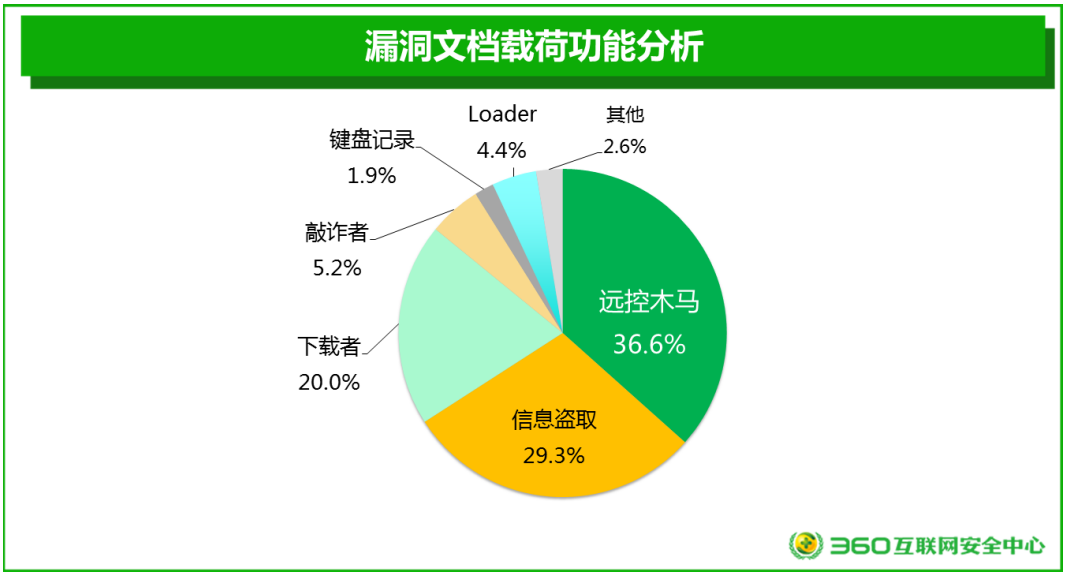

被利用的漏洞变化趋势分析
cve-2017-0199
cve-2012-0158
cve-2015-1641
cve-2015-2545
cve-2010-0188
80.00%
70.00%
60.00%
50.00%
40.00%
30.00%
20.00%
10.00%
0.00%
第一月
第二月
第三月
第四月
第五月
第六月
360互联网安全中心

# 第二章　漏洞文档载荷综述

## 一、　载荷功能分析

下图给出了漏洞文档载荷下载或释放的恶意程序功能占比，可以看出在所有的恶意程序中，远控木马和信息盗取木马依然是主流，分别达到了 36.6%和 29.3%。远控木马会使用户计算机变成肉鸡，并随时窃取用户资料，并且攻击者通常也会使用肉鸡进行二次攻击，如 DDOS 等。信息窃取木马会获取计算机上保存的邮件账户密码和浏览器中保存的账户密码。此外，下载者占比也达到了 20%，这类程序通常是连接云端下载恶意程序，以便更好的控制用户计算机，或进行推广以达到盈利目的。

需要特别引起注意的是，随着恶意软件的发展，越来越多的攻击者倾向于开始倾向于直接获取利益，这直接导致了敲诈者病毒的泛滥。2017 年上半年统计数据显示漏洞文档携带的敲诈者病毒占比达到 5.2%。敲诈者病毒是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。在今年 5 月 12 日，爆发了“WanaCrypt0r”（永恒之蓝）勒索病毒，使全球多个国家的地区机构及个人电脑遭受攻击，据不完全统计，它在爆发后的几个小时内就迅速攻击了 99 个国家的近万台设备，并在大量企业组织和个人间蔓延，因此敲诈者病毒不容忽视，建议用户保持杀毒软件随时开启，不要打开来路不明的程序和文件。此外，在今年 6 月 27 日，爆发了 Petya 勒索病毒，使乌克兰、俄罗斯、印度、西班牙、法国、英国以及欧洲多国遭受袭击，其政府、银行、电力系统、通讯系统、企业以及机场都受到了不同程度的影响。通过今年爆发的两次大规模敲诈者病毒中招事件，可以看出敲诈者病毒的盈利模式与技术模式越来越受攻击者喜爱，未来敲诈者病毒将越来越流行。

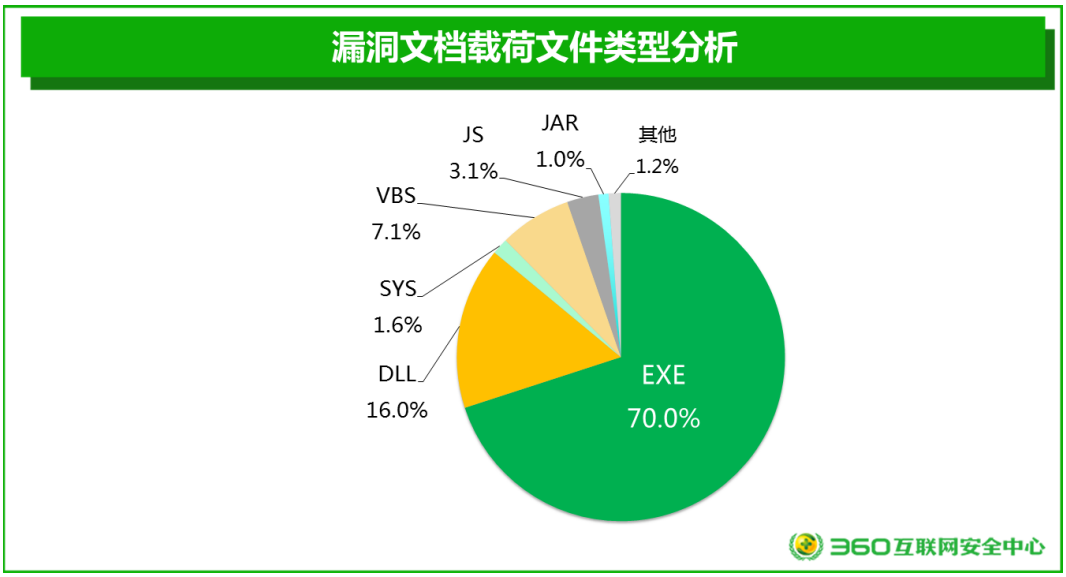



## 二、　载荷文件类型分析

从下图的文件类型分析可以看出，漏洞文档释放或下载的文件类型也更加的多元化，从传统的 PE 文件到各种脚本文件，以及 JAR 文件。但是传统的 PE 文件依然是主流，其中 EXE 和 DLL 依然分别占 70%和 16%。另外不容忽视的是，木马作者对脚本的使用也越来越多，

其中 VBS 和 JS 分别占 7.1%和 3.1%。脚本文件有开发速度快，语法简单而且强大，易混淆等特点，因此在越来越多的漏洞利用样本中被使用。

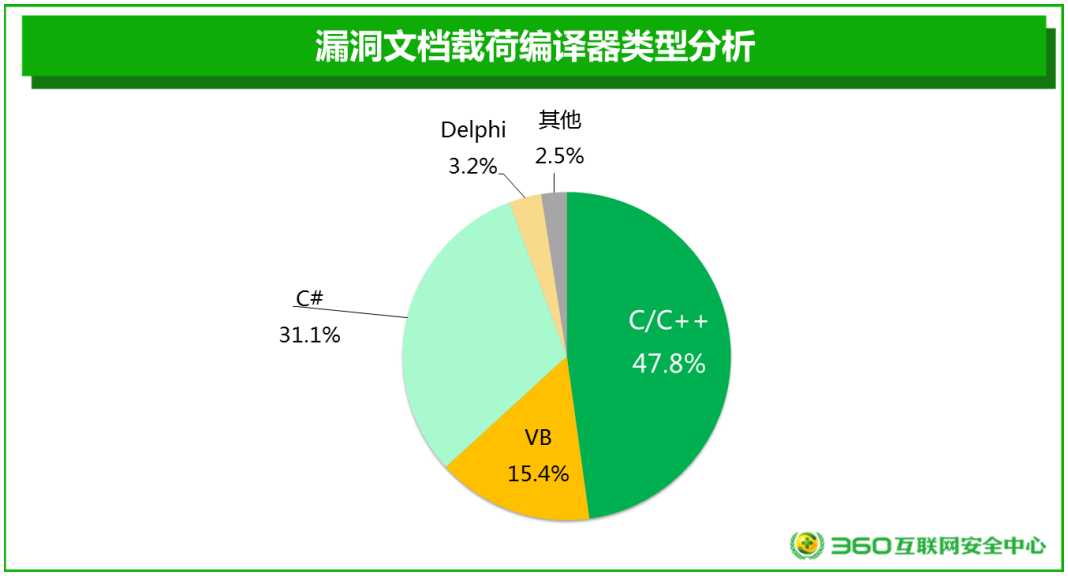
除 PE 文件和脚本文件外，最近还捕获到 JAR 的远控样本。这种变化是由于杀毒软件对传统的 PE 文件的查杀越来越完善，对混淆加壳等技术手段处理后的 PE 类型的木马病毒也能很好的进行查杀。现在越来越多的计算机会安装 JAVA 运行环境，木马作者为了更好的躲避杀毒软件查杀而选择使用 JAVA 进行木马开发。虽然现在 JAVA 开发的样本依然较少，JAR 类型的恶意程序只占有 1.0%，但却代表了病毒木马的一种发展趋势，病毒木马类型已经不再是传统单一的 PE 文件形式了，而是多元化的发展。




## 三、 载荷编译器类型分析

通过对漏洞文档载荷使用的编译器类型统计分析，发现主流的开发语言依然是 C/C++，排名第一，占比高达 47.8%。其次是 C#语言，占比为 31.1%，C#语言由于开发简单快速以及语法优雅等优点，近几年得到了快速发展，很多攻击者也开始选择该语言进行恶意程序开发，但是由于未处理过的 C#能够直接反编译，所以使用 C#进行开发恶意程序的攻击者基本还会进行混淆加壳，防止恶意程序被分析。与此同时，我们还发现越来越多的外壳程序开始使用 C#语言进行开发。排名第三是 VB 语言，虽然占比达到 15.4%，但是分析载荷时发现很多恶意程序是因为外壳代码采用了 VB 语言编写，当把壳代码去掉后，主要恶意功能还是使用其他语言编写，核心代码使用 VB 语言开发的恶意程序相对较少。

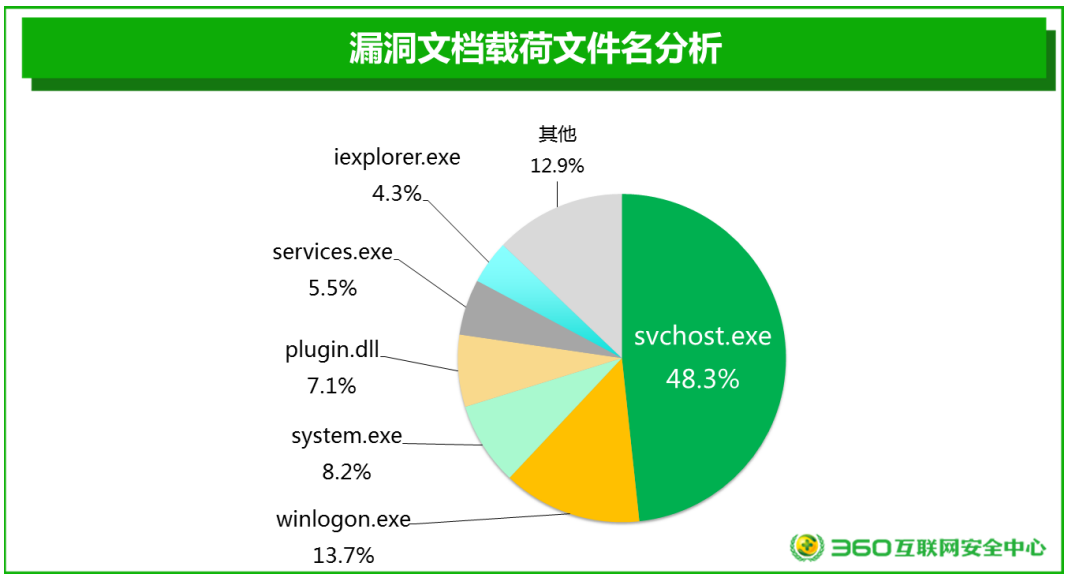
令人比较诧异的是，使用传统语言 Delphi 进行开发的恶意程序越来越少，只占 3.2%，这与 Delphi 语言逐渐没落有关，Delphi 7 以后，尽管 Delphi 版本不断升级改变，但都没有得到广泛应用，很多 Delphi 程序员转向其他平台，导致使用 Delphi 语言进行开发的程序员越来越少，这也是 Delphi 恶意程序占比较低的原因。




## 四、 载荷文件名分析

恶意程序为了更好的隐藏自己，通常会使用特殊的文件名用于迷惑用户，以便能长时间驻留在用户的计算机上。其中漏洞文档载荷最常使用的文件名莫过于 svchost.exe，占比高达 48.3%，由于 svchost.exe 本身就是操作系统系统程序的名称且一般都会存在多个 svchost.exe 进程，多出一个进程用户也很难察觉到，所以该文件名被很多攻击者使用。其他一些系统程序的文件名也常被使用，如 winlogon.exe 占 13.7%，services.exe 占比为 5.5%，伪装成这些文件名普通用户很难被察觉。比较特殊的是 plugin.dll 文件名，该名字之所以出现比例达到 7.1%，主要是由于利用 CVE-2015-2545 漏洞的样本基本都会释放出 plugin.dll 文件，再使用 plugin.dll 进行二次下载。

除使用系统程序的文件名外，攻击者也会使用和系统程序文件名相似度较高的文件名，如 iexplorer.exe 文件名，该文件名与 IE 进程名 iexplore.exe 非常相似，很容易用于迷惑用户。此外，在其他类别中主要包括 bro.exe、name.exe 及随机文件名，用户在网络上要特别注意具有此类文件名的文件。

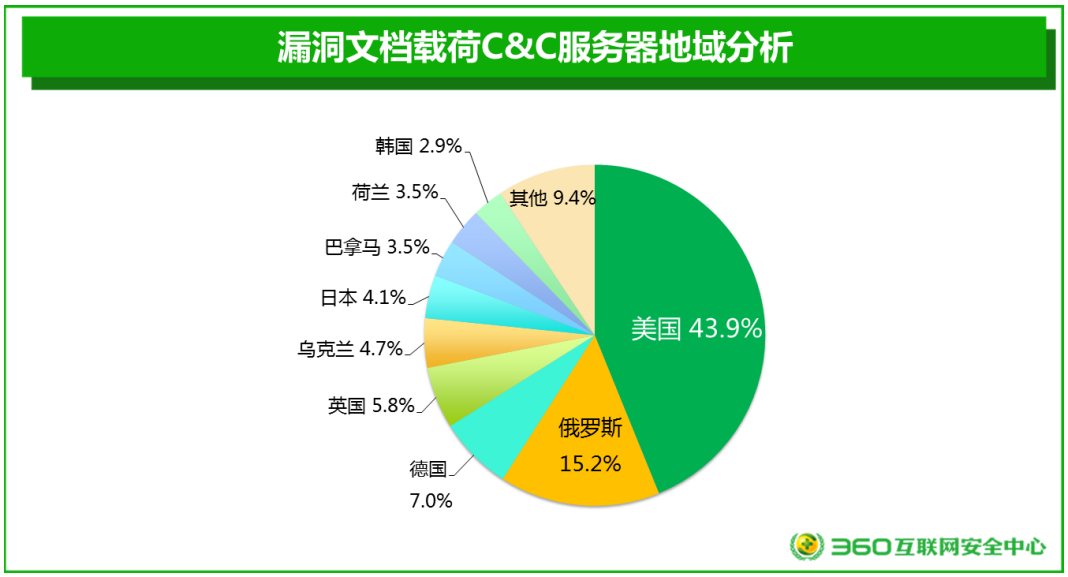


## 五、 载荷 C&C 服务器地域分析

通过统计漏洞文档载荷直接访问或通过域名解析访问的两类 C&C 服务器，并通过 IP 查找服务器所在地发现，恶意程序作者所使用的 C&C 服务器地理位置主要集中在美国、俄罗斯以及德国，其中美国占比最高，达到了 43.9%，成为 C&C 服务器数量最多的国家，排名第二与第三的是俄罗斯与德国，占比分别为 15.2%和 7.0%。紧随其他的有英国、乌克兰等地。

需要特别注意主要是，C&C 服务器地域分布很广，现在一些小国家也逐渐占据了一些比例、如巴拿马与荷兰都占据了 3.5%。另外其他地域占据了 9.4%，这中间主要包括了中国、法国、罗马尼亚、巴西、捷克、伊拉克、土耳其、泰国、马来西亚等国。

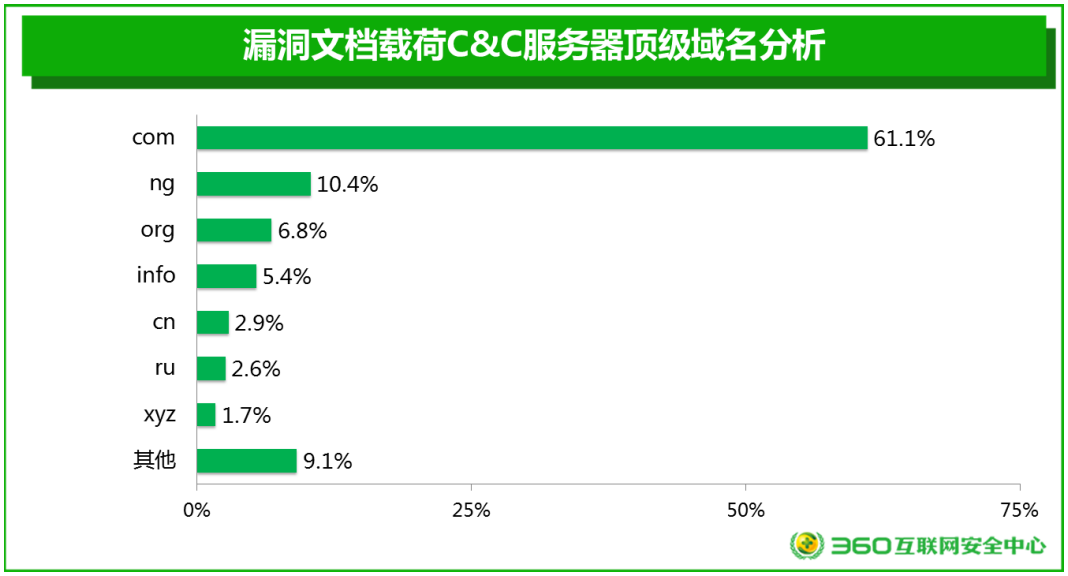
需要特别注意的是：部分攻击者为了更好的隐藏自己，通常会使用除本国以外的其他地域 C&C 服务器，此类攻击者很难被定位到具体位置。




## 六、 载荷 C&C 服务器顶级域名分析

通过统计载荷直接使用域名访问 C&C 服务器的漏洞文档，发现攻击者更喜欢.com 的顶级域名作为 C&C 服务器，其占比高达 61.1%，远远大于其他顶级域名，其原因可能在于.com 域名是国际顶级域名，非国家域名，在国际上使用较早、运用范围广且申请容易，所以很多攻击者选择此类域名作为 C&C 服务器。令人比较诧异的是尼日利亚国家顶级域名.ng，排名第二，占比为 10.4%，该域名在日常生活中所见不多，但是在漏洞文档载荷中该域名出现的频率较高，排名第三位的是.org 域名，占比为 6.8%。

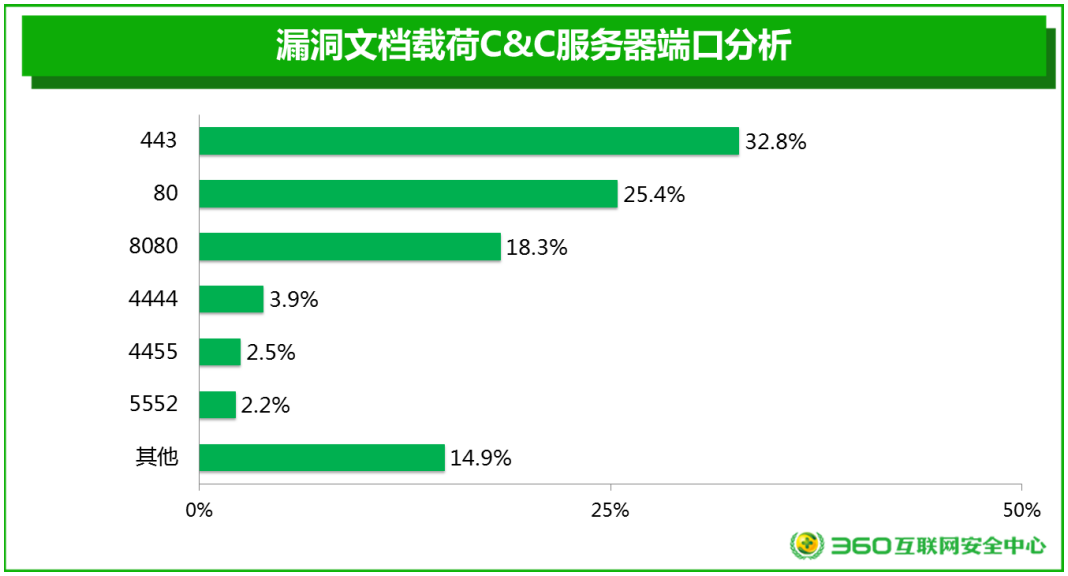
需要特别注意的是，顶级域名.cn 占比达到了 2.6%，该类型的部分 C&C 地址可能是攻击者控制的中转服务器地址。另外，.info、.ru、.xyz 等顶级域名在所有 C&C 地址服务器中也排名靠前，在其他类别中主要包括.us、.ga、.me、.cz、.ro、.in、.net 等顶级域名。




## 七、 载荷 C&C 服务器端口分析

通过统计载荷直接使用 IP 地址访问 C&C 服务器的漏洞文档，发现很多攻击者偏向于使用 443 和 80 端口，占比居前二位，分别为 32.8%与 25.4%，其主要原因在于这两个端口都是浏览网页的常用端口，攻击者使用该端口与 C&C 服务器进行通信时，通常不会被防火墙、网关等设备拦截，攻击者正是利用这一点，才倾向于使用这两个端口进行数据传输。此外，443 端口主要用于 HTTPS 服务，是提供加密和通过安全端口传输的另一种 HTTP，使用该端口安全性很高，攻击者用 443 端口传输重要数据，不易被察觉，这说明了使用漏洞文档进行攻击的攻击者很注重自身安全。排名第三的是 8080 端口，占比为 18.3%， 8080 端口广泛被用于 WWW 代理服务，可以实现网页浏览，攻击者也常利用该端口进行攻击。

需要特别注意的是，攻击者也常使用 4444 与 4455 端口，这两个端口之所以常被使用，是由于网络上广泛流传的 Metasploit 漏洞攻击教程的示例大多使用了这两个端口，部分攻击者依据教程配置荷载时也就同样使用了这两个端口。5552 端口是部分后门程序常使用的端口，另外其他类别主要包括 55555、8000、689 等端口。



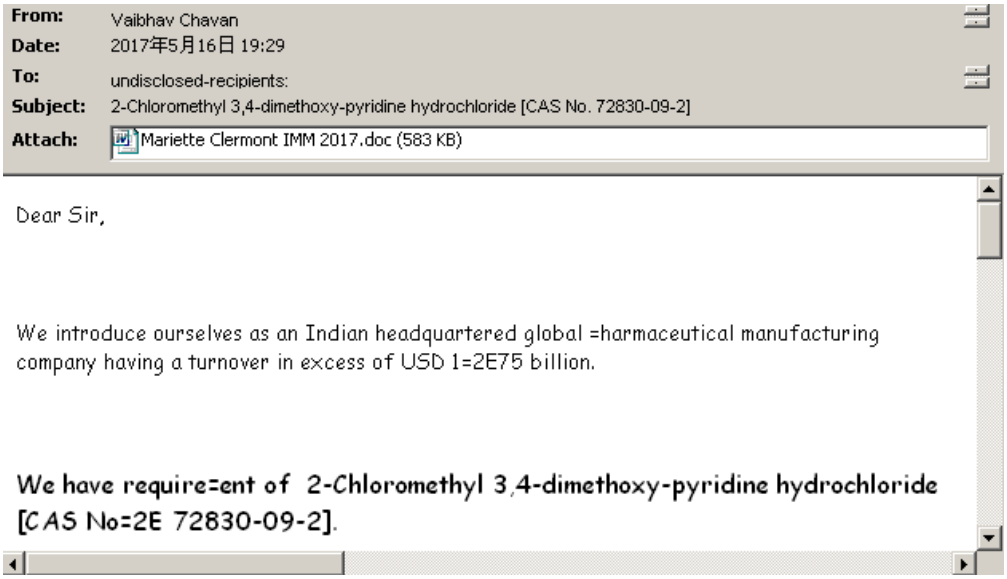
# 第三章　典型漏洞文档案例分析

## 一、　经久不衰之 CVE-2012-0158

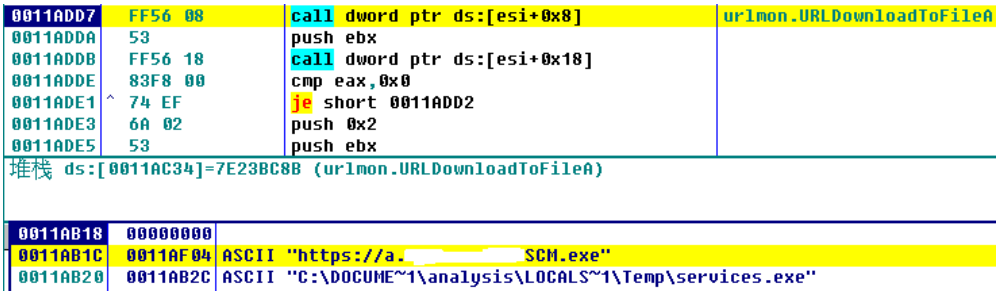
CVE-2012-0158 漏洞是一个栈溢出漏洞，该漏洞是由于微软 Office 办公软件在处理 MSCOMCTL 的 ListView 控件时检查失误造成的，攻击者可以通过精心构造的数据控制程序 EIP 实现任意代码执行。

CVE-2012-0158 虽说 2012 年的漏洞，但其稳定性非常高，其加载恶意代码方式可以为远程下载，也可以附带在文档中释放执行，在一些进行了网络隔离的内网环境中因为系统升级慢，其攻击效果往往比新漏洞效果更好，因此该漏洞很受攻击者青睐，被利用的比例一直很高，从第一章统计的被利用漏洞占比的情况也可以看出该漏洞经久不衰，其占比达到了 17.5%。

下面是一封附带 CVE-2012-0158 漏洞文档的邮件，其中附带的文件名为 Mariette Clermont IMM 2017.doc，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正常的公司资料，从而打开附件中招。我们通过分析该文档，发现文档中嵌入了恶意载荷，通过 CVE-2012-0158 漏洞触发。




调试该载荷，发现该漏洞触发后会连接远端地址，下载恶意程序，存放在临时目录。




通过分析下载文件，知道该文件为 VB 程序，运行后常见挂起的自身程序，注入恶意 PE，该 PE 会利用开源程序 CMemoryExecute、WebBrowserPass、mailpv 盗取用户信息，如浏览器、邮箱、ftp 等帐号密码。

在该实例中发现加载恶意代码的方式是通过远端下载恶意程序，这种方式在漏洞文档中

利用非常普遍，通过第一章统计的漏洞文档载荷类型上看，运用该方式占到了 68.5%。这种方式的好处是下载程序可以由作者自由更换，云控下载方式在漏洞文档中非常广泛。

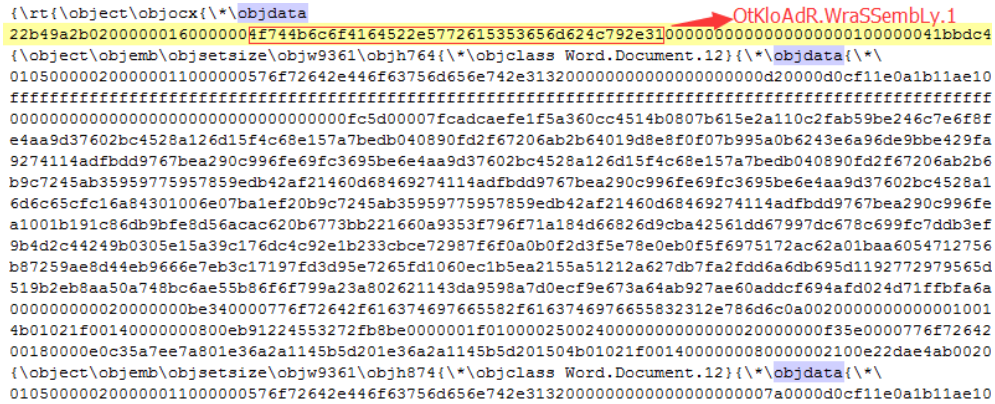
另外，需要说明是通过漏洞文档来盗取用户信息越来越普遍，并且有上涨的趋势，这间接说明了用户数据泄漏现象越来越严重。在此也提醒广大用户注意自身数据的保护，加强安全意识，对于未知邮件需要谨慎处理。

## 二、 稳如泰山之 CVE-2015-1641

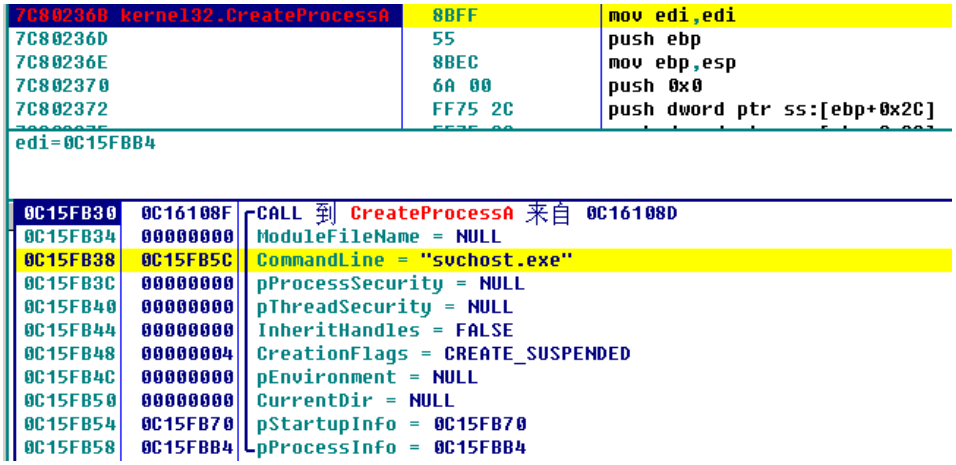
CVE-2015-1641 漏洞为类型混淆漏洞，word 在解析 docx 文档处理 displacedByCustomXML 属性时未对 customXML 对象进行验证，可以传入其他标签对象进行处理，造成类型混淆，导致任意内存写入，最终经过精心构造的标签以及对应的属性值可以造成远程任意代码执行。

该漏洞影响非常广泛，覆盖 Office 2007 SP3，Office 2010 SP2（32 位和 64 位），Office 2013 SP1（32 位和 64 位），Office 2013RT SP1，Word for Mac 2011 以及 Office 在 SharePoint 服务器上的 Office 2010/2013 和 Office Web 2010/2013 等应用，并且 CVE-2015-1641 这个漏洞触发非常稳定，因此很受攻击者喜爱，在 2017 年上半年被利用的漏洞统计中占比达到 11.1%，并且从第一章的被利用的漏洞变化趋势图也可以看出，该漏洞每月出现的次数趋于稳定。

例如下面是一个利用 CVE-2015-1641 漏洞的 RTF 文档，该 RTF 文档内嵌 3 个 OLE 对象，第一个是加载 ActiveX/COM objects otkloadr.WRAssembly.1，通过这个调用 MSVCR71.DLL，MSVCR71.DLL 在编译时不加/DYNAMICBASE 选项，这样库内容的加载地址不变，用于绕过 ASLR 防护。其余两个分别是嵌入的 DOCX 文档，第一个 DOCX 通过 Heap Spray 定位 shellcode 并 ROP 过 DEP 防护(office2007 中并未使用 ROP 过 DEP)，第二个 DOCX 则是触发漏洞的模块，通过漏洞覆盖 MSVCR71.DLL 中的全局函数地址指针跳转到 shellcode 中执行。




通过调试该文档发现，加载恶意代码的方式不是直接的下载文件，而是通过将 shellcode 注入到 svchost.exe 系统进程中，从而执行恶意操作。

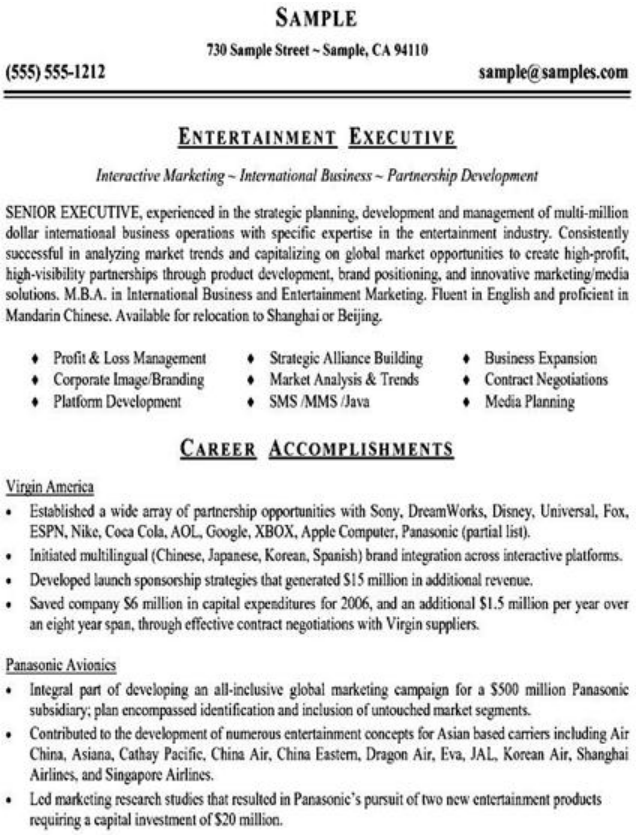



在所统计的文档型漏洞文档中，发现有相当部分漏洞文档都是通过自身载荷注入到系统进程，然后执行恶意功能，或直接在内存中加载恶意程序，不会存放在用户电脑中。因此，在今后很长一段时间内可能都会存在这种基于内存攻击的方式，而不是简单的下载文件并运行。

## 三、 不拘小节之 CVE-2015-2545

CVE-2015-2545 是 Microsoft Office 在处理 EPS 文件时存在内存破坏，攻击者可利用此漏洞构造恶意 Office 文件，允许恶意 Office 中的特殊的 Encapsulated PostScript (EPS)图形文件任意执行代码。

该漏洞影响 Microsoft Office 2007 SP3、Microsoft Office 2010 SP2、Microsoft Office 2013 SP1、Microsoft Office 2013 RT SP1、Microsoft Office for Mac 2011、Microsoft Office for Mac 2016 和 Microsoft Office Compatibility Pack SP3，并且该漏洞有相对应的模版文档，我们发现攻击者在利用 CVE-2015-2545 漏洞时大部分都是基于该模版配置生成。漏洞模版界面如下。



SAMPLE

730 Sample Street ~ Sample, CA 94110

(555) 555-1212 sample@samples.com

ENTERTAINMENT EXECUTIVE

*Interactive Marketing ~ International Business ~ Partnership Development*

SENIOR EXECUTIVE, experienced in the strategic planning, development and management of multi-million dollar international business operations with specific expertise in the entertainment industry. Consistently successful in analyzing market trends and capitalizing on global market opportunities to create high-profit, high-visibility partnerships through product development, brand positioning, and innovative marketing/media solutions. M.B.A. in International Business and Entertainment Marketing. Fluent in English and proficient in Mandarin Chinese. Available for relocation to Shanghai or Beijing.

- Profit & Loss Management
- Corporate Image/Branding
- Platform Development
- Strategic Alliance Building
- Market Analysis & Trends
- SMS /MMS /Java
- Business Expansion
- Contract Negotiations
- Media Planning

CAREER ACCOMPLISHMENTS

Virgin America

- Established a wide array of partnership opportunities with Sony, DreamWorks, Disney, Universal, Fox, ESPN, Nike, Coca Cola, AOL, Google, XBOX, Apple Computer, Panasonic (partial list).
- Initiated multilingual (Chinese, Japanese, Korean, Spanish) brand integration across interactive platforms.
- Developed launch sponsorship strategies that generated $15 million in additional revenue.
- Saved company $6 million in capital expenditures for 2006, and an additional $1.5 million per year over an eight year span, through effective contract negotiations with Virgin suppliers.

Panasonic Avionics

- Integral part of developing an all-inclusive global marketing campaign for a $500 million Panasonic subsidiary; plan encompassed identification and inclusion of untouched market segments.
- Contributed to the development of numerous entertainment concepts for Asian based carriers including Air China, Asiana, Cathay Pacific, China Air, China Eastern, Dragon Air, Eva, JAL, Korean Air, Shanghai Airlines, and Singapore Airlines.
- Led marketing research studies that resulted in Panasonic's pursuit of two new entertainment products requiring a capital investment of $20 million.

打开漏洞文档，首先弹出上图所示的模版内容，接着会加载嵌入的 EPS 文件，该文件是个 PostScript 脚本。PostScript 脚本在处理 forall 指令时，存在 Use-After-Free。通过精心构造 PostScript 脚本能导致任意内存写入，最终造成远程任意代码执行。下图是 PostScript 脚本文件中的触发漏洞的 forall 语句。

```
xx_41
{
    xx_6334 1 eq
    {
        /xx_26500 exch def /xx_19169 exch def exit
    } if
    pop //key
    pop //value
    44 string pop 44 string pop 44 string pop 44 string pop 44 string pop 44 string pop 44 string pop
    44 string pop 44 string pop 44 string pop 44 string pop 44 string pop 44 string pop 44 string pop
    3 3 3 3 3 3
    xx_18467 xx_41 copy
    pop array pop array pop array pop array pop array pop array
    1 1280 put
    35 string pop 35 string pop
    35 string
    0 <00000000
       ff030000
       03000000
       00000000
       00000000
       44444444
       00050000
       00000000
       000000> putinterval
    /xx_6334 xx_6334 1 add def
} forall
```

利用该模版的样本首先会释放 plugin.dll 并加载执行，plugin.dll 运行后又会释放 igfxe.exe 并执行，igfxe.exe 主要功能是下载其他的恶意程序并执行。利用该模版的样本只有 igfxe.exe 中的下载地址不同，其它流程一致。同时还发现利用该漏洞模版进行下载的恶意程序大部分都为远控木马，如 NanoCore，LuminosityLink RAT 等。

此外，需要引起重视的是，在 Office 2010 及以上的 Office 版本中，微软采取了在沙盒中解析 EPS 文件的方式来缓解 EPS 文件解析过程中出现的漏洞，但在今年上半年陆续出现

的高危 EPS 漏洞(如 CVE-2017-0261、CVE-2017-0262)中，攻击者利用这些漏洞结合其他 Windows 提权漏洞（如 CVE-2017-0001、CVE-2017-0263）来绕过 Office 文档的沙盒保护，从而实现攻击目的。可以预测，这种通过利用多个漏洞的相互配合来完成一次高级攻击的技巧或许将会成为一种趋势。

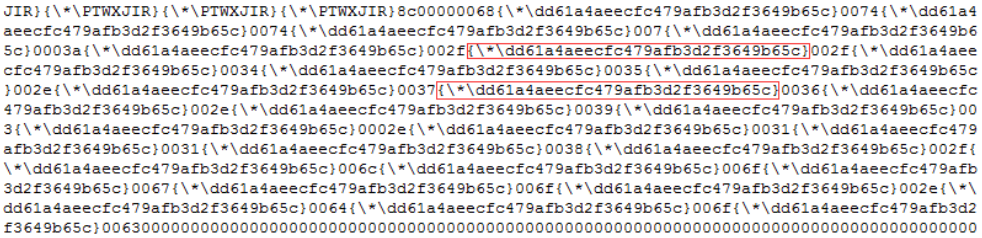
## 四、 后起之秀之 CVE-2017-0199

CVE-2017-0199 是 Microsoft Office 的 OLE 处理机制实现上存在的一个逻辑漏洞，Microsoft Office 在处理内嵌 OLE2LINK 对象时，通过网络更新对象时未正确处理 Content-Type 所形成的一个漏洞。攻击者可利用此漏洞构造恶意 Office 文件，当用户打开特殊构造的恶意 Office 文件后攻击者可以在用户系统上执行任意命令，从而控制用户系统。

该漏洞影响非常广泛，覆盖 Microsoft Office 所有版本，且构造恶意文档相对其它漏洞更加简单，因此当该漏洞在上半年三月份被披露时大量爆发，在四月份集中爆发，一度掩盖经典漏洞 CVE-2012-0158 的光辉，成为攻击者的宠儿，同时它的载荷也非常广泛，从常用的信息盗取木马、远控木马和下载者，再到最近敏感的敲诈者都有涉及。由于敲诈者相对其它病毒木马能够直接获取利益，越来越多的攻击者开始使用敲诈者牟利，今年 5 月 12 日爆发了“WanaCrypt0r”（永恒之蓝）勒索病毒和 6 月 27 日爆发的 Petya 勒索病毒，这说明了敲诈者病毒越来越流行，攻击者也乐于使用它们进行牟利。

下图是利用 CVE-2017-0199 的漏洞文档下载敲诈者病毒运行后的界面，该敲诈者会加密用户计算机上的重要文件，并提醒用户支付赎金购买解密软件，但未必用户支付了赎金就能找回重要文件。


且在最近的研究中我们还发现，利用该漏洞的恶意 Office 文档已经开始混淆更新的 URL，如下。



另外，由于该漏洞利用简单且覆盖 Microsoft Office 所有版本，在以后很可能会成为像 CVE-2012-0158 一样的经典存在而经久不衰。避免这种漏洞文档最直接的方法是及时更新补丁。每当有新的漏洞被披露时，由于很多用户未及时更新补丁，导致自己中招。

# 第四章　结尾

综上所述，越来越多的攻击者更加倾向于利用漏洞文档来进行恶意行为，相比传统的恶意程序更具有迷惑性。若攻击者通过鱼叉或水坑攻击方式，并结合社会工程学手段，精心构造文档名及伪装内容，很多安全意识薄弱的用户很容易中招。

在此，360 互联网安全中心提醒广大用户，陌生人发来的陌生文档不要轻易打开，很可能该文档携带恶意载荷，从而导致自己蒙受损失。同时也建议广大用户一定要在电脑中安装安全软件，并及时更新漏洞补丁，减少漏洞文档触发的可能性。

最后，提醒用户，除了本文研究的漏洞文档外，一些不是利用漏洞进行的恶意文档文件所带来的危害也不容忽略，例如：

一、恶意宏攻击的文档，针对该类文档的防护，建议广大用户不要将 Office 宏安全设置为默认允许所有宏代码执行，对于未知的宏不要轻易运行；

二、嵌入恶意链接的文档，针对这类文档不要轻易点击未知链接，除非确认来源正常，以免遭受损失；

三、嵌入恶意 PowerShell 代码的文档，这种文档一般为 PowerPoint 文档，文档中注册了鼠标悬停回调函数，并在函数中调用恶意的 PowerShell 代码，如“Zusy”文档，这种文档 Office 会提示用户选择是否需要执行该 PowerShell 代码，但大多数用户并不知道这代表什么，如果选择了执行，则恶意的 PowerShell 代码将从远端下载其他恶意程序，从而控制用户电脑。因此，提醒广大用户，请大家养成良好的计算机使用习惯，对于 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。