Spam Campaign Targets Colombian Entities with Custom-made 'Proyecto RAT,' Uses Email Service YOPmail for C&C

- Posted on:July 18, 2019 at 5:01 am
- Posted in:Malware, Spam, Targeted Attacks
- Author:
  Trend Micro

0

by Jaromir Horejsi and Daniel Lunghi (Threat Researchers)

We observed a recent campaign that primarily targets financial institutions and governmental organizations in the South American region, particularly in Colombia. This blog post covers the activities we observed, the remote access tools (RATs) used, the campaign's techniques and procedures, and its indicators of compromise (IoCs). Our findings indicate that the campaign appears to be the work of a group involved in business email compromise (BEC) or cybercrime, and unlikely to be an advanced persistent threat (APT).

It's worth noting that the group uses YOPmail, a disposable email address service, for its command and control server (C&C). The payload, written in Visual Basic 6, is a customized version of a remote access tool called "Proyecto RAT." Our in-depth analysis of the malware is detailed in this **appendix**.

The delivery emails

The infection starts with an email sent to a target, as seen in the screenshot below (Figure 1). In multiple instances, we noticed the attacker used open or compromised mail servers in South America to facilitate the campaigns. The attacker also connected to the compromised servers from IP addresses that were linked to dynamic domain names used as C&Cs by the delivered payloads. This suggests that the attacker uses the same infrastructure to send emails and control victims.

The sender of the email is usually spoofed, and we saw multiple email subjects enticing the receiver to open the attachment, which is an RTF file. Examples of such subjects are:

- "Hemos iniciado un proceso en su contra por violencia laboral." (Loosely translates to "We have filed a lawsuit against you for workplace violence.")

- "Se hara efectivo un embargo a su(s) cuenta(s) Bancarias." (Loosely translates to "Your banking accounts are going to be blocked.")
- "Almacenes exito te obsequia una tarjeta regalo virtual por valor de $500.000." (Loosely translates to "Exito shops offer you a virtual gift worth $500.000.")

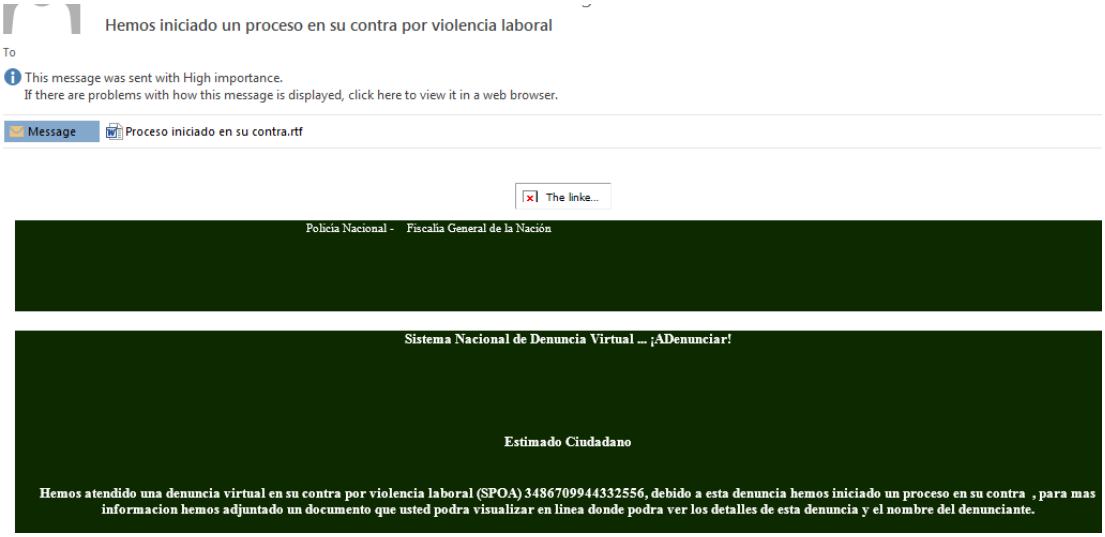

Figure 1. Delivery email

The attached RTF file contains one line of text and a link. The text relates to the email subject, such as "You can see the complaint against you below." or "See the complaint online." Note that the link to the malware uses the URL shortener cort.as, which belongs to the El País newspaper. Unfortunately, this service only enables statistics on demand, and the attacker never enabled them.

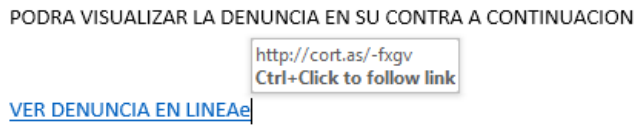

Figure 2. RTF document attached to the delivery email

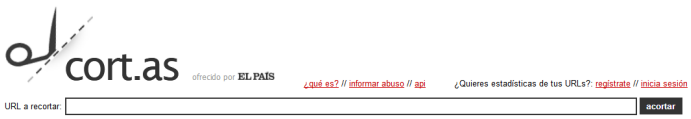

Figure 3. URL shortener cort.as

Clicking on the link redirects the victim to a file on a file-sharing service. The file is a delivery document that contains macros.

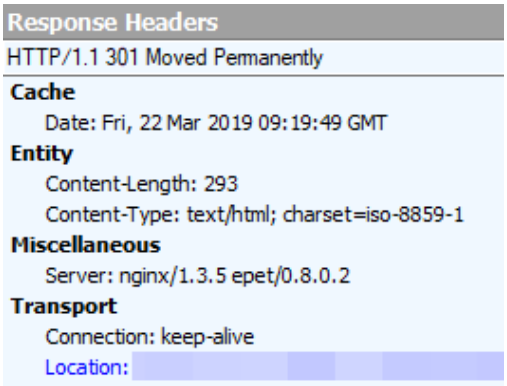

Figure 4. Shortened URL redirects to a file hosted on a cloud file-sharing service

The delivery documents

The majority of the documents we analyzed were in MHTML format, which contains macros. The macro code is a simple downloader for the payload. However, Office files in OLE format were also observed. Most of the document designs have already been published in Qihoo360's blog post; this post will discuss designs that the post did not cover. The documents, which appeared between 2017 and 2019, all asked users to enable macros. The macros will download and execute a RAT.

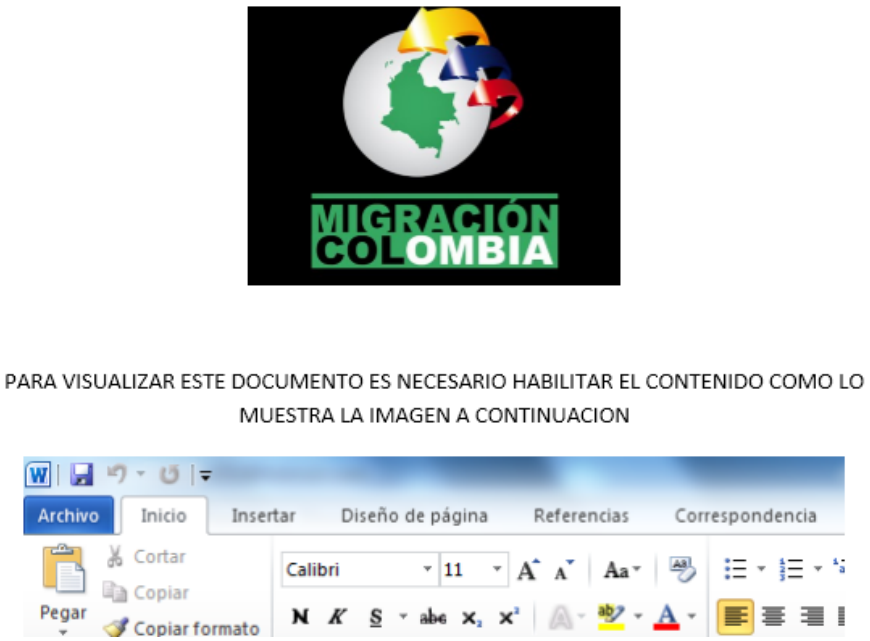

Figure 5. Delivery document purports to come from Migración Colombia, a government website for the Colombian migration authority

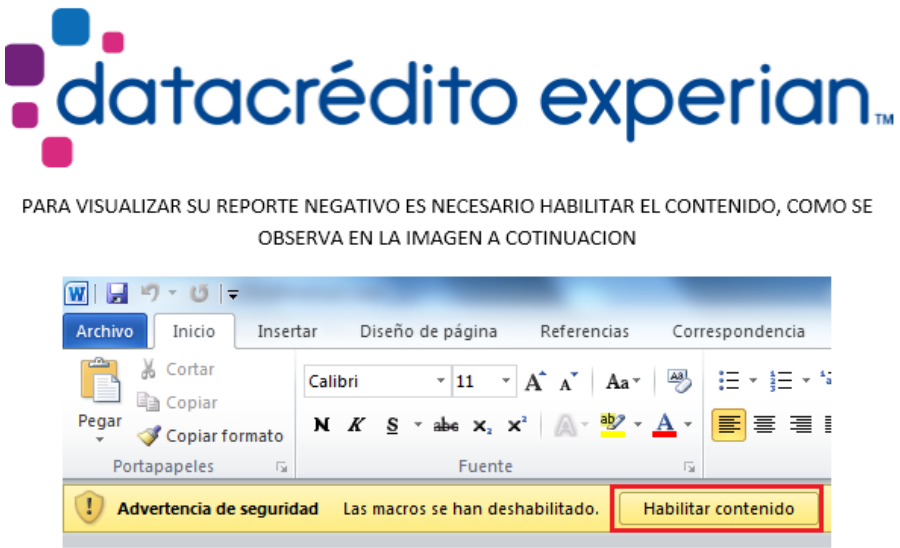

Figure 6. Delivery document purports to come from DataCrédito, a service that allows access to credit history and profile

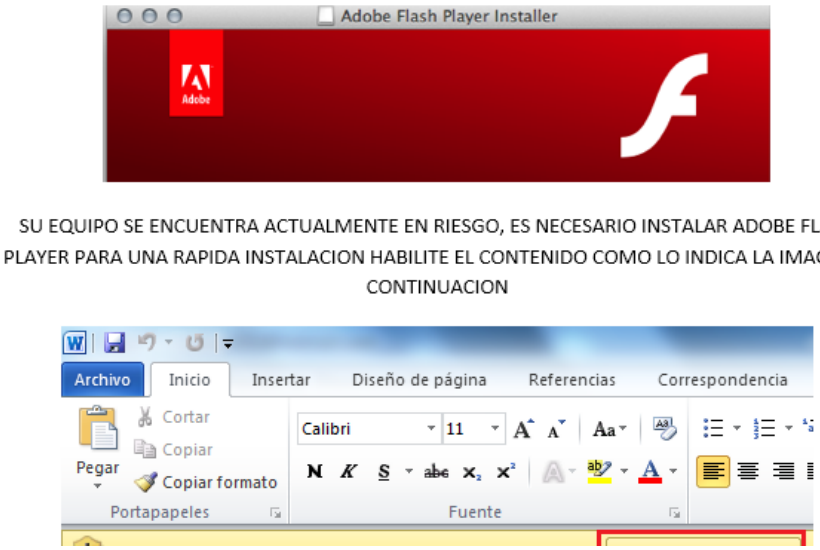

Figure 7. Delivery document with a generic Adobe Flash Player Installer

First stage payload: Remote Access Tool (RAT)

The main payload is usually Imminent Monitor RAT; however, at the beginning of 2018, we also observed the use of LuminosityLink RAT, NetWire RAT, and NjRAT. In a case in June 2019, we also noticed Warzone RAT being used. Warzone RAT is the newer RAT from the list and supports keylogger, web browser-, and Outlook password-stealing features in addition to standard RAT functions.

All of these RATs are standard malware that can be bought for under US$100 or downloaded from various malware repositories.

After the download of Imminent Monitor RAT and observing its network behavior, we noticed an instruction to download and execute another executable file, which is the second stage payload.

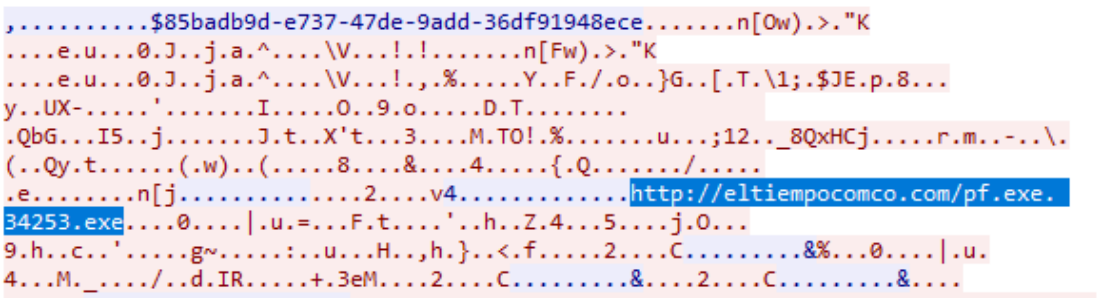

Figure 8. Imminent Monitor RAT traffic

Second stage payload: Proyecto RAT

The second stage payload is written in Visual Basic 6, and has an interesting feature — a C&C URL address acquired from the disposable email service YOPmail. The malware connects to a mailbox, reads the only available email message, parses it, and then extracts the subject of the email. The C&C server URL is between the '¡' characters (upside-down exclamation sign), a character used in the Spanish language. This is the first time we noticed disposable email services being abused this way.

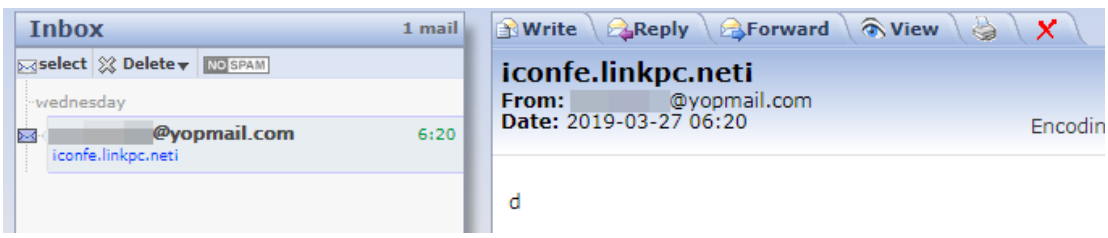

Figure 9. A disposable email with C&C address and email subject

During our analysis, we found three mailboxes related to the malware. We have since reached out to YOPmail and informed them of this threat. YOPmail has responded, saying that they would place specific restrictions.

A detailed technical analysis of the classes, forms, and modules revealed when the malware is decompiled can be found in this **appendix**.

Searching for the malware family

Seeing the many features of the malware, we tried to match it to a known RAT.

The communication between client and server is via TCP, is unencrypted, and uses pipe "|" characters and "¡@#@!" as a separator. This description fits quite well with Xpert RAT. Searching for the x86 hex string from cTimer class also leads to links with Xpert RAT. This tweet from a malware researcher even mentions Xpert RAT.

An online search found two versions of Xpert RAT were found: "XpertRAT v3.0.10 By Abronsius" and "XpertRAT v3.0.9 By Abronsius". After building the payload and infecting the test machine, we could observe the communication in figure 10. Notice the different colors between the incoming and outgoing communication and the separator between both communication streams. However, in Xpert RAT builder, we did not notice any reference to a disposable email, searches for banking website captions, or information written to the configuration file. In addition, Xpert RAT samples generated by the builder have even more functions such as keylogger, runPE, WebCam, Audio, Wipe module, and Remote Desktop.

```
6|C:\|2|1
7|D:\|5|1
8|Favorites|12|1
9|Recent|13|1
10|Windows|14|1
11|System32|14|1
12|Program Files|14|1
.@#@!0|1|5.@#@!1|13|C:\Users
modified: ?3/?26/?2019 ??1:0
```

Figure 10. Original Xpert RAT communication snippet

It seems that the aforementioned Visual Basic malware is an old and limited version of the Xpert RAT — either a custom modification of Xpert RAT or a malware with source code based on Xpert RAT's.

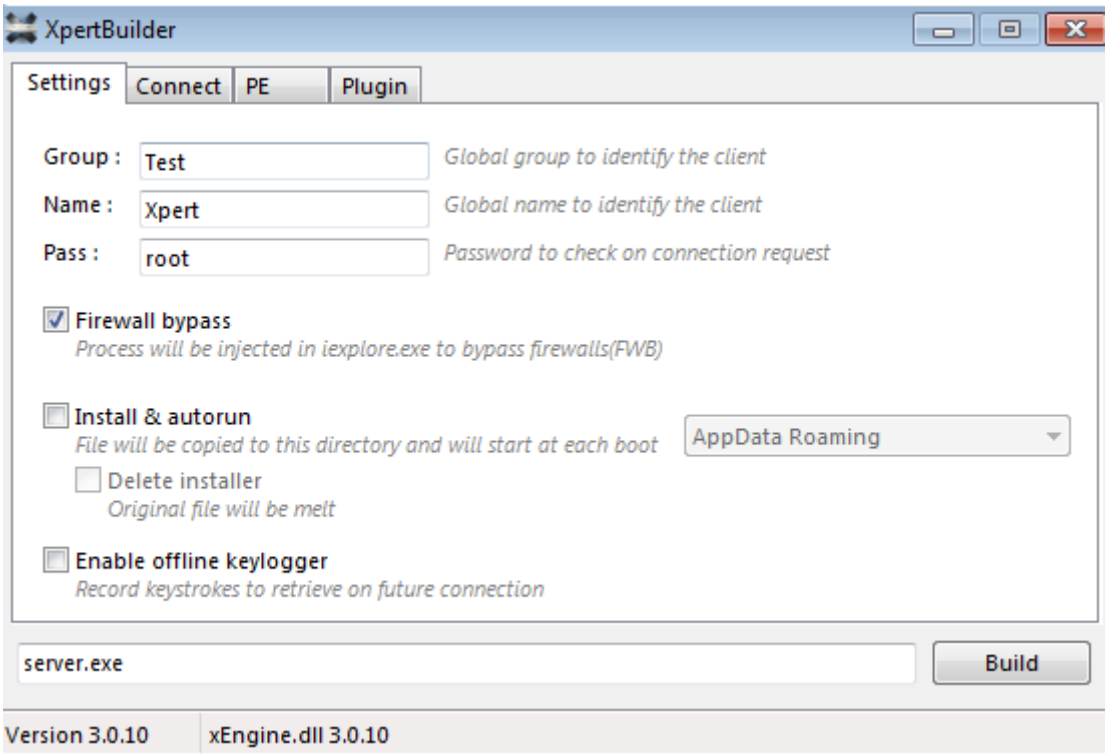

Figure 11. Xpert RAT builder

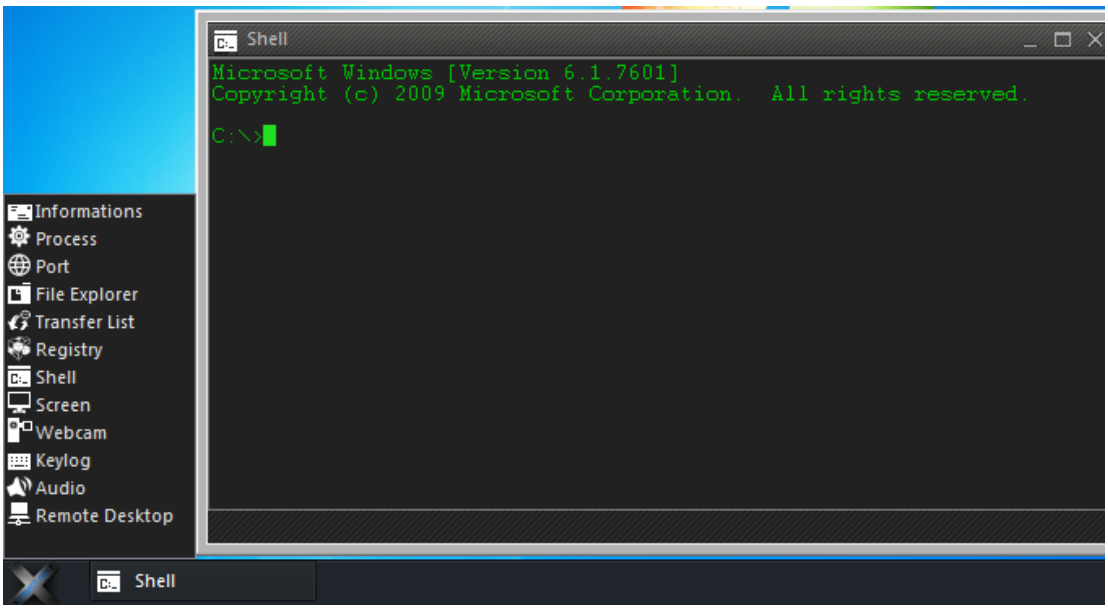

Figure 12. Functions available to an Xpert RAT operator

When searching for class names from the Visual Basic malware, the keyword "ClsRemoteRegistry" leads to a discussion on a Spanish hacking forum (Figure 13). The user, who in his profile offers Prodigy Bot, an IRC bot written in VB6, has a question related to the code from Leandro Ascierto's project called "Proyecto RAT."

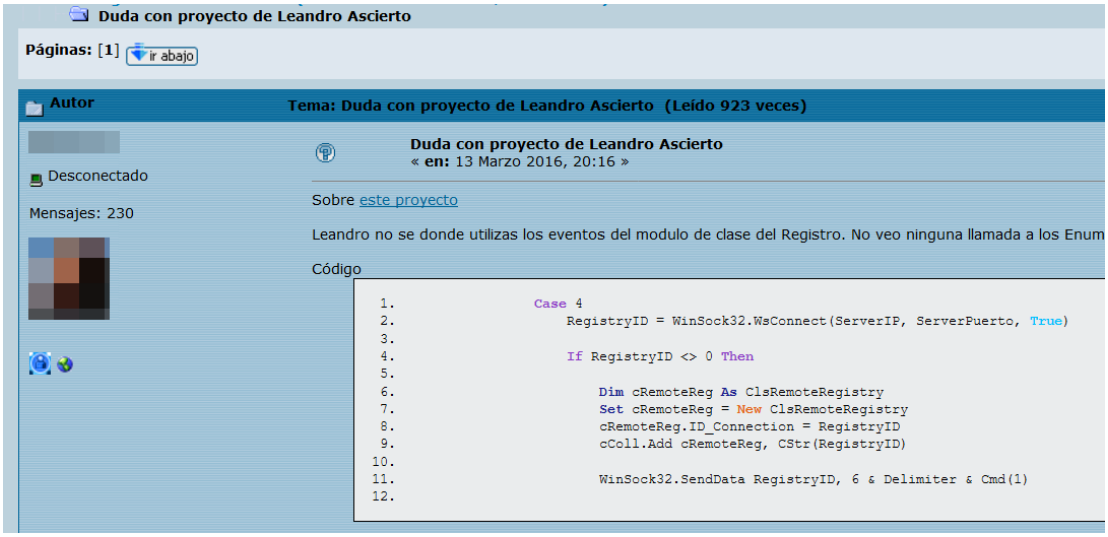

Figure 13. Discussion about ClsRemoteRegisty class on a hacking forum

After downloading and examining the project, we noticed familiar class names, delimiters, strings, and more.

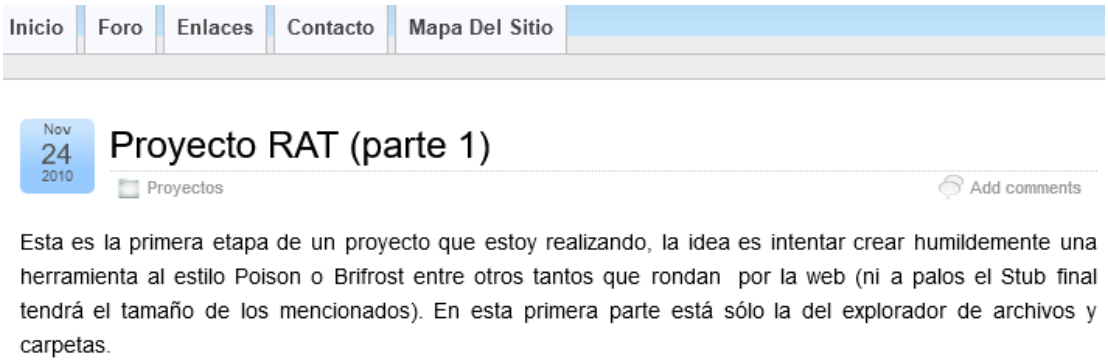

Figure 14. Proyecto RAT website

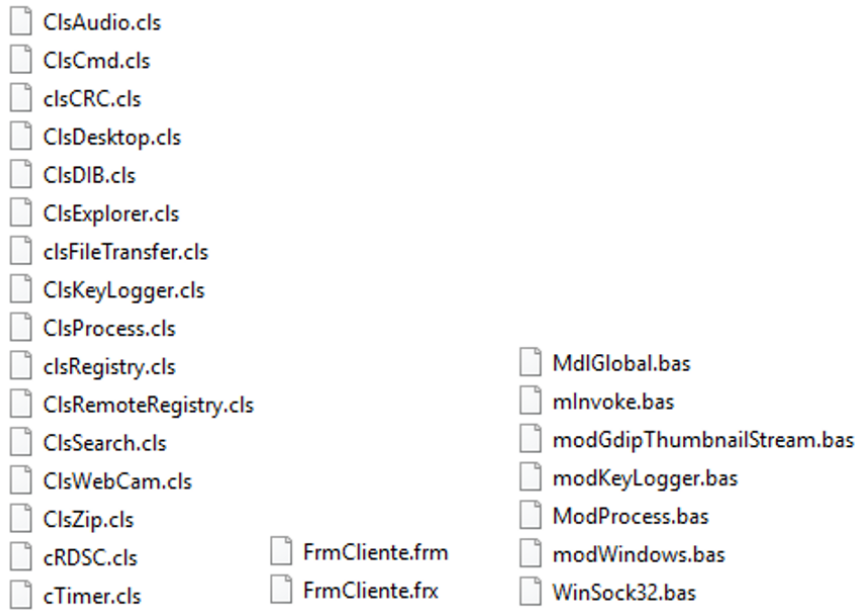

Figure 15. Familiar class, form, and module names

```
Private Const Delimiter As String = "|"
Private Const Delim2 As String = "#%."
Private Const Delim3 As String = "@&|?"
Private Const END_DATA As String = "¡@#@!"
```

Figure 16. Several delimiters used by Proyecto RAT, file ClsRemoteRegistry.cls

```
Private Const asmMain As String = "558BEC50FF7514FF7510FF750CFF75086855555555B866666666FFD0C9C21000"
'                                                                |<pCls>|  |<Proc>|
Private ASM() As Byte          ' Array für AsseblerCode
```

Figure 17. Hex code from cTimer class, with original comments in German, because this code was taken from a different project

Based on these details, we believe this is a customized version of Proyecto RAT.

Affected regions and verticals

Colombia is by far the most targeted country, with other South American countries added to the list. This is consistent with the fact that this actor uses the Spanish language in all the spear phishing documents we observed. However, we also noticed targets in other countries:

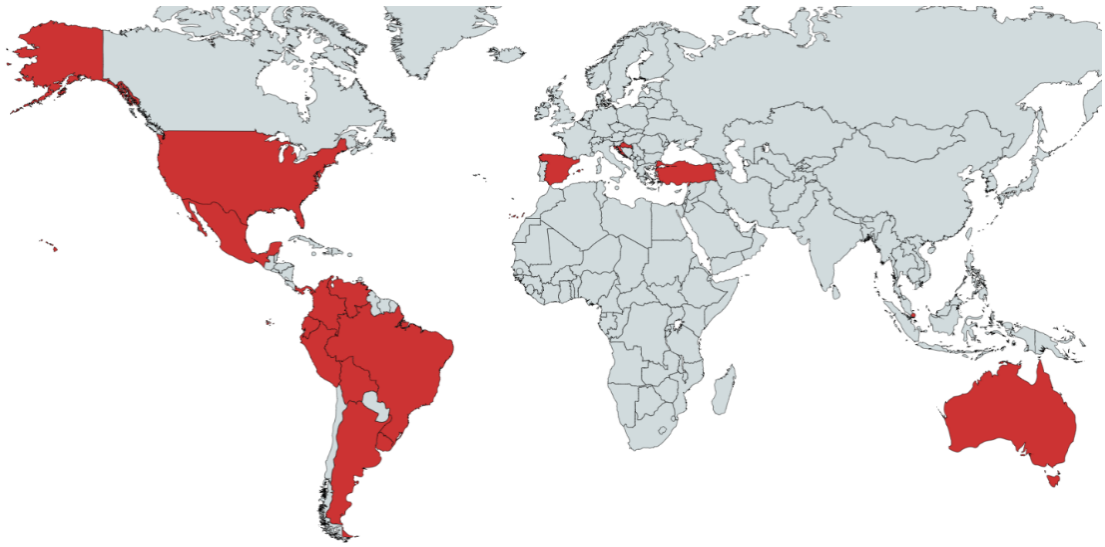

Figure 18. The regions targeted by the spear-phishing documents

In one instance, the attacker used the URL shortener bit.ly, which confirmed that Colombia is the main target. As anyone can follow the link, some of these countries could also be the result of researchers' sandboxes.

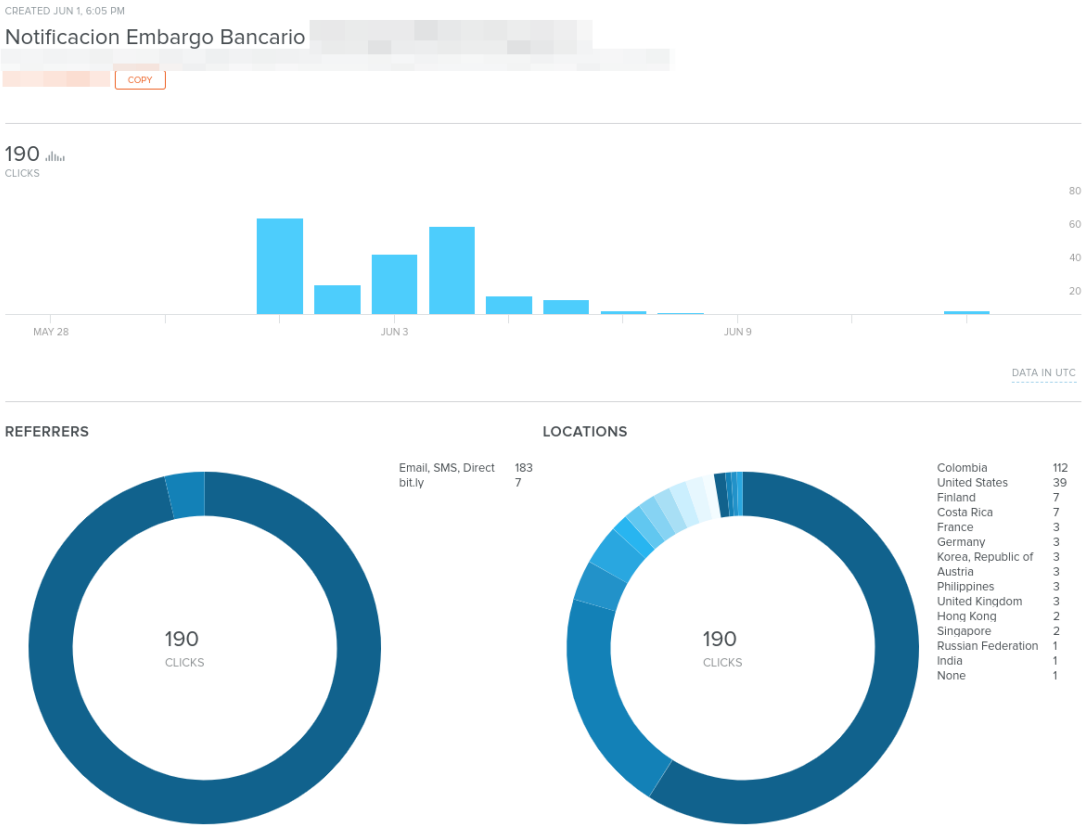

Figure 19. Clicks and locations related to the bit.ly link

Recent campaigns targeted different industries. The most prevalent were government entities, healthcare/pharmaceutical institutions, followed by financial/banking/insurance and agro-industry/food/packaging organizations.

Notably, we noticed that multiple employee savings funds (called "Fondo de empleados" in Colombia) were targeted. These entities barely have access to sensitive information, but they are likely to possess a reasonable amount of money.

Conclusion and mitigation

Xpert RAT reportedly first appeared in 2011. The first version of "Proyecto RAT" was published at the end of 2010. Both projects share similarities, and it is likely that "Proyecto RAT" was inspiration for Xpert RAT and at least a few more malware projects, including the Visual Basic malware in the campaign we previously described.

We can't say for sure what this actor is particularly looking for, but multiple facts lead us to believe it is designed for BEC or cybercrime rather than as an APT:

- These campaigns are noisier and more prevalent than usual APT campaigns.
- The same IP address, which is dynamic, is used to send spear-phishing emails and act as C&C. This is more common to cybercrime.
- Some of the targeted industries might not have access to sensitive information, but are likely to handle a decent amount of money.
- The windows titles that are listed in the configuration file are almost all related to financial services.

Our research shows that this campaign can deliver malware with multiple capabilities that can affect different organizations and industries. It also highlights the importance of securing online infrastructures, particularly the email gateways, to avoid targeted spam campaigns. Organizations should adopt best practices on messaging-related threats and regularly update systems to prevent attackers from taking advantage of any security gaps. Employing additional security mechanisms such as enabling firewalls and intrusion detection and prevention systems will help prevent suspicious network activities that may lead to data exfiltration or C&C communication.

Organizations can also turn to Trend Micro™ endpoint solutions such as Trend Micro Smart Protection Suites and Worry-Free™ Business Security. Both solutions can protect users and businesses from threats by detecting malicious files and spammed messages as well as blocking all related malicious URLs. Trend Micro Deep Discovery™ has an email inspection layer that can protect enterprises by detecting malicious attachments and URLs.

Trend Micro™ Hosted Email Security is a no-maintenance cloud solution that delivers continuously updated protection to stop spam, malware, spear phishing, ransomware, and advanced targeted attacks before they reach the network. It protects Microsoft Exchange, Microsoft Office 365, Google Apps, and other hosted and on-premises email solutions.

Our technical analysis of the malware, IoCs, and other spam email samples related to the campaign can be found in this **appendix**.