APT-C-36 Updates Its Long-term Spam Campaign Against South American Entities With Commodity RATs

trendmicro.com/en_ph/research/21/i/apt-c-36-updates-its-long-term-spam-campaign-against-south-ameri.html

September 13, 2021

APT & Targeted Attacks

APT-C-36 Updates Its Spam Campaign Against South American Entities With Commodity RATs

We have continued tracking APT-C-36, also known as Blind Eagle, since our research on this threat actor in 2019. We share new findings of APT-C-36's ongoing spam campaign targeting South American entities.

By: Jaromir Horejsi, Daniel Lunghi September 13, 2021 Read time: (words)

In 2019, we wrote a blog entry about a threat actor, likely based in Colombia, targeting entities in Colombia and other South American countries with spam emails. This threat actor is sometimes referred to as APT-C-36 or Blind Eagle. Since then, we have continued tracking this threat actor. In this blog entry, we share our new findings about APT-C-36's ongoing spam campaign during that monitoring phase.

APT-C-36 has been known to send phishing emails to various entities in South America using publicly available remote access tools (RATs). Over time, the threat actor switches from one RAT to another. In the past, we have observed that APT-C-36 makes use of RATs such as:

- njRAT
- Imminent Monitor
- A custom modified ProyectoRAT
- Warzone RAT
- Async RAT
- Lime RAT
- Remcos RAT
- BitRAT

The delivery emails

APT-C-36 utilizes different ruses for their targets: Many of the fraudulent emails impersonate Colombia's national directorate of taxes and customs, *Dirección de Impuestos y Aduanas Nacionales* (DIAN), a lure that the threat actor has used before. Such emails claim that a

“seizure order to bank account has been issued,” further details are contained in the email attachment, and that the information is protected with password “dian” (Figure 1). In English, the attachment means “seizure order.pdf” and the email body translates to the following:

> *“Subject: we have sent a seizure order to the bank accounts matching your name*
>
> *Dear taxpayer,*
>
> *For your information, our intelligent IT system detected that your income statement at the Direccion de Impuestos y Aduanas DIAN has 180 days of arrears. For that reason, we will proceed as stated in the law, article 823 until 843-2.*
>
> *We attach the information and your debt with the password : dian"*

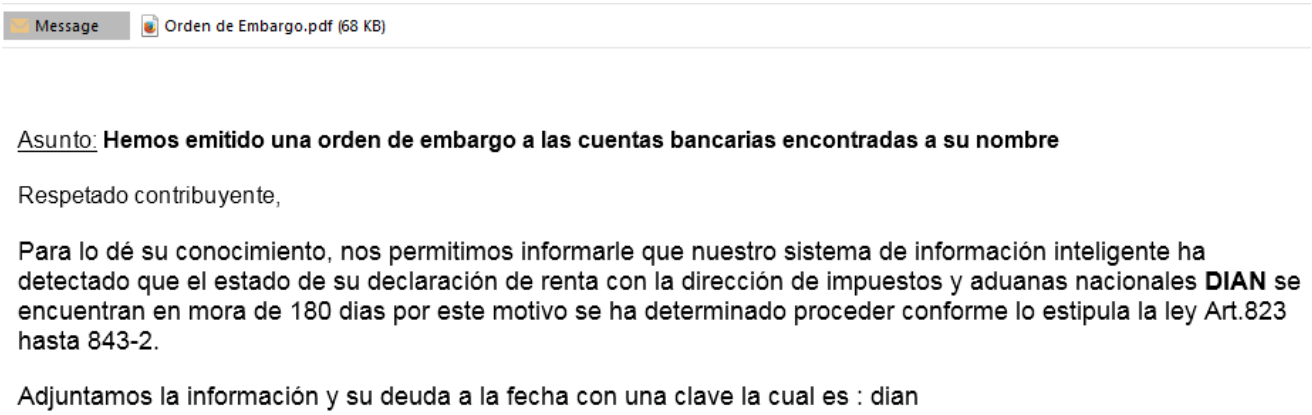

Figure 1. A delivery email impersonating Colombia’s national directorate of taxes and customs

Other fake emails in this campaign claim to contain a photo that would prove that the recipient’s partner is having an affair. In a similar fashion, the recipient is asked to open the email attachment named “attached picture.jpg” and use the password “foto” to view its contents (Figure 2). These emails lack proper punctuation and are badly written, which is a common feature in phishing attempts. In English, the email translates to the following:

> *“Hi how are you, I hope you're fine. I write this email to you as I don't dare telling you directly. Everyone knows except you, open your eyes, you are being cheated on and I don't like how others are laughing about you. I experienced a similar situation, that's why I don't like someone doing it to another person. You know me well, I prefer not to make trouble. I attached a picture where they are kissing, I know it's hard to look at, but it is better than to live a relationship where you believe it is all fine.*
>
> *The picture was too big so I compressed it, you need Winzip or Winrar installed. I will write another email in the following says, I have more things to tell you.*
>
> *I uploaded the picture with a password to avoid other people to look at it. The password is: foto".”*

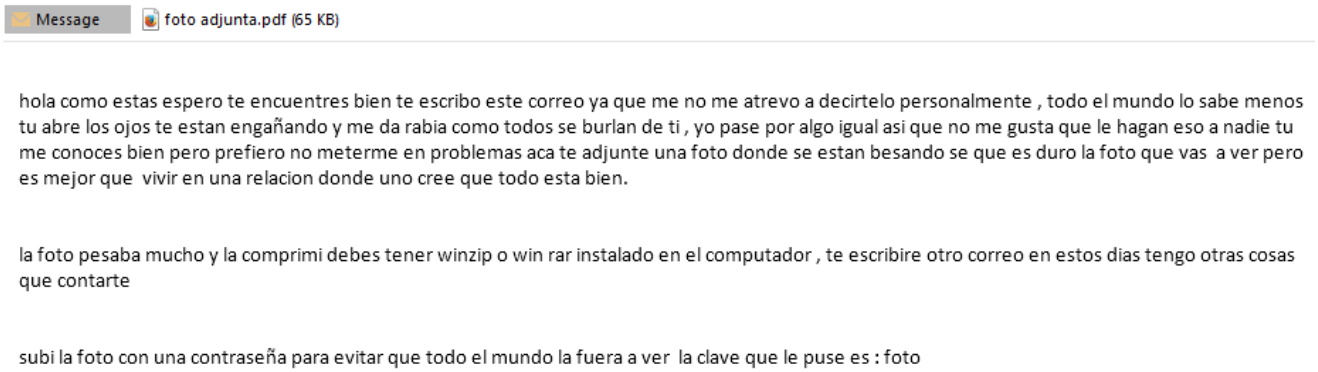

Figure 2. A delivery email pretending to share personal photos

The sender's email address is either a spoofed address impersonating DIAN, or a Hotmail.com address impersonating a fake female profile. The originating IP addresses always belong to a VPN provider.

The delivery documents

The delivery documents in these phishing emails are either a PDF file or DOCX file containing a link. We have found samples of these documents impersonating DIAN (Figure 3), and others impersonating Google Photos (Figure 4).

Figure 3. An email attachment with a link to a URL shortener

Figure 4. The URL leads to a different destination

Hovering over the link will show that the link was generated from a URL shortener. As discussed in our last blog entry on this threat actor, APT-C-36 uses URL shorteners such as cort.as, acortaurl.com and gtly.to. These URL shorteners are capable of geographical targeting, so if a user from a country not targeted by the threat actors clicks on the link, they will be redirected to a legitimate website. The URL shorteners also have the ability to detect the major VPN services, in which case, the shortened link leads the users to a legitimate website instead of redirecting them to the malicious link, as illustrated in Figures 5 and 6.

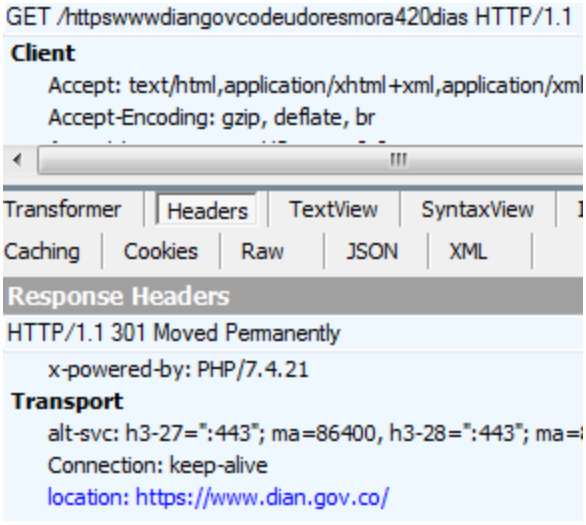

Figure 5. Geographical targeting detects a non-Colombian IP or VPN, so the user is led to the real DIAN website

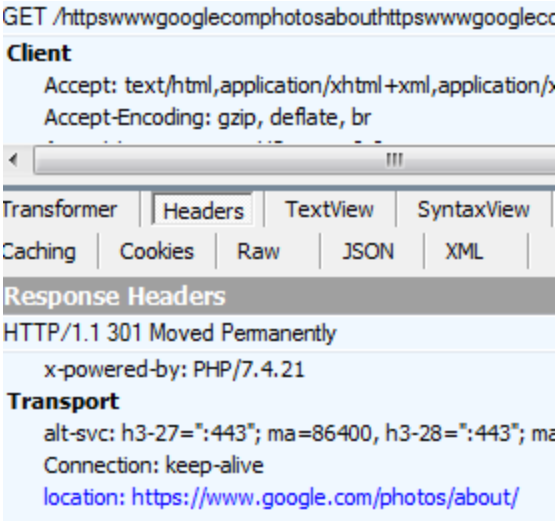

Figure 6. Geographical targeting detects a non-Colombian IP or VPN, so the user is led to the real Google Photos website

However, if the location criteria are met, then the user is redirected to a file hosting server and a file is automatically downloaded (Figure 7).

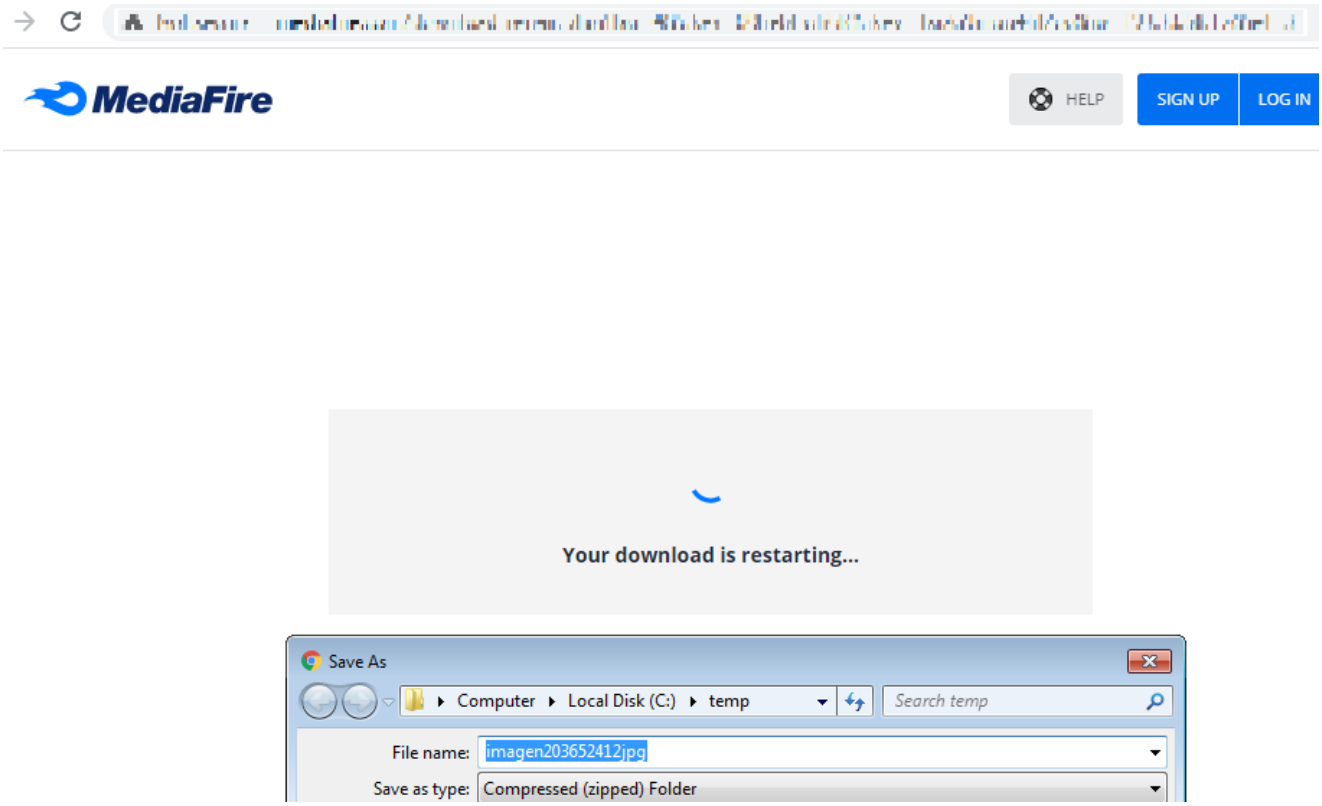

Figure 7. File storage containing a password-protected archive

The downloaded file is a password-protected archive, the password for which is mentioned in the email, the email attachment, or both. These passwords are usually simple, such as “dian,” “foto,” or “1234.”

Payload

After deobfuscating the executable file within the password-protected archive, we are presented with a RAT called BitRAT. This RAT is not new, it has been previously analyzed by security researchers.

Upon analyzing the RAT, the most interesting part of this RAT is its configuration settings seen as an encrypted block of data (Figure 8). There are two hexadecimal strings within the main executable file in BitRAT: the longer string is the encrypted configuration, the shorter one is the first part of the key.

```
0000000000653100009430000072310000000000004578697450726F6365737300005772697
46546696C650047310000000000000000000000230000057310000    495369d5e7c087d052
8c6a1b224d7f5ded87efa815635021ac379945e1931c44253a31c5342a3e29247fedcea9a05
792d9f4e75c8caa9c873b4d6f3574d8713d98a29e48fa867b2e76a16904fc0b1217ea366769
4bf4e50a25e2e38944b41f3c9ee531a8c9922afde080c382b2c8132b821fc3a414f88743a8e
d790338d4b7baa82994a5dd9936874cb195e95d1ef0127a2f537458483742e35c958755bff1
75

                                                  38325a784d6f5630    1.38
 ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/    vector
```

Figure 8. BitRAT's encrypted configuration

Unlike most other malware, BitRAT uses the Camellia cipher with an initialization vector (IV) of 0000000000000000.

Several computational steps are needed to obtain the final key. First, a magic value is computed from bytes found on fixed addresses, as shown in Figures 9 and 10.

```
v58[0] = xmmword_748310;
v58[1] = xmmword_748340;
v59 = 0x3D;
v60 = 0x55;
for ( i = 0; i < 0xA; ++i )
  Str[i] = (37 * (*((_DWORD *)v58 + i) - 8) % 127 + 127) % 127;
```

Figure 9. The algorithm to compute for the magic value of BitRAT's final key

```
00748310  55 00 00 00 3D 00 00 00  34 00 00 00 64 00 00 00  U...=...4...d...
00748320  08 00 00 00 6E 00 00 00  54 00 00 00 64 00 00 00  ....n...T...d...
00748330  09 00 00 00 61 00 00 00  6B 00 00 00 64 00 00 00  ....a...k...d...
00748340  36 00 00 00 4E 00 00 00  6D 00 00 00 64 00 00 00  6...N...m...d...
```

Figure 10. The input data to compute for the magic value of BitRAT's final key

Each byte is transformed using a simple computation formula, as shown below:

> **((((value-0x 08)*0x25) %0x7f)+ 0x7f)% 0x7f**

This formula can be used to compute for the magic value through the following process:

1. For example, using the data from Figures 9 and 10 will result in the string "78hf326f87".
2. This string is appended to the hardcoded string "38325a784d6f5630", forming the string "38325a784d6f563078hf326f87".

3. Afterward, a crc32 checksum is computed from “38325a784d6f563078hf326f87”, resulting in “d8e71d19”.
4. A value of 0x08 is added to the checksum, which then becomes “d8e71d21”.
5. The MD5 hash is computed from the checksum “d8e71d21”, forming “b50d97fb1e3d5fc9cc302384f5718714”.
6. The first half of this MD5 hash, “b50d97fb1e3d5fc9”, is the key for the Camellia cipher.

The configuration is decrypted to the following string, as shown in Figure 11, including a command-and-control (C&C) server and a port.

```
jairoandresotalvarorend.linkpc.net|9086|0|2a44e1dec299239a|windowsdefenderinitser
vices|windowsdefenderinitservice.exe|bfdba24ee3d61f0260c4dc1034c3ee43|tor|
```

Figure 11. Decrypted configuration of BitRAT

Affected regions and industries

The majority of the targets we discovered were located in Colombia, although some were from other South American countries such as Ecuador, Spain, and Panama. This is consistent with the use of Spanish in spear-phishing emails.

Although APT-C-36’s objective remains unclear, we posit that the threat actor carried out this campaign for financial gain. The campaign has affected multiple industries, primarily government, financial, and healthcare entities. We have also seen the campaign affect the finance, telecommunications, and energy, oil and gas industries.

Conclusion

Over the course of this investigation, we have found various new tactics, techniques, and procedures (TTPs) used by APT-C-36. Our research shows that they modify their methods frequently, as evidenced by their use of different link shorteners and RATs. While spear-phishing emails are the initial infection vector for this ongoing campaign, the threat actor is constantly changing their payloads and improving their techniques to avoid detection, such as their use of geolocation filtering.

APT-C-36 selects their targets based on location and most likely the financial standing of the email recipient. These, and the prevalence of the emails, lead us to conclude that the threat actor’s ultimate goal is financial gain rather than espionage.

Security Recommendations

Threat actors like APT-C-36 are constantly seeking new ways to deploy their malware and stay one step ahead of their victims’ defenses. To secure their data from spear-phishing attempts, companies can benefit from tools such as the Trend Micro™ Smart Protection Suites and Worry-Free™ Business Security solutions, which protect end-users and

businesses from these kinds of threats by detecting and blocking malicious files, spam messages, and malicious URLs. They can also turn to tools like Trend Micro™ Email Security, 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.

Indicators of Compromise

You can access the link here for the full list of IOCs.