Numando: Count once, code twice

welivesecurity.com/2021/09/17/numando-latam-banking-trojan/

September 17, 2021

The (probably) penultimate post in our occasional series demystifying Latin American banking trojans.

ESET Research
17 Sep 2021 - 11:30AM

The (probably) penultimate post in our occasional series demystifying Latin American banking trojans.

Before concluding our series, there is one more LATAM banking trojan that deserves a closer look – Numando. The threat actor behind this malware family has been active since at least 2018. Even though it is not nearly as lively as Mekotio or Grandoreiro, it has been consistently used since we started tracking it, bringing interesting new techniques to the pool of Latin American banking trojans' tricks, like using seemingly useless ZIP archives or bundling payloads with decoy BMP images. Geographically, it focuses almost exclusively on Brazil with rare campaigns in Mexico and Spain.

Characteristics

As with all the other Latin American banking trojans described in this series, Numando is written in Delphi and utilizes fake overlay windows to lure sensitive information out of its victims. Some Numando variants store these images in an encrypted ZIP archive inside their .rsrc sections, while others utilize a separate Delphi DLL just for this storage.

Backdoor capabilities allow Numando to simulate mouse and keyboard actions, restart and shutdown the machine, display overlay windows, take screenshots and kill browser processes. Unlike other Latin American banking trojans, however, the commands are defined as numbers rather than strings (see Figure 1), which inspired our naming of this malware family.

```
8D 85 84 FD FF FF    lea     eax, [ebp+var_27C]
50                   push    eax
8D 95 80 FD FF FF    lea     edx, [ebp+var_280]
B8 9C 8E 77 00       mov     eax, offset a5ed21a6a ; "5ED21A6A"
E8 5A 19 DC FF       call    decrypt_string_0 ; <|>
8B 85 80 FD FF FF    mov     eax, [ebp+var_280]
B9 01 00 00 00       mov     ecx, 1
8B 55 FC             mov     edx, [ebp+var_4]
E8 DF 4D C9 FF       call    unknown_libname_162
8B C8                mov     ecx, eax
49                   dec     ecx
BA 01 00 00 00       mov     edx, 1
8B 45 FC             mov     eax, [ebp+var_4]
E8 67 43 C9 FF       call    System_LStrCopy
8B 95 84 FD FF FF    mov     edx, [ebp+var_27C]
8D 85 88 FD FF FF    lea     eax, [ebp+var_278]
E8 DA 47 C9 FF       call    decrypt_string
8B 85 88 FD FF FF    mov     eax, [ebp+var_278]
50                   push    eax
8D 95 7C FD FF FF    lea     edx, [ebp+var_284] ; int
B8 43 3D 8E 00       mov     eax, 9321795
E8 DF EF CA FF       call    System_Sysutils_IntToStr
8B 95 7C FD FF FF    mov     edx, [ebp+var_284]
58                   pop     eax
E8 83 4A C9 FF       call    System_UStrEqual
0F 85 D4 0C 00 00    jnz     def_7776FA
```


Figure 1. Numando command processing – part of command 9321795 processing (red)

Strings are encrypted by the most common algorithm among Latin American banking trojans (shown in Figure 5 of our Casbaneiro write-up) and are not organized into a string table. Numando collects the victimized machine's Windows version and bitness.

Unlike most of the other Latin American banking trojans covered in this series, Numando does not show signs of continuous development. There are some minor changes from time to time, but overall the binaries do not tend to change much.

Distribution and execution

Numando is distributed almost exclusively by spam. Based on our telemetry, its campaigns affect several hundred victims at most, making it considerably less successful than the most prevalent LATAM banking trojans such as Mekotio and Grandoreiro. Recent campaigns simply add a ZIP attachment containing an MSI installer to each spammed message. This installer contains a CAB archive with a legitimate application, an injector, and an encrypted Numando banking trojan DLL. If the potential victim executes the MSI, it eventually runs the legitimate application as well, and that side-loads the injector. The injector locates the payload and then decrypts it using a simple XOR algorithm with a multi-byte key, as in the overview of this process illustrated in Figure 2.

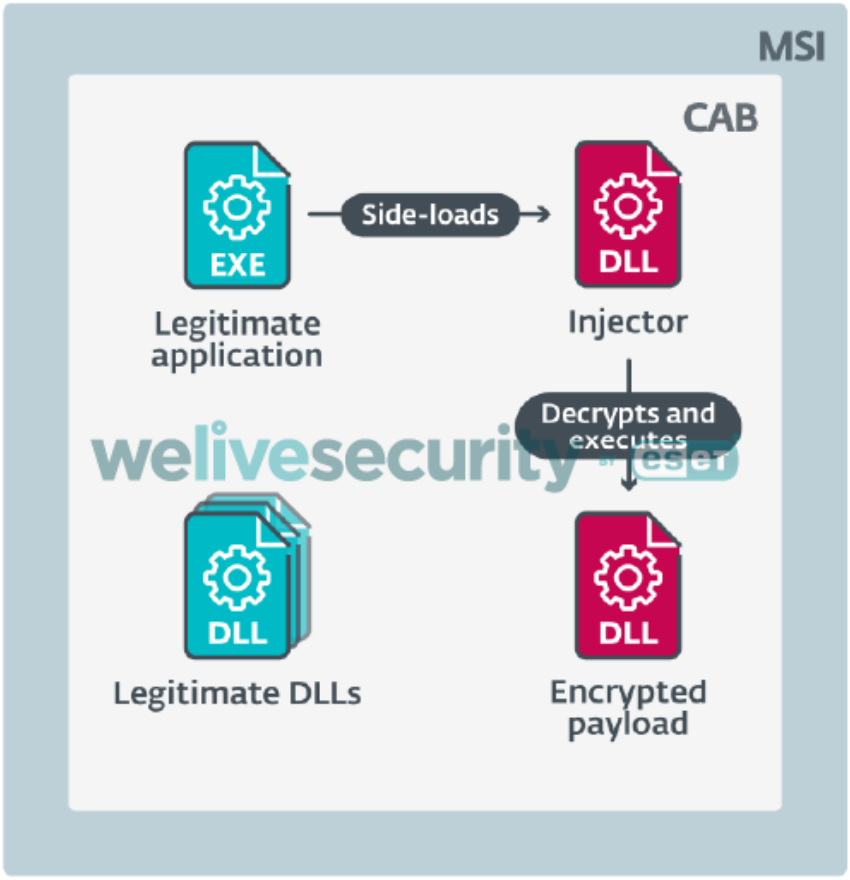

Figure 2. Numando MSI and its contents distributed in the latest campaigns

For Numando, the payload and injector are usually named identically – the injector with the .dll extension and the payload with no extension (see Figure 3) – making it is easy for the injector to locate the encrypted payload. Surprisingly, the injector is not written in Delphi – something very rare among Latin American banking trojans. The IoCs at the end of this blogpost contain a list of legitimate applications we have observed Numando abuse.

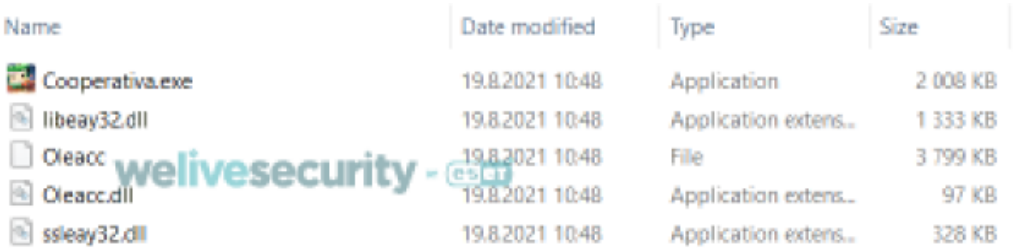

Figure 3. Files used for executing Numando. Legitimate application (Cooperativa.exe), injector (Oleacc.dll), encrypted payload (Oleacc) and legitimate DLLs.

Decoy ZIP and BMP overlay

There is one interesting distribution chain from the recent past worth mentioning. This chain starts with a Delphi downloader downloading a decoy ZIP archive (see Figure 4). The downloader ignores the archive's contents and extracts a hex-encoded encrypted string from the ZIP file comment, an optional ZIP file component stored at the end of the file. The downloader does not parse the ZIP structure, but rather looks for the last { character (used as a marker) in the whole file. Decrypting the string results in a different URL that leads to the actual payload archive.

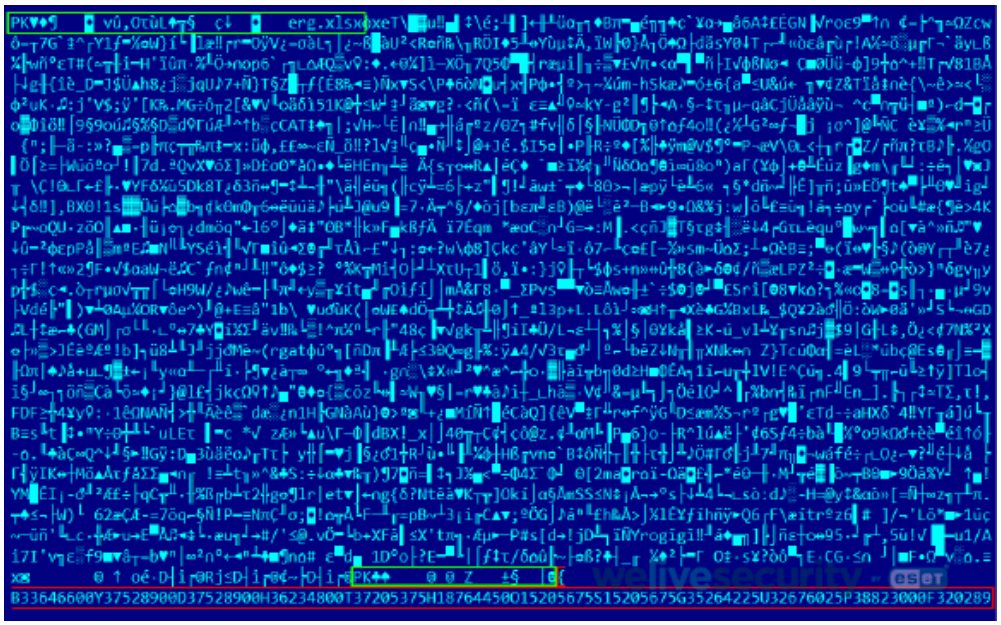

Figure 4. The decoy is a valid ZIP file (ZIP structures highlighted in green) with an encrypted URL included in a ZIP file comment at the end of the archive (red)

The second ZIP archive contains a legitimate application, an injector and a suspiciously large BMP image. The downloader extracts the contents of this archive and executes the legitimate application, which side-loads the injector that, in turn, extracts the Numando banking trojan from the BMP overlay and executes it. The process is illustrated in Figure 5.

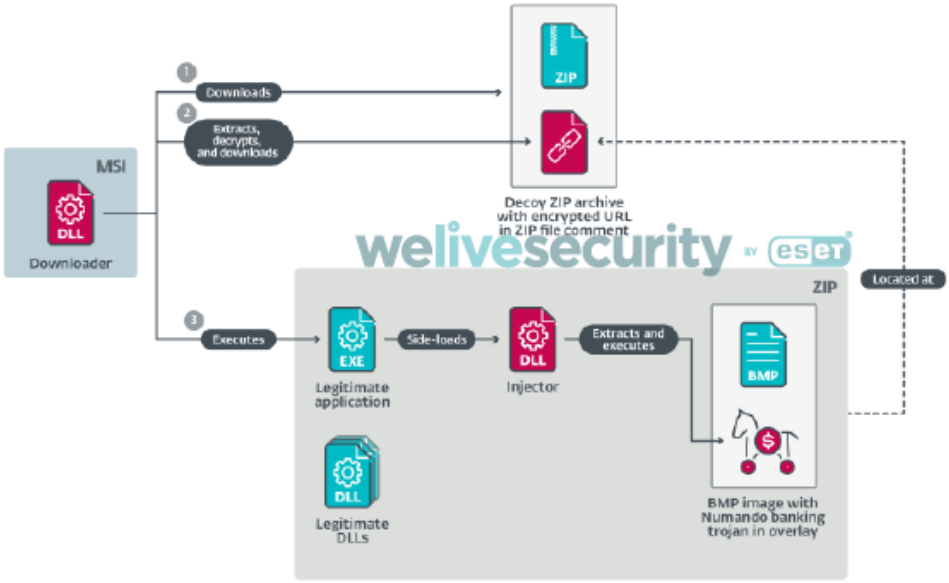

Figure 5. Numando distribution chain using a decoy ZIP archive

This BMP file is a valid image and can be opened in a majority of image viewers and editors without issue, as the overlaly is simply ignored. Figure 6 shows some of the decoy images the Numando threat actor uses.

Figure 6. Some BMP images Numando uses as decoys to carry its payload

Remote configuration

Like many other Latin American banking trojans, Numando abuses public services to store its remote configuration – YouTube and Pastebin in this case. Figure 7 shows an example of the configuration stored on YouTube – a technique similar to Casbaneiro, though much less sneaky. Google took the videos down promptly based on ESET's notification.

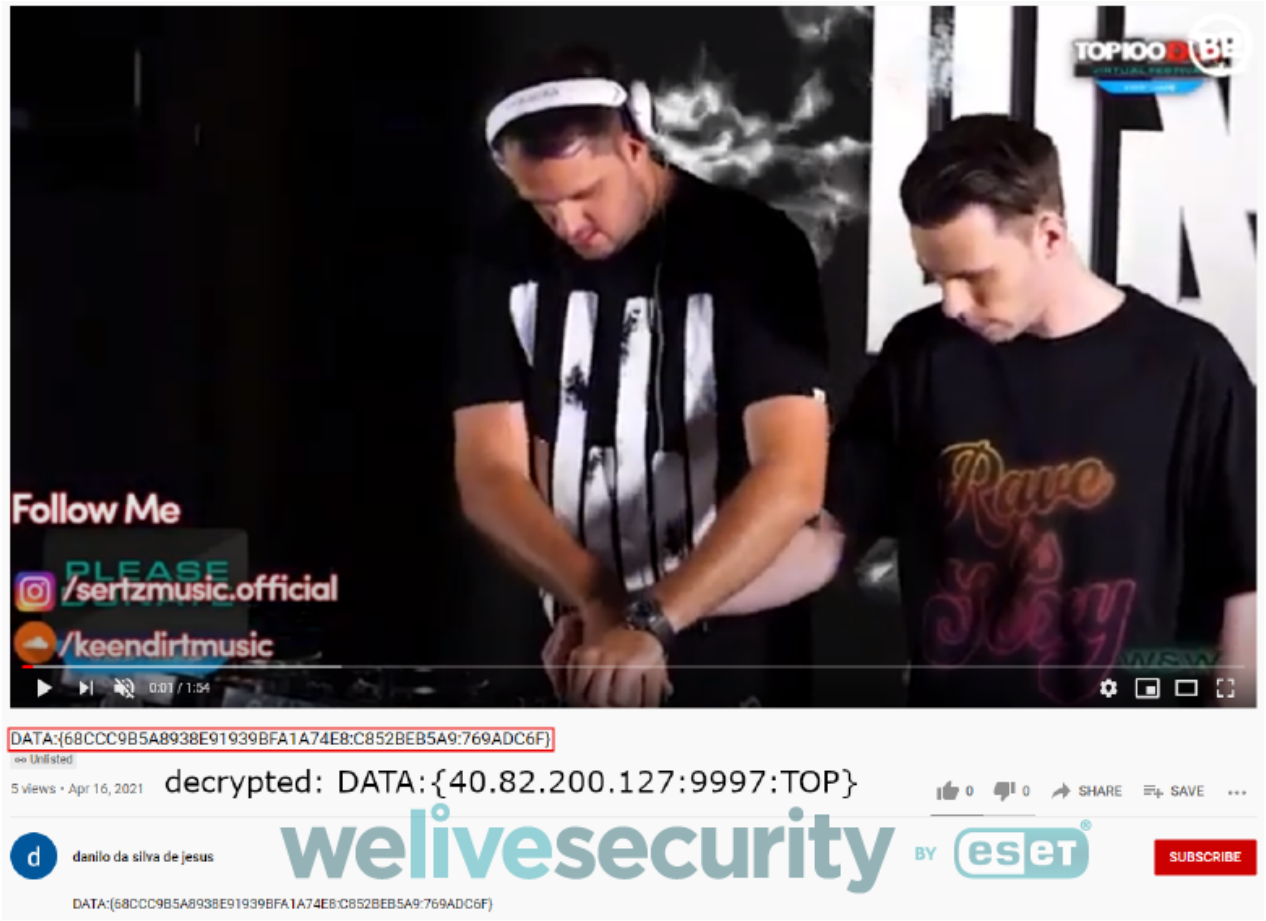

Figure 7. Numando remote configuration on YouTube

The format is simple – three entries delimited by ":" between the DATA:{ and } markers. Each entry is encrypted separately the same way as other strings in Numando – with the key hardcoded in the binary. This makes it difficult to decrypt the configuration without having the corresponding binary, however Numando does not change its decryption key very often, making decryption possible.

Conclusion

Numando is a Latin American banking trojan written in Delphi. It targets mainly Brazil with rare campaigns in Mexico and Spain. It is similar to the other families described in our series – it uses fake overlay windows, contains backdoor functionality and utilizes MSI.

We have covered its most typical features, distribution methods and remote configuration. It is the only LATAM banking trojan written in Delphi that uses a *non*-Delphi injector and its remote configuration format is unique, making two reliable factors when identifying this malware family.

For any inquiries, contact us at threatintel@eset.com. Indicators of Compromise can also be found in our GitHub repository.

Indicators of Compromise (IoCs)

Hashes

SHA-1	Description	ESET detection name
E69E69FBF438F898729E0D99EF772814F7571728	MSI downloader for “decoy ZIP”	Win32/TrojanDownloader.Delf.CQR
4A1C48064167FC4AD5D943A54A34785B3682DA92	MSI installer	Win32/Spy.Numando.BA
BB2BBCA6CA318AC0ABBA3CD53D097FA13DB85ED0	Numando banking trojan	Win32/Spy.Numando.E
BFDA3EAAB63E23802EA226C6A8A50359FE379E75	Numando banking trojan	Win32/Spy.Numando.AL
9A7A192B67895F63F1AFDF5ADF7BA2D195A17D80	Numando banking trojan	Win32/Spy.Numando.AO
7789C57DCC3520D714EC7CA03D00FFE92A06001A	DLL with overlay window images	Win32/Spy.Numando.P

Abused legitimate applications

Example SHA-1	EXE name	DLL name
A852A99E2982DF75842CCFC274EA3F9C54D22859	nvsmartmaxapp.exe	nvsmartmax.dll
F804DB94139B2E1D1D6A3CD27A9E78634540F87C	VBoxTray.exe	mpr.dll
65684B3D962FB3483766F9E4A9C047C0E27F055E	Dumpsender.exe	Oleacc.dll

C&C servers

- 138.91.168[.]205:733
- 20.195.196[.]231:733

- 20.197.228[.]40:779

Delivery URLs

- https://enjoyds.s3.us-east-2.amazonaws[.]com/H97FJNGD86R.zip
- https://lksluthe.s3.us-east-2.amazonaws[.]com/B876DRFKEED.zip
- https://procjdcals.s3.us-east-2.amazonaws[.]com/HN97YTYDFH.zip
- https://rmber.s3.ap-southeast-2.amazonaws[.]com/B97TDKHJBS.zip
- https://sucessmaker.s3.us-east-2.amazonaws[.]com/JKGHFD9807Y.zip
- https://trbnjust.s3.us-east-2.amazonaws[.]com/B97T908ENLK.zip
- https://webstrage.s3.us-east-2.amazonaws[.]com/G497TG7UDF.zip

MITRE ATT&CK techniques

Note: This table was built using version 9 of the MITRE ATT&CK framework.

Tactic	ID	Name	Description
Resource Development	T1583.001	Acquire Infrastructure: Domains	Numando operators register domains to be used as C&C servers.
T1587.001	Develop Capabilities: Malware	Numando is likely developed by its operator.	
Initial Access	T1566	Phishing: Spearphishing Attachment	Numando is distributed as a malicious email attachment.
Execution	T1204.002	User Execution: Malicious File	Numando relies on the victim to execute the distributed MSI file.
Defense Evasion	T1140	Deobfuscate/Decode Files or Information	Numando encrypts its payload or hides it inside a BMP image file, and some variants encrypt and hex encode their main payload URLs in a comment in decoy ZIP files.
T1574.002	Hijack Execution Flow: DLL Side-Loading	Numando is often executed by DLL side-loading.	
T1027.002	Obfuscated Files or Information: Software Packing	Some Numando binaries are packed with VMProtect or Themida.	
T1218.007	Signed Binary Proxy Execution: Msiexec	Numando uses the MSI format for execution.	
Discovery	T1010	Application Window Discovery	Numando monitors the foreground windows.

Tactic	ID	Name	Description
T1082	System Information Discovery	Numando collects the Windows version and bitness.	
Collection	T1113	Screen Capture	Numando can take screenshots.
Command and Control	T1132.002	Data Encoding: Non-Standard Encoding	Numando uses custom encryption.
Exfiltration	T1041	Exfiltration Over C2 Channel	Numando exfiltrates data via a C&C server.

17 Sep 2021 - 11:30AM

Sign up to receive an email update whenever a new article is published in our Ukraine Crisis – Digital Security Resource Center

Newsletter

Discussion