JanelaRAT | ThreatLabz

By Gaetano Pellegrino, Sudeep Singh

Published: 2023-08-10 · Archived: 2026-04-05 13:16:43 UTC

Capabilities

Capture and check window data

JanelaRAT captures the content of windows title bars and checks if they are interesting for the threat attacker. "Interesting" titles will be related to financial and banking data.

The malware implements a periodic behavior triggered every second and consists of three consecutive stages.

Stage 1

At the first stage, JanelaRAT checks if it obtained a list of interesting title bars. If not, then the malware requests a text file named **kepler186f.txt** to the C2. The content is encrypted with the same algorithm used for the strings. (Since the campaign was still active at the time of analysis, we were able to download an instance of such a file.) Once decrypted, you can see that it consists of a pipe-separated ("|") list of capitalized windows titles.

You can see an excerpt of the decrypted content in the box below.

Excerpt from an instance of kepler186f.txt

```
BANCOAZTECATUBANCAENLNEASUEASDECIDESLOGRAS|BITCOIN|SOLANA|ACTINVER|ACCESOALSISTEMABURSANET|ACT
ACCESOCONSULTADESALDOS|EACTINVER|ACCESOABANCABANCOAZTECA|BIENVENIDOSALABANCAENLNEABBVAMXICO
OBIERNOEMPRESASBBVAMXICO|INDEXBBVANET|BBVANETCASH|SANTANDERMXICOSPARTEDELABANCAELECTRNICA|BIT
LE|ETHEREUM|CASADEVECTOR|SANTANDER|SANTANDERM|ENLACESANTANDERCOMMXLOGBETENSCHANNELDRIVERSSO
RATIONNAMELOGINDSENEXTEVENTNAMESTARTDSEPROCESSORSTATEINITIALNOWCHECKINGCOOKIES|BANCOSANTANDE
XWEBCENTERPORTALBANBAJIOHOME|ELBANCODECONFIANZAPARAPERSONASPYMESGOBIERNOYAGRONEGOCIOS|BANC
ETBBCOMMX| … [REDACTED]
```

Kepler186f.txt file content is parsed as an array of strings and stored as a class field for future use.

Stage 2

At the second stage, JanelaRAT checks the same DLL directory for the **block.blq** file. This file has a slightly different structure compared to the kepler186f.txt file. It is still composed of a single, pipe-separated, record but it only contains three fields:

- a timestamp,
- a base64-encoded image
- a list of dash-separated ("-") window titles

The image below shows a snippet, belonging to the malware code, implementing the parsing logic for block.blq. If the file is outdated, then the malware deletes it.

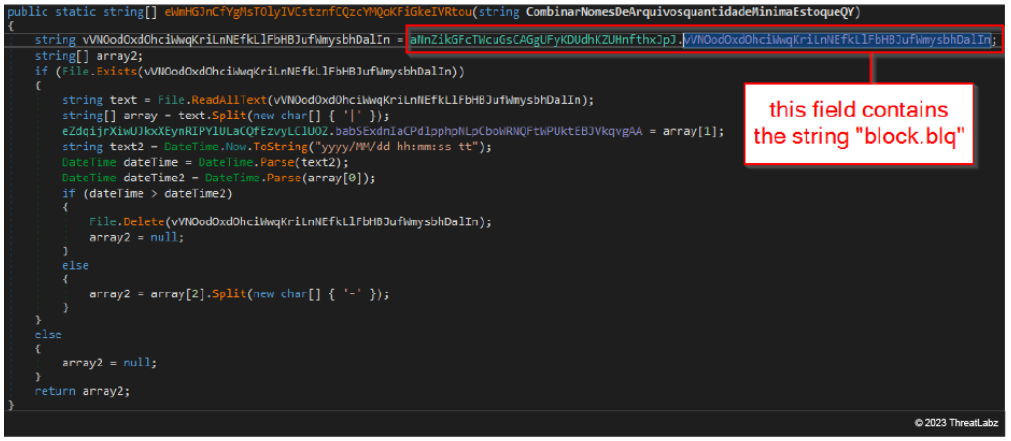

Figure 8: JanelaRAT code snippet implementing the parser for block.blq file content

The window titles included as the third field in block.blq are titles of windows the attacker wants to block. When the title of the foreground window is included in the block.blq, the malware attempts to close it. The blocking mechanism is implemented by invoking the SendMessage API with WM_CLOSE value for the Msg argument. JanelaRat also visualizes a dialog to the victim showing a fake error message.

Stage 3

At the third stage, the malware checks if the title of the window in the foreground is appealing. The check is made after grabbing the title, capitalizing it, and eventually dropping all non-alphabetical characters. By "appealing", we mean what was discussed at Stage 1 (i.e., the title was in a previously parsed instance of kepler186f.txt). If the check succeeds, JanelaRAT opens a C2 channel in the form of a socket as discussed earlier. This channel is later used for alerting the threat attacker about the victim opening interesting windows, sending key logs, mouse clicks, and implementing remote desktop sessions.

Acquire host profile details

JanelaRAT is capable of collecting and sending information about the compromised host to the attacker. This information is encapsulated in a packet containing the fields reported in the following table. As you can see, the field names don't always correlate with their actual content. Moreover, some fields are left to the default values. Those aspects suggest that the original malware source code has been eventually modified or repurposed to fit the new needs of the operator.

JanelaRAT sends basic information about the compromised host to the attacker

Field Name	Field Value
Version	JanelaRAT version string. Hardcoded as **1.0.6.4** for the sample discussed in this section. One of the few unencrypted strings embedded in the malware.
OperatingSystem	A pipe-separated string containing the following fields: OS version major, OS version minor, OS platform, integer pointers size. Example: **0|4|2|32**.
AccountType	A dash-separated string containing the following fields: Role of the user logged in at time of request. Supported values: **Admin**, **User**, **Convidado** (Guest in Portuguese), and **Desconhecido** (Unknown in Portuguese).
Country	A string containing the title of the last “interesting” window opened by the user. For interesting, we mean that is included in the content of the kepler186f.txt file (previously discussed). All non-alphabetical symbols are removed from the original title bar and the chars are upper-cased.
CountryCode	Empty string.
Region	Empty string.
City	Empty string.
ImageIndex	0

Track mouse movements

JanelaRAT is capable of sending mouse activity to through C2. It defines a packet class containing the following fields:

- x-position of the cursor
- y-position of the cursor
- a boolean value set to true if the left button of the mouse is clicked
- a boolean value set to true if the left button of the mouse was double clicked

Once serialized, an instance of this class is shipped.

Track system usage

JanelaRAT is capable of gathering additional information about the infected system usage.

System usage information gathered by JanelaRAT

Index	Element
0	User
1	[username of the user currently logged in]
2	PC
3	[machine name]
4	Ligado [connected in Portuguese, ed.]
5	[time elapsed since the last system reboot. It's a string having the format **{0}d : {1}h : {2}m : {3}s** where {0}, {1}, {2}, {3} are placeholders for the number of days, hours, minutes, and seconds respectively]
6	IP
7	[comma-separated list of IP addresses currently associated with the infected system]

The malware assembles an array of strings containing the elements shown in the table above. Once assembled, the array is sent to the C2.

Open message boxes on the infected system

JanelaRAT gives a threat attacker the ability to open message boxes on the infected system, which may influence the behaviour of the user. After having shown the message box, the malware sends an acknowledgment to the C2. The acknowledge is another packet class containing a single field of type string called "Message" and instantiated with the value **Mensagem mostrada** ("Message shown" in Portuguese).

Perform actions

JanelaRAT is capable of performing a wide range of actions on the attacker's behalf. Those actions are identified by an integer number called "Mode".

JanelaRAT is capable of performing action on behalf of the attacker

Mode	Description
1	Shuts down the infected system by issuing the shutdown shell command.
2	Suspends the infected system.
5	Enables mouse synthesization. This mode allows the attacker to simulate the mouse and issue clicks or double-clicks for the left button.
6	Enables sleep for one second.
8	Enables sleep for one second.
9	Create a file named **1.bat** under the user directory. That file contains the following batch script: cmd /min /C set __COMPAT_LAYER=RUNASINVOKER && start #1 cmd /min /C REG ADD HKCUControl PanelDesktop /v Win8DpiScaling /t REG_DWORD /d 0x00000001 /f cmd /min /C REG ADD HKCUControl PanelDesktop /v LogPixels /t REG_DWORD /d 0x00000060 /f

Mode	Description
	The purpose of this script is to fix potential errors in rendering fonts. This script is executed with **%SystemRoot%\taskmgr.exe** as its first argument, resulting in executing the Task Manager application without requesting administrative privileges. The task Manager window is immediately hidden by running ShowWindow API with the SW_HIDE value for the nCmdShow argument. Finally, 1.bat is removed.
10	Deletes the file **block.blq** if it exists in the same folder as JanelaRAT.
11	Sends a test email by starting a new process with **mailto:teste@teste.com?subject=teste&body=teste**
12	Enables Desktop Windows Manager composition and sets the Aero Windows theme.
51	Disables mouse synthesization.
52	Shows the last selected window, waits 300 milliseconds, and eventually maximizes it.
80	Sends the **{DOWN}** key to the currently active application.
81	Sends the **{UP}** key to the currently active application.
82	Sends the **{TAB}** key to the currently active application.
99	Uninstalls any hook installed by JanelaRAT to monitor keyboard events and mouse events. *In this specific case, there is no acknowledgement sent back to the attacker when the operation completes.*

After an action is performed, with the exception of Mode 99, the malware sends a notification to the C2 by encapsulating Mode as the field of a packet class and shipping the serialized instance.

Capture screenshots

JanelaRAT is capable of capturing and shipping screenshots. It defines an packet class containing three fields:

- Janela (window, in Portuguese): Integer dictating the type of screenshot operation being requested. If Janela is set to 1, the malware captures a magnified screenshot. If Janela is set to 2, then the malware live-captures a screenshot and sends it through the C2.
- Mode: Integer that controls the encoding of the captured screenshot. If this field is set to a value bigger than 10, then the screenshot is encoded as a PNG, otherwise it is encoded as a JPG.
- Number: This field is not used.

Run in special execution modes

JanelaRat ships with the capability of running in special execution modes. Each execution mode affects the malware behaviour and it is identified by a label. The attacker may request the malware to operate in any of those modes.

As an example, when in **_blcoqueio_tempo_determinado** mode, the malware creates a new block.blq file with a limited duration in minutes. The purpose of this behaviour is to temporarily prevent the user from opening windows with specific titles. The file is created only if it doesn't already exist in the malware directory.

When in **_modal_inicial** mode, the malware shows a modal dialog that forces the user to interact with the malware by disabling user interaction with the main window. The foreground image for the dialog is obtained from C2. The malware registers a hook for both keyboard and mouse events.

When in **_modal_win_update** mode, JanelaRAT displays a fake alert warning the user to not shut the system down while the Windows updates are in progress. Most likely, this allows the attacker to operate on the compromised host while the fake warning is shown to the user.

Finally, when in **_modal_loading**, **modal_error**, or **modal_tocalm**, JanelaRAT operates in the same way: it shows an attacker-provided image to the user. The image is different in each mode, but we weren't able to obtain any of those at the time of analysis.

Explore more Zscaler blogs