Debugger and Sandbox Detection

This code provides functions to detect the presence of a debugger or a sandbox environment. It includes the following functions:

`is_debugger_detected() -> bool`

Checks if a debugger is detected.

Returns: `true` if a debugger is present; otherwise, `false`.

`is_sandbox_detected() -> bool`

Checks if a sandbox environment is detected.

Returns: `true` if a sandbox environment is present; otherwise, `false`.

Suspicious Renamed Executable Detection

The function checks for the presence of suspiciously named executables that might indicate a sandbox environment. The suspicious executable names include:

- sample.exe
- bot.exe
- sandbox.exe
- malware.exe
- test.exe
- klavme.exe
- myapp.exe
- testapp.exe
- infected.exe

Suspicious User Name Detection

The function checks if any suspicious user names are present on the system. The suspicious user names include:

- CurrentUser
- Sandbox
- Emily
- HAPUBWS
- Hong Lee
- IT-ADMIN
- Johnson
- Miller
- milozs
- Peter Wilson
- timmy
- user
- sand box
- malware
- maltest
- test user
- virus
- John Doe
- SANDBOX
- 7SILVIA
- HANSPETER-PC
- JOHN-PC
- MUELLER-PC
- WIN7-TRAPS
- FORTINET
- TEQUILABOOMBOOM

Specific Conditions Check

The function checks for specific conditions related to certain users and host names:

- If the user is "Wilber" and the host name starts with "SC" or "SW".
- If the user is "admin" and the host name is "SystemIT" or "KLONE_X64-PC".
- If the user is "John" and the files "C:\take_screenshot.ps1" and "C:\loaddll.exe" exist.

Suspicious File Existence Check

The function checks for the existence of specific files that might indicate a sandbox environment:

- C:\email.doc
- C:\email.htm
- C:\123\email.doc
- C:\123\email.docx

Hardware and System Checks

The function performs the following hardware and system checks:

- Checks if the number of physical CPUs is less than 2.
- Checks if the total space on the C: drive is less than 80 GB (85899345920 bytes).
- Checks if the mouse cursor position remains unchanged after a delay of 10 seconds.
- Checks if the total memory is less than 1 GB (1073741824 bytes).
- Checks if any of the suspicious processes are running.
- Checks the parent process name of the current process.

Network Interface Check

The function checks the network interfaces for specific MAC addresses that might indicate a sandbox environment:

- MAC addresses starting with "00:05:69"
- MAC addresses starting with "00:0c:29"
- MAC addresses starting with "00:1C:14"
- MAC addresses starting with "00:50:56"
- MAC addresses starting with "08:16:3E"
- MAC addresses starting with "08:00:27"

Revision #4
Created 28 June 2023 08:22:06 by Makito
Updated 3 July 2023 10:25:39 by MasterBigD