Analysis Report for: Ä£¿é1.bas

Decoded using latin-1...

Overall Functionality

This VBA code manipulates Microsoft Excel workbooks. It appears designed to automate a report generation or data processing task. The code consists of four main subroutines (`É¾³ý¶àÓà¿Õ°×ÐÐPI`, `¿ÂÀö´ï`, `¿ÂÀö´ï2`, `packinglist`). Each subroutine performs similar operations: copying data from one sheet to another, resizing and repositioning shapes, deleting rows and shapes, pasting values only, and finally deleting all sheets except for a specific target sheet. The code also removes a VB component named "Ä£¿é1". The use of non-standard characters in variable and sheet names suggests localization or obfuscation. The repetitive nature of the subroutines suggests a potential for consolidation and improved efficiency.

Function Summaries

The code contains four subroutines (functions in VBA):

* **`É¾³ý¶àÓà¿Õ°×ÐÐPI()`**: This subroutine copies data from the "PROFORMA INVOICE" sheet to the "PROFORMA INVOICE (2)" sheet, deletes rows based on values from the "±íÍ·" sheet, deletes a shape named "b", converts the remaining data to values, and deletes all sheets except "PROFORMA INVOICE (2)". It also removes a VB component.

* **`¿ÂÀö´ï()`**: This subroutine performs similar operations to the first, but operates on the "Í¼Æ¬" and "¿ÂÀö´ï" sheets. It additionally resizes and repositions shapes on the "¿ÂÀö´ï" sheet.

* **`¿ÂÀö´ï2()`**: This subroutine is nearly identical to `¿ÂÀö´ï()`, but operates on the "Í¼Æ¬" and "¿ÂÀö´ï2" sheets.

* **`packinglist()`**: This subroutine copies data from the "PROFORMA INVOICE" sheet to the "packing list" sheet, resizes and repositions shapes on the "packing list" sheet, deletes rows and a shape named "CHQD", converts the remaining data to values, and deletes all sheets except "packing list". It also removes a VB component.

All subroutines have no parameters and no explicit return value.

Control Flow

The control flow within each subroutine is relatively straightforward:

1. **Data Acquisition:** Values are read from specific cells in the "±íÍ·" sheet.
2. **Conditional Logic:** A conditional statement (`If c = 1502 Then d = 1521 End If`) modifies the value of `d` based on the value of `c`. Another condition (`If Not c = "1521" Then`) controls whether rows are deleted.
3. **Data Manipulation:** Data is copied and pasted between sheets. Shapes are resized and repositioned. Rows are deleted based on the range specified by variables `a`, `b`, `c`, and `d`.
4. **Value Conversion:** The `PasteSpecial` method converts the copied data to values only.
5. **Sheet Deletion:** A loop deletes all sheets except the designated target sheet.
6. **VB Component Removal:** A VB component ("Ä£¿é1") is removed from the project.

The loops are simple `For Each` loops iterating through sheets and shapes. The conditional statements determine which rows are deleted and control the shape manipulation.

Data Structures

The primary data structures used are:

* **Excel Worksheets:** The code interacts extensively with different worksheets within an Excel workbook.
* **Excel Ranges:** Ranges of cells are selected, copied, and pasted.
* **Excel Shapes:** Shapes are manipulated (resized, repositioned, deleted).
* **Variables:** Simple variables (`a`, `b`, `c`, `d`) store integer and string values, primarily representing row numbers and other data from the "±íÍ·" sheet.

Malware Family Suggestion

While this code is not inherently malicious, its structure and functionality raise some concerns:

* **Obfuscation:** The use of non-standard characters in variable and sheet names makes the code harder to understand and analyze, a common obfuscation technique used in malware.
* **Sheet Deletion:** The wholesale deletion of sheets could be used to cover tracks or remove unwanted data. This is concerning if the deleted sheets contain important information.
* **VB Component Removal:** The removal of the "Ä£¿é1" VB component could be an attempt to hide malicious code embedded within that

component. This component could contain a macro virus, or some other malicious program.
* **Repetitive Code:** The high degree of similarity between the three main subroutines suggests a potential for malicious code to be easily copied and adapted to different targets.
* **Unintended Functionality:** The deletion of sheets based on a condition could lead to the unintended deletion of crucial data if the conditions are not correctly defined.

Overall, while not directly exhibiting malicious behavior, the code's design incorporates elements often found in malware, increasing the potential risk if modified or used maliciously. It's more likely to be a poorly written, obfuscated script rather than a dedicated piece of malware. However, a thorough security review is warranted before deploying or using this code. It has the potential to be modified to become a macro virus if used by malicious actors.