Supply Chain Management of

Footwear Industries in Bangladesh

Supply Chain Management of

Footwear Industries in Bangladesh

**Reverse Engineering TTC6510-3002**

Joonatan Ovaska

A K M MAHMUDUL HAQUE

AB0208

**Student number:** 2110841

**WinLab02**

Date: 25.10.2023

**First Step**

* Issue: When the winlab01.exe file is run, a file named IMPORTANT-INFORMATION.txt appears on the desktop.
* Content: The text file states that files have been locked and will be unlocked if a payment of 0.5 BTC is made. Instructions for payment are given via email.
* Encryption: The ransomware adds the .locked extension to affected files. Removing the extension won't recover the files; they remain encrypted.
* File Viewing: Encrypted files with the .locked extension can be viewed in a text editor, but the content remains scrambled.
* Scope: Only files within the user's folder are affected by this ransomware.
* Affected File Types: The ransomware targets specific file types, including .xlsx, .docx, .jpg, .png, .doc, .xls, .txt, and .pdf files. These files are encrypted and cannot be accessed without the decryption key.
* The .locked extension appears to be primarily intended to show which files are affected by the ransomware.

**A screenshot of a computer

Description automatically generated**

**Second Step**

* Visibility: Using procmon, processes linked to the malware can be observed.
* Focus: Specifically, attention is given to processes involved in manipulating files.
* Relevance: These file-related processes are crucial for understanding the malware's behavior and impact on the system.

**A close up of a text

Description automatically generated with medium confidence**

**A white background with black text

Description automatically generated**



**Third Step**

* Regshot Findings: Regshot analysis reveals that 18 registry entries were altered after executing the file.
* Observation: However, upon closer inspection of the regshot output, none of these modifications appear to be pertinent to the current issue at hand.

A screenshot of a computer

Description automatically generated

* Exception Handling: The malware includes a noteworthy top-level exception handling feature.
* Debugging Countermeasure: This feature functions as a countermeasure against debugging attempts. It allows the malware to decide how to respond when an error occurs, a task usually handled by the operating system.
* Usual OS Behavior: Normally, operating systems take control during errors, displaying messages or terminating the program.
* Custom Handler: The malware's custom exception handler comes into play when the application operates without debugging. However, it remains inactive if the application is being debugged.

A screenshot of a computer

Description automatically generated

**Fourth Step**

* File Details: The winlab02.exe file is 14KB in size.
* Location: It is located in the C:\Users\user\Desktop\LABS folder on the Flare-VM machine.
* Analysis Tool: The Cutter analysis tool has been utilized to extract basic information from the file.
* MD5 Hash: Cutter indicates that the program has an MD5 hash value, but the specific hash value is not provided in the given information.

A screenshot of a computer

Description automatically generated

Dependency Walker lists eleven dependencies.



**Fifth Step**

* Analysis Tool: The malware can be examined for valuable information using the strings2 tool.
* In the analysis output, figure shows the filetypes that have been locked and the affected directories.
* Ransom Message: Additionally, the extracted strings reveal a message that requests a payment of 0.5 BTC in exchange for unlocking the encrypted files.

A blue screen with white text

Description automatically generated

* Some relevant assembly functions displayed:
  + PathCombineW
  + PathAppendW
  + StrCmpW
  + SHLWAPI .dll and so on
* MD5 Hash Lookup: Upon searching for the MD5 hash, it is confirmed that the winlab02.exe file is identified as known malware.
* Hybrid Analysis Overview: Figure 13 provides an overview of the file on the malware analysis site Hybrid Analysis. The analysis assigns the winlab02.exe file a threat score of 56/100.

A screenshot of a computer

Description automatically generated

**Sixth Step**

* Scope of Section: This section does not extensively analyze the Assembly code.
* Focus: Instead, it highlights relevant functions in connection with the earlier discussion.
* Comments: Noteworthy comments are included where essential to understanding the context and functionality of the code.

A screen shot of a computer code

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer code

Description automatically generated

* The malware will searches for files of the specified types (see Figure 13) and append them with *.locked.*

A screenshot of a computer code

Description automatically generated

A screenshot of a computer program

Description automatically generated

A screenshot of a computer code

Description automatically generated

A screenshot of a computer

Description automatically generated

* Anti debuggibg:

A screen shot of a computer code

Description automatically generated

A screen shot of a computer code

Description automatically generated