Cybersecurity

Escape from the Digital Dungeon

Introduction

It’s Friday at 4 p.m. You have finished all your work for the week and are ready to leave early to enjoy a needed break. As you prepare to shut off your computer, the familiar *bing* of a new email sounds. Although you want to ignore it, you open your email and read the following email.

DATE: 04/19/2024; 4:00 p.m.

SUBJECT: The clock has started!

“Tonight tonight, my plans I make, tomorrow tomorrow, your [data] I take. You will never win the game, for Rumpelstiltskin is my name!”

That’s right, you have been hacked by Rumpelstiltskin!

You have one hour to solve my riddle or I will post all your sales data on the internet. If you don’t enter the correct password at https://eyarc.site/cyber/index.html within one hour, your data posts!

You get one clue:

Search every person’s files,
Search high and low!
I used just one person’s files
For my password bold.
Password? You say.
What is it? You ask.
Find all the ***digits***
Sum them up!
It’s the only way
To avoid bad luck.

Time is ticking …

Rumpelstiltskin

Your blood runs cold. You just completed a training on cybersecurity and the trainer spoke about the infamous Rumpelstiltskin hacker. The hacker is a notorious joker who appears to hack for fun — never requesting money but presenting challenges, even games, that if not completed, result in Rumpelstiltskin posting a company's sensitive data on the web. The damages to other companies have been in the millions of dollars. You know this is serious and you must act quickly.

You call your team together, share the email and ask everyone to get started. Given the time limit, you know you are going to have to make a plan, divide up responsibilities and hopefully put it all together before the deadline. Thankfully, the cybersecurity training gave you a clue of where to start looking.

- Rumpelstiltskin usually enters a system through old versions of software that have vulnerabilities (i.e., users not using the most recent major version of a software). Once he finds a vulnerable machine or machines, he installs custom software to steal the username and password of the person using that machine. Using the stolen credentials, he downloads documents using the stolen username. He then uses all the documents from a user to create his game.
- From your cybersecurity training, you know that all software may have bugs that can be exploited, but the software with major version changes (not just minor changes or patches) is most easily exploited. Software version updates might look something like this: 4.5.2002. The first number usually depicts major changes in the software, the second number usually depicts minor changes (like improved functionality) in the software, the third number usually depicts patches and any additional numbers are special cases.
- In past attacks, Rumpelstiltskin targets sales files that are uploaded to a company's data lake. These files are usually written in JSON or XML. Your company uses batch processing and JSON. The company uploads these files to its data lake each night. The company uploads each sales rep's file separately. For instance, all sales on 3/21/2023 for Catherine Banks would be saved as **File_2023-3-21 Banks, Catherine.json**. This file, would contain all the sales Catherine made on that day and might appear as follows:

  ```
  [{"OrderID":2043,"CustomerID":6134,"CustomerName":"Awesome Auto","Date":"3/21/2023","EmployeeID":255,"EmployeeName":"Banks, Catherine","":{"Make":["Audi","Mercedes-Benz"],"Model":["R8","S-Class"],"Price":[175000,125000],"Quantity":[1,2]}}]
  ```

- The JSON file is structured so that it can be easily moved between systems as it follows a standard formatting practice. The above code shows that Catherine sold two car models, an Audi and a Mercedes-Benz to Awesome Auto. Additional information is included.
- Your team has pulled the 906 files that Rumpelstiltskin could have accessed and placed them in the folder named **Potential_Hacked_Files**. Thankfully, IT designed the system so that each user is only able to see the JSON files related to their sales. So, with a compromised login, the only files that are at risk of being seen by Rumpelstiltskin and used for his game are the files of the person with that login.

Data description

There are several files included for this case. All the data for this case is contained in a zipped folder labeled **Cybersecurity_case_study_Digital_Dungeon_Potential Hacked_Files.zip**. Unzip the files into a folder on your computer. The zipped folder contains the following files:

- **Cybersecurity_case_study_Digital_Dungeon_Potential_Hacked_Files** folder. Within this folder are 906 csv files. Each of these csv files is a file written in JSON that contains the daily sales information for each person. The file is named using the following convention: **File_YYYY_MM_DD LastName, FirstName.csv**. *Do not open these csv files in Microsoft Excel as this can change the formatting and make the task more difficult*. If you want to see what is contained in one of these files, open it in Notepad or Notepad++.
- **Cybersecurity_case_study_Digital_Dungeon_Master_File.xlsx** is an Excel file with three tabs of information:
  - On the tab "Users" is a list of all the company employees. The UserID is listed for each employee, their first name (Fname), last name (Lname) and email address.
  - On the tab "Installed Software" is a list of all software installed on each employee's computer. The list includes the UserID, the name of the software (SoftwareName) and the version of the software running on the user's machine.
  - On the tab "Software Patching" is a list of all software at the company and the most recent version of the software.

Required

Solve the problem within one hour.

If you solve the problem successfully, you should be able to answer each of the following questions. If you do not solve the entire case, answer as many questions as you can for partial credit.

1. Name of user or users who have unpatched software.
2. Name of unpatched software programs.
3. Possible final password(s) that could avoid the attack.
4. The revealed code once you enter the correct password on the website.

Hints

This case does not require using macros, but it can be solved by using macros.

The Input Data tool in Alteryx can be used to read multiple files at one time. You can learn more at https://help.alteryx.com/20223/designer/input-data-tool.

When importing data into Alteryx, you do not always have to have a "neat and tidy" import if you don't need all the data. You can import, clean it and then structure your data as appropriate.

The RegEx tool is a powerful way to parse data. If you use the Tokenize output method, you can split data into rows.