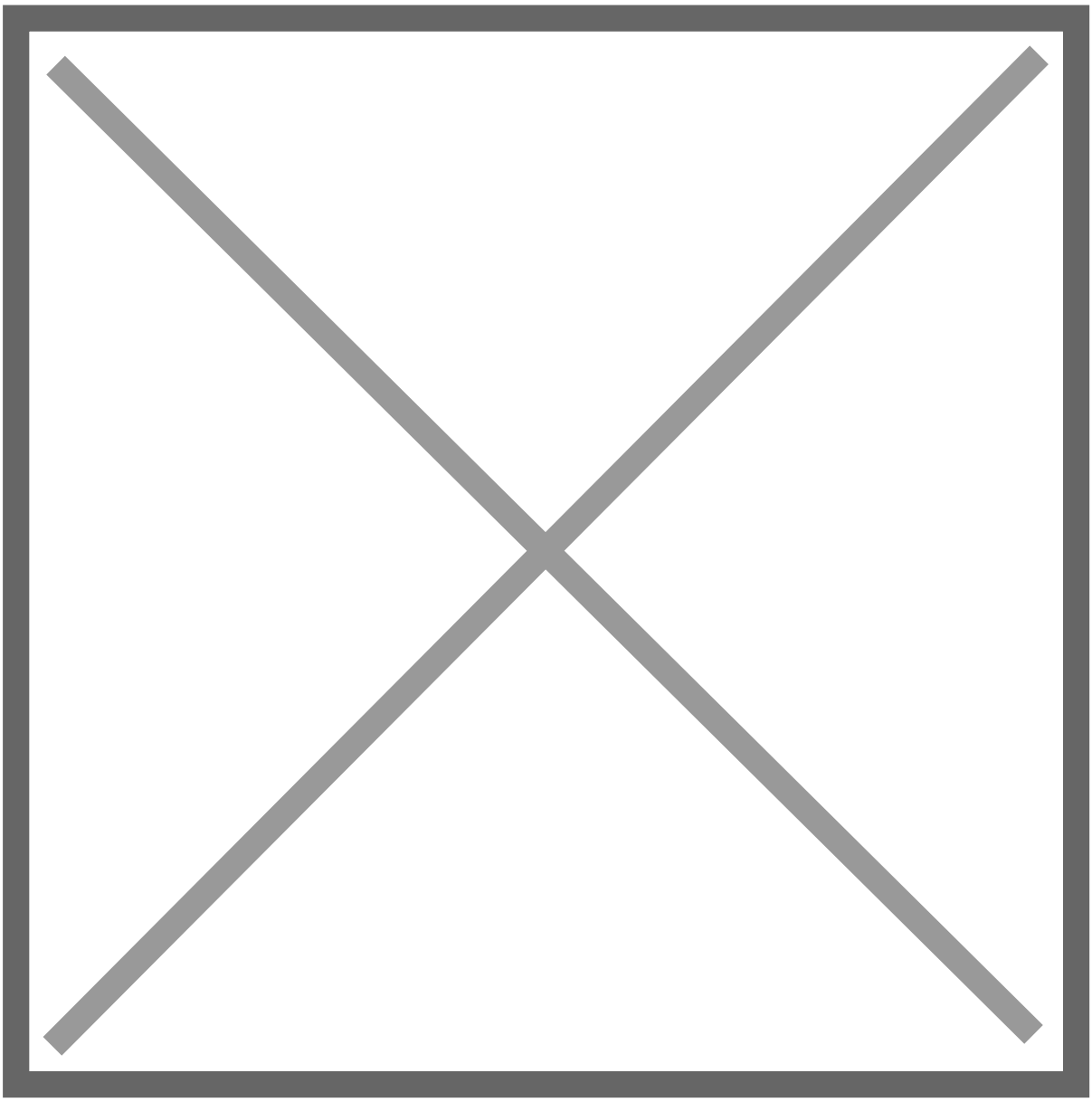
Targeted and Efficien Phishing: Alteryx Workflow

Background

Recently, my friend who works in the accounting industry has been working hard to learn how to use a tool called Alteryx. She occasionally shares her learning experience with me, even though I do not have any knowledge of the accounting industry. Through our conversations, I learned that this software has macro functions. Based on a hacker’s intuition, I wondered if the macros in this software could execute code, even using its importable files for phishing, just like in Microsoft Office products. After some searching and research, I discovered that Alteryx’s importable files could indeed be used to execute client-side code and for phishing, and they can be very targeted and efficient.

Compared to Microsoft Office products, Alteryx software has a more specific target audience, such as accounting, data analysis, and finance professionals. Therefore, this may not be a phishing vector applicable in all situations. However, on the one hand, the macro feature in Microsoft Office products has been abused by attackers to gain client-side code execution through phishing attacks; Microsoft and many security product vendors have taken a series of measures, such as disabling macros in documents by default, strengthening macro scanning, and disabling Win32 API calls (ASR Rules) in macros, and so on. On the other hand, because the audience for Alteryx software is more specific and the software has not yet been used for phishing attacks (I’m not sure if anyone has done so, but I haven’t found any related articles), users of the software may be relatively less vigilant.



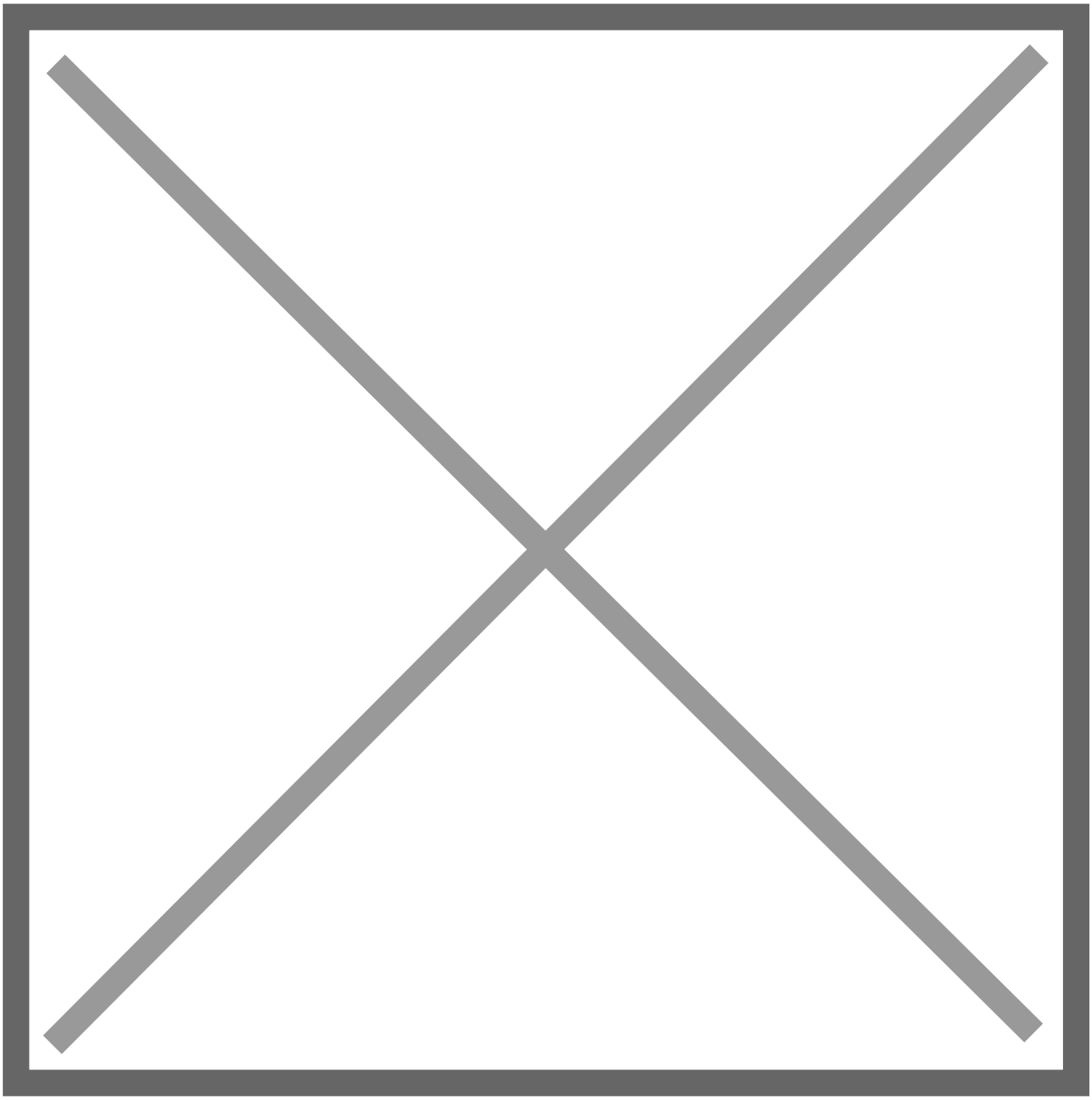
Alteryx Software

Alteryx is a data analytics software that enables users to perform data blending and advanced analytics with ease. It is designed to help analysts and data scientists solve complex data problems quickly and efficiently, without requiring advanced technical skills.

The software offers a drag-and-drop interface that allows users to easily connect and manipulate data from various sources, including spreadsheets, databases, and cloud-based applications. It also provides a wide range of tools for data cleaning, transformation, modeling, and visualization, as well as machine learning algorithms and predictive analytics capabilities.

Alteryx is used in a variety of industries, including finance, healthcare, retail, and manufacturing, among others. It is popular among analysts and data scientists who want to streamline their

workflows and automate repetitive tasks, allowing them to focus on higher-value activities, such as developing insights and making data-driven decisions.



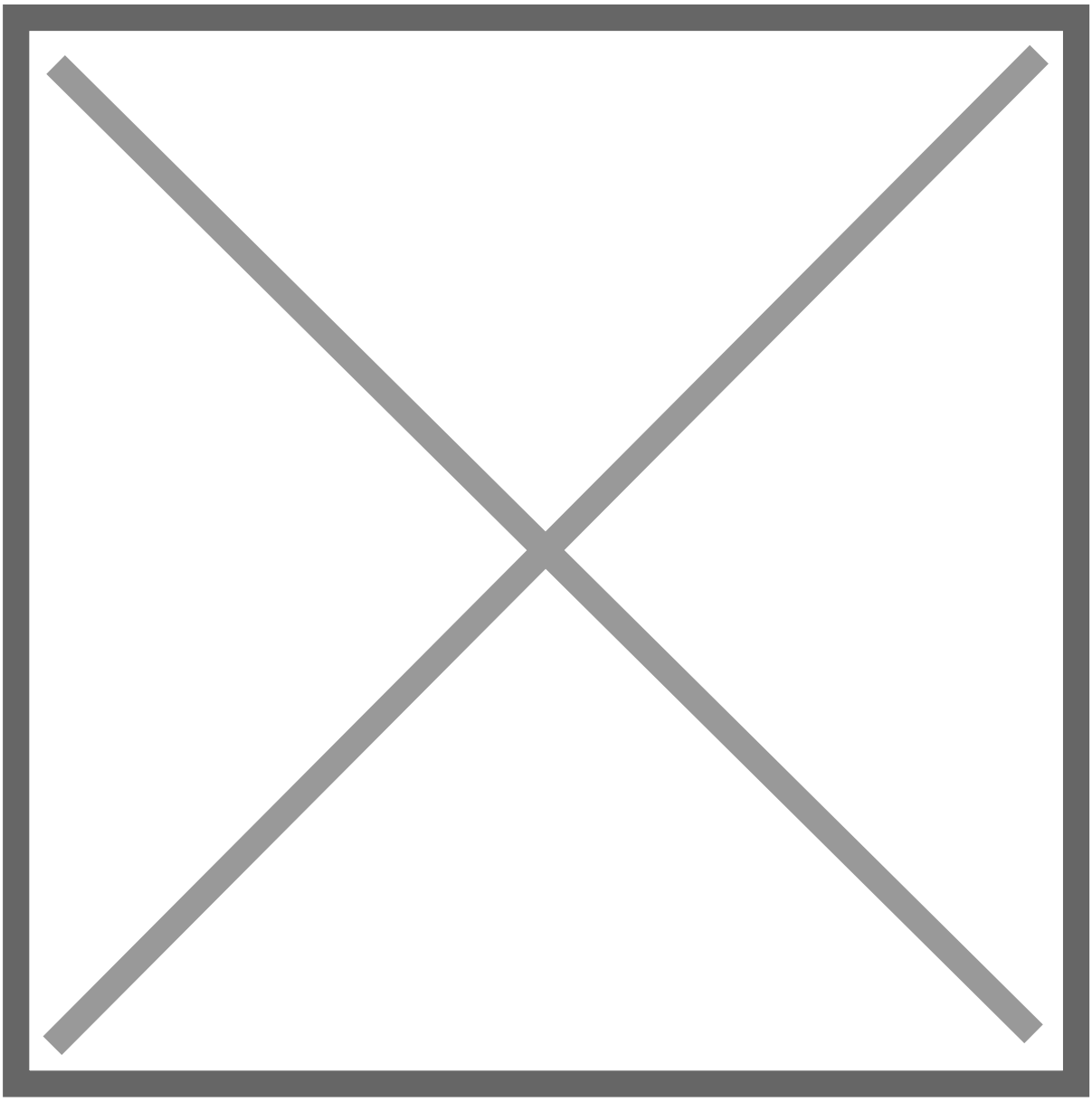
Alteryx Workflow

In Alteryx, A workflow consists of connected tools that perform different functions to process data. A workflow file contains all the information about a particular data workflow, including the data inputs, transformations, and outputs. It is a saved version of the workflow. The file extension of a workflow file is **.yxmd**, it can be imported or exported (save as).

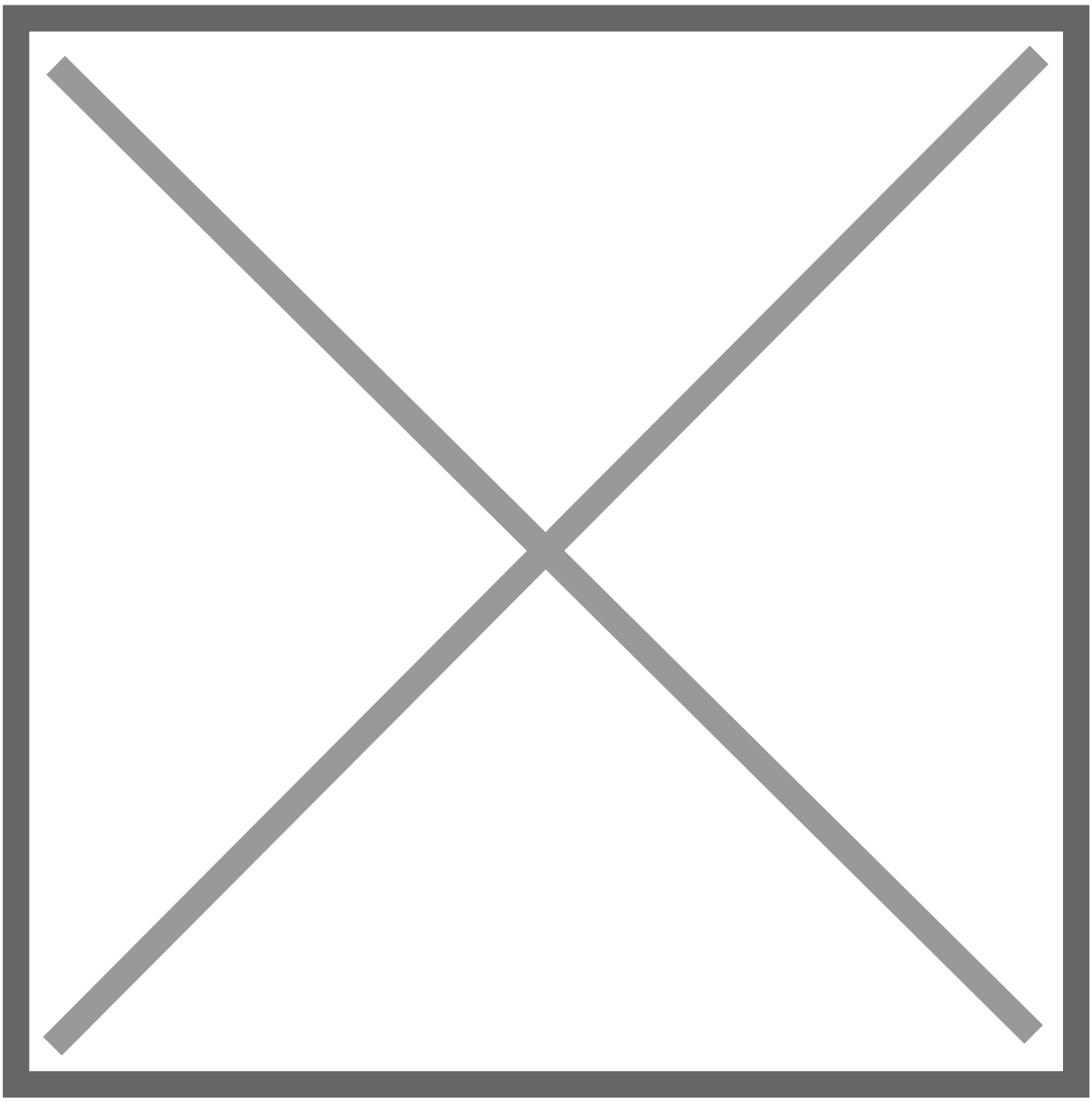
Weaponization

Next, let’s create a payload with Alteryx. We will introduce two importable file types and their pros and cons. Regardless of which file type is chosen, in order to make the phishing scenario as credible as possible to increase the success rate of client-side code execution, some familiarity with the software may be required. You definitely do not want to send an empty importable file to the victim, even if they do not know that Alteryx can be used for phishing, they will not run a workflow without any meaningful content.

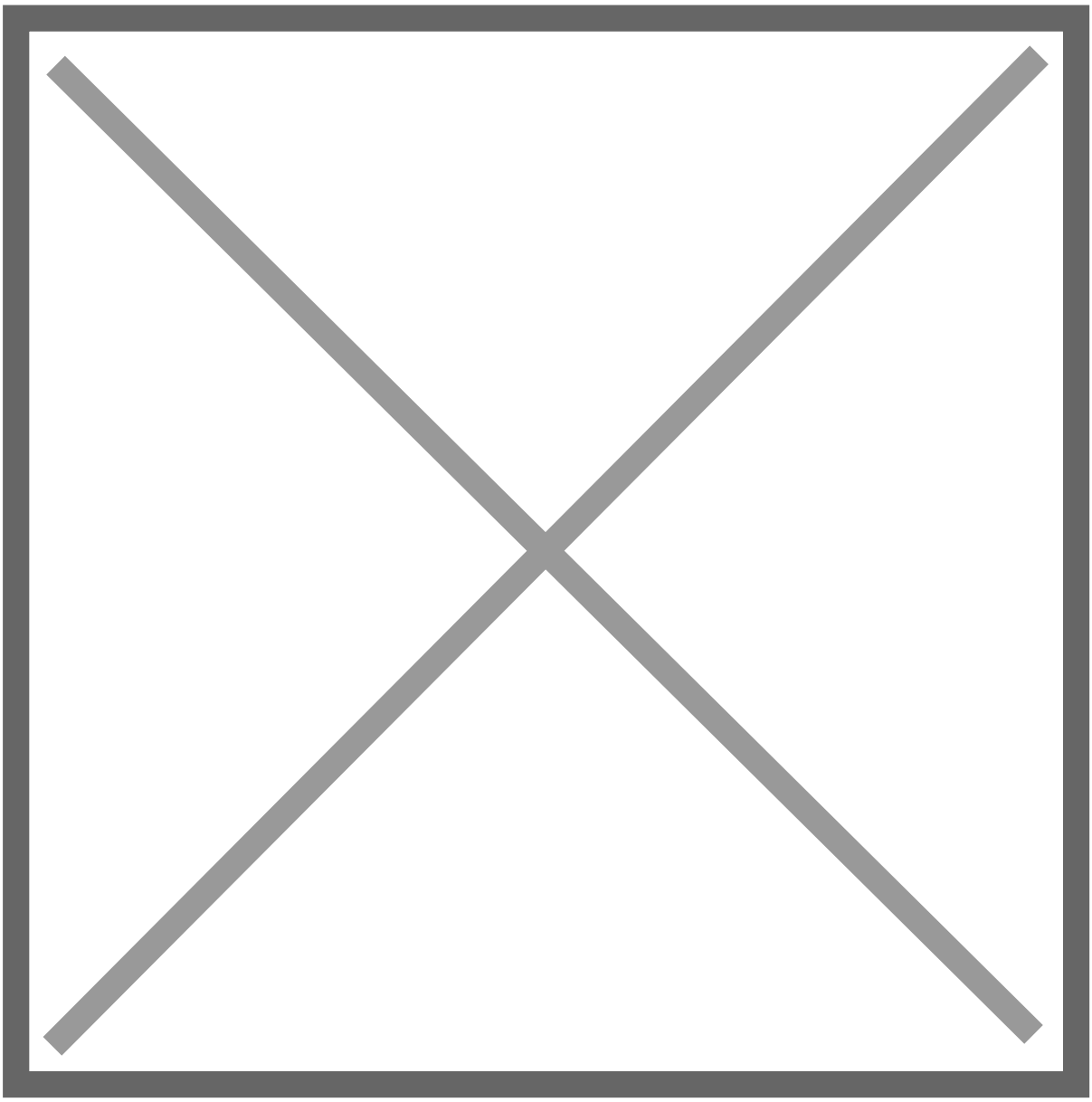
For demonstration purposes, we will not meticulously create a very professional workflow. We can open some built-in template workflows in the software, as shown in the figure below.



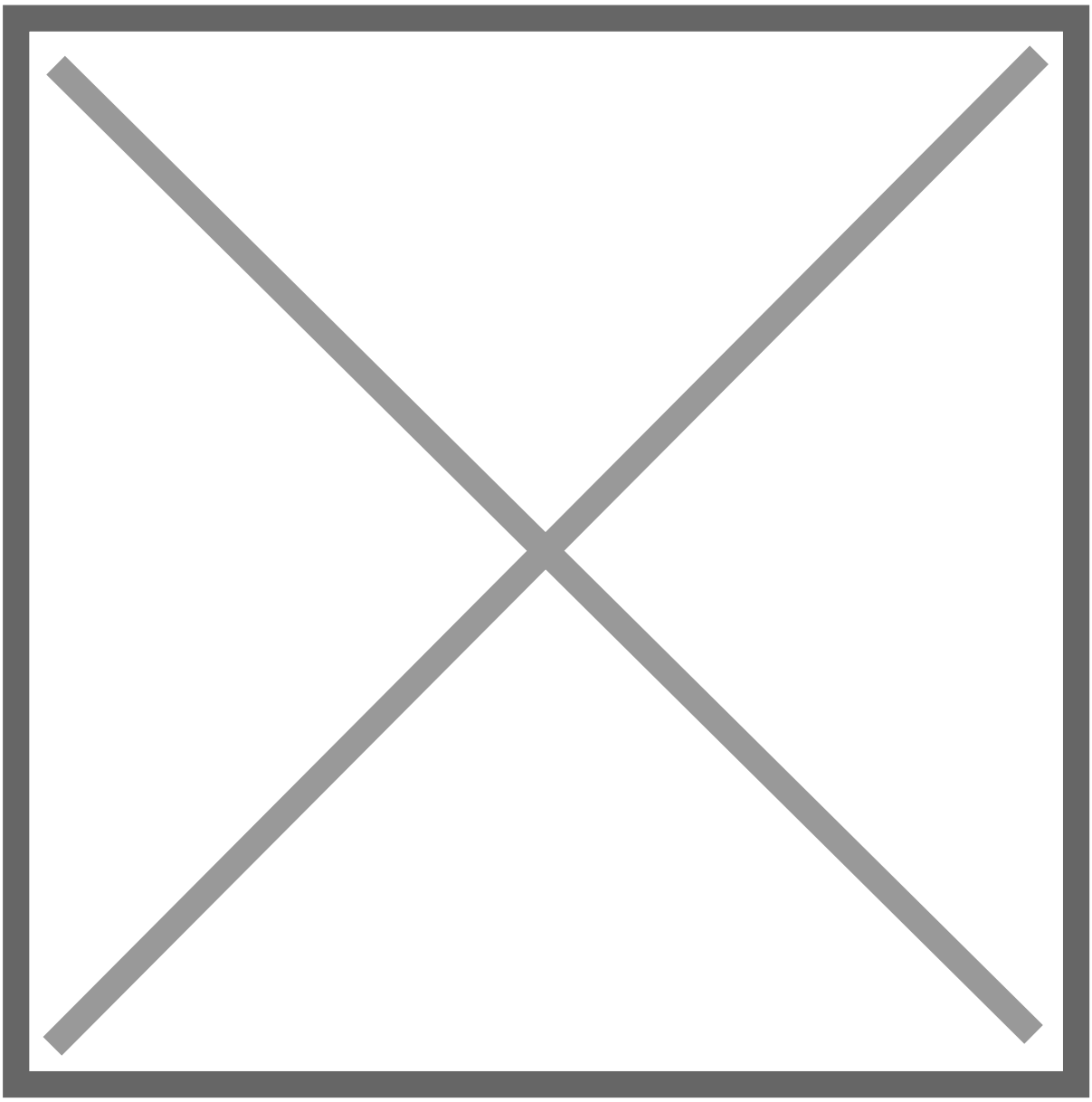
Alternatively, we can download one from the community, such as https://community.alteryx.com/t5/Weekly-Challenge/bd-p/weeklychallenge.



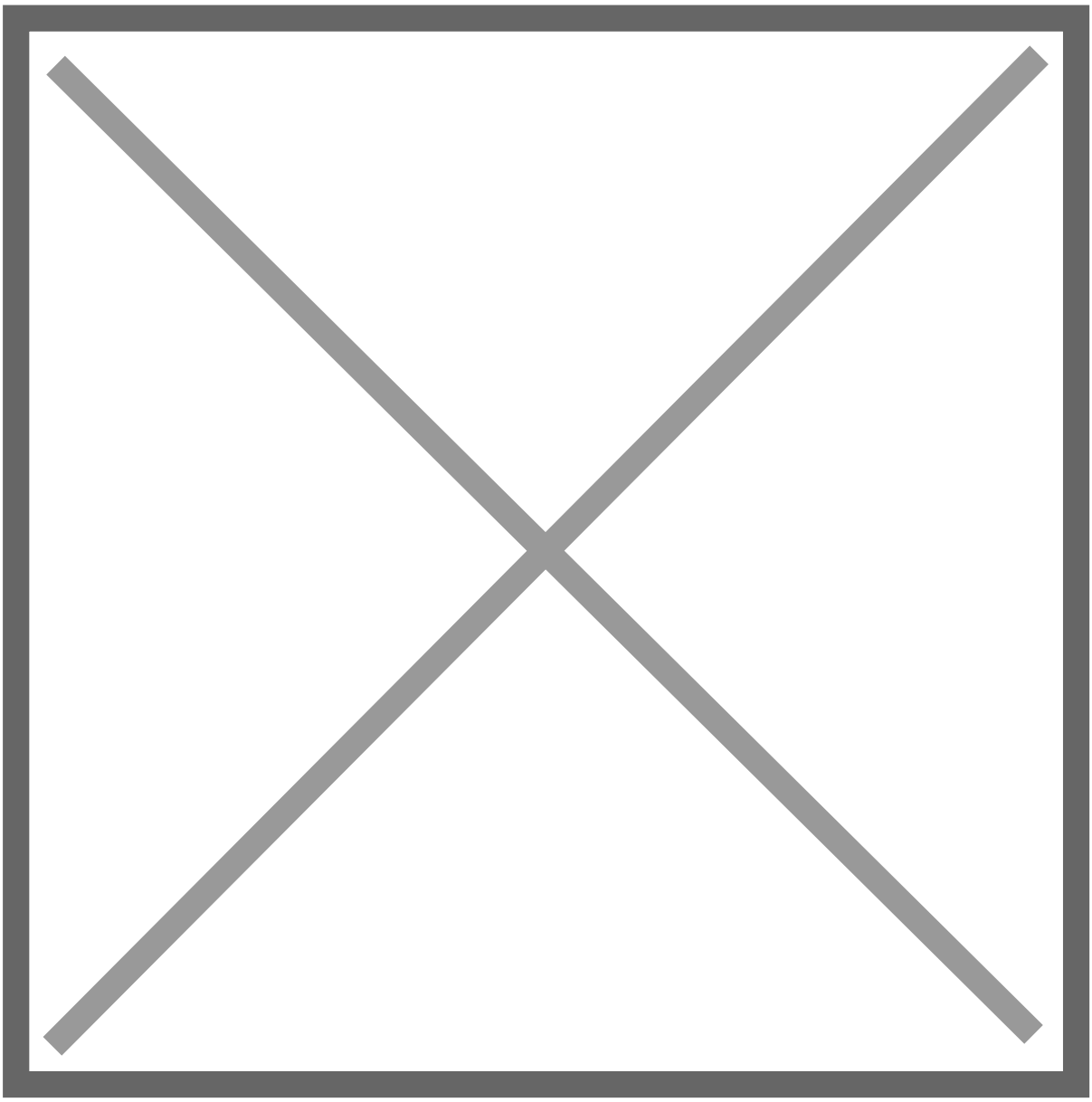
After loading a workflow, select the **Events** tab in the **Configuration** panel under the **Workflow** menu, and add a new event. There are multiple ways to trigger an event, such as **Before Run**, **After Run**, **After Run With Errors**, **After Run Without Errors**. Specify the command to be executed and its parameters, and save the workflow.



We can save the single workflow file (.yxmd), or export all associated assets to a package file (.yxzp).



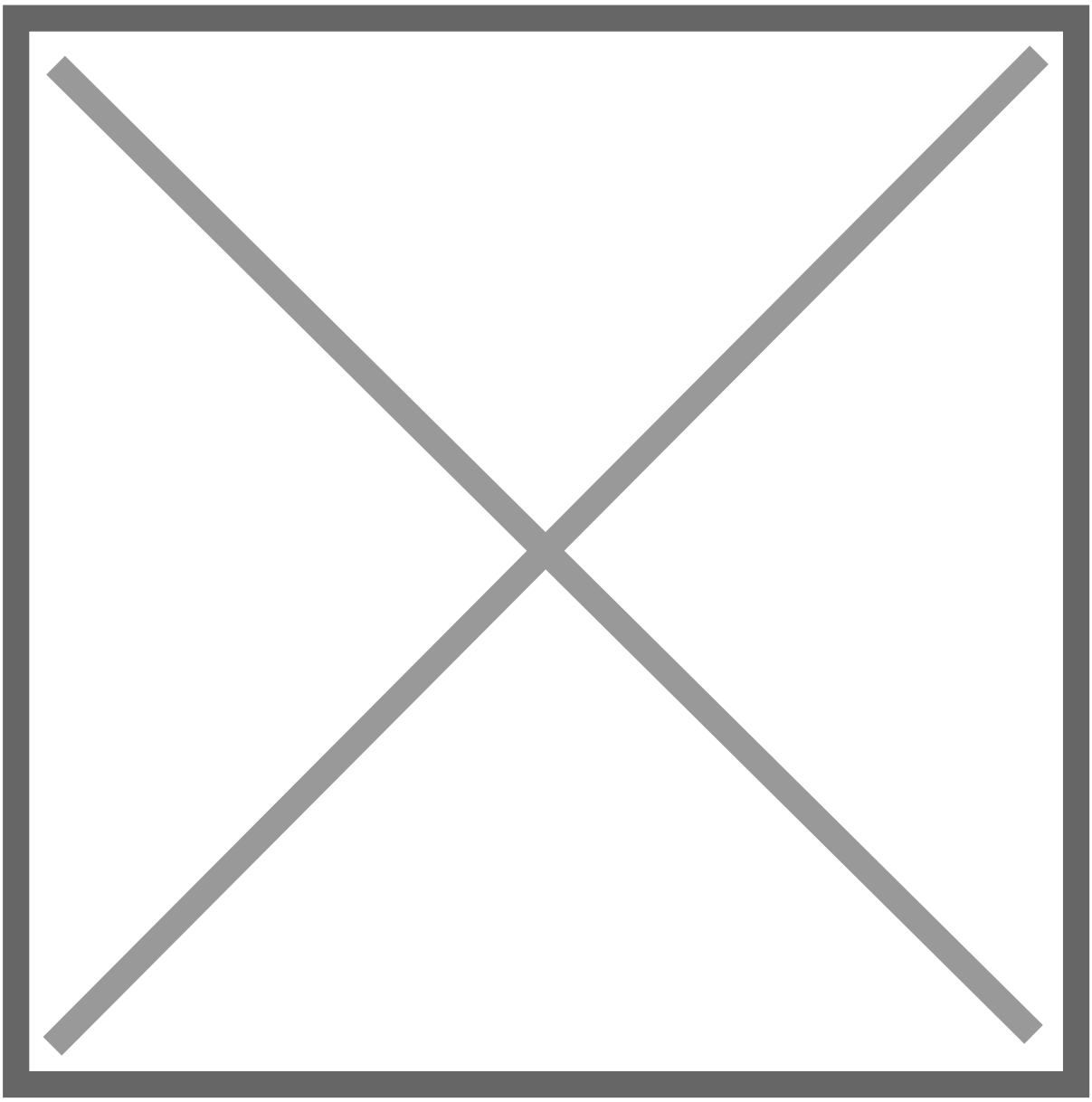
If choose to export all associated assets, make sure you select the program.



From the victim’s perspective, if they have installed Alteryx software, both .yxmd and .yxzp files can be double-clicked or imported within the software. So, what are the subtle differences and pros and cons between the two file types?

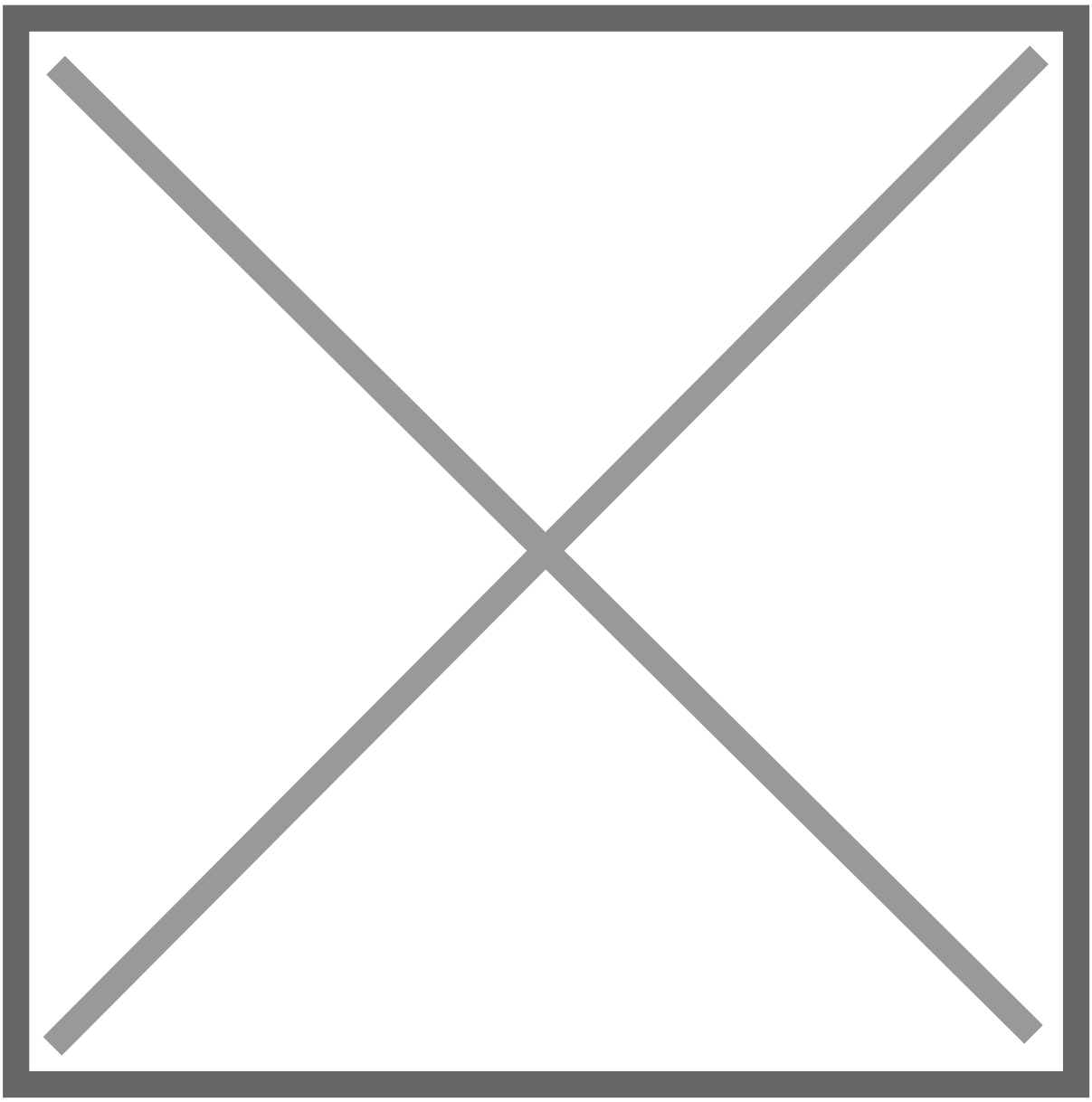
yxmd File

A .yxmd file is essentially an XML file, the program and command line are embedded in it.



When we double-click or import a yxmd file within the software, **there are no warnings or alerts. The victim will not be notified that the workflow file specifies commands or programs to be executed!**

Therefore, the victim can import and run a carefully crafted malicious workflow file without any prompts or warnings. However, more complex workflow files often come with some external assets, such as input data or macros. When importing a yxmd file, if external assets are missing, an error message will be displayed after running the workflow. However, if we set the code execution to happen before running the workflow, by the time the user notices the error messages, we have already obtained client-side code execution.



Pros:

1: No alert or warning

2: The user will not notice any embedded program or command

3: Simple to craft a malicious one

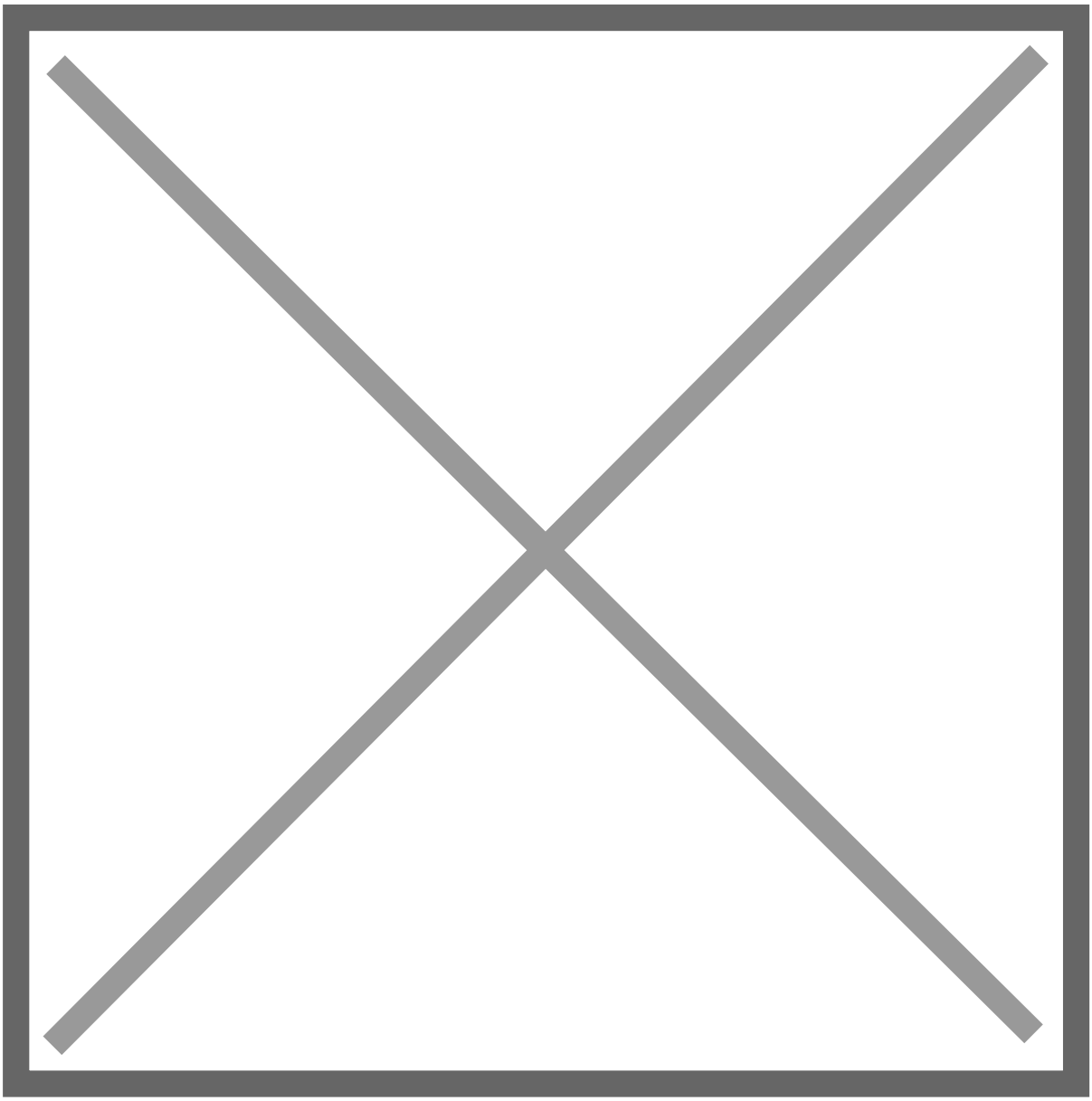
4: Looks very legitimate

Cons:

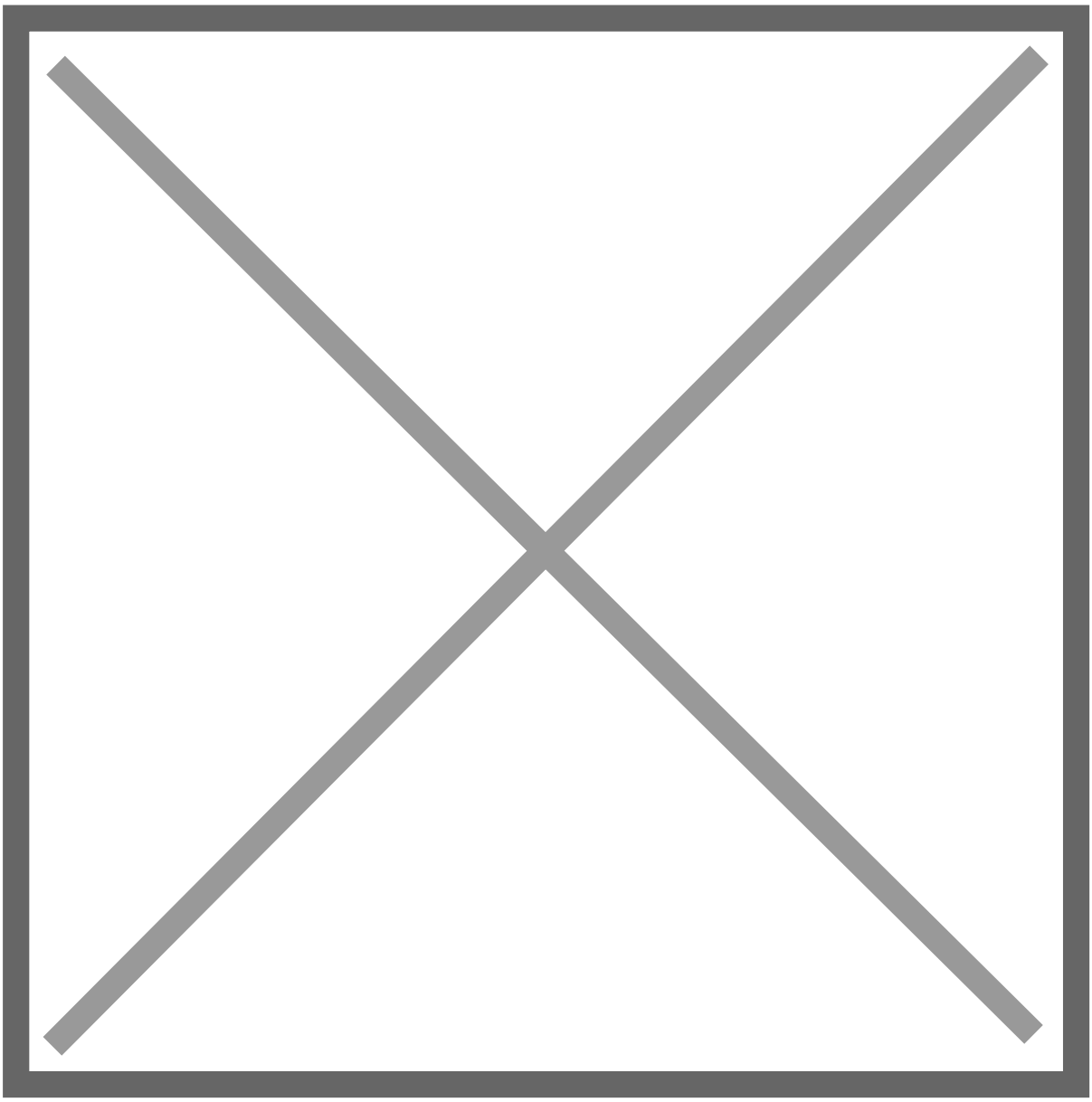
1: The context of the workflow should not be very complex.

yxzp File

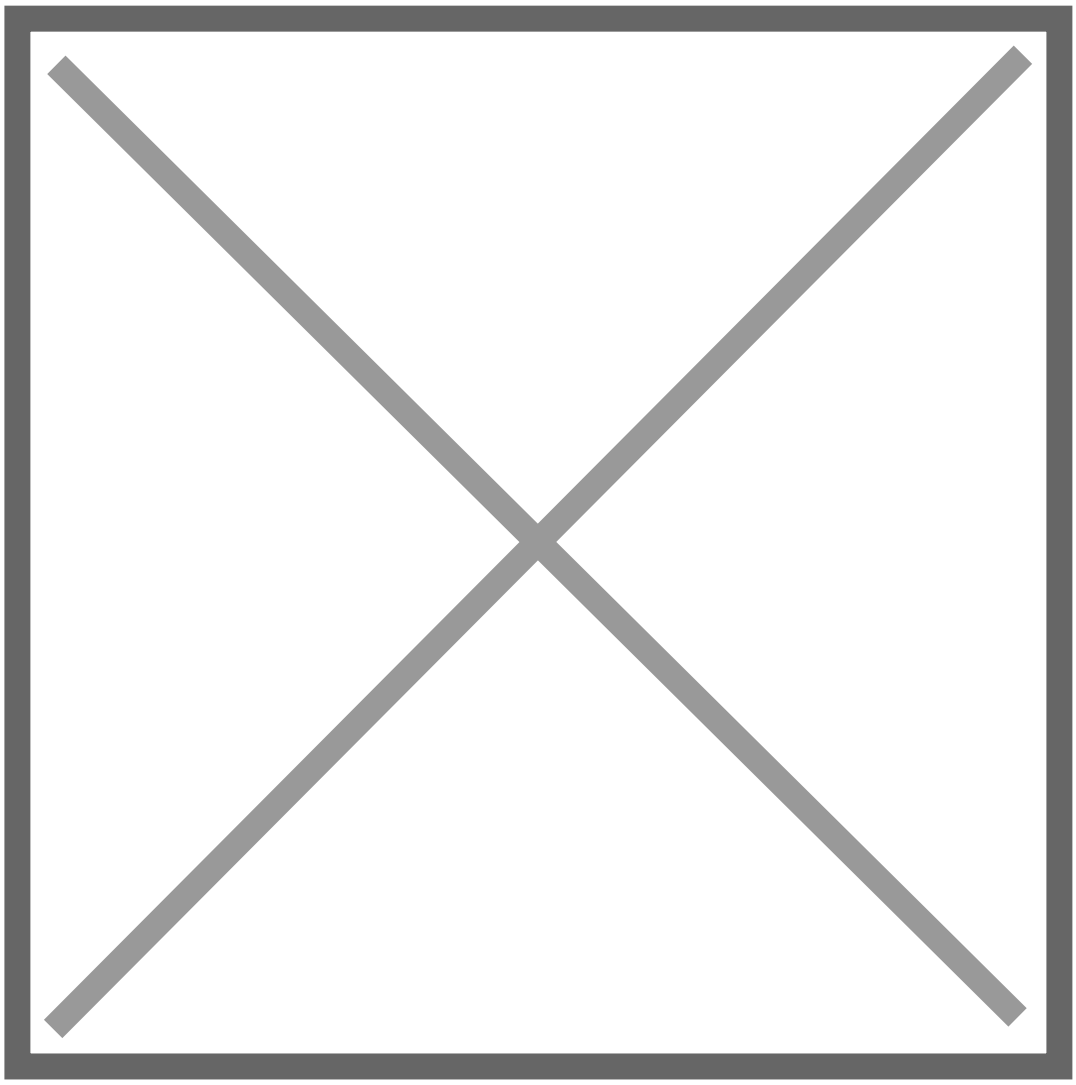
A .yxzp file is a package file, we can use 7-Zip to check its contained folders and files.



And we can find the embedded program within a package file by manually browsing it.



By double-clicking on this .yxzp file or importing it within the software, the victim can see all contained files, including the program we embedded in it. We’d better name the program as legitimate as possible.



The following process is similar. Since the .yxzp file contains all the necessary assets, there will be no error messages due to missing assets.

Pros:

1: No alert or warning

2: The package contain all assets, we can craft a more complex workflow

3: Looks very legitimate

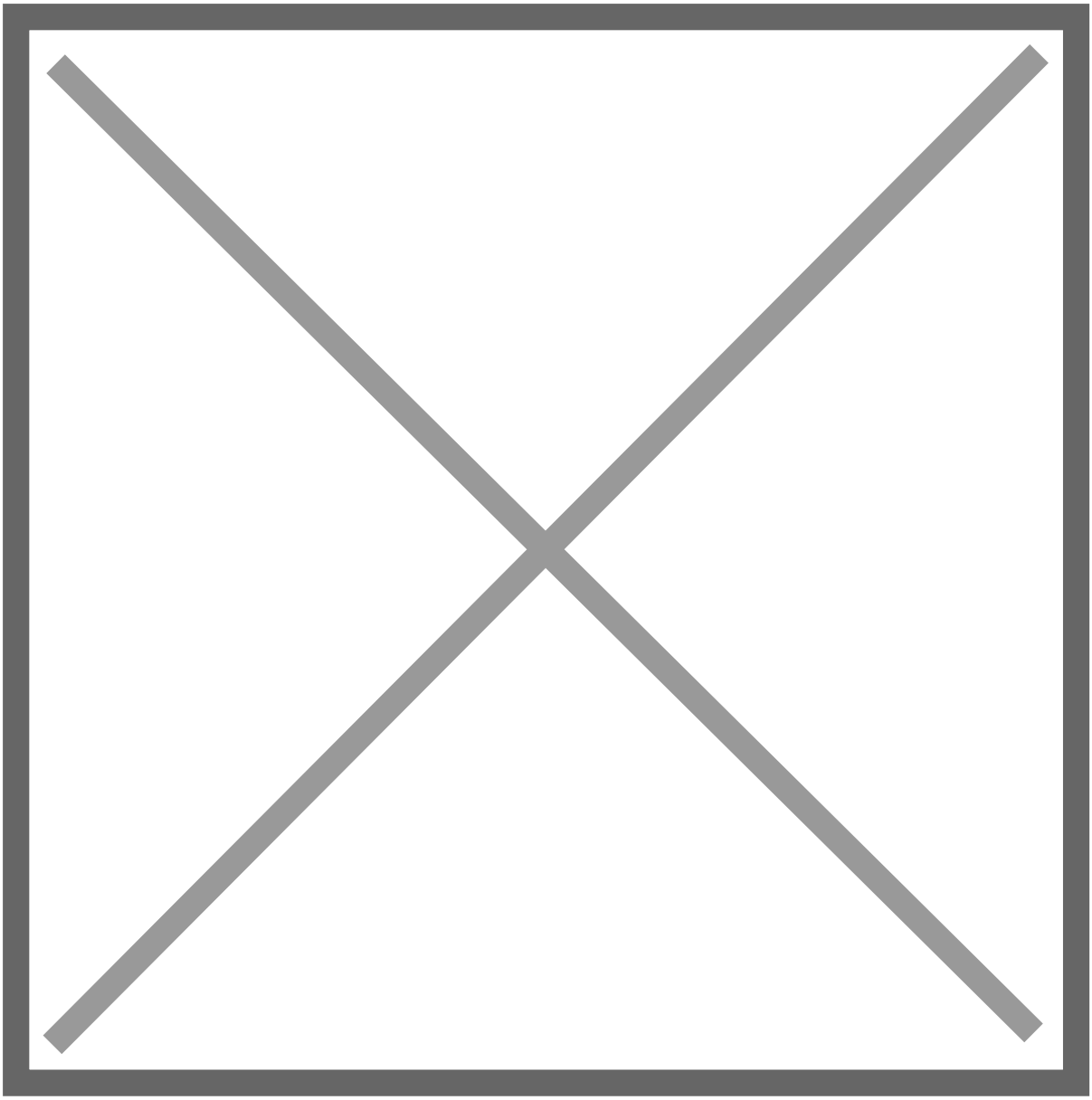
Cons:

1: The user can notice the embedded program

Delivery

For Red Team Operators

For red team operators who are conducting a red team operation, if the target is an enterprise in accounting, finance, data analysis, and some other industries, or if they know that the software is indeed widely used in the target enterprise, this phishing attack can be very effective. For example, the Big Four accounting firms widely use Alteryx software.



A possible phishing pretext:

Dear B company,

Hello! I am a representative from A company and I would like to discuss the possibility of collaborating with your company on the xxx business.

In this email, I would like to present a demonstration that we have prepared specifically for this business, which will be attached in an Alteryx workflow file. This workflow file will allow you to have a better understanding of our business process and provide you with a comprehensive overview.

If you are interested, we can arrange a time to discuss more details. If you wish to take a look at and run the workflow file, please ensure that you have installed the Alteryx software. If you have any questions or requirements, please feel free to contact me at any time.

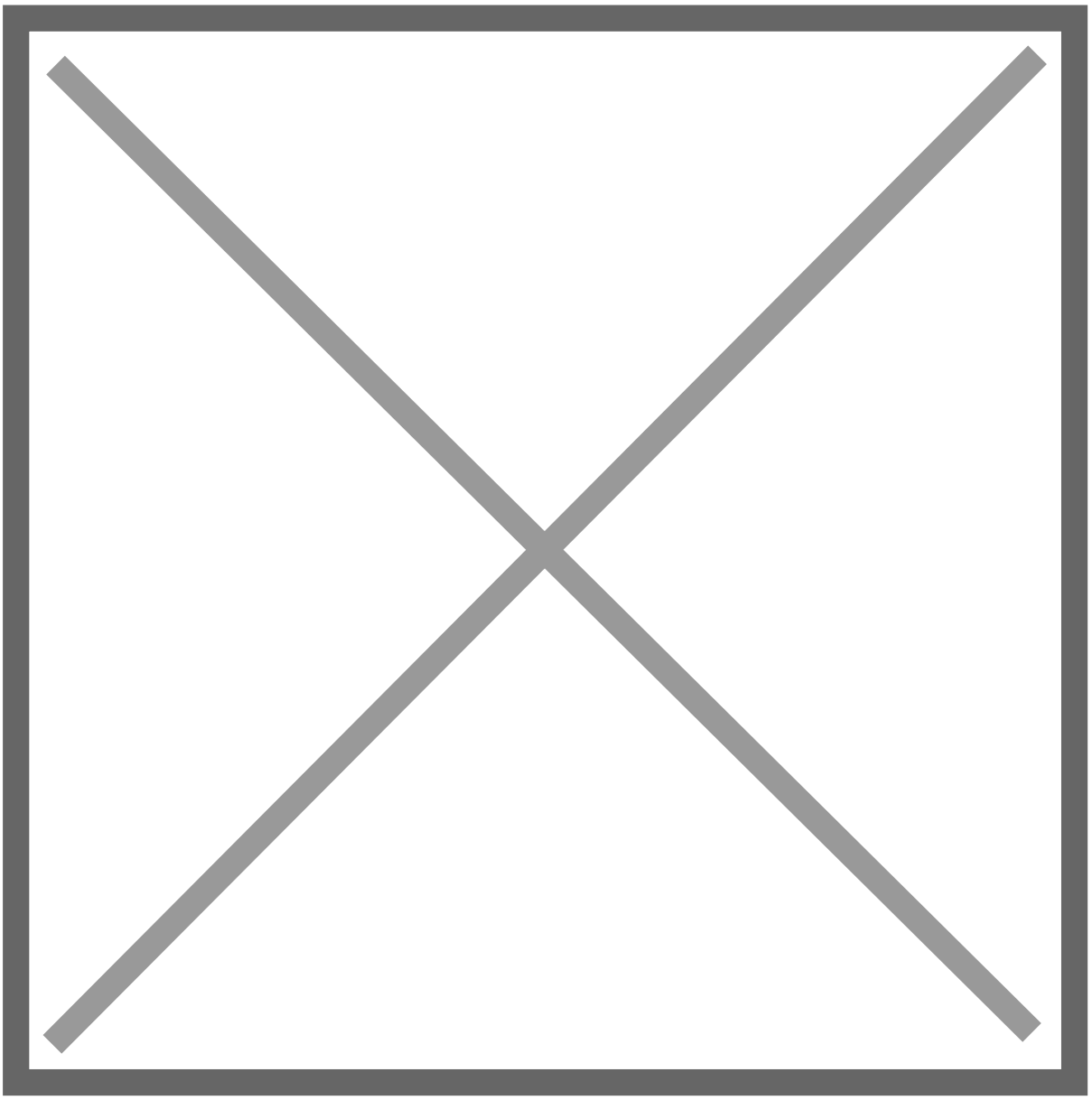
Thank you for your time!

Best regards,

Representative of A company

How may TAs abuse it?

Considering that threat actors (TAs) may not have very specific targets, they may just want to find as many victims as possible and get control of their hosts. So, what will they do once they know about this phishing vector? For example, Alteryx software has official community support, and many software users discuss the solutions to Weekly Challenges in the community. TAs can pretend to be software users who have completed the weekly challenges, post their own answers for other community members to download and run. As this community is a place where software users gather to discuss, a workflow containing malicious programs will quickly spread.



Detection

File

.yxmd file

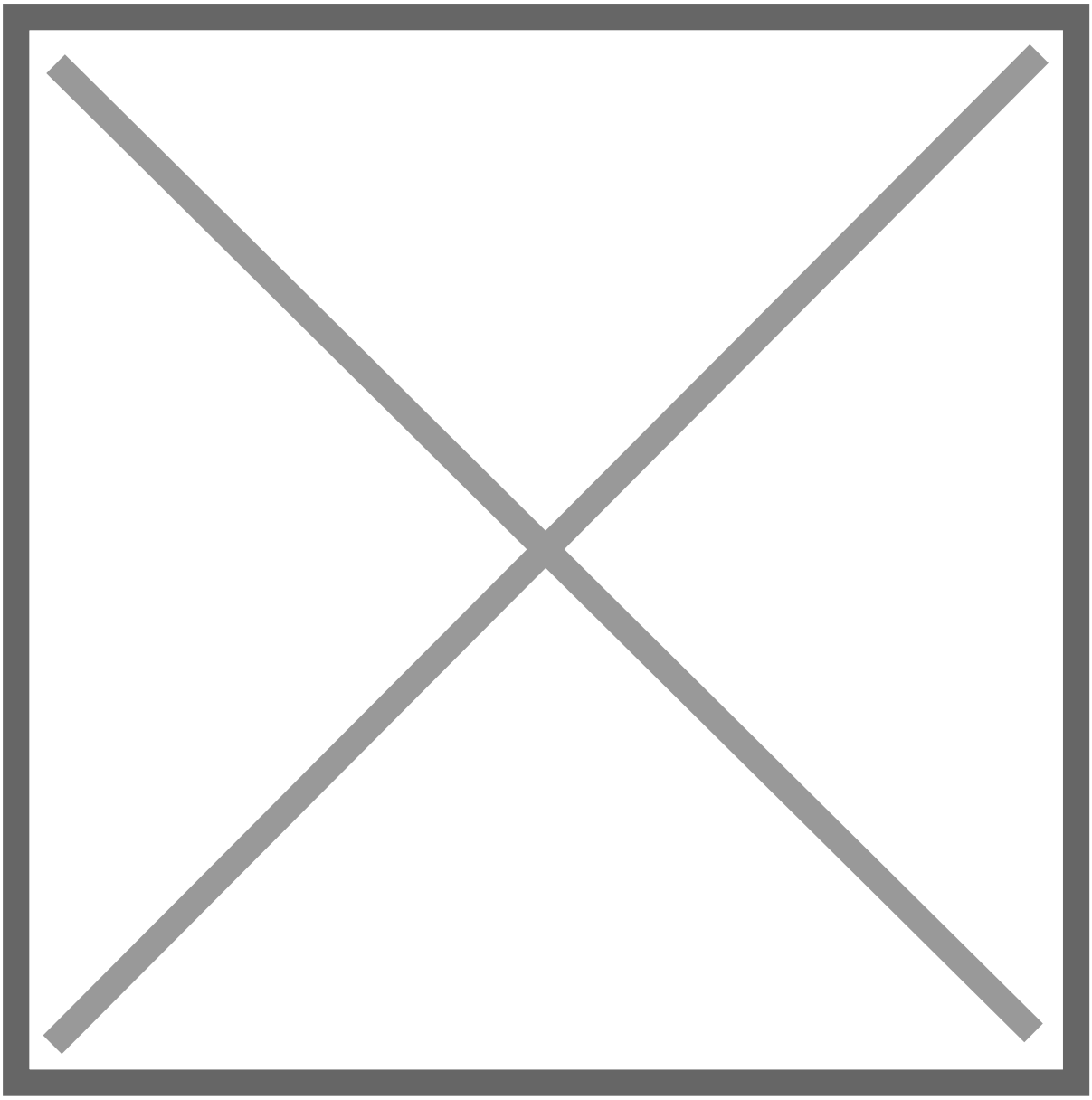
Inspect <Event> section

.yxzp file

Inspect all embedded files

Runtime

If the program embedded in the workflow is run, process **AlteryxGui.exe** will fork a child process **AlteryxEngineCmd.exe**, and the embedded program will be a child process of **AlteryxEngineCmd.exe**.



References

https://techcrunch.com/2022/07/22/microsoft-office-macros-blocked-default/

https://learn.microsoft.com/en-us/deployoffice/security/internet-macros-blocked

https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/attack-surface-reduction-rules-reference?view=o365-worldwide

https://big4accountingfirms.com/the-blog/3-technologies-must-learn-big-4-accounting/

https://www.alteryx.com/customer-center/kpmg-case-study

https://community.alteryx.com/t5/Weekly-Challenge/bd-p/weeklychallenge

https://help.alteryx.com/20223/designer/run-command-tool

https://help.alteryx.com/20223/designer/build-workflows#:~:text=A%20workflow%20consists%20of%20connected,workflow%20select%20File%20%3E%20New%20Workflow

https://chat.openai.com

https://help.alteryx.com/20223/designer/alteryx-file-types

Revision #1
Created 2024-02-28 18:25:53 UTC by winslow
Updated 2024-02-28 18:26:15 UTC by winslow