

Background Info

Phishers unleash simple but effective social engineering techniques using PDF attachments. If you are creating a PDF document, you can bind other types of files to it as an attachment. One file you can attach is an EXE application. If the PDF contains instructions for a small application, binding the EXE to the PDF can give a user both files at once.

Configuration

To perform a PDF based attack, you must first select an attack template that contains a malware simulation (e.g. mixed template or file based template). In the next step you can "hide" the malware simulation within the scenario settings of the respective template in a PDF. Please go to the settings of the template in the lower area and select the PDF option in the dropdown:

Geo Location
 Social Network
 Proxy

Success Action: Data Submit

Collect Data: Full

Double Barrel Attack

Uri Shortener: N/A

Login Regexp: [] [Insert]

Password Regexp: [] [Insert]

File Type: PDF document

Upload PDF File: Choose File No file chosen

PDF Custom Name: [] .zip

Save

Security Update

A major security update has been released in the new versions of Adobe Acrobat Reader. Since Aug 2020 builds it is not possible to open the attached "-.exe" files. More info here:

<https://helpx.adobe.com/acrobat/using/attachments-security-risks-reader-acrobat.html>

From:

<https://wiki.lucysecurity.com/> - **LUCY**

Permanent link:

https://wiki.lucysecurity.com/doku.php?id=pdf_attacks

Last update: **2020/09/07 12:06**

