Background Info about Archiving Options

LUCY allows so-called file based attacks which allow the administrator to combine a phishing simulation with a malware simulation. The malware simulation can be attached to the mail or inserted into a phishing webpage where it may be downloaded by the recipient.

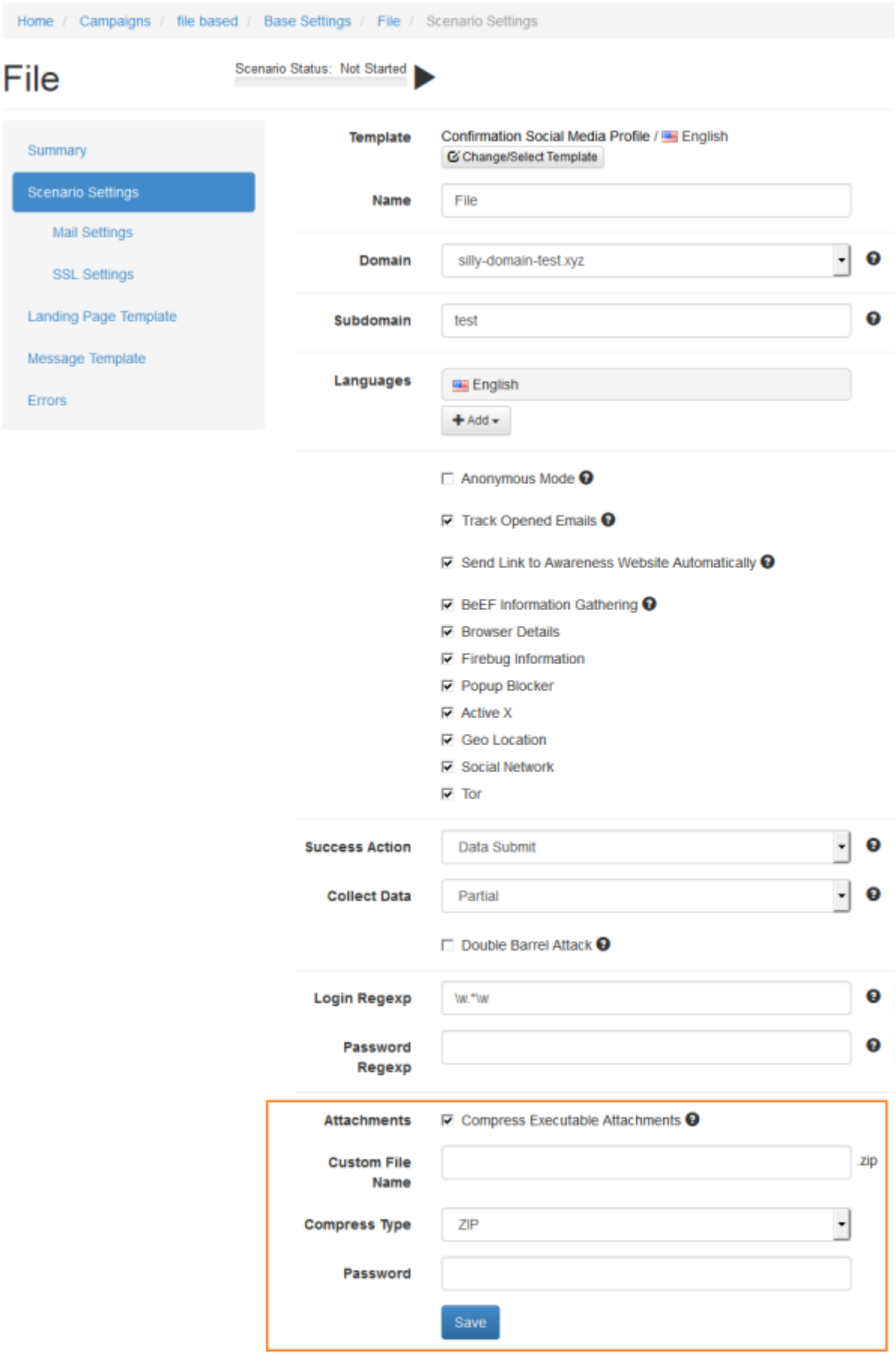
To help protect the computer, mail and web filters in most cases do not allow you to receive files of certain types (such as .exe files) as attachments or within a download, because of their potential for introducing a virus into the computer. Certain mail clients (like Outlook) also block these files by default. So-called Level 1 files (like exe, bat, vbs etc.) cannot be sent in plain form. Otherwise, they will get filtered. LUCY allows the administrator to archive those files (like *.zip or *.rar files). But also just placing them in an archive is not sufficient in most cases. Therefore we also offer the administrator in LUCY > 3.1 to set a password for the archive. This makes it impossible for any filter to analyze the content. If encrypted files are not rejected on a gateway level, this offers the LUCY admin to ensure that the file-based simulations can be downloaded or attached in the simulation.

Configuration

In order to rename, archive and set a password for a file-based attachment or download you can go to the scenario settings of your specific scenario and then at the bottom you can:

- Enable archiving of the file
- Give the archive a custom name
- Set a password for the archive

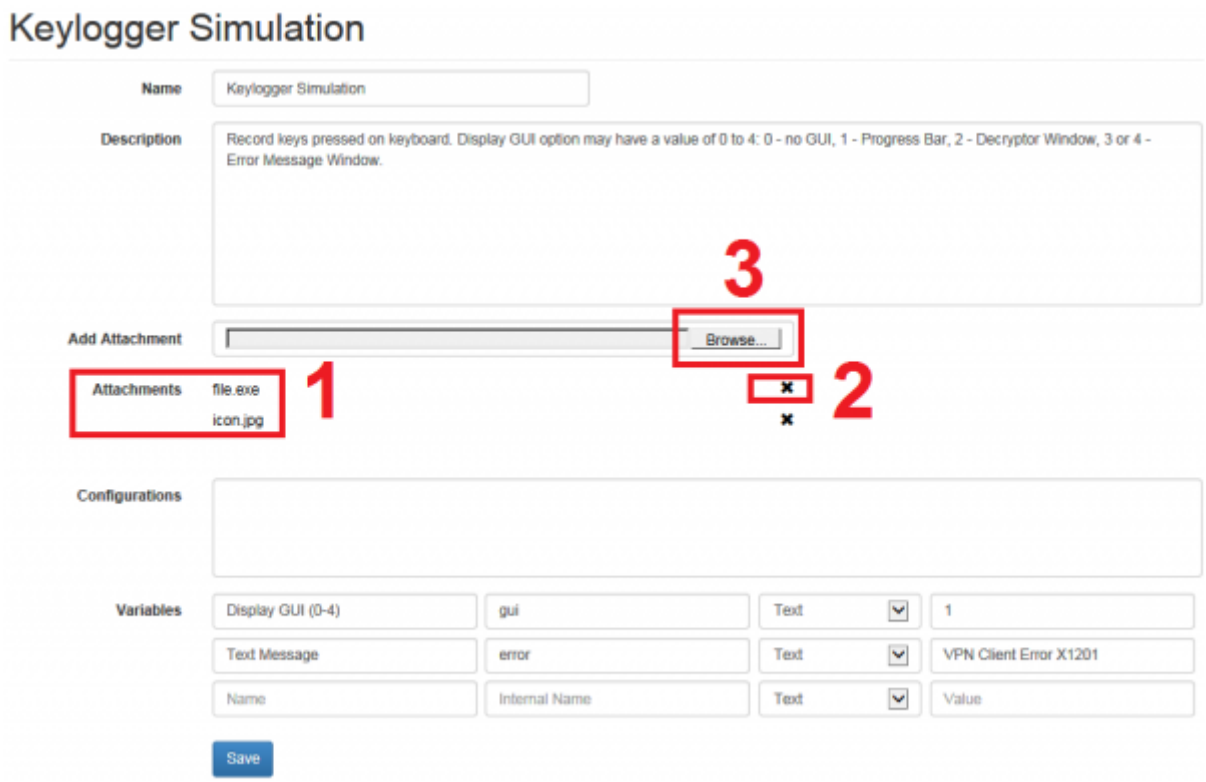
Please note that the compression only applies for Level 1 file types (like .exe) and not Level 2 file types (like .docx, .mp3 etc).


Home / Campaigns / file based / Base Settings / File / Scenario Settings
File
Scenario Status: Not Started
Summary
Scenario Settings
Mail Settings
SSL Settings
Landing Page Template
Message Template
Errors
Template
Confirmation Social Media Profile / English
Change/Select Template
Name
File
Domain
silly-domain-test.xyz
Subdomain
test
Languages
English
Add
Anonymous Mode
Track Opened Emails
Send Link to Awareness Website Automatically
BeEF Information Gathering
Browser Details
Firebug Information
Popup Blocker
Active X
Geo Location
Social Network
Tor
Success Action
Data Submit
Collect Data
Partial
Double Barrel Attack
Login Regexp
\w.*\w
Password Regexp
Attachments
Compress Executable Attachments
Custom File Name
.zip
Compress Type
ZIP
Password
Save

Change the file name of the executable or word file

In LUCY < 3.2 you can change the file name of the executable or word file by:

1) Downloading the original file within the generic file-based template section and locally rename it to the desired file name 2) Deleting the original file name on LUCY by clicking on "X" (e.g. delete "file.exe") 3) Uploading the file with the modified file name



Change the layout of the word file

In LUCY < 3.2 you can change the layout of the word file by:

1) Downloading the original word file within the generic file-based template section and locally change the design to the desired layout 2) Deleting the original file name on LUCY by clicking on "X" (e.g. delete "info.doc") 3) Uploading the file with the modified file name 4) Use the word modified word file in your campaign

Change the file type (e.g. use an excel instead of word)

In LUCY < 3.2 you can change the file type by simply copying the macro from the word file to the desired file format (e.g. Excel) and upload it back to LUCY as a generic file template.

Change the file icon

If you want to change the icon of the executable, you need to manually do that using a free tool (e.g. http://www.angusj.com/resourcehacker/, https://github.com/electron/rcedit/releases, http://winrun4j.sourceforge.net/ etc.). Those tools allow you to download the *.exe, set a custom icon and then download it back to LUCY. After LUCY 3.8 we will provide the possibility to change the icon within the UI.

Issues with files that get filtered by AV or any other security software

Our malware simulations are non-malicious and are intended only for educational use. We can ensure that they are non-persistent (run only in memory) and free of any malicious code. On request we also allow clients to access the source code for each malware simulation. Still, we noticed in the past that AV vendors or content filter added virus signatures for certain file based simulations from LUCY. We are working together with those vendors to remove them from their signature lists. But we cannot guarantee that we cover all products. Therefore we kindly ask our clients to report us if our malware simulations are getting filtered (send us a mail with the vendors signature ID to info@lucysecurity.com).

From:
https://wiki.lucysecurity.com/ - **LUCY**

Permanent link:
https://wiki.lucysecurity.com/doku.php?id=set_a_password_for_the_archive_in_file_based_attacks_or_change_the_file_name&rev=1558540306

Last update: **2019/07/25 12:51**