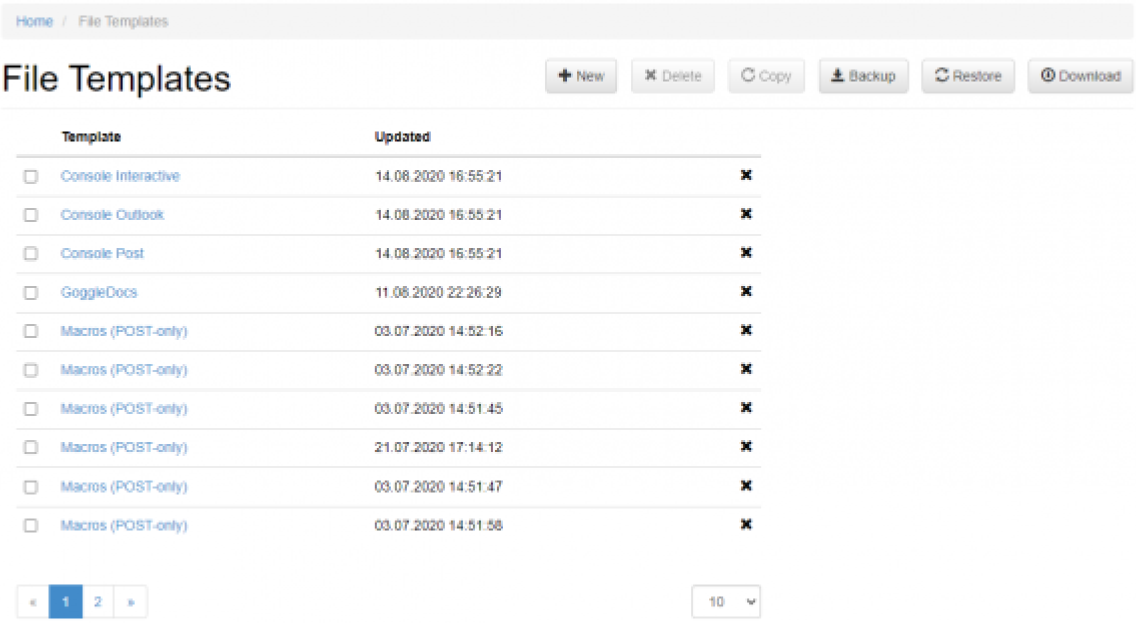
FILE BASED ATTACK SIMULATION TEMPLATES

LUCY can compile different custom Malware Simulations:



File Templates

	Template	Updated	
□	Console Interactive	14.08.2020 16:55:21	✖
□	Console Outlook	14.08.2020 16:55:21	✖
□	Console Post	14.08.2020 16:55:21	✖
□	GoggleDocs	11.08.2020 22:26:29	✖
□	Macros (POST-only)	03.07.2020 14:52:16	✖
□	Macros (POST-only)	03.07.2020 14:52:22	✖
□	Macros (POST-only)	03.07.2020 14:51:45	✖
□	Macros (POST-only)	21.07.2020 17:14:12	✖
□	Macros (POST-only)	03.07.2020 14:51:47	✖
□	Macros (POST-only)	03.07.2020 14:51:58	✖

Each file type can be modified (layout, filetype, name) before using it in a campaign. Currently, LUCY comes with the following file types:

Setting Name	**Description**	**Success action**	**Preferable delivery method**
Console Interactive	This tool allows you to establish a reverse HTTP/HTTPS channel to LUCY. Once the file has been executed, you can see the session in “Sessions”. The tool only runs in the memory (called “file” in Process View). After the termination, the session can no longer be established. You can click on the IP and start executing commands within the Windows shell. The output should appear after a few seconds automatically. This Tool only works with Windows 7/8 in combination with IE and Firefox. More background info can be found here.	File download	Landing page
Console Outlook	Execute commands and send the output back via Outlook (access Outlook hidden via MAPI) to a predefined email address. It also has the ability as a PoC to send back the subject line from last received email in Outlook.	File download	Landing page

Setting Name	**Description**	**Success action**	**Preferable delivery method**
Console post	Execute your commands within the Windows shell and send back the output to LUCY. This tool allows you to use a limited set of commands. Some commands in Windows are not executable. They are built into the command line (Example of command with executable: whoami). If you need to use a command which is a built-in command line, then you should call cmd directly (example for requesting the directory content: "cmd /c dir"). Here a list of possible commands.	File download	Landing page
Console (POST-only)	This console program template just pings back to Lucy when user opens the executable file, without collecting any data.	File download/File open	Landing page
Excel Macros (GET-only)	This macros template just pings back to Lucy when user opens the document, without sending and collecting any data. *Note*: In the campaign settings for the "Get" macro, you need to select type "Click" in "Success action" for a correct statistic.	Click/File download/File open	Email*/Landing page
Excel Macros (GET-only using IE)	This macros template just pings back to Lucy when user opens the document, without sending and collecting any data. *Note*: In the campaign settings for the "Get" macro, you need to select type "Click" in "Success action" for a correct statistic.	Click/File download/File open	Email*/Landing page
Excel Macros (GET-only using IE for tracking file opening)	This macros template just pings back to Lucy when a user opens the document, without sending and collecting any data. To use this template, File Open must be set as Success Action in the phishing scenario settings. *Note*: In the campaign settings for the "Get" macro, you need to select type "Click" in "Success action" for a correct statistic.	Click/File download/File open	Email*/Landing page
Excel Macros (GET-only using WinHTTP)	This macros template just pings back to Lucy when a user opens the document, without sending and collecting any data. Supports WinHTTP proxy. Important notice! This simulation malware template might be blocked by end-user antivirus software. Please use a template without WinHTTP proxy support if your company does not have a proxy. *Note*: In the campaign settings for the "Get" macro, you need to select type "Click" in "Success action" for a correct statistic.	Click/File download/File open	Email*/Landing page

Setting Name	Description	Success action	Preferable delivery method
Excel Macros (GET-only using WinHTTP for tracking file opening)	This macros template just pings back to Lucy when a user opens the document, without sending and collecting any data. To use this template, File Open must be set as Success Action in the phishing scenario settings. Supports WinHTTP proxy. Important notice! This simulation malware template might be blocked by end-user antivirus software. Please use a template without WinHTTP proxy support if your company does not have a proxy. *Note*: In the campaign settings for the "Get" macro, you need to select type "Click" in "Success action" for a correct statistic.	Click/File download/File open	Email*/Landing page
Excel Macros (POST-only using IE)	This macros template just pings back to Lucy when user opens the document, without collecting any data.	File download/File open	Email*/Landing page
Excel Macros (POST-only using WinHTTP)	This macros template just pings back to Lucy when user opens the document, without collecting any data. Supports WinHTTP proxy. Important notice! This simulation malware template might be blocked by end-user antivirus software. Please use a template without WinHTTP proxy support if your company does not have a proxy.	File download/File open	Email*/Landing page
GoggleDocs	This macros template just pings back to Lucy when user opens the document, without collecting any data.	File download	Email*/Portable device (USB)
HTML (Redirect)	This HTML template, when opened, redirects to the scenario phishing website without transferring any data. It is used for a Portable Media Attack (USB) or File Attack campaign.	File download	Landing page
HTML (Redirect Receipt)	This HTML template, when opened, redirects to the scenario phishing website without transferring any data. It is used for a Portable Media Attack (USB) or File Attack campaign.	File download	Landing page
Keylogger	Record keys pressed on keyboard.	File download/Data submit	Email*/Landing page
Macros	Run console commands through Office file that contains a Macro.	File download/File open	Email*/Landing page
Macros (GET-only using IE)	This macros template just pings back to Lucy when a user opens the document, without sending and collecting any data. *Note*: In the campaign settings for the "Get" macro, you need to select type "Click" in "Success action" for a correct statistic.	Click/File download/File open	Email*/Landing page
Macros (GET-only using IE for tracking file opening)	This macros template just pings back to Lucy when a user opens the document, without sending and collecting any data. *Note*: In the campaign settings for the "Get" macro, you need to select type "Click" in "Success action" for a correct statistic.	Click/File download/File open	Email*/Landing page

Setting Name	Description	Success action	Preferable delivery method
Macros (GET-only using WinHTTP)	This macros template just pings back to Lucy when a user opens the document, without sending and collecting any data. Supports WinHTTP proxy. Important notice! This simulation malware template might be blocked by end-user antivirus software. Please use a template without WinHTTP proxy support if your company does not have a proxy. *Note*: In the campaign settings for the "Get" macro, you need to select type "Click" in "Success action" for a correct statistic.	Click/File download/File open	Email*/Landing page
Macros (GET-only using WinHTTP for tracking file opening)	This macros template just pings back to Lucy when a user opens the document, without sending and collecting any data. Supports WinHTTP proxy. Important notice! This simulation malware template might be blocked by end-user antivirus software. Please use a template without WinHTTP proxy support if your company does not have a proxy. *Note*: In the campaign settings for the "Get" macro, you need to select type "Click" in "Success action" for a correct statistic.	Click/File download/File open	Email*/Landing page
Macros (POST-only)	It will do a simple http or https connection back to LUCY upon opening which will notify the LUCY administrator that the word has been opened and the Macro has been activated. The Macro can be used in any file-based or mixed attack scenarios either as a mail attachment or as a file that can be downloaded from a landing page created by LUCY.	File download/File open	Email*/Landing page
Macros (POST-only using IE)	This macros template just pings back to Lucy when a user opens the document, without collecting any data.	File download/File open	Email*/Landing page
Macros (POST-only using WinHTTP)	This macros template just pings back to Lucy when a user opens the document, without collecting any data. Supports WinHTTP proxy. Important notice! This simulation malware template might be blocked by end-user antivirus software. Please use a template without WinHTTP proxy support if your company does not have a proxy.	File download/File open	Email*/Landing page
Malware Testing Toolkit	Test if the target system is vulnerable to miscellaneous malware technologies.	File download/File open	Email*/Portable device (USB)
Malware Testing Toolkit Lite	Test if the target system is vulnerable to miscellaneous malware technologies. The Lite version of the tool does not include the Mimikatz app and IE PassView utility.	File download/File open	Email*/Portable device (USB)
Microphone	Get audio recording from the microphone.	File download/Data submit	Portable device (USB)

Setting Name	Description	Success action	Preferable delivery method
Ransomware (Screen Locker)	Will lock the PC screen and ask the user to enter a password that can be set in the backend. The idea is to have the user call some helpdesk to ask for the password to have a better learning effect.	File download/Data submit	Email*/Portable device (USB)
Recent Documents	Send back a predefined number of documents listed in the recent doc cache to LUCY.	File download/Data submit	Email*/Portable device (USB)
Screen Recorder	Records screenshots and tries to access the webcam to record a few seconds as a PoC.	File download/Data submit	Email*/Portable device (USB)
SVG (Redirect)	This SVG template, when opened, redirects to the scenario phishing website without transferring any data.	File download/File open	Email*/Portable device (USB)

*Please note that there is a high probability that file attacks delivered by email will be blocked on the mail server level by security policies. Procedures for this type of simulation needs to be performed by admins beforehand to ensure that emails will not get blocked by filters.