

LUCY allows you to create files that can be stored on removable media devices (CD, USB, DVD, SD Card, etc.). The most popular is an attack using USB sticks. But keep in mind that this template works for all other variations of removable media types as well.

## Background Info about Portable Media Attacks

At the moment, there are three popular methods that malicious applications use to infect USB flash drives:

**Simple file copy method:** With this method, a malicious application that is installed on an infected computer simply makes copies of itself to all storage devices that are attached to the infected computer. With this method, a malicious file is often named with a sensational filename to lure a victim into launching the file and causing malicious code to be executed. Quite often there are familiar file icons such as Microsoft Windows icons for videos and images that are used to trick unsuspecting victims into thinking that an executable file is a harmless image or video. This infection method requires that the victim manually execute the malicious file from their computer to become infected.

**AutoRun.inf modification method:** Microsoft Windows and some other operating systems have a functionality that is called "AutoRun" (sometimes also referred to as Autoplay). AutoRun functionality is basically designed to perform some actions that are automatically executed when removable media is inserted or removed from a computer. On Microsoft Windows platforms, "autorun.inf" is the file that contains instructions for the AutoRun functionality. The autorun.inf file can instruct AutoRun to use a certain type of icon; add menu commands; and among other things, start an executable. With this infection method, the malicious application modifies or creates an autorun.inf file on all of the network shares, local drives, and removable media (including USB flash drives) that are connected to the computer. When an infected USB flash drive is inserted into another computer, the copy of the malicious application is automatically executed. Under a default configuration of Windows, this infection method does not require any interaction from the victim other than physically attaching the media to the computer.

Reprogramming USB peripherals. To turn one device type into another, USB controller chips in peripherals need to be reprogrammed. Very widely spread USB controller chips, including those in thumb drives, have no protection from such reprogramming.

**BadUSB - Turning devices evil:** Once reprogrammed, benign devices can turn malicious in many ways, including:

- 1. A device can emulate a keyboard and issue commands on behalf of the logged-in user, for example, to exfiltrate files or install malware. Such malware, in turn, can infect the controller chips of other USB devices connected to the computer.
- 2. The device can also spoof a network card and change the computer's DNS setting to redirect traffic.
- 3. A modified thumb drive or external hard disk can - when it detects that the computer is starting up - boot a small virus, which infects the computer's operating system prior to boot.

## Our Portable Media Attack Approach

With LUCY we provide a template for the "Simple file copy method". As mentioned before this

infection method requires that the victim manually execute the malicious file from their computer to become infected. So you have to lure a victim into launching the file and causing malicious code to be executed (e.g. just copy the file with an interesting file name on a USB stick and place them in spots where they will be picked up by other users).

## Setup

In order to create a Portable Media Attack scenario go through the following steps:

**STEP 1 - Create a New Campaign:** After the login, you can create your first Phishing Campaign by pressing the button “New Campaign”. Then choose the Attack Simulation campaign type.

**Campaign Wizard: Type**Close

1. Type

2. Attack Simulation

3. Campaign

4. Attack Template

5. Attack Settings





6. File Settings

7. Recipients

8. Review

9. Finish

Please choose a campaign type you would like to use.

Type	Description
 <b>Attack Simulation</b>	With an attack simulation (phishing, malware, smishing, USB attacks, etc.) you can test whether your employees are really familiar with the dangers of the Internet. LUCY provides a "safe learning environment" where employees can experience what real attacks would feel like.
 <b>Educate Employees</b>	Close knowledge gaps with Lucy's E-Learning. LUCY offers more than 200 interactive, web-based training modules (videos, tests, quizzes, games, etc.) on various security topics that can be provided to employees based on the results of the attack simulations or independently of them.
 <b>Infrastructure Tests</b>	Find out what kind of dangerous file types can get to the employee's Inbox, what can be downloaded and how big the risk is, if such a file is actually executed. Test the local windows security settings, the risks associated with downloads and the security of your mail infrastructure-tests-types.
 <b>Human Firewalls</b>	Turn your employees into human firewalls. The LUCY mail plugin for GMail, Outlook & Office 365 actively integrates your employees into detection of and fight against cyber-attacks. Suspicious e-mails can be reported with just one click and removed from the Inbox. In the LUCY environment the e-mails then analyzed and evaluated.

Skip the wizard and enable expert setupNext >

**STEP 2 - Choose Attack Type:** In order to configure the campaign choose **Portable Media Attacks**.

Campaign Wizard: Attack Simulation

1. Type

2. Attack Simulation

3. Campaign

4. Attack Template

5. Attack Settings


6. File Settings

7. Recipients


8. Review

9. Finish


Please choose an attack simulation type you would like to use.




**Data Entry Attack**  
Data entry attack can include one or more web pages that intercept the input of sensitive information. The available web pages can be easily customized with a LUCY web editor. Additional editing tools allow you to quickly set up functions such as log-in forms, download areas, etc. without HTML knowledge.




**Hyperlink Attack**  
A hyperlink-based attack will send users an e-mail that contains a randomized tracking URL to identify the user who clicked the link. There is no landing page involved in this campaign type. But you can redirect the user to any webpage after he clicked the link.




**File Attack**  
File-based attacks allow the LUCY administrator to integrate different file types (office documents with macros, PDFs, executables, MP3s, etc.) into mail attachments or websites generated on LUCY and to measure their download or execution rate.



**Portable Media Attack**  
LUCY offers the option to perform portable media attacks where a file template (e.g., executable, archive, office document with macros, etc.) can be stored on a portable media device such as USB, SD card, or CD. The activation (execution) of these individual files can be tracked in LUCY.



**Smishing**  
Smishing is, in a sense, "SMS phishing." When cybercriminals "phish," they send fraudulent e-mails that seek to trick the recipient into opening a malware attachment or clicking on a link.



**Vishing**  
Vishing Phishing. Available in LUCY 4.8

Skip the wizard and enable expert setup

Back

Next

**STEP 3 - Select or Create a Client:** Create a client or choose the built-in client (a client can be your own organization or the company that asked you to perform a phishing test). This is important because you can also create view only accounts that are associated with those clients.

LUCY Campaigns Incidents Settings Support Tools

Home / Clients

Clients

Client

☐ 3HCapital

☐ Xu O O

☐ Ucawce Si

☐ Lucy

Templates

Benchmark Sectors

Domains

Dynamic DNS

Adapt Authoring Toolkit

Recipients

Clients

End Users

Administrative Users

Export

New Client

Delete

Client

☐ 3HCapital

☐ Xu O O

☐ Ucawce Si

☐ Lucy

Clients

Client Invoice Settings

**STEP 4 - Select your Attack Template:** Select the scenario called **Portable Media Attack**. If you don't have this scenario among your templates then please download it using the "download" button in the **Settings → Templates → Download Templates**.

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

Campaign Wizard: Attack Template

Close

1. Type

2. Attack Simulation

3. Campaign

4. Attack Template

5. Attack Settings

6. File Settings

7. Recipients

8. Review

9. Finish

Please choose the attack scenario you would like to use in this campaign. If you would like to have multiple scenarios in this campaign, you may add extra scenarios after finishing the wizard.

☐ Only display recommended templates according to your industry type and size

Q

USB

SSD

ISO

**Portable Media Attack**

LUCY allows you to create file that can be stored on removable media devices (CD, USB, DVD, SD Card etc.). The most popular is an attack using USB sticks. But this template works for all other variations of removable media types as well. Read more about this scenario type here: <https://goo.gl/epWzoJ>

Select Language

Back

Next

**STEP 5 - Give the scenario a name and pick a domain or IP address:** This is the domain or IP which is used upon execution: the malware simulation will send the data back to this host.

Campaign Wizard: Attack Settings

✕ Close

1. Type

2. Attack Simulation

3. Campaign

4. Attack Template

5. Attack Settings

6. File Settings

7. Recipients

8. Review

9. Finish

Configure basic attack settings.

Domain

Local IP

127.0.0.1

Generate ISO Images

Success Action

Click

SSL

Use Custom SSL Certificate

?

◀ Back

Next ▶

**STEP 6 - Configure the File template:** This template defines what malware simulation should be running upon execution of the file on the Portable Media Device. Make sure you have the latest malware simulations installed in LUCY. You can download the malware simulations using the "download" button in the template section.

Campaign Wizard: File Settings

✕ Close

1. Type

2. Attack Simulation

3. Campaign

4. Attack Template

5. Attack Settings

6. File Settings

7. Recipients

8. Review

9. Finish

Configure your file.

File

Console Post

Description

Get output from one or multiple console programs. Display GUI option may have a value of 0 to 4: 0 - no GUI, 1 - Progress Bar, 2 - Decryptor Window, 3 or 4 - Error Message Window.

Variables

Commands

ipconfig,whoami

Display GUI (0-4)

1

Text Message

Exection Error XYZ

⏪ Back

Next ⏩

**STEP 7 - Configure Number of Portable Media Devices:** Choose the option **Enter Manually** and add a **Number of Portable Media Devices** to define how many USB sticks you plane to use.

Campaign Wizard: Recipients

✕ Close

1. Type

2. Attack Simulation

3. Campaign

4. Attack Template

5. Attack Settings

6. File Settings

7. Recipients

8. Review

9. Finish

It's time to add recipients or choose an existing recipient group.

Mode

☐ Select Existing Group

☒ Enter Manually

Number of Portable Media Devices

5

⏪ Back

Next ⏩

**STEP 8 - Download Files:** You're all set! Hit Start if you would like to start the campaign right away. You will be able to start the campaign any time later from the campaign summary page.

**Campaign Wizard: Finish**✕ Close

1. Type

2. Attack Simulation

3. Campaign

4. Attack Template

5. Attack Settings

6. File Settings

7. Recipients

8. Review

9. Finish

You're all set!

Hit Start if you would like to start the campaign right away.  
You will be able to start the campaign any time later from the campaign summary page.

Download Files

Go to Campaign

Start

Once you started the campaign LUCY will wait for incoming requests from executed files.

## What are the requirements for an USB stick to report back to LUCY?

In order to for the USB stick to report back to LUCY the following requirements must be met:

- The file (exe) on the stick needs to be executed\*
- The computer where the file on the USB stick gets executed needs access to the internet
- LUCY must be reachable from the internet (with the IP or domain name configured in the USB campaign)
- The campaign must be running

\*You could also purchase USB sticks that will emulate external hardware (like keyboard) and execute the file automatically when attached to a computer  
(<https://shop.hak5.org/products/usb-rubber-ducky-deluxe>)



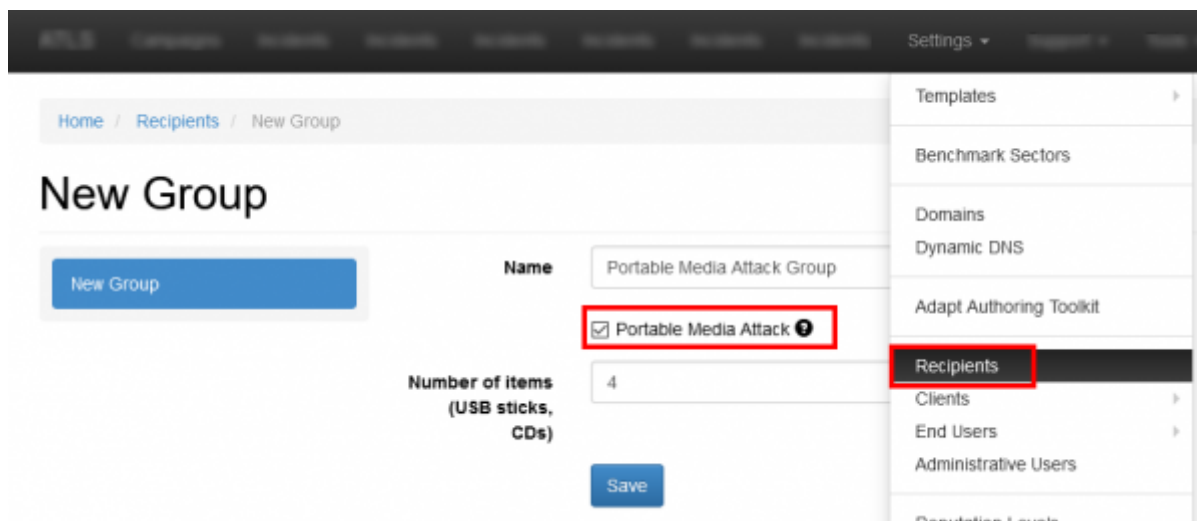
## Important Questions

- Does it need admin rights to execute the files? No - to execute the malware simulations it does not need admin rights. The standard windows user rights will do.
- Can I only place an executable on the USB? No - you can place any type of malware simulation on the USB (.exe, doc with Macro, archived format, etc.)
- How can I get the users to execute the file? You could use simple social engineering techniques and just place some sticks in a public area, rename the executable to something like "decrypt\_accounts.exe" (if you choose for example the malware simulation with the screenshot & webcam tool it will show you some fake decryption GUI upon execution)
- How do I know if users executed the files? The moment the files get executed and the user has internet access the data will be transferred back to LUCY using the build-in browser.
- Will the tool get detected by an AV? No - this should not happen (please let us know if this occurs)
- Will the tool be able to bypass USB filters or windows security settings (like UAC)? No - if you don't allow files from a USB drive to be executed this won't work.

## Create an Attack with CD & DVD's

LUCY > 3.1 offers the administrator to create also ISO images which can be used to burn a CD or DVD. Most CD-ROM burning applications recognize this type of image file. Once the ISO file is burned as an image, then the new CD/DVD is a clone of the original and bootable.

To create an attack with ISO image you first need to create them according to a group within the recipient (make sure you enable the checkbox "portable media attack"):



Next, after you selected a template like the Portable Media Attack scenario, you need to make sure that within the scenario settings you enable the checkbox "generate ISO images":

## New Scenario

Scenario Status: Not Started Download Files

New Scenario

Template

Portable Media Attack / English Change/Select Template

Name

Portable Media Attack

Landing Domain

Local IP

Custom Domain

127.0.0.1

☒ Generate ISO Images

Success Action

Data Submit

Save

After configuring the remaining scenario settings you can add the recipient group which you created for the portable media attack to your scenario. You should see a screen similar to the following example:

Home / Campaigns / USB test campaign / Recipients / Add Group

### USB test ca...

Campaign Status: Not Started ▶

Results

Summary

Statistics

Reports

Exports

Configuration

Base Settings

Recipients

Advanced Settings

User Settings

Custom Fields

Logs

Supervision Log

Group

Portable Media Attack Group

Search

Search by recipient name, email, phone, staff type, location, +

Search

Reset

<input checked="" type="checkbox"/>	Name								
<input checked="" type="checkbox"/>	18f90a30e0@domain.bdi+111111111111	File 4	N/A	N/A	N/A	N/A	N/A	N/A	N/A
<input checked="" type="checkbox"/>	c4e410511e@domain.bdi+111111111111	File 3	N/A	N/A	N/A	N/A	N/A	N/A	N/A
<input checked="" type="checkbox"/>	165937d5c1@domain.bdi+111111111111	File 2	N/A	N/A	N/A	N/A	N/A	N/A	N/A
<input checked="" type="checkbox"/>	3394145463@domain.bdi+111111111111	File 1	N/A	N/A	N/A	N/A	N/A	N/A	N/A

10

Mapping

Campaign + Awareness

☐ Distribute users over selected scenarios.

Scenarios

☒ Select All

☒ Portable Media Attack (ISO) (Portable Media Attack)

Save

Once you started the campaign LUCY will wait for incoming requests from executed files.

Here is also a quick tutorial on how to burn a bootable ISO image on different operating systems:

## Windows 8/8.1/10

- Download the ISO CD image to a folder on your computer.
- Open the folder where you have saved the ISO file.
- Right-click on the .iso file.
- From the menu select Burn disc image.

- The Windows Disc Image Burn will open.
- Select the Disc burner.
- Click on Burn.

## Windows 7/Vista

- Download the ISO CD image to a folder on your computer.
- Insert a blank CD in your CD-RW drive.
- Navigate to the folder where you saved the file.
- Click to highlight the file (Windows 7/Vista) and/or right-click on the file (Windows 7 only) to see the options for creating a disc.

## MacOS

- Download the file .ISO file to your Mac
- Insert a blank disc.
- From the Desktop, click on Utilities (or in some cases, Applications, and then Utilities).
- Launch Disk Utility.
- From the File menu, choose Open Disk Image.
- Select the ISO image to be burned.
- In the list of volumes, you will now see an item representing the ISO file. Select it.
- Click the Burn icon.
- A Select Image to Burn window will appear.
- Select the .iso file you want to burn to a CD/DVD.
- Make sure you have a disc inserted in your drive and then click the Burn.
- A Disk Utility window will appear showing the recording progress.
- Once the recording process has completed, Disk Utility will verify that the image was burned correctly.
- Click OK to eject the disc.

## Protect your Network from USB attacks with a challenge campaign

Unknown USB devices are a serious risk to your network. 67% of employees who find a USB device in a parking lot will plug it into their computer.

### Would your employees put your network at risk and plug in an unknown USB device?

Find out in 3 simple steps:

- Select the USB device
- Select Awareness Training
- Track Awareness Campaign

[START THE USB CHALLENGE AND GET A QUOTE](#)

Last  
update:  
2020/08/13 02:32 create\_a\_campaign\_with\_portable\_media\_devices [https://wiki.lucysecurity.com/doku.php?id=create\\_a\\_campaign\\_with\\_portable\\_media\\_devices](https://wiki.lucysecurity.com/doku.php?id=create_a_campaign_with_portable_media_devices)

---

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

Permanent link:  
[https://wiki.lucysecurity.com/doku.php?id=create\\_a\\_campaign\\_with\\_portable\\_media\\_devices](https://wiki.lucysecurity.com/doku.php?id=create_a_campaign_with_portable_media_devices)

Last update: **2020/08/13 02:32**

