

FILE BASED ATTACKS (INSIDE OUT)

Introduction

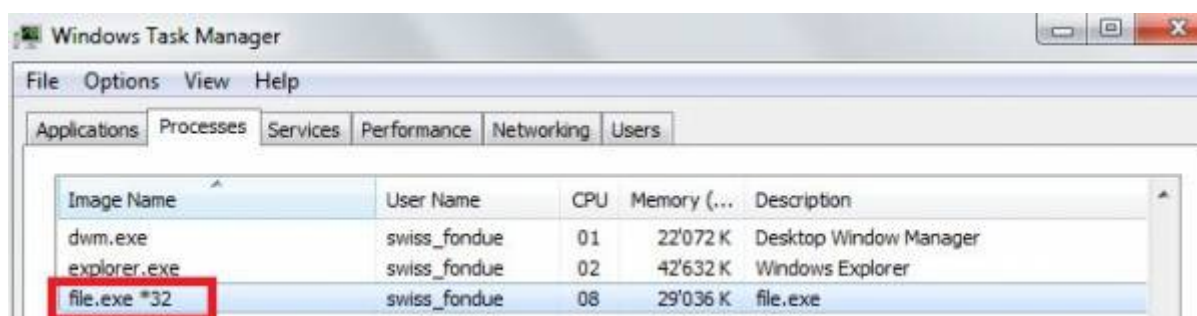
Inside-Out attacks try to initiate network connections from the trusted (corporate) to the untrusted (Internet) network. These attacks require that an "insider" execute code. This is usually because the person that executes the code is unaware of security issues and doesn't realize that an application can do anything to their system within the limits of the access that is granted to that user. The inside out attack consists of three steps:

- STEP 1 Getting the backdoor in the network (delivery)
- STEP 2 Executing the backdoor by the user (execution)
- STEP 3 Sending the data out (output delivery)

LUCY's approach

With LUCY's file-based attack you are able to perform the following steps:

- **STEP 0 Trojan compilation:** Via the Web GUI you will be able to define the settings of the trojan simulation (e.g. what the file should look like & do upon execution). The trojan simulation can be either an executable (which gets compiled during the campaign), some payload which you upload to LUCY yourself or some [Office file that contains a Macro](#).
- **STEP 1 Delivery:** The trojan simulation can be integrated into a landing page on LUCY so it may be downloaded from the clients or it can be attached in the mail.
- **STEP 2 Execution:** By using a phishing mail which can be edited on LUCY you can try to lure the recipient into opening the Trojan simulation. Once the Malware Simulation is executed on a Windows Client, you can see the file in the Task Manager as "file.exe". LUCY has some command restrictions to prevent LUCY administrators from damaging the client's system, therefore not all shell commands are allowed.



- **STEP 3 Output Delivery:** The files compiled by LUCY communicate back to your server using HTTP/HTTPS. Therefore LUCY needs to be reachable via those protocols to make the scenarios work.

Note: The files are non-intrusive, run only in the memory and have no effect on the System (no changes are made). In the current edition, the executable runs only on Windows (Windows 7/8/10).

File based attack simulation templates

List of all **file-based attack templates**, with **Success actions** and **Preferable delivery methods** can be found [here](#).

File based attack simulation configuration

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

Campaign Wizard: Type

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
 Attack Simulation	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.
 Educate Employees	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.
 Infrastructure Tests	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.
 Human Firewall	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 setup

Next

STEP 2 - Choose Attack Type: In order to configure file-based campaign choose **File Attack** type.

Campaign Wizard: Attack Simulation 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 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 malicious link. Smishing simply uses text messages instead of e-mail.

**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](#) which are associated with those clients.

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

Campaign Wizard: Campaign Close

1. Type

2. Attack Simulation

3. Campaign

4. Attack Template

5. Attack Settings

6. File Settings

7. Recipients

8. Review

9. Finish

Here you configure basic campaign settings - its name and the client it is attached to.

Name

File Based Campaign Test

Client

Lucy

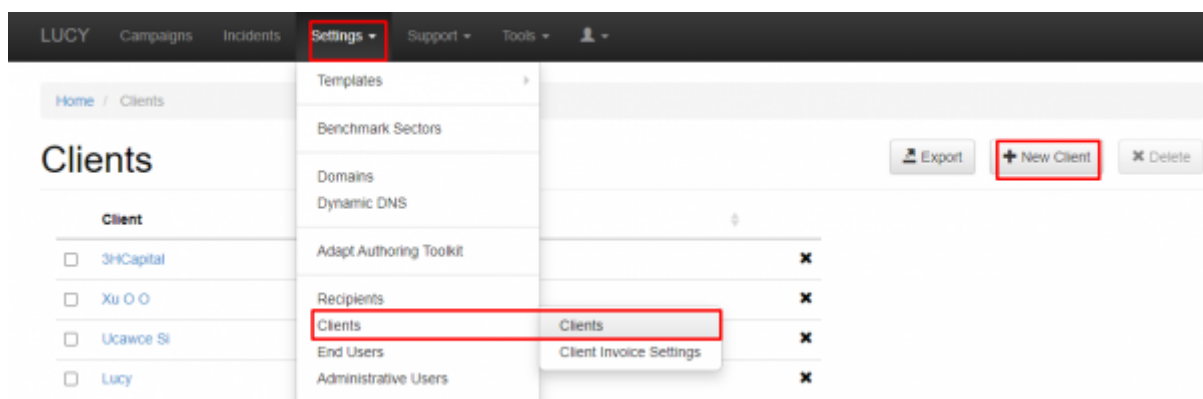
☐ Include training

Advanced Settings

Back

Next

New clients are created under **Settings → Clients → New Client**.



STEP 4 - Select your Phishing Scenario: Now you need to select one or multiple phishing scenarios. Since you are going to do a file-based attack you need to pick a scenario either from the "file-based templates" or the "mixed templates"

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

Search...




Blank (File-Based)
Blank file-based template.

Preview Select Language




Blank (Mixed)
Blank mixed template.

Preview Select Language



Booking.com (Petya Ransomware) ver.2.2
The recipient gets a booking confirmation "Your Booking Berlin Novut Hotel is confirmed". After the link click the user gets redirected to a landing page where he can authenticate with his credentials and download an Word Document. The Word File is required to cancel the reservation and refund the money. Office files containing a Macro are the typical entry point for malware (seen in attacks like Petya).

Preview Select Language



Cirtix Login & Plugin Install
In this mixed template the user has the ability to log in and access his/her company's work environment with a special plugin.

Preview Select Language

Back

Next

You are able to preview every template before selecting it. In the **Preview Mode** you can test the site using all the features (just enter some random login to get to the next page).



Cirtix Login & Plugin Install
In this mixed template the user has the ability to log in and access his/her company's work environment with a special plugin.

Preview Select Language

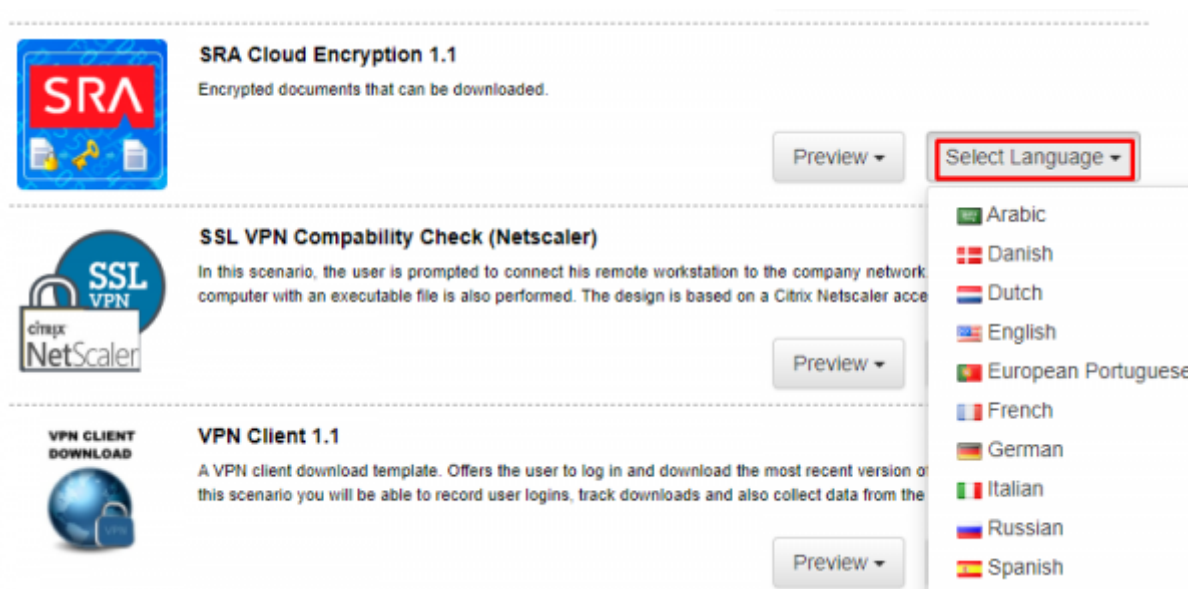


Confirmation Social Media Profile (V2.2)
A social media provider informs the recipient that a profile under his/her name has been created. The user can download a Word file that appears to be a CV. The Word file itself contains a macro through which you can track if the file has been opened.

Preview Select Language

Note: You can allocate multiple scenarios within one campaign and they can all be started simultaneously! Example: A company might want to split the employees into 2 or 3 groups. One group could get a phishing mail with a landing page that contains many obvious errors and should be easily detectable while the other scenario is almost perfect. This way the client can identify the variables that drive the awareness in one single campaign.

STEP 5: For this tutorial, as an example, we select the **SRA Cloud Encryption 1.1** template, where the user will be asked to download an encrypted file. To select the template for the campaign click the **Select Language** button and choose the preferred language from the drop-down menu.



STEP 6 - Configure basic attack settings of Your Campaign Once you have selected the scenario, you need to configure the **Base Settings** of the campaign. First, give your campaign a name and then choose how your recipients will be able to access LUCY by defining the [Domain](#). Finding the appropriate domain name is a very important step for success and it depends very much on your campaign scenario. If you plan to create a fake webmail login you might try to reserve a domain like "webmail-server365.com" and point it to LUCY.

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

Custom Domain

Custom Domain

lucysecurity.com

SSL

☐ Use Custom SSL Certificate ?

Mail Configuration

Sender Name

Test

Sender Email

test@lucysecurity.com

Subject

Employee Documents - Internal Use

Advanced Settings

Back

Next

STEP 7 - Configure Your File: There are several types of the file available in a file-based campaign:

- Archive
- Tunnel Executable
- Java Applet
- PDF document

In this particular case, we choose the Archive type of the file with .RAR extension. Instead of sending the attachment as a plain file (e.g. file.exe) or providing it as an executable file to download, you can set the compression option (this is recommended). Like this, the file will be archived.



Custom file name: you can give the archive a custom name (e.g. "encrypteddoc.zip")

Archive Type: you can choose which compression type you want (the common type which is supported by all windows clients is .zip; other compression types will need additional client software)

Password: You can set up a password for your archive and insert it into the message to make the simulation more realistic. **Delivery Method** checkbox:

Campaign Wizard: File Settings

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 Type

Archive

Archive Type

RAR

Custom File Name

testFile

.rar

Password

Delivery Method

☒ Add as a mail attachment

☐ Insert into landing page

Malware Simulation

File

Macros (POST-only)

Description

This macros template just pings back to Lucy when user opens the document, without collecting any data.

Back

Next

Then add Recipients to the campaign and watch through the **Review** of the campaign.

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

Recipients

+ Add

support@lucysecurity.cor

Oliver Muenchow

Back

Next

The campaign can be started from that point by pushing the **Start** button. Otherwise, push **Go to the Campaign** button in order to set up the campaign further.

All the further configuration is performed through **Base Settings**.

Home / Campaigns / File Based Campaign Test / Base Settings

File Based ...

Campaign Status: Not Started

Export New Scenario

Results

- Summary
- Statistics
- Reports
- Exports
- Automated Export

Configuration

- Base Settings
- Awareness Settings
- Schedule
- Recipients

Advanced Settings

- User Settings
- Filters
- Custom Fields
- Reminders

Logs

Name: File Based Campaign Test

Client: Lucy

Industry: N/A

Notes:

☐ Suppress duplicated recipients in campaign.

☐ Enduser Profiles Enabled

☐ Track Responses

☐ Email Tracking

Antivirus/Firewall Protection Interval: off

☐ Allow Awareness Rescheduling

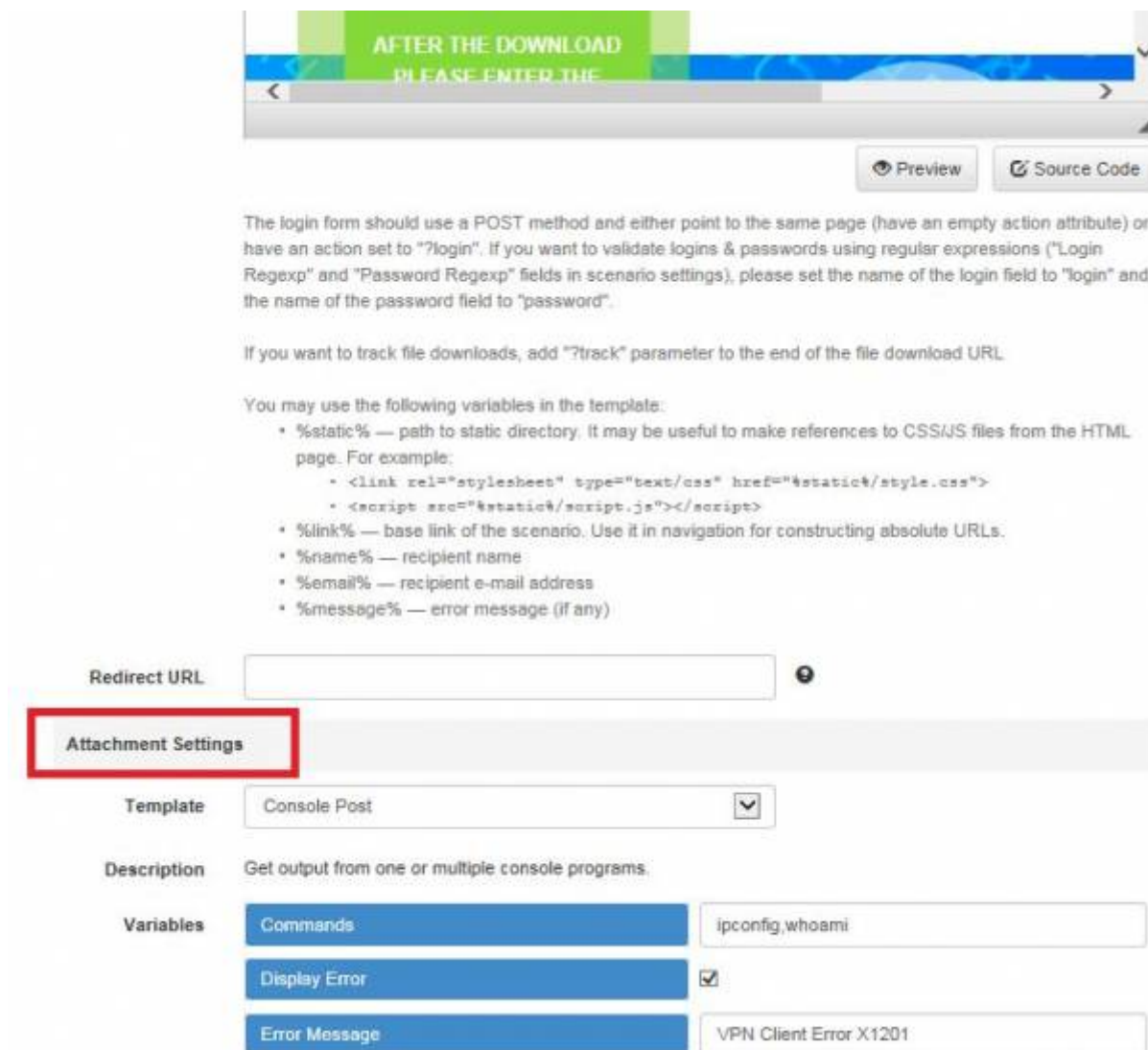
☐ Ignore repeated answers in awareness.

☐ Stop the Campaign Automatically

☐ After I stop the campaign, send me a report to default@user.com

STEP 8 - Edit your Landing Web Page within Your Campaign: After saving the Base Settings, you can now [Edit the Landing Page](#), [Upload Your Own Webpage](#) or simply [copy any website on the internet](#). The Landing Page is the webpage that the users will see when they click on the link in the email they receive. First, select the drop-down menu at the top of the page where you want to edit. Please note that the same landing page may be available in different languages. So make sure you [edit the correct language](#). When you choose a file-based attack scenario you will see some additional configuration options appearing at the bottom of the page. Those settings define what file is provided within the download button for the recipient and what the executable should do upon opening. We recommend starting with a "harmless", non-intrusive trojan simulation that doesn't violate the recipients' data privacy. A harmless simulation is, for example, the ConsolePost" Trojan, which will stealthily execute a few pre-defined commands (like "whoami") in the user's shell and send the output back to LUCY. You have a few additional options:

- Decide if the user should see [some fake GUI](#) upon execution or not
- Specify a specific error message that will appear upon execution
- Specify the Trojan settings (e.g. enable/disable specific Trojan features or define custom commands)



Preview Source Code

The login form should use a POST method and either point to the same page (have an empty action attribute) or have an action set to "?login". If you want to validate logins & passwords using regular expressions ("Login Regexp" and "Password Regexp" fields in scenario settings), please set the name of the login field to "login" and the name of the password field to "password".

If you want to track file downloads, add "?track" parameter to the end of the file download URL.

You may use the following variables in the template:

- * %static% — path to static directory. It may be useful to make references to CSS/JS files from the HTML page. For example:
 - * <link rel="stylesheet" type="text/css" href="%static%/style.css">
 - * <script src="%static%/script.js"></script>
- * %link% — base link of the scenario. Use it in navigation for constructing absolute URLs.
- * %name% — recipient name
- * %email% — recipient e-mail address
- * %message% — error message (if any)

Redirect URL

Attachment Settings

Template Console Post

Description Get output from one or multiple console programs.

Variables

Commands ipconfig,whoami

Display Error ☒

Error Message VPN Client Error X1201

STEP 9 - Configure Message Settings (Email): It's time to set up email communication (if you want you can also use [SMS](#) as an alternative). Choose your sender's name, email address, and subject. Please also choose the language for each group. If you configured an English landing page, then select English also within that recipient group. If you have different groups with different languages within your company you can simply create a group and select a language for each recipient. LUCY then will direct each user to an individual landing page that [matches that language](#). Please read the [Mail Settings Chapter](#) for more configuration options.

LUCY Test Campaign

 Restore Defaults

Summary

General Settings

Landing Template

E-mail Template

Errors

Sender Name

Peter Test

Sender E-mail

peter@phishing-server.com

☐ Random E-mail

Subject

Please access your encrypted mail X

[Forward E-mail](#)

☐ Use Reply-To Header ⓘ

Content

Dear %name%:

You have received an encrypted message with „Microsoft Office 365 Cloud Services“. You can access it using our new webbased mailplatform "Secc-Mail" under the following link: %link%. Please sign in with your Windows username and password to decrypt the message.

Sandra Smith
IT Exchange Team / EMEA

When choosing a file-based scenario LUCY will offer you additionally to send the Trojan simulation via mail. If you already have chosen a landing page where the Trojan simulation can be downloaded it is not necessary to attach it via mail as well. Therefore if you don't want LUCY to send the file via mail choose "NA" within the malware simulation template dropdown menu:

Content

Quellcode

Subject: Employee Documents - Internal Use

Under the following link you received an encrypted document which is accessible via the secure cloud repository [here](#).

This message may contain information that is privileged and confidential. If you received this transmission in error, please notify the sender by reply email and delete the message and any attachments.

Preview

Malware Simulation

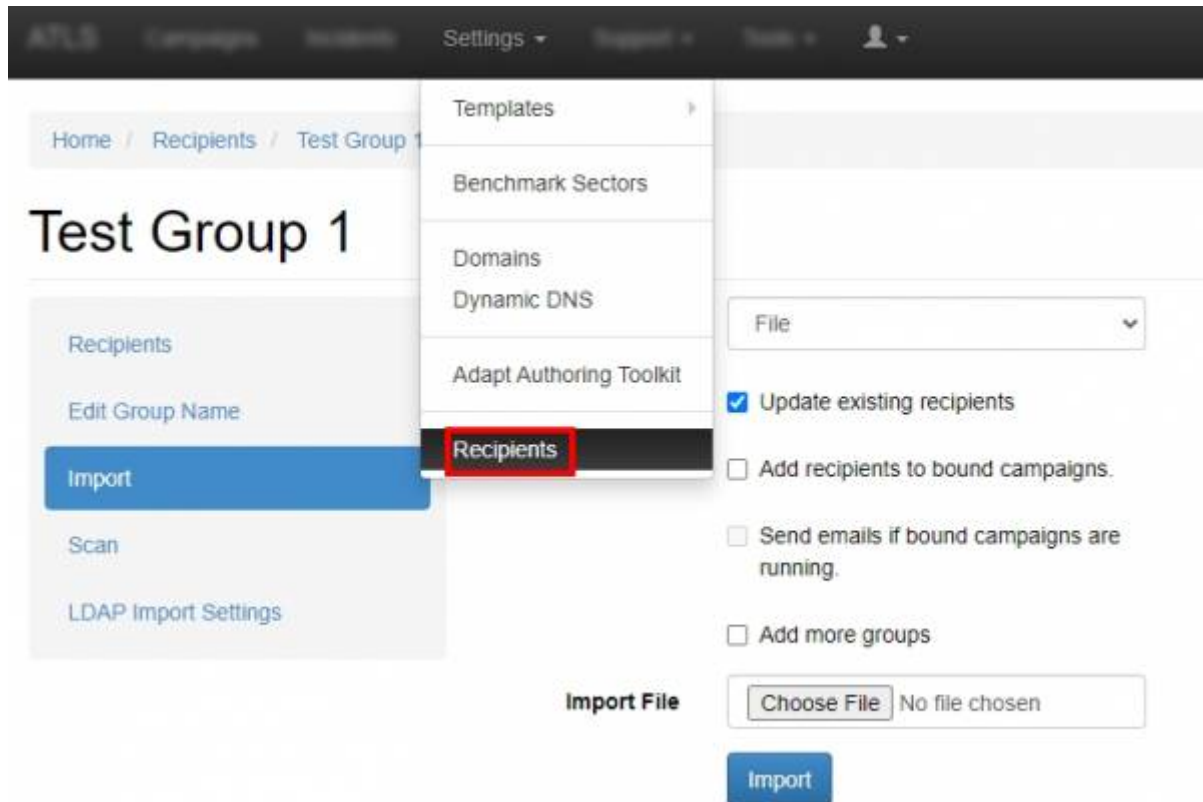
Template Console Post

Description Get output from one or multiple console programs.

Variables

Commands	ipconfig,whoami
Display Error	<input checked="" type="checkbox"/>
Error Message	VPN Client Error X1201

STEP 10 - Add Recipients to Your Campaign: You need to create the Recipients List in the Menu item "Recipients".



This is the list of users that will get the phishing emails. You can add them manually, import a file with all your recipients or even search them on the internet. Once you have created that group, you can select it in your campaign and map it to a specific scenario. You can also define if they should be used only for the Landing Page link, the [Awareness site link \(e-learning\)](#), or both.

Home / Campaigns / Lucy Phishing Campaign / Recipients / Add Group

Lucy Phishi...

Campaign Status: Not Started

Results

- Summary
- Statistics
- Reports
- Exports
- Automated Export

Group Test Group 1

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

☒ Email/Phone ☐ Full Name ☐ Language ☐ Staff ☐ Location ☐ Division

 No recipients.

Configuration

- Base Settings
- Awareness Settings
- Attack Settings
- Schedule
- Recipients**
- Advanced Settings

Mapping Campaign + Awareness

☐ Distribute users over selected scenarios.

Scenarios

- ☐ Select All
- ☐ Lucy Test (Hyperlink)

Please read the [Recipients Settings Chapter](#) for more configuration options.

STEP 11 - Add Scheduling Options to Your Campaign: If you want, you can create a schedule to run the campaign using a delay or customized time delays between campaign phases. If you are new to the system, we'd recommend that you go with the Default Timing Settings and skip this step. Please read the [Schedule Settings Chapter](#) for more configuration options.

Step 12 - Add E-learning Content to Your Campaign There is the option to have LUCY automatically send some e-learning content to all users or only users who have failed the phishing test. This configuration setting is part of an [Separate Chapter \(E-learning\)](#).

Step 13 - Start Your Campaign: Now you are ready to start. Although we recommend performing a test run with a single recipient before you start attacking all users, additionally it is a good idea to use the [LUCY SPAM Checker](#). Just click "Real Attack" and LUCY will test your settings before starting the campaign. If you want to skip the checks, press "Skip Checks". Your first recipients should receive the emails within seconds. Please read the [Start Campaign Settings Page](#) for more configuration options. If you experience any problems with starting/running your campaign, please [Consult the Troubleshoot Section](#) first.

Home / Campaigns / Lucy Phishing Campaign

Lucy Phishi...

Campaign Status: Not Started

Results

- Summary
- Statistics
- Reports

Campaign	Running Time	Created By
Lucy Phishing Campaign	Not running	default@user.com

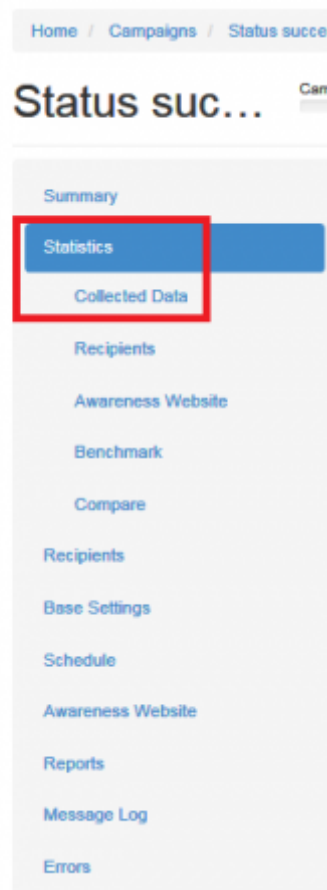
Attack Overview

- Restart
- Resume
- Test Run

Step 14 - Monitor Your Campaign: The progress of the campaign can always be monitored in Real-Time. Click "Statistics" within your campaign. Please read the [Statistics Chapter](#) for more configuration options.



The output from each Trojan execution can be found under "statistics/collected data":

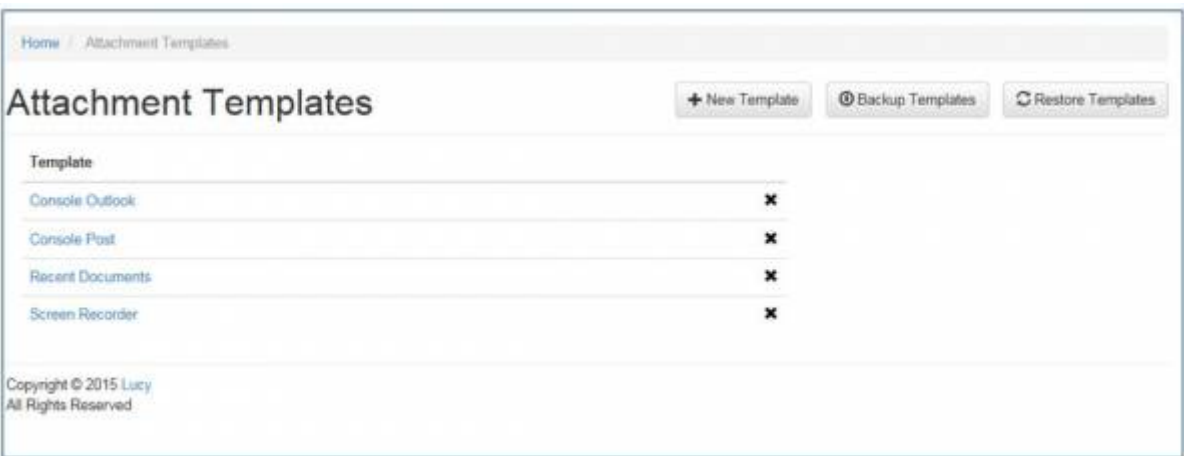


Step 15 - Create Reports: Once you have finished the campaign, you may create different types of reports (PDF, HTML or raw export). Please read the [Creating Reports Chapter](#) for more configuration options.



Edit File based templates

All attachments can be edited within LUCY. The Attachments Settings can be stored as Default templates under Settings/Attachment templates.



The screenshot shows the 'Console Outlook' configuration page. At the top, there are links for 'Home', 'Attachment Templates', and 'Console Outlook'. The page title is 'Console Outlook'. There are two buttons: 'Backup Template' and 'Restore Template'. The 'Name' field is 'Console Outlook'. The 'Description' field contains the text 'Get output from one or multiple console programs and send it by e-mail'. The 'Add Attachment' section has a text input and a 'Browse' button. The 'Attachments' section shows 'file.exe' with a close button. The 'Variables' section is a table with 8 rows and 3 columns.

Variables		
Commands	commands	ipconfig,whoami
Display Error	gui	1
Error Message	error	VPN Client Error X1201
E-mail	mainmail	test@test.com
Subject	subject	Lucy - Console Outlook Output
Steal Last Mail	lastmail	1
Name	Internal Name	Value

At the bottom left, there is a 'Save' button.

You can rename the file templates from file.exe to any filename. In LUCY < 3.2 you can do that by downloading the file.exe, renaming it & then uploading it back to the generic file template.

Technical Details about the data delivery

Upon execution, this tool will execute the predefined commands or access documents. It will open the built-in Internet Explorer or another default browser (in hidden mode) or access Outlook and send out the collected data to LUCY via HTTP or HTTPS or via SMTP (it will automatically choose HTTPS if you run your campaign via SSL). This tool will also work in environments where the Internet is accessed with Proxy servers - only allowing access for authorized Windows users. The file can then be downloaded as a plain exe or as a zipped archive.

Note: The current edition of LUCY will include tools that access files on shares and upload them to the campaign or access the email client via MAPI. These features have restricted configuration options in the community edition (like maximum number of files that can be uploaded, etc.) the same goes for the number of screenshots or length of videos. Only the Commercial Editions have no limitations. You can upload your own custom payload. But keep in mind that reverse channels to LUCY won't work; only attachments from LUCY are compiled in Real Time with certain settings (IP, Domain Name, URL etc.).

Delivery Challenges

Executable files usually cannot be delivered to a user via e-mail attachment. These are blocked by

most email programs.

In order to deliver a malware simulation to the user, the attachment should not be provided via email, but via download on a website. There you have the possibility to download the file:

- Inside an archive (zip, jar, rar etc.)
- Inside an encrypted file (e.g. zip with a password)
- [Inside a PDF](#)
- [Tunneled through an applet](#)
- Download as a plain exe

Those settings can be applied within the scenario settings of the specific template. Choose archive (1), Tunnel (2) or PDF (3) for the according method:

The image displays three distinct configuration panels for a malware simulation tool, each outlined with a red border. The top-left panel, labeled '1', is for 'Archive' and includes fields for 'Archive Type' (set to ZIP), 'Custom File Name' (set to test), and a 'Password' field, with a 'Save' button at the bottom. The top-right panel, labeled '2', is for 'Tunnel Executable' and features a 'Download Path' field set to '%TEMP%' and a 'Save' button. The bottom panel, labeled '3', is for 'PDF document' and includes an 'Upload PDF File' button (labeled 'Choose File' with 'No file chosen' text) and a 'PDF Custom Name' field, also with a 'Save' button.

Q&A

Q: Do the files need to be installed?

A: No, the files are non-intrusive, run only in the memory and have no effect on the System (no changes are made).

Q: Do the files need to be run with elevated permissions?

A: No. The files can run with limited, standard windows user rights.

Q: Our filters block file types like .exe- How can I still use the files?

A: Use a different file format within the scenario settings (e.g. place the exe in an archive like a zip file or place it within a PDF as an attachment).

Q: Can I run the files on MAC or Linux?

A: No. In the current edition, the executable runs only on Windows (Windows 7/8/10).

Q: Windows Defender blocks the files - can this be prevented?

A: Yes, It can be prevented using "whitelisting" inside the Windows Defender Security Center. But it is normal that the defender blocks the code as the defender will block any unknown code which is not officially signed. The files unfortunately cannot be signed, as the hash value is different for each user (the files get compiled on the fly individually for every single user)

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

Permanent link:
https://wiki.lucysecurity.com/doku.php?id=create_a_phishing_campaign_with_malware_simulations

Last update: **2021/12/15 13:20**

