

HTML File Attack

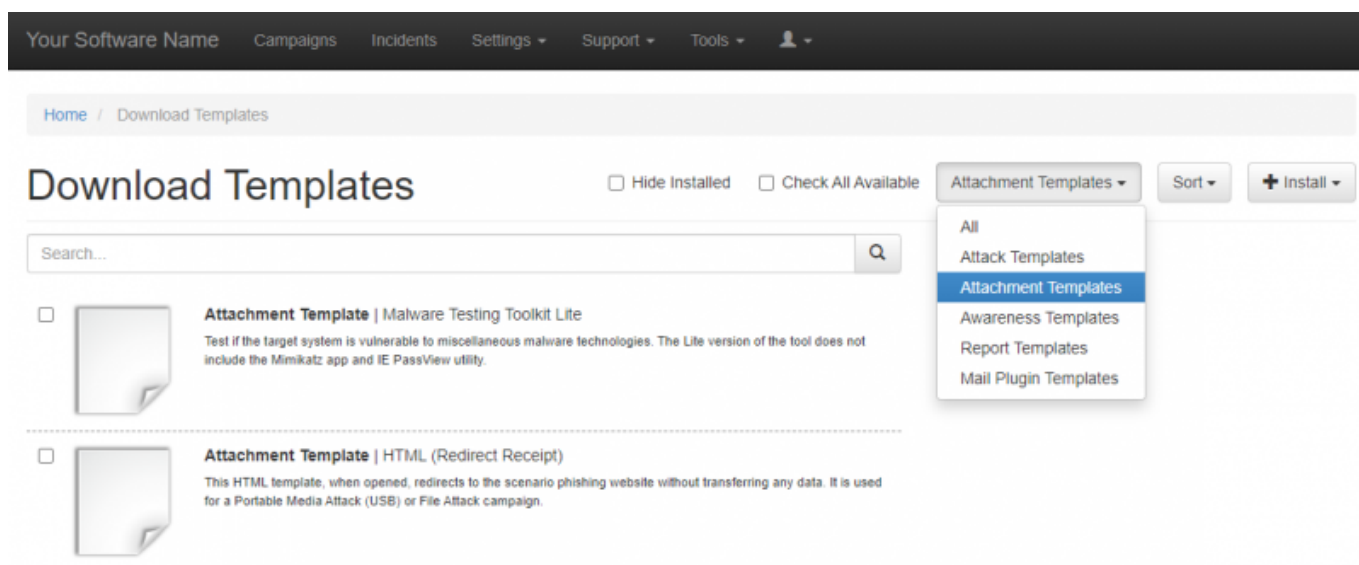
File-based attacks allow the LUCY administrator to integrate different file types (office documents with macros, executables, HTML, etc.) into mail attachments or websites generated on LUCY and to measure their download or execution rate.

In this article, the process of creation of the HTML file-based attack is described.
For the main file-based attack simulation explanation please refer to [this article](#).

Initial Preparation

In order to be able to configure this type of attack, please make sure to download the required template from this section:

Settings > Templates > Download Templates.



Use the filter to show only Attachment Templates and installed all available.

Attack Setup

To set up the campaign please use Wizard (New Campaign button).
Chose an option "Attack Simulation" and press Next.

Campaign Wizard: Type ✕ Close

1. Type





2. Campaign

3. Recipients

4. Review

5. 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. Your Software Name provides a "safe learning environment" where employees can experience what real attacks would feel like.
 Educate Employees	Close knowledge gaps with Your Software Name's E-Learning. Your Software Name 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.
 Engage Employees	Turn your employees into human firewalls. The Your Software Name 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 Your Software Name environment the e-mails then analyzed and evaluated.

Skip the wizard and enable expert setup

Next ➔

On the next screen select "File Attack" and press Next.

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 Your Software Name 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 Your Software Name administrator to integrate different file types (office documents with macros, PDFs, executables, MP3s, etc.) into mail attachments or websites generated on Your Software Name and to measure their download or execution rate.

**Portable Media Attack**


Your Software Name 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 Your Software Name.

**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 Your Software Name 4.8

**IM Phishing**

Skip the wizard and enable expert setup

Back

Next

Enter the required fields for the campaign configuration. 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.

Then 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".

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.

Once you reach the 6th stage of configuration, there will be a screen of the Malware Simulation options.

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

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 Type

N/A

Delivery Method

☐ Add as a mail attachment
☒ Insert into landing page

Malware Simulation

File

HTML (Redirect)

Description

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.

For the HTML attack, the **File Type** should be left default.

Delivery Method can be chosen between "Add as a mail attachment" and "Insert into landing page" options.

And as for the file make sure to select HTML template from the drop-down menu.

Description: 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.

Finish the campaign configuration by adding the recipient groups.

From:

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

Permanent link:

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

Last update: **2021/09/27 17:32**

