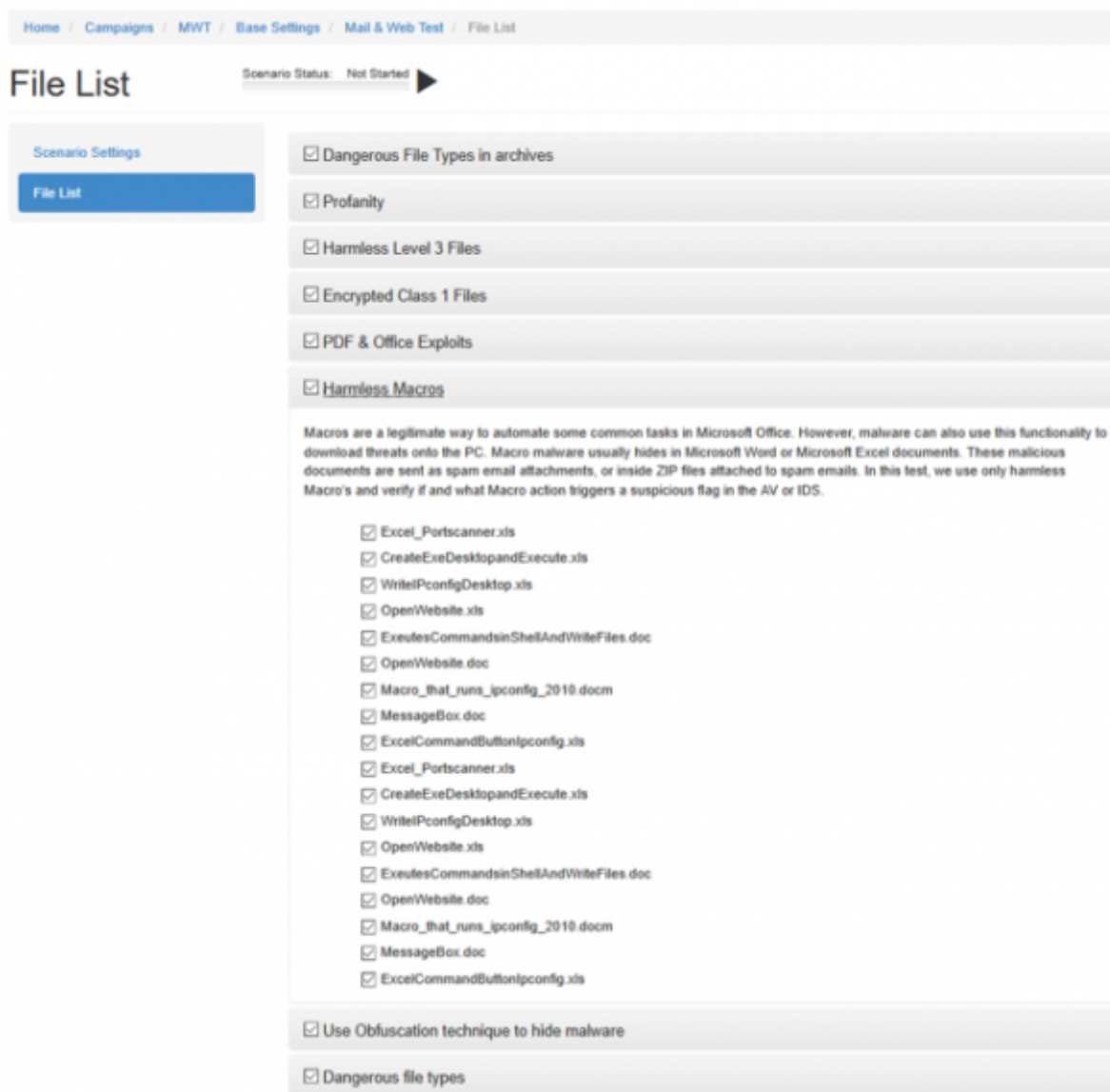


Webfilter and mail filter test

The Email and Internet malware protection test gives you an insight at how your mail server and web proxy handles different variations of test files. You can thus see whether potential malicious code, such as Java files, backdoors, scripts, embedded Office Objects are detected and blocked by the filter infrastructure. Based on these results, you can then carry out targeted phishing campaigns.



With our software you can check which file types could potentially enter the company and which are blocked by the security infrastructure. LUCY works with a wide range of file types that can be brought to the end system via e-mail or on a website for download. You can thus see whether potential malicious code, such as Java files, backdoors, scripts, embedded Office Objects are detected and blocked by the filter infrastructure. Based on these results, you can then carry out targeted phishing campaigns.

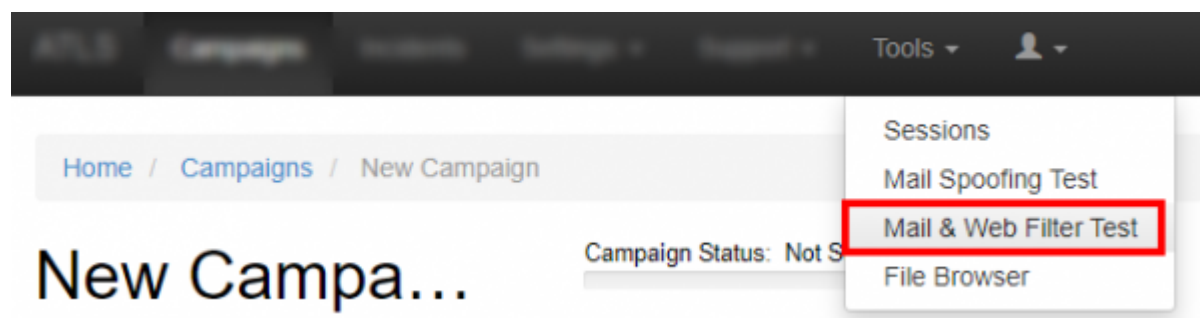
Main Questions answered by this tool:

- How can malware potentially enter your network?
- What type of file types can be send as attachments to the end user?
- What type of file types can be downloaded from a website by the user?

- Does your internet and mail protection software detect potential malware?
- Does your internet and mail protection software detect obfuscated malware?

How to perform a mail- and webfiltertest

- Step 1: Select the mail & web filter test



- Step 2: Select a client, make sure the checkbox for the mail- and web filter test is enabled and click save.

A screenshot of the 'New Campaign' form in the Lucy Security interface. The form includes a 'Name' field with 'Lucy Phishing Campaign', a 'Client' dropdown menu (highlighted with a red box), and a 'Setup Mode' section with four radio buttons: 'Expert Setup (Manual Configuration)', 'Start with Predefined Campaign Template', 'Start with Default Campaign Template', 'Risk Assessment', and 'Mail & Web Test' (selected and highlighted with a red box). Below these are checkboxes for 'Stop the Campaign Automatically', 'Pinned', and 'Delete Protection'. A 'Save' button is at the bottom.

- Step 3: Choose a sender email, from where the mails will be sent. Please choose a sender domain that points to LUCY and where an MX record exists (otherwise the emails will be flagged as spam). Alternatively, you can whitelist the sender domain. However, this only makes sense if the unlocking does not also refer to the mail attachments and lets them through unfiltered. As a recipient choose a mail account on a standard PC from the company you test. The best is to perform this test within a lab/test-pc.

Start with sending a plain text email and verify if it arrives. If the plain text email doesn't arrive, you do not need to proceed to the attachment tests. Try different methods to avoid ending up in spam

[Prevent SPAM issues](#)

Home / Campaigns / Mail and web / Base Settings

Mail and web

Campaign Status Not Started ▶

Summary

Base Settings

Reports

Advanced Settings

User Settings

Logs

Supervision Log

Message Log

Name Mail and web ⓘ

Scenario Mail & Web Test ⓘ

Sender Name Tester ⓘ

Sender email lucytest@lucysecurity.com ⓘ

Subject Test ⓘ

Recipient lucytest@lucysecurity.com Test ⓘ

☐ Disable Mail Test (web filter test only)

Save

- Step 4: Choose a domain (1), from where the files can be downloaded. Using an IP address is not recommended, as websites which run on IP's are generally blocked on most webfilters. Please use the [domain API from LUCY](#), if you shouldnt have a domain yet. Once you have selected a domain, please click on file list (2)

6 new templates available! [Download](#)

Mail & Web...

Scenario Status: Not Started ▶

Scenario Settings

Mail Settings

SSL Settings

File List 2

Template Mail & Web Test / English ⓘ [Change/Select Template](#)

Name Mail & Web Test

Landing Domain cloudspace24.services ⓘ

Subdomain mailfilter ⓘ

Languages English ⓘ

[+ Add](#)

Save

- Step 5: Select the categories you want to mail or download. You can select/deselect categories or single files.

File List

Scenario Status: Not Started



Scenario Settings

File List

☒ Encrypted Class 1 Files

☒ PDF & Office Exploits

☐ Dangerous File Types in archives

☐ Profanity

☒ Harmless Level 3 Files

☒ Harmless Macros

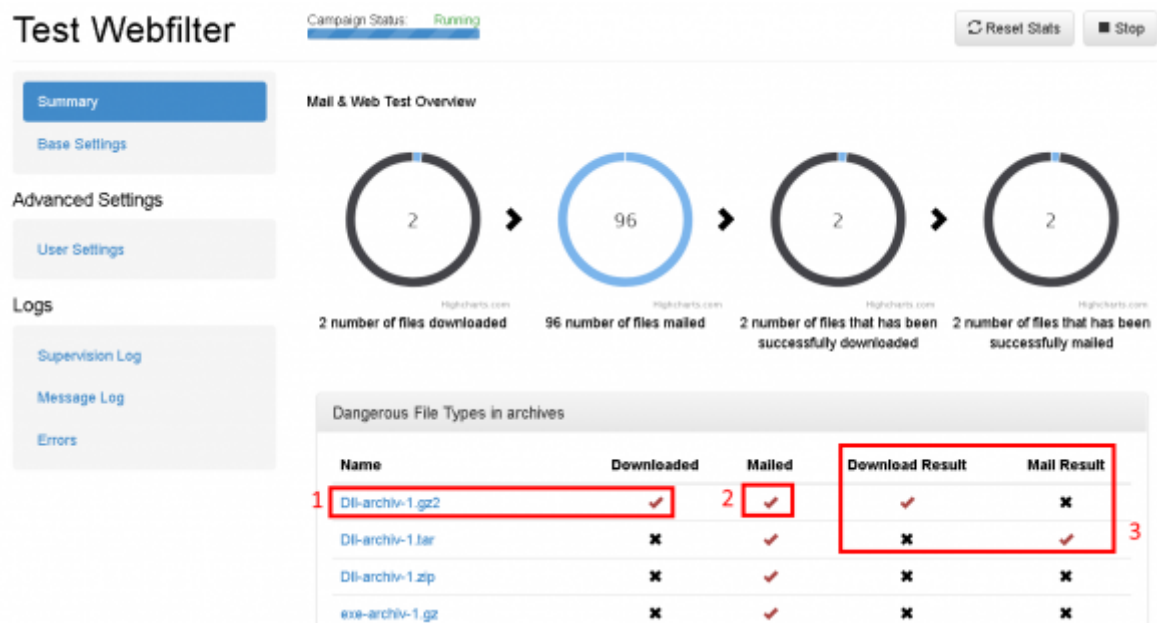
Macros are a legitimate way to automate some common tasks in Microsoft to download threats onto the PC. Macro malware usually hides in Microsoft documents are sent as spam email attachments, or inside ZIP files attached to emails. Macro's and verify if and what Macro action triggers a suspicious flag in the

- ☐ CreateExeDesktopandExecute.xls
- ☐ ExcelCommandButtonIpconfig.xls
- ☒ Excel_Portscanner.xls
- ☒ ExeutesCommandsInShellAndWriteFiles.doc
- ☒ Macro_that_runs_ipconfig_2010.docm
- ☒ MessageBox.doc
- ☒ OpenWebsite.doc
- ☒ OpenWebsite.xls
- ☒ WriteIPconfigDesktop.xls

☐ Use Obfuscation technique to hide malware

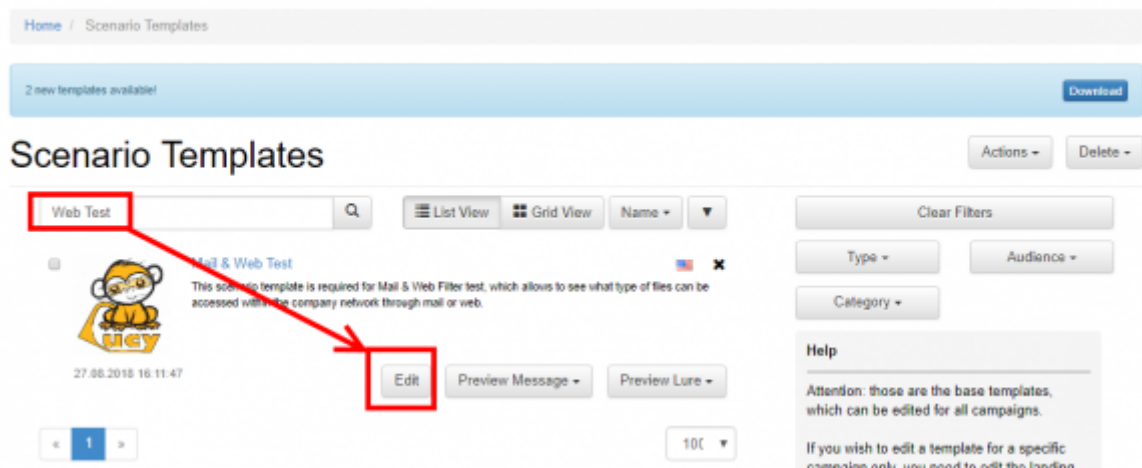
☒ Dangerous file types

- Step 6: Once you started the campaign, LUCY will send the recipients the selected files. Every file that has been sent will automatically be displayed as sent (2). But you still manually need to verify, if the email actually arrived and the attachment was included. If it was, you can click on the according cross next to the file (3). If you click on the file name (1), you will be able to download the file. Also here: the file shows as downloaded the moment you clicked that link. But you will need to manually confirm (3) that the file actually could be downloaded. As a result you will get a matrix that shows the infrastructure team, what type of code can get mailed and downloaded in a company environment.



How to configure the text of the test categories

Go to settings -> scenario templates and edit the mail and web filter test template:



Go to "file list" and then click on the "edit symbol:

Home / Scenario Templates / Mail & Web Test / File List

2 new templates available! [Download](#)

File List

Mime Types + New File + New Class

Edit

Search...

File List

Dangerous File Types in archives

Microsoft assigns a level of risk to every file attachment sent to you. Level 1 is considered unsafe. Level 2 is considered a moderate risk, and you won't be able to open those files directly (e.g. in Outlook). Instead, you have to save the files to disk, and then you'll be able to open them. A packet files is a file in a compressed format. Many operating systems and applications contain commands that enable you to pack a file so that it takes up less memory. Packed files can be read only by the program that packed them because they contain special codes. In this test, we will verify if dangerous file types which are packed, can be send via mail or downloaded by client. Such file formats may be:

DI-archiv-1.gz2	application/x-bzip2	✖
DI-archiv-1.tar	application/x-tar	✖

Now you can edit the text of this text class:

Home / Scenario Templates / Mail & Web Test / File List / Edit File Class

2 new templates available! [Download](#)

Edit File Class

Edit

File List

Name Dangerous File Types in archives

Description Microsoft assigns a level of risk to every file attachment sent to you. Level 1 is considered unsafe. Level 2 is considered a moderate risk, and you won't be able to open those files directly (e.g. in Outlook). Instead, you have to save the files to disk, and then you'll be able to open them. A packet files is a file in a compressed format. Many operating systems and applications contain commands that enable you to pack a file so that it takes up less memory. Packed files can be read only by the program that packed them because they contain special codes. In this test, we will verify if dangerous file types which are packed, can be send via mail or downloaded by client. Such file formats may be:

[Save](#)

Change the payload

How to configure the existing payloads of the tests

1. Go to settings -> scenario templates and edit the mail and web filter test template
2. Go to "file list"
3. Click on the link of the file you want to edit:

File List

Mime Types+ New File+ New Class

EditFile List

Search...

Dangerous File Types in archives

Microsoft assigns a level of risk to every file attachment sent to you. Level 1 is considered unsafe. Level 2 is considered a moderate risk, and you won't be able to open those files directly (e.g. in Outlook). Instead, you have to save the files to disk, and then you'll be able to open them. A packet files is a file in a compressed format. Many operating systems and applications contain commands that enable you to pack a file so that it takes up less memory. Packed files can be read only by the program that packed them because they contain special codes. In this test, we will verify if dangerous file types which are packed, can be send via mail or downloaded by client. Such file formats may be:RARZIPGZ7Z

Dll-archiv-1.gz2	application/x-bzip2	✕
Dll-archiv-1.tar	application/x-tar	✕
Dll-archiv-1.zip	application/zip	✕
exe-archiv-1.gz	application/x-gzip	✕
exe-archiv-1.gz2	application/x-bzip2	✕

- You can now upload/download the file:

Home / Scenario Templates / Mail & Web Test / File List / Edit File

2 new templates available!Download

EditFile List

NameDll-archiv-1.gz2

Mime Typeapplication/x-bzip2

ClassDangerous File Types in archives

FileUploadDownload

Save

(c) 2018 LUCY Security

Additional settings

Home / Scenario Templates / Mail & Web Test / File List

2 new templates available!Download

File List

Mime Types+ New File+ New Class

EditFile List

Search...

Dangerous File Types in archives

Profanity

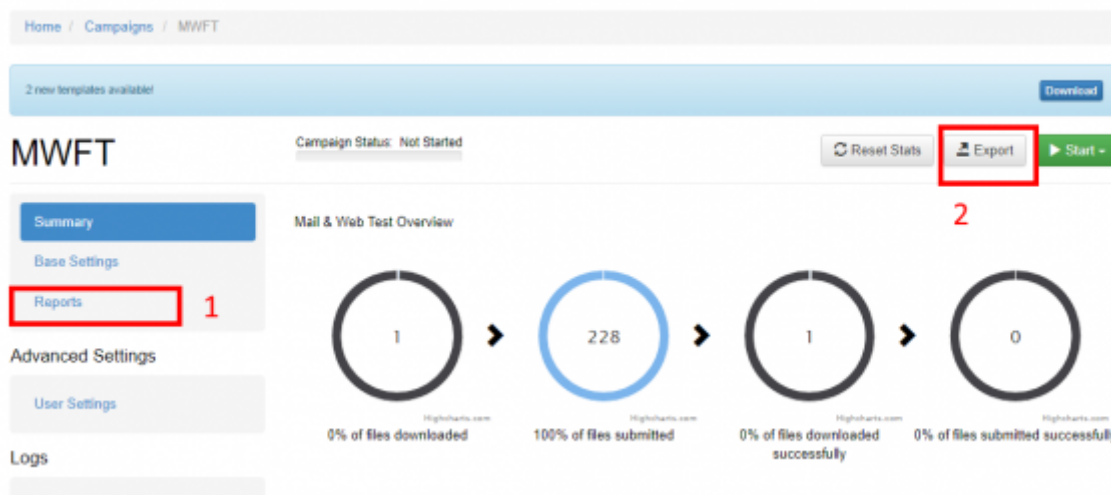
Harmless Level 3 Files

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

1) Create new file: click on new file 2) Create new class: click on new class 3) Change the order of the tests: select the category, press your left mouse button and move the category in your browser

How to create reports or export the data

You can export the results to CSV or XML using the export button (1) or create a report using the report button (2):



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

Permanent link:
https://wiki.lucysecurity.com/doku.php?id=mail_and_webfilter_test&rev=1631782838

Last update: **2021/09/16 11:00**

