# 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.

Home / Campaigns / MWT / Base Se	ttings / Mail & Web Test / File List
File List	o Status: Not Started
Scenario Settings	Dangerous File Types in archives
File List	☑ Profanity
	C Harmless Level 3 Files
	Encrypted Class 1 Files
	PDF & Office Exploits
	E Harmiess Macros
	Macros are a legitimate way to automate some common tasks in Microsoft Office. However, matware can also use this functionality to download threats onto the PC. Macro matware usually hides in Microsoft Word or Microsoft Excel documents. These maticious documents are sent as spam email attachments, or inside ZIP files attached to spam emails. In this test, we use only hamiless Macro's and verify if and what Macro action triggers a suspicious flag in the AV or IDS.
	Excel_Portscanner.xis     CreateExeDesktopandExecute.xis
	✓ WritelPconfigDesktop.xls ✓ OpenWebsite.xls
	ExeutesCommandsinShellAndWitteFiles.doc
	OpenWebsile.doc     Macro_that_runs_ipconfig_2010.docm
	MessageBox.doc
	ExcelCommandButtonlpconfig.xis
	Excel_Portscanner.xis
	CreateExeDesktopandExecute.xts
	WritelPconfigDesktop.xls
	OpenWebsile.xls
	C ExeutesCommandsinShellAndWriteFiles.doc
	C OpenWebsite.doc
	Macro_that_runs_ipconfig_2010.docm
	MessageBox.doc
	ExcelCommandButtonIpconfig.xis
	Use Obfuscation technique to hide malware
	☑ Dangerous file types

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.

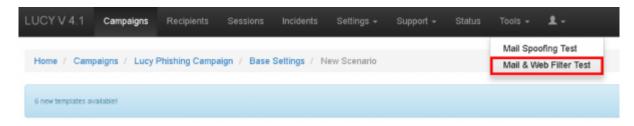
#### Main Questions answered by this tool:

- 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.

Home / Campaigns / New Campaign		
6 newtemplates available!		Download
New Campa	Campaign Status: Not Started	
New Campaign	Name       Lucy Phishing Campaign         Client       Lucy Test         Setup Mode       Expert Setup (Manual Configuration) •         Setup Wizard •       •         Risk Assessment •       •         Start with Predefined Campaign Template •       •         Mail & Web Test •       •         Søve       •	
(c) by LUCY Security 2018		

 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.

UCYV4.1 Campaigns Red	pients Sessions inc	idents Settings - Support - Status Tools	· ±·	
Home / Campaigns / Lucy Phishin	ng Campaign (1) / Base S	ettings		
6 new templates available)				Download
ucy Phishi	Campaign Status: Not S	Started		
Summary	Scenario	Mail & Web Test	· 0	
Base Settings	Sender Name	Mail Filter Test	θ	
dvanced Settings	Sender Email	test@existingdomain-which-is-not-SPF-protected.com	θ	
User Settings	Recipient	testmali@testlaptop.com Test Lab User	9	
ogs		Disable Mail Test (web filter test only)		
Supervision Log		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 newtemplates available!				Downlo
/lail & Web	Scenario Status: Not Started	•		
Scenario Settings Mail Settings	Template Name	Mail & Web Test / English ChangerSelect Template Mail & Web Test		
SSL Settings	Landing Domain	cloudspace24.services		
File List 2	1 Subdomain	maifiter	0	
	Languages	English		
		Save		

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

Scenario Settings	Dangerous File Types in archives
File List	Profanity
	Harmless Level 3 Files
	Encrypted Class 1 Files
	PDF & Office Exploits
	Harmless Macros
	Macros are a legitimate way to automate some common tasks in Microsoft Office. However, malware can also use this functionality to download threats onto the PC. Macro malware usually hides in Microsoft Word or Microsoft Excel documents. These malicious documents are sent as spam email attachments, or inside ZIP files attached to spam emails. In this test, we use only harmless Macro's and verify if and what Macro action triggers a suspicious flag in the AV or IDS.
	Excel_Portscanner.xis
	CreateExeDesktopandExecute.xts
	WritelPconfigDesktop.xls
	Open/Website.xls
	ExeutesCommandsinShellAndWriteFiles.doc
	OpenWebsite.doc     Macro that runs ipconfig_2010.docm
	MastageBox.doc
	ExcelCommandButtonipconfig.xis

• 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 attachement 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.

Test Webfilter	Campaign Status: Running			C R	esel Stats	Stop
Summary Base Settings	Mali & Web Test Overview					
Advanced Settings		96	, (	2) <b>)</b> (	2	
User Settings	$\bigcirc$	$\bigcirc$		ノ	$\bigcirc$	·
Logs	2 number of files downloaded	96 number of files mailed		es that has been 2 numb	er of files that has	been
Supervision Log			successfult	y downloaded s	uccessfully mailed	
Message Log	Dangerous File Types in a	rchives				
Errors	Name	Downloaded	Mailed	Download Result	Mail Result	
	1 DII-archiv-1.gz2	×	2 🗸	1	×	
	DII-archiv-1.tar	×	×	×	1	3
	DII-archiv-1.zip	×	×	×	×	
	exe-archiv-1.gz	×	1	×	×	

# How to configure the text of the test categories

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

Home / Scenario Templates		
2 new templates available!		Download
Scenario Templates		Actions + Delete -
Web Test Q IIIst View III Grid View Name •	Clea	r Filters
This scenare template is required for Mail & Vieb Filter test, which allows to see what type of files can be accessed with the company network through mail or web.	Category +	Audience +
27.68.2018 16.11.47 Edit Preview Message - Preview Lure -	- Help	e base templates,
« 1 »	<ul> <li>which can be edited for</li> <li>If you wish to edit a ter</li> </ul>	mplate for a specific

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

			_
2 new templates available!			Download
File List		III Mime Types + New File	+ New Clas
Edit	Search		0
File List	Dangerous File Types in archives		► ©×
	moderate risk, and you won't be able to op then you'll be able to open them. A packet contain commands that enable you to pact that packed them because they contain sp	le attachment sent to you. Level 1 is considered unsafe. Level 2 is considered those files directly (e.g. in Outlook). Instead, you have to save the file. (files is a file in a compressed format. Many operating systems and appli- k a file so that it takes up less memory. Packed files can be read only by ecial codes.cbn-cbn- In this test, we will verify if dangerous file types while led by client. Such file formats may be: cli>	s to disk, and cations the program ich are
	Dil-archiv-1.gz2	application/x-bzip2	×

Now you can edit the text of this text class:

2 rev lengkates available:			Descho
Edit File Class			
Edit	Name	Dangerous File Types in archives	
File List	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 (a g. in Cudiod). 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 spacial codes scho-cho: In this test, we will verify if dangerous file types which are packed, can be send via mail or downloaded by client. 	•

### 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:

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 consimoderate risk, and you won't be able to open those files directly (e.g. in Outlook). Instead, you have to save the filt then you'll be able to open them. A packet files is a file in a compressed format. Many operating systems and appoint that packed them because they contain special codes 	٩
Microsoft assigns a level of risk to every file attachment sent to you. Level 1 is considered unsafe. Level 2 is considered in the you'll be able to open these files directly (e.g. in Outlook). Instead, you have to save the filt then you'll be able to open them. A packet files is a file in a compressed format. Many operating systems and app contain commands that enable you to pack a file so that it takes up less memory. Packed files can be read only be that packed them because they contain special codes. dispression of the send via mail or downloaded by client. Such file formats may be: 	
moderate risk, and you won't be able to open those files directly (e.g. in Outlook). Instead, you have to save the filten you'll be able to open them. A packet files is a file in a compressed format. Many operating systems and app contain commands that enable you to pack a file so that it takes up less memory. Packed files can be read only b that packed them because they contain special codes. shr>chr> In this test, we will verify if dangerous file types w packed, can be send via mail or downloaded by client. Such file formats may be: di>CAB	© ×
DiFarchiv-1.gz2 application/x-ozip2	ry the program which are
Dil-archiv-1.tar application/x-tar	×
Dil-archiv-1.zip application/zip	×
exe-archiv-1.gz application/x-gzlp	×
exe-archiv-1.gz2 application/x-bzlp2	×

• You can now upload/download the file:

2 new temptates available/				Downlo
dit File				
Edt	Name	Dil-archiv-1.gz2		
File List	Mime Type	application/w-bzip2		
	Class	Dangerous File Types in archives	•	
	File	Upload Download		
		Save		

### **Additional settings**

Home / Scenario Templates	/ Mail & Web	Test / File List		
2 new templates available!				Download
File List			III Mime Types + New File	+ New Class
Edit		Search	1	2 a
File List	3	Dangerous File Types in archives		© ×
		Profanity		© ×
		Harmless Level 3 Files		© ×

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):

Home / Campaigns / MWFT		
2 new templates available!		Devrilad
MWFT	Campaign Status: Not Started	C Reset Stats A Expert Start -
Summary	Mail & Web Test Overview	2
Reports 1 Advanced Settings	( ) <b>,</b>	
User Settings		Aghlaria area Aghlaria area Aghlaria area
Logs	0% of files downloaded	100% of files submitted 0% of files downloaded 0% of files submitted successfully successfully

