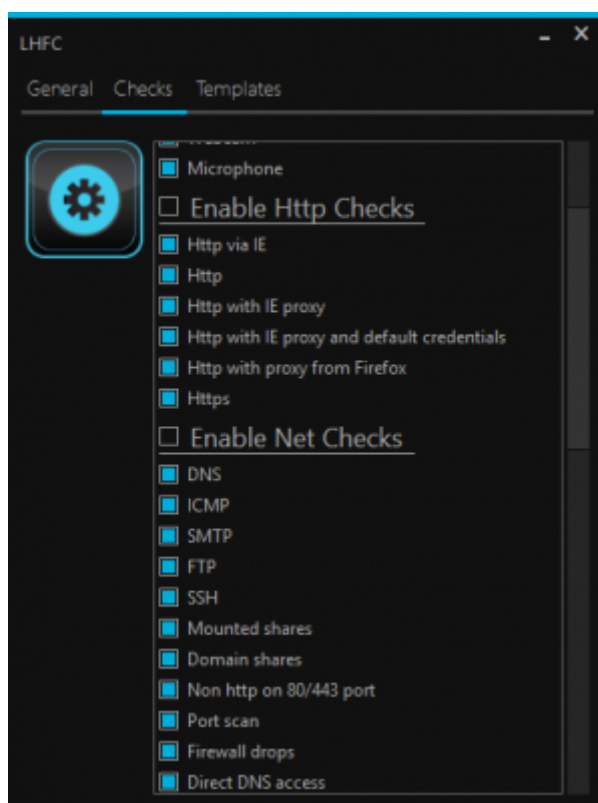


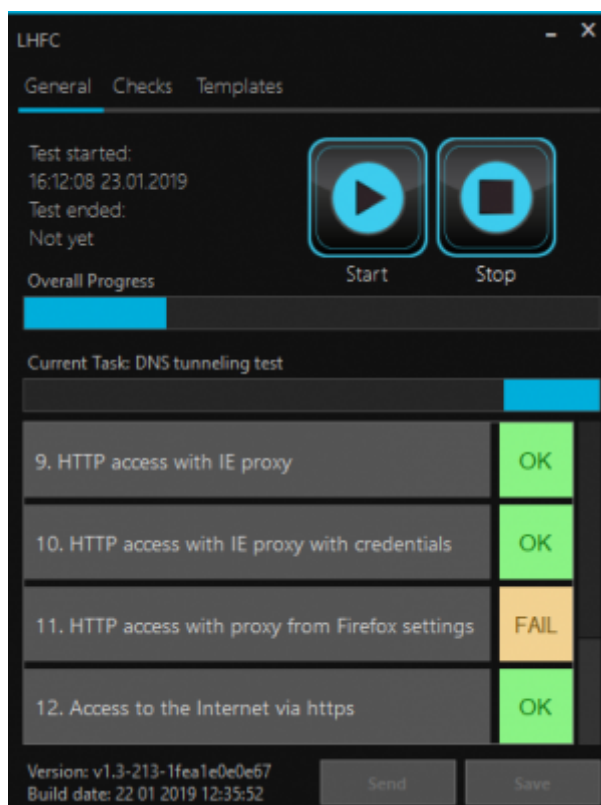
Technical tests without involving employees

LUCY offers the possibility to carry out technical tests without the involvement of employees. These are tests of the infrastructure (network, Windows client etc.).

LHFC - Malware testing Simulation

You have invested time, effort, and money in defenses. However, employees may still execute a malicious file. How do you know your defenses will work? To reduce the risk from malware coming into your environment, you need safe and effective ways to test your systems. This is where LUCY's Malware Simulation Toolkit (LHFC) comes in place. LHFC is an advanced malware simulation suite capable of emulating various threat simulations equivalent to many of the tools employed by hackers. More info about this test can be found [here](#).



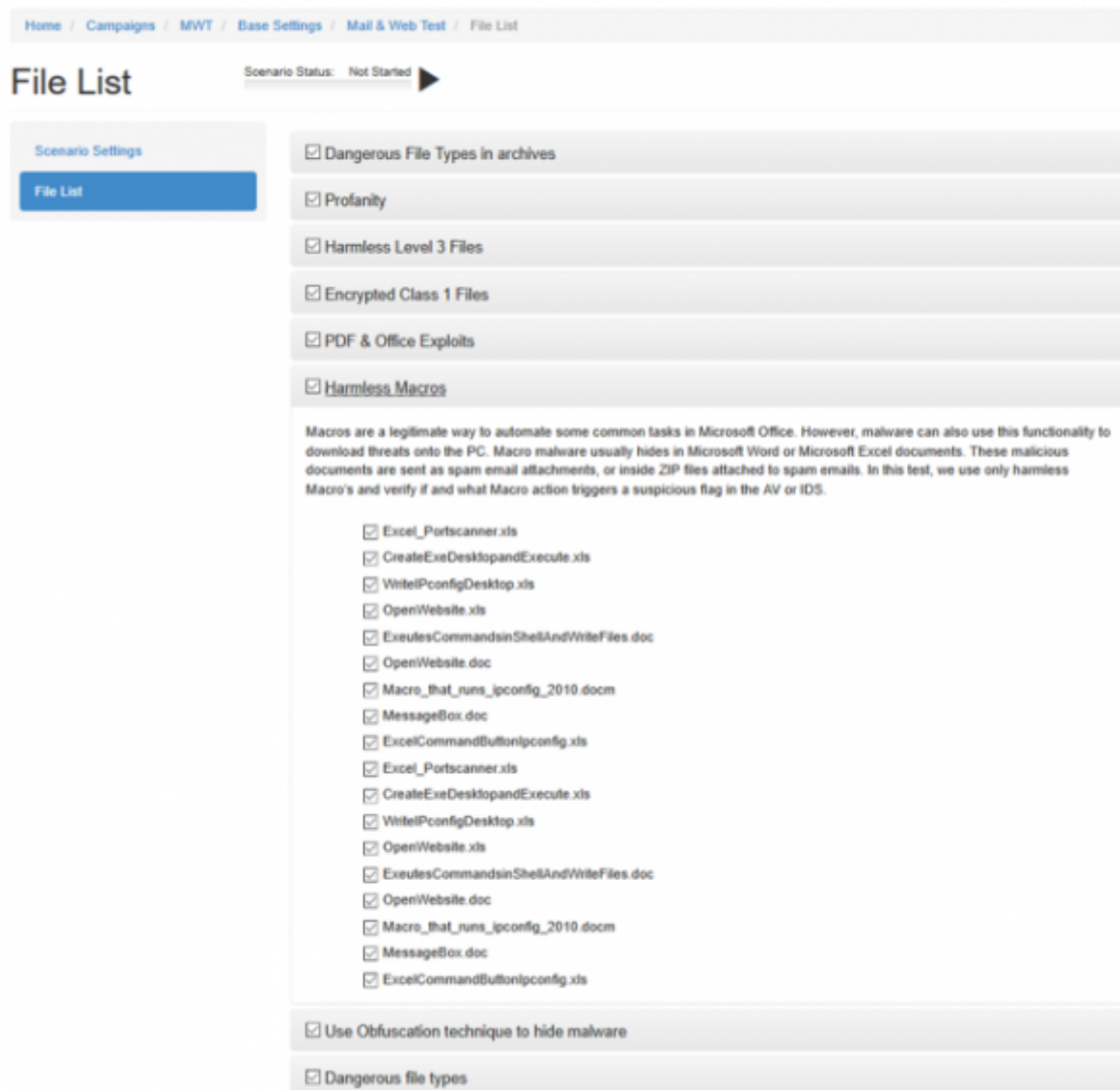


Main Questions answered by this tool:

- Does your AV detect known Malware downloads?
- What happens if an employee falls for a real attack?
- Is your SIEM able to trigger activities from this tool?
- Is Malware able to modify System Settings?
- Is Malware able to communicate to external servers?
- Can Malware access sensitive data on the local host or your intranet?

Mail and Webfilter Test

The Email and Internet malware protection test checks whether the implemented security measures are sufficient to defend against an unstructured or structured malware attack via the e-mail infrastructure or internet infrastructure. 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. More info about this test can be found [here](#).



Main Questions answered by this test:

- 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?

Vulnerable Browser | Vulnerable Client detection

When running a campaign, LUCY will tell you based on the user agent, if there is any vulnerability within the browser or plugins. A User Agent is a short string that web browsers and other applications send to identify themselves to web servers. A user agent string contains the following information: Mozilla/[version] ([system and browser information]) [platform] ([platform details]) [extensions]. Unfortunately, most browsers falsify part of their User-Agent header in an attempt to be compatible with more web servers. LUCY also is only enumerate major versions (like IE 11) but not minor versions which would show the actual patch status, some results might be false positives. Example: if you don't use the latest IE (e.g. IE10) we will query the CVE database and present all vulnerabilities for IE10 (http://www.cvedetails.com/vulnerability-list/vendor_id-26/product_id-9900/version_id-138705/).

But that does not mean the IE is not patched. This only displays all possible vulnerabilities for this browser version. Within the campaign statistics the vulnerable clients are displayed with an exclamation mark:

Home / Campaigns / TEST DL STATS / Statistics / Recipients

TEST DL... Campaign Status: Running

Scenario Plugin OS UA

Summary

User Settings

Statistics

Collected Data

Recipients

Awareness Website

Name	OS	UA	Plugins	Succ	Train
! Oi TEST WORD	Windows 7	Firefox 49		✓	-
Test TEST WORD	-	-		-	-

< 1 >

10

Additionally to the user agent, you can also enable an advanced informagtion gaterihing script to determine, what an external webserver can find out about you. The advanced IG scripts are enabled within the campaign scenario settings:

Landing Domaincloudspace24.services

Subdomainig

☐ Anonymous Mode

☐ Track Opened Emails

☐ Send Link to Awareness Website Automatically

☒ Advanced Information Gathering

- ☒ Browser Details
- ☒ Firebug Information
- ☒ Popup Blocker
- ☒ Geo Location
- ☒ Social Network
- ☒ Proxy

Success ActionData Submit

Collect DataPartial

☐ Double Barrel Attack

The results are under the campaign statistics (recipients):

Base Settings

Awareness Settings

Schedule

Recipients

Advanced Settings

User Settings

Custom Fields

Reminders

Logs

Supervision Log

Message Log

Errors

Training Sent Reported

05.06.2018 00:15:55

Success Rate

53.57%

Click Rate

60.71%

Clicks

1

Successful Attack Trained

✓

Downloaded Files

file.exe

OS

Windows 10

Browser

Chrome 66.3359

IP

178.197.235.193

Vulnerable Applications (0)

N/A

Custom Fields

☒ reported email

nope

Attacked:

20

Success:

12

Trained:

5

Reported Mails:

3

Additional Information

Browser Version

5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.181 Safari/537.36

Browser Language

en-US

Browser Platform

Win32

Window Size

1536 x 824

Cookies Enabled

✓

WebRTC

✓

VBScript

✓

Quicktime

✓

RealPlayer

✓

ActiveX

✓

Java

✓

Proxy

✓

Popup Blocker

✓

Social Networks

N/A

Spoofing Test

The spoofing test will verify, if an anonymous user from the internet can send a spoofed email on behalf of another domain. The test can be found under "tools":

Tools

Sessions

Mail Spoofing Test

Mail & Web Filter Test

File Browser

Home / Mail Spoofing

Mail Spoofing

Procedure:

1. Step 1: Enter the domain you are trying to spoof
2. Step 2: Enter a mail recipient, where the spoofed email should get sent to
3. Step 3: After a short time you will see if the spoofing test worked

Mail Spoofing

1

Domain

microsoft.com

Start Test

Download

2

Recipient Email

oliver@lucysecurity.com

X

Console Window

220 BL2NAM06FT016.mail.protection.outlook.com Microsoft ESMTTP MAIL. Service ready at Fri, 8 Jun 2018 13:01:04 +0000
EHLO microsoft.com
250-BL2NAM06FT016.mail.protection.outlook.com Hello [193.25.100.47]
250-SIZE 157286400
250-PIPELINING
250-DSN
250-ENHANCEDSTATUSCODES
250-STARTTLS
250-8BITMIME
250-BINARYMIME
250-CHUNKING
250-SMTPUTF8
MAIL FROM:
250 2.1.0 Sender OK
RCPT TO:
550 5.7.64 Tenant/Attribution; Relay Access Denied [BL2NAM06FT016.Eop-nam06.prod.protection.outlook.com]
3 Completed! Mail Spoofing is impossible.

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

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

Last update: 2020/01/13 14:47

