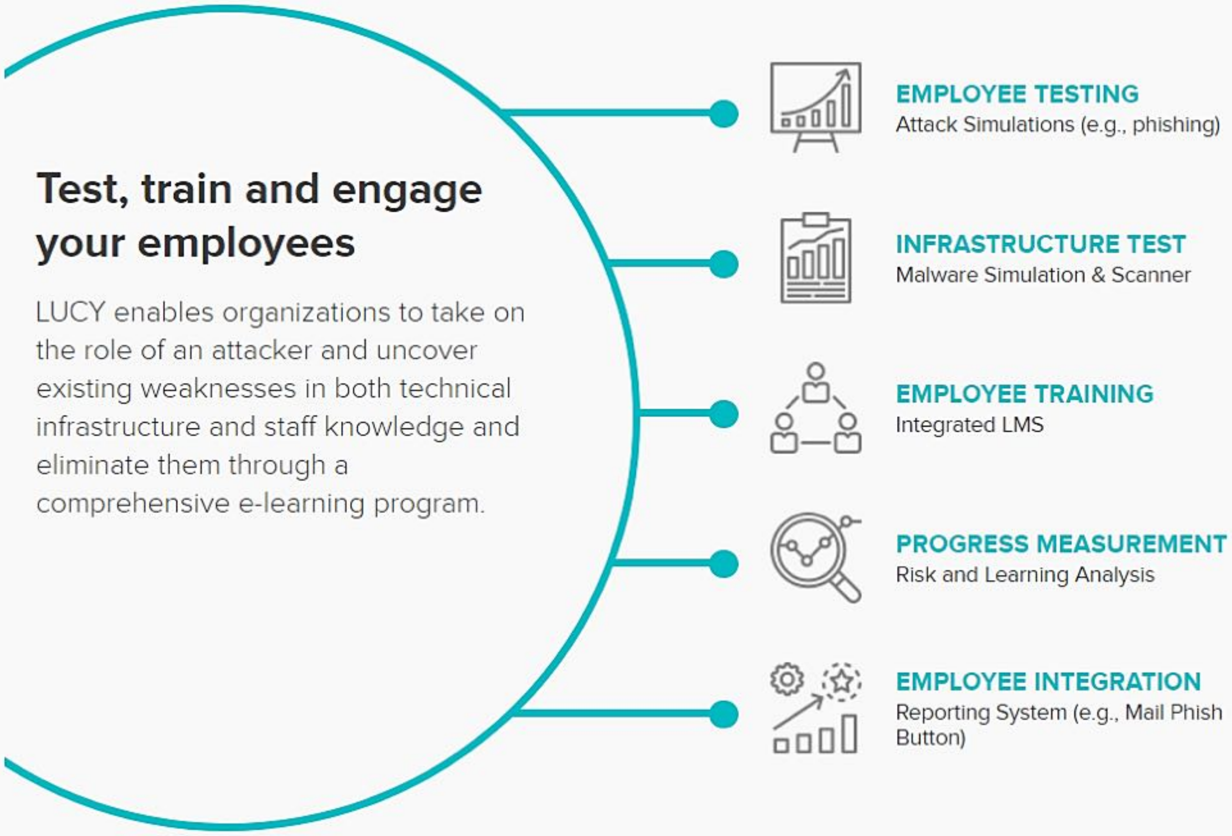
LUCY WHITEPAPER

WHAT IS LUCY?



Test, train and engage your employees

LUCY enables organizations to take on the role of an attacker and uncover existing weaknesses in both technical infrastructure and staff knowledge and eliminate them through a comprehensive e-learning program.

EMPLOYEE TESTING
Attack Simulations (e.g., phishing)

INFRASTRUCTURE TEST
Malware Simulation & Scanner

EMPLOYEE TRAINING
Integrated LMS

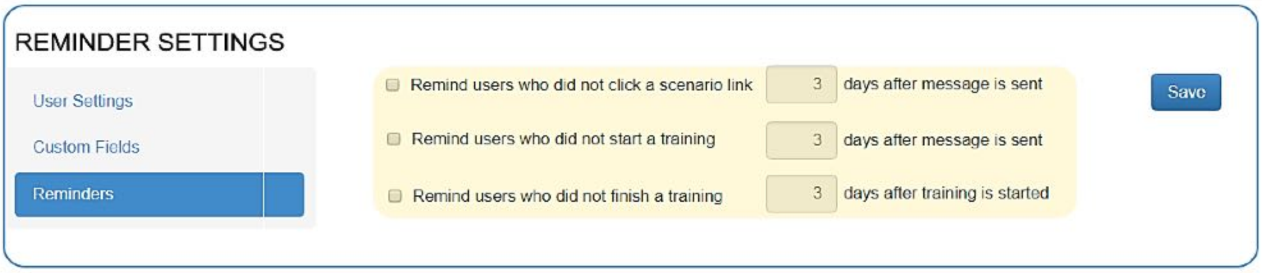
PROGRESS MEASUREMENT
Risk and Learning Analysis

EMPLOYEE INTEGRATION
Reporting System (e.g., Mail Phish Button)

All Rights Reserved 2019

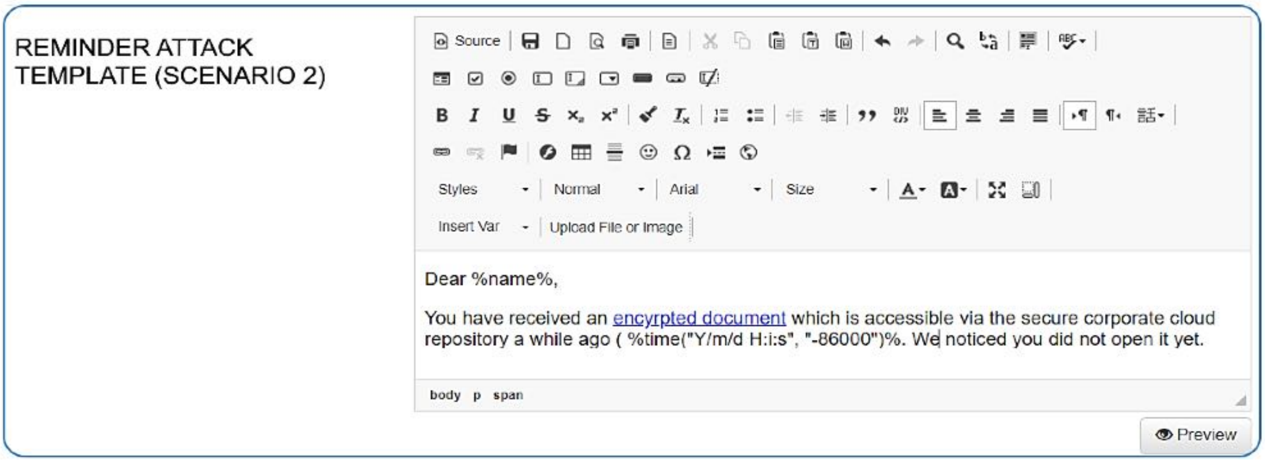
GENERAL FEATURES

- **REMINDERS:** Reminder templates can be used to automatically resend messages to users who have not clicked on an attack link or a training course after a custom period of time.



REMINDER SETTINGS

□ Remind users who did not click a scenario link	3	days after message is sent
□ Remind users who did not start a training	3	days after message is sent
□ Remind users who did not finish a training	3	days after training is started

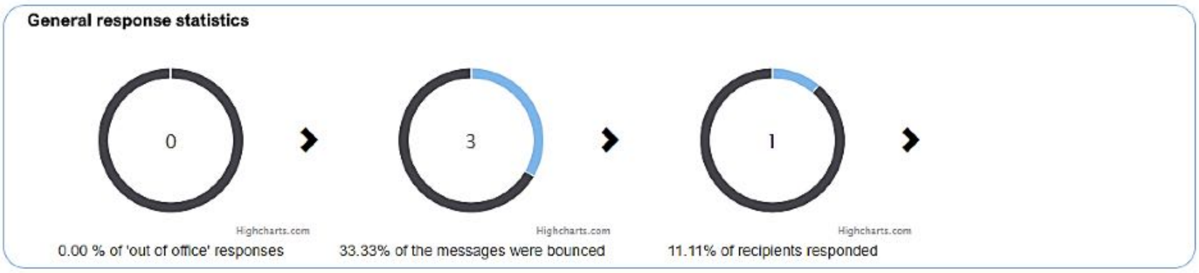


REMINDER ATTACK TEMPLATE (SCENARIO 2)

Dear %name%,

You have received an encyrpted document which is accessible via the secure corporate cloud repository a while ago (%time("Y/m/d H:i:s", "-86000")%. We noticed you did not open it yet.

- **RESPONSE DEDECTION:** The automatic response detection makes it possible to define and analyse automatic e-mail responses (e.g., out of office) as well as mail delivery errors (e.g., user unknown) within the campaign.

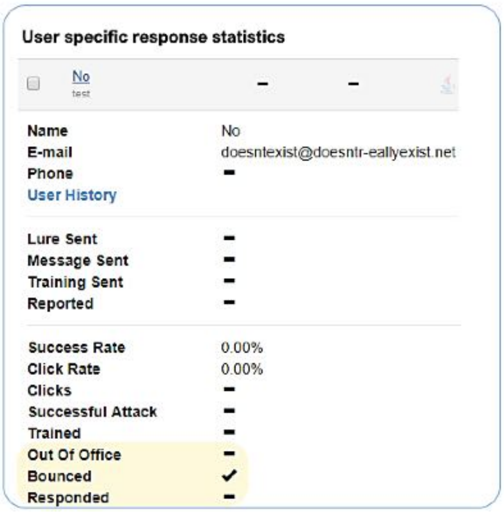


General response statistics

0.00 % of 'out of office' responses

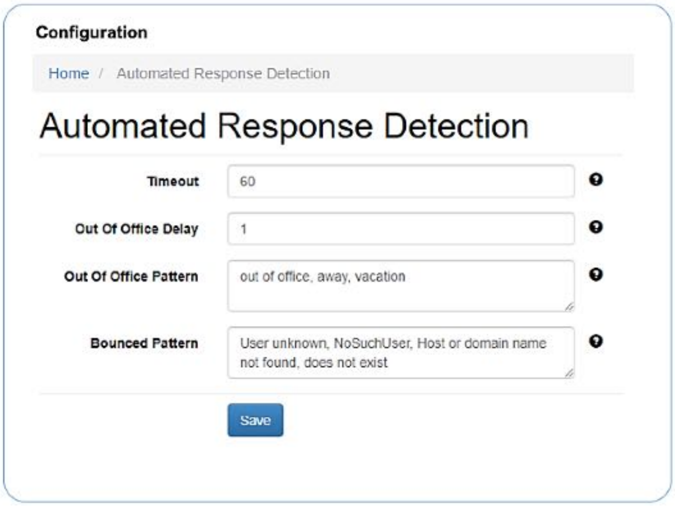
33.33% of the messages were bounced

11.11% of recipients responded



User specific response statistics

□ No test	– –
Name	No
E-mail	doesntexist@doesntr-eallyexist.net
Phone	–
User History	
Lure Sent	–
Message Sent	–
Training Sent	–
Reported	–
Success Rate	0.00%
Click Rate	0.00%
Clicks	–
Successful Attack	–
Trained	–
Out Of Office	–
Bounced	✓
Responded	–



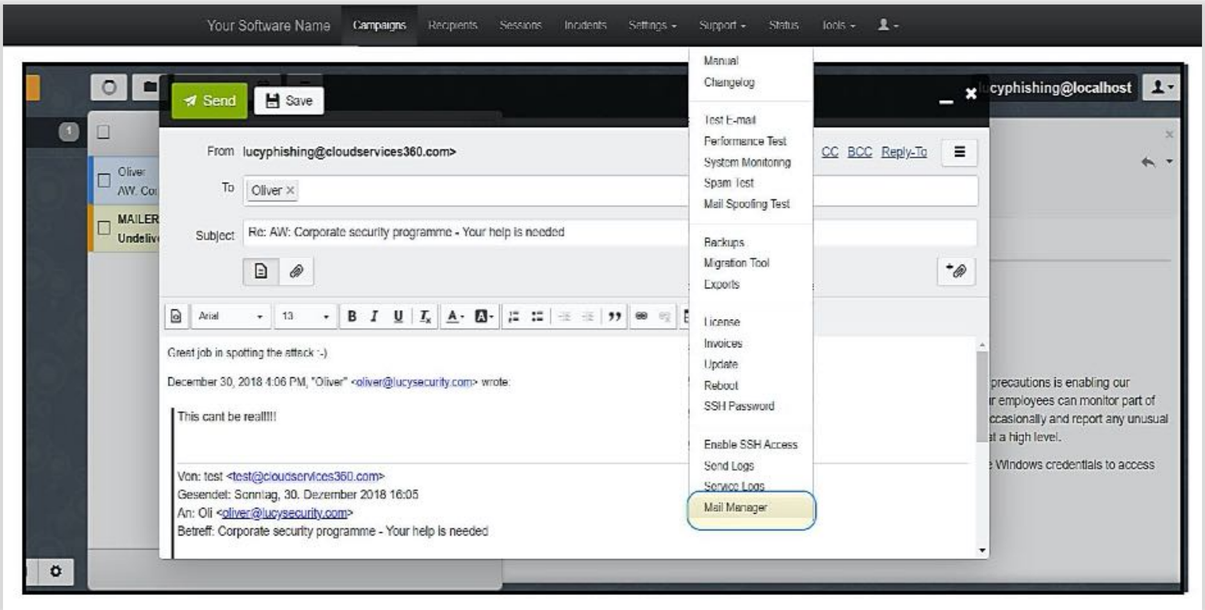
Configuration

Home / Automated Response Detection

Automated Response Detection

Timeout	60
Out Of Office Delay	1
Out Of Office Pattern	out of office, away, vacation
Bounced Pattern	User unknown, NoSuchUser, Host or domain name not found, does not exist

- **FULL MAIL COMMUNICATION CLIENT:** A built-in messaging platform allows the LUCY admin to communicate interactively with the recipients inside or outside the LUCY campaigns. All e-mails are archived and can be evaluated.



From lucyphishing@cloudservices360.com>

To Oliver ×

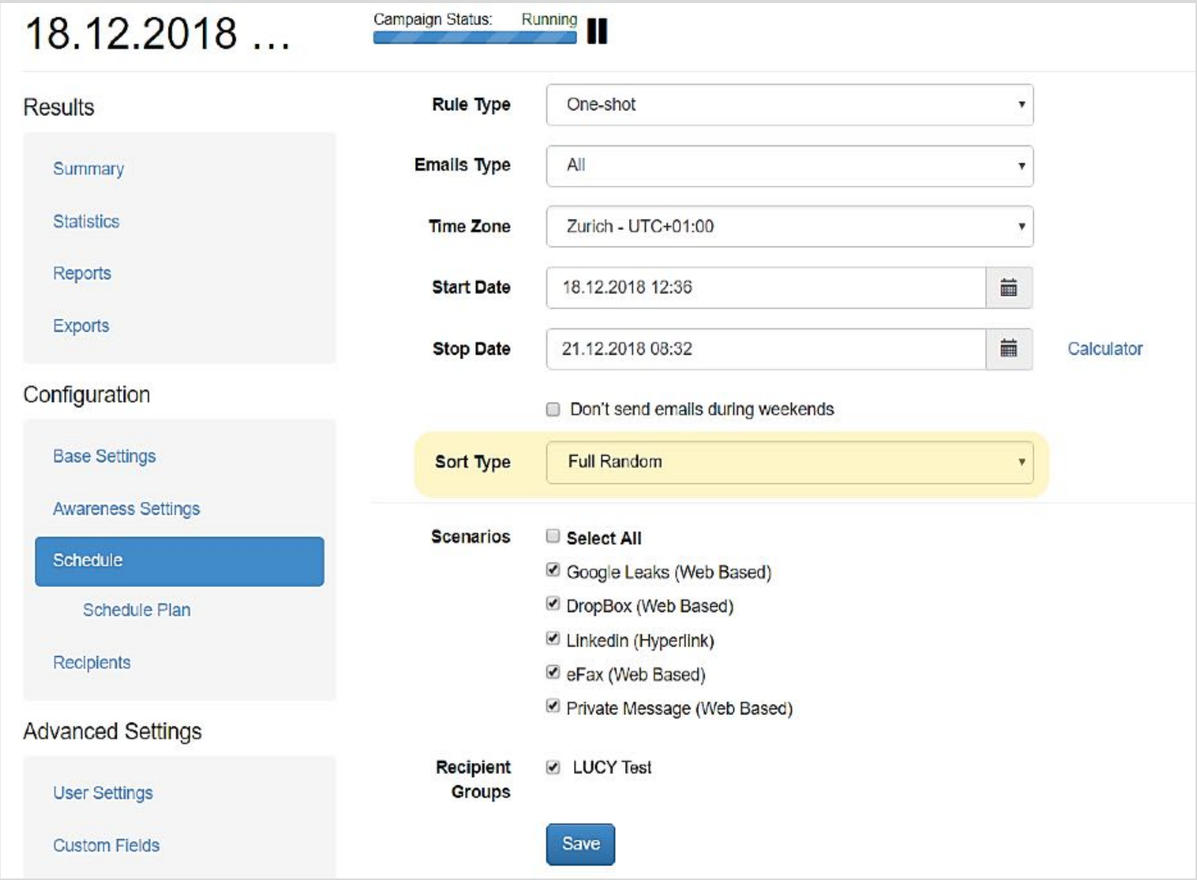
Subject Re: AW: Corporate security programme - Your help is needed

Great job in spotting the attack :-)

December 30, 2018 4:06 PM, "Oliver" <oliver@lucysecurity.com> wrote:

> This cant be real!!!!
>
> Von: test <test@cloudservices360.com>
> Gesendet: Sonntag, 30. Dezember 2018 16:05
> An: Oli <oliver@lucysecurity.com>
> Betreff: Corporate security programme - Your help is needed

- **Scheduler Randomization:** Raising employee awareness at random is the key factor for effective and sustainable awareness within the organization. Randomly sending many concurrent campaigns is one of the best means of training employees.



Campaign Status: Running

Rule Type: One-shot

Emails Type: All

Time Zone: Zurich - UTC+01:00

Start Date: 18.12.2018 12:36

Stop Date: 21.12.2018 08:32

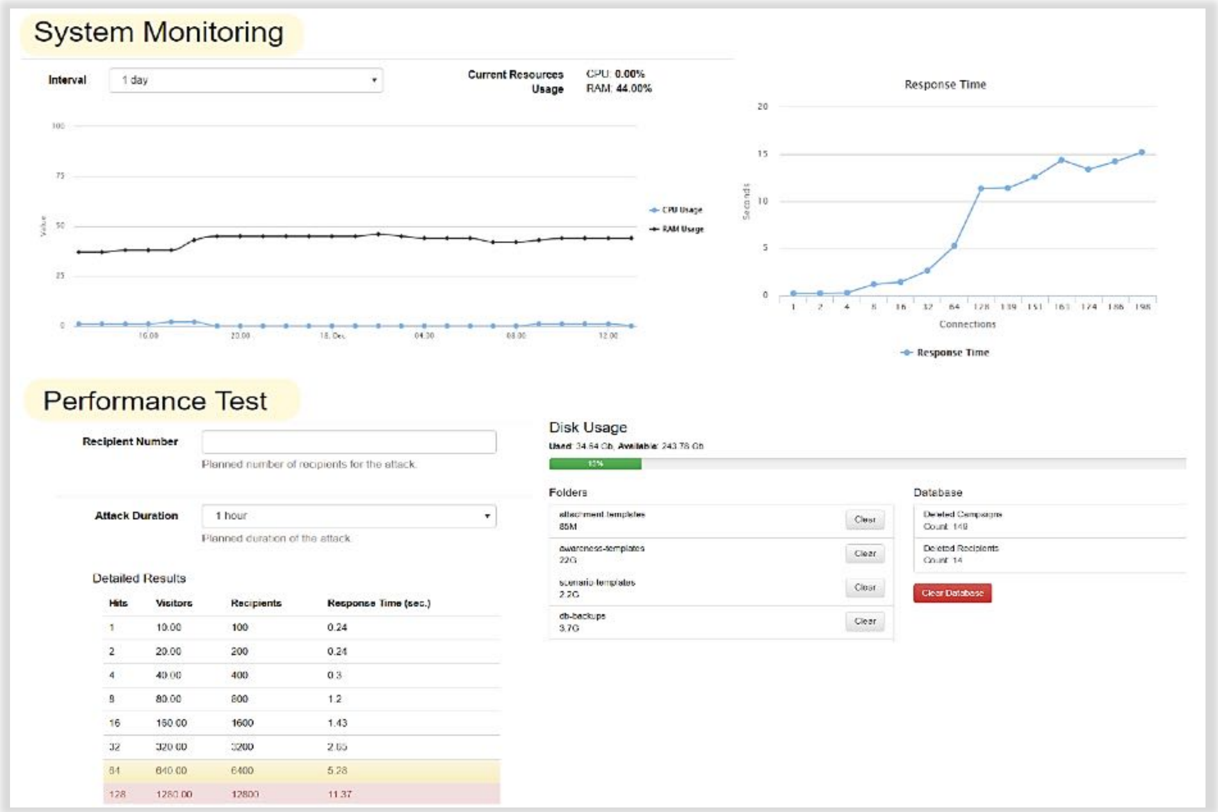
□ Don't send emails during weekends

Sort Type: Full Random

Scenarios:
- □ Select All
- ☑ Google Leaks (Web Based)
- ☑ DropBox (Web Based)
- ☑ LinkedIn (Hyperlink)
- ☑ eFax (Web Based)
- ☑ Private Message (Web Based)

Recipient Groups: ☑ LUCY Test

- **Performance tools**: LUCY smart routines adapt the server installation to the given resources. Applications Server, DBMS Sizing, Memory and CPU usages are calculated during installation or during operations. You can scale a single, cloud-based LUCY installation for 400,000+ users.



System Monitoring

Interval: 1 day

Current Resources Usage: CPU: 0.00% RAM: 44.00%

Performance Test

Recipient Number: Planned number of recipients for the attack.

Attack Duration: 1 hour — Planned duration of the attack.

Detailed Results

Hits	Visitors	Recipients	Response Time (sec.)
1	10.00	100	0.24
2	20.00	200	0.24
4	40.00	400	0.3
8	80.00	800	1.2
16	160.00	1600	1.43
32	320.00	3200	2.65
64	640.00	6400	5.28
128	1280.00	12800	11.37

Disk Usage

Used: 34.64 Gb, **Available:** 243.78 Gb

Folders

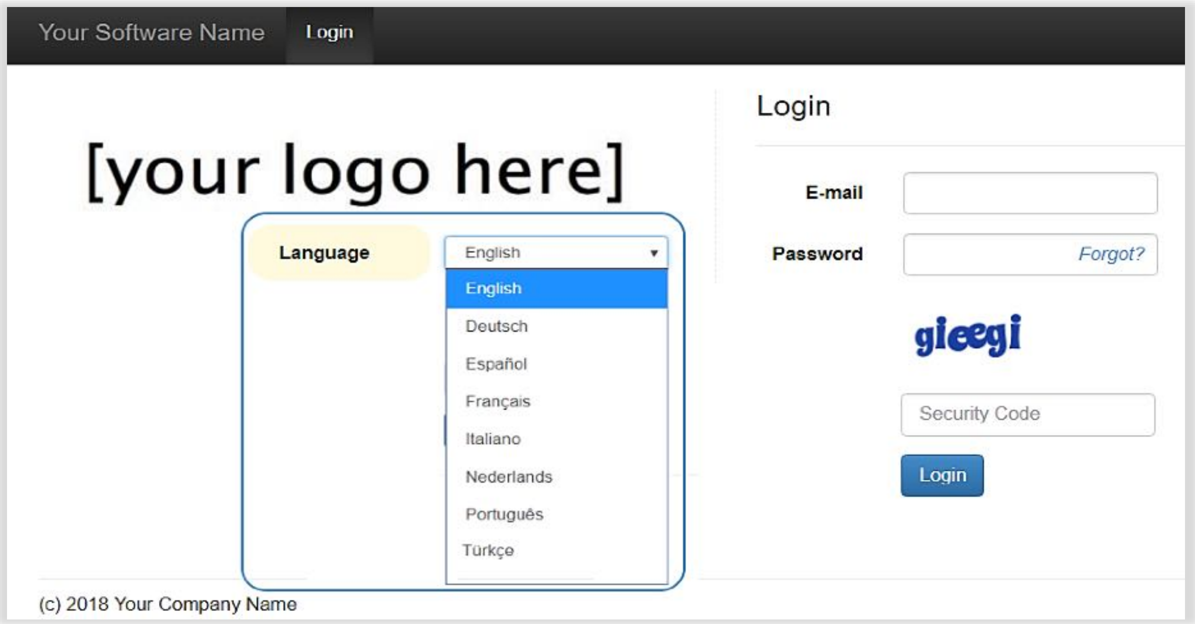
attachment-templates 85M	Clear
awareness-templates 22G	Clear
scenario-templates 2.2G	Clear
db-backups 3.7G	Clear

Database

Deleted Campaigns
Count: 149

Deleted Recipients
Count: 14

- **Multilingual admin interface**: The LUCY admin interface is available in different languages and can be translated into other languages on request.



Language: English

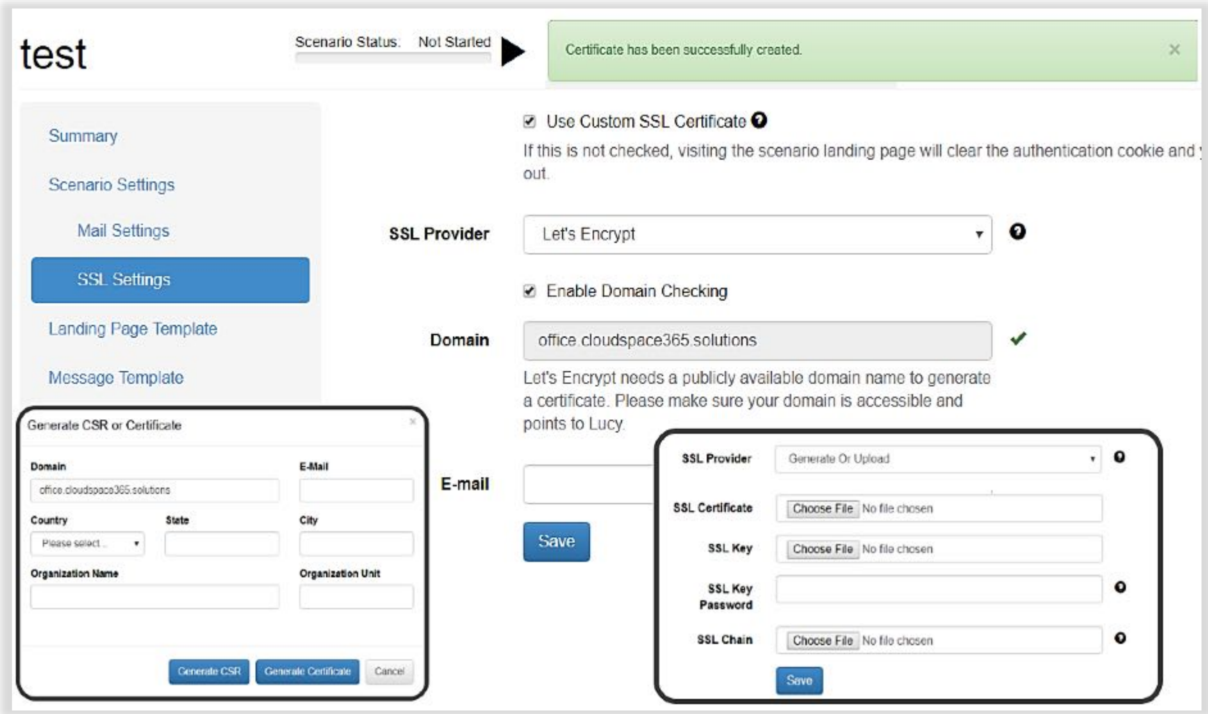
Login

E-mail

Password

(c) 2018 Your Company Name

- **Certificate (SSL):** Allows the automatic creation of official and trusted certificates for the admin, backend as well as for the campaigns. LUCY will automatically use the domain configured in the system to generate the certificate. If you decide to use SSL for the campaign, you can generate a custom certificate or a CSR (Certificate Signing Request). You can also import official trusted certificates.



test

Scenario Status: Not Started

Certificate has been successfully created.

☑ Use Custom SSL Certificate

If this is not checked, visiting the scenario landing page will clear the authentication cookie and
out.

SSL Provider: Let's Encrypt

☑ Enable Domain Checking

Domain: office.cloudspace365.solutions ✓

Let's Encrypt needs a publicly available domain name to generate a certificate. Please make sure your domain is accessible and points to Lucy.

E-mail:

Generate CSR or Certificate

Domain: office.cloudspace365.solutions

E-Mail:

Country: Please select...

State:

City:

Organization Name:

Organization Unit:

SSL Provider: Generate Or Upload

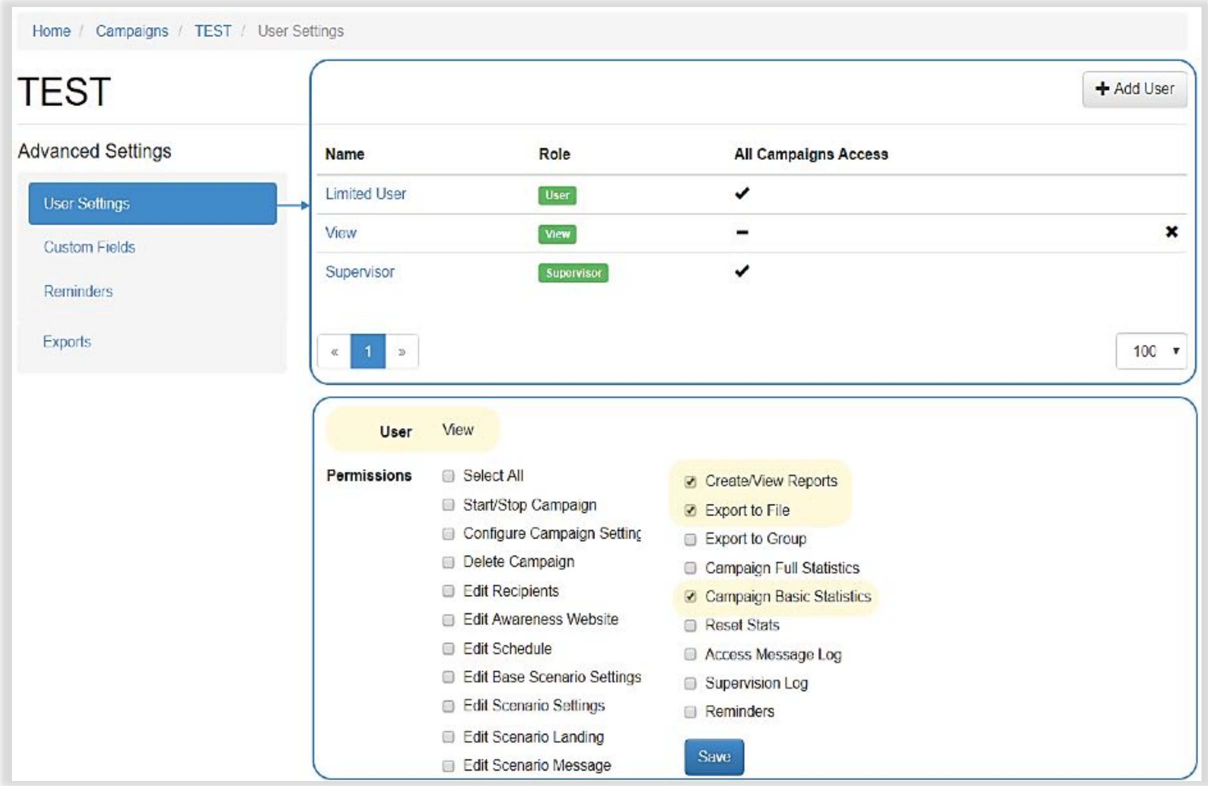
SSL Certificate: Choose File No file chosen

SSL Key: Choose File No file chosen

SSL Key Password:

SSL Chain: Choose File No file chosen

- **Role-based access controls:** LUCY offers a role-based access control (RBAC) that restricts system access to authorized users only. The permissions to perform certain operations are assigned to specific roles within the user settings. Members or staff (or other system users) are assigned particular roles through which to acquire the necessary computer permissions to perform particular LUCY functions.



Home / Campaigns / TEST / User Settings

TEST

Advanced Settings

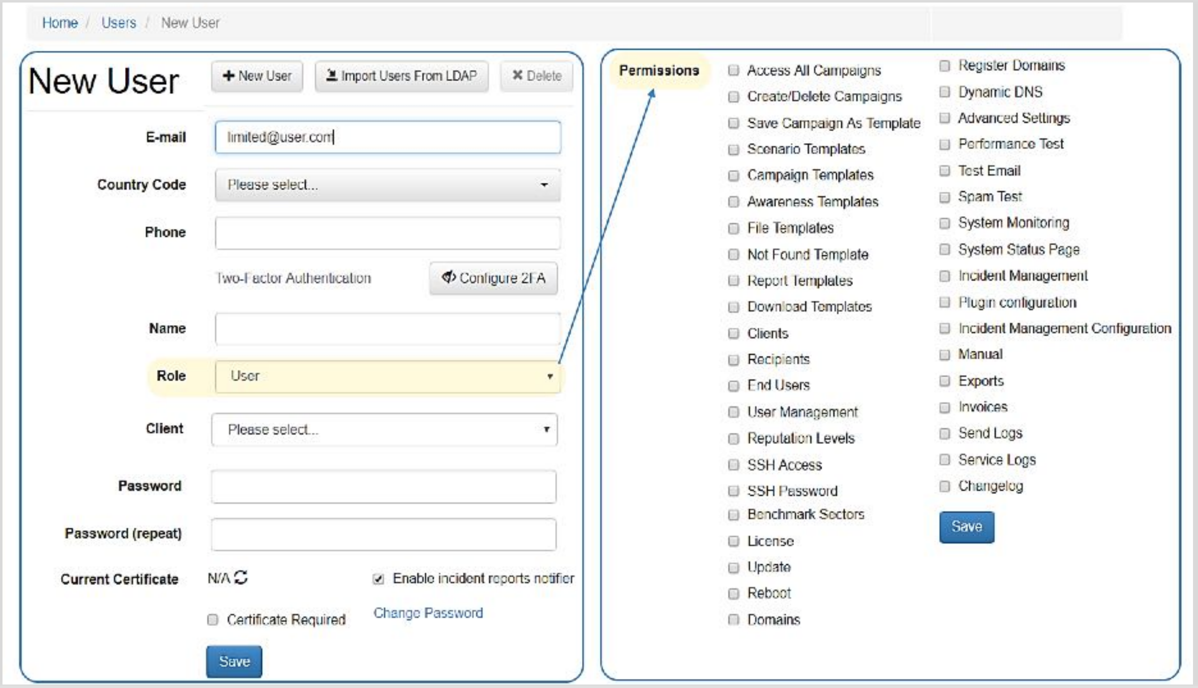
Name	Role	All Campaigns Access	
Limited User	User	✓	
View	View	–	✖
Supervisor	Supervisor	✓	

User View

Permissions

□ Select All
□ Start/Stop Campaign
□ Configure Campaign Setting
□ Delete Campaign
□ Edit Recipients
□ Edit Awareness Website
□ Edit Schedule
□ Edit Base Scenario Settings
□ Edit Scenario Settings
□ Edit Scenario Landing
□ Edit Scenario Message
☑ Create/View Reports
☑ Export to File
□ Export to Group
□ Campaign Full Statistics
☑ Campaign Basic Statistics
□ Reset Stats
□ Access Message Log
□ Supervision Log
□ Reminders

- **Multi-layered user groups:** Quickly upload users in bulk via a CSV, LDAP, or text file. Create different groups, organized by department, division, title, etc. Update users in a running campaign. Build dynamic user groups based on the phishing campaign results.



Home / Users / New User

New User

+ New User | Import Users From LDAP | ✖ Delete

E-mail	limited@user.com
Country Code	Please select...
Phone	
Two-Factor Authentication	Configure 2FA
Name	
Role	User
Client	Please select...
Password	
Password (repeat)	
Current Certificate	N/A

☑ Enable incident reports notifier

□ Certificate Required

Change Password

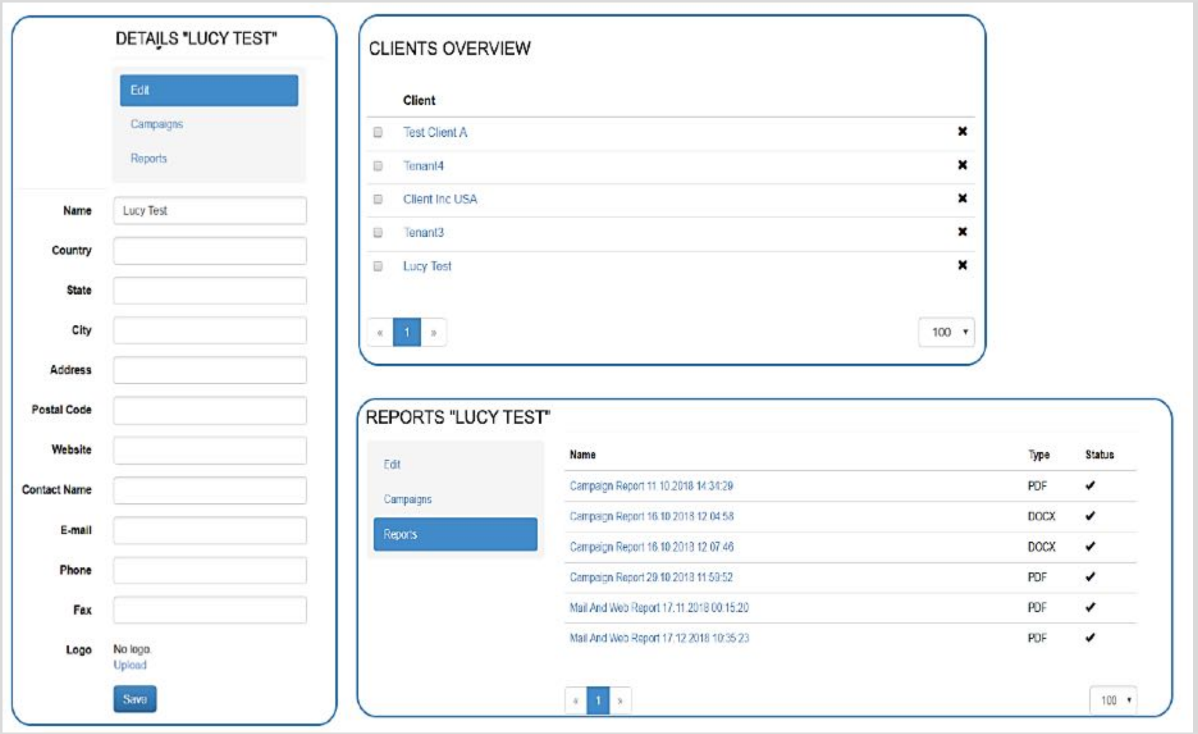
Save

Permissions

□ Access All Campaigns
□ Create/Delete Campaigns
□ Save Campaign As Template
□ Scenario Templates
□ Campaign Templates
□ Awareness Templates
□ File Templates
□ Not Found Template
□ Report Templates
□ Download Templates
□ Clients
□ Recipients
□ End Users
□ User Management
□ Reputation Levels
□ SSH Access
□ SSH Password
□ Benchmark Sectors
□ License
□ Update
□ Reboot
□ Domains
□ Register Domains
□ Dynamic DNS
□ Advanced Settings
□ Performance Test
□ Test Email
□ Spam Test
□ System Monitoring
□ System Status Page
□ Incident Management
□ Plugin configuration
□ Incident Management Configuration
□ Manual
□ Exports
□ Invoices
□ Send Logs
□ Service Logs
□ Changelog

Save

- **Multi-client compatible:** "Clients" can refer to different companies, departments, or groups that have an associated campaign in LUCY. These clients can be used, for example, to allow campaign-specific access or to create customer-specific analysis.



DETAILS "LUCY TEST"

Edit
Campaigns
Reports

Name	Lucy Test
Country	
State	
City	
Address	
Postal Code	
Website	
Contact Name	
E-mail	
Phone	
Fax	
Logo	No logo. Upload

Save

CLIENTS OVERVIEW

	Client	
□	Test Client A	✖
□	Tenant4	✖
□	Client Inc USA	✖
□	Tenant3	✖
□	Lucy Test	✖

« 1 » 100

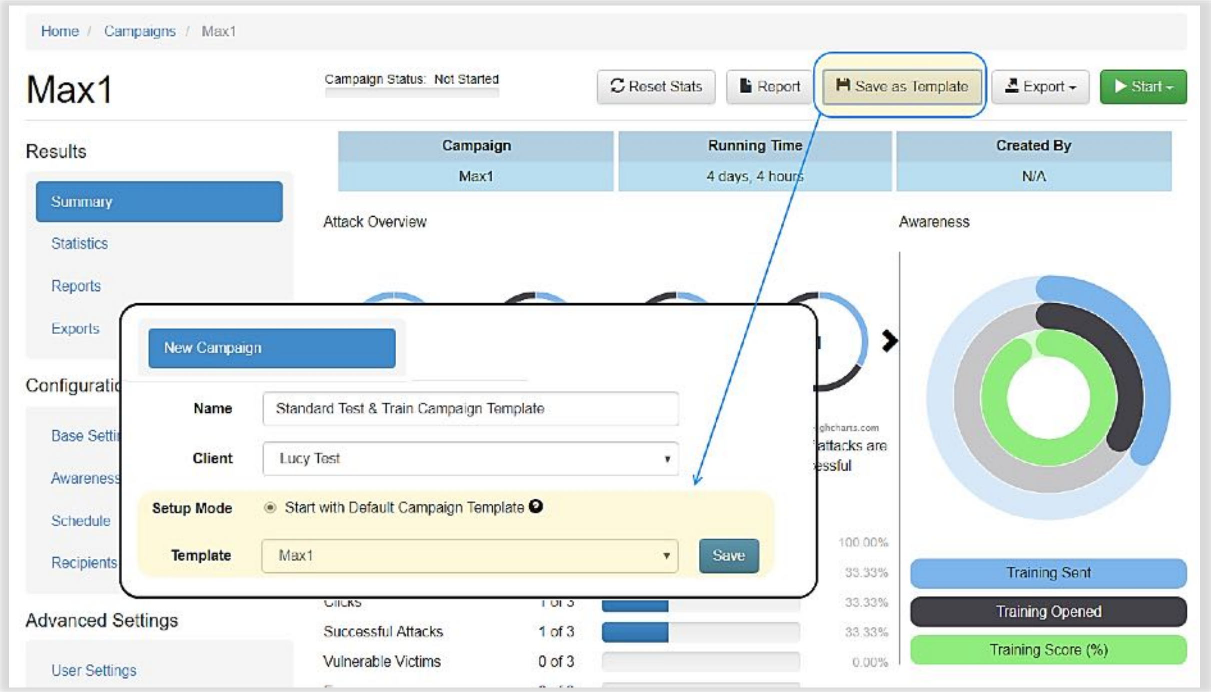
REPORTS "LUCY TEST"

Edit
Campaigns
Reports

Name	Type	Status
Campaign Report 11.10.2018 14:34:29	PDF	✓
Campaign Report 16.10.2018 12:04:58	DOCX	✓
Campaign Report 16.10.2018 12:07:46	DOCX	✓
Campaign Report 29.10.2018 11:59:52	PDF	✓
Mail And Web Report 17.11.2018 00:15:20	PDF	✓
Mail And Web Report 17.12.2018 10:35:23	PDF	✓

« 1 » 100

- **Campaign templates:** In case you want to reuse similar campaigns, you can save a complete campaign with attack templates and eLearning content as a campaign template. This feature allows you to evade having to repeat similar configurations over and over again.



Home / Campaigns / Max1

Max1

Campaign Status: Not Started

Campaign	Running Time	Created By
Max1	4 days, 4 hours	N/A

New Campaign

Name: Standard Test & Train Campaign Template

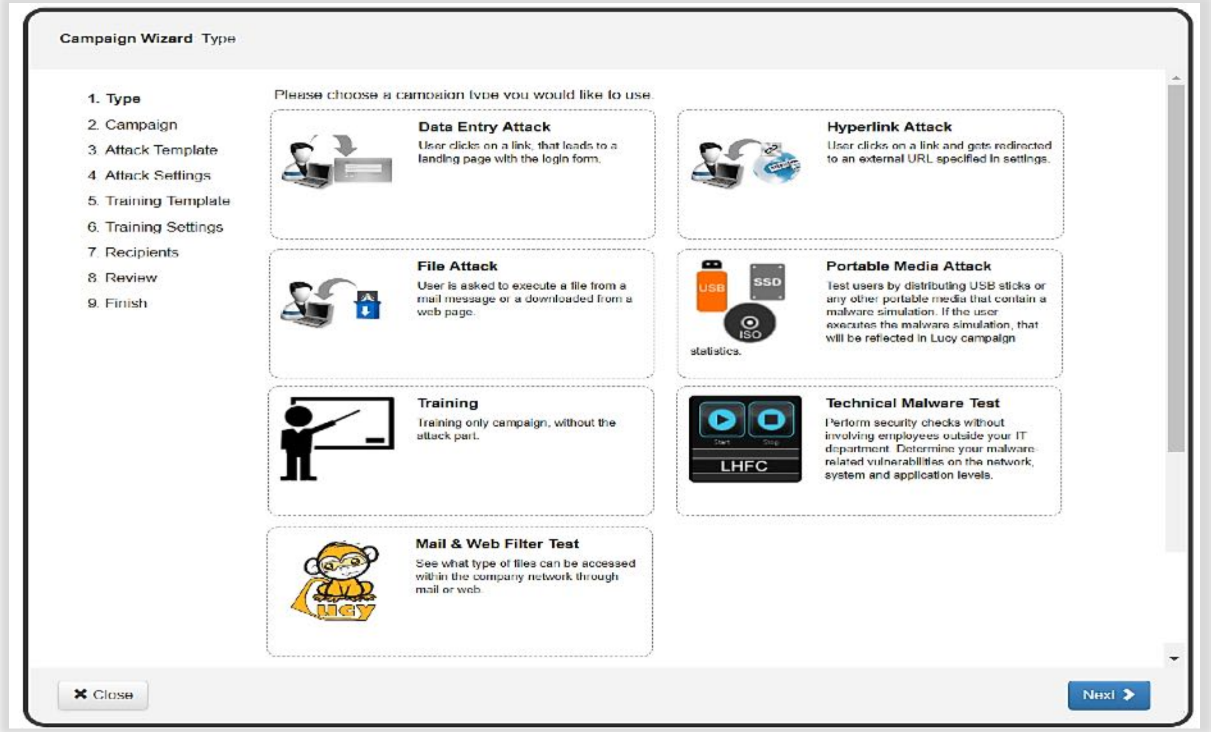
Client: Lucy Test

Setup Mode: ● Start with Default Campaign Template

Template: Max1

Clicks	1 of 3		33.33%
Successful Attacks	1 of 3		33.33%
Vulnerable Victims	0 of 3		0.00%

- **Setup wizard with risk-based guidance:** LUCY offers several Setup Tools. Create a complete campaign in less than 3 minutes using the predefined campaign templates or let the Setup Wizard guide you through the configuration. Optionally, a risk-based setup mode is available, which makes specific suggestions for the selection of attack and awareness templates based on the company's size and industry.



Campaign Wizard Type

1. Type
2. Campaign
3. Attack Template
4. Attack Settings
5. Training Template
6. Training Settings
7. Recipients
8. Review
9. Finish

Please choose a campaign type you would like to use.

Data Entry Attack
User clicks on a link, that leads to a landing page with the login form.

Hyperlink Attack
User clicks on a link and gets redirected to an external URL specified in settings.

File Attack
User is asked to execute a file from a mail message or a downloaded from a web page.

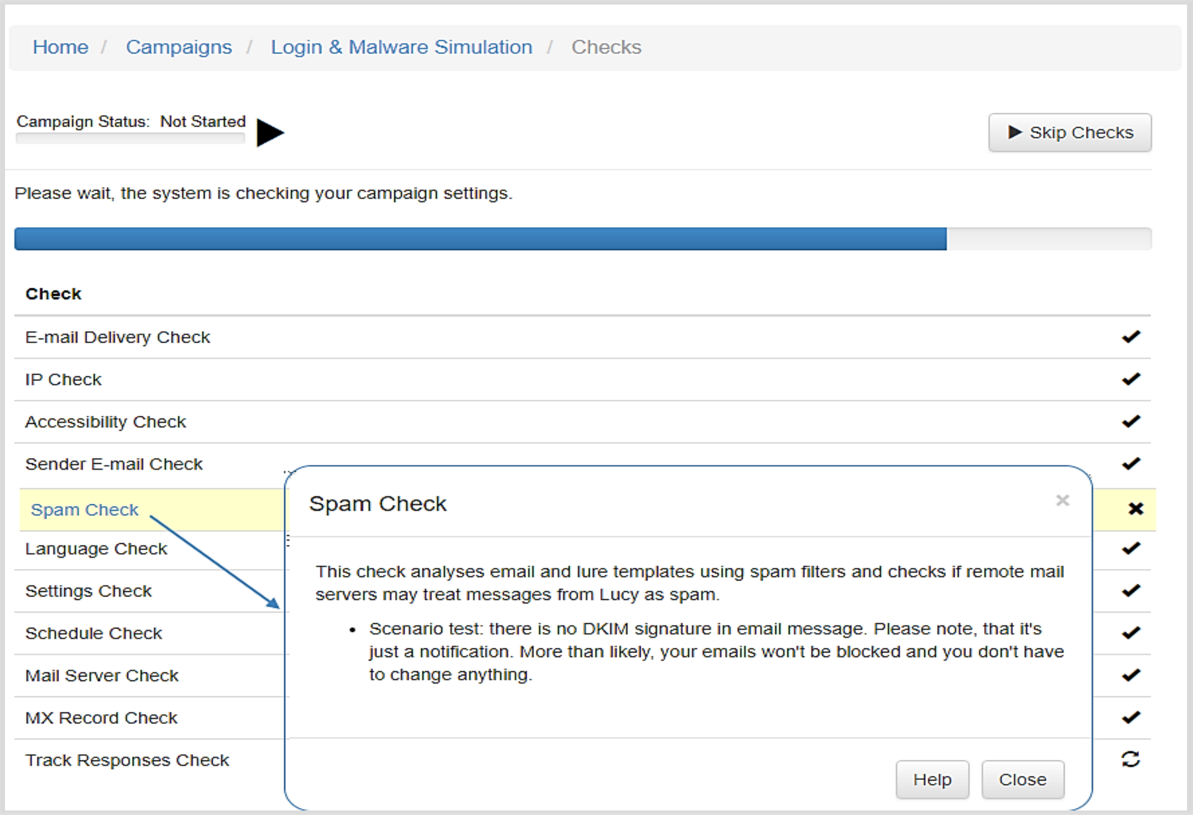
Portable Media Attack
Test users by distributing USB sticks or any other portable media that contain a malware simulation. If the user executes the malware simulation, that will be reflected in Lucy campaign statistics.

Training
Training only campaign, without the attack part.

Technical Malware Test
Perform security checks without involving employees outside your IT department. Determine your malware related vulnerabilities on the network, system and application levels.

Mail & Web Filter Test
See what type of files can be accessed within the company network through mail or web.

- **Campaign checks:** Preliminary checks before starting a LUCY campaign: E-Mail Delivery Check, MX Record Check, Schedule Check, Spam Check, and others.



Home / Campaigns / Login & Malware Simulation / Checks

Campaign Status: Not Started

Please wait, the system is checking your campaign settings.

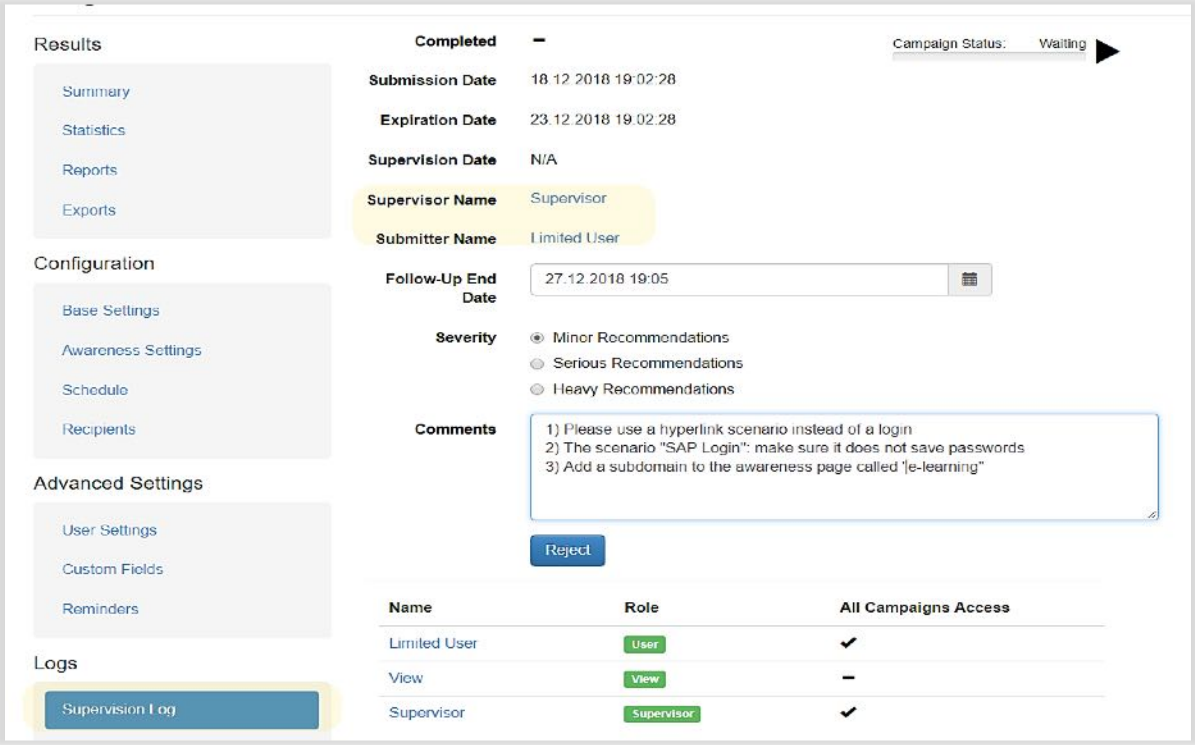
Check	
E-mail Delivery Check	✓
IP Check	✓
Accessibility Check	✓
Sender E-mail Check	✓
Spam Check	✖
Language Check	✓
Settings Check	✓
Schedule Check	✓
Mail Server Check	✓
MX Record Check	✓
Track Responses Check	↻

Spam Check

This check analyses email and lure templates using spam filters and checks if remote mail servers may treat messages from Lucy as spam.

- Scenario test: there is no DKIM signature in email message. Please note, that it's just a notification. More than likely, your emails won't be blocked and you don't have to change anything.

- **Approval workflows:** A given campaign can be submitted to a supervisor in LUCY for approval.



Campaign Status: Waiting

Completed –

Submission Date 18.12.2018 19:02:28

Expiration Date 23.12.2018 19:02:28

Supervision Date N/A

Supervisor Name Supervisor

Submitter Name Limited User

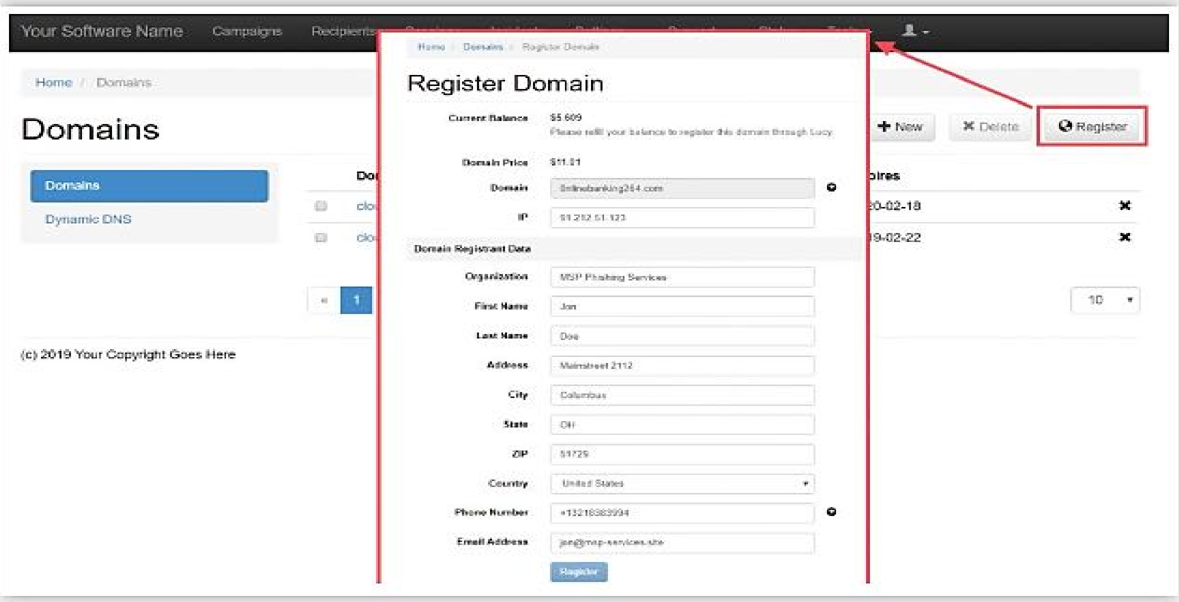
Follow-Up End Date 27.12.2018 19:05

Severity ● Minor Recommendations ○ Serious Recommendations ○ Heavy Recommendations

Comments
1) Please use a hyperlink scenario instead of a login
2) The scenario "SAP Login": make sure it does not save passwords
3) Add a subdomain to the awareness page called 'e-learning"

Name	Role	All Campaigns Access
Limited User	User	✓
View	View	–
Supervisor	Supervisor	✓

- **DNS API:** The DNS API allows the administrator to create any domain on LUCY within seconds. Since attackers very often use similar spellings of a customer's domain (called Typosquatting), this risk can also be represented in LUCY. If the customer's original domain is, for example, "onlinebanking.com", the DNS wizard could be used to reserve domains such as "0nlinebanking.com", "onl1nebanking.com" or "onlinebanking.services" and assign it to a campaign later. LUCY then automatically creates the corresponding DNS entries (MX, SPF, Whois Protection etc) for the IP where LUCY is installed. Of course, the admin can also use his provider's own domains in LUCY.



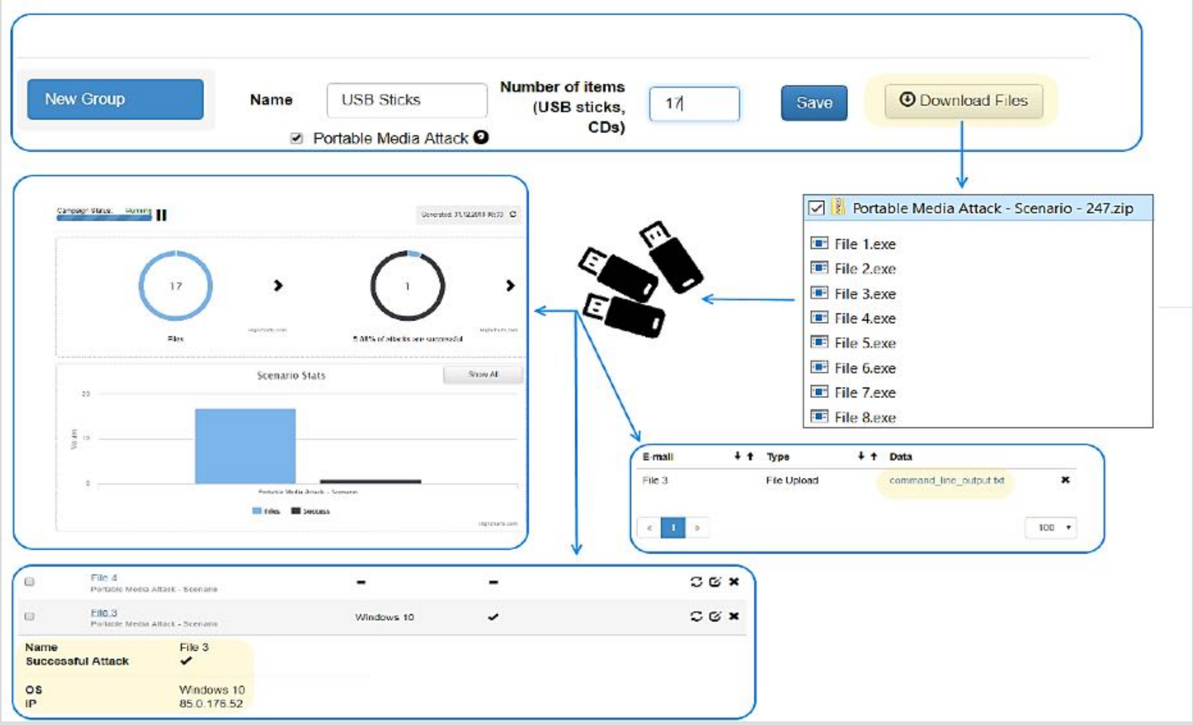
Register Domain

Current Balance	$5.609 Please refill your balance to register this domain through Lucy
Domain Price	$11.01
Domain	0nlinebanking264.com
IP	91.212.51.123
Domain Registrant Data	
Organization	MSP Phishing Services
First Name	Jon
Last Name	Doe
Address	Mainstreet 2112
City	Columbus
State	OH
ZIP	51725
Country	United States
Phone Number	+13218383994
Email Address	jon@msp-services.site

Register

ATTACK SIMULATION

- **Portable media attacks:** Hackers can use portable media drives to gain access to sensitive information stored on a computer or network. 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.



Name: USB Sticks

Number of items (USB sticks, CDs): 17

☑ Portable Media Attack

☑ Portable Media Attack - Scenario - 247.zip

File 1.exe
File 2.exe
File 3.exe
File 4.exe
File 5.exe
File 6.exe
File 7.exe
File 8.exe

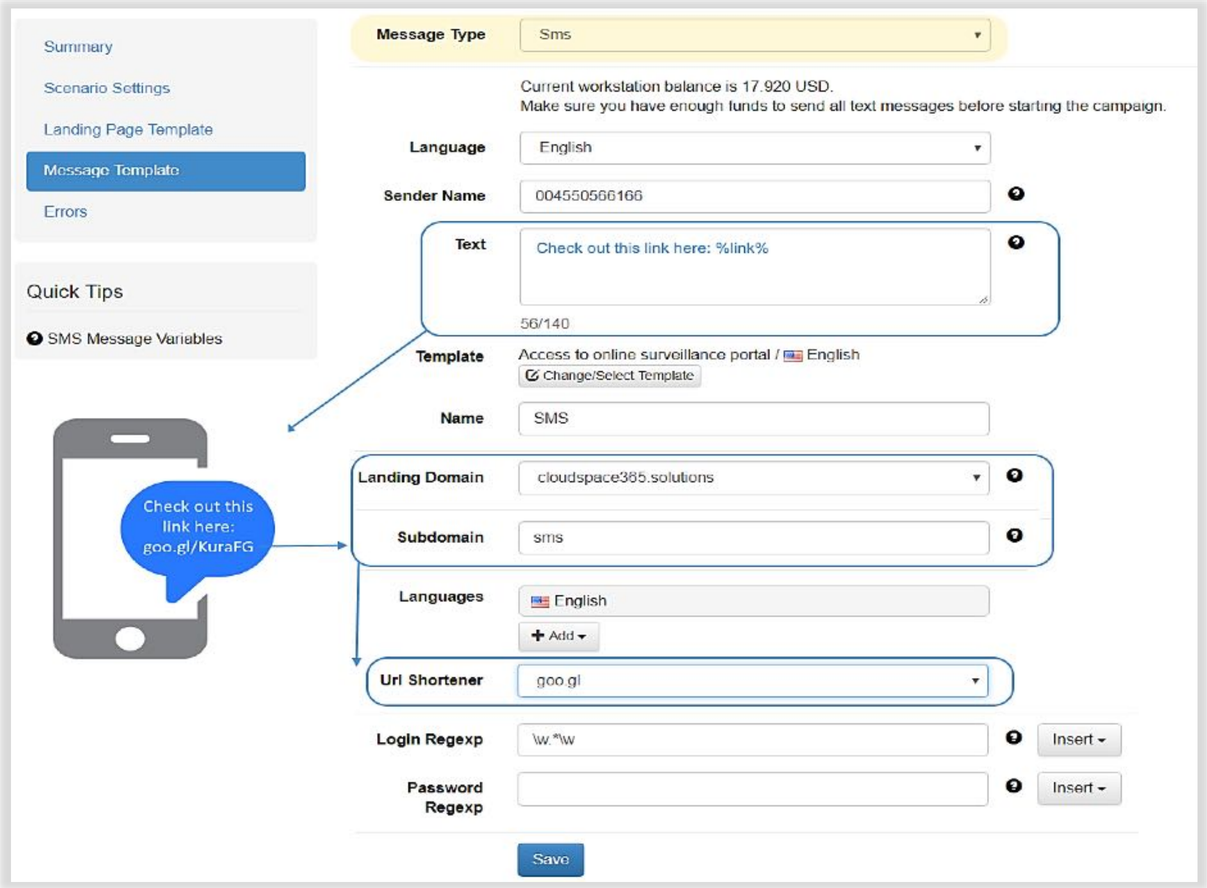
E-mail	Type	Data
File 3	File Upload	command_line_output.txt

File 4 — Portable Media Attack - Scenario — - —

File 3 — Portable Media Attack - Scenario — Windows 10 — ✓

Name	File 3
Successful Attack	✓
OS	Windows 10
IP	85.0.176.52

- **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-laden attachment or clicking on a malicious link. Smishing simply uses text messages instead of e-mail.



Summary
Scenario Settings
Landing Page Template
Message Template
Errors

Quick Tips
SMS Message Variables

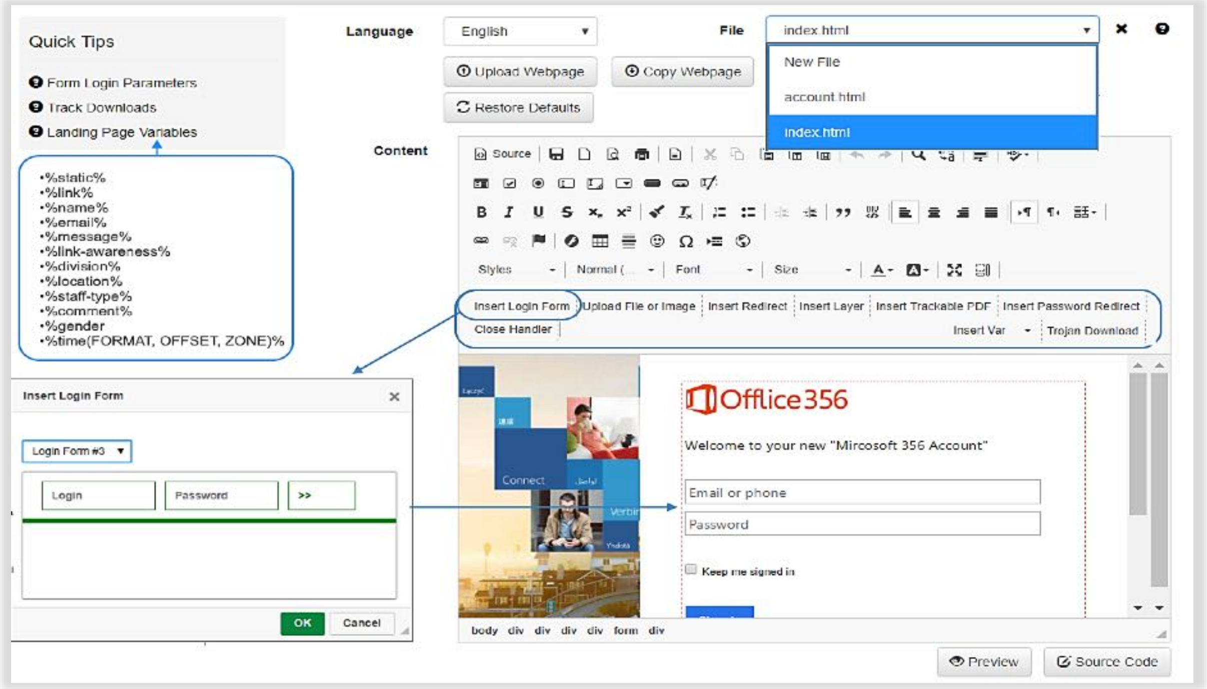
Message Type: Sms

Current workstation balance is 17.920 USD.
Make sure you have enough funds to send all text messages before starting the campaign.

Language: English
Sender Name: 004550566166
Text: Check out this link here: %link%
56/140
Template: Access to online surveillance portal / English
Change/Select Template
Name: SMS
Landing Domain: cloudspace365.solutions
Subdomain: sms
Languages: English
Add
Url Shortener: goo.gl
Login Regexp: \w.*\w
Password Regexp:

Check out this link here: goo.gl/KuraFG

- **Data entry attacks:** Data entry attacks 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.



Quick Tips
Form Login Parameters
Track Downloads
Landing Page Variables

- %static%
- %link%
- %name%
- %email%
- %message%
- %link-awareness%
- %division%
- %location%
- %staff-type%
- %comment%
- %gender
- %time(FORMAT, OFFSET, ZONE)%

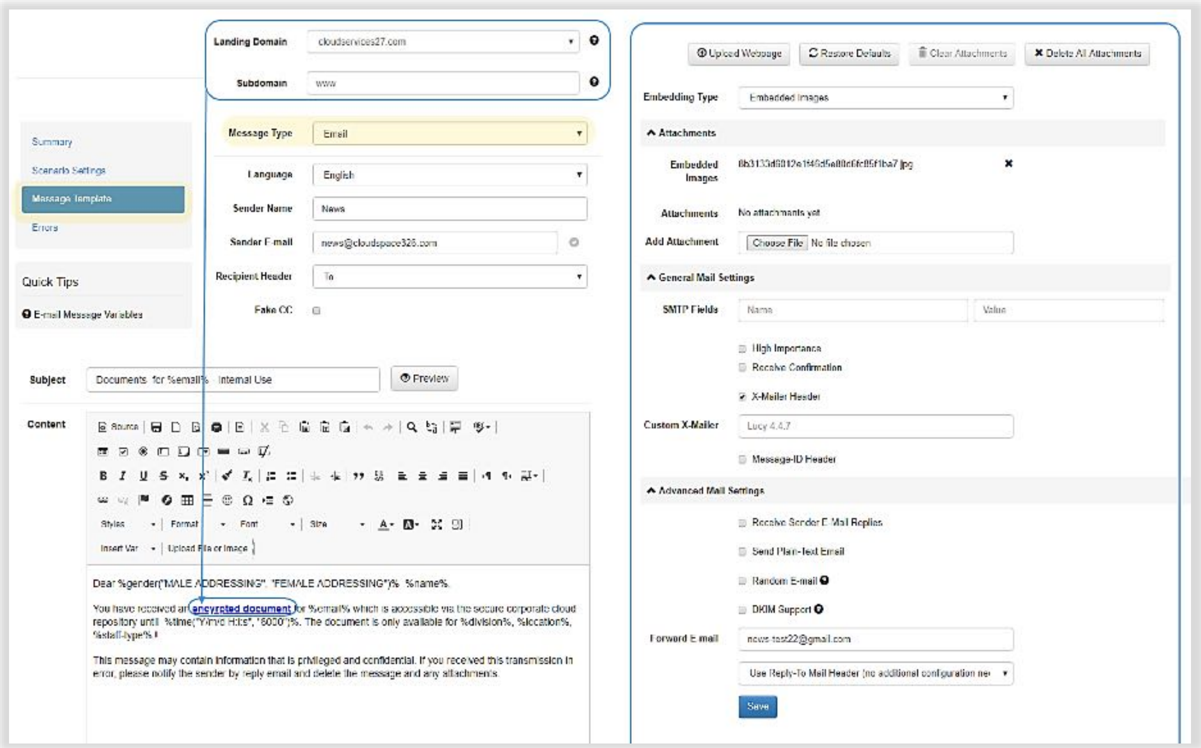
Language: English
File: index.html

Content

Insert Login Form
Login Form #3
Login | Password | >>

Office356
Welcome to your new "Mircosoft 356 Account"
Email or phone
Password
☐ Keep me signed in

- **Hyperlink attacks:** A hyperlink-based campaign will send users an e-mail that contains a randomized tracking URL.



Summary
Scenario Settings
Message Template
Errors

Quick Tips
E-mail Message Variables

Landing Domain: cloudservices27.com
Subdomain: www
Message Type: Email
Language: English
Sender Name: News
Sender E-mail: news@cloudspace326.com
Recipient Header: To
Fake CC: □
Subject: Documents for %email% Internal Use
Content:

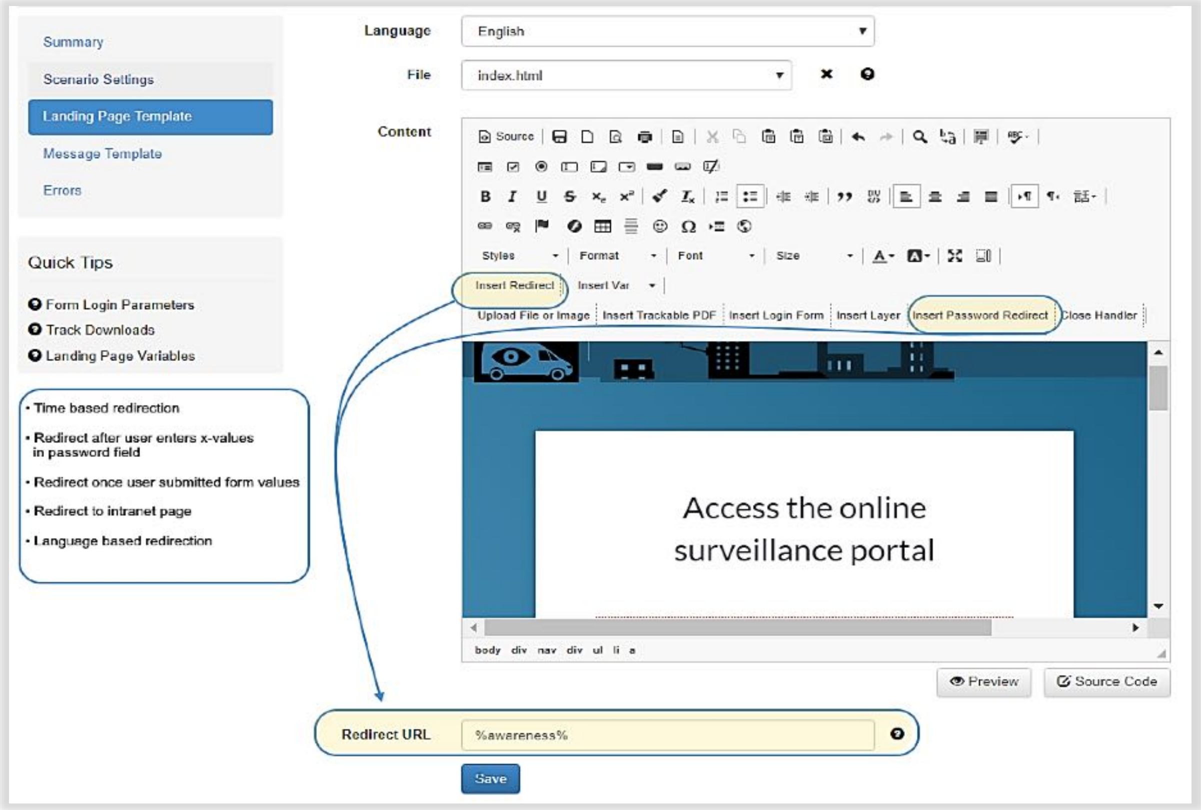
Dear %gender("MALE ADDRESSING", "FEMALE ADDRESSING")% %name%,

You have received an encrypted document for %email% which is accessible via the secure corporate cloud repository until %time("Y-m-d H:i:s", "6000")%. The document is only available for %division%, %location%, %staff-type%!

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.

Embedding Type: Embedded Images
Attachments
Embedded Images: 8b3133d6812e1f46d5e88d6fc85f1ba7.jpg
Attachments: No attachments yet
Add Attachment: Choose File No file chosen
General Mail Settings
SMTP Fields: Name Value
□ High Importance
□ Receive Confirmation
☑ X-Mailer Header
Custom X-Mailer: Lucy 4.4.7
□ Message-ID Header
Advanced Mail Settings
□ Receive Sender E-Mail Replies
□ Send Plain-Text Email
□ Random E-mail
□ DKIM Support
Forward E-mail: news-test22@gmail.com
Use Reply-To Mail Header (no additional configuration ne

- **Powerful URL redirection toolkit:** LUCY's flexible redirection functions allow the user to be guided, at the right moment, to the desired areas of attack simulation or training. For example, after entering the first 3 characters of a password in a phishing simulation, the user can be redirected to a special training page about password protection.



Summary
Scenario Settings
Landing Page Template
Message Template
Errors

Quick Tips
Form Login Parameters
Track Downloads
Landing Page Variables

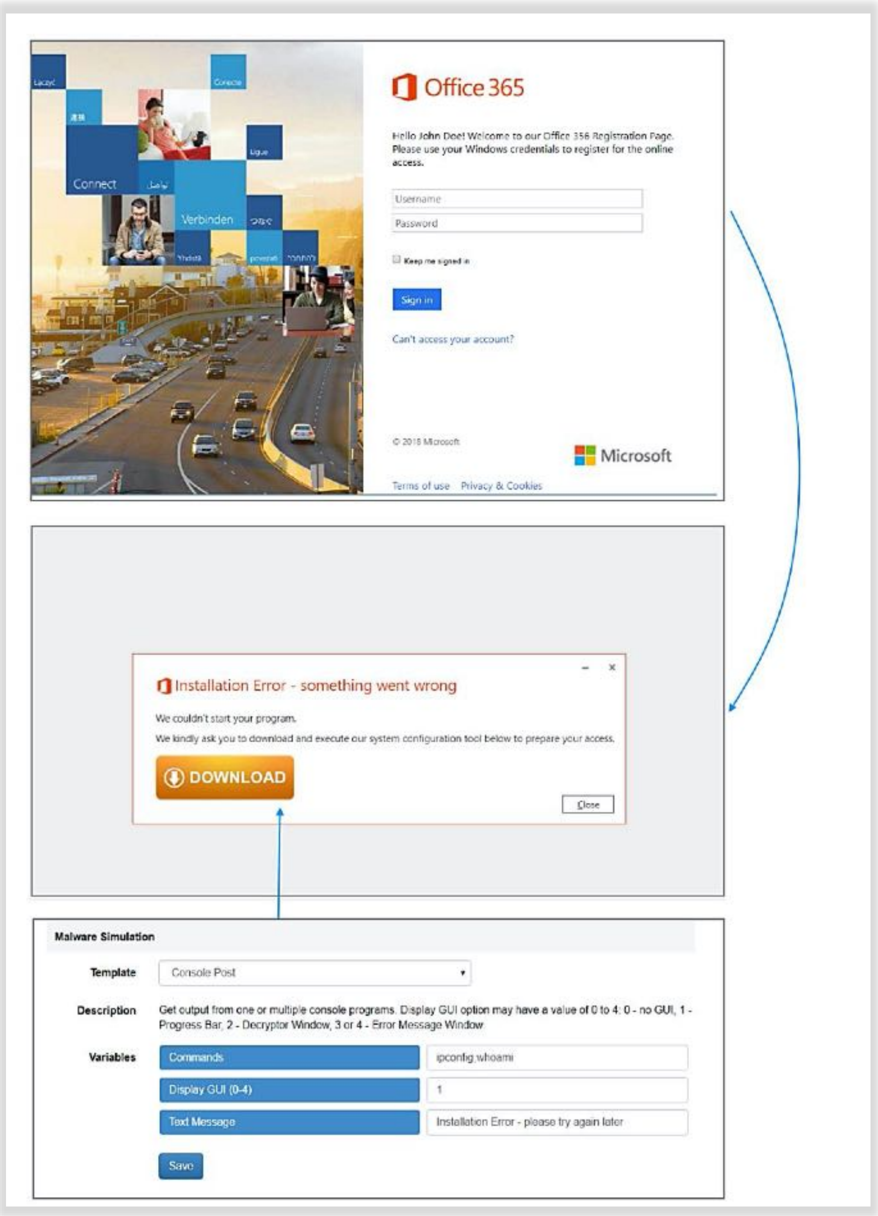
- Time based redirection
- Redirect after user enters x-values in password field
- Redirect once user submitted form values
- Redirect to intranet page
- Language based redirection

Language: English
File: index.html
Content:

Access the online surveillance portal

Redirect URL: %awareness%

- **Mixed attacks:** Mixed attacks allow a combination of multiple scenario types (file-based, data entry, etc.) in the same campaign.



Hello John Doe! Welcome to our Office 356 Registration Page. Please use your Windows credentials to register for the online access.

Username

Password

□ Keep me signed in

Installation Error - something went wrong

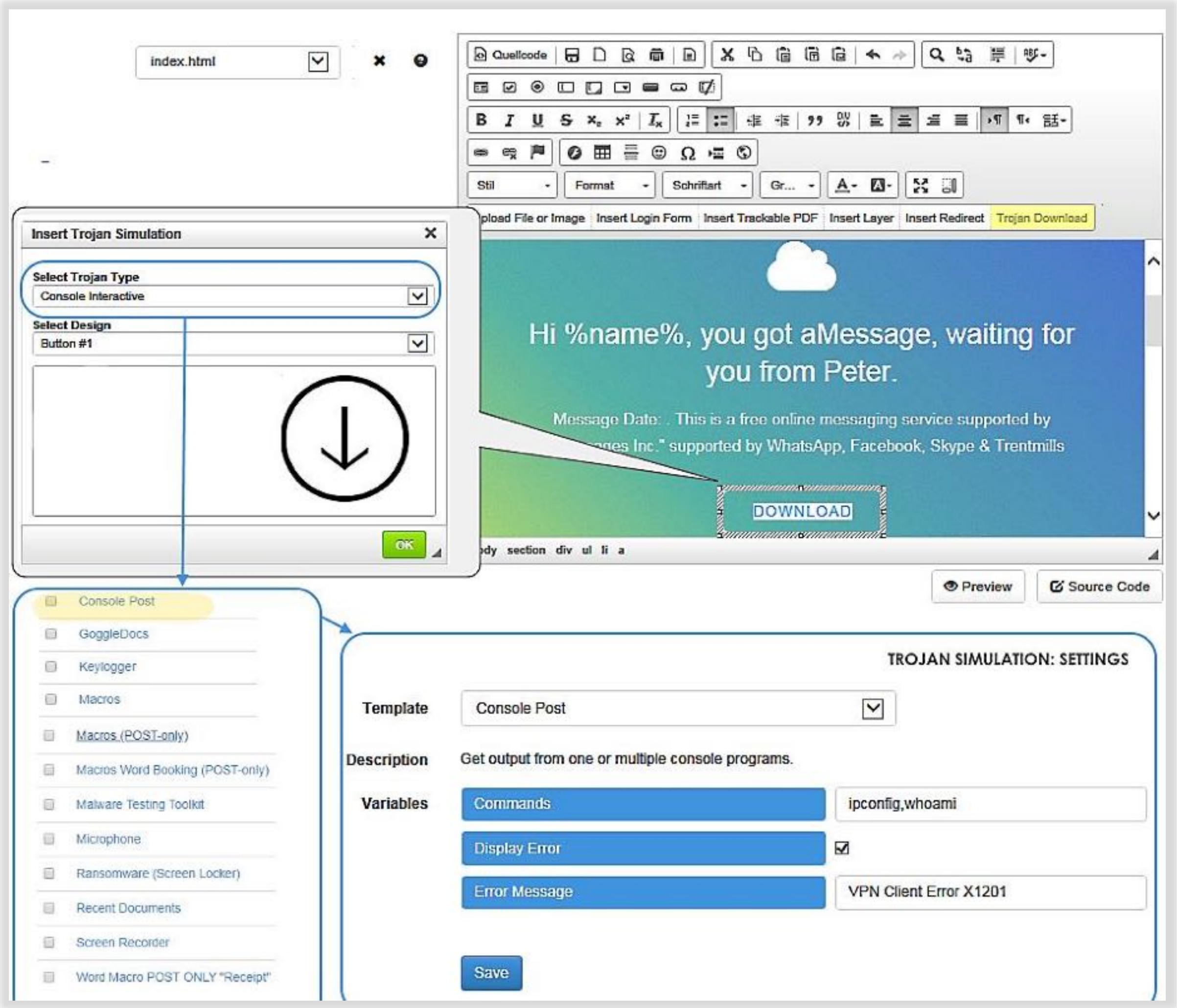
We couldn't start your program.

We kindly ask you to download and execute our system configuration tool below to prepare your access.

Malware Simulation

Template	Console Post ▾
Description	Get output from one or multiple console programs. Display GUI option may have a value of 0 to 4: 0 - no GUI, 1 - Progress Bar, 2 - Decryptor Window, 3 or 4 - Error Message Window
Variables	Commands: ipconfig,whoami
	Display GUI (0-4): 1
	Text Message: Installation Error - please try again later

- **File-based attacks:** 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.



Hi %name%, you got aMessage, waiting for you from Peter.

Message Date: . This is a free online messaging service supported by ...ages Inc." supported by WhatsApp, Facebook, Skype & Trentmills

Insert Trojan Simulation

Select Trojan Type: Console Interactive

Select Design: Button #1

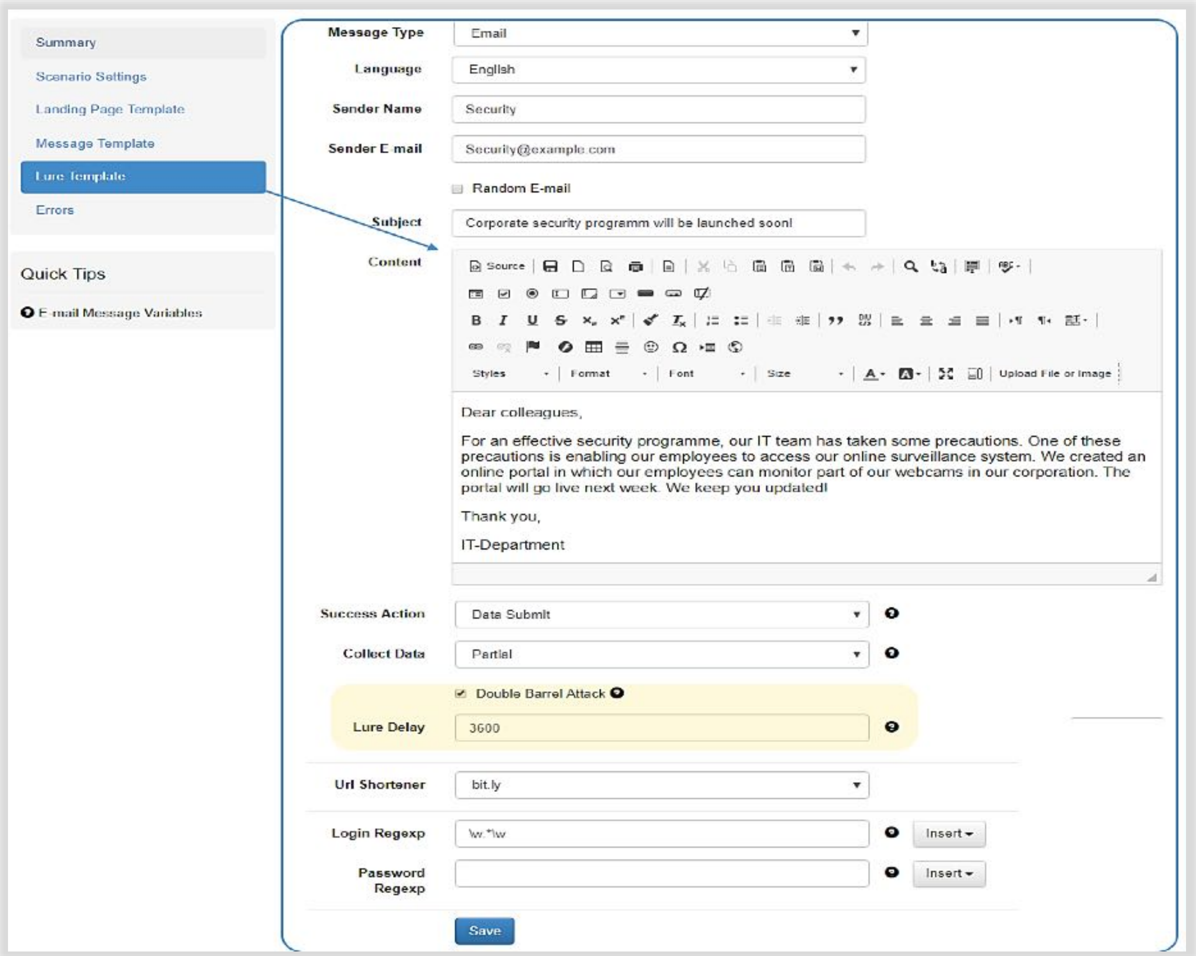
- □ Console Post
- □ GoggleDocs
- □ Keylogger
- □ Macros
- □ Macros (POST-only)
- □ Macros Word Booking (POST-only)
- □ Malware Testing Toolkit
- □ Microphone
- □ Ransomware (Screen Locker)
- □ Recent Documents
- □ Screen Recorder
- □ Word Macro POST ONLY "Receipt"

TROJAN SIMULATION: 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

Save

- **Double barrel attacks:** This feature makes it possible to send multiple phishing e-mails in each campaign, with the first benign e-mail (the bait) containing nothing malicious and not demanding a reply from the recipient.



Message Type: Email

Language: English

Sender Name: Security

Sender E-mail: Security@example.com

□ Random E-mail

Subject: Corporate security programm will be launched soon!

Content:

Dear colleagues,

For an effective security programme, our IT team has taken some precautions. One of these precautions is enabling our employees to access our online surveillance system. We created an online portal in which our employees can monitor part of our webcams in our corporation. The portal will go live next week. We keep you updated!

Thank you,

IT-Department

Success Action: Data Submit

Collect Data: Partial

☑ Double Barrel Attack

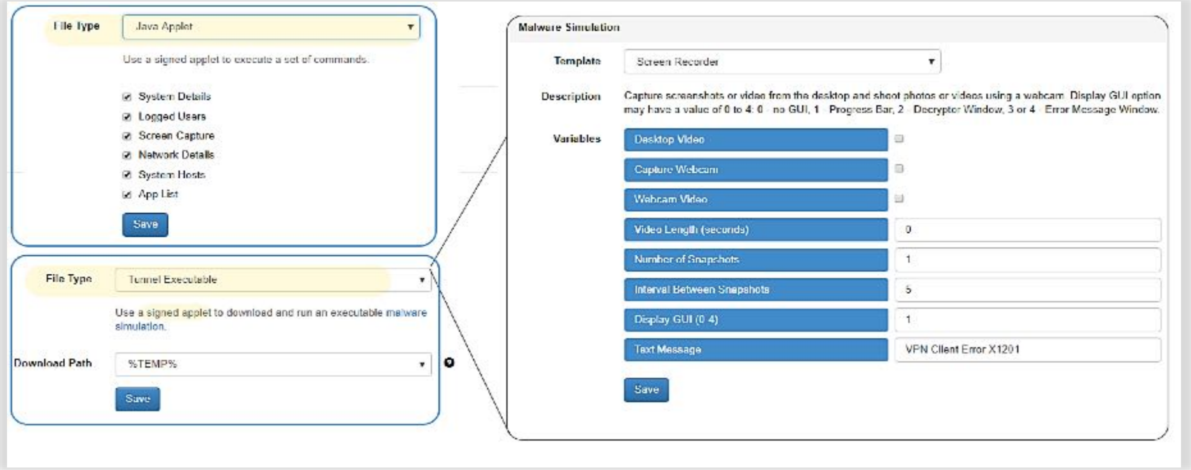
Lure Delay: 3600

Url Shortener: bit.ly

Login Regexp: \w.*\w

Password Regexp:

- **Java-based attacks:** Java-based attacks allow the LUCY administrator to integrate a trusted applet within the file-based or mixed attack templates provided in LUCY and to measure their execution by the user.



File Type: Java Applet

Use a signed applet to execute a set of commands.

☑ System Details
☑ Logged Users
☑ Screen Capture
☑ Network Details
☑ System Hosts
☑ App List

File Type: Tunnel Executable

Use a signed applet to download and run an executable malware simulation.

Download Path: %TEMP%

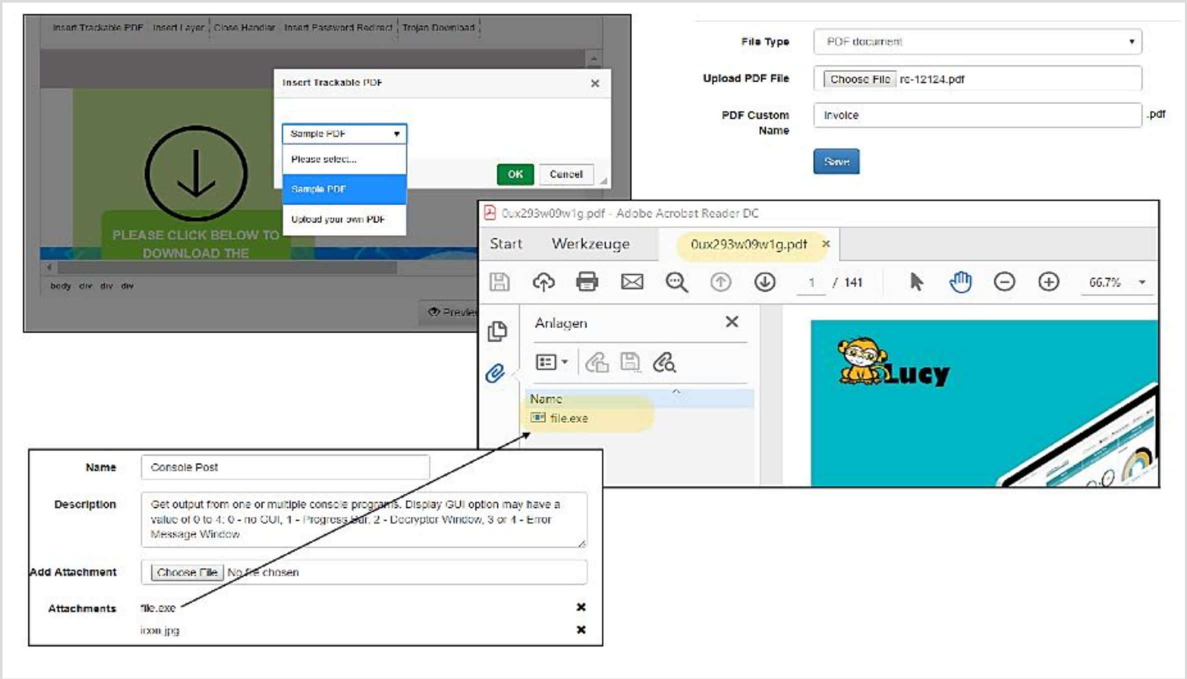
Template: Screen Recorder

Description: Capture screenshots or video from the desktop and shoot photos or videos using a webcam. Display GUI option may have a value of 0 to 4: 0 - no GUI, 1 - Progress Bar, 2 - Decryptor Window, 3 or 4 - Error Message Window.

Variables:

Desktop Video	□
Capture Webcam	□
Webcam Video	□
Video Length (seconds)	0
Number of Snapshots	1
Interval Between Snapshots	5
Display GUI (0-4)	1
Text Message	VPN Client Error X1201

- **PDF-based attacks**: PDF-based phishing attacks can be simulated with this module. LUCY allows "hiding" executable files as PDF attachments and measuring their execution. Furthermore, dynamic phishing links can be also generated within PDFs.



Insert Trackable PDF

Sample PDF ▾
Please select...
Sample PDF
Upload your own PDF

OK Cancel

File Type: PDF document

Upload PDF File: Choose File rc-12124.pdf

PDF Custom Name: Invoice .pdf

Save

0ux293w09w1g.pdf - Adobe Acrobat Reader DC

file.exe

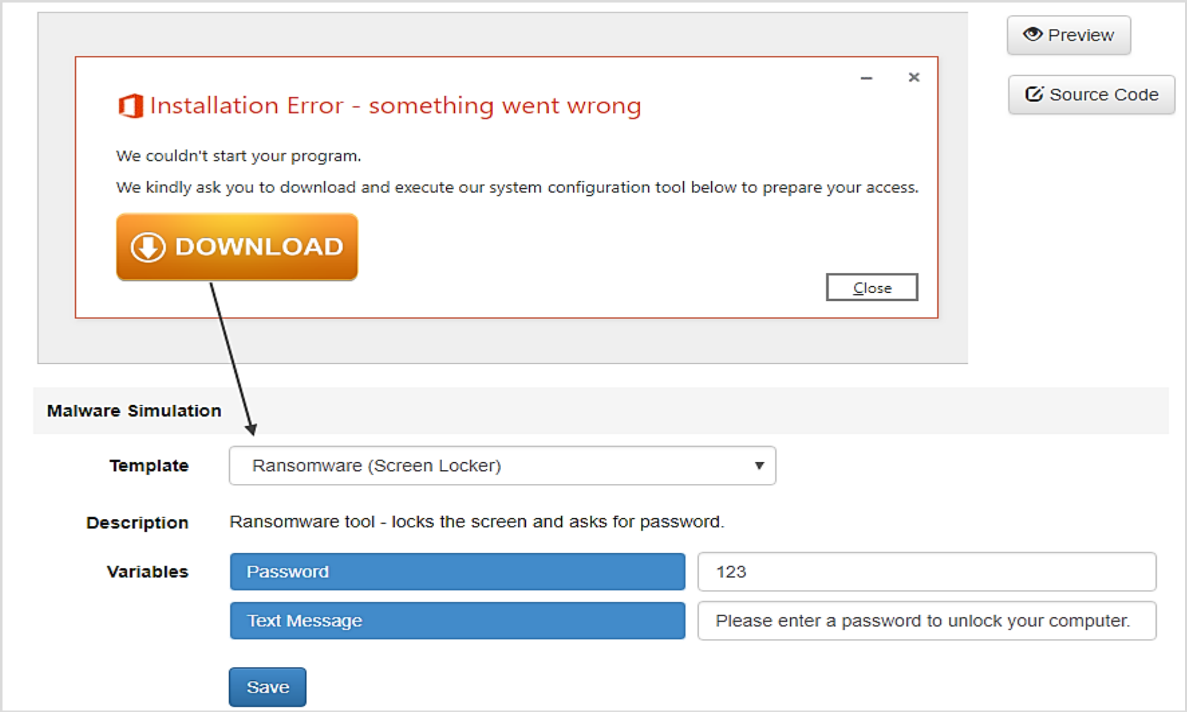
Name: Console Post

Description: Get output from one or multiple console programs. Display GUI option may have a value of 0 to 4: 0 - no GUI, 1 - Progress Bar, 2 - Decryptor Window, 3 or 4 - Error Message Window

Add Attachment: Choose File No file chosen

Attachments: file.exe ✖
icon.jpg ✖

- **Ransomware simulation attacks**: LUCY has two different ransomware simulations, one of which tests the staff, and the other, the infrastructure.



Installation Error - something went wrong

We couldn't start your program.

We kindly ask you to download and execute our system configuration tool below to prepare your access.

Malware Simulation

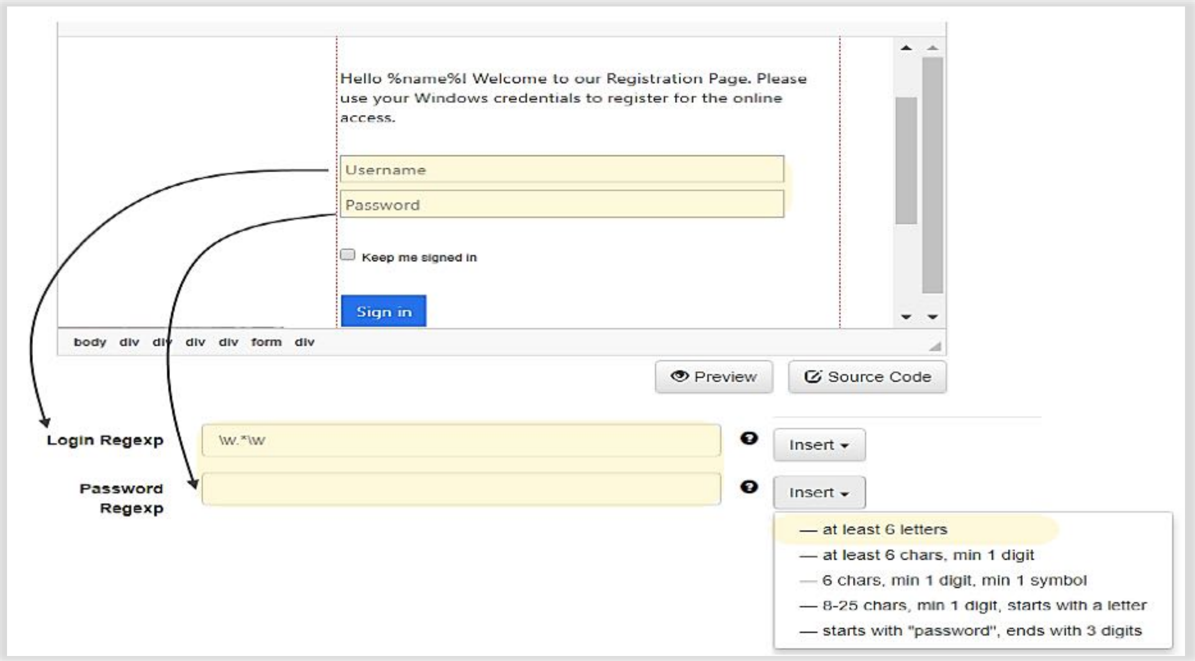
Template: Ransomware (Screen Locker) ▾

Description: Ransomware tool - locks the screen and asks for password.

Variables:
Password: 123
Text Message: Please enter a password to unlock your computer.

Save

- **Data entry validation toolkit:** In phishing simulations, false positives must be prevented for log-in fields (e.g., logging with invalid syntax). The company guidelines may also forbid the transmission of sensitive data such as passwords. For this purpose, LUCY provides a flexible input filtering engine that offers a suitable solution for every requirement.



Hello %name%! Welcome to our Registration Page. Please use your Windows credentials to register for the online access.

Username

Password

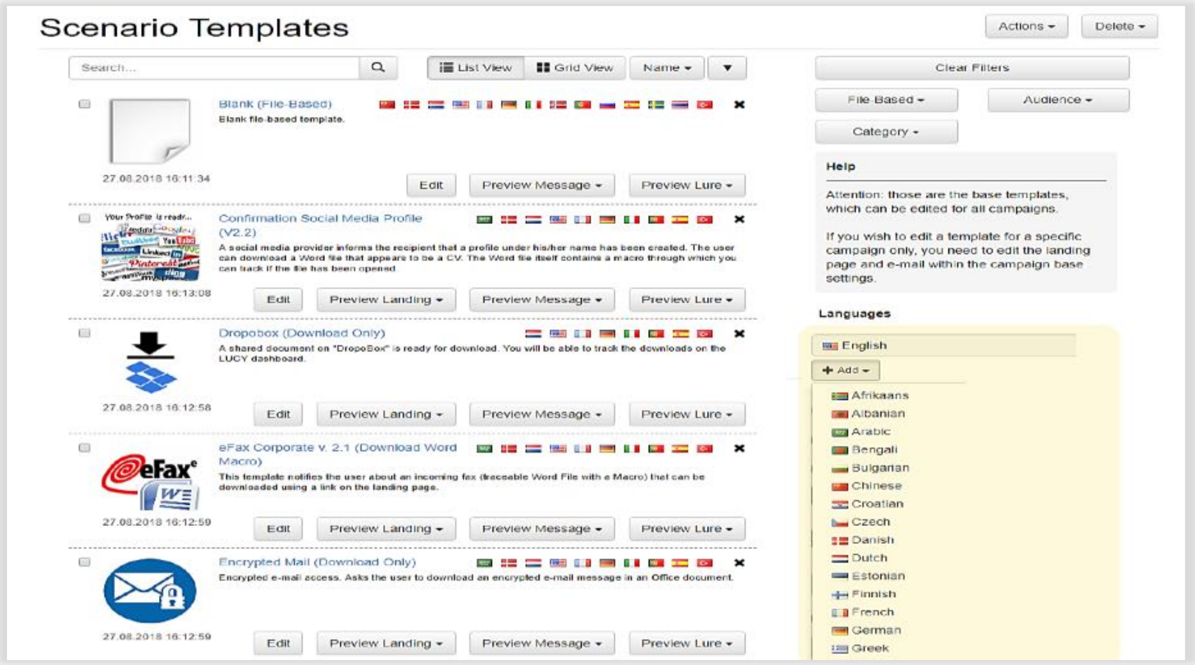
□ Keep me signed in

Login Regexp: \w.*\w

Password Regexp:

- at least 6 letters
- at least 6 chars, min 1 digit
- 6 chars, min 1 digit, min 1 symbol
- 8-25 chars, min 1 digit, starts with a letter
- starts with "password", ends with 3 digits

- **Multilingual Attack Template Library:** LUCY comes with hundreds of predefined attack templates in more than 30 languages in the categories of data entry (templates with a website), file-based (e-mails or websites with a file download), hyperlink (e-mails with a link), mixed (combination of data entry and download), and portable media.



Scenario Templates

□ Blank (File-Based)
Blank file-based template.
27.08.2018 16:11:34

□ 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.
27.08.2018 16:13:08

□ Dropobox (Download Only)
A shared document on "DropoBox" is ready for download. You will be able to track the downloads on the LUCY dashboard.
27.08.2018 16:12:58

□ eFax Corporate v. 2.1 (Download Word Macro)
This template notifies the user about an incoming fax (traceable Word File with a Macro) that can be downloaded using a link on the landing page.
27.08.2018 16:12:59

□ Encrypted Mail (Download Only)
Encrypted e-mail access. Asks the user to download an encrypted e-mail message in an Office document.
27.08.2018 16:12:59

Help

Attention: those are the base templates, which can be edited for all campaigns.

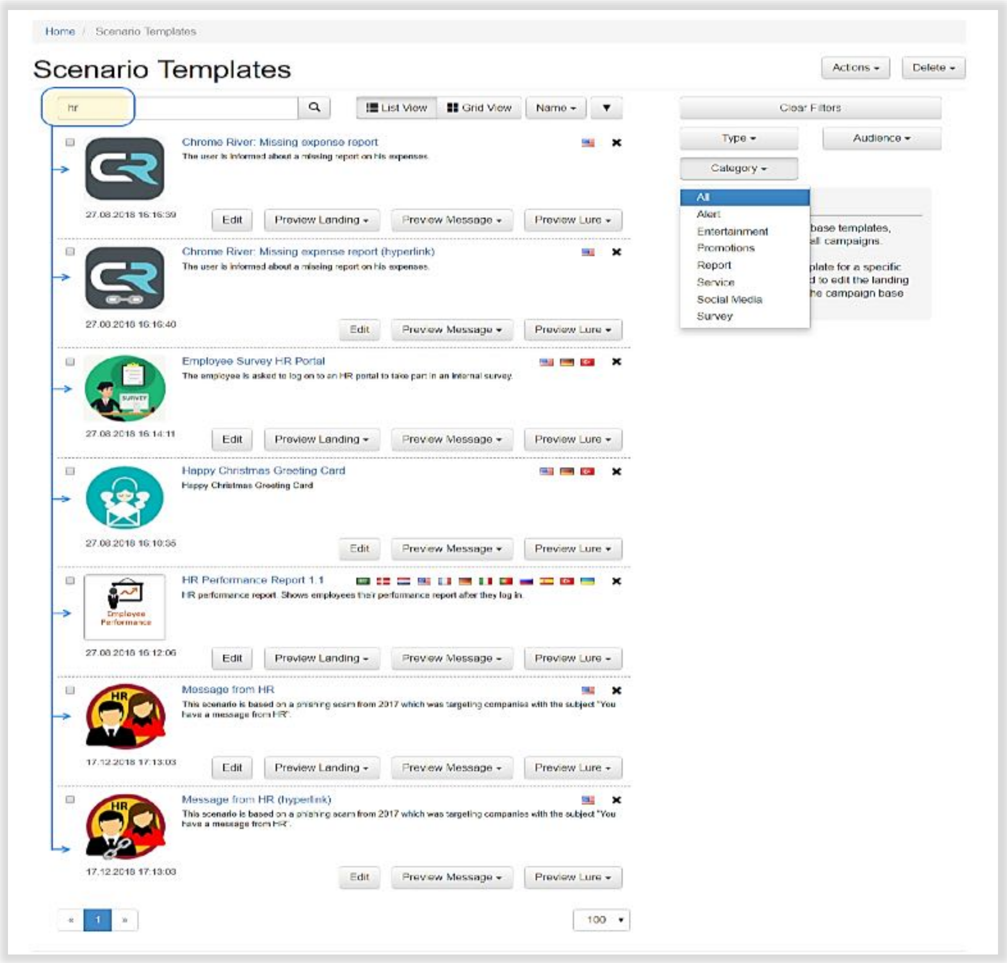
If you wish to edit a template for a specific campaign only, you need to edit the landing page and e-mail within the campaign base settings.

Languages

English

Afrikaans
Albanian
Arabic
Bengali
Bulgarian
Chinese
Croatian
Czech
Danish
Dutch
Estonian
Finnish
French
German
Greek

- **Sector and division specific templates**: Attack templates are available for specific industries or divisions.



Home / Scenario Templates

Scenario Templates

hr

Chrome River: Missing expense report
The user is informed about a missing report on his expenses.
27.08.2018 16:16:39

Chrome River: Missing expense report (hyperlink)
The user is informed about a missing report on his expenses.
27.08.2018 16:16:40

Employee Survey HR Portal
The employee is asked to log on to an HR portal to take part in an internal survey.
27.08.2018 16:14:11

Happy Christmas Greeting Card
Happy Christmas Greeting Card
27.08.2018 16:10:35

HR Performance Report 1.1
HR perfomance report. Shows employees their perfomance report after they log in.
27.08.2018 16:12:06

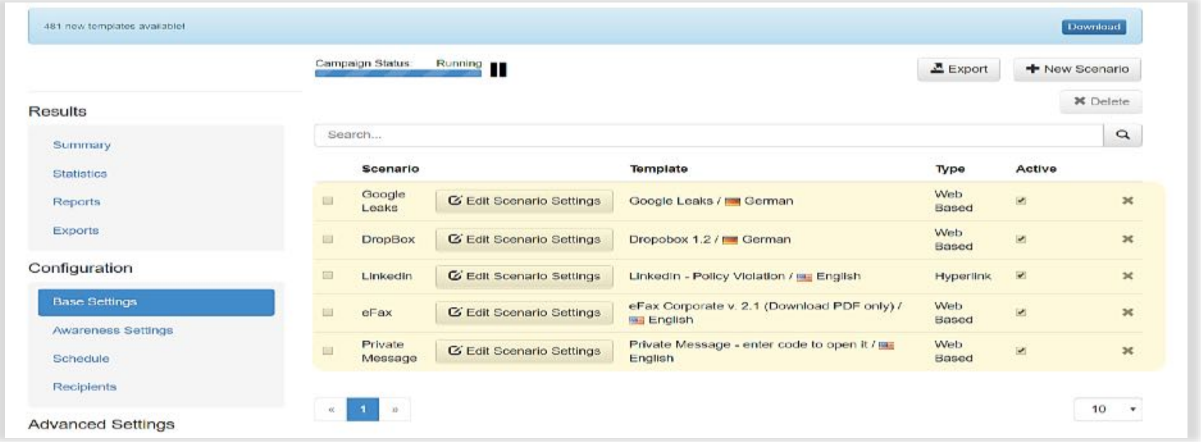
Message from HR
This scenario is based on a phishing scam from 2017 which was targeting companies with the subject "You have a message from HR".
17.12.2018 17:13:03

Message from HR (hyperlink)
This scenario is based on a phishing scam from 2017 which was targeting companies with the subject "You have a message from HR".
17.12.2018 17:13:03

base templates,
all campaigns.

plate for a specific
d to edit the landing
he campaign base

- **Simultaneous attack template usage**: LUCY gives you the option to use multiple simulated attack templates in a single campaign. Mix the different types (hyperlink, file-based, etc.) with different attack themes to achieve the largest possible risk coverage and a better understanding of employee vulnerabilities. In combination with our scheduling randomizer, complex attack patterns can be executed over a longer period of time.

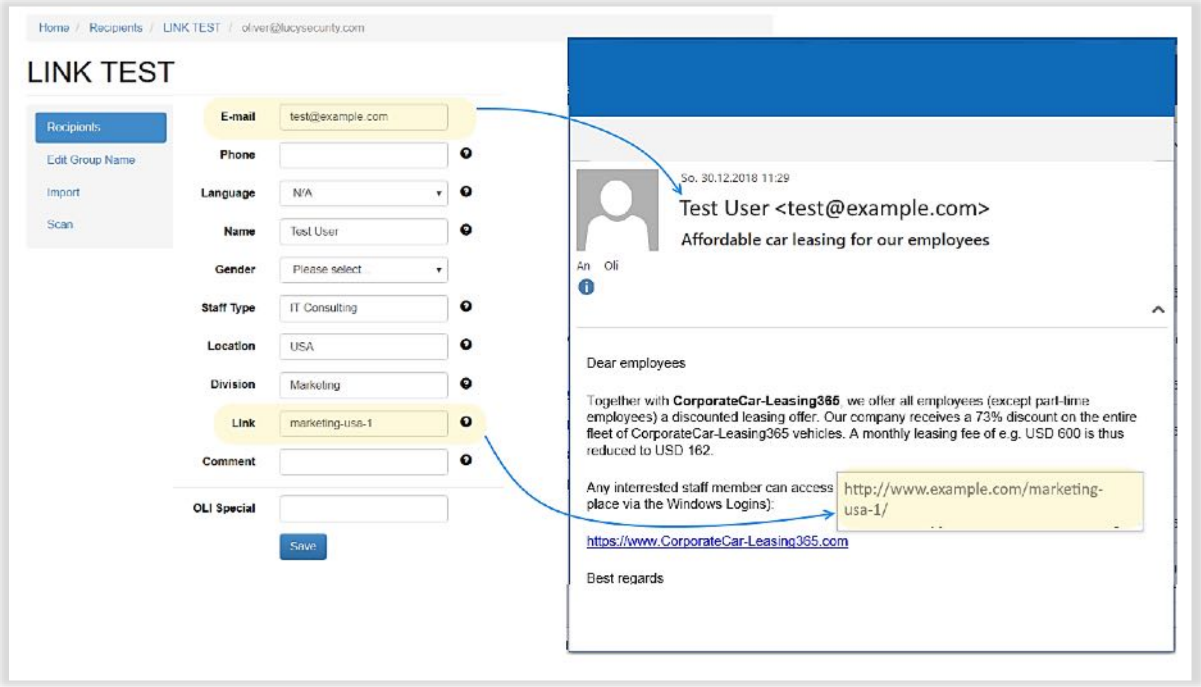


481 new templates available!

Campaign Status: Running

	Scenario		Template	Type	Active	
□	Google Leaks	Edit Scenario Settings	Google Leaks / German	Web Based	✓	✖
□	DropBox	Edit Scenario Settings	Dropobox 1.2 / German	Web Based	✓	✖
□	Linkedin	Edit Scenario Settings	Linkedin - Policy Violation / English	Hyperlink	✓	✖
□	eFax	Edit Scenario Settings	eFax Corporate v. 2.1 (Download PDF only) / English	Web Based	✓	✖
□	Private Message	Edit Scenario Settings	Private Message - enter code to open it / English	Web Based	✓	✖

- **Attack URL variations:** Take control of the generated URLs to identify the recipients. Use automated short (< 5 characters) or long URL strings or set individual URLs for each user. The manual URL creation allows you to form links that a user can easily remember. In environments where link clicks are disabled in e-mails, this is a must.



LINK TEST

E-mail	test@example.com
Phone	
Language	N/A
Name	Test User
Gender	Please select
Staff Type	IT Consulting
Location	USA
Division	Marketing
Link	marketing-usa-1
Comment	
OLI Special	

So. 30.12.2018 11:29

Test User <test@example.com>

Affordable car leasing for our employees

An Oli

Dear employees

Together with **CorporateCar-Leasing365**, we offer all employees (except part-time employees) a discounted leasing offer. Our company receives a 73% discount on the entire fleet of CorporateCar-Leasing365 vehicles. A monthly leasing fee of e.g. USD 600 is thus reduced to USD 162.

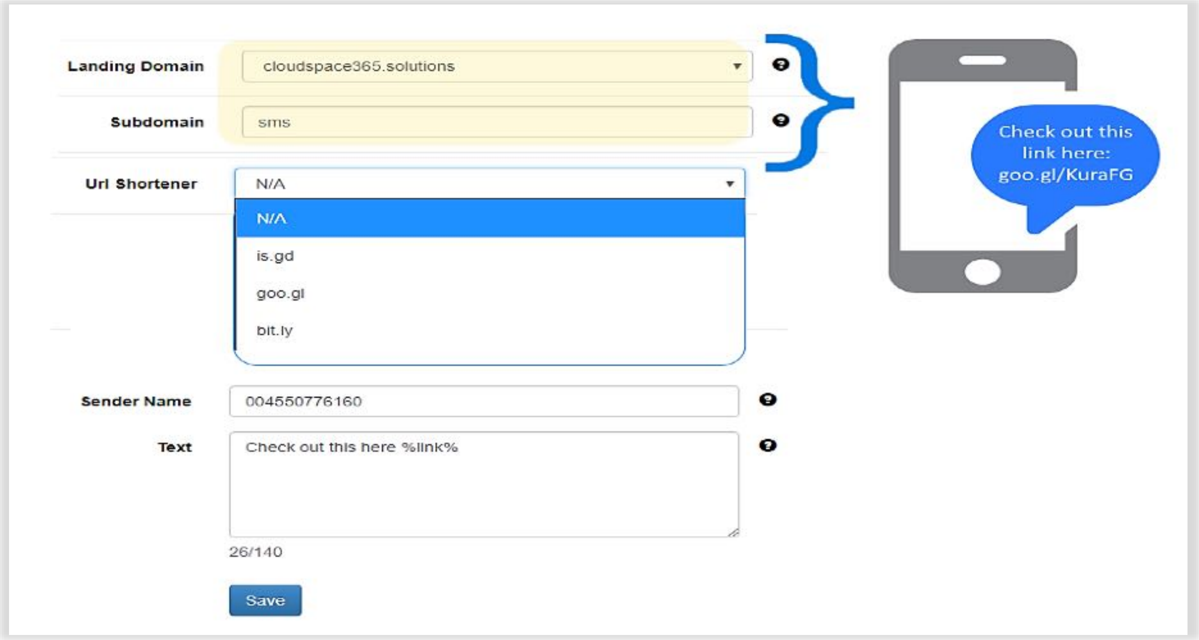
Any interrested staff member can access place via the Windows Logins):

http://www.example.com/marketing-usa-1/

https://www.CorporateCar-Leasing365.com

Best regards

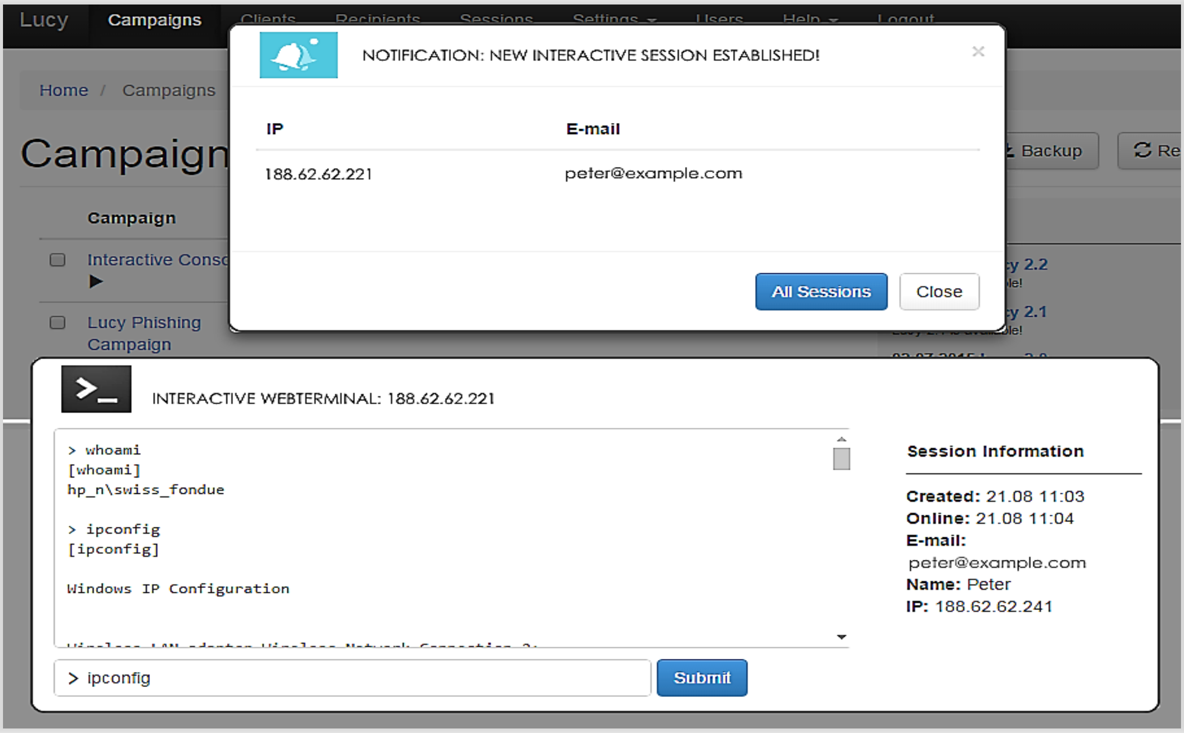
- **URL shortening:** URL shorteners are a relatively new Internet service. As many online social services impose character limitations (e.g., Twitter), these URLs are very practical. URL shorteners, however, can be used by cyber criminals to hide the real target of a link, such as phishing or infected websites. For this reason, LUCY offers the possibility to integrate different shortener services within a phishing or smishing campaign.



Landing Domain	cloudspace365.solutions
Subdomain	sms
Url Shortener	N/A
Sender Name	004550776160
Text	Check out this here %link%

26/140

- **Pentest kit:** The pentest kit is a submodule of the malware simulation toolkit and goes by the name "Interactive Sessions." It allows you to communicate interactively with a client pc that sits behind firewalls by using reverse http/s connections.



NOTIFICATION: NEW INTERACTIVE SESSION ESTABLISHED!

IP	E-mail
188.62.62.221	peter@example.com

INTERACTIVE WEBTERMINAL: 188.62.62.221

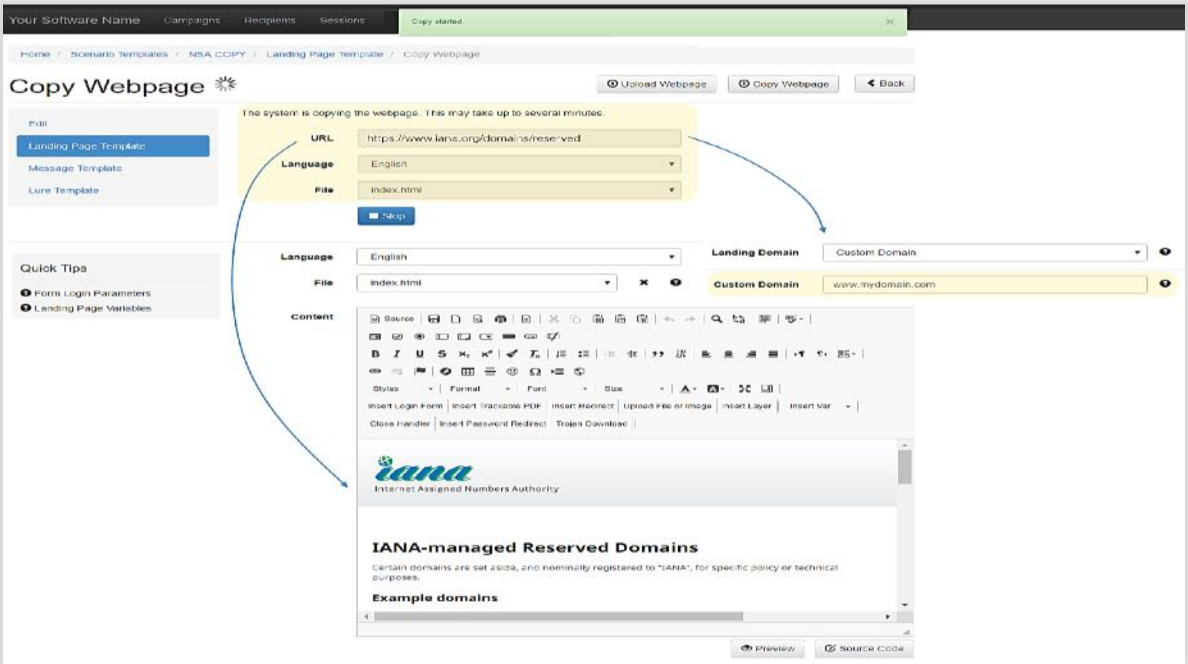
```
> whoami
[whoami]
hp_n\swiss_fondue

> ipconfig
[ipconfig]

Windows IP Configuration

Wireless LAN adapter Wireless Network Connection 2:
```

> ipconfig

Session Information

Created: 21.08 11:03
Online: 21.08 11:04
E-mail:
peter@example.com
Name: Peter
IP: 188.62.62.241

- **Website cloner:** Quickly create highly professional landing pages for your campaigns. Clone existing websites and add additional layers with data entry fields, files for download, and more.



Copy started.

Copy Webpage

The system is copying the webpage. This may take up to several minutes.

URL: https://www.iana.org/domains/reserved
Language: English
File: index.html

Language: English
File: index.html
Landing Domain: Custom Domain
Custom Domain: www.mydomain.com
Content:

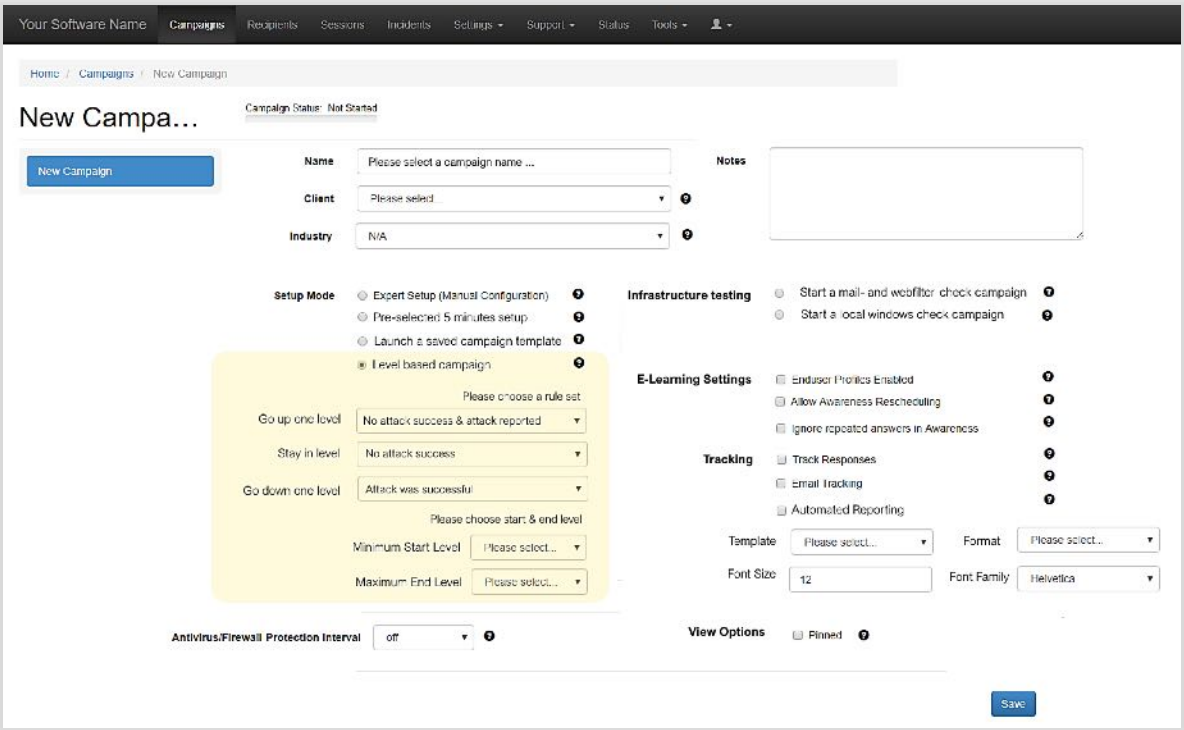
Internet Assigned Numbers Authority

IANA-managed Reserved Domains

Certain domains are set aside, and nominally registered to "IANA", for specific policy or technical purposes.

Example domains

- **Level-based attacks:** Level-based phishing training for employees serves to make the risk of social hacking measurable. Scientific analysis should also identify the most important risk factors so that individual training content can be offered automatically.



New Campa...

Campaign Status: Not Started

Name: Please select a campaign name ...

Client: Please select ▾

Industry: N/A ▾

Notes:

Setup Mode:
○ Expert Setup (Manual Configuration)
○ Pre-selected 5 minutes setup
○ Launch a saved campaign template
● Level based campaign

Please choose a rule set

Go up one level: No attack success & attack reported ▾

Stay in level: No attack success ▾

Go down one level: Attack was successful ▾

Please choose start & end level

Minimum Start Level: Please select... ▾

Maximum End Level: Please select... ▾

Antivirus/Firewall Protection Interval: off ▾

Infrastructure testing:
○ Start a mail- and webfilter check campaign
○ Start a local windows check campaign

E-Learning Settings:
□ Enduser Profiles Enabled
□ Allow Awareness Rescheduling
□ Ignore repeated answers in Awareness

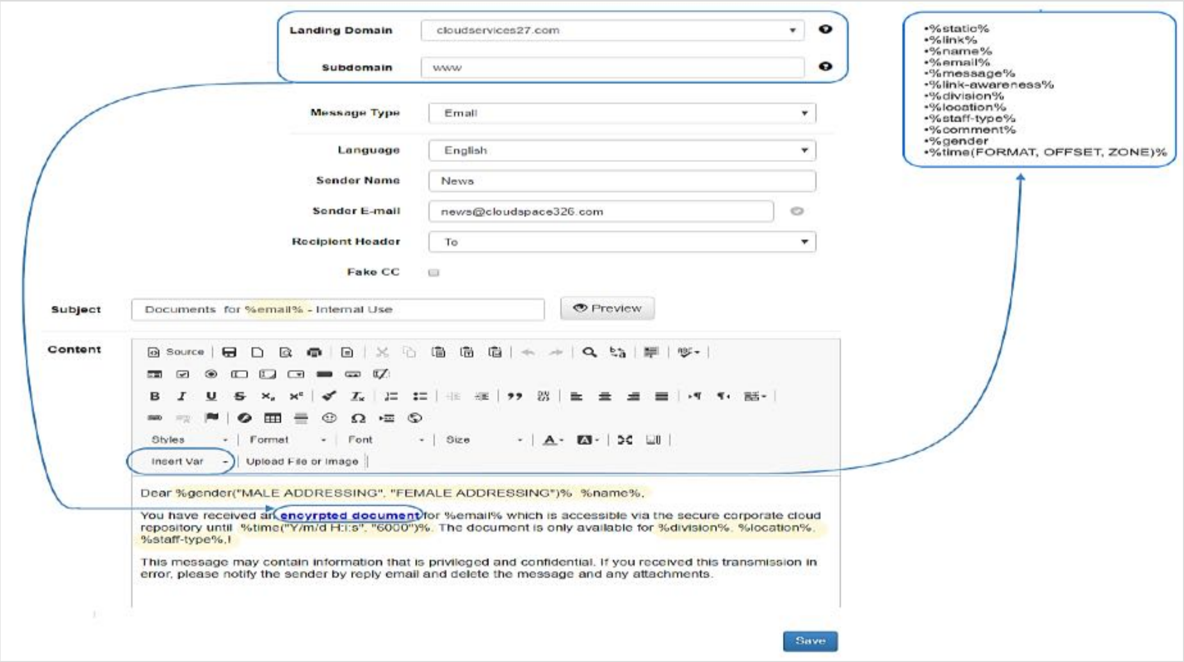
Tracking:
□ Track Responses
□ Email Tracking
□ Automated Reporting

Template: Please select... ▾ Format: Please select... ▾

Font Size: 12 Font Family: Helvetica ▾

View Options: □ Pinned

- **Spear phishing simulation:** The Spear Phish Tailoring works with dynamic variables (gender, time, name, e-mail, links, messages, division, country, etc.) which you can use in landing and message templates.



Landing Domain: cloudservices27.com ▾

Subdomain: www

Message Type: Email ▾

Language: English ▾

Sender Name: News

Sender E-mail: news@cloudspace326.com

Recipient Header: To ▾

Fake CC: □

Subject: Documents for %email% - Internal Use

Content:

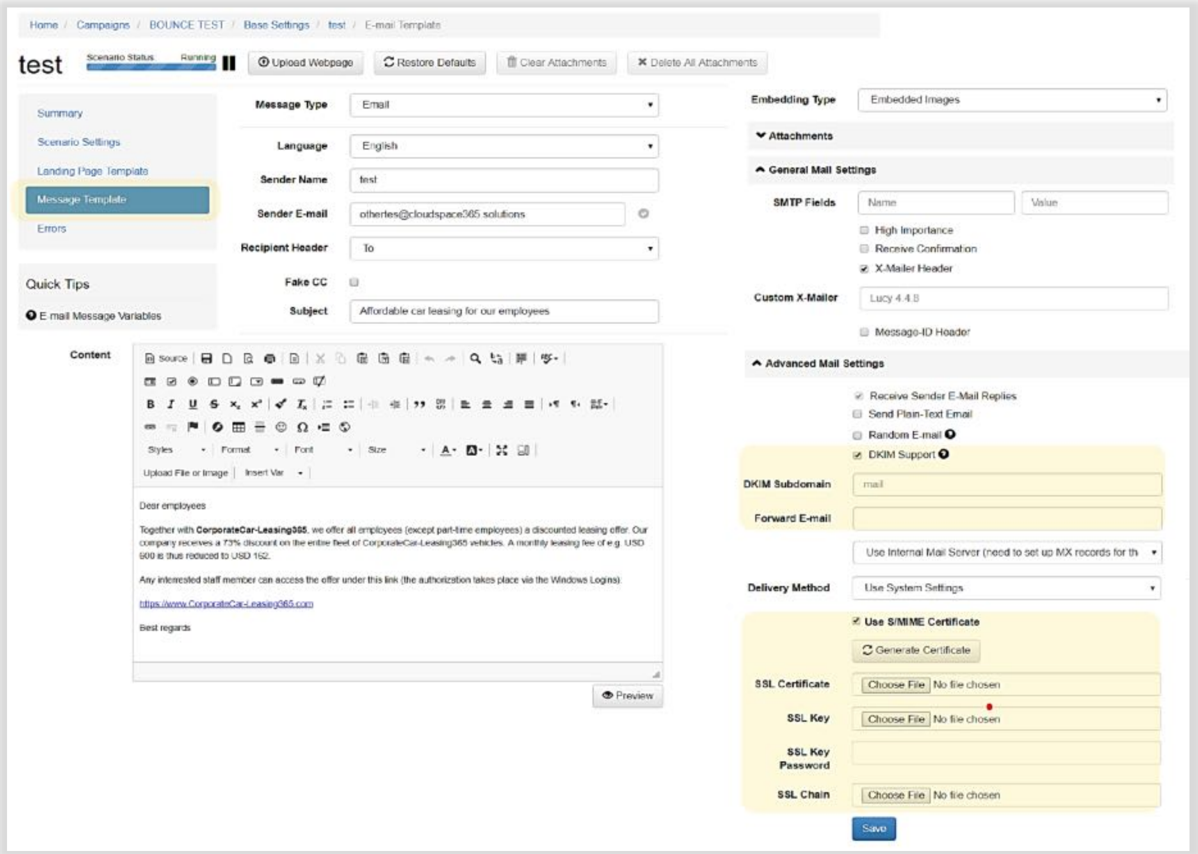
Dear %gender("MALE ADDRESSING", "FEMALE ADDRESSING")% %name%,

You have received an encyrpted document for %email% which is accessible via the secure corporate cloud repository until %time("Y/m/d H:i:s", "6000")%. The document is only available for %division%, %location%, %staff-type%.

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.

- %static%
- %link%
- %name%
- %email%
- %message%
- %link-awareness%
- %division%
- %location%
- %staff-type%
- %comment%
- %gender
- %time(FORMAT, OFFSET, ZONE)%

- **DKIM / S / MIME Support for Phishing e-Mails:** Digital signatures for e-mails: Send signed phishing simulation mails (s/mime). Use DKIM to get a better sender score.



Home / Campaigns / BOUNCE TEST / Base Settings / test / E-mail Template

test — Scenario Status: Running

Message Type: Email

Language: English

Sender Name: test

Sender E-mail: otherles@cloudspace365.solutions

Recipient Header: To

Fake CC: □

Subject: Affordable car leasing for our employees

Content:

Dear employees

Together with **CorporateCar-Leasing365**, we offer all employees (except part-time employees) a discounted leasing offer. Our company receives a 73% discount on the entire fleet of CorporateCar-Leasing365 vehicles. A monthly leasing fee of e.g. USD 600 is thus reduced to USD 162.

Any interested staff member can access the offer under this link (the authorization takes place via the Windows Logins).

https://www.CorporateCar-Leasing365.com

Best regards

Embedding Type: Embedded Images

Attachments

General Mail Settings

SMTP Fields: Name | Value

□ High Importance

□ Receive Confirmation

☑ X-Mailer Header

Custom X-Mailer: Lucy 4.4.8

□ Message-ID Header

Advanced Mail Settings

☑ Receive Sender E-Mail Replies

□ Send Plain-Text Email

□ Random E-mail

☑ DKIM Support

DKIM Subdomain: mail

Forward E-mail:

Use Internal Mail Server (need to set up MX records for th

Delivery Method: Use System Settings

☑ Use S/MIME Certificate

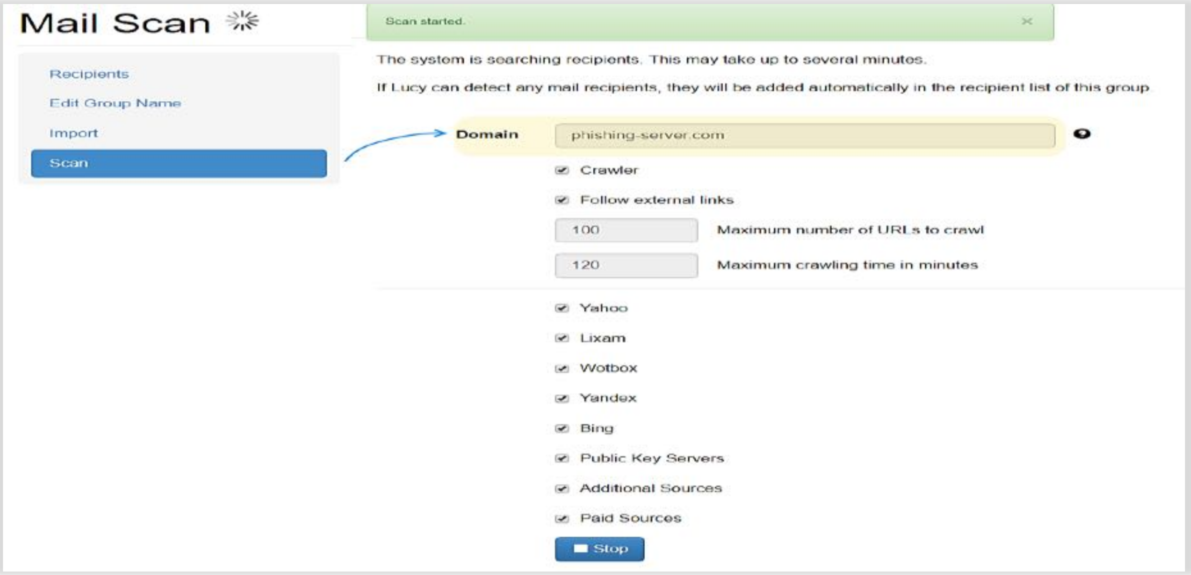
SSL Certificate: Choose File No file chosen

SSL Key: Choose File No file chosen

SSL Key Password:

SSL Chain: Choose File No file chosen

- **Mail scanner:** Curious which e-mail addresses in your organization can be found on the Internet? Use LUCY's mail scanner and find out what a hacker already knows about your company.



Mail Scan

Scan started.

The system is searching recipients. This may take up to several minutes.

If Lucy can detect any mail recipients, they will be added automatically in the recipient list of this group.

Domain: phishing-server.com

☑ Crawler

☑ Follow external links

100 Maximum number of URLs to crawl

120 Maximum crawling time in minutes

☑ Yahoo

☑ Lixam

☑ Wotbox

☑ Yandex

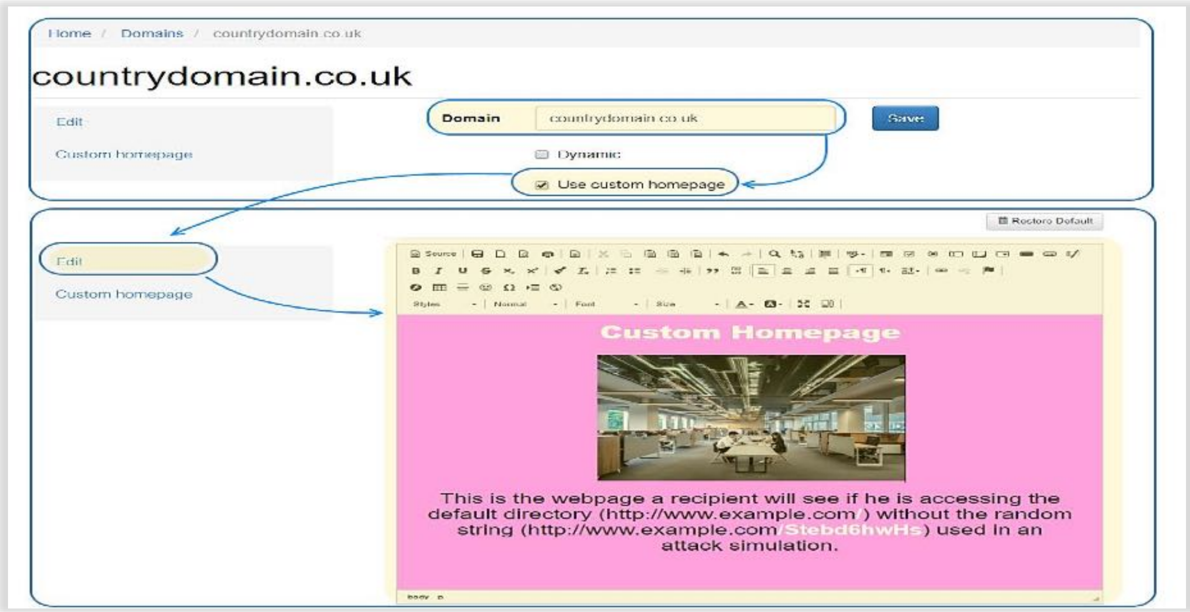
☑ Bing

☑ Public Key Servers

☑ Additional Sources

☑ Paid Sources

- **Custom homepage creation:** Recipients with a better technical understanding could use their browser to call the domain or IP address associated with the randomly generated phishing link. To prevent error messages from appearing or the end user from even coming to the login area of the admin console, you can create generic "homepages" within LUCY for the domains used in the phishing simulation.



Home / Domains / countrydomain.co.uk

countrydomain.co.uk

Edit
Custom homepage

Domain: countrydomain.co.uk

Save

☐ Dynamic

☑ Use custom homepage

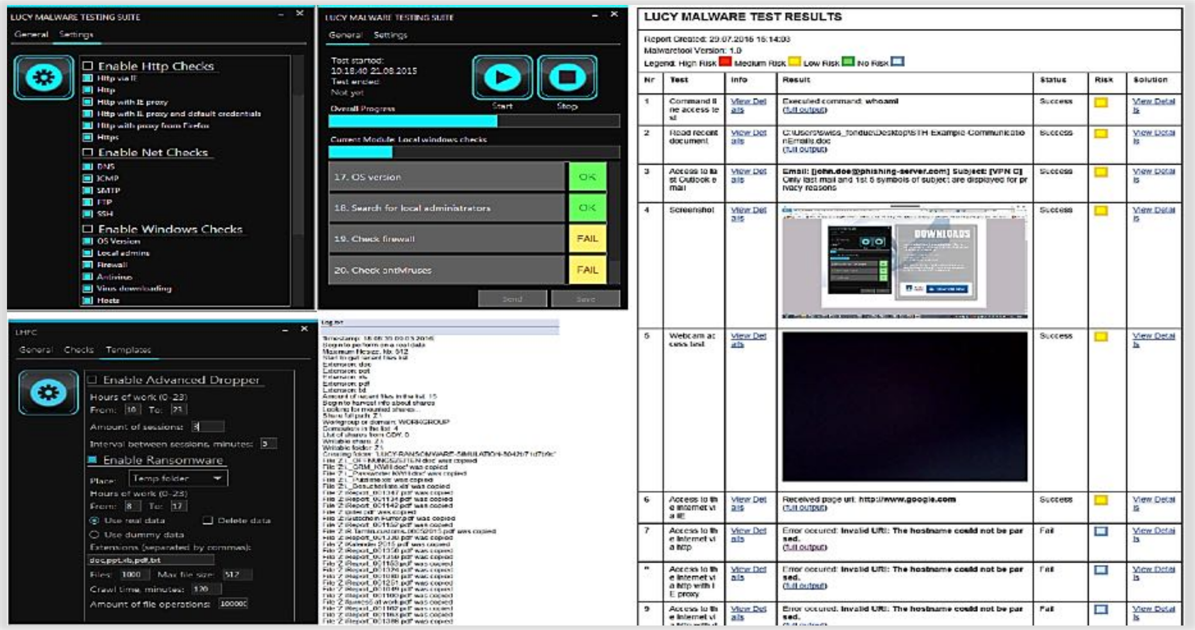
Restore Default

Custom Homepage

This is the webpage a recipient will see if he is accessing the default directory (http://www.example.com/) without the random string (http://www.example.com/Stebd6hwHs) used in an attack simulation.

TEST INFRASTRUCTURE

- **Malware Testing Toolkit:** The Malware Simulation Toolkit is an advanced malware simulation suite capable of emulating various threats. It allows an auditor to access an advanced set of features equivalent to many of the tools employed by cyber criminals. The tool, therefore, allows the LUCY administrator to perform security checks without involving employees outside the IT department.



LUCY MALWARE TESTING SUITE

General | Settings

☐ Enable Http Checks
☑ Http via IE
☑ Http
☑ Http with IE proxy
☑ Http with IE proxy and default credentials
☑ Http with proxy from Firefox
☑ Https

☐ Enable Net Checks
☑ DNS
☑ ICMP
☑ SMTP
☑ FTP
☑ SSH

☐ Enable Windows Checks
☑ OS Version
☑ Local admins
☑ Firewall
☑ Antivirus
☑ Virus downloading
☑ Hosts

LUCY MALWARE TESTING SUITE

General | Settings

Test started:
10.18.40 21.08.2015
Test ended:
Not yet

Overall Progress

Current Module: Local windows checks

17. OS version — OK
18. Search for local administrators — OK
19. Check firewall — FAIL
20. Check antiviruses — FAIL

LHFC

General | Checks | Templates

☐ Enable Advanced Dropper
Hours of work (0-23)
From: 10 To: 23
Amount of sessions: 3
Interval between sessions, minutes: 5

☑ Enable Ransomware
Place: Temp folder
Hours of work (0-23)
From: 8 To: 17
● Use real data ☐ Delete data
○ Use dummy data
Extensions (separated by comma):
doc,ppt,xls,pdf,txt
Files: 1000 Max file size: 512
Crawl time, minutes: 120
Amount of file operations: 100000

Log.txt

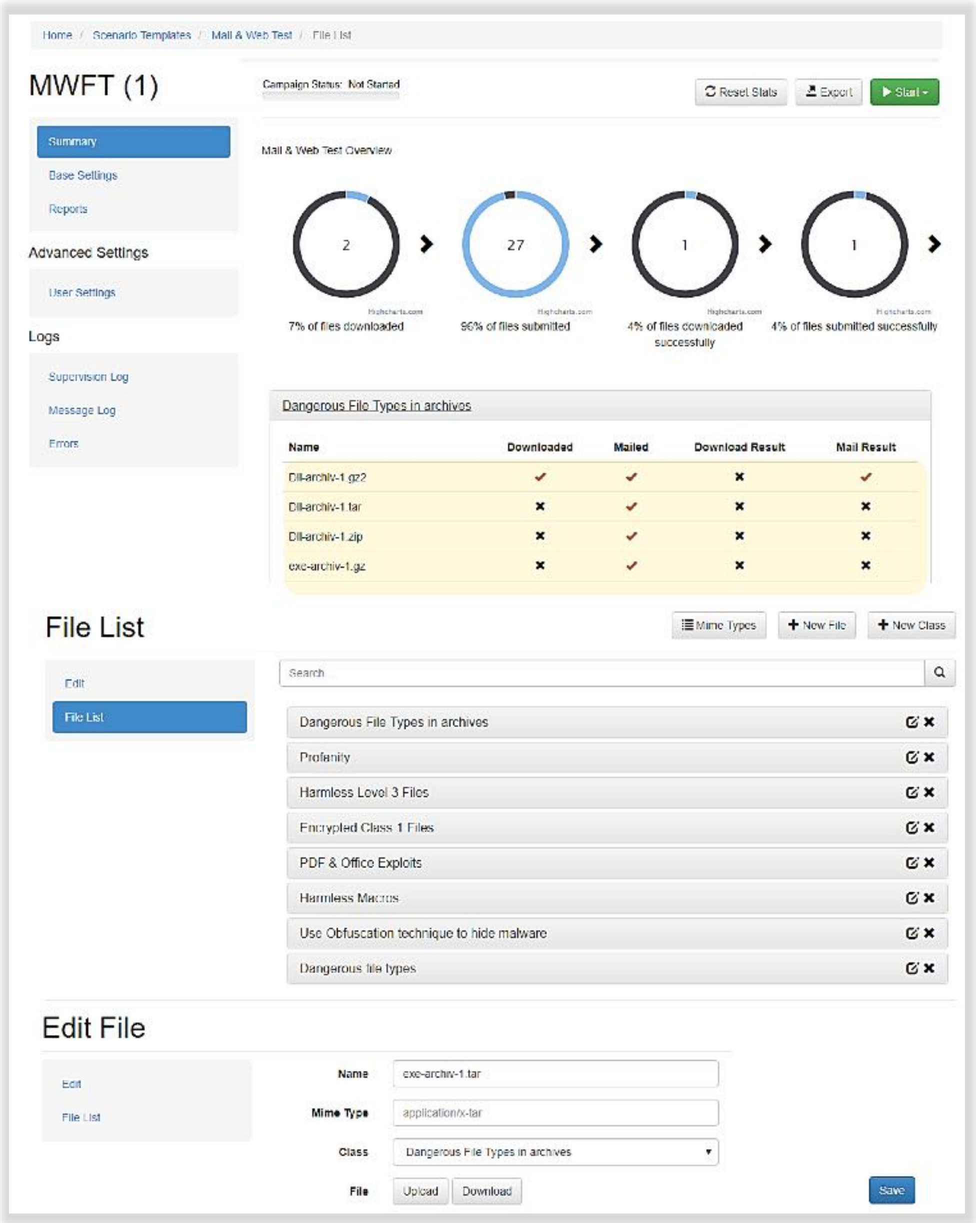
```
Timestamp: 16:06:30 09.03.2016
Begin to perform on a real data
Maximum filesize, Kb: 512
Start to get recent files list
Extension: doc
Extension: ppt
Extension: xls
Extension: pdf
Extension: txt
Amount of recent files in the list: 15
Begin to harvest info about shares
Looking for mounted shares...
Share full path: Z:\
Workgroup or domain: WORKGROUP
Computers in the list: 4
List of shares from CDY: 0
Writable share: Z:\
Writable folder: Z:\
Creating folder: 'LUCY-RANSOMWARE-SIMULATION-[illegible]'
File 'Z:\_OFFNUNGSZEITEN.doc' was copied
File 'Z:\_ORM_KWII.doc' was copied
File 'Z:\_Parameter KWII.doc' was copied
File 'Z:\_[illegible].xls' was copied
File 'Z:\_Besucherliste.xls' was copied
File 'Z:\Report_001347.pdf' was copied
File 'Z:\Report_001134.pdf' was copied
File 'Z:\Report_001142.pdf' was copied
File 'Z:\[illegible].pdf' was copied
File 'Z:\Gutschein Furor.pdf' was copied
File 'Z:\Report_001152.pdf' was copied
File 'Z:\R.Termin.customs.[illegible].pdf' was copied
File 'Z:\Report_001330.pdf' was copied
File 'Z:\Kalender 2015.pdf' was copied
File 'Z:\Report_001350.pdf' was copied
File 'Z:\Report_001350.pdf' was copied
File 'Z:\Report_001153.pdf' was copied
File 'Z:\Report_001326.pdf' was copied
File 'Z:\Report_001080.pdf' was copied
File 'Z:\Report_001251.pdf' was copied
File 'Z:\Report_001049.pdf' was copied
File 'Z:\Report_001100.pdf' was copied
File 'Z:\Success at work.pdf' was copied
File 'Z:\Report_001162.pdf' was copied
File 'Z:\Report_001163.pdf' was copied
File 'Z:\Report_001388.pdf' was copied
```

LUCY MALWARE TEST RESULTS

Report Created: 29.07.2016 16:14:03
Malwaretool Version: 1.0
Legend: High Risk 🟥 Medium Risk 🟨 Low Risk 🟩 No Risk ☐

Nr	Test	Info	Result	Status	Risk	Solution
1	Command line access test	View Details	Executed command: **whoami** (full output)	Success	🟨	View Details
2	Read recent document	View Details	C:\Users\swiss_fondue\Desktop\STH Example CommunicationEmails.doc (full output)	Success	🟨	View Details
3	Access to last Outlook e mail	View Details	**Email: [john.doe@phishing-server.com] Subject: [VPN C]** Only last mail and 1st 5 symbols of subject are displayed for privacy reasons	Success	🟨	View Details
4	Screenshot	View Details		Success	🟨	View Details
5	Webcam access test	View Details		Success	🟨	View Details
6	Access to the internet via IE	View Details	Received page url: **http://www.google.com** (full output)	Success	🟨	View Details
7	Access to the internet via http	View Details	Error occured: **Invalid URI: The hostname could not be parsed.** (full output)	Fail	☐	View Details
8	Access to the internet via http with IE proxy	View Details	Error occured: **Invalid URI: The hostname could not be parsed.** (full output)	Fail	☐	View Details
9	Access to the internet via http with d	View Details	Error occured: **Invalid URI: The hostname could not be parsed.** (full output)	Fail	☐	View Details

- **Mail and Web Filter Test:** This functionality provides the answer to one of the most important questions in securing Internet and mail traffic: Which file types can be downloaded from the Web, and which e-mail attachments are filtered out or not?



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

MWFT (1)

Campaign Status: Not Started

Mail & Web Test Overview

7% of files downloaded

96% of files submitted

4% of files downloaded successfully

4% of files submitted successfully

Dangerous File Types in archives

Name	Downloaded	Mailed	Download Result	Mail Result
Dll-archiv-1.gz2	✓	✓	✗	✓
Dll-archiv-1.tar	✗	✓	✗	✗
Dll-archiv-1.zip	✗	✓	✗	✗
exe-archiv-1.gz	✗	✓	✗	✗

File List

- Dangerous File Types in archives
- Profanity
- Harmless Level 3 Files
- Encrypted Class 1 Files
- PDF & Office Exploits
- Harmless Macros
- Use Obfuscation technique to hide malware
- Dangerous file types

Edit File

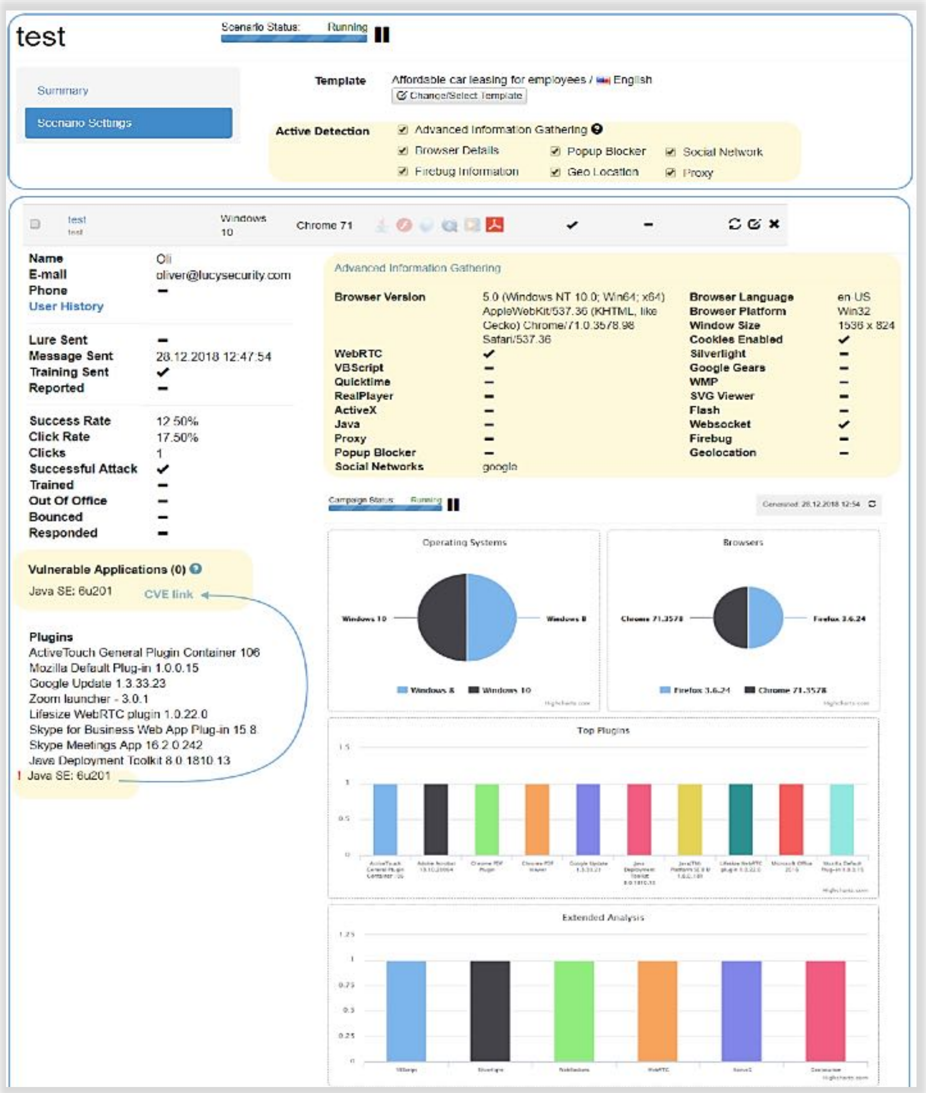
Name: exe-archiv-1.tar

Mime Type: application/x-tar

Class: Dangerous File Types in archives

File: Upload Download

- **Active and Passive Client Vulnerability Detection:** This feature allows local testing of the client browser and detection of possible vulnerabilities based on custom JavaScript libraries and the browser's user agent data. The discovered plugins can be automatically compared with the vulnerability databases (CVE) to identify vulnerable devices.



test

Scenario Status: Running

Summary

Scenario Settings

Template: Affordable car leasing for employees / English

Change/Select Template

Active Detection:
☑ Advanced Information Gathering
☑ Browser Details ☑ Popup Blocker ☑ Social Network
☑ Firebug Information ☑ Geo Location ☑ Proxy

□	test test	Windows 10	Chrome 71	✓	–	

Name	Oli
E-mail	oliver@lucysecurity.com
Phone	–
User History	
Lure Sent	–
Message Sent	28.12.2018 12:47:54
Training Sent	✓
Reported	–
Success Rate	12.50%
Click Rate	17.50%
Clicks	1
Successful Attack	✓
Trained	–
Out Of Office	–
Bounced	–
Responded	–

Advanced Information Gathering

Browser Version	5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/71.0.3578.98 Safari/537.36	Browser Language	en US
		Browser Platform	Win32
		Window Size	1536 x 824
		Cookies Enabled	✓
WebRTC	✓	Silverlight	–
VBScript	–	Google Gears	–
Quicktime	–	WMP	–
RealPlayer	–	SVG Viewer	–
ActiveX	–	Flash	–
Java	–	Websocket	✓
Proxy	–	Firebug	–
Popup Blocker	–	Geolocation	–
Social Networks	google		

Vulnerable Applications (0)

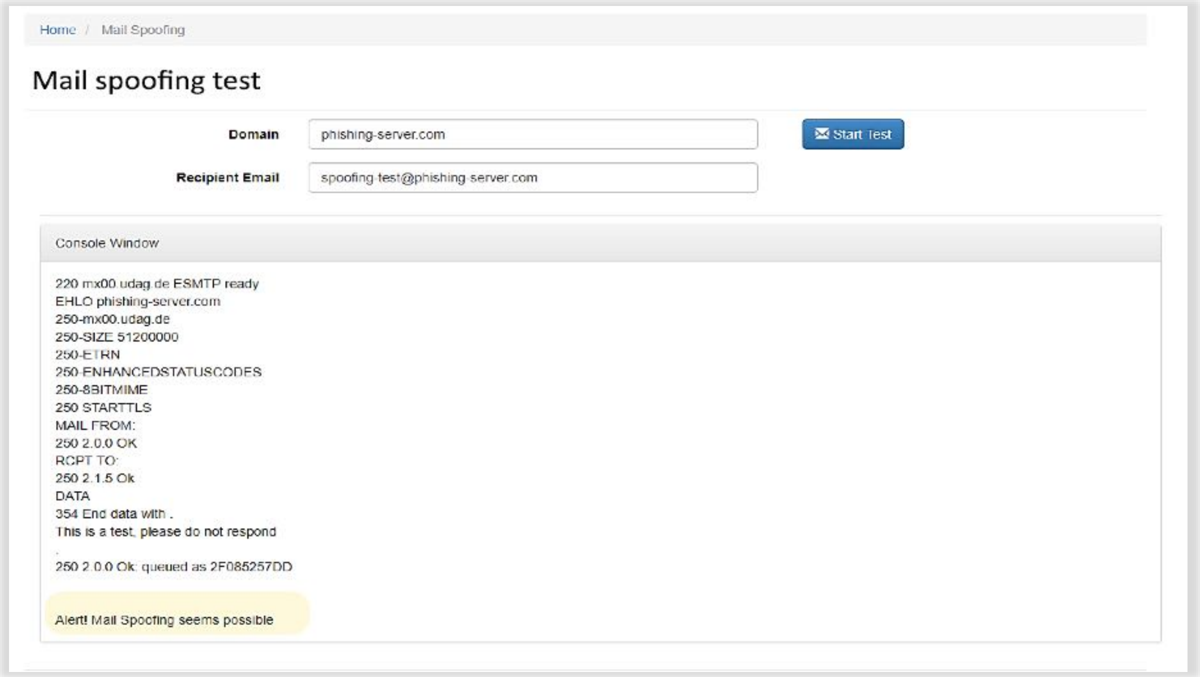
Java SE: 6u201 CVE link

Plugins
ActiveTouch General Plugin Container 106
Mozilla Default Plug-in 1.0.0.15
Google Update 1.3.33.23
Zoom launcher - 3.0.1
Lifesize WebRTC plugin 1.0.22.0
Skype for Business Web App Plug-in 15.8
Skype Meetings App 16.2.0.242
Java Deployment Toolkit 8.0.1810.13
! Java SE: 6u201

Campaign Status: Running

Generated: 28.12.2018 12:54

- **Spoofing Test:** Test your own infrastructure for mail spoofing vulnerabilities.



Mail spoofing test

Domain: phishing-server.com

Recipient Email: spoofing-test@phishing-server.com

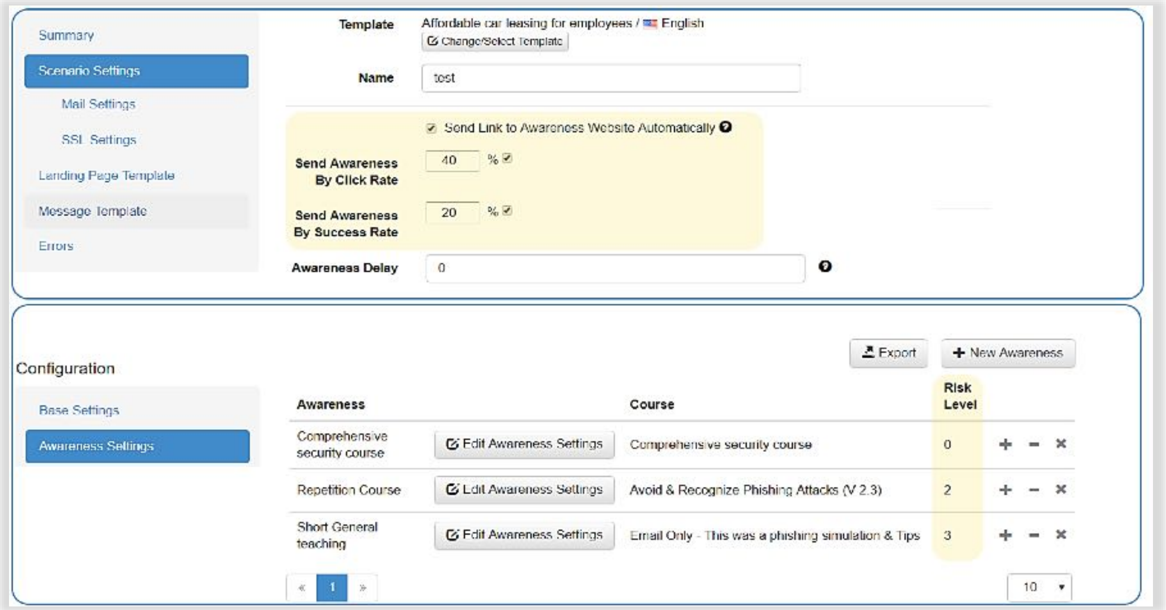
Console Window

```
220 mx00.udag.de ESMTP ready
EHLO phishing-server.com
250-mx00.udag.de
250-SIZE 51200000
250-ETRN
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 STARTTLS
MAIL FROM:
250 2.0.0 OK
RCPT TO:
250 2.1.5 Ok
DATA
354 End data with .
This is a test, please do not respond
.
250 2.0.0 Ok: queued as 2F085257DD
```

Alert! Mail Spoofing seems possible

TECHNICAL TESTING

- **Reputation-Based e-Learning:** Train your employees according to their required skills. Measure employee abilities and enable friendly competition between colleagues (gamification).
  Based on the reputation profiles of each end user, the system can automatically provide them with multiple training sessions. The reputation profiles are based, among other factors, on the user's behaviour in phishing simulations. This ensures that users who are repeated offenders receive different training content from those who click on an attack simulation for the first time.



Template: Affordable car leasing for employees / English

Name: test

☑ Send Link to Awareness Website Automatically

Send Awareness By Click Rate: 40 % ☑

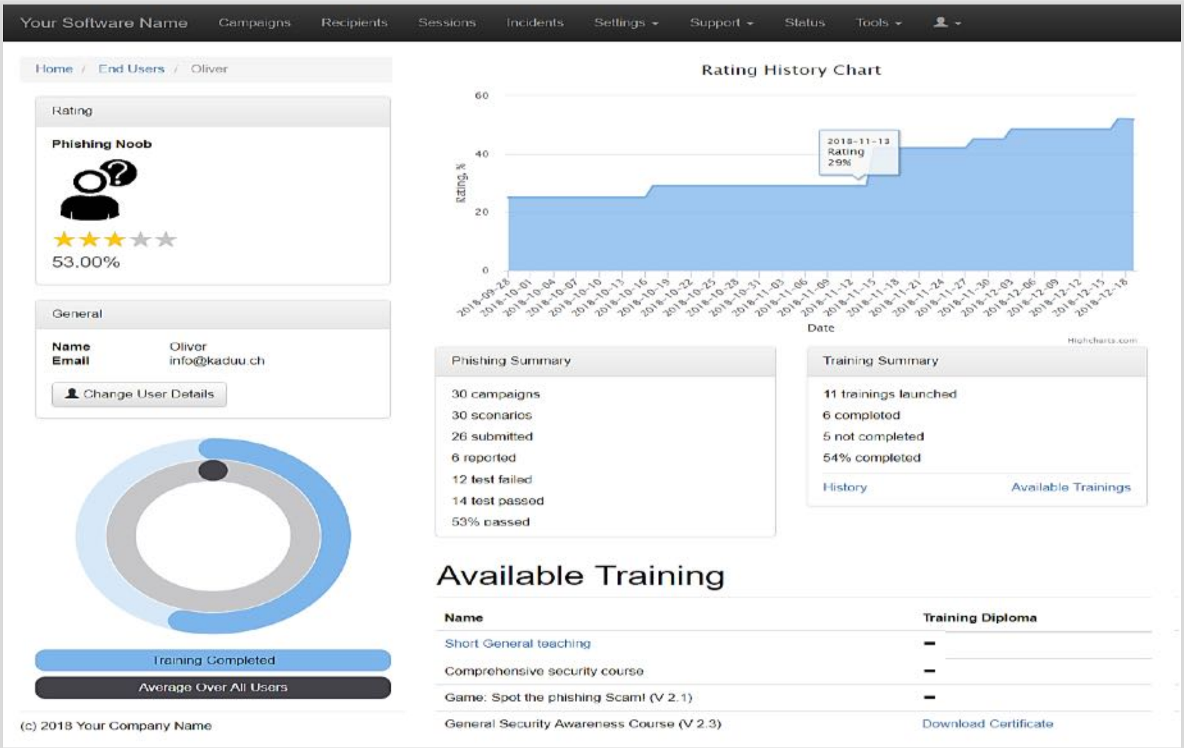
Send Awareness By Success Rate: 20 % ☑

Awareness Delay: 0

Configuration

Awareness		Course	Risk Level
Comprehensive security course	Edit Awareness Settings	Comprehensive security course	0
Repetition Course	Edit Awareness Settings	Avoid & Recognize Phishing Attacks (V 2.3)	2
Short General teaching	Edit Awareness Settings	Email Only - This was a phishing simulation & Tips	3

- **End user Training Portal:** Learning Management System (LMS) functionality: Gives each employee permanent access to a personalized training homepage that features your own courses specifically tailored for them. On this homepage they can view their performance statistics, resume or repeat training, create course certificates, and compare their results with other departments or groups.



Rating

Phishing Noob

★★★☆☆
53.00%

General

Name Oliver
Email info@kaduu.ch

Phishing Summary

30 campaigns
30 scenarios
26 submitted
6 reported
12 test failed
14 test passed
53% passed

Training Summary

11 trainings launched
6 completed
5 not completed
54% completed

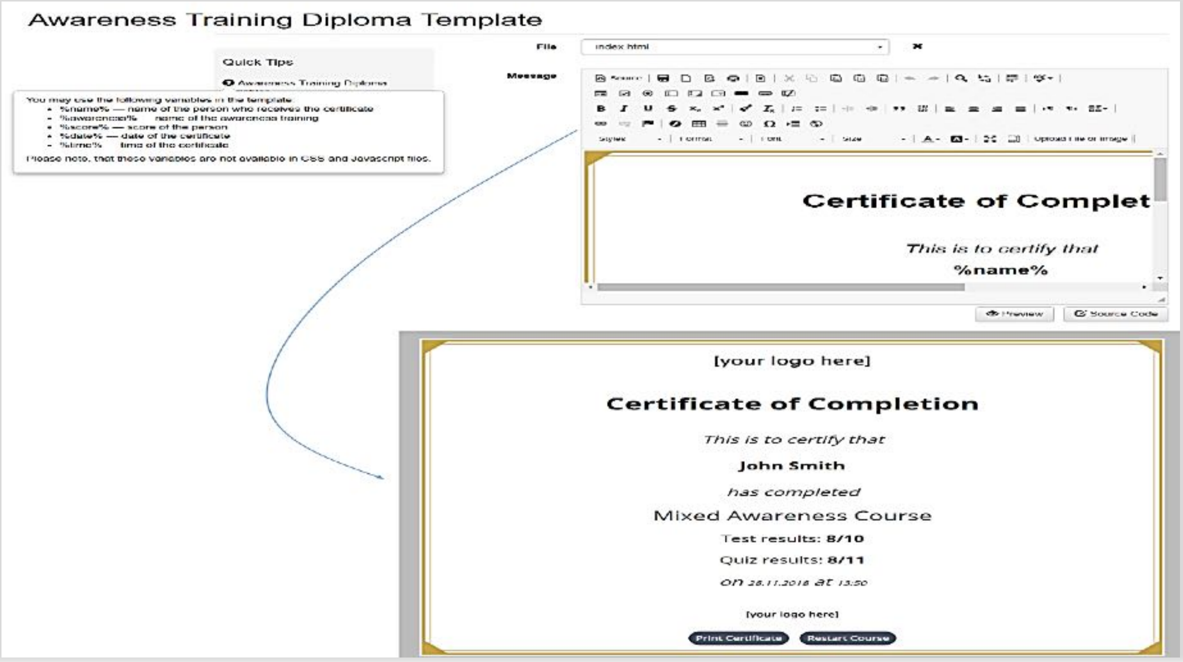
History Available Trainings

Available Training

Name	Training Diploma
Short General teaching	–
Comprehensive security course	–
Game: Spot the phishing Scam! (V 2.1)	–
General Security Awareness Course (V 2.3)	Download Certificate

(c) 2018 Your Company Name

- **Awareness Education Diploma:** Certificates of e-Learning can be created and printed out by the recipient either directly within a training or inside the LMS portal.



Awareness Training Diploma Template

Quick Tips

Awareness Training Diploma

You may use the following variables in the template:

- %name% — name of the person who receives the certificate
- %awareness% — name of the awareness training
- %score% — score of the person
- %date% — date of the certificate
- %time% — time of the certificate

Please note, that these variables are not available in CSS and Javascript files.

Certificate of Complet

This is to certify that

%name%

[your logo here]

Certificate of Completion

This is to certify that

John Smith

has completed

Mixed Awareness Course

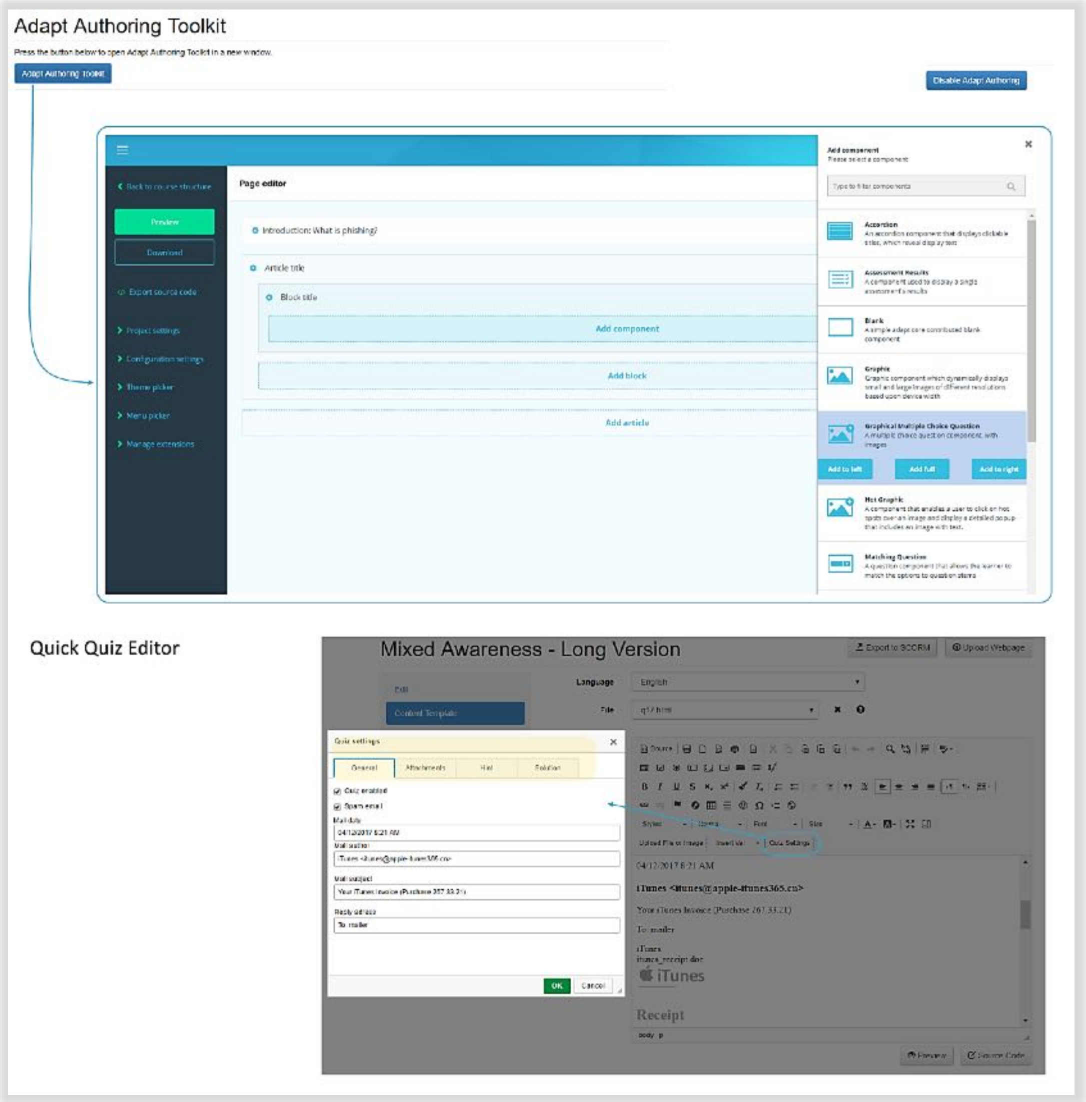
Test results: 8/10

Quiz results: 8/11

on 28.11.2018 at 13:50

[your logo here]

- **e-Learning Authoring Toolkit:** The e-Learning Authoring Toolkit (Adapt) allows the creation of individualized learning content. Drag and drop videos or any other rich media format, insert exams from pre-defined menus, create interactive e-learning content from scratch in a short time.



Adapt Authoring Toolkit

Press the button below to open Adapt Authoring Toolkit in a new window.

Accordion An accordion component that displays clickable titles, which reveal display text

Assessment Results A component used to display a single assessment's results

Blank A simple adapt core contributed blank component

Graphic Graphic component which dynamically displays small and large images of different resolutions based upon device width

Graphical Multiple Choice Question A multiple choice question component with images

Hot Graphic A component that enables a user to click on hot spots over an image and display a detailed popup that includes an image with text.

Matching Question A question component that allows the learner to match the options to question stems

Quick Quiz Editor

Mixed Awareness - Long Version

Language: English

File: q17.html

Quiz settings

☑ Quiz enabled

☑ Spam email

Mail date: 04/12/2017 8:21 AM

Mail author: iTunes <itunes@apple-itunes365.cn>

Mail subject: Your iTunes Invoice (Purchase 267 33.21)

Reply address: To: mailer

04/12/2017 8:21 AM

iTunes <itunes@apple-itunes365.cn>

Your iTunes Invoice (Purchase 267 33.21)

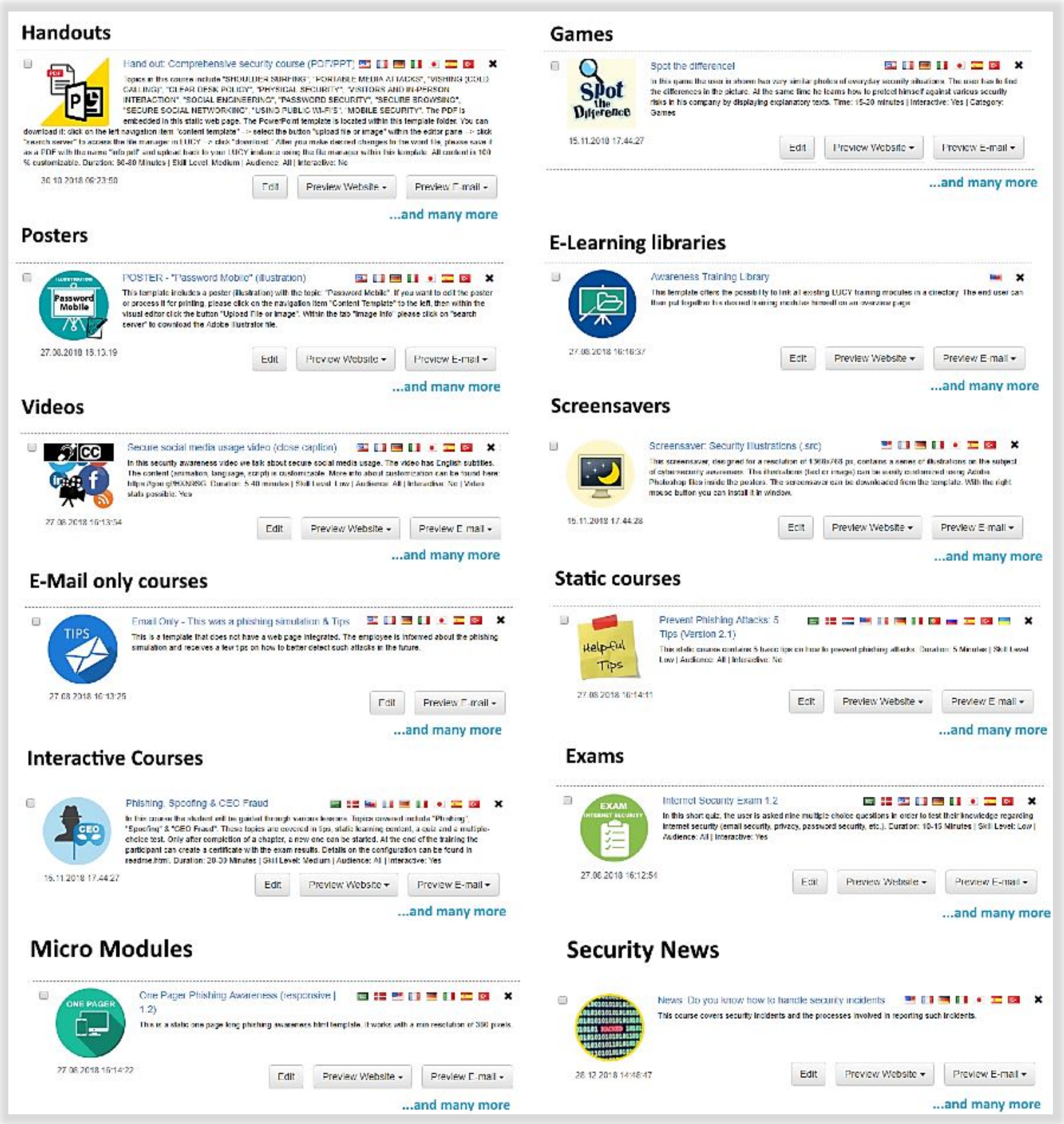
To: mailer

iTunes
itunes_receipt.doc

iTunes

Receipt

- **Rich Media Awareness Training:** Integrate rich media (video, audio, or other elements that encourage viewers to interact and engage with the content) in your awareness trainings. Use the existing educational videos, adapt them, or add your own rich media.



Handouts

Hand out: Comprehensive security course (PDF/PPT)

Topics in this course include "SHOULDER SURFING", "PORTABLE MEDIA ATTACKS", "VISHING (COLD CALLING)", "CLEAR DESK POLICY", "PHYSICAL SECURITY", "VISITORS AND IN-PERSON INTERACTION", "SOCIAL ENGINEERING", "PASSWORD SECURITY", "SECURE BROWSING", "SECURE SOCIAL NETWORKING", "USING PUBLIC WI-FI'S", "MOBILE SECURITY". The PDF is embedded in this static web page. The PowerPoint template is located within this template folder. You can download it: click on the left navigation item "content template" --> select the button "upload file or image" within the editor pane --> click "search server" to access the file manager in LUCY --> click "download." After you make desired changes to the word file, please save it as a PDF with the name "info.pdf" and upload back to your LUCY instance using the file manager within this template. All content is 100 % customizable. Duration: 60-80 Minutes | Skill Level: Medium | Audience: All | Interactive: No

30.10.2018 09:23:50

Posters

POSTER - "Password Mobile" (illustration)

This template includes a poster (illustration) with the topic: "Password Mobile". If you want to edit the poster or process it for printing, please click on the navigation item "Content Template" to the left, then within the visual editor click the button "Upload File or Image". Within the tab "Image Info" please click on "search server" to download the Adobe Illustrator file.

27.08.2018 15:13:19

Videos

Secure social media usage video (close caption)

In this security awareness video we talk about secure social media usage. The video has English subtitles. The content (animation, language, script) is customizable. More info about customization can be found here: https://goo.gl/[illegible] Duration: 5:40 minutes | Skill Level: Low | Audience: All | Interactive: No | Video stats possible: Yes

27.08.2018 16:13:54

E-Mail only courses

Email Only - This was a phishing simulation & Tips

This is a template that does not have a web page integrated. The employee is informed about the phishing simulation and receives a few tips on how to better detect such attacks in the future.

27.08.2018 16:13:25

Interactive Courses

Phishing, Spoofing & CEO Fraud

In this course the student will be guided through various lessons. Topics covered include "Phishing", "Spoofing" & "CEO Fraud". These topics are covered in tips, static learning content, a quiz and a multiple-choice test. Only after completion of a chapter, a new one can be started. At the end of the training the participant can create a certificate with the exam results. Details on the configuration can be found in readme.html. Duration: 20-30 Minutes | Skill Level: Medium | Audience: All | Interactive: Yes

16.11.2018 17:44:27

Micro Modules

One Pager Phishing Awareness (responsive | 1.2)

This is a static one page long phishing awareness html template. It works with a min resolution of 390 pixels.

27.08.2018 16:14:22

Games

Spot the difference!

In this game the user is shown two very similar photos of everyday security situations. The user has to find the differences in the picture. At the same time he learns how to protect himself against various security risks in his company by displaying explanatory texts. Time: 15-20 minutes | Interactive: Yes | Category: Games

15.11.2018 17:44:27

E-Learning libraries

Awareness Training Library

This template offers the possibility to link all existing LUCY training modules in a directory. The end user can then put together his desired training modules himself on an overview page.

27.08.2018 16:16:37

Screensavers

Screensaver: Security Illustrations (.src)

This screensaver, designed for a resolution of 1366x768 px, contains a series of illustrations on the subject of cybersecurity awareness. The illustrations (text or image) can be easily customized using Adobe Photoshop files inside the posters. The screensaver can be downloaded from the template. With the right mouse button you can install it in window.

15.11.2018 17:44:28

Static courses

Prevent Phishing Attacks: 5 Tips (Version 2.1)

This static course contains 5 basic tips on how to prevent phishing attacks. Duration: 5 Minutes | Skill Level Low | Audience: All | Interactive: No

27.08.2018 16:14:11

Exams

Internet Security Exam 1.2

In this short quiz, the user is asked nine multiple choice questions in order to test their knowledge regarding internet security (email security, privacy, password security, etc.). Duration: 10-15 Minutes | Skill Level: Low | Audience: All | Interactive: Yes

27.08.2018 16:12:54

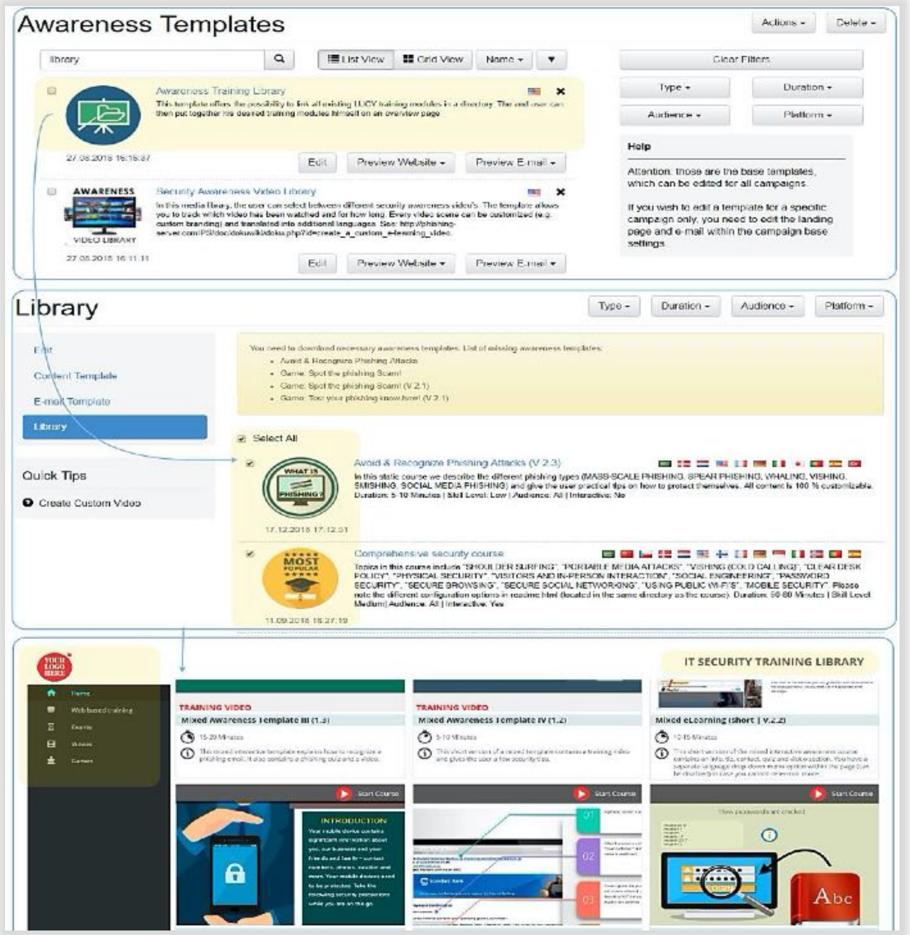
Security News

News: Do you know how to handle security incidents

This course covers security incidents and the processes involved in reporting such incidents.

28.12.2018 14:48:47

- **Training Library**: Your employees can access your organization's training content from an overview page called "training library." It contains a large selection of LUCY's regular e-learning templates, which serve as input. The overview page can be sorted by certain topics (video, quiz, test, etc.).



Awareness Templates

□ Awareness Training Library

This template offers the possibility to link all existing LUCY training modules in a directory. The end user can then put together his desired training modules himself on an overview page

27.08.2018 16:16:37

□ AWARENESS VIDEO LIBRARY — Security Awareness Video Library

In this media library, the user can select between different security awareness video's. The template allows you to track which video has been watched and for how long. Every video scene can be customized (e.g. custom branding) and translated into additional languages. See: http://phishing-server.com/PS/doc/dokuwiki/doku.php?id=create_a_custom_e-learning_video

27.08.2018 16:11:11

Help

Attention: those are the base templates, which can be edited for all campaigns.

If you wish to edit a template for a specific campaign only, you need to edit the landing page and e-mail within the campaign base settings.

Library

You need to download necessary awareness templates. List of missing awareness templates:

- Avoid & Recognize Phishing Attacks
- Game: Spot the phishing Scam!
- Game: Spot the phishing Scam! (V 2.1)
- Game: Test your phishing know-how! (V 2.1)

☑ Select All

☑ Avoid & Recognize Phishing Attacks (V 2.3)

In this static course we describe the different phishing types (MASS-SCALE PHISHING, SPEAR PHISHING, WHALING, VISHING, SMISHING, SOCIAL MEDIA PHISHING) and give the user practical tips on how to protect themselves. All content is 100 % customizable. Duration: 5-10 Minutes | Skill Level: Low | Audience: All | Interactive: No

17.12.2018 17:12:51

☑ Comprehensive security course

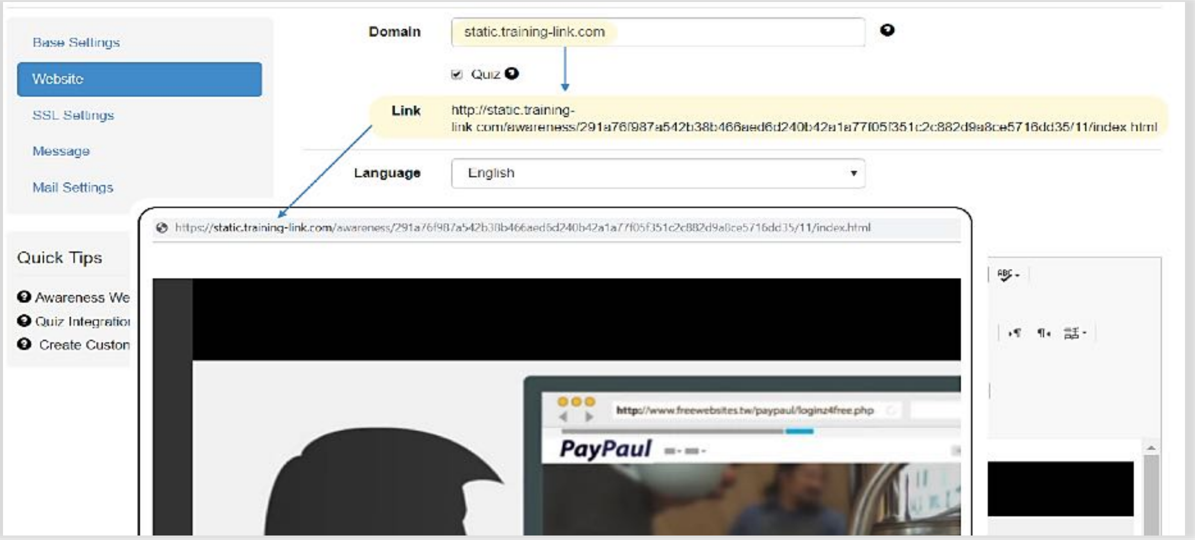
Topics in this course include "SHOULDER SURFING", "PORTABLE MEDIA ATTACKS", "VISHING (COLD CALLING)", "CLEAR DESK POLICY", "PHYSICAL SECURITY", "VISITORS AND IN-PERSON INTERACTION", "SOCIAL ENGINEERING", "PASSWORD SECURITY", "SECURE BROWSING", "SECURE SOCIAL NETWORKING", "USING PUBLIC WI-FI'S", "MOBILE SECURITY". Please note the different configuration options in readme.html (located in the same directory as the course). Duration: 50-80 Minutes | Skill Level Medium | Audience: All | Interactive: Yes

11.09.2018 18:27:19

This mixed interactive template explains how to recognize a phishing email. It also contains a phishing quiz and a video.

This short version of a mixed template contains a training video and gives the user a few security tips.

- **Static Training Support**: Training content can also be published on static pages within LUCY or the intranet, giving the user permanent access to training content, independent of possible attack simulations.



Domain static.training-link.com

☑ Quiz

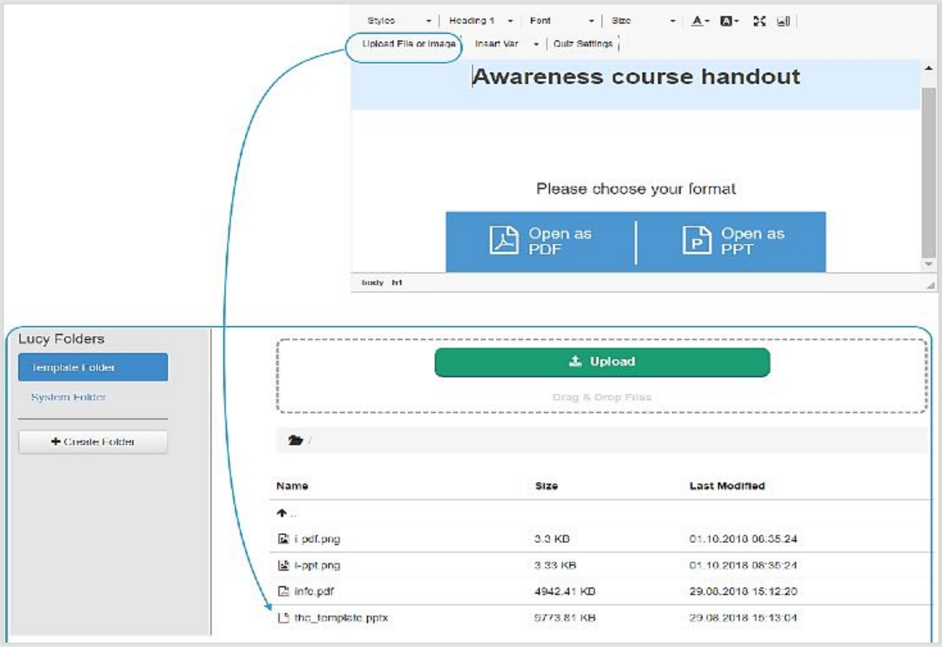
Link http://static.training-link.com/awareness/291a76f987a542b38b466aed6d240b42a1a77f05f351c2c882d9a8ce5716dd35/11/index.html

Language English ▾

https://static.training-link.com/awareness/291a76f987a542b38b466aed5d240b42a1a77f05f351c2c882d9a8ce5716dd35/11/index.html

http://www.freewebsites.tw/paypaul/login4free.php

- **Offline Training Support:** LUCY is supplied with a series of editable templates (Adobe Photoshop or Illustrator files) for awareness training, such as posters, screensavers, fliers, etc.

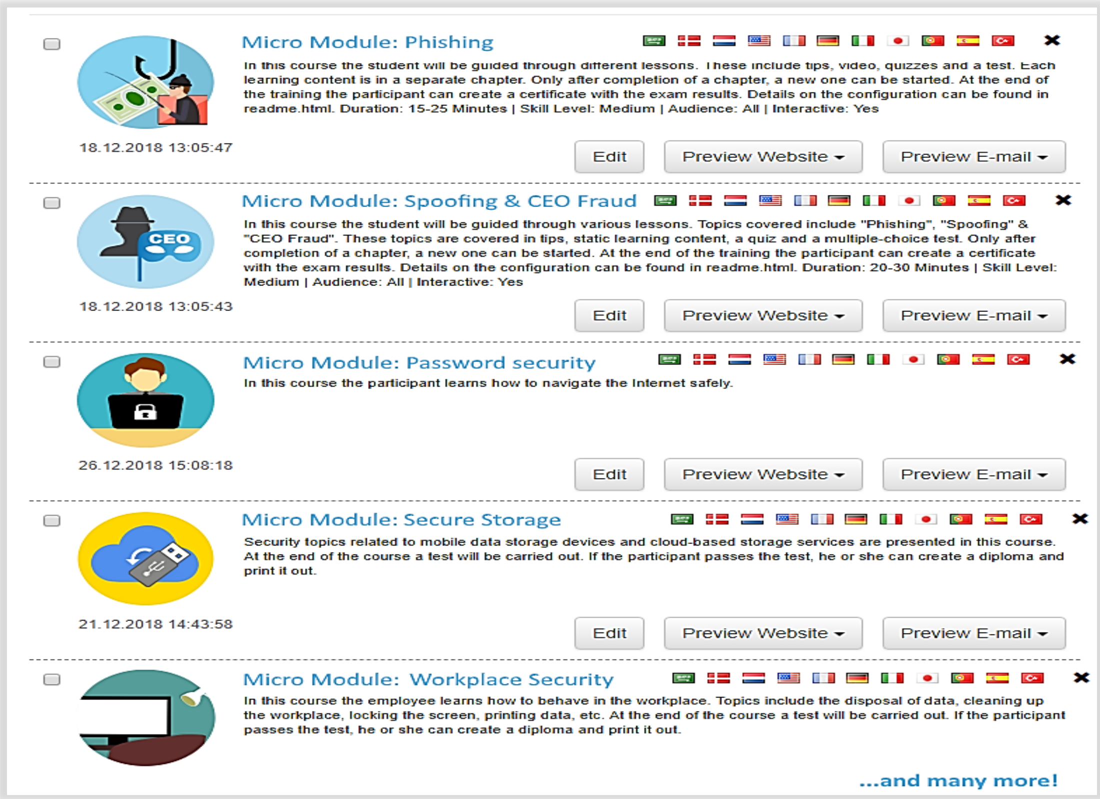


Awareness course handout

Please choose your format

Name	Size	Last Modified
..		
i pdf.png	3.3 KB	01.10.2018 08:35:24
i-ppt.png	3.33 KB	01.10.2018 08:35:24
info.pdf	4942.41 KB	29.08.2018 15:12:20
the_template.pptx	5773.81 KB	29.08.2018 15:13:04

- **Microlearning Modules:** We have designed microlearning training modules (e.g., 1-minute videos or awareness 1-pagers) that can be tailored to the branding and policy needs of your organization.



Micro Module: Phishing

In this course the student will be guided through different lessons. These include tips, video, quizzes and a test. Each learning content is in a separate chapter. Only after completion of a chapter, a new one can be started. At the end of the training the participant can create a certificate with the exam results. Details on the configuration can be found in readme.html. Duration: 15-25 Minutes | Skill Level: Medium | Audience: All | Interactive: Yes

18.12.2018 13:05:47

Micro Module: Spoofing & CEO Fraud

In this course the student will be guided through various lessons. Topics covered include "Phishing", "Spoofing" & "CEO Fraud". These topics are covered in tips, static learning content, a quiz and a multiple-choice test. Only after completion of a chapter, a new one can be started. At the end of the training the participant can create a certificate with the exam results. Details on the configuration can be found in readme.html. Duration: 20-30 Minutes | Skill Level: Medium | Audience: All | Interactive: Yes

18.12.2018 13:05:43

Micro Module: Password security

In this course the participant learns how to navigate the Internet safely.

26.12.2018 15:08:18

Micro Module: Secure Storage

Security topics related to mobile data storage devices and cloud-based storage services are presented in this course. At the end of the course a test will be carried out. If the participant passes the test, he or she can create a diploma and print it out.

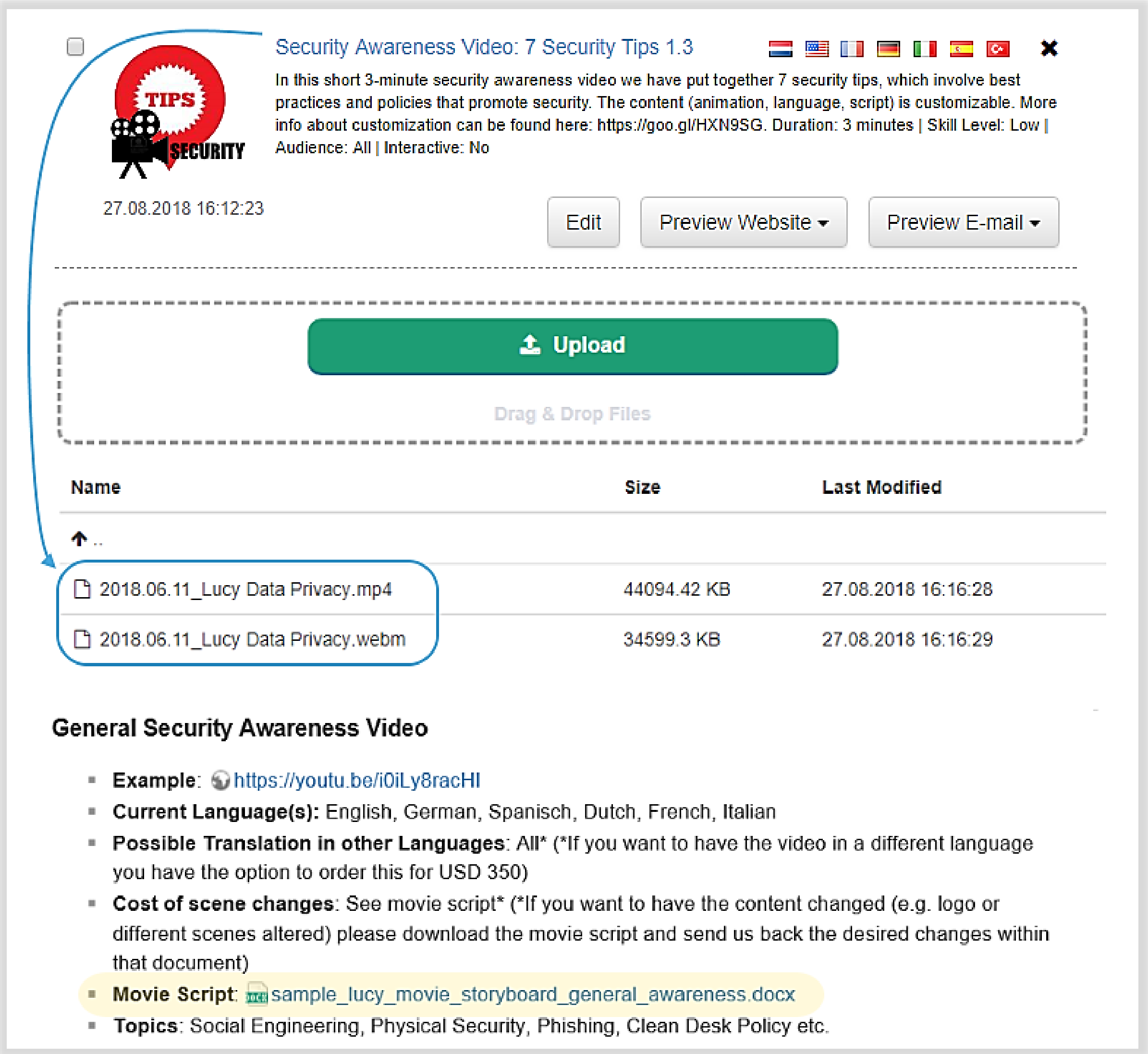
21.12.2018 14:43:58

Micro Module: Workplace Security

In this course the employee learns how to behave in the workplace. Topics include the disposal of data, cleaning up the workplace, locking the screen, printing data, etc. At the end of the course a test will be carried out. If the participant passes the test, he or she can create a diploma and print it out.

...and many more!

- **Video Customization:** Send us your company logo and we will include it in the training videos. You want another language? No problem. We will set the video to play in the language you prefer. You want a different scene? Simply download the video scripts and mark the desired changes.



☐ Security Awareness Video: 7 Security Tips 1.3

In this short 3-minute security awareness video we have put together 7 security tips, which involve best practices and policies that promote security. The content (animation, language, script) is customizable. More info about customization can be found here: https://goo.gl/HXN9SG. Duration: 3 minutes | Skill Level: Low | Audience: All | Interactive: No

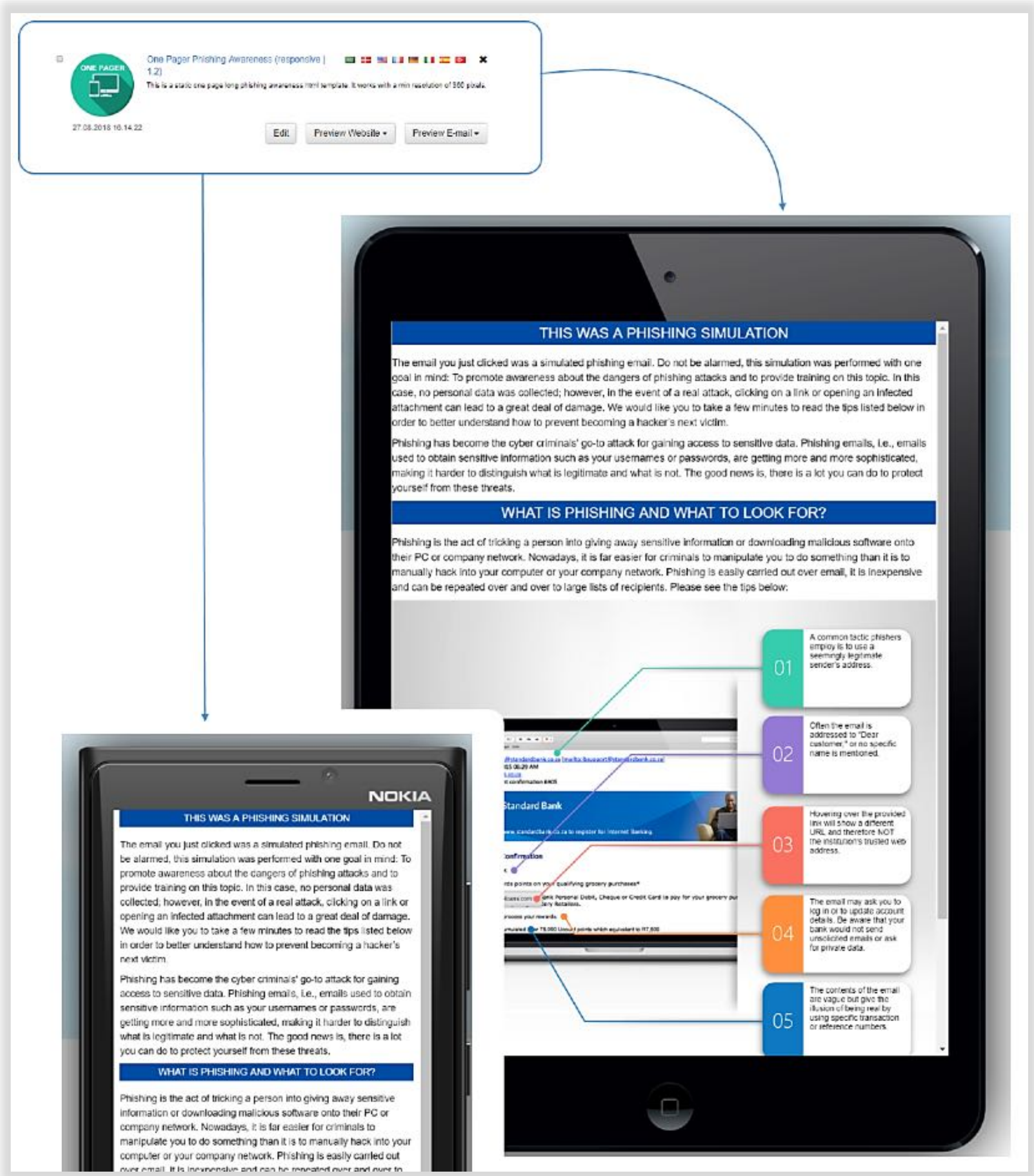
27.08.2018 16:12:23

Name	Size	Last Modified
..		
2018.06.11_Lucy Data Privacy.mp4	44094.42 KB	27.08.2018 16:16:28
2018.06.11_Lucy Data Privacy.webm	34599.3 KB	27.08.2018 16:16:29

General Security Awareness Video

- **Example**: https://youtu.be/i0iLy8racHI
- **Current Language(s):** English, German, Spanisch, Dutch, French, Italian
- **Possible Translation in other Languages**: All* (*If you want to have the video in a different language you have the option to order this for USD 350)
- **Cost of scene changes**: See movie script* (*If you want to have the content changed (e.g. logo or different scenes altered) please download the movie script and send us back the desired changes within that document)
- **Movie Script**: sample_lucy_movie_storyboard_general_awareness.docx
- **Topics**: Social Engineering, Physical Security, Phishing, Clean Desk Policy etc.

- **Mobile-Responsive Format:** Many of LUCY’s built-in modules are available in a mobile-responsive format that gives your users the flexibility to take the training on any type of connected device.



This is a static one page long phishing awareness html template. It works with a min resolution of 360 pixels.

THIS WAS A PHISHING SIMULATION

The email you just clicked was a simulated phishing email. Do not be alarmed, this simulation was performed with one goal in mind: To promote awareness about the dangers of phishing attacks and to provide training on this topic. In this case, no personal data was collected; however, in the event of a real attack, clicking on a link or opening an infected attachment can lead to a great deal of damage. We would like you to take a few minutes to read the tips listed below in order to better understand how to prevent becoming a hacker's next victim.

Phishing has become the cyber criminals' go-to attack for gaining access to sensitive data. Phishing emails, i.e., emails used to obtain sensitive information such as your usernames or passwords, are getting more and more sophisticated, making it harder to distinguish what is legitimate and what is not. The good news is, there is a lot you can do to protect yourself from these threats.

WHAT IS PHISHING AND WHAT TO LOOK FOR?

Phishing is the act of tricking a person into giving away sensitive information or downloading malicious software onto their PC or company network. Nowadays, it is far easier for criminals to manipulate you to do something than it is to manually hack into your computer or your company network. Phishing is easily carried out over email, it is inexpensive and can be repeated over and over to large lists of recipients. Please see the tips below:

01 A common tactic phishers employ is to use a seemingly legitimate sender's address.

02 Often the email is addressed to "Dear customer," or no specific name is mentioned.

03 Hovering over the provided link will show a different URL and therefore NOT the institution's trusted web address.

04 The email may ask you to log in or to update account details. Be aware that your bank would not send unsolicited emails or ask for private data.

05 The contents of the email are vague but give the illusion of being real by using specific transaction or reference numbers.

THIS WAS A PHISHING SIMULATION

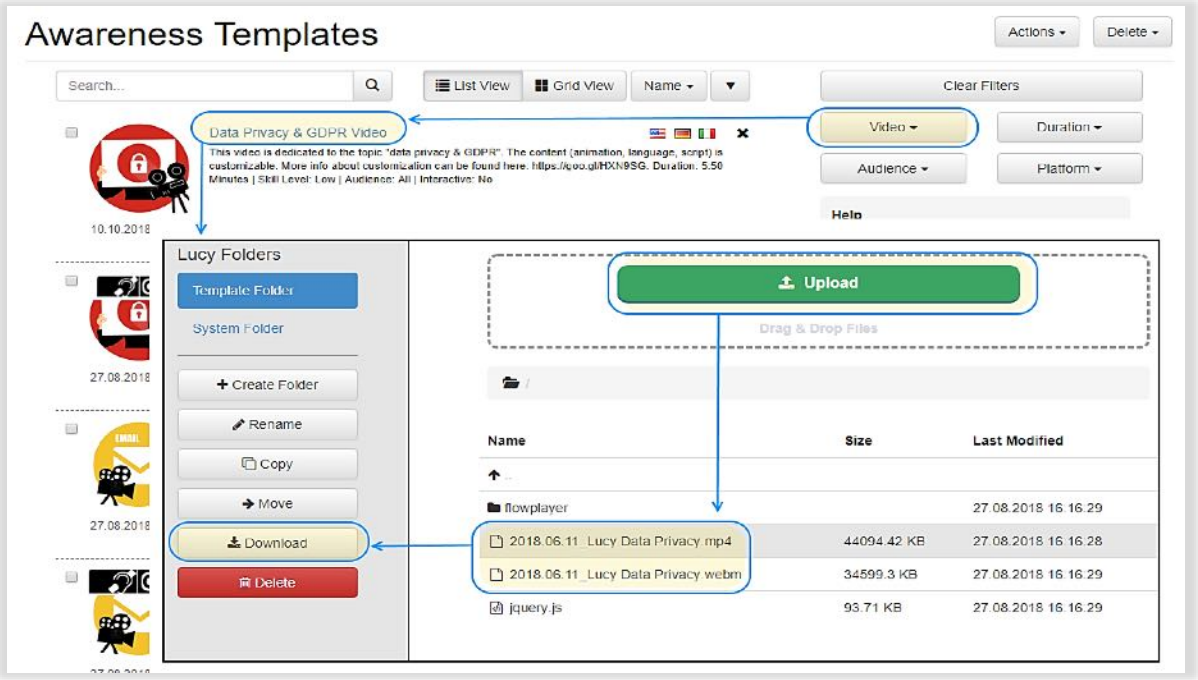
The email you just clicked was a simulated phishing email. Do not be alarmed, this simulation was performed with one goal in mind: To promote awareness about the dangers of phishing attacks and to provide training on this topic. In this case, no personal data was collected; however, in the event of a real attack, clicking on a link or opening an infected attachment can lead to a great deal of damage. We would like you to take a few minutes to read the tips listed below in order to better understand how to prevent becoming a hacker's next victim.

Phishing has become the cyber criminals' go-to attack for gaining access to sensitive data. Phishing emails, i.e., emails used to obtain sensitive information such as your usernames or passwords, are getting more and more sophisticated, making it harder to distinguish what is legitimate and what is not. The good news is, there is a lot you can do to protect yourself from these threats.

WHAT IS PHISHING AND WHAT TO LOOK FOR?

Phishing is the act of tricking a person into giving away sensitive information or downloading malicious software onto their PC or company network. Nowadays, it is far easier for criminals to manipulate you to do something than it is to manually hack into your computer or your company network. Phishing is easily carried out over email. It is inexpensive and can be repeated over and over to

- **Video Import/Export:** You can export LUCY videos to your own system as well as import your own videos into LUCY.



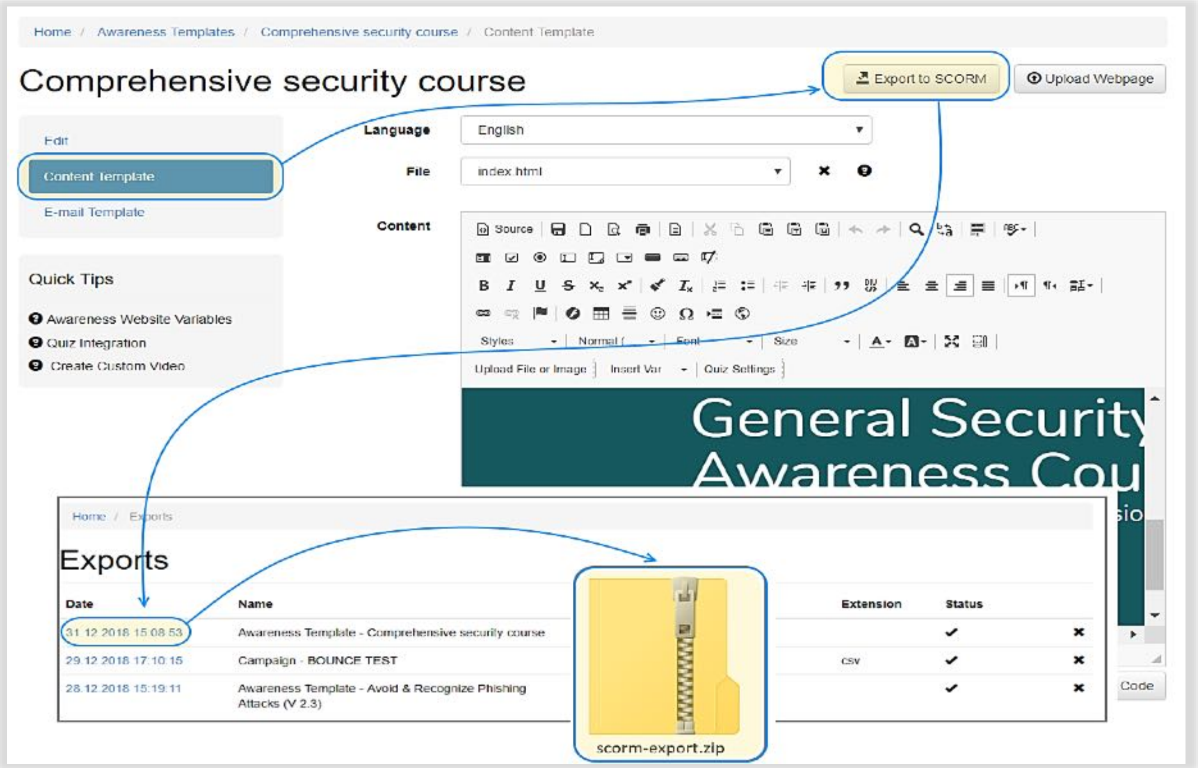
Awareness Templates

Data Privacy & GDPR Video

This video is dedicated to the topic "data privacy & GDPR". The content (animation, language, script) is customizable. More info about customization can be found here. https://goo.gl/HXN9SG. Duration: 5.50 Minutes | Skill Level: Low | Audience: All | Interactive: No

Name	Size	Last Modified
↑ ..		
flowplayer		27.08.2018 16:16:29
2018.06.11_Lucy Data Privacy.mp4	44094.42 KB	27.08.2018 16:16:28
2018.06.11_Lucy Data Privacy.webm	34599.3 KB	27.08.2018 16:16:29
jquery.js	93.71 KB	27.08.2018 16:16:29

- **Dynamic Training Hints:** The implemented dynamic hints allow your administrator to set markers within the attack templates that could indicate to your employees, inside the e-learning material, where the phishing attack may have been detected.



Home / Awareness Templates / Comprehensive security course / Content Template

Comprehensive security course

Language: English

File: index.html

General Security Awareness Cou

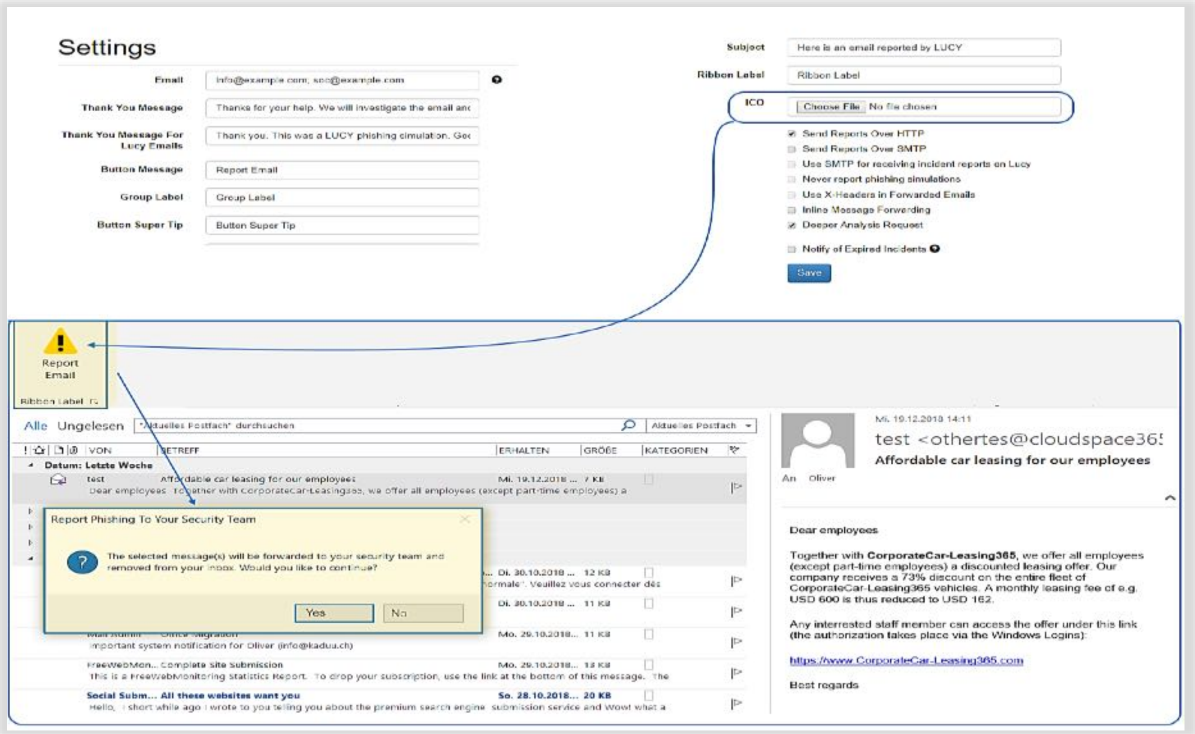
Home / Exports

Exports

Date	Name	Extension	Status	
31.12.2018 15:08:53	Awareness Template - Comprehensive security course		✓	✖
29.12.2018 17:10:15	Campaign - BOUNCE TEST	csv	✓	✖
28.12.2018 15:19:11	Awareness Template - Avoid & Recognize Phishing Attacks (V 2.3)		✓	✖

ENGAGE EMPLOYEES

- **Report E-mails with a single click:** End users can report suspicious e-mails with a single click to one or multiple e-mail accounts and have them forwarded to your LUCY incident analysis console. Your employees, inside the e-learning material, where the phishing attack may have been detected.



Settings

Email: info@example.com; soc@example.com

Thank You Message: Thanks for your help. We will investigate the email and

Thank You Message For Lucy Emails: Thank you. This was a LUCY phishing simulation. Go

Button Message: Report Email

Group Label: Group Label

Button Super Tip: Button Super Tip

Subject: Here is an email reported by LUCY

Ribbon Label: Ribbon Label

ICO: Choose File No file chosen

☑ Send Reports Over HTTP
☐ Send Reports Over SMTP
☐ Use SMTP for receiving incident reports on Lucy
☐ Never report phishing simulations
☐ Use X-Headers in Forwarded Emails
☐ Inline Message Forwarding
☑ Deeper Analysis Request

☐ Notify of Expired Incidents

test — Affordable car leasing for our employees — Mi. 19.12.2018 ... 7 KB
Dear employees Together with CorporateCar-Leasing365, we offer all employees (except part-time employees) a

... Di. 30.10.2018 ... 12 KB
...normale". Veuillez vous connecter dès

Di. 30.10.2018 ... 11 KB

Mail Admin — Office Migration — Mo. 29.10.2018... 11 KB
Important system notification for Oliver (info@kaduu.ch)

FreeWebMon... Complete Site Submission — Mo. 29.10.2018... 13 KB
This is a FreeWebMonitoring Statistics Report. To drop your subscription, use the link at the bottom of this message. The

Social Subm... All these websites want you — So. 28.10.2018... 20 KB
Hello, I short while ago I wrote to you telling you about the premium search engine submission service and Wow! what a

Report Phishing To Your Security Team

The selected message(s) will be forwarded to your security team and removed from your inbox. Would you like to continue?

Mi. 19.12.2018 14:11

test <othertes@cloudspace365

Affordable car leasing for our employees

An Oliver

Dear employees

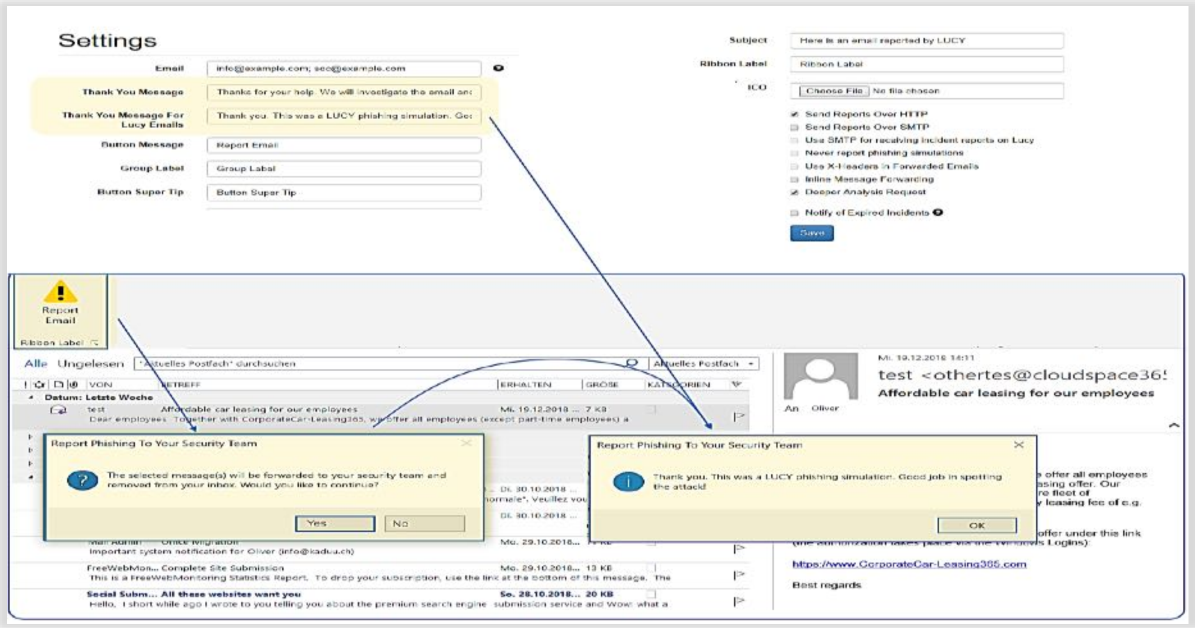
Together with **CorporateCar-Leasing365**, we offer all employees (except part-time employees) a discounted leasing offer. Our company receives a 73% discount on the entire fleet of CorporateCar-Leasing365 vehicles. A monthly leasing fee of e.g. USD 600 is thus reduced to USD 162.

Any interrested staff member can access the offer under this link (the authorization takes place via the Windows Logins):

https://www.CorporateCar-Leasing365.com

Best regards

- **Positive Behavior Reinforcement:** Our plugin automatically provides positive behaviour reinforcement by showing gratitude to end users via a custom message defined by your organization.



Settings

Email: info@example.com; soc@example.com

Thank You Message: Thanks for your help. We will investigate the email and

Thank You Message For Lucy Emails: Thank you. This was a LUCY phishing simulation. Go

Button Message: Report Email

Group Label: Group Label

Button Super Tip: Button Super Tip

Subject: Here is an email reported by LUCY

Ribbon Label: Ribbon Label

ICO: Choose File No file chosen

☑ Send Reports Over HTTP
☐ Send Reports Over SMTP
☐ Use SMTP for receiving incident reports on Lucy
☐ Never report phishing simulations
☐ Use X-Headers in Forwarded Emails
☐ Inline Message Forwarding
☑ Deeper Analysis Request

☐ Notify of Expired Incidents

test — Affordable car leasing for our employees — Mi. 19.12.2018 ... 7 KB
Dear employees Together with CorporateCar-Leasing365, we offer all employees (except part-time employees) a

Mail Admin — Office Migration — Mo. 29.10.2018...
Important system notification for Oliver (info@kaduu.ch)

FreeWebMon... Complete Site Submission — Mo. 29.10.2018... 13 KB
This is a FreeWebMonitoring Statistics Report. To drop your subscription, use the link at the bottom of this message. The

Social Subm... All these websites want you — So. 28.10.2018... 20 KB
Hello, I short while ago I wrote to you telling you about the premium search engine submission service and Wow! what a

Report Phishing To Your Security Team

The selected message(s) will be forwarded to your security team and removed from your inbox. Would you like to continue?

Report Phishing To Your Security Team

Thank you. This was a LUCY phishing simulation. Good job in spotting the attack!

Mi. 19.12.2018 14:11

test <othertes@cloudspace365

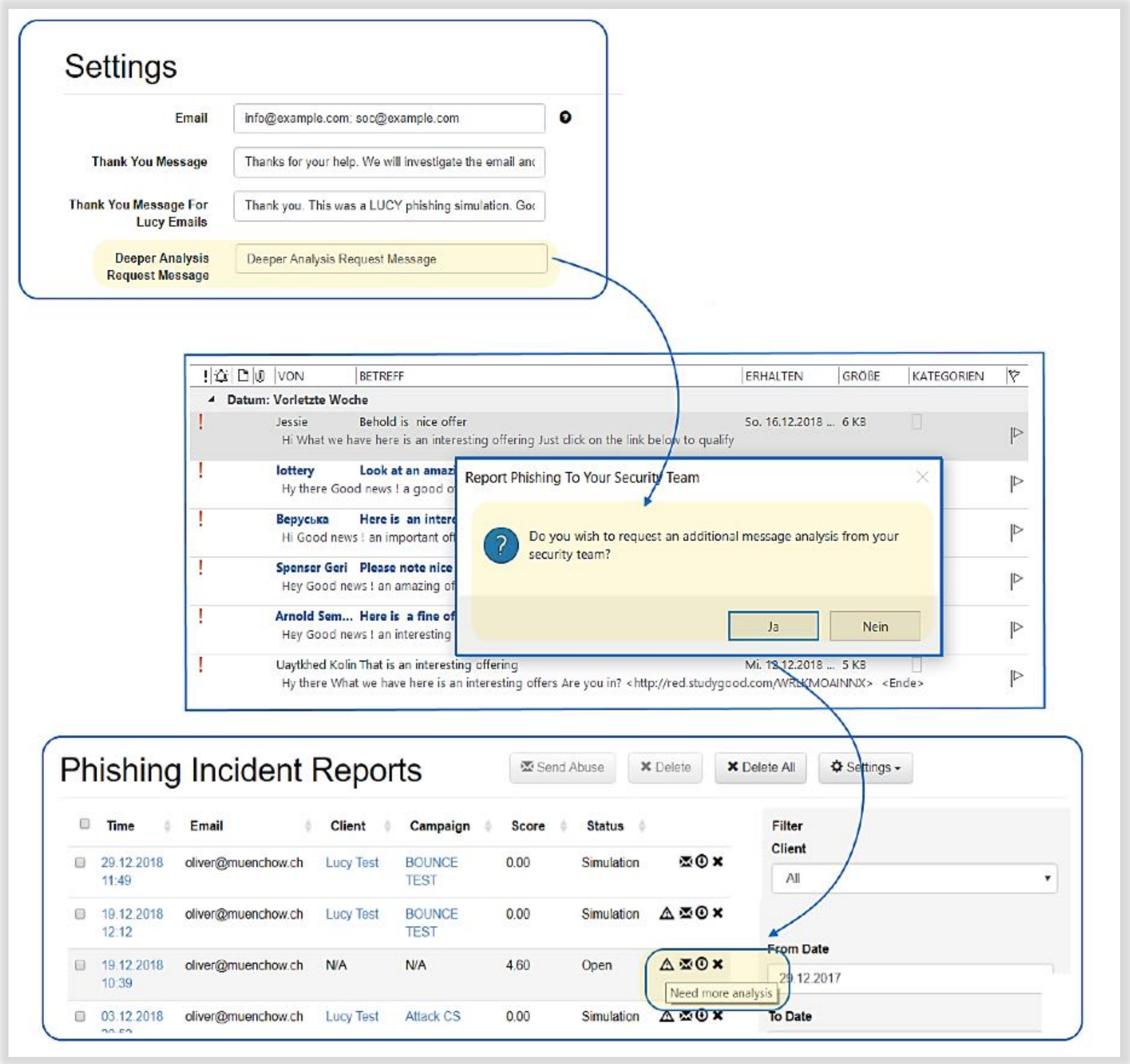
Affordable car leasing for our employees

An Oliver

https://www.CorporateCar-Leasing365.com

Best regards

- **Deep inspection request:** Sometimes users want to know if the received e-mail can be opened safely. The user can optionally use the “deep inspection request” within the local plugin to tell the security team that he wants feedback on the reported e-mail.



Settings

Email	info@example.com; soc@example.com
Thank You Message	Thanks for your help. We will investigate the email anc
Thank You Message For Lucy Emails	Thank you. This was a LUCY phishing simulation. Goc
Deeper Analysis Request Message	Deeper Analysis Request Message

!	VON	BETREFF	ERHALTEN	GRÖßE	KATEGORIEN
	Datum: Vorletzte Woche				
!	Jessie	Behold is nice offer Hi What we have here is an interesting offering Just click on the link below to qualify	So. 16.12.2018 ...	6 KB	
!	lottery	Look at an amazi Hy there Good news ! a good o			
!	Верусьна	Here is an intere Hi Good news ! an important of			
!	Spenser Geri	Please note nice Hey Good news ! an amazing of			
!	Arnold Sem...	Here is a fine of Hey Good news ! an interesting			
!	Uaytkhed Kolin	That is an interesting offering Hy there What we have here is an interesting offers Are you in? <http://red.studygood.com/WRLKMOAINNX> <Ende>	Mi. 12.12.2018 ...	5 KB	

Report Phishing To Your Security Team

Do you wish to request an additional message analysis from your security team?

Phishing Incident Reports

□	Time	Email	Client	Campaign	Score	Status
□	29.12.2018 11:49	oliver@muenchow.ch	Lucy Test	BOUNCE TEST	0.00	Simulation
□	19.12.2018 12:12	oliver@muenchow.ch	Lucy Test	BOUNCE TEST	0.00	Simulation
□	19.12.2018 10:39	oliver@muenchow.ch	N/A	N/A	4.60	Open
□	03.12.2018	oliver@muenchow.ch	Lucy Test	Attack CS	0.00	Simulation

Need more analysis

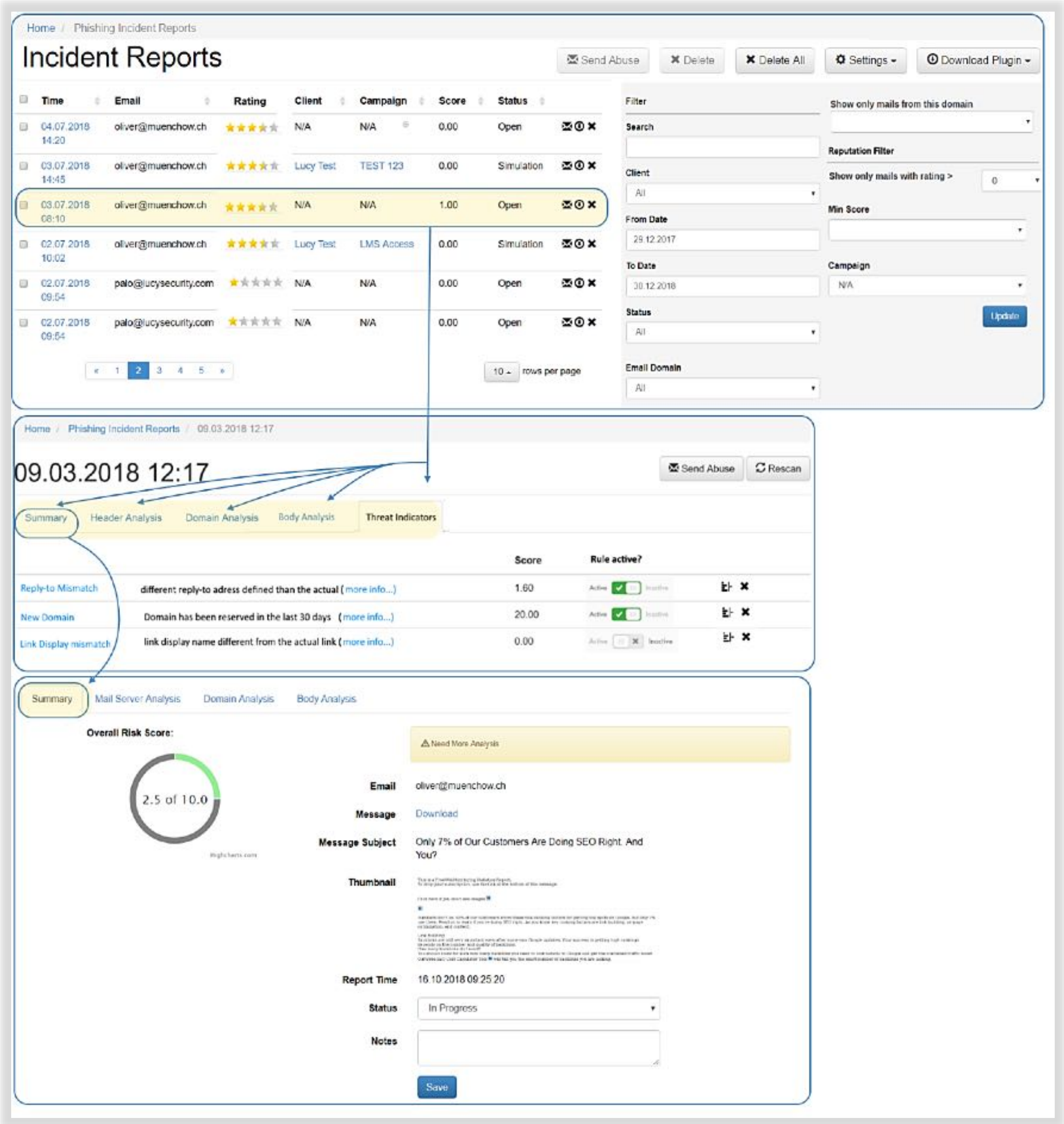
Filter

Client: All

From Date: 29.12.2017

To Date

- **Automatic Incident Analysis:** Manage and respond to reported suspicious e-mails using a centralized management console: LUCY analyzer allows an automated inspection of reported messages (header & body). The analyzer includes an individual risk score, providing a real-time ranking of reported e-mails. The Threat Analyzer brings a noticeable relief for the safety team's work load.



Home / Phishing Incident Reports

Incident Reports

□	Time	Email	Rating	Client	Campaign	Score	Status
□	04.07.2018 14:20	oliver@muenchow.ch	★★★★☆	N/A	N/A	0.00	Open
□	03.07.2018 14:45	oliver@muenchow.ch	★★★★☆	Lucy Test	TEST 123	0.00	Simulation
□	03.07.2018 08:10	oliver@muenchow.ch	★★★★☆	N/A	N/A	1.00	Open
□	02.07.2018 10:02	oliver@muenchow.ch	★★★★☆	Lucy Test	LMS Access	0.00	Simulation
□	02.07.2018 09:54	palo@lucysecurity.com	★☆☆☆☆	N/A	N/A	0.00	Open
□	02.07.2018 09:54	palo@lucysecurity.com	★☆☆☆☆	N/A	N/A	0.00	Open

10 rows per page

Filter

Search:

Client: All

From Date: 29.12.2017

To Date: 30.12.2018

Status: All

Email Domain: All

Show only mails from this domain

Reputation Filter

Show only mails with rating > 0

Min Score

Campaign: N/A

Home / Phishing Incident Reports / 09.03.2018 12:17

09.03.2018 12:17

		Score	Rule active?
Reply-to Mismatch	different reply-to adress defined than the actual (more info...)	1.60	Active
New Domain	Domain has been reserved in the last 30 days (more info...)	20.00	Active
Link Display mismatch	link display name different from the actual link (more info...)	0.00	Inactive

Overall Risk Score:

2.5 of 10.0

⚠ Need More Analysis

Email: oliver@muenchow.ch

Message: Download

Message Subject: Only 7% of Our Customers Are Doing SEO Right. And You?

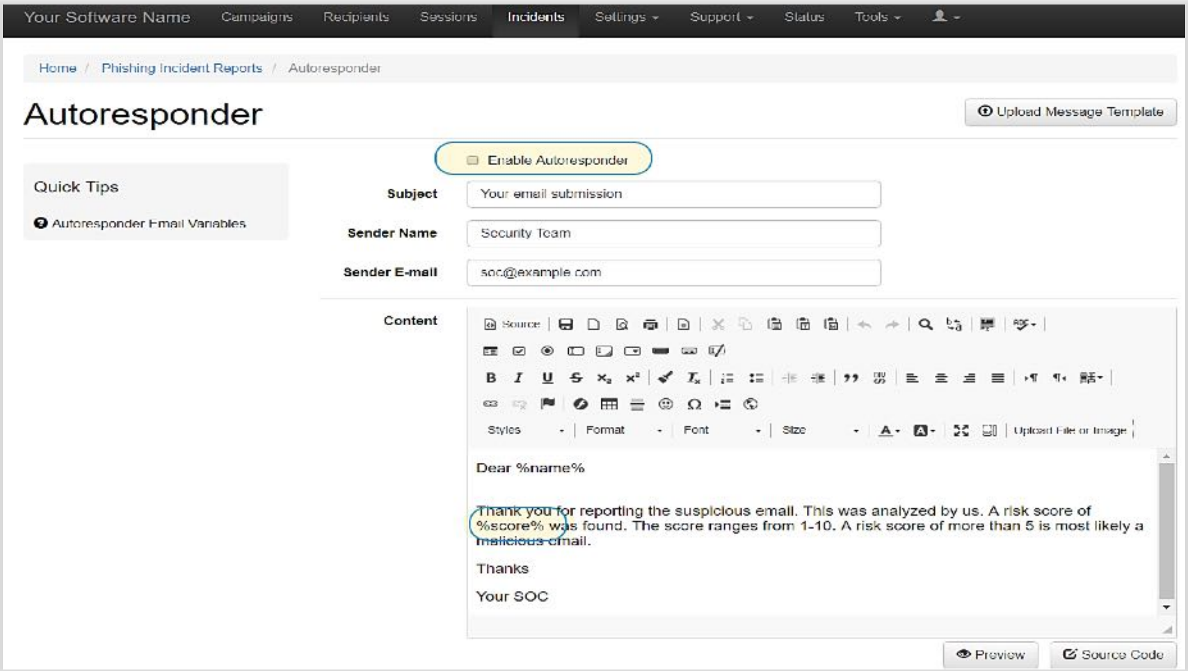
Thumbnail

Report Time: 16.10.2018 09:25:20

Status: In Progress

Notes:

- **Incident Auto Feedback:** The Incident Autoresponder allows sending an automated notification to the end user providing the results of the e-mail threat analysis. The message text is freely configurable, and the LUCY E-mail Risk Score can also be included, if required.



Autoresponder

□ Enable Autoresponder

Subject: Your email submission

Sender Name: Security Team

Sender E-mail: soc@example.com

Content:

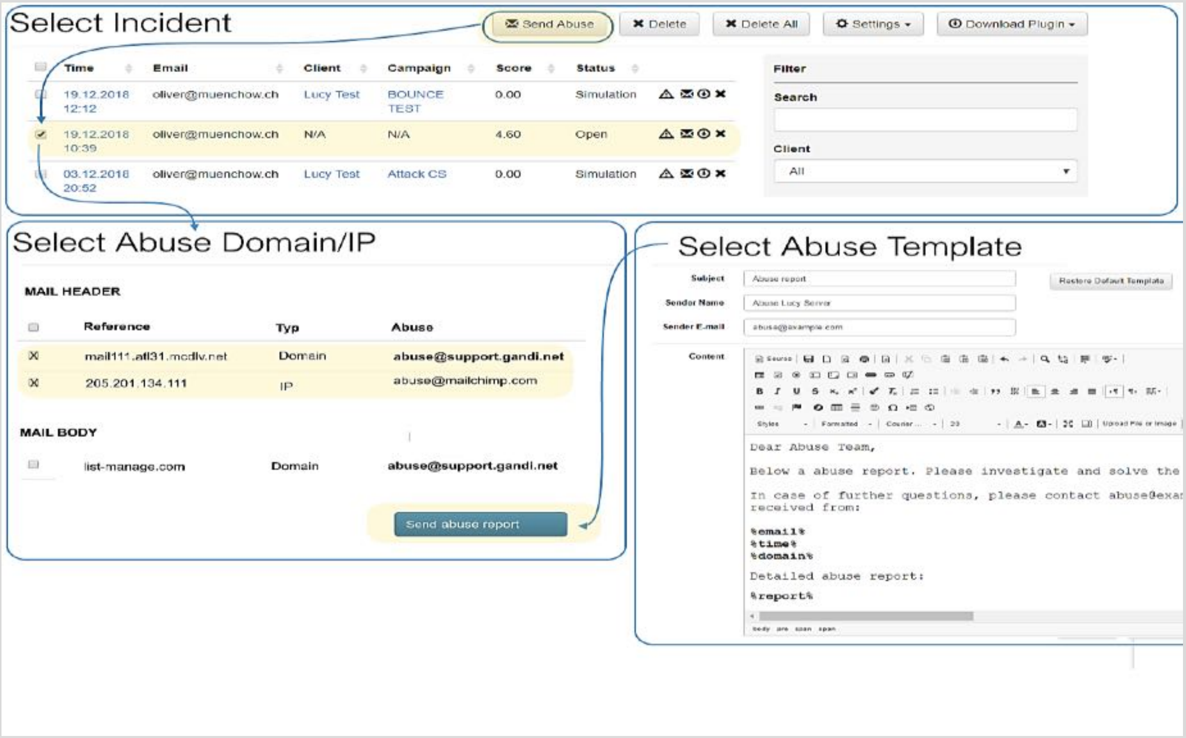
Dear %name%

Thank you for reporting the suspicious email. This was analyzed by us. A risk score of %score% was found. The score ranges from 1-10. A risk score of more than 5 is most likely a malicious email.

Thanks

Your SOC

- **Threat Mitigation:** The behavioural threat mitigator is a revolutionary approach to eliminating e-mail risks. It will support the security admin in shutting down the attack (e.g., sending an automated report to specified abuse team of providers involved in the attack).



Select Incident

□	Time	Email	Client	Campaign	Score	Status
□	19.12.2018 12:12	oliver@muenchow.ch	Lucy Test	BOUNCE TEST	0.00	Simulation
☑	19.12.2018 10:39	oliver@muenchow.ch	N/A	N/A	4.60	Open
□	03.12.2018 20:52	oliver@muenchow.ch	Lucy Test	Attack CS	0.00	Simulation

Client: All

Select Abuse Domain/IP

MAIL HEADER

□	Reference	Typ	Abuse
☒	mail111.atl31.mcdlv.net	Domain	abuse@support.gandi.net
☒	205.201.134.111	IP	abuse@mailchimp.com

MAIL BODY

□	Reference	Typ	Abuse
□	list-manage.com	Domain	abuse@support.gandi.net

Select Abuse Template

Subject: Abuse report

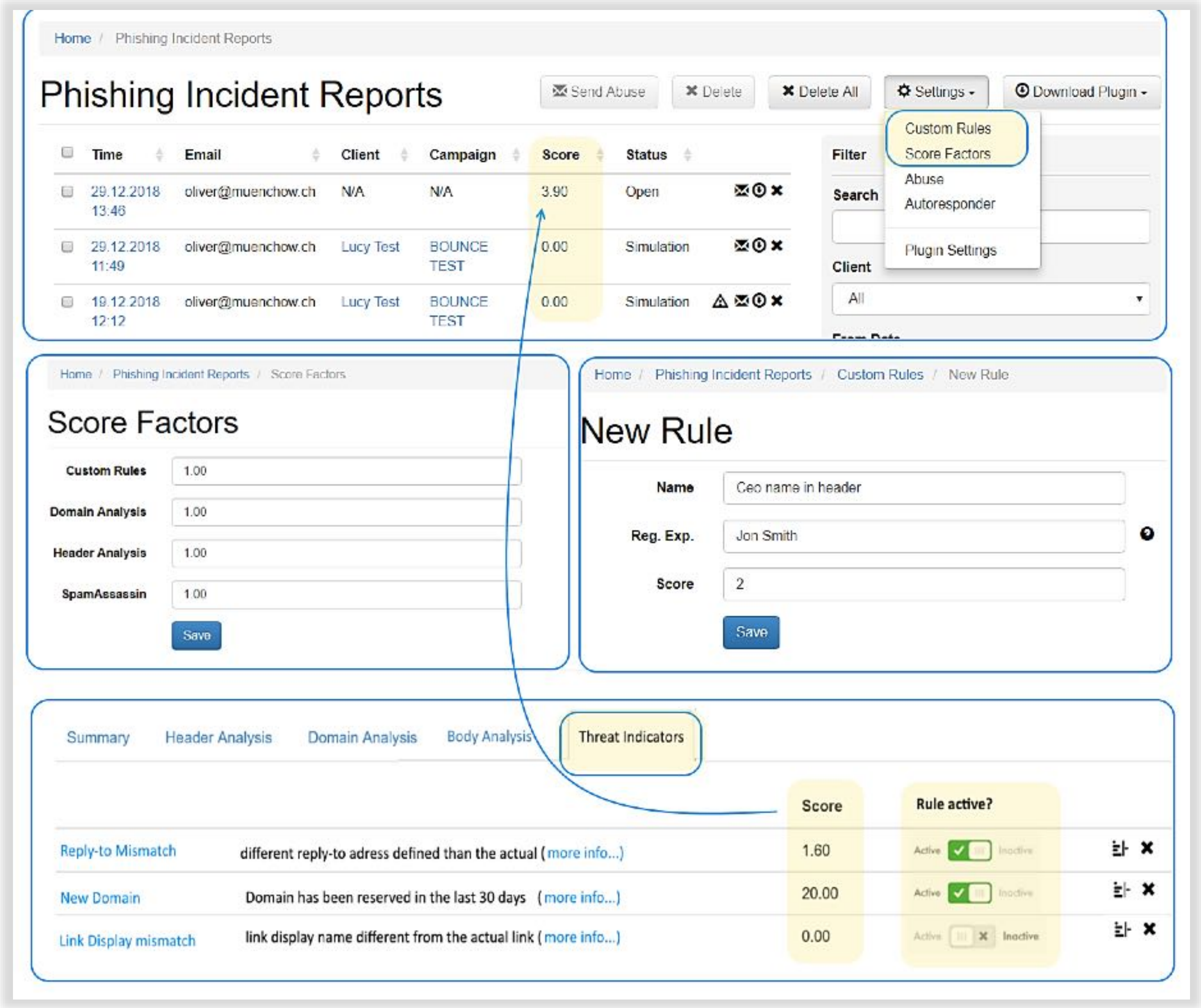
Sender Name: Abuse Lucy Server

Sender E-mail: abuse@example.com

Content:

```
Dear Abuse Team,

Below a abuse report. Please investigate and solve the

In case of further questions, please contact abuse@exa
received from:

%email%
%time%
%domain%

Detailed abuse report:

%report%
```

- **Custom rule-based analysis:** Define your own rules for e-mail analysis and risk calculations.



Phishing Incident Reports

□	Time	Email	Client	Campaign	Score	Status
□	29.12.2018 13:46	oliver@muenchow.ch	N/A	N/A	3.90	Open
□	29.12.2018 11:49	oliver@muenchow.ch	Lucy Test	BOUNCE TEST	0.00	Simulation
□	19.12.2018 12:12	oliver@muenchow.ch	Lucy Test	BOUNCE TEST	0.00	Simulation

Filter

Search:

Client: All

Score Factors

Custom Rules: 1.00

Domain Analysis: 1.00

Header Analysis: 1.00

SpamAssassin: 1.00

New Rule

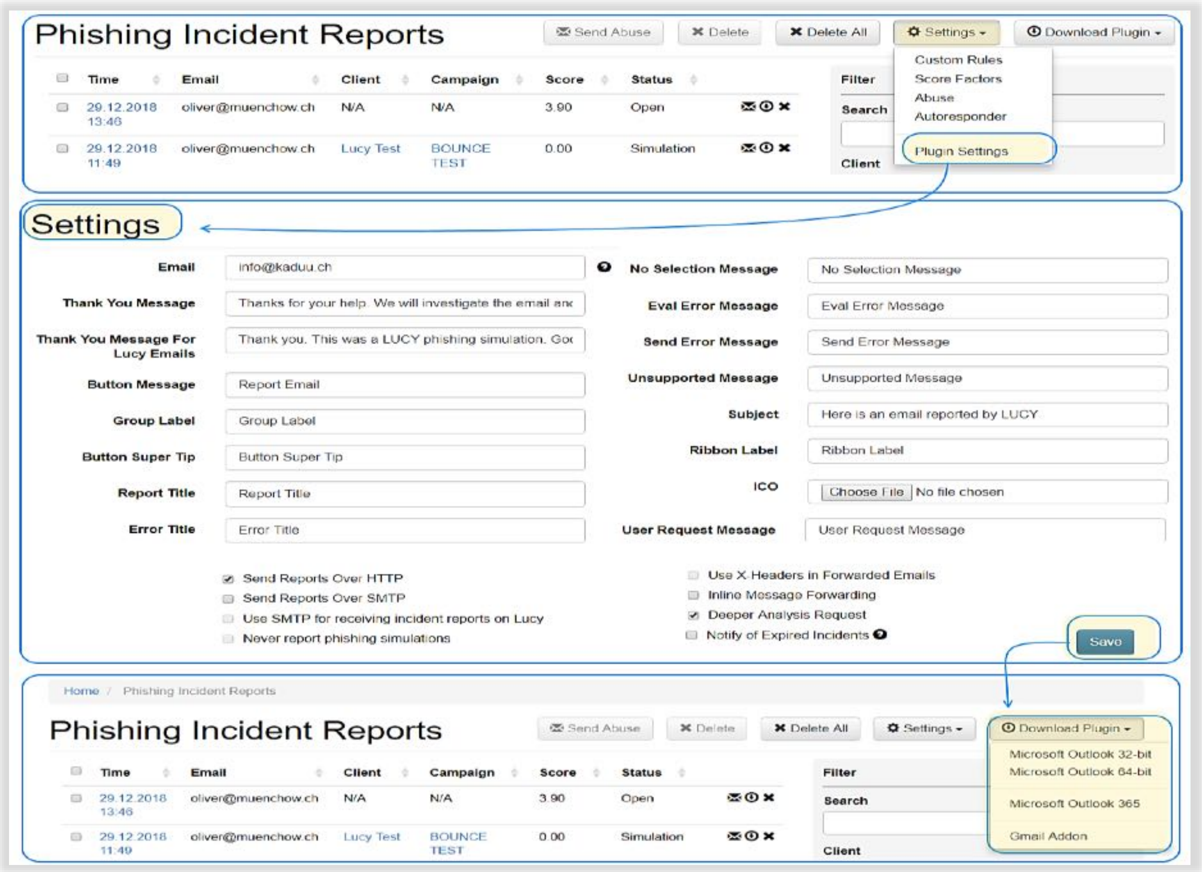
Name: Ceo name in header

Reg. Exp.: Jon Smith

Score: 2

		Score	Rule active?
Reply-to Mismatch	different reply-to adress defined than the actual (more info...)	1.60	Active ✓
New Domain	Domain has been reserved in the last 30 days (more info...)	20.00	Active ✓
Link Display mismatch	link display name different from the actual link (more info...)	0.00	✗ Inactive

- **Plugin customization options:** LUCY allows an easy customization and a complete white labelling of various plugin functions (displayed icon, feedback messages, ribbon label, transmission protocol, sent header, etc.).



Phishing Incident Reports

□	Time	Email	Client	Campaign	Score	Status	
□	29.12.2018 13:46	oliver@muenchow.ch	N/A	N/A	3.90	Open	✉ ⓘ ✖
□	29.12.2018 11:49	oliver@muenchow.ch	Lucy Test	BOUNCE TEST	0.00	Simulation	✉ ⓘ ✖

Settings

Email	info@kaduu.ch	No Selection Message	No Selection Message
Thank You Message	Thanks for your help. We will investigate the email and	Eval Error Message	Eval Error Message
Thank You Message For Lucy Emails	Thank you. This was a LUCY phishing simulation. Goc	Send Error Message	Send Error Message
Button Message	Report Email	Unsupported Message	Unsupported Message
Group Label	Group Label	Subject	Here is an email reported by LUCY
Button Super Tip	Button Super Tip	Ribbon Label	Ribbon Label
Report Title	Report Title	ICO	Choose File No file chosen
Error Title	Error Title	User Request Message	User Request Message

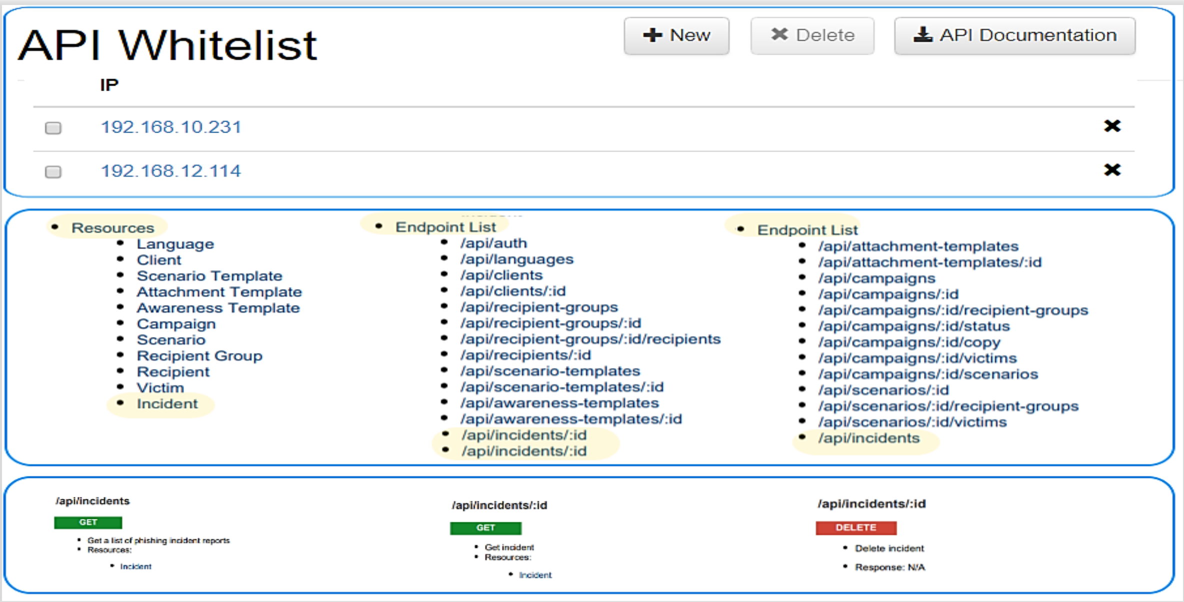
☑ Send Reports Over HTTP
□ Send Reports Over SMTP
□ Use SMTP for receiving incident reports on Lucy
□ Never report phishing simulations

□ Use X-Headers in Forwarded Emails
□ Inline Message Forwarding
☑ Deeper Analysis Request
□ Notify of Expired Incidents

Phishing Incident Reports

□	Time	Email	Client	Campaign	Score	Status	
□	29.12.2018 13:46	oliver@muenchow.ch	N/A	N/A	3.90	Open	✉ ⓘ ✖
□	29.12.2018 11:49	oliver@muenchow.ch	Lucy Test	BOUNCE TEST	0.00	Simulation	✉ ⓘ ✖

- **Third party integration:** Using LUCY's incident REST API automation, we can process reported e-mails and help your security team stop active phishing attacks while in progress.



API Whitelist

□	IP	
□	192.168.10.231	✖
□	192.168.12.114	✖

- Resources
  - Language
  - Client
  - Scenario Template
  - Attachment Template
  - Awareness Template
  - Campaign
  - Scenario
  - Recipient Group
  - Recipient
  - Victim
  - Incident

- Endpoint List
  - /api/auth
  - /api/languages
  - /api/clients
  - /api/clients/:id
  - /api/recipient-groups
  - /api/recipient-groups/:id
  - /api/recipient-groups/:id/recipients
  - /api/recipients/:id
  - /api/scenario-templates
  - /api/scenario-templates/:id
  - /api/awareness-templates
  - /api/awareness-templates/:id
  - /api/incidents/:id
  - /api/incidents/:id

- Endpoint List
  - /api/attachment-templates
  - /api/attachment-templates/:id
  - /api/campaigns
  - /api/campaigns/:id
  - /api/campaigns/:id/recipient-groups
  - /api/campaigns/:id/status
  - /api/campaigns/:id/copy
  - /api/campaigns/:id/victims
  - /api/campaigns/:id/scenarios
  - /api/scenarios/:id
  - /api/scenarios/:id/recipient-groups
  - /api/scenarios/:id/victims
  - /api/incidents

/api/incidents

GET

- Get a list of phishing incident reports
- Resources:
  - Incident

/api/incidents/:id

GET

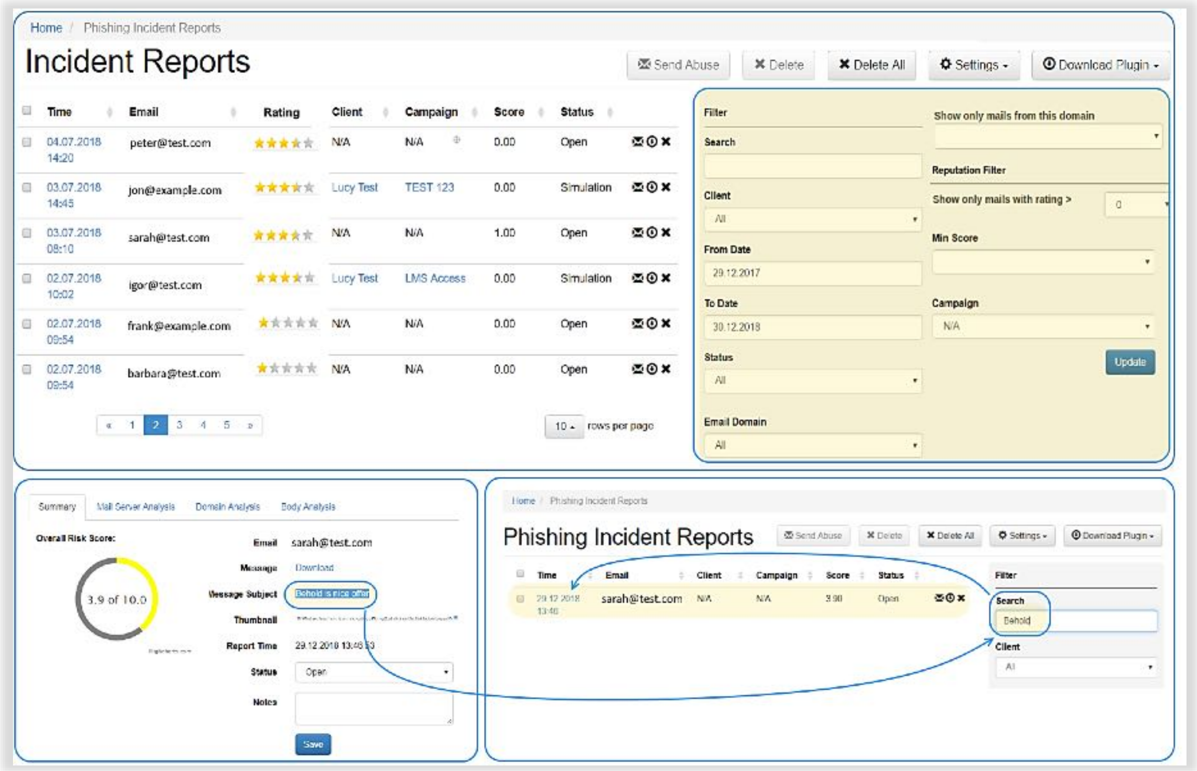
- Get incident
- Resources:
  - Incident

/api/incidents/:id

DELETE

- Delete incident
- Response: N/A

- **Identify attacks with common patterns:** Apply LUCY’s dashboard filters to detect common attack vectors across your organization. Search within all reported e-mails for similar indicators of compromise.



Home / Phishing Incident Reports

Incident Reports

□	Time	Email	Rating	Client	Campaign	Score	Status	
□	04.07.2018 14:20	peter@test.com	★★★★☆	N/A	N/A	0.00	Open	✉ ⊙ ✖
□	03.07.2018 14:45	jon@example.com	★★★★☆	Lucy Test	TEST 123	0.00	Simulation	✉ ⊙ ✖
□	03.07.2018 08:10	sarah@test.com	★★★★☆	N/A	N/A	1.00	Open	✉ ⊙ ✖
□	02.07.2018 10:02	igor@test.com	★★★★☆	Lucy Test	LMS Access	0.00	Simulation	✉ ⊙ ✖
□	02.07.2018 09:54	frank@example.com	★☆☆☆☆	N/A	N/A	0.00	Open	✉ ⊙ ✖
□	02.07.2018 09:54	barbara@test.com	★☆☆☆☆	N/A	N/A	0.00	Open	✉ ⊙ ✖

« 1 2 3 4 5 » 10 rows per page

Filter
Search:
Client: All
From Date: 29.12.2017
To Date: 30.12.2018
Status: All
Email Domain: All
Show only mails from this domain:
Reputation Filter
Show only mails with rating > 0
Min Score:
Campaign: N/A
Update

Summary | Mail Server Analysis | Domain Analysis | Body Analysis

Overall Risk Score: 3.9 of 10.0

Email: sarah@test.com
Message: Download
Message Subject: Behold is nice offer
Thumbnail
Report Time: 29.12.2018 13:46:53
Status: Open
Notes:
Save

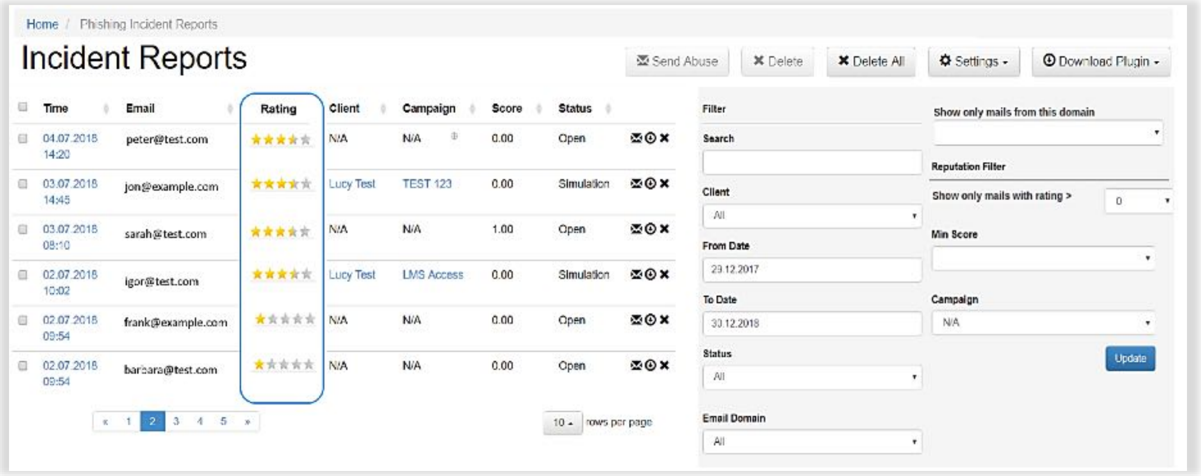
Home / Phishing Incident Reports

Phishing Incident Reports

□	Time	Email	Client	Campaign	Score	Status	
□	29.12.2018 13:46	sarah@test.com	N/A	N/A	3.90	Open	✉ ⊙ ✖

Filter
Search: Behold
Client: All

- **Incident user reputation profiles:** Classify users with an incident reputation score.



Home / Phishing Incident Reports

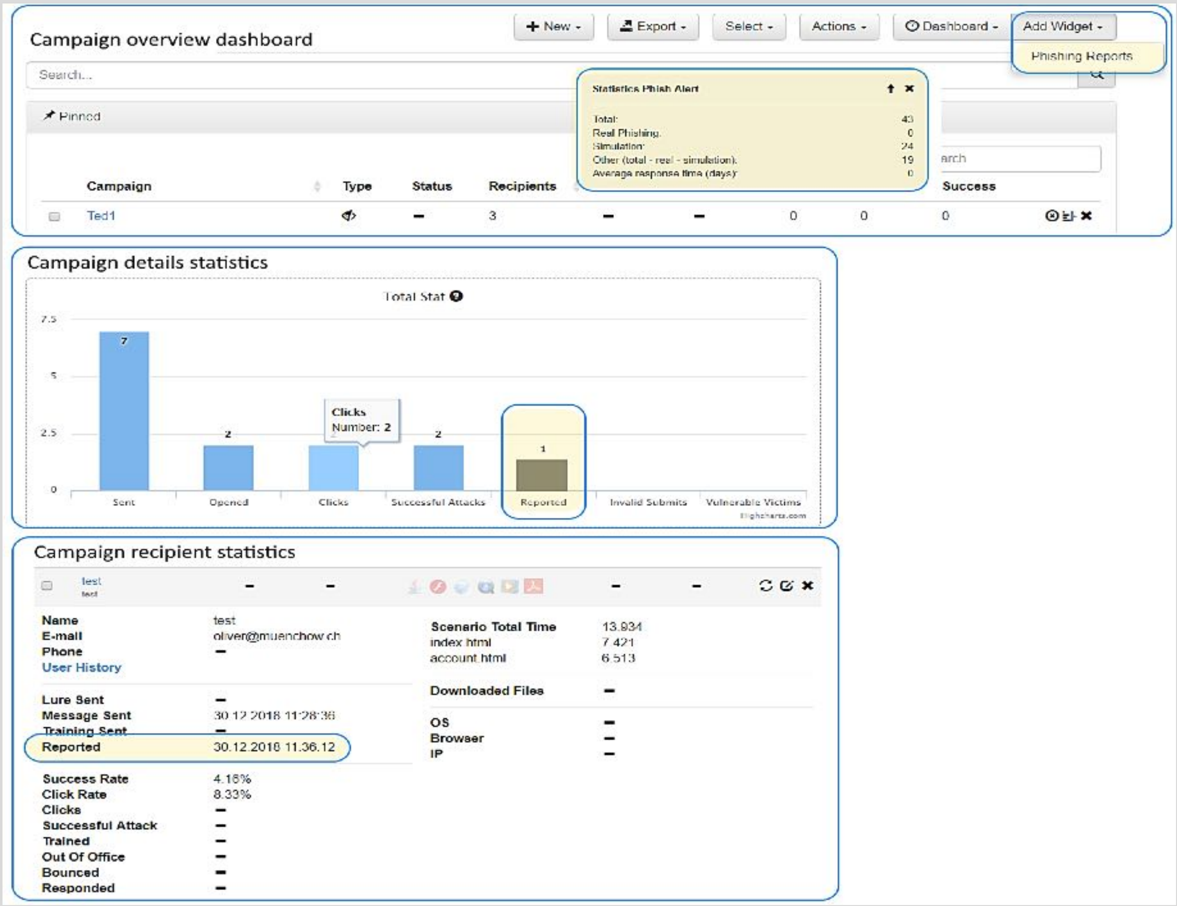
Incident Reports

□	Time	Email	Rating	Client	Campaign	Score	Status	
□	04.07.2018 14:20	peter@test.com	★★★★☆	N/A	N/A	0.00	Open	✉ ⊙ ✖
□	03.07.2018 14:45	jon@example.com	★★★★☆	Lucy Test	TEST 123	0.00	Simulation	✉ ⊙ ✖
□	03.07.2018 08:10	sarah@test.com	★★★★☆	N/A	N/A	1.00	Open	✉ ⊙ ✖
□	02.07.2018 10:02	igor@test.com	★★★★☆	Lucy Test	LMS Access	0.00	Simulation	✉ ⊙ ✖
□	02.07.2018 09:54	frank@example.com	★☆☆☆☆	N/A	N/A	0.00	Open	✉ ⊙ ✖
□	02.07.2018 09:54	barbara@test.com	★☆☆☆☆	N/A	N/A	0.00	Open	✉ ⊙ ✖

« 1 2 3 4 5 » 10 rows per page

Filter
Search:
Client: All
From Date: 29.12.2017
To Date: 30.12.2018
Status: All
Email Domain: All
Show only mails from this domain:
Reputation Filter
Show only mails with rating > 0
Min Score:
Campaign: N/A
Update

- **Integration with attack simulations:** Seamless report and dashboard integration with phishing simulations: identify the users who have behaved exemplarily in a phishing simulation.



Campaign overview dashboard

Statistics Phish Alert

Total:	43
Real Phishing:	0
Simulation:	24
Other (total - real - simulation):	19
Average response time (days):	0

	Campaign	Type	Status	Recipients					Success	
□	Ted1		–	3	–	–	0	0	0	

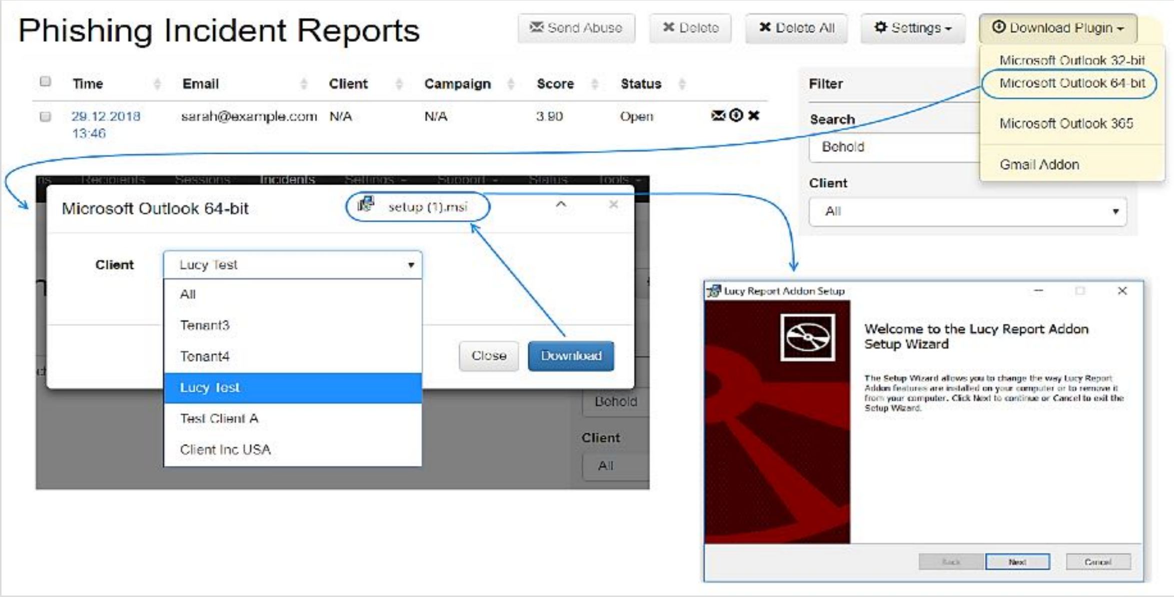
Campaign details statistics

Campaign recipient statistics

□	test test	–	–	–	–

Name	test	Scenario Total Time	13.934
E-mail	oliver@muenchow.ch	index.html	7.421
Phone	–	account.html	6.513
User History			
Lure Sent	–	Downloaded Files	–
Message Sent	30.12.2018 11:28:36	OS	–
Training Sent	–	Browser	–
Reported	30.12.2018 11.36.12	IP	–
Success Rate	4.16%		
Click Rate	8.33%		
Clicks	–		
Successful Attack	–		
Trained	–		
Out Of Office	–		
Bounced	–		
Responded	–		

- **Easy Installation:** Install the Phishing Incident Plugin for Outlook, Gmail, Office365.



Phishing Incident Reports

□	Time	Email	Client	Campaign	Score	Status	
□	29.12.2018 13:46	sarah@example.com	N/A	N/A	3.90	Open	

Filter

Search: Behold

Client: All

Microsoft Outlook 64-bit

Client: Lucy Test

Lucy Report Addon Setup

Welcome to the Lucy Report Addon Setup Wizard

The Setup Wizard allows you to change the way Lucy Report Addon features are installed on your computer or to remove it from your computer. Click Next to continue or Cancel to exit the Setup Wizard.