



LUCY WHITEPAPER



CHE COS'È LUCY?

Metti alla prova, forma e coinvolgi i tuoi impiegati

LUCY permette alle società di prendere il ruolo di un aggressore e rivelare le debolezze esistenti in infrastruttura tecnica e competenze del personale, eliminandole attraverso un programma di e-learning completo.



TEST IMPIEGATI

Simulazione di attacchi (ad esempio phishing)



TEST INFRASTRUTTURE

Simulazione e scansione malware



FORMAZIONE IMPIEGATI

LMS integrato



MISURAZIONE RISULTATI

Progressi su rischi e apprendimento



INTEGRAZIONE PER IMPIEGATI

Sistema di segnalazione (ad esempio, pulsante per mail phishing)





LUCY WHITEPAPER



SOMMARIO

FUNZIONI GENERALI

- Promemoria
- Rilevamento Risposte
- Client di comunicazione e-mail completo
- Scheduler randomizzazione
- Strumenti di prestazione
- Interfaccia amministratore multilingue
- Certificato (SSL)
- Controllo degli accessi basato sui ruoli
- Gruppi di utenti a più livelli
- Compatibilità con più clienti
- Modelli di campagna
- Configurazione guidata basata sui rischi
- Verifica champagne
- Approvazione del flusso di lavoro
- API DNS

SIMULAZIONE DI ATTACCO

- Attacchi con dispositivi multimediali portatili
- SMiShing
- Attacchi di inserimento dati
- Attacchi con collegamenti ipertestuali
- Toolkit di reindirizzamento URL potente
- Attacchi misti
- Attacchi basati su file
- Attacchi doppietta
- Attacchi basati su Java
- Attacchi basati su PDF
- Attacchi di simulazione ransomware
- Toolkit di convalida inserimento dati
- Libreria di modelli di attacco multilingue
- Modelli specifici per settore e divisione
- Utilizzo simultaneo di modelli di attacco
- Variazioni degli URL di attacco
- Accorciamento URL
- Kit pentest
- Duplicatore siti web
- Attacchi basati su livelli
- Simulazione di spear phishing
- Supporto DKIM / S / MIME per email di phishing
- Scansione email
- Creazione homepage personalizzata

TEST INFRASTRUTTURE

- Toolkit test malware
- Test filtri email e web
- Rilevamento vulnerabilità client passiva e attiva
- Test di spoofing

TEST TECNICI

- e-Learning basato sulla reputazione
- Portale di formazione utente finale
- Diploma di formazione sulla sensibilizzazione
- Toolkit di creazione e-learning
- Formazione sulla sensibilizzazione su media interattivi
- Libreria di formazione
- Supporto per formazione statica
- Supporto per formazione offline
- Moduli di microapprendimento
- Personalizzazione video
- Formato adatto per dispositivi mobile
- Importazione / Esportazione video
- Suggerimenti di formazione dinamica

COINVOLGIMENTO IMPIEGATI

- Segnalazione delle email con un solo click
- Rafforzamento del comportamento positive
- Richiesta di ispezione approfondita
- Analisi degli incidenti automatica
- Feedback degli incidenti automatico
- Mitigazione minacce
- Analisi con regole personalizzate
- Opzioni di personalizzazione plugin
- Integrazione di terze parti
- Identificazione attacchi con schemi comuni
- Profili di reputazione degli utenti sugli incidenti
- Integrazione con attacchi simulati
- Installazione facile

FUNZIONI GENERALI

- Ngpt ck nptg 8i** modelli di promemoria possono essere utilizzati per rispedire automaticamente messaggi agli utenti che non hanno cliccato su un link di attacco o su un corso di formazione dopo un periodo di tempo personalizzato.

REMINDER SETTINGS

User Settings

Custom Fields

Reminders

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

Save

REMINDER ATTACK TEMPLATE (SCENARIO 2)

Source | [Icons] | Styles: Normal | Arial | Size: [A-] [A+] | [Icons]

Insert Var - | Upload File or Image

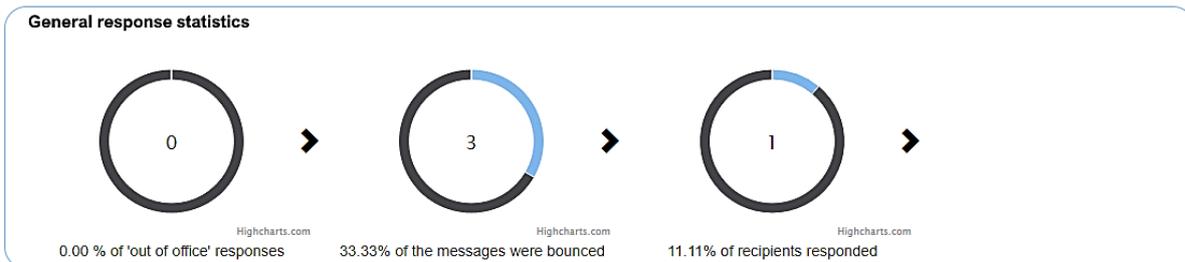
Dear %name%,

You have received an [encrypted 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.

body p span

Preview

- Pgct_k cl mptgnmqrc 8i** rilevamento automatico delle risposte permette di definire e analizzare le risposte automatiche alle email (ad es. fuori ufficio) e gli errori di consegna della posta (ad es. utente sconosciuto) all'interno della campagna.



User specific response statistics

No test

Name	No
E-mail	doesntexist@doesnt-eallyexist.net
Phone	-
User History	
Lure Sent	-
Message Sent	-
Training Sent	-
Reported	-
<hr/>	
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

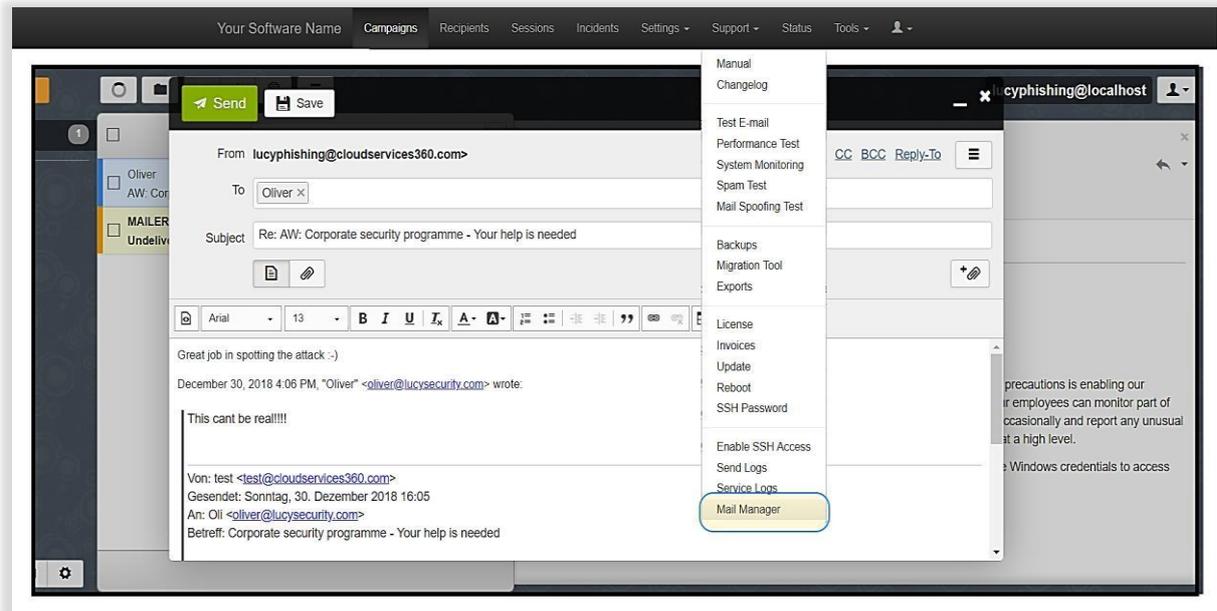
Out Of Office Delay

Out Of Office Pattern

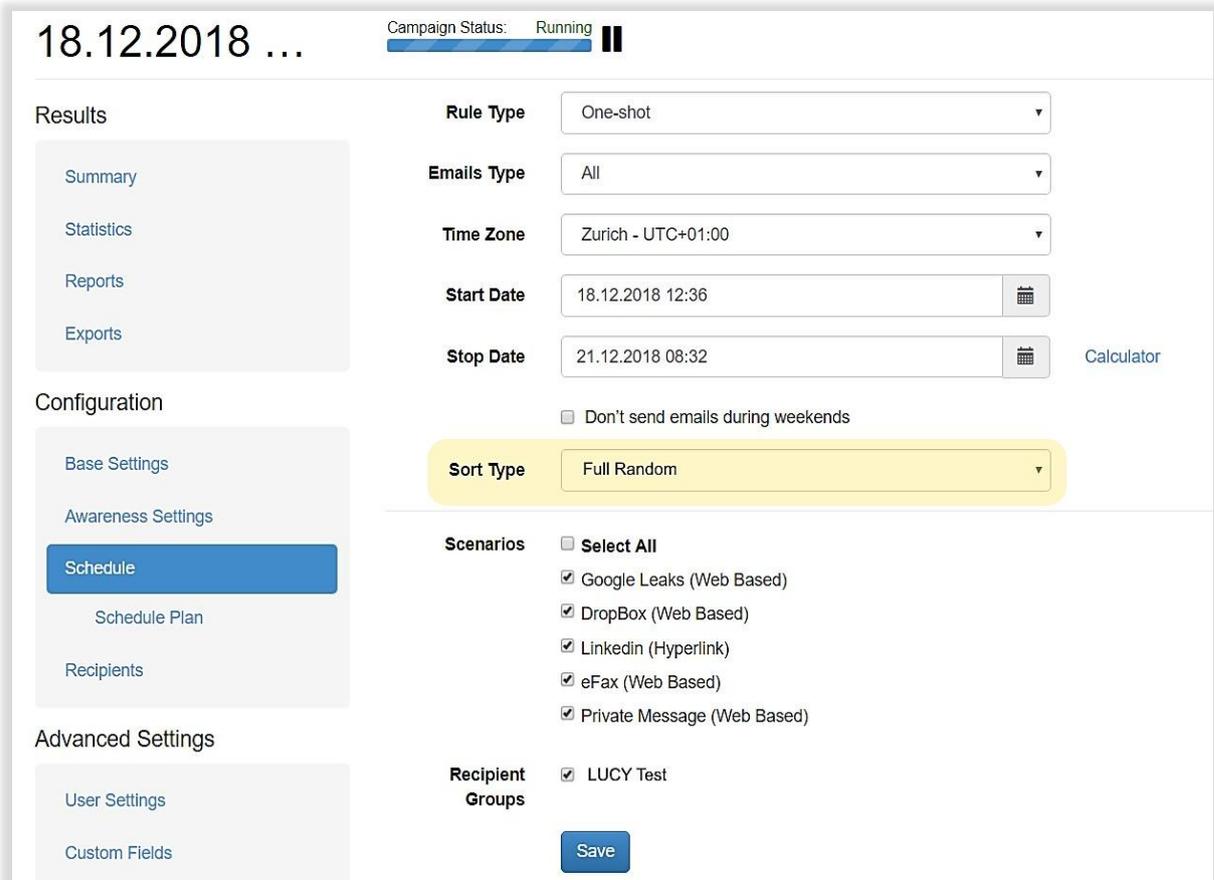
Bounced Pattern

Save

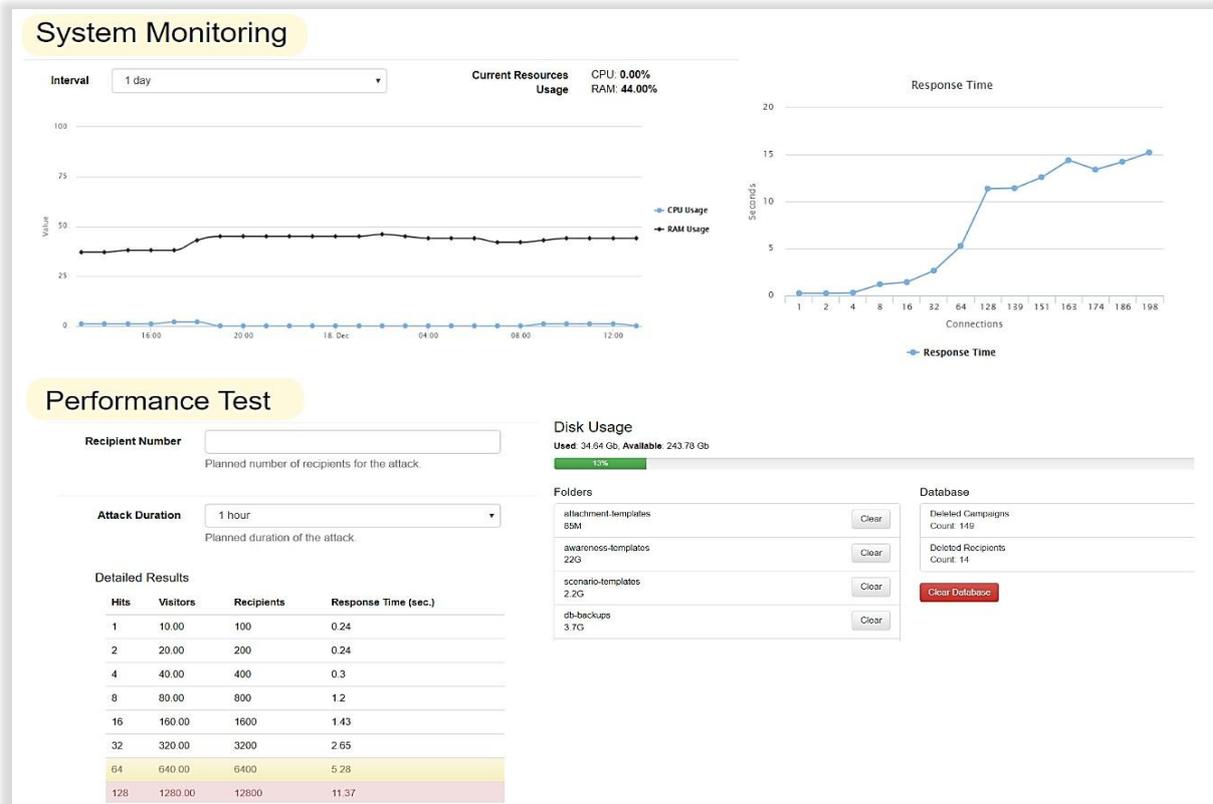
- Ajgl r bgark sl g_xgrl c ck _g ank njcm8** una piattaforma di messaggistica integrata permette all'amministratore LUCY di comunicare in modo interattivo con i destinatari all'interno o all'esterno delle campagne LUCY. Tutte le email vengono archiviate e possono essere esaminate.



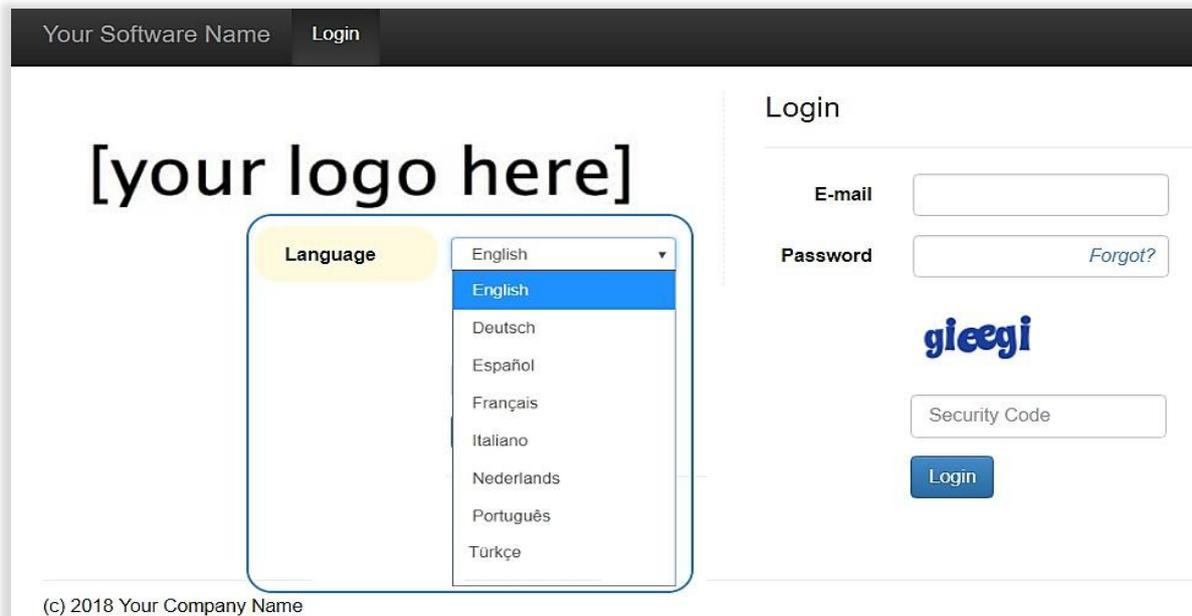
- Schedulatore randomizzazione:** sensibilizzare gli impiegati in modo casuale è un fattore chiave per una sensibilizzazione efficace e sostenibile all'interno della società. Inviare più campagne simultanee in modo casuale è uno dei migliori mezzi per la formazione degli impiegati.



- Strumenti di prestazione:** le routine smart LUCY adattano l'installazione del server alle risorse date. Durante installazioni o operazioni vengono calcolate operazioni server, dimensionamento DBMS, utilizzo memoria e CPU. Puoi dimensionare una singola installazione LUCY su cloud per oltre 400.000 utenti.



- Interfaccia amministratore multilingue:** l'interfaccia amministratore LUCY è disponibile in diverse lingue e può essere tradotta in altre lingue su richiesta.



- Certificato (SSL):** permette la creazione automatica di certificati ufficiali e verificati per amministratore, backend e campagne. LUCY utilizzerà automaticamente il dominio configurato nel sistema per generare il certificato. Se decidi di utilizzare SSL per la campagna, è possibile generare un certificato personalizzato o un CSR (certificate signing request). Puoi anche importare certificati ufficiali verificati.

- Controllo degli accessi basato sui ruoli:** LUCY offre un controllo di accesso basato sui ruoli (RBAC) che limita l'accesso al sistema solo agli utenti autorizzati. I permessi per eseguire determinate operazioni vengono assegnati a ruoli specifici all'interno delle impostazioni dell'utente. A membri o personale (o ad altri utenti del sistema) vengono assegnati ruoli particolari attraverso i quali acquisire i permessi necessari per eseguire particolari funzioni di LUCY.

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

Permissions	View
<input type="checkbox"/> Select All	<input checked="" type="checkbox"/> Create/View Reports
<input type="checkbox"/> Start/Stop Campaign	<input checked="" type="checkbox"/> Export to File
<input type="checkbox"/> Configure Campaign Setting	<input type="checkbox"/> Export to Group
<input type="checkbox"/> Delete Campaign	<input type="checkbox"/> Campaign Full Statistics
<input type="checkbox"/> Edit Recipients	<input checked="" type="checkbox"/> Campaign Basic Statistics
<input type="checkbox"/> Edit Awareness Website	<input type="checkbox"/> Reset Stats
<input type="checkbox"/> Edit Schedule	<input type="checkbox"/> Access Message Log
<input type="checkbox"/> Edit Base Scenario Settings	<input type="checkbox"/> Supervision Log
<input type="checkbox"/> Edit Scenario Settings	<input type="checkbox"/> Reminders
<input type="checkbox"/> Edit Scenario Landing	
<input type="checkbox"/> Edit Scenario Message	

- Gruppi di utenti a più livelli:** carica rapidamente utenti in gruppo tramite CSV, LDAP o file di testo. Crea diversi gruppi, organizzati per dipartimento, divisione, titolo ecc. Aggiorna gli utenti in una campagna in corso. Costruisci gruppi di utenti dinamici basati sui risultati della campagna di phishing.

Home / Users / New User

New User

E-mail

Country Code

Phone

Two-Factor Authentication

Name

Role

Client

Password

Password (repeat)

Current Certificate
 Enable incident reports notifier

Certificate Required

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

- Compatibilità con più clienti:** "clienti" si riferisce a diverse società, dipartimenti o gruppi che hanno una campagna associata su LUCY. Questi clienti possono essere utilizzati, per esempio, per consentire accesso specifico alla campagna o per creare analisi specifiche per il cliente.

DETAILS "LUCY TEST"

Name

Country

State

City

Address

Postal Code

Website

Contact Name

E-mail

Phone

Fax

Logo No logo

CLIENTS OVERVIEW

Client

<input type="checkbox"/> Test Client A	✘
<input type="checkbox"/> Tenant4	✘
<input type="checkbox"/> Client Inc USA	✘
<input type="checkbox"/> Tenant3	✘
<input type="checkbox"/> Lucy Test	✘

« 1 »

REPORTS "LUCY TEST"

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 »

- Modelli di campagna:** nel caso in cui voglia riutilizzare campagne simili, è possibile salvare una campagna completa con modelli di attacco e contenuti di e-learning come modello di campagna. Questa funzione consente di evitare di dover ripetere più volte configurazioni simili.

The screenshot shows the Lucy campaign management interface. At the top, the campaign name is 'Max1' and its status is 'Not Started'. There are buttons for 'Reset Stats', 'Report', 'Save as Template', 'Export', and 'Start'. Below this is a table with columns for 'Campaign', 'Running Time', and 'Created By'. The 'Max1' campaign is listed with a running time of '4 days, 4 hours' and 'N/A' for 'Created By'. A 'New Campaign' modal is open, showing configuration options: Name 'Standard Test & Train Campaign Template', Client 'Lucy Test', Setup Mode 'Start with Default Campaign Template', and Template 'Max1'. A 'Save' button is visible in the modal. To the right, there is a donut chart showing progress: 100.00% for 'Training Sent', 33.33% for 'Training Opened', and 0.00% for 'Training Score (%)'. Below the chart are buttons for 'Training Sent', 'Training Opened', and 'Training Score (%)'. The 'Advanced Settings' section shows 'Successful Attacks' as 1 of 3 and 'Vulnerable Victims' as 0 of 3.

- Configurazione guidata basata sui rischi:** LUCY offre diversi strumenti di configurazione. Crea una campagna completa in meno di 3 minuti utilizzando i modelli di campagna predefiniti o usufruisci della praticità della configurazione guidata. È disponibile una modalità di configurazione basata sui rischi opzionale, che fornisce suggerimenti specifici per la selezione di modelli di attacco e di sensibilizzazione in base alle dimensioni e al settore della società.

The screenshot shows the 'Campaign Wizard' interface. It has a sidebar with steps: 1. Type, 2. Campaign, 3. Attack Template, 4. Attack Settings, 5. Training Template, 6. Training Settings, 7. Recipients, 8. Review, 9. Finish. The main area is titled 'Please choose a campaign type you would like to use.' and contains several options:

- 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.

At the bottom, there are 'Close' and 'Next' buttons.

- **Verifica campagne:** effettua verifiche preliminari prima di avviare una campagna LUCY: verifica delle consegne via email, verifica dei record MX, verifica dei programmi, verifica di spam e altre.

Home / Campaigns / Login & Malware Simulation / Checks

Campaign Status: Not Started ▶ Skip Checks

Please wait, the system is checking your campaign settings.

Check	Status
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.

Help Close

- **Approvazione del flusso di lavoro:** una determinata campagna può essere sottoposto a un supervisore in LUCY per l'approvazione.

Results Completed — Campaign Status: Waiting ▶

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

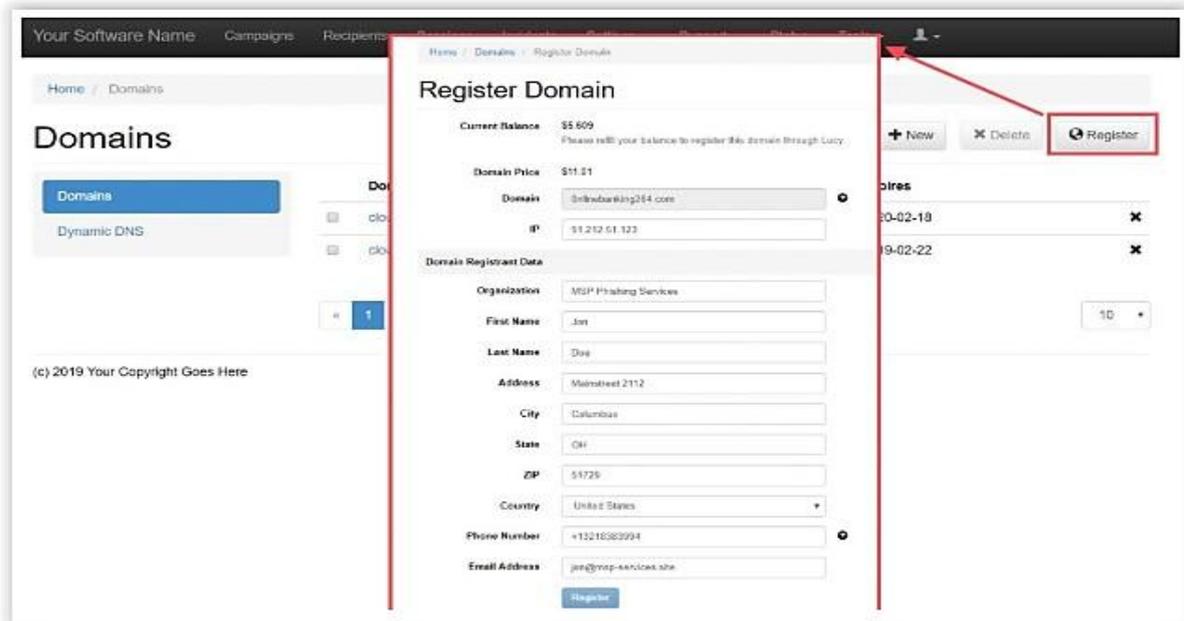
Comments

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 'le-learning'

Reject

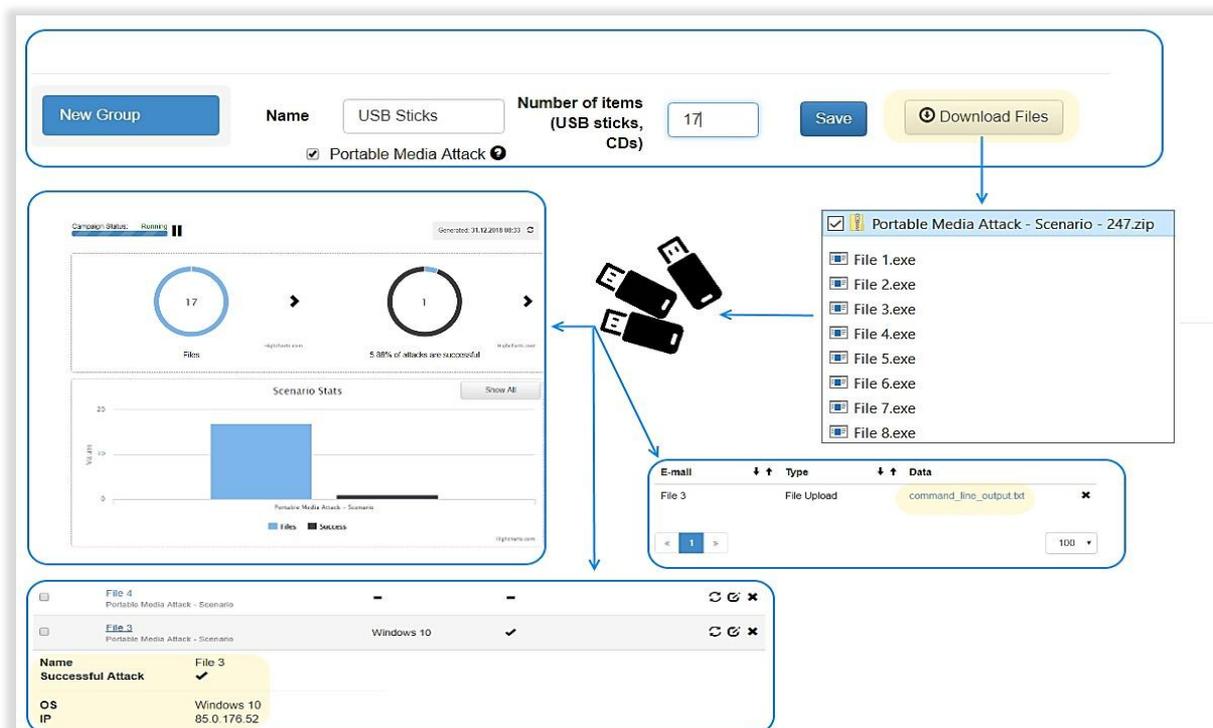
Name	Role	All Campaigns Access
Limited User	User	✓
View	View	—
Supervisor	Supervisor	✓

- API DNS:** L'API DNS consente all'amministratore di creare qualsiasi dominio su LUCY in pochi secondi. Dato che gli aggressori utilizzano nomi di dominio simili a quelli di un cliente (pratica chiamata typosquatting), è possibile rappresentare questo rischio su LUCY. Se il dominio originale del cliente è, ad esempio, "onlinebanking.com", l'API DNS potrebbe essere utilizzato per riservare domini come "Onlinebanking.com", "onl1nebanking.com" o "onlinebanking.services" e assegnarlo successivamente a una campagna. LUCY crea quindi automaticamente le voci DNS corrispondenti (MX, SPF, protezione whois ecc.) per l'IP su cui è installato LUCY. Ovviamente, l'amministratore può utilizzare anche i domini del proprio provider su LUCY.



SIMULAZIONE DI ATTACCO

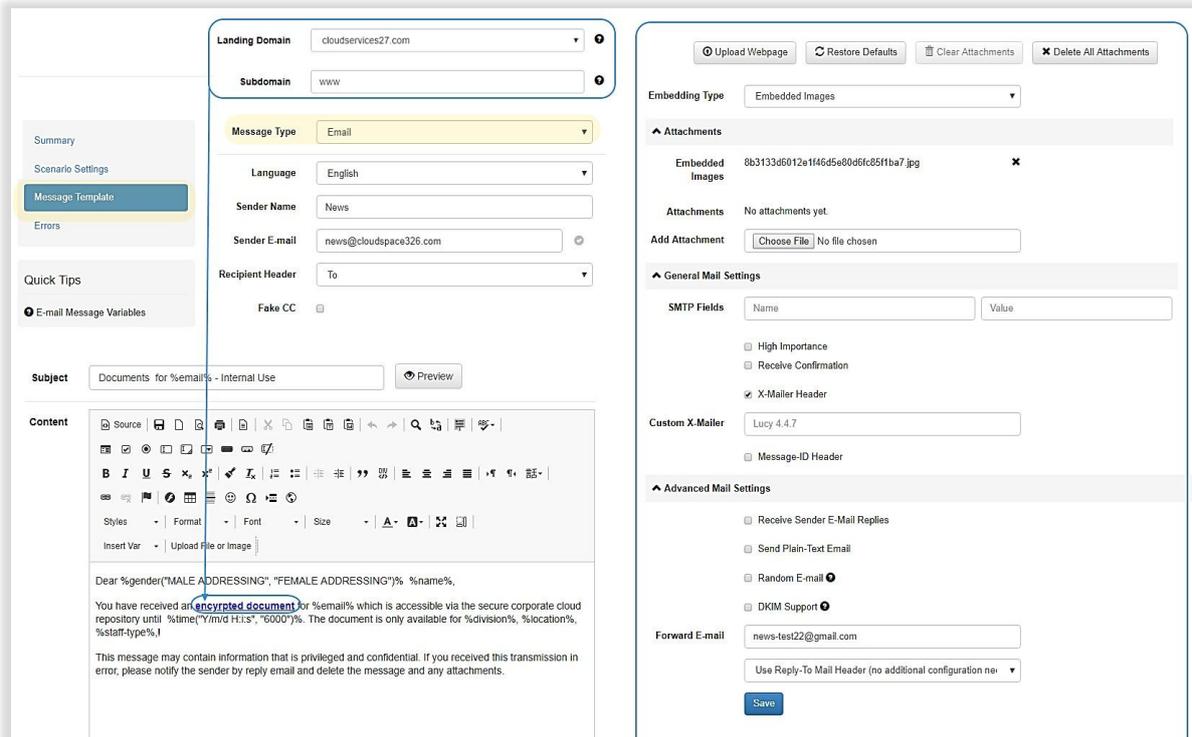
- Attacchi con dispositivi multimediali portatili:** gli hacker possono utilizzare dispositivi multimediali portatili per accedere a informazioni sensibili memorizzate su un computer o una rete. LUCY offre la possibilità di eseguire attacchi con dispositivi multimediali portatili in cui un file modello (ad esempio, file eseguibile, archivio, documento word con macro ecc.) può essere memorizzato su un dispositivo multimediale portatile come USB, scheda SD o CD. È possibile monitorare attivazione (esecuzione) di questi singoli file su LUCY.



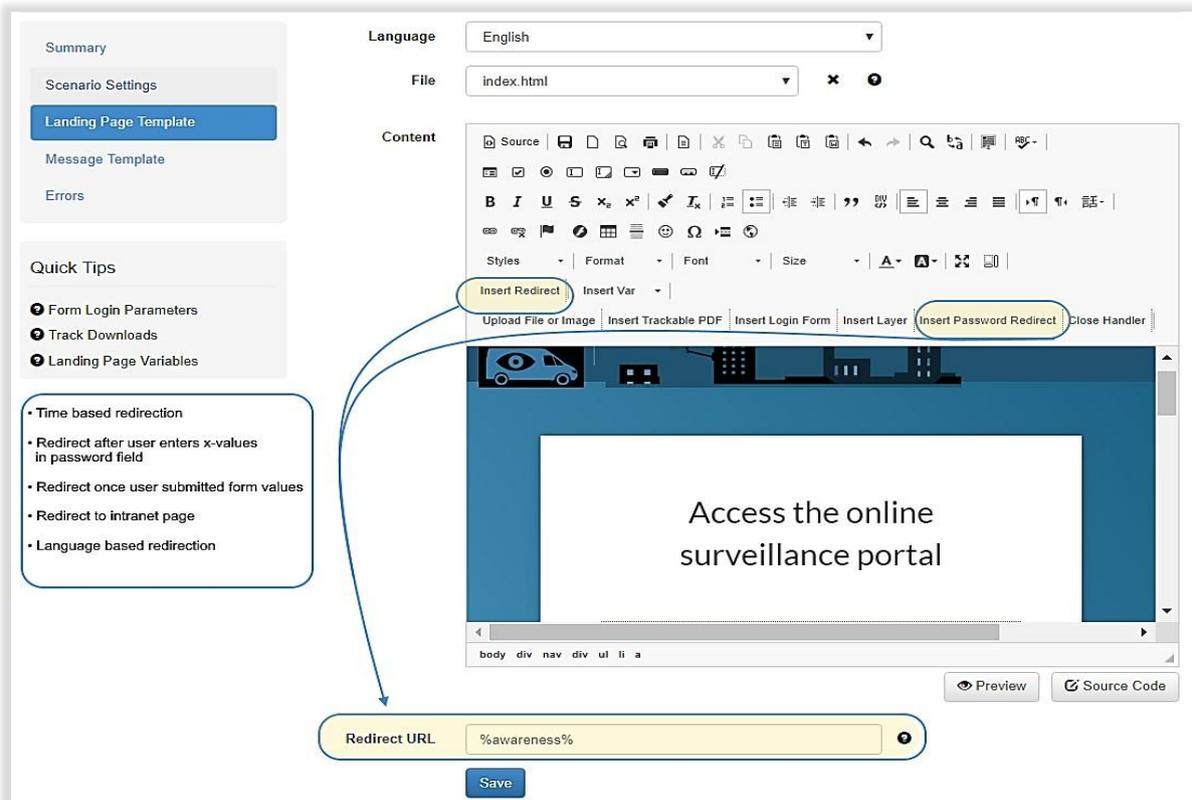
- SMiShing:** lo smishing è, in un certo senso, "phishing SMS". Quando i criminali informatici effettuano "phishing", inviano email fraudolente per ingannare il destinatario ad aprire un allegato con malware o cliccare su un link malevole. Lo smishing utilizza i messaggi di testo anziché le email.

- Attacchi di inserimento dati:** gli attacchi di inserimento dati possono comprendere una o più pagine web che intercettano l'inserimento di informazioni sensibili. Le pagine web disponibili possono essere facilmente personalizzate con l'editor web LUCY. Altri strumenti di editing consentono di impostare rapidamente funzioni come moduli di login, aree di download ecc. senza dover conoscere codice HTML.

- **Attacchi con collegamenti ipertestuali:** una campagna basata su collegamenti ipertestuali invia agli utenti un'email contenente un URL di tracciamento randomizzato.



- **Toolkit di reindirizzamento URL potente:** le funzioni di reindirizzamento flessibili di LUCY consentono all'utente di essere guidato, al momento giusto, nell'area desiderata della simulazione di attacco o del corso di formazione. Per esempio, dopo aver inserito i primi 3 caratteri di una password in una simulazione di phishing, l'utente può essere reindirizzato alla pagina di formazione speciale relativa alla protezione delle password.



- **Attacchi misti:** gli attacchi misti consentono una combinazione di tipi di scenario multipli (basati su file, inserimento dati ecc.) nella stessa campagna.

The image illustrates a multi-stage attack simulation. The top panel shows a legitimate Office 365 registration page with a 'Sign in' button. A blue arrow points from this button to the middle panel, which shows an 'Installation Error - something went wrong' dialog box. A second blue arrow points from the 'DOWNLOAD' button in the error dialog to the bottom panel, which shows the configuration for this error message in a 'Malware Simulation' tool.

Office 365 Registration Page:

Hello John Dee! Welcome to our Office 365 Registration Page. Please use your Windows credentials to register for the online access.

Username:

Password:

Keep me signed in

[Sign in](#)

Can't access your account?

© 2018 Microsoft

[Terms of use](#) [Privacy & Cookies](#)

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.

[DOWNLOAD](#) [Close](#)

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

[Save](#)

- Attacchi basati su file:** gli attacchi basati su file consentono all'amministratore LUCY di integrare diversi tipi di file (documenti word con macro, PDF, eseguibili, MP3 ecc.) in allegati email o siti web generati su LUCY e di misurarne la velocità di download o esecuzione.

The screenshot displays the LUCY web editor interface. At the top, a browser window shows a simulated message with the text: "Hi %name%, you got aMessage, waiting for you from Peter." Below this, it says "Message Date: . This is a free online messaging service supported by ... supported by WhatsApp, Facebook, Skype & Trentmills". A "DOWNLOAD" button is visible on the message. The "Insert Trojan Simulation" dialog is open, showing "Console Interactive" selected under "Select Trojan Type" and "Button #1" under "Select Design". A large downward arrow icon is present in the dialog. Below the dialog, a list of simulation templates is shown, with "Console Post" selected. The "TROJAN SIMULATION: SETTINGS" panel is also visible, showing the following configuration:

- 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** button

- Attacchi doppietta:** questa funzione permette di inviare più email di phishing in ogni campagna, tra cui una prima email benigna (l'esca) che non contiene nulla di maligno e che non richiede una risposta da parte del destinatario.

The screenshot shows the configuration interface for a phishing email campaign. On the left, a sidebar contains navigation options: Summary, Scenario Settings, Landing Page Template, Message Template, Lure Template (highlighted in blue), Errors, Quick Tips, and E-mail Message Variables. The main area is titled 'Message Type' and contains the following fields:

- 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:** A rich text editor containing the following text:

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,

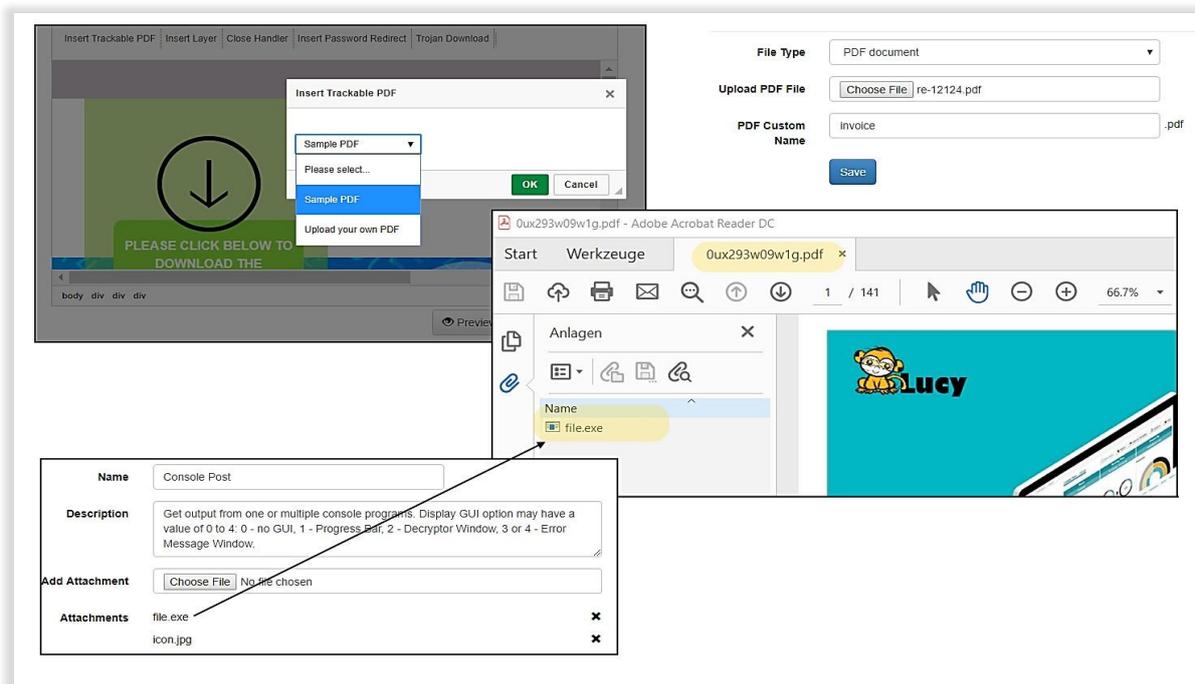
IT-Department
- Success Action:** Data Submit
- Collect Data:** Partial
- Double Barrel Attack (highlighted in yellow)
- Lure Delay:** 3600
- Url Shortener:** bit.ly
- Login Regexp:** lw.*lw
- Password Regexp:** (empty)
- Save** button

- Attacchi basati su Java:** gli attacchi basati su Java consentono all'amministratore LUCY di integrare un applet verificato all'interno dei modelli di attacco basati su file o misti forniti su LUCY e di misurarne l'esecuzione da parte degli utenti.

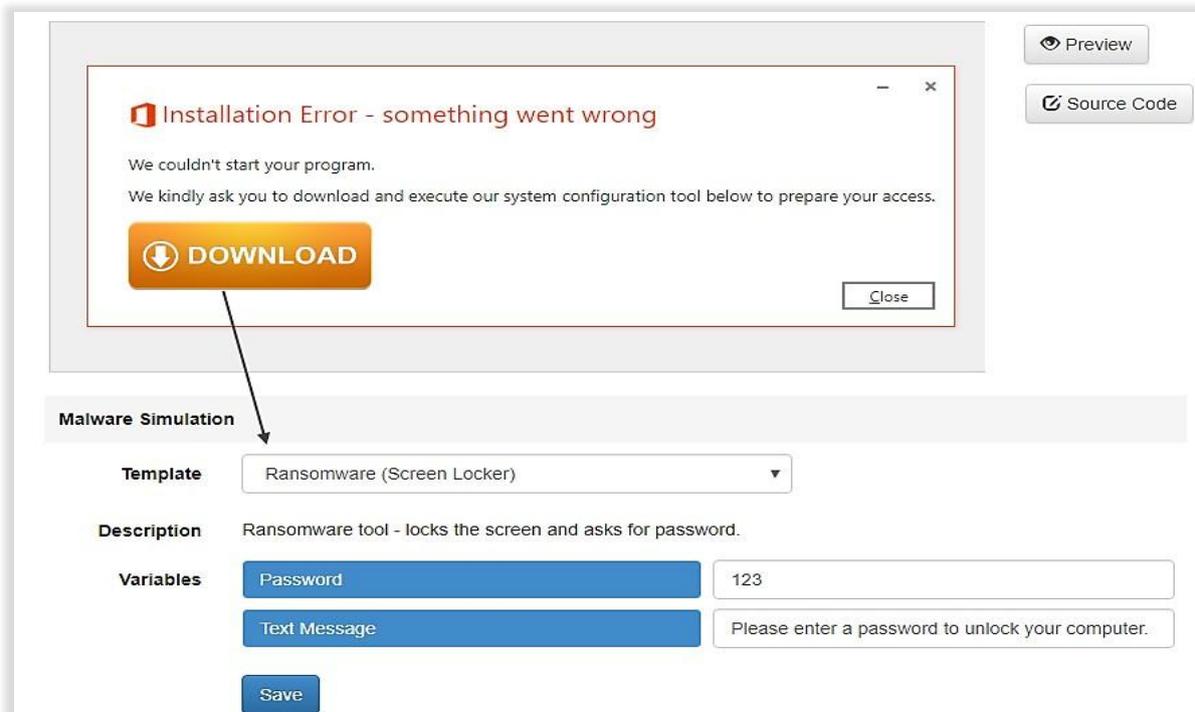
The screenshot shows the configuration interface for a Java-based attack simulation. It is divided into three main sections:

- 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
 - Save** button
- File Type: Tunnel Executable**
 - Use a signed applet to download and run an executable malware simulation.
 - Download Path:** %TEMP%
 - Save** button
- Malware Simulation**
 - 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
 - Save** button

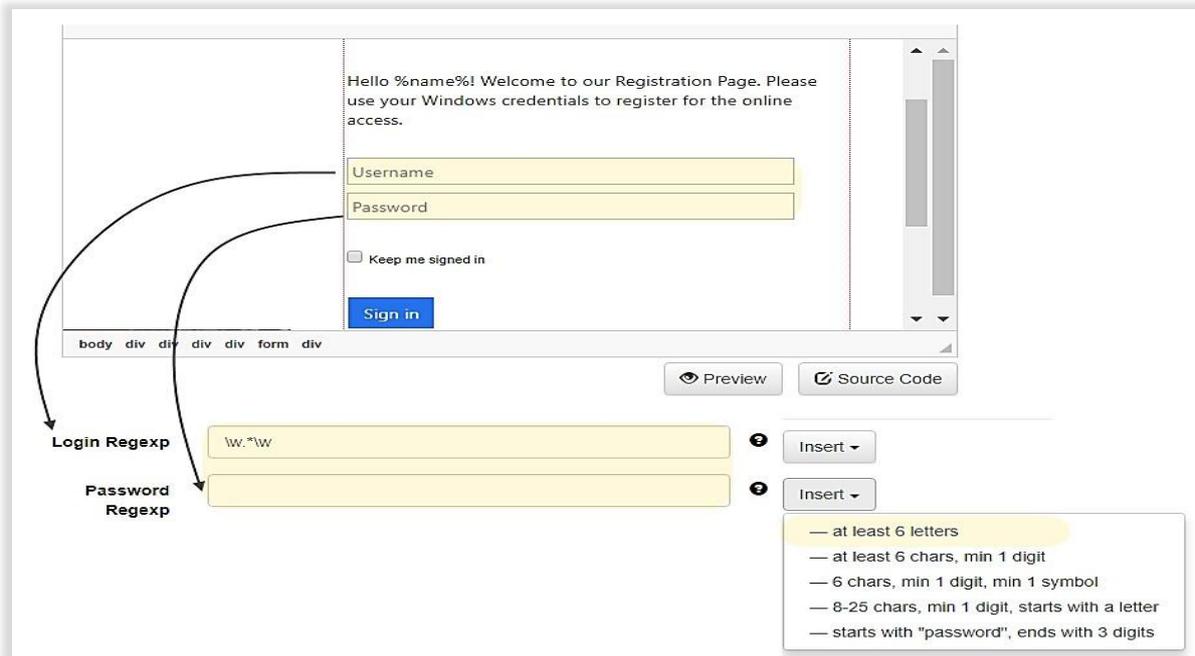
- Attacchi basati su PDF:** con questo modulo è possibile simulare attacchi di phishing basati su PDF. LUCY consente di "nascondere" file eseguibili come allegati PDF e di misurarne l'esecuzione. Inoltre, è possibile generare collegamenti di phishing dinamici all'interno dei PDF.



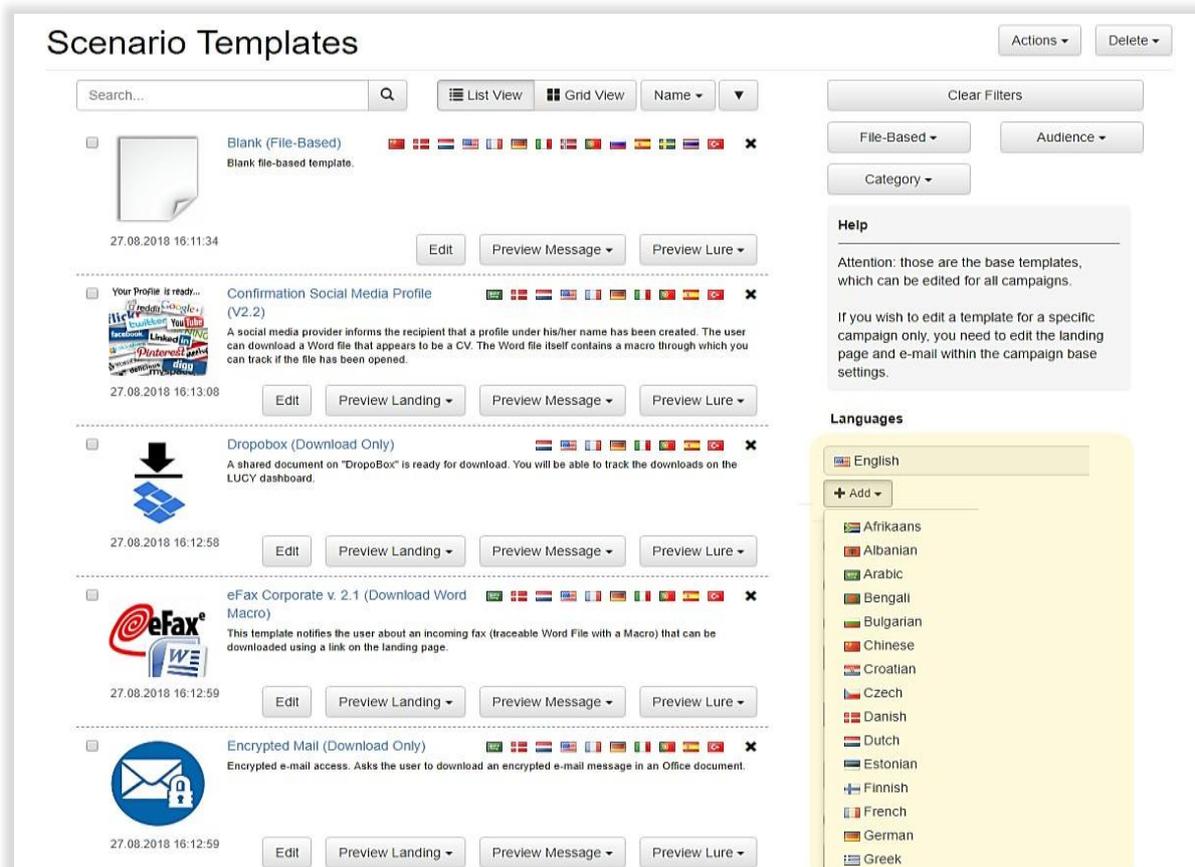
- Attacchi di simulazione ransomware:** LUCY offre due diverse simulazioni di ransomware, una per mettere alla prova gli impiegati e l'altra l'infrastruttura.



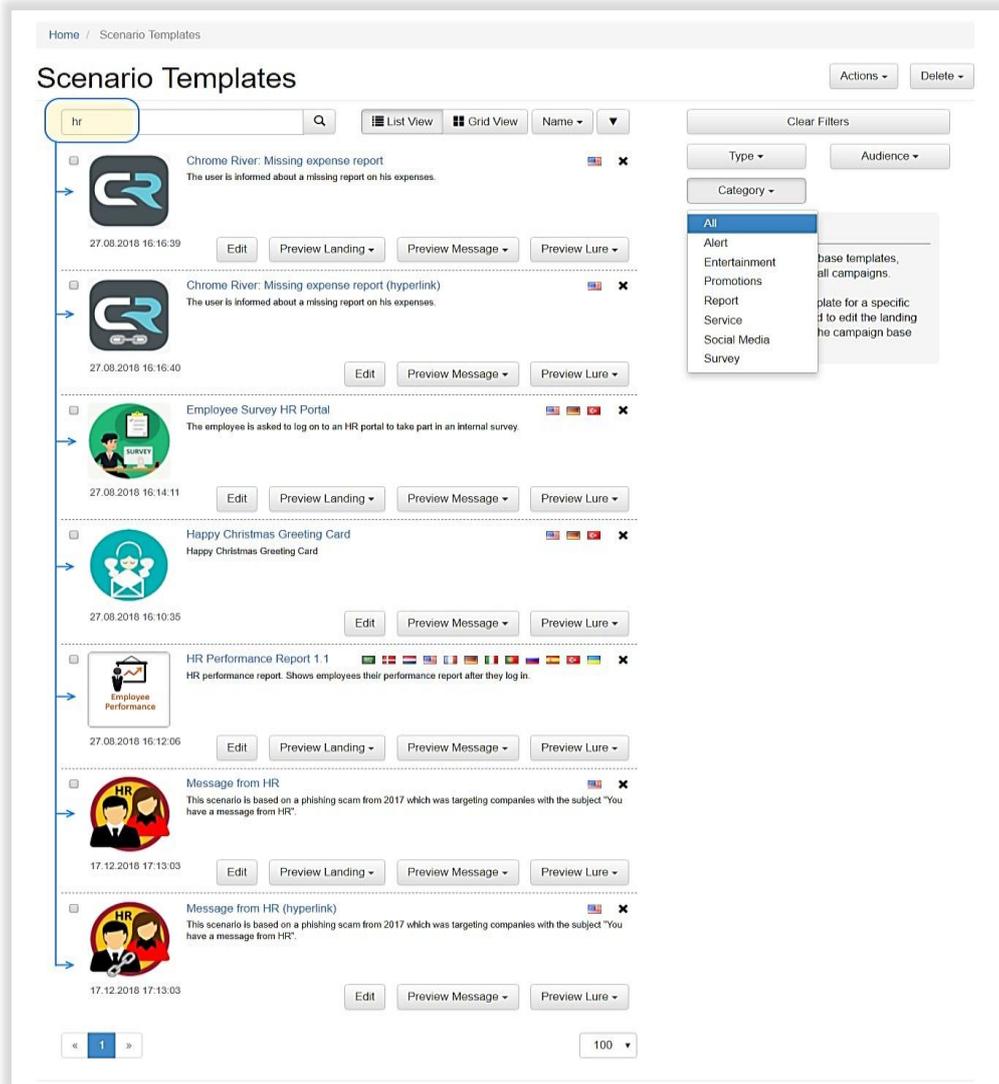
- Toolkit di convalida inserimento dati:** nelle simulazioni di phishing, è importante prevenire falsi positivi nei campi di accesso (ad esempio, accesso con sintassi non valida). Le direttive societarie possono anche vietare la trasmissione di dati sensibili come password. Per questo motivo, LUCY mette a disposizione un motore di filtraggio dei dati inseriti flessibile che offre una soluzione adatta ad ogni esigenza.



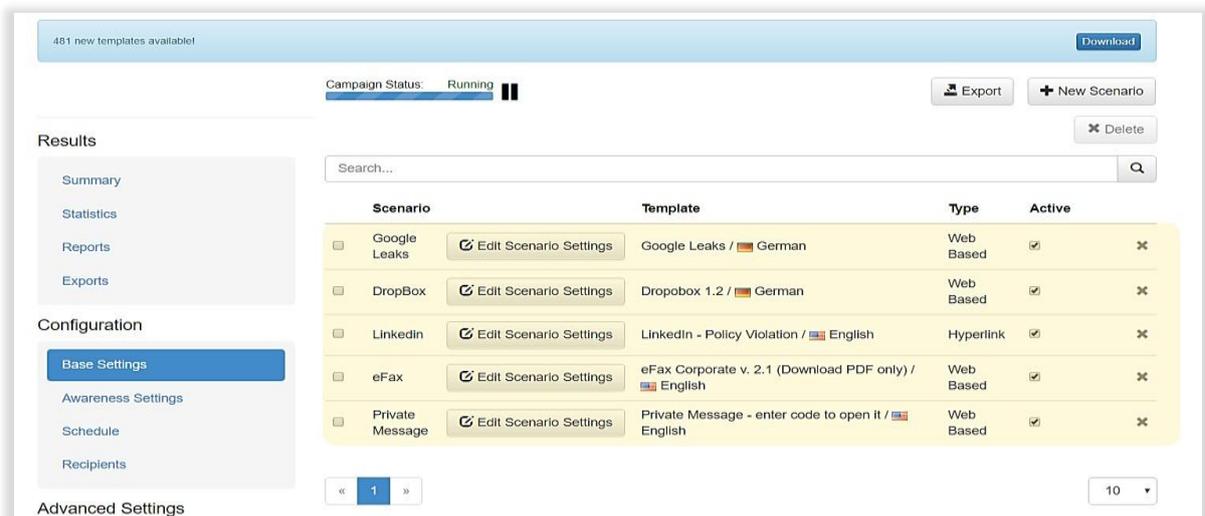
- Libreria di modelli di attacco multilingue:** LUCY dispone di centinaia di modelli di attacco predefiniti in più di 30 lingue nelle categorie di inserimento dati (modelli con un sito web), basati su file (email o siti web con un download di file), collegamenti ipertestuali (email con un link), misti (combinazione di inserimento dati e download) e dispositivi multimediali portatili.



- **Modelli specifici per settore e divisione:** sono disponibili modelli di attacco specifici per settore o divisione.



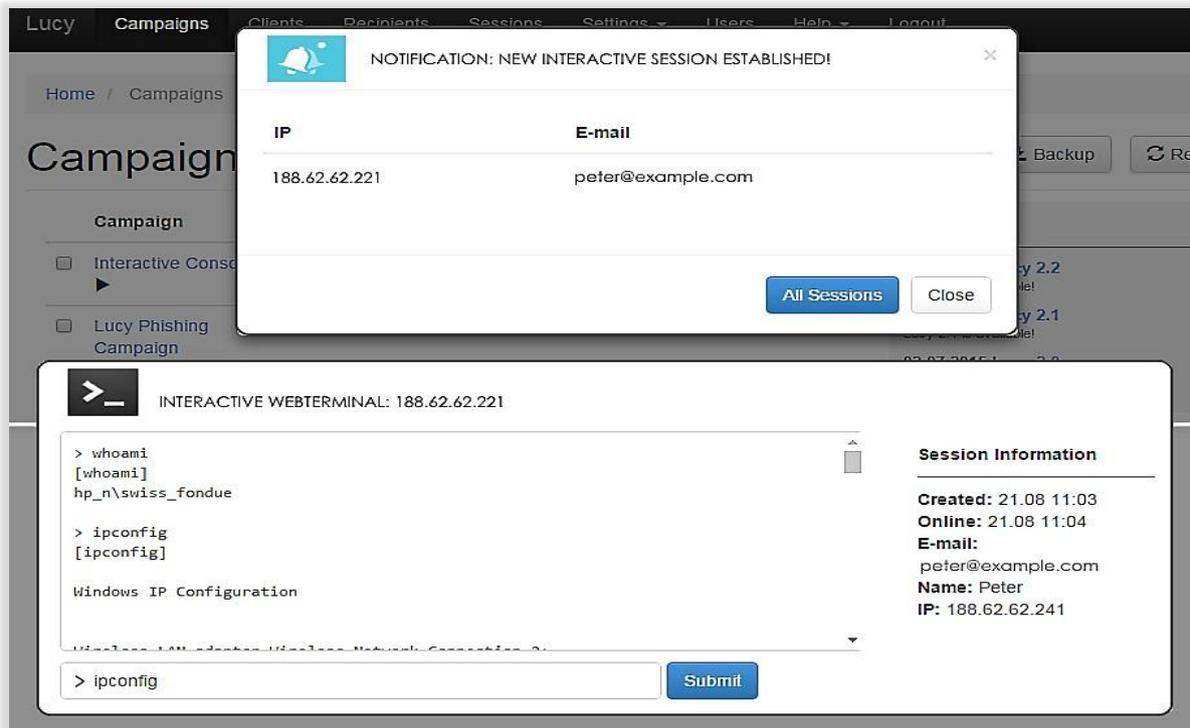
- **Utilizzo simultaneo di modelli di attacco:** LUCY ti offre la possibilità di utilizzare più modelli di attacco simulato in una singola campagna. Combina diversi tipi (collegamenti ipertestuali, basati su file ecc.) con diversi temi di attacco per ottenere la più ampia copertura di rischio possibile e una migliore comprensione delle vulnerabilità degli impiegati. In combinazione con il nostro schedatore randomizzato, è possibile eseguire modelli di attacco complessi per un periodo di tempo più lungo.



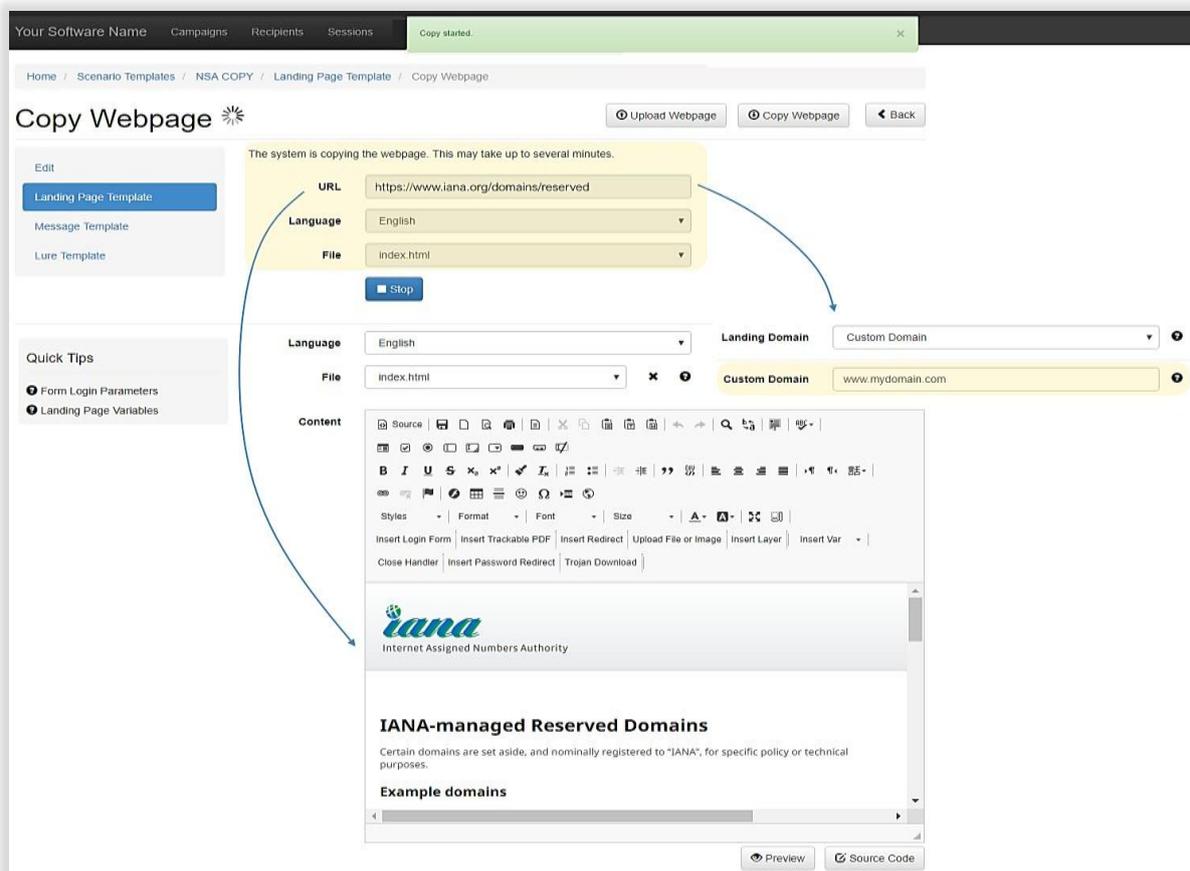
- Variazioni degli URL di attacco:** prendi il controllo degli URL generati per identificare i destinatari. Utilizza stringhe di URL brevi (< 5 caratteri) o lunghe automatizzate o imposta URL singoli per ogni utente. La creazione manuale di URL consente di formare link che un utente può facilmente ricordare. Questo è indispensabile negli ambienti in cui i click sui link sono disabilitati nelle email.

- Accorciamento URL:** l'accorciamento degli URL è un servizio internet relativamente nuovo. Dato che molti servizi social online impongono limitazioni sui caratteri (ad es. Twitter), questi URL sono molto pratici. L'accorciamento di URL può, tuttavia, essere utilizzato da criminali informatici per nascondere il vero obiettivo di un link, come ad esempio phishing o siti web infetti. Per questo motivo LUCY offre la possibilità di integrare diversi servizi di accorciamento all'interno di una campagna di phishing o smishing.

- Kit pentest:** il kit pentest è un sottomodulo di un toolkit di simulazione malware ed è indicato con il nome di "sessioni interattive". Consente di comunicare in modo interattivo con un pc client che si trova dietro i firewall usando connessioni http/s inverse.



- Duplicatore siti web:** crea rapidamente delle landing page altamente professionali per le tue campagne. Duplica siti web esistenti e aggiungi ulteriori livelli con campi di inserimento dati, file da scaricare e altro.



- Attacchi basati su livelli:** il programma di formazione sul phishing basato su livelli per gli impiegati serve per rendere misurabile il rischio di hackeraggio sociale. Le analisi scientifiche permettono di identificare i fattori di rischio in modo da poter offrire contenuti di formazione individuali automaticamente.

The screenshot shows the 'New Campaign' configuration page. The 'Setup Mode' section is highlighted in yellow and includes the following options:

- Expert Setup (Manual Configuration)
- Pre-selected 5 minutes setup
- Launch a saved campaign template
- Level based campaign** (selected)

Under 'Level based campaign', there are several sub-sections:

- 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...

Other visible settings include 'Infrastructure testing', 'E-Learning Settings', 'Tracking', and 'View Options'. A 'Save' button is located at the bottom right.

- Simulazione di spear phishing:** il sistema di simulazione spear phishing funziona con variabili dinamiche (genere, orario, nome, email, link, messaggi, divisione, nazione ecc.) utilizzabili in modelli di landing o messaggi.

The screenshot shows the spear phishing simulation configuration page. The 'Content' field is highlighted with a blue box, and a list of dynamic variables is shown on the right. The variables include:

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

The 'Content' field contains the following text:

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.

A 'Save' button is located at the bottom right.

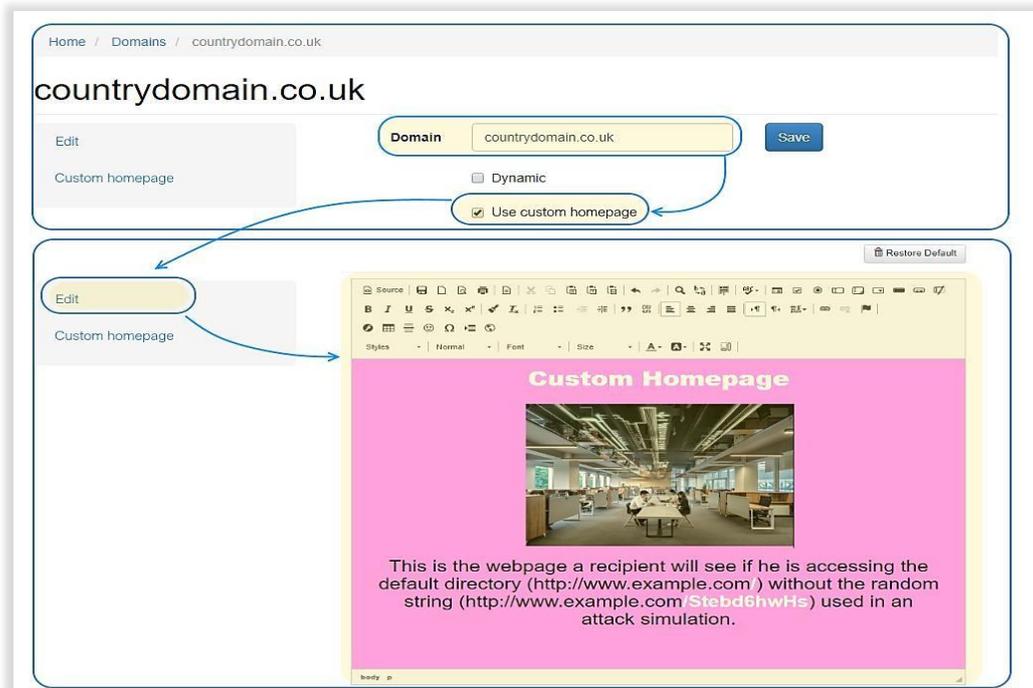
- **Supporto DKIM / S / MIME per email di phishing:** firme digitali per email: invia email di phishing simulato firmate (s/mime). Usa DKIM per ottenere un punteggio mittente migliore.

The screenshot shows the 'test' email configuration page. The 'Message Type' is set to 'Email', 'Language' to 'English', and 'Sender Name' to 'test'. The 'Recipient Header' is set to 'To'. The 'Subject' is 'Affordable car leasing for our employees'. The 'Embedding Type' is 'Embedded Images'. The 'General Mail Settings' include 'SMTP Fields' and 'Custom X-Mailer' set to 'Lucy 4.4.8'. The 'Advanced Mail Settings' section is highlighted in yellow and includes options for 'DKIM Support', 'DKIM Subdomain' (set to 'mail'), 'Forward E-mail', 'Delivery Method' (set to 'Use System Settings'), and 'Use S/MIME Certificate' (checked). There are also fields for 'SSL Certificate', 'SSL Key', 'SSL Key Password', and 'SSL Chain', all currently set to 'No file chosen'. A 'Save' button is at the bottom right.

- **Scansione email:** vuoi scoprire quali indirizzi email della tua società si possono trovare su Internet? Utilizza il sistema di scansione email LUCY e scopri cosa un hacker conosce già sulla tua società.

The screenshot shows the 'Mail Scan' interface. A green notification bar at the top says 'Scan started.' Below it, a message states: '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.' The 'Domain' field is set to 'phishing-server.com'. The 'Scan' button is highlighted in blue. The interface also includes a 'Recipients' section with 'Edit Group Name' and 'Import' options. A list of search engines and sources is shown with checkboxes: 'Crawler', 'Follow external links', 'Yahoo', 'Lixam', 'Wotbox', 'Yandex', 'Bing', 'Public Key Servers', 'Additional Sources', and 'Paid Sources'. A 'Stop' button is at the bottom.

- Creazione homepage personalizzata:** i destinatari con migliori competenze tecniche potrebbero usare il loro browser per trovare il dominio o l'indirizzo IP associato al link di phishing generato in modo casuale. Per evitare che compaiano messaggi di errore o che l'utente finale arrivi addirittura nell'area di accesso della console amministratore, è possibile creare delle "homepage" generiche all'interno di LUCY per i domini utilizzati nella simulazione di phishing.



TEST INFRASTRUTTURE

- Toolkit test malware:** il toolkit di simulazione malware è un programma di simulazione malware avanzato in grado di emulare varie minacce. Consente a un revisore di accedere a un set di funzioni avanzate equivalente a tanti strumenti utilizzati da criminali informatici. Lo strumento, pertanto, consente all'amministratore LUCY di effettuare delle verifiche di sicurezza senza coinvolgere gli impiegati al di fuori del dipartimento informatico.

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

- **Test filtri email e web:** questa funzionalità fornisce una risposta a una delle questioni più importanti della protezione di traffico internet ed email: quali tipi di file possono essere scaricati dal web e quali allegati email vengono filtrati o meno?

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

MWFT (1)

- Summary
- Base Settings
- Reports

Advanced Settings

- User Settings

Logs

- Supervision Log
- Message Log
- Errors

Campaign Status: Not Started
Reset Stats
Export
Start

Mail & Web Test Overview

2

7% of files downloaded

27

96% of files submitted

1

4% of files downloaded successfully

1

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

Mime Types
+ New File
+ New Class

- 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

Edit
File List

Name

Mime Type

Class

Dangerous File Types in archives

File

- Rilevamento vulnerabilità client passiva e attiva:** questa funzione consente di testare in modo locale il browser client e rilevare le possibili vulnerabilità basate su librerie JavaScript personalizzate e dati dell'user agent del browser. I plugin trovati possono essere automaticamente comparati con database di vulnerabilità (CVE) per identificare dispositivi vulnerabili.

test
Scenario Status: Running ||

Summary

[Scenario Settings](#)

Template Affordable car leasing for employees / English

[Change/Select Template](#)

Active Detection

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

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 -

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

Advanced Information Gathering

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

Campaign Status: Running || Generated: 28.12.2018 12:54

Operating Systems

Windows 10 | Windows 8

Browsers

Chrome 71.3578 | Firefox 3.6.24

Top Plugins

Extended Analysis

- **Test di spoofing:** esamina le tue infrastrutture per individuare vulnerabilità di spoofing email.

Home / Mail Spoofing

Mail spoofing test

Domain: ✕ Start Test

Recipient Email:

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

TEST TECNICI

- **e-Learning basato sulla reputazione:** forma i tuoi impiegati secondo le competenze richieste. Misura le abilità degli impiegati e favorisci una competizione amichevole tra colleghi (gamification). Sulla base della reputazione di ogni utente, il sistema è in grado di fornire sessioni di formazione multiple. La reputazione è basata sul comportamento dell'utente nelle simulazioni di phishing, oltre che altri fattori. Questo assicura che gli utenti recidivi ricevano contenuti di formazione diversi rispetto a coloro che cliccano su una simulazione di attacco per la prima volta.

Summary

- Scenario Settings
- Mail Settings
- SSL Settings
- Landing Page Template
- Message Template
- Errors

Template Affordable car leasing for employees / English

Change/Select Template

Name

Send Link to Awareness Website Automatically

Send Awareness By Click Rate %

Send Awareness By Success Rate %

Awareness Delay

Configuration

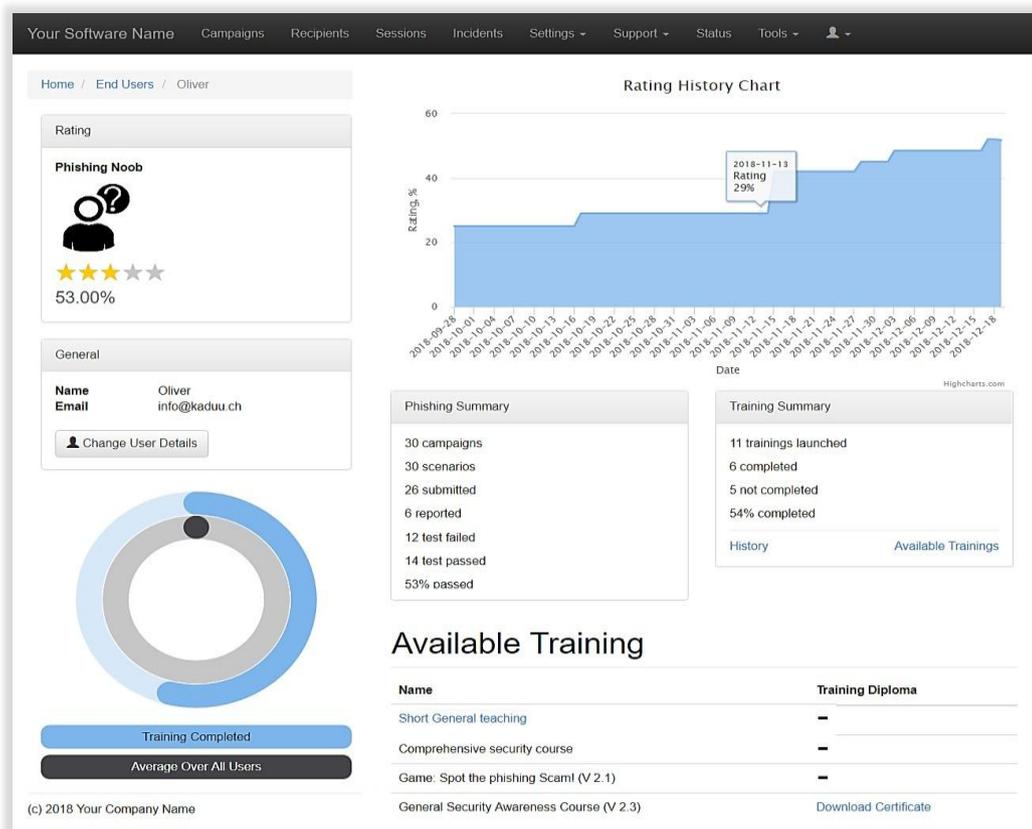
- Base Settings
- Awareness Settings

Export + New Awareness

Awareness	Course					
Comprehensive security course	<input checked="" type="checkbox"/> Edit Awareness Settings	Comprehensive security course	0	+	-	✕
Repetition Course	<input checked="" type="checkbox"/> Edit Awareness Settings	Avoid & Recognize Phishing Attacks (V 2.3)	2	+	-	✕
Short General teaching	<input checked="" type="checkbox"/> Edit Awareness Settings	Email Only - This was a phishing simulation & Tips	3	+	-	✕

< 1 >
10 ▾

- Portale di formazione utente finale:** learning management system (LMS): permette a tutti gli utenti di accedere in modo permanente a una homepage di formazione personalizzata che include i tuoi corsi su misura per loro. Su questa homepage possono vedere le statistiche prestazionali, riprendere o ripetere corsi di formazione, creare certificati dei corsi e comparare i loro risultati con altri dipartimenti o gruppi.



- Diploma di formazione sulla sensibilizzazione:** è possibile creare dei certificati di e-learning, stampabili dai destinatari direttamente dentro un corso di formazione o il portale LMS.

Awareness Training Diploma Template

File: index.html

Message

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 Completion

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**

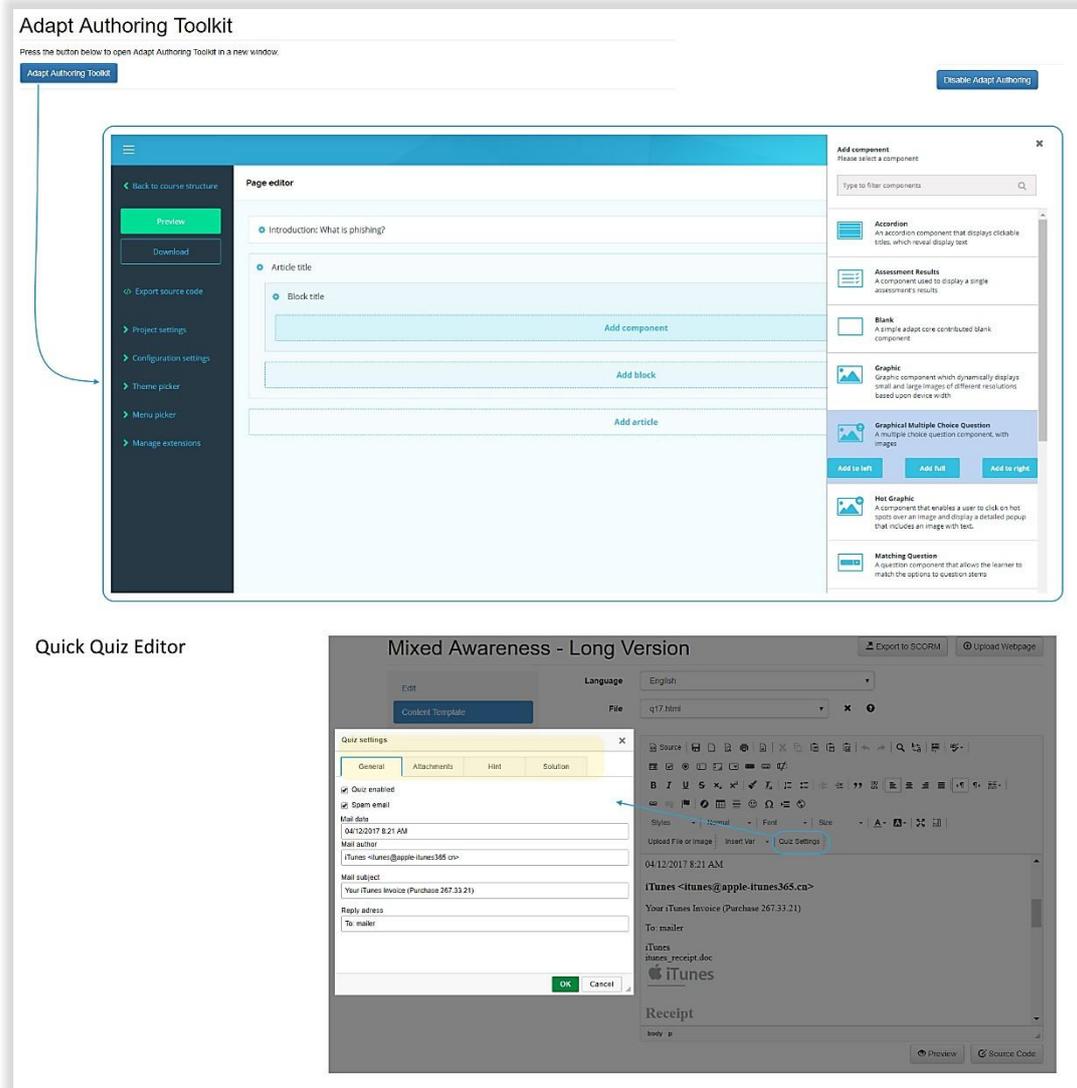
Quiz results: **8/11**

ON 28.11.2018 at 13:50

[your logo here]

Print Certificate Restart Course

- Toolkit di creazione e-learning:** il toolkit di creazione e-learning (Adapt) permette di creare contenuti di formazione individualizzati. Copia e incolla video o altri media interattivi, inserisci esami da menu predefiniti, crea contenuti di e-learning interattivo da zero in breve tempo.



- Formazione sulla sensibilizzazione su media interattivi:** integra media interattivi (video, audio o altri elementi che incoraggiano gli spettatori a interagire con i contenuti) nei corsi di formazione sulla sensibilizzazione. Usa video di formazione esistenti, adattali o aggiunti i tuoi media interattivi personali.

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", "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

[...and many more](#)

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 16:13:19

[...and many more](#)

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://go.gi/1XW9SG>. Duration: 5:40 minutes | Skill Level: Low | Audience: All | Interactive: No | Video stats possible: Yes

27.08.2018 16:13:54

[...and many more](#)

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

[...and many more](#)

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

15.11.2018 17:44:27

[...and many more](#)

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 360 pixels.

27.08.2018 16:14:22

[...and many more](#)

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

[...and many more](#)

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

[...and many more](#)

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 windows.

15.11.2018 17:44:28

[...and many more](#)

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

[...and many more](#)

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

[...and many more](#)

Security News

News: Do you know how to handle security incidents 🇺🇸 🇩🇪 🇫🇷 🇮🇹 🇪🇸 🇬🇧 🇮🇸 🇯🇵 🇰🇷 🇸🇪 🇸🇮 🇻🇪 🇽

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

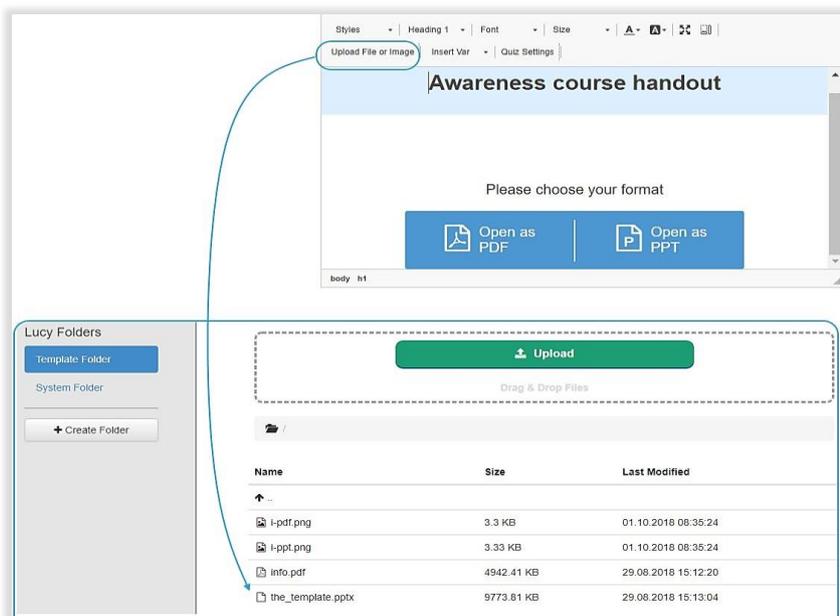
28.12.2018 14:48:47

[...and many more](#)

- Libreria di formazione:** i tuoi impiegati possono accedere ai contenuti di formazione della società da una pagina di panoramica chiamata "libreria di formazione". Contiene una vasta selezione di modelli di e-learning regolari di LUCY, che servono come input. La pagina di panoramica può essere ordinata secondo certi argomenti (video, quiz, test ecc.).

- Supporto per formazione statica:** i contenuti di formazione possono essere pubblicati anche su pagine statiche all'interno di LUCY o dell'intranet, conferendo all'utente un accesso permanente, indipendentemente da possibili simulazioni di attacco.

- **Supporto per formazione offline:** LUCY viene fornito con una serie di modelli modificabili (file Adobe Photoshop o Illustrator) per formazione su sensibilizzazione, come poster, screensaver, volantini ecc.



- **Moduli di microapprendimento:** abbiamo progettato dei moduli di microapprendimento (ad esempio, video di 1 minuto o testi di sensibilizzazione di 1 pagina) che possono essere adattati alle esigenze del marchio e alle politiche della tua società.

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

Edit
Preview Website ▾
Preview E-mail ▾

Micro Module: Spoofting & CEO Fraud

In this course the student will be guided through various lessons. Topics covered include "Phishing", "Spoofting" & "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

Edit
Preview Website ▾
Preview E-mail ▾

Micro Module: Password security

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

26.12.2018 15:08:18

Edit
Preview Website ▾
Preview E-mail ▾

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

Edit
Preview Website ▾
Preview E-mail ▾

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!

- Personalizzazione video:** inviaci il logo della tua società e lo includeremo nei video di formazione. Vuoi un'altra lingua? Nessun problema. Imposteremo il video nella lingua che preferisci. Vuoi una scena diversa? Basta scaricare gli script del video e contrassegnare le modifiche desiderate.



27.08.2018 16:12:23

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

🇧🇪 🇺🇸 🇫🇷 🇩🇪 🇮🇹 🇪🇸 🇨🇳 ✕

Edit
Preview Website ▾
Preview E-mail ▾

Upload

Drag & Drop Files

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.

- Formato adatto per dispositivi mobile:** molti moduli integrati di LUCY sono disponibili in un formato adatto a dispositivi mobile che offre ai tuoi utenti la possibilità di seguire il corso di formazione sul qualsiasi dispositivo collegato.

ONE PAGER 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 300 pixels.
 27.03.2018 10:14:22 [Edit] [Preview Website] [Preview E-mail]

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:

- A common tactic phishers employ is to use a seemingly legitimate sender's address.
- Often the email is addressed to "Dear customer" or no specific name is mentioned.
- Hovering over the provided link will show a different URL and therefore NOT the institution's trusted web address.
- 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.
- 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 large lists of recipients. Please see the tips below:

- Importazione / Esportazione video:** puoi esportare i video LUCY sui tuoi sistemi oltre che importare i tuoi video su LUCY.

The screenshot shows the 'Awareness Templates' interface. At the top, there are search and view options (List View, Grid View) and a dropdown menu for 'Name'. Below this, a video titled 'Data Privacy & GDPR Video' is selected. A blue circle highlights the 'Video' dropdown menu, and another blue circle highlights the 'Upload' button in the 'Lucy Folders' section. A third blue circle highlights the 'Download' button in the 'Lucy Folders' section. The main content area shows a file list with columns for Name, Size, and Last Modified. The files listed are:

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

- Suggerimenti di formazione dinamica:** i suggerimenti dinamici integrati permettono all'amministratore di impostare dei marcatori all'interno dei modelli di attacco che potrebbero indicare ai tuoi impiegati il punto dove è possibile rilevare l'attacco di phishing, nel materiale di e-learning.

The screenshot shows the 'Comprehensive security course' interface. At the top, there are navigation links (Home / Awareness Templates / Comprehensive security course / Content Template) and buttons for 'Export to SCORM' and 'Upload Webpage'. The 'Export to SCORM' button is highlighted with a blue circle. Below this, there are settings for 'Language' (English) and 'File' (index.html). The main content area shows a rich text editor with a toolbar and a preview of the course content, which includes the text 'General Security Awareness Cou'. Below the editor, there is a 'Quick Tips' section with three items: 'Awareness Website Variables', 'Quiz Integration', and 'Create Custom Video'. At the bottom, there is an 'Exports' section with a table showing a list of 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		✓ ✗
28.12.2018 15:19:11	Awareness Template - Avoid & Recognize Phishing Attacks (V 2.3)		✓ ✗

A blue circle highlights the date '31.12.2018 15:08:53' in the 'Exports' table. A blue circle also highlights the 'scorm-export.zip' file name in the 'Exports' section.

COINVOLGIMENTO IMPIEGATI

- Segnalazione delle email con un solo click:** gli utenti finali possono segnalare email sospette con un solo click su uno o più account email e inoltrarle alla console di analisi incidenti LUCY.

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. Good job in spotting the attack!

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

[Save]

Report Email

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?

[Yes] [No]

- Rafforzamento del comportamento positivo:** il nostro plugin fornisce automaticamente rafforzamento del comportamento positivo mostrando gratitudine agli utenti finali tramite un messaggio personalizzato definito dalla tua società.

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. Good job in spotting the attack!

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

[Save]

Report Email

Report Phishing To Your Security Team

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

[OK]

- Richiesta di ispezione approfondita:** a volte gli utenti vogliono sapere se l'email ricevuta può essere aperta in sicurezza. L'utente può utilizzare la "richiesta di ispezione approfondita" nel plugin locale per informare il team di sicurezza che desidera ricevere un feedback sull'email segnalata.

The screenshot illustrates the workflow for requesting a deeper analysis of a phishing email. It is divided into four main sections:

- Settings:** A configuration panel where users can define messages. The "Deeper Analysis Request Message" field is highlighted, indicating the text used for the request.
- Email List:** A list of incoming emails. One email with a score of 4.60 and status "Open" is highlighted.
- Report Phishing To Your Security Team Dialog:** A modal window that appears when a user reports a phishing email. It asks, "Do you wish to request an additional message analysis from your security team?" with "Ja" (Yes) and "Nein" (No) buttons.
- Phishing Incident Reports Table:** A table listing reported incidents. The entry corresponding to the highlighted email in the list is shown with a "Need more analysis" button.

Time	Email	Client	Campaign	Score	Status	Actions
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	⚠️🚫🔍🗑️ Need more analysis
03.12.2018 06:57	oliver@muenchow.ch	Lucy Test	Attack CS	0.00	Simulation	⚠️🚫🔍🗑️

- Analisi degli incidenti automatica:** Gestisci e rispondi alle email sospette segnalate utilizzando una console di gestione centralizzata. Il sistema di analisi LUCY permette di ispezionare automaticamente i messaggi segnalati (intestazione e corpo). Il sistema di analisi include un punteggio di rischio individuale, fornendo una classifica in tempo reale delle email segnalate. Inoltre, riduce il carico di lavoro del team di sicurezza.

Home / Phishing Incident Reports

Incident Reports

Send Abuse Delete Delete All Settings Download Plugin

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

Filter: Show only mails from this domain
 Search:
 Reputation Filter: Show only mails with rating >
 Client: All
 From Date: 29.12.2017
 To Date: 30.12.2018
 Status: All
 Email Domain: All
 Update

10 rows per page

Home / Phishing Incident Reports / 09.03.2018 12:17

09.03.2018 12:17

Send Abuse Rescan

Summary Header Analysis Domain Analysis Body Analysis Threat Indicators

	Score	Rule active?
Reply-to Mismatch different reply-to address defined than the actual (more info...)	1.60	Active <input checked="" type="checkbox"/> Inactive <input type="checkbox"/>
New Domain Domain has been reserved in the last 30 days (more info...)	20.00	Active <input checked="" type="checkbox"/> Inactive <input type="checkbox"/>
Link Display mismatch link display name different from the actual link (more info...)	0.00	Active <input type="checkbox"/> Inactive <input checked="" type="checkbox"/>

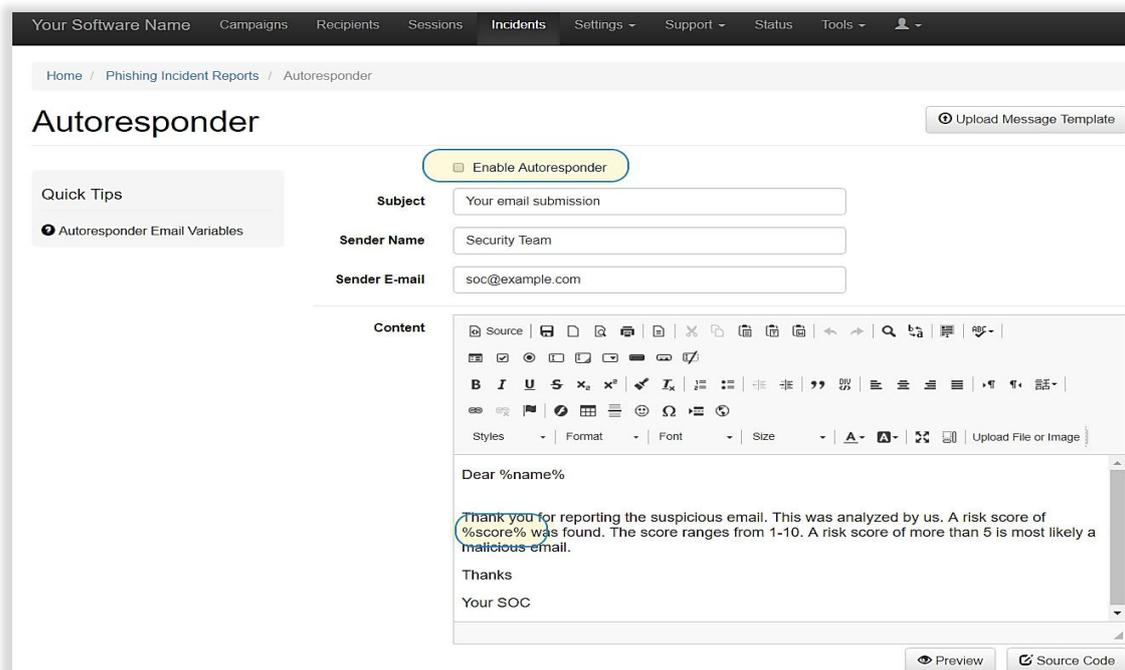
Summary Mail Server Analysis Domain Analysis Body Analysis

Overall Risk Score: 2.5 of 10.0

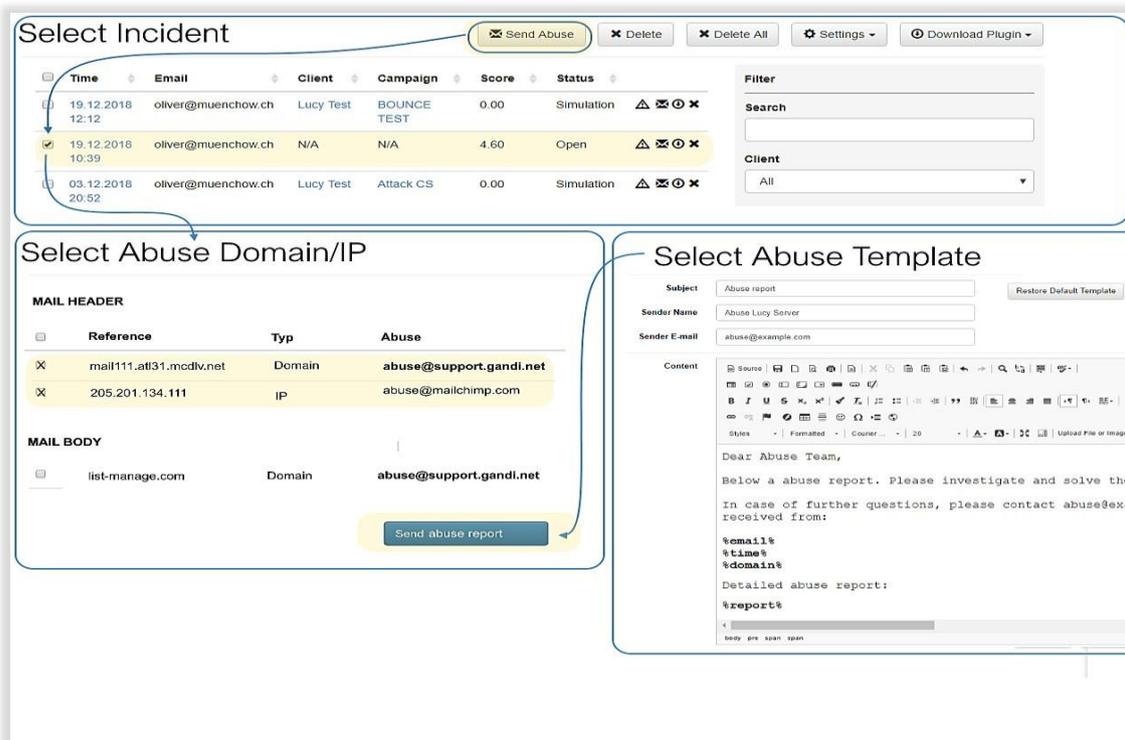
Need More Analysis

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:
 Save

- Feedback degli incidenti automatico:** il sistema di risposta incidenti automatico permette di inviare una notifica automatica all'utente finale fornendo i risultati di un'analisi delle minacce. Il messaggio di testo è configurabile liberamente ed è possibile includere anche il punteggio di rischio email LUCY, se richiesto.



- Mitigazione minacce:** il sistema di mitigazione minacce è un approccio rivoluzionario per eliminare i rischi delle email. Supporta l'amministratore di sicurezza in relazione al bloccare l'attacco (ad es. inviando un report automatico al gruppo di provider specifico coinvolto nell'attacco).



- **Analisi con regole personalizzate:** definisci le tue regole per analisi email e calcolo dei rischi.

Home / Phishing Incident Reports

Send Abuse Delete Delete All Settings Download Plugin

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	⚠ ⊗ ⊕ ✕

Score Factors

Custom Rules:

Domain Analysis:

Header Analysis:

SpamAssassin:

Save

New Rule

Name:

Reg. Exp.:

Score:

Save

Summary
Header Analysis
Domain Analysis
Body Analysis
Threat Indicators

		Score	Rule active?	
Reply-to Mismatch	different reply-to adress defined than the actual (more info...)	1.60	Active <input checked="" type="checkbox"/> Inactive <input type="checkbox"/>	⊞ ✕
New Domain	Domain has been reserved in the last 30 days (more info...)	20.00	Active <input checked="" type="checkbox"/> Inactive <input type="checkbox"/>	⊞ ✕
Link Display mismatch	link display name different from the actual link (more info...)	0.00	Active <input type="checkbox"/> Inactive <input checked="" type="checkbox"/>	⊞ ✕

- **Opzioni di personalizzazione plugin:** LUCY permette di personalizzare facilmente diverse funzioni e plugin (icone mostrate, messaggi di feedback, etichette, protocolli di trasmissione, intestazioni ecc.).

The screenshot displays the 'Phishing Incident Reports' interface. At the top, there is a table with columns: Time, Email, Client, Campaign, Score, Status, and Client. Below the table, a 'Settings' dropdown menu is open, showing options like 'Custom Rules', 'Score Factors', 'Abuse', 'Autoresponder', and 'Plugin Settings'. A blue arrow points from 'Plugin Settings' to a 'Settings' form below. The form contains various input fields for messages (e.g., 'No Selection Message', 'Eval Error Message', 'Send Error Message', 'Unsupported Message', 'Subject', 'Ribbon Label', 'ICO', 'User Request Message') and checkboxes for reporting preferences (e.g., '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'). A 'Save' button is at the bottom right. Below the settings form, another 'Phishing Incident Reports' table is shown, with a 'Download Plugin' dropdown menu open, listing options like 'Microsoft Outlook 32-bit', 'Microsoft Outlook 64-bit', 'Microsoft Outlook 365', and 'Gmail Addon'.

- **Integrazione di terze parti:** utilizzano l'automazione API REST incidenti LUCY, siamo in grado di elaborare email segnalate e aiutare il team di sicurezza a fermare attacchi di phishing in corso.

The screenshot shows the 'API Whitelist' interface. At the top, there are buttons for '+ New', 'Delete', and 'API Documentation'. Below, there is a table with columns for IP addresses and a delete icon. Two IP addresses are listed: 192.168.10.231 and 192.168.12.114. Below the table, there are three sections: 'Resources', 'Endpoint List', and another 'Endpoint List'. The 'Resources' section lists various entities like Language, Client, Scenario Template, Attachment Template, Awareness Template, Campaign, Scenario, Recipient Group, Recipient, Victim, and Incident. The 'Endpoint List' sections list various API endpoints such as /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, /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, and /api/incidents. At the bottom, there are three API endpoint cards: /api/incidents (GET), /api/incidents/:id (GET), and /api/incidents/:id (DELETE), each with a brief description of its function.

- Identificazione attacchi con schemi comuni:** applica i filtri della dashboard LUCY per rilevare vettori di attacco comuni nella tua società. Ricerca tra tutte le email segnalate indicatori di compromissione simili.

The screenshot displays the 'Incident Reports' dashboard. At the top, there are navigation links for 'Home / Phishing Incident Reports' and several action buttons: 'Send Abuse', 'Delete', 'Delete All', 'Settings', and 'Download Plugin'. Below this is a table of incident reports with columns for Time, Email, Rating, Client, Campaign, Score, and Status. A filter panel on the right allows users to refine results based on domain, reputation, and score.

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

Below the table, there is a pagination control and a 'rows per page' selector set to 10. A detailed view of a report for 'sarah@test.com' is shown on the right, featuring a 'Summary' tab, an 'Overall Risk Score' of 3.9 of 10.0, and fields for Message, Subject, Report Time, Status, and Notes.

- Profili di reputazione degli utenti sugli incidenti:** classifica gli utenti con un punteggio di reputazione incidenti.

This screenshot shows the 'Incident Reports' dashboard with a focus on the 'Rating' column. The table lists various incidents, and the 'Rating' column is highlighted with a red box. The filter panel on the right is also visible, showing options to filter by domain, reputation, and score.

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

- **Integrazione con attacchi simulati:** report illimitati e integrazioni dashboard per simulazioni di phishing: identifica gli utenti che si sono comportati meglio in una simulazione di phishing.

Campaign overview dashboard

Search...

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

Campaign details statistics

Total Stat

Category	Value
Sent	7
Opened	2
Clicks	2
Successful Attacks	2
Reported	1
Invalid Submits	0
Vulnerable Victims	0

Campaign recipient statistics

Name	E-mail	Phone	User History	Scenario Total Time	Downloaded Files	OS	Browser	IP
test	oliver@muenchow.ch	-	-	13.934	-	-	-	-
test	-	-	-	7.421	-	-	-	-
test	-	-	-	6.513	-	-	-	-

Success Rate: 4.16%
Click Rate: 8.33%
Clicks: -
Successful Attack: -
Trained: -
Out Of Office: -
Bounced: -
Responded: -

- **Installazione facile:** installa il plugin per incidenti di phishing su Outlook, Gmail e Office365.

Phishing Incident Reports

Send Abuse Delete Delete All Settings Download Plugin

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

Filter: Microsoft Outlook 32-bit, Microsoft Outlook 64-bit, Microsoft Outlook 365, Gmail Addon

Client: All

Microsoft Outlook 64-bit setup (1).msi

Client: Lucy Test, All, Tenant3, Tenant4, Lucy Test, Test Client A, Client Inc USA

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.

Back Next Cancel