



LIVRO BRANCO DO LUCY



O QUE É O LUCY?

Teste, forme e envolva os seus funcionários

O LUCY permite que as organizações desempenhem o papel de um atacante e revelem fragilidades existentes, tanto na infraestrutura técnica como nos conhecimentos da equipa, eliminando-as por meio de programas abrangentes de elearning.



TESTE DOS FUNCIONÁRIOS

Simulações de Ataque (por exemplo, phishing)



TESTE DA INFRAESTRUTURA

Simulação de Scanner de Malware



FORMAÇÃO DOS FUNCIONÁRIOS

SGA Integrado



MEDIÇÃO DO PROGRESSO

Análise do Risco e da Aprendizagem



INTEGRAÇÃO DOS FUNCIONÁRIOS

Sistema de Denúncia (por exemplo, Botão de e-mail com Phishing)



CARACTERÍSTICAS GERAIS

- LEMBRETES:** Podem utilizar-se modelos de lembretes para reenviar mensagens automaticamente para utilizadores que não tenham clicado num link de ataque ou para realizar um curso de formação após um período de tempo personalizado.

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]

[Rich Text Editor Icons]

Styles - Normal - Arial - Size - [Font Size Icons]

Insert Var - Upload File or Image

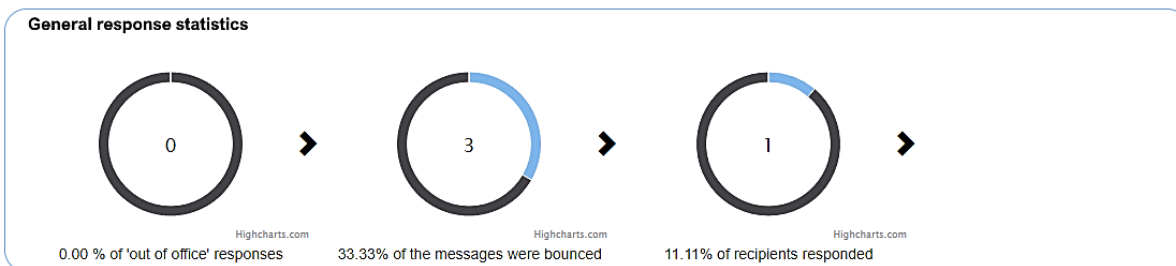
Dear %name%,

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](#)

- DETEÇÃO DE RESPOSTA:** A deteção automática de resposta permite definir e analisar respostas automáticas por e-mail (por exemplo, fora do escritório), bem como erros de entrega de e-mail (por exemplo, utilizador desconhecido) dentro da campanha.



User specific response statistics

No test

| | |
|------------------------------|----------------------------------|
| Name | No |
| E-mail | doestexist@doesnt-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

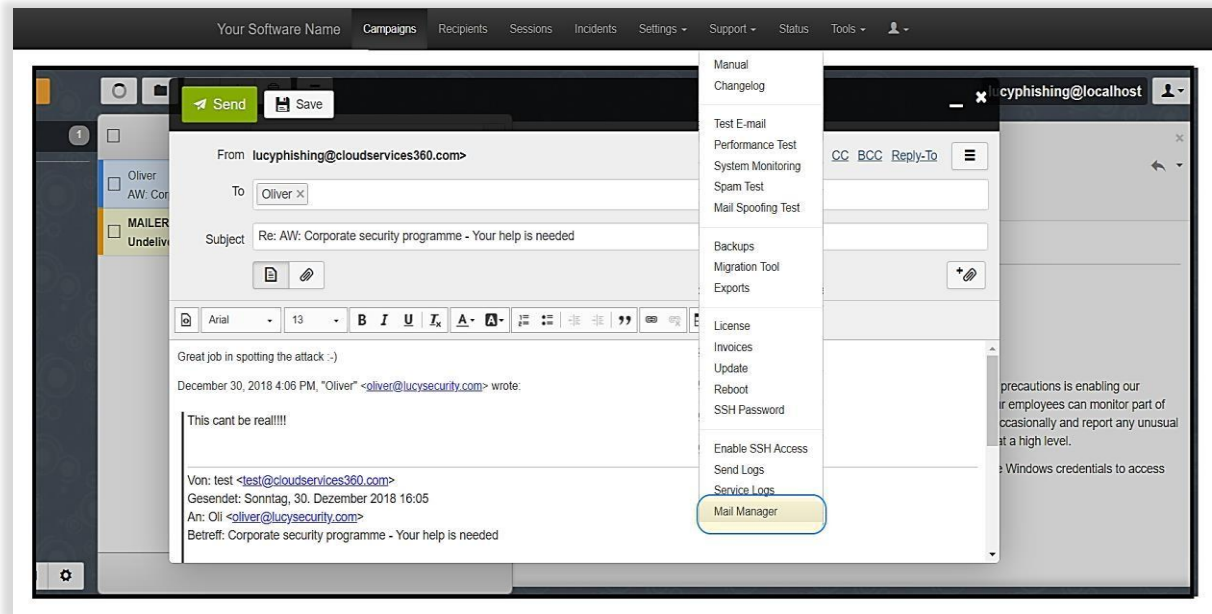
Out Of Office Delay

Out Of Office Pattern

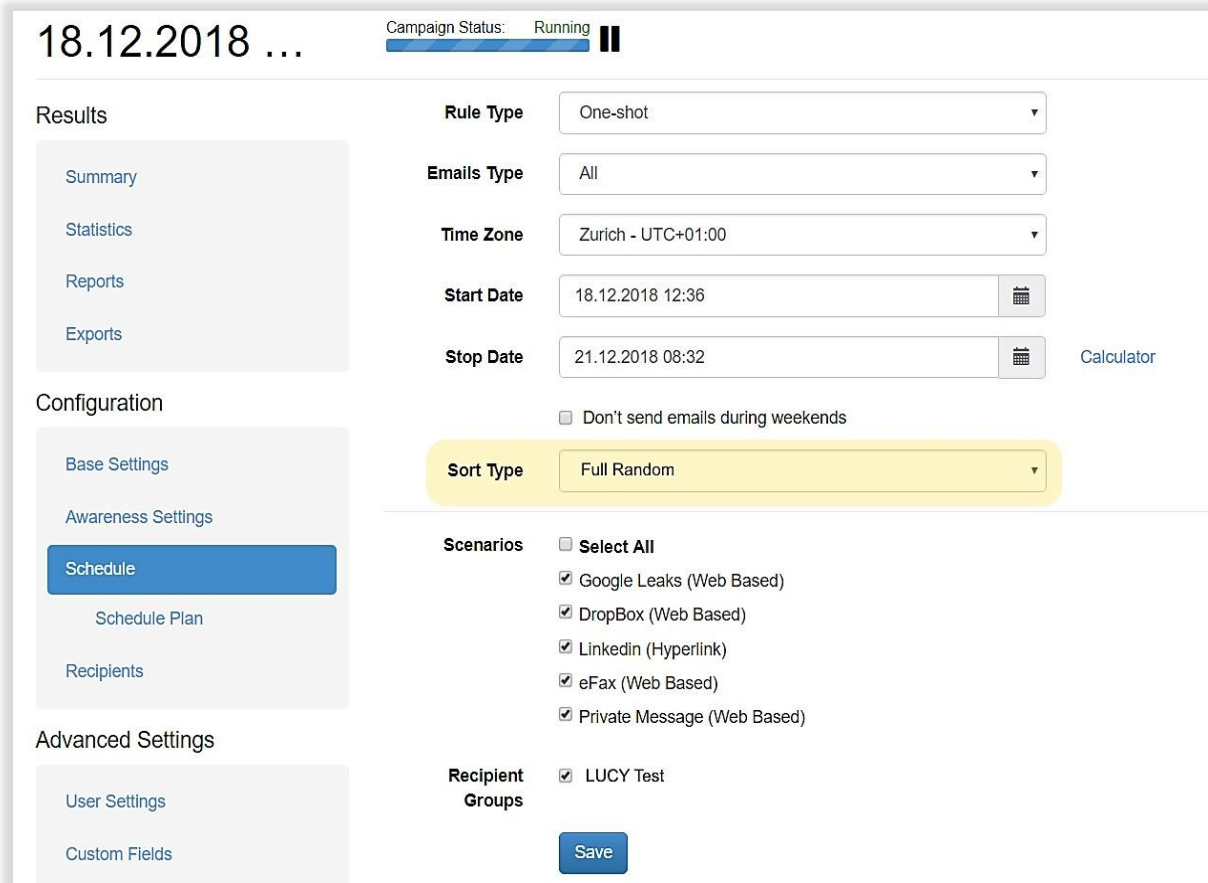
Bounced Pattern

[Save](#)

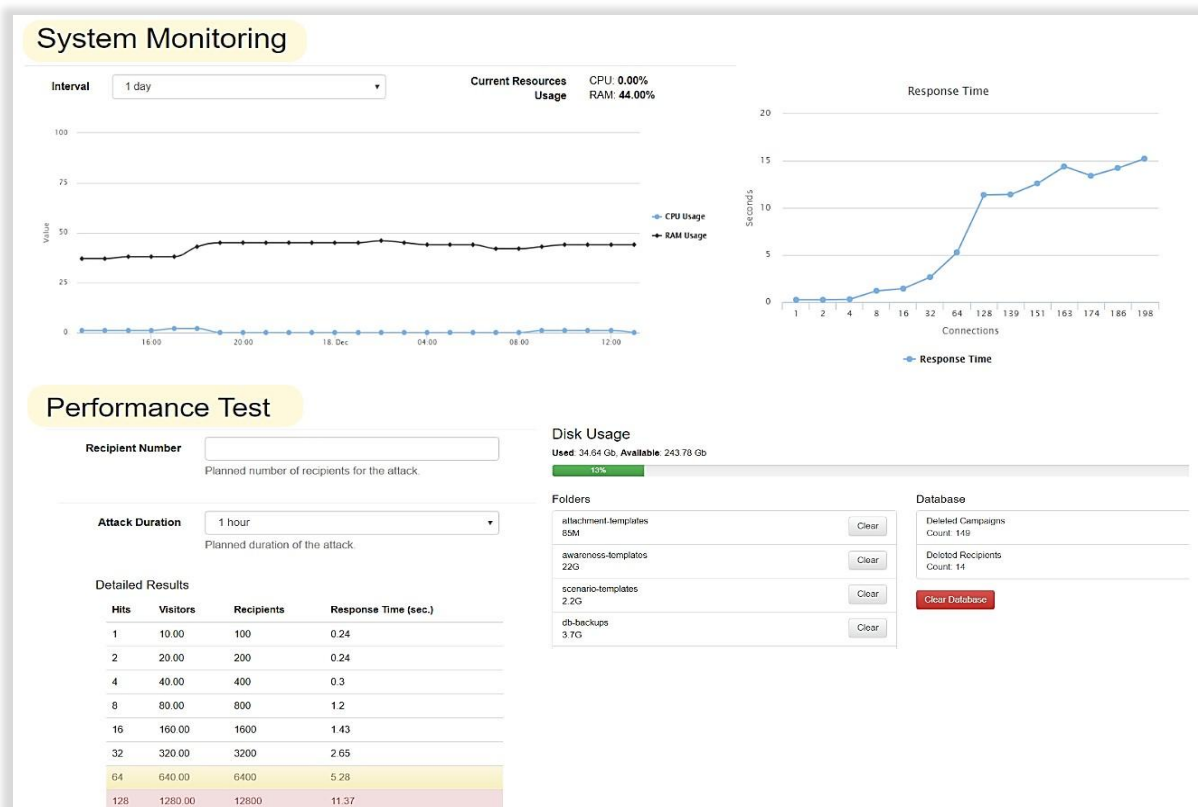
- CLIENTE DE COMUNICAÇÃO INTEGRAL:** Uma plataforma de mensagens incorporada permite que o administrador do LUCY comunique interativamente com os destinatários dentro ou fora das campanhas LUCY. Todos os e-mails são arquivados e podem ser avaliados.



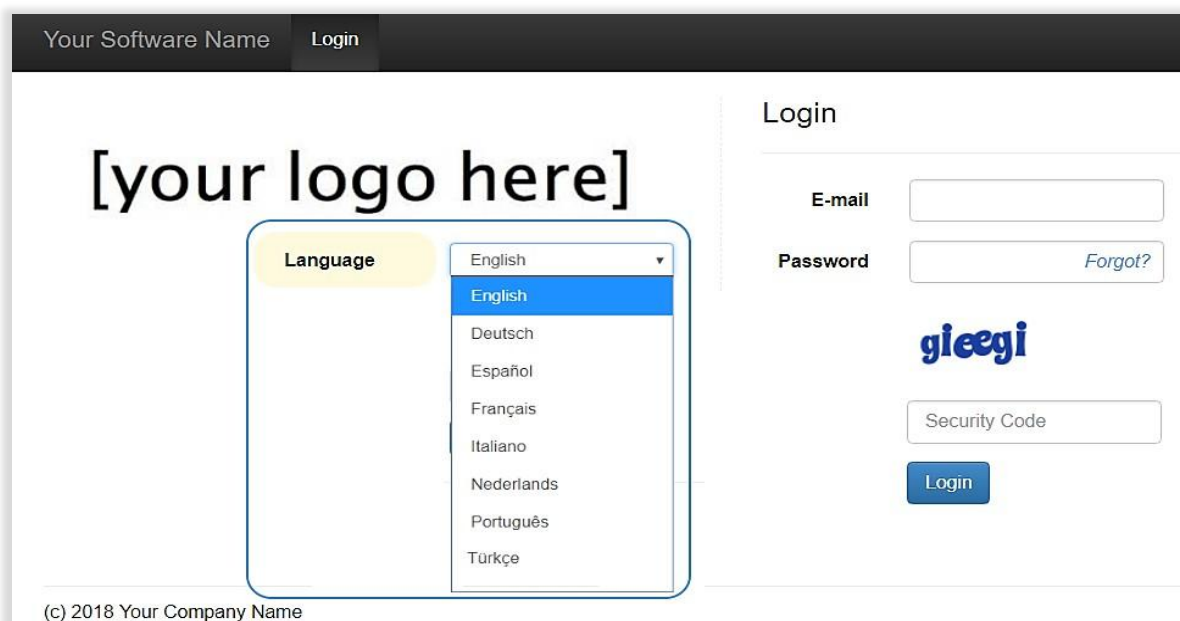
- Aleatorização do agendamento:** Aumentar a consciencialização dos colaboradores aleatoriamente é o fator chave para a consciencialização efetiva e sustentável dentro da organização. O envio aleatório de muitas campanhas em simultâneo é um dos melhores meios de formação dos colaboradores.



- Ferramentas de desempenho:** as rotinas inteligentes do LUCY adaptam a instalação do servidor aos recursos indicados. O servidor de aplicações, o dimensionamento de SGBD, as utilizações da memória e do CPU são calculados durante a instalação ou durante as operações. Pode escalar uma única instalação LUCY baseada na nuvem para mais de 400 000 utilizadores.



- Interface de administração multilingue** A interface de administração LUCY está disponível em diferentes idiomas e pode ser traduzida noutras línguas mediante pedido.



- Certificado (SSL):** Permite a criação automática de certificados oficiais e fiáveis para a administração, backend e para as campanhas. O LUCY irá usar automaticamente o domínio configurado no sistema para gerar o certificado. Se decidir usar SSL para a campanha, pode gerar um certificado personalizado ou uma RAS (Requisição de Assinatura de Certificado). Também pode importar certificados oficiais de confiança.

The screenshot displays the 'SSL Settings' configuration page. At the top, a green notification box states 'Certificate has been successfully created.' The main content area includes a sidebar with navigation options like 'Summary', 'Scenario Settings', and 'SSL Settings'. The main settings include:

- Use Custom SSL Certificate
- SSL Provider: Let's Encrypt
- Enable Domain Checking
- Domain: office.cloudspace365.solutions

 Two modal windows are overlaid:

- Generale CSR or Certificate:** A form for generating a CSR or certificate with fields for Domain, E-Mail, Country, State, City, Organization Name, and Organization Unit. It has 'Generate CSR', 'Generate Certificate', and 'Cancel' buttons.
- SSL Provider:** A form for uploading a custom certificate with fields for SSL Certificate, SSL Key, SSL Key Password, and SSL Chain, each with a 'Choose File' button. It has a 'Save' button.

- Controlos de acesso baseados em funções:** O LUCY oferece um controlo de acesso baseado nas funções (RBAC), que restringe o acesso ao sistema apenas aos utilizadores autorizados. As permissões para realizar certas operações são atribuídas a funções específicas, no âmbito das configuração do utilizador. São atribuídas funções específicas aos membros ou funcionários (ou a outros utilizadores do sistema), através das quais adquirem as permissões de computador necessárias para desempenhar determinadas funções LUCY.

The screenshot shows the 'User Settings' page for a campaign named 'TEST'. It features a table of users and a detailed permissions configuration for a selected user.

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

 Below the table, the permissions for the selected user are shown:

- 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

- Grupos de utilizadores multicamada:** Faz rapidamente o upload em massa de ficheiros CSV, LDAP ou de texto. Cria grupos diferentes, organizados por departamento, divisão, título, etc. Atualiza os utilizadores numa campanha em execução. Cria grupos de utilizadores dinâmicos com base nos resultados da campanha de phishing.

- Compatível com multiciente:** "Clientes" pode referir-se a diferentes empresas, departamentos ou grupos que tenham uma campanha associada com o LUCY. Estes clientes podem ser utilizados, por exemplo, para permitir o acesso específico à campanha ou para criar análises específicas para o cliente.

- Modelos de campanha:** No caso de querer reutilizar campanhas semelhantes, pode guardar uma campanha completa com modelos de ataque e conteúdo de elearning como modelo de campanha. Esta funcionalidade permite-lhe evitar ter de repetir configurações semelhantes repetidamente.

The screenshot shows the 'Max1' campaign page. At the top, there are buttons for 'Reset Stats', 'Report', 'Save as Template' (highlighted with a red box), 'Export', and 'Start'. Below this is a table with columns 'Campaign', 'Running Time', and 'Created By'. The 'Max1' campaign is listed with a running time of '4 days, 4 hours' and 'Created By' as 'N/A'. On the left, there is a sidebar with 'Results' (Summary, Statistics, Reports, Exports) and 'Configuration' (Base Settings, Awareness, Schedule, Recipients, Advanced Settings, User Settings). A 'New Campaign' modal is open, showing fields for 'Name' (Standard Test & Train Campaign Template), 'Client' (Lucy Test), 'Setup Mode' (Start with Default Campaign Template), and 'Template' (Max1). A 'Save' button is visible. On the right, there is a donut chart showing 'Attacks are successful' at 100.00%, and a progress bar for 'Training Sent' (33.33%), 'Training Opened' (33.33%), and 'Training Score (%)' (0.00%).

- Assistente de configuração com orientação baseada no risco:** O LUCY disponibiliza várias ferramentas de configuração. Crie uma campanha completa em menos de 3 minutos usando os modelos predefinidos da campanha ou deixe o assistente de configuração guiá-lo no processo de configuração. Opcionalmente, está disponível um modo de configuração baseado no risco, que faz sugestões específicas para a seleção de modelos de ataque e consciencialização, com base na dimensão e setor da empresa.

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.

- **Verificações de campanha:** Verificações preliminares antes de iniciar uma campanha LUCY: verificação de entrega de e-mail, verificação de registo MX, verificação de agendamento, verificação de spam e outros.

Home / Campaigns / Login & Malware Simulation / Checks

Campaign Status: Not Started ▶ Skip Checks

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.

Help Close

- **Fluxo de trabalho de aprovação:** uma determinada campanha pode ser enviada a um supervisor no LUCY para aprovação.

Results Completed — Campaign Status: Waiting ▶

Summary

- Summary
- Statistics
- Reports
- Exports

Configuration

- Base Settings
- Awareness Settings
- Schedule
- Recipients

Advanced Settings

- User Settings
- Custom Fields
- Reminders

Logs

- Supervision Log

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 📅

Severity

- Minor Recommendations
- Serious Recommendations
- Heavy Recommendations

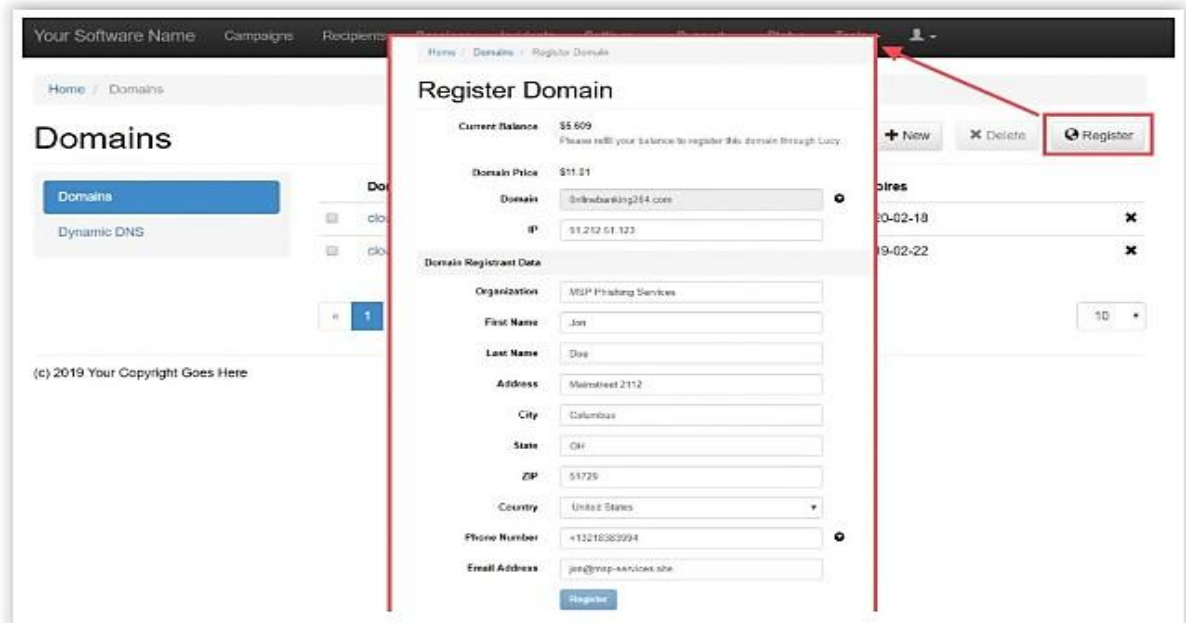
Comments

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

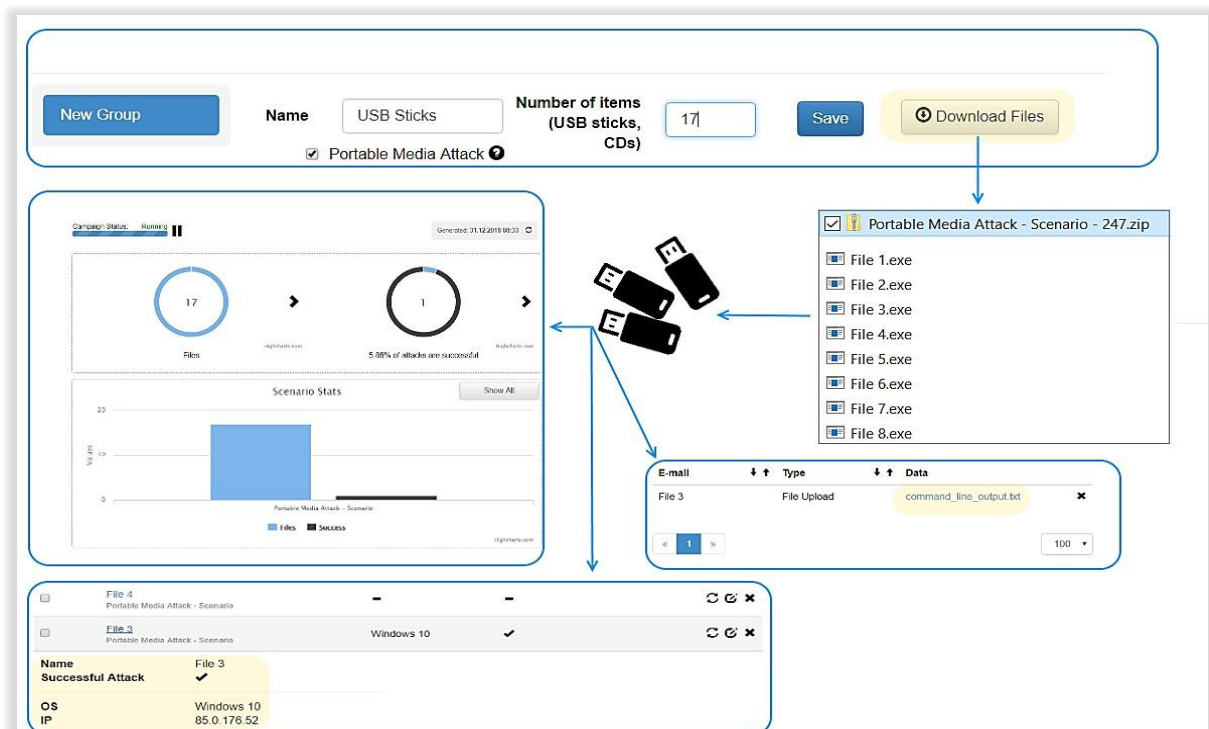
| Name | Role | All Campaigns Access |
|--------------|-------------------------|----------------------|
| Limited User | User | ✓ |
| View | View | — |
| Supervisor | Supervisor | ✓ |

- API de DNS:** A API de DNS permite ao administrador criar qualquer domínio no LUCY em segundos. Dado que os atacantes usam muitas vezes grafias semelhantes ao domínio de um cliente (chamado Typosquatting), este risco também pode ser apresentado no LUCY. Se o domínio original do cliente é, por exemplo, "onlinebanking.com", o assistente DNS pode ser usado para reservar domínios como "0nlinebanking.com", "onl1nebanking.com" ou "onlinebanking.services" e atribuí-lo a uma campanha posteriormente. Depois, o LUCY cria automaticamente as entradas DNS correspondentes (MX, SPF, proteção Whois, etc.) para o IP onde o LUCY está instalado. Claro que o administrador também pode usar os próprios domínios do seu provedor no LUCY.



SIMULAÇÃO DE ATAQUE

- Ataques de média portátil:** Os hackers podem usar unidades de média portáteis para obter acesso a informações sensíveis armazenadas num computador ou rede. O LUCY oferece a opção de executar ataques de média portátil em que um modelo de ficheiro (por exemplo, executável, arquivo, documento do office com macros, etc.) pode ser armazenado num dispositivo de média portátil, tal como USB, cartão SD ou CD. A ativação (execução) destes ficheiros individuais pode ser rastreada no LUCY.



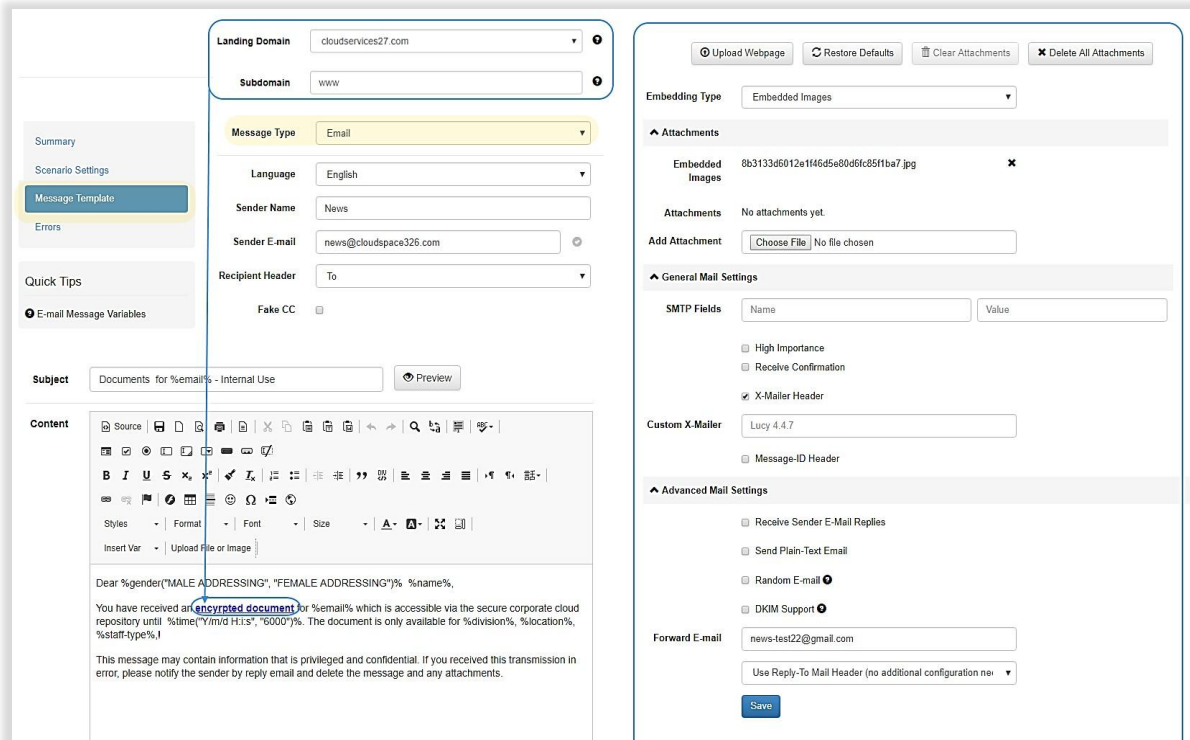
- SMiShing:** O smishing é, em certo sentido, "phishing por SMS." Quando os cibercriminosos fazem um "phish", enviam e-mails fraudulentos que procuram enganar o destinatário, para que este abra um anexo carregado de malware ou clique num link malicioso. O smishing usa simplesmente mensagens de texto, em vez de e-mail.

The screenshot shows the 'Message Template' configuration page in the Lucy web editor. The 'Message Type' is set to 'Sms'. The current workstation balance is 17.920 USD. The message text is 'Check out this link here: %link%'. The sender name is 004550566166. The template is 'Access to online surveillance portal / English'. The landing domain is 'cloudspace365.solutions' and the subdomain is 'sms'. The URL shortener is 'goo.gl'. The login regexp is 'lw.*lw' and the password regexp is empty. A 'Save' button is at the bottom.

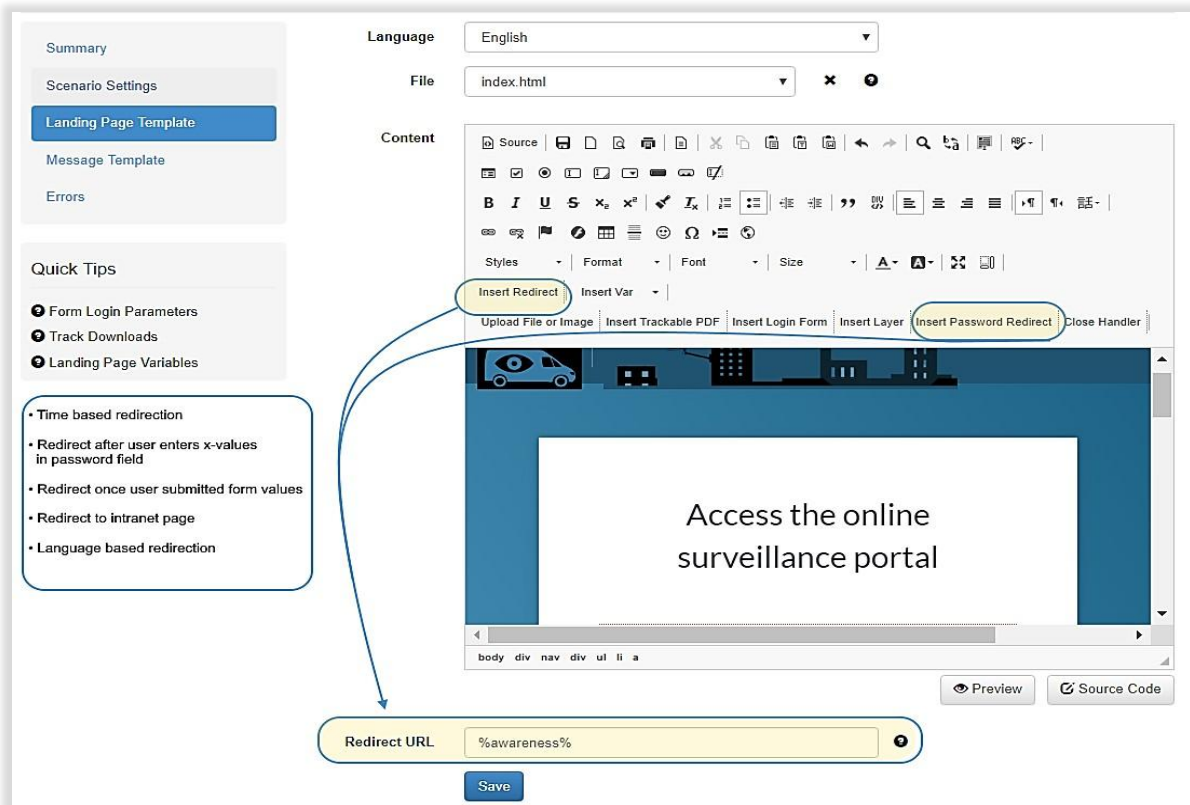
- Ataques de introdução de dados:** Os ataques de introdução de dados podem incluir uma ou mais páginas web que interceptam a entrada de informações sensíveis. As páginas web disponíveis podem ser facilmente personalizadas com um editor web do LUCY. Ferramentas adicionais de edição permitem configurar rapidamente funções como formulários de log-in, áreas de download, etc., sem conhecimentos de HTML.

The screenshot shows the 'Landing Page Variables' configuration page in the Lucy web editor. The 'Language' is set to 'English'. The 'File' is 'index.html'. The 'Content' area shows a preview of the login form. The 'Insert Login Form' dialog box is open, showing the 'Login Form #3' with 'Login' and 'Password' fields. The preview shows a 'Microsoft 366 Account' login form with 'Email or phone' and 'Password' fields. A 'Preview' button is at the bottom right.

- **Ataques com hiperligações:** Uma campanha baseada em hiperligações enviará aos utilizadores um e-mail que contém um URL de rastreamento aleatório.



- **Ferramenta poderosa de redirecionamento de URL:** As funções de redirecionamento flexíveis do LUCY permitem que o utilizador seja guiado, no momento certo, para as áreas desejadas de simulação de ataque ou formação. Por exemplo, depois de inserir os 3 caracteres de uma palavra-passe numa simulação de phishing, o utilizador pode ser redirecionado para uma página de formação especial sobre a proteção com palavra-passe.



- **Ataques mistos:** Os ataques mistos permitem uma combinação de vários tipos de cenário (baseado em ficheiros, introdução de dados, etc.) na mesma campanha.

The diagram illustrates a multi-stage attack simulation. It consists of three main components:

- Office 365 Registration Page:** A legitimate-looking registration page for Office 365. It includes a header with the Office 365 logo, a greeting "Hello John Dee! Welcome to our Office 365 Registration Page. Please use your Windows credentials to register for the online access.", and a sign-in form with fields for "Username" and "Password". There is a "Sign in" button and a "Keep me signed in" checkbox. At the bottom, it says "© 2018 Microsoft" and "Terms of use Privacy & Cookies".
- Installation Error Dialog:** A Windows-style error dialog box titled "Installation Error - something went wrong". The message reads: "We couldn't start your program. We kindly ask you to download and execute our system configuration tool below to prepare your access." Below the message is a prominent orange "DOWNLOAD" button with a download icon. A "Close" button is in the bottom right corner.
- Malware Simulation Configuration:** A configuration interface for a malware simulation. It has a "Template" dropdown set to "Console Post". The "Description" field contains: "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." Under "Variables", there are three rows: "Commands" with the value "ipconfig,whoami", "Display GUI (0-4)" with the value "1", and "Text Message" with the value "Installation Error - please try again later". A "Save" button is at the bottom.

Blue arrows indicate the flow of the attack: from the registration page to the error dialog, and from the error dialog to the simulation configuration.

- Ataques baseados em ficheiros:** Ataques baseados em ficheiros permitem ao administrador LUCY integrar diferentes tipos de ficheiros (documentos do office com macros, PDFs, executáveis, MP3s, etc.) em anexos de e-mail ou sites gerados no LUCY e medir a sua taxa de download ou execução.

The screenshot illustrates the LUCY web editor interface for inserting a Trojan simulation. It is divided into three main sections:

- Insert Trojan Simulation Dialog:** A modal window with a title bar and close button. It contains:
 - Select Trojan Type:** A dropdown menu set to "Console Interactive".
 - Select Design:** A dropdown menu set to "Button #1".
 - Design Preview:** A large circular icon containing a downward-pointing arrow.
 - OK Button:** A green button at the bottom right.
- Preview Area:** A central window showing a simulated message. The message text reads:


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

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

 Below the message is a blue button labeled "DOWNLOAD". The background of the message is a blue-to-green gradient with a white cloud icon.
- TROJAN SIMULATION: SETTINGS Panel:** A configuration panel located at the bottom right. It includes:
 - Template:** A dropdown menu set to "Console Post".
 - Description:** The text "Get output from one or multiple console programs."
 - Variables:** Three blue buttons with corresponding input fields:
 - Commands:** Input field containing "ipconfig,whoami".
 - Display Error:** Input field with a checked checkbox.
 - Error Message:** Input field containing "VPN Client Error X1201".
 - Save Button:** A blue button at the bottom.

Arrows in the image indicate the flow of configuration: from the "Insert Trojan Simulation" dialog to the "TROJAN SIMULATION: SETTINGS" panel, and from the "TROJAN SIMULATION: SETTINGS" panel to the "Preview" area.

- Ataques de cano duplo:** Esta funcionalidade possibilita o envio de vários e-mails de phishing em cada campanha, em que o primeiro e-mail benigno (o isco) não contém nada malicioso e não exige uma resposta do destinatário.

The screenshot shows the 'Lure Template' configuration page in the LUCY interface. The left sidebar contains navigation options: Summary, Scenario Settings, Landing Page Template, Message Template, Lure Template (selected), and Errors. Below this is a 'Quick Tips' section with 'E-mail Message Variables'. The main content area is divided into several sections:

- 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,

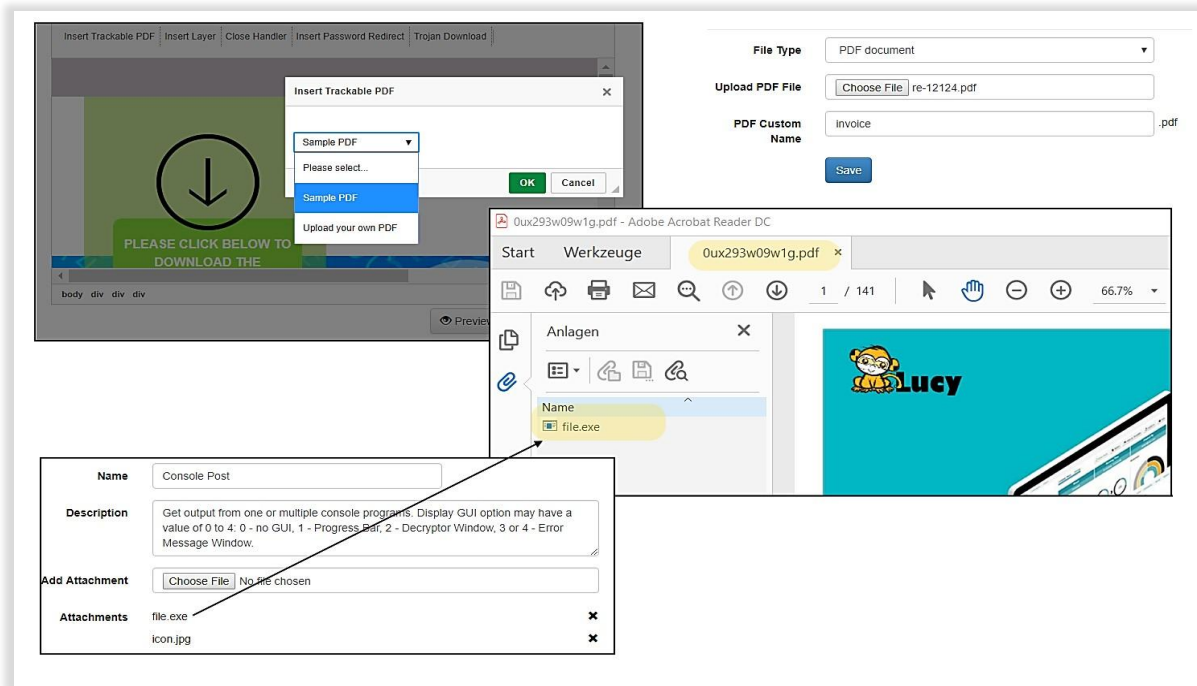
IT-Department
- Success Action:** Data Submit
- Collect Data:** Partial
- Double Barrel Attack
- Lure Delay:** 3600
- Uri Shortener:** bit.ly
- Login Regexp:** \w.*\w (with an 'Insert' button)
- Password Regexp:** (with an 'Insert' button)
- Save** button at the bottom.

- Ataques baseados em Java:** Ataques baseados em Java permitem que o administrador LUCY integre um applet fiável dentro dos modelos de ataque baseados em ficheiros ou mistos fornecidos pelo LUCY e meça a sua execução pelo utilizador.

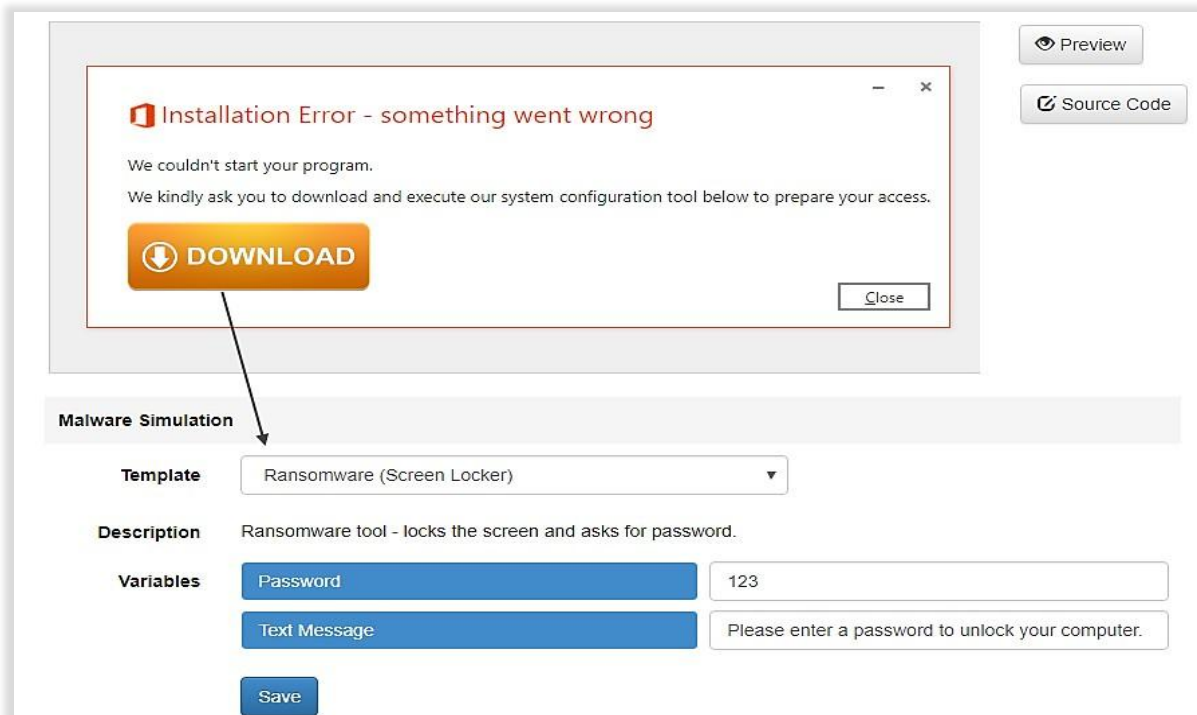
The screenshot shows two configuration panels in the LUCY interface:

- Java Applet Configuration:**
 - File Type:** Java Applet
 - Use a signed applet to execute a set of commands.
 - Checklist of actions:
 - System Details
 - Logged Users
 - Screen Capture
 - Network Details
 - System Hosts
 - App List
 - Save** button.
- Tunnel Executable Configuration:**
 - File Type:** Tunnel Executable
 - Use a signed applet to download and run an executable malware simulation.
 - Download Path:** %TEMP%
 - Save** button.
- Malware Simulation Configuration:**
 - 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.

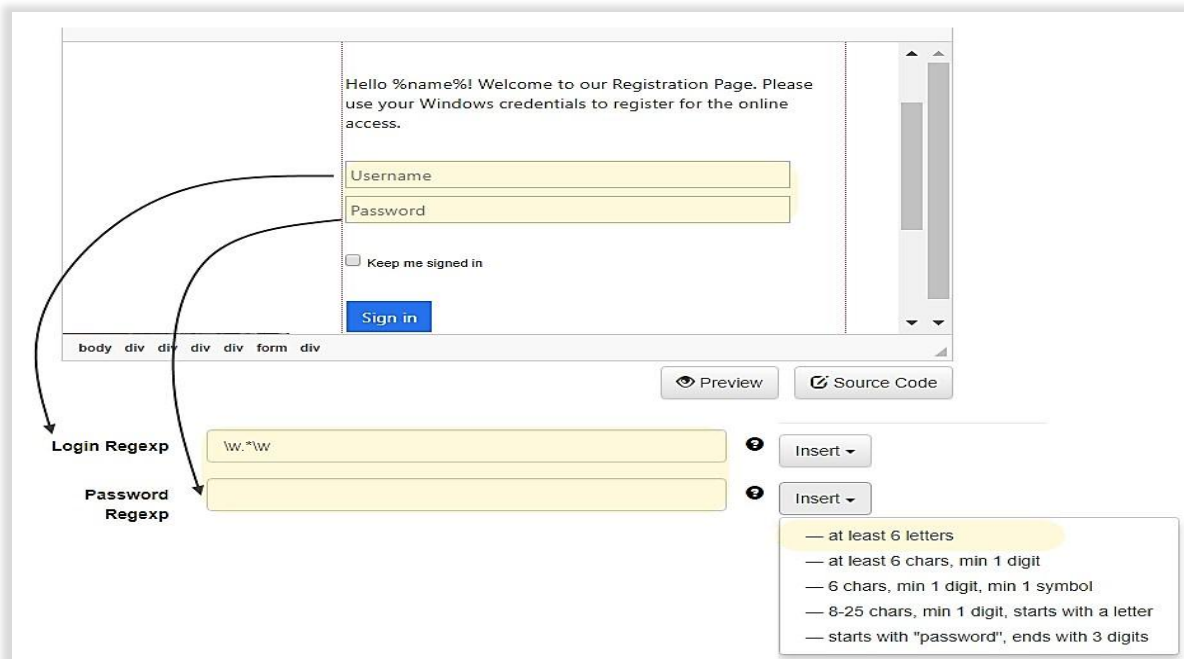
- Ataques baseados em PDF:** Os ataques de phishing baseados em PDF podem ser simulados com este módulo. O LUCY permite "esconder" ficheiros executáveis como anexos PDF e medir a sua execução. Além disso, também podem ser geradas ligações dinâmicas de phishing dentro dos PDFs.



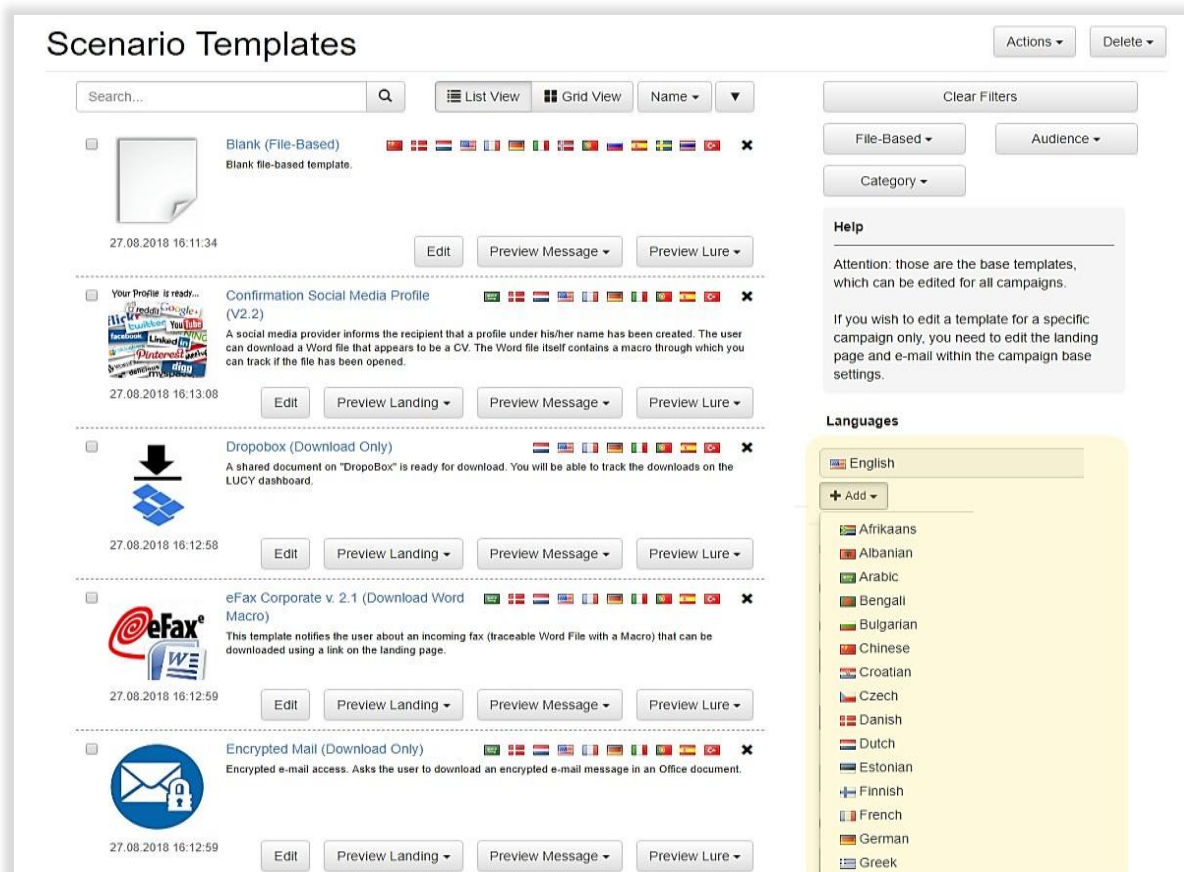
- Ataques de simulação de ransomware:** O LUCY tem duas simulações diferentes de ransomware, uma das quais testa a equipa, e a outra, a infraestrutura.



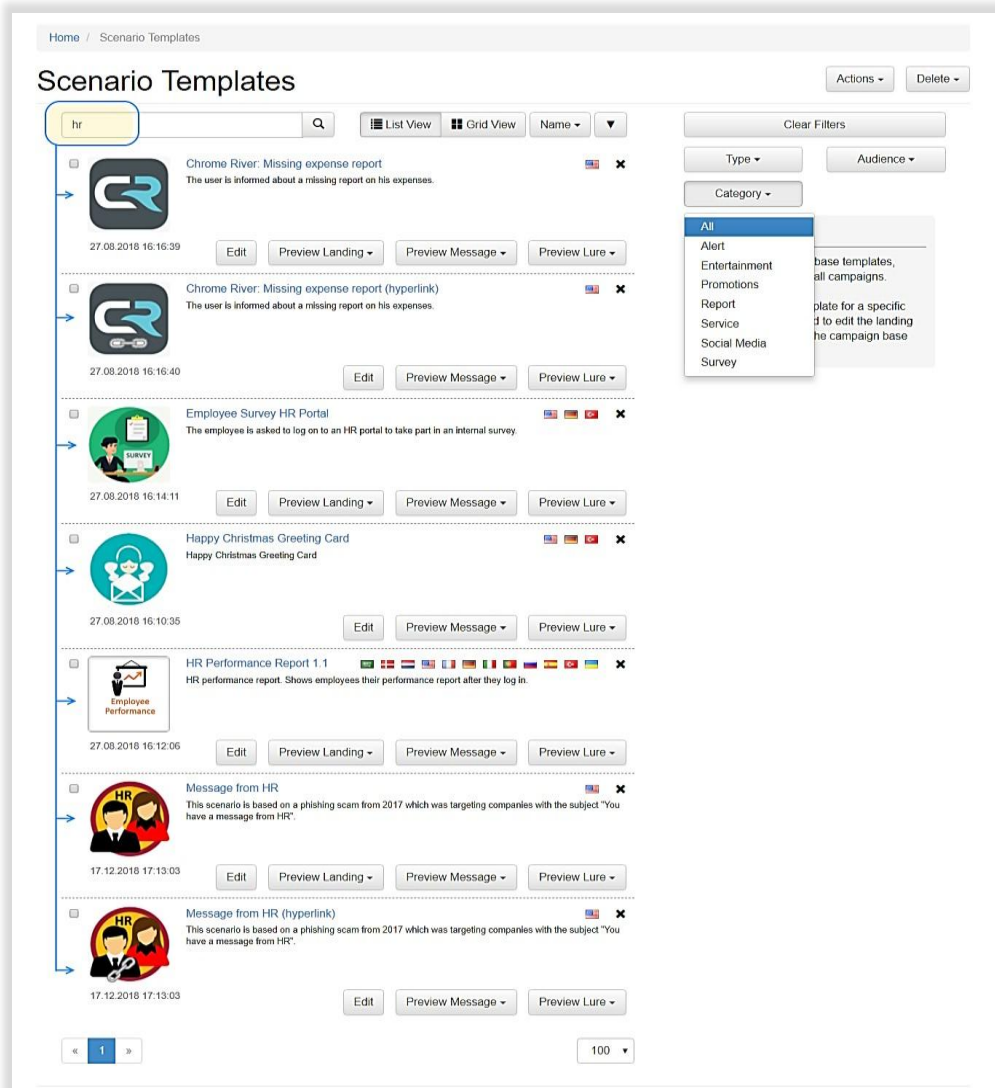
- Ferramenta de validação de introdução de dados:** Em simulações de phishing, os falsos positivos devem ser evitados para os campos de login (por exemplo, acessos com sintaxe inválida). As diretrizes da empresa também podem proibir a transmissão de dados sensíveis, como palavras-passe. Para este fim, o LUCY fornece um motor flexível de filtragem de entrada que oferece uma solução adequada para cada requisito.



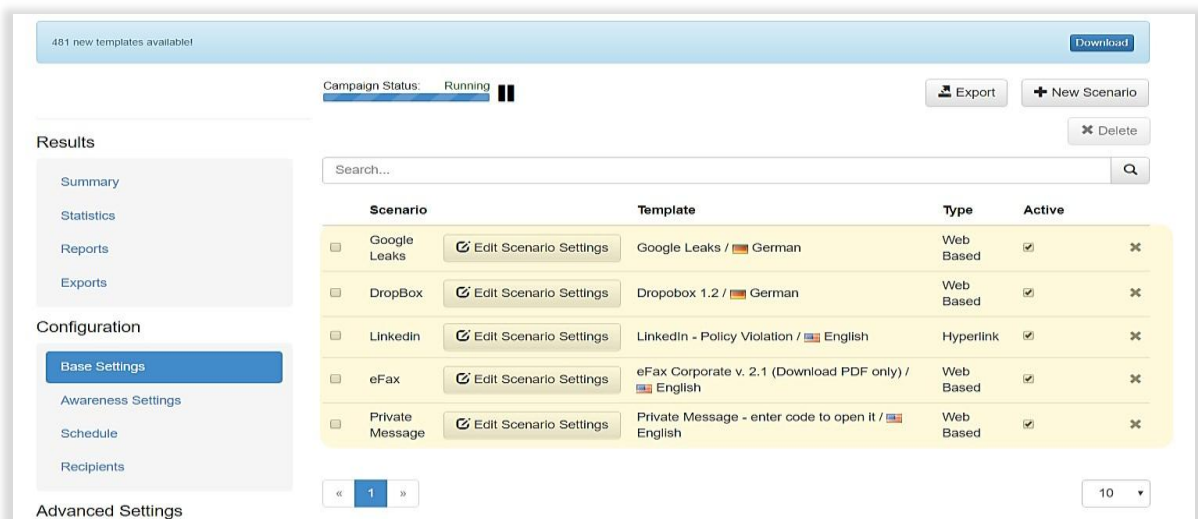
- Biblioteca de modelos de ataque multilingue:** O LUCY vem com centenas de modelos de ataque predefinidos em mais de 30 idiomas nas categorias de introdução de dados (modelos com um site), baseados em ficheiros (e-mails ou sites com um download de ficheiro), hiperligação (e-mails com um link), mistos (combinação de introdução e download de dados), e média portátil.



- Modelos específicos de setor e divisão:** Estão disponíveis modelos de ataque para setores ou divisões específicas.



- Utilização simultânea de modelos de ataque:** O LUCY dá-lhe a opção de usar vários modelos de ataque simulados numa única campanha. Misture os diferentes tipos (hiperligação, baseado em ficheiros, etc.) com diferentes temas de ataque para alcançar a maior cobertura de risco possível e uma melhor compreensão das vulnerabilidades dos funcionários. Em combinação com o nosso gerador aleatório de agendamento, podem ser executados padrões complexos de ataque durante um longo período de tempo.



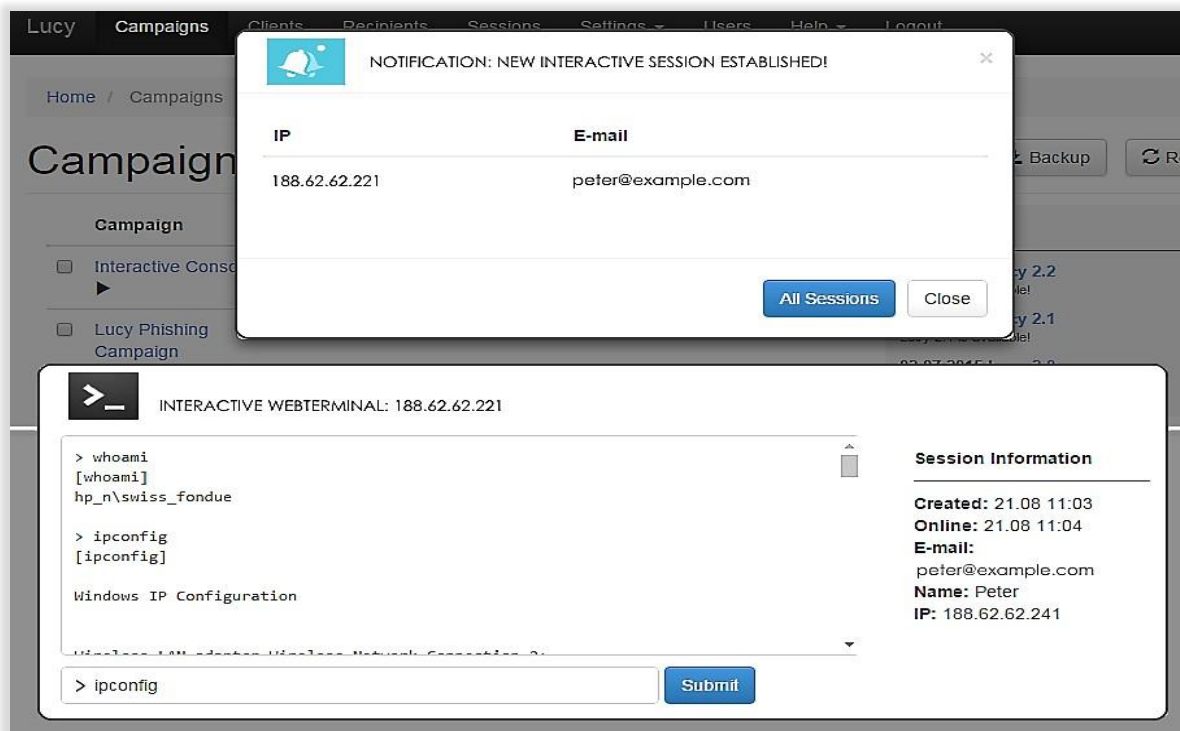
- Variações de URL de ataque:** Assuma o controle dos URLs gerados para identificar os destinatários. Use strings de URL curtas (< 5 caracteres) ou longas automatizadas ou defina URLs individuais para cada utilizador. A criação manual de URL permite-lhe formar links que um utilizador pode memorizar facilmente. Nos ambientes em que os cliques no link são desativados nos emails, isso é obrigatório.

The screenshot displays the 'LINK TEST' configuration page. On the left, a form allows setting recipient details: E-mail (test@example.com), Name (Test User), Location (USA), Division (Marketing), and a custom Link (marketing-usa-1). On the right, a simulated email is shown with the subject 'Affordable car leasing for our employees' and a body containing a link to the custom URL. A yellow box highlights the link in the email body, with an arrow pointing to the 'Link' field in the form.

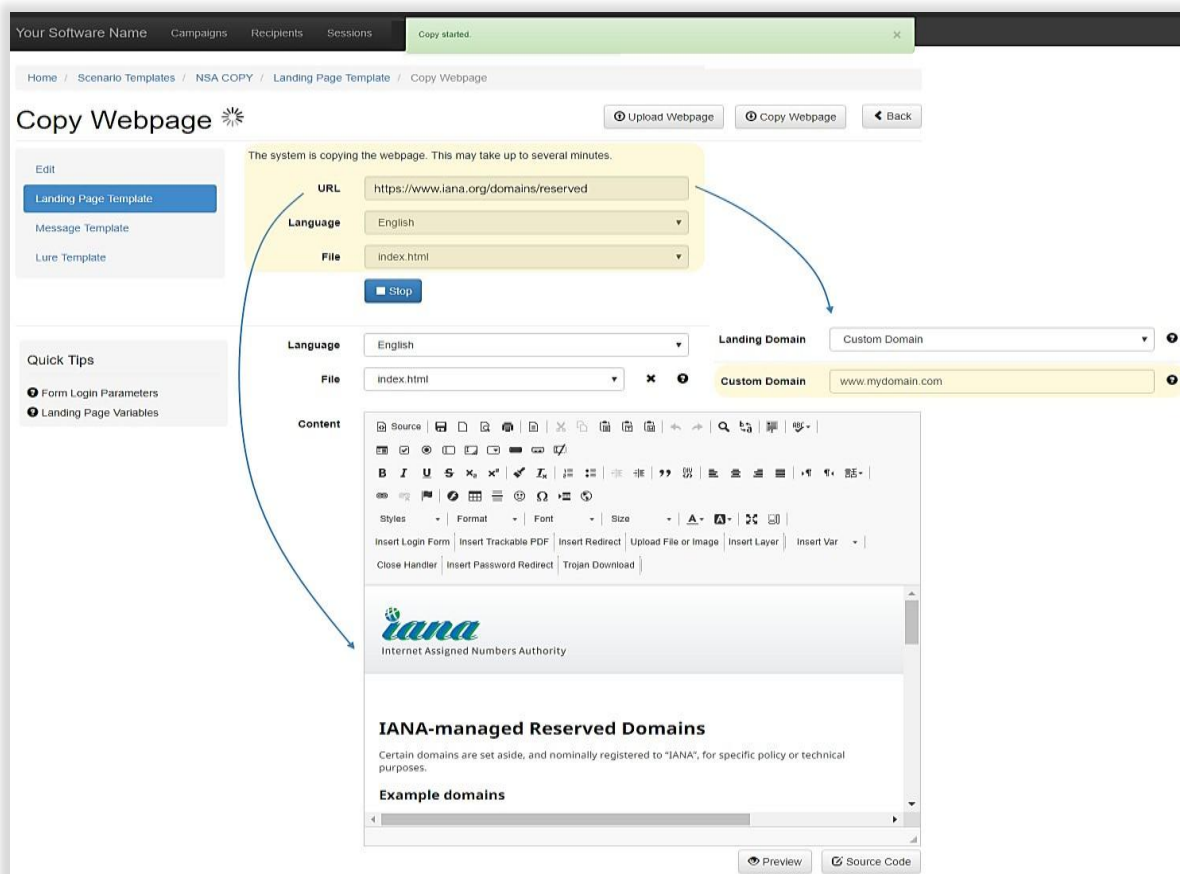
- Encurtamento de URL:** O encurtamento de URL é um serviço de Internet relativamente novo. Como muitos serviços sociais online impõem limitações de caracteres (por exemplo, o Twitter), estes URLs são muito práticos. No entanto, o encurtamento de URL pode ser usado por cibercriminosos para esconder o alvo real de um link, tal como phishing ou site infetados. Por esta razão, o LUCY oferece a possibilidade de integrar diferentes serviços de encurtamento dentro de uma campanha de phishing ou smishing.

The screenshot shows the URL shortening configuration page. Fields include: Landing Domain (cloudspace365.solutions), Subdomain (sms), Url Shortener (N/A), Sender Name (004550776160), and Text (Check out this here %link%). A blue bracket groups the Landing Domain and Subdomain fields. To the right, a smartphone icon displays a speech bubble with the text 'Check out this link here: goo.gl/KuraFG', illustrating the use of a URL shortener.

- Kit pentest:** O kit pentest é um sub-módulo da ferramenta de simulação de malware e dá-se pelo nome de "Sessões Interativas." Ele permite-lhe comunicar interativamente com um PC cliente que esteja atrás de firewalls, usando conexões http/s inversas.



- Clonador de site:** Crie rapidamente páginas de destino altamente profissionais para as suas campanhas. Clone sites existentes e adicione camadas adicionais com campos de introdução de dados, ficheiros para download e muito mais.



- Ataques baseados em nível:** A formação de phishing baseado em nível para funcionários serve para tornar o risco de hacking social mensurável. A análise científica também deve identificar os fatores de risco mais importantes para que o conteúdo da formação individual possa ser disponibilizado automaticamente.

- Simulação de spear phishing:** O Spear Phish Tailoring trabalha com variáveis dinâmicas (sexo, hora, nome, email, links, mensagens, divisão, país, etc.) que pode usar nos modelos de destino e mensagem.

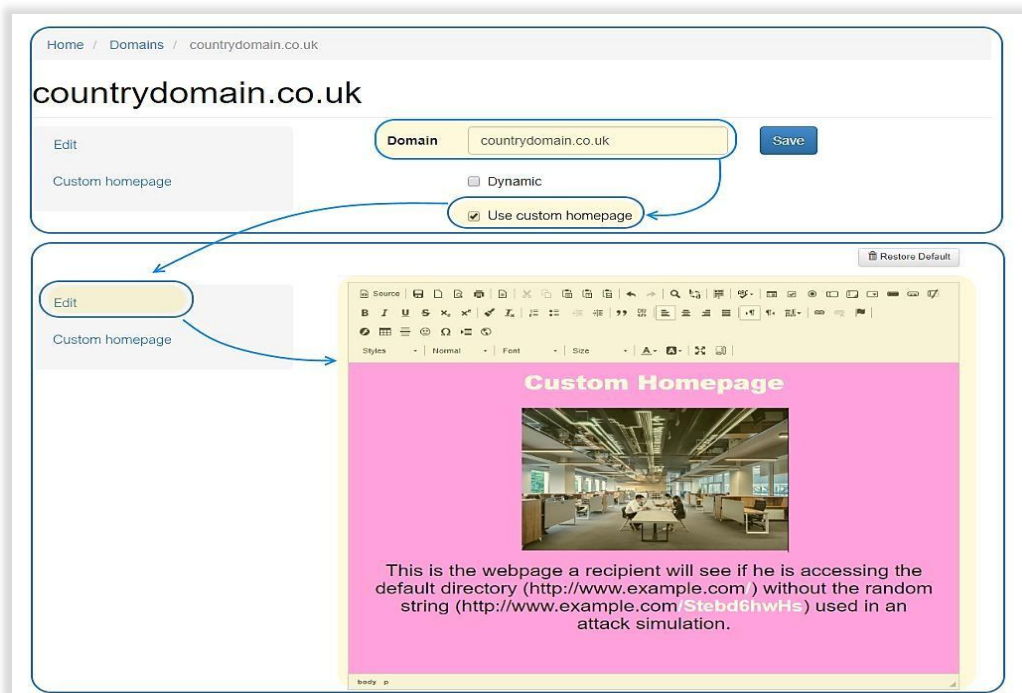
- Suporte DKIM / S / MIME para e-mails de Phishing:** Assinaturas digitais para e-mails: enviar mensagens de simulação de phishing assinadas (s/mime). Use o DKIM para obter uma melhor pontuação de remetente.

The screenshot shows the 'test' configuration page for an email campaign. The 'Message Type' is set to 'Email', 'Language' to 'English', and 'Sender Name' to 'test'. The 'Sender E-mail' is 'otheres@cloudspace365.solutions'. The 'Recipient Header' is 'To' and the 'Subject' is 'Affordable car leasing for our employees'. The 'Embedding Type' is 'Embedded Images'. Under 'General Mail Settings', 'X-Mailer Header' is checked with the value 'Lucy 4.4.8'. In the 'Advanced Mail Settings' section, 'DKIM Support' is checked, and the 'DKIM Subdomain' is 'mail'. There are also fields for 'Forward E-mail', 'Delivery Method', and 'Use S/MIME Certificate' which is checked with a 'Generate Certificate' button. SSL Certificate, Key, and Chain fields are present but empty.

- Scanner de e-mail:** Curioso sobre quais são os endereços de e-mail da sua organização que podem ser encontrados na Internet? Use o scanner de correio da LUCY e descubra o que é que um hacker já sabe sobre a sua empresa.

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 highlighted in yellow and contains 'phishing-server.com'. Below the domain field, there are several options: 'Crawler' (checked), 'Follow external links' (checked), 'Maximum number of URLs to crawl' (100), and 'Maximum crawling time in minutes' (120). A list of search engines is shown with checkboxes: Yahoo (checked), Lixam (checked), Wotbox (checked), Yandex (checked), Bing (checked), Public Key Servers (checked), Additional Sources (checked), and Paid Sources (checked). A 'Stop' button is at the bottom.

- Criação de páginas iniciais personalizadas:** Os destinatários com um melhor entendimento técnico podem usar o navegador para chamar o domínio ou o endereço de IP associado ao link de phishing gerado aleatoriamente. Para evitar que apareçam mensagens de erro ou que o utilizador final chegue à área de autenticação da consola de administração, poderá criar "páginas iniciais" genéricas dentro do LUCY para os domínios usados na simulação de phishing.



TESTE DA INFRAESTRUTURA

- Ferramenta de teste de malware:** A ferramenta de simulação de malware é um pacote avançado de simulação de malware capaz de emular várias ameaças. Ela permite que um auditor acesse um conjunto avançado de recursos equivalentes a muitas das ferramentas utilizadas por cibercriminosos. Portanto, a ferramenta permite ao administrador LUCY realizar verificações de segurança sem envolver funcionários externos ao departamento de TI.

| Test | Info | 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\STH1 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 last 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 Internet Explorer | Error occurred: Invalid URI: The hostname could not be parsed. (full output) | Fail | Low | View Details |
| 9 | Access to the Internet via Chrome | Error occurred: Invalid URI: The hostname could not be parsed. (full output) | Fail | Low | View Details |

- Deteção de vulnerabilidade ativa e passiva do cliente:** Esta funcionalidade permite testar localmente o navegador do cliente e detetar possíveis vulnerabilidades, com base em bibliotecas personalizadas de JavaScript e nos dados do agente de utilizador do navegador. Os plugins descobertos podem ser automaticamente comparados com as bases de dados de vulnerabilidade (CVE) para identificar dispositivos vulneráveis.

test
Scenario Status: Running ||

Summary
 Scenario Settings

Template Affordable car leasing for employees / English
 Change/Select Template

Active Detection

| | | |
|--|---|--|
| <input checked="" type="checkbox"/> Advanced Information Gathering | <input checked="" type="checkbox"/> Popup Blocker | <input checked="" type="checkbox"/> Social Network |
| <input checked="" type="checkbox"/> Browser Details | <input checked="" type="checkbox"/> Geo Location | <input checked="" type="checkbox"/> Proxy |
| <input checked="" type="checkbox"/> Firebug Information | | |

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 -

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

- **Teste de spoofing:** Teste a sua própria infraestrutura a vulnerabilidades de spoofing por correio.

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

TESTES TÉCNICOS

- **Elearning baseado na reputação:** Treine os seus funcionários de acordo com as suas competências de que necessitam. Meça as competências dos funcionários e facilite uma concorrência amigável entre colegas (gamificação).
Com base nos perfis de reputação de cada utilizador final, o sistema pode fornecer-lhes automaticamente várias sessões de formação. Os perfis de reputação baseiam-se, entre outros fatores, no comportamento do utilizador em simulações de phishing. Isto garante que os utilizadores que são infratores recorrentes recebem conteúdos de formação diferentes daqueles que clicam numa simulação de ataque pela primeira vez.

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

« 1 »
10 ▾

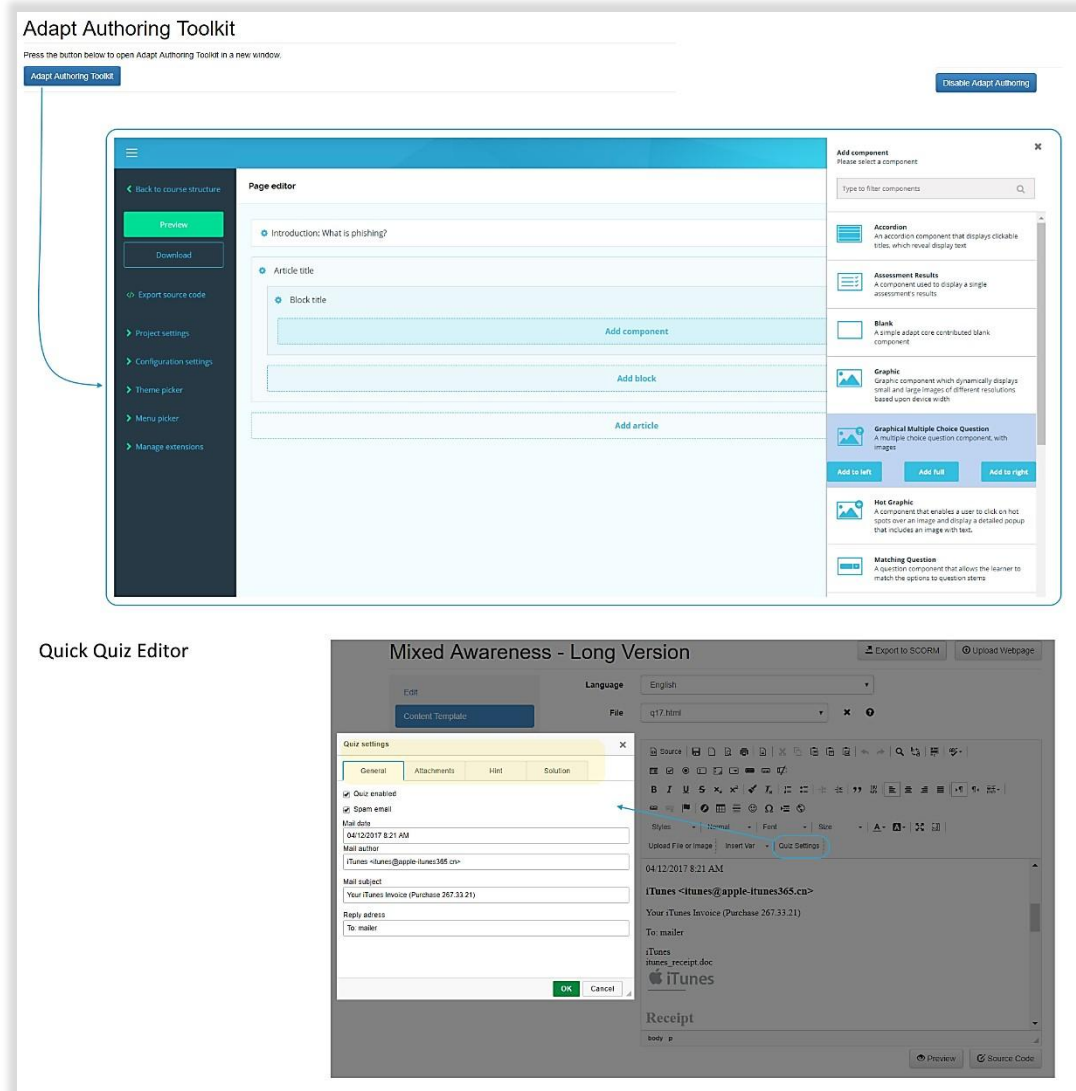
- Portal de formação do utilizador final:** Funcionalidade do Sistema de Gestão de Aprendizagem (SGA): dá a cada funcionário acesso permanente a uma página inicial de formação personalizada que apresenta os seus próprios cursos, especificamente adaptados para eles. Nesta página inicial eles podem ver as suas estatísticas de desempenho, retomar ou repetir a formação, criar certificados de curso e comparar os seus resultados com outros departamentos ou grupos.

The screenshot shows a user profile for 'Oliver' with a 'Phishing Noob' rating of 53.00%. A 'Rating History Chart' shows a steady increase in rating percentage over time, with a callout for 2018-11-13 showing a 29% rating. Summary statistics include 30 campaigns, 30 scenarios, 26 submitted, 6 reported, 12 test failed, 14 test passed, and 53% passed. Training statistics show 11 trainings launched, 6 completed, 5 not completed, and 54% completed. A table of available training includes 'Short General teaching', 'Comprehensive security course', 'Game: Spot the phishing Scam! (V 2.1)', and 'General Security Awareness Course (V 2.3)' with a 'Download Certificate' link.

- Diploma de educação de consciencialização:** Os certificados de elearning podem ser criados e impressos pelo destinatário, quer diretamente no âmbito de uma formação, quer dentro do portal SGA.

The screenshot shows a WYSIWYG editor for an 'Awareness Training Diploma Template'. A 'Quick Tips' box lists variables like %name%, %score%, %date%, and %line%. The editor displays a certificate preview with the text: 'Certificate of Completion', 'This is to certify that %name%', and 'John Smith has completed Mixed Awareness Course'. Test results are shown as 8/10 for the quiz and 8/11 for the test, dated 28.11.2018 at 13:50. Buttons for 'Print Certificate' and 'Restart Course' are visible at the bottom.

- Ferramenta de autoria de elearning:** A ferramenta de autoria de elearning (Adapt) permite a criação de conteúdo de aprendizagem individualizado. Arrastar e largar vídeos ou qualquer outro formato de rich media, inserir exames de menus predefinidos, criar conteúdo interativo de elearning a partir do zero num curto período de tempo.



- Formação de consciencialização rich media:** Integre rich media (vídeo, áudio ou outros elementos que incentivam os visualizadores a interagir e envolver-se com o conteúdo) nas suas formações de consciencialização. Use os vídeos educacionais existentes, adapte-os ou adicione a sua própria 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", "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.gd/HXW5GQ>. 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

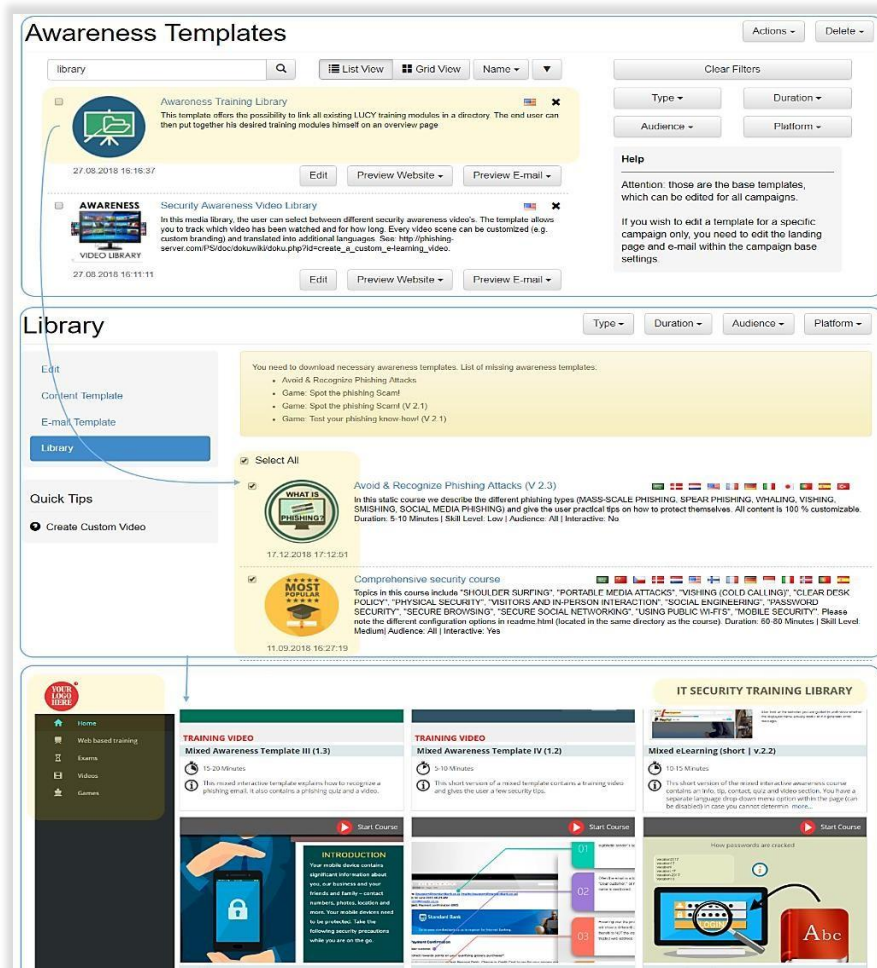
News: Do you know how to handle security incidents 🇺🇸 🇩🇪 🇬🇧 🇪🇸 🇮🇹 🇯🇵 🇧🇷 🇨🇦 🇦🇺

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

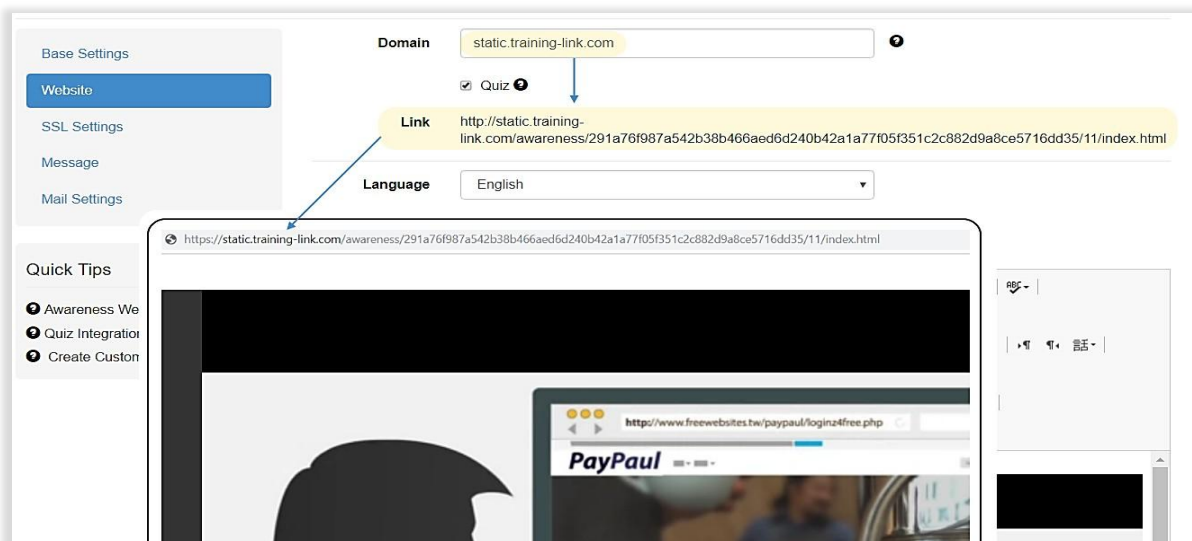
28.12.2018 14:48:47

[...and many more](#)

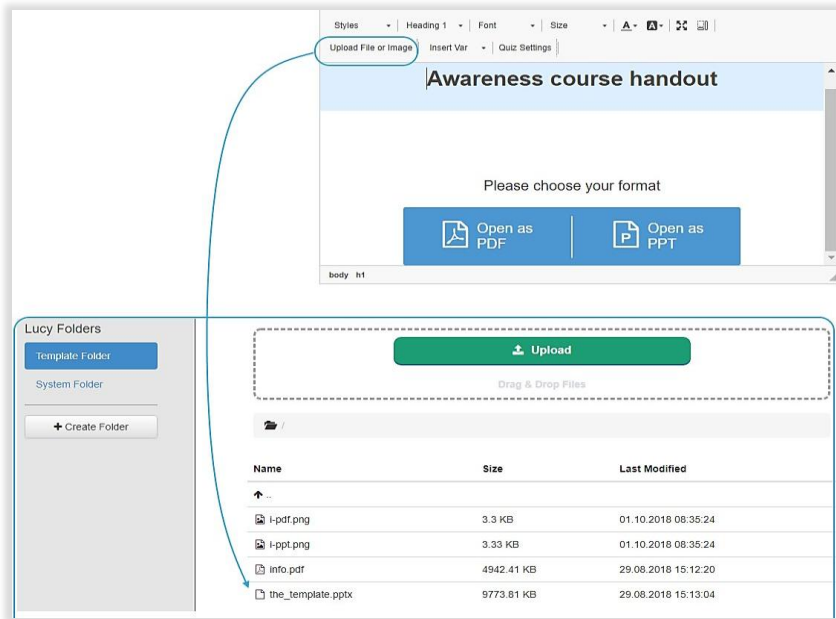
- Biblioteca de formação:** Os seus funcionários podem aceder ao conteúdo de formação da sua organização a partir de uma página de resumo chamada "biblioteca de formação." Ela contém uma grande seleção de modelos regulares de elearning do LUCY, que servem como introdução. A página de resumo pode ser ordenada por determinados tópicos (vídeo, quiz, teste, etc.).



- Suporte de formação estática:** O conteúdo de formação também pode ser publicado em páginas estáticas dentro do LUCY ou na intranet, dando ao utilizador acesso permanente ao conteúdo de formação, independente de possíveis simulações de ataque.



- Suporte de formação offline:** O LUCY tem uma série de modelos editáveis (ficheiros do Adobe Photoshop ou Illustrator) para formação de consciencialização, tais como posters, protetores de ecrã, panfletos, etc.



- Módulos de microaprendizagem:** Concebemos módulos de formação de microaprendizagem (por exemplo, vídeos de 1 minuto ou documentos de uma página para consciencialização) que podem ser adaptados às necessidades da marca e às políticas da sua organização.

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: 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

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!

- Personalização de vídeo:** Envie-nos o logotipo da sua empresa e incluímo-lo nos vídeos de formação. Pretende outro idioma? Não há problema. Definimos o vídeo para ser reproduzido no idioma que preferir. Quer uma cena diferente? Basta descarregar os guiões de vídeo e assinalar as mudanças desejadas.



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 para dispositivos móveis:** Muitos dos módulos incorporados do LUCY estão disponíveis num formato compatível com dispositivos móveis, que dá aos seus utilizadores a flexibilidade de participar da formação em qualquer tipo de dispositivo conectado.



- Importação / exportação de vídeo:** Pode exportar vídeos LUCY para o seu próprio sistema, bem como importar os seus próprios vídeos para o 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'. A video titled 'Data Privacy & GDPR Video' is selected, with a description: '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'. Below the video, there are filters for 'Video', 'Duration', 'Audience', and 'Platform'. A 'Lucy Folders' sidebar on the left contains options like 'Template Folder', 'System Folder', 'Create Folder', 'Rename', 'Copy', 'Move', 'Download', and 'Delete'. The main content area shows a file list with columns for 'Name', 'Size', and 'Last Modified'. The file list includes '2018.06.11_Lucy Data Privacy.mp4' (44094.42 KB), '2018.06.11_Lucy Data Privacy.webm' (34599.3 KB), and 'jquery.js' (93.71 KB). A green 'Upload' button is visible at the top of the file list area.

- Dicas dinâmicas de formação:** As dicas dinâmicas implementadas permitem ao seu administrador definir marcadores nos modelos de ataque que podem indicar aos seus funcionários, dentro do material de elearning, onde é que o ataque de phishing pode ter sido detetado.

The screenshot shows the 'Comprehensive security course' interface. At the top, there are navigation links: 'Home / Awareness Templates / Comprehensive security course / Content Template'. The main content area has a 'Content Template' button and an 'Export to SCORM' button. Below the 'Content Template' button, there are options for 'Language' (English) and 'File' (index.html). The 'Content' area shows a rich text editor with various formatting options. Below the editor, there is a preview of the course content, including the text 'General Security Awareness Cou'. At the bottom, there is an 'Exports' table with columns for 'Date', 'Name', 'Extension', and 'Status'. The table lists three exports: '31.12.2018 15:08:53' (Awareness Template - Comprehensive security course), '29.12.2018 17:10:15' (Campaign - BOUNCE TEST), and '28.12.2018 15:19:11' (Awareness Template - Avoid & Recognize Phishing Attacks (V 2.3)). A yellow folder icon labeled 'scorm-export.zip' is shown next to the first export entry.

ENVOLVER OS FUNCIONÁRIOS

- Denunciar e-mails com um único clique:** Os utilizadores finais podem denunciar e-mails suspeitos com um único clique em uma ou várias contas de e-mail e reencaminhá-los para a sua consola de análise de incidentes LUCY.

The screenshot displays the LUCY interface. On the left, the 'Settings' panel is visible, with the 'Report Email' ribbon button highlighted. A blue arrow points from this button to the 'Report Email' ribbon button in the email client interface. Below the ribbon button, a dialog box titled 'Report Phishing To Your Security Team' is shown, asking the user to confirm if the selected message(s) should be forwarded to the security team and removed from the inbox. The email client interface shows an inbox with a message from 'test <otherthes@cloudspace36!>' with the subject 'Affordable car leasing for our employees'. The message content is partially visible, showing a phishing attempt related to 'CorporateCar-Leasing365'.

- Reforço de comportamento positivo:** O nosso plugin fornece automaticamente reforço de comportamento positivo, manifestado gratidão aos utilizadores finais, através de uma mensagem personalizada, definida pela sua organização.

The screenshot displays the LUCY interface, similar to the previous one. The 'Settings' panel is visible, with the 'Report Email' ribbon button highlighted. A blue arrow points from this button to the 'Report Email' ribbon button in the email client interface. Below the ribbon button, a dialog box titled 'Report Phishing To Your Security Team' is shown, asking the user to confirm if the selected message(s) should be forwarded to the security team and removed from the inbox. The email client interface shows an inbox with a message from 'test <otherthes@cloudspace36!>' with the subject 'Affordable car leasing for our employees'. The message content is partially visible, showing a phishing attempt related to 'CorporateCar-Leasing365'. A second dialog box titled 'Report Phishing To Your Security Team' is shown, displaying a positive feedback message: 'Thank you. This was a LUCY phishing simulation. Good job in spotting the attack!'.

- Pedido de inspeção aprofundada:** Por vezes, os utilizadores querem saber se o e-mail recebido pode ser aberto com segurança. Opcionalmente, o utilizador pode usar o "pedido de inspeção aprofundada" dentro do plugin local para dizer à equipa de segurança que quer um feedback sobre o e-mail comunicado.

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 dialog.
- Email List:** A list of incoming emails. One email is selected, and a dialog box is triggered.
- Report Phishing To Your Security Team Dialog:** A yellow dialog box with a question mark icon asking, "Do you wish to request an additional message analysis from your security team?". It includes "Ja" (Yes) and "Nein" (No) buttons.
- Phishing Incident Reports Table:** A table listing detected phishing incidents. The "Need more analysis" button is highlighted for a specific entry.

| 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 | oliver@muenchow.ch | Lucy Test | Attack CS | 0.00 | Simulation | ⚠️ 🗑️ 📧 📧 |

- Análise automática de incidentes:** Gerir e responder a e-mails suspeitos denunciados por meio de uma consola de gestão centralizada: o analisador do LUCY permite fazer uma inspeção automatizada das mensagens denunciadas (cabeçalho e corpo). O analisador inclui uma pontuação de risco individual, fornecendo uma classificação em tempo real de e-mails denunciados. O analisador de ameaças representa um alívio notável da carga de trabalho da equipa de segurança.

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 | <input type="button" value="Send Abuse"/> <input type="button" value="Delete"/> |
| 03.07.2018 14:45 | oliver@muenchow.ch | ★★★★★ | Lucy Test | TEST 123 | 0.00 | Simulation | <input type="button" value="Send Abuse"/> <input type="button" value="Delete"/> |
| 03.07.2018 08:10 | oliver@muenchow.ch | ★★★★★ | N/A | N/A | 1.00 | Open | <input type="button" value="Send Abuse"/> <input type="button" value="Delete"/> |
| 02.07.2018 10:02 | oliver@muenchow.ch | ★★★★★ | Lucy Test | LMS Access | 0.00 | Simulation | <input type="button" value="Send Abuse"/> <input type="button" value="Delete"/> |
| 02.07.2018 09:54 | palo@lucysecurity.com | ★★★★★ | N/A | N/A | 0.00 | Open | <input type="button" value="Send Abuse"/> <input type="button" value="Delete"/> |
| 02.07.2018 09:54 | palo@lucysecurity.com | ★★★★★ | N/A | N/A | 0.00 | Open | <input type="button" value="Send Abuse"/> <input type="button" value="Delete"/> |

| | | 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"/> |

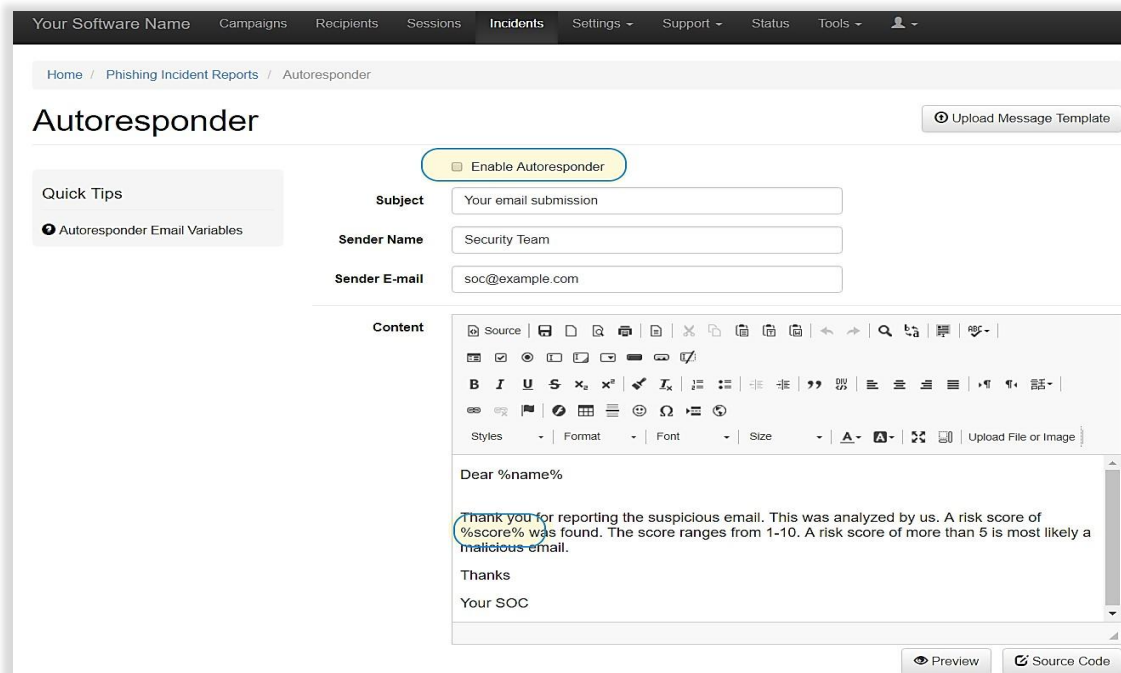
Home / Phishing Incident Reports / 09.03.2018 12:17

09.03.2018 12:17

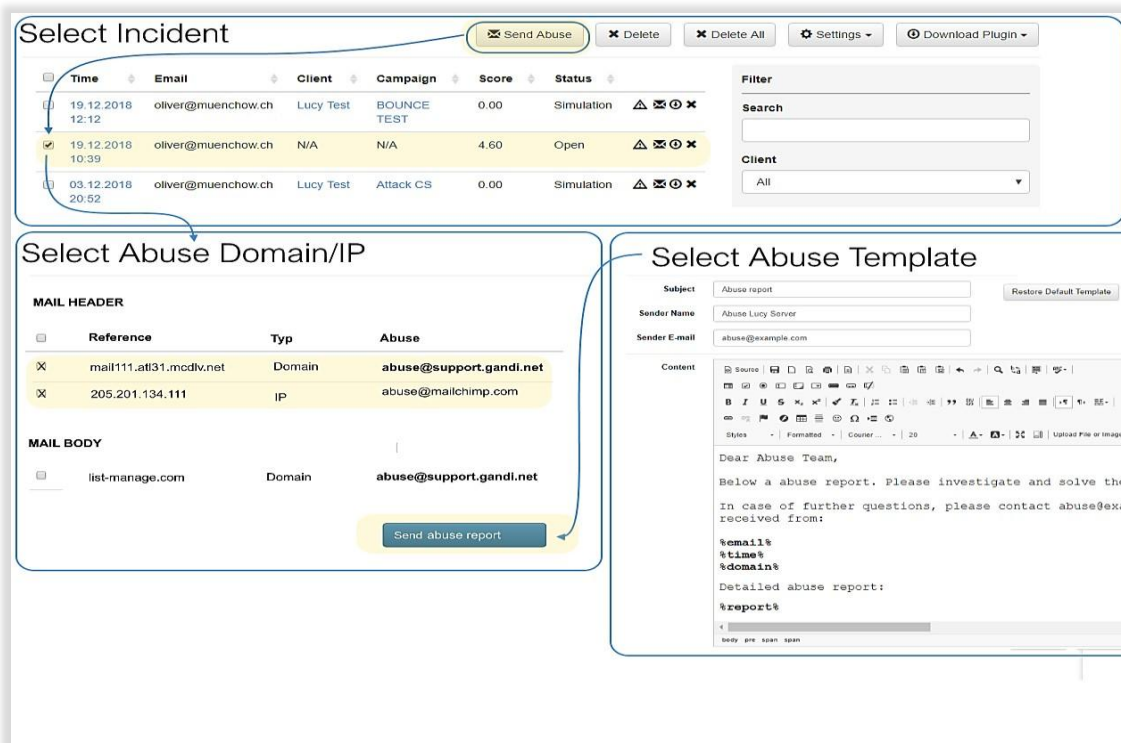
Overall Risk Score: 2.5 of 10.0

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:

- Feedback automático de incidentes:** A resposta automática a incidentes permite o envio de uma notificação automática para o utilizador final, fornecendo os resultados da análise de ameaças por e-mail. O texto da mensagem é livremente configurável e a pontuação de risco do e-mail dada pelo LUCY também pode ser incluída, se necessário.



- Mitigação de ameaças:** O mitigador de ameaças comportamentais é uma abordagem revolucionária para eliminar os riscos de e-mail. Ele apoiará o administrador de segurança na anulação do ataque (por exemplo, enviando um relatório automatizado para a equipa de fornecedores de abuso especificada envolvida no ataque).



- Análise personalizada baseada em regras:** Define as suas próprias regras para a análise de e-mail e cálculos de risco.

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"/> | ⊗ ✕ |

- Opções de personalização do plugin:** O LUCY permite uma personalização fácil e uma marca branca completa de várias funções do plugin (ícone apresentado, mensagens de feedback, etiqueta da fita, protocolo de transmissão, cabeçalho enviado, etc.).

The screenshot shows the 'Phishing Incident Reports' interface. At the top, there is a table with columns: Time, Email, Client, Campaign, Score, Status, and icons for actions. Below the table, there are buttons for 'Send Abuse', 'Delete', 'Delete All', 'Settings', and 'Download Plugin'. The 'Settings' dropdown menu is open, showing options: Custom Rules, Score Factors, Abuse, Autoresponder, and Plugin Settings. Below this is a 'Settings' form with various input fields and checkboxes. The 'Save' button is highlighted. Below the settings form, the 'Phishing Incident Reports' table is shown again, with the 'Download Plugin' dropdown menu open, listing options like 'Microsoft Outlook 32-bit', 'Microsoft Outlook 64-bit', 'Microsoft Outlook 365', and 'Gmail Addon'.

- Integração de terceiros:** Usando a automação de API REST de incidentes do LUCY, podemos processar e-mails denunciados e ajudar a sua equipa de segurança a interromper ataques de phishing ativos enquanto estão em ação.

The screenshot shows the 'API Whitelist' interface. At the top, there are buttons for '+ New', 'Delete', and 'API Documentation'. Below this is a table with columns: IP, and a delete icon. The table contains two rows of IP addresses: 192.168.10.231 and 192.168.12.114. Below the table, there are three sections: 'Resources', 'Endpoint List', and 'Endpoint List'. The 'Resources' section lists: 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 details: /api/incidents (GET), /api/incidents/:id (GET), and /api/incidents/:id (DELETE).

- Identifique ataques com padrões comuns:** Aplique os filtros do painel do LUCY para detetar vetores de ataque comuns em toda a sua organização. Procura indicadores semelhantes de comprometimento em todos os e-mails denunciados.

The screenshot displays the 'Incident Reports' dashboard. On the left, a table lists several reports with columns for Time, Email, Rating, Client, Campaign, Score, and Status. A detailed view of a report for 'sarah@test.com' is shown on the right, featuring a circular 'Overall Risk Score' gauge (3.9 of 10.0) and a 'Message Subject' field containing the text 'Behold is also often'. A blue circle highlights the 'Behold' text in the subject line, and a blue arrow points from this circle to the 'Search' field in the filter panel on the right, which also contains the text 'Behold'. This illustrates how common attack patterns can be identified and filtered.

- Perfis de reputação de utilizador do incidente:** Classifica os utilizadores com uma pontuação de reputação do incidente.

This screenshot shows the 'Incident Reports' table with the 'Rating' column highlighted by a blue box. The ratings are represented by star icons: five stars for the highest rating and one star for the lowest. The table shows various reports from different clients and campaigns, with scores ranging from 0.00 to 1.00. The filter panel on the right is also visible, showing options to filter by domain, reputation, and score.

- Integração com simulações de ataque:** Integração contínua de relatórios e painel com simulações de phishing; identifica os utilizadores que se comportaram de maneira exemplar numa simulação de 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%

- Instalação fácil:** Instale o plugin de Incidente de Phishing para Outlook, Gmail, 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