SECURA ANGLER

Secura delivers world-class security test tools. Secura Angler is a sophisticated phishing test platform aimed at both security awareness campaigns as well as offensive security assessments. It simulates phishing campaigns that mimic the attack without causing any harm to the employee's IT-environment or violating their privacy.

THE ULTIMATE PHISHING TEST PLATFORM

Secura has worked in information security and privacy for nearly two decades. This is why we uniquely understand the challenges that you face like no one else and would be delighted to help you address your information security matters efficiently and thoroughly. We work in the areas of people, processes and technology. For our customers we offer a range of security testing products and services varying in depth and scope.

WHAT IS SECURA ANGLER?

Phishing is the most common way for attackers and criminals to strike at your organization. By tricking users to click on links or attachments in email, they attempt to obtain sensitive information such as usernames, passwords, and credit card details. Security-aware organizations strive to protect their employees from phishing attacks by educating them not to respond to suspicious emails and other electronic communication, and to report such attacks to the IT department. However, it is usually not easy to continuously assess and train the overall level of the employee awareness of phishing attacks.

Secura Angler is a sophisticated phishing test platform aimed at both security awareness campaigns as well as offensive security assessments. It allows you to regularly assess the employees' response to phishing attacks in the form of a simulated phishing campaign that mimics the attack without causing any harm to the employee's it-environment or violating their privacy. Following the campaign, a clear management report is created showing how many people ignored the phishing attempt, how many visited the link and how many attempted to enter their credentials. The credentials are discarded in the 'awareness campaign' scenario.

Besides using the Secura Angler platform as a Continuous Security Awareness tool, it can also be used by security professionals in security assessments like Red Teaming and Social Engineering. In these ethical hacking assignments, the goal is to gain access to the IT systems, which means that phishing is used as one of the techniques to gather credentials. In this use case, (targeted) phishing campaigns are used to harvest credentials, fingerprint users' browsers, or distribute well-controlled malware. For more information on Secura's Red Teaming offering, please refer to our leaflet on that topic.

WHY SECURA ANGLER?

Normally, setting up a phishing campaign is time consuming and error prone. A plausible scenario needs to be drafted, it must be sent in a personalized way to multiple recipients and the result of the campaign needs to be measured and stored securely. The 'landing page', the website the electronic communication refers to, needs to look genuine and trustworthy. Small mistakes (layout, domain name, and spelling) will reduce the effectiveness of the phishing campaign. Furthermore, sending vast amounts of messages will most likely trigger spam filters. Secura Angler automates all these point using templates and allows to dry run a complete campaign without actually sending out emails.

In the offensive security testing mode, credentials are securely stored in an encrypted database and only retrievable by pre-selected users that require to login using two-factor authentication.

Once the campaign is setup and tested, the phishing campaign is executed with a single mouse-click. Secura Angler supports multiple spam evasion techniques to ensure all emails, even sent in bulk, will arrive at the recipient.

A clear management report is available per campaign and shows the statistics of each campaign, which can be used as a direct input for a tailored security awareness training.

FEATURES

- Template driven email creation;
- Automation of domain name registration and landing page deployment;
- Automation of TLS certificate generation;
- Management of email lists per company/campaign;
- Managing phishing campaign's lifecycle, including:
  - Creating a new campaign;
  - Setting up target organization details;
  - Defining email templates;
  - Dry-run /verify phishing campaign;
  - Starting/pause/stop phishing campaign;
  - Monitoring and statistics per campaign;
  - Permanently deleting the campaign and/or its results.
- Managing target users lists (emails, names, salutations etc.);
- Sending out phishing messages via phishing email server (SMTP) and monitoring target employees' responses;
- Supporting the following attack mechanisms:
  - Email with URL and tracking image;
  - Email with attachment: DOC, XLS, PDF, EXE, ZIP etc.;
  - Email with malware that takes control of the PC (the safe malware created by Secura);
- Extensive spam filter evasion;
- Two-factor authentication for specific roles;
- Browser fingerprinting;
- Generating campaign report in HTML and PDF formats.

BENEFITS

- Easy and reliable creation, execution and management of phishing campaigns;
- Automatic administration of domain names and security certificates;
- Periodic execution of phishing campaigns to determine trends and align with company security awareness programs;
- Offensive Security testing mode to collect credentials or distribute malicious payload.

INTERESTED?

Would you like to learn more about our services? Please do not hesitate to contact us.

Follow us on

Vestdijk 59
5611 CA Eindhoven
Netherlands

Karspeldreef 8
1101 CJ Amsterdam
Netherlands

T +31 (0)40 23 77 990
E info@secura.com
W www.secura.com