Phishing on Demand
Pascal Gerig
Bachelor Thesis, 1st presentation
29 October 2019
Phishing is diverse

Where?
Phone, social media (social engineering)
Web, email, SMS (content spoofing)
Mobile & desktop apps (trojan horses)

What?
Sensitive information
(credentials, personal data, access tokens)

Why?
Gain access to protected resources
(information, money, credibility, services, …)
Everybody’s life: phishing emails
Real or fake?
Real or fake?

- That's not Facebook's URL
- The real page says “Log in” in the title. Ironically, the phishing site is more consistent than Facebook on this.
- No SSL padlock
- “Email address” not “Email” on the real page
- Wrong year in copyright message
- “Forgot” not “Forgot” on the real page
- Different languages
- Missing links
State of the art

Professional frameworks for testing awareness

Online guides & “educational” videos
State of the art

Professional frameworks for testing awareness

COMPLEX!

Online guides & “educational” videos

TIME CONSUMING!

= hand-crafted phishing pages which require a lot of work (and maintenance)
This project...

What if you could phish websites on demand?

1) Redirect webpage requests to phishing server

2) Run phishing instance for each webpage request

3) User receives on the fly phished webpages
... and the idea behind

Screenshots & dynamic content injection

1. tracking user actions
2. user data
3. apply user input
4. rendering web page
5. screenshotting
6. screenshot & metadata
7. rendering image (…)

client

HTTP server

headless web browser
Our goal
Our goal
Research questions

RQ1: Is screenshotting a possible phishing technique?

RQ2: What are the limits of such a phishing technique?

RQ3: How likely is it to trick people?
Work plan

JavaScript code to collect and transmit user input

Local rendering of input boxes and loading indicators

Java code to control headless Browser

Evaluation
Summary

Phishing is diverse

Setup for Phishing pages takes time

Phishing on Demand with Screenshots