VadeSecure
Advanced email Protection

SCIENTIST PRESENTATION

DETECTION OF PHISHING WEBPAGES WITH SUPERVISED LEARNING

Adrien Gendre
Chief Solution Architect
+1 (415) 509-2025
adrien.gendre@vadesecure.com

Sebastien GOUTAL
Chief Science Officer
+1 (415) 696-3005
sebastien.goutal@vadesecure.com

AGENDA

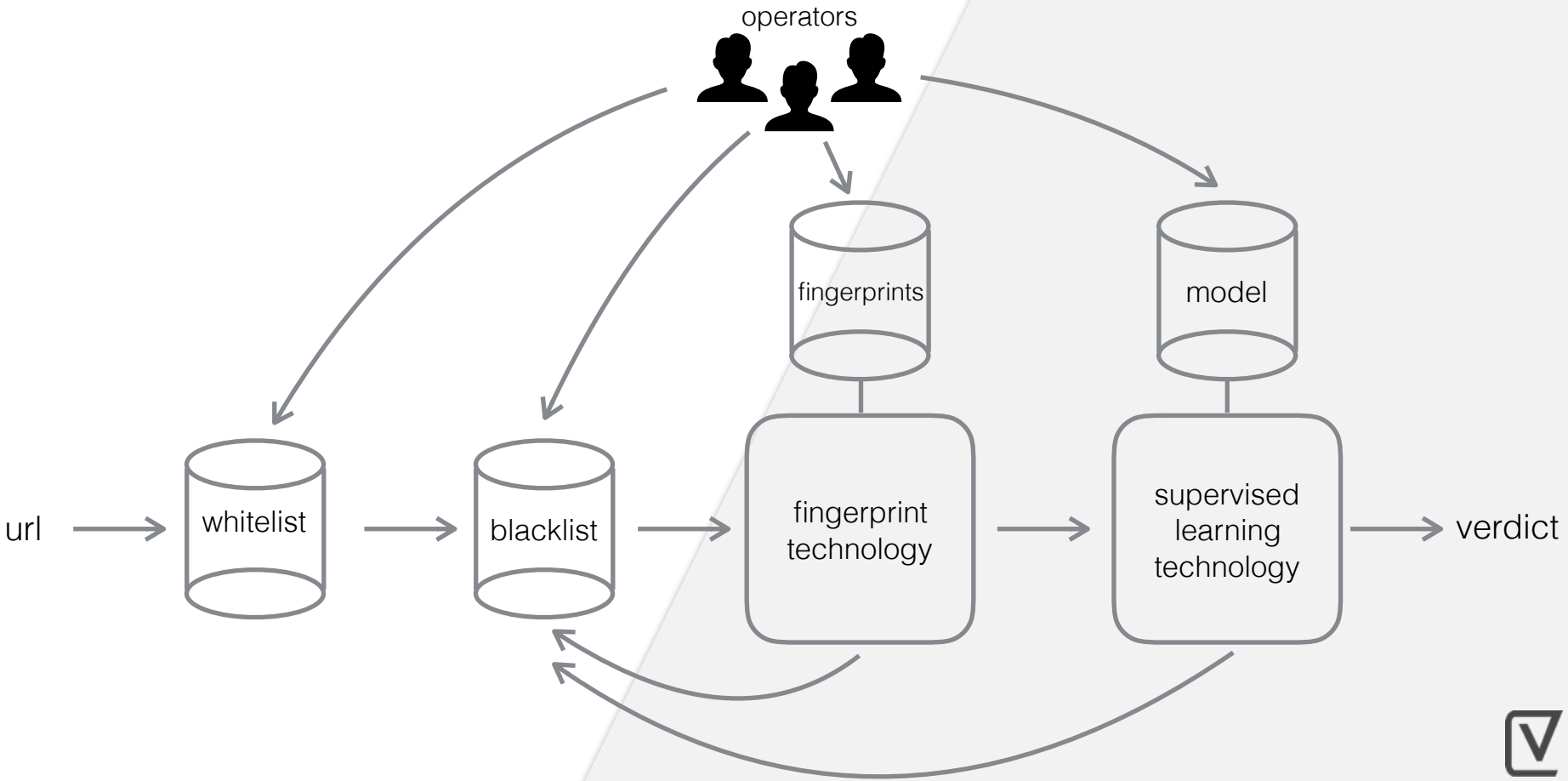
PHISHING DETECTION PIPELINE

BRAND DETECTION

SUPERVISED LEARNING TECHNOLOGY

RESULTS

PHISHING DETECTION PIPELINE



BRAND DETECTION - A UNIQUE APPROACH

- A phishing attack always impersonates a brand (PayPal, Apple…)
- Pros:
  - Improve catch rate with brand specific features
  - Alert brand when a URL is detected

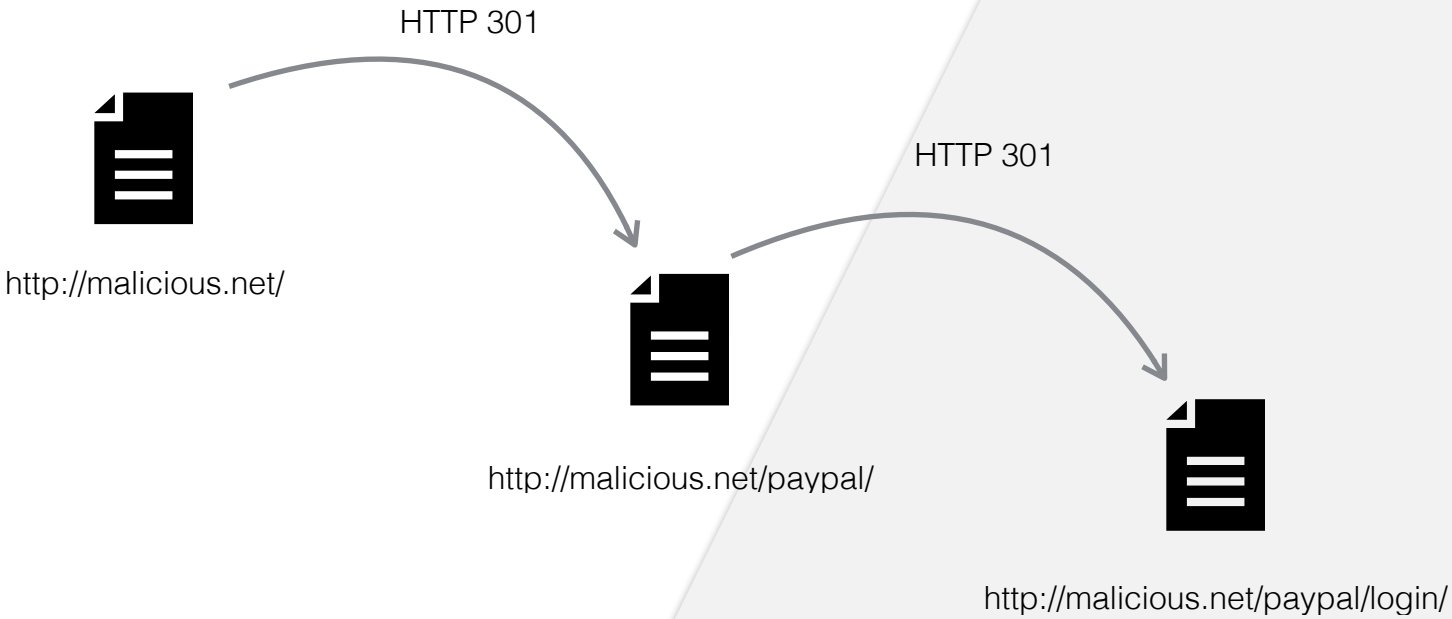
SUPERVISED LEARNING TECHNOLOGY

- Collect data
- Build features vector
- Classify vector

SUPERVISED LEARNING TECHNOLOGY - COLLECT DATA

- **Input**: url
- **Output**: final url and final document
- Redirections are followed
  - HTTP 4xx status code
  - Meta refresh
  - Javascript

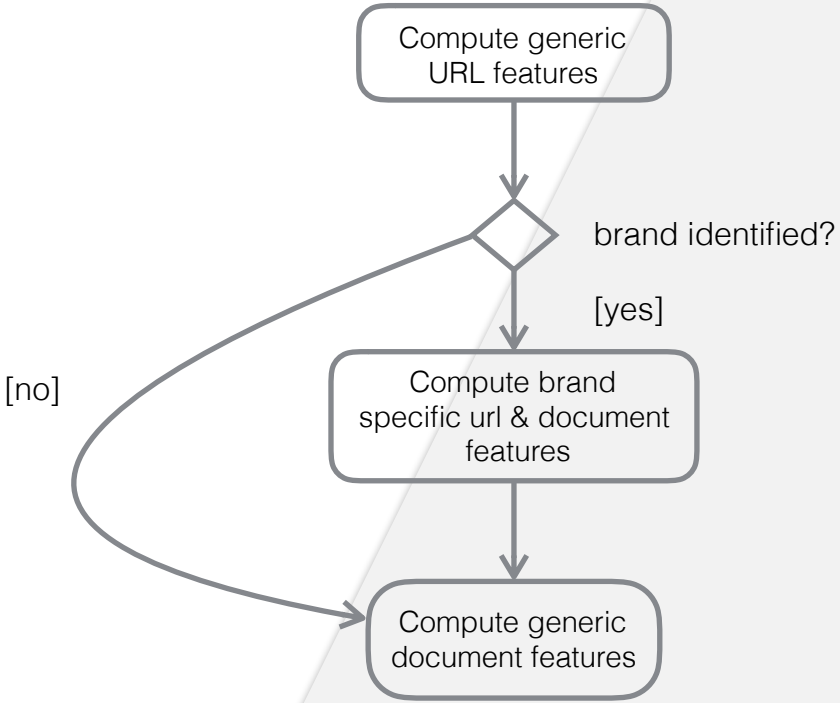
SUPERVISED LEARNING TECHNOLOGY - COLLECT DATA



SUPERVISED LEARNING TECHNOLOGY - BUILD FEATURES VECTOR

- Binary features
- A feature relates either to a URL or a document
- Feature type can be:
  - Generic: common to most phishing webpages
  - Brand specific: specific to a brand (Paypal, Apple…)

SUPERVISED LEARNING TECHNOLOGY - BUILD FEATURES VECTOR



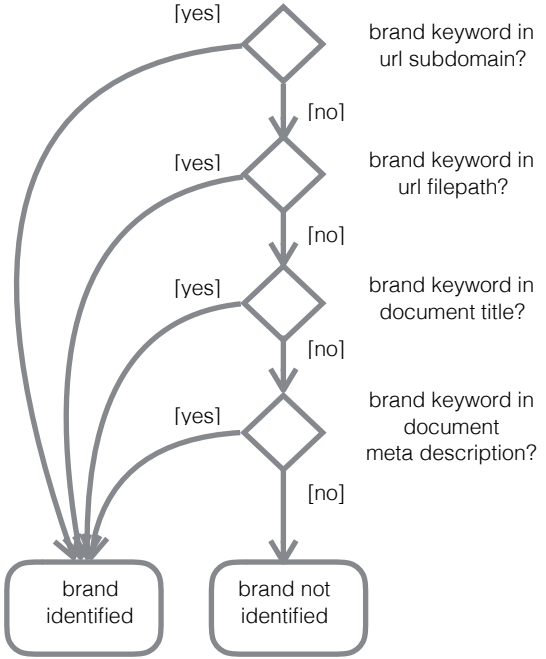
SUPERVISED LEARNING TECHNOLOGY - BUILD FEATURES VECTOR

Generic URL features

Feature	Exemple
URL_HOSTNAME_IPV4	http://**75.125.43.213**/itunees
URL_MANY_SUBDOMAINS	http://**login.paypal.com**.arest.net/websrc
URL_WORDPRESS_PATH_COMPONENT_OR_TILDE	http://econergy.info/**wp-includes**/ppl/ http://13.185.121.59/~cadas507/index1.php
URL_ACTION_KEYWORD_SUSPECT	http://zgcake.com/wellsfargo/**signon**.htm http://odn.zce.szcecin.cz/**login**/ http://ausgreesoar.com.au/logn.php

SUPERVISED LEARNING TECHNOLOGY - BUILD FEATURES VECTOR

Identify brand




```
<brand name="apple">
  <keyword>apple</keyword>
  <keyword>icloud</keyword>
  <keyword>itunes</keyword>
  [...]
</brand>
```

brand keyword in url subdomain,
match can be fuzzy

`http://75.125.43.213/itunees`

SUPERVISED LEARNING TECHNOLOGY - BUILD FEATURES VECTOR

Brand specific features

Feature	Description
URL_SUBDOMAIN_SUSPECT	One the URL subdomain matches one of the brand **`keyword`** elements. Match can be fuzzy.
URL_PATH_SUSPECT	One the URL path element matches one of the brand **`keyword`** elements. Match can be fuzzy.
DOCUMENT_TITLE_OR_METADESCRIPTION_SUSPECT	Document title (resp. meta description) matches at least one of the brand **`title`** (resp. **`meta_desc`**) elements
DOCUMENT_ICON_OR_CSS_OR_JS_SUSPECT	Document icon (resp. CSS and JS) matches at least one of the brand **`icon`** (resp. **`css`** and **`js`**) elements
DOCUMENT_HIGH_DOMAIN_RATE	At least 50% of document links have a domain matching the brand **`domain`** elements
DOCUMENT_DATA_SUSPECT	There is data in the document that matches at least one of the brand **`data`** elements

SUPERVISED LEARNING TECHNOLOGY - BUILD FEATURES VECTOR

Brand description

```
<brand name="apple">
  <keyword>apple</keyword>
  <keyword>icloud</keyword>
  <keyword>itunes</keyword>
  <domain>apple.com</domain>
  <domain>icloud.com</domain>
  <domain>cdn-apple.com</domain>
  <title>Apple</title>
  <title>iCloud</title>
  <title>iTunes</title>
  <meta_desc>Apple ID</meta_desc>
  <meta_desc>iCloud</meta_desc>
  <css>signin.css</css>
  <js>signin.js</js>
  <js>apple.js</js>
  <data>Apple ID</data>
</brand>
```

A brand can have multiple services or products

Most resources (images, CSS, JS…) are stored on these domains

SUPERVISED LEARNING TECHNOLOGY - GENERIC DOCUMENT FEATURES

Feature	Description
DOCUMENT_FORM_SUSPECT	A form contains a keyword in its attribute that is relevant of a required user action within the phishing process. Example: <form id="form" action="**login.**php" method="post"> <form method="POST" id="**signIn**" name="**Connect**Form" action="u-send.php">
DOCUMENT_CREDENTIAL_FIELD	An input field is a password field or a credit card security code field. Example: <input autocomplete="off" **type="password"** id="loginpwd" name="loginpwd" value=""> <input name="**cvc**" maxlength="4" id="**cvc**" autocomplete="off" style="width:47px;" type="text">
DOCUMENT_SUSPECT_TECHNIC	There is a suspect technic.

SUPERVISED LEARNING TECHNOLOGY - SUSPECT TECHNICS

Technic	Example
Homoglyph attack	Google PayPal
HTML hex encoding	Appl&#101
JS hex encoding	`document.write(unescape('%53%69%67%6E%20%49%6E'))`

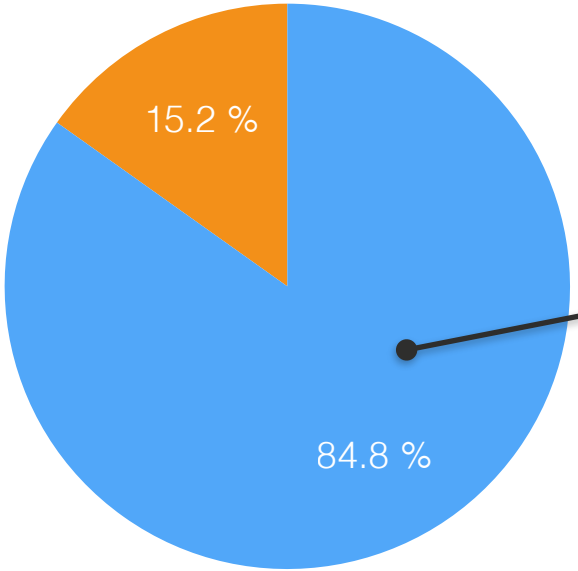
JS AES 256 encryption	`var hea2p = ('0123456789[…]nopqrstuvxyz');`
	`var hea2t = 'XwHq/n3w[…]yFz/19lQ==';`
	`var output = Aes.Ctr.decrypt(hea2t, hea2p, 256);`
	`document.write(output)`

SUPERVISED LEARNING TECHNOLOGY - CLASSIFY VECTOR

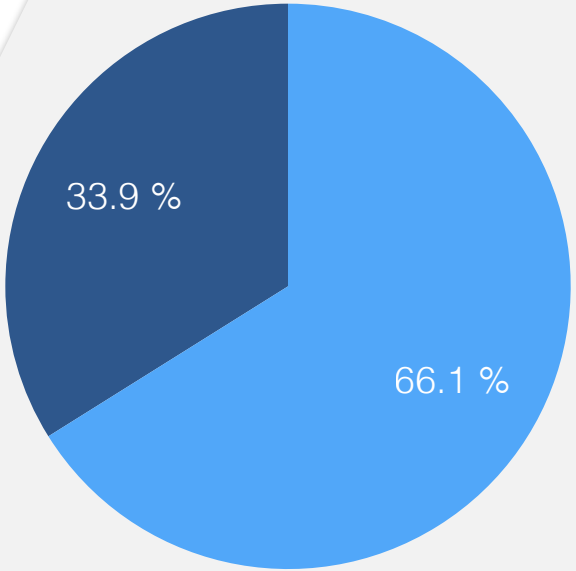
- Binary classifier: SVM with Gaussian RBF kernel
- Training & test corpus:
  - Phishing: fingerprint technology, operators decisions
  - Clean: urls matching whitelist, operators decisions
- Goal : 0 false positive

RESULTS

Phishing catch rate

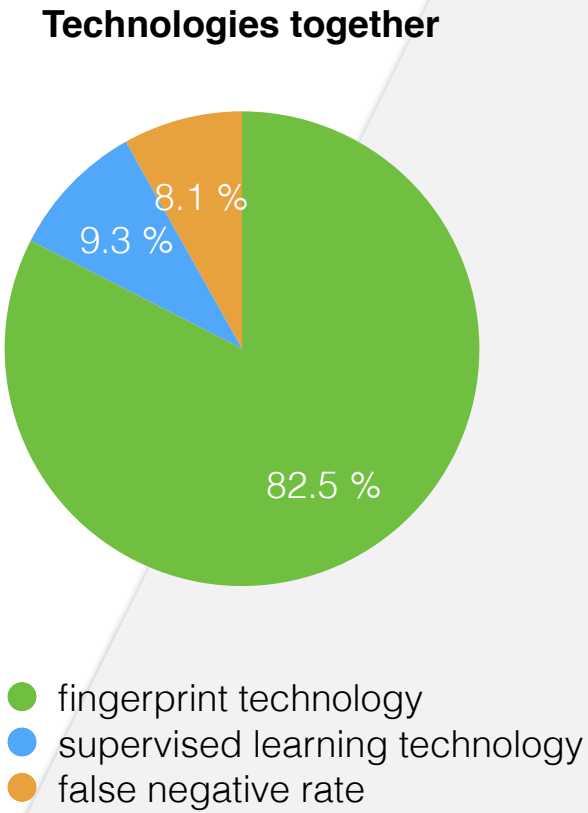


Brand detection



catch rate false negative rate brand detected no brand detected

RESULTS


Technologies together
8.1 %
9.3 %
82.5 %
fingerprint technology
supervised learning technology
false negative rate

CONCLUSION

	Pros	Cons
Fingerprint technology	High catch rate Fast Flexible	Binary output Fails to detect unknown threats
Supervised learning technology	High catch rate Output is a probability	Slow Difficult to scale brands

Merci

Feel free to exchange with our lead scientist

Sebastien GOUTAL
Chief Science Officer
+1 (415) 696-3005
sebastien.goutal@vadesecure.com

If you want to use it: IsItPhishing.org

Free for Researchers and Students