

PhishEye: Live Monitoring of Sandboxed Phishing Kits

Xiao Han

Nizar Kheir

Davide Balzarotti



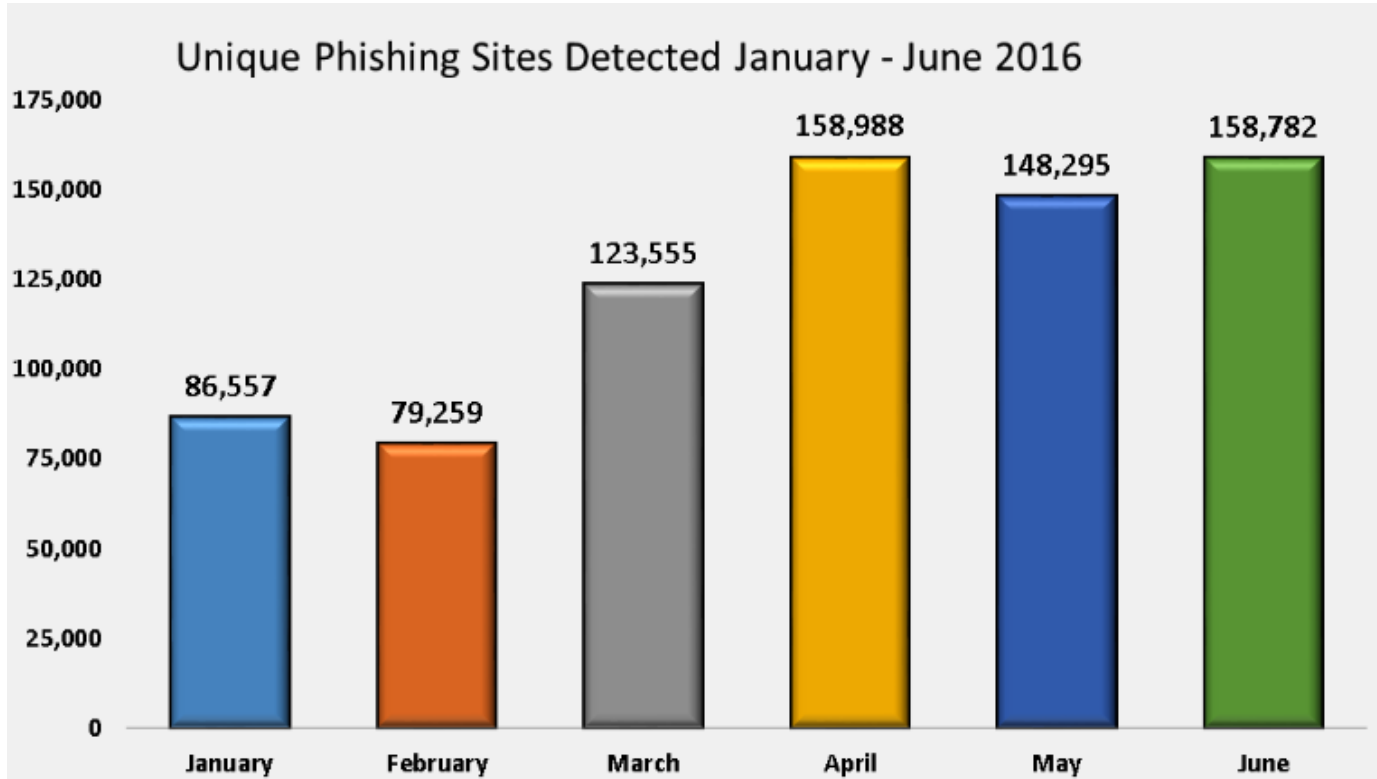
Summary

Motivation

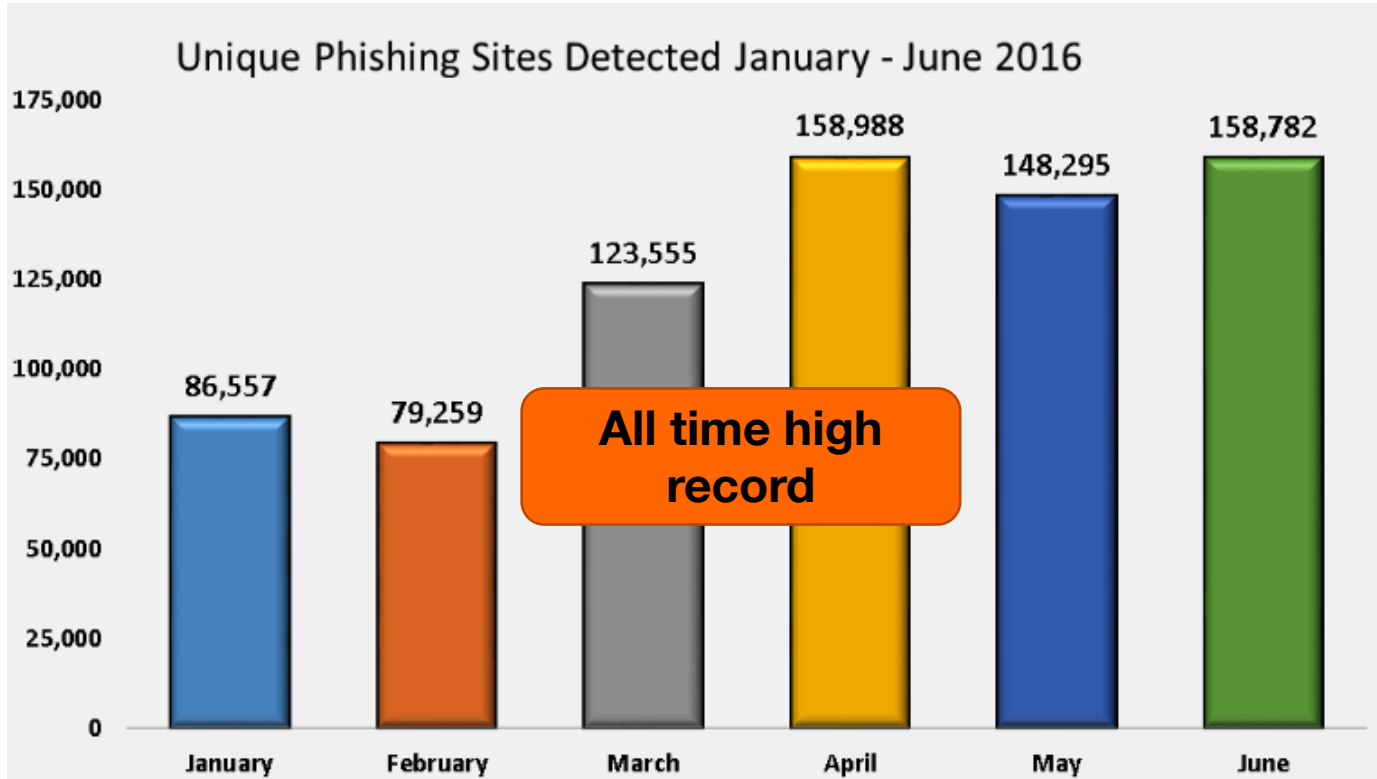
Sandboxed phishing kits

Implementation

Results



[APWG Phishing Activity Trends Report 2nd Quarter 2016]



[APWG Phishing Activity Trends Report 2nd Quarter 2016]

Motivation

- PKs monitored only **after** being detected by anti-phishing services

Motivation

- PKs monitored only **after** being detected by anti-phishing services
- Details about entire **lifecycle** of a phishing kit are still **missing**

Motivation

- PKs monitored only **after** being detected by anti-phishing services
- Details about entire **lifecycle** of a phishing kit are still **missing**
- **71.4%** of the domains that hosted phishing pages were **compromised websites** [APWG global phishing report 2014]

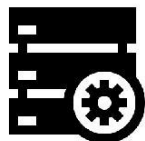
Monetization



Vulnerable Web Server



Attacker



Phishing Pages



Social Engineering



Victims



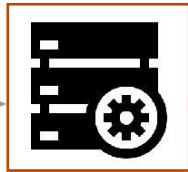
Technical Subterfuge



Monetization



Vulnerable Web Server



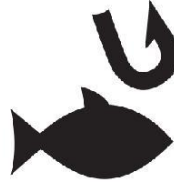
Attacker



Know your enemy: Phishing [HoneyNet 05]

Evil searching [FC 09]

Phishing Pages



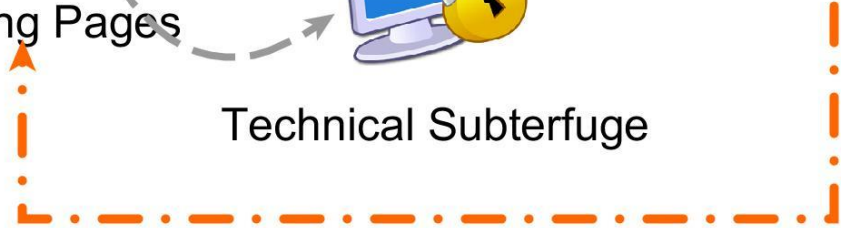
Social Engineering



Technical Subterfuge



Victims



Monetization



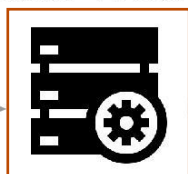
Browser plugin: N. Chou [NDSS 04]

User education: P. Kumaraguru [TOIT 10]



Attacker

Vulnerable Web Server



Phishing Pages



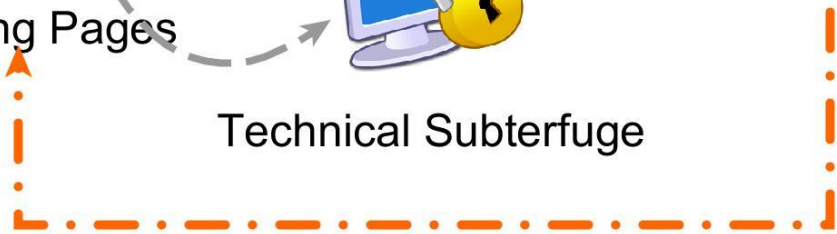
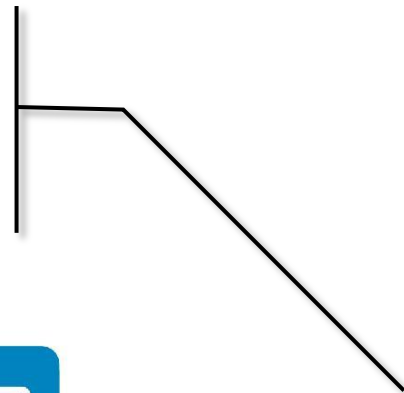
Social Engineering



Technical Subterfuge



Victims



Monetization



Learning to detect phishing emails [www 07]

Discovering phishing dropboxes using email metadata [eCrime 12]



Attacker

Vulnerable Web Server



Phishing Pages

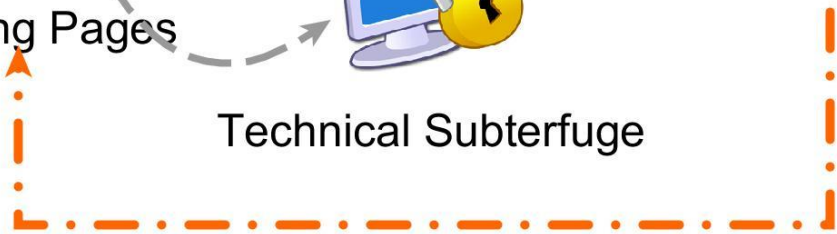


Social Engineering



Technical Subterfuge

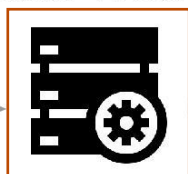
Victims



Monetization



Vulnerable Web Server



Attacker



Phishing Pages



Social Engineering



Technical Subterfuge



Victims



Detection: Cantina [www 07], C. Whittaker [NDSS 10]

Blocking: Google Safe Browsing (GSB), Phish Tank, ...

Take down: Examining the impact of website take-down on phishing [eCrime 07]

Monetization

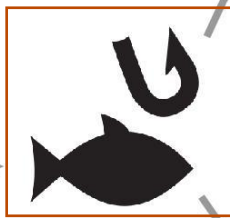


Handcrafted fraud and extortion [IMC 14]



Attacker

Vulnerable Web Server



Phishing Pages

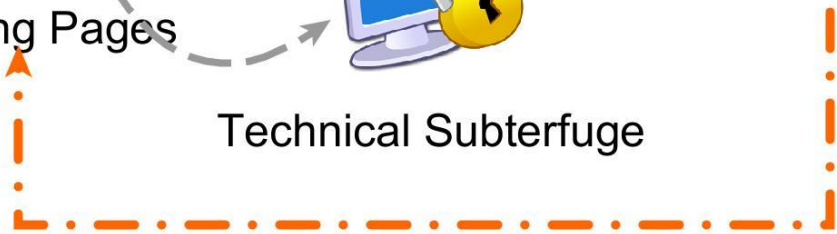


Social Engineering



Technical Subterfuge

Victims



Monetization



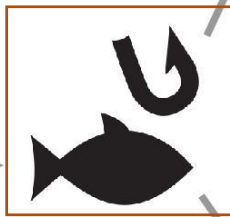
Vulnerable Web Server



Attacker



Phishing Pages



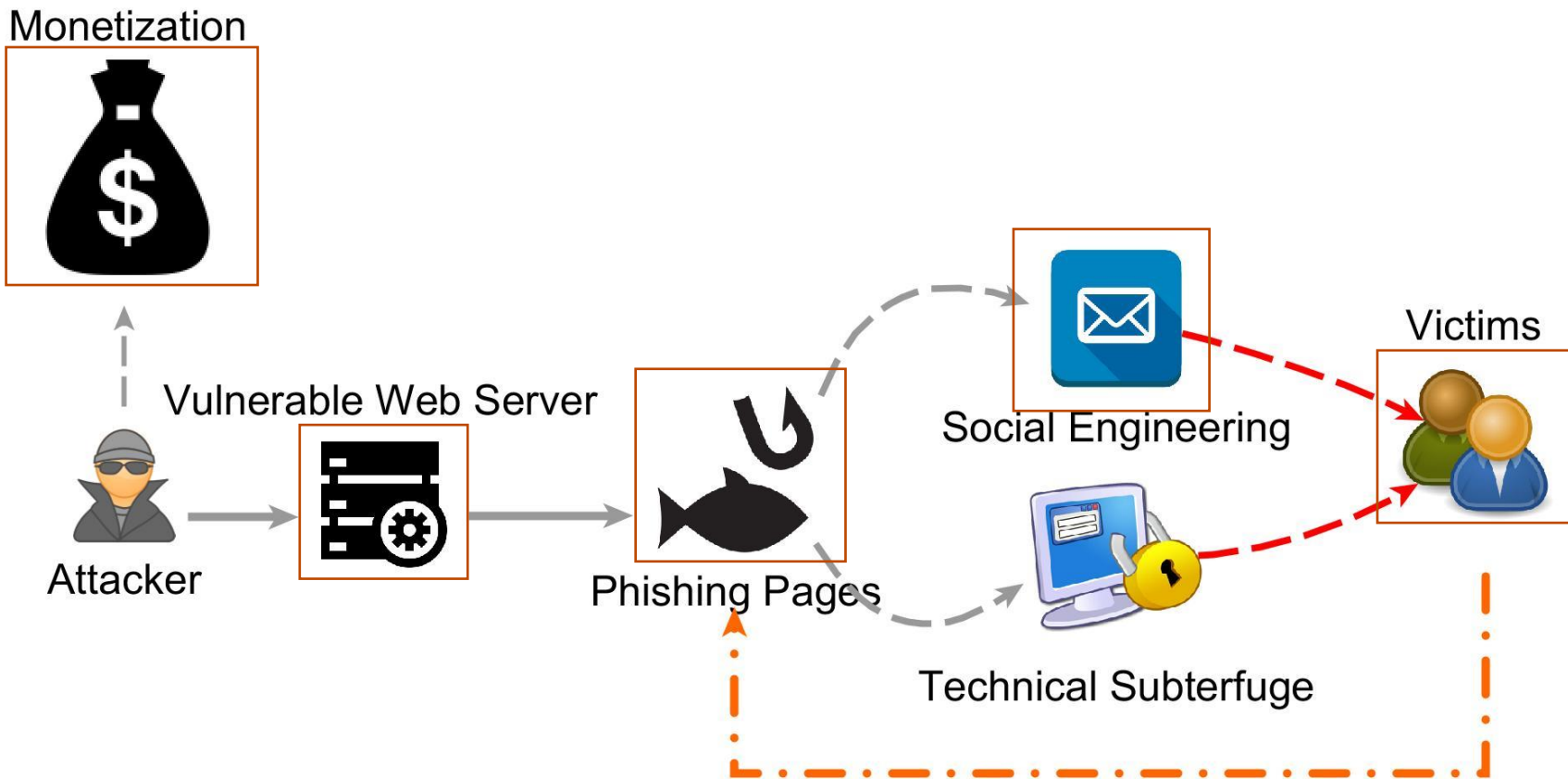
Technical Subterfuge



Social Engineering



Victims



Monetization

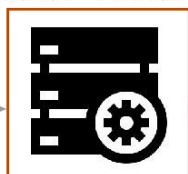


**Incomplete and fragmented
view of PKs lifecycle**



Attacker

Vulnerable Web Server



Phishing Pages



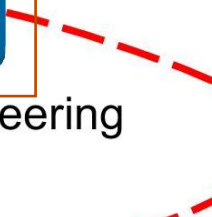
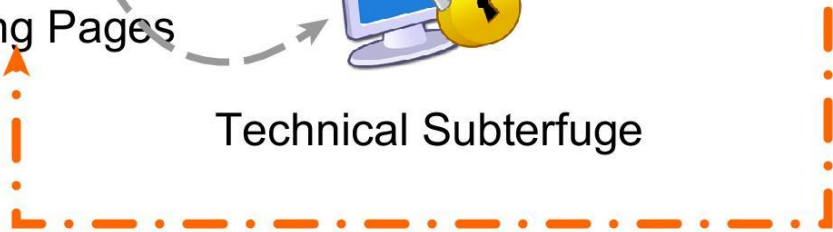
Social Engineering



Technical Subterfuge



Victims





Web honeypot

Attacker identification

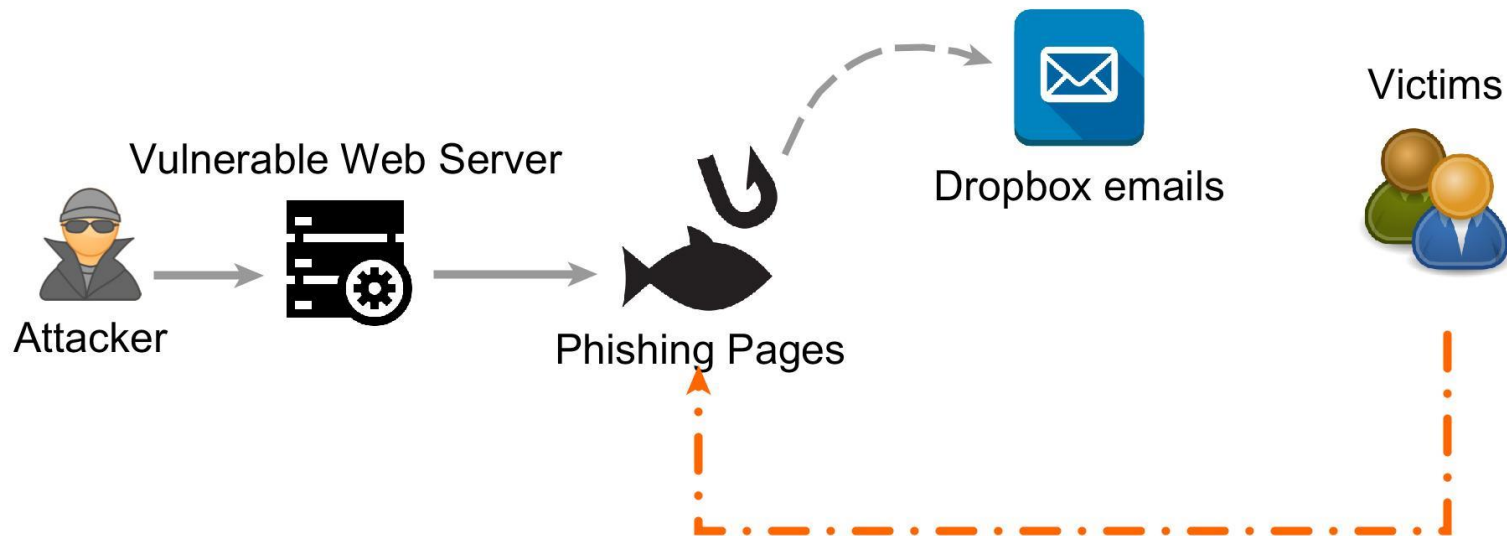
Privacy protection

[Credits: Idea Sandbox, Neutrons]

Sandboxed Phishing Kits

Global Picture:

- **Attackers, victims, and security researchers**
- **Phishing blacklist services**
- **Complete privacy protection**



Implementation

Web Honeypot

5 vulnerable web applications

x

100 domain names

D. Canali [NDSS 13]



Implementation



PK installation



Web Honeypot

5 vulnerable web applications

X

main names

ali [NDSS 13]

PayPal

Email

Mot de passe

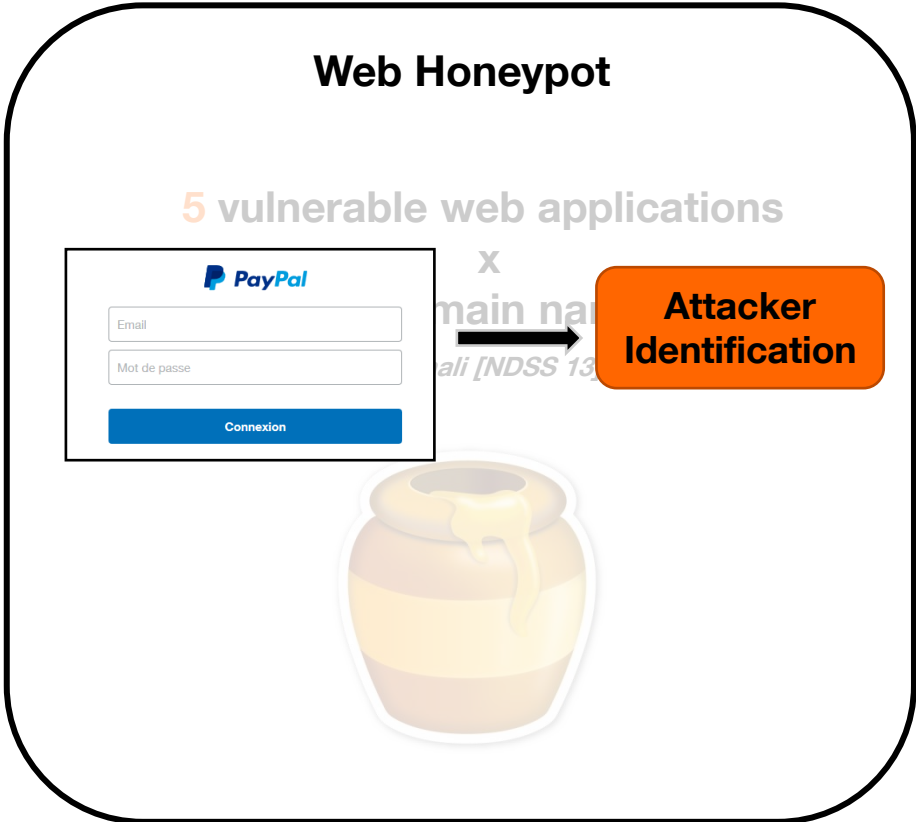
Connexion



Implementation



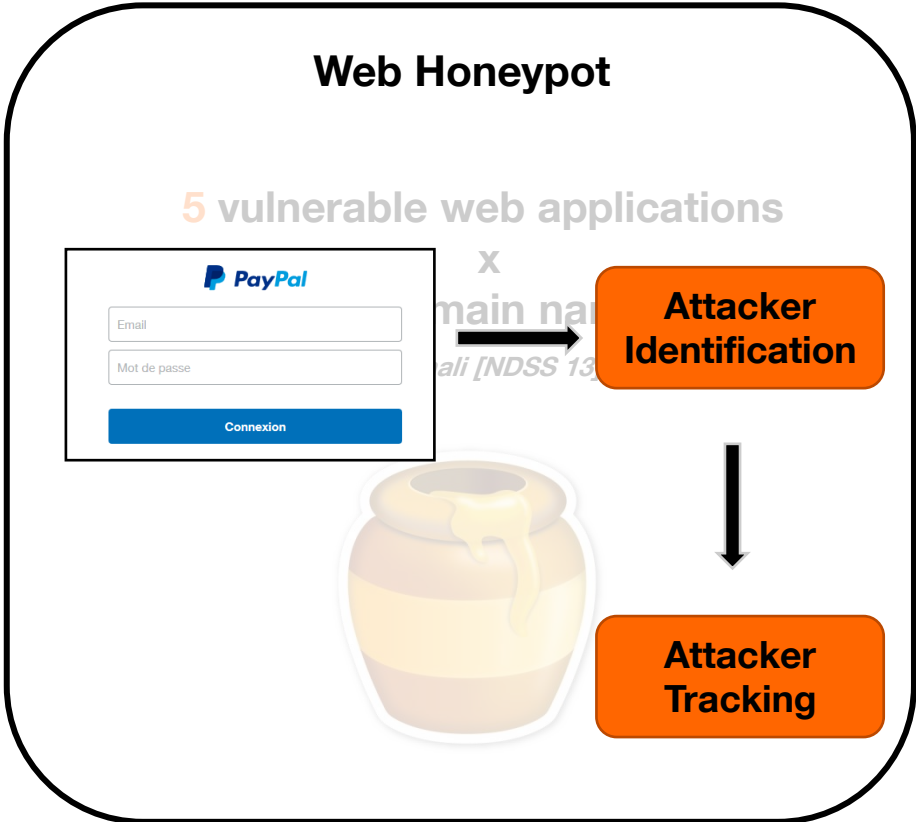
PK installation



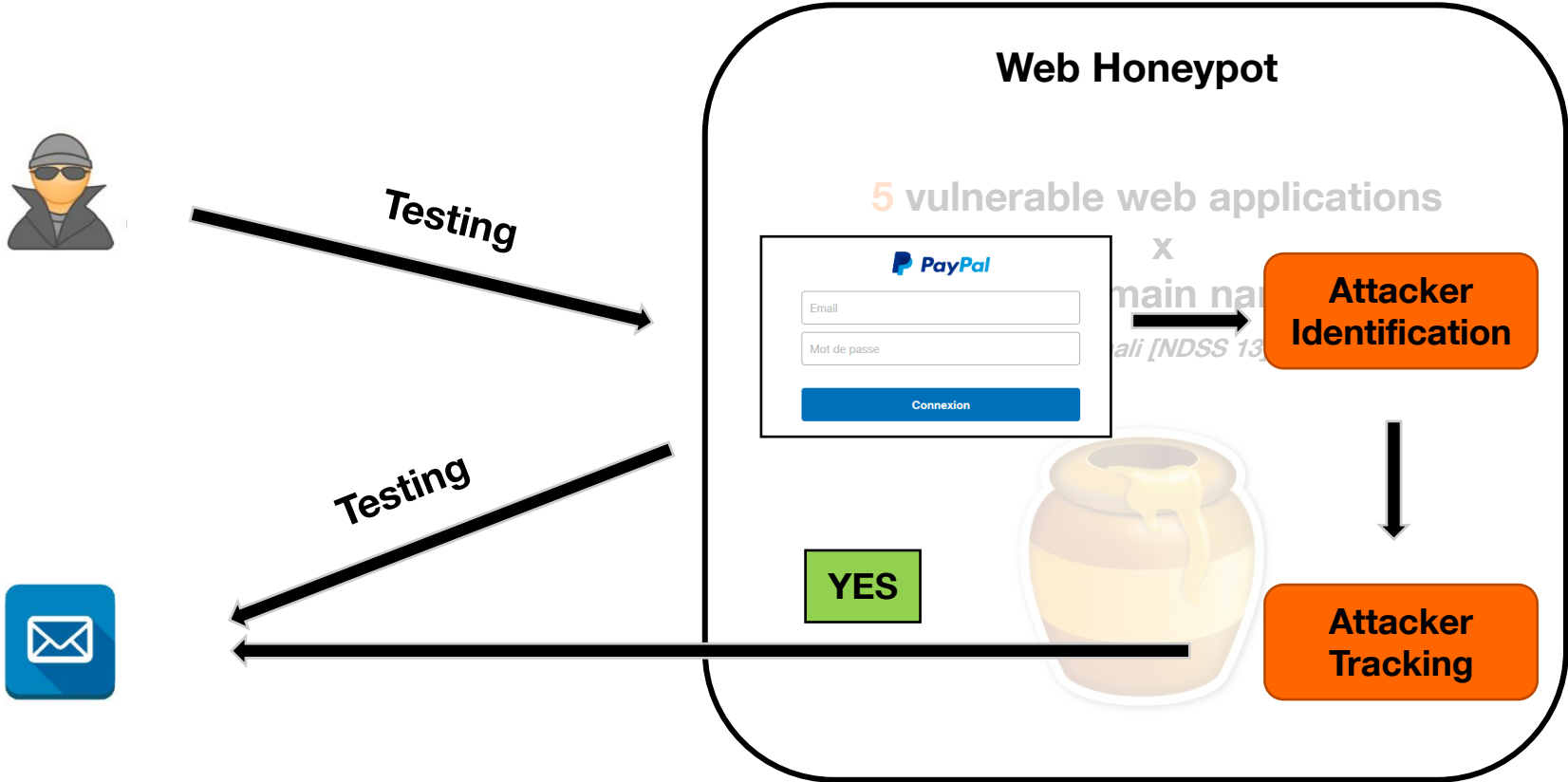
Implementation



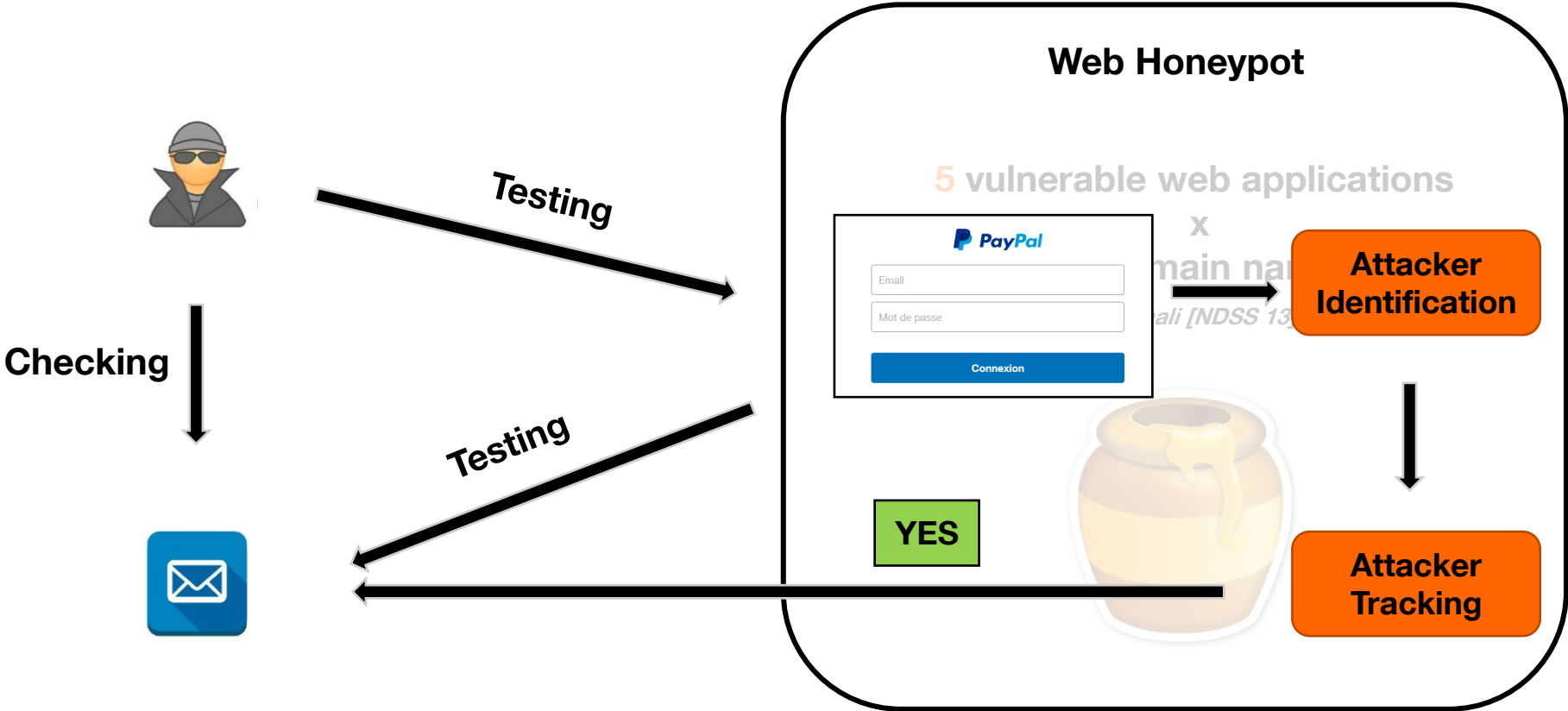
Testing



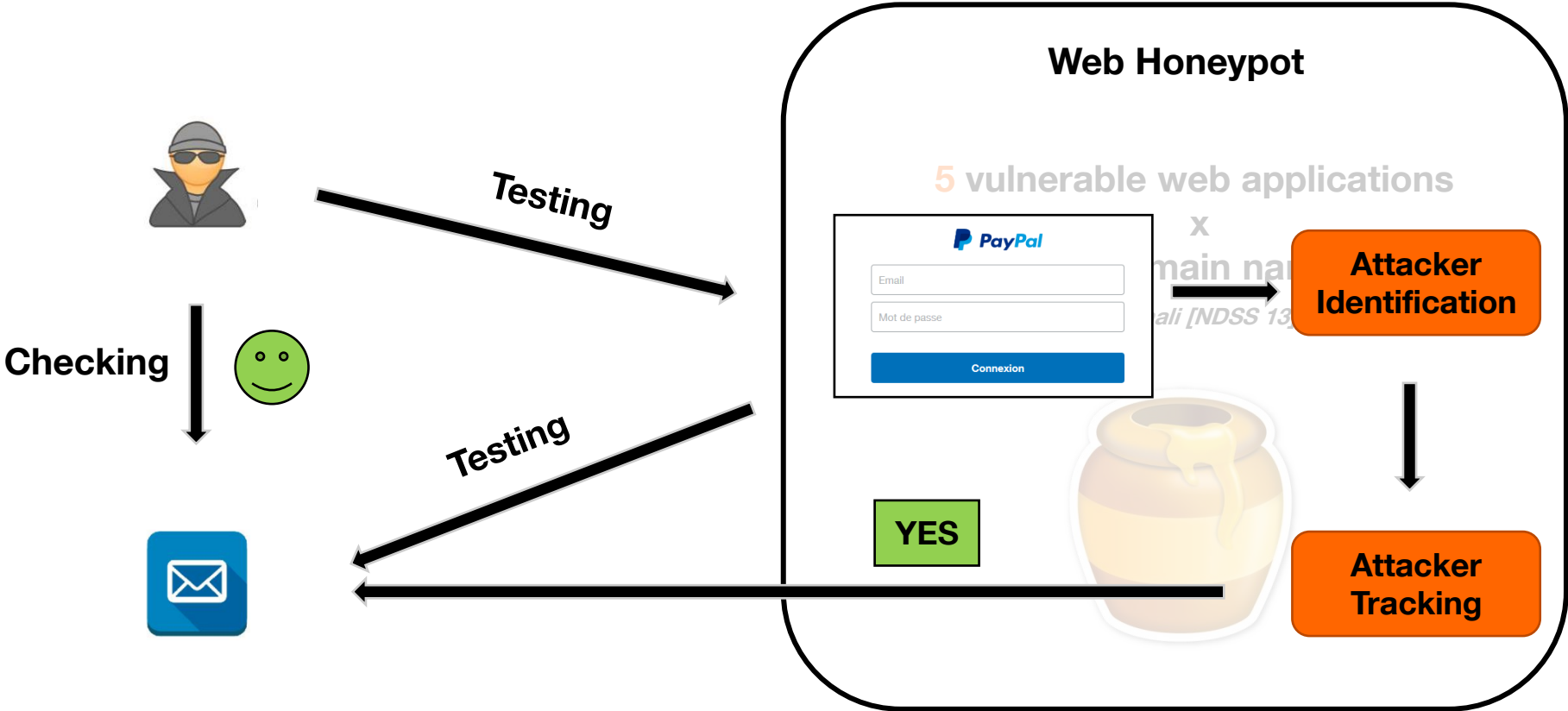
Implementation



Implementation



Implementation



Implementation

Victims



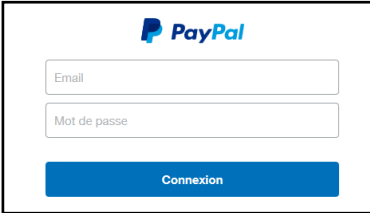
Web Honeypot

5 vulnerable web applications

X

main names

ali [NDSS 13]



PayPal

Email

Mot de passe

Connexion



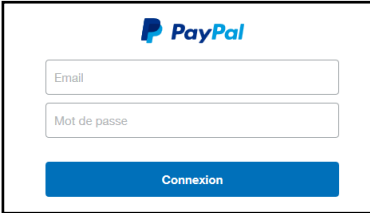
Implementation

Victims



Web Honeypot

5 vulnerable web applications



PayPal

Email

Mot de passe

Connexion

X
main na
ali [NDSS 1

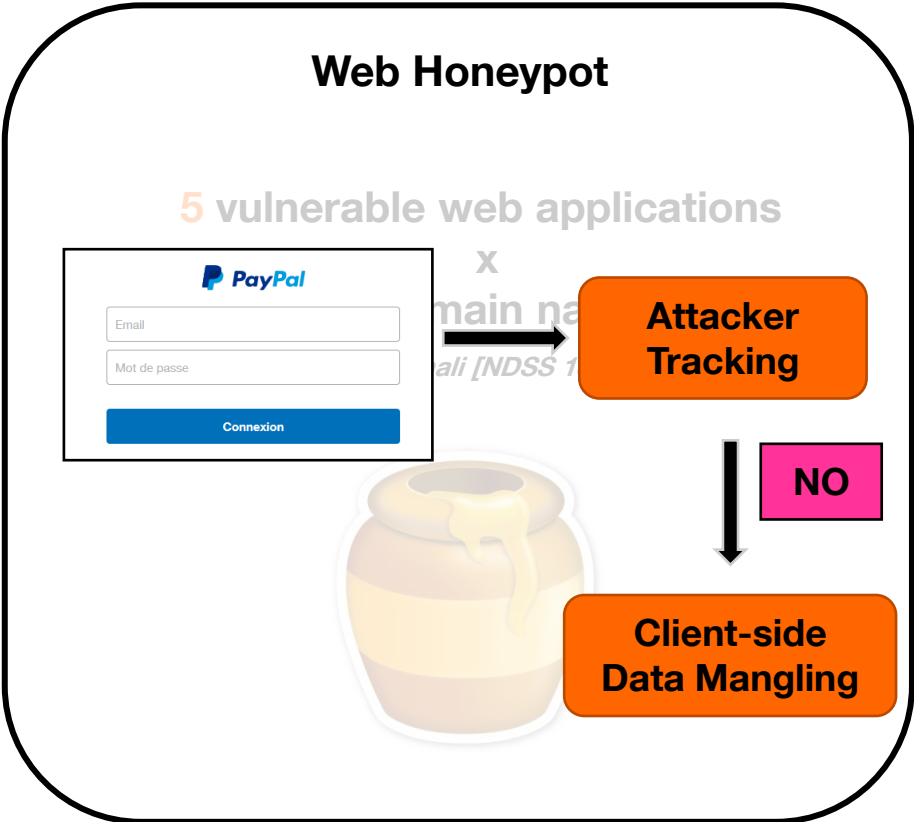


Attacker Tracking



Implementation

Victims



Implementation

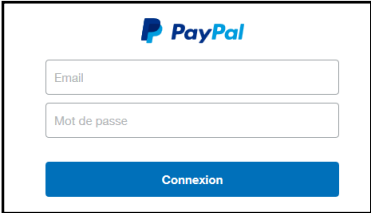
Victims



**Inject
JavaScript to
prevent data
leakage**

Web Honeypot

5 vulnerable web applications



X
main na
ali [NDSS 1

**Attacker
Tracking**



NO

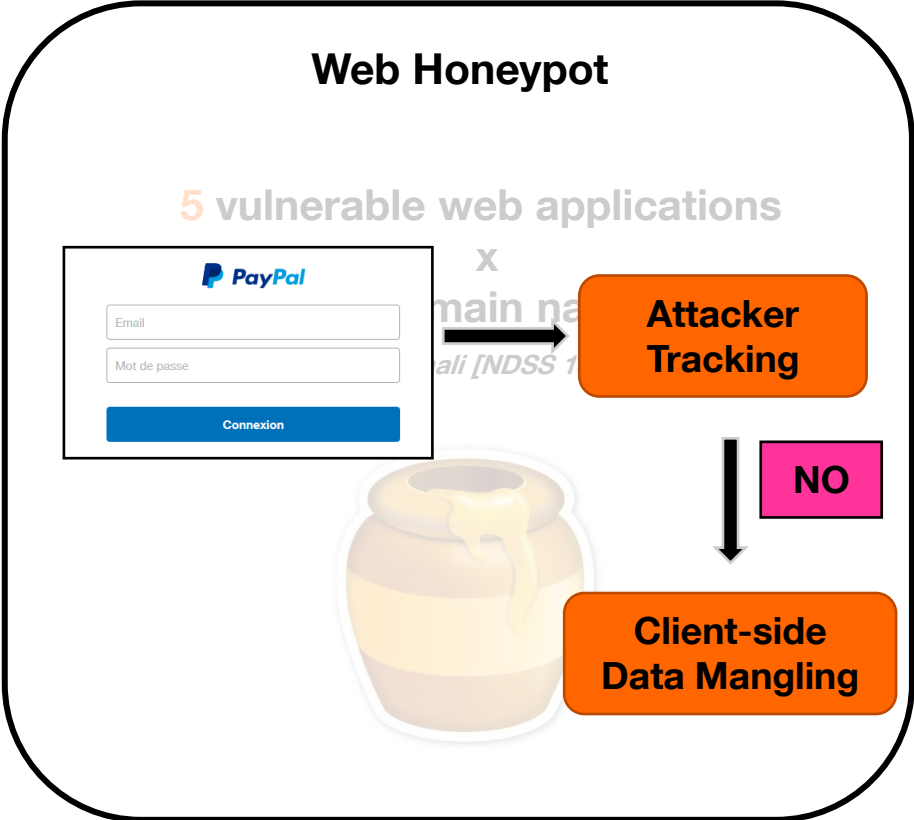
**Client-side
Data Mangling**

Implementation

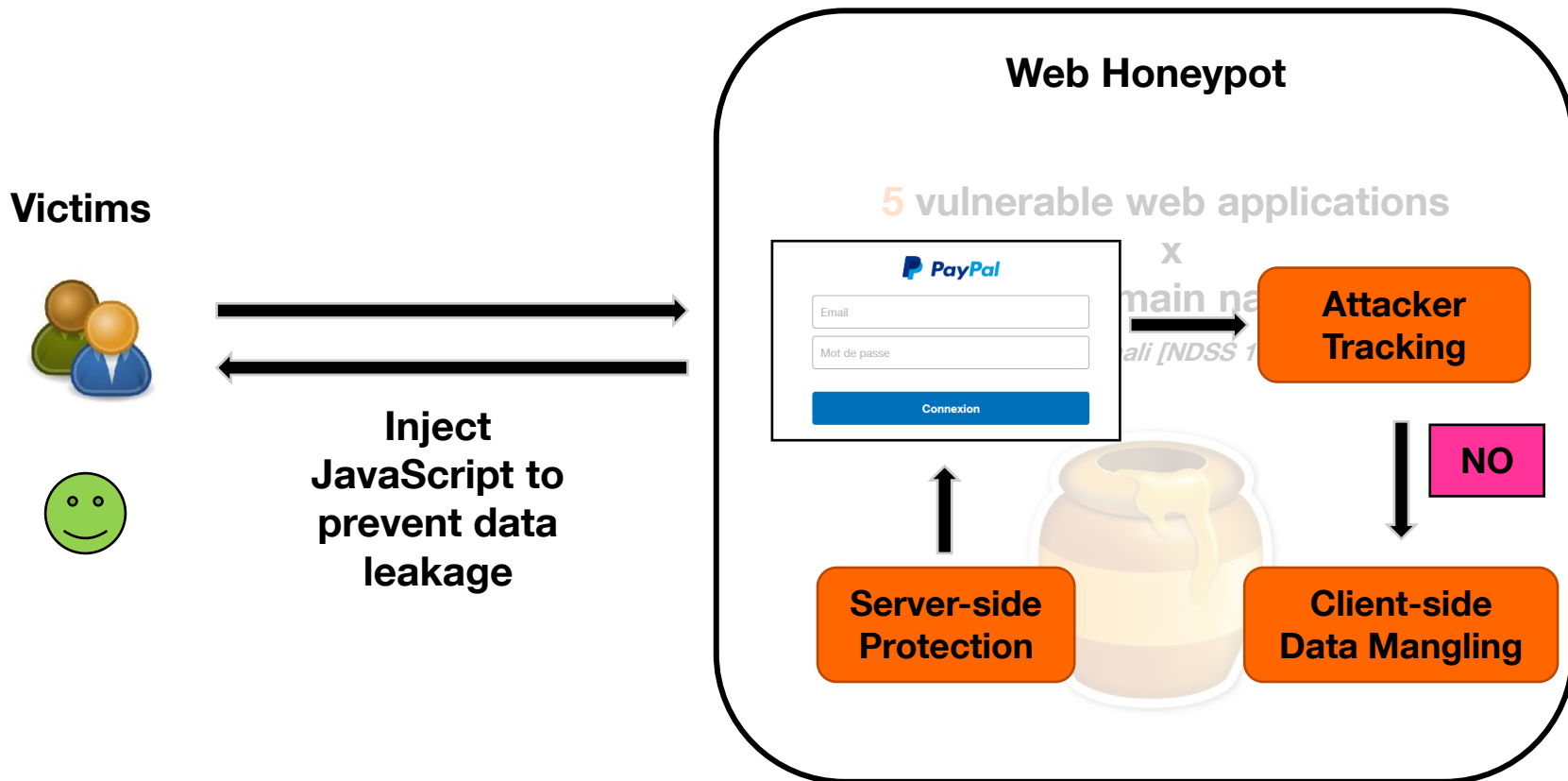
Victims



**Inject
JavaScript to
prevent data
leakage**



Implementation



Overview

- **Five months from September 2015 to the end of January 2016**
- **474 phishing kits (PayPal, Apple, Google, Facebook ...)**



Installation



Upload 1min

Overview

- Five months from September 2015 to the end of January 2016
- 474 phishing kits (PayPal, Apple, Google, Facebook ...)



Installation Testing



Upload 1min 10min

Overview

- Five months from September 2015 to the end of January 2016
- 474 phishing kits (PayPal, Apple, Google, Facebook ...)



Overview

- Five months from September 2015 to the end of January 2016
- 474 phishing kits (PayPal, Apple, Google, Facebook ...)

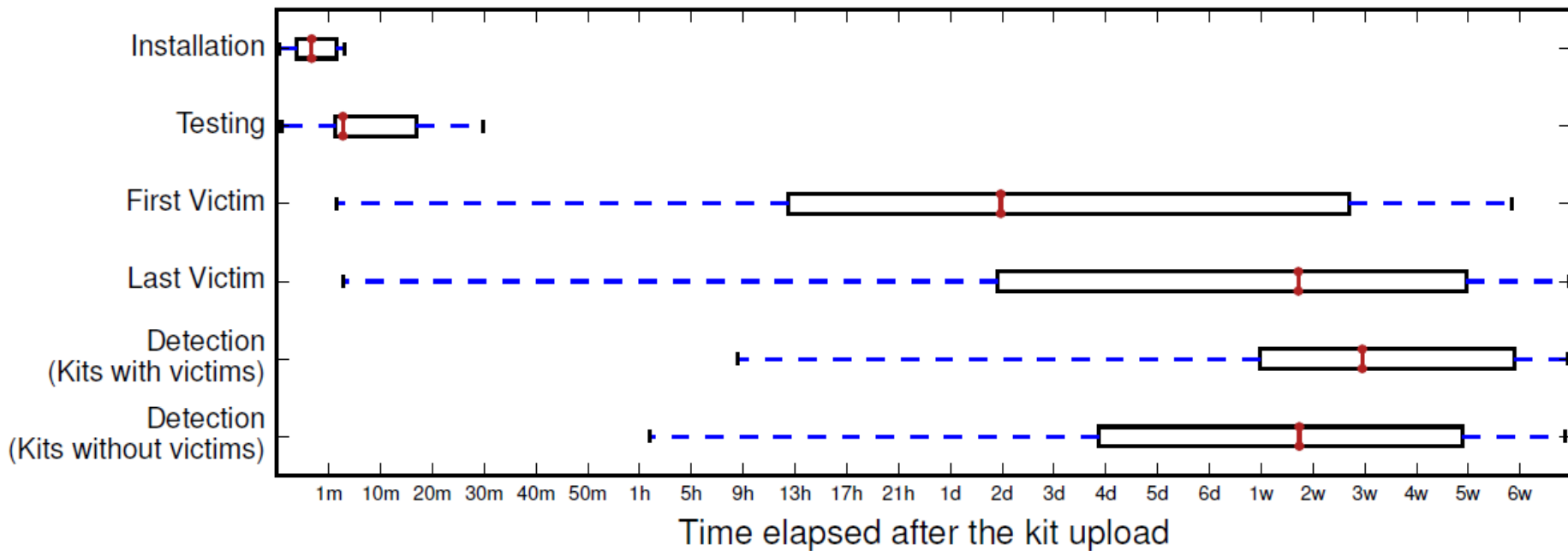


Overview

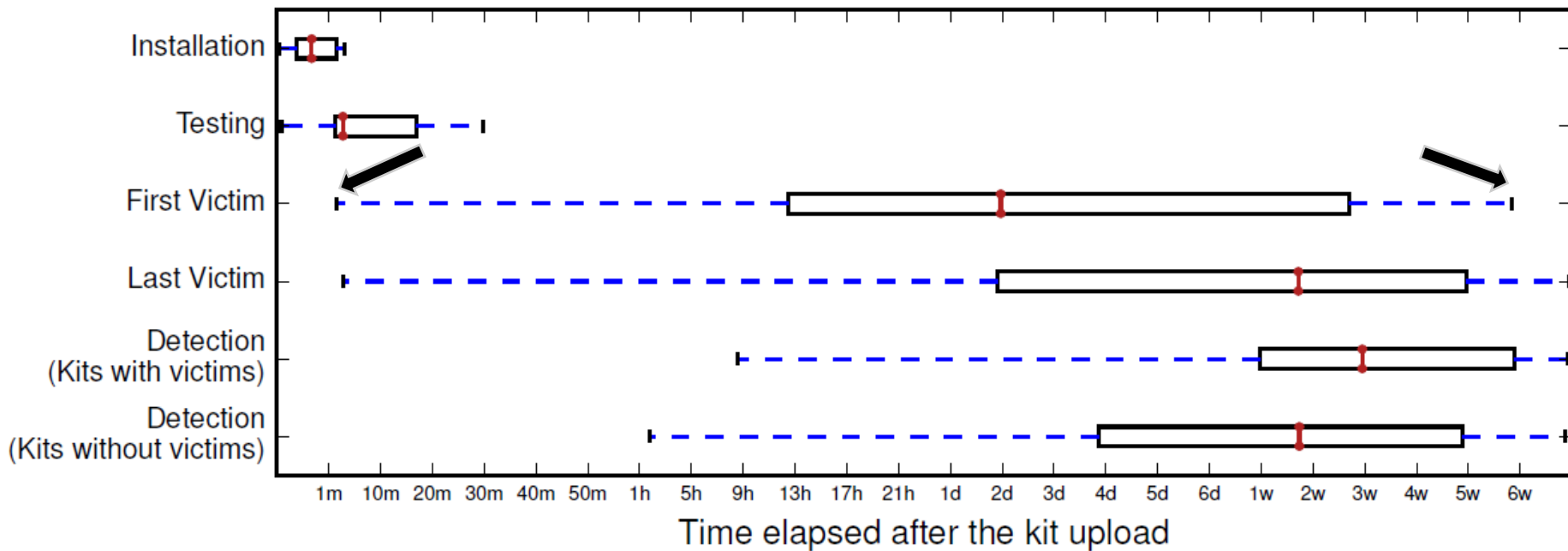
- Five months from September 2015 to the end of January 2016
- 474 phishing kits (PayPal, Apple, Google, Facebook ...)



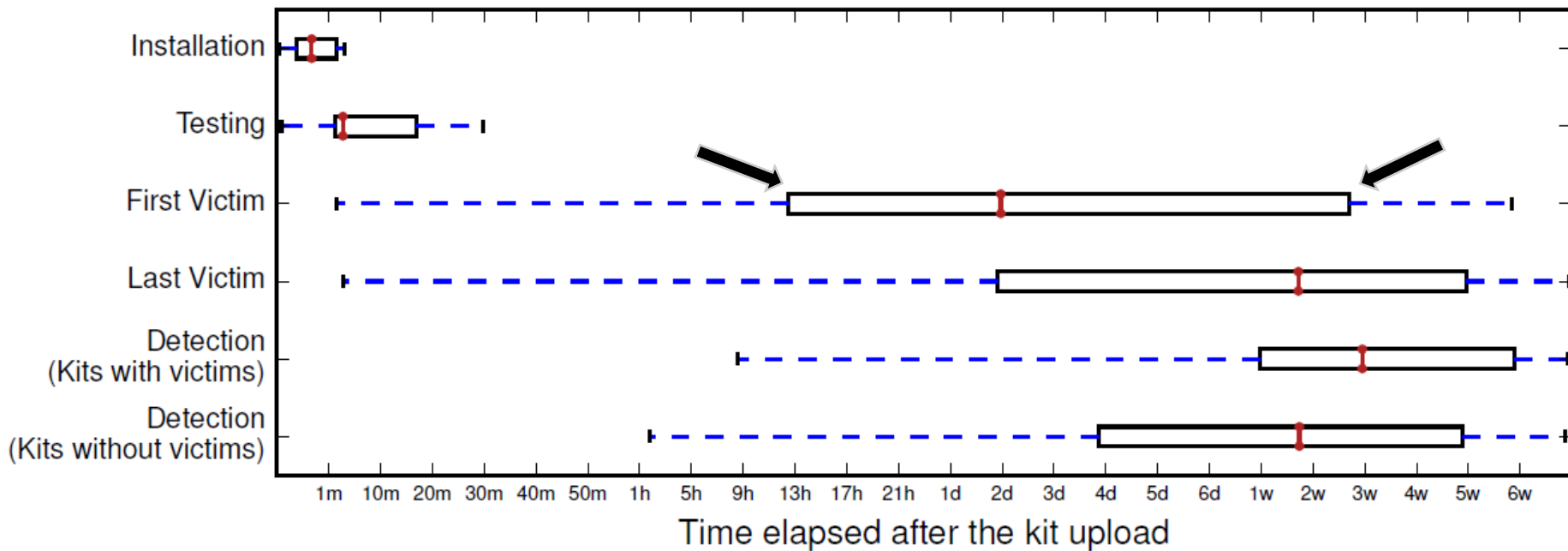
Phishing Attack Global Picture



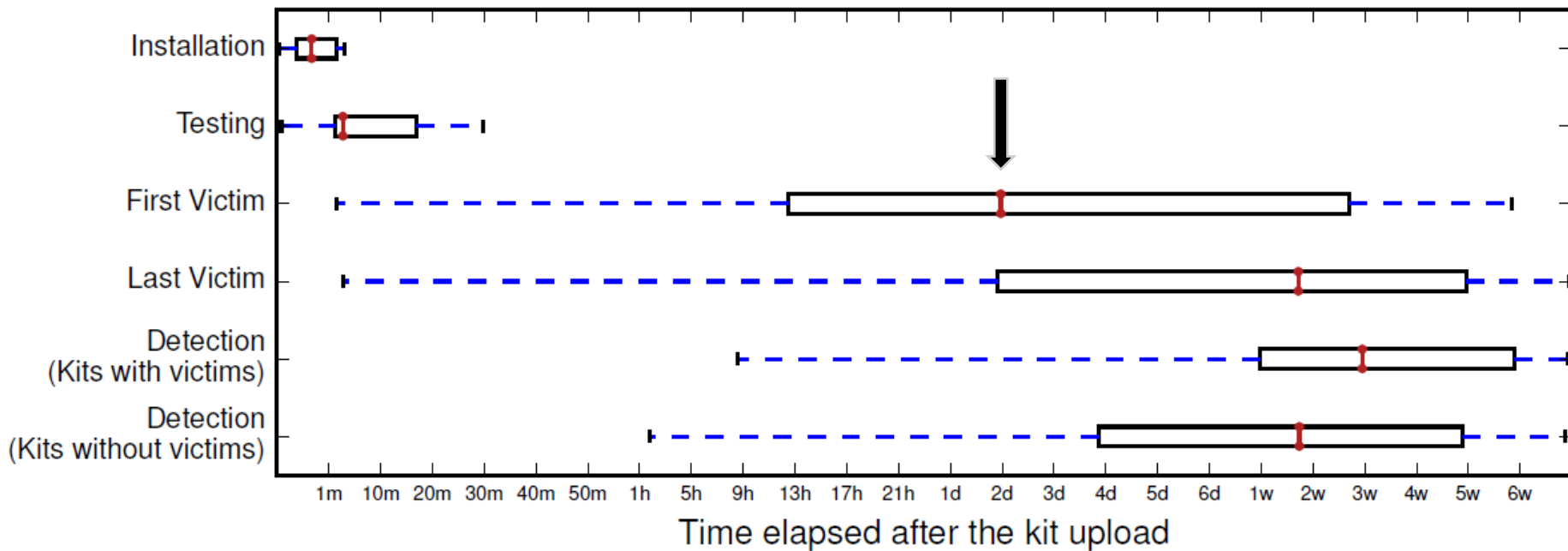
Phishing Attack Global Picture



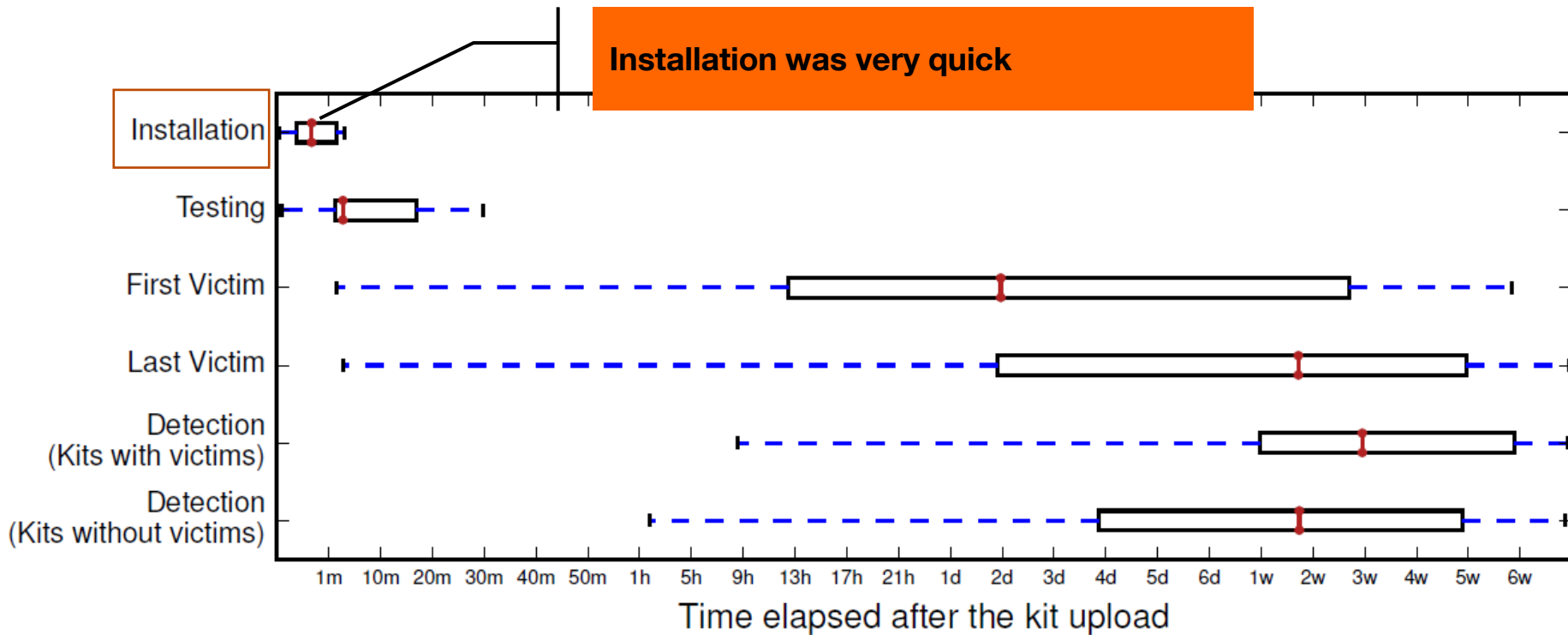
Phishing Attack Global Picture



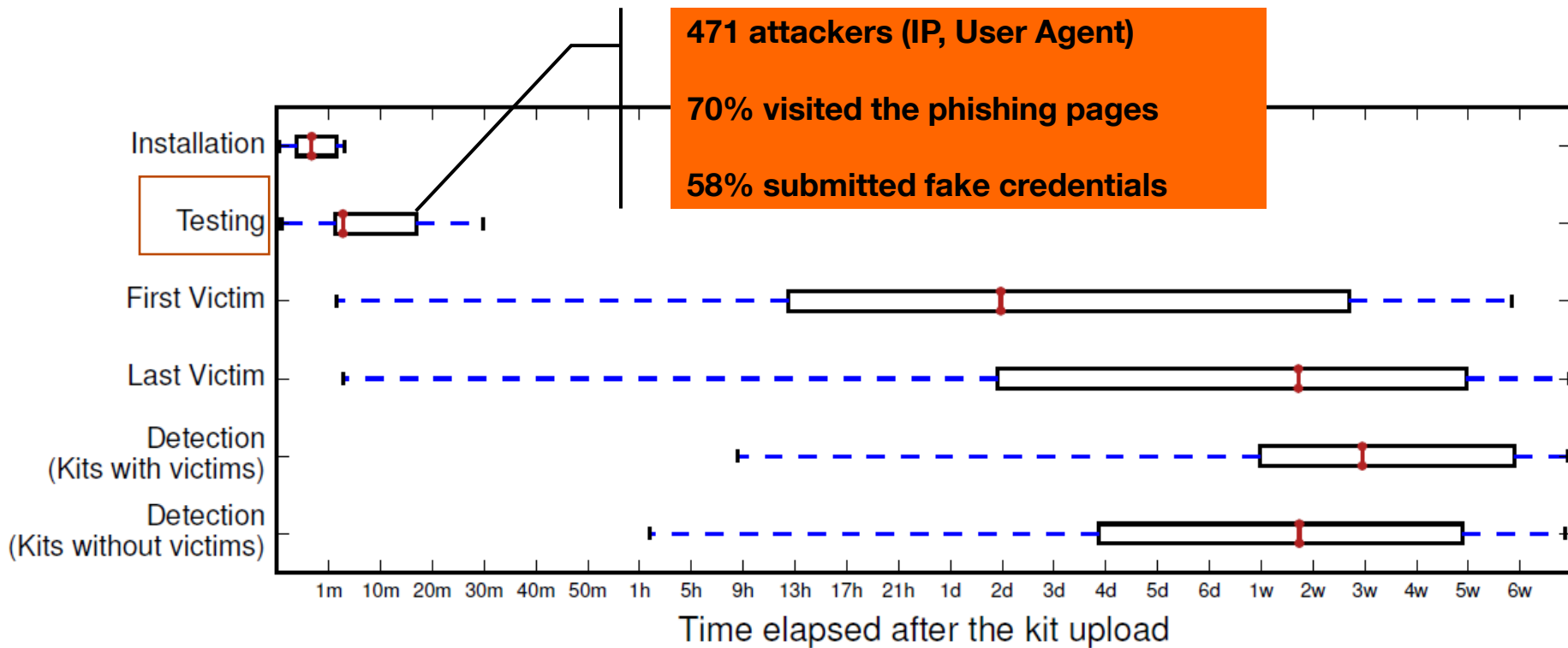
Phishing Attack Global Picture



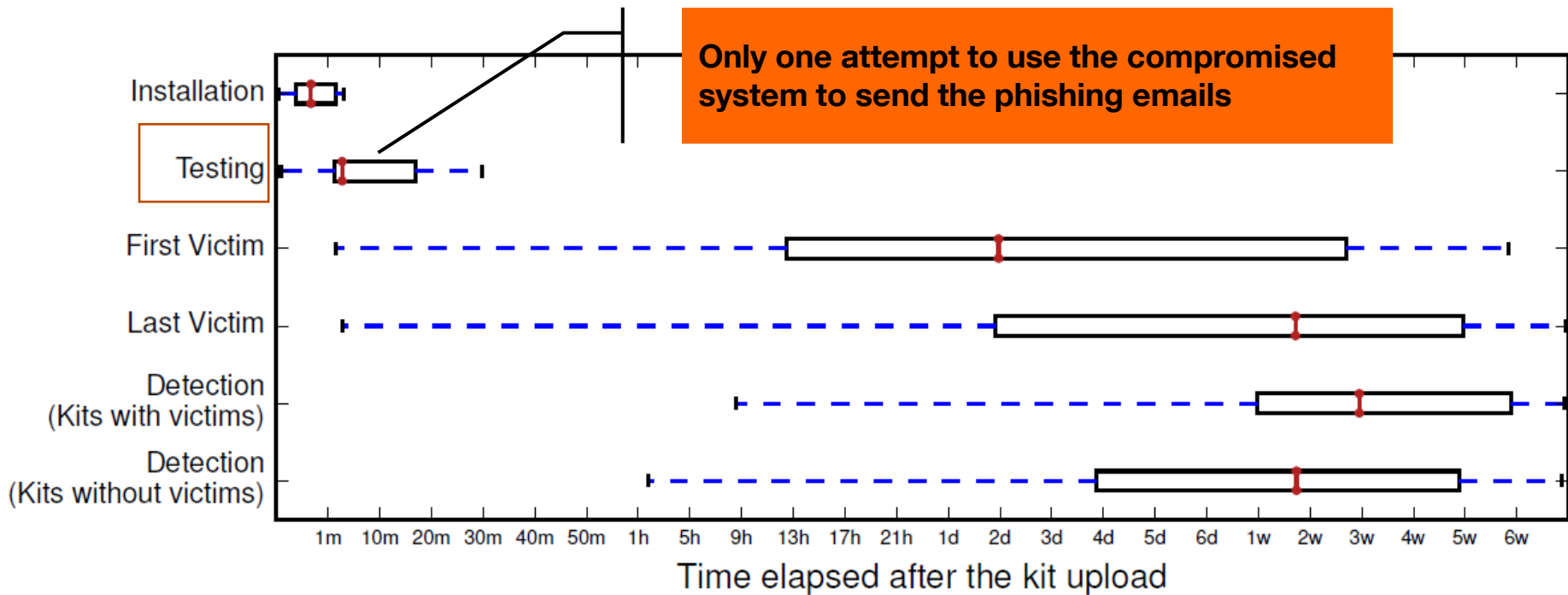
Phishing Attack Global Picture



Phishing Attack Global Picture



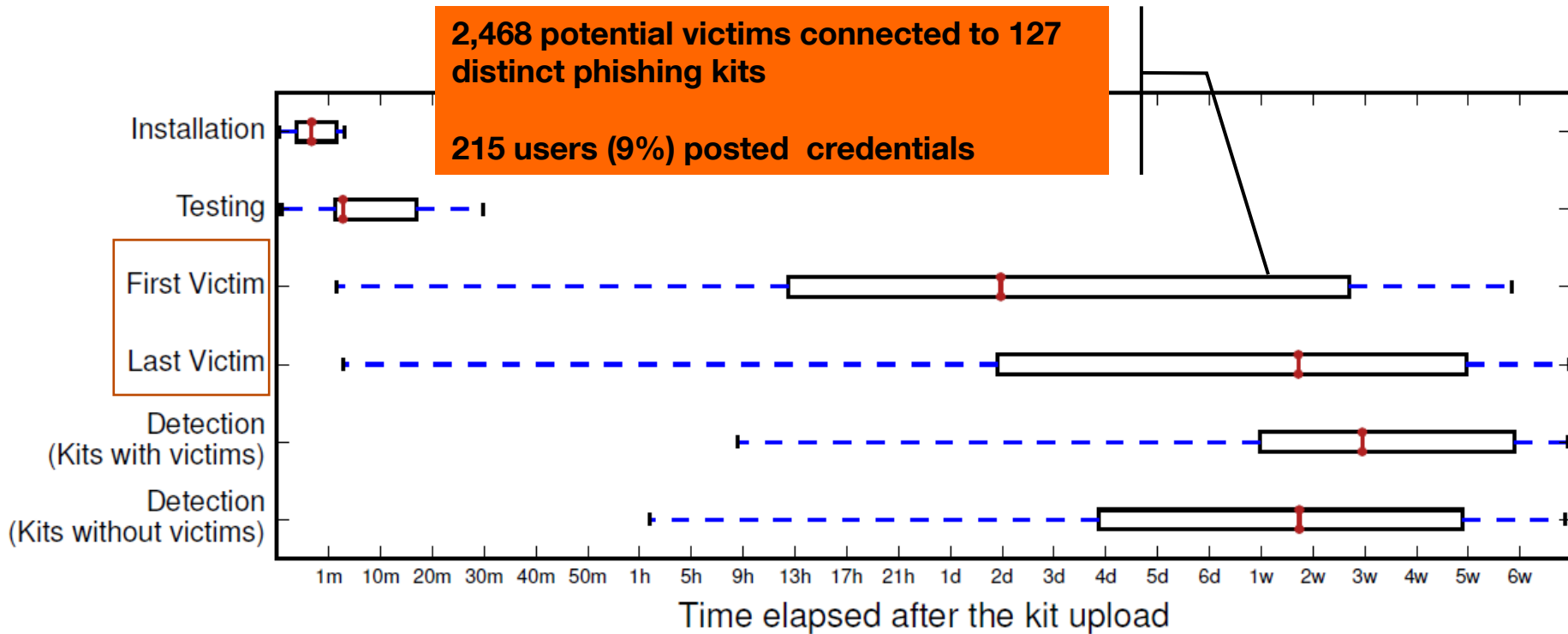
Phishing Attack Global Picture



Phishing Attack Global Picture

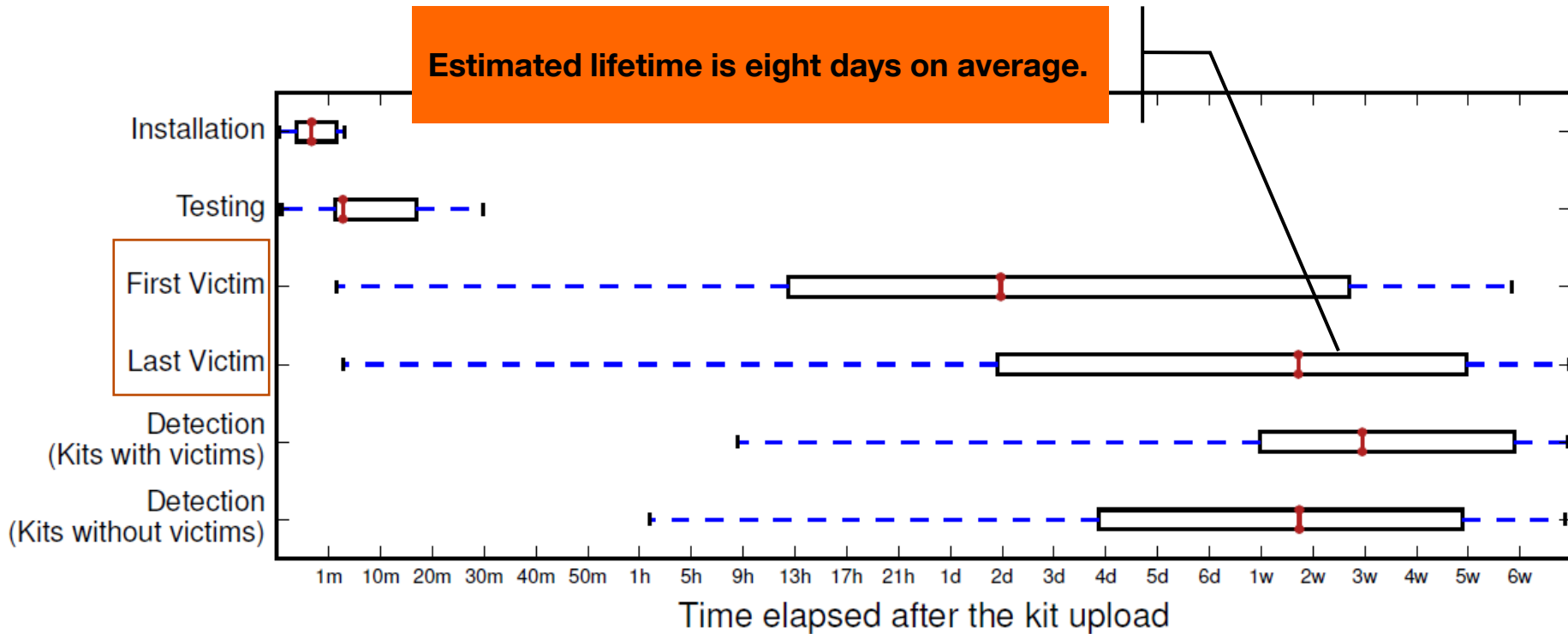
2,468 potential victims connected to 127 distinct phishing kits

215 users (9%) posted credentials

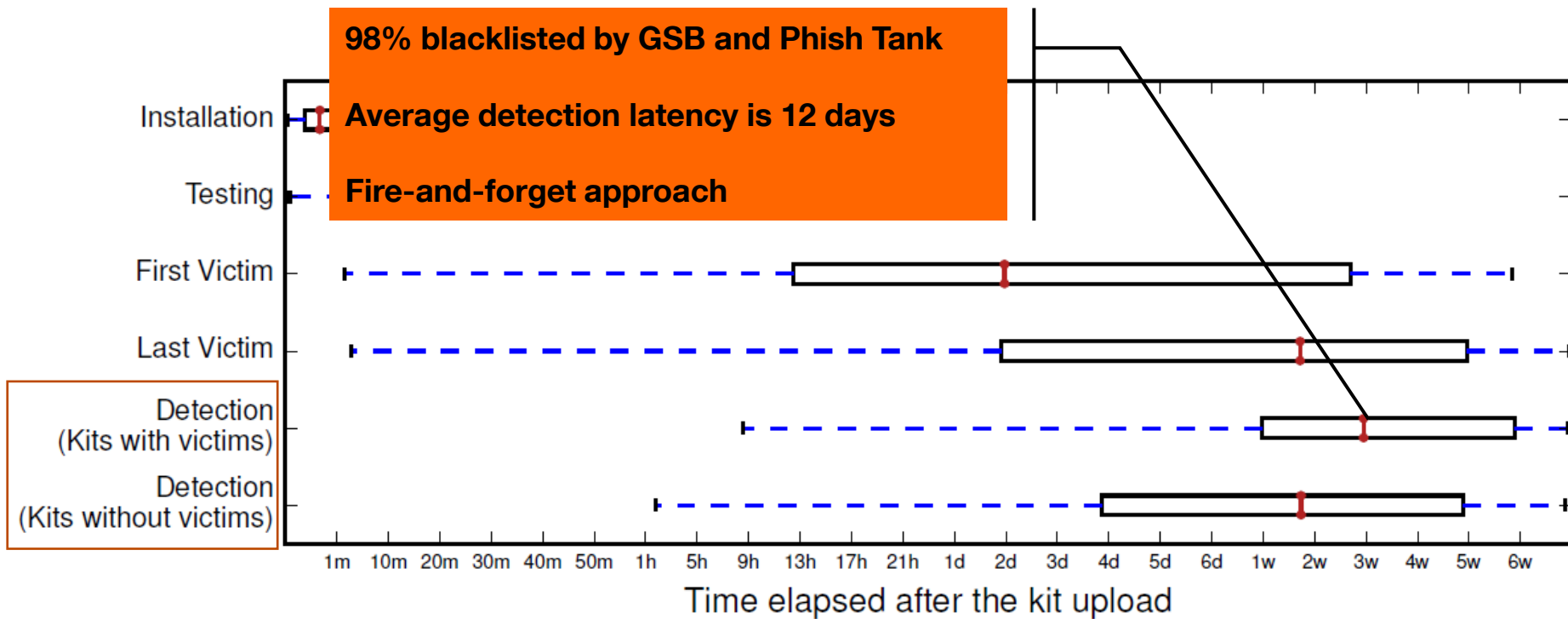


Phishing Attack Global Picture

Estimated lifetime is eight days on average.



Phishing Attack Global Picture



Blacklist Evasion

```
$random=rand(0,1000000000000);  
$md5=md5("$random");  
$base=base64_encode($md5);  
$dst=md5("$base");
```



New connection

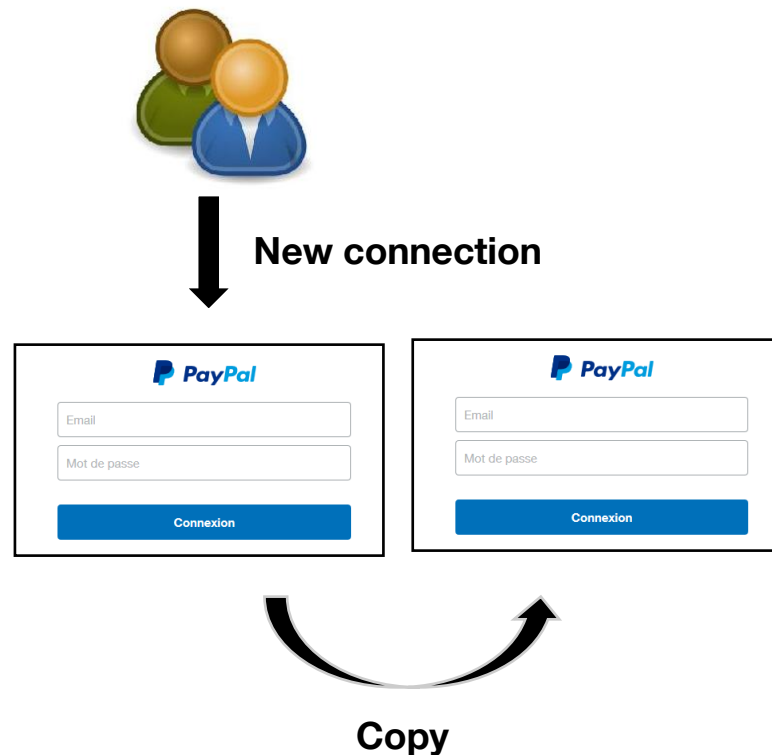
A screenshot of a PayPal login form. At the top is the PayPal logo. Below it are two input fields: "Email" and "Mot de passe". At the bottom is a blue button labeled "Connexion".

Email	<input type="text"/>
Mot de passe	<input type="password"/>
<input type="button" value="Connexion"/>	

Blacklist Evasion

```
$random=rand(0,1000000000000);  
$md5=md5("$random");  
$base=base64_encode($md5);  
$dst=md5("$base");
```

```
$src="source";  
recursive_copy( $src, $dst );
```

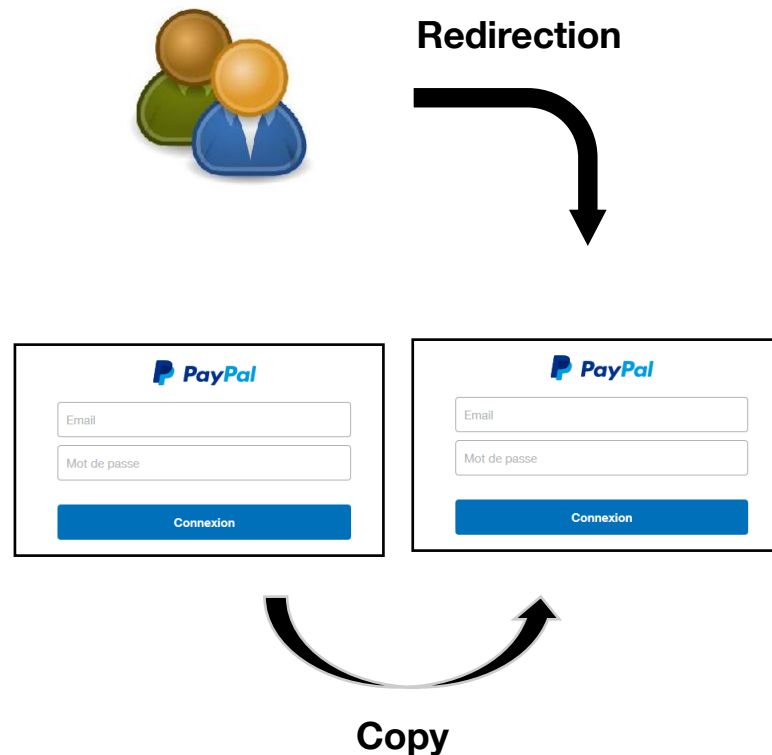


Blacklist Evasion

```
$random=rand(0,1000000000000);  
$md5=md5("$random");  
$base=base64_encode($md5);  
$dst=md5("$base");
```

```
$src="source";  
recursive_copy( $src, $dst );
```

```
header("location:$dst");
```

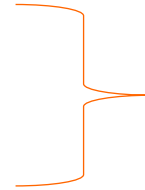


Blacklist Evasion

[12/Nov/2015:18:57:41] 14.xx.xxx.198

GET /kit/ 302

User-Agent: curl/7.25.0



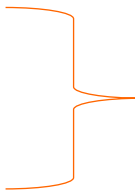
First connection

Blacklist Evasion

[12/Nov/2015:18:57:41] 14.xx.xxx.198

GET /kit/ 302

User-Agent: curl/7.25.0



First connection

[12/Nov/2015:19:01:35] 213.xx.xxx.100

GET /kit/8c5fcf4518e94a9f272d60ee75c309a7 301

User-Agent: Mozilla/4.0

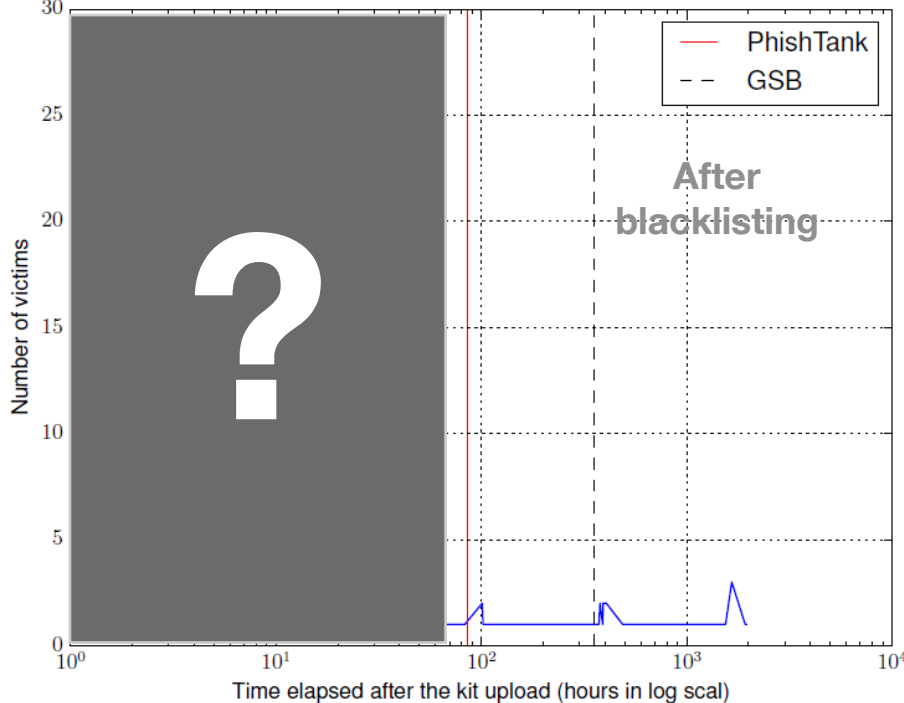
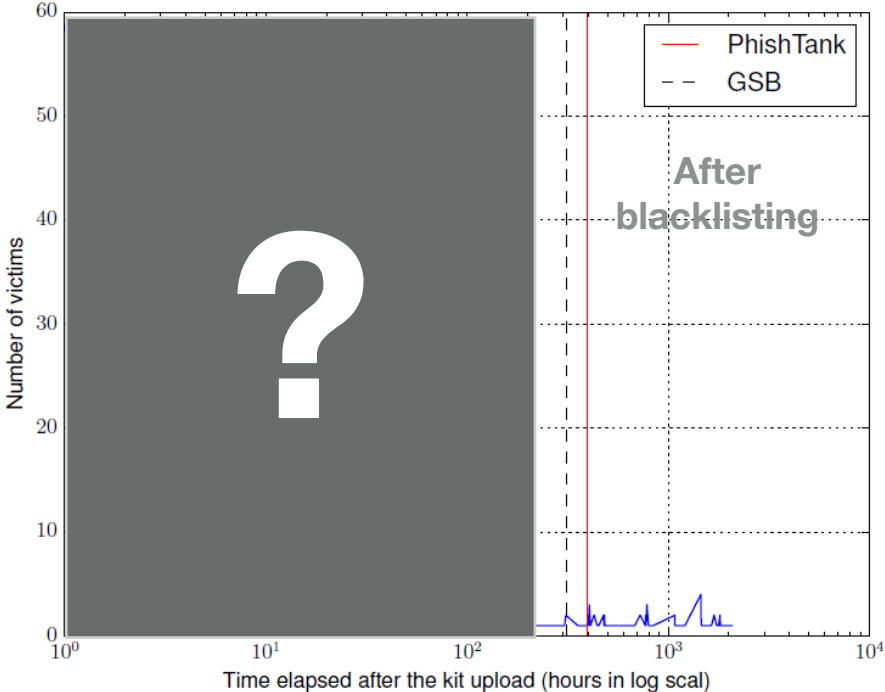
[12/Nov/2015:19:20:45] 213.xx.xxx.100

GET /kit/8c5fcf4518e94a9f272d60ee75c309a7/redirection.php 200

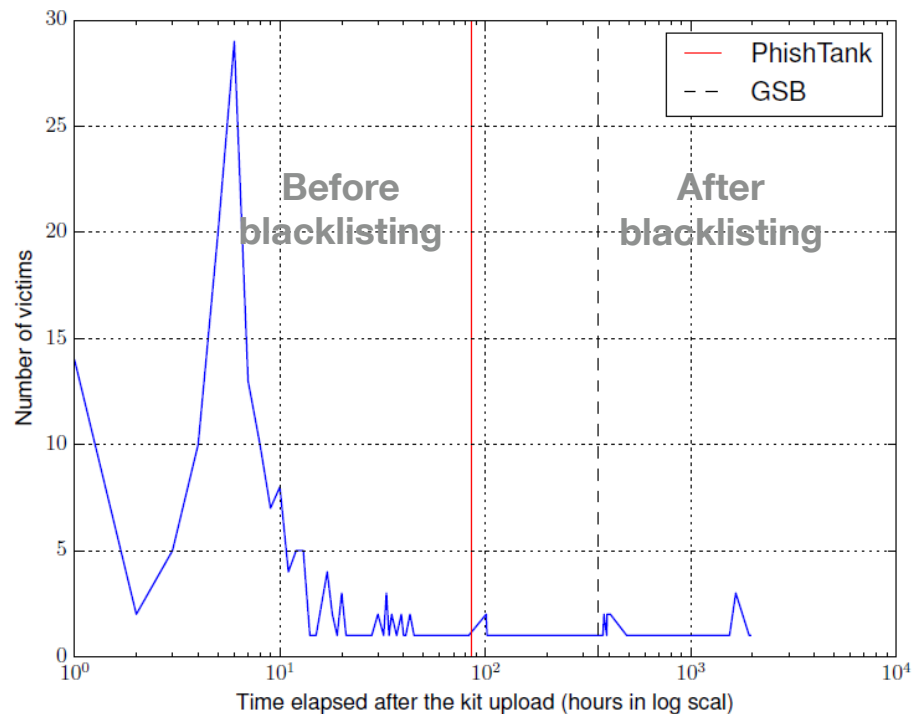
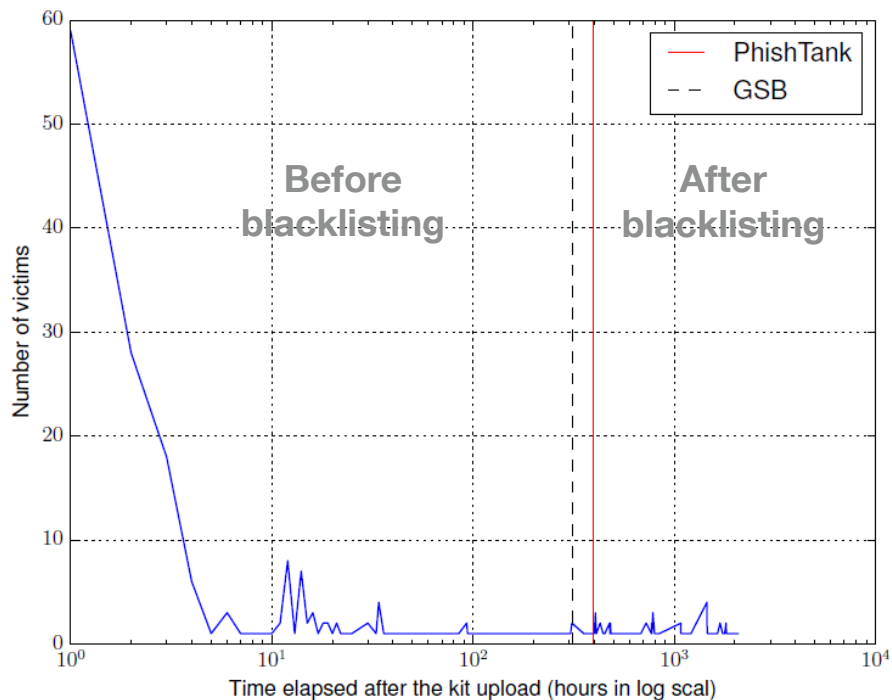
User-Agent: Mozilla/4.0

**Reported
phishing URL**

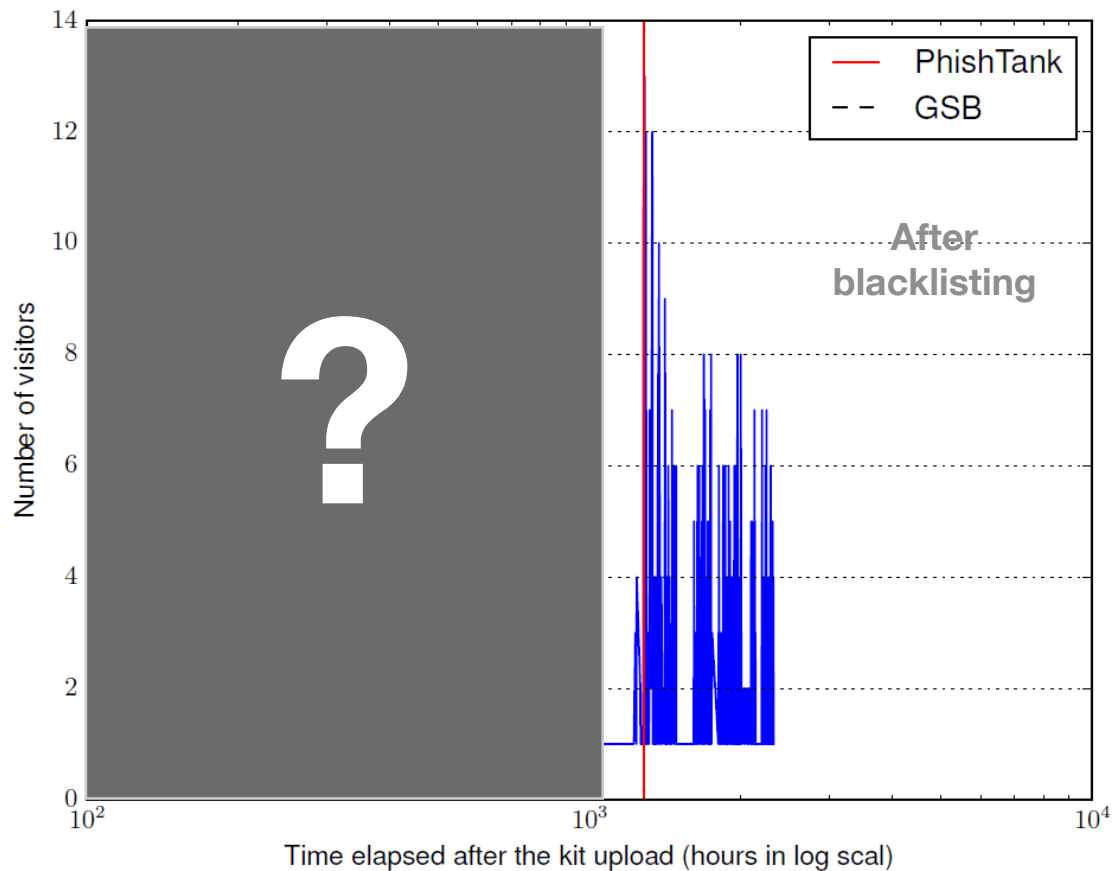
Early Victims



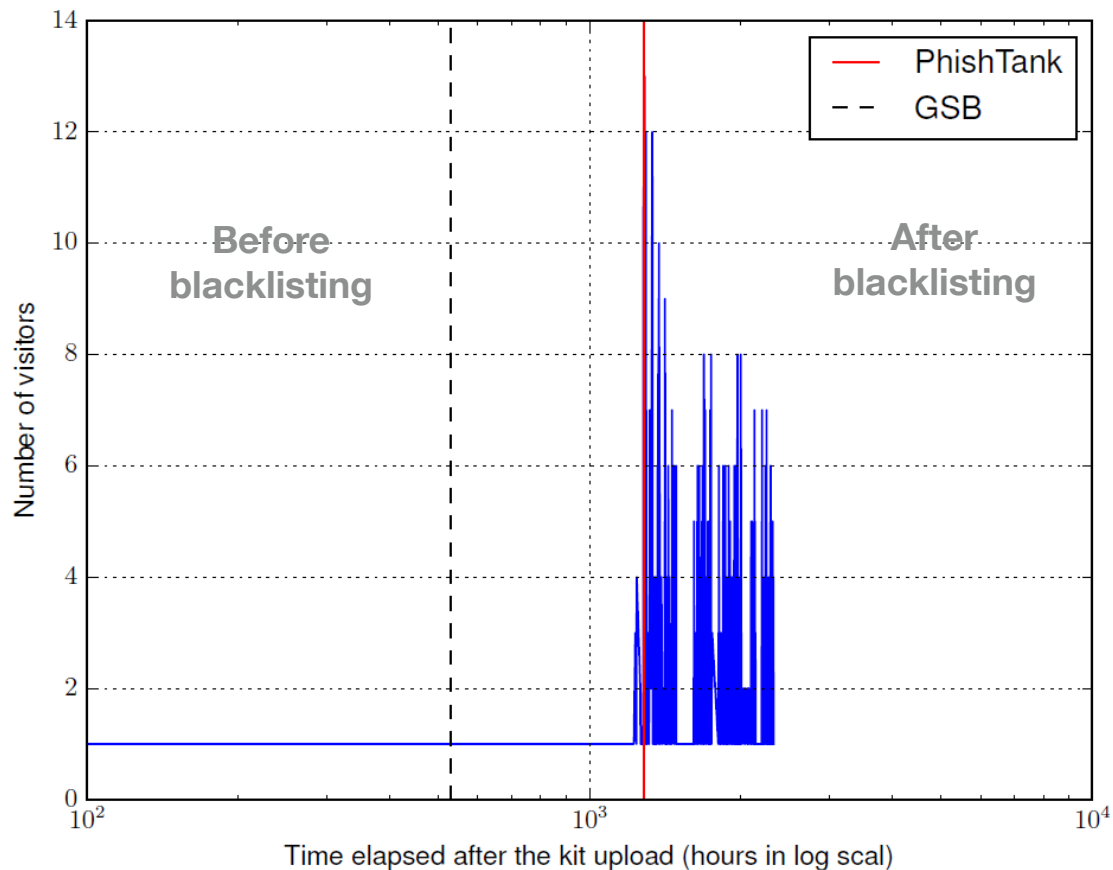
Early Victims



Flash Crowd Effect



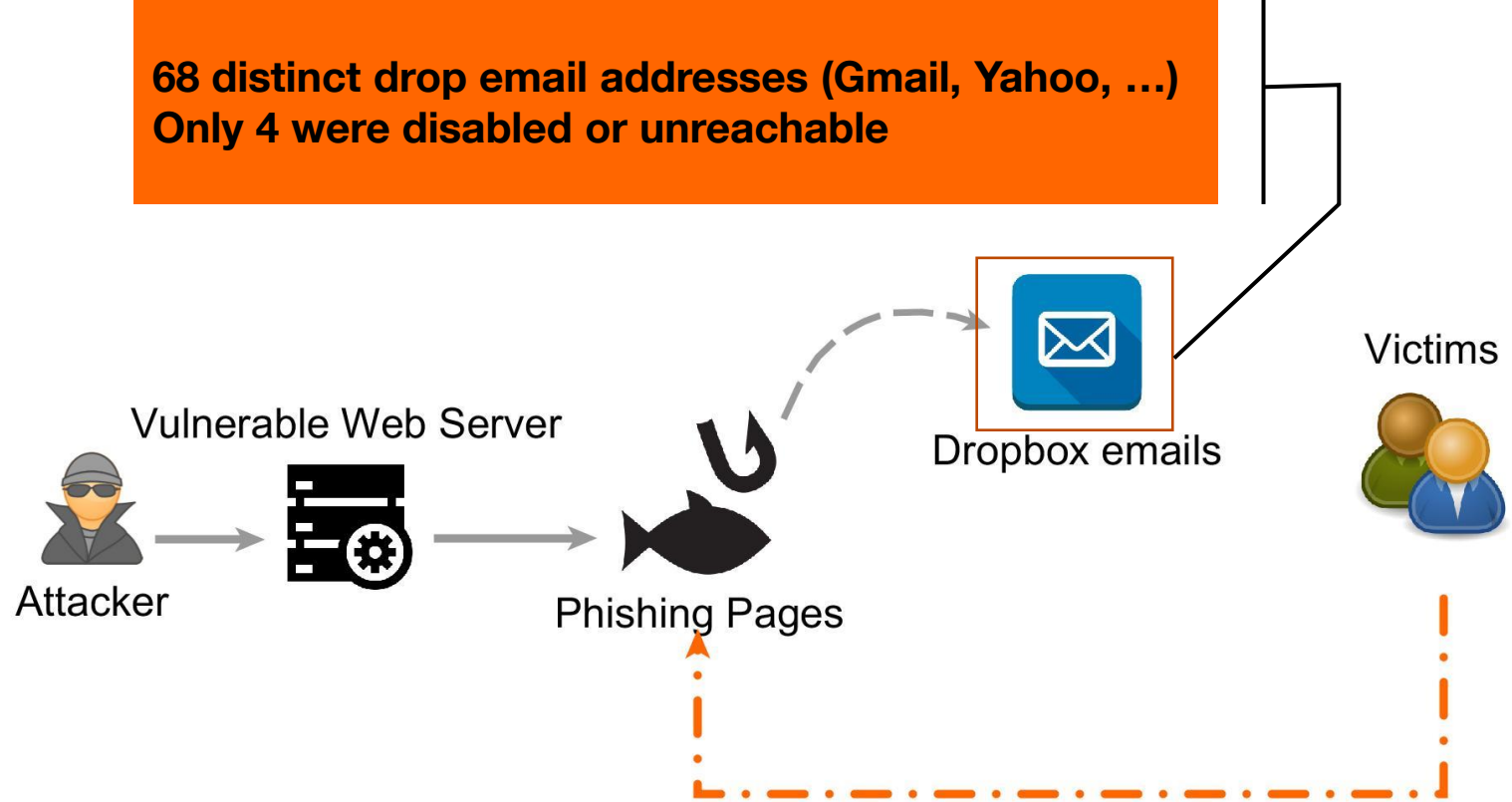
Flash Crowd Effect



- Third party visitors:**
- **Universities**
 - **Security vendors**

Real-time Drop Email Detection

68 distinct drop email addresses (Gmail, Yahoo, ...)
Only 4 were disabled or unreachable



Conclusion

- **Novel approach to sandbox live phishing kits**
- **Observe the entire lifecycle of a phishing kit**
- **Findings**
 - **Attackers manually test their PKs**
 - **Separate hosting and spamming infrastructures**
 - **Many PKs with few victims each**
 - **Blacklist very effective to protect users, but detection is not fast enough**
 - **Attackers move quickly between PKs once they get blacklisted**

Appendix

Elimination of Other Malicious Files

- **Heuristics**
- **Manual classification**

Appendix

Data Exfiltration by Client-Side Side Channels

- **Disguised as a HTML img**
- **Defeated by our client-side protection**