PhishEye: Live Monitoring of Sandboxed Phishing Kits

Xiao Han
Nizar Kheir
Davide Balzarotti
Summary

Motivation

Sandboxed phishing kits

Implementation

Results
Unique Phishing Sites Detected January - June 2016

January: 86,557
February: 79,259
March: 123,555
April: 158,988
May: 148,295
June: 158,782

[APWG Phishing Activity Trends Report 2nd Quarter 2016]
All time high record
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

Technical Subterfuge

Victims
Know your enemy: Phishing [Honeynet 05]

Evil searching [FC 09]
Monetization

Browser plugin: N. Chou [NDSS 04]

User education: P. Kumaraguru [TOIT 10]

Vulnerable Web Server
Attacker
Phishing Pages
Social Engineering
Technical Subterfuge
Victims
Learning to detect phishing emails [WWW 07]

Discovering phishing dropboxes using email metadata [eCrime 12]
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]
Handcrafted fraud and extortion [IMC 14]
Incomplete and fragmented view of PKs lifecycle

Monetization

Vulnerable Web Server

Attacker

Phishing Pages

Social Engineering

Technical Subterfuge

Victims
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 domain names
D. Canali [NDSS 13]

[Diagram showing a visual representation of the implementation process]
Implementation

PK installation

Web Honeypot

5 vulnerable web applications
x
Domain names

Attacker Identification

D. Canali [NDSS 13]
Implementation

Web Honeypot

5 vulnerable web applications
x
100 domain names
D. Canali [NDSS 13]

Attacker Identification

Attacker Tracking
Implementation

Web Honeypot

5 vulnerable web applications
x
Domain names
D. Canali [NDSS 13]

Attacker Identification

Attacker Tracking

YES

Testing

Testing
Implementation

5 vulnerable web applications
×
100 domain names

D. Canali [NDSS 13]

Web Honeypot

Attacker Identification

Attacker Tracking

YES
Implementation

Web Honeypot

5 vulnerable web applications
x
100 domain names
D. Canali [NDSS 13]

Attacker Identification

Attacker Tracking

Checking

Testing

YES
Implementation

Victims

Web Honeypot

5 vulnerable web applications x 100 domain names

Canali [NDSS 13]
Implementation

5 vulnerable web applications × 100 domain names

Victims

Web Honeypot

Attacker Tracking
Implementation

5 vulnerable web applications x 100 domain names

Web Honeypot

Attacker Tracking

Client-side Data Mangling

Victims
5 vulnerable web applications x 100 domain names

D. Canali [NDSS 13]

Web Honeypot

Attacker Tracking

Client-side Data Mangling

Victims

Inject JavaScript to prevent data leakage
Implementation

5 vulnerable web applications x 100 domain names =

Victims

Inject JavaScript to prevent data leakage

Web Honeypot

Attacker Tracking

Client-side Data Mangling

NO
Implementation

Victims

Inject JavaScript to prevent data leakage

Web Honeypot

5 vulnerable web applications

.x domain names

Attacker Tracking

Server-side Protection

Client-side Data Mangling

D. Canali [NDSS 13]
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 ...)

Diagram:

- Installation
- Testing
- First victim

Timeline:
- Upload: 1min
- 10min
- 2 days
Overview

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

Installation: 1 min
Testing: 10 min
First victim: 2 days
Last victim: 10 days
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](image)

- **Installation**
- **Testing**
- **First Victim**
- **Last Victim**
- **Detection (Kits with victims)**
- **Detection (Kits without victims)**

**Time elapsed after the kit upload**
Phishing Attack Global Picture

- Installation
- Testing
- First Victim
- Last Victim
- Detection (Kits with victims)
- Detection (Kits without victims)

Time elapsed after the kit upload
Phishing Attack Global Picture

The diagram illustrates the timeline of events following the kit upload. It includes stages such as Installation, Testing, First Victim, Last Victim, Detection (Kits with victims), and Detection (Kits without victims). The horizontal axis represents the time elapsed after the kit upload, with markers indicating key milestones.
Phishing Attack Global Picture

Installation was very quick
Phishing Attack Global Picture

- 471 attackers (IP, User Agent)
- 70% visited the phishing pages
- 58% submitted fake credentials
Phishing Attack Global Picture

Only one attempt to use the compromised system to send the phishing emails
2,468 potential victims connected to 127 distinct phishing kits

215 users (9%) posted credentials
Estimated lifetime is eight days on average.
Phishing Attack Global Picture

- 98% blacklisted by GSB and Phish Tank
- Average detection latency is 12 days
- Fire-and-forget approach
$random=rand(0,100000000000);
$md5=md5("$random");
$base=base64_encode($md5);
$dst=md5("$base");
Blacklist Evasion

```php
$random = rand(0, 100000000000);  
$md5 = md5("$random");  
$base = base64_encode($md5);  
$dst = md5("$base");  

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

```php
$random = rand(0, 100000000000);
$md5 = md5("$random");
$base = base64_encode($md5);
$dst = md5("$base");

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

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

GET /kit/ 302
User-Agent: curl/7.25.0

First connection
Blacklist Evasion

GET /kit/ 302
User-Agent: curl/7.25.0

GET /kit/8c5fcf4518e94a9f272d60ee75c309a7 301
User-Agent: Mozilla/4.0

GET /kit/8c5fcf4518e94a9f272d60ee75c309a7/redirection.php 200
User-Agent: Mozilla/4.0
Early Victims

A phenomenon is observed where, after blacklisting, there is a significant reduction in the number of victims. The graphs illustrate this by showing a sharp decline in the number of victims after the blacklisting period.
Early Victims

Before blacklisting
After blacklisting

Before blacklisting
After blacklisting

PhishTank
GSB

Number of victims

Time elapsed after the kit upload (hours in log scal)

Number of victims

Time elapsed after the kit upload (hours in log scal)
Flash Crowd Effect

After blacklisting
Flash Crowd Effect

Third party visitors:
- Universities
- Security vendors

After blacklisting

Before blacklisting

Number of visitors

Time elapsed after the kit upload (hours in log scal)
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