The background of the slide is a dark, atmospheric photograph. It shows a hallway or stage area with heavy, dark red curtains hanging from the top. A spotlight is cast onto the floor in the center, creating a bright circular area. The overall mood is mysterious and dramatic.

# Phishing-as-a-Service, AI and Real-time phishing, the Underground Card Shop's Arsenal against 3DSecure

2025-03-15 DEVCORE CONF.

Godiva Donut & Strawberry Donut



## Godiva Donut

Ent. CSIRT's Blue Team, Detection Engineering, Threat Intelligence, Incident & Response. HITCON (Hacks in Taiwan Conference) volunteer. chroot study group member.



## Strawberry Donut

Data Scientist focused on Fraud Detection. Operationalized multiple fraud detection ML pipelines.

Researching the underground world as a hobby.  
Please protect our identity. Slides will be released.

An abstract graphic on the left side of the slide, featuring a dark background with vibrant red geometric shapes. These shapes include triangles and polygons that overlap and intersect, creating a complex, crystalline structure. The red light effect gives it a sense of depth and movement.

## Agenda

- The Underground card shops business  
產業現況和分工：AI 和技術進步帶來挑戰
- No-OTP Phishing vs.  
Real-time Phishing 同步魚：中間人攻擊
- PhaaS: Phishing-as-a-Service & Case Study  
魚塘：雲端代管訂閱制釣魚網站平台 案例
- Detection & Countermeasures
- Conclusion & Next Steps

## Disclaimer

**This research is conducted in  
full compliance with the law,  
and no criminal activity was  
involved.**



The background of the slide is a solid black field. Overlaid on this are several horizontal streaks of bright red light. These streaks are blurred, giving them a sense of motion or a long-exposure photograph. There are three main groups of these red streaks, one in the upper left, one in the upper center, and one in the upper right. Below each of these groups, there are several thinner, more distinct red lines that appear to be part of the same light trails. The overall effect is mysterious and high-tech.

# The Underground card shops business

In Taiwan, card fraud caused 3.2 billion TWD lost in 2023.  
Over 12.4 billion TWD all kinds of scam lost in 2024.

## 聯卡中心：2023年詐欺通報金額衝破32億元 年增47%

2024.02.21 / 18:36 / 工商時報 孫彬訓

#聯卡中心

#詐欺通報金額

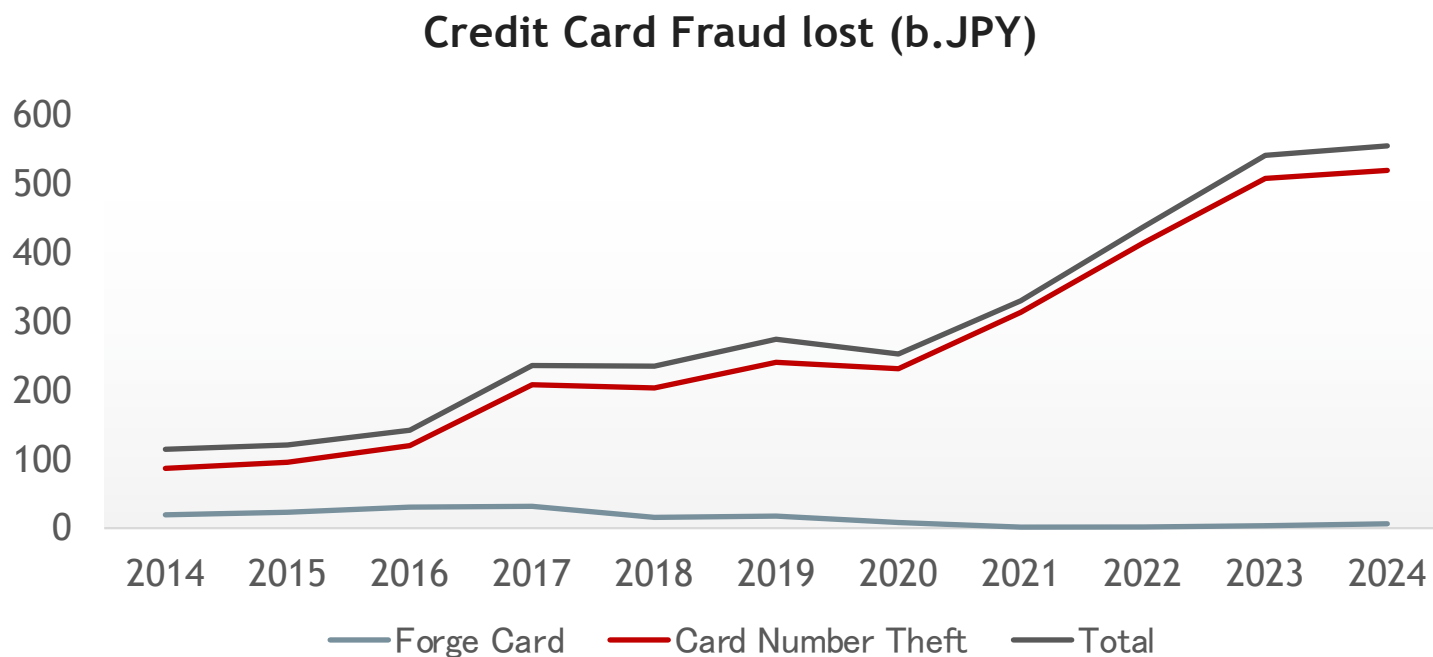
#信用卡



國內發卡機構詐欺通報趨勢。圖／聯卡中心提供

聯合信用卡處理中心統計出爐，2023年國內發卡機構詐欺通報金額達32億9,816萬元，相較2022年22億3,823萬元，增加10億5,993萬元，年增率達47.4%，呈現增長趨勢，續創歷史新高。

In Japan, credit card fraud reached 55 billion yen in 2024, the highest amount ever.



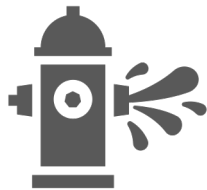
Source: 日本クレジット協会

# Methods to acquire credit card info

Server hacked

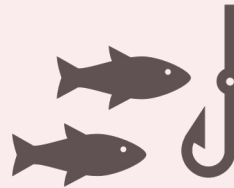


JavaScript  
Injection

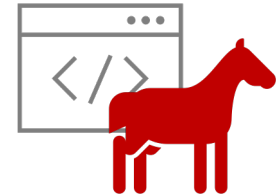


Data Breach

User hacked



Phishing

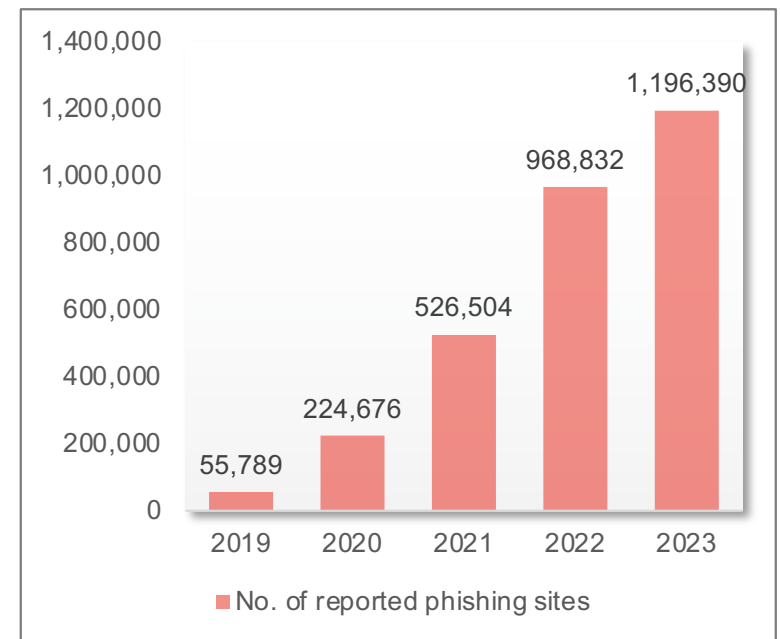


Trojan  
Malware

# AI's Impact: Lowering costs & increasing incentive for phishing attacks

- LLM-assisted social engineering phishing emails have higher click-through rates compared to those created by humans.
- LLM can automate phishing generation, cutting labor costs by 95% (20x faster)
- A phishing site can be made or updated with LLM in a few mins

Phishing sites grew 20X in 5 years



Source:

- Devising and Detecting Phishing Emails Using Large Language Models, IEEE
- フィッシング対策協議会

「Amazonを不正利用された」——SNS上で報告相次ぐ  
「二段階認証を突破された」などの声も

## Amazon Misused - Reports Flood Social Media: 'Two-Factor Authentication Bypassed'

「Amazon.co.jpを不正利用された」——X（元Twitter）では9月上旬からそんな投稿が相次いでいる。「Amazonギフトカードを大量購入された」「二段階認証を設定していたのに、それを突破された」などの報告が上がっている。



NHK 事件記者 / 取材 note

“10分間で736万円” 不正送金の被害

73.6 Million Yen Fraudulent Transfer in 10 Minutes



Goal: to understand the structure of Real-time phishing,  
and how it changed the phishing value chain



# Chinese card shop ecosystem targeting APAC

## APAC is one of the main targets of credit card fraud

- Lots of Leaked Data in the dark web
- Lower Language barrier: to send out phishing sites & cooperate with local criminals
- Cheap Price for sim card purchase
- Lots of card fraud marketplaces in the dark web (IRC/Forum → QQ/WeChat → TG)



**Goal: to understand the value chain of Chinese carding fraud**



# Online Training



## 【第一章】（第一课） CVV盗刷教学

（第一课）C料如何获得

（第二课）通道如何获得

（第三课）环境如何搭建

（第四课）产品转运方式

（第五课）产品变现方法

（第六课）如何自建鱼塘

（第七课）如何群发邮件

（第八课）如何获得数据

（第九课）银行入侵改3D

（毕业总结）毕业篇小问题总结

### 【鱼料】

利用钓鱼源码模拟成主流人群使用的克隆网站，引诱受害者填写大量详细的信用卡和个人资料，其中包含卡号信息3D支付密码信息，账单地址，邮箱账号密码，受害者受害IP，浏览器指纹信息等等，信息更全，用途更广，好的鱼料深受人们的喜爱，但是相应的价格也会很高，一般在100-200不等。

### 【鱼料的结构】

```
#-----[ Amazon账号 ]-----#
Amazon账号 :masahito_genki@yahoo.co.jp
Amazon密码 :jmckg962
#-----[ 信用卡信息 ]-----#
银行 : RAKUTEN KC CO., LTD.
品牌 : VISA - CREDIT
等级 : TRADITIONAL
卡一下名義人: Nagai masahito
卡一下番号 : 4297690102170893
有効期限 : 8/2025
CVV : 664
#-----[ 3D密码信息 ]-----#
Web ID : Mmasahito88522
Password 3D : Tmckg0033
#-----[ 账单信息 ]-----#
氏名 : 永井優人
都道府県 : 千葉県
住所1 : 船橋市前原東5-5-18
住所2 : 戸建
郵便番号 : 274-0824
生年月日 : 1962-9-9
電話番号 : 080-3915-0840
#-----[ 指纹信息 ]-----#
IP Address: 60.76.134.132
IP Region: Chiba
IP City: Ichikawa
IP Continent: Asia
IP Timezone: Asia/Tokyo
OS/Browser: Android / Handheld Browser
User Agent: Mozilla/5.0 (Linux; Android
```

### 料主提供

真正的鱼料料主多数是自己假设鱼站，成本也是不小，所以日本的鱼料大致价格在120-200不等，美国的相对低一些也不会差很多，80-150都有。  
个人建议不要入手低于100一条的料，尤其是不熟悉的料商。如果各位真的需要购买，可以先咨询一下客服，打听一下群里兄弟，看看这个料主名声如何再入手。

### 自建鱼塘

有时候很多人想着节省成本，也想去钓鱼群发降低成本，其实钓鱼当中存在很多技术问题，平凡的更替源码，做防红，群发数据采购，群发邮件SMTP协议。邮局调试等等都是技术活和辛苦活，每个人精力有限，不能又钓鱼又刷货，最后两边都搞不好，如果有一些基础，可以慢慢探索和学习尝试成为一名料主，如果没有一些基础的技术知识，那就从基础做起，不要好高骛远，先多看视频多学习，感觉掌握一些技巧之后，花点钱买点料，跳过技术门槛，直接刷货，发货就变现，赚钱了稳定了，形成良好循环了，再想去尝试学习钓鱼也不是不可以。  
自建鱼塘也就是所谓的搭建服务器--调试源码--群发邮件--上鱼，这种方式当然是最好的，因为是你自己钓的，除了你和受害者，谁也不知道料的信息，所以料能放住，这很重要。

### 料站购买

料站靠谱的不多，当然也有一些老牌子料站，这里不打广告，料站需要用虚拟币充值余额，再用余额购买，有一些料站是自带测试接口的，如果购买之后测试是死亡，会退给你余额，你可以重新购买，但是经常会遇到测试不准确，一条料几十美金打水漂，况且靠谱的料站多数是老外的，售后相对麻烦。

### 黑市购买

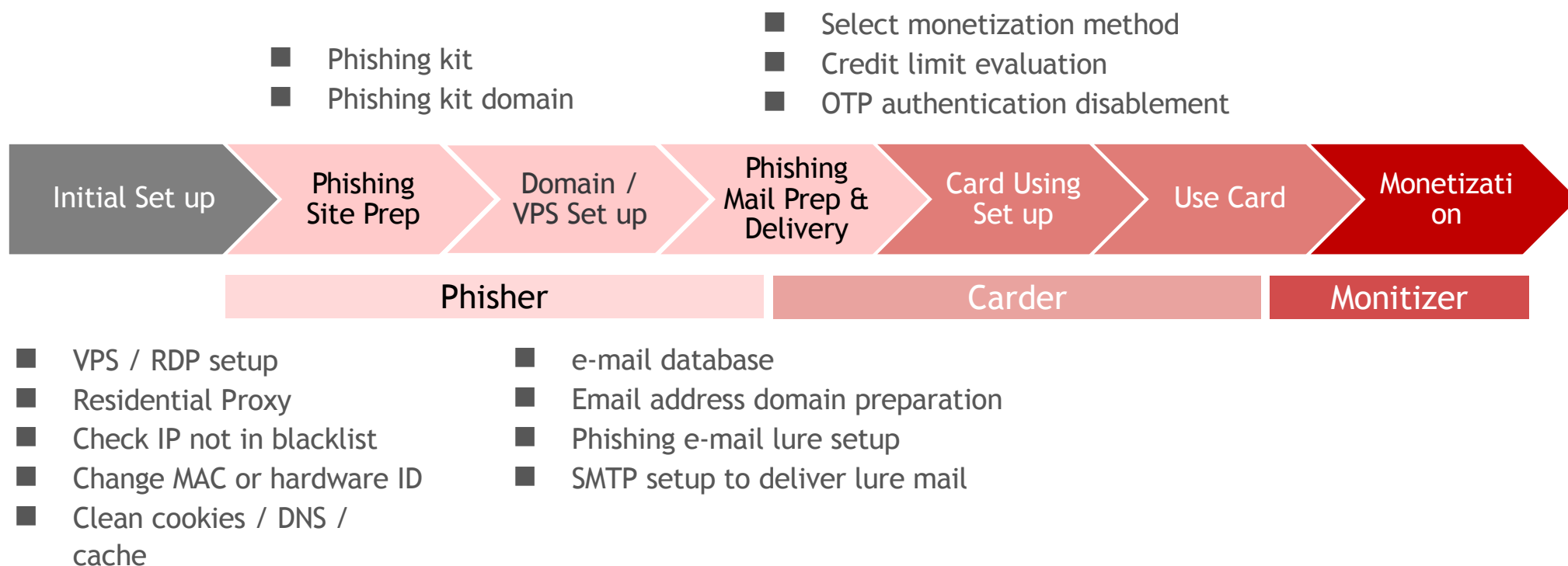
黑市购买相对来说能靠谱一些，与料站的auto自选采购模式不同，黑市是B2C模式交易，类似淘宝，由平台制衡双方交易和调节，最有代表性的网站当然是目前最大的阿尔法。前几年关了，现在起死回生，由当年的程序员重新开放，推荐去逛一逛。

### 自由者联盟担保下单

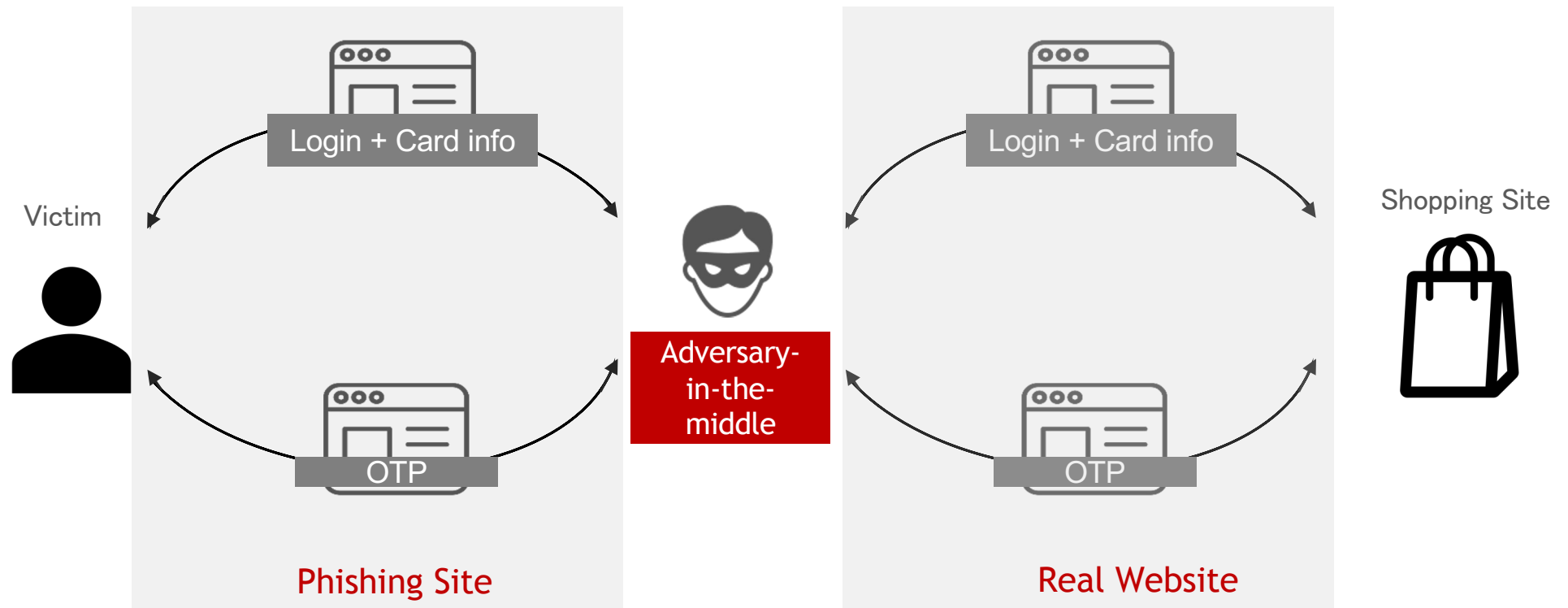
如果实在不放心，也可以在自由者下单，主选项有CVV买卖，平台不收取利润，只负责垫付担保金的商家发站和更新卡头，如果各位购买之后发现问题，自由者客服介入调解，确定问题如果归商家，直接扣除担保金补偿客户，这一点比较人性化，所以各位可以放心。

No-OTP Phishing vs.  
Real-time Phishing 同步魚(中間人攻撃)

# No-OTP Phishing 傳統流程：從釣魚網站、盜刷到套現



## Real-time Phishing 同步魚 became popular since 2020~



CN Actors called the TTP Real-time Phishing 同步魚 while Microsoft referred it as Adversary-in-the-middle Phishing.

<https://www.microsoft.com/en-us/security/blog/2023/06/08/detecting-and-mitigating-a-multi-stage-aitm-phishing-and-bec-campaign/>

Victim



Linkt

?

Please bind the payment card number

Name on card \*

afsafs

Credit card \*

4205420542054205

Card Expiry(MM/YY) \*

11/23

Security Code \*

....

All required field \*

VISA

AMEX

Apple Pay

Google Pay

Submit

Need help?

Operated by

Transurban



Adversary-  
in-the-  
middle

```
#-----[ 信用卡详情 ]-----#
银行      : visa
卡主名字   : YUUDAI
卡号       : 4897 1196
到期日     : 7/2025
cvv        : 393
#-----[ 3D 密码 ]-----#
web ID : yuudai0411205@gmail.com
Password 3D : aiai0331
#-----[ 个人信息 ]-----#
姓名       : 勇大
所在州     : 東京都
地址1      : 江戸川区中葛西
地址2      : 1703
国家       : Japan
邮编       : 1340083
生日       : 2000-4-
手机号码   : 0701-186
#-----[ 指纹信息 ]-----#
ip : 42.147.160.162
UserAgent : Mozilla/5.0 (iPhone; CPU iPhone OS 14_7_1 like Mac OS X) Apple
(KHTML, like Gecko) Version/14.1.2 Mobile/15E148 Safari/604.1
Region : Edogawa
Time Date : 14:07:33 13/09/2021
#-----#
卡号       : 4897 1196
到期日     : 7/2025
cvv        : 393
生日       : 2000-4-11
手机号码   : 070186
```



# Actor 後台：

来新订单了，请及时处理！

0.02 / 0.11

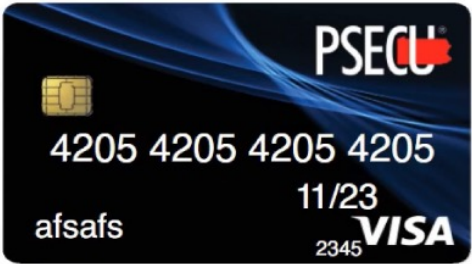


AU-ETC发财后台 V1.0

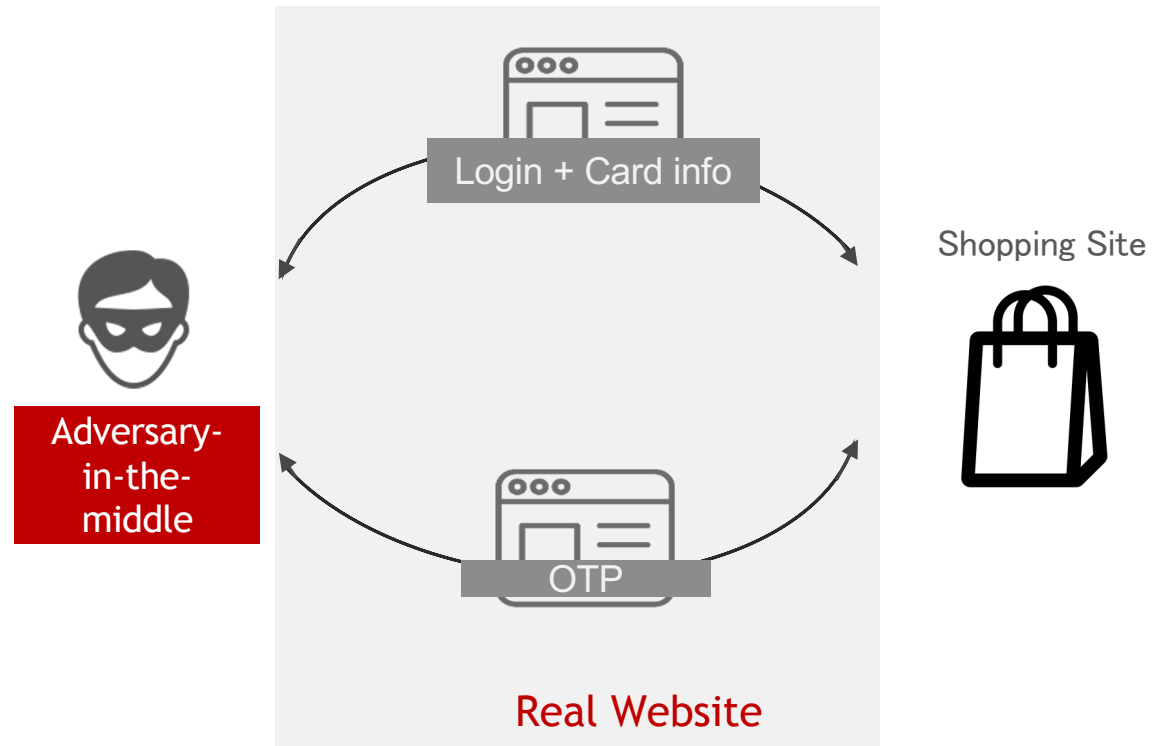
欢迎管理员 facai1

个人信息中心

点击刷新

当前清单/总计:5

ID	姓名	卡号	有效期	安全码	登录放行	SMS验证码	SMS放行	状态	ip	卡图	创建时间
299	afsafs	4205420542054205	11/23	2345	<div>放行</div> <div>错误</div>	等待输入	<div>放行</div> <div>错误</div>	等待处理	156.251.141.193		2023-01-19 14:36:09
298	kurasato sekiguchi	4205420542054205	02/23	3445	<div>放行</div> <div>错误</div>	等待输入	<div>放行</div> <div>错误</div>	账号错误	156.251.141.193		2023-01-19 14:35:34
297	dfsdfs	4205420542054205	01/23	2345	<div>放行</div>	等待输入	<div>放行</div>	账号错误	156.251.141.193		2023-01-19 14:34:54



Victim



Linkt

?

Authentication

One verification code has been sent to your registered mobile phone. Please check and submit it to verify you are the account holder.

Amount

\$6.95

Date

19/01/2023

Card

xxxx xxxx xxxx 4205

Verification code

01:30

[Get another verification code](#)

VISA

AMEX

Apple Pay

Google Pay

SAMSUNG pay

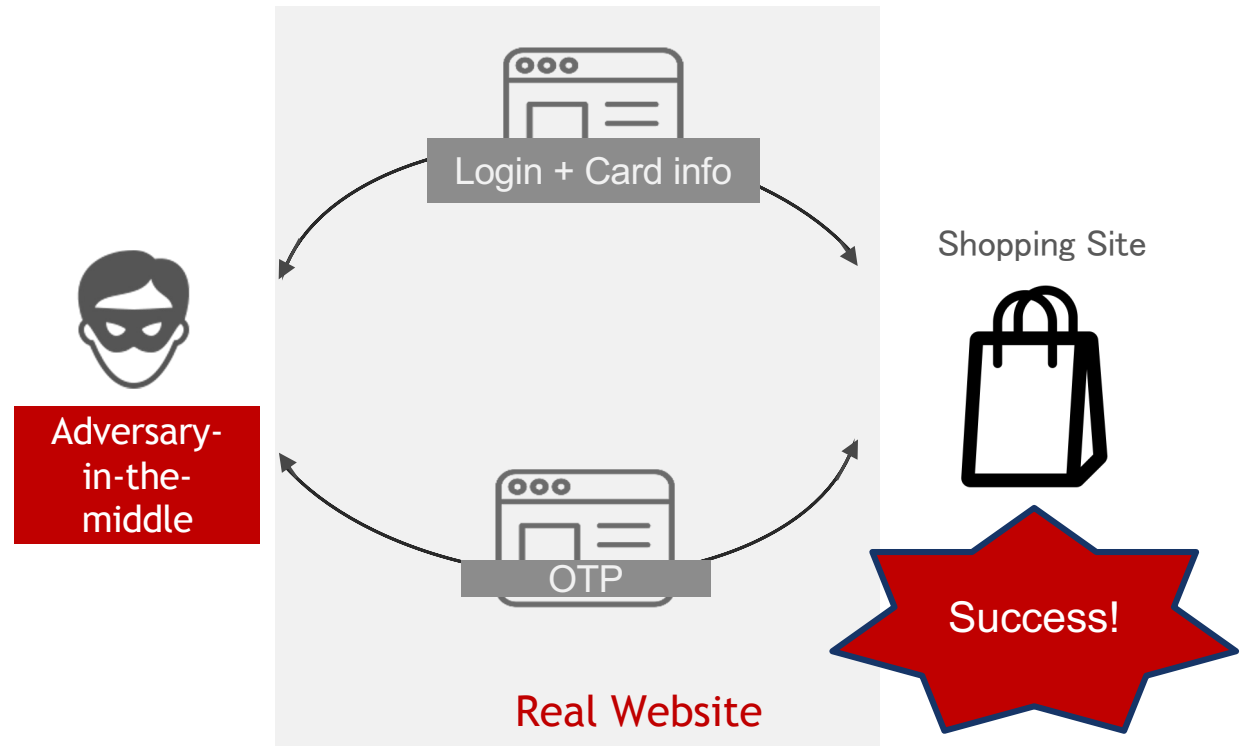
Submit

Operated by

Transurban

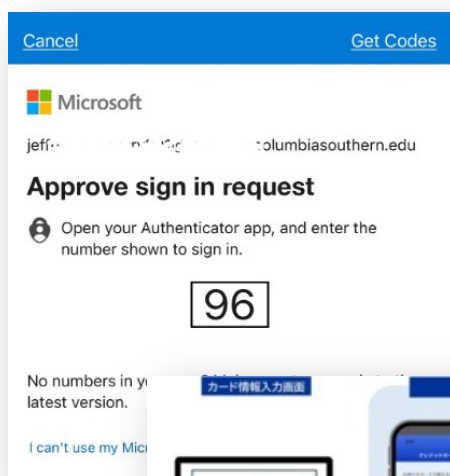


Adversary-  
in-the-  
middle



# Why doesn't OTP code work well?

- Adversary-in-the-middle always relay
- Or just ask the user for challenge code



## 防範簡訊詐欺 聯卡中心OTP驗證6月起將新增「一步驟」

2024/05/29 19:03

付款頁面

交易驗證碼確認

特約商店：聯卡中心商店  
交易金額：301.00 TWD  
信用卡號：\*\*\*\*\*0078  
交易日期：2023/12/13 15:51:37

已發送 OTP 請檢視你的手機訊息

網頁識別碼：VVAD

請輸入網路刷卡簡訊OTP服務密碼

驗證完成

取消

沒有收到簡訊OTP服務密碼？  
[重新取得簡訊OTP服務密碼](#)

● 交易驗證碼有效時間為5分鐘  
● 請輸入您接收到的網路刷卡簡訊OTP服務密碼

付款頁面

交易驗證碼確認

特約商店：聯卡中心商店  
交易金額：301.00 TWD  
信用卡號：\*\*\*\*\*0078  
交易日期：2023/12/13 16:55:46

網頁識別碼選擇錯誤，請重新選擇

請選擇網頁識別碼：

☒ VVAD ☐ KENA  
☐ AHEK ☐ LWEM

請輸入網路刷卡簡訊OTP服務密碼

驗證完成

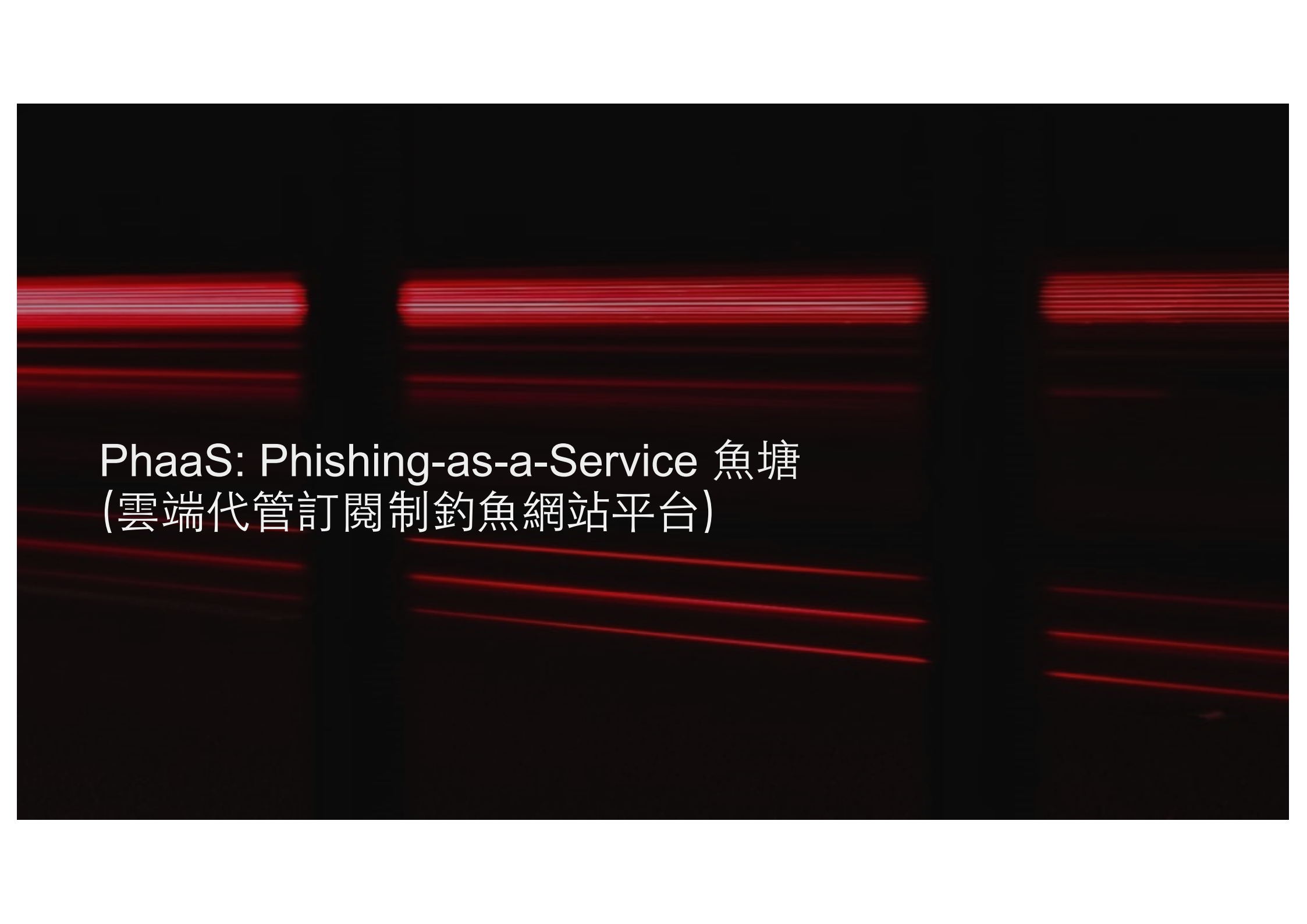
取消

沒有收到簡訊OTP服務密碼？  
[重新取得簡訊OTP服務密碼](#)

● 交易驗證碼有效時間為5分鐘  
● 請輸入您接收到的網路刷卡簡訊OTP服務密碼

基本款：1 組識別碼，確認付款頁面之識別碼與簡訊中相符  
進階款：4 組識別碼，於付款頁面中挑出與簡訊中相同  
後始輸入 OTP

防範簡訊詐欺，聯合信用卡中心在OTP驗證簡訊及付款頁面中增加「識別碼」，將配合發行進度自6月起陸續上線。（聯卡中心提供）



# PhaaS: Phishing-as-a-Service 魚塘

(雲端代管訂閱制釣魚網站平台)



# Online Training



## 【第一章】（第一课） CVV盗刷教学

### （第一课）C料如何获得

### （第二课）通道如何获得

### （第三课）环境如何搭建

### （第四课）产品转运方式

### （第五课）产品变现方法

### （第六课）如何自建鱼塘

### （第七课）如何群发邮件

### （第八课）如何获得数据

### （第九课）银行入侵改3D

### （毕业总结）毕业篇小问题总结

#### 【鱼料】

利用钓鱼源码模拟成主流人群使用的克隆网站，引诱受害者填写大量详细的信用卡和个人资料，其中包含卡号信息3D支付密码信息，账单地址，邮箱账号密码，受害者受害IP，浏览器指纹信息等等，信息更全，用途更广，好的鱼料深受人们的喜爱，但是相应的价格也会很高，一般在100-200不等。

#### 【鱼料的结构】

#-----[ Amazon账号 ]-----#  
Amazon账号 :masahito\_genki@yahoo.co.jp  
Amazon密码 :jmckg962  
#-----[ 信用卡信息 ]-----#  
银行 : RAKUTEN KC CO., LTD.  
品牌 : VISA - CREDIT  
等级 : TRADITIONAL  
卡一下名義人: Nagai masahito  
卡一下番号 : 4297690102170893  
有効期限 : 8/2025  
CVV : 664  
#-----[ 3D密码信息 ]-----#  
Web ID : Mmasahito88522  
Password 3D : Tmckg0033  
#-----[ 账单信息 ]-----#  
氏名 : 永井優人  
都道府県 : 千葉県  
住所1 : 船橋市前原東5-5-18  
住所2 : 戸建  
郵便番号 : 274-0824  
生年月日 : 1962-9-9  
電話番号 : 080-3915-0840  
#-----[ 指纹信息 ]-----#  
IP Address: 60.76.134.132  
IP Region: Chiba  
IP City: Ichikawa  
IP Continent: Asia  
IP Timezone: Asia/Tokyo  
OS/Browser: Android / Handheld Browser  
User Agent: Mozilla/5.0 (Linux; Android

#### 料主提供

真正的鱼料料主多数是自己假设鱼站，成本也是不小，所以日本的鱼料大致价格在120-200不等，美国的相对低一些也不会差很多，80-150都有。  
个人建议不要入手低于100一条的料，尤其是不熟悉的料商。如果各位真的需要购买，可以先咨询一下客服，打听一下群里兄弟，看看这个料主名声如何再入手。

#### 自建鱼塘

有时候很多人想着节省成本，也想去钓鱼群发降低成本，其实钓鱼当中存在很多技术问题，平凡的更替源码，做防红，群发数据采购，群发邮件SMTP协议，邮局调试等等都是技术活和辛苦活，每个人精力有限，不能又钓鱼又刷货，最后两边都搞不好，如果有一些基础，可以慢慢探索和学习尝试成为一名料主，如果没有一些基础的技术知识，那就从基础做起，不要好高骛远，先多看视频多学习，感觉掌握一些技巧之后，花点钱买点料，跳过技术门槛，直接刷货，发货就变现，赚钱了稳定了，形成良好循环了，再想去尝试学习钓鱼也不是不可以。  
自建鱼塘也就是所谓的搭建服务器--调试源码--群发邮件--上鱼，这种方式当然是最好的，因为是你自己钓的，除了你和受害者，谁也不知道料的信息，所以料能放住，这很重要。

#### 料站购买

料站靠谱的不多，当然也有一些老牌子料站，这里不打广告，料站需要用虚拟货币充值余额，再用余额购买，有一些料站是自带测试接口的，如果购买之后测试是死亡，会退给你余额，你可以重新购买，但是经常会遇到测试不准确，一条料几十美金打水漂，况且靠谱的料站多数是老外的，售后相对麻烦。

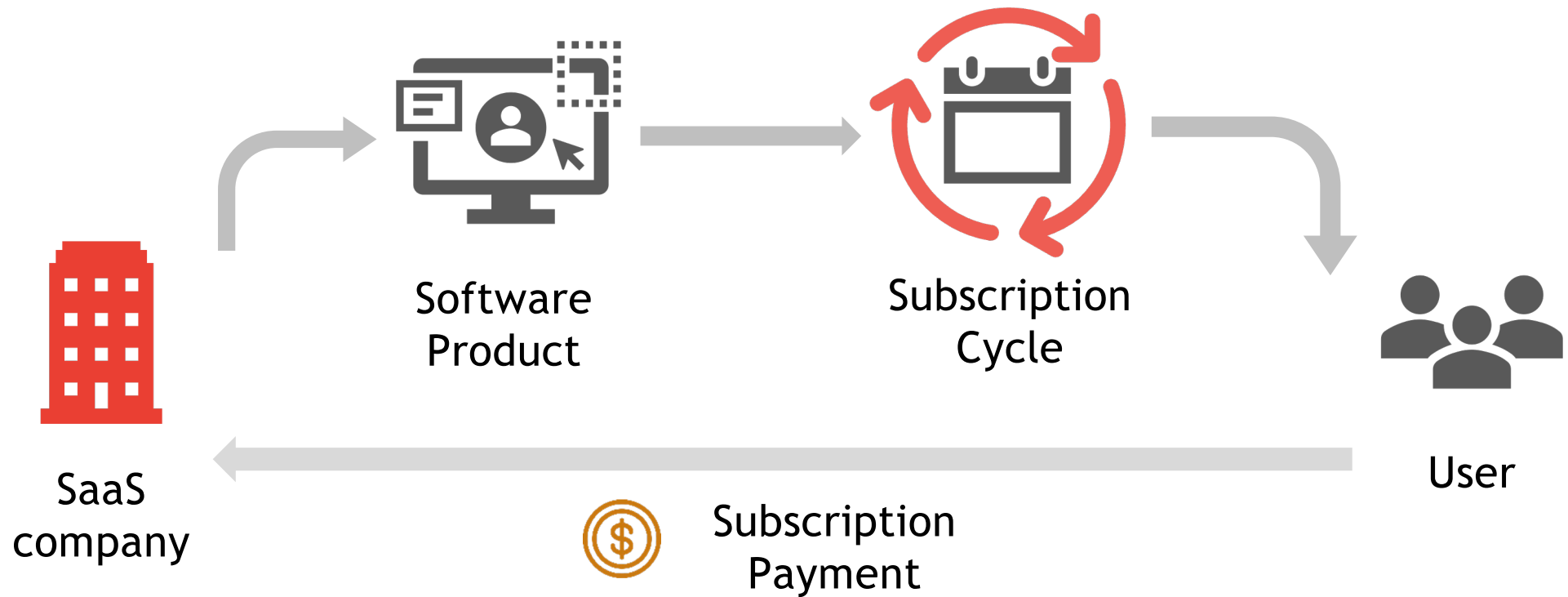
#### 黑市购买

黑市购买相对来说能靠谱一些，与料站的auto自选采购模式不同，黑市是B2C模式交易，类似淘宝，由平台制衡双方交易和调节，最有代表性的网站当然是目前最大的阿尔法。前几年关了，现在起死回生，由当年的程序员重新开放，推荐去逛一逛。

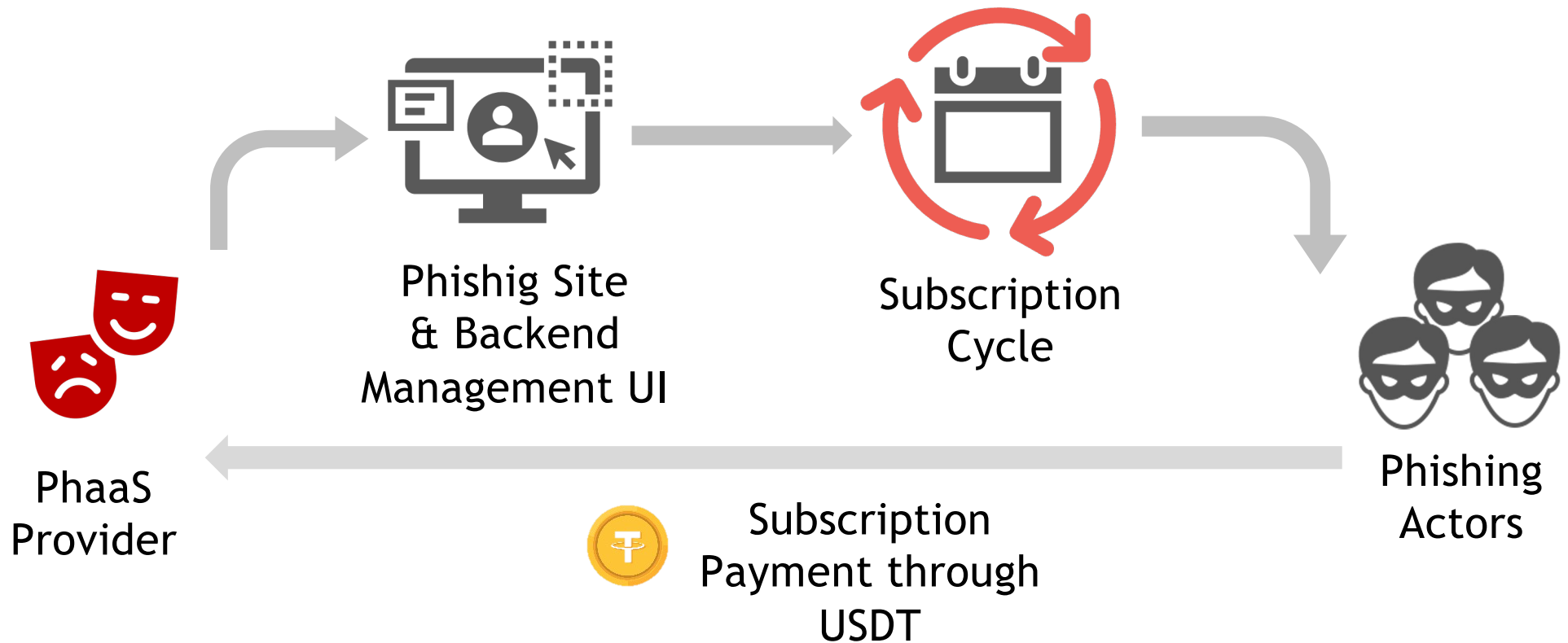
#### 自由者联盟担保下单

如果实在不放心，也可以在自由者下单，主页面有CVV买卖，平台不收取利润，只负责替付先担保金的商家发帖和更新卡头，如果各位购买之后发现问题，自由者客服介入调解，确定问题如果归商家，直接扣除担保金补偿客户，这一点比较人性化，所以各位可以放心。

# SaaS Business Model explained





# PhaaS Business Model (魚塘) 雲端代管訂閱制釣魚網站

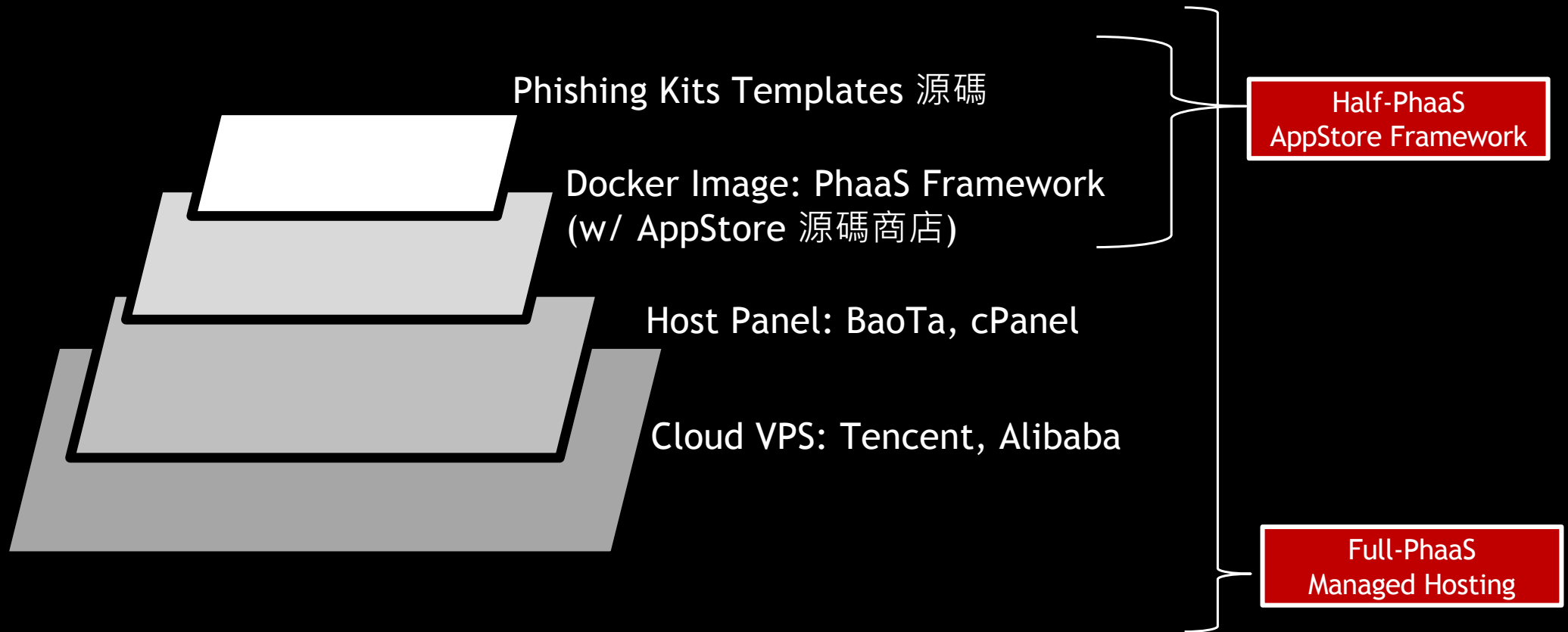


# Types of Phishing-as-a-Service

	Phishing Kit Preparation	Domain / VPS Set Up	Phishing Mail Prep & Delivery	Card Using Set up	Use Card	Monetization
	Phisher			Carder		Monetizer
<b>No PhaaS</b> Full-stack Engineer						
<b>Half PhaaS</b> 源碼商店 AppStore Framework						
<b>Full PhaaS</b> 鱼塘 Managed Hosting						

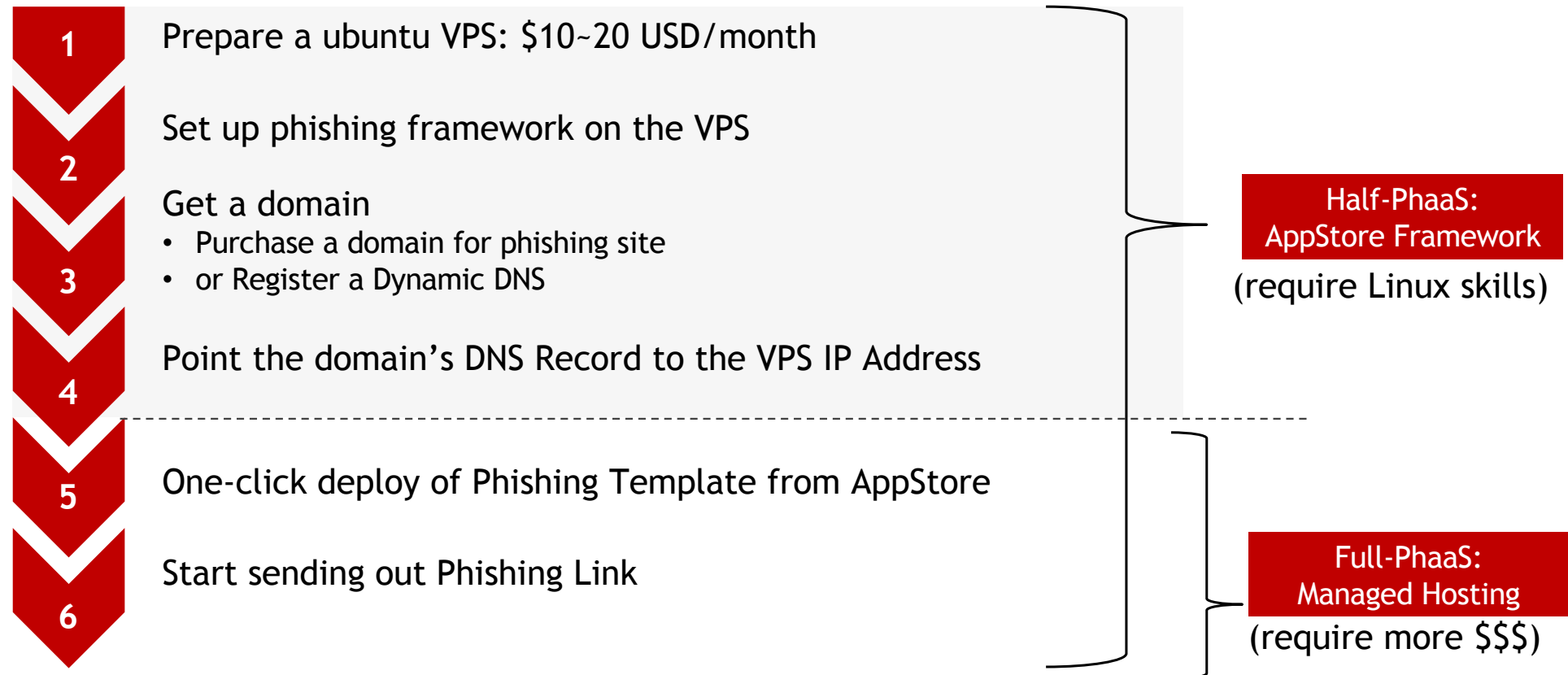
 PhaaS provider role     Phishing Actor role

# Tech Stack of Half / Full PhaaS



# Definition of Half/Full PhaaS

Phisher's job:





# From early 2023, 50+ of PhaaS providers observed across Chinese Card Shops, mostly w/Real-time Phishing

The collage displays several screenshots from different PhaaS provider interfaces, illustrating the scale and complexity of these services. The interfaces are primarily in Chinese and show various data tables and user management features.

**Top Left Screenshot:** A table listing users with columns for ID, Name, Status, and Action. The table includes entries for users like 'Yolaine Inepi', 'Cristina Pineda', 'Basilio Lopez', 'Keren', 'Miguel Angel Sanchez', 'Ana Yessen Perez', 'Brenda Nolas', 'Wilson Hernandez', 'Elio Lucrecio Sanchez', 'Andrea Benavente', and 'Hector Cardona'.

**Top Middle Screenshot:** A screenshot of a web browser showing a phishing page with a login form and a 'Real-time Phishing' status indicator.

**Top Right Screenshot:** A screenshot of a phishing page with a login form and a 'Real-time Phishing' status indicator.

**Bottom Left Screenshot:** A screenshot of a phishing page with a login form and a 'Real-time Phishing' status indicator.

**Bottom Middle Screenshot:** A screenshot of a phishing page with a login form and a 'Real-time Phishing' status indicator.

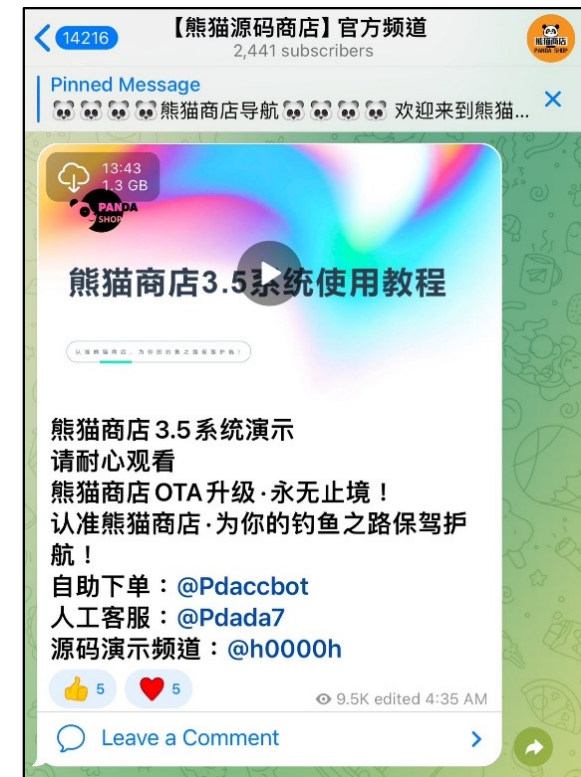
**Bottom Right Screenshot:** A screenshot of a phishing page with a login form and a 'Real-time Phishing' status indicator.

# PhaaS: Phishing as a Service Case Study

# Case Study 1/2 - Panda Shop 熊猫源码商店

- Subscribers: 2600+
- Focused on Delivery Services
- Pricing: Pay with USDT

Options	Daily	Weekly	Monthly
<b>No PhaaS</b> Phishing Kit Source Code	520U One time		
<b>Half-PhaaS</b> AppStore Framework No domain & VPS	30U	90U	220U
<b>Full-PhaaS</b> Managed Hosting		120U	260U



## Case Study 2/2 - Magic Cat 神奇貓貓

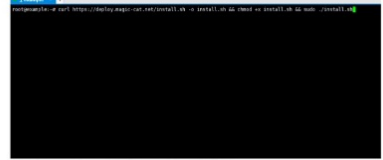
- Subscribers: 3000+
- Focused on various Post Office theme
- Pricing: Pay with USDT

Options	Daily	Weekly	Monthly
<b>No PhaaS</b> Phishing Kit Source Code		-	
<b>Half-PhaaS</b> AppStore Framework No domain & VPS	-	88U	288U
<b>Full-PhaaS</b> Managed Hosting	-	138U	338U

小小灰 RCS IM/神奇猫猫 (全球)  
 2,932 subscribers


购买服务器教程参考，需要Ubuntu22.04的系统的服务器，最低配置2h2g  
<https://zhuanlan.zhihu.com/p/103893335>  
 如果你不知道怎么连接服务器可以参  
<https://zhuanlan.zhihu.com/p/606759161>  
 xshell服务器连接工具下载地址  
<https://www.netsarang.com/en/free-for-home-school/>

在连接好服务器后，粘贴这个安装代码  
 curl https://deploy.magic-cat.world/install.sh -o install.sh && chmod +x install.sh && sudo ./install.sh




粘贴后回车，注意不要复制错了

等待出现这样的提示就是安装好了










然后再执行 cat public/config.json 来查看后台账号密码



# PhaaS Providers: Earning like senior software engineer!





**Panda Shop**




**USDT** | EOA ⓘ  
TVwU6X2iWjSHcrgKzp8FcRtgJsPA78Rc1b ⓘ   
Multi-Chain:   

**Overview**   Data updated 12 min(s) ago 

Balance	Txs count
470.9798 USDT	1,350
First seen (UTC)	Last seen (UTC)
Jun 02, 2023, 01:57 PM	Jun 03, 04:42 PM
<b>Total received</b>	Total spent
<b>204,246.6099 USDT</b>	201,675.4381 USDT
Incoming txn	Outgoing txn
1,329	21

**Magic Cat**

**USDT** | EOA ⓘ  
TUJ3PmB5f6cN1Pvin5uz7A8aMRRY1qPhw3 ⓘ   
Multi-Chain:   

**Overview**   Data updated seconds ago 

Balance	Txs count
6,183.5165 USDT	1,947
First seen (UTC)	Last seen (UTC)
Oct 29, 2023, 10:04 AM	Jun 04, 10:17 AM
<b>Total received</b>	Total spent
<b>300,515.9233 USDT</b>	294,332.4067 USDT
Incoming txn	Outgoing txn
865	1,082

# A lot of related phishing sites built on the same VPS IP

43.153.3.98

Search

×

Help

Search results (19 / 19, sorted by date, took 34ms)

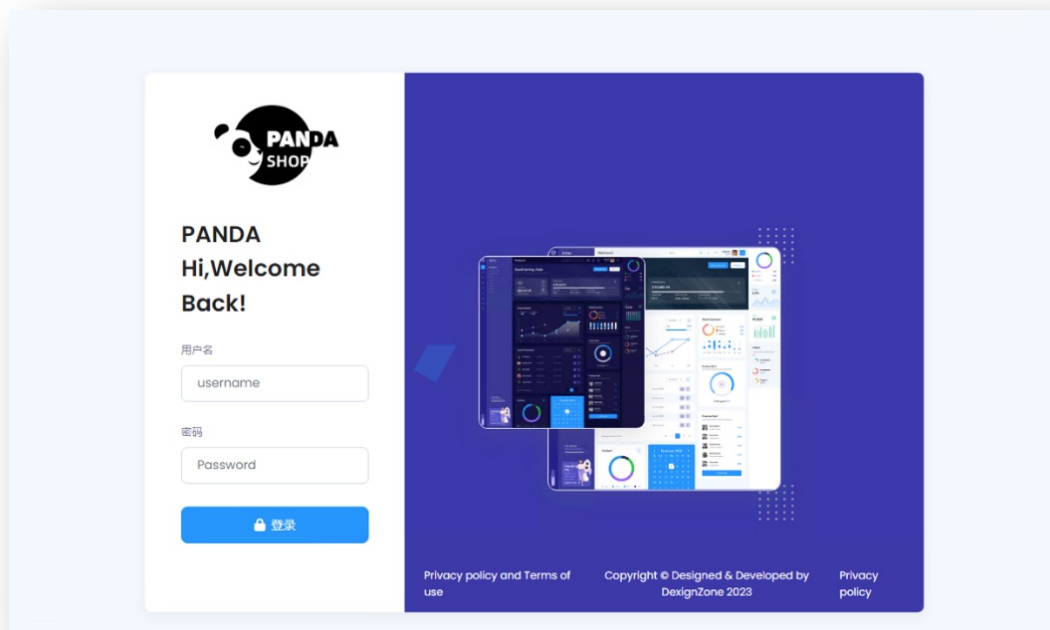
Showing All Hits

Details: Hidden

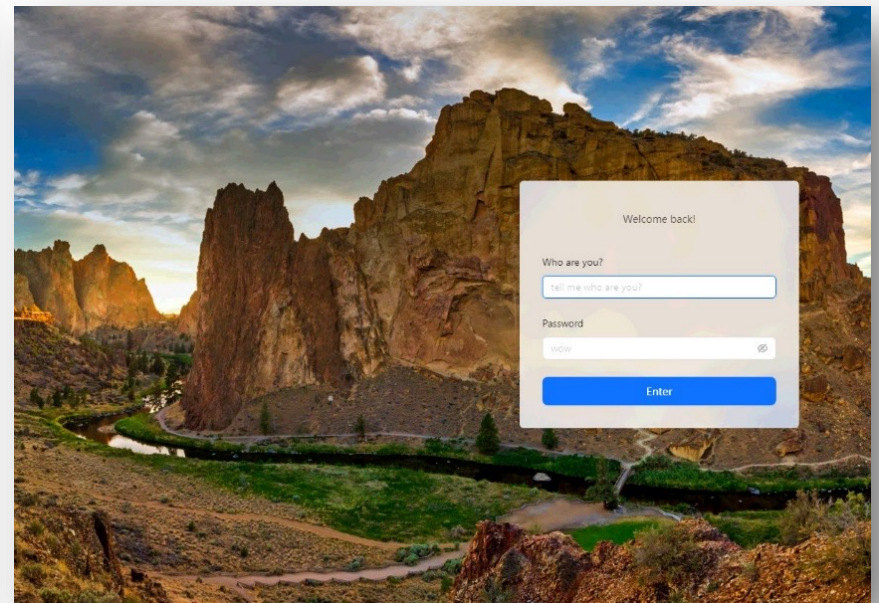
URL		Age		Size		IPs		
<a href="http://www.canadapost-postescanada.ca/cpc/en/home.page">www.canadapost-postescanada.ca/cpc/en/home.page</a>		Unlisted	15 days		5 MB	82	8	3
<a href="http://www.dhl.com/gb-en/home.html?locale=true">www.dhl.com/gb-en/home.html?locale=true</a>		Unlisted	2 months		1 MB	59	5	2
<a href="http://www.post.ch/de">www.post.ch/de</a>		Public	2 months		2 MB	85	12	3
<a href="http://www.canadapost-postescanada.ca/cpc/en/home.page">www.canadapost-postescanada.ca/cpc/en/home.page</a>		Public	2 months		5 MB	97	10	1
<a href="http://www.canadapost-postescanada.ca/cpc/en/home.page">www.canadapost-postescanada.ca/cpc/en/home.page</a>		Public	2 months		5 MB	91	11	1
<a href="http://www.canadapost-postescanada.ca/cpc/en/home.page">www.canadapost-postescanada.ca/cpc/en/home.page</a>		Public	2 months		5 MB	96	11	3
<a href="http://www.canadapost-postescanada.ca/cpc/en/home.page">www.canadapost-postescanada.ca/cpc/en/home.page</a>		Public	2 months		5 MB	96	11	3
<a href="http://www.amazon.co.jp/">www.amazon.co.jp/</a>		Public	2 months		4 MB	300	19	5
<a href="http://www.post.ch/de">www.post.ch/de</a>		Public	2 months		2 MB	85	12	3
<a href="http://www.post.ch/de">www.post.ch/de</a>		Public	2 months		2 MB	81	10	3
<a href="http://www.post.ch/de">www.post.ch/de</a>		Unlisted	2 months		2 MB	84	12	3
<a href="http://www.smbc.co.jp/">www.smbc.co.jp/</a>		Unlisted	2 months		9 MB	408	71	2
<a href="http://www.canadapost-postescanada.ca/cpc/en/home.page">www.canadapost-postescanada.ca/cpc/en/home.page</a>		Public	2 months		5 MB	96	11	3
<a href="http://www.smbc.co.jp/">www.smbc.co.jp/</a>		Public	2 months		9 MB	423	71	2
<a href="http://www.smbc.co.jp/">www.smbc.co.jp/</a>		Public	2 months		8 MB	449	75	6
<a href="http://www.smbc.co.jp/">www.smbc.co.jp/</a>		Public	2 months		9 MB	413	75	6



# Let's explore the frameworks



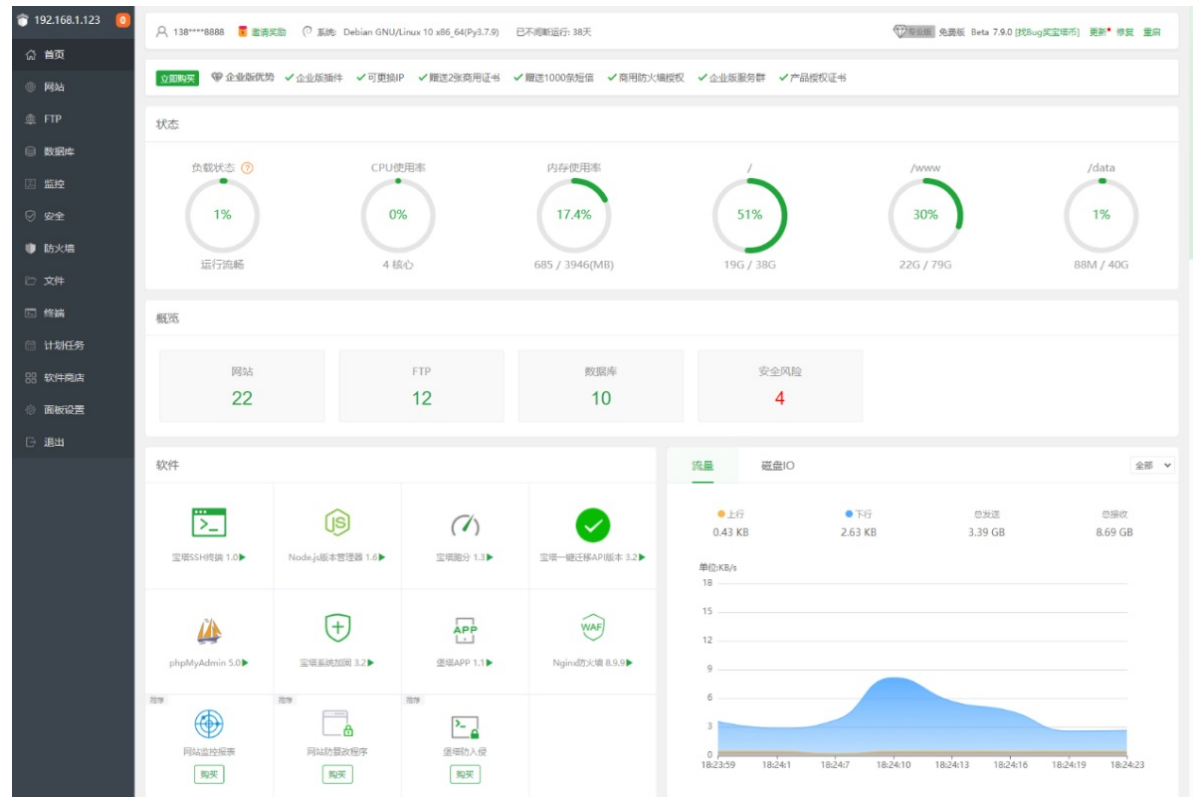
Panda Shop



Magic Cat

# How to deploy a PhaaS Framework to VPS

- 宝塔Linux面板 一鍵 install  
OR
- Docker install  
`curl https://deploy.magic-cat.world/install.sh`
- 教學影片 step by step

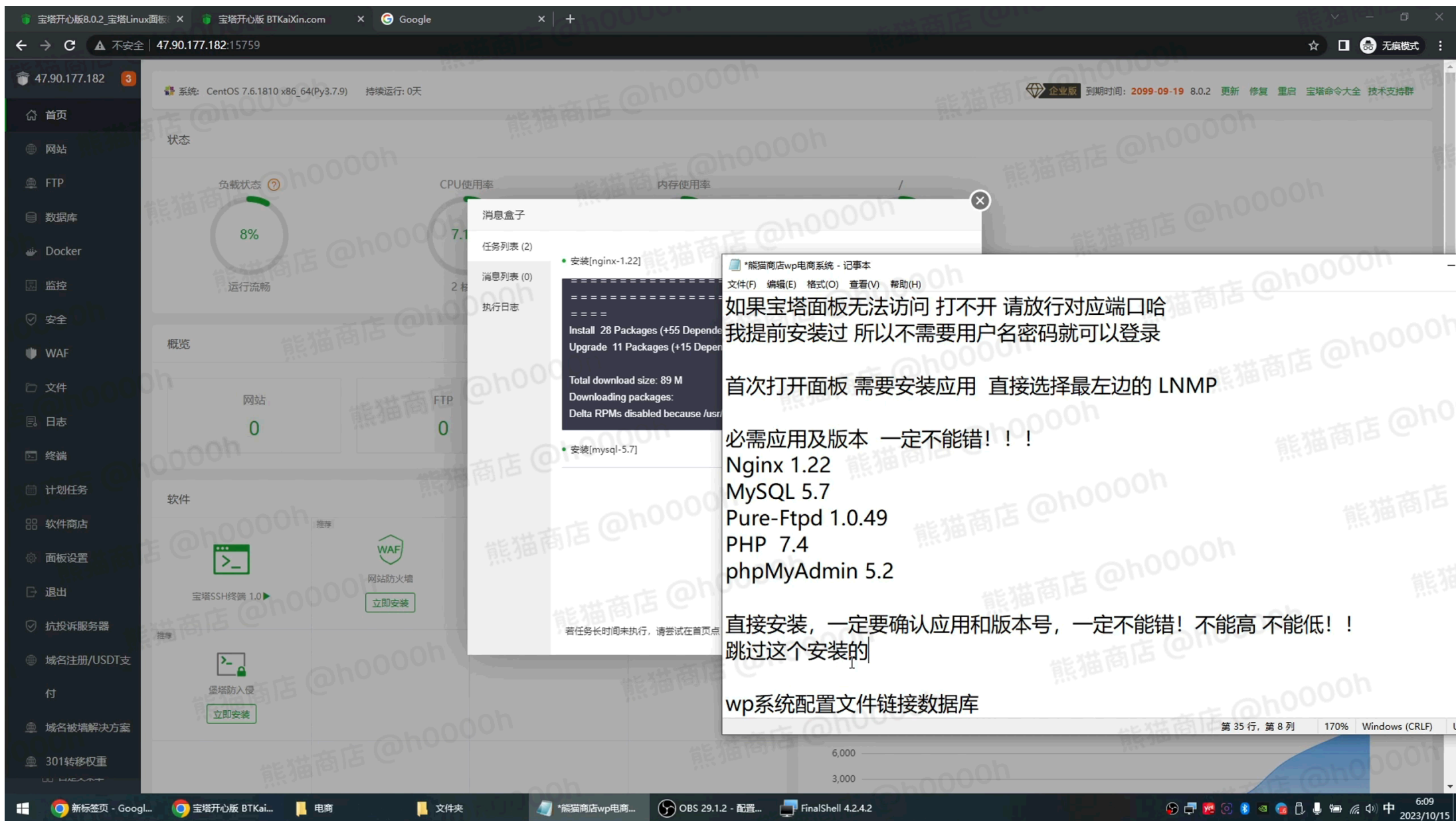






# 熊猫商店电商搭建教程

认准熊猫商店，为你的钓鱼之路保驾护航！



# MagicCat Docker & License Daemon

- Docker 安裝 script 貼上就自動裝，隨機產生後台密碼

```
Total reclaimed space: 305.9MB
[+] Restarting 4/4
✓ Container root-api-1          Started
✓ Container root-mysql-1       Started
✓ Container root-web-msg-sender-1 Started
✓ Container root-web-1         Started
root@example:~#
```

```
root@example:~# cat public/config.json
{
  "admin-entripoint": "cg5cGavQrl", 后台登录地址
  "admin-user": "0Kitu8Bbri", 后台账号
  "admin-passwd": "YqVzX7ngNuCko0n" 后台密码
}root@example:~#
```

# App Store - US phishing sites

神奇猫猫

已下载 源码列表 TG通知设置

编号:  说明:

重置 查询

此列表不定期更新

手动输入编号 C I 刷新

编号	说明	操作
arm_post	亚美尼亚包裹 <a href="https://www.haypost.am">https://www.haypost.am</a>	安装
irs	国税局, Internal Revenue Service 是美国联邦政府的税收服务机构, 负责征收美国联邦税款并执行联邦法定税法的主体	安装
mercari	美国的mercari账号	安装
us_amazon	美国亚马逊退款 英语、意大利语、葡萄牙语	安装
us_post_fedex	美国FedEx快递 <a href="https://www.fedex.com">https://www.fedex.com</a>	安装
us_post_ups	美国UPS <a href="https://www.ups.com">https://www.ups.com</a>	安装
usps	美国包裹USPS-废弃 <a href="https://www.usps.com">https://www.usps.com</a>	安装
usps_new	新局的美国USPS <a href="https://www.usps.com">https://www.usps.com</a>	安装

US Mercari

US Amazon

Fedex

UPS

USPS

USPS (new)

IRS: Internal Revenue Service

# App Store - SG phishing sites

2.125.63/rO4qxLd4Y6/#/pages/pages-list

## 神奇猫猫

已下载 源码列表 TG通知设置

编号:  说明:

此列表不定期更新

编号	说明	操作
tw_line	TW-Line	安装

## 神奇猫猫

已下载 源码列表 TG通知设置

编号:  说明:

此列表不定期更新

编号	说明
jp_amazon	日本亚马逊(同步)
jp_elbill_tepco	日本电费欠费通知 <a href="https://www.tepco.co.jp">https://www.tepco.co.jp</a>
jp_etc_nexco	日本ETC <a href="https://www.e-nexco.co.jp">https://www.e-nexco.co.jp</a>
jp_kddi_points	日本积分 <a href="https://www.au.com">https://www.au.com</a>
jp_mizuho_bank	日本瑞穗银行, 同步, 可以自行安装测试流程
jp_post_heimao	日本黑猫包裹 <a href="https://www.kuronekoyamato.co.jp/">https://www.kuronekoyamato.co.jp/</a>
jp_smart_ex	日本新干线smart-ex <a href="https://smart-ex.jp">https://smart-ex.jp</a>
jp_smbc	日本三井银行, 同步, 可以自行安装测试流程
jp_smbc_vpass	日本三井网银



编号	说明	操作	ch1_post	智利 <a href="http://www.correos.cl/">http://www.correos.cl/</a>	isl_post	冰岛包裹 <a href="https://posturinn.is">https://posturinn.is</a>	mys_points_c	马来西亚celcom积分 <a href="https://www.celcom.com.my/">https://www.celcom.com.my/</a>	sgp_etc	新加坡ETC <a href="https://url.ta.gov.sg">https://url.ta.gov.sg</a>
abw_post	阿鲁巴包裹 <a href="https://www.postaruba.com">https://www.postaruba.com</a>		civ_post	科特迪瓦包裹 <a href="https://laposte.ci/post">https://laposte.ci/post</a>	isl_gov	以色列政府补贴 <a href="https://b2b.bt.gov.il/">https://b2b.bt.gov.il/</a>	mys_points_f	马来西亚maxis积分 <a href="https://www.maxis.com.my">https://www.maxis.com.my</a>	sgp_points_fi	新加坡fairprice.com.sg积分 <a href="https://www.fairprice.com.sg">https://www.fairprice.com.sg</a>
ago_post	安哥拉包裹 <a href="https://www.correiosdeangola.co.ao/">https://www.correiosdeangola.co.ao/</a>		col_etc	哥伦比亚ETC <a href="https://www.gov.co">https://www.gov.co</a>	ita_etc	意大利ETC <a href="https://www.telepass.com">https://www.telepass.com</a>	mys_points_j	马来西亚touchngo积分 <a href="https://www.touchngo.com.my">https://www.touchngo.com.my</a>	sgp_points_s	新加坡Singtel积分 <a href="https://www.singtel.com">https://www.singtel.com</a>
alb_post	阿尔巴尼亚包裹 <a href="https://www.postashqiptare.al/">https://www.postashqiptare.al/</a>		col_points_cl	哥伦比亚claro电信积分 <a href="https://www.c">https://www.c</a>	ita_points_tin	意大利TIM积分 <a href="https://www.tim.it">https://www.tim.it</a>	mys_post	马来西亚包裹 <a href="https://www.pos.com.my/home">https://www.pos.com.my/home</a>	sgp_post	新加坡包裹 <a href="https://www.singpost.com">https://www.singpost.com</a>
amazon_post	亚马逊包裹(英语,默认\$可以自行修改货币来用于其它国家) <a href="https://www.amazon.com">https://www.amazon.com</a>		col_post	哥伦比亚包裹 <a href="https://www.4-72.com.ita">https://www.4-72.com.ita</a>	ita_post	意大利包裹 <a href="https://business.poste.it">https://business.poste.it</a>	mys_post_ite	马来包裹(英语) <a href="https://www.itexpress.my/">https://www.itexpress.my/</a>	slv_post	萨尔瓦多包裹 <a href="https://www.correos.gob.sv">https://www.correos.gob.sv</a>
aomen_dianx	<a href="https://www.1888.com">https://www.1888.com</a>		crl_points	哥斯达黎加积分 <a href="https://www.grupocie">https://www.grupocie</a>	ita_postepay	意大利Postepay网银 <a href="https://www.post">https://www.post</a>	nam_post	纳米比亚包裹 <a href="https://www.nampost.com.na">https://www.nampost.com.na</a>	smr_post	圣马力诺包裹 <a href="https://www.poste.sm">https://www.poste.sm</a>
aomen_ydon	<a href="https://www.1888.com.mo">https://www.1888.com.mo</a>		crl_post	哥斯达黎加 <a href="https://correos.go.cr">https://correos.go.cr</a>	jam_post	牙买加包裹 <a href="https://jamaicapost.gov.jm">https://jamaicapost.gov.jm</a>	netflix	奈飞会员体验 <a href="https://www.netflix.com">https://www.netflix.com</a>	srb_post	塞尔维亚包裹 <a href="https://www.posta.rs">https://www.posta.rs</a>
apple	日本苹果·有ID和填卡步骤		cub_post	古巴包裹 <a href="https://www.correos.cu">https://www.correos.cu</a>	jor_points_ar	约旦arabbank积分(英语/阿拉伯语) <a href="https://www.jor">https://www.jor</a>	nga_post	尼日利亚包裹 <a href="https://www.nipost.gov.ng">https://www.nipost.gov.ng</a>	svk_post	斯洛伐克包裹 <a href="https://www.posta.sk/">https://www.posta.sk/</a>
appleid_en	AppleID		cyp_post	塞浦路斯包裹 <a href="https://www.cypruspost">https://www.cypruspost</a>	jor_post	约旦包裹 <a href="https://jordanpost.com.jo">https://jordanpost.com.jo</a>	nic_post	尼加拉瓜包裹 <a href="http://www.correos.gob.ni">http://www.correos.gob.ni</a>	svn_points_te	斯洛文尼亚电信积分 <a href="https://www.telekom.si">https://www.telekom.si</a>
appleid_refur	AppleID退款(钓卡) <a href="https://support.apple.com/apple-id">https://support.apple.com/apple-id</a>		cze_post	捷克包裹 <a href="https://www.ceskaposta.cz">https://www.ceskaposta.cz</a>	jp_amazon	日本亚马逊(同步)	nld_cjbj	荷兰交通罚款 <a href="https://digitalloket.cjbj.nl/">https://digitalloket.cjbj.nl/</a>	svn_post	斯洛文尼亚包裹 <a href="https://www.posta.si/zasebno">https://www.posta.si/zasebno</a>
are_damanhr	阿联酋健康卡 <a href="https://damanhealth.ae">https://damanhealth.ae</a>		darcula	电商支付插件,支持woocommece·s· jp_elbill_tepcc	日本电费欠费通知 <a href="https://www.tepco">https://www.tepco</a>	nld_easypark	荷兰easypark账号异常 <a href="https://www.easypark.com/nl">https://www.easypark.com/nl</a>	swe_post	瑞典包裹 <a href="https://www.postnord.se/">https://www.postnord.se/</a>	
are_points_bi	阿联酋积分 <a href="https://www.bankfab.com">https://www.bankfab.com</a>		deu_points_t	德国电信Telekom积分 <a href="https://www.tel">https://www.tel</a>	jp_etc_nexco	日本ETC <a href="https://www.e-nexco.co.jp">https://www.e-nexco.co.jp</a>	nld_post	荷兰包裹 <a href="https://postnl.post/2?language=nl">https://postnl.post/2?language=nl</a>	tha_cimbthai	泰国cimbthai网银 <a href="https://www.cimbthai.com">https://www.cimbthai.com</a>
are_points_di	阿联酋DU积分(英语) <a href="https://www.du.ae">https://www.du.ae</a>		deu_post	德国DHL包裹 <a href="https://www.dhl.de/">https://www.dhl.de/</a>	jp_kddi_point	日本积分 <a href="https://www.au.com">https://www.au.com</a>	nor_etc	挪威ETC <a href="https://www.autopass.no">https://www.autopass.no</a>	tha_krungsri	泰国krungsrionline网银 <a href="https://www.krungsrionline.com">https://www.krungsrionline.com</a>
are_points_ei	阿联酋航空积分 <a href="https://www.emirates.com/">https://www.emirates.com/</a>		deu_tvpayme	德国电视费滞纳金缴费单 <a href="https://www">https://www</a>	jp_mizuohabar	日本瑞穗银行·同步·可以自行安装	nor_post	挪威包裹 <a href="https://www.posten.no">https://www.posten.no</a>	tha_points_ai	泰国积分 <a href="https://www.ais.th">https://www.ais.th</a>
are_points_et	阿联酋etisalat电信积分(英语) <a href="https://www.etisalat.ae">https://www.etisalat.ae</a>		dhk_gov	丹麦政府补贴 <a href="https://skat.dk/">https://skat.dk/</a>	jp_post_heim	日本黑猫包裹 <a href="https://www.kuronekoye">https://www.kuronekoye</a>	npl_post	尼泊尔包裹 <a href="https://www.gpo.gov.np/Home/DomesticTrac">https://www.gpo.gov.np/Home/DomesticTrac</a>	tha_post	泰国包裹 <a href="https://www.thailandpost.co.th">https://www.thailandpost.co.th</a>
are_points_nu	阿联酋Noon商城积分 <a href="https://www.noon.com">https://www.noon.com</a>		dhl_post_fr	摩洛哥-DHL包裹-法语 <a href="https://www.dh">https://www.dh</a>	jp_smart_ex	日本新干线smart-exhttps://smart-ex.j	nzetc	新西兰ETC <a href="https://www.nzta.govt.nz">https://www.nzta.govt.nz</a>	tha_post_flas	泰国包裹 <a href="https://www.flashexpres.co.th/">https://www.flashexpres.co.th/</a>
are_post	阿联酋包裹(英语/阿拉伯语) <a href="https://www.emiratespost.ae">https://www.emiratespost.ae</a>		dnk_post	丹麦包裹 <a href="https://www.postnord.dk">https://www.postnord.dk</a>	jp_sbmc	日本三井银行·同步·可以自行安装	nzn_post	新西兰包裹 <a href="https://www.nzpost.co.nz/">https://www.nzpost.co.nz/</a>	tkm_post	土库曼斯坦包裹 <a href="https://post.tm">https://post.tm</a>
are_post_ara	阿联酋aramex包裹 <a href="https://www.aramex.com/ae/en">https://www.aramex.com/ae/en</a>		dom_post	多米尼加包裹 <a href="https://inposdom.gob.d">https://inposdom.gob.d</a>	jp_sbmc_upar	日本三井网银	omn_points_s	阿曼Omantel积分 <a href="https://www.omantel.om">https://www.omantel.om</a>	tto_post	特立尼达和多巴哥包裹 <a href="https://tftpost.net">https://tftpost.net</a>
are_post_zajk	阿联酋包裹 <a href="https://zajel.com">https://zajel.com</a>		dubai_water	迪拜水费缴纳,英语和阿拉伯语 <a href="https://">https://</a>	kaz_points_kz	哈萨克斯坦Kcell积分 <a href="https://kcell.kz/ki">https://kcell.kz/ki</a>	omn_post	阿曼包裹 <a href="https://www.omanpost.om/ar/node">https://www.omanpost.om/ar/node</a>	tun_post	突尼斯包裹(法语) <a href="https://www.poste.tn">https://www.poste.tn</a>
arg_etc	阿根廷ETC <a href="https://telepase.com.ar">https://telepase.com.ar</a>		dza_post	阿尔及利亚包裹 <a href="https://www.poste.dz">https://www.poste.dz</a>	kaz_post	哈萨克斯坦包裹 <a href="https://post.kz/service">https://post.kz/service</a>	ontario	西班牙的 ontario 资料	tur_etc	土耳其ETC <a href="https://www.kgm.gov.tr">https://www.kgm.gov.tr</a>
arg_post	阿根廷包裹 <a href="https://www.correoargentino.com.ar/">https://www.correoargentino.com.ar/</a>		ecu_points_n	厄瓜多尔movistar积分 <a href="https://www.m">https://www.m</a>	ken_post	肯尼亚包裹(英语) <a href="https://posta.co.ke">https://posta.co.ke</a>	pak_post	巴基斯坦包裹 <a href="https://ep.gov.pk">https://ep.gov.pk</a>	tur_post	土耳其包裹 <a href="https://www.ptt.gov.tr/">https://www.ptt.gov.tr/</a>
arg_post_two	阿根廷包裹-另一个官网的 <a href="https://www.andreani.com">https://www.andreani.com</a>		ecu_post	厄瓜多尔包裹 <a href="https://www.serviciopos">https://www.serviciopos</a>	kgh_post	吉尔吉斯斯坦(俄语) <a href="https://kyrgyzpost">https://kyrgyzpost</a>	pan_post	巴拿马包裹 <a href="https://www.correospanama.gob.pa/">https://www.correospanama.gob.pa/</a>	tw_line	TW-Line
arm_post	亚美尼亚包裹 <a href="https://www.haypost.am">https://www.haypost.am</a>		egy_post	埃及包裹 <a href="https://www.egyptpost.org">https://www.egyptpost.org</a>	khm_post	柬埔寨包裹 <a href="https://cambodiapost.com">https://cambodiapost.com</a>	per_points_cj	秘鲁claro电信积分 <a href="https://www.claro.com.pe/">https://www.claro.com.pe/</a>	tza_post	坦桑尼亚包裹 <a href="https://www.posta.co.tz/">https://www.posta.co.tz/</a>
au_etc	澳大利亚etc <a href="https://www.linkt.com.au">https://www.linkt.com.au</a>		eki	日本EKI	khn_wingbai	柬埔寨网银 <a href="https://ibanking.wingbank">https://ibanking.wingbank</a>	per_post	秘鲁包裹 <a href="https://www.gob.pe/serpost">https://www.gob.pe/serpost</a>	uk_gov	英国政府补贴 <a href="https://www.gov.uk">https://www.gov.uk</a>
au_mygov	澳大利亚 税务退款 <a href="https://my.gov.au">https://my.gov.au</a>		esp_bbva	西班牙BBVA网银 <a href="https://www.bbva.co">https://www.bbva.co</a>	kor_etc	韩国ETC <a href="https://www.hipass.co.kr">https://www.hipass.co.kr</a>	phl_bdoBank	菲律宾BDO网银 <a href="https://www.bdo.com.ph">https://www.bdo.com.ph</a>	uk_gov_yehicl	英国纳税提醒 <a href="https://yehicl.tax.service.gov.uk">https://yehicl.tax.service.gov.uk</a>
au_mygts	澳大利亚积分 <a href="https://www.coles.com.au">https://www.coles.com.au</a>		esp_etc	西班牙ETC <a href="https://www.autopistas.coi">https://www.autopistas.coi</a>	kor_post	韩国包裹 <a href="https://www.koreapost.go.ki">https://www.koreapost.go.ki</a>	phl_points_gi	菲律宾积分 <a href="https://www.globe.com.ph">https://www.globe.com.ph</a>	uk_points_ee	英国ee积分 <a href="https://ee.co.uk/">https://ee.co.uk/</a>
au_points_oo	澳洲ootus积分 <a href="https://www.optus.com.au/">https://www.optus.com.au/</a>		esp_etc_dct	西班牙dct-ETC罚款 <a href="https://www.dct.e">https://www.dct.e</a>	kwf_nbk_ban	科威特nbk银行 <a href="https://www.nbk.com/">https://www.nbk.com/</a>	dhl_points_gr	菲律宾积分 <a href="https://www.grab.com/ph/">https://www.grab.com/ph/</a>	uk_post_rova	英国皇家邮政 <a href="https://www.royalmail.com/track-your-item">https://www.royalmail.com/track-your-item</a>
au_points_tel	澳洲telstra Plus积分 <a href="https://pl">https://pl</a>		esp_etc_kwt	科威特STC积分 <a href="https://www.stc.kw">https://www.stc.kw</a>	kwf_points_k	科威特STC积分 <a href="https://www.stc.kw">https://www.stc.kw</a>	pol_points_uk	波兰积分 <a href="https://www.poczta.polska.pl/">https://www.poczta.polska.pl/</a>	ukr_post	乌克兰 <a href="https://www.ukrposhta.ua">https://www.ukrposhta.ua</a>
au_post	澳大利亚包裹 <a href="https://www.australia">https://www.australia</a>		esp_etc_kwt	科威特STC积分 <a href="https://www.stc.kw">https://www.stc.kw</a>	kwf_points_k	科威特STC积分 <a href="https://www.stc.kw">https://www.stc.kw</a>	pol_points_uk	波兰积分 <a href="https://www.poczta.polska.pl/">https://www.poczta.polska.pl/</a>	us_post_fede	美国FedEx快递 <a href="https://www.fedex.com">https://www.fedex.com</a>
au_post_two	澳洲 <a href="https://www.australia">https://www.australia</a>		esp_post	爱沙尼亚 <a href="https://www.omnina.ee">https://www.omnina.ee</a>	kwf_post	爱沙尼亚 <a href="https://www.omnina.ee">https://www.omnina.ee</a>	pol_points_uk	波兰积分 <a href="https://www.poczta.polska.pl/">https://www.poczta.polska.pl/</a>	us_post_ups	美国UPS <a href="https://www.ups.com">https://www.ups.com</a>
au_qantas	澳洲航空积分 <a href="https://accounts.qantas.com">https://accounts.qantas.com</a>		est_post	爱沙尼亚 https://www.omnina.ee	kwf_post	爱沙尼亚 https://www.omnina.ee	pol_points_uk	波兰积分 <a href="https://www.poczta.polska.pl/">https://www.poczta.polska.pl/</a>	usps	美国包裹USPS-废弃 <a href="https://www.usps.com">https://www.usps.com</a>
au_transport	澳大利亚 Opal帐户检测到异常 <a href="https://transportnsw.info">https://transportnsw.info</a>		fin_nairshop	芬兰积分 <a href="https://www.finairshop.com">https://www.finairshop.com</a>	kwf_water	科威特水电费 <a href="https://www.mew.gov.k">https://www.mew.gov.k</a>	pol_points_uk	波兰积分 <a href="https://www.poczta.polska.pl/">https://www.poczta.polska.pl/</a>	usps_new	新写的美国USPS https://www.usps.com
aut_points_a	奥地利积分 <a href="https://www.a1.net">https://www.a1.net</a>		fin_post	芬兰包裹 <a href="https://www.posti.fi">https://www.posti.fi</a>	lalamove_pos	拉玛ove包裹 https://www.lal	pol_points_uk	波兰积分 <a href="https://www.poczta.polska.pl/">https://www.poczta.polska.pl/</a>	ven_post	委内瑞拉包裹 <a href="https://www.ipostel.gob.ve/">https://www.ipostel.gob.ve/</a>
aut_post	奥地利 <a href="https://www.post.at">https://www.post.at</a>		fra_etc	法国ETC <a href="https://www.bipandgo.com">https://www.bipandgo.com</a>	lbn_post	黎巴嫩包裹 <a href="https://www.libanpost.com">https://www.libanpost.com</a>	pol_post	波兰包裹 <a href="https://emonitoring.poczta-polska.pl/">https://emonitoring.poczta-polska.pl/</a>	vnm_points_v	越南积分Viettel <a href="https://vietteltelecom.vn">https://vietteltelecom.vn</a>
aze_post	阿塞拜疆包裹 <a href="https://www.azerpost.az">https://www.azerpost.az</a>		fra_points_sf	法国SF积分 <a href="https://www.sfr.fr">https://www.sfr.fr</a>	lbya_post	利比亚包裹 <a href="https://lbyapost.ly">https://lbyapost.ly</a>	pol_post_inpc	波兰包裹(新的) <a href="https://inpost.pl/">https://inpost.pl/</a>	vnm_post	越南包裹 <a href="https://vietnampost.vn">https://vietnampost.vn</a>
be_points_pr	比利时proximus积分 <a href="https://www.proximus.be/fr/personal">https://www.proximus.be/fr/personal</a>		fra_post	法国包裹 <a href="https://www.laposte.fr">https://www.laposte.fr</a>	lie_post	列支敦士登包裹 <a href="https://post.li">https://post.li</a>	prt_etc	葡萄牙ETC	vnm_post_unio	越南包裹-新的 <a href="https://viettelpost.com.vn">https://viettelpost.com.vn</a>
be_lpost	比利时包裹 <a href="https://track.bpost.cloud/btr/web/#/home?lang=nl">https://track.bpost.cloud/btr/web/#/home?lang=nl</a>		fra_post_chri	法国chronopost包裹 <a href="https://www.chro">https://www.chro</a>	lka_points_di	斯里兰卡Dialog积分 <a href="https://www.dialo">https://www.dialo</a>	prt_post	葡萄牙包裹 <a href="https://www.ctt.pt">https://www.ctt.pt</a>	westernunion	西联汇款网银 <a href="https://www.westernunion.com/">https://www.westernunion.com/</a>
bgd_post	孟加拉包裹 <a href="https://bdpost.portal.gov.bd">https://bdpost.portal.gov.bd</a>		gbr_post_ewi	英国EWR包裹 <a href="https://www.ewi.com">https://www.ewi.com</a>	lka_post	斯里兰卡包裹 <a href="https://slpost.gov.lk">https://slpost.gov.lk</a>	pry_post	巴拉圭包裹 <a href="https://www.correoparaguayo.gov.py/stio/inde">https://www.correoparaguayo.gov.py/stio/inde</a>	worldvision	马来捐款(卡和网银) <a href="https://www.worldvision.com.my/en/my-giving">https://www.worldvision.com.my/en/my-giving</a>
bgr_post	保加利亚包裹 <a href="https://new.bgpost.bg">https://new.bgpost.bg</a>		geo_post	格鲁吉亚包裹 <a href="https://www.gpost.ge">https://www.gpost.ge</a>	ltu_ebill	立陶宛电费 <a href="https://www.perlasgo.lt">https://www.perlasgo.lt</a>	pse_post	巴勒斯坦包裹 <a href="https://www.palpost.ps">https://www.palpost.ps</a>	yem_post	也门包裹 <a href="https://www.post.ye">https://www.post.ye</a>
bhr_gov_kims	巴林健康卡 <a href="https://www.kimshealth.org">https://www.kimshealth.org</a>		gha_post	加纳包裹 <a href="https://ghanapost.com.gh">https://ghanapost.com.gh</a>	ltu_points_tel	立陶宛Telia积分 <a href="https://www.telia.lt/">https://www.telia.lt/</a>	qat_donate	卡塔尔捐款 <a href="https://www.qcharity.org">https://www.qcharity.org</a>	youtube	Youtube会员体验 <a href="https://www.youtube.com">https://www.youtube.com</a>
bhr_points_bi	巴林电信积分(英语) <a href="https://batelco.com">https://batelco.com</a>		grc_etc	希腊ETC <a href="https://www.aodos.gr">https://www.aodos.gr</a>	ltu_post	立陶宛包裹 <a href="https://www.post.lt">https://www.post.lt</a>	qat_gov_qa	卡塔尔住房补贴 <a href="https://www.gco.gov.qa/">https://www.gco.gov.qa/</a>	za_points	南非积分 Vodacom积分·支持英语、德语、西班牙语、希腊语 <a href="https://www.vodacom">https://www.vodacom</a>
bhr_post	巴林包裹 <a href="https://www.bahrain.bh">https://www.bahrain.bh</a>		grc_points_ci	希腊cosmote积分 <a href="https://www.cosmo">https://www.cosmo</a>	ltu_water	立陶宛水费 <a href="https://savitarna.v.lt">https://savitarna.v.lt</a>	qat_gov_hukr	卡塔尔健康卡 <a href="https://hukoomi.gov.qa">https://hukoomi.gov.qa</a>	za_post	南非包裹
bhr_post_en	巴林包裹英语版 <a href="https://www.bahrain.bh">https://www.bahrain.bh</a>		grc_post	希腊包裹 <a href="https://www.elta-courier.gr">https://www.elta-courier.gr</a>	lux_points_po	卢森堡Post积分(卢森堡的包裹和积分	qat_gov_suppr	卡塔尔补给卡 <a href="https://hukoomi.gov.qa/en/service/issue-rai">https://hukoomi.gov.qa/en/service/issue-rai</a>	zaf_gov_esko	南非电费 <a href="https://www.eskom.co.za">https://www.eskom.co.za</a>
bih_post	波黑(波斯尼亚/黑塞哥维那)包裹 <a href="https://www.posta.ba">https://www.posta.ba</a>		grc_post_eltz	新的希腊包裹 <a href="https://elta.gr/">https://elta.gr/</a>	lux_post	卢森堡包裹 <a href="https://www.post.lu">https://www.post.lu</a>	qat_gov_trav	卡塔尔旅行卡充值 <a href="https://www.qr.com.qa/top-up">https://www.qr.com.qa/top-up</a>	zaf_points_ce	南非celc积分 <a href="https://www.celc.co.za/celc/home">https://www.celc.co.za/celc/home</a>
blr_post	白俄罗斯包裹 <a href="https://www.belpost.by">https://www.belpost.by</a>		grc_water	希腊水费 <a href="https://www.eydpar.gr">https://www.eydpar.gr</a>	lwa_points	拉脱维亚Tele2积分 <a href="https://www.tele2">https://www.tele2</a>	qat_points_di	卡塔尔多哈银行积分 <a href="https://qa.dohabank.com">https://qa.dohabank.com</a>	zaf_points_fn	南非FNB积分 <a href="https://www.fnb.co.za">https://www.fnb.co.za</a>
bmo_post	百慕大包裹 <a href="https://www.bdashipping.bm">https://www.bdashipping.bm</a>		gtm_post	危地马拉包裹 <a href="https://correosytelegrafi">https://correosytelegrafi</a>	lwa_post	拉脱维亚包裹 <a href="https://pasts.lv">https://pasts.lv</a>	qat_points_oi	卡塔尔电信积分Ooredoo(英语/阿拉伯语) <a href="https://www.oo">https://www.oo</a>	zaf_points_fm	南非MTN积分 <a href="https://www.mtn.co.za">https://www.mtn.co.za</a>
bmo_bank	BMO网银 <a href="https://www1.bmo.com">https://www1.bmo.com</a>		guy_post	圭亚那包裹 <a href="https://guypost.gy">https://guypost.gy</a>	mar_points_i	摩洛哥积分 <a href="https://www.iam.ma">https://www.iam.ma</a>	qat_points_qi	卡塔尔航空积分 <a href="https://www.qatarairways.com">https://www.qatarairways.com</a>	zaf_points_te	南非telkom积分 <a href="https://www.telkom.co.za/">https://www.telkom.co.za/</a>
bol_post	玻利维亚 <a href="http://tracking.correos.gob.bo/">http://tracking.correos.gob.bo/</a>		hnd_post	洪都拉斯包裹 <a href="https://honducor.gob.hr">https://honducor.gob.hr</a>	mco_post	摩纳哥包裹 <a href="https://www.lapostemonac">https://www.lapostemonac</a>	qat_points_qi	卡塔尔Qib银行积分 <a href="https://www.qib.com.qa/en">https://www.qib.com.qa/en</a>	zaf_post	新版本的南非邮政 <a href="https://www.postoffice.co.za/">https://www.postoffice.co.za/</a>
bra_elebill	巴西电费缴纳 <a href="https://www.gov.br">https://www.gov.br</a>		hva_post	克罗地亚包裹 <a href="https://www.posta.hr">https://www.posta.hr</a>	mco_post	摩纳哥多瓦包裹 <a href="https://www.posta">https://www.posta</a>	qat_points_vc	卡塔尔沃达丰积分 <a href="https://www.vodafone.qa">https://www.vodafone.qa</a>		
bra_points_vb	巴西Vivo积分 <a href="https://www.vivo.com.br">https://www.vivo.com.br</a>		hun_points_e	匈牙利积分 匈牙利语罗马尼亚语 <a href="https">https</a>	mdv_post	马代尔夫包裹 <a href="https://www.maldivespo">https://www.maldivespo</a>	qat_post	卡塔尔包裹 <a href="https://qatarpost.qa">https://qatarpost.qa</a>		
bra_post	巴西包裹 <a href="https://rastreamento.correios.com.br">https://rastreamento.correios.com.br</a>		hun_post	匈牙利包裹 <a href="https://www.dpd.com/hu/l">https://www.dpd.com/hu/l</a>	menggu_pos	蒙古包裹 <a href="https://www.mongolpost.mn">https://www.mongolpost.mn</a>	qat_post_two	卡塔尔包裹-英语的 <a href="https://qatarpost.qa">https://qatarpost.qa</a>		
brn_post	文莱包裹 <a href="https://www.post.gov.bn">https://www.post.gov.bn</a>		hun_post_dhl	匈牙利DHL包裹 <a href="https://www.dhl.com/">https://www.dhl.com/</a>	mercari	约美国的mercari账号	qat_qnb	卡塔尔QNB <a href="https://www.qnb.com">https://www.qnb.com</a>		
bs_post	巴哈马包裹 <a href="https://www.bahamas.gov.bs/postalservice">https://www.bahamas.gov.bs/postalservice</a>		idn_points_te	印尼积分telkomsel(印尼语言/英语) <a href="http">http</a>	mex_points_t	墨西哥telcel电信积分 <a href="https://www.tek">https://www.tek</a>	rou_post	罗马尼亚包裹 <a href="https://www.posta-romana.ro">https://www.posta-romana.ro</a>		
bwa_post	博茨瓦纳包裹 <a href="https://botswanaipost.post">https://botswanaipost.post</a>		ind_post	印度包裹 <a href="https://www.posindonesia.c">https://www.posindonesia.c</a>	mex_post_uk	墨西哥UPS包裹 <a href="https://www.ups.com">https://www.ups.com</a>	rus_post	俄罗斯包裹 <a href="https://www.pochta.ru">https://www.pochta.ru</a>		
can_points_rj	加拿大Rogers积分 <a href="https://www.rogers.com/">https://www.rogers.com/</a>		il_post	以色列包裹 <a href="https://israelpost.co.il">https://israelpost.co.il</a>	mex_post_dh	墨西哥DHL包裹 <a href="https://www.dhl.com/">https://www.dhl.com/</a>	sau_etc	沙特ETC <a href="https://mot.gov.sa">https://mot.gov.sa</a>		
can_post	加拿大包裹 <a href="https://www.canadapost-postescanada.ca">https://www.canadapost-postescanada.ca</a>		ind_post	印度包裹(英语/印地语) <a href="https://www">https://www</a>	mex_post_es	墨西哥包裹 <a href="https://www.estafeta.com">https://www.estafeta.com</a>	sau_etc_absl	沙特ETC <a href="https://www.absher.sa">https://www.absher.sa</a>		
che_points_s	瑞士航空积分 <a href="https://www.swiss.com/ch">https://www.swiss.com/ch</a>		ir_points_eir	爱尔兰Eir积分(英文的沃达丰也可以用	mex_post_up	墨西哥UPS包裹 <a href="https://www.ups.com">https://www.ups.com</a>	sau_points_a	沙特afursan.saudia航空积分(英语/阿拉伯语) <a href="https://afursan.saudia.com/">https://afursan.saudia.com/</a>		
che_points_u	瑞士ubsBank积分 <a href="https://www.ubs.com/ch">https://www.ubs.com/ch</a>		ir_post	爱尔兰包裹 <a href="https://www.anpost.com">https://www.anpost.com</a>	mkd_post	马其顿包裹 <a href="https://www.posta.com">https://www.posta.com</a>	sau_points_n	沙特mobily积分(英语/阿拉伯语) <a href="https://www.mobily.com.sa">https://www.mobily.com.sa</a>		
ch_post	瑞士包裹 <a href="https://www.post.ch/de">https://www.post.ch/de</a>		irn_post	伊朗包裹 <a href="https://www.post.ir">https://www.post.ir</a>	mlt_post	马耳他包裹 <a href="https://www.maltapost.co">https://www.maltapost.co</a>	sau_points_s	沙特sabbnet银行积分(英语) <a href="https://www.security.online-banking.sabbnet.com/">https://www.security.online-banking.sabbnet.com/</a>		
chl_etc	智利ETC <a href="https://www.autopase.cl/">https://www.autopase.cl/</a>		irq_post	伊拉克包裹 <a href="https://www.dhl.com/qr-er">https://www.dhl.com/qr-er</a>	mlt_water	马耳他水费缴纳 <a href="https://arms.com.mt">https://arms.com.mt</a>	sau_points_s	沙特STC积分(英语/阿拉伯语) <a href="https://www.stc.com.sa">https://www.stc.com.sa</a>		
chl_points_sa	智利Santander银行积分 <a href="https://banco.santander.cl">https://banco.santander.cl</a>		irs	国税局, Internal Revenue Service 是美国	mne_post	黑山包裹 <a href="https://www.postag.me">https://www.postag.me</a>	sau_post	沙特包裹(英语和阿拉伯语) <a href="https://splonline.com.sa/ar/shipmentdetailsstatic">https://splonline.com.sa/ar/shipmentdetailsstatic</a>		
chl_points_te	智利积分telefonica <a href="https://www.telefonica.com">https://www.telefonica.com</a>		isl_points_sin	冰岛siminn积分 <a href="https://www.siminn.is">https://www.siminn.is</a>	mne_post	毛里求斯包裹 <a href="https://www.mauritius.sau">https://www.mauritius.sau</a>	post_sm	沙特包裹 <a href="https://www.smsaexpress.com/">https://www.smsaexpress.com/</a>		

70% Post Office

20% Telecom Bill

10% Others

# App Store: 300 Phishing templates 140 countries available

70% Post Office  
20% Telecom Bill  
10% Others

# Downloaded phishing template displayed

The screenshot displays a web interface for managing phishing templates. On the left is a sidebar with navigation links: 数据浏览, 访问日志, 源码配置, 访客黑名单, and 管理员. The main content area has a green header with instructions: '前台的打开方式: 必须使用手机端访问绑定好的域名加/前台入口, 比如: example.com/xxx, 默认会拦截VPN访问, 测试的时候你可以点击源码配置来关闭IP过滤(发送的时候要开启IP过滤)'. Below this, it says: '如果前台域名提示不安全, 你需要点击左下角的申请证书, 为域名申请一个证书. 如果你没有正确打开前台, 可以在绑定域名后访问域名, 然后点击【访问日志】来查看拦截原因, 并根据日志提示操作. 如果遇到任何错误, 请尽量截图错误提示(或者描述清楚具体情况)后联系我。' A modal window is open, showing a template titled 'jp\_elbill\_tepco' with the subtitle '日本电费欠费通知 https://www.tepco.co.jp'. It includes a field for '前台的入口' set to '无' and a '绑定的域名:' field. At the bottom of the modal are '配置' and '更新' buttons. In the bottom left, there is a '申请证书' section with instructions: '请输入要申请证书的域名(不带后缀)', '在申请之前你要确保DNS已经生效了', and '如果域名使用了Cloudflare, 那么就不要再申请证书了, 直接在域名前面加上 https:// 就行了'. It features a text input field and a '确认' button.

前台的打开方式: 必须使用手机端访问绑定好的域名加/前台入口, 比如: example.com/xxx, 默认会拦截VPN访问, 测试的时候你可以点击源码配置来关闭IP过滤(发送的时候要开启IP过滤)

如果前台域名提示不安全, 你需要点击左下角的申请证书, 为域名申请一个证书. 如果你没有正确打开前台, 可以在绑定域名后访问域名, 然后点击【访问日志】来查看拦截原因, 并根据日志提示操作

如果遇到任何错误, 请尽量截图错误提示(或者描述清楚具体情况)后联系我。

jp\_elbill\_tepco

日本电费欠费通知 https://www.tepco.co.jp

前台的入口: 无

绑定的域名:

配置 更新

申请证书

- 请输入要申请证书的域名(不带后缀)
- 在申请之前你要确保DNS已经生效了
- 如果域名使用了Cloudflare, 那么就不要再申请证书了, 直接在域名前面加上 https:// 就行了

确认

Japanese Electricity  
Phishing Site Downloaded

# Phishing Site App store, with one-click SSL Encryption

The screenshot displays a web management interface for a phishing site. On the left is a sidebar with navigation links: 数据浏览, 访问日志, 源码配置, 访客黑名单, and 管理员. The main content area has a green header with instructions: '前台的打开方式: 必须使用手机端访问绑定好的域名加/前台入口, 比如: example.com/xxx, 默认会拦截VPN访问, 测试的时候你可以点击源码配置来关闭IP过滤(发送的时候要开启IP过滤)'. Below this, a paragraph explains the process of applying for a certificate and checking logs. A modal window titled '申请证书' (Apply for Certificate) is open, showing a list of instructions and a text input field for the domain name. The instructions include: '请输入要申请证书的域名(不用带后缀)', '在申请之前你要确保DNS已经生效了', and '如果域名使用了Cloudflare, 那么就不要再申请证书了, 直接在域名前面加上 https:// 就行了'. The input field contains 'jp\_elbill\_tepco' and the URL 'https://www.tepco.co.jp'. There are '配置' (Configure) and '更新' (Update) buttons at the bottom of the modal.

前台的打开方式: 必须使用手机端访问绑定好的域名加/前台入口, 比如: example.com/xxx, 默认会拦截VPN访问, 测试的时候你可以点击源码配置来关闭IP过滤(发送的时候要开启IP过滤)

如果前台域名提示不安全, 你需要点击左下角的申请证书, 为域名申请一个证书。如果你没有正确打开前台, 可以在绑定域名后访问域名, 然后点击【访问日志】来查看拦截原因, 并根据日志提示操作

如果遇到任何错误, 请尽量截图错误提示(或者描述清楚具体情况)后联系我。

jp\_elbill\_tepco

日本电费欠费通知 https://www.tepco.co.jp

前台的入口: 无

绑定的域名:

配置 更新

申请证书

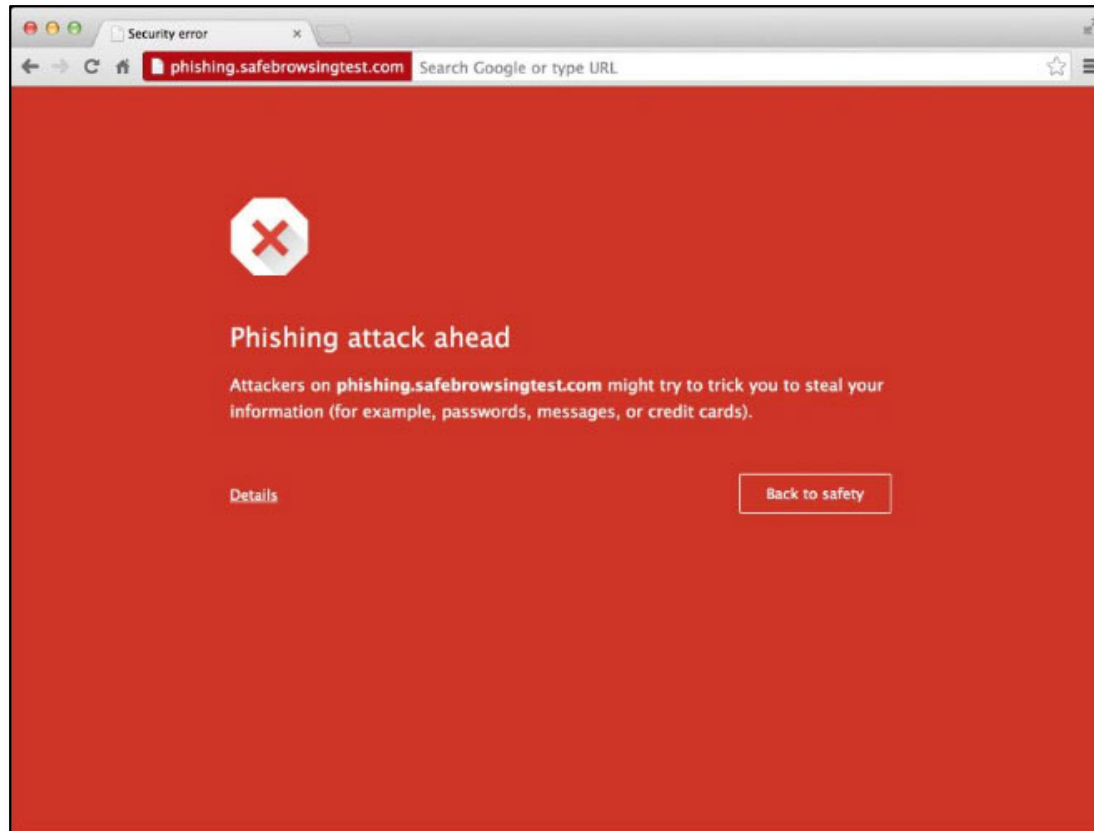
- 请输入要申请证书的域名(不用带后缀)
- 在申请之前你要确保DNS已经生效了
- 如果域名使用了Cloudflare, 那么就不要再申请证书了, 直接在域名前面加上 https:// 就行了

确认

One-click SSL (Let's Encrypt)  
No need for Cloudflare CDN



# Anti-Red 防红



## ! Red: Phishing Warning

Anti-Red: A method to block out organizations and visitors that may threaten the existence of the website

# User-friendly Anti-Red Features

The screenshot shows the 'Anti-Red Setting' (防红设置) interface in the Panda 3.5 application. The interface is divided into several sections with input fields and checkboxes. Red callout boxes highlight specific features:

- IP API KEY填写** (IP API KEY input): e53jjkx4kxo7jc93
- 白名单国家代码** (Allowlist Country): (例: cn,tw,nk)
- 拉黑后重定向跳转URL** (Redirect URL after card input): https://www.rakuten.cc
- 完成后跳转URL** (Redirect URL after card input): https://www
- 白名单IP** (Allowlist IP): 0.0.0.0
- 随机KEY入口** (URL Entrance Key): logIn
- 目前KEY** (URL Entrance Key): 复制链接
- 开启入口KEY验证** (Enable URL Entrance Key): ☒
- 开启防红验证** (Enable Anti-Red shield): ☒
- 更新设置** (Update Settings): 按钮

- IP API Key: GeoIP/Reputation lookup
- Allowlist IP, Countries
- Redirect URL
- Entrance Key when visiting URL  
Only when URL parameter is correct  
can the phishing site be accessed

[X] http://tepco.phisher.tk

[V] http://tepco.phisher.tk/?donut

# Actors work very hard 24 x 7 值班工讀生

Support 24 x 7  
Monitoring Alert to  
wake up actor from  
sleeping

The screenshot displays the 'Settings' page of the 'Panda 3.5' application. The interface is divided into two main sections: 'Notification Sound' and 'TG Notification'.

**Notification Sound Section:**

- 自定义填卡通知 (Custom Card Arrival Notification):** Includes a text input field '填卡了' and a '尝试播报' (Try Broadcast) button. A red label 'Voice alert on Card arrival' points to this section.
- 自定义验证码通知 (Custom OTP Verification Code Notification):** Includes a text input field '填验证码了' and a '尝试播报' (Try Broadcast) button. A red label 'Voice alert on OTP arrival' points to this section.
- 音效测试 (Sound Effect Test):** A dropdown menu showing '音效 1', '音效 2', '音效 3' (selected), and '音效 4'. A red label 'Sound effects' points to this dropdown.
- 是否播报订单ID (Whether to broadcast order ID):** A checkbox that is checked.
- 是否播放订单音效 (Whether to play order sound effect):** A checkbox that is checked.
- 更新设置 (Update Settings):** A blue button at the bottom.





**TG Notification Section:**

- TG 群通知 (TG Group Notification):** Includes a 'TG CHAT ID' input field and a '获取CHAT ID教程' (Get CHAT ID Tutorial) button. A red label 'TG Chat ID' points to this field.
- TG BOT TOKEN:** Includes a '输入BOT TOKEN' (Enter BOT TOKEN) input field and a '获取BOT TOKEN教程' (Get BOT TOKEN Tutorial) button. A red label 'TG BOT Token' points to this field.
- 通知类型 (Notification Type):** Two radio buttons: '完整版信息' (Complete info) (selected) and '简洁版信息' (Precise info). Red labels 'Complete info' and 'Precise info' point to these options.
- 是否通知验证码 (Whether to notify verification code):** A checkbox that is checked. A red label 'Notify on OTP' points to this checkbox.
- 更新设置 (Update Settings):** A blue button at the bottom.

**Left Sidebar:**

- Panda 3.5** logo and version.
- 首页 (Home)** icon.
- 订单管理 (Order Management)** icon.
- 功能设置 (Function Settings)** icon, which is expanded to show:
  - 用户管理 (User Management)
  - 系统设置 (System Settings)
  - 通知设置 (Notification Settings)
- 剩余时间: 5天5时45分10秒 (Remaining Time: 5 days 5 hours 45 minutes 10 seconds)** display.
- Speak out order ID** and **Enable sound effect** buttons.

# Support Front End & Notification Change



→

指定卡头高亮提醒


Highlight specified card BINs

金色:囍有钱	429769	更新设置
粉色:通道专用	358787	更新设置
橙色:特殊卡头	设置卡头后请点击应用, 否则控制	更新设置
蓝色:可绑苹果	设置卡头后请点击应用, 否则控制	更新设置
紫色:可绑谷歌	设置卡头后请点击应用, 否则控制	更新设置
灰色:狗都不要	设置卡头后请点击应用, 否则控制	更新设置

前端默认文案修改

Custom front-end message

拒绝卡的文案	Card information is incorrect	更新设置
拒绝码的文案	Verification code error	更新设置
提示app验证的文案	app verification reminder	更新设置
卡号不符合规则的文案	Not the correct card nu	更新设置
拉黑卡头的文案	This card is not supported	更新设置
提示换卡的文案	Change to another card	更新设置



Let's try the phishing site..

TEPCO 省エネプロ

ポイントがたまるプ  
家電のメンテナンス  
省エネや光熱費の  
キャンペーンを実

番号を入力して請求書を確認してください  
12345

請求書を確認する

電気をオンラインで支払う

you owe me donuts

カード所有者  
Strawberry Donut

カード番号  
1234 5678 1234 5678

このカードはこの取引をサポートしていません。別のカードをお試しください

The card does not support the transaction, please use another card

を送信する

Another weird Japanese

# Receive victim card info & OTP code in real time

The dashboard displays real-time credit card data. The top navigation bar shows the user is logged in as 'Admin'. The main content area features a table with columns: ID, 姓名 (Name), 卡号 (Card Number), 有效期 (Validity), CVV, 类型 (Type), OTP, 当前页面 (Current Page), 创建时间 (Creation Time), 状态 (Status), and 订单操作 (Order Action).

ID	姓名	卡号	有效期	CVV	类型	OTP	当前页面	创建时间	状态	订单操作
0087	Destini Tamboer	553	10/26	081	debit		已提交卡号, 等待处理	2023/11/17 00:28:10	在线	订单操作
0086	Dianne Graham	4334	03/28	134	debit		已提交卡号, 等待处理	2023/11/17 00:28:05	在线	订单操作
0085	Alexus Pointdujour	未输入	未输入	未输入			已填信息, 进入卡号页面	2023/11/17 00:23:44	离线	订单操作
0084	Natalie Hancock	未输入	未输入	未输入			重复填写, 进入卡号页面	2023/11/17 00:17:31	离线	订单操作
0083	Yessica Oseguera	402	10/28	600	debit		已拒绝, 提示更换卡	2023/11/17 00:18:44	在线	订单操作

On the left side of the dashboard, there are three notification boxes:

- 更新通知 x ID0076 输卡了
- 更新通知 x ID0087 输卡了
- 更新通知 x ID0086 输卡了

The bottom of the dashboard shows a Windows taskbar with the following applications: FinalShell 4.2.4.2, 临渊商店-PANDAS, and a system clock showing 0:28 on 2023/11/17.

## Meanwhile behind the scene... (actor's backstage)

神奇猫猫

实时动态 前台在线人数:1, 分流人数: 0

已刷新在线用户列表

编号: 3 未知 12345 Strawberry Donut 1234 5678 1234 5678 01/25 123 验证码

实时动态 Realttime status 1 分钟前

当前正在填卡页面 | 在手机号填页(1条数据) > 在填卡页(4条数据) > 填卡历史(1条数据) >

Inputting card

数据浏览

访问日志

神奇猫猫

实时动态 前台在线人数:1, 分流人数: 0

刷新 设置

编号: 3 debit 12345 Strawberry Donut 5166 9417 9845 3787 01/25 123 验证码

18 秒前

此用户已提交卡号, 请及时处理 | 在手机号填页(1条数据) > 在填卡页(4条数据) > 填卡历史(1条数据) >

The user has submitted the card info,  
Please respond ASAP!

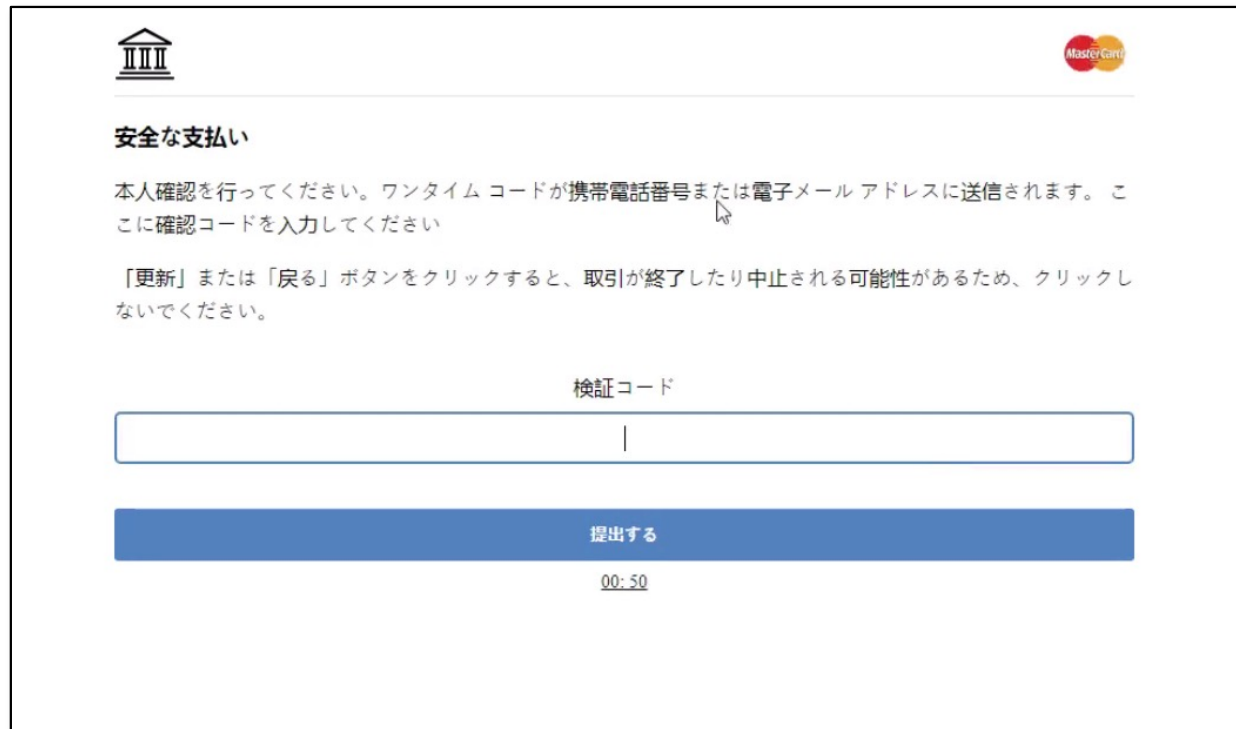
验证码验证 OTP

APP验证 APP verification

拒绝卡号 Deny card

跳转完成 Skip to complete

# OTP page



The screenshot shows a web page for OTP verification. At the top left is a logo of a classical building. At the top right is the Master Card logo. The main heading is '安全な支払い' (Safe Payment). Below it, the text reads: '本人確認を行ってください。ワンタイムコードが携帯電話番号または電子メールアドレスに送信されます。ここに確認コードを入力してください。' (Please confirm your identity. The one-time code will be sent to your mobile phone number or email address. Enter the confirmation code here.) Below this is another line of text: '「更新」または「戻る」ボタンをクリックすると、取引が終了したり中止される可能性があるため、クリックしないでください。' (Clicking the 'Update' or 'Back' button may result in the transaction ending or being canceled, so please do not click.) There is a text input field labeled '検証コード' (Verification Code) with a vertical cursor. Below the input field is a blue button labeled '提出する' (Submit). At the bottom center, there is a timer showing '00:50'.

- Unnatural Japanese instructions & Button
- Master Card Logo



# 50+ versions of PhaaS observed in Chinese Card shop

The collage displays several screenshots from different web applications, likely related to the investigation of PhaaS versions in a Chinese card shop.

- Top Left:** A screenshot of a PhaaS management interface showing a list of versions with columns for ID, Name, Status, and Actions. The interface is in Chinese.
- Top Center:** A screenshot of a card shop interface showing a list of cards with columns for Card ID, Card Name, Card Type, Card Status, and Card Actions. The interface is in Chinese.
- Top Right:** A screenshot of a user management interface showing a list of users with columns for User ID, User Name, User Type, User Status, and User Actions. The interface is in Chinese.
- Bottom Left:** A screenshot of a card shop interface showing a list of cards with columns for Card ID, Card Name, Card Type, Card Status, and Card Actions. The interface is in Chinese.
- Bottom Center:** A screenshot of a user management interface showing a list of users with columns for User ID, User Name, User Type, User Status, and User Actions. The interface is in Chinese.
- Bottom Right:** A screenshot of a user management interface showing a list of users with columns for User ID, User Name, User Type, User Status, and User Actions. The interface is in Chinese.

# Real-time Phished Collected Victim Info

## Essential

---

- Card Number: Accept / Deny
- OTP: Accept / Deny
- Card Expiration Date
- CVV

## Advanced

---

- Personal Info: Name, Phone, Zipcode, Birth Date, e-mail

## Meta-data

---

- Card Type: Debit / Credit
- BIN info: Card country, Brand, Issuer Bank, Card Rank
- IP
- Visitor Status: Online / Offline
- Visitor Stage: Accessing / Filling in card info / Waiting for OTP input / Completed input
- Referral Link

# Visualization Dashboard - example



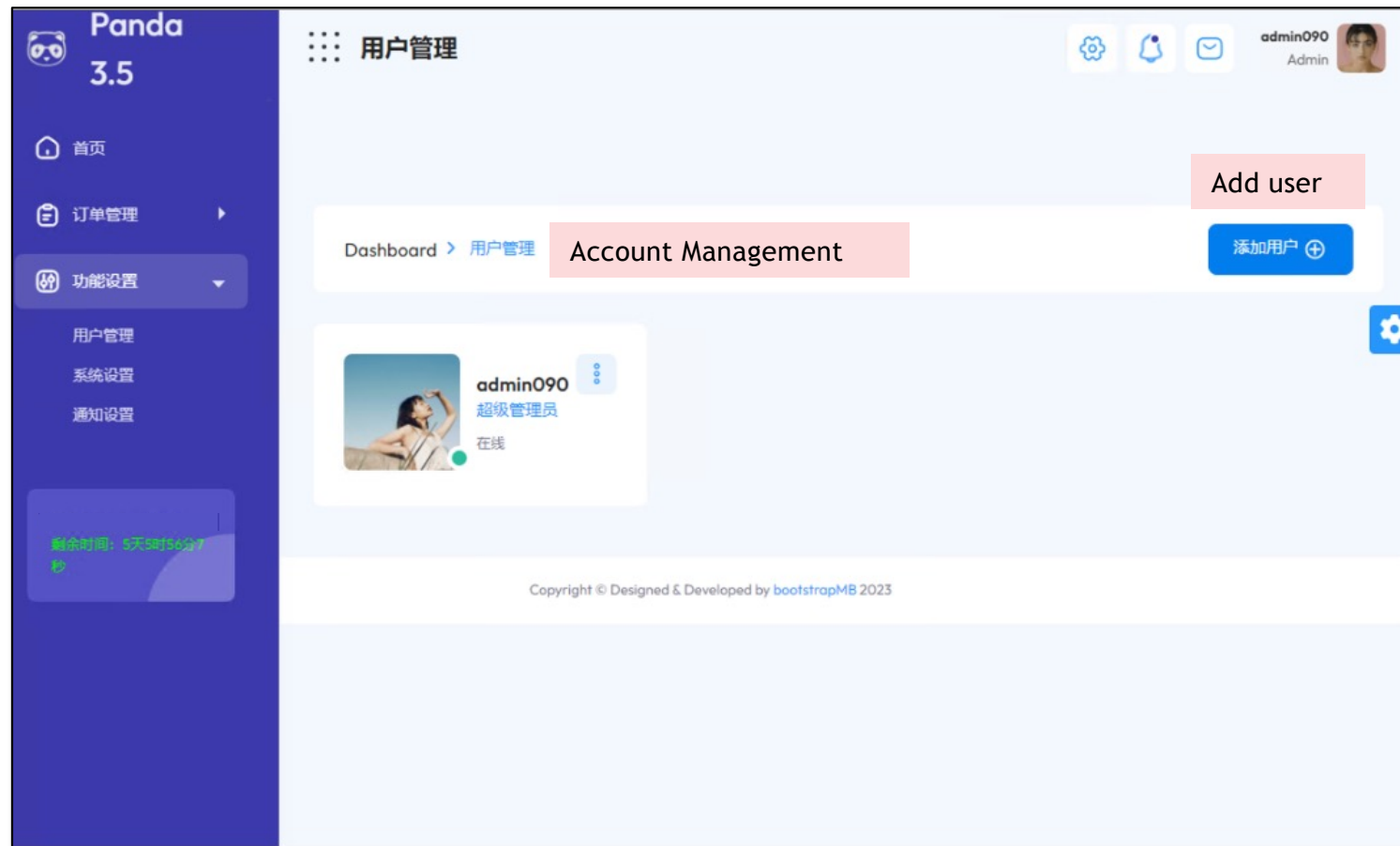
Total clicks

Successful visit

Interceptions



No. of users

# Account Management 增加帳號給工讀生

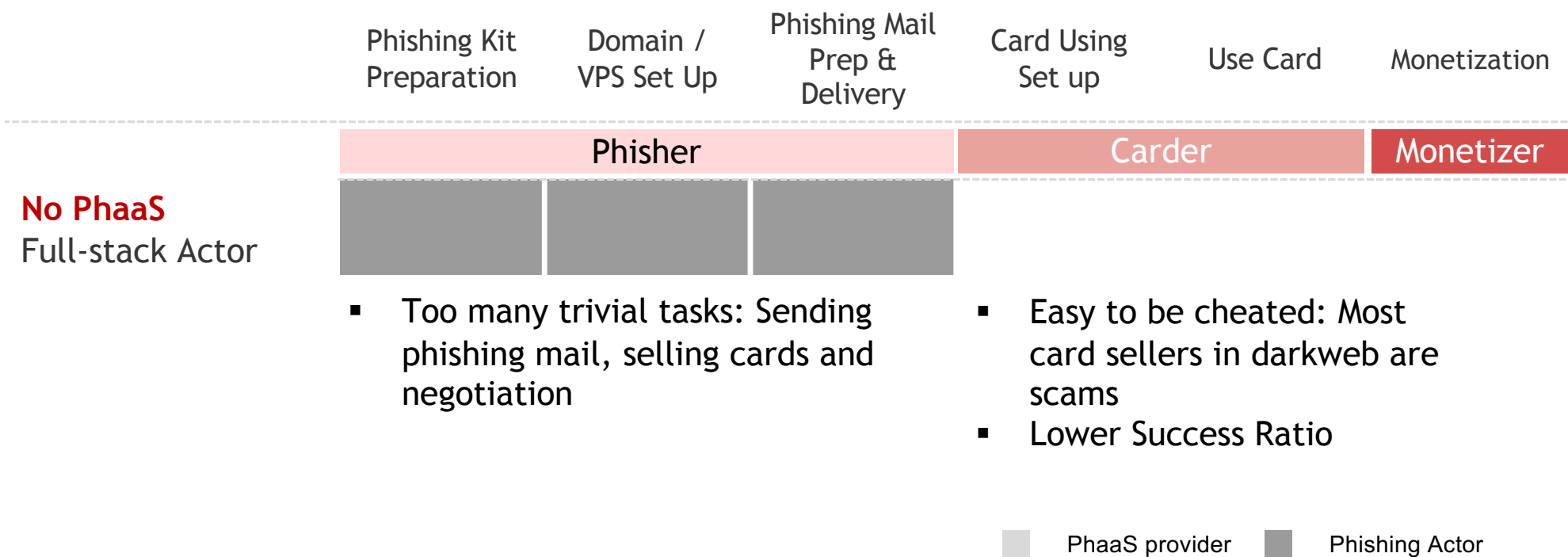


# Types of Phishing-as-a-Service

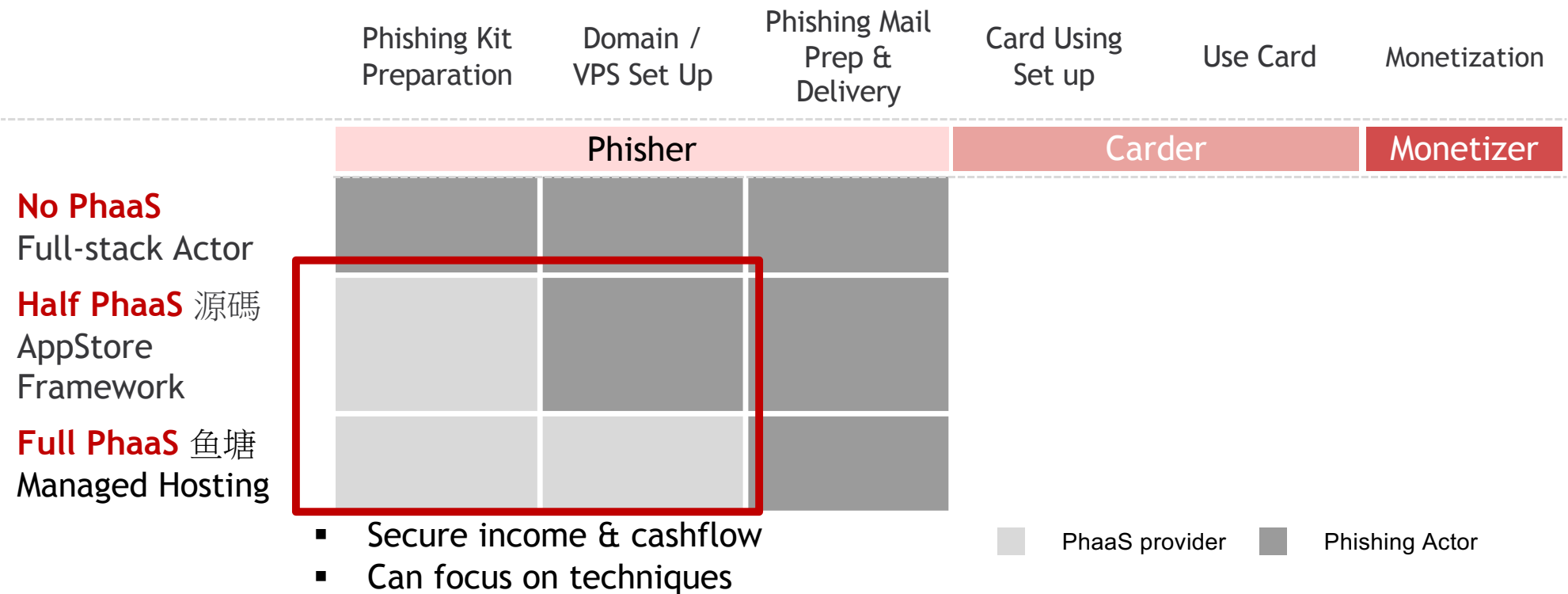
	Phishing Kit Preparation	Domain / VPS Set Up	Phishing Mail Prep & Delivery	Card Using Set up	Use Card	Monetization
	Phisher			Carder		Monetizer
<b>No PhaaS</b> Full-stack Actor						
<b>Half PhaaS</b> 源碼 AppStore Framework						
<b>Full PhaaS</b> 鱼塘 Managed Hosting						

 PhaaS provider     Phishing Actor

# Disadvantages of No-PhaaS



# Advantages of PhaaS: A more secure and positive environment for credit card fraudsters



# Advantages of PhaaS: A more secure and positive environment for credit card fraudsters

	Phishing Kit Preparation	Domain / VPS Set Up	Phishing Mail Prep & Delivery	Card Using Set up	Use Card	Monetization
	Phisher			Carder		Monetizer
<b>No PhaaS</b> Full-stack Actor						
<b>Half PhaaS</b> 源碼 AppStore Framework						
<b>Full PhaaS</b> 鱼塘 Managed Hosting						

- Earn illegal money without coding ability
- Low possibility to be cheated
- Have more control on the card information and quality



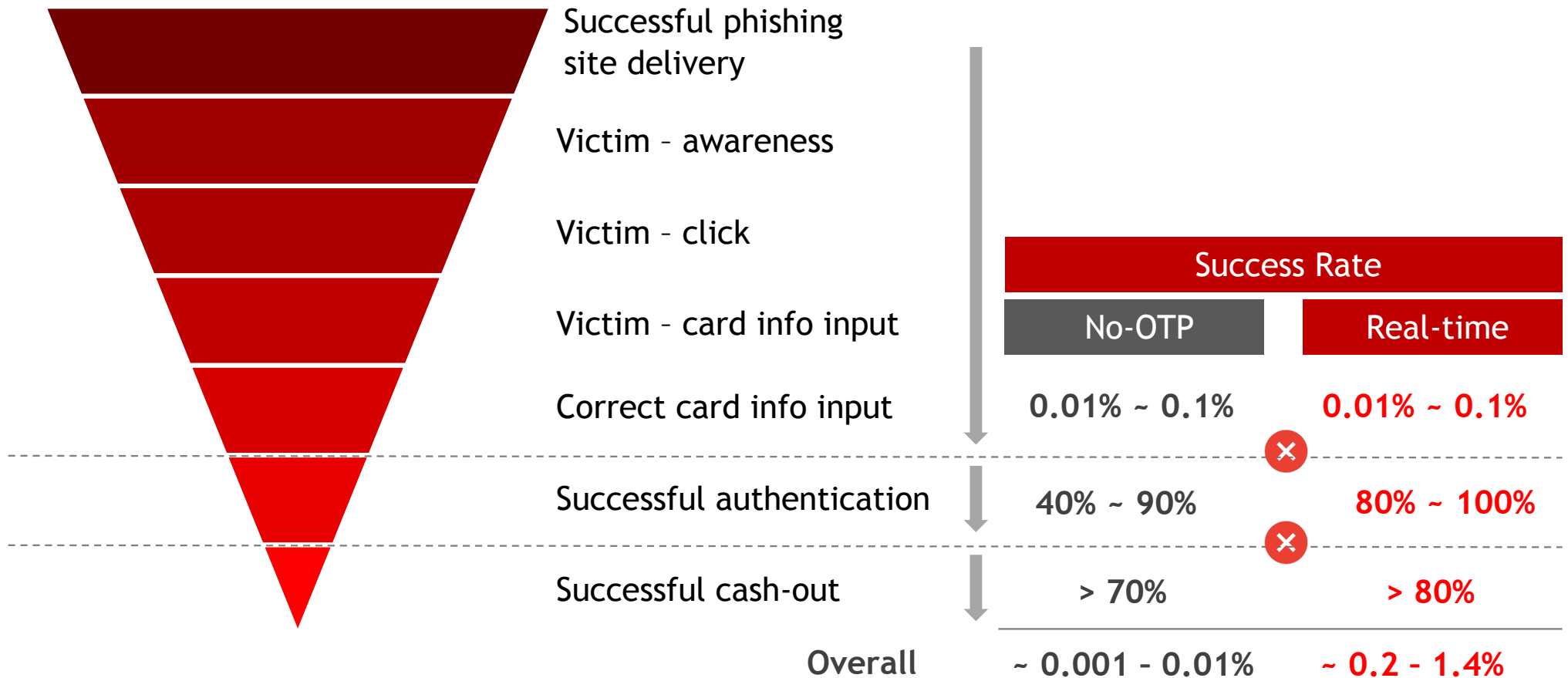
# Multiple income sources for the PhaaS providers

	Phishing Kit Preparation	Domain / VPS Set Up	Phishing Mail Prep & Delivery	Card Using Set up	Use Card	Monetization
	Phisher			Carder		Monetizer
<b>No PhaaS</b> Full-stack Actor						
<b>Half PhaaS</b> 源碼 AppStore Framework						
<b>Full PhaaS</b> 鱼塘 Managed Hosting						
	<ul style="list-style-type: none"> <li>Secure income &amp; cashflow</li> <li>Can focus on techniques</li> <li><b>Gain second-hand card info to resell / resue</b></li> </ul>			<ul style="list-style-type: none"> <li>Earn illegal money without coding ability</li> <li>Low possibility to be cheated</li> <li>Have more control on the card information and quality</li> </ul>		

The background of the slide is a solid black field. It is decorated with several horizontal streaks of bright red light. These streaks are blurred, giving them a sense of motion or a long-exposure photograph of light trails. There are three main horizontal streaks in the upper half of the slide, and several more in the lower half, some of which are slightly angled. The overall effect is modern and high-tech.

## Conclusion & Next Steps

## Success Rate of Real-time phishing is 2X of No-OTP !

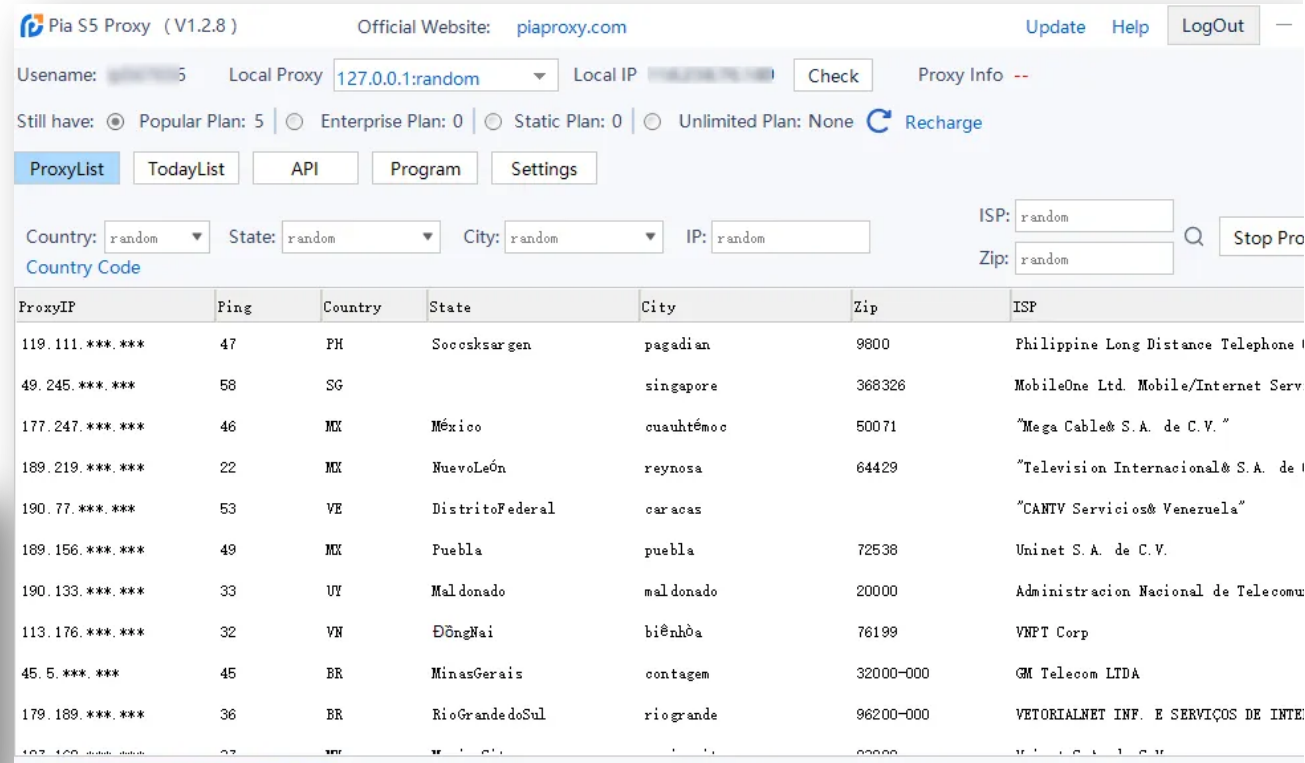
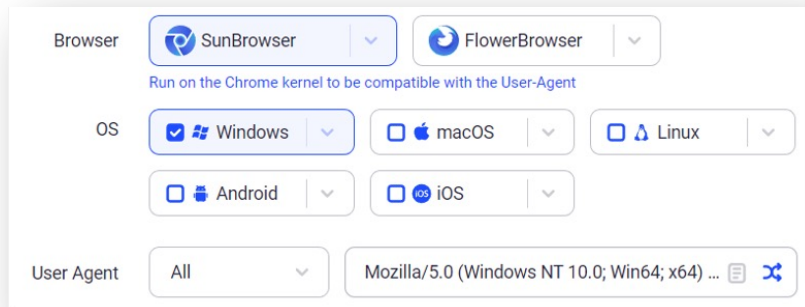


# No-OTP phishing fraudsters always mimic victims' environment in a more sophisticated manner than Real-time phishing

## No-OTP Phishing

### Challenges for defenders

- IP addresses can be forged through Residential Proxy
- User-agent can be forged through tools such as Adspower



# Real-time phishing is easier to detect due to inconsistent environment/behavior

## No-OTP Phishing

---

### Challenges for defenders

- IP addresses can be changed through Residential Proxy
- Useragent can be changed through tools such as Adspower

### Countermeasures for defenders

- Residential proxy database
- 3DSecure
- Passkeys and FIDO
- For Non-real-time services: Contact your customer

## Real-time Phishing

---

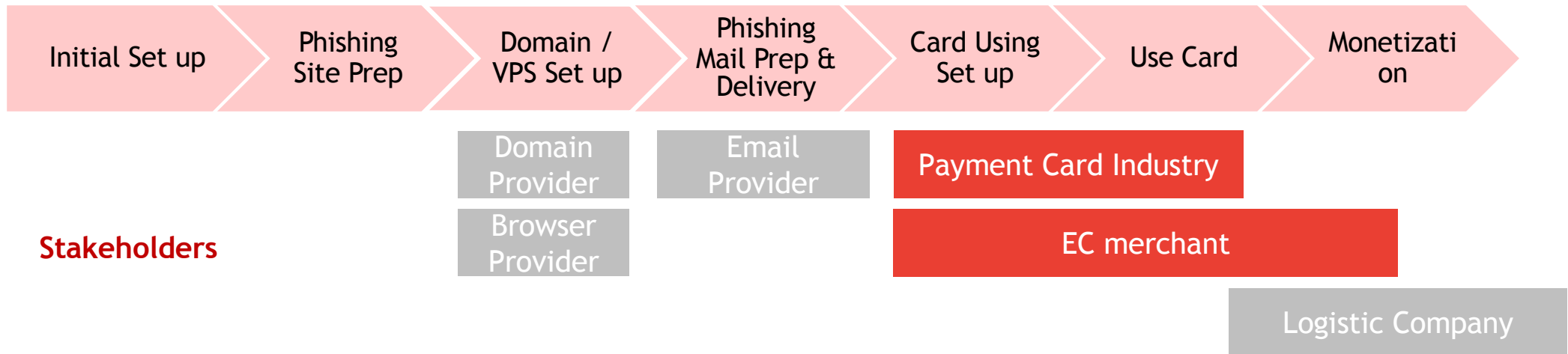
### Challenges for defenders

- Card Holder protection issue

### Countermeasures for defenders

- User Agent, IP, ISP, Language, screen size, geo-info not recorded → Can Easily Detect abnormal user behavior
- Fraudsters typically reuse device fingerprints & User Agents → Simplifying the tracking process
- For Non-real-time services: Contact your customer

# Countermeasures across the Phishing Value Chain



Payment Card Industry	<ul style="list-style-type: none"><li>▪ Mobile Identity Verification: Identity verification through telecom SIM</li><li>▪ Call/SMS your customer to verify transactions</li></ul>
EC	<ul style="list-style-type: none"><li>▪ Strong Authentication: Passkey, FIDO, Biometric Authentication, etc</li><li>▪ Device Fingerprinting, timezone, GPU, IP reputation</li><li>▪ Leverage AI/ML fraud detection Model</li><li>▪ Call/SMS your customer to verify transactions</li></ul>

# Key Takeaways

- PhaaS (Phishing-as-a-Service, 魚塘) 雲端代管訂閱制釣魚平台的流行，代表釣魚產業的專業分工更細緻化，用 AppStore 快速佈署新 phish kit，平台內建防紅等多種規避偵測，讓沒有技術背景的 actor 也能輕鬆上手！
- Real-time phishing (同步魚) 中間人攻擊的流行，突破 OTP 驗證機制，actor 必須 24 小時值班，收到通知立刻盜刷交易，尚不易模擬完整環境
- 專業分工、攻擊手法、經濟環境讓各國釣魚網站以 +50% YoY 高速成長，盜刷成功率達以往兩倍，GenAI 以 20 倍速產生新社交釣魚信和 Phish Kit
- 防守方也必須不斷更新偵測方法，傳統阻擋規則逐漸被 ML 偵測模型取代，參數的增加、每週重新訓練、各方情資交換、合作阻擋才能應對新手法。



Thank you

[strawberry.donut.research@gmail.com](mailto:strawberry.donut.research@gmail.com)

Twitter @strawberrylux