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
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
Mobile phone Trojan steals 20 million contacts

February 28, 2015 01:31 Source: Beijing Times

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
A notable case: Silent Plugin

- A criminal case

“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

- **2016**: Nougat
- **2017**: Oreo
- **2018**: Pie
- **2019**: Android 10
- **2020**: Android 11
- **2021**: Android 12
- **2022**: Android 13

**Timeline Events**

- **2013**: Arrested
- **2015**: Media report
- **2016**: Nougat
- **2017**: Oreo
- **2018**: Pie
- **2019**: Android 10
- **2020**: Android 11
- **2021**: Android 12
- **2022**: Android 13

**Key Highlights**

- **Triada** emerged “rooted” in 2017
- **First Triada in OEM, Google action** in 2017
- **Cosiloon on 100+ Android phones** in 2019
- **US government-provide phones found with pre-installed malware**
- **White-labelled Phone implanted with malware**
- **Sold in Africa Pre-installed Triada**
- **WhatsApp, APKpure mods Triada**
- **Gigaset 3rd party**

**Other Details**

- **36 Android Phones pre-installed with malware**
- **XHelper Pre-installed**
- **OEM image ✲ Vendor (Yehuo)**
- **Re-flashing subsided “silent Plugin”**
- **2011-2012**

**Additional Notes**

- **Stole 20M address book**
- **Silent Plugin**
- **Myanmar, Brazil**
- **3rd party**

**Abbreviations**

- **OEM**: Original Equipment Manufacturer
- **APKpure**: A platform for Android apps
- **WhatsApp**: A popular messaging app
- **Gigaset**: A brand for mobile phones
- **Yehuo**: A vendor mentioned in the context of Triada
- **Android**: A mobile operating system
Examples of news covering Triada

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 Upstream Systems.

By Michael Kan August 24, 2020
Triada Delivered via FOTA/OTA

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
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

Official client for the APKPure Android store compromised with malware

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

Version 3.17.19 of the APKPure application contained a copy of the TuxKino 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 app are advised to update to version 3.17.19, released earlier today, which remedied the malware from their devices.

ZCoup SDK Integration

1. Introduction
2. Integration ZCoup SDK

The Lemon Group: SMS PVA dealer
Public encounter of Lemon group

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.duoc.com (6.27.5). It is also strange that EngineerMode and Memory-calls and SMS climb on drapi.lemor91.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.
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!

*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
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
Lemon network Infrastructure can be linked to Malicious Android Applications
Lemon “pluggable” Apps Design

Preinstalled Loader

C2 request

backend
Other plugins from Lemon Group

Lemon Group Supply
Chain Compromise
Architecture
SMS PVA and acquisition of short messages
SMS PVA + SMS Interception

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
SMS PVA +SMS Interception

1. Account creation success
   - Type confirmation code to the platform where account is registered and continue registration

2. Sign up with Facebook
   - Username
   - Password
   - Singapore
   - Email
   - 9876543210
   - Mobile number

3. Initiate registration process on the service website or application till the confirmation number for SMS

4. Receive a confirmation code using PVA portal request
   - On the PVA portal request a phone number and type it as a confirmation number for SMS

5. SMS intercepted and sent to PVA related C2
   - SMS is landed on the victim phone while intercepted and sent to PVA related C2
   - One intercepts SMS, matches regular expression: "Carousell.\?\(\d\(4\)\)."
   - SMS is not visible to a phone owner
   - This happens on the infected phone

By signing up, you agree to Carousell's Terms of Service & Privacy Policy
SMS PVA + SMS Interception

**Account creation success**

SMS intercepted and sent to PVA related C2

**5**

**SMS is landed on the victim phone while intercepted and sent to PVA related C2**

**dex file running on infected phone intercepts SMS, matches regular expression:**

`.\*Carousell\.*\(\d\{4\}\)`

**SMS is not visible to a phone owner**

*This happens on the infected phone*
SMS Plugin (Guerilla)

Receive RegEx from C2 for SMS interception “wsRuleList”

Intercept SMS “startHook”

Send SMS to backend with matching RegEx “matchedBody”
Lemon SMS PVA Codes Project List

<table>
<thead>
<tr>
<th>Project ID (parameter pid=)</th>
<th>Platform</th>
<th>URL Detection</th>
<th>Sample SMS OTP</th>
<th>RegEx</th>
</tr>
</thead>
<tbody>
<tr>
<td>pid=0148</td>
<td>LINE</td>
<td>744651</td>
<td>Please enter 1234 into LINE within .<em>?(d(4,6)).</em>(?:(?:?LINE)</td>
<td>(?)))</td>
</tr>
<tr>
<td>pid=0092</td>
<td>Jingdong</td>
<td>8556</td>
<td>The verification code is 123456 (do. .*?(d(6)).<em>JD.</em></td>
<td>*(?:(?:?JD)</td>
</tr>
<tr>
<td>pid=0275</td>
<td>WeChat</td>
<td>391</td>
<td>WeChat verification code (123456). *(?:(?:?WeChat)</td>
<td>(?))))</td>
</tr>
<tr>
<td>pid=0146</td>
<td>Jingdong</td>
<td>205</td>
<td>The verification code is 123456, pl.e. .*?(d(6)).<em>JD.</em></td>
<td>*(?:(?:?JD)</td>
</tr>
<tr>
<td>pid=0013</td>
<td>Facebook</td>
<td>138</td>
<td>123456 is Name's Facebook confirm. *(?:(?:?Facebook)</td>
<td>(?)))*</td>
</tr>
<tr>
<td>pid=0107</td>
<td>WhatsApp</td>
<td>110</td>
<td>your whatsapp code: 123-456 you can .[^\d]+(\d[\d]-\d[\d])[[^\d]+.]*</td>
<td>*(?:(?:?Facebook)</td>
</tr>
<tr>
<td>pid=0504</td>
<td>up live</td>
<td>100</td>
<td>【Uplive】 [123456] is your verification code. *(?:(?:?Uplive)</td>
<td>(?)))*</td>
</tr>
<tr>
<td>pid=1115</td>
<td>Albert (Financial)</td>
<td>89</td>
<td>Use 123456 as your login code for T.<em>Tinder.</em>?(d(6)).*</td>
<td>*(?:(?:?Tinder)</td>
</tr>
<tr>
<td>pid=0046</td>
<td>Tinder</td>
<td>68</td>
<td>[Taobao.com] You applied for mob. *(?:(?:?Taobao)</td>
<td>(?)))*</td>
</tr>
<tr>
<td>pid=0015</td>
<td>Taobao</td>
<td>25</td>
<td>Authentic your Skype callers will .*?(AZ</td>
<td>az|0-9)[6]).*Skype.</td>
</tr>
<tr>
<td>pid=0389</td>
<td>Skype</td>
<td>8</td>
<td>09111111 You apply registration .<em>?(d(4,6)).</em></td>
<td>*(?:(?:?Skype)</td>
</tr>
<tr>
<td>pid=0085</td>
<td>Alipay</td>
<td>6</td>
<td>WeChat verification code (123456). *(?:(?:?WeChat)</td>
<td>(?))))</td>
</tr>
<tr>
<td>pid=0066</td>
<td>WeChat</td>
<td>5</td>
<td>G-123456 is your Google verification. *(?:(?:?WeChat)</td>
<td>(?))))</td>
</tr>
<tr>
<td>pid=0097</td>
<td>Gmail</td>
<td>3</td>
<td>&lt;#&gt; 1234 is your onetime verification. *(?:(?:?IRCTC)</td>
<td>(?)))*</td>
</tr>
<tr>
<td>pid=0183</td>
<td>irctc</td>
<td>1</td>
<td>【Apple】 Your Apple ID verification. *(?:(?:?Apple)</td>
<td>(?)))*</td>
</tr>
<tr>
<td>pid=123</td>
<td>Apple ID</td>
<td>1</td>
<td></td>
<td>*(?:(?:?Apple)</td>
</tr>
</tbody>
</table>

1000+ RegEx rules?
SMS PVA Codes for Jingdong Fraud

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

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

http://www.myzaker.com/article/5f44bf728e9f09748031fb92
Proxy Plugin (Guerilla)

- Proxy plugin
- Opens a proxy (socks5) service
- On infected device for requested period of time
So who is lemon? A Company in Hainan?
Recent developments: durian, no more lemon!
impact of compromised SMSes and verification codes
Coordinated Inauthentic Behavior

- Anonymity
- Circumvent regional restriction
- Consumer Privacy (compromised phone)

Sign-in Bonuses (abuse)
App Gamification Bonus (abuse)

Avoiding penalties, liabilities

Other Scams, Fraud
Identity theft and SMS interception

• In many countries phones are de-facto 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 third-party 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 fake 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 or 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)

- 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
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


Thank you!
Questions?