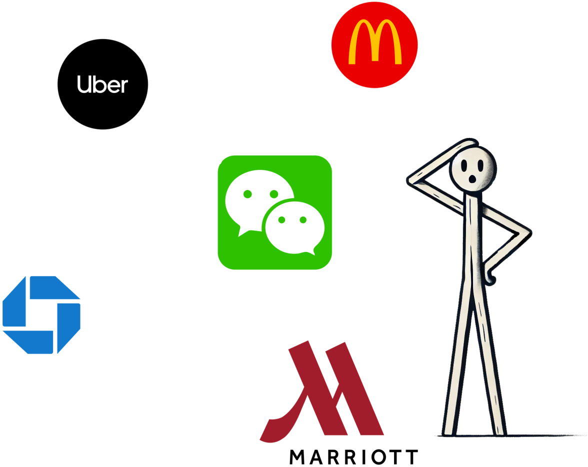
The Dark Side of Super Apps: Unmasking the Threats from Miniapp Malware

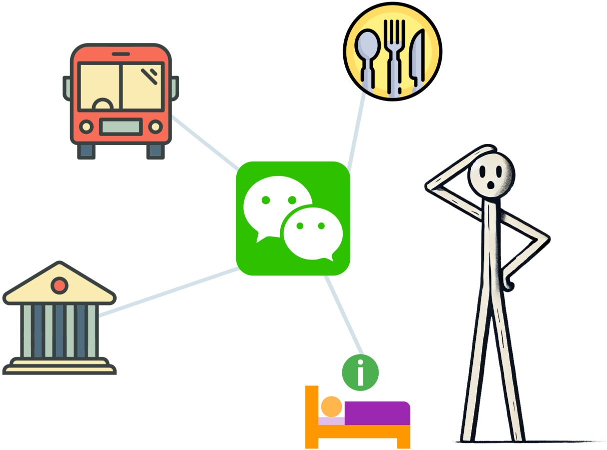
Zhiqiang Lin
Distinguished Professor of Engineering
zlin@cse.ohio-state.edu

October 14^{th}, 2024

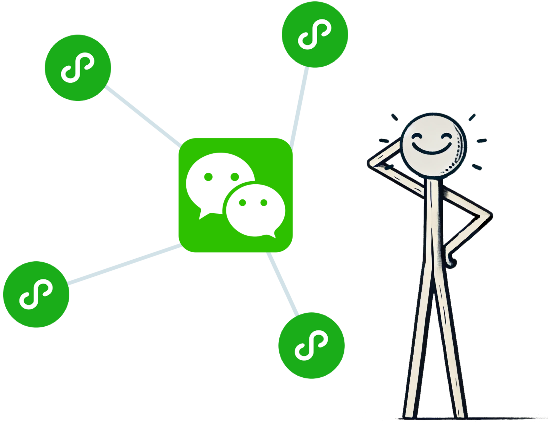
The Birth of “Miniapps”



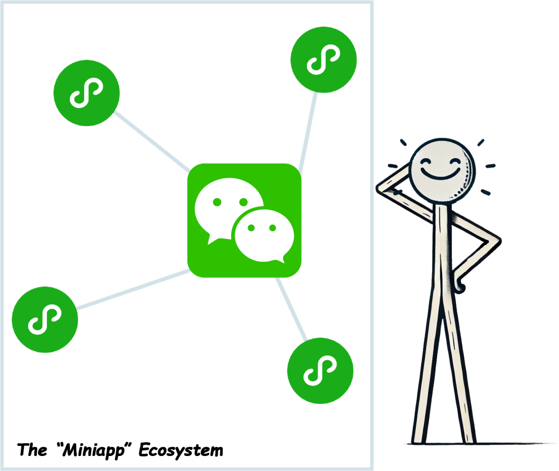
The Birth of “Miniapps”



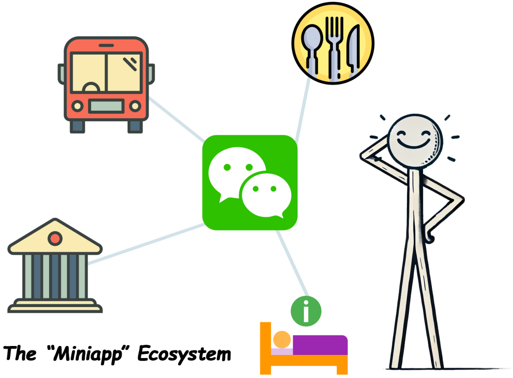
The Birth of “Miniapps”



The Birth of “Miniapps”

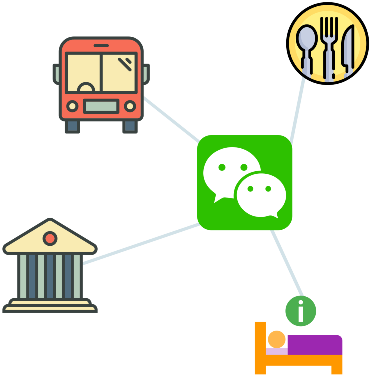


The Birth of “Miniapps”



- A **cross-platform** (Android/iOS) solution
- A product that “**meets all user needs**”
- Merges **convenience** in both PC webpage and mobile QR code

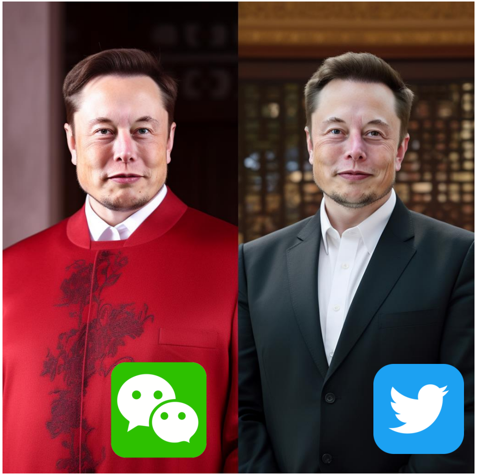
The case of WeChat



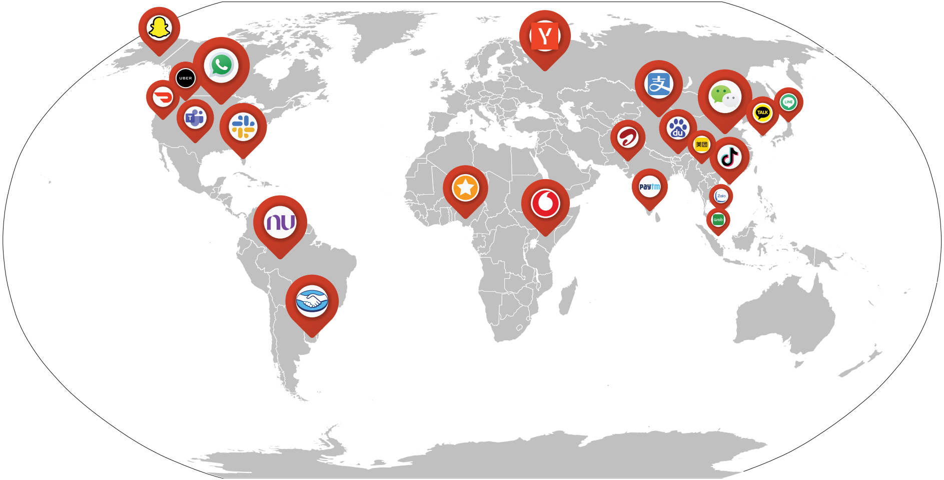
- Miniapps are **extending** WeChat
- WeChat provides a single **unified** environment for miniapps
- All miniapps are **centralized** under WeChat platform
- More than **four million** miniapps

What is WeChat?

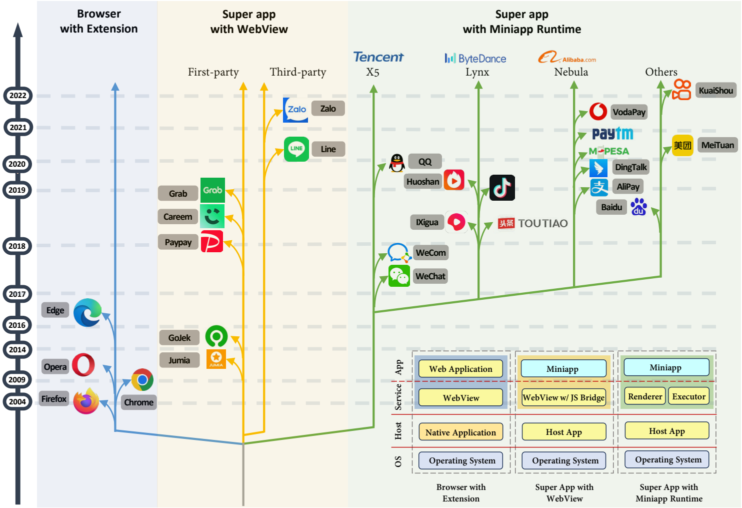
> ”It’s sort of like Twitter, plus PayPal, plus a whole bunch of things all rolled into one, with a great interface.”
>
> — Elon Musk



Successors worldwide



Successors worldwide

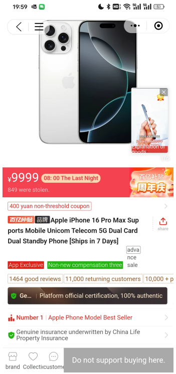


Case study: PinDuoDuo (Shopping Miniapp)

- Chinese shopping app
- 600M+ monthly user
- Mkt cap $200B

Case study: PinDuoDuo (Shopping Miniapp)

- Chinese shopping app
- 600M+ monthly user
- Mkt cap $200B



¥9999 08: 00 The Last Night

849 were stolen.

400 yuan non-threshold coupon

百亿补贴 品牌 Apple iPhone 16 Pro Max Supports Mobile Unicom Telecom 5G Dual Card Dual Standby Phone [Ships in 7 Days]

advance sale

App Exclusive | Non-new compensation three

1464 good reviews | 11,000 returning customers | 10,000 + p

Ge... | Platform official certification, 100% authentic

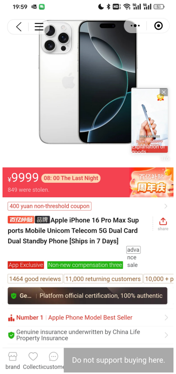
Number 1 | Apple Phone Model Best Seller

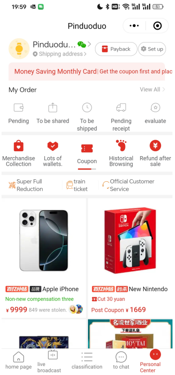
Genuine insurance underwritten by China Life Property Insurance

Do not support buying here.

Case study: PinDuoDuo (Shopping Miniapp)

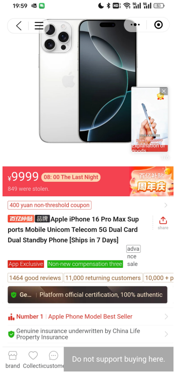
- Chinese shopping app
- 600M+ monthly user
- Mkt cap $200B

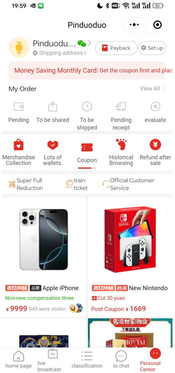

¥9999 08: 00 The Last Night
849 were stolen.
400 yuan non-threshold coupon
百亿补贴 品牌 Apple iPhone 16 Pro Max Supports Mobile Unicom Telecom 5G Dual Card Dual Standby Phone [Ships in 7 Days]
App Exclusive | Non-new compensation three | advance sale
1464 good reviews | 11,000 returning customers | 10,000 + p
Ge... | Platform official certification, 100% authentic
Number 1 | Apple Phone Model Best Seller
Genuine insurance underwritten by China Life Property Insurance
Do not support buying here.

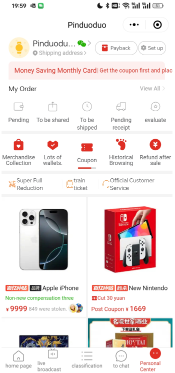

Pinduoduo
Money Saving Monthly Card | Get the coupon first and plac
My Order
百亿补贴 品牌 Apple iPhone
Non-new compensation three
¥9999 849 were stolen.
百亿补贴 秒杀 New Nintendo
Cut 30 yuan
Post Coupon ¥1669

Case study: PinDuoDuo (Shopping Miniapp)

- Chinese shopping app
- 600M+ monthly user
- Mkt cap $200B


19:59
¥9999 08: 00 The Last Night
849 were stolen.
百亿补贴
周年庆
400 yuan non-threshold coupon
百亿补贴 品牌 Apple iPhone 16 Pro Max Supports Mobile Unicom Telecom 5G Dual Card Dual Standby Phone [Ships in 7 Days]
share
App Exclusive
Non-new compensation three
advance sale
1464 good reviews
11,000 returning customers
10,000 + p
Ge... Platform official certification, 100% authentic
Number 1 Apple Phone Model Best Seller
Genuine insurance underwritten by China Life Property Insurance
brand
Collect
customer
Do not support buying here.





Case study: Mini Jumper (Gaming Miniapp)

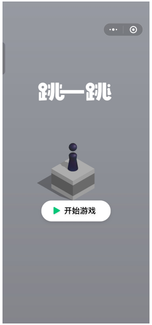
- Mini Jumper
- A miniapp game
- 100M+ daily user

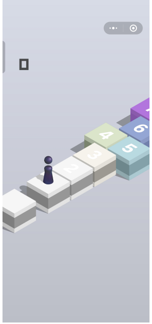
Case study: Mini Jumper (Gaming Miniapp)

- Mini Jumper
- A miniapp game
- 100M+ daily user

Case study: Mini Jumper (Gaming Miniapp)

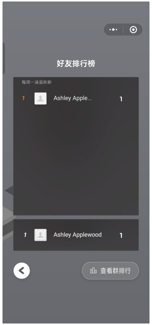
- Mini Jumper
- A miniapp game
- 100M+ daily user



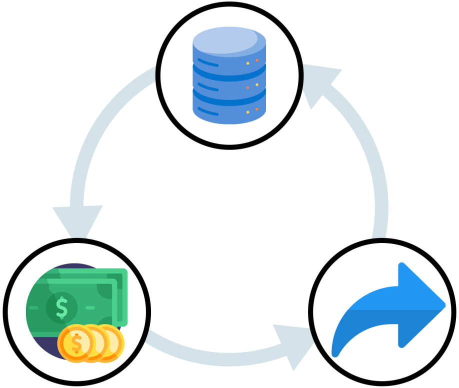


Case study: Mini Jumper (Gaming Miniapp)

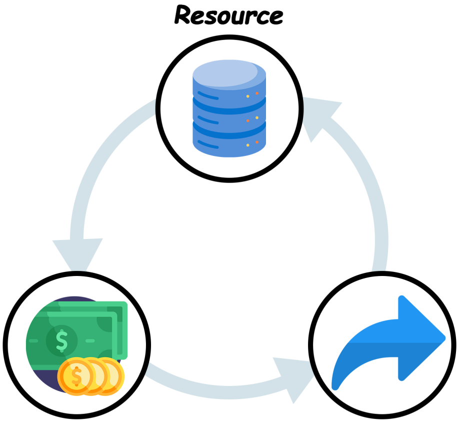
- Mini Jumper
- A miniapp game
- 100M+ daily user



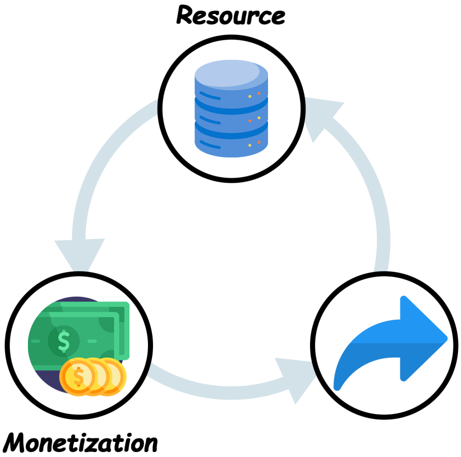
The Miniapp Capability Model



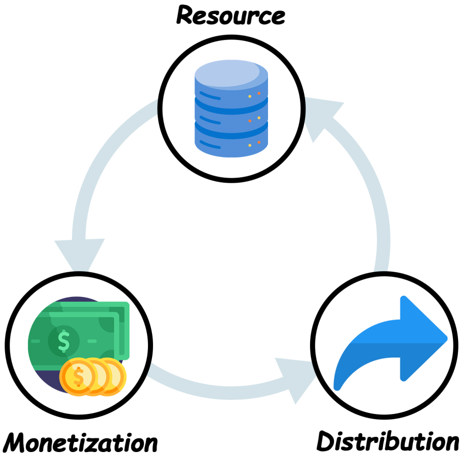
The Miniapp Capability Model



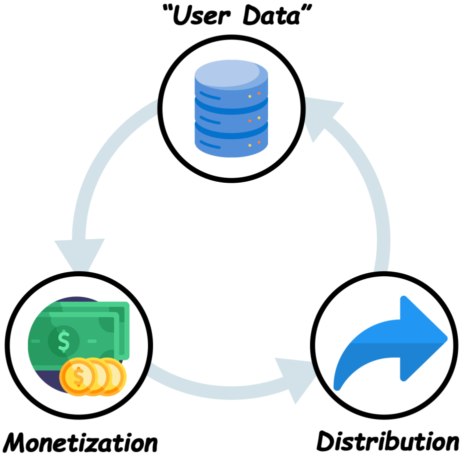
The Miniapp Capability Model



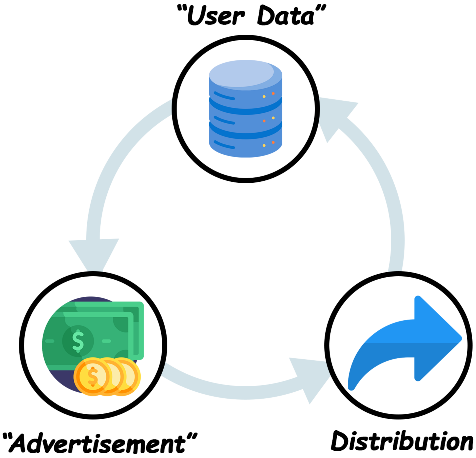
The Miniapp Capability Model



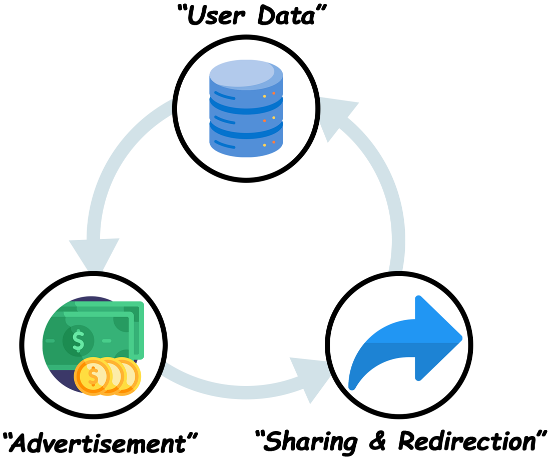
The Miniapp Capability Model



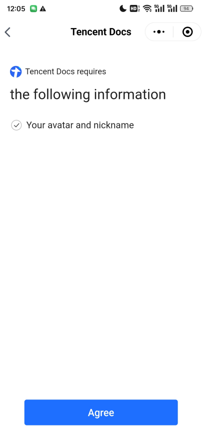
The Miniapp Capability Model



The Miniapp Capability Model



Resources: platform-managed user data



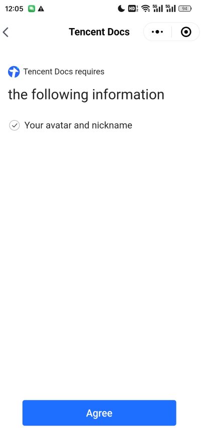
Tencent Docs

Tencent Docs requires

the following information

✓ Your avatar and nickname

Resources: platform-managed user data



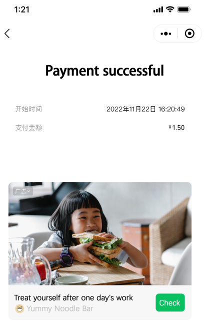
Tencent Docs requires

the following information

✓ Your avatar and nickname

User Data	APIs	Description
userInfo	wx.getUserInfo	User information
userLocation	wx.getLocation	Geographic location
userFuzzyLocation	wx.getFuzzyLocation	Fuzzy location
userLocationBackground	wx.startLocationUpdateBackground	Location in background
address	wx.chooseAddress	Postal address
invoiceTitle	wx.chooseInvoiceTitle	Invoice title
invoice	wx.chooseInvoice	Gets invoice
werun	wx.getWeRunData	WeRun step counts
record	wx.startRecord	Recording feature
writePhotosAlbum	wx.saveImageToPhotosAlbum	Saves to album
writePhotosAlbum	wx.saveVideoToPhotosAlbum	Saves to album
camera	camera Component	Camera
addPhoneContact	wx.addPhoneContact	Add to contact
addPhoneCalendar	wx.addPhoneRepeatCalendar	Add to calendar

Monetization: traffic-based advertisements (texts are translated)



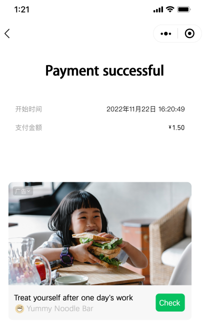
1:21

Payment successful

开始时间	2022年11月22日 16:20:49
支付金额	¥1.50

Payment Ad

Monetization: traffic-based advertisements (texts are translated)



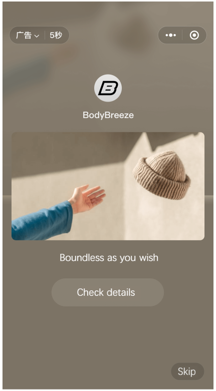
1:21

Payment successful

开始时间 2022年11月22日 16:20:49

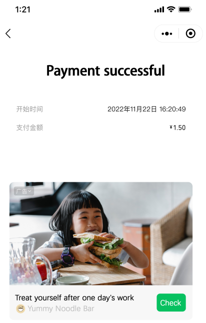
支付金额 ¥1.50

Payment Ad



Cover Ad

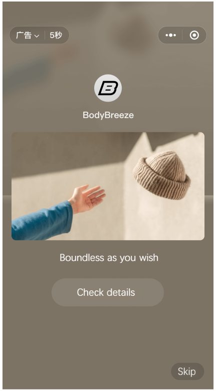
Monetization: traffic-based advertisements (texts are translated)



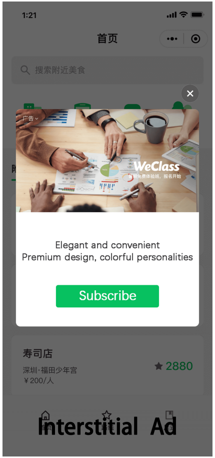
Payment successful

开始时间	2022年11月22日 16:20:49
支付金额	¥1.50

Payment Ad



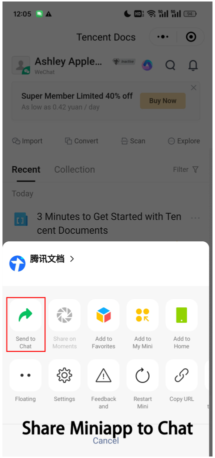
Cover Ad



Elegant and convenient
Premium design, colorful personalities

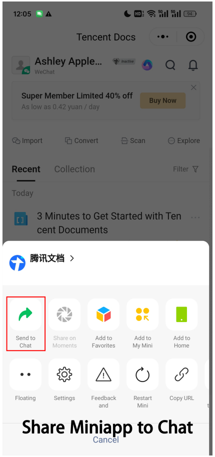
Interstitial Ad

Distribution: platform-controlled channels (texts translated)

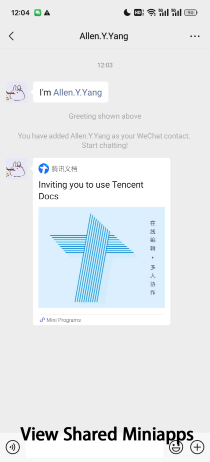


Share Miniapp to Chat

Distribution: platform-controlled channels (texts translated)



Share Miniapp to Chat



I'm Allen.Y.Yang

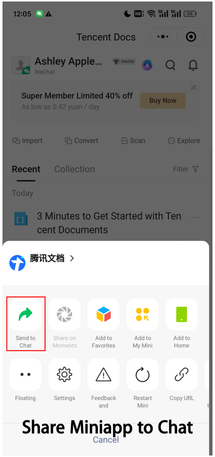
Greeting shown above

You have added Allen.Y.Yang as your WeChat contact. Start chatting!

Inviting you to use Tencent Docs

View Shared Miniapps

Distribution: platform-controlled channels (texts translated)



12:05

Tencent Docs

Ashley Apple...
WeChat

Super Member Limited 40% off
As low as 0.42 yuan / day
Buy Now

Import Convert Scan Explore

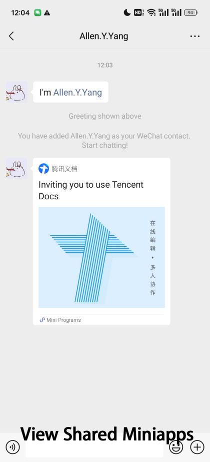
Recent Collection Filter

Today

3 Minutes to Get Started with Tencent Documents

腾讯文档 >

Share Miniapp to Chat



12:04

Allen.Y.Yang

12:03

I'm Allen.Y.Yang

Greeting shown above

You have added Allen.Y.Yang as your WeChat contact. Start chatting!

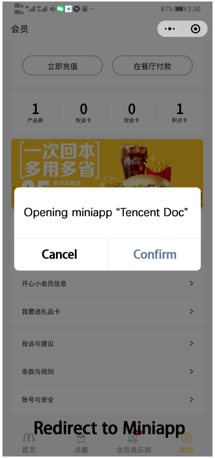
腾讯文档

Inviting you to use Tencent Docs

在线编辑，多人协作

Mini Programs

View Shared Miniapps



87% 2:30

会员

立即充值 在餐厅付款

1	0	0	1
产品券	权益卡	现金卡	积点卡

Opening miniapp “Tencent Doc”

Cancel Confirm

开心小会员信息 >

我要送礼品卡 >

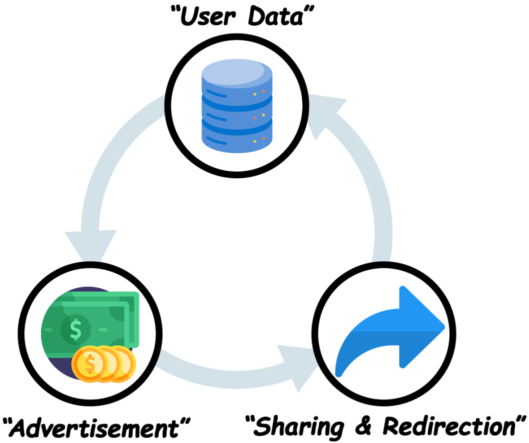
投诉与建议 >

条款与规则 >

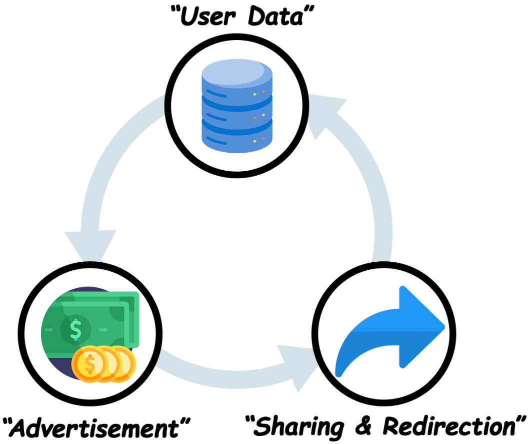
账号与安全 >

Redirect to Miniapp

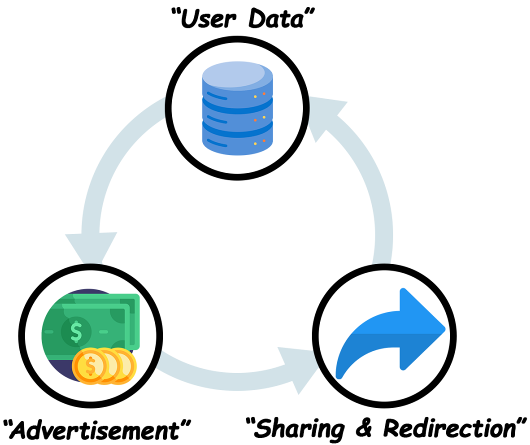
To ensure a secure platform...



To ensure a secure platform...

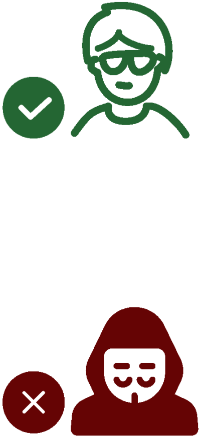


To ensure a secure platform...

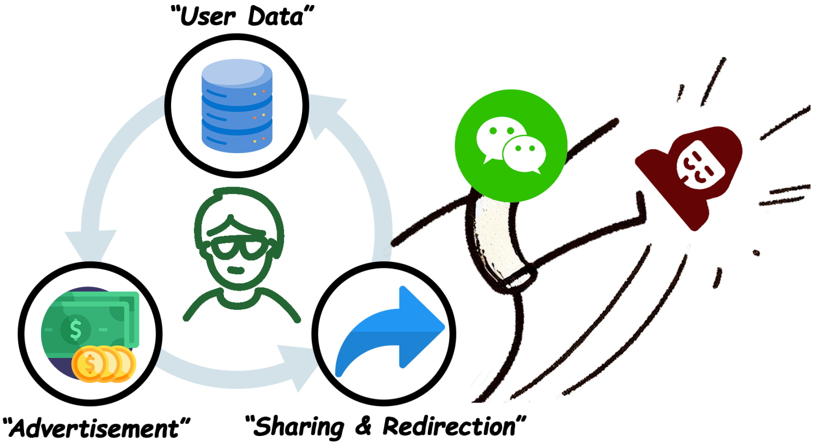

"User Data"

"Advertisement"

"Sharing & Redirection"



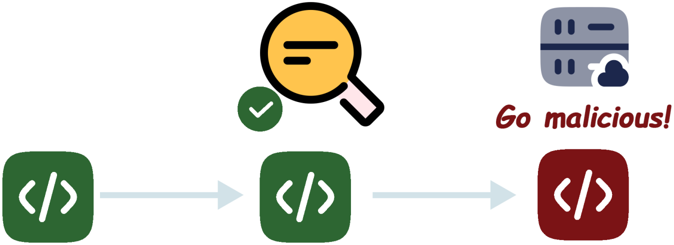
To ensure a secure platform...



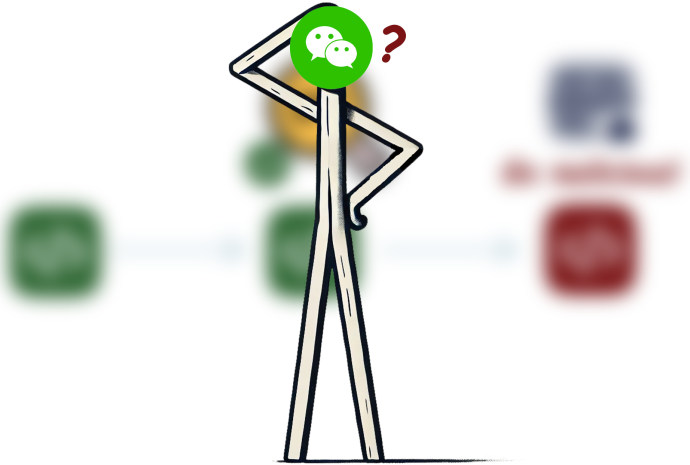
To ensure a secure platform...

Miniapp Vetting!

How to Break the Vetting?



How to Break the Vetting?



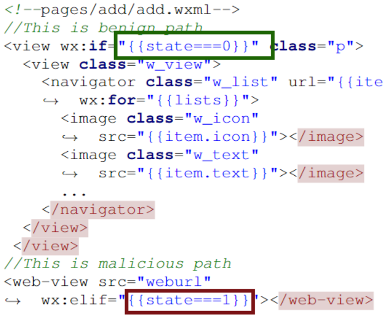
How to Break the Vetting?

- **Split behavior**: dynamically changing miniapp behavior
  - **Content vetting** evasion

How to Break the Vetting?

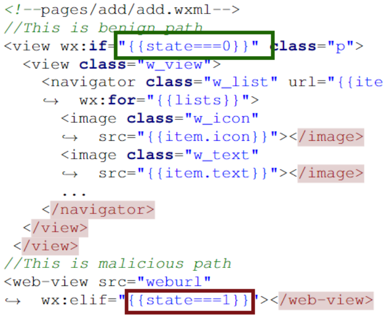
- **Split behavior**: dynamically changing miniapp behavior
  - **Content vetting** evasion
  - **Code vetting** evasion

Content Vetting Evasion

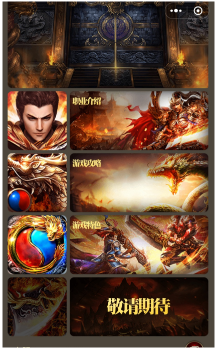


```
<!--pages/add/add.wxml-->
//This is benign path
<view wx:if="{{state===0}}" class="p">
  <view class="w_view">
    <navigator class="w_list" url="{{ite
    ↪  wx:for="{{lists}}">
      <image class="w_icon"
      ↪  src="{{item.icon}}"></image>
      <image class="w_text"
      ↪  src="{{item.text}}"></image>
      ...
    </navigator>
  </view>
 </view>
//This is malicious path
<web-view src="weburl"
↪  wx:elif="{{state===1}}"></web-view>
```

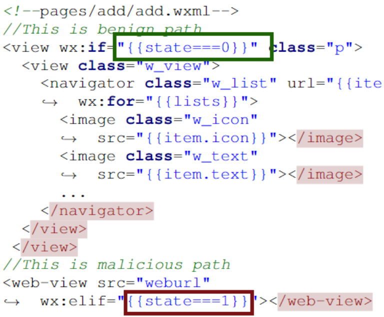
Content Vetting Evasion



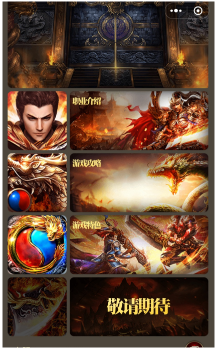
```
<!--pages/add/add.wxml-->
//This is benign path
<view wx:if="{{state===0}}" class="p">
  <view class="w_view">
    <navigator class="w_list" url="{{ite
    ↪   wx:for="{{lists}}">
      <image class="w_icon"
      ↪   src="{{item.icon}}"></image>
      <image class="w_text"
      ↪   src="{{item.text}}"></image>
      ...
    </navigator>
  </view>
 </view>
//This is malicious path
<web-view src="weburl"
↪   wx:elif="{{state===1}}"></web-view>
```

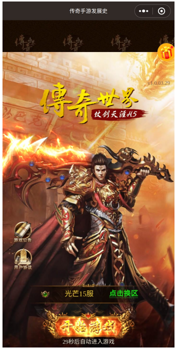


Content Vetting Evasion



```
<!--pages/add/add.wxml-->
//This is benign path
<view wx:if="{{state===0}}" class="p">
  <view class="w_view">
    <navigator class="w_list" url="{{ite
    ↪   wx:for="{{lists}}">
      <image class="w_icon"
      ↪   src="{{item.icon}}"></image>
      <image class="w_text"
      ↪   src="{{item.text}}"></image>
      ...
    </navigator>
  </view>
 </view>
//This is malicious path
<web-view src="weburl"
↪   wx:elif="{{state===1}}"></web-view>
```

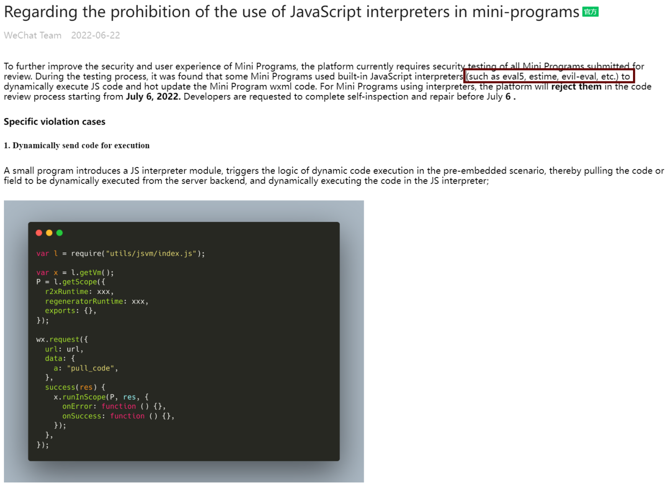




Content Vetting Evasion

- `state == 0`: A “Tool” Miniapp providing game tutorial
- `state == 1`: A camouflaged gaming miniapp supporting fraudulous payment
- Webview points to URL **controlled fully by malicious developers**

Code Vetting Evasion: Libs supporting hot-update banned in 2022



Regarding the prohibition of the use of JavaScript interpreters in mini-programs 官方

WeChat Team 2022-06-22

To further improve the security and user experience of Mini Programs, the platform currently requires security testing of all Mini Programs submitted for review. During the testing process, it was found that some Mini Programs used built-in JavaScript interpreters (such as eval5, estime, evil-eval, etc.) to dynamically execute JS code and hot update the Mini Program wxml code. For Mini Programs using interpreters, the platform will **reject them** in the code review process starting from **July 6, 2022.** Developers are requested to complete self-inspection and repair before July **6 .**

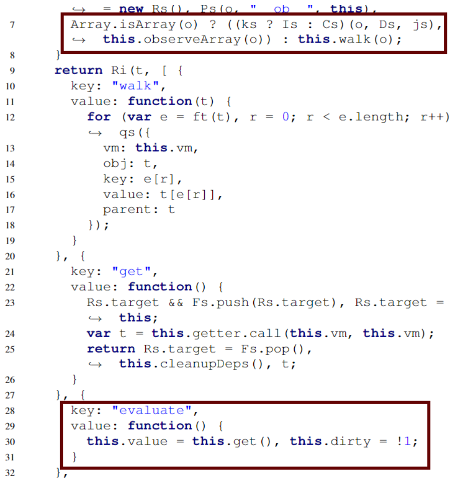
Specific violation cases

1. Dynamically send code for execution

A small program introduces a JS interpreter module, triggers the logic of dynamic code execution in the pre-embedded scenario, thereby pulling the code or field to be dynamically executed from the server backend, and dynamically executing the code in the JS interpreter;

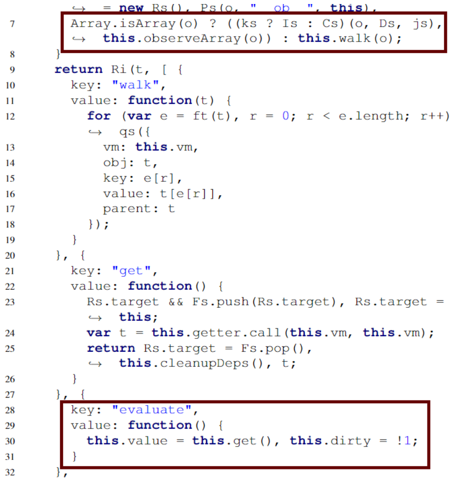
```
var l = require("utils/jsvm/index.js");

var x = l.getVm();
P = l.getScope({
  r2xRuntime: xxx,
  regeneratorRuntime: xxx,
  exports: {},
});

wx.request({
  url: url,
  data: {
    a: "pull_code",
  },
  success(res) {
    x.runInScope(P, res, {
      onError: function () {},
      onSuccess: function () {},
    });
  },
});
```

Code Vetting Evasion: Developing their own hot-update code



```
  ↪  = new Rs(), Ps(o, "  ob  ", this),
  Array.isArray(o) ? ((ks ? Is : Cs)(o, Ds, js),
  ↪  this.observeArray(o)) : this.walk(o);
}
return Ri(t, [ {
  key: "walk",
  value: function(t) {
    for (var e = ft(t), r = 0; r < e.length; r++)
    ↪  qs({
      vm: this.vm,
      obj: t,
      key: e[r],
      value: t[e[r]],
      parent: t
    });
  }
}, {
  key: "get",
  value: function() {
    Rs.target && Fs.push(Rs.target), Rs.target =
    ↪  this;
    var t = this.getter.call(this.vm, this.vm);
    return Rs.target = Fs.pop(),
    ↪  this.cleanupDeps(), t;
  }
}, {
  key: "evaluate",
  value: function() {
    this.value = this.get(), this.dirty = !1;
  }
},
```

Code Vetting Evasion: Developing their own hot-update code



```
      ↪  = new Rs(), Ps(o, "  ob  ", this),
    Array.isArray(o) ? ((ks ? Is : Cs)(o, Ds, js),
    ↪  this.observeArray(o)) : this.walk(o);
  }
  return Ri(t, [ {
    key: "walk",
    value: function(t) {
      for (var e = ft(t), r = 0; r < e.length; r++)
      ↪  qs({
        vm: this.vm,
        obj: t,
        key: e[r],
        value: t[e[r]],
        parent: t
      });
    }
  }, {
    key: "get",
    value: function() {
      Rs.target && Fs.push(Rs.target), Rs.target =
      ↪  this;
      var t = this.getter.call(this.vm, this.vm);
      return Rs.target = Fs.pop(),
      ↪  this.cleanupDeps(), t;
    }
  }, {
    key: "evaluate",
    value: function() {
      this.value = this.get(), this.dirty = !1;
    }
  },
```

- Implements APIs to evaluate node value
- Resembles relevant code in hot update libs

Defining the maliciousness signatures

- Assumption: malware **must** pass the vetting to cause effect

Defining the maliciousness signatures

- Assumption: malware **must** pass the vetting to cause effect
- The “**Evasive signature**” check:

Defining the maliciousness signatures

- Assumption: malware **must** pass the vetting to cause effect
- The “**Evasive signature**” check:
  - Code-based evasion: signatures of “hot-update” libraries
  - Content-based evasion: webview in conditional rendering (wx:if)

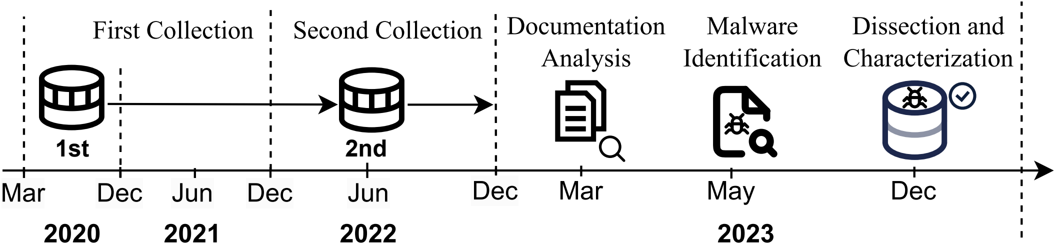
Defining the maliciousness signatures

- Assumption: malware **must** pass the vetting to cause effect
- The “**Evasive signature**” check:
  - Code-based evasion: signatures of “hot-update” libraries
  - Content-based evasion: webview in conditional rendering (wx:if)
- The “**Platform removal**” check:

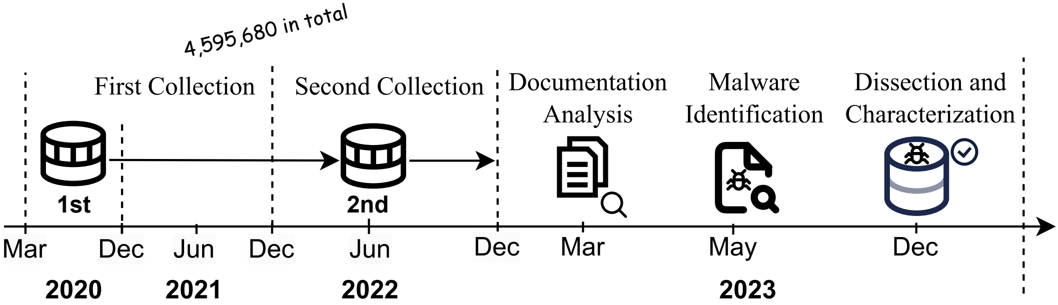
Defining the maliciousness signatures

- Assumption: malware **must** pass the vetting to cause effect
- The “**Evasive signature**” check:
    - Code-based evasion: signatures of “hot-update” libraries
    - Content-based evasion: webview in conditional rendering (wx:if)
- The “**Platform removal**” check:
    - Delisted miniapps are highly likely to violate regulation
    - Finding delisted miniapps helps to certify “evasive signature” check

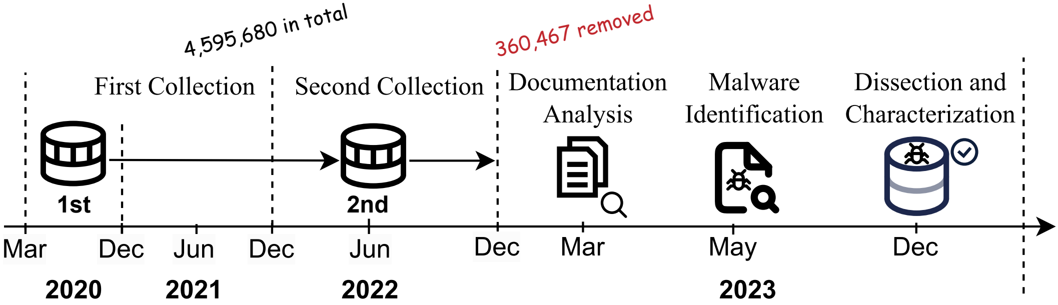
A three year collection process



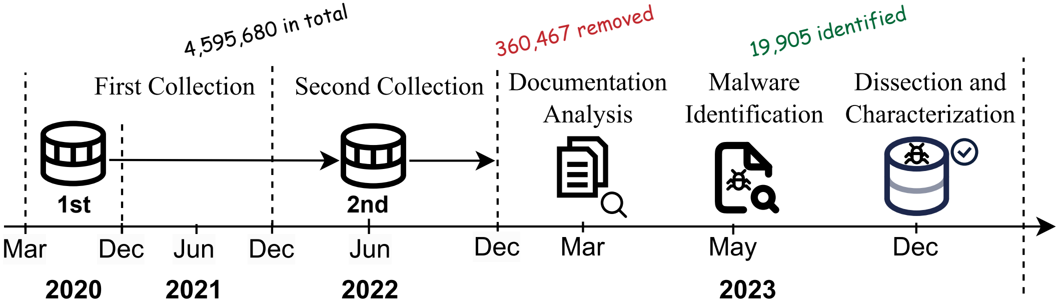
A three year collection process



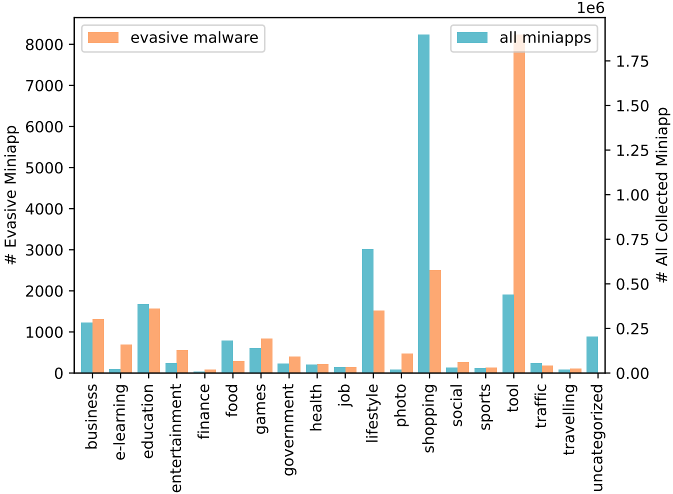
A three year collection process



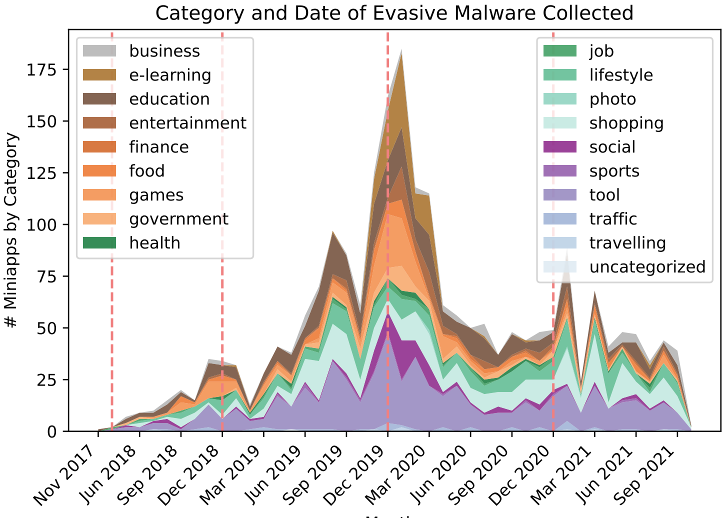
A three year collection process



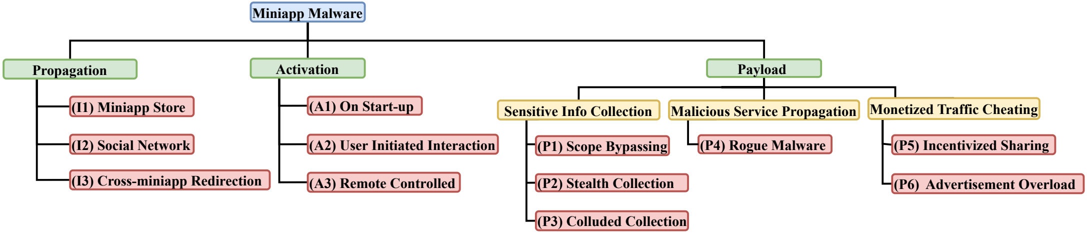
Categorial Distribution



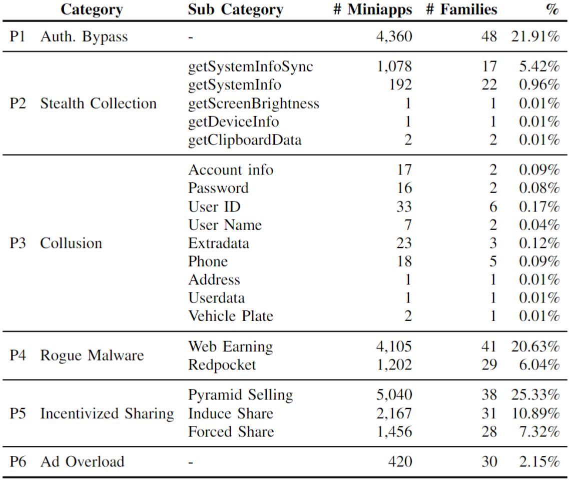
Longitudinal Distribution



Malware Lifecycle

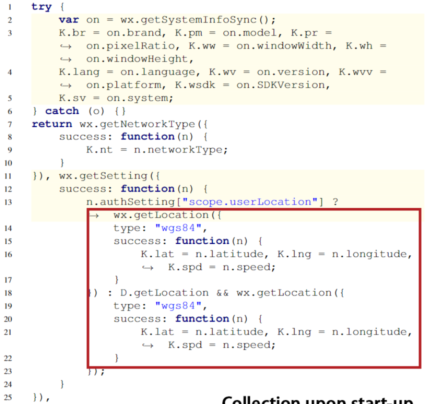


Malware Payloads



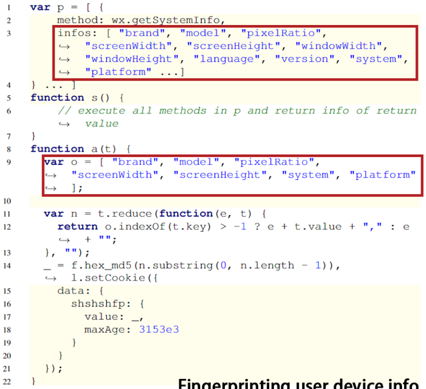
	Category	Sub Category	# Miniapps	# Families	%
P1	Auth. Bypass	-	4,360	48	21.91%
P2	Stealth Collection	getSystemInfoSync	1,078	17	5.42%
		getSystemInfo	192	22	0.96%
		getScreenBrightness	1	1	0.01%
		getDeviceInfo	1	1	0.01%
		getClipboardData	2	2	0.01%
P3	Collusion	Account info	17	2	0.09%
		Password	16	2	0.08%
		User ID	33	6	0.17%
		User Name	7	2	0.04%
		Extradata	23	3	0.12%
		Phone	18	5	0.09%
		Address	1	1	0.01%
		Userdata	1	1	0.01%
		Vehicle Plate	2	1	0.01%
P4	Rogue Malware	Web Earning	4,105	41	20.63%
		Redpocket	1,202	29	6.04%
P5	Incentivized Sharing	Pyramid Selling	5,040	38	25.33%
		Induce Share	2,167	31	10.89%
		Forced Share	1,456	28	7.32%
P6	Ad Overload	-	420	30	2.15%

Privacy Collection Going Stealth



```
try {
    var on = wx.getSystemInfoSync();
    K.br = on.brand, K.pm = on.model, K.pr =
    ↪ on.pixelRatio, K.ww = on.windowWidth, K.wh =
    ↪ on.windowHeight,
    K.lang = on.language, K.wv = on.version, K.wvv =
    ↪ on.platform, K.wsdk = on.SDKVersion,
    K.sv = on.system;
} catch (o) {}
return wx.getNetworkType({
    success: function(n) {
        K.nt = n.networkType;
    }
}), wx.getSetting({
    success: function(n) {
        n.authSetting["scope.userLocation"] ?
        ↪ wx.getLocation({
            type: "wgs84",
            success: function(n) {
                K.lat = n.latitude, K.lng = n.longitude,
                ↪ K.spd = n.speed;
            }
        }) : D.getLocation && wx.getLocation({
            type: "wgs84",
            success: function(n) {
                K.lat = n.latitude, K.lng = n.longitude,
                ↪ K.spd = n.speed;
            }
        });
    }
}),
```

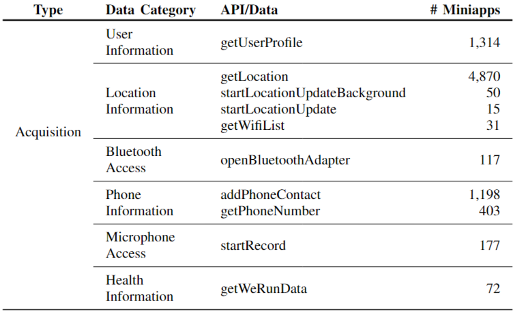
Collection upon start-up



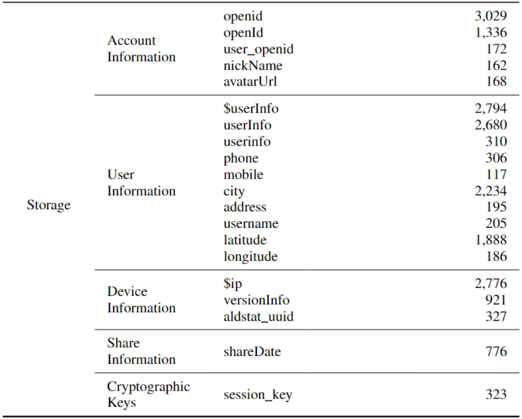
```
var p = [ {
    method: wx.getSystemInfo,
    infos: [ "brand", "model", "pixelRatio",
    ↪ "screenWidth", "screenHeight", "windowWidth",
    ↪ "windowHeight", "language", "version", "system",
    ↪ "platform" ...]
} ... ]
function s() {
    // execute all methods in p and return info of return
    ↪ value
}
function a(t) {
  var o = [ "brand", "model", "pixelRatio",
  ↪ "screenWidth", "screenHeight", "system", "platform"
  ↪ ];

  var n = t.reduce(function(e, t) {
    return o.indexOf(t.key) > -1 ? e + t.value + "," : e
    ↪ + "";
  }, "");
  _ = f.hex_md5(n.substring(0, n.length - 1)),
  ↪ l.setCookie({
    data: {
      shshshfp: {
        value: _,
        maxAge: 3153e3
      }
    }
  });
}
```

Fingerprinting user device info

Data Acquisition Being Sensitive

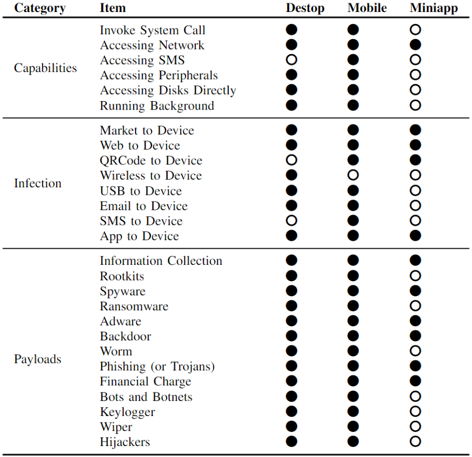


Type	Data Category	API/Data	# Miniapps
Acquisition	User Information	getUserProfile	1,314
	Location Information	getLocation	4,870
		startLocationUpdateBackground	50
		startLocationUpdate	15
		getWifiList	31
	Bluetooth Access	openBluetoothAdapter	117
	Phone Information	addPhoneContact	1,198
		getPhoneNumber	403
	Microphone Access	startRecord	177
	Health Information	getWeRunData	72



Storage	Account Information	openid	3,029
		openId	1,336
		user_openid	172
		nickName	162
		avatarUrl	168
	User Information	$userInfo	2,794
		userInfo	2,680
		userinfo	310
		phone	306
		mobile	117
		city	2,234
		address	195
		username	205
		latitude	1,888
		longitude	186
	Device Information	$ip	2,776
		versionInfo	921
		aldstat_uuid	327
	Share Information	shareDate	776
	Cryptographic Keys	session_key	323

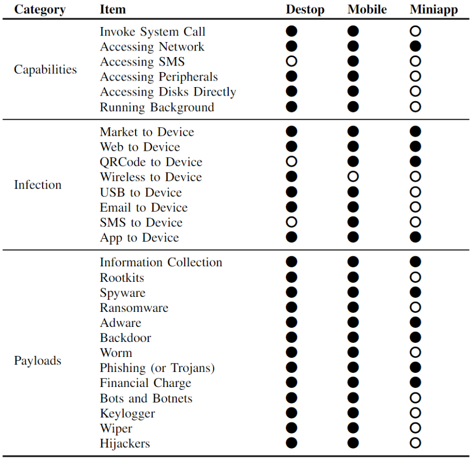
Miniapp Malware vs Traditional Malware



Category	Item	Destop	Mobile	Miniapp
Capabilities	Invoke System Call	●	●	○
	Accessing Network	●	●	●
	Accessing SMS	○	●	○
	Accessing Peripherals	●	●	○
	Accessing Disks Directly	●	●	○
	Running Background	●	●	○
Infection	Market to Device	●	●	●
	Web to Device	●	●	●
	QRCode to Device	○	●	●
	Wireless to Device	●	○	○
	USB to Device	●	●	○
	Email to Device	●	●	○
	SMS to Device	○	●	○
	App to Device	●	●	●
Payloads	Information Collection	●	●	●
	Rootkits	●	●	○
	Spyware	●	●	●
	Ransomware	●	●	○
	Adware	●	●	●
	Backdoor	●	●	●
	Worm	●	●	○
	Phishing (or Trojans)	●	●	●
	Financial Charge	●	●	●
	Bots and Botnets	●	●	○
	Keylogger	●	●	○
	Wiper	●	●	○
	Hijackers	●	●	○

- Miniapp capabilities are more restricted

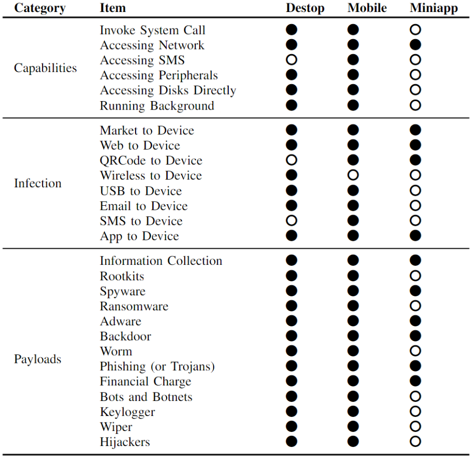
Miniapp Malware vs Traditional Malware



Category	Item	Destop	Mobile	Miniapp
Capabilities	Invoke System Call	●	●	○
	Accessing Network	●	●	●
	Accessing SMS	○	●	○
	Accessing Peripherals	●	●	○
	Accessing Disks Directly	●	●	○
	Running Background	●	●	○
Infection	Market to Device	●	●	●
	Web to Device	●	●	●
	QRCode to Device	○	●	●
	Wireless to Device	●	○	○
	USB to Device	●	●	○
	Email to Device	●	●	○
	SMS to Device	○	●	○
	App to Device	●	●	●
Payloads	Information Collection	●	●	●
	Rootkits	●	●	○
	Spyware	●	●	●
	Ransomware	●	●	○
	Adware	●	●	●
	Backdoor	●	●	●
	Worm	●	●	○
	Phishing (or Trojans)	●	●	●
	Financial Charge	●	●	●
	Bots and Botnets	●	●	○
	Keylogger	●	●	○
	Wiper	●	●	○
	Hijackers	●	●	○

- Miniapp capabilities are more restricted
- Miniapps rely on social networks

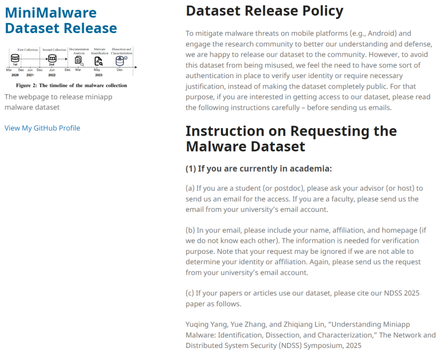
Miniapp Malware vs Traditional Malware



Category	Item	Destop	Mobile	Miniapp
Capabilities	Invoke System Call	●	●	○
	Accessing Network	●	●	●
	Accessing SMS	○	●	○
	Accessing Peripherals	●	●	○
	Accessing Disks Directly	●	●	○
	Running Background	●	●	○
Infection	Market to Device	●	●	●
	Web to Device	●	●	●
	QRCode to Device	○	●	●
	Wireless to Device	●	○	○
	USB to Device	●	●	○
	Email to Device	●	●	○
	SMS to Device	○	●	○
	App to Device	●	●	●
Payloads	Information Collection	●	●	●
	Rootkits	●	●	○
	Spyware	●	●	●
	Ransomware	●	●	○
	Adware	●	●	●
	Backdoor	●	●	●
	Worm	●	●	○
	Phishing (or Trojans)	●	●	●
	Financial Charge	●	●	●
	Bots and Botnets	●	●	○
	Keylogger	●	●	○
	Wiper	●	●	○
	Hijackers	●	●	○

- Miniapp capabilities are more restricted
- Miniapps rely on social networks
- Victims can be the super apps

Dataset Release



MiniMalware Dataset Release

Figure 2: The timeline of the malware collection

The webpage to release miniapp malware dataset

View My GitHub Profile

Dataset Release Policy

To mitigate malware threats on mobile platforms (e.g., Android) and engage the research community to better our understanding and defense, we are happy to release our dataset to the community. However, to avoid this dataset from being misused, we feel the need to have some sort of authentication in place to verify user identity or require necessary justification, instead of making the dataset completely public. For that purpose, if you are interested in getting access to our dataset, please read the following instructions carefully – before sending us emails.

Instruction on Requesting the Malware Dataset

(1) If you are currently in academia:

(a) If you are a student (or postdoc), please ask your advisor (or host) to send us an email for the access. If you are a faculty, please send us the email from your university's email account.

(b) In your email, please include your name, affiliation, and homepage (if we do not know each other). The information is needed for verification purpose. Note that your request may be ignored if we are not able to determine your identity or affiliation. Again, please send us the request from your university's email account.

(c) If your papers or articles use our dataset, please cite our NDSS 2025 paper as follows.

Yuqing Yang, Yue Zhang, and Zhiqiang Lin, "Understanding Miniapp Malware: Identification, Dissection, and Characterization," The Network and Distributed System Security (NDSS) Symposium, 2025

[0] **"Understanding Miniapp Malware: Identification, Dissection, and Characterization"** Yuqing Yang, Yue Zhang, and Zhiqiang Lin. In NDSS 2025

Thank You

The Dark Side of Super Apps: Unmasking the Threats from Miniapp Malware

Zhiqiang Lin
Distinguished Professor of Engineering
zlin@cse.ohio-state.edu

October 14^{th}, 2024