XcodeGhost

Seon-Bok Yi
Yuan Ji

What is Xcode?

- An Integrated Development Environment (IDE) published by Apple.
- For developing software and apps for Mac computers, iphones, and ipads.

Xcode

What is XcodeGhost?

- Versions of Xcode modified by hackers.
- Injects malicious code into the apps during development of the application.

XcodeGhost

How was XcodeGhost discovered?

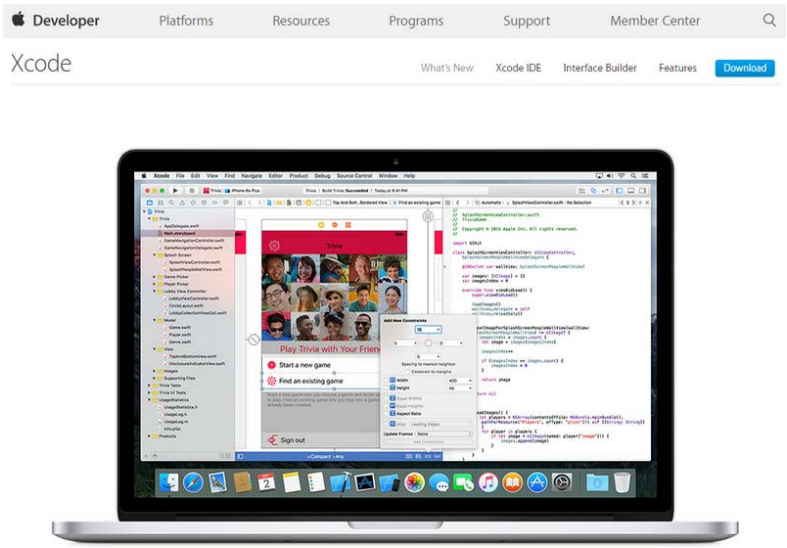
- In Sep, 2015, some Chinese iOS developers discovered third party code was injected into their apps.

How was XcodeGhost discovered?

- Extra library files were found in Xcode installer.

```
Xcode.app: a sealed resource is missing or invalid
file added: /Volumes/Xcode/Xcode.app/Contents/Developer/Platforms/iPhoneOS.platform/Developer/SDKs/Library/Frameworks/CoreServices.framework/CoreService
file added: /Volumes/Xcode/Xcode.app/Contents/Developer/Platforms/iPhoneOS.platform/Developer/SDKs/Library/PrivateFrameworks/IDEBundleInjection.framework/_
file added: /Volumes/Xcode/Xcode.app/Contents/Developer/Platforms/iPhoneOS.platform/Developer/SDKs/Library/PrivateFrameworks/IDEBundleInjection.framework/I
file added: /Volumes/Xcode/Xcode.app/Contents/Developer/Platforms/iPhoneOS.platform/Developer/SDKs/Library/PrivateFrameworks/IDEBundleInjection.framework/I
file added: /Volumes/Xcode/Xcode.app/Contents/Developer/Platforms/iPhoneOS.platform/Developer/SDKs/Library/PrivateFrameworks/IDEBundleInjection.framework/V
file added: /Volumes/Xcode/Xcode.app/Contents/Developer/Platforms/iPhoneSimulator.platform/Developer/SDKs/Library/Frameworks/CoreServices.framework/CoreSer
file added: /Volumes/Xcode/Xcode.app/Contents/Developer/Platforms/iPhoneSimulator.platform/Developer/SDKs/Library/PrivateFrameworks/IDEBundleInjection.fram
file added: /Volumes/Xcode/Xcode.app/Contents/Developer/Platforms/iPhoneSimulator.platform/Developer/SDKs/Library/PrivateFrameworks/IDEBundleInjection.fram
file added: /Volumes/Xcode/Xcode.app/Contents/Developer/Platforms/iPhoneSimulator.platform/Developer/SDKs/Library/PrivateFrameworks/IDEBundleInjection.fram
file added: /Volumes/Xcode/Xcode.app/Contents/Developer/Platforms/iPhoneSimulator.platform/Developer/SDKs/Library/PrivateFrameworks/IDEBundleInjection.fram
file added: /Volumes/Xcode/Xcode.app/Contents/Developer/Platforms/MacOSX.platform/Developer/SDKs/Library/Frameworks/CoreServices.framework/CoreService
file added: /Volumes/Xcode/Xcode.app/Contents/Developer/Platforms/MacOSX.platform/Developer/SDKs/Library/PrivateFrameworks/IDEBundleInjection.framework/IDE
file added: /Volumes/Xcode/Xcode.app/Contents/Developer/Platforms/MacOSX.platform/Developer/SDKs/Library/PrivateFrameworks/IDEBundleInjection.framework/Res
file added: /Volumes/Xcode/Xcode.app/Contents/Developer/Platforms/MacOSX.platform/Developer/SDKs/Library/PrivateFrameworks/IDEBundleInjection.framework/Ver
file added: /Volumes/Xcode/Xcode.app/Contents/Developer/Platforms/MacOSX.platform/Developer/SDKs/Library/PrivateFrameworks/IDEBundleInjection.framework/Ver
file added: /Volumes/Xcode/Xcode.app/Contents/Developer/Platforms/MacOSX.platform/Developer/SDKs/Library/PrivateFrameworks/IDEBundleInjection.framework/Ver
file added: /Volumes/Xcode/Xcode.app/Contents/Developer/Platforms/MacOSX.platform/Developer/SDKs/Library/PrivateFrameworks/IDEBundleInjection.framework/Ver
file added: /Volumes/Xcode/Xcode.app/Contents/Developer/Platforms/MacOSX.platform/Developer/SDKs/Library/PrivateFrameworks/IDEBundleInjection.framework/Ver
```

Why did developers use XcodeGhost to develop apps?



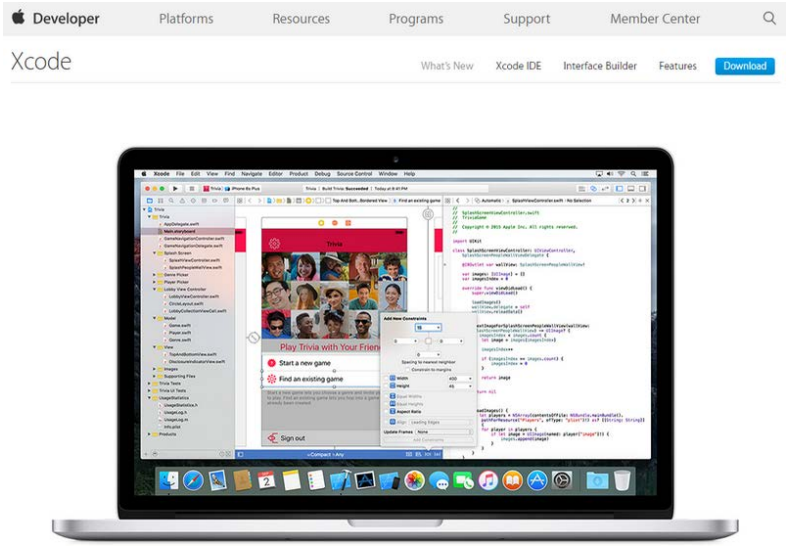
Apple's official website

Third party cloud storage

very slow

fast

Why did developers use XcodeGhost to develop apps?

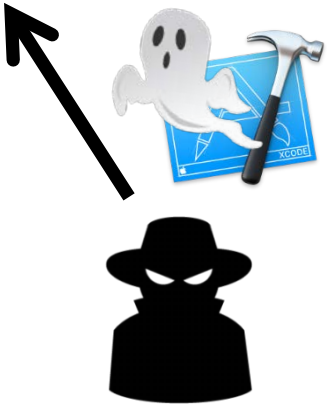


Apple's official website

Third party cloud storage

very slow

fast



How was malicious code injected into apps by XcodeGhost?

- When building an app, a compiler integrates code from library files into the app during compilation.

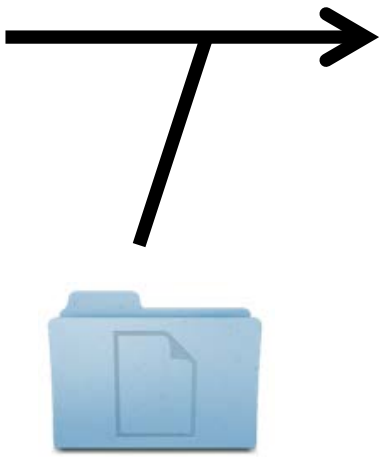
```
@interface TwitterRequest : NSObject {
    NSString        *username;
    NSString        *password;
    NSMutableData   *receivedData;
    NSURLRequest    *theRequest;
    NSURLConnection *theConnection;
    id               delegate;
    SEL              callback;
    SEL              errorCallback;
}

@property(nonatomic, retain) NSString      *username;
@property(nonatomic, retain) NSString      *password;
@property(nonatomic, retain) NSMutableData *receivedData;
@property(nonatomic, retain) id             delegate;
@property(nonatomic) SEL                    callback;
@property(nonatomic) SEL                    errorCallback;

-(void)friends_timeline:(id)requestDelegate requestSelector:(SEL)requestSelector;
-(void)request:(NSURL *) url;

@end
```

Compiled to machine language



Library files: offer in-app purchase, database support

How was malicious code injected into apps by XcodeGhost?

- Hacker modified the library files provided by the Xcode IDE.

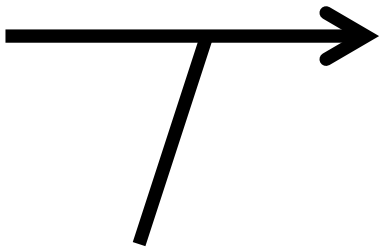
```
@interface TwitterRequest : NSObject {
    NSString        *username;
    NSString        *password;
    NSMutableData   *receivedData;
    NSURLRequest    *theRequest;
    NSURLConnection *theConnection;
    id               delegate;
    SEL              callback;
    SEL              errorCallback;
}

@property(nonatomic, retain) NSString      *username;
@property(nonatomic, retain) NSString      *password;
@property(nonatomic, retain) NSMutableData *receivedData;
@property(nonatomic, retain) id             delegate;
@property(nonatomic) SEL                    callback;
@property(nonatomic) SEL                    errorCallback;

-(void)friends_timeline:(id)requestDelegate requestSelector:(SEL)requestSelector;
-(void)request:(NSURL *) url;

@end
```

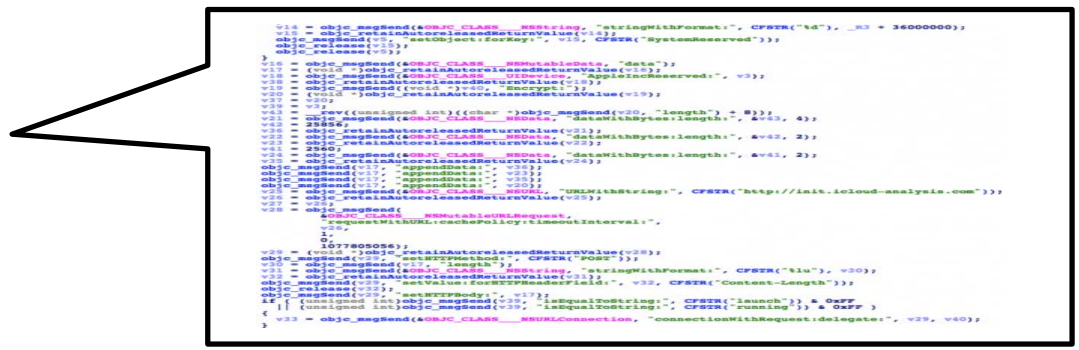
Compiled to machine language

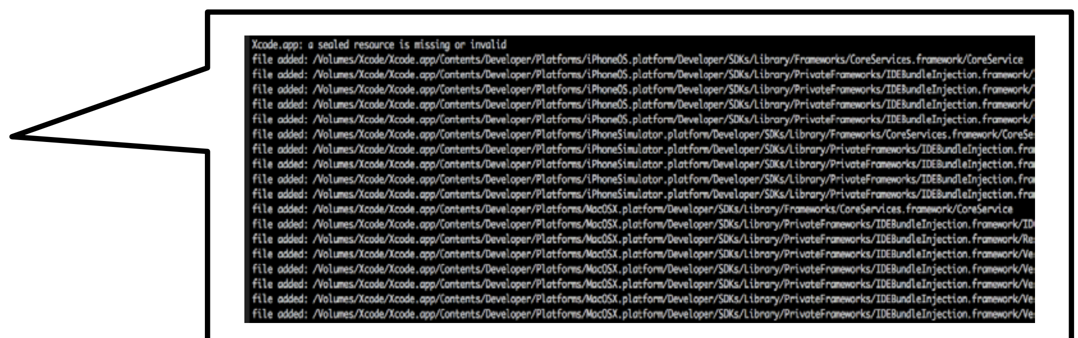


Library files: now contain malicious code

Which parts of the C.I.A. Triangle are violated by XcodeGhost?

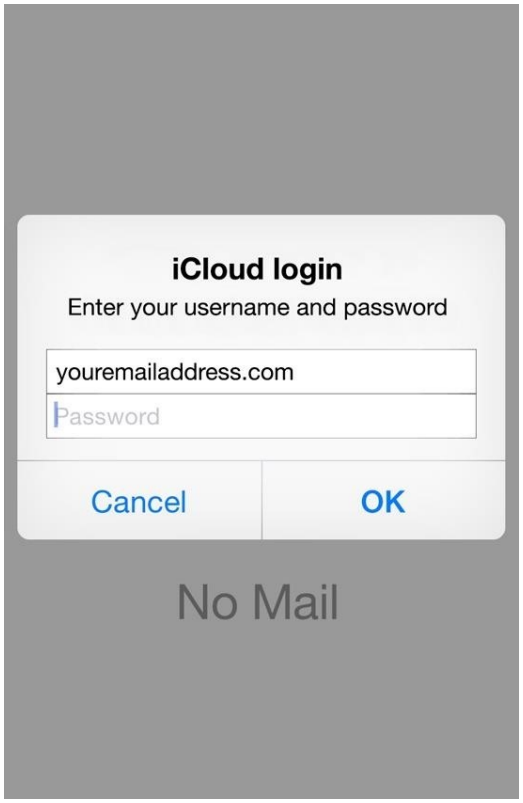
- Violation of software integrity

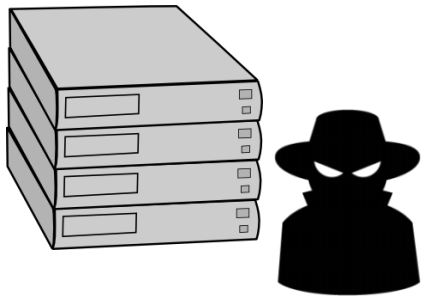




Which parts of the C.I.A. Triangle are violated by XcodeGhost?

- Violation of users' confidentiality
- Prompt a fake alert dialog to phish user credentials

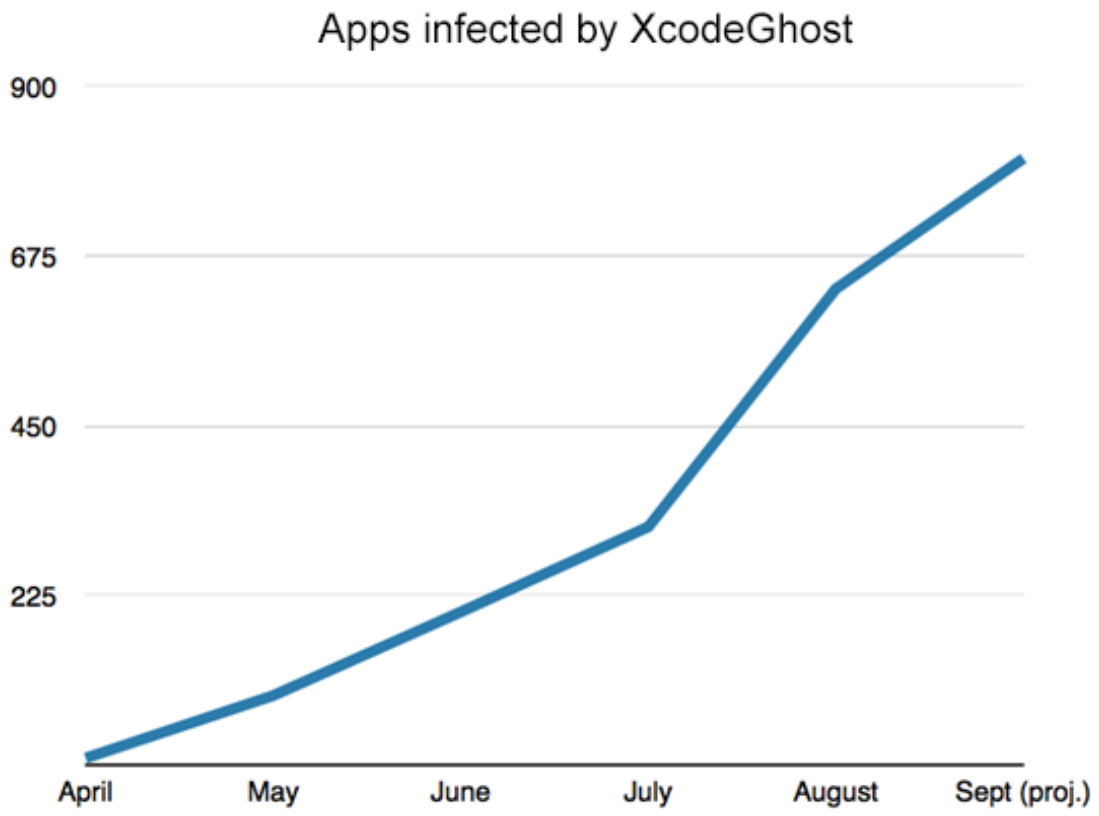




Hacker's server

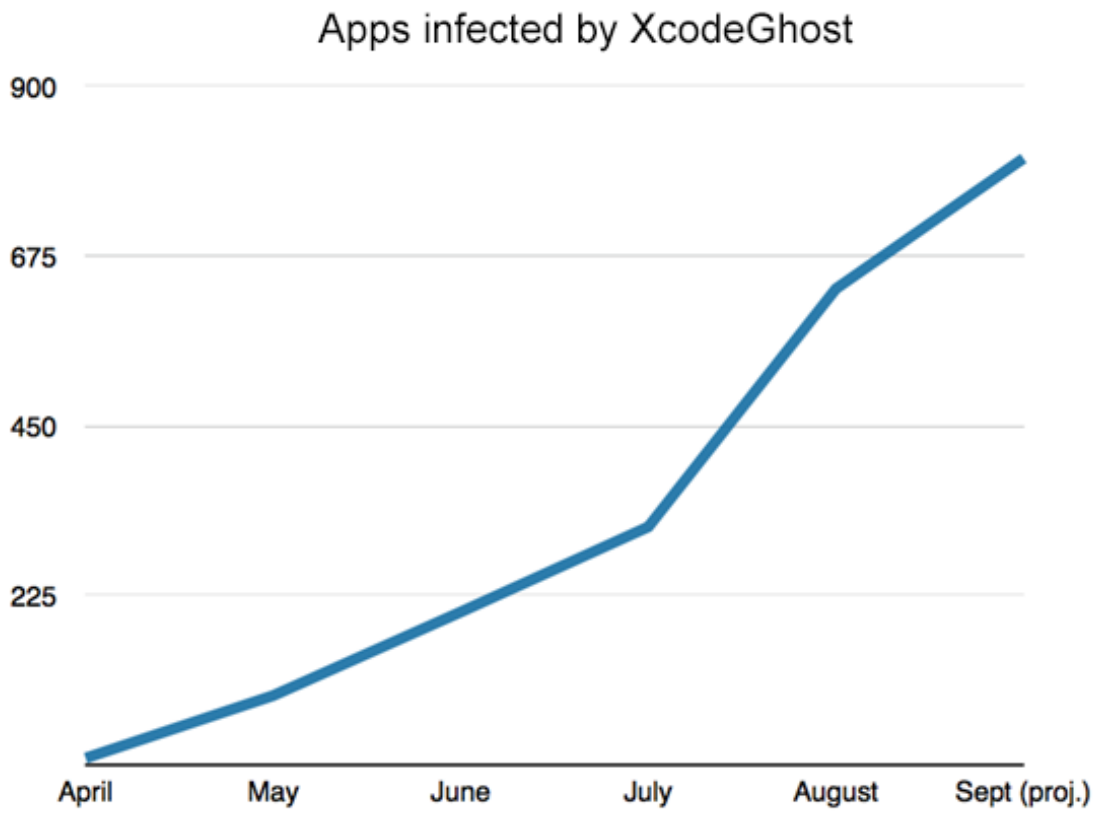
Apps infected by XcodeGhost

- XcodeGhost infected apps passed App Store review and were downloaded by millions of users.

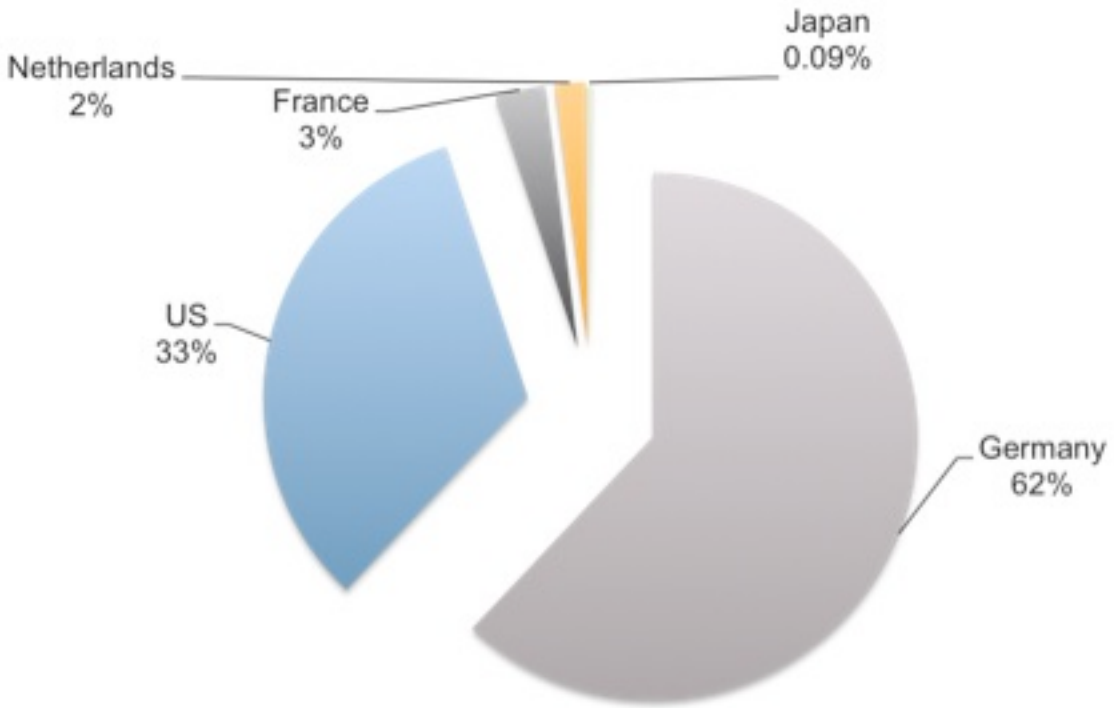


Apps infected by XcodeGhost

- XcodeGhost infected apps passed App Store review and were downloaded by millions of users.



Users outside China are also affected by XcodeGhost



Top five countries where XcodeGhost infected apps attempted to connect to the hacker's servers

What did Apple do after the discovery of XcodeGhost?

- Removed infected apps from App Store
- Introduced new security features in iOS 9 to prevent communication between XcodeGhost infected apps and the hackers' servers.

What can we do to prevent ourselves from security problems caused by XcodeGhost?

- As developers
  - Always download development tools from legitimate sources
- As users
  - Keep our iOS systems and all apps up to date (Two months after the discovery of XcodeGhost, 70% of infected devices are still not upgraded to iOS 9)

Questions that may appear on the exam

- Why are apps infected by XcodeGhost?
  - Answer: App developers used Xcode that had been modified by hackers to develop apps.
- How is malicious code injected into apps by XcodeGhost?
  - Answer: By the compiler during compilation process.
- Which parts of the CIA are violated by XcodeGhost?
  - Answer: Software integrity, users' confidentiality

Thank you !