安全预警：借贷软件变脸绕过应用市场审核

第一章 发现“变脸”应用

一、 背景

近日，360 烽火实验室接到一例反馈：用户描述从某应用市场下载了一个记事本应用， 经过一段时间的使用后发现该应用内容变成与贷款相关。

图 1-1 初次使用时的软件内容

图 1-2 经过一段时间之后的软件内容

随即我们根据用户反馈的内容进行快速跟进，发现该应用具有随机变换界面的功能，且变换后的应用功能已与原应用无关，因此将此应用称为“变脸”应用。

二、 应用分类及上架平台

截止到 2019 年 6 月，360 烽火实验室共发现“变脸”应用 5400+余款，其中约 10%的应用以工具类软件当“外衣”，“变脸”后变成投资理财或贷款类应用；约 90%的应用为投资理财或贷款类应用，“变脸”只是更换一种理财或贷款产品，应用类型并没有改变。

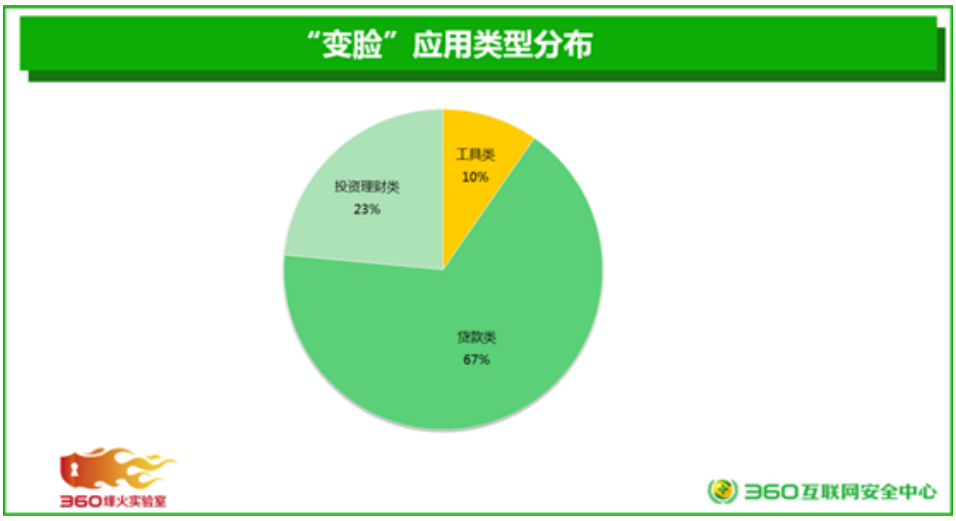

图 1-3 “变脸”应用类型分布情况

360 烽火实验室在跟踪“变脸”应用的过程中发现，“变脸”应用在多个国内主流移动应用市场均有上架且广受好评，部分应用好评率达到 95%，而且大部分应用的评论与应用功能介绍不符。

以一款名为“小猪白卡（手机）”的应用为例，该应用的介绍称其“为用户提供一键检测、智能估价、快速放款、安全可靠的专业回收服务。”在该应用的评论区可以看到近乎满分的打分和 97%的好评率。而且评论内容中随处可见“贷款”、“借钱”的字样，评论内容和软件自身介绍的手机回收服务没有任何关系。这款软件实际运行后可发现内容充斥着大量网络借贷软件的推广。

图 1-4 软件介绍与实际运行内容不符

第二章 解析“变脸”过程

一、 “变脸”行为流程概述

二、 软件行为分析

“变脸”应用首先会进行网络判断，在有网络连接的情况下访问服务器以获取“脸谱”指令，根据具体指令进行“脸谱”展示。

```
if(!this.isNetworkAvailable(((Activity)this))) {
    this.mNoInternetLayout.setVisibility(0);
}                                          判断网络连接
else if(!this.proxy.isWifiProxy()) {
    this.getVersionNameFromServer();
    this.judgeBeforeAndAfter();            指令获取
}
```

图 2-2 判断网络连接

```
myXutils.get("http://123.57.228.16/Android/Status/My/BaiDu/DuGan.json",
ublic void onResponse(String arg7) {
  try {
    String v2 = new JSONObject(arg7).getString("status");   指令
```

图 2-3 访问服务器获取指令

“变脸”应用获取的指令格式为{"status":指令}，当指令为“before”时，对应的代码内容及页面展示为：

```
if("before".equals(v2)) {
    MainActivity.this.mLayoutBefore.setVisibility(0);
    MainActivity.this.mRabtnNews1.setText("首页");
    MainActivity.this.mRabtnNews3.setText("我的");
    MainActivity.this.mRabtnNews4.setText("添加");
    MainActivity.this.showAndHide(0x7F0800F7, DebitAndCreditFragmentNews.class);
}
```

图 2-4 指令为“before”时对应代码内容

图 2-5 指令为“before”时对应页面展示

当指令为“after”时，对应的代码内容及页面展示为：

```
if("after".equals(v2)) {
    MainActivity.this.mLayoutAfter.setVisibility(0);
    MainActivity.this.rabtn1.setText("推荐");
    MainActivity.this.rabtn2.setText("全部借款");
    MainActivity.this.rabtn3.setText("一定借到钱");
    MainActivity.this.rabtn4.setText("我的");
    MainActivity.this.showAndHide(0x7F0800F6, DebitAndCreditFragment.class);
}
```

图 2-6 指令为“after”时对应代码内容

图 2-7 指令为“after”时对应页面展示

当指令为“secondH5”时，应用访问服务器获取 HTML5 链接地址，利用 WebView 进行加载。

```
if(!"secondH5".equals(v2)) {
    return;
}

MainActivity.this.mH5Layout.setVisibility(0);
MainActivity.this.mLayoutBefore.setVisibility(8);
MainActivity.this.mLayoutAfter.setVisibility(8);
MainActivity.this.myDialog = new MyDialog(MainActivity.this);
MainActivity.this.myDialog.showDialog();
MainActivity.this.getH5UrlPath();
```

图 2-8 指令为“secondH5”对应代码内容

```
x.http().get(new RequestParams("http://123.57.228.16/Android/Status/H5/BaiDu/DuGan.json"),
    public void onCancelled(CancelledException arg1) {
    }

    public void onError(Throwable arg3, boolean arg4) {
        Log.i("fajfkaljf", arg3.getMessage().toString());
    }

    public void onFinished() {
    }

    public void onSuccess(Object arg1) {
        this.onSuccess(((String)arg1));
    }

    public void onSuccess(String arg9) {
        try {
            JSONObject v5 = new JSONObject(arg9);
            MainActivity.this.geth5Path = v5.getString("h5Path");
            JSONArray v2 = v5.getJSONArray("hostArr");
            int v3;
            for(v3 = 0; v3 < v2.length(); ++v3) {
                MainActivity.this.hostList.add(v2.getJSONObject(v3).getString("host"));
            }

            MainActivity.this.setmWebView(MainActivity.this.geth5Path);
        }
```

HTML5地址

利用web View加载

图 2-9 访问服务器获取 HTML5 地址并加载

图 2-10 指令为“secondH5”时对应页面展示

“变脸”应用如果接收到的指令为“secondH5”，展示的内容则是 HTML5 页面。HTML5 地址在访问服务器后返回的数据中，该数据由服务器使用者控制，具有不确定性。在分析“变脸”应用的过程中，我们实现将服务器返回的 HTML5 地址进行修改，替换成如下图所示内容。因“变脸”应用可能加载任意 HTML5 页面，用户使用过程中的风险性也就增加。

图 2-11 HTML5 地址替换

第三章 剖析“脸谱”线索

根据合作厂商提供的资料，北京某科技发展有限公司曾申请上架“变脸”应用。利用该公司名称查询到官网地址等信息。

图 3-1 北京某科技发展有限公司信息

根据公司官网地址进行 whois 查询到联系邮箱等信息。

域名 [redacted].cn 的信息 以下信息更新时间：2019-06-14 15:57:54 立即更新

域名	[redacted].cn [whois 反查] 其他常用域名后缀查询： cn com cc net org
注册商	阿里云计算有限公司（万网）
联系人	北京[redacted]科技发展有限公司 [whois反查]
联系邮箱	haoxiangdai@foxmail.com [whois反查]
创建时间	2018年02月27日
过期时间	2020年02月27日
DNS	dns23.hichina.com dns24.hichina.com
状态	域名普通状态(ok)

图 3-2 whois 查询

通过联系人邮箱进行 whois 反查，关联到七个公司。

域名	注册者	电话	注册商
wc[redacted]ai.cn	北京[redacted]化传媒有限公司	...	阿里云计算有限公司（万网）
ch[redacted]me.cn	北京[redacted]科技发展有限公司	...	阿里云计算有限公司（万网）
ch[redacted]iqianbao.cn	北京[redacted]网络科技有限公司	...	阿里云计算有限公司（万网）
wr[redacted].cn	北京[redacted]文化传播有限责任	...	阿里云计算有限公司（万网）
wc[redacted]ayou.cn	北京[redacted]文化传播有限责任	...	阿里云计算有限公司（万网）
sy[redacted].cn	北京[redacted]技发展有限公司	...	阿里云计算有限公司（万网）
sy[redacted].cn	北京[redacted]技发展有限公司	...	阿里云计算有限公司（万网）
sy[redacted].cn	北京[redacted]技发展有限公司	...	阿里云计算有限公司（万网）
ba[redacted]huhua.cn	北京[redacted]文化传媒有限公司	...	阿里云计算有限公司（万网）
jie[redacted]daohang.cn	北京[redacted]文化传媒有限公司	...	阿里云计算有限公司（万网）
qi[redacted]ouhua.cn	北京[redacted]文化传媒有限公司	...	阿里云计算有限公司（万网）
jd[redacted].cn	北京[redacted]化传媒有限公司	...	阿里云计算有限公司（万网）

图 3-3 联系人邮箱 whois 反查

不难看出这些公司注册的域名与贷款和钱包有关系，同时我们也追踪到，上述七个公司上架国内移动应用市场的应用包含贷款类、投资理财类，并且是“变脸”应用。

与贷款类、投资理财类应用相比，工具类应用更容易上架移动应用市场，他们利用这点优势以工具类应用名称做伪装，以达到顺利上架移动应用市场的目的，经过“变脸”后，变成贷款类、投资理财类应用。

2019 年 1 月，360 烽火实验室发布了一篇《移动平台新型诈骗解析》的文章，简述了在传统恶意应用难以获利的环境下，利用赌博、伪贷、投资理财等手段的获利模式逐步显现。这些应用从实际功能看并无恶意行为，但是它们利用法律漏洞和用户需求，能在短期内获取高额利润。目前，新的检测手段还未成熟，需要消耗更高的人工成本，体现更多的是软件审核工作者和恶意应用开发者的较量。