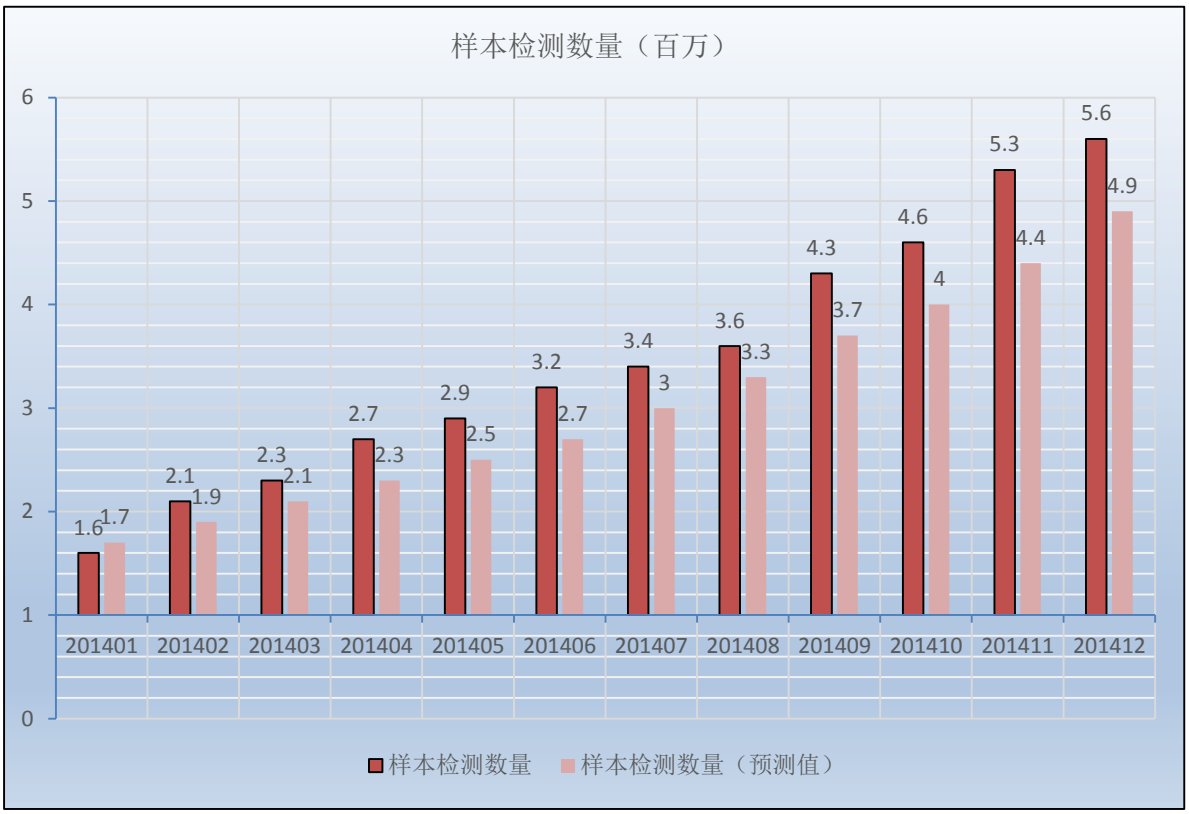
趋势科技移动客户端病毒报告

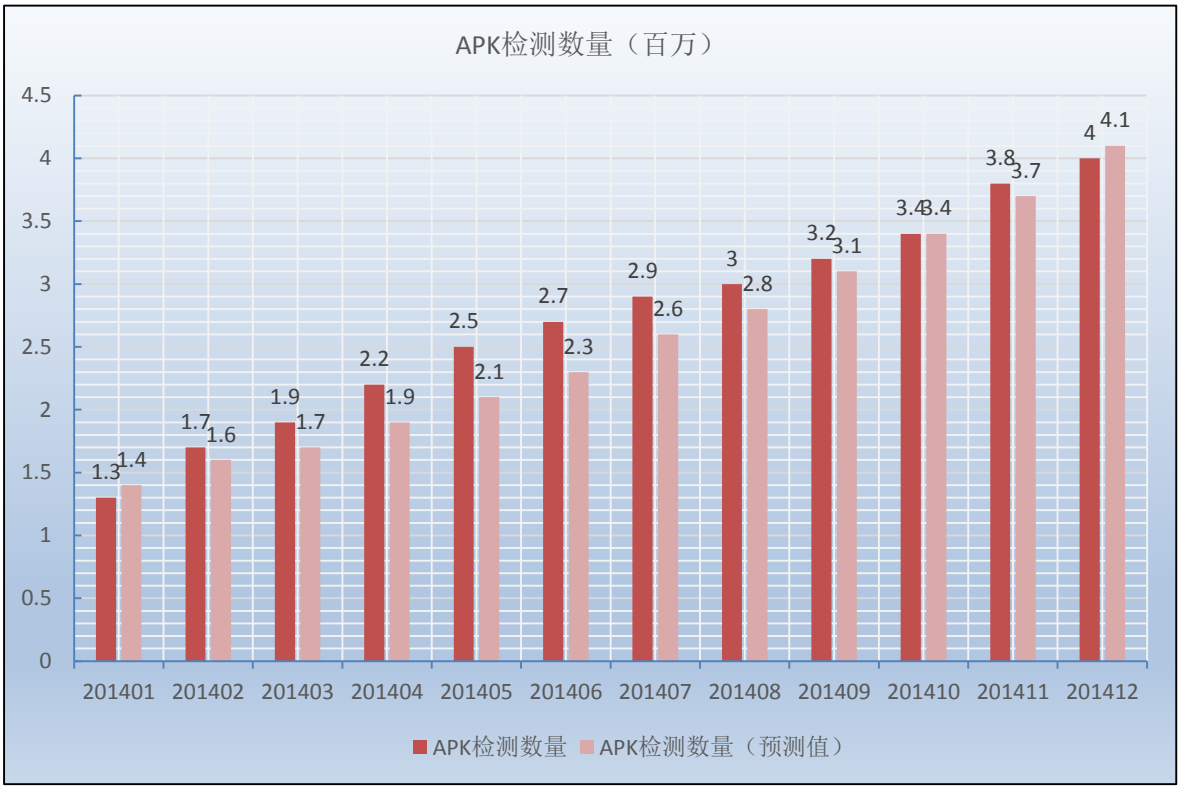
2014年12月移动客户端安全威胁概况

本月，截至 2014.12.31 日，发布中国区移动客户端病毒 1.805.00，大小 36,695,532 字节。

样本检测数量



APK检测数量


APK检测数量（百万）
4.5
4
3.5
3
2.5
2
1.5
1
0.5
0
1.3
1.4
1.7
1.6
1.9
1.7
2.2
1.9
2.5
2.1
2.7
2.3
2.9
2.6
3
2.8
3.2
3.1
3.4
3.4
3.8
3.7
4
4.1
201401
201402
201403
201404
201405
201406
201407
201408
201409
201410
201411
201412
APK检测数量
APK检测数量（预测值）

警惕：HTML5 应用可以重新打包成 Android 恶意程序

随着 HTML5 标准的确定，HTML5 Web 应用的数量将会迅速增加。由于 Web 应用的平台独立性，预计 HTML5 将促进 Web 应用重打包为手机恶意程序的这一趋势。

HTML5 Android 程序

根据我们的监测，2014 年，将 HTML5 程序重新打包为 Android 程序的数量比 2013 年增加了 200%。比 2012 的数量激增了 600%。

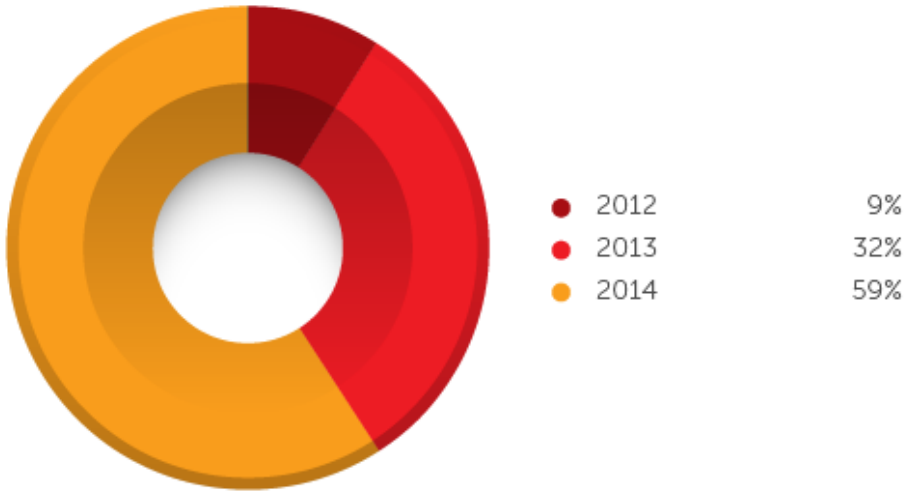


图 1. 2012 年至 2014 年 HTML5-packaged 程序在 Android 平台中所占比例

我们同时注意到，HTML5 打包的恶意软件或 PUAs（潜在威胁软件)的数量也在增长，其中 2014 年近 50%的 HTML5 恶意软件/PUAs 伪装为游戏应用。

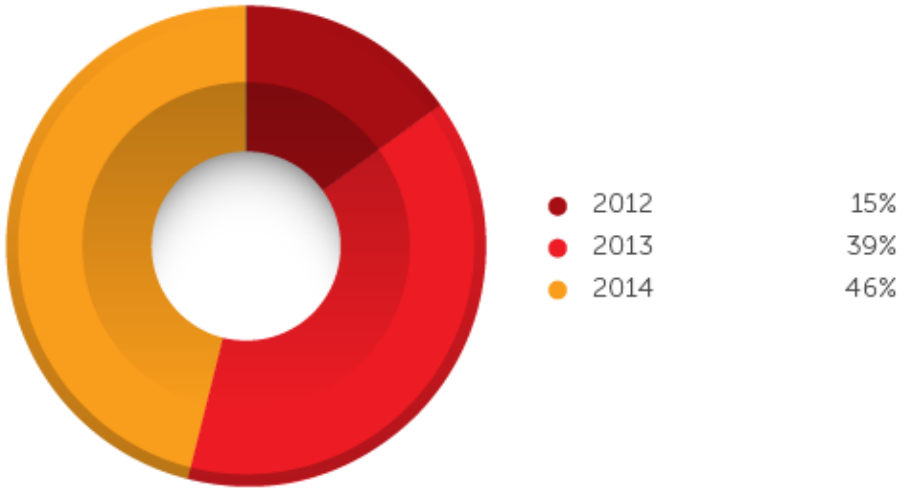


图 2.2012 年至 2014 年 HTML5-packaged Android 恶意软件比例

一个名为小步枪（Tiny Rifles）的 APP 就是款典型的需要 com.html5.game2 包的 HTML5 游戏。运行它以后，浏览器除了会加载 HTML5 游戏的 webview，还会通过代码注入恶意广告 SDK。该款恶意应用目前已经在 Google Play 中下架，我们将它检测为潜在威胁软件（PUA）。

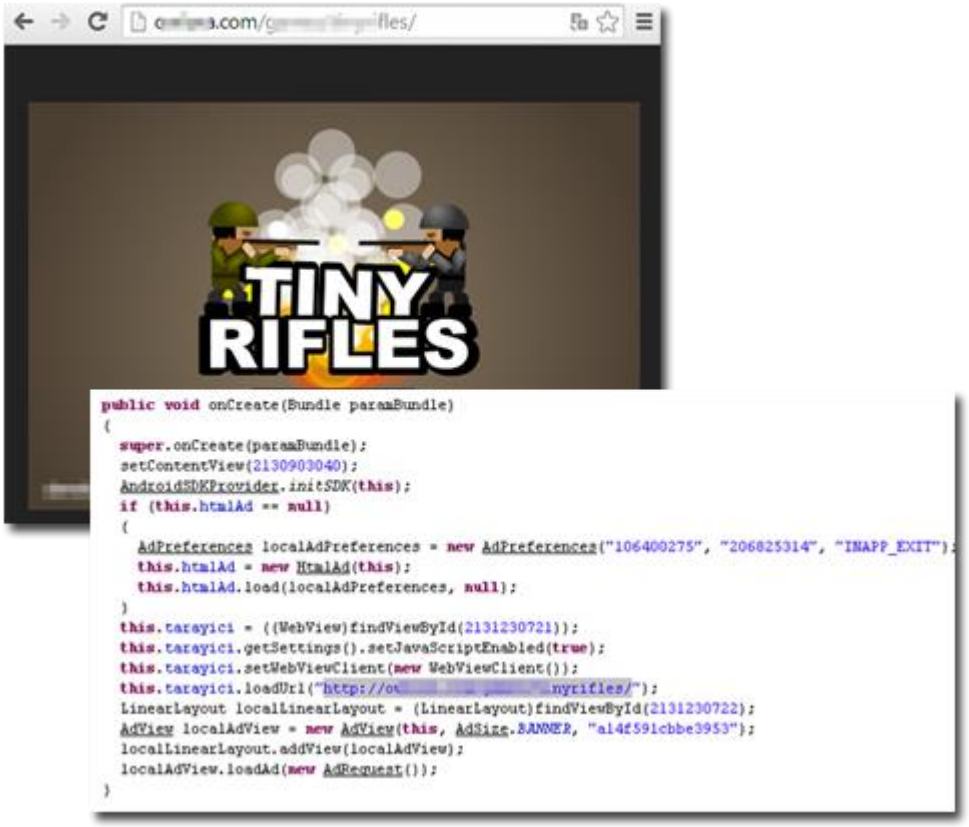


图 3. 假冒游戏 Tiny Rifles

HTML5 安卓恶意软件的两种攻击方式

根据我们的分析，HTML5 打包的恶意软件主要使用两种攻击方式：

方法一：初始化本地 webview

这是一种非常受黑客欢迎的攻击方式，使用它并不用改变 HTML5 应用的代码。黑客只需要初始化一个本地 webview，加载本地或远程的 HTML5/JavaScript/CSS 代码即可。这样主程序仍能运行，而产生的却是新的安卓应用。

然而，大多数黑客并不会在这里止步，因为只把 Web 应用转为安卓应用是完全没有意义的。黑客在大多数时候会在发布应用之前将恶意代码注入其中。

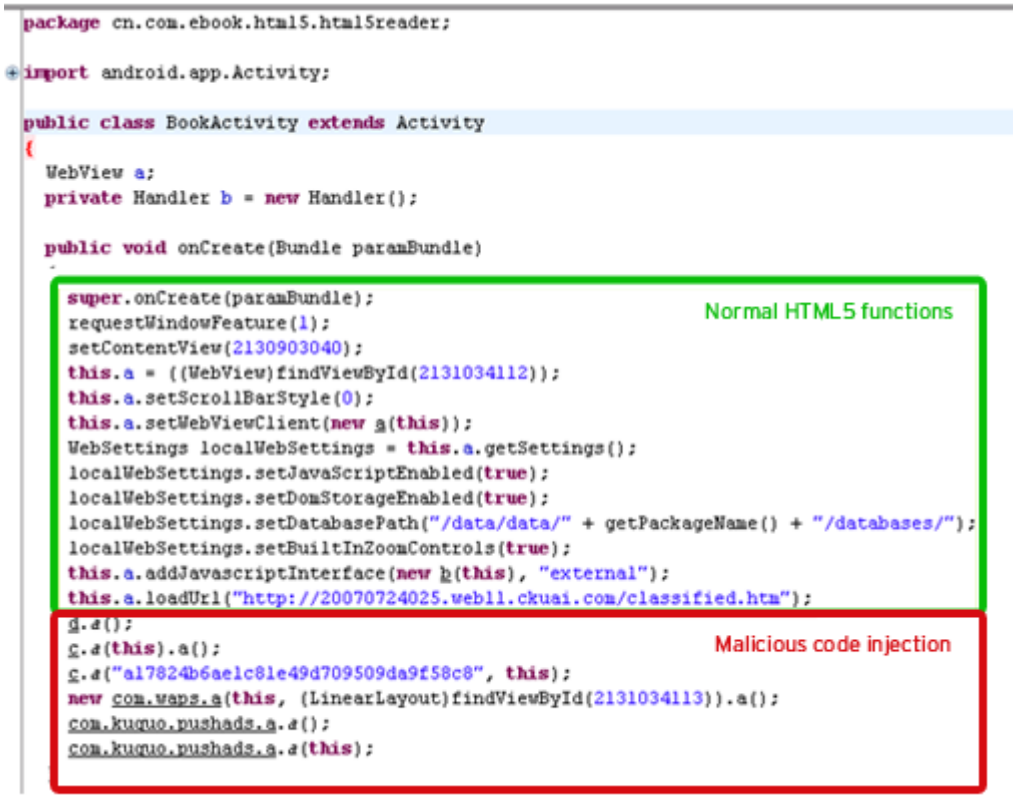


图4.被注入的 Java 恶意代码

这样打包应用的话，恶意代码和正常代码会在源代码里分离。黑客只需要关心注入的部分代码，而不用太在意 HTML5 的那部分，这样使得代码逻辑清晰简单。

方法二：把 HTML5 应用打包，通过中间件注入恶意 JS 代码

随着安卓越来越受大众的欢迎，许多中间件由此诞生，方便人们开发跨平台的应用。中间件是一种第三方软件/框架，在应用和操作系统之间作桥梁之用。

对于 HTML5 与相关 web 应用，现今有几种开源框架支持跨平台开发，比如：Phonegap，Apache Cordova， Crosswalk， Cocoonjs 等等，而且这些中间件通常都支持 HTML5，其中一个典型例子就是 Apache Cordova。

除了使用 webview 的 HTML5/JavaScript/CSS 代码外，适用于那些中间件的应用通常都基于那些框架核心库运行，就如那些定制的浏览器一样。由于那些中间件强大的 API 给开发者提供了许多便捷，他们只需要使用 JS 代码就能与安卓进行交互。换句话说，如果 HTML5 应用利用了中间件的特性，可以轻松进行恶意代码注入和执行。

index.html

```
<!DOCTYPE html>
<html>
    <head>
        <meta charset="utf-8" />
        <meta name="format-detection" content="telephone=no" />
        <!-- WARNING: for iOS 7, remove the width=device-width and height=device-height
        <meta name="viewport" content="user-scalable=no, initial-scale=1, maximum-scale
        <link rel="stylesheet" type="text/css" href="css/index.css" />
        <script type="text/javascript" src="config.js"></script>
        <title>Hello World</title>
    </head>
    <script type="text/javascript" charset="utf-8" src="cordova.js"></script>
    <script type="text/javascript">
        var PhoneGap = cordova;

        cordova.define("cordova/plugin/installation", function (require, exports, modul
            var exec = require("cordova/exec");
            module.exports = {
                install: function (success, fail, fileName) {
                    exec(success, fail, "InstallIntent", "install", [fileName]); //Inste
                }
            };
        });
        var installation = cordova.require("cordova/plugin/installation");

        var sms = {
            send: function( successCallback, failureCallback,phone, message, method) {
                cordova.exec(
                    successCallback,
                    failureCallback,
                    'Sms',
                    'send',
                    [phone, message, "NOINTENT", expiredTime, config.counts]
                );
            }
        }
```

图5.用 Cordova 发送短信的 JavaScript 恶意代码

结语

HTML5 使得开发更强大的 web 应用变得更加简单，因其开发的 web 应用的平台低依赖性，安卓平台因此有较大优势。对于开发者来说，跨平台开发的难度降低，可以说是一次开发多方通用（WORA，write once, run anywhere），并不会在跨平台上耗费精力。对于用户来说，他们可以在不同的移动平台分享喜爱的应用。这些意味着使用 HTML5 进行 web 应用开发，对于诸方都是有利的。

当然，跨平台也会带来隐患比如跨平台注入，JS 代码保护的机制太少，导致 web 应用可以被轻松复制和重新打包。理论上来讲，通过代码注入和重新打包，黑客可以剽窃任何他们想要的 HTML5 的跨平台 web 应用。

在未来，我们可以预见到这种由 HTML5 开发的恶意软件可以通杀不同的移动平台（比如 iOS，Android，WinPhone）。为了避免这种情况，开发者应多花点精力在代码混淆和使用其他编码技巧上，这样可以在一定程度上保护他们的应用程序。家庭用户需要使用新的应用程序时，最好去官方应用商店下载。

关于趋势科技（Trend Micro）

趋势科技是全球虚拟化及云计算安全的领导厂商 ,致力于保障企业及消费者交换数字信息环境的安全。趋势科技始终秉持技术革新的理念，基于业内领先的云计算安全技术(Smart Protection Network)核心技术架构，为全世界各地用户提供领先的整合式信息安全威胁管理技术能防御恶意软件、垃圾邮件、数据外泄以及最新的 Web 信息安全，保障信息与财产的安全。同时，遍布全球各地的 1,500 余名趋势科技安全专家可为各国家和地区的企业级个人用户提供 7×24 的全天候响应及技术支持服务。更多关于趋势科技公司及最新产品信息，请访问：www.trendmicro.com.cn。请访问 Trend Watch：www.trendmicro.com/go/trendwatch 查询最新的信息安全威胁的详细资讯。