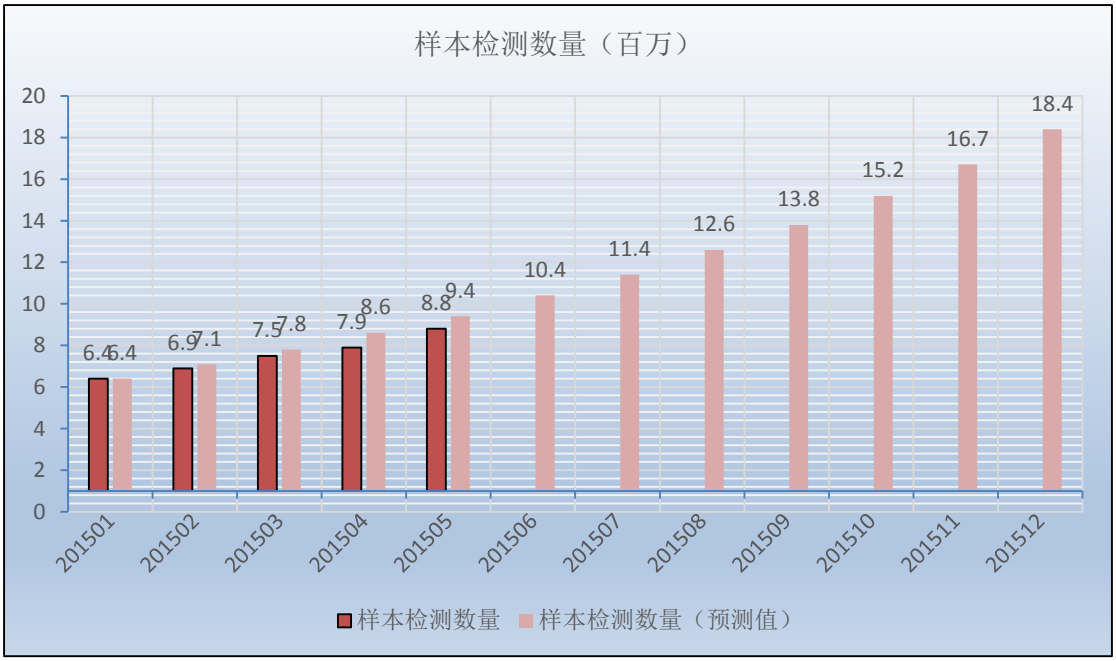
趋势科技移动客户端病毒报告

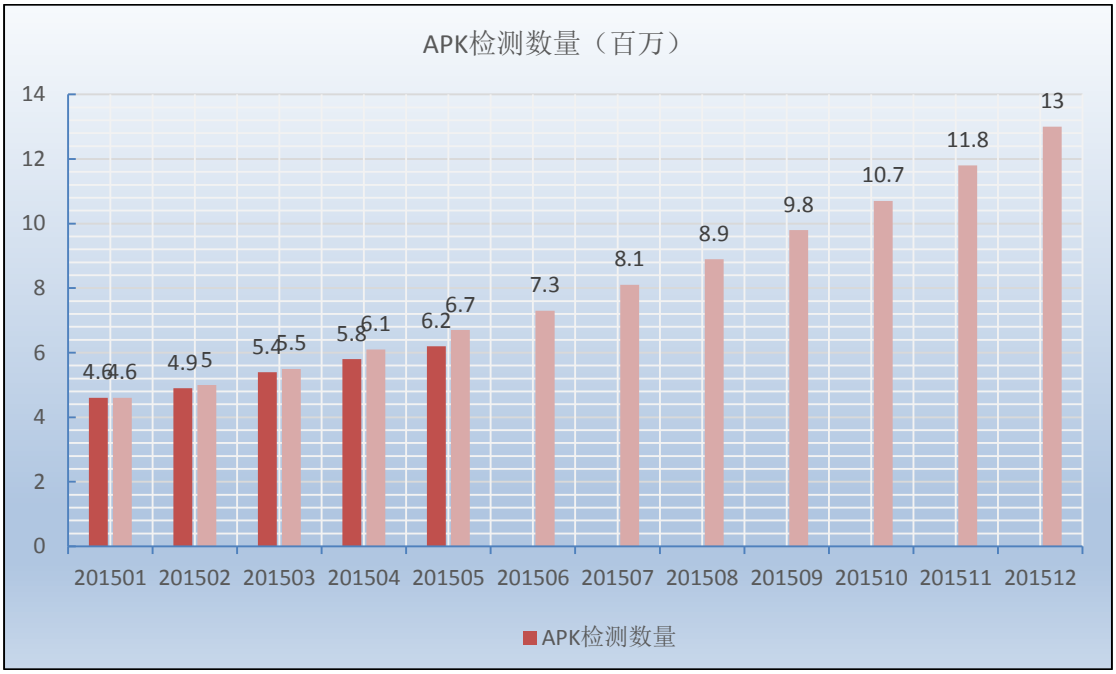
2015年5月移动客户端安全威胁概况

本月，截至 2015.5.31 日，发布中国区移动客户端病毒码 1.889.00，大小 4,194,621 字节。

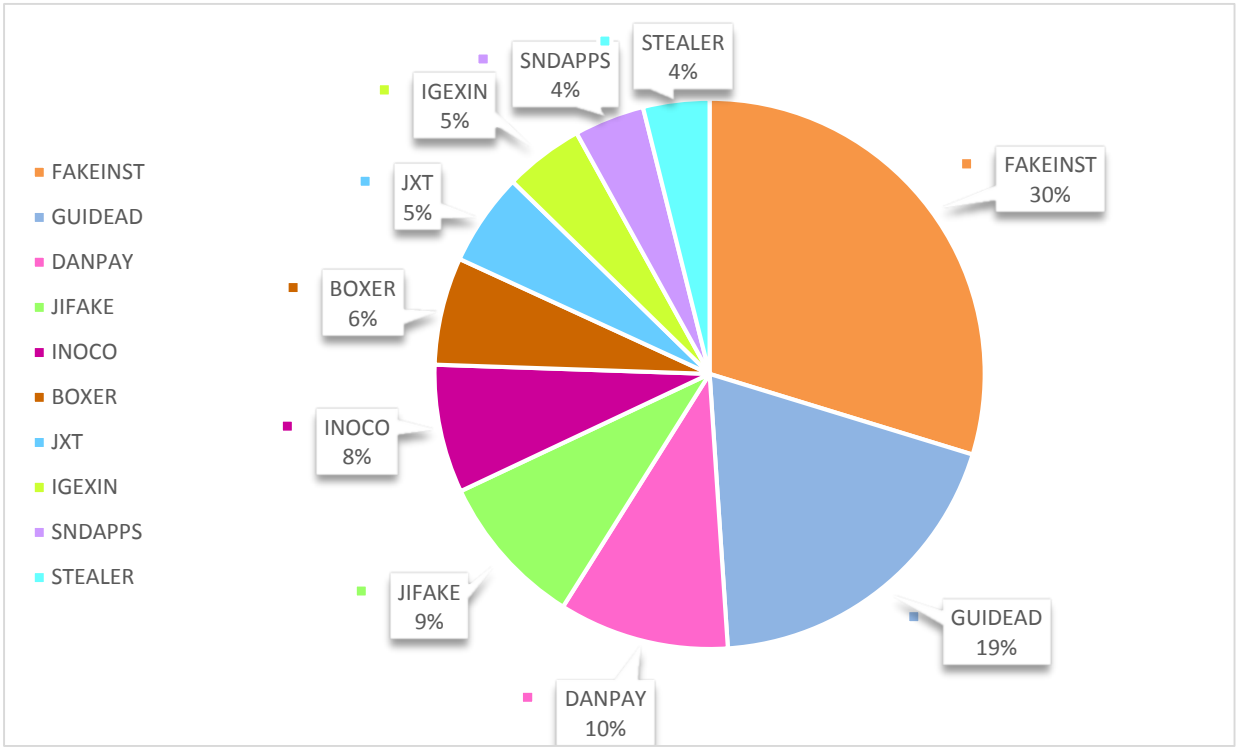
样本检测数量



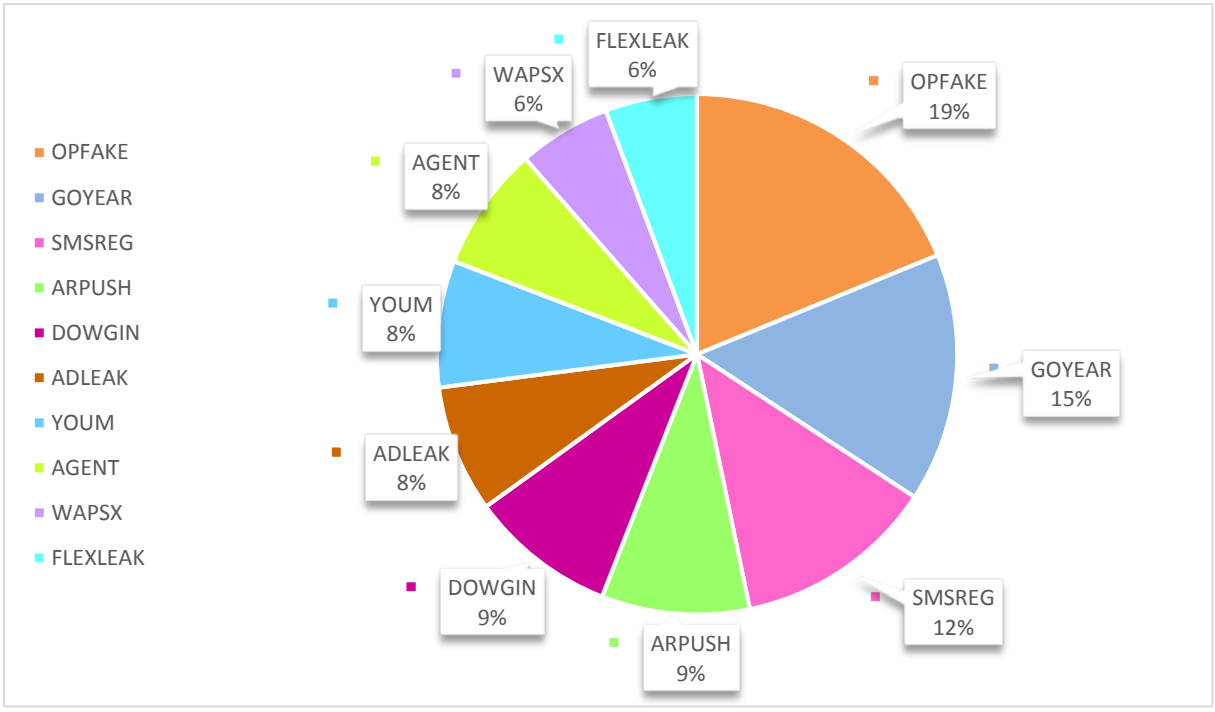
APK检测数量


APK检测数量（百万）
14
12
10
8
6
4
2
0
4.6
4.6
4.9
5
5.4
5.5
5.8
6.1
6.2
6.7
7.3
8.1
8.9
9.8
10.7
11.8
13
201501
201502
201503
201504
201505
201506
201507
201508
201509
201510
201511
201512
APK检测数量

十大恶意软件家族


FAKEINST
GUIDEAD
DANPAY
JIFAKE
INOCO
BOXER
JXT
IGEXIN
SNDAPPS
STEALER
FAKEINST 30%
GUIDEAD 19%
DANPAY 10%
JIFAKE 9%
INOCO 8%
BOXER 6%
JXT 5%
IGEXIN 5%
SNDAPPS 4%
STEALER 4%

十大广告软件家族


OPFAKE
GOYEAR
SMSREG
ARPUSH
DOWGIN
ADLEAK
YOUM
AGENT
WAPSX
FLEXLEAK
OPFAKE 19%
GOYEAR 15%
SMSREG 12%
ARPUSH 9%
DOWGIN 9%
ADLEAK 8%
YOUM 8%
AGENT 8%
WAPSX 6%
FLEXLEAK 6%

警惕：移动恶意软件已经开始使用隐写术

能够使用各种方法逃避检测的恶意软件，一直以来被认为是最危险的威胁。在当今最受关注的定向攻击和零日漏洞利用中都经常使用某些方法来逃避检测。能否成功保持隐藏有时候决定了攻击是否能成功，所以隐藏往往成为攻击者追求的首要目标。下面我们将介绍一种黑客常用的逃避检测和分析的手段。

Steganos 是希腊语，含义是“隐藏”。对于黑客来说，这个词简直太好了。本篇文章是介绍隐写术和恶意软件的系列文章的第一篇。我们将探讨什么是隐写术，以及该技术是如何应用于恶意软件的。

当然，你也可以在现实生活中应用隐写术。例如，将秘密的信息放在奇怪的位置（下图就是个例子），我们将着重探讨数据文件的隐藏以及这项技术是如何被黑客利用的。

To the Members of the California State Assembly:

I am returning Assembly Bill 1176 without my signature.

For some time now I have lamented the fact that major issues are overlooked while many unnecessary bills come to me for consideration. Water reform, prison reform, and health care are major issues my Administration has brought to the table, but the Legislature just kicks the can down the alley.

Yet another legislative year has come and gone without the major reforms Californians overwhelmingly deserve. In light of this, and after careful consideration, I believe it is unnecessary to sign this measure at this time.

Sincerely,

Arnold Schwarzenegger

图1.加州前州长阿诺德施瓦辛格回复某议员的一份电子邮件，该议员曾在讲话时污染了施瓦辛格州长。这封邮件每行的头一个字母组成了一句带侮辱性质的话。

下面我们讨论的方法并非全部都可以称为隐写术。然而，这些区别仅仅是语义上的。在我们的系列文章里，我们认为“隐写术”是黑客用来在隐秘通道内隐藏数据的一切可能方法。

ZeusVM:在 JPG 图片里隐藏恶意软件的配置文件

有一类 Zeus 病毒的变种用一种特殊的方法隐藏它的配置文件。对，就是利用图片。图片末尾包含了冗余的数据，当正确被解密后，会生成配置文件。无论从哪点来看，这就是一张正常的图片，所以安全网关等设备不会报警，而用户也只能看到图片本身。

图 2.ZeusVM 用来隐藏配置文件的图片

关于这个 Zeus 变种，我们曾在去年的博客中探讨过，请参考 *Sunsets and Cats Can Be Hazardous to Your Online Bank Account.*

VAWTRAK 用收藏夹图标来隐藏配置文件

我们最近发现这个阴险的网银木马用网站的图标文件隐藏自己的配置。favicon.ico 是浏览器中显示在 URL 左侧的图标。几乎所有的网站都有自己的 favicon.ico，所以安全软件几乎对这个文件不做检查。而且，Vawtrak 的服务器位于 TOR 网络中。这也为追踪该病毒增加了不少难度。

VAWTRAK 的图片隐藏采用了 LSB（least significant bits，最低位）方式。它将图片文件的像素颜色做了最轻微的改变。例如，一个像素颜色编码为 0,0,0。表明这是一个全黑的点。如果将其改变为 0,0,1，那么这个像素将携带信息，然而我们用肉眼是几乎不能观测出来的。

任何一个被修改的像素点都将携带信息，而任何一个知道这种编码方式的人都可以用逆运算求出编码之前的信息。其他不知情的人只看到一幅和原来几乎一模一样的图片。

关于这个 VAWTRAK 利用的技术您可以参考 *SecurityAffairs* 网站。我们的病毒百科中也有关于其的更为详尽的信息。

FakeReg 在程序图标中隐藏配置文件

网站图标并不是唯一的选择。我们发现不止一种 Android 病毒（ANDROIDOS_SMSREG.A）将配置文件隐藏在程序图标中。

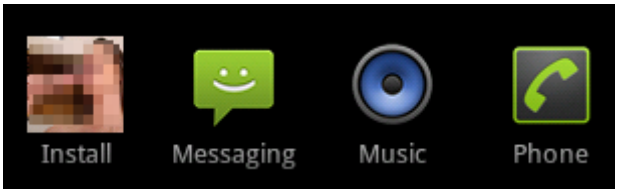


图3.携带病毒配置文件的安卓图标。由于图片包含色情内容，我们进行了模糊处理

关于这个病毒的详细信息，请您参考 *spreitzenbarch forensics blog*

VBKlip 在 HTTP 协议中隐藏数据

最后一个例子，我们不再围绕图片进行，而是网络协议。VBKlip 这个网银木马（在波兰非常流行）监控用户使用的网银账户。

一旦其发现可用的账户，它便将这个 26 位的账号的每位数字进行变换，生成新的账号，用来截获用户的支付。新的账号属于一个洗钱组织，这个账号由 C&C 服务器用一种非常规的方式下达。该病毒向 C&C 发起一个没有实际意义的 HTTP 连接，如下

```
GET g4x6a9k2u.txt HTTP/1.1
```

这是一个对文字信息的 GET 请求，几乎没人会注意到这种请求。然而 C&C 服务器返回的信息包含了重要内容（为了节省篇幅，我们仅截取了部分重要的 HTTP header）

```
HTTP/1.1 400 Site Not Installed
Server: .V06 Apache
Content-Type: text/html
MDEwMTAyMDIwMjAyMDMwMzAzMDMwMzAzMDM=
```

上面的 base64 编码的字符串，解码后是一个银行账号，例如 0101-02020202-03030303030303。受害者将会向这个账号付款，而不是真实账户。虽然这不是完全意义上的隐写术，但它符合我们之前提到的判定标准：它利用非常规的渠道隐藏重要数据，导致外人很难察觉。

以上我们简要介绍了隐写术，以及恶意软件是如何利用隐写术隐藏数据的。下一篇博客中我们将探讨恶意软件是如何隐藏可执行文件的。

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。