卡巴斯基实验室报告

2014 年金融网络威胁

ANTIY
安天实验室
技术公益翻译组
非官方中文译本

2015 年 2 月

KASPERSKY lab

2014 年金融网络威胁

非官方中文译文·安天技术公益翻译组 译注

文档信息			
原文名称	Financial Cyber Threats in 2014		
原文作者	卡巴斯基实验室	**原文发布日期**	2015 年 2 月 12 日
作者简介	卡巴斯基实验室是一家国际软件安全公司，在全球近 200 个国家和地区运营。该公司总部设在俄罗斯莫斯科，在英国注册了控股公司。卡巴斯基实验室目前拥有超过 2,850 名专家人才，在 30 个国家设立了 31 个有代表办事处，其产品和技术向全球 3 亿用户和超过 25 万个企业客户提供服务。 http://en.wikipedia.org/wiki/Kaspersky_Lab		
原文发布单位	卡巴斯基实验室		
原文出处	http://cdn.securelist.com/files/2015/02/KSN_Financial_Threats_Report_2014_eng.pdf		
译者	安天技术公益翻译组	**校对者**	安天技术公益翻译组
免责声明	本译文译者为安天实验室工程师，本文系出自个人兴趣在业余时间所译，本文原文来自互联网的公共方式，译者力图忠于所获得之电子版本进行翻译，但受翻译水平和技术水平所限，不能完全保证译文完全与原文含义一致，同时对所获得原文是否存在臆造、或者是否与其原始版本一致未进行可靠性验证和评价。 本译文对应原文所有观点亦不受本译文中任何打字、排版、印刷或翻译错误的影响。译者与安天实验室不对译文及原文中包含或引用的信息的真实性、准确性、可靠性、或完整性提供任何明示或暗示的保证。译者与安天实验室亦对原文和译文的任何内容不承担任何责任。翻译本文的行为不代表译者和安天实验室对原文立场持有任何立场和态度。 译者与安天实验室均与原作者与原始发布者没有联系，亦未获得相关的版权授权，鉴于译者及安天实验室出于学习参考之目的翻译本文，而无出版、发售译文等任何商业利益意图，因此亦不对任何可能因此导致的版权问题承担责任。 本文为安天内部参考文献，主要用于安天实验室内部进行外语和技术学习使用，亦向中国大陆境内的网络安全领域的研究人士进行有限分享。望尊		

	重译者的劳动和意愿，不得以任何方式修改本译文。译者和安天实验室并未授权任何人士和第三方二次分享本译文，因此第三方对本译文的全部或者部分所做的分享、传播、报道、张贴行为，及所带来的后果与译者和安天实验室无关。本译文亦不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天实验室一律不予承担。

目录

执行摘要和主要发现

2013 年，卡巴斯基实验室记录了针对用户的财务信息和资金的数量骤增的攻击。卡巴斯基实验室的《2013 年金融网络威胁》报告对 2013 年金融网络威胁全景的这一趋势及其它方面进行了详细讨论。

2014 年，情况发生了巨大改变：

金融钓鱼攻击：

- 针对银行、支付系统和网店的金融钓鱼攻击占所有钓鱼攻击总量的 28.73% （与 2013 年相比，减少了 2.72 个百分点）。
- 银行钓鱼攻击的数量占了所有攻击数的 16.27% （与 2013 年相比，减少了 5.93 个百分点）。
- 利用知名品牌支付系统的钓鱼攻击所占比例增加了 2.4 个百分点，从 2013 年的 2.74% 上升至 2014 年的 5.14%。
- 针对网店的钓鱼攻击的数量略有增加，从 2013 年的 6.51%上升至 2014 年的 7.32%，增加了 0.81 个百分点。

金融恶意软件攻击：

2014 年，卡巴斯基实验室产品检测到针对 2700 万用户的 2 亿 2900 万起利用金融恶意软件的攻击。这意味着，攻击次数与上年同比减少了 19.23%，目标用户数与上年同比减少了 29.77%。

- 在所有遭受任一类型恶意软件攻击的用户中，4.86%的用户遇到了包含某种金融威胁的攻击-比 2013 年降低了 1.34 个百分点。
- 虽然金融攻击的总量减少了，但是，把网上银行凭证作为目标的攻击比重上升了 8.89 个百分点，占了 2014 年中所有金融攻击总量的 75.63%。
- 比特币挖掘攻击达到 3 倍，从 2013 年的 360,065 起增加到 2014 年的 1,204,987 起。

Android 金融恶意软件攻击：

- 被卡巴斯基实验室产品阻断的针对 Android 设备用户的攻击的 48.15%利用针对金融数据的恶意软件。
- 与 2013 年相比，2014 年针对 Android 用户的金融攻击是之前的 3.25 倍（从 2013 年 711,993 起增加到 2014 年 2,317,194 起），且目标用户的数量增加到 3.64 倍（从

2013 年 212,890 位增加到 2014 年 775,887 位）。

攻击和受灾用户的总数减少了超过 20%，金融钓鱼攻击总数也是如此。这也许是由以下几点原因导致。首先，全球的执法机构积极控诉那些传播金融恶意软件和钓鱼攻击的网络罪犯。值得一提的是，美国和英国的执法机构在今年夏季制止了两项危险的恶意活动 -Gameover / Zeus 和 Shylock。

其次，可能是由于网络罪犯将攻击目标从之前的终端用户转向了与金融信息和支付工具打交道的组织。去年全年，经常有关于大型商店、连锁酒店和快餐店（这些受害场所每天都有上百万的客流量）被恶意攻击的报导。每一起案例中的欺诈者都使用了可以从受害组织所使用的 POS 机内存中直接盗取银行卡信息的恶意软件。银行也成为了网络罪犯的新目标，2014 年，卡巴斯基实验室调查的几起攻击，都将银行定位攻击目标而不是用户账户。 这些新型攻击中，没有一起引起了持续的新型反病毒检测。因为，与参与反病毒解决方案的私人用户相比，所牵扯的组织太少；因此，要对比攻击数很难。然而，鉴于受这类攻击的损失有上百万美元，所以，这些威胁不容小觑。

第三，根据卡巴斯基实验室的专家们在 2014 年的观察：网络攻击数目减少是其总趋势所致。根据专家的观点，网络罪犯对针对用户的大批量攻击的兴趣降低，他们开始偏爱少量的、目标更明确的攻击。这一点可以从钓鱼攻击目标等级的提高看出：欺诈者只对特定用户群（比如网上银行用户）进行攻击，而不是去批量发送包含恶意链接的钓鱼邮件。

通过这种策略（发送的恶意消息越少，其被安全研究员发现的机会就越少）网络罪犯妄想精挑细选的恶意邮件不被 IT 安全专家检测到，因此，恶意链接和恶意软件样本的寿命就会得以延长。这种伎俩不一定会成功，但使用它的后果之一即注册网络攻击的绝对数量的减少。

我们会在本报告的后续章节中讨论恶意攻击是如何随着时间发展，了解它们的地理分布及攻击目标。

金融钓鱼攻击

由卡巴斯基实验室的启发式反钓鱼攻击组件检测到的 2014 年包含针对银行、支付系统和网店在内的金融钓鱼攻击占所有钓鱼攻击数量的 28.73%。每次攻击都试图把钓鱼页面下载到用户的浏览器。邮件消息、来自即时通信服务或社交网络等的消息都可能是链接的携带源。

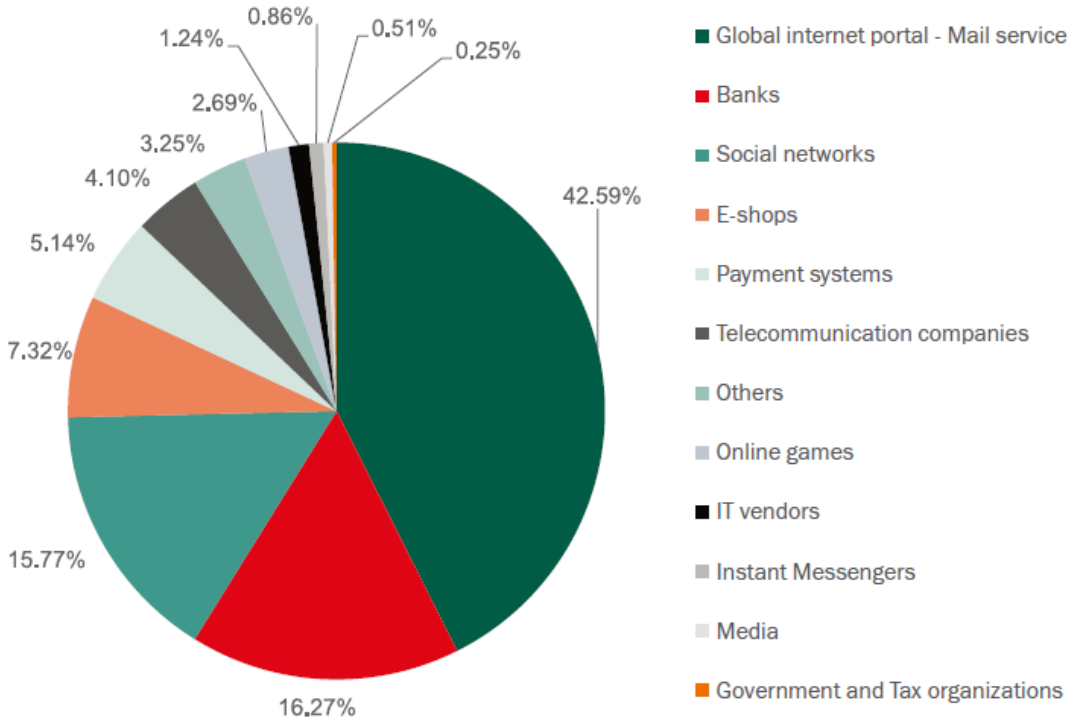

图 1：2014 年钓鱼攻击的分布

与 2013 年相比，金融钓鱼攻击所占比重减少了 2.72 个百分点。针对银行的钓鱼攻击减少了 5.93 个百分点（从 2013 年的 22.2%减少到 2014 年的 16.27%）。针对网店的钓鱼攻击数量略有增加，增加了 0.81 个百分点（从 2013 年的 6.51%增加到 2014 年 7.32%）；然而针对支付系统的钓鱼攻击增加了 2.4 个百分点（从 2013 年 2.74%增加到 2014 年 5.14%）。根据卡巴斯基实验室的专家，银行攻击数目的减少是因为之前曾受到重创的银行组织采取了应对措施。这些措施包括：对客户进行安全教育、执行反垃圾邮件和反诈骗解决方案使欺诈者难以成功实行钓鱼攻击。这些应对措施确实奏效，然而，这使得骗子开始更多关注其它目标了：支付系统和电子商务组织。

Type of phishing	Share in 2013	Share in 2014
Total share of financial phishing	31.45%	28.73%
Financial phishing/Banks	22.2%	16.27%
Financial phishing/E-commerce	6.51%	7.32%
Financial phishing/Payment systems	2.74%	5.14%

表 1：2013 年和 2014 年不同种类金融钓鱼攻击所占比重

金融钓鱼攻击细节

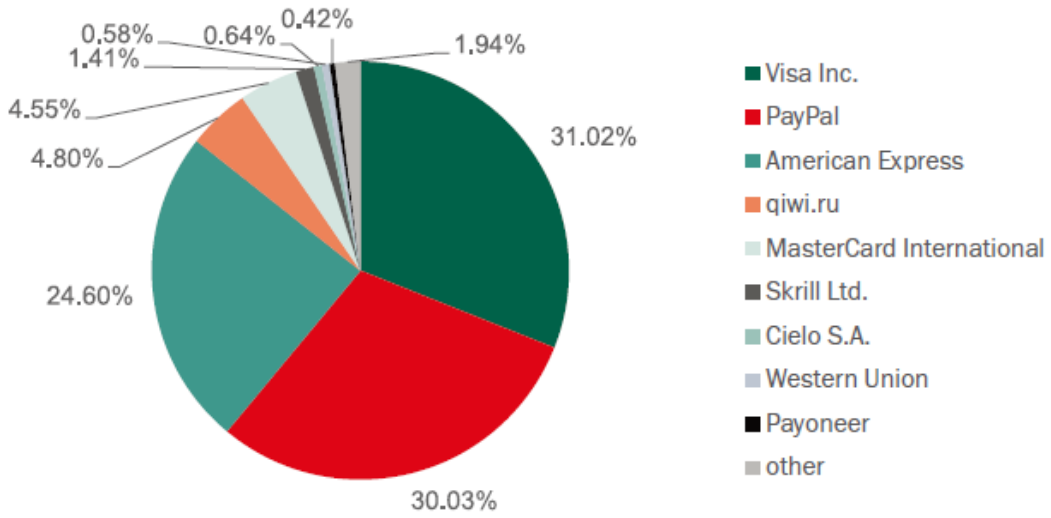

图 2：2014 年针对支付系统的钓鱼攻击的分布

针对 Visa 卡用户的钓鱼攻击从 2013 年的 6.36%飙升到 2014 年的 31.02%。这类攻击一直以来的首要目标-PayPal，以占所有被卡巴斯基实验室产品在 2014 年制止的对支付系统用户攻击比重的 30.33%退居第二。针对 PayPal 用户的攻击比从 2013 年的 44.12%下降到 2014 年 30.33%，减少了 14.09 个百分点。值得注意的是，Visa 名列榜首是因为针对 PayPal 用户的攻击量减少而得，事实上，针对 Visa 用户的攻击量与上一年相比相差无几。

根据 PayPal 和安全伙伴 Agari 向卡巴斯基实验室提供的信息，针对大名鼎鼎的支付系统 PayPal 用户的攻击急剧减少是因为 PayPal 和全球邮件供应商执行了 DMARC[1]策略。该策略允许阻止来自未授权域名的邮件，从而阻止了钓鱼邮件的传播。PayPal 和 Agari 估计，美国超过 85%、全球超过 65%的用户邮箱都受 DMARC 的保护。DMARC 的有效性从很大程度上取决于有多少个电子邮件供应商采取了该政策。去年，这类供应商的数量增加了也产生了相应的结果:攻击所占比重的减少。

[1] Domain-based Message Authentication, Reporting and Conformance or DMARC is a method of email authentication that is a way to mitigate email abuse. Source: http://en.wikipedia.org/wiki/DMARC.

总的来讲，2014 年最常受攻击的支付系统品牌与 2013 年的相差无几。MasterCard，Skrill，Cielo 和 Western Union 依然是易受攻击的品牌。PostFinance， WebMoney 和 Epoch 被攻击的数量减少，由 Qiwi 和 Payoneer systems 取而代之。

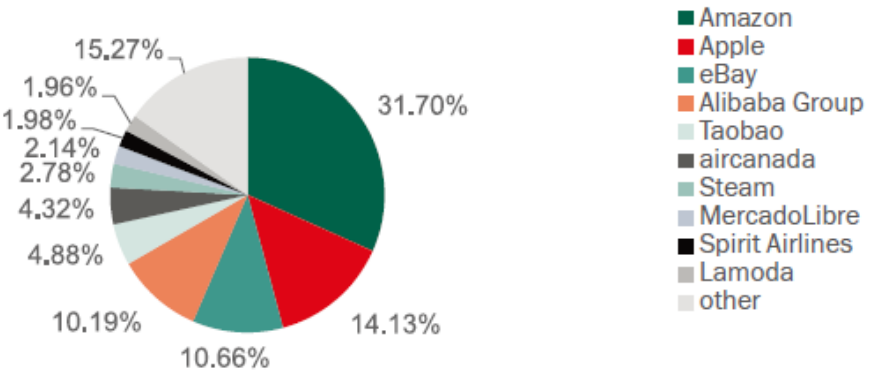

图 3：2014 年针对网店的钓鱼攻击的分布

Amazon 依然是最常被欺诈者利用的电子商务平台，31.7%的钓鱼攻击是针对使用该平台的网店。然而，这一比例大概是 2013 年的一半（下降了 29.41 个百分点），当时，所有对网店的攻击有 61.11%是针对 Amazon 用户的。

对 Apple （Store, iTunes 等）用户的攻击量所占比重增加了 1.24 个百分点，从 2013 年的 12.89%增加到了 2014 年的 14.13%。欺诈者仍将继续利用 Apple 产品的流行去行事。多数情况下，他们试图伪造 iTunes 的官方网页以此来盗取用户的凭证和信用卡号。

银行

2014 年，超过一半的恶意攻击时针对 13 家最有名的国际金融机构。其余 49.49%的恶意攻击则分布在一千多家不同的银行中。而在 2013 年，有近一半的恶意攻击是针对 25 家知名银行进行的。这一改变表明欺诈者有意减少大范围攻击，而是将攻击对象集中在几家知名银行以提高成功率。

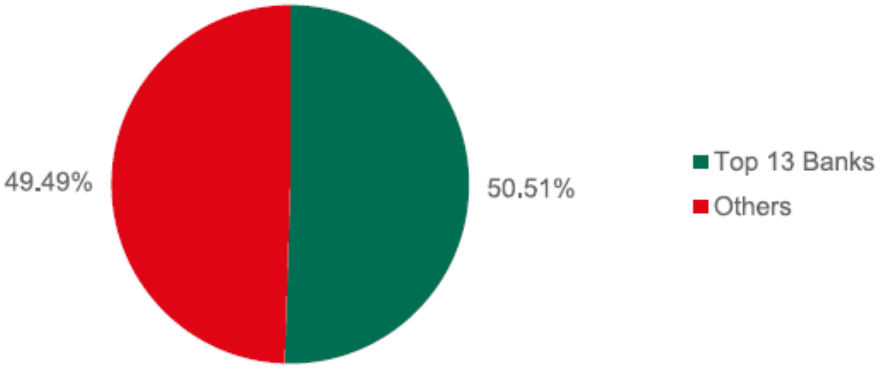

图 4：2014 年针对银行的钓鱼攻击分布

Mac OS X 金融钓鱼攻击

在完成报告期间，卡巴斯基实验室反钓鱼攻击检测中大约有 48.53%涉及 Apple 计算机的 “金融”钓鱼页面（银行+支付系统+网店）。该比例比 2013 年时多了 9.61 个百分点。

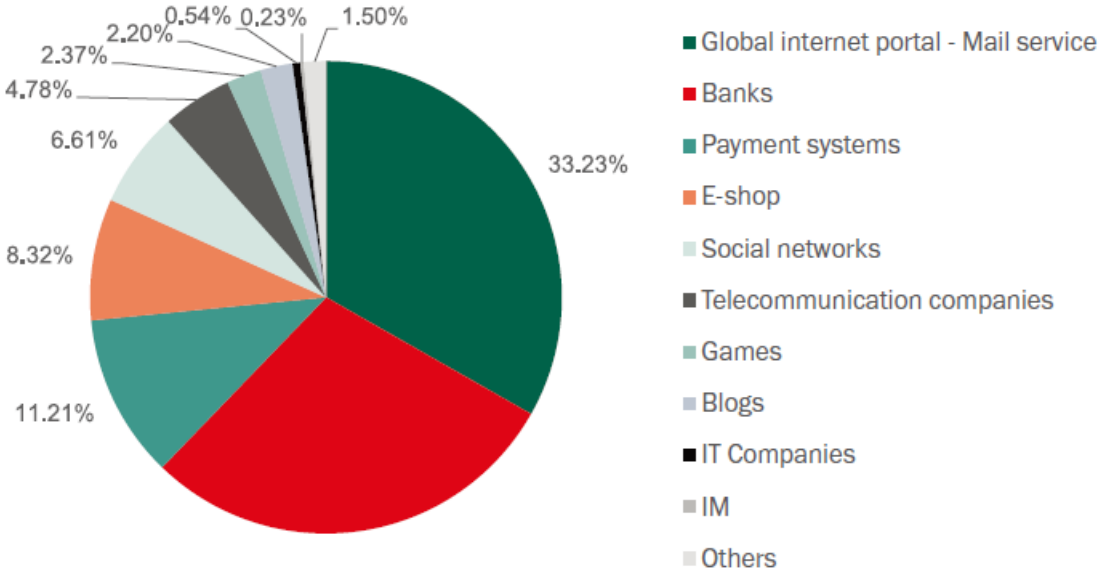

图 5：2014 年针对 Mac OS X 用户的钓鱼攻击分布

银行钓鱼攻击所占比减少了 0.86 个百分点，针对网店的攻为 8.23%（2013 年为 6.6%）。在 OS X 计算机内针对支付系统的受攻击次数比其它任何种类受攻击次数增加都多-从 2013 年的 2.46%增加到 2014 年 11.21%，增加了 8.75 个百分点。换句话说，卡巴斯基安全网络的数据表明，2014 年 Mac 用户所面临的钓鱼攻击的频率与 Windows 用户是相同的。

金融恶意软件

在所有遭受到任何形式的恶意攻击的用户中，4.86%的受害者曾受到某种金融威胁。该比例比 2013 年减少 1.34 个百分点，却比 2012 年（4.78%）略有增加。

2014 年，恶意攻击共达到 22,947,229 次。比 2013 年（28,411,384 次）同比下降 19.23%。被攻击的用户为 2,698,509 位，比 2013 年（3,842,246 位）下降 29.77%。

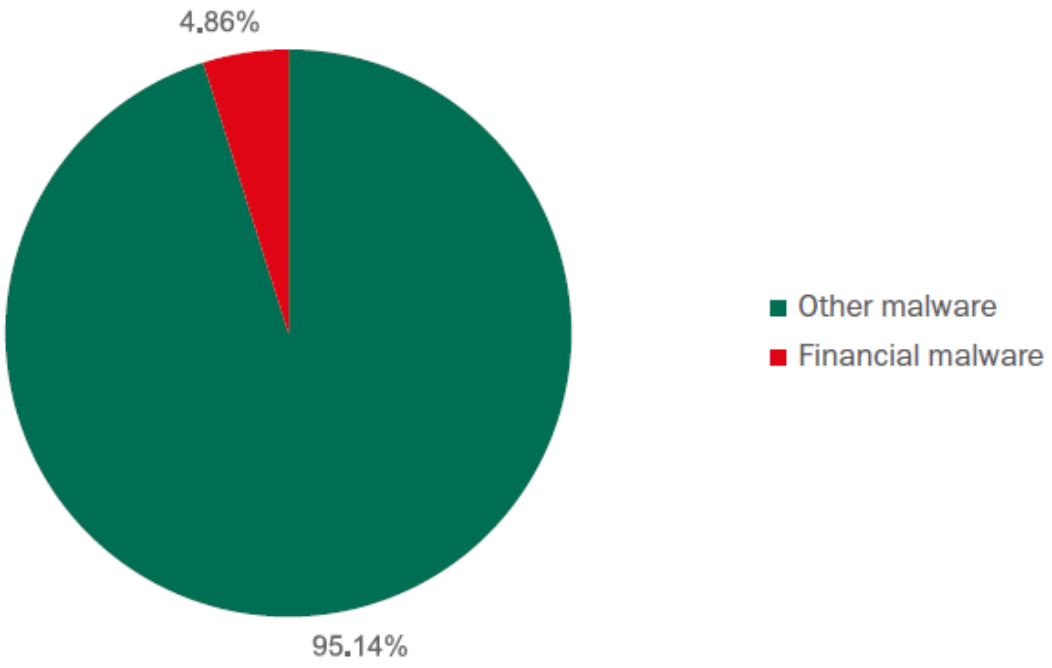

图 6：2014 年遭受金融恶意软件攻击的用户比例

根据卡巴斯基实验室研究人员在 2014 年的观察：该现象的原因是网络罪犯从海量攻击转为精确攻击。该策略的出发点很明了：恶意攻击活动范围越广，就可越早开启针对该活动的安全检测。该策略并不一定成功，但它影响了安全解决方案的检测次数。

然而，虽然攻击量和受攻击的用户数减少了，但是攻击的强度却增大了。2014 年，平均每个受到金融恶意软件攻击的用户都被攻击 8.5 次，而在 2013 年受害者是被攻击 7.2 次，2012 年为 6.9 次。

有趣的是，2014 年包括所有类型恶意软件在内的恶意攻击的平均强度从 2013 年每个用户 106 次攻击降低到每个用户 81.8 次。

金融恶意软件的种类

虽然，金融恶意软件攻击在 2014 年有所减少，但是银行恶意软件攻击在所有金融恶意软件攻击中所占比例上升了 8.89 个百分点，达到 75.63%。与此同时，其它类型金融恶意软件攻击所占比例有所下降。

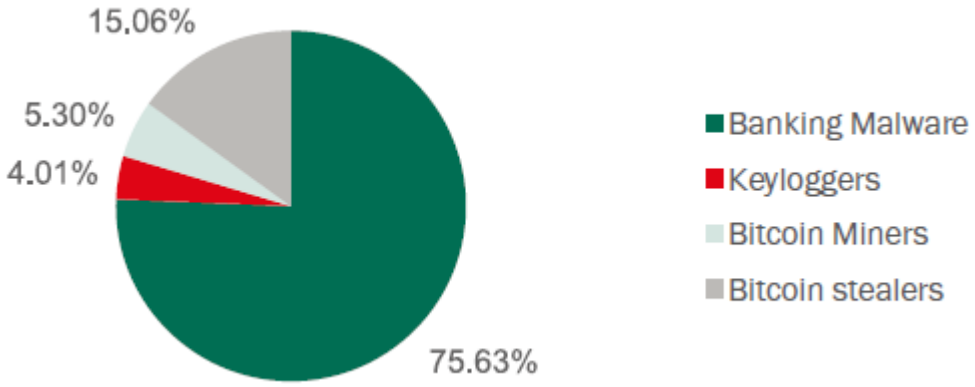

图 7：014 年不同类型金融恶意软件攻击分布

2013 年如图：

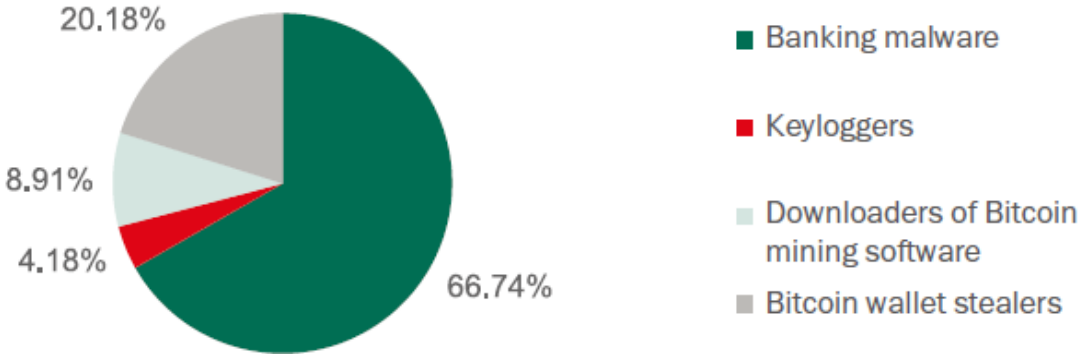

图 8：2013 年不同类型金融恶意软件攻击分布

攻击动态

如图所见，2013 年 7 月-12 月，攻击量明显增多。

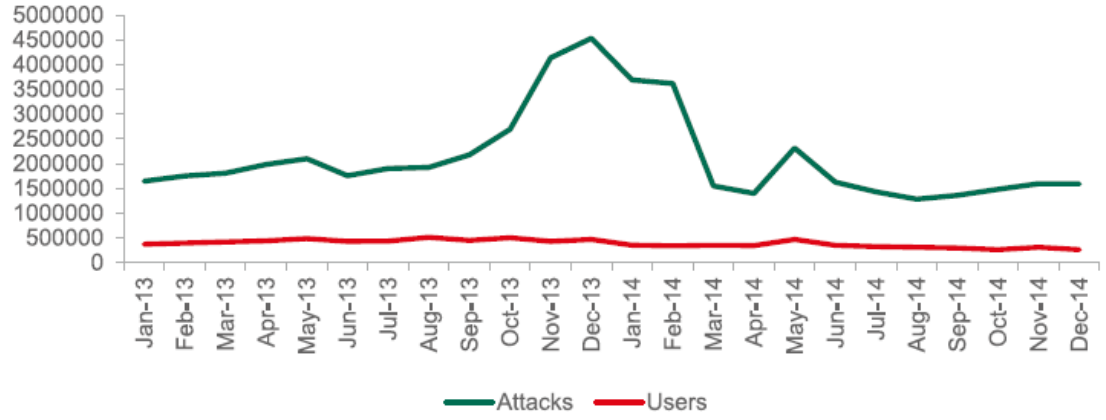

图 9：2013 年和 2014 年的金融恶意软件攻击

在《2013 年金融网络威胁》报告介绍了该攻击量增多的原因。其主要是由 Zbot, Carberp, Cridex 的幕后罪犯和其它旨在从网上银行和其他金融服务账户中盗取身份认证的恶意程序所致。

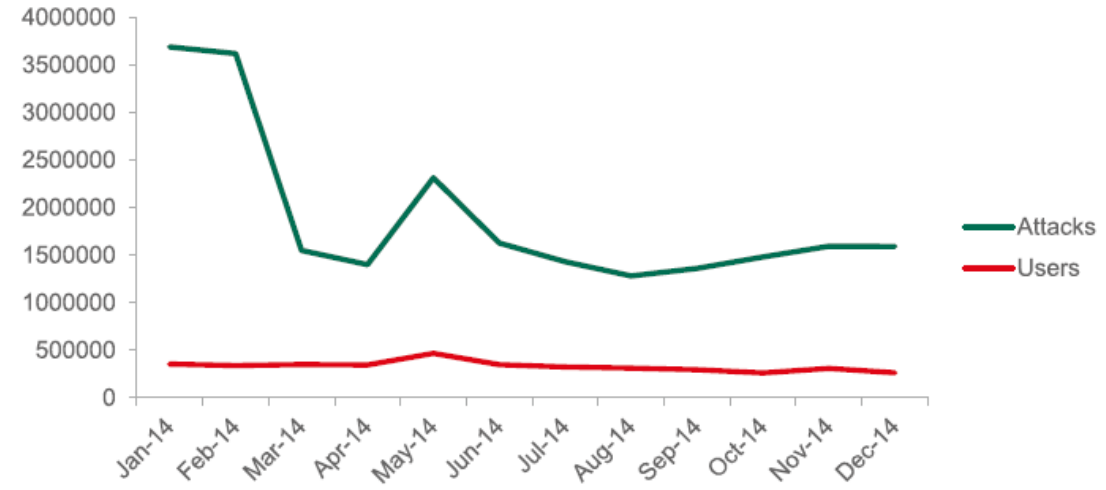

图 10：2014 年使用金融恶意软件的恶意攻击

有趣的是，2014 年检测到的攻击次数和被攻击用户数量的减少是由几乎同一恶意软件家族中的恶意软件的活动减少所致。

银行恶意软件

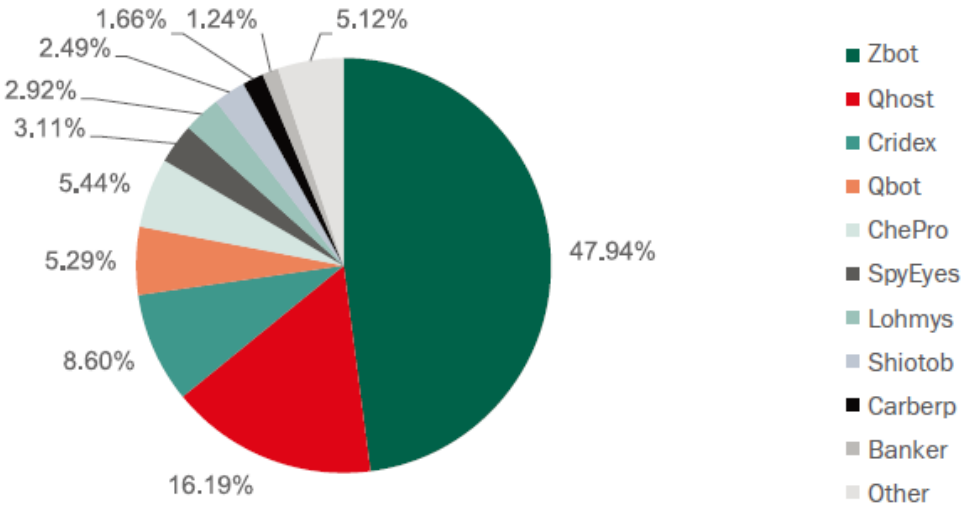

图 11：前 10 名最常被使用的银行恶意软件家族

如以上饼图所示， 10 个恶意软件家族导致了超过 94%以上的银行恶意软件攻击。这并不奇怪，榜首的位置再次由臭名昭著的 Zbot 占据- 最广泛和最危险的银行恶意软件家族之一。

Zbot 活动减少

但在这一年，我们也看到了在金融威胁环境的 Zbot 影响力下降的迹象。虽然这一年这个家族导致了 47.94%的银行恶意软件攻击，随着时间的过去，Zbot 的份额（以及其他几个“大型”威胁）显著下降：从 2014 年一月份的 34.86%下降至十二月的 26.02%。

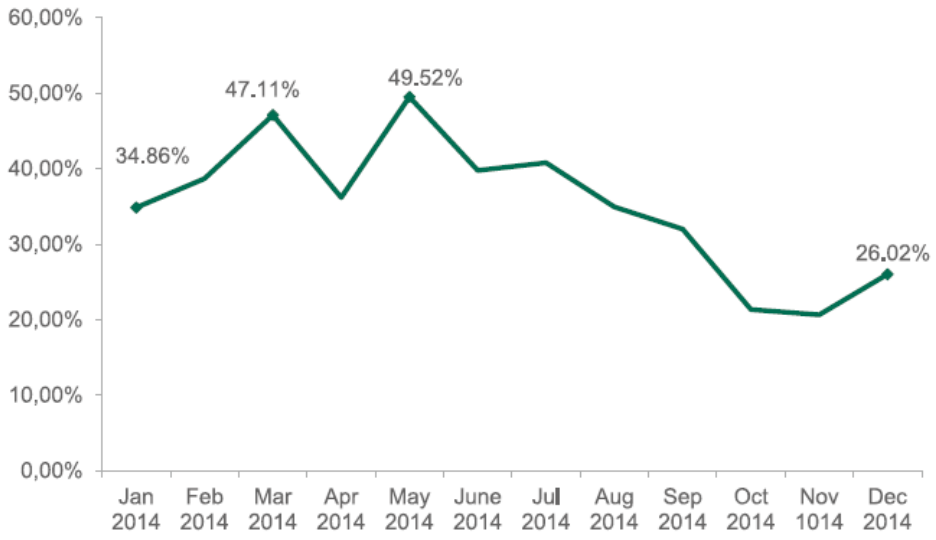

图 12：Zbot 全年攻击比例

用 Zbot 进行攻击的数量变化是这一过程的很好例证。

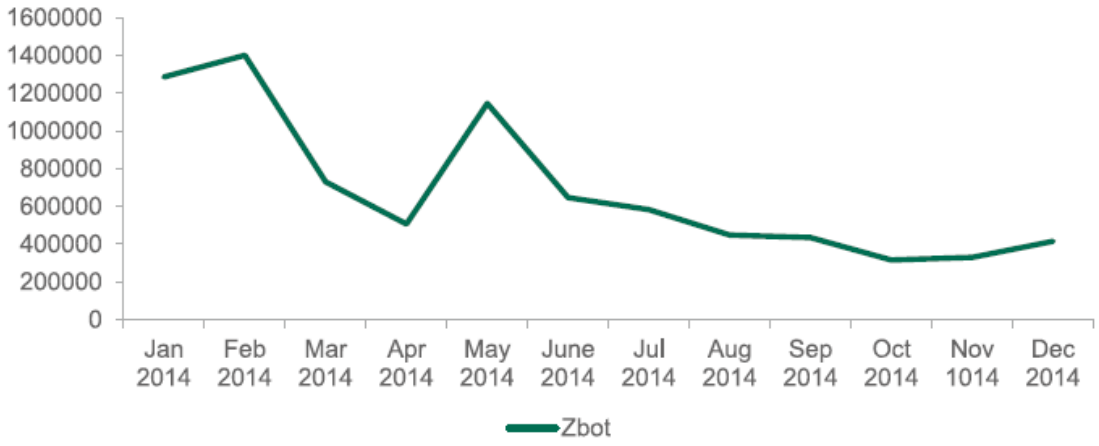

图 13：2014 年使用 Zbot 恶意软件家族的攻击

一次显著和持久的下降期始于 6 月。在该月初 ,联邦调查局和美国司法部宣布利用 ZeuS 恶意软件的最大的僵尸网络之一的 ZeuS \Gameover 僵尸网络的关闭。我们认为，正是由于该事件减少了攻击活动。

利用 Cridex 蠕虫，SpyEye 特洛伊木马，Carberp 和其他一些恶意家族而进行攻击的数量也有所减少，这对攻击总数和被攻击用户数的减少也产生了显着影响。

然而在 2014 年也看到了其它新型威胁的出现，这些新型威胁已变得颇为流行。

特别是 ChePro 和 Lohmys 特洛伊木马。

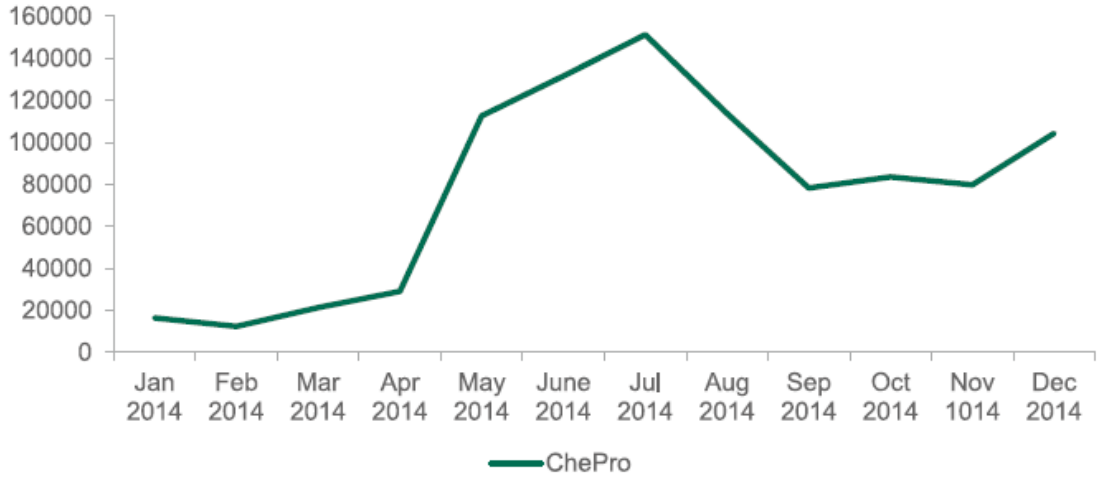

图 14：2014 年使用 ChePro 恶意软件家族的攻击

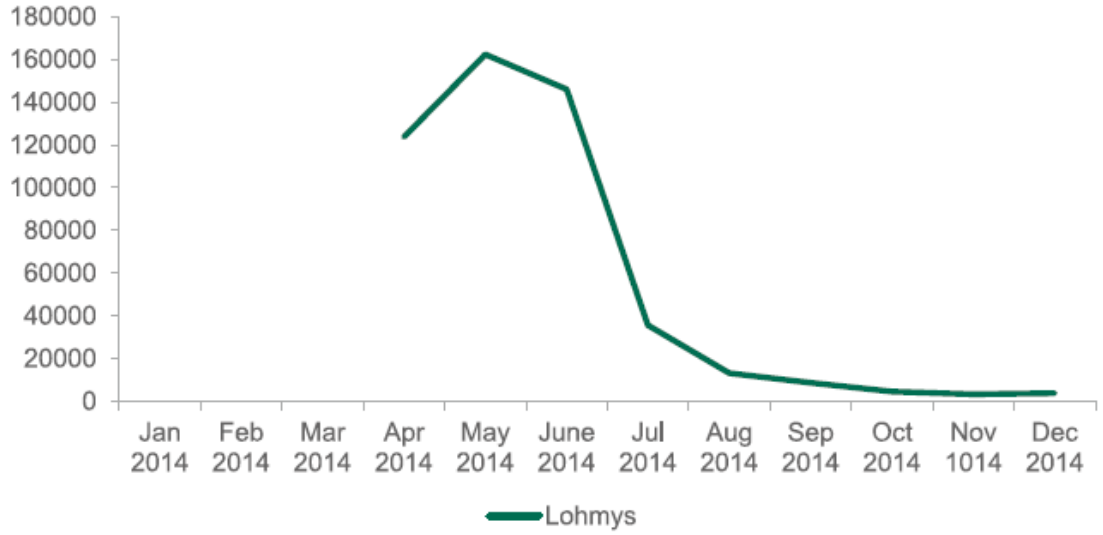

图 15：2014 年使用 Lohmys 恶意软件家族的攻击

有趣的是，尽管这两种木马程序产生的攻击足以名列全球前 10 名银行的恶意软件，但在其流行区域来看，它们几乎不具备 “全球性”。这两大家族主要针对巴西用户（更多内容见地理分布章节）。

其它金融威胁：键盘记录器和比特币恶意软件

键盘记录器攻击的时间表展示了与 2013 年相比该攻击的稳步减少。这反映了由于网络罪犯采取了更复杂的一体化恶意软件（如银行木马）而对单一键盘记录功能的需求下降，其中包括记录击键的能力。

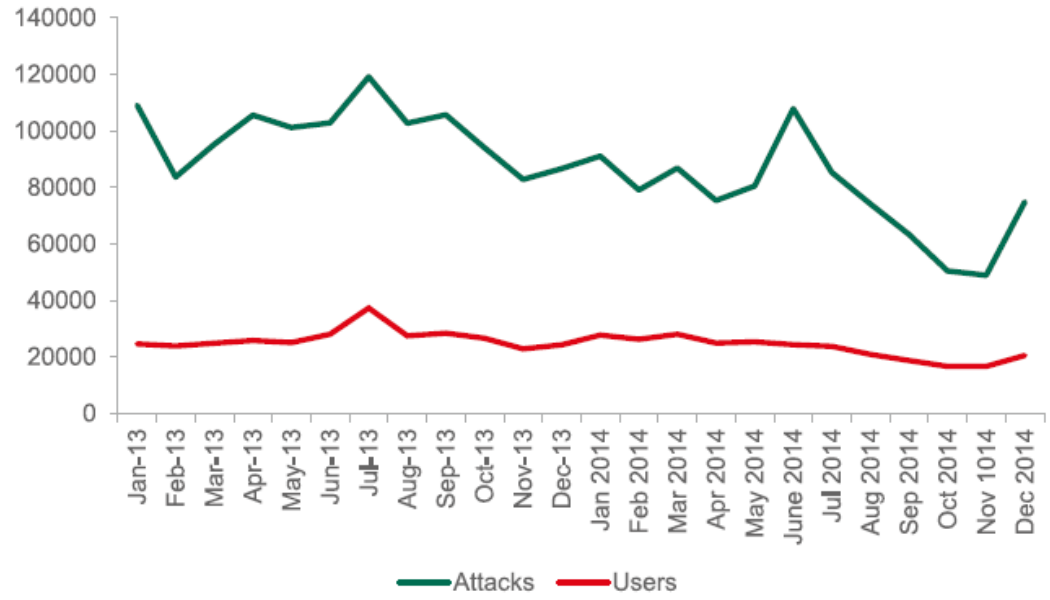

图 16：2013 年和 2014 年期间使用键盘记录器的攻击

谈到比特币恶意软件 其情况有所不同。2014 年 比特币汇率从显示 1 月 1 号的 7,725,301 美元将至 12 月 31 日 314,440 美元。

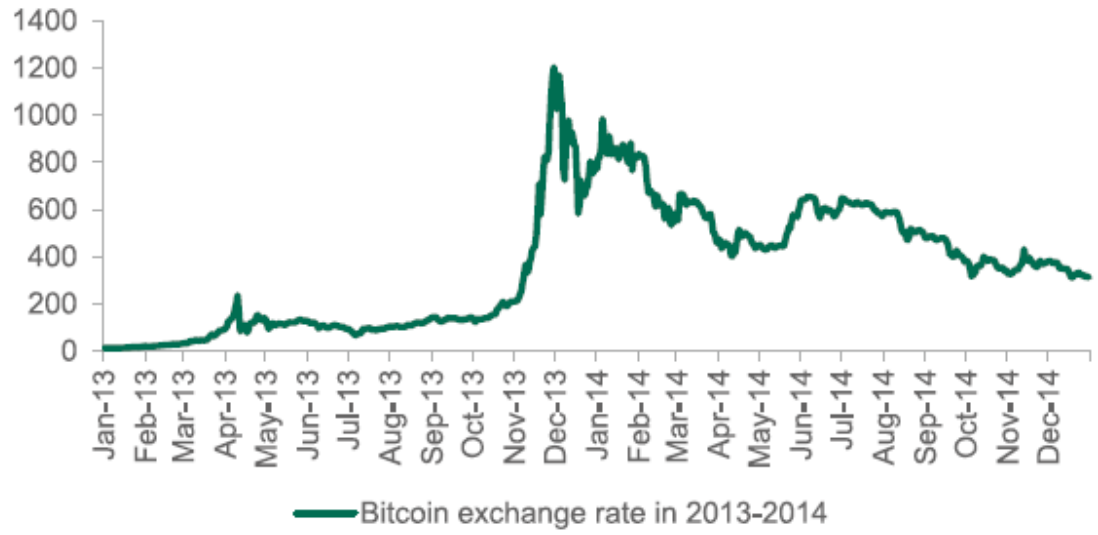

图 17：2013-2014 年比特币汇率

然而，这并没有降低犯罪分子对传播比特币为主题的恶意软件的热情。卡巴斯基实验室检测到两类这样的恶意程序。一种是能够安装比特币挖掘软件的恶意软件。

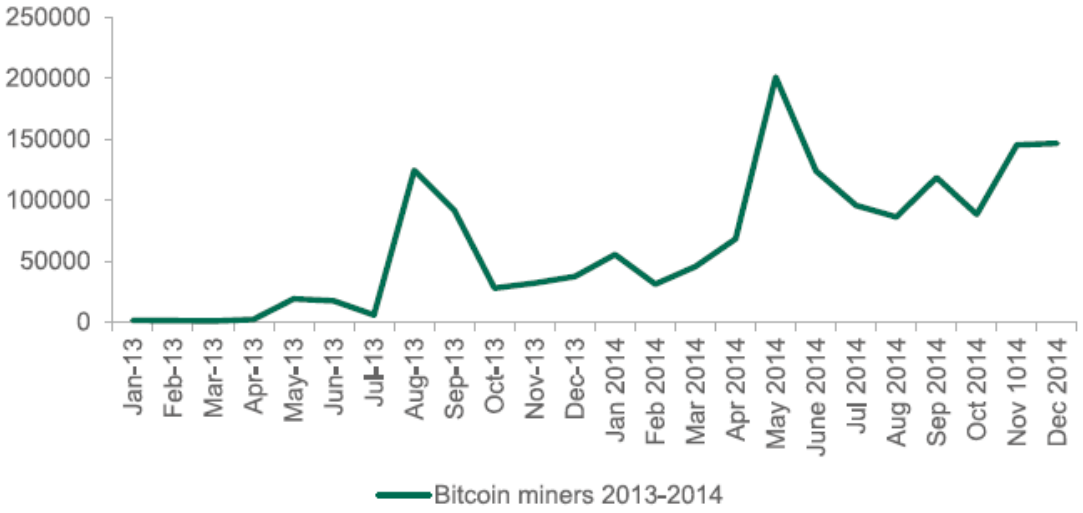

图 18：2013 和 2014 年使用可以安装比特币挖掘软件的恶意软件的攻击

使用比特币开采恶意软件攻击的数量增加了两倍：从 2013 年的 360,065 次增加到 2014 年的 1,204,987 次。看来，尽管比特币的整个生成过程的技术限制使其很难在有限的时间和 CPU 资源环境下大量生成加密货币，罪犯还是能找到使用比特币开采软件来感染用户计算机的理由。另一个有趣的事情是，犯罪分子在汇率较高时开始传播恶意软件时，但它需要一些

时间才能广泛传播。

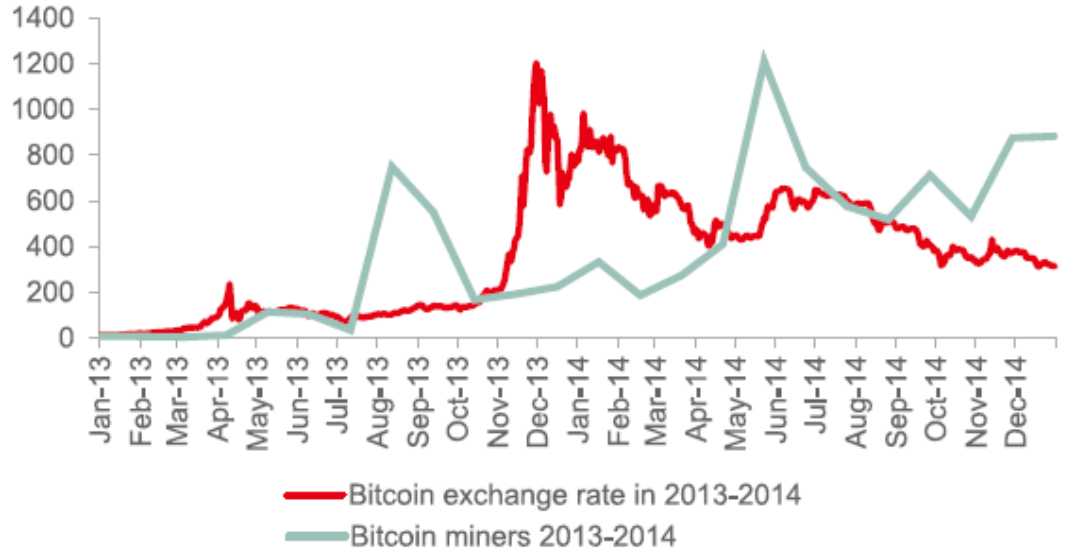

图 18.1：2013-2014 年比特币的汇率及使用比特币挖掘软件进行的攻击

第二种比特币恶意软件是可以盗取比特币钱包的恶意程序。

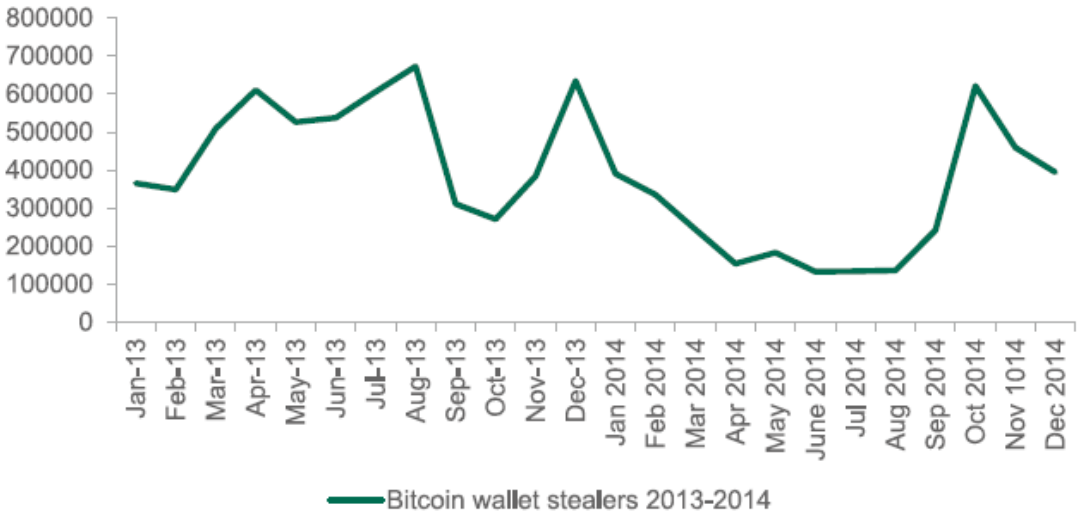

图 19：2013 和 2014 年使用可盗取比特币钱包的恶意软件进行的攻击

含有比特币钱包盗取程序攻击的数量下降了 40.7%，从 2013 年 5,775,942 次袭击下降到 2014 年 3,424,558 次攻击。这一年的年内的检测数量是相当低的；然而，卡巴斯基实验室发现，八月至十月期间，利用这种类型的恶意软件的攻击数量有所增长。很难确定利用比特币钱包盗取程序的攻击数量大起大落背后的原因，但很显然，比特币钱包深受在一个月内发动不少于 10 万次连续攻击的网络罪犯的青睐。

金融攻击的地理分布

2014 年，俄罗斯受攻击数量所占百分比明显下降，从 2013 年占被攻击总量的 45.93% 下降到 29.97%（减少了 15.96 个百分点）；即便这样，俄罗斯在被攻击区域中仍高居榜首。巴西从之前的第 8 名一跃而起至第 2 名，土耳其从第 5 名上升到第 3 名，美国从之前的第 2 名下滑到第 6 名。

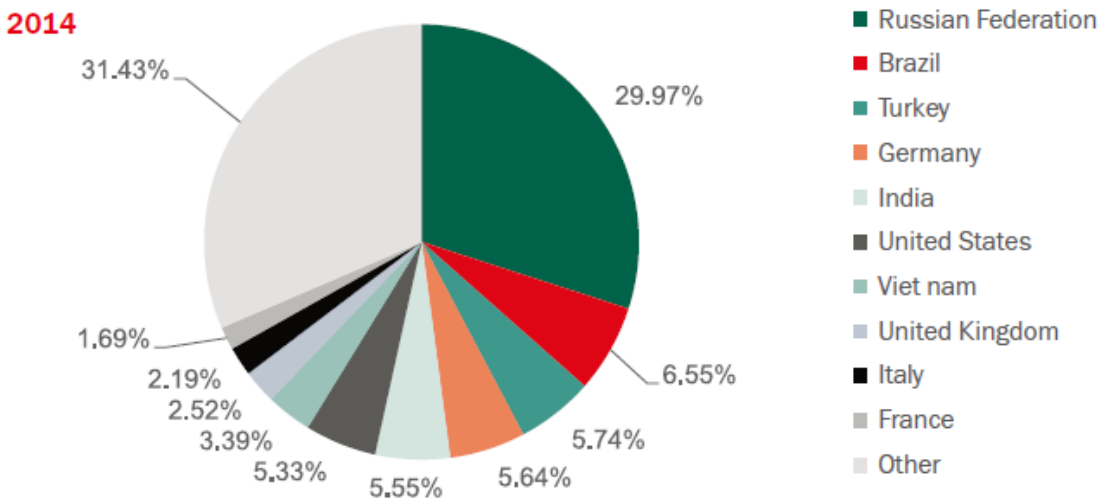

图 20：2014 年金融恶意软件攻击的地理分布[2]

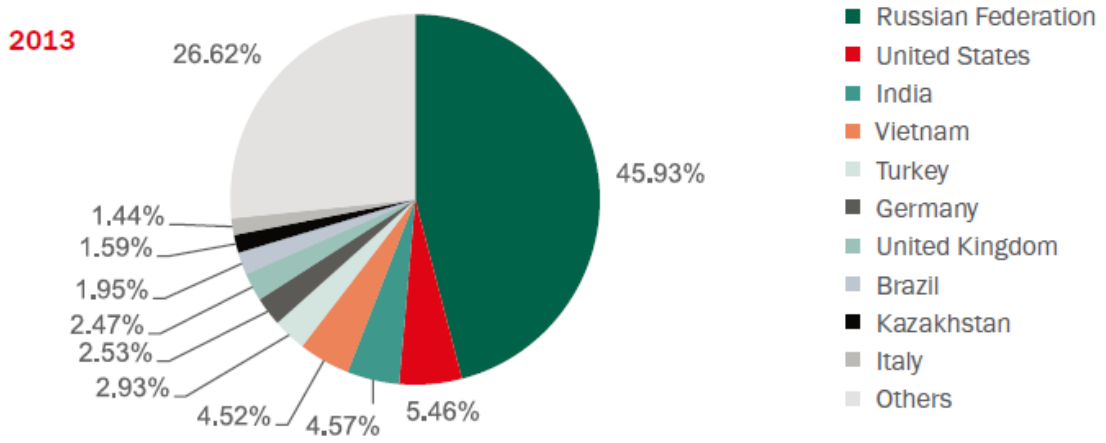

图 21：013 年金融恶意软件攻击的地理分布

[2] 应强调的是，卡巴斯基实验室产品的用户数量因国家而异，因此这项研究的结果也许不能完全反映现有一些国家的情况。然而，对卡巴斯基安全网络（KSN）收集的统计数据的多年监控经验表明，在大多数情况下，对于特定网络威胁或网络威胁类型的传播，以及使用运行不同操作系统的设备的用户分布百分比，KSN 数据的准确性达到 95%。

然而 ,当我们把遭受金融恶意软件攻击的用户数当做所有被任何恶意软件攻击的用户总数时情况就不同了。据统计 KSN 统计数据，2014 年，巴西有五分之一（ 20.05％）用户遇到金融恶意软件攻击。土耳其以被攻击用户占 14.9％位居第 2 位。意大利以被攻击用户占 8.5％位列第 3 名。俄罗斯，被攻击次数最多，以被攻击用户占 3.6％仅排第 8 名。

Country	% of users attacked by any type of malware in 2014	% of users attacked by any type of malware in 2013
Brazil	20.05%	10.4%
Turkey	14.9%	12.01%
Italy	8.5%	8.39%
United Kingdom	5.6%	5.6%
Germany	5.2%	5.5%
India	4.2%	6.7%
Vietnam	4.1%	7.4%
Russian Federation	3.6%	6.1%
France	2.1%	2.7%
United States	1.8%	3.1%

表 2：2013-2014 遭受任意类型的金融恶意软件攻击的用户数量占用户总数的百分比

针对美国用户的攻击明显减少 ,正如受金融恶意软件攻击的用户一样也同样减少。这显然是由 Zbot 家族的行为引起的。受此恶意软件攻击所占百分比占全国注册的所有恶意金融攻击的 75.54％。Zbot 攻击的下降导致了美国的金融攻击的整体下降。

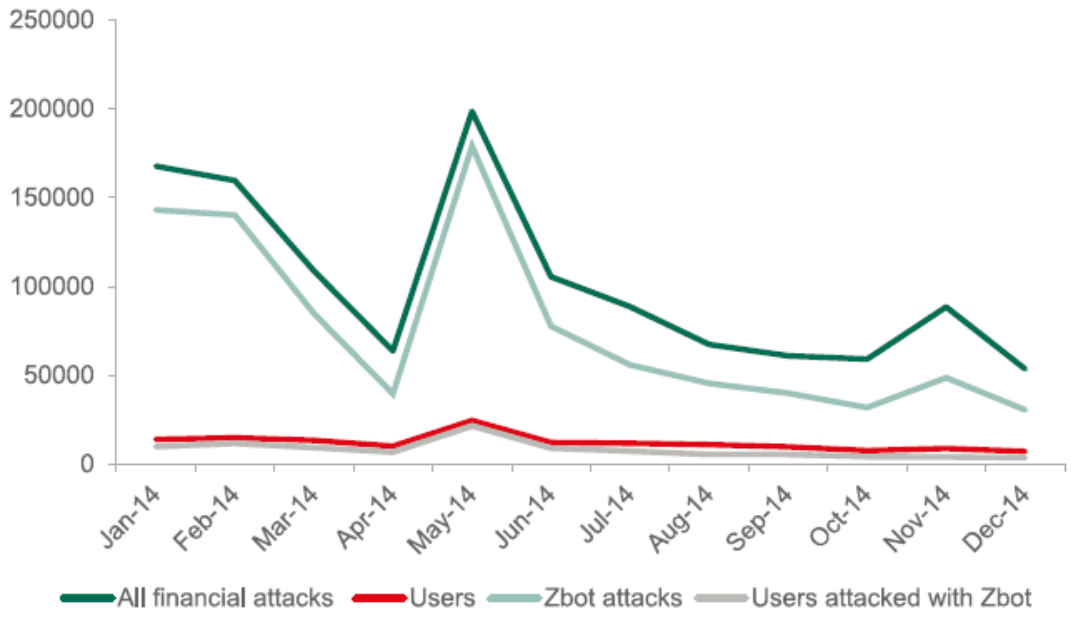

图 22：2014 年记录的美国金融恶意软件攻击

如上述曲线图所示，金融攻击在美国基本上就是指 Zbot 攻击。其他恶意金融程序在该国的流行程度极低。

这一点尤为重要，即在最常遭受到金融恶意软件攻击的国家中，Zbot 家族往往是攻击的领头羊。其攻击在俄罗斯名列第一（占所有攻击的 24.06%）德国（占所有攻击的 43.35%），印度（占所有攻击的 39.32%），英国（占所有攻击的 59.75%），意大利（85.23%）和法国（66.18%）。然而，在一些国家，ZeuS 的利用率却位于 Mt Olympus 之下。例如，巴西。

从 2014 年 1 月到 3 月，巴西受金融恶意软件攻击的形势相对平静。但是，从 4 月起，被注册的检测量飞速增加。

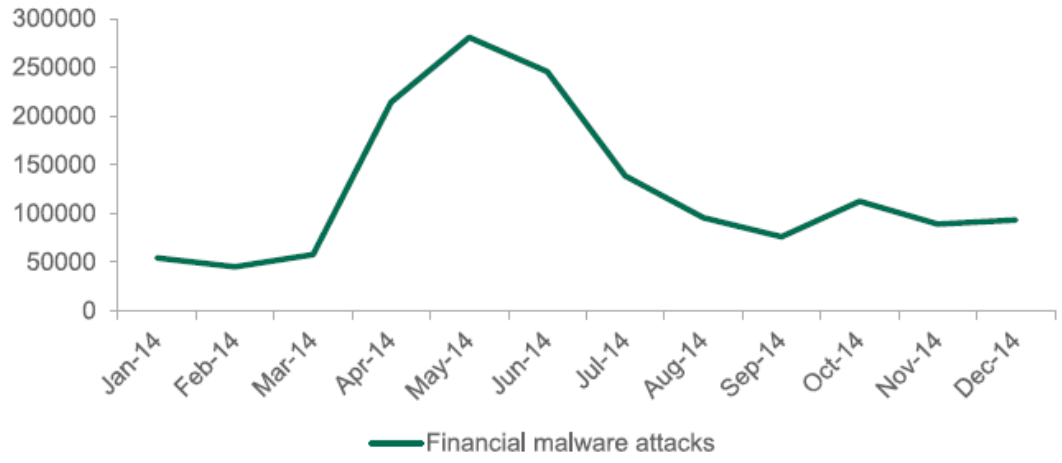

图 23：2014 年记录的巴西金融恶意软件攻击

对该形势更详细地调查表明 恶意攻击量的增加很大程度上由 Trojan-Banker 家族所致。

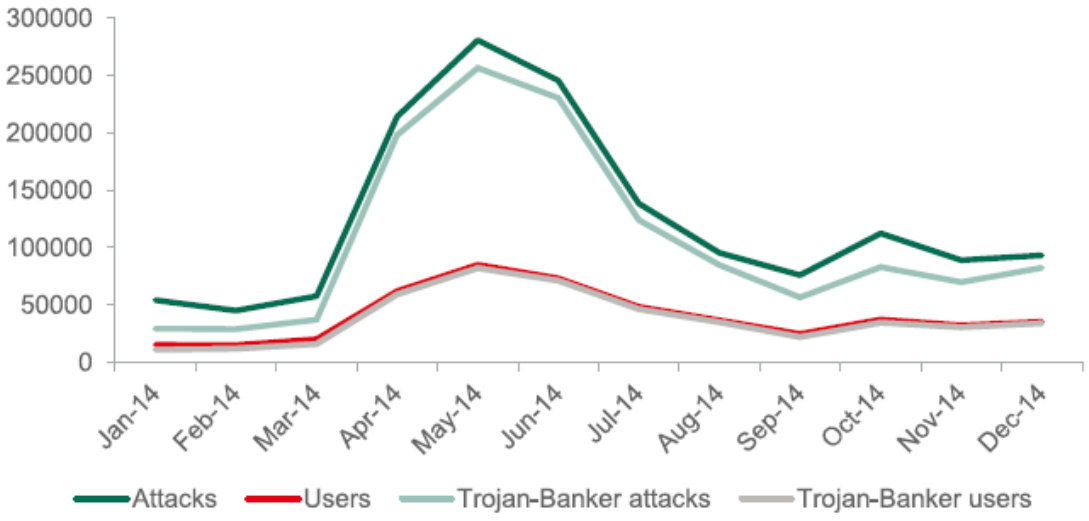

图 24：2014 年巴西金融恶意软件攻击与 Trojan-Banker 攻击的对比

进一步调查表明 ,导致攻击量增加的两大主要原因是其背后的两种恶意程序 :ChePro 和 Lohmys。

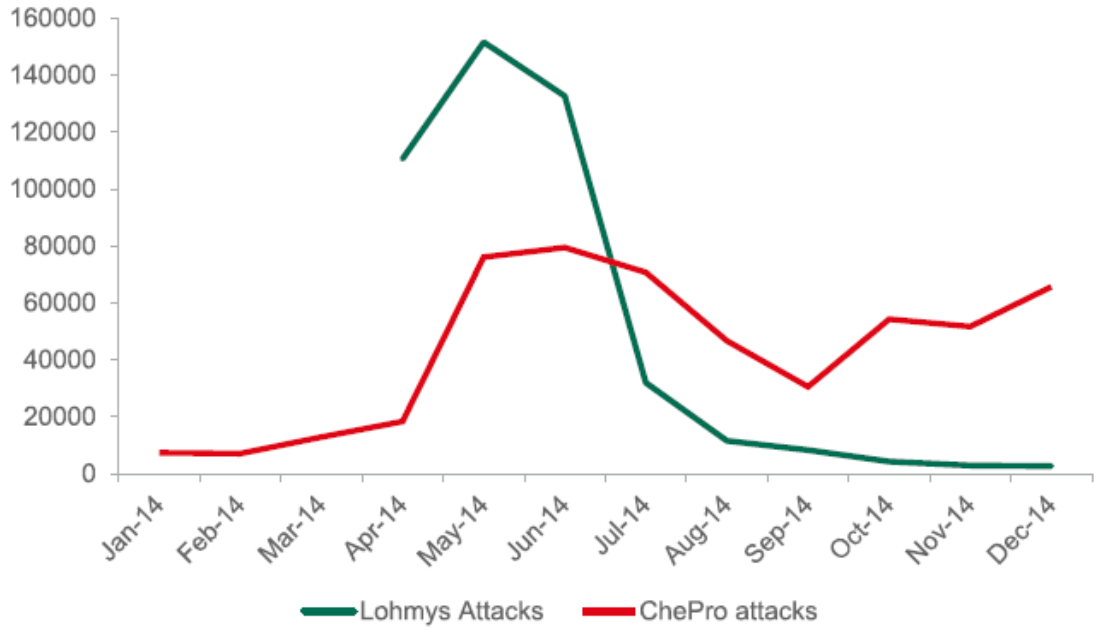

图 25：2014 年记录的巴西 Lomys 和 ChePro 攻击

两个家族具有相同的功能，并通过包含网上银行相关主题的垃圾邮件传播（例如，来自网上银行服务的付款通知）。该邮件包含一个附加图片的 Word 文档：点击图片来启动执行恶意代码。这两种威胁在巴西最流行的金融恶意软件中排名中高居榜首。虽然 Lohmys 活动期间相对较短：从 4 月到 6 月，但 ChePro 木马却在全年持续攻击巴西用户。

Android 金融威胁

2014 年，卡巴斯基实验室与国际刑警组织发布了关于移动网络威胁的联合研究等，包括针对 Android 用户的金融恶意软件。根据研究结果，从 2013 年 8 月 1 日到 2014 年 7 月 31 日，共记录了针对 1,023,202 位用户的 3,408,112 次攻击。大约有 50 万用户曾至少一次受到旨在盗取金钱的移动恶意软件攻击。有趣的是，虽然所有针对 Android 用户的所有恶意攻击中有 59.06%的攻击是旨在盗取用户金钱而发起的(Trojan-SMS 和 Trojan-Banker)，但是，由于 Trojan-SMS 检测在 2014 年春天迅速崩溃，卡巴斯基安全网络检测到这种攻击在下半场显著减少。引发 Trojan-SMS 攻击数量减少的一个原因可能是俄罗斯的移动电话运营商采用了收费通知机制。这意味着，每次客户（或 SMS 木马）尝试向收费号码发送消息时，运营商都会通知客户这项服务将花费多少，并请求用户再次确认。

距离卡巴斯基实验室和国际刑警组织的研究终止日期已经过去了大半年，这便是从那时起事情是如何变化的。

2014 年，卡巴斯基实验室的 Android 产品一共阻止了全球针对 775,887 个用户的 2,317,194 次攻击。这些攻击中的大多数（针对 750,327 个用户的 2,217,979 次攻击）使用的是 Trojan-SMS 恶意软件，其余的(针对 59, 200 个用户的 99,215 次攻击)使用的是 Trojan-Banker 恶意软件。

2014 年由卡巴斯基实验室检测到的使用 Trojan-SMS 和 Trojan- Banker 恶意程序的攻击，共占所有针对 Android 用户恶意攻击的 48.15%。

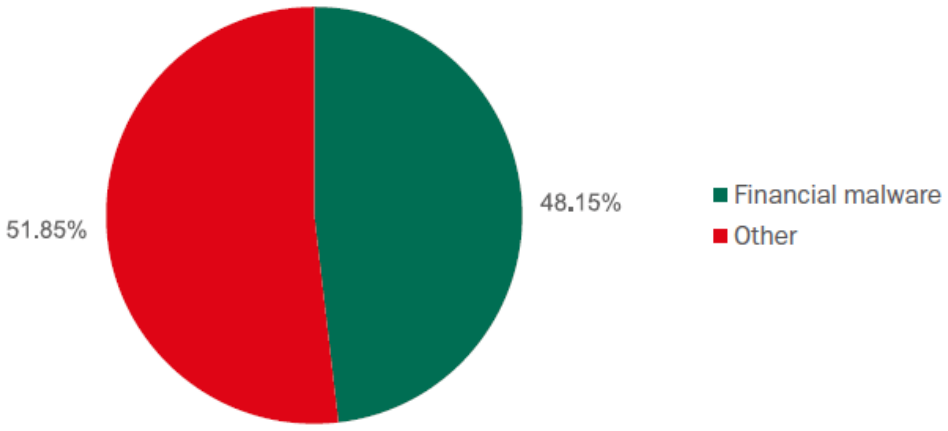

图 26：2014 年针对 Android 设备的用户的金融攻击百分比

与 2013 相比，针对 Android 用户的金融攻击的数量增长到 3.25 倍（从 711,993 次增加到 2,317,194 次），并且被攻击的用户数上升为之前的 3.64 倍（从 212,890 位增加到 775,887 位）。[3]

[3] 应该强调的是，与 2013 年相比，2014 年卡巴斯基实验室的 Android 产品用户数比之前增加了两倍。

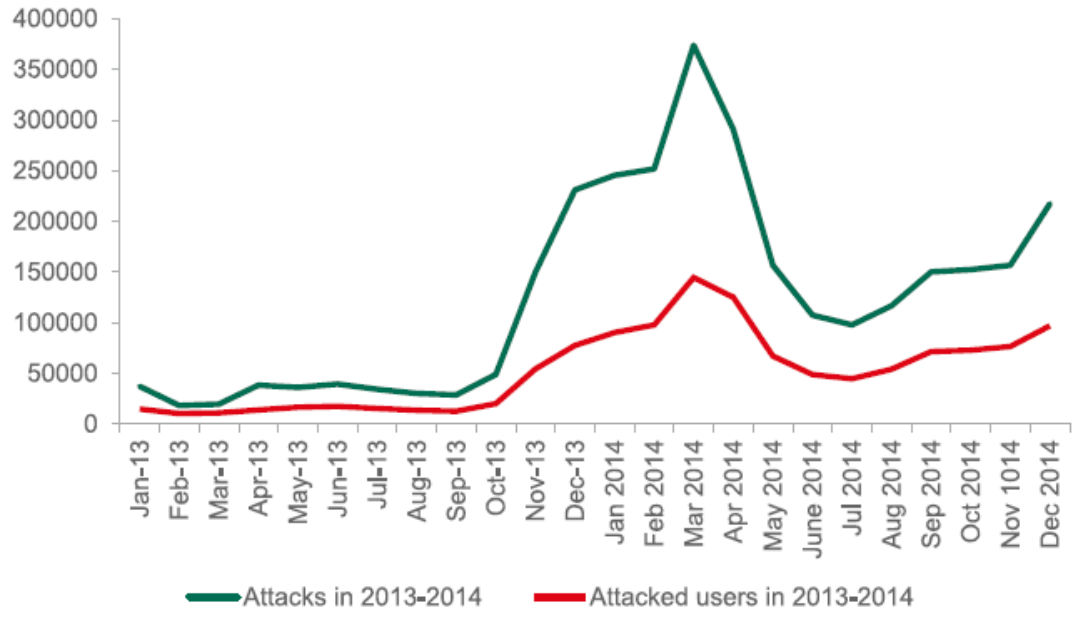

图 27：2013 和 2014 年针对 Android 设备的用户的金融攻击

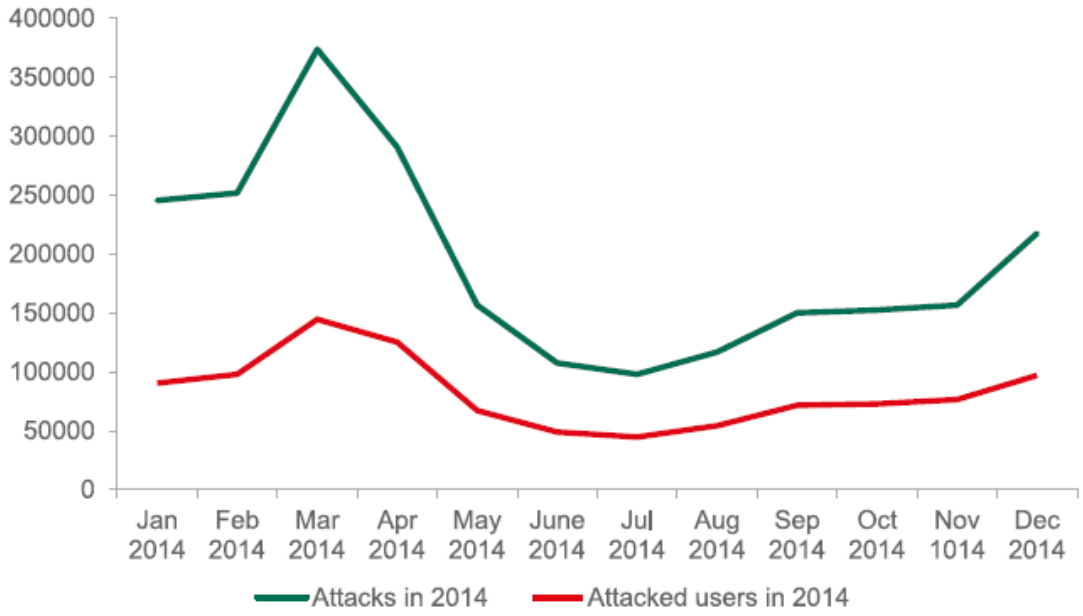

图 28：2014 年针对 Android 设备的用户的金融攻击

早前在七月份完成的报告中我们曾指出此类攻击的减少 ,接着此类攻击在全年剩余时间内稳步上升。攻击量的飞速增长出现在十二月 ,一个贸易和罪犯设定金融数据目标的“繁荣”季节。判断十二月出现的攻击量和被攻击用户的增加是否是 Trojan-SMS 复活的迹象还为时尚早 , 但根据卡巴斯基实验室专家的观点 , 这很可能是。他们已经观察到了即使已在蜂窝网络中应用了收费通知机制 , 也能够感染和窃取的恶意软件的例子 , 例如 , 这种功能近期由卡巴斯基专家在 Opfake.a 和 Fakeinst 恶意软件修改中发现。两者都是非常活跃的 Trojan-SMS 的代表。

虽然 Trojan-Banker 对 Android 用户的金融攻击的量在总量中所占比例相对较小 ,但它的攻击在持续增长。

在这一年中 , 卡巴斯基实验室产品从 Trojan-Banker 中检测到 20 种不同的恶意程序。但它们当中只有三种算是星级表演家：Faketoken , Svpeng 和 Marcher。 Svpeng 和 Marcher 能够通过更换被感染设备上的手机银行应用程序和应用程序商店的应用程序的认证领域而窃取网上银行和信用卡信息的身份认证信息。Faketoken 可拦截用于多因素身份验证系统的 mTAN 代码 , 并将该代码转发给犯罪分子。

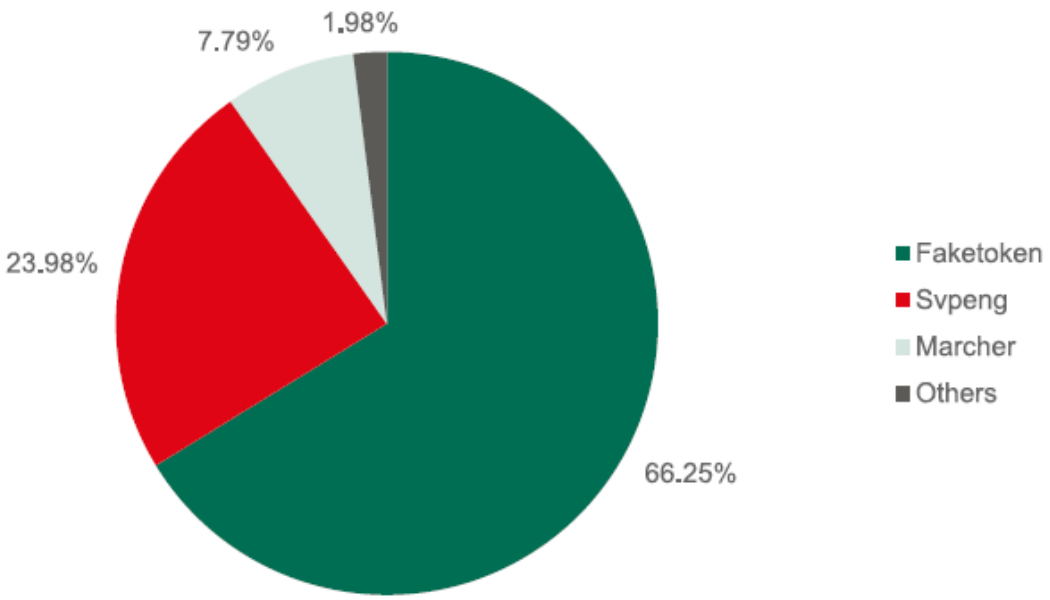

图 29：三大主要 Android 银行恶意软件家族的攻击分布

这三大家族占所有 Trojan-Banker 攻击量的 98.02%。从四月到十月 , 这三大程序基本是按兵不动 , 但随着假期的开始 , 这些恶意软件背后的不法分子便活跃起来 , 继而攻击量也开始增长。

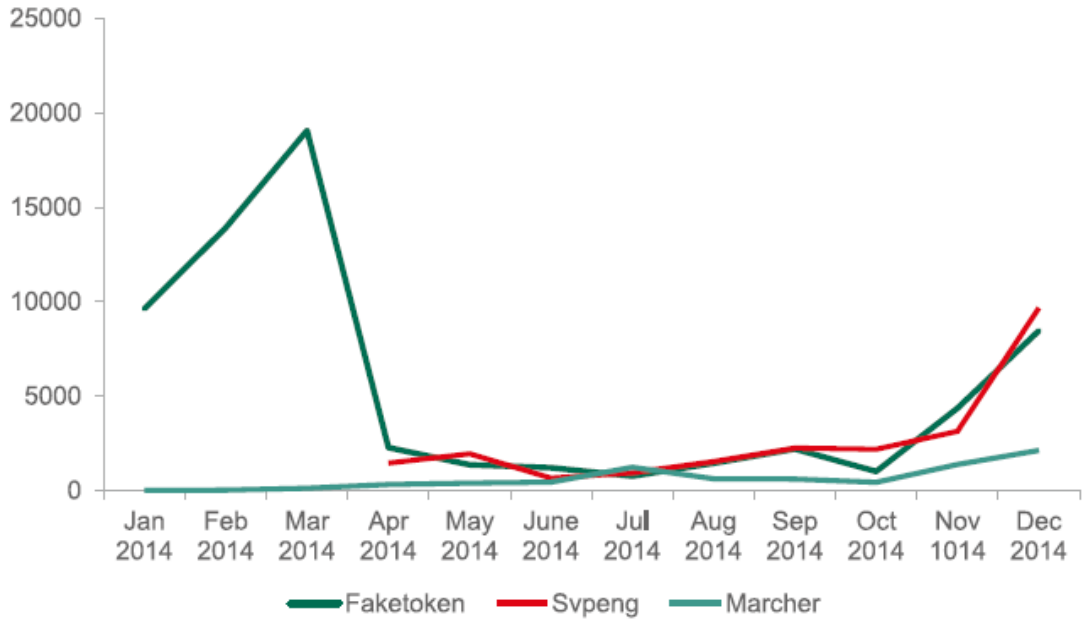

图 30：2014 年使用主要 Android 银行恶意软件家族的攻击

使用金融恶意软件的金融攻击的地理分布正如所料。俄罗斯（63.87%）是 Trojan-SMS 和 Trojan-Banker 的头号攻击目标。其次是哈萨克斯坦（5.67%）,乌克兰（2.95%）,德国（2.78%）和马来西亚（2.69%）。

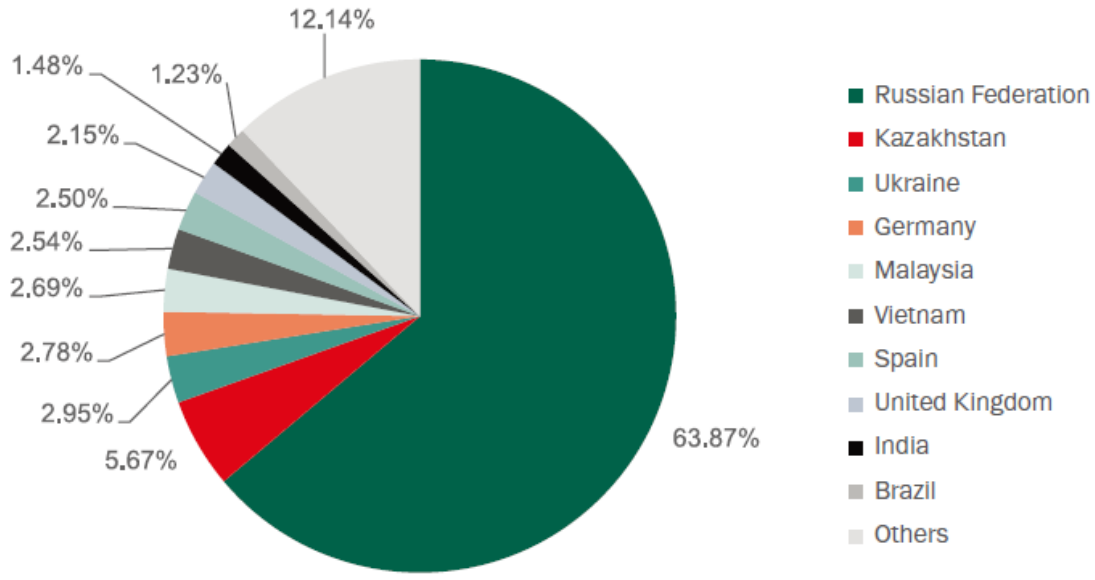

图 31：2014 年以 Android 设备的用户为目标的金融恶意软件攻击的地理分布

谈到受到金融恶意软件攻击的用户数和受到任何恶意软件攻击的基于 Android 设备的用户数的比较时，情况稍有不同。俄罗斯和哈萨克斯坦的排名要对掉。其次是西班牙，乌克兰和马来西亚分别有 63.3%，60.5%和 58.4%的用户遇到金融威胁。

Country	% of users attacked by any type of malware
Kazakhstan	71.7%
Russan Federation	71.1%
Spain	63.3%
Ukraine	60.5%
Malaysia	58.4%
United Kingdom	50.9%
Vietnam	46.3%
Germany	41.7%
Brazil	38,20%
India	9,40%

表 3：2014 年受金融恶意软件攻击的 Android 用户占所有遭受恶意软件攻击的 Android 的用户总数的百分比

这些国家中的多数因其预付费移动合同的普及和优质的 SMS 服务使它们成为金融攻击的主要目标 –以上两个因素引发网络罪犯专门从事短信诈骗活动 ,因为它们使得网络罪犯可以轻易地从用户的移动账号盗取钱财。这就是为什么这些国家的用户在其设备上安装移动应用程序时要特别谨慎。

结论和建议

研究表明，在线资金损失仍然是全球上百万用户面临的现实问题：2014 年，随着攻击的平均强度的加大 ,把网上银行证书作为目标的恶意软件攻击所占比例明显增加。这也表明，越来越多的基于 Android 设备的用户将成为金融攻击的目标，并揭示了罪犯试图获得更多违法所得的前进方向。为了帮助您在网络威胁面前保护好自己，卡巴斯基实验室的专家们提出以下建议：

家庭用户

- 不要点击任何来自陌生人或您的朋友通过社交网站或电子邮件发送的可疑链接；
- 不要在您的设备上下载、打开或存储陌生的文件；
- 不要使用不可靠的（公共的）Wi-Fi 网络进行网上支付；
- 输入您的数据之前，请务必检查任何网站的真伪；最起码，检查该网站地址栏中的地址，以确保它是该组织的官方网站；
- 只使用有安全连接的网站（网站的地址应该以 HTTPS://开头而不是 HTTP://）;
- 在进行在线金融交易时，尽量使用多因素身份验证技术（一次性口令等），并尽可能避免不使用这些技术的服务；
- 基于 Android 的移动设备是网络罪犯的重要目标，特别是在广泛使用预付费移动合同和通过 SMS 进行电子支付的国家。为了设备的安全，应遵守几项基本的安全规则：防止来自第三方商店应用程序的安装，并确保你已经在你的智能手机或平板电脑上安装了最新版本的操作系统。
- 加密货币吸引了很多网络罪犯，所以如果你是一个比特币钱包持有人，一定要保管好它：不要把比特币放在一个钱包；可能的话，将钱包存储在加密形式的外部媒介内。不要使用在线服务来存储加密的货币。
- 使用计算机或移动设备时，除了提供传统的反恶意软件、反钓鱼攻击和其它安全技术外，请使用能够为在线金融交易提供额外保护技术的可靠的安全解决方案。

企业用户

- 为了避免财务数据的丢失 建议组织不仅要在公司所有的工作站使用可靠的安全解决方案，同时也要针对不同用户类型制定不同的策略，并在企业设备上追踪用户活动记录；
- 使用移动设备管理系统 以便控制金融交易时哪些设备可以使用 怎么用 由谁用，并保护它们免受可能的网络威胁；
- 在进行在线金融交易时，尽量使用多因素身份验证技术（一次性口令等），并尽可能避免不使用这些技术的服务；
- 随着金融网络威胁的复杂性和在线欺诈所使用方法的不断增加 不要忘记定期更新所有安全解决方案和反威胁措施；
- 不要忽视对员工进行网络安全基础知识培训的重要性（尤其是那些财务工作者）；
- 对于金融服务公司 建议在其基础设施和包括移动设备在内的用户设备中部署专门的反诈骗解决方案，这有助于防止可能发生的金融攻击，而不是去事后修复，最终防止公司金融和声誉受损。

研究方法

研究中使用的非个性化数据来自卡巴斯基安全网络。卡巴斯基安全网络是一个用来实时处理卡巴斯基实验室用户遇到的威胁数据的基于云的分布式基础设施。卡巴斯基安全网络的建立是为了确保关于最新威胁的信息以最快的速度传递给卡巴斯基实验室产品的用户。通过此网络，在先前未知的威胁被发现后的几分钟内，关于该威胁的信息就被添加到数据库中。KSN 的另一个功能是处理出现在用户计算机上的威胁的去个性化的统计数据。用户自由决定是否向 KSN 提供信息。以这种方式接收到的数据是此报告的研究基础。

研究人员研究了卡巴斯基实验室组件成功防御针对 Windows and Mac OS X 的钓鱼攻击、针对 Windows 设备的恶意软件攻击以及针对 Android 的移动恶意软件攻击的次数。另外，此研究着眼于被攻击用户数的统计数据。该研究还分析了攻击的地理分布信息。

该研究涵盖了 2014 年全年；并且对收集来的数据与 2013 年收集到的等效数据进行了对比分析。该研究的主题之一就是网络钓鱼活动的目标：下载伪造的支付系统、网上银行系统、网店及其他与金融机构有关的目标的阻断次数。此外，卡巴斯基实验室的专家们挑选了几十个专门盗取金融数据的恶意软件样本，并研究它们被发现的频率。

由于加密货币比特币在 2014 年的盛行，卡巴斯基实验室的专家们将与生成和盗取这种货币相关的威胁单独分类，并跟进其发展演变。

关于负责任的信息传播

本文分析了 Windows 和 Android 平台的网络威胁全景。本文基于卡巴斯基实验室安全产品检测到的不安全或恶意的应用程序和网页(由于其功能而被视为不安全或恶意)的实例信息。为了避免误解文件中提到的事实，卡巴斯基实验室想强调几点与报告编写方式相关的问题。

1. 术语

该报告使用了几个描述安全产品是如何与恶意软件相互作用的术语。术语“攻击”是最常被使用的。在卡巴斯基实验室的术语中，攻击是指安全产品在受保护设备内检测到任一被当作是恶意的或属于网络钓鱼的软件或网页，不管是否检测到了执行恶意代码的企图。术语“用户”专指由卡巴斯基实验室产品保护的设备所有者。

2. 数据库及其地理分布

所有的计算和结论作为这项研究的一部分，完全依赖于来自卡巴斯基实验室客户群体的数据，这是来自超过 200 个国家和地区的 8000 万用户的数据。应该强调的是，卡巴斯基实验室产品的用户数量因国家而异，因此这项研究的结果可能并不能完全反映有些国家的现状。然而，对卡巴斯基安全网络（KSN）所收集的统计数据的多年监控经验表明，对于特定网络威胁或网络威胁类型的传播，以及使用运行不同操作系统的设备的用户分布百分比，KSN 数据的准确性达到 95%。KSN 还与其它来源（专注于收集和分析统计数据的公司）的数据联系紧密。

负责任的信息传播

这项研究可以自由共享和传播。鉴于前面提到与 KSN 统计数据的收集方法相关的问题，卡巴斯基实验室要求那些认为该研究中所阐述的信息有趣并实用的读者在准备公开材料时注明出处。

Securelist, the resource for Kaspersky Lab experts' technical research, analysis, and thoughts.

Follow us

Kaspersky Lab global Website

Eugene Kaspersky Blog

Kaspersky Lab B2C Blog

Kaspersky Lab B2B Blog

Kaspersky Lab security news service

Kaspersky Lab Academy

KASPERSKY lab