2016 年黑色星期五威胁概述

卡巴斯基实验室

2016 年 11 月

2016 年黑色星期五威胁概述

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	Kaspersky Lab Black Friday Threat Overview 2016		
原文作者	卡巴斯基实验室	**原文发布日期**	2016 年 11 月
作者简介	卡巴斯基实验室是一家国际网络安全和反病毒提供商，总部设在俄罗斯的莫斯科。 https://en.wikipedia.org/wiki/Kaspersky_Lab		
原文发布单位	卡巴斯基实验室		
原文出处	https://securelist.com/files/2016/11/KASPERSKY-LAB-BLACK-FRIDAY-THREAT-OVERVIEW-2016.pdf		
译者	安天技术公益翻译组	**校对者**	安天技术公益翻译组
分享地址	请浏览创意安天论坛 bbs.antiy.cn 安天公益翻译板块		
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

简介

互联网彻底改变了人们购物的方式。到 2018 年底 ,世界上大约有 20%的人在网上购物，且有更多的人通过移动设备而不是通过电脑购物。据估计，到 2017 年底，将有 60%的电子商务来自智能手机，届时将有数百万人疯狂的在家里、公司、餐馆、机场和火车站、街头、商店、度假时在网上浏览、购买商品，且经常连接私人无线网络，脱离安全保护。

且不论使用的设备 ,每一次交互和交易都会产生云数据 ,商家往往会捕获该数据以便推送更多有针对性、个人化的服务。不幸的是，其他人也在伺机获取顾客的交易信息，例如通过不安全的公共无线网络，钓鱼邮件和被感染的网站，或其它方式。他们被称为网络罪犯，完全不把顾客和商家的最佳利益放在心上。

在一年之中最繁忙的购物季，零售商和网购用户面临最高的风险：例如，11 月份的感恩节购物周（从黑色星期五到网购星期一），12 月份的圣诞节和新年购物活动。

随着交易量和成交速度增加，网络威胁也在增加。本概述中，卡巴斯基实验室披露了在火爆的购物期针对消费者和零售商的网络攻击。

以某个黑色星期五和网购星期一为例 ,我们回顾一下过去几年网络威胁的发展态势如何。

2013 年，黑色星期五和网购星期一在北美就已初具规模并开始在其它地方快速发展。仅在美国，2012 年网购星期一线上销售增长了 21%，销售额达到 22.7 亿美元，而黑色星期五则获得了价值为 19.3 亿美元的成交量 ,最终超过平均销售值。17%的销售总额是通过移动客户端完成的，2012 年增长了 55%。在英国，线上销售则稍逊一筹，11 月增长了 16%，据预测仅网购星期一线上的成交额将超过 6 亿美元。

同年，美国零售商 Target 发现在 11 月 27 日到 12 月 15 期间大约有 4000 万顾客的信用卡信息被盗。显然，是通过店内的销售点系统入侵的。

2014 年影响恶劣的索尼攻击事件，导致 2013 年的记录被打破。2014 年美国感恩节见证了用于在线浏览的移动设备（52%）比电脑（48%）更多。与 2013 年同天相比，2014 年黑色星期五线上销售增长了 21%，大约 1/3（30%）的订单通过移动设备完成。 Adobe 估计美国黑色星期五网上销售总额为 24 亿美元，感恩节 13 亿美元和网购星期一 27 亿美元。在英国，线上销售在黑色星期五期间达到了顶峰，与节前一周比飚增了 44%，比 2013 年同周相比令人震惊，增长了 135%，而移动端销售增长了 83%。

2015 年所有的记录再次被打破。2015 年网购星期一是美国线上销售额最大的一天。网

上顾客当天创下了 30.7 亿美元，和感恩节周 4 天 80.3 亿美元的成交记录。IBM 分析表明，2014 年总的销售额增长了 26%，其中 40%的销售额来自移动设备。

本季顾客信息被盗，涉及恶意软件攻击世界各地宾馆销售点系统，包括 Hyatt, Starwood 和 Hilton 等酒店。

2016 年消费记录再次被盗看起来已成定局，罪犯可能竭尽所能利用购物活动窃取银行账户认证信息或甚至直接抢钱。本概述包含了买家、卖家和支付系统供应商在接下来的几周可能面临的网络威胁。

方法和主要发现

本文基于卡巴斯基实验室恶意软件和网络钓鱼检测系统（攻击次数和被攻击的用户）收集的信息，事件分析和地下黑客论坛的信息。本文包括 2013 年、2014 年和 2015 年第四季度和 2016 年的几个月。虽然官方的“黑色星期五”销售期截止到网购星期一，恰好感恩节之后。几天之后便是另一个销售高峰开始：称为圣诞节前期，也是一年中零售商最赚钱的时候。10 月份也被算在销售高峰期，因为被称为“黑色星期五”的销售活动实际上经常在销售日前就已开始（万圣节销售就是一个很好的例子），更重要的是，网络罪犯通常提前很多天做好诈骗的准备。

本概述也包含了针对一些普通用户、店主和支付设施所有者预防销售高峰期诈骗的措施。

主要发现：

- 销售高峰季金融网络钓鱼比例为 9%，比同年其它时候比例更高。
- 在此期间，针对网上购物和支付系统期间的钓鱼攻击比例通常高于针对银行的钓鱼攻击。
- 在某些特定的日子，例如黑色星期五，网购星期一和圣诞节前后，网络罪犯设法关注恶意活动，例如散布金融恶意软件和钓鱼网页。
- 卡巴斯基实验室收集的病毒包括 36 个销售点（PoS）恶意软件，其中 6 个是 2016 年添加的。与之相比，银行恶意软件的数量只有 30 个。
- 地下读卡器和伪造信用卡供应商销售正火爆。2015 年 12 月读卡器的销售增加了十多倍：从 25-30 个增长到 500 个。
- 卡巴斯基研究人员预计,节日期间针对网上零售商会遭到 DDoS 勒索攻击。

网络钓鱼

网络钓鱼是网络罪犯用来窃取支付卡信息和线上银行账户认证最常用的方法之一。制定网络钓鱼计划相对简单（诈骗犯甚至不需要知道如何编写恶意代码，只需懂得所需的基本网页开发和设计技术即可），但该方法很有效，因为它们大多基于社会工程技术。节日期间，用户渴望物美价廉的商品，渴望在浏览网页时看到特价商品。网络罪犯了解消费者的特点并试图尽可能利用这一弱点。

金融钓鱼占总攻击量的比例

去年数据表明，金融网络钓鱼比例通常不低于一年中记录的所有的网络钓鱼攻击。例如，2013 年，占到了所有登记网络钓鱼攻击的 31.45%，2014 年占 28.74%，2015 年占 34.33%。今年的统计数据虽未出来，但根据季度数据判断趋势与之前一致。

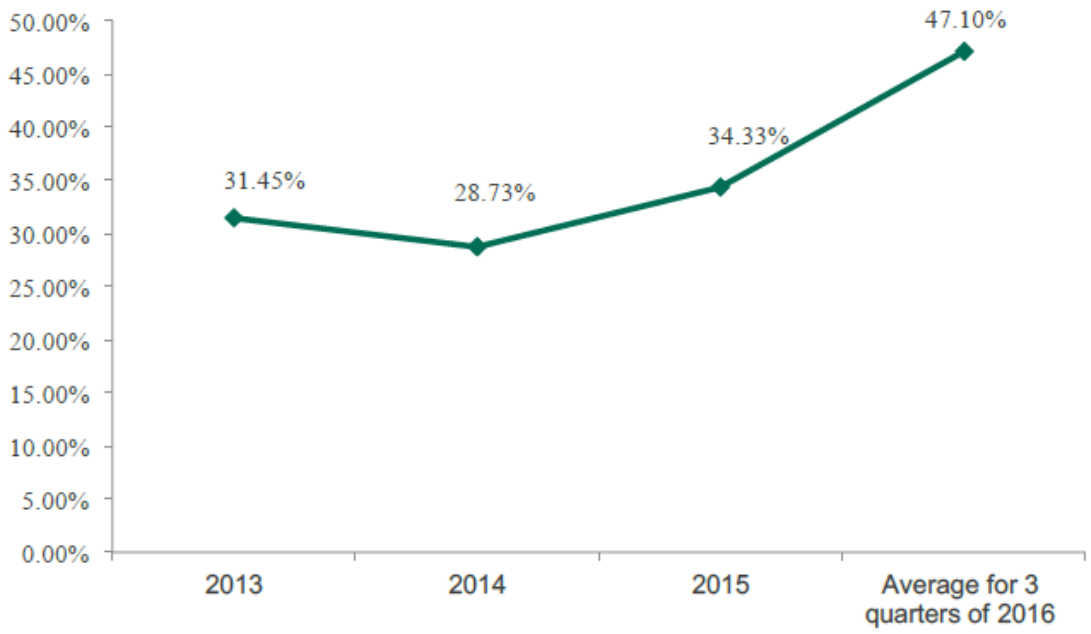

图 1：2013 年-2016 年网络钓鱼占攻击总数的份额

当遇到节日销售期时，然而事情就变得截然不同。正如预料的一样，这次金融网络钓鱼比例明显比一般年份的比例要高。

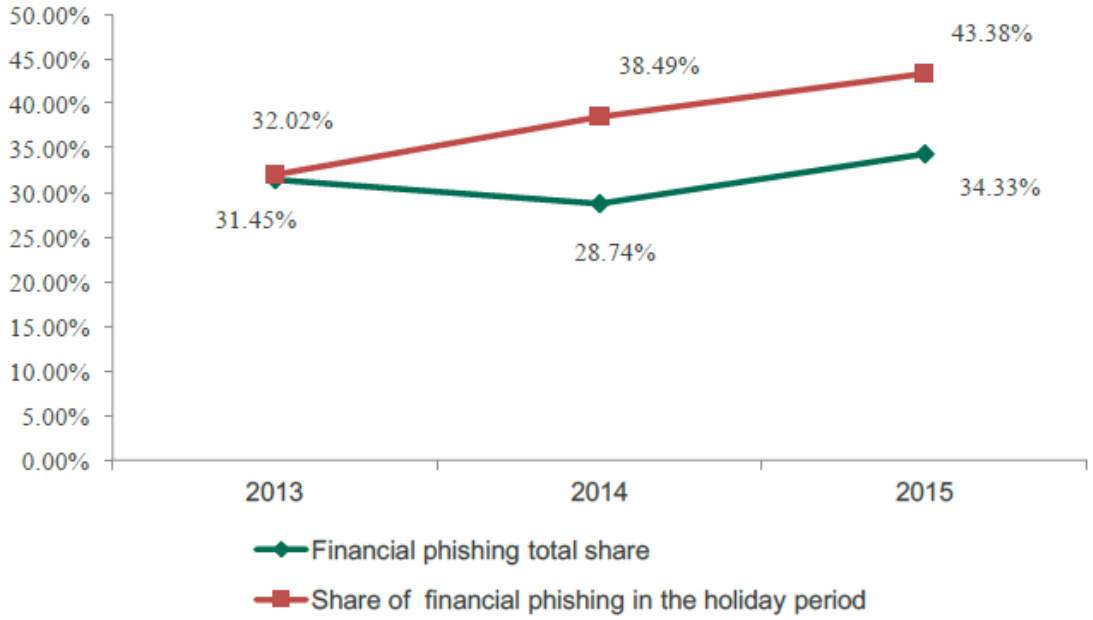

图 2：与假期相比，不同时期的金融网络钓鱼比例

虽然 2013 年金融网络钓鱼攻击在销售高峰期只比同年总攻击高了 0.5 个百分点。2014 和 2015 年，我们发现节日期间攻击比例差别明显，大约有 9 个百分点。当然，这些数据不足以表明很强的倾向。无论怎样，今年很可能再次出现很大的差别。

金融网络钓鱼类型

卡巴斯基实验室对三类主要的金融网络钓鱼进行了区分 :银行业 ,电子支付和电子购物。它们都是网络钓鱼网页，通过模仿相应的合法机构处理金融交易。基于 2014 和 2015 年第四季度观察到的数据发现，节日期间分开不同类型的金融网络钓鱼其全年的结果也不同。

例如 ,2013 年期间网络钓鱼攻击与上个节日季度相差不大——不到一个百分点。然而，内部的类别差异要更明显。

那年第四季度电子购物比例增长超过 1%到 7.8%。且针对用户普遍使用的支付系统的网络钓鱼（5.46%）与今年剩下时间网络钓鱼（2.74%）相比超过两倍。同时，针对线上银行网络钓鱼（18.76%）比例比今年（22.2%）要低。

这一情形明年会再次出现，但幅度更加明显。购物网络钓鱼在节日季比全年高了 5.32 个百分点。支付系统网络钓鱼高了 2.78 个百分点。

2013	**Full year**	**Q4**
Financial phishing total	31.45%	32.02%
E-shop	6.51%	7.80%
E-banks	22.20%	18.76%
E-payments	2.74%	5.46%
2014	**Full year**	**Q4**
Financial phishing total	28.73%	38.49%
E-shop	7.32%	12.63%
E-banks	16.27%	17.94%
E-payments	5.14%	7.92%
2015	**Full year**	**Q4**
Financial phishing total	34.33%	43.38%
E-shop	9.08%	12.29%
E-banks	17.45%	18.90%
E-payments	7.08%	12.19%

图 3：2013-2015 年不同类型金融网络钓鱼的份额变化

这些差别伴随着针对特定的目标进行攻击。2014 年，卡巴斯基实验室研究人员组织了就黑色星期五动态攻击的小调查，发现企图加载网络钓鱼的网页被装有卡巴斯基实验室产品的用户检测、拦截，表明攻击实际上在不断增长。

这是一些时间线图，是网络钓鱼骗子最常攻击的目标。

以美国运通（American Express）为例，2014 和 2015 年的网络钓鱼攻击非常相似。

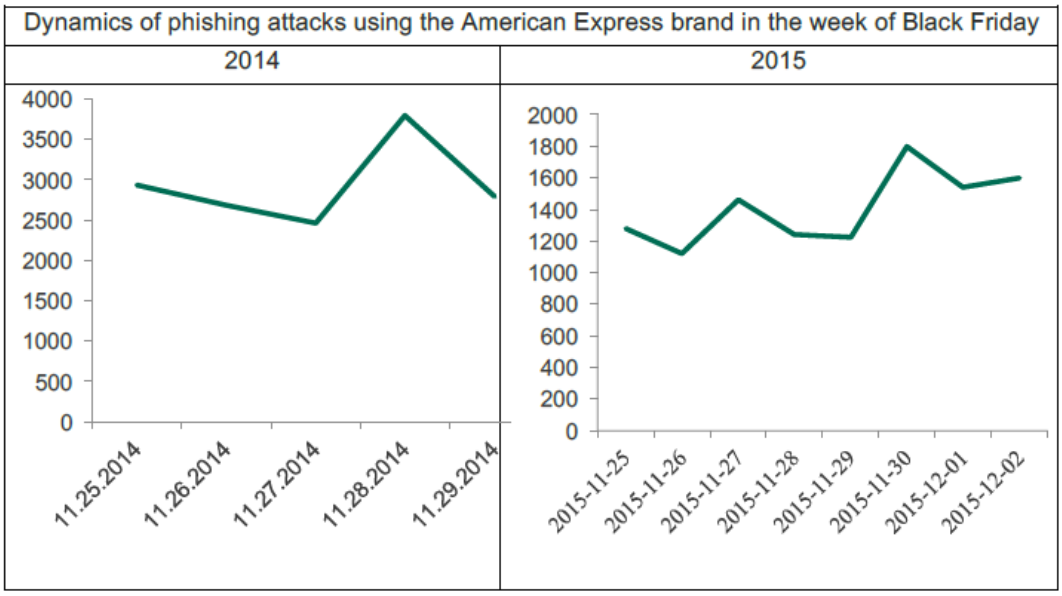

图 4：针对特定目标的攻击时间线示例

对于其他涉及网上购物的品牌，情形也是类似的。虽然 2015 年黑色星期五后攻击出现增长，且于网购星期一达到顶峰。

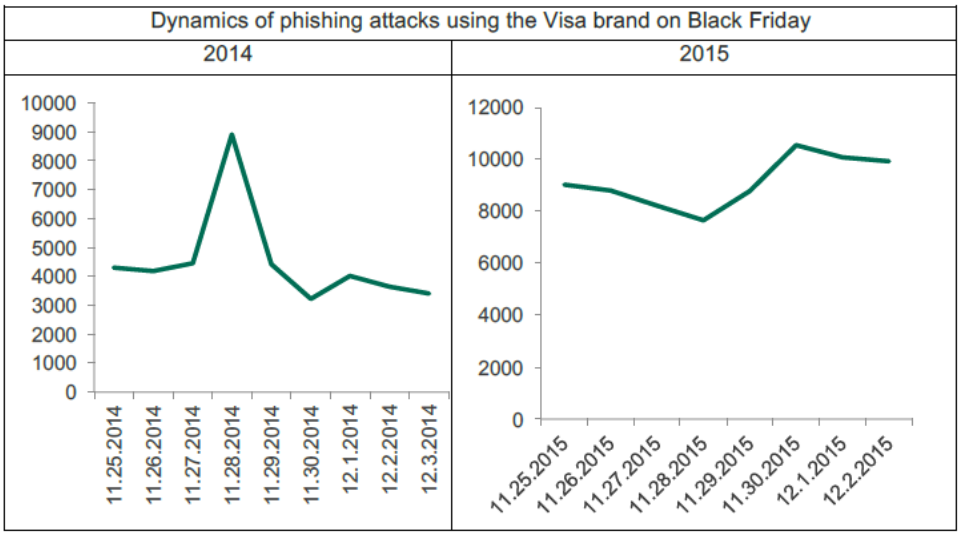

图 5：针对特定目标的攻击时间线示例

最后，利用网上购物品牌的网络钓鱼攻击也显然与特定日期有关，例如黑色星期五。

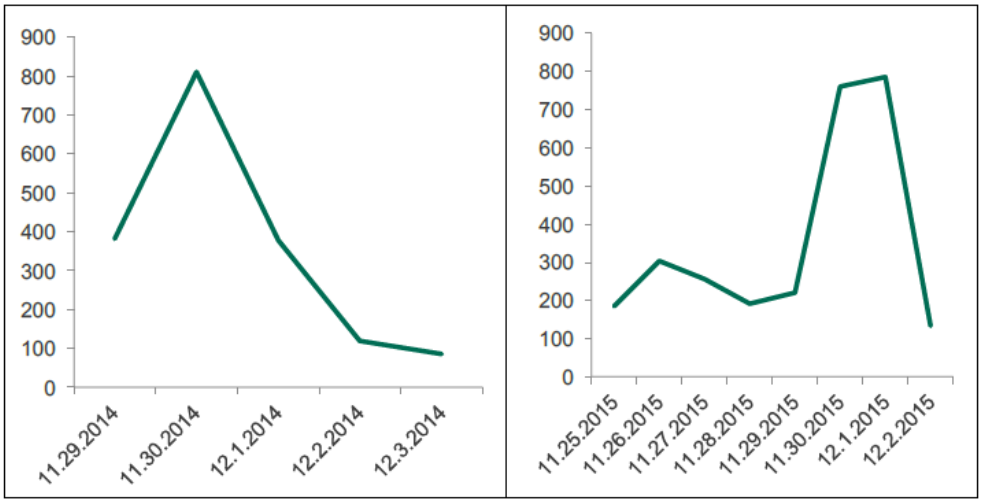

图 6：针对特定目标的攻击时间线示例

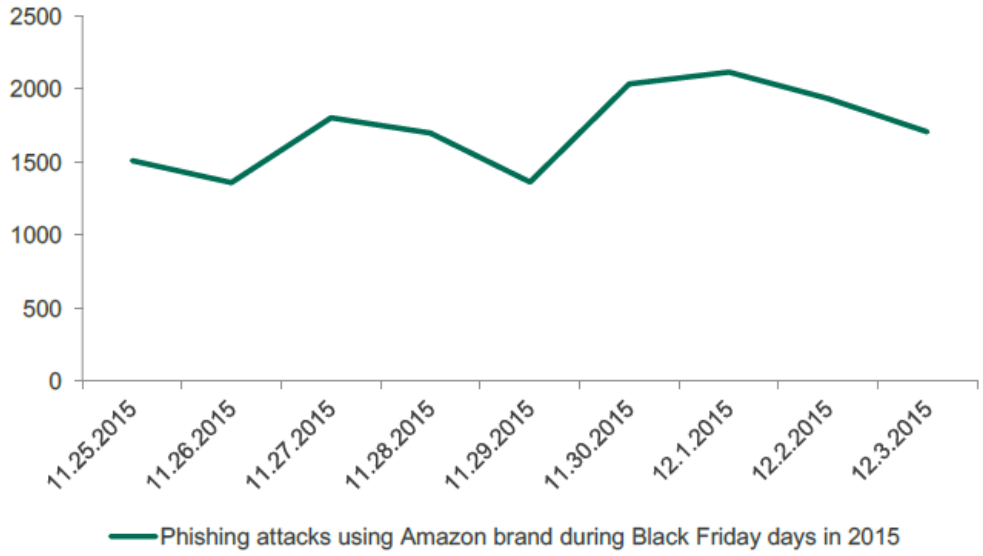

图 7：针对特定目标的攻击时间线示例

圣诞和新年通常也是攻击高峰时期，基本上是全季度第二高峰期。另外，本文不仅将展示网络钓鱼攻击高峰的典型特征，也将展示金融恶意软件攻击高峰。

“节日”网络钓鱼案例

大多数情况下，网络罪犯不会费心去编造事情，只是复制合法商店、网上银行和支付系统的网页。

如下所示，网络钓鱼复制的亚马逊商店的图片与原网站极其相似。

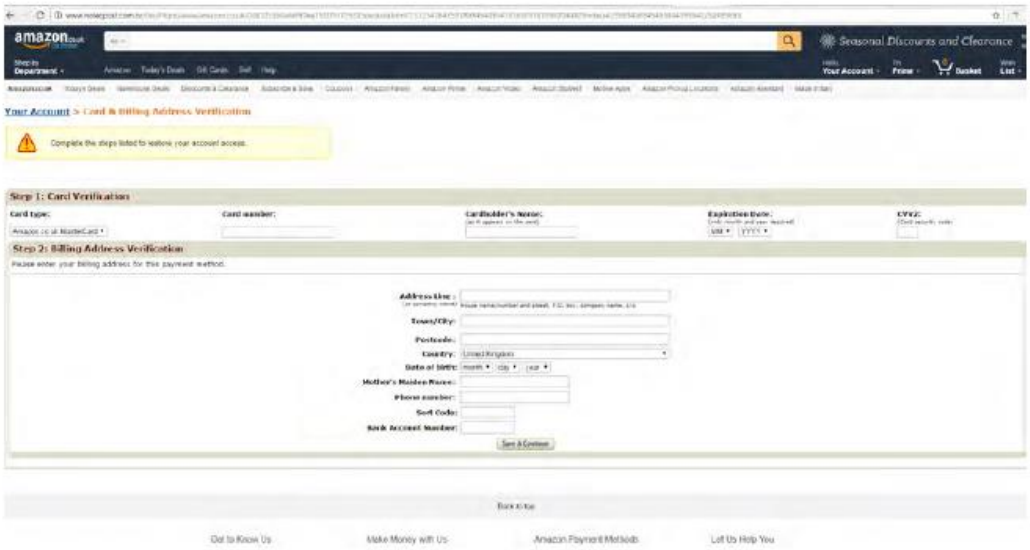

图 8：假冒亚马逊网店示例

网络罪犯对支付系统和银行做法也类似。下面是钓鱼网站模仿 Visa 和美国运通卡数据提交表单的图片。还有其它一些公司也遭遇此类经历，通常，这两个公司是被网络钓鱼者假冒靠前的品牌。

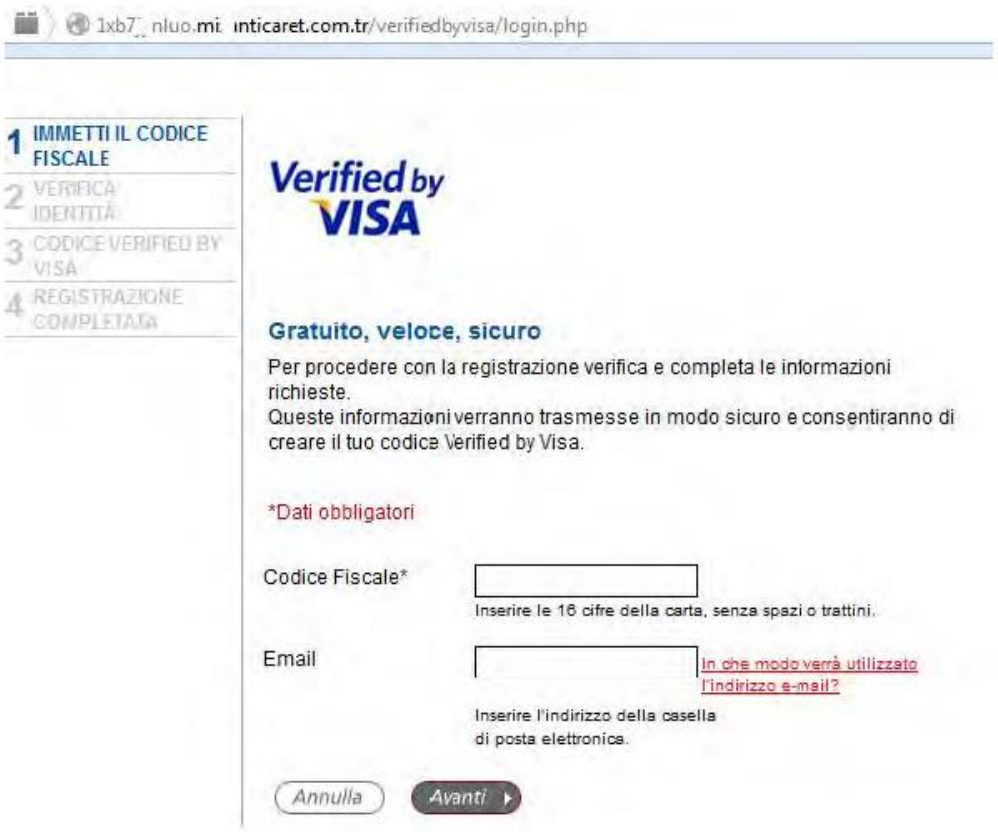

图 9：假冒 Visa 支付表格示例

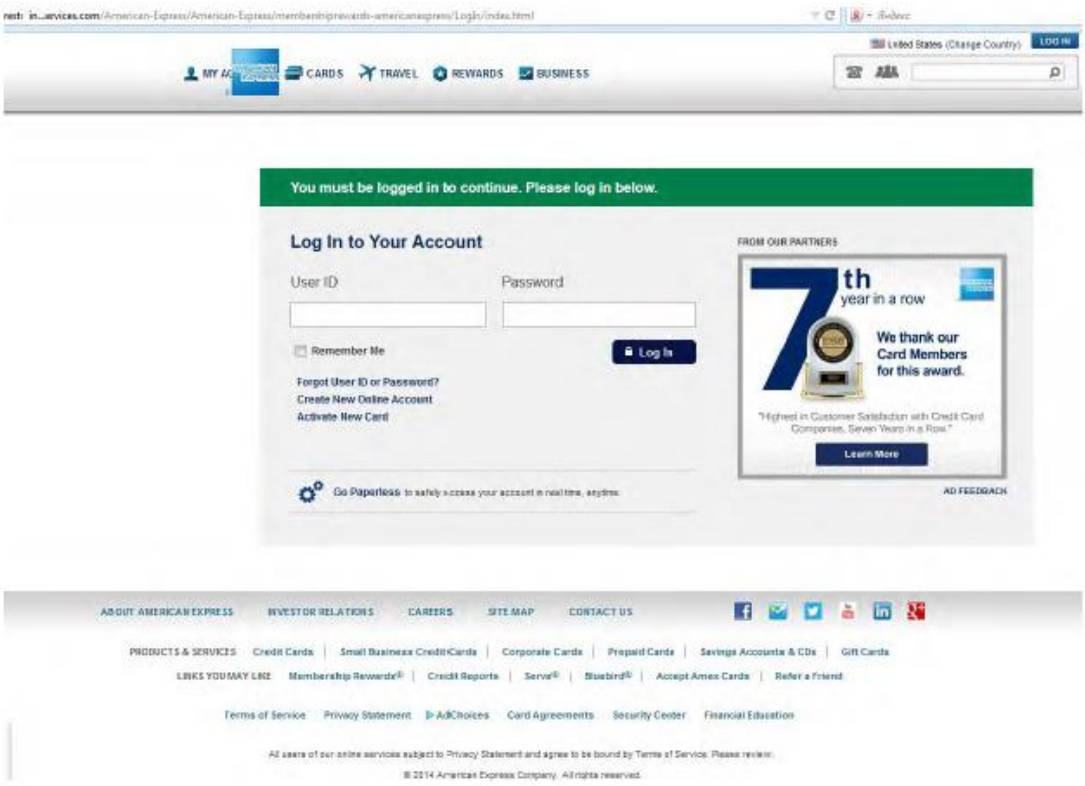

图 10：假冒运通支付表格示例

有时候，罪犯会伪造网上商店，目的是收集受害者的信用卡数据。

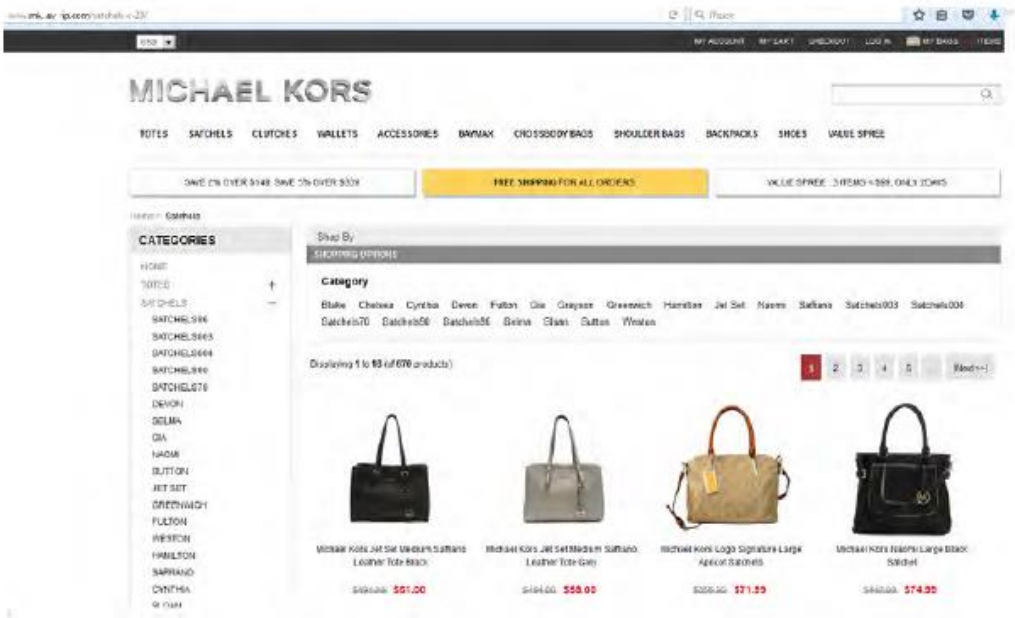

图 11：完全假冒网店示例

罪犯以极低的价格售卖名牌商品吸引受害者。然后当受害者选择好喜欢的商品进行支付时，他们轻松的窃取其金融认证信息。

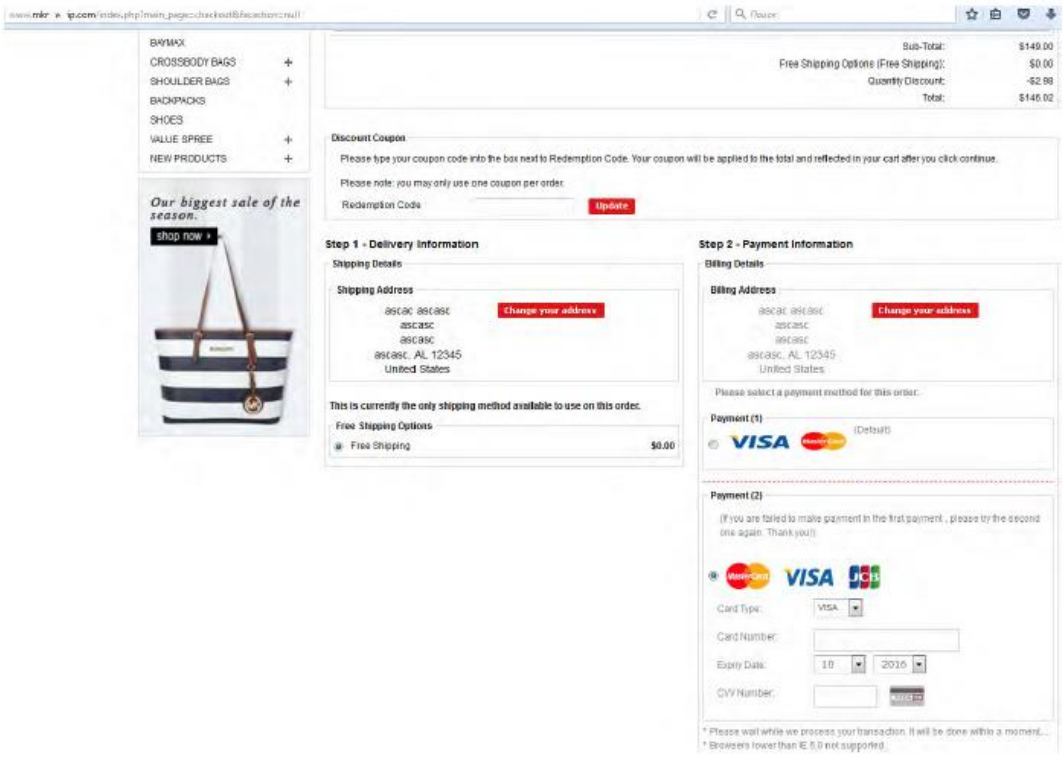

图 12：完全假冒网店示例（支付页面）

罪犯利用销售火爆期钓鱼的另一种方式是创建貌似合法的网站，他们销售能够在合法网上商店抵现的礼品卡和优惠券，但是是假的。其唯一目的是收集银行卡的认证信息。下面展示了此类网站的图例。

图 13：假店销售假券

当然，罪犯也会利用黑色星期五本身的品牌，并在之前就已做好了准备。当卡巴斯基实验室研究人员准备本概述时恰好发现了一些假的网站以黑色星期五的名义放出消息就奢侈商品进行折扣处理。

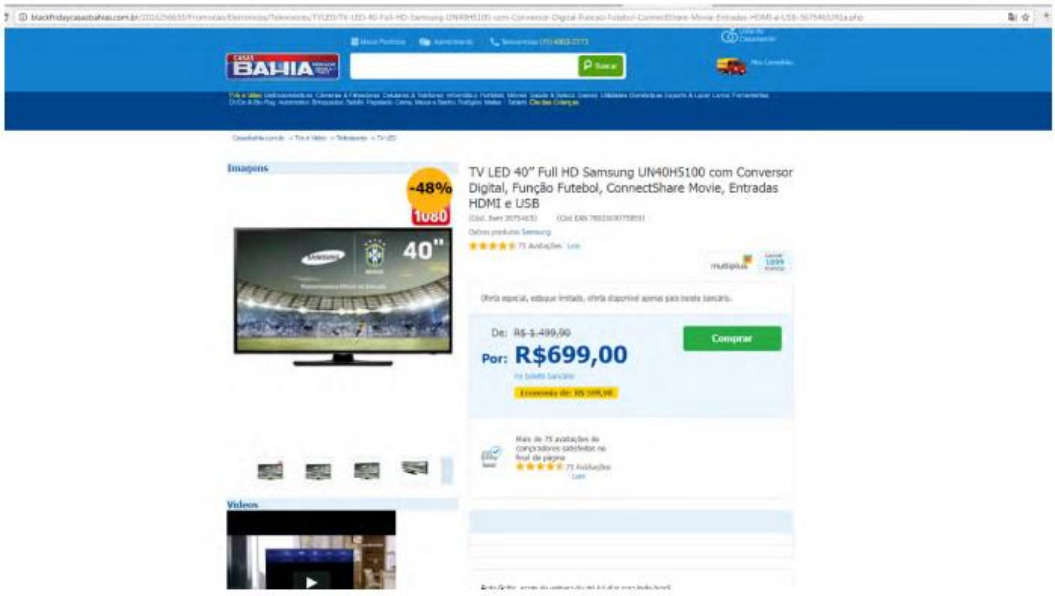

图 14：以黑色星期五为主题的假店

卡巴斯基实验室安全专家预计，去年出现的趋势将在 2016 年继续发生，因为网络钓鱼仍是罪犯窃取行用卡数据的主要来源，仍是设置诈骗方案最简便的方式。

金融恶意软件

数年来，银行木马是网络空间最危险的威胁。不像一般的间谍软件窃取各种认证信息，大多数情况下，它不太复杂。银行木马针对具体的网络银行用户和远程银行系统。罪犯倾向于投入大量资源开发此类软件，同时开发不同的复杂技术避免被反病毒产品检测到，并尽可能的高效传播恶意软件。最出名的银行恶意软件例子有：ZeuS，SpyEye，Carberp，Citadel，Emotet, Lurk 等。

去年，卡巴斯基的专家准备了两份报告，报道 2013 和 2014 年全球金融恶意软件态势。但自那以后，发生了很多事，首先遭到银行恶意软件攻击的用户数量已开始下降。这很可能是由于罪犯已把他们大部分的注意力从银行客户转移到银行本身，因针对银行进行复杂的攻击比针对普通用户利润更可观。另一个原因是加密勒索软件的兴起，被证实是相对有效获取非法钱财的有效方式。而未变的是罪犯大部分的注意力仍在高销售季。

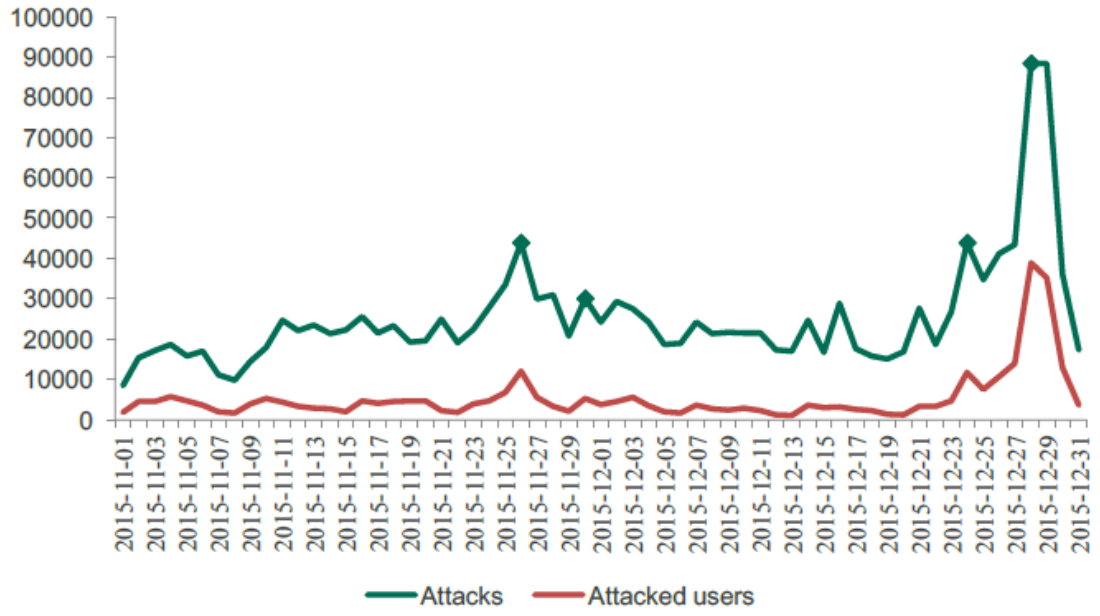

图 15：攻击次数和被攻击用户的数量变化（2015 年 11 月-12 月）

根据卡巴斯基实验室的遥感技术，2015 年节假日期间，共有 261,000 用户遭到恶意软件攻击，比一年前同时期的 307,600 用户相比大大减少。然而，2015 年明显表明罪犯对黑色星期五，网购星期一和圣诞节很感兴趣。10 月份，遭受攻击的用户为 61,674，11 月份为 81,038，12 月份为 154,324。一年前，即 2014 年，有 101,300 用户 10 月份遭受攻击，11 月份 16400，12 月份达到 102,900。

模式很明显。

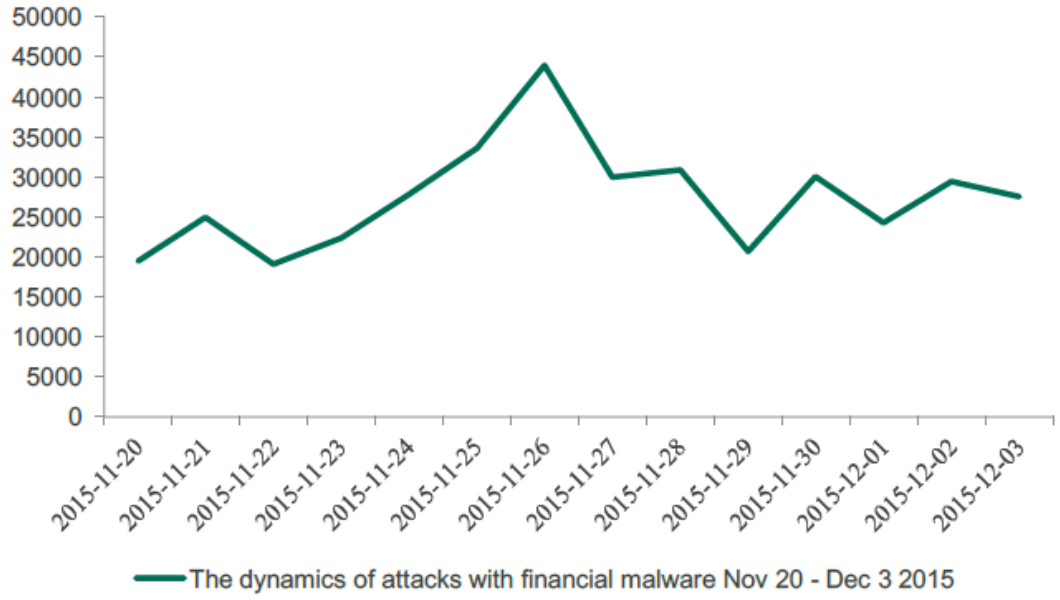

图 16：金融恶意软件的动态（2015 年 11 月 20 日-12 月 3 日，即黑色星期五到网购星期一）

如上图可见，遭到攻击的用户从 11 月 22 号开始增长，11 月 26 达到顶峰，恰好是 2015 年黑色星期五前一天。下一个高峰是 11 月 30 日，是该年网购星期一。我们注意到这两个高峰是该时期开始后遭受攻击的高峰期。

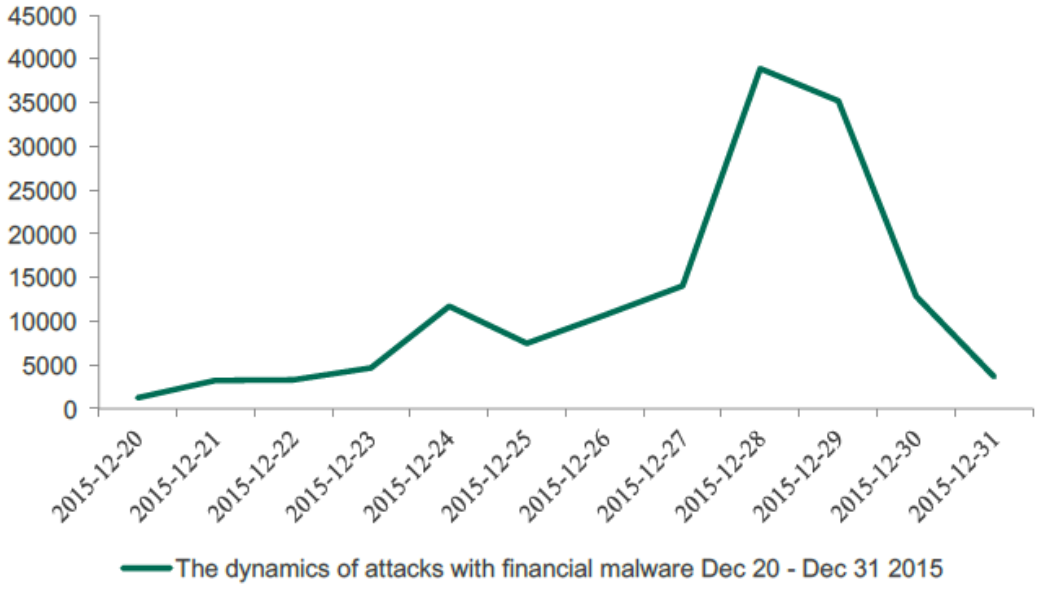

图 17：金融恶意软件的动态（2015 年圣诞）

攻击数量和被攻击用户下一次增长发生在 12 月 24 日，恰好圣诞节前夕，紧接着检测到除夕前 28,29 号为期两天的大高峰。

2014 年，节假季攻击高峰不那么明显，但清楚表明黑色星期五受到特别关注：11 月 24 日攻击开始明显上升，11 月 27 日达到峰值，也是黑色星期五的前一天。之后，另一个峰值出现在 12 月 1 日，网购星期一当天。

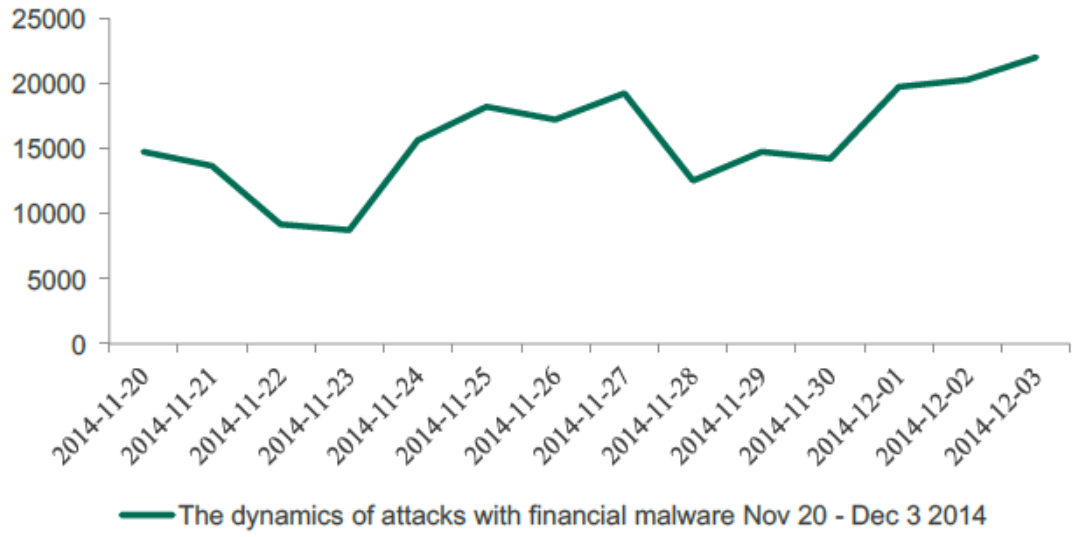

图 18：金融恶意软件的动态（2014 年 11 月 20 日-12 月 3 日，即黑色星期五到网购星期一）

2014 年圣诞节也表明了节假日和攻击之间的关联：12 月 24 日和 12 月 28 日是攻击峰值。

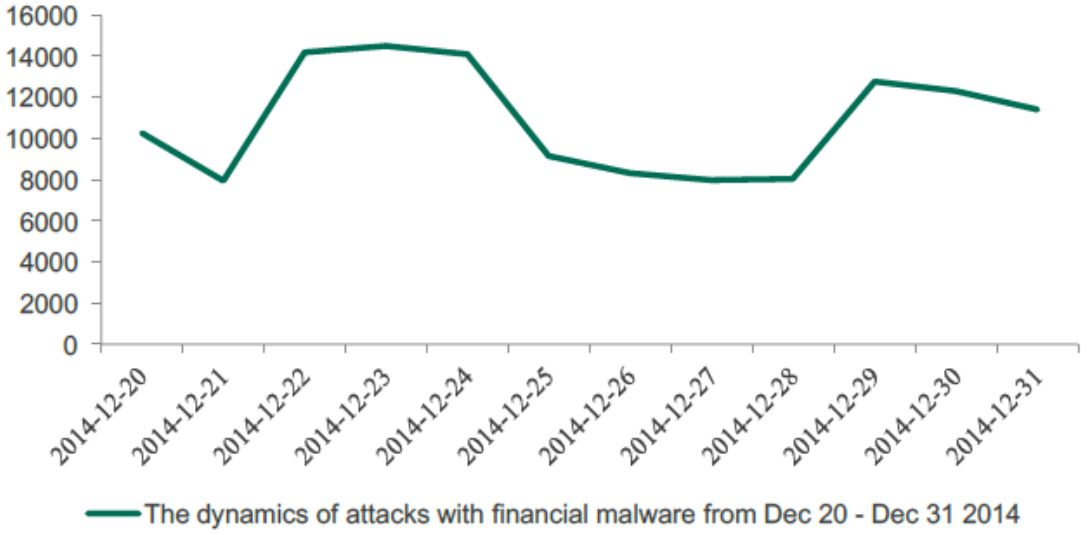

图 19：金融恶意软件的动态（2014 年圣诞）

同样，移动设备恶意软件攻击峰值几乎在同一时期。下图中检测到的攻击是由一些恶意软件发动的：Faketoken，Svpeng 和 Acecard。这四个是安卓移动银行的主要威胁。明显，背后的罪犯利用节假日活跃的传播恶意程序，2014 年尤其明显：

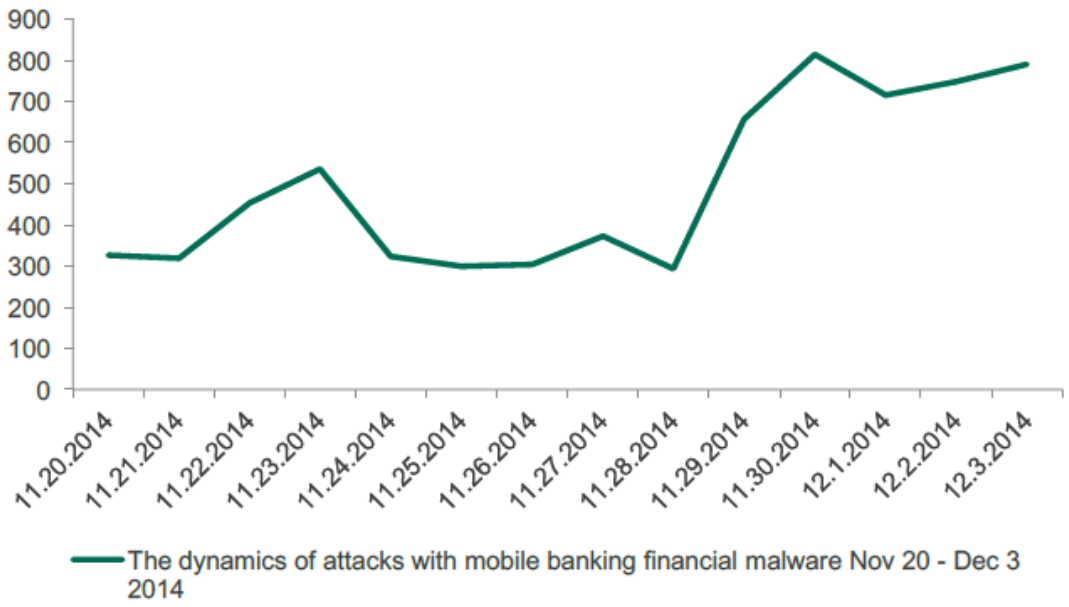

图 20：金融恶意软件的动态（2014 年黑色星期五到网购星期一）

就攻击检测到的次数而言，2015 年很平静，但仍有攻击峰值。

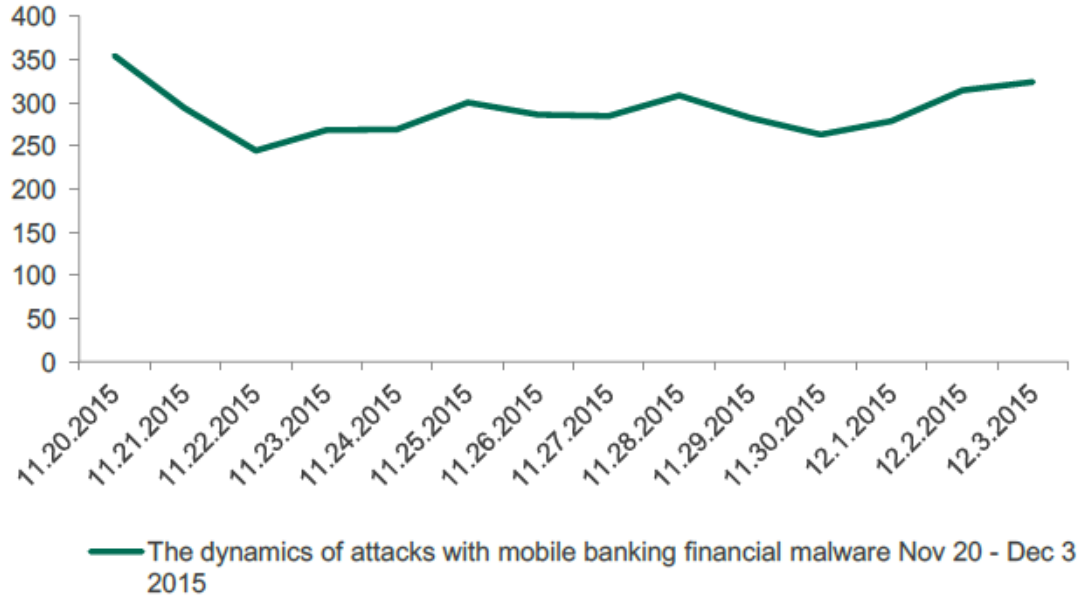

图 21：金融恶意软件的动态（2015 年黑色星期五到网购星期一）

销售点恶意软件

我们发现了的另一种危险的恶意软件，预计在本季会碰到是销售点恶意软件。这种金融恶意软件感染销售终端操作系统，然后窃取这些设备的信用卡认证信息。到目前为止，由于这种设备的特殊特质，这类恶意软件倾向于攻击，但目前我们还未掌握节日期间相关的检测数据。

通过计算近年来专家添加的恶意软件家族数，我们可以估计威胁形势。2013 年只添加了 4 个家族到收集的恶意软件家族目录，但 2013 年针对目标入侵激励了许多罪犯企图复制那些入侵著名零售商的“成功”事件，2014 年超过 12 个销售恶意软件也添加进去了。就销售点恶意软件来说，2015 年是最热闹的一年，添加了 14 个新的恶意软件家族。但 2016 年到目前为止相对平静：从年前开始，有 6 个新的家族添加到我们的目录中。但总共至少有 36 款恶意软件家族能够从销售点终端窃取数据。其数量甚至比用户恶意家族更大，其中 30 多种恶意家族现在收集在卡巴斯基实验室目录中。

预估新的攻击

攻击背后的动机显然与具体的日期相关 :网络罪犯暗示用户在节假日使用网络金融账户比任何一天的概率都要高。因此，罪犯倾向于加倍努力提高窃钱的几率。从 2014 和 2015 年“假日”动态攻击判断，卡巴斯基实验室预计 2016 年情形可能再现。

地下市场的消息

当网络消费者为即将来临的销售季制定购物愿望单时，零售商正在为大量的访客装饰商店，金融设施所有者（银行和支付系统）在为巨额交易做准备，同时罪犯也在为销售季做准备。为了发布这份报告，卡巴斯基实验室专家就几起秘密发生、只有邀请码才能参加的秘密论坛的事件和讨论进行了调查，该论坛上的用户声称该论坛涉及各种金融诈骗倾向于收集和讨论。

网购星期一的更多信息

基于调查结果，我们得出结论，至少东欧论坛上的罪犯，对网购星期一更感兴趣与黑色星期五相比。这可能是因为网购星期一更多是关于网络销售。网上有很多特接处理的广告，这对他们来说更容易把网络钓鱼诈骗隐藏在合法的特价中。

同样从物流角度看，网购星期一比黑色星期五更便捷，因为黑色星期五更多是线下销售。罪犯不必通过物理方式接触 ATMs 以便随后安装和收集扫描信息。而是，他们可以利用网络钓鱼或恶意攻击收集认证信息然后通过多种方式套现。

那就是说， ATM 扫描攻击将发生于黑色星期五期间，并将持续到其它的节日：例如圣诞节和新年。

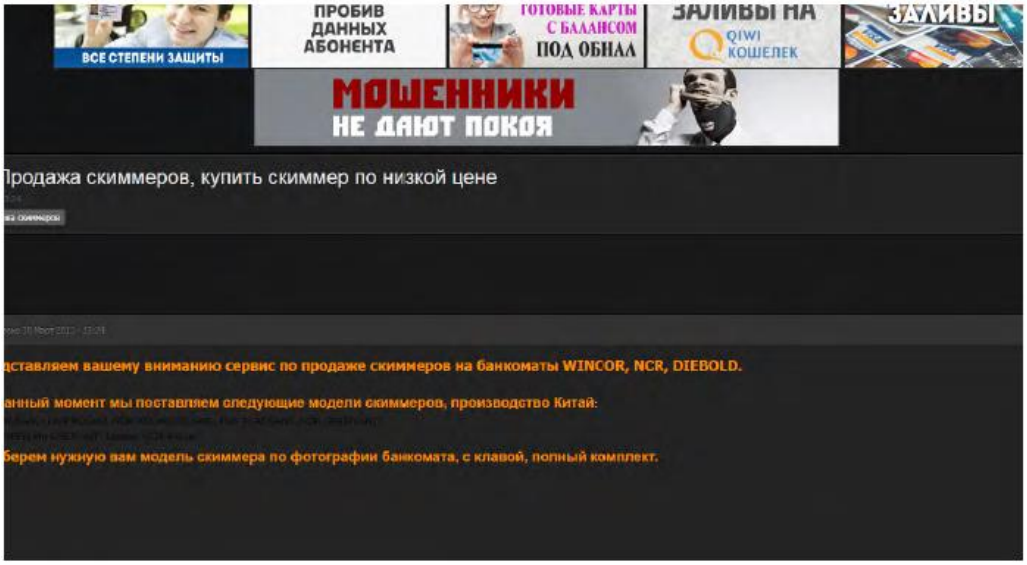

图 21：黑客论坛上的读卡器广告

基于去年信息，2015 年期间超过 500 多个读卡器在东欧黑市售卖，而一般的情况下每月销售 25-30 台设备。这些设备装有所有能够成功窃取数据的东西，像假的 PIN-输入板，隐藏的摄像头等。绝大多数读卡器（大约 96.5%）模仿四款流行供应商的产品，剩下的 3.5% 的读卡器复制自定义模式。

2015 年假日诈骗活动结果表明，罪犯在提取入侵信用卡现金时遇到了一些问题。基于相应网页资源对话，套现项目（为其它罪犯套现的团体）严重过载以致于套现订单需花费三个月才能处理完。这是由于大量的盗窃认证信息等待套现。根据卡巴斯基实验室数据，2015 年 12 月期间，网络罪犯大约能够收集 10 倍于的认证信息相比非节假日期间。基本上等于节假日之外的所有信用卡总的信息量。

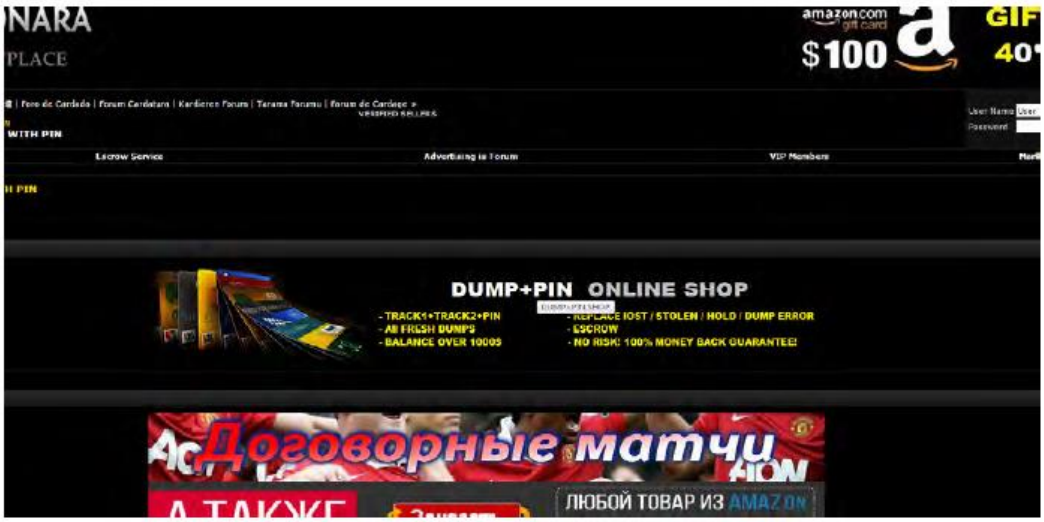

图 23：销售被盗信用卡凭证的商店

一些论坛信息表明，2016 年在黑色星期五一个月前，读卡器供应商已出现销售增加的现象，同时银行卡供应商随后也将用于复制盗窃的信用卡。同时，一些供应商提供新一代的销售点扫描机安装在合法的销售点设备上。与之前的读卡器不同，新一代的读卡器安装在读卡器内部，用肉眼更加难以发现。

另一种有趣的趋势是，许多罪犯避免以恶意软件进行诈骗活动，而是选择网络钓鱼攻击因为他们认为网络钓鱼攻击更加有效、安全。而且，他们积极利用能够直接与受害者联系的方法获取钱财。在这些攻击中，诈骗者会冒充银行给受害者打电话，并试图利用心里技巧获取信用卡认证信息。

卡巴斯基实验室专家预计今年假日季会有更多的通过苹果支付和三星支付系统诈骗的案子发生。最近新增国家支持的系统鼓舞了一些罪犯团体。绑定苹果 ID 的卡能够用于支付真实商品，给犯罪分子套现带来了便利。而那些专注于通过从网上和实体店购买商品进行套现的罪犯也会套现虚拟卡，他们通过虚拟商品套现窃取的认证信息。

在研究地下网络罪犯时，卡巴斯基实验室研究人员得出了另一个有趣的结论，诈骗犯认为能从假日季攫取巨额利润，特别是圣诞节前后到新年这段时间，这段时间内不仅有大量的买家想办法花钱，同时因为（基于分享在论坛上的经验）该时期银行反诈骗部分力度减弱。因为很多员工节假日要去度假，银行人员闲散，从理论上看罪犯更容易在合法的网页下隐藏进行诈骗操作。

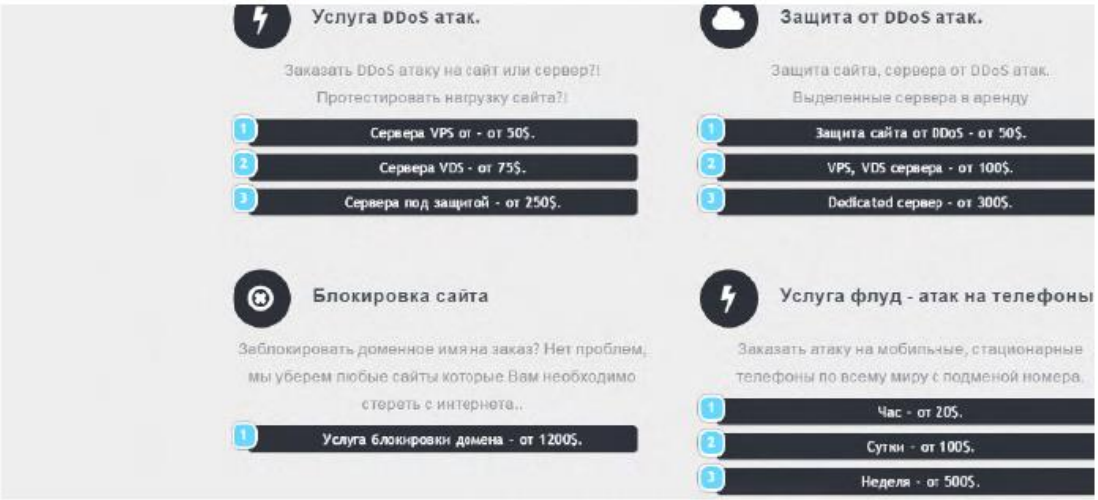

图 24：提供 DDoS 攻击服务的网站

其它类型的犯罪团体，例如那些专注于 DDOS 攻击的，很可能试图以勒索意图攻击线上商店。这是他们用来针对中小型零售机构攻击的著名策略。通过设定 DDOS 攻击，拦截被攻击店铺的访问直到店主支付赎金，否则继续拦截。因不愿无法访问店铺损失钱的店主通常会支付赎金。而这很可能发生在即将来临的假日季。

结论与建议

本报告的主要目的在于提高应对风险的意识，它可能毁了线上普通用户、消费者和店主和金融设施所有者店铺的即将来临的假日季。卡巴斯基实验室遥测和发生在地下的对话分析表明网络罪犯将对即将来临的高销售季特别关注。但这并不意味着假日注定已经毁了。

如果准备周全，该进程中的任何合法一方：买家、卖家和金融服务供应商最终都会获利。他们只要遵循以下简单的建议。

普通用户

- 不要点击任何社交网站朋友或经邮件发自陌生人或可疑的链接。很可能是恶意链接用于下载恶意软件到设备上转到网络钓鱼网页，获取用户认证。
- 不要下载、打开或在设备上存储不熟悉的文件，很可能是恶意软件。
- 不要使用不信任的无线网络进行网上支付，因为热点很容易入侵用于窃听用户流量盗窃机密信息。
- 不要在陌生或可疑网址输入信用卡信息避免落入网络罪犯之手。
- 切记在输入认证信息或机密信息之前仔细检查网页是否为真（至少瞄一眼 URL）。假冒网站可能与真的很相似。
- 只使用运行安全连接的网站（网站地址应以 HTTPS://开头而不是 HTTP://）阻止盗窃信息传输。
- 不要告诉任何人你以前的密码或 pin 码，以及银行代表。网络罪犯可能利用该数据窃取钱财。
- 在设备上安装内置技术安全解决方案旨在预防金融诈骗。例如，卡巴斯基实验室安全资金技术解决方案为金融交易创立全方位安全支付环境。
- 使用移动设备进行金融交易时不要忘记安装安全解决方案，因为网络罪犯和骗子也会攻击移动设备。

零售商

- 把电商平台更新到最新版本。每一次更新可能包含使系统更安全的补丁。
- 注意个人注册信息。诈骗犯倾向于隐藏身份，但毫无新意的账户可能暗示是骗局。约翰·史密斯的邮件地址显示为 21192fjdj@xmail.com 可能是罪犯。如果需要请核查、查询更过关于顾客的个人信息。添加验证码可能是有效的应对措施。
- 限制交易的数额。罪犯通常购买时多次输入正确的卡号。使用验证码和增加再次输入卡号的间隔时间。
- 使用双重验证(Visa 验证 ,主卡安全码等)会极大的降低银行卡非法使用的案例。
- 谨慎处理可疑订单。一些不相关的超过 500 美元的高额物品或需额外支付快运到另一个国家可能罪犯急于尽快脱手。这种情况建议电话联系客户确认订单。
- 使用定制的安全解决方案保护销售点终端远离恶意软件攻击 ,确保销售点终端运行最新版软件。
- 罪犯可能企图 DDOS 店铺网站勒索赎金。确保 IT 安全团队准备此类攻击，如果没有询问主机提供商是否可能购买 DDOS 防护服务。
- 对客户就可能在线上和线下遇到的网络威胁进行培训。

金融机构

- 引进带有特别部分安装在 ATM 和互联网银行安全的全企业防诈骗策略。随着攻击变得越来越复杂，ATM 逻辑安全，物理安全和制定防诈骗措施应全部解决。
- 每年组织安全审查和渗入测试。最好让专业人士检测漏洞而不是坐等被网络罪犯发现。

- 针对诈骗选择多层加密方法和技术 ,同时培训员工借助专业的防诈骗解决方案发现可疑交易。基于革新技术的金融安全软件可以帮助检测并与超出人控范围的诈骗活动作斗争。
- 不要让客户独立自卫。要培训所有的顾客几乎是不可能的。最好是创立多层安全架构给各级安全提供所有必要的服务。
- 谨记内部人员或多或少与网络安全事件有关。使用安全方法允许检测内部架构中可疑和潜在的危险活动。
- 确保假日期反诈骗部门人员齐备。