



不为人知的 数字经济

被盗数字信息市场

目录

此报告的研究及编写人员：

Charles McFarland

François Paget

Raj Samani

简介	3
显而不易见	4
财务数据	5
登录访问权限	10
在线服务访问权限	12
身份信息	15
结束语	18



简介

我们将重点介绍数据泄露受害者态度漠然的原因，最后介绍这些数据所有人遭遇信息泄露后可能付出的极大代价。

数据就像数字经济中的“油脂”一样。个人数据商业市场正在高速发展，而包含大量订购用户信息的数据库显著提升了其所属公司的价值（即使许多公司尚未盈利）。随着个人数据商业价值的增长，网络犯罪分子长期以来将窃取的数据贩卖给他人而牟取经济利益，买家通过计算机浏览器和数字支付方式进行交易。

在 2013 年的 McAfee Labs 报告 [Cybercrime Exposed: Cybercrime-as-a-Service](#)（网络犯罪曝光：网络犯罪即服务）中，我们介绍了网络犯罪分子如何利用现今的工具、产品和服务谋取利益的事实（不管他们的技术能力如何）。我们随后撰述了 [Digital Laundry: An analysis of online currencies, and their use in cybercrime](#)（数字洗钱：在线货币及其在网络犯罪中的应用分析）这一份报告，详细介绍了虚拟货币以及如何使用虚拟货币将窃取的数据转化为现金收益。在 2013 年发表数字洗钱时，相关机构[对 Silk Road 采取了法律强制手段](#)，因此公众知悉了可以轻松地在在线购买非法产品。这些犯罪行为力证了传统犯罪是如何借助网络世界发展变化的。

网络犯罪曝光和数字洗钱重点介绍了有助于攻击的工具。本报告将尝试解答以下问题：成功造成数据泄露后会怎样？

在 Target 数据泄露事件发生后，我与同伴共同撰写了一篇博客，介绍了销售被盗信用卡的跟踪情况，结果表明，就像传统经济一样，被盗信用卡的价格随着市场上新盗卡的大量涌入而下跌。Target 数据泄露案例只是冰山一角。本报告将更加深入地介绍这种不为人知的数据经济。

—Raj Samani, Intel Security 欧洲、中东和非洲地区首席技术官

Twitter@Raj_Samani
Twitter@McAfee_Labs



显而不易见

本报告的标题表明，恶意产品地下市场的隐藏之门是我们这些局外人所找不到的。实际上，这种市场并没有我们想象地那么隐秘，根本不需要事先去打探小道消息。[网络犯罪曝光：网络犯罪即服务](#)重点介绍了浏览器用户轻而易举地就找到了这些产品、工具和服务。在此我们不想重复介绍前期报告的结果，该报告毕竟是两年前编写的，现在已经过时。

有何改变？这种地下市场已发展到囊括几乎一切能想到的网络犯罪产品的局面，这些产品既可以出售也可以出租。我们正确地预见了一种“即服务”模式的兴起成为网络犯罪发展壮大的重要驱动因素。最新发表的 [McAfee Labs 威胁报告：2015 年 5 月](#)借助勒索软件 CTB-Locker 的兴起力证了这一点。CTB-Locker 的作者制定了一个联盟计划作为其业务策略的一部分：盟友使用其僵尸网络向潜在受害者发送垃圾邮件；对于受害者有支付赎金的每一次成功感染，盟友都会获得一定比例的款项。

所有攻击组成部分（研究、网络犯罪工具和基础设施）之间的“即服务”经济不断增长，具体而言“黑客即服务”经济在提供窃取数据方面起着最重要的作用。我们将重点介绍数据泄露受害者态度漠然的原因，最后介绍这些数据所有人遭遇信息泄露后可能付出的极大代价。

数据泄露相关阅读材料的负面效应是导致读者产生“数据泄露疲劳”概念，即“漠然”。近期文章 [《I Feel Nothing: The Home Depot Hack and Data Breach Fatigue》](#)（无动于衷：Home Depot 黑客入侵和数据泄露疲劳）对这种疲劳效应提供了一个极好的例子：

“如果有人滥用我们的信用卡，银行会负责处理整个事件，我们只需申领新卡（虽然麻烦，但不会改变生活），对这类黑客入侵新闻，我们除了耸耸肩膀也无可奈何，”作者这样写道。

在一系列语气平和的数据泄露通知和案例详述数百万记录被盗时，虽然失望是可以理解的，但重要的是要意识到这些数据是与我们息息相关的数据。我们的信息被公然贩卖，在一段时间内毫无任何个人反响。

这就是为什么我们要发表本报告的原因：我们要克服漠然感。我们不是想散布恐慌情绪，而是想要说明我们作为一个社会人员为什么应在收到数据泄露通知时加以重视，因为我们需要考虑前瞻性措施，以此降低成为受害者的可能性。

最后要说的是：我们不知道此报告中的一些示例是可信的，还是像卖方所说的那样完全是品牌效应。实际上，此类知名品牌的良好声誉通常会沦为窃贼宣传这种在线欺诈的基础。

财务数据

贩卖窃取的财务数据是一个相对宽泛的话题，并且许多销售和市场数据类型在通过标准浏览器访问的可见网络和通过其他方式访问方式访问的“黑市网络”之间有所不同。

涉及窃取财务数据（特别是支付卡信息）的数据泄露会继续成为关注的焦点。特别是会影响零售商，窃取的此类信息总是会导致相关数据出现在可见网络上。这些市场中提供的支付卡信息的价格根据大量选项的不同有所不同。下表显示了这些选项的快照。

前述类别与随同支付卡号一起提供的信息有关：

- “CVV”是卡验证值的业界首字母缩略词。CVV1是卡磁条上编码的唯一三位数值。CVV2是卡背面打印的三位数值。
- “软件生成值”是主帐号 (PAN)、到期日和软件生成的 CVV2 号的有效组合值。卖方将有效的数值组合称为“随机”值。有效的信用卡号生成器可以购买，也可以在线免费查找。
- “Fullzinfo”表示卖方提供有关卡及其所有者的所有详细信息，例如全名、帐单邮寄地址、支付卡号、到期日、PIN 码、社会保险号码、母亲的姓氏、出生日期和 CVV2。

有时，还会提供附加信息进行贩卖。包含“with COB”的支付卡数据提供的是这些卡以及关联的登录名和密码信息。使用这些凭据，买方可以更改送货地址或帐单邮寄地址，也可以添加新地址。

购买之后，某些卖方不能提供此数据。毕竟，卖方不提供窃取的信息，买方终归是投诉无门的吧？但是，如下图所示，许多卖方都会提供窃取的卡信息和所有关联的信息。

支付卡号和 CVV2	美国	英国	加拿大	澳大利亚	欧盟
软件生成值	5–8 美元	20–25 美元	20–25 美元	21–25 美元	25–30 美元
银行 ID 号	15 美元	25 美元	25 美元	25 美元	30 美元
出生日期	15 美元	30 美元	30 美元	30 美元	35 美元
Fullzinfo	30 美元	35 美元	40 美元	40 美元	45 美元

对于窃取的支付卡数据，每张卡（Visa、MasterCard、Amex、Discover）以美元为单位的估价。

资料来源：McAfee Labs

Freesh 2 CC from GERMANY

Name: [REDACTED]
 Adresse: [REDACTED]
 Stadt: 42119 Wuppertal (NRW)
 Telefon: 0202/[REDACTED]
 Geboren: [REDACTED]/1975
 Ausweisnummer: 300-[REDACTED]
 Ablaufdatum: [REDACTED]/2019
 Bank: Kreis[REDACTED] in Walsrode
 BLZ: 25[REDACTED]
 Kontonr: 62[REDACTED]
 IBAN: DE90[REDACTED]
 (Genauere Kontoinfos / BIC)
 CC: Mastercard
 No: 54[REDACTED]
 CVV: [REDACTED]
 Exp: 03/2018

支付卡数据和附加信息。

买方可选择许多选项，包括卡的地理来源和卡的可用余额。这两个选项都会影响卡的价格，就像下表显示的一样。

磁道转储和高额余额	价格
Track 1&2: PinATM 美国	110 美元
Track 1&2: PinATM 英国	160 美元
Track 1&2: PinATM 加拿大	180 美元
Track 1&2: PinATM 澳大利亚	170 美元
Track 1&2: PinATM 欧盟	190 美元

每张卡的磁道转储价格。

资料来源: McAfee Labs

转储一词是指以电子方式从信用卡和借记卡背面磁条中复制的信息。每张卡的磁条上均有两个数据磁道（Track 1 和 Track 2）。Track 1 是字母数字数据，包含客户的姓名和帐号。Track 2 是数字数据，包含帐号、到期日、CVV1 代码和随机机构数据。

列表价格根据供给、余额和有效性的不同有所不同。下图详述了其中某些要素。



We are offering top quality cards:

All our cards come with PINs and instructions. You can use them at any ATM worldwide.
Our cards are equiped with magnetic strip and chip.
Once you purchase, we will email you a Full Guide on how to safely cash out.

Us cards - available balance \$2,500(minimum) and up to \$5,000.
usage:
✓ ATM
✓ Stores
✓ Online

Eu cards - available balance 2,500 Euro(minimum) and up to 4,500 Euro.
usage:
✓ ATM
✓ Stores
✓ Online

American Express cards - available balance \$6,000 (minimum) and up to \$8,000.
usage:
✓ ATM
✓ Stores
✓ Online

Daily withdrawal limits (ATM limits)
US cards have a \$700-\$1000 daily withdrawal limit.
✓ no limit online or in stores

支付卡购买列表。

如前图所示，买方可做出多种选择。

贩卖支付卡数据是很常见的，[近期的迈克菲系列博客](#)对此有详细记载。但是，此类支付卡的财务数据并不是开放市场上针对的并随后贩卖的常见数据类型。就像卡一样，开放市场上还会贩卖在线支付服务帐户，其价格由更多的要素决定。但与支付卡相比，此类要素的限制相当多，并且余额是影响价格的唯一定义要素，如下表所示。

在线支付服务帐户余额	每个帐户的估价
400–1000 美元	20–50 美元
1000–2500 美元	50–120 美元
2500–5000 美元	120–200 美元
5000–8000 美元	200–300 美元

贩卖的在线支付服务帐户。

资料来源：McAfee Labs

此表中的价格是估计价格。我们看到过许多服务贩卖价格超出这些价格范围的例子。

一切信息都有出售。在下图中，我们看到还有贩卖银行之间转帐信息，以及可用的银行登录凭据。

pnc bank login - \$22xx balance + info

Vendor smoothhydra (5) (3.6 ★)
Price ₱0.833 (\$190)
Ships from Worldwide
Escrow No



Product description

This is a listing for a pnc bank login account with around \$2200 in balance

贩卖的银行登录凭据示例。



登录访问权限

贩卖的其他数据类型包括组织受信任的网络内部的系统访问权限。进入系统的方式各不相同，有的很简单，可以直接访问（例如使用登录凭据），有的则需要具备一定的技术能力才能访问（比方说利用系统安全漏洞）。在下图中，我们可以看到允许潜在买方访问位于欧洲、亚洲和美国的银行和航空系统的漏洞货源。

DreamMarket Forum
DreamMarket user forum.

[Index](#) [User list](#) [Search](#) [Register](#) [Login](#)

You are not logged in.

[Index](#) » [Advertising and Promotions](#) » [Web Vulnerabilities in Banks and Airlines](#)

Pages: 1

2015-03-31 14:25:46

daflame
Member

Registered: 2015-03-31
Posts: 2

Offline

selling a package of 30 vulnerabilities in different organizations, most of them banks and some airlines. on the package you can find major banks and they're in Europe, Asia, US.
I'll display name of the banks to the interested people only. The vulnerability gives access to the organizations databases, where you can explore/go deep if you wish to.

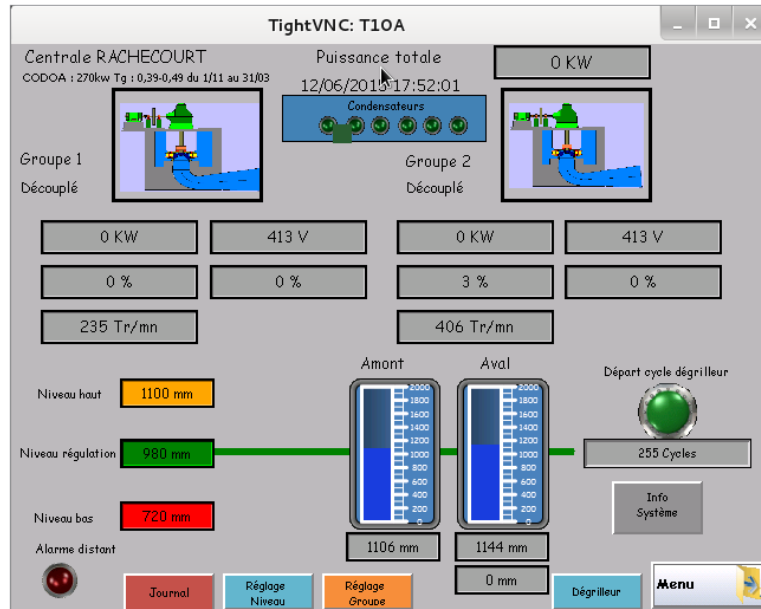
these are web vulnerabilities.

for people interested reply with your Jabber then we can start the negotiation.
I'll show proofs of banks db BEFORE any procedure.

贩卖的银行和航空系统访问权限示例。

与贩卖财务数据一样，卖方竭力为出价合适的潜在买方提供一定程度的印样。

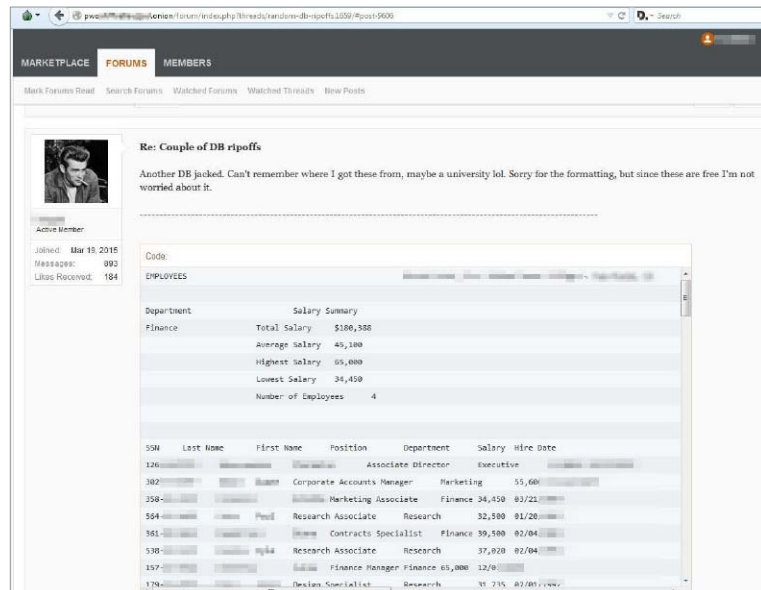
网络犯罪专家 Idan Aharoni 的近期研究表明，目前贩卖访问权限的系统犯罪类型包括关键基础设施系统。在 Aharoni 的《[SCADA Systems Offered for Sale in the Underground Economy](#)》（以地下经济方式贩卖 SCADA 系统）一文中，介绍了一个例子：卖方提供了一个看似法国水力发电机的截屏，可证明他们有访问权限。



一家卖方声称，这是一个法国水力发电机的截屏，可证明他们有关键基础设施 SCADA 系统的访问权限。

与之前的示例一样，买方会质疑提供的访问权限是否真实有效。生成截屏并暗示此截屏代表有访问权限并不是特别难；但此消息确实意味着一个令人担心的趋势（正如 Aharoni 指出的一样）。

此外，还有贩卖窃取的企业数据。在下图中，我们看到卖方在出售从某大学窃取的数据。



贩卖从某大学窃取的信息的示例。

在线服务访问权限

许多人订购了数字服务，包括音乐、视频、忠诚度计划等等。由于此类帐户相对便宜，人们可能会觉得这些帐户的信息不会提供足够的回报。但不管此类经济是什么，多个市场中都分布有此类帐户的货源，这表明潜在客户有这种需求。

当窃取的在线帐户受到危害时，肯定会影响到合法所有者多方面的利益。帐户会因买方的恶意活动（有时会发生数周的支持电话费用）被控制或关闭。受害者还可能会因买方使用存储的信用卡信息购物而遭遇经济损失，也可能会失去免费福利（例如在帐户使用期间收集的忠诚积分）的访问权限。更糟糕的是，还存在导致令人不安的情况。

下图显示了一个贩卖在线服务帐户的示例。



贩卖在线视频流帐户的示例。

在线视频流用户是唯一的受害者？几乎没有。令人沮丧的现实是，几乎每个可以想到的在线服务的访问权限都有货源。我们发现另一个在线视频流服务帐户的售价是 0.55 美元。单个数字服务帐户的售价不到一美元，犯罪分子必须迁移大量在线帐户才值得投入。

★ SkypeMan's █████ Accounts ★ Highly Resellable ★ BRAND NEW! ★ 1\$ ★



Seller	skypeman (4.89% - 287)
Price	0.55 USD
FE	Yes
Digital item	Yes
Currency	Bitcoin
Quantity	1

Buy It Now

另一个在线视频流服务帐户的售价不到 1 美元。

许多在线流媒体娱乐服务通常也会出售。我们发现电视流服务的 HBO NOW 和 HBO GO 帐户以及其他光纤电视流服务的帐户售价不到 10 美元。很明显，视频流服务的需求较高。即使是高级专业体育运动流服务，售价也不过是 15 美元。我们还发现有人贩卖其他在线帐户，包括高级版色情内容帐户的终身使用权，以及黑市网络市场 Agora 的免费推荐人链接。

HBO GO Account [LIFETIME + FREEBIES]



Seller	Drawkward (4.99% - 662)
Price	7.5 USD
FE	No
Shipping from	WW
Shipping to	WW
Currency	Bitcoin
Quantity	1

0 USD - Digital Delivery - through Nucleus private message - 8 c

Buy It Now

贩卖的 HBO GO 帐户访问权限示例。

Marvel-Unlimited [Lifetime Account]



Seller	AccountGuru (4.97% - 269)
Price	0.5 USD
FE	Yes
Digital item	Yes
Currency	Bitcoin
Quantity	1

Buy It Now

网络窃贼还廉价贩卖用于访问数字漫画的 Marvel Unlimited 帐户。



甚至免费的在线帐户也会引起犯罪分子的注意。下图显示了一个有 100000 分积分的酒店忠诚度帐户售价 20 美元。客户可合法免费打开这些帐户，但鉴于这些帐户有销路，导致其失去有时需要多年积累的累积福利。

100,000 **Account**



Seller	flappydloc (958,181)
Price	20 USD
FE	Yes
Digital item	Yes
Currency	Bitcoin
Quantity	1

Buy It Now

甚至有人贩卖酒店忠诚度计划。

购买窃取的在线帐户访问权限的一个动机是，因业务实践不佳或公开欺诈隐藏买方的信誉。希望获得新网上拍卖社区业务身份的买方只需付费即可，但建立一个历史记录良好的帐户却难能可贵。

No Limits Aged Unlimited Allowances 0 to 200
feedbacks Account/Business For Sale

£1,400.00

accounts with no limits and aged with unlimited selling
allowances. 0 to 200 feedbacks business account for sale.
This account is from 8 too 10 years old.

ADD TO CART

Add To Wishlist

Add To Compare

贩卖的一个网上拍卖社区帐户。

因迫切需求减少，在特定帐户类型范围内贩卖的网上拍卖社区帐户包数为 100。

ccPal Store

Products FAQs Register Login

ccPal Store - CCs, CVV2s, accounts

We get new lists every day!
80%+ working guarantee, we will replace if more than 20% dont work!

Product	Price	Quantity
100 accounts	100 USD = 0.340 €	1 X Buy now
100 accounts	100 USD = 0.340 €	1 X Buy now
100 CCs with CVV2	150 USD = 0.509 €	1 X Buy now

ccPal

信用卡销售位置，也可提供网上拍卖社区帐户的访问权限。

身份信息

贩卖受害者身份是最令人恐惧的类别，因为完全是针对个人的。

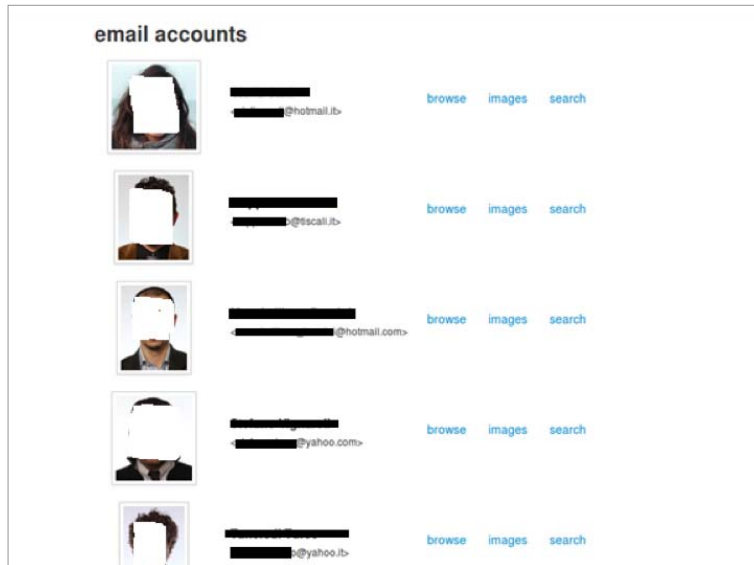
Intel Security [最近协同](#)欧洲的执法机构斩断了 Beebone 僵尸网络。此僵尸网络能够将恶意软件（包括 ZBot 银行密码窃取程序、Necurs 和 ZeroAccess Rootkit、Cutwail Spambot、虚假防病毒软件和勒索软件）下载到毫不设防的用户系统上。我们对用户不采取补救措施感到非常失望，特别是美国和欧洲境外的用户。[Raj Samani 的相关主题博客](#)中曾提到，绝大部分社会人员未能适当地保护其数据 - 通常会产生很大的影响。

在下图中，我们提供了一个个人数字身份被网络窃贼窃取的示例。潜在买方可以控制此人的数字生活（社交媒体、电子邮件等）。（我们已与英国的执法机构共享此信息。）

```
Username(s): [REDACTED]
Emails: [REDACTED]@hotmail.co.uk, [REDACTED]@gmail.com
First Name: [REDACTED]
Last Name: Bright
Gender: Male
Date of Birth: [REDACTED] 1995
Age: 19
Type(s): [REDACTED]
City: Norwich, Norfolk
Postal Code: [REDACTED]
State/Province: Norwich, Norfolk
Country: United Kingdom
Street: [REDACTED]
PlayStation Network: [REDACTED]
=====+ Accounts +=====
http://Twitter.com/[REDACTED]
http://Instagram.com/[REDACTED]
http://Twitch.tv/[REDACTED]
http://Youtube.com/user/[REDACTED]
http://Youtube.com/KzBom3rZz - [REDACTED]
http://Youtube.com/user/[REDACTED]
http://Facebook.com/[REDACTED]
http://Plus.Google.com/[REDACTED]
http://Plus.Google.com/[REDACTED]
http://SteamCommunity.com/profiles/[REDACTED]
http://ConsoleCrunch.org/index.php?members,[REDACTED]
http://NextGenUpdate.com/forums/member/[REDACTED]
http://XenForo.com/community/members/[REDACTED]
=====+ Family +=====
Mother: [REDACTED]
http://Facebook.com/[REDACTED]
Father: [REDACTED]
```

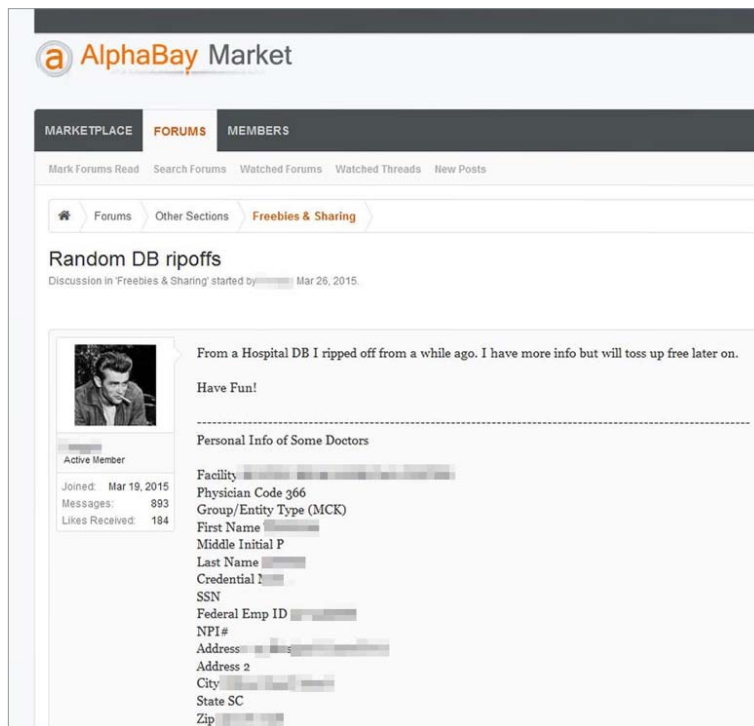
贩卖身份信息的示例。

对于前述示例，虽然信息丰富，但需要买方通读大量文字内容。某些卖方会提供一个图形丰富的界面来吸引潜在买方。以下示例可让买方按电子邮件帐户选择个人，这是控制受害者部分生活的第一步。



此服务可让买方轻松选择配置文件。

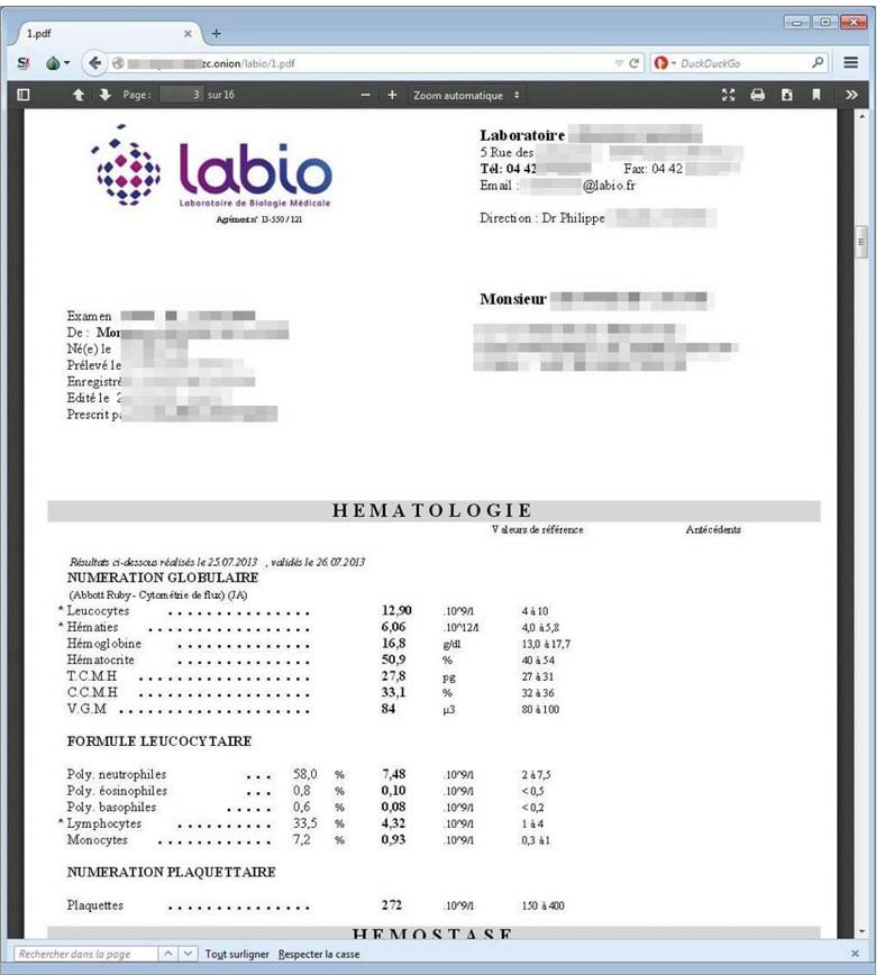
与窃取身份信息的市场密切相关的是，窃取医疗信息的市场。此类数据的购买与支付卡数据一样不易，但医疗信息的卖方是在线销售的。安全记者 Brian Krebs 在其 [《A Day in the Life of a Stolen Healthcare Record》](#)（窃取医疗保健记录生活的一天）一文中讨论过此问题，他提到“诈骗犯泄露了一个大文本文件，其中包含该国许多医师的姓名、地址、社会保险号码等敏感信息。”（请参阅下图。）



贩卖从医疗服务窃取的信息的示例。

资料来源：安全记者 Krebs。

虽然大部分报告重点介绍了贩卖窃取数据，但有时是免费公开共享窃取数据。在下图中，黑客集团 Rex Mundi 泄露了可识别的患者数据，因为 Labio 服务没有支付 20000 欧元赎金。



黑客泄露了客户私人信息，以此惩罚医药公司不支付赎金。

结束语

本报告中的隐藏的数据经济示例只是冰山一角。我们虽未提及许多其他类别和服务，但我们希望这些示例能让大家认清威胁。在本报告中，我们探讨了贩卖的窃取数据。网络犯罪分子还购买了发动攻击的产品。其中包括购买和租赁助长全球感染大量传播的漏洞利用工具包。拟定可用报价的目录是不可能的，因为该领域正在急速发展。

当我们了解数据泄露时，网络犯罪行业可能看似远离日常生活，人们很容易忽视此消息。但网络犯罪只是演变传统犯罪而已。我们必须克服漠然感，关注有关防范恶意软件和其他威胁的建议。否则，我们的数字生活信息可能会被转售给使用互联网连接的其他人。



关注 McAfee Labs



关于 McAfee Labs

McAfee Labs 是威胁研究、威胁情报和网络安全先进理念的全球领先来源之一。利用从跨主要威胁媒介（文件、Web、消息和网络）的数百万传感器获取的数据，McAfee Labs 可提供实时威胁情报、关键分析和专家意见，以便增强保护并降低风险。

www.mcafee.com/cn/mcafee-labs.aspx

关于英特尔安全

迈克菲现在是英特尔安全的一部分。英特尔安全凭借其 Security Connected 战略（创新型硬件增强安全解决方案和独特的 Global Threat Intelligence）致力于开发具有前瞻性且经实践验证的安全解决方案和服务，保护用作商业或个人目的的全球系统、网络和移动设备。Intel Security 将迈克菲的安全经验和专业知识与英特尔的创新和可靠性能相结合，使安全性成为每种体系结构以及每个计算平台的基本要素。Intel Security 的使命是让每位用户放心地在数字世界中安全可靠地工作生活。

www.intelsecurity.com

McAfee. Part of Intel Security.

北京市东城区北三环东路 36 号环球贸易中心 D 座 18 层 邮编: 100022 电话: (8610) 85722000 传真: (8610) 85752299
上海市延安西路 2299 号上海世贸商城 22 层 邮编: 200336 电话: (8621) 23080699 传真: (8621) 63406606
深圳市福田区金田路 4018 号安联大厦 27 层 B01 室 邮编: 518026 电话: (86755) 82825000 传真: (86755) 82825001
销售热线: 400 610 0369 或 800 810 0369 www.intelsecurity.com www.mcafee.com/cn



本文所含信息仅供参考，旨在为迈克菲用户提供便利。此处所含的信息如有变更，恕不另行通知。信息照原样提供，不对信息在任何特定环境或情况下的准确性或适用性提供任何担保或保证。

Intel 以及 Intel 和 McAfee 徽标是 Intel Corporation 或 McAfee, Inc. 在美国和/或其他国家或地区的商标。其他商标和品牌可能是其各自所有者的财产。Copyright © 2015 McAfee, Inc. 62122rpt_hidden-data_0915