McAfee
Together is power.

# 区块链威胁报告

区块链是去中心化在线交易的革命性基础，但有安全风险

# 目录







# 区块链使用者通常是最容易受攻击的目标 - 这是由于初创企业对安全的重视程度不如发展

此报告的研究及编写人员：

- Charles McFarland
- Tim Hux
- Eric Wuehler
- Sean Campbell

## 简介

2017 年年末，有关比特币加密货币的新闻纷纷占据各大媒体的头条。比特币的价值飙升至接近 2 万美元一个，因此引起了主要新闻机构的注意，吸引了准备在该领域投资的人们的目光。比特币是一种基于区块链的领先加密货币，这是一种革命性的新技术。区块链以去中心化的方式记录交易，已经开始改变我们看待金钱的方式，并提供了新途径来解决旧业务问题。

但是新技术存在新的安全问题。恶意用户已经使用社交工程、恶意软件和漏洞利用，将许多区块链实现作为目标。随着更多人群开始使用区块链并围绕它构建工具，他们必须了解安全风险。在本报告中，我们将看看当前的安全问题以及区块链实现中的特定事件。我们会介绍恶意用户用于攻击的技术、目标和恶意软件。

2009 年，区块链的首个实现“比特币”在技术人员和研究者当中掀起了热潮。看上去它是一个老难题的可行解决方案：如何在对等之间确保协议。区块链通过严格的研究实现了去中心化支付系统，其中对等可达成协议并信任账本，从而实现了这一目标，这代表着网络的当前状态。该协议实现了之前不可信的去中心化支付系统并提供了更多保障。

区块链具体是什么?区块链是一系列聚集在一个区块(定义账本的一部分)中的记录或交易。账本在对等之间分布,这些对等使用它作为可信机构(其中的记录是有效的)。账本中的每个区块都与其下一个区块链接,顾名思义,这就形成了链条。任何人都可以查看最新的区块及其"父"区块,从而确定地址的状态。对于加密货币,我们可以确定地址的值并跟踪使得每个相应币生成的每次交易。验证交易是关键。每个节点可单独验证每个链的准确性。

但是如果交易相加,那么每个节点如何了解链已经被修改?区块链技术的一个关键元素是如何将区块链接在一起。借助哈希功能,新的区块嵌入其父级区块的完整性信息。如果更改了自父级的信息,则哈希将会更改 - 中断验证过程。另外,在创建每个区块时,必须提供证据。该证据会表明扩展了某些资源来创建区块。

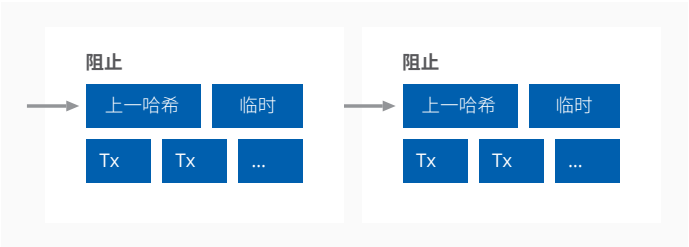


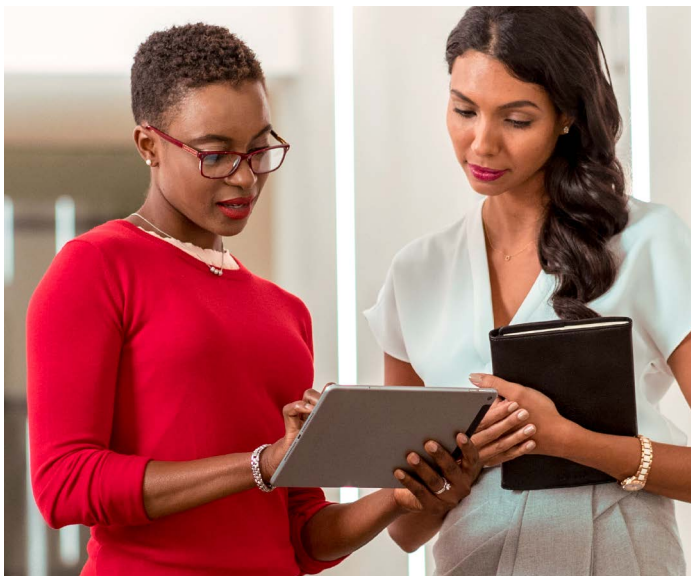

图 1:区块链工作量证明。 资料来源:https://bitcoin.org/bitcoin.pdf

每个区块的创建就称为挖矿,并且挖矿所需的证明对于每个区块链实现不同。最常见的是工作量证明,这是一种 CPU 密集型算法,需要求解问题的所有步骤。不存在已知的数学快捷途径。发现问题的正确解证明所有步骤均已完成,这种情况下使用的是 CPU 资源。发现答案需要许多工作,但是验证答案是否正确则相对简单。因为每个区块需要庞大的证明工作,并且后续区块链接在一起,可以验证需要最多工作的最长链,最长链也是最可信的链。攻击者要耗费大量资源才能创建更长的链并超过任何多数人的账本。将完整性检查和哈希函数以及工作量证明组合,可让人们的整个网络信任分布式账本中的记录。

加密货币是主要专注于货币值和交易的区块链实现。它们是区块链的最常见用途。但并不是说在区块链账本中只能记录金钱。比特币允许将少量额外的数据存储在交易中。研究者们已发现泄露的文档、任意数据,以及甚至是在比特币账本中存储和可检索的色情图文。一些账本设计为存储可由区块链的参与者执行的整个程序。以太币是第二流行的加密货币,以"智能合同"实现。该实现将代码或合同上传至账本。随后可由任何人执行该代码。执行合同的效果取决于创建者设定的规则。在简单的示例中,合同可建立记帐帐户来持有

资金，直至双方履行义务。如果有人想执行合同，则通过使用“gas”（矿工的一种支付形式）支付算力。gas 用以太币向所有智能合同指定成本，以防止会导致网络减速的过度执行。

一些行业希望用自定义区块链解决业务问题。例如，一家大型零售公司提交了专利，使用区块链来跟踪和保护发货。还开发了企业区块链平台来应对另外的实现的不断增长的需求。



## 区块链攻击

在大多数情况下，区块链技术的使用者是最容易受攻击的目标。由于初创企业的普遍心态是重发展，轻安全，而加密货币公司通常也属于这一类别。该类别包括大规模广泛采用区块链的那些加密货币，例如比特币和以太币。攻击者借助成熟的技术采用数种方式来以使用者和企业为目标。主要的攻击媒介包括：

- 网络钓鱼
- 恶意软件（例如：勒索软件、挖矿软件以及 Cryptojacking）
- 实现漏洞
- 技术

### 网络钓鱼

网络钓鱼诈骗是最为常见的区块链攻击，这是由于其普遍性和成功率。看看加密货币 Iota 案例。受害者在持续时间达数月的网络钓鱼诈骗中损失了 400 万美元。攻击者注册了 iotaseed[.]io，为 Iota 钱包提供有效的种子生成器。该服务按宣传的方式工作，可让受害者能够如预期成功创建和使用钱包，从而造成安全和可信的错觉。随后攻击者利用建立起来的信任耐心等待。攻击者用六个月时间收集日志，其中包括秘密种子，然后开始攻击。攻击者在一月份利用之前窃取的信息，将受害者钱包中的所有资金转移走。

网络犯罪分子一般不会在乎自己的网络钓鱼受害者是谁。只要加密货币落入了攻击者手中，所有受害者都成为合法攻击对象。Tor 中间人攻击就是这种情况。Tor 网络通常用于对进行窥探的第三方隐藏浏览者的位置。许多人采用 Tor 来创建隐藏的服务，通过这些服务，使用者可购买和出售商品。加密货币是首选或唯一的支付形式。这些服务也是勒索软件家族通常用来隐藏支付系统的地方。有些人不知道 Tor，因此，出于便利，提供了便于访问的 Tor 代理来帮助受害者访问这些站点和恢复文件。一般情况下，这些站点包括它们通过搜索引擎找到的或通过勒索软件指示被引导至其上的 Tor 代理域。对于受害者而言，不幸的是，攻击者可能无法收到受害者的赎金。在某些情况下，资金通过恶意代理被重定向至不相关的钱包。2018 年初就发生了这样的情况，当时发现了 Tor 代理服务，它用受其控制的地址替换了和勒索软件相关的比特币地址。安全研究者们发现，在 Tor-to-web 代理服务 onion[.]top 背后，操作者为比特币钱包搜索暗网上的站点。一旦定位钱包，网络窃贼就把地址更换为自己的地址。

## 恶意软件

在 2016 年，新的勒索软件家族在数量上呈爆炸式增长。它们是恶意用户获取加密货币使用的主要工具。勒索软件并非新鲜事物，但受到青睐主要是因为加密货币具有转移和隐藏资金的优势。网络犯罪分子还有便于访问的工具，特别是 HiddenTear，它本来是关于勒索软件的“培训”工具，但是很快就被恶意用户用来构建了数百个变体。这些变体通常需要支付比特币作为赎金，也有少数例外，例如 Kirk 勒索软件使用的门罗币。

在 2017 年，勒索软件开发人员扩大了关注范围。恶意用户开始用各种替代性电子货币进行试验，这些货币也称为替代币。门罗币是最受欢迎的替代币，而知名度更低的替代币（例如达世币）也引起了注意。勒索软件 GandCrab 放弃比特币，改为使用达世币。GandCrab 和各种恶意软件一起被添加到最为流行 RIG 利用套件中。GandCrab 和其他恶意软件通过恶意广告对 Microsoft Internet Explorer 和 Adobe Flash Player 发起频繁攻击。

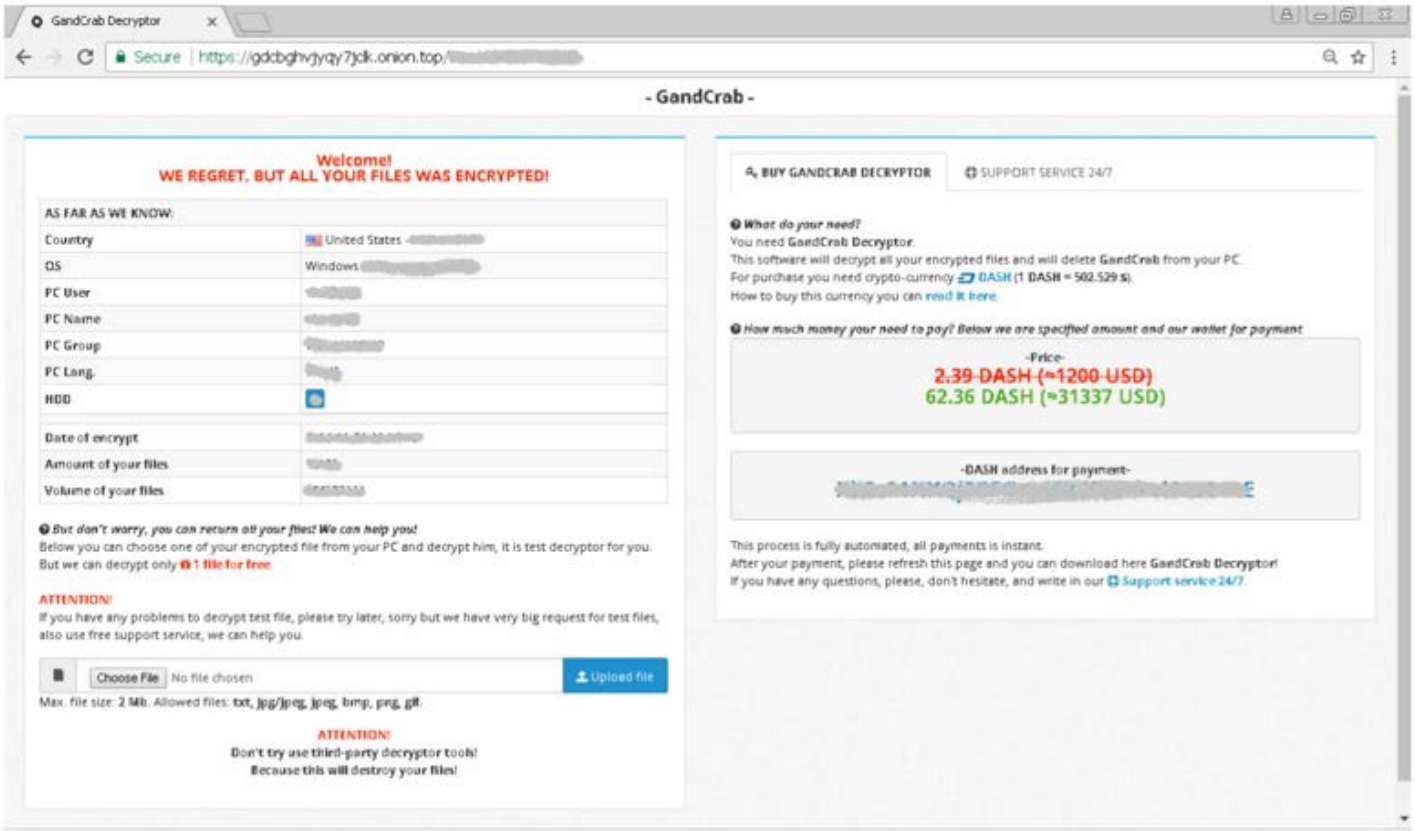



图 2：通过 onion[.]top Tor 代理访问 GandCrab 解密页面。

勒索软件开发人员还在 2018 年初采用主流的以太币。HC7 的变体 Planetary 是首个将以太币作为目标的已知勒索软件，但并非唯一。为了给受害者提供选项和更大的激励，Planetary 允许他们对每个受影响的系统支付相当于 700 美元的等价物，或者为受害者网络上所有受影响的节点支付 5 千美元的等价物。勒索软件还接受比特币和门罗币。

关注

共享

### Cryptojacking

Cryptojacking 是劫持浏览器来挖掘加密货币的方法，并且有令人吃惊的复苏迹象。与勒索软件很相似，Cryptojacking 活动中用替代币进行了试验。2017 年末，Chrome 浏览器的 Archive Poster 插件被发现在没有得到同意的情况下挖掘门罗币。受害者在有人开始抱怨高 CPU 使用率时发现了问题。这时已经下载了挖矿软件的人数超过 10 万。至少有四个版本的应用程序包括来自 Coinhive 的 Cryptojacking JavaScript 代码，它可以方便地将挖矿代码嵌入网站或工具中，最初是通过简单易用的开源 API。Cryptojacking 驻留在灰色区域中。许多组织实现 Coinhive 和其他挖矿软件来将访客的设备资源用于牟利。如果他们同意，则不会认为挖矿是恶意行为，尽管可能认为是不需要的行为。但是许多站点不会披露挖矿，让访客不知道为什么性能下降。

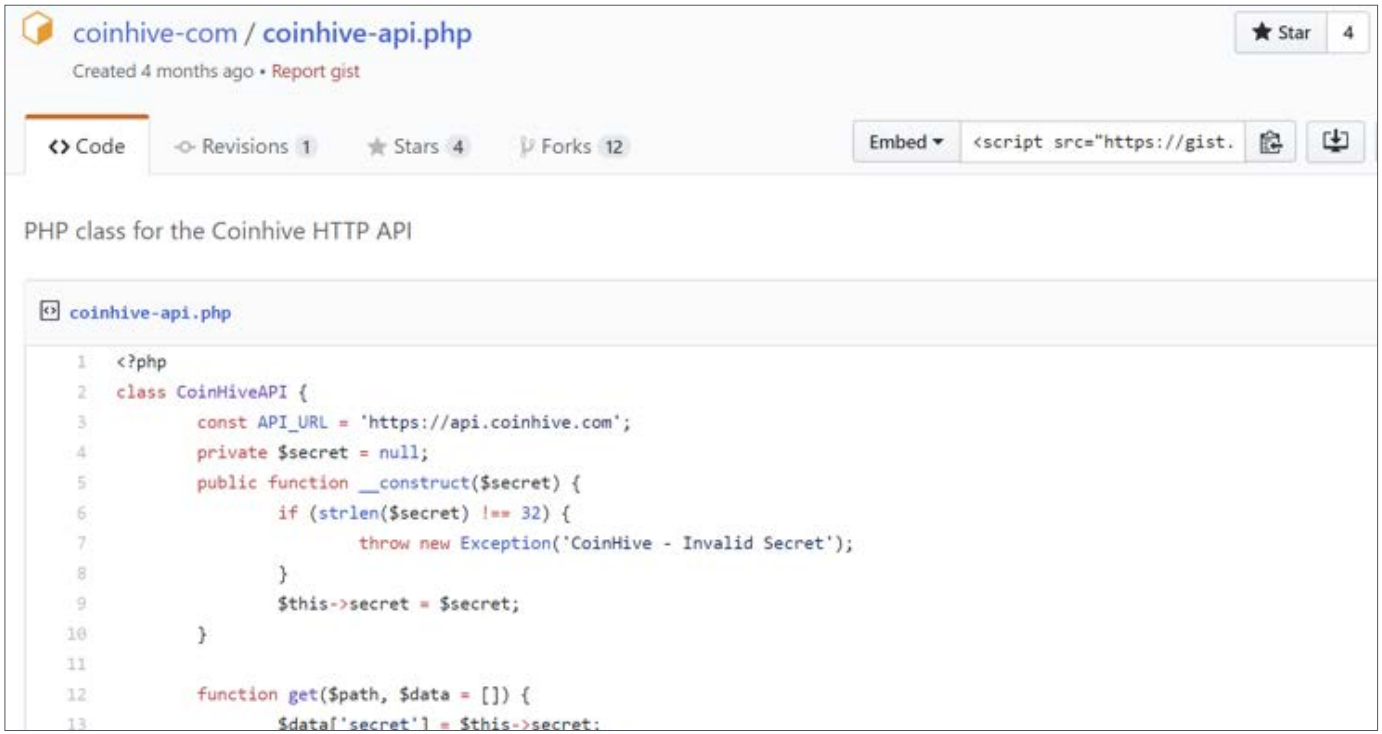


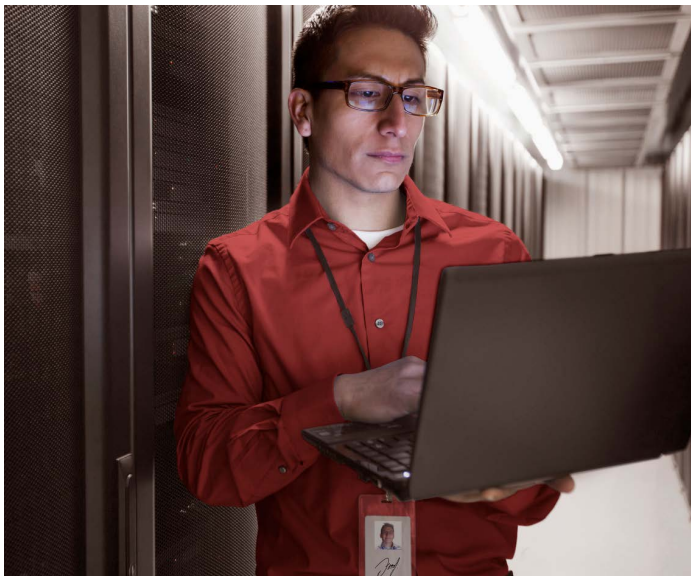

图 3：Coinhive API。

资料来源：https://gist.github.com/coinhive-com/dc37d300b2f4f909006a07139c9d2c71

关注 共享

网站所有者可能不是加入 Cryptojacking 代码的始作俑者 - YouTube 就是这样的情况。该热门视频分享站点中的一个缺陷允许恶意广告商将 cryptojacking 代码注入广告来挖掘比特币或以太币。(YouTube 迅速将恶意广告商从其网络中移除并拦截了挖矿广告。) 网络犯罪分子们已经累积了多年的恶意广告经验，并自行演化了这方面的知识，以满足其加密货币活动的要求。

已知有近 3 万个站点在得到或未得到同意的情况下托管着用于挖矿的 Coinhive 代码。这只是对非模糊处理站点的计数。实际数字可能要高得多。由于这种行为受到越来越多的监视，可以预期将会发现更多的 cryptojacking 挖矿软件。



### 终端挖矿软件

2016 年之前，恶意挖矿是获得加密货币的主要方法。尽管不如勒索软件常见，但在 2017 年末和 2018 年初，挖矿表现出爆炸性复苏迹象。新挖矿软件迅速涌现，而旧恶意软件经过修改后具备了挖矿功能。勒索软件家族甚至开始通过加入挖矿功能而焕发新春。例如，Black Ruby 在 2018 年初被发现，并且要求以比特币支付价值 $650 的勒索赎金。恶意软件在受感染的设备上采用流行的开源 XMRig 门罗币挖矿软件。另一个大规模的挖矿活动在 2018 年 1 月被发现，也使用了 XMRig。这样的开源工具一定程度上造成挖矿恶意软件大幅增加。

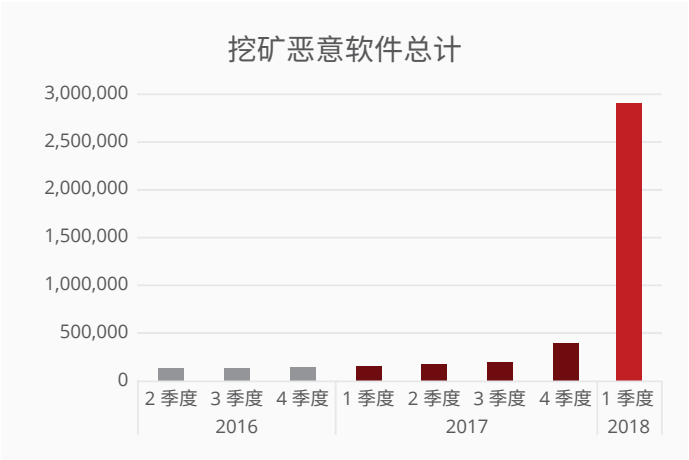



图 4：挖矿恶意软件呈爆炸式增长。 资料来源：McAfee Labs

关注 共享

过去的六个月，许多恶意软件开发人员似乎已经从恶意软件迁移到加密货币挖掘（McAfee® Global Threat Intelligence 数据表明勒索软件在 2018 年第 1 季度和 2017 年第 4 季度相比减少了32%，而货币挖掘增加了1,189%），挖矿软件主要以 PC 为目标，但是其他设备也可能成为受害者。例如在中国就有利用 Android 手机来通过 ADB.Miner 挖掘门罗币的现象，该恶意软件的行为类似蠕虫，在通常用于 ADB 调试接口的端口 5555 上运行。设备也因为 XMRig 挖矿软件而被感染。对 shodan.io 的查询表明有一百万台以上的面向互联网的设备在端口 5555 上运行。其中一部分是 XMRig 挖矿软件。据发现，ADB.Miner 重新利用来自 Mirai 僵尸网络的代码

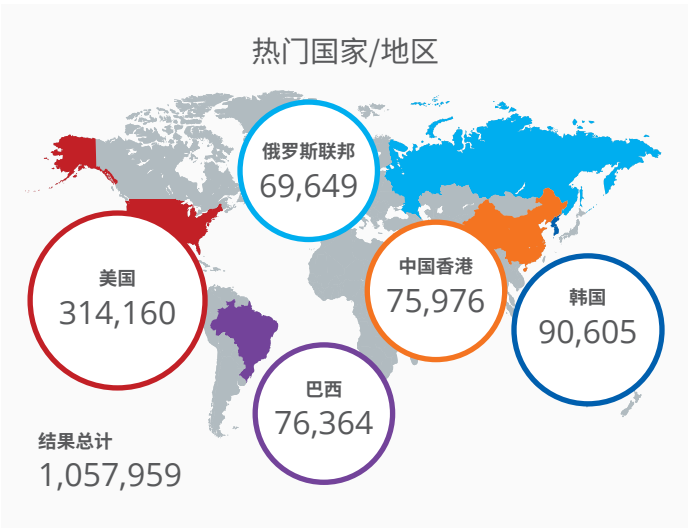



图 5：对端口 5555 设备进行 Shodan.io 搜索。

（最早于 2016 年初出现），并且已被观察到各种全球性攻击。截至 2018 年 2 月，恶意软件背后的威胁实施者已经感染了大约 7000 台设备，其中大多数位于中国和韩国。

在某些情况下，攻击以特定群体为目标，而不是使用地毯式搜索方法。一款恶意挖矿软件以俄罗斯论坛上毫无戒心的玩家为目标，将恶意软件伪装成增强热门游戏的“mod”。玩家在诱导下下载恶意软件，随后利用他们的计算机资源进行盈利。为了持久存在而不引起怀疑，挖矿软件会留意打开窗口的标题，诸如 Windows 任务管理器、Process Hacker 或其他进程管理器。如果看到这样的标题，它就会停止挖矿操作，从而隐藏其活动。该操作背后的嫌疑作者被指控是其他游戏“欺诈”软件背后的主要角色，并且已知在多个俄罗斯论坛上发布了自己的恶意软件，但由于保持匿名而很少被觉察。

对于恶意用户而言，自己编写恶意软件需要较高的成本和较多时间。他们不会自己研究和编写利用代码，许多恶意软件作者选择公开披露的利用代码和已知的漏洞，并假设有许多计算机仍然未修复且可对其发起攻击。这种假设经常被证明是正确的。2017 年下半年，估计非法的挖矿软件 Smominru 获取了价值 3 百万美元以上的门罗币。该活动借助了 Shadow Brokers 黑客小组公开披露的 EternalBlue 利用代码。该利用代码通过高度成功的恶意软件 WannaCry 而成为头条，影响了全球各地的计算机。该利用代码借助了 Microsoft Windows 中 Server Message Block v1 协议中的缺陷（在公告 MS17-010 中披露）。

Smominru 并不是利用 EternalBlue 盈利的唯一恶意软件家族。WannaMine 是一款门罗币挖矿软件，也通过 EternalBlue 利用在网络上传播。对于初始感染，WannaMine 采用常见的网络钓鱼电子邮件来启动批处理文件，并从其控制服务器下载恶意 PowerShell 脚本。随后使用 XMRpool 将设备连接至公共矿池 - 将受害者的系统变为非自愿的参与者。以下三个连接字符串被用于将受害者连接至矿池。

```
stratum+tcp://pool.supportxmr.com:80
stratum+tcp://mine.xmrpool.net:80
stratum+tcp://pool.minemonero.pro:80
```

在另外一个示例中，借助 CVE-2017-10271，攻击者将 Oracle WebLogic 服务器转变为门罗币挖矿僵尸网络。(Oracle 后来修复了漏洞。) 尽管威胁实施者存在于服务器上，但他们显然对于窃取数据或通过赎金获利没有兴趣。他们没有数据窃取行为的表现证明他们的兴趣在于挖矿。

## 实现漏洞

另一种类型的威胁是针对区块链实现本身及其支持工具的攻击。但是越接近区块链技术的核心，攻击就越难以成功。一般而言，这些威胁更多利用传统软件和 Web 应用程序。

比特币 wiki 维护了一份与其官方工具相关的常见漏洞及披露的清单。这些漏洞会导致拒绝服务工具、货币被窃取以及数据曝光等等。尽管漏洞的影响很大，但它们一般都在发布后被发现和修复。难以构建和维持安全代码；区块链的普及性和爆炸式增长加重了这一问题。对于有关核心比特币工具的高严重性漏洞的发现速度已减缓，在一定程度上给使用者带来了信心。这样的信心不能归因于社群和第三方工具。

2018 年 2 月，零日利用袭击了 PyBitmessage，后者是一种对等消息传递工具，可反映比特币的交易和区块传输系统。PyBitmessage 使用区块链工作量证明理念来“支付”消息传递并减少垃圾邮件。攻击者使用该利用通过发送专门构思的信息在设备上执行代码。随后他们运行自动化脚本来寻找以太币钱包，同时创建反向壳以用于未来的访问。

第三方工具通常是更容易受攻击的目标，因为他们的社群更小，并且用于保护代码或响应问题的资源更少。我们很少看到危害实现本身。2017 年针对 Iota 披露的就是这种情况。安全漏洞让攻击者创建哈希冲突和伪造的签名，以便从其他钱包窃取货币。该缺陷已经得到修复，但是在一定程度上要求在网络上采取硬性措施，停止使用 Curl - 一种自定义构建的密码哈希函数。问题源自对加密黄金规则的打破："不要创建自己的加密"。加密是非常难以正确实现的技术。对于自定义代码和加密相关函数的任何自定义代码都应在使用之前经过严格审查。由于基本安全缺陷的问题，在行业从 MD5 迁移至 SHA-1 到 SHA-256 哈希函数时，已经证实，即使现有技术也可能存在问题。

我们可以列举更多不安全的区块链实现的例子。Verge 开发团队在四月初遭受攻击时，没有良好的资源配备来应对其实现中的大量漏洞。攻击者利用缺陷来挖掘新的货币，而不用花费任何挖矿资源。补丁具有将货币"分叉"的不利影响，这在本质上是创建与原货币分离的新货币。对货币的价值的影响仍然可见，但是预期会明显地影响 Verge 保持相关的能力。

在诸如以太币的区块链实现中，用户代码通过智能合同成为账本的一部分。智能合同由用户编写并作为账本的一部分提交。合同可根据合同的规则执行逻辑。如果得到允许，其他人可参与供所有人使用的自我维持的去中心化应用程序。与任何代码一样，它可能存在错误和漏洞。Parity 钱包库结合以太币智能合同使用后，2017 年 11 月发现其中存在严重漏洞。偶然发现的问题可让攻击者造成一些多签名钱包不可用以及将帐户持有者锁定。这导致价值 1.5 亿美元的以太币被冻结。该攻击的规模超过了之前最大型的智能合同黑客攻击，造成了超过 5000 万美元的损失。在针对基于以太币构建的自治组织"DAO"的攻击中，黑客利用递归错误来获取资金。

### 钱包窃取

在一月份，发现威胁实施者绕过面向互联网的挖矿主机并将主机上的钱包地址更改为受实施者控制的地址。网络犯罪分子通过绕过普遍使用的挖矿软件 Claymore Miner 的管理端口进行钱包交易，该挖矿软件默认在端口 3333 上监听。恶意软件 Satori.Coin.Robber 是知名的 Satori 僵尸网络的后续版本，它于 2017 年末在物联网设备上造成了严重破坏。该变体使用硬编码的 IP 地址来控制服务器流量，其中大多数 IP 扫描针对韩国的潜在目标。此外，恶意软件作者留下了注释，表明僵尸程序并非恶意，可通过电子邮件联系他。

网络犯罪分子甚至重新改变了其他已知技术的用途并针对加密货币攻击对其进行了定制。2017 年末发现的一次攻击替换了受害者剪贴板中的电子钱包。尽管擦除数据和替换内容并不新鲜，但这些攻击者是特别针对加密货币。CryptoShuffler 特洛伊木马程序会攻击剪贴板，自 2016 年开始现身，并以一系列数字货币为目标，包括比特币、狗币、耐特币、达世币、以太币、门罗币和大零币。同一作者还发布了以剪贴板为目标的特洛伊木马程序 Evrial。每个特洛伊木马程序位于受害者的计算机上，等待类似加密货币地址的字符串并用攻击者控制的地址来替换该地址。该技术通过替换电子钱包可带来相当可观的利润，已经为 CryptoShuffler 带来 14 万美元以上的利润。

新恶意软件可能使用旧的方式，而旧恶意软件也可能改变自己的行为。银行业特洛伊木马程序也以加密货币为目标。特别是在 2016 年出现了两个木马程序。臭名昭彰的银行业特洛伊木马程序 Dridex 在其一般的银行业凭据窃取之外又添加了钱包窃取功能。特洛伊木马程序 Trickbot 同时将金融机构和加密货币作为目标。Trickbot 添加了 coinbase.com（一个热门的加密货币交易所）作为其攻击媒介。一旦系统被感染，只要受害者访问电子货币交易所，恶意软件就会注入伪造的登录页面，从而让网络犯罪分子窃取受害者的登录数据，以及一系列数字资产，包括比特币、以太币和耐特币。

### 技术攻击

在首个区块链实现发布之前，对于去中心化银行业没有可信的替代方案。但在那之前，对构建此类系统的安全问题进行了大量研究。经过多年的研究，包括 Haber 和 Stornetta 的区块链，在区块链理念上建立了信任。区块链的安全性还取决于特定假设。如果没有符合这些假设，则面临安全风险。

区块链的主要假设之一是对网络的贡献，即比特币的“哈希率”是分布式的。具体而言，没有一个实体或合作组在任何时候处理网络的 50% 以上。如果恶意用户拥有网络的 50% 以上，就会发生多数攻击。如果超过了 50%，就可以比任何人以更快的速度进行处理，根据自己的需要创建自己的链。

这种能力导致或简化其他攻击，例如重复付款，在其中同一个币可花费多次，并让一个接收者什么也得不到。由于用户群庞大，多数攻击从来未对比特币成功实现，但对 Verge 和其他货币成功实现过。规模小得多的货币尤其面临风险。在 Krypton 被证明易受这种攻击之后，团体 51 Crew 将目标转向其他小型货币，并持有这些货币以要求赎金。该风险也适用于内部开发的区块链。许多组织在开发区块链技术来管理库存、数据和其他资产。如果这些自定义网络的贡献群体或哈希率不是足够大，攻击者就可使用云技术、僵尸网络或池来攻击系统。

相关的假设是大多数节点是“最可靠的”，意味着至少有一个连接指向合法节点。不能连接至一个最可靠节点可导致 Sybil 攻击，其中攻击者强制受害者仅和恶意节点通信。攻击者可控制受害者可访问的信息，包括账本。只需要一个最可靠节点即可阻碍该类型攻击，因为攻击不能证明比网络更长的链。重新调用该长链可证明构建链所需的工作量。如果受害者知道了有效链，攻击者必须胜过整个网络的算力。因此，该类型攻击依靠阻止最可靠节点从真正的网络披露信息。

最可靠节点不能阻止攻击者尝试 Sybil 攻击。2016 年发现有大型的节点集合被一起创建。对于多数攻击，较小规模网络成为容易受攻击的目标，尤其是在系统中还未构建额外的应对措施时。

第三个假设是哈希冲突很少见。比特币使用 256 位长度来确定钱包的所有权。每个密钥映射至其他人可向其发送资金的公共地址。只要所有者具有密钥的唯一访问权限，则没有其他任何人可通过钱包提交交易。但是如果冲突不少见呢?攻击者或其他任何人可能偶然能够将资金从某人的钱包中转

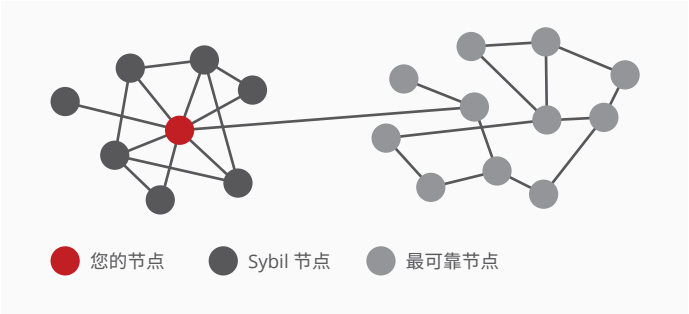



图 6：最可靠节点阻止 Sybil 攻击。

资料来源：https://www.coindesk.com/bitcoins-security-model-deep-dive/

关注

共享

移。钱包和资金的所有权将难以被证明，因为根据网络的立场，双方具有相同的权利。好消息是利用行业标准算法的哈希冲突似乎很少见。没有人能够有意或无意地生成其他人的密钥，至少对于比特币是如此，前提是这些密钥是以正确方式创建。这不能阻止所有者不当创建密钥。对于比特币和范围较小的代币而言，许多人尝试通过“脑钱包”管理自己的私钥，脑钱包通过单词或易于记忆的种子生成密钥。该行为让钱包易于遭受定制的字典攻击。其他密钥可能遭受实现本身危害。 Iota 对不当创建的密钥的信任导致冲突，进而对其采用者造成严重安全风险。对于算法的进一步研究（包括当前标准）可造成攻击更容易发生，正如我们看到的算法 MD5 和 SHA-1 等。

### 现代化的传统攻击

有关区块链的许多安全焦点在于账本的完整性以及基础技术。但是，用户的行为也关系到全面了解安全风险。一种源于不安全行为的知名攻击被重新改变了用途，专门针对当前的区块链实现。

### 字典攻击

字典攻击已经存在了数十年。攻击者通常会尝试破坏受害者的密码或其他身份验证机制。我们来看看典型的字典攻击，尤其是 Rainbow 表格攻击。

当我们为在线帐户创建密码时，服务提供商不应当以纯文本存储密码，而是应当采用密码的加密哈希并存储其值。例如，如果我们使用高度不安全的“password”，服务器可能将其保存为 5baa61e4c9b93f3f0682250b6cf8331b7ee68fd8，

关注

共享

其为字符串“password”的 SHA-1 哈希。我们可使用各种哈希算法和其他程序，例如加盐，来使其更加安全。但是要考虑如果攻击者看到前置字符串会怎样。他们可能会将该字符串视为“password”的哈希。尽管大多数情况下难以根据哈希找到字符串，但是反过来就不是这样了。寻找字符串的哈希在使用命令行解释器（例如 Bash）时尤其简单。

- $echo -n ‘password’ | shasum

哈希函数为单向算法：如果攻击者仅知道哈希值，理论上他们无法计算初始密码。在这种情况下，我们会碰巧同时知道密码及哈希值，让它们之间的转换变得简单。“password1”的 SHA-1 值是什么?这也很容易检索并且会得到 e38ad214943daad1d64c102faec29de4afe9da3d。如果攻击者看到“password”或“password1”的哈希值，他们就可将其转换为初始文本。

| SHA-1 哈希 | 明文 |
|---|---|
| 5baa61e4c9b93f3f0682250b6cf8331b7ee68fd8 | password |
| e38ad214943daad1d64c102faec29de4afe9da3d | password1 |
| 2aa60a8ff7fcd473d321e0146afd9e26df395147 | password2 |
| … | … |
| e13fc576c44eacd178e21b8b253f59fa59aa4cc8 | passwordN |

该转换可对每个可能的密码运行数百万次。唯一的限制是时间，但是攻击者可专注于常用的密码。与明文密码配对的哈希值集合称为 Rainbow 表格。从加密哈希到明文密码的转换就是 Rainbow 表格攻击。

修改的 Rainbow 表格攻击可对区块链实现，尤其是比特币和相关的加密货币。在本报告的剩余部分，所有示例都将特定于比特币，但是相同的技术也可能适用于相似的加密货币 - 也可能适用于超越加密货币范围的区块链的新实现。

在比特币中，地址代表货币驻留在其中的公共接口。用户使用该地址传输货币 - 当他们用货币向某人支付时，交易就通过该地址进行。但是为了验证他们有权通过地址发起交易并花费货币，他们必须使用自己的私钥。该密钥应当仅有所有者知道，并且必须使用比特币的椭圆曲线数字签名算法。这有效地意味着可由 SHA-256 哈希算法生成的几乎所有 256 位数字都有效，这可导致有人粗心大意地采用脑钱包。他们不会记住或存储 64 个看上去随机的字符，他们可只记住自己的正常密码，并在需要自己的私钥的任何时候使用 SHA-256 哈希算法。人们过去会这样做，但非常危险。网络犯罪分子一直在扫描脑钱包。

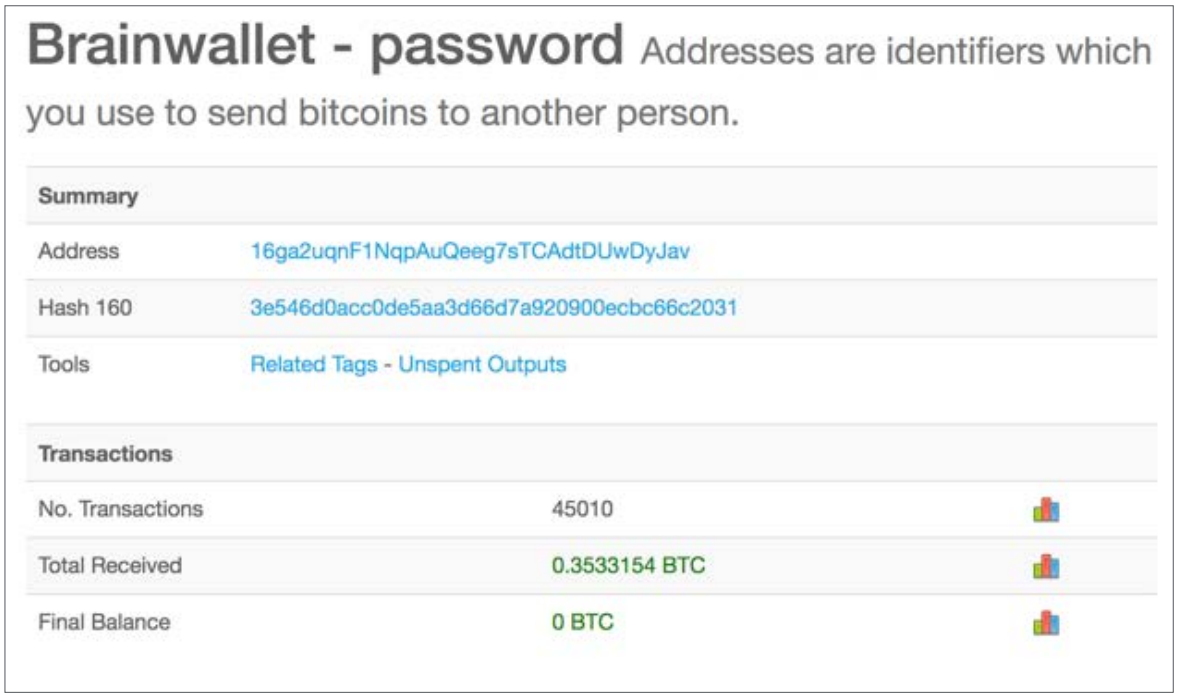



图 7：2018 年 3 月采用“password”生成的私钥的帐户。

资料来源：https://blockchain.info/

关注

共享

在前置图像中，我们看到 45010 个交易在 2012 年 7 月和 2018 年 3 月之间发生，导致余额为零。通过交易观察，我们看到小笔收入的金额不久会跟随支出的交易的模式。在使用“password”、“password1”和“password2”的帐户中，我们计算的交易数为 117212，其中我们无法确定所有者，也无法确定哪些是失窃金额。比特币不是唯一存在该问题的加密货币，即便有许多加密货币是在脑钱包漏洞广为人知后诞生。

研究者们在一段时间内研究了脑钱包的弱点，并且在 2016 年发现了 18,000 个易受攻击的钱包，还发现了攻击的速度优化。结果不仅限于简短密码。列表中有许多也为带有空格、标点和数字的短语。

在我们的研究中，我们偶然遇到了非常常用的脑钱包。不幸的是，我们怀疑其他人可能偶然使用了该钱包，随后失去了自己的钱财。很可能由于用户错误，多个人生成了相同的私钥，并因此共享了该钱包，导致失窃。请查看采用字符串的 SHA-1 哈希的以下两个 Bash 命令：

- $echo -n “$password” | shasum
- $echo -n “$Cryt0p4sswordV3rySecure!” | shasum

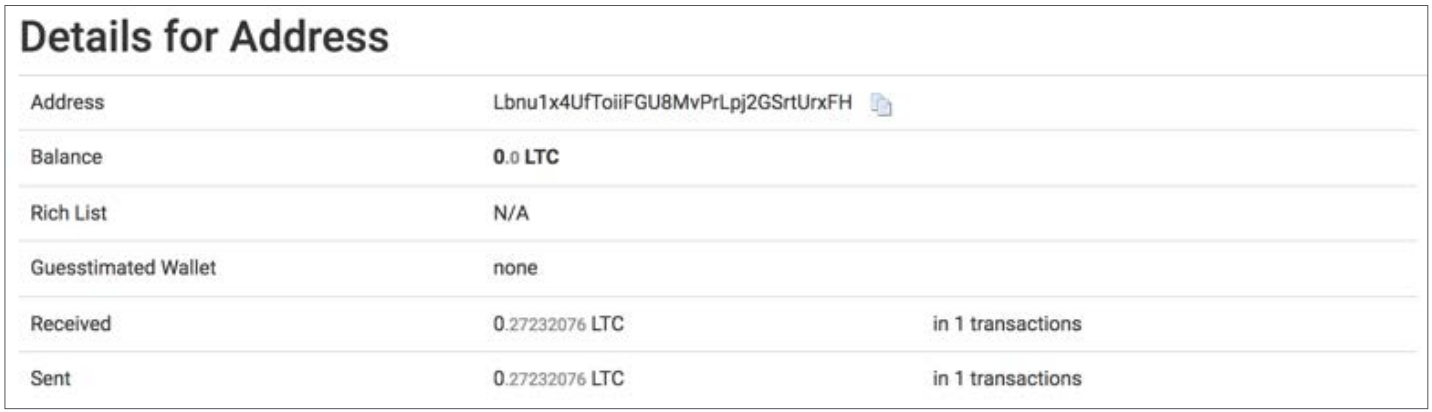



图 8：Litecoin 脑钱包。

资料来源：https://chainz.cryptoid.info/ltc/

关注

共享

我们可能期望两个不同的 SHA-1 哈希，但是二者都返回相同的值：da39a3ee5e6b4b0d3255bfef95601890afd80709。这是容易犯下的错误，由用户和 Bash 语法的详细信息造成。密码中的 $ 符号在 Bash 中是特殊字符，表示变量或特殊参数。字符串开头使用 $ 来让 Bash 将整个字符串处理为变量 - 这将预期字符串转变成该变量的值。在这种情况下，变量中的任一个都不存在，因此 Bash 返回相同的空字符串。犯下该错误导致不希望的私钥共享。它还可能导致损失几乎 59 个比特币（截至 3 月价值 530120 美元）。（参见下面的截屏。）

尽管存在例外，但是大多数已知的脑钱包基于用于其他帐户的相同常见密码。为了更清楚地说明，我们构建了自己的 Rainbow 表格来对比特币帐户进行测试。我们的表格由相对较小的 20 万个最常见密码集合、16 万个以上的以比特币为中心生成的密码、名言列表以及数本容易获得的书籍（包括《战争与和平》以及《爱丽丝的奇妙冒险》）组成。尽管我们的样本规模相对较小（许多字典以数百万度量），也发现了 852 个容易遭受攻击的钱包。这些钱包被转移走了 102 个以上的比特币（在撰写本文时价值约为 100 万美元）。这些数字可能会随着我们的样本规模增大而增大。

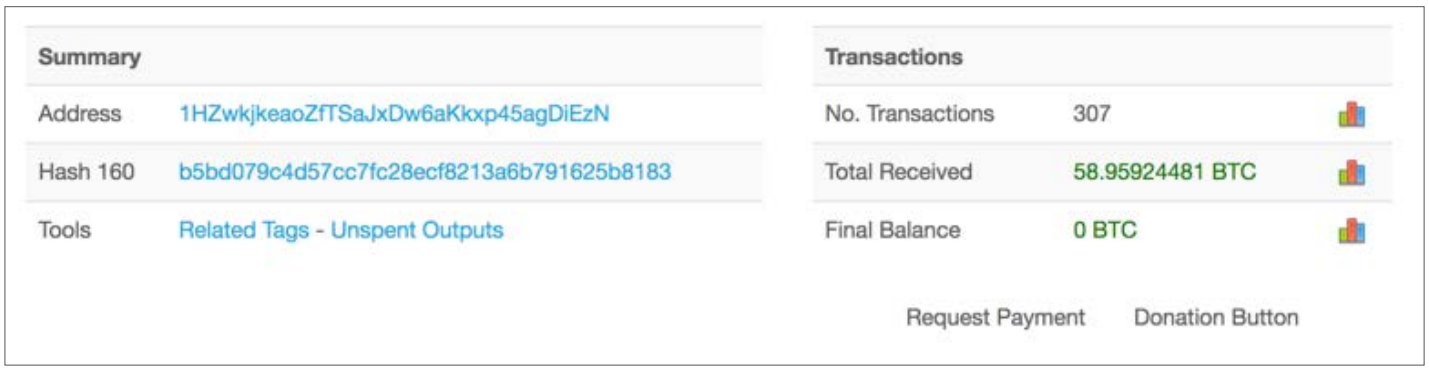



图 9：该钱包最近在 2018 年 3 月 5 日记录了两笔交易。一笔收入和一笔支出交易发生在大约 15 分钟内。 资料来源：https://blockchain.info

我们可以在包括脑钱包的许多在线帐户中看到，“password”仍然被用到。在泄露的数据库中，我们发现了许多密码，包括一些我们的以加密货币为中心的密码。使用来自“Have I Been Pwned”的 Troy Hunt 的密码哈希数据库，我们将自己的结果与已知从各个数据泄露中泄露的密码哈希交叉引用。通过查看我们的以比特币为中心的字典，我们发现了得自 5.01 亿个泄露记录的 5,098 个唯一密码。在该集合中，有一些也是脑钱包，有大约 30 个以上的比特币可被窃取。

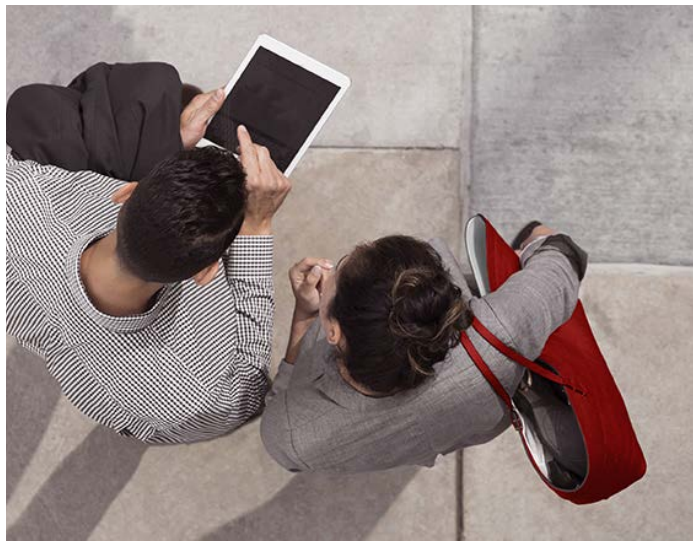
## 攻击下的交易

该领域最为大型的参与者是加密货币交易所，它们是主要目标。加密货币交易所有助于消费者管理自己的货币，并与其他加密货币或实体货币（例如美元）进行交易。这些交易所的行为和传统银行相似，为许多人带来便利。帐户持有者可创建帐户、添加或分发资金并管理自己的加密货币，而无需了解本地钱包软件。最大型的交易所处理多种货币并处理它们之间的交易。对于许多人而言，交易所是处理加密货币的唯一途径，也是使用者可获取货币的主要方式之一。

网络犯罪分子认识到了交易所的受欢迎程度，并将它们作为目标。与银行业相似，交易所如果保护不当会成为金矿。银行拥有通过数十年交易中的安全问题和事件响应累积的经验优势。即使如此，安全问题还是会发生，正如我们过去数年在针对 SWIFT 银行业网络的大量攻击中所见。交易所没有这样的丰富经验，并且在以艰难的方式学习。这些学习到的经验对于交易所和客户群来说代价很高。

### 主要事件

2018 年 1 月，日本首个也是最受欢迎的交易所之一 Coincheck 损失了价值 5.32 亿的新经币，影响到 26 万个投资者。当受害者困惑不已时，交易被停止。一名攻击者获得了员工计算机的访问权限，并且安装了恶意软件，旨在从电子钱包窃取私钥。攻击者设法获得“热”钱包的私钥，这种钱包在线上用于即时交易。在帐户被洗劫一空后，造成了规模最大的交易所黑客攻击。



Coincheck 攻击并非唯一的此类事件。在整个 2016 年和 2017 年，交易所一直是网络犯罪分子的目标。在此期间，我们看到大量成功的攻击。在 2017 年初，我们了解到 2016 年 8 月几乎有 12 万个比特币在 Bitfinex 失窃。货币被转移到其他交易所，包括 LocalBitcoins、Xzzx、BTC-e、Bitcoin.de、Coinbase、Kraken、CoinsBank 和 QuadrigaCX。尽管针对这些金币的价值提供了 5% 的奖励金，失窃的货币也未能被找回。“我们通常知道它是怎样发生的，”Bitfinex 应用程序团队负责人 Drew Samsen 这样写到。“这是专业人员（或团队）为时几个月的行动造成的，他们精明地掩盖了自己的踪迹。”

Gatecoin 是一家中国香港的交易所，以很早就支持以太币而闻名。2016 年 5 月，Gatecoin 披露了 250 比特币以及巨额的 18.5 万以太币损失（价值大约 200 万美元）。其热钱包和“冷储存”离线钱包都受到影响。攻击者通过修改交易所的系统，设法绕过了设置在冷储存上的多签名保护，以改为使用热钱包。

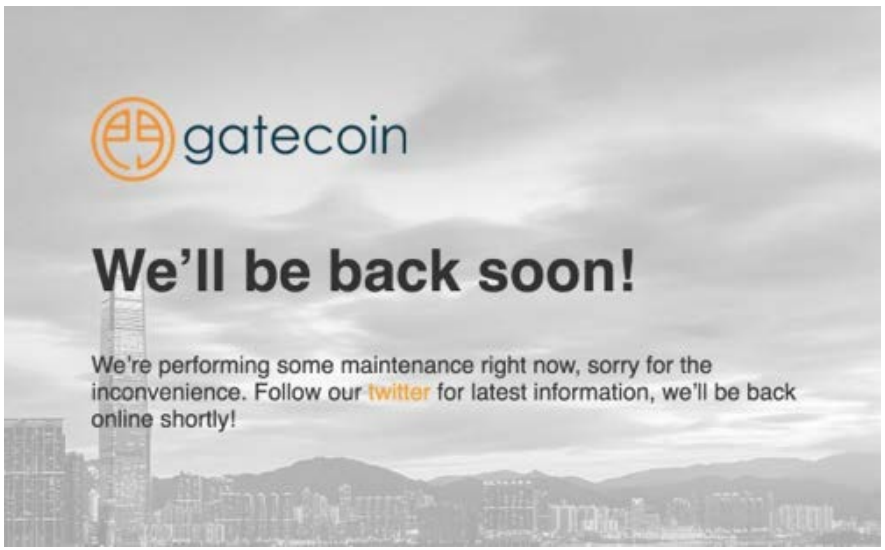



图 10：2016 年 5 月来自交易所 Gatecoin 的截屏。 资料来源：CoinDesk.com

关注 共享

交易所基础设施本身并非总是主要目标。交易所的使用者也可成为直接攻击的受害者。在最辉煌时期，Bithumb 处理全球 10% 的比特币交易，也是韩国以太币的最大交易所，有 44% 的以太币交易是在此进行。2017 年 6 月，Bithumb 报告由于员工计算机数据泄露而丢失了 31800 个 Web 用户的个人身份信息（大约为其用户群的 3%）。攻击者没有以基础设施为目标，而是直接针对使用者，在某些情况扮作 Bithumb 高管并使用传统社交工程和网络钓鱼技术。

与此类似，Enigma（以投资平台的方式运营）的客户也成为攻击目标。使用知名且常见的社交工程技术，攻击者诱使 Enigma 客户使用恶意的以太币地址。通过危害官方 Enigma 网站、时事通讯和 Slack 帐户，攻击者分发了自己拥有的不正确的以太币支付地址。有 1,500 个以上的以太币失窃，其中一些交易发生在危害被公布并修复之后。

| TxHash | Block | Age | From | | To | Value | [TxFee] |
|---|---|---|---|---|---|---|---|
| 0xcf6b4ccc0f91b32... | 5059624 | 14 days 8 hrs ago | 0x21e229f2d307d7f... | IN | Fake_EnigmaPhish | 0.002 Ether | 0.000105 |
| 0xbf45b27df99f5f74... | 4825731 | 55 days 3 hrs ago | 0xdc4ee4e2580b4c... | IN | Fake_EnigmaPhish | 0.00124579 Ether | 0.00042 |
| 0x12580af9ab49fee... | 4313854 | 150 days 6 hrs ago | Fake_EnigmaPhish | OUT | 0x99e331fa7c45671... | 20.2 Ether | 0.000441 |
| 0xbd96745cea0723... | 4262418 | 165 days 10 hrs ago | 0xf4a2f01cd178b88... | IN | Fake_EnigmaPhish | 3 Ether | 0.000441 |

图 11：交易记录。

资料来源：https://etherscan.io/

在数年值得注意的交易所攻击之后，Coincheck 黑客攻击的新闻对信任造成了实际影响。哪怕是一点问题，也会造成客户对于其他交易所的顾虑。Binance 不得不进行计划外维护，选择主动通知自己的客户当心诈骗以及以他们的帐户为目标的骗子。

尽管 Binance 没有遭遇泄露，但在服务器维护不久也遭到了分布式拒绝服务攻击。攻击的新闻没有让用户平息，他们已经对非计划性服务器维护持怀疑态度。为了维持使用者信心，Binance 在二月大多数时间提供 70% 的交易费折扣。

加密货币采用者越来越期望在大范围不稳定的市场上寻得安宁。许多使用者建议其他人将货币分存在数个交易所，防止不可避免的攻击。对于富有经验的用户，本地或基于硬件的钱包是合理的替代品。但是这些选择造成了自己的安全问题，需要由个人来管理。用户对于交易所安全性的信心程度由于行业在平衡发展和安全上遇到的困难而在不断下降。


图 12：来自 Binance 交易所的消息。帐户后来由 Twitter 暂停。

关注

共享

## 恢复

与其他大多数货币相比，由于去中心化性质，从加密货币窃取中恢复显得更加困难和复杂。只有钱包的所有者可更改钱包余额，即便该余额是非法所得。尽管交易所可跟踪货币流向了何处，但是需要当前所有者的协助方可追回那些资金。本质上，交易所必须找到犯罪分子和钱包密钥方可返还任何失窃的货币。对于交易所到交易所转移的情况，如果法律允许可达成协议，将资金返还。交易所通常在内部管理区块链密钥，而帐户则存储在中心，让交易所可以更多地控制钱包。但是，如果资金转移到私人钱包，受害者将无法求助。唯一的希望在于执法机关可找出窃贼，并获得和钱包关联的私钥。几乎在所有场景当中，都是由于资源有限、缺乏管制或管辖权问题而导致的损失。

在最近的事件当中，交易所尝试赔偿客户的损失 - 至少在泄露后存活下来的交易所是这样。Coincheck、Bitfinex 和 Gatecoin 算是其中的幸运者。在 2018 年 3 月，Coincheck 开始偿还受害者损失的新经币。2017 年 4 月，Bitfinex 成功偿还了受害者在 2016 年 8 月的黑客攻击中损失的资金。但是他们并没有直接从业务中拿出资金，而是使用 IOU 的加密货币形式。在披露黑客攻击之后，他们创建了 BTX 令牌，并承诺在未来会以 $1 将每个令牌购回。他们将这些令牌分发至其帐户持有人并在四月完成了回购。2017 年 2 月，中国香港交易所 Gatecoin 完成了 2016 年 5 月黑客攻击中失窃的比特币的偿还。比特币在失窃时的价值介于 $450 和 $750 之间，但是在完成偿还时价值大约为 $1,190。他们还为剩余的失窃以太币拟定了偿还计划。在这种情况下，交易所拉入了来自其他业务部分的利润，包括咨询服务和交易所费用并将利润重新分配至回购。

并非所有交易所都能从袭击中恢复。最为知名的例子是 Mt. Gox 的倒闭，这是一家日本交易所，在 2011 至 2014 年间遭到攻击。价值超过 4.5 亿的比特币失窃。当年，这导致 Mt. Gox 的清算和倒闭。最近又有两家值得注意的交易所遭到了网络攻击造成的无法恢复的影响。Bitcurex 是波兰最大也是最早的交易所之一，在遭遇黑客攻击后一个月内就结束了运营。最初，它以表述不清的措辞披露了一些服务问题，但最后发现有 2,300 个比特币失窃。

Bitcurex 突然在大众困惑几周后关闭，让用户自行承担损失。2017 年 3 月，波兰警方宣布对关闭的背景进行调查，并让所有受害者都站出来。

Youbit 是一家韩国交易所，在受到危害之后无法再维持运营。在 Bitcurex 调查开始仅一周之后，当时称为 Yapizon 的 Youbit 由于黑客攻击损失了 4000 个比特币，这大约相当于其资金的 36%。稍后的详细信息表明，货币在黑客抵达内部系统并访问四个热钱包之后失窃。Youbit 尝试使用相似的方法来补偿其客户。他们将损失分散在所有帐户持有者上，并发布了 IOU 形式的令牌，并承诺之后回购 IOU。但是在 2017 年 12 月，Youbit 遭遇了又一次攻击，损失了其资金的 17%，导致公司破产。具有剩余资金的客户被允许取回其余额的 75%，而剩余的部分则留给破产程序。

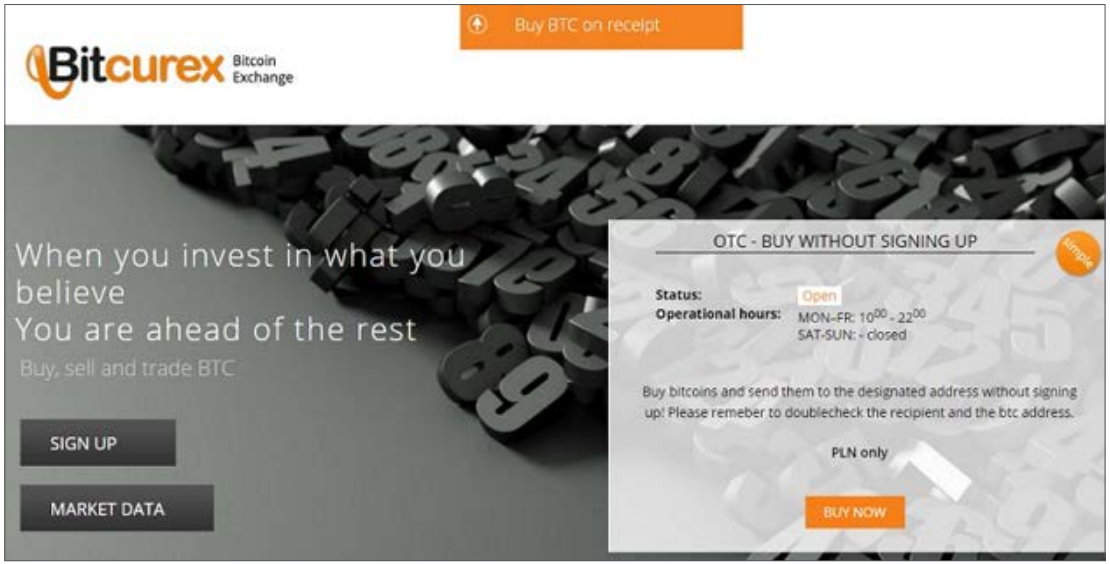



图 13：关闭的 Polish exchange Bitcurex 的广告。

**“2016 年 10 月 13 日，由于自动数据收集和信息处理上的外部干扰，第三方系统服务 www.bitcurex.com [was] 遭到破坏。这些行动的后果是 bitcurex.com/dashcurex.com 损失了部分资产。”**

—翻译自 bitcurex.com 上的波兰语声明

关注

共享

## 总结

由于区块链技术仍然对全球行业有积极和消极两方面的影响，所以我们必须重视安全问题。正如我们所见，网络犯罪分子将发现意想不到的方式来实现自己的目标。尽管区块链经过了充分的研究并解决了有关去中心化信任的许多问题，但未能解决用户或与其网络连接的应用程序的安全问题。我们已经看到经由脑钱包的不安全行为导致加密货币失窃。攻击者们以新方式对比特币私钥使用了旧技术（例如字典攻击）。即使传统的网络钓鱼攻击也可发挥作用，获得钱包或计算机资源的访问权限。我们观察到，不仅是区块链用户成为目标。区块链的主要商业采用者为加密货币交易所，它们接连遭遇了成功的攻击。政府管制机构努力跟上并了解由于网络攻击造成的损失的法律意义。

各企业也必须重视这方面的安全问题。区块链技术因为可解决去中心化支付以外的各种业务需求吸引了大量关注。完全自动化的企业正在使用智能合同进行构建。零售商和其他方面期望用区块链来管理自己的库存。医疗行业正在研究管理医疗文档的方式。对于交易所成功且有影响的攻击数量远远超出了本报告的范围，应当引起警惕。如果没有执行定制的风险评估，则不足以实现和使用新的技术。随着各行业研究和实现自己的区块链，我们可预见网络犯罪分子将部署已知和尚且未知的技术组合来危害它们。在不明确了解风险在何处的情况下，您可能过度信任了区块链实现。正如我们所见，错误在所难免。用户甚至难以控制并且不利地提升风险。我们需要从最近的事件中吸取教训，在面向未来保护我们的技术方面做出更好决策。

## 关于 McAfee

McAfee 是设备到云网络安全公司。在协同工作思想的启迪下，McAfee 研发出了适用于企业用户和家庭用户的解决方案，让网络环境变得更为安全。通过构建与其他公司产品集成的解决方案，McAfee 能够帮助企业部署真正集成的网络环境，通过协作的方式即时进行威胁检测和纠正，从而保护网络安全。通过保护用户的所有设备的网络安全，McAfee 能够随时随地为他们的数字化生活提供安全保障。McAfee 与其他安全参与者同心协力，致力于打击网络犯罪分子，以保护所有用户的利益。

**www.mcafee.com/cn**

北京市东城区北三环东路 36 号
北京环球贸易中心 D 座 18 层，100013
www.mcafee.com/cn



2018 年 6 月