区块链的十大攻击、漏洞及弱点

CSA GCR cloud security alliance GREATER CHINA REGION ®

序 言

分布式账本技术（DLT）被称为技术基础结构和协议，用于在分布于多个位置的网络中以不变的方式进行验证，同时访问和记录更新。由于 DLT 在各个领域和行业中的潜力，因此在技术领域正变得越来越流行。自 12 年前比特币问世以来，加密货币和支持它们的平台一直是攻击的目标。攻击者期望的结果是尽可能多地偷取加密货币利润。为实现这一目标，不良行为者可以针对区块链协议本身攻击特定平台。

《区块链的十大攻击、漏洞及弱点》（Top 10 Blockchain Attacks，Vulnerabilities & Weaknesses）这份报告覆盖了针对加密货币和 DLT 的十大攻击类型。也对这十大攻击类型进行了整体概述。虽然每种攻击类型都可以成为一篇单独的文章，因为篇幅有限，在此次报告中只总结描述了十大攻击，并提供了说明性示例和代价高昂的教训。本文可以帮助开发者，安全合规人员以及日常加密货币用户教育自己如何避免落入许多相同的陷阱。文章深入浅出，总结详尽，值得大家参考。

李雨航 Yale Li
CSA 大中华区主席兼研究院院长

致 谢

本文档《区块链的十大攻击、漏洞及弱点》(Top-10-Blockchain-Attacks-Vulnerabilities-&-Weaknesses)由 CSA 专家编写，CSA 大中华区秘书处组织翻译并审校。

中文版翻译专家组（排名不分先后）：

组　长：顾　伟

翻译组：余晓光　付艳艳　鹿淑煜　冯昌盛　苏泰泉

　　刘　洁　周轩立　郑　宁

审校组：姚　凯　余晓光　付艳艳　鹿淑煜　冯昌盛

　　苏泰泉　刘　洁　周轩立

感谢以下单位对本文档的支持与贡献（按拼音排序）：

三未信安科技股份有限公司　华为技术有限公司

OPPO 广东移动通信有限公司　上海市数字证书认证中心有限公司

英文版专家组：

原创作者：　Julio Barragan　John Jefferies　DaveJevans

原创贡献者：Bill Izzo　Ashish Mehta　Jyoti Ponnapalli　Kurt Seifried

Adalberto Valle

CSA 研究项目经理：Hillary Baron

CSA 员工：　Claire Lehnert (Design)　AnnMarie Ulskey (Cover)

特别鸣谢：　CipherTrace

在此感谢以上专家。如译文有不妥当之处，敬请读者联系 CSA GCR 秘书处给与雅正！联系邮箱：research@c-csa.cn；　云安全联盟 CSA 公众号。

目录

执行摘要

注意：对于虚拟资产的顶级攻击将会针对企业区块链再次发生

有一种强烈的误解，认为分布式账本技术（DLT）系统的不可篡改性使其本质上是安全的。但是，针对区块链应用程序的攻击途径广泛存在，攻击针对从密码学原语到共识机制漏洞或智能合约漏洞的范围。

自 12 年前比特币问世以来，加密货币和支持它们的平台一直是攻击的目标。攻击者期望的结果是尽可能多地偷取加密货币利润。为实现这一目标，不良行为者既可以针对区块链协议本身攻击特定平台（集中式或分散式），也可以针对持有加密资产的个人。

这份报告覆盖了针对加密货币和 DLT 的十大攻击类型

- 交易所黑客攻击
- DeFi 黑客攻击
- 51%攻击
- 钓鱼（为了获得私钥）
- 抽地毯/退出骗局
- 勒索软件
- SIM 卡交换攻击
- 投资骗局
- 高调倍增骗局
- 勒索

这份报告是对十大攻击的整体概述，每种攻击类型都很容易形成一篇单独的文章。本报告中列出的攻击，提供了说明性示例和代价高昂的教训，可以帮助从开发人员到合规官到日常加密货币用户的任何人，教育大家如何避免陷入相同的陷阱。

虚拟资产的承载性质，使攻击者的注意力集中于从虚拟资产服务提供商（VASP）和个人加密货币用户那里窃取私钥上。加密领域的格言“不是你的密钥；不是你的币”描述了这一现实，如果攻击者控制了私钥，就控制了虚拟资产。SIM 卡交换这类技术起源于某 Twitter 帐户接管工具，已被重新部署以控制用户的

双因子认证（2FA）， 并最终接管加密帐户，窃取用户的资金。

如果有权访问冷热钱包存储的管理员成为这些攻击的受害者，那么安全协议不足的新兴加密公司可能会遭受无法挽回的损失。更重要的是，未经审计的智能合约和安全协议中的疏忽也可能导致中心化和去中心化交易所的重大损失。 在过去五年中，43 个交易所被黑客公然入侵，超过 49 个 DeFi 协议被利用，造成超过 28 亿美元的损失。

加密货币还使旧的欺诈模式能够以新的方式运作，勒索软件、在线勒索和投资欺诈案件的加速增长就证明了这一点。 在过去五年中，至少有 14 家交易所和钱包托管商实施了退出欺诈，7 个 DeFi 项目实施了抽地毯式欺诈，被盗用户资金超过 45 亿美元。与此同时，根据 Palo Alto Networks《2021 年勒索软件威胁报告》，勒索软件攻击的复杂程度和严重程度有所增加，2020 年勒索软件的平均支付金额超过 312,493 美元——与 2019 年相比增长了 171%。 幸运的是，可靠的区块链分析工具提供了前所未有的能力，可以追踪虚拟资产并确定这些犯罪分子兑现资金的地方。

勒索软件攻击 2017-2021		
攻击类型	**主要攻击数**	**总金额**
交易所退出	14	43.83 亿美金
交易所黑客攻击	43	17.02 亿美金
DeFi 黑客攻击	49	11.22 亿美金
DeFi 抽地毯	7	1.24 亿美金
51%攻击	14	0.24 亿美金（使用双花攻击）

十大 DLT 攻击类型

1. 交易所黑客攻击

在本报告发布之时，加密货币的日均交易量超过 1800 亿美元，而且行业还处于起步阶段，所以很明显为什么这么多黑客瞄准加密货币交易所。 Mt Gox 是第一个遭受重大损失的中心化交易所，在 2014 年遭受攻击时损失了 850,000 BTC，价值 4.5 亿美

元。 在过去五年中，49 个中心化交易所遭到黑客公然攻击，造成超过 18 亿 美元的损失。

现在，随着交易所持续加强其云安全控制，攻击者已转向通过社会工程和信任计划，以人类用户为目标，这突显了对员工进行适当的安全培训的重要性。典型的交易所攻击分为以下几类：

- 网络钓鱼获取用户访问凭据，访问加密货币帐户并转移资金。这些有时与 SMS 劫持结合，接管目标用户的基于 SMS 的身份验证码。
- 针对交易所的技术攻击，渗透进交易所的内部系统，包括：
  a. 账号完成创建或访问后的 SQL 注入攻击
  b. 用于交易操作的软件漏洞
  c. 未打补丁的交易所软件
- 对交易所员工采取鱼叉式网络钓鱼，获得对提款的优先控制。
- 对交易所的员工进行鱼叉式网络钓鱼，植入恶意软件（特别是远程访问木马），允许攻击者访问内部系统并在基础设施节点之间跳转。
- 利用 API 漏洞获取私钥等存储的凭据。攻击者通常使用存储在内部系统中计算机上的凭据访问其他系统。
- 日常操作中对冷钱包（离线私钥存储）与热钱包（在线密钥存储）的使用不恰当或不正确。一个交易所 90%的加密货币应该存储在没有连接到互联网的冷钱包中。必须有一个协议，可以完全脱机地初始化冷钱包，并在热钱包和冷钱包之间驱动资金转移请求（通常需要一个带有签名指令的 USB 驱动器）。可以考虑采用多签名的方式访问冷钱包，即要求同时有两名员工在资金从冷钱包转移到热钱包之前对交易操作签名。
- 内部人员威胁在交易所中很常见。员工可以访问热钱包或冷钱包密钥，并复制它们，或在内部系统中植入恶意软件或远程访问木马，允许以后访问这些密钥以窃取加密资产。
- 反编译交易所应用程序（iOS 或 Android），发现嵌入在应用程序中秘密的云 API 密钥，然后使用这些密钥访问内部 API——通过这些 API 可访问热钱包或用户凭据。
- 复制钱包恢复密钥。比起保护热钱包或冷钱包，交易所需要付出更多努力保护钱包恢复密钥。如果攻击者获得了恢复密钥的副本，那么交易所的全部资产，包括冷钱包都可能被盗。永远不要在电子媒体上存储恢复密钥。把它们写在纸上，并保

存在实体的保险库中。与纸相比，物理金属装置可更防火。

- 利用交易所实施某特定货币时的漏洞攻击该货币。例如，许多 XRP（Ripple）实现都有一个允许部分支付的漏洞。如果一个交易所集成了 XRP 账本（Ledger），假设支付的金额字段总是已交付的全部金额——在这种情况下，恶意行为者可能会利用这一假设从该机构窃取资金。该漏洞可以用于攻击网关、交易所或商家，只要这些机构的软件不能正确处理部分支付。在 2020 年 9 月的前 9 天，三家交易所持有的 XRP 被完全清空。

过去三年较集中的交易所黑客攻击事件

日期	交换所	损失金额
2019 Q1	Cryptopia	1600 万美元
2019 Q1	Coinbene	1.05 亿美元
2019 Q1	DragonEx	100 万美元
2019 Q2	Bitrue	470 万美元
2019 Q2	Binance	4070 万美元
2019 Q2	GateHub	1000 万美元
2019 Q2	Silkkitie	200 万美元
2019 Q2	Bitpoint	3200 万美元
2019 Q2	Bitcoins Norway	未披露的
2019 Q4	Upbit	4900 万美元
2020 Q1	Exmo	1050 万美元
2020 Q1	Altsbit	7250 万美元
2020 Q1	Coinhako	未披露的
2020 Q1	Crex24	11,200 美元
2020 Q3	KuCoin	2.81 亿美元
2020 Q3	Eterbase	160 万美元
2020 Q3	2gether	140 万美元
2020 Q3	Cashaa	300 万美元
2020 Q4	LiveCoin Hack	未披露的

2. DeFi 黑客攻击

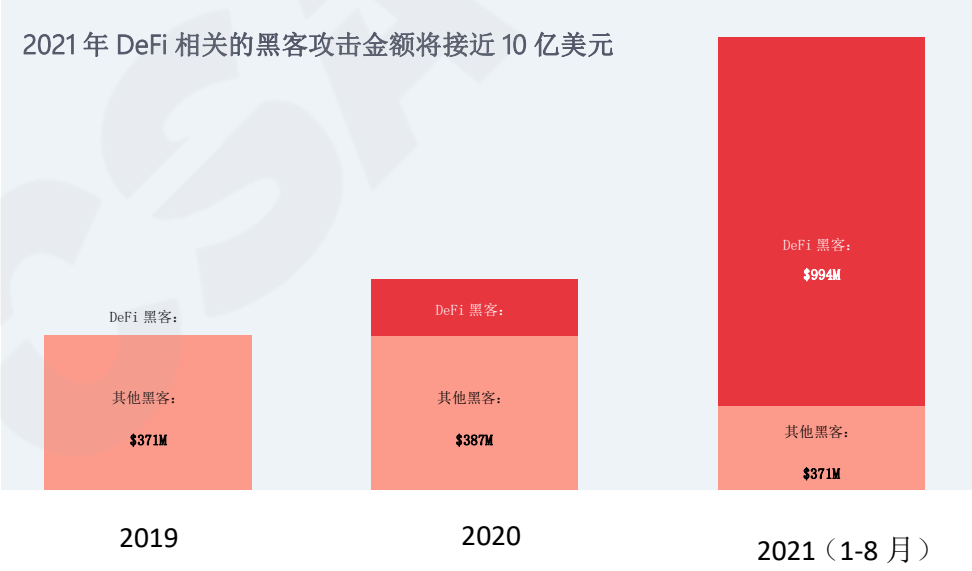
攻击者通常通过快速贷款为区块链金融攻击提供资金，这些贷款不需要抵押品或了解客户(Know-Your-Customer，KYC)身份数据，从而越来越难抓住不良行为者。虽然更多的去中心化交易所开始审计合约以期防止攻击，但精明的黑客仍在不断发现新漏洞。

例如:2021 年 5 月 8 日，与协议的新 Alpha Homora 集成相关的 Rari Capital ETH 池的“恶意合约”漏洞导致 1000 万美元的资产被盗。

在“恶意合约”的攻击中，攻击者欺骗智能合约，使其认为“恶意合约”具有适当的访问权限或许可。在黑客对 Rari Capital 的攻击中，该漏洞导致 HomoraBank 的合约做出了一个错误的假设，即黑客在平台上建立了一个 ibETH 池。攻击者使用去中心化加密货币交易所 dYdX 的闪贷 ETH 反复将存款注入流动性池，从而人为地使价值膨胀，并提取由于膨胀而比最初存入的更多的 ETH。

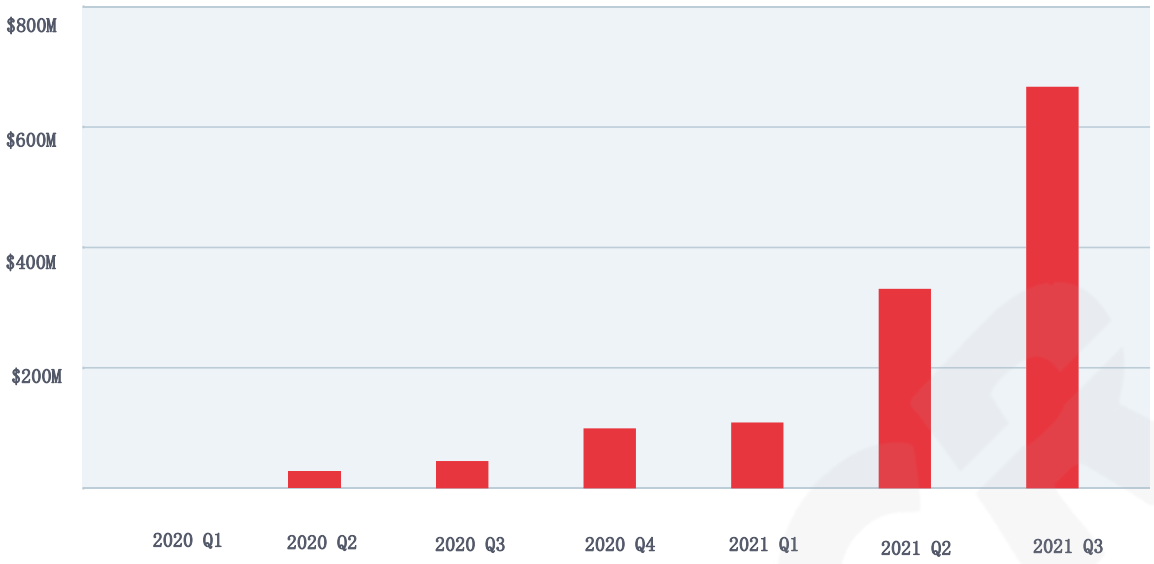
虽然对 Rari 对 Alpha 的集成进行了审计，但在审计期间没有检测到该漏洞。

根据 CipherTrace 的研究，截止本报告发布时，针对区块链金融的攻击造成的损失总计达 9.94 亿美元，占 2021 年加密货币遭黑客攻击总量的 90%。区块链金融攻击和欺诈行为的增加表明，区块链金融相关的犯罪有明显的上升趋势，如下图所示：



资料来源：CipherTrace 加密货币情报

DeFi 黑客攻击和欺诈行为继续呈指数级增长



资料来源：CipherTrace 加密货币情报

2.1 案例研究

8 月 10 日，Poly Network 遭受了 6.12 亿美元的黑客攻击，这是迄今为止规模最大的与加密相关的黑客攻击。典型的 DeFi 黑客攻击针对特定的 DeFi 工具，所造成的损失要小得多。这次攻击针对保利网络（Poly Network）的基础设施，重点集中在 DeFi 平台本身，并针对去中心化交易所（DEX）的智能合约的控制。结果，主跨链合约完全被黑客控制，允许黑客解锁本应锁定在合约内的令牌，将令牌发送到他们控制的地址，然后跨多个链重复攻击。

该黑客在首次攻击后的几天内就返还了几乎所有的资金。然而，在本报告发表时，大部分返还资金约 2.35 亿美元仍在一个多签名的钱包中，处于 Poly Network 和黑客的控制之下。这意味着，如果没有黑客的私钥，Poly Network 就无法将资金从这个钱包中转移出来。到目前为止，该黑客一直拒绝释放他的私钥。

这一破纪录的黑客攻击事件证明了智能合约安全和审计标准对于确保代码质量和减少代码漏洞的重要性。随着 DeFi 黑客攻击和欺诈行为继续呈指数级增长，DeFi 犯罪的前景将很严峻。如果 DeFi 犯罪演变得更加复杂，智能合约很可能会成为更大规模攻击的目标。

过去三年较大规模的去中心化黑客攻击		
日期	协议	金额
2020 Q1	bZX	$318, 000
2020 Q1	bZX	$636, 000
2020 Q2	Bancor	$135, 229
2020 Q2	Bisq	$250, 000
2020 Q2	UniSwap	$300, 000
2020 Q2	Lendf.me	2500 万美元
2020 Q3	Balancer	$500, 000
2020 Q3	Yearn Finance (emmence)	1500 万美元
2020 Q3	Opyn	$371, 000
2020 Q3	bZX	810 万美元
2020 Q4	Cover Protocol	440 万美元
2020 Q4	Cover Protocol	400 万美元
2020 Q4	Value: DeFi	600 万美元
2020 Q4	Axion	$500, 000
2020 Q4	Warp Finance	770 万美元
2020 Q4	wLEO	$42, 000
2020 Q4	Cheese Bank	330 万美元
2020 Q4	Origin Protocol	700 万美元
2020 Q4	Pickle Finance	1970 万美元
2020 Q4	Akropolis	200 万美元
2020 Q4	Harvest Finance	2400 万美元
2021 Q1	Roll (WHALE, RARE, and PICA)	570 万美元
2021 Q1	DODO DEX	380 万美元
2021 Q1	PAID Network	316 万美元
2021 Q1	Furucombo (iouCOMBO)	1400 万美元
2021 Q1	CREAM Finance + Alpha Finance (Alpha Homora)	3750 万美元
2021 Q1	Year.Finance	1100 万美元
2021 Q2	EasyFi	8100 万美元
2021 Q2	Eleven.Finance	450 万美元

2021 Q2	Alchemix	650 万美元
2021 Q2	Bogged Finance	300 万美元
2021 Q2	Belt Finance	620 万美元
2021 Q2	Rari Capital	1000 万美元
2021 Q2	Value.Defi (governance RecoverUnsupported())	1000 万美元
2021 Q2	Value.Defi (vSwap AMM vSwap pools)	1100 万美元
2021 Q2	bEarn	1100 万美元
2021 Q2	Xtoken	2450 万美元
2021 Q2	Pancake Bunny	4500 万美元
2021 Q2	Spartan Protocol	3050 万美元
2021 Q2	Burger Swap	720 万美元
2021 Q3	Chainswap	80 万美元
2021 Q3	Chainswap	800 万美元
2021 Q3	ThorChain	500 万美元
2021 Q3	ThorChain	800 万美元
2021 Q3	AnySwap	790 万美元
2021 Q3	Bondly	590 万美元
2021 Q3	Levyathen	150 万美元
2021 Q3	Popsicle Finance	2000 万美元
2021 Q3	Poly Network	6.11 亿美元

3. 51% 攻击

51%攻击是对工作量证明（Proof Of Work）区块链的一种攻击，即一群控制着网络50%以上的挖矿哈希值的矿工利用这种控制力阻止新的交易被确认，或推翻在控制下完成的交易，导致双花攻击（double-spend attack）。一旦发生这种情况，往往没有任何区块链技术可以阻止这种攻击。51%的攻击导致的最大损失是丧失区块链的信心。

知名的 51%攻击影响范围包括：

- Krypton
- Shift
- MonaCoin
- Bitcoin gold
- Zencash
- Litecoin Cash
- Feathercoin
- Vertcoin
- Bitcoin Gold
- Ethereum Classic
- Verge
- Bitcoin SV

3.1 案例研究

2020 年 8 月，ETC 经历了一次 51%的攻击，造成 7000 多个区块的重组，大约相当于两个采矿日。四个主要的交易所受到双花的影响，造成 460 万美元的损失。

3.2 缓解 51%攻击

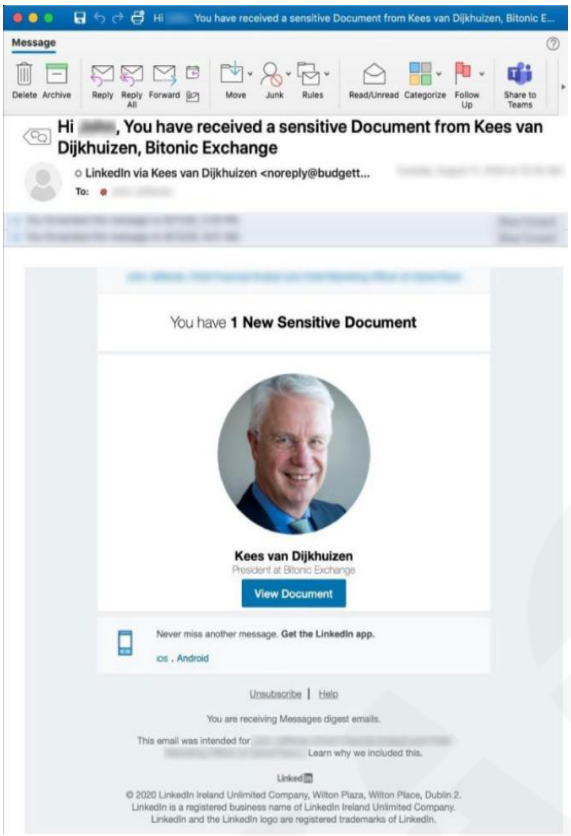
51%的攻击导致的双花给区块链带来了安全和信任问题。一种改善安全协议和控制的方式可以通过交易所完成。一些交易所要等待 6 个确认区块深度才允许使用货币，并且一旦区块链通知交易所攻击正在进行，则可能会扩展到 30 个或更多的确认区块深度。其目的是让 49%的少数矿工有更多的时间重新获得区块链的哈希值并挫败攻击。这对交易所有利，因为他们不会因为双花而损失货币。

4. 钓鱼

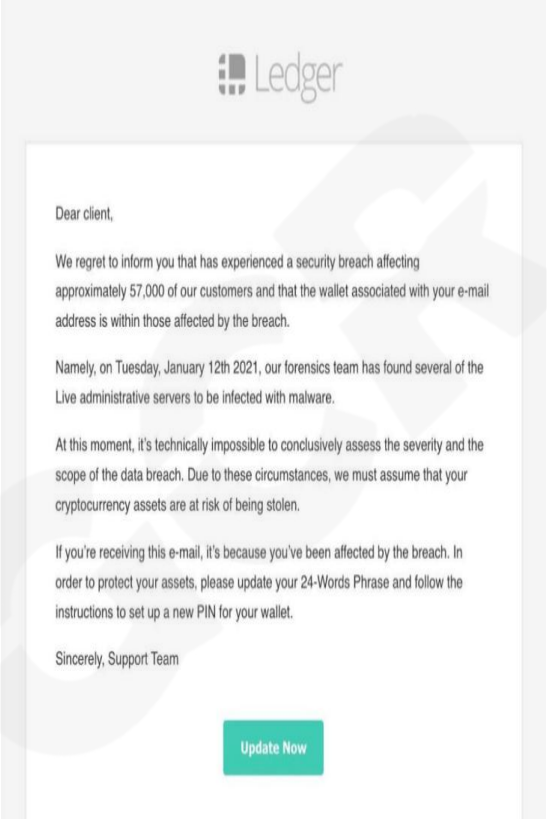
钓鱼攻击在区块链经济内外都很常见。在传统的网络钓鱼攻击中，犯罪分子会通过广撒网和群发邮件来“钓 取”目标，冒充合法机构来欺骗读者提供敏感数据，如用户名、密码、银行和信用卡信息以及其他个人身份信息。网络钓鱼已经超出了电子邮件的范围，包括电话、短信和社交媒体平台。

在加密空间中越来越常见的是非常有针对性的鱼叉式钓鱼攻击。在这些类型的攻击中，犯罪分子拥有关于受害者的额外细节，他们可以利用这些细节来定制他们的攻击，而且往往看起来是来自更值得信赖的来源。

在加密货币硬件钱包供应商 Ledger 的数据泄露后，许多买家收到了鱼叉式钓鱼邮件，声称用户需要使用所提供的链接更新他们的种子短语。然而，这样做的结果是攻击者获得了用户的私钥副本，使他们完全控制了 Ledger 所持有的所有加密货币。



叉式钓鱼攻击的例子，该攻击似乎来自 LinkedIn 上的一个联系人，该联系人是基于一个真实的银行高管身份。



Ledger 数据泄露后的钓鱼攻击样例

针对加密货币用户的常见网络钓鱼攻击途径包括：

- 冒充目标使用的钱包提供商或交易所的鱼叉式钓鱼电子邮件
- 冒充合法加密货币钱包提供商和交易所的独特钓鱼网站
- 社交媒体（Reddit、Twitter、Telegram）上的欺诈团体和人员在寻找机会时进行的鱼叉式钓鱼攻击

4.1 案例研究

虽然大多数人可能认为网络钓鱼攻击就是欺诈性的电子邮件，但加密货币黑客有许多途径可从中钓鱼获取私钥。。在过去的一年中，最引人注目的钓鱼攻击之一来自于一个普通加密货币钱包应用程序的欺诈性谷歌广告。

2020 年 12 月初，CipherTrace 分析师注意到，在线加密货币社区内关于用户资金被冒充加密货币钱包和浏览器扩展 MetaMask 的 Chrome 浏览器扩展钓鱼攻击的警报和评论有所上升。欺诈性的浏览器扩展将信息指向 maskmeha[.]io，随后重定向到 https[:]/installmetamask[.]com。该钓鱼网站完美地镜像了真正的 MetaMask 网站。

当$WHALE 社区在 Medium 上发表了一篇文章，指示用户将$WHALE 资金发送到 MetaMask，并引用欺诈性的 https[:]//installmetamask[.]com 域名作为 MetaMask 钱包的下载页面时，这个问题变得更加复杂。这很可能是原始发帖人做了快速搜索，并复制了他们发现的第一个链接。而由于该钓鱼网购买了谷歌广告，使得该网站出现在任何谷歌搜索的顶部，这凸显了此类网络钓鱼攻击的危险性，因为可信的来源使钓鱼网站具有可信性。

5. 抽地毯/退出骗局

在加密货币领域，退出骗局是指交易所带着用户资金消失，似乎是突然发生的，让客户无法从账户中提取。这通常是执行团队的一名或多名成员挪用用户资金的结果，可能是在交易所成立之初就计划好的，也可能是由于没有足够的保障措施防止挪用而突然发生的。

抽地毯与退出骗局类似；两者都涉及内部人员带着大部分（如果不是全部）的用户资金离开。虽然二者经常互换使用，但退出骗局更经常与已建立的实体或项目意外关闭（“退出”）有关，会带走用户的资金。例如，在 2020 年 11 月，DeFi 的 SharkTron 项目似乎蒙受了退出骗局并损失了 1000 万美元的用户资金，关闭了其网站，让用户蒙在鼓里。

另一方面，抽地毯是一种特定类型的退出骗局，涉及通过出售 DeFi 池的大部分货币，从投资者（用户）手中 “抽出地毯”，从而耗尽特定货币的流动资金。抽地毯通常是通过写在智能合约中的故意后门完成的。在 DeFi 的 Compounder.Finance 项目案例

中，写在智能合约中的一个隐藏的后门使得开发者在 2020 年 11 月从项目的流动池中抽出 1080 万美元。

DeFi 项目 Unicats 在 10 月份也进行了类似的抽地毯，耗尽了用户的全部资金。这两个骗局都强调了用户审查其资金平台的重要性。无论是在中心化的交易所还是去中心化的应用程序中，用户都应该检查平台，仔细寻找任何危险信号。所有的核心开发者都是匿名的吗，就像 WhaleFarm 抽地毯一样？智能合约是否经过社区审核和审查？白皮书是否可疑地短小含糊？平台的奖励保证是否好得不像真的？创始人或执行团队的可信度如何？这些只是审查项目时需要考虑的几件事。

5.1 案例研究

2019 年初，加密货币社区被 QuadrigaCX 的爆炸新闻所吸引，QuadrigaCX 公司曾是加拿大最大的加密货币交易所。2019 年 1 月 14 日，QuadrigaCX 客户第一次得知该公司 CEO 杰拉尔德·科顿（Gerald Cotten）一个多月前去世。他的遗孀在 QuadrigaCX 网站上发布公告称，科顿在印度一家孤儿院开幕的时候去世。大约在科顿被报道死亡的时候，客户们开始报告他们的加密货币在退出交易所时遇到了麻烦，导致许多客户相信交易所的资金和 CEO 一起消失了。2 月 9 日，有消息称事实上，科顿把公司所有加密资产的密码带到了另一个世界。QuadrigaCX 的客户震惊地发现他们的加密货币无法访问。

在 1 月 31 日提交给新斯科舍省（Nova Scotia）最高法院的宣誓书中，他的遗孀詹妮弗·罗伯逊（Jennifer Robertson）表示，该交易所欠其客户大约 2.5 亿加元（1.95 亿美元）的加密货币和法定货币。QuadrigaCX 的客户得知该交易所向新斯科舍省最高法院提交了债权人保护申请后感到愤怒，声称在找回“存放在冷钱包中的非常重要的加密货币储备”方面存在问题。

法院在 uadrigaCX 破产案中任命的监督方安永会计师事务所(Ernst and Young, EY）于 2019 年 6 月发布了第五份报告。据报道，科顿涉嫌多年来利用客户资金为自己和妻子（当时的女友）致富。大量客户的加密货币从 Quadriga 平台转入科顿在竞争对手交易所控制的账户。然后，Quadriga 客户的加密货币要么在这些交易所交易，要么作为科顿建立的个人保证金交易账户的抵押品。Quadriga 的加密货币储备最终因其交易损失以及这些竞争对手交易所收取的增量费用而受损。

安永还声称，科顿将 Quadriga 的用户资金视为个人银行账户，已确认向科顿及其

妻子詹妮弗·罗伯逊（Jennifer Robertson）进行了大量法定货币转账。他们两人度过了昂贵的假期，乘坐私人飞机，并购买了大量房产。他们积累的资产包括房地产、现金、一架飞机、一艘帆船、豪华汽车以及金币和银币，价值约 1200 万加元。

最后，报告指出了 Quadriga 运营基础设施中的重大缺陷，这一缺陷最初占据了世界各地的头条新闻。“此外，监督方还了解到科顿一个人持有密码，并且似乎 Quadriga 未能确保制定适当的安全程序，以便在发生关键事件（如关键管理人员的死亡）时将密码和其他关键操作数据传输给其他 Quadriga 代表。”

6. 勒索软件

在 Colonial Pipeline 和 Kaseya 黑客攻击之后，勒索软件继续困扰着全球的公共和私营部门。勒索软件不仅仅是简单的金融犯罪，例如近几个月来，这些袭击影响了医院提供救生护理的能力，也影响到公用事业可靠地满足客户对电力等基本需求的能力，而政府所有级别的机构都遭受了敏感数据泄露威胁。

Revil、Netwalker 和 Darkside 等勒索软件即服务业务的快速增长成为威胁者有利可图的生意。最近针对关键基础设施的这些攻击证明了勒索软件不仅影响个人。2021 年 6 月 3 日，美国司法部、国防部宣布将优先处理勒索软件事件，将其列为对国家安全的重大威胁。联邦调查局局长克里斯托弗·雷最近就该局把工作重点转到全球勒索软件威胁与当年在 9/11 事件后转向全球恐怖主义相比较。根据雷的说法，FBI 目前正在调查 100 多种不同的软件变种勒索软件攻击。

为了充分对抗勒索软件，信息共享是关键。6 月中旬，RAAS 运营商 REvil 宣布，它已经更新了其宗旨和目标，以供在选择攻击目标时考虑，包括将学校和医院从勒索软件受害者中去除。此更新很可能是为了 REvil 的形象考虑，以免成为美国司法部的优先目标。

6.1 勒索软件即服务（RaaS）

在 RaaS 操作模型中，恶意软件开发人员与第三方分支机构（黑客）合作，后者负责获取网络访问权限、加密设备和协商赎金、让受害人付款。由于这种相对较新的模式，勒索软件现在可以很容易地由一些不良行为者使用，他们缺乏自己创建恶意软件的技术

能力，但非常愿意并能够渗透目标。

随后赎金在附属公司和运营商（开发商）之间获得分配。勒索软件运营商和导致感染的附属机构之间的这种分裂通常是 RaaS 的警示信号。在大多数 RaaS 模型中，运营商的分成比例为 15-30%，附属公司的分成比例为 0-85%。

6.2 打击勒索软件

区块链分析提供了追踪勒索软件所需的关键加密货币情报。只有通过像勒索软件特别工作组这样的组织合作，加密货币情报公司才能应对这些威胁。关键是不仅要追踪勒索软件的收益，找到并阻止经营者，也要加强制度建设，并教育公众这些如何发生。事件响应公司和网络安全组织拥有客户支付赎金的庞大数据库；识别跟踪这些资金可以帮助建立勒索软件集团的完整档案。

由于勒索软件的参与者使用公共区块链来接收付款，因此所有交易都可以在链上查看，使执法部门（或任何人）能够追踪资金流向。利用区块链分析工具为追踪和调查提供了额外的情报，例如用于识别资金何时存入交易所。一旦资金达到集中交易，执法部门可以通过要求交易所冻结账户，如果用户必须经历 YC 流程，则可以识别地址背后的个人。

6.3 将损害降至最低的最佳做法

公司可以采取几个步骤来最大限度地减少勒索软件攻击造成的损害。

预防措施包括：

- 准备事件响应/业务连续性计划，并在攻击发生前准备就绪。
- 选择一家使用有效区块链进行分析的事件响应公司，并使用加密货币智能软件，如 CipherTrace，跟踪加密货币支付给黑客的款项。
- 考虑购买网络安全保险。
- 备份系统并测试备份。
- 启用日志以确保您可以在支付赎金之前收集尽可能多的有关黑客和攻击的信息。
- 评估进行勒索软件支付是否违反制裁规定。制裁违规行为可能导致昂贵的民事罚款，甚至被勒索方入狱。

应对措施包括：

- 用比特币支付。避免使用匿名增强技术或隐私币支付赎金。通过这种方式，调查人员可以更容易地跟踪资金流，以确定潜在的关闭跟踪和协助扣押资产。
- 向国家执法部门报告所有勒索软件攻击。

7. SIM 卡交换攻击

在 SIM 卡交换攻击中，黑客使用社会工程手段（包括从黑市购买的被盗凭据）欺骗电信提供商将受害者的电话号码转移到他们控制的 SIM 卡（物理或虚拟）。技术的进步使得服务提供商的客户服务团队可以快速地将号码转移到新的 SIM 卡上，从而加剧了这种情况。这通常是为用户的电话丢失或被盗的情况而保留的。曾经的网络罪犯收到电话号码后，他们可以用它来重置密码并侵入受害者的账户。包括加密货币交易所的账户。大型加密货币投资者越来越多成为此攻击的目标，通常从黑客通过网络钓鱼电子邮件或从暗网购买来收集有关受害者的信息开始。

7.1 SIM 卡交换攻击的工作原理

这种攻击通常是通过社会工程手段或通过勾结内部人员发起的，通常是在零售点。硅谷 REACT 任务小组的约翰·罗斯中尉说：“如果你在一家手机店工作，每小时挣 12 美元，突然有人给你 400 美元，让你换一张 SIM 卡，这看起来是一笔相当不错的交易。”

使用窃取的身份，黑客联系受害者的移动服务提供商，并要求提供商将受害者的电话号码移植到诈骗者的 SIM 卡。

通过使用 SIM 交换，黑客可以抑制安全警报或通知，因为一旦电话号码被切换到黑客的 SIM 卡，受害者的电话没有语音、电子邮件或短信服务。因此，他们不知道任何极不寻常的转移，直到窃贼带着他们的资金逃走。

7.2 防止 SIM 卡交换攻击

阻止SIM卡交换对于用户来说几乎是不可能的,这是由于他们手机公司的业务流程。用户可以通过不使用他们的电话号码来进行以SMS或移动电话呼叫为第二因素的双因素身份认证及二步验证，以减少 SIM 卡更换攻击的影响。在可能的情况下，用户应使用更强大的 2FA/MFA 因素，例如基于应用程序的双因素身份验证，甚至是硬件钱包。

此外，客户还可以致电其电话提供商并启用单独的 PIN。例如：全部 T-Mobile 帐户

分配有 6-15 位数的 PIN。所有帐户都有此保护，客户的在未验证该 PIN 的情况下，无法移植号码。当顾客打电话给客服中心时，也会使用此 PIN 验证身份。[1]

7.3 案例研究

2018 年初，一名黑客使用这种技术，据称从一名富有的投资者那里窃取了 2380 万美元。顺便说一句，他正在起诉美国电话电报公司（AT&T），要求赔偿被盗的数百万美元以及另外 2 亿美元惩罚性赔偿。到 2018 年秋季，黑客使用 SIM 卡交换攻击来侵入 CrowdMachine，一个总部位于加州的加密货币初创公司，并窃取了其所有的储备币，价值 1400 万美元。在 2018 年 7 月，保加利亚警方逮捕了 3 名嫌疑人，他们涉嫌通过 SIM 卡交换窃取 500 万美元。同月，加州警方指控一名 20 岁的大学生盗窃 500 万美元。2018 年 11 月，硅谷 React 团队逮捕了一名涉嫌盗窃 100 万美元的 21 岁男子，他使用了相同的技术。

2021 年 2 月，欧洲执法机构欧洲刑警组织（Europol）逮捕了 10 人，原因是他们在 2020 年期间参与了一系列针对数千名受害者的 SIM 卡交换攻击，其中包括著名的互联网名人、体育明星、音乐家及其家人。袭击者估计有价值 1 亿美元的加密货币被盗。

SIM 卡交换攻击通常有三种主要类型：

- 社会工程

例如：你好，我的手机丢了，我有紧急情况，我需要尽快将我的电话号码转移到新手机上，因为我在等一个非常重要的电话，是的，我知道我的社会安全号码，家庭住址和猫的名字。[2]

- 侵入具有以下特征的实体（如购物中心的手机信息亭）的计算机，对端口电话号码的特权访问。这是通过网络钓鱼、物理攻击等。
- 手机公司的内部人员向攻击者出售 SIM 卡进行攻击。

有关避免 SIM 卡交换攻击的其他有用建议，请访问不列颠哥伦比亚大学（the University of British Columbia）的隐私问题网站。

[1] Jacinto, P. (2020, July 7). *How T-Mobile Helps Customers Fight Account Takeover Fraud.* T-Mobile Newsroom.https://www.t-mobile.com/news/press/how-to-fight-account-takeover-fraud

[2] Franceschi-Bicchierai, L. (2019, May 13). *AT&T Contractors and a Verizon Employee Charged With Helping SIM Swapping Criminal Ring.*Vice.https://www.vice.com/en/article/d3n3am/att-and-verizon-employees-charged-simswapping-criminal-ring

8. 投资骗局

投资骗局是披着新外衣的旧骗局——BitConnect 就是一个很好的例子。这很简单：您购买 BitConnect Coins（BCC），然后通过托管借贷投资 BitConnect Coins 平台（BitConnect.Co）。其他人借了 BitConnect 币，做了一些事情，然后偿还了贷款。从表面上看，对于缺乏经验的投资者来说，这听起来并不过分欺诈。BitConnect 声称每天的回报率为 1%，这是一个高得不能再高的持续回报率。这也表明任何借用 BitConnect 的人都需要每天支付至少 1%的费用,这应该是一个的危险信号——要么你是在向高利贷者借钱，要么你的投资风险太大。你可能不应该借钱从事这种高风险的活动。

不出所料，BitConnect 被证明是一个庞氏骗局（Ponzi scheme，早期投资者只是得到了来自后来的投资者的回报）。只要投资增加，庞氏骗局就会起作用，但在某些时候，可用的投资者将会枯竭，或者有人会认定这是一个庞氏骗局（破坏投资者信心）。2018 年 1 月，德克萨斯州证券委员会（Texas State Securities Board）向该公司发出停止令，称其为庞氏骗局，原因是该公司在用户收益透明度方面存在缺陷和误导性陈述，BitConnect 关闭，BitConnect 币的价格暴跌。

随后出现了后续骗局：一种名为 BitConnect X（BCCX）的二次硬币和一种首次代币发行（ICO）的尝试。尽管各法院都发布了停止令，但不清楚是否有任何法律实体（如公司）实际适用指令。随后在印度逮捕了一人，但没有追回任何资金。当然，投资者损失了大部分或全部资金（除了那些购买了 BitConnect（BCC）币的人，由于 BCC 的价值崩溃，他们没有将其借出）。

三年多后的 2021 年 5 月，美国证券交易委员会（SEC）提起民事诉讼，在曼哈顿联邦法院对虚拟资产 BitConnect 的五名发起人提起诉讼。这个诉讼称，这五人在推销未注册的证券前，没有按照法律要求注册为经纪人，就从散户投资者那里筹集了 20 多亿美元。

这不是美国证券交易委员会（SEC）第一次指控虚拟货币推销商欺骗散户投资者。那些希望推广虚拟货币的人应该谨慎行事，因为这类行为可能构成证券销售。在美国证券交易委员会提起诉讼之前，BitConnect 已经存在三年多，这一事实表明他们愿意违反《证券法》（Securities Act），无论这种行为是何时发生。

9. 高调倍增骗局

比特币倍增骗局很简单，通常由犯罪分子在社交媒体上传播。倍增骗局向新投资者承诺——通常以知名人士为幌子——只需将资金发送到一个特定的地址，他们便可获返还最初投资的双倍资金。这些骗局通常对时间很敏感，会促使受害者产生紧迫感，希望他们不太可能对提议进行批判性思考。

这些诈骗通常针对的是不太熟悉加密货币的用户，骗子通常会伪装成比尔·盖茨（Bill Gates）或埃隆·马斯克（Elon Musk）这样的高净值个人，打着他们试图回馈社区的幌子。这通常是通过分享篡改社交媒体帖子的屏幕截图， 或修改过去直播的视频来完成的，其中包含新嵌入的信息，敦促人们将资金发送到特定地址。这些骗局有时会通过使用包含知名人士姓名的虚荣地址获得额外的合理性。

这些骗局通常很容易识别，因为它们是通过新账户广播出，和他们与之相关的知名人士没有任何关联。然而，在 2020 年 7 月，推特上的多个受信账户遭到黑客攻击。随后，黑客得以在全球范围内制造出一个备受瞩目的倍增骗局——这是同类骗局中规模最大的。最终，这名推特黑客从 430 多名受害者那里窃取了 12.5 万美元，其中大部分是在许多知名的、与加密货币无关的账户遭到入侵之后发生的。

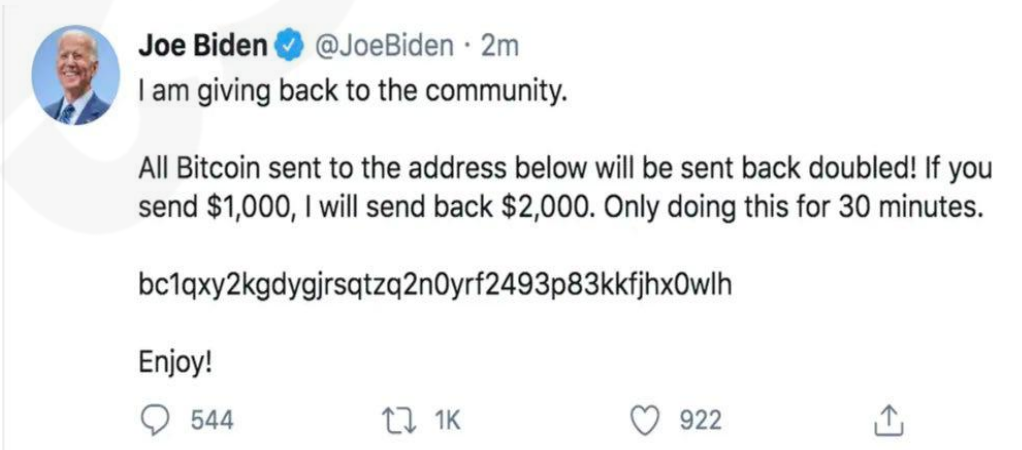
9.1 案例研究

2020 年 7 月 15 日，多个知名的加密货币交易所、公众人物和各种实体的 Twitter 帐户被黑客接管，以宣传比特币倍增骗局。 与加密货币相关的流行用户

AngeloBTC、币安（Binance）、币安 CEO 赵长鹏（Changpeng zhao）、CoinDesk、Coinbase、Gemini、Kucoin 和波场（Tron）创始人孙宇晨（Justin Sun） 的 Twitter 账户被黑客入侵。 这些帐户中的每一个都发布或转发了以下内容：

该网站声称将分发 5000 个 BTC 作为赠品，条件是如果个人向捐赠地址发送 0.1 个 BTC 到 20 个 BTC，那么 Cryptoforhealth 将返还两倍的金额。

在最初的推特浪潮之后，包括杰夫·贝佐斯（Jeff Bezos）、优步（Uber）、巴拉克·奥巴马（Barack Obama）、乔·拜登（Joe Biden）和埃隆·马斯克（Elon Musk）在内的多个账户遭到入侵。这些被泄露的账户直接引用了比特币加倍骗局，其中还包括了比特币存款地址，而不是将受害者重定向到一个网站。结果，所提供地址中的比特币数量开始飙升。



截图来自美国总统乔·拜登（Joe Biden）被盗推特账户，宣传此骗局

9.2 缓解倍增骗局

虽然利用多个验证 Twitter 账户等信任标记是为了欺骗用户，让他们认为比特币倍增骗局是合法的，但与被入侵账户的广泛覆盖范围相比，黑客获得的金额微不足道。这可以归结为两个主要因素：一是正当交易所的反洗钱（AML）系统实施阻止了新用户在诈骗高峰期向黑客发送他们的代币，二是当涉及到常见的加密币诈骗时，加密币用户对此更加了解了。

大多数诈骗受害者可能已经在数字货币交易所开设了账户，因为即使是通过自动清算系统（ACH）转账，在信誉良好的交易所开设账户并在一天内完成存款和转账几乎是不可能的。在可以更快地开户的交易所中，用户通常会要求以电汇的方式而不是自动清算系统的方式进行法定存款。在电汇完成之前，这些账户将无法交易任何加密货币，这可能需要三天时间来完成。而这正可能阻止了黑客利用那些尚未持有加密货币或在交易所维持账户的人。

10. 勒索

自从加密货币被广泛采用以来，网络敲诈企图急剧增加。其中有一种特别常见的勒索方式——“性勒索”。犯罪分子可以使用来自 Yahoo!、Experian 和 Facebook 漏洞所盗取的数据来个性化他们的通信，以欺骗电子邮件收件人，让他们相信自己被录下了观看网络色情或参与其他危害他人的活动。在一个例子中，勒索者威胁要公开一段分屏视频，其中一半显示正被进行勒索的接收者，另一半则显示他们当时正在观看的视频。这位“性勒索者”提出，如果受害者将付款发送到一个比特币地址中，就可以让他们脱身。

有时，勒索者声称已经用恶意软件感染了一个色情网站，利用受害者的电脑记录按键，以访问显示屏和网络摄像头。勒索邮件显示的是过去某个时间点的真实密码。然而，这些密码是通过数据泄漏得到的而不是通过受感染的站点所获取的。 这些鱼叉式网络钓鱼攻击为电子邮件增加了一层真实性，增加了受害者付款的可能性。

诈骗者进一步声称已经获取了受害者的通讯记录，并威胁他们说，如果没有收到赎金，他们就会把视频发送到名单上的人。赎金通常在几百美元到一千多美元不等。CipherTrace 对在线勒索支付地址的分析表明，大多数这些在线勒索邮件都是极具欺诈

性的，但这些邮件足够吓人，即使是无辜的受害者也可能出于恐惧而支付赎金。

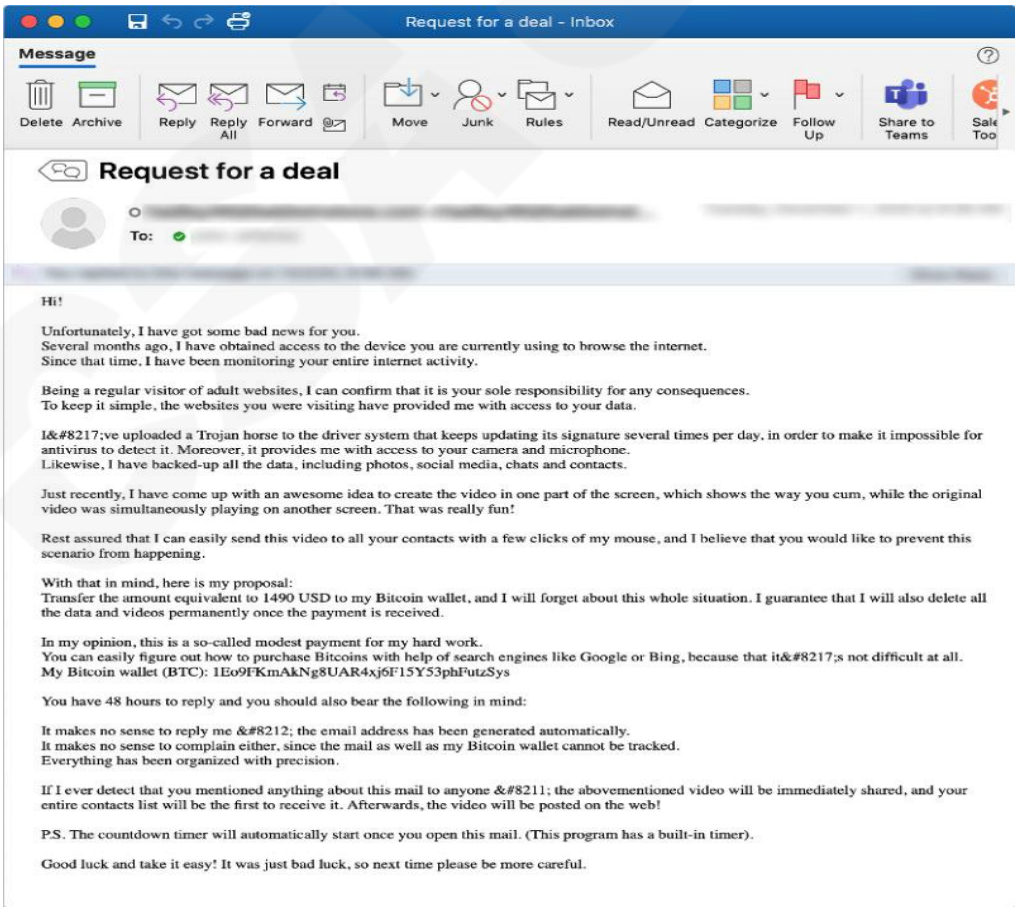
10.1 防止勒索攻击

通常情况下，这些勒索骗局都是假的——这意味着支付或不支付都将导致相同的结果：什么事都没有。建议不要为勒索骗局支付或回复这些电子邮件。

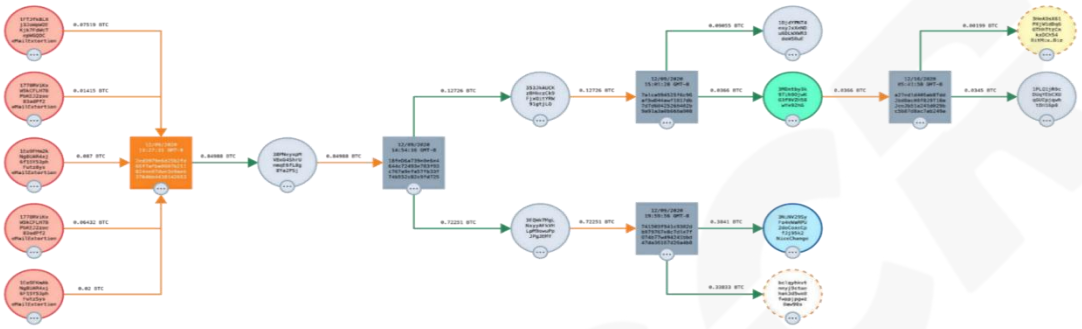
勒索诈骗通常通过鱼叉式网络钓鱼获得合法性。 为了保护自己免受此类攻击，人们可以做的一件事是冻结所有信用机构账户，如 Equifax、Experian、Transunion、Innovis 和 NCTUE（由 Equifax 所有）。 APWG 加密货币工作组还建议消费者通过致电 1-888-5-OPT-OUT (1-888-567-8688) 或访问 OptOutPrescreen.com 选择退出预先批准的信用优惠，并选择退出主要数据经纪人，包括 Lexus Nexis (https://optout.lexisnexis.com/) 和 Acxiom (www.aboutthedata.com)。

10.2 案例研究

下面是一封勒索邮件的真实文本：



对这个地址 1Eo9FKmAkNg8UAR4xj6F15Y53phFutzSys 在区块链链上数据分析显示，共有 20 名受害者被勒索诈骗。如下图所示，在洗钱过程中，诈骗者将合并资金转移到混币服务中，混淆资金流动，从而更难识别他们使用了哪些加密货币交易所作为出口。加密货币交易所通常用于将加密货币转换为法定货币，以便在现实世界中使用；然而，现在许多人收集 KYC 信息，如果调查人员能够跟踪加密货币，就可以识别骗子。



资料来源：CipherTrace 加密货币情报

11. 额外红利：钱包安全

11.1 伪造的软件钱包

创建移动端应用程序并将其在 Apple 或者 Google Play 应用程序商城上架并非是不可能的。截至本报告发布时，Apple 应用商店中有 196 万个应用，Google Play 应用商店中有 287 万个应用。 虽然两家公司都在努力确保恶意应用程序不会被上架，但由于其应用程序数量庞大，要阻止所有的此类恶意应用程序上架当然是不可能的。

许多恶意软件钱包已通过这两个应用程序商店发布。它获利的原理很简单：制作一款“山寨”应用并将其投放到应用商店只需花费几千美元。而即便只有一个用户上当受骗，攻击者就能轻松获利。[3]

由于一个组织有能力创建看起来很专业的应用程序和网站，并为应用程序评级刷分（谷歌搜索“购买应用程序评级”，你会看到大量的公司广告），用户很难确定一款应

[3] Albergotti, R. (2021, March 30). *He believed Apple's App Store was safe. Then a fake app stole his life savings in bitcoin.* Washington Post.https://www.washingtonpost.com/technology/2021/03/30/ trezor -scam-bitcoin-1-million/

用程序是“真实的”还是“伪造的”。随机挑选一款软件钱包，结果会发现：

- 一个看起来合法的申请和企业名称
- 应用中的企业名称和开发公司名称不完全匹配
- 一名自称是乌克兰人的 CEO
- 一家自称拥有约 12 名员工的美国公司
- 没有搜索到这家公司的记录
- 在 Apple 应用商店中，该应用程序只有一条五星评价。而在 Google Play 应用商店中则有近 2000 条评价。

缺乏评论（仅在 Apple 应用商店中有一条评价，而在 Google Play 应用商店中有近 2000 条评价），再加上无法搜索到该公司（除了一个官网外），表明这可能是一个骗局。单独一条应用评价显得很奇怪 —— 骗子通常会花钱为其 Apple 应用程序获得正面评价。此外，开发者对 Google Play 应用商店中的任何负面评论都会做出回应，所以这要么是一个长期骗局，要么开发者主要关注 Android 市场而不是 Apple 市场。

最后，要确定一个移动应用程序的可信度是非常困难的，除非它来自一家非常大的知名公司。此外，即使你能验证该应用程序，他们也可能将应用程序或公司出售给第三方；例如：有记录表明恶意人员正试图购买 Web 浏览器扩展插件。[4]

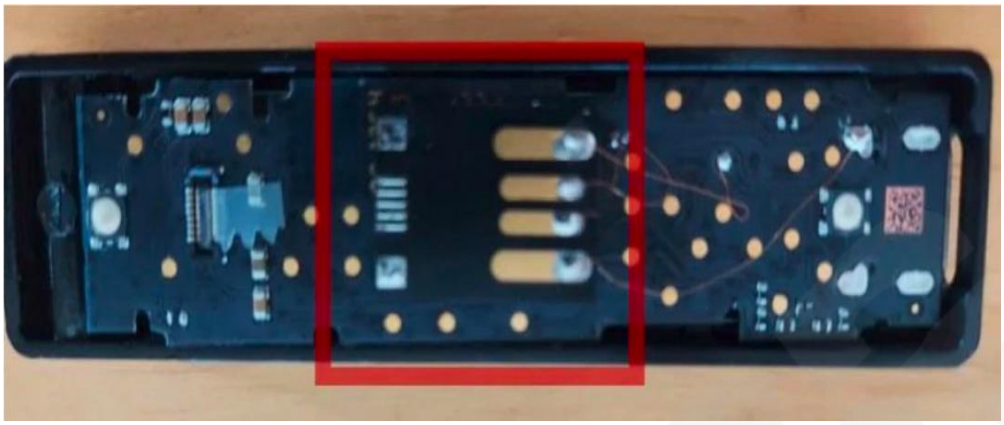
11.2 伪造的硬件钱包

目前有两类硬件钱包：一类是用于插入计算机的 USB 接口，本质上像一个密钥管理服务；另一类实际上是一个自带屏幕的计算机，其可以通过扫描和展示二维码来进行数据传输。对于 USB 设备来说，其无法确认用户插入的计算机是否安全是一个显而易见的事实。[5] 例如，攻击者可以在接入计算机时加载 USB 设备中的恶意程序并自动执行，也可以通过配置 USB 设备向计算机发送指令（例如，伪装成键盘或鼠标）。如果用户拆解这些设备并进行检查就可以发现，如额外焊接的引线、芯片的改装。需要注意的是，

[4] *Many temptations of an open-source chrome extension developer · Discussion #670 · extesy/hoverzoom. (n.d.)*. GitHub. Retrieved September 9, 2021, fromhttps://github.com/extesy/hoverzoom/discussions/670

[5] Open Source Security. (April 21, 2019). *Hypothetical security: What if you find a USB flash drive?* Open Source Security Podcast.https://opensourcesecurity.io/2019/04/21/episode-142-hypothetical- security-what-if-you-finda-usb-flash-drive/

如果攻击者构建一个定制的电路板并制造它（每块电路板不到 10 美元就可以小批量制造）的唯一方法是将硬件与制造商的原理图（这些原理图一般都无法获得）进行比较。



资料来源：比特币杂志

2020 年，硬件钱包公司 Ledger 发生了数据泄露。随后，攻击者向 Ledger 的客户邮寄了“新的”硬件钱包，而这些钱包被修改过，在插入电脑时可以运行恶意软件。据报道，在 2021 年，有多起得到证实的事件关于有用户收到新的收缩包装的硬件钱包以及 Ledger CEO 的一封信。这些硬件钱包被改装新增一个 USB 存储芯片。较早的报告包括用户在亚马逊上购买硬件钱包，但硬件钱包已经被初始化（这是用户应该做的步骤，以确保其被安全地设置）。如果用户使用了一个已经初始化的硬件钱包，那么攻击者就拥有用于恢复硬件钱包的助记词，进而使得攻击者可以劫持与该硬件钱包相关的任何资产[6]

一般来说，在购买硬件钱包时，最好直接从厂商处购买，并确保有遵循其设置和初始化流程。对于来路不明的硬件钱包，就像厂商主动提供的支持或电子邮件一样，应该直接忽略或者反馈给相应的厂商。从理论上讲，任何硬件设备都可以被拆卸并检查是否有多余的引线/芯片——但实际上大多数用户并不会这么做，且对于有足够动机和资金的攻击者来说，其有可能使用伪造或重新贴牌的芯片或在真实芯片中加载了恶意软件制造出一个看起来与真品相同的电路板。

[6] *Ongoing phishing campaigns.* (2021, June 17).Ledger.https://www.ledger.com/phishing- campaigns-status

总结

有一个很大的误区：用户会认为分布式账本技术（DLT）系统的不可篡改性和区块链技术的加密性使得其天生是安全的。然而，正如本文所说明的，情况并非如此。未经审计的智能合约可能会导致 DeFi 平台遭到大规模黑客攻击。如果一个人或组织拥有大量的算力，则一些算力较小的区块链将面临 51%攻击的风险。新手很容易成为常见的诈骗和勒索手法的受害者。而钓鱼攻击将持续以 DLT 系统背后的人作为目标，造成从中心化交易所被黑到个人私钥被盗的各种事件。

这 10 种 DLT 攻击类型突出了造成全球加密货币丢失的最常见威胁途径：

- 交易所黑客攻击
- DeFi 黑客攻击
- 51%攻击
- 钓鱼（为了获得私钥）
- 抽地毯/退出骗局
- 勒索软件
- SIM 卡交换攻击
- 投资骗局
- 高调倍增骗局
- 勒索

许多虚拟资产可以轻松的兑换为法定货币，这使它们成为许多基于线上犯罪的目标和机制。加密货币的即时、伪匿名特性使勒索软件和在线敲诈等新的犯罪商业模式成为可能。随着中心化交易所加强了其云安全管控，攻击者转而以个人用户为目标进行社会工程学攻击以及信任诈骗。幸运的是，由于大多数区块链的开放性，区块链分析工具提供了前所未有的虚拟资产追踪能力。以调查加密货币犯罪，扣押资产并起诉不法分子。

参考材料

Albergotti, R. (2021, March 30). *He believed Apple's App Store was safe. Then a fake app stole his life savings in bitcoin.* Washington Post. https://www.washingtonpost.com/technology/2021/03/30/ trezor-scam-bitcoin-1-million/

Franceschi-Bicchierai, L. (2019, May 13). *AT&T Contractors and a Verizon Employee Charged With Helping SIM Swapping Criminal Ring.* Vice.https://www.vice.com/en/article/d3n3am/att-and- verizon-employees-charged-simswapping-criminal-ring

Jacinto, P. (2020, July 7). *How T-Mobile Helps Customers Fight Account Takeover Fraud.* T-Mobile Newsroom. https://www.t-mobile.com/news/press/how-to-fight-account-takeover-fraud

Many temptations of an open-source chrome extension developer · Discussion #670 · extesy/hoverzoom. (n.d.). GitHub. Retrieved September 9, 2021, from https://github.com/extesy/hoverzoom/discussions/670

Ongoing phishing campaigns. (2021, June 17). Ledger.https://www.ledger.com/phishing-campaigns- status

Open Source Security. (April 21, 2019). *Hypothetical security: What if you find a USB flash drive?* Open Source Security Podcast. https://opensourcesecurity.io/2019/04/21/episode-142-hypothetical- security-what-if-you-find-a-usb-flash-drive/