Cobo 安全团队：WazirX 被盗币事件分析

Cobo 安全团队针对近期印度加密货币交易所 WazirX 被攻击事件进行了详细的分析，并从风险控制机制、安全体系等方面分享了 Cobo 如何帮助客户抵御网络攻击。

1 事件概述

2024 年 7 月 18 日，印度加密货币交易所 WazirX 的一个多签钱包被盗超过 2.3 亿美元。该多签钱包为 Safe{Wallet} 智能合约钱包。攻击者诱导多签签名者签署了合约升级交易，攻击者通过升级后的合约直接转移了钱包中的资产，最终将约超过 2.3 亿美元的资产全部转出。

2 攻击过程分析

注：以下分析基于 WazirX 和 Liminal 事后报告、链上数据、互联网公开信息，可能存在信息不全或误差，从而导致分析结论有所偏差。分析结果仅供参考，具体以当事厂商后续调查结果为准。

原文链接：

WazirX 博客：https://wazirx.com/blog/wazirx-cyber-attack-key-insights-and-learnings/

Liminal Custody 博客：https://www.liminalcustody.com/blog/update-on-wazirx-incident/

2.1 多签钱包配置与攻击过程

根据双方披露的信息，WazirX 使用 Safe (前称 Gnosis Safe) 进行资金管理，并通过 Liminal 进行协管。该 Safe 钱包采用 4/6 的签名方式，其中 5 把私钥为 WazirX 成员通过硬件钱包管理，1 把私钥由 Liminal 通过 HSM 管理。

正常流程下，WazirX 通过 Liminal 平台的网页发起交易转账，转账地址受 Liminal 平台维护的地址白名单限制。WazirX 的 5 位签名者中的 3 位确定交易无误后，使用硬件钱包签名。Liminal 平台收集到 3 个签名后，再使用 HSM 添加最后的签名，并使交易上链。从链上攻击交易中看，攻击交易中确实包含了 3 个合法签名，且第 4 个签名为交易发起者（即 Liminal），与披露的钱包管理架构一致。

结合 Liminal 和 WazirX 双方报告，这笔恶意多签交易发起的流程如下：

攻击者通过某种未知手段（包括不限于 0-day 网络攻击、社会工程学攻击等）诱导 WazirX 签名交易。

WazirX 3 名成员，分别通过书签等登录 Liminal 平台，进行 Google 验证及 MFA 验证通过后，查看到待签名交易为 2 笔 GALA 和 1 笔USDT 转账交易，并使用硬件钱包进行了签名。但实际受害人签署的内容并不是代币转账交易，而是多签钱包的合约升级交易。由于实际交易内容与声称的转账交易不一致，Liminal 平台分别拒绝了 3 笔交易。

至此攻击者收集到 3 名成员对于合约升级交易的签名，再次向 Liminal 平台提交恶意的合约升级交易，并附带 3 个正确的签名。

Liminal 平台检查签名无误后，作为第 4 个签名人发起交易，交易上链后，钱包合约升级，控制权转移到攻击者手中。

根据 WazirX 的描述，签名人员使用硬件钱包保管私钥。攻击者也是通过伪造转账交易的方法收集到了 3 个签名人的签名。因此推断 3 位 WazirX 管理者并不存在私钥泄露的情况。同样 Liminal 也不存在私钥泄露的情况，否则攻击者无须通过 Liminal 平台发起最后一笔交易。

另一方面，根据 WazirX 的描述，签名人员通过书签访问了正确的 Liminal 平台，并进行了 Google 与 MFA 验证。Liminal 平台也记录到了三笔异常交易的日志，因此也可以排除 WazirX 登录了虚假 Liminal 平台钓鱼页面被收集签名的可能。另外根据 WazirX 披露的设备初步取证结果，也认为 WazirX 3 名签名人的设备没有受到攻击。

综上所述，可能的一种攻击手段是，攻击者通过中间人攻击、XSS 攻击或其他零日攻击等手段劫持了 WazirX 受害人的浏览器前端页面，伪造展示给 WazirX 受害人合法的交易内容。攻击者收集齐 3 个 WazirX 受害人的签名后，通过已有会话向 Liminal 平台提交了最终的合约升级攻击交易，并通过 Liminal 平台风控后成功上链。

2.2 攻击事件暴露出的问题

根据前述分析，WazirX 和 Liminal 双方在事件中均暴露出一定问题。

Liminal 平台风控不严格：

从最终链上的攻击交易中可以看出，Liminal 平台对合约升级交易进行了签名并上链。平台的白名单转账风控策略没有起到应有的作用。

Liminal 平台披露的日志中可以看出，平台已经发现并拒绝了三笔可疑交易，但没有第一时间向用户告警或冻结钱包转账交易。

WazirX 没有仔细核对硬件钱包签名内容：

硬件钱包中展示的内容才是真实待签署的交易内容。WazirX 签名人员在签署多签交易时，信任了 Liminal 页面展示的交易，没有仔细核对硬件钱包待签名内容与 Liminal 页面展示的交易是否一致而直接签名，提供了攻击者所需要的合约升级交易的签名。

3 Cobo 如何帮助客户抵御网络攻击

3.1 完善的风险控制机制

Cobo 提供多种风控机制，旨在解决存储、管理和转移数字资产中遇到的安全挑战。根据钱包类型不同，Cobo 风控引擎允许客户运行独立的风控程序或者链上的风控合约。即使 Cobo 遭受安全攻击，客户侧与链上的风控检查依然可以保障用户资金安全。

客户可以灵活的按需设置链上和链下交易风控、业务风控以及用户角色和权限，针对不同业务类型配置所需要的风控、权限规则：

交易风控：客户可以轻松创建和编辑链上和链下交易风控，并通过设置审批动作（包括自动通过、自动拒绝和多人审批）来自动处理每笔交易。

业务风控：客户可以定义各类平台管理操作（如删除团队成员或冻结团队账号）的审批规则。

用户角色与权限：客户可以为指定团队成员分配特定用户角色。目前，Cobo Portal 提供了五种预设角色——观察员、提币员、审批员、操作员和管理员。客户也可以根据自己的业务需求创建其他角色。



3.1.1 交易风控

客户可以轻松设置和编辑链下和链上的交易风控。

链下交易风控由 Cobo Portal 的后端系统管理。Cobo 的风控引擎可根据用户配置的规则对代币转账、合约调用进行细粒度的检查与控制，保障交易内容符合用户的限制要求。值得一提的是，针对 MPC钱包，我们支持在 MPC-TSS 签名人节点上部署自定义的风控程序（称为 Callback）。该风控程序独立于 Cobo ，部署在客户自身的 MPC-TSS 节点上。这个位置的风控可以在 Cobo 遭受攻击的极端情况下，为客户提供最后一道保障。在本案例中的场景，如果 WazirX 签名人是具备 Callback 保护的 MPC-TSS 节点，则攻击者无法收集到非预期交易的签名。

链上交易风控则通过区块链网络上的智能合约管理。我们支持通过 Cobo Safe 框架在智能合约钱包上配置风控规则，其中包括配置链上转账白名单，攻击者很难对链上的白名单机制造成破坏。在本案例中的场景，如果使用 Cobo Safe 链上转账白名单机制，那么攻击者将无法发起白名单外的任何交易。

3.1.2 业务风控

客户可以设置业务风控以定义批准某些操作（如删除团队成员、修改成员角色、冻结团队账号）所需的团队成员数量。根据操作的不同，默认要求至少 50% 的管理员批准或仅由其中一位管理员批准。客户也可以手动编辑规则，设置自动通过、自动拒绝、或审批门槛。

了解关于业务风控的更多信息，请查看业务风控介绍：https://cobo-6.mintlify.app/cn/portal/organization/governance-intro。

3.1.3 用户角色与权限

用户角色由预定义的一组规则组成，可用于为团队内的指定成员分配特定权限。Cobo 提供了五个预设角色，客户还可以根据具体需求创建其他角色。

了解关于用户角色和权限的更多信息，请查看用户角色和权限简介：https://cobo-6.mintlify.app/cn/portal/organization/roles-and-permissions。

3.2 为客户提供安全技术支持

Cobo 提供 7×24 全天侯客服支持，如果遇到任何安全问题，客户可第一时间向我们反馈，我们将全力协助每一位客户排查安全隐患。

4 Cobo 安全体系

针对本次盗币事件两个可能的原因：网络钓鱼和系统漏洞，Cobo 在公司整体网络建设、员工终端、以及交易过程等多个维度上都设有完善的安全防护措施，以应对各种形式的攻击，防范类似安全事件的发生。

4.1 安全且多样化的钱包技术

Cobo Portal 将四种钱包技术整合到单一平台上，提供最先进的安全架构，且其链和代币覆盖范围为业内最广（参考全托管钱包和 MPC 钱包了解 Cobo Portal 支持的代币与链）。

全托管钱包：https://manuals.cobo.com/cn/portal/supported-tokens-custodial

MPC 钱包：https://manuals.cobo.com/cn/portal/supported-tokens-mpc

全托管钱包：全托管钱包采用先进的加密技术和风险控制引擎，确保客户的资金免遭未经授权的访问和潜在攻击。它采用了稳健的三层（热-温-冷）私钥存储架构，95% 的资金安全地存储在冷钱包中，只有 5% 的资金存储在热钱包和温钱包中。

MPC钱包：多方计算 (MPC) 是一种用于区块链私钥管理的先进加密技术。Cobo Portal 提供了两种类型的 MPC 钱包：机构钱包，让机构能够完全控制自有资金或其终端用户的资产；终端用户钱包，让终端用户能够完全控制其数字资产。

智能合约钱包：这类钱包支持各种智能合约钱包，主要包括 Safe{Wallet} 以及其他账户抽象智能钱包。它还支持灵活地委托外部账户 (EOA) 钱包来与智能合约生态系统进行无缝交互。

交易所钱包：交易所钱包是轻松管理多个交易所账户的一站式解决方案。它将所有交易所账户集中呈现在用户友好的单一界面中，可无缝查看、监控和管理各个交易所中的资产。

4.2 Cobo Guard——多功能的 iOS 安全应用程序

Cobo Guard 是一款由 Cobo 独立研发的多功能 iOS 安全应用程序，旨在增强数字资产的传输安全性。它采用非对称加密技术保护资产，可充当交易审批工具和 MPC 私钥分片管理器。同时，Cobo Guard 支持作为 Cobo Accounts 的多重身份验证（MFA），并提供无密码登录机制。

Cobo Guard 为每个用户生成唯一的公钥和私钥对，确保您绑定的应用程序拥有强大的安全基础设施。

用户的公钥与 Cobo 共享，而私钥则安全存储在您 iPhone 的原生 Secure Enclave 中。这种设置确保所有操作审批均通过您的私钥进行签名，并使用您与 Cobo 共享的公钥进行身份验证。

采用最先进的生物识别认证技术（如指纹扫描、Face ID 或设备 PIN 码）轻松授权请求，从而增强身份验证过程的完整性。

绑定 Cobo Guard 后，每笔提币和支付交易都需要在 Cobo Guard 内进行二次确认。这一额外的安全层显著提升了交易保护，降低了未经授权访问的风险。

Cobo Guard 可以交易审核过程中展示用户友好的交易解析内容，方便审核人员进行判断。

4.3 针对网络钓鱼

因成本低，实施容易，能够以较小的成本获得显著的收益等特点，网络钓鱼现在已成为攻击者常用的手段之一。Cobo 深知网络钓鱼的危害，针对这一威胁采取了以下措施：

使用领先的终端安全防护产品，实时监测和应对潜在威胁

使用硬件 Key 保护终端安全

权限划分细致，任何权限都需要申请

定期进行内部钓鱼演练，提升员工的安全意识

4.4 针对网络攻击

Cobo 始终保持对网络攻击的高度警惕，并实施全面的安全措施，以确保系统的高效韧性和对潜在威胁的全面保护。我们基于完善的防护措施，自 2017 年投入运营以来，一直保持着安全事件「零发生」的完美记录，安全系统坚不可摧。

实施 7×24 监控和维护，确保系统全天候稳定运行

针对业务系统定期进行全量渗透测试和代码审计

定期进行内部和外部攻防演练

通过知名安全厂商，每半年进行一次渗透测试，未发现任何安全问题

Cobo 基础设施目前有 200+ 条安全策略，并定期进行安全巡检

具备抵御 DDOS 以及拦截常见安全漏洞的能力

获得 ISO-27001 和 SOC 2 type 2 合规认证