Nex Vault

Web3.0

加密货币交易所安全风险指南精编_

NexVault Security Team

nexvault.com

目录

1. 关于

1.1. 关于我们

NexVault 团队由某头部交易所安全负责人及其核心团队所创立。

团队于 2022 年底完成了第一版《Web3 中心化交易所安全风险实践指南》(以下简称“指南”, 点这里查看指南), 这份指南汇聚了团队在一线交易所实战近五年时间所得的实践心得, 具备较强的实战理念和可落地性。

1.2. 关于指南

我们在 2023 年开始小范围推广这份指南，并依照这套指南框架协助多家交易所完成了安全风险的分析、评估及持续改造，均得到了不错的效果和反馈。

时间来到 2024 年, 我们又陆续收到一些来自交易所及安全同业的反馈和需求, 但彼时, 我们已决定将重心放到 nexvault.com 产品之上，启动了新功能开发与迭代，团队无暇顾及这些反馈，指南也随之停更。

1.3. 关于精编

在 2024 年底，行业迎来新机遇，加密资产在政策面和市场面都出现较多利好，身边一些熟知的朋友也开始重提指南 v2.0 之后的更新问题，我们综合了一些历史反馈、以及考虑到指南 v2.0 中的一些不成熟的细节和问题, 于是着手准备《加密交易所安全风险指南精编》（以下简称“精编”）。精编是来自指南 v2.0 中的内容，是指南的删减版，两者差异在于，指南关注交易所安全风险的全面性，精编更关注安全与交易所业务的相关性，因此一些对资金业务没有直接影响的部分也就未出现在这份精编内容之中，如，办公网、线上安全等。

但是精编从内容上却又比指南更为丰富，因为精编不再只是一个框架，而是综合我们的实践经验，将每一个风险场景更具象的展开、总结成文字。这就为交易所安全从业者提供了比指南 v2.0 更直接的参考，既免去了指南 v2.0 这一副框架可能带来的“哑谜”，也算是对我们这一程的总结和复盘。当然，如果还能因此给 Web3.0 安全做出一点点贡献的话 —— 也算不枉我们这些从业者们的 Web3 builder 之名。

2. 写在前面

2.1. 风险展示问题

在接下来的内容中我们可能会对交易所面临的某些风险细节及对抗手段进行展开，而在此过程中，应该会有两个问题被质疑和频繁提出：

- 展开去讲交易所的风险细节，是否会教更多的人去攻击、入侵交易所
- 针对不同的风险场景进行对抗分析，是否让黑客学会了如何绕过交易所安全措施

针对这两个问题：

- **是否会让更多人学会攻击和入侵交易所**

  理论上 —— 会

  实际上 —— 难，想法和执行的差距总是如隔鸿沟，况且，文中其实并没有涉及太多可操作的攻击细节，所以我认为，可放心食用。

- **是否会教黑客绕过安全措施**

  在安全对抗过程中，本质上是成本对抗，这包括了直接的经济成本、过程的时间成本、以及后续的变现成本等等多个方面。安全工作就是提升每一个环节的成本。

  多数情况下，我们是不会过分担心所谓的策略暴露可能带来的影响，我们更应关注风险场景，因为风险本身就存在无数变数、策略也应如此，去随风险的变化而变化，将整个对抗过程去监测、去发现、去改进、再去对抗，如此往复。

  我们只是给出一些几年前的经验参考，这大概也只能作为当前对抗环境下的一个基础参考版本，所以，无需过分担忧。

2.2. 参考资源问题

在文章内我会给出一些可参考的资源（包括数据、工具、教学文章等），针对这些参考资源的一些说明，请务必阅读并知晓，否则请不要轻易使用：

- 链接均为早期（约 2015~2021 年期间）收集整理，其中大部分数据和工具仅在早期收集使用时进行过验证，在编写本文过程中未进行详细的二次验证，无法保障全部内容依然完全可用且有效
- 因收集时间较早，所以一些工具可能显得有些老旧过时，大家根据现状各取所需
- 所有链接会以开源免费的数据或工具为主，但读者也需知晓，大部分开源数据和工

具的时效性相对商业方案依然会有所减弱或延迟，请勿对其抱有巨大期望

- 提供的数据和工具主要是辅助风险说明、用于提供参考学习，并不能确保所提供之内容能够完整覆盖当前风险，使用者需根据自身业务情况判断使用
- 很多安全工具会兼顾“黑客”属性，强烈建议打开前先通过 virustotal.com 等工具扫描，并根据个人能力酌情使用，如有怀疑切勿点击
- 最后，所有内容仅供安全技术研究学习，切勿将其用于攻击、入侵

3. 快速索引

用户注册与认证	匿名邮箱/一次性邮箱注册	利用匿名服务注册，快速获取大量账号
	注册用户来自批量注册的邮箱	利用某些邮箱服务特性，可实现邮箱批量注册
	注册用户来源地或设备存在风险	注册来源IP被标记，注册来源设备存在风险
	使用仿造证件认证	使用虚假信息进行KYC，绕过认证
	同源注册/同人注册	多人注册，但背后为一人或深度关联的人群
用户端风险	用户账户被盗	用户因安全防护不足导致账户被盗，账号内资产面临风险
	用户API泄露	用户端出现API泄露，导致威胁其账户内资产
	用户访问钓鱼仿冒网站	用户被钓鱼，导致账户被盗
	交易所数字品牌保护	
	用户前端被黑	用户端浏览器被黑客控制，账户内资产面临风险
热钱包充提安全	实时对账与防篡改	链路防篡改，全链路业务安全兜底能力
	热钱包地址管理	热钱包地址分类及地址间安全管理机制
	链上AML（KYA/KYT）	充值来源地址存在可疑行为
	异常充提行为	用户充提行为异常的分析与识别
	上币安全	
	供应链安全	
	在线签名热钱包	在线签名暴露更大风险，需更多额外保障
	Defi协议交互风险	热钱包链上交互风险
冷钱包安全	签名设备管理风险	签名终端保护不到位，导致被盗或不能使用
	助记词管理安全	助记词生成、保管过程不当，导致签名权限丢失
	签名环境安全	签名环境存在风险，可能在签名过程中窃取敏感信息
	灾备安全	
	签名安全	签名执行过程中的安全风险
关键岗位风险	冷钱包签名人风险	签名权限人异常行为导致资金无法使用或滥用
	财务人员风险	
	客服团队风险管理	
	运营/商务/人事/前台等	

4. 交易所安全风险

4.1. 用户注册与认证

用户注册与认证环节的风险问题，主要集中于任何可能利用注册逻辑、KYC 验证缺陷等方面的虚假注册、或养号行为。这类账号可能导致的风险多集中于刷取日常运营活动奖励、渠道数据伪造、养号销售、被用于恶意交易等。

4.1.1. 匿名邮箱/一次性邮箱注册

风险说明	● 较多一次性邮箱可被任意用户访问，极少数正常用户可能为隐蔽敏感信息而使用了此类服务，但是使用服务过程中未能充分了解此类服务的特性，导致其注册后出现信息泄露等风险 ● 恶意用户使用一次性邮箱隐匿身份，若平台 KYC 要求不严格，使用匿名邮箱注册后便可具备一定的交易、充提权限，将可用于活动薅羊毛、恶意交易（如，对敲）、长期养号等
检测与防御	● 注册时检查邮箱合法性 ● 长期来看，应对邮箱进行持续的分类管理，如，公共邮箱、企业邮箱、匿名邮箱等不同类别的识别，以及公众人物、已标记为黑邮箱等具体个人信箱地址的分类库 ● 邮箱分类管理可通过开源情报等手段建立，部分参考： ➢ 匿名/一次性邮箱 https://github.com/disposable-email-domains/disposable-email-domains ➢ 已标记黑邮箱地址 https://raw.githubusercontent.com/WSTNPHX/scripts-n-tools/master/malware-email-addresses.txt ➢ 公共邮箱域名列表 https://help.gong.io/docs/public-email-domains-exclusion-list ➢ 另有大量付费服务提供 KYC/EDD 数据，需根据平台所持不同地区牌照的合规要求而选择，此处不再赘述

处置建议	拦截此类邮箱注册，标记记录用户注册来源信息，对用户展示风险提示

4.1.2. 注册用户来自批量注册的邮箱

风险说明	目前仍有一些邮箱存在批量注册的“漏洞”，从而轻易获取大量免费邮箱，使用批量注册而来的邮箱，多是来自同一人或同一群人
检测与防御	● 某较短时间窗口内大量同域名邮箱注册，且符合以下一个或多个特征： ➢ 前缀连续性检测，如，abc001、abc002（手段老，目前少见） ➢ 组合特征检测，批量注册邮箱的前缀使用固定的组合模式，如，四个随机英文字符+四个随机数字，可对组合字符的单词含义、或缩略语义含义进行检测（如，使用单词本匹配） ➢ 机器学习对抗，已知一些批量邮箱注册工具的前缀名借鉴了类似 DGA 算法来批量生成，目前对于 DGA 算法有较多的反向识别、对抗手段，可直接用来进行检测对抗 ➢ 其他补充：在所有检测之前，使用者需初步了解目前市面上哪些公共邮箱存在批量注册的可能性，以实现初步的快速筛选 ● 在 Gmail 邮箱中，以下用户前缀都等同于 abcd@gmail.com，利用这一特性，这一个 Gmail 邮箱即可等同于 4 个邮箱： ➢ a.bcd@gmail.com ➢ ab.cd@gmail.com ➢ abc.d@gmail.com ● 自注册域名：恶意用户使用自有域名开通邮件服务，为自己批量定制同域名的邮箱，如，用户注册 myfakedomain.com，随后开通 MX 解析、批量定义 xxx@myfakedomain.com 多个邮箱，此类场景，检测手段主要集中对其域名的有效性做多维度反向检测，不再详述 ● 暗网售卖：暗网也会提供一些未 KYC 或初级 KYC 的账号，可爬取暗网数据或购买暗网情报获取 *【注】以上所有检测思路，提供的都是初步检测方法，一旦检测发现异常，可在检测结果内做二次深度特征分析，以获取更多维度的检测、挖掘更多的异常注册数据*

处置建议	● 对异常注册用户进行标记 ● 出现大额充提、交易或敏感行为时，触发 KYC 等二次验证动作

4.1.3. 注册用户来源地或设备存在风险

风险说明	● 用户注册来自敏感 IP 地址或地址段，如，被标记为长期运行自动化脚本、自动化爬虫的 IP 地址（段） ● 注册时使用的邮箱或手机号，可能符合“接码”特征 ● 使用了越狱、或是安装多个恶意 App 的移动终端 ● 使用了伪造身份的证件或经过修图的证件照
检测与防御	● 检测注册 IP 地址是否来自高危地区（如，制裁地区） ● 采集整理“接码”平台及手机号码数据，建立手机号黑库 ● 对敏感号码进行探活及真人验证（批量探活可参考智能客服类服务） ● 注册使用的 KYC 归属+来源 IP+用户端运行环境，三者冲突 ● 深度检测：除 IP 外，可综合手机、浏览器及语言特征 ● 深度检测：手机端越狱设备检测、动态调试检测、其他异常 App 检测 ● 借助外部开源或商业威胁情报，可对 IP 地址做以下针对性检测： ➢ 大量来自长期运行自动化程序的 IP 地址 ➢ 大量来自异常 IP 地址段（如，某些长期租赁的 IDC 等） ➢ IP 有“秒拨”特征（秒拨需持续动态检测，较复杂，此处不做阐述） ● 开源及商业情报参考： ➢ https://otx.alienvault.com/（老牌情报服务） ➢ https://github.com/1aN0rmus/TekDefense-Automater ➢ https://github.com/HurricaneLabs/machinae（两个自动化工具）
处置建议	● 对用户进行标记处理，实现全业务路径的持续跟踪 ● 在触发敏感动作时可增加二次 KYC（EDD），如，注册后快速充提 ● 转为沉寂用户时，增加持久化标记（建议标记在业务内实现）

4.1.4. 使用仿造证件认证

风险说明	目前一些 KYC 服务仅对证件照内信息进行解析，并不验证证件照真伪，这

	就使仿造证件绕过 KYC 检测成为可能。另一方面，基于 AI 生成的伪造身份（如深度伪造的 KYC 视频或合成证件照片）也在逐步成为新威胁。
检测与防御	● 对使用了含有 PS 等修图痕迹的证件照片，有较多本地化扫描检测方案，可搜索开源工具尝试 ● 使用的证件照中，含有在线生成伪造证件照的普遍特征，如，veriftools，可收集此类平台生成的仿造文件并进行批量的特征分析 ● 其他图像特征检测，如，仿造图像内的相似特征，另有大量商业服务提供了基于 AI 的深度检测服务与对抗能力 ● 增强活体检测的 KYC 服务
处置建议	进行补充 KYC

4.1.5. 同源注册（同人注册）

风险说明	● 用户使用同一网络、同一设备或亲属关系注册 ● 注册后多针对各类带有奖励的运营活动进行羊毛行为 ● 少数可能因个人身份不符合注册要求，而借用身份，此类行为则存在资产被盗风险。若借用身份的人有意隐瞒其敏感身份，还可能因其身份敏感性而导致平台被司法调查
检测与防御	建立用户端指纹能力（Web 和 App 端），采集进行多维度关联。建立链上分析能力，进行链上行为关联。可按需考虑引入图计算进行身份及链上的图谱关系建设，增加准确性与效率。同源、同人识别参考思路： ● 同设备及关联设备判断（即，同人） ➢ 设备信息 + 设备指纹 ➢ 设备信息 + 网络出口 ➢ 设备信息 + 区域坐标 + 基站 ➢ 账号曾用登录源、账号曾用出口等 历史记录关联 ● 多网络之间关联 ➢ 网络出口归属地 + 设备信息 ➢ WIFI SSID + 出口归属地 ➢ 历史数据（同上）

	● 链上分析 ➢ 充提地址关联：来源去向的地址一致性、时间相似性等 ➢ 借助图谱社群关系分析，建立链上交易地址关联 ➢ 链上交易手续费关联 ● KYC 与活体认证
处置建议	无，因此类行为多涉及运营奖励，需各平台根据自家运营规则而定

4.2. 用户端风险

4.2.1. 用户账户被盗

风险说明	用户安全意识不足导致的信息泄露，或使用了存在漏洞的云端服务导致个人信息泄露，黑客利用泄露信息成功盗取账户。可能遭遇的方式： ● 邮箱被盗，被盗邮箱用于注册交易所且作为关键 2FA 验证 ● 用户访问了仿冒的钓鱼站点 ● 遭遇 SIM Swap Attack，且短信作为 MFA 或密码找回的关键机制 ● 在不安全的云端存储了敏感信息，如，云端短信、云文档等 ● 用户设备中毒，导致敏感信息被盗，或剪切板被黑客控制 ● 用户遭遇信息泄露，个人信息在社工库内被恶意利用
检测与防御	因用户自我保护不当而导致的账户密码泄露、MFA 泄露等账户被盗事件，干预方式分为两个层面，第一层在其事前和事中，因其敏感信息被盗过程均脱离于交易所视野之外，因此交易所方面难以通过体系化的手段在泄露发生过程中干预，只可依靠一些碎片化手段对用户进行事前风险干预： ● 定期检查用户 MFA，建议用户使用至少两种相互隔离的 MFA ● 不同敏感环节使用差异化 MFA 交叉验证 ● 用户历史上存在多次来自不同地址的登录错误尝试 ● 针对该用户历史上存在找回密码、申请客服恢复 MFA 等，多次有关敏感认证信息的错误尝试 对于此类风险场景，更多有效的安全工作只能在事后（即，黑客成功盗取账户并登入交易所）进行监测和处置，包括： ● 用户来自非常用地、非常用设备登录

	● 新出现的登录端与保持会话的登录端类型和来源地存在差异，如，Web 及 App 端、API 与 App 端 等 ● 用户新地址提币，地址与白名单或历史交易地址相似但不相同 ● 用户新地址提币时，应进行 MFA 等验证，但验证未通过，或验证超时 ● 用户登录来源可疑且向新地址发起提币，此时可使用短信或邮箱进行上行验证，但验证未通过，或验证超时 ● 发起了可疑的对敲交易，试图转移资产（对敲交易参考下一节）
处置建议	发现疑似被盗情况时，可按场景提供如下处置： ● 触发关键动作时使用活体快速验证拦截（如，提币、交易等） ● 触发关键动作时使用 MFA 验证拦截（此处 MFA 不建议使用邮件） ● 下行邮件或短信提示，可要求用户回复上行邮件或短信进行验证 ● 提供快速冻结通道（需防止被滥用）

4.2.2. 用户 API 泄露

风险说明	用户在交易平台生成、复制、传递 API 的过程中，均可能通过多种途径泄露，而这一过程与上述账户问题相似，泄露过程几乎脱离于交易平台，因此交易所平台在其中所能进行的安全干预较为有限，此处暂先列举用户常见失误而导致 API 泄露的场景： ● 生成 API 的环境不安全（生成时被偷拍、电脑中毒等） ● 将 API 存储于不安全的云端（云端服务被黑、个人云账户泄露） ● 将 API 托管到其他资管平台，资管平台作恶滥用或平台被黑 ● 进行自动化交易的服务器被入侵，导致 API 泄露 ● 将 API 编码到程序中，并将程序托管到 github 等平台，导致泄露 ● 明文传递过程失误，发送给错误对象，或使用不安全的通道发送
检测与防御	交易所可通过以下策略在事前帮助用户缓解一定风险： ● 精细化划分 API 权限，为不同场景设计不同的 API 权限分类 ● 对于提币等高权限 API，严格要求用户绑定 IP ● 限定 API 仅能向地址白名单提币，设置白名单时需验证 MFA ● 可按需限定 API 的交易资产类型、交易币种、交易金额

	● 生成/复制 API 过程中分段显示、分段复制，每段复制内容中插入随机干扰文字（干扰文字符合自然语言，用户可读，但对机读不友好） ● 为防止前端被黑导致黑客以隐秘手段创建并获取 API，可增加： ➢ 前端设置防御 CSRF 等措施 ➢ 创建 API 时强制进行 MFA 验证 在 API 创建完成后因用户保管不当而泄露，其整个过程脱离于交易所，安全手段极为有限，仅能通过定期对 github 等平进行扫描、发现、并通知停用等手段，在 API 泄露的过程中，尽可能帮助用户规避损失： ● 全网主动监测用户 API 泄露 ➢ 在原有 API key 基础上增加一个可控字段，该可控字段需具备一定隐秘性、周期变化性、且可基于某种规则自动生成 ➢ 借助可控字段为核心匹配规则，定期扫描 ds、tg、github 等社群及代码仓库，一旦触发后，即可通知用户并停用或限制提币 对于 API 已泄露并被黑客利用的情况下，可识别的风险： ● 使用 API 交易、提币过程中，API 调用 IP、API 创建 IP、其他有效 session 会话期内的端 IP（如，app 端），三者之间存在明显冲突 ● 使用 API 高频交易流动性较低的小币种，且符合以下全部或部分特征，则可能正在使用 API 对敲交易转移资产： ➢ 交易标的为盘浅、量低、流动性差、甚至没有做市的小币对 ➢ 交易对手单一用户或少量用户，且存在以下一个或多个行为： ◆ 注册时间较长，但历史交易及充提行为均较为低频 ◆ 存在疑似养号行为（参考上一节） ◆ 历史上层将其标记为可疑用户 ◆ 存在同源、同人的可能性（参考上一章节） ➢ 从交易过程看，缓慢且均匀，有极为稳定的盘面波动操控行为 ➢ 从交易结果看，交易对手方均有明显的获利（存在转移行为）
处置建议	发现用户 API 异常交易时，可考虑暂停 API 使用，或通过 MFA、KYC 等阻塞式手段干预，但干预过程中需关注用户资产情况，避免干预过程中因价格波动、阻塞时间较长而导致用户资产的二次损失 —— 所以，对于可能

	有资损的用户，应采取更加及时有效的方式直接触达干预

4.2.3. 用户访问钓鱼仿冒网站

风险说明	用户可能通过以下来源获取到仿冒（钓鱼）站点，并在仿冒（钓鱼）网站上输入敏感信息（黑客通过自动转发或反代等方式获取访问权），进而导致账户丢失、资产被盗： ● 通过 Google 等搜索引擎搜索关键字，广告位为钓鱼站点 ● 通过社群（X/DS/TG 等）内传播的信息，访问了钓鱼站点 ● 收到来自交易所的仿冒邮件，其中包含有钓鱼站点链接
检测与防御	无论用户通过何种渠道获取并访问钓鱼仿冒站点，其结果基本指向几种： 第一， 账户被盗，资金被提到黑客地址 第二， 无法提币，通过对敲等方式将资金交易转移至黑客账户 第三， 无任何有效变现措施，恼羞成怒、进行恶意交易 对于黑客盗取账户后的提币防护：参考 4.2.1 对于黑客盗取账户后的对敲防护：参考 4.2.2 对于恶意交易行为，需分类甄别，无法逐一阐述
处置建议	N/A

4.2.4. 交易所数字品牌保护

风险说明	交易所数字品牌保护主要包括：人员身份冒用、品牌冒用、恶意舆情、网站仿冒、社群仿冒、域名安全等方面，其中，可能对用户资产直接造成资金风险的有： ● 网站仿冒，用户访问钓鱼网站导致账户资金被盗 ● 社群仿冒，仿冒社群发布虚假消息导致交易盘面异常 ● 域名安全，黑客控制域名直接获取用户账户信息盗取资金 对于以上几类风险，其一般常规的攻击路径有： ● 网站仿冒 ➢ 通过投放搜索引擎关键字，在广告位设置钓鱼网站 ➢ 黑客注册相似域名，通过邮件、社群等渠道投放钓鱼网站

	➢ SPF/DMARC 设置不当导致黑客利用交易所域名发送虚假邮件 ➢ 直接使用公共邮箱仿冒交易所邮件 ➢ 抢注不同后缀域名，如，abc.com 与 abc.shop ➢ punny code 等高仿真域名，如，ü.com 和 u.com ● 社群仿冒（x/ds/tg 等） ➢ 抢注相似社交账号名，如，Abc 与 Abc_Global、AbcHQ 等 ➢ 社群账号管理不当，被黑客直接盗用 ➢ 社群账号管理不当、审核机制不足，被内部员工滥用或误用 ● 域名安全 ➢ 域名服务商被黑，导致域名被控 ➢ 域名管理员被定向攻击，导致域名 NS 等关键记录被修改 ➢ 域名到期未续费，导致黑客抢注域名 ➢ 域名到期弃用，但依然有其他业务引用该域名内资源
检测与防御	网站仿冒检测： ● 自建仿冒黑库 ➢ 常规相近字符仿冒、punny code 仿冒组建成黑地址库 ➢ 每日对黑库内地址进行存活性巡检 ➢ 对存活站点可增加站点内容相似性检测（按需，非必要） ➢ Punny Code 工具参考 https://github.com/anilyuk/punydomaincheck ● 每日新增域名检测： ➢ 对每日新增域名进行黑库匹配 ➢ 每日新增域名与交易所所有域名进行相似性比对 ➢ 对每日新增域名进行站点内容相似性检测（按需，非必要） ● 其他 ➢ 周期性搜索引擎及社群搜索、扫描，查找仿冒站点 ➢ 外部非搜索引擎或知名站点，引用交易所主站资源的访问 ➢ 外部非搜索引擎或知名站点，跳转至交易所主站的访问 社群仿冒检测：

	● 注册保护：注册时需尽可能覆盖更多命名组合 ● 社群账号安全管理 ➢ 强制开启 MFA 等多重认证，MFA 与密码信息隔离管理 ➢ 定期更换登录密码，定期清除授权绑定、定期检查 session 未过期的客户端合法性，对非法端踢下线并进行安全检查 ➢ 设置发布规则及关键内容发布的审核机制，规避内部作恶 ➢ 设置发布监测，对自家社群发布消息有第一时间感知能力 ➢ 社群账号交接管理制度，避免因人员离职导致账号丢失 ● 提供官方验证渠道，验证社群、网站的真实性 域名安全保护，需建立域名维护机制，确保域名的控制权： ● 统计自有域名使用情况，以及承载业务 ● 新域名注册统一流程，确保每次新域名注册后相关信息被记录在案 ● 自有域名的过期跟踪，续费管理，防止抢注 ● 对于可能临期不再续费、且承载一定业务的域名，提前公示 ● 梳理内部业务的域名调用关系，防止调用链路被滥用、盗用 ● 设立域名管理账号的安全保护机制，如，MFA、电话、短信等 ● 用于存储 MFA 或接收短信的手机需有统一续费管理及安全保管机制 ● 为域名设置转移保护，防止被异常转移或停用 ● 为 NS 等关键记录设定全球多链路监测机制，防止劫持、污染等
处置建议	当通过域名检测发现高仿站点或虚假广告投放时，一般域名（或空间）服务商、搜索引擎广告服务商均提供了投诉入口，可对其进行投诉下架，另外也可使用专业品牌保护公司的服务，完成索引、投诉、下架一站式服务

4.2.5. 用户前端被黑

风险说明	用户前端被黑场景主要集中在用户浏览器被劫持或被插入恶意程序，一旦浏览器被控制，可能导致用户在无感知的情况下被执行交易、创建 API、替换充提币地址等，而导致浏览器被劫持的情况主要有以下几种： ● 安装了恶意的扩展程序（如，恶意的 Chrome extension） ● 链路被劫持，导致访问交易所时被插入了恶意的前端代码

	● 交易所引用的第三方前端代码被替换（第三方供应商被黑） ● 用户被定向攻击，如，近源污染导致其访问链路被插入恶意代码 ● 用户电脑被植入后门
检测与防御	对于此类情况，因其发生在用户端，且发生过程脱离于交易所，难以实现事前和事中干预，常规情况下，仅能从其可能造成的几类安全风险结果进行干预: ● 被恶意执行交易、创建 API ➢ 做好 CSRF 等前端防御工作 ➢ 创建 API 等关键动作，需 MFA 二验 ● 替换前端充提地址：略（高危场景，展开较多，此处暂不详述） ● 供应链安全（引用的第三方代码被替换） ➢ 三方代码本地化，常用 package 的自建源 ➢ 代码托管权限管理、文件版本及文件变更管理 ➢ 外部仿真链路检测（多地区多源访问）
处置建议	N/A

4.3. 热钱包充提安全

4.3.1. 实时对账与防篡改

风险说明	不以特定威胁为前提，考虑在黑客入侵成功后，若未掌控全部系统及业务逻辑、但又控制了大部分关键系统的情况下，热钱包系统可能会遭遇的最大风险便是数据篡改: 黑客在其权限范围内, 篡改业务数据实现盗取资金，如，拦截某笔交易，修改其中 to_address 为黑客地址，或是直接修改数据库等关键业务节点，手动创建一笔 to_address 为黑客地址的交易，随后等待其被业务抓取执行，为此需引入防篡改与对账能力
检测与防御	**防篡改能力（简要思路）** ● 防篡改能力独立于充提链路、且不嵌入业务流程（并行） ● 防篡改对钱包服务有干预能力（非串行，以信号指令方式干预） ● 可实现业务执行顺序、执行状态、每次执行有效性等维度的实时监测 **对账能力（简要思路）**

	● 对账包括实时对账和周期对账 ● 实时对账需独立于充提链路、且不嵌入业务流程（并行） ● 可实时将业务发起到执行完成情况、与链上实际发生状态进行比对 ● 业务数据应尽可能覆盖全链路数据 ● 实时对账可有效检出大部分假充值、双花、及黑客篡改行为 （注，其检出覆盖度，与实际场景和接入数据的有效性、完整性、实时性有较大关联性，因此只能定义为“大部分”） ● 周期对账：财务对账，此处不做阐述
处置建议	N/A

4.3.2. 热钱包地址管理

风险说明	热钱包依照其业务功能不同，可能会划分多个类型的地址，如，用户充值地址、手续费地址、出币地址、运营（手续费等）收入地址、空投地址等，其中风险点主要包括： ● 地址间的信任机制（白名单），以及白名单检测与处置机制 ● 地址（私钥/助记词）生成过程的安全性 ● 地址（私钥/助记词）到签名机部署的安全性 ● 地址（私钥/助记词）日常灾备安全
检测与防御	● 地址间信任机制 ➢ 信任机制的建立：略（根据业务和地址分类情况自行判断） ➢ 地址间资产归集或转移，需纳入到实时对账及防篡改体系 ➢ 用户地址资产归集，与系统地址资产转移，其触发程序分离 ● 地址生成过程的风险 ➢ 某些算法可规避生成时私钥暴露风险，如，MPC，但相对的，热钱包采用这些算法则需考虑： ◆ 新引入算法的执行效率与业务效率的匹配度 ◆ 新引入算法的安全性与持续安全性保障的维护能力 ➢ 主链原生助记词（或私钥）生成方式，遵循原则： ◆ 不可直接暴露助记词或私钥，应加密输出

	◆ 提供黑盒验证机制，可验证助记词密文及明文有效性 ◆ 助记词或私钥的解密密钥与密文隔离管理 ◆ 全流程以黑盒及“双人四眼”为基础保障 ◆ 需独立的隔离网络环境执行 （可根据以上原则，定制热钱包生成程序） ● 地址到签名机部署安全原则（略，基本原则同上） ● 地址日常灾备安全（略，基本原则同上）
处置建议	N/A

4.3.3. 链上 AML（KYA/KYT）

风险说明	链上 AML 以链上资金来源及去向地址的风险为主要判别依据，需充分了解用户充提上下游资金详情及风险。对于充提过程中可能出现的制裁地址、涉案资金、被盗资金等情况，可能会对交易平台造成风险： ● 因上游资金涉案、涉及黑客事件而引发司法风险 ● 因热钱包地址被用于诈骗传销等违法活动收币地址，引发司法风险 ● 充值热钱包及关联地址被执行司法冻结的风险（如，USDT）
检测与防御	● 采用商业 KYA/KYT 服务 ● 维护更新制裁地址，如，OFAC SDN LIST：https://sanctionslist.ofac.treas.gov/Home/SdnList ● 可能存在可疑的资金行为（部分案例参考）： ➢ 固定地址列表的高频等额充、提 ➢ 大额充值后的大规模、等额（或规律金额）提币 ➢ 多地、多人、同性别、同币种，向同一地址或相关联地址的等额或规律金额的提币行为 ➢ 多地、多人、同币种，向同一未知合约的提币行为（需结合合约情况进行判断） ➢ 多地、多人，同一特殊日期，向同一地址或相关联地址的特殊金额转账行为 ➢ 开源情报：常见利用加密货币的非法集资、传销、杀猪、赌博等行

	为所暴露的地址，与自身交易所地址的关联性 建议对于提币地址进行周期性的汇聚分析，根据数量、规模等特性汇聚提币目标地址及其下一层地址，并进行关联分析，常见关联分析手段： ● 同时间窗口内的充提关系 ● 手续费地址关联关系 ● 社群关系（参考知识图谱） ● 最终地址汇聚 ● 等额等频等
处置建议	单一策略命中后，可标记观察； 对于频繁命中策略，需进行额外 KYC/EDD 等

4.3.4. 异常充提行为

风险说明	异常充提行为可能是多类风险事件的前奏，在此总结部分场景
检测与防御	● 频繁大额充提（买卖提等行为） ● 异常额度 ➢ 贴近大额临界值的规律性测试 ➢ 持续等额等频充提（需要结合来源及去向地址分析） ● 来自某个项目地址的大额充值（略） ● 沉寂账户+可疑账户+充提异常 （沉寂+可疑账户：定义参考 4.1 部分） ➢ 沉寂且可疑账户出现小额充提测试行为 ➢ 沉寂且可疑账户出现 PoW 币种的小额测试行为 ➢ 沉寂且可疑账户出现 PoW 币种的大额充值 ● 当命中 PoW 币种的异常充值时（此处 PoW 多为算力小、分布广的 PoW 小币种，对于 BTC 等算力稳定的大币种可忽略），需关注： ➢ 是否突然出现不知名算力 ➢ 某些知名或未知算力出现转移 ➢ 支持该 PoW 币种的算力租借价格突然飙升 ➢ 支持该 PoW 币种的可用租借算力突然减少

	➢ 是否有其他交易所提供该 PoW 币种的交易 ➢ 当前设置的安全上账次数，是否在所有支持该 PoW 币种的交易平台中设置的最低 命中以上算力异常中的一条或多条，且同时出现对应 PoW 币种的充提异常时，需关注对应账户、及经链上回滚情况
处置建议	充提异常：需根据不同币种、命中用户情况自行评估； PoW 潜在回滚风险：可临时上调上账次数，或对特定异常用户增加提币审核及人工验证。

4.3.5. 上币安全

风险说明	上币过程需对合约代码、解锁机制、高权限账户等相关机制进行必要的安全审计，以规避常见的假充值、逻辑漏洞、权限、解锁等问题
检测与防御	略（相关介绍较多、提供类似服务供应商完善，不再赘述）
处置建议	N/A

4.3.6. 供应链安全

风险说明	毫无疑问，供应链安全是一个普遍性问题，也是一个可能存在于交易所各环节的问题，但是，就其伤害性来讲，供应链安全问题在热钱包中必然是伤害最大，故而将其归类于此。供应链安全风险主要体现： ● 使用的第三方组件存在漏洞，如，fastjson 反序列化漏洞 ● 代码引用的第三方组件被替换 ➢ 钱包或其他应用，引用商业组件，供应商被黑后插入恶意程序，例如，Web 前端各类计数器、页端客服系统等 ➢ 引用了开源组件，开源组件被替换、或插入恶意程序 ➢ 官方 Package 源（npm、pip 等）中混入了恶意程序，并被安装 ● 业务系统中关键节点依赖三方服务，如，区块链节点 ● 云服务权限管理不当，导致存储的关键文件被替换（如，**.apk） ● 软硬件供应商风险 ➢ 仿冒的供应商邮件（附带更新链接、附件等）

	➢ 供应商被黑，产品更新时更新了后门程序 ➢ 邮寄的硬件设备途中被替换或植入硬件后门
检测与防御	● 使用的第三方组件存在漏洞 ➢ 建立可追溯、可闭环的 SDL 体系 ➢ 实现全业务链路的软件成分分析能力，建立组件基础信息库 ➢ 定期追踪组件，确保“最小化更新+最小化风险”原则 ● 代码引用的第三方组件被替换 ➢ 组件引用实现本地化，尽量避免直接引用线上组件 ➢ 本地化组件经过必要的安全审计 ➢ 建立自有软件源，维护可信 package 列表，定期检查文件变更 ➢ 建立多线路的前端（web、app 等）探测机制，检测可疑变更 ➢ 热钱包签名组件优先选择离线签名，对签名机进行隔离管理 ● 业务系统中关键节点依赖第三方服务，如，区块链节点 ➢ 可建立多个三方节点依赖机制，避免单点（单厂家）风险 ➢ 区块链节点可建立辅助验证流程，借助自建或其他三方节点进行事后延迟校验，保障效率的同时实现一定的交叉双验 ● 云服务权限管理不当：略 ● 软硬件供应商风险：略
处置建议	N/A

4.3.7. 在线签名热钱包

风险说明	对于支持离线签名的主链，可将其签名组件与网络实现逻辑隔离，仅限制内部业务系统中必要组件的特定类型请求，相对安全可控; 相比之下，不支持离线签名的钱包（主链），其签名组件与互联网必须有通信，风险暴露面更大，需设置额外的安全保障机制。
检测与防御	仅支持在线签名的热钱包，其安全检测与防御: ● 信息安全保障机制部分：略（访问通道、系统、权限控制等方式为主） ● 除常规信息安全防护外，在签名设计和业务链路上，应严格遵循以下原则以降低风险、以及风险暴露后可能的损失:

	➢ 出币热钱包地址，进行必要的分散管理与单地址金额上限控制 ➢ 其他在线热钱包地址转账设置白名单，签名后、上链前，增加独立的交易白名单检查与控制手段 ➢ 设置较小的资金归集时间窗口，降低资金停留在热钱包的时间 ➢ 进行准实时的业务对账机制，确保每笔转出资金都能匹配到正确的上游业务请求 ➢ 防篡改机制应能覆盖以上链路
处置建议	N/A

4.3.8. Defi 协议交互风险

风险说明	交易所理财服务可能需要支持 Defi 交互，当 DApp 出现安全事故，以及热钱包不当的交易处理，可能导致资产损失。
检测与防御	● 监控交互 DApp 合约链上行为 ➢ DApp 权限、代码等变更行为 ➢ 高权限操作行为 ➢ 资产出现大额转移等事件 ● 对交互的 Defi DApp 进行严格白名单控制 ● 对 Defi 合约安全审计及后续可能的升级审计更新 ● 优先选择经过权威安全公司审计并开源的协议
处置建议	暂停热钱包 Defi 交互功能

4.4. 冷钱包安全

4.4.1. 签名设备管理风险

风险说明	作为冷钱包签名设备，无论其形态如何（硬件钱包、App、笔记本电脑等），在保管方面都可能存在以下常见风险： ● 设备损坏导致无法开机使用： ➢ 电池损坏导致无法开机，对硬件钱包，建议选择“电池+USB Cable”两种启动方式的钱包，或仅使用 USB Cable 方式 ➢ 闪存损坏，此类属于易忽略风险，目前硬件钱包、手机、甚至主流

	笔记本，其存储均采用闪存，理论上闪存数据保存具有时效性，在诸如高温、潮湿环境下，都可能会造成数据丢失 ● 设备长期不使用，导致密码遗忘 ● 设备保管不安全，导致被盗、或被恶意破坏 ● 设备安全防护机制不足，被盗后轻易被破解
检测与防御	建立必要的、周期性的巡检机制，对硬件设备进行巡检： ● 有效性巡检，硬件可用、可正常开机进入界面 ● 签名巡检，可正确输入密码、启动程序、并签名 ● 日志巡检，距上次使用后，设备未被他人使用 为签名设备制定必要的安全选型的基线要求： ● 对于电脑，应支持并启用硬盘加密 ● 对于手机或硬件钱包，应支持并启用密码多次错误后自毁 ● 硬件保管位置的安全性（根据情况按需决策） ● 远程抹除能力（被盗时处置）
处置建议	N/A

4.4.2. 助记词管理安全

风险说明	● 因保管不当而导致被盗 ● 因保管过于隐秘，在需要恢复时无法找到 ● 保管环境不当，导致受潮、受损等 ● 助记词保管过程中被偷拍、盗摄 ● 对于多签钱包，单一人员可完全接触多于一个助记词 ● 对于单签钱包，单一人员可完全接触助记词
检测与防御	● 建议助记词加密保管，加密密码与助记词隔离管理 ● 需谨慎算法加密软件与加密算法，应采用经过长时间验证的安全加密算法及工具，如：https://www.openssl.org/ ● 若不具备加密保管条件，可拆分管理，拆分方式可采取直接字符分片方式，或参考 Shamir 算法：https://iancoleman.io/shamir/ ● 使用防潮卡片，使用不易退色的水笔记录

	● 设置专用防偷拍的物理环境，提供记录、转移、存储过程的安全 ● 定期检查助记词保管环境，确保存放安全性
处置建议	N/A

4.4.3. 签名环境安全

风险说明	● 人员身份信息泄露，人身安全 ● 签名环境未进行网络隔离，个人可带电子设备进入 ● 签名环境被安装偷拍摄像头 ● 盗贼使用物理手段破坏签名室入口 ● 签名环境入口、监控、环境内保险柜等保护机制，完全由单人掌控，出现单点作恶风险
检测与防御	● 签名物理环境应最大可能保障签名人身份的隐秘性 ● 签名环境应网络隔离，如有条件，可设置电磁屏蔽屋 ● 签名环境应定期进行物理检测，防止偷拍偷录设备 ● 可按需设置多个签名环境，实现轮换或分散签名 ● 签名环境外设置 7*24 小时监控，但监控仅需覆盖进出位置 ● 签名环境不应使用可通过电子手段破坏的门禁系统，如，电磁门 ● 各监控、保护机制，应进行必要的人员权限分离管理
处置建议	N/A

4.4.4. 灾备安全

风险说明	● 备份有效性未进行验证，导致备份无法使用或不完整 ● 备份未与主签名环境充分隔离，导致主备在自然灾害时同时损毁 ● 备份转移过程中的盗抢风险 ● 缺少备份恢复流程，导致需恢复时遇到障碍 ● 备份验证及恢复机制长期未进行实操演练，导致需恢复过程缓慢 ● 备份人中出现单人权限过大，导致备份被单人物理或技术转移
检测与防御	● 建立分权限的多角色管理机制，应涵盖备份的操作、转移、恢复 ● 制定备份恢复计划

	● 定期进行灾备实操演习，为避免演习过程中的泄露风险，可定制少量专用的非业务私钥备份，专用于演习
处置建议	N/A

4.4.5. 签名安全

风险说明	● 冷钱包未使用多签 ● 钱包生成环境存在风险：随机数风险、生成过程助记词泄露等 ● 签名未实现所见即所签，导致风险交易无法识别 ● 待签名信息传递过程被篡改或损坏
检测与防御	● 冷钱包应使用主链原生多签 ● 签名地址生成时，确保随机数充分性 ➢ 可采用主流软硬件钱包 ➢ 自研签名程序则需根据其运行平台选择安全随机数生成器，或直接采用鼠标、Mic 等外部输入采集环境噪声 ● 对于 EVM 等多签数据，可提供原始待签名数据下载及验证功能，以实现所见即所签 ● 传递过程应提供非对称加密保护待签名数据，解密权限人与转移操作人角色分离，通过待签数据的所见即所签提供人工二次验证
处置建议	N/A

4.5. 关键岗位风险

4.5.1. 冷钱包签名人风险

风险说明	● 异常原因导致失联，无法完成签名，或影响签名时效 ● 多个权限人联合作恶，转移资金或拒绝签名 ● 签名设备保管不当导致丢失、损毁或忘记密码 ● 被定向攻击，如，线上钓鱼、线下诱骗等
检测与防御	● 异常失联无法签名：设定人员备份机制与配套的人事机制 ➢ 设定 3-of-5 多签，留有较为充分的人员备签空间 ➢ 签名人同时请假或差旅人数不可超过最小签名阈值

	➢ 设置必要的预签交易，用于紧急情况广播 ● 多个权限人联合作恶 ➢ 预设良好的灾备机制，可在必要时恢复给任意指定人 ➢ 设置必要的预签交易，用于紧急情况广播 ➢ 合规地区，应充分借助法务与认识机制 ● 其他 ➢ 因签名人保密需求，应为签名机制设立独立的安全管理人，管理人仅对签名人做日常签名协助与部分人事协调，不参与签名 ➢ 其他风险，如，定向攻击、设备损毁等，可参考冷钱包安全章节内关于签名环境与设备保管的部分
处置建议	N/A

4.5.2. 财务人员风险

风险说明	相比传统企业，Web3.0 企业的财务人员所面临风险更大。财务人员并非技术人员，但手中往往掌握通往其任职公司加密资产大门的钥匙或方法，所以更应对财务人员加以关注: ● 财务人员被定向攻击 ● 财务人员存在单人可访问加密资产钱包或相关管理系统的权限 ● 财务与其他员工网络混用，其他员工中毒后快速传播至财务网络 ● 财务电脑缺少严格的物理、及线上防控机制，易被攻击感染 ● 财务操作加密资产及财务数据的电脑，与日常生活电脑混用 ● 财务的存储设备（如 U 盘）在不同财务电脑与生活电脑上混用
检测与防御	● 财务网络划分独立 VLAN，并限定严格的 ACL 隔离策略 ● 财务配套的系统应尽可能收敛至办公网服务器区或其他特定隔离区 ● 财务系统严格控制其他网络访问权限，可限制仅财务网络可访问 ● 财务可能操作财务系统、加密资产、链上交互、财务数据的电脑，应设立专用电脑，不可与日常办公、个人上网及娱乐电脑混用 ● 不允许财务个人生活娱乐电脑带入公司，不允许财务人员的移动设备、非办公电脑接入财务的隔离网络

	● 所有需要与财务电脑连接的外设，如，打印机、移动硬盘等，均需设立专用设备，此类专用设备不能与其他电脑或个人电脑相连 ● 财务专用的打印机等可能联网的设备，应设置独立的管理权限 ● 办公网内其他哑终端设备 ➢ 办公网内如有非办公用的哑终端或智能设备，如，咖啡机、售货柜等，应该遵循以下原则 ➢ 优先选择自带 4G/5G 联网功能的哑终端进入办公区 ➢ 若必须链接办公网络，应为其设置独立隔离区，该区仅允许外联至特定地址，禁止内部一切横向访问
处置建议	● 设定财务规则及奖惩机制，定期对规则进行宣讲，并辅以安全培训 ● 部署 EDR/DLP/AV 等端点能力，对违规行为进行定期通报处置

4.5.3. 客服团队风险管理

风险说明	客服团队作为业务团队中较为特殊的角色，掌握着与客户个人数据及业务数据相关的系统权限，而同时客服又是连接用户与交易所的桥梁，因此不可避免的面临较多风险： ● 恶意人员通过威胁、冒用身份等手段进行信息或权限欺诈 ● 攻击者收买客服获取内部敏感信息 ● 客服人员作恶，未授权情况下查询用户信息 ● 客服人员接收到外部文件，文件中含有病毒或后门
检测与防御	● 客服团队在职场、网络等方面实行独立管理 ● 客服系统中对用户信息的展示进行必要的脱敏、及电子水印处理 ● 为客服系统设立监测机制，对于高频访问、异常时间访问、未授权访问、越权访问、使用他人账号访问等情况进行记录、预警 ● 如客服采用电话服务，可建立进线触发机制，避免查询权限问题 ● 客服终端安全控制 ➢ 部署 EDR/DLP/AV 等端点能力 ➢ 客服系统服务端屏蔽用户上传可执行文件的可能性 ➢ 客服终端上，限制执行任何类型的可执行程序

	➢ 客服系统提供在线打开 pdf/word/excel 等文件的能力，或，为客服提供安全的第三方 pdf/word/excel 程序 ➢ 如有可能，客服终端可采用瘦终端/云桌面方案
处置建议	客服团队设立安全制度及奖惩机制，定期进行安全培训

4.5.4. 运营/商务/人事/前台等

风险说明	运营、商务、人事、前台等岗位，其通用特征在于: ● 日常与较多陌生人直接接触 ● 有较多机会接收到外部的邮件或 IM 信息 ● 有较多机会与外部陌生人直接近距离接触 此类岗位主要风险集中于: ● 被定向执行在线攻击，如，假冒项目方、合作供应商、应聘候选人发送邮件或 IM 消息，消息内带恶意链接或含后门的附件（pdf/word 等） ● 被定向执行线下攻击（物理手段） ➢ 直接近身接触手机或电脑，植入后门或窃取信息 ➢ 以礼品、样品、试用等方式，寄送含有恶意程序的电子礼品
检测与防御	对于此类防御手段，原则上基本雷同，就不再占据篇幅重复描述; 但值得关注的是，技术手段永远无法覆盖人员安全意识问题，所有手段都需要有持续的培训、教学、以及必要的人事制度作为辅助。
处置建议	N/A

5. 写在最后

5.1. 编写说明

经过不断的取舍与修剪，终于完成了以上的精编内容。

如开篇所讲，精编目的在于更加贴近业务实战，因此我们基于《Web3 中心化交易所安全风险实践指南》进行了较大幅度的删减，如读者对出现在指南、但又没有收录进精编的某部分内容有兴趣，欢迎沟通探讨。如精编内容出现错漏或不详之处，也望指正。

最后，还有一些我们曾使用过的安全资源，因数量较多、难以在上述正文中与每一项风险进行逐一的匹配分类，也在此作为补充统一列出，可根据需求取用。

5.2. 补充参考

5.2.1. 漏洞相关

漏洞管理是信息安全管理中首当其冲的重点项目，稳定的漏洞信息源是大规模漏洞管理及 threat hunting 的必要基础，CVE 作为权威是必不可少的：

- https://cassandra.cerias.purdue.edu/CVE_changes/
- https://github.com/CVEProject/cvelist

CVE 漏洞可做基础安全基线管理之用，但因缺少漏洞可用性验证，因此，在具体使用过程中依然需要甄别。当然，如果你还听说过 SCAP 或是 USGCB 这种上古安全基线检测机制的话，还可以关注 https://ncp.nist.gov/repository，但如果对此并无概念的话，到也无需花费额外经历学习。

作为漏洞方面的补充，我们还推荐 Proofpoint Emerging Threats Rules，该服务分为 Pro 和 Open 两个版本，提供了主流漏洞、C&C 服务器、sinkhole IP 等网络层规则，规则格式覆盖 snort、suricata、ipf、iptables、pix 等，最重要的就是，该项目即便是开源部分的更新响应依然非常及时，其时效性甚至优于很多商业产品：https://rules.emergingthreats.net/。

5.2.2. 数据泄露及社工相关

数据泄露调查及入侵源头分析过程中，都难免需涉及到一些数据溯源、人员定位的工作，这些过程中涉及到一些可能的工具参考如下：

- https://haveibeenpwned.com/ 看域名就知道了，老牌工具
- https://amibreached.com/
- https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/ 关于数据泄露的报告，其中还附带来源
- https://www.spokeo.com/ 个人在互联网残留信息搜索（现在好像需要付费了）
- https://pipl.com/ 该工具以前也是一个免费的互联网痕迹调查工具，但现在好像改为商业服务了，可按需参考使用
- https://www.tineye.com/ 相似图片搜索，算是 Google 搜图的一个补充
- https://www.osintux.org/sobre-distribucion-osintux 这是一个 OSINT 调查用的 LiveCD，如果不是对开源情报抱有执念的话，就不用看了
- https://www.maltego.com/ 老牌互联网痕迹调查工具，有些年头的安全从业者都应该知道 maltego 的含金量

5.2.3. 恶意程序检测与样本

如果是日常攻防对抗强度较高的团队，建议关注并围绕以下这些开源信息建立自己的恶意程序样本库，一方面可用于验证规则或是训练模型，另一方面可定期对样本库特征做关联分析，自建样本背后的攻击者画像，这些画像之中的某人，可能就是你未来某一天的对手：

- https://www.virustotal.com/gui/home/upload C 位留给 VT
- https://www.hybrid-analysis.com/ 与 VT 类似，也是在线分析检测工具
- https://malware-traffic-analysis.net/ 虽然每次更新数量不多，但内容非常细致
- https://malwaretips.com/forums/malware-url-samples.104 样本分享论坛
- https://malshare.com/
- https://app.any.run/submissions 沙箱服务 AnyRun 及其样本集
- https://www.nomoreransom.org/zh/index.html 提供一些可解锁的 ransomware

5.2.4. IP/域名情报数据源

IP 情报数据是开源或付费情报中最普遍的一种，但同时，黑 IP 列表在安全策略中的深度整合也是最难的，在此仅提供几个可用的 IP 情报数据服务 —— 需要注意的是，我们未对以下链接进行分类，里面可能会包含攻击扫描类 IP、被爬虫滥用的 IP、C&C 服务器、僵尸网络、暗网（Tor Node）IP、以及各类原因而被标记为 Sinkhole 的 IP 地址：

- https://feed.ellio.tech/
- https://www.abuseipdb.com/
- https://intercept.sh/threatlists/
- https://feodotracker.abuse.ch/
- https://www.dan.me.uk/tornodes
- https://metrics.torproject.org/exonerator.html
- https://jamesbrine.com.au/

作为最容易获取的比对规则，IP 情报数据多数情况下不应独立使用，除使用以上标记的黑标签外，还可以结合诸如 ipip.net 等服务提供的 IP 地址公共标签，将两类标签联合分析研判。而且 IP 地址逐一分析使用的效率过于低下且共性特征会变小，所以更适合规模化分析使用，如，秒拨 IP 的分析，结合区域性的地址归属、地址属性分布、以及轮换特征等进行批量分析，对秒拨实现区域化或聚类行为的捕获。

相比 IP 情报来说，域名情报的准确性就要更高，而且域名情报多指向钓鱼、欺诈类站点，在办公网出口部署、拦截几乎是立竿见影的，但与 IP 类似的则，如果想要从域名情报背后挖出更多有价值的信息、并进一步扩展完善识别规则，难度也不小，这里就不再展开详细说明了，先给出一些相关推荐：

- https://urlscan.io/
- https://www.phishtank.com/index.php
- https://openphish.com/phishing_database.html
- https://feed.seguranca-informatica.pt/index.php

5.2.5. 网站排名数据

网站排名数据可用于清洗网站黑白名单，并将其置于网络出口处进行快速的可疑外联行为发现，如，C&C 服务器等：

- https://s3-us-west-1.amazonaws.com/umbrella-static/index.html (Cisco Umbrella)
- https://majestic.com/reports/majestic-million （Majestic Million）

以上两个数据都提供了全球高频访问网站的列表，其实早先 Alexa 的 TOP1m 覆盖面会更好，但自 Alexa 被收购后，已不再提供 TOP1m 数据的公开下载。

另外，需要特别关注的是，使用高频访问的排名网站列表清洗白名单已不再是安全专属，反而也会被很多黑客关注，所以不可完全依赖 TOP 列表清洗“白”名单，其中也可能清洗出

“黑”名单，可参考：https://mp.weixin.qq.com/s/HZaXGyI1kDjFpmwlEzCy0A

5.2.6. APT 相关

- https://attack.mitre.org/groups

只看 MITRE 域名就应该知道它的含金量了，这里提供了知名的 APT 组织清单，例如，在 Web3 行业耳熟能详的 Lazarus（拉撒路）。另外，如果你的整个安全对抗体系建设是基于 ATT&CK 分层和路径式建设的话，那么就更巧了，ATT&CK 模型也来自于 MITRE，所以在这份 APT 组织名单的技术分析部分，MITRE 给出了每个组织常用攻击技巧与 ATT&CK 模型的分层映射关系，这就相当于给你现有建设的安全路径做了一个快速指引。

- https://live.sysinternals.com

这个团队早些年专门给 Windows 写各种小工具，写着写着就被微软收了，他们的很多核心工具也被收录到微软的 Resource Kits 里，这些工具时至今日依然在持续更新，是 Windows 下的绝对利器，用好这些工具，可以徒手撸掉 Windows 下大部分后门。

- https://learn.microsoft.com/zh-cn/sysinternals/downloads/sysmon

  https://learn.microsoft.com/zh-cn/archive/blogs/motiba/sysinternals-sysmon-unleashed

以上两篇是微软 sysmon 的参考文章，sysmon 也是来自上面所说的 sysinternals 团队，可实现 Windows 平台下精细化的事件捕获、分析，定制完善的话，可用于常态病毒分析、大规模 threat hunting、批量化安全事件发现、以及自定义蜜罐搭建等，是 Windows 下免费 EDR 的不二之选。

- https://www.nextron-systems.com/thor/

Thor 是一个跨平台的 APT 检测工具，其好处在于支持 Yara 和 IOC，这样就可实现规则动态部署，做线上发现处置非常灵活、响应迅速。

Nex **Vault** × Key **Vault**

官网
nexvault.com

Email
info@nexvault.com

Twitter
x.com/NexVault