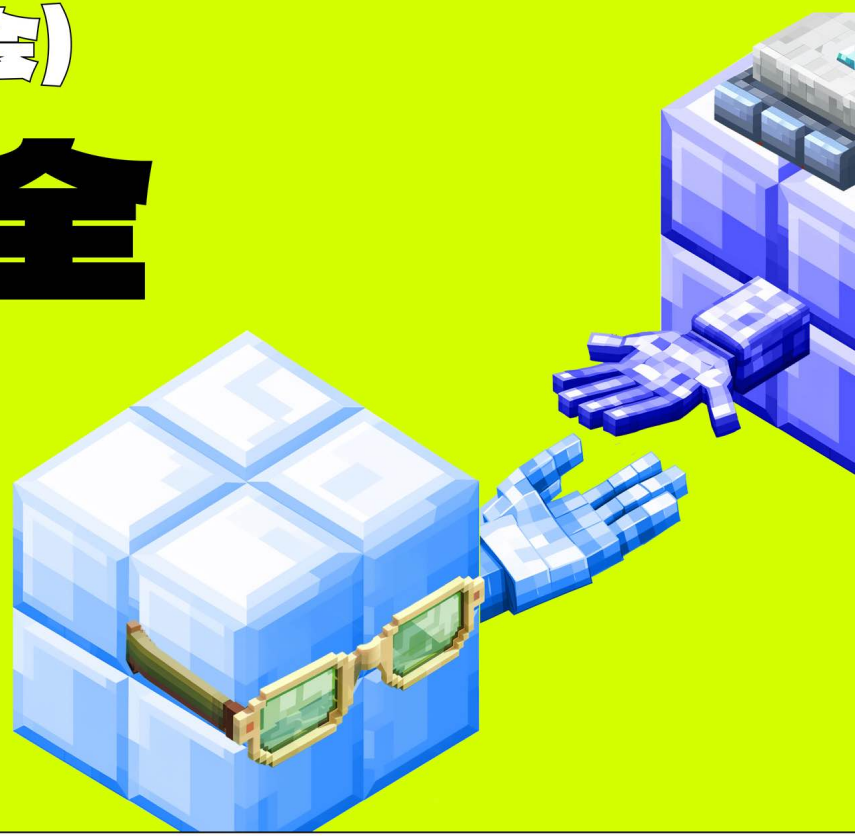
ETHPanda LXDAO

Web3 实习计划（分享会）

Web3 安全



时间 **1月14日 (周三) 8:30-10PM (UTC+8)**

地点 https://us06web.zoom.us/j/89656606782?pwd=DcFMa4RKvxGvevGmtn7yW7pFGoKhrA.1

Meeting ID: 896 5660 6782
Passcode: 261573

Zoom 会议

嘉宾

Adam
@adamsong_web3

@GoPlusSecurity
安全研究院负责人

特别支持 南塘 DAO OGBC SCALINGX Kite AI DataDance SpoonOS ethereum foundation dev growth OneKey NODIT

合作伙伴 reactive PLUTOS CAPITAL

Web3 实习计划

Web3 安全与风险趋势

谁在偷走你的加密资产？

ETHPanda LXDAO

- **01** 不容乐观的 Web3 2025 安全数据
- **02** 典型案例与攻击手法解密
- **03** AI 时代下的安全新挑战
- **04** GoPlus 安全建议

1.11 - 2.8

2025年安全态势总览：损失超35亿美元

安全事件数量

> 1200 起

总损失金额

> 35 亿美元

攻击趋势

精准猎杀 + 广撒网

2025年Web3领域共发生了超过1200起较严重的安全事件，总损失金额超过35亿美元。
值得注意的是，攻击趋势呈现出 “精准猎杀” 和 “广撒网” 并行的特点。
2025年Web3领域安全事件频发，攻击手段呈现多样化和复杂化趋势，对行业构成严重威胁。

精准猎杀：2025损失金额Top事件

- 2月21日，Bybit 遭攻击，损失约15亿美元，原因系 Safe 多签服务器遭渗透篡改交易指令。后续处理：与 FBI 等执法机构合作，冻结超 4000 万美元被盗资产，平台已通过补充储备金，确保用户资产未受损失。
- 5月22日，Cetus Protocol 遭攻击，在 #Sui 上损失约2.23亿美元，原因系Move智能合约漏洞， $CETUS 价格跌超16%。后续处理：Sui 链迅速协同并冻结了 1.62 亿美元被盗资产，社区投票通过了 100% 赔付方案，并获得 Sui 基金会 3000 万美元紧急信贷支持。
- 11月03日，Balancer 遭攻击，多链损失约1.28亿美元，系 Balancer V2 智能合约漏洞。后续处理：Berachain 协调验证者执行紧急硬分叉并冻结攻击者地址；白帽操作员已归还 1280 万美元资金，StakeWise 利用合约管理机制追回约 2000 万美元资产。
- 6月18日，伊朗交易所 Nobitex 遭攻击，多链损失约9000万美元。后续处理：该事件具有地缘政治色彩，攻击者将资金转入无法使用的羞辱性地址，旨在造成瘫痪而非直接获利。
- 4月1日，UPCX 遭攻击，损失约7000万美元，原因系管理员私钥泄露导致ProxyAdmin合约遭非法升级。**后续处理**：转移剩余代币并联合执法部门追踪被盗资产。
- 1月23日，Phemex 遭攻击，多链损失约6910万美元，原因系热钱包被盗。后续处理：发布储备证明（PoR）证实冷钱包安全；平台通过自有资金对受损用户进行分阶段全额赔付。
- 8月14日，土耳其交易所 BtcTurk 遭攻击，损失约5400万美元，原因系热钱包被盗，这是该交易所热钱包在14个月内第二次被盗。后续处理：启动 240 万美元赏金计划寻求线索。
- 12月20日，高净值投资者地址（0xcB8078）遭“地址投毒（Address Poisoning）”钓鱼攻击，损失 4999 万美元 USDT。后续处理：受害者发出链上消息，提议支付 100 万美元作为白帽赏金以换取 98% 资金退回，但目前该攻击者已将资金兑换为 ETH 并通过 Tornado Cash 混币 。
- 2月24日，Infini 遭攻击，损失约4950万美元，原因系管理员权限管理漏洞。后续处理：创始人公开致歉并设立专项赔偿基金，承诺在 2026 年前完成对所有受影响用户的 100% 赔付。
- 7月20日，印度交易所 CoinDCX 遭攻击，损失约4420 万美元，原因系热钱包被盗。后续处理：指定用户补偿计划并追踪被盗资产。
- 7月9日，GMX 遭攻击，损失约4050 万美元，原因系智能合约漏洞。后续处理：攻击者在 48 小时内接受了项目方提出的 10%（约 500 万美元）白帽赏金协议，并归还了约 4000 万美元的被盗资产。
- 12月2日，韩国交易所Upbit 遭攻击，在 #Solana 上损失约 3000 万美元，原因系朝鲜黑客组织渗透攻击。后续处理：与全球交易平台协作对黑客关联地址进行实时黑名单标记及资金追踪拦截。

CeFi成为主要的黑客取款机：2025年单体损失金额超3000万美元的攻击事件 12 起，其中CeFi占了7起，管理员私钥被盗、热钱包私钥被盗是最主要的原因，暴露了显著的风险。

DeFi漏洞越来越深入：DeFi领域的安全性在2025年表现出相比往年更好的抗压性，合约漏洞导致的损失却远低于TVL的增长率 。但值得注意的是 Balancer、Yearn 这类已安全运营数年的智能合约不断被挖掘出新的漏洞，以及Move智能合约漏洞明显增多，体现出攻击者利用 AI 技术挖掘智能合约漏洞的能力正在不断增强。

国家级黑客的“业绩”巅峰：2025年，朝鲜黑客组织（如 Lazarus Group）盗取的资金继续高速增长，在2025年至少盗取了20.2亿美元的加密资产，较2024年增长了51%，创下朝鲜通过网络攻击获取资产的历史新高 。朝鲜黑客的攻击模式在2025年完成了深度进化：

- **社会工程**：通过伪装成Web3或AI公司的招聘人员，在LinkedIn等平台进行数月的关系维护，最终通过“技术面试”环节诱导目标员工下载带有后门的测试代码 。
- **精准猎杀**：他们将精力集中在少数拥有巨额资金储备的机构或个人身上。在2025年的所有机构级侵害事件中，朝鲜黑客贡献了超76%的金额 。
- **洗钱工业化**：资金在被盗后迅速进入一个高度自动化的洗钱链条，通常可以在45天内完成从链上混币到非法平台法币结算的全过程 。

广撒网：高频攻击与欺诈类型

ETHPanda LXDAO

私钥窃取
Private Key Theft

发生次数:**> 300 起**

损失金额:**> 18 亿美元**

针对性狩猎，基于病毒木马、社工和供应链渗透。

钓鱼攻击
Phishing Attacks

发生次数:**> 400 起**

损失金额:**> 7.5 亿美元**

AI生成钓鱼，全平台化，签名陷阱。

Rug Token
Token Scam

发生次数:**约 300 起**

损失金额:**> 6 亿美元**

碎片化撤池，隐藏后门，职业化与团伙化。

与此同时，“广撒网” 式的攻击也在持续泛滥。私钥窃取、钓鱼攻击 和 Rug Token 是最高发的三种类型。特别是随着 AI 技术的普及， 钓鱼攻击变得更加难以辨别， 而 Rug Token 也呈现出职业化和团伙化的趋势。

典型案例与攻击手法解密

ETHPanda LXDAO

2.1 Bybit – 史诗级多签前端篡改攻击

这是2025 年全球 Web3 领域损失最惨重的安全事件，典型的“供应链”式攻击，攻击者没有直接攻击目标本身，而是侵入了其依赖的多签基础设施 Safe{Wallet}。

- **原理解析与过程分析**
  - **入侵前端**：朝鲜黑客组织 Lazarus Group 入侵了 Safe{Wallet} 一名具有系统发布权限的开发者的设备。随后，他们获取了 Safe 在 AWS 上的账户权限，向官方前端代码中注入了恶意脚本。
  - **定向欺诈**：恶意脚本仅针对 Bybit 的特定多签钱包地址生效。当 Bybit 的三名多签管理员使用被污染的 Safe 官方前端进行日常资金调拨时，前端界面显示正常，但背后生成的交易数据却被替换为调用黑客预先部署的恶意合约。
  - **盲签漏洞**：管理员使用硬件钱包签名时，由于设备无法完整解析和显示复杂的合约调用交易内容，导致了“盲签”，未能发现交易异常。
  - **夺取控制权**：恶意交易通过 `DelegateCall` 方式，将钱包的逻辑合约升级为攻击者控制的合约，从而完全掌握了该多签钱包的控制权，转走了巨额资产。
- **安全建议**
  - **对项目方**：涉及大额资产的操作，应建立独立的多方验证机制，避免所有签名者使用同一前端或服务。
  - **对用户**：在进行重要交易签名时，务必在钱包等设备上仔细核对交易数据的哈希和详细内容，警惕任何“盲签”请求。

2.2 UXLINK – AI 深伪（Deepfake）与社工攻击

这起事件揭示了即使采用多签，“人”始终是最脆弱的安全风险。

- **原理解析与过程分析**
  - **AI 深伪获取信任**：攻击早在9月22日之前就开始了，攻击者在 Telegram 上冒充可信的商业伙伴，营造出一种熟悉的假象。发起视频会议，并使用 Deepfake 技术（实时换脸和语音克隆）骗取了 UXLINK 人员的信任。
  - **木马植入**：会议期间，攻击者诱导 UXLINK 人员点击恶意链接，导致个人电脑被静默植入病毒木马，多个多签账户私钥泄露。
  - **夺取合约权限**：利用窃取到的私钥，攻击者移除了原管理员，并添加自己为新的管理员。
  - **盗取与增发**：攻击者首先转走了钱包内的现存资产。随后，他们恶意增发了大量UXLINK代币并在市场抛售。
- **安全建议**
  - **权限隔离**：严格区分**资金钱包**与**权限钱包**。用于管理合约权限的多签钱包不应存放大量资金，且签名设备必须与其他上网设备物理隔离。
  - **强化人员安全**：对核心成员进行持续的安全意识培训，警惕各类社交工程攻击。
  - **治理升级**：对于已部署合约及管理员地址，应及时进行治理与替换，避免长期不变产生风险。

2.3 Balancer – 计算精度与合约漏洞

这起事件展示了DeFi协议在复杂业务逻辑和数学计算中，微小的错误可能引发的巨大风险和损失。

- **原理解析与过程分析**
  - 漏洞根源：Balancer 攻击事件的根本原因是计算精度（向下取整）问题。
  - Balancer Vault在 `swap` 计算时存在精度损失，即每次计算的结果都是向下取整，这影响到了Vault中的Token价格。
  - `batchSwap` 进行批量 `swap` 放大了该漏洞，攻击者可以通过构造批量 `swap` 的参数，极大地压低Vault中Token的价格，攻击者利用价格差获利。
- **安全建议**
  - **持续的深层业务漏洞挖掘**：充分应用 AI、形式化验证等能力更强，效率更高的安全技术，提高漏洞挖掘效果，尤其对于深层业务漏洞，不能仅依赖于人工审计。

2025年，Web3安全威胁的演变呈现出显著的技术融合、智能化与自动化特征。攻击者不再局限于单一技术，而是将新型协议特性、供应链漏洞、人工智能与自动化工具深度融合，构建出破坏力更强、更隐蔽、成本更低的攻击范式。

更多案例： https://x.com/GoPlusZH https://x.com/GoPlusSecurity

攻击方式演变与新技术骗局

3.1. EIP-7702与新型钓鱼

EIP-7702 作为以太坊 Pectra 升级的核心提案，旨在实现 EOA 账户的智能化，提升账户抽象能力和用户体验。然而，这一创新也迅速被黑客武器化，催生出攻击门槛更低、隐蔽性更强的钓鱼攻击模式。

原理说明：

EIP-7702的核心机制是允许 EOA 通过 `SetCode` 操作临时注入代码，实现委托（Delegation）授权。攻击者利用这一特性，预先控制已泄露的私钥地址，并将其授权给恶意 `Delegator` 合约。该合约会将用户后续转入的资金进行自动化转移。

与传统钓鱼不同，此模式不依赖前端UI欺诈，传统的恶意授权、签名检测等安全机制也无法生效，进一步放大了风险，用户易陷入“私钥即资产”的认知偏差，导致资产损失。此外，结合批量执行（`Batch`）能力，也大大提升了钓鱼攻击效率。

EIP-7702 新型钓鱼通常可分为四个阶段：

1. **准备阶段**：攻击者从暗网或历史泄露数据库获取私钥，并授权给多链部署的恶意Delegator合约（ETH、BSC、Base较常见）。
2. **诱导阶段**：通过私信等社媒方式让用户接触到这些地址私钥，并诱导用户以为“天上掉馅饼”。
3. **执行阶段**：一旦用户转入Gas或Token，恶意Delegator合约就会自动将用户转入的资金提走，用户资产即时流失。
4. **洗钱阶段**：资金通过混币器或跨链桥自动化转移，追踪难度高。

更多案例：

2025年Q2，Inferno Drain 团伙利用EIP-7702的新型钓鱼案例大爆发，窃取了数百万美元的加密资产，其中不乏单一案例金额超150万美元的大案。更多详情请参考：

- https://x.com/GoPlusZH/status/1930805446262284771
- https://x.com/GoPlusZH/status/1946113759938019701
- https://x.com/GoPlusZH/status/1942854235542245386
- https://x.com/GoPlusSecurity/status/1930614660996518198
- https://x.com/GoPlusSecurity/status/1946510327312797930
- https://x.com/GoPlusSecurity/status/1942916699579421117

3.2 软件供应链攻击：自传播蠕虫与跨生态破坏

2025年，开源供应链攻击案例激增，以Shai-Hulud及其变种2.0为代表的蠕虫式恶意软件，对npm、Maven等生态造成全球性冲击，影响超过25,000个GitHub仓库。

原理说明：

不同于单一包投毒，Shai-Hulud采用自复制蠕虫机制：入侵维护者账户后，注入 `postinstall` / `preinstall` 脚本，实现凭证窃取和自动传播。核心利用TruffleHog工具扫描文件系统，窃取AWS/GCP/Azure密钥、npm令牌和GitHub PATs。随后，蠕虫遍历依赖图谱，注入恶意负载并发布新版本，实现指数级扩散。

软件供应链攻击通常可分为三个阶段：

1. **初始入侵**：通过钓鱼等方式窃取流行开源项目（如 `debug`，`chalk`）开发人员的账户权限，并向代码仓库中发布有毒代码。
2. **蠕虫行为：** 恶意脚本（如 `setup_bun.js`）在安装阶段（`preinstall`）执行，自动窃取开发环境中的 npm 令牌和 GitHub PAT，并利用这些凭证自动扫描该开发者名下的所有其他仓库，注入恶意代码并重新发布，实现跨项目感染。
3. **执行与窃取**：一旦其他开发者使用了包含有毒代码的仓库，攻击者就会通过远程加载、后台执行等方式实施破坏和窃取。
4. **跨生态传播**：从npm蔓延到Maven/Java，攻击窗口通常在数小时到数天不等，影响10亿+下载。

更多案例：

Shai-Hulud 2.0 波及超过700个npm包和25,000个GitHub仓库。由于受影响的底层库每周下载量以亿计，导致全球数千个DApp前端在不知情下沦为黑客的资金窃取工具。

软件供应链攻击的危害不仅限于大规模传播，对单一项目的针对性攻击也是需要重点防范的内容，12月25日，Trust Wallet 浏览器钱包 2.68.0 版本被植入了恶意后门，波及大量用户，损失超七百万美元。

3.3 AI深伪与社会工程：数字身份信任的系统性崩塌

AI 的飞速发展使社会工程攻击从静态欺诈转向动态、个性化互动，Web3社会工程学攻击中，应用AI深伪技术的占比超56%，2025年因AI深伪与社会工程造成的损失，增长高达3000%。

原理说明：

利用 AI 大模型能力，实时生成伪造的视频/语音，结合大数据分析受害者社交足迹，构建“鱼叉式”钓鱼。核心是模拟人类交互行为，AI代理可进行长时间对话，诱导用户安装木马、分享私钥或转账交易。

AI深伪攻击通常可分为三个阶段：

1. **情报收集**：从X、TG、Discord 收集受害者信息，选定目标。
2. **伪造生成**：使用AI工具创建视频/语音。
3. **互动诱导**：通过视频会议或语音通话建立信任，诱导用户安装木马、分享私钥或转账交易。
4. **执行与逃逸**：资产转移后销毁痕迹，攻击成本大大降低，成功率提高超50%。

更多案例：

2025是Web3领域AI深伪与社会工程攻击高度爆发的一年，案例数不甚数，典型的如UXLINK事件和Venus大户钓鱼事件，更多详细内容：

3.4 AI智能合约漏洞挖掘：自动化攻防的军备竞赛

AI 智能合约漏洞挖掘在2025年展现出独立发现和利用智能合约漏洞的能力，推动传统智能合约漏洞挖掘与利用的范式转变。

原理说明：

AI 模型如Claude Sonnet 4.5+ 和 GPT-5+，通过训练海量Solidity代码，模拟执行路径识别语法错误、逻辑缺陷等智能合约漏洞，并利用AI生成攻击脚本，自动化实现漏洞的挖掘与利用。

AI智能合约漏洞挖掘通常可分为三个阶段：

1. **漏洞扫描**：AI分析合约代码，识别零日漏洞。
2. **模拟验证**：AI分析漏洞，进行有效性验证。
3. **漏洞利用**：AI生成攻击代码，进行自动化漏洞利用。

更多案例：

2025年，Balancer、Yearn 等多个已安全运营数年的智能合约不断被挖掘出新的漏洞，体现出攻击者利用 AI 挖掘深层智能合约漏洞的能力正在不断增强。更多详细内容：

GoPlus 安全建议

ETHPanda LXDAO

对用户：养成安全习惯

- 养成“不点、不签、不装、不转”的好习惯。
- 通过官方渠道下载App并交叉验证。
- 安装安全插件，警惕钓鱼链接。
- 签名时务必核对内容，拒绝盲签。
- 购买代币时核对合约地址，检查风险。
- 妥善保管私钥/助记词，冷热钱包分离。

对生态：全周期安全管理

开发阶段：安全左移

采用安全合约模板，集成 AI Auditing 工具。

运行阶段：全周期监控

集成安全 API， 透明化锁仓。

响应阶段：快速应急

与安全团队合作，预先建立沟通机制。

原生安全：协议层升级

安全是Web3通往大规模应用的必经之路，安全不再是事后补救的成本，而是决定Web3能否走向主流的关键基础设施。