GeekCon

「DAF漏洞与利用挑战赛

DAF Contest

」



种下一颗不让世界变坏的念头

One seed, a world unspoiled

GeekCon

DAF漏洞与利用挑战赛

守护 V.S 掠夺：加密钱包竟成洗劫入口？

一种利用未知缺陷控制多款虚拟货币硬件钱包
窃取助记词 / 实现“恶意”转账的挑战

种下一颗不让世界变坏的念头

One seed, a world unspoiled

攻防速写｜假如捡到 Web3 硬件钱包的人是黑客

原创 攻防速写 DARKNAVY 2025年03月30日 10:25 上海

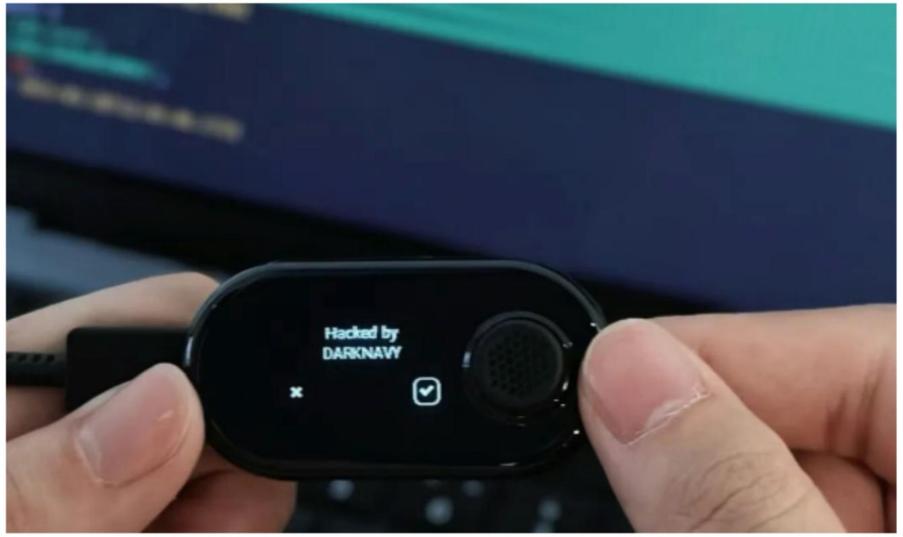


2024年，由私钥泄露引发的Web3安全事件频发，总计造成了高达8.55亿美元的巨额损失。

私钥作为账户的唯一凭证，直接关联链上所有资产（加密货币、NFT等）。由于区块链的去中心化特性，丢失私钥即永久失去账户控制权，泄露则导致资产被盗。**硬件钱包**通过离线存储私钥、采用安全芯片等技术，成为资产保护的主流选择。

但当黑客的指尖触碰到硬件钱包金属外壳的瞬间，数字深渊的潘多拉魔盒会被打开吗？

在本篇攻防速写中，我们将从攻击者视角梳理DARKNAVY对Web3硬件钱包开展的一点研究。



DARKNAVY对流行Web3硬件钱包的破解

硬件钱包安全

我们在两款钱包的 MCU 上实现了 RCE,
但仅仅在屏幕上显示 Hacked 并不能造成实质性的危害

许多硬件钱包使用安全芯片〔SE〕校验 PIN 码、保护助记词和私钥,
在 RCE 之后，PIN 码 / 助记词 / 私钥是否仍然安全?

硬件钱包安全

本次项目，两款钱包使用的 SE 都不典型。

Cypherock X1：Vault + Card

- Vault 有 SE，但仅用于真实性验证
- Card 存放〔部分〕私钥、验证 PIN，实际相当于外置 SE

硬件钱包安全

本次项目，两款钱包使用的 SE 都不典型。

Blockstream Jade：Device + cloud blind oracle

- 设备无 SE，助记词加密保存
- 云端 “blind oracle” 校验 PIN、储存助记词的解密密钥，相当于虚拟 SE

硬件钱包安全

MCU 与这两种 “SE” 的通信都需要用户辅助〔刷卡 / 转发请求〕

两种 “SE” 仅对私钥的安全存储有意义，而钱包的生成和使用：

- **钱包初始化时，助记词直接由 MCU 创建；**
- **解锁设备后，私钥直接保存在 MCU 内存中。**

硬件钱包安全

攻击场景:

攻击者事先控制受害者的PC（投毒、钓鱼……）

检测到用户连接并解锁钱包后，发起攻击、窃取私钥

两款钱包均受影响

硬件钱包安全

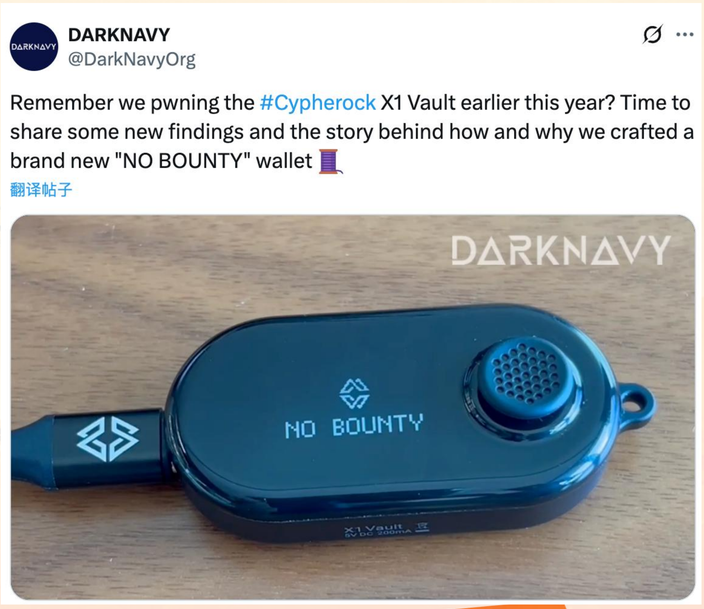
针对两款设备的特性，还有更多的利用方式：

- Jade 允许 self-host blind oracle，通过 RCE 读取通信密钥并修改配置，可以实现 MCU – virtual SE 之间的中间人攻击
- 邪恶女仆场景：
  机主下一次解锁时，中间人远程截获 PIN 码、解密助记词

硬件钱包安全

针对两款设备的特性，还有更多的利用方式：

- X1 自行编写的 bootloader 一言难尽，RCE 的能力可以刷入任意固件并绕过启动校验
- 供应链场景：
  控制“随机”生成的助记词 / nonce



GeekCon

「谢谢」



种下一颗不让世界变坏的念头

One seed, a world unspoiled