昨日，外媒报道 Nomad 代币桥遭遇了漏洞攻击，导致其 1.9
亿美元资产被掏空。
与此同时，不知名的攻击者也在周二晚间扫荡了数千个包含价值至少 400 万美元的 Solana 和 USDC 的加密货币钱包。Decrypt.co
指出，攻击发生于太平洋标准时晚间 20:00，并且似乎起源于 Solana 浏览器钱包 Phantom 。

分析人士推测，用户的密钥可能遭到了破解，结果导致超过 5000
个钱包被掏空数百万美元，并让 Solana 币价在数小时内发生了暴跌。

> 区块链审计公司 OtterSec 在晚间披露 —— 过去数小时内，超过 5000 个 Solana 钱包被洗劫一空。
>
> 这些交易由实
> 际所有者签署，因而意味着
> 发生了某种形式的私钥泄露。（不久后，Watcher Guru 将计数更新至 8000+ ）

事件发生后，许多工程师携手努力了解漏洞利用的细节和严重程度。ETH 钱包 MetaMask 的一位发言人称：

> 我们正在与受影响的加密货币钱包团队积极沟通，以提供力所能及的帮助，并确定怎样才能更好地保障用户安全。

早期报告重点提到了 Phantom 浏览器钱包和 Solana 生态系统，而后 CoinMarketCap 数据显示：

> 黑客攻击事件曝光后两个小时内，Solana 币价跌去了 8% 。且在过去 24 小时内，其交易量大涨了 45% 。

加密货币投资者兼分析师 Miles Deutscher 写道：

> 有个未知的 $SOL 漏洞正在利用 Phantom 加密货币钱包，目前已知有 600 万美元资产被盗。
>
> 如果你在 Phantom 存有资金，还请将之转移到硬件钱包 +

确保撤销所有权限。

此外热门 Solana NFT 市场 Magic Eden 也在官方 Twitter 账号上发布了这一漏洞警告：

刚刚曝出了一个影响广泛的 SOL 漏洞利用，其正在扫荡整个生态系统的钱包。

与此同时，Magic Eden 也分享了如何移除可疑链接权限的说明。

至于 Phantom，该钱包团队表示正在与多方保持密切合作，以查明 Solana 生态系统中曝出的新漏洞，后续会及时分享更多细节。

不幸躺枪的 Twitter 网友 @JustinBarlow 哭道：“我存在 @slope_finance 和 @TrustWallet 上的 ERC-20 和 SPL USDC 都被洗劫一空了”。

而后加密分析师 @0xfoobar 证实：“攻击者正在窃取原生（SOL）和 SPL 代币（USDC），事件波及许多 6 个月未曾活跃过的钱包账户”。

理论上讲，本次事件或属于“上游依赖型供应链攻击”，但就算参照其它区块链大事件而撤销回滚，转移到冷钱包的加密代币也是无法被追回的。

深究下来，还是因为这些 SOL 和 SPL 代币是借由用户私钥签署、而非经过第三方批准而转让的 —— 这意味着幕后可能发生了大规模的私钥泄露。

对此，Solana Labs 联合创始人 Anatoly Yakovenko 澄清道：

所谓的交互性并没有让钱包本身的安全性变得更加脆弱，毕竟只有特定于代币的委托、自动批准、或泄露的 seed，才能从用户的钱包中转移资产。

最后附上本轮黑客攻击事件中最受关注的涉案钱包地址：

- https://solscan.io/account/Htp9MGP8Tig923ZFY7Qf2zzbMUmYneFRAhSp7vSg4wxV#solTransfers

- https://solscan.io/account/CEzN7mqP9xoxn2HdyW6fjEJ73t7qaX9Rp2zyS6hb3iEu#solTransfers

- https://solscan.io/account/5WwBYgQG6BdErM2nNNyUmQXfcUnB68b6kesxBywh1J3n#splTransfers

- https://solscan.io/account/GeEccGJ9BEzVbVor1njkBCCiqXJbXVeDHaXDCrBDbmuy#solTransfers