2月15日，bZx团队在官方电报群上发出公告，称有黑客对bZx协议进行了漏洞攻击，造成部分ETH已经丢失；2月18日，bZx疑似遭遇第二次攻击，不同的是本次的对象是ETH/sUSD交易对。

这一事件被高度关注，因为它并非一起简单的、针对单一漏洞的“黑客式”攻击，它本质上更像是利用DeFi协议和产品的一次套利操控。“攻击者”充分利用DeFi的多个协议和产品的功能，以很低成本获得资金，通过操纵价格，实现获利。

借DeFi十几秒套利百万美金

首次攻击发生在2月15日，攻击者通过“闪电贷”0成本借得1万个ETH作为初始资金，利用多个DeFi协议的相互调用，实现了一笔非常不合理的交易。

第一步：通过“闪电贷”0抵押物从dYdX借出1万个ETH；

第二步：将其中5500ETH在Compound中抵押借贷112 WBTC 的贷款抵押；

第三步：将1300ETH在bZx被发送到fulcrum，打开了一个ETH/BTC交易对的5倍杠杆空头头寸；

第四步：通过Kyber Reserve到Uniswap WBTC pool卖5637ETH（150 万美金），获得51.34BTC（51万美金）；

第五步：把Compound借出来的112BTC，在 Uniswap WBTC pool卖112 WBTC,获得6800 ETH；

第6步：将 3200 ETH + 6800 ETH（卖 112 BTC 获利）=10000ETH 还给 dydx。

据悉，攻击者获得总利润为1193ETH，目前价值 29.8万美元。

2月18日，bZx再次发现了使用“闪电贷”进行的可疑交易，尽管首次攻击发生之后，bZx关闭了Fulcrum
交易平台进行维护，但该攻击者再出新招，使用了Synthetix进行交易，目前bZx已暂时关闭被利用的合约。

Ethhub 创始人Eric
Conner估算到，这一次攻击者获利2388个ETH，约64.4万美金。

这两起攻击事件或许暴露出DeFi系统性金融风险的隐患，并对行业的发展具有很强的警示意义。

此次事件也给了DeFi从业者一个警示，随着DeFi领域锁定资金量级的增加，设计产品一定要考虑所接入的其他协议可能会对本身协议造成的影响和风险。