基于以太坊的浪人桥被黑客窃取了173600个以太坊和价值2500万美元的USDC，总价值超过6亿美元。

这次攻击成为了DeFi历史上最大的一次攻击。，比保利网络黑客事件还多。这两种攻击有一定的相似性，都是针对智能合约的一些固有漏洞。

Ronin对攻击进行了初步分析，并采取了一定的安全措施来防止进一步的损失。

当前，去中心化交易市场Katana和Ronin的交易已经停止。

此外，Ronin团队声称，他们目前正在与执法官员和其他专家合作，&quot追回或要求退款&quot所有基金中。AXS、罗恩和SLP&#039；桥上的美国资金仍然是安全的。

黑客利用Ronin验证器和AxieDAO验证器中的一系列漏洞盗取资金。相关报告显示黑客用被黑的私钥取钱。我们发现这个攻击是因为一个用户说5000以太坊不能从Bridge中提现。

随着事情发酵，黑客通过SkyMavis和AxieDAO控制的验证器。，获得了私钥。后者被&quot滥用&quot以太坊跨链解决方案中无供气RPC节点。

SkyMavis验证者可以签署之前合作的AxieDAO交易。这为黑客提供了额外的攻击点。

帖子还指出，黑客一旦接入SkyMavis系统，就可以通过使用RPC从AxieDAO验证器获取签名，无需气费。我们已经确认恶意提现中的签名与五个疑似验证者一致。

Ronin将交易的验证者阈值从5提高到8，这将在短期内防止进一步攻击的风险。

该解决方案将迁移其节点，并保持其网桥在多个平台上暂停。。当&quot我们确信没有钱会有危险&quot，大桥将重新开放。

Ronin背后的团队将与ChainAnalysis公司合作，跟踪监控被盗资金。最重要的是他们正在与中央交换机通信，以阻止与黑客有关的地址。

然而，由于发现这起黑客事件花了近一周的时间，这些黑客可能已经将一些资金转移到了CryptoExchange的Crypto.com和FTX。

Crypto交易所FTX的首席执行官Sam Bankman-Fried表示他们目前正在进行调查，并将“酌情”采取行动。

积极提供可扩展解决方案的以太坊开发者KelvinFichter在看了这篇报道后，对黑客攻击进行了评论。

费希特认为SkyMavis运行多个Ronin节点是一个错误。，并指出了此次事件与其他黑客事件的区别。

费希特说，这和以前的桥牌黑客很不一样，他们基本上攻击的是智能合约的漏洞。。这件事更多的是一个&quot经典&quot对多密钥安全设置中私钥的攻击。

我认为这里最根本的错误是对基于验证者的桥的依赖。浪人桥有一个基本的假设，就是绝大部分的密钥都不能泄露。明显地这个假设已经被打破了。

浪人还有一个&quot最低监控和报警&quot系统，这给了黑客可乘之机。这让浪人队看起来&quot坏&quot，但它也可以用作类似解决方案的安全警告。

费希特在推特上发布了他认为的解决方案。首先，如果你有安全假设的工程实践，验证者桥是可以工作的。其次，虽然建立可信桥梁的难度更大，但这条线路更安全。

n

原文来自比特币，由区块链奈特编译，英文版权归原作者所有。中文转载请联系编辑。

本文来源：区块链骑士n原标题：解读以太坊浪人桥黑客入侵事件价值逾6亿美元声明：本文为作者&#039；在&quot火星&quot且不代表火星财经官方立场。n转载请联系页面下方：内容合作栏目。，邮件授权。授权后转载请注明本文来源、作者及链接。未经许可转载本站文章将被追究相关法律责任，并追究侵权行为。n提示：投资有风险，入市需谨慎。这些信息不会被用作投资和财务建议。声明：作为区块链信息平台本站提供的信息不代表任何投资建议，本站发布的文章仅代表个人观点，与火星财经官方立场无关。虚拟货币不具有等同于法定货币的法律地位，参与虚拟货币投资交易存在法律风险。火星金融反对各种代币投机。请投资者理性对待市场风险。由提供的n语音技术关键词：黑客道安全以太坊攻击