

Kahf钱包已经恢复运行 2.0公测版本正式上线

原创 Qitmeer Network Qitmeer 中文社区 2022-06-24 08:30 发表于香港



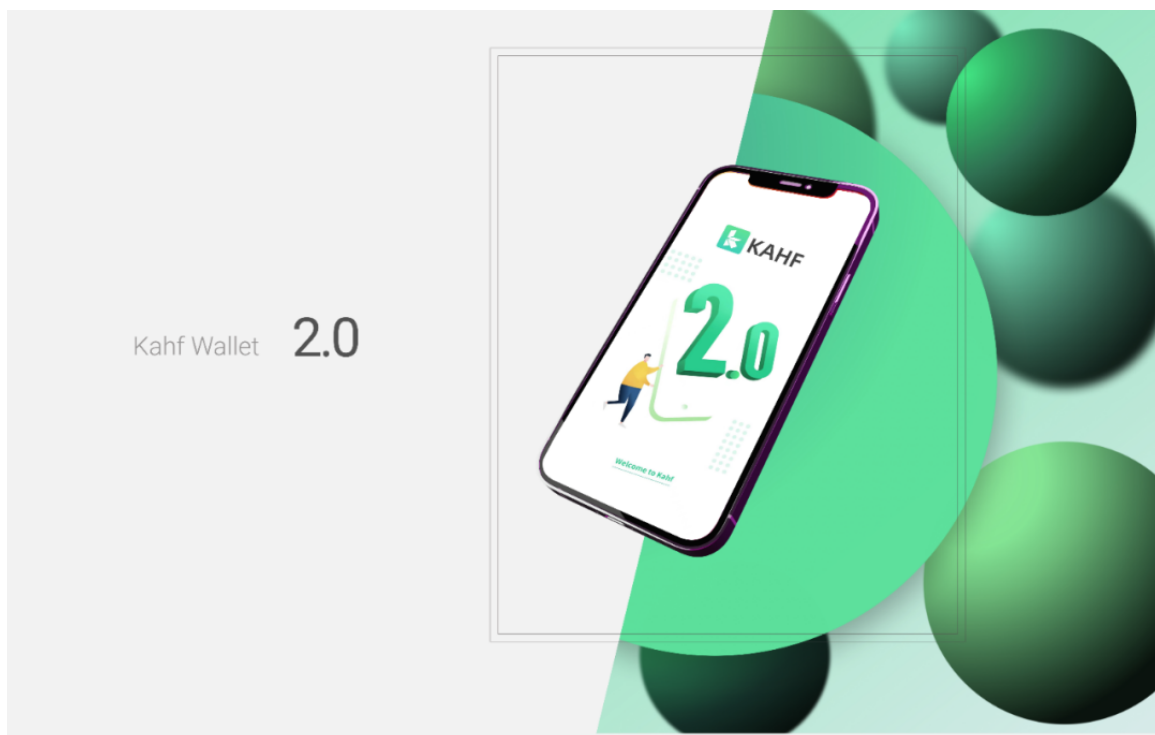
目前钱包及官方网站访问已经恢复正常

尊敬的Qitmeer社区用户：

Kahf钱包在6月20日遭遇DDOS攻击后，团队紧急暂停了Kahf钱包的下载、转账、提现等功能。在对钱包进行紧急维护的同时，考虑到服务器安全策略的升级，并且新版本钱包已经开发完成，**为了提高各项测试效率，加强钱包网站安全性，提升用户体验，我们决定提前上线Kahf 2.0版本钱包，让用户体验更多新的功能。**由于本次维护更新时间较长，给社区用户带来的不便，我们深表歉意！

1

目前钱包及官方网站访问已经恢复正常，请大家进入官网（<https://kahf.io/>）或者谷歌商店及App Store下载更新，体验Kahf2.0版本全新功能。



Kahf是一个支持多链的自托管钱包，支持ETH，BSC等主流公链。Kahf钱包用户通过一套助记词，即可管理所有 10+ 主链的各种数字货币。用户可以完全控制自己的加密资产，安全存储加密数字货币，资产自我掌控。

去中心化钱包完全依靠私钥或助记词来管控资产，一旦私钥或助记词丢失将无法找回，若是私钥或助记词泄露或被盗，将直接威胁资产安全。因此在更新2.0版本钱包之前，请大家妥善备份自己的助记词，请勿授权异常域名钱包权限。

本次2.0版本更新的主要内容有：

- 1) 本次更新版本为2.0的公测版本，集成了QNG Testnet版本。
- 2) 升级视觉UI，给用户带来非同一般的全新视觉盛宴。
- 3) 除Qitmeer Network外，同时还支持多种主流网络钱包。
- 4) 支持各类DEFI应用，基于Qitmeer Network的生态应用已列入DAPP浏览器。
- 5) 集成多链搜索引擎功能，随时进入多链去中心应用世界。



钱包客户端的出现是为了让普通用户使用起来更加便捷，一般而言，这种可视化界面的代码程序是储存在中心化服务器上的，当然也有一些去中心化的解决方案。在遭遇攻击后用户使用客户端钱包的功能就会受到影响，对于一些不了解区块链运作的用户而言，因看不见资产显示就担心自己的资产消失了从而造成不必要的恐慌。实际上只是可视化界面显示出现问题（由于攻击），用户的资产是储存在区块链上的，只要区块链网络是安全的，用户的资产也是安全的。

除Kahf钱包之外，**Qitmeer 拥有适配网络的命令行钱包 qitmeer-wallet**，能够提供基础的钱包功能，你可以使用它进行私钥管理以及交易转账。只需要从官方代码库克隆代码后进行编

译后，匹配好配置文件和节点间的对应，之后就可以创建一个属于你自己的钱包啦！下图简单演示了使用该命令行钱包获取账户余额的一种使用方式：

```
D:\git\qitmeer-wallet>qitmeer-wallet.exe console
wallet-cli:2022-06-23|20:04:08.037 [INFO] Established connection to RPC server 127.0.0.1:18131 module=RPCCLI
2022-06-23|20:04:08.092 [INFO] notification rescan block start=858339 end=858346
update history block:858346/858346
wallet-cli:help
Usage:
<command> [arguments]
The commands are:
<createNewAccount> : Create a new account. Parameter: [account]
<getBalance> : Query the specified address balance. Parameter: [address]
<listAccountsBalance> : Obtain all account balances. Parameter: []
<getTx> : Gets transaction by ID. Parameter: [txID]
<getListTxByAddr> : Gets all transactions that affect specified address, one transaction could affect MULTIPLE addresses. Parameter: [address] [stype:in,out,all]
<getBillByAddr> : Gets all payments that affect specified address, one payment could affect only ONE address. Parameter: [address] [filter:in,out,all]
<getNewAddress> : Create a new address under the account. Parameter: [account]
<getAddressesByAccount> : Check all addresses under the account. Parameter: [account]
<getAccountByAddress> : Inquire about the account number of the address. Parameter: [address]
<importPrivKey> : Import private key. Parameter: [priKey]
<importWifPrivKey> : Import wif format private key. Parameter: [priKey]
<dumpPrivKey> : Export wif format private key by address. Parameter: [address]
<getAccountAndAddress> : Check all accounts and addresses. Parameter: []
<sendToAddress> : Transfer transaction. Parameter: [address] [coin] [num]
<updateblock> : Update Wallet Block. Parameter: []
<syncheight> : Current Synchronized Data Height. Parameter: []
<unlock> : Unlock Wallet. Parameter: [password]
<help> : help
<exit> : Exit command mode

wallet-cli:getAccountAndAddress
Wrong command getAccountAndAddress
wallet-cli:getAccountAndAddress
account:imported, address:Mm1URDpnkEmE8zrwZ4eQCFBLxmtEPBx2UsQ
wallet-cli:getBalance Mm1URDpnkEmE8zrwZ4eQCFBLxmtEPBx2UsQ
coin:MEER
0
wallet-cli:
wallet-cli:
```

关于该钱包的详细使用方法欢迎参照说明文档或者到官方论坛进行讨论。

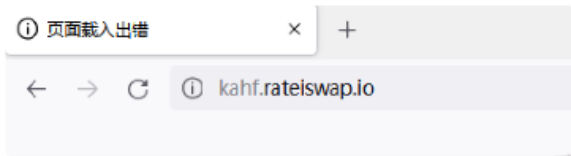
Qitmeer-wallet 官方代码库：

<https://github.com/Qitmeer/qitmeer-wallet>

3

关于此次Kahf钱包遭受攻击事件，专注于区块链安全的零时科技公司对此次事件做了详细分析报告，并给出了相应的安全建议。

钓鱼网站：访问后浏览器显示<http://kahf.rateiswap.io/>网址：



可以明显看出对ratel进行了混淆，钓鱼网站使用了大写 i 来替换 ratel 中的 l。已达到欺骗用户的效果。

钓鱼网站相关域名及IP

解析域名	域名发现时间	微步判定	微步标签	解析IP
rateiswap.io	2022-06-22	未知	暂无	113.114.212.123
kahf.rateiswap.io	2022-06-22	未知	暂无	113.114.212.123

该钓鱼网站初始页面，可下载APP。

从上述攻击事件来看，这是一起蓄谋已久的攻击，攻击者主要通过DDOS攻击使得官网网站不得已进行维护，随后在维护期间向内测用户传播疑似官网的钓鱼链接，窃取用户私钥完成获利。

给官方的安全建议

- 建议升级后端服务器配置
- 建议备份网站，用来在可能发生的攻击后通知用户网站处于维修
- 建议社区给用户发布正确官网的渠道及APP下载渠道，避免再次损失资金

给用户的安全建议：

- 建议对官网有做记录，或者访问官网时仔细确定是否为官方域名
- 建议从官方应用商店安装加密钱包应用，不要从第三方来源下载
- 如果有不小心泄露助记词，需要立即将钱包资金转移

报告详细内容如下：

附（零时科技针对Kahf钱包被黑客DDOS攻击的事件分析报告）：

<https://github.com/meerfans/meerdocs/blob/main/KahfDDoSAnalysisReport.pdf>

I 零时科技

深圳零时科技有限公司（简称：零时科技），公司成立于2018年11月，是一家专注于区块链生态安全的实战创新型网络安全企业，团队扎根区块链安全技术研究，以丰富的安全攻防实战经验结合大数据分析处理，为用户提供区块链安全漏洞风险检测与安全防御、企业级区块链应用创新解决方案。

官方网站：<https://www.noneage.com/>

II Qitmeer Network

Qitmeer Network 是基于BlockDAG技术的新一代支付网络基础设施，采用Layer1+Layer2（链上+链下）的扩容方案，以跨链智能合约链接整个区块链生态。

官方网站：<https://www.qitmeer.io>

关注Qitmeer Network社区

了解最新网络信息

“向上滑动查看”





官方网站

<https://www.gitmeer.io>



GitHub 开源社区交流

<https://github.com/Qitmeer/>

