Kahf 钱包遭攻击

0x1 前言

2022/06/20下午4点，Kahf钱包测试域名***http://kahf.ratelswap.io/***遭遇了DDOS攻击，黑客借助钱包团队对服务器进行维护的期间，向内测用户传播钓鱼链接，部分测试用户下载了非官方版本测试apk文件，被钓取个人助记词，导致资产丢失。根据社区用户反馈，累计资产损失达7000USDT。

0x2 钓鱼网站分析

相关网站如下：

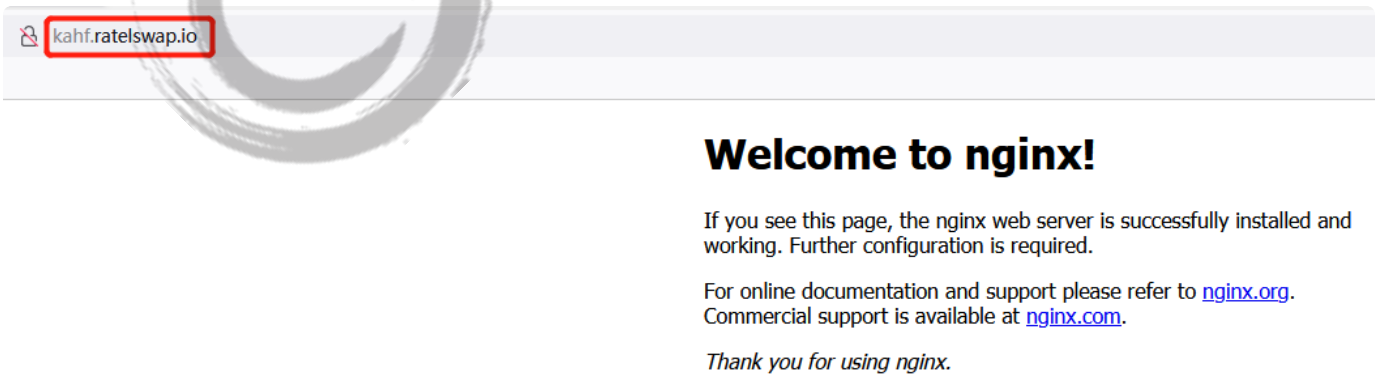
官网网站：http://kahf.ratelswap.io/

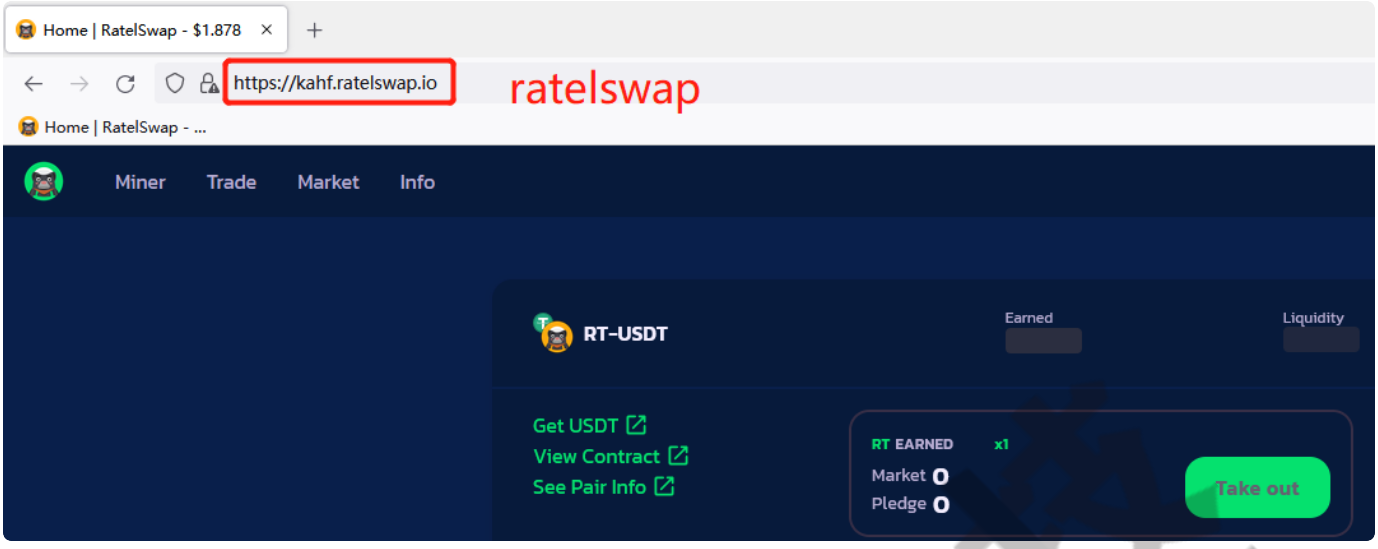
钓鱼网站：http://kahf.ratelswap.io/

以上两网站地址中，无法判断钓鱼网站。

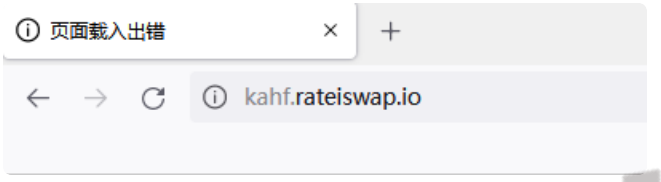
通过简单方式进行分辨：浏览器访问查看

官网网站：访问后浏览器显示正常http://kahf.ratelswap.io/网址（正在维护）





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。

0x3 钓鱼APP分析

钓鱼APP名称：KAHF Test

APP运行后会有两个逻辑功能：

1.创建新钱包（该功能无法使用）

2.导入已有钱包（可导入助记词）

尝试输入助记词后该页面会刷新，如无意外，这一步正是攻击者获取用户私钥的操作。

抓取提交私钥的数据：

```
GET /1.js HTTP/1.1
Host: kahf.rateiswap.io
User-Agent: Mozilla/5.0 (Linux; Android 9; Pixel 3 Build/PQ3A.190605.003; wv)
AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/102.0.5005.78 Mobile
Safari/537.36 Html5Plus/1.0 (Immersed/24.0)
Accept: */*
X-Requested-With: plus.H5BF97A0E
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en-GB;q=0.8,en-US;q=0.7,en;q=0.6
Connection: close
```

可以看到攻击者已将网站关闭，已不能与服务器通信，存在逻辑的js文件已无法访问。

0x4 总结与建议

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**