近日，马斯克的一条动态又引起了币圈的震动，暴跌的风暴卷席而来。而他也遭到了国际黑客组织“匿名者”的公开威胁。2021注定是币圈不一样的一年，政府加强力度的监控、各大佬的吹捧与唱衰……无不给币圈带来了许多不稳定的因素。在这种否定与肯定的声音中，散户和大庄们的博弈却一直在进行，从未停止。

5月份，中国互联网金融协会、中国银行业协会、中国支付清算协会联合发布公告，重申了虚拟货币兑换和交易的定义。

同日，内蒙古自治区发展和改革委员会发布通知宣布设立虚拟货币“挖矿”企业举报平台。尽管政策逐渐变的严明，一些平台也暂停了开通中国大陆新用户合约、杠杆等服务 。但依然阻挡不了一些人入场的脚步。若赢，则暴富，若输，则归零，是很多玩家的信仰。

"一切的罪恶都源于人的欲望"。币圈血雨腥风的背后，衍生了各种敛财模式。关于它，黑灰经过去没少提过。

在这种币币交易的环境下，USDT优势在于能保障投资者在币圈的资产不随市场涨跌缩水，但也因为这个优势衍生出了另一种敛财方式。

6月2号收集到一个名为USDTPaxx(该平台还在运营，后面用xx代替字母)虚拟币充值提现平台的IP，便对它发起了攻ji。扫描它发现存在phpmyadmin，使用弱口令对数据库连接进行检测，被禁止远程数据库。在远程操作的过程中发现有几个端口是开放着的。上传了ntunnel_mysql.php脚本，发现可getshell。由于该日志处于关闭状态，执行sql开启并修改了权限。往日志中挂了马，

使用菜刀连接了日志中的mu马文件，并利用mimikatz进行读取管理员组登录密码，远程登录服务器的大门很快就被打开。