一，王天佑的几点补充陈述：

1，黑客盗币事件的性质是：网络盗窃，金融犯罪。

金融犯罪是手段，网络盗窃是目的。

2，受害人王天佑没有超出既定的规则和功能。

Fast API授权是机器人提供的功能，受害人王天佑没有超出机器人提供的功能。

API第三方授权是交易所提供的功能，受害人王天佑没有超出交易所提供的功能。

3，受害人王天佑没有超出他的能力圈做事。

合约交易，王天佑不懂，所以受害人王天佑不做合约交易。

至于信息安全和软件工程，王天佑也不懂，所以王天佑外包给经纪商（机器人）和托管方（交易所）了。

4，王天佑授权了API，但是王天佑没授权非法的交易和划转行为。

5，亏损是金融风险，盗币是安全风险，这是两个性质。

作为投资者和做市商，王天佑只负责承担金融风险，至于安全风险，是经纪商AntBot和托管方BInance应该承担的责任。

王天佑的工作是投资组合管理，以及作为做市商的流动性提供。所以，王天佑可以承担金融风险，但王天佑不应该负责和承担安全风险。

王天佑只懂投资组合，和做市策略。至于软件工程，编码实现，信息安全，网络安全和密码学，不是王天佑的专业范围，所以王天佑外包给专业人士了。既然王天佑已经外包出去了，王天佑就不应该负责和承担这个安全风险了。

二，Binance的对称加密使用的加密算法是——HMAC

币安客服的回应

关于HMAC

这个是在API上的请求签名（Signature）签名的生成是以密钥（secret key）和请求参数进行生成的。

关于这个签名的生成，可以查看这个文档链接。

https://binance-docs.github.io/apidocs/spot/cn/#signed-trade-user_data-and-margin-endpoint-security

关于 Fast API

这个是给予第三方平台提供的一个功能。这个是用户同意以币安登录第三方平台并在第三方平台上自动生成的API并进行绑定（以应有的权限设置）。可以查看以下链接。

https://www.binancezh.jp/zh-CN/support/faq/%E5%A6%82%E4%BD%95%E5%B0%8D%E6%8E%A5fast-api-6aa7e2253c544d91b60746bfd03fd75d

三，AntBot的非对称加密使用的加密算法是——RSA

查书《应用密码学：协议，算法与C源程序》知道，对RSA算法，有选择密文攻击，公共模数攻击，低加密指数攻击，低解密指数攻击等攻击方式。

在使用RSA的时候，e不能特别小，d也不能特别小。现在建议e至少大于65537，d至少大于n^{1/4}

与RSA算法本身的实际缺陷相比，更多的是操作员错误问题。

使用低级的随机数生成器（RNG）的结果是，它们生成的随机数是很差的质数会导致生成私钥，而私钥更容易受到破坏。

最后总结一下，KeyFactor研究表明：

RSA是安全的，但是在很多情况下，IoT制造商都在错误地使用RSA；

由于分解式攻击，每172个RSA密钥中有超过1个有遭受危害的风险；

ECC是RSA的更安全替代方案；

ECC密钥比RSA小，但更安全，因为它们不依赖RNG；

ECC由于其较低的计算开销而可以很好地扩展；

ECC对量子计算的抵抗力更大；

相关企业和物联网设备制造商都需要在安全性方法上提高加密敏捷性。

由上信息，可推出，此次事件可能的攻击原因：

1，AntBot 使用了低级的随机数生成器（RNG），造成 RSA 加密算法被破解。

2，AntBot 没有使用可信任的 RSA 开源库，造成 RSA 加密算法被破解。

3，AntBot 自行开发 RSA 加密算法，导致其有漏洞，造成 RSA 加密算法被破解。

4，AntBot 的 RSA 参数设置（e不能特别小，d也不能特别小）不符合安全标准，造成 RSA 加密算法被破解。

5，AntBot 的 RSA 密钥长度太短，不符合安全标准，造成 RSA 加密算法被破解。

6，AntBot 没有及时将落后的 RSA 加密算法更新换代为 ECC 加密算法。