从Certik-Kraken争议看行业痛点：去中心化安全解决方案何时来？

撰文：Haotian

其实，在明晰的法律责任定性出来之前，对「白帽」的职业操守和中心化交易所的漏洞披露机制以及漏洞悬赏机制的质疑，会有不同角度的声音。但，在安全圈这个问题一点都不「新鲜」：

1）一个规范的漏洞披露机制其实是安全公司乙方和客户甲方就发现漏洞、漏洞修复、漏洞赏金等问题进行协调的过程，之后才是大家看到的漏洞修复后再披露的皆大欢喜，Certik 和 Kraken 很显然是协调过程出现了问题：

1、发现漏洞并及时向客户报告，描述漏洞的类型以及危害程度及如何复现；若「白帽」发现漏洞不披露，则直接就成了黑客性质，而既然选择了向客户披露，那说明主观意愿并非攻击；

2、确认漏洞并评估风险，安全公司和客户确认漏洞的存在，以及漏洞严重程度、影响范围以及修复方案设计等；这个过程会商定漏洞修复如何分工协作，漏洞赏金如何制定等，不然很容易出现，客户以漏洞为「已报告」漏洞为由，而拒付相应的漏洞赏金，可能会让白帽白忙活一场。

3、制定修复方案并复测确保漏洞成功修复；这个过程一般为客户开发团队和安全公司技术人员共同商定并统一实施代码修复，一般能推进到这一步说明双方已经就「漏洞危害等级和应付的漏洞赏金」达成一致，因此双方的一致目标就是及时修复漏洞，之后再发个新闻稿公示并披露漏洞，公开整个发现漏洞并联合修复的过程。

2）Certik 这家安全公司究竟是有口皆碑还是有口皆谤，仅仅从道德上口诛笔伐很难有结果，在此不做评价。只一点，若安全公司常招惹是非，一定是牵扯的利益关系太过复杂且处理不得当招致的。

我和几个安全公司的朋友沟通了下，认为这事情的过程可能是：

1、Certik 确实发现并向 Kraken 报告了漏洞，说明起心动念并非「黑客」行为，但发酵至今已经成为安全行业的一大丑闻，其背后的前因后果需要厘清楚；

2、标记为 Certik 工作人员 KYC 的账户只新增了 4 美元，说明漏洞测试一开始在合理界限内，之后无论何由都以双方的证据为准，但目前看，的确超出了职业操守边界；

3、双方在漏洞赏金和修复漏洞分工协作上估计没谈拢，有可能 Kraken 交易所以漏洞被报告理由拒绝给相应的赏金，因此 Certik 在修复期间处于「个人」报复也好，公司蓄意行为也罢，进行了更大规模「测试」；

这个过程存在多种扯皮的可能性，但本质上就是利益纠葛问题，Kraken 中心化交易所的漏洞披露低效且不透明，Certik 的安全漏洞介入程度缺乏规范和标准。

总结：以上仅为合理的推测，具体以进一步的结果披露为准，但安全白帽在提交 Bug 上所遭遇甲方中心化机构的「慢待」和中心化组织在漏洞披露和修复过程中的不透明流程问题才是双方出现「纠纷和摩擦」的关键。这才是大家应该关注的焦点问题。

这也是我之前发文赞赏@GoPlusSecurity 构建开放、无需可、用户驱动模块化安全层的根本原因，纯中心化的安全纠纷存在各种暗箱可能性。而一套去中心化的安全服务解决方案才能在整个安全防护生命周期发挥作用（尤其是人为原因造成的不可控因素），虽然这条路道阻且长，但势在必行。

过去几年，安全审计服务从一单接一单的业务合作模式，这过程中出现的背书风波，审计后 Rug 丑闻，直到今天甲方和乙方之间的对掐都是源于安全服务存在的信息不透明和审计业务本身在信息敏感利害关系上的复杂性息息相关。希望安全行业能随着问题的曝光，能进一步有更规范的标准、更优化的流程、更专业的服务。

无论如何，某些安全公司地位可以被替代，但安全守护者的神圣形象不容垮塌。与此同时，安全白帽的贡献也应受到市场的尊重。