1

标题：韩国多个加密货币交易所因魔窟加密型勒索软件攻击被盗数亿美元

来源：bing

摘要：

席维斯说，2018年，东北亚某国黑客攻击虚拟货币交易所盗窃了2.5亿美元虚拟货币，涉案资金经过上百次自动资金转账进行了洗钱，目的是避免执法部门追踪资金来源。黑客提供伪造的照片和身份证明文件，规避了交易所的交易人员身份披露规则。部分洗钱资金用于购买实施金融黑客行为的工具。

2017年12月至2019年4月，田寅寅、李家东共计实施了价值1亿美元的洗钱行为，这些资金来自于上文所述的黑客。田寅寅、李家东为黑客提供账户，进行汇款，获取服务费。两名被告人在美方境内实施金融犯罪行为，并从未到金融犯罪执法网络进行注册。

起诉书称，黑客于2019年11月从韩国虚拟货币交易所盗窃了价值4850万美元的虚拟货币。证据显示，实施犯罪行为所使用的部分设备位于东北亚某国境内。

田寅寅、李家东在犯罪行为中，与拉扎鲁斯小组存在合作关系。该小组建立于2007年，曾经参与了实施了魔窟加密型勒索软件攻击事件，导致美方、加拿大、新西兰的约30万台计算机出现故障。从孟加拉中央银行敲诈了8000万美元。成功导致英国公共健康系统宕机，影响了成千病人就医，导致英国损失了1.12亿美元。

魔窟加密型勒索软件利用“永恒之蓝”漏洞，通过互联网对全球运行Microsoft Windows操作系统的计算机进行攻击，该软件是加密型勒索软件，也是一种蠕虫病毒。

该病毒利用AES-128和RSA算法恶意加密用户文件以勒索比特币，使用Tor软件进行通讯，为WanaCrypt0r 1.0的变种。

田寅寅、李家东使用1448694美元购买了8823张Apple iTunes预付费礼品卡、虚拟货币种类为比特币。Apple iTunes预付费礼品卡被用于掩盖资金走向。

起诉书称，2018年年中时，韩国虚拟货币交易所的一名工作人员与一位未知客户进行电子邮件通信，在此过程，该工作人员点击运行了电子邮件中的恶意软件，该软件在运行后对交易所的计算机系统实施了攻击。软件攻击导致黑客得到了远程控制权限，黑客利用远程控制权限获取了控制加密钱包的私人秘钥。黑客利用私钥从该交易所共计盗窃了10777.94个比特币（价值2.5亿美元）、218790个以太币（价值9400万美元），此外还有价值1.31亿美元的其他种类虚拟货币。

在这些犯罪行为发生的同时，联邦调查局刑事调查处对东北亚某国互联网国际出口通信情况进行了监控发现，该互联网国际出口出现了大量的信息检索行为，其中涉及的信息包括：黑客、谷歌邮件黑客、钓鱼找、如何将以太币转换为比特币、韩国虚拟货币交易所情况及该交易所首席执行官的个人情况。

这些监控信息被作为证据使用。

执法机构聘请的第三方机构调查发现，田寅寅、李家东及其共犯实施的行为，虽然经过上百次转账隐藏，但这些行为还是被记录于区块链中。虚拟货币本来就是构筑于区块链技术之上的。

黑客使用盗窃资金设立了Celas公司（网址：celasllc.com）并通过该公司提供电子邮件服务、虚拟货币交易服务，celasllc.com存在计算机病毒及Fallchill恶意软件，提醒不要从该网站下载或运行任何软件。这个网站及这款病毒软件与2016年的另一起金融机构被攻击事件有关。

黑客提供电子邮件服务的目的是，发送上千封电子邮件，引诱收件人下载运行恶意软件，使用恶意软件获取用户的个人资料。

为了显得真实可靠，黑客还为Celas公司注册并编辑了个各种社交媒体账号。黑客将自己伪装了毕业于鹿特丹大学，并自命名为瓦力·达威士，并称瓦力·达威士是Cel

as公司的工作人员。

Marin Chain公司也是黑客们创建的公司，该公司负责为该国船舶行业提供加密货币服务。

起诉书称，APT38小组成功盗窃了10亿美元。这些资金大大部分用于导弹及核研发。

经过调查，执法部门发现，犯罪嫌疑人使用了虚拟个人网络软件，但真实IP地址位于东北亚地区。

田寅寅、李家东在2018年7月至2019年4月间，使用“snowsjohn”、“khaleesi”这两个假名，对价值100812842.54美元的虚拟货币进行了转账操作，或帮助兑换为法定货币，并获取了服务费。

两名被告人在创建113个虚拟货币账号时，使用了真实世界的银行账号信息。执法部门通过调查真实银行账号，发现了两名被告人的真实身份。113个虚拟货币账号已经被检察机关扣押。

第三方商业机构参与本案调查，通过分析犯罪行为涉及的区块链，得到了虚拟货币地址用户的真实身份。调查结果被检察机关作为证据提交给了哥伦比亚特区联邦法庭。