题：盗取虚拟币6亿元！揭秘新型网络黑客犯罪

3名专业化网络技术人员组成的犯罪团伙，几乎没有留下线索，悄无声息地盗取了高达6亿元的虚拟币！

近日，西安警方破获了一起特大网络黑客盗窃虚拟货币案，随着案件办理的深入，新型网络黑客犯罪的手段和路径逐渐浮出水面。

上亿元市值虚拟货币被盗，查案似入不断变化的“迷宫”

3月30日，西安市公安局经开分局接到受害人张某报警，称其个人电脑疑似被非法入侵，大量比特币、以太坊等虚拟货币被洗劫一空，市值达上亿元。西安市公安局迅速成立专案组开展侦破工作。

然而，警方面对的是一个颇为复杂的局面：经初步调查，受害人没有进行过任何操作，犯罪嫌疑人以高超的网络黑客技术远程控制，盗取安全性较高的虚拟货币账户，几乎没有留下任何作案痕迹。

“这种新型网络技术犯罪案在全国范围内都很罕见。”西安市公安局经开分局副局长杨世英介绍。

专案组成员、西安市反诈骗中心民警卫元祥第一时间对被盗走的虚拟货币展开追踪，发现犯罪嫌疑人的技术能力十分“了得”：犯罪嫌疑人将盗取的虚拟货币分为三等份，再分别经由不同的虚拟货币交易平台反复拆分、转移，以此增加迷惑性，最终再汇集到一个账户中，准备变卖转换成人民币提现。

办案民警介绍，以比特币为例，由于其账号只是一串基于区块链生成的编码，称为“地址”，一般情况下并不能通过该地址直接追溯到个人。虚拟账户的匿名性特征，大大增加了办案难度。

“打个形象的比喻，由于服务器都在国外，且数据链随时在变化，我们面对的是一个不断变化的迷宫。想要破案，必须守住‘变现’这个唯一的‘出口’。”西安市公安局经开分局凤城路派出所民警左桐说。

为攻破“迷宫”，专案组派出多路干警奔赴国内多个省市。在一些知名互联网公司协助下，历经3个月、摸排3万余条线索信息后，犯罪嫌疑人周某浮出水面。随后，专案组围绕周某开展调查工作，最终锁定了分别在北京、长春活动的两名同伙崔某

和张某。8月15日，在湖南、吉林、北京警方配合下，专案组3个抓捕组同时展开行动，将3名犯罪嫌疑人抓获。

据了解，这个团伙窃取了多个账户，总案值保守估计达6亿元。

警方披露破案细节：黑客高智商犯罪特征明显

经调查，3名犯罪嫌疑人均为高级黑客，都曾在国内一些知名互联网科技公司工作。他们普遍具有高超的互联网技术，且反侦查能力极强。

匿名性是各类虚拟货币最显著的特性之一，较好地保护了交易者的隐私，但也在一定程度上为非法交易提供了掩护。本案中，被盗取的虚拟财产全部在服务器设在国外的交易平台上进行转手和交易，更增添了办案的难度。

“3名犯罪嫌疑人堪称‘专家’。我们是一边办案、一边学习，他们用一个星期去转手和交易，我们往往需要花费更长时间才能理清其中的脉络。”卫元祥说，在不同的交易平台，不同币种虚拟货币的转移和支付规则不相同，警方在向国外公司征询、调取相关数据之前，必须搞清楚相应规则，只有说内行话才能顺利得到对方配合。

西安市公安局经开分局凤城路派出所民警杨龙说，本案犯罪嫌疑人反侦查能力很强。3人绝大多数时间都分处三地活动，用服务器设在国外的社交软件和网络电话联络，如有人回复信息稍晚，另外2人便有所警觉。

即使在线下，犯罪嫌疑人也具备极高的警惕性。嫌疑人之一周某生活在湖南一个小县城，尽管犯罪所得数额巨大，他却没有任何奢侈性消费，日常穿着与普通年轻人无异。一次，周某在网吧打游戏时，看到一旁有便衣警察抓人，便迅速离开。直到数小时后搞清楚抓捕与自己无关才返回家中，并通知两名同伙“警报解除”。

尽管在抓捕前半个多月就已经锁定了周某，但警方并没有立即实施抓捕。“我们要确定他作案的电脑和他本人是不是在同一个地方。”左桐说，如果抓捕时机不成熟、研判信息不准确，嫌疑人就可能迅速毁掉所有交易资料，或拒不交出相关账户密钥。一旦如此，所有努力便前功尽弃。

黑客犯罪并非无法防御，“物理储存”信息是关键

一位计算机技术专家告诉记者，在“互联网＋”时代，一些互联网、物联网终端的安全问题逐渐暴露出来。联网的打印机、智能家电、手机甚至运动手环等，都可能成为被黑客利用的“后门”，借以窃取个人隐私和商业资料。

办案民警表示，尽管黑客技术水平高超，但并非无法防御。比如，在管理虚拟货币钱包地址和密钥时，采取“冷钱包”或是物理储存的方式，将虚拟货币的相关信息写在记事本上、记录在不连接互联网的电脑或相关设备上，就能有效切断黑客的“黑手”。

西安市公安局刑侦局三处副处长林檀建议，在处理虚拟财产的电脑或手机上不要乱点来历不明的链接、下载来历不明的软件，对相关查杀“木马”病毒的软件经常更新和升级。此外，在支付和转移虚拟货币时，尽量设置“多签密钥”，即由几个人或是几个处在不同网络的终端共同授权签署密码。“这样一来，就能极大增加黑客进行网络犯罪的成本和难度，最大限度保障自身权益不受侵害。”林檀说。

业内人士建议，在处理虚拟财产时除物理储存密钥或采用“多签密钥”之外，还应强化对身边物联网设备的安全排查及日常监控。特别是要重点排查相关设备是否存在漏洞、过往是否曾被攻击等相关情况。同时要关闭不必要的远程服务端口和相关软硬件权限，定期自评自估网络安全风险，提高防护水平。

来源： 新华社“新华视点”记者姚友明、陈晨