

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。



漫画绘制 朱慧卿

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码。一旦如此，所有努力便前功尽弃。

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。

据新华社

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

优秀的红军政治工作者——王平章

在湖北省汉川市平章小学门口，竖着一座铜像，一位军人身着戎装，目光坚定地望向前方。他就是曾任红25军、红28军政治委员的王平章。

王平章，1901年生，湖北汉川人。1920年考入武昌省立第一师范学校，开始接触马列主义。后参加陈潭秋创办的进步团体“湖北人民通讯社”，并在党领导的“启明工读学校”和“汉江印刷社”从事印刷革命书刊的工作。

1924年，王平章加入中国社会主义青年团，同年转入中国共产党。后回家乡创办济人、全人小学和《汉川青年》杂志，宣传革命思想，发动爱国反帝斗争，建立中共基层党组织和农民协会。1927年3月被选为湖北省农民协会执行委员。

大革命失败后，王平章参加南昌起义。起义部队南下后，他奉命重返湖北，任中共鄂中特委书记兼汉川、天门、京山、应县四县暴动总指挥，领导恢复发展各级党组织和农民武装，发动鄂中地区秋收暴动。

1929年11月起，王平章任中共鄂豫边特委常委、鄂豫皖中央分局常委、鄂豫皖省苏维埃政府人民委员会委员长、中国工农红军第25军政治委员，参加领导鄂豫皖苏区的建设和历次反“围剿”斗争。

1932年10月红四方面军主力转移后，王平章任中共鄂豫皖省委委员兼皖西北特委书记，参与领导重建红25军，任政治委员。在国民党军实行重兵“清剿”的严重情况下，领导军民继续坚持鄂豫皖边区的斗争。

1933年1月，王平章参与组建红28军，任政治委员。曾和军长廖荣坤指挥双河山等战斗。在艰难困苦的形势下，王平章十分重视发挥政治工作的威力。他和红25军秘书长程坦合作写了一首《红军三大任务歌》，在红军和边区群众中广泛传唱。歌中唱道：“红军三大任务：打倒帝国主义，



铲除封建势力，实行土地革命。要建立起工农政权，坚决斗争，革命到底……”

1933年3月中旬，红28军奉命向鄂东北转移，与那里的红25军会合，以集中兵力与敌作战。28日，部队进至河南商城门坎山（今属安徽金寨）时，与敌一个旅遭遇。激战中，王平章壮烈牺牲，时年32岁。

为纪念王平章烈士，湖北省人民政府于1952年将他创办的汉川“全人小学”改名为“平章小学”，汉川市人民政府于1996年在学校内设立王平章纪念馆。2005年，纪念馆被评为孝感市青少年思想道德教育示范基地，2014年入选孝感市中共党史教育基地。

汉川市党史办原主任余波说：“王平章烈士是一位典型的中国传统知识分子。他心系祖国与人民，积极寻找救国救民的道路，并为此奉献了一生。”

据新华社

为了民族复兴 英雄烈士谱

连云港“12·9”重大爆炸事故调查结果公布

新华社电 记者22日从应急管理厅了解到，国务院安全生产委员会办公室近日挂牌督办的江苏连云港聚鑫生物科技有限公司“12·9”重大爆炸事故，其调查报告经国务院安委办审核同意，由江苏省人民政府批复并公布。

调查认定，连云港聚鑫生物科技有限公司“12·9”重大爆炸事故是一起生产安全责任事故。依据《安全生产法》《生产安全事故报告和调查处理条例》等法律、法规，事故企业聚鑫公司受到500万元罚款、吊销安全生产许可证的行政处罚，45名相关责任人将分别被追究刑责、受到党纪和行政处分、给予行政处罚。

2017年12月9日2时9分，连云港聚鑫生物科技有限公司二氯苯装置发生爆炸，造成10人死亡、1人轻伤，直接经济损失4875万元。

据调查，聚鑫公司未落实安全生产主体责任，是事故发生的主要原因。事故发生还存在三方面原因：一是设计、监理、评价、设备安装等技术服务单位违法违规进行设计、安全评价、设备安装、竣工验收；二是灌南县委县政府和化工园区管委会对安

全生产工作重视不够；三是负有安全生产监管和建设项目管理的有关部门未认真履行职责。

目前，聚鑫公司总经理王小富等9名相关责任人已被司法机关采取措施。同时调查报告建议，对涉嫌重大责任事故罪的原聚鑫公司安全总监王汝仁等4人，司法机关追究其刑事责任；对灌南县人民政府党组成员、化工园区管委会主任吴爱军等29人给予党纪和行政处分；对江苏智诚工程设计有限公司法人代表刘亚兵等3人给予行政处罚。

调查报告责成连云港市安全生产监督管理局对聚鑫公司给予500万元的经济处罚，依法吊销聚鑫公司安全生产许可证。

针对这起事故暴露出的突出问题，调查报告提出了进一步强化安全生产红线意识、严格落实部门监管职责和行政许可审批手续、进一步加大中介机构监管力度、全面管控危险化学品安全风险、切实加强环保尾气系统改建项目的安全风险评估等5项事故防范措施建议，要求进一步加强危险化学品安全生产工作，有效防范类似事故重复发生。