

AI或成黑客新武器

1.1亿美元比特币失窃

近日,加拿大硬件钱包厂商 Coinkite 旗下的 Coldcard 曝出存在随机数生成缺陷漏洞,导致大量离线“冷钱包”生成的助记词可被系统性推算,从而使得价值超过1.1亿美元的比特币被盗。

多位受访行业专家认为,随着人工智能(AI)挖掘漏洞的能力大幅提升,比特币乃至整个加密货币行业的安全攻防对抗升级,行业的安全防御体系面临更为严峻的挑战。

加密资产被盗风险上升

老牌比特币硬件钱包 Coldcard 爆发安全危机。近日,知名加拿大硬件钱包厂商 Coinkite 旗下的 Coldcard 设备曝出固件漏洞,该设备在 2021 年至 2026 年发布的多个固件版本代码编译配置失误,导致硬件真随机数发生器被静默禁用,改用可预测的软件伪随机数生成助记词。

这使得攻击者无需物理接触设备,可以在普通计算设备上批量枚举候选种子(用于生成伪随机数序列的初始数值),再利用公开区块链上的地址和余额验证猜测。一旦找到匹配的种子,就能在自己的电脑上生成私钥并签署转账。数据显示,截至8月3日,攻击者已从约5000个受影响钱包中转走超过1755枚比特币,按当时市值计算约合1.1亿美元。部分后续统计显示损失可能扩大至1.3亿美元。设备制造商 Coinkite 已确认该漏洞,并发布修复固件,呼吁用户及时更新。

中国通信工业协会区块链专委会共同主席于佳宁表示,从技术层面观察,此次事件问题出在随机数生成环节的工程失误。Coldcard 在 2021 年 3 月发布的 4.0.0 版固件中出现配置错误,设备本应调用的 STM32 硬件随机数发生器被绕开,密钥生成退化为依赖可预测的软件伪随机算法,有效熵值在部分型号上坍塌至约 40 比特,这意味着攻击者可以在可承受的算力成本内通过穷举法重建私钥。

全球最大的 Web3 安全公司 CertiK 统计显示,2026 年上半年,全球共发生 344 起链上安全事件,损失约 13.16 亿美元,扣除被冻结和追回的资金后,净损失约 12 亿美元。其中,钱包被攻破是损失最高的攻击类别,共发生 33 起,造成约 4.45 亿美元损失;代码漏洞虽然单笔损失相对分散,但事件数量达到 204 起,是发生频率最高的攻击类型。

CertiK 区块链安全专家董文钊告诉

记者:“我们近期在另一款硬件钱包中发现并协助修复一项与外部通信处理有关的漏洞。它与 Coldcard 的随机数漏洞并不相同,但说明了同一个原则:即使私钥始终留在设备内,设备仍需要安全地处理来自外部的软件、指令和数据;任何一处实现或验证失误,都可能成为影响资产安全的入口。”

加密货币钱包 BitgetWallet 首席运营官 Alvin Kan 分析指出,Coldcard 此前被认为安全,主要是因为其采用离线签名、隔离网络等设计,可以降低远程入侵和私钥外泄的风险。但“离线”只能防范特定攻击路径,并不能保证设备内部运行的所有代码都没有缺陷。如果私钥在生成时就缺乏足够的随机性,那么之后再强的隔离、加密和安全芯片都无法弥补这个问题。这次事件说明硬件钱包不是一个购买后即可自动获得绝对安全的“黑盒”,其安全性取决于完整链条,包括随机数生成、固件代码、硬件供应链、备份方式、恢复流程以及用户操作。任何一个关键环节出现问题,都可能削弱整体安全性。

行业安全防御面临挑战

如果计入此次 Coldcard 事件,年内针对比特币持有者的重大盗窃呈现明显的高发态势。于佳宁表示,Coldcard 的这一漏洞在开源代码中潜伏了五年之久而未被社区审计发现,说明硬件钱包的安全性从来都取决于芯片、固件、供应链与审计机制构成的完整工程链条,任何单一环节的疏漏都足以令“冷存储”(通过离线设备生成并保存数字资产私钥的存储技术)这一安全承诺失效。所谓最安全的存储方式,安全边界始终是有条件的,而市场往往低估了这种条件的脆弱性。

Alvin Kan 认为,比特币及加密资产被盗风险上升,主要有以下几个原因:一是攻击方式正在从大范围、低成功率

的钓鱼,转向更少但金额更高的定向攻击;二是大量长期持币用户的安全设置可能多年未更新,一旦历史漏洞被攻击者系统性利用,就可能在短时间内出现多轮集中清扫;三是比特币交易不可逆,攻击者一旦获得私钥并完成链上转账,原持有人通常无法单方面撤销交易。这使得私钥、助记词和签名权限成为高价值攻击目标。

董文钊表示,AI可加快反编译、旧代码检索、漏洞复现,虽然没有确凿证据证明 Coldcard 攻击者一定使用了 AI 发现这个 2021 年的漏洞,但今年非开源代码/旧代码衍生的攻击确实很多。用户需要从“相信一台设备”升级为建立多层防护体系,确保任何单点失效都无法直接导致资产转移;机构需要加强硬件端的测试、随机数调用验证、编译失败保护、外部审计等措施,以及从密钥生成到权限控制的全面安全建设。

成都链安创始人杨霞分析指出,今年以来,加密资产行业安全事件频发主要有两方面原因:一是攻击面外延,与加密货币相关的安全风险从原来的智能合约安全风险拓展至软硬件供应链、公司

内部运营治理、用户授权链路等多个方面;二是 AI 大模型能力的增强大幅降低社会工程学钓鱼攻击门槛,导致针对项目方、用户的攻击愈加专业化、自动化、规模化。底层硬件、代码迭代、运维审计、用户习惯等环节的每一个微小漏洞,都可能成为黑客攻击的突破口,应加强对多签钱包(需要多个密钥共同授权交易)签名、云端密钥存储、开发者设备与运维系统安全的监测,建立全链路、全周期的体系化防御。

于佳宁指出,数字资产的安全防御体系与其所承载的资产规模之间存在明显的不匹配。安全问题本质上是一个基础设施问题,从个体层面看,持有人应当放弃对单一设备、单一厂商的信任依赖,采用多重签名、多设备分散、异构冗余等纵深防御安排,将单点失效的损失控制在可承受范围之内。从行业层面看,硬件钱包亟须建立类似传统金融基础设施的第三方安全认证、固件变更审计与漏洞强制披露标准,同时以 AI 对抗 AI,将自动化漏洞扫描与实时链上监测纳入常态化防御体系。

(界面 财联)



(CFP 供图)

国际金价显著跳涨

多家黄金品牌单日报价涨超55元

本报讯 受到美元走软、美国国债收益率下降以及中东局势积极进展消息影响,8月6日,国际金价出现显著跳涨,现货黄金价格重返4200美元/盎司上方,并一度突破4300美元/盎司关口,单日涨幅超过4%。

受此影响,多家黄金珠宝品牌6日公布的境内足金首饰价格较前一日均有所上调,多家黄金品牌单日报价涨超55元。(央视)

上半年我国黄金产量同比下降

消费量同比增长1.23%

据新华社电 记者8月6日从中国黄金协会了解到,今年上半年我国黄金产量152.908吨,同比下降14.62%;黄金消费量511.412吨,同比增长1.23%。

从生产端看,上半年国内原料产量152.908吨,同比下降14.62%;进口原料产量77.080吨,同比增长4.62%。

中国黄金协会表示,今年上半年,重点产金省份开展矿山安全大排查大整治与专项治理等,部分矿山停产自查,在一定程度上影响了国内黄金产量。同时,大型黄金集团境外产能稳步增长,上半年实现矿产金产量48.098吨,同比增长21.43%。

从消费端看,上半年,我国黄金消费量511.412吨,同比增长1.23%。其中,黄金首饰132.133吨,同比下降33.88%;金条及金币339.336吨,同比增长28.42%;工业及其他用金39.943吨,同比下降2.9%。

中国黄金协会表示,随着金价高位大幅波动叠加黄金税收新规落地实施,国内黄金消费结构持续分化,金条、金币成为市场热门品类。同时,高金价推高了工业企业用金成本,工业用金量随之下降。

上半年,我国黄金市场呈现成交量缩减、成交额增长的量价背离特征。上海黄金交易所全部黄金品种成交量双边3.21万吨,同比下降4.37%;成交额双边33.14万亿元,同比上升36.75%。上海期货交易所全部黄金期货期权成交量双边11.71万吨,同比下降22.46%;成交额双边93.15万亿元,同比上升4.80%。

2026年6月底,上海黄金交易所Au9999黄金收盘价为每克879.03元,较年初开盘价下降11.21%。受金价走弱等因素影响,2026年上半年,国内黄金ETF增仓量为28.677吨,较去年同期下降66.17%。截至6月底,国内黄金ETF持仓量为276.529吨。

“新”意盎然 外资机构持续看好中国经济

据新华社电 7月底召开的中共中央政治局会议指出,“我国经济呈现新动能向新、结构向优的发展态势”,同时,“要高度重视经济运行中的困难挑战”。多位外资金融机构人士表示,尽管面临不少内外风险挑战,但中国经济仍展现出稳定性、确定性以及强大韧性和活力。

“中国低成本且庞大的电力容量、持续增长的人才库以及在大数据和物理AI领域的领先布局,推动AI产业链快速发展。”野村全球宏观研究主管及全球市场研究部联席主席苏博文表示,深度求索、月之暗面等中国企业发布的开放权重模型,不仅性能突出,且词元调用成本低,有助于扩大AI在更多领域的应用范围。

摩根士丹利中国首席经济学家邢自强表示,中国在先进制造领域的竞争优势同样突出——新能源汽车全球渗透率超六成,新型储能总装机约占全球份额50%,创新药对外技术授权交易额快速提升等,构成了外资对中国硬科技领域及制造业龙头企业的长期投资逻辑。

当前中国经济运行也面临一些困难挑战,中共中央政治局会议在部署下半年经济工作时强调,“宏观政策要发力提效”“加大逆周期调节力度,加大内需、优化供给”。

星展银行经济研究部高级经济学家周洪礼注意到,当前,供需矛盾仍较突出,居民消费及部分企业盈利依然承压。他认为,作为扩内需、稳增长的重要抓手,“六张网”规划建设短期内能有效对冲民间投资的下行压力,中长期有望显著降低全社会的物流与能源成本,优化资源配置,拉动潜在经济增速。同时,更具韧性的新型基础设施有助于加强供应链安全,降低面对外部冲击与地缘政治风险时的脆弱性。

在不少外资金融人士看来,落实好各项政策措施将是下半年中国经济持续向好的关键所在。“经济运行需要‘松刹车’与‘踩油门’配合。”瑞银证券中国首席经济学家宋宇表示,一方面,加快财政支出和债券资金使用进度、谋划出台增量政策,并推动财政金融政策更好协同,另一方面,破除制约居民消费的障碍,给企业营造更好的营商环境,将进一步稳定市场预期,提振消费者、企业和投资者信心。“随着逆周期调节加力,宏观政策落地显效,中国经济有望在下半年呈现稳中有进的运行轨迹,全年主要预期目标预计将顺利实现。”周洪礼说。

欧洲经济遭遇高温天气多重“炙烤”

今年夏季,欧洲多地持续遭受热浪、干旱和野火侵袭,一些河流水位刷新历史低值。欧洲观察人士认为,极端高温已不再是短期天气事件,水运能力下降、发电成本上升和农业产出减少相叠加,不仅推高企业经营成本和消费品价格,也给本已增长乏力的欧洲经济增加新的下行压力,极端天气正成为经济运行中越来越难以忽视的系统性风险。

物流动脉受阻

持续高温和降雨不足导致欧洲主要河流水位下降。德国联邦水路与航运管理局数据显示,5日,莱茵河咽喉要道考布河段水位打破2018年创下的历史最低纪录,预计未来几天水位将继续下降。

考布河段是判断莱茵河航运能力的“风向标”。莱茵河连接欧洲北海港口和德国西部工业区,承担德国大部分内河货运量,沿岸分布着大量化工、钢铁、炼油和能源企业,水位下降直接影响原材料运入和工业产品运出。

德国工商大会数字经济、基础设施和区域政策部负责人迪尔克·宾丁表示,如果干旱持续,化工、钢铁和“油物”等行业供应链将受到冲击,部分企业可能被迫减产。

据德国媒体报道,通过内河油船将油品从鹿特丹运往卡尔斯鲁厄的费用,已由6月底的每吨约45欧元升至每吨150至160欧元。

德国巴斯夫集团表示,如果水位继续下降,其位于路德维希港工厂的供应可能受到影响。德国钢铁制造商蒂森克虏伯已削减杜伊斯堡工厂铁水产量,并租用吃水较浅的外部船舶运送散装原材料。

作为欧洲重要航运门户,荷兰部分船闸为节约淡水资源、维持运河水位而关闭,不少企业面临原材料运不进、产品运不出的困境。奥地利和匈牙利境内多瑙河部分河段的货运能力也明显下降。

德国基尔世界经济研究所经济学家斯特凡·科茨估计,低水位可能给德国第三季度造成10亿至20亿欧元经济损失。

能源系统承压

热浪给欧洲能源系统带来双重压力:一方面,制冷设备使用增加,用电需求骤增;另一方面,水资源不足、河流水温升高限制核电、水电等运行,能源供应能力下降。

法国现有57个核反应堆,均建在沿河流或沿海地区以满足机组持续冷却需要。高温导致部分河流水温升高,流量下

降,为遵守取水和热排放规定,法国电力公司不得不降低部分核电机组功率,甚至暂停个别机组运行。

匈牙利的能源供应压力更加突出。该国保克什核电站多个机组相继停运,面临投入运行44年来首次完全关闭的风险。匈政府不得不暂停晚间用电高峰时段的大部分铁路货运。

在意大利、希腊和塞浦路斯,高温推动制冷负荷持续上升,多地用电需求接近或创下夏季同期高点,部分国家增加天然气发电或启用备用电源,电力系统运行成本和企业用能成本随之上升。

能源供应趋紧还可能冲击铁路货运、钢铁和化工等行业,并增加通胀压力。如果电力供应紧张,工业企业将面临限电、减产和成本上升风险。

农牧业受冲击

农牧业是最直接受高温冲击的行业之一。持续热浪增加作物和牲畜用水需求,推高灌溉、饲料、保险和防灾等成本。根据法国政府通报,该国部分地区的农业灌溉和牲畜饮水已出现困难。据估算,今年高温可能导致农业总产值下降10%,给法国造成最高约60亿欧元损失,

相当于该国全年国内生产总值的0.2%。

奥地利农业商会预计,今年该国谷物总产量较去年下降15%,部分地块面临绝收。全国天然草场干草产量下降近一半,超过六成奶牛已提前动用冬季储备饲料,跨地区饲草采购价格明显上涨。

意大利中小农场主协会表示,奶牛和家禽因热应激而出现产奶量、产蛋率下降,养殖成本持续增加。

东南欧部分灌溉设施相对薄弱的地区灾情更为严重。波黑部分地区青贮玉米大片枯萎,一些蔬菜遭受严重损失。

高温引发的野火进一步放大了经济损失。联合国欧洲经济委员会数据显示,今年欧洲已有超过43.4万公顷土地被野火烧毁,野火不仅摧毁森林、农田、牧场、住宅和基础设施,还导致道路封闭、游客减少,并推高消防、防灾、保险和灾后重建成本。

欧洲观察人士认为,本轮高温所暴露的已不局限于欧洲河流水位下降或某类农作物减产,而是欧洲交通、能源、水资源和产业体系对极端气候适应不足。极端天气正从偶发的外部冲击,逐渐转变为影响欧洲经济增长、物价稳定和产业竞争力的长期变量。

(新华)

全球并购交易正恢复活力

中国市场呈现鲜明结构性特征

本报讯 近日发布的一份报告显示,全球并购交易正恢复活力,而在全球并购格局重塑的同时,中国市场呈现鲜明的结构性特征。

《全球并购趋势与中国并购市场展望》报告由毕马威发布。这份报告基于对全球20个国家和地区逾700名并购交易参与者的系统调研,并结合对中国市场的洞察,系统梳理全球并购市场新特征。

报告显示,全球并购交易正在重新恢复活力,多数机构预计未来交易数量将持续上升。但增长不均衡,亚太和美洲地区的预期相对乐观,而欧洲、中东和非洲地区的信心相对偏低。

与此同时,立法和监管的波动性、不断演变的贸易制度以及全球税收框架的变革,正在重塑未来的成本结构和投资回报模式。

报告还关注到人工智能(AI)在并购

生命周期中的广泛应用。目前,AI已逐步嵌入尽职调查、建模和整合规划中,在投资组合审查与交易来源识别环节的应用已较为普遍。

报告认为,AI的优势在于扩张决策的广度和深度,可实现详细的合同审查、持续集成风险监控和历史交易模式识别,处理能力远超人力极限。

在中国本土市场,并购交易数量维持低位震荡,但单笔平均交易规模显著扩张,前十大并购交易金额占比大幅提升,战略性政策引导效应显现。行业结构上,制造与

科技业并购占比显著提升,占据市场主导地位,在半导体、新能源等领域尤为显著。

中国企业海外并购方面,交易数量从阶段性高点有所回落,平均交易金额经历调整后出现反弹,交易筛选标准大幅提高,资金向高质量标的集中。制造与科技业主导地位延续,消费品与金融为第二梯队,医疗保健行业波动较大,更多企业转向产品授权引入海外资产。

“本土市场的并购在新质生产力战略框架下,呈现战略性行业加速集整合的趋势。”毕马威中国交易咨询服务主管合

伙人林琳称。

报告进一步提出影响中国并购市场格局的核心趋势。战略与新兴行业加速并购,成为并购主战场,信息技术、高端制造、新能源、新材料、医药生物等领域成为引领经济高质量发展的核心引擎,国资国企聚焦战略性新兴产业投资整合,资本与金融市场积极支持战略性并购重组。

“当前,中国的并购市场正从规模导向迈向价值创造新阶段,并购理念从简单的买得便宜转向管出价值。”毕马威中国交易战略与并购融资主管合伙人王虹称。(中新)