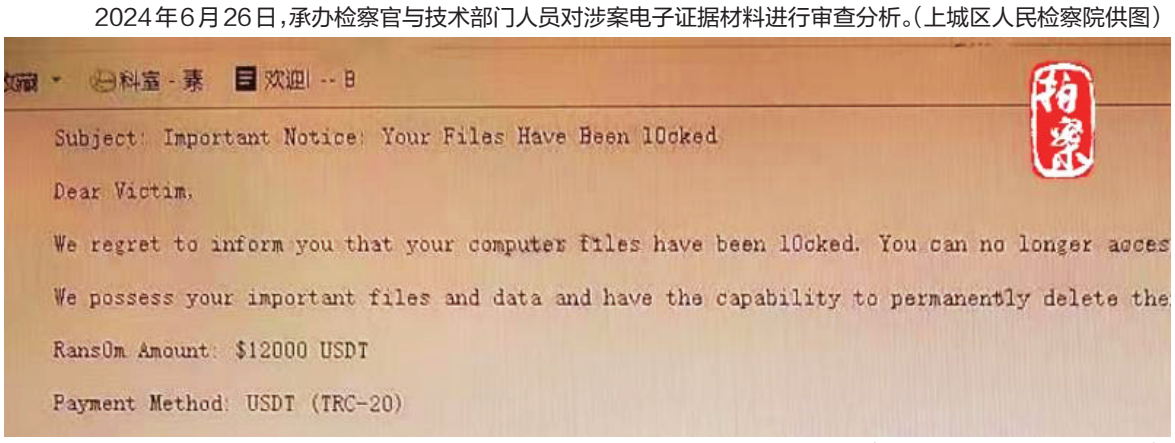
网安卫士竟“变身”木马黑客！

警惕网络敲诈勒索

原本从事网络安全工作的工程师，竟干起黑客的勾当，利用木马病毒“黑”掉企业网络系统，索要数字加密货币作“赎金”……近日，浙江杭州市上城区人民法院一审宣判了一起特殊的敲诈勒索案件，四名被告分别以犯敲诈勒索罪、侵犯公民个人信息罪被判处有期徒刑。

2024年6月26日，承办检察官与技术部门人员对涉案电子证据材料进行审查分析。（上城区人民检察院供图）



这是提示文件已经被锁定的勒索信息。（杭州市公安局上城分局供图）

“老字号”遭遇黑客攻击 “赎金”是虚拟货币

2023年底的一天，杭州一家“老字号”医疗机构技术部负责人陆续接到各个科室的来电，反映系统无法正常登录。进入操作页面发现，所有的系统文件都变成了“。uncle”的后缀。经过排查，后台管理系统中一个名为read-me。html的文件十分可疑。点开一看，里面赫然写着：“Important Notice! Your Files Have Been Locked!”（“注意！你们的文件已经被锁定！”）随后，技术人员陆续在文件中找到了“Payment Method”（支付方式）“Wallet Address”（钱包地址）等内容。这起系统瘫痪的始作俑者被确定为网络黑客。

经核实，公司共计89台服务器无法运行，包括电子病历、批发连锁在内的业务系统彻底陷入瘫痪。为尽快恢复线上挂号等业务，最大程度保障患者不延误诊疗，该医疗机构无奈答应了对方支付数字加密货币作为“解锁赎金”。

无独有偶，这家机构报案之后，杭州警方又发现两家被该团伙敲诈勒索的企业。经统计，三家被害企业为恢复正常经营，共计花费33万余元向第三方购买数字加密货币支付给了对方。

杭州市上城区公安分局网警大队民警介绍，嫌疑人在短时间内集中进行了大量技术操作，且反侦查意识很强，设立了多个“跳板”服务器，IP地址涉及境内外多处地点。从种种迹象看，该起案件大概率是组织严密、分工明确的团伙作案。

通过技术手段追踪侦查，公安机关逐步锁定了涉案人员的真实身份。2023年12月，以祁某某为首的四人犯罪团伙在内蒙古呼和浩特、北京等地被相继抓获归案。

一心赚“快钱” 网安卫士变勒索黑客

四人到案后，承认了利用木马病毒开展敲诈勒索的犯罪事实，案件真相逐渐浮出水面。

原来，祁某某、韩某某、李某某三人原是北京某科技有限公司负责网络安全维护的工程师，而郝某某是和祁某某、韩某某熟识的好友，也从事网络安防工作。

由于熟悉网络安全的“门道”，祁某某、郝某某、韩某某开始谋划利用技术赚点“快钱”。一开始他们盯上贩卖公民信息的生意：2023年4月至7月，祁某某等人通过服务器漏洞对系统数据进行非法爬取，共获取包含收货人、收货地址、电话等信息累计6万余条，通过非法贩卖，共获利人民币20余万元。

但这类数据在“黑市”上的价格逐渐走低，他们决定换一条“赛道”，用病毒搞敲诈勒索。

为了提升效率，祁某某、韩某某等人在呼和浩特市的出租房内开起“勒索工作室”。四名成员分工明确：祁某某、韩某某事先编写好勒索代码并进行测试，郝某某、李某某对有漏洞的企业服务器进行收集并添加漏洞“后门”，随后由祁某某、韩某某从“后门”进入网站，上传定时执行加密任务的木马病毒进行勒索。

承办检察官表示，这几人在从事网安工作的时候，就时常关注技术论坛中发布的服务器共性漏洞，在网上寻找可以攻破的堡垒机。“为了提升网络攻击效果，他们还利用人工智能技术辅助修改病毒程序代码。”

就这样，在短短一周不到的时间内，该团伙陆续作案三起，对被害企业造成损失。

扎好安全“篱笆” 应对网络勒索

2024年9月11日，上城区人民检察院分别以敲诈勒索罪和侵犯公民个人信息罪对祁某某等四人依法提起公诉。2025年3月，该案件在上城区人民法院开庭审理。近日，四名被告人被一审判处有期徒刑三年至七年六个月不等，并处罚金。目前该判决已生效。

“没耐心想要‘挣快钱’，这种心态害了自己。”面对法官的讯问，郝某某流下后悔的泪水。四名被告在一审宣判后，均表示服从判决结果不上诉。

承办检察官表示，近年来，人工智能技术的发展进一步降低了攻击门槛，导致针对企业服务器，尤其是网安能力薄弱的中小民营企业的黑客攻击勒索发案频率有所提升，加大了案件侦办难度。

网络安防专家建议，面对网络勒索，企业除了事发后要及时固定证据报警，平时要定期做好“冷备份”，即平均每7天对所有服务器数据做一次线下备份。一旦发生勒索攻击，至少可以将系统恢复到7天以内的数据，不至于陷入完全瘫痪；此外还可以选用“专用设备+安全保险”服务模式，部署一套防勒索检测设备的同时，加入一份安全保险，对因为黑客勒索造成的损失获得有效赔付。

魔高一尺，道高一丈。尽管人工智能技术和虚拟货币等的运用，让传统犯罪“花样翻新”，但调查取证手段在不断更新，相关法律法规也日益完善，建起愈加牢固的网络安全“篱笆”。同时，企业特别是中小企业要提高风险意识、完善安防措施，一旦遭遇网络敲诈勒索，及时固证维权。

（据新华社杭州5月19日电 记者吴帅帅）