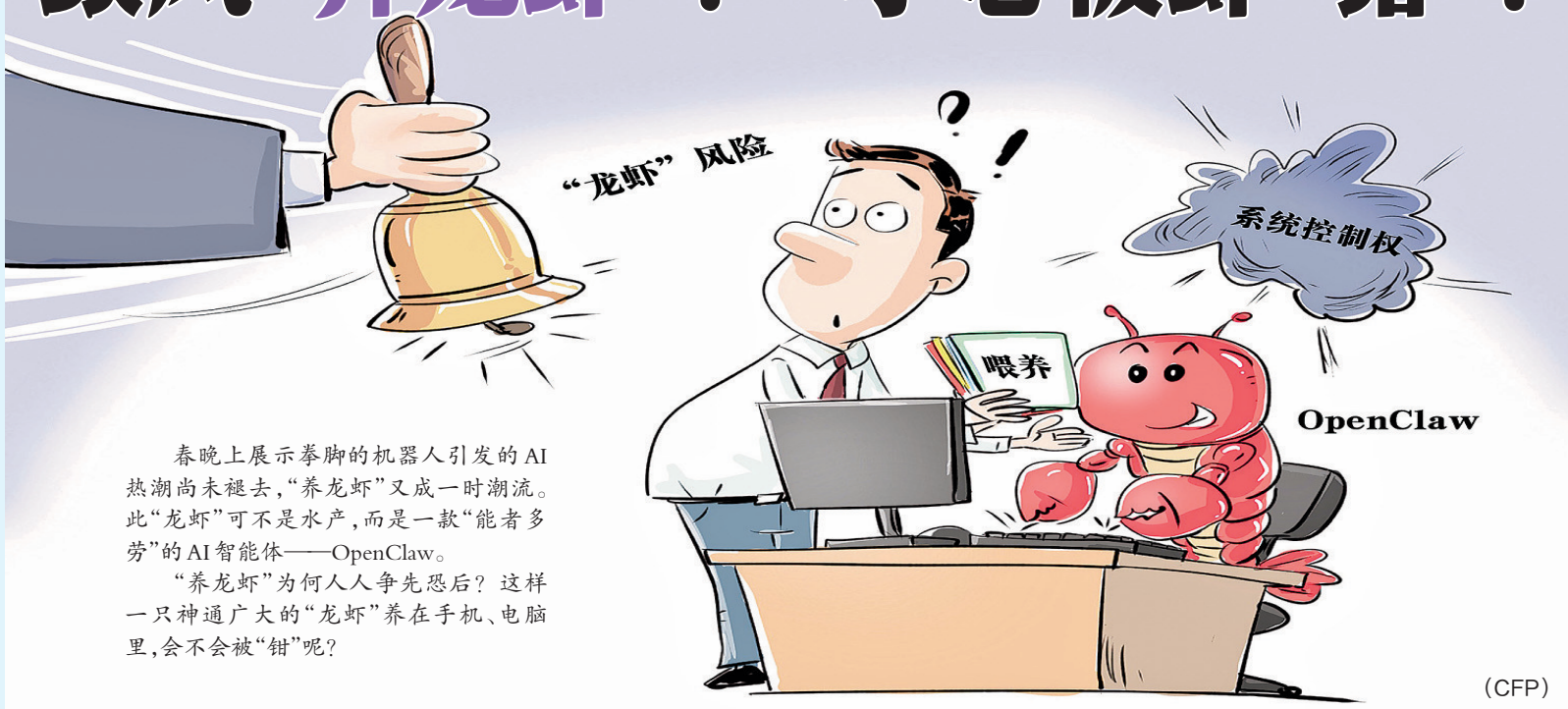
安装“能者多劳”的AI智能体——OpenClaw成为潮流

跟风“养龙虾”？ 小心被虾“钳”！



（CFP）

春晚上展示拳脚的机器人引发的AI热潮尚未褪去，“养龙虾”又成一时潮流。此“龙虾”可不是水产，而是一款“能者多劳”的AI智能体——OpenClaw。

“养龙虾”为何人人争先恐后？这样一只神通广大的“龙虾”养在手机、电脑里，会不会被“钳”呢？

今天，你“养龙虾”了吗？

OpenClaw由奥地利技术人员彼得·斯坦伯格研发，2025年11月推出原型版本，2026年1月正式确定名称。发布以来，它已成为全球用户增长最快的AI开源项目之一。OpenClaw使用红色龙虾作为标识，将其部署安装在个人终端上训练开发的行为，被网友形象地称为“养龙虾”。

奇安信安全专家汪列军表示，OpenClaw之所以广受关注，主要是因为与当前主流的生成式大模型相比，它实现了从被动应答向主动决策、自主执行的转变，具备主动执行任务的能力。举例来说，如果用户询问北京有哪些美食，普通大模型通常会搜索一番给出答案，对话就此结束。但OpenClaw不同，它甚至能帮用户点一份外卖。

这意味着，用户一旦将这款智能体部署在手机、电脑等终端，并赋予其充分权限，它就具备调用生产生活工具的能力，乃至召唤出一个“虚拟大脑”远程控制和操作个人设备。

记者在国内一家云平台上花费近100元购买了OpenClaw相关云服务器和大模型套餐，约1小时完成部署。调试后发现，它可以完成文件整理，具备持续学习和模仿等功能，记忆力强大，还可自主进行迭代优化。

眼下，哪些群体热衷于“养龙虾”？

科技自媒体、博主“打头阵”。有的宣称“不赶紧‘养龙虾’，你就Out（落伍）了”；有的更标榜OpenClaw能“自主执行、自动赚钱”，“养龙虾”可辅助炒股、“挂机躺赚”，相关代理安装与训练教学已成为生意。目前，国内不少老年人、学生也为这股潮流所裹挟。

部分国内企业、厂商闻风而动，火速开放部署通道。截至3月10日，腾讯云、阿里云、百度智能云、火山引擎等多家国内云服务商均已上线OpenClaw部署功能，宣称“零代码、5分钟快速上线”。部分平台为吸引用户，默认开放较高权限和公网端口。此外，部分券商、电商乃至中小企业也开始尝试将其应用于客服、数据处理等场景。

部分地方政府也鼓励“尝鲜”。3月7日，广东深圳龙岗区发布引导文件，就OpenClaw一类应用提供免费算力、数据要素乃至最高1000万元股权投资等支持；3月9日，无锡市高新区发布“养龙虾”12条，单项支持最高500万元。

全民“养龙虾”，安全置何处？

用上OpenClaw这样的AI智能体可以“撒手不管”吗？正如摩尔线程创始人张建中所言：“如果你是老板，雇了一名能力超强的新员工，就会直接把自己的电脑给他使用吗？”OpenClaw这位新员工，可能带来哪些风险隐患呢？

——权限太大，可能失控。安恒信息终端安全专家胡宇介绍，OpenClaw需要较高系统权限才能完成复杂任务。如果配置不当或遭恶意引导，可能绕过人为设定的安全限制。

有报道称，此前美国Meta公司相关负责人在使用OpenClaw清理邮箱时，就发现它会无视“未经许可不得操作”的安全提示，置紧急叫停于不顾，最终将工作邮件也全部清空。

——插件众多，后门须防。汪列军介绍，OpenClaw的各类插件固然有文件读写、代码执行、网络访问的“三头六臂”，但一旦遭到非法控制，用户的各类密码、加密钱包、API密钥等信息都可能泄露。

美国网络安全机构SecurityScorecard监测发现，有大量OpenClaw相关框架存在远程代码执行漏洞，攻击者可借此控制设备。这些插件还可能伪装成常用应用，窃取浏览器Cookie、SSH密钥、API密钥等敏感信息。

——信息泄露，不容小觑。汪列军表示，很多用户缺乏安全意识，直接将OpenClaw管理接口暴露在公共网络，且未修改默认账号密码或关闭不必要端口，很容易被黑客扫描并接管。

奇安信网络空间测绘平台数据显示，目前暴露在公网的OpenClaw相关实例超过20万个，弱口令、未授权访问一类漏洞大量存在，极易成为攻击目标。如果“龙虾”部署在存储身份证照片、财务数据乃至工作机密的设备上，一旦被入侵，相关数据极易大规模泄露。

“虚火”应退，监管要跟上

那么，想“养龙虾”到底该注意什么？专家建议，使用中应遵循“物理隔离”和“最小权限”原则。

首先，不在日常办公电脑和存有重要资料（照片、文档、账号密码）的个人电脑上直接安装OpenClaw，力避AI失控执行删除操作或被黑客控制时造成不可逆损失。为求稳妥，可使用闲置电脑部署，或专门为其组装一台未存储重要数据的电脑。有条件者可选择更安全的云服务器虚拟机。

其次，选择安全可信的技能包Skills下载来源。专家建议，从通过安全检测的官方可信来源下载，避免下载可能被“投毒”的Skills，并在本地电脑上加强权限控制，严格限制AI只能访问特定的非敏感文件夹。

3月10日，国家互联网应急中心发布风险提示，建议相关单位和个人用户在部署和应用中，要强化网络控制，不将OpenClaw默认管理端口直接暴露于公网，并通过身份认证、访问控制等安全控制措施，对访问服务作出安全管理。

OpenClaw在架构设计、默认配置、漏洞管理、插件生态、行为管控等方面存在较大安全风险，一旦被攻击者利用，可能导致服务器被控制、敏感数据泄露等严重安全问题。

3月13日，国家网络安全通报中心发布《OpenClaw安全风险预警》：国家网络与信息安全信息通报中心监测数据显示，目前全球活跃的OpenClaw互联网资产已超20万个，其中境内活跃的OpenClaw互联网资产约2.3万个，呈现爆发式增长态势，主要集中在北京、上海、广东、浙江、四川、江苏等互联网资源密集区域。大量暴露于互联网的OpenClaw资产存在重大安全风险，极易成为网络攻击的重点目标。

此外，专家指出，个人使用办公网络、单位电脑进行部署需慎之又慎，警惕数据安全风险。而部分政府部门、国有企业盲目跟风，仓促开展试点、设备采购甚至出台补贴政策等，更不可取。

针对“养龙虾”滋生的虚假宣传、违规培训、远程操控、信息窃取，以及平台不充分告知相关使用风险和信息共享权限范围等行为，相关部门要尽快制定并出台约束性规范，为行业“虚火”降温，为企业和公众安全防护“织网”。 （半月谈 郭宇靖 张骁）