2026年3月10日 星期二 齐鲁晚报

最近，“养龙虾”突然火了。不过，这只“龙虾”并非餐桌上的海鲜，而是一款名为OpenClaw的开源AI智能体。OpenClaw是奥地利程序员彼得·斯坦伯格开发的个人AI智能体，于2026年1月最终选定名字并开源。3月6日，在深圳腾讯大厦楼下，不少市民带着电脑赶到现场，排队参加OpenClaw（“龙虾”）AI智能体工具的免费安装活动，场面十分热闹。近期，工业和信息化部网络安全威胁和漏洞信息共享平台监测发现OpenClaw开源AI智能体部分实例在默认或不当配置情况下存在较高安全风险，极易引发网络攻击、信息泄露等安全问题。爆火的“龙虾”，跟以往的AI工具有何区别？能为我们带来哪些全新的体验？又可能带来哪些安全隐患？

『养龙虾』火了，是AI普惠还是安全惊雷？

『鸡排哥』式工作难题有解了 『养虾』门槛高普通人还需提高『厨艺』


3月6日，腾讯大厦门口排队“养虾”的人。 图源网络

“养龙虾”成AI圈新宠

所谓“养龙虾”并不是什么生鲜养殖指南，而是从开源智能体项目OpenClaw兴起的AI圈热词。该项目的Logo是一只红色卡通龙虾，因此部署并运营于OpenClaw被大家戏称为“养龙虾”，也就是安装一个属于个人的AI Agent。

这个由奥地利退休程序员彼得·斯坦伯格(Peter Steinberger)主导开发的开源项目，从一个周末副业项目，快速成长为GitHub历史上增速最快的开源项目之一，发布仅四个多月就登顶星标榜，被视为AI Agent实用化的里程碑事件。

与ChatGPT等停留在对话框里提供“建议”的产品不同，OpenClaw可以7×24小时自动执行任务——读取文件、搜索信息、编写代码、发送邮件等。很多程序员将其当作一个能动手干活的数字员工，人手一只“龙虾”。

随着OpenClaw快速走红，市场已迅速催生出专业化代装服务，其中上门安装收费普遍为500元/次，远程安装价格在50至300元区间。在咸鱼上搜索“OpenClaw部署”，平台行情显示近7日成交均价为37.38元；淘宝上，50元的远程部署服务链接，已有600+人下单付款。

3月6日，深圳腾讯大厦门口出现排队热潮。近千名开发者与AI爱好者来到腾讯大厦，在腾讯云工程师的协助下，免费完成了OpenClaw的云端安装，集体化身“云上养虾人”。

事实上，不少大厂都在密集推进自己的“龙虾”。MiniMax推出MaxClaw，Kimi推出Kimi Claw。小米开始内测MiclawAgent，希望把AI代理嵌入小米“人车家全生态”的系统里，让手机、汽车、电视和家电都成为AI的执行节点。雷军亲自下场点评，留下四个字：“手机龙虾”。阿里开源的桌面Agent工具CoPaw主打一键在本地和云端部署，并支持基于CoPaw进行二次开发。百度智能云推出移动版OpenClaw，无需部署、云端环境隔离更安全，Token消耗限时免费。

打破“鸡排哥”式工作难题

去年爆火的景德镇“鸡排哥”，很多人可能还有印象。视频中，“鸡排哥”一边忙着炸鸡排，一边连声招呼顾客：“先做你的，再做你的，然后做你的。”节奏紧凑又充满喜感。

在OpenClaw出现之前，“鸡排哥”式的工作难题，其实也是许多AI工具共同面临的痛点。不同任务往往需要依赖不同的AI工具，就像鸡排因人口味不同而需要不同调味一样：有的AI擅长处理文案，有的负责制作视频和图片，有的用于回复邮件，还有的可以帮助修改和调试代码。

“如果它们能互相认识，听我的统一指挥就好了。”——这正是OpenClaw试图解决的问题。

对外经济贸易大学国家对外开放研究院教授陈建伟接受采访时表示，OpenClaw与此前的聊天式AI存在明显区别。

以往的聊天AI更像一个“咨询助手”，主要停留在对话层面，根据用户提问给出建议或信息；而OpenClaw则能够主动执行具体任务，例如访问本地文件、调用工具或运行相关命令，真正具备“做复杂事情”的能力。通俗来说，OpenClaw更像是一个“调度员”。它并不一定要成为最聪明的AI，而是站在中间，把各种不同能力的AI连接起来，像织网一样将它们串联在一起。

你只需要对它说一句话，比如：“帮我总结一下今天的邮件，把重要事项加入日历，顺便在团队群里通知一声。”——接下来，它就会在后台自动调用不同的工具，把这些事情一步步完成。

在陈建伟看来，OpenClaw让AI的角色从单纯的被动响应，逐渐转向能够主动完成任务的“代理者”，也推动人工智能从单一的聊天工具，向更具有实用性的执行型助手演进。

“一人公司”成为可能

那么，OpenClaw到底能做些什么呢？

春节前，猎豹移动董事长兼CEO傅盛滑雪时髋关节脱臼，只能卧床。他用1157条消息、22万字对话，从零“养”了一只AI“龙虾”，取名“三万”。春节里，“三万”帮他给611人拜年，安排未来一个月行程，还写出好几篇阅读量破万的公众号文章。养到第14天，“三万”自己长成一支8人智能体团队，7×24小时自动运转，邮件、日历、信息扫描、内容创作、社区运营，全自动化。“这不是工具，是一个系统。”傅盛感慨地说。

“养龙虾”的网友“春秋”，主要用“龙虾”解决三件事：快速理解项目、获取外部信息、投研和排错。春节前，他已经用“龙虾”跑了七八份固定报表。“这件事在运营层面等于替代了一个人。发现异常的人很贵，干活的人反倒不贵。”

技术的发展，让“一人公司”成为可能。越来越多的自由职业者、小微创业者开始利用OpenClaw+大模型等组合，以低成本实现自动化套利、全自动客服、规模化内容生产。在这个新风口下，个体的杠杆被无限放大，只要会“养龙虾”，就能拥有复制员工的资本。

“养虾”，“厨艺”得过关

想“养”这只“小龙虾”，使用者也需要具备一定的“厨艺”。

首先，很多有意向的“养虾人”，往往就卡在了安装和配置这一关。对于不少普通用户来说，从环境搭建到软件部署，再到模型和插件的配置，每一步都需要一定的技术基础，如果缺乏相关经验，很容易在最开始就被“门槛”拦住。目前，在一些网购交易平台上，已经有人围绕安装需求做起了生意，提供“OpenClaw上门安装”服务并从中获利。

就算顺利完成了安装和配置，接下来面对的各种功能和“技能”，也常常让人眼花缭乱，无从下手。不同的插件、工具和自动化流程各有用途，从文件管理、信息检索，到代码执行、日程安排，功能看起来样样齐全，但如何搭配使用、如何让它们协同完成任务，对不少新手来说仍然面临不小的问题。

陈建伟指出，目前OpenClaw在实际部署和使用过程中仍存在一定门槛。比如在安装阶段，用户往往需要搭建Docker容器、配置API密钥(应用程序编程接口身份验证凭证)，并持续关注Token(数字标识符)的消耗情况，这些技术性操作就可能让不少普通用户在最初阶段“卡壳”。在使用层面，如何编写有效的指令、调试AI代理的行为，同样具有一定难度，往往需要具备一定的编程基础。

不过他预计，随着开源社区不断推出简化工具和一键安装包，这类技术障碍有望逐步降低，从而推动AI智能体被更广泛地应用。未来可能出现大量基于OpenClaw开发的行业解决方案，比如自动化办公助手、内容生产助手、电商运营助手等，通过预设模板和流程，把复杂的AI能力封装成可直接使用的工具。

据新华社、中新社、上游新闻、极目新闻等

相关链接

“养龙虾”须提防信息安全问题

近日，工业和信息化部网络安全威胁和漏洞信息共享平台监测发现，OpenClaw开源AI智能体部分实例在默认或不当配置情况下存在较高安全风险，极易引发网络攻击、信息泄露等安全问题。

新华社发文提示，建议相关单位和用户在部署和应用OpenClaw时，充分核查公网暴露情况、权限配置及凭证管理情况，关闭不必要的公网访问，完善身份认证、访问控制、数据加密和安全审计等安全机制，并持续关注官方安全公告和加固建议，防范潜在的网络安全风险。

也有用户反映，“龙虾”在执行任务时可能出现误操作。比如有用户让OpenClaw检查邮箱，并提出“列出需要归档或删除的邮件”，还特意设置了常见的“安全词”作为限制，希望系统在执行前进行确认。然而，这些约束并未如预期生效。OpenClaw在理解指令后，直接开始批量删除邮件，而且在执行过程中难以及时中止操作。最终，这名用户不得不通过“物理关机”的方式强行终止程序，才让这只“龙虾”停下来。

陈建伟指出，与主要停留在对话层面的聊天AI不同，像OpenClaw这类具备代理能力的系统能够调用工具、访问文件甚至执行代码，一旦被滥用，可能带来数据泄露、恶意代码执行等安全隐患，在某些情况下更容易被不当利用。

他建议，在实际使用过程中应当注意做好信息隔离，并对AI执行的关键操作进行必要的人工检视，避免完全“放手”交给系统自动处理。

据新华社、中新社

编辑：武俊 组版：侯波