对AI模型和算力的非法访问，正迅速成为网络犯罪地下世界中最炙手可热的商品。黑客试图利用昂贵的大语言模型进行勒索、战争和间谍活动。

谷歌威胁情报集团（Google Threat Intelligence Group）首席分析师John Hultquist表示，该网络安全部门今年观察到所谓“LLM劫持”（LLM-jacking）攻击大幅增加，其中包括出售公共AI工具被盗的登录凭证，以及一些团体窃取算力资源，以便免费运行自己的模型。

这位拥有20年网络安全经验的资深人士Hultquist称：“我们在地下市场看到的是，一个围绕AI访问权限而形成的经济正在不断增长。”

Hultquist警告称，以低成本获得昂贵AI资源，会让网络攻击者在经济上获得相对于攻击目标的优势，因为后者同样需要使用这些AI工具来保护自己。

他说：“归根结底，所有这些行为都会让他们在经济上或效率上获得某种相对于我们的优势，因为他们实际上能够以便宜得多的价格获得这些token。”

谷歌威胁情报部门的研究人员发现，暗网上的一些交易市场正在出售Anthropic、Google和OpenAI等公司AI模型的访问权限，折扣最高可达97%。ChatGPT和Claude最高级版本的AI订阅服务，每名用户每月费用最高可达200美元。

Hultquist表示，鉴于AI实验室会监测此类滥用迹象，一些卖家甚至提供“保证访问”，承诺如果最初的账户被封禁，将免费提供新的登录凭证。

在其他情况下，犯罪团伙和国家支持的组织会入侵企业托管在云端的服务器，并将自己的AI模型部署到目标系统中运行。这种方式与此前威胁行为者试图入侵第三方计算机进行加密货币挖矿类似。

Hultquist表示，AI已经被“所有威胁行为者”使用，并补充称，因此AI工具未来也必须成为网络安全体系中不可或缺的一部分。在Anthropic最近一期关于AI滥用的季度报告中，该公司发现，来自包括美国、英国和也门在内20多个国家的威胁行为者曾试图利用其Claude工具从事恶意活动。

他说：“任何认为AI只是一阵风潮、想让它就这样从自己身边过去的人，终有一天醒来时会发现自己已经被淹没。他们将面临比以往任何时候都更多的安全事件、更多警报、更多攻击。我们现在就必须把自己的事情处理好。”

Hultquist警告称，随着越来越多大型企业寻求将定制化AI模型部署在自己的服务器上，而不是从云服务提供商租用算力，这些系统本身也将成为攻击目标，因此必

须受到严密保护。“如果你正在为算力付费，而算力可能非常昂贵……那么这就会成为威胁行为者眼中一项极具吸引力的潜在资源。”

Hultquist还表示，现在正是黑客“潜入”目标账户和计算机服务器的最佳时机，因为企业仍在摸索自己究竟会使用多少AI资源。

他说：“你可能会觉得，算力使用量突然大幅增加是完全正常的，因为你刚刚部署了这么多AI基础设施。这确实给了某些人一个隐藏在噪声之中的机会。”