反思您的想法，并用三百个字或更多的单词来分析和评价全球网络犯罪活动中的两种最新威胁。

全球网络犯罪活动日益猖獗，其威胁形式不断演变。当前两种最新且严重的威胁是勒索软件攻击和供应链攻击。这些威胁具有复杂性、高破坏性，并挑战传统的网络安全防御策略。

首先，勒索软件攻击是近年来最具破坏力的威胁之一。攻击者利用恶意软件加密目标系统或数据，并要求支付赎金以恢复访问。勒索软件的技术手段日趋先进，尤其是“双重勒索”模式，即除了加密数据外，攻击者还窃取敏感信息并威胁公开，以加大受害者的压力。最近，一些攻击组织甚至利用人工智能（AI）生成更复杂的恶意代码或欺骗性社会工程攻击，提升其成功率。关键基础设施如医疗系统、能源供应链和政府机构成为主要目标，这不仅导致巨额经济损失，还可能危及社会公共安全。

其次，供应链攻击的兴起对网络安全提出了新挑战。这类攻击通过侵入供应链中的第三方系统实施，例如在合法软件或硬件中植入恶意代码。SolarWinds 攻击便是一个典型案例，攻击者通过污染其软件更新渠道，成功渗透到多个政府机构和企业网络中。供应链攻击的隐蔽性和传播范围使其危害显著增加，受害者往往难以及时发现漏洞，从而为攻击者提供了长时间的访问窗口。

综上所述，勒索软件攻击和供应链攻击代表了网络犯罪活动的复杂化和隐蔽性趋势。这两种威胁的共同特点在于它们高度依赖技术创新和复杂的操作手段，这不仅使防御更加困难，也凸显出全球网络安全合作的重要性。未来，企业和政府需要加强威胁情报共享、实施更严格的供应链安全审查，并研发更智能化的安全技术来应对这些新兴威胁。