网络安全预警通报

2024 年第 4 期 （总第 47 期）

西安交通大学网络信息中心 2024 年 7 月 2 日

【预警类型】 **高危预警**

【预警内容】

TeamViewer IT 系统遭 APT 攻陷，安全专家建议暂时删除

一、漏洞概述

安全内参 7 月 1 日消息，国际知名远程连接软件厂商 TeamViewer 上周五确认，一家极其活跃的俄罗斯黑客组织在上周早些时候入侵了其公司 IT 环境。在最新声明中，该公司将最近宣布的事件归咎于 APT29。这家黑客组织又叫 Cozy Bear、BlueBravo 和 Midnight Blizzard。据信，该组织隶属于俄罗斯的对外情报局（SVR），参与了过去十年中几起最重要的黑客事件，包括 2020 年的“太阳风”（SolarWinds）黑客事件和 2016 年对美国民主党全国委员会的攻击。

二、漏洞详情

TeamViewer 解释说，上周三的黑客攻击利用了公司 IT 环境中“一个普通员工账号的凭证”。声明中提到，目前“没有证据”表明 APT29 能够访问 公司的产品环境或客户数据，并指出公司 IT 网络与其他系统是隔离的。

公司解释说：“这意味着我们将所有服务器、网络和账号严格分开，从而防止未经授权的访问，以及在不同环境之间的横向移动。” TeamViewer 发言人没有回应有关 APT29 访问了哪些系统或数据的问题。上周五下午，TeamViewer 发布信息更新，确认攻击“仅限于 TeamViewer 的内部公司 IT 环境，并未触及产品环境、连接平台或任何客户数据。”公司承诺将继续调查该事件。

该事件在上周四曝光。当时一些组织开始警告客户和成员，APT29 对 TeamViewer 发动了攻击。网络安全公司 NCC Group 和一家医疗行业网络安全联盟都针对入侵事件发布了私密警报。NCC Group 全球威胁情报负责人 Matt Hull 建议，在更多信息出现之前，删除 TeamViewer 软件“将有助于预防通过这一途径的任何潜在入侵。” Hull 表示：“我们还建议检查安装了该软件的主机是否有异常行为。如有异常，说明主机可能已被入侵。如果您无法删除该应用程序，则应对安装了该程序的主机加以高度监控，这样能会为您提供进一步的保障。”谷歌云安全公司 Mandiant 的首席分析师 John Hultquist 表示，APT29 是“我们跟踪的最具挑战性的行为者之一，他们正在针对各种规模的科技公司发动攻击。”该组织一般会努力保持隐匿，但“并不害怕发动大胆的供应链攻击。” Hultquist 表示，APT29 的重点是获取有助于克里姆林宫做出战略决策的情报，特别是能够提供对外事务洞见的数据。APT29 最近被牵涉到对微软的一次重大攻击中。这次攻击暴露了几家美国联邦机构的电子邮件，这些邮件可能包含认证详细信息或凭证。彭博社在上周四晚间报道，微软已经开始通知更多的组织，他们的电子邮件和其他信息在 APT29 的攻击中被访问。Hultquist 指出，APT29 最近还针对

德国的政党进行了攻击。他说：“由于乌克兰冲突，俄罗斯安全部门正承受着巨大的压力，需要支持战争行为和俄罗斯领导层。俄罗斯间谍能够收集情报的任何地方都将感受到这种压力。”

三、处置建议

TeamViewer 公司多次更新公告强调，此次攻击的受影响范围仅限内部 IT 环境，不涉及产品、TeamViewer 连接平台或任何客户数据。由于近年来供应链攻击屡创纪录，安全专家建议暂时删除 TeamViewer。