8、南美

2025 年，受地缘政治摩擦影响，南美地区逐渐成为网络攻击活动的热点区域。从巴拉圭全国公民个人数据被勒索，到巴西、秘鲁、哥伦比亚等国金融系统遭遇网络攻击，再到委内瑞拉的系统性数据泄露与能源基础设施被攻击，该地区网络攻击活动规模和破坏性显著增加。

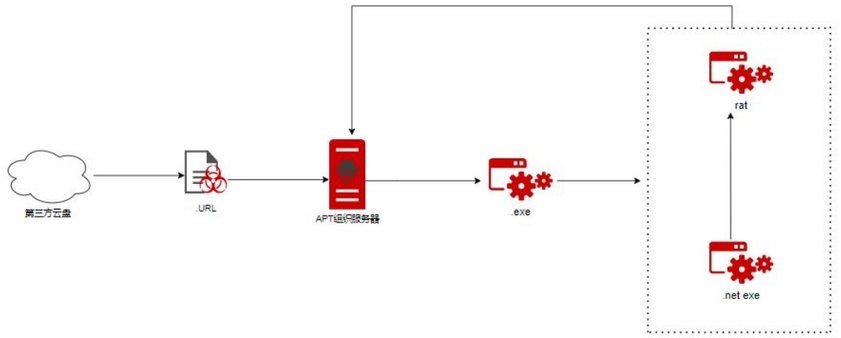
南美地区最活跃的 APT-C-36 （盲眼鹰）组织在攻击活动中组合使用 2024 年 11 月披露的 Windows 系统漏洞和第三方云平台服务，大大提升了攻击效率。同时我们发现该组织在最新的攻击活动中引入了成熟的加载器程序以丰富其攻击手段。

8.1 、 APT-C-36 （盲眼鹰）

APT-C-36 （盲眼鹰）组织近期攻击活动主要针对哥伦比亚、委内瑞拉、厄瓜多尔、巴拿马和阿根廷等南美地区国家。

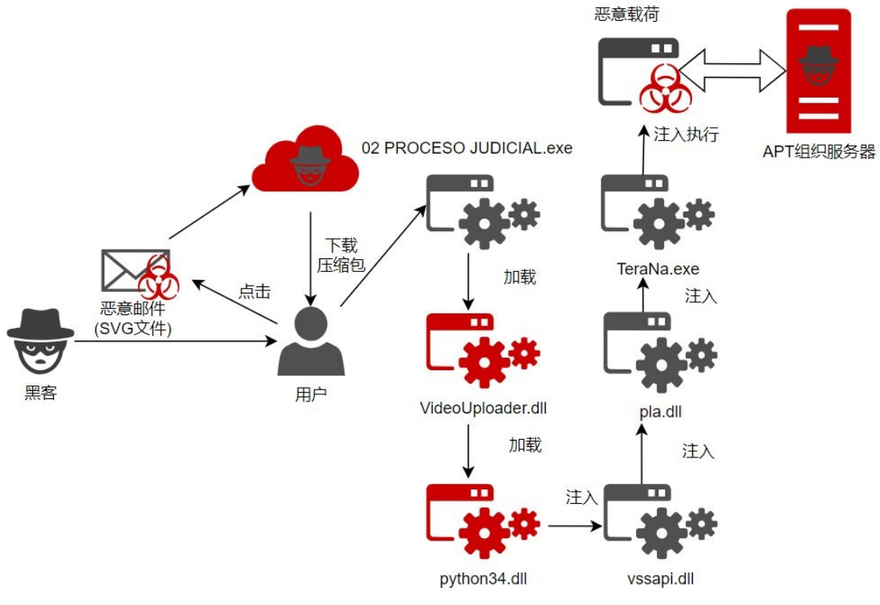
2024 年 11 月 12 日，微软披露了 Windows 系统漏洞 CVE-2024-43451 ，该漏洞载荷文件被触发后，会下载并执行恶意文件。 APT-C-36 （盲眼鹰）组织在随后的攻击活动中对未修复该漏洞的终端进行攻击。

攻击者使用钓鱼邮件向哥伦比亚政府以及司法系统人员投递钓鱼邮件，诱使用户从 Google Drive 和 Dropbox 第三方云平台下载恶意 .url 文件并执行 RemcosRAT 木马。



图①

APT-C-36 （盲眼鹰）组织在 2025 年 10 月份实施了新一轮攻击活动。攻击者使用 Hijackloader 加载器加载恶意载荷。该加载器使用各类注入手段，多阶段、反复进行 shellcode 注入，最终加载 Pure 远程控制木马，实现对受害者计算机的控制。



图②

▲图①： APT-C-36 （盲眼鹰）组织攻击流程示意图图②： APT-C-36 （盲眼鹰）组织攻击流程示意图