LevelBlue - Open Threat Exchange

By CyberHunterAutoFeed

Archived: 2026-04-05 16:46:15 UTC

CVE: 2 | **FileHash-MD5:** 42 | **FileHash-SHA1:** 41 | **FileHash-SHA256:** 54 | **URL:** 8 | **YARA:** 5 | **Domain:** 7 | **Email:** 2

根据开源信息，从2023年5月27日开始，CL0P勒索软件团伙，也被称为TA505，开始利用Progress Software的管理文件传输(MFT)解决方案MOVEit transfer中先前未知的SQL注入漏洞(CVE-2023-34362)。面向互联网的MOVEit Transfer网络应用程序被一个名为LEMURLOOT的网络外壳感染，然后被用来从底层MOVEit Transfer数据库窃取数据。在类似的活动中，TA505在2020年和2021年对Accellion文件传输设备(FTA)设备进行了零日漏洞攻击，在2023年初对Fortra/Linoma GoAnywhere MFT服务器进行了零日漏洞攻击。 CL0P于2019年2月出现，从CryptoMix勒索软件变种演变而来，在大规模鱼叉式网络钓鱼活动中被用作勒索软件即服务(RaaS)，该活动使用经过验证和数字签名的二进制文件来绕过系统防御。CL0P以前以使用“双重勒索”策略而闻名，即窃取和加密受害者数据，拒绝恢复受害者访问权限，并通过CL0P-LEAKS网站在Tor上发布泄露的数据。2019年，TA505攻击者利用CL0P勒索软件作为网络钓鱼活动的最后有效载荷，该活动涉及一个启用宏的文档，该文档使用Get2恶意软件发射器下载SDBot和FlawedGrace。在最近从2021年开始的攻击活动中，CL0P更倾向于主要依靠数据泄露而不是加密。 除了CL0P勒索软件之外，TA505还以频繁更改恶意软件和推动全球犯罪恶意软件分发趋势而闻名。TA505被认为是全球最大的网络钓鱼和垃圾邮件分发者之一，据估计，它已经攻击了3000多个美国组织和8000多个全球组织。

Source: https://otx.alienvault.com/browse/pulses?q=tag:flawedammyy