新闻发布– 2023 年 10 月 26 日

借助 AxProtector CTP，软件更能坚守抗盗版和逆向工程阵地

- **威步的软件保护机制采用了先进的混淆技术。**
- **最新的编译时保护技术利用 LLVM 编译器框架，以实现高效的保护目标。**
- **AxProtector CTP 确保应用程序的安全性，同时符合特定平台的指导原则，无需运行时代码修改。**
- **最近的 CodeMeter 保护套件更新已支持 Windows、Linux 和 macOS 系统。**

新的混淆技术使 C/C++应用程序的代码结构变得几乎无法被辨认。

德国卡尔斯鲁厄——**作为全球软件许可和保护行业的领导者，威步宣布其 CodeMeter 保护套件新增了一个反盗版和防逆向工程的自动化软件保护功能。这个名为编译时混淆（CTO）的新功能，现已适用于 AxProtector Windows、AxProtector Linux 和 AxProtector macOS。为了实现这个功能，威步还引入了一项名为 AxProtector 编译时保护（CTP）的新技术。**

这种创新技术采用了全新的软件保护方法，通过在编译过程中混淆整个应用程序来实现。AxProtector CTP 将混淆技术提升到与加密为基础的保护工具相同的安全水平，它混淆名称和控制流程、插入额外的代码块，并隐藏代码中的逻辑连接，从而提高抵御逆向工程的保护级别。AxProtector CTP 技术已经作为 AxProtector Windows、AxProtector Linux 和

AxProtector macOS 产品中的可选功能（CTO）进行商业化销售；它支持 Intel、ARMHF 和 AARCH64 平台，并目前支持 C 和 C++编程语言，其他语言可根据需求提供。

找到对抗网络攻击者的正确防御技术是至关重要的。正是因为 LLVM 的多功能性，AxProtector CTP 才能支持多种操作系统、架构和平台。此外，AxProtector 原有的各种功能，包括由可信的加密算法支撑的灵活许可机制，在新的 CTP 技术下也得以完善。应用程序通过授权、加密和混淆三者的紧密协同，达到了最优的保护效果。

AxProtector CTP 与传统的基于加密的保护方法有所不同。传统方法是在编译后加密应用程序，然后在运行时再进行解密。但 AxProtector CTP 直接在编译阶段进行修改，因此运行时无需任何更改。这不仅满足了像 macOS 这样的平台禁止在运行时更改代码的要求，还确保了攻击者在尝试破解受保护的应用时面临巨大的挑战。为此，我们专门设计了更高级别的防护措施。

新的 AxProtector CTP 提供的保护需要特定的构建环境，这些环境需要与威步制作的修改后的 Clang 编译器和一个额外的插件兼容。只需要对编译器进行最小的调整；软件开发者可以根据威步提供的设置指南进行这些调整。这些调整的目的仅仅是为了激活插件的使用。为了方便，威步在安装程序中提供了一个预先构建的版本。鉴于 Visual Studio 和 Xcode 等主流开发环境都支持 Clang 编译器，AxProtector CTP 的功能能够即刻投入使用，同时它还继承了标准 AxProtector 的跨平台保护特性。

> *“在面对日益变化的网络威胁时，单靠加密手段已不足以应对。AxProtector CTP 采用更先进的策略，通过编译时的代码混淆，让其对于即便是最高手的黑客也成为难以破解的难题。”威步销售总监和大客户管理 Stefan Bamberg 如是说。*

AxProtector CTP 采用先进的混淆机制，加强了 Windows、Linux 和 macOS 应用程序对抗盗版和逆向工程的保护。

威步信息系统（上海）有限公司

电话 +86-21-5566-1790
info@wibu.com.cn
https://www.wibu.com.cn/

威步信息系统为全球数据安全及软件授权管理领域的领导者。我们致力于为用户提供专业的安全解决方案，保护开发者的数字资产知识产权，促进其充分发挥技术专业知识货币化的潜能。
威步提供的软、硬互连的综合解决方案，可有效地防止盗版、逆向工程、篡改、破坏以及跨平台和行业的网络攻击，以满足软件开发者和智能设备制造商日益灵活、细分和复杂的需求。

更多图片资源请访问：https://www.wibu.com.cn/cn/图片库.html