AUTODESK

下載盜版軟體的風險

瞭解惡意程式碼對您和您企業潛藏的危險

什麼 **是惡意程式碼？**

惡意程式碼通常隱藏在盜版軟體中，專門用於擾亂、破壞或未經授權存取電腦系統。

是誰 **建立惡意程式碼？**

網路犯罪份子，這可以是個人或團體，他們利用技術來進行惡意活動。

為何 **惡意程式碼有危險性？**

一旦進入了您的電腦系統，它就可以存取金錢、重要資料、文件、財務資訊，以及對您、您的員工和公司有價值的一切。

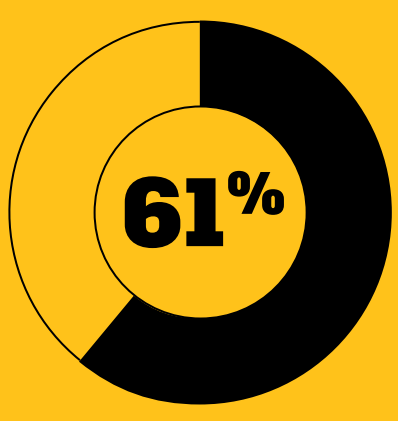
每次惡意程式碼攻擊平均會造成公司 240 萬美元的損失，解決時間可能需要長達 50 天。

來源：BSA - 全球軟體調查

$2.4 百萬

在 2020 年，有 61% 的組織經歷了勒索軟體攻擊而導致業務營運中斷。

來源：Mimecast



在盜版的 Autodesk 熱門軟體中，有 30% 至 70% 感染了惡意程式碼。這是您願意承擔的風險嗎？

來源：Autodesk Keygen Weaponization Research (Autodesk 註冊機武器化研究)，2021 年 4 月

惡意程式碼旅程

有多少位使用者，就有多少個惡意程式碼旅程。以下範例說明公司中如果有員工出於善意地只想把工作做好，但卻不瞭解情況時，會發生什麼事情。

1 需求

有位員工找到了完美的 Autodesk 產品，並將其用來完成交期緊迫的工作。由於這位員工知道新授權的核准流程很長，而且對內部伺服器的存取權受到限制，**所以該員工要尋找更容易存取軟體的方法。**

2 機會

這位員工透過了快速搜尋找到了免費的線上版本。這個網站看起來合法，而且他們很高興能透過這項交易節省時間和金錢。這位員工毫不猶豫地點擊了下載。

3 爆發

該軟體感染了惡意程式碼 (30% 到 70% 的盜版軟體含有惡意程式碼)，並且開始在整個公司的網路中傳播。與此同時，該員工繼續使用該軟體，並且在效能方面遇到了一些小問題。

4 攻擊

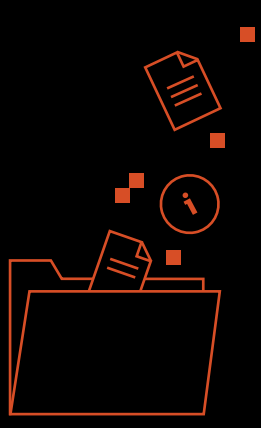
惡意程式碼在後台迅速傳播，其行為視惡意程式碼的類型而定：

→ 它可以無聲無息地在幕後工作，並且收集機密資料。

→ 它可以要求使用者下載外掛程式或更新軟體，這很可能會使他們的電腦和檔案感染額外的惡意程式碼。

→ 它可以封鎖對檔案和資訊的存取，並要求贖金。

5 結果



盜版的 Autodesk 軟體中的惡意程式碼會對整個組織造成重大破壞和不可逆轉的後果，例如：

→ 設計盜竊
→ 客戶名單盜竊
→ 財務資料盜竊
→ 機密工作在公開發佈日前外洩

認識惡意程式碼類型

木馬

將自己偽裝成合法軟體，對使用者的檔案進行後門存取，以透過資料和檔案破壞或贖金尋求經濟利益。

PUA
(潛在附加軟體)

他們以搜尋引擎或防毒程式為目標，對使用者的電腦造成損害或影響軟體效能。

勒索軟體

首先，他們會封鎖您的軟體與檔案。然後他們直接聯絡您，要求您交出贖金才能取回軟體和檔案。

註冊機 (或金鑰產生器) 最常被作為武器，以用來向受影響的使用者索取財務資料。這通常會透過使用木馬或 PUA 來完成。大約有 90% 的盜版金鑰產生器都是用惡意程式碼作為攻擊武器。

來源：Autodesk Keygen Weaponization Research (Autodesk 註冊機武器化研究)，2021 年 4 月

如何 保護貴公司不受到惡意程式碼的侵害？

步驟一 **從可靠來源購買正版軟體**

您知道嗎？從不信任來源下載的 Autodesk 軟體中，有 30% 至 70% 感染了惡意程式碼，從可靠來源 (Autodesk 或授權經銷商) 購買軟體是保護您的公司和員工的第一步。

步驟二 **定期進行適當維護**

軟體資產管理 (SAM) 涉及到您組織內部軟體的最佳化、維護和處置方式。這關係到您是否只保留所需要的軟體並對其進行更新。

步驟三 **安裝適當的防毒軟體並定期檢查**

並非所有防毒軟體都內建相同的能力，因為它們並不一定能偵測到電腦或組織內的惡意程式碼。根據 Autodesk 威脅情報團隊最近進行的研究指出，72 間防毒供應商的平均檢測率為 28%。也就是說，您應該定期執行防毒軟體以保持一切正常。