KASPERSKY lab

ATM 和 POS 安全指南

讓重要的支付系統獲得有效的高效率安全防護

www.kaspersky.com

隱憂

嵌入式系統有特定的安全隱憂。這些系統通常分散在各地，因此對管理構成挑戰，而且甚少執行更新。ATM 和銷售點 (Point of Sale) 裝置的運作伴隨著真正的金錢與信用卡認證，因此成為網路犯罪者選擇的目標，所以需要頂級的集中式智慧防護。

過時的軟體是非常常見的問題，而且不僅只是消費者的作業系統會受到影響，最知名的範例便是某些仍在繼續運作的人造衛星，使用的是數十年的老舊硬體和軟體。工業控制系統也有相同的問題，使用非常老舊的作業系統，而且更新的週期時間極為長久。同樣的問題也發生在銀行系統，而且不僅是端點—內部的自動化銀行系統通常有好幾年的時間不會更新。就 ATM 而言，80% 較小的銀行傾向等到下一個結束週期 (可能要等 5 到 10 年，甚至更久)，才會購買已經安裝全新軟體的新機器，而不是在新版推出時更新。

Windows XP 系列仍是 ATM 和 POS 裝置最常使用的作業系統。此作業系統的結束支援，已經對許多企業和政府機構造成影響。在全球有許多 ATM 執行 Windows XP Professional for Embedded Systems 的銀行業和零售業，受到的影響特別嚴重。事實上，這種系統已經在 2014 年 4 月隨著消費版 Windows XP 實際停止支援。

全面更換 ATM 及 POS 系統軟體，是一項耗費多時、所費不貲，而且工程浩大的處理流程。除此之外，更換軟體通常表示也要更換仍在運作的硬體 (如果技術過時)。

威脅情況

ATM 是一種在銀行實體安全防護範圍外運作的裝置，而且內含真正的現金，而 POS 系統會擷取已驗證的個人資料與信用卡詳細資料，兩者必然高居網路犯罪者的攻擊清單上。

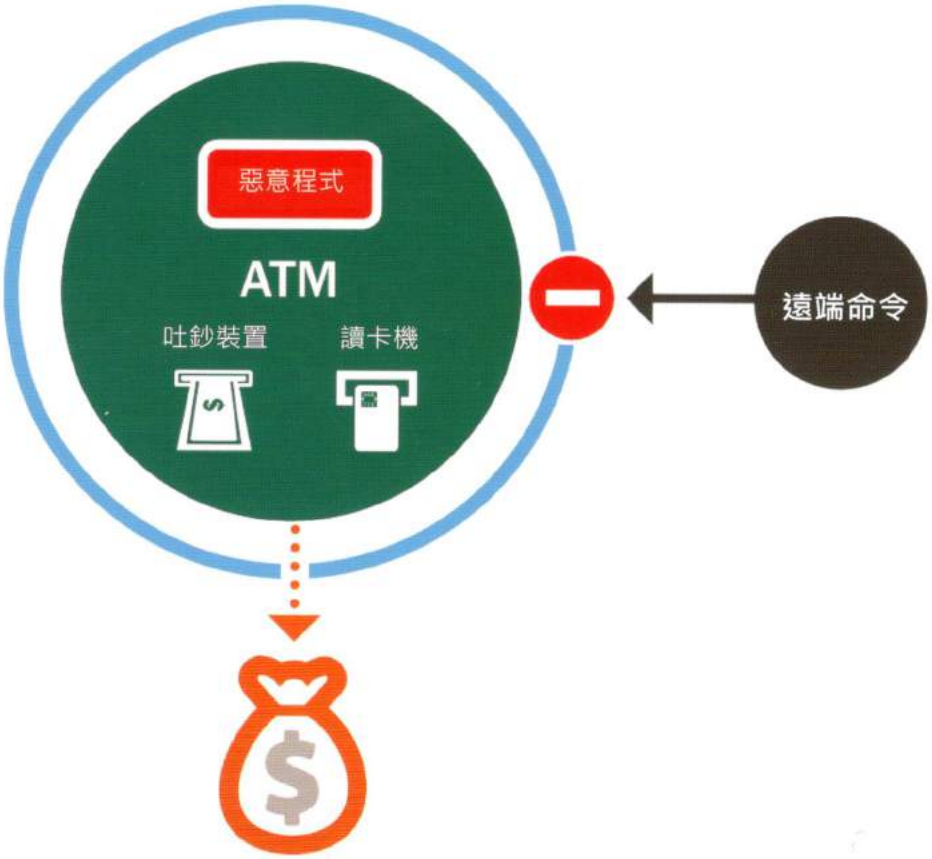
自 Skimer 惡意程式在 2009 年發動首起針對 ATM 的嚴重攻擊開始，攻擊的數量和品質便逐年大幅增加。對 ATM 和 POS 系統發動的攻擊在 2015 年創下新高，使用的惡意程式包含 Ploutus、Tyupkin、Carbanak、CardStealer、vSkimmer、Chewbacca、POSeydon 及 FindPOS。

傳統的防毒軟體無法完全防止所有的威脅，而且 ATM 和 POS 具有脆弱管道、低階硬體和過時軟體的限制，造成安裝和部署方面的挑戰，而且這麼做通常不切實際。因此這些病毒可以不斷成功入侵大型金融機構和零售商每天使用的 ATM 和 POS 系統。

同時，在專業的開發人員製作下，高度針對性 ATM 和 POS 惡意程式數量持續增加，還有最新且最強大的系統和硬體提供支援。

簡單的 ATM 攻擊，就是快速輕鬆取得現金的方法。不過在更多的攻擊情況中，ATM 感染也是其中一部份。我們已經看見，進階持續威脅攻擊 (例如：2015 年的 Carbanak) 如何導致全球超過 10 億美金財物損失。

ATM 攻擊機制



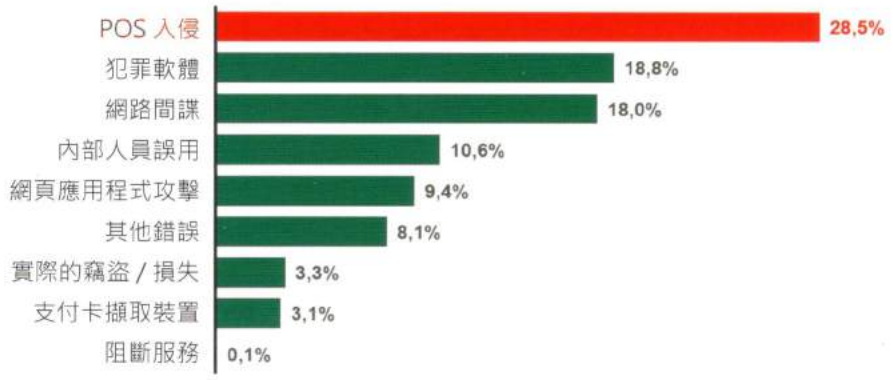
在地理上分處各地的 ATM 端點，是針對性攻擊過程中非常理想的惡意程式感染目標，特別是 USB 存取連接埠及鍵盤位於 ATM 本身後方的系統服務機櫃，只靠一個基本鎖保護，取用非常方便。

事實上，甚至上鎖本身可能也不是個問題。當地服務工程師長時間插著 USB，或是為了節省反覆解鎖的動作而將 LAN/ 數據機纜線拉出 ATM 服務機櫃，其實並不罕見。為了提高安全性而停用機櫃中的 USB 連接埠或 CD/DVD 光碟機這並不實際，因為維修工程師為了維護機器，必須定期使用這些裝置。

一旦惡意程式透過一台機器進入 ATM 系統，便會徹底隱藏在其中一段時間，讓系統繼續正常運作，同時取得各項資訊並預作準備。等到時機成熟後，使用特定的卡片或 PIN 碼觸發系統邏輯中的變化，即可讓每部受感染的 ATM 依照犯罪者的命令吐出其中的鈔票。

POS 型威脅

發生 IT 安全事件的頻率
已確認的資料外洩類別

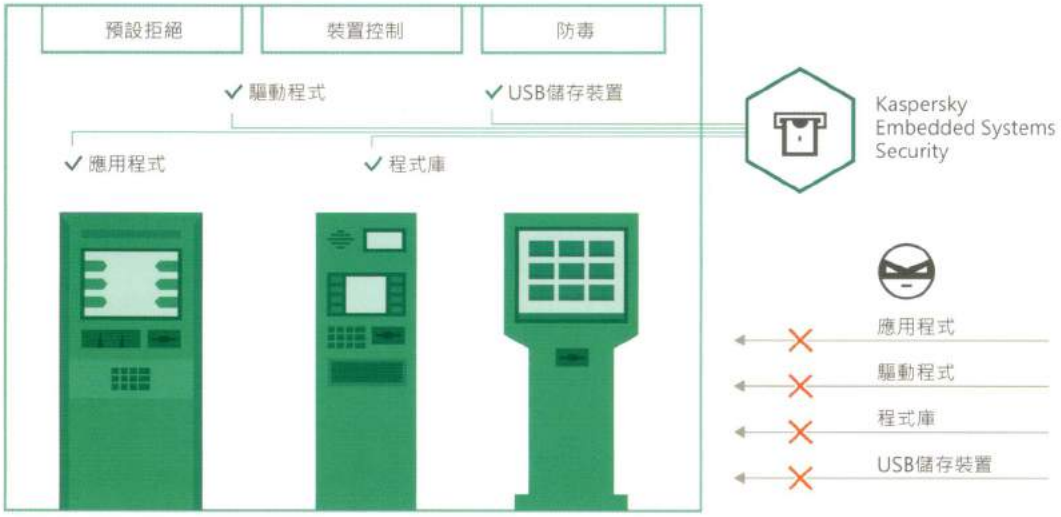


*** 資料外洩調查報告 2015 年版本**

銷售點系統的特定弱點區域，是該系統所需的中介軟體。這種中介軟體通常是由小型第三方供應商或內部製作。其功能性可能會因為設計考量而優先於安全性，但是對 ATM 而言，容易存取 USB 連接埠和 CD/DVD 光碟機通常被視為方便使用，而不是安全弱點。

大多數的 POS 系統會搭配信用卡 / 簽帳卡運作，因此就和 ATM 一樣，會受到 PCI DSS 法規的限制。所有的 POS 系統都會處理客戶的個人資料，無一例外，因此該系統的防護責任就落在 POS 系統所有人的身上。另外，所有的 POS 系統都連線至內部網路，讓 POS 成為針對性攻擊有利的進入點。

KASPERSKY EMBEDDED SYSTEMS SECURITY



卡巴斯基實驗室特別針對使用 ATM 和 POS 系統的企業組織，以及這些系統所面臨的威脅環境建立安全解決方案，以反應其獨特的功能及作業系統、管道與硬體要求，而且完全支援 Windows XP 系列。

Kaspersky Embedded Systems Security 可緩解嵌入式系統中既有的安全風險。此解決方案是專為 ATM 和 POS 系統設計，可防止特別針對這些架構的攻擊面，並且重視相關硬體和效率方面的考量。針對管理端點、重要系統及整個 IT 基礎結構的有效多層次安全，單一的直覺式主控台可提供所需的控制能力與可視性。

針對應用程式、驅動程式和程式庫執行預設拒絕，並經由裝置控制功能強化，是確保技術方面「過時」的系統可持續安全使用的唯一方法。

Kaspersky Embedded Systems Security 提供「僅預設拒絕」的操作模式，最低系統需求為 256Mb RAM 和 50Mb HDD 空間，因此很適合低階硬體執行的 Windows XP 型系統。由 Kaspersky Security Network 提供技術支援的選購防毒模組具備依需求指定掃描的功能，也可視需求提供修補程式管理的設備。

因此，這項單一解決方案可以滿足三個主要目標：

- 以高效率保護「難以管理」的系統
- 符合 PCI DSS 要求 5.1、5.1.1、5.2、5.3 和 6.2 的標準
- 為更換過時的系統硬體提供彈性時間表。

預設拒絕

大部分的傳統防毒解決方案無法完全防止工業目前所面臨的進階針對性惡意程式威脅。預設拒絕功能提供更具基本面的不同方法。若無安全系統管理員的中央核准，軟體防護以外的可執行檔、驅動程式和程式庫均無法在任何的 ATM 或 POS 端點上執行。

裝置控制

卡巴斯基實驗室的裝置控制，可針對嘗試與系統硬體進行實體連線的 USB 儲存裝置進行控制，防止任何未經授權的裝置對 ATM 或 POS 裝置進行存取。因此，系統弱點的進入點便能加以封鎖；這些系統弱點經常被網路犯罪者使用，做為惡意軟體攻擊的第一步。

Windows XP 至 Windows 10 就緒

經過了 12 年，Windows XP Embedded 的支援在 2016 年 1 月 12 日終止，而 Windows Embedded for Point of Service 在 2016 年 4 月 12 日終止。Windows XP 作業系統將不再有安全性更新或技術支援。Kaspersky Embedded Systems Security 100% 支援 Windows XP 系列。

專為嵌入式系統硬體設計

Kaspersky Embedded Systems Security 在設計上，可以在大部分 ATM 和 POS 硬體所採用的低階系統上充分發揮效果。Windows XP 系列的最低需求僅需 256 Mb 的 RAM，而系統硬碟僅需約 50 Mb 的空間。在「依需求指定」模式中運作時，另外安裝的防毒模組在設計上僅會在手動或排程掃描期間使用硬體資源。

防毒軟體和 Kaspersky Security Network

PCI DSS 法規表示，與信用卡或簽帳卡接觸的所有系統，都必須安裝防毒軟體並定期更新。Kaspersky Embedded Systems Security 提供高效率的防毒保護，同時可視需要進行定期自動或手動惡意程式特徵碼更新。因為在 ATM 和 POS 系統中發現的惡意軟體中，有超過半數是透過零日 / 零秒入侵程式進入，所以卡巴斯基實驗室也建議以 Kaspersky Security Network 知識庫的形式實行智慧安全，以防止和緩解入侵程式型安全風險，並將反應時間縮到最短。

PCI DSS 法務遵循

Kaspersky Security for Embedded Systems 的功能符合且高於 PCI DSS 3.1 版子項目下的所有安全標準：

5.1：在經常受到惡意軟體影響的所有系統中，部署防毒軟體 (尤其是個人電腦及伺服器)。

5.1.1：確保防毒程式能夠偵測、移除及防護所有已知類型的惡意軟體。

5.2：確保所有的防毒機制都會持續更新、執行定期掃描，並產生符合 PCI DSS 要求 10.7 的稽核記錄。

5.3：確保防毒機制持續運作，而且除非管理階層以個案方式針對特定時期做出特別授權，否則使用者無法停用或變更。

6.2：確保安裝適當的供應商所提供的安全性修補程式，以保護所有系統元件和軟體的已知弱點。在發佈的一個月內安裝重大安全性修補程式。

防毒以外的要求

支付卡產業資料安全標準 (PCI DSS) 針對信用卡資料型的系統制定許多技術要求與設定。不過，ATM 和銷售點裝置的安全法規似乎只包含防毒型安全。上述內容與近期的攻擊，充分證明單純的防毒方法對於目前的 ATP/POS 威脅效果有限。因此為重要的嵌入式系統套用已經在其他安全防護場合充分驗證的裝置控制及預設拒絕，目前正是時候。

如需進一步了解更有效保護關鍵支付系統端點的做法，請與卡巴斯基實驗室企業銷售團隊連絡。