利用 ATM 惡意程式大發利市

完整剖析各種攻擊型態

趨勢科技前瞻威脅研究 (FTR) 團隊、
歐洲刑警組織 (Europol) 歐洲網路犯罪中心 (EC3)
聯合製作

TrendLabs 研究報告

作者：
David Sancho 與 Numaan Huq
— 趨勢科技前瞻威脅研究 (FTR) 團隊
Massimiliano Michenzi
— 歐洲刑警組織 (Europol) 歐洲網路犯罪中心 (EC3)

內容

前言

2016 年 4 月，趨勢科技和歐洲刑警組織 (Europol) 率先發表第一份民間產業與政府執法部門共同合作的研究報告，聚焦 ATM 惡意程式的威脅。該報告詳細分析了這項崛起中的威脅，以及該如何防範這類犯罪。不幸的是，情勢的演變正如該報告所預言，這類犯罪不僅複雜性不斷提升，地理分布區域也越來越廣。

2017 年，這份報告又再度更新，並且發現歹徒所用的惡意程式已大幅演進，而且攻擊的範圍和規模也相對擴大。儘管民間產業與政府執法部門之間的合作已更加緊密，而警方也已破獲了不少重大案例，但犯罪的情況依然不減。這是因為網路犯罪集團的獲利實在太驚人。

這份報告將評估這項威脅未來的發展動向，希望它能成為民間產業及政府執法部門合作的藍本。

Steven Wilson
Europol 歐洲網路犯罪中心 (EC3)
主席

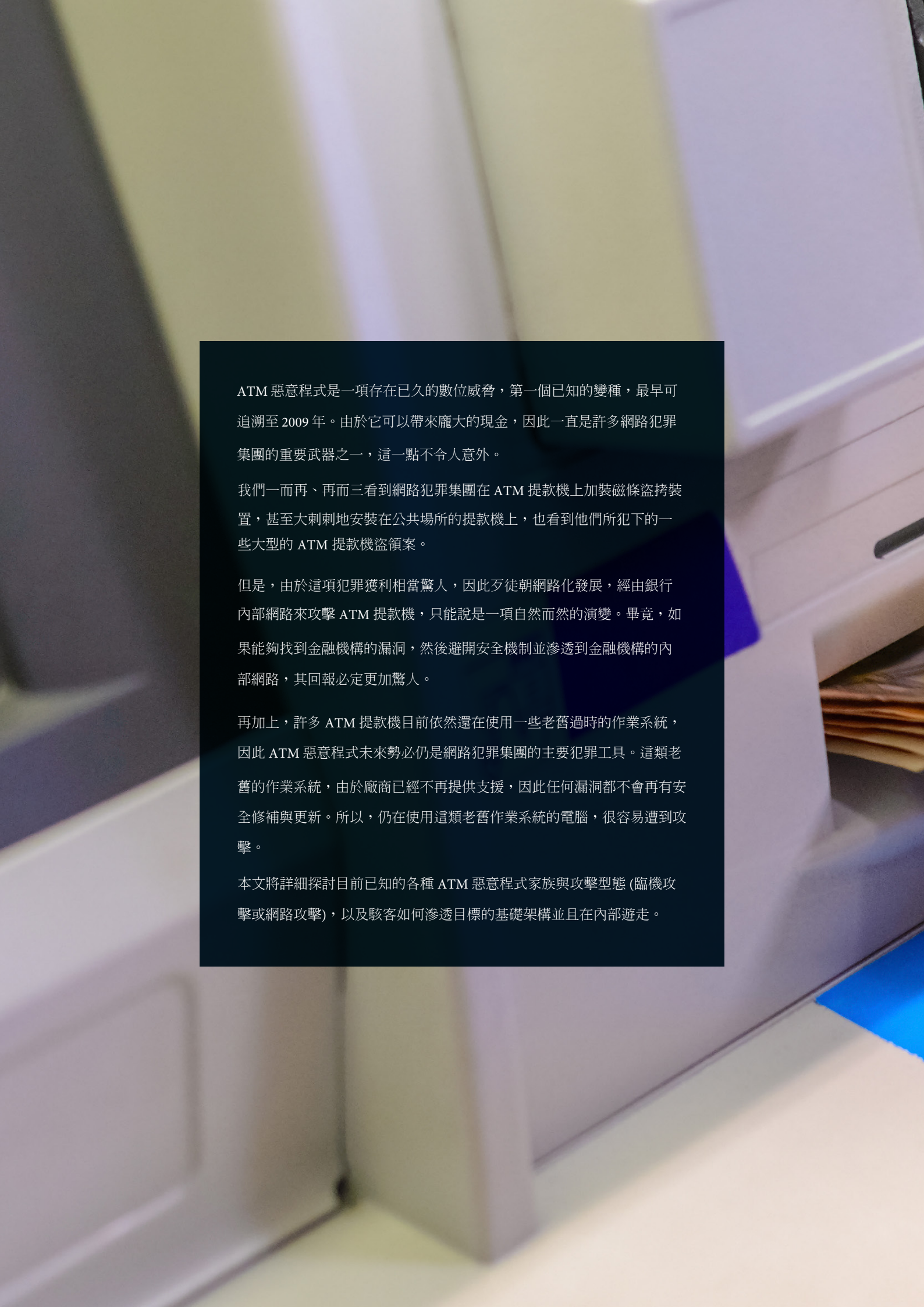
Martin Roesler
趨勢科技前瞻威脅研究 (FTR) 團隊
資深總監

ATM 惡意程式攻擊在全球各地不斷登上媒體版面，並且對金融業造成重大損失。然而若從更大的角度來看，這意味著 ATM 提款機的數位安全相當令人擔憂。我們不難猜測，歹徒使用 ATM 惡意程式的情況將逐漸開始普遍，因為網路犯罪集團隨時都在精進其攻擊手法，為的就是希望能夠避開偵測以避免遭到逮捕。這一點，對於金融機構與執法機關來說將是個日益嚴重的問題。但只要我們同心協力，就能提升安全。

藉由這份探討當今各 ATM 惡意程式家族與攻擊手法的聯合研究報告當中，Europol 歐洲網路犯罪中心 (EC3) 與趨勢科技前瞻威脅研究 (FTR) 團隊希望能夠提升金融業的整體意識，並協助政府單位，讓他們能夠順利瓦解那些動不動就造成全球企業數十萬美元損失的網路犯罪集團。

當 ATM 惡意程式攻擊已經超越了必須臨機操作的層次，相關企業必須比以往更加小心謹慎並採取必要的防護。正因如此，我們的報告詳細介紹了 ATM 惡意程式的發展，以及過去幾年來所見過的攻擊型態，和犯罪集團發動聯合攻擊的配合技巧。

在 Europol EC3 資安專家的配合下，趨勢科技相信威脅情報是維繫數位安全與策略不可或缺的重要元素。希望這份詳盡的報告會對金融機構與執法機關都有所幫助，進而改善網路資安情勢。



ATM 惡意程式是一項存在已久的數位威脅，第一個已知的變種，最早可追溯至 2009 年。由於它可以帶來龐大的現金，因此一直是許多網路犯罪集團的重要武器之一，這一點不令人意外。

我們一而再、再而三看到網路犯罪集團在 ATM 提款機上加裝磁條盜拷裝置，甚至大剌剌地安裝在公共場所的提款機上，也看到他們所犯下的一些大型的 ATM 提款機盜領案。

但是，由於這項犯罪獲利相當驚人，因此歹徒朝網路化發展，經由銀行內部網路來攻擊 ATM 提款機，只能說是一項自然而然的演變。畢竟，如果能夠找到金融機構的漏洞，然後避開安全機制並滲透到金融機構的內部網路，其回報必定更加驚人。

再加上，許多 ATM 提款機目前依然還在使用一些老舊過時的作業系統，因此 ATM 惡意程式未來勢必仍是網路犯罪集團的主要犯罪工具。這類老舊的作業系統，由於廠商已經不再提供支援，因此任何漏洞都不會再有安全修補與更新。所以，仍在使用這類老舊作業系統的電腦，很容易遭到攻擊。

本文將詳細探討目前已知的各種 ATM 惡意程式家族與攻擊型態 (臨機攻擊或網路攻擊)，以及駭客如何滲透目標的基礎架構並且在內部遊走。

從臨機攻擊到網路攻擊：ATM 惡意程式演化史

2016 年，我們發表了一份非公開的研究報告，詳細介紹了一些已知專門攻擊 ATM 提款機的惡意程式家族。該份報告的主要重點在說明這些惡意程式家族如何利用 ATM 應用程式開發介面 (API) 與金融服務延伸功能 (eXtensions for Financial Services，簡稱 XFS) 的 API，來與 ATM 的相關硬體溝通，其中最主要的是讀卡機和吐鈔機。

當時，我們發現駭客感染 ATM 提款機主要是靠臨機攻擊：駭客實際打開提款機外殼，在裸機的情況下使用 USB 隨身碟或 CD 光碟將提款機系統重新開機。這樣的攻擊方式雖然至今仍然可見，不過，最近已開始出現上次報告曾經暗示過的一種新式攻擊，那就是：網路攻擊。

儘管當時我們只是推測這樣的情況有可能發生，並未料到我們竟然一語成讖。隨著銀行開始對 ATM 提款機的臨機攻擊有所警覺，並且採取一些必要的防範措施，駭客也跟著開始另闢途徑，也就是 ATM 網路攻擊。

要經由網路感染 ATM 提款機，駭客需要更多的事前規劃與準備，其最大的困難在於從銀行內部網路進入 ATM 網路。因為，在一個規劃良好的網路架構中，這兩個網路通常會分開獨立，因此要從某個網路進到另一個網路必須穿越防火牆和其他可能的安全機制。不幸的是，某些銀行並未實施網路分割。就算兩者分開獨立，在某些已知的案例當中，歹徒還是能夠經由銀行內部網路將惡意軟體安裝到 ATM 提款機上。

為了讓讀者有個大致的概念，以下我們將所有已知的攻擊分成兩大類：

1. 經由臨機操作方式進入 ATM 提款機的攻擊：在這類案例當中，歹徒通常利用一把萬能鑰匙或用暴力的方式打開提款機外殼。
2. 經由網路進入 ATM 提款機的攻擊：這類攻擊通常需要先駭入銀行內部網路。

在介紹過這兩種攻擊之後，我們會在第三節當中再介紹兩種較為特殊且較為罕見的攻擊型態。我們相信這兩種攻擊雖然較不常見，但仍值得注意，因為只要是之前曾經發生過的案例，之後還是可能會再出現。為了力求完整，我們也將介紹一個用來測試上述攻擊方式的工具。儘管該工具不會用在攻擊當中，但卻顯示歹徒在實際行動之前如何測試其攻擊手法。

在這份報告的最後，我們將探討 ATM 攻擊背後的犯罪集團。然而，追溯攻擊源頭是件棘手的問題，因此我們主要將著眼於整體的威脅情勢，並約略分析一下歹徒在這類攻擊當中的獲利模式。

最後請記住，在所有已知的攻擊案例當中，歹徒使用 ATM 惡意程式的最終目標都是為了在提款機上安裝一個程式來吐光提款機內的鈔票，或是盜取提款機內保留的金融卡資料，或兩者都有。

ATM 基本構造：如何進入 ATM 提款機內部

ATM 惡意程式的主要目標就是連上並操控提款機內的周邊裝置，進而讓提款機吐鈔，或者/並且蒐集銀行客戶的金融卡資料。因此，要了解 ATM 惡意程式如何攻擊提款機，首先必須認識提款機的內部構造。以最簡單明瞭的方式來看，ATM 提款機基本上就是一台電腦再加上一個小金庫，然後外面用一個機殼加以包覆。此外，ATM 提款機還可連接一些周邊裝置來為客戶提供多樣化服務，例如：提款、存款、轉帳、付款等等。儘管 ATM 提款機有各種外觀樣式和體型，但內部構造其實大同小異。下圖示範 ATM 提款機的基本構造與各部分元件：

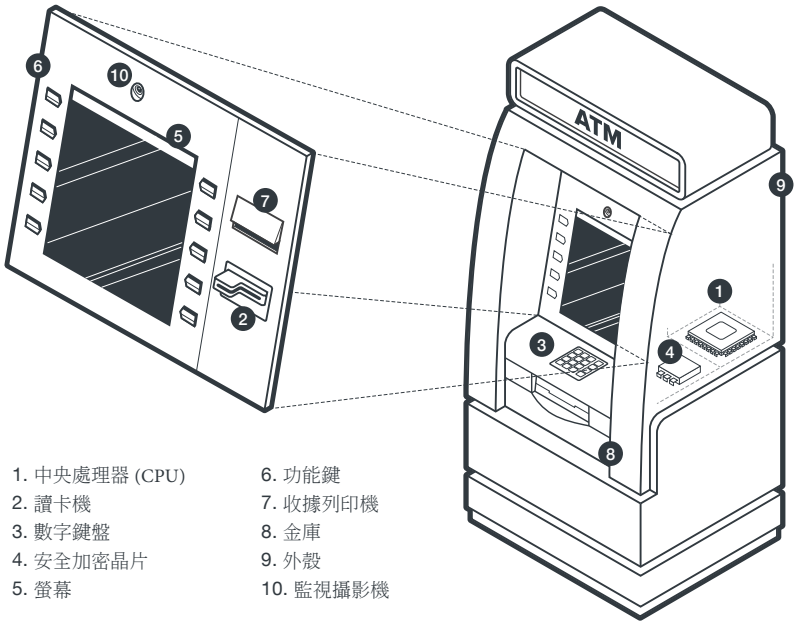


圖 1：ATM 提款機各部分元件。

ATM 提款機主要由以下單元所構成：

1. **中央處理器 (CPU)：**負責控制使用者操作介面、通訊、管理周邊裝置、處理交易。
2. **讀卡機：**磁條或晶片卡讀卡機，負責讀取金融卡。
3. **數字鍵盤：**具備加密功能的數字鍵盤 (EPP)，可將鍵盤上輸入的 PIN 碼加密。
4. **安全加密晶片：**負責通訊的加密與解密，所有交易皆採用 AES 或 3DES 加密演算法。
5. **螢幕：**負責顯示 ATM 的操作介面，某些較新的 ATM 會採用觸控螢幕和虛擬功能鍵。
6. **功能鍵：**螢幕或觸控螢幕旁邊的按鍵，用來選擇螢幕上的選項或常用功能。
7. **收據列印機：**用來列交易記錄，某些 ATM 還可補登存摺。
8. **金庫：**這是 ATM 最重要的元件，採用高張力鋼板打造。金庫內包含了吐鈔機制、支票和現鈔存款機制、鈔票進出登記系統、鈔票箱以及安全鎖。
9. **內層機殼：**這是一層客製化的金屬機殼，外層機殼基本上是採用高硬度熱成形 ABS 塑膠製造，並且貼有銀行的標誌。
10. **保全設備：**ATM 提款機同時也會配備監視攝影機，以及 (磁鐵、溫度、地震、瓦斯等等) 安全感應裝置、喇叭、指示燈等等。

今日的 ATM 提款機再也不像以往採用特殊規格的硬體，而是一般標準的 PC 與 USB、乙太網路、IP 通訊協定以及 Windows® 作業系統等等。最主要的原因應該是成本的考量，除了零件更便宜之外，軟體的支援度以及互通性也更好。

目前全球安裝的 ATM 提款機絕大多數都仍在使用 Windows XP 或 Windows XP Embedded 作業系統。某些更老舊的提款機甚至還在使用 Windows NT®、Windows CE® 或 Windows 2000。Microsoft® 早在 2014 年 4 月 8 日就已終止 Windows XP 的支援。Windows XP Embedded 的延長支援也在 2016 年 1 月 12 日截止。此外，Windows Embedded Standard 2009 的延長支援也預計在 2019 年 1 月 8 日截止。這意味著，至

少有數十萬台 ATM 提款機所使用的作業系統，早已不再或者即將不再收到安全更新，無法修補新發現的漏洞。ATM 上的應用程式會使用 XFS 中介軟體來和周邊裝置溝通 (後面會再進一步深入探討 XFS 中介軟體的問題)。

ATM 會透過 ADSL 或撥號連線數據機，經由電話線或專線連上網路。ATM 所使用的低階網路通訊協定為 SNA over SDLC、TC500 over Async、X.25, 以及 TCP/ IP over Ethernet[1]。ATM 會連上一些跨行網路 (NYCE、PULSE、PLUS、Cirrus、AFFN、Interac、STAR、LINK、MegaLink 及 BancNet) 並且經由「ISO 8583：Financial transaction card originated messages – Interchange message specifications」金融卡交易訊息交換規格來溝通[2、3]。ISO 8583 並未包含路由資訊，因此需搭配一個 TPDU 標頭[4]。交易訊息內容會以 AES 或 3DES 加密。為了提高安全性，ATM 提款機與跨行網路之間的所有通訊，也可能會再經過 SSL 加密。

PC 和 ATM 之間的相似之處

如果我們將 ATM 提款機看成一台 Microsoft Windows PC 連接著一個裝滿鈔票並經由軟體控制的保險箱，那就不難理解為何歹徒會視 ATM 提款機為肥羊。不過，ATM 和一般桌上型 PC 還是有些重要差別，主要有兩點：

1. 第一，也是最重要的，就是 ATM 提款機內部不是一般人可以碰觸的。使用者只能經由讀卡機和數字鍵盤來操作 ATM 提款機，無法輕易碰觸到內部硬體。換句話說，歹徒必須經由讀卡機來感染提款機，不然就是設法將外接裝置連接到內部主機板。

   過去雖然出現過使用磁條讀卡機來感染 ATM 提款機的案例[5]，但由於情況太過特殊，所以不值得一提。歹徒最常見的感染手法，還是設法打開提款機的外殼，然後直接將外接裝置連上內部的連接埠。USB 是歹徒最常使用的連接埠，但如果遇到一些更老的機器，可能就要透過 CD/DVD 光碟機，不過基本上原理是一樣的。

2. ATM 提款機和桌上型 PC 第二個最重要的差別在於網路連線能力。ATM 通常不會直接連接銀行的內部網路，而且當然不會連上網際網路。最常見的設定是將 ATM 透過虛擬私人網路 (VPN) 方式連接到銀行分行。有些偏遠地區的 ATM 提款機甚至會經由衛星連線到銀行的網路。在這樣的架構下，歹徒只要有辦法入侵網路基礎架構或是其網路安全設定不正確，就會出現問題。

中介軟體 – 進入保險箱的關鍵

XFS 是一種為金融業所特有、專為 Microsoft Windows 平台上的金融軟體提供主從式架構的中介軟體[6]。ATM 提款機系統中通常都會安裝 XFS 中介軟體，而 ATM 廠商和金融服務供應商也大多支援 XFS。XFS 的規格定義了一整套軟體介面，包括：

- 一組應用程式開發介面 (API)
- 一組對應的服務供應商介面 (SPI)
- 負責處理 API 和 SPI 的支援服務

XFS 為使用者應用程式提供一個介面來存取 ATM 提款機內連接的裝置與執行中的金融服務。由於這些裝置 (數字鍵盤、磁條讀卡機、收據列印機、吐鈔機) 都是複雜、特殊規格且不易管理的硬體，因此使用 XFS 可為金融機構及其服務供應商提供多項好處。

使用 XFS API 來與周邊裝置 (數字鍵盤、吐鈔機、收據列印機) 或銀行服務 (如跨行網路) 溝通的應用程式，只需透過這套介面就能與符合 XFS 標準的不同廠商裝置或服務溝通，無須修改程式碼。這就如同程式設計師只要使用 Windows API 就能順利開啟檔案而不必管系統上安裝的是哪一種硬碟。這也是為何撰寫 ATM 惡意程式的駭客會透過 XFS API 來入侵 ATM 提款機：因為這樣可以很容易和外接周邊裝置溝通，而且這樣一來，惡意程式也可以在不同廠牌的 ATM 提款機上執行而不需修改程式碼。

以下是 XFS 系統架構示意圖：

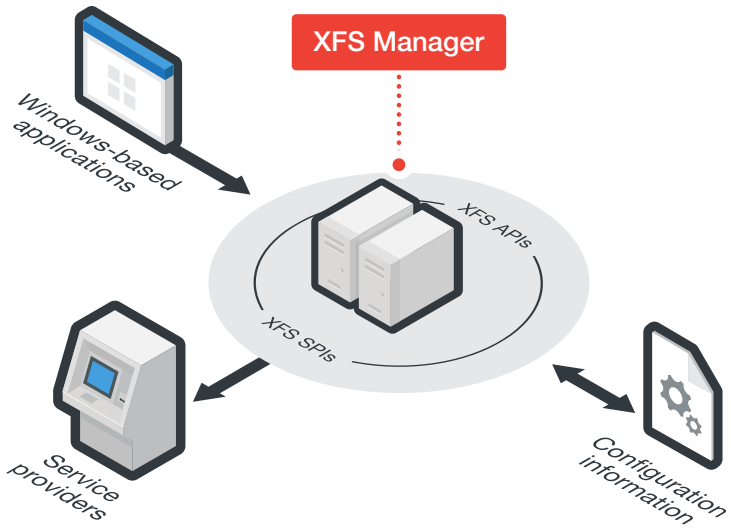


圖 2：XFS 系統架構。

應用程式利用 API 經由 XFS Manager 來取得所需的服務。XFS Manager 將 API 呼叫轉成 SPI 呼叫。SPI 再與周邊裝置溝通，所以應用程式等於利用不同廠牌皆通用的 API 間接透過 XFS Manager 來呼叫 SPI。API 可讓應用程式不須操心裝置間的個別差異與呼叫的動作。這就是為何應用程式不須修改或稍微修改程式碼就能在各家不同製造商的 ATM 提款機上順利執行。

以下是 XFS API 的大致功能[7]：

- **基本功能** — 例如：StartUp/CleanUp (啟動/ 清理)、Open/Close (開啟/ 關閉)、Lock/Unlock (鎖定/ 解鎖) 以及 Execute (執行) 都是所有 XFS 裝置/ 服務皆具備的功能。
- **管理功能** — 例如：裝置初始化、重設、暫停、繼續。這些功能也用於裝置和服務管理。
- **特殊指令** — 用於請求有關某裝置/服務的資訊，以及啟動裝置/服務的特殊功能。這些會以 GetInfo 和 Execute 等基本功能的參數形式傳送至裝置/服務。

SPI 會盡可能對應 API。還有某些指令是針對 XFS Manager 的特殊指令，因此不會對應至 SPI。

攻擊模式：先感染、後擊破

ATM 惡意程式作者感染 ATM 提款機有兩項主要目的：

- 第一是掏空金庫內的現鈔，俗稱「中大獎」(Jackpotting)，同時也是 ATM 惡意程式最顯而易見的目的。
- 第二是竊取提款機中的提款記錄，裡面有金融卡資料。此時惡意程式就如同虛擬的磁條盜拷裝置一樣。

而且這兩項目的不相違背，因此可以同時進行，許多惡意程式也確實兼具這兩種功能。前面提過，歹徒只有兩種攻擊 ATM 提款機的方式。其一是實際打開提款機外殼，然後將裝置連接到主機板；其二是透過銀行內部網路來感染提款機。如果是從內部網路來感染提款機，駭客就必須能夠進入 ATM 的 VPN 網路或特定網段。

不管是哪一種方式，歹徒之所以能夠成，可能性有兩種：

- 駭客熟悉銀行內部運作，或者有內賊協助，才知道如何進入網路，或解除機器的硬體保護。
- 歹徒利用通用的萬能鑰匙來打開機殼，這樣就能接觸到內部。這方法並非天方夜譚，很多公共場所的硬體設施經常使用一般的鎖來防止路人開啟。這類簡易的鎖，通常用於一些較為無關緊要、不須特殊

安全戒備的設施。但若用在 ATM 提款機上，顯然就太過輕忽竊盜的風險，所以才會讓有心的駭客輕易進入內部。

駭客一旦進入提款機內部，就能透過 USB 連接埠或 CD/DVD 光碟機，使用含有惡意程式的隨身碟或光碟來將提款機重新開機。重新開機之後，提款機就成了駭客的囊中之物。接著，駭客會掛載提款機的檔案系統，將惡意程式複製到提款機上，然後修改作業系統來讓惡意程式在下次重新開機時自動啟動。接著，提款機正常重新開機之後，惡意程式就會開始運作，並且能夠操作相關的硬體，例如：數字鍵盤、讀卡機以及盛裝各種不同面額現鈔的鈔票箱。整個過程大約只需不到 10 分鐘。

本文所描述的惡意攻擊有別於所謂的「黑箱式」(black box) 攻擊。在黑箱式攻擊當中，歹徒是將吐鈔機與 ATM 提款機分離，然後再接上另一部電腦，然後對吐鈔機下達吐鈔指令。這兩種攻擊，歹徒都是直接操作 ATM 提款機的硬體。最大的差別在於，黑箱式攻擊不須用到惡意程式，因此防範的方式就會截然不同。

圖 3：舊式使用硬體設備來盜拷卡片磁條資料的攻擊方法[8]。

ATM 惡意程式臨機攻擊

第一種 ATM 惡意程式攻擊使用的是之前常見的舊式 ATM 惡意程式，不過多年來駭客已做了不少改進。近來出現的一些較新的惡意程式家族也屬於這一種，後面會再討論到。

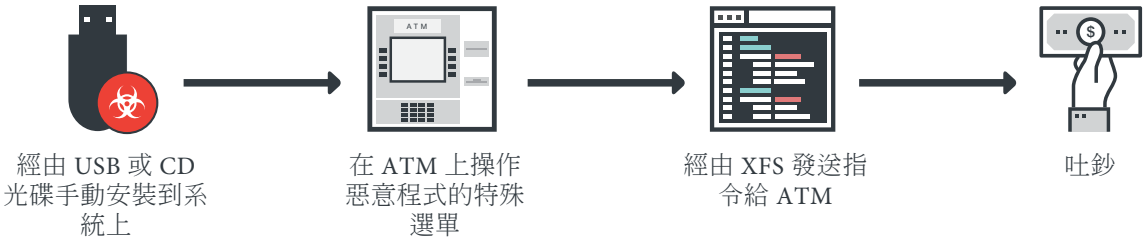


圖 4：傳統的 ATM 惡意程式臨機攻擊程序。

Skimer：目前已知的第一個 ATM 惡意程式

Skimer 是目前已知第一個專門攻擊 ATM 提款機的惡意程式，首次有人討論是在 2009 年三月的一篇 SophosLabs 部落格文章，而且被認為是專門用來盜拷 ATM 金融卡的惡意程式[9]。然而 Skimer 可能早在 2007 年 7 月就已存在，它曾被發現用於攻擊俄羅斯和烏克蘭境內的 ATM 提款機[10]。它只針對 Diebold® 公司所生產的 ATM 提款機，該公司證實 Skimer 的感染案例並未涉及網路層級的安全入侵。換句話說，此惡意程式是手動植入到 ATM 上[11]。

近期的 ATM 惡意程式家族都會直接或間接透過 XFS 中介軟體來操作 ATM 周邊裝置，如：吐鈔機、數字鍵盤、收據列印機。但 Skimer 卻是透過 Diebold 的一個客製化中介軟體 (功能類似 XFS) 來操作 ATM 的周邊裝置。不確定是否所有 Diebold 生產的提款機還是只有較老的機型才使用客製化中介軟體。此外，也不確定 Diebold 客製化中介軟體是否會呼叫 XFS。

目前在外流傳的 Skimer 有兩種：Skimer v2009 會讀取使用者在數字鍵盤上輸入的資料，還會吐鈔並蒐集提款機的交易資料。Skimer v2011 是 v2009 的精簡版，只會蒐集資料。直到今天，兩種 Skimer 變種都仍受犯罪集團青睞。

重點整理：

- Skimer 很可能是經由臨機方式透過 USB 或可開機 CD 光碟植入 ATM 提款機內。
- 目前已知在外流傳的 Skimer 變種有 v2009 和 v2011 兩種。
- Skimer v2009 會讀取使用者在數字鍵盤上輸入的資料，還會吐鈔並蒐集提款機的交易資料。此外，它在吐鈔之前會要求輸入一個授權碼。因此，操作 ATM 的車手必須先從掌控 Skimer 的犯罪集團取得這個授權碼。
- Skimer v2011 是 Skimer v2009 的精簡版，只會蒐集資料。它會將蒐集到的資料寫成記錄檔 (log)，然後用 RC4 演算法將這些檔案加密。車手必須使用一張「主控」(master) 卡來認證惡意程式。此外，也用來讀取惡意程式竊取盜的金融卡資料。
- 犯罪集團目前仍在使用這兩個 Skimer 變種。

Ploutus：對 ATM 瞭若指掌的專家

Ploutus 專門攻擊 NCR® 公司所生產的 ATM 提款機。Ploutus 最早是在 2013 年 9 月由資安廠商 SafenSoft 所發現，當時有墨西哥境內的 ATM 提款機遭到此惡意程式攻擊[12]。

就在該惡意程式被發現後一個月，又出現了一個採用模組化架構的 Ploutus 進階變種[13]。這個新的變種命名為 Ploutus.B，此變種採用了三個不同的模組，因此在偵測上比單一惡意程式更加困難。而此次重新設計也讓惡意程式的功能進一步擴充。在一些較近期的感染案例中，ATM 機殼內甚至被安裝了一台手機。這台手機用來接收提款指令的簡訊，然後將指令傳送給 Ploutus.B 惡意程式，這樣就可以盡量減少領錢的車手操作提款機的步驟。

撰寫 Ploutus 的作者似乎對 NCR 生產的 ATM 提款機瞭若指掌，也對這方面的軟體開發相當有經驗。但是，在 2016 年 10 月，一個名為 Ploutus.C 的新變種又再度出現，增加了可入侵並操控某跨廠牌 ATM 管理軟體架構的能力。

2017 年 1 月又出現了另一個新的版本叫做 Ploutus.D，增加了一個從遠端管理 ATM 的模組。這項新的功能或許在媒體上噱頭十足，但實務倒是意義不大。因為像這類的功能，(以及 Ploutus.B 可接收簡訊的功能) 只是讓第二波的吐鈔行動更方便而已，但實際上，根據我們訪問過的銀行發現，他們在發現某台 ATM 遭到

攻擊之後便會立即停用該台提款機。此時，提款機將被離線進行鑑識分析。除非歹徒所攻擊的銀行採取的政策不同，不然安裝一個硬體在提款機內來方便發動第二波攻擊，只是讓犯罪調查人員掌握更多線索而已。

這裡給我們的啟示是，Ploutus 目前仍相當活躍，不斷衍生出新的版本。從新增的功能可以看出，網路犯罪集團相當熟悉 ATM 提款機以及銀行的內部環境，因此他們的攻擊都相當有針對性。

重點整理：

- 原本第一代的 Ploutus 惡意程式當中有些西班牙文的字串，後來在第二版時都已翻譯成英文。有些資安專家認為這很可能意味著 Ploutus.B 也應用在其他國家。
- 撰寫 Ploutus 的作者似乎對 NCR 生產的 ATM 提款機瞭若指掌，也對這方面的軟體開發相當有經驗。
- Ploutus 的首次感染應該是經由一張可開機的 CD-ROM 光碟。歹徒很可能是經由開鎖方式或使用鑰匙來打開 ATM 外殼，然後再插入一張含有 Ploutus 惡意程式的 CD-ROM 光碟。
- 最原始的 Ploutus 惡意程式需要一個八位數的啟動碼。車手在利用 Ploutus 來提款之前，必須先輸入該啟動碼。這是一項控管手段，讓車手到提款機領錢時，必須先打電話回犯罪集團以取得啟動碼才能提錢。
- Ploutus.B 需要一個 16 位數的代碼來啟動，如果輸入錯誤，惡意程式會休眠 500 分鐘，如果重複輸入錯誤，惡意程式將永遠失效。這又是另一個安全控管手段。
- Ploutus.B 一旦收到正確的啟動碼之後會有 24 小時的活動時間。車手只能在這段 24 小時期間提款，之後就要再次輸入啟動碼。如果過了這段期間，Ploutus 就不會吐鈔，並且會列印錯誤訊息。
- Ploutus 可從提款機的數字鍵盤或是外接的鍵盤接收使用者輸入。而 Ploutus.B 則僅能從 ATM 數字鍵盤接收輸入資料。
- Ploutus.B 無法指定吐出來的鈔票張數。惡意程式會先檢查每一個鈔票箱內的鈔票數量，然後將第一個鈔票數量 40 張 (含) 以上的鈔票箱吐光。每次接收到新的吐鈔命令時都會重複這樣的流程。
- 較新的 Ploutus 版本 (Ploutus.C 和 Ploutus.D) 每次都新增特別針對特定情況或特定銀行的功能。這顯示惡意程式的發展非常活躍，同時，犯罪集團對其鎖定的銀行研究非常透徹。

Padpin-Tyupkin：暗夜行者

Padpin 是由 Symantec 在 2014 年 5 月首次發現。此惡意程式家族偷遍了歐洲和東南亞地區，得手金額高達數百萬美元[14、15]。隨後在 2014 年 10 月，Kaspersky Labs 又發現了另一個新的版本，取名為 Tyupkin[16]。據專家對其程式碼的分析以及 ATM 製造商 NCR 的確認，Padpin 和 Tyupkin 兩者都是從相同的基礎程式碼衍生而來[17]。

重點整理：

- Padpin 專門攻擊 NCR 所生產且安裝有 McAfee® Solidcore 軟體的 ATM 提款機。
- Padpin 是經由可開機的 CD-ROM 光碟機安裝到 ATM 提款機上。最可能的方式是打開 ATM 提款機外殼的鎖，直接進入內部利用可開機光碟感染 ATM 系統。
- Padpin 會接收 ATM 提款機數字鍵盤的輸入，歹徒就能從數字鍵盤操控該惡意程式。
- 在預設情況下，Padpin 會在每週日和週一凌晨 1:00 至 5:00 之間活動，表示其幕後的犯罪集團都是在夜間行動以避人耳目。
- Padpin 可讓犯罪集團的車手直接從 ATM 提領現金，而且會利用啟動碼來確保車手必須在犯罪集團監控之下才能領錢。

GreenDispenser：具備自我毀滅功能的惡意程式

GreenDispenser 是美國資安廠商 Proofpoint 在 2015 年 9 月發現的一個 ATM 惡意程式家族，專門攻擊墨西哥境內的 ATM 提款機[18]。不過早在 2015 年 9 月，病毒分析機構 VirusTotal 就曾經收到來自印度和墨西哥的 GreenDispenser 惡意程式樣本。然而就現有證據來看，兩國之間的 GreenDispenser 並無關聯。有可能是網路犯罪集團將惡意程式的開發外包給印度的程式設計師，但目前並無進一步的證據。

重點整理：

- GreenDispenser 惡意程式只在 2015 年 1 月 1 日至 8 月 31 日之間才會執行。我們分析到的樣本是專為特定一段期間的行動所開發。
- 感染 GreenDispenser 的提款機，螢幕上會出現一個錯誤訊息畫面，上面寫著：「We regret this ATM is temporary out of service」(很抱歉，這台提款機目前暫停服務)。因此，一般人將無法使用受感染的提款機。
- GreenDispenser 並不會專門鎖定特定廠牌的 ATM 提款機。它可感染任何使用 XFS 中介軟體的 ATM 提款機。

- GreenDispenser 的車手在提款之前，需經過兩階段認證才能進入吐鈔選單。
- 第一道認證金鑰用來關閉錯誤訊息畫面。錯誤訊息關閉之後，GreenDispenser 就會顯示一個新的畫面，上面有一個 QR code 和一些選單項目，並寫著：「Enter second key. Press 9 to pause, 8 to permanently delete.」(輸入第二道鑰。按 9 來暫停，按 8 來永久刪除。)
- 第二道認證金鑰是透過 Windows 內建的加密功能所產生。QR 所顯示的就是加密過的第二道金鑰。
- 負責提款的車手，必須掃描螢幕上的 QR code，然後利用一個特殊的應用程式來解出裡面的金鑰，不然就必須聯絡幕後的犯罪集團來解開金鑰。車手必須在提款機的數字鍵盤上輸入解開後的第二道金鑰，才會進入吐鈔選單。
- 每次吐鈔之後，畫面上就會顯示提款機內還剩多少現鈔，GreenDispenser 假設提款機內只有一種面額的現鈔。
- GreenDispenser 還精心製作了一個解除安裝程序，可清除所有感染的痕跡。當 GreenDispenser 徹底清除之後，ATM 提款機就會完全恢復正常作業。
- GreenDispenser 可能是經由銀行的不肖人員或犯罪集團成員手動安裝到 ATM 提款機內。

Alice：專門掏空金庫

趨勢科技是在 2016 年 11 月期間與 Europol EC3 合作進行研究時首次發現 Alice ATM 惡意程式。我們已經蒐集了一系列的雜湊碼，也從 VirusTotal 取得了對應這些雜湊碼的檔案來進行深入分析[19]。

我們原先以為其中一個檔案是 Padpin 惡意程式家族的新變種。不過在經過逆向工程之後，我們發現這是一個全新的家族，因此我們將它命名為「Alice」。

Alice 有幾個特點。首先，它的功能非常陽春，不像我們分析過的其他 ATM 惡意程式，它僅有一些用來掏空 ATM 金庫的基本功能。Alice 只會操控提款機內的吐鈔機，並不會用到數字鍵盤。合理的推測是，使用 Alice 惡意程式的犯罪集團打算實際打開 ATM 提款機的外殼，然後經由 USB 或 CD-ROM 來感染提款機，然後再連接一個鍵盤到提款機的主機板來操作惡意程式。

另一種可能是開啟一個遠端桌面，然後經由網路遠端操作選單，就像泰國發生的駭客攻擊與其他近期案例。但是，我們並未看過歹徒以這樣的方式使用 Alice。由於 Alice 在吐鈔之前必須輸入一個密碼，這表示

歹徒必須親臨提款機來發動攻擊。而且 Alice 也沒有複雜的安裝或解除安裝機制，歹徒只要在適當的環境將它執行起來即可。

Alice 的用戶認證機制與其他 ATM 惡意程式類似。車手必須從犯罪集團收到密碼才能進行提款。車手要先輸入第一道指令來植入清除腳本，接著再輸入個別提款機的密碼，才會進入吐鈔畫面。每個惡意程式樣本的密碼都不相同，這樣可以防止車手將密碼提供給他人以避開犯罪集團掌控，同時可追蹤個別車手。在我們拿到的樣本中，密碼只有四位數，不過長度倒是可以輕易更改。如果車手試圖猜測密碼，惡意程式會在密碼輸入錯誤一定次數之後自我毀滅。

由於 Alice 專挑採用 XFS 中介軟體的提款機，而且不會特別偵測什麼的硬體，我們認為它應該可以在任何使用 Microsoft XFS 中介軟體的提款機上執行。

重點整理：

- Alice 是一個功能非常陽春的 ATM 惡意程式，其目的只有掏空提款機內的現鈔。
- Alice 可直接執行而不需安裝程序。
- Alice 需要外接一個鍵盤來輸入指令。
- Alice 可在任何廠牌的 ATM 提款機上執行。

ATM 惡意程式網路攻擊

ATM 惡意程式攻擊的第二種型態是經由網路來進入 ATM。根據我們從各種不同已知攻擊事件所觀察到的結果，駭客有時只需一封針對銀行員工的網路釣魚郵件，就有辦法進入銀行的內部網路。雖然這並非進入銀行內部網路的唯一途徑，但卻是最簡單的方式，因此也最為常見。

駭客一旦進入銀行內部網路，就可以開始四處遊走，找尋 ATM 所在的子網路。正常來說，銀行都會將自己的內部網路與 ATM 網路隔離，使用不同的路由器和防火牆，或是其他防護措施。然而有些銀行卻採用單一網路，因此，駭客就能很輕易地得逞，但這畢竟是少數。

以下我們將討論五起曾經在媒體上披露的攻擊事件：

- 2016 年 7 月台灣第一銀行 ATM 盜領事件
- Cobalt Strike
- Anunak/Carbanak
- Ripper
- ATMitch

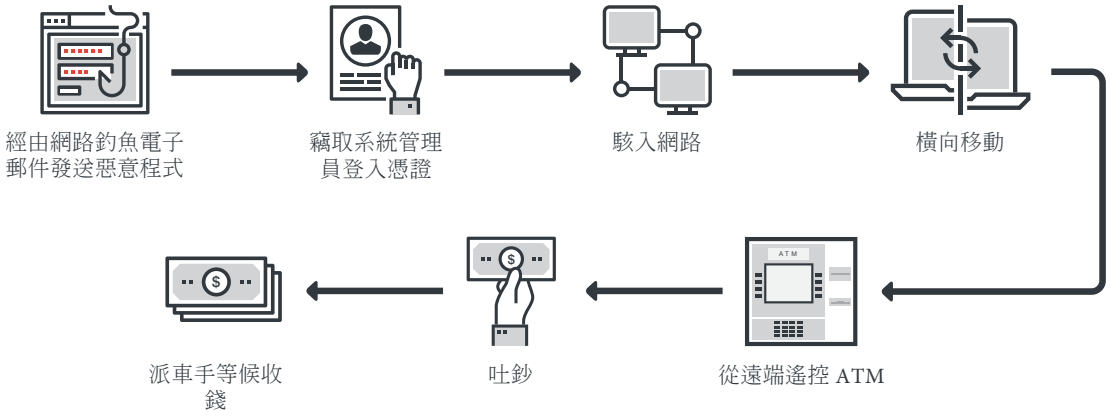


圖 5：ATM 惡意程式網路攻擊的一般流程。

台灣第一銀行 ATM 盜領事件：一場精心策劃的攻擊

2016 年 7 月初，台灣第一銀行 22 家分行共 41 台由 Wincor Nixdorf® 所生產的 ATM 提款機遭歹徒盜領 8,000 萬台幣。歹徒完全沒有用到金融卡，也沒有用到提款機上的數字鍵盤[20]。一開始，銀行並未公布歹徒所使用的 ATM 惡意程式，不過銀行倒是緊急暫停了 1,000 台同一型提款機的提款功能，直到問題解決為止。歹徒最後也遭到逮捕，而大部分的款項也都追查回來，不過直到 9 月中，台灣警方與法務部調查局才公布其聯合調查的結果。結果中顯示，歹徒策劃了一場相當精密的網路攻擊。根據 iThome 雜誌內容所描述，歹徒的攻擊過程如下：

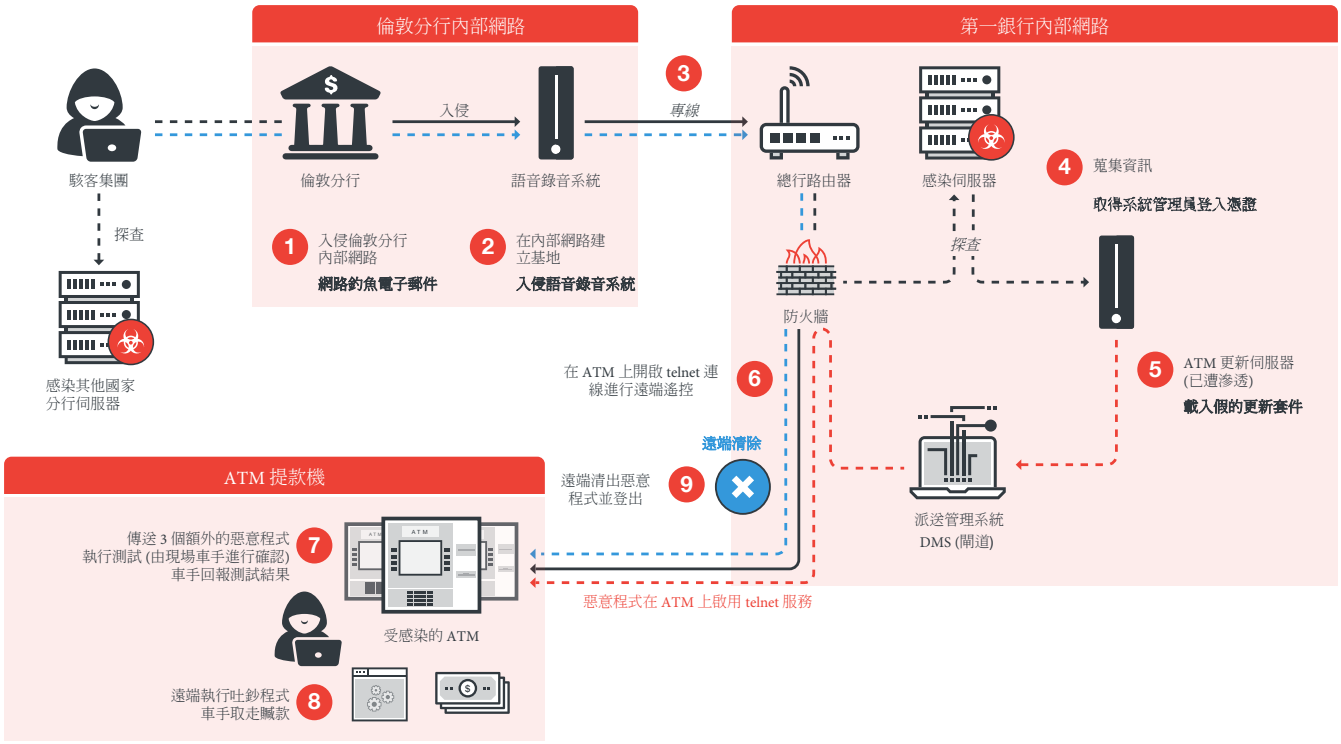


圖 6：台灣第一銀行 ATM 盜領事件過程示意圖。

1. 儘管銀行網路一開始遭到入侵的地點在國外，但實際攻擊時發動的地點也是從倫敦分行開始。
2. 駭客在入侵了倫敦分行網路之後，接著就駭入該銀行的語音錄音系統，並竊取了網域管理員的帳號登入憑證。
3. 有了這組憑證，駭客接著利用 VPN 經由銀行專線進入台灣總行，穿過了路由器和防火牆，並掌握了台灣總行內部網路的某些伺服器。
4. 經由這些伺服器，駭客就能找出銀行內部網路的架構。他們發現了 ATM 更新派送系統，並取得了該系統管理員的登入憑證。
5. 駭客接著登入 ATM 更新伺服器，並且在更新派送管理系統上安排了一份假的更新套件。接著，更新套件上傳至 ATM 提款機上。此套件會啟用 ATM 提款機上的 telnet 服務。
6. 一旦 telnet 服務啟用之後，駭客就能經由 telnet 連線從遠端遙控 ATM 提款機。

7. 接著，駭客上傳了三個程式到幾台特定的提款機測試吐鈔口是否會正常打開，並且派車手到現場確認。車手在提款機前透過手機上的 Wickr Me 安全即時通訊軟體，將測試結果回報給遠端駭客。
8. 在確認沒問題之後，駭客會上傳一個被修改過的廠商測試工具，一次可吐 40 張鈔票。(基於硬體設計上的限制，這已是吐鈔機一次可吐的上限。) 車手會負責在提款機前收取吐出來的鈔票，得手之後，就繼續前往下一台提款機，然後重複同樣的流程。
9. 此時，遠端的駭客就負責清除 ATM 提款機上的所有惡意程式，並且登出。

這起攻擊事件具體展現了駭客如何經由銀行的內部網路來入侵 ATM 提款機。在這起案例當中，歹徒的策劃相當嚴密，因此他們不僅能在每台提款機上安裝他們想要的軟體 (光這點就足以掏空提款機)，而且還有辦法從遠端 telnet 遙控。

Cobalt Strike：資安軟體也遭利用

接下來我們要討論的案例叫做 Cobalt Strike，由當初發現的資安廠商 Group-IB 所命名[21]。根據該公司所發表的報告，駭客集團先利用網路釣魚郵件發送含有漏洞攻擊程式以及含有惡意執行檔的加密壓縮檔給某一俄羅斯銀行的員工們。該報告指出，駭客使用了一個名叫「Cobalt Strike」的資安軟體來入侵目標網路，因此才將這起案例取名為「Cobalt Strike」。此軟體是一套白帽駭客經常使用的合法滲透測試工具，用來評估客戶的網路安全狀況。此外，駭客還使用了 Mimikatz 這個軟體來入侵目標的網域和本地端帳號。一旦駭客滲透網路並且取得適當的登入憑證，就會開始尋找能夠經由遠端桌面 (RDP) 來管理 ATM 提款機的銀行員工。當駭客有辦法進入 ATM 提款機後，就會從遠端登入提款機並上傳他們所需的軟體。他們用來吐鈔的程式是一個自製的執行檔，可透過 XFS 來操作 ATM 的吐鈔機。

根據 Group-IB 的報告，歹徒在盜領時有兩種手法：第一種是由車手站在提款機前，等候遠端駭客觸發惡意程式讓提款機吐鈔。第二種是由車手來觸發，車手會從手機接收到一個六位數的密碼，輸入密碼就能觸發惡意程式讓機器吐鈔 (做法類似 Skimer、Ploutus、GreenDispenser 等等)。這兩種手法所牽涉的犯罪組織架構截然不同，**由於無法經由公開管道取得這些 ATM 上的惡意程式樣本，因此這方面我們無法做任何進一步的分析。**

同樣地，駭客同樣是先駭入銀行的內部網路，然後再進入 ATM 提款機網路。在此案例當中，該銀行是透過遠端桌面來管理 ATM 提款機，所以看來這是歹徒用來入侵的管道。

Anunak/Carbanak：從網路釣魚到橫向移動

這起案例與上一個非常相似，而且受害的也是俄羅斯的銀行。Group-IB 和 Kaspersky 皆曾經從不同角度來說明這起攻擊事件。由於 Group-IB 同時分析了這起攻擊和 Cobalt Strike 攻擊，並且認為 Cobalt Strike 和 Anunak/Carbanak 兩者不同，因此我們認為這兩起攻擊應該是由不同駭客集團所為。由於我們並未參與這兩起事件的應變行動，因此掌握到的資訊不如這兩家公司完整，所以也無法反駁他們的說法，只不過從他們所發表的報告來看，兩起攻擊似乎有相當雷同之處。

Anunak/Carbanak 一開始是利用網路釣魚郵件與網站漏洞攻擊套件來感染使用者電腦。一旦感染到一台具備本地端管理權限的電腦，駭客就能利用密碼破解軟體 (如 Mimikatz)，在網路內入侵更多電腦。駭客可在銀行內部網路四處遊走並操控其他伺服器，然後利用這些伺服器來找出網域系統管理員的登入憑證，最後駭入網域控制器。進入網域控制器之後，駭客就能找出內部網路的各個網段，以及哪些電腦用來管理 ATM 網路。根據 Kaspersky 的報告，接下來駭客從遠端登入 ATM 提款機，並且上傳軟體到提款機上執行[22]。駭客用來吐鈔的軟體是從 ATM 廠商的測試工具修改而來。負責領錢的車手同樣也是必須到提款機前等候提款機吐鈔。不過不像上次的案例，此事件的報告當中多了不少關於這項工具的資訊，Group-IB 的報告還附上幾張螢幕抓圖[23]。該程式並非 ATM 惡意程式，而是一個由 Wincor Nixdorf (目前已改名 Diebold Nixdorf®) 公司所撰寫的文字模式介面吐鈔測試工具修改而來的程式。

這起攻擊與 Cobalt Strike 攻擊案例幕後的駭客集團是否相同並不重要。重要的是，駭客有辦法先駭入銀行的內部網路，然後再找到並入侵 ATM 網路。在兩起案例當中，駭客都是經過一番監視與探查之後，就能找到隔離的 ATM 網路，並竊取到適當的管理員登入憑證，然後就能從遠端安裝軟體到 ATM 提款機上執行。

Ripper：大量吐鈔的範例

2016 年 7 月和 8 月，泰國曼谷的政府儲蓄銀行 (Government Savings Bank，簡稱 GSB) 位於曼谷總行的 NCR ATM 提款機遭駭客攻擊，裡面的現鈔被提領一空[24]。駭客使用了一個新的 ATM 惡意程式，名為「Ripper」。

根據 NCR 的說法，駭客應該是先駭入銀行的內部網路，然後再假冒 InfoMindz 公司的 Software Distribution and Management System v2.3.0 這套軟體派送管理系統來將惡意程式安裝到 ATM 上[25]。當車手到提款機前取款時，會使用一個修改過金融卡來通過提款機上的 Ripper 惡意程式認證，然後將提款機內高達 40,000 泰銖 (約合 1,160 美元) 的鈔票提領一空。

Ripper 與前面幾個 ATM 惡意程式 (如 Padpin 和 GreenDispenser) 都有一些共同的功能，它們都能停用提款機的網路卡以防止銀行即時防盜系統發現，而且還能刪除提款機上的攻擊痕跡，讓鑑識分析更加困難。我們所分析到的樣本並未開啟停用網路卡的功能，但既然程式碼已經存在，所以歹徒應該有打算使用這項功能，或者過去已經用過，只是後來因為不需要才停用，不過這一切都只是揣測。Ripper 也有能力感染 Diebold 和 Wincor Nixdorf (現已合併為 Diebold Nixdorf) 的 ATM 提款機，因為它是透過 XFS API 與硬體溝通，因此無須修改程式就能操控三家不同廠商的吐鈔機。另一個有趣的現象是，負責在 ATM 前取款的車手，必須使用一個特製的晶片金融卡來通過 Ripper 的認證 (這一點與 Skimer 類似)。

這起攻擊特殊的地方在於它經由銀行內部網路進入 ATM 網路來安裝 ATM 惡意程式。這是第一個不須實際打開提款機外殼就能感染提款機的案例。由於現在銀行和廠商都開始在加強提款機的安全措施以避免歹徒進入提款機內部，我們認為 ATM 惡意程式的作者將開始朝著網路攻擊的型態發展。

除此之外，值得一提的是，在這一波新式的 ATM 攻擊當中，銀行最脆弱的環節反倒不是實體保全與離線防禦機制。要保障 ATM 提款機的安全，銀行更需要的是線上防禦機制，也就是：防火牆、白名單機制以及其他 ATM 提款機上所安裝，用來監控日常作業系統與應用程式執行的監控軟體。

另一項觀察結論是，歹徒通常都是先利用包含社交工程技巧的網路釣魚郵件來進入銀行內部網路。因此，整個攻擊過程當中最脆弱的環節是銀行的人員，尤其是那些可能點選惡意連結或開啟惡意附件執行檔的人員。

ATMitch：從鍵盤和文字檔案讀取指令

ATMitch 是由 Kaspersky 於 2017 年 4 月處理俄羅斯一樁銀行攻擊案例時首次發現。由於他們只找到了動態連結程式庫 (DLL)，因此我們或許並未掌握整起攻擊的完整樣貌。不過我們倒是掌握了兩點新發現：第一，此惡意程式似乎並無使用者操作介面，因此駭客只能經由鍵盤輸入指令。第二，我們也從其他可靠來源得知，此惡意程式還可接受一個文字檔作為輸入，然後從文字檔內讀取指令。不過這檔案如何提供給程式就不得而知，因此我們無法判定這個方法的確切運作方式。

假設 ATMitch 惡意程式是用於臨機攻擊，那麼駭客必須完全掌控整台提款機才行，不是打開外殼然後外接一個鍵盤，就是將整台提款機運走，帶回去慢慢破解。後者不太可能，因為 Kaspersky 的報告指出惡意程式是從遭到攻擊的銀行當中找到的。

所以，最可能的情況是，惡意程式經由銀行網路安裝到提款機上，然後直接從遠端發送指令給吐鈔機[26]，並且叫車手到 ATM 前面等著取款。尤其 ATMitch 並未設計任何認證機制來防止車手黑吃黑，私自到每一台提款機偷領，因此這樣的推測相當合理。

重點整理：

- ATMitch 僅是整起攻擊當中所用到的一個元件。在缺乏其他塊拼圖的情況下，很難掌握的攻擊的完整樣貌。
- ATMitch 只能透過一般的鍵盤來操控，或從一個傳送至系統上的文字檔中讀取指令。
- ATMitch 並無防止車手黑吃黑的認證機制。
- ATMitch 支援 XFS，因此任何 ATM 提款機都通吃。
- ATMitch 沒有任何選單或使用者操作介面，駭客必須知道如何輸入指令。
- ATMitch 很可能只是整體銀行網路攻擊的其中一個環節。

其他值得注意的 ATM 惡意程式攻擊

NeoPocket：鎖定目標攻擊

NeoPocket 是一個資訊竊取程式，專門針對 Diebold 生產的 ATM 提款機所設計。NeoPocket 是 2014 年 4 月由網路資安廠商 S21sec 所發現[27]。NeoPocket 有別於絕大多數的 ATM 惡意程式，其目標是 ATM 提款機內的交易資料，而非鈔票。它是藉由中間人 (MitM) 攻擊的方式來竊取提款機內的交易資料並且側錄特定應用程式視窗內收到的使用者輸入。犯罪集團偷到的資料，可拿到深層網路的地下市集上販賣、用來製作偽卡，或將受害者帳戶上的錢匯走。由於提款機內的錢不會減少，因此不易被發現，所以經常可以長期潛伏，這樣一來犯罪集團就能蒐集大量的敏感資料。

NeoPocket 是一種非常具有針對性的攻擊，因為本質上是針對特定目標。歹徒非常熟悉目標提款機的安全措施，而且，惡意程式在執行時也只需很短的時間，執行完就會自行清除所有痕跡。由於它的最終目標是竊取機器上的金融卡交易資料，因此銀行的資安人員通常不會發現，因此反而更加危險。這類威脅非常難以防範，同時也顯示犯罪集團在銀行當中應該有內應。

重點整理：

- 這起中間人攻擊成功的第一要件就是要熟悉 Diebold Agilis® 軟體並了解系統架構。
- 由於提款機內的錢不會減少，因此不易被發現，所以經常可以長期潛伏，這樣一來犯罪集團就能蒐集大量的敏感資料。
- NeoPocket 在過了某個日期之後就不會執行。該日期之後，惡意程式會終止但不會自行解除安裝。

- 就像其他 ATM 惡意程式一樣，NeoPocket 也需要安裝金鑰。這麼做可以讓駭客追蹤並控管它所感染的 ATM 提款機數量，防止集團底下的車手私下將該程式安裝到任意提款機並蒐集交易資料。
- NeoPocket 是經由手動方式安裝到 ATM 提款機上。駭客必須使用鍵盤在畫面上顯示的安裝視窗內輸入安裝金鑰。NeoPocket 不會與提款機的周邊裝置溝通，也不會用到提款機的數字鍵盤。
- NeoPocket 會側錄使用者在某些視窗內輸入的內容，該視窗的標題包括「Enter the 'A' key」、「Escriba la clave 'A'」…等等。至於這些視窗內所輸入的資訊為何，以及如何輸入 (透過外接鍵盤或 ATM 數字鍵盤) 就不得而知。有趣的一點是，NeoPocket 所檢查的視窗標題包含了英文和西班牙文。
- NeoPocket 具備了一個終止「SMC.exe」這個執行程序的功能，這是 Symantec Endpoint Protection 軟體的執行程序。我們認為 NeoPocket 鎖定的目標應該是拉丁美洲的某些金融機構。因為其文字當中含有西班牙文「ingresar」這個動詞，因此顯然惡意程式是來自拉丁美洲，而非西班牙，因為只有拉丁美洲在這個情況下才會使用這個字，西班牙不會。除此之外，我們也私下向 S21sec 公司確認，其蒐集到的樣本也是來自該地區。
- NeoPocket 執行時會從機器連接的 USB 裝置接收指令。惡意程式採用非傳統的方式經由 USB 裝置接收使用者的指令。

Suceful：駭客測試工具

Suceful 是一個 ATM 惡意程式原型開發工具，由美國網路資安廠商 FireEye 於 2015 年 9 月首次在部落格上披露[28]。VirusTotal 在 2015 年 8 月 28 日收到兩個 Suceful 的樣本，其中一個是從法國上傳，另一個則來自俄羅斯。不過，上傳 VirusTotal 的來源國家可以透過 VPN 服務來造假，因此確切的來源還是無法確定。

在參考 Ploutus 和 Padpin-Tyupkin 等其他 ATM 惡意程式的報告之後，看來 Suceful 應該是一個新的 ATM 惡意程式家族。仔細分析過程式碼之後，我們推測 Suceful 實際上應該是一個原型開發工具，而非真正用來攻擊 ATM 提款機的惡意程式。由於到目前為止都還未有人發現或通報 Suceful 的感染案例，因此我們的推測應該沒錯。犯罪集團很有可能正利用 Suceful 來開發一些目前仍未被偵測到的 ATM 惡意程式。

重點整理：

- 在 Suceful 的使用者操作介面可看到它主要攻擊的是 Diebold 和 NCR 所生產的 ATM 提款機，但程式碼當中卻無專門針對 NCR 提款機的設計。
- 有可能 NCR 的提款機是 Suceful 幕後集團未來鎖定的目標，所以其操作介面才會出現 NCR 字樣的按鈕。

- Suceful 可讀取已插入的金融卡磁條資料。
- Suceful 可從 ATM 提款機的鍵盤接收使用者輸入。
- Suceful 可操控 ATM 提款機的防開啟感應器、警報感應器、通用感應器、鑰匙開關感應器、指示燈、備用指示燈，以及機器額外連接的強化音訊控制器。
- 其操縱感應器與指示燈單元 (SIU) 連接埠的能力表示歹徒很可能會臨機入侵 ATM 提款機。
- Suceful 並不具備使用者存取控管機制，而這一點反而是所有 ATM 惡意程式樣本所共同具備的功能。
- Suceful 當中的吐鈔功能並未經過實測，Suceful 犯罪集團很可能只是想蒐集金融卡資料。
- Suceful 犯罪集團已取得外流的 Diebold Agilis XFS 手冊。

儘管 Suceful 在研究人員首次對外公開時造成了相當大的轟動，但它卻只是一個測試工具，從未曾實際用於攻擊當中。不過，它的確存在著吐鈔以及一些進階的功能，例如：停用與啟用警報器和其他 ATM 特殊硬體，但這似乎是某個惡意程式作者的私人測試功能而已。該工具內可看到一些俄羅斯文字串，這表示它來自東歐國家的網路犯罪組織，應該是因為該組織的一個不小心才會外流到資安研究社群。

此工具對整體 ATM 惡意程式犯罪情勢的意義是，它證明了犯罪集團相當熟悉 XFS 平台所提供的功能，並且非常懂得如何善用這些功能。除此之外，此工具目前並未參與真正的 ATM 攻擊，或許未來有機會。

ATM 惡意程式犯罪集團分析

從前面的幾個 ATM 惡意程式家族及其發源地，我們可以看出一些清楚的模式。其中有兩個比較老舊的 ATM 惡意程式 (Skimer 和 Ploutus) 是來自南美洲，程式內有西班文的字串。這些字串很可能是程式設計師所留下的，因此應該是來自南美洲無疑。Skimer 和 Ploutus 兩個惡意程式一個是專門針對 NCR 生產的 ATM 提款機，另一個是針對 Diebold 生產的 ATM 提款機。

因此有一種說法是兩者都來自同一源頭或近似的源頭，而且其目的就是希望能夠涵蓋市面上絕大多數的 ATM 提款機 (因為市場上第三大 ATM 廠商的提款機不在攻擊之列，而且顯然在該地區也不普遍)。請記住，這些威脅都是在 XFS 中介軟體出現之前，因此開發人員必須分別針對不同的平台撰寫不同的程式碼。唯一沒看到的是一個只會盜取金融卡資料而不會吐鈔的 Ploutus 版本。這樣的版本就算存在，也從未在外流傳。由於只盜取金融卡資料的惡意程式不像會吐鈔的惡意程式那樣容易被察覺，因此有可能隱藏多年之後才被人發現。

不過令人不解的是，Skimer v2009 首次在俄羅斯和烏克蘭被發現。v2009 和 v2011 兩個版本在程式撰寫風格以及它們感染系統與操控 ATM 相關硬體方面顯然有某種程度的關係。很可能原因是，原始程式碼是在東歐開發，然後被拉丁美洲的犯罪集團拿去用，接著再從中演化出只會盜取金融卡資料的版本。

GreenDispenser 是較近期才從該地區竄起的惡意程式。它看起來有點像只會吐鈔的 Skimer 或 Ploutus，只不過可支援多廠牌的提款機。由於 Skimer 和 Ploutus 目前仍舊活躍，因此我們認為，GreenDispenser 應該是出自另一個競爭對手集團，或者是原集團之前的成員自立門戶出來搶生意。

接下來是 NeoPocket，這是一個源自於拉丁美洲的磁條資料盜取程式。我們看不出來 NeoPocket 和前面幾個惡意程式 (Skimer、Ploutus、GreenDispenser) 有任何關連，因為它似乎更有針對性。NeoPocket 比較像是專為攻擊某家銀行而量身訂做，且似乎有內部人員從中協助，不然也有可能整起攻擊都是內賊所策劃。不論如何，它在我們所分析過的惡意程式當中算是獨樹一格。

除上述地區之外，我們發現有另一個犯罪集團來自俄羅斯，或者至少是講俄羅斯語的地區。Padpin 惡意程式應該就是來自這個東歐犯罪集團，而且也率先攻擊俄羅斯和鄰近國家，然後再慢慢拓展至其他東歐國家。我們最近看到一位摩爾多瓦 (Moldovan，原蘇聯共和國成員，現為獨立國協及聯合國會員國) 的駭客因為在英國倫敦及近郊入侵了 50 多台 ATM 提款機而遭到逮捕[29]。這更讓我們相信這個犯罪集團的存在，且其成員似乎已在西歐國家建立一些據點。此外，我們也經由側面消息聽到一些俄羅斯人常出沒的土耳其觀光地區 出現零星的 ATM 盜領事件。這也印證了 Padpin 的背後應該是某個東歐犯罪集團。

至於 Suceful 則可能是這個東歐犯罪集團在開發 ATM 惡意程式 (如 Padpin 或其他還未被發現的木馬程式) 時用來測試和除錯的工具。

接下來，讓我們仔細看一下 2014 年馬來西亞所發生的案例。這起攻擊的幕後集團有好幾種說法，其中可信度較高的有兩種：

1. 有些人認為這起案件是南美洲的犯罪集團所為。因為，攻擊中所用的惡意程式每次可吐 40 張鈔票[30]。這一點和 Ploutus 惡意程式相同，而 Ploutus 就是來自南美洲。其次，有些報告指出，銀行監視系統所拍到的嫌犯看起來像南美洲人[31]。

2. 另一種推測是絕大多數資安廠商發現它跟 Padpin 有關，因此應該是歐洲犯罪集團所為。有些媒體報導認為倫敦落網的那位歹徒也涉及了馬來西亞盜領事件，因為該名歹徒當時人正好在馬來西亞[32]。警方對於此案並未發布官方調查報告，但根據我們所掌握的技術細節，該案最有可能是東歐犯罪集團某個單位利用 Padpin 惡意程式所為。東歐犯罪集團在全球各地與渡假勝地犯案的說法，也符合我們前述所描繪的情況。

2016 年 1 月 5 日，羅馬尼亞執法單位 DIICOT 破獲了一個使用 Padpin 惡意程式在羅馬尼亞/摩爾多瓦地區盜領 ATM 提款機的犯罪集團[33]。這又是另一起該集團所犯的案例之一，至於這些歹徒是自行開發了 Padpin，或是從其他集團取得該程式，就不得而知。

目前，由於全球商業銀行的網路資安措施普遍不足，因此網路犯罪集團已改弦易轍，紛紛從舊式的臨機攻擊升級成利用 ATM 惡意程式來盜取金融卡資料。這樣的情況在拉丁美洲和東歐已經相當普遍，而且歹徒還在將這樣的手法輸出到其他國家。

圖 7：重大 ATM 惡意程式攻擊事件時間表。

如上所述，我們已經看到 ATM 網路攻擊開始逐漸興起，歹徒不是使用自行開發的惡意程式，就是利用提款機廠商所開發的測試工具來讓機器吐鈔。這些網路攻擊都有一個共通點，那就是全都源自於東歐。

目前全球 ATM 犯罪的情勢大致上就像拉丁美洲的情況，歹徒仍在使用自行開發的惡意程式，例如 Ploutus 近期才又推出新的版本。

另一方面，東歐的犯罪集團則採用兩種獲利模式。第一種是 Padpin 作者所採用的方式，也就是將其開發的惡意程式賣給較小的犯罪團體，這些團體再到全球各地發動迅雷不及掩耳的攻擊，通常會選在某個週末。

東歐犯罪集團最近浮上檯面的第二種手法是雇用駭客來入侵銀行的內部網路，然後再找到 ATM 網路並加以滲透，進而感染 ATM 提款機，此手法與 Padpin 犯罪集團的犯案模式截然不同。Ripper 犯罪團體則是巧妙地融合兩種手法，Ripper 是第一個經由網路來感染的 ATM 惡意程式。從這個惡意程式缺乏使用者認證機制就可看出，程式的開發者與實際作案的歹徒是同一批人。我們認為這樣的作法將開創先例。

另外值得一提的是，Padpin 惡意程式犯罪集團非常積極地販售他們的惡意程式。這批人不僅在地下市場上提供惡意程式，更提供如何利用該程式來感染 ATM 提款機的指示說明。為了不洩漏自己的身分，他們大多經由 Tor 洋蔥路由器網路來經營。

同樣類似的情況，Ploutus 背後的作者 (或是某個宣稱擁有原始程式碼的人) 也是靠販售程式來賺錢。這些人或許並非最初的作者，因為作者並未提供完整的說明，因此販賣的人必須自己搞清楚惡意程式如何運作。也有可能他們刻意說謊，試圖引誘他人踏入這一行。不管怎樣，眼前的狀況就是 ATM 惡意程式在犯罪圈內的名聲越來越響亮。

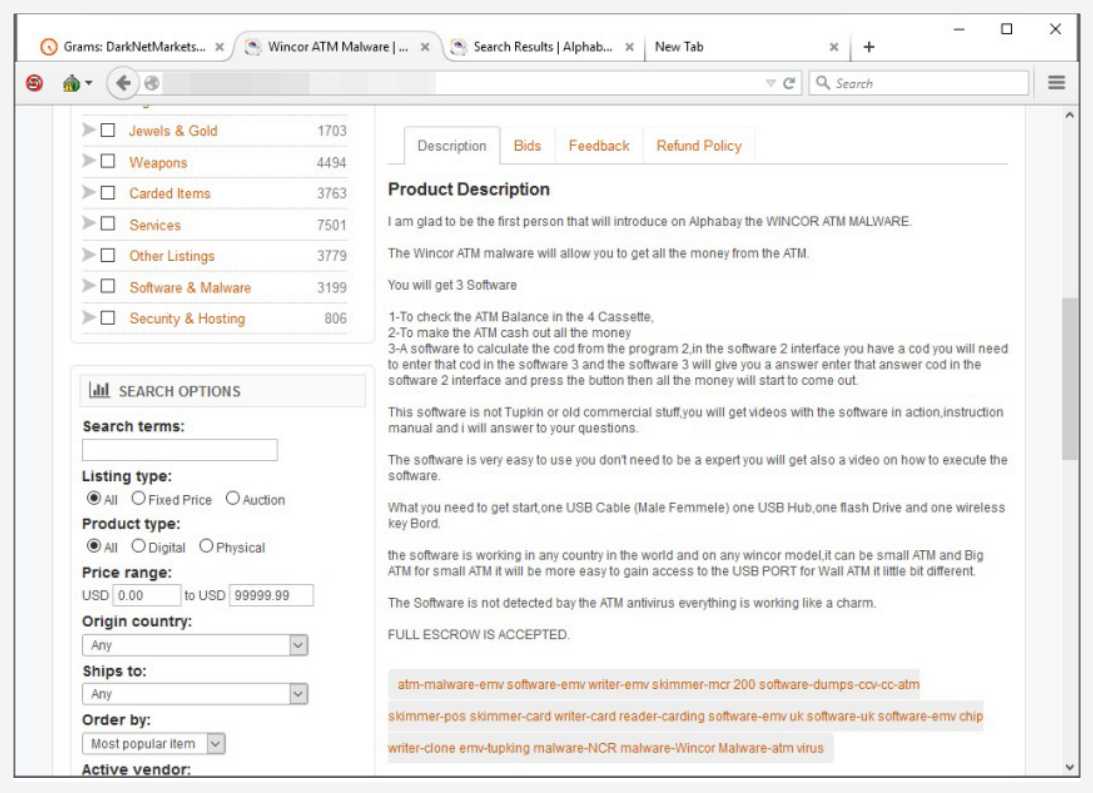


圖 8：自稱是 Ploutus 惡意程式的作者在深層網路市集上刊登的產品說明。

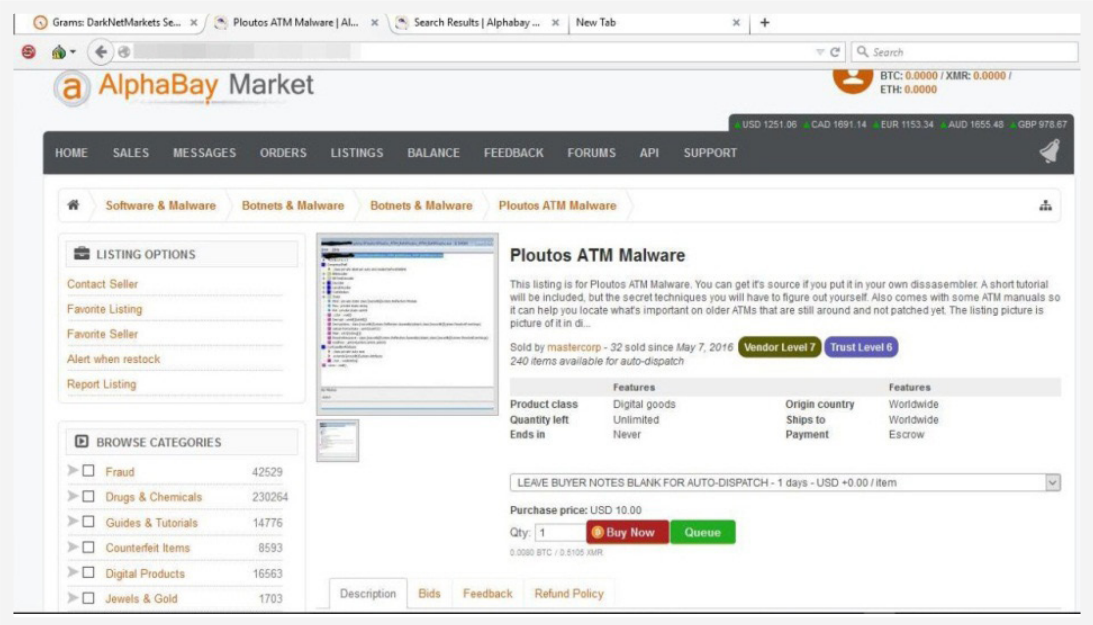


圖 9：另一位自稱是 Ploutus 惡意程式的作者在深層網路市集上刊登的產品說明。

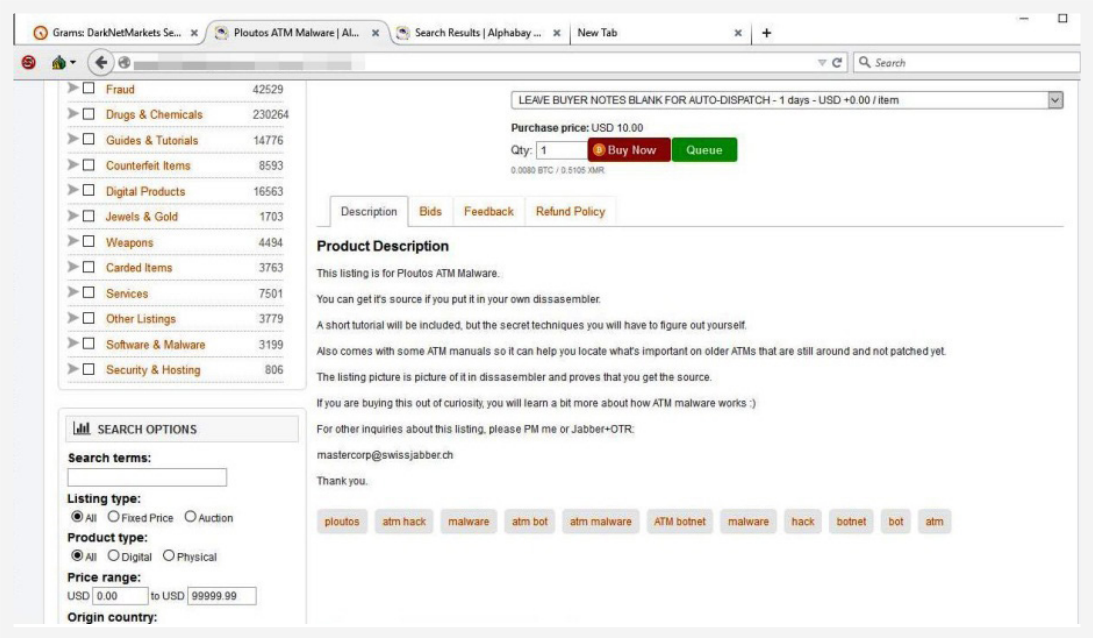


圖 10：自稱是 Ploutus 惡意程式的作者在深層網路上刊登的販售價格只有 10 美元。

在這份報告的研究期間，美國和加拿大並未出現任何重大或範圍較廣的 ATM 惡意程式攻擊。這或許是因為網路犯罪集團希望避免攻擊一些較大的國家，以免容易被逮。不過在地下網路上，從業餘駭客到專業的網路犯罪集團都在不斷開發、販售及使用 ATM 惡意程式。因此，相信未來美國和加拿大應該也會出現類似的攻擊，只是時間早晚的問題。

結論

早在 2009 年左右，網路犯罪集團就已經發現可利用軟體漏洞來攻擊 ATM 提款機並讓它感染惡意程式。從那時起，便有越來越多犯罪集團嘗試發動這類攻擊並且得逞，而且浮上檯面的 ATM 惡意程式家族也越來越多，從 2015 年開始快速成長速度。在趨勢科技與歐洲刑警組織 (Europol) 合作的研究當中，我們發現 2016 年開始出現一個令人不安的新趨勢：犯罪集團意識到，要攻擊 ATM 提款機不一定需親自接觸提款機，經由網路也可以達到相同目的。網路駭客只要能夠掌握銀行的內部網路，然後設法在提款機上安裝惡意程式，就能直接從遠端操控提款機，讓提款機吐鈔。

不論是經由網路駭入提款機的網路犯罪集團，或是實際打開提款機進行臨機攻擊的傳統犯罪份子，其目的都一樣，就是讓提款機吐鈔。只是網路犯罪集團不需親自打開提款機外殼，然後經由 USB 或 CD 光碟手動將惡意程式安裝到提款機上。他們只需從遠端遙控，然後再派車手到提款機前等候鈔票自己吐出來，再打包帶走即可。

這批人有可能本來就已經駭入銀行的內部網路，然後意外發現他們也可以駭入 ATM 網路。不過就 Ripper 的案例來看，歹徒是刻意尋找 ATM 網路並加以攻擊，而非意外發現 ATM 網路。他們不僅意圖明顯，而且具備高度的專業知識來攻擊 ATM 提款機而非其他資源。儘管美國和加拿大這類較大的國家在這次的研究當中並未出現 ATM 網路攻擊的案例，但我們認為這只是時間早晚的問題，也許 2017 年或未來就會開始出現同樣的案例。

ATM 網路攻擊現在已經不是什麼祕密，過去，銀行或許還以為只要將網路隔離，就能保障 ATM 網路的安全，防止駭客覬覦。但現在情勢顯然已經不同，執法機關應該深刻體認犯罪集團已經將目光牢牢鎖定 ATM 提款機，而金融機構也應採取更多安全措施來保障 ATM 提款機的安全。

值得一提的是，銀行、ATM 廠商以及資安廠商都已相當努力地開發及部署了一些方案，來解決本文所提到各種攻擊管道上的所有漏洞。但這並非表示 ATM 提款機就百分之百安全無虞，畢竟世間沒有什麼是萬無一失的。不過，規劃完善的資安策略，確實能大幅提升 ATM 提款機的安全，讓歹徒不得其門而入。

參考資料

1. International Organization for Standardization。(2003 年)。「ISO 8583-1:2003 金融卡交易訊息交換規格 - 第一部：訊息、資料元素與代碼值」(ISO 8583-1:2003 Financial transaction card originated messages – Interchange message specifications – Part 1: Messages, data elements and code values)。上次存取時間 2017 年 5 月 29 日： http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=31628.
2. International Organization for Standardization。(1998 年)。「ISO 8583-1:2003 金融卡交易訊息交換規格 - 第二部：機構識別碼之應用與註冊程序」(ISO 8583-1:2003 Financial transaction card originated messages – Interchange message specifications – Part 2: Application and registration procedures for Institution Identification Codes (IIC)。上次存取時間 2017 年 5 月 29 日：http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=23632.
3. International Organization for Standardization。(2003 年)。「ISO 8583-1:2003 金融卡交易訊息交換規格 - 第三部：訊息、資料元素與代碼值之維護程序」(ISO 8583-1:2003 Financial transaction card originated messages – Interchange message specifications – Part 3: Maintenance procedures for messages, data elements and code values)。上次存取時間 2017 年 5 月 29 日：http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=35363.
4. EFT Lab。(2015 年)。「TPDU - 交易通訊協定資料單元」(TPDU – The Transaction Protocol Data Unit)。上次存取時間 2017 年 5 月 29 日：https://www.eftlab.co.uk/index.php/site-map/our-articles/295-tpdu-the-transaction-protocol-data-unit.
5. Brian Krebs。(2014 年)。「竊賊在 ATM 提款機內植入惡意程式」(Thieves Planted Malware to Hack ATMs)。上次存取時間 2017 年 6 月 2 日：https://krebsonsecurity. com/2014/05/thieves-planted-malware-to-hack-atms/.
6. Wikimedia Foundation, Inc.。(2015年)。「CEN/XFS」。上次存取時間 2017 年 6 月 2 日：https://en.wikipedia.org/wiki/CEN/XFS.
7. European Committee for Standardization。(2000 年)。「金融服務延伸功能 (XFS) 介面規格 - 3.0 版 - 第一部：應用程式開發介面 (API) - 服務供應商介面 (SPI)；程式設計參考手冊」(Extensions for Financial Services (XFS) interface specification - Release 3.0 – Part 1: Application Programming Interface (API) - Service Provider Interface (SPI); Programmer's Reference)。上次存取時間 2017 年 8 月 1 日：http://read.pudn.com/downloads135/sourcecode/others/573815/01-Application%20Programming%20Interface.pdf.
8. Kazan First。(2015 年)。「Скарты 18-летнего челнинца в Елабуге мошенники сняли 340 000 рублеи 」。上次存取時間 2017 年 6 月 2 日：http://kazanfirst.ru/online/54389.
9. Vanja Svajcer。(2009 年)。「專門盜取卡片磁條資料的惡意程式入侵 ATM 提款機」(Credit card skimming malware targeting ATMs)。上次存取時間 2017 年 5 月 29 日：https://nakedsecurity. sophos.com/2009/03/17/credit-card-skimming-malware-targeting-atms/.
10. Kim Zetter。(2009 年)。「新的 ATM 惡意程式會竊取 PIN 碼和現金 - 更新」(New ATM malware captures PINS and Cash – Updated)。上次存取時間 2017 年 5 月 29 日：http://www. wired.com/2009/06/new-atm-malware-captures-pins-and-cash/.
11. Graham Cluley。(2009 年)。「Diebold ATM 木馬程式案例進一步細節」(More details on the Diebold ATM Trojan horse case)。上次存取時間 2017 年 5 月 29 日：https://nakedsecurity.sophos.com/2009/03/18/details-diebold-atm-trojan-horse-case/.
12. Daniel Regalado。(2013 年)。「Ploutus 後門程式重裝上陣 - Ploutus 離開墨西哥」(Backdoor.Ploutus Reloaded – Ploutus Leaves Mexico)。上次存取時間 2017 年 5 月 29 日：http://www.symantec.com/connect/blogs/backdoorploutus-reloaded-ploutus-leaves-mexico.
13. Daniel Regalado。(2014 年)。「利用手機簡訊遙控 ATM 提款機：網路犯罪手法越來越高明」(Texting ATMs for Cash Shows Cybercriminals Increasing Sophistication)。上次存取時間 2017 年 5 月 29 日：https://www.symantec.com/connect/blogs/texting-atms-cash-shows-cybercriminals-increasing-sophistication.
14. Daniel Regalado。(2014 年)。「Padpin 後門程式」(Backdoor.Padpin)。上次存取時間 2017 年 5 月 29 日：https://www.symantec.com/security_response/writeup.jsp?docid=2014-051213-0525-99.
15. FSLabs。(2014 年)。「NCR ATM 提款機應用程式開發介面文件外流到百度」(NCR ATM API Documentation Available on Baidu)。上次存取時間 2017 年 5 月 29 日：https://www.f-secure. com/weblog/archives/00002751.html.
16. Kaspersky Lab 全球研究分析團隊。(2014 年)。「Tyupkin：操控 ATM 提款機惡意程式」(Tyupkin: manipulating ATM machines with malware)。上次存取時間 2017 年 5 月 29 日：https://securelist.com/tyupkin-manipulating-atm-machines-with-malware/66988/.
17. Suzanne Cluckey。(2014 年)。「ATM 產業能否阻止 Tyupkin 的進擊？」(Can the ATM industry stop Tyupkin in its tracks?)。上次存取時間 2017 年 5 月 29 日：http://www. atmmarketplace.com/articles/can-the-atm-industry-stop-tyupkin-in-its-tracks/.

18. Thoufique Haq。(2015 年)。「新型態 ATM 惡意程式 GreenDispenser 現身」(Meet GreenDispenser: A New Breed of ATM Malware)。上次存取時間 2017 年 5 月 29 日：https://www. proofpoint.com/us/threat-insight/post/Meet-GreenDispenser.

19. David Sancho 與 Numaan Huq。(2016 年)。「Alice：輕量化精簡版實用 ATM 惡意程式」(Alice: A Lightweight, Compact, No-Nonsense ATM Malware)。上次存取時間 2017 年 6 月 6 日：http://blog.trendmicro.com/trendlabs-security-intelligence/alice-lightweight-compact-no-nonsense-atm-malware/.

20. Huang Yan Fen。(2016 年)。「【詳細圖解】駭客入侵一銀 ATM 流程追追」。上次存取時間 2017 年 6 月 6 日：http://www.ithome.com.tw/news/107294.

21. Group-IB。(2016 年)。「Cobalt：針對 ATM 的軟體攻擊」(Cobalt: logical attacks on ATMs)。上次存取時間 2017 年 6 月 6 日：http://www.group-ib.com/cobalt.html.

22. Kaspersky Labs。(2015 年)。「Carbanak APT：銀行大搶案」(Carbanak APT: The Great Bank Robbery)。上次存取時間 2017 年 6 月 6 日：https://securelist.com/files/2015/02/Carbanak_APT_eng.pdf.

23. Group-IB 與 Fox-It。(2014 年)。「Anunak：針對金融機構的持續性滲透攻擊」(Anunak: APT against Financial Institutions)。上次存取時間 2017 年 6 月 6 日：http://www.group-ib.com/files/Anunak_APT_against_financial_institutions.pdf.

24. Wichit Chantanusornsiri 與網路記者。(2016 年)。「全國 10,000 台 ATM 提款機有遭駭的危險」(10,000 ATMs nationwide hack-prone)。上次存取時間 2017 年 6 月 6 日：http://www.bangkokpost.com/archive/10-000-atms-nationwide-hack-prone/1069237.

25. NCR Corporation。(2016 年)。「NCR 安全更新：泰國惡意程式攻擊」(NCR Security Update: Malware Attacks in Thailand)。上次存取時間 2017 年 6 月 6 日：https://www.ncr.com/sites/default/files/ncr_security_alert_-_2016-12_network_malware_attack_in_thailand_-_sdms_160829_final_ for_review.pdf.

26. Sergey Golovanov。(2017 年)。「ATMitch：遠端遙控 ATM 提款機」(ATMitch: remote administration of ATMs)。上次存取時間 2017 年 6 月 6 日：https://securelist. com/77918/atmitch-remote-administration-of-atms/.

27. Jozsef Gegeny 與 Santiago Vicente。(2014 年)。「NeoPocket：新的 ATM 惡意程式」(NeoPocket: A new ATM malware)。上次存取時間 2017 年 5 月 31 日：https://www.s21sec.com/en/blog/2014/04/neopocket-a-new-atm-malware/.

28. Daniel Regalado。(2015 年)。「SUCEFUL：新一代 ATM 惡意程式」(SUCEFUL: Next Generation ATM Malware)。上次存取時間 2017 年 6 月 2 日：https://www.fireeye. com/blog/threat-research/2015/09/suceful_next_genera.html.

29. Sam Adams。(2015 年)。「Grigore Paladi：短短一個週末就盜領 160 萬英鎊的犯罪集團成員入獄」(Grigore Paladi: Gang member jailed for helping steal £1.6m from cash machines in ONE weekend)。上次存取時間 2017 年 6 月 5 日： http://www.mirror.co.uk/news/uk-news/grigore-paladi-gang-member-jailed-5115228.

30. Finance Twitter。(2014 年)。「馬來西亞 ATM 提款機如何遭拉丁美洲駭客盜領 3 百萬馬來幣」(Here's How Malaysian ATMs were Hacked of RM3 Million by Latin Americans)。上次存取時間 2017 年 6 月 5 日：http://www.financetwitter.com/2014/09/here-is-how-malaysian-atms-were-hacked-of-rm3-million-by-latin-americans.html.

31. Opalyn Mok。(2014 年)。「馬來西亞 Bayan Baru 地區的銀行成為最新 ATM 駭客攻擊目標」(Bank in Bayan Baru latest target of ATM hacking)。上次存取時間 2017 年 6 月 5 日：http://www. themalaymailonline.com/malaysia/article/bank-in-bayan-baru-latest-target-of-atm-hacking.

32. Atiqa Hazellah。(2014 年)。「ATM 竊盜嫌犯將在英國受審」(ATM theft suspect to be charged in UK)。上次存取時間 2017 年 6 月 5 日：http://www.nst.com.my/news/2015/09/atm-theft-suspect-be-charged-uk.

33. DIICOT。(2016 年)。「Comunicat de presa 05.01.2016」。上次存取時間 2017 年 6 月 5 日：http://www.diicot.ro/index.php/arhiva/1643-comunicat-de-presa-05-01-2016.

34. Bradley Barth。(2017 年)。「俄羅斯銀行提款機竊盜案調查線索指向 ATMitch 惡意程式」(Clues from Russian banking machine theft leads investigators to ATMitch malware)。上次存取時間 2017 年 6 月 1 日：https://www.scmagazine.com/clues-from-russian-banking-machine-theft-leads-investigators-to-atmitch-malware/article/648423/.

35. Ivana Kottsova。(2016 年)。「駭客不用提款卡就從 ATM 提款機盜領數百萬元」(Hackers steal millions from ATMs without using a card)。上次存取時間 2017 年 6 月 1 日：http://money.cnn.com/2016/07/14/news/bank-atm-heist-taiwan/.

36. Faith Hung。(2016 年)。「台灣表示已逮捕盜領 200 萬美元的外國 ATM 網路竊賊」(Taiwan says foreign suspects arrested over $2 million ATM cyber robbery)。上次存取時間 2017 年 6 月 1 日：http://www.reuters.com/article/us-taiwan-banks-theft-idUSKCN0ZX0N7.

37. Daniel Regalado。(2016 年)。「ATM 提款機惡意程式 RIPPER 與 1,200 萬泰銖盜領案」(RIPPER ATM Malware and the 12 Million Baht Jackpot)。上次存取時間 2017 年 6 月 1 日：https://www.fireeye.com/blog/threat-research/2016/08/ripper_atm_malwarea.html.

38. David Sancho 與 Numaan Huq。(2016 年)。「Alice：輕量化精簡版實用 ATM 惡意程式」(Alice: A Lightweight, Compact, No-Nonsense ATM Malware)。上次存取時間 2017 年 6 月 1 日：http://blog.trendmicro.com/trendlabs-security-intelligence/alice-lightweight-compact-no-nonsense-atm-malware/.

39. Mohit Kumar。(2017 年)。「警方逮捕 5 名利用惡意程式從 ATM 提款機盜領 320 萬美元的網路竊賊」(Police Arrest 5 Cyber Thieves Who Stole 3.2 Million From ATMs Using Malware)。上次存取時間 2017 年 6 月 1 日：http://thehackernews.com/2017/01/atm-hack-malware.html.

作者：

TrendLabs

趨勢科技全球技術支援與研發中心

趨勢科技

趨勢科技是全球雲端安全領導廠商，致力為企業和消費者開發網際網路內容安全與威脅管理解決方案，建立一個安全的數位資訊交換世界。身為伺服器安全的先驅，擁有 20 多年經驗，我們專門提供符合客戶及合作夥伴需求的頂尖用戶端、伺服器及雲端安全防護，更快攔截新的威脅，保護實體、虛擬及雲端環境內的資料。我們領先業界的雲端運算防護技術、產品及服務皆以趨勢科技 Smart Protection Network™ 基礎架構為後盾，能在威脅出現的來源，也就是網際網路，直接攔截威脅，並且還有全球 1,000 多位威脅情報專家在背後支援。如需更多資訊，請至：www.trendmicro.tw

TREND MICRO™

Securing Your Journey to the Cloud

www.trendmicro.tw