
cp<r>
CHECK POINT RESEARCH
網路攻擊趨勢
2018 年年中報告
Check Point
SOFTWARE TECHNOLOGIES LTD

Check Point 網路攻擊趨勢：2018 年年中報告

簡介

全球網路環境所承受的威脅不斷進步，企業組織及安全社群也不斷面臨挑戰。有些利用區塊鏈交易系統，有些在蓬勃的行動領域發展出全新的攻擊方法，還有些因應雲端環境改造過去所用的攻擊工具，最新技術發展及各類技術的興起，在 2018 年的網路威脅環境顯然大行其道。

今年度截至目前為止，諸多事實已經證明不同病毒株惡意軟體及其撰寫者的能力已經超乎人們所能想像，不但更老練狡詐，敏捷度也有了新的突破。從我們的 GandCrab 勒索軟體分析結果看來，惡意軟體現在已經能夠迅速適應安全廠商提供的安全解決方案。

目前最盛行的趨勢包括了加密貨幣挖礦程式 (Cryptominer)，以及所有牽涉到加密的威脅。事實上，加密貨幣挖礦程式已經迅速席捲整個世界，在今年度超越勒索軟體，成為最受威脅者青睞的攻擊向量。目前為止，加密貨幣挖礦程式不但能力大增，更提升了其目標群的等級：伺服器、行動裝置、工業系統及雲端基礎架構，一個也沒少。

2018 上半年也出現了一些頗有意思的新趨勢。舉例來說，雲端基礎架構成了威脅者磨刀霍霍的對象；雲端環境儲存了極大量的敏感資料及可用運算資源，因此很容易就吸引攻擊者的注意。特斯拉 (Tesla) 的雲端伺服器在今年稍早感染門羅幣 (Monero) 挖礦程式，以及 FedEx 客戶的大量敏感資料外洩事件，只不過是發生在 2018 年的其中兩個例子。

為提供各企業組織最強大的防護等級，安全專家們必須理解不斷變化的環境，以及最新的威脅與攻擊手法。Check Point 全球威脅情資趨勢 (Global Threat Intelligence Trends) 報告綜述加密貨幣挖礦程式、勒索軟體、銀行及行動威脅等主要類別的惡意軟體威脅態勢，報告引用準據是 ThreatCloud 世界網路威脅地圖 (ThreatCloud World Cyber Threat Map) 2018 年 1 月到 6 月之間的資料。

全球趨勢

加密貨幣挖礦程式的發展

加密貨幣挖礦的攻勢波濤洶湧，令人難以忽視。2018 上半年，加密貨幣挖礦程式獨霸世界網路攻擊及惡意軟體系列兩方面領先地位。加密貨幣挖礦程式超越勒索軟體，波及全世界逾 42% 的企業組織，而在 2017 年年底，其影響範圍還在 20.5% 之譜。過去六個月來，加密貨幣挖礦攻擊為使用者「賺進」的金額據估超過 25 億美元，並且這一數字還在持續增長。

加密貨幣挖礦程式出現至今，已取得長足發展。據觀察，加密貨幣挖礦程式一開始只是發動入侵網站等簡易型的攻擊，今年卻已經透過 Facebook Messenger、YouTube 廣告及 Google Play 大肆傳播，波及無數的網站、個人電腦，以及功能強大的伺服器，例如 Jenkins。加密貨幣挖礦程式在 2018 年更加進化，其能力大幅精進，不但越來越複雜，就連破壞力也益發強大。

加密貨幣挖礦程式的興起明顯是為了增加運算資源利用百分比，也為了提高獲利，如今，加密貨幣挖礦程式更將可能構成妨礙的一切視為目標。這正是加密貨幣挖礦程式鎖定 SQL 資料庫、工業系統、某俄國核電廠，甚至覬覦雲端基礎架構的理由。加密貨幣挖礦程式近來的發展也有突飛猛進之勢，不但會利用高調的漏洞，更能規避沙箱及安全防護產品，從而提升感染率。

在加密貨幣挖礦程式的攻勢之下，行動領域也不能倖免。去年 4 月，名為 HiddenMiner 的 Android 加密貨幣挖礦程式鎖定了無數台裝置，這個挖礦程式會連續挖掘門羅幣，直到裝置的資源全數枯竭才罷休。行動挖礦程式甚至得以破壞 Apple 的防衛機制，成功滲透 App Store，利用惡意軟體竊取受害者的加密貨幣錢包登入認證。

屋漏偏逢連夜雨，2018 年年初開始，許多會利用加密貨幣交易系統潛藏漏洞的新型攻擊手法一一浮上檯面。除了其他手段之外，這些手法還包括盜用虛擬錢包及認證、操縱加密貨幣交易以及數位貨幣首次發行詐騙 (Initial Coin Offering, ICO)，也就是誘騙受害者投資假的未成熟加密貨幣。

雪上加霜的是，其他惡意軟體系列也開始跟進並結合挖礦功能；勒索軟體，以及 Panda 和 TrickBot 等眾所皆知的銀行特洛伊木馬病毒，現在不但鎖定銀行帳戶，更增加了盜用加密貨幣認證的功能，將加密貨幣錢包和交易系統帳戶也列為下手目標。

威脅者知道加密貨幣有利可圖，甚至比其他非法手段更有賺頭，於是，各類加密威脅幾乎天天登上新聞頭條版面。

轉型採用雲端技術可能面臨的新型態威脅

雲端環境改變了公司行號管理、儲存及共用資料、應用程式和工作內容的方式。雲端基礎架構縱有諸多優點，卻也是個有利可圖又深具吸引力的新環境，許多攻擊者開始對雲端環境數不清的可用運算資源及敏感資料虎視眈眈。

2018 年確實出現了許多以雲端儲存服務為主的精密技術和工具。光就去年一年來看，全世界就有 51% 的企業組織曾經遭逢雲端攻擊，FedEx、Intel 以及 Honda 也在受害者之列。

有幾種雲端攻擊是利用不夠完善的安全措施，其中尤以涉及竊取資料和外洩資訊的攻擊為主。談到威脅者是透過什麼樣的方式存取和控制雲端環境中未受保護的資源，在公開程式碼儲存機制中公開認證資料，或是使用弱式密碼，只不過是其中幾個例子罷了。

另一類大肆攻擊雲端環境的新興威脅，就是惡名昭彰的加密貨幣挖礦程式，這類程式會鎖定雲端基礎架構並盜用其中龐大的運算能力，為威脅者帶來了可觀的獲利。2018 上半年，加密貨幣挖礦程式就鎖定了雲端的兩大核心要素 - Docker 系統和 Kubernetes 系統。舉例來說，特斯拉 (Tesla) 的內部雲端伺服器就是因為如此而在幾個月前感染了門羅幣加密貨幣挖礦程式。

用於管理服務、進行服務交互操作以及自服務中擷取資訊的應用程式開發介面 (Application Programming Interface，API)，也成為威脅者鎖定的目標。由於只要連上網際網路就能找到雲端 API，因此威脅者輕而易舉就能運用這個管道肆無忌憚地存取雲端應用程式。

看來，雲端威脅會隨著時間一直進化；攻擊者會繼續挑戰公有雲服務的極限，不斷針對雲端環境開發出越來越多工具。事實上，新型態雲端破壞手法浮上檯面之際，下一波攻擊早就已經發生了。

多平台攻擊：桌面和行動

2018 年年初，人們發現了一款名為「Dark Caracal」的新型態進階持續性威脅 (Advanced Persistent Threat，APT)，但這類威脅在暗中從事破壞行動恐怕早有五年的時間了。APT 團體在過去數年間多次從事間諜活動，而其存在正代表著一種獨特的操作手法，也彰顯了 2018 年其中一股最猖獗的趨勢。起初，這類攻擊手段會收集存在行動裝置中的敏感資料，近來進一步改採更能發揮效益的技術，也就是利用一個能夠感染 Windows、Linux 及 Mac OS 的惡意軟體。無論是否以一個惡意軟體為主，多平台攻擊都會對其受害者造成莫大損失，因為這類攻擊手段可以同時發動攻擊，其目標可能是私人住宅中所有的桌上型器材、行動裝置及消費裝置，也可能是企業內部所用的工業系統及資料中心。

直到 2017 年年底之前，多平台惡意軟體曝光的場合寥寥可數，但不出所料，就在連線消費裝置越來越多、非 Windows 作業系統的市佔率越來越高之際，跨平台惡意軟體的數量也開始增加。破壞活動主事者運用各式各樣的技術，控制各種遭破壞活動感染的平台。

2018 上半年，Android 銀行特洛伊木馬病毒「Roaming Mantis」的攻勢更甚以往，其目標包括 iOS 使用者以及用於採礦作業的個人電腦資源，為的就是讓病毒撰寫者能夠急速提高感染率。

功能強大的智慧型手機與 Office 365 等新穎技術問世後，潛在受害者不再使用單一端點，而是同時運用數種連線功能完善的裝置及服務。

這種現象造就了一個全新的環境，受害者在其中會面臨更多攻擊向量，威脅者可能會試圖在其中找出最弱的個人或企業組織資料連結並加以利用。

滲透整個供應鏈的行動惡意軟體

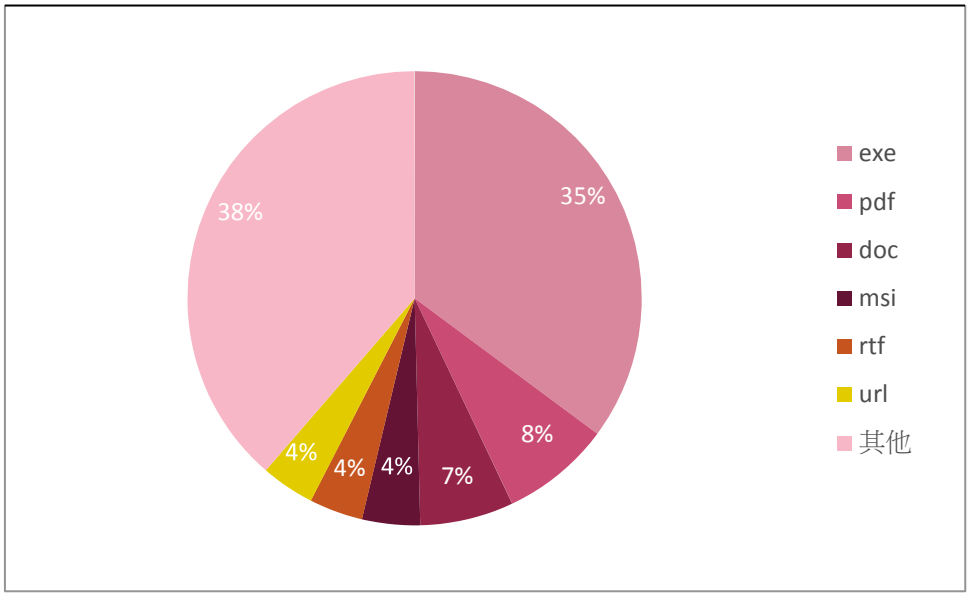
對現代人而言，行動裝置感染惡意軟體已經是司空見慣的現象了。裝置遭駭的途徑無所不在，從透過惡意 URL 下載或偽裝成看似單純的行動應用程式，各種手段比比皆是。

不過，今年上半年出現了一個有趣的趨勢 – 預先安裝的惡意軟體。從幾次的事件看來，感染惡意軟體的途徑既非應用程式商店，也不是惡意 URL，而是本來就安裝在裝置中的。今年 3 月，Check Point 研究人員揭發了大肆散播的行動殭屍網路，其名稱是「RottenSys」，遭感染的 Android 裝置數量近五百萬之譜。RottenSys 喬裝成正常的「系統 Wi-Fi」應用程式，數以百萬計的全新智慧型手機都已預先安裝這款應用程式，這些手機的製造商不乏知名品牌，包括華為 (Huawei)、小米 (Xiaomi)、Vivo 以及三星 (Samsung)。另一宗個案，則是在已經售出的 42 款平價智慧型手機中發現了預先安裝的 Triada 銀行特洛伊病毒。威脅者入侵供應鏈的能力令人憂心，未來也將繼續造成困擾。

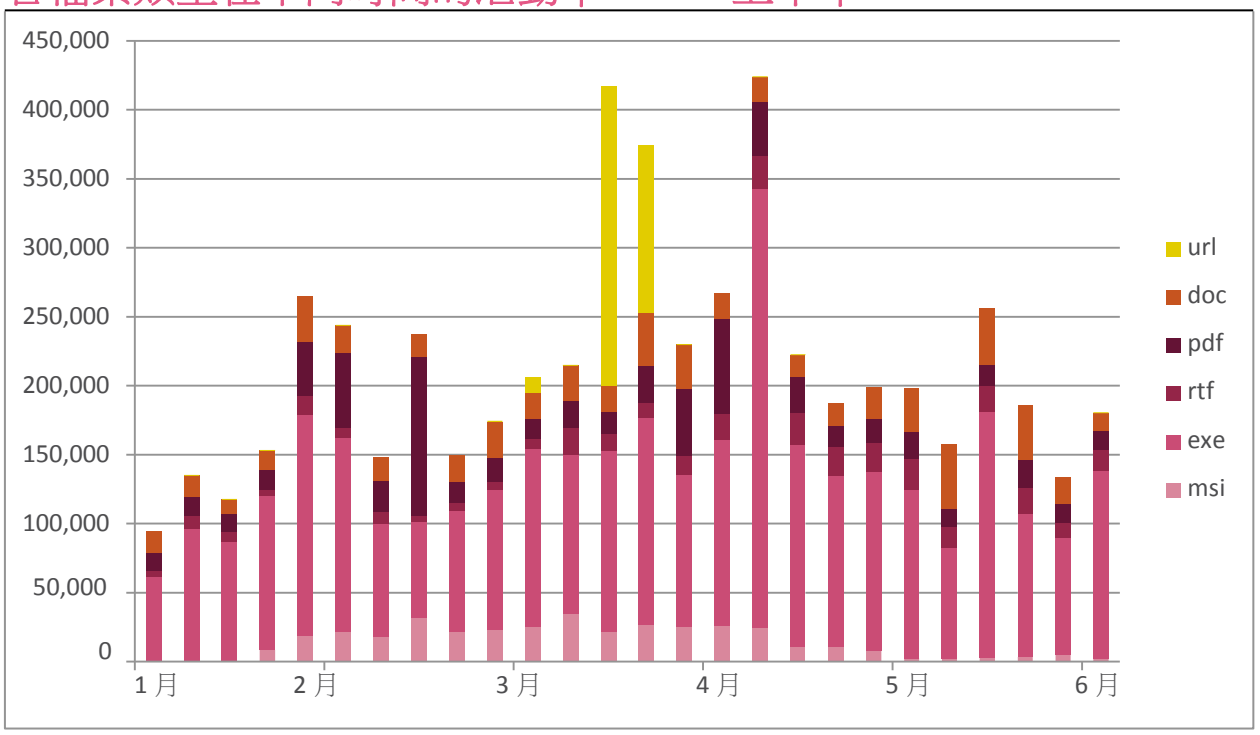
此外，人們對行動裝置的依賴日益加重，許許多多專為提升裝置電池效能，讓使用者能夠稍為延長手機使用時間的應用程式，也在應用程式市場上如雨後春筍般紛紛冒出。我們發現，這些應該安全無虞的應用程式，實際上有一大部分是惡意軟體喬裝而成的，這恐怕意味著威脅者今年似乎在這塊市場找到了潛在商機。其中，銀行特洛伊木馬病毒、廣告軟體，甚至連 AndroRAT 之類精密複雜的 RAT，都被偽裝成一款名為「TrashCleaner」的工具應用程式，不但可以竊取行動網路資訊、儲存容量、行事曆活動，還能執行殼層命令。

我們透過極其容易遭到入侵的裝置管理一切私人及工作生活，因此，預先安裝惡意軟體及惡意行動應用程式持續增加這兩種現象，在在反映出威脅者是多麼汲汲營營於大肆利用這個領域。

最普遍的惡意檔案類型 – 2018 上半年



各檔案類型在不同時間的活動率 - 2018 上半年



全球惡意軟體統計資料

本報告以下各節所示的資料對照結果，是以 2018 年 1 月到 6 月間的 Check Point ThreatCloud 網路威脅地圖為準據。

主要惡意軟體系列

全球

圖 1：全球最普遍的惡意軟體：
公司網路遭遇每類惡意軟體的百分比

我們針對以下每一個區域各列舉兩張圖表。第一張詳細說明該地區最普遍的惡意軟體，接下來的第二張圖表則詳細說明該地區相較於其他地區出現比例最高的惡意軟體系列。

美洲

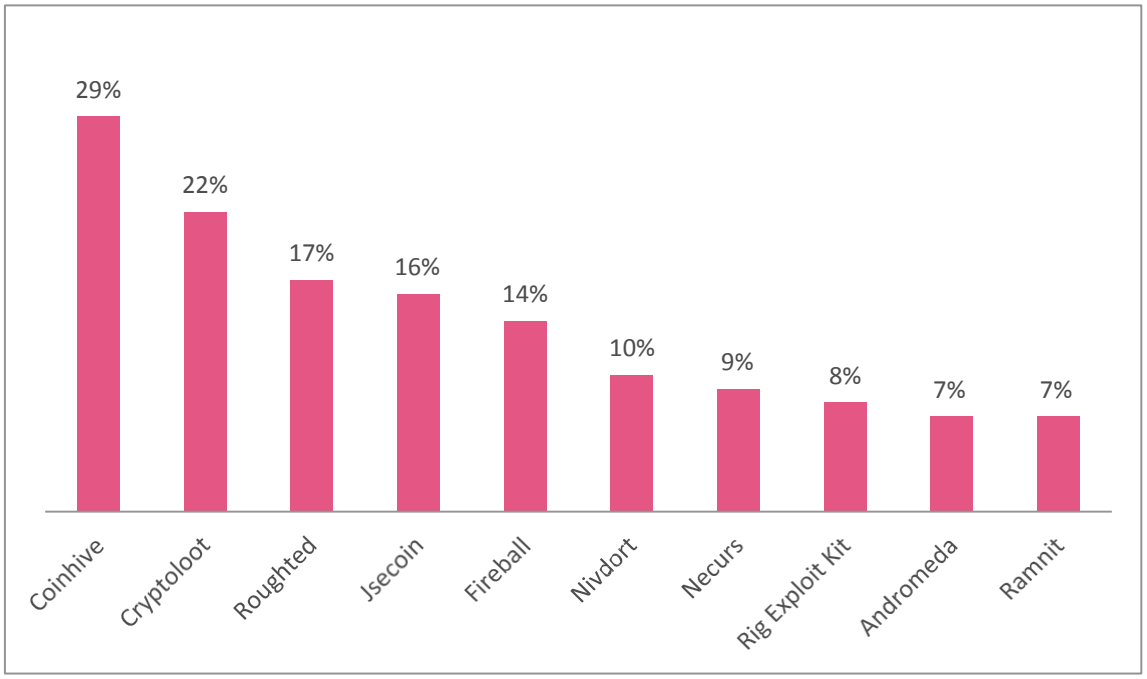


圖 2：美洲最普遍的惡意軟體

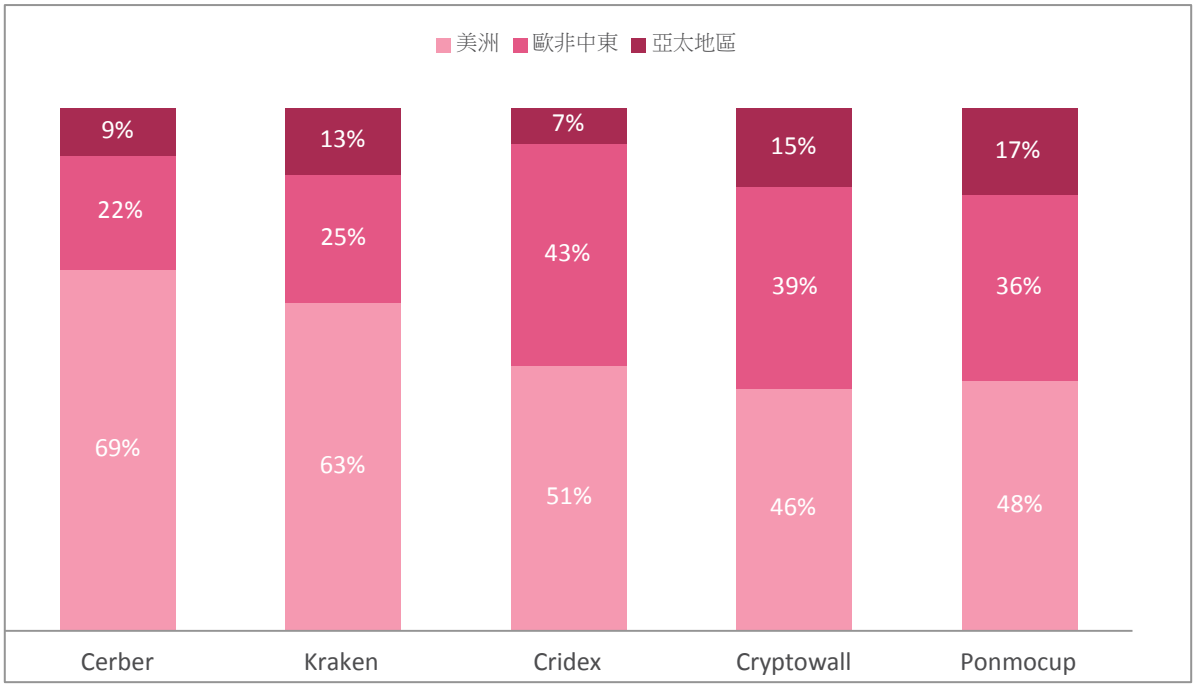


圖 3：主要鎖定美洲的惡意軟體

歐洲、中東和非洲 (EMEA)

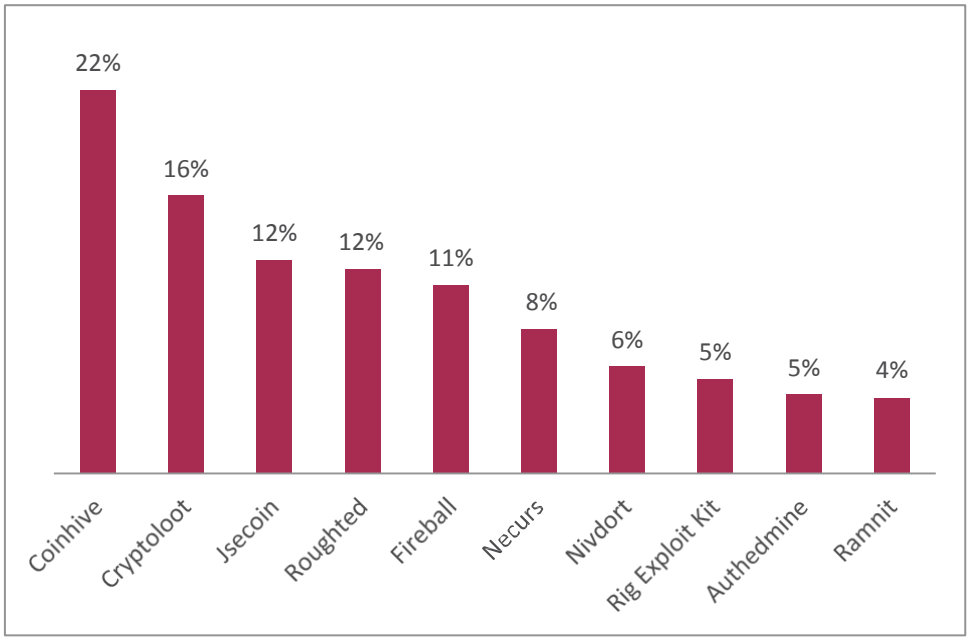


圖 4：歐非中東最普遍的惡意軟體

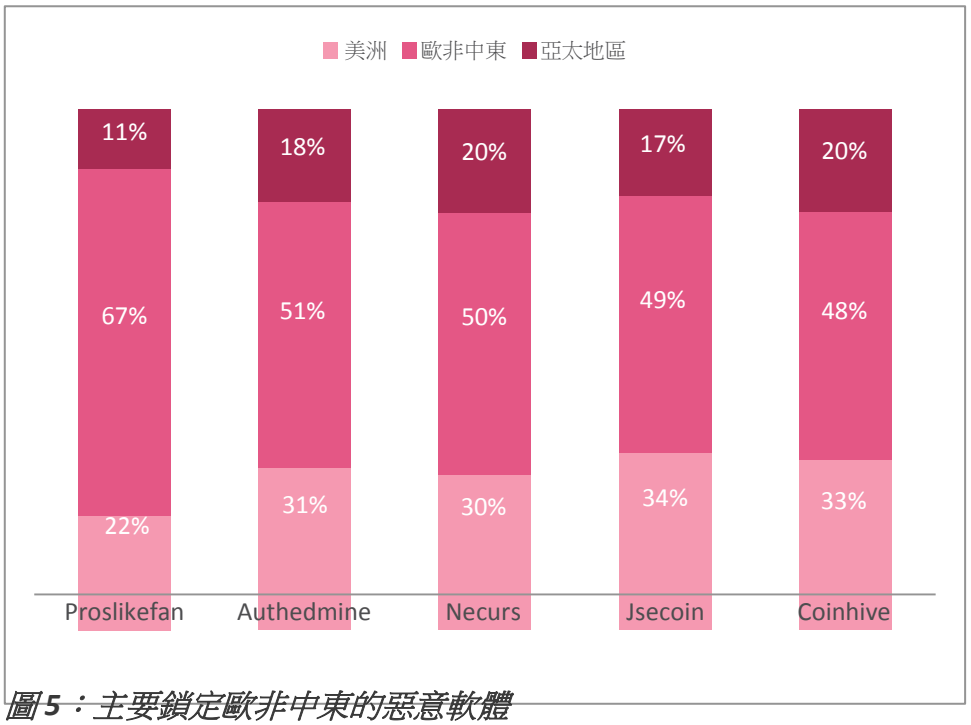


圖 5：主要鎖定歐非中東的惡意軟體

亞太地區 (APAC)

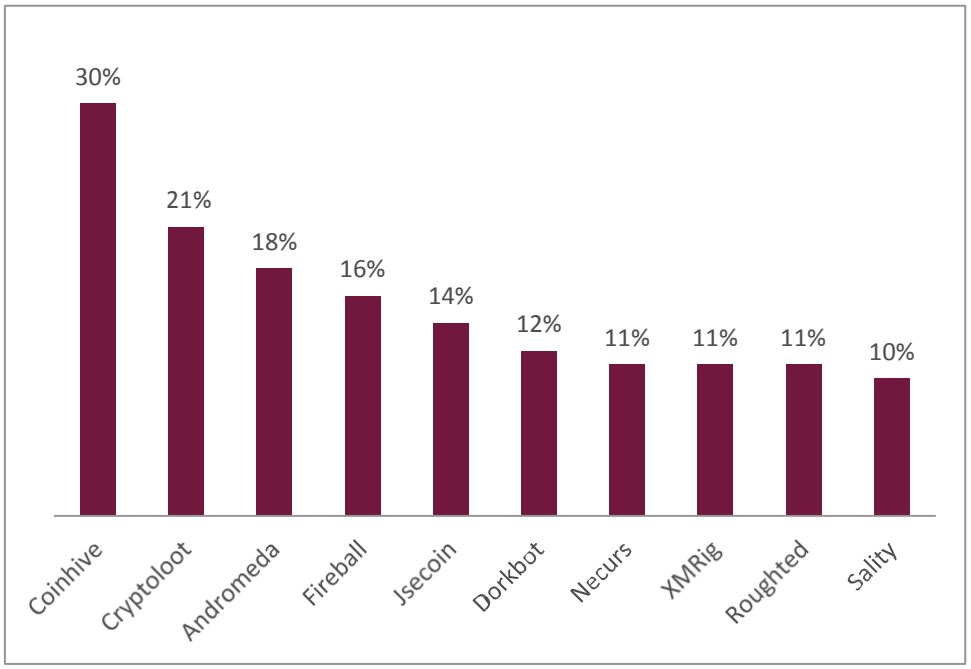


圖 6：亞太地區最普遍的惡意軟體

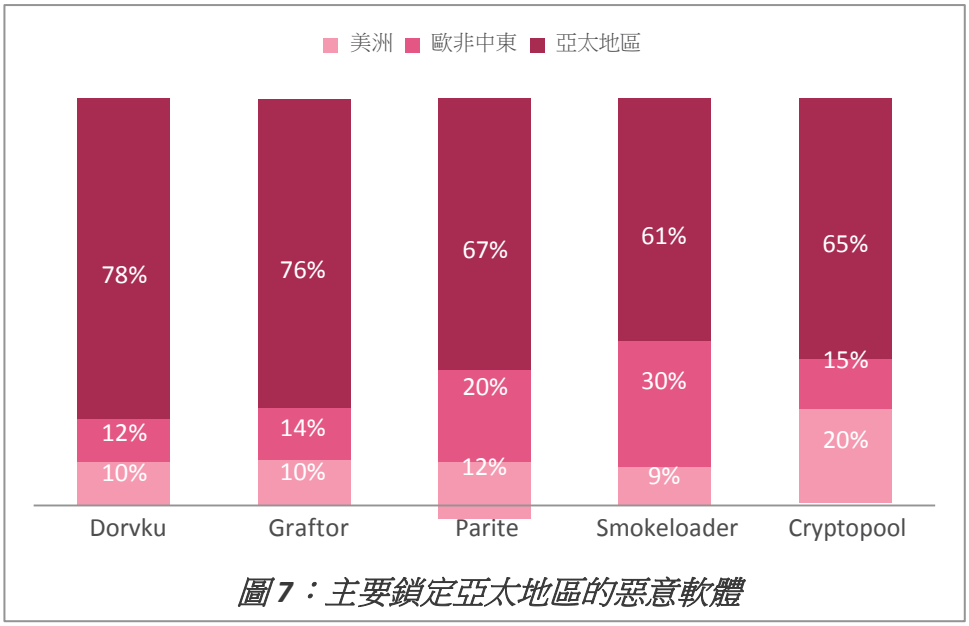


圖 7：主要鎖定亞太地區的惡意軟體

主要惡意軟體全球分析

CoinHive 是一款受歡迎的門羅幣加密貨幣網頁挖礦程式，這款程式獨霸全球及區域排行榜，全球 25% 的企業組織都曾經成為它的目標。CoinHive、Cryptoloot 和 Jesscoin 構成的加密貨幣挖礦程式小隊影響所及大約佔了全球的 40%，而且絲毫沒有呈現出任何式微的跡象。自從 CoinHive 在去年 9 月初次公佈其 JavaScript 挖礦程式碼後，無數個網站隨時都有可能被植入這個程式碼，它會利用訪客的運算資源，取代威脅者採用的線上廣告，成為新的生財工具。今年，Coinhive 的散播範圍更廣，就連 YouTube 廣告也暗藏這個程式碼，不但透過 Google 的 DoubleClick 平台及 Facebook Messenger 散播，也內嵌在數千個網站中。

RIG 漏洞攻擊套件是目前幾個不同非法活動最慣用的漏洞攻擊套件，普及率更在全球及區域排行榜上急速竄升。RIG 感染鏈的起點是重新導向至暗藏 JavaScript 的登陸頁面，這個頁面會檢查有無易受攻擊的外掛程式，也會利用瀏覽器。Rig 會針對 Flash、Java、Silverlight 及 Internet Explorer 發動漏洞攻擊，今年在 IE 發現了一種新形態零時差漏洞 (CVE-2018-8174)，而 Rig 正是第一個將這種漏洞列入攻擊目標的套件。2018 上半年，RIG 已經擠下 Bunitu、加密貨幣挖礦程式及常見的 SmokeLoader 等各種封包內容，成為熱門新聞話題。

主要加密貨幣挖礦惡意軟體

本節圖表說明受各加密貨幣挖礦惡意軟體波及之組織的百分比。圖表內容說明主要加密貨幣挖礦惡意軟體肆虐全球及各區域的情勢。

全球

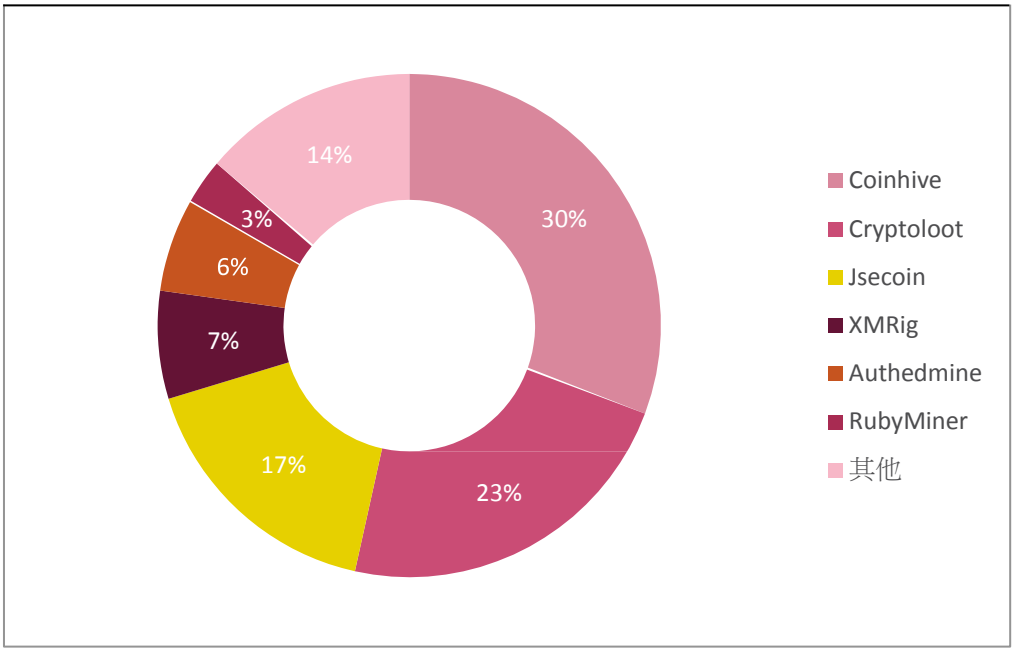


圖 8：全球主要加密貨幣挖礦惡意軟體

美洲

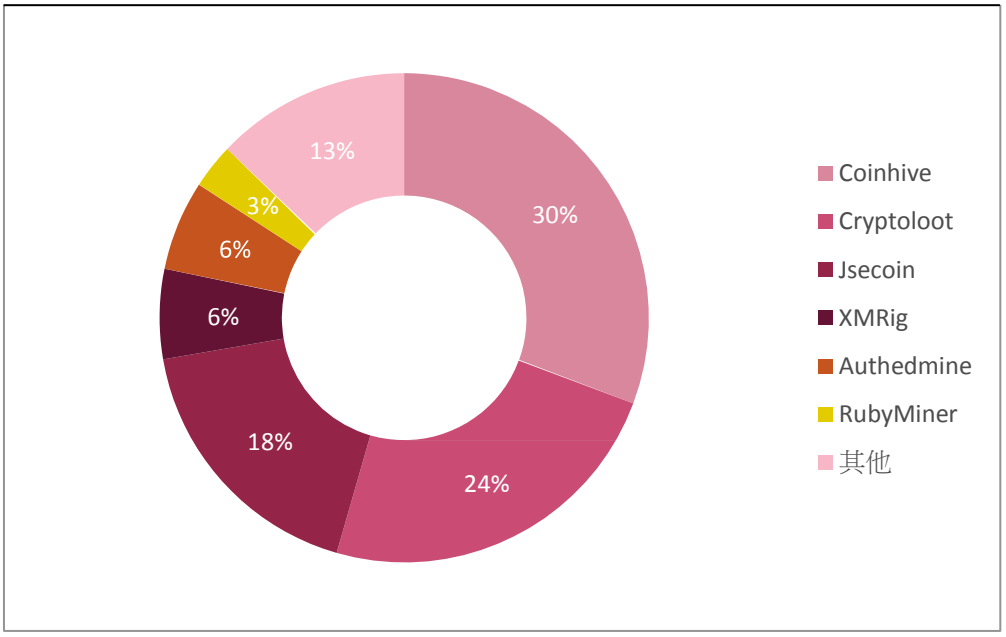


圖 9：美洲主要加密貨幣挖礦惡意軟體

歐非中東

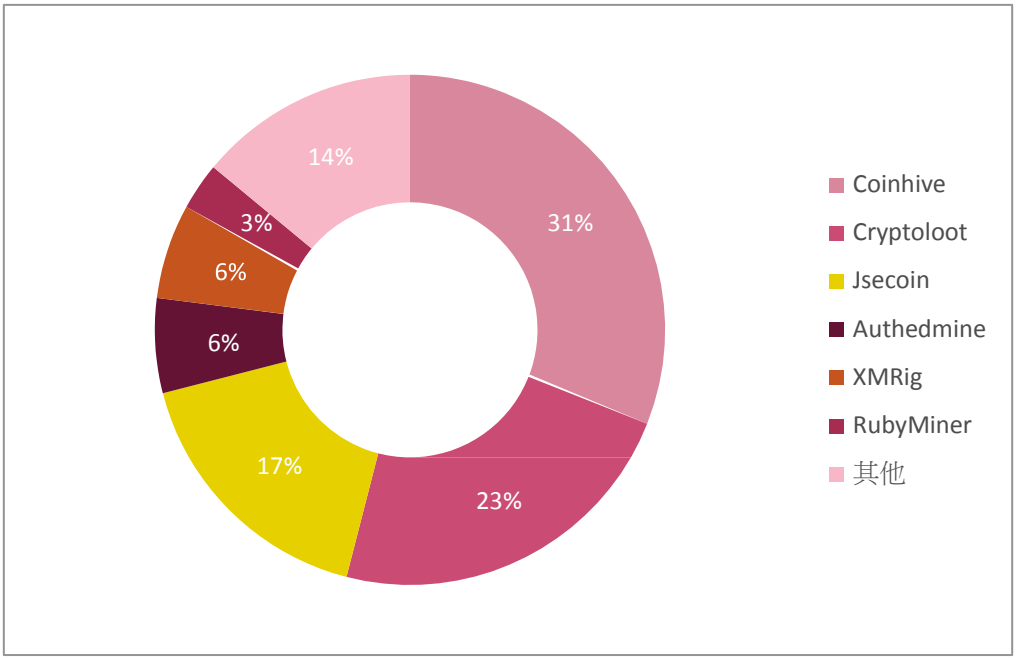


圖 10：歐非中東主要加密貨幣挖礦惡意軟體

亞太地區

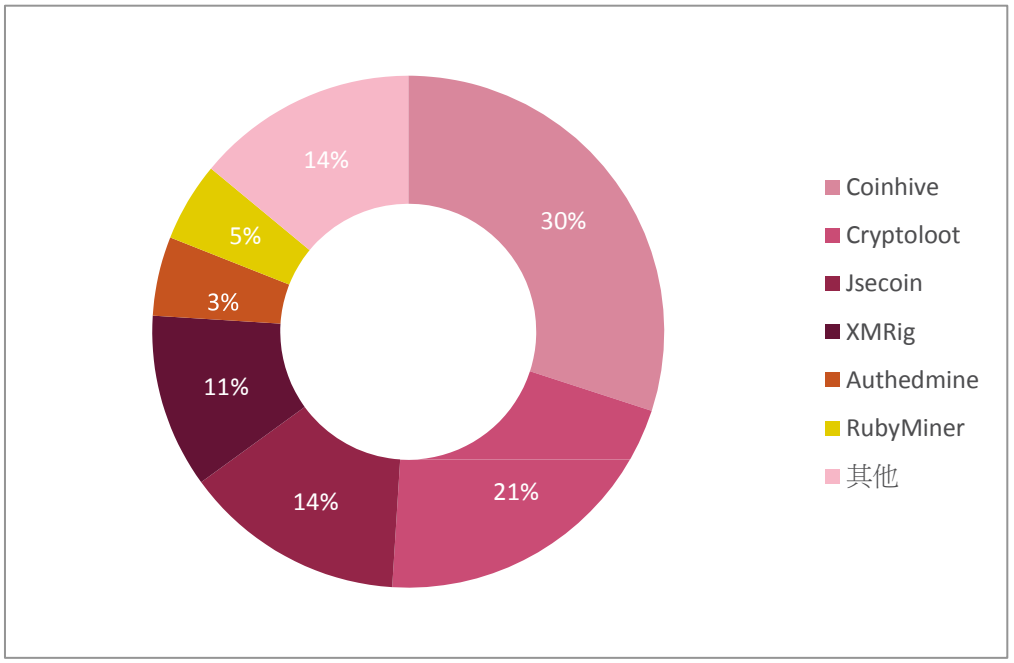


圖 11：亞太地區主要加密貨幣挖礦惡意軟體

加密貨幣挖礦程式全球分析

2017 年 5 月首度現蹤的開放原始碼 CPU 挖礦軟體 **XMRig**，在所有區域均名列第三。XMRig 挖礦程式碼是威脅者最愛用的挖礦專用程式碼，光是 2018 上半年之內，已經有眾多加密貨幣病毒株利用這個程式碼，**RubyMiner** 就是其中之一。Check Point 研究人員在去年 1 月獨家偵測到 Rubyminer，之後這個病毒株也登上了全球和地區排行榜。RubyMiner 捨棄排行榜上多數其他惡意程式植入於網站的手法，轉而鎖定沒有套用修補程式的 Windows 及 Linux 伺服器，目前為止，RubyMiner 已經嘗試攻擊了全球 30% 的公司網路，目的就是將強大的伺服器變成其幕後黑手的挖礦工具。

主要勒索軟體

本節圖表說明受各勒索軟體波及之組織的百分比。圖表內容說明各類主要勒索軟體肆虐全球及各區域的情勢。

全球

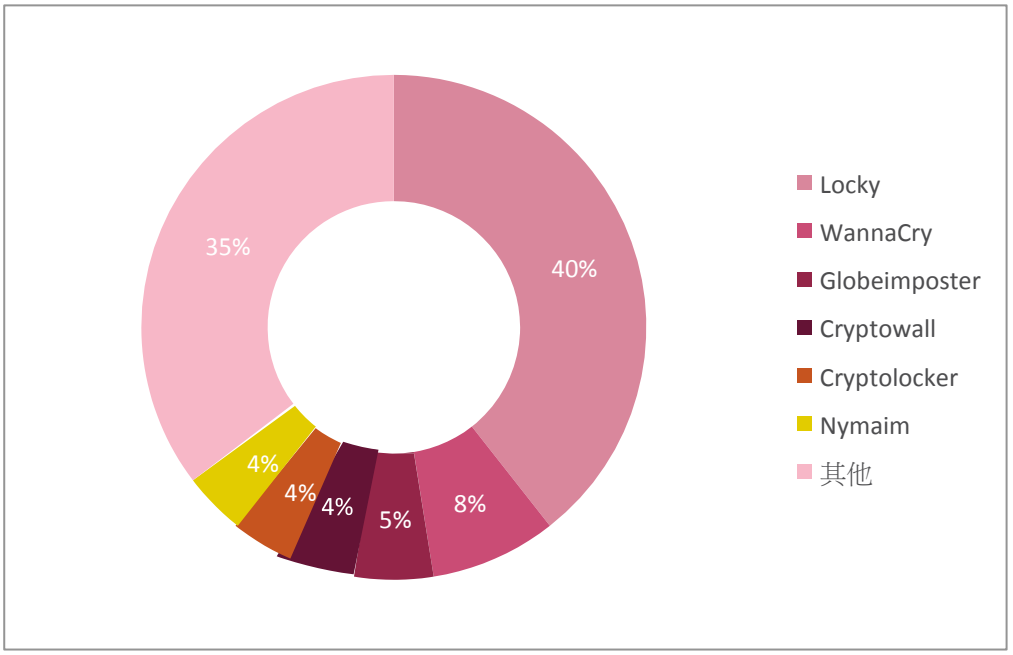


圖 12：全球最普遍的勒索軟體

美洲

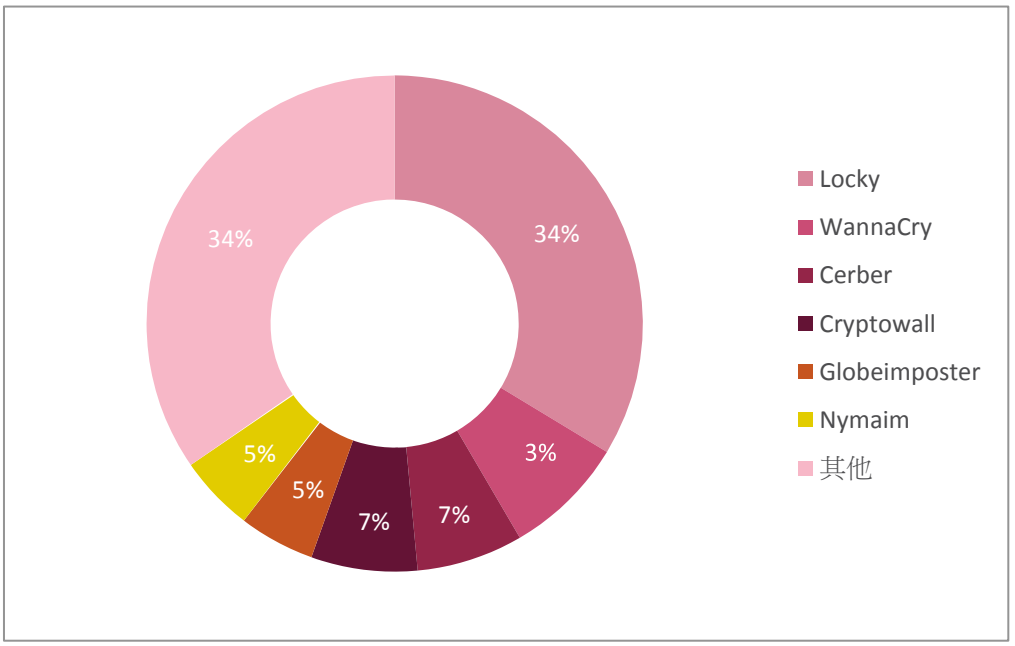


圖 13：美洲最普遍的勒索軟體

歐非中東

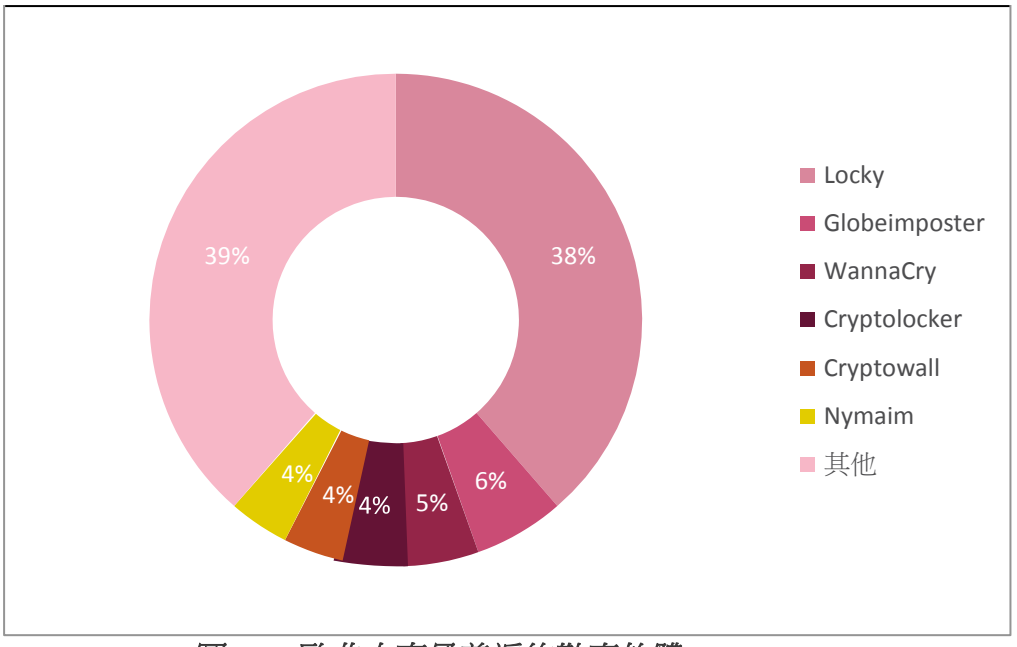


圖 14：歐非中東最普遍的勒索軟體

亞太地區

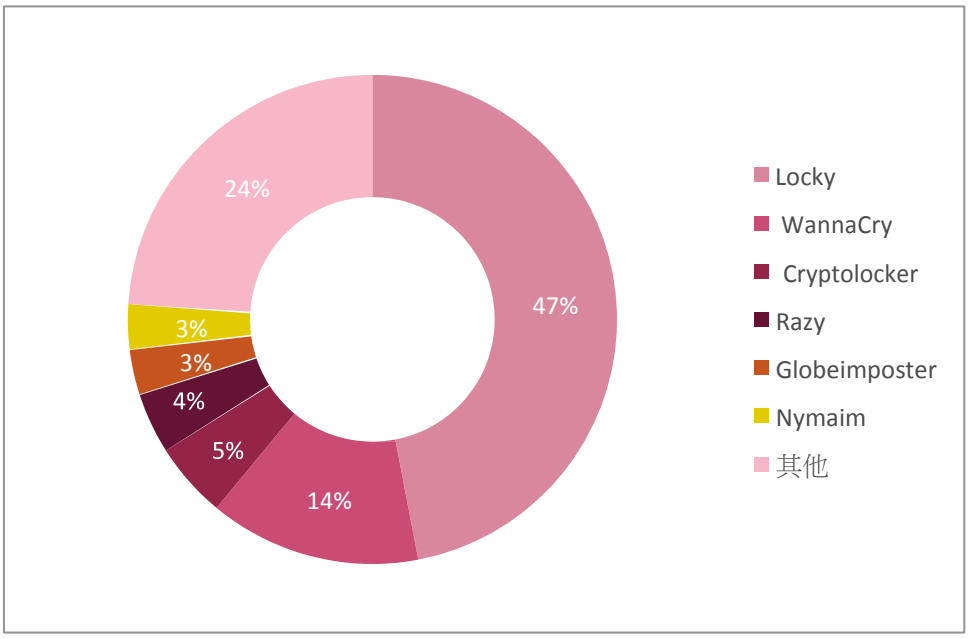


圖 15：亞太地區最普遍的勒索軟體

勒索軟體全球分析

2016 年 2 月，**Locky** 勒索軟體初次現蹤，此後始終佔據全球及區域排行榜之首，是 2018 最普遍的勒索軟體之一。令人訝異的是，同樣惡名昭彰的 **WannaCry** 依然保持了 2017 年的排行榜戰績，即使這款勒索軟體如野火般散播感染無數裝置的事件距今已一年有餘，其攻擊力仍未減退。看來，儘管是一年後的現在，仍然有許多感染了 WannaCry 的電腦不斷在網際網路上搜尋易受攻擊的 Windows 電腦。

主要銀行惡意軟體

報告中本節的圖表說明受各銀行惡意軟體波及之組織的百分比。圖表內容說明主要銀行惡意軟體肆虐全球及各區域的情勢

全球

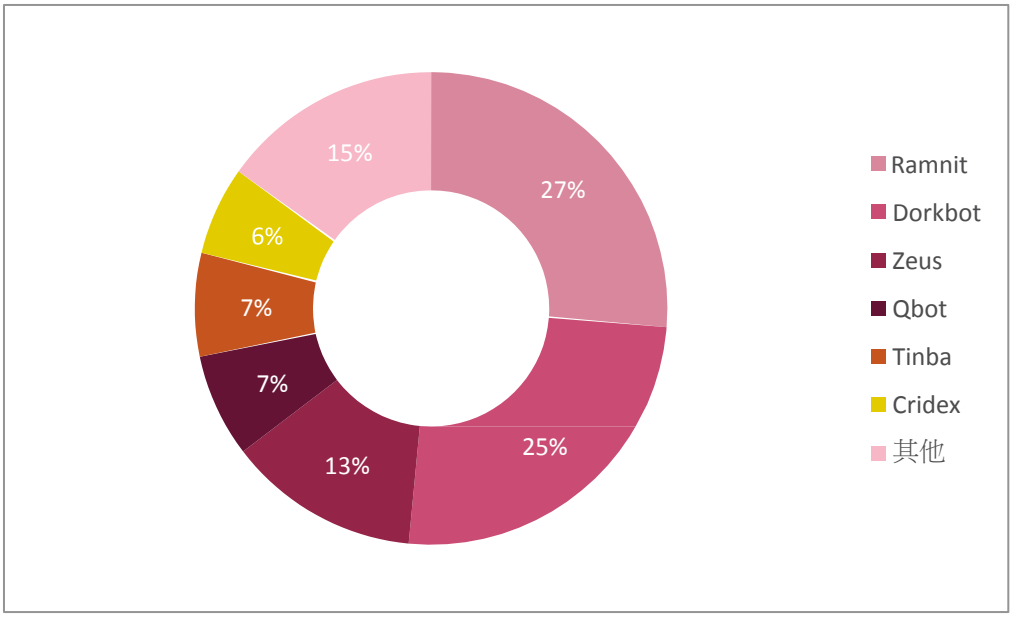


圖 16：全球最普遍的銀行惡意軟體

美洲

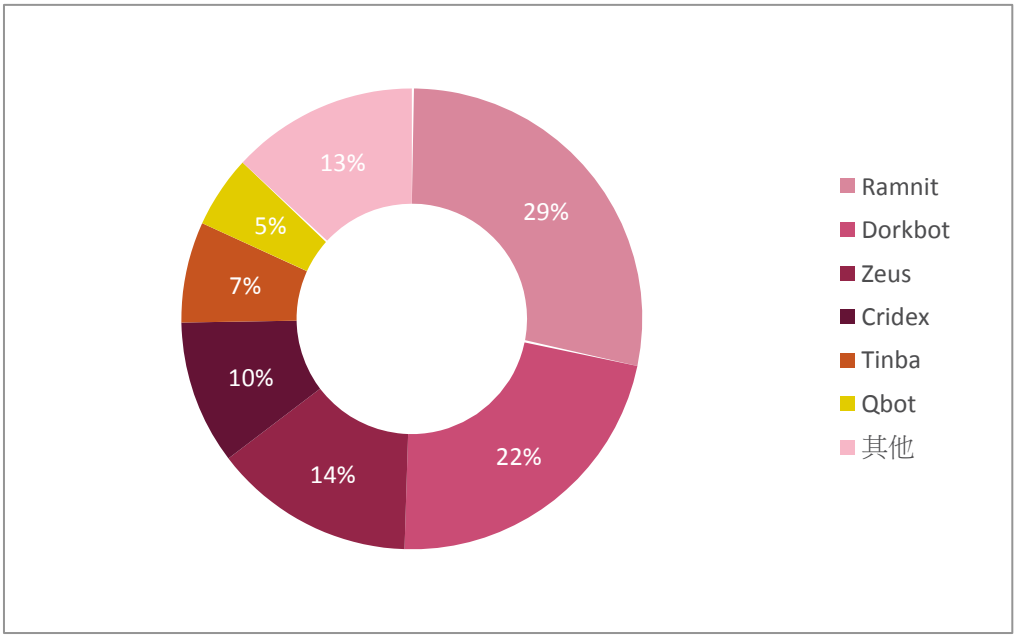


圖 17：美洲最普遍的銀行惡意軟體

歐非中東

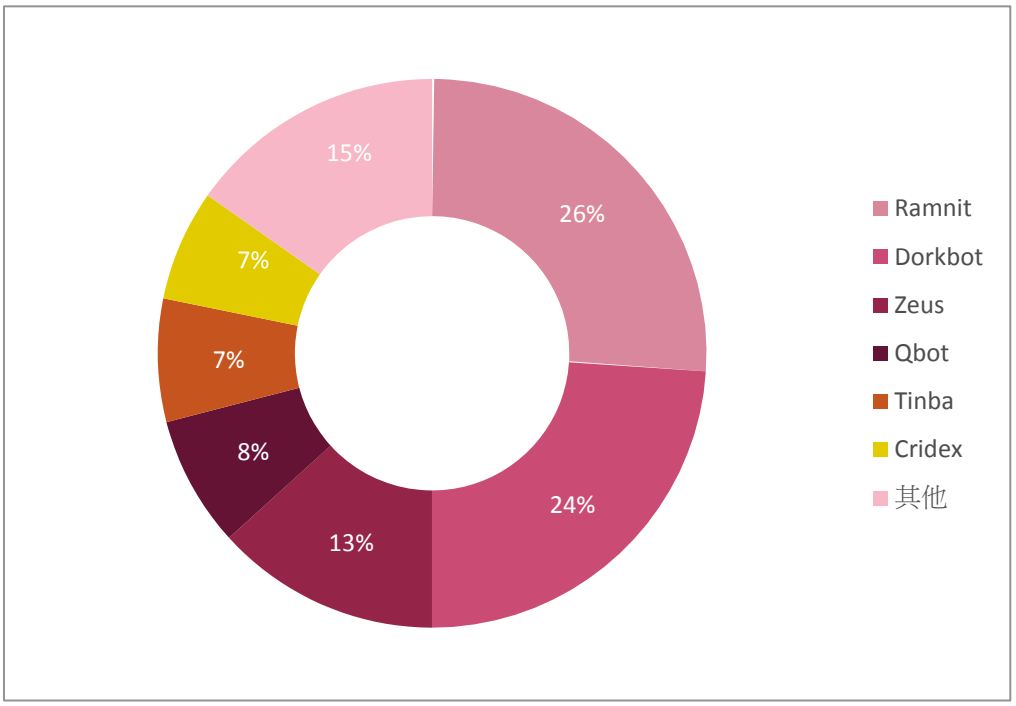


圖 18：歐非中東最普遍的銀行惡意軟體

亞太地區

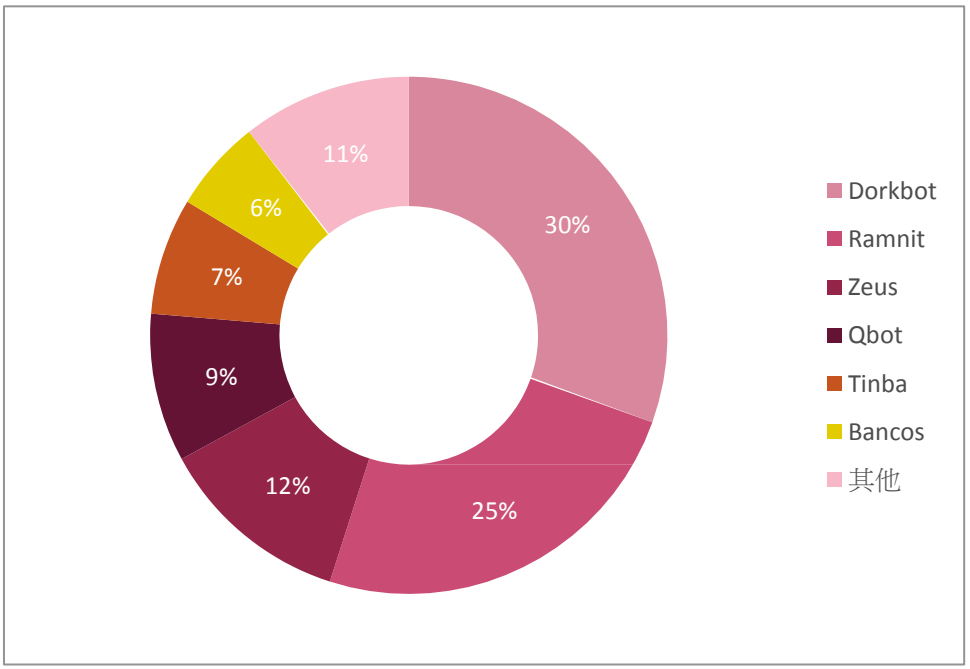


圖 19：亞太地區最普遍的銀行惡意軟體

銀行惡意軟體全球分析

最猖獗的銀行特洛伊木馬病毒，也就是稱霸全球主要銀行惡意軟體名單的 **Ramnit** 和 **Zeus**，自 2017 年下半年以來，始終在名單上名列前茅，地位久久不墜。兩者皆是存在已久且不斷進步的銀行特洛伊木馬病毒，能夠辨識造訪銀行交易網站的受害者，再利用鍵盤記錄或網頁注入等功能竊取登入認證或其他敏感資訊，例如 PIN 碼。此外，2012 年被發現的已知的惡意軟體 **Dorkbot** 再度重回排行榜，不但在亞太地區成為最常見的銀行惡意軟體，在美洲、歐非中東及全球也名列第二。Dorkbot 的功用是讓其幕後黑手能夠在遠端執行程式碼，主要目的就在於竊取敏感的銀行交易資訊；去年 4 月，人們發現這款惡意軟體會運用一種稱為「Early bird」的新式程式碼注入技術，以利規避防惡意軟體安全產品的偵測。

主要行動惡意軟體

報告中本節的圖表說明受各行動惡意軟體波及之組織的百分比。圖表內容說明主要行動惡意軟體肆虐全球及各區域的情勢。

全球

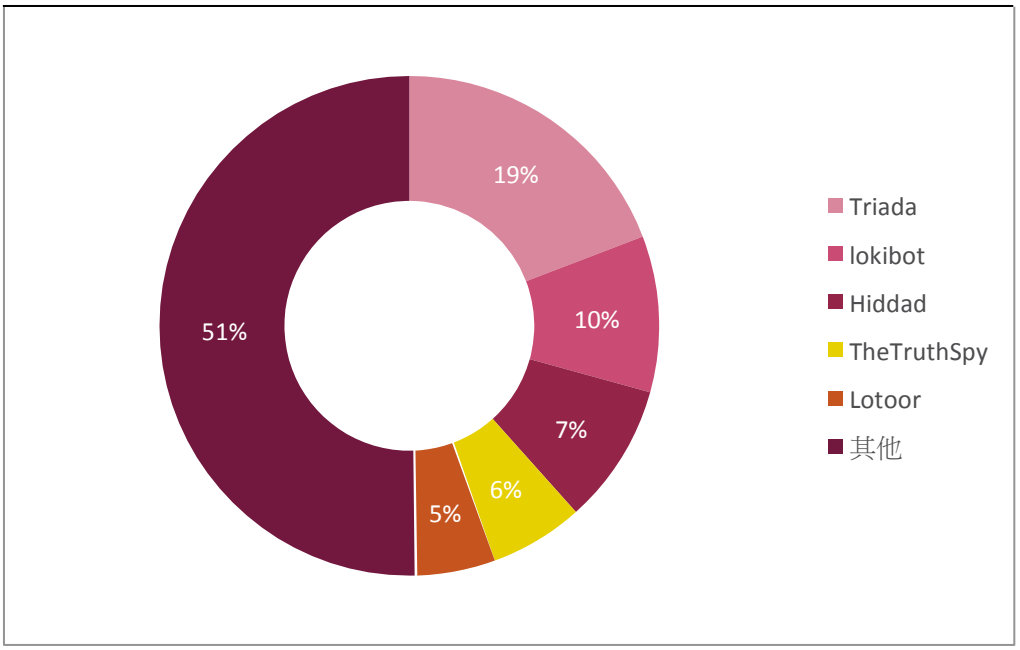


圖 20：全球主要行動惡意軟體

美洲

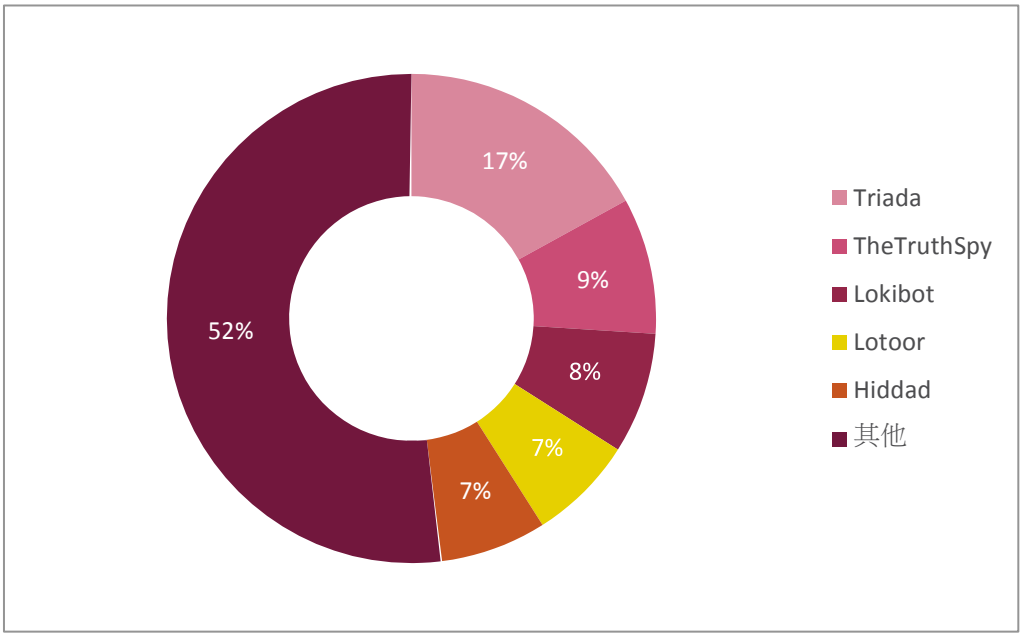


圖 21：美洲主要行動惡意軟體

歐非中東

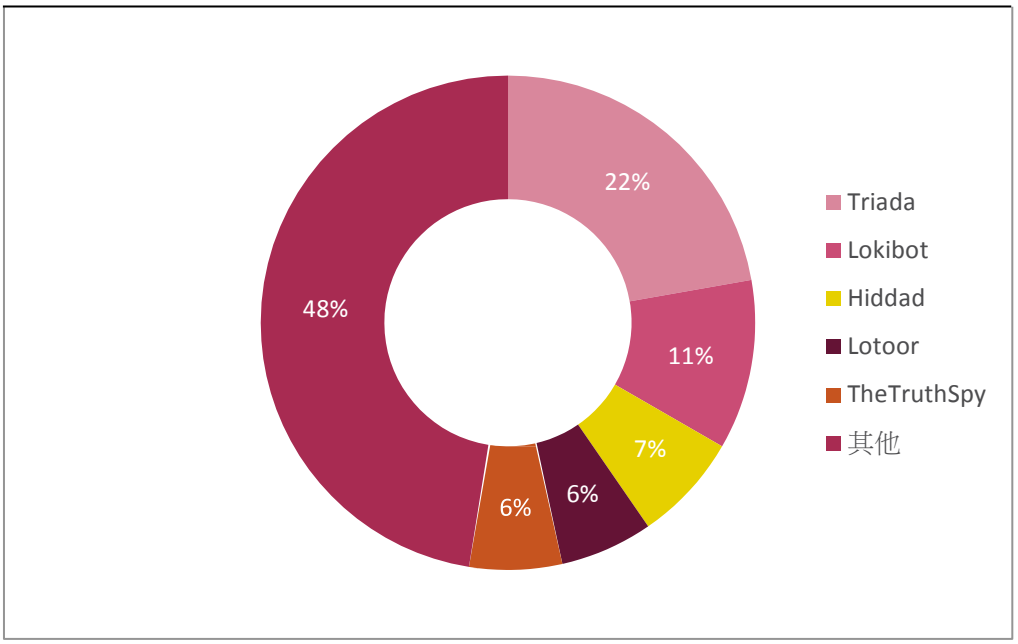


圖 22：歐非中東主要行動惡意軟體

亞太地區

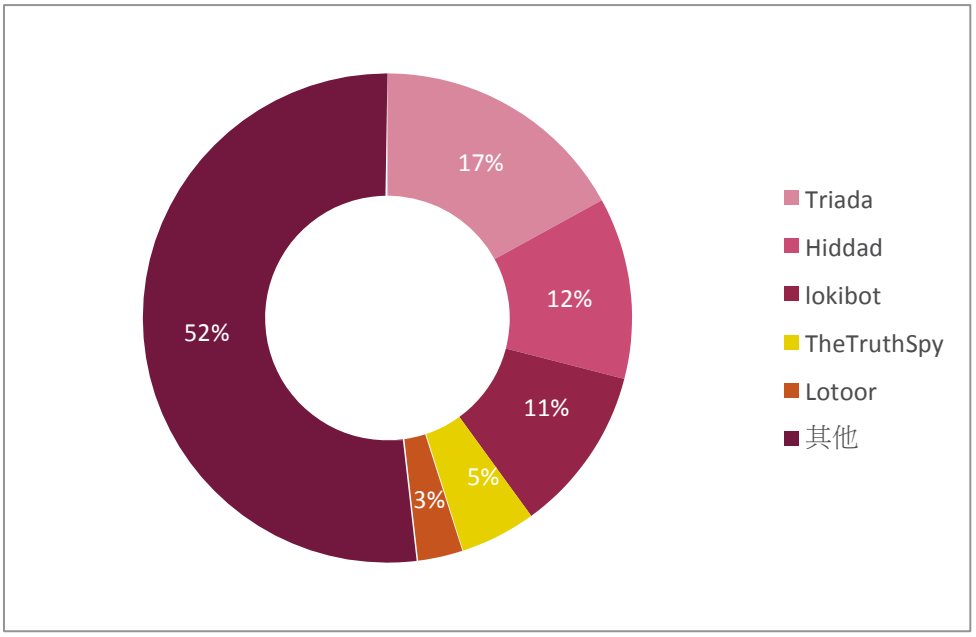
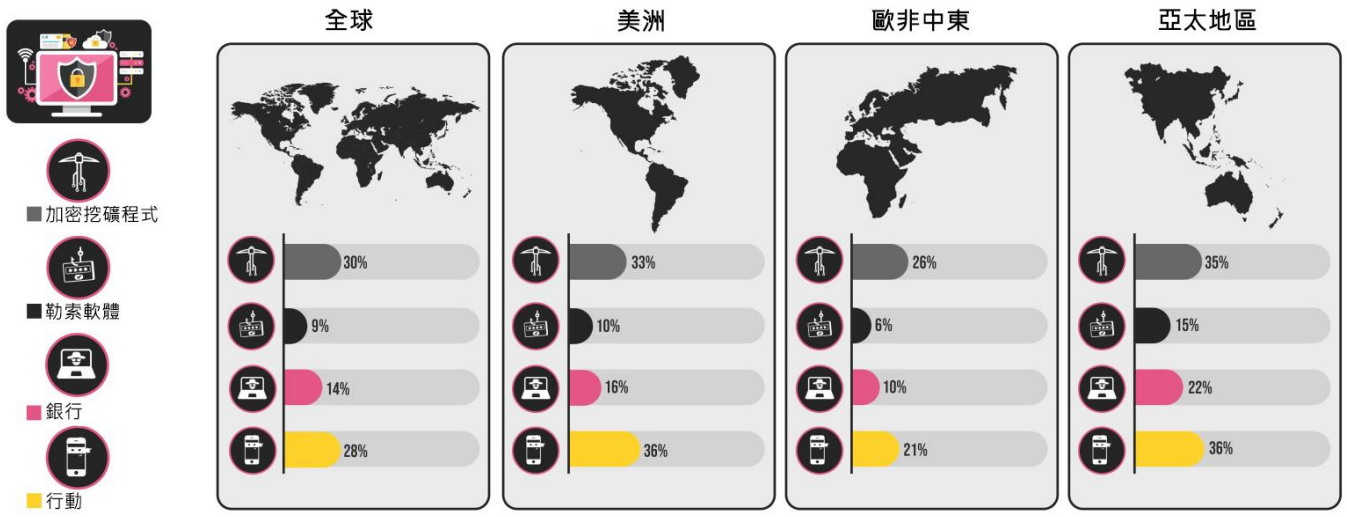


圖 23：亞太地區主要行動惡意軟體

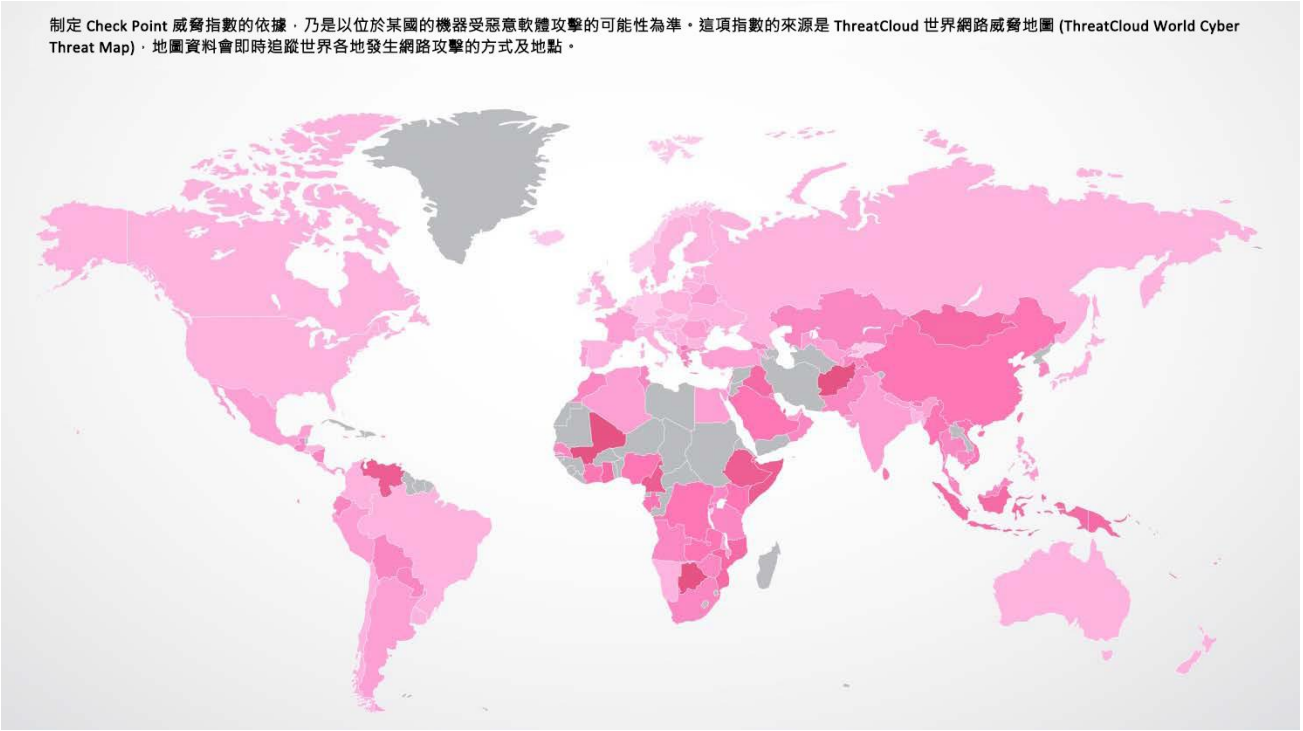
行動惡意軟體全球分析

Triada 是一款非常強大的 Android 銀行特洛伊木馬病毒，2016 年為人所知，是非常先進的行動威脅，目前位居全球及區域排行榜之首。去年 3 月，人們發現 42 款平價智慧型手機預先安裝了 Triada，無數受害者因此受到感染，信用卡資料也遭到盜用。更糟的是，排行榜上又多了 **TheTruthSpy** 這個全新的行動惡意軟體系列；這個系列的惡意軟體能夠監控 WhatsApp 訊息、Facebook 聊天內容以及網際網路瀏覽記錄。TheTruthSpy 才在 2018 年 5 月現蹤，就已經在全世界名列第三，更在歐非中東及亞太地區名列第二。

各地區的網路攻擊類別



全球威脅指數地圖



重大網路漏洞 (2018 上半年)

目前為止，2018 年的網路漏洞仍然影響著各行各業的公司行號，也讓數十億人口的敏感資訊暴露在風險之中。再者，所有區域全都遭逢數不清的攻擊，顯見威脅者鎖定的目標涵蓋所有地理位置。以下簡要說明各區域的大規模攻擊。

美洲

- **2 月**：威脅者挾持一個安全防護措施不夠完善的 MongoDB 資料庫後索討贖金，導致逾 1950 萬加州居民的選民登記資訊外洩。沙加緬度地方報 Sacramento Bee 坦承是外洩源頭，但拒付贖金，並將該資料庫刪除。
- **3 月**：知名健身公司「Under Armour」的應用程式 MyFitnessPal 發生嚴重外洩事件，令該公司備受其擾。該公司宣佈此次攻擊事件導致 1.5 億名應用程式使用者的資料外洩，使用者的姓名、電子郵件地址及雜湊密碼全數曝光。
- **3 月**：Orbitz 是 Expedia 旗下的旅遊網站，該公司宣佈遭到資料外洩攻擊，導致 880,000 筆用於線上購物的付款卡資料及其他屬於客戶的個人資訊全數曝光。事件發生時間在 2016 年 10 月到 2017 年 12 月之間。
- **4 月**：Saks Fifth Avenue 及 Lord & Taylor 的母公司 Hudson's Bay 發生公司付款系統遭受重大攻擊的事件，令該公司 備受其擾。發動攻擊的元凶是 FIN7 APT 團體，這個團體成功竊取了約五百萬名消費者的信用卡及金融卡資訊，受害者全都是曾經向這兩家零售商購物的消費者。
- **5 月**：資料採礦公司 Cambridge Analytica 遭控利用 Facebook 收集多達 8,700 萬人的個人詳細資料，只為鎖定美國 2016 年總統大選的選民。該公司利用一款應用程式成功收集到這類資料，只要使用者願意做一項人格測驗並同意應用程式收集資料，他們就會付錢給使用者。

歐洲、中東和非洲 (EMEA)

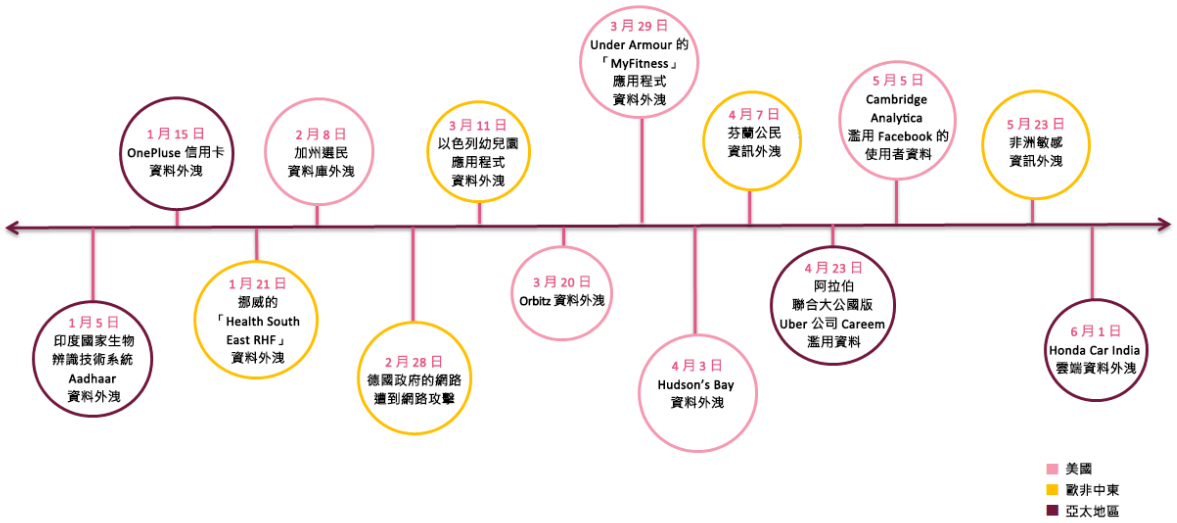
- **1 月**：挪威最大的衛生機關 Health South East RHF 發生資料外洩事件，影響所及廣達該國半數以上的人口。網路犯罪者竊取了約 290 萬名挪威居民的個人資訊和健康記錄。
- **2 月**：德國政府宣佈數個政府網路遭逢大規模網路攻擊，其中也包括一個獨立網路，所有遭到波及的網路都發生了資料外洩問題，感染惡意軟體的時間大約是一年。這次外洩事件是在 12 月發現的，該國內政部及其他未指明機關的伺服器都是攻擊對象。德國當局懷疑發動這場攻擊的幕後黑手是俄國駭客團體 APT28。

- **3 月**：一款名為「Remini」的應用程式遭逢嚴重安全漏洞攻擊，致使數百萬張以色列兒童的 相片及逾 100,000 名家長的個人詳細資料流入網際網路。幼兒園教師會運用這款應用程式與家長聯絡並分享任何相關資訊，包括課堂活動時間表、相片影片及個人資訊。
- **4 月**：芬蘭赫爾辛基的新商務中心 (New Business Center) 發生嚴重資料外洩事件，因而成為受害者 。
  威脅者竊取了逾 130,000 名使用者的登入使用者名稱和密碼，這些全都是以純文字格式存放於網站中的資料。
- **5 月**：某個資料庫發生資料外洩，資料庫中存放的近百萬名南非民眾的敏感個資流入網際網路。有關當局在一個屬於某公司行號的公開網頁伺服器上發現了這個資料庫，這家公司負責處理南非的交通罰款電子繳費事宜，而存放於資料庫中的資料則包括姓名、身分證件號碼、電子郵件地址以及密碼。

亞太地區 (APAC)

- **1 月**：Aadhaar 是印度的國家生物辨識技術系統，威脅者成功竊取逾十萬名印度民眾的個資，讓這個系統成為嚴重資料外洩事件的受害者。威脅者之後透過 WhatsApp 提供了一項付費服務，幫助受害者找回自己的資訊，包括姓名、地址、郵遞區號、相片、電話號碼以及電子郵件地址。
- **1 月**：中國智慧型手機製造商 OnePlus 發生信用卡資料外洩事件，波及該公司逾 40,000 名客戶。攻擊者在該公司的付款網頁程式碼中注入惡意指令碼，直接利用瀏覽器視窗成功竊取完整的信用卡資訊，其中包括信用卡卡號、到期日及安全碼。
- **4 月**：阿拉伯聯合大公國版 Uber 服務 Careem 遭駭客入侵，導致 1,400 萬名司機和客戶的私人資料失竊，其中包括他們的姓名、電話號碼、電子郵件及開車/搭車資料。
- **6 月**：Honda Car India 使用兩個不安全的 Amazon S3 公用貯體，導致逾 50,000 名使用者的個人資料外洩。外洩資料屬於 Honda Connect App 這款遠端汽車管理應用程式，資料內容則包括姓名、電話號碼、電子郵件、密碼、汽車識別號碼 (VIN)、汽車連線代碼等。

年中資料外洩時間軸



全球最常遭到利用的漏洞

下方所列的常見攻擊清單以 Check Point 入侵防護系統 (Intrusion Prevention System，IPS) 解決方案收集到的資料為準據，內容詳述 Check Point 研究人員在 2018 上半年觀察到的一部分熱門及引人注目的攻擊技術和漏洞攻擊。

Drupalgeddon2 和 Drupalgeddon3 (CVE-2018-7600、CVE-2018-7602)

Drupal 是一款強大的內容管理系統 (Content Management System，CMS)，這套系統出現了非常重大的瑕疵，對威脅環境造成相當大的影響。這些漏洞波及了上百萬個 Drupal 網站，未通過驗證的攻擊者可以趁著人們安裝 Drupal 時在遠端執行控制碼，利用這些漏洞全面控制受害網站。已經發佈的概念驗證導致未套用修補程式的 Drupal 網站不斷遭受攻擊。從植入於伺服器和網站的各類加密貨幣挖礦程式，乃至於散播 RAT 及資訊竊取惡意軟體、進行技術支援詐騙，以及製造大量的殭屍網路，各種攻擊手法包羅萬象，無奇不有。

RTF (CVE-2017-11882、CVE-2017-0199、CVE-2018-0802)

2018 上半年，威脅者肆無忌憚地濫用 Microsoft Office RTF 格式 (Rich Text Format)。只要使用者開啟惡意文件，攻擊者就能利用這些安全漏洞在目標電腦上進行下載，還能執行含 PowerShell 命令的惡意指令碼。今年許多惡意垃圾郵件活動廣泛利用這類漏洞，其中不乏幾項由 APT 團體發動的攻擊，而各類惡意軟體用於偽裝下載程式的文件中也經常利用這些漏洞。經常利用這些漏洞的惡意軟體包括 LockyBot、Remcos RAT、 KevDroid Android RAT、ThreadKit 漏洞攻擊建立工具套件，以及 Zyklon。

「Double Kill」(CVE-2018-8174)

Double Kill 是存在於 Windows VBScript 引擎的遠端程式碼執行 Internet Explorer (IE) 零時差漏洞，會影響 IE 的最新版本，以及任何其他運用 IE 元件的應用程式。遠端攻擊者可以利用這個漏洞，在 Office 文件或網站中嵌入惡意 VBScript，然後在遠端伺服器上執行惡意封包內容。在瀏覽器中發現零時差漏洞已經是兩年前的事了，而此次事件更成為 2018 年的熱門新聞，因此也給了 APT-C-06 團體和惡名昭彰的 RIG 漏洞攻擊套件等威脅者一個機會，利用這一漏洞傳播門羅幣加密貨幣挖礦程式。

IoT 漏洞 (CVE-2018-10561、CVE-2018-10562)

逾百萬台 Dasan GPON 家用路由器在今年遭爆出現安全瑕疵，因此這類裝置容易遭受各式各樣的攻擊。任何攻擊者都能利用這些漏洞在任何 URL 附加某個字串，進入路由器設定後，輕而易舉就能奪得裝置控制權。殭屍網路首腦大舉利用這些漏洞壯大陣容，其中包括 Satori、Mirai 及 TheMoon 等殭屍網路。

有趣的是，根據 Check Point 的全球攻擊感應器在 2018 上半年觀察到的結果，99% 的攻擊利用的是在 2017 年或更早之前出現的漏洞，更有 40% 以上的攻擊是利用至少七年前出現的漏洞。

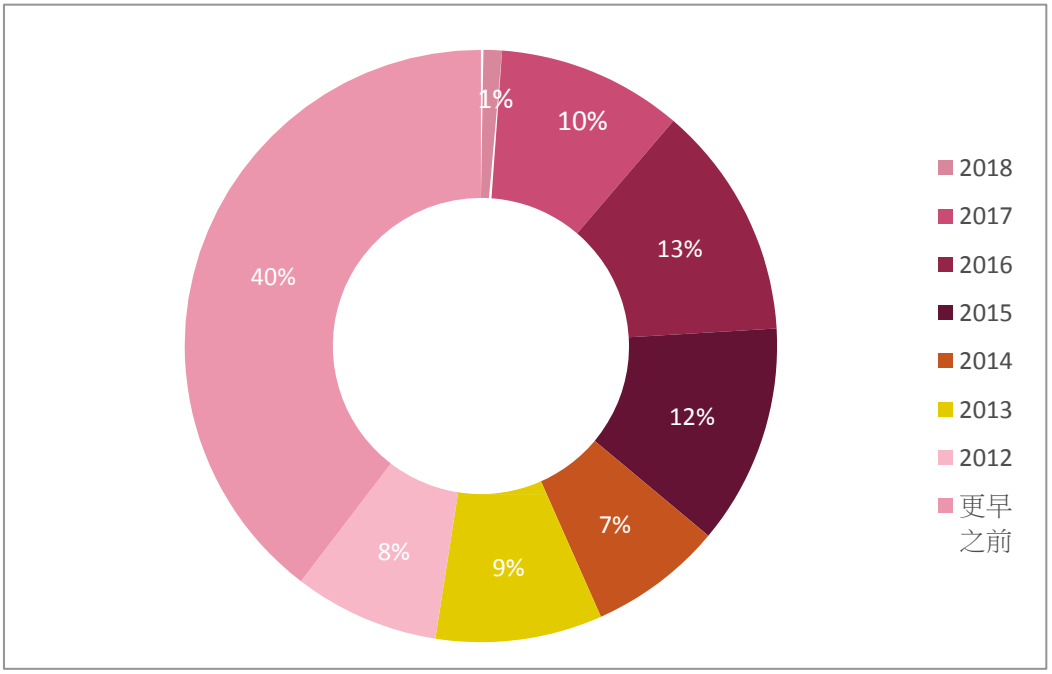


圖 24：攻擊利用 2012 年及更早之前發現之漏洞的百分比。

其他觀察結果/結論

第五代網路威脅環境如今大勢底定，不出所料，2017 年浮現的威脅類型繼續延燒到 2018 年。這些威脅類型絲毫沒有放慢速度的跡象。要說有什麼特別之處，那就是這些威脅的防衛能力越來越強，現在也已經開始近一步深入企業組織的 IT 基礎架構內部。

無論是透過行動供應鏈中預先安裝的惡意軟體自行嵌入，或是利用雲端平台的高等運算資源挖掘珍貴的加密貨幣，威脅者只會不斷利用現代技術為己牟利。此外，大規模資料外洩問題絲毫沒有減輕，也讓遭受攻擊的目標蒙受莫大的信譽及財務損失。

因此，全球企業組織普遍開始運用最高階先進的防護技術自我防衛，希望能夠搶在攻擊趨勢前頭，避免本身成為下一個登上頭條版面的受害者。

建議

您需要選擇先進的防護技術，幫助您識別來自未知攻擊以及更老練且能規避傳統特徵技術的攻擊，為您提供零時差防護。

Check Point Sand Blast 能夠提供這樣的技術，其重點包含以下兩大要素：
威脅模擬與威脅萃取。

威脅模擬是非常強大的防規避沙箱技術，能夠主動結合威脅萃取技術，將安全無毒的檔案交付給使用者。一方面只允許安全無毒檔案進入企業組織內部的主動防護法，另一方面威脅模擬技術則能識別企圖進入網路的零時差及未知的惡意軟體，綜合運用以上兩大要素，您就能夠安心防範一般網路攻擊的未知手法，尤其不用擔心加密貨幣挖礦攻擊。

Sand Blast 也包括一系列專為防護整個 IT 基礎架構而設計的產品。

Sand Blast 適用於所有 Check Point 閘道，能夠妥善保護您的郵件、在您的網路中瀏覽網頁的使用者，以及您的資料中心。

根據目前所見的情況，網頁瀏覽是最容易遭受攻擊的活動；Sand Blast 代理程式安裝於端點上，能夠直接運用先進技術防護所有端點，也能針對端點內瀏覽器發揮整合式防護作用。

Sand Blast 也是 Cloud Guard 不可或缺的核心要素，能夠同時保護 SaaS 和 IaaS，讓您的所有雲端資產也能全數躲在這項先進技術的保護傘下。

Sand Blast Mobile 能防護 iOS 及 Android 裝置，抵禦各類已知及未知的行動攻擊，包括透過 Wi-Fi 網路發動的中間人攻擊，以及經由 SMS 和 OS 攻擊漏洞傳送的惡意連結。

Sand Blast 還隨附一個 API，因此，倘若您尚未運用 Sand Blast 系列的其他產品嚴密防護某些業務流程或業務邏輯，也可以將 Sand Blast 的功能與這些業務流程或業務邏輯整合起來。

附錄 – 惡意軟體系列說明

Andromeda	Andromeda 是模組化惡意活動殭屍程式 (Bot)，於 2011 年首度浮出檯面。其主要用途是能在遭感染的主機上散播其他惡意軟體的後門程式，但若經過修改，也能製造出不同類型的殭屍網路。
AndroRAT	AndroRAT 是鎖定 Android 裝置的開放原始碼工具，初次現蹤是在 2012 年。AndroRAT 可以讓遠端攻擊者掌控受害者的電腦；利用遭感染的裝置打電話及傳簡訊；取得受害者的 GPS 座標；以及使用麥克風和相機。

Authedmine	Authedmine 是惡名昭彰的 JavaScript 挖礦程式 CoinHive 的其中一個版本。Authedmine 與 CoinHive 類似，是一種網頁加密貨幣挖礦程式，會趁著使用者造訪網頁之際，在使用者未察覺或未同意的情況下上線挖掘門羅幣這種加密貨幣，假使用者之手大肆牟利。不過，Authedmine 不像 CoinHive，未經網站使用者明確同意前，Authedmine 無法執行挖礦指令碼。
Bancos	Bancos 利用鍵盤記錄功能，趁受害者在目標銀行網頁輸入資訊時記下其認證，藉以竊取財務資訊。Bancos 也可以使用偽造的網頁，補充或取代真正的銀行登入頁面。
Cerber	Cerber 也稱為 Zerber，2016 年 2 月初次為人所知這是一款離線勒索軟體，也就是說，它不需要與其 C2 伺服器通訊就能將遭感染電腦上的檔案加密。
Coinhive	這是一款加密貨幣挖礦程式，會在使用者造訪網頁之際，在未經使用者同意的情況下上線挖掘門羅幣加密貨幣。威脅者植入的 JS 會在一般使用者的電腦上耗用大量運算資源，因此會影響電腦效能。
Cridex	Cridex 是攻擊 Windows 平台的蠕蟲，會試圖竊取受害者的認證資料，例如信用卡資訊。它可以在遭感染的系統上下載及執行其他惡意檔案，還能經由抽取式磁碟及網路共用區自行散播。
Cryptolocker	Cryptolocker 是一款鎖定 Windows 平台的勒索軟體，第一次被偵測到的時間點在 2013 年。Cryptolocker 會在背景執行，入侵主機後將它所找到的各種檔案及文件加密起來。
Cryptoloot	這是一款 JavaScript 加密貨幣挖礦程式，會在使用者造訪網頁之際，在未經使用者同意的情況下上線挖掘門羅幣加密貨幣。威脅者植入的 JS 會在一般使用者的電腦上耗用大量運算資源，因此會影響電腦效能。Cryptoloot 是 Coinhive 的競爭對手。
Cryptopool	這是一款網頁加密貨幣挖礦程式，會在使用者造訪網頁之際，在未經使用者同意的情況下上線挖掘門羅幣加密貨幣。 威脅者植入的 JavaScript 會在一般使用者的電腦上耗用大量運算資源，因此會影響電腦效能。

Cryptowall	Cryptowall 是相當知名的勒索軟體特洛伊木馬病毒，會在遭感染的電腦上將檔案加密，使用者必須付贖金才能將檔案解密。這種病毒的散播途徑是惡意廣告及網路釣魚活動。Cryptowall 在 2014 首度現蹤。
Dorkbot	IRC 蠕蟲的設計原理是允許操作者在遠端執行程式碼，同時可以將其他惡意軟體下載至受感染的系統，主要動機就是為了竊取敏感資訊及發動阻斷服務攻擊。
Dorvku	Dorvku 是以 Windows 平台為目標的特洛伊木馬病毒。這款惡意軟體會收集系統資訊，再將資訊傳送至遠端伺服器。此外，它還會利用鎖定的網頁瀏覽器收集敏感資訊。
Fireball	Fireball 是由中國數位行銷公司卿燁科技 (Rafotech) 大肆散播的廣告軟體。這是一種瀏覽器綁架軟體，會更改預設搜尋引擎並安裝追蹤像素，但也可以變成功能完整的惡意軟體下載程式。
Gamarue	Gamarue 是含下載程式的模組化殭屍程式，會自其 C&C 伺服器下載其他模組。其下載程式具備防 VM 及防偵錯功能。Gamarue 的注入目標是受信任的處理序，藏匿其中後再刪除原始的殭屍程式。
GandCrab	GandCrab 是一款勒索軟體，主要目標是英語系國家/地區。GandCrab 會經由 Rig 和 GrandSoft 漏洞攻擊套件及垃圾電子郵件散播。這款勒索軟體採加盟方案模式運作，參加方案者須將贖金收入的 30%-40% 付給 GandCrab 撰寫者。加盟者能夠得到的則是一個功能完備的網頁介面以及技術支援。
Globeimposter	GlobeImposter 是一款勒索軟體，會喬裝成另一款名為 Globe 的勒索軟體。人們在 2017 年 5 月初次發現 Globeimposter，其散播途徑包括垃圾行銷活動、惡意廣告，以及漏洞攻擊套件。

Graftor	Graftor 既是廣告軟體，也是一款功能類似特洛伊木馬病毒的瀏覽器綁架軟體，更是可供其他惡意軟體利用的攻擊向量。此外，它還能將可執行檔及 DLL 暗藏在 PNG 檔案中，以利規避偵測技術
HackerDefender	HackerDefender 是用於 Windows 2000 及 Windows XP 的 Rootkit，也適用於更新款的 Windows NT 系統。 這款 Rootkit 會修改數種 Windows 及原生 API 功能，讓安全軟體無法偵測其存在。
Hiddad	一款 Android 惡意軟體，能重新包裝合法應用程式，再將其發佈至第三方商店。其主要功能是顯示廣告，但也能存取內建於作業系統的重要安全性詳細資料
HiddenMiner	這是在 2018 年 4 月發現的一種 Android 加密貨幣挖礦程式病毒株。HiddenMiner is 會透過假的 Google Play 更新應用程式散播，再耗盡裝置資源來挖掘門羅幣。
Jsecoin	這是一款網頁加密貨幣挖礦程式，會在使用者造訪網頁之際，在未經使用者同意的情況下上線挖掘門羅幣加密貨幣。威脅者植入的 JavaScript 會在一般使用者的電腦上耗用大量運算資源，因此會影響電腦效能。
Kraken	Kraken 是以 Windows 平台為目標的勒索軟體特洛伊木馬病毒。這款惡意軟體會收集系統資訊，再利用 Discord 聊天服務將收集到的資訊傳送給遠端攻擊者。這款惡意軟體會將遭感染系統中使用特定副檔名的檔案加密。它會在遭感染的系統上下載及執行解密程式，藉此要求受害使用者付解密贖金。Kraken 還能強制終止處理序。
Locky	Locky 是以 Windows 平台為目標的勒索軟體特洛伊木馬病毒。這款惡意軟體會將系統資訊傳送至某個遠端伺服器，然後接收可在遭感染系統上加密檔案的加密金鑰。
Lokibot	這是一款行動銀行特洛伊木馬病毒，會鎖定 Android 智慧型手機，只要使用者試著移除 Lokibot 的管理權限，它就會轉變成勒索軟體。LokiBot 主要是銀行特洛伊木馬病毒，能蓋過常用的銀行交易應用程式並顯示假的登入畫面。 這類銀行勒索軟體的原始設計是以行動銀行交易應用程式為對象，不過也會鎖定 WhatsApp、Outlook 及 Skype 等其他熱門應用程式。

Lotoor	Lotoor 是一款駭客工具，能夠入侵 Android 作業系統的漏洞，在遭駭的行動裝置上掌握 Root 權限。
Necurs	在目前肆虐於全球的垃圾郵件殭屍網路中，Necurs 的規模數一數二，根據估計，它在 2016 年的殭屍程式數量就已經高達 600 萬之譜。這款殭屍網路的用途是大量散播惡意軟體變種，其中尤以銀行特洛伊木馬病毒及勒索軟體為主。
Nivdort	Nivdort 是以 Windows 平台為目標的特洛伊木馬病毒系列。 它會收集密碼及系統資訊，或者是設置 Windows 版本、IP 位址、軟體組態以及大致位置等設定。
Nymaim	Nymaim 是惡意軟體植入程式，第一次浮出檯面是在 2013 年。 Nymaim 起初是經由黑洞漏洞攻擊套件 (Black Hole Exploit Kit) 散播，成功後再植入勒索軟體。後來，Nymain 也開始傳播其他類型的惡意軟體，例如 Vawtrak、Miuref、Pony 和 Ursnif。這款惡意軟體的散播攻勢在 2014 稍降，2015 年卻又再度活躍了起來。
Panda	Panda 是 Zeus 的變種，2016 年年初首度現蹤，會經由漏洞攻擊套件散播。Panda 一出現就鎖定歐洲和北美的金融機構。在 2016 年奧運會之前，Panda 也針對巴西銀行發動了一場特別的攻擊活動。
Parite	Parite 是一種千面人病毒 (polymorphic virus)，會感染受害主機和網路硬碟中的可執行檔 (EXE 及 SCR)。它會在 Windows 暫存資料夾中植入一個惡意 DLL 檔 (注入於 explorer.exe 處理序)。
Ponmocup	Ponmocup 是從 2006 年開始活躍至今的殭屍網路，2011 年達到巔峰，當時受到控制的電腦大約有 240 萬台。其基礎架構相當複雜，還包含了用於處理各種任務的專用伺服器。
Proslikefan	Proslikefan 是一種蠕蟲，會鎖定支援 JavaScript 的 Windows 系統。 這款惡意程式會試圖經由網路共用區、抽取式磁碟以及點對點程式散播。它會試圖將系統資訊傳送至遠端伺服器。

Qbot	Qbot 是屬於 Qakbot 系列的後門程式，能植入及下載其他惡意程式。它還會在未經使用者同意的情況下連上遠端 HTTP 伺服器，然後竊取敏感資訊。
Ramnit	Ramnit 是銀行特洛伊木馬病毒，能合併橫向移動功能。Ramnit 會竊取網頁工作階段資訊，讓蠕蟲操作者能夠竊取使用者所用之所有服務的帳戶認證資料，包括銀行帳戶、公司網路帳戶以及社交網路帳戶。
Rig 漏洞攻擊套件	Rig EK 在 2014 年 4 月初次浮出檯面。此後經過數次大規模更新，迄今仍然十分猖獗。Rig 為許多威脅者效力，會在順利入侵受害者後開始散播其惡意軟體。
Roaming Mantis	Roaming Mantis 是一款 Android 銀行特洛伊木馬病毒，2018 年 3 月初次現蹤，能夠竊取使用者的敏感資訊、登入認證資料以及兩階段驗證密碼。Roaming Mantis 會偽裝成 Chrome 瀏覽器或 Facebook 應用程式，再經由 DNS 綁架攻擊進行散播。Roaming Mantis 的進化版還能鎖定 iOS 裝置發動網路釣魚攻擊，並且能夠利用 CoinHive 加密貨幣挖礦指令碼入侵桌上型電腦及筆記型電腦。
RottenSys	RottenSys 是一款廣泛散播的 Android 特洛伊木馬病毒，目前已經鎖定的目標達近 500 萬台 Android 裝置。RottenSys 會偽裝成正常的「系統 Wi-Fi 服務」應用程式，並預先安裝於裝置上。RottenSys 惡意軟體原本的用途是在使用者的裝置上大量顯示廣告，但也具備相當多其他功能，包括偷偷安裝其他應用程式及 UI 自動化功能。
Roughted	這是一種大規模惡意廣告活動，用於顯示各種惡意網站及封包內容，例如詐騙程式、廣告軟體以及勒索軟體。可用於攻擊任何類型的平台和作業系統，而且會利用廣告封鎖程式規避技術及指紋辨識技術。

RubyMiner	Rubyminer 是門羅幣加密軟體挖礦程式，會鎖定 Windows 和 Linux 伺服器，試圖找出易受攻擊的版本 (例如 PHP、Microsoft IIS 和 Ruby on Rails)，從而利用這些版本充當挖礦工具，然後安裝名為 XMRig 的開放原始碼門羅幣挖礦程式。
Sality	Sality 是一種病毒，會透過感染 .exe 及 .scr 檔案自行散播，也能經由抽取式硬碟及網路共用區散播。遭 Sality 感染的系統可以透過點對點 (peer-to-peer，P2P) 網路通訊，達到發送垃圾郵件的目的。
Smokeloader	SmokeLoader 是一款特洛伊木馬病毒，可讓攻擊者遠端控制遭到感染的電腦並執行各式各樣惡意活動，包括根據受害者的地理位置下載及安裝其他惡意軟體，以及竊取密碼。
TheTruthSpy	一款在 2017 年 5 月出現的 Android 間諜軟體。TruthSpy 能監控 WhatsApp 訊息、Facebook 聊天內容以及網際網路瀏覽記錄。
Tinba	Tinba 是銀行特洛伊木馬病毒，主要鎖定歐洲銀行客戶，並且會利用黑洞漏洞攻擊套件。Tinba 會利用網頁注入竊取受害者的認證資料，一旦使用者試著連上自己的帳戶，就會啟動這項功能。
Triada	這是一款 Android 模組化後門程式，會授予高階使用者權限，允許其下載惡意軟體。Triada 也會假冒載入至瀏覽器中的 URL。
TrickBot	Trickbot 是在 2016 年 10 月出現的 Dyre 變種。Trickbot 從一開始便以鎖定澳洲及英國地區的銀行為主，最近也開始出現在印度、新加坡及馬來西亞。
WannaCry	2017 年 5 月趁著一場大規模攻擊散播的勒索軟體，其散播手法是利用名為永恆之藍 (EternalBlue) 的 Windows SMB 漏洞，在網路內部與不同網路之間大肆傳播。
XMRig	XMRig 是開放原始碼 CPU 探勘軟體，會鎖定處理序進行門羅幣加密貨幣挖礦作業，初次現蹤的時間是 2017 年 5 月。
Zeus	Zeus 是一款大規模散播的 Windows 特洛伊木馬病毒，主要用於竊取銀行交易資訊。只要電腦遭到入侵，這款惡意軟體就會利用 C&C 伺服器鏈，將帳戶認證資料等資訊傳送給攻擊者。