卡巴斯基 APT 情報報告提供：

- 在持續調查期間、搶在公開發布之前**獨家取得**先進威脅的技術說明。
- **洞察非公開的 APT。**並非所有備受關注的威脅都會公開通知。被影響的受害者、資料機密性、弱點修正程序性質或相關執法活動等原因，都可能使部分威脅不會公開。不過所有威脅都會向我們的客戶回報。
- **詳細支援**的技術資料，包括 OpenIOC 或 STIX 等標準格式的入侵指標 (IOC) 擴充清單，並可存取我們的 Yara 規則。
- **持續監控 APT 活動。**取得調查期間的可行動情報 (APT 分佈、IOC、命令與控制項基礎結構等資訊)。
- **適用於不同對象的內容。**每份報告都包含管理階層導向的執行摘要，以容易理解的方式說明相關的 APT。執行摘要之後是詳細的 APT 技術說明，其中包含相關 IOC 和 Yara 規則，可以為安全研究人員、惡意程式分析師、安全工程師、網路安全分析師，以及 APT 研究人員提供可據以行動的建議，以實現對相關威脅的優異防護。
- **追溯分析。**訂閱期間均可取用所有先前發布的私人報告。
- **APT 情報入口網站。**包括最近 IoC 在內的所有報告，都可以透過我們的 APT 情報入口網站取得，為我們的客戶建立順暢的使用者體驗。API 也可以在此取得。

注意 - 訂閱者限制

由於本服務提供的報告含有部分敏感性和特定性質的資訊，我們有責任將訂閱對象限制為信任的政府、公眾及私人組織。

APT 情報報告

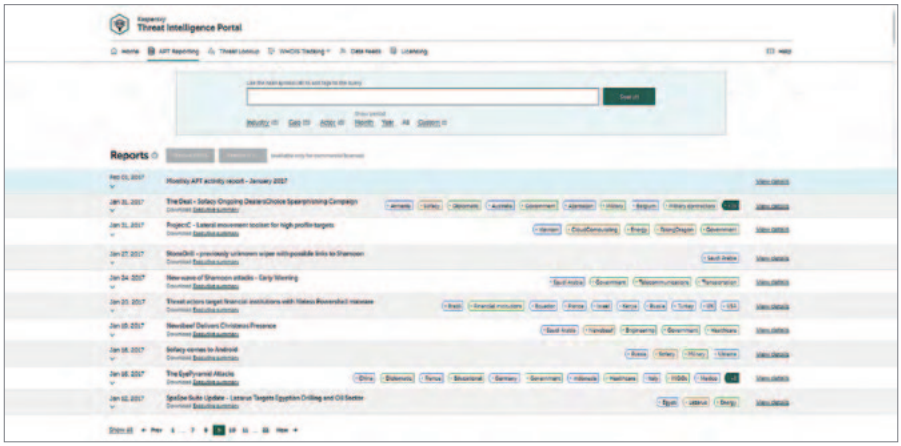
透過卡巴斯基實驗室提供的全方位實用報告，提升備受關注網路間諜活動方面的認知與知識。

運用報告提供的資訊可讓您迅速回應全新威脅和弱點 - 阻擋透過已知媒介發動的攻擊、減少進階攻擊造成的損害，以及強化您或客戶的安全策略。

卡巴斯基實驗室發現了許多有史以來最重大的 APT 攻擊。不過，並非所有發現的進階持續性威脅都會立即回報，有許多威脅從未公開過。

如果訂閱卡巴斯基 APT 情報報告，我們會持續獨家提供您各項調查與發現，包括以各種格式提供的完整技術資料；在 APT 揭露後便會報告，並包括不為人知的威脅。在 2016 年間，我們建立了超過 100 份報告！

我們的專家是業界中具備高度專業技能、也是最成功的 APT 獵人；如果偵測到網路犯罪團體的手段出現任何改變，就會立即向您提出警告。您也可以使用卡巴斯基實驗室的完整 APT 報告資料庫 - 加入到您企業的安全武裝，進一步強化研究和分析元件。



量身訂做的威脅報告

客戶專屬的威脅報告

攻擊貴企業組織的最佳方式為何？當攻擊者專門針對您時，可採用哪些路徑或哪些資訊？是否已經發動攻擊，或者您即將受到威脅？

卡巴斯基的客戶專屬威脅報告不僅可為您解答上述問題，還能提供更多資訊；我們的專家可針對目前的攻擊狀態拼湊出完整樣貌、找出可實行入侵的弱點，並揭露過去、現在及預計的攻擊證據。

有了這項獨特見解，您可以專心擬定防禦策略來防範網路犯罪者的主要目標區域、迅速採取精準行動以驅逐入侵者，將攻擊成功的風險降到最低。

這些報告開發時使用開放原始碼情報 (OSINT)、卡巴斯基實驗室專家系統與資料庫的深度分析，以及我們手邊有關網路犯罪者地下網路的相關知識，而報告涵蓋的領域包括：

- **辨識威脅媒介：**辨識您網路中外部可用的重要元件並進行狀態分析，包括 ATM、視訊監控和其他使用行動技術的系統、員工社群網路設定檔及個人電子郵件帳戶等，這些都是潛在的攻擊目標。

- **惡意程式和網路攻擊追蹤分析：**辨識、監控及分析鎖定貴企業組織的任何活動中或非活動中惡意程式樣本、任何過去或現在的殭屍網路活動，以及任何可疑的網路式活動。

- **第三方攻擊:**將您的客戶、合作夥伴及訂閱者作為目標的威脅和殭屍網路活動證據，攻擊者可能使用這些受感染的系統攻擊您。

- **資訊洩漏：**我們仔細監控地下線上論壇和社群，可發現駭客是否正在討論攻擊您的計畫；或是舉例而言，是否有不法員工正在進行資訊交易。

- **目前的攻擊狀態：**APT 攻擊可以持續好幾年都偵測不到。如果我們偵測到目前影響您基礎結構的攻擊，會提供有效修復的相關建議。

快速啟動、輕鬆使用且無須資源

一旦建立參數和偏好的資料格式，便無須使用額外的基礎結構啟用卡巴斯基實驗室服務。

卡巴斯基量身訂做的威脅報告不會影響資源 (包括網路資源) 的完整性與可用性。

服務能夠以一次完成專案或定期訂閱 (例如每季) 的方式提供。

國家專屬的威脅報告

國家的網路安全包括對其所有主要機構和組織的防護。對政府機關發動的進階持續性威脅 (APT) 可能會影響國家安全；針對製造、運輸、電信、銀行和其他關鍵產業的網路攻擊可能會導致財務損失、生產事故、網路通訊封鎖，以及民怨等國家層級的重大損失。

如果您對鎖定貴國的惡意程式與駭客攻擊目前的攻擊面和趨勢有所了解，即可將防禦策略的重點放在已經指出的網路犯罪者主要目標領域、迅速採取精準行動以驅逐入侵者，將攻擊成功的風險降到最低。

國家專屬的威脅報告在建立時使用開放原始碼情報 (OSINT)、卡巴斯基實驗室專家系統與資料庫的深度分析，我們手邊有關網路犯罪者地下網路的相關知識等方法，這些報告涵蓋的領域包括：

- **辨識威脅媒介：**國家外部可用重要 IT 資源的辨識與狀態分析 - 包括容易遭到攻擊的政府應用程式、電信設備、工業控制系統的原件 (例如，SCADA、PLC 等)、ATM 等。

- **惡意程式和網路攻擊追蹤分析：**鎖定貴國的 APT 活動、活動中或非活動中的惡意程式樣本、過去或現在的殭屍網路活動，以及其他知名威脅，是根據我們獨家內部監控資源中的可用資料進行辨識與分析。

- **資訊洩漏：**透過對秘密論壇與線上社群的秘密監控，我們便能發現駭客是否正在討論攻擊計畫，準備向特定組織發動攻擊。對於遭到入侵之後，可能會讓受害企業組織和機構暴露於風險中的知名帳戶，我們也會予以揭露 (例如在 Ashley Madison 入侵事件中，可能會被用來發送黑函、屬於政府機構員工的帳戶)。

卡巴斯基威脅情報報告不會影響受檢查網路資源的完整性與可用性。這項服務是以非侵入性的網路偵察方法，以及公開來源和限制存取資源中可用資訊的分析為基礎。

您將在服務的總結階段獲得一份報告，內含不同國家產業與機構的知名威脅說明，以及詳細技術分析結果的額外資訊。報告會透過加密的電子郵件訊息提供。