KASPERSKY lab

卡巴斯基
網路安全服務
2018

www.kaspersky.com

真正的網路安全

網路犯罪無國界，犯罪技術更是進步神速：我們都清楚網路攻擊變得越來越複雜，我們的使命就是協助全球防範各類型的網路威脅。為了達到此目標並落實網際網路的使用安全，即時分享威脅情報至關重要。持續有效防護資料和網路的關鍵，就在於即時存取資訊。

尤金卡巴斯基 (Eugene Kaspersky)
卡巴斯基實驗室董事長兼執行長

簡介

每天出現的網路威脅越來越多，不僅偽裝形式各異，更透過許多不同的媒介攻擊。

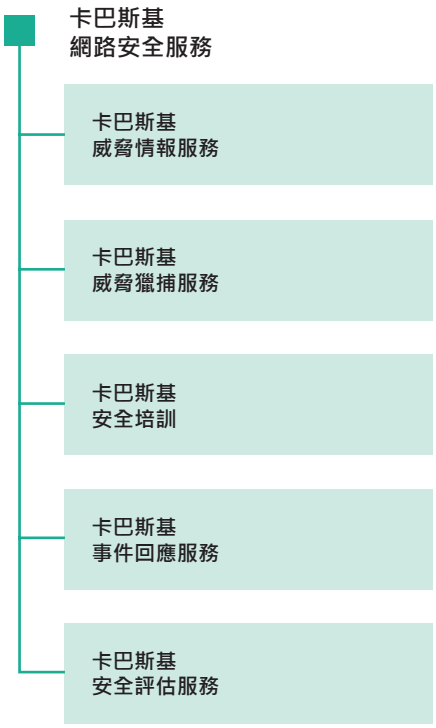
沒有任何單一解決方案能夠提供全方位防護。然而，在大數據的領域中，了解從何尋找危險對於對抗最新威脅很有幫助。

身為一位業務經理人，您需要負責保護貴企業組織對抗現今威脅，並預測未來幾年可能出現的危險。不僅需要透過智慧的營運防護來防範已知威脅，還需要具備一定水準的策略安全情報；企業通常沒有這樣的內部開發資源。

卡巴斯基實驗室了解，只有長期持久的關係才能持續為企業帶來繁榮。

卡巴斯基實驗室隨時透過各種管道與您的團隊分享最新情報，是能為您帶來重大價值的企業合作夥伴。我們提供各式各樣的交付方式，協助您的安全營運中心 (SOC)/IT 安全團隊隨時做好準備，保護企業組織免受任何線上威脅。

即便貴企業組織未使用卡巴斯基實驗室的產品，仍可享有卡巴斯基實驗室網路安全服務。



全球頂尖的安全

我們掌握領先全球的安全情報 - 可讓我們提供市面上最強大的惡意程式防護，並且協助我們建立決策。

我們是一家由上而下的技術導向公司 - 由我們的執行長尤金卡巴斯基 (Eugene Kaspersky) 帶頭做起。

我們的全球研究和分析團隊 (GReAT) 是由 IT 安全專家組成的菁英團隊，已經率先發現許多全球最危險的惡意程式威脅與針對性攻擊。

INTERPOL、Europol、CERT 及倫敦市警察廳等**全球最受敬重的多間安全組織和執法機構**均積極向我們尋求協助。

卡巴斯基實驗室在內部開發並完善其所有自有核心技術，因此我們的產品與情報自然更加穩定且更有效率。

最受歡迎的產業分析師 - 包含顧能 (Gartner)、Forrester Research 和國際數據資訊 (IDC)，在許多主要的 IT 安全類別中，給予卡巴斯基領導者的評價。

超過 130 家 OEM 廠商 - 包含 Microsoft、Cisco、Blue Coat、Juniper Networks、阿爾卡特朗訊 (Alcatel Lucent) 等，在其產品與服務中使用我們的技術。

卡巴斯基威脅情報服務

追蹤、分析、解譯及緩解不斷進化的 IT 安全威脅，是一項艱鉅的任務。各行各業均面臨最新相關資料短缺的問題，而企業正需要這樣的資料來協助管理 IT 安全威脅相關的風險。

卡巴斯基
網路安全服務

- **卡巴斯基威脅情報服務**
  - 威脅資料摘要
  - APT 情報報告
  - 量身訂做的威脅報告
  - 卡巴斯基威脅查詢
  - 卡巴斯基網路釣魚追蹤
  - 卡巴斯基殭屍網路追蹤
- **卡巴斯基威脅獵捕服務**
- **卡巴斯基安全培訓**
- **卡巴斯基事件回應服務**
- **卡巴斯基安全評估服務**

卡巴斯基實驗室的威脅情報服務，由領先全球的研究人員和分析師團隊提供您緩解這些威脅所需的情報。

卡巴斯基實驗室在網路安全各方面的知識、經驗及深度情報，使其成為 INTERPOL 和 CERT 等全球各大執法機構與政府機關的信任合作夥伴。如今您在企業組織內便可運用這樣的情報。

卡巴斯基實驗室威脅情報服務包括：

- 威脅資料摘要
- APT 情報報告
- 量身訂做的威脅報告
- 卡巴斯基威脅查詢
- 卡巴斯基網路釣魚追蹤
- 卡巴斯基殭屍網路追蹤

威脅資料摘要

最高層級的安全防護供應商及企業均使用歷史悠久且極富權威的卡巴斯基威脅資料摘要**來製作進階安全解決方案或保護其企業**。

網路攻擊每天都會發生。網路威脅的頻率、複雜度與製造混亂的能力持續增加，因為網路威脅會試圖**入侵您的防護措施**。敵人目前使用複雜的入侵**狙殺鍊**、活動，以及自訂的**戰術、技術和程序 (TTP)，藉此干擾您的企業或是造成您客戶的損失**。

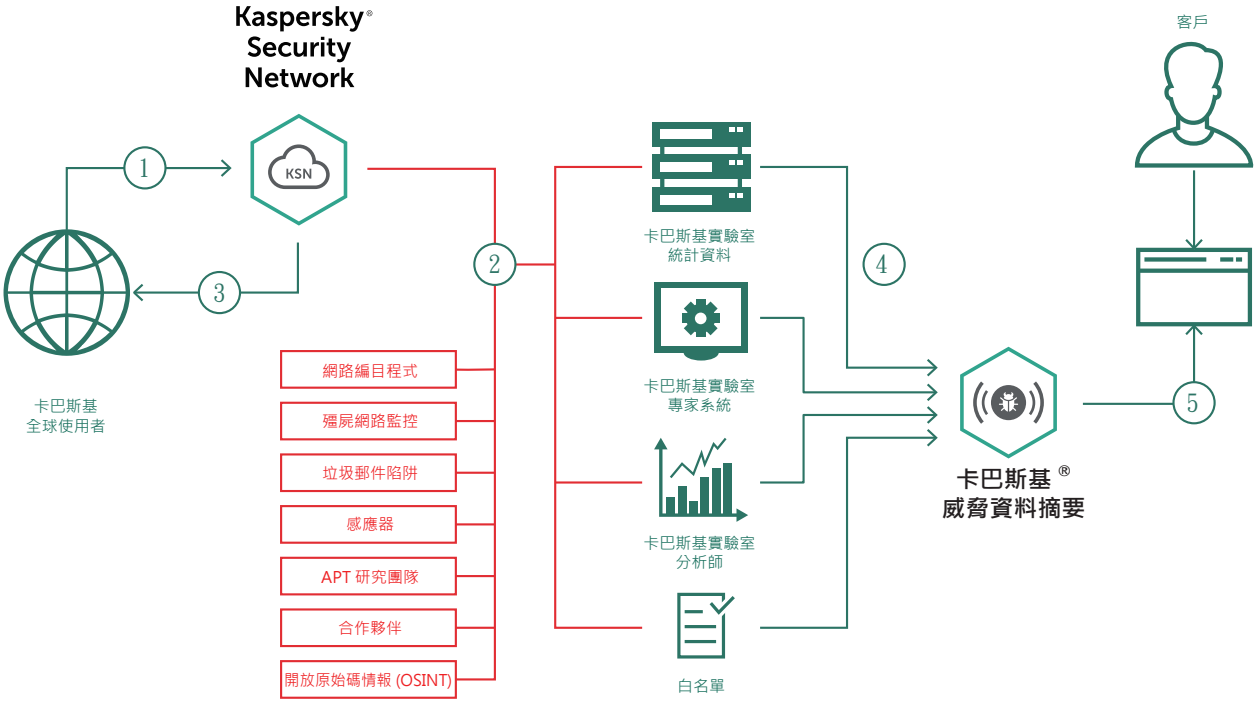
卡巴斯基實驗室提供**持續更新的**威脅資料摘要，**可以讓貴企業或客戶了解與網路威脅相關的風險與影響**，因此可以協助您**更有效緩解威脅**，甚至可以在攻擊發動之前**進行防護**。

情報循環

資料摘要

摘要包括下列組合：

- **IP 評價摘要** - 內容包含可疑和惡意主機的一組 IP 位址；
- **惡意及網路釣魚網址摘要** - 包含惡意和網路釣魚的連結與網站；
- **殭屍網路命令與控制項網址摘要** - 包含桌上型電腦殭屍網路命令與控制項伺服器及相關惡意物件；
- **行動殭屍網路命令與控制項網址摘要** - 包含行動殭屍網路命令與控制項伺服器。找出和命令與控制項伺服器進行通訊的受感染設備；
- **勒索軟體網址摘要** - 內含主機勒索軟體物件或這些物件存取的連結
- **APT IoC 摘要** (可供我們 APT 情報報告的活躍客戶使用) - 內含惡意網域、主機、惡意 IP 位址、對手發動 APT 攻擊所使用的惡意檔案，以及相關檔案或者甚至是惡意程式系列的 YARA 規則
- **惡意雜湊摘要** - 包含最危險、常見和新興的惡意程式；
- **行動惡意雜湊摘要** - 針對可以感染行動 Android 及 iPhone 平台的惡意物件提供偵測支援；
- **P-SMS 木馬程式摘要** - 針對可以讓攻擊者竊取、刪除並回覆 SMS 訊息，以及向行動使用者收取高額通話費用的 SMS 木馬程式提供偵測支援；
- **白名單資料摘要** - 為協力廠商解決方案與服務提供合法軟體的系統化知識。
- **卡巴斯基 Maltego 轉換服務** - 為 Maltego 使用者提供一組可以存取卡巴斯基實驗室威脅資料摘要的轉換。卡巴斯基 Maltego 轉換服務可讓您根據卡巴斯基實驗室的摘要檢查網址、雜湊以及 IP 位址。此轉換可以判斷物件的類別，並提供可據以行動的內容。



卡巴斯基威脅資料摘要包含即時徹底調查來自真實世界的威脅指標資料。

內容資料

每筆資料摘要中的所有紀錄都有許多**可據以行動的內容**（威脅名稱、時間戳記、地理位置、受感染網頁資源的解析 IP 位址、雜湊、普及率等）。內容資料可以協助找出「更完整的事件全貌」，如此可以進一步驗證和支援用途廣泛的資料。有了這些內容，您可以使用資料更快解決**主使者、事件、位置、時間等方面的疑問**，引領您找出對手，藉此協助您及時制定決策，並採取**適合貴企業組織**的行動。

服務特性

- **誤判率**偏高的資料摘要並沒有價值，因此在摘要發佈之前均經過極廣泛的測試和篩選，才能確保提供 100% 調查完成的資料；
- 資料摘要會依據全球調查結果即時自動產生 (Kaspersky Security Network 可以查看相當比例的所有網際網路流量，範圍涵蓋超過 213 個國家數千萬名使用者)，具備高**偵測率**與高精準度；
- 所有摘要都是以高容錯的基礎結構產生並加以監控，因此可確保**連續可用性**；
- 資料摘要可**立即偵測**用於主機網路釣魚的網址、惡意程式、入侵程式、殭屍網路命令與**控制項網址**及其他惡意內容；
- 所有流量類型（網頁、電子郵件、P2P、即時訊息...）和鎖定行動平台的**惡意程式**也可以**立即加以偵測**和辨識；
- 透過 **HTTPS** 或臨機操作做為傳遞機制的單純輕量化**傳播**格式 (**JSON**、**CSV**、**OpenIoC**、**STIX**)，有助於將摘要輕鬆整合至安全解決方案；
- 由來自全球的**安全分析師**、全球知名的 **GReAT 團隊以及頂尖的研發團隊**所組成的數百名**安全專家**，齊心協力產出這些摘要。安全人員可以收到由最高品質資料所產生的關鍵資訊及警示，而不會有可疑指標和警告氾濫的風險；
- **容易執行。**補充文件、樣本、專屬的技術客服經理，以及來自卡巴斯基實驗室的技術支援，全都能夠加以結合，因此可以實現簡單整合。

收集和處理

資料摘要會利用融合、異質與高可靠性的來源進行彙總，這些來源包括 Kaspersky Security Network 和我們自己的網路編目程式、殭屍網路監控服務（全年無休監控殭屍網路及其目標和活動）、垃圾郵件陷阱、研究團隊及合作夥伴等。

接著卡巴斯基會運用多種預先處理的技巧即時仔細檢查並選粹彙總的所有資料，例如統計準則、卡巴斯基實驗室專家系統（沙箱、啟發法引擎、多重掃描器、相似性工具、行為剖析等）、分析驗證和白名單驗證：

優勢

- **強化您的網路防護網路解決方案**，包括 SIEM、防火牆、IPS/IDS、安全 Proxy、DNS 解決方案、APT 防護，配合持續更新的入侵指標 (IOC) 及可據以行動的內容，可以為您提供網路攻擊的見解，並讓您更深入了解您對手的意圖、能力與目標。完整支援業界領導的 SIEM（包括 HP ArcSight、IBM QRadar、Splunk 等）；
- 開發或強化**防護網及邊緣網路裝置的惡意程式防護**（例如路由器、閘道、UTM 裝置）。
- 提供安全 /SOC 團隊與威脅相關的實用資訊，以及為隱藏在針對性攻擊背後的真實情況提供整體見解，**藉此提升並加快您的事件回應速度與鑑識能力。**以更高的效率和更有效的方式診斷並分析主機與網路中的安全事件，並利用內部系統發送的訊號來排列未知威脅的優先順序，藉此將事件回應速度縮到最短，並且在關鍵系統和資料受損之前中斷狙殺鍊；
- **為企業訂閱者提供威脅情報。**利用新興惡意程式及其他惡意威脅的第一手資訊，**可以率先強化您的防護結構並防止入侵**；
- **協助緩解針對性攻擊。**調整防禦策略對抗貴企業組織所面臨的特定威脅，利用戰術及策略威脅情報來強化您的安全結構；
- 使用威脅情報**偵測您網路和資料中心內的惡意內容**；
- **防止敏感性資產及智慧財產外流**，可防止從受感染的電腦流出到企業組織外，並快速偵測受感染的資產、防止失去競爭優勢和商機，並保護您品牌的商譽；
- 針對威脅指標（例如，命令與控制項通訊協定、IP 位址、惡意網址或檔案雜湊）進行深度搜尋，加上可為攻擊排定優先順序的人力驗證威脅內容，可以改善 IT 支出及資源配置決策，**並可讓您專注在緩解對貴企業構成最大風險的威脅**；
- 使用我們的專業知識及可據以行動的內容情報，**可以強化您產品和服務所提供的防護**例如網頁內容篩選、垃圾郵件 / 網路釣魚封鎖等；
- **若是託管安全服務供應商 (MSSP)**，可以透過為您的客戶提供業界頂尖的威脅情報作為進階服務讓貴企業成長。**若是電腦緊急事件回應團隊 (CERT)**，可以強化和擴充您的網路威脅偵測與辨識能力。

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

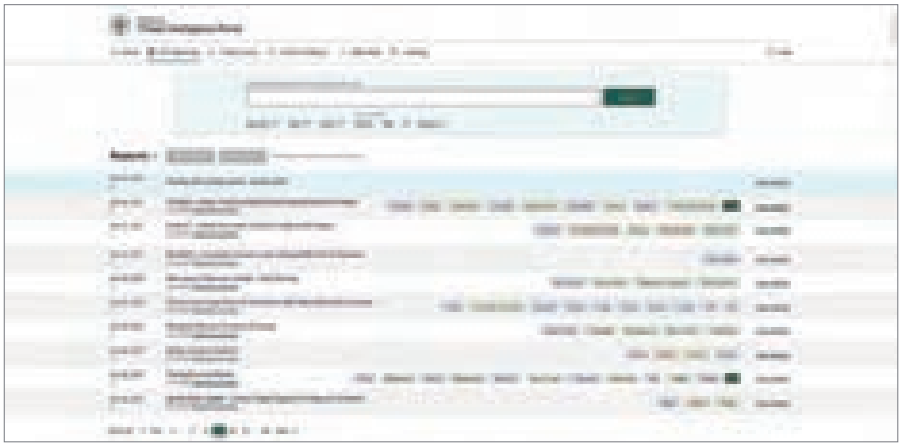
透過卡巴斯基實驗室提供的全方位實用報告，提升備受關注網路間諜活動方面的認知與知識。

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。

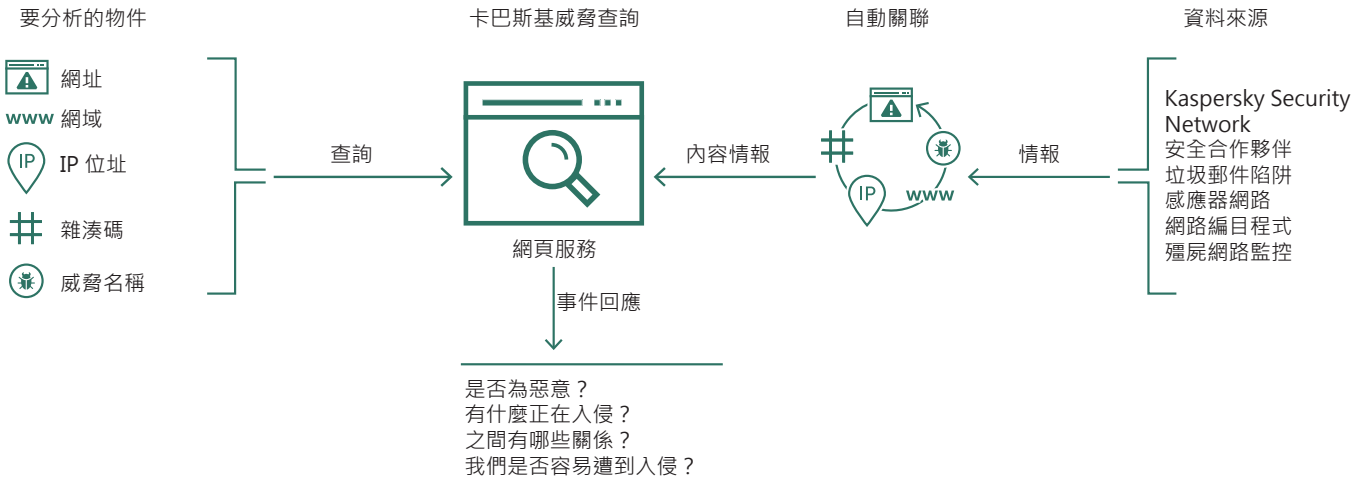
- **惡意程式和網路攻擊追蹤分析：**鎖定貴國的 APT 活動、活動中或非活動中的惡意程式樣本、過去或現在的殭屍網路活動，以及其他知名威脅，是根據我們獨家內部監控資源中的可用資料進行辨識與分析。

- **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。

威脅查詢



服務特性

- **可信任的情報：**卡巴斯基威脅查詢的其中一個重要屬性，就是我們威脅情報資料的可靠性，以及搭配的可據以行動的內容。卡巴斯基實驗室產品在防惡意程式測試的領域位居領導地位[1]，提供幾乎零誤判率的最高偵測率，展現出無與倫比的安全情報品質。
- **威脅獵捕：**主動防止、偵測及回應攻擊，將攻擊的影響和頻率降到最低。盡早追蹤並積極排除攻擊。您可以更快找出威脅。造成的損害越小，修復的速度就越快，而且網路作業可以更快恢復正常。
- **沙箱分析：**[2] 在安全的環境執行可疑物件來偵測未知威脅，並可透過容易閱讀的報告查看完整的威脅行為與產物。
- **多種匯出格式：**將 IOC (入侵指標) 或是可據以行動的內容，匯出為廣泛使用且更有條理的機讀共用格式，例如 STIX、OpenIOC、JSON、Yara、Snort，或者甚至是 CSV，即可充分利用威脅情報的優點、將操作的工作流程自動化，或是整合至 SIEM 等安全控制。
- **容易使用的網頁介面或 RESTful API：**您可以根據個人偏好，在手動模式下透過網頁介面 (透過網頁瀏覽器) 使用服務，或是透過簡單的 RESTful API 進行存取。

網路犯罪無國界，犯罪技術更是進步神速：我們發現攻擊變得越來越複雜，因為網路犯罪者使用暗網資源來威脅其目標。網路威脅的頻率、複雜度與製造混亂的能力持續增加，因為網路犯罪者嘗試利用新的手法來攻陷您的防護措施。攻擊者在其攻擊活動中使用複雜的狙殺鍊 (以及自訂的戰術、技術和程序 (TTP)) 來干擾您的企業、竊取您的資產，或是造成您客戶的損失。

卡巴斯基威脅查詢提供卡巴斯基實驗室所擁有、有關各種網路威脅與彼此之間關聯的所有知識，並匯集為單一、強大的網頁服務。其目標是盡可能為您的安全團隊提供充分的資料，以便在網路攻擊影響貴企業組織之前進行防護。該平台會擷取最新的詳細威脅相關情報，包含網址、網域、IP 位址、檔案雜湊、威脅名稱、統計 / 行為資料、WHOIS/DNS 資料、檔案屬性、地理位置資料、下載鏈結、時間戳記等。這些情報最後可為您提供全新與新興威脅的整體可視性，協助您保護貴企業組織並大幅提升事件回應的能力。

卡巴斯基威脅查詢提供的威脅情報，是由一個高度容錯的基礎結構進行即時產生與監控，因此可確保持續的可用性與一致的效能。由來自全球的安全分析師、我們全球知名的 GReAT 團隊，以及頂尖的研發團隊所組成的數百名安全專家，都有助於產生寶貴的實際威脅情報。

主要優勢

- 提供安全 /SOC 團隊與威脅相關的實用資訊，以及為隱藏在針對性攻擊背後的真實情況提供整體見解，**藉此提升並加快您的事件回應速度與鑑識能力**。以更高的效率和更有效的方式診斷並分析主機與網路中的安全事件，並利用內部系統發送的訊號來排列未知威脅的優先順序，藉此將事件回應速度縮到最短，並且在關鍵系統和資料受損之前中斷狙殺鍊。

- 針對 IP 位址、網址、網域或檔案雜湊等**威脅指標進行深度搜尋**，配合高度驗證的威脅內容，讓您排列攻擊的優先順序、改善人員及資源配置的決策，並且專注在緩解對貴企業構成最大風險的威脅。

- **緩解針對性攻擊。**調整防禦策略進行迎擊，並利用戰術及策略威脅情報來強化您的安全基礎結構。

1 http://www.kaspersky.com/top3

2 此功能預計於 2017 年下半年發佈。

現在您可以

- 透過網頁式介面或 RESTful API 查詢威脅指標。
- 了解物件必須視為惡意程式的原因。
- 檢查找到的物件是普遍或獨特的物件。
- 檢查包含憑證、經常使用的名稱、檔案路徑，或是相關網址在內的進階詳細資料，以找出全新的可疑物件。

這些僅是範例。您還有許多方法可以利用這種持續提供大量相關精密情報資料的來源。

了解您的敵人和朋友。認識經過證實非惡意程式的檔案、網址及 IP 位址，藉此提升調查速度。在分秒必爭的時刻，不能將寶貴的時間浪費在分析受信任的物件。

我們的使命就是協助全球防範各類型的網路威脅。為了達到此目標並落實網際網路的使用安全，「即時」分享和存取威脅情報至關重要。持續有效防護資料和網路的關鍵，就在於及時存取資訊。現在，卡巴斯基威脅查詢可讓您以較過去更高的效率直接存取這種情報。

所有的卡巴斯基網路釣魚追蹤通知都會透過 HTTPS 提供，而其中包括：

- 網路釣魚網址的螢幕擷取畫面；
- 網路釣魚網址的 HTML 程式碼；
- 包括下列欄位的 JSON
- 檔案：
  - 網路釣魚網址；
  - 網路釣魚網址鎖定的品牌名稱；
  - 第一次見到的時間戳記；
  - 最後一次見到的時間戳記；
  - 網路釣魚網址的普及率；
  - 受到網路釣魚網址影響的使用者地理位置；
  - 遭竊資料的類型 (信用卡資訊、銀行憑證、電子郵件或社群網路、個人資訊等)；
  - 攻擊類型 (威脅封鎖帳戶、提供下載檔案、要求更新個人資訊等)；
  - 此網路釣魚網址的解析 IP 位址；
  - WHOIS 資料；
  - 以及其他類型。

網路釣魚追蹤

網路釣魚 (特別是針對性的魚叉式網路釣魚) 是目前最危險且最有效的線上詐騙方法之一。偽造網站會擷取登入及密碼資訊來劫持使用者的線上身分識別，接著利用遭到入侵的電子郵件帳戶及社群網路平台竊取金錢或散播垃圾郵件和惡意程式。這是網路犯罪者武器庫中的一項強大武器，而且攻擊的頻率和多樣性持續增加。

而且不僅是金融機構遭到攻擊。從線上零售商到 ISP 和政府機構，所有人現在都遭到魚叉式網路釣魚的持續攻擊。將您的網站分毫不差加以重現並加上企業品牌標示，或是冒充為您的企業管理人員並發出訊息，都能夠輕易騙到使用者，讓他們提供機密資料 - 這些不僅會對他們本身造成損害，也可能會讓您的企業產生大規模損失。

一次成功的網路釣魚攻擊，便會對其企業受害者造成巨大的影響。除了直接損失外，還有所有的間接成本，例如清理遭到入侵的網站和帳戶。當然，這也會對商譽造成損害，這可能是受害最嚴重的部分 - 蠶食使用者對您線上服務的信任，可以預見未來幾年會有客戶流失的問題，並且面臨信用挑戰。網路犯罪無國界，犯罪技術更是進步神速：我們發現攻擊變得越來越複雜，因為網路犯罪者使用暗網資源來威脅其目標。網路威脅的頻率、複雜度與製造混亂的能力持續增加，因為網路犯罪者嘗試利用新的手法來攻陷您的防護措施。攻擊者在其攻擊活動中使用複雜的狙殺鍊 (以及自訂的戰術、技術和程序 (TTP)) 來干擾您的企業、竊取您的資產，或是造成您客戶的損失。

我們的解決方案 - 卡巴斯基網路釣魚追蹤服務

此服務會主動追蹤鎖定您品牌的網路釣魚網站並提供即時警示，並可為您提供與貴企業有直接關係的相關、精確且詳細的網路釣魚或詐騙活動持續報告，包括會竊取您使用者憑證、敏感性資訊、財務資訊，以及個人資料的植入式惡意程式及網路釣魚網址。這項服務也會監控特定頂層網域 (TLD)，或者甚至是網路釣魚網站出沒的整個地區。

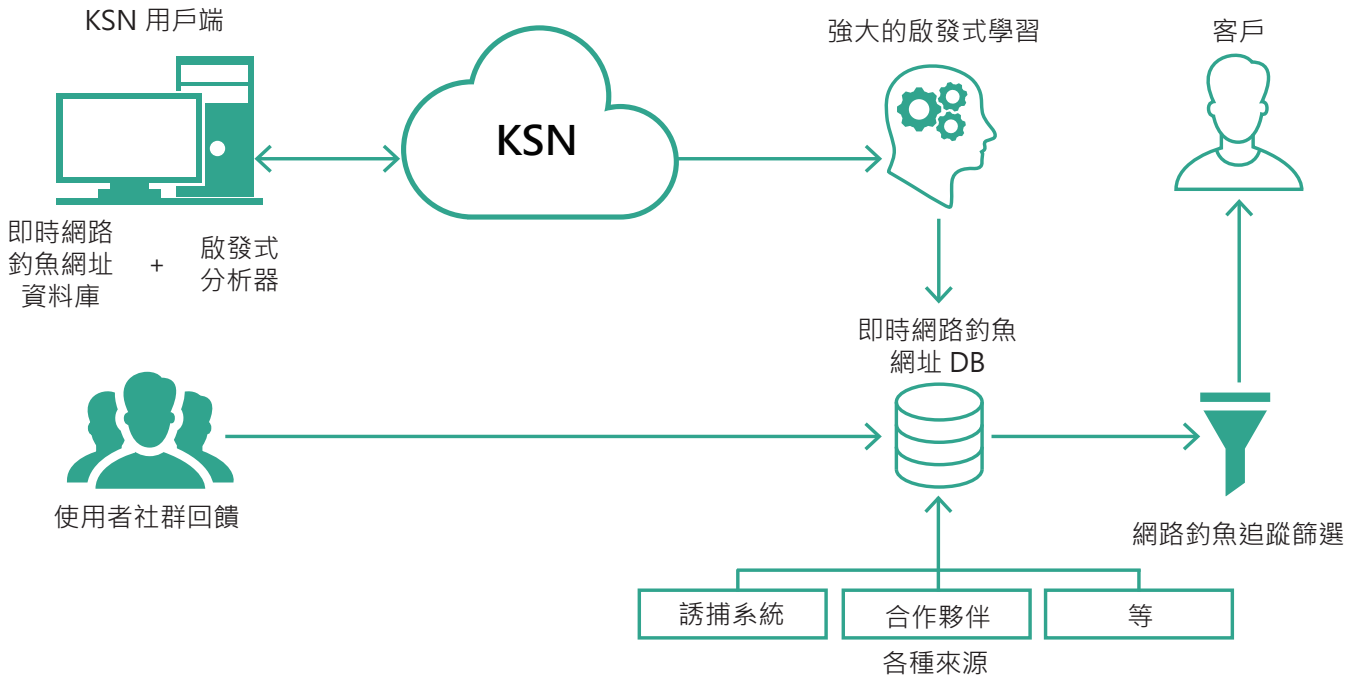
確認為針對您品牌、公司名稱或商標的網路釣魚威脅，便會持續發出電子郵件通知。所有通知都會針對日益複雜的網路釣魚攻擊，提供深入、高精確度且可靠的資訊，讓您可以對動態產生的網路釣魚網域和網址以及網路釣魚災情的爆發，迅速做出反應。搭配網路釣魚網站清單，您將收到額外的情報，讓您可以立即採取具體措施，對抗任何網路釣魚攻擊。

在這種經過專業驗證的及時情報協助下，您可以迅速採取精確的行動，以緩解網路釣魚活動對貴企業組織及使用者的影響，積極主動對應詐騙行為。

情報來源

卡巴斯基網路釣魚追蹤結合來自異質、高可靠性情報來源的資料，其中包含 Kaspersky Security Network (KSN)、強大的啟發法引擎、電子郵件誘捕系統、網頁編目程式、垃圾郵件陷阱、研究團隊、合作夥伴，以及卡巴斯基實驗室收集超過近 20 年與惡意物件相關的其他歷史資料。之後，彙總的資料會即時接受完整檢查，然後使用多種預先處理的技巧進行選粹，這些技巧包括統計準則、卡巴斯基實驗室專家系統 (沙箱、啟發法引擎、相似性工具、行為剖析等)、內容分析驗證，以及白名單驗證工具。

Kaspersky Security Network 的全球涵蓋範圍，結合卡巴斯基實驗室的偵測技術和一系列的測試與篩選，對任何類型網路釣魚和威脅都能確保沒有誤判率，並發揮出最大的偵測效果，這些都在獨立測試中不斷獲得證實 *。



您的網路釣魚攻擊預警

訂閱卡巴斯基網路釣魚追蹤服務，可以讓您畫出關鍵防線。針對正在進行或仍在計畫階段，且鎖定您品牌、線上服務及客戶的網路釣魚攻擊獲得預警，可以讓您以更務實、更準確且更有成本效益的方式保護資源並緩解風險。

搶得先機

關鍵資訊會即時提供，並透過惡意活動的定期報告來呈現，報告會指出規劃階段與正在進行的進階攻擊。現在正是您搶得先機的時候，而不是將機會拱手讓給鎖定您的網路犯罪者。

增進您的使用者體驗

一旦您知道並了解您的魚叉式網路釣魚對手，便能規劃適當的防護，從禁用過時軟體到引進 SMS 型驗證，全都有助於您的線上客戶得到更好的保護和保證。

將影響降到最低

知道網路釣魚網站的網址，表示可以通知託管網站的 ISP，防止網站取得的任何個人資料進一步外洩，並且在攻擊切入點阻止攻擊。

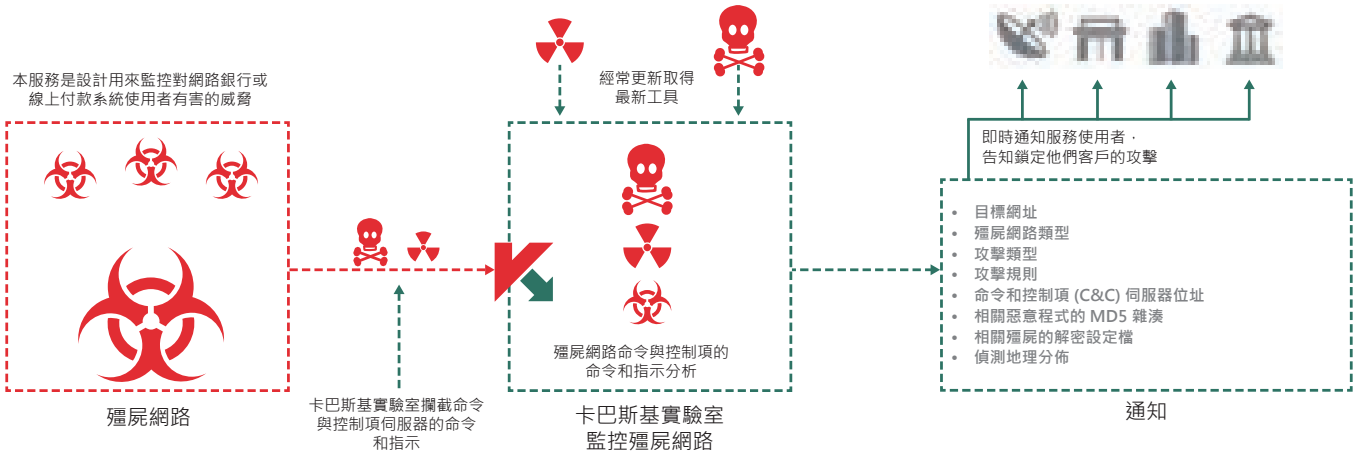
獲得更靈通的消息

此流程具有相關性、準確性並提供詳細資訊，不會發生「誤判」或浪費時間，可以為您帶來全新的見解，協助您了解並強化目前與未來的安全策略。現在，您和貴企業可以對線上詐騙採取積極主動的作法。

* AV-comparatives 測試報告可供索取。

殭屍網路追蹤

專家監控和通知服務可辨識威脅客戶和公司聲譽的殭屍網路。



使用案例 / 服務優勢

- 針對鎖定線上使用者的殭屍網路威脅主動提出警告，讓您隨時搶先一步防禦攻擊
- 辨識出鎖定線上使用者的殭屍網路命令與控制項伺服器網址清單，可讓您傳送要求至 CERT 或執法機構加以封鎖
- 了解攻擊本質，改良網路銀行 / 付款機制
- 訓練線上使用者辨識出攻擊使用的社交工程，避免落入其圈套

使用即時交付項目採取行動：

本服務可讓您訂閱個人化通知，內容涵蓋符合品牌名稱的相關情報，而這些名稱是追蹤卡巴斯基實驗室監控的殭屍網路關鍵字而來。您可以透過電子郵件或 RSS 傳送 HTML 或 JSON 格式的通知。通知包含：

- **目標網址** - 殭屍惡意程式的設計會等候使用者存取目標組織的網址，然後展開攻擊。
- **殭屍網路類型** - 精準了解網路犯罪者用來破壞客戶交易時採用的惡意程式威脅。例如 Zeus、SpyEye 及 Citadel 等。
- **攻擊類型** - 找出網路犯罪者使用惡意程式的意圖；例如植入網路資料、清除畫面、擷取影片或轉發至網路釣魚網址。
- **攻擊規則** - 了解使用的各種網路代碼植入規則，例如 HTML 要求 (取得 / 張貼)、植入前的網頁資料、植入後的網路資料。
- **命令與控制項 (C&C) 伺服器位址** - 讓您通知網際網路服務供應商違規伺服器，迅速擺脫威脅。
- **相關惡意程式的 MD5 雜湊** - 卡巴斯基實驗室提供驗證惡意程式用的雜湊總和。
- **相關殭屍的解密設定檔** - 找出目標網址的完整清單。
- **偵測地理分佈 (前 10 大國家)** - 全球各地相關惡意程式樣本的統計資料。

卡巴斯基威脅獵捕服務

所有產業的安全團隊，都在努力打造全方位防護的系統，防範快速演進的網路威脅。不過，大部分團隊對於網路安全事件仍採取「警示」導向的方法，這樣只能在事件發生之後做出反應。根據近期的研究，仍有大部分的安全事件尚未偵測到。這些威脅採取隱密行動，讓企業誤以為自己非常安全。因此，愈來愈多的企業組織同意，必須主動狩獵目前尚未發現，但仍在其基礎結構中活動的威脅。卡巴斯基威脅獵捕服務由具備高度專業能力與經驗的安全專業人員執行主動威脅獵捕技巧，有助於找出隱藏在企業組織中的進階威脅。

卡巴斯基
網路安全服務

- **卡巴斯基**
  威脅情報服務
- **卡巴斯基**
  威脅獵捕服務
  卡巴斯基託管防護針對性攻擊探索
- **卡巴斯基**
  安全培訓
- **卡巴斯基**
  事件回應服務
- **卡巴斯基**
  安全評估服務

卡巴斯基託管防護

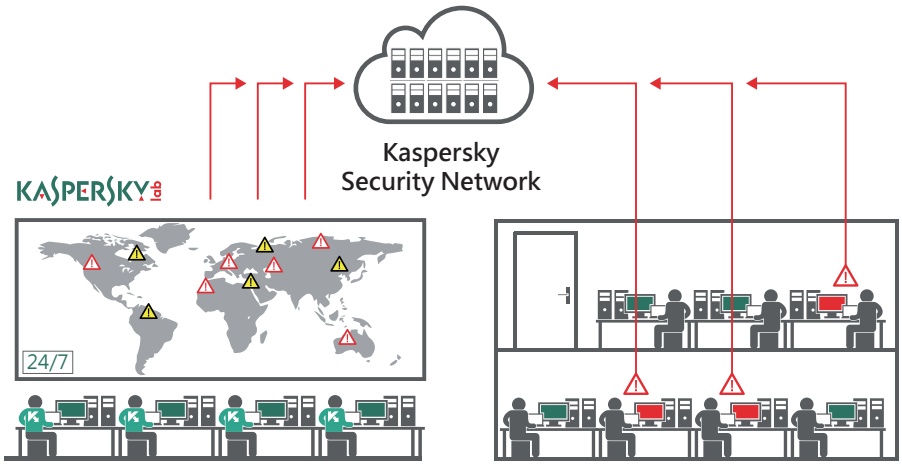
卡巴斯基託管防護服務可以為 Kaspersky Endpoint Security 及 Kaspersky Anti Targeted Attack Platform 的使用者提供完全託管的服務，此服務會部署一系列獨特的進階技術措施，可以偵測和防止貴企業組織中的針對性攻擊。此服務包括卡巴斯基實驗室專家二十四小時的監控，並持續分析網路威脅資料，以確保能即時偵測鎖定重要資訊系統的已知和全新網路間諜和網路犯罪活動。

服務特性

- 高水準的持續防護防止針對性攻擊和惡意程式，並加上您專屬的卡巴斯基實驗室專家「精銳部隊」所提供的全年無休監控與支援，以及深厚的專家技巧和持續提供的威脅情報。
- 及時且準確偵測非惡意程式的攻擊、利用先前未知工具的攻擊，以及利用零日弱點的攻擊。
- 透過防毒資料庫自動更新，立即防止任何偵測到的威脅。
- 事件及威脅獵捕的追溯分析，包括威脅者對貴企業組織所使用的方法和技術。
- 整合的方法 - 卡巴斯基實驗室的產品組合，含有您執行針對性攻擊完整週期防護所需的所有技術和服務：準備 - 偵測 - 調查 - 資料分析 - 自動防護。

服務優勢

- 高效率的快速偵測，讓緩解和修復更快更有效率。
- 對任何可疑活動都能立即明確辨識並加以分類，不會因為誤判而浪費時間。
- 減少整體安全成本。不需要雇用和培訓多種類型的內部專家。
- 即使是最複雜創新的非惡意程式威脅，您也可以放心，因為您知道正持續受到保護。
- 針對攻擊者、動機、方法和工具以及可能造成的潛在損害提出見解，有助於研擬出資訊完善的有效防護策略。



更細緻的服務

卡巴斯基針對性攻擊探索包含下列活動：

威脅情報的蒐集與分析。目標是要在遭到攻擊時取得快照 - 網路犯罪者和網路間諜的威脅與攻擊，可能將您的資產視為目標，或正在積極規劃行動。我們會利用內部及外部的情報來源，包括騙徒秘密社群，以及內部的卡巴斯基實驗室監控系統。例如，分析這些情報可以讓我們在您的基礎結構中，找出網路犯罪者目前有興趣的弱點，或是遭到入侵的帳戶。

現場資料收集與初期事件回應。除了我們實驗室自己收集的威脅情報活動，卡巴斯基實驗室的專家也會在現場收集網路和系統產物，以及任何可用的 SIEM 資訊。我們也可能會執行簡短的弱點評估，找出是否有最關鍵的安全漏洞需要採取立即行動。如果事件已經發生，我們將收集證據進行調查。在這個階段，我們會提供您過渡性建議，用於短期修復步驟。

資料分析。收集的網路及系統產物將帶回實驗室，利用卡巴斯基實驗室的入侵指標 (IoC)、命令與控制項 (C&C) 黑名單、沙箱技術等知識庫進行分析，確實了解您系統中所發生的事件。例如，如果在此階段找到全新的惡意程式，我們將提供您可以立即偵測這種程式的建議和工具 (即 YARA 規則)。整個過程我們都會與您保持密切聯繫，若情況適合，將於您的系統進行遠端作業。

準備報告。最後，我們會準備正式的報告，內含針對性攻擊探索結果，以及我們對於進一步修復活動的建議。

針對性攻擊探索

卡巴斯基實驗室的專家會提供主動式針對性攻擊探索服務，以確保貴企業的資產真正受到保障。

針對性攻擊探索的結果，可以讓您在您的網路中找出目前網路犯罪者和網路間諜的活動、了解這些事件的背後原因及可能來源，以及有效規劃有助於避免未來發生類似攻擊的緩解活動。如果您擔心針對您產業的攻擊、在您本身的系統中發現可能的可疑行為，或是貴企業組織只是了解到定期預防檢查的好處，卡巴斯基針對性攻擊探索服務的設計目的，是要告訴您：

- 您目前是否遭到攻擊、攻擊方式、被誰攻擊
- 攻擊如何影響您的系統、您的因應方法
- 防止進一步攻擊的最佳做法

服務的提供方式

我們享譽國際的獨立專家會找出、辨識與分析您網路中的持續性事件、進階持續威脅 (APT)、網路犯罪者和網路間諜活動。他們將協助您找出惡意活動、了解事件的可能來源，以及規劃最有效的修復活動。

我們採用以下方式執行：

- 分析威脅情報來源，以了解貴企業組織的具體威脅現況
- 針對您的 IT 基礎結構和資料 (例如紀錄檔) 進行深度掃描，找出可能的入侵跡象
- 分析您的連外網路連線，尋找任何可疑的活動
- 找出攻擊的可能來源，以及其他可能遭到入侵的系統

結果

我們以詳細報告提供發現結果，包括：

整體探索結果 - 確認您的網路中是否有入侵跡象存在

深度分析 - 針對收集的威脅情報資料，以及揭露的入侵指標 (IoC)。

詳細說明 - 針對遭到入侵的弱點、可能的攻擊來源，以及受到影響的網路元件。

修復建議 - 提出建議步驟，其有關緩解所揭露事件的結果，並防止您的資源在未來遭到類似的攻擊。

其他服務

您也可以要求我們的專家分析事件徵狀、針對特定系統執行深度數位分析、找出惡意程式二進位檔 (若有) 並進行惡意程式分析。這些選購的服務可以個別報告，其中包括進一步的修復建議。

我們也可依您的要求，在您的網路永久部署 **Kaspersky Anti Targeted Attack (KATA) Platform**，或是用來執行「概念驗證」。此平台結合最新的技術和全球分析，可立即偵測和回應針對性攻擊，因此在您系統中的生命週期所有階段都能對抗攻擊。

卡巴斯基安全培訓

企業面臨越來越多持續進化的威脅，網路安全教育對企業而言更是不可或缺的工具。IT 安全人員需要專精於進階技巧，這些進階技巧是有效企業威脅管理與緩解策略的關鍵要素。

卡巴斯基
網路安全服務

- **卡巴斯基威脅情報服務**
- **卡巴斯基威脅獵捕服務**
- **卡巴斯基安全培訓**
  - 數位鑑識
  - 惡意程式分析及逆向工程
  - 進階數位鑑識
  - 進階惡意程式分析及逆向工程
  - 事件回應
  - Yara
  - KATA 系統管理
  - KATA 安全分析師
- **卡巴斯基事件回應服務**
- **卡巴斯基安全評估服務**

這些課程涵蓋網路安全主題、技巧及評估的多樣化課程，範圍從初級至高級均有。授課場所可以是客戶提供的教室場地，或是當地 / 所屬區域的卡巴斯基實驗室辦公室 (若有)。

課程設計包含理論課程和「實驗室」實機操作。學員完成每項課程後，將受邀參加評量測驗，檢驗自己習得的知識。

服務優勢

數位鑑識及進階數位鑑識

充實內部數位鑑識和事件回應團隊的專業知識。課程設計的目的為彌補經驗差距 - 培養並強化實務技巧，包括搜尋網路犯罪的數位蹤跡，以及分析不同類型的資料以還原攻擊時間軸和來源。完成課程之後，學員將有能力完成電腦事件調查，並提升企業的安全等級。

惡意程式分析與逆向工程，以及進階惡意程式分析與逆向工程

逆向工程培訓的設計，是要協助事件回應小組調查惡意攻擊。這項課程是為了 IT 部門的員工和系統管理員所設計。學員將學習分析惡意軟體、收集 IoC (入侵指標)、撰寫可偵測受感染電腦中惡意程式的特徵碼，以及還原遭到感染 / 加密的檔案和文件。

事件回應

課程會引導您的內部團隊，進行事件回應流程的所有階段，並且讓他們擁有成功修復事件所需的全方位知識。

Yara

將協助您了解如何撰寫最有效的 Yara 規則、如何測試這些規則，並提升規則的威脅尋找能力，達到所向披靡的程度。

KATA 系統管理

KATA 系統管理培訓可提供規劃、安裝和設定解決方案所需的所有關鍵知識，以將其威脅偵測效率調整到最佳狀態。

KATA 安全分析師

培訓課程納入許多基於真實威脅偵測情況的實務練習，其中包含的知識可在監控、解譯和回應 KATA 警示時更有信心。

實際操作的體驗

由安全領導供應商提供，與全球專家們共事與學習，透過專家在網路犯罪偵測與防範領域的「前線」自身經驗來激勵學員。

方案說明

主題	期間	習得技能
數位鑑識		
• 數位鑑識介紹 • 現場回應和證據採集 • Windows 登錄內部 • Windows 產物分析 • 瀏覽器鑑識 • 電子郵件分析	5 天	• 打造數位鑑識實驗室 • 收集數位證據並妥善處理 • 重新建構事件並使用時間戳記 • 根據 Windows 作業系統中的產物尋找入侵蹤跡 • 尋找及分析瀏覽器和電子郵件歷程紀錄 • 能夠使用數位鑑識工具和儀器
惡意程式分析和逆向工程		
• 惡意程式分析和逆向工程目標與技術 • Windows 內部、可執行檔、x86 組合程式 • 基本靜態分析技術 (字串擷取、匯入分析、PE 進入點一覽、自動解壓縮等) • 基本動態分析技術 (除錯、監視工具、流量攔截等) • .NET、Visual Basic、Win64 檔案分析 • 指令碼和非 PE 分析技術 (批次檔、Autoit、Python、Jscript、JavaScript、VBS)	5 天	• 打造分析惡意程式的安全環境：部署沙箱和所有必要工具 • 了解 Windows 程式執行原則 • 解壓縮、除錯及分析惡意物件並辨識其功能 • 分析指令碼惡意程式來偵測惡意網站 • 執行快速惡意程式分析
進階數位鑑識		
• 深度 Windows 鑑識 • 資料復原 • 網路和雲端鑑識 • 記憶體鑑識 • 時間軸分析 • 真實世界的針對性攻擊鑑識實務	5 天	• 能夠執行深度的檔案系統分析 • 能夠復原已刪除的檔案 • 能夠分析網路流量 • 從傾印 (dump) 揭露惡意活動 • 重新建構事件時間軸
進階惡意程式分析與逆向工程		
• 惡意程式分析和逆向工程目標與技術 • 進階靜態分析技巧 (靜態分析 Shellcode、剖析 PE 標頭、TEB、PEB、利用不同雜湊演算法載入功能) • 進階動態分析技巧 (PE 結構、手動與進階解壓縮、將儲存有加密形式完整可執行檔的惡意封裝檔解壓縮) • APT 逆向工程 (涵蓋 APT 的攻擊形式，從網路釣魚電子郵件開始，並盡可能深入) • 通訊協定分析 (分析加密的 C2 通訊協定、如何解密流量) • Rootkit 及 Bootkit 分析 (使用 Ida 及 VMWare 為開機磁區除錯，使用 2 台虛擬機器的核心除錯、分析 Rootkit 範本)	5 天	• 能夠遵循逆向工程的最佳實務，並且認識反逆向工程的技巧 (混淆、反除錯) • 能夠針對 Rootkit/Bootkit 解構套用進階惡意程式分析 • 能夠分析嵌入不同檔案類型的入侵 Shellcode 以及非 Windows 惡意程式

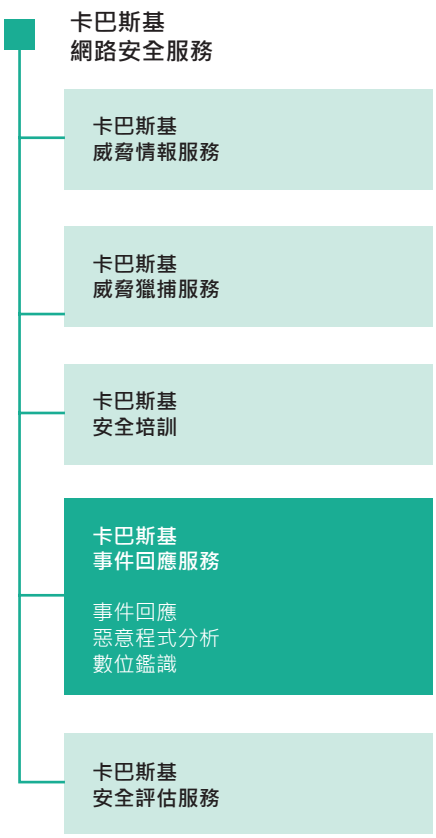
方案說明

主題	期間	習得技能
事件回應		
• 事件回應介紹 • 偵測及主要分析 • 數位分析 • 建立偵測規則 (YARA、Snort、Bro)	5 天	• 區分 APT 和其他威脅 • 了解攻擊者的各種技巧，以及針對性攻擊的剖析 • 套用特定的監控與偵測方法 • 遵循事件回應工作流程 • 重新建構事件發生順序和邏輯 • 建立偵測規則和報告
Yara		
• Yara 語法簡介 • 建立快速且有效規則的秘訣與技巧 • Yara 產生器 • 測試 Yara 規則的誤判率 • 狩獵 VT 中未偵測的全新範本 • 在 Yara 中使用外部模組以進行有效狩獵 • 異常搜尋 • 許多 (!) 現實生活的範本 • 可提升您 Yara 技巧的一組練習	2 天	• 建立有效的 Yara 規則 • 測試 Yara 規則 • 提升規則的威脅尋找能力，達到所向披靡的程度
KATA 系統管理		
• 一般解決方案的部署形式及伺服器位置 • 規模考量 • 授權模式 • 沙箱伺服器 • 中央節點 • 感應器 • 整合基礎結構 • 安裝端點感應器 • 新增授權及更新資料庫 • 解決方案作業演算法	1 天	• 設計符合客戶環境的執行計畫 • 安裝及設定所有的 KATA 元件 • 維護及監控解決方案
KATA 安全分析師		
• KATA 警示解譯 • 偵測及分析技術說明 • 評分及風險引擎說明	1 天	• 了解評分方式，以及風險引擎如何運用評分 • 能夠在監控、解譯和回應 KATA 警示時具有信心

卡巴斯基事件回應服務

當 IT 和安全專家努力確保各個網路元件的安全足以對抗入侵者，同時保有合法使用者的完整使用權利時，只要有一項弱點便會使門戶大開，網路犯罪者就有可能取得資訊系統控制權。沒有人能夠倖免：無論您的安全控制多麼有效，都有可能成為受害者。

防止資訊安全事件變得日益困難。不過，雖然我們可能無法每次都在攻擊突破您的安全防線之前加以制止，但我們絕對有能力可以限制造成的損害，以及防止攻擊擴散。



事件回應的整體目標，是要降低安全入侵或是攻擊對您 IT 環境所造成的影響。此服務涵蓋整個事件調查週期，從現場的證據採集到其他入侵指標的辨識，進而制定修復計畫並完整排除對貴企業組織的威脅。

我們採用以下方式執行：

- 找出遭到入侵的資源。
- 隔離威脅。
- 防止攻擊擴散。
- 尋找並蒐集證據。
- 分析證據並重新建構事件發生順序和邏輯。
- 分析攻擊使用的惡意程式 (如果有找到惡意程式)。
- 找出攻擊的來源，以及其他可能遭到入侵的系統 (可能的話)。
- 對您的 IT 基礎結構進行工具輔助掃描，以找出可能的入侵跡象。
- 分析您的網路和外部資源間的連外連線，以偵測任何可疑活動 (例如可能的命令與控制項伺服器)。
- 排除威脅。
- 針對您可採取的進一步修復行動提出建議。

視您是否擁有專屬的事件回應團隊而定，您可以要求我們的專家執行完整的調查週期、僅辨識和隔離遭到入侵的電腦並防止威脅傳播，或是進行惡意程式分析或數位鑑識。

卡巴斯基實驗室的事件回應服務，是由具有豐富經驗的網路入侵偵測分析師和調查員執行。我們傾盡數位鑑識及惡意程式分析方面的全球專業知識，可以用來為您解決安全事件。

惡意程式分析

惡意程式分析可讓您通盤了解，以貴企業組織為目標的特定惡意程式檔案行為與目標。卡巴斯基實驗室的專家會詳細分析您提供的惡意程式樣本並建立詳細報告，內容包括：

- **樣本屬性：**簡要說明樣本和惡意程式分類結果。

- **惡意程式的詳細說明：**深入分析惡意程式樣本的功能、威脅行為及目標 (包括 IOC)，提供您終止其活動所需的資訊。

- **修復情境：**此報告會提供建議步驟讓您完整維護企業組織安全，以對抗該類型的威脅。

數位鑑識

如果調查期間發現任何惡意程式，數位鑑識內容會包含上述惡意程式分析。卡巴斯基實驗室專家會拼湊證據，了解實際發生情形，包括使用硬碟映像、記憶體傾印及網路追蹤。調查後將為您詳盡說明整個事件。身為客戶的您可蒐集證據並提供事件概述，即可開始整個程序。卡巴斯基實驗室專家會分析事件徵狀、找出惡意程式二進位檔 (若有) 並進行惡意程式分析，以提供修復步驟等詳細報告。

交付選項

卡巴斯基實驗室的事件回應服務提供方式：

- 藉由訂閱
- 回應單一事件

兩種選項都是以我們專家解析事件所花費的時間為根據 - 這會在簽署合約之前與您協商。您可以指定您希望花費的工作時數，或是依照我們專家根據特定事件和您的個人需求所提供的建議。

卡巴斯基安全評估服務

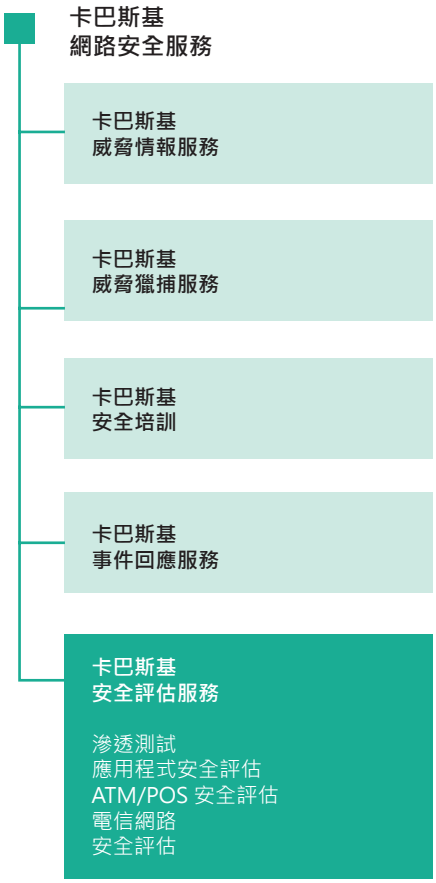
卡巴斯基實驗室的安全評估服務是由我們內部專家提供的服務，這些專家都是具備實力的全球權威人士；身為安全情報方面的全球領導廠商，這些專家的知識與經驗是我們維護聲譽的基石。

由於不會有兩個完全一樣的 IT 基礎結構，也因為最強大的網路威脅往往是為了入侵各企業組織的特定弱點而特別製造，所以我們的專家服務也是量身打造。接下來說明的服務是我們專業工具組的一部分，與您合作時可能會部分或完整使用下列的部分或所有服務。

最重要的是，我們的目標是與您一對一合作、成為您的專家顧問、協助評估風險、強化安全並緩解日後威脅。

安全評估服務包括：

- 滲透測試
- 應用程式安全評估
- ATM/POS 安全評估
- 電信網路安全評估



滲透測試

對於任何組織而言，確保 IT 基礎結構安全無虞並對抗潛在的網路攻擊是一項永不停歇的挑戰，即便是擁有數千名員工、數百台資訊系統以及在全球各地擁有據點的大型企業更是如此。

滲透測試是一項展現可能攻擊情況的實用方法，惡意攻擊者可能會嘗試略過企業網路的安全控制，以取得重要系統的高級權限。

卡巴斯基實驗室的滲透測試可讓您進一步了解基礎結構中的安全漏洞、揭露弱點、分析不同形式攻擊的可能結果、評估目前安全措施的效果，並建議修復動作及改善方法。

卡巴斯基實驗室的滲透測試可協助您和貴企業組織：

- **找出網路中的弱點**，讓您能針對精力與預算投注的項目做出明智決策，以降低日後風險。
- 主動偵測並修復弱點以防範攻擊發生，**避免因網路攻擊造成財務、營運及聲譽上的損失**。
- 符合對於這種類型安全評估 (例如支付卡產業資料安全標準 [PCI DSS]) 有所需求的**政府、業界或內部企業標準**。

滲透測試結果

此服務是設計用來揭露安全缺點；這些安全缺點可能用於入侵，目標是在未經授權的情況下存取重要網路元件。其中包括：

- 易受攻擊的網路架構、網路防護措施不足
- 會導致網路流量遭到攔截並重新導向的弱點
- 多項不同服務的驗證與授權措施不足
- 使用者認證措施孱弱
- 設定方面的問題，包括使用者權限過高
- 應用程式程式碼錯誤造成的弱點 (程式碼植入、路徑穿越、用戶端弱點等)
- 使用無最新安全更新的過期軟硬體版本所造成的弱點
- 資訊揭露

在最終報告中提供結果，包括測試流程的詳細技術資訊、結果、已揭露弱點、修復建議，以及概述測試結果和提供攻擊媒介的執行摘要。如有需要，也可為技術團隊和管理高層提供影片和簡報。

服務範圍和選項

您可以根據您的需求和 IT 基礎結構，選擇使用任何一項或所有服務：

- **外部滲透測試：**對系統不具初步認識的「攻擊者」會透過網際網路執行安全評估。
- **內部滲透測試：**以內部攻擊者作為基準製造出來的情境，例如僅實際造訪辦公室的訪客或是系統存取權有限的承包商。
- **社交工程測試：**模擬網路釣魚、電子郵件中的虛擬惡意連結、可疑附件等社交工程攻擊，進行人員安全認知評估。
- **無線網路安全評估：**我們的專家會造訪您的場地，並分析 WiFi 安全控制措施。

IT 基礎結構的任何一部分均可列入滲透測試的範圍，但強烈建議您考慮將整體網路或最大區段納入；如果我們的專家與潛在入侵者所擁有的條件相同，測試結果會更有價值。

關於卡巴斯基實驗室滲透測試的方法

滲透測試會模擬真正的駭客攻擊，這些測試會緊密控管；測試是由卡巴斯基實驗室安全專家執行，執行時會充分保護您系統的機密性、完整性及可用性，並嚴格遵守國際標準與最佳實務，包括：

- 滲透測試執行標準 (PTES)
- NIST 特刊 800-115 資訊安全測試與評估技術指南
- 開放原始碼安全測試方法手冊 (OSSTMM)
- 資訊系統安全評估架構 (ISSAF)
- Web 應用安全聯盟 (WASC) 威脅分類
- 開放 Web 應用安全計畫 (OWASP) 測試指南
- 通用弱點評分系統 (CVSS)

專案團隊成員都是經驗豐富的專業人員，均具備該領域深厚的最新實用知識，並獲得 Oracle、Google、Apple、Microsoft、Facebook、PayPal、Siemens 及 SAP 等業界領導廠商認可為安全顧問。

交付選項

視安全評估服務的類型、您的系統特性與工作實務而定，安全評估服務可以採遠端或現場方式進行。大部分的服務都可遠端執行，而內部滲透測試也可透過 VPN 存取方式執行，但部分服務 (無線網路安全評估等) 需要現場實施。

應用程式安全評估

無論您是自行開發企業應用程式，或是向第三方購買，都必須知道只要有一個程式碼出現錯誤就會產生弱點，讓您暴露在造成嚴重財務或聲譽受損的攻擊風險之中。在應用程式的生命週期中也可能產生新弱點，原因可能是軟體更新或不安全的元件設定，或是透過全新攻擊方式所引發。

卡巴斯基實驗室的應用程式安全評估可揭露各種應用程式的弱點，包括大型雲端式解決方案、ERP 系統、網路銀行和其他特定業務應用程式，乃至不同平台 (iOS、Android 等) 的嵌入式和行動應用程式。

我們的專家結合實用知識和經驗及國際最佳實務，能夠偵測出可能使貴企業組織暴露於威脅的安全漏洞，包括：

- 竊取機密資料
- 滲透並修改資料和系統
- 啟動阻斷服務攻擊
- 執行詐騙活動

遵照我們的建議，便可修正所揭露的應用程式弱點，並避免此類攻擊。

服務優勢

卡巴斯基實驗室應用程式安全評估服務可協助應用程式持有人與開發人員：

- 主動偵測攻擊應用程式時所使用的弱點並加以修正，**避免造成財務、營運及聲譽上的損失**
- 在推廣至使用者環境之前，針對尚在開發與測試階段的應用程式追蹤其弱點 (後續修正可能導致長時間中斷及龐大費用)，如此便可**省下修復費用**。
- **支援安全的軟體開發生命週期** (S-SDLC)，致力建立及維護安全的應用程式。
- **符合**包含應用程式安全 (例如 PCI DSS 或 HIPAA) 的**政府、業界或內部企業標準**

服務範圍和選項

接受評估的應用程式可以是官方網站和企業應用程式、標準或雲端式應用程式，包括內嵌式與行動應用程式。

本服務是針對您的需求和應用程式特性量身打造，可能包括：

- **黑箱測試** - 模擬外部攻擊者
- **灰箱測試** - 模擬擁有各種設定檔的合法使用者
- **白箱測試** - 以應用程式的完整存取權限進行分析，包括原始程式碼；此方法為揭露大量弱點的最有效方法
- **應用程式防火牆成效評估** - 在啟用 / 未啟用防火牆防護的情況下測試應用程式，以找出弱點並驗證是否已阻擋潛在的弱點入侵

關於卡巴斯基實驗室進行應用程式安全評估時採用的方法

卡巴斯基實驗室的安全專家將以手動方式與使用自動化工具執行應用程式的安全評估，執行時會充分保護您系統的機密性、完整性及可用性，並嚴格遵守國際標準與最佳實務，例如：

- Web 應用安全聯盟 (WASC) 威脅分類
- 開放 Web 應用安全計畫 (OWASP) 測試指南
- OWASP 行動安全測試指南
- 根據貴企業組織業務與地點的其他標準

結果

卡巴斯基實驗室應用程式安全評估服務可以找出的弱點包括：

- 驗證與授權的漏洞，包括多重階段驗證
- 程式碼植入 (SQL 植入、作業系統命令等)
- 導致詐騙的邏輯弱點
- 用戶端弱點 (跨網站指令碼、跨網站偽造要求等)
- 使用低強度的密碼編譯
- 用戶端伺服器通訊中的弱點
- 資料儲存或傳輸不安全，例如付款系統缺乏 PAN 遮罩
- 引發工作階段攻擊等設定問題
- 敏感性資訊揭露
- 引發 WASC 威脅分類 2.0 版和 OWASP 十大弱點所列威脅的其他 Web 應用程式弱點。

在最終報告中提供結果，包括評估流程的詳細技術資訊、結果、已揭露弱點、修復建議，以及概述管理影響的執行摘要。如有需要，也可為技術團隊和管理高層提供影片和簡報。

專案團隊成員都是經驗豐富的專家，均具備該領域深厚的最新實用知識，包括各種平台、程式設計語言、架構、弱點及攻擊方式。這些專家都曾經在重要的國際會議上發表，並且為 Oracle、Google、Apple、Facebook 及 PayPal 等應用程式和雲端服務主要廠商提供安全諮詢服務。

交付選項

視安全評估服務的類型、範圍內的系統特性以及您的工作條件需求而定，安全評估服務可以採遠端或現場方式進行。服務大多數都能以遠端方式執行。

ATM/POS 安全評估

ATM 及 POS 裝置的弱點不再限於 ATM 竊盜或卡片側錄等實體攻擊。銀行和 ATM/POS 供應商採用的防護措施逐漸進化，對這些裝置的攻擊也隨之升級，變得越來越複雜。駭客會利用 ATM/POS 基礎結構架構和應用程式中的弱點，而且會建立專為 ATM/POS 量身訂做的惡意程式。卡巴斯基實驗室的 ATM/POS 安全評估服務可協助了解您 ATM/POS 裝置中的安全漏洞，並可緩解遭到入侵的風險。

ATM/POS 安全評估會完整分析您的 ATM 及 / 或 POS 裝置，其設計可找出攻擊者可能用於未經授權提領現金、執行未經授權交易、取得您客戶支付卡資料，或是啟動阻斷服務等活動的弱點。這項服務可以找出您 ATM/POS 基礎結構中可能遭到不同類型攻擊入侵的任何弱點、列舉遭到入侵的可能結果、評估您現有安全措施的有效性，以及協助您針對偵測到的漏洞規劃修復活動並提升您的安全。

服務優勢

卡巴斯基實驗室的 ATM/POS 安全評估可協助供應商及金融組織：

- **了解其 ATM/POS 裝置中的弱點**，並改善您對應的安全流程
- 透過主動偵測和修復攻擊者可能利用的弱點，**防止攻擊可能造成的財務、營運和商譽損失**。
- **符合**規定執行 PCI DSS (支付卡產業資料安全標準) 等安全評估的**政府、業界或內部企業標準**。

服務範圍

服務包含完整的 ATM/POS 分析，其中包括在測試環境中進行的模糊測試與攻擊示範。這項服務可以在單一 ATM/POS 裝置或裝置的網路中執行。我們建議您選擇評估貴企業組織中最廣泛使用的 ATM/POS 裝置類型，或是在其典型配置中最關鍵 (例如已經遭遇事件) 的裝置類型。

ATM/POS 安全評估結果

ATM/POS 安全評估服務可能會找出一系列的弱點，包括：

- 網路架構和網路防護不足的弱點。
- 讓攻擊者得以躲過資訊站模式、可未經授權存取作業系統的弱點。
- 存在於協力廠商安全軟體中、能夠讓潛在攻擊者繞過安全控制的弱點。
- 輸入和輸出裝置防護不足 (讀卡機、發鈔裝置等)，包括裝置通訊中可以允許攔截和修改傳輸資料的弱點。
- 應用程式碼錯誤，或是使用過時硬體和軟體版本所導致的弱點 (緩衝區溢位、程式碼植入等)
- 資訊揭露。

評估結束後，您將收到一份報告，內含測試流程、結果、弱點和建議的詳細技術資訊；以及一份易於了解的執行摘要，其概述我們根據測試結果所得到的結論，並展示各種攻擊切入點。此外，如有需要，可為技術團隊和管理高層提供攻擊示範的影片和簡報。

卡巴斯基實驗室的 ATM/POS 安全評估方法

在進行分析期間，我們的專家不僅會尋找和辨識配置漏洞和過時軟體版本的弱點，也會針對您 ATM/POS 裝置執行工作流程背後的邏輯進行深入分析、執行安全研究以找出元件等級的任何全新 (零日) 弱點。如果我們找到可能會讓攻擊者獲利的弱點 (例如，導致未經授權的現金提款)，我們的專家可以利用特別製作的自動化工具或裝置展現可能的攻擊形式。

雖然為了實際評估您防護的有效性，ATM/POS 安全評估包括模擬真正駭客的攻擊行為，但完全沒有安全疑慮，而且不具侵入性。此服務是由卡巴斯基實驗室經驗豐富的安全專家執行，這些專家會特別注意您系統的機密性、完整性及可用性，並嚴格遵守國際法和最佳實務。如果我們在客戶的 ATM/POS 中發現全新的弱點，我們會致力於遵循適用的揭露政策、通知供應商，以及為準備修復提供諮詢協助。

卡巴斯基實驗室提供的 ATM/POS 安全評估符合下列國際標準和最佳實務：

- 支付卡產業標準
  - 資料安全標準
  - 支付應用程式資料安全標準
  - PIN 碼交易安全
- 開放原始碼安全測試方法手冊 (OSSTMM)
- 資訊系統安全評估架構 (ISSAF)
- 通用弱點評分系統 (CVSS)
- 適用於特定商業模式和地理位置的其他標準 (視需要而定)。

專案團隊成員是在實務安全方面擁有豐富經驗的專業人員，他們具備該領域的深厚知識並持續提升其技巧，會定期為 ATM/POS 供應商提供安全諮詢，並在頂尖資訊安全會議 (例如黑帽) 中，介紹我們的 ATM/POS 安全研究結果。

電信網路安全評估

服務概要

電信公司的 IT 基礎結構包含許多根據各種功能和技術互相連線的網路。這些網路通常包括含有核心無線電網路 (GSM/UMTS/LTE) 等管理元件的企業網路，可以為訂閱者提供寬頻網際網路存取、專用高速主幹通道、主機和雲端服務。這個基礎結構的每個部分對企業都非常重要，而且應該具備良好保護不受駭客攻擊，才可將財務、營運和商譽風險降到最低。卡巴斯基實驗室的電信網路服務可讓您了解您系統中的弱點，並且透過導入控制措施的方式將這些弱點去除或修復其影響，因此可以降低這些風險。

卡巴斯基實驗室針對電信網路提供下列安全評估服務：

- IT 基礎結構滲透測試
- IT 基礎結構配置安全評估
- GSM/UMTS/LTE 網路的安全評估
- 應用程式安全評估 (適用於提供各種服務的應用程式：IP-TV、用戶端自助服務入口網站等)

- VoIP 安全評估
- 電信設備安全評估

服務成果

每次安全評估的最後，您將會得知您電信網路中的安全漏洞 (以技術觀點與高層觀點提供)，以及對您安全控制措施效用的結論。這些結果可以用來提升網路安全，進而緩解有關資訊安全威脅的財務、營運和商譽風險。

這份報告包含下列資訊：

- 您電信網路目前安全等級的高層觀點結論
- 服務方法和流程的說明。
- 偵測到的弱點詳細說明，包括嚴重性等級、入侵複雜度、對有弱點的系統可能造成的影響，以及弱點存在的證據 (若可能)。
- 排除弱點的建議，包括變更配置、更新、變更原始程式碼，或是在無法排除弱點的情況下執行補償性控制措施

卡巴斯基實驗室
企業網路安全：www.kaspersky.com/enterprise
網路威脅新聞：www.securelist.com
IT 安全新聞：business.kaspersky.com/

真正的網路安全
#HuMachine

www.kaspersky.com

台灣聯繫人：台灣銷售總監 黃茂勳 eden.huang@kaspersky.com