KASPERSKY lab

卡巴斯基反針對性攻擊平台

即時檢測高級威脅

www.kaspersky.com

危及企業安全的針對性攻擊日益猖獗，攻擊者使用的攻擊技術也越來越複雜。如今，檢測出針對性攻擊與威脅已變得更加困難，而要阻止和清除針對性攻擊與威脅更是難上加難 ，因此，企業需要部署一套全面綜合的適應性安全策略。

安全漏洞與高級威脅

大多數企業花費大量資金購買傳統的 IT 安全解決方案，這些安全解決方案多為網關安全防護軟體。雖然這些防禦性安全技術可有效抵禦常見威脅，包括惡意軟體、數據洩漏、網路攻擊等，但企業安全事故與漏洞確仍屢見不鮮。

高級針對性威脅可潛藏數周、數月甚至數年之久而不被發現，網路罪犯便會在這段時間秘密竊取用戶的重要資料，干擾重要業務流程的正常運作。若遭到此類攻擊，防禦性安全技術僅能檢測出部分事件，但通常無法識別更加危險與複雜的個別攻擊問題，這些攻擊會給企業造成嚴重損失，甚至長期的危害。

針對性攻擊潛藏時間長，對受攻擊者的網路安全構成嚴重威脅，並且使攻擊者在未經授權的情況下控制受攻擊者的 IT，還可避開傳統安全技術的檢測。

雖然部分攻擊者會使用非常有效、成本高昂的高級可持續性威脅(APTs)，但其他攻擊者則會採用單一的技術，如先進的惡意軟體或零日漏洞。

為增強傳統安全解決方案的防護水平，許多企業通過安全訊息與事件管理(SIEM)系統實現自動化流程。一些企業還開始研究專門的安全操作中心，從而將事件與數據相關聯，實現統一的安全管理並對安全事件做出響應。但是，要充分發揮這種方法的效用，就必須在網路威脅分析方面擁有全球化的安全視野與深入的專業知識。即便是跨國企業往往也難以聘請、培養並留住其內部安全團隊中的重要專家。

突破防禦性安全技術的侷限

由於過去的防禦性安全解決方案無法有效抵禦針對性攻擊，或者無法在網路罪犯入侵企業系統時將其檢出，企業需要重新審視他們的安全問題。

作為享譽全球的網路威脅研究機構，卡巴斯基實驗室建議企業安裝可持續不斷的多層級針對性攻擊防禦程序。

僅發現惡意樣本或未經授權的連接並不足以檢測出針對性攻擊。先進有效地檢測需了解正常的系統與用戶行為並對所有活動進行持續分析，以確保所有 IT 基礎設施的高可見度。為有效檢測出最新威脅，企業還需接受前瞻性的威脅更新獲取有關全球各地新興攻擊方式的情報。

企業所做的安全防護準備工作越充分，網路罪犯入侵企業系統的成本就越高。首先，企業必須明確其當前系統中存在的安全漏洞並主動清除這些安全隱患。企業還須確保樹立員工的安全風險意識，因為當網路罪犯發現有可能出現的人為錯誤，便會在發動攻擊時故意將企業員工作為攻擊對象。此外，企業安全工作人員還應接受相關培訓，學會識別針對性攻擊相關的事故並按輕重緩急將事故排序。

適應性安全策略

作為安全行業的領導者，卡巴斯基實驗室三分之一的員工都是安全研究專家，在檢測針對性攻擊與高級可持續性威脅(APT)方面成績斐然。此外，基於雲端技術的卡巴斯基安全網路(KSN)會源源不斷的接受來自全球各地發出的新威脅數據。這些”實際”獲取的寶貴數據幫助卡巴斯基實驗室每天檢測出超過 31 萬種新興惡意程序和威脅。

卡巴斯基實驗室是幫助企業改變安全策略的開創者，並以此幫助企業更好的抵禦高級威脅與針對性攻擊。我們依託世界領先的安全情報，為企業用戶提供獨有的技術和服務。在攻擊尚未造成嚴重危害前，幫助企業及早檢測出針對性攻擊並減輕攻擊風險。

我們相信，每家企業都需要建立一套基於以下四大重要因素的適應性安全策略:

- **預測**–幫助企業評估當前安全情況，明確針對性攻擊日後會如何攻擊企業基礎設施。
- **回應**–幫助企業展開調查並清除安全隱患。

- **防禦**–幫助企業抵禦高級威脅並減輕遭到針對性攻擊的風險。
- **檢測**–實施持續監控，識別針對性攻擊跡象。

卡巴斯基反針對性攻擊平台之所以可達到如此之高的攻擊檢測率，是因為卡巴斯基安全網路向平台即時傳送基於最新全球安全與威脅情報的訊息。

提供多層級適應性安全策略

卡巴斯基反針對性攻擊平台是企業適應性組成安全解決方案的一部分。即時網路流量監控、沙箱啟動與端點行為分析可讓企業 IT 基礎設施中發生的一切一目了然。適應性安全策略可有效保護企業免遭大部分複雜威脅、針對性攻擊、新型惡意軟體(包含所勒索軟體與犯罪軟體)與高級可持續性攻擊。

通過將網路、端點與全球威脅趨勢等多個層面中的事件相互關聯，卡巴斯基反針對性攻擊平台為用戶提供”幾乎即時”的複雜威脅檢測，使追溯性調查成為可能。

可疑對象負載分析–與高級持續性威脅攻擊檢測

為對可疑對象進行多層分析，卡巴斯基反針對性攻擊平台設有:

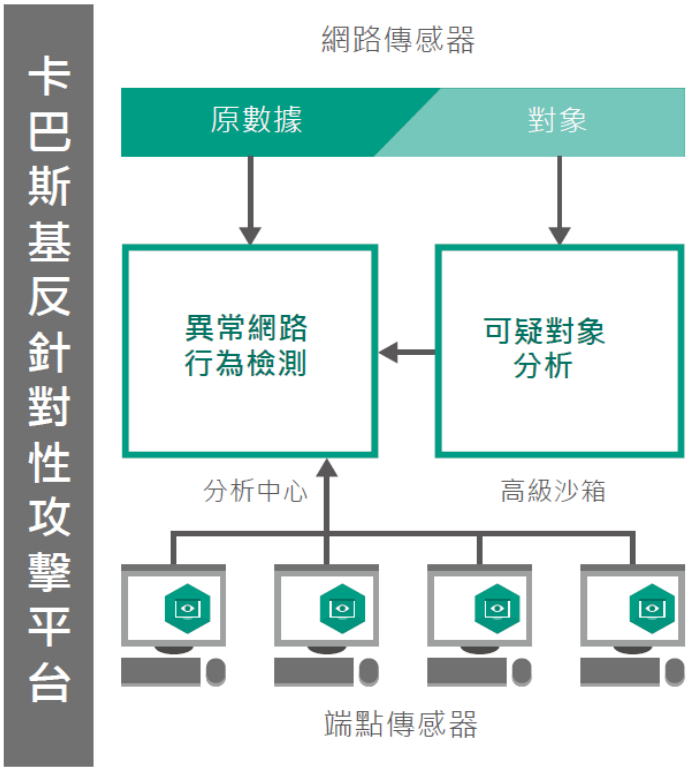
- 網路傳感器:通過監控網路流量，檢測出網路攻擊跡象。
- 郵件傳感器:過濾電子郵件中可疑危險對象。
- 網頁傳感器:使用 ICAP 協議過濾網頁中的可疑對象
- 高級沙箱技術:提供一個獨立的虛擬環境，在該環境中對來自網路、郵件及網頁傳感器的可疑對象以及這些傳感器所生成的”副產品”進行動態研究。
- 針對性攻擊分析程序會將源自網路極端點傳感器的數據與”基線圖”相結合並進行比對，以檢測可疑活動並為安全團隊提供即時準確的安全警報。

高級沙箱程序採用若干先進技術，使惡意軟體無法檢測到其正在沙箱環境中運行，因而不會自動終止運行，從而暴露其活動訊息。

異常與可疑行為監控

為進行高級網路行為分析，卡巴斯基反針對性攻擊平台設有:

- 端點傳感器(輕代理):收集企業端點上關於網路活動程序的訊息數據。
- 網路傳感器:攫截原始 IP 流量與網路活動，過濾原數據。
- 針對性攻擊分析程序:掌控正常行為模式，對網路傳感器原數據與端點傳感器發出的數據進行監控，從而檢測企業網路中的異常行為。



操作管理簡便

針對性攻擊分析程序會接收並深入分析網路傳感器與端點傳感器發出的數據，從而檢測判斷出攻擊。所有的檢測結果都會被妥善儲存，用於攻擊後調查。

其介面具備便捷輸出過濾功能，可顯示活動與安全隱患詳情，讓活動與安全隱患一目了然，從而幫助企業及早發現安全事件。此外，為方便事件回應與攻擊後調查，警報日誌還會被記錄下來，用於在卡巴斯基反針對性攻擊平台中進行分析。事件日誌紀錄還可傳送到用戶安全訊息與事件管理(SIEM)系統。

針對攻擊性事件回應服務

當卡巴斯基反針對性攻擊平台檢測到企業正遭受攻擊時，卡巴斯基實驗室的安全專家團隊會為企業提供全方位的安全事件回應服務，對攻擊進行分析與修復。安全事件回應服務涵蓋事件初步評估，證據收集、鑑定分析、詳細調查報告與修復計畫提交等全方面服務。

針對性攻擊檢測服務

小型企業有時會遭受到持續時間非常長且不易被檢測發現的網路攻擊，因此，卡巴斯基實驗室為用戶提供專門的針對性攻擊檢測服務。該服務為用戶提供單獨審查，用戶無須再另行購買其他針對性攻擊檢測產品。

此外，卡巴斯基實驗室的安全專家團隊還會為用戶提供滲透測試服務、應用程序安全評估服務與網路安全培訓服務，以確保企業可更好地應對日後的攻擊。