Comodo Valkyrie
Global Threat Analysis in Cloud

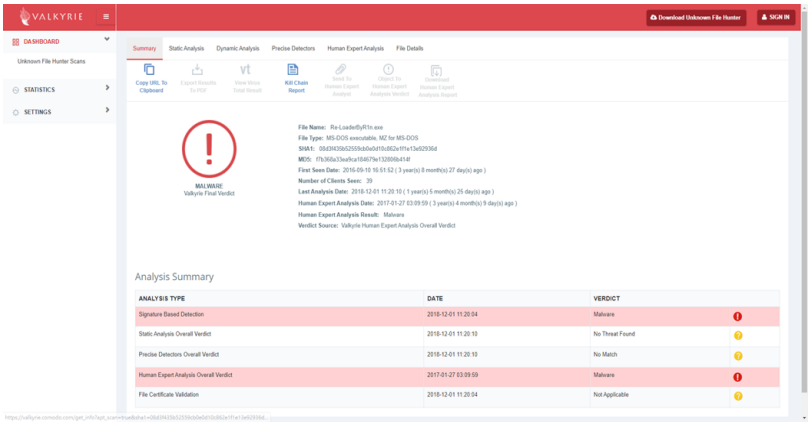
Comodo Valkyrie 是一個全球威脅分析雲服務平台，使用者可提交未知和 Zero-Day 程式至威脅分析平台進行自動化分析，Valkyrie 威脅分析平台會針對所提交的程式進行各種面向的分析作業，分析作業分為靜態分析、動態分析和進階的專家分析。Comodo 威脅分析平台在全球使用每日查詢量超過 2 億個程式，每年分析超過 3 億個未知程式。

Comodo Valkyrie 在其自動判斷系統中整合了機器學習功能與專家協同分析。研究和分析推動了“大數據”算法和方法論的發展，從而增加了判決的覆蓋範圍和準確性。成千上萬的惡意程式和信任程式用於訓練動態機器學習模型，並且定期使用新程式進行改進。

機器學習訓練技術結合了多種演算法和從程式中提取的數百種靜態特徵。機器學習模型中使用了大量惡意和乾淨程式，並定期用新程式刷新。讓機器學習的模型具備高度的準確性，並減少日常維運與漏洞利用驗證和響應相關的管理開銷。 Comodo 使用靜態、動態和更廣泛的機器學習模型來檢測惡意程式。

靜態機器學習模型知道乾淨程式的特徵。他們可以檢測潛在的新惡意程式以進行分析，例如 Zero-Day 惡意程式，這些惡意程式具有的功能尚不明確，且傳統方法不太可能檢測到。此外，針對特定惡意程式類型進行訓練的機器學習模型有助於提高自動技術的準確性。與靜態機器學習技術一樣，動態機器學習的優勢來自於發現 Zero-Day 惡意程式的高可用性。

Comodo 的動態機器學習技術使用了從程式的運行時行為中提取的數百種特徵，並結合了演算法，可產生最佳效果。 Comodo 的更廣泛的機器學習模型專注於統計相關性和趨勢，以識別攻擊活動等。 Comodo 擁有超過 25 種靜態檢測器和動態檢測器，它們被用作具有數以千計的不同特徵的統計關聯的模型，以檢測惡意程式的共同特徵並確定利用活動。



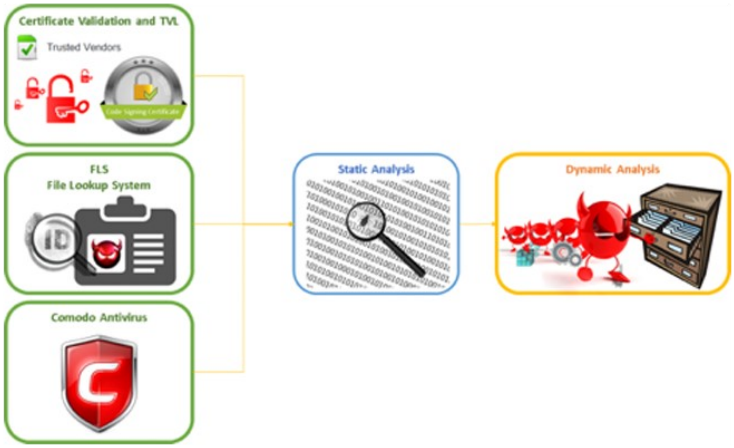
Comodo 專注於研究機器學習的模型，這些模型主要在確保準確識別漏洞利用活動的威脅。我們還透過 Comodo 全球體驗用戶與授權用戶端和獨立研究人員社群對漏洞提交的趨勢進行分析。這有助於我們確定新型態威脅的攻擊面，廣度，地理位置，行業和其他有用的元資訊，以分析和快速抑制進階威脅攻擊。

靜態分析： 26 個以上的靜態檢測器

自動靜態分析允許檢測惡意程式，這些程式可能不會被傳統技術（如防毒引擎和黑名單）識別。例如，惡意程式編寫者經常“偽裝”或壓縮其惡意程式以使其模糊並逃避分析。 Valkyrie 靜態分析支持超過 450 個拆解技術，以確保這些規避策略失敗。

Comodo Valkyrie 提取並分析提交的 PE 文件上的靜態檢測資料，並確定判決。靜態分析檢測包括： binary level analysis、libraries、embedded code、extractable links、string analysis 和 system calls，以及許多其他用於確定信任判定的檢測機制。

通過僅使用程式的二進制功能（例如格式，格式異常和程序中的 Session，Session 的內容，Session 的位置和 Session 異常）來完成自動靜態分析。靜態分析可以應用於任何類型的程式，例如 32/64 位可執行 Windows 程式，pdf 文件，Office 文檔，html 文件和獨立腳本文件，例如 bat，py，js。靜態分析是一種快速的方法，與動態分析的行為方法相比，它能夠在更短的時間內處理大量程式，但是動態分析在捕獲靜態分析遺漏的內容方面起著至關重要的作用。



動態分析：行為監控

動態分析可檢測到傳統技術可能無法識別的惡意程式。動態分析運行並監視程式的活動行為，以捕獲靜態分析方法無法檢測到的惡意程式。動態分析比靜態分析需要更長的時間，但這是檢測中重要的關鍵部分。

透由檢查程式的運行行為（例如，它是否正在嘗試創建，刪除或修改文件，機碼，進程，內存位置或其他特定的操作系統實體和網路連接）來完成自動動態分析。動態分析可以應用於不同的程式類型，例如 32/64 位可執行 Windows 文件，pdf 文件，Office 文檔和 html 文件，其中包括可執行腳本和獨立腳本文件（例如 bat，py，js）。

對提交的 PE 文件執行 Comodo Valkyrie 沙箱動態分析。自動動態分析包括對未知程式的行為和環境分析，其中包括以下內容：'反沙箱 ' 逃避，VM 逃逸嘗試，旨在等待分析的睡眠命令，對機碼的修改，檔案系統污染，系統 API 調用和回報，還有許多有助於確定信任判定的技術（程式是安全或是惡意，沒有預設）。

專家分析

Comodo 解決方案可提供由 Comodo Threat Labs 執行的專家人為分析，該解決方案可自動與支持雲的 Valkyrie Verdict Driven Platform 集成。

平均而言，Valkyrie 判決系統可在 30 秒內對提交的所有程式中的 83%提供加速判決，這是競爭解決方案的 3 倍。 但是，由於程式問題和特定的程式類型，以及惡意程式採用和發展新技術來逃避檢測和分析，大約 17%的提交無法通過靜態或動態分析獲得分析結果。

這就是為什麼 Comodo 納入專家分析，業界唯一的 100%信任判定系統的原因，在該系統中，所有程式都會得到安全或惡意的判定結果。 憑藉 Comodo SLA 服務水準平協議，Comodo 是市場上第一家也是唯一一家提供人工智能與自動分析的自動化威脅分析服務平台。

研究夥伴

Valkyrie 全球威脅分析雲服務平台提供惡意程式研究人員、合作夥伴或對惡意程式研究感興趣的任何人提供了一個強大的分析服務平台。 使用者可以透過網路直接將程式上傳到 Valkyrie 全球威脅分析雲服務平台，同時可以使用 Plug-in 插件或 RestAPI 與 Valkyrie 全球威脅分析雲服務平台服務構建更高級的互動體驗。

台灣科摩多 | 台北市大安區和平東路一段14號11樓 | TEl 02-2230-8147 | FAX 02-3322-9577
Comodo Security Solutions, Inc.| 1255 Broad Street, Clifton, NJ 07013 United States