白皮書

Symantec™ Advanced Threat Protection

利用 Symantec Cynic™ 偵測進階威脅與規避偵測的惡意程式

目 錄

簡　介…… 1

採用雲端服務的執行環境…… 1

偵測與追蹤進階威脅…… 2

將執行資料轉變成可採取行動的情報…… 3

總　結…… 4

本白皮書的目標讀者

本白皮書將說明雲端型方法的優勢，並詳述 Symantec Advanced Threat Protection中包含的 Symantec Cynic 偵測機制。

簡 介

威脅發動者使用的惡意程式開發工具，能夠以低廉的方式輕鬆地開發出自訂的目標式惡意程式，而且傳統安全系統還無法偵測到。這些相同工具涵蓋的功能也可以讓惡意程式不會被最暢銷的沙箱產品偵測到，因此儘管使用沙箱檢查，您在進階威脅偵測方面的投資仍然是毫無用武之地，不肖人士同樣可以入侵您的網路。賽門鐵克投資數十年的時間，打造能夠大規模精確辨識惡意檔案的技術；有了Symantec™ Advanced Threat Protection，我們透過新一代分析服務Symantec Cynic™，將賽門鐵克完整的分析能力直接提供給您的企業。

Cynic不單單只是沙箱偵測應用程式，更是集結許多技術的雲端型惡意程式分析平台，包括沙箱與疫情、靜態式偵測、檔案信譽、內容情報及網路流量分析。有別於要求客戶提供專屬虛擬機器或企業專用影像，以揭露疫情與偵測惡意程式的大多數沙箱分析產品，Cynic會使用此分析技術套件，進行涵蓋多種作業系統和應用程式版本的分析。以雲端服務方式執行可大規模且迅速地進行分析，這是簡易型內部部署沙箱產品幾乎無法達到的目標。由於雲端服務可以快速更新而且不會導致停機，因此賽門鐵克可以隨時更新疫情爆發環境的作業系統與應用程式，以便在攻擊和惡意程式變化時加以因應。

再者，我們可以在Cynic雲端平台上運用實體硬體，以觸發可感知虛擬機器的惡意程式；這類程式經過精心設計、專門入侵現今的沙箱偵測。快速分析多個案例、平台及應用程式版本，再搭配龐大的全球偵測器網路資料所提供的情報，意謂著Symantec Advanced Threat Protection能夠快速又精確地偵測惡意程式碼，並將誤報風險降至最低。

下列三種Symantec Advanced Threat Protection控制點產品均包含Symantec Cynic：

- Symantec™ Advanced Threat Protection：Endpoint
- Symantec™ Advanced Threat Protection：Network
- Symantec™ Advanced Threat Protection：Email

採用雲端服務的執行環境

賽門鐵克在提供高可用性雲端服務方面建立了良好的口碑，而且近20年來，Symantec Email Security.cloud和Symantec Web Security.cloud均達到SLA效能。

在真正的雲端方式中，Cynic這項彈性服務可隨選擴充，視需求處理大量物件和要求。而Cynic不受限於特定規模或處理能力，可透過Symantec Workspace Virtualization技術運用大量且各式各樣的影像，也可以快速循環處理多個涵蓋各種不同應用程式版本的案例，以觸發進階惡意程式，並有效追蹤其執行行為。

最後，賽門鐵克以雲端服務方式執行這項作業，便能升級Cynic偵測技術、新增全新檔案類型支援以及新增案例，客戶方面完全不必進行升級或變更；也就是說，隨時都能享有最佳防護能力，無需定期強制執行升級工作，藉此降低維護和管理內部部署方面的安全基礎架構所需的成本。

偵測與追蹤進階威脅

Cynic可透過專屬的判定引擎偵測惡意程式碼與可疑行為，以使用賽門鐵克十多幾年來研究和開發所打造的各種防範與偵測技術來檢測檔案。這項判定引擎可根據各項元件分析檔案產生的結果，以及龐大網路情報和偵測器網路提供的資料，來判定檔案為善意或惡意。

為了確保能夠精確偵測惡意行為，Cynic的執行環境採用各種行為追蹤技術監控使用者模式與核心模式勾點(kernel-mode hook)。此方式不僅可觀察作業系統和應用程式，也可透過外部封包擷取方式觀察網路活動。

這項行為追蹤技術只有在觸發惡意程式時才能發揮價值。為了擁有有效的執行環境，此技術備有能讓惡意程式執行的各種大量影像。這些影像和案例包含作業系統版本、作業系統修補程式等級、應用程式版本及執行階段環境版本等各種排列。

談到規避偵測的惡意程式時，惡意檔案自行偵測和辨識執行環境的情況有增長的趨勢，因此可以規避偵測或展現出完全不同的行為，以擺脫安全解決方案對其所做的偵測。惡意程式有很多方式可以根據環境嘗試修改自身的行為：

1. 尋找由代理程式行為追蹤建立和使用的特定安全廠商程序、檔案或登錄機碼。
2. 目前的沙箱技術會限制執行和分析檔案所耗費的時間，因此惡意程式通常會設法避過該時限後再開始動作。
3. 在啟動酬載(payload)之前以檢查特定人為互動證明的方式，尋找已抵達實際端點(非虛擬機器)的證據，例如滑鼠捲動或點按、鍵盤操作或甚至特定的裝置驅動程式。
4. 惡意程式也會嘗試和外部網路位置通訊，藉此偵測追蹤、偵測隔離或甚至和指令與控制伺服器通訊等，這些都屬於感染的動作。由於Cynic會在安全環境下執行惡意程式，因此可讓惡意程式對外通訊，並分析此流量做為傳回到判定引擎之資料的一部分。
5. 有些惡意程式偵測到特定硬體資源時不會執行(例如尋找實體CPU核心)，並運用存取特性做為避免偵測的方法。舉例來說，模擬或幾乎抽象的CPU回應時間和實體硬體中實際CPU的回應時間可能有所不同。

為了不讓這些或其他惡意程式規避技術得逞，Cynic已設計出大量內建技術，包括可複製實際人類行為的專用人類行為模擬器，並搭配實際執行環境，做為對抗虛擬機器感知程式碼的另一項措施。Cynic可根據其他分析引擎中的觀察，動態決定要將哪些檔案路由至這項實際執行環境，包括傳送至證據引擎的異常狀況或可疑結果，例如如果偵測到規避技術和異常的靜態分析結果。情報導向的執行功能也是Cynic脫穎而出的關鍵。Cynic具有運用賽門鐵克大量遙測資料的獨特優勢，可根據檔案信譽或在執行環境中的不同行為(相較於實際環境)做出明智決策。

提供Cynic做為雲端服務所賦予的運算能力在數分鐘內便可執行檔案、追蹤以及進行判定，而不會像內部部署解決方案需要耗費數小時或數天的時間。證據判定和檔案行為會直接傳回Symantec Advanced Threat Protection，這樣就能夠找出可能規避偵測的攻擊，並使用詳細情報快速搜尋整個基礎架構中的任何其他相關攻擊跡象。

將執行資料轉變成可採取行動的情報

三個Symantec Advanced Threat Protection控制點都可以將可疑或未知檔案傳送到Cynic進行分析。檔案經過處理後，Cynic最多會將三組資料回傳到Advanced Threat Protection平台。

1. 判定結果：二元決策，非善意即惡意。
2. 執行報告：執行時的完整追蹤檔案行為。
3. 情報報告：賽門鐵克對於該威脅所掌握的任何及所有資訊。

Symantec Advanced Threat Protection以資安事端的方式讓提供這三種資料集的整合檢視，也就是重要性足以引起安全分析師重視的一或多個可疑活動或行動集合。所有跨端點、網路及電子郵件的企業基礎架構資安事端，都會顯示在Incident Manager中。這是Symantec Advanced Threat Protection管理主控台的單一檢視畫面，安全分析師可以在此協調可疑和惡意檔案的調查和矯正措施。調查和矯正功能的相關示範請參閱http://atp.symantec.com

當Cynic傳回惡意檔案的結果時，Symantec Advanced Threat Protection會自動執行兩個動作。

1. 在Incident Manager中建立新的資安事端。
2. 如果判定結果在電子郵件系統管理員設定的保留時間上限內傳回，Advanced Threat Protection: Email會攔截電子郵件傳送。

此資安事端包含做為執行報告一部分所傳回的資料，亦即事件摘要和檔案執行時採取的行動。此報告輸出內容會詳述磁碟讀取和寫入、該物件啟動的任何網路通訊，以及已建立或修改的任何檔案、程序及登錄機碼。也會包含該物件採用的入侵技術相關資料，例如處於睡眠狀態的時間，或是排定執行的任何工作或程序。安全分析師可藉由這些資料點，利用Symantec Advanced Threat Protection內建的強大搜尋和清除能力探索整個企業中的其他感染。

除了此檔案的專屬資料，Cynic還會提供賽門鐵克對於該攻擊所掌握的詳細資訊，包括之前已觀察到該攻擊或檔案的國家、首次和最後一次觀察到的時間、所有已知和替代路徑與檔案名稱、建立的替代檔案和任何相關或相似檔案，以及賽門鐵克是否認為這是專門針對企業所發動的攻擊。

Symantec Advanced Threat Protection也會在單一位置交叉比對符合或和此攻擊有關的任何資安事端，完全不必手動搜尋。安全分析師可以顯示所有相關的攻擊元件並迅速矯正。例如做為攻擊一部分所使用或建立的檔案、攻擊鎖定的所有電子郵件地址，以及所有惡意IP位址和網域。

此舉可大幅減少安全分析師需要調查的資安事端數量，這表示進階攻擊不僅能夠獲得偵測，還能在數分鐘內加以遏止，無須花費數週或數月的時間。

總 結

賽門鐵克的多面向分析是真正的新一代執行環境。Cynic可運用許多賽門鐵克業界最佳的專利申請中技術，而且每天吸收60GB的全新彙總安全情報做為後盾。此情報是由數百萬個端點和閘道中的數百億則事件所提供。這些全都可以提供判定和分析結果給您，以及賽門鐵克在範例中所掌握的珍貴威脅情報，提供您採取行動所需的相關資訊。

Cynic可以針對所有可攜式執行檔類型，以及 Java 配置區、PDF 文件、Microsoft Office 文件和 ZIP 等容器檔案，處理並傳回情報。其他適用的檔案類型和作業系統將會陸續新增。

關於賽門鐵克 (Symantec)

賽門鐵克 (Symantec) 已於 2019/11 併入全球網通晶片巨擘--博通 (BroadCom，美國股市代號 AVGO，全世界網際網路流量有 99.9% 經過博通的網通晶片) 軟體事業部的企業安全部門 (SED)，特別是近年以半導體的嚴謹、系統化以及零錯誤思維來改造核心技術、管理框架以及整合最完整的資安生態體系，讓賽門鐵克的解決方案在穩定性、相容性、有效性以及資安生態系整合擴充性，有著脫胎換骨並超越業界的長足進步。博通 (Broadcom) 是務實的完美主義者，致力於追求卓越、關注細節並且有系統和紀律地投入科技創新與嚴謹工藝，同時也大大降低交易複雜性。Symantec 持續創新的技術能為日新月異的資安問題提供更好的解決方案，近三年 Symantec 很少出現在由公關機制產生的頭版文章中，而且在全球前兩千大企業的市佔率及營收成長均遠遠高於併入博通之前，增長幅度也領先其他競爭對手，是科技創新驅動的解決方案非常穩健可靠深受大型企業信賴的實證，也顯示大型企業顧客對轉型中的新賽門鐵克未來充滿信心。(美籍華人王嘉廉創辦的企業軟體公司，組合國際電腦（CA Technologies）以及雲端運算及「硬體虛擬化」的領導廠商--VMware， 也是博通軟體事業部的成員)。2021 年八月，因應國外發動的針對性攻擊日益嚴重，美國網路安全暨基礎架構安全管理署（CISA）宣布聯合民間科技公司，發展全國性聯合防禦計畫 JCDC(Joint Cyber Defense Collaborative)，而博通賽門鐵克是首輪被徵招的一線廠商，如就地緣政治考量，Symantec 也絕對是最安全的資安廠商。擁有更強大資源與技術為後盾的賽門鐵克已更專注於整合各種最新科技於既有領先業界的端點、郵件、網頁以及身分認證等安全解決方案。

關於保安資訊 www.savetime.com.tw

保安資訊團隊是台灣第一家專注在賽門鐵克解決方案的技術型領導廠商，被業界公認為賽門鐵克解決方案專家。自 1995 年起就全心全力專注在賽門鐵克資訊安全解決方案的技術支援、銷售、規劃與整合、教育訓練、顧問服務，特別是提供企業 IT 專業人員的知識傳承 (Knowledge Transfer)、協助顧客符合邏輯地解決資安問題本質的效益上，以及基於比原廠更孰悉用戶使用情境的優勢能提供更快速有效的技術支援回應，深獲許多中大型企業與組織的信賴，長期合作的意願與滿意度極高。許多顧客樂意與我們建立起長期的友誼，把我們當成可信任的資安建議者、可以提供良好諮商的資安策略夥伴以及總是第一個被想到的求助暨諮詢對象。

保安資訊連絡電話：**0800-381-500**。