Acronis

白皮書

為什麼 Acronis 網路防護解決方案能防範各種威脅？

什麼是網路攻擊以及如何運作？

簡介

目前存在的網路威脅不計其數：不同的攻擊類型和媒介，專為突破企業與家庭用戶網路安全而設計。網路罪犯追求的目標不外乎是金錢、資料或造成業務中斷，他們會利用各式各樣的惡意軟體和感染媒介來達成這些目標。好的網路防護和網路安全解決方案必須能將其一網打盡。在本白皮書中，我們將針對目前存在的各類威脅和網路防護與網路安全的差異進行說明，以及 Acronis 網路防護解決方案抵禦所有的攻擊媒介，並提供最極致的端對端網路防護。

什麼是網路攻擊？

高層級的網路攻擊是對電腦、智慧型裝置或網路進行的數位攻擊。網路罪犯會利用各類攻擊媒介和技術來入侵並感染系統，最終達成其帶有惡意的目的。

我們必須區別大規模攻擊和針對性攻擊。大規模攻擊一般透過攻擊活動進行，並包含涵蓋廣大受害者的「服務式」配置。攻擊活動可能是垃圾郵件、網路釣魚，以及合法網站的大規模感染等。這些類型的攻擊會自動執行，每個人都可能成為受害者。

另一方面，針對性攻擊則會事先挑選並分析受害者，而這類的攻擊通常以手動執行。最高明的針對性攻擊名為進階持續性威脅 (APT)。這類的攻擊通常包含數個階段，可能長達數月之久，且難以偵測。

所有的攻擊都包括基本的階段：準備、感染和後續執行。試想一下，如果您的安全解決方案無法回應其中幾個階段，很可能就會遺漏或太晚才偵測到威脅。

攻擊媒介

攻擊包含多個媒介，而您的安全防禦策略必須能對應所有類型。

最常見的攻擊媒介為：

- 電子郵件，例如：惡意附件
- 偷渡式入侵，例如：帶有瀏覽器入侵程式的網站
- 暴露在風險中的服務，例如：易受攻擊的 RDP 伺服器
- 有效帳戶，例如：帳戶盜用
- 供應鏈，例如：軟體更新綁架
- 硬體，例如：USB 快閃記憶體

首先，也是關鍵的一點，是透過電子郵件。攻擊可以透過網路或應用程式電子郵件用戶端來傳遞。威脅會透過電子郵件傳遞，並會以多種形式呈現：惡意連結、惡意附件、社交工程等等。我們稍後會談到所有的選項。

威脅也能透過軟體和服務內的弱點入侵進行傳遞。弱點儘管一無是處，但在受到入侵前都不具危險性。不巧的是，不管您是使用者或系統管理員，都不會知道弱點是否曾遭到入侵。這就是為什麼您必須修補所有已知弱點，並針對沒有修補程式的零時差攻擊和未知弱點進行防範。弱點可能常駐於遭暴露的伺服器服務中，例如：Microsoft DNS 伺服器，該伺服器曾有過遠端程式碼執行弱點 (CVE-2020-1350)，並已於七月修復。然而，弱點也存在於網頁瀏覽器等用戶端應用程式中，如果您造訪惡意製作的網站，就可能遭到入侵，這種方式又名為偷渡式下載攻擊。

您可能因帳戶盜用而遭到感染：網路罪犯控制了合法帳戶，並作為執行惡意動作的大本營。例如，如果網路罪犯猜中密碼並損毀系統管理員帳戶，便能夠刪除備份，同時複製機密資訊。

另一個有點類似於帳戶盜用的攻擊媒介稱為信任關係或供應鏈攻擊。這與您的合作夥伴或服務供應商受到入侵有關。如果使用的應用程式軟體廠商遭到入侵，您就可能自動從他們的網站下載惡意更新。華碩在 2019 年初就發生了這樣的事，他們當時遭到入侵，並在不知情的情況下開始散播受感染的驅動程式更新。

攻擊者有時候會利用實體裝置，例如內藏惡意軟體的 USB 快閃記憶體，並刻意放在公眾場合或遭鎖定企業的附近，期盼有人會出於好奇而插入電腦之中。

值得注意的是，每種攻擊媒介都可能使用不同的攻擊技術。這些就是人們在我們談論安全性威脅時所想到的。

網路攻擊技術

所有不同的攻擊媒介，都可能套用不同的方法和技術。有些概念可套用至不同的群組 (例如，社交工程)，而其他的技術 (如探查) 則能讓罪犯尋找有用的資訊，以發動後續攻擊。

社交工程

社交工程不外乎人為因素。攻擊者會編造一則具有說服力的故事，誘騙使用者執行特定的動作。這是目前最危險也最有效的網路攻擊技術。人們一向是資安中最弱的一環，因為若您的創意十足，幾乎能說服人們做任何事。

社交工程可以結合帳戶盜用和模擬攻擊，讓探索工作窒礙難行。例如，如果您老闆的帳戶遭到入侵，就很難證實指示您開啟附件的電子郵件不是您老闆傳來的。這就是為什麼即使您的人員已受過適當的網路釣魚垃圾郵件訓練，您還是須備妥適當的網路安全解決方案。

密碼攻擊

密碼攻擊是帶著非法意圖來試圖取得或使用使用者密碼的行為。網路罪犯可能使用密碼探查程式、字典攻擊和破解程式來取得使用者的密碼。由於雙因素驗證大多派不上用場，有些時候，罪犯光靠密碼攻擊就能帶走他們想要的。您只要具備基本的常識 (不告訴別人密碼、不寫下密碼、不在多項服務上使用相同的密碼)，並使用高強度的長密碼或密碼管理員，就能防止密碼攻擊。

網路釣魚和魚叉式網路釣魚攻擊

網路釣魚是一項使用看似來自可靠來源的詐騙通訊 (電子郵件、訊息、SMS 和網站) 的技術。攻擊者會模擬合法的服務品牌，利用人們對那些品牌一直以來的信任感，來誘騙他們分享認證。例如，網路罪犯可以建立一個看似 Office 365 入口網站的網頁，就能在背景竊取使用者認證。這是一項相當常見攻擊技術，並常與社交工程一併使用。網路釣魚可能導致您公開自己的機密資料 (PII、信用卡號等財務資料等)、安裝惡意軟體，或造訪受感染或惡意網站。

魚叉式網路釣魚也有目的相同，但專門鎖定經過社交網路分析的真實人物，再發動攻擊。魚叉式網路釣魚通常令人深信不疑，若網路安全產品未能察覺，一般都難以辨識。

偷渡式攻擊

偷渡式攻擊散佈惡意軟體的方法既隱密又危險。這也是在您朋友辯稱「我不會點任何連結，也不會造訪任何可疑網站」，所以不需要執行網路安全時，可以引用的好例子。

偷渡式攻擊的運作方式如下：網路罪犯會利用設定草率或未經修補的網站，並將惡意指令碼插入其中一個網頁。一旦使用者造訪網站，該指令碼即會入侵瀏覽器或外掛程式中的弱點，並在電腦中安裝惡意軟體。在大部分的情況下，這些指令碼都會經過混淆處理，導致難以偵測。這類型的攻擊之所以稱為偷渡式，是因為受害者只需造訪遭到入侵的網站，不需要執行任何動作，就可執行。

零時差攻擊弱點入侵

零時差攻擊弱點在世界各地出現的當下，廠商還無從得知的軟體弱點，所以沒有可用的修補程式。正因如此，您只能倚賴修補程式來保護自己。零時差攻擊弱點通常伴隨著會濫用該缺陷的零時差攻擊而來。一般的網路安全解決方案很難偵測到這類攻擊，因為這不僅需要對系統有透徹的了解，還要不時地監控所有應用程式。終有一天所有弱點都會攤在陽光下，漏洞也可用安全修補程式填補。問題是，有時候即使沒有花上好幾年，也要花好幾個月才能獲得解決。

SQL 插入攻擊

結構性查詢語言 (SQL) 經常在含 Web 伺服器在內的伺服器中使用。SQL 插入表示攻擊者在使用 SQL 的伺服器中插入惡意程式碼，並強制伺服器揭露平常不會揭露的資訊。例如，攻擊者只要在易受攻擊的網站搜尋方塊中提交惡意程式碼，便能執行 SQL 插入，並取得這個 Web 應用程式的所有者帳戶。

跨站台指令碼處理 (XSS) 攻擊

與 SQL 插入類似，跨站台指令碼處理 (XSS) 是一種攻擊者可以從原本可靠的網站將惡意指令碼傳送至內容的插入缺口。由於設定草率或弱點之故，讓攻擊者得以將程式碼附加至 Web 應用程式，才會發生這類事件，惡意程式碼會隨著傳送至受害者瀏覽器的動態內容一起傳送。入侵程式會包含以 JavaScript、Flash、HTML、Java 和 Ajax 等語言撰寫的惡意指令碼。

惡意軟體攻擊

許多網路攻擊都使用了惡意軟體。如同我們先前說明的，惡意軟體有許多管道能進入系統：使用者下載並啟動、以偷渡方式自動安裝、透過弱點自動下載並執行等等。

中間人 (MITM) 攻擊

中間人 (MitM) 攻擊會在攻擊者攔截流量以竊取或修改傳輸的資料 (即登入資訊、密碼和財務資料等) 時發生。攻擊者會冒充成合法服務，並像 Proxy 般傳送所有流量。攻擊通常會在不安全的公共 Wi-Fi 網路上發生，攻擊者可以在訪客的裝置和網路之間將自己輕鬆插入。如此一來，他們就可以安裝惡意軟體或將使用者重新導向至惡意網路。大家都認為 HTTPS 能防止這類攻擊，但事實並非如此。簡單的 HTTPS 加密只能保護到伺服器端的流量，但無法驗證伺服器端點的真實性。

惡意軟體類型

木馬程式

有時候稱作特洛伊木馬程式，木馬程式是最普遍的惡意程式類型。木馬程式不會像病毒般複製，但會大肆破壞。木馬程式不但會發動攻擊，還會建立方便日後攻擊的後門程式。

勒索軟體

這個常見的惡意軟體類型會阻止您存取系統的資料。勒索軟體通常會使用非常強大的加密演算法來對資料進行加密，所以您無法靠自己解密資料。若想解密資料，就得用加密貨幣支付贖金。若不支付贖金，攻擊者也可能威脅發佈或刪除機密資訊。

病毒

這是一種惡意程式，但多數媒體或使用者誤標為所有的惡意軟體程式。數位病毒可以修改其他合法的主機檔案 (或其指標)，讓受害者的檔案在執行時，也會同時執行病毒。單純的病毒可以進行複製，但目前並不常見。

廣告軟體和 PUA (潛在的垃圾應用程式)

危險性不大，但相當擾人的軟體程式，常被可疑的企業當作行銷工具。這些通常會應用程式執行時以廣告或橫幅的形式顯示。

蠕蟲

蠕蟲的自我複製以及在網路上傳播的特性是明顯的特徵。蠕蟲的危險之處在於使用者不必互動就能傳播。

根目錄與開機套件

這是一種精密的惡意程式，可隱藏在硬碟的主開機記錄或作業系統中。原本開機套件是一個能啟用電腦或網路的系統管理員存取權的工具集合。如今開機套件已相當罕見，通常與惡意軟體相關聯，例如木馬程式、蠕蟲和病毒等，它們會隱藏其存在與動作，不讓使用者或其他系統處理程序發現。

間諜軟體

這類型的惡意軟體針對蒐集受害者機器上的資訊而設計的。間諜軟體會在不經您同意或在您不知情的情況下追蹤您執行的所有動作，並直接將資訊傳遞到遠端的網路罪犯。間諜軟體也可以透過網際網路在系統上安裝其他惡意應用程式。

執行指令的惡意軟體或惡意的指令碼

這些惡意軟體之前稱為巨集病毒。但一般來說，它們都是由合法程式所執行，以執行惡意活動的任何類型的指令碼。這幾年來，它們與無檔案型攻擊無端扯上關係。但只要想想該詞彙便知，指令碼仍是硬碟中或是任何其他儲存來源中的檔案。

殭屍網路

您的機器會被執行惡意活動所控制，這些活動包括散播惡意軟體、阻絕服務和分散式阻絕服務攻擊。相對來說，光靠殭屍病毒造成的損害並不大，若沒有連線到命令與控制伺服器更是如此。那就是殭屍病毒與殭屍網路整合時，殭屍網路能造成讓業務完全停擺等重大損害的原因。

無檔案型攻擊

無檔案型攻擊通常是與惡意軟體和入侵相關聯的網路威脅。無檔案型攻擊的定義數量眾多，還有一些變種形式。簡單來說，無檔案型攻擊是以磁碟為標的之無特定惡意檔案的攻擊。

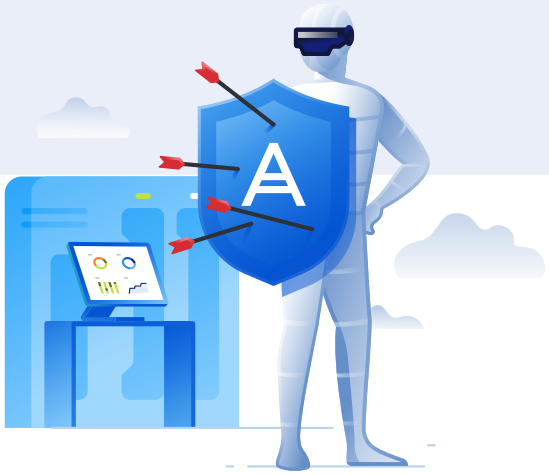
無檔案型攻擊利用合法的應用程式和處理程序來執行權限提升、承載傳遞和資料蒐集等惡意活動。若在無檔案型攻擊中使用了預先安裝的合法軟體，則這項技術通常稱為離地攻擊。通常我們只看到部分的攻擊鏈階段使用無檔案技術，從技術的角度來看，整個攻擊並非無檔案。

這一切都可能只發生在隨機存取記憶體 (RAM) 中，且不會在機器重新開機後留下任何痕跡。這表示，不會針對與應寫入目標硬碟的惡意活動相關的事物發動攻擊，意味著無檔案型攻擊對檔案型白名單、特徵碼偵測及硬體驗證等現有的安全偵測技術有十足的免疫力，因為基本上不會留下數位鑑定資料調查人員用來識別並得知日後攻擊的證據。

ACRONIS 網路防護解決方案處理這些攻擊技術的方式

透過網路安全和 Acronis Cyber Protect Cloud 等網路防護解決方案或內部部署解決方案 Acronis Cyber Protect，來抵禦這些潛在的網路攻擊並維護系統與資料安全是至關重要的。當前的網路安全產業所面臨的問題是單一產品很難防護所有類型的威脅，所以企業常得使用多個解決方案，或被迫讓步，並在安全界限上留下漏洞，而這樣的作法不但危險也不明智。通常網路安全解決方案無法保護資料，並保證快速復原和企業的永續經營。

Acronis 網路防護解決方案，結合了網路安全與資料防護，是一項能解決所有威脅的近乎完美的解決方案。這項解決方案提供了創新的整合式多層次防護，搭配每個解決方案內適當調校的技術，以阻絕本白皮書中所談到的威脅。這就是所謂的 Acronis 網路防護方法。我們看看下表，當中涵蓋了先前說明的所有媒介和技術，以及對應的 Acronis 安全技術。



ACRONIS 安全技術			
攻擊媒介或技術	**主動式階段**	**使用中階段**	**回應式階段**
透過電子郵件發動攻擊		URL 篩選	URL 篩選、行為型引擎、靜態 AI 分析器、雲端偵測、防止入侵
利用弱點，包括零時差攻擊弱點	弱點評估、修補程式管理	防止入侵	
帳戶盜用			URL 篩選、行為型引擎、靜態 AI 分析器、雲端偵測、防止入侵
信任關係或供應鏈攻擊			URL 篩選、行為型引擎、靜態 AI 分析器、雲端偵測、防止入侵
社交工程		URL 篩選	URL 篩選、行為型引擎、靜態 AI 分析器、雲端偵測、防止入侵
網路釣魚和魚叉式網路釣魚攻擊		URL 篩選	URL 篩選
無檔案型攻擊	弱點評估、修補程式管理	URL 篩選、行為型引擎、雲端偵測、防止入侵	靜態 AI 分析器
偷渡式攻擊		URL 篩選、行為型引擎、防止入侵	
惡意軟體攻擊		行為型引擎、雲端偵測、防止入侵、Acronis Active Protection、靜態 AI 分析器	靜態 AI 分析器
中間人 (MitM) 攻擊		行為型引擎、雲端偵測、URL 篩選	靜態 AI 分析器
密碼攻擊	2FA	暴力破解偵測	
包含殭屍網路		行為型引擎、雲端偵測	靜態 AI 分析器
竄改			Acronis Notary (透過區塊鏈)
SQL 插入攻擊		URL 篩選	
跨站台指令碼處理 (XSS) 攻擊		URL 篩選	

主動式 (或預防) 階段

事前預防威脅、修補系統、使用驗證等。

使用中階段

安全技術會偵測目前在系統中執行的使用中威脅或攻擊。

回應式階段

威脅可能已在系統中，或已執行第一階段的攻擊。例如，您收到了網路釣魚電子郵件。請務必記住，即使威脅已經進入系統，並不代表系統也會遭到破壞，這是因為實際的承載可能在很久之後才會下載，而我們在這個階段就會偵測到威脅。

如您所見，搭配多層次安全性堆疊的整合式 ACRONIS 解決方案可以戰勝上述的所有技術，並維護系統與資料的安全。