本月威脅：無檔案惡意軟體

這是什麼？

在每場魔術表演中總有些時刻，您能清楚地瞭解到台上的魔術師展示令人驚嘆幻象的方法。這可能是因為在您的注意力被帶往某個方向時，魔術師悄悄地在另一個方向施展了巧妙的手法。您可以用相同的方式來理解無檔案惡意程式；就像個彆腳的演員，在您注意錯誤方向時試著偷偷讓惡意軟體侵入您的防禦。防毒軟體一直在掃描您的硬碟？這種鬼鬼祟祟的惡意軟體會從 RAM 中運作，不會在硬碟中寫入任何檔案。因此不管您怎麼掃描，都不可能找到任何東西。在掃描的同時，新的惡意軟體會在您的筆記型電腦中建立指令和控制通道。在您認為軟體動了手腳時，（壞）兔子就已被帶出帽子了。

為何您應該關心？

任何先進到足以躲過特定類型偵測的威脅都值得您付出時間關心。無檔案技術已存在一段時間，而且能用來隱藏既有的惡意軟體。舉例來說，**Kovter** 最初是勒索軟體，在生命週期中曾透過垃圾郵件和惡意廣告傳播，最近更發現了能避開傳統偵測的無檔案惡意軟體版本。另一種知名的攻擊採用 **DNS Messenger** 的形式。這種攻擊方式會發動多階段攻擊，其中至少有一部份就是透過無檔案惡意軟體的方式避開偵測。最近的 DNS Messenger 活動開始於一封鎖定目標的魚叉式網路釣魚電子郵件。這封電子郵件偽裝成美國證券交易委員會 (SEC) 傳送的郵件，藉此提高合理性並說服使用者打開郵件。這封電子郵件包含一個看起來為官方附件，但會在開啟時啟動複雜的一系列活動，藉此引發惡意軟體感染。

無檔案惡意軟體如何運作？

無檔案惡意程式是種極難偵測的駐記憶體式惡意軟體，能夠從系統記憶體（而不是硬碟）中發揮作用，不會建立任何檔案。儘管讓所有活動不留痕跡是幾乎不可能達成的事，無檔案惡意軟體在硬碟中通常不會留下太多活動證據。證據保留的時間也會因攻擊動機和攻擊者能多快達成攻擊目標，隨攻擊者而異。除了證據留存的問題之外，由於此類惡意軟體在記憶體中執行，只要受害者的電腦重新開機，記憶體中的惡意軟體和所有可供偵測及入侵後鑑識調查的證據都會隨之遭到清除。

為何我們重視這一點？

防毒軟體和其他端點技術會掃描檔案，偵測惡意或可疑的程式碼。防毒軟體還會特別搜尋符合已知不良檔案的特徵。由於具備沒有檔案可供掃描或從中產生雜湊以供比較的特性，無檔案惡意軟體能避開檔案中心式技術的偵測，在您的環境中隱藏較久的時間。

深入閱讀

思科 Talos™：DNSMessenger
http://cs.co/9000DLppO

思科 Talos：DNSMessenger 更新
http://cs.co/9005DLpVH

思科 AMP 示範：
http://cs.co/9008DLpTE

CXX-XXXXXX-00　09/18

瞭解我該怎麼做？

若要偵測並封鎖無檔案惡意軟體，需要採用進階的端點保護並將其納入更廣泛的防禦策略中。攻擊者會嘗試運用各種技術組合來入侵您的網路，因此您需準備好相應的防禦措施。例如，面對 DNS Messenger（以及任何使用 DNS 連線至惡意網路基礎架構的惡意軟體型態）時，DNS 層安全性就能非常有效地遏止攻擊。如果能實施多層安全措施，同時搭配有效的最前線防禦（例如 DNS 層）和最後防線（偵測特徵以外的端點技術），就能提高您看穿魔術技倆的機會，避免魔術師在一陣煙霧中帶著您的資料遠走高飛。

思科如何保護您？

進階惡意軟體防護 (AMP) 終端版	使用記憶體防護和入侵指標來偵測無檔案惡意軟體，例如異常網域名稱系統 (DNS) 通訊和混淆化的 Windows 登錄機碼。
思科電子郵件安全設備	偵測並封鎖網路釣魚
思科資安防護傘™	封鎖命令控制流量
新世代防火牆/ 新世代入侵防禦系統/ 思科 Stealthwatch®	偵測並封鎖惡意流量，例如命令控制流量、試圖傳播惡意軟體等。