資安

追求隱形：無檔案惡意軟體


Marc Blackmer
2018 年 9 月 13 日 3 則留言

我最近聽到一則報導，是關於一份問卷詢問人們會想選擇飛行還是隱形能力。的確，這是個蠢問題*。但人們做出各自選擇的*原因*卻顯得十分有趣。大多數人選擇飛行。讓我覺得十分有趣的是，問卷的作者認為多數人實際上更想選擇隱形能力。然而，他們選擇飛行是因為隱形會讓他們聯想到不道德和犯罪的行為。

這樣的聯想當然會讓我想到資安問題。隱形是網路犯罪分子努力想達成的目標，而無檔案惡意軟體的開發讓他們十分接近隱形。

無檔案惡意軟體是一種駐記憶體式惡意軟體。如字面意義所示，這種惡意軟體不是磁碟中的檔案，而是從植入於受害者的系統記憶體。由於沒有檔案可供掃描，因此更難偵測這種惡意軟體。另外，由於這種惡意軟體會在受害者電腦重新開機時消失，因此也會讓鑑識調查更難進行。

和其他任何惡意軟體一樣，無檔案惡意軟體可透過網路釣魚、惡意網站等方式進入網路。差別在於無檔案惡意軟體不會在感染時安裝或執行任何可執行檔。因此這種惡意軟體才稱之為「無檔案」惡意軟體。這種惡意軟體會在系統記憶體內執行，操縱管理公用程式（例如 Windows PowerShell 和 Windows Management Instrumentation (WMI)）為其工作。由於許多資安技術明確地信任這些公用程式，這種惡意軟體就能躲過偵測，使活動呈現良性。

思科 Talos 威脅情報團隊曾在 2017 年底發布一篇部落格文章，講述他們稱之為 DNSMessenger，富有創意的無檔案惡意軟體案例。（您可在此閱讀完整的 DNSMessenger 相關部落格文章）攻擊者透過電子郵件傳送遭到感染的 Word 文件給受害者，並引誘使用者在文件中啟用巨集。一旦啟用，巨集就會啟動 Windows PowerShell 指令檔，透過 WMI 連線至特定網域。惡意軟體會從與這些網域相關的 DNS TXT 檔案收到進一步的指示。

由於不會安裝任何檔案，且將惡意指示巧妙地放在受害者網路*外*的 DNS 記錄中，因此以檔案為中心的傳統惡意軟體偵測技術無法偵測到這種威脅。由於從以檔案為主的角度看來一切如常，需要更仔細監控 DNS 流量才能偵測到威脅。

無檔案惡意軟體作者使用的另一種技術，是將編碼指令放到一個或多個特定的 Windows 登錄機碼中。登錄是資安產品偵測惡意軟體時通常不會去注意的區域。資安產品信任登錄。因此，PowerShell 指令檔讀取登錄機碼的活動不會遭視為異常。異常之處在於，登錄機碼通常不會編碼。再次強調，由於檔案式惡意軟體偵測無法發現此類威脅，因此我們需要能搜尋混淆化登錄機碼的端點防護。

請參考以下案例，瞭解攻擊者能夠將受信任程序和個別資安技術間的缺口運用到什麼程度。

攻擊者不會在試過一種攻擊媒介發現沒效後直接放棄。為了在您的網路中取得立足點，他們會撬動每個門把、檢查每扇窗戶，並測試能把哪些東西塞入門縫。而防護中的缺口有助於他們達成目的。因此，合理推斷一種資安技術無法防範所有種類的攻擊。我們需要封鎖網路釣魚攻擊、從電子郵件中去除惡意附件、阻擋前往不良網域的流量，以及監控端點資料中心內外的網路流量是否有異常。

透過單一攻擊媒介偵測到威脅時，還需要與所有防禦技術分享情報，而且最好要能自動分享。

幸好我們不只能完成以上所有工作，還能提供更多服務。首先，我們已開發無檔案惡意軟體的入侵指標，例如偵測到異常 DNS 請求內容，或可能用於混淆惡意指令的異常 Windows 登錄機碼時，能夠予以示警。

其次，我們每天會從數千億封電子郵件和超過 1000 億個 DNS 請求中收集遙測資料，並分析近 200 萬個惡意軟體樣本。我們透過數千個誘捕系統 (honeypot) 和惡意軟體反向工程進行研究，同時也在進行漏洞研究。由於研究範圍包括網路、端點、網頁、雲端、電子郵件和檔案，我們能瞭解及偵測更多威脅。所有的研究成果均用於我們整個資安產品組合，藉以為您提供保護。

若您想深入瞭解無檔案惡意軟體，請務必閱讀前文的 Talos 部落格文章連結，並可在此閱讀該篇文章的後續。這兩篇文章的結尾都提供了一張清單，說明我們能如何協助減輕無檔案惡意軟體的威脅。一如往常，我們很樂意提供即時線上示範或我們資安專家的個人化示範，藉此與您分享我們的技術。

* 我會選什麼？我會選飛行。真的，我沒騙人。

您是否喜愛這些類型的文章？訂閱「本月威脅」系列部落格文章，以便在識別出威脅時獲得警示。

標籤：

- AMP
- 無檔案惡意軟體
- 惡意軟體
- 資安
- 資安思維領導
- 本月威脅