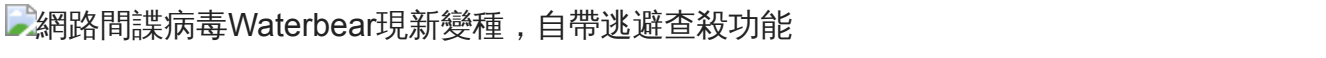
網路間諜病毒Waterbear現新變種，自帶逃避查殺功能

2020年01月03日*12:50:08* 科技 1521 閱讀模式



BlackTech，一個主要以東亞地區（尤其是中國台灣，也包括中國香港和日本）的技術公司和政府機構為攻擊目標的網路間諜組織，且並被認為是惡意軟體「Waterbear」的幕後操控者。

Waterbear是一種模塊化惡意軟體，已經存在了多年，其載入模塊能夠通過從命令和控制（C2）伺服器下載有效載荷來實現不同的功能。在大多數情況下，有效載荷都是後門程序，可以接收和載入其他模塊。

最近，網路安全公司趨勢科技（Trend Micro）捕獲了Waterbear的一個最新變種，其載入模塊不僅會下載第一階段後門，而且還會下載一個會將代碼注入特定的安全產品中進行API掛鉤來隱藏第一階段後門惡意行為的有效載荷。

舊版本Waterbear

如上所述，Waterbear具有模塊化的結構，通過載入模塊（DLL文件）解密並執行RC4加密的有效載荷。一般情況下，有效載荷都是第一階段後門，用於從攻擊者那裡接收並載入其他可執行文件。

根據功能的不同，第一階段後門大致可分為兩種：第一種，連接C2伺服器；第二種，偵聽特定埠。

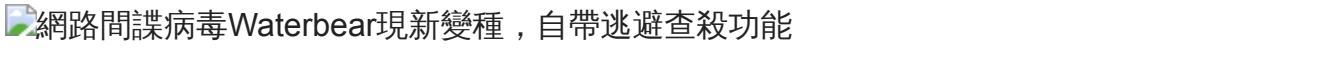


圖1.典型的Waterbear感染鏈

如上圖所示，典型的Waterbear感染從一個惡意DLL載入程序開始，而涉及到的觸發技術也分為兩種：第一種，修改合法的伺服器應用程序以導入和載入DLL載入器；第二種，執行虛擬DLL劫持和DLL端載入。

為了逃避安全檢測，有效載荷會在執行實際的惡意常式之前對所有的函數塊進行加密，然後只會在需要使用函數時，解密相應函數並執行，而之後則會再次對函數加密。

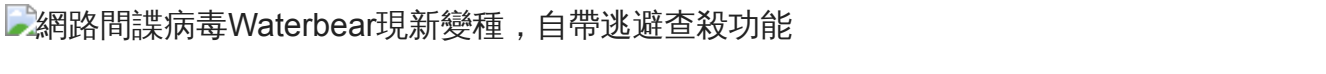


圖2.解密-執行-加密函數

新版本Waterbear

與之間的版本不同，趨勢科技此次捕獲的新版本Waterbear載入了兩個有效載荷。其中，第一個有效載荷會將代碼注入特定的安全產品中進行API掛鉤來隱藏其惡意行為，而第二個有效載荷則是典型的Waterbear第一階段後門。

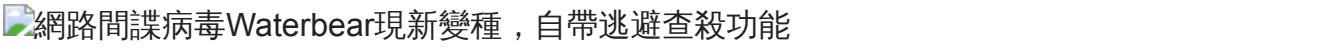


圖3.新的Waterbear感染鏈

兩種有效載荷均經過加密處理，存儲在受感染計算機的磁碟上，並注入到同一服務（如LanmanServer）中。

趨勢科技表示，新版本Waterbear的載入程序首先會試圖從文件中讀取並解密有效載荷，然後對其解密，並按如下條件執行線程注入：

1.如果在磁碟上找不到第一個有效載荷，則將終止載入程序而不會載入第二個有效載荷（即第一階段後門）。

2.如果第一個有效載荷被成功解密並注入到服務中，那麼不管第一個線程發生了什麼，第二個有效載荷也將被載入並注入。

3.在第一個注入的線程中，如果找不到來自特定安全產品的必要可執行文件，那麼該線程將被終止，而不會執行其他惡意常式。需要注意的是，只有線程將被終止，而服務仍將運行。

為了隱藏第一階段後門，第一個有效載荷使用了API掛鉤技術來逃避特定安全產品的檢測。具體來說，它掛鉤了兩個不同的API，即「ZwOpenProcess」和「GetExtendedTcpTable」，以隱藏其特定進程。

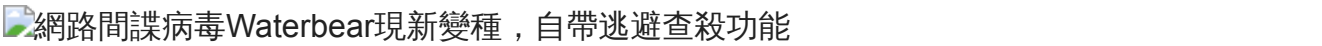


圖4.「ZwOpenProcess」的函數掛鉤，用於檢查和修改函數的輸出

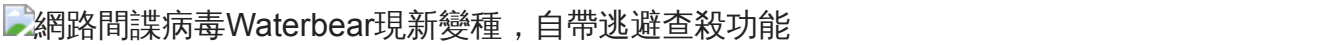


圖5.被修改後的「ZwOpenProcess」

結論

趨勢科技表示，這是他們首次觀察到Waterbear試圖隱藏其後門活動。

根據硬編碼的安全產品名稱，趨勢科技認為攻擊者應該十分了解受害者所使用的安全產品，甚至連這些安全產品是如何在客戶端的端點和網路上收集信息的都十分清楚。因為只有這樣，他們才有可能知道具體要掛鉤哪些API。

此外，由於API掛鉤shellcode採用的是通用方法，因此攻擊者之後還可能會使用類似的代碼段來應對其他安全產品，使得Waterbear活動更加難以檢測。