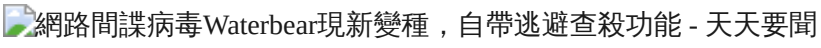
網路間諜病毒Waterbear現新變種，自帶逃避查殺功能 - 天天要聞

By 天天要聞

Published: 2020-01-03 · Archived: 2026-04-05 19:43:55 UTC

2020年01月03日*12:50:08* 科技 1521



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。

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。

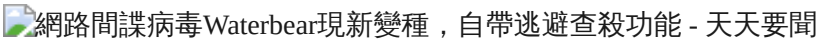


圖1.典型的Waterbear感染鏈

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。

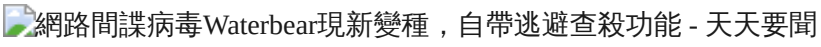


圖2.解密-執行-加密函數

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。

網路間諜病毒Waterbear現新變種，自帶逃避查殺功能 - 天天要聞

圖4.「ZwOpenProcess」的函數掛鉤，用於檢查和修改函數的輸出

網路間諜病毒Waterbear現新變種，自帶逃避查殺功能 - 天天要聞

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。

科技分類資訊推薦

追趕英偉達，必須自研GPU？梁文峰給中國晶元指了另一條路 - 天天要聞 科技

如果讓梁文峰主導GPU晶元開發，要多久追上英偉達？在梁文峰的採訪中，他說英偉達的GPU沒有技術秘密，追趕是時間問題。我理解就是技術和理論上是可行的，就是如何在追趕中組織創新人才研究和創新的問題。那麼，假如：如果讓梁文峰主導，組織團隊，進行G

04月06日 1565

家裡的WiFi路由器，到底是怎麼讓人們連上互聯網的？ - 天天要聞 科技

有人正拿著手機刷視頻，突然畫面卡住不動了，那個小圈圈轉啊轉，急得他直想蹦高。這時候他八成會瞅一眼牆角那個閃著小燈的路由器，這玩意兒是不是又耍脾氣了？咱今天就嘮嘮這個方頭方腦的小盒子到底有啥能耐，咋就能讓你舒舒服服連上互聯網，看劇聊天打遊戲一

04月06日 1228

齊魯師範學院召開「人工智慧+」專題研討會 - 天天要聞 科技

為深入貫徹國家教育數字化戰略行動與教育部「四個未來」政策要求，加快推進人工智慧與教育教學、科學研究、校園治理的深度融合，3月20日，學校在章丘校區第二會議室召開「人工智慧+」專題研討會。

04月06日 1154

比預告更早：曝「超級小愛」PC 客戶端正推送給小米筆記本 Pro 14 - 天天要聞 科技

IT之家 4 月 5 日消息，據博主 @懶醬的日記本 今日分享，小米「超級小愛」PC 客戶端正推送給 Xiaomi Book Pro 14 筆記本（即小米筆記本 Pro 14），比官網底部注釋寫的四月中旬稍微提早。據介紹，小米筆記本 Pro 14 的鍵盤擁有「超級小愛鍵」，按下後就能完整使用筆記本里的 AI 服務，包括 AI 深度搜索、AI 多模態問答、創建

04月06日 3691

剛剛，Claude 4小時血洗全球最安全系統！人類最後防線失守 - 天天要聞 科技

全球最安全的一批系統里，FreeBSD一直算得上那塊最硬的骨頭。現在，這塊骨頭被AI在4小時內啃開了。FreeBSD官方這次公布的，是編號為CVE-2026-4747的內核遠程代碼執行漏洞。

04月06日 1293

有問題也要飛，美國阿爾忒彌斯2號發射成功，為啥感覺差點意思 - 天天要聞 科技

大家都盯著熱搜，美國阿爾忒彌斯2號到底還是上天了。這事實在是大，畢竟自從1972年阿波羅17號帶人離開月球之後，這半個多世紀里，全人類的載人航天基本都在離地幾百公里的近地軌道上打轉。空間站建了一個又一個，但真要往深空走，誰都沒邁出那一步。

04月06日 1540

1-2月轿车前二十销量榜		
排名	车辆名称	1-2月销量（辆）
1、	吉利星愿	56369
2、	朗逸	39592
3、	速腾	39119
4、	帕萨特	34787
5、	轩逸	33207
6、	星瑞	31420
7、	迈腾	30538
8、	凯美瑞	28598
9、	新帝豪	27310
10、	逸动	25013
11、	艾瑞泽8	24608
12、	宝马3系	24085
13、	红旗H5	24046
14、	奥迪A6L	23409
15、	奔驰E级	20702
16、	宝马5系	20223
17、	雅阁	18455
18、	亚洲龙	18312
19、	Model 3	14560
20、	MG4	14093
鬼斗车制表 数据源于乘联会零售销量		

科技

車市逐漸回暖之後，網友們開始打開錢包準備買車。如今，轎車依然是網友們關注的重點，那麼，哪些轎車產品值得網友們重點關注，不妨看看銷量榜單，了解一下實際的銷量情況，然後，再決定該如何選擇。

04月06日 6158

科技

近日，一汽-大眾全新新能源序列ID.AURA的首款車型，其路試諜照正式對外披露。據了解，這款新車精準定位於中型SUV領域，依託全新CEA電子電氣架構精心構建，更配備激光雷達，值得一提的是，它堪稱大眾旗下首款搭載激光雷達的純電SUV。此外，新車計劃於2026年下

04月05日 7904

單日狂賣25萬台，華為這款新機贏麻了 - 天天要聞 科技

華為在春季新品發布會上，帶來了華為全新的暢享90系列。華為暢享90系列包含兩款機型，分別是華為暢享90ProMax、華為暢享90Plus、暢享90三款機型。華為暢享90，起售價格1299元。華為暢享90Plus，起售價格1499元。華為暢享

04月05日 1753

空歡喜？美載人繞月成功，6400億砸下去，卻連登月一半都沒完成 - 天天要聞 科技

北京時間2026年4月2日清晨6時35分，美國佛羅里達州肯尼迪航天中心，一枚98米高的SLS火箭拖著尾焰衝天而起。四名宇航員搭乘獵戶座飛船升空，開啟為期10天的繞月飛行。這是1972年阿波羅17號之後，時隔54年，人類再次飛向月球方向。消息

04月05日 1907
