Daxin(*大新)：專為攻擊安全強化過之頑強網路環境而設計隱秘的後門程式

2022 年 2 月 28 日發布｜威脅情報

威脅獵手團隊
賽門鐵克

該間諜工具是賽門鐵克研究人員從與中國有關聯的行為者身上發現的最先進的惡意軟體。

賽門鐵克【現為網通晶片巨擘博通--Broadcom (美國股市代號：AVGO，全世界網際網路流量有 99.9% 都經過博通的晶片設備) 企業安全部門】威脅獵手團隊的新研究發現，與中國有關聯的威脅行動者正在使用一種高度複雜的惡意軟體，表現出這種行動者以前從未見過的技術複雜性。該惡意軟體似乎被用於針對特定政府和其他關鍵基礎設施目標的長期間諜行動。

有強而有力的證據顯示，惡意軟體 Backdoor.Daxin 允許攻擊者在受感染的電腦上執行各種通信和資料收集作業，最近在 2021 年 11 月被與中國有關的攻擊者使用。大多數目標似乎是對中國具有戰略意義的組織和政府。此外，在部署 Daxin (*大新) 一些相同電腦上還發現與中國間諜行為者有關的其他工具。

毫無疑問，Daxin (*大新) 是賽門鐵克研究人員看過與中國有關聯的行動者所使用最先進惡意軟體。考慮到其能力和所部署的攻擊性質，Daxin 經過最佳化可以對付戒備森嚴、良好防備的目標，它允許攻擊者深入到目標的網路中，在不引起懷疑的情況下竊取資料。

透過賽門鐵克在網路國防聯合協同計畫 (Joint Cyber Defense Collaborative，JCDC) 的成員資格，賽門鐵克研究人員與美國網路安全暨基礎架構管理署 (CISA)合作，與多個被 Daxin (*大新) 後門程式列為目標的外國政府接觸，並協助進行偵測及緩解。

這是一系列部落格中的第一篇。這篇部落格概述 Daxin (*大新) 的能力，隨後將有更多部落格提供進一步的深入分析。

Daxin (* 大新) 技術概述

正如下文更詳細描述，Daxin (*大新) 是以 Windows 核心模式驅動程式的形式出現，這是目前相對罕見的惡意軟體格式。它展現了先進的通信功能，既提供高度的隱蔽性，又允許攻擊者在無法直接連接網際網路的高度安全網路上，與受感染的電腦進行通信。這些功能讓人想起賽門鐵克在 2014 年發現的進階間諜工具：Regin，其他人已將其與西方情報部門聯繫起來。

Daxin (*大新) 的功能顯示，攻擊者投入大量精力來開發通信技術，這些技術可以在目標網路上與正常的網路流量混在一起而不被發現。具體而言，該惡意軟體避免啟動自己的網路服務。相反，它可以濫用已經在受感染電腦上運行的任何合法服務。

Daxin (*大新) 還能夠在受攻擊組織內的受感染電腦網路中轉發其通信。攻擊者可以在受感染的電腦中選擇一個任意的路徑，並發送一條指令，指示這些電腦建立所要求的連線。Daxin (*

大新) 的設計者對這一使用模式進行了優化。

Daxin (*大新) 還具有網路隧道功能，允許攻擊者與受害者網路上的任何受感染的電腦進行合法服務的通信。

Daxin (* 大新) 詳細介紹

Daxin (*大新) 是一個後門，允許攻擊者在受感染的電腦上進行各種行動任務，例如：讀寫任意檔案。攻擊者還可以啟動任意程序並與之互動。據了解 Daxin (*大新) 操作範圍很窄，但它對攻擊者的真正價值在於其隱蔽性和通信能力。

Daxin (*大新) 能夠透過劫持合法 TCP/IP 連線來進行通信。為此，它監控所有內送的 TCP 流量之特定模式。只要檢測到這些模式，Daxin (*大新) 就會切斷合法接收者的連線並接管該連線。然後它與遠端電腦進行點對點 (P2P) 的自訂金鑰交換，雙方遵循相互匹配的步驟。惡意軟體既可以是金鑰交換的發起者，也可以是目標。一個成功的金鑰交換打開一個加密的通信通道，用於接收命令和傳遞回應。Daxin (*大新) 使用劫持 TCP 連線為其通信提供高度的隱蔽性，有助於在具備嚴格防火牆規則的網路上建立連線。它還可降低被安全監控中心 (SOC) 分析師發現的風險。

Daxin (*大新) 的內建功能可以透過在受感染的電腦上部署額外的元件而得到增強。Daxin (*大新) 透過建置一個名為 ".Tcp4 " 的設備，為這些元件提供專屬的通信機制。惡意元件可以打開這個設備來註冊自己的通信。每個元件都可以將一個 32 位元的服務標識與開啟中的 "Tcp4" 設備維持很好的通訊。然後，遠端攻擊者能夠透過在發送某種類型的訊息時指定一個對應的服務標識來與選定的元件進行通信。驅動程式還包括一個機制，可以回傳任何回應。

還有一些原始網路封包被封裝成專用的資料包，透過本地網路介面卡傳輸。然後，Daxin (*大新) 追蹤網路流量，並擷取任何回應的資料包並轉發給遠端攻擊者。這允許攻擊者與目標網路上受感染的機器可建立合法的通信服務，並與被遠端攻擊者鎖定的內部伺服器使用網路通訊隧道 (Tunnels) 互動。

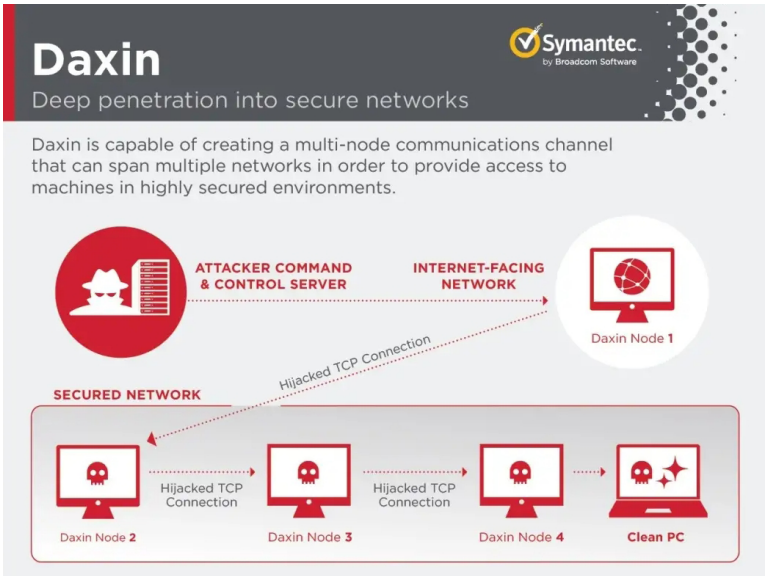


*圖1. Daxin (*大新) 可以建立隱蔽的通信通道，以便與高度安全的網路上的電腦進行互動*

也許最耐人尋味的功能是能夠橫跨多台受感染的電腦，建立全新的通信通道，其中節點的清單是由攻擊者在一個命令中提供。對於每個節點資訊包括建立通信所需的所有細節，特別是節點的 IP 地址、TCP埠號，以及在自訂金鑰交換過程中使用的憑證。當 Daxin (*大新) 收到相關訊息時，它會從清單中挑選下一個節點。然後它使用自己 TCP/IP 協定層連接到清單中的 TCP 伺服器。一旦連接上，Daxin (*大新) 就開始啟動發起方協議。如果遠端點對點通訊 (P2P) 的電腦感染 Daxin (*大新)，這將導致打開一個新的加密通信通道。透過這個新通道發送原始資訊的更新副本，重覆這些動作到下一個節點，直到對列表上的其餘節點重複進行完成為止。

雖然攻擊者的通信在網路中透過多節點來躲過防火牆的作法並不罕見，通常也能避免引起懷疑，但這通常是逐步進行，因此每個節點都需要單獨的行動。然而在 Daxin (*大新) 的案例中，這個過程是一個單一的操作，這表明該惡意軟體是為了攻擊守衛森嚴的網路而設計，攻擊者可能需要定期重新連線到被攻擊的電腦。

時間軸

賽門鐵克威脅獵手團隊已發現政府組織及電信、運輸和製造部門的實體中部署了 Daxin (*大新)。其中幾個受害者是在 PWC (台灣稱：資誠) 威脅情報團隊的協助下發現。

雖然最近一次與 Daxin (*大新) 有關的攻擊發生在 2021 年 11 月，但已知最早的惡意軟體樣本可以追溯到 2013 年，包括從最新的變種中看到所有進階功能，程式庫很大一部分已經被完全開發。這表明，攻擊者在 2013 年已經建立良好的基礎，Daxin (*大新) 的特點反映他們當時就具備的專業技術。

我們相信，在著手開發 Daxin(*大新) 之前，攻擊者已經對建構 Daxin (*大新) 部分技術進行一段時間的實驗。一個較早的惡意軟體--Backdoor.Zala (又名 Exforel) --包含一些共同的特徵，但不具備 Daxin (*大新) 許多進階功能。Daxin (*大新) 似乎建立在 Zala 的網路技術上，重複使用大量獨特的程式碼，甚至共用某些神奇的常數。除此之外，還有某個用於執行掛鉤 (Hooking) 的公共函數庫，在 Daxin (*大新) 和 Zala 的某些變種之間也是常見。廣泛的共用顯示，Daxin (*大新) 的設計者至少有機會接觸到 Zala 的程式庫。我們認為，這兩個惡意軟體家族都是由同一行為人使用，該行為人在 2009 年之前就開始活躍。

與已知間諜參與者的關聯

已知有幾個攻擊的例子，與中國間諜參與者有關的工具被觀察到，同時我們認為是 Daxin(*大新) 的變種。

在 2019 年 11 月對一家資訊技術公司的攻擊中，攻擊者使用單一的 PsExec 會話，首先嘗試部署 Daxin(*大新)，然後再布署 Trojan.Owprox。Owprox 與中國相關的 Slug(又名Owlproxy) 有關。

2020 年 5 月，在屬於另一個組織（一家科技公司）的一台電腦上發生涉及 Backdoor.Daxin (*大新) 和 Trojan.Owprox 的惡意活動。

在 2020 年 7 月對一個軍事目標的攻擊中，攻擊者進行兩次不成功的嘗試，以部署一個可疑的驅動程式。當這些嘗試失敗後，攻擊者轉而使用不同的惡意軟體，即 Trojan.Emulov 的變種。賽門鐵克沒有獲得這次攻擊使用的兩個可疑驅動程式中的任何一個。然而，這次攻擊與早期使用 Daxin(*大新) 活動有很強的相似性，這表明攻擊者極有可能試圖部署 Daxin(*大新)，然後再回到其他惡意軟體上。

發展分析

綜上所述，Daxin (*大新) 包括我們在一個極有可能與中國有關的惡意軟體行動所看到一些最複雜的特徵。我們將在未來幾天發表後續部落格，提供更詳細的技術分析和我們研究和合作的其他見解。

保護／緩解措施

有關最新的防護更新，請訪問賽門鐵克原廠最新的防護公告 (Protection Bulletins)。

入侵／感染指標 (IOC)

與大新活動相關的惡意程式：

81c7bb39100d358f8286da5e9aa838606c98dfcc263e9a82ed91cd438cb130d1 Backdoor.Daxin) (32-bit core)

06a0ec9a316eb89cb041b1907918e3ad3b03842ec65f004f6fa74d57955573a4 Backdoor.Daxin (64-bit core)

0f82947b2429063734c46c34fb03b4fa31050e49c27af15283d335ea22fe0555 Backdoor.Daxin (64-bit core)

3e7724cb963ad5872af9cfb93d01abf7cd9b07f47773360ad0501592848992f4 Backdoor.Daxin (64-bit core)

447c3c5ac9679be0a85b3df46ec5ee924f4fbd8d53093125fd21de0bff1d2aad Backdoor.Daxin (64-bit core)

49c827cf48efb122a9d6fd87b426482b7496ccd4a2dbca31ebbf6b2b80c98530 Backdoor.Daxin (64-bit core)

5bc3994612624da168750455b363f2964e1861dba4f1c305df01b970ac02a7ae Backdoor.Daxin (64-bit core)

5c1585b1a1c956c7755429544f3596515dfdf928373620c51b0606a520c6245a Backdoor.Daxin (64-bit core)

6908ebf52eb19c6719a0b508d1e2128f198d10441551cbfb9f4031d382f5229f Backdoor.Daxin (64-bit core)

7867ba973234b99875a9f5138a074798b8d5c65290e365e09981cceb06385c54 Backdoor.Daxin (64-bit core)

7a08d1417ca056da3a656f0b7c9cf6cd863f9b1005996d083a0fc38d292b52e9 Backdoor.Daxin (64-bit core)

8d9a2363b757d3f127b9c6ed8f7b8b018e652369bc070aa3500b3a978feaa6ce Backdoor.Daxin (64-bit core)

b0eb4d999e4e0e7c2e33ff081e847c87b49940eb24a9e0794c6aa9516832c427 Backdoor.Daxin (64-bit core)

b9dad0131c51e2645e761b74a71ebad2bf175645fa9f42a4ab0e6921b83306e3 Backdoor.Daxin (64-bit core)
cf00e7cc04af3f7c95f2b35a6f3432bef990238e1fa6f312faf64a50d495630a Backdoor.Daxin (64-bit core)
e7af7bcb86bd6bab1835f610671c3921441965a839673ac34444cf0ce7b2164e Backdoor.Daxin (64-bit core)
ea3d773438c04274545d26cc19a33f9f1dbbff2a518e4302addc1279f9950cef Backdoor.Daxin (64-bit core)
08dc602721c17d58a4bc0c74f64a7920086f776965e7866f68d1676eb5e7951f Backdoor.Daxin (dropper)
53d23faf8da5791578c2f5e236e79969289a7bba04eee2db25f9791b33209631 Backdoor.Daxin (dropper)
7a7e8df7173387aec593e4fe2b45520ea3156c5f810d2bb1b2784efd1c922376 Backdoor.Zala (32-bit core)
8dafe5f3d0527b66f6857559e3c81872699003e0f2ffda9202a1b5e29db2002e Backdoor.Zala (32-bit core)
96bf3ee7c6673b69c6aa173bb44e21fa636b1c2c73f4356a7599c121284a51cc Backdoor.Trojan (32-bit core)
9c2f3e9811f7d0c7463eaa1ee6f39c23f902f3797b80891590b43bbe0fdf0e51 Backdoor.Trojan (32-bit core)
c0d88db11d0f529754d290ed5f4c34b4dba8c4f2e5c4148866daabeab0d25f9c Backdoor.Trojan (32-bit core)
e6a7b0bc01a627a7d0ffb07faddb3a4dd96b6f5208ac26107bdaeb3ab1ec8217 Backdoor.Trojan (32-bit core)

與大新惡意活動相關的檔案名稱：

"ipfltdrvs.sys"
"ndislan.sys"
"ndislan_win2008_x64.sys"
"ntbios.sys"
"patrol.sys"
"performanceaudit.sys"
"print64.sys"
"printsrv64.sys"
"prv64.sys"
"sqlwriter.sys"
"srt.sys"
"srt64.sys"
"syswant.sys"
"usbmrti.sys"
"vncwantd.sys"
"wantd.sys"
"win2k8.sys"
"wmipd.sys"
"[CSIDL_SYSTEM]driverspagefile.sys"
"[CSIDL_SYSTEM]spooldriversntds.sys"

在重覆活動期間被觀察到的惡意軟體：

705be833bd1880924c99ec9cf1bd0fcf9714ae0cec7fd184db051d49824cbbf4 suspected Backdoor.Daxin

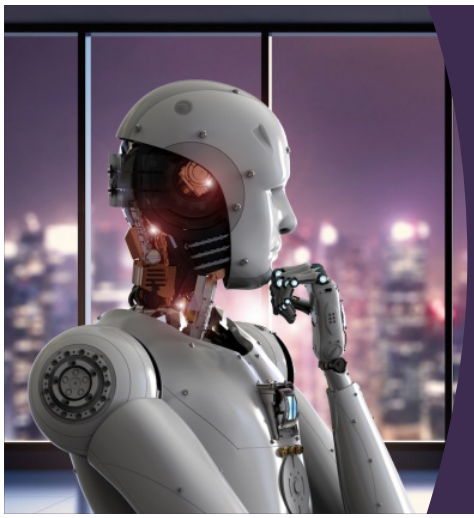
c791c007c8c97196c657ac8ba25651e7be607565ae0946742a533af697a61878 suspected Backdoor.Daxin

514d389ce87481fe1fc6549a090acf0da013b897e282ff2ef26f783bd5355a01 Trojan.Emulov (core)

1a5c23a7736b60c14dc50bf9e802db3fcd5b6c93682bc40141d6794ae96138d3 Trojan.Emulov (dropper)

a0ac5f7d41e9801b531f8ca333c31021c5e064f13699dbd72f3dfd429f19bb26 Trojan.Owprox (core)

aa7047a3017190c66568814eb70483bf74c1163fb4ec1c515c1de29df18e26d7 Trojan.Owprox (dropper)



關於作者

威脅獵手團隊
賽門鐵克

威脅獵手 (Threat Hunter) 團隊是賽門鐵克內部的一群安全專家，其任務是調查有針對性的攻擊，推動賽門鐵克產品的增強保護，並提供分析以幫助客戶應對攻擊。

原廠網址：https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/daxin-backdoor-espionage
本文件由保安資訊有限公司專業細心整理後提供。如有遺誤、更新或異動均以上Symantec原廠公告為準，請知悉。2022/02

更多資訊 請造訪我們的網站 http://www.SaveTime.com.tw
(好記：幫您節省時間.的公司.在台灣)

關於保安資訊：

從協助顧客簡單使用賽門鐵克方案開始，到滿足顧客需求更超越顧客期望的價值。

- 保安資訊被業界公認為最專業的賽門鐵克解決方案的專家。
- 保安資訊的團隊自 1995 年起就專注於賽門鐵克資訊安全解決方案的銷售、規劃與整合、技術支援、教育訓練、顧問服務，特別是提供企業 IT 專業人員的技能傳承(Knowledge Transfer)的效益上，以及比原廠更快速的技術支援回應，深獲許多中大型企業與組織的青睞(特別是有 IT Team 的組織)，長期合作的意願與滿意度極高。
- 與許多系統整合或服務公司不同的是，我們不吝惜分享我們的專業技能與經驗給顧客的 IT Team，經由常態性的教育訓練、精簡的快速手冊、標準 SOP 文件的提供，以及基於比原廠更孰悉顧客的使用環境與現況的快速回應的品質，在業界建立扎實的口碑。
- 保安資訊一直專注於賽門鐵克領先業界的資訊系統基礎架構上的安全性與可用性的解決方案。進而累積了許多與基礎架構整合的成功經驗，讓導入 Symantec 解決方方案的成效非常卓越。我們的顧客都能免除Try & Error 的時間浪費及不確定的投入或自行摸索的運作風險。
- 關於我們：

保安資訊有限公司
http://www.savetime.com.tw
0800-381500、0936-285588