Cicada (* 蟬)：中國進階持續性威脅 (APT) 集團在近期間諜活動中擴大目標

2022 年 4 月 5 日發布 | 威脅情報

威脅獵手團隊
賽門鐵克

政府組織與非政府組織在範圍廣泛和持續的攻擊行動中成為受害者。

一個由中國政府支持的進階持續性威脅 (APT) 組織，正在攻擊全球各地的組織，這可能是一場持續長達數個月的間諜活動。

此次 Cicada (又名 APT10) 攻擊行動的受害者，包括世界多個國家 (蘊含歐洲、亞洲和北美) 的政府、法務、宗教和非政府組織 (NGO)。這次活動的目標部門和地區引人入勝。幾年前，Cicada 最初活動主要集中在與日本有關聯的公司，但在最近幾次活動中，它與對全球範圍更廣的託管服務提供者 (MSP) 之攻擊有關。然而，這場活動似乎確實顯示 Cicada 的目標進一步擴大。

將此活動歸罪於 Cicada 是基於受害者網路上存在自訂的載入器和自訂的惡意軟體，這些惡意軟體被認為僅由該 APT 組織使用。

博通旗下的企業安全部門--賽門鐵克公司的研究人員發現，雖然 Cicada 與 2009 年的間諜活動有關，但此次行動最早發生在 2021 年年中，最近一次發生在 2022 年 2 月，因此這是一場可能仍在進行的長期攻擊行動。

受感染網路上的活動

在幾個案例中，受害者網路上的初始活動是在 Microsoft Exchange 伺服器上看到，這顯示在某些情況下，Microsoft Exchange 中未修補的已知漏洞可能已被用於入侵受害者網路。

一旦攻擊者成功進入受害者電腦，我們觀察到他們部署各種不同的工具，包括自訂的載入器和 Sodamaster 後門。此次活動中部署的載入器也部署在之前的 Cicada 攻擊行動中。

Sodamaster 是一種已知的 Cicada 工具，據了解它僅由該集團所採用。它是一種無檔案式的惡意軟體，具有多種功能，包括透過檢查登錄機碼 (Registry Key) 或延遲執行來逃避沙箱中的檢測；枚舉目標系統的用戶名稱、主機名稱和作業系統；搜索正在執行的程序，下載和執行額外的有效酬載。它還能夠混淆和加密發送回其命令和控制 (C&C) 伺服器的流量。這是 Cicada 至少從 2020 年開始使用的強大後門。

在此行動中，還看到攻擊者轉存憑證，包括使用自訂 Mimikatz 載入器。此版本的 Mimikatz 藉由植入 mimilib.dll 以獲取任何正在入侵的受感染主機用戶的純文字憑證，並在重新啟動後能持續運行。

攻擊者還透過 VLC 導出功能啟動自訂載入器來利用合法的 VLC 媒體播放器，並使用 WinVNC 工具遠端控制受害電腦。

此攻擊行動中使用的其他工具包括：

- RAR 壓縮工具--可用於壓縮、加密或歸檔，還有可用於洩露。
- 系統／網路搜尋--攻擊者確定哪些系統或服務連接到受感染的機器的方法。
- WMIExec--Microsoft 命令列工具，可用於在遠端電腦上執行命令。
- NBTScan--據觀察，該 APT 集團正在使用這種開放原始碼工具，在受害網路內進行內部偵察。

受害者

這起攻擊行動的受害者似乎主要是與政府有關的機構或非政府組織，其中一些非政府組織的受害者屬於教育和宗教領域。在電信、法律界和製藥行業也有受害者。

受害者涵蓋多個地區，包括美國、加拿大、香港、土耳其、以色列、印度、蒙特內哥羅和義大利。日本卻只有一個受害者，這是值得注意的，因為 Cicada 之前全力專注於與日本有關聯的公司。

攻擊者在一些受害者的網路內潛伏長達九個月的時間。

彙整目標受害者、這次行動中所部署的各種工具，以及我們對 Cicada 過去活動的了解都顯示，這次活動最有可能的目的是間諜活動。2018 年，美國政府官員將 Cicada 活動與中國政府聯繫起來。

本次活動彰顯的意義

誠如我們在 2022 年 2 月這次活動中所觀察到最新攻擊行動，這是一場由民族國家所支持的老練、經驗豐富駭客組織所發動的長期活動。同時瞄準不同地區多個大型組織需要大量資源和技術，而這些資源和技能通常只能在民族國家支持的群體中看到，並且顯示 Cicada 應該擁有非常強大的火力，足以發動更嚴峻的網路攻擊。

防護能力

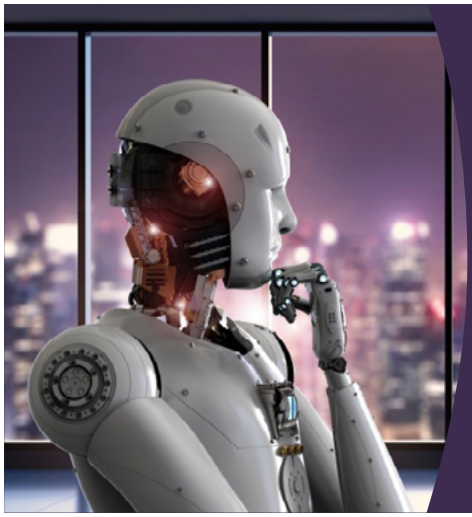
有關最新的防護更新，請訪問賽門鐵克原廠最新的防護公告 (Protection Bulletins)。

入侵指標 (IOCs)

我們的威脅獵手團隊持續偵測與分析相關 IOC，並隨時保持 Symantec Endpoint 產品能偵測到並攔截最新的惡意IOC：

01b610e8ffcb8fd85f2d682b8a364cad2033c8104014df83988bc3ddfac8e6ec
056c0628be2435f2b2031b3287726eac38c94d1e7f7aa986969baa09468043b1
062ce400f522f90909ed5c4783c5e9c60b63c09272e2ddde3d13e748a528fa88

0b452f7051a74a1d4a544c0004b121635c15f80122dc6be54db660ceb2264d6f
0ec48b297dd1b0d6c3ddd15ab63f405191d7a849049feedfa7e44096c6f9d42a
20fc3cf1afcad9e6f19e9abebfc9daf374909801d874c3d276b913f12d6230ec
2317d3e14ab214f06ae38a729524646971e21b398eda15cc9deb8b00b231abc3
2417da3adebd446b9fcb8b896adb14ea495a4d923e3655e5033f78d8e648fcc8
37f56127226ce96af501c8d805e76156ca6b87da1ba1bb5d227100912f6c52d9
3aa54e7d99b69a81c8b25ab57aeb971644ed0a206743c9e51a80ec1852f03663
3ff2d6954a6b62afb7499e1e317af64502570181fd49ac5a74e2f7947e2e89db
4f6a768841595293146ca04f879efa988e4e95ce0f2bc299cb669fea55e78b65
5269db6b19a1d758c75e58ee9bbf2f8fd684cfedbfe712d5b0182d7bbd3a1690
5bc68df582c86c884b563b15057cc223f2e9bc1022ebb297e32a9a7e3036228b
6b4692029f05489ecda10e11cfacfc3b19097856b88647d3695f3bdc7dd83ce9
7b581c0305c78f28bad60028c63e852dc34fc9e28f39e4b0af73d80c1d9680c9
83030f299a776114878bcd2ade585d97836ef4ddb6943cb796be2c88bcb83a83
90a03dabfc4e56a12cc3bac5cbe991db044b900a01ec341803c864506e467ffa
9917a2213f114e87745867e5fea6717efd727d7c08fdc851969224be2f0e019b
9b5f9ff82ed238bcbd83628ed3ec84988dc05f81cec9e45a512fbd2c8ac45c33
adfe177ade7d9bfe4df251a69678102aec1104a4ba9f73032dd90aba76d8bdd9
b76fde584f87c88bdd21fab613335ce7fc05788aa4bb3191d1517ec16ef4d11a
ce45af43dd2af52d6034e981515474147802efdfe036e00078fee29a01694fd6
d461347388ccf0c2008332a1674885a41f70b94b2263bddef44e796d3b1b43b5
df993dca434c3cd2da94b6a90b0ae1650d9c95ea1d5f6a5267aca640d8c6d00e
ee46e714660f7652502d5b3633fae0c08c8018f51cfb56a487afd58d04dd551a
fe33fdd5a63fee62362c9db329dde11080a0152e513ef0e6f680286a6a7b243f
88[.]198.101[.]58
168[.]100.8[.]38



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/cicada-apt10-china-ngo-government-attacks

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