Bumblebee (* 大黃蜂)：新的載入程式迅速成為網路犯罪生態系統中的運作中樞

2022 年 6 月 28 日發布 | 威脅情報

威脅獵手團隊
賽門鐵克

維沙爾・坎布林
首席威脅分析工程師

新的惡意軟體與多個威脅者有關聯，包括幾個備受矚目的勒索軟體營運商。

Bumblebee 是最近開發的惡意軟體載入程式，已迅速成為各種網路犯罪攻擊的關鍵元件，並且似乎已經取代許多較舊的載入程式，顯示它已被既有威脅者所採用，並且是預先有計畫地轉移到 Bumblebee。

透過分析，最近 Bumblebee 有涉入的攻擊行動中所使用的其他三種工具，賽門鐵克的威脅獵手團隊 (博通軟體事業部的企業安全部門) 將該工具與許多勒索軟體營運商關聯起來，包括 Conti、Quantum 和 Mountlocker。這些舊攻擊中使用的攻擊手法、技術與過程 (TTPs) 支援 Bumblebee 可能已被導入作為 Trickbot 和 BazarLoader 替代載入程式的假設，因為最近 Bumblebee 所涉入的活動與這些載入程式的舊攻擊之間有所交集。

Bumblebee (* 大黃蜂) 和 Quantum (* 量子)：大黃蜂在傳遞勒索軟體中舉足輕重的角色

最近一次涉及 Quantum (*量子) 勒索軟體的攻擊行動顯示，Bumblebee (*大黃蜂)現在如何被攻擊者用來傳遞勒索軟體。

初始感染媒介是魚叉式網路釣魚電子郵件，其附件包含 ISO 檔。這個 ISO 檔包含一個 Bumblebee DLL 檔和一個 LNK 檔，它使用 rundll32.exe 載入 Bumblebee DLL 檔。

- rundll32.exe teas.dll,kXlNkCKgFC

Bumblebee 支援多個指令，例如：用於持續性殭屍的“Ins”、用於 DLL 注入的“Dij”和用於下載可執行檔的“Dex”。

使用 Bumblebee“Ins”指令建立一個排程，每 15 分鐘執行一個 VBS 腳本檔。

- wscript.exe CSIDL_COMMON_APPDATAe147c18f9167cd0ff30b25c870238567.vbs
- CSIDL_SYSTEMrundll32.exe" CSIDL_COMMON_APPDATAe147c18f9167cd0ff30b25c870238567.dll

幾個小時後，Bumblebee 使用“Dex”指令在 %APPDATA% 位置注入並執行名為“wab.exe”的 Cobalt Strike 惡意軟體，並執行“systeminfo”指令。

- wmiprvse.exe --> wab.exe
- wmiprvse.exe --> wab.exe --> cmd.exe /C systeminfo

然後 Bumblebee 使用“Dij”指令，將 Metasploit DLL 注入合法程序“ImagingDevices.exe”中，這是一個 Windows Photo Viewer 可執行檔。

此外，Bumblebee 使用“Dij”指令將 Cobalt Strike 惡意程式注入到合法的“wab.exe”中，這是一個 Windows Mail 可執行檔。

然後，Bumblebee 使用“Dij”指令刪除 AdFind 工具，並嘗試列出與網域相關的資訊，例如：信任網域、網域使用者、網域群組和群組權限等。

在這時，Bumblebee 使用“Dij”指令注入 Quantum 勒索軟體。攻擊者使用 DLL 和 EXE 有效籌載來加密檔案。

- rundll32.exe CSIDL_COMMON_APPDATA2429189468.dll,start shareall nolog
- CSIDL_COMMON_APPDATA2431789750.exe /shareall /NOLOG

Quantum 使用 WMI 收集系統資訊和用戶資訊。它還會檢查與 SQL 相關的服務，如果發現這些服務正在執行，則會將其停止。Quantum 還會檢查與惡意軟體分析相關的一些程序，例如：procmon、wireshark、cmd、工作排程器和記事本，如果發現它們正在執行，則會終止它們。

關聯 1： AdFind 連接

最近 Bumblebee 攻擊中使用的工具已經出現在較舊的攻擊裡，早於 Bumblebee 的出現。在 2022 年 5 月中旬開始的一系列涉及 Bumblebee 攻擊中，攻擊者也部署 AdFind (SHA256：b1102ed4bca6dae6f2f498ade2f73f76af527fa803f0e0b46e100d4cf5150682) 的版本。AdFind 是一種用於查詢 Active Directory 的公開工具，近年來已被一系列威脅攻擊者廣泛使用。

與前面提到的範例類似，附加到網路釣魚電子郵件的惡意 ISO 檔是初始的感染媒介，攻擊者部署合法的 ConnectWise 遠端桌面軟體 (以前稱為ScreenConnect)，以及另一個合法的遠端存取工具 Atera 和 Meterpreter，Metasploit 記憶體有效籌載，為攻擊者提供反向殼層。在所有情況下，攻擊從未達到有效酬載階段。但是，其他攻擊中使用的 TTP 相似性顯示勒索軟體是預期的有效酬載。

在最近 Bumblebee 攻擊中使用這個版本的 AdFind 可追溯到 2021 年 6 月的攻擊，當時它與 Cobalt Strike 結合使用以佈署 Avaddon 勒索軟體。

2021 年 8 月，在一次未得逞的勒索軟體攻擊中，它再次出現。當時它與許多其他合法軟體套件包一起使用，包括 AnyDesk--一種公開的遠端桌面工具、Splashtop--另一個遠端桌面工具、7-Zip--公開可用的壓縮／解壓縮檔工具。在部署勒索軟體有效籌載之前，攻擊已停止。

在 2022 年 5 月另一次未得逞的勒索軟體攻擊中，也部署 AdFind 的變種。同樣攻擊者將 Atera、Splashtop 和 AnyDesk 結合使用。一併部署廣泛使用的憑證轉存工具 Mimikatz、LaZagne 和

NetScan 網路掃描工具。攻擊者還利用一個名為 cve-2021-34527.ps1 的 PowerShell 腳本，該腳本之前已與 Conti 洩露的攻擊劇本相關聯。

此版本的 AdFind 還出現在 2022 年 5 月涉及 Quantum 勒索軟體攻擊中。攻擊者也使用 Cobalt Strike、Ligolo--一種公開可用的通道工具 (用於滲透測試目的，但已被許多間諜和勒索軟體攻擊者使用)、用於憑證轉存的 ProcDump、以及Rclone--一種合法的開源工具 (可以合法用於管理雲端中的內容，但勒索軟體攻擊者經常使用它來竊取資料)。

最近，這個相同版本的 AdFind 被用於試圖提供 Diavol 有效籌載的攻擊中。攻擊者使用的初始載入程式並未被發現，但 AdFind 與 Bumblebee 活動的連結顯示它可能已被攻擊者使用。

關聯 2： adf.bat

2022 年 6 月初，在一次受攔截的攻擊中發現 Bumblebee。儘管未部署有效籌載，但所使用的 TTPs 與勒索軟體有關聯。攻擊者使用一個名為 adf.bat (SHA256：1e7737a57552b0b32356f5e5e54dd84a9ae85bb3acff05ef5d52aabaa996282dfb) 的批次處理腳本，以及前面提到 AdFind 版本 (SHA256：b1102ed4bca6dae6f2f498ade2f73f76af527fa803f0e0b46e100d4cf5150682) 和 AdFind 另一個版本 (SHA256：9d0fa4b88e5b36b8801b55508ab7cda9909d639d70436e972cb3761d34eda)。

此 adf.bat 腳本至少自 2021 年以來一直在攻擊中使用。例如：在 2021 年 9 月，該檔出現在一次嘗試勒索軟體攻擊中。它與前面提到 AdFind 版本一起被使用 (SHA256：b1102ed4bca6dae6f2f498ade2f73f76af527fa803f0e0b46e100d4cf5150682)、Cobalt Strike 和 PowerSploit，一個最初為滲透測試開發的開發框架。

該腳本也被用於 2021 年 11 月另一次遭攔截的勒索軟體攻擊中，再次與前面提到 AdFind 版本一起被使用。攻擊者再次使用許多公開可用的工具，包括 Atera agent、Splashtop 和 Cobalt Strike。雖然傳遞機制沒有被發現，但使用一些基本架構已經與以前 BazarLoader 使用的基本架構相關聯，BazarLoader 與 Trickbot (又名 Wizard Spider) 是挖礦網路犯罪組織經常搭配使用的主要惡意軟體之一。兩者皆經常被利用於發動 Ryuk 和 Conti 勒索軟體家族攻擊鏈中的傳遞分工。

關聯 3：find.exe/adfind.exe

AdFind 第三個版本 (SHA256：9d0fa4b88e5b36b8801b55508ab7bc7cda9909d639d70436e972cb3761d34eda) 也被用於最近涉及 Bumblebee 的攻擊。該工具已在勒索軟體攻擊中使用至少一年。

2021 年 5 月，它與 Cobalt Strike 一起被用於針對大型電子組織的勒索軟體攻擊。此攻擊的一個特徵是攻擊者在某些遭入侵的電腦上安裝 VirtualBox VM。雖然未檢索 VM 檔案，但勒索軟體有效籌載似乎位於 VM 上，並在作業系統完全啟動後執行。VM 可能有權限存取主機的檔案和目錄 (透過 runner.exe 設置“SharedFolders”)，進而讓它加密主機上的檔案。雖然惡意軟體沒有被辨識到，但與 Conti 和 Mountlocker 勒索軟體營運商脫不了關係。

在 2021 年 5 月另一次攻擊中，它再次與 Cobalt Strike 結合使用，用於針對美國組織另一次未得逞的勒索軟體攻擊。雖然沒有植入惡意軟體，但相關一些 TTPs 與早期 Conti 攻擊關係密切。

同樣在 2021 年 5 月，這個版本的 AdFind 與 Cobalt Strike 一起被利用，對加拿大的一個組織進行攻擊。在此個案中，使用 Conti 勒索軟體。

合法軟體的使用增加

除了 Bumblebee 與一系列勒索軟體攻擊關係密切，許多經調查的攻擊事件之間的另一個共同點，是在勒索軟體攻擊期間部署的合法軟體工具的數量。除了 Rclone 之外，ConnectWise、Atera、Splashtop 和 AnyDesk 等遠端桌面工具也經常出現在勒索軟體調查中，Rclone 現在被廣泛用於數據洩露目的。

最近，賽門鐵克觀察到攻擊者使用 AvosLocker 勒索軟體在攻擊中利用 PDQ Deploy。PDQ Deploy 是一個合法的軟體套件包，除了部署自定義腳本外，還允許使用者管理多個軟體套件包上的修補。至少有一個分支 AvosLocker 現在正在使用它在受害者網路上的多台電腦上執行惡意 PowerShell 指令，使用 PowerShell Empire 部署 AvosLocker 惡意軟體。

Bumblebee 的威脅

Bumblebee 與許多備受矚目的勒索軟體營運商的關係菲淺，它現在成為網路犯罪生態系統中的運作中樞。任何在其網路上發現 Bumblebee 感染的組織都應該以高優先順序處理此事件，因為它可能是好幾種危險的勒索軟體威脅的途徑。

感染指標／入侵指標 (IOC：Indicators of Compromise)

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。

6804cff68d9824efeb087e1d6ff3f98ed947f002626f04cf8ae7ef26b51e394b-Bumblebee
daf055e5c7f843a3dbe34c3c7b848e5bbe9c53b65df2556b4b450390154af3bb-Bumblebee
7259b7a91df7c9bc78b0830808fe58c6ff66aa79bb856cf1bf50a107875b3651-Bumblebee
ac20f3f9ed0c1e6b2160976a1dc4167e53fbb8c71b4824a640131acf24c71bfd-Bumblebee
71f91acc6a9162b600ff5191cc22f84a2b726050a5f6d9de292a4deeea0d9803-Bumblebee
f06566e1e309123e03a6a65cdfa06ce5a95fdd276fb7fcbcb33f5560c0a3cd8c-Cobalt Strike
2e349b3224cc0d958e6945623098c2d28cc8977e0d45480c0188febbf7b8aa78-Bumblebee
302a25e21eea9ab5bc12d1c5f9e5c119619e617677b307fe0e3044c19581faea-可能是 Bumblebee
65e205b500160cbec44911080621d25f02ad7fcfcf2c3e75ce33f6f821a808b8-與Bumblebee-有關的 DLL
905e87d8433fa58f3006ee685bb347024b46550a3ceda0777016f39e88519142-與Bumblebee-有關的 DLL
6727d493d4ecc8cca83ed8bf7af63941175decff7218e599355065ae6c9563c4-與Bumblebee-有關的 DLL

c8db63bfab805179a1297f8b70a90a043581c9260e8c97725f4920ab93c03344-與Bumblebee-有關的 DLL
261b06e30a4a9960e0b0ae173486a4e456c9bd7d188d0f1c9c109bb9e2281b59- 與Bumblebee-有關的 DLL
24bf01c1a39c6fcab26173e285d226e0c2dcd8ebf86f820f2ba5339ac29086e5-與Bumblebee-有關的 DLL
86d7f7b265aae9eedb36bc6a8a3f0e8ec5fa08071e2e0d21774a9a8e3d4ed9e7-與Bumblebee-有關的 DLL
4c3d85e7c49928af0f43623dcbed474a157ef50af3cba40b7fd7ac3fe3df2f15-尚未經確認，可能是VM檢測工具
b1102ed4bca6dae6f2f498ade2f73f76af527fa803f0e0b46e100d4cf5150682-AdFind
9d0fa4b88e5b36b8801b55508ab7bc7cda9909d639d70436e972cb3761d34eda-AdFind
af.bat 1e7737a57552b0b32356f5e54dd84a9ae85bb3acff05ef5d52aabaa996282dfb-af.bat
adf.bat 5a1b3f9589b468a06e9427eae6b0a855d1df6cb35ab71ddbfa05279579e9cda3-adf.bat
ee5fbc193f875a2b8859229508ca79a2ffe19d8a120ae8c5ca77b1d17233d268-wab.exe
5ad4fa74e71fb4ce0a885b1efb912a00c2ce3c7b4ad251ae67e6c3a8676ede02-wabmig.exe
02ea7b9948dfc54980fd86dc40b38575c1f401a5a466e5f9fbf9ded33eb1f6a7-wabmig.exe
b722655b93bcb804802f6a20d17492f9c0f08b197b09e8cd57cf3b087ca5a347-imagingdevices.exe
a60136d7377bc1ba8c161021459e9fe9f49c692bf7b397fea676211a2da4444d-惡意的 MSI檔案
86c564e9fb7e45a7b0e03dd5a6e1c72b7d7a4eb42ebe6aa2e8f8a7894bed4cb5-VBS 檔案
1825e14e1ea19756b55b5ccec5afbb9c2dba0591403c553a83c842bb0dd14432-ConnectWise
3dea930cfb0ea48c2ce9f7a8bd98ee37e2feca5fb4da8844890fa2d4f62dd105-Atera
52f145a4ccc0f540a130bedbf04370a842daff1ee8d8361c75a8e0d21a88cf5a-Atera
update.exe 3b7512cfa21bd65bd5beecc8cb859ab4f7f5538f3caaf0703a68ec14389b357a-ConnectWise
4c6a865771fdb400456b1e8bc9198134ac9d2f66f1654af42b4b8fc67ae018f2-ConnectWise
fef7d54d6c09a317d95300d10ffcc6c366dbb8f5ebf563dec13b509fff361dc1-ConnectWise
165b491e5b9e273a61c16de0f592e5047740658c7a2e3047f6bf518a17e59eca-ConnectWise
a8faf08997e11a53f9d38797d997c51c1a3fcf89412c3da8dcca6631c6f314a8-ConnectWise
01e22210e07708c0b9a0061d0f912041808e48bb8d59f960b545d0b9e11d42d2-ConnectWise
f5218aaa046776a12b3683c8da4945a0c4c0934e54802640a15152d9dae15d43-ConnectWise
bc41569c4c9b61f526c78f55993203806d09bb8c3b09dbbeaded61cd1dc2fcc2-caexec.exe(可能與PAExec類似)
29767c912919cb38903f12c7f41cdd1c5f39fccb9641302c97b981e4b5e31ee5-vSphere PowerCLI 元件
911c152d4e37f55bd1544794cc324364b6f03aff118cdf328127355ccc25282a-vSphere PowerCLI 元件
f5cd44f1d72ef8fc734c76ca62879e1f1cb4c0603cfdc0b85b5ad6ad8326f503-vSphere PowerCLI 元件
0650722822e984da41d77b90fbd445f28e96a90af87043581896465c06ed1e44-ConnectWise
f01a3f2186e77251acfac9d53122a1579182bde65e694487b292a8e09cf8d465-Cobalt Strike
290b698d41525c4c74836ca934c0169a989a5eafde7208d90300a17a3f5bd408-Ransom.Quantum
3d41a002c09448d74070a7eb7c44d49da68b2790b17337686d6dd018012db89d-Ransom.Quantum
51.68.146.200-AS16276 OVH SAS
154.56.0.221-AS60602 Inovare-Prim SRL
3.85.198.66-AS14618 AMAZON-AES
3.144.143.242-AS16509 AMAZON-02

adaptivenet[.]hostedrmm[.]com
hxxp://127.0.0[.]1:[high-ephemeral-port]/
hxxps://ec2-3-144-143-242.us-east-2.compute.amazonaws[.]com
hxxps://ec2-3-85-198-66[.]compute-1.amazonaws[.]com
adaptivenet[.]hostedrmm[.]com / 52.53.233.237-AS16509 AMAZON-02
hxxp://adaptivenet[.]hostedrmm[.]com/LabTech/Updates/LabtechUpdate_220.124.zip
hxxp://adaptivenet[.]hostedrmm[.]com/LabTech/Updates/LabtechUpdate_220.77.zip
hxxp://adaptivenet[.]hostedrmm[.]com/LabTech/transfer/tools/caexec.exe
hxxp://adaptivenet[.]hostedrmm[.]com/LabTech/Deployment.aspx?Probe=79EA559BB87BF3C8403C40586993D4AC&ID=660
URLs containing URI string "/LabTech/"
45.153.243.93-Bumblebee C&C

防護方案／緩解措施

賽門鐵克端點防護--Symantec Endpoint Protection (SEP) 使用多種靜態和動態技術抵禦勒索軟體攻擊。賽門鐵克已經於第一時間提供多種有效保護。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

檔案型防毒防護：

- Backdoor.Cobalt!gm1
- Backdoor.Cobalt!gm5
- Ransom.Quantum
- Ransom.Quantum!gm1
- Trojan Horse
- Trojan.Bumblebee
- Trojan.Bumblebee!g1
- Trojan.Gen.2
- Trojan.Gen.9
- Trojan.Gen.MBT

基於行為偵測技術(Snoar)的防護：

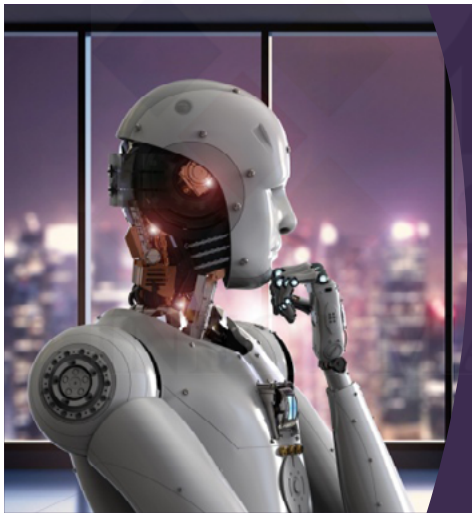
- SONAR.SuspLoad!g12
- SONAR.Module!gen3
- SONAR.WMIC!gen13
- SONAR.WMIC!gen10
- SONAR.RansomGen!gen1
- SONAR.Ransomware!g13
- SONAR.RansomQuantm!g1
- SONAR.Dropper

- SONAR.Ransomware!g1
- SONAR.Ransomware!g3
- SONAR.Ransomware!g7

網路層保護引擎 (IPS)--入侵預防系統防護：

- 28589: Attack: Meterpreter Reverse HTTPS
- System Infected: Trojan.Backdoor Activity 373
- 32721: Audit: ADFind Tool Activity

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)。



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。

關於作者

維沙爾 • 坎布林
首席威脅分析工程師

維沙爾 • 坎布林是賽門鐵克安全技術和回應團隊的成員，他專注於研究未來的網路威脅。

原廠網址：https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/bumblebee-loader-cybercrime
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。2022/06

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