Blackfly 間諜組織瞄準材料科技行業

2023 年 2 月 28 日發布｜威脅情報

威脅獵手團隊
賽門鐵克

目標是亞洲某企業的多家子公司

Blackfly 間諜組織 (又名 APT41、Winnti Group、Bronze Atlas) 持續對亞洲的目標發動攻擊，最近瞄準一家亞洲企業的兩個子公司，這兩家子公司主要業務是有關原物料和複合材料，顯示 Blackfly 可能正試圖竊取智慧財產。

目前 Blackfly 所使用的工具

以下工具曾在 2022 年和2023年的攻擊中被使用：

- **Backdoor.Winnkit**

SHA256: caba1085791d13172b1bb5aca25616010349ecce17564a00cb1d89c7158d6459
SHA256: cf6bcd3a62720f0e26e1880fe7ac9ca6c62f7f05f1f68b8fe59a4eb47377880a
SHA256: e1e0b887b68307ed192d393e886d8b982e4a2fd232ee13c2f20cd05f91358596
SHA256: a3078d0c4c564f5efb1460e7d341981282f637d38048501221125756bc740aac
SHA256: 714cef77c92b1d909972580ec7602b0914f30e32c09a5e8cb9cb4d32aa2a2196
SHA256: 192ef0dee8df73eec9ee617abe4b0104799f9543a22a41e28d4d44c3ad713284
已知與 Blackfly 有關的 rootkit。

- **Credential-dumping tool**

SHA256: 100cad54c1f54126b9d37eb8c9e426cb609fc0eda0e9a241c2c9fd5a3a01ad6c
使用 C:\windows\temp\1.bin\lsass.exe 來竊取憑證。

- **Screenshotting tool**

SHA256: 452d08d420a8d564ff5df6f6a91521887f8b9141d96c77a423ac7fc9c28e07e4
將所有開啟的視窗截圖並存為 .jpg 檔。

- **Process-hollowing tool**

SHA256: 1cc838896fbaf7c1996198309fbf273c058b796cd2ac1ba7a46bee6df606900e
注入一段看起來只有顯示 "Hello World" 的惡意程式到 C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted。

- **SQL tool**

  SHA256: 4ae2cb9454077300151e701e6ac4e4d26dc72227135651e02437902ac05aa80d
  用來查詢 SQL 資料庫的工具。

- **Mimikatz**

  SHA256: b28456a0252f4cd308dfb84eeaa14b713d86ba30c4b9ca8d87ba3e592fd27f1c
  獲取 Windows 明文密碼的開源工具。

- **ForkPlayground**

  SHA256: a3acb9f79647f813671c1a21097a51836b0b95397ebc9cd178bc806e1773c864
  使用 ForkLib 傾印任一處理程的記憶體內容，並建立概念驗證樣本。

- **Proxy configuration tool**

  SHA256: 5e51bdf067e5781d2868d97e7608187d2fec423856dbc883c6f81a9746e99b9f
  SHA256: d4e1f09cb7b9b03b4779c87f2a10d379f1dd010a9686d221c3a9f45bda5655ee
  SHA256: f138d785d494b8ff12d4a57db94958131f61c76d5d2c4d387b343a213b29d18f
  更改 C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted 的內容，設定代理伺服器。

- **Proxy configuration tool**

  SHA256: 88113bebc49d40c0aa1f1f0b10a7e6e71e4ed3ae595362451bd9dcebcf7f8bf4
  SHA256: 498e8d231f97c037909662764397e02f67d0ee16b4f6744cf923f4de3b522bc1
  代理伺服器的設定檔案 c:\users\public\conf.dat。

長期存在的 APT 組織

Blackfly 是中國存在最久的進階持續性滲透攻擊 (APT) 組織之一，早期使用 PlugX／Fast (Backdoor.Korplug)、Winnti／Pasteboy (Backdoor.Winnti)、Shadowpad (Backdoor.Shadowpad)……等惡意軟體攻擊電腦遊戲產業而聞名。隨後更擴展攻擊目標到半導體、電信、材料製造、製藥、媒體和廣告、酒店、自然資源、金融科技和食品行業等行業。

Blackfly 與另一個名為 Grayfly 的中國 APT 組織關係密切，常被視為相同的共犯結構：APT41。在 2020 年的起訴書中揭示這兩個組織曾進行數百次的網路攻擊，而且有部分共同的工作人員。

有恃無恐

儘管 Blackfly 已被美國政府起訴，Blackfly 仍無視警告持續進行網路攻擊。它最初是因為攻擊遊戲產業而聞名，但目前更專注於竊取各個行業的智慧財產。

防護方案／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。

cf6bcd3a62720f0e26e1880fe7ac9ca6c62f7f05f1f68b8fe59a4eb47377880a – Backdoor.Winnkit
e1e0b887b68307ed192d393e886d8b982e4a2fd232ee13c2f20cd05f91358596 – Backdoor.Winnkit
a3078d0c4c564f5efb1460e7d341981282f637d38048501221125756bc740aac – Backdoor.Winnkit
714cef77c92b1d909972580ec7602b0914f30e32c09a5e8cb9cb4d32aa2a2196 – Backdoor.Winnkit
192ef0dee8df73eec9ee617abe4b0104799f9543a22a41e28d4d44c3ad713284 – Backdoor.Winnkit
caba1085791d13172b1bb5aca25616010349ecce17564a00cb1d89c7158d6459 – Backdoor.Winnkit
452d08d420a8d564ff5df6f6a91521887f8b9141d96c77a423ac7fc9c28e07e4 – Screenshotting tool
1cc838896fbaf7c1996198309fbf273c058b796cd2ac1ba7a46bee6df606900e – Process-hollowing tool
4ae2cb9454077300151e701e6ac4e4d26dc72227135651e02437902ac05aa80d – SQL tool
560ea79a96dc4f459e96df379b00b59828639b02bd7a7a9964b06d04cb43a35a – DCSync
b28456a0252f4cd308dfb84eeaa14b713d86ba30c4b9ca8d87ba3e592fd27f1c – Mimikatz
a3acb9f79647f813671c1a21097a51836b0b95397ebc9cd178bc806e1773c864 – ForkPlayground
5e51bdf067e5781d2868d97e7608187d2fec423856dbc883c6f81a9746e99b9f – Proxy configuration tool
d4e1f09cb7b9b03b4779c87f2a10d379f1dd010a9686d221c3a9f45bda5655ee – Proxy configuration tool
f138d785d494b8ff12d4a57db94958131f61c76d5d2c4d387b343a213b29d18f – Proxy configuration tool
88113bebc49d40c0aa1f1f0b10a7e6e71e4ed3ae595362451bd9dcebcf7f8bf4 – Proxy configuration tool
498e8d231f97c037909662764397e02f67d0ee16b4f6744cf923f4de3b522bc1 – Proxy configuration tool
100cad54c1f54126b9d37eb8c9e426cb609fc0eda0e9a241c2c9fd5a3a01ad6c – Credential-dumping tool

原廠網址：https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/blackfly-espionage-materials

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。

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