

# Hydrochasma：一個不為人知的組織 瞄準亞洲的醫療和航運機構

2023 年 2 月 22 日發布 威脅情報



威脅獵手團隊  
賽門鐵克

## 攻擊活動中沒有安裝惡意軟體，完全依賴開源工具軟體。

亞洲的航運公司和醫療實驗室正面臨一個成為情報收集目標的活動，該活動完全仰賴公開可用的現成工具軟體。

Hydrochasma 是該活動的威脅行為者，尚未發現其與任何已知的駭客組織有關連，但似乎對涉及 COVID-19 相關治療或疫苗的行業感興趣。

此活動從 2022 年 10 月以來一直持續在進行。Symantec 沒有在此活動中發現任何數據外洩的事件，但是從 Hydrochasma 針對的目標及使用的工具軟體來看，此次活動最可能的動機是情報收集。

## 網路攻擊鏈

Hydrochasma 一開始使用的攻擊方式最可能是一封釣魚郵件。首先用當地文字的郵件引誘受害者開啟一個名稱類似：

*“[TRANSLATED FROM THE ORIGINAL] Product Specification-Freight-Company Qualification Information wps-pdf Export.pdf.exe”*

另一個釣魚郵件看起來像是在模仿一份履歷：

*“[TRANSLATED FROM THE ORIGINAL] [REDACTED] University-Development Engineer.exe”*

在取得入侵初期權限 (initial access) 之後，攻擊者開始投放一個 Fast Reverse Proxy (FRP) 的工具軟體，這是一個可以將位於 NAT 或防火牆後面的伺服器暴露在網際網路上的工具。然後，攻擊者會投放另一個看起來像是一個合法的 Microsoft Edge 瀏覽器更新檔案：

*%TEMP%\MicrosoftEdgeUpdate.exe*

以及另一個檔案：*%TEMP%\msedgeupdate.dll*。但是，這些檔案實際上是 Meterpreter，這是 Metasploit（用於滲透測試）架構的一個模組，可用於遠端存取。

隨後在這個受害者的網絡上看到的其他工具包括：

- **Gogo scanning tool**：一個自動掃描引擎，最初是為紅隊模擬入侵攻擊設計。
- **Process Dumper (lsass.exe)**：一個允許攻擊者傾印網域密碼的工具。

- **Cobalt Strike Beacon**：一個現成的工具，可用於執行命令、注入其他程序、提升當前程序權限或模擬其他處理程序以及上傳和下載檔案。它原先的用途是作為合法的滲透測試工具，但總是被利用來做惡意行為。
- **AlliN scanning tool**：一個滲透測試掃描工具，可用於內網的橫向滲透。
- **Fscan**：一個公開可用的漏洞掃描工具，可以做端口掃描等。
- **Dogz proxy tool**：一個免費的 VPN 代理工具。

此外，一個代碼載入 (shellcode loader) 和一個損壞的可攜式執行檔案 (corrupted portable executable) 也被部署在這個受害者的網路上。

其他在此次攻擊活動中使用的戰術、技巧和程序 (TTPs) 包括：

- **SoftEtherVPN**：這個工具的存在是 Symantec 研究人員最初開始調查這個活動的原因。它是一款免費、開源、跨平台的 VPN 軟體。
- **Procdump**：這是微軟 Sysinternals 的工具，用於監視 CPU 尖峰的應用程式以及產生損毀傾印，但也可以用作一般的處理程序的傾印。
- **BrowserGhost**：一個可以從瀏覽器中獲取密碼的工具。
- **Gost proxy**：一個通道工具。
- **Ntlmrelay**：NTLM 中繼攻擊允許攻擊者攔截經過驗證的身份驗證請求，以便存取網路服務。
- **Task Scheduler**：允許在電腦上自動執行任務。
- **Go-strip**：縮小 Go 二進位檔的工具。
- **HackBrowserData**：一個可以解密瀏覽器數據的開源工具。

Hydrochasma 所部署的工具表明他們希望實現對受害者機器的持續和隱蔽的存取，並努力在受害者網路中擴散。

雖然 Symantec 研究人員沒有觀察到從受害者機器中數據洩漏，但 Hydrochasma 部署的某些工具可以實現遠端存取，潛在地可以用於外洩數據。被針對的行業也表明這次攻擊的動機是情報收集。

值得注意的是，在此次攻擊中未使用任何自定義的惡意軟體。僅依賴於現有的和公開可用的工具可以使攻擊更加隱蔽，同時使追查原因更加困難。Symantec 沒有看到證據將此活動與已知的惡意行為聯繫起來，因此我們建立 Hydrochasma 的新的辨識指標，以標識此行為。

## 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。

### 檔案指標

#### SHA256

409f89f4a00e649ccd8ce1a4a08afe03cb5d1c623ab54a80874aebf09a9840e5 - Fast Reverse Proxy  
47d328c308c710a7e84bbfb71aa09593e7a82b707fde0fb9356fb7124118dc88 - GoGo Scanning Tool  
6698a81e993363fab0550855c339d9a20a25d159aaa9c4b91f60bb4a68627132 - Dropper  
7229bd06cb2a4bbe157d72a3734ba25bc7c08d6644c3747cdc4bcc5776f4b5b9 - Process Dumper (lsass.exe)  
72885373e3e8404f1889e479b3d46dd8111280379c4065bfc1e62df093e42aba - Fast Reverse Proxy  
72bc8b30df3cdde6c58ef1e8a3eae9e7882d1abe0b7d4810270b5a0cc077bb1a - Cobalt Strike Beacon  
7b410fa2a93ed04a4155df30ffde7d43131c724cdf60815ee354988b31e826f8 - Fast Reverse Proxy  
7f0807d40e9417141bf274ef8467a240e20109a489524e62b090bccdb4998bc6 - Process Dumper (lsass.exe)  
8c0f0d1acb04693a6bdd456afcd37243e502b21d17c8d9256940fc7943b1e9a - Cobalt Strike Beacon  
8e32ea45e1139b459742e676b7b2499810c3716216ba2ec55b77c79495901043 - Fast Reverse Proxy  
981e5f7219a2f92a908459529c42747ac5f5a820995f66234716c538b19993eb - GoGo Scanning Tool  
9ebd789e8ca8b96ed55fc8e95c98a45a61baea3805fd440f50f2bde5ffd7a372 - Fast Reverse Proxy  
9f5f7ba7d276f162cc32791bfbaa0199013290a8ac250eb95fd90bc004c3fd36 - Cobalt Strike Beacon  
a0f5966fcc64ce2d10f24e02ae96cdc91590452b9a96b3b1d4a2f66c722ecc34 - AllIn Scanning Tool  
cb03b5d517090b20749905a330c55df9eb4d1c6b37b1b31fae1982e32fd10009 - Fscan  
d1c4968e7690fd40809491acc8787389de0b7cbbc672c235639ae7b4d07d04dd4 - Shellcode Loader  
de01492b44372f2e4e38354845e7f86e0be5fb8f5051baafd004ec5c1567039f - Cobalt Strike Beacon  
e378d8b5a35d4ec75cae7524e64c1d605f1511f9630c671321ee46aa7c4d378b - PE File  
eba22f50eedfec960fac408d9e6add4b0bd91dd5294bee8cff730db53b822841 - Dropper  
fc4b5f2ee9da1fe105bb1b7768754d48f798bf181cbc53583387578a5ebc7b56 - Dogz Proxy Tool  
02fe00ffd1b076983f3866c04ca95c56cef88c2564fab586e11e54986e87ba7  
084d1fc4236011d442801e423485c8e58f68dc14ec0a8b716fa0fd210de43dda  
1744fac628262aa0cf3810bd5168375959be41764c8ca2fa41950a7b1f8f2fad  
1d087f6a17227769bcebc799a2cdf1bb2a8fdf6ba560d21a88bb71f1c213a42c  
327fc116f8f48f97292184bb50cb3db418f368b3e2a0fb41267ba40254a35a89  
3516f94b0fb57e93c6659d813cbf5fb3617dea7a667c78cb70a1914306327906  
41b6d26926706bb68530dfff234f69757e3bbef91c47eb0255313ed86cb3f806  
44223e5abd106c077908f03c93b8c8baee7d630f1718f9750f16b786cf88fd06  
553e0763cf3a938b5754c9d89939a118abe0b235e4be6920c34f562bd758e586  
5a62abc0a2208679e414cc71d1f36ffa14b48df2b73ac520e45d557ad77dd004  
6770f815480d7cfa0a6fc8599c08ca6013f608d257a2121233e77374e21c53f8  
6cb815863088a0ad367b2a525a572323600596f6875a79536aee57202ef24fd5  
6f017ad84d0d06f50b6213a0742838b5ec510f3d06f96e0300048f2da6a35c41  
7394ab0ed6d1f62e83fc5f8f1eb720ddd07cbd2bcd6a00b9b63ef6018fa5f90  
7800a4fb0cbdf29815c521ea8b00a23e28d7eb365653f2afcfb5572622727218  
7f6a1d6950a9464f27d8651a267563d4630d223bf7ac66851917a57f8fac6550  
84502fbe3e5172c39e9a97734e6caac79255abffcb55c22752620d908ff33940

916b63b88de2549c4a5c8e13d51df4cf6996067ae30f24c8bb35c66db7c061df  
968b28f7d6abb845f2cc7efa93cdcf7660585e22d589267695726de13afea260  
9e8b5a84ad108a761619ca040788dcbf07996a9101cecc5c30ba61f9a06945c1  
b53d0a43ea91b3c80bc6c87c0c6946816c38876b2cb2f6f772afe94c54d3ad30  
b5c4f420067499522b748a34161ad6e140a7f30ab0b8fa63feef760c5e631679  
d0ae66022929c17f31ddf98d88817f0aa70a56ce2ff2df9595b8889c2d3d7e31  
d92c50a91bd5b2f06f41a9a5f9937e50b78658d46e3cd04bc3a85f270ce288c2  
dc3b714fd6f93c0c0cd2685b6b8cd551896855474bdd09593b8c6b4b7ab6bac2  
e7684a4984d9d82115c5cc1b43b9f63a11e7ed333a4e2d92dc15b6e931634bf4  
ebc3dabf0a2dafb0790be6dbb4d3509b5ce1259b955172910618a32627b3b668  
ee9aefde33ed48d16ecb1c41256fc7d93ddfa8bedfa59b95e8810282ac164d0d  
f35b206fe10ad3f57d9c4ecf71a2d2cc06d7c7fe905e567b989f72f147da99dc  
f73738e6e33286657cda81f618a74b74745590915a8f4451e7c00473cbe89e1d  
fc8a67b80b0b0ecd10dfd90820ffc64923b94c32b04dbb6929a79b9ce027563c  
ffdcf74968805e9cc897ca932e4da0f22ea7b3e9b96fcc9082c0c5300ae4cb0d

## 網路指標

### IPs

39.101.194[.]61 - Cobalt Strike Beacon C&C  
47.92.138[.]241 - Cobalt Strike Beacon C&C  
106.14.184[.]148  
180.119.234[.]147

### Domains

alidocs.dingtalk[.]com.wswebpic[.]com - Cobalt Strike Beacon C&C  
csc.zte[.]com.cn.wswebpic[.]com - Cobalt Strike Beacon C&C  
taoche[.]cn.wswebpic[.]com - Cobalt Strike Beacon C&C

### URLs

hxxp://47.92.138[.]241:8090/update.exe  
hxxp://47.92.138[.]241:8000/agent.exe  
hxxp://47.92.138[.]241:8000/update.exe  
hxxp://47.92.138[.]241:8000/ff.exe  
hxxp://47.92.138[.]241:8000/aa.exe  
hxxp://47.92.138[.]241:8000/runas.exe  
hxxp://47.92.138[.]241:8090/a.exe  
hxxp://47.92.138[.]241:8000/t.exe  
hxxp://47.92.138[.]241:8000/po.exe  
hxxp://47.92.138[.]241:8080/t.exe  
hxxp://47.92.138[.]241:8899/t.exe  
hxxp://47.92.138[.]241:8000/logo.png  
hxxp://47.92.138[.]241:8080/t.png  
hxxp://47.92.138[.]241:8000/frp.exe

原廠網址 : <https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/hydrochasma-asia-medical-shipping-intelligence-gathering>  
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。2023/2



## 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，以及基於比原廠更熟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**