Harvester(* 收割者）：民族國家支持的團體使用新的工具集來瞄準南亞的受害者

2021 年 10 月 18 日發布｜威脅情報

威脅獵手團隊
賽門鐵克

前所未見的攻擊組織針對 IT，電信和政府部門的受害者發動間諜行動。

一個前所未見的行動者，可能是民族國家支援的，正在瞄準南亞的組織，特別是阿富汗，這似乎是一場使用全新工具組的資訊竊取行動。

Harvester (*收割者) 組織在其攻擊中使用了自定義惡意軟體和公開可用的工具，該攻擊始於 2021 年 6 月，近期活動發生在 2021 年 10 月。鎖定行業包括電信、政府和資訊技術 (IT)。這些工具功能、它們客製化開發及針對的受害者，都表明 Harvester 是一個由民族國家支持的參與者。

部署了新工具組

關於此行動最值得注意的事情是攻擊者部署的前從未見的工具組。

攻擊者在受害者電腦上部署了一個名為 Backdoor.Graphon 的自定義後門，以及其他下載器和螢幕截圖工具，為攻擊者提供遠端存取，並允許他們監視用戶活動並洩露資訊。

我們不知道 Harvester (*收割者) 用來破壞受害者網路的初始感染媒介，但發現 Harvester (*收割者) 在受害者電腦上活動第一個證據是惡意的網址。然後，該集團開始部署各種工具，包括其自定義的 Graphon 後門，以獲得對網路的遠端存取。該組織還試圖藉由利用合法的 CloudFront 和 Microsoft 等基礎設施進行命令和控制 (C&C) 活動，將其活動與合法網路流量混合在一起。

使用的工具：

- Backdoor.Graphon -- 是一個使用 Microsoft 基礎設施進行 C&C 活動的自定義後門。
- 自訂下載程式 -- 使用 Microsoft 基礎架構進行 C&C 活動。
- 自訂螢幕截圖器 -- 定期將螢幕截圖記錄到檔案中。
- Cobalt Strike Beacon -- 使用 CloudFront 基礎設施進行 C&C 活動 (Cobalt Strike 是一種現成工具，可用於執行命令、注入其他程序、提權當前程序或冒充其他程序及上傳和下載檔案)。
- Metasploit -- 一個現貨模組化框架，可用於受害者電腦上的各種惡意目的，包括權限提升、螢幕擷取、設置持久後門等。

攻擊者使用的自定義下載程式利用了 Costura 程式集載入程式。進入受害電腦後，它會檢查是否存在以下檔案：

- [ARTEFACTS_FOLDER]winser.dll

如果該檔案不存在，它將從以下網址下載：

- hxxps://outportal[.]azurewebsites.net/api/Values_V2/Getting3210

接下來，如果以下檔案不存在，則將採用以下步驟產生：

- "[ARTEFACTS_FOLDER]Microsoft Services[.]vbs"

然後，它修改以下登錄表的機碼來建立載入點：

- HKEY_CURRENT_USERSOFTWAREMicrosoftWindowsCurrentVersionRun"MicrosoftSystemServices" = "[ARTEFACTS_FOLDER]Microsoft Services[.]vbs"

最後，它使用以下網址在自己的 使用者介面 (UI) 中打開嵌入式 Web 瀏覽器：

- hxxps://usedust[.]com

雖然最初看起來這個網址可能是 Backdoor.Graphon 的載入點，但經過進一步調查，它似乎是一個誘餌，可以迷惑任何受影響的使用者。

Backdoor.Graphon 被編譯為 .NET 的 PE DLL 檔案，導出「Main」和以下 .PDB 附檔名的檔案：

- D:OfficeProjectsUpdated Working Due to Submission4.5Outlook_4.5Outlook 4.5.2 32 bit New without presistancyNPServicesbinx86DebugNPServices[.]pdb

當執行此操作時，它會嘗試與攻擊者的 C&C 伺服器進行通信，這些伺服器託管在 Microsoft 基礎架構上。

- hxxps://microsoftmsdn[.]azurewebsites.net/api/Values_V1/AuthAsyncComplete_V1?Identity=[INFECTION_ID]
- hxxps://microsoftsgraphapi[.]azurewebsites.net/api/Values_V1/AuthAsyncComplete_V1?Identity=[INFECTION_ID]
- hxxps://msdnmicrosoft.azurewebsites[.]net/api/Values_V1/AuthAsyncComplete_V1?Identity=[INFECTION_ID]

然後，攻擊者執行命令來控制其輸入流並擷取輸出和錯誤流。他們還定期向 C&C 伺服器發送 GET 請求，提取任何返回的訊息的內容，然後將其刪除。

從 cmd.exe 輸出和錯誤流中提取的數據將被加密併發送回攻擊者的伺服器。

自定義螢幕截圖工具還包含 Costura Assembly Loader。螢幕截圖工具會將照片保存到受密碼保護的 ZIP 壓縮檔進行洩漏，並刪除所有超過一周的存檔。

正在進行的活動

雖然我們還沒有足夠的證據將 Harvester (*收割者) 的活動歸因於特定的民族國家，但該組織使用自定義後門，為隱藏其惡意活動而採取的廣泛措施以及其目標都表明它是國家贊助的行動

者。Harvester 使用合法的基礎設施來託管其 C&C 伺服器，以便與正常的網路流量混合，這是該參與者採取的隱蔽步驟的一個例子。

鑒於阿富汗最近發生的巨大動蕩，在這場行動中以阿富汗各組織為目標也令人感興趣。Harvester 進行的活動清楚地表明，該行動的目的是間諜活動，這是民族國家支持的活動背後的典型動機。

Harvester 最近的活動是在本月早些時候看到的，這意味著所提到的行業和地區的組織應該對本部落格中概述的惡意活動保持警惕。

保護

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：

基於行為偵測技術(Snoar)的防護：

- Backdoor.Graphon

點擊此處獲取有關賽門鐵克的最新防護公報，或與保安資訊聯繫可獲得最快最有效的協助。

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

0740cc87a7d028ad45a3d54540b91c4d90b6fc54d83bb01842cf23348b25bc42
303f93cc47c58e64665f9e447ac11efe5b83f0cfe4253f3ff62dd7504ee935e0
3c34c23aef8934651937c31be7420d2fc8a22ca260f5afdda0f08f4d3730ae59
3c8fa5cc50eb678d9353c9f94430eeaa74b36270c13ba094dc5c124259f0dc31
470cd1645d1da5566eef36c6e0b2a8ed510383657c4030180eb0083358813cd3
691e170c5e42dd7d488b9d47396b633a981640f8ab890032246bf37704d4d865
a4935e31150a9d6cd00c5a69b40496fea0e6b49bf76f123ea34c3b7ea6f86ce6
c4b6d7e88a63945f3e0768657e299d2d3a4087266b4fc6b1498e2435e311f5d1
cb5e40c6702e8fe9aa64405afe462b76e6fe9479196bb58118ee42aba0641c04
d84a9f7b1d70d83bd3519c4f2c108af93b307e8f7457e72e61f3fa7eb03a5f0d
f4a77e9970d53fe7467bdd963e8d1ce44a2d74e3e4262cd55bb67e7b3001c989

網址

hxxps://perfect-couple.com/perfectcouple[.]exe --樣本是由此網址下載的

原廠網址：https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/harvester-new-apt-attacks-asia
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。2021/10

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