北韓駭客組織 Lazarus 針對化工行業進行間諜活動

2022 年 4 月 14 日發布 | 威脅情報

威脅獵手團隊
賽門鐵克

持續行動的 Dream Job 將北韓與間諜活動中 APT 目標組織關聯起來。

Broadcom 軟體公司旗下的賽門鐵克觀察到，與北韓有關的進階持續威脅（APT）組織 Lazarus 正在針對化工行業內的組織開展間諜活動。這場活動似乎是被稱為“Dream Job行動”的 Lazarus 活動之延續，該行動於 2020 年 8 月首次被觀察到。賽門鐵克以 Pompilus 的名稱追跡 Lazarus 這一子系列活動。

Dream Job 行動

Dream Job 行動涉及 Lazarus 利用假的工作機會引誘受害者點擊惡意連結或打開惡意附件，最終導致安裝用於間諜活動的惡意軟體。

在 2020 年 8 月和 2021 年 7 月觀察到的活動中，過去 Dream Job 活動針對國防、政府和工程部門的個人。

最近的針對行業

2022 年 1 月，賽門鐵克在韓國多家組織的網路上檢測到攻擊活動。這些組織主要在化學部門，有些在資訊技術（IT）部門。然而，IT 目標很可能被用作進入企業組織化學部門的一種手段。

有足够證據顯示，最近這項活動是“Dream Job”行動的延續。這些證據包括檔案雜湊、檔名以及在之前 Dream Job 活動中觀察到的工具。

典型的攻擊始於收到惡意 HTM 檔案時，可能是電子郵件中的惡意連結或從 web 下載的惡意連結。HTM 檔案被複製到名為 scskapplink.dll 的 DLL 檔案中，並注入合法的系統管理軟體 INISAFE Web EX 用戶端。

scskapplink.dll 檔通常是一個經過簽名並添加惡意匯出的特洛伊木馬工具。攻擊者被觀察到使用以下簽名：DOCTER USA, INC和“A” MEDICAL OFFICE, PLLC。再者，scskapplink.dll 從命令和控制（C&C）伺服器下載，並執行具有 URL 參數鍵／值“prd_fld=racket”的額外有效載荷。

此步驟啟動一系列 shellcode 載入程式，這些載入程式從攻擊者那裡下載並執行任意命令，以及其他惡意軟體，這些惡意軟體通常是從添加到特洛伊木馬工具，如：Tukaani 專案 LZMA

Utils 程式庫（XZ Utils）的惡意匯出中執行。

攻擊者使用 Windows Management Instrumentation（WMI）在網路上橫向移動，並透過其他機器上的 DreamSecurity 注入 MagicLine。

在某些情況下，攻擊者被發現從註冊表轉存憑證，安裝 BAT 檔以獲得持續性，並設定以特定使用者身份執行的排程工作。

攻擊者還被觀察到部署入侵後的工具，包括一個用於以設定的時間間隔拍攝在受感染機器上查看的網頁螢幕截圖工具（SiteShoter）。他們還使用 IP 日誌記錄工具（IP Logger）、遠端啟動電腦的協定（WakeOnLAN）、檔案和目錄複制程式（FastCopy）以及在 MagicLine 程序下執行的檔案傳輸協定（FTP）。

個案研究

以下是一個案例研究，詳細介紹化學部門組織中的逐步攻擊者活動。

2022年1月 17日

00:51--收到惡意 HTM 檔：

- e31af5131a095fbc884c56068e19b0c98636d95f93c257a0c829ec3f3cc8e4ba - csidl_profile\appdata\local\microsoft\windows\inetcache\ie\3tygrjkm\join_06[1].htm

HTM 檔案複製了 DLL 檔案：

- rundll32.exe CSIDL_PROFILE\public\scskapplink.dll,netsetcookie Cnusrmgr

此 DLL 檔被注入到合法的系統管理軟體 INISAFE Web EX 用戶端。該檔是用於 Notepad++ 的 ComparePlus 外掛程式的已簽名特洛伊木馬版本，並添加了惡意匯出。

01:02--該檔被執行並從命令和控制（C&C）伺服器，URL參數鍵／值“prd_fld=racket”下載並執行有效後門負載 (final.cpl - 5f20cc6a6a82b940670a0f89eda5d68f091073091394c362bfcaf52145b058db)。

檔案 final.cpl 是添加惡意匯出 (AppMgmt) 的 Tukaani 項目 LZMA Utils 程式庫 (XZ Utils) 的特洛伊版本。

惡意軟體連接到以下遠端位置，下載、解碼和執行殼層代碼：

- hxxp[:]//happy[.]nanoace.co.kr/Content/rating/themes/krajee-fas/FrmAMEISMngWeb.asp

01:04--執行另一個 CPL 檔 （61e305d6325b1ffb6de329f1eb5b3a6bcafa26c856861a8200d717df0dec48c4）。同樣，此檔是帶有惡意匯出 LZMA Utils 的特洛伊木馬版本。

01:13--shellcode 載入器（final.cpl）會再次執行幾次。

01:38--執行從 SAM 和系統機碼 hive 轉存憑證指令。

在接下來的幾個小時裡，攻擊者透過 final.cpl 以不同的間隔執行未知的 shellcode，可能會收集轉存的系統機碼 hive 等。

06:41--攻擊者建立一個排程工作，以確保系統重新啟動時的持續性：

- schtasks /create /RU Skynet.help\175287 /ST 15:42 /TR "cmd.exe /c C:\ProgramData\Intel\Intel.bat" /tn arm /sc MINUTE

排程工作設定系統在每天 15：42 以使用者“Skynet.help”的身份執行“Intel.bat”，服務名稱為“arm”。目前尚不清楚這是透過轉存的註冊表配置單元破解的帳戶，還是攻擊者能夠使用管理員權限建立的帳戶。

攻擊者還被觀察到透過 CPL 檔案安裝 Cryptodome（PyCrypto fork）Python 加密模組。

攻擊者還全新安裝了 BitDefender。雖然未經證實，但威脅參與者可能已經安裝該軟體的舊版本（從2020年開始），該漏洞允許攻擊者遠端執行任意指令。

1月 18日

00:21--再次執行 final.cpl 檔案。

00:49--執行名為 wpm.cpl (942489ce7dce87f7888322a0e56b5e3c3b0130e11f57b3879fbefc48351a78f6) 的新 CPL 檔案。

- CSIDL_COMMON_APPDATA\finaldata\wpm.cpl Thumbs.ini 4 30

此檔案包含並連接到一個 IP 位址清單，並記錄連接是否成功。

01:11--同樣的，final.cpl shellcode 載入器被多次執行，執行一些未知的 shellcode。該活動間歇性地持續到 23:49。

23:49--CPL 檔案的檔名變更為“ntuser.dat”。檔案位置和命令列參數則維持不變。

1月 19日

00:24--CPL shellcode 載入程序檔案（final.cpl 和 ntuser.dat）被執行多次。

00:28--攻擊者在另一台機器上建立排程工作，可能是確保持續性：

- schtasks /create /RU SKYNET\i21076 /ST 09:28 /TR "cmd.exe /c C:\ProgramData\Adobe\arm.bat" /tn arm /sc MINUTE

該命令於每天 09：28 以“SKYNET”帳戶和“arm”服務名稱執行“arm.bat”檔。

00:29--使用以下命令列參數執行 arm.dat 檔（48f3ead8477f3ef16da6b74dadc89661a231c82b96f3574c6b7ceb9c03468291）：

- CSIDL_SYSTEM\rundll32.exe CSIDL_COMMON_APPDATA\adobe\arm.dat,packageautoupdater LimitedSpatialExtent_U_f48182 -d 1440 -i 10 -q 8 -s 5

arm.dat檔是用於每 10 秒在受損的電腦上顯示的網頁截圖 (SiteShoter) 的工具，根據命令列參數決定。截圖將被儲存在 Appdata\local 按日期順序的最上層。

06:50--shell code loader（final.cpl）被多次執行。

07:34--新的addins.cpl（5f20cc6a6a82b940670a0f89eda5d68f091073091394c362bfcaf52145b058db）檔被多次執行，這又是另一個shellcode載入程式，並且具有相同的命令列參數，如final.cpl所示：

- CSIDL_SYSTEM\rundll32.exe CSIDL_COMMON_APPDATA\addins.cpl, AppMgmt EO6-CRY-LS2-TRK3

07:39--建立工作排程：

- sc create uso start= auto binPath= “cmd.exe /c start /b C:\Programdata\addins.bat” DisplayName= uso

該排程於每次系統啟動時自動啟動並執行addins.bat。該排程使用“uso”服務名稱（以前在針對安全研究人員的Dream Job活動中使用的檔名）。

攻擊者再次執行addins.cpl以指令啟動服務，然後直接刪除服務：

- CSIDL_SYSTEM\rundll32.exe CSIDL_COMMON_APPDATA\addins.cpl, AppMgmt EO6-CRY-LS2-TRK3
- sc start uso (via cmd.exe)
- sc delete uso

然後執行以下指令以收集網路配置、攻擊者登錄的當前用戶、電腦上的活動使用者、可用的共享磁碟以及“addins”目錄內的相關的資訊。

- ipconfig /all
- whoami
- query user
- net use
- dir CSIDL_WINDOWS\addins

07:41--adince.cpl 檔案在建立預定的排程執行 addins.bat 啓動服務，並立即刪除服務前被多次執行。

- sc create uso start= auto binPath= "cmd.exe /c start /b C:\Windows\addins\addins.bat" DisplayName= uso
- sc start uso
- sc delete uso

1月20日

攻擊者將重新執行adince.cpl， 指令與先前相同。

沒有觀測到進一步的活動。

Lazarus 集團可能會將目標對準化學行業的組織，以獲取知識產權，推動北韓在這一領域的發展。在賽門鐵克和其他公司的見證下，該集團繼續開展“Dream Job”行動，這顯示該行動已相當成功。因此，各組織應確保有足够的安全措施，並對此類攻擊保持警惕。

與往常一樣，用戶應該警惕點擊鏈接或檔案下載，即使它們來自看似可靠的來源。

防護／緩解

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)

SHA-256

164f6a8f7d2035ea47514ea84294348e32c90d817724b80ad9cd3af6f93d83f8
18686d04f22d3b593dd78078c9db0ac70f66c7138789ad38469ec13162b14cef
1cb8ea3e959dee988272904dbb134dad93539f2c07f08e1d6e10e75a019b9976
2dd29b36664b28803819054a59934f7a358a762068b18c744281e1589af00f1f
32bfdf1744077c9365a811d66a6ea152831a60a4f94e671a83228016fc87615f
35de8163c433e8d9bf6a0097a506e3abbb8308330d3c5d1dea6db71e1d225fc3
4277fcaada4939b76a3df4515b7f74837bf8c4b75d4ff00f8d464169eede01e3
4446efafb4b757f7fc20485198236bed787c67ceffc05f70cd798612424384ce
48f3ead8477f3ef16da6b74dadc89661a231c82b96f3574c6b7ceb9c03468291
4a2236596e92fa704d8550c56598855121430f96fe088712b043cba516f1c76c
54029bd4fcc24551564942561a60b906bee136264f24f43775b7a8e15095a9e0
56da872e8b0f145417defd4a37f357b2f73f244836ee30ac27af7591cda2d283
5e7edc8f1c652f53a6d2eabfbd9252781598de91dbe59b7a74706f69eb52b287
5f20cc6a6a82b940670a0f89eda5d68f091073091394c362bfcaf52145b058db
61e305d6325b1ffb6de329f1eb5b3a6bcafa26c856861a8200d717df0dec48c4
67f1db122ad8f01e5faa60e2facf16c0752f6ab24b922f218efce19b0afaf607
7491f298e27eb7ce7ebbf8821527667a88eecd5f3bc5b38cd5611f7ebefde21e
79b7964bde948b70a7c3869d34fe5d5205e6259d77d9ac7451727d68a751aa7d
7aa62af5a55022fd89b3f0c025ea508128a03aab5bc7f92787b30a3e9bc5c6e4
8769912b9769b4c11aabc523a699d029917851822d4bc1cb6cc65b0c27d2b135
8aace6989484b88abc7e3ec6f70b60d4554bf8ee0f1ccad15db84ad04c953c2d

942489ce7dce87f7888322a0e56b5e3c3b0130e11f57b3879fbefc48351a78f6
a881c9f40c1a5be3919cafb2ebe2bb5b19e29f0f7b28186ee1f4b554d692e776
bdb76c8d0afcd6b57c8f1fa644765b95375af2c3a844c286db7f60cf9ca1a22a
d815fb8febaf113f3cec82f552dfec1f205071a0492f7e6a2657fa6b069648c6
e1997d1c3d84c29e02b1b7b726a0d0f889a044d7cd339f4fb88194c2c0c6606d
e31af5131a095fbc884c56068e19b0c98636d95f93c257a0c829ec3f3cc8e4ba
ef987baef9a1619454b14e1fec64283808d4e0ce16fb87d06049bfcf9cf56af3
f29d386bdf77142cf2436797fba1f8b05fab5597218c2b77f57e46b8400eb9de
f7359490d6c141ef7a9ee2c03dbbd6ce3069e926d83439e1f8a3dfb3a7c3dc94
f8995634b102179a5d3356c6f353cb3a42283d9822e157502486262a3af4447e
ff167e09b3b7ad6ed1dead9ee5b4747dd308699a00905e86162d1ec1b61e0476

Network

52.79.118.195
61.81.50.174
[URL]/[FOLDER]/[FILENAME]asp?prd_fld=racket
happy.nanoace[.]co.kr
hxxp://happy.nanoace[.]co.kr/Content/rating/themes/krajee-fas/FrmAMEISMngWeb.asp
hxxps://mariamchurch[.]com/board/news/index.asp
hxxps://www.aumentarelevisite[.]com/img/context/offline.php
mariamchurch.com
www.aumentarelevisite[.]com
www.juneprint[.]com
www.jungfrau[.]co.kr
www.ric-camid[.]re.kr

File names

addins.cpl
dolby.cpl
ezhelp.cpl
final.cpl
officecert.ocx
skynet.cpl
wpm.cpl
Services
arm
uso

原廠網址：https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/lazarus-dream-job-chemical

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