UFO-1

福爾摩斯場景

在工業控制系統 (ICS) 產業，你的安全團隊需要隨時保持最新狀態，並了解產業內針對組織的威脅。你剛開始擔任威脅情報實習生，並擁有一些安全營運中心 (SOC) 經驗。你的經理給你佈置了一項任務，旨在測試你的研究技能，以及你如何有效利用 Mitre ATT&CK 來獲得優勢。你應該研究一下 Sandworm 團隊（又稱 BlackEnergy 集團和 APT44）。利用 Mitre ATT&CK 了解如何以可操作的形式繪製對手的行為和策略。爭取通過評估，給你的經理留下深刻印象，因為你對威脅情報充滿熱情。

關於UFO-1
這個 Sherlock 主要是使用來自該組織的 Mitre Att&ck 頁面的數據來研究 Sandworm 團隊的歷史和能力。

任務 1

根據 Mitre 引用的消息來源，沙蟲小組於哪一年開始行動？

`2009`

任務 2

Mitre 指出，在 2016 年針對烏克蘭電網的攻擊活動中，BlackEnergy 組織使用了兩種憑證存取技術來存取受感染網路中的多個主機。其中一種是 LSASS 記憶體存取 (T1003.001)。另一種攻擊的攻擊 ID 是什麼？

`T1110`

企業	T1110	暴力破解	在2016 年烏克蘭電力攻擊期間，Sandworm 團隊使用腳本嘗試對多台主機進行 RPC 驗證。[2]

任務 3

在2016年的攻擊活動中，我們觀察到攻擊者在操作過程中使用了VBS腳本。這個VBS檔案的名字是什麼？

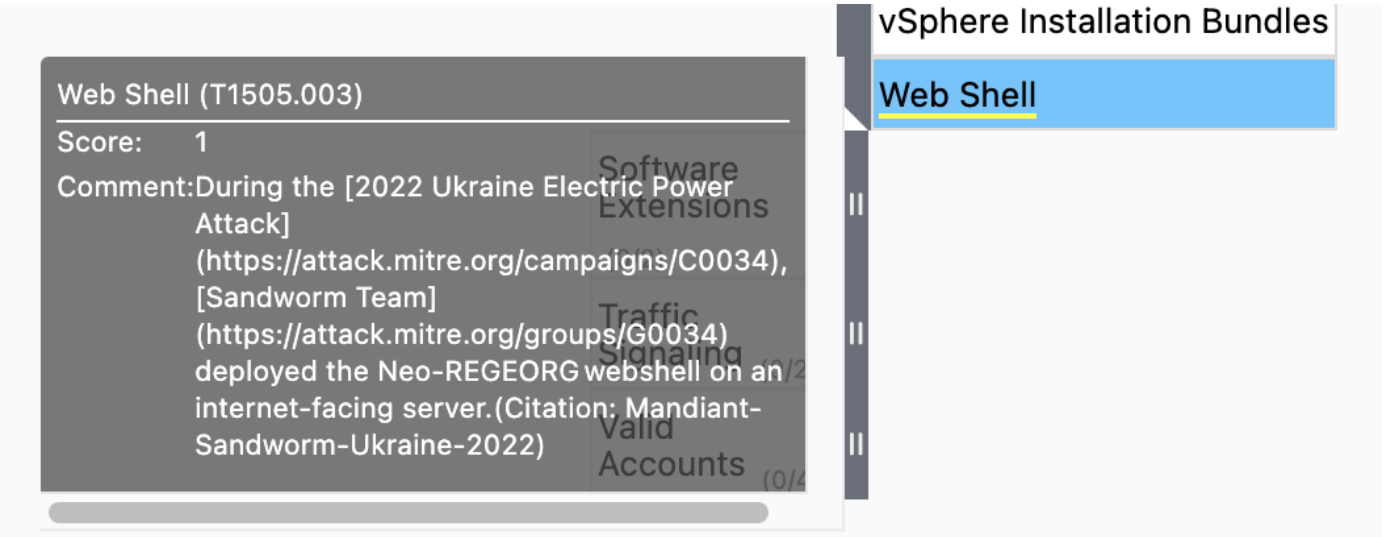
`ufn.vbs`

ICS	T0867	橫向工具轉移	在2016年烏克蘭電力攻擊事件中，Sandworm 團隊使用 VBS 腳本進行工具橫向轉移。此 VBS 腳本用於複製 ICS 專用 Payload，指令如下：`cscript C:\Backinfo\ufn.vbs C:\Backinfo\101.dll C:\Delta\101.dll` [2]

任務 4

該 APT 組織在 2022 年開展了一場大規模攻擊活動。該伺服器應用程式被濫用來維持持久性。該組織使用的持久性技術允許他們進行遠端訪問，其 Mitre Att&ck ID 是什麼？

T1505.003



任務 5

問題 4 中使用的惡意軟體/工具的名稱是什麼？

Neo-reGeorg

任務 6

在 2022 年的同一場活動中，該組織濫用了哪個 SCADA 應用程式二進位檔案來在 SCADA 系統上實現程式碼執行？

`scilc.exe`

ICS	T0895	Autorun Image	During the 2022 Ukraine Electric Power Attack, Sandworm Team used existing hypervisor access to map an ISO image named `a.iso` to a virtual machine running a SCADA server. The SCADA server's operating system was configured to autorun CD-ROM images, and as a result, a malicious VBS script on the ISO image was automatically executed.[1]
ICS	T0807	Command-Line Interface	During the 2022 Ukraine Electric Power Attack, Sandworm Team leveraged the SCIL-API on the MicroSCADA platform to execute commands through the `scilc.exe` binary.[1]
ICS	T0853	Scripting	During the 2022 Ukraine Electric Power Attack, Sandworm Team utilizes a Visual Basic script `lun.vbs` to execute `n.bat` which then executed the MicroSCADA `scilc.exe` command.[1]
ICS	T0894	System Binary Proxy Execution	During the 2022 Ukraine Electric Power Attack, Sandworm Team executed a MicroSCADA application binary `scilc.exe` to send a predefined list of SCADA instructions specified in a file defined by the adversary, `s1.txt`. The executed command `C:\sc\prog\exec\scilc.exe -do pack\scil\s1.txt` leverages the SCADA software to send unauthorized command messages to remote substations.[1]
ICS	T0855	Unauthorized Command Message	During the 2022 Ukraine Electric Power Attack, Sandworm Team used the MicroSCADA SCIL-API to specify a set of SCADA instructions, including the sending of unauthorized commands to substation devices.[1]

任務 7

確定與問題 6 中的工具執行相關的完整命令列，以針對 SCADA 環境中的變電站執行操作。

`C:\sc\prog\exec\scilc.exe -do pack\scil\s1.txt`

任務 8

在同一活動期間，使用了什麼惡意軟體/工具在受損環境中進行資料破壞？

`CaddyWiper`

Software

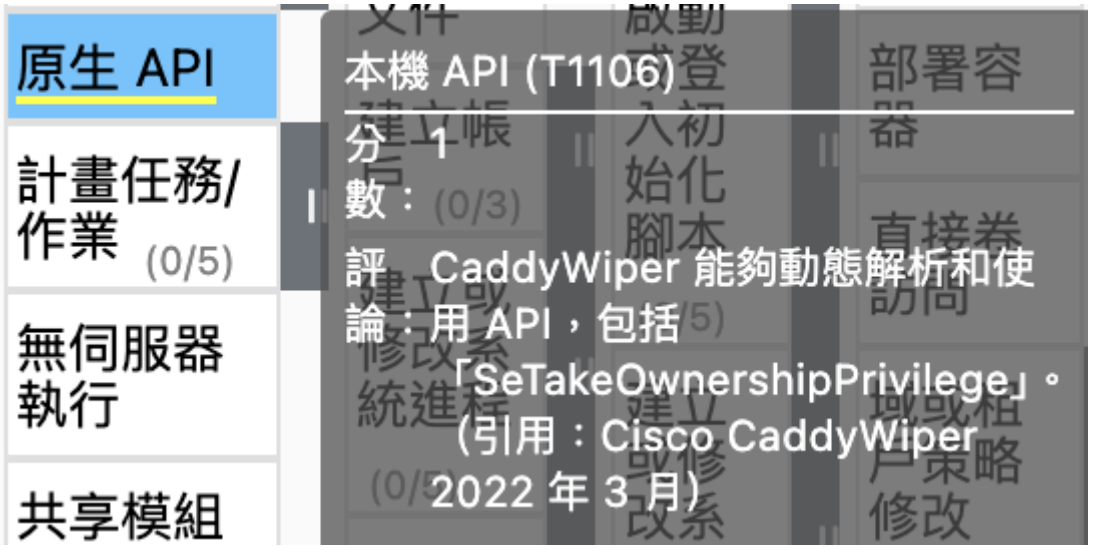
ID	Name	Description
S0693	CaddyWiper	[1]

任務 9

問題 8 中辨識出的惡意軟體/工具還具備其他功能。它在執行策略中可以執行的具體技術的 Mitre Att&ck ID 是什麼？

T1106

https://mitre-attack.github.io/attack-navigator//#layerURL=https%3A%2F%2Fattack.mitre.org%2Fsoftware%2FS0693%2FS0693-enterprise-layer.json



任務 10

Sandworm 團隊在攻擊活動中使用過各種工具。他們與一款自動傳播的惡意軟體有關，該惡意軟體既充當勒索軟體，又具有蠕蟲病毒的特徵。這款惡意軟體叫什麼名字？

NotPetya

任務 11

問題 10 中的惡意軟體用來在全球傳播的漏洞的 Microsoft 安全公告 ID 是什麼？

查詢：eternalblue vulnerability cve

https://yashpawar1199.medium.com/eternalblue-ms17-010-cve-2017-0144-exploit-and-vulnerability-overview-e9e22b84534f

MS17-010

任務 12

該組織用來攻擊調製解調器的惡意軟體/工具的名稱是什麼？

AcidRain

任務 13

威脅行為者也會在其基礎設施中使用非標準連接埠來維護營運安全。據報道，Sandworm 團隊在哪個連接埠上建立了用於監聽的 SSH 伺服器？

任務 14

Sandworm 小組在多項行動中得到了其他 APT 組織的協助。目前已知哪個組織與他們合作過？