TLP:White

MuddyWater 攻擊事件之應變

臺灣學術網路危機處理中心團隊(TACERT)製

2022 年 03 月

一、前言

MuddyWater 是最近被美國網路司令部歸入伊朗情報與安全部 (MOIS) 的 APT 組織。111/01 伊朗國家級駭客 MuddyWater 針對美國、歐洲、中東和南亞的電信、政府、石油、國防和金融部門展開了各種攻擊活動。該組織採用的典型 TTP 是在其感染鏈中大量使用腳本，使用 PowerShell 和 Visual Basic 等語言，以及頻繁使用本地二進製文件 (LoLBins)。在學網中 111/2 發生 MuddyWater 攻擊事件共有 50 件，其中以大專院校遭受攻擊件數最多。

二、 惡意軟體資訊

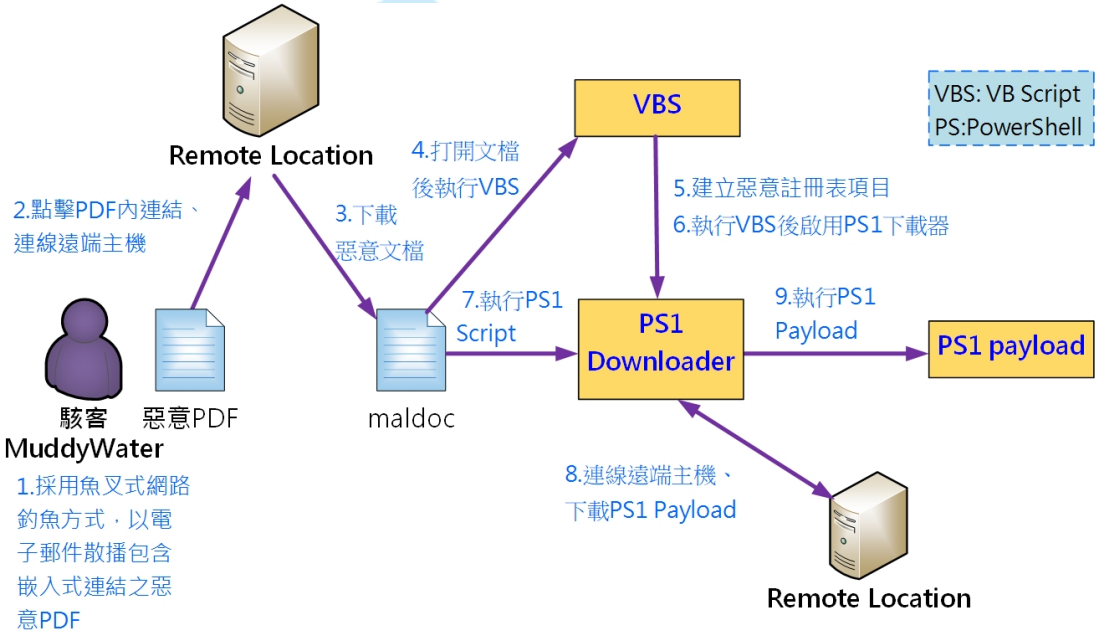
NO	項目	內容
1	惡意軟體名稱	MuddyWater (又稱為 TEMP.Zagros、Static Kitten、Seedworm 和 Mercury)
2	偵測規則	MALWARE-OTHER Ps1.Downloader.MuddyWater payload download attempt
3	發動攻擊之目的	其攻擊目的有三 **(1)間諜活動** 支持民族國家在中東的政治主導地位，出於民族國家利益的動機。 **(2)智慧財產權竊取(資料竊取)** 為民族國家帶來經濟優勢。這一目標是通過對私營機構和政府附屬機構（如大學和研究中心）展開積極的攻擊行動來實現的。 **(3)勒索軟體攻擊** 它曾試圖在受害者網路上部署諸如滅霸之類的勒索軟體，以破壞其入侵的證據或破壞私人組織的運作。
4	攻擊特徵	MuddyWater 攻擊事件會連線目的 IP:222.231.49.89:80，該 IP 為一個韓國網站。該網址被 Virustotal 檢測其惡意比例為 0/93，為非惡意網址。因無法發現目的 IP 連線有任何惡意行為與防毒軟體無法檢測出它的存在，故受害者不易發現受害主機有任何異常。從受害主機連線目的 IP:222.231.49.89:80 之封包發現受害主機與目的 IP 建立連線後，有傳輸東西給目的 IP。
5	攻擊設備	受害設備有電腦主機與手機。

三、 MuddyWater 攻擊手法

以兩種不同的方式進行攻擊。

1. 基於惡意文檔(Maldoc)之感染鏈

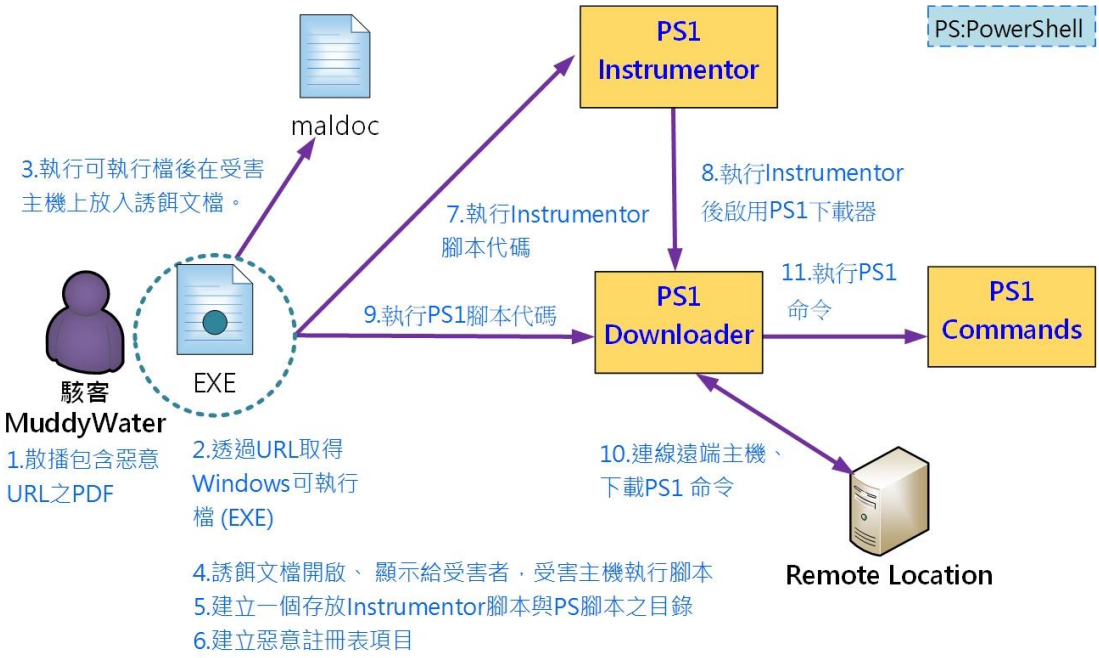
通過製作帶有嵌入式按鈕的惡意 PDF 檔案來執行的，單擊該按鈕會下載 XLS 檔案。XLS 檔案中的惡意 VBA 巨集隨後將開始感染過程，並通過產生新的註冊表項來建立持久性。同時，使用 PowerShell 下載器下載 VBScript 以從 C2 獲取主要有效負載(Payload)。



資料來源:本中心參考 TALOS 資料整理
(https://blog.talosintelligence.com/2022/01/iranian-apt-muddywater-targets-turkey.html)

2. 基於可執行檔(EXE)之感染鏈

使用特製的 EXE 執行檔而不是 XLS 檔案，但它仍然使用 PowerShell 下載器，並插入新的註冊表項以獲得持久性。



資料來源:本中心參考 TALOS 資料整理
(https://blog.talosintelligence.com/2022/01/iranian-apt-muddywater-targets-turkey.html)

五、建議措施

學校在處理 MuddyWater 攻擊事件時，使用對受害主機掃毒方式無法發現惡意程式所在，而檢視目的 IP 網站亦無法看出惡意行為。因此，在處理本類型資安事件時，有下列處理建議提供學校參考。

1. 向開單單位索取該事件封包來進行分析，以判斷是否有惡意傳輸行為。
2. 在受害設備上執行觀察網路連線之軟體(例如:TCPView)，以找出連線目的 IP 之惡意程式。
3. 因該類型惡意程式會新增註冊表項目，讓自己於每次開機時啟動，故在移除惡意程式時，需先中斷其程式執行後，再進行完整移除。惡意程式移除後，建議確認開機後背景程式之內容是否仍有其存在。
4. 若學校因網路架構為 NAT 架構而無法找到受害設備，則建議學校可先行封鎖校內 IP 對目的 IP 之連線，以免重複觸發該類型事件。