如何保護CI供水系統安全

◆ 華梵大學特聘教授 — 朱惠中

水是生命的必需品，網路犯罪分子對關鍵基礎設施供水系統的攻擊行動已與日俱增，恐對人命造成危害。

水設施是攸關生命的關鍵基礎設施

美國擁有超過 15 萬公共飲用水系統和 1 萬 6 千個公有廢水處理系統，8 成以上美國人從這些飲用水系統獲得飲用水，75% 美國人會使用此廢水系統。「水和廢水系統部門」（Water and Wastewater Systems Sector, WWS，簡稱水設施）容易受到各種攻擊，包括物理攻擊（例如：致命毒劑汙染或有毒氣體化學釋放）、網路攻擊。任何攻擊都可能導致大量疾病與人員傷亡。

安全飲用水是保護公眾健康和所有人類活動的先決條件，妥善處理廢水對於預防疾病和保護環境至關重要。因此，確保水設施安全為關鍵基礎設施（CI）防護的重要工作。

美國 CI 的安全漏洞

事實上，美國水設施系統仍未做好網路安全保護，因為提高營運效率而透過網路來連接各種設施的系統架構，已帶來網路威脅風險。

美國 ICS-CERT 所發布的資料顯示，在 2021 年下半年，共計有 253 個漏洞諮詢，其中近 8 成漏洞為嚴重及高風險等級；至於這些漏洞所影響之產業別，第一名為關鍵製造業、第二名為能源領域、第三名則為水設施，此排名與 2019、2020 年，以及 2021 年上半年一致，研判水設施名列前茅之原因，係該產業採用之設備廠牌廣泛，此一特性亦同時帶來管理的複雜度。

水設施的網路安全事件

2018 年 2 月，以色列工控威脅偵測資安公司 Radiflow 在他們的水設施客戶網路中發現加密挖礦惡意軟體。

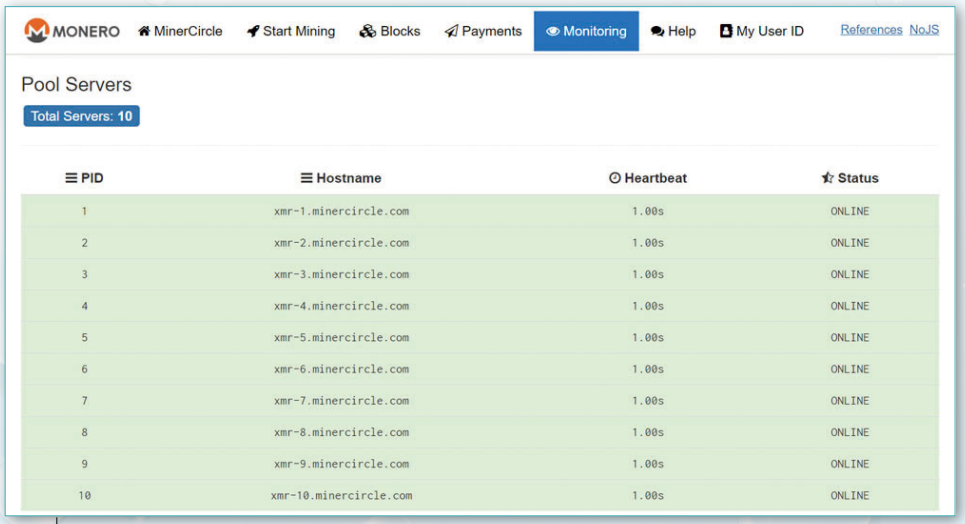
2019 年 3 月，位於美國堪薩斯州水設施的離職員工，試圖利用其在辭職後尚未被撤銷之數位憑證（Digital Certificate）來進行遠端存取，操控相關設施威脅飲用水安全，所幸未成功。

2019 年 3 月，美國科羅拉多州供水系統，遭受勒索軟體攻擊。該水廠擁有 4 萬 5 千名用戶，此次並非該水廠首度遭受攻擊。本次攻擊雖未損害到操作系統，然已促使水區關閉相關訊息服務。

2020 年 4 月，駭客攻擊以色列水設施網路系統，並試圖破壞水設施，以及調節氯氣和其他化學物質添加量的控管系統。

2020 年 9 月，美國新澤西州水設施工作人員發現潛在的 Makop 勒索軟體已經破壞了他們系統中的重要文件。

2020 年 12 月，伊朗政府資助一個經常針對以色列的攻擊組織，唆使其攻擊以色列的水設施系統，侵入遠端存取軟體，並駭進控制設備的 HMI [1] 管理主機來操控化學參數。



2018 年 2 月，以色列工控威脅偵測資安公司 Radiflow 在他們的水設施客戶網路中發現加密挖礦惡意軟體。（Source: Radiflow, https://www.radiflow.com/case-studies/detection-of-a-crypto-mining-malware-attack-at-a-water-utility）

[1] HMI 是 Human Machine Interface 的縮寫，人機界面，是系統和用戶進行互動和訊息交換的媒介。https://www.easyatm.com.tw/wiki/HMI。

2021 年 1 月，駭客試圖毒害美國舊金山灣區的水設施。

2021 年 2 月，駭客攻擊美國佛州奧爾德斯瑪市的水設施，將水中的氫氧化鈉濃度從百萬分之一百調高 111 倍。攻擊者利用水設施使用的 TeamViewer [2] 漏洞來存取工廠的控制系統，並更改相關參數至超標數值。幸運的是，控制臺操作人員立即注意到，並緊急進行修正，因而未對成千上萬的奧爾茲瑪居民造成嚴重影響。

2021 年 3 月，駭客使用變種勒索軟體對美國內華達州水設施進行攻擊，該軟體影響到監控和數據採集系統（Supervisory Control and Data Acquisition, SCADA），並造成該系統功能部分受阻。

2021 年 8 月，駭客使用 Ghost 變種勒索軟體攻擊美國加州的水設施。所幸，在發動攻擊前，系統管理者在 SCADA 系統上發現勒索軟體，並發現此軟體已在系統中存在大約一個月之久。

2021 年 7 月，駭客將 ZuCaNo 勒索軟體使用遠端存取方式，入侵美國緬因州水設施的 SCADA 系統，造成該系統只能以人工操作，且無法與遠端設施連線。

2021 年 5 月，澳洲昆士蘭州審計辦公室指出，SunWater 自來水廠被駭客入侵潛伏於該水設施網路長達 9 個月，攻擊者並接管該水廠儲存客戶資料的網頁伺服器，長達 10 個月之久。

這次攻擊大都試圖篡改水設施的管控系統，藉此產生含過量化學物質的飲用水；而這些化學物質原本添加目的，**主要是微量使用以減少水中病原體、礦物質或其他汙染物殘留**，然這些化學物質若遭過量添加，恐將對人體造成非常嚴重的危害。

駭客針對水設施之攻擊模式

由前揭諸多案例顯示，水設施的資安防護系統仍相當脆弱。網路犯罪本身又是一個不斷推陳出新的行業，CI 網路安全所面臨挑戰將更形艱鉅。綜整水設施駭客之攻擊方式與目標如下：

2021 年 5 月，澳洲昆士蘭州審計辦公室指出，SunWater 自來水廠被駭客入侵，攻擊者接管該水廠儲存客戶資料的網頁伺服器，時間長達 10 個月之久。（Photo Credit: Sunwater Facebook, https://www.facebook.com/Sunwater/posts/310060041166187）

[2] TeamViewer 為遠端存取和控制軟體，允許維護遠端電腦和其他設備。

駭客攻擊試圖篡改水設施的管控系統，將主要用以減少水中病原體、礦物質或其他汙染物的微量化學物質過量添加，此舉恐將對人體造成嚴重危害。

一、先針對資安防護可能不足的小型水設施，即蒐集資安防護明顯脆弱的外站，作為初始入侵的目標。

二、攻擊者目標是用於控制閥門的可編程邏輯控制器（PLC）。

三、可能為供應鏈攻擊，攻擊者針對的是合法使用供水設施的承包商。

四、挑選沒有設定適當網路安全組態來應對更複雜的攻擊，比如有針對性的魚叉式網路釣魚（Spear Phishing）的擁有者。

五、使用變種勒索軟體進行攻擊。

六、破壞 SCADA 系統中的文件。

七、攻擊者主要目標是破壞，特別是破壞 ICS 系統的完整性。

八、利用遠端登入及存取來進行入侵。

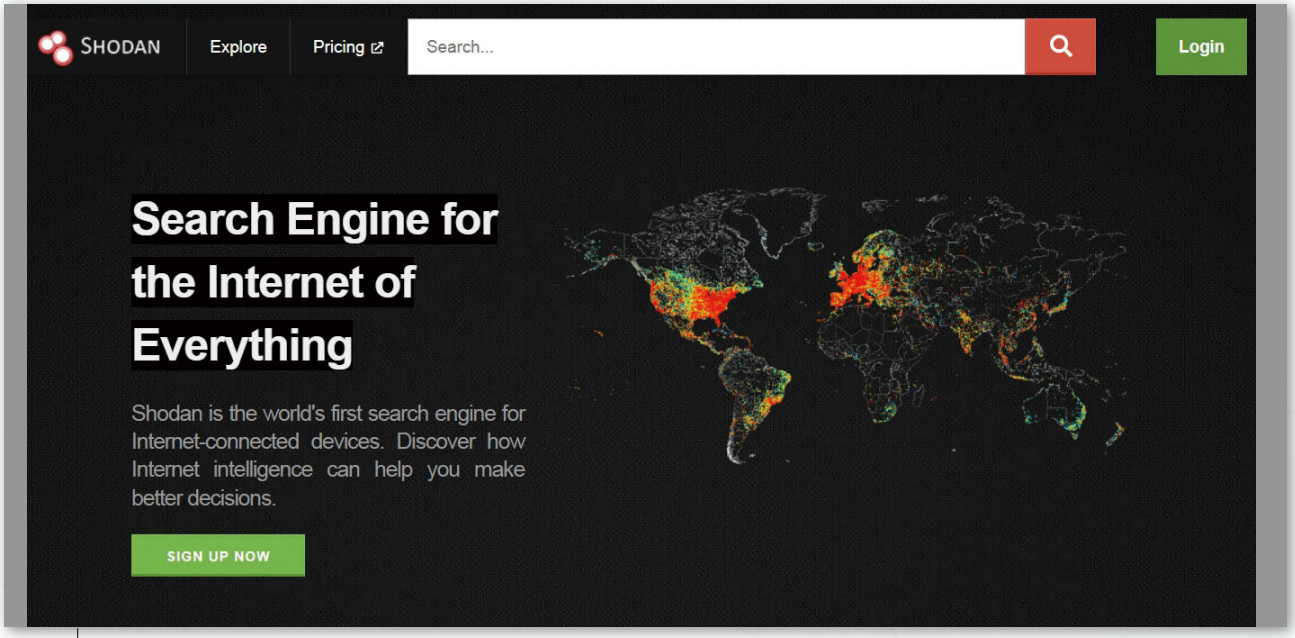
九、SCADA 與 AP 系統共用相同的密碼。

水設施的安全準則

自 2021 年 2 月佛州奧爾德斯瑪市水設施遭駭客攻擊後，美國網路安全和基礎設施安全局（Cybersecurity and Infrastructure Security Agency, CISA）、環境保護局（Environmental Protection Agency, EPA）、聯邦調查局（Federal Bureau of Investigation, FBI）及國土安全部（Department of Homeland Security, DHS）等單位針對水設施，提供以下三個面向的安全準則：

一、水設施業者應密切留意網路安全法規動態，並主動防範網路攻擊：

1. 分割（Segmenting）和隔離（Segregating）網路和功能。
2. 限制不必要的橫向交流（Lateral Communications）。
3. 強固網路設備之安全，如選擇 HA 設備。
4. 確保對基礎設施設備的存取安全。
5. 伺服器系統及網路設備的遠端管理，宜執行頻外管理。
6. 驗證硬體和軟體的完整性，即確保資料無論是在傳輸或儲存的生命週期中，保有其正確性與一致性。
7. 利用搜尋軟體（如 Shodan）蒐集水設施暴露在網路上的系統，並加以適當的處置，以降低可以從 Internet 存取 Intranet 的風險。



Shodan 是一種搜尋裝置，目標是連上網路的物聯網設備，種類包含電腦、交換器、網路攝影機，甚至於工業控制系統等，其會掃描全世界的 IP，全天候更新資料庫，使用者能迅速獲得最新資訊。

8. 更改已暴露在網路上的控制系統密碼，並確保軟體都是最新版。

二、遠端工作會帶來額外的風險，故需要採取額外的預防措施；CISA 等單位建議更改預設密碼、限制網路（段）存取、加密機敏資料、安裝防火牆、維護／更新防毒軟體版本、審慎執行共享資訊以及選擇使用聲譽卓著的 VPN 產品來連接內外網，另亦須訂定遠端存取軟體的安全要求。

三、水設施業者應制定緊急事件「應變計畫」，特別是如何自救、互救及他救；細節包括事前的準備（自救），在發生被攻擊時可請求其他水設施網路人員和執法人員名單（互救），及事後的復原（他救）。另須檢查是否依照不同災害類別與情境建立應變計畫與處理程序，並驗證其合理性、可操作性及可執行性。

他山之石，可以攻錯

時值臺灣逐漸進入夏季之際，供水將成為關鍵的民生問題，前述美國、澳洲及以色列等國所發生的案例，應可以作為我們借鏡。

另各 CI 擁有者未來評估、採購 ICS（PCL）設備時，建議應將設備是否符合 IEC 62443-4-2 標準，作為評估考量因素之一，避免未經資安測試的產品，直接部署於相關場域中，以增加駭客入侵 OT 場域並利用 ICS 設備漏洞發動攻擊之困難度。