

# 以 Volt Typhoon 攻擊滲透美非 國家電力設施之實例，探討 LotL 類型的攻擊對應策略

Based on 2023 Cybersecurity Annual Report by TXOne Networks

TXOne Networks | Jeffrey Cheng

# 資訊戰成為地緣政治的前哨

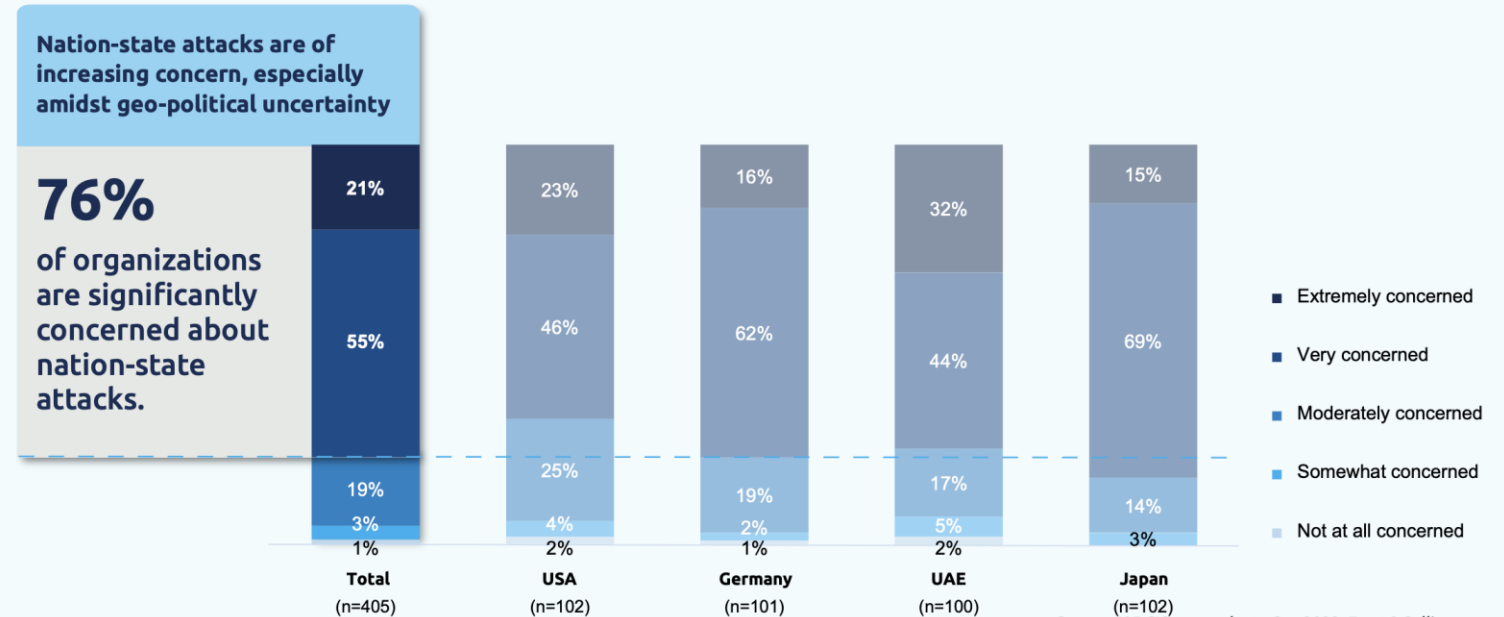


# 76%

of organizations  
expressed significant  
concerns over  
nation-state attacks.

## How concerned are you about nation-state attacks?

### Level of Concern Regarding Nation-State Attacks



# Volt Typhoon – 中國對準西方世界的資訊武器

## 初見

2023年五月  
微軟公布重大發現  
美軍基地被中國駭客入侵數月

手法精巧 難以追蹤  
寄生合法軟體行非法活動

## CISA (\*) 跟進調查結果

2024二月公布美國受害單位包括：  
能源部/環保局/運輸安全部

值得關注的西方世界受害單位：  
紐 / 澳 / 加 / 英等國家資安中心

主要攻擊對象區塊：  
能源 / 通訊 / 運輸 / 水資源  
(皆為民生必需)

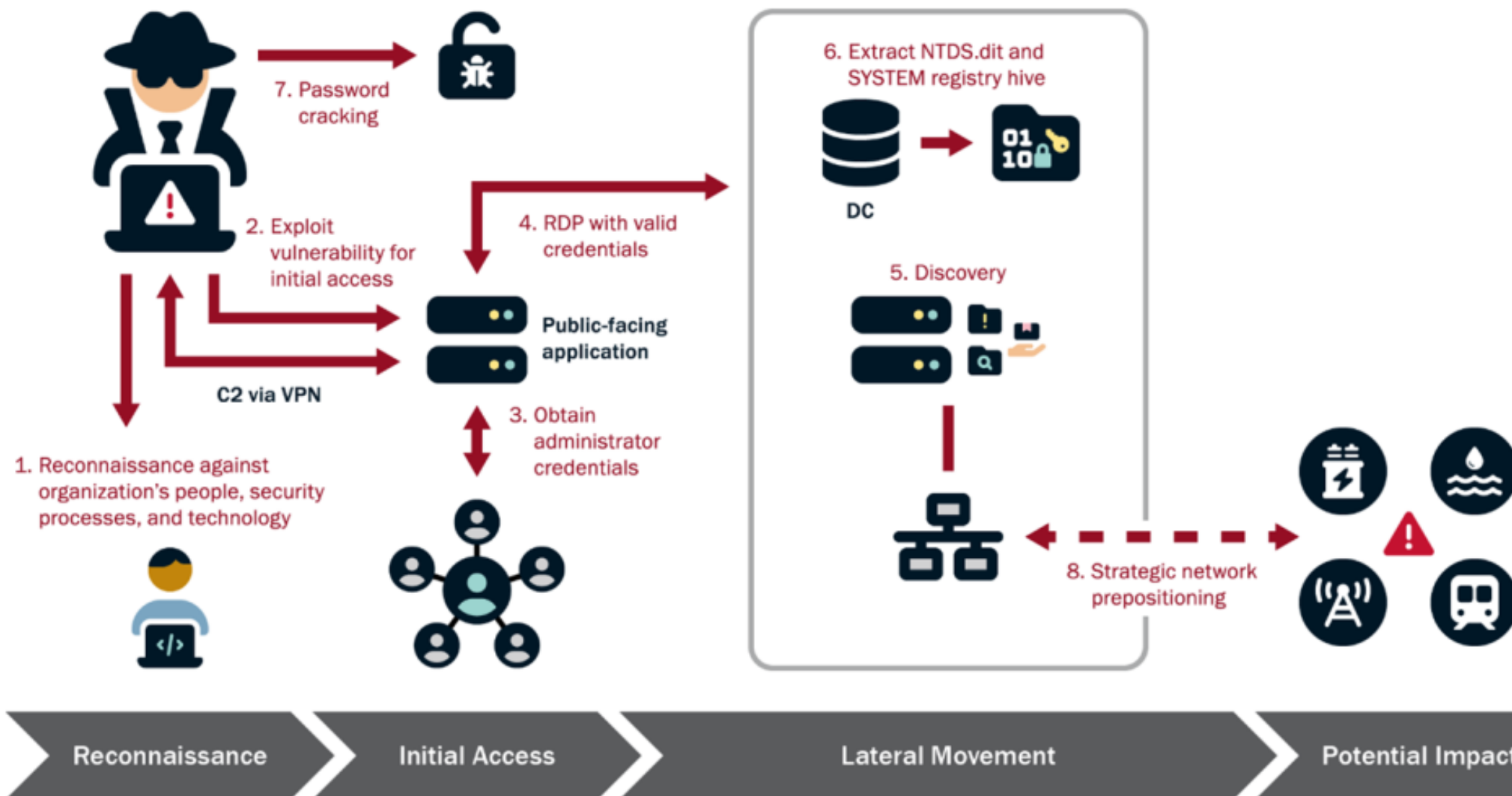
## 其餘民間調查發現

類似的駭客團體主要活躍在  
美國 / 非洲 / 亞洲

以前述區塊為主要攻擊對象

類似手法也不斷針對台灣的各  
關鍵基礎設施進攻

# 寄生合法工具行惡事的 LoTL 攻擊



# LoTL 攻擊難以應對的原因

## 技術面

前端滲入跳板常無法佈建資安軟體

後段工作無惡意檔案可供現有資安軟體辨識

使用通用性的工具執行通用性的工作內容

## 執行面

軟硬體安全更新難以即時實施

資安人員配置質量不足

穿梭在誤判警報中找出實際問題的成本過高

## OT 場域特殊現狀

多人共用設備常在人員認證的部分便宜行事

設備年限長導致軟體更新窒礙難行

其他來自供應商的商務與技術限制阻礙了資安軟體的佈建

# 工控場域系統更新不易



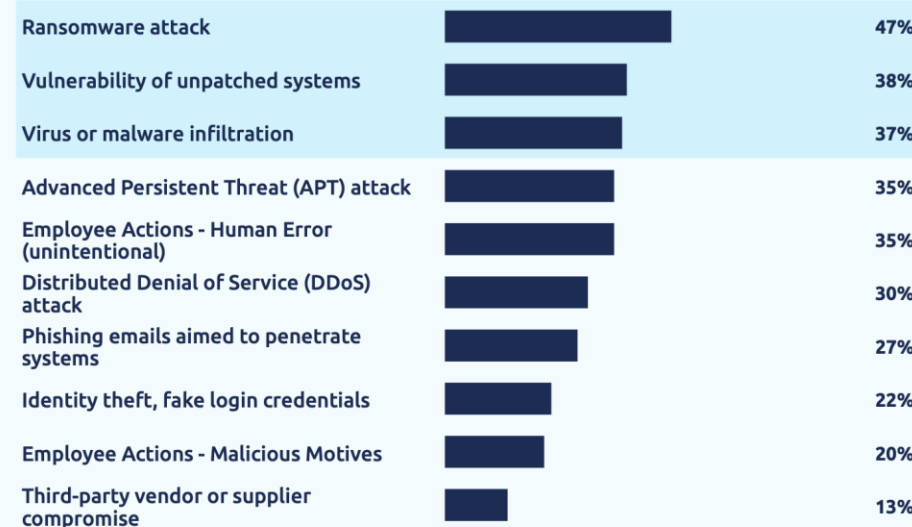
# 38%

of organizations  
faced challenges with  
unpatched system  
vulnerabilities.

## Which of the following OT security incidents have you encountered in your organization in the past 12 months?

### OT Security Incidents Encountered in the Past 12 Months

Total (n=186)



### OT Security Incidents

USA (n=49)	Germany (n=54)	UAE (n=42)	Japan (n=41)
51%	37%	52%	49%
31%	50%	33%	34%
47%	26%	48%	27%
31%	41%	31%	37%
35%	31%	33%	41%
20%	31%	29%	39%
31%	30%	21%	27%
22%	28%	24%	12%
18%	31%	10%	20%
18%	7%	17%	10%

Source: 405 CIO respondents, Sep 2023, Frost & Sullivan

# CISA 的建議行動準則及實際難處

## 行動準則

連網裝置安裝最新的安全更新

根據常見系統弱點更新其相對應的元件

採用多因子認證避免不當的帳號授權

將所有的營運及資安相關日誌檔集中管理

對所有設備提出相對應的汰修規劃

## 實際難處

既有服務無法中斷 / 無可用更新

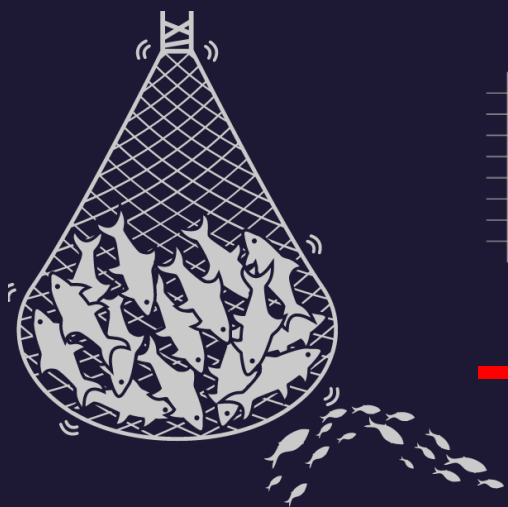
無可用更新 / 更新後的相容性問題

公用帳號問題在OT現場很常見 / 系統不具備多用戶設定功能

未能配置稱職的解讀員

工控產品壽命太長 / 無後繼機種

# 以技術手段提升防禦強度



高密度控管



高精度偵防

應用程式信任清單

網路指令使用限縮

納入工控情境

加入端點偵測及回應

增加資安的可視度



# 以政策力道推升資安態勢



提供誘因

獎勵性補貼 (如科專 / 減稅)

編列預算專款執行 (公部門)

政府力道成為關鍵



強制執行

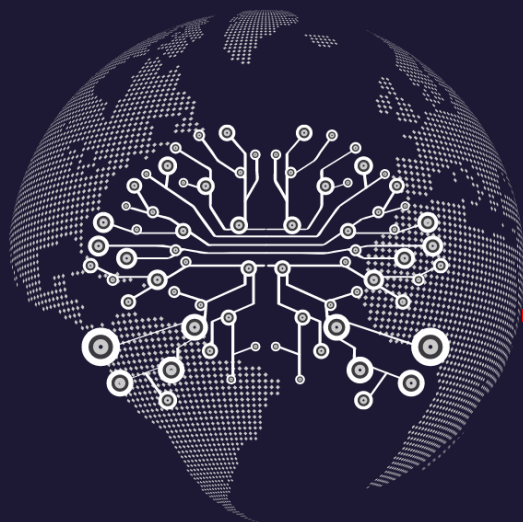
納入採購條件

稽核帶罰則

# New Regulations Propel OT/ICS Defense



# 以產業情資先期準備應變



主動比對



他山之石

US-CERT / ICS-CERT / 區域型 CERT

資產盤點及風險 / 弱點管理

SOC 角色吃重

國內 / 跨國 ISAC 情資共享平台

完整如實揭露資安情資

*Thank You*  
for your attention