戰場清理報告（Battlefield Cleanup Report）

提供遭加密/遭入侵企業管理層快速理解「現在風險在哪、我們做了什麼、為什麼需要端點防護」

近期我們在兩家不同客戶的現場支援中觀察到同一個模式：

- **事發後才靠人工排查，通常只能看到表面現象（例如：電腦異常、被加密、系統不穩）。**
- **真正的風險往往在「看不到的地方」：攻擊者仍在內網活動、仍在建立後門、或有惡意程式殘留存活。**

我們在現場透過端點檢測，直接抓到兩種最關鍵的風險

端點防護的價值不是「多裝一套軟體」，而是讓公司做到：

- **看得見**：每台電腦正在跑什麼命令、誰在執行、是否是後門行為
- **停得下來**：把正在進行式的攻擊即時阻斷，不讓它擴散
- **清得乾淨**：把事件後仍存活的惡意程式一次挖出來，避免二次災害
- **防復發**：用持續監控與政策管理，降低再次中招的機率與成本

1. 案例一：入侵後的潛伏攻擊（嘗試建立 AD 高權限帳號）

1.1 現場背景

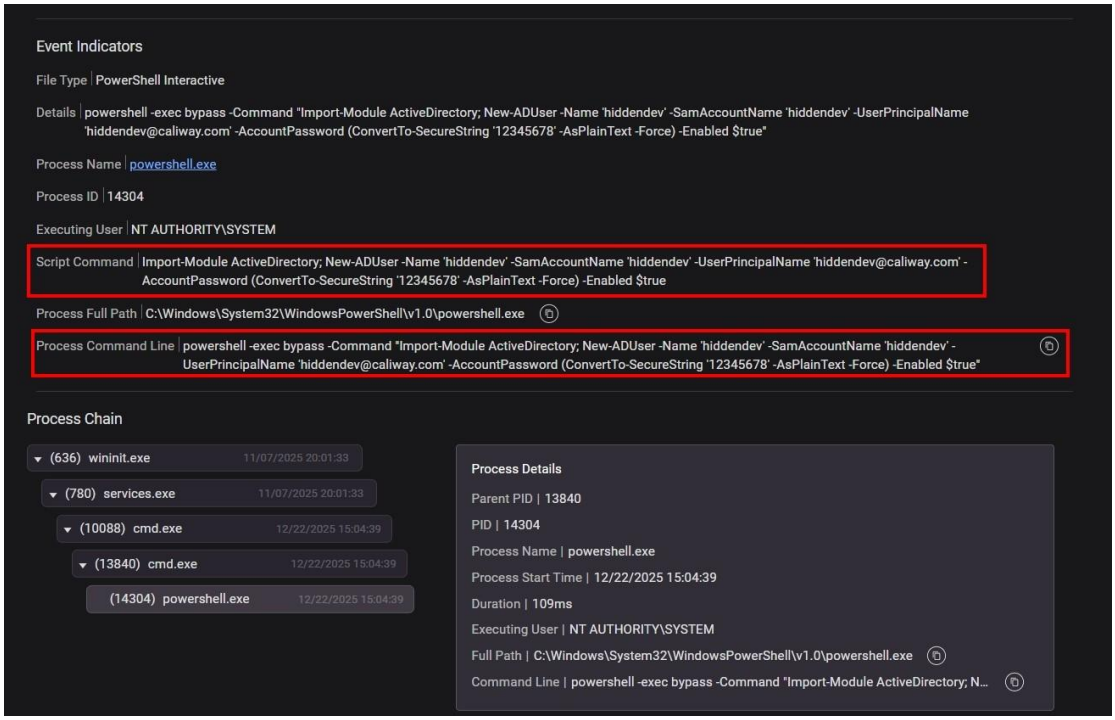
- 客戶已確認遭入侵，我方受通知到場協助。
- 目標是確認：**攻擊者還在不在？是否還在持續動作？**

1.2 我們看到的事實

在端點偵測中發現：系統以 PowerShell 執行命令，**嘗試建立新的 AD 帳號**（疑似高權限/後門帳號用途）。

- **執行者身分**：SYSTEM（代表是用服務或排程等方式在最高權限下跑）
- **行為內容**：載入 ActiveDirectory 模組，建立新使用者（New-ADUser）
- **特徵**：使用 -ExecutionPolicy Bypass（繞過 PowerShell 限制，常見於攻擊者手法）
- **程序鏈**：服務程序 → 命令列 → PowerShell（代表非人工手動點開，而是以"背景方式"觸發）

📌 **圖 1：端點預測性攔截 PowerShell 建立 AD 帳號的命令與程序鏈**



攻擊者不是"可能想做壞事"，而是已經在系統裡用最高權限下指令，準備建立可長期控制公司網域的帳號。

1.3 這代表什麼風險

如果這種 AD 帳號建立成功，攻擊者通常可以：

- **反覆登入、長期潛伏**（清掉一次還會再回來）
- **擴散到其他伺服器與電腦**（含檔案伺服器、ERP、產線控制主機）
- **準備第二階段**：資料外洩、勒索加密、刪除備份、癱瘓 AD

1.4 戰場清理

- **立即隔離可疑端點**（避免命令擴散、避免帳號建立成功後擴權橫向移動）
- **阻斷正在進行式的命令行為**（把"現在正在做的壞事"停下來）
- **回收證據**：保留命令列、程序鏈、時間點，作為後續追查與管理層決策依據

Deep Instinct 的優勢與價值

攻擊者使用 -ExecutionPolicy Bypass 配合 SYSTEM 權限 ，這在傳統掃描中屬於「合法系統行為」。

Deep Instinct 不需要病毒碼，它是透過深度學習預測該指令鏈（程序鏈） 具有攻擊意圖，在帳號尚未建立前就達成「預測性攔截」。

1.5 可量化果（老闆看得懂）

- ✅ **阻止攻擊者擊者建立後門帳號**（避免長期控制風險）
- ✅ **把正在進行的潛伏攻擊即時拉停**（不是事後推測）
- ✅ **提供清楚證據鏈**，讓管理層能判斷是否要擴大應變與投資防護

2. 案例二：WannaCry 存活感染（出事後才發現“一堆還活著”）

2.1 現場背景

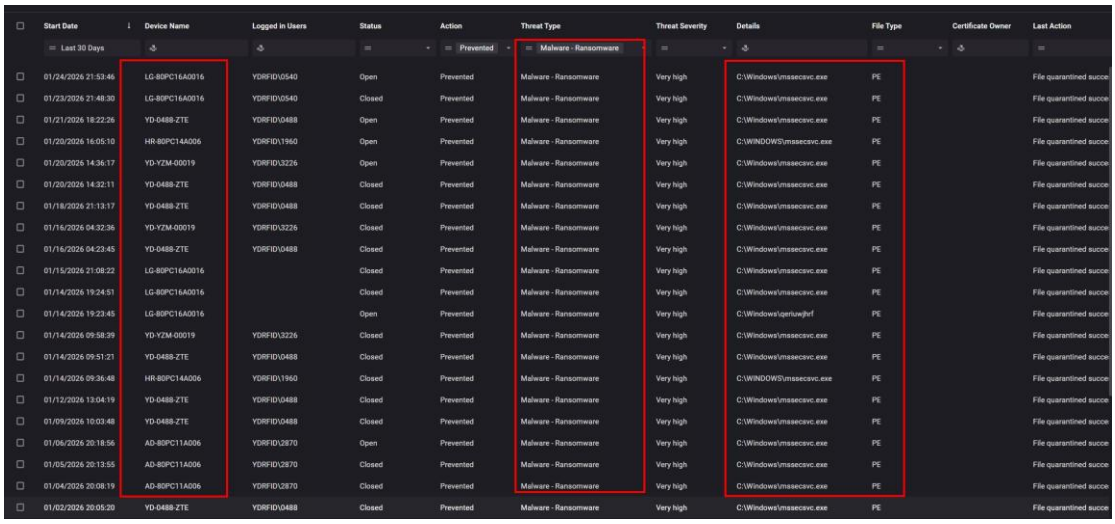
- 客戶已發生事件，擔心產線電腦與辦公 PC 還有殘留感染。
- 我方協助佈署端點檢測後，發現多台主機仍存在 WannaCry 存活元件。

2.2 我們看到的事實

端點告警顯示多台設備偵測到「勒索軟體 / 蠕蟲」相關檔案，並成功處置（隔離/收斂）。

- **威脅類型**：Malware – Ransomware（勒索軟體）
- **嚴重度**：Very High（極高）
- **常見檔名**：C:\Windows\mssecsvc.exe（WannaCry 常見組件之一）
- **涵蓋範圍**：多台設備、跨產線與一般電腦（代表不是單點，而是“面”的問題）

📌 **圖 2：端點掃描在多台主機找到 WannaCry 存活元件**



Start Date	Device Name	Logged in Users	Status	Action	Threat Type	Threat Severity	Details	File Type	Certificate Owner	Last Action
Last 30 Days				Prevented	Malware - Ransomware					
01/24/2026 21:53:46	LG-80PC16A0016	YDRFID\0540	Open	Prevented	Malware - Ransomware	Very high	C:\Windows\mssecsvc.exe	PE		File quarantined succe
01/23/2026 21:48:30	LG-80PC16A0016	YDRFID\0540	Closed	Prevented	Malware - Ransomware	Very high	C:\Windows\mssecsvc.exe	PE		File quarantined succe
01/21/2026 18:22:26	YD-0488-ZTE	YDRFID\0488	Open	Prevented	Malware - Ransomware	Very high	C:\Windows\mssecsvc.exe	PE		File quarantined succe
01/20/2026 16:05:10	HR-80PC14A006	YDRFID\1960	Open	Prevented	Malware - Ransomware	Very high	C:\WINDOWS\mssecsvc.exe	PE		File quarantined succe
01/20/2026 14:36:17	YD-YZM-00019	YDRFID\3226	Open	Prevented	Malware - Ransomware	Very high	C:\Windows\mssecsvc.exe	PE		File quarantined succe
01/20/2026 14:32:11	YD-0488-ZTE	YDRFID\0488	Closed	Prevented	Malware - Ransomware	Very high	C:\Windows\mssecsvc.exe	PE		File quarantined succe
01/18/2026 21:13:17	YD-0488-ZTE	YDRFID\0488	Closed	Prevented	Malware - Ransomware	Very high	C:\Windows\mssecsvc.exe	PE		File quarantined succe
01/16/2026 04:32:36	YD-YZM-00019	YDRFID\3226	Closed	Prevented	Malware - Ransomware	Very high	C:\Windows\mssecsvc.exe	PE		File quarantined succe
01/16/2026 04:23:45	YD-0488-ZTE	YDRFID\0488	Closed	Prevented	Malware - Ransomware	Very high	C:\Windows\mssecsvc.exe	PE		File quarantined succe
01/15/2026 21:08:22	LG-80PC16A0016		Closed	Prevented	Malware - Ransomware	Very high	C:\Windows\mssecsvc.exe	PE		File quarantined succe
01/14/2026 19:24:51	LG-80PC16A0016		Closed	Prevented	Malware - Ransomware	Very high	C:\Windows\mssecsvc.exe	PE		File quarantined succe
01/14/2026 19:23:45	LG-80PC16A0016		Open	Prevented	Malware - Ransomware	Very high	C:\Windows\qeriuwjhrf	PE		File quarantined succe
01/14/2026 09:58:39	YD-YZM-00019	YDRFID\3226	Closed	Prevented	Malware - Ransomware	Very high	C:\Windows\mssecsvc.exe	PE		File quarantined succe
01/14/2026 09:51:21	YD-0488-ZTE	YDRFID\0488	Closed	Prevented	Malware - Ransomware	Very high	C:\Windows\mssecsvc.exe	PE		File quarantined succe
01/14/2026 09:36:48	HR-80PC14A006	YDRFID\1960	Closed	Prevented	Malware - Ransomware	Very high	C:\WINDOWS\mssecsvc.exe	PE		File quarantined succe
01/12/2026 13:04:19	YD-0488-ZTE	YDRFID\0488	Closed	Prevented	Malware - Ransomware	Very high	C:\Windows\mssecsvc.exe	PE		File quarantined succe
01/09/2026 10:03:48	YD-0488-ZTE	YDRFID\0488	Closed	Prevented	Malware - Ransomware	Very high	C:\Windows\mssecsvc.exe	PE		File quarantined succe
01/06/2026 20:18:56	AD-80PC11A006	YDRFID\2870	Open	Prevented	Malware - Ransomware	Very high	C:\Windows\mssecsvc.exe	PE		File quarantined succe
01/05/2026 20:13:55	AD-80PC11A006	YDRFID\2870	Closed	Prevented	Malware - Ransomware	Very high	C:\Windows\mssecsvc.exe	PE		File quarantined succe
01/04/2026 20:08:19	AD-80PC11A006	YDRFID\2870	Closed	Prevented	Malware - Ransomware	Very high	C:\Windows\mssecsvc.exe	PE		File quarantined succe
01/02/2026 20:05:20	YD-0488-ZTE	YDRFID\0488	Closed	Prevented	Malware - Ransomware	Very high	C:\Windows\mssecsvc.exe	PE		File quarantined succe

事件過後，惡意程式不一定消失。這裡顯示在多台電腦仍找到勒索軟體/蠕蟲元件，代表未來仍可能再次爆發或擴散。

2.3 這代表什麼風險

WannaCry 這類蠕蟲特性是：

- **會自己找下一台去感染**（不用人操作）

- **常從老舊系統/舊漏洞下手**（產線特別常見）
- **一次沒清乾淨，之後就可能"再炸一次"**
  尤其當公司以為「都修好了」而鬆懈時，最容易二次災害。

Deep Instinct 的優勢與價值

產線電腦通常效能有限或無法隨時連網更新。

Deep Instinct Agent 極小、不佔 CPU 資源且具備長期離線防護能力，非常適合案例二中分佈於產線的設備，能在不影響產能的前提下，把殘留的 WannaCry 元件一次清除 。

2.4 戰場清理動作

- **對全網端點進行快速檢測與收斂**（找出存活感染）
- **隔離/處置高風險檔案**（避免持續擴散）
- **列出感染清單**（哪些機器、什麼時間、什麼檔案、處置結果）

2.5 可量化成果

- ✅ **把存活感染一次性挖出來**（避免"以為好了其實沒好"）
- ✅ **降低蠕蟲再擴散機率**（保住產線/營運連續性）
- ✅ **提供清單化證據**：哪些主機需要優先修補、重灌或加強管控

3. 管理層決策建議

3.1 為什麼“人工排查”不夠

- 人工排查通常只看到「表面症狀」(被加密、當機、某台怪怪的)
- 攻擊者要的是「長期控制」與「擴散能力」
- 所以需要能在每一台端點上，看到**正在跑什麼命令、什麼程序鏈、誰在執行**，並能立即收斂

3.2 建議採取的三段式做法

第一段：止血（48 小時內）

- 全網快速部署端點檢測
- 隔離高風險主機
- 先把“正在進行式”停下來

第二段：清創（1–2 週）

- 清單化盤點：感染主機、可疑帳號、可疑排程/服務
- 針對產線與辦公網做分區收斂（避免互相傳染）
- 建立最小可用的持續監控

第三段：防復發（持續性）

- 端點防護常態化（預防 + 偵測 + 回應）
- 弱點修補與資產盤點制度化
- 每月/每季提供管理層報表（用營運風險語言呈現）

Deep Instinct 的優勢與價值

人工排查只能處理「已知的痛」，但駭客要的是「長期控制」。
在第一階段（止血）： 利用 DI 快速部署，達成毫秒級的「預測性預防」，而非等加密後才反應。

在第三階段（防復發）： 將 DI 常態化，讓系統具備自發性的免疫力，減少未來每月/每季人工重複掃描的成本。