TrustONE

匿蹤主動防禦

Stealth and Active Defense

CHALLENGES

問題及威脅

- 現有資安產品防禦率只有80~90%(可擋已知攻擊及病毒)，對於一到二成的新形態攻擊及勒索軟體無法防禦
- 所有的資安產品都在努力縮短駭客或勒索軟體潛伏時間
- 常見駭客攻擊手法是拿到系統管理者帳密權限後再進行攻擊

SOLUTION

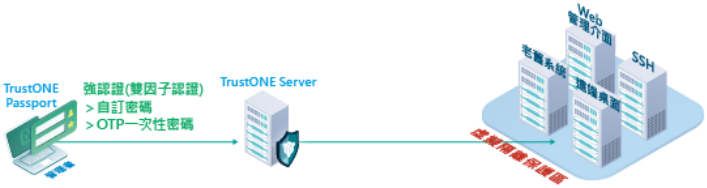
TrustONE 跳板式OTP防勒索軟體解決方案說明

1. 多因子及雙因子身分辨識

A. 主機系統管理者透過TrustONE Entry，取得TrustONE OTP雲端服務傳送的APP或E-mail驗證碼(雙因子認證)。

B. 通過身分辨識的合法管理者，可經由TrustONE server進入營運主機管理介面。

C. 就算駭客取得系統管理者的帳號密碼，如果沒有通過TrustONE OTP強認證流程就無法進入營運主機管理介面。

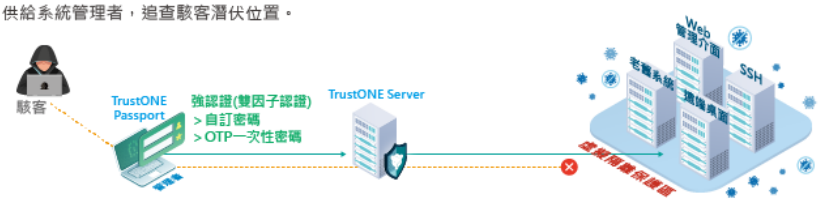


2. 跳板機虛擬隔離區

跳板式OTP機制提供跳板機功能，建置虛擬隔離區，將既有環境內的營運主機納入虛擬隔離保護區內，再加上雙因子或多因子OTP身分辨識流程，避免保護區內的營運主機遭受駭客或勒索軟體攻擊。

3. 誘敵追捕

與TrustONE Server搭配使用，可阻擋未經授權之網路連線，將駭客非法連線的行為事件紀錄、威脅情資提供給系統管理者，追查駭客潛伏位置。



硬體規格建議

TrustONE Server	
安裝環境	建議硬體設備
■ Microsoft Windows Server 2012-2019 Standard以上	■ Intel® Xeon® E-Series 處理器以上 ■ 16GB RAM or above ■ 2GB可用硬碟空間 ■ TrustONE Tunnel： ■ 1 Gbps or above乙太網路配接卡

TrustONE Passport	
安裝環境	建議硬體設備
■ Microsoft Windows 8.1-11家用進階版以上	■ 4GB RAM or above 請依作業系統與應用程式官方所列需求 ■ 250MB可用硬碟空間卡

立即洽詢

業務洽詢：零壹科技 (02)2656-5656 #805 劉先生 marshall.liu@zerone.com.tw
#213 王小姐 arisa.wang@zerone.com.tw

TrustONE | ZERONE 零壹科技

防網頁竄改攻擊

TrustONE

ZERO TRUST

TrustONE 防網頁竄改解決方案

面對新型態攻擊與既有防網頁竄改產品之瓶頸，TrustONE以「ZeroTrust零信任」技術為主軸，可防止駭客從內部入侵網站伺服器或從外部攻擊網頁漏洞，避免網頁被刪除竄改、被放置惡意程式或植入後門程式等威脅。

零壹科技提供
緊急救援服務方案!! (名額有限)

立即諮詢
零壹顧問服務

防護功能

1. 零信任Zero Trust可因應新型態攻擊

以「零信任」為技術主軸，將網站資料夾設為「唯讀保護區」，保護區內的資料夾即使透過安全程序也無法刪寫，如同將網頁製成光碟，只能瀏覽無法寫入，不讓駭客有竄改機會。

2. 不影響主機效能

不進行偵測或回復，無須消耗硬體系統運作效能，即可做到網頁防竄改效果。

3. 可保護常見網頁格式

針對目前常見的網頁格式提供防駭保護，就算駭客竊取到最高管理者權限，也無法修改或移除。

管理功能

事件紀錄及主動警示

可搭配 TrustONE Server 的事件紀錄及主動警示功能，監控受保護的網頁檔案資料夾，將違規事件紀錄提供給管理者，如果違到大量違規條件，系統將主動警示管理者。

可提供 API 整合第三方平台

TrustONE Server 提供 API 功能，可以與第三方應用程式協同作業，如：SOC 資安監控服務，將蒐集到的威脅情資匯出以便管理者判斷分析。

TrustONE

ZERONE 零壹科技

業務洽詢: 零壹科技 (02)2656-5656
#217 傅小姐 / ivy.fu@zerone.com.tw
#805 劉先生 / marshall.liu@zerone.com.tw