TrustONE

備份主機

防勒索疫苗

勒索軟體當道
為備份主機檔案接種疫苗才是防勒索之道

CHALLENGES

問題及威脅

- 病毒進入到社區感染，公衛專家建議施打疫苗增加防護力才是解決方案。
- 根據FBI調查報告指出勒索軟體潛伏在企業網路內部平均多達280天。
- 面對勒索軟體已經進入企業網路(社區感染)威脅，防勒索也要超前部署。
- 勒索軟體最喜歡透過網路芳鄰或網路磁碟機方式攻擊備份主機。
- 針對備份主機檔案接種安裝防勒索疫苗，是最優先也是最重要的選擇。

SOLUTION

TrustONE 推出防勒索疫苗方案

- TrustONE 匿蹤防疫使用「Hidden Defense」技術提供匿蹤、隔離及底層防護功能，讓備份主機檔案具有保護力防範勒索軟體攻擊。

- 可針對備份主機檔案所在的資料夾，設定為「匿蹤防疫保護區」，欺騙勒索軟體看不見保護區並且使其攻擊失靈，避免備份主機檔案被加密及被竊取。

備份主機防勒索疫苗方案說明

1. 備份主機檔案資料夾設定為「匿蹤保護區」。

2. 備份軟體讀取檔案的服務程式已被加入保護區的安全程式，所以備份軟體可以正常讀取及備份到被隱藏保護的備份主機檔案。

3. 前端檔案主機透過備份軟體可正常存取及備份檔案到備份主機的匿蹤資料夾，但勒索軟體則無法碰到被保護的檔案。

RESULTS

備份主機防勒索疫苗方案效益

- 「匿蹤」功能讓勒索軟體找不到也就無法攻擊。
- 可以做到事前預防，事中防禦第二波攻擊，有效防範勒索軟體。
- 備份軟體(包括Acronis, Commvault、Veeam及Veritas)都可正常存取備份被匿蹤保護的備份主機檔案，不影響備份軟體正常運作。
- 備份主機疫苗方案建置導入容易，不需要改變備份軟體操作使用習慣。

「匿蹤防疫保護區」

本身提供自主防護功能

底層防護
勒索軟體無法透過作業系統底層停止服務及卸載程式。

安全程序
勒索軟體不在安全程式名單，也無法帶入保護區執行。

防刪寫
勒索軟體及駭客無法寫入保護區內的檔案。

TrustONE
碩壹資訊股份有限公司

02-2627-8689 service@trustone.com.tw 台北市內湖區瑞光路335號5樓

www.TrustONE.com.tw