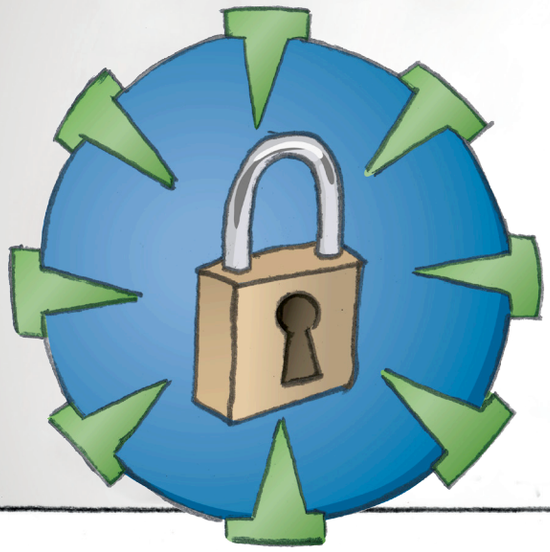

ProLion

CryptoSpike

NETAPP 儲存設備的勒索軟體 RANSOMWARE 保護

勒索軟體Ransomware（也稱為cryptotrojans）由對電腦上的資料進行加密的惡意程式組成。要求受影響的公司支付贖金以解鎖檔案； 通常與比特幣交易有關。不能保證網路罪犯是否確實發送了解密密鑰，因為他們常常沒有這樣做。

知名的惡意軟體的包括WannaCry和Petya。他們通過更改連結或電子郵件附件，偽裝成廣告以及網路釣魚或垃圾郵件進入公司。

《 Cybersecurity Insiders 2017勒索軟體報告》的事實與數據

公司與公共機構現在將勒索軟體攻擊視為最大的網路安全風險。

每年有75%的受影響組織遭受1-5次勒索軟體攻擊。 25%的人會經歷6次以上的攻擊。對於企業而言，這意味著：41%的停機時間、39%的生產力損失、30%的資料損失。

最糟糕的是：員工只需單擊一下就可以感染網路。

不僅是員工本地電腦上的檔案被損壞，電腦也可以存取授權與連接的網路上的檔案。結果加密通常還會影響中央儲存設備。因此使用NetApp CIFS / NFS授權作為NAS（網路附加儲存設備）的任何客戶都應採取針對勒索軟體的保護措施。

勒索軟體氾濫成災。每40秒就有一家公司被感染。而且許多人只在為時已晚時才注意到。

惡意軟體程式通常在背景執行數月之久卻未被察覺。結果由於原始檔案已超過備份週期，因此無法再還原它們。因為備份媒體保存的是被勒索軟體加密的檔案版本。

解決方案：CryptoSpike 即時對抗數位勒索

沒有作業系統能夠抵抗勒索軟體攻擊。許多公司甚至都不知道儲存的數百萬個檔案的那些檔案已經被加密勒索。使用CryptoSpike 您可以快速偵測到惡意軟體並防止其散播。

CryptoSpike是專門為NetApp ONTAP儲存設備系統設計的。FPolicy API記錄被攻擊CIFS與NFS的用戶。該解決方案即時監視NetApp儲存設備中的每個交易，尋找與檔案副檔名或用戶行為相關的異常。

特點

- 勒索軟體攻擊增加，每40秒就有一家公司遭到勒索軟體攻擊。
- 惡意電子郵件附件與連結的單擊足以使有害軟體開始在背景加密檔案。不僅是存放在本地PC上而且在每個授權的網路硬碟上。
- ✓ CryptoSpike可即時掃描NetApp儲存設備的檔案存取並使用三階段策略來識別勒索軟體的攻擊，並立即阻斷“攻擊與爆發”。
- ✓ 受影響的用戶被阻斷、加密檔案已識別。這樣可以防止繼續加密，進而防止關鍵服務失敗。
- ✓ 攻擊在萌芽階段被扼殺，勒索企圖被停止。

詳細 產品資訊請洽 商丞科技股份有限公司 02-29148001

運作方式：

允許使用軟體影像檔 Software Image來輕鬆安裝的架構

提供CryptoSpike FPolicy Server軟體包裝，它們可以是OVA格式（VMware的虛擬機）。該軟體影像檔僅安裝在VMware環境中。並使用CryptoSpike Manager直覺式介面完成設定、配置管理以及規則與定義臨界值。

三種攻擊偵測的統一策略

白名單White list：基於允許的檔案副檔名清單，例如.doc .xls .pdf。如果偵測到新的未知副檔名，則CryptoSpike會阻斷用戶。如果是允許的新應用程式，則管理員可以將其增加到白名單中。

第一個白名單是在安裝過程中自動產生的。為此CryptoSpike會自動掃描公司的所有儲存設備。

黑名單Black list：基於當前已知的勒索軟體副檔名或檔案名（大約每天更新）的清單大約有1800個（數量正在迅速增加！）。只要有新的黑名單可用就會通知客戶，他們可以點擊以接受。

學習者Learner：基於與 讀/寫/開啟/關閉檔案操作有關的用戶行為模式。為此記錄網路中的最後例如50,000筆交易。該數量可以自由設定。學習者產生的結果是"白色模式White Patterns"清單：這是允許的交易清單。

CryptoSpike還提供了"黑色模式Black Patterns"清單：這是透過追蹤例如 WannaCry與其他勒索軟體在受監控的爆發中的行為而建立的，因為該算法始終遵循相同的 開啟Open / 加密Encrypt /關閉Close操作模式。該清單可以透過客戶所遭受攻擊的模式進行補充。

為什麼學習者Learner是至關重要的組成元件

由於許多惡意程式碼不再將檔案副檔名更改為.crypto或.locky之類的副檔名，勒索軟體攻擊正變得越來越有問題。結果您將無法再確定.xls檔案是否完好無損。

為了在這種情況下偵測到攻擊，學習者Learner充當了第二個、密合性更高的安全網。例如如果未在"白色模式White Pattern"中定義的時間單位內打開檔案類型，則該算法會即時將其識別為不允許的模式，阻斷用戶並發出警報。

量身定制合適的策略

根據需要將策略組合部署。原則上策略是由上向下傳遞的，即從NetApp叢集傳遞到共享。還可以為每個NetApp SVM（儲存設備虛擬機）以及將來的每個共享等級部署不同的策略：例如，業務部具有嚴格的白名單策略以及白色模式清單，而開發人員則具有更大的靈活的黑名單策略和黑色模式清單。

警報：即時阻斷與快速復原

- FPolicy Server即時追蹤每個交易。如果偵測到異常，系統將發出警報並阻斷受攻擊的員工，以防止在NetApp儲存設備上進一步蔓延。
- 被阻斷的員工現在具有唯讀存取權限。
- CryptoSpike首先提供關鍵資訊：哪些檔案受到影響？管理員會自動接收受影響的檔案的路徑與數量的詳細資訊，並查看最近的交易。
- 如果員工被錯誤地阻斷，例如該員工是測試新應用程式的開發人員，則管理員可以立即解除對他們的阻斷，並在必要時修改模式。
- 如果是勒索軟體攻擊，管理員將分析在背景執行的惡意程式。員工可以在清理後被解除阻斷，CryptoSpike會透過一系列受影響的檔案來支援復原過程，因此可以使用Snapshot快速復原它們。

效益

✓ 透過軟體影像檔Software Image易於安裝

✓ 即時監視NetApp儲存設備中的每個交易，並立即阻斷受影響的用戶。

✓ 檢查檔案副檔名、檔名與用戶行為是否存在異常。

✓ 量身定制的監控策略，可滿足不同部門的需求。

✓ 提供發生攻擊的位置相關的即時資訊，並支援還原被損壞的檔案。

價格模式

CryptoSpike遵循分級定價模式，具體取決於NetApp 儲存設備控制器的數量與型號大小。

NetApp Compatible

NetApp Alliance Partner

Visit us on:
www.prolion.at/

詳細 產品資訊請洽 商丞科技股份有限公司 02-29148001