勒索軟體攻擊鏈

五個步驟封鎖橫向移動

勒索軟體的散播不是靠著入侵單一電腦或裝置。網路犯罪者利用這種惡意軟體變種，盡可能加密網路上的一切資料，以確保受害公司支付贖金。

據估計，

勒索軟體攻擊
今年將**每 11 秒**
發生一次且造成 **200 億美元**損失。[1]

您對現有的網路安全機制有信心嗎？

若貴公司仍然依賴舊式防火牆區隔網路，就無法阻止勒索軟體在公司網路橫向散播，鎖住重要應用程式和基礎架構。

1. **最初立足點**
   (魚叉式) 網路釣魚或漏洞服務
2. **橫向移動**
   散佈至整個網路以獲最大效果
3. **資料竊取**
   尋找並竊取寶貴的資料
4. **加密**
   PKI 搭配加密防範破解
5. **勒贖信函**
   桌布、電子郵件、勒贖 txt 檔案等
6. **影響**
   資料、財務、品牌等

入侵無可避免。

您需要一套能夠在資料中心之間橫向流量中偵測威脅，並封鎖橫向移動的安全解決方案。

阻止勒索軟體擴散

萬全準備

就靠**辨識** IT 環境中執行的每一個應用程式與資產。

預防

建立規則，以封鎖常用的勒索軟體散播手段。

偵測

接收警示，以掌握區隔的應用程式與備份資料的所有存取嘗試。

補救

在偵測到攻擊時**發動**威脅阻絕與隔離機制。

復原

使用視覺化且支援階段式復原策略的功能。

自 2018 年起，

勒索軟體攻擊已增加 350%，
而平均贖金金額更在 2020 年
增加超過 100%。[2]

如果貴公司尚未準備防範更頻繁攻擊與更高額的贖金，應盡快在防衛策略中導入網路區隔與能見度。

讓我們為您示範。

進一步瞭解

www.guardicore.com/solutions/prevent-lateral-movement

Guardicore