OPSWAT.

攻擊者使用規避技術來躲避防毒軟體的偵測，如何有效的避免規避技術對企業造成的重大威脅

惡意軟體在不斷發展，惡意軟體規避技術也在不斷發展。在熱拿亞大學進行的一項研究中，分析了 180,000 個 Windows 惡意軟體樣本來進行測試，其中多達 40%使用至少一種的規避技術。在這篇文章中，我們探討了攻擊者用來繞過防毒（AV）軟體的兩種方法。

我們分析惡意軟體行為，以了解攻擊者如何使用看似無害的 Excel 檔案來感染組織。該檔案包含一個聚集，下載描述檔並對其進行解碼以提取有效惡意負載。

VelvetSweatshop 密碼

“VelvetSweatshop”默認密碼是 2012 年首次引入的舊漏洞。它最近被用來傳播 LimeRAT 惡意軟體。網路犯罪分子之所以選擇這種策略，是因為 Microsoft Excel 能夠使用嵌入式默認密碼 VelvetSweatshop 來解密檔案，以只讀模式打開它而無需密碼，並同時運行嵌入式巨集。

通過使用 VelvetSweatshop 密碼加密的樣本中，某些防病毒掃描引擎無法偵測到惡意代碼。在我們的測試中，40 個防毒軟體中中只有 15 個發現了威脅。

受密碼保護的巨集

就像密碼保護的工作表一樣，Microsoft Excel 讓使用者鎖定 Excel 中的巨集以防止查看。但是，此功能並不會加密巨集。

當我們使用此功能隱藏樣本惡意軟體巨集時，這也使某些 AV 的偵測的效果降低。成功偵測到惡意軟體樣本的三個 AV 引擎在巨集受密碼保護時無法看到威脅。

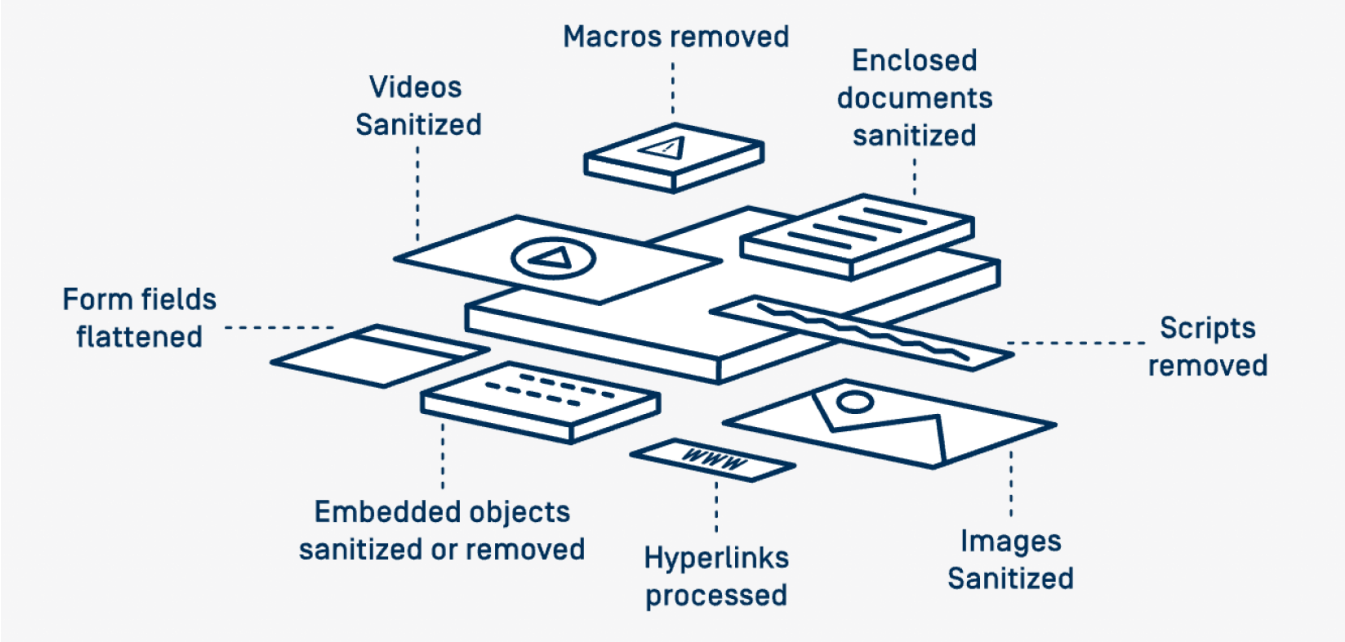
如果我們結合這兩種攻擊模式會發生什麼？

當應用 VelvetSweatshop 密碼和密碼保護的巨集功能來幫助惡意樣本檢測時，我們看到掃描結果顯著下降。40 個 AV 引擎中只有 13 個能夠檢測到威脅。

防止惡意軟體逃避技術的解決方案是什麼？

威脅行為者總是尋找新技術來隱藏他們的惡意檔案免受防病毒系統的偵測。擊敗規避惡意軟體的最佳實踐之一是禁用傳輸到系統的檔案中的所有潛在惡意物件。即使是無害的巨集也可能在以後成為漏洞。

OPSWAT 深度內容撤防和重建 （Deep CDR） 刪除檔案中的所有嵌入活動內容（包括巨集、OLE 物件、超連結等），並僅使用合法元件重建檔案。此外，Deep CDR 使您能夠在不知道密碼的情況下偵測並針對受密碼保護的巨集進行刪除。OPSWAT 的這項行業領先技術對於防止已知和未知威脅非常有效，包括零時差針對性攻擊和高級規避惡意軟體。



通過 Deep CDR 對示例進行清理後，我們現在擁有一個具有完整功能的無威脅檔案。

如果您的業務日常工作需要巨集，則使用多個 AV 同時掃描每個檔案以增加威脅檢測的機會非常重要。OPSWAT 開創了多防毒引擎掃描的概念，使用 30 個以上商業反惡意軟體引擎掃描檔案。OPSWAT 多防毒引擎掃描技術結合了各種分析機制和技術，包括特徵、啟發式偵測、AI/ML 和模擬行為模式，以較低的成本 （TCO） 最大限度地提高檢測率。

瞭解有關 OPSWAT Deep CDR 和多防毒引擎掃描的更多資訊，或與 OPSWAT 技術專家交談，以發現防止零時差攻擊和高級規避惡意軟體的最佳安全解決方案。