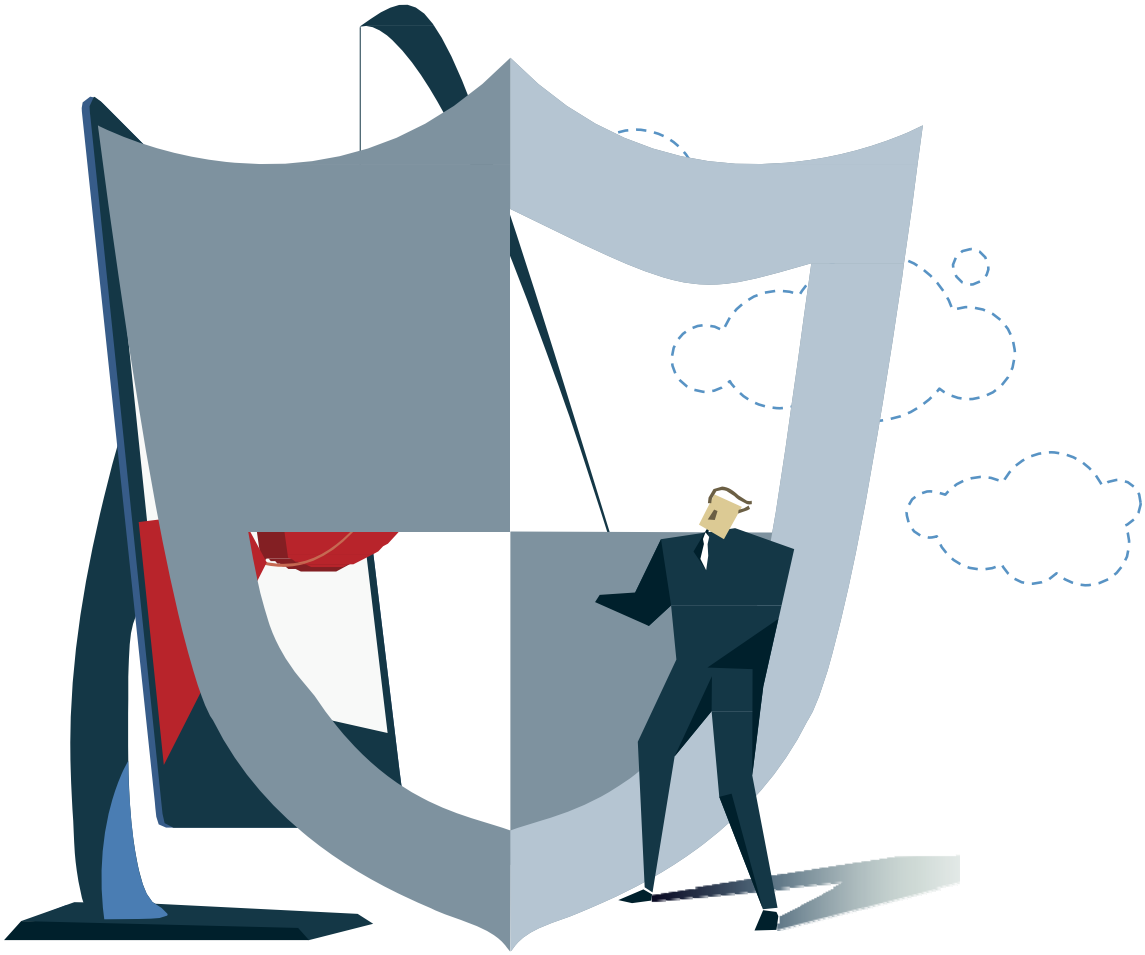
netwrix



勒索軟體保衛戰

1. 前言

Ransomware 加密勒索軟體是目前發展最快、感染率高的惡意軟體。有別於傳統的惡意程式，加密勒索軟體並不會偷你的資料，相反地，它將感染者的文件檔案進行無差別式的加密，而感染媒介通常是透過一些目標式攻擊的危險郵件。一般要求[贖金]，平均每一件勒索事件約為美金$150–$500 不等，運用難以追查來源對象的方式進行付款(如比特幣或透過一些手機系統扣款..)。公司機關內的檔案伺服器也首當其衝，加密勒索軟體會透過網路分享來擴散災情。根據網路威脅研究機構 CTA 表示，光是 CryptoWall version 3.0 這支勒索軟體，就為全球感染者造成美金$325 million 的贖金損失。

Ransomware 加密勒索軟體是如何讓受害電腦被感染呢？有三大類型的感染途徑：

1. 透過夾帶惡意軟體或感染惡意巨集程式檔案的電子郵件
2. 磁碟分享感染或其他網路惡意廣告造成
3. 因弱點被惡意程式利用而做成惡意檔案連結下載

1.1 透過夾帶惡意軟體或感染惡意巨集程式檔案的電子郵件

許多案例都是透過電子郵件附檔來傳播惡意程式，為了提高感染的成功率，攻擊方會運用社交工程手法來誘拐受害者點開郵件。因此該附加檔案通常會跟受害者能接受的真實情境有關，而檔案格式會寫成或夾帶一般常用的文件格式的字眼(如".doc" 或 ".xls"，收信者會直覺以熟悉的檔案格式來識別為哪種檔案型態。例如：某完整檔案名稱為"Paper.doc.exe"，輕忽大意的收信者就可能把該檔案看成"Paper.doc"，而沒注意到它其實是個執行檔。

某附加檔案也許是一個.doc 檔，但內容可能含有有害的巨集指令。如果有人點開這類文件，就會啟動 Office 文件中夾帶的巨集(預設微軟會自動呼叫指令來執行巨集)，接著就會自動安裝惡意程式。如果停用巨集指令的話，就會看到內容變成亂碼且出現錯誤訊息，如” Enable macro if the data encoding is incorrect."，這時若若乖乖聽話地去啟動巨集，接著就是惡意程式安裝感染的悲慘下場。

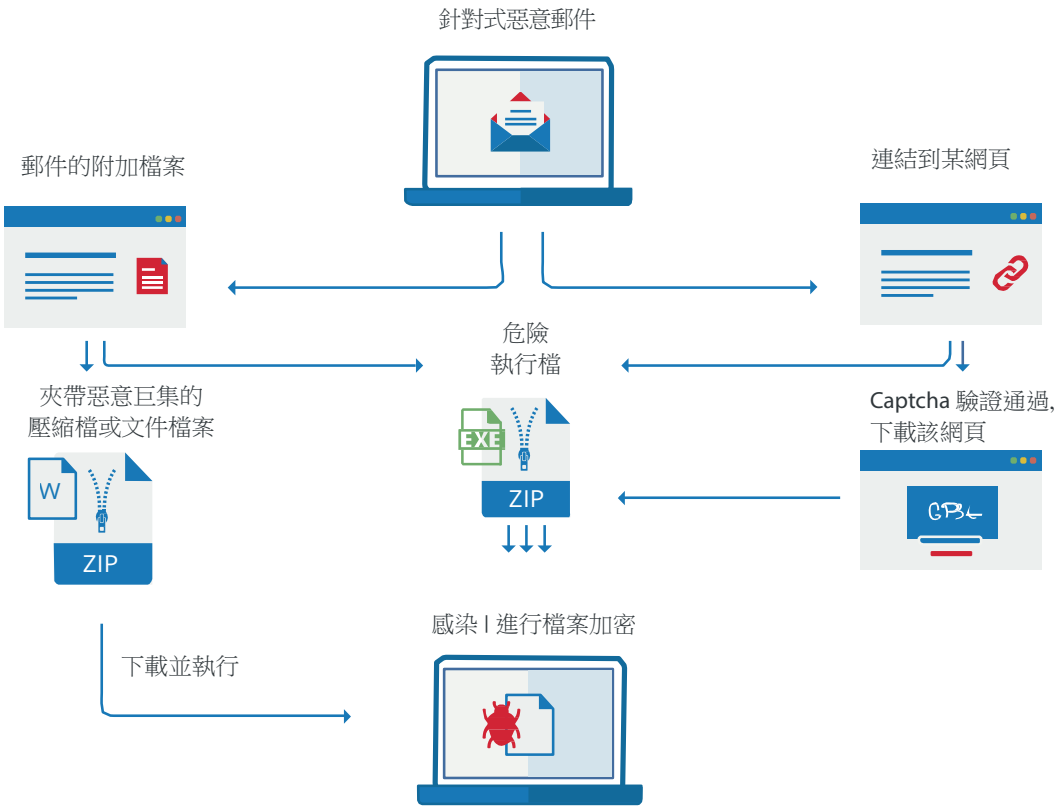


圖 1. 透過電子郵件來傳播加密勒索軟體的示意圖

1.2 磁碟分享感染或其他網路惡意廣告造成

檔案裡有惡意程式或惡意巨集，這些檔案也可能感染到磁碟。透過點擊惡意廣告啟動連結這類檔案，也有可能造成類似的感染。一旦有人點開這類檔案，加密勒索軟體就開始散播，災情開始蔓延。

1.3 因弱點被惡意程式利用而做成惡意檔案連結下載

使用者會因為不經意地瀏覽一個被掛馬的網頁，就有可能被感染加密勒索軟體。例如，透過用 Flash 製作的廣告橫幅(Banner)，瀏覽即下載惡意程式碼，再經過多次網頁重導向，最後再下載惡意軟體。若這些目標電腦都不進行漏洞修補的話，舉凡瀏覽器、應用程式、或作業系統的存在漏洞都有可能被利用來攻擊。

例如，CryptoWall 就利用 Angler、Neutrino、Nuclear 等漏洞攻擊套件，針對其鎖定的網頁瀏覽器、Java、PDFs、Flash 所存在的漏洞來進行感染。

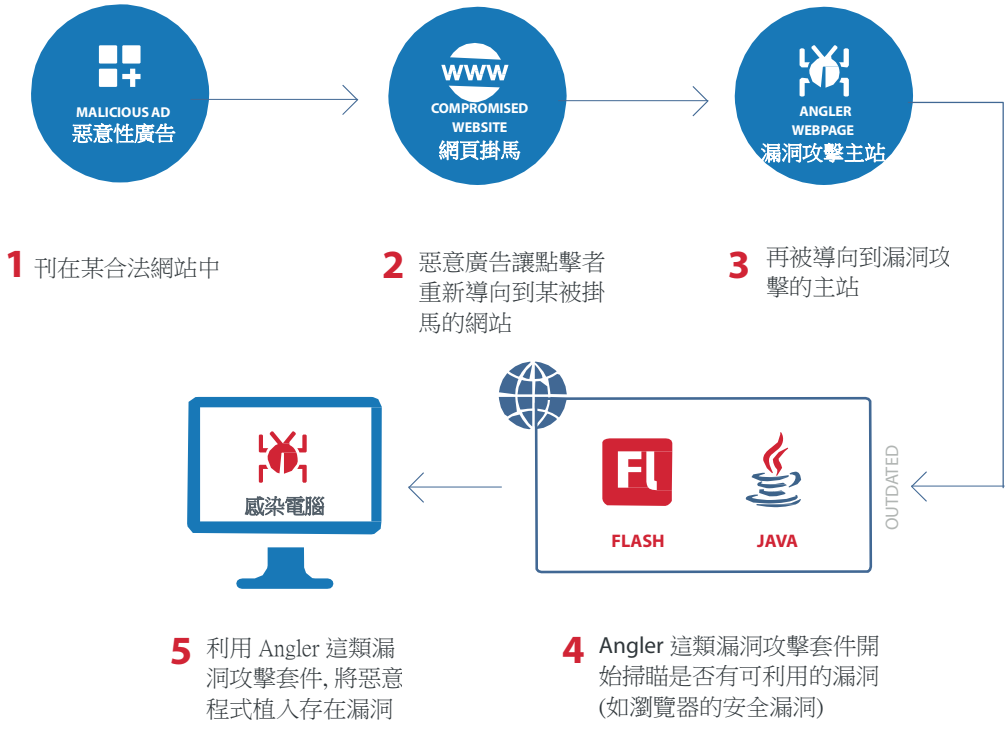


圖 2.如何運用網頁重導向及軟體漏洞來進行感染

2. Ransomware 加密勒索軟體感染步驟

Rransomware 加密勒索軟體的典型感染步驟如下:

1. 滲透入侵

一旦開啟惡意郵件的附加檔案或瀏覽網頁掛馬的網站，就成為 Rransomware 加密勒索軟體的感染者。

2. 安裝加密勒索軟體

惡意軟體就會”自體繁殖”從感染電腦開始複製到更多地方，例如利用下列語法:

- <%appdata%>
- <%startup%>
- <%rootdrive%>/random_folder/
- 某個帶有隨機名稱的 %WINDOWS%目錄名稱，例如 “%WINDOWS%\ycizilys.exe”

然後會編寫註冊檔，讓所有系統重開機後惡意程式會自動啟動。

3. 產生加密金鑰

Ransomware 的感染電腦端會跟遠端的 C&C server 建立 SSL 加密通訊連線，同時產生一組公鑰+私鑰來對感染檔案進行加密。感染電腦端可能會使用類似 Tor network(可隱藏 IP 的匿名網路)去匿名連線，藉此干擾後續的追查。有些加密勒索軟體會產生一組金鑰並存放在被感染的電腦中，這種情形下就不須對外連線來進行檔案加密。

加密勒索軟體會使用很強的加密模式(如 RSA-2048)，這樣可避免人們破解而進行檔案解密。

4. 資料加密

本階段會使用受害者的存取權限，加密勒索軟體會對能存取得到的實體及雲端磁碟中檔案進行加密。

5. 勒索要錢

加密勒索軟體接著顯示一些指示資訊，告知受害者要如何付錢了事(檔案解密)的方法及步驟。

3. 立馬上手的最佳管理實務

透過分析加密勒索軟體攻擊手法報告，我們發現導致攻擊成功的原因如下：

- 系統防護太薄弱
- 員工資安意識不夠強，或需要資安宣導、相關教育訓練，讓他們開信或瀏覽網頁時要更謹慎，不要輕易去點擊
- 組織使用過時/無更新的軟體，存在一些會被利用的系統漏洞

將這些被加密檔案進行全部解密，也許要經歷一段很長的時間(如果有機會解密復原的話，也許幾個月、甚至長達一年以上)。因此，更重要的是必須採取避免被感染的步驟，及準備檔案備份以進行復原之用。
一些關鍵實務如下：

- 經常性備份你系統中的檔案，並將這些備份進行離線保存。若組織內發生加密勒索軟體的危害事件時，你可輕鬆地運用備份檔案來進行還原。若要進階保護這些備份資料的話，建議可考慮為這些資料加密、放在與內部網路不同的存放位置。
- 適當地設定分享資料夾的存取權限。若你使用分享網路資料夾，請針對每一位使用者建立單一的網路分享。若不小心有加密勒索軟體進到組織內，當惡意軟體用受害者的存取權限來進行散播時，儘量讓感染範圍限縮到最小範圍。若不這樣做，全面套用分享權限給每一個人，就會快速將所有檔案都被勒索軟體加密。
- 儘量限制使用者存取權限為”Read”，沒有了”完全控制”的權限，加密勒索軟體就無法對檔案進行存取加密。
- 將你的作業系統、軟體更新到最新版本，安裝最新的修補程式。尤其要隨時留意：Adobe Flash、Microsoft Silverlight、 web browsers 是否更新到最新版本。
- 適當地設定群組原則：
    - 封鎖從網路連內來執行 Office 文件中的巨集指令
    - 封鎖執行檔。可運用軟體限制原則(Software Restriction Policy)來避免執行這些危險檔案，該原則會封鎖執行嘗試啟用檔案的語法，包含解壓縮。
    - 封鎖自動播放(AutoPlay)，停用從可攜式儲存媒體中自動執行軟體
    - 運用是否允許執行軟體的黑白名單，做為應用程式管控的群組原則(Application Control Group Policy)。
- 將一些匿名網路 IP 位址列入黑名單，有些惡意軟體會使用匿名網路(Tor network)來連接到外部的 C&C server(command-and-control server)。封鎖這些 IP，有助於避免安裝 Ransomware。

- 適當地設定你的網頁過濾機制(web filter)、防火牆、防毒軟體，有助於封鎖連線到一些惡意性網站，及下載檔案前先進行掃毒。
- 教育你的員工，讓他們瞭解如何留意一些釣魚郵件。幫助他們學會辨別檔案格式，尤其要留意一般惡意軟體常利用的檔案格式，包含.exe,.com, .js, .wbs, .hta, .bat , .cmd.等
- 預設成以記事簿來開啟JS 檔案內容，這將有助於避免使用 JavaScript 來危害的惡意軟體。

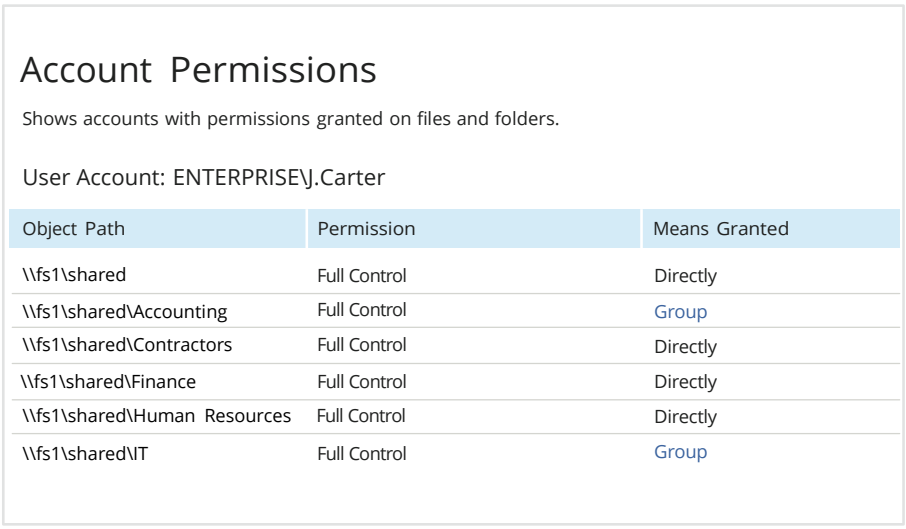
4. 如何運用 Netwrix Auditor 來降低 Ransomware 加密勒索軟體的危害

要對抗 Rransomware 加密勒索軟體，建置多層次的安全防護機制是最有效方法，能避免企業組織因這類災害而造成營運中斷、財務損失、有損商譽。

Netwrix Auditor 能協助您降低因惡意軟體感染擴散內部網路所造成的風險，偵測出惡意軟體進行攻擊的活動記錄，將有助於減少災害範圍，迅速回復損害的檔案。

4.1 建立並實施最小特權的模式

- 定期檢視使用者帳戶的存取權限(如透過 Netwrix 下例報表)，以確保每個帳戶被授予的權限的確跟他的職務角色有相符合，同時要確認不要有存取權限是授予給"Everyone"的情形。若發生惡意軟體感染事件，事後可運用該報表去確認因受害使用者而感染到哪些檔案，可瞭解整體感染範圍。



Account Permissions

Shows accounts with permissions granted on files and folders.

User Account: ENTERPRISE\J.Carter

Object Path	Permission	Means Granted
\\fs1\shared	Full Control	Directly
\\fs1\shared\Accounting	Full Control	Group
\\fs1\shared\Contractors	Full Control	Directly
\\fs1\shared\Finance	Full Control	Directly
\\fs1\shared\Human Resources	Full Control	Directly
\\fs1\shared\IT	Full Control	Group

- 檢視誰有權限存取到某些重要檔案或資料夾，運用 Netwrix 下例報表，可協助管理者基於資料保護及組織營運的需要，而評估這些權限分配的適切性。

Object Permissions by Object

Shows file and folder permissions granted to accounts, grouped by object path.

Object: \\fs1\shared\Finance (Permissions: Different from parent)

Account	Permissions	Means Granted
ENTERPRISE\A.Kowalski	Full Control	Group
ENTERPRISE\A.Watson	Full Control	Group
ENTERPRISE\Administrator	Full Control	Group
ENTERPRISE\G.Brown	Full Control	Group
ENTERPRISE\J.Carter	Full Control	Directly
ENTERPRISE\P.Anderson	Full Control	Group
ENTERPRISE\T.Simpson	Full Control	Directly
fs1\Administrator	Full Control	Group

- 檢視有檔案/資料夾存取權限的使用者帳戶，從他的存取次數來瞭解是否經常使用檔案，也能瞭解其權限是否是源自群組設定。若有些權限設定過大、或為不必要的授權，為避免攻擊發生因而擴大感染範圍，可評估縮小權限範圍。

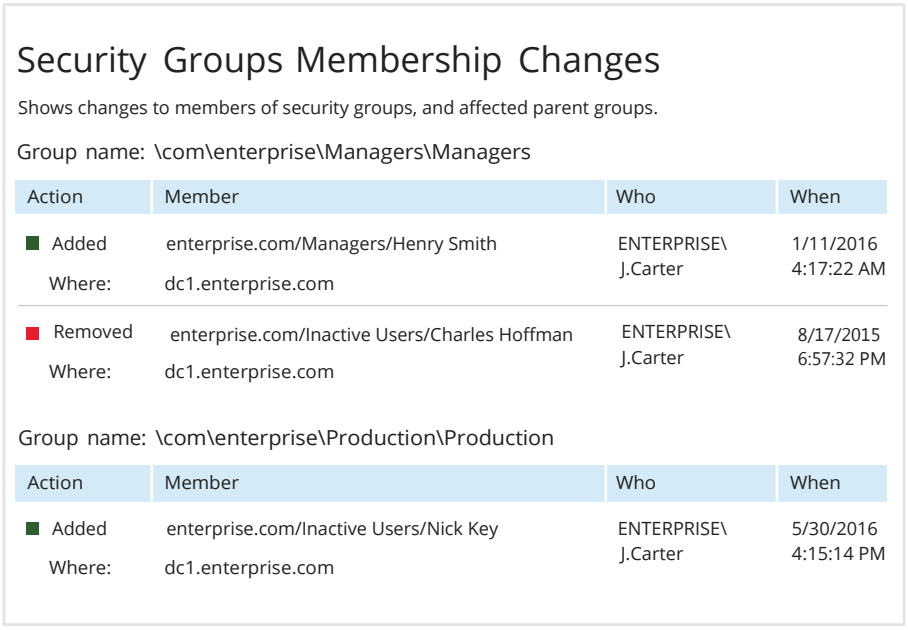
Excessive Access Permissions

Shows accounts with permissions for infrequently accessed files and folders.

Object: \\fs1\shared (Permissions: Different from parent)

Account	Permissions	Means Granted	Times Accessed
ENTERPRISE\A.Watson	Full Control	Group	0
ENTERPRISE\Administrator	Full Control	Group	0
ENTERPRISE\B.Atkins	Full Control	Directly	0
ENTERPRISE\D.Galaher	Full Control	Group	0
ENTERPRISE\G.Molls	Write and list folder contents	Directly	0

- 持續檢視權限設定是否有異動(包含安全群組成員的變動)，透過下例報表就能即時發現這些變動，若有不合適的存取權限分派也可即早矯正。



Security Groups Membership Changes

Shows changes to members of security groups, and affected parent groups.

Group name: \com\enterprise\Managers\Managers

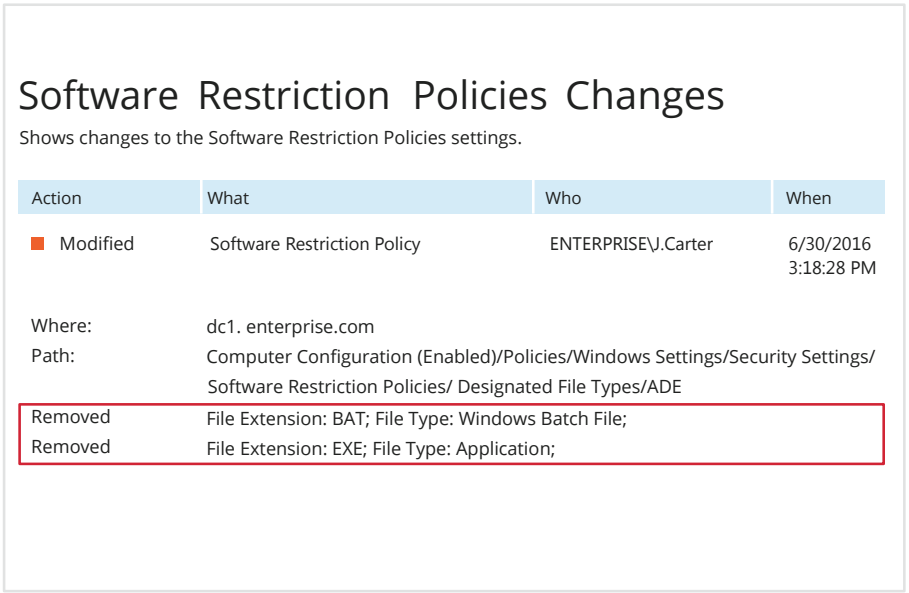
Action	Member	Who	When
Added Where:	enterprise.com/Managers/Henry Smith dc1.enterprise.com	ENTERPRISE\ J.Carter	1/11/2016 4:17:22 AM
Removed Where:	enterprise.com/Inactive Users/Charles Hoffman dc1.enterprise.com	ENTERPRISE\ J.Carter	8/17/2015 6:57:32 PM

Group name: \com\enterprise\Production\Production

Action	Member	Who	When
Added Where:	enterprise.com/Inactive Users/Nick Key dc1.enterprise.com	ENTERPRISE\ J.Carter	5/30/2016 4:15:14 PM

4.2 控制內部允許安裝哪些應用程式

- 透過監看群組原則 GPO 的變動，包含軟體限制原則設定(Software Restriction Policy settings)，透過下例報表就能即時發現可安裝軟體的白名單是否有異動，即早發現異常以防範事態擴大而更嚴重。

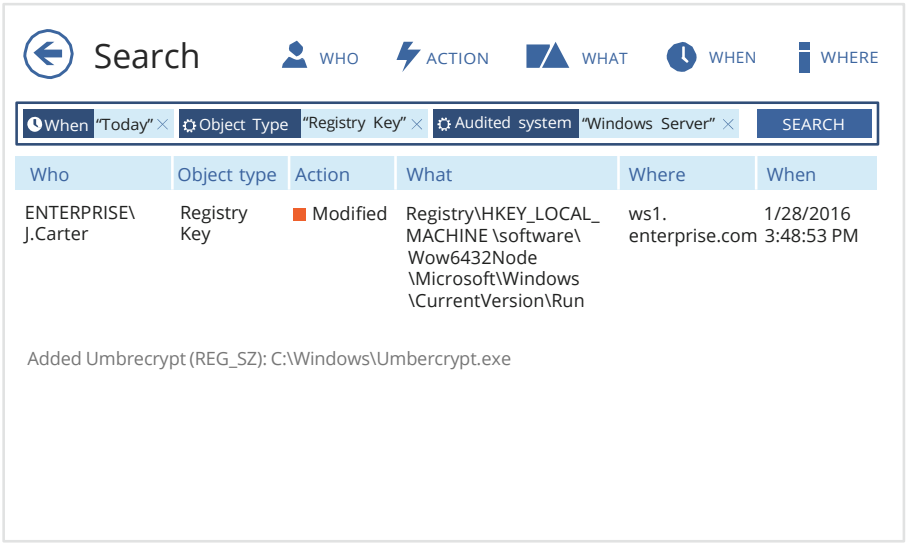


Software Restriction Policies Changes

Shows changes to the Software Restriction Policies settings.

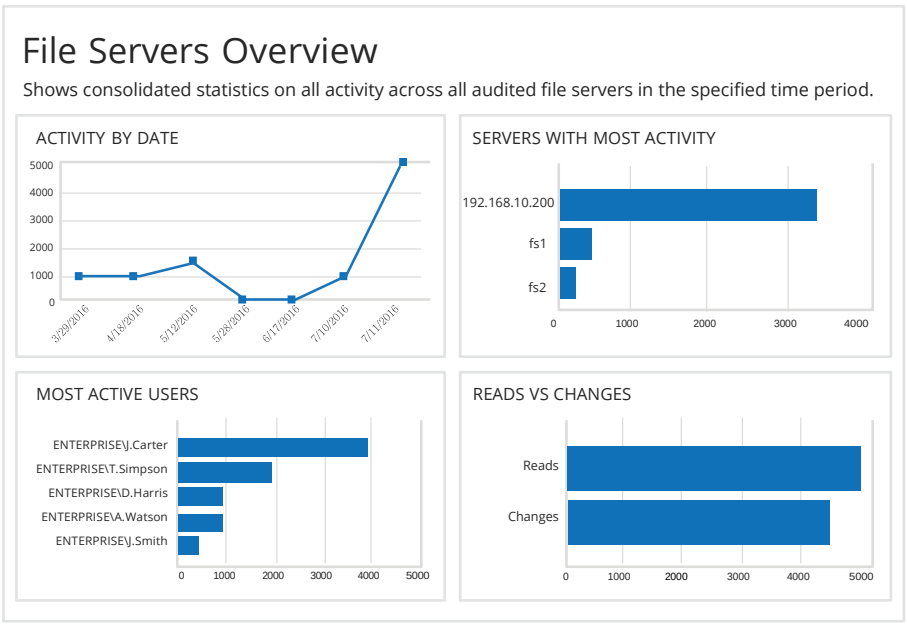
Action	What	Who	When
Modified	Software Restriction Policy	ENTERPRISE\J.Carter	6/30/2016 3:18:28 PM
Where:	dc1. enterprise.com		
Path:	Computer Configuration (Enabled)/Policies/Windows Settings/Security Settings/ Software Restriction Policies/ Designated File Types/ADE		
Removed	File Extension: BAT; File Type: Windows Batch File;		
Removed	File Extension: EXE; File Type: Application;		

- 檢視 Windows 註冊啟用金鑰的變動(Windows registry startup keys)，要特別留意這些執行金鑰的設定，如果加密勒索軟體已經變更這些設定，透過 Netwrix 下例報表就能發現這些變動，會顯示這些危險執行檔的路徑，以利於進行軟體移除及修復作



4.3 偵測攻擊活動並找出是誰造成加密勒索軟體這場災難

- 偵測是否有異常頻繁的使用者存取檔案，尤其是監看檔案分享的資料夾及檔案伺服器的使用活動，若發現異常的大量存取，藉由 Netwrix 的存取活動統計儀表板及展開多款存取稽核報表來進行追查。



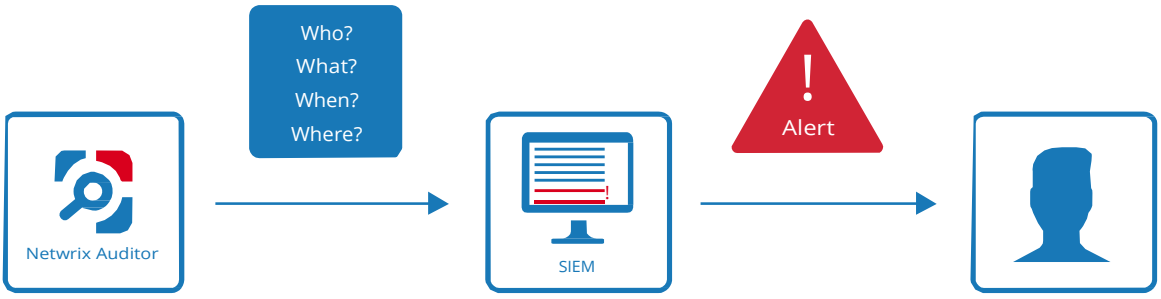
- 訂閱基於門檻值進行統計的檔案存取活動報表，無論是否有展現出與加密勒索軟體的確切操作活動，也會顯示出一些相關活動徵兆，例如在極短時間內產生非常大量的檔案讀取、修改等活動。

User Activity Summary

Shows the most active users. Use this report to detect suspicious user activity such as high numbers of failed access attempts or file reads.

Who	Changes	Reads	Failed Attempts	Deletions
ENTERPRISE\J.Carter	1502	1502	867	1490
ENTERPRISE\MEA_FS	0	0	56	0
ENTERPRISE\T.Simpson	38	9	3	3
NT AUTHORITY\SYSTEM	0	2	0	0
system	9	0	0	0

- 針對疑似與加密勒索軟體感染所產生的活動，運用 Netwrix 與 SIEM 設備的整合可設定發送警示通知。



4.4 優化資料回復流程

- 運用 Netwrix 下例報表，可知道被感染而刪除的檔案一覽表，並藉以從備份檔案中進行回復，將會更有效率地進行災難回復。

Files and Folders Deleted

Shows removed files and folders with their attributes.

Action	Object Type	What	Who	When
Removed Where: fs1	File	\\fs1\shared\Finance2016\bills.rtf	ENTERPRISE\J.Carter	7/18/2016 5:02:02 PM
Removed Where: fs1	File	\\fs1\shared\Finance2016\cache_11_10_15.rtf	ENTERPRISE\J.Carter	7/18/2016 5:02:03 PM
Removed Where: fs1	File	\\fs1\shared\Finance2016\Budget.xlsx	ENTERPRISE\J.Carter	7/18/2016 5:02:04 PM
Removed Where: fs1	File	\\fs1\shared\Human Resources\users.csv	ENTERPRISE\J.Carter	7/18/2016 5:02:05 PM

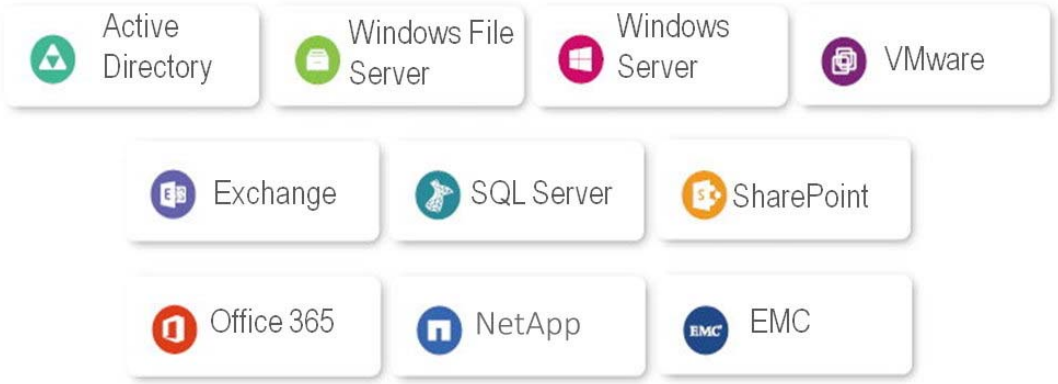
5. About Netwrix Auditor

Netwrix Auditor 是系統設定變更暨存取記錄稽核的全球領先品牌，公司於 2006 年於美國成立，歷年來產品獲得多項國際認證及獎項，性價比佳。全球有數千家客戶，包含各產業的領先業者。

可監看 Windows 重要伺服器(如 AD 網域伺服器及 Windows 檔案伺服器...等)的設定變更及存取稽核，偵測是否有產生資安風險或系統穩定性的重要設定變動及存取活動，提供報表及即時警示通知。

Netwrix 稽核記錄支持長期歸檔保存，提供多款法規遵循報表，可流暢地進行**合規性稽核**、**強化安全**、發生問題時能**簡化根本原因分析**，有助於迅速找出肇因並解決問題。

Netwrix Auditor **稽核範圍廣泛**，涵蓋多樣化重要系統及應用程式：



- **保護機敏資料，防範資料外洩**
- **偵測可疑存取及權限異動**
- **提供系統快照，快速回復設定屬性**
- **數百款稽核報表(符合資安法規標準，如 ISO27001)**
- **Event log、操作活動側錄 全程稽核**

台灣區銷售代理

Softnext 中華數位科技

www.softnext.com.tw
服務電話:02-25422526