保安資訊--本周(台灣時間2022/06/10)賽門鐵克原廠防護公告重點說明

前言

賽門鐵克原廠首要任務就是保護我們的顧客，被譽為賽門鐵克解決方案專家的保安資訊更能發揮我們被高度認可的專業知識與技能、豐富經驗以及專為幫助客戶成功的服務熱忱，與顧客共同創造賽門鐵克解決方案的最大效益，並落實最佳實務的安全防護。攻擊者從不休息，我們更不會。一支技術精湛且敬業的團隊不斷創造新的防護措施，以應對每天發布成千上萬的新威脅。儘管不可能詳述我們已經可以防禦的每種新威脅，但該站點至少反映了我們的努力。這些公告分享針對當前熱門新聞話題有關威脅的保護更新，確保您已知道自己受到最佳的保護。點擊此處獲取賽門鐵克原廠防護公告(Protection Bulletins)。

關於 保安資訊有限公司 | 從協助顧客簡單使用賽門鐵克方案開始，到滿足顧客需求更超越顧客期望的價值。

在端點啟用賽門鐵克入侵預防系統(IPS) 的好處(以下皆為美國時間)

賽門鐵克的入侵預防系統 (IPS) 是業界一流的深層封包檢測技術引擎，可保護包括財富 500 強企業和消費者在內的數億個端點(桌機／筆電／伺服主機)。

過去的 7 天內，SEP 的網路層保護引擎 (IPS) 在 110 萬個受保護端點上總共阻止了1.947億次攻擊。這些攻擊中有 95% 在感染階段前就被有效阻止：**(2022/06/06)**

- 在**21萬700**台端點上，阻止了**9,680萬**次嘗試掃描**Web**服務器的漏洞。
- 在**42萬3,400**台端點上，阻止了**3,760萬**次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**7萬6,600**台**Windows**伺服主機上，阻止了**2,130萬**次攻擊。
- 在**15萬900**端點上，阻止了**970萬**次嘗試掃描伺服器漏洞。
- 在**8萬2,300**台端點上，阻止了**400萬**次嘗試掃描在**CMS**漏洞。
- 在**11萬9,000**台端點上，阻止了**380萬**次嘗試利用的應用程式漏洞。
- 在**34萬2,200**台端點上，阻止了**860萬**次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**550**台端點上，阻止了**340萬**次加密貨幣挖礦攻擊。
- 在**11萬2,700**台端點上，阻止了**590萬**次向惡意軟體**C&C**連線的嘗試。
- 在**8,000**台端點上，阻止了**25萬5,200**次加密勒索嘗試。

強烈建議用戶在桌機／筆電／伺服主機上啟用 IPS (不要只把SEP/SES當一般的掃毒工具用，它有多個超強的主被動安全引擎，在安全配置正確下，駭客會知難而退)，以獲得最佳保護。點擊此處獲取有關啟用 IPS 的說明，或與保安資訊聯繫可獲得最快最有效的協助。

2022/06/09

對 VMware ESXi 伺服器窮追不捨的 Black Basta (*黑巴斯塔) 勒索軟體

據報導，Black Basta 是另一個針對 VMware ESXi 伺服器的加密勒索軟體變種。惡意軟體的二進位檔案搜索 ESXi 伺服器上儲存虛擬機器檔的 /vmfs/volumes 目錄。該勒索軟體將 .basta 副檔名新增到被加密檔案中，並以 readme.txt 檔的形式發佈勒索說明，提示用戶連到一個 .onion 的暗網網站以獲得進一步指示。

賽門鐵克已經於第一時間提供多種有效保護(SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.Basta
- Ransom.Basta!gm
- WS.SecurityRisk.4

2022/06/08

SVCReady 載入程式被濫用於散佈 RedLine 竊密程式的攻擊行動中

一種被稱為 SVCReady 全新載入程式正被濫用來散佈惡意 Word 檔有關的網路釣魚攻擊。據報導，SVCReady 利用一種特殊的技術來載入惡意軟體的有效籌載。雖然許多惡意文件檔只是使用惡意巨集下載有效籌載，但這裡的惡意軟體使用 VBA 巨集程式碼執行隱藏在檔案中的 Shellcode。最近一次使用 SVCReady 的行動中，Redline 竊密程式被作為有效籌載植入被攻擊的系統中。

賽門鐵克已經於第一時間提供多種有效保護(SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

檔案型(基於回應式樣本的病毒定義檔)防護：

- ISB.Downloader!gen177
- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- W97M.Downloader
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.B
- Heur.AdvML.C
- Heur.AdvML.M

基於網頁防護(如果您有使用WSS--地端或雲端網頁分類／過濾／安全服務)：

被發現的惡意網域名稱已於第一時間收錄於不安全分類列表中。

2022/06/08

攻擊者利用 MSDT Follina 漏洞來傳播惡意軟體

博通軟體事業部的企業安全部門--賽門鐵克，觀察到威脅者利用被稱為 Follina (CVE-2022-30190) 遠端程式碼執行 (RCE) 漏洞，將惡意軟體植入到易受攻擊的脆弱系統上。多個攻擊者在漏洞利用得逞後的最後階段使用各種有效籌載。在其中一個例子中，賽門鐵克觀察到攻擊者部署了被稱為 AsyncRAT 的遠端存取木馬。在另一個例子中，攻擊者部署了一個竊密程式，目標是 Firefox、Chrome 和 Edge 等網路瀏覽器 cookies 和儲存的登錄資料。

在我們部落格有更多詳細資訊--攻擊者利用 MSDT Follina 漏洞注入遠端存木馬、竊密程式

賽門鐵克已經於第一時間提供多種有效保護(SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Backdoor.ASync
- Downloader
- Infostealer

網路層防護：

我們的 Webpulse (網頁脈衝) 網頁自動回饋框架以及其他先進的網路層防護技術，已將其列為如下分類的網頁型攻擊：

- Web Attack: MSDT Remote Code Execution CVE-2022-30190

基於安全強化政策(適用於使用DCS)：

DCS 預設政策就有針對 MS Office 應用程式特別作安全強化。DCS 防止 MS Office 應用程式啟動命令解譯器，包括 cmd.exe、powerhell.exe 和其他子程序。此外，對於這個編號的漏洞，可以透過將 *\msdt.exe 新增到沙箱執行控制 "Microsoft Office不可執行的程式" 中來防止遠端程式碼執行漏洞。

2022/06/07

YourCyanide-- 一種基於 cmd 的勒索軟體

YourCyanide 是類似 GonnaCope、Kekpop 或 Kekware……等，基於 cmd 勒索軟體變種的後繼版本。據報導，這種最新的惡意軟體透過包含 Powershell 腳本的 .lnk 檔案傳播，來傳遞勒索軟體的有效籌載。該勒索軟體被認為仍在積極開發中，因為它的最新版本目前沒有實際加密任何東西--它們只是重命名所選磁碟目錄中的檔案。YourCyanide 還可以從受感染的電腦上收集使用者的機密資料。為了竊取這些資料，惡意軟體利用 Telegram 聊天機器人 API。

賽門鐵克已經於第一時間提供多種有效保護(SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Downloader
- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- PasswordRevealer
- WS.Malware.1

基於行為偵測技術(Snoar)的防護：

- SONAR.SuspBeh!gen650

基於機器學習的防禦技術：

- Heur.AdvML.C

2022/06/06

Ginzo (又名Zingo) --不法竊密程式惡意活動繼續活躍

今年初，一個名為 Ginzo (又稱Zingo) 的竊密程式被觀察到在網路上到處流竄，至今有越來越多的行跡被發現，特別是由於它最初是在駭客論壇、網站和 Telegram 上免費提供。從功力來看，它就是一支普通的竊密程式，目標是各種密碼、Discord 權杖和加密錢包。它還能夠下載其他二進位檔案、竊取檔案和系統資訊。最近的活動顯示，威脅者主要利用瀏覽網頁時順道下載作為感染的媒介，並且主要針對消費者。

賽門鐵克已經於第一時間提供多種有效保護(SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

郵件安全防護機制：

不管是地端自建 (SMG／SMSEX) 的郵件過濾／安全閘道及主機防護、雲端郵件安全服務 (E-mail Security.Cloud) 以及郵件威脅隔離 (ETI)，都能提供終端用戶隔絕或隔離威脅於境外的保護 (威脅不落地)。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan Horse

基於機器學習的防禦技術：

- Heur.AdvML.B

網路層防護：

我們的 Webpulse (網頁脈衝) 網頁自動回饋框架以及其他先進的網路層防護技術，已將其列為如下分類的網頁型攻擊：

- System Infected: Trojan.Backdoor Activity 634

2022/06/06

惡意軟體 Qakbot 在最新的行動中使用 LNK 和 XLTM

惡名昭彰的 Qakbot 銀行惡意軟體沒有任何停止的跡象，因為賽門鐵克繼續觀察反復出現的行動。多年來，Qakbot 垃圾郵件行動的幕後主謀已經迴圈使用攻擊鏈技術手冊，有時還包括新技術。最近幾天，有兩個不同的行動，其中惡意的 XLTM 和 LNK 檔被用來作為下載惡意二進位檔案的一種手段。

賽門鐵克已經於第一時間提供多種有效保護(SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

郵件安全防護機制：

不管是地端自建 (SMG／SMSEX) 的郵件過濾／安全閘道及主機防護、雲端郵件安全服務 (E-mail Security.Cloud) 以及郵件威脅隔離 (ETI)，都能提供終端用戶隔絕或隔離威脅於境外的保護 (威脅不落地)。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Downloader
- ISB.Downloader!gen347
- Trojan Horse
- XLM.Downloader!gen1
- XLM.Downloader!gen2

基於機器學習的防禦技術：

- Heur.AdvML.B