保安資訊--本周(台灣時間2023/05/05)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 75 萬 9,000 台受保護端點上總共阻止了 8,850 萬次攻擊。這些攻擊中有 91% 在感染階段前就被有效阻止：**(2023/05/01)**

- 在**14萬6,100**台端點上，阻止了**3,720**萬次嘗試掃描**Web**服務器的漏洞。
- 在**26萬300**台端點上，阻止了**1,810**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**5萬2,300**台**Windows**伺服主機上，阻止了**1,390**萬次攻擊。
- 在**7萬9,600**台端點上，阻止了**240**萬次嘗試掃描伺服器漏洞。
- 在**1萬6,000**台端點上，阻止了**91萬7,100**次嘗試掃描在**CMS**漏洞。
- 在**5萬8,800**台端點上，阻止了**190**萬次嘗試利用的應用程式漏洞。
- 在**26萬4,200**台端點上，阻止了**500**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**1萬8,800**台端點上，阻止了**290**萬次加密貨幣挖礦攻擊。
- 在**15萬8,200**台端點上，阻止了**1,080**萬次向惡意軟體**C&C**連線的嘗試。
- 在**2,400**台端點上，阻止了**9萬5,900**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。

2023/05/04

Earth Longzhi進階持續威脅(APT)駭客組織持續不斷進化其攻擊媒介(Attack Vector)

Earth Longzhi 進階持續威脅 (APT) 駭客組織仍然保持活躍並持續不斷進化其攻擊媒介 (Attack Vector)。最近針對亞太地區發動攻擊行動中，攻擊者利用熱門網頁開發程式語言所撰寫的小程式 (web shell)--Behinder 來攻擊 Microsoft IIS 和 Exchange Server ，該 web shell 進一步用來佈署 Cobalt Strike Beacon (信標：CroxLoader) 和使用遭感染電腦上惡意 DLL 側載 (DLL Side-loading) 工具來停用安全軟體。DLL 側載是攻擊者慣用伎倆，利用 Windows 掛載合法應用程序所需的 DLL 必要機制風險。對於上述攻擊行動，攻擊者濫用 Windows Defender 安全軟體來啟動其惡意 DLL 檔。

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：

基於行為偵測技術(SONAR)的防護：

- SONAR.TCP!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan Horse
- Trojan.Gen.MBT

基於機器學習的防禦技術：

- Heur.AdvML.A
- Heur.AdvML.B

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／IP位址已於第一時間收錄於不安全分類列表中。

2023/05/03

SQL Server用戶請注意--CLR SqlShell惡意軟體攻擊MS-SQL伺服器日益增多

據觀察，CLR SqlShell (CLR為common Language Runtime) 惡意軟體日益被濫用於攻擊 MS-SQL 伺服器。攻擊者正在濫用允許在 MS-SQL 環境中管理和執行程式碼的 CLR 儲存功能。CLR SqlShell 惡意軟體主要用於初始攻擊階段，以執行攻擊者的指令並下載額外的有效籌載。最近採用 SqlShell 的某些攻擊後續造成 Trigona 勒索軟體、MRBMiner、MyKings 或 LoveMiner 等惡意挖礦軟體的傳播，但攻擊者也可能使用類似的攻擊鏈部署許多其他各種惡意軟體、後門或惡意代理軟體。

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.Trojan
- Trojan Horse
- Trojan.Gen

- Trojan.Gen.2
- Trojan.Gen.MBT
- WS.Malware.2

基於安全強化政策(適用於使用DCS)：

賽門鐵克重要主機防護系統：DCS(data Center Security) 能有效針對 MS-SQL 伺服器 CLR SqlShell 攻擊提供零時差保護：

- DCS 內建 SQL 伺服器沙箱環境 (最小權限、最低資源) 可以限縮內部受信任用戶的過多權限存取，防止攻擊者透過暴力或字典攻擊獲得內部人員初始的存取權限之後續危害。還可以增加額外 DCS 規則來偵測 (Detect)／稽核 (Audit) 任意或意外的入埠連線，以增強安全性。
- DCS 阻止 SQL 伺服器啟動命令模式，包括 cmd.exe、powershell.exe 和其他作為子程序。DCS 強化策略還能阻止將任何其他惡意有效負載下載到伺服器上。

更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。

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／IP位址已於第一時間收錄於不安全分類列表中。

2023/05/02

DangerousPassword／SnatchCrypto網路攻擊行動也開始針對macOS

DangerousPassword (又名 SnatchCrypto 或 CryptoCore) 是駭客集團 BlueNoroff (也與惡名昭彰的北韓 Lazarus 駭客集團有關聯) 的長期行動。該攻擊行動出於經濟動機，鎖定在盜取加密貨幣。已知該駭客集團在其攻擊中採用各種感染媒介，諸如：利用 Windows 捷徑檔、MS Office 檔案、.chm 或 OneNote 等類型的檔案。最近觀察到攻擊行動還針對 macOS 平台，並使用惡意 .pdf 檔和惡意 PDF 閱讀器程式。該發行版中的最終有效籌載是一種稱為 RustBucket 基於 Rust 的惡意軟體，一旦執行，它將幫助攻擊者對目標系統進行預期性的破壞。

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：

- CL.Downloader!gen195
- OSX.Trojan.Gen
- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.NPE
- Trojan.Pidief
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.C

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／IP位址已於第一時間收錄於不安全分類列表中。

2023/05/01

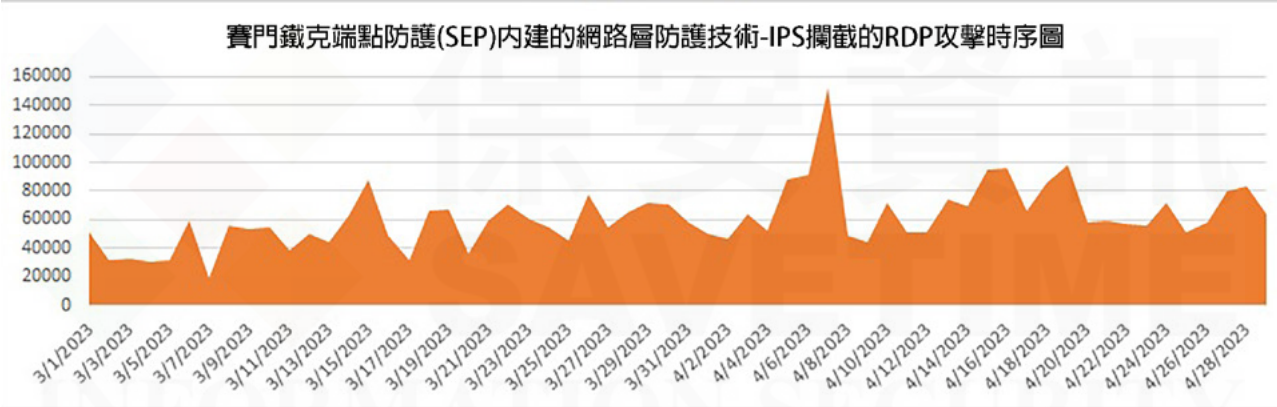
防護亮點：SEP的網路層防護技術--IPS有效防護RDP攻擊

～防護亮點～

遠端桌面通訊協定 (Remote Desktop Protocol-RDP) 是 Microsoft Windows 的一項功能，可提供遠端存取。遠端工作人員使用它連接到實際位於其辦公室的電腦，而 IT 專家可以使用它來修復來自世界各地的使用者的電腦。它在 COVID-19 疫情爆發之前就已經很流行，但自從疫情爆發後，大量企業員工突然需要居家辦公，RDP 連線的使用呈指數性成長。不幸的是，它對那些懷有惡意的人來說同樣方便，並且駭客不斷進行 RDP 攻擊以存取和入侵企業網路。

RDP 攻擊是一種網路攻擊，它試圖使用 RDP 協議存取遠端電腦。這些攻擊是駭客利用不安全系統、面向公眾網路的暴險服務和易受攻擊的網路端點一種非常熱門手法。成功的 RDP 攻擊可能允許攻擊者獲取憑證、執行惡意程式碼，甚至讓他們完全控制目標系統。

賽門鐵克每週攔截超過數十萬次 RDP 攻擊。



令人擔憂的是，RDP 攻擊正越來越被網路犯罪分子和國家級駭客用來發動勒索軟體攻擊。透過 RDP 存取受害者的電腦，攻擊者可以安裝勒索軟體來加密受害者的檔案並要求支付解密密鑰的費用。

攻擊者使用多種工具和伎倆來發動 RDP 攻擊：

* 掃描工具：攻擊者可能會使用掃描工具來搜索連接到網際網路且容易受到攻擊的 RDP 伺服器。這些工具可以幫助攻擊者識別 RDP 攻擊的潛在目標。
* 暴力破解工具：暴力破解工具用於透過多種不同的組合來試圖破解密碼，直到找到正確的組合。攻擊者可以使用這些工具來嘗試存取受弱密碼或易猜密碼狀態的 RDP 連接。
* 漏洞利用工具包：這些是用於識別和利用軟體漏洞的工具和漏洞利用的軟體包。一些漏洞利用工具包專門針對 RDP 漏洞而設計。
* 憑證竊取惡意軟體：攻擊者可能會使用目的在從受害者電腦竊取登錄憑證的惡意軟體。這種類型的惡意軟體可用於竊取 RDP 登錄憑證及儲存在受害者電腦上的其他登錄憑證。
* 社交工程：攻擊者可能會使用網路釣魚電子郵件等社交工程伎倆來誘騙受害者洩露其登錄憑證或下載可用於執行 RDP 攻擊的惡意軟體。

RDP 攻擊構成重大威脅，個人和組織都應認真對待。使用強密碼、雙因素身份驗證和其他安全措施確保 RDP 連接得到適當保護非常重要。

賽門鐵克經長時間證實的 RDP 攻擊的**零時差**保護，效益卓越，端點防護內建的網路層防護技術-IPS 可偵測最新攻擊如下：

網路層的攔截定義檔：

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：

- Attack: NCrack Tool RDP BruteForce Activity
- OS Attack: Microsoft Windows Remote Desktop Services RCE CVE-2019-0708*
- OS Attack: RDP Scan Attempt 2
- Web Attack: Microsoft RDP Exploit Attempt
- Attack: Microsoft RDP CVE-2012-0002 4
- System Infected: GoldBrute RDP BruteForce Attempt

* 這表示同一個名稱涵蓋多個相似的攻擊偵測能力。

欲瞭解更多有關於賽門鐵克端點安全入侵防護系統 (IPS) 的更多訊息，請點擊此處。

欲瞭解更多有關賽門鐵克端點安全安全完整版更多資訊，請點擊此處。

2023/05/01

散布Aurora竊密程式的活動明顯增加

Aurora 竊密程式是一種基於 Golang 程式語言的惡意程式，以惡意軟體即服務 (MaaS) 營運模式進行銷售。該惡意軟體於 2022 年首次出現，自發布以來已經多次進行優化與更版。Aurora 具有相當典型的竊密程式功能，它主要在竊取系統資訊、憑證、銀行帳號資訊、加密貨幣錢包、cookie 等。在過去的幾個星期中，賽門鐵克觀察到與散布 Aurora 竊密程式相關的惡意活動有所增加，這可能顯示該惡意軟體家族在威脅環境中越來越受歡迎。

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：

基於行為偵測技術(SONAR)的防護：

- AGR.Terminate!g2
- SONAR.ProcHijack!g45
- SONAR.Susp.Beh!gen93
- SONAR.SuspLaunch!g52
- SONAR.SuspLaunch!g266
- SONAR.TCP!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Infostealer
- Infostealer.Aurora!g1
- Packed.Generic.528
- Packed.Generic.616
- Trojan Horse

- Trojan.Gen.2
- Trojan.Gen.MBT
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.B
- Heur.AdvML.B!100
- Heur.AdvML.B!200
- Heur.AdvML.C

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: Aurora Infostealer Activity
- System Infected: Trojan.Backdoor Activity 634
- System Infected: Trojan.Backdoor Activity 735

2023/04/28

多個Xorist勒索軟體變種持續在真實網路環境興風作浪

Xorist 勒索軟體家族（也稱為 EnCiPhErEd）在過去幾年中一直很活躍，並且該惡意軟體的新變種持續在網路上嶄露頭角，危及消費者和企業用戶。已知 Xorist 勒索軟體透過破解軟體的安裝檔、偷渡式下載或惡意垃圾郵件攻擊行動進行傳播。被加密的檔案所新增的副檔名會因該惡意軟體的不同變種而異。最近發現該勒索軟體變種使用一些副檔名案例包括：.VoNiX、.gold、.kmbgdftfgdlf、.WiKoN、.GpCODE、.EnCrYpTeD 等。

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：

基於行為偵測技術(SONAR)的防護：

- SONAR.SuspBeh!gen616
- SONAR.SuspTempRun
- SONAR.SuspTempRun2
- SONAR.TCP!Gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Downloader
- Ransom.CryptoTorLocker
- Trojan.Ransomlock
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.A
- Heur.AdvML.B

2023/04/28

PaperCut遠端程式碼執行(RCE)漏洞--CVE-2023-27350在網路上遭開採利用

據報導，熱門的 PaperCut 列印管理軟體中一個嚴重漏洞已被許多攻擊者在網路開採利用。該漏洞被歸類為 CVE-2023-27350。如果被開採利用，該漏洞可能允許未經身份驗證的攻擊者繞過未修補系統上的身份驗證並導致執行任意程式碼。

雖然原廠商已經發布修補程式正來解決這個漏洞，但賽門鐵克正在觀察攻擊者目前利用這個漏洞注入各種惡意籌載，包括 coinminers 和反向 shell。賽門鐵克的網路層保護技術入侵防禦系統 (IPS) 一直在為開採利用 PaperCut 漏洞的攻擊期間觀察到的利用嘗試和反向 shell 連接提供主動防護，讓用戶高枕無憂。

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：

基於行為偵測技術(SONAR)的防護：

- SONAR.SuspLaunch!g286

檔案型(基於回應式樣本的病毒定義檔)防護：

- Downloader.Trojan
- ISB.Downloader!gen205
- Miner.XMRig!gen9
- Trojan.Horse
- Trojan.Gen.2
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- Web.Reputation.1
- WS.Malware.1

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: Malicious Java Payload Upload 2
- Web Attack: Malicious Java Payload Upload 19

基於機器學習的防禦技術：

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

基於安全強化政策(適用於使用DCS)：

賽門鐵克的重要主機防護系統：DCS(data Center Security) 內建的強化策略能為 PaperCut 的遠端程式碼執行 (RCE) 漏洞--CVE-2023-27350 提供零時差攻擊保護。DCS 內建 Windows 應用程式伺服器的預設強化政策，會阻止並記錄任何 cmd 和 powershell 執行 PaperCut 漏洞利用的後脅迫 (Post-Exploitation) 技術。更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。

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／IP位址已於第一時間收錄於不安全分類列表中。

2023/04/28

Atomic macOS竊密程式(AMOS)

在真實網路環境發現一種名為 Atomic（又名 AMOS）的 macOS 平台上全新竊密程式。該惡意軟體透過 Telegram 頻道銷售，並以專為 macOS 平台開發的變種為號召。AMOS 會嘗試從受感染的電腦中竊取包羅萬象之敏感資料，包括系統資訊、金鑰密碼、使用者檔案、cookie、瀏覽器資料、信用卡詳細資訊、加密貨幣錢包等。再將收集到的訊息壓縮到一個 .zip 檔中，並外洩到攻擊者所操控的網域中。

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：

- Trojan.Horse
- OSX.Trojan.Gen.2
- WS.Malware.2

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／IP位址已於第一時間收錄於不安全分類列表中。