保安資訊--本周(台灣時間2024/10/04)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 47 萬 7,200 台受保護端點上總共阻止了 4,680 萬次攻擊。這些攻擊中有 80.7% 在感染階段前就被有效阻止：**(2024/09/30)**

- 在**8萬6,600**台端點上，阻止了**1,240**萬次嘗試掃描**Web**伺服器的漏洞。
- 在**10萬7,400**台端點上，阻止了**890**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**3萬**台**Windows**伺服主機上，阻止了**7萬2,000**次攻擊。
- 在**5萬5,800**台端點上，阻止了**170**萬次嘗試掃描伺服器漏洞。
- 在**1萬300**台端點上，阻止了**63萬1,200**次嘗試掃描在**CMS**漏洞。
- 在**5萬3,800**台端點上，阻止了**240**萬次嘗試利用的應用程式漏洞。
- 在**13萬3,700**台端點上，阻止了**450**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**7,200**台端點上，阻止了**100**萬次加密貨幣挖礦攻擊。
- 在**9萬9,800**台端點上，阻止了**810**萬台次向惡意軟體**C&C**連線的嘗試。
- 在**560**台端點上，阻止了**8萬6,300**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。

有憑有據!SEP的瀏覽器延伸防護功能，在上周所帶來的好處？

賽門鐵克的入侵預防系統 (IPS) 是業界最佳的深度資料包檢測引擎，可保護數億個端點(桌上型電腦和伺服器)，其中包括財富 500 強企業和消費者。

賽門鐵克端點安全 (SES) 或賽門鐵克端點防護 (SEP) 代理透過谷歌 Chrome 瀏覽器和微軟 Edge 瀏覽器的延伸供瀏覽器保護。這些延伸有兩個組成部分：

- 瀏覽器的入侵預防，利用 IPS 引擎保護客戶免受各種威脅的侵害。
- 網頁信譽，可識別可能包含惡意軟體、欺詐、網路釣魚和垃圾郵件等惡意內容的網域和網頁帶來的威脅，並阻止瀏覽這些網頁。

在過去 7 天內，賽門鐵克透過端點防護的瀏覽器延伸防護功能，在 18 萬 1,600 個受保護端點上阻止了總計 670 萬次攻擊。**(2024/09/30)**

- 使用網頁信譽情資，在 **172.2K** 個端點上阻止 **640** 萬次攻擊。
- 攔截 **22.3K** 個端點上 **275.6K** 次攻擊，這些攻擊試圖將用戶重定向到攻擊者控制的網站上。
- 在 **9K** 個端點上攔截 **99.5K** 次瀏覽器通知詐騙攻擊／技術支援詐騙攻擊／加密劫持嘗試。
- 在 **370** 個端點上攔截 **9K** 次攻擊，這些攻擊利用被入侵操控網站上的惡意腳本注入。

建議客戶啟用端點防護 (SEP) 的瀏覽器延伸，以獲得最佳防護。按下此處獲取：整合瀏覽器延伸和 Symantec Endpoint Protection (SEP)，防止惡意網站的說明。

2024/10/04
Falcon鍵盤側錄程式

Falcon 是最近活躍於真實網路情境的鍵盤側錄程式。此惡意軟體較舊的版本甚至可追溯至 2019 年，而最新觀察到的樣本則來自上個月。Falcon 具備記錄受感染機器按鍵、收集系統資訊、螢幕截圖等功能。收集到的資料會持續滲出到攻擊者所操控的 C&C 伺服器。諸如 Falcon 等鍵盤側錄程式可被威脅者用來獲取機密資訊，包括憑證、銀行資料等。

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：

自適應防護技術(包含於SESC)：

- ACM.Untrst-RunSys!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.TCP!gen1

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Downloader
- Trojan Horse
- Trojan.Gen.MBT
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.A!300
- Heur.AdvML.A!400
- Heur.AdvML.A!500
- Heur.AdvML.B
- Heur.AdvML.B!100
- Heur.AdvML.B!200
- Heur.AdvML.C

2024/10/04

Nunu Stealer惡意竊密程式

Nunu Stealer 是最近發現一種採用 Python 撰寫的惡意竊密程式新變種，它源於早先較舊的惡意竊密程式：Akira Stealer。其功能包括竊取並滲出各種機密資訊，例如：銀行詳細資料、信用卡資料、憑證、瀏覽器中儲存的自動填入資料 (autofill data)、cookie、第三方應用程式會話資料 (session data)、「Discord Token」(建立帳戶時產生的 Discord 使用者名稱和密碼的加密)、加密貨幣錢包等。攻擊者可能會利用 Nunu 入侵各種使用者帳戶，並利用這些帳戶進一步推進攻擊鏈。

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：

自適應防護技術(包含於SESC)：

- ACM.Ps-Reg!g1
- ACM.Ps-RgPst!g1

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

檔案型(基於回應式樣本的病毒定義檔)防護：

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

基於機器學習的防禦技術：

- Heur.AdvML.A!500
- Heur.AdvML.C

2024/10/04

VeilShell後門／遠端存取木馬程式(RAT)：來自北韓Vedalia進階持續威脅(APT)駭客集團的全新威脅

根據報告，與北韓有關連的威脅份子一直在針對東南亞國家的攻擊行動中，部署一個至今無紀錄可查的後門及遠端存取木馬程式 (RAT)，稱為 VeilShell。該活動歸咎於Vedalia 進階持續威脅 (APT) 駭客集團 (又稱 APT37、ScarCruft、Reaper)。

該攻擊通常從魚叉式網路釣魚電子郵件所開始觸發，釣魚郵件包含一個 .ZIP 壓縮檔，內含一個 Windows 捷徑 (LNK) 檔案。當執行時，LNK 檔會觸發 PowerShell 程式碼來呼叫／擷取相關元件，包括一個良性的文件檔和一個惡意 DLL。DLL 可作為載入程式，呼叫／擷取從遠端伺服器下載 VeilShell 後端程式的 JavaScript。

VeilShell 被歸類為 PowerShell 類型的後門惡意軟體，可與命令與控制 (C&C) 伺服器通訊，以收集和滲出系統資訊。它可以與檔案系統互動、修改登錄檔 (registry)、建立工作排程，並維持後門存取的常駐能力以進一步進行惡意活動。

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：

自適應防護技術(包含於SESC)：

- ACM.Ps-Base64!g1
- ACM.Ps-CPE!g2
- ACM.Ps-FlPst!g1
- ACM.Ps-Rd32!g1

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

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：

- CL.Downloader!gen241
- CL.Downloader!gen262
- Trojan Horse
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- WS.Malware.1
- WS.SecurityRisk.4

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。

2024/10/04

借力SmartLoader惡意程式載入器，Lumma惡意竊密程式，如虎添翼

SmartLoader 惡意程式載入器可追溯到 2024 年 7 月所涉及的一個名為「user-attachments」的私人 GitHub 帳戶。它觸發於一個包含四個檔案的 .zip 壓縮檔：compiler.exe、conf.txt、Launcher.bat 和 lua51.dll。一旦使用者執行 Launcher.bat，它會使用 conf.txt 執行 compiler.exe，啟動 SmartLoader 並部署 Lumma 惡意竊密程式。這個以 C 語言撰寫的惡意竊密程式會竊取儲存在系統瀏覽器中的資料，以及任何目前存在的加密貨幣錢包。

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：

自適應防護技術(包含於SESC)：

- ACM.Ps-Rd32!g1
- ACM.Ps-RgPst!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.Heur.Dropper
- SONAR.D!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- WS.Reputation.1

基於機器學習的防禦技術：

- Heur.AdvML.A!500
- Heur.AdvML.C
- Heur.AdvML.D

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。

2024/10/03

Key Group：以俄羅斯使用者為目標，與時俱進的勒索軟體駭客集團

Key Group 是一個以財務為動機的勒索軟體駭客集團，主要以俄羅斯使用者為目標，並以透過 Telegram 與受害者談判而聞名。與其他利用洩漏勒索軟體建置程式的駭客集團一樣，Key Group 主要利用 Chaos 勒索軟體建置程式等，並為其指揮與控制 (C&C) 基礎架構運作 GitHub 儲存庫。該駭客集團於 2022 年 4 月被發現，隨著時間的推移已開發多個勒索軟體的後繼新變種，包括 Chaos、Annabelle、RuRansom、Hakuna Matata 以及最新的 NoCry 變種。

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：

自適應防護技術(包含於SESC)：

- ACM.Untrst-FlPst!g1
- ACM.Untrst-RLsass!g1

- ACM.Untrst-RunSys!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.Dropper
- SONAR.RansomGen!gen5
- SONAR.Ransomware!g7
- SONAR.Ransomware!g16
- SONAR.Ransomware!g34
- SONAR.SuspBeh.C!gen18
- SONAR.SuspDrop!gen1

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.HiddenTear!g1
- Ransom.Sorry
- Ransom.RuRan
- Ransom.Wannacry
- Trojan.Gen.MBT
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.A!300
- Heur.AdvML.A!400
- Heur.AdvML.A!500
- Heur.AdvML.B
- Heur.AdvML.B!100
- Heur.AdvML.B!200
- 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。

2024/10/03

BabyLockerKZ--源於MedusaLocker勒索軟體的後繼新變種

BabyLockerKZ 勒索軟體是源於 MedusaLocker 勒索軟體的後繼新變種，自 2023 年起開始活躍。此新變種使用許多與先前 MedusaLocker 攻擊相同的策略、技術和程序 (TTPs)(公開可用的工具、自訂工具、就地取材攻擊素材、聊天和洩漏網站)。負責此勒索軟體的威脅份子自 2022 年起開始活躍，目標受害者遍及全球。最近的受害者大多位於南美洲。Cisco Talos 的研究人員已發佈關於此惡意軟體的其他詳細資訊。

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：

自適應防護技術(包含於SESC)：

- ACM.Ps-Net!g1
- ACM.Ps-RgPst!g1
- ACM.Ps-Wbadmin!g1
- ACM.Untrst-RgPst!g1
- ACM.Untrst-RunSys!g1
- ACM.Vss-DlShcp!g1
- ACM.Wbadmin-DlBckp!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.Ransom!gen14
- SONAR.Ransom!gen107
- SONAR.RansomLckbit!g3
- SONAR.RansomPlay!gen1
- SONAR.SuspLaunch!g18
- SONAR.SuspReg!gen49

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Hacktool.Mimikatz
- ISB.Malscript!gen7
- Ransom.GlobeImposter
- Ransom.MedusaLocker
- Trojan.Gen.MBT
- WS.Malware.1
- WS.SecurityRisk.1

基於機器學習的防禦技術：

- Heur.AdvML.A!300
- Heur.AdvML.A!400
- Heur.AdvML.A!500
- Heur.AdvML.B
- Heur.AdvML.B!100
- Heur.AdvML.B!200
- Heur.AdvML.C

2024/10/03

Silver Oryx Blade--針對巴西的全新銀行惡意軟體

Silver Oryx Blade 是由 Scitum 研究人員發現的全新銀行木馬程式。該惡意軟體主要針對巴西的受害者，並試圖從受感染的機器中竊取銀行資訊。感染鏈由金融或稅務相關的釣魚郵件所觸發。在後續的攻擊鏈階段，威脅者會使用惡意的 .zip 檔案、.msi 植入程式以及 .dll 載入程式。Silver Oryx Blade 會監控 50 多家銀行和金融機構的相關資料，並將擷取的資訊轉送到攻擊者所操控的 C&C 伺服器。

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：

自適應防護技術(包含於SESC)：

- ACM.Ps-Rd32!g1

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

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：

- Scr.Malcode!gen43
- Trojan Horse
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.A!300
- Heur.AdvML.A!400
- Heur.AdvML.A!500
- 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：

- Web Attack: Webpulse Bad Reputation Domain Request

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。

2024/10/03

Gorilla(*大猩猩)殭屍網路：源於Mirai程式碼的全球性全新威脅

有報告指出，一個名為 Gorilla Botnet 的全新殭屍網絡家族所涉入的活動激增，其目標是全球的電信、大學和遊戲產業。這個殭屍網路是源於 Mirai 原始碼的後繼增修版本，相容於各種 CPU 架構，包括 ARM、MIPS、x86_64 和 x86。它擁有先進的 DDoS 攻擊方法，並採用多種技術發動持續性攻擊。

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：

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Linux.Mirai
- Trojan Horse
- Trojan.Gen.NPE
- WS.Malware.1

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。

2024/10/02

CeranaKeeper進階持續威脅(APT)駭客集團所發動的網路攻擊行動

研究人員最近觀察到 CeranaKeeper 進階持續威脅 (APT) 駭客集團所發動的網路攻擊行動。這個與中國有關連的威脅份子以泰國、緬甸、菲律賓、日本和台灣的政府單位為目標。該駭客集團持續更新其工具 (例如：後門) 以逃避偵測，並利用 Dropbox 和 OneDrive 等雲端服務來提供自訂解決方案。他們也利用 GitHub 的功能來建立隱蔽的反向shell，使用該平台作為他們專用的 C&C伺服器。

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：

自適應防護技術(包含於SESC)：

- ACM.Ps-Rd32!g1
- ACM.Untrst-RunSys!g1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Infostealer
- Trojan.Gen.MBT
- 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。

2024/10/02

假冒更新程式安裝檔為幌子的惡意軟體之散播行動讓WarmCookie聲名大噪

一起發生在法國的網路攻擊行動正在利用遭入侵的網站，透過虛假的 Google Chrome 和 Java 等熱門應用程式更新程式安裝檔為幌子，散佈 WarmCookie 後門。威脅組織「SocGolish」所採用的這種策略，會誘騙使用者下載偽裝為合法更新的惡意軟體，這些更新包括瀏覽器以及 Java 和 VMware 等應用程式。最新版本的 WarmCookie 能夠竊取資料、執行指令和執行檔案，足以造成極大的危害。

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：

自適應防護技術(包含於SESC)：

- ACM.Ps-TskReg!g1
- ACM.Untrst-TskReg!g1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Backdoor.Cobalt

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。

2024/10/02

Defi勒索軟體

Defi 是 Makop 勒索軟體家族的最新版本。該惡意軟體會加密檔案，並冠上 .defi1328 及開發人員的電子郵件地址和受害者唯一 ID 的附檔名。勒索贖金支付說明會以「README-WARNING.txt」的文字檔形式存放在磁碟中。該惡意軟體還會變更桌面桌布。Defi 勒索軟體具有刪除受感染機器上的卷影複本的功能。

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：

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.Makop!g1
- WS.SecurityRisk.4

基於機器學習的防禦技術：

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

2024/10/02

Stonefly 駭客集團：鎖定美國，發動打死不退的敲詐勒索軟體攻擊

賽門鐵克的威脅獵手團隊 (Threat Hunter Team) 發現有證據顯示，儘管北韓 Stonefly 駭客集團 (又稱 Andariel、APT45、Silent Chollima、Onyx Sleet) 已被起訴並獲得數百萬美元的賞金，但該駭客集團仍繼續針對美國的組織發動以財務為動機的攻擊。

Broadcom 旗下的賽門鐵克 (Symantec) 在今年 8 月，也就是起訴書公佈的一個月後，發現針對美國三家不同組織的入侵證據。雖然攻擊者並未成功在任何受影響組織的網路中部署勒索軟體，但這些攻擊很可能是出於財務上的動機。所有受害者都是私人公司，所涉及的業務沒有明顯的情報價值。

我們的部落格文章有更詳細的報導：Stonefly 駭客集團：鎖定美國，發動打死不退的敲詐勒索軟體攻擊。

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：

自適應防護技術(包含於SESC)：

- ACM.Ps-Rd32!g1
- ACM.Ps-RgPst!g1
- ACM.Ps-Wscr!g1
- ACM.Untrst-RgPst!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.TCP!gen1
- SONAR.TCP!gen6

檔案型(基於回應式樣本的病毒定義檔)防護：

- Backdoor.Preft
- Backdoor.Silverrat
- Hacktool
- Hacktool.Mimikatz
- PUA.Gen.2
- Trojan Horse
- Trojan.Gen.9
- Trojan.Gen.MBT

- WS.Malware.1
- WS.Malware.2

基於機器學習的防禦技術：

- Heur.AdvML.A!300
- Heur.AdvML.A!400
- Heur.AdvML.A!500
- Heur.AdvML.B!100
- Heur.AdvML.B!200
- 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。

2024/10/01

K4Spreader和Hadooken等惡意軟體，所涉入的最新攻擊

最近研究發現一個濫用Oracle WebLogic 漏洞 (CVE-2017-10271 和 CVE-2020-14883) 針對 Windows 和 Linux 系統的感染鏈。攻擊者使用 Python 和 Bash 腳本來部署 K4Spreader 惡意軟體，該惡意軟體會傳送 Tsunami 後門程式和挖礦程式。還嘗試在 Windows 系統上使用 PowerShell 腳本。另一個研究小組則報告另一項攻擊，Hadooken 惡意軟體利用 WebLogic 伺服器的組態漏洞，使用 shell 和 Python 指令碼安裝一個密碼控制程式和 Tsunami 惡意軟體。

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：

- Linux.Kaiten
- OSX.Isiport
- Trojan Horse
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- Trojan.Gen.NPE.2
- WS.Malware.1
- WS.Malware.2

基於機器學習的防禦技術：

- Heur.AdvML.A!300
- Heur.AdvML.A!400
- Heur.AdvML.A!500
- Heur.AdvML.B
- Heur.AdvML.B!100
- Heur.AdvML.B!200

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。

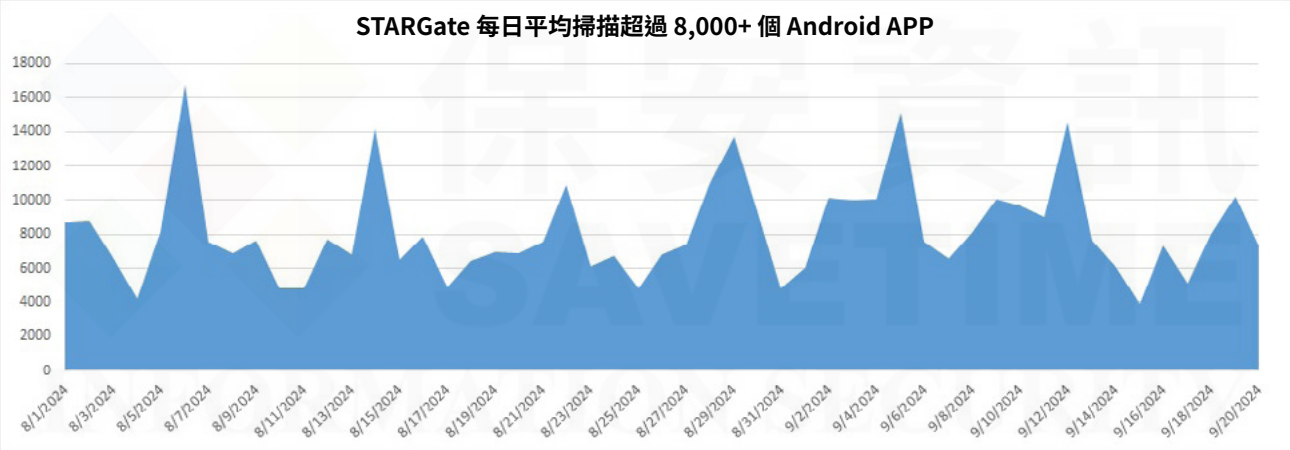
2024/10/01

防護亮點：STARGate(*星際之門)的Mobile Insight(行動鑑識)能有效防止惡意APP下載到手機

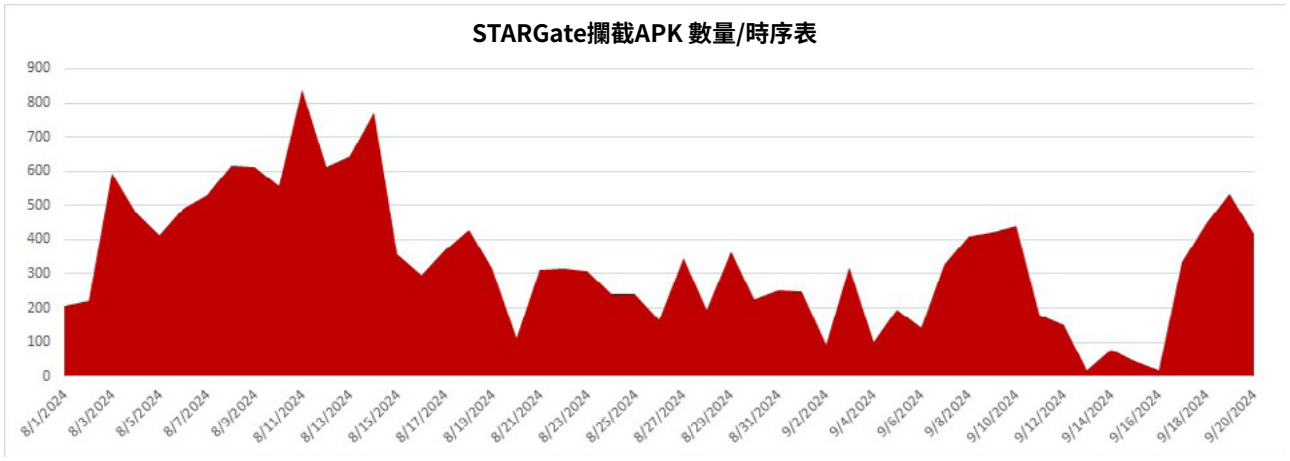
手機與行動裝置上的網路釣魚和 QR 碼／圖碼 (英語：Quick Response Code；全稱為快速回應圖碼) 詐騙正在增加，正如我們在 2024 年 7 月的防護公報中所討論。防止惡意 APP 下載至使用者的手機，可為我們的客戶提供額外且必要的保護層。

STARGate 是一個先進的網路防禦平台，可在賽門鐵克企業產品的廣泛範圍內提供威脅偵測與靜態內容分析。其中 Mobile Insight(行動鑑識) 的功能，可在賽門鐵克產品 (例如：Symantec CloudSOC、Symantec Messaging Gateway 或 Symantec Protection Engine) 的閘道層 (Gateway layer) 上阻止內嵌於 Android Package Kit (APK) 先前未見的手機與行動裝置上的威脅。STARGate 會根據已部署實例的匿名資訊，使用 machine-determined 的機器學習平台特色來識別好或壞的 Android APP。STARGate Mobile Insight 使用與我們的行動威脅防禦系統相同的關係式深度學習解決方案。

目前 STARGate 每日平均掃描超過 8,000+ 個 Android APP，涵蓋及其 Symantec Enterprise 產品。



STARGate 平均每天可阻止約 300 個惡意 APK 進入使用者的手機，在惡意 APK 有機會開始之前就將其阻擋。



Android 行動監視範例

「com.nexipaytoken.app」套件就是這樣一個惡意 Android APP 的範例。此惡意應用程式以「Nexi」品牌自居（Nexiis 是合法的歐洲數位支付解決方案）。一旦部署到用戶的手機上，該應用

程式就有能力執行以下動作：

- 連接至指揮與控制 (C&C) 伺服器以接收指令
- 開啟攝影機
- 擷取通話記錄
- 啟動電話通話
- 鎖定裝置
- 開啟系統設定以解除某些安全機制的限制
- 開啟網址並執行自動點選動作
- 下載其他 APP
- 擷取螢幕截圖
- 開啟或解除安裝特定 APP
- 刪除、傳送簡訊至指定的目標號碼
- 顯示覆蓋視窗，有可能模仿合法網頁
- 建立虛假通知

STARGate Mobile Insight 在閘道層將這個 Android 套件識別為 Mobile Spy，防止惡意 APP 下載到使用者的手機。

欲瞭解有關防護亮點：有效抵禦複雜攻擊鏈的威脅情報--STARGate(*星際之門)，請點擊此處。

2024/10/01

全新的 Rast 勒索軟體威脅以中國政府單位為目標

一種名為 Rast 的全新勒索軟體威脅證實已被發現，專門針對中國政府單位。攻擊媒介包括 RDP 暴力破解和利用 N-day 漏洞來獲得邊界伺服器的存取全縣，接著再以手動方式部署勒索軟體元件。一旦部署完成後，Rast 會將機器名稱和獨特識別碼上傳至遠端 MySQL 資料庫。勒索軟體似乎與時俱進，最新的變種需要在啟動時透過主控台介面進行手動操作，攻擊者必須直接參與才能啟動勒索軟體程序。

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：

自適應防護技術(包含於SESC)：

- ACM.Ps-RgPst!g1
- ACM.Untrst-RgPst!g1
- ACM.Untrst-RunSys!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.Dropper
- SONAR.SuspBeh.C!gen10

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan Horse
- Trojan.Gen.MBT
- W32.Neshuta
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.A!300
- Heur.AdvML.A!400
- Heur.AdvML.A!500
- Heur.AdvML.B
- Heur.AdvML.B!100
- Heur.AdvML.B!200

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。

2024/10/01

俄羅斯能源公司和電子產業供應鏈正遭受一波波的惡意程式攻擊

已發現到鎖定俄羅斯能源公司和電子產業供應鏈的新一波惡意軟體攻擊行動。惡意軟體透過電子郵件附件或當地 Yandex Disk 雲端硬碟服務商的連結傳播，使用包含 .LNK 檔案的 RAR 壓縮檔下載並執行惡意 HTA 檔案。這些檔案會產生 VBS 腳本，透過登錄機碼 (Registry Key) 和工作排程來確保常駐能力。這些腳本會複製使用者主目錄的檔案和 Telegram 資料，並將其滲出到攻擊者所操控的 C&C 伺服器。

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：

自適應防護技術(包含於SESC)：

- ACM.Ps-Mshta!g1
- ACM.Mshta-Http!g1

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

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：

- CL.Downloader!gen203

- CL.Downloader!gen241
- Trojan.Gen.NPE.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。

2024/09/30

微軟本月修補的Windows MSHTML平臺仿冒詐騙漏洞(CVE-2024-43461)，後續發現在修補前已遭Void Banshee駭客組織利用

CVE-2024-43461 是存在 Windows MSHTML 平臺的仿冒詐騙漏洞，在近期 9 月份的微軟例行性安全性更新被揭露。成功開採濫用此漏洞可讓攻擊者在應用程式執行的時候執行任意程式碼。據報導，此漏洞與七月份的另一個 MSHTML 漏洞--CVE-2024-38112 被一起搭配在零時差攻擊中被開採濫用。已被報導的攻擊被歸咎於一個名為 Void Banshee 的威脅組織，該威脅組織散並藉此漏洞佈惡意竊密程式到未修補該漏洞的機構組織。

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：

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: Windows MSHTML Platform CVE-2024-43461

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，DCS 可以對 Microsoft Internet Explorer 的預設強化提供針對 CVE-2024-38112 的零時差防護。預設強化政策會封鎖所有對外連線。套用於 Microsoft IE 的 DCS 沙箱可防止下載任何惡意有效酬載或執行任意程序。
- 套用於 Microsoft IE 的 DCS 沙箱可防止下載任何惡意有效酬載或執行任意程序。

更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。

2024/09/30

北韓駭客利用RustDoor惡意軟體瞄準LinkedIn上的加密貨幣使用者

9 月初，美國聯邦調查局 (FBI) 發出警告，指北韓駭客組織鎖定加密貨幣生態圈為目標。據報導，這些威脅份子試圖在 LinkedIn 上引誘潛在受害者傳遞 RustDoor 惡意軟體。潛在的受害者很可能會被冒充合法的去中心化交易所 (DEX：decentralized cryptocurrency exchange) 招聘人員所誘騙，並由看起來很專業的網站提供支援，以增強虛假實體的合法性。

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：

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政

策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

檔案型(基於回應式樣本的病毒定義檔)防護：

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

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。

2024/09/30

Progress公司旗下的WhatsUp Gold SQL存在SQL注入漏洞：CVE-2024-6670

CVE-2024-6670 是一個最近被揭露的 SQL 注入漏洞，會影響 Progress WhatsUp Gold，這是一個知名的網路監控軟體。成功開採濫用此漏洞可讓未經驗證的攻擊者擷取使用者的加密密碼。該漏洞已被美國網路安全暨基礎設施安全局 (CISA) 列入「已遭成功利用的高風險漏洞名單 (the Known Exploited Vulnerabilities Catalog-KEV)」中，是繼另一個 WhatsUp Gold 漏洞 CVE-2024-6671 之後，被列入的同系列安全性漏洞。

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：

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: WhatsUp Gold CVE-2024-6670

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。

2024/09/30

Unix通用列印系統(Common UNIX Printing System，CUPS)存在一系列新漏洞

賽門鐵克發現在 UNIX 系統上的通用列印系統 (Common UNIX Printing System，CUPS) 發現多個漏洞，攻擊者可開此濫用某些配置取得未經授權的存取，並執行遠端程式碼執行 (RCE)，尤其是利用 cups-browsed 服務。受影響之套件及漏洞編號如下：

- CVE-2024-47076：libcupsfilters--不當輸入驗證／識別漏洞
- CVE-2024-47175：libppd--不當輸入驗證／識別漏洞
- CVE-2024-47176：cups-browsed--綁定到不受限制的 IP 位址漏洞
- CVE-2024-47177：cups-filters--指令注入漏洞 (RCE)

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 的 UNIX 預設鎖定政策就可保護底層 UNIX 伺服器不受此漏洞影響。CUPS 印表機守則的預設沙箱可防止所有來自公開網際網路或區域網路的入埠連線，這在一些公開的部落格中也有提及。此外，此政策防止執行任意指令和限制讀取關鍵作業系統檔案。

更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。

2024/09/29

由AI加持的先進加密貨幣安全威脅：Rhadamanthys惡意竊密程式

據報導，Rhadamanthys 惡意竊密程式最新版本具有更先進的功能，包括使用人工智慧(AI)進行光學字元辨識 (OCR)。此功能可讓 Rhadamanthys 從影像中擷取加密貨幣錢包的助字詞 (Seed Phrase)，對任何擁有加密貨幣的人造成重大威脅。惡意軟體可辨識客戶端的助字詞 (Seed Phrase) 影像，並將其傳輸至命令暨控制 (C&C) 伺服器，以便進一步利用。除針對憑證、系統資訊和財務資料之外，Rhadamanthys 還採用複雜的迴避技術，例如：將自身偽裝成 MSI 安裝程式。

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：

自適應防護技術(包含於SESC)：

- ACM.Untrst-RunSys!g1

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

檔案型(基於回應式樣本的病毒定義檔)防護：

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

基於機器學習的防禦技術：

- Heur.AdvML.A!300
- Heur.AdvML.B
- Heur.AdvML.B!100
- Heur.AdvML.B!200

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。

2024/09/29

DCRat(也稱Dark Crystal RAT)特洛伊木馬

DCRat (也稱 Dark Crystal RAT) 是一款模組化的遠端存取木馬程式，在 2018 年即採用惡意軟體即服務 (malware-as-a-service) 的營運模式問世。它可以執行指令、記錄按鍵和外洩資料。最近，它使用 HTML 挾帶 (HTML smuggling) 這種隱匿手法傳送，在 HTML 中嵌入並混淆有效酬載，以逃避安全軟體的偵測。有效酬載在瀏覽器轉譯／渲染 (Browser Rendering) 時會被啟動，通常需要使用者的互動。Azorult 和 Pikabot 等其他惡意軟體也使用此技術。

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：

自適應防護技術(包含於SESC)：

- ACM.Ps-RgPst!g1
- ACM.Untrst-RgPst!g1
- ACM.Wmi-Schtsk!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.MalTraffic!gen1
- SONAR.SuspBeh.C!gen2
- SONAR.SuspBeh.C!gen18
- SONAR.SuspBeh!gen313

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

檔案型(基於回應式樣本的病毒定義檔)防護：

- ISB.Downloader!gen523
- Scr.Malcode.T!gen
- Trojan.Gen.MBT
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.A!300
- Heur.AdvML.A!400
- Heur.AdvML.A!500
- Heur.AdvML.B
- Heur.AdvML.B!100
- Heur.AdvML.B!200

2024/09/27

CVE-2024-8190--存在Ivanti Cloud Services Appliance的作業系統指令注入漏洞

CVE-2024-8190 是一個影響 Ivanti Cloud Services Appliance (CSA) 4.6 Patch 518 或更舊版本的高嚴重性 (CVSS 風險評分：7.2) 作業系統指令注入漏洞。若成功開採濫用此漏洞，遠端認證的攻擊者可能會執行任意程式碼。值得注意的是，攻擊者必須擁有管理者權限才能開採濫用此漏洞。此漏洞已被美國網路安全暨基礎設施安全局 (CISA) 列入「已遭成功利用的高風險漏洞名單 (the Known Exploited Vulnerabilities Catalog-KEV)」中，之前有報告指出此漏洞與另一個 Ivanti 漏洞 CVE-2024-8963 一起被利用在真實網路情境發動攻擊。

網路上的知識：

Ivanti Cloud Services Appliance (CSA) 是一種網際網路裝置，能透過網際網路提供安全的通訊和功能。它充當控制台與受管理裝置，經由他們的網際網路連線進行連結的會合地－－即使它們位於防火牆之後或使用代理存取網際網路。

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：

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: Ivanti CSA OS Command Injection CVE-2024-8190

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，預設鎖定政策就可保護底層伺服器免受此漏洞影響，包括防止執行任意指令和限制讀取關鍵作業系統檔案。
- DCS 的網路規則政策可設定為，將應用程式限制為受信任的用戶端。

更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。

2024/09/27

知名惡意竊密軟體：Vidar，藉由義大利專用PEC Mail和Telegram個人資料傳播

義大利的 CERT-AGID (類似 TWCERT／CC 台灣電腦網路危機處理暨協調中心) 發現新一起界藉由 PEC 郵箱散佈 Vidar Vidar 惡意竊密軟體攻擊行動。攻擊者仍在利用 Steam 社群設定檔，但一個重要的新策略是利用 Telegram 設定檔。特別是，這些設定檔的個人簡介 (BIOS) 被用來揭露其指揮與控制 (C2) 伺服器的 IP 位址。

網路的知識：

- Steam 社群是由許多熱愛電腦遊戲的玩家所組成。在這裡，您可以找到一起玩遊戲的夥伴、與好友相聚、加入志同道合的群組、主持或加入聊天室，更可參與甚至舉辦大大小小的比賽。
- PEC 郵箱是一款專門為企業量身定制的電子郵件服務，其全稱為『Posta Elettronica Certificata』，意為『認證電子郵件』，是義大利政府推出的一項郵件認證服務。 PEC 郵箱提供安全可靠的電子郵件收發，同時通過獨特的驗證機制，確保郵件內容的合法性和真實性。

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：

自適應防護技術(包含於SESC)：

- ACM.Rgasm-Lnch!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.SuspOpen!gen11

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

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
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.A!300
- Heur.AdvML.B
- Heur.AdvML.B!100
- Heur.AdvML.B!200

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。

2024/09/27

Louse進階持續威脅(APT)駭客組織發起針對中國實體的惡意軟體攻擊行動

據報導，Louse 進階持續威脅 (APT) 駭客組織 (又稱為 Patchwork 和 Dropping Elephant) 發起一個針對中國實體的惡意軟體攻擊行動。攻擊手法涉及惡意 LNK 檔案，可能源自網路釣魚電子郵件。此檔案會執行 PowerShell 指令碼，下載誘餌 PDF 和惡意 DLL，並使用 DLL 側載技術。DLL 接著會解密並執行 shellcode，最終部署稱為 Nexe 新最終有效酬載，其目的是從受攻擊的系統中竊取敏感資訊。

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：

自適應防護技術(包含於SESC)：

- ACM.Ps-CPE!g2
- ACM.Ps-Http!g2

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

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
- 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: Webpulse Bad Reputation Domain Request

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。

關於賽門鐵克 (Symantec)

賽門鐵克 (Symantec) 已於 2019/11 併入全球網通晶片巨擘--博通 (BroadCom，美國股市代號 AVGO，全世界網際網路流量有 99.9% 經過博通的網通晶片) 軟體事業部的企業安全部門 (SED)，特別是近年以半導體的嚴謹、系統化以及零錯誤思維來改造核心技術、管理框架以及整合最完整的資安生態體系，讓賽門鐵克的解決方案在穩定性、相容性、有效性以及資安生態系整合擴充性，有著脫胎換骨並超越業界的長足進步。博通 (Broadcom) 是務實的完美主義者，致力於追求卓越、關注細節並且有系統和紀律地投入科技創新與嚴謹工藝，同時也大大降低交易複雜性。Symantec 持續創新的技術能為日新月異的資安問題提供更好的解決方案，近三年 Symantec 很少出現在由公關機制產生的頭版文章中，而且在全球前兩千大企業的市佔率及營收成長均遠遠高於併入博通之前，增長幅度也領先其他競爭對手，是科技創新驅動的解決方案非常穩健可靠深受大型企業信賴的實證，也顯示大型企業顧客對轉型中的新賽門鐵克未來充滿信心。(美籍華人王嘉廉創辦的企業軟體公司，組合國際電腦（CA Technologies）以及雲端運算及「硬體虛擬化」的領導廠商--VMware， 也是博通軟體事業部的成員)。2021 年八月，因應國外發動的針對性攻擊日益嚴重，美國網路安全暨基礎架構安全管理署（CISA）宣布聯合民間科技公司，發展全國性聯合防禦計畫 JCDC(Joint Cyber Defense Collaborative)，而博通賽門鐵克是首輪被徵招的一線廠商，如就地緣政治考量，Symantec 也絕對是最安全的資安廠商。擁有更強大資源與技術為後盾的賽門鐵克已更專注於整合各種最新科技於既有領先業界的端點、郵件、網頁以及身分認證等安全解決方案。

關於保安資訊 www.savetime.com.tw

保安資訊團隊是台灣第一家專注在賽門鐵克解決方案的技術型領導廠商，被業界公認為賽門鐵克解決方案專家。自 1995 年起就全心全力專注在賽門鐵克資訊安全解決方案的技術支援、銷售、規劃與整合、教育訓練、顧問服務，特別是提供企業 IT 專業人員的知識傳承 (Knowledge Transfer)、協助顧客符合邏輯地解決資安問題本質的效益上，以及基於比原廠更孰悉用戶使用情境的優勢能提供更快速有效的技術支援回應，深獲許多中大型企業與組織的信賴，長期合作的意願與滿意度極高。許多顧客樂意與我們建立起長期的友誼，把我們當成可信任的資安建議者、可以提供良好諮商的資安策略夥伴以及總是第一個被想到的求助暨諮詢對象。

保安資訊連絡電話：**0800-381-500**。