保安資訊--本周(台灣時間2021/12/17)
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 130 萬個受保護端點上總共阻止了 1.621 億次攻擊。這些攻擊中有 94% 在感染階段前就被有效阻止：**(2021/12/12)**

- 在**22萬4,700**台端點上，阻止了**5,550**萬次嘗試掃描**Web**服務器的漏洞。
- 在**53萬3,100**台端點上，阻止了**4,690**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**9萬600**台**Windows**伺服主機上，阻止了**2,190**萬次攻擊。
- 在**17萬3,300**端點上，阻止了**1,190**萬次嘗試掃描伺服器漏洞。
- 在**9萬6,500**台端點上，阻止了**510**萬次嘗試掃描在**CMS**漏洞。
- 在**13萬1,600**台端點上，阻止了**380**萬次嘗試利用的應用程式漏洞。
- 在**48萬200**台端點上，阻止了**1,360**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**5,500**台端點上，阻止了**390**萬次加密貨幣挖礦攻擊。
- 在**5萬2,900**台端點上，阻止了**570**萬次向惡意軟體**C&C**連線的嘗試。
- 在**8,800**台端點上，阻止了**25萬6,000**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。

2021/12/16

Noberus 又名 ALPHV/BlackCat，一種新的由 Rust 程式語言開發的勒索軟體

11 月中旬，賽門鐵克研究人員在受害者網路上發現了一種用 Rust 程式語言所編寫的新勒索軟體，在攻擊過程中部署了三種勒索軟體變種。在部署 Noberus 勒索軟體（也稱為 ALPHV 或 BlackCat）之前不久觀察到的活動中，也執行了 ConnectWise。這可能表明攻擊者可能已利用對 ConnectWise 的存取來部署其有效籌載。儘管 ConnectWise 是一種合法工具，但最近它經常被勒索軟體攻擊者利用來存取受害網路。

在我們的部落格中閱讀更多資訊：

Noberus：技術分析顯示新型基於 Rust 程式語言勒索軟體的複雜性

保安資訊建議：

可瀏覽 Rust 程式設計語言 (rust-lang.org) 網站 https://www.rust-lang.org/zh-TW，有了解及學習 Rust 所需的資訊。

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.Noberus
- Trojan.Gen.2
- Trojan.Gen.MBT
- Trojan.Gen.NPE

基於行為偵測技術(Snoar)的防護：

- SONAR.SuspLaunch!gen4

基於機器學習的防禦技術

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

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：

- Attack: Ransom.Gen Activity 51

2021/12/16

基於 Java 的遠端存取木馬 (RAT)：DarkWatchman

在威脅態勢中觀察到一種名為 DarkWatchman 基於 Java 的遠端存取木馬(RAT)。根據最近報導，該惡意軟體背後的參與者一直在使用惡意電子郵件作為最初的感染媒介。DarkWatchman 是一種普通的遠端存取木馬 (RAT)，但具有無檔案 (Fileless) 功能，因為它利用註冊表試圖減少被檢測到的機會。

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(Snoar)的防護：

- SONAR.DI!gen1

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.Gen.2
- Trojan.Gen.NPE
- Trojan Horse
- WS.Malware.1
- WS.Malware.2

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已於第一時間收錄於不安全分類列表中。

2021/12/15

TinyNuke 惡意軟體在最近針對法國組織的惡意行動中傳播

根據最近發布的一份報告，利用「TinyNuke」銀行惡意軟體的惡意行動在 2021 年一直存在，最近一次活動仍在 11 月活躍。據報導，散布行動的目標是各種法國實體和組織。該惡意軟體利用包含發票或金融等主題誘餌的惡意垃圾郵件活動進行傳播。「TinyNuke」惡意軟體可用於竊取憑證和用戶資訊等。

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- Trojan.Tinukebot
- Trojan.Tinukebot.B
- Trojan.Tinukebot.B!gm

基於行為偵測技術(Snoar)的防護：

- SONAR.SuspDataRun

基於機器學習的防禦技術

- Heur.AdvML.B
- 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。

2021/12/14

已有「Khonsari」勒索軟體，發動「Log4j」漏洞測探攻擊

利用「Log4j 漏洞 (CVE-2021-44228)」早期威脅與惡意挖礦程式和滲透測試工具 Cobalt Strike 相關。正在進行漏洞刺探利用中，最近增加一個名為「Khonsari」勒索軟體家族。監控其感染企圖的研究人員透露，與勒索軟體籌載一起，名為「Orcus」遠端存取木馬 (RAT) 被植入已被感染的電腦上。

該攻擊利用遠端程式碼執行 (RCE) 缺陷，從遠端伺服器下載額外的有效籌載，一個 .NET 的二進位檔案，被加密的檔案會以「.khonsari」的副檔名呈現。

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(Snoar)的防護：

- SONAR.Ransomware!g1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Downloader
- Ransom.Khonsari
- Trojan Horse
- Trojan.Gen.MBT

基於機器學習的防禦技術：

- Heur.AdvML.C

2021/12/14

Rook Ransomware「Rook」勒索軟體

最近名為「Rook」勒索軟體攻擊者越來越活躍。雖然與更惡名昭彰的勒索軟體參與者相比，它們的流行率仍然相對較低，但它們也採用可怕的雙重勒索戰術，這種戰術正在成為全球勒索軟體活動的主要手段。

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：

基於行為偵測技術(Snoar)的防護：

- Sonar.SuspLaunch!g18

檔案型(基於回應式樣本的病毒定義檔)防護：

- Downloader
- Trojan.Gen.MBT

2021/12/14

微軟 12 月安全更新修補的範圍與細節

12 月 14 日，微軟發布了他們定期安排的每月更新。在這次 12 月發布的版本，Microsoft 已修補了 67 個漏洞。 本月初也修補了另外 16 個與 Chromium 相關的漏洞。

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Exp.CVE-2021-43883 (renamed from Bloodhound.Exploit.843)

基於安全強化政策(適用於使用DCS)：

Symantec DCS 為 Windows Installer EOP 漏洞提供零時差保護。特別是 DCS 的 Windows 強化政策能有效攔截，不管是概念性驗證 (Proof of Concept；POC)或是發動真槍實彈的漏洞攻擊來覆寫 Windows 服務二進製檔案和 MSI 檔案的嘗試。

2021/12/14

間諜活動針對電信組織

以色列、約旦、科威特、沙烏地阿拉伯、阿拉伯聯合大公國、巴基斯坦、泰國和寮國的電信組織成為該行動的目標，該行動似乎沒有使用自定義惡意軟體，而是依賴合法工具、公開可用的惡意軟體和就地取材的戰術的組合。雖然攻擊者的身份仍未獲得證實，但有一些證據顯示與伊朗的 Seedworm（又名 MuddyWater）組織有聯繫。鎖定的目標和使用的戰術與伊朗贊助的攻擊者一致。

在我們的部落格中閱讀更多資訊：針對中東和亞洲電信組織的間諜行動。

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Hacktool
- Hacktool.Mimikatz
- Infostealer
- PUA.Gen.6
- Trojan Horse
- Trojan.Gen.2
- WS.Malware.1
- WS.Malware.2
- WS.SecurityRisk.1
- WS.SecurityRisk.3

2021/12/11(至2021/12/20 多次更新)

威脅警報：Apache Log4j 遠端程式碼執行(RCE)漏洞(CVE-2021-44228)，又名 Log4Shell

2021 年 12 月 20 日更新：*Apache 軟體基金會發布了針對 Log4j 中第三個漏洞的修補程式。在發現上一版本 (2.16) 存在問題後，該軟體的 2.17.0 版於 12 月 17 日發布。Apache 表示，2.16 並不能完全防止查找評估中的無限遞迴，且容易受到 CVE-2021-45105 (一種拒絕服務漏洞) 的攻擊。*

2021 年 12 月 15 日更新：*Apache 已修補 Log4j 中的第二個漏洞。該漏洞 (CVE-2021-45046) 源於上一個漏洞 (CVE-2021-44228) 的修復程序並未能在所有情況下完全阻止漏洞利用。該修補功能已在 Log4j 版本 2.16.0 中提供。*

最近披露 Apache Log4j 中一個嚴重的遠端程式碼執行 (RCE) 漏洞，並且現在對外提供多個概念證明。Log4j 是一個 Java 日誌庫，被大量應用程式和服務廣泛使用。Apache Log4j 的 2.0 和 2.14.1 版受到影響，並且已在 2.15.0 版中發布更新修補。這漏洞被安全社群稱為「Log4Shell」。

正如預期，攻擊者已經開始利用此漏洞，例如：挖礦殭屍網路背後的漏洞，Muhskit 就是其中之一。這種惡意軟體已經存在多年了，眾所周知，它被用於各種挖礦和分散式阻斷服務攻擊 (DDoS) 行動。

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：

基於行為偵測技術(Snoar)的防護：

- SONAR.Maljava!g7
- SONAR.Ransomware!g1
- SONAR.Ransomware!g31
- SONAR.Ransomware!g32
- SONAR.SuspLaunch!g184
- SONAR.SuspLaunch!g185

檔案型(基於回應式樣本的病毒定義檔)防護：

- CL.Suspexec!gen106
- CL.Suspexec!gen107
- CL.Suspexec!gen108
- Linux.Kaiten
- Miner.XMRig!gen2
- Ransom.Khonsari
- Ransom.Tellyouthepass
- Ransom.Tellyouthepa!g1
- Ransom.Tellyouthepa!g2
- Trojan Horse
- Trojan.Maljava

基機器學習的防禦技術：

- 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：

- Attack: Log4j2 RCE CVE-2021-44228
- Attack: Log4j2 RCE CVE-2021-44228 2
- Attack: Log4j CVE-2021-45046
- Attack: Malicious LDAP Response
- Audit: Log4j2 RCE CVE-2021-44228
- Audit: Malicious LDAP Response
- Audit: Suspicious Java Class File Executing Arbitrary Commands

基於安全強化政策(適用於使用DCS)：

DCS 針對此漏洞為伺服器工作負載提供了一系列保護：

- 可疑程序執行：預防政策集可防止惡意軟體被植入或在系統上執行。DCS 強化的 Linux 伺服器可防止從臨時或其他可寫位置執行惡意軟體，攻擊者使用這種技術在所報導的 log4shell 漏洞利用中植入 XMRig 等加密程式。
- 查看基於 log4j 應用程序沙箱的 Linux 代理執行清單，並新增，例如：*/curl、*/wget 等其他工具。攻擊者使用這些工具從受害者的 log4j 應用程序連接到外部 C2 伺服器以下載額外的有效籌載。
- DCS 的應用程式沙箱，可以保護 Windows 和 Linux 使用就地取材工具和篡改關鍵系統服務和資源的可疑程序執行。
- 網路控制：能夠阻止與網際網路的離埠連線，並限制來自伺服器工作負載和使用 log4j2 的容器化應用程序到內部可信系統所需的 LDAP、http 和其他流量。
- 檢測策略：系統攻擊檢測：Baseline_WebAttackDetection_Generic_MaliciousUserAgent 規則應更新為包含 *jndi:* 透過選擇字串 jndi:ldap、jndi:rmi、jndi:dns 等使用可疑的 jndi 查找嘗試警告惡意伺服器請求。確保設置 IDS Web 攻擊檢測選項中的 Web 伺服器存取日誌文件的路徑。應該為每個 log4j 應用程序日誌文件新增類似的自定義文本日誌規則。

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)：

我們的 Webpulse (網頁脈衝) 常態監視的流量也包含 Log4jShell 漏洞來提供另一層級的保護。

2021/12/10

新的 Mirai 變種鎖定 TP-Link 無線路由器漏洞

基於 Mirai 的殭屍網路行動的新變種——也稱為 MANGA 或 Dark--針對最近發布的 TP-Link 無線路由器遠端程式碼執行 (RCE) 漏洞 (CVE-2021-41653)。攻擊者利用該漏洞強制設備下載並執行惡意腳本，然後下載主要二進位檔(binary)有效載荷。TP-Link 已經為受影響的硬體版本 (TL-WR840N EU V5) 發布更新的韌體。

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.Mirai
- Trojan.Gen.NPE
- WS.Malware.1
- 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。

2021/12/10

被植入木馬的 Notepad++ 安裝程式，散布惡意軟體

發現被植入木馬的 Notepad++ 編輯器副本正在散布惡意軟體。該惡意軟體安裝包由一個已知的威脅行動者組織所散布，以提供鍵盤側錄和資訊竊取的有效籌載。被植入的惡意軟體具有鍵盤側錄功能，可將側錄的擊鍵轉儲到新建立的隱藏系統檔案中。第二個檔案監視這些新日誌並執行滲漏。此外，惡意軟體還可以從系統中竊取檔案和其他資料。

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.Gen.MBT

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。